Konfigurieren eines IPSec-Tunnels zwischen Routern mit doppelten LAN-Subnetzen

Inhalt

Einführung

Dieses Dokument enthält ein Netzwerkbeispiel, das zwei sich verschmelzende Unternehmen mit demselben IP-Adressierungsschema simuliert. Zwei Router sind mit einem VPN-Tunnel verbunden, und die Netzwerke hinter jedem Router sind identisch. Damit ein Standort auf Hosts am anderen Standort zugreifen kann, wird auf den Routern Network Address Translation (NAT) verwendet, um sowohl die Quell- als auch die Zieladresse in verschiedene Subnetze zu ändern.

Hinweis: Diese Konfiguration wird nicht als permanente Konfiguration empfohlen, da sie aus Sicht der Netzwerkverwaltung verwirrend wäre.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Router A: Cisco Router 3640 mit Cisco IOS® Software, Version 12.3(4)T

- Router B: Cisco 2621 Router mit Cisco IOS® Software Release 12.3(5)

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 unter Cisco Technical Tips Conventions.

Hintergrundinformationen

Wenn in diesem Beispiel Host 172.16.1.2 an Standort A auf denselben IP-adressierten Host an Standort B zugreift, stellt er eine Verbindung mit einer Adresse 172.19.1.2 her und nicht mit der tatsächlichen Adresse 172.16.1.2. Wenn der Host an Standort B auf Standort A zugreift, wird eine Verbindung zu einer Adresse des Standards 172.18.1.2 hergestellt. NAT auf Router A übersetzt alle 172.16.x.x-Adressen so, dass sie dem entsprechenden Host-Eintrag 172.18.x.x entsprechen. NAT auf Router B ändert 172.16.x.x so, dass es wie 172.19.x.x aussieht.

Die Crypto-Funktion auf jedem Router verschlüsselt den übersetzten Datenverkehr über die seriellen Schnittstellen. Beachten Sie, dass die NAT *vor* der Verschlüsselung auf einem Router erfolgt.

Hinweis: Diese Konfiguration ermöglicht nur die Kommunikation zwischen den beiden Netzwerken. Es ermöglicht keine Internetverbindung. Sie benötigen zusätzliche Pfade zum Internet, um Verbindungen zu anderen Standorten als den beiden Standorten herzustellen. Anders ausgedrückt: Sie müssen auf jeder Seite einen anderen Router oder eine Firewall hinzufügen, wobei auf den Hosts mehrere Routen konfiguriert sind.

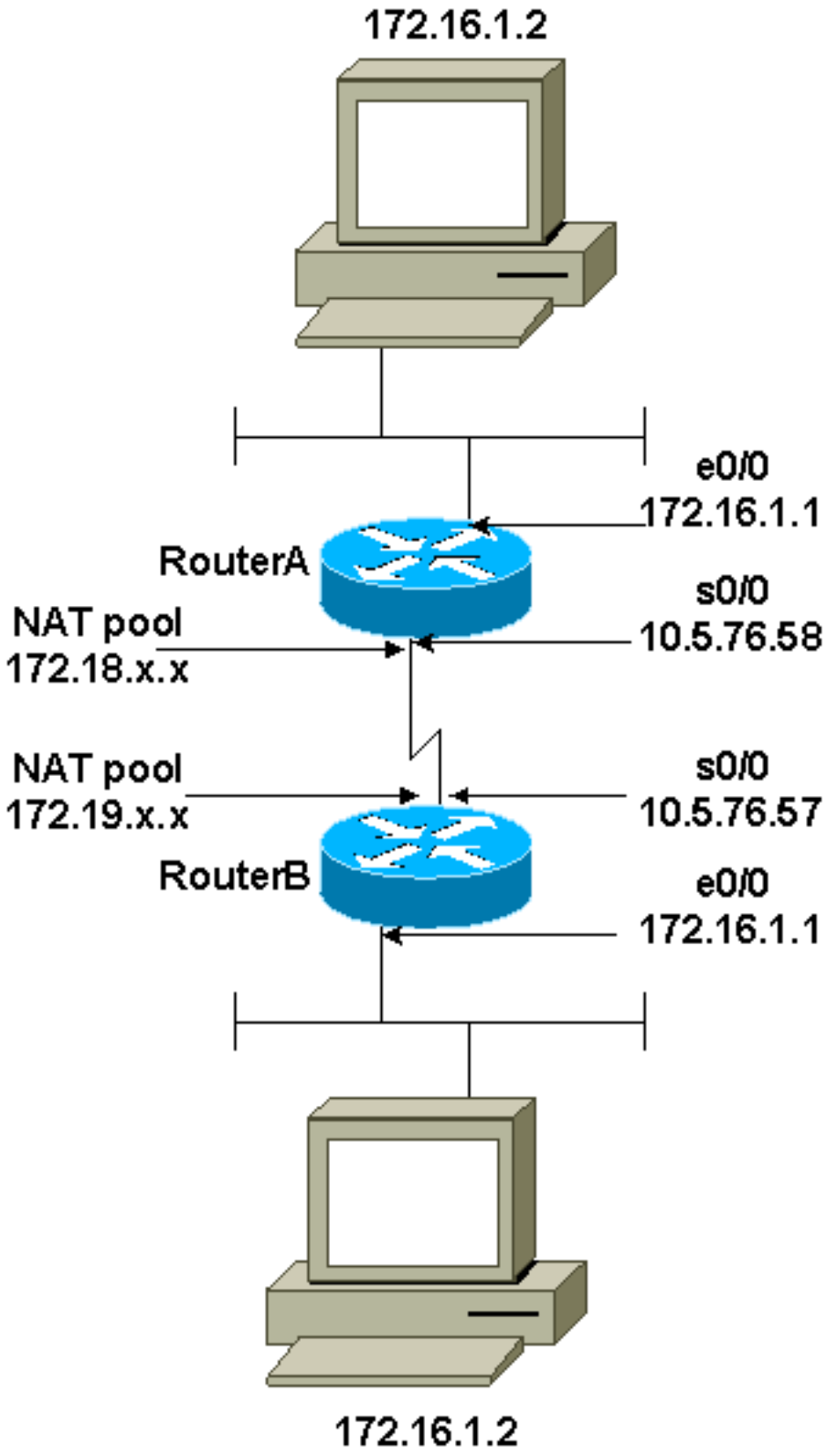
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Router A
- Router B

Router A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.57
 set transform-set myset1
  !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
 description Interface to Internet
 ip address 10.5.76.58 255.255.0.0
 ip nat outside
 clockrate 128000
 crypto map mymap
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Router B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.58
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.58
 set transform-set myset1
!--- Encrypt traffic to the other side.  match address
100
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 description Interface to Internet
```

```
 ip address 10.5.76.57 255.255.0.0
 ip nat outside
 crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
end
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.
- **show ip nat translation** - Zeigt die aktuell verwendeten NAT-Übersetzungen an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug crypto ipsec** - Zeigt die IPSec-Verhandlungen von Phase 2.
- **debug crypto isakmp** - Zeigt die Verhandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) für Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.

Zugehörige Informationen

- IPSec-Support-Seite
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support - Cisco Systems