

PIX/ASA 7.x: Add/Remove a Network on an Existing L2L VPN Tunnel Configuration Example

Document ID: 82209

Introduction

Prerequisites

Requirements

Components Used

Related Products

Conventions

Background Information

Configure

Network Diagram

Adding Network to the IPSec Tunnel

Removing Network from IPSec Tunnel

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample configuration for how to add a new network to an existing VPN tunnel.

Prerequisites

Requirements

Ensure that you have a PIX/ASA Security Appliance that runs 7.x code before you attempt this configuration.

Components Used

The information in this document is based on two Cisco 5500 Security Appliance devices.

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 the PIX 500 Security Appliance.

Conventions

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

Background Information

There is currently a LAN-to-LAN (L2L) VPN tunnel that is between the NY and TN office. The NY office just added a new network to be used by the CSI development group. This group requires access to resources that reside in the TN office. The task at hand is to add the new network to the already existing VPN tunnel.

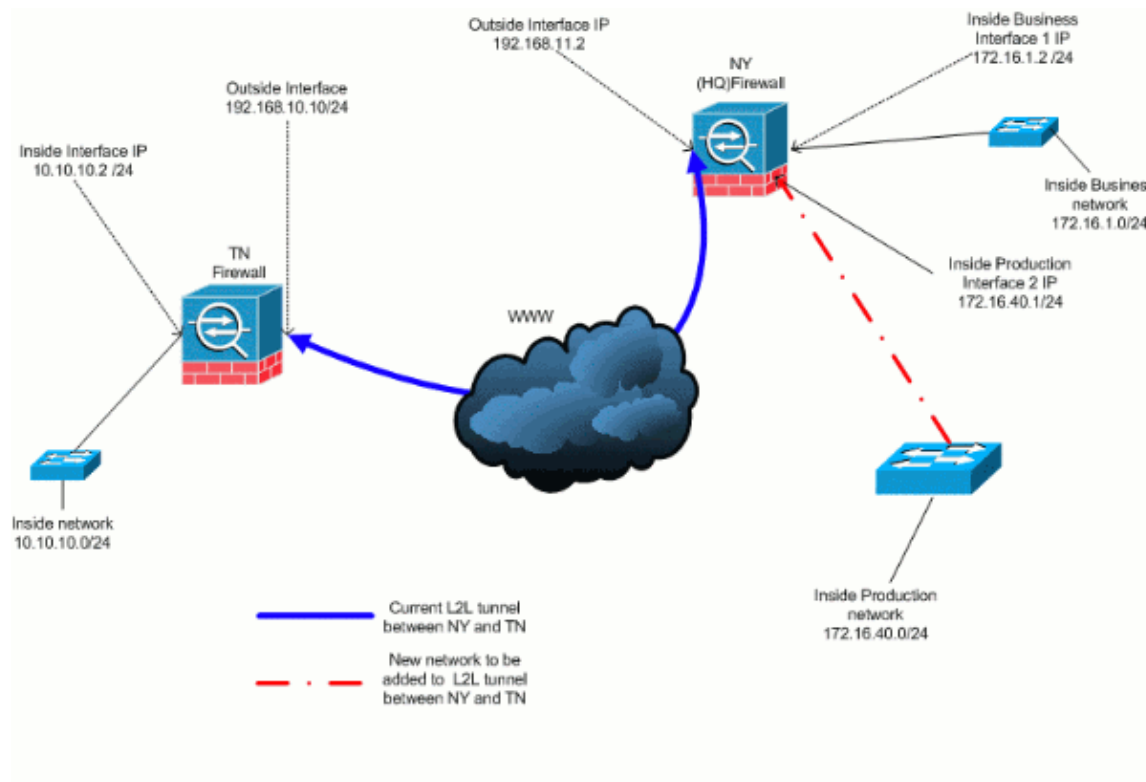
Configure

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) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Adding Network to the IPSec Tunnel

This document uses this configuration:

```
NY (HQ) Firewall Config
ASA-NY-HQ#show running-config
: Saved
:
ASA Version 7.2(2)
!
```

```

hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbul encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 nameif Cisco
 security-level 70
 ip address 172.16.40.2 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp2.com
access-list inside_nat0_outbound extended permit ip 172.16.1.0
 255.255.255.0 10.10.10.0 255.255.255.0

!--- You must be sure that you configure the
!--- opposite of these access control lists
!--- on the other end of the VPN tunnel.

access-list inside_nat0_outbound extended permit ip 172.16.40.0
 255.255.255.0 10.10.10.0 255.255.255.0

access-list outside_20_cryptomap extended permit ip 172.16.1.0
 255.255.255.0 10.10.10.0 255.255.255.0

!--- You must be sure that you configure the
!--- opposite of these access control lists
!--- on the other end of the VPN tunnel.

access-list outside_20_cryptomap extended permit ip 172.16.40.0
 255.255.255.0 10.10.10.0 255.255.255.0

!--- Output is suppressed.

```

```

nat-control
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 172.16.1.0 255.255.255.0

!--- The new network is also required to have access to the Internet.
!--- So enter an entry into the NAT statement for this new network.

nat (inside) 1 172.16.40.0 255.255.255.0

route outside 0.0.0.0 0.0.0.0 192.168.11.100 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10
crypto map outside_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
crypto isakmp nat-traversal 20
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
  pre-shared-key *

!--- Output is suppressed.

: end
ASA-NY-HQ#

```

Removing Network from IPSec Tunnel

Use this steps to remove the network from the IPSec Tunnel configuration. Here, consider that the network 172.16.40.0/24 has been removed from the NY (HQ) Security Appliance configuration.

1. Before remove the network from the tunnel, tear down the IPSec connection, which also clears the security associations related to phase 2.

```
ASA-NY-HQ# clear crypto ipsec sa
```

Clears the security associations related to phase 1 as follows

```
ASA-NY-HQ# clear crypto isakmp sa
```

2. Remove the interesting traffic ACL for the IPSec tunnel.

```
ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

3. Remove the ACL (inside_nat0_outbound), since the traffic is excluded from the nat.

```
ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0
255.255.255.0 10.10.10.0 255.255.255.0
```

4. Clear the NAT translation as shown

```
ASA-NY-HQ# clear xlate
```

5. When ever you modify the tunnel configuration, remove and reapply this crypto commands to take the latest configuration in the outside interface

```
ASA-NY-HQ(config)# crypto map outside_map interface outside
ASA-NY-HQ(config)# crypto isakmp enable outside
```

6. Save active configuration to the flash "**write memory**".

7. Follow the same procedure for the other end – TN Security appliance to remove the configurations.

8. Initiate the IPSec tunnel and verify the connection.

Verify

Use this section to confirm that your configuration works properly.

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

- **ping inside 172.16.40.20**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.40.20, timeout is 2 seconds:
?!!!!|
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

- **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: 192.168.10.10
  Type  : L2L           Role   : initiator
  Rekey : no           State  : MM_ACTIVE
```

- **show crypto ipsec sa**

```

interface: outside
Crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 172.16.40.0 255.255.255.0
local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.40.0/255.255.255.0/0/0)
current_peer: 192.168.10.10

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTU sent: 0, #PMTU rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #rcv errors: 0

local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 4C0547DE

inbound esp sas:
spi: 0x0EB40138 (246677816)
transform: esp-3des esp-sha-hmac none
in use settings =({L2L, Tunnel, })
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28476)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x4C0547DE (1275414494)
transform: esp-3des esp-sha-hmac none
in use settings =({L2L, Tunnel, })
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28476)
IV size: 8 bytes
replay detection support: Y

crypto map tag: outside_map, seq num: 20, local addr: 192.168.11.1

access-list outside_20_cryptomap permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 192.168.10.10

#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#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
#PMTU sent: 0, #PMTU rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #rcv errors: 0

local crypto endpt.: 192.168.11.2, remote crypto endpt.: 192.168.10.10

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 5CC4DEB9

inbound esp sas:
spi: 0xF48286AD (4102194861)
transform: esp-3des esp-sha-hmac none
in use settings =({L2L, Tunnel, })
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274999/28271)
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x5CC4DEB9 (1556405897)
transform: esp-3des esp-sha-hmac none
in use settings =({L2L, Tunnel, })
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4274998/28271)
IV size: 8 bytes
replay detection support: Y

```

Troubleshoot

Refer to these documents for more troubleshooting information:

- [IPsec VPN Troubleshooting Solutions](#)
- [Understanding and Using debug Commands](#)
- [Troubleshooting Connections through the PIX and ASA](#)

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

Cisco – PIX/ASA 7.x: Add/Remove a Network on an Existing L2L VPN Tunnel Configuration Example

NetPro Discussion Forums – Featured Conversations for VPN

Service Providers: VPN Service Architectures

Service Providers: Network Management

Virtual Private Networks: General

Related Information

- [An Introduction to IP Security \(IPsec\) Encryption](#)
- [IPsec Negotiation/IKE Protocol Support Page](#)
- [Security Appliance Command Reference](#)
- [Configuring IP Access Lists](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 10, 2007

Document ID: 82209
