Пример конфигурации "Thin-Client SSL VPN (WebVPN) IOS с SDM"

Содержание

Введение

Технология тонкого клиента SSL VPN может использоваться для предоставления защищенного доступа приложениям, использующим статические порты. Примеры: Telnet (23), SSH (22), POP3 (110), IMAP4 (143) и SMTP (25). Тонкий клиент может управляться на уровне пользователей, политик или обоими способами. Доступ может быть настроен на уровне отдельных пользователей или путем создания групповых политик, включающих одного или нескольких пользователей. Технология SSL VPN может быть настроена в трех основных режимах: бесклиентская сеть SSL VPN (WebVPN), тонкий клиент SSL VPN (переадресация портов) и клиент SSL VPN (SVC / режим полного туннеля).

1. Бесклиентская сеть SSL VPN (WebVPN).

На удаленном клиенте необходим только web-браузер с поддержкой SSL для доступа к web-серверам корпоративной локальной сети, поддерживающим протокол HTTP или HTTPS. Кроме того, файловая система Common Internet File System (CIFS) предоставляет доступ к файлам Windows. Хороший пример реализации HTTP-доступа — клиент Outlook Web Access (OWA).

Дополнительную информацию о бесклиентской сети SSL VPN см. в документе Пример конфигурации бесклиентской сети SSL VPN (WebVPN) на Cisco IOS с SDM.

2. Тонкий клиент SSL VPN (переадресация портов).

На удаленном клиенте необходимо загрузить небольшой Java-апплет, который обеспечивает безопасный доступ для TCP-приложений, использующих статические номера портов. Протокол UDP не поддерживается. Поддерживаемые протоколы: POP3, SMTP, IMAP, SSH и Telnet. Пользователю необходимы локальные административные привилегии, так как производятся изменения в файлах локальной машины. Этот вариант SSL VPN

неприменим для приложений, использующих динамическое назначение портов, например для некоторых FTP-приложений.

3. Клиент SSL VPN (SVC / режим полного туннеля).

На удаленную рабочую станцию загружается небольшой клиент, который обеспечивает полный защищенный доступ к ресурсам внутренней корпоративной сети. Клиент SVC может загружаться на удаленный узел на постоянной основе или удаляться по завершении защищенного сеанса.

Дополнительные сведения о клиенте SSL VPN см. в разделе Пример конфигурации клиента SSL VPN (SVC) на IOS с SDM.

В этом документе демонстрируется простая конфигурация SSL VPN с тонким клиентом на маршрутизаторе на базе Cisco IOS® . Режим SSL VPN с тонким клиентом действует на следующих маршрутизаторах Cisco IOS:

маршрутизаторы Cisco серий 870, 1811, 1841, 2801, 2811, 2821 и 2851;

маршрутизаторы Cisco серий 3725, 3745, 3825, 3845, 7200 и 7301.

Предварительные условия

Требования

Рассматриваемая процедура настройки предполагает выполнение следующих условий:

Требования для маршрутизатора Cisco IOS

Любой из перечисленных маршрутизаторов с загруженным SDM и расширенным образом IOS версии 12.4(6)T или выше.

Станция управления с загруженным SDM.

Новые маршрутизаторы Cisco поставляются с предустановленной копией SDM. Если на вашем маршрутизаторе ПО SDM не установлено, его можно загрузить в разделе загрузок ПО Cisco Security Device Manager. Для этого необходима учетная запись CCO и контракт на обслуживание. Дополнительные сведения см. в разделе Настройка маршрутизатора с помощью диспетчера устройств защиты.

Требования для клиентского компьютера

Рекомендуется наличие у удаленных клиентов прав локального администратора.

Удаленные клиенты должны иметь среду исполнения Java (JRE) версии 1.4 или выше.

Удаленные клиентские браузеры: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari

1.2.2 или Firefox 1.0

Cookie-файлы активированы, всплывающие окна разрешены на удаленных клиентах.

Используемые компоненты

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

Расширенный корпоративный образ ПО (Cisco Advanced Enterprise Software Image) версии 12.4(9)T.

Маршрутизатор с интегрированными сервисами Cisco 3825.

Диспетчер маршрутизаторов Cisco и устройств защиты (SDM) версии 2.3.1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все описываемые в данном документе устройства были запущены со стандартными заводскими настройками. При работе в действующей сети необходимо понимать последствия выполнения любой команды. IP-адреса, используемые для этой конфигурации, относятся к пространству адресов RFC 1918. Они недействительны в Интернете.

Условные обозначения

Подробные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

Задача

В этом разделе содержатся сведения, необходимые для настройки функций, описанных в данном документе.

Схема сети

В настоящем документе используется следующая схема сети:

Настройка SSL VPN с тонким клиентом

Настройте SSL VPN с тонким клиентом в системе Cisco IOS, используя мастера в интерфейсе диспетчера устройств защиты (SDM), либо настройте его вручную. В последнем случае можно использовать интерфейс командной строки (CLI) или ручные операции в приложении SDM. В этом примере используется мастер.

Перейдите на вкладку **Configure** (Настройка).

На панели навигации выберите **VPN > WebVPN**.

Выберите вкладку **Create WebVPN** (Создать WebVPN).

Установите переключатель в положение **Create a new WebVPN** (Создать новое соединение WebVPN).

Нажмите кнопку **Launch the selected task** (Запустить выбранную задачу).

Запустится мастер WebVPN. Нажмите кнопку **Next** (Далее).

Введите IP-адрес и уникальное имя данного шлюза WebVPN. Нажмите кнопку **Next** (Далее).

Экран User Authentication (Аутентификация пользователя) позволит предусмотреть аутентификацию пользователей. В этой конфигурации используется учетная запись, созданная локально на маршрутизаторе. Можно использовать сервер аутентификации, авторизации и учета (AAA).

Для добавления пользователя нажмите кнопку **Add** (Добавить).

На экране Add an Account (Добавление учетной записи) введите сведения о пользователе и нажмите кнопку **OK**.

На экране User Authentication (Аутентификация пользователя) нажмите кнопку **Next** (Далее).

Экран мастера WebVPN позволяет настроить web-сайты интрасети, но мы пропускаем этот шаг, потому что для доступа данного приложения используется переадресация портов. Если нужно разрешить доступ к web-сайтам, используйте бесклиентскую конфигурацию или полноценный клиент SSL VPN. Их применение выходит за рамки этого документа.

Нажмите кнопку **Next** (Далее). The Wizard displays a screen that allows configuration of the Full Tunnel client. К SSL VPN с тонким клиентом (переадресацией портов) этот режим не относится.

Снимите флажок **Enable Full Tunnel** (Разрешить полный туннель). Нажмите кнопку **Next** (Далее).

Настройте внешний вид портала WebVPN или подтвердите внешний вид по умолчанию.

Нажмите кнопку **Next** (Далее).

Ознакомьтесь со сводкой конфигурации и выберите **Finish > Save** (Готово > Сохранить).

Создан шлюз WebVPN и контекст WebVPN со связанной групповой политикой. Настройте порты тонкого клиента, которые станут доступны при подключении клиентов к WebVPN.

Выберите **Configure** (Настройка).

Выберите **VPN > WebVPN**.

Выберите **Create WebVPN** (Создать WebVPN).

Выберите переключатель **Configure advanced features for an existing WebVPN** (Настроить дополнительные функции существующего соединения WebVPN) и выберите **Launch the selected task** (Запустить выбранную задачу).

Экран приветствия знакомит с возможностями мастера. Нажмите кнопку **Next** (Далее).

В раскрывающихся меню выберите контекст WebVPN и группу пользователей. Нажмите кнопку **Next** (Далее).

Выберите **Thin Client (Port Forwarding)** (Тонкий клиент [Переадресация портов]) и нажмите кнопку **Next** (Далее).

Введите ресурсы, которые нужно сделать доступными через переадресацию портов. Порт службы должен быть статическим портом, но можно принять порт по умолчанию на клиентском ПК, назначенный мастером. Нажмите кнопку **Next** (Далее).

Ознакомьтесь со сводкой конфигурации и выберите **Finish > OK > Save** (Готово > OK > Сохранить).

Конфигурация

Итоговая конфигурация SDM.

ausnml-3825-01

Проверка

Проверка конфигурации

Этот раздел позволяет убедиться, что конфигурация работает правильно.

С клиентского компьютера обратитесь к шлюзу WebVPN по адресу **https://ip-адрес_шлюза**. Не забудьте включить имя домена WebVPN, если создавались уникальные контексты WebVPN. Например, если создан домен sales, введите **https://ip-адрес_шлюза/sales**.

Войдите и примите сертификат, предлагаемый шлюзом WebVPN. Щелкните **Start Application Access** (Запустить доступ к приложению).

Появится экран Application Access (Доступ к приложению). KHsfh получить доступ к приложению с локальным номером порта и IP-адресом локального кольцевого интерфейса. Например, для установления сеанса Telnet с маршрутизатором 1 наберите: **telnet 127.0.0.1 3001**. Небольшой Java-апплет посылает эту информацию шлюзу WebVPN, который затем связывает обе стороны сеанса по защищенному каналу. Успешные подключения могут привести к увеличению счетчиков в столбцах **Bytes Out** (Отправлено байт) и **Bytes In** (Получено байт).

Команды

С WebVPN связано несколько команд **show**. Эти команды можно ввести в интерфейсе командной строке (CLI) для отображения статистики и другой информации. Использование команд **show** подробно иллюстрируется в разделе Проверка конфигурации WebVPN.

Интерпретатор выходных данных (OIT), доступный только зарегистрированным пользователям, поддерживает некоторые команды **show**. Посредством OIT можно анализировать выходные данные команд **show**.

Поиск и устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

На клиентских компьютерах должна быть загружена среда выполнения SUN Java версии 1.4 или выше. Копию этого ПО можно получить на сайте загрузки ПО Java.

Команды для устранения неполадок

Примечание. Перед использованием команд **debug** ознакомьтесь с документом Важные сведения о командах debug.

show webvpn ? — с WebVPN связано множество команд **show**. Они запускаются из командной строки и отображают статистику и другие данные. Использование команд **show** подробно иллюстрируется в разделе Проверка конфигурации WebVPN.

debug webvpn ? — использование команд **debug** может неблагоприятно сказаться на работе маршрутизатора. Подробные сведения об использовании команд **debug** см. в разделе Использование команд отладки WebVPN.

Дополнительные сведения

- Cisco IOS SSLVPN
- SSL VPN – WebVPN
- Cisco IOS WebVPN. Вопросы и ответы
- Cisco Systems — техническая поддержка и документация