Configurar el IPSec dinámica a estática de router a router con NAT

Contenido

Introducción

En esta configuración de ejemplo, un router remoto recibe una dirección IP a través de parte de PPP llamado IPCP (IP Control Protocol). El router remoto utiliza la dirección IP para conectar con un router hub. Esta configuración permite al router hub validar las conexiones dinámicas IPSec. El router remoto utiliza la Traducción de dirección de red (NAT) para "unir" los dispositivos con dirección privada de detrás con la red de dirección privada que se encuentra tras el router hub. El router remoto conoce el punto final y puede iniciar las conexiones al router hub. Pero el router hub no conoce el punto final, así que no puede iniciar las conexiones al router remoto.

En este ejemplo, el dr_whoovie es el router remoto y el sam-i-am es el router de eje de conexión. Una lista de acceso especifica qué tráfico debe ser cifrado, así que el dr_whoovie sabe qué tráfico a cifrar y dónde se localiza el punto final del sam-i-am. El router remoto debe iniciar la conexión. Los ambos lados están haciendo la sobrecarga NAT.

prerrequisitos

Requisitos

Este documento requiere una comprensión básica del protocolo IPSec Si desea más información sobre IPSec, consulte Introducción al encripción de seguridad IP (IPSec).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 12.2(24a) de Cisco IOS®
- Cisco 2500 Series Routers

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

En este documento, se utilizan estas configuraciones:

- sam-i-am
- dr_whoovie

sam-i-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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- ping — Utilizado para diagnosticar la conectividad de red básicaEste ejemplo muestra un ping de la interfaz de Ethernet de 10.1.1.1 en el dr_whoovie a la interfaz de Ethernet de 10.2.2.3

en el 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`

- muestre IPSec crypto sa — Muestra a fase 2 asociaciones de seguridad (SA).
- muestre isakmp crypto sa — Muestra la fase 1 SA.

Ejemplo de Salida

Esta salida es del **comando show crypto ipsec sa** publicado en el router de eje de conexión.

`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:`

Este comando muestra el SA de IPSec que se construye entre los dispositivos de peer. El túnel encriptado conecta la interfaz de 100.100.100.1 en el dr_whoovie y la interfaz de 99.99.99.1 en el sam-i-am. Este túnel lleva el tráfico que va entre las redes 10.2.2.3 y 10.1.1.1. Dos Encapsulating Security Payload (ESP) SA son entrantes y salientes construida. Se establece el túnel aunque el sam-i-am no conoce el IP Address de Peer (100.100.100.1). El Encabezado de autenticación SA no se utiliza puesto que hay ningunos AH configurados.

Estas muestras de las salidas muestran que la interfaz serial 0 en el dr_whoovie recibe una dirección IP de 100.100.100.1 con el IPCP.

- Antes de la dirección IP se negocia:`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`
- Después de la dirección IP se negocia:`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`

Este ejemplo fue configurado en un laboratorio con el **comando peer default ip address** de asignar una dirección IP en el extremo remoto de la interfaz del serial0 en el dr_whoovie. Definen a la agrupación IP con el **comando ip local pool** en el extremo remoto.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- depuración crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.
- debug crypto isakmp —muestra las negociaciones de fase 1 del protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP).
- debug crypto engine — muestra el tráfico codificado.
- detallado nacional del IP del debug — (opcional) verifica la operación de la función NAT visualizando la información sobre cada paquete que el router traduzca.**Precaución:** Este comando genera una gran cantidad de salida. Utilice este comando solamente cuando el tráfico en la red del IP es bajo.
- borre el isakmp crypto — Borra los SA relacionados con la fase 1.
- borre el sa crypto — Borra los SA relacionados con la fase 2.
- borre la traducción nacional del IP — Borra las traducciones NAT dinámicas de la tabla de traducción.

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems