PIX/ASA 7.x and later: Site to Site (L2L) IPsec VPN with Policy NAT Configuration Example

Document ID: 99122

Contents

Introduction

This document describes the steps used to translate (NAT) the VPN traffic from one end that travel 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.

The network 192.168.1.0 in PIX−A is translated to 172.18.1.0 network and send the VPN traffic through the IPsec tunnel.

In L2L VPN, you can initiate the IPsec tunnel from either side of tunnel end points. In this scenario, PIX−A of inside network (192.168.1.0) is translated to 172.18.1.0 network using Policy NAT for VPN traffic. Because of this translation, the source network of the interesting traffic 172.18.1.0 is not reachable from PIX−B. If you try to initiate the tunnel from the PIX−B, the destination address of the VPN interesting traffic 172.18.1.0 , for example, natted network address of PIX−A, is not reachable. So you must initiate the VPN tunnel only from the PIX−A.

Prerequisites

Requirements

Ensure that you have configured the PIX 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 these software and hardware versions:

• Cisco PIX 500 Series Security Appliance runs with 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 5500 Series Adaptive Security Appliance runs with software 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:
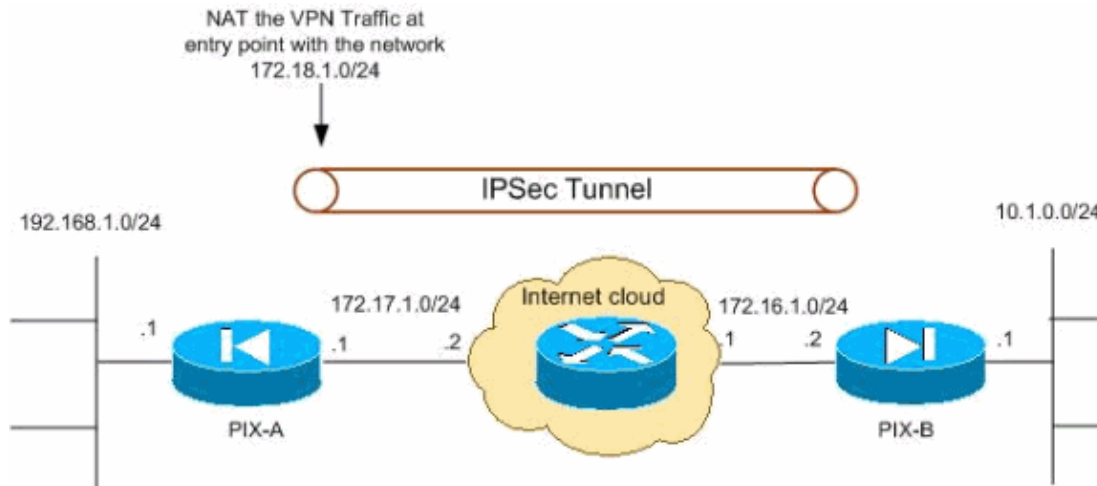
Configurations

This document uses these configurations:

• PIX–A Configuration
• PIX–B Configuration

PIX–A

`PIX-A#`**`show running-config`**
`: Saved`
`:`

```
PIX Version 7.1(1)
!
hostname PIX-A
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.17.1.1 255.255.255.0

!--- 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 172.18.1.0 255.255.255.0 10.1.0.0 255.255.255.0

!--- 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 10.1.0.0 255.255.255.0


!--- 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-511.bin
no asdm history enable
arp timeout 14400

static (inside,outside) 172.18.1.0  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 172.18.1.0
!--- for outbound VPN traffic


global (outside) 1 172.19.1.1
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- The above statements will PAT the internet traffic
!--- except the VPN traffic using the IP address 172.19.1.1


route outside 0.0.0.0 0.0.0.0 172.17.1.2 1
```

```
!--- Output suppressed



!--- PHASE 2 CONFIGURATION ---!
!--- The encryption types for Phase 2 are defined here.

crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-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 172.16.1.2

!--- Sets the IPsec peer (remote end point)

crypto map outside_map 20 set transform-set ESP-AES-256-SHA

!--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- 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 10.
!--- Policy 65535 is included in the configuration by default.
!--- These configuration commands define the
!--- Phase 1 policy parameters that are used.

isakmp identity address
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400

isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400

tunnel-group 172.16.1.2 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 172.16.1.2 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
```

PIX–B

```
PIX-B#show running-config
: Saved
:
PIX Version 8.0(2)
!
hostname PIX-B
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.0.1 255.255.255.0
!

!--- Output Suppressed


access-list 102 extended permit ip 10.1.0.0 255.255.255.0 172.18.1.0 255.255.255.0

!--- This access list (102) is used with the crypto map
!--- outside_map in order to determine which traffic should be encrypted
!--- and sent across the tunnel.

access-list no-nat extended permit ip 10.1.0.0 255.255.255.0 172.18.1.0 255.255.255.0

!--- This access list (no-nat) is used with the
!--- nat zero command.
```

```
!--- This prevents traffic, which matches the access list, from undergoing
!--- network address translation (NAT).


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



nat (inside) 0 access-list no-nat


!--- NAT 0 prevents NAT for networks specified in the ACL (no-nat).


route outside 0.0.0.0 0.0.0.0 172.16.1.1 1

!--- PHASE 2 CONFIGURATION ---!
!--- The encryption types for Phase 2 are defined here.

crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

!--- Define the transform set for Phase 2.


crypto map outside_map 20 match address 102

!--- Define which traffic should be sent to the IPsec peer.


crypto map outside_map 20 set peer 172.17.1.1

!--- Sets the IPsec peer


crypto map outside_map 20 set transform-set ESP-AES-256-SHA

!--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- 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 10.
!--- Policy 65535 is included in the config 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 10
 authentication pre-share
 encryption aes-256
 hash sha
```

```
 group 5
 lifetime 86400

crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
no crypto isakmp nat-traversal

!--- Output 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 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 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.

Sample

Show Commands from PIX–A

```
PIX-A#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: 172.16.1.2
    Type    : L2L            Role    : initiator
    Rekey   : no             State   : MM_ACTIVE

PIX-A#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.17.1.1
```

```
            access-list new permit ip 172.18.1.0 255.255.255.0 10.1.0.0 255.255.255.0
            local ident (addr/mask/prot/port): (172.18.1.0/255.255.255.0/0/0)
            remote ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
            current_peer: 172.16.1.2

            #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
            #send errors: 0, #recv errors: 0

            local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.2

            path mtu 1500, ipsec overhead 76, media mtu 1500
            current outbound spi: 95D66663

        inbound esp sas:
          spi: 0x9A4CB431 (2588718129)
             transform: esp-aes-256 esp-sha-hmac
             in use settings ={L2L, Tunnel, }
             slot: 0, conn_id: 1, crypto-map: outside_map
             sa timing: remaining key lifetime (kB/sec): (4274999/28758)
             IV size: 16 bytes
             replay detection support: Y
        outbound esp sas:
          spi: 0x95D66663 (2513856099)
             transform: esp-aes-256 esp-sha-hmac
             in use settings ={L2L, Tunnel, }
             slot: 0, conn_id: 1, crypto-map: outside_map
             sa timing: remaining key lifetime (kB/sec): (4274999/28756)
             IV size: 16 bytes
             replay detection support: Y

   PIX-A#show nat

NAT policies on Interface inside:
   match ip inside 192.168.1.0 255.255.255.0 outside 10.1.0.0 255.255.255.0
      static translation to 172.18.1.0
      translate_hits = 5, untranslate_hits = 5

   PIX-A#show xlate
1 in use, 2 most used
Global 172.18.1.0 Local 192.168.1.0
```

Show Commands from PIX-B

```
   PIX-B#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.16.1.2

       access-list 102 permit ip 10.1.0.0 255.255.255.0 172.18.1.0 255.255.255.0
       local ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (172.18.1.0/255.255.255.0/0/0)
       current_peer: 172.17.1.1

       #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
       #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 14, #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.: 172.16.1.2, remote crypto endpt.: 172.17.1.1
```

```
            path mtu 1500, ipsec overhead 74, media mtu 1500
            current outbound spi: 9A4CB431

         inbound esp sas:
           spi: 0x95D66663 (2513856099)
              transform: esp-aes-256 esp-sha-hmac none
              in use settings ={L2L, Tunnel, }
              slot: 0, conn_id: 16384, crypto-map: outside_map
              sa timing: remaining key lifetime (kB/sec): (3824998/28712)
              IV size: 16 bytes
              replay detection support: Y
         outbound esp sas:
           spi: 0x9A4CB431 (2588718129)
              transform: esp-aes-256 esp-sha-hmac none
              in use settings ={L2L, Tunnel, }
              slot: 0, conn_id: 16384, crypto-map: outside_map
              sa timing: remaining key lifetime (kB/sec): (3824998/28712)
              IV size: 16 bytes
              replay detection support: Y


   PIX-B#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: 172.17.1.1
       Type    : L2L            Role    : responder
       Rekey   : no             State   : MM_ACTIVE
```

Troubleshoot

Clear Security Associations

When you troubleshoot, be sure to clear existing Security Associations 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) (OIT) 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 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**

Updated: Oct 24, 2008   Document ID: 99122