

Configurando o IPSec dinâmico a estático de roteador a roteador com NAT

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Saída de exemplo](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Nesta configuração de exemplo, um roteador remoto recebe um endereço IP através de parte do PPP chamado IP Control Protocol (IPCP). O roteador remoto usa o endereço IP para conectar a um roteador de hub. Esta configuração permite que o roteador de hub aceite conexões de IPSec dinâmicas. O roteador remoto usa tradução de endereço de rede (NAT) para “ligar” os dispositivos com endereços privados conectados a ele à rede com endereço privado conectada ao roteador de hub. O roteador remoto conhece o ponto de extremidade e pode iniciar conexões com o roteador de hub. Mas o roteador de hub não conhece o ponto de extremidade e, portanto, não pode iniciar conexões com o roteador remoto.

Neste exemplo, a dr_whoovie é o roteador remoto e o sam-i-am é o roteador de hub. Uma lista de acessos específica que tráfego deve ser cifrada, assim que a dr_whoovie sabe que tráfego a cifrar e onde o valor-limite do sam-i-am é encontrado. O roteador remoto deve iniciar a conexão. Os ambos os lados estão fazendo a sobrecarga NAT.

[Pré-requisitos](#)

[Requisitos](#)

Este documento requer uma compreensão básica do protocolo de IPSec. Para saber mais sobre o IPSec, consulte [Uma introdução à criptografia de segurança de IP \(IPSec\)](#).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- [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

```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- [sibilo](#) — Usado para diagnosticar a conectividade de rede básicaEste exemplo mostra um

sibilo da interface Ethernet de 10.1.1.1 na dr_whoovie à interface Ethernet de 10.2.2.3 no 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

- [mostre IPsec cripto sa](#) — Mostra à fase 2 associações de segurança (SA).
- [mostre isakmp cripto sa](#) — Mostra a fase 1 SA.

Saída de exemplo

Esta saída é do comando **show crypto ipsec sa** emitido no roteador de hub.

```
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 mostra o sas de IPsec que é construído entre os dispositivos de peer. O túnel criptografado conecta a relação de 100.100.100.1 na dr_whoovie e a relação de 99.99.99.1 no sam-i-am. Este túnel leva o tráfego que vai entre redes 10.2.2.3 e 10.1.1.1. Dois Encapsulating Security Payload (ESP) SA são de entrada e de partida construídos. O túnel é estabelecido mesmo que o sam-i-am não conheça o endereço IP do peer (100.100.100.1). O Authentication Header (AH) SA não é usado desde que não há nenhum AH configurado.

Estas amostras das saídas mostram que a interface serial 0 na dr_whoovie recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT de 100.100.100.1 com o IPCP.

- Antes do endereço IP de Um ou Mais Servidores Cisco ICM NT é negociado: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
- Após o endereço IP de Um ou Mais Servidores Cisco ICM NT é negociado: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 exemplo estabeleceu-se em um laboratório com o comando **peer default ip address** atribuir um endereço IP de Um ou Mais Servidores Cisco ICM NT na extremidade remota da relação do serial0 na dr_whoovie. O IP pool é definido com o comando **ip local pool** na extremidade remota.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- [IPsec do debug crypto](#) — Mostra as negociações de IPSEC de fase 2.
- [isakmp do debug crypto](#) — Mostra as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- [motor do debug crypto](#) — Mostra o tráfego que é cifrado.
- [debugar detalhado nat IP](#) — (opcional) verifica a operação dos recursos NAT indicando a informação sobre cada pacote que o roteador traduz. **Cuidado:** Este comando gerencie uma grande quantidade de saída. Use este comando somente quando o tráfego na rede IP é baixo.
- [cancele o isakmp cripto](#) — Cancela os SA relativos à fase 1.
- [cancele o sa cripto](#) — Cancela os SA relativos à fase 2.
- [cancele a tradução nat IP](#) — Cancela conversões NAT dinâmica da tabela de tradução.

Informações Relacionadas

- [Página de suporte do IPsec](#)
- [Suporte Técnico - Cisco Systems](#)