ASA: Шикарный Туннель с помощью Примера конфигурации ASDM

Содержание

Введение

Шикарный туннель является соединением между на основе TCP приложение и частный узел, с помощью безклиентого (на основе браузера) сеанс VPN SSL с устройством безопасности как трасса и устройство безопасности как прокси-сервер. Можно определить приложения, к которым вы хотите предоставить умный туннельный доступ и задать локальный путь к каждому приложению. Для приложений, которые работают на Microsoft Windows, можно также потребовать соответствия хэша SHA-1 контрольной суммы как условие для того, чтобы предоставить умный туннельный доступ.

Lotus SameTime и *Microsoft Outlook Express* являются примерами приложений, к которым вы могли бы хотеть предоставить умный туннельный доступ.

Зависящий от того, является ли приложение клиентом или является приложением веб-доступа, умная конфигурация туннеля требует одной из этих процедур:

- Создайте один или несколько умные туннельные списки клиентских приложений, и

затем назначьте список на групповые политики или политику локального пользователя, для кого вы хотите предоставить умный туннельный доступ.
- Создайте одну или более записей списка закладок, которые задают URL приложений веб-доступа, имеющих право на умный туннельный доступ, и затем назначают список на DAP, групповые политики или политику локального пользователя, для кого вы хотите предоставить умный туннельный доступ.Можно также перечислить приложения веб-доступа, для которых можно автоматизировать представление учетных данных входа в систему в умных туннельных соединениях по сеансам VPN SSL без клиента.

Этот документ предполагает, что конфигурация VPN-клиента SSL (SVC) AnyConnect Cisco уже сделана и работает должным образом так, чтобы умная туннельная функция могла быть настроена на существующей конфигурации. Для получения дополнительной информации о том, как настроить VPN-клиента SSL (SVC) AnyConnect Cisco, обратитесь к ASA 8. x: Разрешить раздельное туннелирование для VPN Client AnyConnect на примере конфигурации ASA.

См. Настройку Умная Туннельная Туннельная Политика для получения дополнительной информации о том, как настроить разделенное туннелирование наряду с шикарным туннелем.

Примечание: Удостоверьтесь что шаги *4.b к 4.l* описанный в Конфигурации ASA Использование ASDM 6.0 (2) раздел *ASA 8. x: Позвольте, что Разделенное туннелирование для Клиента AnyConnect VPN Client на Примере конфигурации ASA* не выполнено для настройки умной туннельной функции.

Этот документ описывает настройку интеллектуального туннеля на устройствах адаптивной защиты Cisco ASA серии 5500.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Многофункциональные устройства защиты Cisco ASA серии 5500, который работает под управлением ПО версии 8.0 (2)
- ПК, который выполняет Microsoft Vista, Windows XP SP2 или Windows 2000 Professional SP4 с версией 3.1 Microsoft Installer
- Cisco Adaptive Security Device Manager (ASDM) версии 6.0(2)

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.

Общие сведения

Умная туннельная конфигурация доступа

Умная туннельная таблица показывает умные туннельные списки, каждый из которых определяет одно или более приложений, имеющих право на умный туннельный доступ и его связанную операционную систему (OS). Поскольку каждая групповая политика или поддержки политики локального пользователя один умный туннельный список, необходимо сгруппировать основанные на небраузере приложения, чтобы поддерживаться в умный туннельный список. После конфигурации списка можно назначить его на одного или более полицейских группы или политику локального пользователя.

Примечание: Для получения дополнительной информации об умной конфигурации туннеля обратитесь к Настройке Умный Туннельный Доступ.

Умное туннельное окно (**Конфигурация> VPN для удаленного доступа> Доступ VPN SSL без клиента> Портал> Шикарные Туннели**) позволяет вам завершать эти процедуры:

- **Добавьте умный туннельный список и добавьте приложения на список**Выполните эти шаги, чтобы добавить, что шикарный туннель перечисляет и добавляет приложения на список:**Нажмите Add.**Диалоговое окно Add Smart Tunnel List появляется.**Введите имя списка и нажмите Add.**ASDM открывает Добавление Умной Туннельной коробки Диалогового окно Создать нового VPN-подключение, которая позволяет вам назначать атрибуты шикарного туннеля к списку.После присвоения желаемых атрибутов для шикарного туннеля нажмите **OK**.ASDM отображает те атрибуты в списке.Повторите эти шаги по мере необходимости, чтобы завершить список, и затем нажать **OK** в диалоговом окне Add Smart Tunnel List.
- **Измените умный туннельный список**Выполните эти шаги для изменения умного туннельного списка:Дважды нажмите список или выберите список в таблице и нажмите **Edit**.**Нажмите Add**, чтобы вставить новый набор умных атрибутов туннеля в список или выбрать запись в списке и нажать **Edit** или **Delete**.
- **Удалите список**Для удаления списка выберите список в таблице и нажмите **Delete**.
- **Добавьте закладку**После конфигурации и присвоения умного туннельного списка, можно сделать шикарный туннель простым в использовании путем добавления закладки для сервиса и нажатия **Разрешения Умной опции Tunnel** в диалоговом окне Add или Edit Bookmark.

Умный туннельный доступ позволяет клиенту на основе TCP приложение для использования на основе браузера VPN-подключение для соединения с сервисом. Это предлагает следующие преимущества пользователям, по сравнению с плагинами и устаревшей технологией, переадресацией портов:

- Шикарный туннель предлагает лучшую производительность, чем плагины.
- В отличие от переадресации портов, шикарный туннель упрощает пользовательский опыт, не требует подключения пользователя локального приложения к локальному порту.
- В отличие от переадресации портов, шикарный туннель не требует, чтобы у

пользователей были администраторские привилегии.

Умные туннельные требования, ограничения и ограничения

Общие требования и ограничения

Шикарный туннель имеет следующие общие требования и ограничения:

- Удаленный хост, инициирующий шикарный туннель, должен выполнить 32-разрядную версию Microsoft IE Windows Vista, Windows XP или Windows 2000; или Mac OS 10.4 или 10.5.
- Шикарный туннель автоматический вход в систему поддерживает только Microsoft Internet Explorer на Windows.
- Браузер должен быть включен с Java, Microsoft ActiveX или обоими.
- Шикарный туннель поддерживает только прокси, размещенные между компьютерами, которые выполняют Microsoft Windows и устройство безопасности. Шикарный туннель использует конфигурацию Internet Explorer (т.е. та, предназначенная для использования в масштабе всей системы в Windows). Если удаленный компьютер требует, чтобы прокси-сервер достиг устройства безопасности, URL завершающегося конца соединения должен быть в списке URL, исключенных из сервисов proxy. Если настройка прокси указывает, что трафик, предназначенный для ASA, проходит прокси, весь умный туннельный трафик проходит прокси.В основанном на HTTP сценарии удаленного доступа иногда подсеть не предоставляет пользовательский доступ к Шлюзу VPN. В этом случае прокси, размещенный перед ASA для маршрутизации трафика между сетью и местоположением конечного пользователя, предоставляет веб - доступ. Однако только пользователи VPN могут настроить прокси, размещенные перед ASA. При выполнении так, они должны удостовериться, что эти прокси поддерживают метод ПОДКЛЮЧЕНИЯ. Для прокси, которые требуют аутентификации, шикарный туннель поддерживает только основной тип аутентификации Дайджеста.
- Когда шикарный туннель запускается, туннели устройства безопасности, весь трафик от браузера обрабатывает пользователя, использовали инициировать безклиентый сеанс. Если пользователь запускает другой экземпляр процесса браузера, он передает весь трафик в туннель. Если процесс браузера является тем же, и устройство безопасности не предоставляет доступ к данному URL, пользователь не может открыть его. Как обходной путь, пользователь может использовать другой браузер от того, используемого для установления безклиентого сеанса.
- Перехват управления при отказе с синхронизацией состояния не сохраняет умные туннельные соединения. Пользователи должны воссоединиться после аварийного переключения.

Windows Requirements и ограничения

Следующие требования и ограничения применяются к Windows только:

- Только Winsock 2, на основе TCP приложения имеют право на умный туннельный доступ.
- Устройство безопасности не поддерживает Exchange Microsoft Outlook (MAPI) прокси.

Ни переадресация портов, ни шикарный туннель не поддерживают MAPI. Для связи Exchange Microsoft Outlook с помощью протокола MAPI удаленные пользователи должны использовать AnyConnect.
- Пользователи Microsoft Windows Vista, которые используют шикарный туннель или переадресацию портов, должны добавить URL ASA к зоне Надежного узла. Для доступа к зоне Надежного узла запустите Internet Explorer, и выберите **Tools> Internet Options** и нажмите **Вкладку Безопасность**. Пользователи Vista могут также отключить Защищенный режим для облегчения умного туннельного доступа; однако, Cisco рекомендует против этого метода, потому что это увеличивает уязвимость для нападения.

Требования Mac OS и ограничения

Эти требования и ограничения применяются к Mac OS только:

- Safari 3.1.1 или позже или Firefox 3.0 или позже
- Sun JRE 1.5 или позже
- Только приложения, запущенные из страницы портала, могут установить умные туннельные соединения. Это требование включает умную туннельную поддержку Firefox. Использование Firefox для начала другого экземпляра Firefox во время первого использования шикарного туннеля требует профиля пользователя, названного csco_st. Если этот профиль пользователя не присутствует, сеанс побуждает пользователя создавать тот.
- Приложения с помощью TCP, которые динамично связаны с библиотекой SSL, могут переработать шикарный туннель.
- Шикарный туннель не поддерживает эти функции и приложения на Mac OS:Сервисы proxyАвтоматический вход в системуПриложения, которые используют двухуровневые пространства именОснованные на консоли приложения, такие как Telnet, SSH и ЗАВИХРЕНИЕПриложения с помощью dlopen или dlsym для определения местоположения вызовов libsocketСтатически связанные приложения для определения местоположения вызовов libsocket

Настройка

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.

Добавьте или отредактируйте умный туннельный список

Диалоговое окно Add Smart Tunnel List позволяет вам добавить список умных туннельных записей в настройку устройства защиты. Диалоговое окно Edit Smart Tunnel List позволяет вам модифицировать содержание списка.

Поле

Имя списка — Вводит уникальное имя для списка приложений или программ. Нет никакого ограничения на количество символов на название. Не используйте пробелы. После конфигурации умного туннельного списка имя списка появляется рядом с Умным Туннельным Атрибутом списка в групповых политиках VPN SSL без клиента и политике локального пользователя. Назначьте название, которое поможет вам отличать его содержание или цель из других списков, которые вы, вероятно, настроите.

Добавьте или отредактируйте умную туннельную запись

Добавление или Редактирует Умное Туннельное окно Диалогового окно Создать нового VPN-подключение, позволяет вам задать атрибуты приложения в умном туннельном списке.

- **Идентификатор приложения** — Вводит строку для именования записи в умном туннельном списке. Строка уникальна для ОС. Как правило, это называет приложение, которое будет предоставлено умный туннельный доступ. Для поддержки нескольк версий приложения, для которого вы принимаете решение задать другие пути или значения хеш-функции, можно использовать этот атрибут для дифференциации записей, задавая ОС и название и версию приложения, поддерживаемого каждой записью списка. Строка может составить до 64 символов.
- **Имя процесса** — Вводит имя файла или путь к приложению. Строка может составить до 128 символовWindows требует, чтобы полное соответствие этого значения к правой части пути приложения на удаленном хосте квалифицировало приложение к умному туннельному доступу. При определении только имени файла для Windows VPN SSL не принуждает ограничение местоположения на удаленный хост для квалификации приложения к умному туннельному доступу.Если вы задаете путь, и пользователь установил приложение в другом местоположении, то приложение не квалифицирует. Приложение может находиться на любом пути пока правая часть совпадений строки значение, которое вы вводите.Для открытия доступ приложению для умного туннельного доступа, если он присутствует на одном из нескольких путей на удаленном хосте или задайте только название и расширение приложения в этом поле или создайте уникальную умную туннельную запись для каждого пути.Для Windows, если вы хотите добавить, умный туннельный доступ к приложению запустился с командной строки, необходимо указать, что "cmd.exe" в имени процесса одной записи в шикарном туннеле перечисляют и задают путь к самому приложению в другой записи, потому что "cmd.exe" является родителем приложения.Mac OS требует полного пути к процессу и учитывает регистр. Во избежание определения пути для каждого имени пользователя вставьте тильду (~) перед частичным путем (например, ~/bin/vnc).
- **ОС** — Нажмите Windows или Mac для определения хоста ОС приложения.
- **Хэш** — (*Дополнительный и применимый только для Windows*) для получения этого значения, введите контрольную сумму исполняемого файла в утилиту, которая вычисляет хэш с помощью алгоритма SHA-1. Одним примером такой утилиты является Microsoft File Checksum Integrity Verifier (FCIV), которая доступна в http://support.microsoft.com/kb/841290/. После установки FCIV разместите временную копию приложения, которое будет хешировано на пути, который не содержит пробелов (например, c:/fciv.exe), затем введите приложение fciv.exe-sha1 в командную строку (например, fciv.exe-sha1 c:\msimn.exe) для отображения хэша SHA-1.Хэш SHA-1 всегда является 40 шестнадцатеричными символами.Прежде, чем открыть доступ приложению для умного туннельного доступа, VPN SSL без клиента вычисляет хэш приложения,

совпадающего с идентификатором приложения. Если результат совпадает со значением хэша, это квалифицирует приложение к умному туннельному доступу.Ввод хэша предоставляет разумное обеспечение, что VPN SSL не квалифицирует незаконный файл, который совпадает со строкой, которую вы задали в идентификаторе приложения. Поскольку контрольная сумма меняется в зависимости от каждой версии или исправления приложения, хэш, который вы вводите, может только совпасть с одной версией или исправлением на удаленном хосте. Для определения хэша для нескольких версий приложения создайте уникальную умную туннельную запись для каждого значения хеш-функции.**Примечание:** Необходимо обновить умный туннельный список в будущем, если вы вводите значения хеш-функции, и вы хотите поддержать последующие версии или исправления приложения с умным туннельным доступом. Внезапной проблемой с умным туннельным доступом могла бы быть индикация, что приложение, которое содержит значения хеш-функции, не актуально с обновлением приложения. Можно избежать этой проблемы, не введя хэш.

- Как только вы настраиваете умный туннельный список, необходимо назначить его на групповую политику или политику локального пользователя для нее становиться активным следующим образом:Для присвоения списка на групповую политику выберите **Config> Remote Access VPN> Clientless SSL VPN Access> Group Policies> Add или Edit> Portal**, и выберите умное имя туннеля из выпадающего списка рядом с Умным Туннельным Атрибутом списка.Для присвоения списка на политику локального пользователя выберите **Config> Remote Access VPN> AAA Setup> Local Users> Add или Edit> VPN Policy> Clientless SSL VPN**, и выберите умное имя туннеля из выпадающего списка рядом с Умным Туннельным Атрибутом списка.

ASA шикарный туннель (пример Lotus) конфигурация Использование ASDM 6.0 (2)

Этот документ предполагает, что базовая конфигурация, такая как конфигурация интерфейса, завершена и работает должным образом.

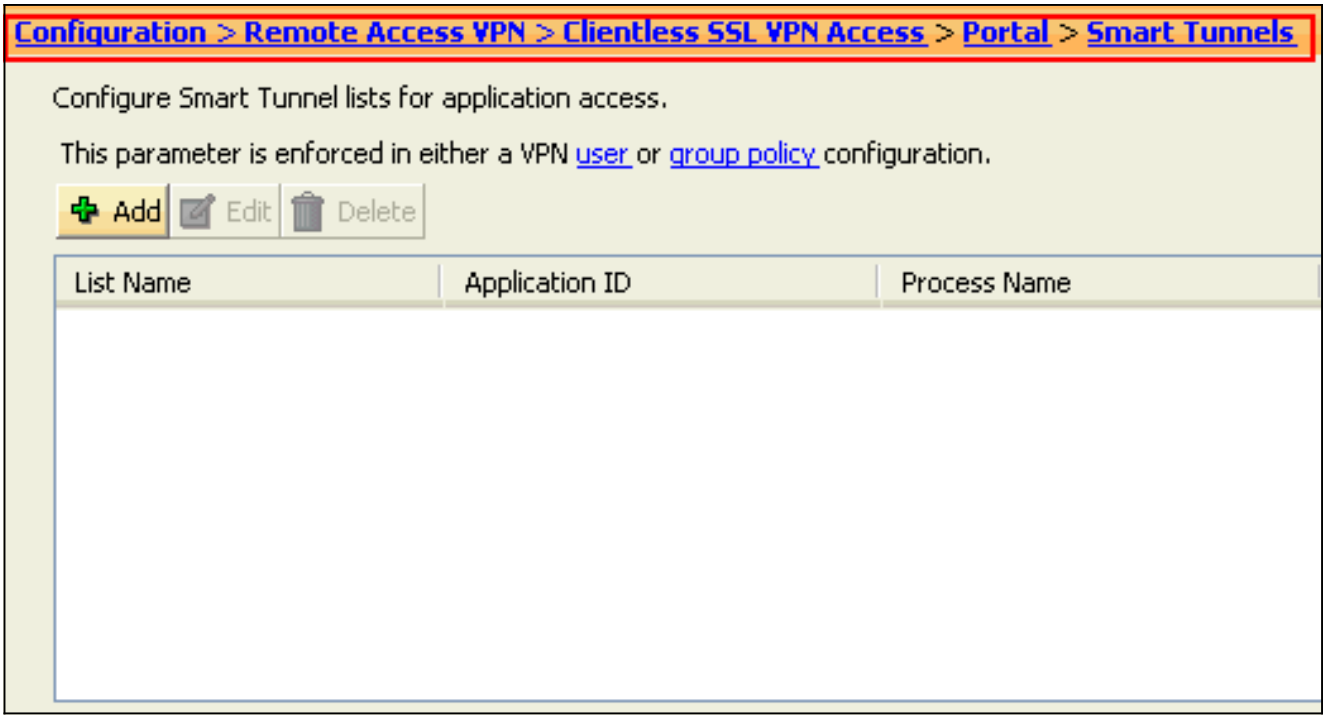
Примечание: Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

Примечание: Нельзя включать WebVPN и ASDM на одном и том же интерфейсе ASA, если не изменены номера портов. Для получения дополнительных сведений обратитесь к документу Включение ASDM и WebVPN на одном и том же интерфейсе ASA.

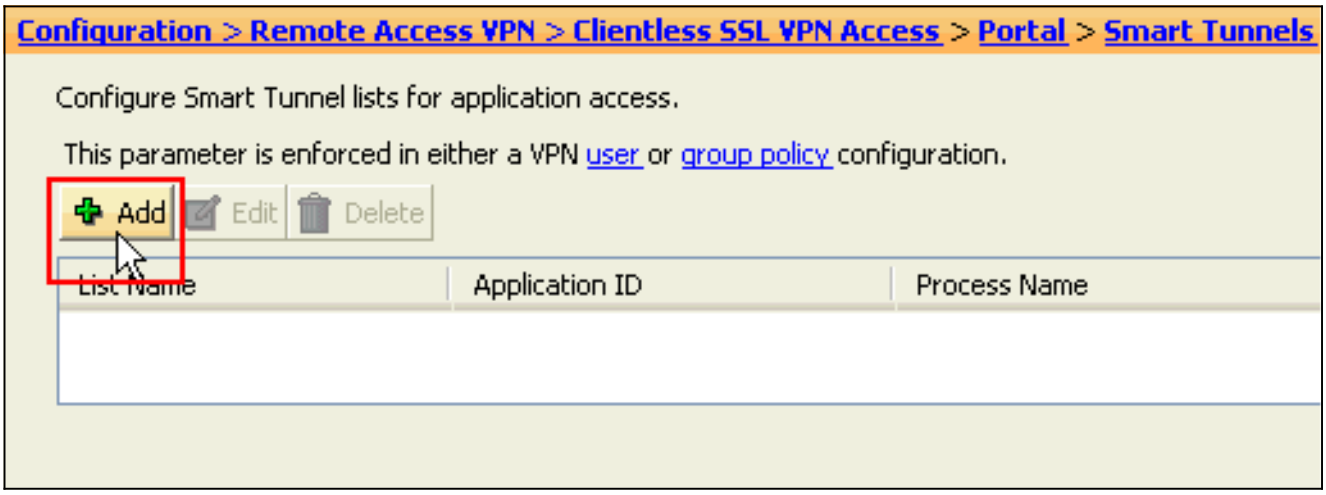
Выполните эти шаги для настройки шикарного туннеля:

Примечание: В этом примере конфигурации шикарный туннель настроен для приложения Lotus.

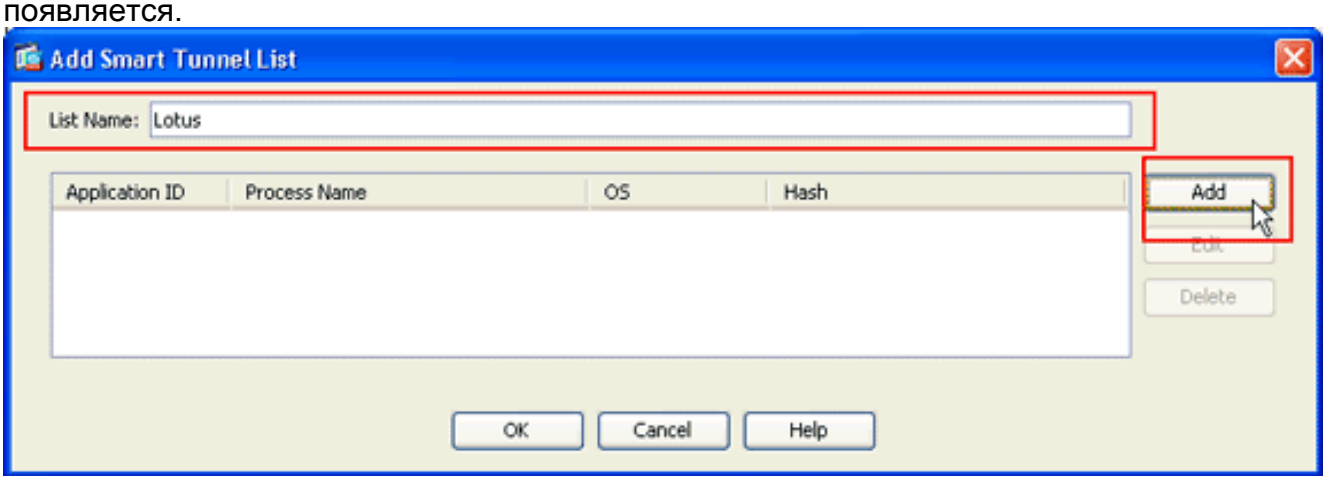
1. Выберите **Configuration> Remote Access VPN> Clientless SSL VPN Access> Portal> Smart Tunnels** для начала Умной Конфигурации туннеля.



2. **Нажмите Add.**

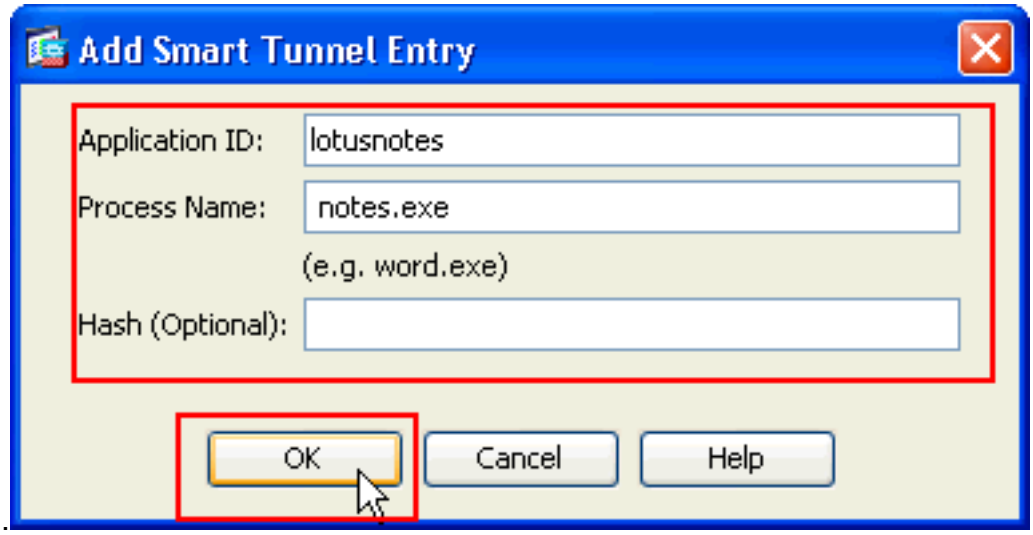


Диалоговое окно Add Smart Tunnel List появляется.

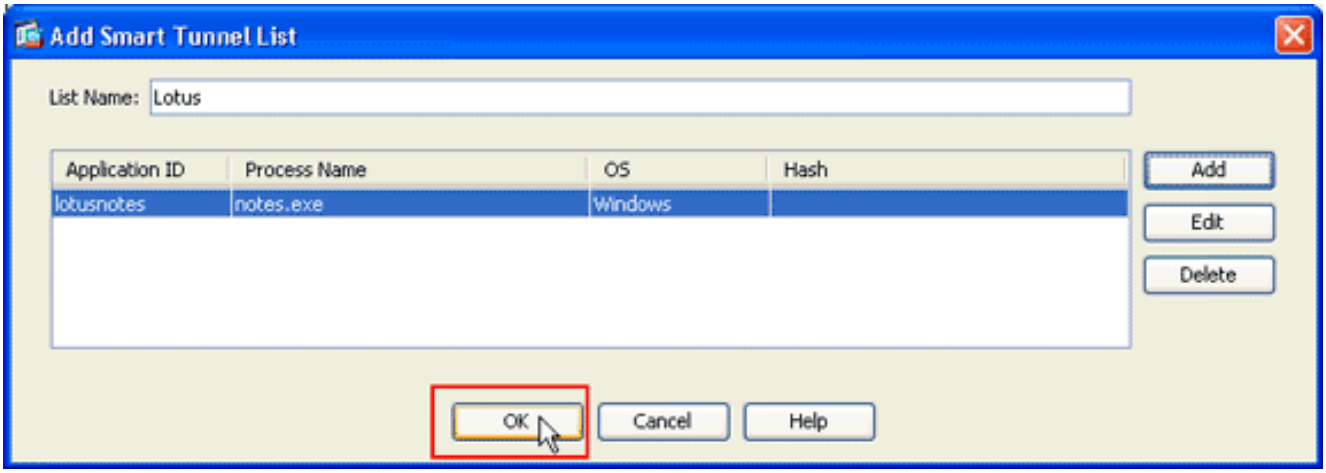


3. В диалоговом окне Add Smart Tunnel List **нажмите Add**.Добавление Умной Туннельной коробки Диалогового окно Создать нового VPN-подключение

появляется.

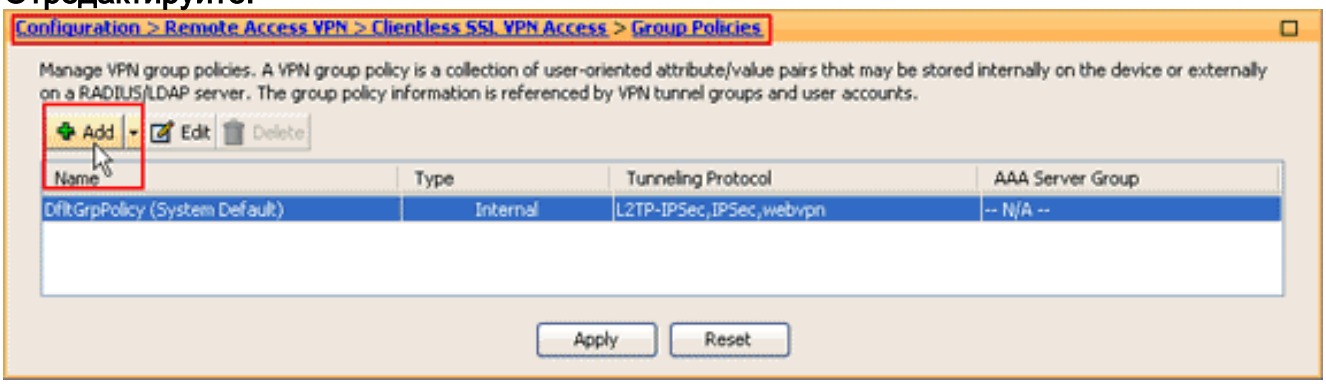


4. В поле Application ID введите строку для определения записи в рамках умного туннельного списка.
5. Введите имя файла и расширение для приложения, и нажмите **OK**.
6. В диалоговом окне Add Smart Tunnel List нажмите **OK**.

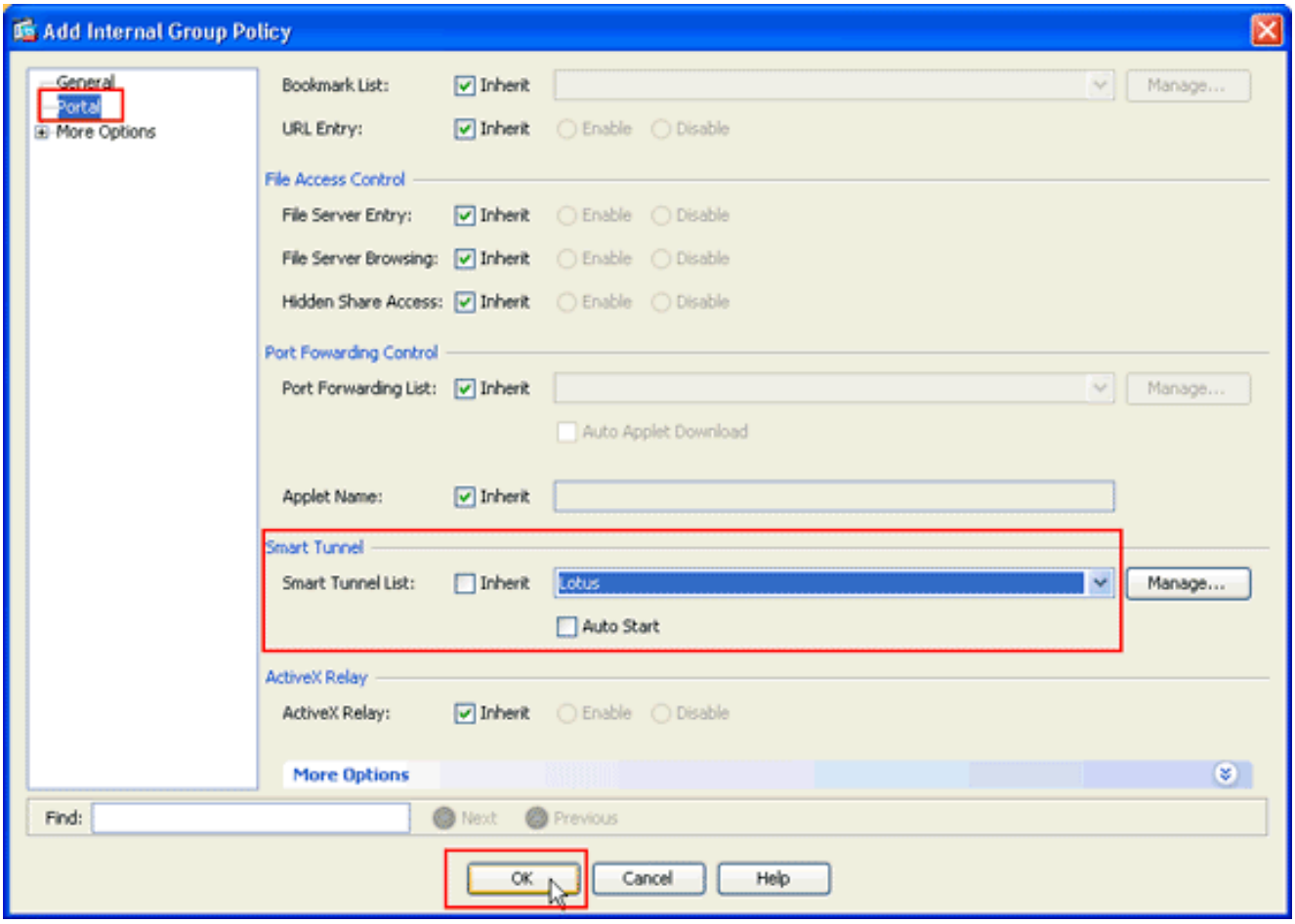


Примечание: Вот команда эквивалентной конфигурации CLI:

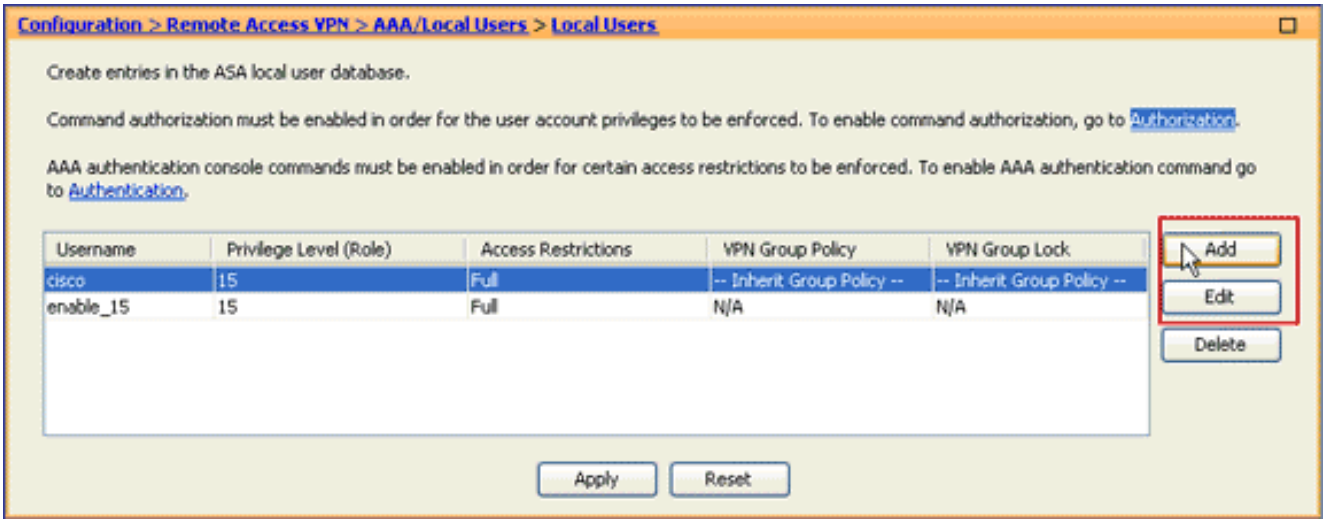
7. Назначьте список на групповые политики и политику локального пользователя, которой вы хотите предоставить умный туннельный доступ к связанным приложениям следующим образом:Для присвоения списка на групповую политику выберите **Configuration> Remote Access VPN> Clientless SSL VPN Access> Group Policies**, и **нажмите Add** или **Отредактируйте.**



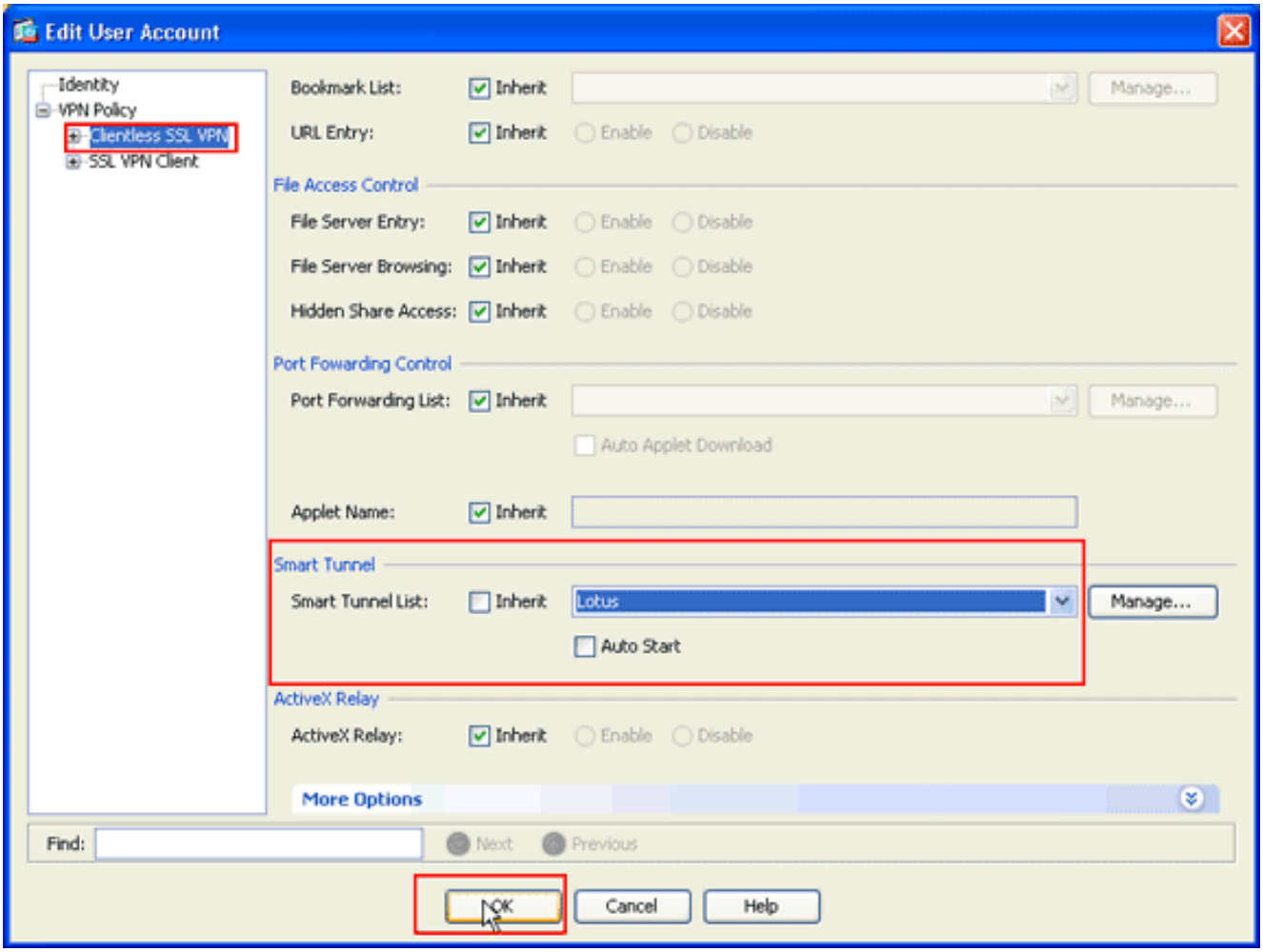
Откроется диалоговое окно Add Internal Group Policy (Добавление внутренней групповой
политики).



8. В диалоговом окне Add Internal Group Policy нажмите **Portal**, выберите умное имя туннеля из Умного Туннельного выпадающего списка Списка и нажмите **OK**.**Примечание:** Данный пример использует *Lotus* в качестве умного туннельного имени списка.
9. Для присвоения списка на политику локального пользователя выберите **Configuration> Remote Access VPN> AAA Setup> Local Users** и **нажмите Add** для настройки, настраивают нового пользователя или нажимают **Edit** для редактирования существующего пользователя.



Диалоговое окно Edit User Account появляется.



10. В диалоговом окне Edit User Account нажмите **Clientless SSL VPN**, выберите умное имя туннеля из Умного Туннельного выпадающего списка Списка и нажмите **OK**.**Примечание:** Данный пример использует *Lotus* в качестве умного туннельного имени списка.

Умная конфигурация туннеля завершена.

Устранение неполадок

Я неспособен подключить использование отмеченного Умного Туннельного URL в безклиентом портале. Почему эта проблема происходит, и как я могу решить его?

Эта проблема происходит из-за проблемы, описанной в идентификаторе ошибки Cisco CSCsx05766 (только зарегистрированные клиенты). Для решения этого вопроса понизьте плагин Среды исполнения Java до более старой версии.

Я могу исказить URL умной туннельной ссылки, настроенной в WebVPN?

Когда шикарный туннель используется на ASA, вы не можете исказить URL или скрыть строку адреса браузера. Пользователи могут просмотреть URL ссылок, настроенных в WebVPN, которые используют шикарный туннель. В результате они могут изменить порт и обратиться к серверу для некоторого другого сервиса.

Для решения этого вопроса используйте ACL WebType. См. Создание ACL WebType для

получения дополнительной информации.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Комментарии к выпуску для клиента AnyConnect VPN Client, выпуска 2.3
- Пример настройки SSL клиента VPN (SVC) на ASA с ASDM
- Cisco Systems – техническая поддержка и документация