

# IO VPN(Router): Adicionar um túnel novo ou o Acesso remoto L2L a um L2L existente VPN

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Diagrama de Rede](#)

[Informações de Apoio](#)

[Adicionar um túnel adicional L2L à configuração](#)

[Instruções passo a passo](#)

[Exemplo de configuração](#)

[Adicionar um acesso remoto VPN à configuração](#)

[Instruções passo a passo](#)

[Exemplo de configuração](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento fornece as etapas exigidas para adicionar um novo túnel de VPN L2L ou um acesso remoto VPN a uma configuração de VPN L2L que já exista em um roteador IOS.

## 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:

- Dois IOS Router que executam as versões de software 12.4 e 12.2
- Uma ferramenta de segurança adaptável de Cisco (ASA) essa executa a versão de software 8.0

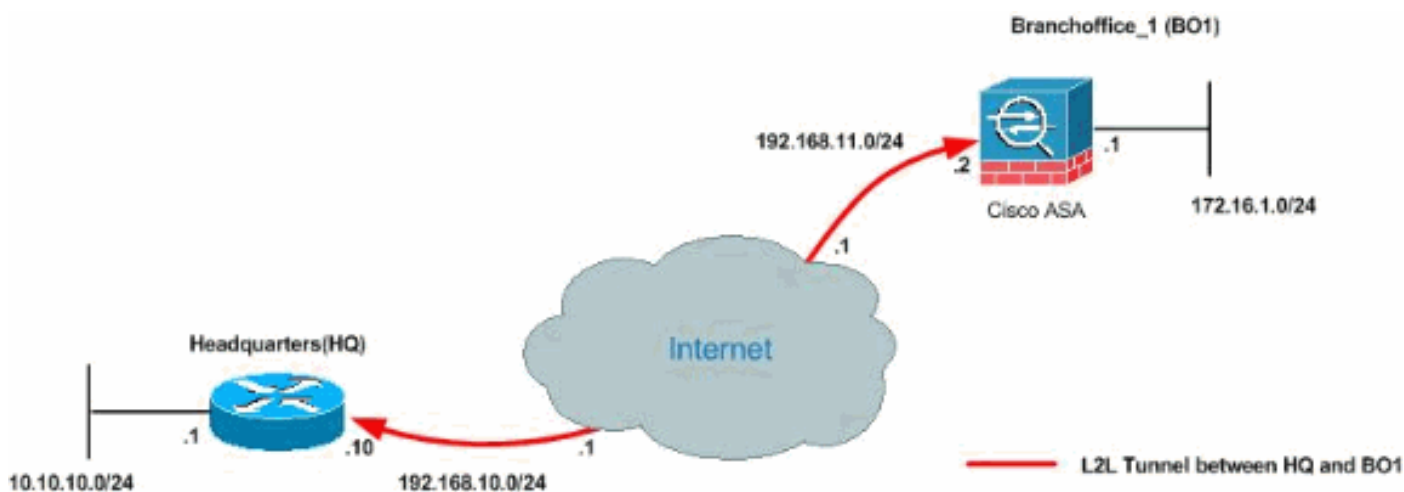
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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



Estas saídas são as configurações em execução atualmente do roteador QG (HUB) e do escritório filial 1 (BO1) ASA. Nesta configuração, há um túnel do IPsec L2L configurado entre QG e BO1 ASA.

### Configuração de roteador atual QG (HUB)

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
  encr 3des
```

```

authentication pre-share
group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.11.2
set transform-set newset
match address VPN_BO1
!
!
!
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside

interface Serial2/0
ip address 192.168.10.10 255.255.255.0
ip nat outside
ip virtual-reassembly
clock rate 64000
crypto map map1
!
interface Serial2/1
no ip address
shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#

```

## Configuração BO1 ASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)

```

```
!  
hostname CiscoASA  
enable password 8Ry2YjIyt7RRXU24 encrypted  
names  
!  
interface Ethernet0  
  nameif inside  
  security-level 100  
  ip address 172.16.1.1 255.255.255.0  
!  
interface Ethernet1  
  nameif outside  
  security-level 0  
  ip address 192.168.11.2 255.255.255.0  
!  
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU  
encrypted ftp mode passive access-list 100 extended  
permit ip 172.16.1.0 255.255.255.0 10.10.10.0  
255.255.255.0  
access-list nonat extended permit ip 172.16.1.0  
255.255.255.0 10.10.10.0 255.255.255.0  
access-list ICMP extended permit icmp any any  
pager lines 24  
mtu outside 1500  
mtu inside 1500  
no failover  
icmp unreachable rate-limit 1 burst-size 1  
asdm image flash:/asdm-602.bin  
no asdm history enable  
arp timeout 14400  
global (outside) 1 interface  
nat (inside) 0 access-list nonat  
nat (inside) 1 10.10.10.0 255.255.255.0  
access-group ICMP in interface outside  
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1  
snmp-server enable traps snmp authentication linkup  
linkdown coldstart  
crypto ipsec transform-set newset esp-3des esp-md5-hmac  
crypto map map1 5 match address 100  
crypto map map1 5 set peer 192.168.10.10  
crypto map map1 5 set transform-set newset  
crypto map map1 interface outside  
crypto isakmp enable outside  
crypto isakmp policy 1  
  authentication pre-share  
  encryption 3des  
  hash sha  
  group 2  
  lifetime 86400  
crypto isakmp policy 65535  
  authentication pre-share  
  encryption 3des  
  hash sha  
  group 2  
  lifetime 86400  
telnet timeout 5  
ssh timeout 5  
console timeout 0  
threat-detection basic-threat  
threat-detection statistics access-list  
!  
class-map inspection_default  
  match default-inspection-traffic  
!
```

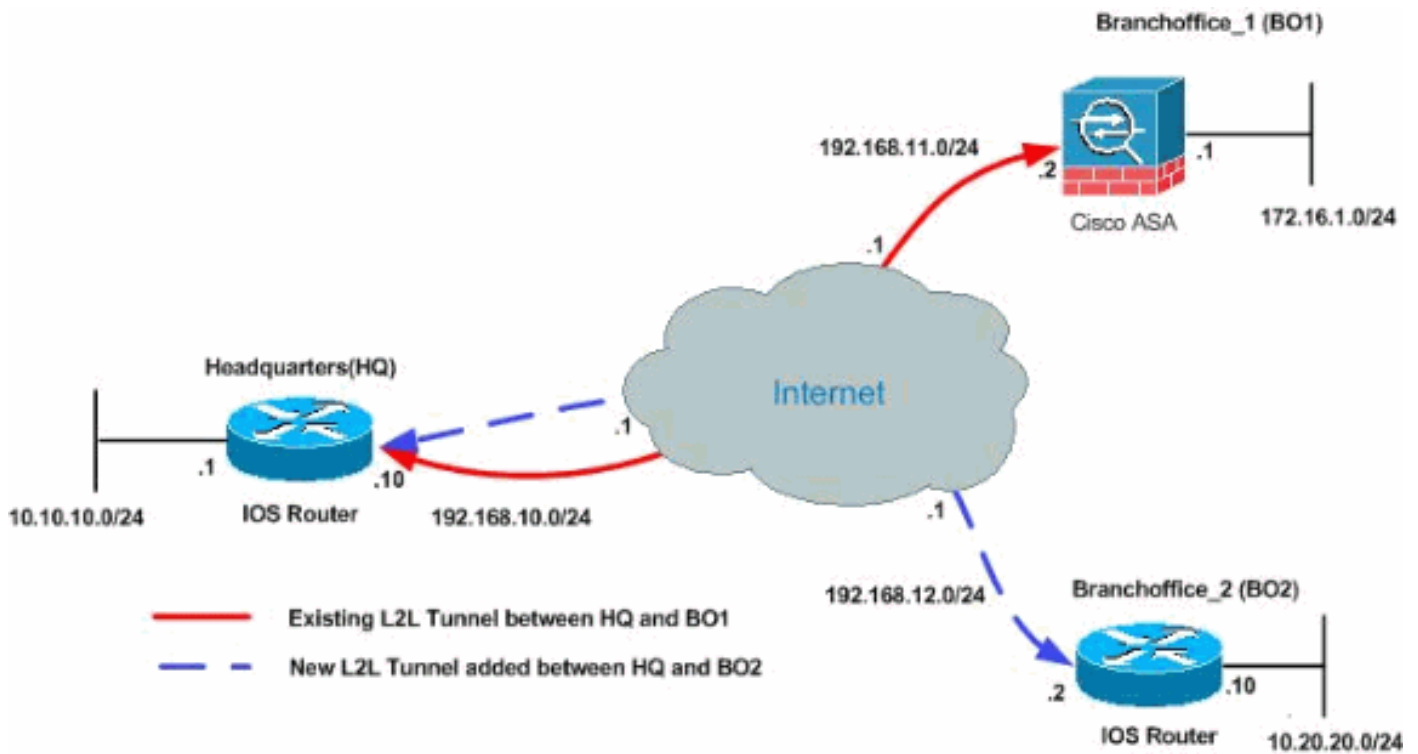
```
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum 512  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect netbios  
    inspect rsh  
    inspect rtsp  
    inspect skinny  
    inspect esmtp  
    inspect sqlnet  
    inspect sunrpc  
    inspect tftp  
    inspect sip  
    inspect xdmcp  
!  
service-policy global_policy global  
tunnel-group 192.168.10.10 type ipsec-l2l  
tunnel-group 192.168.10.10 ipsec-attributes  
  pre-shared-key *  
prompt hostname context  
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e  
: end  
CiscoASA#
```

## [Informações de Apoio](#)

Atualmente, há uma configuração do túnel existente L2L entre o escritório QG e o escritório BO1. Sua empresa tem aberto recentemente um escritório filial novo (BO2). Este escritório novo exige a Conectividade aos recursos locais que são ficados situados no escritório QG. 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 QG.

## [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 no roteador QG do HUB.

Conclua estes passos:

1. Crie esta lista de acesso nova a ser usada pelo crypto map a fim definir o tráfego

```

interessante:HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
  
```

**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:HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
  
```

Adicionar estes ACL ao nonat do mapa de rota existente:HQ\_HUB(config)#route-map nonat permit 10

```

HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
  
```

**aviso:** Para que a comunicação ocorra, o outro lado do túnel deve ter o oposto desta entrada ACL para essa rede particular.

3. Especifique o endereço de peer na configuração da fase 1 como

```

mostrado:HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
  
```

**Nota:** A chave pré-compartilhada deve combinar exatamente em ambos os lados do túnel.

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.HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
HQ_HUB(config-crypto-map)#set peer 192.168.12.2
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#match address VPN_BO2
  
```

5. 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 extended ping sibilando um host na rede interna do túnel remoto. Neste exemplo, uma estação de trabalho no outro lado do túnel com o endereço 10.20.20.16 é sibilada. Isto traz o túnel acima entre o QG e o BO2. Agora, há dois túneis conectados ao escritório QG. Se você não tem o acesso a um sistema atrás do túnel, refira [a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções](#) para encontrar uma solução alternativa usando o acesso de gerenciamento.

## Exemplo de configuração

### HUB\_HQ - Adicionou uma configuração de túnel nova L2L VPN

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
```

```

!
interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255

!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#

```

## Configuração de túnel BO2 L2L VPN

```

BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!

```

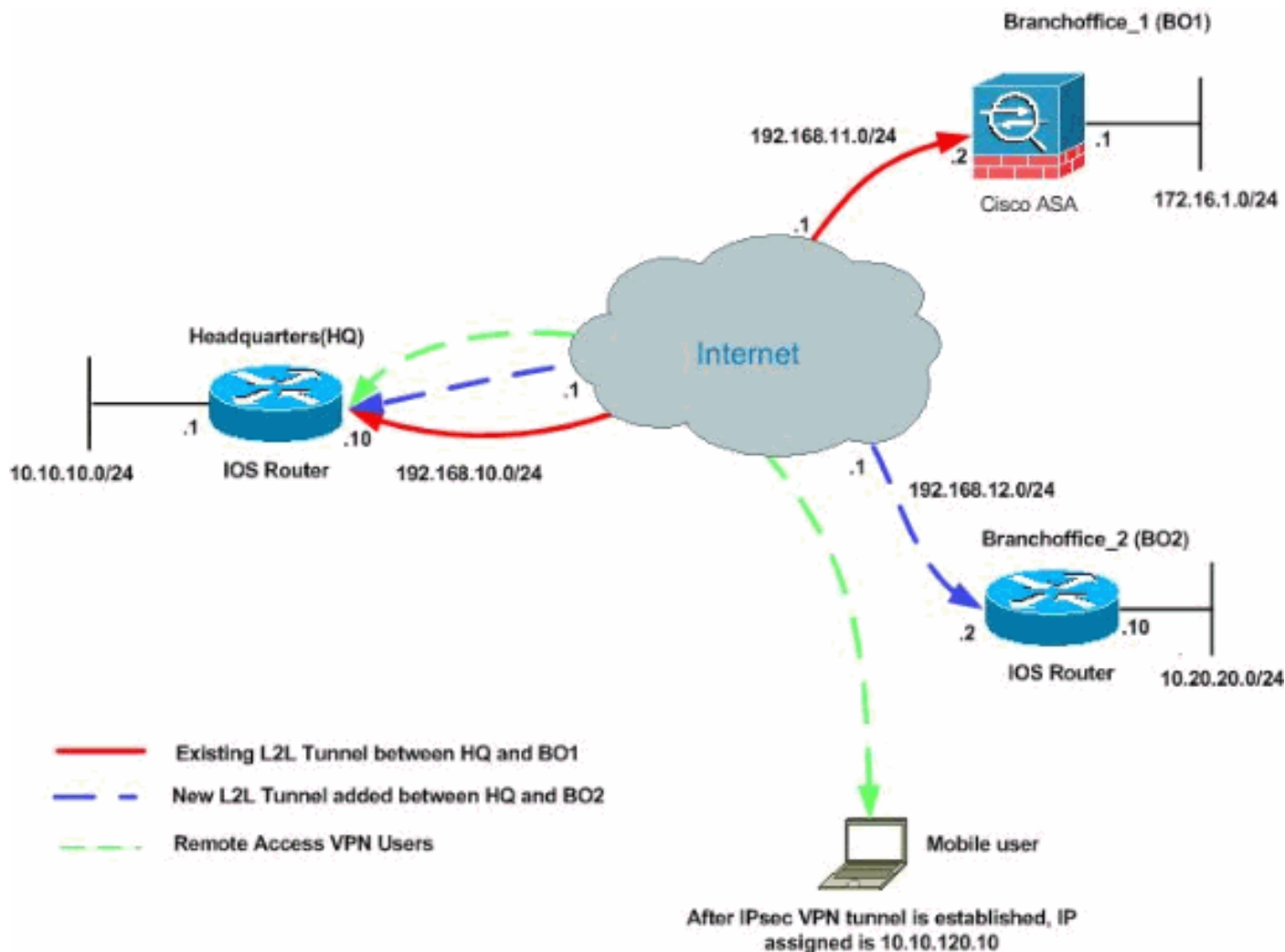


```
!  
!  
!  
!  
ip subnet-zero  
!  
!  
!  
crypto isakmp policy 10  
  authentication pre-share  
  encryption 3des  
  group 2  
crypto isakmp key cisco123 address 192.168.10.10  
!  
!  
crypto ipsec transform-set newset esp-3des esp-md5-hmac  
!  
crypto map map1 5 ipsec-isakmp  
  set peer 192.168.10.10  
  set transform-set newset  
  match address 100  
!  
!  
!  
!  
interface Ethernet0  
  ip address 10.20.20.10 255.255.255.0  
  ip nat inside  
!  
!  
interface Ethernet1  
  ip address 192.168.12.2 255.255.255.0  
  ip nat outside  
  crypto map map1  
!  
interface Serial0  
  no ip address  
  no fair-queue  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
ip nat inside source route-map nonat interface Ethernet1  
overload  
ip classless  
ip route 0.0.0.0 0.0.0.0 192.168.12.1  
ip http server  
!  
access-list 100 permit ip 10.20.20.0 0.0.0.255  
10.10.10.0 0.0.0.255  
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0  
0.0.0.255  
access-list 150 permit ip 10.20.20.0 0.0.0.255 any  
route-map nonat permit 10  
  match ip address 150  
!  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
  login
```

```
!  
end  
BO2#
```

## Adicionar um acesso remoto VPN à configuração

Este é o diagrama da rede para esta configuração:



Neste exemplo, a característica chamada **split-tunneling** é usada. Esta característica 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, decifram, e distribuído então a um destino final. Este conceito aplica a política do Split Tunneling a uma rede especificada. O padrão é escavar um túnel todo o tráfego. A fim ajustar uma política do Split Tunneling, especifique um ACL onde o tráfego significado para o Internet possa ser mencionado.

## 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.

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.

```
HQ_HUB(config)#ip local pool ippool
10.10.120.10 10.10.120.50
```

```
HQ_HUB(config)#username vpnuser password 0 vpnuser123
```

2. Isente o tráfego específico de ser nated.

```
HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit
```

Adicionar estes ACL ao nonat do mapa de rota existente:

```
HQ_HUB(config)#route-map nonat
permit 10
```

```
HQ_HUB(config-route-map)#match ip address NAT_Exempt
```

```
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

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

3. Permita uma comunicação entre os túneis L2L e os usuários existentes do acesso remoto

VPN.

```
HQ_HUB(config)#ip access-list extended VPN_BO1
```

```
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
HQ_HUB(config-ext-nacl)#exit
```

```
HQ_HUB(config)#ip access-list extended VPN_BO2
```

```
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
```

```
HQ_HUB(config-ext-nacl)#exit
```

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 split-tunneling** A fim permitir o Split Tunneling para as conexões de VPN, certifique-se de você configurar um ACL no roteador. Neste exemplo, o comando do **split\_tunnel da lista de acesso** é associado com o grupo para propósitos de split-tunneling, e o túnel é formado a 10.10.10.0 /24 e 10.20.20.0/24 e 172.16.1.0/24 redes. Fluxos de tráfego unencrypted aos dispositivos não no túnel em divisão ACL (por exemplo, o

Internet).

```
HQ_HUB(config)#ip access-list extended split_tunnel
```

```
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
```

```
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
```

```
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
```

```
HQ_HUB(config-ext-nacl)#exit
```

5. Configurar a autenticação local, a autorização e a informação de configuração de cliente, tal como vitórias, dns. tráfego interessante acl e pool IP, para os clientes

VPN.

```
HQ_HUB(config)#aaa new-model
```

```
HQ_HUB(config)#aaa authentication login userauthen local
```

```
HQ_HUB(config)#aaa authorization network groupauthen local
```

```
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
```

```
HQ_HUB(config-isakmp-group)#key cisco123
```

```
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
```

```
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
```

```
HQ_HUB(config-isakmp-group)#domain cisco.com
```

```
HQ_HUB(config-isakmp-group)#pool ippool
```

```
HQ_HUB(config-isakmp-group)#acl split_tunnel
```

```
HQ_HUB(config-isakmp-group)#exit
```

6. Configurar o mapa dinâmico e a informação de mapa do crypto exigidos à criação de túnel

VPN.

```
HQ_HUB(config)#crypto isakmp profile vpnclient
```

```
HQ_HUB(config-isakmp-group)#match identity group vpngroup
```

```
HQ_HUB(config-isakmp-group)#client authentication list userauthen
```

```
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthen
```

```
HQ_HUB(config-isakmp-group)#client configuration address respond
```

```
HQ_HUB(config-isakmp-group)#exit
```

```

HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1

```

## Exemplo de configuração

### Exemplo de configuração 2

```

HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
  key cisco123
  dns 10.10.10.10
  wins 10.10.10.20
  domain cisco.com
  pool ippool
  acl split_tunnel
crypto isakmp profile vpnclient
  match identity group vpngroup
  client authentication list userauthen
  isakmp authorization list groupauthor
  client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
!
crypto dynamic-map dynmap 10

```

```
set transform-set remote-set
set isakmp-profile vpnclient
reverse-route
!
!
crypto map map1 5 ipsec-isakmp
set peer 192.168.11.2
set transform-set newset
match address VPN_BO1
crypto map map1 10 ipsec-isakmp
set peer 192.168.12.2
set transform-set newset
match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside
ip virtual-reassembly
!

interface Serial2/0
ip address 192.168.10.10 255.255.255.0
ip nat outside
ip virtual-reassembly
clock rate 64000
crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255

!
route-map nonat permit 10
match ip address NAT_Exempt
!
!
```

```
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

## 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.

- **sibilo** — Este comando permite que você inicie o túnel L2L VPN como mostrado.

## Troubleshooting

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

- [Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto](#)
- [Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug](#)

**Dica:** Quando você [cancela associações de segurança](#), e não resolve uma edição do IPsec VPN, a seguir remova e reaplique o crypto map relevante a fim resolver uma ampla variedade de edições.

**aviso:** Se você remove um crypto map de uma relação, derruba todos os túneis de IPsec associados com esse crypto map. Siga estas etapas com cuidado e considere a política do controle de alterações de sua organização antes que você continue.

### Exemplo

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## Informações Relacionadas

- [Uma introdução à criptografia do protocolo de segurança IP \(IPSEC\)](#)
- [Página de Suporte de Negociação IPsec/Protocolos IKE](#)
- [Configurando um par dinâmico e clientes VPN do LAN para LAN do roteador de IPsec](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)