AnyConnect: настройте основной SSLVPN для головного узла маршрутизатора IOS с использованием CLI

Содержание

Введение

Этот документ описывает базовую конфигурацию маршрутизатора Cisco IOS как AnyConnect Головной узел SSLVPN.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Операционная система межсетевого взаимодействия Cisco IOS (IOS)
- Клиент Secure Mobility Client AnyConnect

- Общая операция уровня защищенных сокетов (SSL)

Используемые компоненты

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

- Маршрутизатор Cisco 892W, работающий 15.3 (3) M5
- Клиент Secure Mobility Client AnyConnect 3.1.08009

Лицензирование информации для других версий IOS

- securityk9 набор функций требуется, чтобы использовать функции SSLVPN, независимо от которых используется версия IOS.
- IOS 12.x - функция SSLVPN интегрирована во все 12.x образы, которые запускаются с 12.4 (6) T, которые имеют, по крайней мере, лицензию безопасности (ie. advsecurityk9, adventerprisek9, и так далее).
- IOS 15.0 - более ранние версии требуют, чтобы файл LIC был установлен на маршрутизаторе, который обеспечит 10, 25, или 100 подключений пользователя. Право Использовать* лицензии было внедрено в 15.0 (1) M4
- IOS 15.1 - более ранние версии требуют, чтобы файл LIC был установлен на маршрутизаторе, который обеспечит 10, 25, или 100 подключений пользователя. Право Использовать* лицензии было внедрено в 15.1 (1) T2, 15.1 (2) T2, 15.1 (3) T, и 15.1 (4) M1
- IOS 15.2 - все 15.2 версий предлагают Право Использовать* лицензии на SSLVPN
- IOS 15.3 и вне - более ранние версии предлагает Право Использовать* лицензии. Запускаясь в 15.3 (3) M, функция SSLVPN доступна после начальной загрузки в securityk9 комплексную технологию

Для лицензирования RTU будет включена лицензия на пробное пользование, когда первая функция webvpn будет настроена (т.е. шлюз WebVPN GATEWAY1), и Лицензионное соглашение с конечным пользователем (EULA) было принято. После 60 дней эта лицензия на пробное пользование становится постоянной лицензией. Эти лицензии являются основанной честью и требуют, чтобы бумажная лицензия была куплена, для использования функции. Кроме того, вместо того, чтобы быть ограниченным определенным числом использования, RTU обеспечивает максимальное число одновременных подключений, которые платформа маршрутизатора может поддержать одновременно.

Значительные улучшения программного обеспечения

Эти ID дефектов привели к значительным функциям или исправляют для AnyConnect:

- CSCti89976: Добавленная поддержка AnyConnect 3.x к IOS
- CSCtx38806: исправьте для уязвимости BEAST, Microsoft KB2585542

Настройка

Шаг 1. Подтвердите, что Включена Лицензия

Первый шаг, когда AnyConnect настроен на головном узле Маршрутизатора IOS, должен подтвердить, что лицензия была правильно установлена (если применимо) и включена. См. информацию о лицензировании в предыдущем разделе для специфических особенностей лицензирования других версий. Это зависит от версии кода и платформы, перечисляет ли show license SSL_VPN или securityk9 лицензию. Независимо от версии и лицензии, должен будет быть принят EULA, и лицензия покажет как Активная.

Шаг 2. Загрузка и пакет клиента Secure Mobility Client AnyConnect установки на маршрутизаторе

Загружать образ AnyConnect к головной станции VPN служит двум целям. Во-первых, только операционным системам, которые имеют подарок образов AnyConnect на головном узле AnyConnect, разрешат соединиться. Например, Windows - клиенты требуют, чтобы пакет Windows был установлен на головном узле, Linux, 64-разрядные клиенты требуют Linux 64-разрядный пакет и так далее. Во-вторых, образ AnyConnect, установленный на головном узле, будет автоматически оттолкнут к клиентскому компьютеру на соединение. Пользователи, которые соединяются впервые, будут в состоянии загрузить клиента от веб-портала и пользователей, которых return будет в состоянии обновить, если пакет AnyConnect на головном узле является более новым, чем, что установлено на их клиентском компьютере.

Пакеты AnyConnect могут быть получены через раздел Клиента Secure Mobility Client AnyConnect веб-сайта Загрузок Программного обеспечения Cisco. В то время как существует много доступных опций, пакеты, которые должны быть установлены на головном узле, будут маркированы операционной системой и развертываниями Головного узла (PKG). Пакеты AnyConnect в настоящее время доступны для этих платформ операционной системы: Windows, MAC OS X, (32-разрядный) Linux, и 64-разрядный Linux. Обратите внимание на то, что для Linux, существуют и 32 и 64-разрядные пакеты. Каждая операционная система требует, чтобы надлежащий пакет был установлен на головном узле для соединений, которые будут разрешены.

Как только пакет AnyConnect был загружен, он может быть загружен к флэш-памяти маршрутизатора с командой **копии** через TFTP, FTP, SCP или несколько других опций. Например:

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0):
!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]

37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

После того, как вы копируете образ AnyConnect к флэш-памяти маршрутизатора, это должно быть установленный через командную строку. Множественные пакеты AnyConnect могут быть установлены при определении порядкового номера в конце команды установки; это обеспечит маршрутизатор для действия как головной узел для операционных систем несколька клиентов. При установке пакета AnyConnect он также переместит его в **flash:/webvpn/каталог**, если он не был скопирован там первоначально.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1

SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

На версиях кода, которые были освобождены прежде 15.2 (1) T, команда для установки PKG немного отличается.

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

Шаг 3. Включение HTTP-сервера на маршрутизаторе

```
ip http server
ip http secure-server
```

Шаг 4. . Генерируйте криптографическую пару RSA и подписанный сертификат

Когда вы настраиваете SSL или любую функцию, которая внедряет Инфраструктуру открытых ключей (PKI) и цифровые сертификаты, пара ключей Ривест-Шамир-Адлемена (RSA) требуется для подписания сертификата. Придерживаться команда будет генерировать криптографическую пару RSA, которая будет тогда использоваться, когда будет генерироваться самоподписанный сертификат PKI. При использовании модуля 2048 битов это не требование, рекомендуется использовать самый большой модуль, доступный для усиленной безопасности и совместимости с клиентскими компьютерами AnyConnect. Использовать описательную метку также рекомендуется, поскольку она позволит для простоты управления ключами. Генерация ключа может быть подтверждена с **командой show crypto key mypubkey rsa** .

> **Примечание:** Как существует много угроз безопасности, привязанных к созданию экспортных ключей RSA, рекомендованные правила эксплуатации должны гарантировать, что ключи настроены, чтобы быть не экспортными, который является по умолчанию. Риски, которые включены при создании ключей RSA экспортными обсуждены в этом документе: Развертывание Ключей RSA В PKI.

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048

The name for the keys will be: SSLVPN_KEYPAIR

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 3 seconds)



show crypto key mypubkey rsa SSLVPN_KEYPAIR

% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is exportable.
Key Data&colon;
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
```

```
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAFA936 5C866DE8 5184D2D3
6D020301 0001
```

Как только криптографическая пара RSA успешно генерировалась, точка доверия PKI должна быть настроена с информацией и криптографической парой RSA нашего маршрутизатора. Общее имя (CN) в Subject-Name должно быть настроено с IP-адресом или Полным классифицированным именем домена (FQDN), которое пользователи используют для соединения со шлюзом AnyConnect; в данном примере клиенты используют FQDN fdenofa-SSLVPN.cisco.com, когда они пытаются соединиться. В то время как это не является обязательным, когда вы правильно входите в CN, это помогает сокращать количество ошибок сертификата, которым предлагают при входе в систему.

> **Примечание:** Вместо того, чтобы использовать подписанный сертификат, генерируемый маршрутизатором, возможно использовать сертификат, выполненный сторонним CA., Это может быть сделано через несколько других методов, как обсуждено в этом документе: Хранилище сертификатов Настройки для PKI.

```
crypto pki trustpoint SSLVPN_CERT
 enrollment selfsigned
 subject-name CN=fdenofa-SSLVPN.cisco.com
 rsakeypair SSLVPN_KEYPAIR
```

После того, как точка доверия была правильно определена, маршрутизатор должен генерировать сертификат при помощи **команды crypto pki enroll** . С этим процессом возможно задать несколько других параметров, таких как серийный номер и IP-адрес. Однако это не требуется. Генерация сертификата может быть подтверждена с **командой show crypto pki certificates** .

```
crypto pki enroll SSLVPN_CERT

% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

```
show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
    end   date: 20:00:00 EDT Dec 31 2019
```

```
  Associated Trustpoints: SSLVPN_CERT
```

Шаг 5. . Настройте локальные учетные записи пользователя VPN

В то время как возможно использовать внешнюю проверку подлинности, Авторизацию, и Бухгалтерский (AAA) сервер, поскольку используется локальная проверка подлинности данного примера. Эти команды создадут имя пользователя VPNUSER и также создадут список аутентификации AAA (проверка подлинности, авторизация и учет) под названием SSLVPN_AAA.

```
aaa new-model
aaa authentication login SSLVPN_AAA local
username VPNUSER password TACO
```

Шаг 6. Определите Список доступа Пула адресов и Разделения туннеля, который будет Использоваться Клиентами

Пул local IP address должен быть создан для клиентских адаптеров AnyConnect для получения IP-адреса. Гарантируйте настройку достаточно большого пула для поддержки максимального числа одновременных клиентских соединений AnyConnect.

По умолчанию AnyConnect будет работать в полном туннельном режиме, что означает, что любой трафик, генерируемый клиентским компьютером, будет передаваться через туннель. Поскольку это, как правило, не выбираемо, возможно настроить Список контроля доступа (ACL), который тогда определяет трафик, который должен или не должен быть передан через туннель. Как с другими реализациями ACL, неявные запрещают в конце, избавляет от необходимости явное, запрещают; поэтому, только необходимо настроить операторов permit для трафика, который должен быть туннелирован.

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Шаг 7. Настройте виртуальный интерфейс (VTI)

Динамические VTIs предоставляют по требованию отдельный Интерфейс виртуального доступа для каждого сеанса VPN, который позволяет очень безопасный и расширяемое подключение для VPN удаленного доступа. Технология DVTI заменяет динамические криптокарты и динамический осевой метод, который помогает устанавливать туннели. Поскольку функция DVTIs как любой другой реальный интерфейс, они обеспечивают более сложные Удаленные развертывания Accesss, потому что они поддерживают QoS, межсетевой экран, атрибуты для каждого пользователя и другие сервисы безопасности, как только туннель активен.

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
 ip unnumbered Loopback0
```

Шаг 8. Настройте шлюз WebVPN

Шлюз WebVPN - то, что определяет IP-адрес и порт (порты), который будет использоваться головным узлом AnyConnect, а также алгоритмом шифрования SSL и сертификатом PKI, который будет представлен клиентам. По умолчанию шлюз поддержит все возможные

алгоритмы шифрования, которые варьируются в зависимости от версии IOS на маршрутизаторе.

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
 ip unnumbered Loopback0
```

Шаг 9. Настройте контекст WebVPN и групповую политику

Контекст WebVPN и Групповая политика определяют некоторые дополнительные параметры, которые будут использоваться для клиентского соединения AnyConnect. Для основной конфигурации AnyConnect Контекст просто служит механизмом, используемым для вызова Политики группы по умолчанию, которая будет использоваться для AnyConnect. Однако Контекст может использоваться для дальнейшей настройки страницы-заставки WebVPN и операции WebVPN. В Группе определенной политики список SSLVPN_AAA настроен как список аутентификации AAA (проверка подлинности, авторизация и учет), которого пользователи являются участником. **Поддерживающая обращение к операционной системе** команда **функций** является частью конфигурации, которая позволяет пользователям соединяться с **VPN-клиентом SSL (SVC)** AnyConnect, а не просто WebVPN через браузер. Наконец, дополнительные команды SVC определяют параметры, которые относятся только к соединениям SVC: **svc address-pool** говорит шлюзу адресам раздаточных материалов в ACPool клиентам, **svc split включают** , определяет политику раздельных туннелей на ACL 1, определенный выше, и **svc dns-server** определяет сервер DNS, который будет использоваться для разрешения доменного имени. С этой конфигурацией все запросы DNS будут передаваться указанному серверу DNS. Адрес, который получен в ответе запроса, продиктует, передается ли трафик через туннель.

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Шаг 10 (Необязательно). Настройте клиентский профиль

В отличие от этого, на ASA, Cisco IOS не имеет встроенного графического интерфейса пользователя (GUI), который может помочь admin в создании клиентского профиля. Профиль клиента AnyConnect должен создаваться/редактироваться отдельно с Автономным Редактором Профиля.

> **Совет:** Ищите anyconnect-profileeditor-win-3.1.03103-k9.exe

Выполните эти действия для имения маршрутизатора, развертывают профиль:

1. Загрузите его к Флэшу IOS с помощью ftp/tftp
2. Используйте эту команду для определения профиля, который был просто загружен:

1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```
Совет: На версиях IOS, более старых, чем 15.2 (1) T, должна использоваться эта команда:
webvpn импортирует профиль обращения к операционной системе <profile_name> флэш-память: <profile.xml>

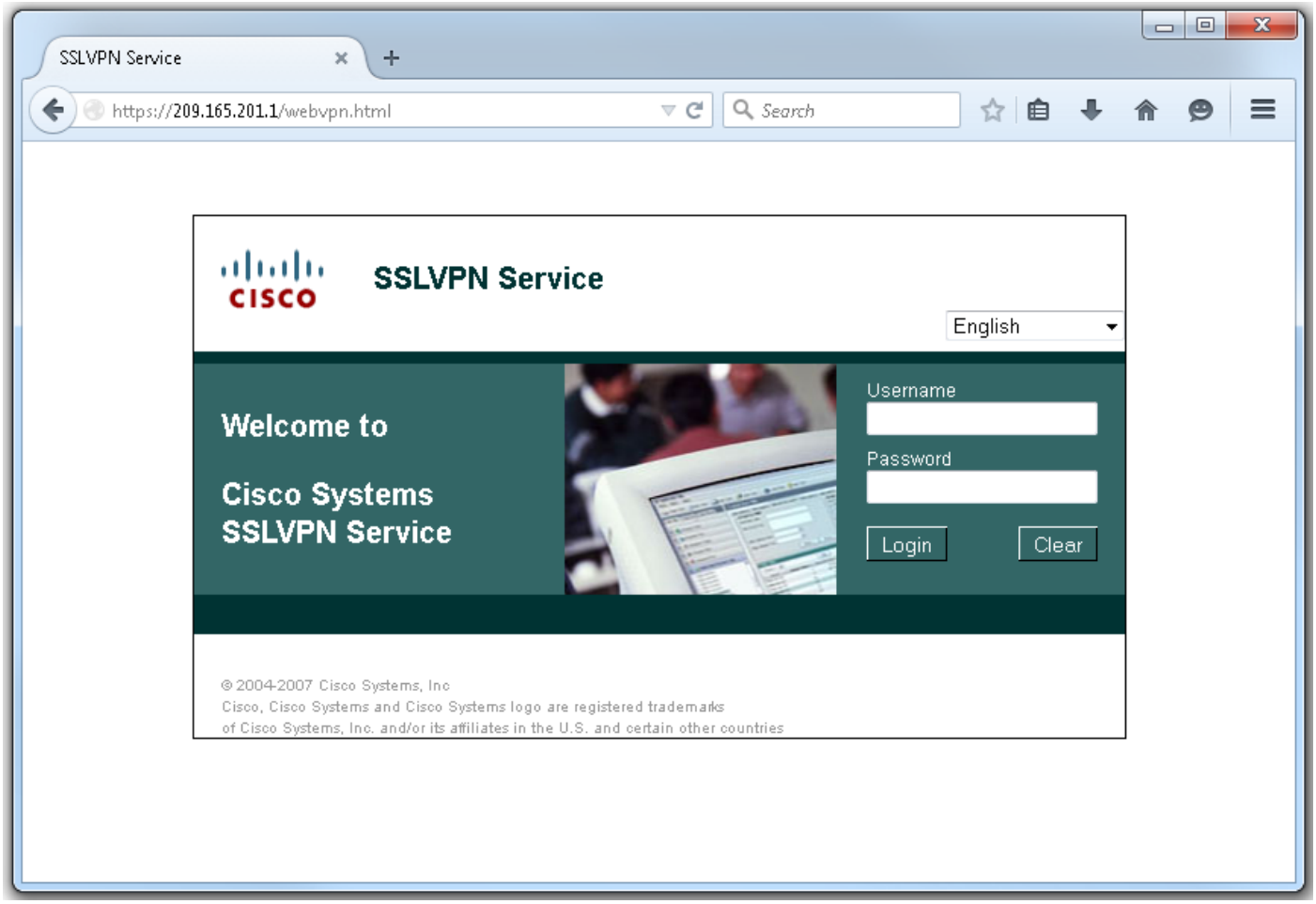
3. Под контекстом используйте эту команду для соединения профиля с тем контекстом:

1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

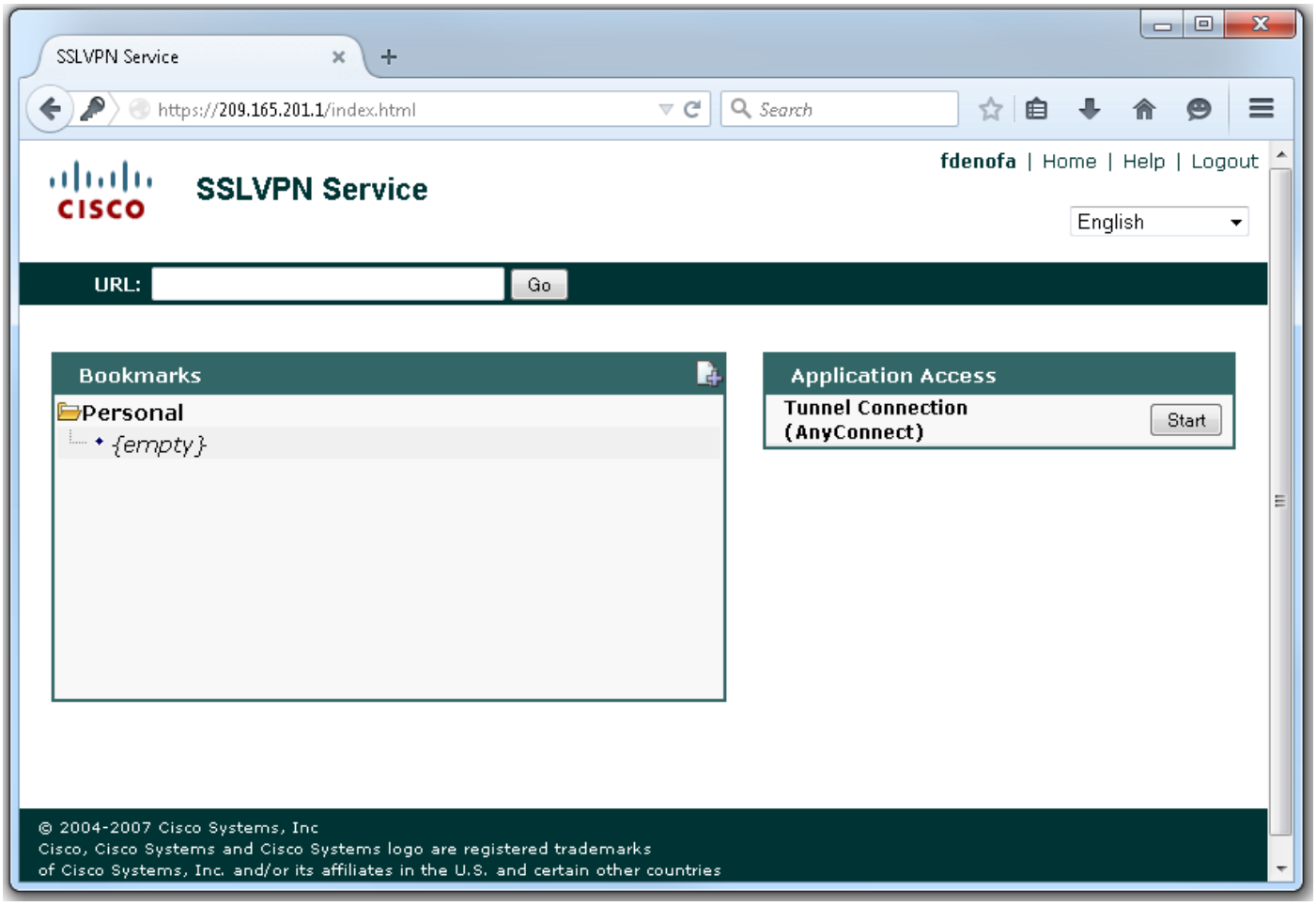
Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

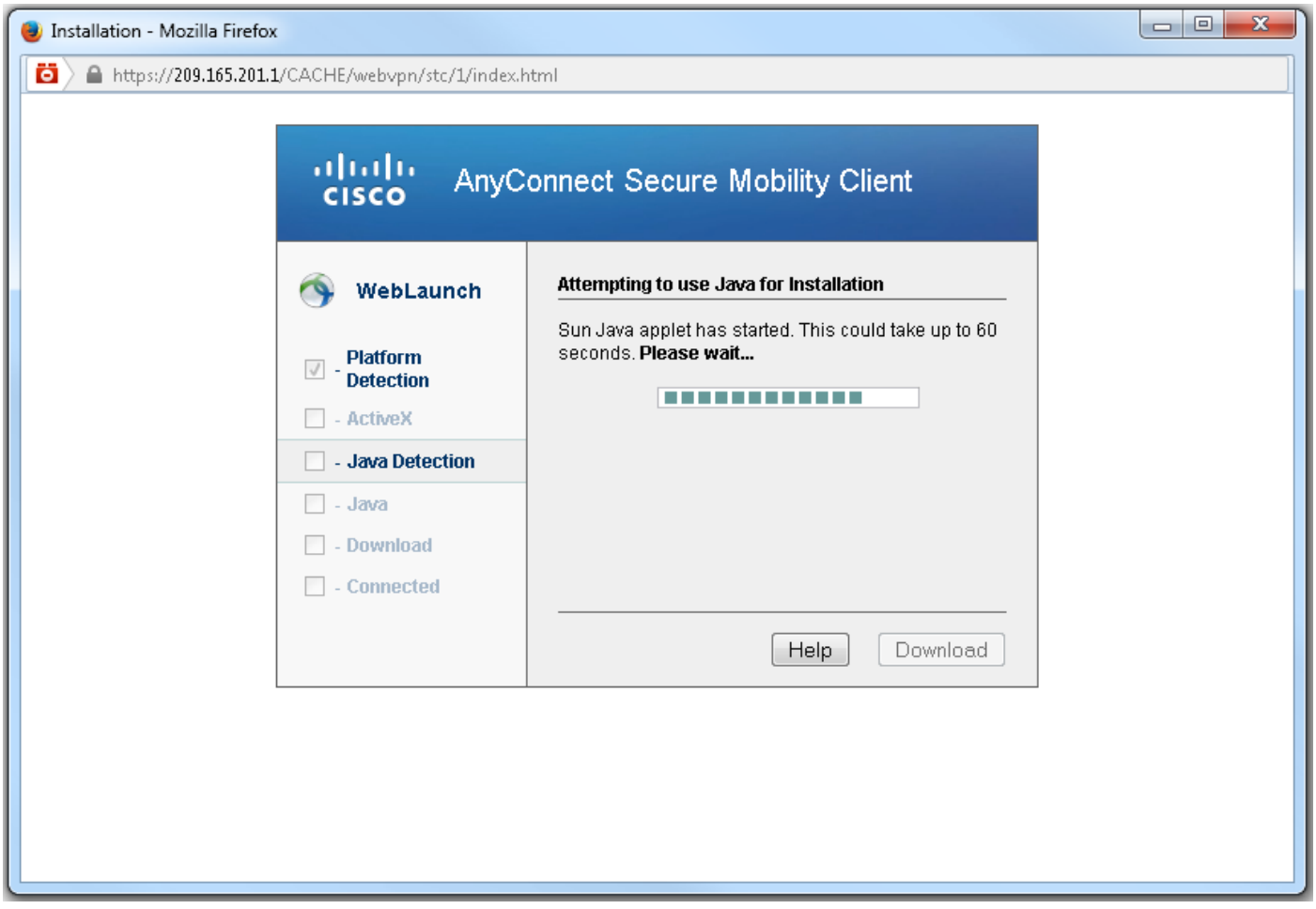
Проверка

Как только конфигурация завершена при доступе к Адресу шлюза и порту через браузер это возвратится к странице-заставке WebVPN.



После регистрации домашняя страница WebVPN отображена. Отсюда, нажмите **Tunnel Connection (AnyConnect).** Когда Internet Explorer используется, ActiveX используется, чтобы оттолкнуть и установить клиента AnyConnect. Если это не будет обнаружено, то Java будет использоваться вместо этого. Все другие браузеры сразу используют Java.

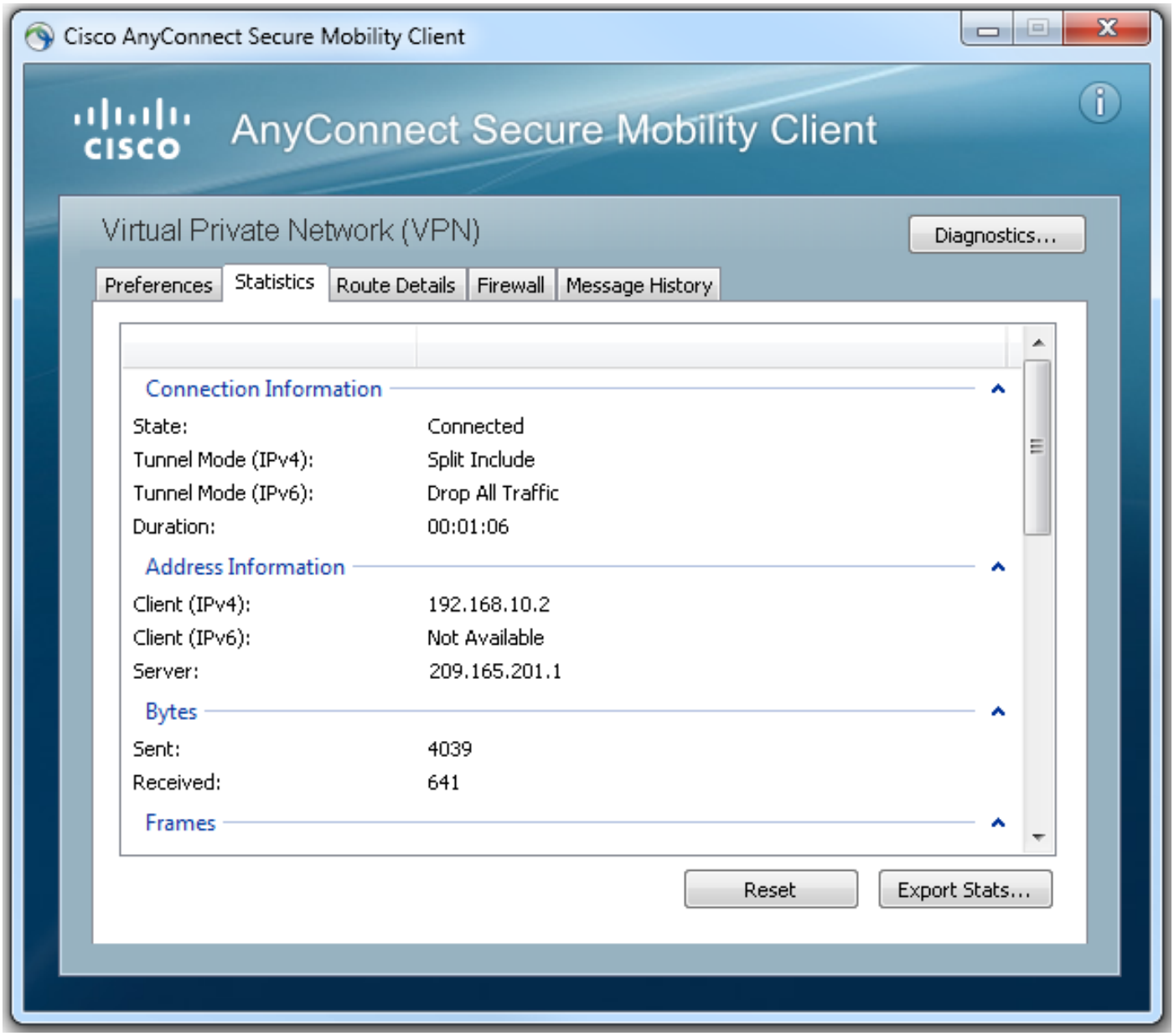


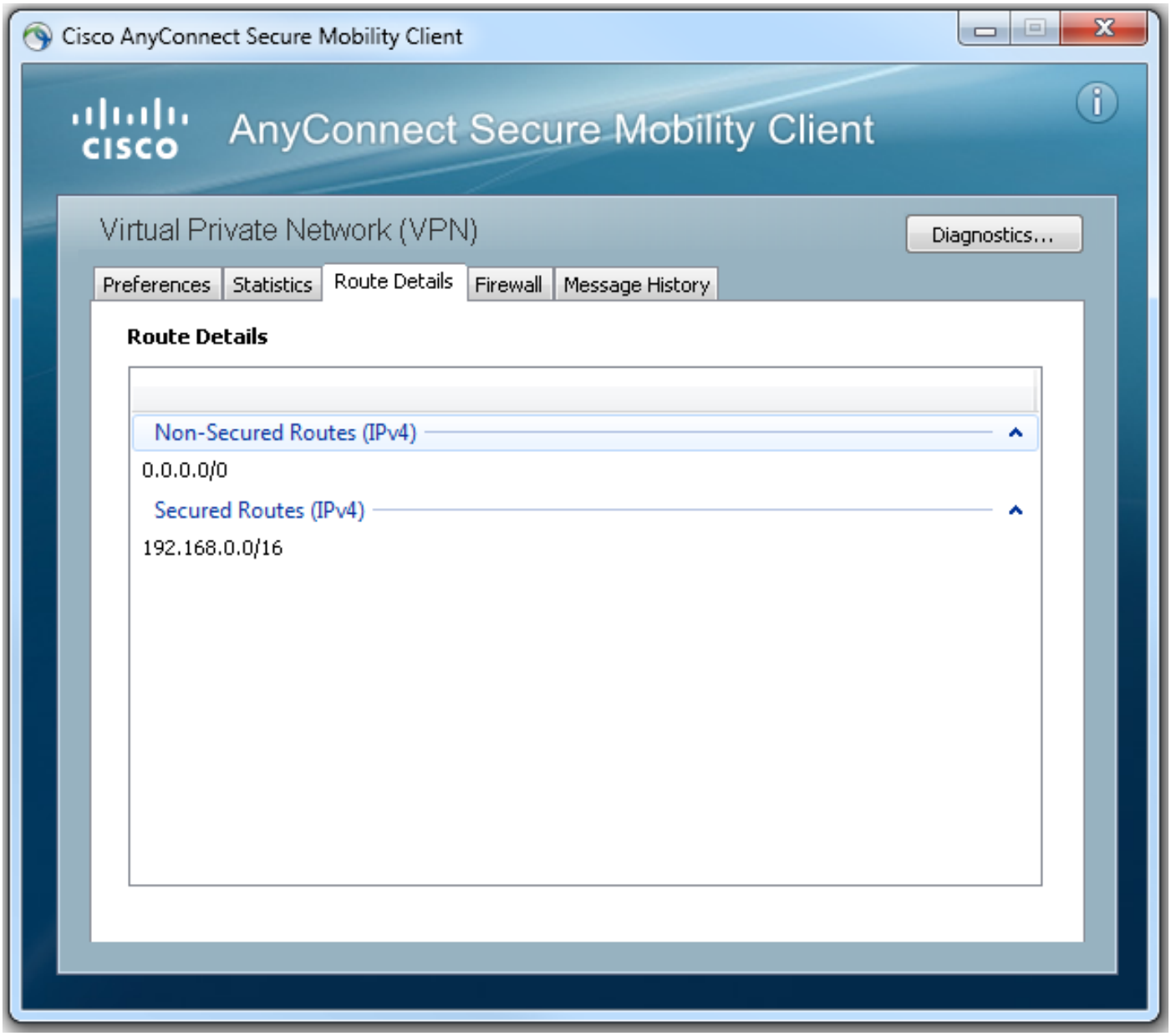


Как только установка завершена, AnyConnect автоматически попытается соединиться со Шлюзом WebVPN. Поскольку подписанный сертификат используется для шлюза для

определения себя, предупреждения несколька серверов сертификатов появятся во время попытки подключения. Они ожидаются и, как должны принимать, для соединения продолжаются. Для предотвращения этих предупреждений сертификата представляемый подписанный сертификат должен быть установлен в хранилище надежного сертификата клиентского компьютера, или если сторонний сертификат используется тогда, сертификат Центра сертификации должен быть в хранилище надежного сертификата.

То, когда соединение завершает согласование, щелкните по значку **механизма** в нижнем левый из AnyConnect, отобразит некоторую усовершенствованную информацию о соединении. На этой странице возможно просмотреть некоторую статистику соединения и подробные данные маршрута, достигнутые от ACL разделения туннеля в конфигурации Групповой политики.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Include
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:06
Address Information
Client (IPv4): 192.168.10.2
Client (IPv6): Not Available
Server: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



Вот заключительная текущая конфигурация , следуют из действий настройки:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Устранение неполадок

Существует несколько общих компонентов для проверки для того, когда вы решаете проблемы Соединения AnyConnect:

- Поскольку клиент должен представить сертификат, это - требование, чтобы сертификат задал в Шлюзе WebVPN быть допустимым. Для запуска **показа, крипто-сертификат**

pki покажет информацию, которая принадлежит всем сертификатам на маршрутизаторе.
- Каждый раз, когда изменение внесено в конфигурацию WebVPN, это - оптимальный метод для запуска не штатный и штатный и на шлюзе и на Контексте. Это гарантирует, что изменения вступают в силу должным образом.
- Как отмечалось ранее, это - требование для имения PKG AnyConnect для каждой клиентской операционной системы, которая соединится с этим шлюзом. Например, Windows - клиенты требуют Windows PKG, Linux, 32-разрядные клиенты требуют Linux 32-разрядный PKG и так далее.
- Когда вы рассматриваете и клиента AnyConnect и на основе браузера WebVPN используют SSL, быть в состоянии обратиться к странице-заставке WebVPN обычно указывает, что AnyConnect будет в состоянии соединиться (предположите, что подходящая конфигурация AnyConnect корректна).

Cisco IOS предлагает некоторые различные опции debug webvpn, которые могут использоваться для устранения проблем отказывающих соединений. Это - выходные данные, генерируемые от aaa debug webvpn, отладка wevpn туннель и show webvpn session после попытки успешного подключения:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  functions svc-enabled
  svc address-pool "SSLVPN_POOL" netmask 255.255.255.0
  svc split include acl 1
  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Дополнительные сведения

- Руководство конфигурации VPN SSL, Cisco IOS Release 15M&T
- VPN AnyConnect (SSL) клиент на маршрутизаторе IOS с примером конфигурации CCP