

PIX/ASA 7.x and Later: LAN-to-LAN IPsec VPN with Overlapping Networks Configuration Example

Document ID: 112049

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- show Commands from ASA-1
- show Commands from ASA-2

Troubleshoot

- Clear Security Associations
- Troubleshooting Commands

Related Information

Introduction

This document describes the steps used to translate (NAT) the VPN traffic that travels over a LAN-to-LAN (L2L) IPsec tunnel between two security appliances and also PAT the Internet traffic. Each security appliance has a private, protected network behind it. In this example two Cisco Adaptive Security Appliances (ASAs) with identical and overlapping internal networks are connected over the VPN tunnel. In a normal scenario, communication across the VPN never happens because the ping packets never leave the local subnet since the user pings the IP address of the same subnet. For these two private internal networks to communicate with each other, Policy NAT is used on both ASAs for translation of the local subnet so that the communication happens as expected.

Prerequisites

Requirements

Make sure you have configured the Cisco Adaptive Security Appliance with IP addresses on the interfaces, and have basic connectivity before you proceed with this configuration example.

Components Used

The information in this document is based on this software version:

- Cisco Adaptive Security Appliance Software version 7.x and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco PIX Security Appliance version 7.x and later.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

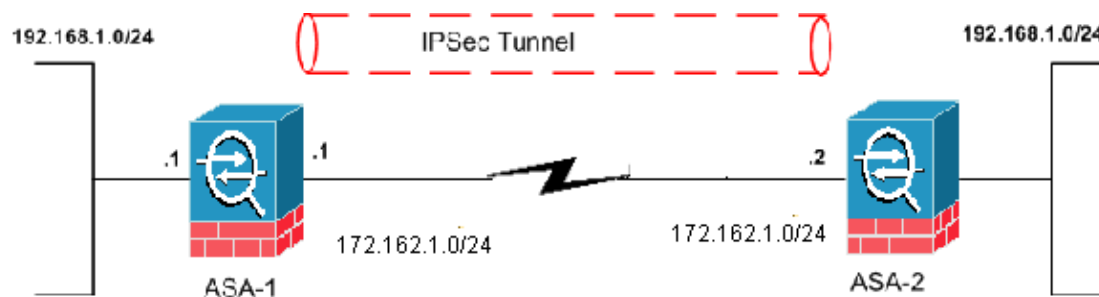
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- ASA-1 Configuration
- ASA-2 Configuration

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

```

Verify

Use this section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output:

- **show crypto isakmp sa** – Shows all current IKE Security Associations (SAs) at a peer.
- **show crypto ipsec sa** – Shows the settings used by current SAs.

show Commands from ASA-1

```
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

```

show Commands from ASA-2

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

```

Troubleshoot

Clear Security Associations

When you troubleshoot, be sure to clear existing SAs after you make a change. In the privileged mode of the PIX, use these commands:

- **clear crypto ipsec sa** – Deletes the active IPsec SAs.
- **clear crypto isakmp sa** – Deletes the active IKE SAs.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** – Displays the IPsec negotiations of Phase 2.

- **debug crypto isakmp** – Displays the ISAKMP negotiations of Phase 1.

Related Information

- **Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions**
 - **PIX 7.0 and Adaptive Security Appliance Port Redirection(Forwarding) with nat, global, static, conduit, and access-list Commands**
 - **PIX/ASA 7.x and FWSM: NAT and PAT Statements**
 - **Cisco ASA 5500 Series Security Appliances**
 - **Cisco PIX 500 Series Security Appliances**
 - **IPsec Negotiation/IKE Protocols**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 09, 2010

Document ID: 112049
