PIX/ASA 7.X: Adicionar um novo túnel ou acesso remoto a uma VPN L2L existente

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Diagrama de Rede](#)
[Informações de Apoio](#)
[Adicionar um túnel L2L adicional à configuração](#)
[Step-by-Step Instructions](#)
[Exemplo de configuração](#)
[Adicionar uma VPN de acesso remoto à configuração](#)
[Step-by-Step Instructions](#)
[Exemplo de configuração](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento fornece as etapas exigidas para adicionar um novo túnel VPN ou uma VPN de acesso remoto para uma configuração de VPN L2L já existente. Consulte Cisco ASA 5500 Series Adaptive Security Appliances - Exemplos de Configuração e Notas Técnicas para obter informações sobre como criar os túneis VPN IPSec iniciais e para obter mais exemplos de configuração.

Prerequisites

Requirements

Certifique-se de configurar corretamente o túnel VPN IPSEC L2L que está operacional no momento antes de tentar esta configuração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dois dispositivos de segurança ASA que executam o código 7.x
- Um PIX Security Appliance com código 7.x

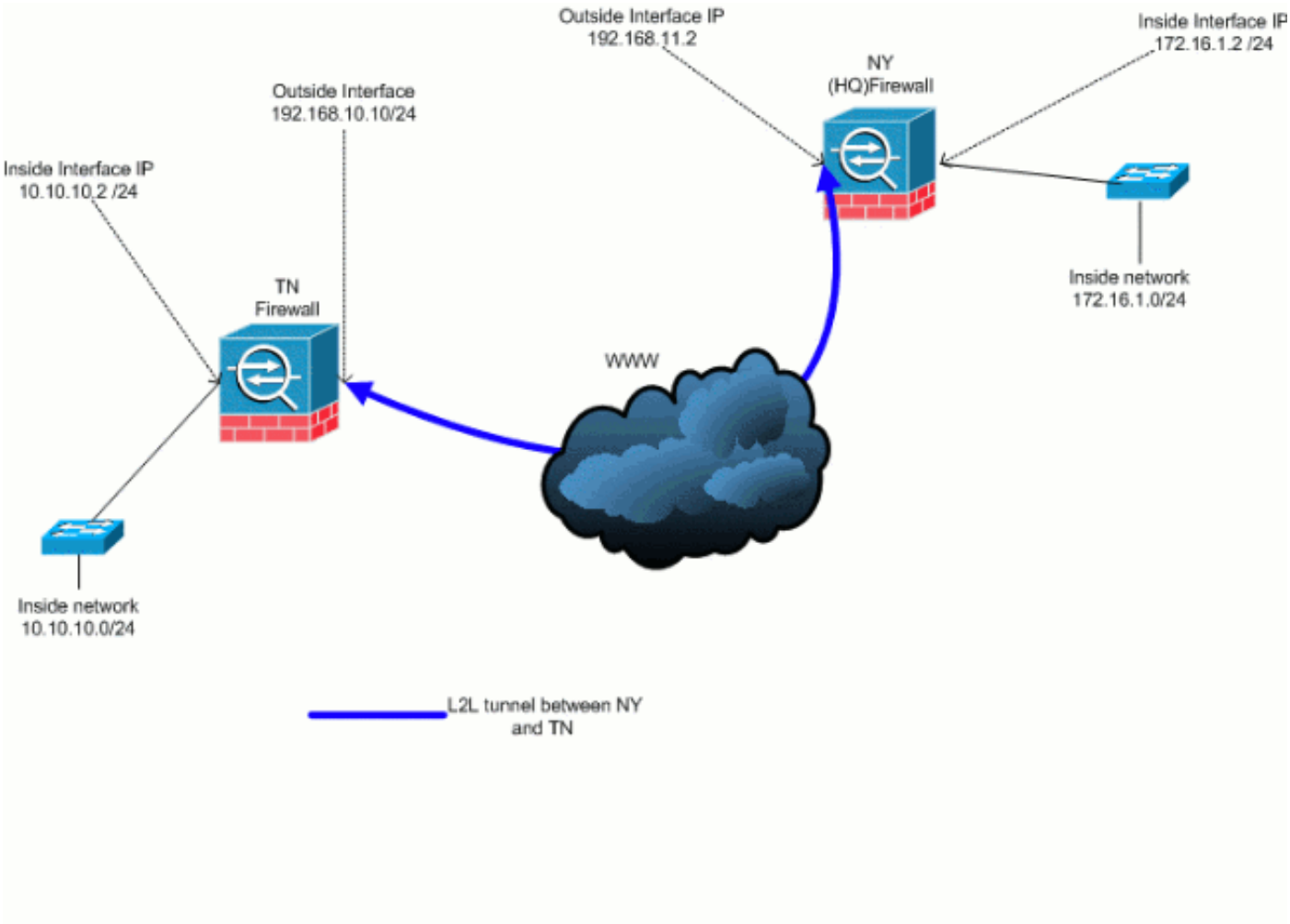
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esta saída é a configuração atual em execução do dispositivo de segurança NY (HUB). Nesta configuração, há um túnel L2L IPSec configurado entre NY(HQ) e TN.

Configuração atual do 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#
```

Informações de Apoio

Atualmente, há um túnel L2L existente configurado entre o escritório NY(HQ) e o escritório TN. Recentemente, sua empresa abriu um novo escritório localizado na TX. Esse novo escritório exige conectividade com recursos locais localizados nos escritórios da NY e da TN. Além disso, há um requisito adicional para permitir que os funcionários tenham a oportunidade de trabalhar em casa e acessem com segurança os recursos localizados na rede interna remotamente. Neste exemplo, um novo túnel VPN é configurado, bem como um servidor VPN de acesso remoto localizado no escritório da NY.

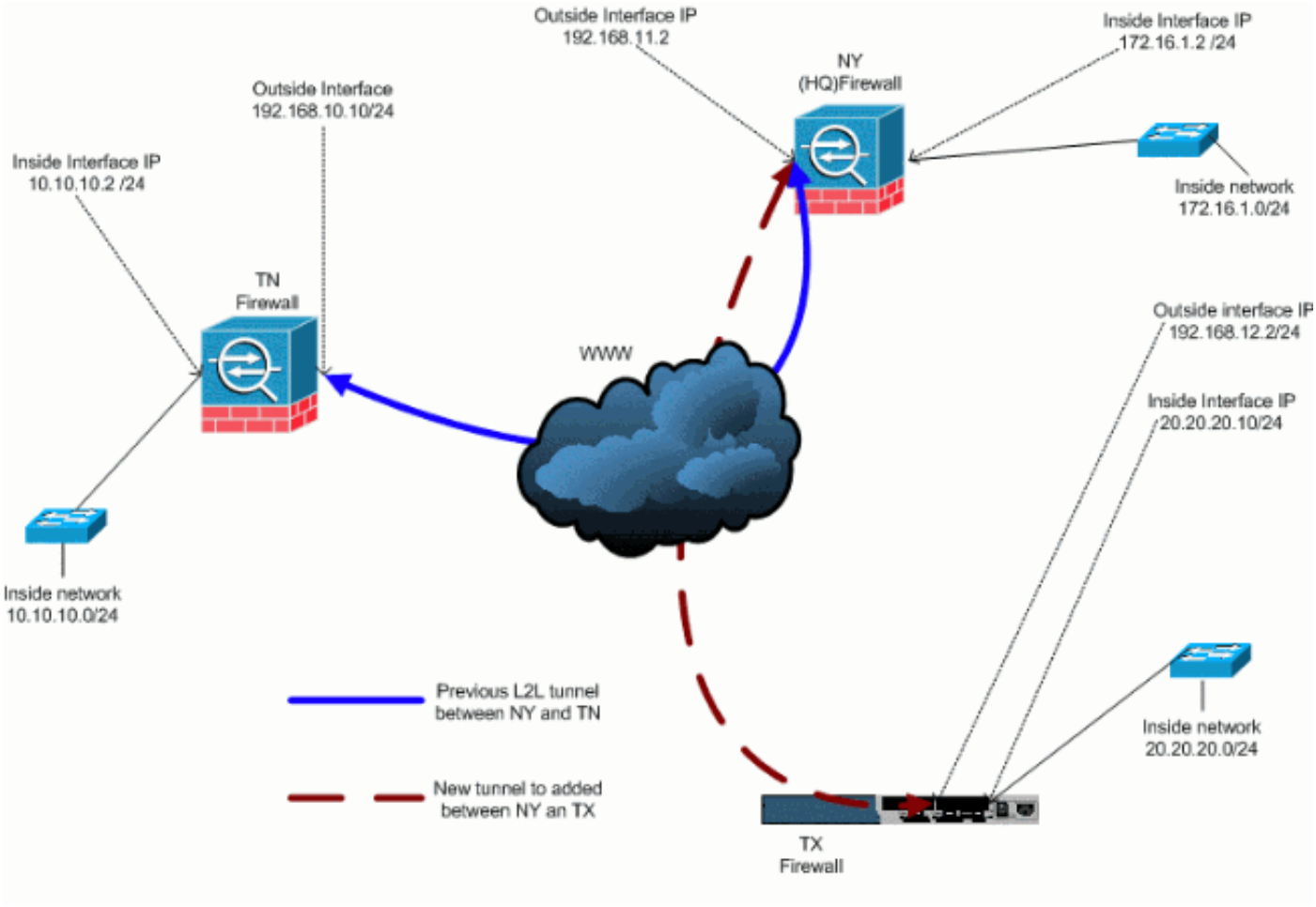
Neste exemplo, dois comandos são usados para permitir a comunicação entre as redes VPN e identificar o tráfego que deve ser encapsulado ou criptografado. Isso permite que você tenha acesso à Internet sem precisar enviar esse tráfego pelo túnel VPN. Para configurar essas duas opções, execute os comandos **split-tunnel** e **same-security-traffic**.

O tunelamento dividido permite que um cliente IPSec de acesso remoto direcione condicionalmente pacotes sobre um túnel IPSec em forma criptografada ou para uma interface de rede em forma de texto claro. Com o tunelamento dividido ativado, os pacotes não destinados aos destinos no outro lado do túnel IPSec não precisam ser criptografados, enviados pelo túnel, descriptografados e, em seguida, roteados para um destino final. Esse comando aplica essa política de tunelamento dividido a uma rede especificada. O padrão é fazer o túnel de todo o tráfego. Para definir uma política de separação de túneis, execute o comando **split-tunnel-policy** no modo de configuração da política de grupo. Para remover a política de separação de túneis da configuração, execute a forma **no** desse comando.

O Security Appliance inclui um recurso que permite que um cliente VPN envie tráfego protegido por IPSec para outros usuários de VPN, permitindo esse tráfego de entrada e saída da mesma interface. Também chamado hairpinning, esse recurso pode ser considerado como spokes VPN (clientes) que se conectam por meio de um hub VPN (Security Appliance). Em outro aplicativo, esse recurso pode redirecionar o tráfego de entrada de VPN através da mesma interface do tráfego não criptografado. Isso é útil, por exemplo, para um cliente VPN que não tem tunelamento dividido, mas precisa acessar uma VPN e navegar na Web. Para configurar esse recurso, execute o comando **same-security-traffic** ***intra-interface*** **no modo de configuração global.**

Adicionar um túnel L2L adicional à configuração

Este é o diagrama de rede para esta configuração:



Step-by-Step Instructions

Esta seção fornece os procedimentos necessários que devem ser executados no dispositivo de segurança HUB (NY Firewall). Consulte o PIX/ASA 7.x: Exemplo de Configuração de Túnel VPN PIX para PIX Simples para obter mais informações sobre como configurar o cliente spoke (Firewall TX).

Conclua estes passos:

1. Crie estas duas novas listas de acesso a serem usadas pelo mapa de criptografia para definir o tráfego 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
```

   Aviso: para que a comunicação ocorra, o outro lado do túnel deve ter o oposto desta entrada da lista de controle de acesso (ACL) para essa rede específica.
2. Adicione estas entradas à instrução no nat para isentar a nação entre estas redes:

```
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
```

Aviso: para que a comunicação ocorra, o outro lado do túnel deve ter o oposto desta entrada de ACL para essa rede específica.

3. Execute este comando para permitir que um host na rede VPN TX tenha acesso ao túnel VPN TN:

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

Isso permite que os pares VPN se comuniquem entre si.

4. Crie a configuração do mapa de criptografia para o novo túnel VPN. Use o mesmo conjunto de transformação usado na primeira configuração de VPN, já que todas as configurações da fase 2 são iguais.

```
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. Crie o grupo de túneis especificado para este túnel juntamente com os atributos necessários para se conectar ao host remoto.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
 ipsec-121

ASA-NY-HQ(config)#tunnel-group 192.168.12.2
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco123
```

Nota:A chave compartilhada deverá ser idêntica nos dois lados do túnel.

6. Agora que você configurou o novo túnel, deve enviar tráfego interessante através do túnel para ativá-lo. Para fazer isso, emita o comando **source ping** para fazer ping em um host na rede interna do túnel remoto.Neste exemplo, uma estação de trabalho no outro lado do túnel com o endereço 20.20.20.16 é enviada por ping. Isso eleva o túnel entre NY e TX. Agora, há dois túneis conectados ao escritório da sede. Se você não tiver acesso a um sistema do outro lado do túnel, consulte Soluções de Troubleshooting de VPN IPSec Mais Comuns para encontrar uma solução alternativa para o uso de management-access.

Exemplo de configuração

Exemplo de configuração 1

```
ASA-NY-HQ#show running-config

 : Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
```

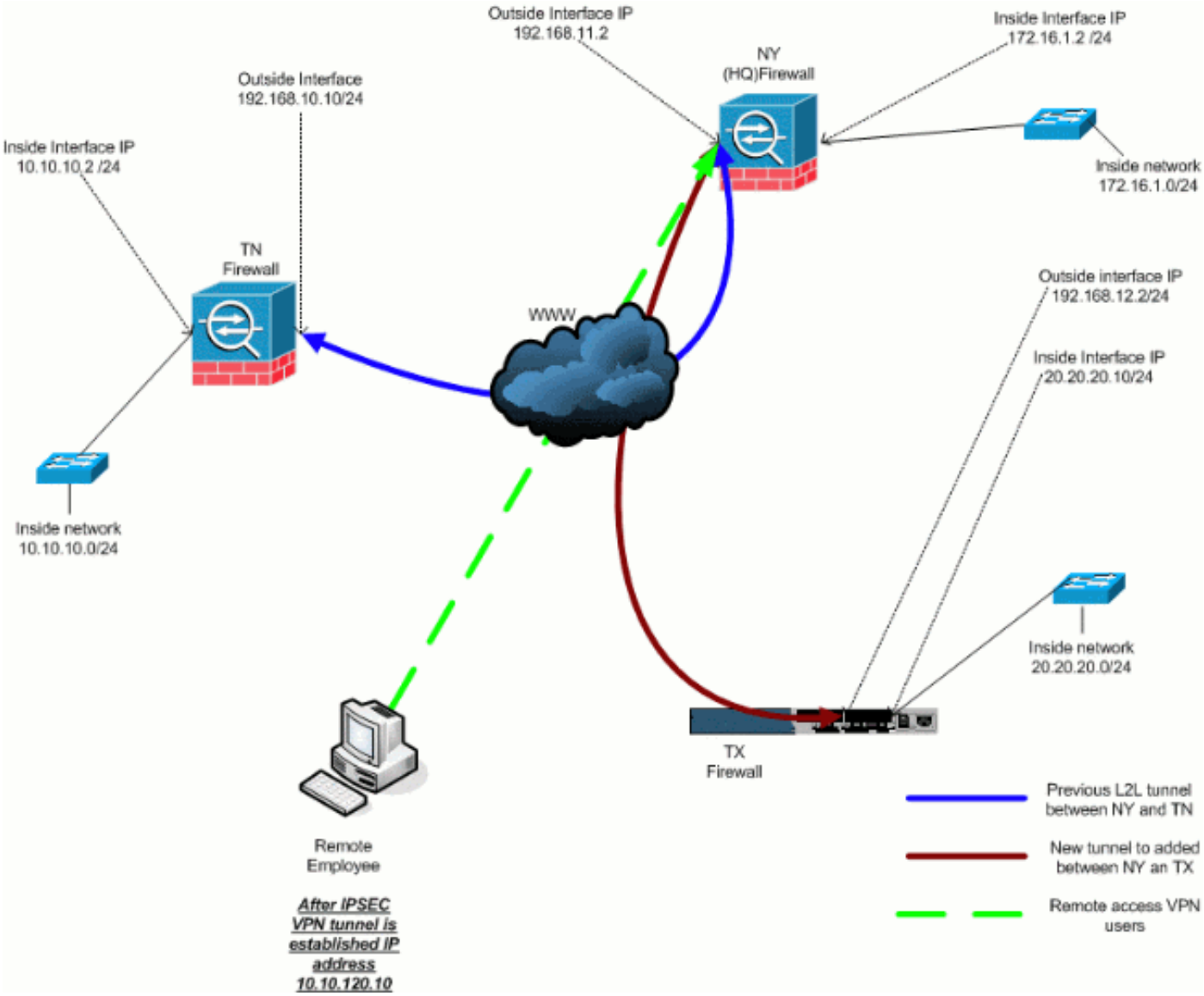
```
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level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

Adicionar uma VPN de acesso remoto à configuração

Este é o diagrama de rede para esta configuração:



Step-by-Step Instructions

Esta seção fornece os procedimentos necessários para adicionar o recurso de acesso remoto e para permitir que usuários remotos acessem todos os locais. Consulte PIX/ASA 7.x ASDM: Restrinja o acesso à rede de usuários VPN de acesso remoto para obter mais informações sobre como configurar o servidor de acesso remoto e restringir o acesso.

Conclua estes passos:

1. Crie um pool de endereços IP a ser usado para clientes que se conectam via túnel VPN. Além disso, crie um usuário básico para acessar a VPN quando a configuração for concluída.

```
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. Isentar que tráfego específico seja nado.

```
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
```

   Observe que a comunicação nat entre túneis VPN está isenta neste exemplo.

3. Permitir comunicação entre os túneis L2L já criados.

```
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
```

   Isso permite que os usuários de acesso remoto se comuniquem com redes por trás dos túneis especificados.**Aviso:** para que a comunicação ocorra, o outro lado do túnel deve ter o oposto desta entrada de ACL para essa rede específica.

4. Configure o tráfego que será criptografado e enviado através do túnel 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. Configure as informações de autenticação local e de política, como os protocolos Wins, DNS e IPSec, para os clientes 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. Defina o IPSec e os atributos gerais, como chaves pré-compartilhadas e pools de endereços IP, que serão usados pelo túnel 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. Crie a política de túnel dividido que usará a ACL criada na etapa 4 para especificar qual tráfego será criptografado e passado pelo túnel.

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

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

8. Configure as informações do mapa de criptografia necessárias para a criação do túnel 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
```

Exemplo de configuração

Exemplo de configuração 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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **ping dentro de x.x.x.x (endereço IP do host no lado oposto do túnel)**—Este comando permite que você envie o tráfego para o túnel usando o endereço de origem da interface interna.

Troubleshoot

Consulte estes documentos para obter informações que você pode usar para solucionar problemas de sua configuração:

- Soluções mais comuns de solução de problemas de VPN IPSec
- Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug
- Troubleshooting de Conexões via PIX e ASA

Informações Relacionadas

- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Referências de comandos dos Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems