Доступ ASA к ASDM от внутреннего интерфейса по примеру конфигурации VPN-туннеля

Содержание

Введение

Этот документ описывает, как настроить Туннель VPN между локальными сетями с использованием двух устройств адаптивной защиты Cisco (ASA) Межсетевые экраны. Cisco Adaptive Security Device Manager (ASDM) работает на удаленном ASA через внешний интерфейс на общедоступной стороне, и это шифрует и обычную сеть и трафик ASDM. ASDM на основе браузера средство конфигурации, которое разработано, чтобы помочь вам устанавливать, настраивать и контролировать свой Межсетевой экран ASA с GUI. Вам не нужны развернутые знания CLI Межсетевого экрана ASA.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Шифрование IPSec
- Cisco ASDM

Примечание: Гарантируйте, что все устройства, которые используются в вашей топологии, удовлетворяют требования, которые описаны в Руководстве по установке оборудования серии 5500 Cisco ASA.

Совет: См. статья Introduction to IP Security (IPSec) Encryption Cisco для получения

знакомства с основным IP - безопасным шифрованием.

Используемые компоненты

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

- Выпуск 9 Программного обеспечения межсетевого экрана Cisco ASA. x.
- ASA 1 и ASA 2 является Межсетевой экран Cisco ASA 5520
- ASA 2 использует Версию 7.2 (1) ASDM

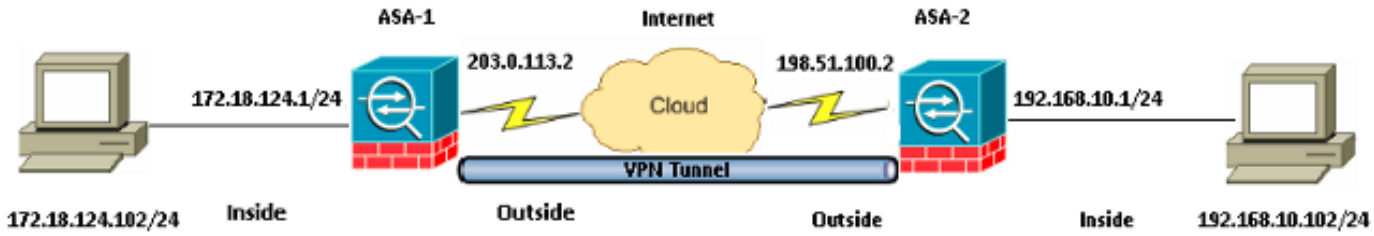
  Примечание: Когда вам предлагают для имени пользователя и пароля для ASDM, настройки по умолчанию не требуют имени пользователя. Если enable password был ранее настроен, введите тот пароль как пароль ASDM. Если нет никакого enable password, выход оба, которые записи имени пользователя и пароля очищают и нажимают **OK** для продолжения.

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.

Настройка

Используйте информацию, которая описана в этом разделе для настройки функций, которые описаны в этом документе.

Схема сети



Конфигурации

Это - конфигурация, которая используется на ASA 1:

ASA-1

```
ASA Version 9.1(5)
!
hostname ASA-1
!
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.18.124.1 255.255.255.0
!

!--- Traffic matching ACL 101 is punted to VPN
!--- Encrypt/Decrypt traffic matching ACL 101

access-list 101 extended permit ip 172.18.124.0 255.255.255.0 192.168.10.0
255.255.255.0

!--- Do not use NAT
!--- on traffic matching below Identity NAT

object network obj_192.168.10.0
subnet 192.168.10.0 255.255.255.0

object network obj_172.18.124.0
subnet 172.18.124.0 255.255.255.0

nat (inside,outside) source static obj_172.18.124.0 obj_172.18.124.0 destination
static obj_192.168.10.0 obj_192.168.10.0 no-proxy-arp route-lookup

!--- Configures a default route towards the gateway router.

route outside 0.0.0.0 0.0.0.0 203.0.113.252 1

!--- Point the configuration to the appropriate version of ASDM in flash

asdm image asdm-722.bin

!--- Enable the HTTP server required to run ASDM.

http server enable

!--- This is the interface name and IP address of the host or
!--- network that initiates the HTTP connection.

http 172.18.124.102 255.255.255.255 inside

!--- Implicitly permit any packet that came from an IPsec
!--- tunnel and bypass the checking of an associated access-group
!--- command statement for IPsec connections.

sysopt connection permit-vpn

!--- Specify IPsec (phase 2) transform set.
!--- Specify IPsec (phase 2) attributes.

crypto ipsec ikev1 transform-set vpn esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 198.51.100.2
crypto map vpn 10 set ikev1 transform-set vpn
crypto map vpn interface outside

!--- Specify ISAKMP (phase 1) attributes.

crypto ikev1 enable outside
```

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- Specify tunnel-group ipsec attributes.

tunnel-group 198.51.100.2 type ipsec-l2l
tunnel-group 198.51.100.2 ipsec-attributes
ikev1 pre-shared-key cisco
```

Это - конфигурация, которая используется на ASA 2:

ASA-2

```
ASA Version 9.1(5)
!
hostname ASA-2
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.10.1 255.255.255.0
!

!--- Traffic matching ACL 101 is punted to VPN
!--- Encrypt/Decrypt traffic matching ACL 101

access-list 101 extended permit ip 192.168.10.0 255.255.255.0 172.18.124.0
255.255.255.0

!--- Do not use NAT
!--- on traffic matching below Identity NAT

object network obj_192.168.10.0
subnet 192.168.10.0 255.255.255.0

object network obj_172.18.124.0
subnet 172.18.124.0 255.255.255.0

nat (inside,outside) source static obj_192.168.10.0 obj_192.168.10.0 destination
static obj_172.18.124.0 obj_172.18.124.0 no-proxy-arp route-lookup

!--- Configures a default route towards the gateway router.

route outside 0.0.0.0 0.0.0.0 198.51.100.252 1

!--- Point the configuration to the appropriate version of ASDM in flash

asdm image asdm-722.bin

!--- Enable the HTTP server required to run ASDM.

http server enable

!--- This is the interface name and IP address of the host or
!--- network that initiates the HTTP connection.
```

```
http 192.168.10.102 255.255.255.255 inside

!--- Add an aditional 'http' configuration to allow the remote subnet
!--- to access ASDM over the VPN tunnel

http 172.18.124.0 255.255.255.0 outside

!--- Implicitly permit any packet that came from an IPsec
!--- tunnel and bypass the checking of an associated access-group
!--- command statement for IPsec connections.

sysopt connection permit-vpn

!--- Specify IPsec (phase 2) transform set.
!--- Specify IPsec (phase 2) attributes.

crypto ipsec ikev1 transform-set vpn esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 203.0.113.2
crypto map vpn 10 set ikev1 transform-set vpn
crypto map vpn interface outside

!--- Specify ISAKMP (phase 1) attributes.

crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- Specify tunnel-group ipsec attributes.

tunnel-group 203.0.113.2 type ipsec-l2l
tunnel-group 203.0.113.2 ipsec-attributes
ikev1 pre-shared-key cisco
```

ASDM/SSH доступа Через VPN-туннель

Для доступа к ASDM через внутренний интерфейс ASA 2 от внутренней сети ASA 1 необходимо использовать команду, которая описана здесь. Эта команда может только использоваться для одного интерфейса. На ASA 2 настройте *управление доступом* с **управлением доступом в** команде:

```
management-access <interface-name>
```

Проверка

Этот раздел предоставляет сведения, который можно использовать, чтобы проверить, что конфигурация работает должным образом.

> **Примечание:** Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show**. Используйте Cisco CLI Анализатор для просматривания аналитику выходных данных команды show.

Используйте эти команды для проверки конфигурации:

- Войдите **show crypto isakmp sa / показывают isakmp sa** команда, чтобы проверить, что Фаза 1 устанавливает правильно.
- Введите **show crypto ipsec sa**, чтобы проверить, что Фаза 2 устанавливает правильно.

Перечень команд

Как только команды VPN введены в ASA, VPN-туннель установлен, когда трафик проходит между ПК ASDM (172.18.124.102) и внутренним интерфейсом ASA 2 (192.168.10.1). На этом этапе ПК ASDM в состоянии достигнуть https://192.168.10.1 и связаться с интерфейсом ASDM ASA 2 по VPN-туннелю.

Устранение неполадок

Этот раздел предоставляет сведения, который можно использовать для устранения проблем конфигурации.

> **Примечание:** См. Проблемы с подключением ASA к статье Cisco Adaptive Security Device Manager Cisco для решения связанных с ASDM проблем.

Пример результата отладки

Введите **команду show crypto isakmp sa** для просмотра туннеля, который сформирован между 198.51.100.2 и 203.0.113.2:

```
ASA-2(config)# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 203.0.113.2
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE
```

Введите **команду show crypto ipsec sa** для просмотра туннеля, который передает трафик между 192.168.10.0 255.255.255.0 и 172. 18.124.0 255.255.255.0:

```
ASA-2(config)# show crypto ipsec sa
interface: outside
Crypto map tag: vpn, seq num: 10, local addr: 198.51.100.2

access-list 101 extended permit ip 192.168.10.0 255.255.255.0
172.18.124.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)
current_peer: 203.0.113.2

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 198.51.100.2/0, remote crypto endpt.: 203.0.113.2/0
path mtu 1500, ipsec overhead 58(36), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: DDE6AD22
current inbound spi : 92425FE5

inbound esp sas:
spi: 0x92425FE5 (2453823461)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: vpn
sa timing: remaining key lifetime (kB/sec): (4373999/28658)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003F
outbound esp sas:
spi: 0xDDE6AD22 (3722882338)
transform: esp-3des esp-md5-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: vpn
sa timing: remaining key lifetime (kB/sec): (4373999/28658)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Дополнительные сведения

- Справочник по командам Cisco ASA
- Cisco Systems – техническая поддержка и документация