PIX/ASA 7.X :向現有L2L VPN新增新隧道或遠端訪問

目錄

簡介

本文檔提供了將新VPN隧道或遠端訪問VPN新增到已經存在的L2L VPN配置所需的步驟。有關如何建立初始IPSec VPN隧道和更多配置示例的資訊，請參閱Cisco ASA 5500系列自適應安全裝置 — 配置示例和技術說明。

必要條件

需求

嘗試此配置之前，請確保正確配置當前可運行的L2L IPSEC VPN隧道。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行7.x代碼的兩台ASA安全裝置
- 一台運行7.x代碼的PIX安全裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

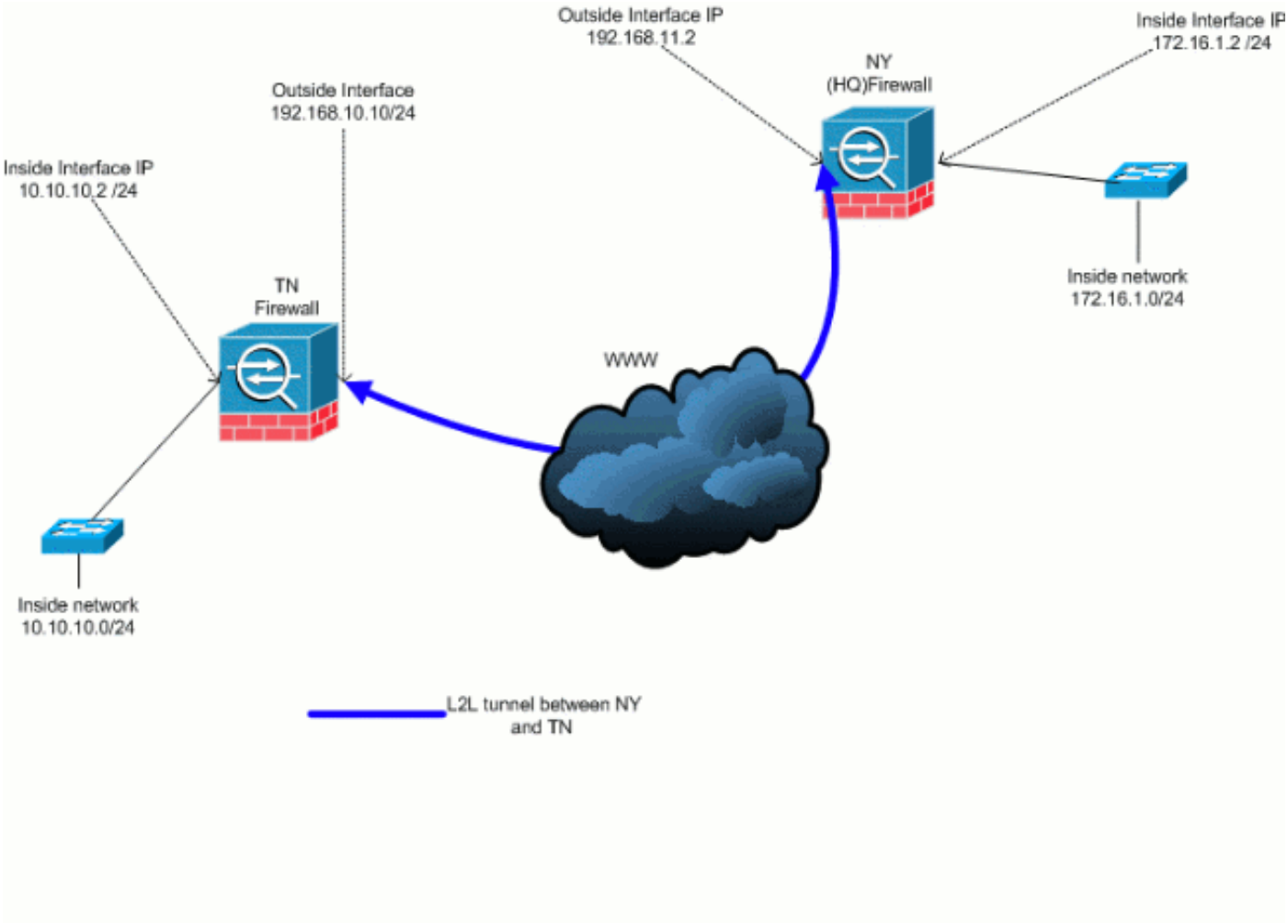
）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

網路圖表

本檔案會使用以下網路設定：



此輸出是NY(HUB)安全裝置的當前運行配置。在此配置中，在NY(HQ)和TN之間配置了IPSec L2L隧道。

當前NY(HQ)防火牆配置

```
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#
```

背景資訊

目前，NY(HQ)辦公室和TN辦公室之間已經建立了L2L隧道。貴公司最近在TX開了一個新辦公室。這個新辦事處需要與紐約辦事處和東京辦事處當地資源連線。此外，還額外要求允許員工有機會在家工作，並安全地遠端訪問內部網路上的資源。在本示例中，配置了新的VPN隧道以及位於紐約辦公室的遠端訪問VPN伺服器。

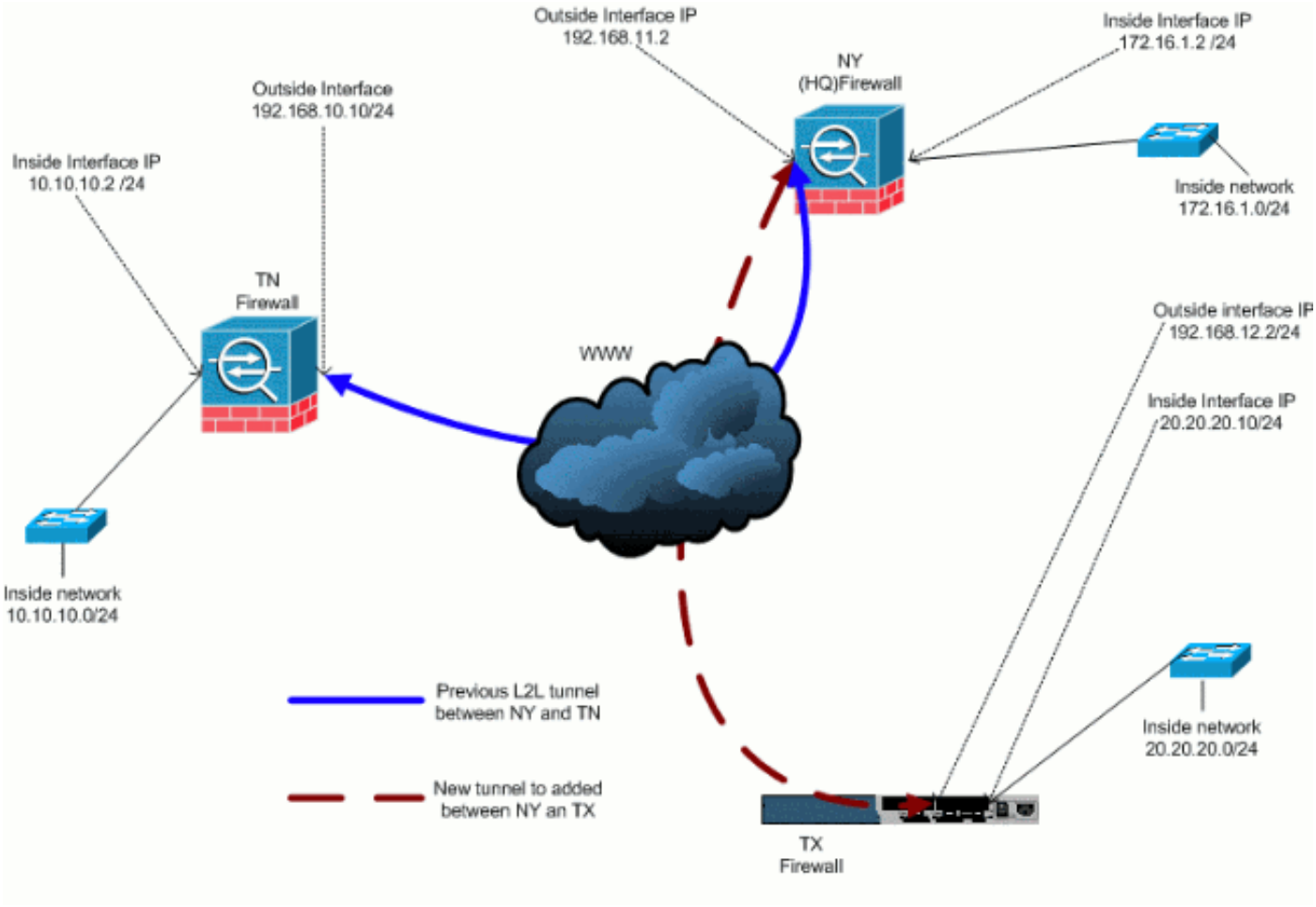
在本示例中，使用兩個命令來允許VPN網路之間的通訊並標識應該通過隧道傳輸或加密的流量。這使您能夠訪問網際網路，而不必通過VPN隧道傳送該流量。若要設定這兩個選項，請發出**split-tunnel**和**same-security-traffic**命令。

分割隧道允許遠端訪問IPSec客戶端有條件地以加密形式通過IPSec隧道將資料包定向或以明文形式定向到網路介面。啟用分割隧道後，未繫結到IPSec隧道另一側上的目標的資料包不必經過加密、通過隧道傳送、解密，然後路由到最終目標。此命令將此分割隧道策略應用於指定的網路。預設為透過通道傳輸所有流量。若要設定分割隧道策略，請在組策略配置模式下發出**split-tunnel-policy**命令。若要從組態中移除分割通道原則，請發出此命令的**no**形式。

安全裝置包括一項功能，允許VPN客戶端通過允許此類流量進出同一介面將受IPSec保護的流量傳送到其他VPN使用者。此功能也稱為迴轉傳輸，可視為通過VPN中心（安全裝置）連線的VPN分支（客戶端）。 在另一個應用中，此功能可以將傳入VPN流量重新定向回通過與未加密流量相同的介面。這非常有用，例如，對於沒有分割隧道但需要訪問VPN和瀏覽Web的VPN客戶端。若要設定此功能，請在全域組態模式下發出**same-security-traffic** intra-interface命令。

將額外的L2L隧道新增到配置

以下是此組態的網路圖：



逐步說明

本節提供必須在HUB（紐約防火牆）安全裝置上執行的必要過程。請參閱PIX/ASA 7.x:簡單的PIX到PIX VPN隧道配置示例，瞭解有關如何配置分支客戶端（TX防火牆）的詳細資訊。

請完成以下步驟：

1. 建立這兩個新的存取清單，以供密碼編譯對應用來定義相關流量：

```
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：若要發生通訊，通道的另一端必須擁有與該特定網路的存取控制清單(ACL)專案相反的專案。
2. 將這些條目新增到no nat語句中，以免除在這些網路之間的命名：

```
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：為了進行通訊，通道的另一端必須擁有與該特定網路的此ACL專案相反的專案。

3. 發出此命令，以使TX VPN網路上的主機能夠訪問TN VPN隧道：

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

這允許VPN對等點彼此通訊。

4. 為新的VPN隧道建立加密對映配置。使用第一個VPN配置中使用的相同轉換集，因為所有階段2設定都相同。

```
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. 建立為此隧道指定的隧道組以及連線到遠端主機所需的屬性。

```
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：預先共用金鑰必須在通道的兩端完全相符。

6. 現在您已設定新通道，您必須透過通道傳送相關流量才能將其啟用。若要執行此操作，請發出**source ping**命令，對遠端隧道內部網路上的主機執行ping。在本例中，對位於隧道另一端、地址為20.20.20.16的工作站執行ping操作。這會在NY和TX之間建立隧道。現在，有兩條隧道連線到總部辦公室。如果您無法訪問通道後面的系統，請參閱最常見的IPSec VPN故障排除解決方案，以查詢有關使用`management-access`的備用解決方案。

組態範例

示例配置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
```

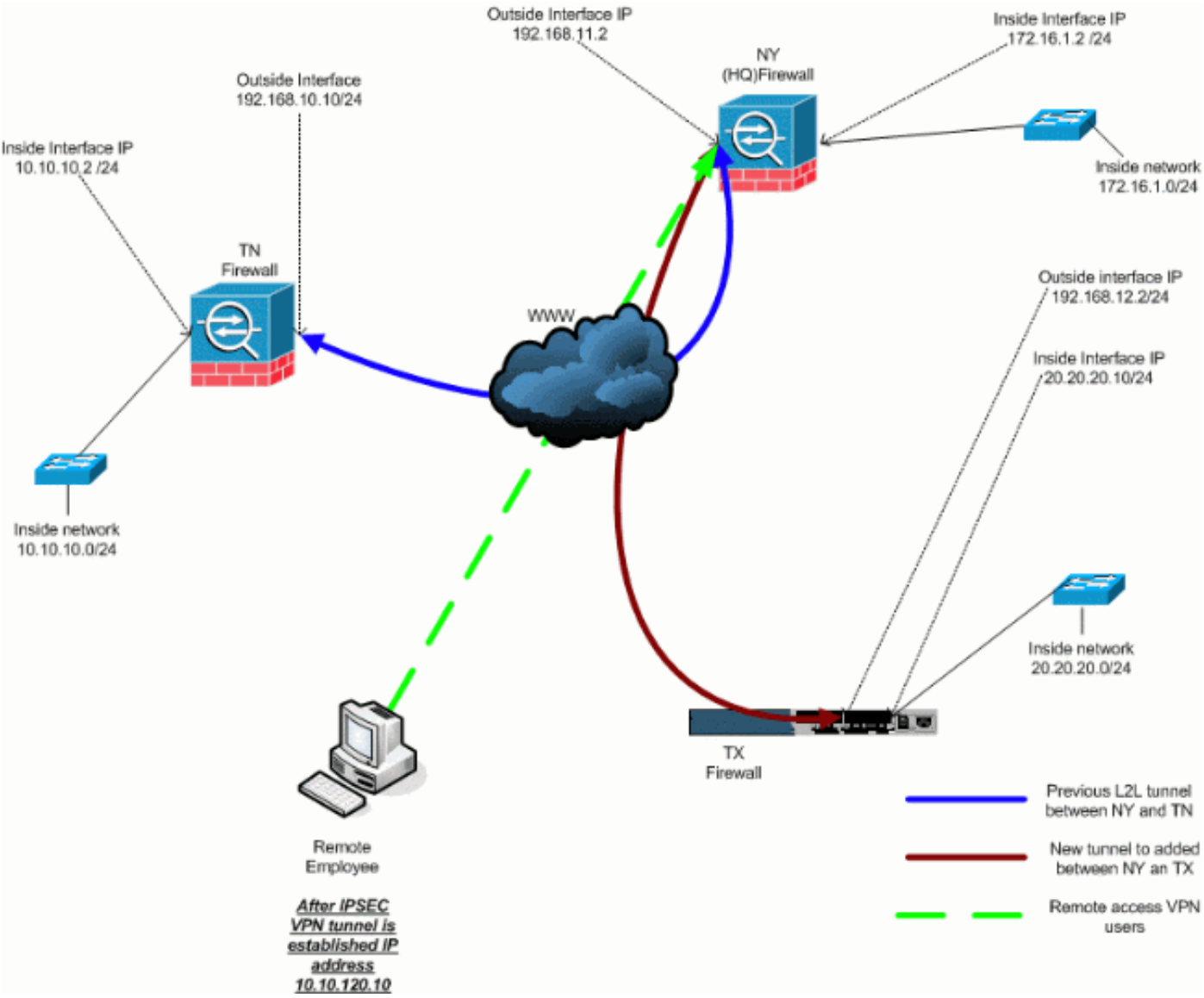
```
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU 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#
```

將遠端訪問VPN新增到配置

以下是此組態的網路圖：



逐步說明

本節提供新增遠端訪問功能和允許遠端使用者訪問所有站點所需的過程。請參閱PIX/ASA 7.x ASDM:限制遠端訪問VPN使用者的網路訪問，以瞭解有關如何配置遠端訪問伺服器和限制訪問的更多資訊。

請完成以下步驟：

1. 建立用於通過VPN隧道連線的客戶端的IP地址池。此外，建立基本使用者，以便在配置完成後

訪問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. 避免指定特定流量。

```
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
```

請注意，在此示例中，VPN隧道之間的nat通訊被免除。

3. 允許已建立的L2L隧道之間的通訊。

```
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
```

這樣，遠端訪問使用者就能夠與指定隧道後的網路通訊。**警告**：為了進行通訊，通道的另一端必須擁有與該特定網路的此ACL專案相反的專案。

4. 配置將通過VPN隧道加密和傳送的流量。

```
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. 為VPN客戶端配置本地身份驗證和策略資訊，例如wins、dns和IPSec協定。

```
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. 設定Hillvalley VPN隧道將使用的IPSec和常規屬性，如預共用金鑰和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. 建立將使用步驟4中建立的ACL的分隔隧道策略，以指定哪些流量將加密並通過隧道。

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

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

8. 配置建立VPN隧道所需的加密對映資訊。

```
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
```

組態範例

示例配置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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- **ping內部x.x.x.x（隧道另一端主機的IP地址）** — 此命令允許您使用內部介面的源地址沿隧道傳送流量。

疑難排解

請參閱這些檔案瞭解可用於對組態進行疑難排解的資訊：

- 最常見的IPSec VPN故障排除解決方案
- IP安全性疑難排解 — 瞭解和使用debug命令
- 排除通過PIX和ASA的連線故障

相關資訊

- **IP安全(IPSec)加密簡介**
- **IPSec協商/IKE通訊協定支援頁面**
- **Cisco ASA 5500系列自適應安全裝置命令參考**
- **技術支援與文件 - Cisco Systems**