PIX/ASA 7.X:向现有的 L2L VPN 添加新隧道或远程访问现有的 L2L VPN

目录

简介

本文档提供向现有的 L2L VPN 配置中添加一条新的 VPN 隧道或远程访问 VPN 所需的步骤。有关如何创建初始 IPSec VPN 隧道的信息以及更多配置示例，请参阅 Cisco ASA 5500 系列自适应安全设备 - 配置示例和技术说明。

先决条件

要求

在您尝试此配置前，请确保正确地配置当前可正常运行的 L2L IPSEC VPN 隧道。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 两台运行 7.x 代码的 ASA 安全设备
- 一台运行 7.x 代码的 PIX 安全设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

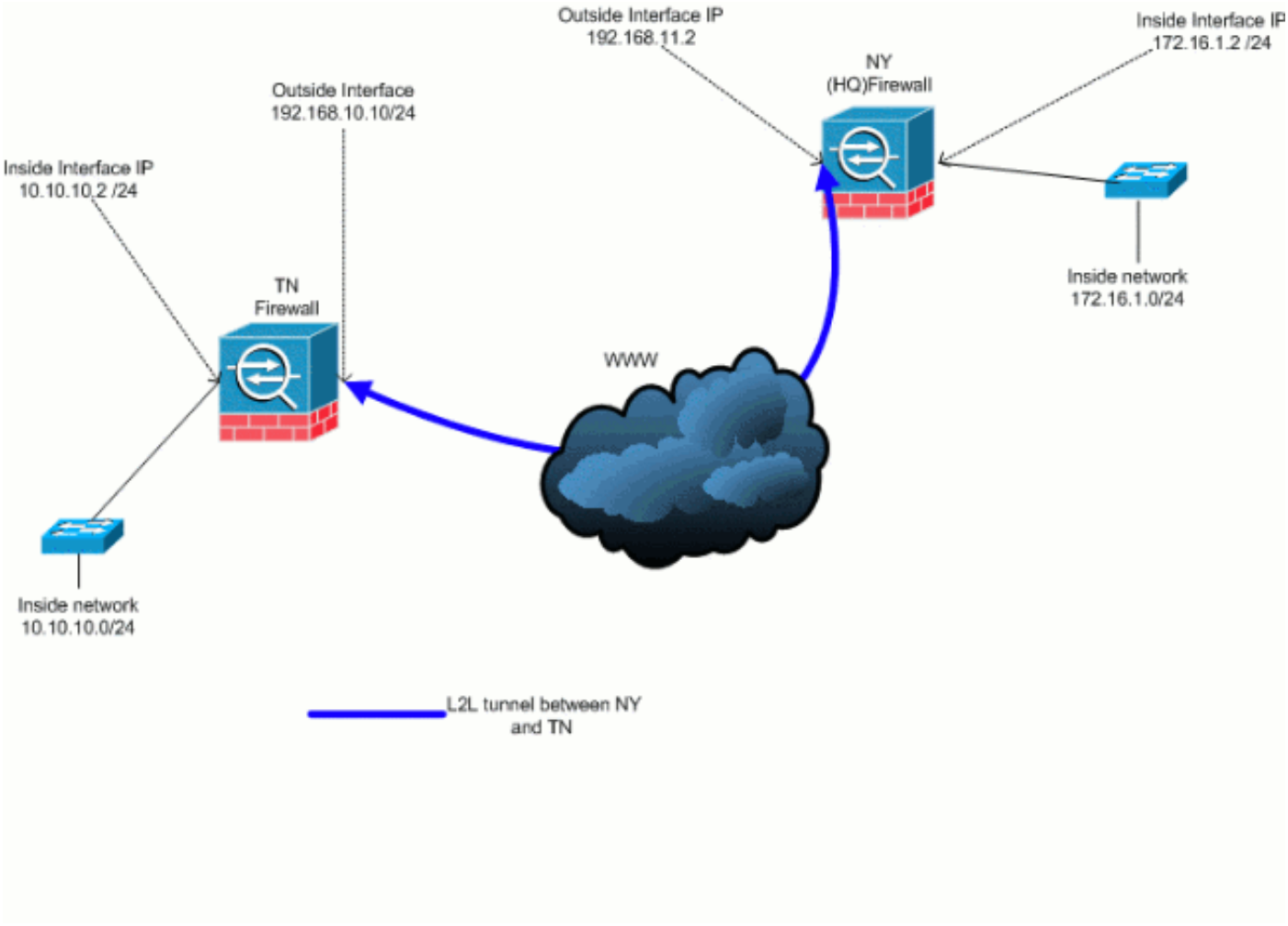
始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络图

本文档使用以下网络设置：



以下输出是 NY (HUB) 安全设备的当前运行配置。在此配置中，在 NY(HQ) 和 TN 之间配有一条 Ipsec L2L 隧道。

当前 NY(HQ) 防火墙配置

```
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#
```

背景信息

目前，在 NY(HQ) 办公室和 TN 办公室之间设有一条现有的 L2L 隧道。您的公司最近在 TX 处新开了一个办公室。这个新办公室需要连接到位于 NY 和 TN 办公室的本地资源。此外，还要求允许员工在家工作并且在远程安全地访问位于内部网络的资源。在本例中，配置一条新的 VPN 隧道以及位于 NY 办公室的远程访问 VPN 服务器。

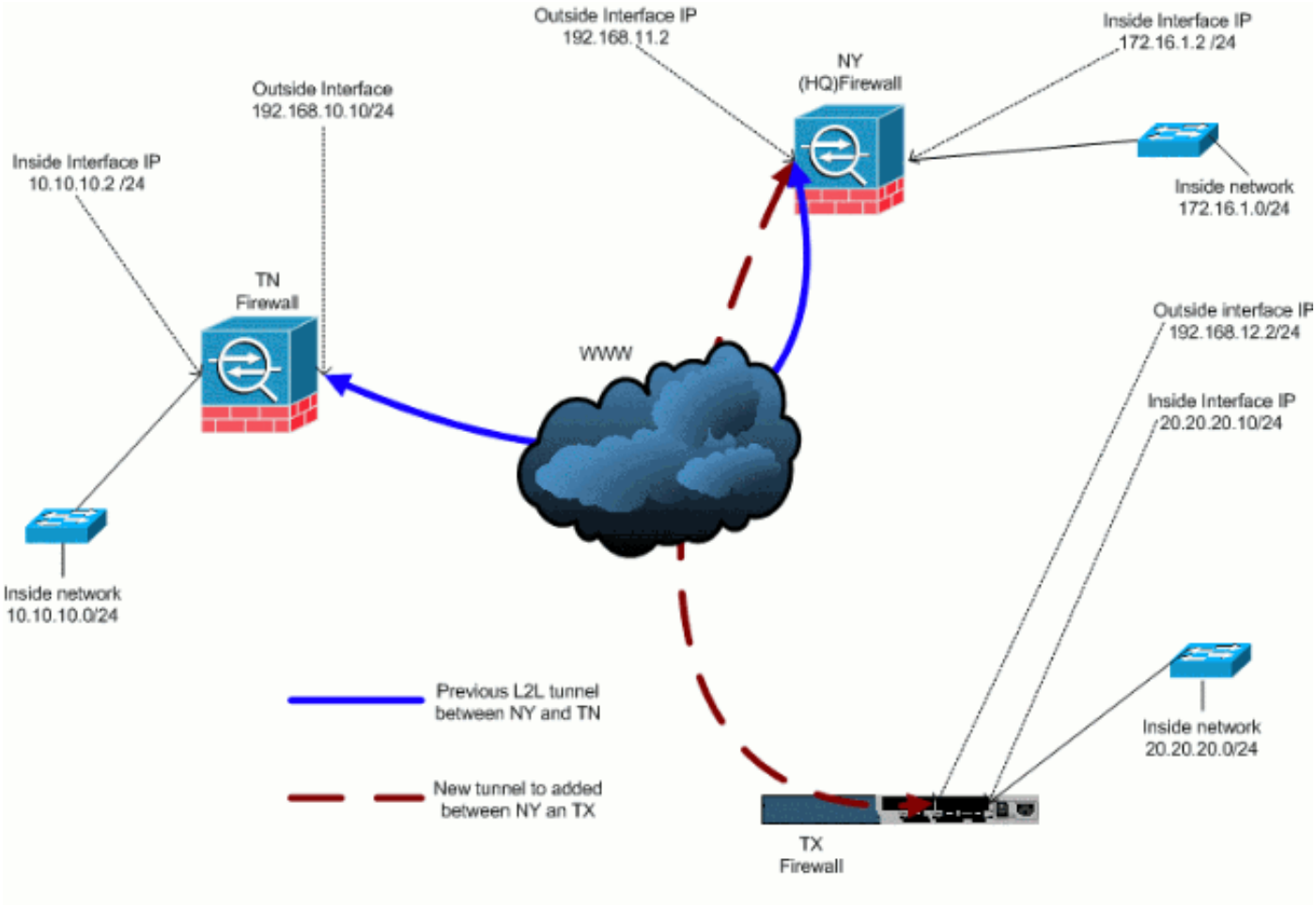
在本例中，使用两个命令以允许 VPN 网络之间的通信并识别应该以隧道传输或加密的数据流。这使您能够访问 Internet，而不必通过 VPN 隧道发送该数据流。要配置这两个选项，请发出 **split-tunnel 和 same-security-traffic 命令。**

分割隧道使远程访问 IPSec 客户端可以有条件地以加密形式通过 IPsec 隧道定向数据包，或者以明文形式将数据包定向到网络接口。启用分割隧道时，在 IPSec 隧道另一端通往目标的数据包不必加密、通过隧道发送、解密，然后路由到最终目标。此命令将此分割隧道策略应用到指定的网络。默认值是以隧道传输所有数据流。要设置分割隧道策略，请在组策略配置模式下发出 **split-tunnel-policy 命令。**要从配置中删除分割隧道策略，请发出此命令的 **no 形式。**

安全设备包含一项功能，它通过允许受 IPSec 保护的数据流进出同一接口来允许 VPN 客户端将此类数据流发送到其他 VPN 用户。此功能也称为发夹，可将其视为通过 VPN 集线器（安全设备）连接的 VPN 分支（客户端）。 在另一个应用中，此功能可以将传入的 VPN 数据流通过同一接口作为未加密的数据流重定向返回。例如，这对于没有分割隧道却要同时访问 VPN 和浏览 Web 的 VPN 客户端很有用。要配置此功能，请在全局配置模式下发出 **same-security-traffic intra-interface** 命令。

向配置中添加另外一条 L2L 隧道

以下是此配置的网络图：



逐步指导

本部分提供必须在 HUB（NY 防火墙）安全设备上执行的过程。有关如何配置分支客户端（TX 防火墙）的更多信息，请参阅 PIX/ASA 7.x：简单的 PIX 到 PIX VPN 隧道配置示例。

请完成以下步骤：

1. 创建以下两个用于加密映射的新访问列表以定义相关数据流：

```
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
```

   警告：要进行通信，隧道的另一端必须与此特定网络的访问控制列表(ACL)条目相反。
2. 将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT：

```
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
```

警告：要进行通信，隧道的另一端必须与此特定网络的ACL条目相反。

3. 发出以下命令以使 TX VPN 网络上的主机能够访问 TN VPN 隧道：

```
ASA-NY-HQ(config)#same-security-traffic permit
 intra-interface
```

这使 VPN 对等体能够在相互之间进行通信。

4. 为新的 VPN 隧道创建加密映射配置。请使用在第一种 VPN 配置中使用的同一转换集，因为所有第 2 阶段的设置都是相同的。

```
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. 创建为此隧道指定的隧道组以及连接到远程主机所需的属性。

```
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
```

注意：预共享密钥在隧道两端必须完全匹配。

6. 既然您配置了新隧道，您必须通过隧道发送相关数据流才能启用该隧道。要执行此操作，请发出 **source ping 命令对远程隧道内部网络上的一台主机执行 ping 操作。**在本示例中，对隧道另一端地址为 20.20.20.16 的工作站执行 ping 操作。此操作启用 NY 与 TX 之间的隧道。此时，有两条隧道连接到总部。如果您无法访问隧道后方的系统，请参阅最常用的 IPSec VPN 故障排除解决方案以查找关于使用 `management-access` 的备用解决方案。

配置示例

配置示例 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
```

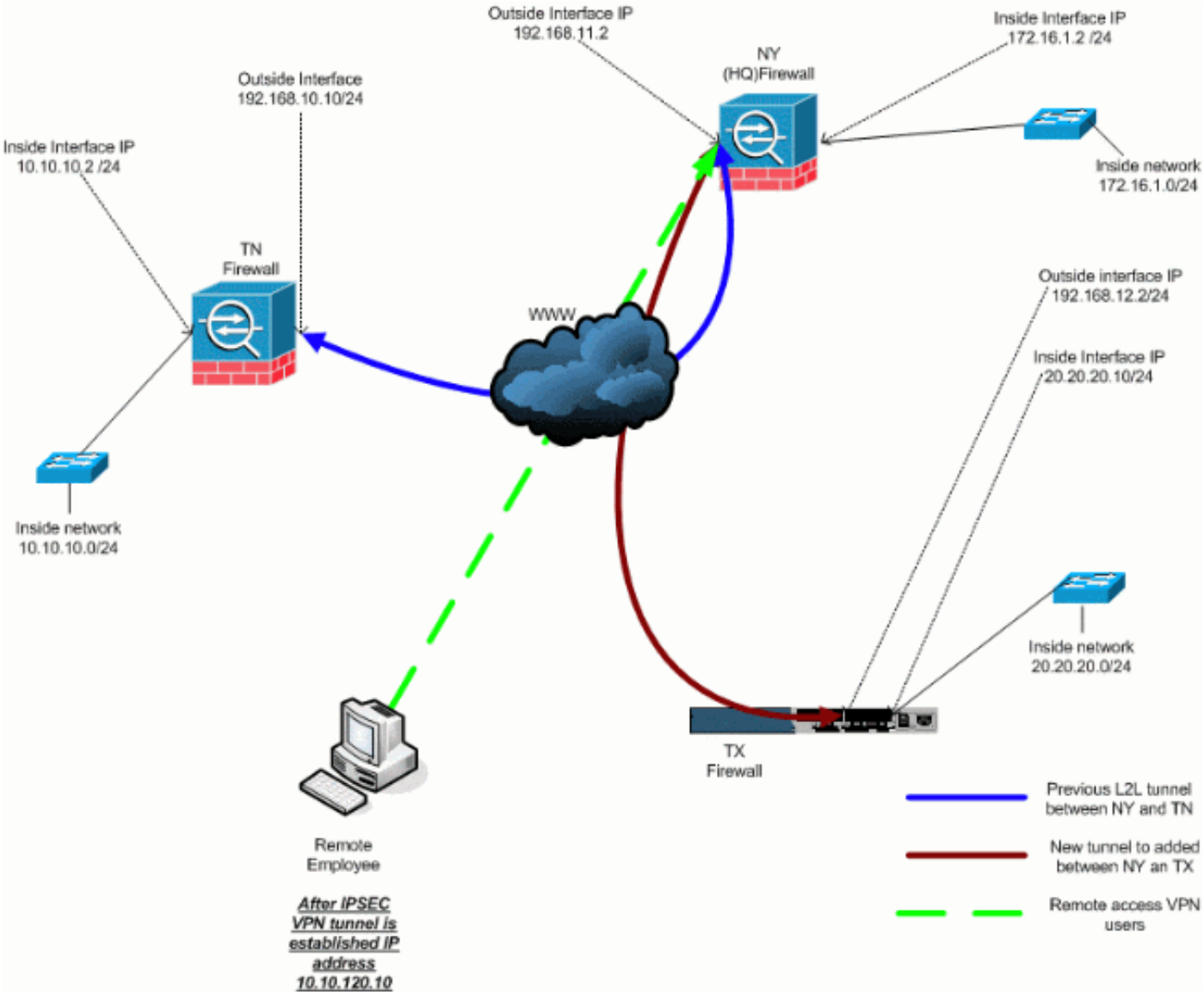
```
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group 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#
```

向配置中添加一个远程访问 VPN

以下是此配置的网络图：



逐步指导

本部分提供添加远程访问功能并允许远程用户访问所有站点所需的过程。有关如何配置远程访问服务器以及限制访问的更多信息，请参阅 PIX/ASA 7.x ASDM：限制远程访问 VPN 用户的网络访问。

请完成以下步骤：

1. 创建一个 IP 地址池以用于通过 VPN 隧道连接的客户端。此外，创建一个基本用户，以便在配置完成后访问 VPN。
   ```
   ASA-NY-HQ(config)#ip local pool Hill-V-IP
   ```

```
 10.10.120.10-10.10.120.100 mask 255.255.255.0

ASA-NY-HQ(config)#username cisco password
 cisco111
```

2. 使特定的数据流免于进行 NAT 处理。

```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 172.16.1.0
    255.255.255.0 10.10.120.0 255.255.255.0

ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-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
```

请注意，在本示例中免除了 VPN 隧道之间的 NAT 通信。

3. 允许已创建的 L2L 隧道之间的通信。

```
ASA-NY-HQ(config)#access-list
 outside_20_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-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
```

此操作使远程访问用户能够与指定的隧道之后的网络进行通信。**警告：**要进行通信，隧道的另一端必须与此特定网络的ACL条目相反。

4. 配置将被加密并且通过 VPN 隧道发送的数据流。

```
ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 172.16.1.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 10.10.10.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 20.20.20.0
    255.255.255.0
```

5. 配置 VPN 客户端的本地身份验证和策略信息，例如 wins、dns 和 IPSec 协议。

```
ASA-NY-HQ(config)#group-policy Hillvalley
 internal

ASA-NY-HQ(config)#group-policy Hillvalley
 attributes

ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20

ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20

ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. 设置将由 Hillvalley VPN 隧道使用的 Ipsec 属性和常规属性，例如预共享密钥和 IP 地址池。

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
 ipsec-attributes
```

```
ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234

ASA-NY-HQ(config)#tunnel-group Hillvalley
 general-attributes

ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP

ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. 创建将使用第 4 步中创建的 ACL 的分割隧道策略，以指定哪些数据流将被加密并且通过隧道传输。

```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecified

ASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```

8. 配置创建 VPN 隧道所需的加密映射信息。

```
ASA-NY-HQ(config)#crypto ipsec transform-set
 Hill-trans esp-3des esp-sha-hmac

ASA-NY-HQ(config)#crypto dynamic-map
 outside_dyn_map 20 set transform-set
 Hill-trans

ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
 set reverse-route

ASA-NY-HQ(config)#crypto map outside_map 65535
 ipsec-isakmp dynamic
 outside_dyn_map
```

配置示例

配置示例 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#
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **ping inside x.x.x.x（隧道对侧的主机 IP 地址）** - 通过此命令，您可以使用内部接口的源地址通过隧道发送数据流。

故障排除

有关排除配置故障时可用的信息，请参阅以下文档：

- 最常用的 IPSec VPN 故障排除解决方案
- IP安全故障排除-了解和使用debug命令
- 排除通过 PIX 和 ASA 的连接故障

相关信息

- IP 安全 (IPsec) 加密简介
- IPsec 协商/IKE 协议支持页
- Cisco ASA 5500 系列自适应安全设备命令参考
- 技术支持和文档 - Cisco Systems