VPN 터널을 통한 내부 인터페이스에서 ASDM에 대한 ASA 액세스 컨피그레이션 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[VPN 터널을 통해 ASDM/SSH 액세스](#)
[다음을 확인합니다.](#)
[명령 요약](#)
[문제 해결](#)
[디버그 출력 샘플](#)
[관련 정보](#)

소개

이 문서에서는 두 Cisco ASA(Adaptive Security Appliance) 방화벽을 사용하여 LAN-to-LAN VPN 터널을 구성하는 방법에 대해 설명합니다.Cisco ASDM(Adaptive Security Device Manager)은 원격 ASA에서 퍼블릭 측의 외부 인터페이스를 통해 실행되며, 일반 네트워크와 ASDM 트래픽을 모두 암호화합니다.ASDM은 GUI를 사용하여 ASA 방화벽을 설정, 구성 및 모니터링하는 데 도움이 되도록 설계된 브라우저 기반 컨피그레이션 툴입니다.ASA 방화벽 CLI에 대한 폭넓은 지식이 필요하지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IPsec 암호화
- Cisco ASDM

참고:토폴로지에서 사용되는 모든 디바이스가 Cisco ASA 5500 Series 하드웨어 설치 가이드에 설명된 요구 사항을 충족하는지 확인합니다.

팁:기본 IPsec 암호화에 대한 친숙성을 얻으려면 An Introduction to IP Security (IPSec) Encryption Cisco 문서를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA Firewall 소프트웨어 릴리스 9.x.
- ASA-1 및 ASA-2는 Cisco ASA Firewall 5520
- ASA 2는 ASDM 버전 7.2(1)을 사용합니다.

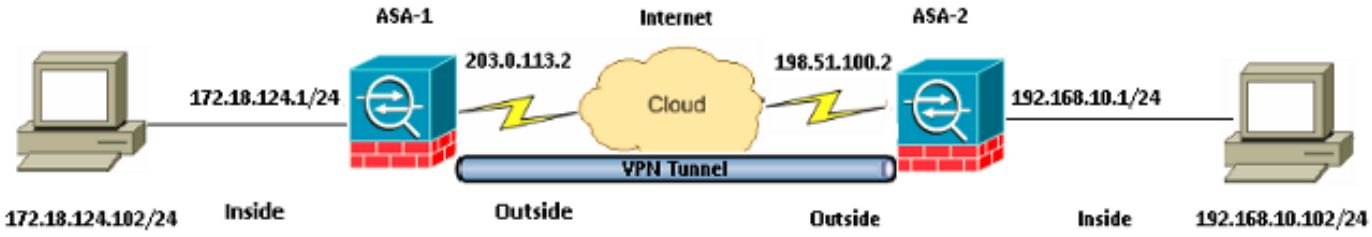
  참고:ASDM에 대한 사용자 이름 및 비밀번호를 입력하라는 프롬프트가 표시되면 기본 설정에 사용자 이름이 필요하지 않습니다.enable 비밀번호가 이전에 구성된 경우 해당 비밀번호를 ASDM 비밀번호로 입력합니다.enable 비밀번호가 없으면 사용자 이름과 비밀번호 항목을 모두 비워 두고 **OK**(확인)를 클릭하여 계속 진행합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 문서에 설명된 기능을 구성하려면 이 섹션에 설명된 정보를 사용합니다.

네트워크 다이어그램



구성

다음은 ASA-1에서 사용되는 컨피그레이션입니다.

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
```

다음은 ASA-2에서 사용되는 컨피그레이션입니다.

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
```

VPN 터널을 통해 ASDM/SSH 액세스

ASA-1 내부 네트워크에서 ASA-2의 내부 인터페이스를 통해 ASDM에 액세스하려면 여기에 설명된 명령을 사용해야 합니다.이 명령은 하나의 인터페이스에만 사용할 수 있습니다.ASA-2에서 **management-access inside** 명령을 사용하여 *management-access*를 구성합니다.

```
management-access
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:**Cisco CLI Analyzer(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 Cisco CLI Analyzer를 사용합니다.

컨피그레이션을 확인하려면 다음 명령을 사용합니다.

- 1단계가 올바르게 설정되었는지 확인하려면 **show crypto isakmp sa/show isakmp sa** 명령을 입력합니다.
- 2단계가 올바르게 설정되었는지 확인하려면 **show crypto ipsec sa**를 입력합니다.

명령 요약

ASA에 VPN 명령을 입력하면 ASDM PC(172.18.124.102)과 ASA-2(192.168.10.1)의 내부 인터페이스 간에 트래픽이 전달될 때 VPN 터널이 설정됩니다. 이 시점에서 ASDM PC는 https://192.168.10.1에 연결하여 VPN 터널을 통해 ASA-2의 ASDM 인터페이스와 통신할 수 있습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:**ASDM 관련 문제를 트러블슈팅하려면 Cisco Adaptive Security Device Manager Cisco에 대한 ASA 연결 문제 문서를 참조하십시오.

디버그 출력 샘플

198.51.100.2에서 203.0.113.2 사이의 터널을 보려면 **show crypto isakmp sa** 명령을 입력합니다.

```
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
```

192.168.10.0 255.255.255.0~172 사이의 트래픽을 전달하는 터널을 보려면 **show crypto ipsec sa** 명령을 입력합니다. 18.124.0:

```
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
```

관련 정보

- Cisco ASA 명령 참조
- 기술 지원 및 문서 – Cisco Systems