SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC
INSPECTOR
NEXT
GENERATION

Настройка HTTP Antivirus Proxy

www.smart-soft.ru

1. Вступление

Плагин HAVP представляет собой специализированный прокси-сервер, к которому в виде библиотеки подключается антивирусный движок ClamAV. Плагин HAVP обеспечивает централизованную проверку трафика на уровне шлюза.

Поддерживается проверка:

- HTTP-трафика
- FTP over HTTP-трафика (обращение к FTP-серверу через HTTP-прокси)
- HTTPS-трафика, при настроенном функционале перехвата HTTPS-соединений, а также трафик

Механизм антивирусной проверки устроен следующим образом. Пользовательский веб-трафик попадает к демону Squid (по причине наличия у пользователя явных настроек на HTTP-прокси или из-за механизма прозрачного проксирования). В настройках Squid прописан каскад на вышестоящий прокси (HAVP), который, в действительности, выполняется на этой же машине и использует сокет 127.0.0.1:8080. HAVP прокси и интегрированный в него антивирусный движок ClamAV обеспечивают антивирусную проверку трафика.

2. Настройка

Настройка плагина HAVP включает в себя следующие шаги.

2.1 Установка плагина HAVP

Пройдите в раздел Система -> Прошивка -> Обновления, вкладка Плагины и нажмите Проверить наличие обновлений.

Примечание. Для успешной проверки обновлений в вашем устройстве TRAFFIC INSPECTOR NEXT GENERATION должен быть установлен лицензионный сертификат. Для получения информации по установке сертификата, обратитесь к инструкции Начало работы с TRAFFIC INSPECTOR NEXT GENERATION.

В случае успешной проверки обновлений, вы увидите список доступных плагинов. Выберите плагин os-havp и нажмите на значок +, чтобы установить его.

2.2 Настройка веб-прокси Squid

Для работы HAVP плагина, требуется включенный и настроенный веб-прокси. Для получения информации по настройке веб-прокси, обратитесь к инструкции Настройка веб-прокси.

Дополнительно, можно настроить прозрачное проксирование. Суть "прозрачного проксирования" - пользователи не имеют явных настроек на веб-прокси, тем не менее их трафик все равно попадет на прокси. Для получения информации по

настройке прозрачного проксирования, обратитесь к инструкции Настройка прозрачного проксирования.

2.3 Настройка плагина HAVP

Пройдите в раздел Службы -> HTTP Antivirus Proxy -> Администрирование.

Для включения HAVP плагина, установите флаг Включить HAVP.

Примечание. Запуск и перезапуск HAVP-плагина требует времени, так как сопровождается загрузкой антивирусной базы (размером в среднем 100 МБ) в оперативную память.

Для сканирования изображений, установите флаг Включить сканирование изображений.

Определите пороговое значение размера файла в поле Maximum size of scanned file (MB). Файлы большего размера проверяться не будут.

После включения плагина HAVP перезагрузите шлюз – Maintenance -> Перезагрузка.

2.4 Проверка настроек плагина HAVP

Подключитесь к шлюзу по SSH. Для этого можно использовать популярный SSH-клиент Putty. Выполните команду:

cat /usr/local/etc/squid/squid.cong

Конфигурационный файл Squid должен заканчиваться строками:

cache_peer 127.0.0.1 parent 8080 0 no-query no-digest

never_direct allow all

2.5 Настройка исключений

В раздел Службы -> HTTP Antivirus Proxy -> Администрирование, щелкните на значок + в нижнем правом углу экрана. Задайте URL, в отношении которого сканирование выполняться не будет, например:

Примечания.

URL задается в формате без схемы (т.е. без части http://).

Исключение применимо только для указанного URL. Например, если мы исключаем сканирование URL <example.org>, то URL <example.org/example.exe> сканироваться будет.

2.6 Антивирусная проверка

При обнаружении потенциально опасного содержимого, HAVP плагин отображает страницу блокировки в браузере пользователя: