Konfigurieren von IPSec Router-to-Router, vorinstallierter NAT-Overload zwischen einem privaten und einem öffentlichen Netzwerk

Inhalt

Einführung

Diese Beispielkonfiguration zeigt, wie der Datenverkehr zwischen einem privaten Netzwerk (10.103.1.x) und einem öffentlichen Netzwerk (98.98.98.x) mithilfe von IPSec verschlüsselt wird. Das Netzwerk 98.98.98.x kennt das Netzwerk 10.103.1.x von den privaten Adressen. Das Netzwerk 10.103.1.x kennt das Netzwerk 98.98.98.x durch die öffentlichen Adressen.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert ein grundlegendes Verständnis des IPSec-Protokolls. Weitere Informationen zu IPSec finden Sie unter Einführung in die IP-Sicherheit (IPSec)-Verschlüsselung.

Verwendete Komponenten

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

- Cisco IOS® Softwareversion 12.3(5)
- Cisco Router der Serie 3640

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.

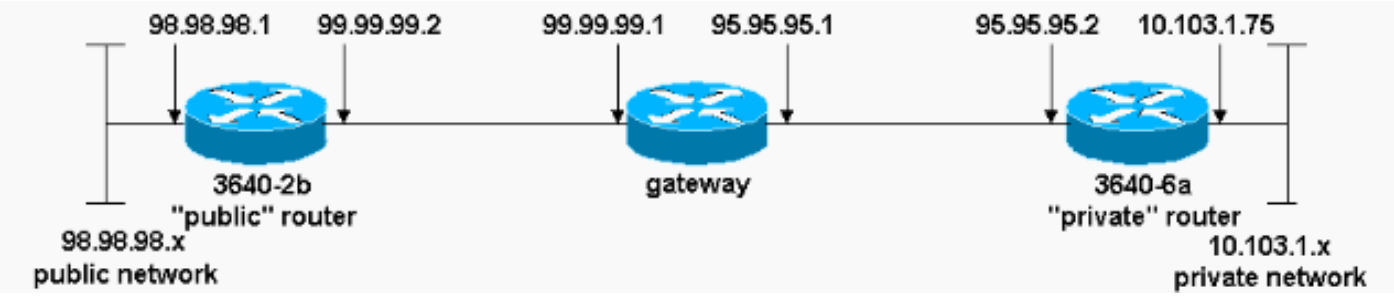
Konfigurieren

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 in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- 3640-2b "Öffentlicher" Router
- "Privater" Router 3640-6a

3640-2b "Öffentlicher" Router

```
rp-3640-2b#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-2b
!
ip subnet-zero
```

```
!

!
!--- Defines the Internet Key Exchange (IKE) policies.
crypto isakmp policy 1

!--- Defines an IKE policy. Use the crypto isakmp policy
!--- command in global configuration mode. IKE policies
!--- define a set of parameters !--- that are used
during the IKE phase I negotiation.


hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 95.95.95.2

!--- Configures a preshared authentication key, used in
!--- global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an acceptable !---
combination of security protocols and algorithms, !---
which has to be matched on the peer router. ! crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to !--- establish the
IPSec security associations (SAs) that protect !--- the
traffic specified by this crypto map entry. set peer
95.95.95.2

!--- Sets the IP address of the remote end. set
transform-set rtpset

!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- This is used to assign an extended access list to a
!--- crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. ! interface Ethernet0/0 ip address
98.98.98.1 255.255.255.0 no ip directed-broadcast !
interface Ethernet0/1
ip address 99.99.99.2 255.255.255.0
no ip directed-broadcast
no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use !--- the crypto map
"rtp" for IPSec. ! . . !--- Output suppressed. . . ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.1

!--- Default route to the next hop address. no ip http
server ! access-list 115 permit ip 98.98.98.0 0.0.0.255
10.103.1.0 0.0.0.255

!--- This access-list option causes all IP traffic !---
that matches the specified conditions to be !---
protected by IPSec using the policy described by !---
```

```
the corresponding crypto map command statements.


access-list 115 deny ip 98.98.98.0 0.0.0.255 any

!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

"Privater" Router 3640-6a

```
rp-3640-6a#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!

!
ip subnet-zero



!--- Defines the IKE policies. ! crypto isakmp policy 1

!--- Defines an IKE policy. !--- Use the crypto isakmp
policy !--- command in global configuration mode. IKE
policies !--- define a set of parameters !--- that are
used during the IKE phase I negotiation.


hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 99.99.99.2

!--- Configures a preshared authentication key, !---
used in global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an !--- acceptable
combination of security protocols and algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to establish !--- the
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. set peer 99.99.99.2

!--- Sets the IP address of the remote end. set
transform-set rtpset
```

```
!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- Used to assign an extended access list to a !---
crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. . . !--- Output suppressed. . . ! interface
Ethernet3/0 ip address 95.95.95.2 255.255.255.0 no ip
directed-broadcast ip nat outside

!--- Indicates that the interface is !--- connected to
the outside network. no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use the !--- crypto map
"rtp" for IPSec. ! interface Ethernet3/2 ip address
10.103.1.75 255.255.255.0 no ip directed-broadcast ip
nat inside

!--- Indicates that the interface is connected to !---
the inside network (the network subject to NAT
translation). ! ip nat pool FE30 95.95.95.10 95.95.95.10
netmask 255.255.255.0

!--- Used to define a pool of IP addresses for !--- NAT.
Use the ip nat pool command in !--- global configuration
mode.


ip nat inside source route-map nonat pool FE30 overload

!--- Used to enable NAT of !--- the inside source
address. Use the ip nat inside source !--- command in
global configuration mode. !--- The 'overload' option
enables the router to use one global !--- address for
many local addresses.


ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1

!--- Default route to the next hop address. no ip http
server ! access-list 110 deny ip 10.103.1.0 0.0.0.255
98.98.98.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any

!--- Addresses that match this ACL are NATed while !---
they access the Internet. They are not NATed !--- if
they access the 98.98.98.0 network. access-list 115
permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255

!--- This access-list option causes all IP traffic that
!--- matches the specified conditions to be !---
protected by IPSec using the policy described !--- by
the corresponding crypto map command statements.


access-list 115 deny ip 10.103.1.0 0.0.0.255 any
```

```
route-map nonat permit 10
match ip address 110
!

!
line con 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.

Um diese Konfiguration zu überprüfen, versuchen Sie einen erweiterten **Ping**-Befehl, der von der Ethernet-Schnittstelle des privaten Routers 10.103.1.75 stammt und für die Ethernet-Schnittstelle des öffentlichen Routers 98.98.98.1 bestimmt ist.

- Ping - Dient zur Diagnose grundlegender Netzwerkverbindungen.

```
rp-3640-6a#ping
Protocol [ip]:
Target IP address: 98.98.98.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.103.1.75
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 98.98.98.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

- show crypto ipsec sa: Zeigt die von aktuellen (IPSec) SAs verwendeten Einstellungen.
- show crypto isakmp sa: **Zeigt alle aktuellen IKE-SAs in einem Peer an.**
- show crypto engine - Zeigt eine Zusammenfassung der Konfigurationsinformationen für die Crypto Engines. Verwenden Sie den Befehl **show crypto engine** im privilegierten EXEC-Modus.

Beispielausgabe

Diese Ausgabe stammt aus dem Befehl **show crypto ipsec sa**, der auf dem Hub-Router ausgegeben wird.

```
rp-3640-6a#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 95.95.95.2

   protected vrf:
   local  ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0)
   current_peer: 99.99.99.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #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.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
     path mtu 1500, media mtu 1500
     current outbound spi: 75B6D4D7

     inbound esp sas:
      spi: 0x71E709E8(1910966760)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4576308/3300)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x75B6D4D7(1974916311)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4576310/3300)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Dieser Befehl zeigt die zwischen Peers erstellten IPSec-SAs. Der verschlüsselte Tunnel wurde zwischen 95.95.95.2 und 99.99.99.2 für Datenverkehr zwischen den Netzwerken 98.98.98.0 und 10.103.1.0 erstellt. Sie sehen die beiden integrierten ESP-SAs (Encapsulating Security Payload) für ein- und ausgehende Anrufe. Authentifizierungs-Header (AH)-SAs werden nicht verwendet, da keine AHs vorhanden sind.

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 sa** - Wird verwendet, um die IPSec-Verhandlungen von Phase 2 anzuzeigen.
- **debug crypto isakmp sa** - Wird verwendet, um die ISAKMP-Verhandlungen von Phase 1 anzuzeigen.
- **debug crypto engine** - Wird zum Anzeigen der verschlüsselten Sitzungen verwendet.

Zugehörige Informationen

- NAT-Betriebsreihenfolge
- IP Security Troubleshooting - Understanding and Using debug Commands
- IPSec-Support-Seite
- NAT-Support-Seite
- Technischer Support - Cisco Systems