Руководство

Переход с устройств Cisco ASA серии 5500 на устройства ASA серии 5500-X среднего уровня

Устройства Cisco ASA серии 5500-X среднего уровня предоставляют множество сервисов безопасности нового поколения. Архитектура оборудования ASA серии 5500-X была перепроектирована для учета потребностей в высокой производительности и необходимости повышения гибкости с одновременным представлением новых сервисов — и все это в прежнем компактном форм-факторе 1RU. Эти изменения следует принять во внимание клиентам, выполняющим переход с платформ ASA серии 5500 на более современное оборудование. В этом документе представлены советы и рекомендации, которых можно придерживаться при миграции на новые устройства ASA серии 5500-X среднего уровня.

В семейство устройств Cisco ASA серии 5500 среднего уровня входят четыре устройства обеспечения безопасности (ASA 5510, ASA 5520, ASA 5540 и ASA 5550). В марте 2012 г. компания Cisco добавила в этот набор еще пять новых устройств среднего уровня. Модели новых устройств можно отличить по индексу «-X»:

- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

Устройства Cisco серии ASA 5500-X предназначены для предоставления сервисов безопасности нового поколения и достижения высоких требований к производительности современных сетей. В их основу положена многоядерная, 64-разрядная архитектура, а для выполнения операций шифрования и обнаружения вторжений используются отдельные выделенные наборы микросхем с поддержкой многоядерности. Аппаратные и программные изменения были внесены без ущерба для компактного форм-фактора устройств.

Путь перехода на оборудование Cisco ASA серии 5500-X

В портфель продуктов Cisco ASA серии 5500 входят четыре платформы на основе единой 32-разрядной процессорной архитектуры. В связи с архитектурными ограничениями эти устройства не могут поддерживать сервисы безопасности нового поколения. В таблице 1 представлен предлагаемый путь перехода на устройства ASA серии 5500-X. Предлагаемый подход является весьма осторожной оценкой.

Таблица 1. Путь перехода с оборудования ASA серии 5500 на ASA серии 5500-X

Устройство ASA серии 5500	Эквивалентное устройство ASA серии 5500-X
ASA 5510	ASA 5512-X
ASA 5510 с лицензией SecPlus	ASA 5515-X или ASA 5512-X с лицензией SecPlus
ASA 5520	ASA 5525-X
ASA 5540	ASA 5545-X
ASA 5550	ASA 5555-X

Путь перехода на программное обеспечение Cisco ASA серии 5500-X

Поддержка ПО для Cisco ASA серии 5500-X доступна в ПО ASA выпуска 8.6 и более позднего. Загрузка более ранних версий ПО ASA на платформы новых устройств будет невозможна.

Планирование успешного перехода

Для упрощения процесса перехода и обеспечения соответствия минимальным требованиям к оборудованию и программному обеспечению необходимо выполнить следующие предмиграционные проверки.

- Лицензии не переносятся автоматически. Перед началом процесса перехода необходимо приобрести все требуемые лицензии и применить их к новым устройствам.
- Для устройств ASA серии 5500-X требуется ПО ASA версии 8.6 или более поздняя. Более ранние версии программного обеспечения не поддерживаются. На новое устройство необходимо загрузить последний выпуск ПО ASA, доступный на веб-сайте Cisco.com.
- Для получения сведений об обновлении версии Cisco Security Manager посетите эту страницу.
- Обновление ПО ASA в существующих устройствах серии 5500 до ПО ASA версии 8.4. Это обновление позволит обновить конфигурацию с отражением миграции лицензий, NAT, фактических IP-адресов и улучшений ACL, представленных в ПО ASA версии 8.3. Если ASA 5500 работает под управлением версии, более ранней чем 8.4, рекомендуется выполнить итерационное обновление с помощью основных редакций. Например, если на устройстве установлено ПО ASA выпуска 7.2, нужно выполнить следующие переходы: 7.2 на 7.4 на 8.0 на 8.2 на 8.4. При использовании этого способа во время обновлений устаревшие функции отслеживаются автоматически.
- Резервное копирование конфигурации с существующего устройства ASA серии 5500 на удаленный компьютер. Это можно сделать с помощью команды CLI «copy» или Cisco Adaptive Security Device Manager (ASDM).
- При наличии модуля сервисов безопасности IPS (SSM) для создания резервной копии конфигурации IPS используется IDM/IME или интерфейс командной строки (CLI).
- Во время резервного копирования конфигурации необходимо экспортировать сертификаты и криптографические ключи со старой платформы.

Перенос лицензий на функции

Лицензии на функции Cisco ASA связаны с серийным номером оборудования. Сведения о лицензиях не включаются в конфигурацию, поэтому при переносе конфигурации с устаревшего оборудования на новое лицензии не переносятся. Прежде чем выполнить процесс перехода, вместо всех лицензий, используемых для старых устройств ASA серии 5500, необходимо приобрести лицензии для нового оборудования ASA серии 5500-X.

Требования к программному обеспечению Cisco ASA для перехода

Для работы всех новых устройств ASA серии 5500-X среднего уровня требуется ПО ASA версии 8.6 или более новая (таблица 2). Более ранние версии не поддерживаются и не будут загружаться на новые платформы.

Таблица 2. Минимальные требования к ПО для перехода с устройств ASA 5500 на устройства ASA 5500-X

Устройство ASA	Минимальная версия ПО	Примечания
ASA серии 5500 (5510, 5520, 5540 и 5550)	ПО ASA версия 8.4.2	Версия 8.6 не поддерживается на этих платформах.
ASA серии 5500-X (5512-X, 5515-X, 5525-X, 5545-X и 5555-X)	ПО ASA версия 8.6	

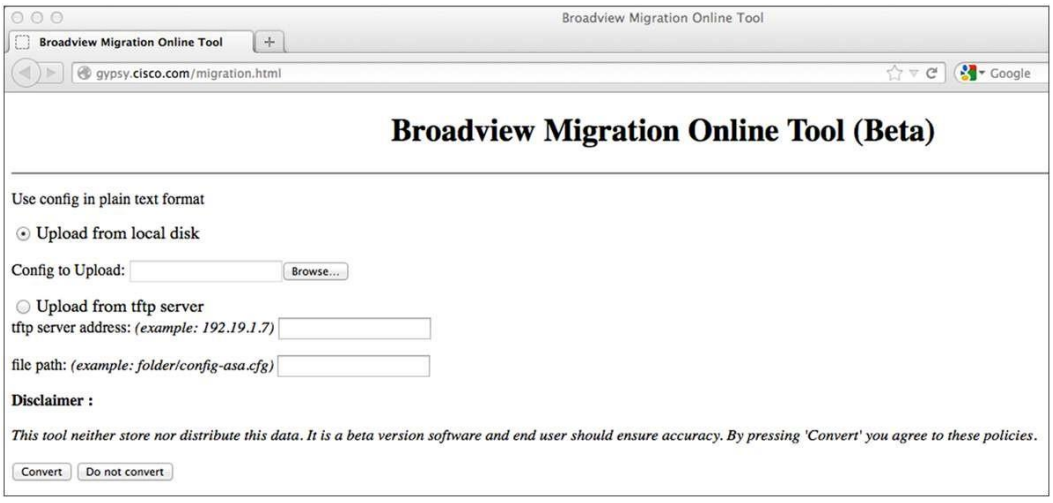
Перед переходом на ASA серии 5500-X устройства ASA серии 5500 необходимо обновить до ПО ASA версии 8.4.2. Подробное описание действий по обновлению см. на странице по адресу: http://www.cisco.com/en/US/docs/security/asa/asa83/upgrading/migrating.html.

Чтобы выполнить обновление устройств ASA серии 5500 до ПО ASA версии 8.4 в автономном режиме, следует воспользоваться внутренним средством миграции, доступном по адресу: http://gypsy.cisco.com/migration.html. Дополнительные сведения об этом средстве представлены в следующем разделе.

Веб-средство миграции NAT для устройств ASA серии 5500

В качестве альтернативного варианта обновления конфигураций ПО ASA предварительного выпуска до ПО ASA версии 8.4 компания Cisco предлагает веб-средство, которое находится по адресу: http://gypsy.cisco.com/migration.html (рис. 1). Для доступа к этому внутреннему средству требуется обратиться в TAC или группу по работе с клиентами.

Веб-средство миграции ПО ASA



Существующую конфигурацию можно отправить с локального компьютера или с удаленного сервера TFTP в корпоративной интрасети Cisco. На заключительном этапе процесса отображается преобразованная конфигурация и журнал миграции. Внимательно изучите журнал, чтобы определить предупреждения или ошибки, возникшие во время переноса. Перенесенную конфигурацию можно скопировать из веб-средства и сохранить в файл.

Средство веб-миграции предназначено для использования в наиболее распространенных сценариях, присутствующих в процессе переноса. При использовании этого средства необходимо учитывать следующие оговорки.

- Средство веб-миграции не создает выходной файл конфигурации. Итоговый результат переноса отображается на веб-странице и требует ручного сохранения (копировать/вставить) в файл для дальнейшего использования.
- Средство не предназначено для переноса многорежимных конфигураций. Оно используется для конфигураций только в режиме маршрутизации или только в прозрачном режиме.
- Средство не было протестировано при работе с большими файлами конфигураций (более 5 Мб).
- Средство нельзя использовать для переноса конфигураций, которые содержат большое количество вложенных объектов и групп объектов, используемых в операторах NAT и списках ACL.

На рис. 2 и 3 показаны примеры постмиграционных выходных результатов.

Рисунок 1. Выходные данные в журнале веб-средства миграции ПО ASA

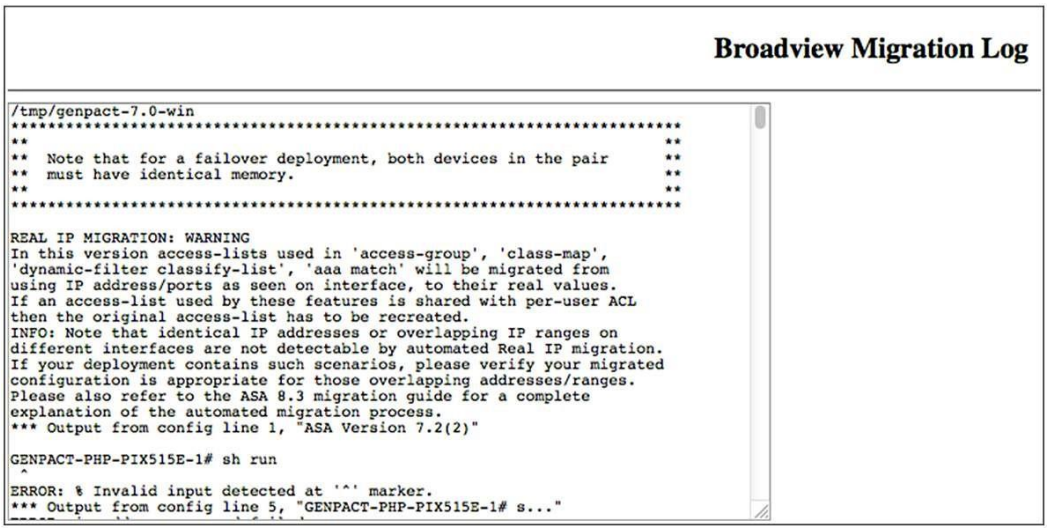
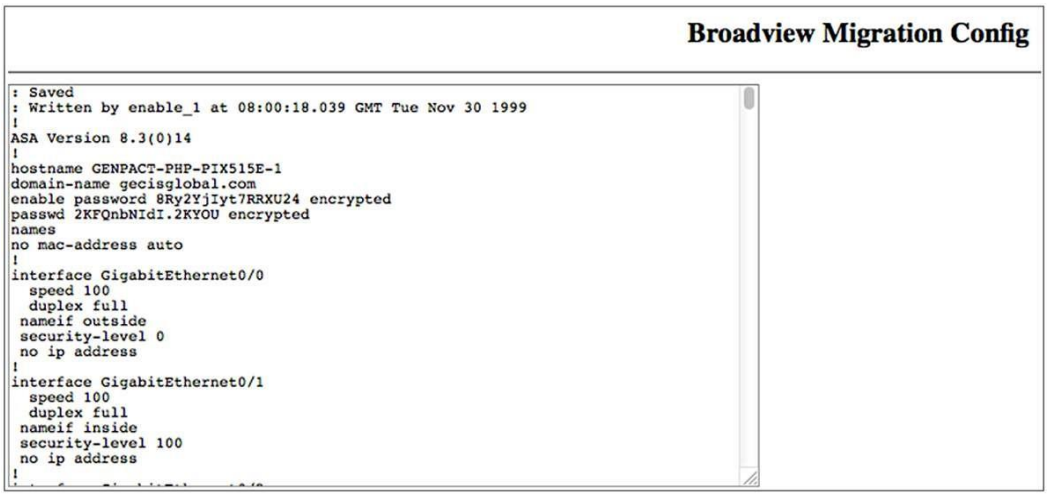


Рисунок 2. Выходная конфигурация в веб-средстве миграции ПО ASA



Предмиграционные проверки на платформе ASA 5500-X

Новые устройства ASA серии 5500-X используют другую аппаратную архитектуру, чем устройства ASA серии 5500. С внешней точки зрения можно заменить изменения в следующих областях.

- Один физический порт управления для управления сервисами ASA и дополнительными сервисами безопасности, такими как IPS.
- Более высокая плотность ввода-вывода на базовой платформе и только портах ввода-вывода Gigabit.
- SSM отсутствует — сервисы работают на основной платформе.

Чтобы при наличии этих архитектурных нововведений выполнить надлежащую миграцию конфигурации, в файл конфигурации ASA серии 5500 требуется внести ряд изменений вручную. Рекомендации по изменению файла конфигурации приводятся в следующих разделах.

Изменения конфигурации порта ввода-вывода

Во всех устройствах ASA серии 5500 (кроме ASA 5510 без лицензии SecPlus) есть порты Gigabit. Предлагаемое далее изменение применяется только к переносам конфигурации с ASA 5510. Во время переноса файла конфигурации все имена интерфейсов (включая подинтерфейсы) следует изменить для отражения портов Gigabit, присутствующих в устройстве ASA 5500-X.

Далее приводится пример изменения интерфейсов для конфигурации 5510, переносимой на устройство 5515-X.

Конфигурация ASA 5510

```
! Physical Interface
  interface Ethernet0/1
  no nameif
  no security-level
  no ip address
  no shutdown
! Creating Subinterfaces on interface E0/1 (two logical networks)
  interface Ethernet0/1.120
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

Измененная конфигурация ASA 5515-X

```
! Physical Interface
  interface GigabitEthernet0/1
  no nameif
  no security-level
  no ip address
  no shutdown
! Creating Subinterfaces on interface G0/1 (two logical networks)
  interface GigabitEthernet0/1.1201
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

Изменения конфигурации порта управления

В устройствах ASA серии 5500-X представлен общий порт управления для сервисов IPS и межсетевой защиты. При переходе с ASA серии 5500 необходимо учитывать следующие ограничения.

- Общий порт управления нельзя использовать как порт данных. Весь трафик, проходящий через устройство и поступающий на порт управления, будет неявным образом отброшен. Этот механизм отключить нельзя.
- Общий порт управления нельзя использовать как часть конфигурации с высоким уровнем доступности.

Если порт управления ASA (M0/0) на устройстве ASA серии 5500 использовался в качестве порта данных, связанная с ним конфигурация должна быть перенесена на один из портов данных Gigabit с номером выше G0/3.

Далее приводится пример конфигурации для переноса с ASA 5520 на ASA 5525-X.

Конфигурация ASA 5520

```
! Dedicated Management Interface
  interface Management0/0
  no nameif
  no security-level
  no ip address
  no management-only
  no shutdown !


! Subinterfaces on interface M0/0
  interface Management0/0.120
  vlan 1222
  nameif fw-out
  security-level 50
  ip address 172.16.61.1 255.255.255.0
```

Конфигурация ASA 5515-X

```
! Dedicated Management Interface
  interface Management0/0
  no nameif
  no security-level
  no ip address
  management-only
  no shutdown


! Management Interface Migrated to GigabitEthernet0/3
  interface GigabitEthernet0/3
  no nameif
  no security-level
  no ip address
  no shutdown

! Subinterfaces on interface G0/3
```

```
interface GigabitEthernet0/3.1201
vlan 1222
nameif fw-out
security-level 50
ip address 172.16.61.1 255.255.255.0
```

Поскольку в ASA серии 5500 нет интерфейса GigabitEthernet0/3 и выше, при миграции на более позднюю версию продукта конфликта конфигураций быть не должно. Аналогично, если интерфейс управления использовался для конфигурации переключения при сбоях, его следует перенести на один из новых неиспользуемых интерфейсов в устройстве ASA 5500-X.

Следующие изменения конфигурации применяются при переносе сервисов ASA и IPS из устройств ASA серии 5500. В устройствах ASA серии 5500 для сервисов ASA и IPS использовались специальные порты управления. В устройствах ASA серии 5500-X для сервисов управления МСЭ и IPS выделен один порт управления. Благодаря изменению архитектуры ввод общего порта управления привел к поддержке нескольких вариантов развертывания. Варианты развертывания описаны в статье по адресу: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_tech_note09186a0080bd5d03.shtml.

Перед реализацией подходящего варианта развертывания и применения изменений конфигурации к новому устройству необходимо внимательно ознакомиться с материалами в указанном выше документе.

Перенос конфигурации IPS

При переносе файла конфигурации IPS не требуются никакие изменения, вносимые вручную. Перед переносом сервиса IPS необходимо внимательно проверить изменения порта управления. К сервису IPS также применяются оговорки лицензирования, действующие для устройств ASA. Процесс активации сервиса IPS состоит из двух этапов и требует использования лицензий для устройства ASA и сервиса IPS. Эти действия описаны в следующей статье на веб-сайте techzone. https://techzone.cisco.com/t5/Intrusion-Preventions-Systems/Troubleshooting-common-ASA-55x5-IPS-K9-Saleen-issues/ta-p/32627.

Заключение

Переход с устройств ASA серии 5500 на новые устройства ASA 5500-X является многоступенчатым процессом, в ходе которого требуется не только использовать средства миграции, но и вносить изменения вручную. В этом документе представлен пошаговый подход, который предназначен для упрощения перехода и позволяет избежать основных проблем, нарушающих функционирование сетевых сервисов.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Отпечатано в США C07-727453-01 05/13