Доступна новая версия универсального шлюза безопасности Traffic Inspector Next Generation

16 сентября 2019 года

Компания «Смарт-Софт» сообщает о выходе новой версии универсального шлюза безопасности (UTM) и системы обнаружения (предотвращения) вторжений Traffic Inspector Next Generation.

В новом релизе Traffic Inspector Next Generation:

1. Осуществлен перевод на актуальную версию OPNsense 19.7.3, что позволяет пользователям использовать все преимущества обновленной платформы.

   Что нового:

   - Логирование правил NAT. При включенной функции в логах межсетевого экрана сохраняется информация о срабатывании правил NAT.
   - WPAD / PAC и поддержка родительского прокси на веб-прокси. Доработка предоставляет возможность автоматической настройки прокси-сервера в браузерах клиентов.
   - Поддержка DNSSEC в DNS-сервере Dnsmasq обеспечивает защиту от подмены IPадресов за счет криптографической проверки подлинности источника данных и проверки целостности данных.
   - OpenVPN client export API предоставляет возможность автоматизации процесса выдачи клиентских сертификатов для OpenVPN.
   - Добавлены новые плагины:

     API backup export –автоматизация работы с резервными копиями;

     Hardware widget – предоставление сведений об аппаратной платформе;

     Nginx –веб-сервер и почтовый прокси-сервер.
   - Добавлено отображение автоматических правил межсетевого экрана в вебинтерфейсе, что позволяет получить полный перечень используемых правил.

- Добавлен сбор и отображение статистики для всех правил межсетевого экрана.
- Обеспечена поддержка синхронизации групп пользователей в LDAP.
- Обеспечена поддержка запросов на генерацию сертификатов (CSR, Certificate Signing Request) – больше нет необходимости полностью генерировать SSL-сертификаты на устройстве, достаточно подписать уже заранее сформированный запрос на сертификат.

2. Добавлена аутентификация пользователей на прокси по их IP/MAC-адресам.
3. Обеспечена возможность сохранения резервных копий конфигурационного файла config.xml в сервисе Яндекс.Диск.
4. При установке нового плагина в меню Traffic Inspector Next Generation автоматически появляется относящийся к новому плагину раздел. Доработка снимает необходимость ручного обновления интерфейса меню администратором при установке каждого нового плагина.
5. Добавлена возможность выбора темы оформления. В базовой поставке Traffic Inspector Next Generation предустановлены две темы. Для использования трех дополнительных тем оформления необходимо установить соответствующие плагины.

Также были исправлены обнаруженные ошибки.

При миграции на новую версию разработчик рекомендует обратить внимание на следующие моменты:

- Графики работоспособности шлюза могут нуждаться в ручном сбросе из-за миграции Apinger в Dpinger. Apinger больше недоступен.
- Правила обнаружения вторжений GeoIP автоматически деактивируются и должны быть вручную перенесены в псевдоним брандмауэра GeoIP.
- Плагин quagga был заменен на FRR плагин. Бинарный пакет quagga сохранен на данный момент.
- Рекомендовано ознакомиться с документацией FRR в отношении необходимых системных перенастроек.
- Загрузка Bhyve UEFI может завершиться ошибкой в качестве гостя. Эта проблема изучается.
- Плагин SNMP был заменен плагином Net-SNMP.
- Привилегия входа через веб-прокси больше недоступна. Вместо этого доступ может быть ограничен селектором группы.
- OpenVPN больше не поддерживает прослушивание групп шлюзов. Вместо этого необходимо использовать localhost в сочетании с переадресацией портов.

Traffic Inspector Next Generation

Универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений Traffic Inspector Next Generation предназначен для организации контролируемого доступа к интернету корпоративных компьютерных сетей и их защиты от внешних угроз. Относится к классу Unified Threat Management. Базируется на открытом коде проекта OPNsense.

Traffic Inspector Next Generation обеспечивает фильтрацию на разных уровнях модели OSI и управление через веб-интерфейс по защищенному HTTPS-подключению, а также по протоколу SSH с использованием терминального доступа. Решение разворачивается в роли шлюза на границе корпоративной сети и позволяет контролировать информационные потоки между локальной сетью и интернетом.

Модели в линейке:

- S100: для небольших домашних и офисных сетей. В качестве аппаратной платформы используются компьютеры x86-64 малого форм-фактора (152,4 x 152,4 мм).
- S500: для среднего бизнеса и государственных учреждений среднего размера.
- M1000: для крупного бизнеса и учреждений госсектора.
- L1000+: топовая модель для крупных коммерческих, государственных, образовательных организаций, учреждений здравоохранения, культуры, спорта и туризма.

Аппаратная платформа моделей S500, M1000 и L1000+: стоечные серверы DEPO формфактора 1U.

Для получения более подробной информации об универсальном шлюзе безопасности (UTM) и системе обнаружения (предотвращения) вторжений Traffic Inspector Next Generation посетите сайт компании «Смарт-Софт».

Компания «Смарт-Софт» – ведущий российский разработчик комплексных систем защиты информации и управления интернет-доступом для бизнеса, предприятий и организаций госсектора, образовательных и медицинских учреждений, учреждений культуры:

- Многофункционального межсетевого экрана и системы обнаружения (предотвращения) вторжений Traffic Inspector,
- Универсального шлюза безопасности (UTM) и системы обнаружения (предотвращения) вторжений Traffic Inspector Next Generation.

Собственные решения на основе уникальных программных алгоритмов полностью соответствуют требованиям российского законодательства в области защиты информации, сертифицированы ФСТЭК России и входят в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Решения компании «Смарт-Софт» защищают компьютеры «Газпрома», «Мегафона», Сбербанка, РЖД, «Роснефти», а также тысяч других компаний крупного, среднего и малого бизнеса и государственных организаций.

«Смарт-Софт» работает на рынке информационной безопасности с 2003 года. Партнерская сеть компании насчитывает более 2500 российских и международных организаций.