Contenido

Introducción

Este documento es una configuración de muestra para el soporte de Cisco IOS® de la característica de Transparencia de Traducción de la Dirección (NAT) de la red IPsec. Introduce el soporte para que el tráfico IPSec viaje a través de NAT o Point Address Translation (PAT) en la red solucionando muchas incompatibilidades sabidas entre NAT e IPSec.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 2621 Router 12.2.13.7T1 y posterior
- Cliente Cisco VPN 3.6.3 (configuración no mostrada)

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.

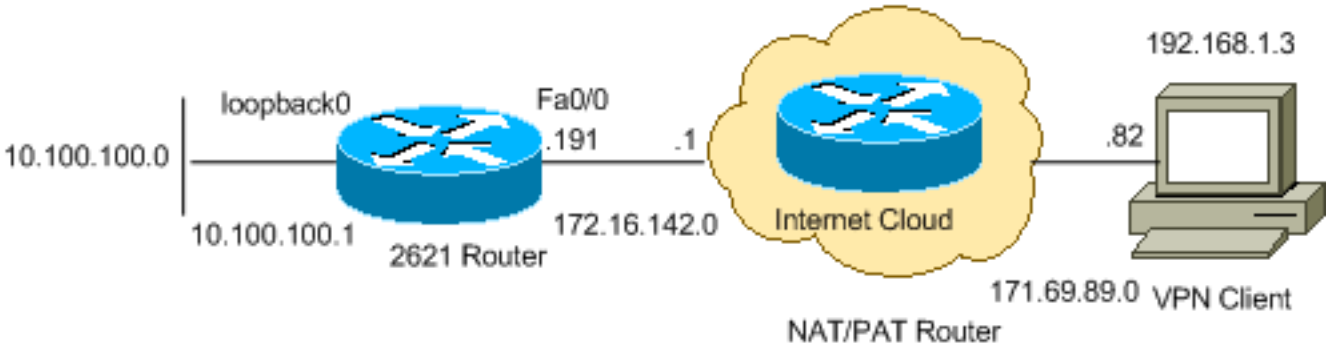
Configurar

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:



Configuración del router

Complete estos pasos:

1. Publique el **comando show version** de visualizar la versión de software que el Switch funciona con.`2621#`**`show version`**`Cisco Internetwork Operating System SoftwareIOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1, MAINTENANCE INTERIM SOFTWARETAC Support: http://www.cisco.com/tacCopyright (c) 1986-2002 by cisco Systems, Inc.Compiled Sat 21-Dec-02 14:10 by ccaiImage text-base: 0x80008098, data-base: 0x818B6330ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)ROM: C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1, MAINTENANCE INTERIM SOFTWARE2621 uptime is 33 minutesSystem returned to ROM by reloadSystem image file is "flash:c2600-ik9o3s3-mz.122-13.7.T1"cisco 2621 (MPC860) processor (revision 0x102) with 60416K/5120K bytes of memory.Processor board ID JAB0407020V (2751454139)M860 processor: part number 0, mask 49Bridging software.X.25 software, Version 3.0.0.Primary Rate ISDN software, Version 1.1.2 FastEthernet/IEEE 802.3 interface(s)2 Channelized T1/PRI port(s)32K bytes of non-volatile configuration memory.16384K bytes of processor board System flash (Read/Write)Configuration register is 0x2102`
2. Publique el **comando show run**.`2621#`**`show run`**`Building configuration...Current configuration : 2899 bytes!version 12.2service timestamps debug datetime msec localtimeservice timestamps log datetime msec localtimeno service password-encryption!hostname 2621!boot system flashlogging queue-limit 100enable secret 5 1dGFC$VA28yOWzxlCKyj1dq8SkE/!username cisco password 0 cisco123username client password 0 testclientaaa new-model!!aaa authentication login userauthen localaaa authorization network foo localaaa session-id commonip subnet-zeroip cef!!no ip domain lookupip domain name cisco.com!!!!crypto isakmp policy 20 encr 3des hash md5 authentication pre-share group 2crypto isakmp keepalive 40 5`*`!--- Allows an IPsec node to send NAT keepalive !--- packets every 20 seconds.`*`**`crypto isakmp nat keepalive 20`**`!crypto isakmp client configuration group cisco key test1234 pool test acl 120!!`*`!--- Transform set "test" which uses Triple DES !--- encryptions and MD5 (HMAC variant) !--- for data packet authentication:`*` **`crypto ipsec transform-set test esp-3des esp-md5-hmac`**`crypto ipsec transform-set foo esp-3des esp-sha-hmac!crypto ipsec profile greprotect!!`*`!--- Dynamic crypto map.`*`**`crypto dynamic-map dynmap 1 set transform-set foo match address 199`**`!!crypto map test client authentication list userauthencrypto map test isakmp authorization list foocrypto map test client configuration address respond`*`!--- Adds a dynamic crypto map set`

```
to a static crypto map set. crypto map test 20 ipsec-isakmp dynamic dynmap!!!voice call
carrier capacity active!!!!!!!no voice hpi capture bufferno voice hpi capture
destination!!mta receive maximum-recipients 0!!controller T1 0/0 framing sf linecode
ami!controller T1 0/1 framing sf linecode ami!!!interface Loopback0 ip address 10.100.100.1
255.255.255.0 ip nat inside!interface FastEthernet0/0 ip address 172.16.142.191
255.255.255.0 ip nat outside no ip route-cache no ip mroute-cache duplex auto speed auto !-
-- Applies a crypto map set to an interface. crypto map test!interface FastEthernet0/1 ip
address 10.130.13.13 255.255.0.0 duplex auto speed auto!ip local pool test 192.168.1.1
192.168.1.250ip nat inside source route-map nonat interface FastEthernet0/0 overloadno ip
http serverno ip http secure-serverip classlessip route 0.0.0.0 0.0.0.0 172.16.142.1!ip pim
bidir-enable!!access-list 101 permit ip any anyaccess-list 101 permit esp any anyaccess-
list 101 permit udp any any eq isakmpaccess-list 101 permit ip 192.168.0.0 0.0.255.255
10.100.100.0 0.0.0.255access-list 111 permit ip 10.100.100.0 0.0.0.255 10.10.10.0
0.0.0.255access-list 112 deny   ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255access-list
112 deny   ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255access-list 112 permit ip
10.100.100.0 0.0.0.255 anyaccess-list 120 permit ip 10.100.100.0 0.0.0.255 192.168.1.0
0.0.0.255!--- IPsec access list defines which traffic to protect.access-list 199 permit ip
10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255access-list 199 permit ip host 172.16.142.191
192.168.1.0 0.0.0.255!route-map nonat permit 10 match ip address 112!radius-server
authorization permit missing Service-Typecall rsvp-sync!!mgcp profile default!dial-peer cor
custom!!!!!line con 0 exec-timeout 0 0line aux 0line vty 0 4 password cisco!!end2621#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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.

- ¿**muestre isakmp crypto sa**? Visualiza todas las asociaciones de seguridad actuales del Internet Key Exchange (IKE) (SA) en un par.
```
2621#show crypto isakmp sa   f_vrf/i_vrf   dst
src             state       conn-id slot       /        172.16.142.191  171.69.89.82
QM_IDLE      4       0
```
- ¿**muestre IPSec crypto sa**? Visualiza las configuraciones usadas por los SA actuales.
```
2621#show crypto ipsec sainterface: FastEthernet0/0    Crypto map tag: test, local
addr. 172.16.142.191   protected vrf:   local  ident (addr/mask/prot/port):
(10.100.100.0/255.255.255.0/0/0) !--- Subnet behind local VPN router. remote ident
(addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0) !--- Subnet behind remote VPN
router. current_peer: 171.69.89.82:4500 PERMIT, flags={} #pkts encaps: 11, #pkts encrypt:
11, #pkts digest 11 #pkts decaps: 11, #pkts decrypt: 11, #pkts verify 11 #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.: 172.16.142.191, remote crypto endpt.: 171.69.89.82 !--- IP address of Encapsulating
Security Payload (ESP) endpoints. path mtu 1500, media mtu 1500 current outbound spi:
9A12903F inbound esp sas: spi: 0xD44C2AFE(3561761534) !--- SPI inbound (ESP tunnel).
transform: esp-3des esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id:
2002, flow_id: 3, crypto map: test        sa timing: remaining key lifetime (k/sec):
(4513510/3476)        IV size: 8 bytes        replay detection support: Y     inbound ah
sas:     inbound pcp sas:     outbound esp sas:      spi: 0x9A12903F(2584907839)!---
Security parameter index (SPI) outbound (ESP tunnel). transform: esp-3des esp-sha-hmac , in
use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2003, flow_id: 4, crypto map: test
sa timing: remaining key lifetime (k/sec): (4513511/3476)        IV size: 8 bytes
replay detection support: Y     outbound ah sas:     outbound pcp sas:   protected vrf:
local  ident (addr/mask/prot/port): (172.16.142.191/255.255.255.255/0/0)!--- Next tunnel.
remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0) current_peer:
171.69.89.82:4500 PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts
decaps: 0, #pkts decrypt: 0, #pkts verify 0 #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.: 172.16.142.191, remote crypto
endpt.: 171.69.89.82 path mtu 1500, media mtu 1500 current outbound spi: 1CD14C06 inbound
```

```
esp sas: spi: 0x1EAC399E(514603422) transform: esp-3des esp-sha-hmac , in use settings
={Tunnel UDP-Encaps, } slot: 0, conn id: 2000, flow_id: 1, crypto map: test sa timing:
remaining key lifetime (k/sec): (4434590/3471) IV size: 8 bytes replay detection support: Y
inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x1CD14C06(483478534) transform:
esp-3des esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: test sa timing: remaining key lifetime (k/sec): (4434590/3469) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```

- **¿muestre el active de la conexión del motor del crypyo**? Muestra las estadísticas del motor de criptografía. Esto muestra las cuentas de paquetes.`2621#`**`show crypyo engine connection active`**
```
ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt   4
FastEthernet0/0 172.16.142.191  set    HMAC_MD5+3DES_56_C        0        02000
FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0        02001
FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0        0 2002
FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0       11 2003
FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C       11        0
```
- **show crypto engine [descripción | ¿configuración]**? Visualiza un resumen de la información de la configuración para los motores de criptografía. Utilice este comando en el modo EXEC privilegiado. Este comando visualiza todos los motores de criptografía y visualiza el nombre del producto AIM-VPN.`2621#`**`show crypto engine configuration`**
```
crypto engine name: unknown!--- Name of the crypto engine as assigned with the !--- key-name argument in the
crypto key generate dss command.        crypto engine type:  software!--- If "software" is
listed, the crypto engine resides in either !--- the Route Switch Processor (RSP) (the Cisco
IOS crypto engine) or !--- in a second-generation Versatile Interface Processor (VIP2).
serial number: A3FFDBBB crypto engine state: installed !--- The state "installed" indicates
that a crypto engine is located !--- in the given slot, but is not configured for
encryption. crypto engine in slot: N/A platform: Cisco Software Crypto Engine Encryption
Process Info: input queue size: 500 input queue top: 34 input queue bot: 34 input queue
count: 0 Crypto Adjacency Counts: Lock Count: 0 Unlock Count: 0 crypto lib version: 14.0.0
ipsec lib version: 2.0.0
```
- **¿muestre el detalle crypto isakmp sa nacional**? Detalles ISAKMP SA NAT de las visualizaciones.`2621#`**`show crypto isakmp sa detail nat`**
```
Codes: C - IKE configuration mode, D - Dead Peer Detection       K - Keepalives, N - NAT-traversal       X - IKE Extended
Authentication       psk - Preshared key, rsig - RSA signature       renc - RSA encryption
f_vrf/i_vrf  Conn id   Local        Remote        Encr Hash Auth DH Lifetime Capabilities
/        4     172.16.142.191  171.69.89.82  3des md5       2  23:56:43 CDXN        NAT
keepalive(sec) 20        In local 172.16.142.191:4500 remote cisco:4500
```
f_vrf/i_vrf - El ruteo virtual de la puerta frontal y la expedición (F_VRF) y el VRF interior (I_VRF) IKE SA. Si el FVRF es global, la salida muestra el `f_vrf` como campo vacío.

Troubleshooting

Use esta sección para resolver 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.

Para obtener información adicional sobre la solución de problemas, consulte Solución de problemas de seguridad IP - Comprensión y uso de los comandos debug.

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

Esta configuración recibe el Keepalives NAT cada 20 segundos según lo configurado.

- ¿**IPSec del debug crypto**? Visualiza los IPSec Negotiations de la fase 2.
- ¿**isakmp del debug crypto**? Visualiza negociaciones ISAKMP de la fase 1.
- ¿**motor del debug crypto**? Visualiza el tráfico se cifra que.`2621#`**`show crypto isakmp sa detail nat`**`Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption` **`f_vrf/i_vrf`** `Conn id Local Remote Encr Hash Auth DH Lifetime Capabilities / 4 172.16.142.191 171.69.89.82 3des md5 2 23:56:43 CDXN NAT keepalive(sec) 20 In local 172.16.142.191:4500 remote cisco:4500`
- ¿**paquete del IP del debug [detail]**? Información de debugging de las visualizaciones IP general y transacciones de seguridad de la Opción de seguridad IP (IPSO).
- ¿**ICMP del IP del debug**? Visualiza la información sobre las transacciones de mensaje de control internas del protocolo (ICMP).`2621#`**`show crypto isakmp sa detail nat`**`Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption` **`f_vrf/i_vrf`** `Conn id Local Remote Encr Hash Auth DH Lifetime Capabilities / 4 172.16.142.191 171.69.89.82 3des md5 2 23:56:43 CDXN NAT keepalive(sec) 20 In local 172.16.142.191:4500 remote cisco:4500`
- ¿**IPSec del debug crypto**? Visualiza los IPSec Negotiations de la fase 2.
- ¿**isakmp del debug crypto**? Visualiza negociaciones ISAKMP de la fase 1.
- ¿**motor del debug crypto**? Visualiza el tráfico se cifra que.`2621#`**`show crypto isakmp sa detail nat`**`Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption` **`f_vrf/i_vrf`** `Conn id Local Remote Encr Hash Auth DH Lifetime Capabilities / 4 172.16.142.191 171.69.89.82 3des md5 2 23:56:43 CDXN NAT keepalive(sec) 20 In local 172.16.142.191:4500 remote cisco:4500`

Información Relacionada

- Página de soporte para cliente Cisco VPN
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems