PIX/ASA 7.X: Hinzufügen eines neuen Tunnels oder Remote-Zugriffs zu einem vorhandenen L2L-VPN

Inhalt

Einführung

Dieses Dokument enthält die erforderlichen Schritte zum Hinzufügen eines neuen VPN-Tunnels oder eines Remote-Access-VPN zu einer bereits vorhandenen L2L-VPN-Konfiguration. Weitere Informationen zum Erstellen der ersten IPSec VPN-Tunnel und weitere Konfigurationsbeispiele finden Sie unter Cisco Adaptive Security Appliances der Serie ASA 5500 - Konfigurationsbeispiele und technische Hinweise.

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 basierend auf folgenden Software- und Hardware-Versionen:

- Zwei ASA Security Appliances mit 7.x-Code
- Eine PIX-Sicherheits-Appliance mit 7.x-Code

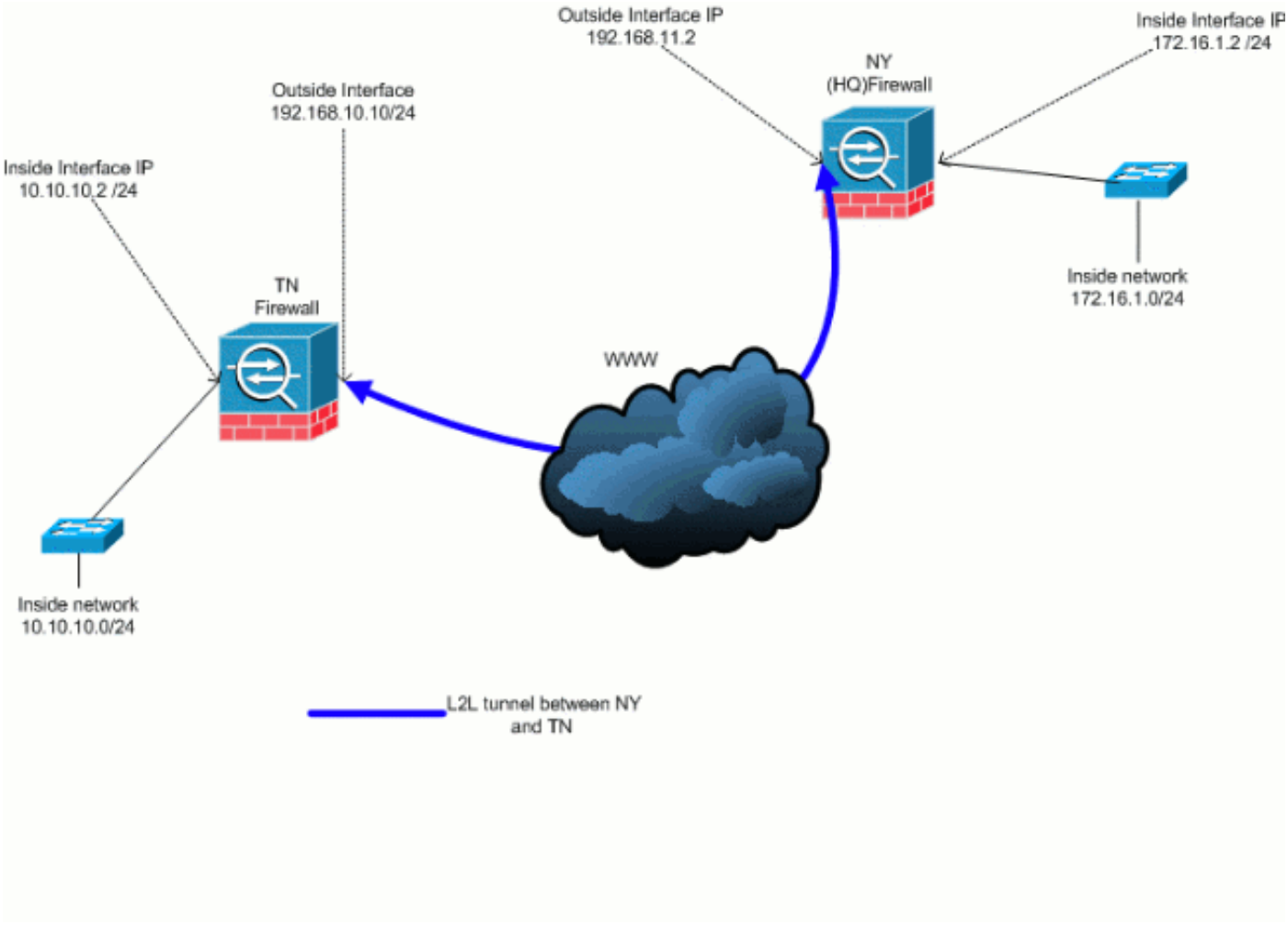
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Diese Ausgabe ist die aktuelle Konfiguration der NY (HUB) Security Appliance. In dieser Konfiguration ist ein IPSec-L2L-Tunnel zwischen NY(HQ) und TN konfiguriert.

Aktuelle Firewall-Konfiguration für NY (HQ)

```
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#
```

Hintergrundinformationen

Derzeit ist ein L2L-Tunnel zwischen der NY(HQ)-Niederlassung und der TN-Niederlassung eingerichtet. Ihr Unternehmen hat vor kurzem eine neue Niederlassung in TX eröffnet. Dieses neue Büro benötigt Verbindungen zu lokalen Ressourcen, die sich in den Zweigstellen in New York und TN 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 den Remote-Zugriff konfiguriert, der sich in der NY-Niederlassung befindet.

In diesem Beispiel werden zwei Befehle verwendet, um die Kommunikation zwischen den VPN-Netzwerken zu ermöglichen und den Datenverkehr zu identifizieren, der getunnelt oder verschlüsselt werden soll. So haben Sie Zugriff auf das Internet, ohne diesen Datenverkehr über den VPN-Tunnel senden zu müssen. Um diese beiden Optionen zu konfigurieren, müssen Sie die Befehle **für Split-Tunnel** und **gleichen Sicherheitsdatenverkehr** ausführen.

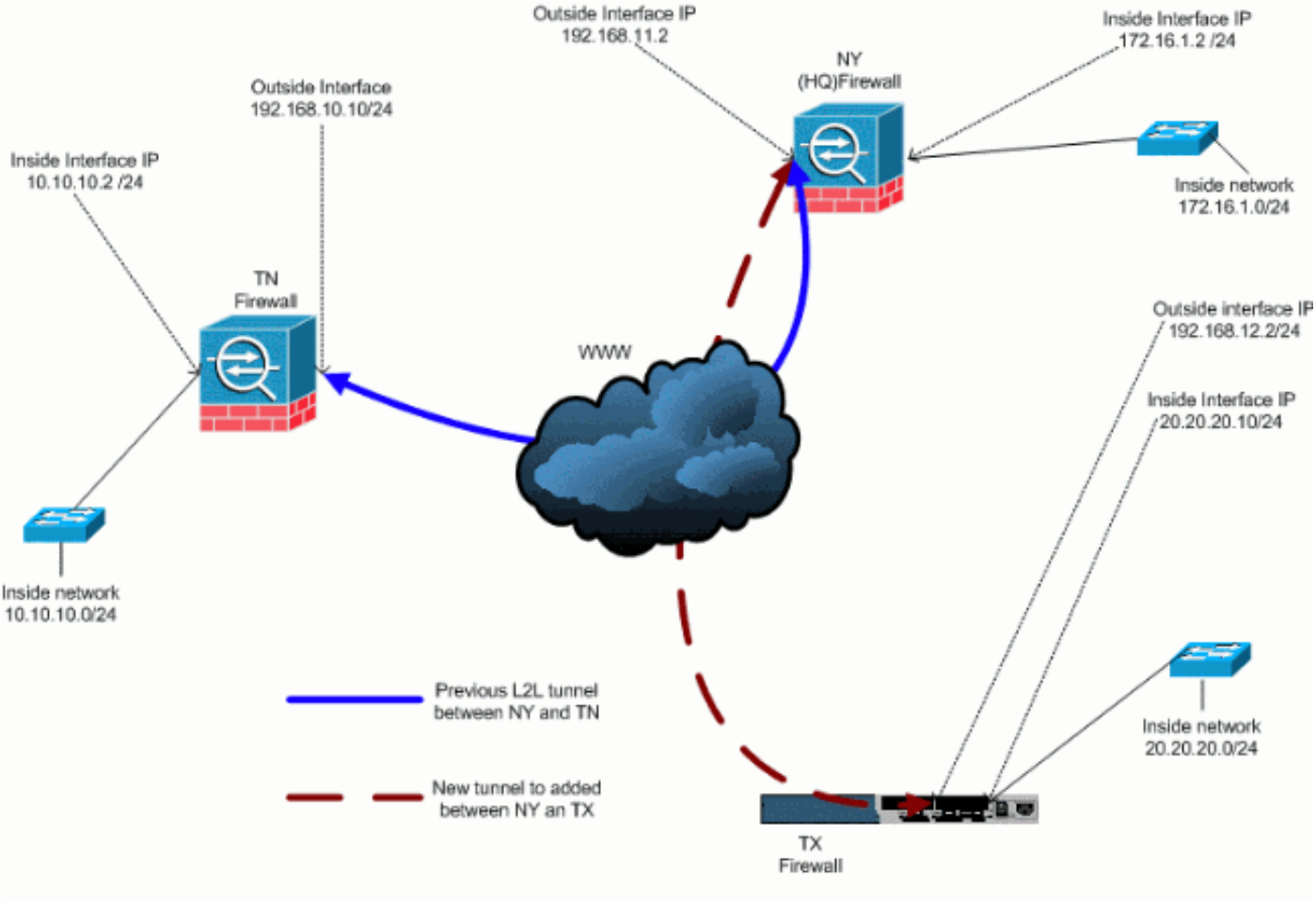
Split-Tunneling ermöglicht einem IPSec-Client mit Remote-Zugriff die bedingte Weiterleitung von Paketen über einen IPSec-Tunnel in verschlüsselter Form oder in Klartextform an eine Netzwerkschnittstelle. Bei aktiviertem Split-Tunneling müssen Pakete, die nicht an Ziele auf der anderen Seite des IPSec-Tunnels gebunden sind, nicht verschlüsselt, über den Tunnel gesendet, entschlüsselt und dann an ein endgültiges Ziel geroutet werden. Dieser Befehl wendet diese Split-Tunneling-Richtlinie auf ein angegebenes Netzwerk an. Standardmäßig wird der gesamte Datenverkehr durch Tunnel weitergeleitet. Führen Sie zum Festlegen einer Split-Tunneling-Richtlinie den Befehl **split-tunnel-policy** im Konfigurationsmodus für Gruppenrichtlinien aus. Um die Split-Tunneling-Richtlinie aus der Konfiguration zu entfernen, geben Sie die **no-**Form dieses Befehls ein.

Die Sicherheits-Appliance umfasst eine Funktion, die es einem VPN-Client ermöglicht, IPSec-geschützten Datenverkehr an andere VPN-Benutzer zu senden, indem dieser ein- und ausgehende Datenverkehr über dieselbe Schnittstelle zugelassen wird. Diese Funktion wird auch als Hairpinning bezeichnet und kann als VPN-Spokes (Clients) bezeichnet werden, die über einen VPN-Hub (Security Appliance) verbunden sind. In einer anderen Anwendung kann diese Funktion eingehenden VPN-Datenverkehr über dieselbe Schnittstelle wie unverschlüsselten Datenverkehr umleiten. Dies ist beispielsweise für einen VPN-Client nützlich, der über kein Split-Tunneling verfügt, aber sowohl auf ein VPN zugreifen als auch im Internet surfen muss. Führen Sie zum

Konfigurieren dieser Funktion im **globalen Konfigurationsmodus** den **Befehl *Intra-Interface* (Datenverkehr *innerhalb der Schnittstelle*) für den gleichen Sicherheitsdatenverkehr aus**.

Hinzufügen eines zusätzlichen L2L-Tunnels zur Konfiguration

Dies ist das Netzwerkdiagramm für diese Konfiguration:



Schritt-für-Schritt-Anleitung

Dieser Abschnitt enthält die erforderlichen Verfahren, die auf der HUB-Sicherheits-Appliance (NY Firewall) durchgeführt werden müssen. Weitere Informationen finden Sie unter PIX/ASA 7.x: Einfaches PIX-zu-PIX VPN-Tunnel-Konfigurationsbeispiel für weitere Informationen zum Konfigurieren des Spoke-Clients (TX-Firewall).

Führen Sie diese Schritte aus:

1. Erstellen Sie diese beiden neuen Zugriffslisten, die von der Crypto Map verwendet werden, um interessanten Datenverkehr zu definieren:

```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0


ASA-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
```

   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:

```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0

ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0

ASA-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
```

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 diesen Befehl ein, um einem Host im TX-VPN-Netzwerk den Zugriff auf den TN-VPN-Tunnel zu ermöglichen:

```
ASA-NY-HQ(config)#same-security-traffic permit
 intra-interface
```

Dadurch können VPN-Peers miteinander kommunizieren.

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.

```
ASA-NY-HQ(config)#crypto map outside_map 30 match
 address outside_30_cryptomap

ASA-NY-HQ(config)#crypto map outside_map 30 set
 peer 192.168.12.2

ASA-NY-HQ(config)#crypto map outside_map 30 set
 transform-set
 ESP-3DES-SHA
```

5. Erstellen Sie die Tunnelgruppe, die für diesen Tunnel angegeben ist, zusammen mit den für die Verbindung mit dem Remotehost erforderlichen Attributen.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
 ipsec-l2l

ASA-NY-HQ(config)#tunnel-group 192.168.12.2
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco123
```

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

6. Nachdem Sie den neuen Tunnel konfiguriert haben, müssen Sie interessanten Datenverkehr über den Tunnel senden, um ihn aufzunehmen. Führen Sie dazu den Befehl **source 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 20.20.20.16 angepingt. Dadurch wird der Tunnel zwischen NY und TX erstellt. Nun sind zwei Tunnel mit dem Hauptsitz verbunden. Wenn Sie keinen Zugriff auf ein System hinter dem Tunnel haben, finden Sie unter Häufigste IPSec VPN-Problemlösung eine alternative Lösung in Bezug auf die Verwendung von `Managementzugriff`.

Beispielkonfiguration

Beispielkonfiguration 1

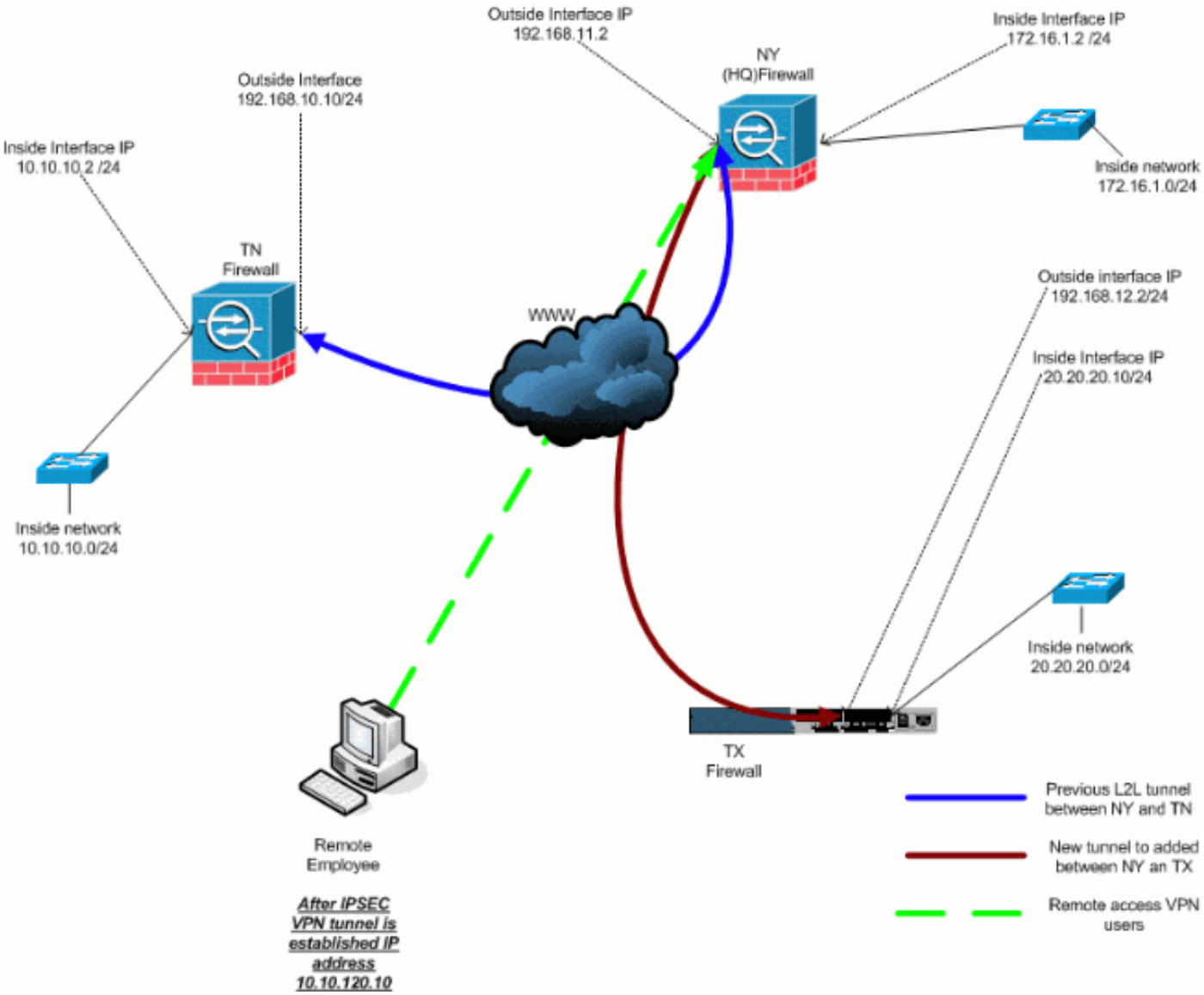
```
ASA-NY-HQ#show running-config

 : 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#
```

Hinzufügen eines Remote Access VPN zur Konfiguration

Dies ist das Netzwerkdiagramm für diese Konfiguration:



Schritt-für-Schritt-Anleitung

Dieser Abschnitt enthält die erforderlichen Verfahren zum Hinzufügen von Remote-Zugriffsfunktionen und zum Zugriff auf alle Standorte durch Remote-Benutzer. Weitere Informationen finden Sie unter PIX/ASA 7.x ASDM: Beschränken Sie den Netzwerkzugriff von VPN-Benutzern mit Remote-Zugriff, um weitere Informationen zur Konfiguration des Remote-Zugriffsservers und zur Einschränkung des Zugriffs zu erhalten.

Führen Sie diese Schritte aus:

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.

```
ASA-NY-HQ(config)#ip local pool Hill-V-IP
 10.10.120.10-10.10.120.100 mask 255.255.255.0


ASA-NY-HQ(config)#username cisco password
 cisco111
```

2. Verhindern Sie, dass bestimmter Datenverkehr vernetzt wird.

```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 172.16.1.0
    255.255.255.0 10.10.120.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-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
```

Beachten Sie, dass die NAT-Kommunikation zwischen VPN-Tunneln in diesem Beispiel ausgenommen ist.

3. Erlauben Sie die Kommunikation zwischen den bereits erstellten L2L-Tunneln.

```
ASA-NY-HQ(config)#access-list
 outside_20_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-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
```

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. Konfigurieren Sie den Datenverkehr, der verschlüsselt und über den VPN-Tunnel gesendet wird.

```
ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 172.16.1.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 10.10.10.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 20.20.20.0
    255.255.255.0
```

5. Konfigurieren Sie lokale Authentifizierungs- und Richtlinieninformationen wie Win-, DNS- und IPSec-Protokolle für die VPN-Clients.

```
ASA-NY-HQ(config)#group-policy Hillvalley
 internal

ASA-NY-HQ(config)#group-policy Hillvalley
 attributes

ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20

ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20

ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. Legen Sie IPSec und allgemeine Attribute fest, z. B. vorinstallierte Schlüssel und IP-Adresspools, die vom VPN-Tunnel in Hillvalley verwendet werden.

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
```

```
cisco1234

ASA-NY-HQ(config)#tunnel-group Hillvalley
 general-attributes

ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP

ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. Erstellen Sie die Split-Tunnel-Richtlinie, die die in Schritt 4 erstellte ACL verwendet, um anzugeben, welcher Datenverkehr verschlüsselt und durch den Tunnel geleitet wird.

```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecified

ASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```

8. Konfigurieren Sie die erforderlichen Cryto Map-Informationen für die Erstellung des VPN-Tunnels.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
 Hill-trans esp-3des esp-sha-hmac

ASA-NY-HQ(config)#crypto dynamic-map
 outside_dyn_map 20 set transform-set
 Hill-trans

ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
 set reverse-route

ASA-NY-HQ(config)#crypto map outside_map 65535
 ipsec-isakmp dynamic
 outside_dyn_map
```

Beispielkonfiguration

Beispielkonfiguration 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#
```

Überprüfung

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 inside x.x.x.x (IP-Adresse des Hosts auf der gegenüberliegenden Seite des Tunnels)** - Mit diesem Befehl können Sie Datenverkehr im Tunnel unter Verwendung einer Quelladresse der internen Schnittstelle senden.

Fehlerbehebung

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

- Häufigste IPSec VPN-Fehlerbehebungslösungen
- IP Security Troubleshooting - Understanding and Using debug Commands
- Fehlerbehebung bei Verbindungen über PIX und ASA

Zugehörige Informationen

- Eine Einführung in die IP Security (IPSec)-Verschlüsselung
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Befehlsreferenzen
- Technischer Support und Dokumentation für Cisco Systeme