PIX/ASA 7.x 以降：オーバーラップ ネットワーク構成を使用した LAN-to-LAN IPSec VPN の例

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[関連製品](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[確認](#)
[ASA-1 からの show コマンド](#)
[ASA-2 からの show コマンド](#)
[トラブルシュート](#)
[セキュリティ アソシエーションの消去](#)
[トラブルシューティングのためのコマンド](#)
[関連情報](#)

概要

このドキュメントでは、2 台のセキュリティ アプライアンス間の LAN-to-LAN (L2L) IPSec トンネルを通過する VPN トラフィックの変換 (NAT) の手順と、インターネット トラフィックの変換 (PAT) の手順について説明します。各セキュリティ アプライアンスには、その背後に保護された、プライベート ネットワークがあります。次の例では、まったく同じオーバーラップしている内部ネットワークを持つ 2 台の Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) が、VPN トンネル上で接続されています。通常のシナリオでは、ユーザが同じサブネットの IP アドレスを ping 送信しても ping パケットがローカル サブネットから離れないため、VPN 上の通信は不可能です。これらの 2 つの内部ネットワークは相互通信に使用されるため、通信が正常に行われるように Policy NAT が両方の ASA でローカル サブネットの変換に使用されます。

前提条件

要件

この設定例に進む前に、インターフェイス上の IP アドレスを使って Cisco 適応型セキュリティ アプライアンスが設定されていること、および基本的な接続が確立されていることを確認してください。

使用するコンポーネント

このドキュメントの情報は次のソフトウェア バージョンに基づいています。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

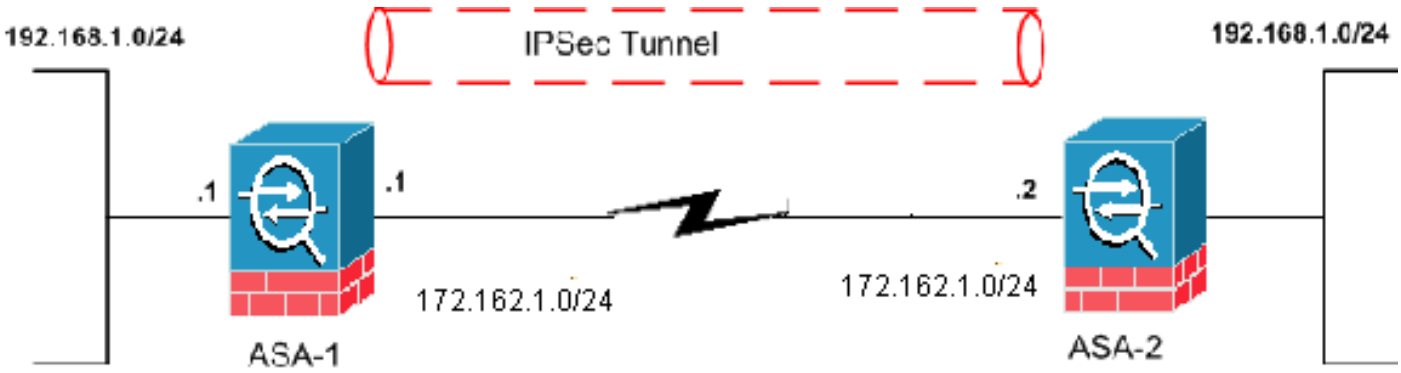
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されるコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- ASA-1 の設定
- ASA-2 の設定

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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto isakmp sa**：ピアの現在の IKE セキュリティ アソシエーション（SA）すべてを表示します。
- **show crypto ipsec sa**：現在の SA が使用している設定を表示します。

ASA-1 からの show コマンド

```
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-2 からの show コマンド

```
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
```

トラブルシュート

セキュリティ アソシエーションの消去

トラブルシューティングで変更を行った後、既存の SA を必ず消去してください。PIX の特権モードで、次のコマンドを使用します。

- **clear crypto ipsec sa：アクティブな IPSec SA を削除します。**
- **clear crypto isakmp sa：アクティブな IKE SA を削除します。**

トラブルシューティングのためのコマンド

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の解析を表示するには、OIT を使用します。

注：debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

- **debug crypto ipsec：フェーズ 2 の IPsec ネゴシエーションを表示します。**
- **debug crypto isakmp：フェーズ 1 の ISAKMP ネゴシエーションを表示します。**

関連情報

- 一般的な L2L およびリモート アクセス IPsec VPN のトラブルシューティング方法について
- nat、global、static および access-list コマンドを使用した PIX 7.0 および適応型セキュリティ アプライアンスのポート リダイレクション（フォワーディング）
- PIX/ASA 7.x と FWSM：NAT および PAT ステートメント
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems