# SSL AnyConnect по IPv4+IPv6 к конфигурации ASA

## Содержание



## Введение

Этот документ предоставляет пример конфигурации для устройства адаптивной защиты Cisco (ASA), чтобы позволить защищенному мобильному клиенту Cisco AnyConnect Secure Mobility (называемый "AnyConnect" в оставшейся части этого документа) устанавливать VPN-туннель SSL по сети IPv4 или IPv6.

Кроме того, эта конфигурация позволяет клиенту передавать IPv4 и трафик IPv6 по туннелю.

## Предварительные условия

### Требования

Для успешного установления туннеля SSLVPN по IPv6 удовлетворите эти требования:

- Сквозное подключение IPv6 требуется
- Версия AnyConnect должна быть 3.1 или позже
- Версия программного обеспечения ASA должна быть 9.0 или позже

Однако, если какое-либо из этих требований не будет удовлетворено, то конфигурация, обсужденная в этом документе, все еще позволит клиенту соединяться по IPv4.

### Используемые компоненты

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

- ASA 5505 с версией программного обеспечения 9.0 (1)

- Клиент Secure Mobility Client AnyConnect 3.1.00495 на Microsoft Windows XP Professional (без поддержки IPv6)
- Клиент Secure Mobility Client AnyConnect 3.1.00495 на Microsoft Windows 7 32-разрядных предприятий

## Условные обозначения

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

## !--- конфигурацию

Прежде всего определите пул IP-адресов, от которых вы назначите тот на каждого клиента, который соединяется.

Если вы захотите, чтобы клиент также нес трафик IPv6 по туннелю, то вам будет нужен пул адресов IPv6. На оба пула ссылаются позже в групповой политике.

```
ip local pool pool4 172.16.2.100-172.16.2.199 mask 255.255.255.0
ipv6 local pool pool6 fcfe:2222::64/64 128
```

Для подключения IPv6 к ASA вам нужен адрес IPv6 на интерфейсе, который клиенты подключат с (как правило, внешний интерфейс).

Для подключения IPv6 по туннелю к внутренним хостам вам нужен IPv6 на внутреннем интерфейсе (интерфейсах) также.

```
interface Vlan90
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0
 ipv6 address 2001:db8:90::2/64
!
interface Vlan102
 nameif inside
 security-level 100
 ip address 192.168.102.2 255.255.255.0
 ipv6 address fcfe:102::2/64
```

Для IPv6 вам также нужен маршрут по умолчанию, указывающий на маршрутизатор следующего перехода к Интернету.

```
ipv6 route outside ::/0 2001:db8:90::5
route outside 0.0.0.0 0.0.0.0 203.0.113.5 1
```

Для аутентификации себя на клиентах ASA должен иметь сертификат идентификации. Инструкции по тому, как создать или импортировать такой сертификат, выходят за рамки этого документа, но могут быть легко найдены в других документах таким как

/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98596-asa-8-x-3rdpartyvendorcert.html

Итоговая конфигурация должна выглядеть подобной придерживающемуся:

```
crypto ca trustpoint testCA
 keypair testCA
 crl configure
```

```
...
crypto ca certificate chain testCA
 certificate ca 00
  30820312 308201fa a0030201 02020100 300d0609 2a864886 f70d0101 05050030
  ...
  quit
 certificate 04
  3082032c 30820214 a0030201 02020104 300d0609 2a864886 f70d0101 05050030
  ...
  quit
```

Затем дайте ASA команду использовать этот сертификат для SSL:

```
ssl trust-point testCA
```

Затем основной webvpn (SSLVPN) конфигурация, где опция активирована на внешнем интерфейсе. Определены клиентские пакеты, которые доступны для скачивания, и мы определяем профиль, определен (больше на этом позже):

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect profiles asa9-ssl-ipv4v6 disk0:/asa9-ssl-ipv4v6.xml
 anyconnect enable
```

В этом базовом примере IPv4 и пулы адреса IPv6 настроены, информация сервера DNS (который будет выдвинут клиенту), и профиль в групповой политике по умолчанию (DfltGrpPolicy). Еще много атрибутов могут быть настроены здесь, и дополнительно можно определить другие групповые политики для других компаний пользователей.

**Примечание:** Атрибут "шлюза-fqdn" является новым в версии 9.0 и определяет FQDN ASA, как это известно в DNS. Клиент изучает этот FQDN из ASA и будет использовать его при роуминге от IPv4 до сети IPv6 или наоборот.

```
group-policy DfltGrpPolicy attributes
 dns-server value 10.48.66.195
 vpn-tunnel-protocol ssl-client
 gateway-fqdn value asa9.example.net
 address-pools value pool4
 ipv6-address-pools value pool6
 webvpn
   anyconnect profiles value asa9-ssl-ipv4v6 type user
```

Затем, настройте одну или более туннельных групп. По умолчанию один (DefaultWEBVPNGroup) используется для данного примера, и настройте его для требования пользователя к используемой аутентификации сертификат:

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
```

По умолчанию клиент AnyConnect пытается соединиться по IPv4 и, только если это отказывает, он пытается соединиться по IPv6. Однако это поведение может быть изменено установкой в профиле XML. Профиль AnyConnect "asa9-ssl-ipv4v6.xml", на который ссылаются в конфигурации выше, генерировался с помощью Редактора Профиля в ASDM (Конфигурация - VPN для удаленного доступа - Сетевого (Клиента) Акксесса - Профиль Клиента AnyConnect).

Получающийся профиль XML (с большей частью части по умолчанию, опущенной для краткости):

```
<?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>
...
```

```
<IPProtocolSupport>IPv6,IPv4</IPProtocolSupport> ... </ClientInitialization> <ServerList>
<HostEntry> <HostName>SSL to ASA9 (IPv4,IPv6)</HostName>
<HostAddress>asa9.example.net</HostAddress> </HostEntry> </ServerList> </AnyConnectProfile>
```

В вышеупомянутом профиле HostName также определен (который может быть чем-либо, это не должно совпадать с действительным именем хоста ASA), и HostAddress (который, как правило, является FQDN ASA).

**Примечание:** Поле HostAddress можно оставить пустым, но поле HostName должно содержать FQDN ASA.

**Примечание:** Пока профиль не предварительно развернут, первое соединение требует, чтобы пользователь ввел в FQDN ASA. Это первоначальное подключение предпочтет IPv4. После успешного подключения будет загружен профиль. Оттуда, параметры настройки профиля будут применены.

## Проверка

Чтобы проверить, связан ли клиент по IPv4 или IPv6, проверьте или клиентский GUI или DB сеанса VPN на ASA:

- На клиенте откройте окно Advanced, перейдите к вкладке Statistics и проверьте IP-адрес "Сервера".Этот первый пользователь соединяется от системы Windows XP без поддержки IPv6:Этот второй пользователь соединяется от хоста Windows 7 с подключением IPv6 к ASA:
- На ASA, от CLI проверяют "Общего IP" в "покажите vpn-sessiondb anyconnect" выходные данные. В данном примере вы видите те же два соединения как выше: один от XP по IPv4 и один от Windows 7 по IPv6:
```
asa9# show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username : Nanashi no Gombei Index : 45
Assigned IP : 172.16.2.101 Public IP : 192.0.2.95 Protocol : AnyConnect-Parent SSL-Tunnel
DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel:
(1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-
Tunnel: (1)SHA1 Bytes Tx : 13138 Bytes Rx : 22656 Group Policy : DfltGrpPolicy Tunnel Group
: DefaultWEBVPNGroup Login Time : 11:14:29 UTC Fri Oct 12 2012 Duration : 1h:45m:14s
Inactivity : 0h:00m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none Username : Uno
Who Index : 48 Assigned IP : 172.16.2.100 Public IP : 2001:db8:91::7 Assigned IPv6:
fcfe:2222::64 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect
Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx :
11068 Bytes Rx : 10355 Group Policy : DfltGrpPolicy Tunnel Group : DefaultWEBVPNGroup Login
Time : 12:55:45 UTC Fri Oct 12 2012 Duration : 0h:03m:58s Inactivity : 0h:00m:00s NAC Result
: Unknown VLAN Mapping : N/A VLAN : none
```

## Дополнительные сведения

- Cisco Systems – техническая поддержка и документация