«Утверждаю»
Гл. метролог
____ А.Р. Хамроев
«12» 10 2023 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на поставку система безопасности, контроля и учёта доступа к ресурсам сети Интернет.

Караулбазар 2023 г.

Оглавление

Основные требования

Комплексное UTM решение включая программный межсетовой экран (файервол) и маршрутизатор, систему обнаружения и предотвращения вторжений (IPS/IDS), **антивирус, и фильтрацию приложений** на основе подписки лицензий. Обязательно наличие модуля **фильтра веб-содержимого, как минимум по 140 типовым категориям**, собственным встроенным VPN сервером и VPN-клиентами, динамической балансировки нагрузки, шейпером для предустановленных политик маршрутизации. Консоль управления должна быть построена на веб технологии без установки дополнительного ПО. Поддержка нескольких IP адресов на одном сетевом интерфейсе, наличие блокировщика пиринговых сетей. Предлагаемые продукты должны быть бессрочны в рамках версии, с возможностью продления только технической поддержки и функций прилагаемых модулей. **Общее число управляемых пользователей – 500**.

Общие требования

Программный межсетевой экран (далее - ПМЭ) должен обладать достаточным функционалом по осуществлению контроля доступа пользователей ЛВС к ресурсам сети Интернет, в том числе осуществлять возможность идентификации пользователей по уникальным парам «имя пользователя\пароль», хранящимся как в локальной пользовательской базе ПМЭ, так и в базе LDAP Active Directory\Apple Open Directory, а также должен включать в себя следующие модули:

- Модуль обнаружения и предотвращения вторжений (IDS\IPS)
- Модуль фильтрации Web протоколов на основании пользовательского списка правил
- **Модуль контентной Web фильтрации**
- **Модуль фильтрации запрещённых слов**
- **Модуль пакетной фильтрации с осуществлением отслеживания пакетов (SPI)**
- **Модуль фильтрации FTP протокола**
- **Модуль антивирусной фильтрации**
- Модуль управления полосой доступа к сети Интернет
- Модуль непрозрачного прокси-сервера
- Модуль организации защищённых соединений с удалёнными пользователями и\или ЛВС (VPN)
- Модуль обнаружения и предотвращения пиринговых соединений (p2p)
- Модуль обнаружения и предотвращения атак с подменой IP адресов(spoofing)
- Модуль фильтрации MAC адресов
- Модуль DHCP
- Модуль сбора статистики доступа пользователей к Интернет ресурсам
- Модуль переадресации DNS
- Поддержка входящих и исходящих подключений по протоколу IPv6
- Возможность интеграции системы управления ПМЭ в единую систему управления компании, выполненную на основе WEB приложений

В том числе ПМЭ должен обладать возможностью работы с двумя линиями доступа к сети Интернет в режиме обработки отказа (failover) и в режиме распределения нагрузки трафика между каналами (network load balancing); при этом в режиме распределения нагрузки ПМЭ должен поддерживать работу от 2 и более линий доступа к сети Интернет.

Технические требования к ПМЭ

Модуль обнаружения и предотвращения вторжений (IDS\IPS)

Модуль обнаружения и предотвращения вторжений (IDS\IPS) должен быть основан на приложении Snort, являющимся отраслевым стандартом. Приложение выполняет прозрачное сканирование проходящего сетевого трафика и сопоставляет его с базой установленных правил безопасности, а также осуществляет контроль входящих и исходящих соединений с публичными чёрными списками хостов:

Botnet Command and Control Servers - http://www.shadowserver.org/wiki/

Dshield Identified Top Attackers - http://www.dshield.org/

Hostile or Compromised Hosts - http://doc.emergingthreats.net/bin/view/Main/CompromisedHost

Russian Business Network - http://doc.emergingthreats.net/bin/view/Main/RussianBusinessNetwork

Spamhaus DROP Listed Networks - http://www.spamhaus.org/drop/

Tor Exit Nodes - http://doc.emergingthreats.net/bin/view/Main/TorRules

Состав чёрных списков системы IDS\IPS должен обновляться не реже чем 1 раз каждые 24 часа.

Состав используемых сигнатур угроз должен контролироваться на предмет ложных срабатываний самим разработчиком, после чего должен предоставляться пользователям системы предотвращения вторжений в качестве отдельного обновления для системы IDS\IPS.

Модуль Web фильтрации на основании пользовательского списка правил

Данный модуль должен предоставлять следующие возможности:

- Возможность создания неограниченного списка правил, применяющихся как к учётным записям пользователей (группам пользователей), так и\или к указанным группам IP адресов
- Возможность использования нескольких методов реагирования на срабатывание правил:
    - Разрешить доступ (с возможностью исключения антивирусной проверки, и\или запретом страниц содержащих запрещённые администратором слова)
    - Отклонить доступ (отобразить страницу с пояснениями причины отказа)
    - Запретить доступ (имитация недоступности Web-страницы)
    - Перенаправить (перенаправление запросов соответствующих критериям правила на указанный URL)
- Возможность разрешения доступа к указанным URL без обязательного прохождения пользователями аутентификации.

Модуль контентной Web фильтрации

Модуль Web фильтрации должен:

- включать в себя не менее 100 категорий блокировки
- обладать облачной базой данных, доступной 24/7
- база данных URL должна насчитывать не менее 500,000,000 определённых URL
- обладать гибкой системой настройки запретов\разрешений

- обладать удобной системой оповещения разработчика о некорректно присвоенных категориях
- обладать возможностью ведения списка исключений (белый список)
- обладать возможность фильтрации шифрованных Web подключений(HTTPS)

Модуль фильтрации запрещённых слов

Данный модуль должен содержать предустановленный список слов, а также давать возможность расширения данного списка. Поиск слов должен осуществляться непосредственно в HTML-коде загружаемых web-страниц, и при достижении некоего показателя блокировки (назначенного администратором), доступ к данной странице должен быть запрещён.

Модуль фильтрации FTP протокола

Данный модуль должен предоставлять следующие возможности:

- Разрешение\запрет указанных команд FTP
- Разрешение\запрет загрузки и\или выгрузки файлов указанного типа (имени\расширения)
- Ведение протоколирования срабатывания каждого правила в отдельности в специальном протоколе ПМЭ
- Возможность применять правила:
    - к отдельным учётным записям и\или группам пользователей
    - к указанным группам IP адресов
    - по указанным интервалам времени

Модуль пакетной фильтрации с осуществлением отслеживания пакетов (SPI)

Данный модуль должен обладать следующим списком возможностей:

- Возможность создания правил фильтрации на основании IP адресов (адресов отдельных хостов, адресов сетей, диапазонов IP адресов, групп IP адресов), учётных записей пользователей (групп пользователей)
- Возможность лёгкого управления трансляцией сетевых адресов (NAT)
- Возможность лёгкой настройки внешнего доступа к внутренним ресурсам ЛВС предприятия (port MAP)
- Логика очерёдности обработки правил фильтра должна соответствовать общепринятой логике – направление обработки сверху-вниз
- Логика работы правил должна исходить из принципа, «что не разрешено, то запрещено»
- Возможность управления протоколированием передачи пакетов, установления соединений и ведения графического отображения передаваемого объёма входящего и исходящего трафика.
- Возможность присвоения значений DSCP(QoS) на выбранные правила фильтра.
- Возможность создания правил, работающих в указанные временные промежутки.
- Логичный и лёгкий в понимании интерфейс.
- Наличие «мастера», позволяющего провести автоматическую настройку правил.

Модуль антивирусной фильтрации

Модуль антивирусной фильтрации должен осуществлять контроль следующих данных:

- Передаваемые данные по WEB протоколам, включая архивные файлы.
- Передаваемые данные по почтовым протоколам POP3\SMTP
- Передаваемые данные по FTP протоколу

Также данный модуль должен обладать возможностью запрета передачи зашифрованных и повреждённых файлов по почтовым и WEB протоколам, в том числе должен обладать возможностью разрешения\запрета установки шифрованных соединений (TLS). Данный модуль должен обладать возможностью разграничения сканирования данных по именам загружаемых\передаваемых файлов, а также по типам MIME.

Модуль управления полосой доступа к сети Интернет

Модуль управления полосой доступа к сети Интернет должен предоставлять:

- возможность определять допустимое потребление полосы доступа объектам ЛВС
- возможность резервирования указанного значения полосы пропускания для различных объектов ЛВС
- возможность работы системы QoS
- возможность создания множества правил управления
- возможность указания данных значений, как в абсолютном, так и в относительном значениях

Модуль непрозрачного прокси-сервера

Модуль непрозрачного прокси-сервера должен:

- обладать поддержкой аутентификации пользователей
- обладать возможностью запрета использования нестандартных (не 443) сетевых портов для установки зашифрованных соединений
- обладать возможностью работы в прозрачном режиме
- обладать возможностью автоматической настройки обозревателей пользователей через модуль DHCP
- обладать возможностью использования родительского прокси-сервера для организации каскадного доступа к ресурсам сети Интернет

Модуль организации защищённых соединений с удалёнными пользователями и\или ЛВС (VPN)

Модуль организации защищённых соединений с удалёнными пользователями и\или ЛВС (далее - Virtual Private Network(VPN), должен соответствовать следующим требования безопасности:

- Передача данных должна осуществляться с шифрованием не менее 128 бит
- Канал управления должен быть зашифрован с использованием протокола Secure Socket Layer и алгоритма AES 255-SHA

Модуль VPN должен:

- обладать расширенной настройкой передаваемой маршрутной информацией для соединений клиент-сервер и сервер-сервер
- обладать настройкой параметров DNS\WINS для соединений клиент-сервер
- обладать возможностью передачи значения шлюза «по умолчанию» для соединений клиент-сервер
- обладать возможностью создания неограниченного количества соединений типа сервер-сервер
- обладать поддержкой IPSec для приёма входящих подключений от удалённых клиентский устройств а так же установления соединений типа сеть-сеть.

Модуль обнаружения и предотвращения пиринговых соединений (p2p)

Модуль обнаружения и предотвращения пиринговых соединений (p2p) должен обладать возможностью расширенной настройки параметров определения p2p соединений, в том числе предоставлять возможность выбора сетевых портов как доверенных\не доверенных, указание количества одновременных соединений, определяемых как p2p передача, а также возможностью настройки реагирования ПМЭ на данную активность.

Модуль обнаружения и предотвращения атак с подменой IP адресов (spoofing)

Модуль обнаружения и предотвращения атак с подменой IP адресов (spoofing) должен корректно определять данные атаки и выполнять их блокировку.

Модуль фильтрации MAC адресов

Модуль фильтрации MAC адресов должен работать в двух режимах: список разрешённых MAC адресов и список запрещённых MAC адресов. Также должен быть доступен выбор сетевого интерфейса, к которому применяются правила фильтра MAC адресов.

Модуль DHCP

Данный модуль должен предоставлять доступ к основным возможностям современных DHCP служб, его наличие должно гарантировать исключение необходимости использования службы DHCP сторонних производителей.

В состав параметров DHCP обязательно должны входить следующие параметры:

- Для поддержки автоматической конфигурации VoIP телефонов:
  - 066-TFTP server name
- Для осуществления сетевой загрузки тонких клиентов:
  - 066-TFTP server name
  - 067-Bootfile name
- Для осуществления автоматической конфигурации настроек прокси-сервера в обозревателях ПК в ЛВС предприятия:
  - 252-MSIE proxy autodiscovery

Также необходима возможность расширения общего списка доступных опций DHCP.

Модуль сбора статистики доступа пользователей к Интернет ресурсам

ПМЭ должен обладать внутренней системой сбора и анализа данных об использовании пользователями компании Интернет ресурсов, со следующими возможностями:

- вывод статистической информации, как по отдельным пользователям, так и по указанным группам пользователей.
- Наличие внутренних инструментов, создания отчётов потребления трафика за указанные периоды времени, и возможность отправки их по электронной почте в виде HTML документов.
- Возможность внесения исключений на основании указанных
    - Учётных записей\групп пользователей
    - URL Интернет ресурсов
    - Групп IP адресов потребителя в ЛВС и сервера в сети Интернет
    - Указанных временных интервалов
- Возможность предоставления доступа к личной статистике, пользователям ПМЭ в ЛВС.

Модуль переадресации DNS

Модуль переадресации DNS должен обладать:

- Максимальной простотой управления
- Внутренним кешем для ускорения доступа к Интернет ресурсам
- Обладать возможностью создания А записей хостов
- Обладать возможностью выдачи имен хостов из таблицы аренды DHCP-сервера
- Обладать модулем создания правил пользовательской адресации DNS запросов, для оптимизации работы данного модуля в многодоменных структурах.

Поддержка входящих и исходящих подключений по протоколу IPv6

ПМЭ должен обладать возможность предоставления доступа хостам ЛВС в сеть Интернет по протоколу IPv6. Также данный ПМЭ должен обладать возможностью предоставления доступа по протоколу IPv6 к ресурсам ЛВС предприятия.

Возможность интеграции системы управления ПМЭ в единую систему управления компании, выполненную на основе WEB приложений

ПМЭ должен обладать общедоступным интерфейсом программирования приложения (Application Programming Interface - API) для обеспечения возможности интеграции системы управления приложением в существующую\создаваемую единую систему управления предприятия на основе Web технологий.

Требования к технической поддержке

Техническая поддержка ПМЭ должна:

- Предоставляться на русском языке сертифицированными специалистами производителя ПМЭ и\или сертифицированными специалистами компаний партнёров производителя ПМЭ, на территории РФ и СНГ.
- WEB-сайт производителя ПМЭ должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке ПМЭ, пополняемую базу знаний, а также форум пользователей ПО.

Составил:
Начальник сектора кибербезопасности Бахронов Б.Х.

Согласовано:
Начальник IT-центра Фазилов А.А.