Передовые примеры внедрения политики импорта-экспорта (PIE) в Cisco NAC

Содержание

Введение

Цель этого документа состоит в том, чтобы выделить указания по применению практиченского опыта для обеспечения успешного внедрения функции Экспорта импорта политики (PIE) в NAC Cisco.

Предварительные условия

Требования

Знакомство требуется с диспетчером Cisco NAC Manager (Уберите Access Manager), веб-интерфейс и политика, которая, как правило, настраивается. См. Комментарии к выпуску для Выпуска 4.5 NAC Cisco для того, что и не поддерживается с КРУГОМ.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Программное обеспечение NAC Cisco 4.5.0

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

Рекомендации по оптимальному использованию КРУГА

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

Придерживайтесь рекомендаций, упомянутых ниже для обеспечения успешного внедрения функции Экспорта импорта политики (PIE) CAM.

1. Cisco рекомендует настроить те же параметры настройки автоматического обновления и на ведущем устройстве и на получателе NACMs (под **Управлением устройствами> Чистый Доступ> Обновления> Обновление**), чтобы гарантировать, что все NACMs имеют те же обновления Cisco перед выполнением Синхронизования Политики. Это вызвано тем, что текущие проверки на основной замене, любой проверяет получатель, если вы выполняете обновления Cisco на получателе NACM с другими параметрами настройки автоматического обновления и затем выполняете Синхронизование Политики.
2. Если у вас есть OOB NACM и какое-либо наследство NACM (s) с лицензией IB-only, удостоверьтесь, что вы используете OOB NACM в качестве основного NACM и наследства NACM (s) как приемники.
3. Как только КРУГ включен для конкретного компонента между ведущим устройством и получателем, таблицы/информация получателя полностью заменены информацией, которая выдвинута от ведущего устройства. Это не кумулятивно на стороне получателя. Например, если получатель имеет правило передачи трафика, которое предоставляет доступ к mcafee.com, и у ведущего устройства есть правила передачи трафика, которые предоставляют доступ к cisco.com и abc.com, но никакое правило для mcafee.com, получателя и ведущего устройства не будет иметь идентичные правила, как только выполняется синхронизование: cisco . com и abc.com. Обратите внимание на то, что правило передачи трафика для mcafee.com не существует на получателе после синхронизования, так как у ведущего устройства не было того правила. Оптимальный метод должен настроить основной NACM, как желаемый, но не модифицировать параметры настройки политики на приемниках.
4. Максимальное число поддерживаемых приемников равняется 10. Несмотря на то, что нет никакого технического ограничения к количеству приемников, рекомендации по оптимальному использованию должны поддержать это к поддерживаемому номеру (меньше, чем или равный 10).**Примечание:** Для пар HA NACM параметры настройки Синхронизования Политики отключены для резервного NACM.
5. Ведущее устройство и получатель (получатели) должны выполнить ту же версию NAC Cisco (4.5 или выше) выпуск.

6. Гарантируйте, что у и менеджеров NAC есть подписанные сертификаты Центра сертификации (CA), и и ведущее устройство и получатель доверяют сертификатам друг друга. Сертификаты являются ключевыми для обеспечения синхронизации между ведущим устройством и получателем. Ведущее устройство должно доверять сертификату, представленному получателем и наоборот. Для этого необходимо гарантировать, что у каждого из них есть узел CA их сертификата однорангового узла (полная цепочка, если посредник вовлечен) в доверяемом списке CA. В развертываниях на производстве оптимальный метод должен заменить подписанные сертификаты на Менеджере NAC с подписанными сертификатами CA. Короче говоря, удостоверьтесь, что менеджер NAC, оптимальные методы сертификата SSL встречены перед реализацией КРУГА.
7. Удостоверьтесь, что в вас входят как пользователь Admin Полного управления основному Менеджеру NAC для выполнения автоматического или ручного Синхронизования Политики.
8. Автоматическое синхронизование позволяет вам планировать автоматическое Синхронизование Политики один раз в *X* чисел дней (минимум составляет 1 день). Если вы желаете использовать автоматическое синхронизование для КРУГА, Cisco строго рекомендует, что вы, чтобы выполнить ручное синхронизование и проверить, что синхронизование работает успешно перед включением автоматического синхронизования между менеджерами NAC.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация