

КОНКУРСНАЯ ДОКУМЕНТАЦИЯ
для участия в конкурсе
«Закупка серверного оборудования для МСС»

(117 листов)

Ташкент - 2020г.

BID DOCUMENTATION
for participation in the Bid
for supply of servers for MCC

(117 pgs.)

Tashkent 2020

СОДЕРЖАНИЕ

- Глава I.**
Объявление о проведении конкурса.
- Глава II.**
Инструкция Участникам Конкурса.
Общие сведения.
Порядок подачи Конкурсных предложений.
- Глава III.**
Порядок рассмотрения и оценки Конкурсных предложений.
- Глава IV.**
Критерии оценки.
- Глава V.**
Заключительные положения.
- Глава VI.**
Проект Контракта.

CONTENT

- Chapter I.**
Announcement of the contest.
- Chapter II.**
Instructions for Bid Participants.
General information.
Procedure for submission of Bid Proposals.
- Chapter III.**
Procedure of review and evaluation of bids.
- Chapter IV.**
Evaluation criterion.
- Chapter V.**
Final provisions.
- Chapter VI.**
Draft Contract.

I. Глава
ОБЪЯВЛЕНИЕ О ПРОВЕДЕНИИ КОНКУРСА

ООО «Uzbekistan GTL» (Заказчик) в рамках реализации инвестиционного проекта «Производство синтетического жидкого топлива на базе очищенного метана Шуртанского ГХК», объявляет конкурс на закупку серверного оборудования для МСС.

Конкурс проводится по адресу: 100060, Республика Узбекистан, г. Ташкент, Яшнабадский район, ул. Фаргона йули, д. 7Б, e-mail: Procurement2@gtl.uz

Конкурсная документация загружена на
<http://www.oltinyolgtl.com/russian/196/>

Контактное лицо Заказчика: Главный специалист по закупкам
Гумаров Тимур. Х.
(тел. +998 71 202 40 36)

Участники конкурса предоставляют свои предложения на русском языке.

К рассмотрению будут приняты конкурсные предложения в конвертах, опечатанные участниками конкурса, поступившие по вышеуказанному адресу в срок до 12-00 по местному времени «6» мая 2020 года.

Вскрытие конвертов с предложениями участников конкурса состоится в 16:00 местного времени «6» мая 2020 года по вышеуказанному адресу: Республика Узбекистан, г. Ташкент 100060, Яшнабадский район, ул. Фаргона йули, д. 7Б.

Разъяснения по конкурсной документации могут быть предоставлены после официального запроса на фирменном бланке участника с использованием средств почтовой или электронной связи по адресу: Procurement2@gtl.uz не позднее чем за пять дней до крайней даты подачи предложений.

Chapter I.
ANNOUNCEMENT OF BID

As part of implementation of the “Production of synthetic liquid fuel on the basis of purified methane of Shurtan GCC” Investment Project, ”Uzbekistan GTL” LLC (Client) announces Bid for supply of servers for MCC.

The Bid will be held at the following address: the Republic of Uzbekistan, Tashkent, 100060, Yashnabad district, Fargona Yuli str., 7b, E-mail: Procurement2@gtl.uz.

Bid documentation is uploaded to
<http://www.oltinyolgtl.com/russian/196/>

The Client’s contact person: Chief Procurement Specialist –
Gumarov Timur
(tel.+998 71 202 40 36)

The participants of the Bid shall provide their proposals in Russian.

Proposals in envelopes sealed by participants of the Bid, received at the above address until 6 of May 2020 12:00 p.m., will be accepted for consideration.

Opening of the envelopes with the participants’ proposals will be held on 6 of May 2020 at 16:00 at the above address: the Republic of Uzbekistan, Tashkent, 100060, Yashnabad district, Fargona Yuli str., 7b.

Clarification on the Bid documentation could be received after official request submitted on the participant’s letterhead using postal or electronic communication to e-mail address: Procurement2@gtl.uz no later than 5 days before the deadline of offer’s submission.

Participants of the Bid have the right to take part in opening of proposals.

Участники конкурса, имеют право принять участие во вскрытии предложений.

Просим участников перед подачей конкурсных предложений проверять их на предмет соответствия конкурсной документации Заказчика.

We request the participants to check their bid proposals for compliance with the Client's Bid documentation prior to submission.

II. Глава Инструкция Участникам Конкурса

1. Общие сведения

ООО «Uzbekistan GTL» (Заказчик) в рамках реализации инвестиционного проекта «Производство синтетического жидкого топлива на базе очищенного метана Шуртанского ГХК», объявляет конкурс на закупку серверного оборудования для МСС.

Конкурс проводится по адресу: Республика Узбекистан, г. Ташкент 100060, Яшнабадский район, ул. Фаргона йули, д. 7Б, e-mail: Procurement2@gtl.uz

Конкурсная документация загружена на
<http://www.oltinyolgtl.com/russian/196/>

Контактное лицо Заказчика: главный специалист по закупкам Гумаров Т.Х.
(тел. +998 71 202 40 36)

Разъяснения по конкурсной документации могут быть предоставлены после официального запроса на фирменном бланке участника с использованием средств почтовой или электронной связи по адресу: Procurement2@gtl.uz не позднее чем за пять дней до крайней даты подачи предложений.

2. Порядок подачи Конкурсных предложений

2.1. Конкурсное предложение, подготовленное Поставщиком (далее по тексту Участник конкурса), а также вся корреспонденция и документация, связанная с этим предложением, **должны быть оформлены на русском языке**. Участник торгов может представить свое предложение на другом языке при условии предоставления предложения с заверенным переводом на русский язык, в соответствии с требованиями **пункта 2.8** настоящей Конкурсной документации. **Не предоставление перевода не является поводом для дисквалификации участников конкурса.**

Chapter II Instruction for the Bid Participants

1. General Provisions

As part of implementation of the “Production of synthetic liquid fuel on the basis of purified methane of Shurtan GCC” investment project, Uzbekistan GTL LLC (Client) announces Bid for supply of servers for MCC.

The Bid will be held at the the following address: the Republic of Uzbekistan, Tashkent, 100060, Yashnabad district, Fargona Yuli str., 7b, E-mail: Procurement2@gtl.uz

The Bid documentation is uploaded to
<http://www.oltinyolgtl.com/russian/196/>

The Client’s contact person: Chief Procurement Specialist – Timur Gumarov
(tel.+998 71 202 40 36)

Clarification on the Bid documentation could be received after official request submitted on the participant’s letterhead using postal or electronic communication to e-mail address: Procurement2@gtl.uz no later than 5 days before the deadline of offer’s submission.

2. Procedure for submission of proposals

2.1. The bid proposal prepared by the Supplier (hereinafter referred to as the Participant of the Bid), as well as all correspondence and documentation related to this proposal, **must be issued in Russian**. The bid participant may submit offer in another language, subject to the submission of a proposal with a certified translation into Russian, in accordance with the requirements of Clause 2.8 of this Bid documentation. **Failure to provide translation is not a reason for disqualification of bidders.**

2.2. Цена Товара должна указываться в национальной валюте (для резидентов), для иностранных компаний (для нерезидентов) указывается в долларах США.

Примечание: Заказчик в соответствии с постановлением Президента Республики Узбекистан от 29.12.2016 г. № ПП-2706 и постановлением Кабинета Министров Республики Узбекистан от 06.10.2017 г. № 803 освобожден от уплаты таможенных платежей (за исключением сборов за таможенное оформление), в соответствии с постановлением Президента Республики Узбекистан от 16.07.2018г. № ПП-3857 не является плательщиком НДС.

2.3. Последний срок подачи Конкурсных предложений: до 12-00 местного времени «6» мая 2020 года. К рассмотрению будут приняты Конкурсные предложения, поступившие до истечения срока, по адресу: Республика Узбекистан, г. Ташкент 100060, Яшнабадский район, ул. Фаргона йули, д. 7Б.

2.4. Конкурсные предложения, поступившие по почте после 12-00 местного времени «6» мая 2020 года, приниматься, вскрываться и рассматриваться не будут, независимо от причин опоздания. Предложения, полученные после истечения крайнего срока подачи предложений посредством почты, не вскрываются, и могут быть возвращены в течение 15 дней уполномоченному представителю, по истечению указанного срока. Заказчик не несет ответственность за их сохранность.

2.5. Конкурсная комиссия Заказчика вскрывает общий конверт с Конкурсными предложениями (по адресу: 100060, Республика Узбекистан, г. Ташкент, Яшнабадский район, ул. Фаргона йули, д. 7Б.) в 16-00 «6» мая 2020 года.

2.6. Представитель Участника конкурса, имеет право принять участие во вскрытии его Конкурсного предложения, для чего Участник конкурса должен до истечения срока подачи Конкурсных предложений подать заявление об его участии на вскрытии. Для присутствия на вскрытии представитель Участник конкурса должен представить документ, подтверждающий необходимые полномочия, участвовать от имени Участника конкурса (удостоверение или доверенность Участник конкурса).

2.7. Участник конкурса несет все расходы, связанные с подготовкой и подачей Конкурсного предложения. Заказчик не имеет обязательств и не несет ответственности за такие затраты.

2.2. Price of the Goods shall be indicated in national currency (for residents), and for foreign companies (for non-residents) it shall be specified in US Dollars.

Note: the Client is exempt from paying customs duties (except for customs clearance fees) in accordance with Decree of the President of the Republic of Uzbekistan dd. 29.12.2016 No.PP-2706 and Decree of the Cabinet of Ministers of the Republic of Uzbekistan dd. 06.10.2017 No. 803, and is not a VAT payer in accordance with Decree of the President of the Republic of Uzbekistan dd. 16.07.2018 No. PP-3857.

2.3. The deadline for submission of the Bid Proposals is until 12-00 p.m. local time on 6 of May 2020. The Bid Proposals which are received before the deadline to: the Republic of Uzbekistan, Tashkent, 100060, Yashnabad district, Fargona Yuli str., 7b, will be accepted for consideration.

2.4. The Bids received after 12-00 local time 6 of May 2020 will not be accepted, opened and considered regardless of the reasons of the delay. Proposals submitted by post mail after deadline will not be opened and could be returned back within 15 days to Representative of the Participants after expiry of the specified period. The Client shall not be responsible for their safety.

2.5. The Bid Committee of the Client shall open the common envelope with the Bid Proposals (at: the Republic of Uzbekistan, Tashkent, 100060, Yashnabad district, Fargona Yuli str., 7b.) at 16-00 on 6 of May 2020.

2.6. Representative of the Participant shall have the right to take part in opening procedure of its Bid Proposal, for which the Participant shall submit an application for its participation in the opening before the bid closing date. In order to attend the opening procedure, the representative of the Participant shall provide a document confirming the necessary powers to attend on a behalf of Participant. (Identity card or power of attorney of the Participant).

2.7. The Participant shall bear all costs related to preparation and submission of the Bid Proposal. The Client shall have no obligation or liability for such costs.

2.8. Конкурсное предложение должно находиться в запечатанном общем конверте, и включает:

- Общие и квалификационные сведения об Участнике конкурса;
- **конверт № 1** содержащий Техническое предложение Участника конкурса в одном экземпляре (оригинал), а также электронный носитель с копией Технического предложения в формате Microsoft Office.

- **конверт № 2** содержащий Коммерческое предложение Участника конкурса, подготовленное в соответствии с Приложением №3 к Конкурсной документации, в одном экземпляре (оригинал).

Общий конверт, конверты № 1 и 2 должны быть опечатаны и подписаны лицом (лицами), наделённым полномочиями для подписания Конкурсного предложения от имени Участника конкурса. **На всех конвертах должны быть обозначены номера конвертов, название конкурса и название Участника конкурса.**

Все страницы Конкурсного предложения должны быть подписаны лицом (лицами), подписавшим Конкурсные предложения, пронумерованы и прошиты.

Если наружный конверт не запечатан и не помечен в соответствии с вышеуказанными требованиями, Заказчик не несет никакой ответственности за утерю его содержимого.

Перечень документов, необходимых для участия в Конкурсе

Перечень документов общего конверта

1. Общие и квалификационные сведения об Участнике Конкурса (**Приложение 1 к Конкурсной документации**).
2. Копии действующих лицензий, разрешений, допусков, сертификатов на осуществляемые видов деятельности, необходимые для проведения поставок, выставленных на Конкурс, указанных в п.10 Технического задания.
3. Оригинал доверенности или **нотариально** заверенная копия доверенности лицу, подписавшему Конкурсное предложение, на право принимать обязательства от имени Участника конкурса, если такое лицо не наделено соответствующими полномочиями согласно учредительным документам Участника.
4. Копия свидетельства о регистрации юридического лица Участника.

2.8. The Bid Proposal shall be in a sealed common envelope, which includes:

- General and qualification information of the Bid Participant;
- **Envelope No. 1** containing a Technical proposal in one counterpart (original copy) and electronic media in one copy of Technical proposal in Microsoft Office format.

- **envelope No. 2** with a Commercial Proposal in accordance with Attachment #3 to Bid documentation in one counterpart (original copy);

The common envelope, envelopes 1 and 2 shall be sealed and signed by a person (s) authorized to sign the Bid Proposal on behalf of the Participant. **All envelopes shall bear the name of the Bid, envelope numbers and the name of Participant.**

All pages of the Bid Documentation shall be signed by the person (s) who signed the Bid Proposals, enumerated and stitched.

If the outer envelope is not sealed and marked in accordance with the above requirements, the Client shall not be liable for loss of its contents.

List of documents required for participation in the Bid

List of common envelope documents

1. General and qualification information of the Bid Participant (**Attachment 1 to the Bid Documentation**).
2. Copies of existing licenses, permits, permissions, and certificates for types of activities are required for deliveries which are put out to the Bid, as specified in clause 10 of the Technical Specification.
3. Original copy of power of attorney or a **notarized** copy of the power of attorney to the person who signed the Bid Proposal, for the right to accept obligations on behalf of the Bid Participant, if such person is not properly authorized according to the constituent documents of the Participant.
4. A copy of the registration certificate of the Participant's legal entity.

5. Оригинал банковской Гарантии безотзывности конкурсного предложения или копия поручения банка об обеспечении Гарантии безотзывности конкурсного предложения в денежной форме или обеспечительная сумма в размере 15000 (пятнадцать тысяч) долларов США в виде платежного поручения.

Перечень документов конверта «1»

1. Техническое предложение, составленное в соответствии с требованиями Технического задания (**Приложение №2 к Конкурсной документации**).

2. В конверт «1» также вкладывается электронный носитель (CD-R) с электронными версиями вложений конверта «1» в формате приложений стандартного конверта Adobe Acrobat (PDF) версий 5.0 и выше; возможно предоставление документов в формате .DOC.

Примечание: Документы, входящие в конверт «1», не должны содержать никакой информации относительно цены Конкурсного предложения. Все цены, тарифы и итоговые суммы, составляющие Предложение, должны содержаться только в документах конверта «2». При несоблюдении данного условия Участник дисквалифицируется.

Перечень документов конверта «2»

1. Ценовое предложение (Приложение 3).
2. Таблица цен (Приложение 3).

2.9. Участник конкурса в дополнение к поданному Конкурсному предложению может представить альтернативное предложение, которое является привлекательным с технической и/или коммерческой точки зрения и может предоставить Заказчику существенную экономию затрат. Данное предложение должно быть вложено в отдельный конверт с надписью «**Альтернативное предложение**».

2.10. Альтернативное предложение Участника конкурса, поданное без представления Конкурсного предложения, рассматриваться не будет.

2.11. Конкурсное предложение должно оставаться в силе в течение 90 (девяносто) дней с даты подачи предложения. При необходимости, заказчик может отправить запрос о продлении срока действия предложения на определенный период, требуемый для оценки предложений. Это должно быть подтверждено представленной участником Конкурса Гарантией безотзывности конкурсного предложения, в случае предоставления

5. The Bank guarantee (original copy) of the irrevocability of Bid or a copy of the bank's order to secure the guarantee of the irrevocability of Bid in cash or a security amount in the amount of 15,000 (fifteen thousand) US Dollars in payment order format.

The list of documents of envelope 1

1. Technical proposal drawn up in accordance with requirements of Technical Specification (**Attachment 2 to the Bid Documentation**).

2. Envelope 1 shall also include an electronic media (CD-R) with electronic versions of Envelope 1 inclusions in the format of standard Adobe Acrobat (PDF) 5.0 and higher; documents in .DOC. format can also be submitted.

Note: Documents included in Envelope 1 must not contain any information regarding the Bid price. All prices, tariffs, and totals that make up the Proposal must be contained only in documents of Envelope 2. Failure to satisfy this condition leads to disqualification of the Participant.

List of documents of Envelope 2

1. Price proposal (Attachment 3).
2. Price table (Attachment 3).

2.9. In addition to the submitted Bid Proposal, the Bid Participant may submit an alternative proposal that is technically and/or commercially attractive and may deliver substantial cost savings to the Client. This proposal shall be enclosed in a separate envelope marked as “**Alternative proposal**”.

2.10. An Alternative Proposal submitted by a bidder without a Bid Proposal will not be considered.

2.11. The bid proposal must remain valid for 90 (ninety) days from the date of submission of the proposal. If necessary, the customer can send a request to extend the validity period of the proposal for a certain period required for the evaluation of proposals. This must be confirmed by the guarantee of irrevocability of the bid submitted by the bidder, if the guarantee provides irrevocability of the bid in cash, this amount will be withheld until the expiration of the above period.

Гарантией безотзывности конкурсного предложения в денежной форме, то данная сумма будет удерживаться до истечения вышеуказанного срока.

2.12. Гарантия безотзывности конкурсного предложения в размере 15 000 (пятнадцать тысяч) долларов США может быть представлена до даты вскрытия конкурсной комиссией Заказчика конвертов:

- в виде банковской гарантии;
- в денежной форме путем перечисления на расчетный счет Заказчика, по следующим реквизитам:

Юридическое лицо: ООО "Uzbekistan GTL"

Адрес юр. лица: Республика Узбекистан, г. Ташкент 100060, Яшнабадский район, ул. Фаргона йули, д. 7Б.

ИНН: 207041936

ОКЭД: 35210

Банк: Головной офис АКБ "Асака"

Адрес банка: 100015, г. Ташкент, Мирабадский р-н, ул. Нукусская, д. 67, тел.: (+99871) 120-82-10, (+99871) 200-55-22

МФО: 00873

ИНН: 201589828

р/с в нац.валюте 2021 4000 7048 1968 0008

р/с в ин.валюте USD 2021 4840 5048 1968 0011

SWIFT код: ASBKUZ22

Детали платежа: Гарантия безотзывности конкурсного предложения для участия в Конкурсе «**Закупка серверного оборудования для МСС**»

2.13. Гарантия считается предоставленной после поступления от уполномоченного банка Заказчика подтверждения о зачислении необходимой суммы денежных средств на расчетный счет Заказчика, не позднее срока подачи Конкурсных предложений. Резиденты Республики Узбекистан вправе представить указанную Гарантию в национальной валюте, сумма которой рассчитывается по текущему обменному курсу Центрального Банка РУз на день оформления Гарантии. Участники, которые предоставляют оригинал Банковской гарантии на фирменном бланке Банка, должны обеспечить отправку SWIFT-сообщения в формате MT 799 от банка, выпустившего гарантию. Данное SWIFT-сообщение должно содержать информацию, подтверждающую выпуск банковской гарантии в размере и на срок, указанном в настоящей конкурсной документации. **Конкурсное**

2.12. The guarantee of irrevocability of the bid proposal in the amount of 15,000 (fifteen thousand) US dollars could be submitted to the date of opening of envelopes by Client's Bid committee:

- in the form of a bank guarantee;
- in cash by transfer to the Customer's bank account, at the following details:

Legal Name: Uzbekistan GTL LLC

Address: 7B, Fargona Yuli, Yashnabad district, Tashkent 100060, Republic of Uzbekistan.

TIN: 207041936

OKED: 35210

Bank: Head office of JSCB "Asaka"

Bank address: 100015, Tashkent, Mirabad district, ul. Nukusskaya, 67, tel. : (+99871) 120-82-10, (+99871) 200-55-22

MFI: 00873

ITN: 201589828

Account No (sum) 2021 4000 7048 1968 0008

Account No USD 2021 4840 5048 1968 0011

SWIFT: ASBKUZ22

Payment Details: Guarantee of irrevocability of the Bid for participation in the Bid "**Supply of servers for MСС**"

2.13. The guarantee is considered to be provided after receipt of confirmation from the authorized bank of the Customer about the crediting of the necessary amount of funds to the Customer's bank account, no later than the deadline for submission of Bids. Residents of the Republic of Uzbekistan are entitled to submit the specified Guarantee in national currency, the amount of which is calculated at the current exchange rate of the Central Bank of Uzbekistan at the date of issue of the Guarantee. Participants who provide the original Bank guarantee on Bank's letterhead must ensure that the SWIFT message is sent in MT 799 format from the bank that issued the guarantee. This SWIFT message must contain information confirming the issuance of a bank guarantee in the amount and for the period specified in this bid documentation. The Bid of the Participant, which submitted a copy of the Bank guarantee of the Bid Application, is rejected. A bank guarantee must be valid for 30 (thirty) days

предложение Участника, представившего копию Банковской гарантии обеспечения Конкурсной заявки, отклоняется. Банковская гарантия должна быть действительна в течение 30 (тридцати) дней после истечения срока действия Конкурсной заявки (всего 120 (сто двадцать) дней с момента вскрытия конвертов с Конкурсными предложениями).

Обеспечения Конкурсных заявок, представленные в форме ОРИГИНАЛА Банковской гарантии на фирменном бланке Банка, возвращаются проигравшим Участникам конкурса в течение 5 (пяти) дней после окончания срока действия их Банковских гарантий.

2.14. Гарантия безотзывности конкурсного предложения подлежит возврату:

- участникам Конкурса, которые не определены в качестве победителя или резервного победителя, по истечении 5 (пяти) рабочих дней после завершения конкурса;
- победителю Конкурса после подписания с ним Контракта и представления им Гарантии Исполнения Контрактных Обязательств;
- резервному победителю после подписания контракта с победителем Конкурса;
- в случае отмены конкурсных торгов.

2.15. Гарантия безотзывности конкурсного предложения не возвращается в следующих случаях:

- участник Конкурса необоснованно отзывает свое предложение, либо вносит изменения после истечения срока подачи конкурсных предложений;
- участникам Конкурса, в отношении конкурсных предложений которых выявлены признаки корпоративного сговора, что могло повлиять на выбор победителя Конкурса;
- участникам Конкурса, представившим подложные документы;
- победитель Конкурса своевременно не подписал Контракт с Заказчиком и/или не представил Заказчику Гарантию исполнения контрактных обязательств.

2.16. Участник Конкурса несет все расходы по представлению Гарантии безотзывности конкурсного предложения, а также по возврату суммы Заказчиком Гарантии безотзывности конкурсного предложения, внесенной в денежной форме. Участник торгов несет все расходы, связанные с подготовкой и подачей своего Конкурсного предложения. Заказчик ни в коем

after the expiration of the Bid Application (a total of 120 (one hundred twenty) days from the moment of opening the envelopes with the Bids).

Provision of Bid applications submitted in ORIGINAL copy of Bank Guarantee on the Bank's letterhead shall be returned to lose participants within 5 (five) days after the expiration of their Bank guarantees.

2.14. The irrevocability guarantee of the bid proposal is refundable:

- to participants of the Bid who are not defined as the winner or reserve winner, after 5 (five) business days after the completion of the Bid;
- to the winner of the Bid after signing the Contract with him and submitting to him the Guarantee for the Performance of Contractual Obligations;
- to the reserve winner after signing the contract with the winner of the Bid;
- in case of cancellation of competitive bidding.

2.15. The irrevocability guarantee of the bid proposal is not returned in the following cases:

- the bidder unreasonably withdraws his proposal, or make changes after the deadline for submitting bid proposals;
- participants of the Bid, in relation to the competitive offers of which signs of corporate conspiracy were revealed, which could affect the choice of the winner of the Bid;
- Participants of the Bid who submitted false documents;
- the winner of the Bid did not sign the Contract with the Customer on time and / or did not provide the Customer with the Guarantee of Contractual Obligations.

2.16. The Bidder shall bear all expenses for the presentation of the Guarantee of the Irrevocability of the bid proposal, as well as for the return of the amount by the Customer of the Guarantee of the Irrevocability of the bid proposal, made in cash. The Bidder shall bear all expenses associated with preparation and submission of the Bid. The Client shall in no case be liable or liable for these costs, regardless of the nature of the conduct and results of the bidding.

случае не отвечает и не несет обязательств по этим расходам, независимо от характера проведения и результатов торгов.

III. Глава

3. Порядок рассмотрения и оценка Конкурсных предложений

3.1. Рассмотрение, вскрытие и оценка предложений участников Конкурса, осуществляется в два этапа:

I этап – общая квалификационная оценка и техническая оценка;

II этап – коммерческая оценка.

3.2. На I этапе Конкурсная комиссия Заказчика:

- вскрывает общий конверт участников Конкурса;
- проверяет содержимое конверта на предмет его комплектности;
- проводит квалификационную оценку Участников конкурса.
- вскрывает конверты № 1 предложений Участников конкурса;
- проверяет содержимое конвертов № 1 на предмет их комплектности;
- проводит техническую оценку конкурсных предложений на предмет их соответствия требованиям Технического задания Заказчика (Приложение № 2 к Конкурсной документации);
- определяет Участников конкурса, предложения которых считаются соответствующими требованиям Технического задания Заказчика на основе Приложения №1 к Техническому заданию, указанной в Приложении № 2 к Конкурсной документации.

3.3. Предложения участников Конкурса, которые соответствуют требованиям Технического задания Заказчика, передаются на II этап.

3.4. На II этапе Конкурсная комиссия Заказчика:

- вскрывает конверт № 2 с коммерческими предложениями Участников конкурса - победителей I этапа;
- проверяет содержимое конвертов № 2 на предмет их комплектности;
- проводит коммерческую оценку коммерческих предложений на предмет их соответствия требованиям проекта Контракта (Приложение № 4 к Конкурсной документации), содержания спецификации и приемлемость цены по отношению к представленным техническим решениям;

Chapter III

3. The procedure of review and evaluation of the proposals

3.1. Proposals of the Bid Participants shall be reviewed and evaluated in two stages:

Stage I-general qualification evaluation & technical assessment;

Stage II-commercial evaluation.

3.2. At Stage I, the Client's Bid Commission shall:

- open the common envelope of the Bid Participants;
- check the contents of the Common envelope for completeness;
- conduct a qualification assessment of the Bid Participants.
- open Envelope 1 of the Bid Participants proposals;
- check contents of Envelopes 1 for completeness;

- conduct technical evaluation of the bids for their compliance with requirements of the Client's Technical Specification (Attachment 2 to the Bid Documentation);

- determine the Bid Participants whose proposals are considered to meet requirements of the Client's Technical specification based on Attachment 1 to Technical Specification specified in Attachment 2 to the Bid Documentation.

3.3. Proposals of the Bid Participants which meet requirements of the Client's Technical specification shall be passed to Stage II.

3.4. At Stage II, the Bid Commission of the Client shall:

- open envelope 2 with commercial proposals of the Bid Participants -winners of Stage I;
- check contents of Envelopes 2 for completeness;
- conduct commercial evaluation of commercial proposals for their compliance with requirements of the Draft Contract (Attachment 4 to the Bid Documentation), content of specification and affordability in terms of presented technical solutions;
- determine the winner of Bid which offered the best conditions for performance of the Contract based on criteria specified in Article #5 of the Bid Documentation;

- определяет победителя конкурса, предложившего лучшие условия исполнения контракта на основе критериев согласно Главе №5 Конкурсной документации;
- по усмотрению, определяет резервного исполнителя, предложение которого по решению Конкурсной комиссии признано наилучшим после предложения победителя конкурса.

Примечание. Конверт № 2 с коммерческим предложением Участников конкурса, не прошедших I этап, не вскрываются и возвращаются Участникам конкурса.

IV. Глава 4. Критерии оценки

4.1. Конкурсные предложения оцениваются Конкурсной комиссией, на соответствия требованиям Заказчика, включая технической части Конкурсного предложения на первом этапе оценки, а также предлагаемой цены Конкурсного предложения и с учетом предлагаемых сроков, объёма и качества поставляемого Товара на втором этапе оценки.

4.2. При этом, оцениваются только те Конкурсные предложения, которые признаются соответствующими требованиям Конкурсной документации на каждом этапе.

4.3. Конкурсные предложения, признанные несоответствующими требованиям Конкурсной документации, могут быть отклонены Конкурсной комиссией на любом этапе конкурса.

Квалификационные и Технические критерии оценки

Предложение, отраженное в первом конверте будет оцениваться закупочной комиссией на соответствие условиям конкурсной документации, в том числе Техническому заданию.

Не соответствующие требованиям технического задания, не будут рассматриваться и допускаться к оценке коммерческой части, если такие отклонения, по решению закупочной комиссии существенно будут влиять на поставку качественного товара и сопутствующих услуг.

Коммерческая оценка

Победителем признается участник конкурса, чье предложение признано соответствующим техническим требованиям и предложивший наилучшую

- At its discretion, determine backup Contractor whose proposal is recognized the best after proposal of the winner of the Bid, by the decision of the Bid Commission.

Note. Envelope 2 containing commercial proposal of the Bid Participant who have not passed Stage I, shall not be opened and shall be returned to the Bid Participants.

Chapter IV. 4. Criteria of Evaluation

4.1. The Bid Proposals shall be evaluated by the Bid Commission based on Client's requirement including technical part of the Bid Proposal on first stage, as well as the proposed Bid price on second stage taking into account the proposed terms, volume, and quality of the Goods to be delivered.

4.2. At this, only those Bid Proposals shall be evaluated which are recognized as meeting the requirements of the Bid Documentation on each stage.

4.3. Bid proposals which are found not meeting the requirements of the Bid Documentation may be rejected by the Bid Commission.

Qualification & Technical evaluation criteria

Proposal reflected in common envelope and Envelope #1 will be evaluated by Bid commission for compliance of Bid documentation, including Technical Specification.

Technical proposals not meeting the requirements of the Technical specification will not be reviewed and will not be admitted to evaluation of the commercial part if such deviation found by Bid commission will influence on supply of quality Goods and related services.

Commercial evaluation

Bid Participant whose proposal is recognized as meeting the technical requirements and which offered the best price for the required Goods volume and delivery time, and accepting the terms of the Contract shall be recognized the winner of the Bid (Attachment 4).

цену на требуемый объем и сроки поставки Товара, с принятием условий контракта (приложение №4).

V. Глава

5. Заключительные положения

5.1 Заказчик заключает контракт с победителем Конкурса и после его подписания все предшествующие переговоры и переписка по нему теряют силу.

5.2 Решения конкурсной комиссии указываются в соответствующих протоколах ее заседаний.

5.3 Заказчик заключает контракт с победителем Конкурса, с момента подписания которого победитель Конкурса должен представить Заказчику Гарантию обеспечения исполнения контрактных условий в размере 5 % стоимости Контракта, которая может быть в виде в виде банковской гарантии либо в виде внесения денежных средств на расчетный счет Заказчика.

VI. Глава

6. Проект контракта

6.1. К настоящей Конкурсной документации прилагается проект Контракта, который подпишут Заказчик и победивший Участник.

6.2. По истечению срока подачи конкурсных предложений, все комментарии к проекту Контракта не допускаются и не принимаются. Победивший Участник обязан подписать Контракт, на условиях оговоренных в конкурсной документации и в предложении Участника конкурса.

Chapter V

5. Final provision

5.1. The Client shall enter into the Contract with the winner of the Bid, and after its execution all previous negotiations and correspondence on the Contract shall become invalid.

5.2. Decisions of the Bid Commission shall be set out in respective minutes of its meetings.

5.3. The client signs a contract with the winner of the Bid and from the date of its signing the winner must provide to the Client a Guarantee of performance bond in amount of 5 % of the amount of the Contract, which can be in the form of Bank guarantee or depositing cash to the account of the Customer.

Chapter VI

6. Draft Contract

6.1. This Bid Documentation is accompanied by a draft Contract which will be signed by the Client and the winning Participant.

6.2. After bid closing date, no comments to the draft Contract shall be allowed or accepted. The winning Bidder shall sign the Contract based on terms stated in Bid documentation and in accordance with proposal of Participant.

Общие сведения.

| | |
|---|--|
| Наименование юридического лица | |
| Организационно-правовая форма | |
| Юридический (почтовый) адрес | |
| Фактическое местонахождение. | |
| Телефон | |
| Факс | |
| e-mail | |
| Контакт | |
| Место регистрации | |
| Год регистрации | |
| Банковские реквизиты | |
| Форма собственности (с государственная, частная, с гос. участием) | |
| Номер и дата сертификата об аккредитации | |
| ИНН | |
| ОКЭД | |

General information.

| | |
|--|--|
| Name of Legal entity | |
| Organizational and legal form | |
| Legal (postal) address | |
| Actual location | |
| Phone | |
| Contact | |
| E-mail | |
| Fax | |
| Place of registration | |
| year of registration | |
| Bank details | |
| Form of ownership (JV, state, private, with state participation) | |
| Number and date of certificate of accreditation | |
| TIN | |
| OKED | |

Достоверность всех представленных данных подтверждаем, и сообщаем о согласии участвовать в конкурсе «**Закупка серверного оборудования для МСС**» в соответствии с требованиями Конкурсной документации.

We confirm credibility of all the data submitted and inform you of our consent to participate in the Bid for “**supply of servers for MCC**” in accordance with requirements of the Bid Documentation.

| | |
|---------------------------------|--|
| Наименование Участника Конкурса | |
| Адрес | |

Name of the Bid Participant
Address

Руководитель
м.п.

Ф.И.О.

Director
(seal)

Full Name

Квалификационные сведения.

1. Сведения о документах дающих право на осуществление видов деятельности, (лицензия).

| | Название документа | № документа | Область применения | Дата выдачи | Срок действия |
|--|--------------------|-------------|--------------------|-------------|---------------|
| | | | | | |

2. К участнику Конкурса предъявляются следующие квалификационные требования, которые он обязан подтвердить необходимыми документами:

3. Свидетельство о регистрации юридического лица;

4. Правомочность лица, уполномоченного на заключение контракта (приказ или решение о назначении директора, Устав или доверенность);

5. Сведения о текущих или планируемых в 2020 г. процедурах ликвидации/банкротства/реорганизациях Участника (слиянии, разделении, присоединении и т.д.).

6. Сведения об отсутствии участника задолженности по уплате налогов и других обязательных платежей. (Справка налоговой инспекции);

7. Отсутствие введенных в отношении участника процедур банкротства (справка банка).

8. Отсутствие нахождения в состоянии судебного разбирательства с Заказчиком и/или его аффилированными лицами;

Information of Qualification

1. Information about documents which give the right to perform activities (licensing).

| | Document name | Document number | Scope | Issue date | Expiration date |
|--|---------------|-----------------|-------|------------|-----------------|
| | | | | | |

2. The following qualification requirements to the Bid participant, which they must confirm with necessary documents:

3. Certificate of registration of the legal entity;

4. Competence of the person authorized to enter into the Contract (order or decision of Director appointment, Charter or power of attorney);

5. Information about current or planned liquidation/bankruptcy/reorganization procedures of the Participant in 2020 (merger, division, consolidation, etc.).

6. Information about absence of tax arrears and other mandatory payments due by the Participant. (Certificate from tax Committee).

7. The absence of bankruptcy procedures introduced against the participant (bank certificate).

8. The absence of a state of litigation with the Customer and / or its affiliates;

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Закупка серверного оборудования, сетевого оборудования и систем безопасности для МСС (main computing center) в г. Ташкенте, узлов связи строительной площадки на территории Кашкадарьинской области Республики Узбекистан – KFCS (karshi factory computing site), KVCS (karshi village computing site).

1. Заказчик: ООО «Uzbekistan GTL», ул. Фаргона йули, дом 7Б, 100060, г. Ташкент, Республика Узбекистан, тел.: +99871 2024080, факс: +99871 2024051.

2. Наименование объекта: офис ООО «Uzbekistan GTL» ул. Фаргона йули, дом 7Б, 100060, г. Ташкент, Республика Узбекистан.

3. Основание для закупки товаров: в соответствии с постановлением Президента Республики Узбекистан № ПП-2706 от 29.12.2016 г. для производства в Республике Узбекистан синтетического жидкого топлива из очищенного метана Шуртанского ГХК осуществляется строительство завода.

4. Цель приобретения товаров: в целях проведения дальнейшей модернизации информационно-коммутиционных технологий, а также внедрения передовых систем осуществляется полная модернизация действующего центра обработки данных с учетом текущих и будущих потребностей в вычислительных мощностях.

5. Источники финансирования: Собственные средства Заказчика и/или кредитные средства в рамках инвестиционного проекта «Производство синтетического жидкого топлива на базе очищенного метана Шуртанского ГХК».

6. Описание товара и его технические характеристики:

| № | Наименование товарной позиции | Кол-во | Техническое описание | Примечание |
|----------------------------------|-------------------------------|--------|----------------------|---|
| Сегмент - Серверное оборудование | | | | |
| 1 | Сервера SRVVM | 10 шт | Приложение №1 | Не допускается предложение разных |

TECHNICAL SPECIFICATION

Purchase of server equipment, network equipment and security systems for MCC (main computing center) in Tashkent, communication nodes of the construction site in Kashkadarya region of Uzbekistan - KFCS (karshi factory computing site), KCCS (karshi village computing site).

1. The customer: "Uzbekistan GTL" LLC, Fargona Yuli str., 7B, 100060, Tashkent, Republic of Uzbekistan, phone: +99871 2024080, fax: +99871 2024051.

2. Name of the object: the office of LLC "Uzbekistan GTL" str. 7B Fargona Yuli street, 100060, Tashkent, Republic of Uzbekistan.

3. Basis for purchase of goods: in accordance with the Decree of the President of the Republic of Uzbekistan № PP-2706 of 29.12.2016 for the production of synthetic liquid fuel from purified methane in the Republic of Uzbekistan Shurtan MCC is building a plant.

4. Purchase of goods: in order to further upgrade information and communication technologies as well as to introduce advanced systems, the existing data centre is being fully upgraded to meet current and future computing capacity requirements.

5. Sources of financing: Own funds of the Customer and/or credit funds under the investment project "Production of synthetic liquid fuel based on purified methane at Shurtanskiy MCC".

6. Description of the product and its technical characteristics:

| № | Product Position Name | Q-ty | Technical description | Note |
|---|-----------------------|------|-----------------------|------|
| | | | | |

| | | | | |
|---------------------------------------|---|---------|----------------|--|
| 2 | Сервера SRVRVM | 2 шт | Приложение №2 | производителей оборудования в рамках одного сегмента |
| 3 | Сервера SRVRS | 3 шт | Приложение №3 | |
| 4 | Система виртуализации DCVRTM | 1 комп | Приложение №4 | |
| Сегмент - Сетевое оборудование | | | | |
| 5 | Коммутатор SWCRAG | 6 шт | Приложение №5 | Не допускается предложение разных производителей оборудования в рамках одного сегмента |
| 6 | Коммутатор SWAG | 1 шт | Приложение №6 | |
| 7 | Коммутатор MGMT | 2 шт | Приложение №7 | |
| 8 | Коммутатор доступа SWACS24 | 16 шт | Приложение №8 | |
| 9 | Коммутатор доступа SWACS48 | 6 шт | Приложение №9 | |
| 10 | Аксессуары SWACSKIT | 1 комп. | Приложение №10 | |
| 11 | Система управления и мониторинга SWMGMT | 1 комп. | Приложение №11 | |
| Сегмент - Сетевая безопасность | | | | |
| 12 | Файрвол FWMCC | 2 шт | Приложение №12 | Не допускается предложение разных производителей оборудования в рамках одного сегмента |
| 13 | Файрвол FWRS | 2 шт | Приложение №13 | |
| 14 | Файрвол FWUP | 1 шт | Приложение №14 | |

| | | | | |
|-----------------------------------|---|---------|--------------|--|
| 1 | SRVVM Servers | 10 pcs. | Annex No. 1 | It is not allowed to offer different equipment manufacturers within the same segment |
| 2 | SRVRVM Servers | 2 pcs. | Annex No. 2 | |
| 3 | SRVRS Servers | 3 pcs. | Annex No. 3 | |
| 4 | DCVRTM Virtualization System | 1 comp | Annex No. 4 | |
| 5 | Switchboard SWCRAG | 6 pcs. | Annex No. 5 | It is not allowed to offer different equipment manufacturers within the same segment |
| 6 | Switchboard SWAG 1 each | | Annex No. 6 | |
| 7 | Switchboard MGMT 2 pcs | | Annex No. 7 | |
| 8 | SWACS24 Access Switch 16 pcs. | | Annex No. 8 | |
| 9 | SWACS48 Access Switch 6 pcs. | | Annex No. 9 | |
| 10 | SWACSKIT Accessories 1 comp. | | Annex No. 10 | |
| 11 | Management and Monitoring System SWMGMT 1 comp. | | Annex No. 11 | |
| Segment - Network Security | | | | |

| | | | | |
|-------------------------|----------------------------------|--------|----------------|--|
| 15 | Песочница SNDBX | 1 шт | Приложение №15 | |
| 16 | Управление безопасностью SECMGMT | 1 комп | Приложение №16 | |
| Сегмент - Прочие | | | | |
| 17 | Шкаф телекоммуникационный RCKRS | 2 шт | Приложение №17 | |

| | | | | |
|-------------------------|---|--------------|--|--|
| 12 | Firewall FWMCC 2 pcs. | Annex No. 12 | | It is not allowed to offer different equipment manufacturers within the same segment |
| 13 | Firewall FWRS 2 pcs. | Annex No. 13 | | |
| 14 | Firewall FWUP 1 each | Annex No. 14 | | |
| 15 | Sandbox SNDBX 1 each | Annex No. 15 | | |
| 16 | Security Management SECMGMT 1 set | Annex No. 16 | | |
| Segment - Others | | | | |
| 17 | Telecommunication RCKRS cabinet 2 pcs. | Annex No. 17 | | |

. Поставщик должен обеспечить пуско-наладку оборудования и программного обеспечения, поставляемого в рамках настоящего технического задания учитывая при этом общую схему развертывания, указанную в Приложении №18.

. Подписка на функционал файрволов должна составлять 36 месяцев с момента поставки.

. Сервера SRVVM, SRVRVM, SWACS24, SWACS48 и MGMT должны быть одной модели с идентичными комплектующими.

. Файрволы FWMCC и FWRS должны быть одной модели с идентичными комплектующими.

. Коммутаторы SWCRAG, SWACS24, SWACS48 и MGMT должны быть

The Supplier shall ensure the commissioning of the equipment and software supplied as part of this assignment, taking into account the general deployment scheme as specified in Annex No. 18.

The subscription to the firewall functionality should be 36 months from the date of delivery.

The SRVVM, SRVRVM, SWACS24, SWACS48 and MGMT servers must be the same model with identical components.

WMCC and FWRS firewalls must be the same model with identical components.

одной модели с идентичными комплектующими.

- Все оборудование должно работать от напряжения в сети 220V $\pm 5\%$, выходное напряжение UPS 220V $\pm 5\%$, при температуре воздуха 10-30°C, и относительной влажности 15-80 %
- Все оборудование поставляется и устанавливается «под ключ»: инсталляция оборудования, запуск оборудования и системного программного обеспечения (холодный старт всей системы)
- Аксессуары. Должен быть представлен полный заводской комплект для инсталляции и запуска в эксплуатацию в головном вычислительном центре и удаленных сайтах всего набора оборудования. Участник обязан предоставить список заводского комплекта аксессуаров, дополнительно поставляемых аксессуаров, а также письменное подтверждение достаточности представленных аксессуаров для монтажа, подключения и запуска комплекса оборудования
- Все оборудование должно устанавливаться в телекоммуникационные шкафы 19" типоразмера.
- Система удаленного аппаратного управления всех серверов должна быть одинаковой на всех серверах и интегрируемой в отдельную сетевую инфраструктуру для безопасности управления
- Система удаленного управления всех коммутаторов должна быть одинаковой на всех коммутаторах и интегрируемой в отдельную сетевую инфраструктуру для безопасности управления
- Система удаленного аппаратного управления всех фаерволов должна быть одинаковой на всех коммутаторах и интегрируемой в отдельную сетевую инфраструктуру для безопасности управления
- Поставляемое серверное оборудование должно быть обеспечено:
 - управление сбоями (информация о сбое, анализе ошибок, сбор статистической информации, восстановление данных после сбоя);
 - управление конфигурацией (хранение конфигураций серверов, отслеживание их изменений, наблюдение за системой).
- Производитель должен иметь свою зарегистрированную марку и присутствовать на рынке ИТ не менее 10 лет до даты подачи предложения.
- Участник должен иметь авторизацию от производителя Товара (услуги) на

Switches SWCRAG, SWACS24, SWACS48 and MGMT must be the same model with identical components.

All equipment should operate at 220V $\pm 5\%$ network voltage, UPS 220V $\pm 5\%$ output voltage, at an air temperature of 10-30°C, and relative humidity of 15-80%.

All equipment is supplied and installed on a turnkey basis: equipment installation, hardware and system software start-up (cold start of the entire system).

Accessories. A complete factory-fitted kit must be provided for installation and commissioning in the mainframe and remote sites of the entire equipment set. The Participant must provide a list of the factory set of accessories, the accessories supplied and a written confirmation of the sufficiency of the presented accessories for installation, connection and commissioning of the equipment set.

It must be installed in 19" size telecommunication cabinets.

The remote hardware management system of all servers must be the same on all servers and integrated into a separate network infrastructure for security management.

The remote management system of all switches must be the same on all switches and be integrated into a separate network infrastructure for security management.

The remote hardware management system of all firewalls must be the same on all switches and integrated into a separate network infrastructure for security management.

The supplied server hardware must be provided:

failure management (information on failure, error analysis, statistical information collection, data recovery after failure);

configuration management (storage of server configurations, tracking their changes, system monitoring).

The manufacturer must have its registered trademark and be present on the IT market for at least 10 years before the date of filing the offer.

The participant must provide a copy of the company registration certificate.

ее поставку в адрес ООО «Uzbekistan GTL»

- . Участник должен предоставить копию свидетельства о регистрации компании.
- . Участник должен быть правомочным заключать контракты и иные хозяйственные соглашения в соответствии с законодательством Республики Узбекистан.
- . Участник должен предоставить письмо о наличии Сервис центра на поставляемое оборудование на территории Республики Узбекистан.
- . Участник не должен находиться в стадии реорганизации, ликвидации или банкротства, а также в состоянии судебного разбирательства.
- . Участник должен иметь персонал, способный обеспечить квалифицированную поддержку поставляемого оборудования.

7. Требования к размерам, упаковке, отгрузке и перевозке товара:

Участник обеспечивает полную сохранность и защиту от повреждений при транспортировке всего оборудования до места определенного в соответствии с условиями поставки. Каждое изделие должно быть упаковано, с обеспечением защиты от внешних воздействий. Наличие маркировки, либо упаковочных бирок обязательно.

8. Требования к качеству поставляемых комплектующих: Участник гарантирует, что доставленные товары новые, ранее не использованные. Все части и детали выполнены из качественных материалов и качественно изготовлены, в них отсутствуют дефекты, и они соответствуют целям использования. Оборудование, имеющее какие-либо дефекты, должны быть заменены на новые.

9. Требования к году производства товара: Товар должен быть произведен не ранее 2020 года, новым, ранее не использованным и не эксплуатированным. Подтверждается письмом о новизне от производителя оборудования или его регионального представительства.

10. Передаваемая вместе с товаром документация:

Необходимые сертификаты качества (соответствия), сертификат происхождения, а также иные документы необходимые для проведения дальнейшей таможенной очистки;

11. Требования к участнику: Участник должен предоставить письмо от производителя о наличии партнёрства, а также о праве продавать данный вид

A participant shall be entitled to conclude contracts and other economic agreements in accordance with the legislation of Uzbekistan.

The participant should provide a letter on the availability of the Service Center for the supplied equipment in the Republic of Uzbekistan.

A participant must not be in the stage of reorganization, liquidation or bankruptcy, or in the state of legal proceedings.

The participant must have personnel who can provide qualified support for the equipment supplied.

7. Requirements for size, packaging, shipment and transport of goods:

The Participant shall ensure complete safety and protection against damage during transportation of all equipment to the place determined in accordance with the delivery conditions. Each product must be packaged, with protection from external influences. Marking or packing tags are mandatory.

8. Requirements for quality of supplied components:

The Participant guarantees that the delivered goods are new and not used before. All parts and components are made of quality materials and are made of quality materials, they are free of defects and correspond to the purpose of use. Equipment that has any defects must be replaced by new ones.

9. The documentation that is transferred with the product:

Necessary certificates of quality (conformity), certificate of origin, as well as other documents necessary for further customs clearance;

10. Requirements for the year of production:

The product must be produced no earlier than 2020, new, previously unused and not operated. Confirmed by a letter of novelty from the equipment manufacturer or its regional representative.

оборудования.

12. Техническая поддержка: Наличие официального веб сайта с соответствующей документацией и программным обеспечением, доступным для круглосуточного и беспрепятственного скачивания.

13. Требования к производителю оборудования: широко известный в мире производитель имеющий мировой опыт поставок подобного оборудования, а также входящий в квадрант Гартнера.

14. Гарантия – Гарантия на поставляемое оборудование должна составлять 12 месяцев с момента их получения.

15. Требования к производителю оборудования: широко известный в мире производитель имеющий мировой опыт поставок подобного оборудования, а также входящий в квадрант Гартнера.

16. Цены на Продукцию указываются:

- для иностранных участников: в Долларах США на условиях поставки CIP г. Ташкент, Таможенный терминал (согласно требованиям Инкотермс 2010 года);
- для отечественных участников: в национальной валюте на условиях поставки DDP г. Ташкент, ул. Фаргона йули , дом 7Б (согласно требованиям Инкотермс 2010 года);

17. Срок поставки товара: 45 календарных дней с даты подписания Контракта. Допускается также предоставления иных дат поставки товара.

11. Requirements for the participant: The participant must submit a letter from the manufacturer stating the existence of a partnership as well as the right to sell this type of equipment.

12. Technical support: Availability of an official website with relevant documentation and software, available for download 24 hours a day, 7 days a week.

13. Requirements to the equipment manufacturer: the manufacturer widely known in the world having world experience of deliveries of the similar equipment, and also entering into Gartner quadrant.

14. Warranty - The warranty for the supplied equipment must be 12 months from the date of receipt.

15. Requirements to the equipment manufacturer: the manufacturer widely known in the world having.

world experience of deliveries of the similar equipment, and also entering into Gartner quadrant.

16. The prices of the Products are indicated:

for foreign participants: in US Dollars on CIP delivery terms, Tashkent, Customs terminal (according to Incoterms 2010);

for domestic participants: in local currency on terms of DDP delivery to Tashkent, 7B Fargoona Yuli Street, Tashkent (according to Incoterms 2010);

17. Delivery time of the goods: 45 calendar days. It is also allowed to provide other dates for the delivery of goods.

| | |
|--|---|
| <p>Сервер – количество 10 штук (тип – SRVVM)</p> <p>Общие требования Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту не более 2RU; Иметь комплект телескопических направляющих для установки вычислительного узла в стойку в комплекте с рукавом для укладки кабелей; Должен иметь датчик открытия корпуса с возможностью настройки удаленного оповещения об этом событии;</p> <p>Процессор Иметь не менее 2 установленных процессоров, каждый из которых должен иметь не менее 20 ядер, а в сумме на два процессора 40 ядер, работающих на частоте не ниже 2.1 ГГц, поддерживать работу памяти с частотой не менее 2933 МГц, иметь кэш-память объемом не менее 27.5 МБайт. Максимальная расчетная мощность процессора должна быть не более 125 Ватт. Должна быть реализована возможность работы с x64 разрядными приложениями на аппаратном уровне. При этом максимальная тактовая частота с технологией Turbo Boost должна быть не менее 3.9 ГГц; Литография установленных процессоров не менее 14 nm;</p> <p>Оперативная память Наличие не менее 24 слотов DDR4 для установки модулей памяти; Должно быть установлено не менее 8 модулей памяти RDIMM Dual Rank объемом не менее 32 Гбайт каждый, а в сумме 256 Гбайт, работающих на частоте не менее 2 933 МГц;</p> <p>Хранение данных Поддерживать одновременную установку не менее чем 24 жестких дисков форм-фактора 2.5; Иметь RAID-контроллер с поддержкой интерфейса подключения жестких дисков SAS 3.0 и уровней RAID не ниже 0, 1, 10, 5, 50, 6, 60</p> | <p>Server - quantity 10 pcs (type - SRVVM)</p> <p>General requirements Have a form factor to install in a standard server rack and be no higher than 2RU; Have a set of telescopic guides for installing the computing unit in a rack complete with a cable laying sleeve; Must have an enclosure opening sensor that can be set up for remote notification of this event;</p> <p>Processor To have at least 2 installed processors, each of which should have at least 20 cores, and a total of 40 cores per two processors operating at a frequency of at least 2.1 GHz, to support memory operation at a frequency of at least 2933 MHz, have a cache of at least 27.5 MB. The maximum rated processor power shall not exceed 125 watts. It should be possible to work with x64-bit applications on the hardware level. The maximum clock frequency with Turbo Boost technology should be not less than 3.9 GHz; Lithography of installed processors at least 14 nm;</p> <p>RAM Availability of at least 24 DDR4 slots for installing memory modules; At least 8 RDIMM Dual Rank memory modules of at least 32 Gbytes each and 256 Gbytes each, operating at a frequency of at least 2,933 MHz, should be installed;</p> <p>Data Storage Support the simultaneous installation of at least 24 form factor 2.5 hard drives;</p> |
|--|---|

с объемом кэш-памяти не менее 2 Гбайт. Поддержка не менее 24 жестких дисков;

Иметь не менее 24 установленных твердотельных накопителей объемом не менее 960 Гбайт и интерфейсом не хуже SATA 6 Гбит/с, с параметром DWPD не менее 1 и TWB не менее 1700. Каждый накопитель должен быть оснащен функциями горячей замены и Read Intensive, при необходимости допускается добавление/замена дисков на Write Intensive для развертывания виртуальной среды хранения данных;

Должен поддерживать возможность опциональной установки не менее 3х карт SD(XC) внутрь сервера, две из которых должны поддерживать аппаратный RAID 1 для отказоустойчивой загрузки и работы для гипервизора;

Должен быть установлен картридер, включающий в себя не менее двух портов micro-SD

Должно быть установлено не менее двух microSDHC/SDXC карт объемом не менее 32Гбайт

Слоты расширение и карты расширения

Наличие не менее 4 слотов PCIe 3.0 x8 для установки карт расширения;

Должно быть установлено не менее 1 сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+, а также не менее 2 порта 1000BASE-T. Сетевой адаптер не должен занимать слот PCIe, предназначенный для установки карт расширения;

Должно быть установлено не менее 1 полноразмерного сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+.

Электропитание

Иметь не менее двух блоков питания мощностью не менее 1000 Вт каждый с возможностью горячей замены, иметь поддержку резервирования питания и поддерживать установку блоков питания мощностью до 2400 Вт каждый;

Иметь комплект кабелей для подключения к сети питания в достаточном количестве (C13/C14 10A);

Дополнительные функции

Have a RAID controller that supports SAS 3.0 hard disk drives and RAID levels of at least 0, 1, 10, 5, 50, 6, 60 with a cache size of at least 2 GB. Support for at least 24 hard disks;

Have at least 24 installed SSDs with a capacity of at least 960 GB and an interface no worse than SATA 6 Gb/s, with a DWPD of at least 1 and TWB of at least 1700. Each drive must be hot-swappable and Read Intensive, and it is possible to add/replace drives to Write Intensive for virtual storage deployment if required;

Must support the optional installation of at least 3 SD(XC) cards inside the server, two of which must support hardware RAID 1 for fault-tolerant loading and operation for the hypervisor;

A card reader with at least two micro-SD ports must be installed

A minimum of two microSDHC/SDXC cards with a minimum of 32GB capacity should be installed

Expansion slots and expansion cards

There are at least 4 PCIe 3.0 x8 slots for installing expansion cards;

At least 1 network adapter including at least 2 10GbE SFP+ ports and at least 2 1000BASE-T ports must be installed. The network adapter must not occupy the PCIe slot designed for installing expansion cards;

At least 1 full-size network adapter including at least 2 10GbE SFP+ ports must be installed.

Power supply

Have at least two hot-swappable power supplies of at least 1000W each, support redundant power supply and support installation of power supplies up to 2400W each;

Have a sufficient number of cables for connecting to the mains (C13/C14 10A);

| | |
|---|---|
| <p>Иметь запираемую на ключ лицевую панель, ограничивающую доступ к жестким дискам;</p> <p>Должен иметь жидкокристаллический экран состояния и диагностики системы на передней панели с разрешением не менее 128x20 пикселей и кнопками навигации, экран должен быть полностью виден при закрытой передней панели корпуса сервера;</p> <p>Иметь не менее 5 портов USB (2 USB 2.0 на лицевой панели, 1 USB 3.0 внутри сервера и 2 USB 3.0 на задней стороне сервера);</p> <p>Иметь не менее 1 порта micro-USB на лицевой панели для возможности прямого подключения к контроллеру управления и мониторинга сервера;</p> <p>Должны быть установлены не менее 6 высокопроизводительных турбин для охлаждения;</p> <p>Должен быть совместим как минимум со следующими операционными системами и гипервизорами: Microsoft Windows Server 2012R2, 2016 и выше; Red Hat Enterprise Linux 6.9 и выше, 7.3 и выше; VMware ESXi 6.0U3, 6.5 и выше; vSAN; Ubuntu 16.04 LTS и выше; Citrix XenServer 7.1 и выше;</p> <p>Должен иметь встроенные аппаратно-программные средства для удаленного управления и мониторинга, обеспечивающие следующие функции:</p> <p>Удаленный доступ к консоли управления вычислительного узла посредством веб-браузеров, интерфейса командной строки по протоколам ssh и telnet, IPMI и Redfish;</p> <p>Поддержки возможности использования функционала отслеживания состояния и управления вычислительного узла с использованием мобильных устройств, поддерживающих передачу данных с использованием стандартов Bluetooth, WiFi (при наличии в составе сервера отдельного модуля связи и управления);</p> <p>Автоматическое информирование администратора обо всех сбоях и предсказаниях нарушения функционирования дисковой подсистемы, модулей памяти, блоков питания, вентиляторов и процессоров по средствам электронной почты или выведения сообщения на консоль администратора;</p> | <p>Additional features</p> <p>Have a lockable front panel that restricts access to hard drives;</p> <p>Must have a liquid crystal display of system status and diagnostics on the front panel with a resolution of at least 128x20 pixels and navigation buttons, the screen should be fully visible when the front panel of the server case is closed;</p> <p>Have at least 5 USB ports (2 USB 2.0 on the front panel, 1 USB 3.0 inside the server and 2 USB 3.0 on the back of the server);</p> <p>Have at least 1 micro-USB port on the front panel for direct connection to the server control and monitoring controller;</p> <p>At least 6 high-performance cooling turbines must be installed;</p> <p>Must be compatible with at least the following operating systems and hypervisors: Microsoft Windows Server 2012R2, 2016 and above; Red Hat Enterprise Linux 6.9 and above, 7.3 and above; VMware ESXi 6.0U3, 6.5 and above; vSAN; Ubuntu 16.04 LTS and above; Citrix XenServer 7.1 and above;</p> <p>Must have built-in hardware and software tools for remote management and monitoring that provide the following functions:</p> <p>Remote access to the computing node management console via web browsers, command line interface via ssh and telnet, IPMI and Redfish;</p> <p>Supports the ability to use the functionality of tracking and management of the computing node using mobile devices that support data transfer using Bluetooth, WiFi standards (if the server has a separate communication and management module);</p> <p>Automatically inform the administrator of all failures and predictions of malfunctions of the disk subsystem, memory modules, power supplies, fans and processors by e-mail or by displaying a message to the administrator console;</p> |
|---|---|

| | |
|---|---|
| <p>Отображение инвентаризационной информации обо установленных компонентах вычислительного узла, включая информацию об установленных версиях микрокодов компонент сервера, информацию о MAC-адресах и WWN сетевых контроллеров и FC-адаптерах, в т.ч. и виртуальных;</p> <p>Удаленная перезагрузка, включение/выключение вычислительного узла (в том числе загрузка с виртуального оптического диска);</p> <p>Удаленный перехват консоли управления вычислительного узла (виртуальная консоль): экрана, клавиатуры и координатно-графического указателя как на этапе загрузки вычислительного узла, так и во время работы операционных систем. Виртуальная консоль должна иметь возможность управления питанием вычислительного узла, возможность указания загрузочного устройства, с одновременным подключением до 6 пользователей и взаимодействием в режиме обмена сообщениями. Виртуальная консоль должна поддерживать работу с использованием веб-браузера и стандарта HTML5, без необходимости использования плагинов Java и ActiveX;</p> <p>Возможность сбора информации об уровне утилизации центрального процессора и оперативной памяти сервера без необходимости установки агентского ПО в ОС;</p> <p>Возможность управления RAID-контроллерами, устанавливаемых внутри корпуса вычислительного узла, через веб-интерфейс или командный интерфейс модуля управления без необходимости установки агентского ПО в ОС. Как минимум должна обеспечиваться возможность:</p> <p>Возможность управления RAID-контроллером без необходимости перезагрузки вычислительного узла;</p> <p>Отслеживание состояния накопителей, подключенных к RAID-контроллеру, в т.ч. и NVMe-накопителей;</p> <p>Отслеживание состояния виртуальных дисков;</p> <p>Создание, удаление и конфигурирование виртуальных дисков;</p> <p>Изменение настроек RAID-контроллера;</p> <p>Расширение ёмкости виртуальных дисков без прерывания доступа к ним;</p> <p>Изменения уровня RAID виртуальных дисков без прерывания доступа к ним;</p> | <p>Displaying inventory information about installed computing node components, including information about installed versions of microcodes of server components, information about MAC addresses and WWN of network controllers and FC adapters, including virtual ones;</p> <p>Remote reboot, enable/disable the computing node (including booting from the virtual optical drive);</p> <p>Remote capture of the management console of the computing node (virtual console): screen, keyboard and coordinate graphical pointer both at the stage of loading the computing node and during operation of operating systems. The virtual console should be able to control the power of the computing node, the ability to specify the boot device, with simultaneous connection of up to 6 users and interaction in the message exchange mode. The Virtual Console should support work with a web browser and HTML5 standard, without the need to use Java and ActiveX plugins;</p> <p>Ability to collect information on the utilization level of the CPU and RAM of the server without the need to install agent software in the operating system;</p> <p>It is possible to manage RAID controllers installed inside the computing node housing through a web interface or command interface of the management module without the need to install agent software in the OS. At a minimum, it should be possible to do so:</p> <p>Ability to manage the RAID controller without having to reboot the computing node;</p> <p>Track the status of drives connected to the RAID controller, including NVMe drives;</p> <p>Tracking the status of virtual disks;</p> <p>Create, delete and configure virtual disks;</p> <p>Change the RAID controller settings;</p> <p>Extend the capacity of virtual drives without interrupting access to them;</p> <p>Change the RAID level of virtual drives without interrupting access to them;</p> |
|---|---|

| | |
|--|---|
| <p>Запись конфигурации вычислительного узла, драйверов, хранения резервного образа вычислительного узла для перезагрузки в случае возникновения неполадок на энергонезависимый носитель, устанавливаемый внутри корпуса вычислительного узла или на сетевой файловый ресурс;</p> <p>Возможность генерации NMI;</p> <p>Возможность сохранения скриншота экрана описания системного сбоя с выводом диагностической информации;</p> <p>Возможность через веб-интерфейс или интерфейс командной строки экспорта диагностической информации о состоянии вычислительного узла, включая логи как с модуля управления сервером, так и логи операционной системы или гипервизора, в едином консолидированном отчёте.</p> <p>Запись конфигурации модуля управления на выделенный энергонезависимый накопитель, устанавливаемый внутри корпуса вычислительного узла, для быстрого восстановления работоспособности вычислительного узла в случае замены материнской платы;</p> <p>Возможность использования аппаратно-программных средств для подготовки к установке операционной системы (конфигурирование томов, создание разделов, копирование драйверов, создание файлов ответа для инсталляторов ОС), не требующие использования внешних носителей информации;</p> <p>Возможность применения обновлений микрокодов компонент вычислительного узла как через интерфейс модуля управления сервером, так и из поддерживаемых операционных систем;</p> <p>Модуль управления сервером должен иметь функционал безопасной проверки целостности и неизменности пакетов обновлений микрокодов компонент вычислительного узла на этапе подготовки обновления;</p> <p>Модуль управления сервером должен поддерживать возможность перевода модуля в режим запрета вноса каких-либо изменений в конфигурацию сервера, таких, как настройки BIOS, обновление микрокода, настроек модуля управления;</p> <p>Модуль управления сервера должен поддерживать возможность управления группой идентичных серверов до не менее 90 шт.</p> <p>Должен поставляться с гарантийными обязательствами производителя в течение годового гарантийного срока с даты</p> | <p>Recording of the computing node configuration, drivers, storage of the backup image of the computing node for reboot in case of a problem on the non-volatile media installed inside the computing node enclosure or on the network file share;</p> <p>NMI generation capability;</p> <p>It is possible to save a screenshot of a description screen of a system failure with diagnostic information output;</p> <p>The ability to export diagnostic information about the state of the computing node, including logs from the server management module, as well as logs of the operating system or hypervisor, in a single consolidated report through a web interface or command line interface.</p> <p>Write the control module configuration to a dedicated non-volatile drive installed inside the computing node case to quickly restore the computing node in case the motherboard is replaced;</p> <p>The ability to use hardware and software tools to prepare for operating system installation (configuring volumes, creating partitions, copying drivers, creating answer files for OS installers) that do not require external media;</p> <p>It is possible to apply updates of microcode components of the computing node both through the server management module interface and from supported operating systems;</p> <p>The server management module should have the functionality of securely verifying the integrity and consistency of microcode service packs of the computing node components during the update preparation stage;</p> <p>The Server Management Module should support the ability to disable any changes to the server configuration such as BIOS settings, microcode updates, control module settings;</p> <p>The Server Management Module must support the ability to manage a group of identical servers up to a minimum of 90 pieces.</p> |
|--|---|

| | |
|--|---|
| <p>продажи конечному пользователю. Гарантийные обязательства производителя должны включать:</p> <p>Круглосуточные консультации инженеров «горячей линии» производителя по вопросам восстановления работоспособности, эксплуатации оборудования и программного обеспечения в режиме реального времени;</p> <p>Замена неисправных аппаратных компонент на месте эксплуатации авторизованными сервисными инженерами производителя/уполномоченными производителем на площадке заказчика на следующий рабочий день;</p> <p>Возможность приобретения оборудования с гарантийными обязательствами производителя до 7 (семи) лет с даты продажи конечному пользователю;</p> <p>Наличие опции невозврата неисправных жестких дисков производителю в случае их аппаратной неисправности не менее 3 (трех) лет.</p> | <p>Must be delivered with the manufacturer's warranty within a one-year warranty period from the date of sale to the end user. The manufacturer's warranty obligations shall include:</p> <p>Round-the-clock consultations of the manufacturer's hotline engineers on the issues of recovery, equipment and software operation in real time;</p> <p>Faulty hardware components are replaced at the customer's site by the manufacturer's authorized service engineers/authorized by the manufacturer on the next working day;</p> <p>Possibility to purchase equipment with manufacturer's warranty up to 7 (seven) years from the date of sale to the end user;</p> <p>The option of not returning faulty hard disks to the manufacturer in case of hardware malfunction for at least 3 (three) years.</p> |
|--|---|

| | |
|--|--|
| <p>Сервер – количество 2 штук (тип – SRVRVM)</p> <p>Общие требования Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту не более 2RU; Иметь комплект телескопических направляющих для установки вычислительного узла в стойку в комплекте с рукавом для укладки кабелей; Должен иметь датчик открытия корпуса с возможностью настройки удаленного оповещения об этом событии;</p> <p>Процессор Иметь не менее 2 установленных процессоров, каждый из которых должен иметь не менее 16 ядер, а в сумме на два процессора 32 ядер, работающих на частоте не ниже 2.1 ГГц, поддерживать работу памяти с частотой не менее 2400 МГц, иметь кэш-память объемом не менее 22 Мбайт. Максимальная расчетная мощность процессора должна быть не более 100 Ватт. Должна быть реализована возможность работы с x64 разрядными приложениями на аппаратном уровне. При этом максимальная тактовая частота с технологией Turbo Boost должна быть не менее 3.2 ГГц; Литография установленных процессоров не менее 14 nm;</p> <p>Оперативная память Наличие не менее 24 слотов DDR4 для установки модулей памяти; Должно быть установлено не менее 4 модулей памяти RDIMM Dual Rank объемом не менее 32 Гбайт каждый, а в сумме 128 Гбайт, работающих на частоте не менее 2 400 МГц;</p> <p>Хранение данных Поддерживать одновременную установку не менее чем 12 жестких дисков форм-фактора 3.5; Иметь RAID-контроллер с поддержкой интерфейса подключения жестких дисков SAS 3.0 и уровней RAID не ниже 0, 1, 10, 5, 50, 6, 60 с</p> | <p>Server - quantity 2 pcs (type - SRVRVM)</p> <p>General requirements Have a form factor to install in a standard server rack and be no higher than 2RU; Have a set of telescopic guides for installing the computing unit in a rack complete with a cable laying sleeve; Must have an enclosure opening sensor that can be set up for remote notification of this event;</p> <p>Processor To have at least 2 installed processors, each of which should have at least 16 cores, and a total of 32 cores per two processors operating at a frequency of not less than 2.1 GHz, to support memory operation at a frequency of not less than 2400 MHz, have a cache memory of at least 22 MB. The maximum rated CPU power shall not exceed 100 Watts. It should be possible to work with x64-bit applications on the hardware level. The maximum clock frequency with Turbo Boost technology should be not less than 3.2 GHz; Lithography of installed processors at least 14 nm;</p> <p>RAM Availability of at least 24 DDR4 slots for installing memory modules; At least 4 RDIMM Dual Rank memory modules of at least 32 Gbytes each and 128 Gbytes each, operating at a frequency of at least 2,400 MHz, should be installed;</p> <p>Data Storage Support the simultaneous installation of at least 12 form factor 3.5 hard drives; Have a RAID controller that supports SAS 3.0 hard disk drives and RAID levels of at least 0, 1, 10, 5, 50, 6, 60 with a cache size of at least 2 GB. Support for at least 24 hard disks;</p> |
|--|--|

объемом кэш-памяти не менее 2 Гбайт. Поддержка не менее 24 жестких дисков;

Иметь не менее 12 установленных накопителей объёмом не менее 8 Тбайт, скоростью вращения шпинделя не менее 7200 и интерфейсом не хуже NLSAS 12 Гбит/с. Каждый накопитель должен быть оснащен функциями горячей замены, при необходимости допускается добавление твердотельных дисков Write Intensive для развертывания виртуальной среды хранения данных;

Должен поддерживать возможность опциональной установки не менее 3х карт SD(XC) внутрь сервера, две из которых должны поддерживать аппаратный RAID 1 для отказоустойчивой загрузки и работы для гипервизора;

Должен быть установлен картридер, включающий в себя не менее двух портов micro-SD

Должно быть установлено не менее двух microSDHC/SDXC карт объемом не менее 32Гбайт

Слоты расширение и карты расширения

Наличие не менее 4 слотов PCIe 3.0 x8 для установки карт расширения; Должно быть установлено не менее 1 сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+, а также не менее 2 порта 1000BASE-T. Сетевой адаптер не должен занимать слот PCIe, предназначенный для установки карт расширения;

Должно быть установлено не менее 1 полноразмерного сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+.

Электропитание

Иметь не менее двух блоков питания мощностью не менее 1000 Вт каждый с возможностью горячей замены, иметь поддержку резервирования питания и поддерживать установку блоков питания мощностью до 2400 Вт каждый;

Иметь комплект кабелей для подключения к сети питания в достаточном количестве (C13/C14 10A);

Дополнительные функции

Иметь запираемую на ключ лицевую панель, ограничивающую доступ к жестким дискам;

Have at least 12 installed drives of at least 8 Tbytes in size, a spindle speed of at least 7200 and an interface no worse than NLSAS 12 Gb/s. Each drive shall be hot-swappable, and Write Intensive SSDs may be added if required to deploy a virtual storage environment;

Must support the optional installation of at least 3 SD(XC) cards inside the server, two of which must support hardware RAID 1 for fault-tolerant loading and operation for the hypervisor;

A card reader with at least two micro-SD ports must be installed

A minimum of two microSDHC/SDXC cards with a minimum of 32GB capacity should be installed

Expansion slots and expansion cards

There are at least 4 PCIe 3.0 x8 slots for installing expansion cards;

At least 1 network adapter must be installed, including at least 2 10GbE SFP+ ports and at least 2 1000BASE-T ports. The network adapter must not occupy the PCIe slot designed for installing expansion cards;

At least 1 full-size network adapter including at least 2 10GbE SFP+ ports must be installed.

Power supply

Have at least two hot-swappable power supplies of at least 1000W each, support redundant power supply and support installation of power supplies up to 2400W each;

Have a sufficient number of cables for connecting to the mains (C13/C14 10A);

Additional features

Have a lockable front panel that restricts access to hard drives;

| | |
|---|---|
| <p>Должен иметь жидкокристаллический экран состояния и диагностики системы на передней панели с разрешением не менее 128x20 пикселей и кнопками навигации, экран должен быть полностью виден при закрытой передней панели корпуса сервера;</p> <p>Иметь не менее 5 портов USB (2 USB 2.0 на лицевой панели, 1 USB 3.0 внутри сервера и 2 USB 3.0 на задней стороне сервера);</p> <p>Иметь не менее 1 порта micro-USB на лицевой панели для возможности прямого подключения к контроллеру управления и мониторинга сервера;</p> <p>Должны быть установлены не менее 6 высокопроизводительных турбин для охлаждения;</p> <p>Должен быть совместим как минимум со следующими операционными системами и гипервизорами:</p> <p>Microsoft Windows Server 2012R2, 2016 и выше;</p> <p>Red Hat Enterprise Linux 6.9 и выше, 7.3 и выше;</p> <p>VMware ESXi 6.0U3, 6.5 и выше;</p> <p>vSAN;</p> <p>Ubuntu 16.04 LTS и выше;</p> <p>Citrix XenServer 7.1 и выше;</p> <p>Должен иметь встроенные аппаратно-программные средства для удаленного управления и мониторинга, обеспечивающие следующие функции:</p> <p>Удаленный доступ к консоли управления вычислительного узла посредством веб-браузеров, интерфейса командной строки по протоколам ssh и telnet, IPMI и Redfish;</p> <p>Поддержки возможности использования функционала отслеживания состояния и управления вычислительного узла с использованием мобильных устройств, поддерживающих передачу данных с использованием стандартов Bluetooth, WiFi (при наличии в составе сервера отдельного модуля связи и управления);</p> <p>Автоматическое информирование администратора обо всех сбоях и предсказаниях нарушения функционирования дисковой подсистемы, модулей памяти, блоков питания, вентиляторов и процессоров по средствам электронной почты или выведения сообщения на консоль администратора;</p> <p>Отображение инвентаризационной информации обо установленных компонентах вычислительного узла, включая информацию об установленных версиях микрокодов компонент сервера, информацию</p> | <p>Must have a liquid crystal display of system status and diagnostics on the front panel with a resolution of at least 128x20 pixels and navigation buttons, the screen should be fully visible when the front panel of the server case is closed;</p> <p>Have at least 5 USB ports (2 USB 2.0 on the front panel, 1 USB 3.0 inside the server and 2 USB 3.0 on the back of the server);</p> <p>Have at least 1 micro-USB port on the front panel for direct connection to the server control and monitoring controller;</p> <p>At least 6 high-performance cooling turbines must be installed;</p> <p>Must be compatible with at least the following operating systems and hypervisors:</p> <p>Microsoft Windows Server 2012R2, 2016 and above;</p> <p>Red Hat Enterprise Linux 6.9 and above, 7.3 and above;</p> <p>VMware ESXi 6.0U3, 6.5 and above;</p> <p>vSAN;</p> <p>Ubuntu 16.04 LTS and above;</p> <p>Citrix XenServer 7.1 and above;</p> <p>Must have built-in hardware and software tools for remote management and monitoring that provide the following functions:</p> <p>Remote access to the computing node management console via web browsers, command line interface via ssh and telnet, IPMI and Redfish;</p> <p>Supports the ability to use the functionality of tracking and management of the computing node using mobile devices that support data transfer using Bluetooth, WiFi standards (if the server has a separate communication and management module);</p> <p>Automatically inform the administrator of all failures and predictions of malfunctions of the disk subsystem, memory modules, power supplies, fans and processors by e-mail or by displaying a message to the administrator console;</p> <p>Displaying inventory information about installed computing node components, including information about installed versions of microcodes</p> |
|---|---|

о MAC-адресах и WWN сетевых контроллеров и FC-адаптерах, в т.ч. и виртуальных;

Удаленная перезагрузка, включение/выключение вычислительного узла (в том числе загрузка с виртуального оптического диска);

Удаленный перехват консоли управления вычислительного узла (виртуальная консоль): экрана, клавиатуры и координатно-графического указателя как на этапе загрузки вычислительного узла, так и во время работы операционных систем. Виртуальная консоль должна иметь возможность управления питанием вычислительного узла, возможность указания загрузочного устройства, с одновременным подключением до 6 пользователей и взаимодействием в режиме обмена сообщениями. Виртуальная консоль должна поддерживать работу с использованием веб-браузера и стандарта HTML5, без необходимости использования плагинов Java и ActiveX;

Возможность сбора информации об уровне утилизации центрального процессора и оперативной памяти сервера без необходимости установки агентского ПО в ОС;

Возможность управления RAID-контроллерами, устанавливаемых внутри корпуса вычислительного узла, через веб-интерфейс или командный интерфейс модуля управления без необходимости установки агентского ПО в ОС. Как минимум должна обеспечиваться возможность:

Возможность управления RAID-контроллером без необходимости перезагрузки вычислительного узла;

Отслеживание состояния накопителей, подключенных к RAID-контроллеру, в т.ч. и NVMe-накопителей;

Отслеживание состояния виртуальных дисков;

Создание, удаление и конфигурирование виртуальных дисков;

Изменение настроек RAID-контроллера;

Расширение ёмкости виртуальных дисков без прерывания доступа к ним;

Изменения уровня RAID виртуальных дисков без прерывания доступа к ним;

Запись конфигурации вычислительного узла, драйверов, хранения резервного образа вычислительного узла для перезагрузки в случае возникновения неполадок на энергонезависимый носитель, устанавливаемый внутри корпуса вычислительного узла или на сетевой файловый ресурс;

of server components, information about MAC addresses and WWN of network controllers and FC adapters, including virtual ones;

Remote reboot, enable/disable the computing node (including booting from the virtual optical drive);

Remote capture of the management console of the computing node (virtual console): screen, keyboard and coordinate graphical pointer both at the stage of booting the computing node and during the operation of operating systems. The virtual console should be able to control the power of the computing node, the ability to specify the boot device, with simultaneous connection of up to 6 users and interaction in the message exchange mode. The Virtual Console should support work with a web browser and HTML5 standard, without the need to use Java and ActiveX plugins;

Ability to collect information on the utilization level of the CPU and RAM of the server without the need to install agent software in the operating system;

It is possible to manage RAID controllers installed inside the computing node housing through a web interface or command interface of the management module without the need to install agent software in the OS. At a minimum, it should be possible to do so:

Ability to manage the RAID controller without having to reboot the computing node;

Track the status of drives connected to the RAID controller, including NVMe drives;

Tracking the status of virtual disks;

Create, delete and configure virtual disks;

Change the RAID controller settings;

Extend the capacity of virtual drives without interrupting access to them;

Change the RAID level of virtual drives without interrupting access to them;

Recording of the computing node configuration, drivers, storage of the backup image of the computing node for reboot in case of a problem on the

| | |
|--|--|
| <p>Возможность генерации NMI;</p> <p>Возможность сохранения скриншота экрана описания системного сбоя с выводом диагностической информации;</p> <p>Возможность через веб-интерфейс или интерфейс командной строки экспорта диагностической информации о состоянии вычислительного узла, включая логи как с модуля управления сервером, так и логи операционной системы или гипервизора, в едином консолидированном отчёте.</p> <p>Запись конфигурации модуля управления на выделенный энергонезависимый накопитель, устанавливаемый внутри корпуса вычислительного узла, для быстрого восстановления работоспособности вычислительного узла в случае замены материнской платы;</p> <p>Возможность использования аппаратно-программных средств для подготовки к установке операционной системы (конфигурирование томов, создание разделов, копирование драйверов, создание файлов ответа для инсталляторов ОС), не требующие использования внешних носителей информации;</p> <p>Возможность применения обновлений микрокодов компонент вычислительного узла как через интерфейс модуля управления сервером, так и из поддерживаемых операционных систем;</p> <p>Модуль управления сервером должен иметь функционал безопасной проверки целостности и неизменности пакетов обновлений микрокодов компонент вычислительного узла на этапе подготовки обновления;</p> <p>Модуль управления сервером должен поддерживать возможность перевода модуля в режим запрета вноса каких-либо изменений в конфигурацию сервера, таких, как настройки BIOS, обновление микрокода, настроек модуля управления;</p> <p>Модуль управления сервера должен поддерживать возможность управления группой идентичных серверов до не менее 90 шт.</p> <p>Должен поставляться с гарантийными обязательствами производителя в течение годичного гарантийного срока с даты продажи конечному пользователю. Гарантийные обязательства производителя должны включать:</p> <p>Круглосуточные консультации инженеров «горячей линии» производителя по вопросам восстановления работоспособности,</p> | <p>non-volatile media installed inside the computing node enclosure or on the network file share;</p> <p>NMI generation capability;</p> <p>It is possible to save a screenshot of a description screen of a system failure with diagnostic information output;</p> <p>The ability to export diagnostic information about the state of the computing node, including logs from the server management module, as well as logs of the operating system or hypervisor, in a single consolidated report through a web interface or command line interface.</p> <p>Write the control module configuration to a dedicated non-volatile drive installed inside the computing node case to quickly restore the computing node in case the motherboard is replaced;</p> <p>The ability to use hardware and software tools to prepare for operating system installation (configuring volumes, creating partitions, copying drivers, creating answer files for OS installers) that do not require external media;</p> <p>It is possible to apply updates of microcode components of the computing node both through the server management module interface and from supported operating systems;</p> <p>The server management module should have the functionality of securely verifying the integrity and constancy of microcode service packs of the computing node components during the update preparation stage;</p> <p>The Server Management Module should support the ability to disable any changes to the server configuration such as BIOS settings, microcode updates, control module settings;</p> <p>The Server Management Module must support the ability to manage a group of identical servers up to a minimum of 90 pieces.</p> <p>Must be delivered with the manufacturer's warranty within a one-year warranty period from the date of sale to the end user. The manufacturer's warranty obligations shall include:</p> |
|--|--|

| | |
|--|---|
| <p>эксплуатации оборудования и программного обеспечения в режиме реального времени;</p> <p>Замена неисправных аппаратных компонент на месте эксплуатации авторизованными сервисными инженерами производителя/уполномоченными производителем на площадке заказчика на следующий рабочий день;</p> <p>Возможность приобретения оборудования с гарантийными обязательствами производителя до 7 (семи) лет с даты продажи конечному пользователю;</p> <p>Наличие опции невозврата неисправных жестких дисков производителю в случае их аппаратной неисправности не менее 3 (трех) лет.</p> | <p>Round-the-clock consultations of the manufacturer's hotline engineers on the issues of recovery, equipment and software operation in real time;</p> <p>Faulty hardware components are replaced at the customer's site by the manufacturer's authorized service engineers/authorized by the manufacturer on the next working day;</p> <p>Possibility to purchase equipment with manufacturer's warranty up to 7 (seven) years from the date of sale to the end user;</p> <p>The option of not returning faulty hard disks to the manufacturer in case of hardware malfunction for at least 3 (three) years.</p> |
|--|---|

| | |
|--|--|
| <p>Сервер – количество 3 штук (тип – SRVRS)</p> <p>Сервер должен удовлетворять следующим требованиям:</p> <p>Общие требования Иметь форм-фактор для установки в стандартную серверную стойку и иметь высоту не более 2RU; Иметь комплект телескопических направляющих для установки вычислительного узла в стойку в комплекте с рукавом для укладки кабелей; Должен иметь датчик открытия корпуса с возможностью настройки удаленного оповещения об этом событии;</p> <p>Процессор Иметь не менее 2 установленных процессоров, каждый из которых должен иметь не менее 16 ядер, а в сумме на два процессора 32 ядер, работающих на частоте не ниже 2.1 ГГц, поддерживать работу памяти с частотой не менее 2400 МГц, иметь кэш-память объемом не менее 22 МБайт. Максимальная расчетная мощность процессора должна быть не более 100 Ватт. Должна быть реализована возможность работы с x64 разрядными приложениями на аппаратном уровне. При этом максимальная тактовая частота с технологией Turbo Boost должна быть не менее 3.2 ГГц; Литография установленных процессоров не менее 14 nm;</p> <p>Оперативная память Наличие не менее 24 слотов DDR4 для установки модулей памяти; Должно быть установлено не менее 4 модулей памяти RDIMM Dual Rank объемом не менее 32 Гбайт каждый, а в сумме 128 Гбайт, работающих на частоте не менее 2 400 МГц;</p> <p>Хранение данных Поддерживать одновременную установку не менее чем 24 жестких дисков форм-фактора 2.5;</p> | <p>Server - quantity 3 pcs (type - SRVRS)</p> <p>The server must meet the following requirements:</p> <p>General requirements Have a form factor to install in a standard server rack and be no higher than 2RU; Have a set of telescopic guides for installing the computing unit in a rack complete with a cable laying sleeve; Must have an enclosure opening sensor that can be set up for remote notification of this event;</p> <p>Processor To have at least 2 installed processors, each of which should have at least 16 cores, and a total of 32 cores per two processors operating at a frequency of not less than 2.1 GHz, to support memory operation at a frequency of not less than 2400 MHz, have a cache memory of at least 22 MB. The maximum rated CPU power shall not exceed 100 Watts. It should be possible to work with x64-bit applications on the hardware level. The maximum clock frequency with Turbo Boost technology should be not less than 3.2 GHz; Lithography of installed processors at least 14 nm;</p> <p>RAM Availability of at least 24 DDR4 slots for installing memory modules; At least 4 RDIMM Dual Rank memory modules of at least 32 Gbytes each and 128 Gbytes each, operating at a frequency of at least 2,400 MHz, should be installed;</p> <p>Data Storage Support the simultaneous installation of at least 24 form factor 2.5 hard drives;</p> |
|--|--|

Иметь RAID-контроллер с поддержкой интерфейса подключения жестких дисков SAS 3.0 и уровней RAID не ниже 0, 1, 10, 5, 50, 6, 60 с объемом кэш-памяти не менее 2 Гбайт. Поддержка не менее 24 жестких дисков;
Иметь не менее 24 установленных твердотельных накопителей объемом не менее 960 Гбайт и интерфейсом не хуже SATA 6 Гбит/с, с параметром DWPD не менее 1 и TWB не менее 1700. Каждый накопитель должен быть оснащен функциями горячей замены и Read Intensive, при необходимости допускается добавление/замена дисков на Write Intensive для развертывания виртуальной среды хранения данных;
Должен поддерживать возможность опциональной установки не менее 3х карт SD(XC) внутрь сервера, две из которых должны поддерживать аппаратный RAID 1 для отказоустойчивой загрузки и работы для гипервизора;
Должен быть установлен картридер, включающий в себя не менее двух портов micro-SD
Должно быть установлено не менее двух microSDHC/SDXC карт объемом не менее 32Гбайт

Слоты расширение и карты расширения

Наличие не менее 4 слотов PCIe 3.0 x8 для установки карт расширения;
Должно быть установлено не менее 1 сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+, а также не менее 2 порта 1000BASE-T. Сетевой адаптер не должен занимать слот PCIe, предназначенный для установки карт расширения;
Должно быть установлено не менее 1 полноразмерного сетевого адаптера, включающий в себя не менее чем с 2 порта 10GbE SFP+.

Электропитание

Иметь не менее двух блоков питания мощностью не менее 1000 Вт каждый с возможностью горячей замены, иметь поддержку резервирования питания и поддерживать установку блоков питания мощностью до 2400 Вт каждый;
Иметь комплект кабелей для подключения к сети питания в достаточном количестве (C13/C14 10А);

Дополнительные функции

Иметь запираемую на ключ лицевую панель, ограничивающую доступ к жестким дискам;
Должен иметь жидкокристаллический экран состояния и диагностики системы на передней панели с разрешением не менее 128x20 пикселей и

Have a RAID controller that supports SAS 3.0 hard disk drives and RAID levels of at least 0, 1, 10, 5, 50, 6, 60 with a cache size of at least 2 GB. Support for at least 24 hard disks;

Have at least 24 installed SSDs with a capacity of at least 960 GB and an interface no worse than SATA 6 Gb/s, with a DWPD of at least 1 and TWB of at least 1700. Each drive must be hot-swappable and Read Intensive, and it is possible to add/replace drives to Write Intensive for virtual storage deployment if required;

Must support the optional installation of at least 3 SD(XC) cards inside the server, two of which must support hardware RAID 1 for fault-tolerant loading and operation for the hypervisor;

A card reader with at least two micro-SD ports must be installed

A minimum of two microSDHC/SDXC cards with a minimum of 32GB capacity should be installed

Expansion slots and expansion cards

There are at least 4 PCIe 3.0 x8 slots for installing expansion cards;

At least 1 network adapter must be installed, including at least 2 10GbE SFP+ ports and at least 2 1000BASE-T ports. The network adapter must not occupy the PCIe slot designed for installing expansion cards;

At least 1 full-size network adapter including at least 2 10GbE SFP+ ports must be installed.

Power supply

Have at least two hot-swappable power supplies of at least 1000W each, support redundant power supply and support installation of power supplies up to 2400W each;

Have a sufficient number of cables for connecting to the mains (C13/C14 10A);

Additional features

Have a lockable front panel that restricts access to hard drives;

Must have a liquid crystal display of system status and diagnostics on the front panel with a resolution of at least 128x20 pixels and

| | |
|---|--|
| <p>кнопками навигации, экран должен быть полностью виден при закрытой передней панели корпуса сервера;</p> <p>Иметь не менее 5 портов USB (2 USB 2.0 на лицевой панели, 1 USB 3.0 внутри сервера и 2 USB 3.0 на задней стороне сервера);</p> <p>Иметь не менее 1 порта micro-USB на лицевой панели для возможности прямого подключения к контроллеру управления и мониторинга сервера;</p> <p>Должны быть установлены не менее 6 высокопроизводительных турбин для охлаждения;</p> <p>Должен быть совместим как минимум со следующими операционными системами и гипервизорами:</p> <p>Microsoft Windows Server 2012R2, 2016 и выше;</p> <p>Red Hat Enterprise Linux 6.9 и выше, 7.3 и выше;</p> <p>VMware ESXi 6.0U3, 6.5 и выше;</p> <p>Ubuntu 16.04 LTS и выше;</p> <p>Citrix XenServer 7.1 и выше;</p> <p>Должен иметь встроенные аппаратно-программные средства для удаленного управления и мониторинга, обеспечивающие следующие функции:</p> <p>Удаленный доступ к консоли управления вычислительного узла посредством веб-браузеров, интерфейса командной строки по протоколам ssh и telnet, IPMI и Redfish;</p> <p>Поддержки возможности использования функционала отслеживания состояния и управления вычислительного узла с использованием мобильных устройств, поддерживающих передачу данных с использованием стандартов Bluetooth, WiFi (при наличии в составе сервера отдельного модуля связи и управления);</p> <p>Автоматическое информирование администратора обо всех сбоях и предсказаниях нарушения функционирования дисковой подсистемы, модулей памяти, блоков питания, вентиляторов и процессоров по средствам электронной почты или выведения сообщения на консоль администратора;</p> <p>Отображение инвентаризационной информации обо установленных компонентах вычислительного узла, включая информацию об установленных версиях микрокодов компонент сервера, информацию о MAC-адресах и WWN сетевых контроллеров и FC-адаптерах, в т.ч. и виртуальных;</p> <p>Удаленная перезагрузка, включение/выключение вычислительного узла (в том числе загрузка с виртуального оптического диска);</p> <p>Удаленный перехват консоли управления вычислительного узла (виртуальная консоль): экрана, клавиатуры и координатно-графического указателя как на этапе загрузки вычислительного узла, так и во время работы операционных</p> | <p>navigation buttons, the screen should be fully visible when the front panel of the server case is closed;</p> <p>Have at least 5 USB ports (2 USB 2.0 on the front panel, 1 USB 3.0 inside the server and 2 USB 3.0 on the back of the server);</p> <p>Have at least 1 micro-USB port on the front panel for direct connection to the server control and monitoring controller;</p> <p>At least 6 high-performance cooling turbines must be installed;</p> <p>Must be compatible with at least the following operating systems and hypervisors:</p> <p>Microsoft Windows Server 2012R2, 2016 and above;</p> <p>Red Hat Enterprise Linux 6.9 and above, 7.3 and above;</p> <p>VMware ESXi 6.0U3, 6.5 and above;</p> <p>Ubuntu 16.04 LTS and above;</p> <p>Citrix XenServer 7.1 and above;</p> <p>Must have built-in hardware and software tools for remote management and monitoring that provide the following functions:</p> <p>Remote access to the computing node management console via web browsers, command line interface via ssh and telnet, IPMI and Redfish;</p> <p>Supports the ability to use the functionality of tracking and management of the computing node using mobile devices that support data transfer using Bluetooth, WiFi standards (if the server has a separate communication and management module);</p> <p>Automatically inform the administrator of all failures and predictions of malfunctions of the disk subsystem, memory modules, power supplies, fans and processors by e-mail or by displaying a message to the administrator console;</p> <p>Displaying inventory information about installed computing node components, including information about installed versions of microcodes of server components, information about MAC addresses and WWN of network controllers and FC adapters, including virtual ones;</p> <p>Remote reboot, enable/disable the computing node (including booting from the virtual optical drive);</p> <p>Remote capture of the management console of the computing node (virtual console): screen, keyboard and coordinate graphical pointer</p> |
|---|--|

систем. Виртуальная консоль должна иметь возможность управления питанием вычислительного узла, возможность указания загрузочного устройства, с одновременным подключением до 6 пользователей и взаимодействием в режиме обмена сообщениями. Виртуальная консоль должна поддерживать работу с использованием веб-браузера и стандарта HTML5, без необходимости использования плагинов Java и ActiveX; Возможность сбора информации об уровне утилизации центрального процессора и оперативной памяти сервера без необходимости установки агентского ПО в ОС;

Возможность управления RAID-контроллерами, устанавливаемых внутри корпуса вычислительного узла, через веб-интерфейс или командный интерфейс модуля управления без необходимости установки агентского ПО в ОС. Как минимум должна обеспечиваться возможность:

Возможность управления RAID-контроллером без необходимости перезагрузки вычислительного узла;

Отслеживание состояния накопителей, подключенных к RAID-контроллеру, в т.ч. и NVMe-накопителей;

Отслеживание состояния виртуальных дисков;

Создание, удаление и конфигурирование виртуальных дисков;

Изменение настроек RAID-контроллера;

Расширение ёмкости виртуальных дисков без прерывания доступа к ним;

Изменения уровня RAID виртуальных дисков без прерывания доступа к ним;

Запись конфигурации вычислительного узла, драйверов, хранения резервного образа вычислительного узла для перезагрузки в случае возникновения неполадок на энергонезависимый носитель, устанавливаемый внутри корпуса вычислительного узла или на сетевой файловый ресурс;

Возможность генерации NMI;

Возможность сохранения скриншота экрана описания системного сбоя с выводом диагностической информации;

Возможность через веб-интерфейс или интерфейс командной строки экспорта диагностической информации о состоянии вычислительного узла, включая логи как с модуля управления сервером, так и логи операционной системы или гипервизора, в едином консолидированном отчёте.

Запись конфигурации модуля управления на выделенный энергонезависимый накопитель, устанавливаемый внутри корпуса вычислительного узла, для быстрого восстановления работоспособности вычислительного узла в случае замены материнской платы;

both at the stage of loading the computing node and during operation of operating systems. The virtual console should be able to control the power of the computing node, the ability to specify the boot device, with simultaneous connection of up to 6 users and interaction in the message exchange mode. The Virtual Console should support work with a web browser and HTML5 standard, without the need to use Java and ActiveX plugins;

Ability to collect information on the utilization level of the CPU and RAM of the server without the need to install agent software in the operating system;

It is possible to manage RAID controllers installed inside the computing node housing through a web interface or command interface of the management module without the need to install agent software in the OS. At a minimum, it should be possible to do so:

Ability to manage the RAID controller without having to reboot the computing node;

Track the status of drives connected to the RAID controller, including NVMe drives;

Tracking the status of virtual disks;

Create, delete and configure virtual disks;

Change the RAID controller settings;

Extend the capacity of virtual drives without interrupting access to them;

Change the RAID level of virtual drives without interrupting access to them;

Recording of the computing node configuration, drivers, storage of the backup image of the computing node for rebooting in case of a problem on the non-volatile media installed inside the computing node enclosure or on the network file share;

NMI generation capability;

It is possible to save a screenshot of a description screen of a system failure with diagnostic information output;

The ability to export diagnostic information about the state of the computing node, including logs from the server management module, as well as logs of the operating system or hypervisor, in a single

| | |
|---|--|
| <p>Возможность использования аппаратно-программных средств для подготовки к установке операционной системы (конфигурирование томов, создание разделов, копирование драйверов, создание файлов ответа для инсталляторов ОС), не требующие использования внешних носителей информации;</p> <p>Возможность применения обновлений микрокодов компонент вычислительного узла как через интерфейс модуля управления сервером, так и из поддерживаемых операционных систем;</p> <p>Модуль управления сервером должен иметь функционал безопасной проверки целостности и неизменности пакетов обновлений микрокодов компонент вычислительного узла на этапе подготовки обновления;</p> <p>Модуль управления сервером должен поддерживать возможность перевода модуля в режим запрета вноса каких-либо изменений в конфигурацию сервера, таких, как настройки BIOS, обновление микрокода, настроек модуля управления;</p> <p>Модуль управления сервера должен поддерживать возможность управления группой идентичных серверов до не менее 90 шт.</p> <p>Должен поставляться с гарантийными обязательствами производителя в течение годового гарантийного срока с даты продажи конечному пользователю. Гарантийные обязательства производителя должны включать: Круглосуточные консультации инженеров «горячей линии» производителя по вопросам восстановления работоспособности, эксплуатации оборудования и программного обеспечения в режиме реального времени;</p> <p>Замена неисправных аппаратных компонент на месте эксплуатации авторизованными сервисными инженерами производителя/уполномоченными производителем на площадке заказчика на следующий рабочий день;</p> <p>Возможность приобретения оборудования с гарантийными обязательствами производителя до 7 (семи) лет с даты продажи конечному пользователю;</p> <p>Наличие опции невозврата неисправных жестких дисков производителю в случае их аппаратной неисправности не менее 3 (трех) лет.</p> | <p>consolidated report through a web interface or command line interface.</p> <p>Write the control module configuration to a dedicated non-volatile drive installed inside the computing node case to quickly restore the computing node in case the motherboard is replaced;</p> <p>The ability to use hardware and software tools to prepare for operating system installation (configuring volumes, creating partitions, copying drivers, creating answer files for OS installers) that do not require external media;</p> <p>It is possible to apply updates of microcode components of the computing node both through the server management module interface and from supported operating systems;</p> <p>The server management module should have the functionality of securely verifying the integrity and constancy of microcode service packs of the computing node components during the update preparation stage;</p> <p>The Server Management Module should support the ability to disable any changes to the server configuration such as BIOS settings, microcode updates, control module settings;</p> <p>The Server Management Module must support the ability to manage a group of identical servers up to a minimum of 90 pieces.</p> <p>Must be delivered with the manufacturer's warranty within a one-year warranty period from the date of sale to the end user. The manufacturer's warranty obligations shall include:</p> <p>Round-the-clock consultations of the manufacturer's hotline engineers on the issues of recovery, equipment and software operation in real time;</p> <p>Faulty hardware components are replaced at the customer's site by the manufacturer's authorized service engineers/authorized by the manufacturer on the next working day;</p> <p>Possibility to purchase equipment with manufacturer's warranty up to 7 (seven) years from the date of sale to the end user;</p> <p>The option of not returning faulty hard disks to the manufacturer in case of hardware malfunction for at least 3 (three) years.</p> |
|---|--|

| | |
|--|---|
| <p>Система виртуализации DCVM - количество 1 комплект (тип – DCVRTM)</p> <p>Общие требования Образ гипервизора модуля виртуализации должен иметь возможность записывания на SD карту, установленную внутри сервера.</p> <p>Гипервизор Установка гипервизора на «голое железо» (bare-metal); Отсутствие базовой ОС общего назначения в составе гипервизора; Минимальный объем гипервизора (не более 200 МБ); Поддержка 32- и 64-битных гостевых операционных систем (ОС); работающих на серверах стандартной архитектуры x86; Возможность объединения физических серверов в кластер до 64 узлов, обеспечивающих постоянную доступность виртуальной машины с числом виртуальных процессоров до 4, даже в случае отказа физического сервера; Сохранение работоспособности кластерной службы при отказе более половины серверов; Поддержка хост-серверов с количеством процессоров до 480; Поддержка хост-серверов с объемом памяти до 12 ТБ; Подсистема взаимодействия с системами хранения данных Интеграция с системами хранения данных для повышения производительности операций ввода-вывода; Использование специализированной кластерной файловой системы для оптимизации работы с виртуальными машинами и снижения издержек по управлению размещением дисков виртуальных машин; Поддержка томов системы хранения до 64 ТБ; Управление приоритетом операций ввода-вывода для пользовательских ВМ и служебных нужд на разных физических хостах при работе с хранилищем; Поддержка передачи данных по протоколу Fiber Channel, включая все элементы сети хранения данных, со скоростью до 16 Гбит/сек; Поддержка репликации данных виртуальных машин между хранилищами через сеть LAN или WAN встроенными средствами системы виртуализации;</p> | <p>DCVM virtualization system – quantity 1 set (type - DCVRTM)</p> <p>General requirements The hypervisor image of the virtualization module should be able to be written to an SD card installed inside the server.</p> <p>Hypervisor Installation of hypervisor on bare-metal; Lack of basic general-purpose OS in the hypervisor; Minimum hypervisor volume (not more than 200 MB); Support of 32- and 64-bit guest operating systems (OS); running on x86 standard architecture servers; The ability to cluster physical servers into a cluster of up to 64 nodes, ensuring constant availability of the virtual machine with the number of virtual processors up to 4, even in the event of a physical server failure; Keeping the cluster service up and running when more than half the servers fail; Support for host servers with up to 480 processors; Supports host servers with up to 12 TB of memory; Subsystem for interaction with data storage systems Integration with storage systems for improved I/O performance; Use a specialized cluster file system to optimize work with virtual machines and reduce the cost of managing disk placement of virtual machines; Supports storage volumes up to 64 TB; Managing the priority of I/O operations for user VMs and service needs on different physical hosts while working with the storage; Support for Fiber Channel transmission, including all elements of the storage network, at up to 16 Gbps; Supports replication of virtual machine data between stores over LAN or WAN with built-in virtualization tools;</p> |
|--|---|

| | |
|--|---|
| <p>Поддержка кеширования данных виртуальных машин, предназначенных для записи на диск на локальной твердотельной памяти сервера (SSD).</p> <p>Подсистема взаимодействия с сетью передачи данных</p> <p>Управление приоритетом операций ввода-вывода для пользовательских ВМ и служебных нужд на разных физических хостах при работе с локальной сетью;</p> <p>Обеспечение поддержки виртуальных коммутаторов с технологиями Port Groups, Traffic Shaping и VLAN;</p> <p>Поддержка распределенных виртуальных коммутаторов для серверов виртуализации, управляемых централизованно;</p> <p>Поддержка распределенных по физическим серверам виртуальных коммутаторов.</p> <p>Функционал гипервизора должен быть не хуже чем функционал vSphere Standard edition</p> | <p>Support for caching virtual machine data to be written to disk on the server's local solid state memory (SSD).</p> <p>Subsystem of interaction with a data transmission network</p> <p>Managing I/O priority operations for user VMs and service needs on different physical hosts when working with a local network;</p> <p>Provide support for virtual switches with Port Groups, Traffic Shaping and VLAN technologies;</p> <p>Supports distributed virtual switches for centrally managed virtualization servers;</p> <p>Support for virtual switches distributed across physical servers.</p> <p>The functionality of the hypervisor must be no worse than that of vSphere Standard edition</p> |
| <p>Требования к виртуальным машинам</p> <p>Поддержка создания виртуальных машин с объемом оперативной памяти не менее 4 ТБ;</p> <p>Поддержка не менее 128 виртуальных процессоров для одной виртуальной машины (ВМ);</p> <p>Возможность распределения виртуальных процессоров ВМ по виртуальным сокетам, создание многоядерных виртуальных процессоров для отдельных ВМ;</p> <p>«Горячее» добавление процессоров и оперативной памяти для работающей гостевой ОС (для поддерживаемых ОС - без остановки работы гостевой ОС);</p> <p>Поддержка vNUMA для «горячего» добавления памяти;</p> <p>Возможность создания снимков состояния ВМ (как работающей, так и остановленной);</p> <p>Поддержка виртуального графического адаптера с изменяемым размером памяти (до 128 МБ) и поддержка 3D графики для виртуальных машин;</p> <p>Поддержка технологии 3D графики NVIDIA GRID;</p> <p>«Горячее» добавление и увеличение размеров виртуальных дисков для работающей гостевой ОС. Горячее отключение дисков из конфигурации виртуальной машины;</p> <p>Поддержка дисков виртуальных машин объемом до 62 ТБ;</p> <p>Возможность прямого подключения тома системы хранения к ВМ;</p> <p>Поддержка устройств USB (включая версию 3.0) в виртуальных машинах;</p> <p>Возможность прямого подключения PCI/PCIe устройств физического сервера к ВМ;</p> | <p>Requirements for virtual machines</p> <p>Support for creating virtual machines with at least 4 TB of RAM;</p> <p>Support for at least 128 virtual processors for one virtual machine);</p> <p>Ability to distribute VM virtual processors on virtual sockets, creating multi-core virtual processors for individual VMs;</p> <p>"Hot" addition of processors and RAM for running guest OS (for supported OS - without stopping the guest OS);</p> <p>Support vNUMA for "hot" memory addition;</p> <p>Possibility to take pictures of the VM state (both running and stopped);</p> <p>Support for virtual graphics adapter with variable memory size (up to 128 MB) and 3D graphics support for virtual machines;</p> <p>Support for NVIDIA GRID 3D graphics technology;</p> <p>"Hot" add and resize virtual disks for a running guest OS. Hot Disconnect disks from virtual machine configuration;</p> <p>Support for virtual machine drives up to 62 TB;</p> <p>Ability to directly connect the storage volume to the VM;</p> <p>Support for USB devices (including version 3.0) in virtual machines;</p> <p>The ability to directly connect PCI/PCIe devices of the physical server to the VM;</p> |

| | |
|---|---|
| <p>Создание виртуальных машин с динамически расширяющимися дисками (выделение пространства по мере заполнения); Поддержка технологии NPIV.</p> <p>Дополнительные функции Поддержка создания иерархичной структуры пулов вычислительных ресурсов (CPU/RAM) физических серверов с назначением приоритетов или выделенного резерва по ресурсам; Миграция VM между системами хранения данных без простоев с поддержкой миграции нескольких VM одновременно; Миграция VM между виртуальными коммутаторами без простоев; Миграция VM между серверами управления без простоев; Миграция VM с задержками в канале до 100 мс RTT и расстоянием между сайтами до 3000 км без простоев; Поддержка автоматической балансировки нагрузки между серверами виртуализации с учетом загрузки ОЗУ и процессоров; Поддержка настраиваемых шаблонов VM с возможностью определения настроек VM при разворачивании из шаблона; Наличие веб-клиента как средства централизованного управления виртуальной инфраструктурой;</p> <p>Система управления виртуальным хранилищем Решение должно быть тесно интегрировано с гипервизором или быть в его составе Управление при помощи политик, автоматизирующих выполнение стандартных задач и обеспечивают балансировку ресурсов хранения для ускорения процессов управления и оптимизации работы инфраструктуры в целом Единая консоль управления входящая в состав Системы централизованного контроля, управления и визуализации Система управления виртуальным хранилищем должна использовать встроенный кэш на серверных устройствах хранения данных Система должна обеспечивать гибкое горизонтальное и вертикальное масштабирования путем добавления дополнительных серверов в кластер и/или устройств хранения данных в существующие узлы кластера Должна обеспечивать не менее 25 снимков или клонов на одну VM Должна обеспечивать не менее 12000 снимков или клонов на один кластер</p> | <p>Create virtual machines with dynamically expanding disks (allocate space as you fill); Support for NPIV technology.</p> <p>Additional features upport for creating a hierarchical structure of computing resource pools (CPU/RAM) for physical servers with assigned priorities or dedicated reserve resources; VM migration between storage systems without downtime with support for simultaneous migration of multiple VMs; VM migration between virtual switches without downtime; VM migration between control servers without downtime; VM migration with channel delays of up to 100 ms RTT and site spacing of up to 3000 km without downtime; Support for automatic load balancing between virtualization servers based on RAM and processor load; Support for customizable VM templates with the ability to define VM settings when deployed from the template; Availability of a web client as a means of centralized virtual infrastructure management;</p> <p>Virtual Storage Management System The solution must be closely integrated with the hypervisor or be part of it. Manage with policies that automate the execution of standard tasks and balance storage resources to speed up management processes and optimize overall infrastructure performance</p> <p>Single management console included in the Centralized Control, Management and Visualization System The virtual storage management system should use an embedded cache on the server storage devices The system should provide flexible horizontal and vertical scaling by adding additional servers to the cluster and/or storage devices to existing cluster nodes Must provide at least 25 images or clones per VM Must provide at least 12,000 images or clones per cluster</p> |
|---|---|

| | |
|---|--|
| <p>Должна выполнять асинхронную репликацию ВМ в различных средах создавая точки восстановления не более чем 5 минут</p> <p>Должна осуществлять вычисление контрольных сумм для обеспечения целостности данных</p> <p>Должна поддерживать архитектуру: Только твердотельные накопители SAS/SATA накопители Режим mixed</p> <p>Функционал системы управления виртуальным хранилищем должен быть не хуже чем vSAN Standard edition</p> <p>Системами аварийного восстановления и резервирования</p> <p>Система должна полностью интегрироваться с гипервизором, системой управления виртуальным хранилищем и системой централизованного контроля, управления и визуализации</p> <p>Должна выполнять автоматизированное тестирование аварийного переключения в изолированной сети</p> <p>Должна выполнять выполнение аварийное переключение или плановый перенос и возврат восстановленных виртуальных машин в основную среду в рамках единого плана восстановления одним нажатием кнопки.</p> <p>Полная интеграция с виртуальной сетью, для устранения необходимости в перенастройке IP-адресов на восстановленных ВМ.</p> <p>На восстановленных ВМ политики безопасности также должны сохраняться.</p> <p>Система централизованного контроля, управления и визуализации</p> <p>Система централизованного контроля, управления и визуализации должна обеспечивать следующие функции:</p> <p>Клиент на основе HTML 5</p> <p>Интеллектуальный вход в систему позволяющий выполнить один раз и обращаться ко всем экземплярам ПО без повторной проверки подлинности.</p> <p>Поиск по иерархии: удобный поиск по всей иерархии, в том числе по виртуальным машинам, узлам, хранилищам данных и сетям.</p> <p>Оповещения и уведомления: поддержка новых объектов, показателей и событий, таких как оповещения, связанные с определенным хранилищем данных и виртуальной машиной. Эти оповещения могут запускать новые автоматизированные рабочие процессы для устранения и предотвращения возникновения проблем.</p> | <p>Should perform asynchronous replication of VMs in different environments, creating recovery points for no more than 5 minutes</p> <p>Must perform checksumming to ensure data integrity</p> <p>Must support architecture: Solid State Drives Only SAS/SATA drives mixed mode</p> <p>The functionality of the virtual storage management system should be no worse than vSAN Standard edition</p> <p>Disaster recovery and redundancy systems</p> <p>The system should be fully integrated with the hypervisor, the virtual storage management system and the centralized control, management and visualization system.</p> <p>Must perform automated testing of isolated network emergency switching</p> <p>Must perform a failover or scheduled migration and return of recovered virtual machines to the primary environment within a single one-click recovery plan.</p> <p>Full integration with the virtual network, to eliminate the need to reconfigure IP addresses on recovered VMs.</p> <p>Security policies should also be maintained in the restored VM.</p> <p>Central monitoring, control and visualization system</p> <p>The centralized control, management and visualization system shall provide the following functions:</p> <p>HTML 5 based client</p> <p>Intelligent login that allows you to run once and access all instances of the software without having to re-authenticate.</p> <p>Hierarchy Search: Easy search across the hierarchy, including virtual machines, hosts, data warehouses and networks.</p> <p>Alerts and notifications: support for new objects, indicators and events, such as alerts associated with a particular data warehouse and virtual machine. These alerts can launch new automated workflows to fix and prevent problems.</p> |
|---|--|

Встроенные средства резервного копирования и восстановления: готовое решение по резервному копированию на уровне файлов с удобным пользовательским интерфейсом.

Средство планирования резервного копирования и восстановления.

Стандартизация и упрощение управления конфигурациями узлов

Сохранение схемы проверенной конфигурации, включающей в себя параметры сети, хранилища и безопасности, и ее развертывание на множестве узлов для упрощения настройки. Использование политик профилей узлов для отслеживания соответствия нормативным требованиям.

Управление ресурсами виртуальных машин, выделение ресурсов процессора и памяти виртуальным машинам, которые выполняются на одном физическом сервере. Определение минимальных, максимальных и пропорциональных долей ресурсов для ЦП, памяти, диска и полосы пропускания сети. Изменение выделенного объема ресурсов во время работы ВМ.

Динамическое наращивание ресурсов приложений в пиковые периоды нагрузки.

Система должна постоянно отслеживать использование пулов ресурсов и выделяет доступные ресурсы виртуальным машинам на основе заданных правил, отражающих потребности бизнеса и смену приоритетов.

Журналы аудита: регистрация существенных изменений в конфигурации и экспорт отчетов для отслеживания событий.

Централизованное управление исправлениями и обновлениями для обеспечения соответствия стандартам в области установки исправлений за счет автоматического сканирования работающих узлов

Интерфейс управления устройством: в удобном пользовательском интерфейсе

Статистические показатели сетей и баз данных, объем используемого дискового пространства и показатели работоспособности, а также статистические данные процессора и памяти для выполнения задач мониторинга и эксплуатации.

Упрощение управления путем автоматизации выполнения не менее чем 600 задач с помощью готовых рабочих процессов или процессов, составляемых путем перетаскивания элементов.

Требования по количеству

Количество лицензий системы виртуализации должно соответствовать количеству приобретаемого серверного оборудования, указанного в сегменте

Built-in backup and recovery tools: a complete file-level backup solution with a user-friendly interface.

Backup and recovery planning tool.

Standardizing and simplifying management of node configurations
Save a proven configuration schema that includes network, storage and security settings and deploy it to multiple nodes for easy configuration. Use node profile policies to track compliance.

Managing virtual machine resources, allocating processor and memory resources to virtual machines that run on the same physical server. Determining minimum, maximum and proportional shares of resources for CPU, memory, disk and network bandwidth. Change the allocated amount of resources during VM operation.

Dynamic growth of application resources during peak load periods.

The system must constantly monitor the use of resource pools and allocate available resources to virtual machines based on defined rules that reflect business needs and changing priorities.

Audit logs: record significant configuration changes and export reports to track events.

Centralized management of patches and updates to ensure compliance with patching standards through automatic scanning of running nodes

Device control interface: in a user-friendly interface

Network and database statistics, disk space utilization and performance indicators, as well as processor and memory statistics for monitoring and operational tasks.

Simplify control by automating at least 600 tasks with ready-made workflows or drag and drop processes.

Requirements for quantity

The number of virtualization system licenses must correspond to the number of purchased server hardware specified in the Server

| | |
|--|--|
| <p>Серверное оборудование, а именно SRVVM, SRVRVM, SRVRS (ядра и/или процессоры).</p> <p>Количество лицензий системы управления виртуальным хранилищем должно соответствовать количеству приобретаемого серверного оборудования, указанного в сегменте Серверное оборудование, а именно SRVM (ядра и/или процессоры)</p> <p>Допускается поставка лицензий для гипервизора и системы управления виртуальным хранилищем по количеству запускаемых виртуальных машин, а именно для кластера из всех серверов SRVVM не менее 100 виртуальных машин, для кластера SRVRVM не менее 25 виртуальных машин, для кластера из двух серверов SRVRS не менее 25 виртуальных машин, для отдельно стоящего сервера SRVRS не менее 15 виртуальных машин.</p> <p>Топология развертывания:</p> <p>SRVVM – основной гиперконвергентный кластер вычислений, включающий в себя виртуализированное хранилище данных из числа всех дисков узлов SRVVM</p> <p>SRVRVM – резервный, географически НЕ разнесённый, гиперконвергентный кластер вычислений, включающий в себя виртуализированное хранилище данных из числа всех дисков узлов SRVRVM</p> <p>SRVRS – географически удаленные объекты подключающиеся посредством корпоративной сети в MCC (main computing center)</p> <p>В комплект поставки должен быть включен достаточное количество лицензий для развертывания Системы централизованного контроля, управления и визуализации, гипервизора, системы управления виртуальным хранилищем, системами аварийного восстановления и резервирования и др.</p> | <p>hardware segment, namely SRVVM, SRVRVM, SRVRS (cores and/or processors).</p> <p>The number of Virtual Storage Management System licenses must correspond to the number of server hardware purchased, specified in the Server hardware segment, namely SRVM (cores and/or processors).</p> <p>It is allowed to supply licenses for hypervisor and virtual storage management system by the number of virtual machines running, namely for a cluster of all SRVVM servers at least 100 virtual machines, for a cluster of SRVRVM at least 25 virtual machines, for a cluster of two SRVRS servers at least 25 virtual machines, for a stand-alone SRVRS server at least 15 virtual machines.</p> <p>Deployment topology:</p> <p>SRVVM is a core hyper-converged computing cluster that includes virtualized storage of data from all SRVVM node disks.</p> <p>SRVRVM is a redundant, geographically undistributed, hyperconverged computing cluster that includes virtualized storage of data from all SRVRVM node disks.</p> <p>SRVRS - geographically and remotely connected objects via the corporate network in the MCC (main computing center)</p> <p>The package should include a sufficient number of licenses to deploy the Centralized Control, Management and Visualization System, hypervisor, virtual storage management system, disaster recovery and backup systems, etc.</p> |
|--|--|

| | |
|---|--|
| <p>Коммутатор - количество 6 штук (тип – SWCRAG)</p> <p>Требования к коммутатору: Тип – Ethernet коммутатор Наличие порта USB для загрузки конфигурации и проведения операций по модернизации программного обеспечения Объем оперативной памяти не менее 8 ГБ Объем SSD-памяти не менее 32 ГБ Коммутатор должен работать под управлением модульной операционной системы, позволяющей производить запуск, остановку, перезагрузку отдельных программных процессов без влияния на другие работающие процессы Операционная система коммутатора должно поддерживать возможность проверки непротиворечивости конфигурации перед применением конфигурации, пакетное применение команд конфигурации, применения проверенной конфигурации в заранее установленное время, возврата на предыдущую работоспособную конфигурацию в случае ошибки администратора Производительность не менее 1070 млн. пакетов в секунду. Производительность не менее 1440 Гбит/секунду.</p> <p>Требование к физическим интерфейсам Не менее 32 портов 1000BASE-X/10GBASE-X с разъемами для модулей SFP/SFP+ Не менее 4 портов 40GBASE-X с разъемами для модулей QSFP+ Наличие не менее 2 выделенных интерфейса 10/100/1000Base-T для управления через Ethernet Наличие консольного порта RJ45 для управления по протоколу RS-232 Наличие консольного Mini-USB порта для управления по протоколу RS-232</p> <p>Поддержка следующих типов трансиверов: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-USR, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR, 40GBASE-SR4, 40GBASE-ESR4, 40GBASE-LR4, 40GBASE-LX4, 4x10BASE-IR, 40GBASE-IR4</p> | <p>Switch - quantity 6 pcs (type - SWCRAG)</p> <p>Requirements for the switch: Type - Ethernet switch Availability of USB port for downloading configuration and software upgrade operations At least 8 GB of RAM SSD memory capacity of at least 32 GB The switch should operate under the control of a modular operating system that allows to start, stop, reboot individual program processes without affecting other running processes</p> <p>The switch operating system must support the ability to verify configuration consistency before applying the configuration, apply configuration commands in batch, apply the validated configuration at a predetermined time, return to the previous valid configuration in case of an administrator error.</p> <p>Capacity of at least 1,070 million packets per second. Performance at least 1440 Gbps.</p> <p>Requirement for physical interfaces At least 32 ports 1000BASE-X/10GBASE-X with connectors for SFP/SFP+ modules At least 4 40GBASE-X ports with connectors for QSFP+ modules At least 2 dedicated 10/100/1000Base-T interfaces for Ethernet control. Presence of RJ45 console port for RS-232 protocol management Presence of Mini-USB console port for RS-232 protocol control.</p> <p>Support for the following types of transceivers: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-USR, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER,</p> |
|---|--|

Физические параметры

Наличие возможности питания от переменного тока с параметрами 50Гц/220В
Возможность установки резервируемых блоков питания по схеме N+N с балансировкой нагрузки между ними

Наличие съемных резервируемых блоков вентиляторов, поддержка их замены без выключения коммутатора

Наличие встроенного температурного датчика

Максимальное энергопотребление коммутатора не более 360 Вт

Дизайн для установки в монтажный конструктив 19” соответствующий стандарту ANSI/EIA-310

Комплект поставки должен включать:

кабели питания – не менее 2 шт.,

консольный кабель,

набор для монтажа в стойку

Коммутатор должен поставляться с двумя блоками питания

Направление движения воздушного потока охлаждения **Горячий**

воздух должен выбрасываться со стороны блоков питания. Подача холодного воздуха со стороны портов Ethernet.

Требования к программному обеспечению

Не менее 4 сессий для анализа на уровне порта (mirroring)

Поддержка анализа трафика (mirroring) на порту, VLAN

Поддержка функции анализа микровсплесков трафика

Требования к функциональности физического уровня

Поддержка digital optical monitoring (DOM)

Требования к функциональности 2-го уровня

Поддержка кадров большой длины, не менее 9216 байт

Количество одновременно поддерживаемых VLAN не менее 4091

Максимальное количество поддерживаемых MAC адресов не менее 288 000

Количество записей ARP не менее 48 000

Поддержка стандарта IEEE802.3ad – Link Aggregation Control Protocol (LACP)

Поддержка технологии агрегации Ethernet каналов с балансировкой по MAC-адресу источника/назначения, IP-адресу источника/назначения, TCP/UDP-портам источника/назначения

Не менее 32 портов в агрегационной группе

10GBASE-ZR, 40GBASE-SR4, 40GBASE-ESR4, 40GBASE-LR4, 4x10BASE-IR, 40GBASE-IR4, 40GBASE-LR.

Physical parameters

Availability of power supply from AC with parameters 50Hz/220V

Ability to install redundant power supplies in N+N circuit with load balancing between them

Availability of removable redundant fan blocks, support for their replacement without switching off the switch.

Presence of an integrated temperature sensor

Maximum switch power consumption not exceeding 360W

Design for installation in 19" ANSI/EIA-310 compliant mounting structure

The scope of delivery must include:

power cables - at least 2 pcs,

console cable,

rack mounting kit

The switch should come with two power supplies

Direction of air cooling flow Hot air should be discharged from the power supply side. Cold air supply on the Ethernet port side.

Software Requirements

At least 4 sessions for analysis at the port level (mirroring)

Support for mirroring on port, VLAN

Support for microburst traffic analysis function

Requirements for physical layer functionality

Support for digital optical monitoring (DOM)

Requirements for Level 2 functionality

Support long frame length, at least 9216 bytes

Number of simultaneously supported VLANs at least 4091

Maximum number of addresses supported by ICA at least 288,000

Number of ARP records at least 48,000

IEEE802.3ad - Link Aggregation Control Protocol (LACP) support

| | |
|--|--|
| <p>Не менее 128 поддерживаемых агрегационных групп</p> <p>Поддержка стандартов</p> <p>IEEE802.1D – Spanning Tree Protocol (STP);</p> <p>IEEE802.1w – Rapid Spanning Tree Protocol (RSTP);</p> <p>IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);</p> <p>Поддержка стандартов IEEE 802.1AB: Link Layer Discovery Protocol LLDP;</p> <p>IEEE 802.1p: Class-of-service (CoS) prioritization;</p> <p>IEEE 802.1Q-in-Q: VLAN Stacking</p> <p>Поддержка Private VLAN и QinQ на одном интерфейсе</p> <p>Поддержка интерфейса IRB в Private VLAN</p> <p>Требования к функциональности 3-го уровня</p> <p>Поддержка Jumbo-frames на логических интерфейсах VLAN</p> <p>Поддержка Статической маршрутизации (RFC 1812)</p> <p>Количество IPv4 Unicast маршрутов не менее 128 000</p> <p>Количество IPv6 Unicast маршрутов не менее 64 000</p> <p>Поддержка протокола Bidirectional Forwarding Detection (BFD)</p> <p>Поддержка протоколов маршрутизации RIP v1/v2, OSPF v1/v2</p> <p>Поддержка протоколов маршрутизации BGP, MP-BGP, IS-IS, IS-IS for IPv6, IPv6 BGP при наличии приобретаемой отдельно лицензии на расширенный функционал маршрутизации</p> <p>Поддержка протоколов маршрутизации OSPFv3, RIPng</p> <p>Поддержка IPv4 VRF-lite , IPv4 VRF-lite для PIM и IGMP</p> <p>Требования к функциональности MPLS</p> <p>Поддержка RSVP LSP, LDP LSP, LDP over RSVP, MPLS L2 VPN, MPLS L3 VPN, MPLS Fast Reroute, MPLS OAM ping</p> <p>Протоколы конвергентных сетей</p> <p>Поддержка Data Center Bridging Capability Exchange protocol (DCBX), FIP snooping, Priority-based flow control (PFC), Enhanced Transmission Selection (ETS), FC-BB-6, Virtual Fiber Channel Gateway (VFG), FCoE LAG, FC-BB-6 VN2VN snooping</p> <p>Многоадресная передача (Multicast)</p> <p>Количество IPv4 Multicast маршрутов не менее 104 000</p> <p>Количество IPv6 Multicast маршрутов не менее 52 000</p> <p>Поддержка протоколов многоадресной передачи:</p> | <p>Supports Ethernet link aggregation technology with balancing by source/destination MAC address, source/destination IP address, TCP/UDP source/destination ports</p> <p>At least 32 ports in the aggregation group</p> <p>At least 128 supported aggregation groups</p> <p>Support for standards</p> <p>IEEE802.1D - Spanning Tree Protocol (STP);</p> <p>IEEE802.1w - Rapid Spanning Tree Protocol (RSTP);</p> <p>IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);</p> <p>Support for IEEE 802.1AB standards: Link Layer Discovery Protocol LLDP;</p> <p>IEEE 802.1p: Class-of-service (CoS) prioritization;</p> <p>IEEE 802.1Q-in-Q: VLAN Stacking</p> <p>Supports Private VLAN and QinQ on the same interface</p> <p>Support for IRB interface in Private VLAN</p> <p>Requirements for Level 3 functionality</p> <p>Support for Jumbo-frames on VLAN logical interfaces</p> <p>Supports Static Routing (RFC 1812)</p> <p>Number of IPv4 Unicast routes at least 128,000</p> <p>Number of IPv6 Unicast routes at least 64,000</p> <p>Bidirectional Forwarding Detection (BFD) protocol support</p> <p>Support for RIP v1/v2, OSPF v1/v2 routing protocols</p> <p>Support of BGP, MP-BGP, IS-IS, IS-IS for IPv6, IPv6 BGP routing protocols if a license for advanced routing functionality is purchased separately</p> <p>Support for OSPFv3, RIPng routing protocols</p> <p>Support IPv4 VRF-lite , IPv4 VRF-lite for PIM and IGMP</p> <p>MPLS Functionality Requirements</p> <p>Support RSVP LSP, LDP LSP, LDP over RSVP, MPLS L2 VPN, MPLS L3 VPN, MPLS Fast Reroute, MPLS OAM ping</p> <p>Convergent network protocols</p> <p>Поддержка Data Center Bridging Capability Exchange protocol (DCBX), FIP snooping, Priority-based flow control (PFC), Enhanced Transmission Selection (ETS), FC-BB-6, Virtual Fiber Channel Gateway (VFG), FCoE LAG, FC-BB-6 VN2VN snooping</p> |
|--|--|

Internet Group Management Protocol (IGMP) v1/v2/v3
Поддержка IGMP snooping v1/v2/v3, IGMP фильтрации
Поддержка протоколов PIM-SM, PIM-SSM
Поддержка Multicast Listener Discovery (MLD) Protocol v1/v2
Поддержка Multicast Source Discovery Protocol

Качество обслуживания (QoS)

Поддержка стандартов:
RFC 2474: DiffServ Precedence
RFC 2598: DiffServ Expedited Forwarding (EF)
RFC 2597: DiffServ Assured Forwarding (AF)
Поддержка механизмов управления очередями:
Weighted Tail Drop scheduling,
Smoothed Deficit Weighted Round Robin (SDWRR) queuing, Weighted early detection (WRED), Strict priority queuing (LLQ)
Поддержка классификации множественных полей на L2 – L4 уровнях для постановки в очередь и перезаписи
Перемаркировка полей DSCP, IEEE 802.1p и IP precedence на логических L3 интерфейсах VLAN
Классификация на логических L3 интерфейсах VLAN
Поддержка механизмов CoS на логических агрегированных интерфейсах
Количество аппаратных очередей на порт не менее 12

Стекирование

Поддержка функции стекирования коммутаторов при которой несколько объединённых в стек коммутаторов представляют собой единое логическое устройство
Количество коммутаторов, которые можно объединить в стек не менее 10
Агрегированная максимальная производительность шины стека не менее 640 Гбит/с
Возможность объединения в стек с моделями коммутаторов других серий

Высокая доступность

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора

Multicast

Number of IPv4 Multicast routes at least 104,000
Number of IPv6 Multicast routes at least 52,000
Support for multicast protocols:
a. Internet Group Management Protocol (IGMP) v1/v2/v3
Support IGMP snooping v1/v2/v3, IGMP filtering
Support for PIM-SM, PIM-SSM protocols
Support for Multicast Listener Discovery (MLD) Protocol v1/v2
Support for Multicast Source Discovery Protocol

Quality of Service (QoS)

Support for standards:
RFC 2474: DiffServ Precedence
RFC 2598: DiffServ Expedited Forwarding (EF)
RFC 2597: DiffServ Assured Forwarding (AF) .
Support for queue management mechanisms:
Weighted Tail Drop scheduling,
Smoothed Deficit Weighted Round Robin (SDWRR) queuing,
Weighted early detection (WRED), Strict priority queuing (LLQ)
Support for multiple field classification at L2 - L4 levels for queuing and rewriting
DSCP, IEEE 802.1p and IP precedence fields marked on logical L3 VLAN interfaces
Classification on logical L3 VLAN interfaces
Support for CoS mechanisms on logical aggregated interfaces
Number of hardware queues per port at least 12

Stacking

Support for switch stacking where multiple stacked switches represent a single logical device
Number of switches that can be stacked at least 10
Aggregate maximum stack bus performance of at least 640 Gbps
Ability to stack with models of switches of other series

High availability

стека плоскость передачи данных не выполняет реинициализацию, что минимизирует влияние на передаваемые данные.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления протоколов маршрутизации 3 уровня OSI с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость управления не выполняет перестройки топологии протоколов маршрутизации 3 уровня OSI.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления протоколов 2 уровня OSI с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость управления не выполняет перестройки топологии протоколов 2 уровня OSI.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке возможно обновление программного обеспечения без выключения всего стека

Поддержка механизма высокой доступности при котором возможно обновление программного обеспечения коммутатора без его перезагрузки

Поддержка Virtual Router Redundancy Protocol

Поддержка Multichassis link aggregation group (MC-LAG/M-LAG) или аналога

Информационная безопасность

Поддержка:

Port-based ACL (PACL) для входящего трафика и исходящего трафика;

VLAN-based ACL (VACL) для входящего и исходящего трафика;

Router-based ACL (RACL) для входящего и исходящего трафика

Поддержка фильтрации средствами списков контроля доступа на уровнях 2-4 модели OSI

Поддержка ограничения количества MAC-адресов на порту

Возможность ручной настройки разрешенных MAC-адресов на порту

Поддержка механизма Dynamic ARP inspection (DAI)

Поддержка механизма IP source guard

Поддержка механизма DHCP snooping

Поддержка протоколов RADIUS и TACACS+

Защита плоскости управления от атак DoS/DDoS

Support for a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the control information with the main master switch and, in the event of a failure of the main stack master switch, the data plane does not reinitialize, minimizing the impact on the data being transmitted.

Supports a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the routing protocol management information for layer 3 routing protocols with the master stack master switch and, if the master stack master switch fails, the management plane does not reconfigure the routing protocol topology for layer 3 OSI routing protocols.

Supports a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant master stack switch synchronizes the OSI layer 2 protocol management information with the master stack master switch and, in the event of a failure of the master stack master switch, the control plane does not reconfigure the OSI layer 2 protocol topology.

Support for a high availability mechanism where the switches in the stack can update the software without shutting down the entire stack

Support for a high availability mechanism where the switch software can be updated without rebooting the switch

Support for Virtual Router Redundancy Protocol

Support for Multichassis link aggregation group (MC-LAG/M-LAG) or analogue

Information Security

Support:

Port-based ACL (PACL) for incoming and outgoing traffic;

VLAN-based ACL (VACL) for incoming and outgoing traffic;

Router-based ACL (RACL) for inbound and outbound traffic

Support for filtering by Drop Lists at Layers 2-4 of the OSI

Support for limiting the number of MAC addresses on the port

Possibility to manually set the allowed MAC addresses on the port

Support for Dynamic ARP inspection (DAI) mechanism

IP source guard mechanism support

DHCP snooping mechanism support

| | |
|---|--|
| <p>Поддержка аутентификации 802.1X (port-based, multiple supplicant, с возможностью назначения VLAN, динамических списков контроля доступа на основе атрибутов RADIUS)</p> <p>Поддержка аутентификации 802.1X MAC-RADIUS</p> <p>Поддержка внутреннего инструмента операционной системы, который выполняет сканирование памяти, директорий ОС и исполняемых файлов на наличие вредоносного кода (malware)</p> <p>Управление</p> <p>Поддержка sFlow v5</p> <p>Поддержка OpenFlow v.1.0 и v.1.3.1 или выше</p> <p>Возможность настройки коммутатора как через интерфейс командной строки, так и через telnet</p> <p>Поддержка SSHv2</p> <p>Поддержка протокола SNMP v1/v2c/v3 в том числе для мониторинга статистики туннельных интерфейсов</p> <p>Поддержка конфигурационного файла ASCII</p> <p>Возможность написания и выполнения скриптов SLAX, XSLT, Python</p> <p>Поддержка сторонних YANG-моделей</p> <p>Поддержка OpenConfig</p> <p>Поддержка конфигурационного файла в формате JSON</p> <p>Поддержка gRPC для интерфейса сбора статистических данных с устройства</p> <p>Поддержка хранения на устройстве резервной конфигурации устройства</p> <p>Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию, поддержка возврата устройства на предыдущую версию ПО</p> <p>Не менее 49 конфигураций, которые автоматически сохраняются в памяти устройства, на которые возможно осуществить возврат конфигурации устройства</p> <p>Поддержка протоколов DNS, Syslog</p> <p>Поддержка функциональности DHCP сервера, DHCP Relay</p> | <p>Support for RADIUS and TACACS+ protocols</p> <p>Protect the management plane from DoS/DDoS attacks</p> <p>Supports 802.1X authentication (port-based, multiple supplicant, with VLAN assignment, dynamic access control lists based on RADIUS attributes)</p> <p>Supports 802.1X MAC-RADIUS authentication</p> <p>Support for an internal operating system tool that scans memory, OS directories and executable files for malware</p> <p>Management</p> <p>Support for sFlow v5</p> <p>Support for OpenFlow v.1.0 and v.1.3.1 or higher</p> <p>Ability to configure the switch both via command line interface and via telnet</p> <p>Support SSHv2</p> <p>Support SNMP v1/v2c/v3 protocol including for monitoring statistics of tunnel interfaces</p> <p>Support for ASCII configuration file</p> <p>Ability to write and execute SLAX, XSLT, Python scripts</p> <p>Support for third-party YANG models</p> <p>OpenConfig support</p> <p>Support for JSON format configuration file</p> <p>Support for gRPC for the device statistics collection interface</p> <p>Supports storage on device backup configuration</p> <p>Supports storage on the device back-up configuration, as well as return of the device to the previous configuration, support for return of the device to the previous version of software</p> <p>At least 49 configurations that are automatically saved in the device memory, to which it is possible to return the device configuration</p> <p>Support for DNS protocols, Syslog</p> <p>Support for DHCP server functionality, DHCP Relay</p> |
|---|--|

| | |
|--|---|
| <p>Коммутатор- количество 1 штук (тип – SWAG)</p> <p>Требования к коммутатору: Тип – Ethernet коммутатор Наличие порта USB для загрузки конфигурации и проведения операций по модернизации программного обеспечения Объем оперативной памяти не менее 8 ГБ Объем SSD-памяти не менее 32 ГБ Коммутатор должен работать под управлением модульной операционной системы, позволяющей производить запуск, остановку, перезагрузку отдельных программных процессов без влияния на другие работающие процессы Операционная система коммутатора должно поддерживать возможность проверки непротиворечивости конфигурации перед применением конфигурации, пакетное применение команд конфигурации, применения проверенной конфигурации в заранее установленное время, возврата на предыдущую работоспособную конфигурацию в случае ошибки администратора Производительность не менее 1070 млн. пакетов в секунду. Производительность не менее 1440 Гбит/секунду.</p> <p>Требование к физическим интерфейсам Не менее 24 портов 1000BASE-X/10GBASE-X с разъемами для модулей SFP/SFP+ Не менее 4 портов 40GBASE-X с разъемами для модулей QSFP+ Наличие не менее 2 выделенных интерфейса 10/100/1000Base-T для управления через Ethernet Наличие консольного порта RJ45 для управления по протоколу RS-232 Наличие консольного Mini-USB порта для управления по протоколу RS-232</p> <p>Поддержка следующих типов трансиверов: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-USR, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR, 40GBASE-SR4, 40GBASE-ESR4, 40GBASE-LR4, 40GBASE-LX4, 4x10BASE-IR, 40GBASE-IR4</p> | <p>Switch - quantity 1 pcs (type - SWAG)</p> <p>Requirements for the switch: Type - Ethernet switch Availability of USB port for downloading configuration and software upgrade operations At least 8 GB of RAM SSD memory capacity of at least 32 GB The switch should operate under the control of a modular operating system that allows to start, stop, reboot individual program processes without affecting other running processes</p> <p>The switch operating system must support the ability to verify configuration consistency before applying the configuration, apply configuration commands in batch, apply the validated configuration at a predetermined time, return to the previous valid configuration in case of an administrator error.</p> <p>Capacity of at least 1,070 million packets per second. Performance at least 1440 Gbps.</p> <p>Requirement for physical interfaces At least 24 ports 1000BASE-X/10GBASE-X with connectors for SFP/SFP+ modules At least 4 40GBASE-X ports with connectors for QSFP+ modules At least 2 dedicated 10/100/1000Base-T interfaces for Ethernet control. Presence of RJ45 console port for RS-232 protocol management Presence of Mini-USB console port for RS-232 protocol control.</p> <p>Support for the following types of transceivers: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-USR, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER,</p> |
|--|---|

Физические параметры

Наличие возможности питания от переменного тока с параметрами 50Гц/220В
Возможность установки резервируемых блоков питания по схеме N+N с балансировкой нагрузки между ними

Наличие съемных резервируемых блоков вентиляторов, поддержка их замены без выключения коммутатора

Наличие встроенного температурного датчика

Максимальное энергопотребление коммутатора не более 360 Вт

Дизайн для установки в монтажный конструктив 19” соответствующий стандарту ANSI/EIA-310

Комплект поставки должен включать:

кабели питания – не менее 2 шт.,

консольный кабель,

набор для монтажа в стойку

Коммутатор должен поставляться с двумя блоками питания

Направление движения воздушного потока охлаждения **Горячий**

воздух должен выбрасываться со стороны блоков питания. Подача холодного воздуха со стороны портов Ethernet.

Требования к программному обеспечению

Не менее 4 сессий для анализа на уровне порта (mirroring)

Поддержка анализа трафика (mirroring) на порту, VLAN

Поддержка функции анализа микровсплесков трафика

Требования к функциональности физического уровня

Поддержка digital optical monitoring (DOM)

Требования к функциональности 2-го уровня

Поддержка кадров большой длины, не менее 9216 байт

Количество одновременно поддерживаемых VLAN не менее 4091

Максимальное количество поддерживаемых MAC адресов не менее 288 000

Количество записей ARP не менее 48 000

Поддержка стандарта IEEE802.3ad – Link Aggregation Control Protocol (LACP)

Поддержка технологии агрегации Ethernet каналов с балансировкой по MAC-адресу источника/назначения, IP-адресу источника/назначения, TCP/UDP-портам источника/назначения

Не менее 32 портов в агрегационной группе

10GBASE-ZR, 40GBASE-SR4, 40GBASE-ESR4, 40GBASE-LR4, 4x10BASE-IR, 40GBASE-IR4, 40GBASE-LR.

Physical parameters

Availability of power supply from AC with parameters 50Hz/220V

Ability to install redundant power supplies in N+N circuit with load balancing between them

Availability of removable redundant fan blocks, support for their replacement without switching off the switch.

Presence of an integrated temperature sensor

Maximum switch power consumption not exceeding 360W

Design for installation in 19" ANSI/EIA-310 compliant mounting structure

The scope of delivery must include:

power cables - at least 2 pcs,

console cable,

rack mounting kit

The switch should come with two power supplies

Direction of air cooling flow Hot air should be discharged from the power supply side. Cold air supply on the Ethernet port side.

Software Requirements

At least 4 sessions for analysis at the port level (mirroring)

Support for mirroring on port, VLAN

Support for microburst traffic analysis function

Requirements for physical layer functionality

Support for digital optical monitoring (DOM)

Requirements for Level 2 functionality

Support long frame length, at least 9216 bytes

Number of simultaneously supported VLANs at least 4091

Maximum number of addresses supported by ICA at least 288,000

Number of ARP records at least 48,000

IEEE802.3ad - Link Aggregation Control Protocol (LACP) support

| | |
|--|---|
| <p>Не менее 128 поддерживаемых агрегационных групп</p> <p>Поддержка стандартов</p> <p>IEEE802.1D – Spanning Tree Protocol (STP);</p> <p>IEEE802.1w – Rapid Spanning Tree Protocol (RSTP);</p> <p>IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);</p> <p>Поддержка стандартов IEEE 802.1AB: Link Layer Discovery Protocol LLDP;</p> <p>IEEE 802.1p: Class-of-service (CoS) prioritization;</p> <p>IEEE 802.1Q-in-Q: VLAN Stacking</p> <p>Поддержка Private VLAN и QinQ на одном интерфейсе</p> <p>Поддержка интерфейса IRB в Private VLAN</p> <p>Требования к функциональности 3-го уровня</p> <p>Поддержка Jumbo-frames на логических интерфейсах VLAN</p> <p>Поддержка Статической маршрутизации (RFC 1812)</p> <p>Количество IPv4 Unicast маршрутов не менее 128 000</p> <p>Количество IPv6 Unicast маршрутов не менее 64 000</p> <p>Поддержка протокола Bidirectional Forwarding Detection (BFD)</p> <p>Поддержка протоколов маршрутизации RIP v1/v2, OSPF v1/v2</p> <p>Поддержка протоколов маршрутизации BGP, MP-BGP, IS-IS, IS-IS for IPv6, IPv6 BGP при наличии приобретаемой отдельно лицензии на расширенный функционал маршрутизации</p> <p>Поддержка протоколов маршрутизации OSPFv3, RIPng</p> <p>Поддержка IPv4 VRF-lite , IPv4 VRF-lite для PIM и IGMP</p> <p>Требования к функциональности MPLS</p> <p>Поддержка RSVP LSP, LDP LSP, LDP over RSVP, MPLS L2 VPN, MPLS L3 VPN, MPLS Fast Reroute, MPLS OAM ping</p> <p>Протоколы конвергентных сетей</p> <p>Поддержка Data Center Bridging Capability Exchange protocol (DCBX), FIP snooping, Priority-based flow control (PFC), Enhanced Transmission Selection (ETS), FC-BB-6, Virtual Fiber Channel Gateway (VFG), FCoE LAG, FC-BB-6 VN2VN snooping</p> <p>Многоадресная передача (Multicast)</p> <p>Количество IPv4 Multicast маршрутов не менее 104 000</p> <p>Количество IPv6 Multicast маршрутов не менее 52 000</p> <p>Поддержка протоколов многоадресной передачи:</p> | <p>Supports Ethernet link aggregation technology with balancing by source/destination MAC address, source/destination IP address, TCP/UDP source/destination ports</p> <p>At least 32 ports in the aggregation group</p> <p>At least 128 supported aggregation groups</p> <p>Support for standards</p> <p>IEEE802.1D - Spanning Tree Protocol (STP);</p> <p>IEEE802.1w - Rapid Spanning Tree Protocol (RSTP);</p> <p>IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);</p> <p>upport for IEEE 802.1AB standards: Link Layer Discovery Protocol LLDP;</p> <p>IEEE 802.1p: Class-of-service (CoS) prioritization;</p> <p>IEEE 802.1Q-in-Q: VLAN Stacking</p> <p>Supports Private VLAN and QinQ on the same interface</p> <p>Support for IRB interface in Private VLAN</p> <p>Requirements for Level 3 functionality</p> <p>Support for Jumbo-frames on VLAN logical interfaces</p> <p>Supports Static Routing (RFC 1812)</p> <p>Number of IPv4 Unicast routes at least 128,000</p> <p>Number of IPv6 Unicast routes at least 64,000</p> <p>Bidirectional Forwarding Detection (BFD) protocol support</p> <p>Support for RIP v1/v2, OSPF v1/v2 routing protocols</p> <p>Support of BGP, MP-BGP, IS-IS, IS-IS for IPv6, IPv6 BGP routing protocols if a license for advanced routing functionality is purchased separately</p> <p>Support for OSPFv3, RIPng routing protocols</p> <p>Support IPv4 VRF-lite , IPv4 VRF-lite for PIM and IGMP</p> <p>MPLS Functionality Requirements</p> <p>Support RSVP LSP, LDP LSP, LDP over RSVP, MPLS L2 VPN, MPLS L3 VPN, MPLS Fast Reroute, MPLS OAM ping</p> <p>Convergent network protocols</p> <p>Поддержка Data Center Bridging Capability Exchange protocol (DCBX), FIP snooping, Priority-based flow control (PFC), Enhanced Transmission Selection (ETS), FC-BB-6, Virtual Fiber Channel Gateway (VFG), FCoE LAG, FC-BB-6 VN2VN snooping</p> |
|--|---|

Internet Group Management Protocol (IGMP) v1/v2/v3
Поддержка IGMP snooping v1/v2/v3, IGMP фильтрации
Поддержка протоколов PIM-SM, PIM-SSM
Поддержка Multicast Listener Discovery (MLD) Protocol v1/v2
Поддержка Multicast Source Discovery Protocol

Качество обслуживание (QoS)

Поддержка стандартов:
RFC 2474: DiffServ Precedence
RFC 2598: DiffServ Expedited Forwarding (EF)
RFC 2597: DiffServ Assured Forwarding (AF)
Поддержка механизмов управления очередями:
Weighted Tail Drop scheduling,
Smoothed Deficit Weighted Round Robin (SDWRR) queuing, Weighted early detection (WRED), Strict priority queuing (LLQ)
Поддержка классификации множественных полей на L2 – L4 уровнях для постановки в очередь и перезаписи
Перемаркировка полей DSCP, IEEE 802.1p и IP precedence на логических L3 интерфейсах VLAN
Классификация на логических L3 интерфейсах VLAN
Поддержка механизмов CoS на логических агрегированных интерфейсах
Количество аппаратных очередей на порт не менее 12

Стекирование

Поддержка функции стекирования коммутаторов при которой несколько объединённых в стек коммутаторов представляют собой единое логическое устройство
Количество коммутаторов, которые можно объединить в стек не менее 10
Агрегированная максимальная производительность шины стека не менее 640 Гбит/с
Возможность объединения в стек с моделями коммутаторов других серий

Высокая доступность

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора

Multicast

Number of IPv4 Multicast routes at least 104,000
Number of IPv6 Multicast routes at least 52,000
Support for multicast protocols:
Internet Group Management Protocol (IGMP) v1/v2/v3
Support IGMP snooping v1/v2/v3, IGMP filtering
Support for PIM-SM, PIM-SSM protocols
Support for Multicast Listener Discovery (MLD) Protocol v1/v2
Support for Multicast Source Discovery Protocol
Quality of Service (QoS)
Support for standards:
RFC 2474: DiffServ Precedence
RFC 2598: DiffServ Expedited Forwarding (EF)
RFC 2597: DiffServ Assured Forwarding (AF) .
Support for queue management mechanisms:
Weighted Tail Drop scheduling,
Smoothed Deficit Weighted Round Robin (SDWRR) queuing,
Weighted early detection (WRED), Strict priority queuing (LLQ)
Support for multiple fields classification at L2 - L4 levels for queuing and rewriting
DSCP, IEEE 802.1p and IP precedence fields marked on logical L3 VLAN interfaces
Classification on logical L3 VLAN interfaces
Support for CoS mechanisms on logical aggregated interfaces
Number of hardware queues per port at least 12

Stacking

Support for switch stacking where multiple stacked switches represent a single logical device
Number of switches that can be stacked at least 10
Aggregate maximum stack bus performance of at least 640 Gbps
Ability to stack with models of switches of other series

High availability

стека плоскость передачи данных не выполняет реинициализацию, что минимизирует влияние на передаваемые данные.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления протоколов маршрутизации 3 уровня OSI с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость управления не выполняет перестройки топологии протоколов маршрутизации 3 уровня OSI.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления протоколов 2 уровня OSI с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость управления не выполняет перестройки топологии протоколов 2 уровня OSI.

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке возможно обновление программного обеспечения без выключения всего стека

Поддержка механизма высокой доступности при котором возможно обновление программного обеспечения коммутатора без его перезагрузки

Поддержка Virtual Router Redundancy Protocol

Поддержка Multichassis link aggregation group (MC-LAG/M-LAG) или аналога

Информационная безопасность

Поддержка:

Port-based ACL (PACL) для входящего трафика и исходящего трафика;

VLAN-based ACL (VACL) для входящего и исходящего трафика;

Router-based ACL (RACL) для входящего и исходящего трафика

Поддержка фильтрации средствами списков контроля доступа на уровнях 2-4 модели OSI

Поддержка ограничения количества MAC-адресов на порту

Возможность ручной настройки разрешенных MAC-адресов на порту

Поддержка механизма Dynamic ARP inspection (DAI)

Поддержка механизма IP source guard

Поддержка механизма DHCP snooping

Поддержка протоколов RADIUS и TACACS+

Защита плоскости управления от атак DoS/DDoS

Support for a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the control information with the main master switch and, in the event of a failure of the main stack master switch, the data plane does not reinitialize, minimizing the impact on the data being transmitted.

Supports a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the routing protocol management information for layer 3 routing protocols with the master stack master switch and, if the master stack master switch fails, the management plane does not reconfigure the routing protocol topology for layer 3 OSI routing protocols.

Supports a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant master stack switch synchronizes the OSI layer 2 protocol management information with the master stack master switch and, in the event of a failure of the master stack master switch, the control plane does not reconfigure the OSI layer 2 protocol topology.

Support for a high availability mechanism where the switches in the stack can update the software without shutting down the entire stack

Support for a high availability mechanism where the switch software can be updated without rebooting the switch

Support for Virtual Router Redundancy Protocol

Support for Multichassis link aggregation group (MC-LAG/M-LAG) or analogue

Information Security

Support:

Port-based ACL (PACL) for incoming and outgoing traffic;

VLAN-based ACL (VACL) for incoming and outgoing traffic;

Router-based ACL (RACL) for inbound and outbound traffic

Support for filtering by Drop Lists at Layers 2-4 of the OSI

Support for limiting the number of MAC addresses on the port

Possibility to manually set the allowed MAC addresses on the port

Support for Dynamic ARP inspection (DAI) mechanism

IP source guard mechanism support

DHCP snooping mechanism support

| | |
|---|--|
| <p>Поддержка аутентификации 802.1X (port-based, multiple supplicant, с возможностью назначения VLAN, динамических списков контроля доступа на основе атрибутов RADIUS)</p> <p>Поддержка аутентификации 802.1X MAC-RADIUS</p> <p>Поддержка внутреннего инструмента операционной системы, который выполняет сканирование памяти, директорий ОС и исполняемых файлов на наличие вредоносного кода (malware)</p> <p>Управление</p> <p>Поддержка sFlow v5</p> <p>Поддержка OpenFlow v.1.0 и v.1.3.1 или выше</p> <p>Возможность настройки коммутатора как через интерфейс командной строки, так и через telnet</p> <p>Поддержка SSHv2</p> <p>Поддержка протокола SNMP v1/v2c/v3 в том числе для мониторинга статистики туннельных интерфейсов</p> <p>Поддержка конфигурационного файла ASCII</p> <p>Возможность написания и выполнения скриптов SLAX, XSLT, Python</p> <p>Поддержка сторонних YANG-моделей</p> <p>Поддержка OpenConfig</p> <p>Поддержка конфигурационного файла в формате JSON</p> <p>Поддержка gRPC для интерфейса сбора статистических данных с устройства</p> <p>Поддержка хранения на устройстве резервной конфигурации устройства</p> <p>Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию, поддержка возврата устройства на предыдущую версию ПО</p> <p>Не менее 49 конфигураций, которые автоматически сохраняются в памяти устройства, на которые возможно осуществить возврат конфигурации устройства</p> <p>Поддержка протоколов DNS, Syslog</p> <p>Поддержка функциональности DHCP сервера, DHCP Relay</p> | <p>Support for RADIUS and TACACS+ protocols</p> <p>Protect the management plane from DoS/DDoS attacks</p> <p>Supports 802.1X authentication (port-based, multiple supplicant, with VLAN assignment, dynamic access control lists based on RADIUS attributes)</p> <p>Supports 802.1X MAC-RADIUS authentication</p> <p>Support for an internal operating system tool that scans memory, OS directories and executable files for malware</p> <p>Management</p> <p>Support for sFlow v5</p> <p>Support for OpenFlow v.1.0 and v.1.3.1 or higher</p> <p>Ability to configure the switch both via command line interface and via telnet</p> <p>Support SSHv2</p> <p>Support SNMP v1/v2c/v3 protocol including for monitoring statistics of tunnel interfaces</p> <p>Support for ASCII configuration file</p> <p>Ability to write and execute SLAX, XSLT, Python scripts</p> <p>Support for third-party YANG models</p> <p>OpenConfig support</p> <p>Support for JSON format configuration file</p> <p>Support for gRPC for the device statistics collection interface</p> <p>Supports storage on device backup configuration</p> <p>Supports storage on the device back-up configuration, as well as return of the device to the previous configuration, support for return of the device to the previous version of software</p> <p>At least 49 configurations that are automatically saved in the device memory, to which it is possible to return the device configuration</p> <p>Support for DNS protocols, Syslog</p> <p>Support for DHCP server functionality, DHCP Relay</p> |
|---|--|

| | |
|---|--|
| <p>Коммутатор - количество 2 штук (тип – MGMT)</p> <p>Требования к коммутатору управления:</p> <p>Тип устройства - Ethernet коммутатор. Наличие порта USB для загрузки конфигурации и проведения операций с программным обеспечением. Производительность коммутатора должна составлять не менее 95 млн. пакетов в секунду Производительность коммутатора должна составлять не менее 128 Гбит/с Коммутатор должен работать под управлением модульной операционной системы, позволяющей производить запуск, остановку, перезагрузку отдельных программных процессов без влияния на другие работающие процессы Операционная система коммутатора должно поддерживать возможность проверки непротиворечивости конфигурации перед применением конфигурации, применения проверенной конфигурации в заранее установленное время, возврата на предыдущую работоспособную конфигурацию в случае ошибки администратора. Дизайн коммутатора должен соответствовать для установки в монтажный конструктив 19” соответствующий стандарту ANSI/EIA-310.</p> <p>Требование к физическим интерфейсам Не менее 4SFP интерфейсов стандарта 1000/10GBASE-X, которые можно установить в коммутатор. Не менее 24 не блокируемых, работающих на полной скорости среды, портов стандарта 10/100/1000BASE-T RJ-45. Не менее 1 выделенного интерфейса управления через Ethernet Не менее 1 консольного порта RJ-45 для управления по протоколу RS-232 Не менее 1 консольного порта miniUSB для управления по протоколу RS-232 Наличие порта USB для подключения внешних накопителей</p> <p>Физические параметры Наличие возможности питания от переменного тока с параметрами 50Гц/220В</p> | <p>Switch - quantity 2 pcs (type - MGMT)</p> <p>Requirements for the control switch:</p> <p>Device type - Ethernet switch. Availability of a USB port for downloading configuration and performing operations with the software. The performance of the switch should be at least 95 million packets per second. The performance of the switch shall be at least 128 Gbps. The switch should operate under the control of a modular operating system that allows to start, stop, reboot individual program processes without affecting other running processes</p> <p>The switch operating system must support the ability to verify configuration consistency before applying the configuration, apply the validated configuration at a predetermined time, return to the previous valid configuration in case of an administrator error.</p> <p>The switch design must comply with the ANSI/EIA-310 standard for installation in a 19" mounting structure.</p> <p>Requirement for physical interfaces At least 4SFP interfaces of standard 1000/10GBASE-X, which can be installed in the switch. At least 24 non-lockable 10/100/1000BASE-T RJ-45 standard ports operating at full speed.</p> <p>At least 1 dedicated control interface over Ethernet At least 1 RJ-45 console port for RS-232 protocol control At least 1 miniUSB console port for RS-232 protocol control. Availability of USB port for connecting external drives</p> <p>Physical parameters Availability of power supply from AC with parameters 50Hz/220V</p> |
|---|--|

Наличие встроенного температурного датчика
Шум, издаваемый устройством должен составлять не более 34,2 dBA
Энергопотребление не более 55 Вт
Комплект поставки должен включать кабель питания, консольный кабель, набор для монтажа в стойку

Требования к программному обеспечению

Поддержка анализа трафика (mirroring) на порту, VLAN, избирательный захват трафика на основе списков доступа
Поддержка анализа трафика (mirroring) нескольких портов назначения в один порт анализатора
Поддержка анализа трафика с удаленного устройства
Поддержка при наличии приобретаемой отдельно лицензии функции настройки программных пробников в виде пакетов протоколов ICMP, UDP/TCP, HTTP для определения доступности узлов сети и параметров каналов связи
Поддержка языка написания скриптов (сценариев) непосредственно на коммутаторе. Язык написания скриптов должен поддерживать общепринятые команды языка Stylesheet Language Alternative Syntax (SLAX) и/или Extensible Stylesheet Language Transformations (XSLT) и/или TCL и/или Python

Требования к функциональности физического уровня

При наличии отдельной лицензии поддержка механизма обеспечения резервирования каналов между коммутаторами. При этом в качестве каналов могут выступать как отдельные физические линии связи, так и логические каналы, состоящие из нескольких физических линий связи
Наличие функции рефлектометра (Time-domain reflectometry, TDR) для определения обрывов и замыканий кабеля
Наличие функции Auto MDI/MDIX
Поддержка диагностики оптических линий Digital Optical Monitoring
Поддержка Energy Efficient Ethernet (EEE)

Требования к функциональности 2-го уровня

Поддержка фреймов большой длины (9216 Байт)
Не менее 4093 Количество поддерживаемых VLANов
Поддерживаемые идентификаторы VLAN (1-4094)
Количество MAC адресов не менее 16000
Количество ARP записей не менее 1500

Presence of an integrated temperature sensor
Noise emitted by the device shall not exceed 34.2 dBA
17. Power consumption not more than 55 Watt
Supply includes power cable, console cable, rack mounting kit.

Software Requirements

Support for mirroring on port, VLAN, selective capturing of traffic based on access lists
Supports mirroring multiple destination ports into a single analyzer port
Support for traffic analysis from remote device
Support for customizing software probes in the form of ICMP, UDP/TCP, HTTP packets to determine the availability of network nodes and link parameters, if a license is purchased separately
Scripting language support directly on the switch. The scripting language must support common Stylesheet Language Alternative Syntax (SLAX) and/or Extensible Stylesheet Language Transformations (XSLT) and/or TCL and/or Python commands.

Requirements for physical layer functionality

If you have a separate license, support for the mechanism of providing channel redundancy between switches. Thus as channels can act both separate physical communication lines, and the logic channels consisting of several physical communication lines
Availability of the Time-domain reflectometry (TDR) function for the detection of cable breaks and short circuits.
Presence of Auto MDI/MDIX function
Support for Digital Optical Monitoring line diagnostics
Supports Energy Efficient Ethernet (EEE)

Requirements for Level 2 functionality

Support long frame lengths (9216 bytes)
At least 4093 Number of VLANs supported
Supported VLAN IDs (1-4094)

| | |
|---|--|
| <p>Поддержка стандарта IEEE802.3ad – Link Aggregation Control Protocol (LACP) Поддержка технологии агрегации Ethernet каналов с балансировкой по MAC-адресу источника/назначения, IP-адресу источника/назначения, TCP/UDP-портам источника/назначения. Не менее 8 портов в агрегационной группе Не менее 128 агрегационных групп Поддержка стандартов IEEE802.1D – Spanning Tree Protocol (STP); IEEE802.1w – Rapid Spanning Tree Protocol (RSTP); IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP); Не менее 64 поддерживаемых экземпляров протокола IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP) Поддержка стандартов IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED; IEEE 802.1p: Class-of-service (CoS) prioritization; IEEE 802.1Q-2006: VLAN tagging; IEEE 802.3: 10BASE-T; IEEE 802.3u: 100BASE-T; IEEE 802.3ab: 1000BASE-T; IEEE 802.3z: 1000BASE-X; IEEE 802.3x: Pause Frames/Flow Control Поддержка IEEE 802.1ad Q-in-Q VLAN Stacking Поддержка Q-in-Q с несколькими S-VLAN на порту с селективным назначением VLAN с использованием списков доступа Поддержка Layer 2 protocol tunneling (L2PT) Поддержка Multiple VLAN Registration Protocol, IEEE 802.1ak</p> | <p>Number of MAC addresses at least 16000 Number of ARP records less than 1500 IEEE802.3ad - Link Aggregation Control Protocol (LACP) support Supports Ethernet link aggregation technology with balancing by source/destination MAC address, source/destination IP address, TCP/UDP source/destination ports. At least 8 ports in the aggregation group At least 128 aggregation groups Support for standards IEEE802.1D - Spanning Tree Protocol (STP); IEEE802.1w - Rapid Spanning Tree Protocol (RSTP); IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP); At least 64 supported IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP) instances Support for standards IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED; IEEE 802.1p: Class-of-service (CoS) prioritization; IEEE 802.1Q-2006: VLAN tagging; IEEE 802.3: 10BASE-T; IEEE 802.3u: 100BASE-T; IEEE 802.3ab: 1000BASE-T; IEEE 802.3z: 1000BASE-X; IEEE 802.3x: Pause Frames/Flow Control Support IEEE 802.1ad Q-in-Q VLAN Stacking Q-in-Q support with some S-VLANs on the port with selective VLAN assignment using access lists Support for Layer 2 protocol tunneling (L2PT) Support Multiple VLAN Registration Protocol, IEEE 802.1ak</p> <p>Requirements for Level 3 functionality Supports Static Routing (RFC 1812) At least 1500 IPv4 Unicast routes Number of IPv4 Unicast /32 routes less than 4096 Support for Bidirectional Forwarding Detection (BFD), BFD for static routes, for OSPFv3 with a license purchased separately</p> <p>Support for RIP v1/v2 routing protocols</p> |
| <p>Требования к функциональности 3-го уровня Поддержка Статической маршрутизации (RFC 1812) Не менее 1500 IPv4 Unicast маршрутов Количество IPv4 Unicast /32 маршрутов не менее 4096 Поддержка протокола Bidirectional Forwarding Detection (BFD), BFD для статических маршрутов, для OSPFv3 при наличии приобретаемой отдельно лицензии Поддержка протоколов маршрутизации RIP v1/v2 Поддержка протоколов маршрутизации RIPng при наличии приобретаемой отдельно лицензии</p> | |

| | |
|---|---|
| <p>Поддержка протоколов маршрутизации OSPF v1/v2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов VRRP, VRRPv3 при наличии приобретаемой отдельно лицензии</p> <p>Многоадресная передача (Multicast)</p> <p>Поддержка протоколов многоадресной передачи:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Listener Discovery v1/2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Source Discovery protocol (MSDP) при наличии приобретаемой отдельно лицензии</p> <p>Поддержка IGMP snooping v1/v2/v3</p> <p>Не менее 2000 поддерживаемых записей IGMP snooping</p> <p>Поддержка протоколов PIM-SM, PIM-SSM, PIM-DM при наличии приобретаемой отдельно лицензии</p> <p>Не менее 2048 поддерживаемых маршрутов multicast</p> <p>Не менее 2048 поддерживаемых групп multicast</p> <p>Качество обслуживание (QoS)</p> <p>Поддержка стандартов:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF)</p> <p>Поддержка механизмов управления очередями:</p> <p>Tail Drop scheduling и WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Поддержка классификации множественных полей на L2 – L4) уровнях для постановки в очередь и перезаписи</p> <p>Поддержка критериев классификации по входному интерфейсу, MAC-адресу, полю EtherType, полям 802.1p, тэгу VLAN, IP-адресу, полям DSCP/IP precedence и номерам портов TCP/UDP</p> <p>Стекирование</p> | <p>Support for RIPng routing protocols if a license is purchased separately</p> <p>Support for OSPF v1/v2 routing protocols if a license is purchased separately</p> <p>Support for VRRP, VRRPv3 protocols if a license is purchased separately</p> <p>Multicast</p> <p>Support for multicast protocols:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 with a license purchased separately</p> <p>Support for Multicast Listener Discovery v1/2 protocol if a license is purchased separately</p> <p>Multicast Source Discovery protocol (MSDP) support if a license is purchased separately</p> <p>Support IGMP snooping v1/v2/v3</p> <p>At least 2000 supported IGMP snooping records</p> <p>Support for PIM-SM, PIM-SSM, PIM-DM protocols if a license is purchased separately</p> <p>At least 2048 supported multicast routes</p> <p>At least 2048 supported multicast groups</p> <p>Quality of Service (QoS)</p> <p>Support for standards:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF) .</p> <p>Support for queue management mechanisms:</p> <p>Tail Drop scheduling and WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Support for multiple fields classification at L2 - L4) levels for queuing and rewriting</p> <p>Supports classification criteria by input interface, MAC address, EtherType field, 802.1p fields, VLAN tag, IP address, DSCP/IP precedence fields and TCP/UDP port numbers</p> <p>Stacking</p> |
|---|---|

| | |
|---|---|
| <p>Поддержка функции стекирования коммутаторов при которой несколько объединённых в стек коммутаторов представляют собой единое логическое устройство</p> <p>Коммутатор должен поддерживать распределенный стек</p> <p>Поддержка стекирования через встроенные порты 100010GBASE-X SFP/SFP+ коммутатора</p> <p>Возможность объединения не менее 8 физических портов в один логический для увеличения пропускной способности шины стека</p> <p>Возможность объединения не менее 4 коммутаторов в стек</p> <p>Максимальная агрегированная пропускная способность шины стека не менее 80 Гбит/с</p> <p>Поддержка Graceful Restart для коммутаторов, соединенных в стеке</p> <p>Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость передачи данных не выполняет реинициализацию, что минимизирует влияние на передаваемые данные. Поддержка указанного механизма для протоколов ARP и базы данных коммутации</p> | <p>Support for switch stacking where multiple stacked switches represent a single logical device</p> <p>The switch must support the distributed stack</p> <p>Supports stacking via built-in ports 100010GBASE-X SFP/SFP+ switch</p> <p>Ability to combine at least 8 physical ports into one logical port to increase the stack bus bandwidth</p> <p>Ability to stack at least 4 switches</p> <p>Maximum aggregate stack bandwidth of at least 80 Gbps</p> <p>Graceful Restart support for switches connected in the stack</p> <p>Support for a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the control information with the main master switch and, in the event of a failure of the main stack master switch, the data plane does not reinitialize, minimizing the impact on the data being transmitted. Supports this mechanism for ARP and switching database protocols</p> |
| <p>Информационная безопасность</p> <p>Защита подсистемы управления от атак типа «Отказ в обслуживании» (DoS) и распределенный отказ в обслуживании DDOS</p> <p>Количество поддерживаемых списков контроля доступа (ACL) не менее 256 для каждого типа в каждом направлении</p> <p>Количество записей списков контроля доступа (ACL), на систему не менее 2000</p> <p>Поддержка:</p> <p>Port-based ACL (PACL) для входящего и исходящего трафика ;</p> <p>VLAN-based ACL (VACL) для входящего и исходящего трафика;</p> <p>Router-based ACL (RAACL) для входящего и исходящего трафика</p> <p>Поддержка ограничения количества MAC-адресов на порту</p> <p>Возможность ручной настройки разрешенных MAC-адресов на порту</p> <p>Поддержка механизма Dynamic ARP inspection (DAI)</p> <p>Поддержка механизма DHCP snooping</p> <p>Поддержка протокола 802.1X</p> <p>Поддержка аутентификации через Captive portal на Layer 2 интерфейсе</p> | <p>Information Security</p> <p>Control subsystem protection against Denial of Service (DoS) and distributed denial of service (DDOS) attacks</p> <p>Number of supported access control lists (ACLs) of at least 256 for each type in each direction</p> <p>Number of access control list (ACL) records per system, at least 2000</p> <p>Support:</p> <p>a. Port-based ACL (PACL) for inbound and outbound traffic ;</p> <p>VLAN-based ACL (VACL) for incoming and outgoing traffic;</p> <p>Router-based ACL (RAACL) for inbound and outbound traffic</p> <p>Support for limiting the number of MAC addresses on the port</p> <p>Possibility to manually set the allowed MAC addresses on the port</p> <p>Support for Dynamic ARP inspection (DAI) mechanism</p> <p>DHCP snooping mechanism support</p> <p>802.1X protocol support</p> <p>Support for authentication via Captive portal on Layer 2 interface</p> |

| | |
|---|---|
| <p>Поддержка назначения динамических списков контроля доступа при аутентификации по протоколу 802.1X на основе атрибутов RADIUS</p> <p>Поддержка типов 802.1X EAP: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> | <p>Support for assigning dynamic access control lists when authenticating via 802.1X protocol based on RADIUS attributes</p> <p>Support for 802.1X EAP types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> |
| <p>Управление</p> <p>Поддержка sFlow RFC 3176</p> <p>Поддержка HTTP/HTTPs управления</p> <p>Поддержка SSHv2/Secure Copy</p> <p>Поддержка протокола SNMP v1/v2c/v3</p> <p>Поддержка RMON (RFC 2819), Группы 1,2,3,9</p> <p>Поддержка протоколов RADIUS и TACACS+</p> <p>Поддержка конфигурационного файла ASCII</p> <p>Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию, поддержка возврата устройства на предыдущую версию ПО</p> <p>Не менее 49 сохраняемых автоматически предыдущих конфигураций, на которые можно осуществить возврат в любое время</p> <p>Неограниченное количество сохраняемых по требованию конфигураций, на которые можно осуществить возврат в любое время</p> <p>Поддержка возврата устройства на предыдущую версию ПО</p> <p>Возможность выполнения настройки устройства через web-интерфейс</p> <p>Поддержка протоколов NTP, DNS resolver, Syslog</p> <p>Поддержка функциональности DHCP сервера, DHCP proxy, DHCP Relay, DHCP helper, поддержка опции 82.</p> | <p>Management</p> <p>Support for sFlow RFC 3176</p> <p>Support HTTP/HTTPs management</p> <p>Support SSHv2/Secure Copy</p> <p>SNMP v1/v2c/v3 protocol support</p> <p>Support RMON (RFC 2819), Groups 1,2,3,9</p> <p>Support for RADIUS and TACACS+ protocols</p> <p>Support for ASCII configuration file</p> <p>Supports storage on the device back-up configuration, as well as return of the device to the previous configuration, support for return of the device to the previous version of software</p> <p>At least 49 automatically saved previous configurations to which you can return at any time</p> <p>Unlimited number of on-demand saved configurations that can be returned at any time</p> <p>Support for returning the device to a previous version of software</p> <p>Ability to configure the device via web-interface</p> <p>Support for NTP protocols, DNS resolver, Syslog</p> <p>Support for DHCP server functionality, DHCP proxy, DHCP Relay, DHCP helper, 82 option support.</p> |

| | |
|--|---|
| <p>Коммутатор доступа - количество 16 штук (тип – SWACS24)</p> <p>Требования к коммутатору:</p> <p>Тип устройства - Ethernet коммутатор. Наличие порта USB для загрузки конфигурации и проведения операций с программным обеспечением. Производительность коммутатора должна составлять не менее 95 млн. пакетов в секунду Производительность коммутатора должна составлять не менее 128 Гбит/с Коммутатор должен работать под управлением модульной операционной системы, позволяющей производить запуск, остановку, перезагрузку отдельных программных процессов без влияния на другие работающие процессы Операционная система коммутатора должно поддерживать возможность проверки непротиворечивости конфигурации перед применением конфигурации, применения проверенной конфигурации в заранее установленное время, возврата на предыдущую работоспособную конфигурацию в случае ошибки администратора. Дизайн коммутатора должен соответствовать для установки в монтажный конструктив 19” соответствующий стандарту ANSI/EIA-310.</p> <p>Требование к физическим интерфейсам Не менее 4 SFP-интерфейсов стандарта 1000/10GBASE-X, которые можно установить в коммутатор Не менее 24 не блокируемых, работающих на полной скорости среды, портов стандарта 10/100/1000BASE-T RJ-45 Поддержка стандартов 802.3af и 802.3at на всех портах 10/100/1000BASE-T RJ-45 Обеспечение питания согласно стандартов 802.3af и 802.3at на всех портах 10/100/1000BASE-T RJ-45 Максимальный бюджет PoE+ не менее 365 Вт Наличие выделенного интерфейса управления через Ethernet Наличие консольного порта RJ-45 для управления по протоколу RS-232</p> | <p>Access switch - quantity 16 pcs (type - SWACS24)</p> <p>Requirements for the switch:</p> <p>Device type - Ethernet switch. Availability of a USB port for downloading configuration and performing operations with the software. The performance of the switch should be at least 95 million packets per second. The performance of the switch shall be at least 128 Gbps. The switch should operate under the control of a modular operating system that allows to start, stop, reboot individual program processes without affecting other running processes</p> <p>The switch operating system must support the ability to verify configuration consistency before applying the configuration, apply the validated configuration at a predetermined time, return to the previous valid configuration in case of an administrator error.</p> <p>The switch design must comply with the ANSI/EIA-310 standard for installation in a 19" mounting structure.</p> <p>Requirement for physical interfaces At least 4 SFP-interfaces of the 1000/10GBASE-X standard, which can be installed in the switch At least 24 10/100/1000BASE-T RJ-45 standard ports that are not lockable and operate at full speed of the environment. Support for 802.3af and 802.3at standards on all 10/100/1000BASE-T RJ-45 ports Power supply according to 802.3af and 802.3at standards on all 10/100/1000BASE-T RJ-45 ports Maximum PoE+ budget at least 365 watts Dedicated control interface via Ethernet Presence of RJ-45 console port for RS-232 protocol control.</p> |
|--|---|

Наличие консольного порта miniUSB для управления по протоколу RS-232
Наличие порта USB для подключения внешних накопителей

Физические параметры

Наличие возможности питания от переменного тока с параметрами 50Гц/220В
Наличие встроенного температурного датчика
Шум, издаваемый устройством не более 40,6 dBA
Энергопотребление системы без учета PoE+ не более 80 Вт
Комплект поставки должен включать кабель питания, консольный кабель, набор для монтажа в стойку

Требования к программному обеспечению

Не менее 4 сессий для анализа (mirroring)
Поддержка анализа трафика (mirroring) на порту, VLAN, избирательный захват трафика на основе списков доступа
Поддержка анализа трафика (mirroring) нескольких портов назначения в один порт анализатора
Поддержка анализа трафика с удаленного устройства
Поддержка при наличии приобретаемой отдельно лицензии функции настройки программных пробников в виде пакетов протоколов ICMP, UDP/TCP, HTTP для определения доступности узлов сети и параметров каналов связи
Поддержка языка написания скриптов (сценариев) непосредственно на коммутаторе. Язык написания скриптов должен поддерживать общепринятые команды языка Stylesheet Language Alternative Syntax (SLAX) и/или Extensible Stylesheet Language Transformations (XSLT) и/или TCL и/или Python

Требования к функциональности физического уровня

При наличии отдельной лицензии поддержка механизма обеспечения резервирования каналов между коммутаторами. При этом в качестве каналов могут выступать как отдельные физические линии связи, так и логические каналы, состоящие из нескольких физических линий связи
Наличие функции рефлектометра (Time-domain reflectometry, TDR) для определения обрывов и замыканий кабеля
Наличие функции Auto MDI/MDIX
Поддержка диагностики оптических линий Digital Optical Monitoring
Поддержка Energy Efficient Ethernet (EEE)

Требования к функциональности 2-го уровня

Presence of miniUSB console port for RS-232 protocol control.
Availability of USB port for connecting external drives

Physical parameters

Availability of power supply from AC with parameters 50Hz/220V
Presence of an integrated temperature sensor
Noise emitted by the device not exceeding 40.6 dBA
System power consumption excluding RoE+ not exceeding 80W
Supply includes power cable, console cable, rack mounting kit.

Software Requirements

At least 4 sessions for analysis (mirroring)
Support for mirroring on port, VLAN, selective capturing of traffic based on access lists
Supports mirroring multiple destination ports into a single analyzer port
Support for traffic analysis from remote device
Support for customizing software probes in the form of ICMP, UDP/TCP, HTTP packets to determine the availability of network nodes and link parameters, if a license is purchased separately

Scripting language support directly on the switch. The scripting language must support common Stylesheet Language Alternative Syntax (SLAX) and/or Extensible Stylesheet Language Transformations (XSLT) and/or TCL and/or Python commands.

Requirements for physical layer functionality

If you have a separate license, support for the mechanism of providing channel redundancy between switches. Thus as channels can act both separate physical communication lines, and the logic channels consisting of several physical communication lines
Availability of the Time-domain reflectometry (TDR) function for the detection of cable breaks and short circuits.
Presence of Auto MDI/MDIX function
Support for Digital Optical Monitoring line diagnostics

| | |
|--|--|
| <p>Поддержка фреймов большой длины (9216 Байт) Не менее 4093 поддерживаемых VLANов Не менее 1-4094 поддерживаемых идентификаторов VLAN Не менее 16000 MAC адресов Не менее 1500 ARP записей Поддержка стандарта IEEE802.3ad – Link Aggregation Control Protocol (LACP) Поддержка технологии агрегации Ethernet каналов с балансировкой по MAC-адресу источника/назначения, IP-адресу источника/назначения, TCP/UDP-портам источника/назначения Не менее 8 портов в агрегационной группе Не менее 128 агрегационных групп Поддержка стандартов IEEE802.1D – Spanning Tree Protocol (STP); IEEE802.1w – Rapid Spanning Tree Protocol (RSTP); IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP); Не менее 64 поддерживаемых экземпляров протокола IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP) Поддержка стандартов IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED; IEEE 802.1p: Class-of-service (CoS) prioritization; IEEE 802.1Q-2006: VLAN tagging; IEEE 802.3: 10BASE-T; IEEE 802.3u: 100BASE-T; IEEE 802.3ab: 1000BASE-T; IEEE 802.3z: 1000BASE-X; IEEE 802.3x: Pause Frames/Flow Control Поддержка IEEE 802.1ad Q-in-Q VLAN Stacking Поддержка Q-in-Q с несколькими S-VLAN на порту с селективным назначением VLAN с использованием списков доступа Поддержка Layer 2 protocol tunneling (L2PT) Поддержка Multiple VLAN Registration Protocol, IEEE 802.1ak</p> <p>Требования к функциональности 3-го уровня Поддержка Статической маршрутизации (RFC 1812) Не менее 1500 IPv4 Unicast маршрутов Не менее 4096 IPv4 Unicast /32 маршрутов</p> | <p>Supports Energy Efficient Ethernet (EEE) Requirements for Level 2 functionality Support long frame lengths (9216 bytes) At least 4093 supported VLANs At least 1-4094 supported VLAN IDs At least 16,000 MAC addresses At least 1500 ARP records IEEE802.3ad - Link Aggregation Control Protocol (LACP) support</p> <p>Supports Ethernet link aggregation technology with balancing by source/destination MAC address, source/destination IP address, TCP/UDP source/destination ports At least 8 ports in the aggregation group At least 128 aggregation groups Support for standards IEEE802.1D - Spanning Tree Protocol (STP); IEEE802.1w - Rapid Spanning Tree Protocol (RSTP); IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP); At least 64 supported IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP) instances Support for standards IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED; IEEE 802.1p: Class-of-service (CoS) prioritization; IEEE 802.1Q-2006: VLAN tagging; IEEE 802.3: 10BASE-T; IEEE 802.3u: 100BASE-T; IEEE 802.3ab: 1000BASE-T; IEEE 802.3z: 1000BASE-X; IEEE 802.3x: Pause Frames/Flow Control Support IEEE 802.1ad Q-in-Q VLAN Stacking Q-in-Q support with some S-VLANs on the port with selective VLAN assignment using access lists Support for Layer 2 protocol tunneling (L2PT) Support Multiple VLAN Registration Protocol, IEEE 802.1ak</p> <p>Requirements for Level 3 functionality Supports Static Routing (RFC 1812) At least 1500 IPv4 Unicast routes</p> |
|--|--|

| | |
|---|---|
| <p>Поддержка протокола Bidirectional Forwarding Detection (BFD), BFD для статических маршрутов, для OSPFv3 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов маршрутизации RIP v1/v2</p> <p>Поддержка протоколов маршрутизации RIPng при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов маршрутизации OSPF v1/v2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов VRRP, VRRPv3 при наличии приобретаемой отдельно лицензии</p> <p>Многоадресная передача (Multicast)</p> <p>Поддержка протоколов многоадресной передачи:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Listener Discovery v1/2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Source Discovery protocol (MSDP) при наличии приобретаемой отдельно лицензии</p> <p>Поддержка IGMP snooping v1/v2/v3</p> <p>Не менее 2000 записей IGMP snooping</p> <p>Поддержка протоколов PIM-SM, PIM-SSM, PIM-DM при наличии приобретаемой отдельно лицензии</p> <p>Не менее 2048 поддерживаемых маршрутов multicast</p> <p>Не менее 2048 поддерживаемых групп multicast</p> <p>Качество обслуживание (QoS)</p> <p>Поддержка стандартов:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF)</p> <p>Поддержка механизмов управления очередями:</p> <p>Tail Drop scheduling и WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Поддержка классификации множественных полей на L2 – L4) уровнях для постановки в очередь и перезаписи</p> | <p>At least 4096 IPv4 Unicast /32 routes</p> <p>Support for Bidirectional Forwarding Detection (BFD), BFD for static routes, for OSPFv3 with a license purchased separately</p> <p>Support for RIP v1/v2 routing protocols</p> <p>Support for RIPng routing protocols if a license is purchased separately</p> <p>Support for OSPF v1/v2 routing protocols if a license is purchased separately</p> <p>Support for VRRP, VRRPv3 protocols if a license is purchased separately</p> <p>Multicast</p> <p>Support for multicast protocols:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 with a license purchased separately</p> <p>Support for Multicast Listener Discovery v1/2 protocol if a license is purchased separately</p> <p>Multicast Source Discovery protocol (MSDP) support if a license is purchased separately</p> <p>Support IGMP snooping v1/v2/v3</p> <p>At least 2000 IGMP snooping records</p> <p>Support for PIM-SM, PIM-SSM, PIM-DM protocols if a license is purchased separately</p> <p>At least 2048 supported multicast routes</p> <p>At least 2048 supported multicast groups</p> <p>Quality of Service (QoS)</p> <p>Support for standards:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF) .</p> <p>Support for queue management mechanisms:</p> <p>Tail Drop scheduling and WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Support for multiple fields classification at L2 - L4) levels for queuing and rewriting</p> |
|---|---|

| | |
|---|--|
| <p>Поддержка критериев классификации по входному интерфейсу, MAC-адресу, полю EtherType, полям 802.1p, тэгу VLAN, IP-адресу, полям DSCP/IP precedence и номерам портов TCP/UDP</p> <p>Стекирование Поддержка функции стекирования коммутаторов при которой несколько объединённых в стек коммутаторов представляют собой единое логическое устройство Коммутатор должен поддерживать распределенный стек Поддержка стекирования через встроенные порты 100010GBASE-X SFP/SFP+ коммутатора Возможность объединения не менее 8 физических портов в один логический для увеличения пропускной способности шины стека Возможность объединения не менее 4 коммутаторов в стек Максимальная агрегированная пропускная способность шины стека не менее 80 Гбит/с Поддержка Graceful Restart для коммутаторов, соединенных в стеке Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость передачи данных не выполняет реинициализацию, что минимизирует влияние на передаваемые данные. Поддержка указанного механизма для протоколов ARP и базы данных коммутации</p> <p>Информационная безопасность Защита подсистемы управления от атак типа «Отказ в обслуживании» (DoS) и распределенный отказ в обслуживании DDOS Количество поддерживаемых списков контроля доступа (ACL) не менее 256 для каждого типа в каждом направлении Количество записей списков контроля доступа (ACL), на систему не менее 2000 Поддержка: Port-based ACL (PACL) для входящего и исходящего трафика ; VLAN-based ACL (VACL) для входящего и исходящего трафика; Router-based ACL (RACL) для входящего и исходящего трафика Поддержка ограничения количества MAC-адресов на порту Возможность ручной настройки разрешенных MAC-адресов на порту</p> | <p>Supports classification criteria by input interface, MAC address, EtherType field, 802.1p fields, VLAN tag, IP address, DSCP/IP precedence fields and TCP/UDP port numbers</p> <p>Stacking Support for switch stacking where multiple stacked switches represent a single logical device</p> <p>The switch must support the distributed stack Supports stacking via built-in ports 100010GBASE-X SFP/SFP+ switch Ability to combine at least 8 physical ports into one logical port to increase the stack bus bandwidth Ability to stack at least 4 switches Maximum aggregate stack bandwidth of at least 80 Gbps Graceful Restart support for switches connected in the stack Support for a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the control information with the main master switch and, in the event of a failure of the main stack master switch, the data plane does not reinitialize, minimizing the impact on the data being transmitted. Supports this mechanism for ARP and switching database protocols</p> <p>Information Security Control subsystem protection against Denial of Service (DoS) and distributed denial of service (DDOS) attacks Number of supported access control lists (ACLs) of at least 256 for each type in each direction Number of access control list (ACL) records per system, at least 2000</p> <p>Support: Port-based ACL (PACL) for inbound and outbound traffic ; VLAN-based ACL (VACL) for incoming and outgoing traffic; Router-based ACL (RACL) for inbound and outbound traffic Support for limiting the number of MAC addresses on the port</p> |
|---|--|

| | |
|--|---|
| <p>Поддержка механизма Dynamic ARP inspection (DAI) Поддержка механизма DHCP snooping Поддержка протокола 802.1X Поддержка аутентификации через Captive portal на Layer 2 интерфейсе Поддержка назначения динамических списков контроля доступа при аутентификации по протоколу 802.1X на основе атрибутов RADIUS Поддержка типов 802.1X EAP: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> <p>Управление Поддержка sFlow RFC 3176 Поддержка HTTP/HTTPs управления Поддержка SSHv2/Secure Copy Поддержка протокола SNMP v1/v2c/v3 Поддержка RMON (RFC 2819), Группы 1,2,3,9 Поддержка протоколов RADIUS и TACACS+ Поддержка конфигурационного файла ASCII Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию, поддержка возврата устройства на предыдущую версию ПО Не менее 49 сохраняемых автоматически предыдущих конфигураций, на которые можно осуществить возврат в любое время Неограниченное количество сохраняемых по требованию конфигураций, на которые можно осуществить возврат в любое время Поддержка возврата устройства на предыдущую версию ПО Возможность выполнения настройки устройства через web-интерфейс Поддержка протоколов NTP, DNS resolver, Syslog Поддержка функциональности DHCP сервера, DHCP проху, DHCP Relay, DHCP helper, поддержка опции 82.</p> | <p>Possibility to manually set the allowed MAC addresses on the port Support for Dynamic ARP inspection (DAI) mechanism DHCP snooping mechanism support 802.1X protocol support Support for authentication via Captive portal on Layer 2 interface Support for assigning dynamic access control lists when authenticating via 802.1X protocol based on RADIUS attributes Support for 802.1X EAP types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> <p>Management Support for sFlow RFC 3176 Support HTTP/HTTPs management Support SSHv2/Secure Copy SNMP v1/v2c/v3 protocol support Support RMON (RFC 2819), Groups 1,2,3,9 Support for RADIUS and TACACS+ protocols Support for ASCII configuration file Supports storage on the device back-up configuration, as well as return of the device to the previous configuration, support for return of the device to the previous version of software At least 49 automatically saved previous configurations to which you can return at any time Unlimited number of on-demand saved configurations that can be returned at any time Support for returning the device to a previous version of software Ability to configure the device via web-interface Support for NTP protocols, DNS resolver, Syslog Support for DHCP server functionality, DHCP proxy, DHCP Relay, DHCP helper, 82 option support.</p> |
|--|---|

| | |
|---|--|
| <p>Коммутатор доступа - количество 6 штук (тип – SWACS48)</p> <p>Требования к коммутатору:</p> <p>Тип устройства - Ethernet коммутатор. Наличие порта USB для загрузки конфигурации и проведения операций с программным обеспечением. Производительность коммутатора должна составлять не менее 130 млн. пакетов в секунду Производительность коммутатора должна составлять не менее 170 Гбит/с Коммутатор должен работать под управлением модульной операционной системы, позволяющей производить запуск, остановку, перезагрузку отдельных программных процессов без влияния на другие работающие процессы Операционная система коммутатора должно поддерживать возможность проверки непротиворечивости конфигурации перед применением конфигурации, применения проверенной конфигурации в заранее установленное время, возврата на предыдущую работоспособную конфигурацию в случае ошибки администратора. Дизайн коммутатора должен соответствовать для установки в монтажный конструктив 19” соответствующий стандарту ANSI/EIA-310.</p> <p>Требование к физическим интерфейсам Не менее 4 SFP-интерфейсов стандарта 1000/10GBASE-X, которые можно установить в коммутатор Не менее 48 не блокируемых, работающих на полной скорости среды, портов стандарта 10/100/1000BASE-T RJ-45 Поддержка стандартов 802.3af и 802.3at на всех портах 10/100/1000BASE-T RJ-45 Обеспечение питания согласно стандартам 802.3af и 802.3at на всех портах 10/100/1000BASE-T RJ-45 Максимальный бюджет PoE+ не менее 730 Вт Наличие выделенного интерфейса управления через Ethernet Наличие консольного порта RJ-45 для управления по протоколу RS-232 Наличие консольного порта miniUSB для управления по протоколу RS-232</p> | <p>Access switch - quantity 6 pcs (type - SWACS48)</p> <p>Requirements for the switch:</p> <p>Device type - Ethernet switch. Availability of a USB port for downloading configuration and performing operations with the software. The performance of the switch should be at least 130 million packets per second. The performance of the switch should be at least 170 Gbps. The switch should operate under the control of a modular operating system that allows to start, stop, reboot individual program processes without affecting other running processes</p> <p>The switch operating system must support the ability to verify configuration consistency before applying the configuration, apply the validated configuration at a predetermined time, return to the previous valid configuration in case of an administrator error.</p> <p>The switch design must comply with the ANSI/EIA-310 standard for installation in a 19" mounting structure.</p> <p>Requirement for physical interfaces At least 4 SFP-interfaces of the 1000/10GBASE-X standard, which can be installed in the switch At least 48 non-lockable 10/100/1000BASE-T RJ-45 standard ports operating at full speed of the environment. Support for 802.3af and 802.3at standards on all 10/100/1000BASE-T RJ-45 ports Power supply according to 802.3af and 802.3at standards on all 10/100/1000BASE-T RJ-45 ports Maximum PoE+ budget not less than 730W Dedicated control interface via Ethernet</p> <p>Presence of RJ-45 console port for RS-232 protocol control.</p> |
|---|--|

Наличие порта USB для подключения внешних накопителей

Физические параметры

Наличие возможности питания от переменного тока с параметрами 50Гц/220В

Наличие встроенного температурного датчика

Шум, издаваемый устройством не более 51 dBA

Энергопотребление системы без учета PoE+ не более 100 Вт

Комплект поставки должен включать кабель питания, консольный кабель, набор для монтажа в стойку

Требования к программному обеспечению

Не менее 4 сессий для анализа (mirroring)

Поддержка анализа трафика (mirroring) на порту, VLAN, избирательный захват трафика на основе списков доступа

Поддержка анализа трафика (mirroring) нескольких портов назначения в один порт анализатора

Поддержка анализа трафика с удаленного устройства

Поддержка при наличии приобретаемой отдельно лицензии функции настройки программных пробников в виде пакетов протоколов ICMP, UDP/TCP, HTTP для определения доступности узлов сети и параметров каналов связи

Поддержка языка написания скриптов (сценариев) непосредственно на коммутаторе. Язык написания скриптов должен поддерживать общепринятые команды языка Stylesheet Language Alternative Syntax (SLAX) и/или Extensible Stylesheet Language Transformations (XSLT) и/или TCL и/или Python

Требования к функциональности физического уровня

При наличии отдельной лицензии поддержка механизма обеспечения резервирования каналов между коммутаторами. При этом в качестве каналов могут выступать как отдельные физические линии связи, так и логические каналы, состоящие из нескольких физических линий связи

Наличие функции рефлектометра (Time-domain reflectometry, TDR) для определения обрывов и замыканий кабеля

Наличие функции Auto MDI/MDIX

Поддержка диагностики оптических линий Digital Optical Monitoring

Поддержка Energy Efficient Ethernet (EEE)

Требования к функциональности 2-го уровня

Presence of miniUSB console port for RS-232 protocol control.

Availability of USB port for connecting external drives

Physical parameters

Availability of power supply from AC with parameters 50Hz/220V

Presence of an integrated temperature sensor

Noise emitted by the device not exceeding 51 dBA

System power consumption excluding RoE+ not more than 100W

Supply includes power cable, console cable, rack mounting kit.

Software Requirements

At least 4 sessions for analysis (mirroring)

Support for mirroring on port, VLAN, selective capturing of traffic based on access lists

Supports mirroring multiple destination ports into a single analyzer port

Support for traffic analysis from remote device

Support for customizing software probes in the form of ICMP, UDP/TCP, HTTP packets to determine the availability of network nodes and link parameters, if purchased separately

Scripting language support directly on the switch. The scripting language must support common Stylesheet Language Alternative Syntax (SLAX) and/or Extensible Stylesheet Language Transformations (XSLT) and/or TCL and/or Python commands.

Requirements for physical layer functionality

If you have a separate license, support for the mechanism of providing channel redundancy between switches. Thus as channels can act both separate physical communication lines, and the logic channels consisting of several physical communication lines

Availability of the Time-domain reflectometry (TDR) function for the detection of cable breaks and short circuits.

Presence of Auto MDI/MDIX function

Support for Digital Optical Monitoring line diagnostics

Supports Energy Efficient Ethernet (EEE)

Поддержка фреймов большой длины (9216 Байт)
 Не менее 4093 поддерживаемых VLANов
 Не менее 1-4094 поддерживаемых идентификаторов VLAN
 Не менее 16000 MAC адресов
 Не менее 1500 ARP записей
 Поддержка стандарта IEEE802.3ad – Link Aggregation Control Protocol (LACP)
 Поддержка технологии агрегации Ethernet каналов с балансировкой по MAC-адресу источника/назначения, IP-адресу источника/назначения, TCP/UDP-портам источника/назначения
 Не менее 8 портов в агрегационной группе
 Не менее 128 агрегационных групп
 Поддержка стандартов
 IEEE802.1D – Spanning Tree Protocol (STP);
 IEEE802.1w – Rapid Spanning Tree Protocol (RSTP);
 IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);
 Не менее 64 поддерживаемых экземпляров протокола IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP)
 Поддержка стандартов
 IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED;
 IEEE 802.1p: Class-of-service (CoS) prioritization;
 IEEE 802.1Q-2006: VLAN tagging;
 IEEE 802.3: 10BASE-T;
 IEEE 802.3u: 100BASE-T;
 IEEE 802.3ab: 1000BASE-T;
 IEEE 802.3z: 1000BASE-X;
 IEEE 802.3x: Pause Frames/Flow Control
 Поддержка IEEE 802.1ad Q-in-Q VLAN Stacking
 Поддержка Q-in-Q с несколькими S-VLAN на порту с селективным назначением VLAN с использованием списков доступа
 Поддержка Layer 2 protocol tunneling (L2PT)
 Поддержка Multiple VLAN Registration Protocol, IEEE 802.1ak

Требования к функциональности 3-го уровня

Поддержка Статической маршрутизации (RFC 1812)
 Не менее 1500 IPv4 Unicast маршрутов
 Не менее 4096 IPv4 Unicast /32 маршрутов

Requirements for Level 2 functionality

Support long frame lengths (9216 bytes)
 At least 4093 supported VLANs
 At least 1-4094 supported VLAN IDs
 At least 16,000 MAC addresses
 At least 1500 ARP records
 IEEE802.3ad - Link Aggregation Control Protocol (LACP) support
 Supports Ethernet link aggregation technology with balancing by source/destination MAC address, source/destination IP address, TCP/UDP source/destination ports
 At least 8 ports in the aggregation group
 At least 128 aggregation groups
 Support for standards
 IEEE802.1D - Spanning Tree Protocol (STP);
 IEEE802.1w - Rapid Spanning Tree Protocol (RSTP);
 IEEE802.1s – Multiple Instance Spanning Tree Protocol (MSTP);
 At least 64 supported IEEE802.1s Multiple Instance Spanning Tree Protocol (MSTP) instances

Support for standards
 IEEE 802.1AB: Link Layer Discovery Protocol (LLDP), LLDP-MED;
 IEEE 802.1p: Class-of-service (CoS) prioritization;
 IEEE 802.1Q-2006: VLAN tagging;
 IEEE 802.3: 10BASE-T;
 IEEE 802.3u: 100BASE-T;
 IEEE 802.3ab: 1000BASE-T;
 IEEE 802.3z: 1000BASE-X;
 IEEE 802.3x: Pause Frames/Flow Control
 Support IEEE 802.1ad Q-in-Q VLAN Stacking
 Q-in-Q support with some S-VLANs on the port with selective VLAN assignment using access lists
 Support for Layer 2 protocol tunneling (L2PT)
 Support Multiple VLAN Registration Protocol, IEEE 802.1ak

Requirements for Level 3 functionality

Supports Static Routing (RFC 1812)

| | |
|---|--|
| <p>Поддержка протокола Bidirectional Forwarding Detection (BFD), BFD для статических маршрутов, для OSPFv3 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов маршрутизации RIP v1/v2</p> <p>Поддержка протоколов маршрутизации RIPng при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов маршрутизации OSPF v1/v2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протоколов VRRP, VRRPv3 при наличии приобретаемой отдельно лицензии</p> <p>Многоадресная передача (Multicast)</p> <p>Поддержка протоколов многоадресной передачи:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Listener Discovery v1/2 при наличии приобретаемой отдельно лицензии</p> <p>Поддержка протокола Multicast Source Discovery protocol (MSDP) при наличии приобретаемой отдельно лицензии</p> <p>Поддержка IGMP snooping v1/v2/v3</p> <p>Не менее 2000 записей IGMP snooping</p> <p>Поддержка протоколов PIM-SM, PIM-SSM, PIM-DM при наличии приобретаемой отдельно лицензии</p> <p>Не менее 2048 поддерживаемых маршрутов multicast</p> <p>Не менее 2048 поддерживаемых групп multicast</p> <p>Качество обслуживание (QoS)</p> <p>Поддержка стандартов:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF)</p> <p>Поддержка механизмов управления очередями:</p> <p>Tail Drop scheduling и WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Поддержка классификации множественных полей на L2 – L4) уровнях для постановки в очередь и перезаписи</p> | <p>At least 1500 IPv4 Unicast routes</p> <p>At least 4096 IPv4 Unicast /32 routes</p> <p>Support for Bidirectional Forwarding Detection (BFD), BFD for static routes, for OSPFv3 with a license purchased separately</p> <p>Support for RIP v1/v2 routing protocols</p> <p>Support for RIPng routing protocols if a license is purchased separately</p> <p>Support for OSPF v1/v2 routing protocols if a license is purchased separately</p> <p>Support for VRRP, VRRPv3 protocols if a license is purchased separately</p> <p>Multicast</p> <p>Support for multicast protocols:</p> <p>Internet Group Management Protocol (IGMP) v1/v2/v3 with a license purchased separately</p> <p>Support for Multicast Listener Discovery v1/2 protocol if a license is purchased separately</p> <p>Multicast Source Discovery protocol (MSDP) support if a license is purchased separately</p> <p>Support IGMP snooping v1/v2/v3</p> <p>At least 2000 IGMP snooping records</p> <p>Support for PIM-SM, PIM-SSM, PIM-DM protocols if a license is purchased separately</p> <p>At least 2048 supported multicast routes</p> <p>At least 2048 supported multicast groups</p> <p>Quality of Service (QoS)</p> <p>Support for standards:</p> <p>RFC 2474: DiffServ Precedence, including 8 queues/port</p> <p>RFC 2598: DiffServ Expedited Forwarding (EF)</p> <p>RFC 2597: DiffServ Assured Forwarding (AF) .</p> <p>Support for queue management mechanisms:</p> <p>Tail Drop scheduling and WRED,</p> <p>Shaped Deficit Weighted Round Robin (SDWRR) queuing,</p> <p>Strict priority queuing,</p> <p>Support for multiple fields classification at L2 - L4) levels for queuing and rewriting</p> |
|---|--|

Поддержка критериев классификации по входному интерфейсу, MAC-адресу, полю EtherType, полям 802.1p, тэгу VLAN, IP-адресу, полям DSCP/IP precedence и номерам портов TCP/UDP

Стекирование

Поддержка функции стекирования коммутаторов при которой несколько объединённых в стек коммутаторов представляют собой единое логическое устройство

Коммутатор должен поддерживать распределенный стек

Поддержка стекирования через встроенные порты 100010GBASE-X SFP/SFP+ коммутатора

Возможность объединения не менее 8 физических портов в один логический для увеличения пропускной способности шины стека

Возможность объединения не менее 4 коммутаторов в стек

Максимальная агрегированная пропускная способность шины стека не менее 80 Гбит/с

Поддержка Graceful Restart для коммутаторов, соединенных в стеке

Поддержка механизма высокой доступности при котором, при работе коммутаторов в стеке, коммутатор, работающий как резервный ведущий коммутатор стека синхронизирует информацию управления с основным ведущим коммутатором и в случае отказа основного ведущего коммутатора стека плоскость передачи данных не выполняет реинициализацию, что минимизирует влияние на передаваемые данные. Поддержка указанного механизма для протоколов ARP и базы данных коммутации

Информационная безопасность

Защита подсистемы управления от атак типа «Отказ в обслуживании» (DoS) и распределенный отказ в обслуживании DDOS

Количество поддерживаемых списков контроля доступа (ACL) не менее 256 для каждого типа в каждом направлении

Количество записей списков контроля доступа (ACL), на систему не менее 2000

Поддержка:

Port-based ACL (PACL) для входящего и исходящего трафика ;

VLAN-based ACL (VACL) для входящего и исходящего трафика;

Router-based ACL (RACL) для входящего и исходящего трафика

Поддержка ограничения количества MAC-адресов на порту

Возможность ручной настройки разрешенных MAC-адресов на порту

Supports classification criteria by input interface, MAC address, EtherType field, 802.1p fields, VLAN tag, IP address, DSCP/IP precedence fields and TCP/UDP port numbers

Stacking

Support for switch stacking where multiple stacked switches represent a single logical device

The switch must support the distributed stack

Supports stacking via built-in ports 100010GBASE-X SFP/SFP+ switch

Ability to combine at least 8 physical ports into one logical port to increase the stack bus bandwidth

Ability to stack at least 4 switches

Maximum aggregate stack bandwidth of at least 80 Gbps

Graceful Restart support for switches connected in the stack

Support for a high availability mechanism where, when the switches in the stack are running, a switch operating as a redundant stack master switch synchronizes the control information with the main master switch and, in the event of a failure of the main stack master switch, the data plane does not reinitialize, minimizing the impact on the data being transmitted. Supports this mechanism for ARP and switching database protocols

Information Security

Control subsystem protection against Denial of Service (DoS) and distributed denial of service (DDOS) attacks

Number of supported access control lists (ACLs) of at least 256 for each type in each direction

Number of access control list (ACL) records per system, at least 2000

Support:

Port-based ACL (PACL) for inbound and outbound traffic ;

VLAN-based ACL (VACL) for incoming and outgoing traffic;

Router-based ACL (RACL) for inbound and outbound traffic

Support for limiting the number of MAC addresses on the port

Possibility to manually set the allowed MAC addresses on the port

| | |
|--|---|
| <p>Поддержка механизма Dynamic ARP inspection (DAI) Поддержка механизма DHCP snooping Поддержка протокола 802.1X Поддержка аутентификации через Captive portal на Layer 2 интерфейсе Поддержка назначения динамических списков контроля доступа при аутентификации по протоколу 802.1X на основе атрибутов RADIUS Поддержка типов 802.1X EAP: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> <p>Управление Поддержка sFlow RFC 3176 Поддержка HTTP/HTTPs управления Поддержка SSHv2/Secure Copy Поддержка протокола SNMP v1/v2c/v3 Поддержка RMON (RFC 2819), Группы 1,2,3,9 Поддержка протоколов RADIUS и TACACS+ Поддержка конфигурационного файла ASCII Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию, поддержка возврата устройства на предыдущую версию ПО Не менее 49 сохраняемых автоматически предыдущих конфигураций, на которые можно осуществить возврат в любое время Неограниченное количество сохраняемых по требованию конфигураций, на которые можно осуществить возврат в любое время Поддержка возврата устройства на предыдущую версию ПО Возможность выполнения настройки устройства через web-интерфейс Поддержка протоколов NTP, DNS resolver, Syslog Поддержка функциональности DHCP сервера, DHCP проху, DHCP Relay, DHCP helper, поддержка опции 82.</p> | <p>Support for Dynamic ARP inspection (DAI) mechanism DHCP snooping mechanism support 802.1X protocol support Support for authentication via Captive portal on Layer 2 interface Support for assigning dynamic access control lists when authenticating via 802.1X protocol based on RADIUS attributes Support for 802.1X EAP types: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Protected Extensible Authentication Protocol (PEAP)</p> <p>Management Support for sFlow RFC 3176 Support HTTP/HTTPs management Support SSHv2/Secure Copy SNMP v1/v2c/v3 protocol support Support RMON (RFC 2819), Groups 1,2,3,9 Support for RADIUS and TACACS+ protocols Support for ASCII configuration file Supports storage on the device back-up configuration, as well as return of the device to the previous configuration, support for return of the device to the previous version of software At least 49 automatically saved previous configurations to which you can return at any time Unlimited number of on-demand saved configurations that can be returned at any time Support for returning the device to a previous version of software Ability to configure the device via web-interface Support for NTP protocols, DNS resolver, Syslog Support for DHCP server functionality, DHCP proxy, DHCP Relay, DHCP helper, 82 option support.</p> |
|--|---|

| | |
|--|--|
| <p>Аксессуары - количество 1 комплект (тип – SWACSKIT)</p> <p>Количество аксессуаров Small Form Factor Pluggable 10 GE, SFP+, SR– не менее 132 штук. SFP 1000Base-SX GE, LC, 850nm for up to 550m, Transmission on MMF – не менее 60 штук Small Form Factor Pluggable 10 GE, SFP+, дистанция не менее 2 км – не менее 8 штук QSFP+ DAC cable, 1m – не менее 10 штук SFP 1000BASE-T GE module – не менее 6 штук</p> <p>Общие требования Поставщик в праве изменить количество поставляемых аксессуаров в соответствии с внедряемым решением, при условии обеспечения полной работоспособности схемы внедрения. При этом необходимо учесть ЗИП для аксессуаров в количестве 5% от каждого поставляемого аксессуара.</p> | <p>Accessories - quantity 1 set (type - SWACSKIT)</p> <p>Number of accessories Small Form Factor Pluggable 10 GE, SFP+, SR- at least 132 pieces. SFP 1000Base-SX GE, LC, 850nm for up to 550m, Transmission on MMF - at least 60 pieces Small Form Factor Pluggable 10 GE, SFP+, distance not less than 2 km - not less than 8 pieces QSFP+ DAC cable, 1m - at least 10 pieces SFP 1000BASE-T GE module - at least 6 pieces</p> <p>General requirements The supplier has the right to change the number of supplied accessories in accordance with the implemented solution, provided that the implementation scheme is fully operational. In this case it is necessary to take into account the NIP for accessories in the amount of 5% of each delivered accessory.</p> |
|--|--|

| | |
|--|--|
| <p>Система управления и мониторинга - количество 1 комплект (тип – SWMGMT)</p> <p>Требование к функционалу Форм-фактор виртуальная машина или аппаратный программный комплекс Возможность развертывания на гипервизорах VMWare ESXi и KVM (при условии виртуальной машины) автоматизированное обнаружение сетевых узлов в реальном масштабе времени отправка конфигурационных команд на сетевые узлы сбор и представление инвентаризационных данных управляемых устройств: серийные номера, версии ПО, количество портов, слотов и модулей поддержка управления через интерфейс WEB2.0 управление процессом инвентаризации для автоматизированного сбора данных инвентаризации с оборудования наглядное представление данных физической и логической инвентаризации оборудования с возможностью построения пользовательских отчетов наглядное представление статистических данных о работе сетевых узлов, данных о состоянии функционирующих сетевых узлов автоматизированная синхронизация конфигурации на оборудовании возможность автоматизированного исследования сетевой топологии включая сетевое оборудование и соединения централизованная установка ПО на все управляемые устройства топологии включая сетевое оборудование и соединения возможность интеграции с программным обеспечением сторонних производителей для мониторинга состояния сетевых устройств и анализа производительности обеспечение управления конфигурациями управляемых устройств: копирование конфигураций с устройств в депозитарий системы, отслеживание версий, возможность загрузки резервной конфигурации на устройство, возможность синхронизации конфигурации сетевого оборудования с централизованной базой данных конфигураций, которая ведется средствами системы</p> | <p>Control and monitoring system - quantity 1 set (type - SWMGMT)</p> <p>Requirement for functionality Form factor virtual machine or hardware software system</p> <p>Ability to deploy on VMWare ESXi and KVM hypervisors (subject to virtual machine) real-time automated discovery of network nodes configuration commands to network nodes collection and presentation of inventory data of managed devices: serial numbers, software versions, number of ports, slots and modules management support via WEB2.0 interface management of the inventory process for automated collection of inventory data from equipment Visual presentation of physical and logical equipment inventory data with the ability to build custom reports visual presentation of statistical data on network nodes operation, data on the state of functioning network nodes machine synchronization capability of automated network topology research including network equipment and connections centralized software installation on all managed topology devices including network equipment and connections Ability to integrate with third-party software for network device monitoring and performance analysis Providing management of managed device configurations: copying configurations from devices to the system repository, version tracking, possibility of downloading backup configuration to the device, possibility of synchronization of network equipment configuration with a centralized database of configurations maintained by the system facilities simultaneous configuration of several devices using templates device failure detection</p> |
|--|--|

| | |
|---|--|
| <p>возможность одновременного конфигурирования нескольких устройств при помощи шаблонов</p> <p>детектирование отказов устройств</p> <p>мониторинг параметров производительности и сбоев устройств (загрузка и состояние интерфейсов, сетевая доступность устройств)</p> <p>поддержка конфигурирования устройств средствами NetConf, Device Management Interface (DMI), на базе схем XML, загрузки конфигурационных файлов в текстовом формате, считывание данных Syslog</p> <p>управление должно осуществляться через программируемый интерфейс, использующий в качестве транспортного протокола протокол SSH (Secure Shell)</p> <p>сбор необходимой информации об устройстве с которым произошел сбой и содействие при обращении в сервисную поддержку производителя</p> <p>возможность отслеживания официальных уведомлений производителя о багах в программном обеспечении оборудования и анализ влияния этих багов на работу сети</p> <p>возможность отслеживания уведомлений о снятии оборудования с производства.</p> | <p>Monitor performance parameters and device failures (interface loading and status, network availability of devices)</p> <p>support for configuring devices using NetConf, Device Management Interface (DMI), based on XML schemes, loading configuration files in text format, reading Syslog data</p> <p>control must be exercised through a programmable interface that uses SSH (Secure Shell) as the transport protocol.</p> <p>Collection of necessary information about the device with which the failure occurred and assistance in contacting the manufacturer's service support</p> <p>ability to track official manufacturer's bug alerts in hardware software and analyze the impact of these bug alerts on network performance</p> <p>ability to track down disposable notices</p> |
|---|--|

| | |
|---|--|
| <p>Требования к файрволам следующего поколения, - количество 2 устройства в режиме кластера актив/актив (тип FWMCC)</p> <p>Общие требования</p> <p>Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.</p> <p>Решение должно поддерживать DHCP, сервер и relay.</p> <p>Решение должно поддерживать HTTP & HTTPS proxy.</p> <p>Решение должно поддерживать функционал reverse proxy.</p> <p>Решение должно включать в себя возможность работы в режиме Transparent/Bridge.</p> <p>Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).</p> <p>Решение должно поддерживать Firewall, IPS, URL-фильтрацию, DLP, Antitbot, Antivirus, Управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge.</p> <p>Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.</p> <p>Решение должно поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений. В режиме высокой доступности или режиме распределения нагрузки должно поддерживаться до 8 узлов кластера.</p> <p>Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.</p> <p>По умолчанию, должно поддерживаться 2 виртуальные системы, а с применением дополнительной лицензии должно поддерживаться до 20 виртуальных шлюзов на одном физическом шлюзе.</p> <p>Сетевые возможности: решение должно поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами).</p> <p>Эффективное обеспечение безопасности: каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall,</p> | <p>Requirements for next generation firewalls – quantity 2 devices in cluster mode active/active (FWMCC type)</p> <p>General requirements</p> <p>The Security Gateway should use link state monitoring based on detailed link and application analysis to monitor and control network flow.</p> <p>The solution must support DHCP, server and relay.</p> <p>The solution must support HTTP & HTTPS proxy.</p> <p>The solution must support reverse proxy functionality.</p> <p>The solution must include the ability to work in Transparent/Bridge mode.</p> <p>The solution must support layer 2 of the OSI model (bridge mode).</p> <p>The solution must support Firewall, IPS, URL filtering, DLP, Antitbot, Antivirus, Application Management, HTTPS inspection, Identity Awareness and Sandboxing in bridge mode.</p> <p>The solution must support Active/Standby clustering in bridge mode.</p> <p>The solution must support high gateway availability and load balancing with synchronized network connection states. In high availability mode or load balancing mode, up to 8 cluster nodes must be supported.</p> <p>The solution must support security gateway virtualization to consolidate multiple virtual gateways on a single physical device.</p> <p>By default, 2 virtual systems must be supported, and with an additional license, up to 20 virtual gateways must be supported on a single physical gateway.</p> <p>Networking capabilities: The solution must support virtual switches and virtual routers to configure network communications between virtual systems (virtual gateways).</p> <p>Effective security: Each virtual gateway must be able to run its own set of security services. For example, one Virtual Gateway works as Firewall, one Virtual Gateway works as Firewall and IPS, one Virtual</p> |
|---|--|

| | |
|---|---|
| <p>второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.</p> <p>Выделение ресурсов: решение должно обеспечивать управление вычислительными мощностями, гарантируя, что каждая виртуальная система получит то количество процессорной мощности и оперативной памяти, которая необходима для выполнения ее задач.</p> <p>Решение должно обеспечивать поддержку IPv6.</p> <p>Решение должно поддерживать политику, основанную на QoS.</p> <p>Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.</p> <p>Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.</p> <p>Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).</p> <p>Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.</p> <p>Решение должно обеспечивать функционал Идентификации пользователей.</p> <p>Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.</p> <p>Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.</p> <p>Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.</p> <p>Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.</p> <p>База данных управления приложениями должна содержать свыше 8000 известных приложений.</p> <p>Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.</p> <p>Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.</p> <p>Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.</p> <p>Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное аномальное сетевое поведение.</p> | <p>Gateway works as Firewall, IPS, Application Control, URL Filtering, and so on.</p> <p>Allocation of resources: The solution must provide computational power management, ensuring that each virtual system gets the amount of processor power and RAM needed to perform its tasks.</p> <p>The solution must support IPv6.</p> <p>The solution must support a policy based on QoS.</p> <p>The solution must be able to guarantee or limit bandwidth and manage latency for a specific IP source, destination IP or service.</p> <p>The solution must be able to randomly apply QoS rules to VPN traffic.</p> <p>The solution must provide IPS (intrusion prevention system) functionality.</p> <p>The IPS system should be based on the following detection mechanisms: use of signatures, tracking of protocol anomalies, application management and behavioral based detection.</p> <p>The solution must provide user identification functionality.</p> <p>Must be able to collect user IDs by requesting Microsoft Active Directory based on security events.</p> <p>Must have a browser-based method of authenticating user ID for non-domain users or computers.</p> <p>There must be a special agent that can be installed by policy on the users' computers, and that can collect and pass IDs to the security gateway.</p> <p>The solution must provide application management functionality and URL filtering.</p> <p>The Application Management Database must contain over 8000 known applications.</p> <p>The solution must provide detailed security control for at least 250000 Web 2.0 widgets.</p> <p>The solution must provide URL categorization, which includes more than 200 million URLs.</p> <p>The solution must provide Anti-Bot and Anti-Virus functionality.</p> <p>The Anti-bot application must be able to detect and stop suspicious abnormal network behavior.</p> <p>The Anti-Bot application must use a multi-layered discovery mechanism that includes IP, URL and DNS reputation and bot discovery via communication protocol templates.</p> |
|---|---|

| | |
|---|--|
| <p>Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.</p> <p>Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.</p> <p>Приложение Anti-virus должно быть способно проверять зашифрованный SSL трафик.</p> <p>Решение должно обеспечивать функционал инспекции SSL (входящего / исходящего трафика).</p> <p>Решение должно интегрироваться с «песочницей» - Sandboxing (инспекция – в облаке или на выделенном локальном устройстве) путем приобретения дополнительной лицензии.</p> <p>Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО – обеспечивая защиту в период до появления статических сигнатур, защищающих от таких угроз.</p> <p>Топология внедрения:</p> <p>Поддержка режима сетевой «песочницы» (network based).</p> <p>Поддержка режима инлайн (bridge mode).</p> <p>Поддержка режима почтового агента (Mail Transfer Mode, MTA).</p> <p>Поддержка режима зеркального порта (TAP/SPAN порт).</p> <p>Решение не должно содержать отдельную инфраструктуру для защиты почты и веба.</p> <p>Решение должно поддерживать кластеризацию для обеспечения отказоустойчивости.</p> <p>Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.</p> <p>Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе и специально настроенные образы.</p> <p>Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.</p> <p>Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Мбайт.</p> <p>Решение должно детектировать атаки на стадии выполнения эксплойта (exploitation) – т.е. до того как запускается шелл-код и осуществляется загрузка/исполнение самого кода зловредного ПО.</p> <p>Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege</p> | <p>The Anti-virus application should prevent access to malicious websites and stop incoming malicious files.</p> <p>The Anti-virus application must be able to verify SSL encrypted traffic.</p> <p>The solution should provide SSL (inbound/outbound traffic) inspection functionality.</p> <p>The solution must integrate with Sandboxing (inspection - in the cloud or on a dedicated local device) by purchasing an additional license.</p> <p>The sandbox feature should provide protection against zero-day attacks, as well as unknown malware - providing protection until static signatures appear to protect against such threats.</p> <p>Implementation topology:</p> <p>Supports network based sandbox mode.</p> <p>Support for in-line (bridge mode).</p> <p>Support for Mail Transfer Mode (MTA).</p> <p>Supports mirror port mode (TAP/SPAN port).</p> <p>The solution must not contain a separate infrastructure to protect the mail and the web.</p> <p>The solution must support clustering to ensure fault tolerance.</p> <p>The solution must emulate executable files, archives, documents including Java and flash.</p> <p>The emulation engine must support a variety of operating systems, such as XP and Windows 7, including specially configured images.</p> <p>The emulation engine should inspect, emulate, prevent and transmit events to the anti-malware infrastructure.</p> <p>The solution should provide emulation of files both small and larger than 10Mbytes.</p> <p>The solution must detect attacks at the executable execution stage (i.e. before the shell code is launched and the malware code itself is loaded/executed).</p> <p>The solution must detect ROP (return oriented programming) and other exploit techniques (including privilege escalation) by monitoring the execution of the CPU instruction sequence.</p> <p>The solution should provide link scanning inside email messages to protect against zero-day attacks as well as unknown malware.</p> <p>The solution should contain the means to combat the methods of detecting the performance in the "sandbox".</p> |
|---|--|

| | |
|---|--|
| <p>exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.</p> <p>Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.</p> <p>Решение должно содержать средства борьбы с методиками детектирования исполнения в «песочнице».</p> <p>Решение должно обеспечивать возможность управления им с централизованного менеджмента.</p> <p>Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.</p> <p>Решение должно обеспечивать устранение угроз и удаление опасного содержимого, включая активный контент и встроенные объекты.</p> <p>Решение должно обеспечивать реконструирование файлов с использованием безопасных элементов.</p> <p>Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален.</p> <p>Решение должно обеспечить возможность получения оригинала файла после эмуляции через портал самообслуживания без подключения администратора системы.</p> <p>Решение должно обеспечивать функционал Anti-Spam и Безопасности электронной почты.</p> <p>Решение должно обеспечивать функционал IPSEC VPN.</p> <p>Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.</p> <p>Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.</p> <p>Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20</p> <p>Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC</p> <p>Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:</p> <p>Полносвязная сеть (все-со-всеми);</p> <p>Звездообразная сеть (удаленные офисы к центральному сайту);</p> | <p>The solution must be able to manage it from a central management point of view.</p> <p>The solution should generate a detailed report on the results of each infected file.</p> <p>The solution must eliminate threats and remove dangerous content, including active content and embedded objects.</p> <p>The solution should allow for the reconstruction of files using secure elements.</p> <p>The solution should provide flexible settings to support the original file format and specify the types of content to be removed.</p> <p>The solution should make it possible to receive the original file after emulation through a self-service portal without administrator connection.</p> <p>The solution must provide Anti-Spam and email security functionality.</p> <p>The solution must provide IPSEC VPN functionality.</p> <p>There should be support for an internal CA (Certificate Authority) as well as external third party CAs.</p> <p>The solution must support 3DES and AES-256 encryption for phase I and II IKEv2 as well as "Suite-B-GCM-128" and "Suite-B-GCM-256" for phase II.</p> <p>The decision must support at least the following Diffie-Hellman groups: Group 1 (768 bits), Group 2 (1024 bits), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 and Group 20.</p> <p>The solution should support md5, sha1 SHA-256, SHA-384 and AES-XCBC data integrity.</p> <p>The solution must include support for VPNs like site-to-site in the following topologies:</p> <p>Fully connected network (all of them);</p> <p>Star network (remote offices to the central site);</p> <p>Fan network (remote site through a central site to another remote site);</p> <p>Have the opportunity to purchase a license for DLP functionality. DLP functionality should provide control over confidential information leaks via SMTP, FTP, HTTP, HTTPS, TLS and webmail, the ability to decrypt SSL traffic should be supported. The ability to identify sensitive documents by predefined templates or by watermarked documents must be supported. The system must support over 500 file types;</p> |
|---|--|

Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт);

Иметь возможность приобретения лицензии на функционал DLP. Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP, HTTPS, TLS и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или по метке документов водяными знаками. Система должна поддерживать более 500 типов файлов;

Аппаратные и рабочие требования к шлюзу.

Форм-фактор не более 1U.

Продуктивные сетевые интерфейсы (минимальные требования):

6x1 Гбит/с медные Ethernet.

4x1 Гбит/с оптические порты SFP

4x SR SFP трансиверов

Пропускная способность IPS: минимум 2.9 Гбит/с.

Пропускная способность Firewall: минимум 15 Гбит/с.

Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 2.5 Гбит/с.

Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачная «песочница»): минимум 1.1 Гбит/с.

Одновременные соединения: минимум 3,2 миллиона.

Новые соединения: минимум 120 000 в секунду.

Локальное дисковое пространство: не менее 1x1 TB HDD.

ОЗУ: не менее 16 Гб.

Не менее 1 блок питания AC (AC 250V 50Hz)

Поддержка и подписка.

Техническая поддержка и подписки от производителя сроком на 3 года, 9x5, гарантированное время реакции – 4 часа.

Hardware and working requirements for the gateway.

The form factor is not more than 1U.

Productive network interfaces (minimum requirements):

6x1 Gbps copper Ethernet.

4x1 Gbps optical SFP ports

4x SR SFP transceivers

IPS bandwidth: minimum 2.9 Gbps.

Firewall bandwidth: minimum 15 Gbps.

NGFW throughput (with Firewall, Application Control and IPS activated): minimum 2.5 Gbps.

Throughput Threat Prevention (with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, and cloud sandbox activated): minimum 1.1 Gbps.

Simultaneous connections: minimum 3.2 million.

New connections: minimum 120,000 per second.

Local disk space: at least 1x1 TB HDD.

RAM: at least 16 GB.

At least 1 AC power supply (AC 250V 50Hz)

Support and subscription.

Technical support and subscriptions from the manufacturer for 3 years, 9x5, guaranteed reaction time - 4 hours.

| | |
|---|--|
| <p>Требования к файрволу следующего поколения - количество 2 штук (тип FWRS)</p> <p>Общие требования</p> <p>Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.</p> <p>Решение должно поддерживать DHCP, сервер и relay.</p> <p>Решение должно поддерживать HTTP & HTTPS proxy.</p> <p>Решение должно поддерживать функционал reverse proxy.</p> <p>Решение должно включать в себя возможность работы в режиме Transparent/Bridge.</p> <p>Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).</p> <p>Решение должно поддерживать Firewall, IPS, URL-фильтрацию, DLP, Antidot, Antivirus, Управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge.</p> <p>Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.</p> <p>Решение должно поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений. В режиме высокой доступности или режиме распределения нагрузки должно поддерживаться до 8 узлов кластера.</p> <p>Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.</p> <p>По умолчанию, должно поддерживаться 2 виртуальные системы, а с применением дополнительной лицензии должно поддерживаться до 20 виртуальных шлюзов на одном физическом шлюзе.</p> <p>Сетевые возможности: решение должно поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами).</p> <p>Эффективное обеспечение безопасности: каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall,</p> | <p>Requirements for the next generation firewall – quantity 2 pcs (FWRS type)</p> <p>General requirements</p> <p>The Security Gateway should use link state monitoring based on detailed link and application analysis to monitor and control network flow.</p> <p>The solution must support DHCP, server and relay.</p> <p>The solution must support HTTP & HTTPS proxy.</p> <p>The solution must support reverse proxy functionality.</p> <p>The solution must include the ability to work in Transparent/Bridge mode.</p> <p>The solution must support layer 2 of the OSI model (bridge mode).</p> <p>The solution must support Firewall, IPS, URL filtering, DLP, Antidot, Antivirus, Application Management, HTTPS inspection, Identity Awareness and Sandboxing in bridge mode.</p> <p>The solution must support Active/Standby clustering in bridge mode.</p> <p>The solution must support high gateway availability and load balancing with synchronized network connection states. In high availability mode or load balancing mode, up to 8 cluster nodes must be supported.</p> <p>The solution must support security gateway virtualization to consolidate multiple virtual gateways on a single physical device.</p> <p>By default, 2 virtual systems must be supported, and with an additional license, up to 20 virtual gateways must be supported on a single physical gateway.</p> <p>Networking capabilities: The solution must support virtual switches and virtual routers to configure network communications between virtual systems (virtual gateways).</p> <p>Effective security: Each virtual gateway must be able to run its own set of security services. For example, one Virtual Gateway works as Firewall, one Virtual Gateway works as Firewall and IPS, one Virtual Gateway works as Firewall, IPS, Application Control, URL Filtering, and so on.</p> |
|---|--|

второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.

Выделение ресурсов: решение должно обеспечивать управление вычислительными мощностями, гарантируя, что каждая виртуальная система получит то количество процессорной мощности и оперативной памяти, которая необходима для выполнения ее задач.

Решение должно обеспечивать поддержку IPv6.

Решение должно поддерживать политику, основанную на QoS.

Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

Решение должно обеспечивать функционал Идентификации пользователей.

Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

База данных управления приложениями должна содержать свыше 8000 известных приложений.

Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.

Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное аномальное сетевое поведение.

Allocation of resources: The solution must provide computational power management, ensuring that each virtual system gets the amount of processor power and RAM needed to perform its tasks.

The solution must support IPv6.

The solution must support a policy based on QoS.

The solution must be able to guarantee or limit bandwidth and manage latency for a specific IP source, destination IP or service.

The solution must be able to randomly apply QoS rules to VPN traffic.

The solution must provide IPS (intrusion prevention system) functionality.

The IPS system should be based on the following detection mechanisms: use of signatures, tracking of protocol anomalies, application management and behavioral based detection.

The solution must provide user identification functionality.

Must be able to collect user IDs by requesting Microsoft Active Directory based on security events.

Must have a browser-based method of authenticating user ID for non-domain users or computers.

There must be a special agent that can be installed by policy on the users' computers, and that can collect and pass IDs to the security gateway.

The solution must provide application management functionality and URL filtering.

The Application Management Database must contain over 8000 known applications.

The solution must provide detailed security control for at least 250000 Web 2.0 widgets.

The solution must provide URL categorization, which includes more than 200 million URLs.

The solution must provide Anti-Bot and Anti-Virus functionality.

The Anti-bot application must be able to detect and stop suspicious abnormal network behavior.

The Anti-Bot application must use a multi-layered discovery mechanism that includes IP, URL and DNS reputation and bot discovery via communication protocol templates.

The Anti-virus application should prevent access to malicious websites and stop incoming malicious files.

| | |
|---|---|
| <p>Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.</p> <p>Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.</p> <p>Приложение Anti-virus должно быть способно проверять зашифрованный SSL трафик.</p> <p>Решение должно обеспечивать функционал инспекции SSL (входящего / исходящего трафика).</p> <p>Решение должно интегрироваться с «песочницей» - Sandboxing (инспекция – в облаке или на выделенном локальном устройстве) путем приобретения дополнительной лицензии.</p> <p>Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО – обеспечивая защиту в период до появления статических сигнатур, защищающих от таких угроз.</p> <p>Топология внедрения:</p> <p>Поддержка режима сетевой «песочницы» (network based).</p> <p>Поддержка режима инлайн (bridge mode).</p> <p>Поддержка режима почтового агента (Mail Transfer Mode, MTA).</p> <p>Поддержка режима зеркального порта (TAP/SPAN порт).</p> <p>Решение не должно содержать отдельную инфраструктуру для защиты почты и веба.</p> <p>Решение должно поддерживать кластеризацию для обеспечения отказоустойчивости.</p> <p>Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.</p> <p>Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе и специально настроенные образы.</p> <p>Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.</p> <p>Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Мбайт.</p> <p>Решение должно детектировать атаки на стадии выполнения эксплойта (exploitation) – т.е. до того как запускается шелл-код и осуществляется загрузка/исполнение самого кода зловредного ПО.</p> <p>Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege</p> | <p>The Anti-virus application must be able to verify SSL encrypted traffic.</p> <p>The solution should provide SSL (inbound/outbound traffic) inspection functionality.</p> <p>The solution must integrate with Sandboxing (inspection - in the cloud or on a dedicated local device) by purchasing an additional license.</p> <p>The sandbox feature should provide protection against zero-day attacks, as well as unknown malware - providing protection until static signatures appear to protect against such threats.</p> <p>Implementation topology:</p> <p>Supports network based sandbox mode.</p> <p>Support for in-line (bridge mode).</p> <p>Support for Mail Transfer Mode (MTA).</p> <p>Supports mirror port mode (TAP/SPAN port).</p> <p>The solution must not contain a separate infrastructure to protect the mail and the web.</p> <p>The solution must support clustering to ensure fault tolerance.</p> <p>The solution must emulate executable files, archives, documents including Java and flash.</p> <p>The emulation engine must support a variety of operating systems, such as XP and Windows 7, including specially configured images.</p> <p>The emulation engine should inspect, emulate, prevent and transmit events to the anti-malware infrastructure.</p> <p>The solution should provide emulation of files both small and larger than 10Mbytes.</p> <p>The solution must detect attacks at the executable execution stage (i.e. before the shell code is launched and the malware code itself is loaded/executed).</p> <p>The solution must detect ROP (return oriented programming) and other exploit techniques (including privilege escalation) by monitoring the execution of the CPU instruction sequence.</p> <p>The solution should provide link scanning inside email messages to protect against zero-day attacks as well as unknown malware.</p> <p>The solution should contain the means to combat the methods of detecting the performance in the "sandbox".</p> |
|---|---|

| | |
|---|---|
| <p>exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.</p> <p>Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.</p> <p>Решение должно содержать средства борьбы с методиками детектирования исполнения в «песочнице».</p> <p>Решение должно обеспечивать возможность управления им с централизованного менеджмента.</p> <p>Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.</p> <p>Решение должно обеспечивать устранение угроз и удаление опасного содержимого, включая активный контент и встроенные объекты.</p> <p>Решение должно обеспечивать реконструирование файлов с использованием безопасных элементов.</p> <p>Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален.</p> <p>Решение должно обеспечить возможность получения оригинала файла после эмуляции через портал самообслуживания без подключения администратора системы.</p> <p>Решение должно обеспечивать функционал Anti-Spam и Безопасности электронной почты.</p> <p>Решение должно обеспечивать функционал IPSEC VPN.</p> <p>Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.</p> <p>Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.</p> <p>Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20</p> <p>Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC</p> <p>Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:</p> <p>Полносвязная сеть (все-со-всеми);</p> <p>Звездообразная сеть (удаленные офисы к центральному сайту);</p> | <p>The solution must be able to manage it from a central management point of view.</p> <p>The solution should generate a detailed report on the results of each infected file.</p> <p>The solution must eliminate threats and remove dangerous content, including active content and embedded objects.</p> <p>The solution should allow for the reconstruction of files using secure elements.</p> <p>The solution should provide flexible settings to support the original file format and specify the types of content to be removed.</p> <p>The solution should make it possible to receive the original file after emulation through a self-service portal without administrator connection.</p> <p>The solution must provide Anti-Spam and email security functionality.</p> <p>The solution must provide IPSEC VPN functionality.</p> <p>There should be support for an internal CA (Certificate Authority) as well as external third party CAs.</p> <p>The solution must support 3DES and AES-256 encryption for phase I and II IKEv2 as well as "Suite-B-GCM-128" and "Suite-B-GCM-256" for phase II.</p> <p>The solution must support at least the following Diffie-Hellman groups: Group 1 (768 bits), Group 2 (1024 bits), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 and Group 20.</p> <p>The solution should support md5, sha1 SHA-256, SHA-384 and AES-XCBC data integrity.</p> <p>The solution must include support for VPNs like site-to-site in the following topologies:</p> <p>Fully connected network (all of them);</p> <p>Star network (remote offices to the central site);</p> <p>Fan network (remote site through a central site to another remote site);</p> <p>Have the opportunity to purchase a license for DLP functionality.</p> <p>DLP functionality should provide control over confidential information leaks via SMTP, FTP, HTTP, HTTPS, TLS and webmail, the ability to decrypt SSL traffic should be supported. The ability to identify sensitive documents by predefined templates or by</p> |
|---|---|

Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт);

Иметь возможность приобретения лицензии на функционал DLP. Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP, HTTPS, TLS и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или по метке документов водяными знаками. Система должна поддерживать более 500 типов файлов;

Аппаратные и рабочие требования к шлюзу.

Форм-фактор не более 1U.

Продуктивные сетевые интерфейсы (минимальные требования):

6x1 Гбит/с медные Ethernet.

4x1 Гбит/с оптические порты SFP

4x SR SFP трансиверов

Пропускная способность IPS: минимум 2.3 Гбит/с.

Пропускная способность Firewall: минимум 14 Гбит/с.

Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 2 Гбит/с.

Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачная «песочница»): минимум 1 Гбит/с.

Одновременные соединения: минимум 3,2 миллиона.

Новые соединения: минимум 110 000 в секунду.

Локальное дисковое пространство: не менее 1x1 TB HDD.

ОЗУ: не менее 16 Гб.

Не менее 1 блок питания AC (AC 250V 50Hz)

Поддержка и подписка.

Техническая поддержка и подписки от производителя сроком на 3 года, 9x5, гарантированное время реакции – 4 часа.

watermarked documents must be supported. The system must support over 500 file types;

Hardware and working requirements for the gateway.

The form factor is not more than 1U.

Productive network interfaces (minimum requirements):

6x1 Gbps copper Ethernet.

4x1 Gbps optical SFP ports

4x SR SFP transceivers

IPS bandwidth: minimum 2.3 Gbps.

Firewall bandwidth: minimum 14 Gbps.

NGFW throughput (with Firewall, Application Control and IPS activated): minimum 2 Gbps.

Throughput Threat Prevention (with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, and cloud sandbox activated): minimum 1 Gbps.

Simultaneous connections: minimum 3.2 million.

New connections: minimum 110,000 per second.

Local disk space: at least 1x1 TB HDD.

RAM: at least 16 GB.

At least 1 AC power supply (AC 250V 50Hz)

Support and subscription.

Technical support and subscriptions from the manufacturer for 3 years, 9x5, guaranteed reaction time - 4 hours.

| | |
|--|---|
| <p>Требования к файрволу следующего поколения - количество 1 штук (тип FWUP)</p> <p>Общие требования</p> <p>Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.</p> <p>Решение должно поддерживать DHCP, сервер и relay.</p> <p>Решение должно поддерживать HTTP & HTTPS proxy.</p> <p>Решение должно поддерживать функционал reverse proxy.</p> <p>Решение должно включать в себя возможность работы в режиме Transparent/Bridge.</p> <p>Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).</p> <p>Решение должно поддерживать Firewall, IPS, URL-фильтрацию, DLP, Antitbot, Antivirus, Управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge.</p> <p>Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.</p> <p>Решение должно поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений. В режиме высокой доступности или режиме распределения нагрузки должно поддерживаться до 8 узлов кластера.</p> <p>Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.</p> <p>По умолчанию, должно поддерживаться 2 виртуальные системы, а с применением дополнительной лицензии должно поддерживаться до 20 виртуальных шлюзов на одном физическом шлюзе.</p> <p>Сетевые возможности: решение должно поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами).</p> <p>Эффективное обеспечение безопасности: каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall,</p> | <p>Requirements for the next generation firewall - quantity 1 pcs (FWUP type)</p> <p>General requirements</p> <p>The Security Gateway should use link state monitoring based on detailed link and application analysis to monitor and control network flow.</p> <p>The solution must support DHCP, server and relay.</p> <p>The solution must support HTTP & HTTPS proxy.</p> <p>The solution must support reverse proxy functionality.</p> <p>The solution must include the ability to work in Transparent/Bridge mode.</p> <p>The solution must support layer 2 of the OSI model (bridge mode).</p> <p>The solution must support Firewall, IPS, URL filtering, DLP, Antitbot, Antivirus, Application Management, HTTPS inspection, Identity Awareness and Sandboxing in bridge mode.</p> <p>The solution must support Active/Standby clustering in bridge mode.</p> <p>The solution must support high gateway availability and load balancing with synchronized network connection states. In high availability mode or load balancing mode, up to 8 cluster nodes must be supported.</p> <p>The solution must support security gateway virtualization to consolidate multiple virtual gateways on a single physical device.</p> <p>By default, 2 virtual systems must be supported, and with an additional license, up to 20 virtual gateways must be supported on a single physical gateway.</p> <p>Networking capabilities: The solution must support virtual switches and virtual routers to configure network communications between virtual systems (virtual gateways).</p> <p>Effective security: Each virtual gateway must be able to run its own set of security services. For example, one Virtual Gateway works as Firewall, one Virtual Gateway works as Firewall and IPS, one Virtual Gateway works as Firewall, IPS, Application Control, URL Filtering, and so on.</p> |
|--|---|

второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.

Выделение ресурсов: решение должно обеспечивать управление вычислительными мощностями, гарантируя, что каждая виртуальная система получит то количество процессорной мощности и оперативной памяти, которая необходима для выполнения ее задач.

Решение должно обеспечивать поддержку IPv6.

Решение должно поддерживать политику, основанную на QoS.

Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

Решение должно обеспечивать функционал Идентификации пользователей.

Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

База данных управления приложениями должна содержать свыше 8000 известных приложений.

Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.

Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное аномальное сетевое поведение.

Allocation of resources: The solution must provide computational power management, ensuring that each virtual system gets the amount of processor power and RAM needed to perform its tasks. The solution must support IPv6.

The solution must support a policy based on QoS.

The solution must be able to guarantee or limit bandwidth and manage latency for a specific IP source, destination IP or service.

The solution must be able to randomly apply QoS rules to VPN traffic.

The solution must provide IPS (intrusion prevention system) functionality.

The IPS system should be based on the following detection mechanisms: use of signatures, tracking of protocol anomalies, application management and behavioral based detection.

The solution must provide user identification functionality.

Must be able to collect user IDs by requesting Microsoft Active Directory based on security events.

Must have a browser-based method of authenticating user ID for non-domain users or computers.

There must be a special agent that can be installed by policy on the users' computers, and that can collect and pass IDs to the security gateway.

The solution must provide application management functionality and URL filtering.

The Application Management Database must contain over 8000 known applications.

The solution must provide detailed security control for at least 250000 Web 2.0 widgets.

The solution must provide URL categorization, which includes more than 200 million URLs.

The solution must provide Anti-Bot and Anti-Virus functionality.

The Anti-bot application must be able to detect and stop suspicious abnormal network behavior.

| | |
|---|---|
| <p>Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.</p> <p>Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.</p> <p>Приложение Anti-virus должно быть способно проверять зашифрованный SSL трафик.</p> <p>Решение должно обеспечивать функционал инспекции SSL (входящего / исходящего трафика).</p> <p>Решение должно интегрироваться с «песочницей» - Sandboxing (инспекция – в облаке или на выделенном локальном устройстве) путем приобретения дополнительной лицензии.</p> <p>Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО – обеспечивая защиту в период до появления статических сигнатур, защищающих от таких угроз.</p> <p>Топология внедрения:</p> <p>Поддержка режима сетевой «песочницы» (network based).</p> <p>Поддержка режима инлайн (bridge mode).</p> <p>Поддержка режима почтового агента (Mail Transfer Mode, MTA).</p> <p>Поддержка режима зеркального порта (TAP/SPAN порт).</p> <p>Решение не должно содержать отдельную инфраструктуру для защиты почты и веба.</p> <p>Решение должно поддерживать кластеризацию для обеспечения отказоустойчивости.</p> <p>Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.</p> <p>Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе и специально настроенные образы.</p> <p>Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.</p> <p>Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Мбайт.</p> <p>Решение должно детектировать атаки на стадии выполнения эксплойта (exploitation) – т.е. до того как запускается шелл-код и осуществляется загрузка/исполнение самого кода зловредного ПО.</p> <p>Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege</p> | <p>The Anti-Bot application must use a multi-layered discovery mechanism that includes IP, URL and DNS reputation and bot discovery via communication protocol templates.</p> <p>The Anti-virus application should prevent access to malicious websites and stop incoming malicious files.</p> <p>The Anti-virus application must be able to verify SSL encrypted traffic.</p> <p>The solution should provide SSL (inbound/outbound traffic) inspection functionality.</p> <p>The solution must integrate with Sandboxing (inspection - in the cloud or on a dedicated local device) by purchasing an additional license.</p> <p>The sandbox feature should provide protection against zero-day attacks, as well as unknown malware - providing protection until static signatures appear to protect against such threats.</p> <p>Implementation topology:</p> <p>Supports network based sandbox mode.</p> <p>Support for in-line (bridge mode).</p> <p>Support for Mail Transfer Mode (MTA).</p> <p>Supports mirror port mode (TAP/SPAN port).</p> <p>The solution must not contain a separate infrastructure to protect the mail and the web.</p> <p>The solution must support clustering to ensure fault tolerance.</p> <p>The solution must emulate executable files, archives, documents including Java and flash.</p> <p>The emulation engine must support a variety of operating systems, such as XP and Windows 7, including specially configured images.</p> <p>The emulation engine should inspect, emulate, prevent and transmit events to the anti-malware infrastructure.</p> <p>The solution should provide emulation of files both small and larger than 10Mbytes.</p> <p>The solution must detect attacks at the executable execution stage (i.e. before the shell code is launched and the malware code itself is loaded/executed).</p> <p>The solution must detect ROP (return oriented programming) and other exploit techniques (including privilege escalation) by monitoring the execution of the CPU instruction sequence.</p> |
|---|---|

| | |
|---|--|
| <p>exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.</p> <p>Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.</p> <p>Решение должно содержать средства борьбы с методиками детектирования исполнения в «песочнице».</p> <p>Решение должно обеспечивать возможность управления им с централизованного менеджмента.</p> <p>Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.</p> <p>Решение должно обеспечивать устранение угроз и удаление опасного содержимого, включая активный контент и встроенные объекты.</p> <p>Решение должно обеспечивать реконструирование файлов с использованием безопасных элементов.</p> <p>Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален.</p> <p>Решение должно обеспечить возможность получения оригинала файла после эмуляции через портал самообслуживания без подключения администратора системы.</p> <p>Решение должно обеспечивать функционал Anti-Spam и Безопасности электронной почты.</p> <p>Решение должно обеспечивать функционал IPSEC VPN.</p> <p>Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.</p> <p>Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.</p> <p>Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20</p> <p>Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC</p> <p>Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:</p> <p>Полносвязная сеть (все-со-всеми);</p> <p>Звездообразная сеть (удаленные офисы к центральному сайту);</p> | <p>The solution should provide link scanning inside email messages to protect against zero-day attacks as well as unknown malware.</p> <p>The solution should contain the means to combat the methods of detecting the performance in the "sandbox".</p> <p>The solution must be able to manage it from a central management point of view.</p> <p>The solution should generate a detailed report on the results of each infected file.</p> <p>The solution must eliminate threats and remove dangerous content, including active content and embedded objects.</p> <p>The solution should allow for the reconstruction of files using secure elements.</p> <p>The solution should provide flexible settings to support the original file format and specify the types of content to be removed.</p> <p>The solution should make it possible to receive the original file after emulation through a self-service portal without administrator connection.</p> <p>The solution must provide Anti-Spam and email security functionality.</p> <p>The solution must provide IPSEC VPN functionality.</p> <p>There should be support for an internal CA (Certificate Authority) as well as external third party CAs.</p> <p>The solution must support 3DES and AES-256 encryption for phase I and II IKEv2 as well as "Suite-B-GCM-128" and "Suite-B-GCM-256" for phase II.</p> <p>The solution must support at least the following Diffie-Hellman groups: Group 1 (768 bits), Group 2 (1024 bits), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 and Group 20.</p> <p>The solution should support md5, sha1 SHA-256, SHA-384 and AES-XCBC data integrity.</p> <p>The solution must include support for VPNs like site-to-site in the following topologies:</p> <p>Fully connected network (all of them);</p> <p>Star network (remote offices to the central site);</p> |
|---|--|

Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт);

Иметь возможность приобретения лицензии на функционал DLP. Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP, HTTPS, TLS и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или по метке документов водяными знаками. Система должна поддерживать более 500 типов файлов;

Удаленный мобильный доступ

Решение должно обеспечивать функционал Удаленного мобильного доступа для неограниченного количества одновременных соединений пользователей.

Решение должно поддерживать управляемые и неуправляемые устройства доступа, такие как BYOD (принеси собственное устройство)

Решение должно обеспечивать Мобильный VPN-Клиент: VPN-приложение, обеспечивающее безопасный доступ к корпоративным ресурсам через SSL или IPsec туннель.

Решение должно обеспечивать SSL VPN-Портал: механизм для безопасного подключения к корпоративным ресурсам через портал из веб-браузера.

Решение должно обеспечивать функционал безклиентного VPN: плагин, который обеспечивает удаленный доступ с предоставлением полной возможности сетевого соединения для IP-приложений. Решение должно обеспечивать функционал SSL VPN 3-уровня по запросу для подключения к корпоративным ресурсам. Решение должно поддерживать любое IP-приложение, включая ICMP, TCP и UDP, не требуя сложной конфигурации для поддержки каждого приложения. Он должен работать на удаленных компьютерах, не требуя прав администратора.

Решение должно обеспечивать технологию виртуального рабочего стола, которая позволяет защищать данные во время сеансов пользователей и позволяет чистить кэш после окончания сеансов. Технология виртуального рабочего стола должна защищать все данные конкретной сессии на стороне клиента, а также:

Создавать безопасную виртуальную среду, изолированную от хоста,

Шифровать и удалять кэш, файлы и т.д. браузера и приложений, когда сеанс окончен.

Решение должно обеспечивать двухфакторный механизм СМС аутентификации. Решение должно быть конфигурируемым, чтобы отправлять

Fan network (remote site through a central site to another remote site);

Have the opportunity to purchase a license for DLP functionality. DLP functionality should provide control over confidential information leaks via SMTP, FTP, HTTP, HTTPS, TLS and webmail, the ability to decrypt SSL traffic should be supported. The ability to identify sensitive documents by predefined templates or by watermarked documents must be supported. The system must support over 500 file types;

Remote mobile access

The solution must provide Remote Mobile Access functionality for an unlimited number of simultaneous user connections.

The solution must support managed and unmanaged access devices such as BYOD (bring your own device)

The solution must provide a Mobile VPN Client: a VPN application that provides secure access to corporate resources over an SSL or IPsec tunnel.

The solution should provide SSL VPN Portal: a mechanism for secure connection to corporate resources through the portal from a web browser.

The solution must provide client-free VPN functionality: a plugin that provides remote access with full network connectivity for IP applications. The solution must provide 3-level SSL VPN functionality on demand to connect to corporate resources. The solution must support any IP application including ICMP, TCP and UDP without requiring complex

Configuration to support each application. It should run on remote computers without requiring administrator rights.

The solution must provide virtual desktop technology that protects data during user sessions and allows the cache to be cleaned after

одноразовый пароль (OTP) на устройство связи конечного пользователя (например, мобильный телефон) посредством СМС сообщения. Двухфакторная СМС аутентификация обеспечивает дополнительный уровень безопасности, устраняя трудности, связанные с управлением аппаратными ключами.

Решение должно реализовать функционал интегрированной системы предотвращения вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг, настраиваемый модуль блокирования HTTP червей, защиту от обхода каталога (directory traversal), защиту от отклонения заголовков (header rejection), защиту от вредоносного HTTP-кода.

В целом, решение должно обеспечивать следующие функции:

Безопасный SSL VPN доступ

Двухфакторная аутентификация

Ассоциирование мобильных устройств с конечными пользователями

Мобильный бизнес-портал

Обеспечение соответствия конечных точек соединения корпоративной политике

Аппаратные и рабочие требования к шлюзу.

Форм-фактор не более 1U.

Продуктивные сетевые интерфейсы (минимальные требования):

6x1 Гбит/с медные Ethernet.

4x1 Гбит/с оптические порты SFP

4x SR SFP трансиверов

Пропускная способность IPS: минимум 2.3 Гбит/с.

Пропускная способность Firewall: минимум 14 Гбит/с.

Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 2 Гбит/с.

Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачная «песочница»): минимум 1 Гбит/с.

Одновременные соединения: минимум 3,2 миллиона.

Новые соединения: минимум 110 000 в секунду.

Локальное дисковое пространство: не менее 1x1 TB HDD.

ОЗУ: не менее 16 Гб.

Не менее 1 блок питания AC (AC 250V 50Hz)

sessions are over. Virtual Desktop technology should protect all data from a particular session on the client side as well:

Create a secure virtual environment that is isolated from the host, Encrypt and delete the cache, files, etc. of the browser and applications when the session is over.

The solution should provide a two-factor authentication mechanism for SMS. The solution must be configurable to send a one-time password (OTP) to an end user communication device (e.g. mobile phone) via SMS. Two-factor SMS authentication provides an additional level of security by eliminating the complexity associated with managing hardware keys.

The solution must implement the functionality of an integrated intrusion prevention system against malicious code transmitted in web applications. The solution should be able to block worms, various attacks such as buffer overflow, SQL and command injection, cross-site scripting, custom HTTP worm blocking module, directory traversal, header rejection, protection against HTTP malicious code.

In general, the solution should provide the following functions:

Secure SSL VPN access

Two-factor authentication

Mobile device association with end users

Mobile business portal

Ensure endpoint connectivity complies with corporate policy

Hardware and working requirements for the gateway.

The form factor is not more than 1U.

Productive network interfaces (minimum requirements):

6x1 Gbps copper Ethernet.

4x1 Gbps optical SFP ports

4x SR SFP transceivers

IPS bandwidth: minimum 2.3 Gbps.

Firewall bandwidth: minimum 14 Gbps.

NGFW throughput (with Firewall, Application Control and IPS activated): minimum 2 Gbps.

Throughput Threat Prevention (with Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, and cloud sandbox activated): minimum 1 Gbps.

Поддержка и подписка.

Техническая поддержка и подписки от производителя сроком на 3 года, 9x5, гарантированное время реакции – 4 часа.

Simultaneous connections: minimum 3.2 million.
New connections: minimum 110,000 per second.
Local disk space: at least 1x1 TB HDD.
RAM: at least 16 GB.

At least 1 AC power supply (AC 250V 50Hz)

Support and subscription.

Technical support and subscriptions from the manufacturer for 3 years, 9x5, guaranteed reaction time - 4 hours.

| | |
|--|---|
| <p>Требования к аппаратной «песочнице» - количество 1 штук (тип - SNDBX)</p> <p>«Песочница» должна быть полностью интегрирована в систему централизованного управления безопасностью указанных в Требованиях к SECMGMT.</p> <p>«Песочница» должна обеспечивать инспекцию файлов в сетевом трафике при помощи технологий Firewall, антибот, антивирус, запуск исполняемого файла в изолированной среде.</p> <p>«Песочница» должна поддерживать следующие режимы работы: Inline (L2-Transparent Bridge), SPAN, MTA, ICAP, а также должна иметь возможность работать в “standalone” режиме, без необходимости управления со стороннего сервера.</p> <p>При наличии соответствующей подписки «песочница» должна иметь функционал NGFW с функцией идентификации приложений и дальнейшего DPI</p> <p>Количество идентифицируемых приложений не менее 8000.</p> <p>Не менее 8 одновременно запущенных виртуальных машин.</p> <p>Эмуляция не менее 1 000 уникальных файлов в час.</p> <p>Пропускная способность не менее 650 Мбит/с.</p> <p>Поддержка виртуальных машин с ОС MS Windows XP SP3 32 бит, Windows 7 32 и 64 бит, Windows 8.1 32 и 64 бит, Windows 10 32 и 64 бит.</p> <p>Одновременная динамическая проверка (эмуляция) каждого неизвестного файла в нескольких виртуальных машинах с разными версиями Windows и прикладного ПО MS Office, Adobe Reader, Flash, Java, браузеров (мульти-версионный анализ).</p> <p>Лицензирование ОС и прикладного ПО, обновление и техническая поддержка виртуальных машин должна осуществляться производителем</p> <p>Динамическая проверка (эмуляция) документов форматов MS Office 2003/2007/2016 и более поздних версий, PDF, CSV.</p> <p>Динамическая проверка (эмуляция) исполняемых файлов и скриптов, включая EXE, SCR, CPL, COM, PIF, JAR.</p> <p>Проверка файлов внутри архивов, включая ZIP, GZIP, RAR, 7z, CAB, TAR, TGZ, BZ2, ISO.</p> | <p>Requirements for the hardware sandbox - quantity 1 pcs (type - SNDBX)</p> <p>The "Sandbox" must be fully integrated into the central safety management system specified in the SECMGMT Requirements.</p> <p>"The Sandbox should provide inspection of files in network traffic using Firewall technologies, antibot, antivirus, running the executable file in an isolated environment.</p> <p>"The Sandbox must support the following operating modes: Inline (L2-Transparent Bridge), SPAN, MTA, ICAP, and must also be able to operate in "standalone" mode, without the need for management from a third-party server.</p> <p>If there is a corresponding subscription, the sandbox must have NGFW functionality with the function of application identification and further DPI.</p> <p>The number of identifiable applications is at least 8000.</p> <p>At least 8 virtual machines running simultaneously.</p> <p>Emulation of at least 1,000 unique files per hour.</p> <p>The throughput capacity is at least 650 Mbit/s.</p> <p>Support for MS Windows XP SP3 32-bit, Windows 7 32 and 64-bit, Windows 8.1 32 and 64-bit, Windows 10 32 and 64-bit virtual machines.</p> <p>Simultaneous dynamic check (emulation) of each unknown file in several virtual machines with different versions of Windows and MS Office application software, Adobe Reader, Flash, Java, browsers (multiversion analysis).</p> <p>Licensing of operating system and application software, updating and technical support of virtual machines should be provided by the manufacturer.</p> <p>Dynamic check (emulation) of MS Office 2003/2007/2016 and later documents, PDF, CSV.</p> |
|--|---|

Проверка файлов внутри зашифрованных ZIP-архивов с подбором пароля по статическому словарю и тексту электронного письма, в том числе на русском языке.

Возможность блокировать неизвестные вредоносные файлы в веб и почтовом трафике, обнаруженные путем их эмуляции в песочнице, до их доставки получателю (предотвращение первой и последующих попыток заражения/взлома)

Возможность мгновенной доставки безопасной версии проверяемых документов MS Office и PDF пользователям за счет удаления активного содержимого и элементов документа с высокой степенью риска.

Возможность мгновенной доставки безопасной версии проверяемых документов MS Office пользователям за счет их конвертации в PDF либо без конвертации с сохранением оригинального формата.

Возможность мгновенной доставки безопасной версии графических изображений во вложениях и теле электронного письма за счет их конвертации с сохранением идентичного внешнего вида.

Возможность детектировать и блокировать новые эксплойты за счет анализа буфера центрального процессора, а не только поведения в эмулируемой ОС, включая эксплойты, использующие возвратно-ориентированное программирование (Return-Oriented-Programming, ROP).

Возможность детектировать и блокировать составные веб-атаки, использующие эксплойты Flash-анимации, которая требует запуска SWF-файла с параметрами в составе веб-страницы.

Проверка ссылок в теле письма по репутации.

Автоматическое скачивание и динамическая проверка (эмуляция) файлов по ссылкам в теле письма с предварительной проверкой синтаксиса ссылки, чтобы исключить нежелательные автоматические действия от лица пользователей, такие как сброс/подтверждение пароля, подписка на рассылку.

Сетевые интерфейсы: не менее 9x1 Гбит/с Ethernet медь

Габариты по высоте – не более 2U.

Поддержка и подписка.

Техническая поддержка и подписки от производителя сроком на 3 года, 9x5, гарантированное время реакции – 4 часа.

Dynamic verification (emulation) of executable files and scripts including EXE, SCR, CPL, COM, PIF, JAR.

Checking files inside archives including ZIP, GZIP, RAR, 7z, CAB, TAR, TGZ, BZ2, ISO.

Checking files inside encrypted ZIP-archives with password recovery using static dictionary and e-mail text, including in Russian.

Ability to block unknown malicious files in web and email traffic detected by emulating them in the sandbox before they are delivered to the recipient (preventing first and subsequent infection/hacking attempts).

Ability to instantly deliver a secure version of MS Office and PDF documents to users by removing active content and high-risk document elements.

Ability to instantly deliver a secure version of MS Office documents to users by converting them to PDF or without conversion while preserving the original format.

Ability to instantly deliver a secure version of graphic images in attachments and the body of an email by converting them while maintaining an identical appearance.

The ability to detect and block new exploits by analyzing the CPU buffer, not just the behavior in the emulated OS, including exploits that use Return-Oriented-Programming (ROP).

The ability to detect and block composite web attacks using Flash animation exploits that require a SWF file with parameters as part of a web page.

Checking references in the body of the letter by reputation.

Automatic download and dynamic verification (emulation) of files by links in the body of the email with a preliminary check of the link syntax to exclude unwanted automatic actions on behalf of users, such as reset/confirmation of password, subscription to the newsletter.

Network interfaces: at least 9x1 Gbit/s Ethernet copper

Dimensions in height - no more than 2U.

Support and subscription.

Technical support and subscriptions from the manufacturer for 3 years, 9x5, guaranteed reaction time - 4 hours.

| | |
|---|--|
| <p>Централизованный центр управления безопасности Требования к централизованному управлению безопасностью, анализу событий и отчетности. - количество 1 комплект (тип - SECMGMT) Решение должно обеспечивать функционал централизованного управления безопасностью. Все приложения безопасности Брандмауэра следующего поколения должны быть управляемыми с центральной консоли GUI. Централизованное управление безопасностью должно управлять не менее 10 шлюзами. Приложение для управления безопасностью должно поддерживать учетные записи администраторов на основе ролей. Например, только роли для управления политикой брандмауэра или только роль для просмотра журнала. Решение должно обеспечивать возможность обеспечения высокой доступности системы управления, используя резервный сервер управления, который автоматически синхронизируется с активным сервером. Решение должно включать возможность централизованного распространения и применения новых версий шлюзового программного обеспечения. Решение должно включать инструмент для централизованного управления лицензиями всех шлюзов, контролируемых станцией управления. Решение должно обеспечивать механизм обновления во всех приложениях включая IPS, Управление приложениями, URL-фильтрацию, Anti-Bot и Anti-Virus. Решение должно обеспечивать функционал Централизованного Протоколирования и Мониторинга. Система централизованного протоколирования событий должна быть частью системы управления. Решение должно протоколировать все правила. У средства просмотра журналов событий должна быть возможность индексированного поиска. Решение должно иметь возможность протоколирования событий во всех интегрированных приложениях безопасности на шлюзе (включая виртуальные шлюзы), включая Firewall, IPSEC VPN, IPS, Идентификация</p> | <p>Centralized security management Requirements for centralized security management, event analysis and reporting. – quantity 1 set (type - SECMGMT) The solution must provide the functionality of centralized security management. All next generation firewall security applications must be managed from a central GUI console. Centralized security management must manage at least 10 gateways. The security management application must support role-based administrator accounts. For example, only roles to manage firewall policy, or only a log viewer role. The solution must be able to provide high availability of the management system, using a backup management server that automatically synchronizes with the active server. The solution should include the ability to centrally distribute and apply new versions of gateway software. The solution must include a tool to centrally manage the licenses of all gateways controlled by the control station. The solution must provide an update mechanism in all applications including IPS, Application Management, URL filtering, Anti-Bot and Anti-Virus. The solution should provide Centralized Logging and Monitoring functionality. The centralized event logging system should be part of the control system. The solution must log all the rules. The event log viewer must be able to perform an indexed search. The solution must be able to log events in all integrated security applications at the gateway (including virtual gateways), including Firewall, IPSEC VPN, IPS, User Identification, Mobile Access, DLP,</p> |
|---|--|

пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрацию, Anti-Bot, Anti-Virus, Sandboxing.

У системы протоколирования должен быть безопасный канал для передачи данных для предотвращения подслушивания, канал передачи должен быть зашифрован и проходить проверку подлинности.

Журналы событий должны безопасно передаваться между шлюзом и управлением или выделенным сервером журналов и консолью просмотра журналов в компьютере администратора.

Решение должно включать опцию динамического блокирования активного соединения в графическом интерфейсе системы протоколирования событий без необходимости внесения изменений в базу правил.

Решение должно включать настраиваемую установку пороговых значений параметров для выполнения действий при достижении определенных пороговых значений на шлюзе. Действия должны включать: запись события, оповещение, отправка SNMP trap, отправка электронного письма и выполнение определенного пользователем предупреждения.

Решение должно включать предварительно настроенные графики для мониторинга трафика во времени и системных счетчиков: главные правила безопасности, основные пользователи P2P, VPN туннели, сетевой трафик и другая полезная информация. Решение должно обеспечивать возможность создания новых графиков с различными типами диаграмм.

Решение должно обеспечивать функционал Централизованной Корреляции событий и Отчетов.

Решение должно иметь возможность корреляции событий из всех приложений, включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрация, Anti-Bot, Anti-Virus, Sandboxing.

Решение должно включать инструмент для корреляции событий из всех функций шлюза и сторонних устройств.

Приложение корреляции событий должно обеспечивать графическое представление событий на основе времени.

Решение должно включать возможность поиска внутри списка событий, углубления в детали для изучения и расследования инцидентов.

Решение должно включать predetermined ежечасные, ежедневные, еженедельные и ежемесячные отчеты, в том числе, как минимум, Основные события, Основные источники, Основные пункты назначения, Основные сервисы, Основные источники и их основные события, Основные пункты

Application Management, URL filtering, Anti-Bot, Anti-Virus, Sandboxing.

The logging system must have a secure channel for data transmission to prevent eavesdropping, the transmission channel must be encrypted and authenticated.

Logs should be securely transferred between the gateway and management or a dedicated log server and the log viewer console on the administrator computer.

The solution should include the option of dynamically blocking the active connection in the GUI of the event logging system without the need to make changes to the rule base.

The solution must include a configurable setting of parameter thresholds for actions to be performed when certain thresholds are reached at the gateway. Actions should include: event recording, alert, sending SNMP trap, sending e-mail and executing user-defined alert.

The solution should include pre-configured schedules for monitoring time traffic and system counters: main security rules, main P2P users, VPN tunnels, network traffic and other useful information. The solution must provide the ability to create new graphs with different types of charts.

The solution should provide the functionality of the Centralized Event and Report Correlation.

The solution must be able to correlate events from all applications including Firewall, IPSEC VPN, IPS, User Identification, Mobile Access, DLP, Application Management, URL filtering, Anti-Bot, Anti-Virus, Sandboxing.

The solution must include a tool to correlate events from all gateway and third-party functions.

The event correlation application should provide a graphical representation of events based on time.

The solution should include the ability to search within the list of events, to go into detail to study and investigate incidents.

The solution shall include predetermined hourly, daily, weekly, and monthly reports, including at a minimum the Main Event, Main Sources, Main Destinations, Main Services, Main Sources and their Main Events, Main Destinations and their Main Events, and Main Services and their Main Events.

назначения и их основные события, и Основные сервисы и их основные события.

Решение должно поддерживать автоматическое распространение отчетов по электронной почте, загрузку на FTP/Веб-сервер и скрипт рассылки внешних пользовательских отчетов.

Решение должно обеспечивать функционал управления рисками и соответствия требованиям (GRC) – лучших практик безопасности.

Решение должно обеспечивать оценку соблюдения основных регуляторных требований в режиме реального времени (поддержка стандартов ISO 27001/27002, PCI-DSS, HiPPA, SOX и т.д.).

Решение должно предоставлять рекомендации по реализации лучших практик безопасности.

Решение должно переводить регуляторные требования в инструкции для выполнения лучших практик безопасности.

Решение должно постоянно контролировать конфигурацию шлюза при помощи лучших практик безопасности.

Решение должно генерировать автоматические отчеты по оценке для определения рейтинга соответствия регуляторным требованиям.

Решение должно полностью интегрироваться в Архитектуру программного обеспечения и Инфраструктуру управления.

Решение должно обеспечивать мгновенное уведомление об изменениях политики, влияющих на соответствие регуляторным требованиям.

Технические требования, поддержка и подписка. Система централизованного управления безопасностью должна быть выполнена в виде аппаратного комплекса.

Аппаратные требования к серверу управления

Форм-фактор не более 1U.

Не менее 5x1 Гбит/с медные Ethernet порты

Не менее 1x2 TB HDD

ОЗУ не менее 32 Гб

Не менее 1 блок питания AC (AC 250V 50Hz)

Поддержка и подписка.

Техническая поддержка от производителя сроком на 3 года, 9x5, гарантированное время реакции – 4 часа. В предложение должны быть включены все необходимые подписки на модули системы управления.

The solution should support automatic distribution of reports by e-mail, upload to an FTP/Web server and a script for sending external user reports.

The solution must provide risk management and compliance (GRC) functionality - best security practices.

The solution must provide real-time assessment of compliance with key regulatory requirements (support for ISO 27001/27002, PCI DSS, HiPPA, SOX, etc.).

The solution should provide recommendations for implementing best security practices.

The solution should translate regulatory requirements into instructions for best security practices.

The solution must constantly monitor the gateway configuration with best security practices.

The solution should generate automatic assessment reports to determine the regulatory compliance rating.

The solution must be fully integrated into the Software Architecture and Management Infrastructure.

The solution should provide instant notification of policy changes affecting regulatory compliance.

Technical requirements, support and subscription. The centralized security management system must be implemented as a hardware complex.

Hardware requirements for the management server

The form factor is not more than 1U.

At least 5x1 Gbps copper Ethernet ports

At least 1x2 TB HDD

RAM at least 32 GB

At least 1 AC power supply (AC 250V 50Hz)

Support and subscription.

Technical support from the manufacturer for 3 years, 9x5, guaranteed reaction time - 4 hours. The offer should include all necessary subscriptions to the control system modules.

Шкаф телекоммуникационный (тип – RCKRS)

Общие требования

Напольный 19" монтажный шкаф, разборный, однодверный, 42U (ВхШхГ) не менее 2010х600х800, стальная дверь с перфорацией

Предназначен для размещения активного и пассивного телекоммуникационного и серверного оборудования формата 19"

Климатическое исполнение Предназначено для эксплуатации внутри помещений.

Материал исполнения Сталь 1,5 – 2,0 мм.

Разборная конструкция. Состоит из основания, крыши, двух сварных рам соединяемых комплектом швеллеров, двери и боковые стенки.

Жесткость конструкции обеспечивается наличием в базовой комплектации элементов усиления жесткости (ребра жесткости/ горизонтальные кулисы/ стяжки треугольной формы). Минимально допустимое количество элементов усиления жесткости в базовой комплектации бшт., для крепление в верхней, средней и нижней части боковых плоскостей конструкции.

Вентиляция обеспечивается следующим образом - двери шкафов с перфорацией по всей площади (зона покрытия перфорацией не менее 90% от общей площади двери). Возможность установки на крышу шкафа активных модулей с вентиляторами. В базовой комплектации область установки вентиляторных блоков закрыта защитными шторками.

Винтовые опоры (ножки). Комплектация шкафов/стоек винтовыми опорами для регулирования и выравнивания по уровню пола. Винтовые опоры должны входить в базовую комплектацию шкафов, минимум 4шт. для каждого шкафа.

Монтажные и крепежные изделия, необходимые для полного и законченного сбора шкафа, входят в базовую комплектацию шкафа.

Система заземления. Система заземления шкафа входит в базовую комплектацию.

Наличие кабельных вводов. Кабельные вводы в верхней и нижней частях шкафов.

Стенки шкафа съемные, с замками. Возможность доступа внутрь шкафа для монтажа и обслуживания с четырёх сторон.

Telecommunication cabinet - quantity 2 pcs (type - RCKRS)

General requirements

Floor 19" mounting case, collapsible, single door, 42U (VhShHHG) at least 2010h600h800, steel door with perforation

It is intended for accommodation of the active and passive telecommunication and server equipment of a format 19".

Climatic design Designed for indoor use.

Material of execution Steel 1.5 - 2.0 mm.

Disassembled structure. Consists of a base, a roof, two welded frames connected by a set of channels, doors and side walls.

The stiffness of the structure is ensured by the presence of stiffening elements (stiffening ribs / horizontal wings / triangular tie bars) in the basic configuration. The minimum permitted number of stiffening elements in the basic configuration is 6 pcs., for mounting in the upper, middle and lower part of the side planes of the structure.

Ventilation is provided in the following way - cupboard doors with perforations over the entire area (the area covered by perforations is at least 90% of the total door area). It is possible to install active modules with fans on the roof of the cabinet. In the basic configuration the area of installation of fan units is covered with protective shutters.

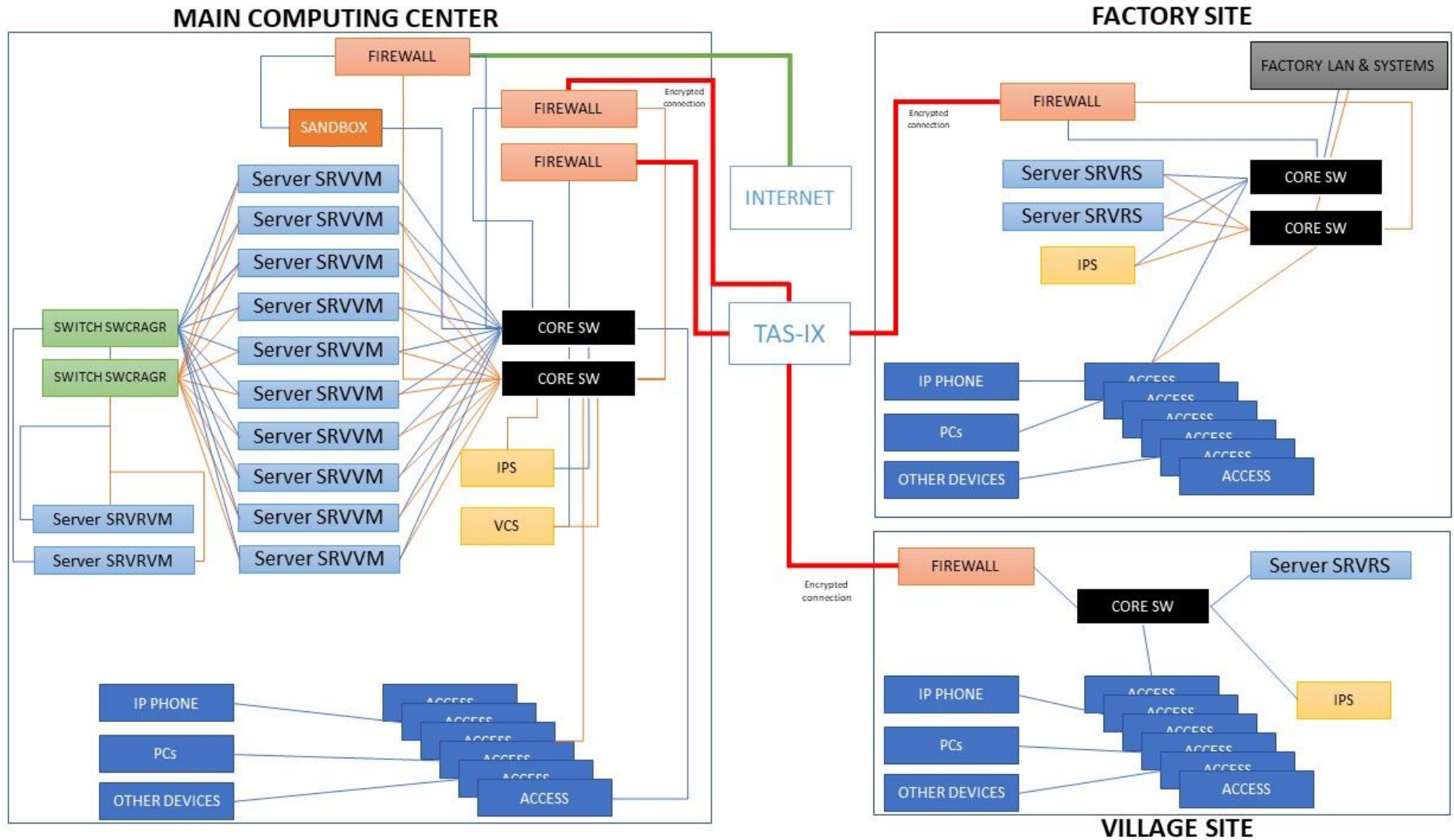
Screw supports (legs). Enclosure/rack assembly with screw supports for regulation and leveling of the floor. Screw supports should be included in the basic set of cabinets, minimum 4 pcs. for each cabinet.

Mounting and fastening products required for complete and complete assembly of the enclosure are included in the basic equipment of the enclosure.

Grounding system. The cabinet earthing system is included in the basic package.

Presence of cable glands. Cable glands in the upper and lower parts of cabinets.

| | |
|--|--|
| <p>Регулируемые вертикальные направляющие шкафа для крепления оборудования.</p> <p>Обеспечение возможности регулирования фиксации расстояния между лицевыми и тыльными вертикальными направляющими.</p> <p>Допустимая нагрузка до 600кг.</p> | <p>The walls of the cabinet are removable, with locks. Ability to access inside the cabinet for mounting and servicing from four sides.</p> <p>Adjustable vertical cabinet rails for equipment attachment.</p> <p>Providing the possibility of regulating the fixation of the distance between the face and the face with the rear vertical rails.</p> <p>Allowable load up to 600 kg.</p> |
|--|--|



НА ФИРМЕННОМ БЛАНКЕ

COMPANY BLANK

**ЦЕНОВОЕ ПРЕДЛОЖЕНИЕ
на закупку серверного оборудования для МСС**

**PRICE OFFER
for the supply of servers for MCC**

Дата: (вписать дату подачи конкурсного предложения).

КОМУ: Закупочной комиссии.

Мы, нижеподписавшиеся, заявляем, что изучили конкурсную документацию в целом и ознакомились с характером требуемых Товаров.

Проанализировав все требования, конкурсной документации и проекта контракта предлагаем следующие условия:

- **условия оплаты:** – 100% оплата по факту поставки в течение 10 дней с даты подписания Акта приемки;
- **условия поставки:** для иностранных участников: в Долларах США на условиях поставки СІР г. Ташкент, Таможенный терминал (согласно требованиям Инкотермс 2010 года); для местных участников: в национальной валюте на условиях поставки DDP г. Ташкент, ул. Фаргона йули, дом 7Б (согласно требованиям Инкотермс 2010 года);
- **сроки поставки** – не более 45 календарных дней с даты подписания Контракта. Допускается также предоставления иных дат поставки товара.

Общая сумма по Контракту с учетом доставки составляет _____ (указать общую сумму конкурсного предложения цифрами и прописью, а также валюту платежа) и указана в прилагаемой таблице цен, которая является частью настоящего конкурсного предложения. Мы согласны придерживаться положений настоящего предложения в течение 90 дней, начиная с даты, установленной как день окончания приема Конкурсных предложений. Это Конкурсное предложение будет оставаться для нас обязательным и может быть принято в любой момент до истечения указанного периода.

Дата: «__» _____ 2020г.

Ф.И.О. и подпись руководителя или уполномоченного лица
Место печати

Date: (date of submission of Bid).

TO: Procurement Commission.

We undersigned, declare that we have studied the Bid documentation generally and have become acquainted with the scope of required Goods.

Having analyzed all requirements of Bid documentation and the draft Contract, we offer the following conditions:

- **payment conditions:** - 100% payment after full delivery within 10 business days after signing of Acceptance report;
- **delivery conditions:** for foreign participants: in US dollars on terms of delivery CIP Tashkent, Customs terminal (according to the requirements of Incoterms 2010); for domestic participants: in national currency on terms of DDP delivery. Tashkent, st. Fargona yuli , house 7B (according to the requirements of Incoterms 2010);
- **delivery time** - no more than 45 calendar days from Contract date. It is also allowed to provide other dates for the delivery of goods.

The total amount under the Contract, taking into account delivery, is _____ (indicate the total Bid amount in figures and words, as well as the payment currency) and is indicated in the attached price table, which is part of this Bid.

We agree to adhere to the provisions of this proposal for 90 days, starting from the date set as the deadline for accepting Bids. This Bid will remain binding on us and may be accepted at any time before the expiration of this period.

Date: "___" _____ 2020

FULL NAME. and signature of the manager or authorized person
Print place

ТАБЛИЦА ЦЕН

PRICE TABLE

| № | Наименование Товара | Ед. изм. | Кол-во | Цена за единицу | Сумма с учетом количества. |
|----|---------------------|----------|--------|-----------------|----------------------------|
| 1. | | | | | |

| № | Description | Unit. | Q-ty | Unit price | Total |
|----|-------------|-------|------|------------|-------|
| 1. | | | | | |

Ф.И.О. и подпись руководителя или уполномоченного лица

Signature of authorized person & FULL NAME _____
seal

Место печати

Дата: «__» _____ 2020г.

Date: «__» _____ 2020г.

Приложение № 4 к Конкурсной документации

| | |
|---|---|
| <p>SALE AND PURCHASE CONTRACT № _____</p> <p>Tashkent _____/_____/2020</p> <p>“Uzbekistan GTL” Limited Liability Company (hereinafter referred to as the “Client”), represented by _____, acting on the basis of Charter, on the one part, and _____ (hereinafter referred to as the “Seller”), represented by Director _____, acting on the basis of Charter, stated as a bid winner based on Protocol of Bid Committee on the other part,</p> <p>have concluded the this Contract # _____ (hereinafter referred to as the “Contract”) as follows: Client and Seller are hereinafter referred to as a “Party” individually and as the “Parties” collectively.</p> <p>1. THE SUBJECT OF THE CONTRACT</p> <p>1.1. The Seller shall supply the Goods to the Client, as set out in the Attachment No. 1 hereto, and the Client shall accept and pay for the Goods in accordance with the terms and conditions set forth herein.</p> <p>1.2. All Goods and its components shall be brand-new and should be produced not earlier than 2020.</p> <p>1.3. Description, quantity, unit price, customs code (Code TNVED) of the Goods shall be shown in Attachment No.1 hereto.</p> <p>2. CONTRACT PRICE</p> <p>2.1. The unit price for the Goods is indicated in the Attachment No. 1 hereto. The prices for the Goods are lump sum, therefore they are not subject to any change due to increase or decreases in material pricing, wage rates or any other changes in cost items impacting the costs of the Goods.</p> | <p>КОНТРАКТ КУПИ-ПРОДАЖИ № _____</p> <p>г. Ташкент _____ . ____ . 2020</p> <p>Общество с ограниченной ответственностью «Uzbekistan GTL» (далее - «Заказчик»), в лице _____, действующего на основании Устава, с одной стороны, и _____, (далее - «Продавец»), в лице Директора _____, действующего на основании Устава, признанное победителем Конкурса на основании Протокола Конкурсной комиссии № PR _____ - _____ от ____ . ____ . 2020 г., с другой стороны, заключили настоящий Контракт № _____ (далее - «Контракт») о нижеследующем: Заказчик и Продавец здесь и далее совместно именуются «Стороны», а по отдельности «Сторона».</p> <p>1. ПРЕДМЕТ КОНТРАКТА</p> <p>1.1. Продавец осуществит поставку Покупателю Товаров, указанных в Приложении №1 к настоящему Контракту, а Заказчик обязуется принять и оплатить Товара в соответствии с условиями, изложенными в настоящем Контракте.</p> <p>1.2. Все Товара и компоненты должны быть произведены не ранее 2020 года</p> <p>1.3. Наименование, количество, цена за единицу Товара, код ТН ВЭД указаны в Приложении №1 к настоящему Контракту.</p> <p>2. ЦЕНА КОНТРАКТА</p> <p>2.1. Цена за единицу Товара указана в Приложении №1 к настоящему Контракту. Цены на Товар являются фиксированными, не будут меняться в связи с любым увеличением или снижением стоимости Товаров, ставок оплаты труда, или других изменений в стоимостных статьях, влияющих на Цену Товара.</p> |
|---|---|

2.2. The Contract Price is (*the sum in figures and words*) (*payment currency*) without Customs payments and VAT (Client in accordance with the Resolution of President of the Republic of Uzbekistan dated December 29, 2016 No. PP-2706 and the Resolution of Cabinet of Ministers of the Republic of Uzbekistan dated 06.10.2017 No.803 is exempted from Customs payments (except customs clearance fees) in accordance with the Resolution of the President of the Republic of Uzbekistan dated July 16, 2018 No. PP-3857 is exempted from VAT).

3. PAYMENT TERMS

3.1. The Contract price shall be paid in *US dollars*\sum (*indicate currency*) through the bank transfer.

3.1.1. The Client pays 100% of the cost of the Goods within 10 calendar days from the date of signing by the Parties of the Acceptance Certificate of the entire Goods under the Agreement, as well as the receipt by the Client of the appropriate invoice issued by the Seller.

3.1.2. All commissions and other banking charges relate to the performance of this Contract within the territory of the Republic of Uzbekistan shall be borne by the Client, and by the Seller outside the territory of the Republic of Uzbekistan.

3.2. The Seller shall within 10 banking days from the date of signing the Contract, transfer to the Client's account a cash amount of 5 % (five) of the Contract in the currency of payment as a Guarantee for the Contract execution ("Security Amount"). In the payment purpose Seller must indicate that the funds are transferred as a security amount under the Contract. A security amount is deemed provided upon receipt Client confirmation of bank on crediting the Security amount to the Client's settlement account. The security amount will be in the Client's current account. The Client has the right to repay from the Security Amount any claims against the Seller that the Client may have due to non-fulfillment or improper performance by the Supplier of obligations under the Agreement, as well as non-contractual obligations related to the Agreement, reversing, respectively, all or part of the Security amounts to your property. The rest of the Security amount shall be returned to the Supplier

2.2. Цена Контракта составляет [*сумму в цифрах и прописью*] [*валюта оплаты*] без таможенных платежей и НДС (Заказчик в соответствии с постановлением Президента Республики Узбекистан от 29.12.2016 г. № ПП-2706 и постановлением Кабинета Министров Республики Узбекистан от 06.10.2017 г. № 803 освобожден от уплаты таможенных платежей (за исключением сборов за таможенное оформление) в соответствии с постановлением Президента Республики Узбекистан от 16.07.2018г. № ПП-3857 освобожден от уплаты НДС).

3. УСЛОВИЯ ОПЛАТЫ

3.1. Цена Контракта должна быть оплачена в *долларах США*\суммах (*нужное указать*) путем банковского перевода. **3.1.1.** Заказчик оплачивает 100% стоимости Товара в течение 10 календарных дней со дня подписания Сторонами Акта приёма всего Товара по Договору, а также получения Покупателем соответствующего счёта-фактуры (инвойса), выставленного Продавца.

3.1.2. Все комиссии и другие банковские расходы в связи с исполнением настоящего Контракта на территории Республики Узбекистан оплачиваются Покупателем, а за пределами Республики Узбекистан оплачиваются Продавцом.

3.2. Продавец обязуется в течение 10 банковских дней с момента подписания Договора Сторонами перечислить на расчетный счет Покупателя денежную сумму в размере 5 % (пяти) от суммы Контракта в валюте платежа в качестве Гарантии исполнения Контракта («Обеспечительная сумма»). В назначении платежа Продавец должен указать, что денежные средства перечисляются как обеспечительная сумма по Договору. Обеспечительная сумма считается предоставленной после получения Покупателем подтверждения банка о зачислении Обеспечительной суммы на расчётный счёт Покупателя. Обеспечительная сумма будет находиться на расчетном счете Покупателя. Заказчик имеет право погашать из Обеспечительной суммы любые требования к Продавцу, которые Заказчик может иметь в связи с неисполнением или ненадлежащим

after 10 days after the parties have signed the Transfer Acceptance Act. The security amount does not accrue in favor of the Supplier and is not subject to payment to the Supplier of the interest provided applicable law.

4. OBLIGATIONS OF THE SELLER

4.1. Within 10 (ten) banking days from the date of conclusion of this Contract, Seller shall provide to the Client with a Guarantee of the Contract in the amount of 5 % (five) of the amount of this Contract in the form of a bank guarantee or in the form of a deposit by transferring funds to the Client's settlement account at the details specified in section 17 of this The contract.

4.2. The Seller shall deliver the Goods together with invoice, manual guidelines, warranty documents as well as certificates passport and other necessary documents.

4.3. Failure to submit the documents set out in the Clause 4.2 can lead to delay in payment to the Seller with no liability by the Client.

4.4. The Seller commits: (a) to properly ship Goods in accordance with the requirements of Client and the country of destination; (b) to make no charge for transportation of Goods, unless otherwise stated herein.

5. THE TERMS OF SUPPLY

5.1. Delivery time – according to Attachment #1.

5.2. Delivery terms: for foreign participants: in US dollars on terms of delivery CIP Tashkent, Customs terminal (according to the requirements of Incoterms 2010);

for domestic participants: in national currency on terms of DDP delivery. Tashkent, st. Fargona yuli , house 7B (according to the requirements of Incoterms 2010);

5.3. The Seller is responsible for the accuracy of execution of the documents.

6. ACCEPTANCE OF THE GOODS

исполнением Поставщиком обязательств по Договору, а также внедоговорных обязательств, связанных с Договором, обращая, соответственно, всю или часть Обеспечительной суммы в свою собственность. Остаток Обеспечительной суммы подлежит возврату Поставщику по истечении 10 дней после подписания Сторонами Акта приемки передач. На Обеспечительную сумму не начисляются в пользу Поставщика и не подлежат уплате Поставщику проценты, предусмотренные применимым правом.

4. ОБЯЗАННОСТИ ПРОДАВЦА

4.1. В течение 10 (десяти) банковских дней со дня заключения настоящего Контракта предоставить Покупателю Гарантию исполнения Контракта в размере 5% (пяти) от суммы настоящего Контракта в виде банковской гарантии или в виде задатка путем перечисления денежных средств на расчетный счет Покупателя по реквизитам, указанным в разделе 17 настоящего Контракта.

4.2. Продавец обязан поставить Товар с инвойсом, руководством по эксплуатации, гарантийными документами, а также сертификатом соответствия и прочими необходимыми документами.

4.3. Не представление документов, указанных в пункте 4.2. может отсрочить платеж на счет Продавца без какой-либо ответственности Покупателя.

4.4. Продавец обязуется: (а) надлежащим образом доставить Товара в соответствии с требованиями Покупателя, и страны назначения; (b) не требовать оплаты за доставку Товаров, если не указано обратное в настоящем Контракте.

5. УСЛОВИЯ ПОСТАВКИ

5.1. Срок поставки Товара – в соответствии с Приложением №1.

5.2. Условия Поставки: для иностранных участников: в Долларах США на условиях поставки CIP г. Ташкент, Таможенный терминал (согласно требованиям Инкотермс 2010 года); для местных участников: в национальной валюте на условиях поставки DDP г. Ташкент, ул. Фаргона йули, дом 7Б (согласно требованиям Инкотермс 2010года);

5.3. Продавец является ответственным за правильность оформления документов.

6.1. The Goods are considered as delivered by the Seller and accepted by the Client:

based on the quantity – according to the supporting documents;

based on the quality – according to the quality certificate issued by the Seller.

6.2. Acceptance of the Goods by the Client and the signing of the Acceptance report does not limit the Client's right to claim for completeness or quality of the Goods.

6.3. Goods acceptance is confirmed when Acceptance report is signed.

7. FORCE MAJEURE EVENT

7.1. Any delay or failure of either party to perform its obligations shall be excused if it is the result of an event or occurrence beyond the reasonable control of the party and without its fault or negligence, including without limitations, acts of God, actions by any government authority (whether valid or invalid), fires, floods, windstorms, explosions, riots, natural disasters, wars, sabotage; provided that written notice of such delay (including the anticipated duration of the delay) shall be issued by the affected party to the other party as soon as possible after the event or occurrence (but in any event no later than 10 days thereafter). During the period of such delay or failure to perform obligations by the Seller, the Client, at its own discretion, can purchase the Goods from other sources and reduce the volume of the Goods supplied by the Seller according to the by such quantities, without liability to Seller, or have Seller provide the Goods from other sources in quantities and at times requested by Client, and at the price set forth in this Contract. If the delay lasts more than 30 days, Client may immediately terminate this Contract without liability.

6. ПРИЕМКА ТОВАРОВ

6.1. Товар считается доставленным Продавцом и принятым Покупателем:

по количеству - в соответствии с сопроводительными документами;

по качеству – в соответствии с сертификатом качества Продавца.

6.2. Приемка Покупателем Товара и подписание Акта приёмки Товара не ограничивает право Покупателя заявлять претензии по комплектности или качеству Товара.

6.3. Приемка Товаров осуществляется путем подписания Сторонами Акта приема-передачи.

7. ФОРС-МАЖОРНЫЕ ОБСТОЯТЕЛЬСТВА

7.1. Любая задержка или невыполнение какой-либо из сторон своих обязательств должно быть оправдано, если оно является результатом какого-либо события или явления, возникшего независимо от воли сторон, не по вине или неосторожности сторон, включая, но не ограничиваясь, стихийные бедствия, действия любого государственного органа (как правомерные, так и неправоммерные), пожар, наводнение, ураган, взрывы, беспорядки, природные катастрофы, военные действия, акты саботажа, при условии, что пострадавшая сторона направит другой стороне письменное уведомление о такой задержке (включая предполагаемый период такой задержки) в максимально возможные сроки после возникновения такого события или явления (но в любом случае не позднее 10 дней после такого события или явления). В течение срока такой задержки или неисполнения Продавцом своих обязательств Заказчик, по своему усмотрению, может приобретать Товара у других продавцов, а также уменьшить объем Товаров, поставляемых Продавцом, при этом он не несет ответственность за это перед Продавцом, или поручить Продавцу приобрести и поставить Товара у других продавцов в соответствии с количеством и согласно срокам, определенных Покупателем, а также по цене, установленной настоящим Контрактом. Если обстоятельства непреодолимой силы продолжаются свыше 30 дней, то Заказчик вправе незамедлительно расторгнуть настоящий Контракт, при этом он не

7.2 The Seller shall not be held responsible for failure or delay in delivery of the entire lot or a portion of the Goods under this Contract in consequence of any Force Majeure incidents.

7.3 When, due to the change of law of the Parties, the Seller fails to deliver the Goods on time or the Client cannot take delivery of the Goods on time, the Seller shall not take any responsibility and shall not compensate any loss of the Client. The Parties shall solve the matter of delivery through negotiation in good faith.

8. WARRANTY

The Seller guarantees that the Goods set forth herein will conform to the specifications, samples, or descriptions furnished to or received by the Client, and will be merchantable, of good material and according to the quality standards and free from any defect. In addition, the Seller acknowledges that the Seller is aware of the Client's intended use and guarantees that all Goods set forth herein and has been selected, designed, manufactured or assembled by Seller are suitable and fit for use according to the particular purposes stated by the Client. The warranty period shall be 12 months from the date of delivery of the Goods.

9. LIABILITY

9.1. The Client is entitled to require from the Seller to pay a penalty in the amount of 0.5% of the cost of non-supplied Goods (zero-point five percent) for delay in delivery of the Goods for each day of delay unless the delivery is failed due to the fault of the Client. At the same time the total amount of penalty shall not exceed 40 % of total cost of the Contract. The Client can deduct the penalty amount from the payment due by the Client to Seller for the delivered Goods.

будет нести ответственность перед Продавцом в связи с этим.

7.2 Продавец не несет ответственности за собой или задержку доставки всей партии или части Товара по настоящему Контракту вследствие любых форс-мажорных обстоятельств.

7.3 Если в связи с изменением законодательства Сторон Продавец не может доставить Товар вовремя или Заказчик не может принять поставку Товара вовремя, Продавец не несет никакой ответственности и не возмещает убытки Покупателя. Стороны добросовестно решают вопрос доставки путем переговоров.

8. ГАРАНТИЯ

Продавец гарантирует, что Товара, предусмотренные настоящим Контрактом, соответствуют спецификациям, образцам и описаниям, предоставленным Покупателем или полученным Покупателем, находятся в коммерчески пригодном состоянии, изготовлены из надлежащих материалов и с учетом стандартов качества, а также не имеют никаких дефектов. Более того, Продавец признает, что знает о назначении использования Товара Покупателем, и гарантирует, что все Товара, предусмотренные настоящим Контрактом, которые были отобраны, сконструированы, изготовлены или собраны Продавцом в соответствии с назначением использования, указанным Покупателем, подходят и пригодны для использования в конкретных целях, определенных Покупателем. Гарантийный период составляет 12 месяцев с даты поставки Товаров.

9. ОТВЕТСТВЕННОСТЬ

9.1. За любую просроченную поставку всех Товаров или части Товаров, Заказчик вправе потребовать от Продавца оплатить пеню в размере 0,5% (ноль целых пять десятых процентов) от суммы не поставленного Товара за каждый день просрочки, за исключением случаев, когда поставка просрочена по вине Покупателя. При этом общая сумма пени не должна превышать 40 % общей стоимости Контракта. Заказчик может удержать сумму неустойки из платежа, подлежащего к оплате со

9.2. The Seller shall respond in respect of the claim relate to the Contract, if any, in writing and no later than 5 (five) working days from the day of receiving a claim notice, unless earlier response is required due to production needs. If the Seller fails to respond on the claim in such a period from the date of receiving the claim, it shall be deemed that the Seller agrees to satisfy the claim of the Client in full.

9.3. If the Seller does not submit the documents stated herein or submits the documents executed improperly, the Seller shall bear the full responsibility for the expenses appeared in result of such execution, including without limitations, the expenses for Goods storage in temporary warehouses, and damage inflicted to the Goods in this connection.

10. LIMITATION OF LIABILITY

10.1 Notwithstanding any contrary provision hereof, either Party shall be liable against the counterpart for any indirect or other consequential loss, including without limitations:

- a) production loss, inability to produce, process, use, accept the delivery, transport or supply, or delay or interruption in production, processing, use, acceptance of delivery;
- b) any failure to perform, loss, damage, direct or indirect costs or expenses resulted from any of the foregoing including without limitations any loss or damage incurred, or liquidated or pre-estimated damages or sums of any kind whatsoever borne or payable under any Contract;
- c) any loss or anticipated loss of profit, any loss or anticipated loss of, or delay in revenue or income, non-execution or expected non-execution of any Contract,

стороны Покупателя Продавцу за поставленные Товара.

9.2. Продавец должен ответить на претензию, касающуюся Контракта, при наличии таковой, в письменной форме и не позднее 5 (пяти) рабочих дней со дня получения уведомления о претензии, если только более ранний ответ не требуется в связи с производственной необходимостью. Если Продавец не отвечает на претензию в такой срок с момента получения претензии, то Продавец считается давшим согласие удовлетворить претензию Покупателя в полном объеме.

9.3 Если Продавец не предоставляет документы, указанные в настоящем Контракте, или предоставляет неправильно оформленные документы, то затраты, возникающие, в связи с этим, включая, но не ограничиваясь, расходами по хранению Товаров на складе временного хранения, причиненный, в связи с этим вред Товару, в полном объеме будет нести Продавец.

10. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

10.1 Несмотря на что-либо прямо противоположное, ни одна из Сторон не несет ответственности перед другой Стороной за любые косвенные или иные сопутствующие убытки, которые помимо прочего включают:

- a) производственные потери, неспособность добывать, перерабатывать, использовать, принять поставку, транспортировать или поставлять, или задержку или перерыв в добыче, переработке, использовании, поставке;
- b) любое неисполнение, убыток, ущерб, издержки или расходы, прямо или косвенно вызванные любым из вышеперечисленных, в том числе, помимо прочего, любые причиненные потери или ущерб, или оцененные или заранее оцененные убытки или суммы любого рода, понесенные или причитающиеся согласно любому контракту;
- c) любая потеря или ожидаемая потеря прибыли, любая потеря или предполагаемая потеря, отсрочка или предполагаемая отсрочка дохода или выручки, незаключение или предполагаемое

failure to receive the Contract or other business opportunity; and

d) any loss or anticipated loss, damage, costs or expenses appeared as a result of any actions, claims, suit demands or court judgment followed or appeared from any action of the foregoing, howsoever arising, whether under Contract, tort (including negligence), and/or breach of duty (statutory or otherwise).

11. CONFIDENTIALITY AND DATA PROTECTION

11.1. For the purposes of this Contract, the confidential information is any information which, includes:

- content and the terms and conditions of the transaction hereunder and any negotiations or discussions relate to this Contract;
- all internal information, in whatever format and irrespective of the medium in which it is contained, acquired or produced by the Client in connection with the Goods, including without limitations, work schedules, security measures, identities and contact details of the employees, plans, budgets, agreements, drawings, reports, specifications, estimations and documents acquired or produced by or in connection with the Goods;

- other internal technical, proprietary or other business and operational information relate to the Parties, whether such information is labelled or not, or identified otherwise as private, proprietary or confidential; and

- any internal information which has been identified by the owner thereof as confidential, and transferred by either Parties to the counterpart in the course of the Contract implementation. This section shall not apply to information which:

незаключение какого-либо контракта, неполучение контракта или другие упущенные коммерческие возможности; и

d) любые убытки или ожидаемые потери, ущерб, затраты или расходы, возникающие в результате каких-либо действий, претензий, исков, исковые требования и решений суда, явившиеся следствием или возникшие из действия любого из вышеперечисленных, независимо от того, какая ответственность –по контракту, по иску из гражданского правонарушения (включая халатность), и/или из-за нарушения служебных обязанностей (по закону или иным образом).

11 КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ДАННЫХ

11.1. Под Конфиденциальной информацией для целей настоящего Контракта понимается любая информация, включающая:

- содержание и условия сделки, упомянутой в рамках настоящего Контракта, и любые переговоры или обсуждения, связанные с данным Контрактом;
- вся внутренняя информация, в любом формате и вне зависимости от носителя информации, в котором она содержится, получена или произведена Покупателем в связи с Товарами, включая без ограничения, график работы, системы охраны, личности и контактные данные работников, планы, бюджеты, соглашения, чертежи, отчеты, спецификации, расчеты, и документы, полученные или произведенные в связи с Товаром;

- другая внутренняя техническая, конфиденциальная, служебная или прочая деловая и операционная информация, имеющая отношение к Сторонам, вне зависимости от того, помечена ли такая информация или иным способом обозначена как частная, служебная или конфиденциальная, или нет; и

- любая внутренняя информация, которая была определена ее обладателем как конфиденциальная, передаваемая любой из Сторон другой Стороне в процессе реализации настоящего Контракта. Этот раздел не применяется к информации, которая:

- является общедоступной;

- is generally available to the public;
- is available or becomes available to either Party on a non-confidential basis from a source other than the other Party,
- is disclosed by the Party to a third party without restriction;
- is developed by either Party without application of any information furnished by the other Party, or of any information furnished on a confidential basis;
- is disclosed pursuant to the requirements of the Uzbek law and the law of the Seller's country.

Confidential information can be contained in the letters, reports, analytical materials, results of surveys, schemes, charts, specifications and other documents, both in material and electronic forms.

11.2. Unless otherwise specified by the Uzbek law or the law of Seller's country, the Parties shall:

- not share, discuss the content, provide copies, publish or disclose Confidential information in any other form to third parties without the prior written consent of the other Party. The written consent is not required in the instances of disclosure to the state authorities authorized to request such information under the Uzbek law on the basis of the duly executed request to provide such information, and to judicial bodies and representatives of the relevant Party for the purpose of defending and exercising rights under the Contract (in all abovementioned cases – without notifying the other Party);
- take all measures and use all legal means for protecting Confidential information and avoiding its unauthorized disclosure;

- известна или становится известной одной Стороне на не конфиденциальной основе от иного источника, нежели другая Сторона;
- раскрывается Стороной третьим лицам без ограничения;
- разработана одной Стороной без использования сведений, предоставленных другой Стороной, или сведений, носящих конфиденциальный характер;
- раскрываются в соответствии с требованиями законодательства Республики Узбекистан или законодательства страны Продавца. Конфиденциальная информация может содержаться в письмах, отчетах, аналитических материалах, результатах исследований, схемах, графиках, спецификациях и других документах, оформленных как на бумажных, так и на электронных носителях.

11.2. Стороны обязуются, если иное не предусмотрено законодательством Республики Узбекистан или законодательством страны Продавца:

- не разглашать, не обсуждать содержание, не предоставлять копий, не публиковать и не раскрывать в какой-либо иной форме третьим лицам Конфиденциальную информацию без получения предварительного письменного согласия другой Стороны. При этом получение письменного согласия не требуется в случаях раскрытия информации государственным органам, уполномоченным запрашивать такую информацию в соответствии с законодательством Республики Узбекистан, на основании должным образом оформленного запроса на предоставление указанной информации, а также судебным органам и представителям соответствующей Стороны для целей защиты и реализации прав по настоящему Контракту (во всех указанных случаях – без уведомления другой Стороны);
- предпринимать все меры и использовать все законные средства для защиты Конфиденциальной информации и предотвращения ее несанкционированного раскрытия;
- использовать Конфиденциальную информацию только в целях исполнения обязательств по настоящему Контракту;

- use Confidential information only for the purposes of the Contract implementation;
- not disclose to third parties the fact of the transfer or obtaining of Confidential information.

11.3. The confidentiality obligations shall last for a period of 10 (ten) years from the date of signing of this Contract.

12. INDEMNIFICATION

12.1 If the Seller damages the property of the Client or third parties upon delivery of the Goods, the Seller shall indemnify and hold Client harmless from and against any liability, claims, demands or expenses (including attorney's and other professional fees) for damages to the property or injuries (including death) to the Client, its employees or any other person arising from or in connection with Seller's performance of work or use of the Client's property, except for such liability, claim, or demand arising out of the sole negligence of Client.

13. NON-ASSIGNMENT

13.1 Parties are not entitled to assign or delegate its rights or obligations hereunder without Client's prior written consent.

14. TERMINATION

14.1 Client reserves the right to terminate all or any part of this Contract, (and the Client has no any liability against Seller in this situation), if the Seller: (a) repudiates or breaches any term of this Contract, including Seller's warranties; (b) fails to perform Goodss or deliver the Goods as specified by the Client; (c) is incapable to provide all Goodss in appropriate or in time maner and fails to remedy such non-performance or breach within 10 days (or shorter period of time if commercially reasonable under the circumstances) after receipt of written notice from Client specifying such failure or breach.

- не разглашать третьим лицам факта передачи или получения Конфиденциальной информации.

11.3. Обязательства по неразглашению Конфиденциальной информации действуют в течение 10 (десять) лет с даты подписания настоящего Контракта.

12. ВОЗМЕЩЕНИЕ УЩЕРБА

12.1 Если Продавец при доставке Товара наносит вред имуществу Покупателя или третьих лиц, то Продавец гарантирует Покупателю возмещение ущерба и освобождает Покупателя от какой-либо ответственности в отношении любых обязательств, исков, требований или расходов (включая расходы на адвоката (юристов) и иные расходы на оплату Товаров специалистов), возникающих в связи с нанесением вреда имуществу или причинением телесных повреждений (включая смерть) Покупателю, его работнику или любому другому лицу в процессе или в связи с осуществлением Продавцом работ или использованием имущества Покупателя, за исключением таких обязательств, исков или требований, которые возникли исключительно вследствие неосторожности Покупателя.

13. ОГРАНИЧЕНИЯ ПО ПЕРЕУСТУПКЕ ПРАВ

13.1 Стороны не вправе переуступить или передавать свои права и обязательства по настоящему Контракту без предварительного письменного согласия Покупателя.

14. РАСТОРЖЕНИЕ КОНТРАКТА

14.1 Заказчик сохраняет за собой право расторгнуть настоящий Контракт полностью или в части (причем за это он не несет ответственности перед Продавцом), если Продавец: (a) откажется выполнять или нарушит любое условие Контракта, включая гарантии Продавца; (b) окажется не в состоянии оказывать Товара или предоставить Товара, указанные Покупателем; (c) окажется не в состоянии надлежащим образом обеспечивать своевременное и полное предоставление Товаров, и не устранил такое невыполнение или нарушение в течение 10 дней (или в более короткий срок, коммерчески оправданный в сложившихся

15. DISPUTE RESOLUTION, GOVERNING LAW AND LANGUAGE

15.1. Validity and interpretation of this Contract and the legal relations of the Parties hereto shall be governed by and construed in accordance with the law of the Republic of Uzbekistan.

15.2. All documents, correspondence and communications between the Client and the Seller in connection with this Contract shall be written in the English or Russian languages.

15.3. Parties shall take measures to settle disputes, claims or disagreements arising out of issues envisaged by or in the connection with this Contract through negotiations amicably and in good faith. If the Parties cannot reach an agreement within 30 (thirty) calendar days from the date of the failure of negotiations, this dispute shall be referred to Tashkent local economic Court.

16. MISCELLANEOUS

16.1. This Contract shall become effective on the date of its signing and registration by the authorized bodies of the Republic of Uzbekistan and valid until full fulfillment of the obligations by the Parties.

16.2. This Contract and its attachments, exhibits, supplements or other conditions of the Client expressly specified herein shall constitute the entire agreement between Seller and Client with respect to the matters contained in this Contract and supersedes all prior verbal or written representations and agreements between the Parties.

16.3. The Parties acknowledge and agree that any change of terms and conditions of the Contract shall require respective amendment or additional agreement. All attachments, amendments and supplemental

обстоятельствах) после получения письменного уведомления от Покупателя с указанием конкретного неисполненного обязательства или нарушения.

15. РАЗРЕШЕНИЕ СПОРОВ, ПРИМЕНИМОЕ ПРАВО И ЯЗЫК

15.1. Действительность и толкование настоящего Контракта и правоотношения Сторон будут регулироваться и толковаться в соответствии с законодательством Республики Узбекистан.

15.2. Все документы, переписка и сообщения между Покупателем и Продавцом в связи с настоящим Контрактом, должны составляться на английском или на русском языках.

15.3. В случае возникновения споров, претензий или разногласий по вопросам, предусмотренным настоящим Контрактом или в связи с ним, Стороны примут все меры к разрешению их путем переговоров. Если стороны не могут прийти к согласию в течение 30 (тридцати) календарных дней со дня прекращения переговоров, то данное разногласие должно быть урегулировано в Ташкентским межрайонном экономическом суде.

16. ПРОЧИЕ ПОЛОЖЕНИЯ

16.1. Настоящий Контракт вступает в силу с момента подписания и регистрации его в уполномоченных органах Республики Узбекистан и действует до полного выполнения Сторонами своих обязательств.

16.2. Настоящий Контракт, включая все приложения, спецификации, дополнения и прочие условия Покупателя, специально оговоренные в настоящем Контракте, составляют полное соглашение, достигнутое между Продавцом и Покупателем по вопросам, затронутым в настоящем Контракте, и заменяют все предварительные устные или письменные заявления и договоренности сторон.

16.3. Стороны признают и соглашаются, что любое изменение условий Контракта требует соответствующей поправки или дополнительного соглашения. Все приложения, поправки и

agreements hereto shall be valid if they are made in writing, duly signed and stamped by the authorized representatives of both Parties and registered by the authorized bodies of the Republic of Uzbekistan.

16.4. This Contract is made in two copies in Russian and English of equal legal force. In case of contradiction between the versions in English and Russian, the Russian version shall prevail.

17. THE LEGAL ADDRESSES AND BANK DETAILS OF THE PARTIES

**CLIENT:
UZBEKISTAN GTL LLC**

Address: 7-b, Fargona yuli str.,
Tashkent, Republic of Uzbekistan/
Bank Name: ASAKA BANK
Currency Bank account: 20214840604819680001
Bank Code: 00873
Tax ID: 207041936
SWIFT Code: ASBKUZ22

_____ **Client**

SELLER:
[to insert name of legal entity]
[to include the address].

Bank Details:
TAX ID :
Bank Name:
Bank Code:
Bank account:
SWIFT code:

_____ **Seller**

дополнительные соглашения к настоящему Контракту имеют силу только, если они оформлены в письменном виде, подписаны и скреплены печатью надлежащим образом уполномоченными представителями обеих Сторон и зарегистрированы в уполномоченных органах Республики Узбекистан.

16.4. Настоящий Контракт составлен в двух экземплярах на английском и русском языках, каждый из которых имеет одинаковую силу. В случае возникновения разногласий между версиями Контракта на английском и русском языках, версия Контракта на русском языке имеет преимущественную силу.

17. ЮРИДИЧЕСКИЕ АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН:

**ЗАКАЗЧИК:
ООО «UZBEKISTAN GTL»**

Адрес: Республика Узбекистан, г. Ташкент,
ул. Фаргона йули, д. 7-б
Наименование Банка: АСАКА БАНК
Валютный банковский счет:
20214840604819680001
Код Банка: 00873
ИНН: 207041936
Код SWIFT: ASBKUZ22

_____ **Заказчик**

ПРОДАВЕЦ:
[включить наименование юридического лица],
[включить адрес].

Банковские реквизиты:
TAX ID :
Банк:
Bank Code:
Банковский счет:
SWIFT код:

_____ **Продавец**

**Attachment #1 to the Contract_____ /
Приложение №1 к контракту на поставку
№_____ от _____**

| № | Goods description \ Наименование | Unit / Ед. изм. | Q-ty / Кол-во | Unit price / Стоимость за ед. | Total price \ Общая стоимость |
|----|--|--------------------|------------------|-------------------------------------|-------------------------------------|
| 1 | Server SRVVM / Сервер SRVVM в комплекте: | Set/К-т. | 10 | | |
| 2 | Server SRVRVM /Сервера SRVRVM в комплекте: | Set/К-т. | 2 | | |
| 3 | Server SRVRS /Сервера SRVRS в комплекте: | Set/К-т. | 3 | | |
| 4 | Virtualization system DCVRTM / Система виртуализации DCVRTM состоящая из: | Set/К-т. | 1 | | |
| 5 | Switch SWCRAG / Коммутатор SWCRAG | Each/Шт. | 6 | | |
| 6 | Switch SWAG / Коммутатор SWAG | Each/Шт. | 1 | | |
| 7 | Switch MGMT / Коммутатор MGMT | Each/Шт. | 2 | | |
| 8 | Switch access SWACS24/ Коммутатор доступа SWACS24 | Each/Шт. | 16 | | |
| 9 | Switch access SWACS48/ Коммутатор доступа SWACS48 | Each/Шт. | 6 | | |
| 10 | Accessories SWACSKIT / Аксессуары SWACSKIT в составе: | Set/К-т. | 1 | | |
| | Small Form Factor Pluggable 10 GE, SFP+, SR | Each/Шт. | 132 (+5%) | | |
| | SFP 1000Base-SX GE, LC, 850nm for up to 550m, Transmission on MMF | Each/Шт. | 60 (+5%) | | |
| | Small Form Factor Pluggable 10 GE, SFP+, дистанция не менее 2 км | Each/Шт. | 8 (+5%) | | |
| | QSFP+ DAC cable, 1m | Each/Шт. | 10 (+5%) | | |
| | SFP 1000BASE-T GE module | Each/Шт. | 6 (+5%) | | |
| 11 | Monitoring & Management system / Система управления и мониторинга SWMGMT в комплекте: | Set/К-т. | 1 | | |
| 12 | Firewall / Файрвол FWMCC | Each/Шт. | 2 | | |
| 13 | Firewall /Файрвол FWRS | Each/Шт. | 2 | | |
| 14 | Firewall /Файрвол FWUP | Each/Шт. | 1 | | |
| 15 | SandBox / Песочница SNDBX | Set/К-т. | 1 | | |
| 16 | Управление безопасностью SECMGMT в комплекте: | Each/Шт. | 1 | | |
| 17 | Шкаф телекоммуникационный RCKRS в комплекте: | Set/К-т. | 2 | | |
| | Total contract price / Общая стоимость Контракта: | | | | |

| | |
|--|--|
| | Delivery point / Пункт назначения: |
| | Delivery period / Дата 45 calendar days from Contract date / 45 календарных дней с даты подписания Договора. Допускается также поставки Товара: предоставления иных дат поставки товара/ It is also allowed to provide other dates for the delivery of goods. |
| | List of shipping documentation / Перечень Товаросопроводительной документации: |
| | 1) Invoice / Счет-фактура и Акт приема передачи товара – 2 оригинал и 2 копии; 2) Waybill / Транспортная накладная и/или расходная накладная – 1 оригинал и 2 копии; 3) Packing list / Упаковочный лист – 1 оригинал и 2 копии; 4) Certificate of Conformity / Сертификат соответствия Товара – 1 копия; 5) Manual for the Goods/ Паспорт на Товар; |

Signatures/ Подписи Сторон

Client / От Покупателя:

Подпись _____

Name / Ф.И.О.

М.П. Генеральный директор

Seller / От Продавца:

Подпись _____

Name / Ф.И.О.

М.П. Position / Должность