PIX/ASA 7.X : Add a New Tunnel or Remote Access to an Existing L2L VPN

Contents

Introduction

This document provides the steps required to add a new VPN tunnel or a remote access VPN to a L2L VPN configuration that already exists. Refer to Cisco ASA 5500 Series Adaptive Security Appliances - Configuration Examples and TechNotes for information on how to create the initial IPSec VPN tunnels and for more configuration examples.

Prerequisites

Requirements

Ensure that you correctly configure the L2L IPSEC VPN tunnel that is currently operational before you attempt this configuration.

Components Used

The information in this document is based on these software and hardware versions:

- Two ASA security appliances that run 7.x code
- One PIX security appliance that runs 7.x code

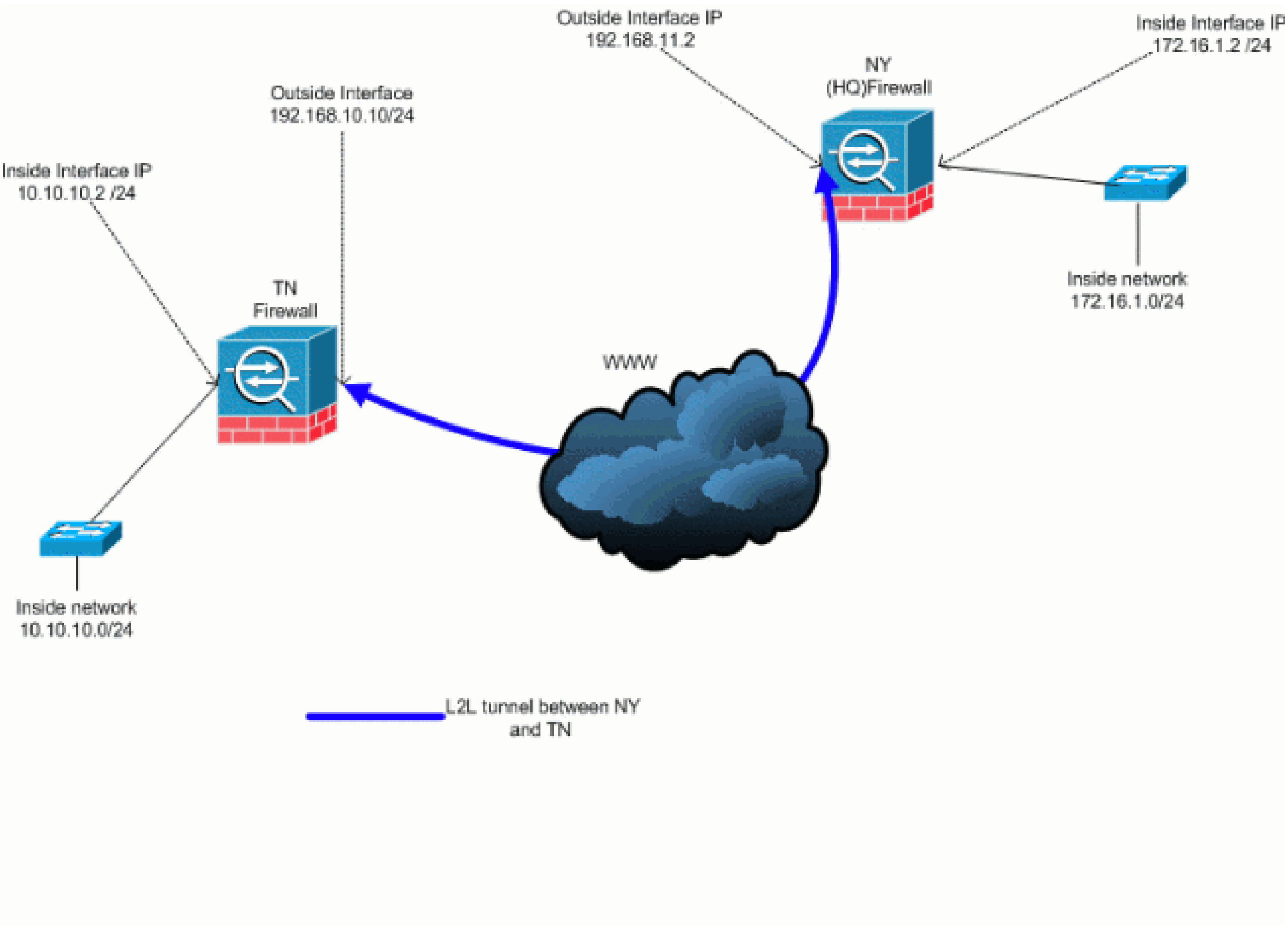
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Network Diagram

This document uses this network setup:



This output is the current running configuration of the NY (HUB) security appliance. In this configuration, there is an IPSec L2L tunnel configured between NY(HQ) and TN.

Current NY (HQ) Firewall Configuration

```
ASA-NY-HQ#show running-config : Saved : ASA Version 7.2(2) !
hostname ASA-NY-HQ domain-name corp2.com enable password
WwXYvtKrnjXqGbu1 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 shutdown no nameif no security-level no ip
address ! 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 access-list
outside_20_cryptomap extended permit ip 172.16.1.0
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 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 *
telnet timeout 1440 ssh timeout 5 console timeout 0 ! class-
map inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end ASA-NY-
HQ#
```

Background Information

Currently, there is an existing L2L tunnel set up between the NY(HQ) office and TN office. Your company has recently opened a new office that is located in TX. This new office requires connectivity to local resources that are located in the NY and TN offices. In addition, there is an additional requirement to allow employees the opportunity to work from home and securely access resources that are located on the internal network remotely. In this example, a new VPN tunnel is configured as well as a remote access VPN server that is located in the the NY office.

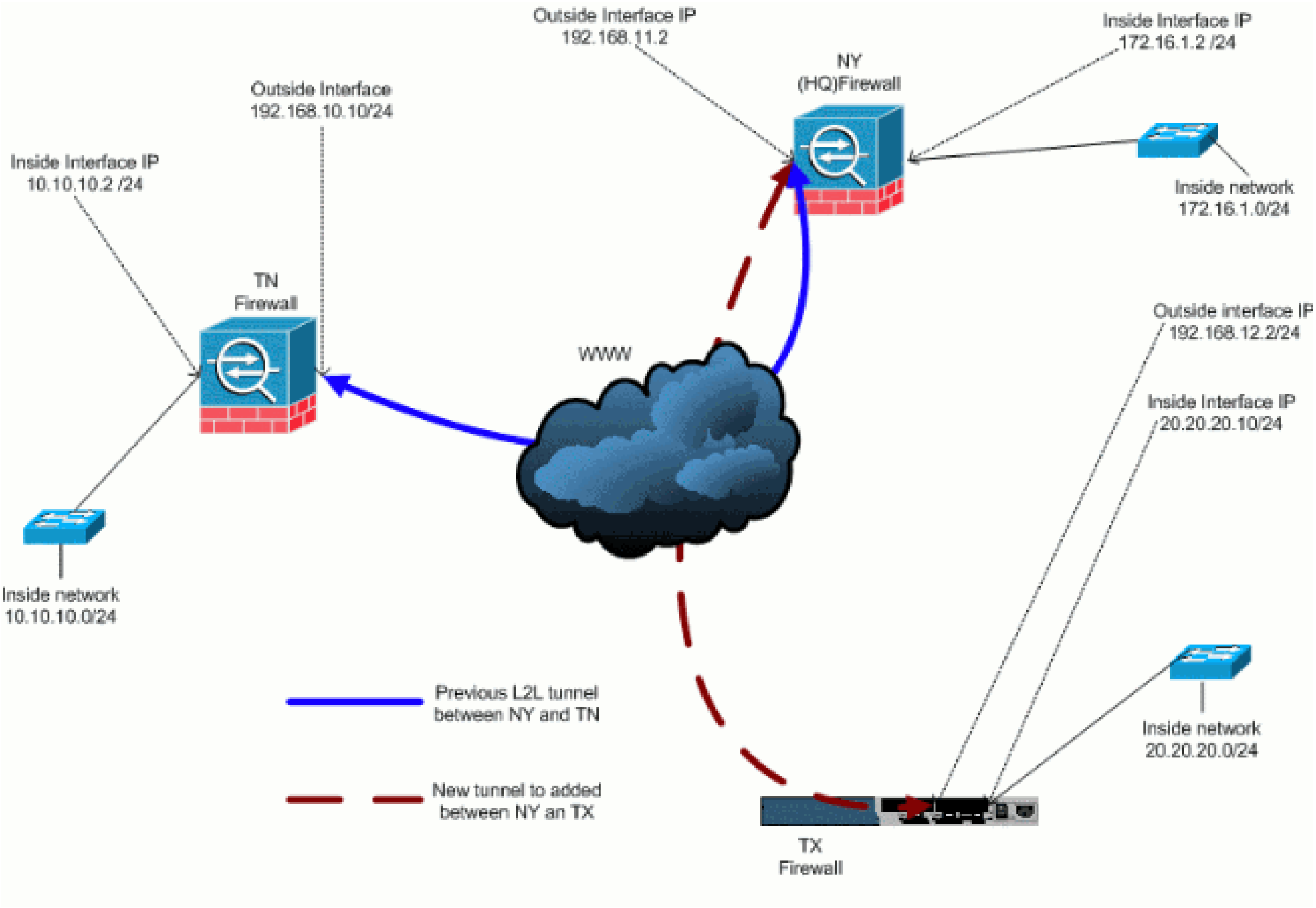
In this example, two commands are used in order to allow the communication between the VPN networks and identify the traffic that should be tunneled or encrypted. This enables you to have access to the internet without having to send that traffic through the VPN tunnel. In order to configure these two options, issue the **split-tunnel** and **same-security-traffic** commands.

Split tunneling allows a remote-access IPSec client to conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the IPSec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. This command applies this split tunneling policy to a specified network. The default is to tunnel all traffic. In order to set a split tunneling policy, issue the **split-tunnel-policy** command in the group-policy configuration mode. In order to remove the split-tunneling-policy from the configuration, issue the **no** form of this command.

The security appliance includes a feature that allows a VPN client to send IPSec-protected traffic to other VPN users by allowing such traffic in and out of the same interface. Also called hairpinning, this feature can be thought of as VPN spokes (clients) that connect through a VPN hub (security appliance). In another application, this feature can redirect incoming VPN traffic back out through the same interface as unencrypted traffic. This is useful, for example, to a VPN client that does not have split tunneling but needs to both access a VPN and browse the web. In order to configure this feature, issue the **same-security-traffic** *intra-interface* command in the global configuration mode.

Add an Additional L2L Tunnel to the Configuration

This is the network diagram for this configuration:



Step-by-Step Instructions

This section provides the required procedures that must be performed on the HUB (NY Firewall) security appliance. Refer to the PIX/ASA 7.x: Simple PIX-to-PIX VPN Tunnel Configuration Example for more information on how to configure the spoke client (TX Firewall).

Complete these steps:

1. Create these two new access-lists to be used by the crypto map in order to define interesting traffic:

```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0
ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```

Warning: In order for the communication to take place, the other side of the tunnel must have the opposite of this access control list (ACL) entry for that particular network.

2. Add these entries to the no nat statement in order to exempt the nating between these networks:
   ```
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
    extended permit ip 172.16.1.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
    extended permit ip 10.10.10.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
    extended permit ip 20.20.20.0 255.255.255.0
      10.10.10.0 255.255.255.0
   ```
   Warning: In order for the communication to take place, the other side of the tunnel must have the opposite of this ACL entry for that particular network.
3. Issue this command in order to enable a host on the TX VPN network to have access to the TN VPN tunnel:
   ```
   ASA-NY-HQ(config)#same-security-traffic permit
    intra-interface
   ```
   This allows VPN peers to talk between each other.
4. Create the crypto map configuration for the new VPN tunnel. Use the same transform set that was used in the first VPN configuration, as all the phase 2 settings are the same.
   ```
   ASA-NY-HQ(config)#crypto map outside_map 30 match
    address outside_30_cryptomap
   ASA-NY-HQ(config)#crypto map outside_map 30 set
    peer 192.168.12.2
   ASA-NY-HQ(config)#crypto map outside_map 30 set
    transform-set
    ESP-3DES-SHA
   ```
5. Create the tunnel-group that is specified for this tunnel along with attributes needed to connect to the remote host.
   ```
   ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
    ipsec-l2l
   ASA-NY-HQ(config)#tunnel-group 192.168.12.2
    ipsec-attributes
   ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
   cisco123
   ```
   Note: The pre-shared-key must match exactly on both sides of the tunnel.
6. Now that you have configured the new tunnel, you must send interesting traffic across the tunnel in order to bring it up. In order to perform this, issue the **source ping** command to ping a host on the inside network of the remote tunnel.In this example, a workstation on the other side of the tunnel with the address 20.20.20.16 is pinged. This brings the tunnel up between NY and TX. Now, there are two tunnels connected to the HQ office. If you do not have access to a system behind the tunnel, refer to Most Common IPSec VPN Troubleshooting Solutions to find an alternate solution in respect to using `management-access`.

Example Configuration

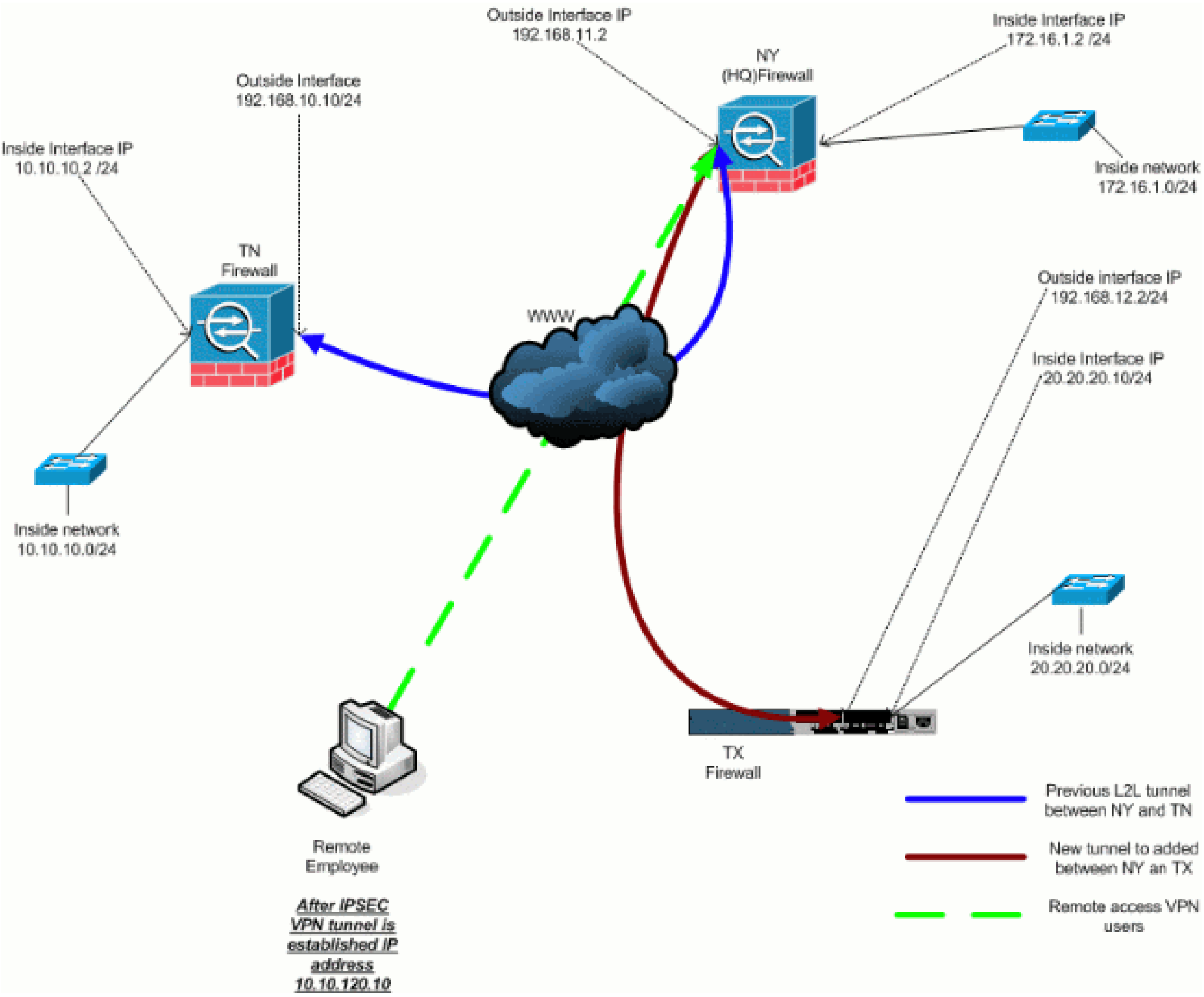
Example Configuration 1

```
ASA-NY-HQ#show running-config : Saved : ASA Version 7.2(2) !
hostname ASA-NY-HQ domain-name corp2.com enable password
WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 192.168.11.1
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 shutdown no nameif no security-level no ip
address ! 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 same-security-traffic permit
intra-interface access-list inside_nat0_outbound extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0 access-list
```

```
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 20.20.20.0
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 access-list
outside_20_cryptomap extended permit ip 20.20.20.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
outside_30_cryptomap extended permit ip 172.16.1.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
outside_30_cryptomap extended permit ip 10.10.10.0
255.255.255.0 20.20.20.0 255.255.255.0 logging enable logging
asdm informational mtu outside 1500 mtu inside 1500 mtu man
1500 no failover icmp unreachable rate-limit 1 burst-size 1
no asdm history enable arp timeout 14400 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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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 username sidney password
3xsopMX9gN5Wnf1W encrypted privilege 15 aaa authentication
telnet console LOCAL 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 30 match address
outside_30_cryptomap crypto map outside_map 30 set peer
192.168.12.2 crypto map outside_map 30 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 * tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes pre-shared-key *
telnet timeout 1440 ssh timeout 5 console timeout 0 ! class-
map inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae : end ASA-NY-
HQ#
```

Add a Remote Access VPN to the Configuration

This is the network diagram for this configuration:



Step-by-Step Instructions

This section provides the required procedures to add remote access capability and to allow remote users to access all sites. Refer to PIX/ASA 7.x ASDM: Restrict the Network Access of Remote Access VPN Users for more information on how to configure the remote access server and restrict access.

Complete these steps:

1. Create an IP address pool to be used for clients that connect via the VPN tunnel. Also, create a basic user in order to access the VPN once the configuration is completed.
   ```
   ASA-NY-HQ(config)#ip local pool Hill-V-IP
    10.10.120.10-10.10.120.100 mask 255.255.255.0ASA-NY-HQ(config)#username cisco password
    cisco111
   ```
2. Exempt specific traffic from being nated.
   ```
   ASA-NY-HQ(config)#access-list
    inside_nat0_outbound extended permit ip 172.16.1.0
       255.255.255.0 10.10.120.0 255.255.255.0ASA-NY-HQ(config)#access-list
    inside_nat0_outbound extended permit ip 10.10.120.0
       255.255.255.0 10.10.10.0 255.255.255.0ASA-NY-HQ(config)#access-list
    inside_nat0_outbound extended permit ip 10.10.120.0
       255.255.255.0 20.20.20.0 255.255.255.0
   ```
   Notice that the nat communication between VPN tunnels is exempted in this example.

3. Allow communication between the L2L tunnels that are already created.
   ```
   ASA-NY-
   HQ(config)#access-list
    outside_20_cryptomap extended permit ip 10.10.120.0
       255.255.255.0 10.10.10.0 255.255.255.0ASA-NY-HQ(config)#access-list
    outside_30_cryptomap extended permit ip 10.10.120.0
       255.255.255.0 20.20.20.0 255.255.255.0
   ```
   This allows remote access users the ability to communicate with networks behind the specified tunnels.⚠ **Warning:** In order for the communication to take place, the other side of the tunnel must have the opposite of this ACL entry for that particular network.
4. Configure the traffic that will be encrypted and sent across the VPN tunnel.
   ```
   ASA-NY-
   HQ(config)#access-list
    Hillvalley_splitunnel standard permit 172.16.1.0
       255.255.255.0ASA-NY-HQ(config)#access-list
    Hillvalley_splitunnel standard permit 10.10.10.0
       255.255.255.0ASA-NY-HQ(config)#access-list
    Hillvalley_splitunnel standard permit 20.20.20.0
       255.255.255.0
   ```
5. Configure local authentication and policy information, such as wins, dns and IPSec protocols, for the VPN clients.
   ```
   ASA-NY-HQ(config)#group-policy Hillvalley
    internalASA-NY-HQ(config)#group-policy Hillvalley
    attributesASA-NY-HQ(config-group-policy)#wins-server
   value 10.10.10.20ASA-NY-HQ(config-group-policy)#dns-server value
   10.10.10.20ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
   IPSec
   ```
6. Set IPSec and general attributes, such as pre-shared keys and IP address pools, that will be used by the Hillvalley VPN tunnel.
   ```
   ASA-NY-HQ(config)#tunnel-group Hillvalley
    ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
   cisco1234ASA-NY-HQ(config)#tunnel-group Hillvalley
    general-attributesASA-NY-HQ(config-tunnel-general)#address-pool
   Hill-V-IPASA-NY-HQ(config-tunnel-general)#default-group-policy
   Hillvalley
   ```
7. Create the split tunnel policy that will use the ACL created in step 4 in order to specify what traffic will be encrypted and passed through the tunnel.
   ```
   ASA-NY-HQ(config)#split-tunnel-policy
    tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value
    Hillvalley_splitunnel
   ```
8. Configure the cryto map information required to the VPN tunnel creation.
   ```
   ASA-NY-
   HQ(config)#crypto ipsec transform-set
    Hill-trans esp-3des esp-sha-hmacASA-NY-HQ(config)#crypto dynamic-map
    outside_dyn_map 20 set transform-set
    Hill-transASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
    set reverse-routeASA-NY-HQ(config)#crypto map outside_map 65535
    ipsec-isakmp dynamic
    outside_dyn_map
   ```

Example Configuration

Example Configuration 2

```
ASA-NY-HQ#show running-config : Saved hostname ASA-NY-HQ ASA
Version 7.2(2) enable password WwXYvtKrnjXqGbu1 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 shutdown no nameif no
security-level no ip address ! 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 same-
security-traffic permit intra-interface !--- This is required
for communication between VPN peers. access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.10.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 20.20.20.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.120.0 255.255.255.0 access-list
inside_nat0_outbound extended permit ip 10.10.120.0
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 access-list
outside_20_cryptomap extended permit ip 20.20.20.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
outside_20_cryptomap extended permit ip 10.10.120.0
255.255.255.0 10.10.10.0 255.255.255.0 access-list
Hillvalley_splitunnel standard permit 172.16.1.0
255.255.255.0 access-list Hillvalley_splitunnel standard
permit 10.10.10.0 255.255.255.0 access-list
Hillvalley_splitunnel standard permit 20.20.20.0
255.255.255.0 access-list outside_30_cryptomap extended
permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0 access-list
outside_30_cryptomap extended permit ip 10.10.120.0
255.255.255.0 20.20.20.0 255.255.255.0 logging enable logging
asdm informational mtu outside 1500 mtu inside 1500 mtu man
1500 ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400 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 route outside 0.0.0.0 0.0.0.0 192.168.11.1 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 group-
policy Hillvalley internal group-policy Hillvalley attributes
wins-server value 10.10.10.20 dns-server value 10.10.10.20
vpn-tunnel-protocol IPSec split-tunnel-policy tunnelspecified
split-tunnel-network-list value Hillvalley_splitunnel
default-domain value corp.com username cisco password
dZBmhhbNIN5q6rGK encrypted aaa authentication telnet console
LOCAL 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 ipsec transform-set Hill-trans esp-3des
esp-sha-hmac crypto dynamic-map outside_dyn_map 20 set
transform-set Hill-trans crypto dynamic-map dyn_map 20 set
reverse-route 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 30 match address
outside_30_cryptomap crypto map outside_map 30 set peer
```

```
192.168.12.1 crypto map outside_map 30 set transform-set ESP-
3DES-SHA crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map 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 * tunnel-group 192.168.12.2
type ipsec-l2l tunnel-group 192.168.12.2 ipsec-attributes
pre-shared-key * tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes address-pool Hill-
V-IP default-group-policy Hillvalley tunnel-group Hillvalley
ipsec-attributes pre-shared-key * telnet timeout 1440 ssh
timeout 5 console timeout 0 ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default inspect dns
preset_dns_map 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 prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48 ASA-NY-HQ#
```

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 x.x.x.x (IP address of host on opposite side of tunnel)**—This command allows you to send traffic down the tunnel using the a source address of the inside interface.

Troubleshoot

Refer to these documents for information you can use in order to troubleshoot your configuration:

- Most Common IPSec VPN Troubleshooting Solutions
- IP Security Troubleshooting - Understanding and Using debug Commands
- Troubleshoot Connections through the PIX and ASA

Related Information

- **An Introduction to IP Security (IPSec) Encryption**
- **IPSec Negotiation/IKE Protocols Support Page**
- **Cisco ASA 5500 Series Adaptive Security Appliances Command References**
- **Technical Support & Documentation - Cisco Systems**