Приложение 1

Технические требования к оборудованию и программному обеспечению

№	Описание	Характеристики
1.	Межсетевой экран	**Технические требования:** – возможность объединения МСЭ в единый отказоустойчивый кластер; – минимальная производительность: Firewall Throughput: не менее 36 Gbps; Одновременное количество сессий: не менее 8 Млн; Количество новых соединений: не менее 300000 в сек; IPS Throughput: не менее 5.2 Gbps; Производительность на уровне контроля приложений: не менее 14 Gbps; Производительность защиты в режиме полной проверки: не менее 4,7 Gbps; Количество виртуальных МСЭ (доменов): не менее 10; Количество интерфейсов: не менее 2x 10GE SFP+/GE SFP, 8x GE SFP, 10x GE RJ45; Количество USB портов: не менее 2; Жесткий диск: не менее 240GB SSD, количество - не менее 2; Блок питания: не менее 100–240V AC, 50–60 Hz, количество - не менее 2. **Функциональные требования:** – лицензирование системы должно осуществляться для неограниченного количества пользователей; – система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; – система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: • с холодным резервом (active/passive); • с горячим резервом (active/active); • кластер балансировки; – система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений; – система должна иметь функциональность балансировки нагрузки;

		– система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); – система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); – система должна обеспечивать анализ SSH трафика (ssh inspection); – система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; – система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента); – система должна обеспечивать оптимизацию WAN соединений; – система должна иметь функционал защиты от утечек данных DLP; – система должна обеспечивать антивирусную защиту с аппаратным ускорением; – система должна обеспечивать защиту от спама (антиспам); – система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением; – система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; – принудительное включение режима безопасного поиска в популярных поисковых системах; – система должна иметь функциональность контроля приложений; – система должна иметь функциональность WEB proxy; – система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию; – система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика; – система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; – система должна иметь возможность помещать инфицированные сообщения в карантин; – система должна иметь возможность блокировки передачи файлов в зависимости от размера; – система должна иметь возможность блокировки передачи файлов в зависимости от типа; – система должна поддерживать соединения множества WAN сетей; – система должна поддерживать протокол PPPoE и L2TP; – система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”; – система должна поддерживать маршрутизацию на основе политик; – система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP; – система должна поддерживать использование зон безопасности; – система должна поддерживать маршрутизацию между зонами; – система должна поддерживать маршрутизацию между виртуальными сетями; – система должна поддерживать администрирование на основе ролей;

		– система должна поддерживать несколько уровней администраторов и пользователей; – система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс; – система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО; – система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; – система должна поддерживать Kerberos аутентификацию пользователей; – 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; – система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; – система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; – система должна поддерживать аутентификацию на основе групп пользователей; – система должна поддерживать функции NAT, PAT, «прозрачный» (мост); – система должна поддерживать функции NAT на основе политик; – система должна поддерживать функции VLAN Tagging (802.1Q); – система должна поддерживать функции SIP/H.323 NAT Traversal; – система должна поддерживать настройку профилей безопасности; – система должна иметь возможность блокировки по URL/ключевому слову/фразе; – система должна поддерживать «Белые» списки URL; – система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; – система должна уметь предотвращать не менее 4000 типов сетевых атак; – система должна иметь возможность настройки списка сигнатур атак; – система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; – система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; – система должна поддерживать проверку заголовков MIME; – система должна поддерживать фильтрацию электронной почты по ключевым словам и фразам; – система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; – система должна иметь возможность отсылки логов на удаленный syslog сервер; – система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; – система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; – система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках;

		– система должна поддерживать протокол VRRP; – система должна поддерживать интеграцию с IBM QRadar SIEM; – система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; – система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; – система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; – система должна поддерживать управление через Web интерфейс; – система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; – система должна поддерживать протоколы NetFlow, sFlow; – система должна обеспечивать режим обратного прокси-сервера (reverse proxy); – система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); – система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; – система должна обеспечивать поддержку антивирусной базы сигнатур, которая должна создаваться самим производителем оборудования(не использовать базы сигнатур сторонних компаний). Межсетевой экран должен иметь подписки на сервисы безопасности в течение 1 года: – Контроль приложений – IPS – AV – Web Filtering – Antispam **Требование к обслуживанию и гарантии:** – система должна обеспечиваться расширенной технической поддержкой производителя в режиме 24x7 и подпиской на сервисы безопасности не менее года.