e-mail: info@uzairways.com
tel: +998 (78) 140-46-23
fax: +998 (71) 236-75-00

www.uzairways.com

UZBEKISTAN airways

Aksiyadorlik jamiyati *Joint-Stock Company*

У Т В Е Р Ж Д А Ю
Первый заместитель
Председателя правления
АО «Uzbekistan Airways»

_____ Xusanov U.A.
«__» _____ 2022г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

по расширению существующей сетевой инфраструктуры АО «Uzbekistan Airways», развёрнутой на базе межсетевого экрана Fortinet.

Общие требования к организационной технике

Требования к техническим характеристикам межсетевого экрана указаны в настоящей документации. Технические параметры всего предложенного оборудования должны строго соответствовать или превосходить параметры, указанные в данной документации. Межсетевые экраны должны иметь на корпусе лейбл производителя. Кабеля питания также должны быть совместимы без использования переходников с разъёмами розеток страны Заказчика (Республика Узбекистан). Все поставляемое оборудование должно быть новым и не бывшим в употреблении, а также не снятым с производства. Все компоненты поставляемого оборудования должны быть оригинальными, иметь все необходимые ярлыки, бирки, стикеры и т.д., для осуществления возможности проверки подлинности и другой информации от изготовителя. Гарантия на поставляемый товар должна составлять не менее 36 месяцев. Оборудования должно полностью с интегрировано с существующими в АО межсетевыми экранами на базе Fortinet.

Параметр	Минимальные требования
Тип оборудования	**Межсетевой экран конфигурации №1**
Кол-во (шт)	6 комплектов
модель	Участник торгов должен указать модель предложенной оборудования.
Сборка	Оборудование должно быть собрано (в сборку включаются все компоненты, оговоренные техническим заданием) и протестировано на заводах фирмы изготовителя.
Технические требования к межсетевому экранированию	1. Firewall Throughput (1518/512/64 byte UDP): не менее 10/10/7 Gbps; 2. Одновременное количество сессий: не менее 1.5 Млн; 3. Скорость установки новых соединений: не менее 45 000 в сек; 4. IPS Throughput Enterprise Mix: не менее 1.4 Gbps; 5. Application Control Throughput (HTTP 64K): не менее 1.8 Gbps; 6. Threat Protection Throughput Enterprise Mix: не менее 0.8 Gbps; 7. SSL Inspection Throughput: не менее 0.7 Gbps; 8. Количество виртуальных контекстов безопасности: не менее 10; 9. Количество интерфейсов: не менее 6 x GE RJ45, 2 x GE RJ45 or SFP Shared Ports. 10. Количество USB портов: не менее 1; 11. Жесткий диск SSD 128Гбайт: не менее 1;
Функциональные требования к межсетевому экранированию	1. лицензирование системы должно осуществляться для неограниченного количества пользователей; 2. система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; 3. система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: 3.1.с холодным резервом (active/passive); 3.2.с горячим резервом (active/active); 3.3.кластер балансировки; 4. система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений; 5. система должна иметь функциональность балансировки нагрузки; 6. система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); 7. система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); 8. система должна обеспечивать анализ SSH трафика (ssh inspection); 9. система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; 10. система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента); 11. система должна обеспечивать оптимизацию WAN соединений; 12. система должна иметь функционал защиты от утечек данных DLP; 13. система должна обеспечивать антивирусную защиту с аппаратным ускорением; 14. система должна обеспечивать защиту от спама (антиспам); 15. система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением; 16. система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов;

	17. принудительное включение режима безопасного поиска в популярных поисковых системах; 18. система должна иметь функциональность контроля приложений; 19. система должна иметь функциональность WEB proxy; 20. система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию; 21. система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика; 22. система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; 23. система должна иметь возможность помещать инфицированные сообщения в карантин; 24. система должна иметь возможность блокировки передачи файлов в зависимости от размера; 25. система должна иметь возможность блокировки передачи файлов в зависимости от типа; 26. система должна поддерживать соединения множества WAN сетей; 27. система должна поддерживать протокол PPPoE и L2TP; 28. система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”; 29. система должна поддерживать маршрутизацию на основе политик; 30. система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP; 31. система должна поддерживать использование зон безопасности; 32. система должна поддерживать маршрутизацию между зонами; 33. система должна поддерживать маршрутизацию между виртуальными сетями; 34. система должна поддерживать администрирование на основе ролей; 35. система должна поддерживать несколько уровней администраторов и пользователей; 36. система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс; 37. система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО; 38. система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; 39. система должна поддерживать Kerberos аутентификацию пользователей; 40. система должна поддерживать аутентификацию пользователей посредством Windows Active Directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей; 41. система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; 42. система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; 43. система должна поддерживать аутентификацию на основе групп пользователей; 44. система должна поддерживать функции NAT, PAT, «прозрачный» (мост); 45. система должна поддерживать функции NAT на основе политик; 46. система должна поддерживать функции VLAN Tagging (802.1Q); 47. система должна поддерживать функции SIP/H.323 NAT Traversal;

	48. система должна поддерживать настройку профилей безопасности; 49. система должна иметь возможность блокировки по URL/ключевому слову/фразе; 50. система должна поддерживать «Белые» списки URL; 51. система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; 52. система должна уметь предотвращать не менее 4000 типов сетевых атак; 53. система должна иметь возможность настройки списка сигнатур атак; 54. система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; 55. система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; 56. система должна поддерживать проверку заголовков MIME; 57. система должна поддерживать фильтрацию электронной почты, по ключевым словам, и фразам; 58. система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; 59. система должна иметь возможность отсылки логов на удаленный syslog сервер; 60. система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; 61. система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; 62. система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках; 63. система должна поддерживать протокол VRRP; 64. система должна поддерживать интеграцию с IBM QRadar SIEM; 65. система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; 66. система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; 67. система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; 68. система должна поддерживать управление через Web интерфейс; 69. система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; 70. система должна поддерживать протоколы NetFlow, sFlow; 71. система должна обеспечивать режим обратного прокси-сервера (reverse proxy); 72. система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); 73. система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; 74. система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях; 75. система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике

	безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа; 76. система должна обеспечивать возможность управления беспроводными точками доступа; 77. система должна обеспечивать возможность управления коммутаторами;
Требование к обслуживанию и гарантии	система должна обеспечиваться расширенной технической поддержкой от производителя в режиме 24x7 не менее 3 лет;
Комплектация	заводское крепление для монтажа в серверный шкаф типа RACK 19-дюймов. Power cord cable c13-c14

Параметр	**Минимальные требования**
Тип оборудования	**Межсетевой экран конфигурации №2**
Кол-во (шт)	5 комплектов
модель	Участник торгов должен указать модель предложенной оборудования.
Сборка	Оборудование должно быть собрано (в сборку включаются все компоненты, оговоренные техническим заданием) и протестировано на заводах фирмы изготовителя.
Технические требования к межсетевому экранированию	1. Firewall Throughput (1518/512/64 byte UDP): не менее 20/18/10 Gbps; 2. Одновременное количество сессий: не менее 1.5 Млн; 3. Скорость установки новых соединений: не менее 56 000 в сек; 4. IPS Throughput Enterprise Mix: не менее 2.6 Gbps; 5. Application Control Throughput (HTTP 64K): не менее 2.2 Gbps; 6. Threat Protection Throughput Enterprise Mix: не менее 1 Gbps; 7. SSL Inspection Throughput: не менее 1 Gbps; 8. Количество виртуальных контекстов безопасности: не менее 10; 9. Количество интерфейсов: не менее 2 x GE RJ45 DMZ ports, 2 x GE RJ45 WAN ports, 2 x GE RJ45 HA ports, 12 x GE RJ45 ports, 2 x 10G SFP+, 4 x GE SFP, 16 x GE RJ45, 4 x GE RJ45 or SFP Shared Ports. 10. Количество USB портов: не менее 1; 11. Жесткий диск SSD 480Гбайт: не менее 1; 12. Блок питания: 100–240VAC,50–60 Hz; не менее 2 на один комплект 13. В каждый комплект поставки должны присутствовать совместимые оптические трансиверы в количестве: 13.1.10GE SFP+ MM – 1 штук 13.2.10GE SFP+ SM – 1 штук 13.3.GE SFP MM – 2 штук 13.4.GE SFP SM – 2 штук
Функциональные требования к межсетевому экранированию	1. лицензирование системы должно осуществляться для неограниченного количества пользователей; 2. система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; 3. система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: 3.1.с холодным резервом (active/passive); 3.2.с горячим резервом (active/active); 3.3.кластер балансировки; 4. система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений;

	5. система должна иметь функциональность балансировки нагрузки; 6. система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); 7. система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); 8. система должна обеспечивать анализ SSH трафика (ssh inspection); 9. система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; 10. система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента); 11. система должна обеспечивать оптимизацию WAN соединений; 12. система должна иметь функционал защиты от утечек данных DLP; 13. система должна обеспечивать антивирусную защиту с аппаратным ускорением; 14. система должна обеспечивать защиту от спама (антиспам); 15. система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением; 16. система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; 17. принудительное включение режима безопасного поиска в популярных поисковых системах; 18. система должна иметь функциональность контроля приложений; 19. система должна иметь функциональность WEB proxy; 20. система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию; 21. система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика; 22. система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; 23. система должна иметь возможность помещать инфицированные сообщения в карантин; 24. система должна иметь возможность блокировки передачи файлов в зависимости от размера; 25. система должна иметь возможность блокировки передачи файлов в зависимости от типа; 26. система должна поддерживать соединения множества WAN сетей; 27. система должна поддерживать протокол PPPoE и L2TP; 28. система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”; 29. система должна поддерживать маршрутизацию на основе политик; 30. система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP; 31. система должна поддерживать использование зон безопасности; 32. система должна поддерживать маршрутизацию между зонами; 33. система должна поддерживать маршрутизацию между виртуальными сетями; 34. система должна поддерживать администрирование на основе ролей; 35. система должна поддерживать несколько уровней администраторов и пользователей; 36. система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс;

	37. система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО; 38. система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; 39. система должна поддерживать Kerberos аутентификацию пользователей; 40. система должна поддерживать аутентификацию пользователей посредством Windows Active Directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей; 41. система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; 42. система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; 43. система должна поддерживать аутентификацию на основе групп пользователей; 44. система должна поддерживать функции NAT, PAT, «прозрачный» (мост); 45. система должна поддерживать функции NAT на основе политик; 46. система должна поддерживать функции VLAN Tagging (802.1Q); 47. система должна поддерживать функции SIP/H.323 NAT Traversal; 48. система должна поддерживать настройку профилей безопасности; 49. система должна иметь возможность блокировки по URL/ключевому слову/фразе; 50. система должна поддерживать «Белые» списки URL; 51. система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; 52. система должна уметь предотвращать не менее 4000 типов сетевых атак; 53. система должна иметь возможность настройки списка сигнатур атак; 54. система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; 55. система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; 56. система должна поддерживать проверку заголовков MIME; 57. система должна поддерживать фильтрацию электронной почты по ключевым словам и фразам; 58. система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; 59. система должна иметь возможность отсылки логов на удаленный syslog сервер; 60. система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; 61. система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; 62. система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках; 63. система должна поддерживать протокол VRRP; 64. система должна поддерживать интеграцию с IBM QRadar SIEM; 65. система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности;

	66. система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; 67. система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; 68. система должна поддерживать управление через Web интерфейс; 69. система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; 70. система должна поддерживать протоколы NetFlow, sFlow; 71. система должна обеспечивать режим обратного прокси-сервера (reverse proxy); 72. система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); 73. система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; 74. система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях; 75. система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа; 76. система должна обеспечивать возможность управления беспроводными точками доступа; 77. система должна обеспечивать возможность управления коммутаторами;
Требование к обслуживанию и гарантии	система должна обеспечиваться расширенной технической поддержкой от производителя в режиме 24x7 не менее 3 лет

Параметр	**Минимальные требования**
Тип оборудования	**Межсетевой экран конфигурации №3**
Кол-во (шт)	2 комплекта
модель	Участник торгов должен указать модель предложенной оборудования.
Сборка	Оборудование должно быть собрано (в сборку включаются все компоненты, оговоренные техническим заданием) и протестировано на заводах фирмы изготовителя.
Технические требования к межсетевому экранированию	1. Система должна иметь возможность объединения шлюзов безопасности в единый отказоустойчивый кластер; 2. Firewall Throughput IPv4 (1518/512/64 byte UDP): 195/190/140 Gbps; 3. Firewall Throughput (Packet per Second): 200 Mpps; 4. IPS Throughput: 16 Gbps; 5. Одновременное количество сессий: 12 Млн; 6. Скорость установки соединений: 730 000 в сек; 7. IPsec VPN пропускная способность: 50 Gbps; 8. Application Control Throughput (HTTP 64K): 32 Gbps; 9. SSL Inspection Throughput: 12 Gbps; 10. Количество виртуальных контекстов безопасности: 10 (с возможностью расширения до 250);

	11. Количество интерфейсов: не менее 4x 40GE QSFP+, 12x 25 GE SFP28 /10 GE SFP+, 8x GE SFP, 12x GE RJ45. 12. Количество USB 3.0 портов: не менее 1; 13. Жесткий диск SSD 1 Тбайт: не менее 2; 14. Блок питания 115–230V AC, 50–60 Hz: не менее 2; 15. В каждый комплект поставки должны присутствовать совместимые оптические трансиверы в количестве: 15.1.10GE SFP+ MM – 10 штук 15.2.10GE SFP+ SM – 2 штук 15.3.GE SFP MM – 4 штук 15.4.GE SFP SM – 4 штук
Функциональные требования к межсетевому экранированию	1. лицензирование системы должно осуществляться для неограниченного количества пользователей; 2. система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; 3. система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: 3.1.с холодным резервом (active/passive); 3.2.с горячим резервом (active/active); 3.3.кластер балансировки; 4. система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений; 5. система должна иметь функциональность балансировки нагрузки; 6. система должна поддерживать технологию интеллектуального управления трафиком SD-WAN (Software-Defined Wide Area Network, программно-конфигурируемая сеть); 7. система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); 8. система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); 9. система должна обеспечивать возможность реализации концепции ZTNA (Zero Trust Network Access); 10. система должна обеспечивать анализ SSH трафика (ssh inspection); 11. система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; 12. система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента); 13. система должна обеспечивать оптимизацию WAN соединений; 14. система должна иметь функционал защиты от утечек данных DLP; 15. система должна обеспечивать антивирусную защиту с аппаратным ускорением; 16. система должна обеспечивать защиту от спама (антиспам); 17. система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением; 18. система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; 19. должна обеспечиваться WEB фильтрация трафика по не менее 85 категориям;

	20. принудительное включение режима безопасного поиска в популярных поисковых системах; 21. система должна иметь функциональность контроля приложений; 22. система должна иметь функциональность WEB proxy; 23. система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию; 24. система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика; 25. система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; 26. система должна иметь возможность помещать инфицированные сообщения в карантин; 27. система должна иметь возможность блокировки передачи файлов в зависимости от размера; 28. система должна иметь возможность блокировки передачи файлов в зависимости от типа; 29. система должна поддерживать соединения множества WAN сетей; 30. система должна поддерживать протокол PPPoE и L2TP; 31. система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”; 32. система должна поддерживать маршрутизацию на основе политик; 33. система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP; 34. система должна поддерживать использование зон безопасности; 35. система должна поддерживать маршрутизацию между зонами; 36. система должна поддерживать маршрутизацию между виртуальными сетями; 37. система должна поддерживать администрирование на основе ролей; 38. система должна поддерживать несколько уровней администраторов и пользователей; 39. система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс; 40. система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО; 41. система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; 42. система должна поддерживать Kerberos аутентификацию пользователей; 43. система должна поддерживать аутентификацию пользователей посредством Windows Active Directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей; 44. система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; 45. система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; 46. система должна поддерживать аутентификацию на основе групп пользователей; 47. система должна поддерживать функции NAT, PAT, «прозрачный» (мост); 48. система должна поддерживать функции NAT на основе политик; 49. система должна поддерживать функции VLAN Tagging (802.1Q); 50. система должна поддерживать функции SIP/H.323 NAT Traversal;

	51. система должна поддерживать настройку профилей безопасности; 52. система должна иметь возможность блокировки по URL/ключевому слову/фразе; 53. система должна поддерживать «Белые» списки URL; 54. система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; 55. система должна уметь предотвращать не менее 10000 типов сетевых атак; 56. система должна иметь возможность настройки списка сигнатур атак; 57. система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; 58. система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; 59. система должна поддерживать проверку заголовков MIME; 60. система должна поддерживать фильтрацию электронной почты; 61. система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; 62. система должна иметь возможность отсылки логов на удаленный syslog сервер; 63. система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; 64. система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; 65. система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках; 66. система должна поддерживать отправку файлов и URL на анализ в cloud sandbox для обнаружения неизвестных угроз класса “0-day”; 67. система должна иметь лицензирование в комплекте поставки для анализа в cloud sandbox не менее 10 000 объектов (файлов и URL) в день (24 часа); 68. система должна поддерживать протокол VRRP; 69. система должна поддерживать интеграцию с SIEM; 70. система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; 71. система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; 72. система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; 73. система должна поддерживать управление через Web интерфейс; 74. система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; 75. система должна поддерживать протоколы NetFlow, sFlow; 76. система должна обеспечивать режим обратного прокси-сервера (reverse proxy); 77. система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); 78. система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; 79. система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной

	системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях; 80. система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа; 81. система должна обеспечивать возможность управления беспроводными точками доступа; 82. система должна обеспечивать возможность управления коммутаторами;
Требование к обслуживанию и гарантии	система должна обеспечиваться расширенной технической поддержкой от производителя в режиме 24x7 не менее 3 лет, а также шлюзы безопасности должны иметь подписки на сервисы в течение 3 лет: 1. Контроль приложений 2. IPS 3. AV 4. Web Filtering 5. Antispam 6. Sandbox Cloud 7. Сервис оценки соответствия лучшим практикам 8. База промышленных протоколов и IoT устройств

Параметр	Минимальные требования
Тип оборудования	**Блок питание №3**
Кол-во (шт)	2 комплекта
модель	Участник торгов должен указать модель предложенной оборудования.
Сборка	Оборудование должно быть собрано (в сборку включаются все компоненты, оговоренные техническим заданием) и протестировано на заводах фирмы изготовителя. И должно быть полностью совместимо с Межсетевым экраном конфигурации №1
Технические требования	Pack of 5 AC power adaptors

ТРЕБОВАНИЯ К ПОСТАВКЕ

Место поставки	Склад Департамента закупок АО «UZBEKISTAN AIRWAYS», 100167, г.Ташкент, Международный аэропорт Ташкент им.И.Каримова, тел +/998 71/ 255-05-51, 255-68-37, факс + /998 71/ 255-35-24
Требования к упаковке	Все оборудование должно быть упаковано. Упаковка должна защищать товар от повреждений и обеспечивать его хранение в складских не отапливаемых помещениях. Поставщик должен нести полную ответственность за любые повреждения Товара, имевшие место вследствие несоответствующей упаковки, транспортировки или хранения
Требования к новизне	Закупаемое оборудование должно быть новым, ранее не использованным, не эксплуатируемым, не восстановленным, не являться выставочным образцом, произведенным не ранее 2021 года, не снятым с производства, не иметь дефектов.
Требования к сроку поставки	Максимальный срок поставки товара – 90 рабочих дней с даты предоплаты по договору.
Условия оплаты	15% предоплаты в течении 5 дней с даты подписания договора, 85% по факту поставки товара в течение 10 календарных дней

Требования к гарантийному обслуживанию	Гарантийный срок на аппаратную платформу не менее 36 месяцев после подписания акта приема-передачи. Гарантийный срок лицензий Межсетевой экран конфигурации №3 не менее 36 месяцев после подписания акта приема-передачи
Требования, предъявляемые к участникам отбора	1. Обязательное предоставление подробной спецификация предлагаемого товара, с указанием компании-производителя, модели, подробных технических характеристик; 2. При приемке товара «Поставщик» обязуется предоставить «Заказчику» документы, подтверждающие легальность ввоза товара в Республику Узбекистан; 3. Поставляемый товар должен иметь сертификат соответствия, выданный уполномоченным органом Республики Узбекистан (если требуется законодательство Республики Узбекистан); 4. Все осуществляемые при поставке товара расходы (транспортировка, доставка, отгрузка, маркировка гарантийными стикерами) «Поставщик» берет на себя; 5. Замена дефектного товара должна быть осуществлена «Поставщиком» в течении 15 календарных дней 6. Письмо от производителя дающее право на поставку товаров на территории РУз (MAF) 7. Гарантийное письмо от производителя о легальной сервисной гарантии на все предлагаемое оборудование и подписки 8. Опыт поставок и инсталляций аналогичных товаров (межсетевых экранов) на территории РУз Предоставить информацию о не менее 3 реализованных проектах. 9. Все оборудование должно быть от одного производителя и полностью интегрироваться без дополнительных аппаратных или программных средств (кластеризироваться) с существующими NGFW имеющимися у Заказчика 10. Любые отклонения от заявленных требований в техническом описании не допустимы

РАЗРАБОТАНО:
Начальник Управления информационной безопасности **Kirillov A.A.**

СОГЛАСОВАНО:

Заместитель председателя
правления по цифровизации **Xodjiyev Sh.G.**

Директор департамента закупок **Khodjamov N.K.**

Директор департамента
IT инфраструктуры **Fazilov X.N.**