Dynamisches Konfigurationsbeispiel für einen dynamischen IPsec-Tunnel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein LAN-zu-LAN-IPsec-Tunnel zwischen Cisco-Routern erstellt wird, wenn beide Enden über dynamische IP-Adressen verfügen, das Dynamic Domain Name System (DDNS) jedoch konfiguriert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Site-to-Site-VPN mit IPSec-Tunnel und Generic Routing Encapsulation (GRE)
- IPsec Virtual Tunnel Interface (VTI)
- Dynamische DNS-Unterstützung für Cisco IOS Software

Tipp: Weitere Informationen finden Sie im Abschnitt Konfigurieren von VPN im Software-Konfigurationsleitfaden für die Cisco Serien 3900, 2900 und 1900 und im Artikel Konfigurieren einer Virtual Tunnel Interface mit IP Security.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco 2911 Integrated Services Router, auf dem Version 15.2(4)M6a ausgeführt wird.

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.

Hintergrundinformationen

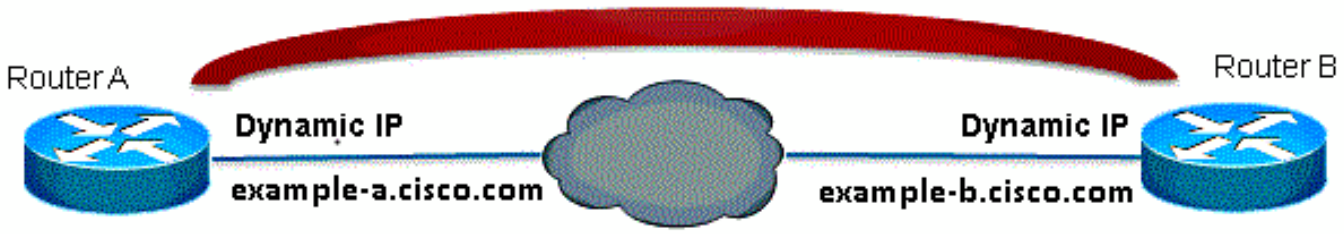
Wenn ein LAN-zu-LAN-Tunnel erstellt werden muss, muss die IP-Adresse beider IPSec-Peers bekannt sein. Wenn eine der IP-Adressen nicht bekannt ist, weil sie dynamisch ist (z. B. über DHCP bezogen), besteht die Alternative darin, eine dynamische Crypto Map zu verwenden. Dies funktioniert, aber der Tunnel kann nur vom Peer mit der dynamischen IP-Adresse aufgerufen werden, da der andere Peer nicht weiß, wo er seinen Peer findet.

Weitere Informationen zu dynamisch zu statisch finden Sie unter Konfigurieren von Dynamic-to-Static IPSec zwischen Router und Router mit NAT.

Konfigurieren

Echtzeit-Auflösung für Peer-Verbindungen im IPsec-Tunnel

Cisco IOS® hat in Version 12.3(4)T eine neue Funktion eingeführt, mit der der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) des IPSec-Peers angegeben werden kann. Wenn ein Datenverkehr einer Crypto Access List entspricht, löst Cisco IOS den FQDN auf und ruft die IP-Adresse des Peers ab. Dann versucht es, den Tunnel hochzufahren.



> **Hinweis**: Diese Funktion ist beschränkt: DNS-Namensauflösung für Remote-IPsec-Peers funktioniert nur, wenn sie als Initiator verwendet werden. Das erste zu verschlüsselnde Paket löst eine DNS-Suche aus. Nachdem die DNS-Suche abgeschlossen ist, lösen nachfolgende Pakete Internet Key Exchange (IKE) aus. Die Problemlösung in Echtzeit funktioniert nicht.

Um die Einschränkung zu umgehen und den Tunnel von jedem Standort aus initiieren zu können, verfügen Sie auf beiden Routern über einen dynamischen Crypto Map-Eintrag, sodass Sie eingehende IKE-Verbindungen der dynamischen Krypto-Verbindung zuordnen können. Dies ist erforderlich, da der statische Eintrag mit der Funktion zur Echtzeit-Auflösung nicht funktioniert, wenn er als Responder fungiert.

Router A

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-b.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Router B

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
```

```
permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-a.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Hinweis: Da Sie nicht wissen, welche IP-Adresse der FQDN verwendet, müssen Sie einen Platzhalter-Pre-Shared-Key verwenden: 0,0 0,0 0,0

Tunnel-Ziel-Update mit Embedded Event Manager (EEM)

Dazu können Sie auch VTI verwenden. Die grundlegende Konfiguration wird hier angezeigt:

Router A

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-b.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Router B

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
```

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-a.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Sobald die vorherige Konfiguration mit einem FQDN als Tunnelziel vorhanden ist, zeigt der Befehl **show run** die IP-Adresse anstelle des Namens an. Dies liegt daran, dass die Entschließung nur einmal geschieht:

```
RouterA(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.201.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end

RouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

Eine Problemumgehung hierfür besteht darin, ein Applet zu konfigurieren, um das Tunnelziel jede Minute aufzulösen:

Router A

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
action 1.0 cli command "enable"
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-b.cisco.com"
```

Router B

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
```

```
action 1.0 cli command "enable"
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-a.cisco.com"
```

Überprüfen

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

```
RouterA(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.200.225 YES NVRAM up up
FastEthernet0/1 192.168.10.1 YES NVRAM up up
Tunnel1 172.16.12.1 YES manual up up


RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.201.1 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up

RouterA(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 2 0 ACTIVE

RouterB(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 1002 0 ACTIVE

RouterA(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.200.225

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.201.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.200.225, remote crypto endpt.: 209.165.201.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x8F1592D2(2400555730)

inbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4501866/3033)
```

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: AIM-VPN/BPII-PLUS:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4501866/3032)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

```
RouterB(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.201.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.200.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.201.1, remote crypto endpt.: 209.165.200.225
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF7B373C0(4155732928)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Nachdem Sie den DNS-Eintrag für b.cisco.com auf dem DNS-Server von 209.165.201.1 auf 209.165.202.129 geändert haben, veranlasst EEM die Aktivierung von Router A und der Tunnel wird mit der richtigen neuen IP-Adresse wiederhergestellt.

```
RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.202.129 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up
```

```
RouterA(config-if)#do show run int tunn1
Building configuration...

Current configuration : 192 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.252
tunnel source fastethernet0/0
tunnel destination 209.165.202.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end

Router1841A#show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.202.129 QM_IDLE 3 0 ACTIVE
```

Fehlerbehebung

Sie können IOS IPSec- und IKE-Debug - IKEv1 Main Mode Troubleshooting für eine gängige IKE/IPsec-Fehlerbehebung nutzen.

Zugehörige Informationen

- Echtzeit-Auflösung für Peer-Verbindungen im IPsec-Tunnel
- Technischer Support und Dokumentation - Cisco Systems