ASA 8. X: AnyConnect был запущен до того, как была настроена возможность входа в систему

Содержание

Введение

С включенным *запуском перед входом (SBL)* пользователь видит, что GUI AnyConnect входит в систему диалоговое окно, прежде чем появится диалоговое окно входа в систему Windows®. При этом вначале устанавливается VPN-подключение. Функция запуска перед входом в систему доступна только для платформ Windows и позволяет администратору управлять использованием сценариев регистрации, кэшированием паролей, назначением сетевых дисков локальным устройствам и другими параметрами. Можно использовать функцию SBL для включения VPN в рамках последовательности входа в систему. По умолчанию функция SBL отключена.

Для получения дополнительной информации о настройке функций Клиента AnyConnect VPN Client обратитесь к Характеристикам клиента AnyConnect Настройки раздела.

Примечание: В клиенте AnyConnect единственная конфигурация, которую вы реализовываете для SBL, должна активировать опцию. Администраторы сети обрабатывают обработку, которая продолжается перед входом в систему, основанным на

требованиях их ситуации. Сценарии входа в систему могут быть назначены на домен или отдельным пользователям. Обычно администраторам домена определили пакетные файлы и т.п. с пользователями или группами в Active Directory. Как только входы пользователя в систему на, выполняется сценарий регистрации.

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, которые работают под управлением ПО версии 8. x
- Версия VPN 2.0 AnyConnect Cisco

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

Точка SBL - то, что он подключает удаленный компьютер с инфраструктурой компании до входа в систему ПК. Например, пользователь может быть вне физической корпоративной сети, неспособной обратиться к корпоративным ресурсам, пока его ПК не присоединился к корпоративной сети. С включенным SBL подключения клиента AnyConnect, прежде чем пользователь видит, что Microsoft входит окно. Когда окно входа в систему Microsoft появляется, пользователь должен также войти, как обычно, к Windows.

Это несколько причин использовать SBL:

- ПК пользователя соединен с инфраструктурой Active Directory.
- Если групповая политика запрещает кэшированные учетные данные т.е. у пользователя не может быть кэшированных учетных данных на ПК.
- Пользователь должен выполнить сценарии регистрации, которые выполняются от сетевого ресурса или которые требуют доступа к сетевому ресурсу.
- У пользователя есть сетевые сопоставленные дисководы, которые требуют аутентификации с инфраструктурой Active Directory.
- Сетевые компоненты, такие как NAC NAP/CS MS, могут потребовать соединения с

инфраструктурой.

SBL создает сеть, которая эквивалентна включению в локальный корпоративный ЛВС. С включенным SBL, так как у пользователя есть доступ к локальной инфраструктуре, сценарии входа в систему, которые обычно работают для пользователя в офисе, также доступны удаленному пользователю.

Для получения информации о том, как создать сценарии входа в систему, обратитесь к этой статье Microsoft TechNet.

Для получения информации о том, как использовать локальные сценарии входа в систему в Windows XP, обратитесь к этой статье microsoft.

В другом примере система может быть настроена для запрещения кэшированных учетных данных для входа в систему ПК. В этом сценарии пользователи должны быть в состоянии связаться с контроллером домена на корпоративной сети для их учетных данных, которые будут проверены до доступа к ПК. SBL требует, чтобы сетевое подключение присутствовало в то время, когда он вызван. В некоторых случаях это не возможно, потому что беспроводное соединение может зависеть от учетных данных пользователя для соединения с беспроводной инфраструктурой. Так как режим SBL предшествует учетной фазе входа в систему, соединение не доступно в этом сценарии. В этом случае беспроводное соединение должно быть настроено для кэширования учетных данных через вход в систему, или другая беспроводная аутентификация должна быть настроена для SBL для работы.

Установите запускаются перед компонентами входа в систему (Windows Only)

Запуск Перед компонентами Входа в систему должен быть установлен после того, как базовый клиент был установлен. Кроме того, AnyConnect 2.2 Запускается, Прежде чем компоненты Входа в систему требуют, чтобы была установлена версия 2.2, или позже, базового клиентского программного обеспечения AnyConnect. Если вы предварительно развертываете клиента AnyConnect и Запуск Перед компонентами Входа в систему с файлами MSI (например, вы в крупной компании, которая имеет ее собственное развертывание ПО (Altiris, Active Directory или CM), необходимо разобраться в заказе. Заказ установки обрабатывается автоматически, когда администратор загружает AnyConnect, если это - развернутая сеть и/или обновленная сеть. Для получения информации о полной установке обратитесь к Комментариям к выпуску для Cisco AnyConnect VPN Client, Выпуска 2.2.

Различия между Windows-Vista\Windows 7 и предварительной перспективой запускаются перед входом в систему

Процедуры для включения SBL расходятся немного в системах Windows 7 и Windows Vista. Системы перед перспективой используют компонент, названный виртуальной частной сетью графическая идентификация и аутентификация (VPNGINA) для реализации SBL. Vista и системы Windows 7 используют компонент под названием PLAP для реализации SBL.

В клиенте AnyConnect Запускается Windows Vista, Прежде чем функция Входа в систему известна как Поставщик услуг доступа перед входом в систему (PLAP), который является соединяемым учетным поставщиком. Эта функция позволяет администраторам сети

выполнить определенные задачи, такие как набор учетных данных или соединения с сетевыми ресурсами, до входа в систему. PLAP предоставляет, Запускаются Перед функциями Входа в систему на Windows Vista, Windows 7 и сервере Windows 2008. PLAP поддерживает 32-разрядные и 64-разрядные версии операционной системы с vpnplap.dll и vpnplap64.dll, соответственно. Функция PLAP поддерживает Windows Vista x86 и x64 версии.

Примечание: В этом разделе VPNGINA обращается к Запуску Перед функцией Входа в систему платформ перед Vista, и PLAP обращается к Запуску Перед функцией Входа в систему систем Windows 7 и Windows Vista.

В системах перед Vista Запустите, Прежде чем Вход в систему использует компонент, известный как VPN, которую Графическая Идентификация и Опознавательная Библиотека динамических каналов (vpngina.dll) для обеспечения Запускают Перед возможностями Входа в систему. Компонент Windows PLAP, который является частью Windows Vista, заменяет компонент Windows GINA.

Когда пользователь нажимает сочетание клавиш Ctrl+Alt+Del, GINA активирован. С PLAP сочетание клавиш Ctrl+Alt+Del открывает окно, где пользователь может принять решение или войти в систему или активировать любые Сетевые подключения (компоненты PLAP) с Сетевой Кнопкой соединения в нижнем правом углу окна.

Разделы, которые сразу придерживаются, описывают параметры настройки и процедуры и для VPNGINA и для PLAP SBL. Для полного описания включения и использования функции SBL (PLAP) на платформе Windows Vista, обратитесь к Настройке, Запускаются Перед Входом в систему (PLAP) в Системах Windows Vista.

Параметры настройки XML для включения SBL

Значение элемента для UseStartBeforeLogon позволяет этой функции быть включенной (истинная) или от (лжи). Если вы устанавливаете это значение в True в профиле, дополнительная обработка происходит как часть последовательности входа в систему. Посмотрите Запуск Перед описанием Входа в систему для дополнительных сведений. Заставьте <Вход в систему UseStartBefore> значение в файле CiscoAnyConnect.xml к **истине** включать SBL:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

Для отключения SBL установите то же значение в False.

Для активации опции UserControllable используйте этот оператор при включении SBL:

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

Любой параметр пользователя, привязанный к этому атрибуту, сохранен в другом месте.

Включите SBL

Для уменьшения времени загрузки загрузки запросов клиента AnyConnect (от устройства безопасности) только основных модулей, в которых это нуждается для каждой функции, которую это поддерживает. Для включения новых характеристик, таких как SBL, необходимо задать название модуля с **командой svc modules** от групповой политики WebVPN или режим

конфигурации WebVPN имени пользователя:

```
[no] svc modules {none | value string}
```

Строковое значение для SBL является **vpngina**.

В данном примере администратор сети переходит в режим атрибутов group-policy для дистанционных пользователей компьютера групповой политики; переходит в режим конфигурации WebVPN для групповой политики; и задает строку VPNGINA для включения SBL:

```
hostname(config)# group-policy telecommuters attributes hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

Кроме того, администратор должен гарантировать, что AnyConnect <profile.xml> файл, где <profile.xml> название, которое администратор сети назначил на XML-файл, **устанавливали** оператор <UseStartBeforeLogon> в True, например:

```
UseStartBeforeLogon UserControllable="false">true
```

Система должна быть перезагружена, прежде Запускаются, Прежде чем Вход в систему вступает в силу. Необходимо также указать на устройстве безопасности, что вы хотите позволить SBL или любые другие модули для дополнительных характеристик. См. описание в Модулях Включения для Дополнительных Функций AnyConnect, страница 2-5 (ASDM) раздел или Модули Включения для Дополнительных Функций AnyConnect, страница 3-4 (CLI) для получения дополнительной информации.

Запустите перед конфигурацией входа в систему с CLI

Этот сценарий показывает вам, как установить XML-файл с CLI:

1. Создайте профиль, который будет оттолкнут к клиентским компьютерам, который выглядит подобным этому:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```
2. Скопируйте файл к Флэшу на устройстве безопасности:

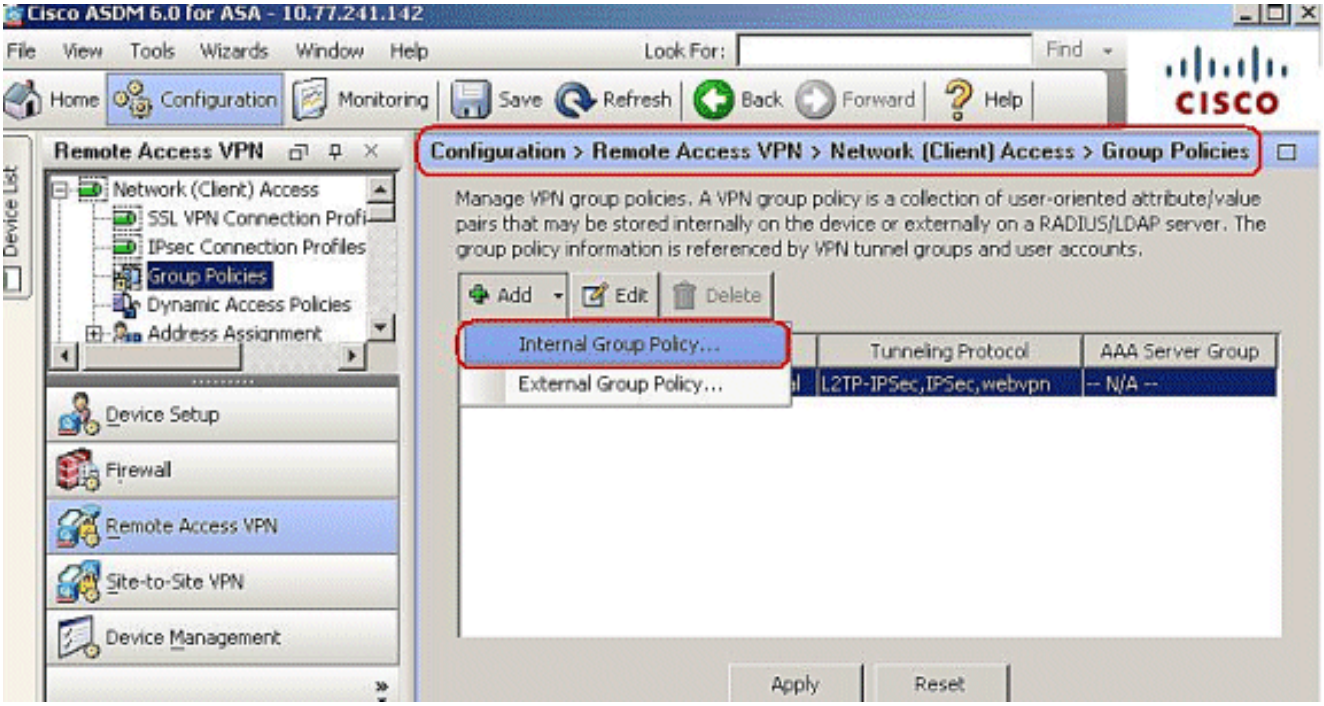
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

3. На устройстве безопасности добавьте профиль как доступный профиль к глобальному разделу WebVPN, пока все остальное установлено правильно для Соединений AnyConnect:`hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml`
4. Отредактируйте групповую политику, которую вы используете и добавляете **команды модули обращения к операционной системе и svc profile**:`hostname(config)# group-policy GroupPolicy internal hostname(config)# group-policy GroupPolicy attributes hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc modules value vpngina hostame(config-group-webvpn)# svc profiles value ReallyNewProfile`

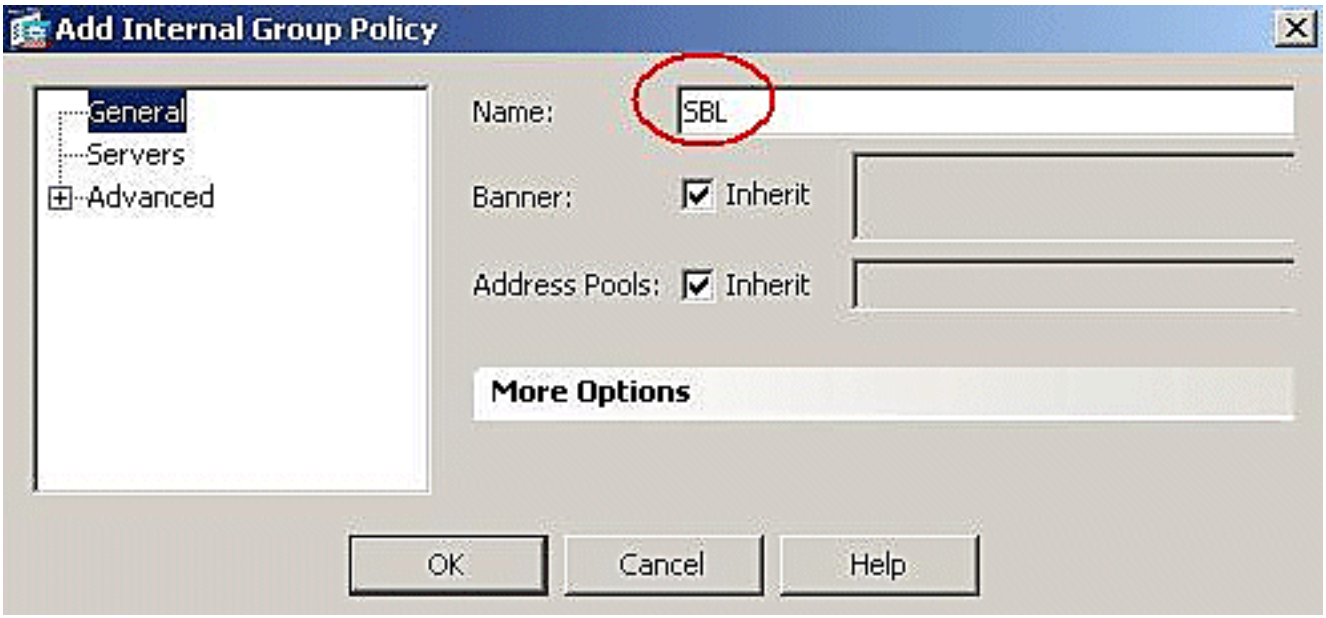
Запустите перед конфигурацией входа в систему с ASDM

Выполните эти шаги для настройки SBL с ASDM:

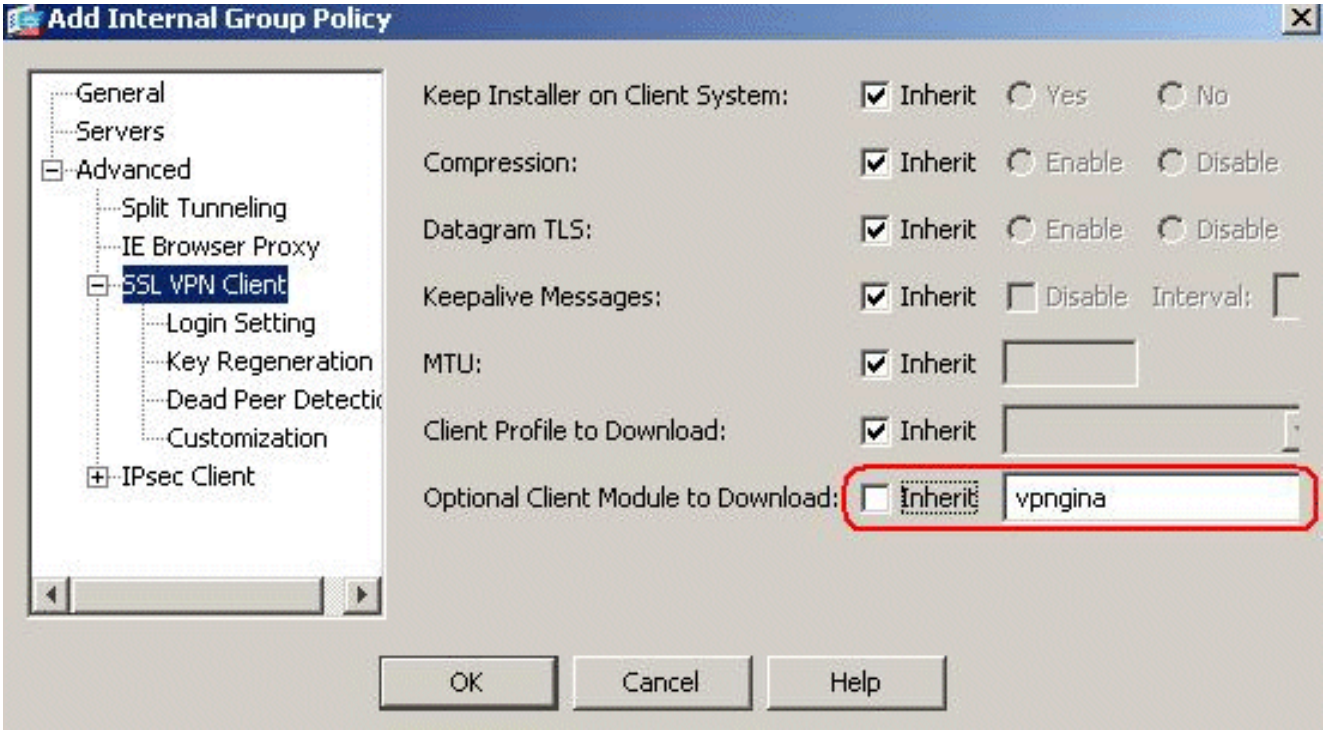
1. Создайте профиль, который будет оттолкнут к клиентским компьютерам, который выглядит подобным этому:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```
2. Сохраните профиль как **AnyConnectProfile.xml** в локальном компьютере.
3. Запустите ASDM и перейдите к Домашней странице.
4. Перейдите **к Конфигурации> VPN для удаленного доступа> сетевой доступ (клиент)>, Групповые политики> Добавляют** и нажимают **Internal Group Policy**.



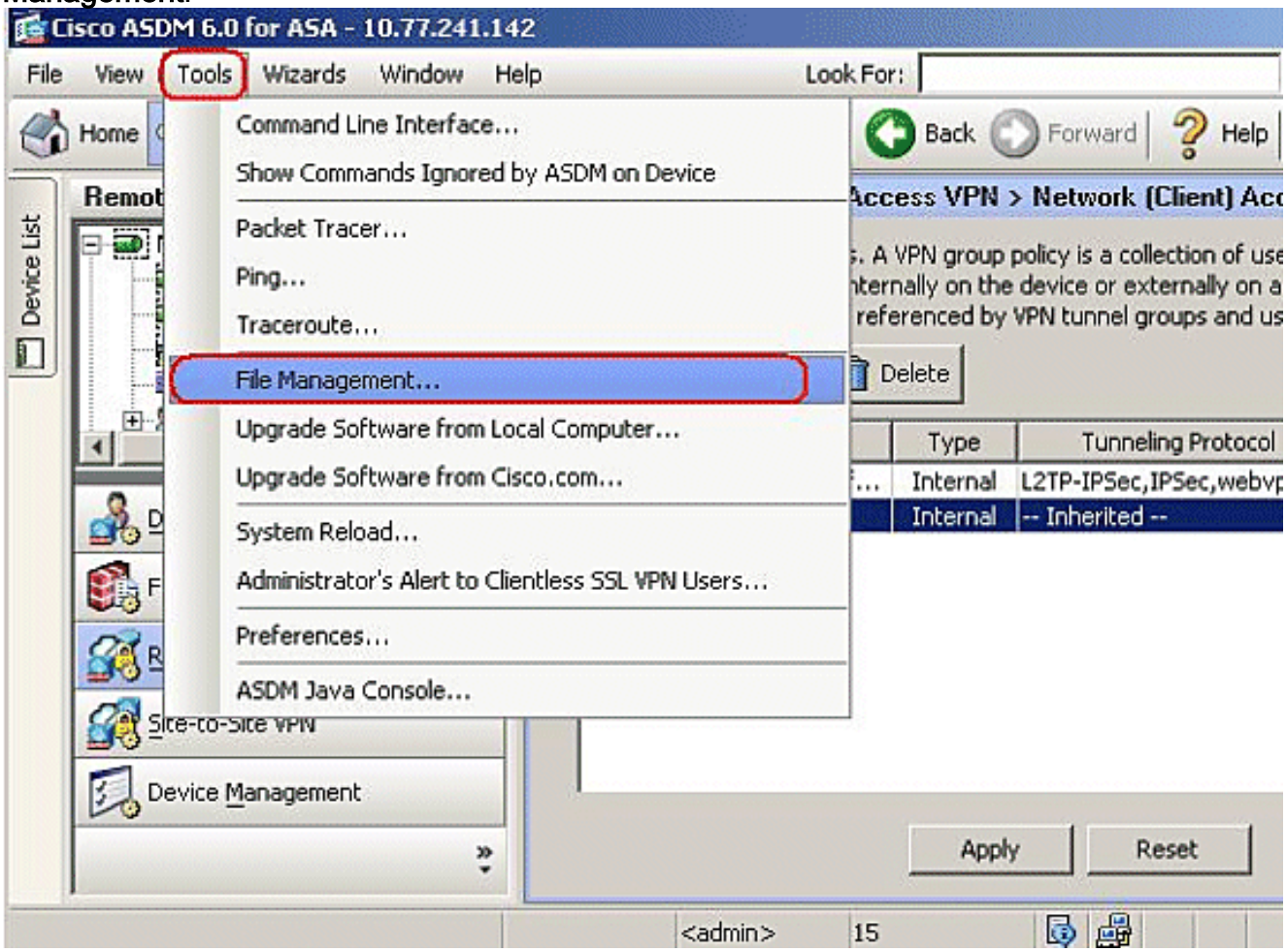
5. Введите имя групповой политики, например, **SBL**.



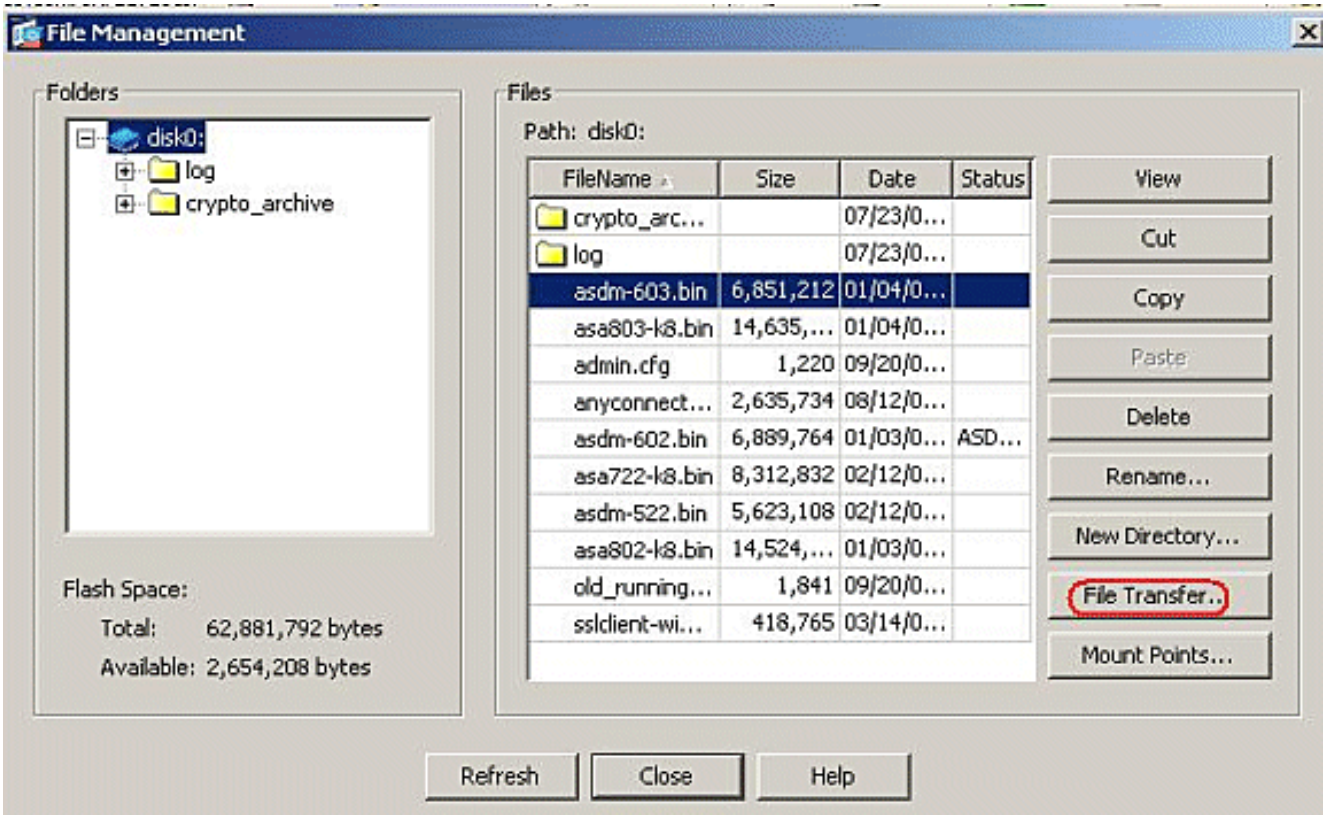
6. Перейдите **Усовершенствованный> VPN-клиент SSL (SVC)**. Удалите Наследовать метку выбора в **Дополнительном Клиентском модуле, чтобы Загрузить**, и выбрать **vpngina** из раскрывающегося окна.



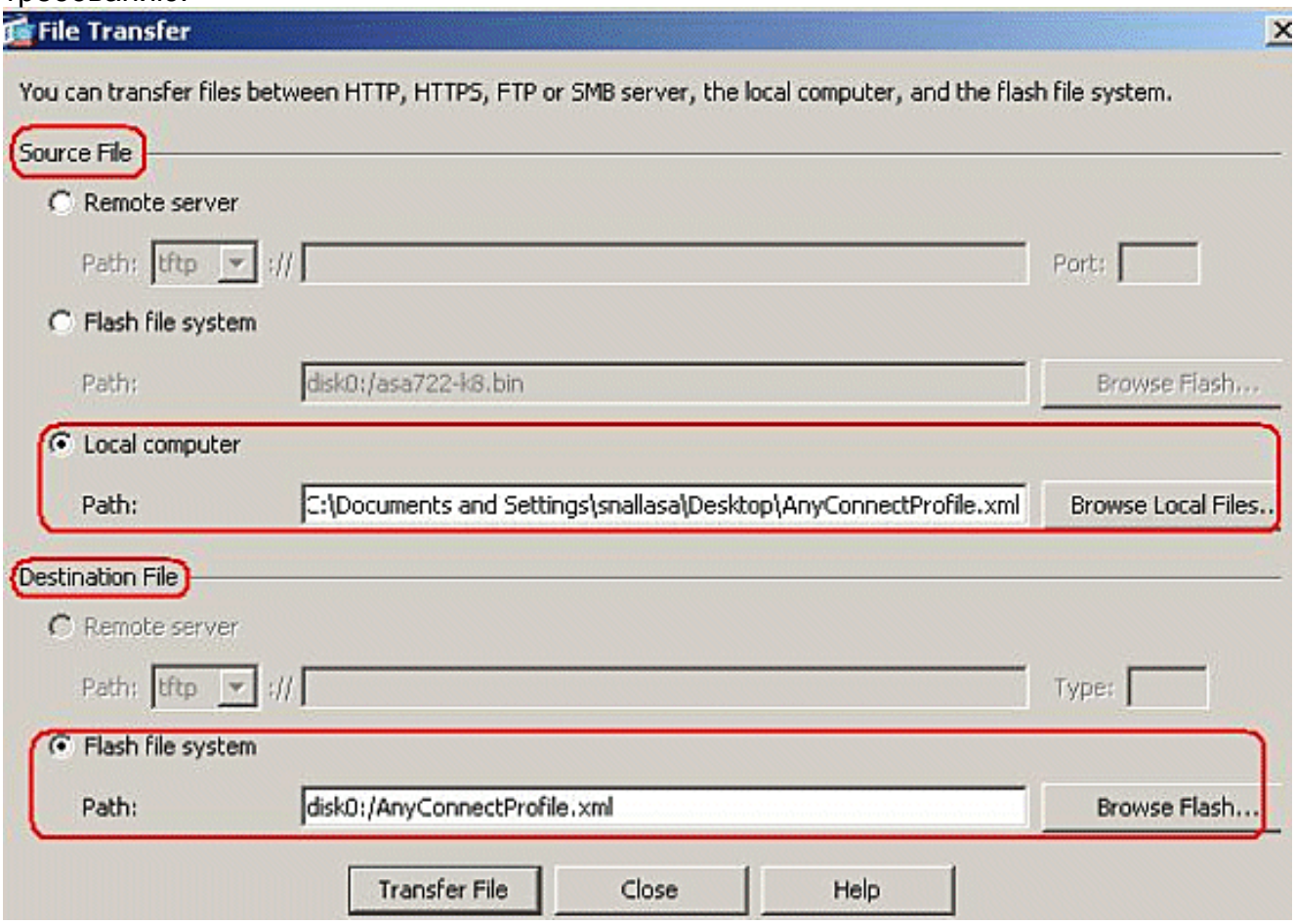
7. Для передачи профиля **AnyConnectProfile.xml** от локального компьютера до Флэша перейдите **к Программным средствам** и нажмите **File Management**.



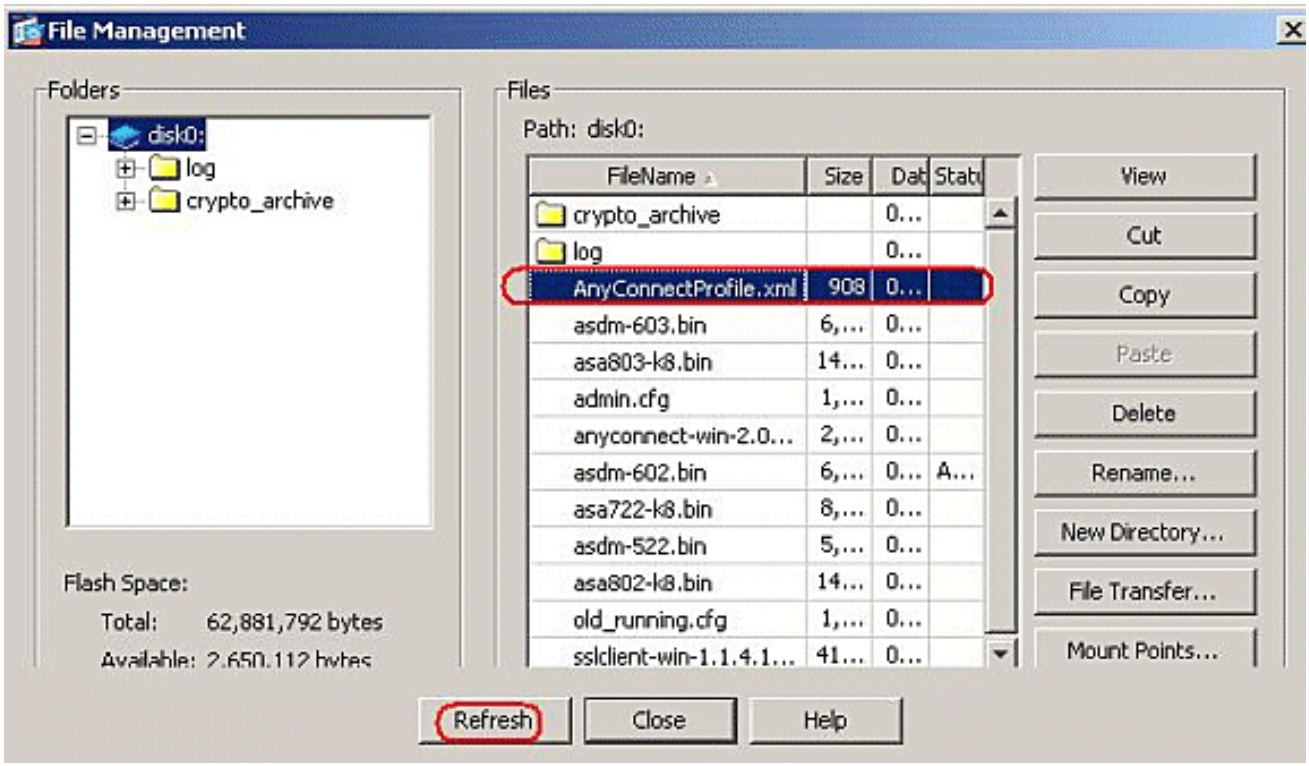
8. Нажмите кнопку **File Transfer**.



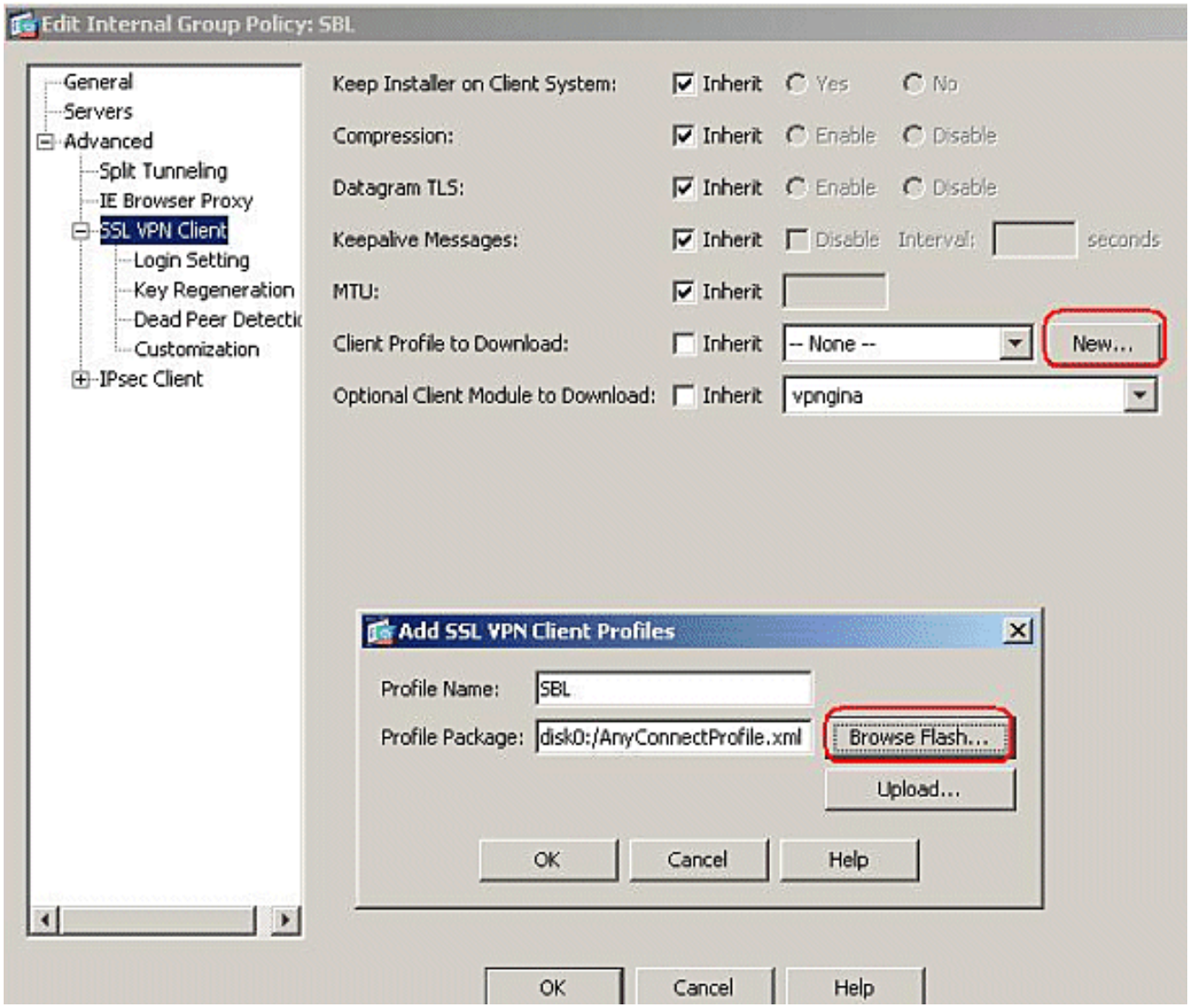
9. Для передачи профиля от локального компьютера до флэш-памяти ASA выберите **Source File**, путь XML-файла (локальный компьютер) и путь **Файла получателя** согласно требованию.



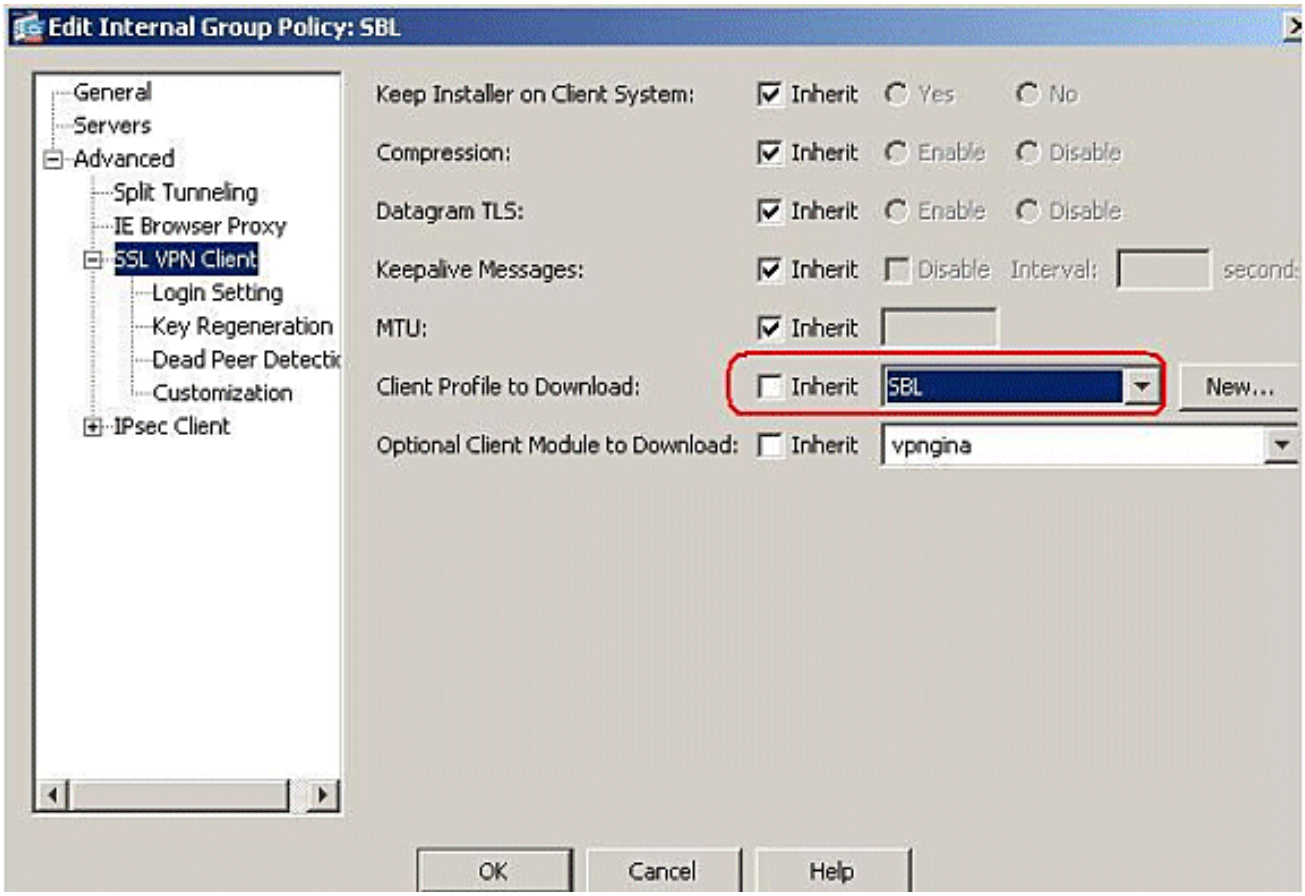
10. После передачи нажмите **Кнопку Обновить**, чтобы проверить, является ли файл конфигурации во флэш-
памяти.



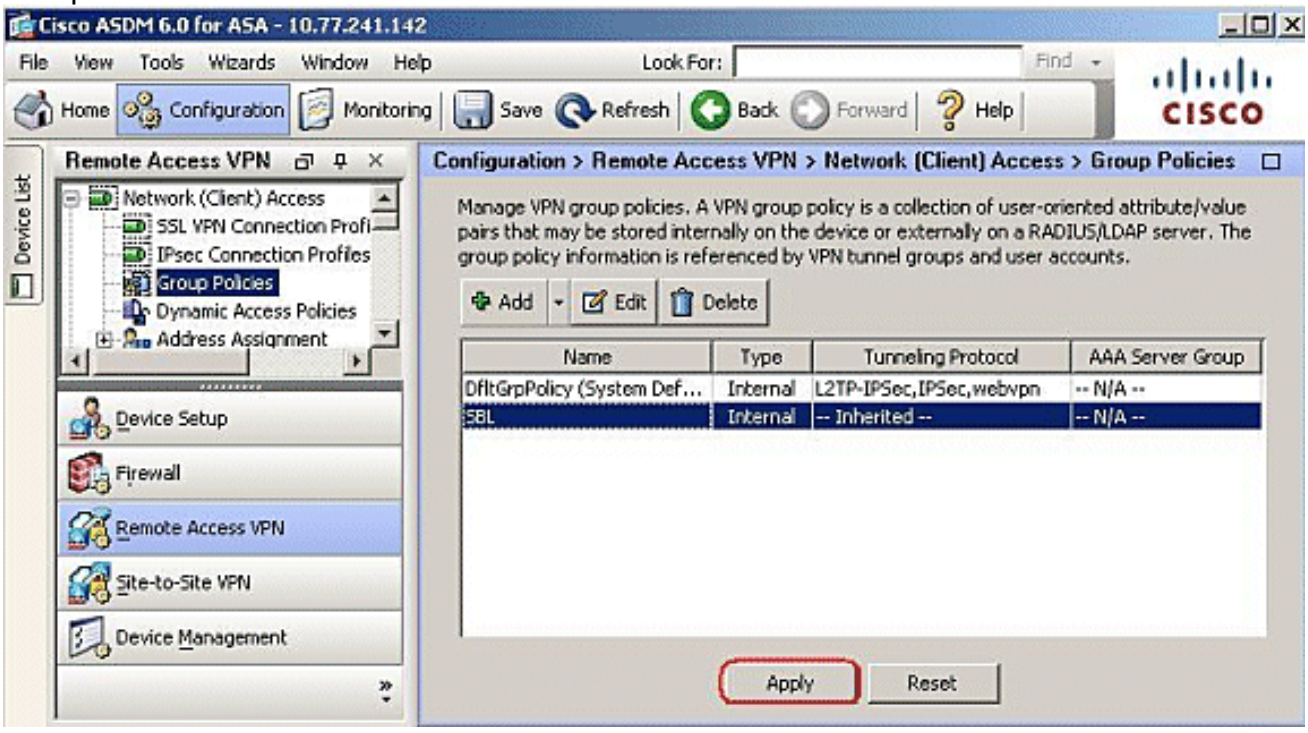
11. Назначьте профиль на внутреннюю групповую политику **(SBL)**.Придерживайтесь этого пути, **Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)>, Групповые политики> Редактируют SBL (политика внутренних групп)> Усовершенствованный> VPN-клиент SSL (SVC)> Клиентский Профиль, чтобы Загрузить**, и нажать кнопку **New**.В **Добавить Профилях VPN-клиента SSL (SVC)** нажмите **Кнопку обзора** для выбора местоположения профиля **(AnyConnectProfile.xml)**, сохраненный во флэш-памяти ASA. Назначьте **Название** для профиля, например, **SBL**. **Нажмите ОК для завершения.**



12. Удалите флажок Inherit и выберите **SBL** в поле **Client Profile to Download**. **Нажмите кнопку**
OK.



13. Нажмите **Apply** для завершения.



Используйте файл манифеста

Пакет AnyConnect, который загружен на устройстве безопасности, содержит файл под названием VPNManifest.xml. Данный пример показывает типовое содержание этого файла:

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
   is_core="yes" type="exe" action="install">
```

```
   <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
 <file version="2.1.0150" id="gina"
   is_core="yes" type="exe" action="install" module="vpngina">
   <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
</vpn>
```

Устройство безопасности сохранило на настроенные профили, как объяснено в Шаге 1, и это также хранит один или множественные пакеты AnyConnect, которые содержат клиента AnyConnect само, утилиту загрузчика, файл манифеста, и любые другие необязательные модули или файлы поддержки.

Когда удаленный пользователь соединяется с устройством безопасности с WebLaunch или текущим автономным клиентом, загрузчик загружен сначала и выполнен. Это использует файл манифеста, чтобы установить, существует ли текущий клиент на ПК удаленного пользователя, который должен быть обновлен, или новая установка требуется. Файл манифеста также содержит информацию о том, существуют ли какие-либо необязательные модули, которые должны быть загружены и установлены, в этом случае, VPNGINA. Клиентский профиль также оттолкнут от устройства безопасности. Установка VPNGINA активирована **командой svc modules value vpngina**, настроенной под командным режимом **групповой политики (webvpn)**, как объяснено в Шаге 4. Клиент AnyConnect и VPNGINA установлены, и пользователь видит Клиента AnyConnect в следующей перезагрузке до входа в систему Домена Windows.

Когда пользователь соединяется, клиент и профиль переданы к пользовательскому ПК; клиент и VPNGINA установлены; и пользователь видит клиента AnyConnect в следующей перезагрузке до входа в систему.

Когда AnyConnect установлен, образец профиля предоставлен на клиентском компьютере: **C : \Documents и Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Устранение неполадок SBL

Используйте эту процедуру при обнаружении с проблемой с SBL:

1. Гарантируйте, что выдвинут профиль.
2. Удалите предшествующие профили; ищите их на жестком диске для обнаружения местоположения: *.xml.
3. Когда вы переходите к Добавлениям/удалениям программы, у вас есть и установка AnyConnect и AnyConnect установкой VPNGINA?
4. Деинсталлируйте клиента AnyConnect.
5. Очистите журнал AnyConnect пользователя в конечном счете Средство просмотра и перетест.
6. Веб-обзор назад к устройству безопасности для переустановки клиента.
7. Удостоверьтесь, что также появляется профиль.
8. Перезагрузка однажды. На следующей перезагрузке вам предлагают с Запуском Перед приглашением Входа в систему.
9. Передайте журнал событий AnyConnect к Cisco в формате .evt.
10. Если вы видите эту ошибку, удаляете профиль пользователя и используете профиль по умолчанию:`Description: Unable to parse the profile`

C:\Documents and Settings\All Users\Application Data\Cisco \Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml. Host data not available.

Проблема 1

Это сообщение об ошибках замечено при попытке загрузить профиль AnyConnect: `Error in validating the XML file against the latest schema`. Как решена эта ошибка?

Решение 1

Это сообщение об ошибках главным образом происходит из-за синтаксиса или проблем конфигурации в профиле AnyConnect. Для решения этого вопроса удостоверьтесь, что настроенный профиль AnyConnect подобен Типовому подарку Профиля AnyConnect в Типовом разделе Профиля и XML-схемы AnyConnect руководства для администратора клиента VPN Cisco AnyConnect.

Дополнительные сведения

- Руководства администратора Cisco AnyConnect VPN Client, версия 2.0
- Создание сценариев входа в систему - Windows TechNet
- Настройка запускается перед входом в систему (PLAP) в системах Windows Vista
- ASA 8. x доступ VPN с примером конфигурации VPN-клиента SSL (SVC) AnyConnect
- Cisco AnyConnect VPN Client
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco Systems – техническая поддержка и документация