PIX/ASA 7.x 이상: 중복 네트워크를 사용하는 LAN-to-LAN IPsec VPN 컨피그레이션 예

목차

소개

이 문서에서는 두 보안 어플라이언스와 인터넷 트래픽을 PAT하여 LAN-to-LAN(L2L) IPsec 터널을 통해 이동하는 VPN 트래픽을 변환(NAT)하는 단계에 대해 설명합니다. 각 보안 어플라이언스에는 그 뒤에 보호되는 사설 네트워크가 있습니다. 이 예에서는 내부 네트워크가 동일하고 겹치는 두 개의 Cisco ASA(Adaptive Security Appliance)가 VPN 터널을 통해 연결됩니다. 일반적인 시나리오에서는 사용자가 동일한 서브넷의 IP 주소를 ping하기 때문에 ping 패킷이 로컬 서브넷에서 나가지 않으므로 VPN 간의 통신이 발생하지 않습니다. 이 두 개인 내부 네트워크가 서로 통신하기 위해 정책 NAT는 로컬 서브넷의 변환을 위해 두 ASA에서 모두 사용되므로 통신이 예상대로 이루어집니다.

사전 요구 사항

요구 사항

이 컨피그레이션 예제를 진행하기 전에 Cisco ASA에 인터페이스의 IP 주소를 구성했는지 확인하고 기본 연결을 설정해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 7.x 이상

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.

관련 제품

이 컨피그레이션은 Cisco PIX Security Appliance 버전 7.x 이상에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

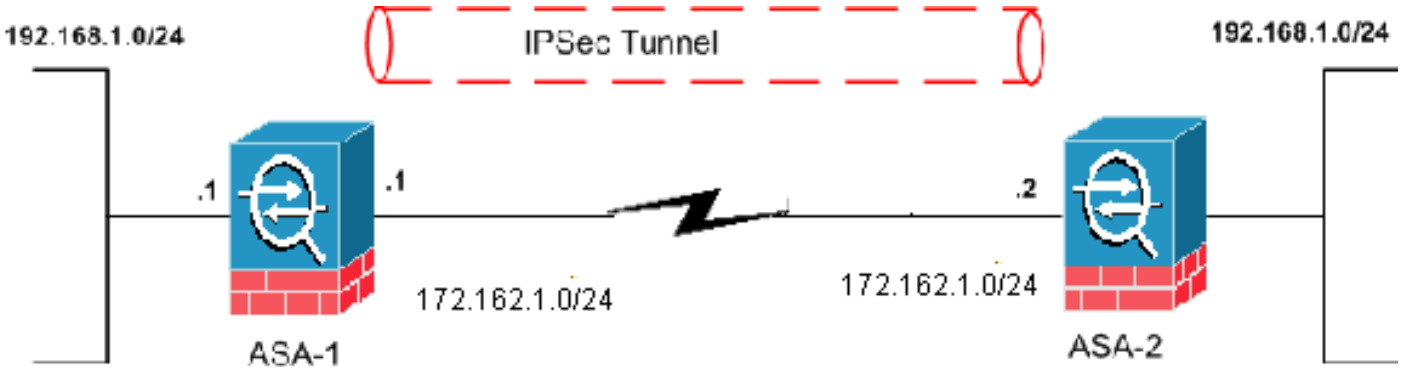
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- ASA-1 컨피그레이션
- ASA-2 컨피그레이션

ASA-1

```
ASA-1#show running-config
: Saved
:
ASA Version 8.0(3)
```

```
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.162.1.1 255.255.255.0
!--- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
192.168.1.1 255.255.255.0 !--- Configure the inside
interface. passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list new extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- This access
list (new) is used with the crypto map (outside_map) !--
- in order to determine which traffic should be
encrypted !--- and sent across the tunnel.
access-list policy-nat extended permit ip 192.168.1.0
255.255.255.0 192.168.3.0 255.255.255.0

!--- The policy-nat ACL is used with the static !---
command in order to match the VPN traffic for
translation.

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-615.bin
no asdm history enable
arp timeout 14400


static (inside,outside) 192.168.2.0  access-list policy-
nat
!--- It is a Policy NAT statement. !--- The static
command with the access list (policy-nat), !--- which
matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.2.0 for outbound VPN
traffic.


global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- The previous statements PAT the Internet traffic !-
-- except for the VPN traffic that uses the IP address
172.17.1.1. route outside 0.0.0.0 0.0.0.0 172.162.1.2 1
!--- Output is suppressed. !--- PHASE 2 CONFIGURATION --
-! !--- The encryption types for Phase 2 are defined
here. crypto ipsec transform-set CISCO esp-des esp-md5-
hmac !--- Define the transform set for Phase 2. crypto
map outside_map 20 match address new !--- Define which
traffic should be sent to the IPsec peer with the !---
access list (new). crypto map outside_map 20 set peer
172.162.1.2 !--- Sets the IPsec peer (remote end point)
crypto map outside_map 20 set transform-set CISCO !---
Sets the IPsec transform set "CISCO" !--- to be used
with the crypto map entry "outside_map" crypto map
outside_map interface outside !--- Specifies the
interface to be used with !--- the settings defined in
this configuration !--- PHASE 1 CONFIGURATION ---! !---
This configuration uses isakmp policy 65535. !--- Policy
65535 is included in the configuration by default. !---
```

```
These configuration commands define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 tunnel-group 172.162.1.2
type ipsec-l2l !--- In order to create and manage the
database of connection-specific records !--- for IPsec-
L2L-IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--
- command in global configuration mode. !--- For L2L
connections, the name of the tunnel group must be !---
the IP address of the IPsec peer (remote peer end).

tunnel-group 172.162.1.2 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared key in order to configure the
authentication method. telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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
Cryptochecksum:33e1e37cd1280d908210dac0cc26e706 : end
```

ASA-2

```
ASA-2#show running-config
: Saved
:
ASA Version 8.0(3)
!
hostname ASA-2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.162.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
!--- Output is suppressed. access-list new extended
permit ip 192.168.3.0 255.255.255.0 192.168.2.0
255.255.255.0 !--- This access list (new) is used with
the crypto map (outside_map) !--- in order to determine
which traffic needs to be encrypted !--- and sent across
the tunnel.
access-list policy-nat extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0

!--- The policy-nat ACL is used with the static !---
command in order to match the VPN traffic for
translation.

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
```

```
asdm image flash:/asdm-615.bin
no asdm history enable
arp timeout 14400



static (inside,outside) 192.168.3.0  access-list policy-
nat
!--- This is a Policy NAT statement. !--- The static
command with the access list (policy-nat), !--- which
matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.3.0 for outbound VPN
traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- The previous statements PAT the Internet traffic !-
-- except the VPN traffic that uses the outside
interface IP address. route outside 0.0.0.0 0.0.0.0
172.162.1.2 1 !--- PHASE 2 CONFIGURATION ---! !--- The
encryption types for Phase 2 are defined here. crypto
ipsec transform-set CISCO esp-des esp-md5-hmac !---
Define the transform set for Phase 2. crypto map
outside_map 20 match address new !--- Define which
traffic needs to be sent to the IPsec peer. crypto map
outside_map 20 set peer 172.162.1.1 !--- Sets the IPsec
peer. crypto map outside_map 20 set transform-set CISCO
!--- Sets the IPsec transform set "CISCO" !--- to be
used with the crypto map entry "outside_map". crypto map
outside_map interface outside !--- Specifies the
interface to be used with !--- the settings defined in
this configuration. !--- PHASE 1 CONFIGURATION ---! !---
This configuration uses isakmp policy 65535 !--- which
is included in the configuration by default. !--- The
configuration commands here define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
address crypto isakmp enable outside crypto isakmp
policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 !--- Output is
suppressed. !--- In order to create and manage the
database of connection-specific !--- records for IPsec-
L2L-IPsec (LAN-to-LAN) tunnels, use the !--- tunnel-
group  command in global configuration mode. !--- For
L2L connections, the name of the tunnel group must be !-
-- the IP address of the IPsec peer.



tunnel-group 172.162.1.1 type ipsec-l2l
tunnel-group 172.162.1.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared key in order to configure the
authentication method. prompt hostname context
Cryptochecksum:6b505b4a05c1aee96a71e67c23e71865 : end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Associations)를 모두 표시합니다.
- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

ASA-1의 명령 표시

```
ASA-1#show crypto isakmp sa



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: 172.162.1.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

ASA-1#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.1

      access-list new permit ip 192.168.2.0 255.255.255.0 192.168.3.0

255.255.2
5.0
      local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 172.162.1.2

      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #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
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.162.1.1, remote crypto endpt.: 172.162.1.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 0BA6CD7E

    inbound esp sas:
      spi: 0xFB4BD01A (4216049690)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824999/27738)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x0BA6CD7E (195480958)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824999/27738)
         IV size: 8 bytes
         replay detection support: Y

ASA-1#show nat
```

```
NAT policies on Interface inside:
  match ip inside 192.168.1.0 255.255.255.0 outside 192.168.3.0 255.255.255.0
    static translation to 192.168.2.0
    translate_hits = 12, untranslate_hits = 5
  match ip inside any outside any
    dynamic translation to pool 1 (172.162.1.1 [Interface PAT])
    translate_hits = 0, untranslate_hits = 0
  match ip inside any inside any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip inside any dmz any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0

ASA-1#show xlate

1 in use, 1 most used
Global 192.168.2.0 Local 192.168.1.0
```

ASA-2의 명령 표시

```
ASA-2#show crypto ipsec sa

interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.2

      access-list new permit ip 192.168.3.0 255.255.255.0 192.168.2.0

255.255.25
5.0
      local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
      current_peer: 172.162.1.1

      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #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
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.162.1.2, remote crypto endpt.: 172.162.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: FB4BD01A

    inbound esp sas:
      spi: 0x0BA6CD7E (195480958)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/26902)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xFB4BD01A (4216049690)
         transform: esp-des esp-md5-hmac none
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 8192, crypto-map: outside_map
```

```
        sa timing: remaining key lifetime (kB/sec): (4274999/26902)
        IV size: 8 bytes
        replay detection support: Y


ASA-2#show crypto isakmp sa

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: 172.162.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

문제 해결

보안 연결 지우기

문제를 해결할 때 변경 후 기존 SA를 지워야 합니다. PIX의 특권 모드에서 다음 명령을 사용합니다.

- **clear crypto ipsec sa** - 활성 IPsec SA를 삭제합니다.
- **clear crypto isakmp sa** - 활성 IKE SA를 삭제합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

관련 정보

- 가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션
- PIX 7.0 및 Adaptive Security Appliance Port Redirection(Forwarding) with nat, global, static, patoral 및 access-list 명령
- PIX/ASA 7.x 및 FWSM: NAT 및 PAT 문
- Cisco ASA 5500 Series 보안 어플라이언스
- Cisco PIX 500 Series 보안 어플라이언스
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems