ASA Access to the ASDM via een interne interface via een VPN-tunnelconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een LAN-to-LAN VPN-tunnel kunt configureren met het gebruik van twee Firewalls van Cisco adaptieve security applicatie (ASA). De Cisco Adaptieve Security Devices Manager (ASDM) gaat op de externe ASA door de externe interface aan de openbare zijde en versleutelt zowel het reguliere netwerk als het ASDM-verkeer. ASDM is een browser-gebaseerd configuratiegereedschap dat ontworpen is om u te helpen uw ASA Firewall met een GUI in te stellen, te configureren en te bewaken. U hebt geen uitgebreide kennis nodig van de ASA Firewall CLI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IPsec-encryptie
- Cisco ASDM

  Opmerking: Zorg ervoor dat alle apparaten die in uw topologie worden gebruikt aan de vereisten voldoen die in de Cisco ASA 5500 Series hardwareinstallatiehandleiding worden beschreven.

  Tip: Raadpleeg het artikel An Inleiding to IP Security (IPSec), encryptie van Cisco om

vertrouwd te raken met de basisencryptie van IPsec.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA-firewallsoftwarerelease 9.x.
- ASA 5520-1 en ASA-2 zijn Cisco ASA Firewall.
- ASA 2 gebruikt ASDM versie 7.2(1)

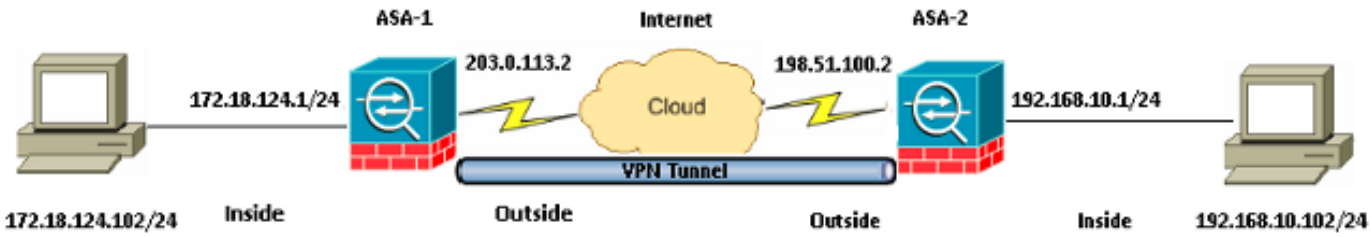
  Opmerking: Wanneer u om een gebruikersnaam en wachtwoord voor de ASDM wordt gevraagd, hebben de standaardinstellingen geen gebruikersnaam nodig. Als u een wachtwoord invoert dat eerder is ingesteld, voert u dat wachtwoord in als het ASDM-wachtwoord. Als er geen wachtwoord wordt ingeschakeld, laat u zowel de gebruikersnaam als de wachtwoorden leeg en klikt u op **OK** om door te gaan.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Gebruik de informatie die in deze sectie wordt beschreven om de functies te configureren die in dit document worden beschreven.

Netwerkdiagram



Configuraties

Dit is de configuratie die gebruikt wordt op 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
```

Dit is de configuratie die gebruikt wordt op 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
```

Access ASDM/SDH via een VPN-tunnelband

Om toegang te krijgen tot ASDM via de binneninterface van ASA-2 van het ASA-1 binnennetwerk moet u de opdracht gebruiken die hier wordt beschreven. Deze opdracht kan alleen voor één interface worden gebruikt. Op ASA-2, vorm *beheer-toegang* met de **beheer-toegang binnen** opdracht:

```
management-access
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te controleren of uw configuratie correct werkt.

> Opmerking: De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show-**opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

Gebruik deze opdrachten om de configuratie van het apparaat te controleren:

- Voer de opdracht **show crypto isakmp sa/show isakmp sa in** om te controleren of fase 1 **correct** is.
- Voer de **show crypto ipsec in zoals** om te verifiëren dat fase 2 correct is ingesteld.

Overzicht van opdrachten

Zodra de VPN-opdrachten in de ASA's zijn ingevoerd, wordt een VPN-tunnel tot stand gebracht wanneer het verkeer verloopt tussen de ASDM-pc (172.18.124.102) en de interne interface van ASA-2 (192.168.10.1). Op dit punt kan de ASDM PC https://192.168.10.1 bereiken en communiceren met de ASDM interface van ASA-2 via de VPN-tunnel.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

> Opmerking: Raadpleeg de ASA Connection-problemen naar het Cisco-artikel van Cisco Adaptieve Security Manager om problemen met ASDM op te lossen.

Voorbeeld van output van foutopsporing

Voer de opdracht **show crypto isakmp in** om de tunnel te bekijken die tussen 198.51.100.2 en 203.0.113.2 wordt gevormd:

```
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
```

Voer de opdracht **show crypto ipsec in** om de tunnel te bekijken die tussen 192.168.10.0 255.255.255.0 en 172.18.124.0 255.255.255.0 vertrekt:

```
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
```

Gerelateerde informatie

- Cisco ASA-opdracht
- Technische ondersteuning en documentatie – Cisco Systems