VPN (router) IOS: Aggiunta di un nuovo tunnel L2L o di un accesso remoto a una VPN L2L esistente

Sommario

Introduzione

In questo documento viene descritto come aggiungere un nuovo tunnel VPN L2L o una VPN ad accesso remoto a una configurazione VPN L2L già esistente in un router IOS.

Prerequisiti

Requisiti

Prima di provare a eseguire la 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 router IOS con software le versioni 12.4 e 12.2
- Una Cisco Adaptive Security Appliance (ASA) con software versione 8.0

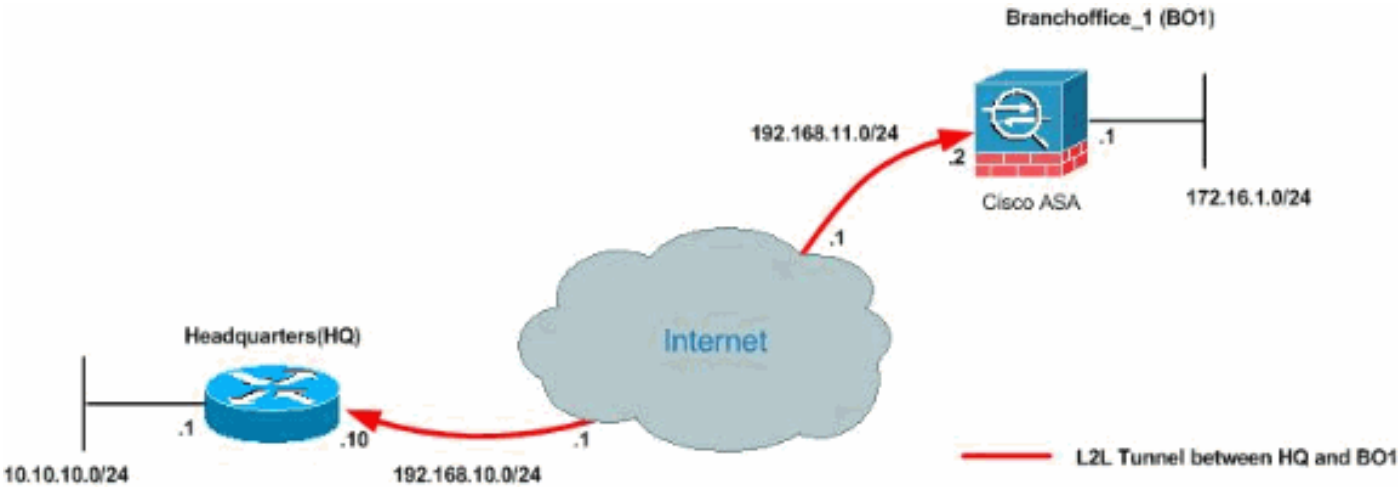
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Queste uscite sono le configurazioni correnti in esecuzione del router HQ (HUB) e dell'ASA Branch Office 1 (BO1). In questa configurazione, è presente un tunnel IPSec L2L configurato tra HQ e BO1 ASA.

Configurazione corrente router HQ (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#
```

Configurazione di 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
```

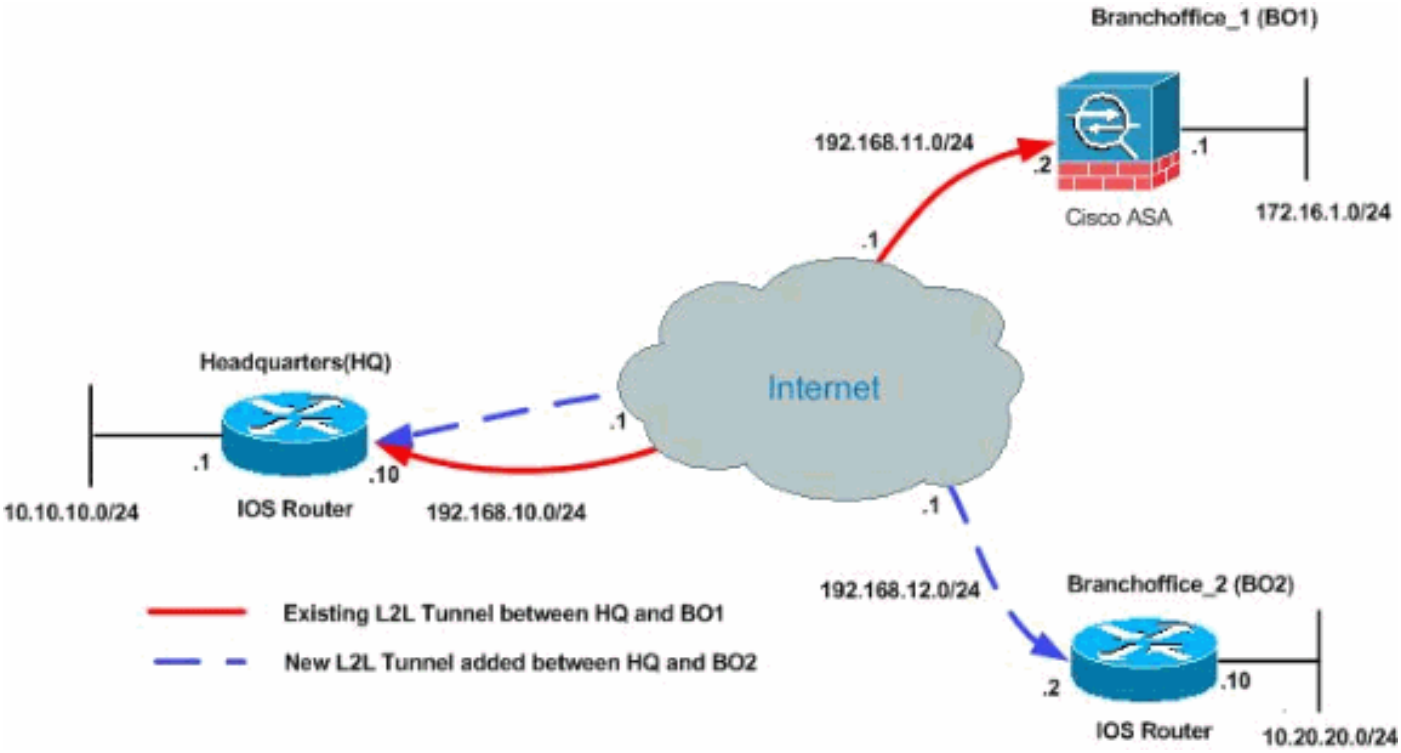
```
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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#
```

Premesse

Attualmente, tra l'ufficio centrale e l'ufficio BO1 è configurato un tunnel L2L esistente. La società ha recentemente aperto una nuova filiale (BO2). Questo nuovo ufficio richiede connettività con le risorse locali che si trovano nella sede centrale. 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. Nell'esempio, viene configurato un nuovo tunnel VPN e un server VPN ad accesso remoto situato nella sede centrale.

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 richieste da eseguire sul router HUB HQ.

Attenersi alla seguente procedura:

1. Creare questo nuovo elenco degli accessi da utilizzare per la mappa crittografica per definire il traffico 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
   ```

   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:
   ```
   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
   ```

   Aggiungere gli ACL seguenti alla mappa dei percorsi esistente **non in corrispondenza**:
   ```
   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
   ```

   Avviso: per consentire la comunicazione, l'altro lato del tunnel deve avere l'opposto di questa voce ACL per quella particolare rete.
3. Specificare l'indirizzo del peer nella configurazione della fase 1 come mostrato:
   ```
   HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
   ```

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

```
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. 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** esteso 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 10.20.20.16. Questo porta il tunnel tra la sede centrale e BO2. Ora, ci sono due tunnel connessi all'ufficio centrale. Se non si dispone dell'accesso a un sistema dietro il tunnel, vedere Soluzioni per la risoluzione dei problemi VPN IPSec di L2L e di accesso remoto più comuni per trovare una soluzione alternativa tramite `management-access`.

Esempio di configurazione

HUB_HQ - Aggiunta nuova configurazione tunnel VPN L2L

```
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#
```

Configurazione tunnel VPN L2L BO2

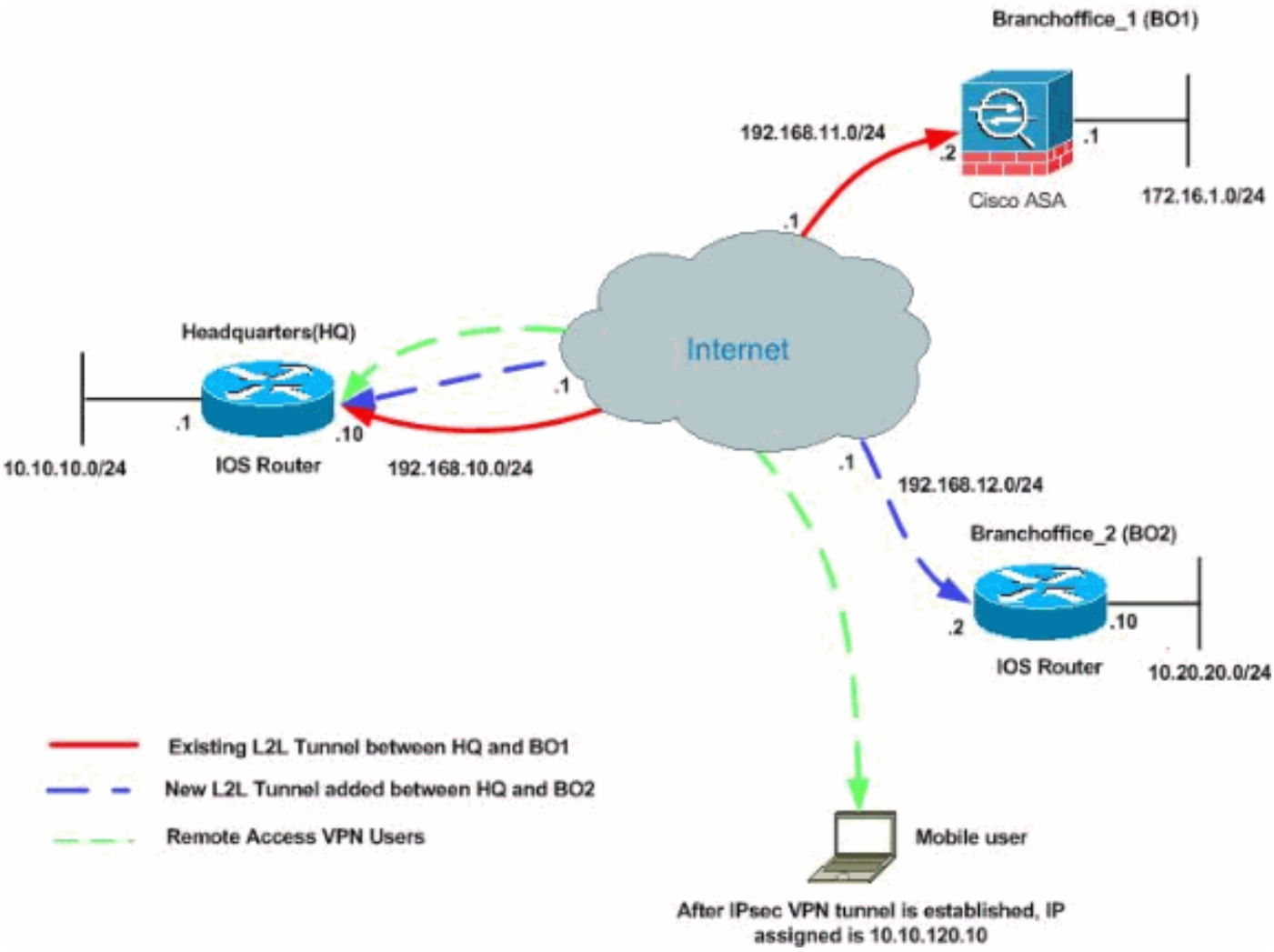
```
BO2#show running-config
Building configuration...

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#
```

Aggiungi VPN di accesso remoto alla configurazione

Questo è il diagramma di rete per la configurazione:



Nell'esempio viene utilizzata la funzione **split-tunneling**. Questa funzionalità 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 concetto applica i criteri 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, specificare un ACL in cui possa essere indicato il traffico destinato a Internet.

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.

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


HQ_HUB(config)#username vpnuser password 0 vpnuser123
```
2. Evita che il traffico specifico venga indicato.
```
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
```
   Aggiungere gli ACL seguenti alla mappa dei percorsi esistente **non in corrispondenza**:
```
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
```
   Si noti che la comunicazione nat tra i tunnel VPN è esentata in questo esempio.
3. Consente la comunicazione tra i tunnel L2L esistenti e gli utenti VPN ad accesso remoto.
```
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
```
   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. **Configurazione del tunneling ripartito**Per abilitare il tunneling suddiviso per le connessioni VPN, verificare di aver configurato un ACL sul router. Nell'esempio, il comando **access-list split_tunnel** viene associato al gruppo per lo split-tunneling e il tunnel viene formato sulle reti 10.10.10.0 /24 e 10.20.20.0/24 e 172.16.1.0/24. Il traffico viene trasmesso in modo non crittografato ai dispositivi non inclusi nel tunnel suddiviso dall'ACL (ad esempio, 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. Configurare le informazioni di autenticazione, autorizzazione e configurazione client locali, ad

esempio wins, dns. interessanti acl del traffico e pool ip, per i client VPN.

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor 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. Configurare la mappa dinamica e le informazioni della mappa crittografica necessarie per la creazione del tunnel 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 groupauthor
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
```

Esempio di configurazione

Esempio di configurazione 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#
```

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**: questo comando consente di avviare il tunnel VPN L2L, come mostrato.

Risoluzione dei problemi

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

- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug

Suggerimento: quando si cancellano le associazioni di sicurezza e questa operazione non risolve un problema della VPN IPsec, rimuovere e riapplicare la mappa crittografica appropriata per risolvere una vasta gamma di problemi.

Avviso: se si rimuove una mappa crittografica da un'interfaccia, tutti i tunnel IPSec associati a tale

mappa crittografica verranno eliminati. Attenersi alla procedura seguente con cautela e considerare i criteri di controllo delle modifiche dell'organizzazione prima di procedere.

Esempio

```
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
```

Informazioni correlate

- Introduzione alla crittografia IP Security (IPSec)
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE
- Configurazione di un router IPsec come peer LAN-to-LAN dinamico e client VPN
- Documentazione e supporto tecnico – Cisco Systems