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

Índice

Introdução

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.

Pré-requisitos

Requisitos

Assegure-se de que você configure corretamente o túnel do IPSEC VPN L2L que é atualmente operacional antes que você tente esta configuração.

Componentes Utilizados

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

- Duas ferramentas de segurança ASA que executam o código 7.x
- Uma ferramenta de segurança PIX que executa o código 7.x

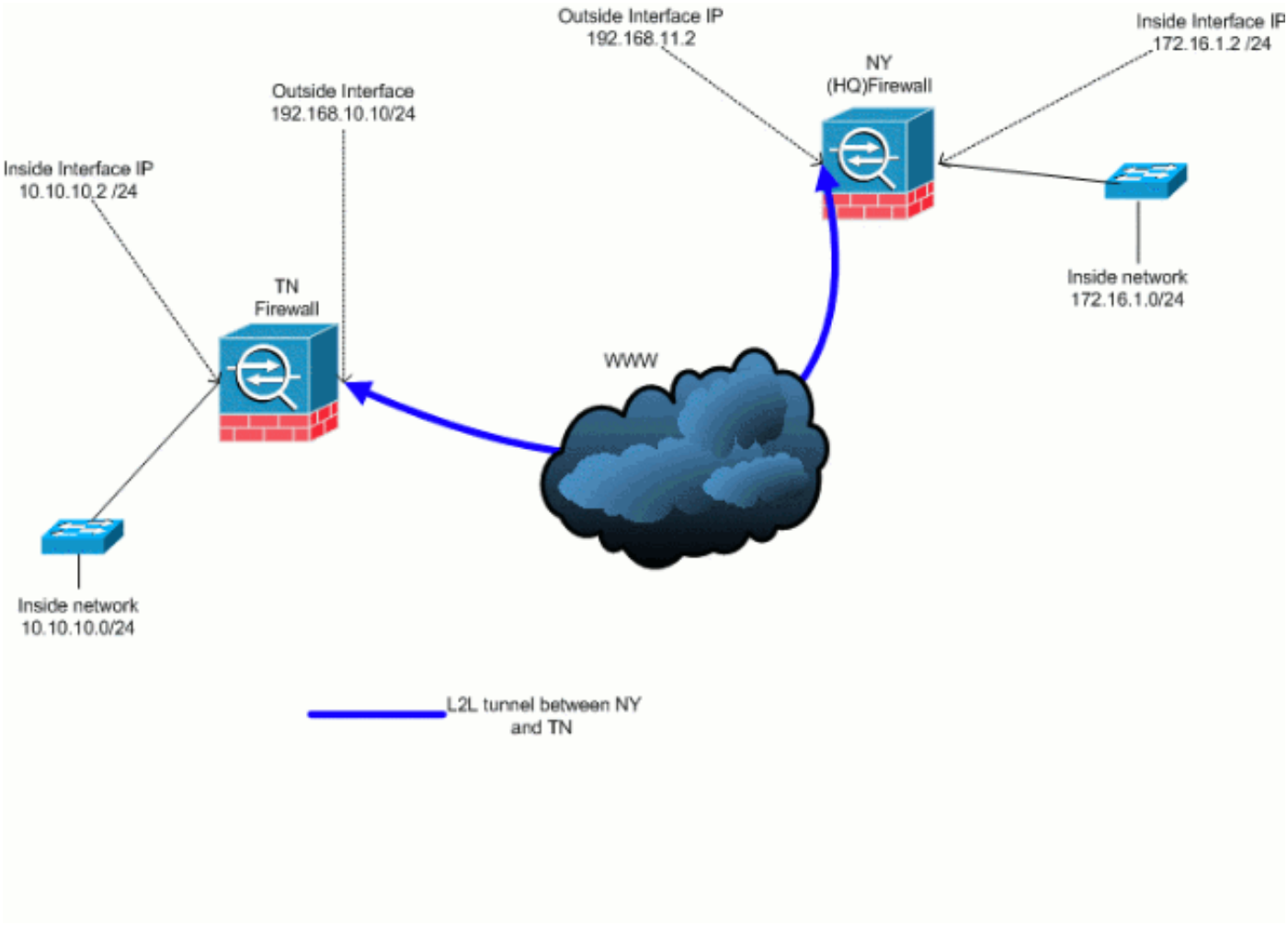
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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 em execução atualmente da ferramenta de segurança NY (HUB). Nesta configuração, há um túnel do IPsec L2L configurado entre NY(HQ) e TN.

Configuração de firewall atual NY (QG)
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 uma configuração do túnel existente L2L entre o escritório NY(HQ) e o escritório TN. Sua empresa tem aberto recentemente um escritório novo que fosse situado em TX. Este escritório novo exige a Conectividade aos recursos locais que são ficados situados nos escritórios NY e TN. Além, há uma exigência adicional permitir a empregados a oportunidade de trabalhar da HOME e de alcançar firmemente os recursos que são ficados situados na rede interna remotamente. Neste exemplo, um túnel novo VPN é configurado assim como um server do acesso remoto VPN que seja ficado situado o no escritório NY.

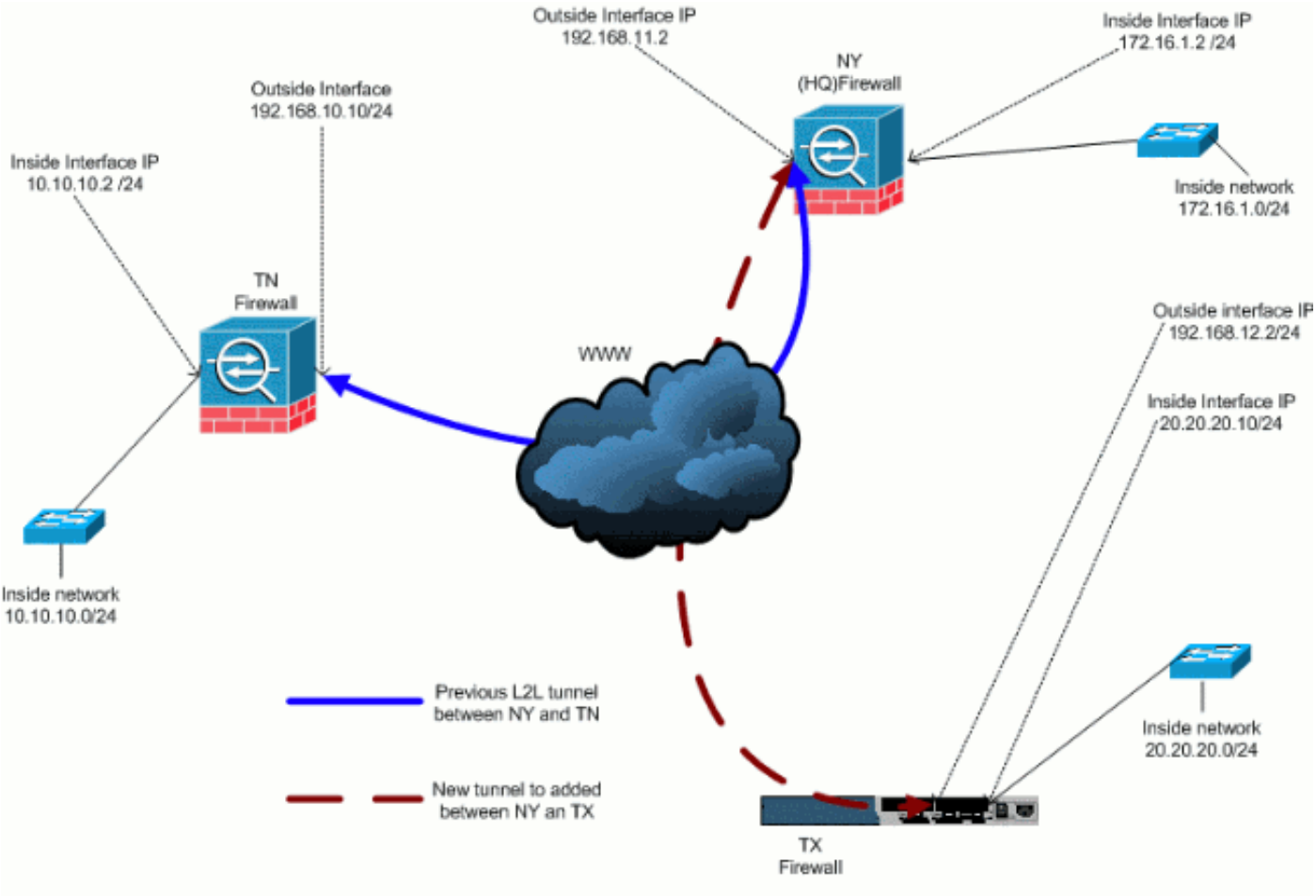
Neste exemplo, dois comandos são usados a fim permitir a comunicação entre as redes VPN e identificar o tráfego que deve ser escavado um túnel ou cifrado. Isto permite-o de ter o acesso ao Internet sem ter que enviar que tráfego através do túnel VPN. Para configurar essas duas opções, execute os comandos **split-tunnel** e **same-security-traffic**.

O Split Tunneling permite que um cliente de IPSec do acesso remoto dirija condicionalmente pacotes sobre um túnel de IPsec no formulário criptografado, ou a uma interface de rede no formulário de texto claro. Com o Split Tunneling permitido, os pacotes não limitados para destinos no outro lado do túnel de IPsec não têm que ser cifrados, enviado através do túnel, decifraram, e distribuído então a um destino final. Este comando aplica esta política do Split Tunneling a uma rede especificada. O padrão é escavar um túnel 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.

A ferramenta de segurança inclui uma característica que permita que um cliente VPN envie o tráfego protegido de IPSec a outros usuários VPN permitindo tal tráfego dentro e fora da mesma relação. O hairpinning igualmente chamado, esta característica pode ser pensado como do spokes VPN (clientes) que conecta através de um hub VPN (ferramenta de segurança). Em um outro aplicativo, esta característica pode reorientar a parte traseira entrante do tráfego VPN para fora através da mesma relação que o tráfego não criptografado. Isto é útil, por exemplo, a um cliente VPN que não tenha o Split Tunneling mas as necessidades alcançar um VPN e para consultar a Web. Para configurar esse recurso, execute o comando **same-security-traffic intra-interface** no modo de configuração global.

Adicionar um túnel adicional L2L à configuração

Este é o diagrama da rede para esta configuração:



Instruções passo a passo

Esta seção fornece os procedimentos exigidos que devem ser executados na ferramenta de segurança do HUB (Firewall NY). Refira o PIX/ASA 7.x: Exemplo de configuração do túnel PIX a PIX VPN simples para obter mais informações sobre de como configurar o cliente do spoke (Firewall TX).

Conclua estes passos:

1. Crie estas duas listas de acesso novas a ser usadas pelo crypto map a fim definir o tráfego interessante:`ASA-NY-HQ(config)#access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-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 do Access Control List (ACL) para essa rede particular.
2. Adicionar estas entradas a nenhuma indicação nat a fim isentar nating entre estas redes:`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-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 ACL para essa rede particular.
3. Emita este comando a fim permitir um host na rede VPN TX de ter o acesso ao túnel TN VPN:`ASA-NY-HQ(config)#same-security-traffic permit intra-interface`Isto permite que os pares VPN falem entre se.
4. Crie a configuração do crypto map para o túnel novo VPN. Use o mesmos transformam o grupo que foi usado na primeira configuração de VPN, como todos os ajustes da fase 2 são o mesmos.`ASA-NY-HQ(config)#crypto map outside_map 30 match address outside_30_cryptomapASA-NY-HQ(config)#crypto map outside_map 30 set peer 192.168.12.2ASA-NY-HQ(config)#crypto map outside_map 30 set transform-set ESP-3DES-SHA`
5. Crie o grupo de túneis que é especificado para este túnel junto com os atributos necessários conectar ao host remoto.`ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type ipsec-l2lASA-NY-HQ(config)#tunnel-group 192.168.12.2 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key cisco123`**Nota:** A chave pré-compartilhada deve combinar exatamente em ambos os lados do túnel.
6. Agora que você configurou o túnel novo, você deve enviar o tráfego interessante através do túnel a fim trazê-lo acima. A fim executar isto, emita o **comando ping da fonte** sibilar 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 sibilada. Isto traz o túnel acima entre o NY e o TX. Agora, há dois túneis conectados ao escritório QG. 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

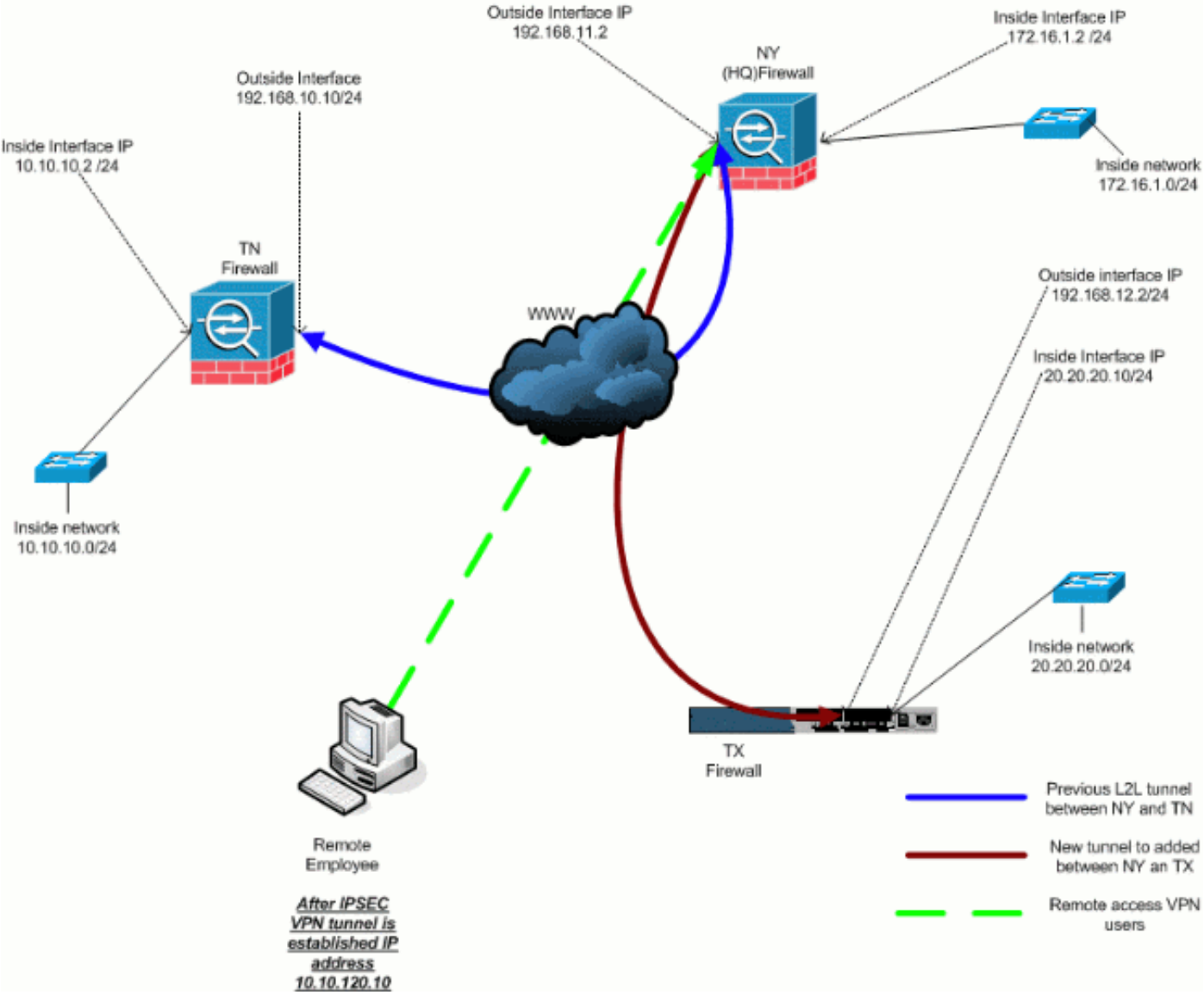
Exemplo de configuração 1
`ASA-NY-HQ#show running-config : Saved : ASA Version 7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable`

```
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 um acesso remoto VPN à configuração

Este é o diagrama da rede para esta configuração:



Instruções passo a passo

Esta seção fornece os procedimentos exigidos para adicionar a capacidade de Acesso remoto e para permitir que os usuários remotos alcancem todos os locais. Refira PIX/ASA 7.x ASDM: Restrinja o acesso de rede de usuários do acesso remoto VPN para obter mais informações sobre de como configurar o servidor de acesso remoto e restringir o acesso.

Conclua estes passos:

1. Crie um pool do endereço IP de Um ou Mais Servidores Cisco ICM NT a ser usado para os

clientes que conectam através do túnel VPN. Também, crie um usuário básico a fim alcançar o VPN uma vez que a configuração é terminada.`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. Isente o tráfego específico de ser 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`Observe que a comunicação nat entre túneis VPN está isentada neste exemplo.
3. Permita uma comunicação entre os túneis L2L que são criados já.`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`Isto permite a usuários de acesso remotos a capacidade para comunicar-se com as redes atrás dos túneis especificados.**aviso:** Para que a comunicação ocorra, o outro lado do túnel deve ter o oposto desta entrada ACL para essa rede particular.
4. Configurar o tráfego que será cifrado e enviado através do túnel VPN.`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. Configurar a autenticação local e a informação sobre a política, tal como vitórias, dns e protocolos IPSec, para os clientes VPN.`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. Ajuste o IPsec e atributos gerais, tais como as chaves pré-compartilhada e as associações do endereço IP de Um ou Mais Servidores Cisco ICM NT, que serão usadas pelo túnel de Hillvalley VPN.`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. Crie a política do túnel em divisão que usará o ACL criado em etapa 4 a fim especificar que tráfego será cifrado e passado através do túnel.`ASA-NY-HQ(config)#split-tunnel-policy tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value Hillvalley_splitunnel`
8. Configurar a informação de mapa do cryto exigida à criação de túnel VPN.`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`

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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **sibile dentro de x.x.x.x (endereço IP de Um ou Mais Servidores Cisco ICM NT do host no lado oposto do túnel) — este** comando permite que você envie o tráfego abaixo do túnel usando um endereço de origem da interface interna.

Troubleshooting

Refira estes documentos para a informação que você pode se usar a fim pesquisar defeitos sua configuração:

- A maioria de soluções do Troubleshooting do IPSec comum VPN
- 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 do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Suporte Técnico e Documentação - Cisco Systems