Часто задаваемые вопросы

Вопросы о лицензиях Nipper

В: Существует триальная лицензия Nipper?
Да. Вы можете использовать триальную лицензию программного обеспечения Nipper в течение 1 месяца для аудита 2х устройств.

В: Распространяются ли лицензии Nipper как лицензии открытого ПО?
Нет, лицензии Nipper Studio - Коммерческие. Однако, Nipper Тип-7 и Nipper IPCalc, распространяются как лицензии открытого ПО и доступны через раздел Labs на сайте.

В: Включена ли техническая поддержка при покупке лицензии?
Да. Техническая поддержка осуществляется как через сайт в разделе SUPPORT, так и через наших локальных представителей.

В: Возможно ли получить скидку, приобретая лицензию более чем на 1 год?
Да. Существуют скидки при подписке на период 2 и 3 года.

В: Что представляет собой устройство?
"Устройство" (device), как указано в лицензии – это индивидуальный брандмауэр, маршрутизатор или коммутатор, который Nipper Studio будет проверять. Если, к примеру, у вас есть система управления, которая объединяет конфигурации 5 индивидуальных брандмауэров, то вам потребуется лицензия на 5 устройств, чтобы охватить их все. Если у вас стек коммутаторов с одной конфигурацией, то он будет считаться одним устройством. Виртуальные устройства обрабатываются также как и физические, и требуют лицензии для отдельных устройств соответственно.

В: Сколько раз я могу осуществлять аудит лицензированного устройства?
Используя Коммерческую лицензию, вы можете использовать Nipper Studio столько раз, сколько хотите. Аудиторская лицензия позволяет использовать Nipper Studio только раз относительно лицензированного устройства.

В: Включены ли обновления в лицензию Nipper?
Лицензии Nipper 1 и Nipper Studio включают в себя все обновления в течение периода подписки. Если у вас есть * Enterprise или аудиторская лицензия Nipper, вы можете загрузить и использовать последнюю версию продукта Nipper Studio бесплатно (в рамках вашей подписки).

* Enterprise лицензии - это Коммерческие лицензии.

В: Могу ли я установить одну лицензию Nipper на все компьютеры в моей компании?
Да. Лицензирование продукта основывается на количестве сетевых устройств, которые проверяются, а не на количестве компьютеров на которое установлено программное обеспечение.

Установка и активация Нипper

В: У меня возникли проблемы с установкой программы.
Пожалуйста, посмотрите видео - руководство по установке.

В:У меня возникли проблемы при активации Nipper.
Чтобы активировать Nipper, вам нужен: код активации, который вы можете найти на странице "Мои лицензии", адрес электронной почты, который совпадает с учетной записью лицензии, и Интернет. Для того, чтобы активировать Nipper необходимо подключиться к серверу обновлений Titania , то есть если Nipper не будет иметь доступа к серверу, то его невозможно будет активировать. Если у вас есть прокси-сервер, то вы должны дать эту информацию Nipper.

Если ваш хост Nipper не подключен к Интернету, или прокси-сервер поддерживает метод аутентификации, который не поддерживает Nipper, то возможно активировать программу и без подключения к Интернету. Для этого вам нужно использовать версию командной строки Nipper. (Для пользователей Windows: командная строка доступна при запуске cmd.exe из меню Пуск).

Для оффлайн активации используйте следующую команду:

nipper –offline-activation

Затем следуйте инструкциям по активации Nipper без соединения с сервером обновлений.

Запуск Нипper

В: Какие файлы нужны для обработки конфигураций CheckPoint?
Файлы, которые потребуются Nipper, будут меняться в зависимости, откуда пришла конфигурация (модули брандмауэра, модуль управления, Nokia IP ...) и от названия настроенной политики. Необходимые файлы могут также меняться в зависимости от содержимого других файлов. Так на устройствах CheckPoint / Nokia IP, сделайте копию всех директорий "conf" или "database" (в зависимости от устройства). Директория, содержащая файлы конфигурации, затем определяется как входные данные, а не как один файл, как для других типов устройства.

Существует руководство пользователя устройствами CheckPoint, которое подробно описывает, как получить то, что вам нужно.

B: В чем принципиальное различие между обычным сканером уязвимостей и Nipper?
Nipper оценивает настройки устройства, используя собственный файл конфигураций устройства. Обычный сканер уязвимостей для определения уязвимостей исследует сетевые порты и сервисы. Так, обычный сканер уязвимостей будет сообщать только о тех результатах, которые он смог обнаружить, в то время как Nipper использует фактическую конфигурацию и может дать много результатов, которые являются наиболее сложными или вовсе неспособными к обнаружению.

Например, используя сканер для выявления недостатков правил брандмауэра можно определить только те, которые брандмауэр позволит увидеть сканирующему устройству. Чтобы перечислить все правила брандмауэра сканеру придется просматривать каждый сетевой порт от всевозможных сетевых адресов до всех остальных, и настройки IDS могут заблокировать сканер задолго до этого. Nipper использует конфигурации устройств, поэтому он может быстро увидеть какие правила установлены и где слабые стороны брандмауэра.

Также существуют и другие отличия, представьте, что сканер пытается обнаружить, когда сетевое устройство регистрируется в сетевом журнале логов или обновляет свои часы из источника центрального времени.

B: Как запланировать в Nipper время проведения аудита?
Nipper может быть запланирован на вашей платформе календарного планирования. В системе Windows, вы можете использовать планировщик заданий, на UNIX- системах можно использовать Cron. Внизу показано как запланировать Nipper для осуществления аудита в определенное время.

Для примера конфигурацией устройства, подлежащего аудиту, будет "myconfig.txt" в директории с именем "configs", и аудит будет запланирован ежедневно на 3:15 (утра).

Windows Task Scheduler
Этот алгоритм был разработан для Windows 7, но в равной степени может быть применен и для других версий Windows (с незначительными изменениями).

1. Откройте планировщик задач Windows Task Scheduler, нажатием на кнопку Пуск, затем Панель управления (Control Panel), затем "Система и безопасность", затем "Администрирование" и, наконец, дважды кликните на "Планировщик заданий" (Task Scheduler).
2. Нажмите на меню Действие (Action), а затем на "Create Basic Task".
3. Введите "Nipper" в качестве имени задачи.
4. Введите календарь, запланированный ежедневно на 3:15 и нажмите кнопку Далее.
5. Выберите запуск программы Nipper затем нажмите кнопку Далее.
6. Выберете программу Nipper (обычно C: \ Program Files\ Nipper\ nipper.exe) и добавьте следующую команду "- input = c: \ configs \ myconfig.txt - output = c: \configs\ myreport.html", затем нажмите кнопку Далее.
7. Нажмите кнопку Готово. (Finish).

Планировщик UNIX Cron
Этот алгоритм использует командную строку, но для вашей системы должен быть GUI интерфейс.

1. Запустите "crontab -l> scheduled- tasks.txt" к списку текущих запланированных задач.
2. Отредактируйте "scheduled- tasks.txt" файл с помощью текстового редактора.
3. Добавьте следующую строку в файл. "15 3 * * * nipper-- input =/configs/myconfig.txt -- output = /configs/report.html".
4. Сохраните файл и выйдите из редактора.
5. Добавьте новое расписание, используя команду "crontab scheduled- tasks.txt"

В: Какие опции конфигурации необходимо выбирать для GTA устройств?
Вы должны сохранить конфигурацию вашего устройства как XML для того, чтобы использовать его с Nipper.

В: Nipper выдал ошибку: Обработка файла неправильного типа (Processing the wrong type of file).
"Обработка файла неправильного типа" происходит, когда Nipper при обработке конфигурационного файла не может определить некоторые параметры конфигурации, которые должны быть у определенного типа устройства. Например, если из конфигурационного файла, который, как правило, содержит информацию о версии, была удалена запись версии. Эта функция была разработана для предотвращения ситуаций, когда при обработке конфигурации Juniper NetScreen, обозначалось устройство Cisco ASA.

Если вы уверены, что файл конфигурации из устройства правильного типа, то вы можете заставить Nipper обработать его и игнорировать тот факт, что обычные параметры не были представлены. Это можно сделать, используя функцию командной строки –force в инструменте командной строки.

В: Коммутатор Cisco имеет возможности маршрутизации. Обрабатывать ли его как маршрутизатор?
Обрабатывайте конфигурацию как для устройства Cisco Catalyst (с помощью инструмента командной строки можно использовать – опцию --ios-catalyst). Если Nipper при обработке файла найдет какие-либо настройки маршрутизации, то они также будут включены в аудит безопасности и в отчет о конфигурации.

В: Отчет по устройству CheckPoint содержит много объектов, но нет правил.
Возможно, у вас неправильный набор конфигурационных файлов вашего брандмауэра. Ваше устройство должно иметь как конфигурации, так и справочник базы данных.

Проверьте таблицы файла .C (если существуют) в директории конфигурации, он должен содержать раздел для политик брандмауэра и указывать, какой файл сохранен. Если этот файл пустой, то у вас либо нет правил в этой системе, либо они сохранены в другом месте. Попробуйте найти правила в .C.

Более подробные инструкции вы найдете в руководстве пользователя устройств CheckPoint.

В: Обработка конфигураций CheckPoint занимает много времени.
Конфигурации CheckPoint могут быть значительно больше и сложнее, чем у Cisco ASA или Juniper NetScreen. Это подтверждает количество конфигурационных файлов и их размер. Кроме того, один набор конфигурационных файлов может охватывать различные межсетевые экраны. В более крупных конфигурациях размер может превышать 1 Гб.

Обработка любой конфигурации, будет зависеть от ряда факторов: размера файла конфигурации, производительности вашего компьютера и настроек Nipper. Подумайте, сколько времени потребуется для копирования конфигураций такого размера, и добавьте время на аудит. Одной из наиболее времязатратных проверок Nipper является проверка правила совпадения и проверка дублированием. Для этого Nipper должен сравнить каждое правило относительно всех последующих правил (в том числе дочерние объекты, группы и так далее). Отключение этих проверок значительно сократит время. Эти проверки включены по умолчанию.

Чтобы отключить проверку правила совпадения и дублирования в Nipper нажмите кнопку "Настройки" (Settings), затем на закладке "Filtering" прокрутите вниз список проверок и отмените функции "Filter rules must not duplicate other rules" (Правила фильтрации не должны дублировать другие правила) и " Filter rules must not contradict other rules " (Правила фильтрации не должны противоречить другим правилам).

Отключить проверку правила совпадения и дублирования в инструменте командной строки Nipper можно, используя файл "C: \ Program Files \ Nipper \ nipper.ini" (или на системах Mac OS X и GNU / Linux - "/etc / nipper.conf"), либо добавлением следующих опций к команде "- -no-filter-duplicates" или "- -no-filter- contradicts".

В: Как получить конфигурацию брандмауэров McAfee Enterprise?
Вы должны извлечь конфигурацию, используя "McAfee Firewall Backup Script", которую можно загрузить из раздела Titania Labs на сайте. Затем подробные инструкции приведены в руководстве пользователя в разделе support сайта "Использование Nipper с брандмауэрами McAfee, Secure Computing и CyberGuard".

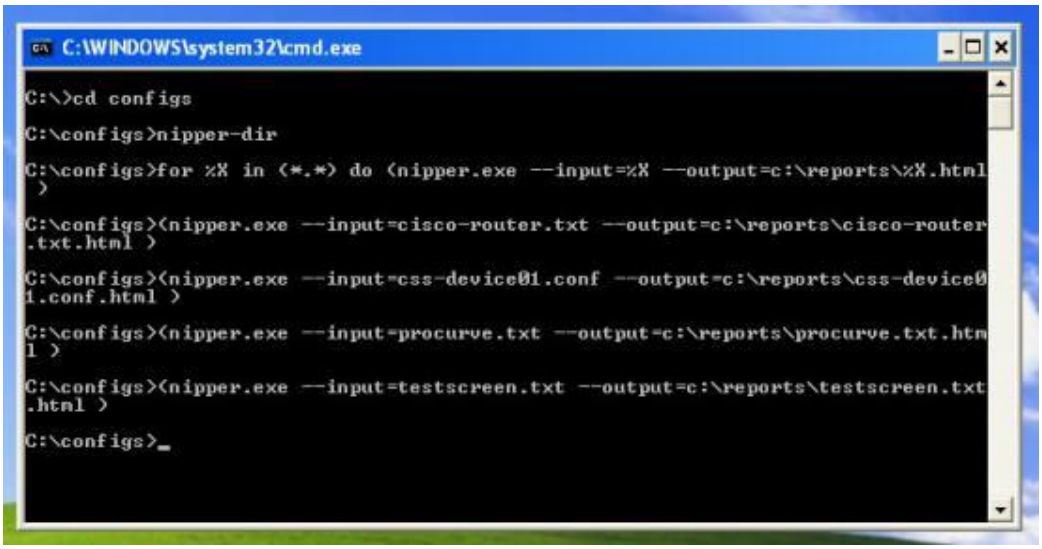
B: Как автоматизировать Nipper для обработки каталога конфигураций?
Nipper Studio способен одновременно обрабатывать несколько конфигураций. Это осуществляется использованием версии командной строки инструмента на любой из поддерживаемых платформ.

Пример ниже демонстрирует, как обработать все содержимое каталога под названием "configs" на Windows, Mac и GNU / Linux. И затем вывести отчеты в каталог под названием "reports".

Microsoft Windows
Создан файл с именем "nipper-dir.bat" и сохранен в директории C: \ Scripts на Windows PC. Этот командный файл содержит:

for% X% в (*.*) do (nipper.exe - -input =% X% - -output= c: \reports \%% X.html)

Тогда для аудита всего каталога конфигураций, используя Nipper, нужно перейти в этот каталог и запустить "nipper-dir". Пакетный скрипт будет обрабатывать все файлы, содержащиеся в этом каталоге, и выведет отчет в каталог "c: \ reports \".



Примечание: Эта процедура предполагает, что Nipper запущен, и когда вы введете "nipper.exe" Windows может найти его и выполнить задание. Вы можете добавить его в свой путь, щелкнув правой кнопкой на значок "Мой компьютер" и выбрав "Свойства". Затем выберите вкладку "Advanced" и нажмите на кнопку "Environment variable" (Переменная среды). Затем можно добавить "; C: \ Program Files \ Nipper ". Кроме того, каталог скриптов также находится в переменной среды.

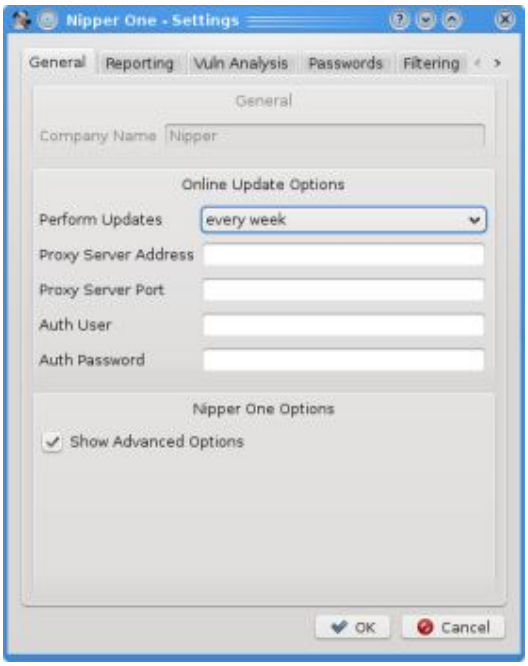
Apple Mac OS X и GNU / Linux

На платформах OS X и GNU / Linux процедура похожа, поэтому они объединены в одном разделе. Создаем скрипт "nipper-dir" и помещаем его в директорию "scripts" в домашнем каталоге. Файлу сценария были присвоены исполняемые разрешения. Подобно сценарию Windows, он берет содержимое текущего каталога, запускает каждый файл через Nipper и выводит отчеты в каталог отчетов.

```
for x в `` ls
do
nipper- -input =$x - -output= /reports/$x.html)
done
```

Обновление Ниппер

В: Nipper сообщает, что требуется обновление "A Nipper update is required".
Nipper может автоматически проверять обновления. Это похоже на автоматическую проверку обновлений Windows или Mac OS X. Вы можете настроить частоту автоматических обновлений на вкладке, используя общие настройки в Nipper (см. ниже).



Для успешного обновления вы должны быть подключены к Интернету для соединения с сервером обновлений Nipper . Если вы получаете сообщение об ошибке, например, "Требуется обновление Nipper ", то Nipper не выполнил обновление. Для устранения этого вы должны убедиться , что Nipper подключен к серверу по Интернету. Если вы используете прокси-сервер сети, то вам необходимо ввести эту информацию во вкладку в настройках, как показано выше.

Примечание: Обновления требуются в некоторых случаях. Лицензия домашнего пользователя требует регулярных обновлений.