Клиент Anyconnect к ASA с использованием DHCP для назначения адреса

Содержание

Введение

Этот документ описывает, как настроить Устройство адаптивной защиты (ASA) Cisco 5500-X Series, чтобы заставить сервер DHCP предоставить IP-адрес клиента всем клиентам Anyconnect с использованием Менеджера устройств адаптивной безопасности (ASDM) (ASDM) или CLI.

Предварительные условия

Требования

В этом документе предполагается, что устройство адаптивной защиты полностью исправно и в нем разрешено изменение конфигурации с помощью Cisco ASDM или интерфейса командной строки.

> **Примечание:** См. Книгу 1: Руководство Конфигурации интерфейса командой строки Общих функционирований Серии Cisco ASA, 9.2 , чтобы позволить устройству, которое будет удаленно настроено ASDM или Secure Shell (SSH).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Cisco ASA 5500-X версия межсетевого экрана 9.2 (1) следующего поколения
- Версия 7.1 (6) менеджера устройств адаптивной безопасности (ASDM)
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility 3.1.05152

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.

Родственные продукты

Эта конфигурация может также использоваться с Версией 7.x серии 5500 Устройства безопасности Cisco ASA и позже.

Общие сведения

VPN адреса удалённого доступа требуются для мобильных сотрудников для безопасного соединения с сетью организации. Мобильные пользователи в состоянии установить безопасное соединение с помощью программного обеспечения Cisco Anyconnect Secure Mobility Client. Защищенный мобильный клиент Cisco AnyConnect Secure Mobility инициирует соединение с устройством центрального узла, настроенным для принятия этих запросов. В данном примере устройство центрального узла является ASA Устройство адаптивной безопасности серии 5500-X, которое использует динамические криптокарты.

В управлении адресами устройства безопасности необходимо настроить IP-адреса, которые подключают клиента с ресурсом на частной сети, через туннель, и позволяют клиентской функции, как будто это напрямую подключилось к частной сети.

Кроме того, вы имеете дело только с закрытыми IP - адресами, которые назначены на клиентов. IP-адреса, назначенные на другие ресурсы на вашей частной сети, являются частью ваших обязанностей по администрированию сети, не частью управления VPN. Поэтому, когда IP-адреса обсуждены здесь, Cisco имеет в виду те IP-адреса, доступные в вашей схеме адресации частной сети, которые позволяют клиентской функции как оконечной точке туннеля.

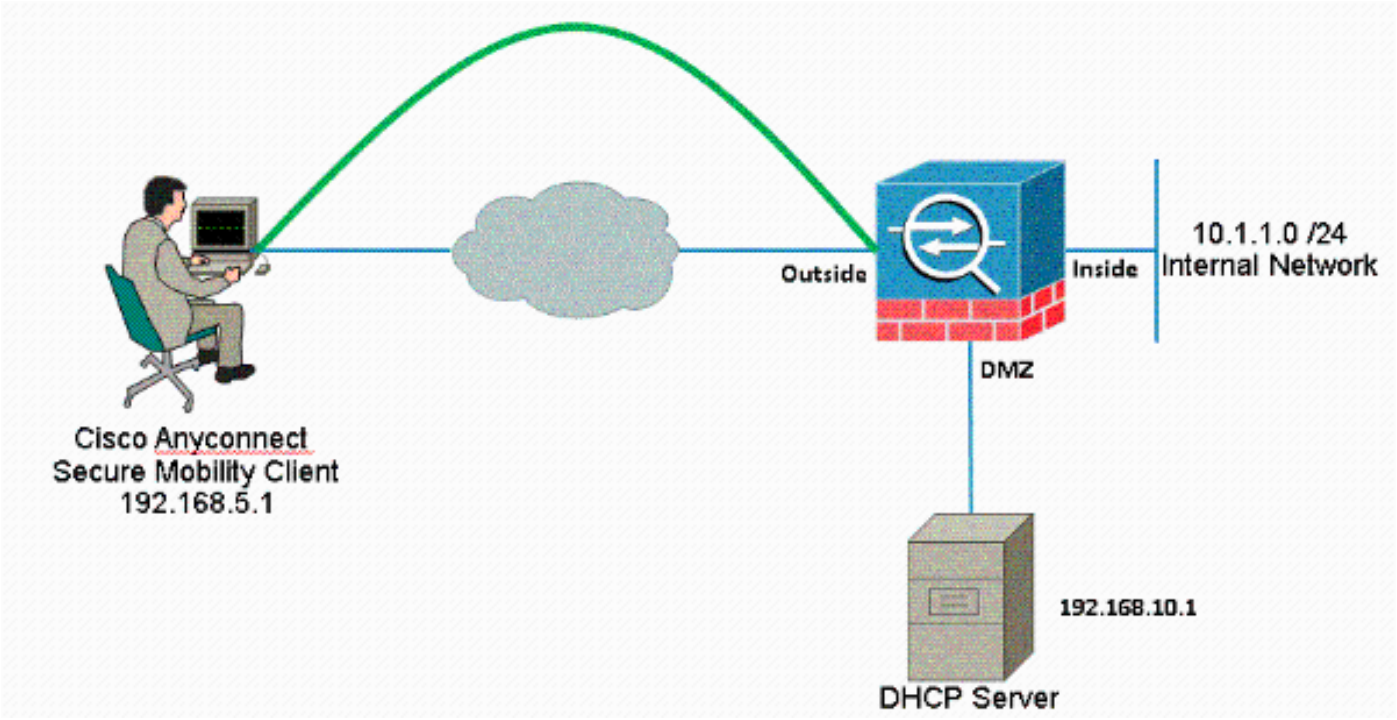
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

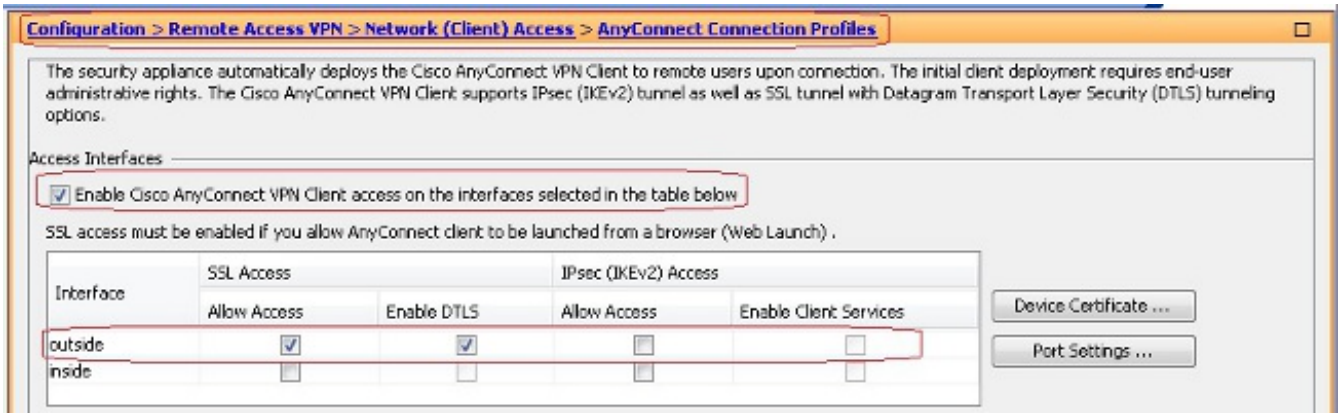
Настройте защищенный мобильный клиент Cisco AnyConnect Secure Mobility

Порядок действий в диспетчере ASDM

Выполните эти шаги, чтобы настроить удаленный доступ через сеть VPN:

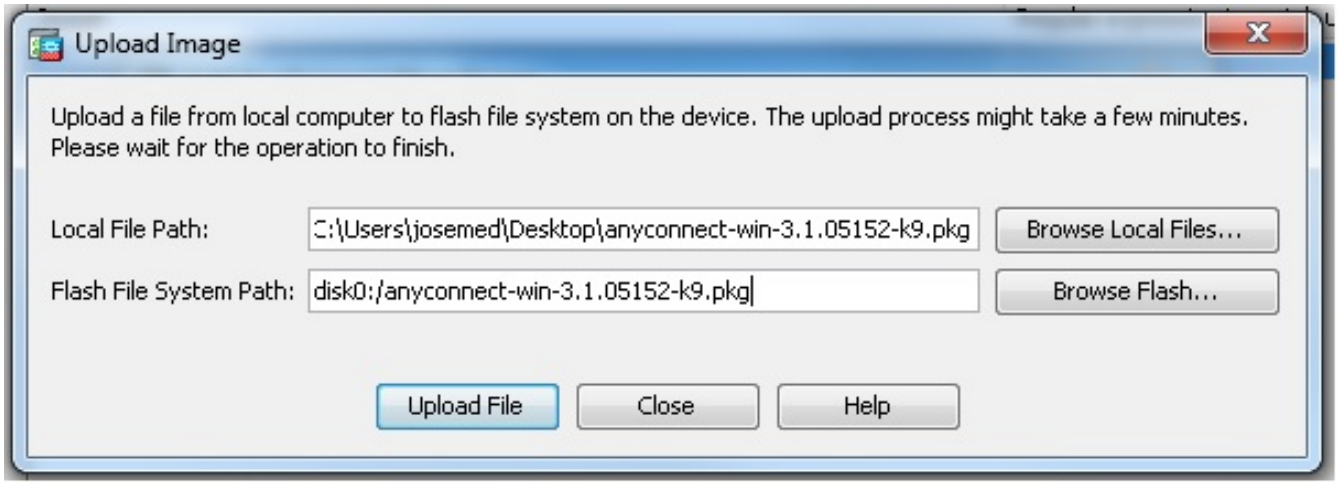
- Включенный WebVPN.

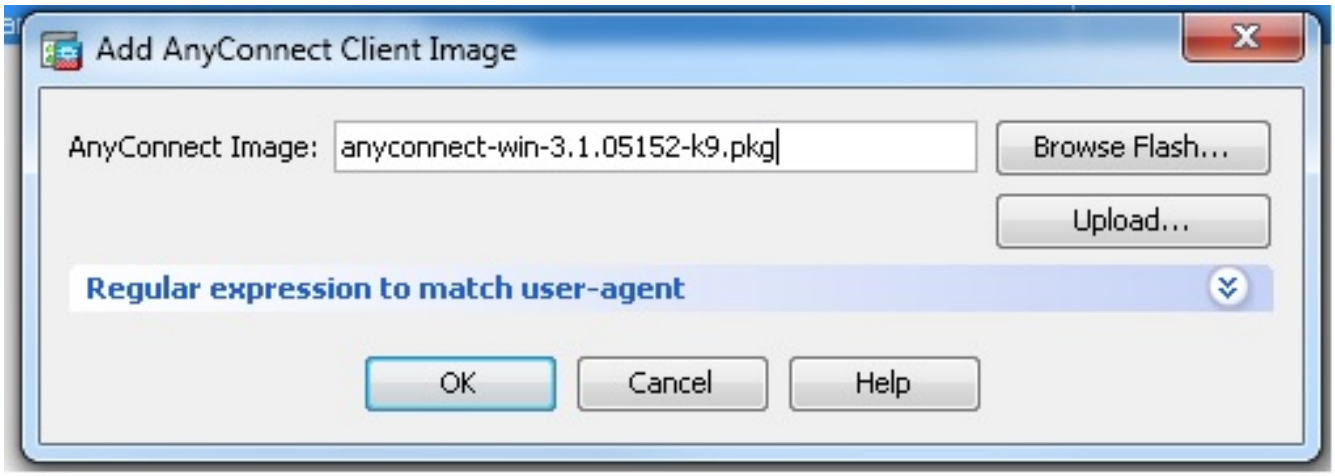
Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles и в разделе Access Interfaces установите флажки Allow Access и Enable DTLS для внешнего интерфейса. Кроме того, проверьте **Разрешать Cisco AnyConnect VPN Client или устаревший доступ VPN-клиента SSL (SVC) на интерфейсе, выбранном в этом** флажке **таблицы** для включения VPN SSL на внешнем интерфейсе.



Щелкните "Применить".

Выберите **Configuration> Remote Access VPN> Network (Client) Access> Anyconnect Client Software> Add** для добавления образа Клиента AnyConnect VPN Client Cisco от флэш-памяти ASA как показано.



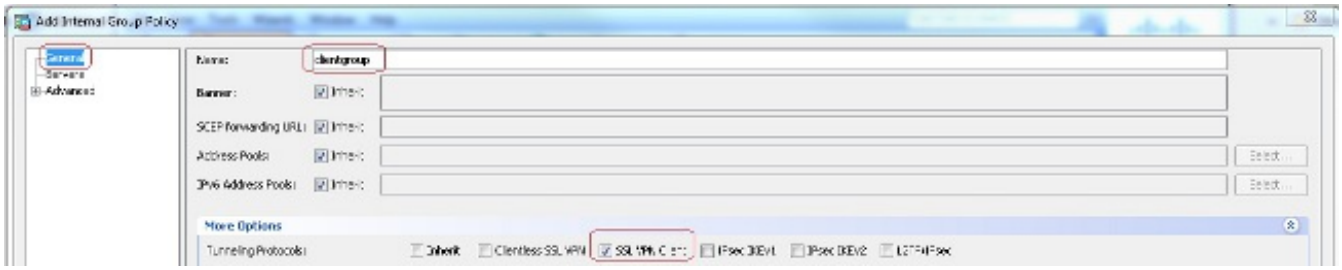


Эквивалентная конфигурация в интерфейсе командной строки:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

- Настройка групповой политики.

Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Group Policies, чтобы создать внутреннюю групповую политику clientgroup. Под **Вкладкой Общие** установите флажок **SSL VPN Client** для включения SSL как протокола туннелирования.



Настройте Область сети DHCP во вкладке **Servers**, выберите **More Options** для настройки Области DHCP для пользователей, чтобы быть назначенными автоматически.

Эквивалентная конфигурация в интерфейсе командной строки:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

- Выберите **Configuration> Remote Access VPN> AAA/Local Users> Local Users> Add** для создания учетной записи нового пользователя **ssluser1**. **Нажмите кнопку OK, а затем Apply.**

Эквивалентная конфигурация в интерфейсе командной строки:`ciscoasa(config)#`**`username ssluser1 password asdmASA`**

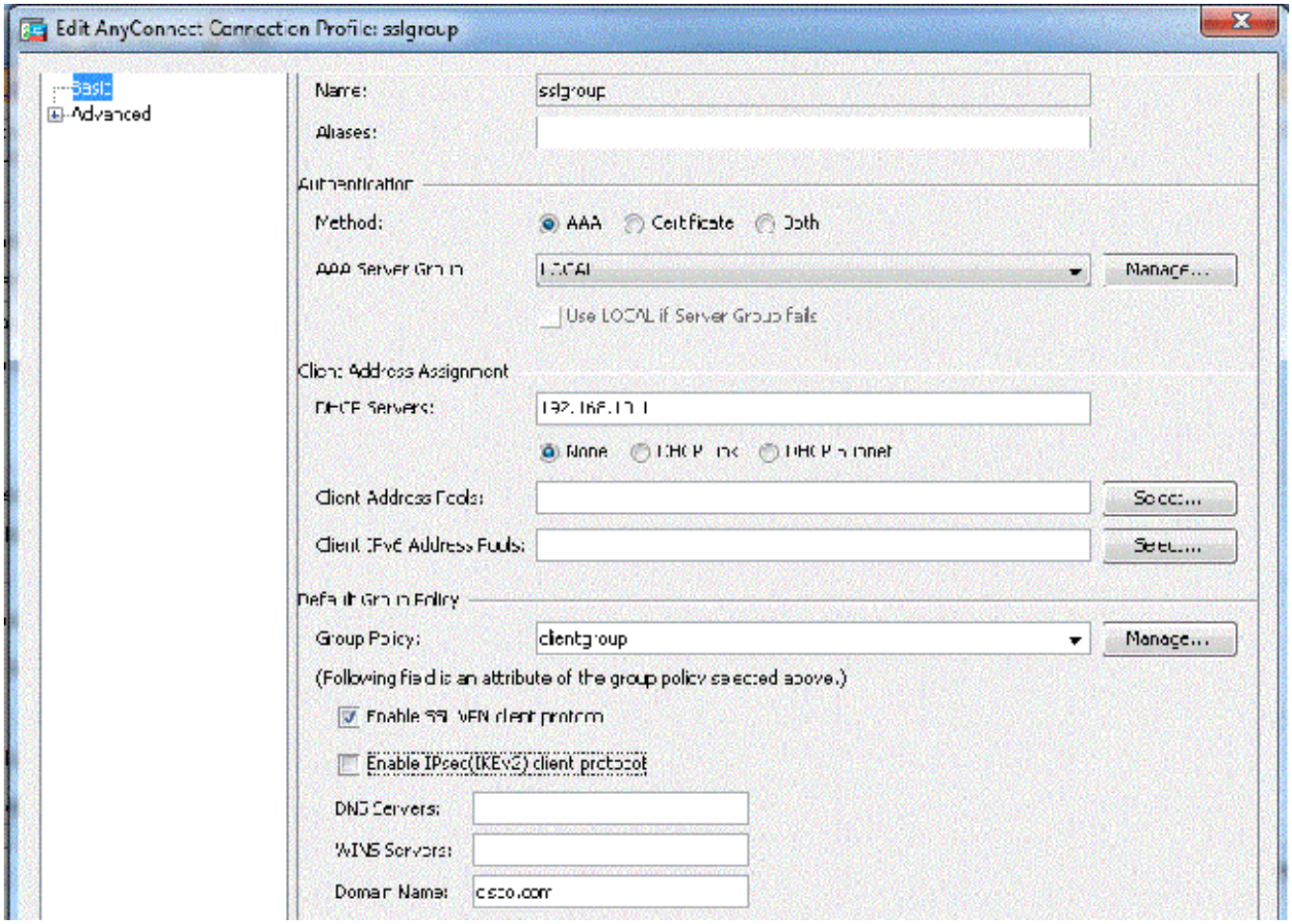
- Настройка группы туннелирования.

Выберите **Configuration> Remote Access VPN> Network (Client) Access> Anyconnect**

Connection Profiles> Add для создания нового **sslgroup** туннельной группы.

На вкладке Basic можно заполнить список конфигурации так, как показано на рисунке:

Назовите группу туннелирования sslgroup.Предоставьте IP - адрес сервера DHCP в пространстве, обеспечил **Серверы DHCP**.Под Политикой Группы по умолчанию выберите групповую политику **clientgroup** из выпадающего списка Групповой политики.Настройте ссылку DHCP или подсеть DHCP.



Под вкладкой **Advanced> Group Alias/Group URL** задайте название псевдонима группы как **sslgroup_users** и нажмите **OK**.

Эквивалентная конфигурация в интерфейсе командной строки:

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#dhcp-server 192.168.10.1
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

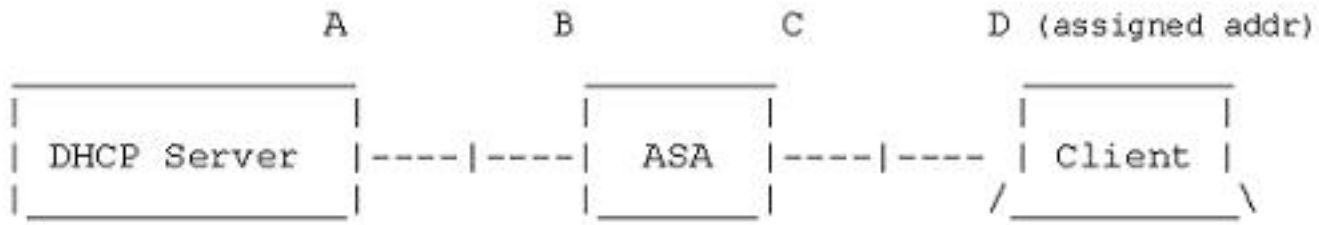
Выбор подсети или выбор канала

Поддержка прокси DHCP для RFC 3011 и RFC 3527 является функцией, представленной в 8.0.5 и 8.2.2, и это поддерживалось в прогрессивных версиях.

- RFC 3011 определяет новый параметр DHCP, опцию выбора подсети, которая позволяет клиенту DHCP задавать подсеть, на которой можно выделить адрес. Эта опция имеет приоритет по методу, что использование сервера DHCP для определения подсети, на которой можно выбрать адрес.
- RFC 3527 определяет новый субпараметр DHCP, субпараметр выбора канала, который позволяет клиенту DHCP задавать адрес, на который должен ответить Сервер DHCP.

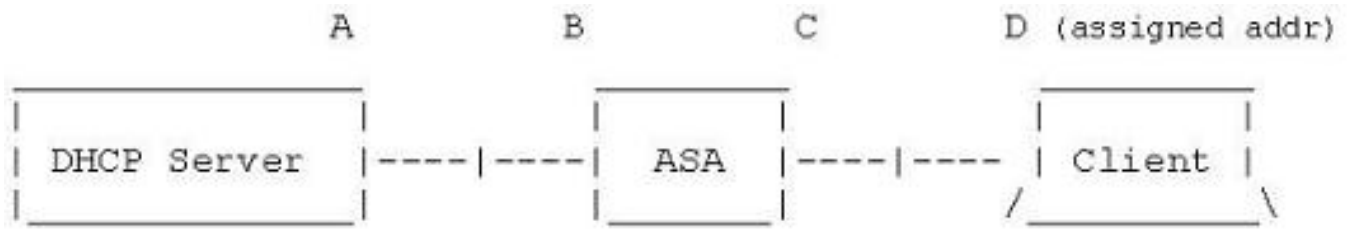
С точки зрения ASA эти RFC позволят пользователю задавать сетевую область dhcp для назначения адреса DHCP, которое не локально для ASA, и Сервер DHCP все еще будет в состоянии ответить непосредственно на интерфейс ASA. Приведенные ниже рисунки должны помочь иллюстрировать новое поведение. Это позволит использованию нелокальные области, не имея необходимость создавать статический маршрут для той области в их сети.

Когда RFC 3011 или RFC 3527 не включены, обмен Прокси DHCP выглядит подобным этому:




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

С любым из этих включенных RFC обмен выглядит подобным этому вместо этого, и клиенту VPN все еще назначают адрес в правильной подсети:



Message Exchange:

Discover: B -> A

Offer: A -> B

Request: B -> A

Ack: A -> B

Release: B -> A

Настройте ASA с использованием CLI

Выполните эти шаги для настройки сервера DHCP для обеспечения IP-адреса клиентам VPN из командной строки. См. серию 5500 Cisco ASA Адаптивные Справочники по командам устройств безопасности для получения дополнительной информации о каждой команде, которая используется.

```
ASA# show run
ASA Version 9.2(1)
!

!--- Specify the hostname for the Security Appliance.

hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!


!--- Configure the outside and inside interfaces.

interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 192.168.10.2 255.255.255.0


!--- Output is suppressed.
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
object network obj-192.168.5.0
subnet 192.168.5.0 255.255.255.0

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1


!--- Specify the location of the ASDM image for ASA to fetch the image
for ASDM access.

asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
obj-192.168.5.0 obj-192.168.5.0
!
object network obj-10.1.1.0
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
```

```
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
!
!--- Enable webvpn and specify an Anyconnect image

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
anyconnect enable
tunnel-group-list enable


group-policy clientgroup internal
group-policy clientgroup attributes


!--- define the DHCP network scope in the group policy.This configuration is Optional

dhcp-network-scope 192.168.5.0


!--- In order to identify remote access users to the Security Appliance,
!--- you can also configure usernames and passwords on the device.

username ssluser1 password ffIRPGpDSOJh9YLq encrypted


!--- Create a new tunnel group and set the connection
!--- type to remote-access.

tunnel-group sslgroup type remote-access


!--- Define the DHCP server address to the tunnel group.

tunnel-group sslgroup general-attributes
default-group-policy clientgroup
dhcp-server 192.168.10.1

!--- If the use of RFC 3011 or RFC 3527 is required then the following command will
enable support for them

tunnel-group sslgroup general-attributes
dhcp-server subnet-selection (server ip) (3011)
hcp-server link-selection (server ip) (3527)

!--- Configure a group-alias for the tunnel-group

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
```

ASA#