IOS-VPN(Router): Hinzufügen eines neuen L2L-Tunnels oder Remote-Zugriffs zu einem vorhandenen L2L-VPN

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Netzwerkdiagramm
Hintergrundinformationen
Hinzufügen eines zusätzlichen L2L-Tunnels zur Konfiguration
Schrittweise Anleitung
Beispielkonfiguration
Hinzufügen eines Remote Access VPN zur Konfiguration
Schrittweise Anleitung
Beispielkonfiguration
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Dieses Dokument enthält die erforderlichen Schritte zum Hinzufügen eines neuen L2L-VPN-Tunnels oder eines Remote-Access-VPN zu einer L2L-VPN-Konfiguration, die bereits in einem IOS-Router vorhanden ist.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie den derzeit betriebsbereiten L2L IPSec VPN-Tunnel korrekt konfigurieren, bevor Sie diese Konfiguration versuchen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Zwei IOS-Router, die die Softwareversionen 12.4 und 12.2 ausführen
- Eine Cisco Adaptive Security Appliance (ASA) mit Softwareversion 8.0

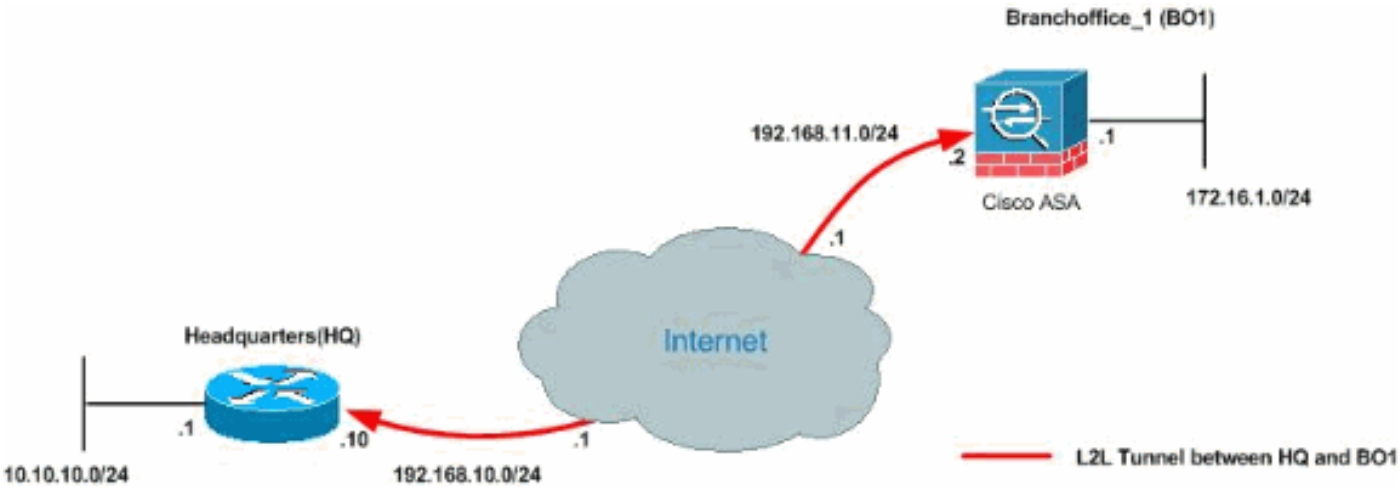
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Diese Ausgänge sind die aktuellen Konfigurationen des HUB-Routers (HQ) und der ASA für Zweigstellen 1 (BO1). In dieser Konfiguration ist ein IPSec-L2L-Tunnel zwischen Hauptsitz und BO1 ASA konfiguriert.

Konfiguration des aktuellen HUB-Routers (HQ)

```
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#
```

BO1 ASA-Konfiguration

```
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
```

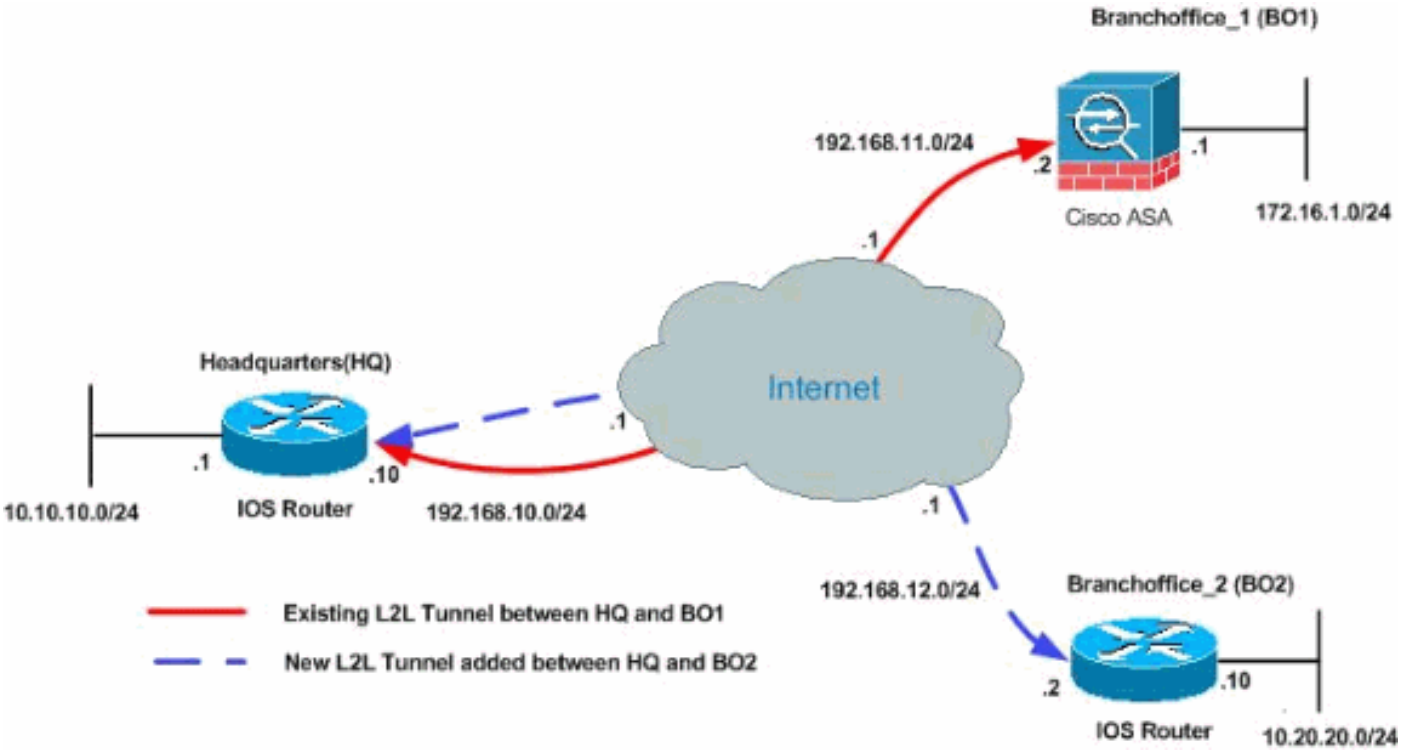
```
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map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

Hintergrundinformationen

Derzeit ist ein L2L-Tunnel zwischen dem Hauptsitz und der BO1-Niederlassung eingerichtet. Ihr Unternehmen hat vor kurzem eine neue Zweigstelle (BO2) eröffnet. Dieses neue Büro benötigt Verbindungen zu lokalen Ressourcen, die sich im Hauptsitz befinden. Darüber hinaus besteht eine zusätzliche Anforderung, dass Mitarbeiter von zu Hause aus arbeiten und sicher auf Ressourcen zugreifen können, die sich im internen Netzwerk befinden. In diesem Beispiel wird ein neuer VPN-Tunnel sowie ein VPN-Server für Remote-Zugriff konfiguriert, der sich im Hauptsitz befindet.

Hinzufügen eines zusätzlichen L2L-Tunnels zur Konfiguration

Dies ist das Netzwerkdiagramm für diese Konfiguration:



Schrittweise Anleitung

Dieser Abschnitt enthält die erforderlichen Verfahren, die auf dem HUB-HQ-Router ausgeführt werden müssen.

Gehen Sie wie folgt vor:

1. Erstellen Sie diese neue Zugriffsliste, die von der Crypto Map verwendet wird, um interessanten Datenverkehr zu definieren:
   ```
   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
   ```

   Warnung: Damit die Kommunikation stattfinden kann, muss auf der anderen Seite des Tunnels das Gegenteil des ACL-Eintrags (Access Control List) für das jeweilige Netzwerk vorhanden sein.
2. Fügen Sie diese Einträge der no nat-Anweisung hinzu, um die Verschachtelung zwischen diesen Netzwerken auszunehmen:
   ```
   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
   ```

   Fügen Sie diese ACLs der vorhandenen Routenzuordnung **nonat** hinzu:
   ```
   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
   ```

   Warnung: Damit die Kommunikation stattfinden kann, muss die andere Seite des Tunnels das Gegenteil dieses ACL-Eintrags für das jeweilige Netzwerk aufweisen.
3. Geben Sie die Peer-Adresse in der Phase 1-Konfiguration wie folgt an:
   ```
   HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
   ```

Hinweis: Der vorinstallierte Schlüssel muss auf beiden Seiten des Tunnels genau übereinstimmen.

4. Erstellen Sie die Konfiguration der Crypto Map für den neuen VPN-Tunnel. Verwenden Sie den gleichen Transformationssatz, der in der ersten VPN-Konfiguration verwendet wurde, da alle Einstellungen in Phase 2 identisch sind.

```
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. Nachdem Sie den neuen Tunnel konfiguriert haben, müssen Sie interessanten Datenverkehr über den Tunnel senden, um ihn aufzunehmen. Führen Sie hierzu den Befehl extended **ping aus,** um einen Host im internen Netzwerk des Remote-Tunnels anzupingen.In diesem Beispiel wird eine Workstation auf der anderen Seite des Tunnels mit der Adresse 10.20.20.16 angepingt. Dadurch wird der Tunnel zwischen Hauptsitz und BO2 hergestellt. Nun sind zwei Tunnel mit dem Hauptsitz verbunden. Wenn Sie keinen Zugriff auf ein System hinter dem Tunnel haben, finden Sie unter Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung, um eine alternative Lösung mit `Managementzugriff` zu finden.

Beispielkonfiguration

HUB_HQ - Neue L2L-VPN-Tunnelkonfiguration hinzugefügt

```
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#
```

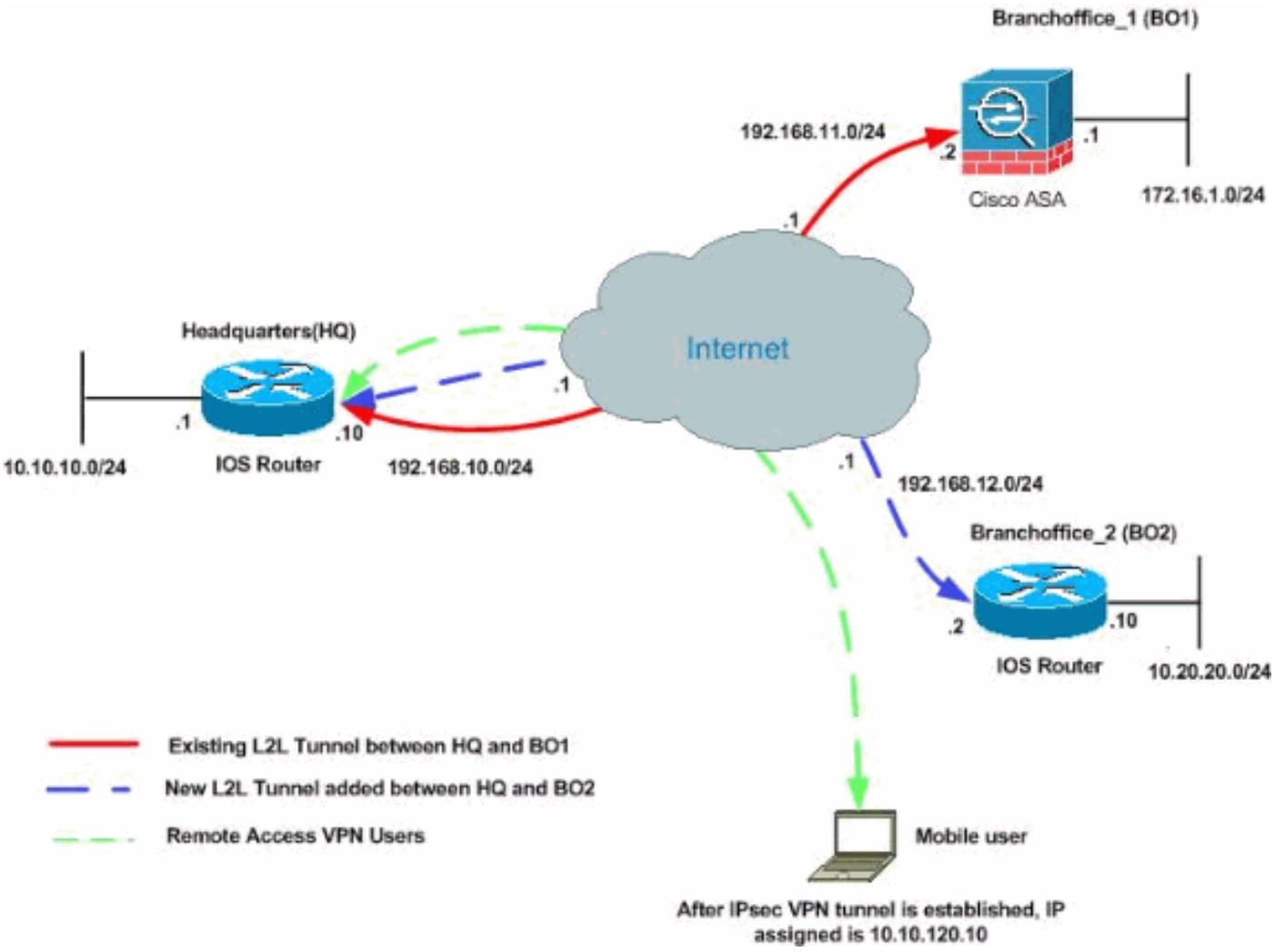
BO2 L2L VPN-Tunnelkonfiguration

```
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#
```

Hinzufügen eines Remote Access VPN zur Konfiguration

Dies ist das Netzwerkdiagramm für diese Konfiguration:



In diesem Beispiel wird die Funktion **Split-Tunneling** verwendet. Diese Funktion ermöglicht einem IPSec-Client mit Remote-Zugriff die bedingte Weiterleitung von Paketen über einen IPSec-Tunnel

in verschlüsselter Form oder in Klartextform an eine Netzwerkschnittstelle. Bei aktiviertem Split-Tunneling müssen Pakete, die nicht an Ziele auf der anderen Seite des IPSec-Tunnels gebunden sind, nicht verschlüsselt, über den Tunnel gesendet, entschlüsselt und dann an ein endgültiges Ziel geroutet werden. Dieses Konzept wendet die Split-Tunneling-Richtlinie auf ein bestimmtes Netzwerk an. Standardmäßig wird der gesamte Datenverkehr durch Tunnel weitergeleitet. Um eine Split-Tunneling-Richtlinie festzulegen, geben Sie eine ACL an, in der der für das Internet bestimmte Datenverkehr angegeben werden kann.

Schrittweise Anleitung

Dieser Abschnitt enthält die erforderlichen Verfahren zum Hinzufügen von Remote-Zugriffsfunktionen und zum Zugriff auf alle Standorte durch Remote-Benutzer.

Gehen Sie wie folgt vor:

1. Erstellen Sie einen IP-Adresspool, der für Clients verwendet wird, die über den VPN-Tunnel eine Verbindung herstellen. Erstellen Sie außerdem einen einfachen Benutzer, um nach Abschluss der Konfiguration auf das VPN zuzugreifen.
   ```
   HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50


   HQ_HUB(config)#username vpnuser password 0 vpnuser123
   ```
2. Verhindern Sie, dass bestimmter Datenverkehr vernetzt wird.
   ```
   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
   ```

   Fügen Sie diese ACLs der vorhandenen Routenzuordnung **nonat** hinzu:
   ```
   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
   ```

   Beachten Sie, dass die NAT-Kommunikation zwischen VPN-Tunneln in diesem Beispiel ausgenommen ist.
3. Ermöglicht die Kommunikation zwischen den vorhandenen L2L-Tunneln und VPN-Benutzern mit Remotezugriff.
   ```
   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
   ```

   So können Remote-Benutzer hinter den angegebenen Tunneln mit Netzwerken kommunizieren.**Warnung:** Damit die Kommunikation stattfinden kann, muss die andere Seite des Tunnels das Gegenteil dieses ACL-Eintrags für das jeweilige Netzwerk aufweisen.
4. **Split-Tunneling konfigurieren**Um Split-Tunneling für die VPN-Verbindungen zu aktivieren, müssen Sie eine ACL auf dem Router konfigurieren. In diesem Beispiel ist der Befehl **access-list split_tunnel** für Split-Tunneling der Gruppe zugeordnet, und der Tunnel wird zu

den Netzwerken 10.10.10.0/24 und 10.20.20.0/24 und 172.16.1.0/24 gebildet. Der Datenverkehr fließt unverschlüsselt zu Geräten, die sich nicht im ACL Split Tunnel befinden (z. B. das 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. Konfigurieren Sie lokale Authentifizierungs-, Autorisierungs- und Client-Konfigurationsinformationen wie WinIns, DNS. interessanter Datenverkehr-ACL und IP-Pool für die VPN-Clients.

```
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. Konfigurieren Sie die dynamische Zuordnung und Cryto Map-Informationen, die für die Erstellung des VPN-Tunnels erforderlich sind.

```
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
```

Beispielkonfiguration

Beispielkonfiguration 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#
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **ping** - Mit diesem Befehl können Sie den L2L-VPN-Tunnel wie gezeigt initiieren.

Fehlerbehebung

In diesen Dokumenten finden Sie Informationen, die Sie zur Fehlerbehebung in Ihrer Konfiguration verwenden können:

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- IP Security Troubleshooting - Understanding and Using debug Commands

Tipp: Wenn Sie Sicherheitszuordnungen löschen und kein IPsec-VPN-Problem behoben wird, entfernen und wenden Sie die entsprechende Crypto Map erneut an, um eine Vielzahl von Problemen zu beheben.

Warnung: Wenn Sie eine Crypto Map von einer Schnittstelle entfernen, werden alle mit dieser Crypto Map verknüpften IPSec-Tunnel deaktiviert. Befolgen Sie diese Schritte mit Vorsicht und ziehen Sie die Änderungskontrollrichtlinie Ihres Unternehmens in Betracht, bevor Sie fortfahren.

Beispiel

```
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
```

Zugehörige Informationen

- Eine Einführung in die IP Security (IPSec)-Verschlüsselung
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle
- Konfigurieren eines IPsec-Routers Dynamische LAN-to-LAN-Peer- und VPN-Clients
- Technischer Support und Dokumentation - Cisco Systems