Konfigurieren von Router-zu-Router Dynamic-to-Static IPSec mit NAT

Inhalt

Einführung

In dieser Beispielkonfiguration erhält ein Remote-Router eine IP-Adresse über einen Teil des PPP, das IP Control Protocol (IPCP) genannt wird. Der Remote-Router verwendet die IP-Adresse, um eine Verbindung zu einem Hub-Router herzustellen. Mit dieser Konfiguration kann der Hub-Router dynamische IPSec-Verbindungen akzeptieren. Der Remote-Router verwendet Network Address Translation (NAT), um die privaten Geräte hinter dem Router mit dem privat adressierten Netzwerk hinter dem Hub-Router "zu verbinden". Der Remote-Router kennt das Endgerät und kann Verbindungen zum Hub-Router initiieren. Der Hub-Router kennt den Endpunkt jedoch nicht, daher kann er keine Verbindungen zum Remote-Router initiieren.

In diesem Beispiel ist dr_whoovie der Remote-Router und sam-i-am der Hub-Router. Eine Zugriffsliste gibt an, welcher Datenverkehr verschlüsselt werden soll. dr_whoovie weiß also, welcher Datenverkehr verschlüsselt werden soll und wo sich der sam-i-am-Endpunkt befindet. Der Remote-Router muss die Verbindung initiieren. Beide Seiten überlasten NAT.

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 12.2(24a)
- Cisco Router der Serie 2500

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 (Technische Tipps zu Konventionen von Cisco).

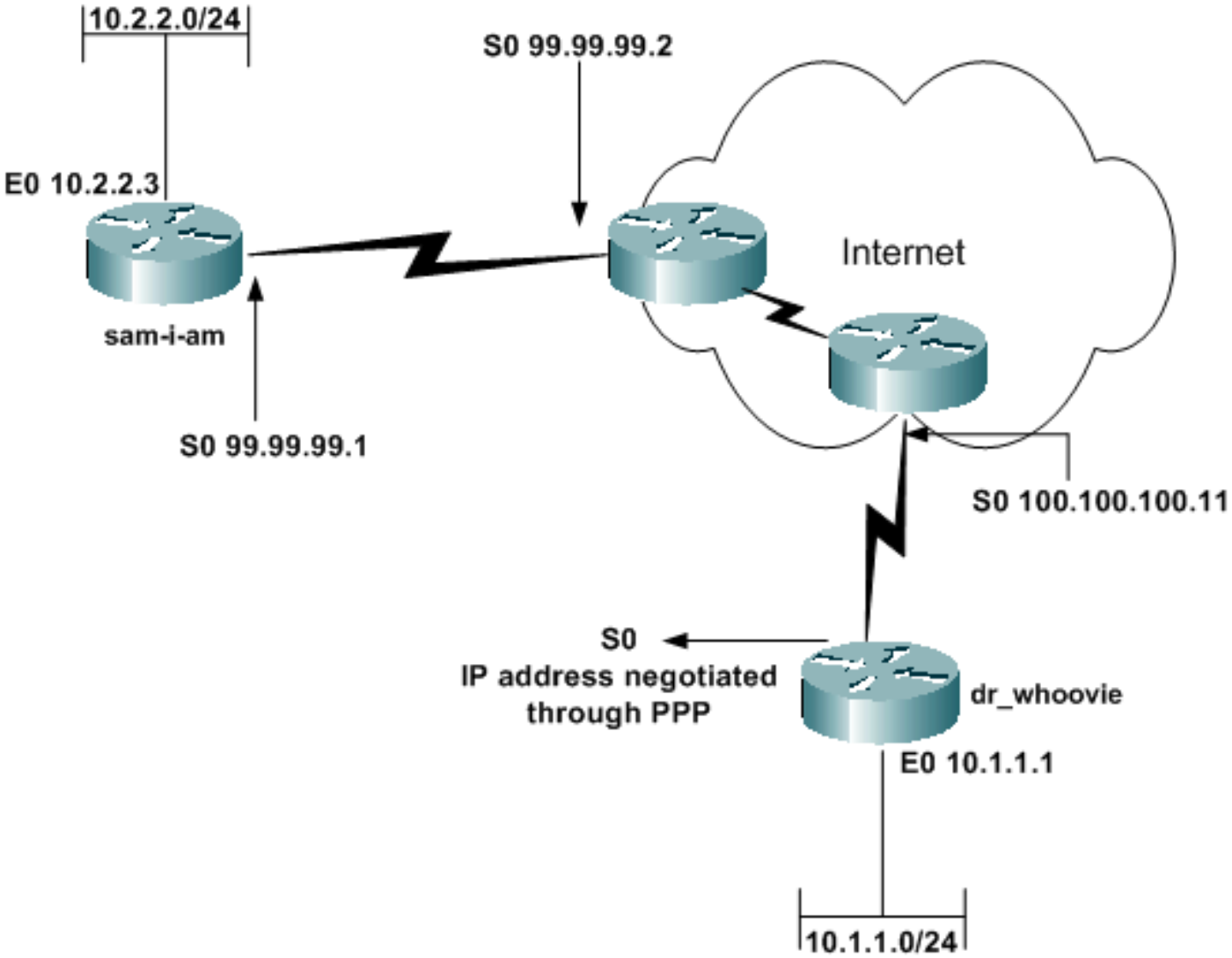
Konfigurieren

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

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- sam-am
- dr_whoovie

sam-am

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
!
ip subnet-zero
!
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
```

```
negotiation.

hash md5
authentication pre-share
!--- Specifies pre-shared keys as the authentication
method. crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0
!--- Configures a pre-shared authentication key, !---
used in global configuration mode. ! !--- These are the
IPSec policies. crypto ipsec transform-set rtpset esp-
des esp-md5-hmac
!--- A transform set is an acceptable combination !---
of security protocols and algorithms. !--- This command
defines a transform set !--- that has to be matched on
the peer router. crypto dynamic-map rtpmap 10
!--- Use dynamic crypto maps to create policy templates
!--- that can be used to process negotiation requests !-
-- for new security associations (SA) from a remote
IPSec peer, !--- even if you do not know all of the
crypto map parameters !--- required to communicate with
the remote peer, !--- such as the IP address of the
peer. set transform-set rtpset
!--- Configure IPSec to use the transform set "rtpset"
!--- that was defined previously. match address 115
!--- Assign an extended access list to a crypto map
entry !--- that is used by IPSec to determine which
traffic !--- should be protected by crypto and which
traffic !--- does not need crypto protection. crypto map
rtptrans 10 ipsec-isakmp dynamic rtpmap
!--- Specifies that this crypto map entry is to
reference !--- a preexisting dynamic crypto map. !
interface Ethernet0
 ip address 10.2.2.3 255.255.255.0
 no ip directed-broadcast
 ip nat inside
  !--- This indicates that the interface is connected to
the !--- inside network, which is subject to NAT
translation. no mop enabled ! interface Serial0
 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast
 ip nat outside
  !--- This indicates that the interface is connected !--
- to the outside network. crypto map rtptrans
!--- Use the crypto map interface configuration command
!--- to apply a previously defined crypto map set to an
interface.

!
ip nat inside source route-map nonat interface Serial0
overload
!--- Except the private network from the NAT process. ip
classless ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 115 deny ip 10.2.2.0 0.0.0.255 any
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 120
deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 120 permit ip 10.2.2.0 0.0.0.255 any
!--- Except the private network from the NAT process.
route-map nonat permit 10
 match ip address 120
```

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

dr_whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
!
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
negotiation.

 hash md5
authentication pre-share
!--- Specifies pre-shared keys as the authentication
method. crypto isakmp key cisco123 address 99.99.99.1
!--- Configures a pre-shared authentication key, !---
used in global configuration mode. ! !--- These are the
IPSec policies. crypto ipsec transform-set rtpset esp-
des esp-md5-hmac
!--- A transform set is an acceptable combination !---
of security protocols and algorithms. !--- This command
defines a transform set !--- that has to be matched on
the peer router. ! crypto map rtp 1 ipsec-isakmp
!--- Creates a crypto map and indicates that IKE will be
used !--- to establish the IPSec SAs for protecting !---
the traffic specified by this crypto map entry. set peer
99.99.99.1
!--- Use the set peer command to specify an IPSec peer
in a crypto map entry.

set transform-set rtpset
!--- Configure IPSec to use the transform set "rtpset"
!--- that was defined previously. match address 115
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. ! interface
Ethernet0
ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
!--- This indicates that the interface is connected to
the !--- inside network, which is subject to NAT
translation. no mop enabled ! interface Serial0
 ip address negotiated
!--- Specifies that the IP address for this interface !-
```

```
-- is obtained via PPP/IPCP address negotiation. !---
This example was set up in a lab with an IP address !---
assigned with IPCP. no ip directed-broadcast ip nat
outside
!--- This indicates that the interface is connected !---
to the outside network. encapsulation ppp no ip mroute-
cache no ip route-cache crypto map rtp
!--- Use the crypto map interface configuration command
!--- to apply a previously defined crypto map set to an
interface.

ip nat inside source route-map nonat interface Serial0
overload
!--- Except the private network from the NAT process. ip
classless ip route 0.0.0.0 0.0.0.0 Serial0 no ip http
server ! access-list 115 permit ip 10.1.1.0 0.0.0.255
10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 120
deny   ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the private network from the NAT process.
dialer-list 1 protocol ip permit dialer-list 1 protocol
ipx permit route-map nonat permit 10
 match ip address 120
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
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.

- Ping - Dient zur Diagnose der grundlegenden Netzwerkverbindungen.Dieses Beispiel zeigt einen Ping von der 10.1.1.1-Ethernet-Schnittstelle dr_whoovie zur 10.2.2.3-Ethernet-Schnittstelle von sam-i-am.

```
dr_whoovie# ping
Protocol [ip]:
Target IP address: 10.2.2.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
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 10.2.2.3,
  timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5),
  round-trip min/avg/max = 36/38/40 ms
```

- show crypto ipsec sa - Zeigt die Sicherheitszuordnungen in Phase 2 (SA) an.
- show crypto isakmp sa: Zeigt die SAs der Phase 1 an.

Beispielausgabe

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

```
sam-i-am# show crypto ipsec sa

interface: Serial0
    Crypto map tag: rtptrans, local addr. 99.99.99.1

   local  ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 100.100.100.1
     PERMIT, flags={}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0

     local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1
     path mtu 1500, ip mtu 1500, ip mtu interface Serial0
     current outbound spi: 52456533

     inbound esp sas:
      spi: 0x6462305C(1684156508)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x52456533(1380279603)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Dieser Befehl zeigt IPSec-SAs an, die zwischen den Peer-Geräten erstellt wurden. Der verschlüsselte Tunnel verbindet die Schnittstelle 100.100.100.1 auf dr_whoovie und die Schnittstelle 99.99.99.1 auf sam-i-am. Dieser Tunnel überträgt den Datenverkehr zwischen den Netzwerken 10.2.2.3 und 10.1.1.1. Zwei Encapsulating Security Payload (ESP)-SAs werden für ein- und ausgehenden Datenverkehr erstellt. Der Tunnel wird erstellt, obwohl sam-i-am die Peer-IP-Adresse (100.100.100.1) nicht kennt. Authentifizierungs-Header (AH)-SAs werden nicht verwendet, da kein AH konfiguriert ist.

Diese Ausgabebeispiele zeigen, dass die serielle Schnittstelle 0 auf dr_whoovie eine IP-Adresse von 100.100.100.1 bis IPCP erhält.

- Bevor die IP-Adresse ausgehandelt wird,

```
dr_whoovie#show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address will be negotiated using IPCP
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

- Nach dem Verhandeln der IP-Adresse:

```
dr_whoovie#show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 100.100.100.1/32
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

Dieses Beispiel wurde in einem Labor mit dem Befehl **peer default ip address** eingerichtet, um am Remote-Ende der seriellen 0-Schnittstelle eine IP-Adresse auf dr_whoovie zuzuweisen. Der IP-Pool wird mit dem Befehl **ip local pool** am Remote-Ende definiert.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

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**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- 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.
- debug ip nat detail —(Optional) Verifiziert den Betrieb der NAT-Funktion, indem Informationen über jedes Paket angezeigt werden, das der Router übersetzt.**Vorsicht:** Dieser Befehl erzeugt eine große Menge an Ausgabe. Verwenden Sie diesen Befehl nur bei geringem Datenverkehr im IP-Netzwerk.

- clear crypto isakmp: Löscht die SAs für Phase 1.
- clear crypto sa: Löscht die SAs für Phase 2.
- clear ip nat translation - Löscht dynamische NAT-Übersetzungen aus der Übersetzungstabelle.

Zugehörige Informationen

- IPSec-Support-Seite
- Technischer Support - Cisco Systems