PIX/ASA 7.X: Aggiunta di un nuovo tunnel o di un accesso remoto a una VPN L2L esistente

Sommario

Introduzione

In questo documento viene descritto come aggiungere un nuovo tunnel VPN o una VPN ad accesso remoto a una configurazione VPN L2L già esistente. Per informazioni su come creare i tunnel VPN IPSec iniziali e per ulteriori esempi di configurazione, fare riferimento a Cisco ASA serie 5500 Adaptive Security Appliance - Esempi di configurazione e note tecniche.

Prerequisiti

Requisiti

Prima di provare a configurare questa configurazione, verificare di aver configurato correttamente il tunnel VPN IPSEC L2L attualmente operativo.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Due appliance di sicurezza ASA con codice 7.x
- Un'appliance di sicurezza PIX con codice 7.x

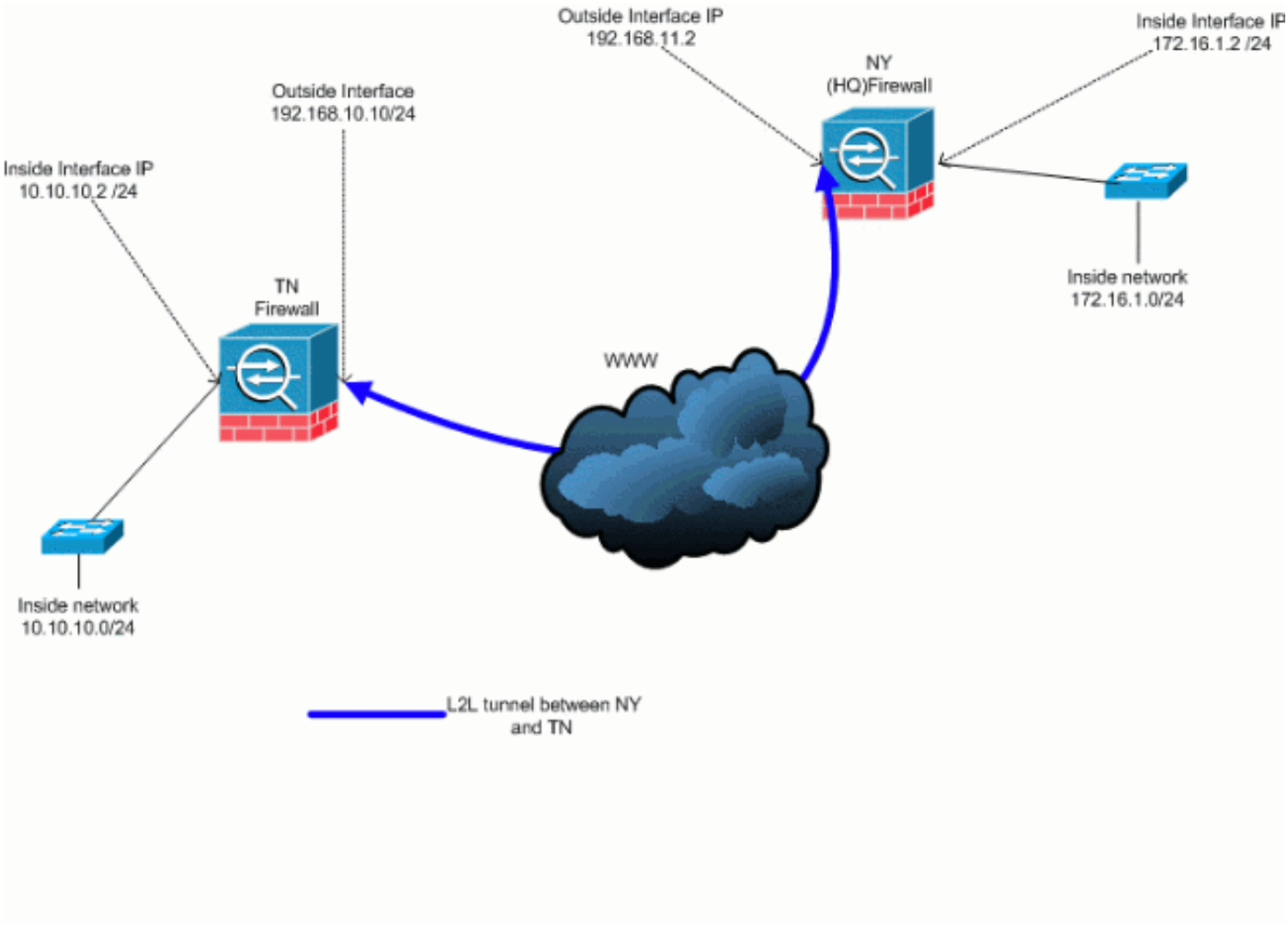
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Questo output è la configurazione corrente in esecuzione dell'appliance di sicurezza NY (HUB). In questa configurazione, è presente un tunnel IPSec L2L configurato tra NY(HQ) e TN.

Configurazione corrente del firewall NY (HQ)
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#
```

Premesse

Attualmente, è presente un tunnel L2L esistente tra l'ufficio di NY (HQ) e l'ufficio di TN. La società ha recentemente aperto un nuovo ufficio in TX. Questo nuovo ufficio richiede la connettività alle risorse locali che si trovano negli uffici di New York e TN. Inoltre, è necessario consentire ai dipendenti di lavorare da casa e di accedere in modo sicuro alle risorse che si trovano sulla rete interna in remoto. In questo esempio, viene configurato un nuovo tunnel VPN e un server VPN ad accesso remoto situato nell'ufficio di NY.

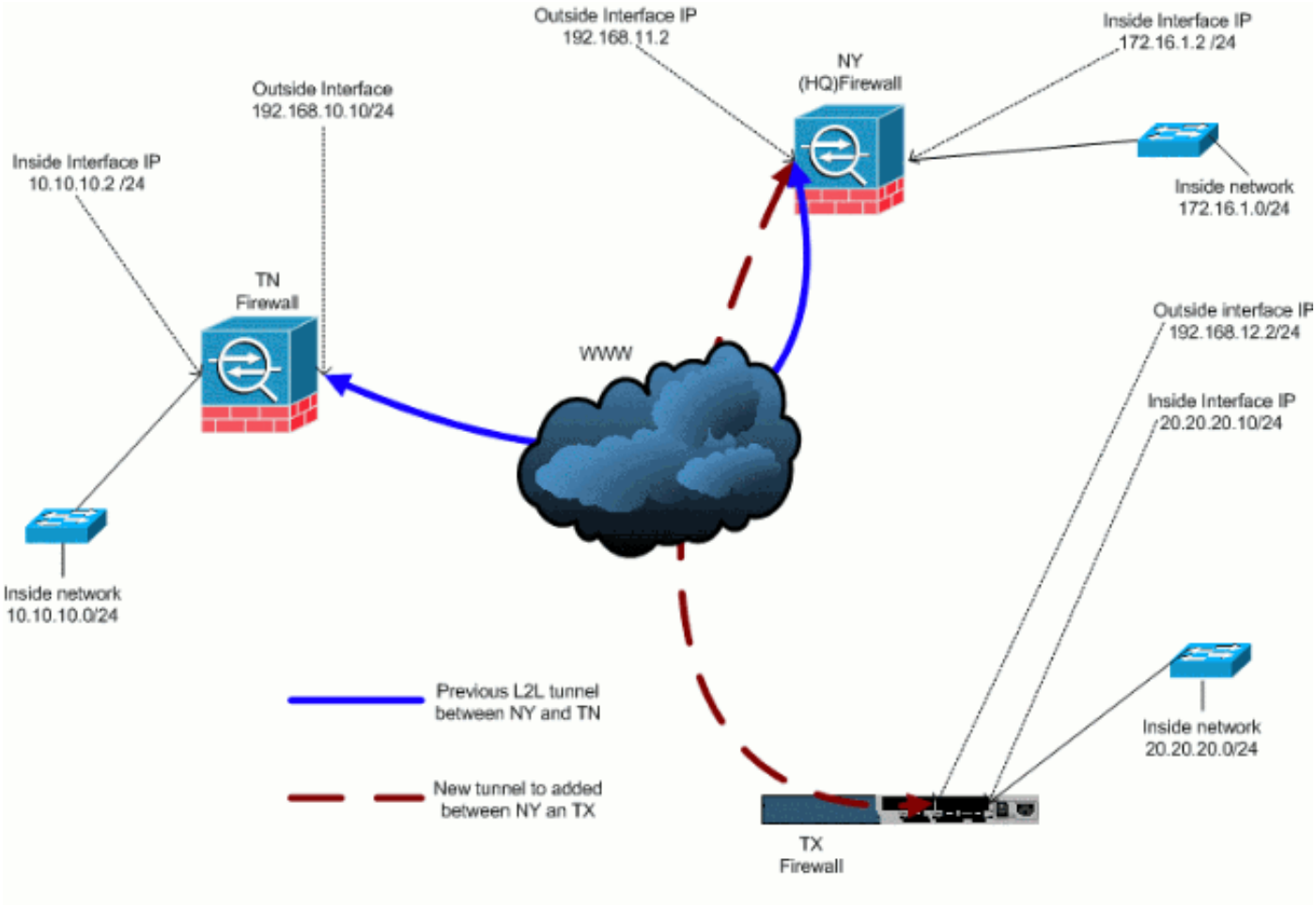
Nell'esempio, vengono usati due comandi per consentire la comunicazione tra le reti VPN e identificare il traffico che deve essere tunneling o crittografato. In questo modo è possibile accedere a Internet senza dover inviare il traffico attraverso il tunnel VPN. Per configurare queste due opzioni, usare i comandi **split-tunnel** e **same-security-traffic**.

Il tunneling ripartito consente a un client IPSec di accesso remoto di indirizzare i pacchetti in modo condizionale su un tunnel IPSec in forma crittografata o a un'interfaccia di rete in formato non crittografato. Se il tunneling suddiviso è abilitato, i pacchetti non associati alle destinazioni sull'altro lato del tunnel IPSec non devono essere crittografati, inviati tramite il tunnel, decrittografati e quindi indirizzati a una destinazione finale. Questo comando applica il criterio di tunneling suddiviso a una rete specificata. Per impostazione predefinita, viene eseguito il tunnel di tutto il traffico. Per impostare un criterio di tunneling suddiviso, utilizzare il comando **split-tunnel-policy** in modalità di configurazione criteri di gruppo. Per rimuovere il criterio di tunneling suddiviso dalla configurazione, usare la forma **no** di questo comando.

L'appliance di sicurezza include una funzionalità che consente a un client VPN di inviare traffico protetto con IPSec ad altri utenti VPN consentendo il traffico in entrata e in uscita dalla stessa interfaccia. Detta anche hairpinning, questa funzione può essere considerata come un VPN Spoke (client) che si connette tramite un hub VPN (appliance di sicurezza). In un'altra applicazione, questa funzionalità può reindirizzare il traffico VPN in ingresso indietro attraverso la stessa interfaccia del traffico non crittografato. Questa funzione è utile, ad esempio, per i client VPN che non dispongono di tunneling suddiviso, ma devono entrambi accedere a una VPN e navigare sul Web. Per configurare questa funzionalità, usare il comando **same-security-traffic** ***intra-interface*** in modalità di configurazione globale.

Aggiunta di un ulteriore tunnel L2L alla configurazione

Questo è il diagramma di rete per la configurazione:



Istruzioni dettagliate

In questa sezione vengono descritte le procedure da eseguire sull'appliance di sicurezza HUB (firewall). Fare riferimento a PIX/ASA 7.x: Esempio di configurazione semplice del tunnel VPN da PIX a PIX per ulteriori informazioni su come configurare il client spoke (firewall TX).

Attenersi alla seguente procedura:

1. Creare questi due nuovi elenchi degli accessi da utilizzare per la mappa crittografica per definire il traffico interessante:

```
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
```

   Avviso: perché la comunicazione abbia luogo, l'altro lato del tunnel deve avere l'opposto di questa voce dell'elenco di controllo di accesso (ACL) per quella particolare rete.
2. Aggiungere queste voci all'istruzione no nat per esentare le connessioni tra queste reti:

```
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
```

Avviso: per consentire la comunicazione, l'altro lato del tunnel deve avere l'opposto di questa voce ACL per quella particolare rete.

3. Per consentire a un host sulla rete VPN TX di accedere al tunnel VPN TN, eseguire questo comando:

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

Questo consente ai peer VPN di comunicare tra loro.

4. Creare la configurazione della mappa crittografica per il nuovo tunnel VPN. Utilizzare lo stesso set di trasformazioni utilizzato nella prima configurazione VPN, poiché tutte le impostazioni della fase 2 sono uguali.

```
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. Creare il gruppo di tunnel specificato per il tunnel insieme agli attributi necessari per la connessione all'host remoto.

```
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
```

Nota: la chiave già condivisa deve corrispondere esattamente su entrambi i lati del tunnel.

6. Ora che il nuovo tunnel è stato configurato, è necessario inviare del traffico interessante attraverso il tunnel per richiamarlo. Per eseguire questa operazione, usare il comando **ping** di origine per eseguire il ping di un host sulla rete interna del tunnel remoto.Nell'esempio, viene eseguito il ping di una workstation sull'altro lato del tunnel con indirizzo 20.20.20.16. Questo porta il tunnel tra NY e TX. Ora, ci sono due tunnel connessi all'ufficio centrale. Se non è possibile accedere a un sistema dietro il tunnel, fare riferimento alla sezione Soluzioni per la risoluzione dei problemi della VPN IPSec più comuni per trovare una soluzione alternativa all'utilizzo dell'`accesso di gestione`.

Esempio di configurazione

Esempio di configurazione 1
ASA-NY-HQ#**show running-config** : Saved : ASA Version 7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com

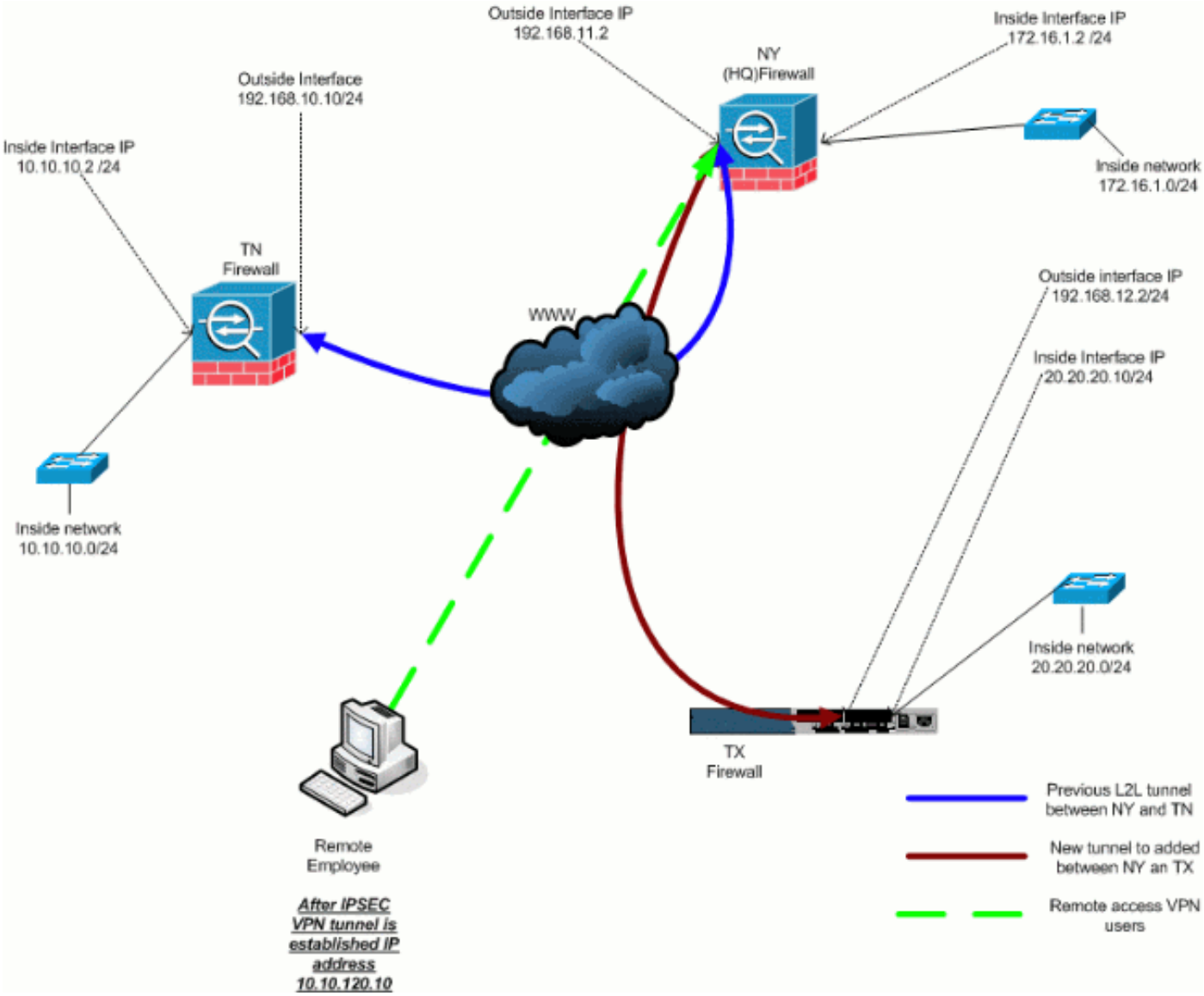
```
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 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#
```

Aggiungi VPN di accesso remoto alla configurazione

Questo è il diagramma di rete per la configurazione:



Istruzioni dettagliate

In questa sezione vengono descritte le procedure necessarie per aggiungere funzionalità di accesso remoto e consentire agli utenti remoti di accedere a tutti i siti. Per ulteriori informazioni, fare riferimento al documento PIX/ASA 7.x ASDM: Limitare l'accesso alla rete degli utenti VPN di Accesso remoto per ulteriori informazioni su come configurare il server di accesso remoto e limitare l'accesso.

Attenersi alla seguente procedura:

1. Creare un pool di indirizzi IP da utilizzare per i client che si connettono tramite il tunnel VPN. Inoltre, creare un utente di base per accedere alla VPN una volta completata la configurazione.
```
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. Evita che il traffico specifico venga indicato.
```
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
```
   Si noti che la comunicazione nat tra i tunnel VPN è esentata in questo esempio.
3. Consente la comunicazione tra i tunnel L2L già creati.
```
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
```
   Ciò consente agli utenti di accesso remoto di comunicare con le reti dietro i tunnel specificati.**Avviso:** per consentire la comunicazione, l'altro lato del tunnel deve avere l'opposto di questa voce ACL per quella particolare rete.
4. Configurare il traffico che verrà crittografato e inviato attraverso il tunnel VPN.
```
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. Configurare l'autenticazione locale e le informazioni sui criteri, ad esempio i protocolli wins,

dns e IPSec, per i client VPN.

```
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. Impostare IPSec e gli attributi generali, ad esempio chiavi già condivise e pool di indirizzi IP, che verranno utilizzati dal tunnel VPN Hillvalley.

```
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. Creare i criteri del tunnel suddiviso che useranno l'ACL creato nel passaggio 4 per specificare il traffico che verrà crittografato e passato attraverso il tunnel.

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

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

8. Configurare le informazioni sulla mappa crittografica necessarie per la creazione del tunnel VPN.

```
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
```

Esempio di configurazione

Esempio di configurazione 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#
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **ping all'interno di x.x.x.x (indirizzo IP dell'host sul lato opposto del tunnel)**: questo comando consente di inviare il traffico sul tunnel utilizzando l'indirizzo di origine dell'interfaccia interna.

Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi relativi alla configurazione, consultare i seguenti documenti:

- Soluzioni più comuni per la risoluzione dei problemi delle VPN IPSec
- Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug
- Risoluzione dei problemi di connessione tramite PIX e ASA

Informazioni correlate

- Introduzione alla crittografia IP Security (IPSec)
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems