Configurando o roteador para roteador, o Pre-shared do IPsec, sobrecarga NAT entre um privado e uma rede pública

Índice

Introdução

Esta configuração de exemplo mostra como criptografar o tráfego entre uma rede privada (10.103.1.x) e uma rede pública (98.98.98.x) com o uso de IPsec. A rede 98.98.98.x conhece a rede 10.103.1.x pelos endereços particulares. A rede 10.103.1.x conhece a rede 98.98.98.x via endereços públicos.

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 12.3(5) de Cisco IOS®
- Cisco 3640 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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

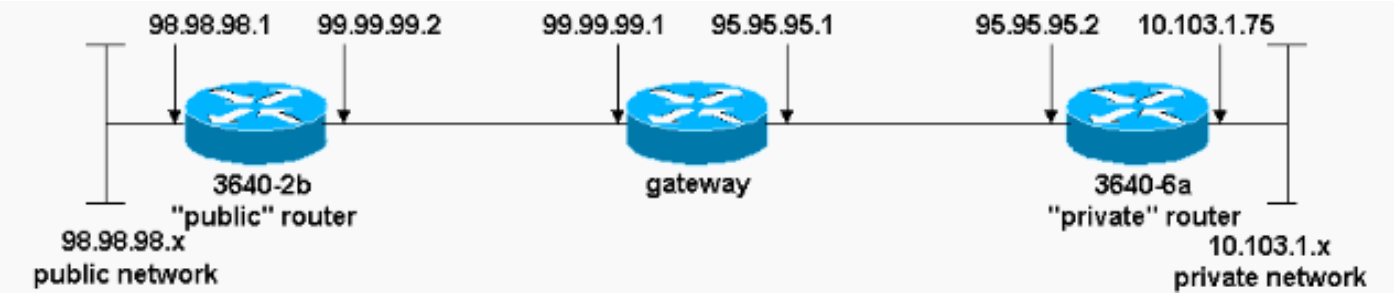
Configurar

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

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza as seguintes configurações:

- roteador 3640-2b “público”
- Roteador “privado” 3640-6a

roteador 3640-2b “público”

```
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

Roteador “privado” 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
```

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.

Para verificar esta configuração, tente um comando extended ping originado da interface Ethernet no roteador privado 10.103.1.75, destinado à interface Ethernet no roteador público 98.98.98.1

- sibilo — Usado para diagnosticar a conectividade de rede básica.`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`
- mostre IPsec cripto sa — Mostra os ajustes usados (IPsec) por SA atuais.
- mostre isakmp cripto sa — Mostra todo o IKE atual SA em um par.
- show crypto engine — Mostra um sumário da informação de configuração para as crypto-engines. Use o **comando show crypto engine no** modo de exec privilegiado.

Exemplo de saída de show

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

```
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:
```

Este comando mostra o IPsec SAs construído entre peers. O túnel criptografado é construído entre 95.95.95.2 e 99.99.99.2 para o tráfego que vai entre redes 98.98.98.0 e 10.103.1.0. Você pode ver as duas SAs de Payload de Segurança de Encapsulamento (ESP) desenvolvidas interna e externamente. O Authentication Header (AH) SA não é usado desde que não há nenhum AH.

Troubleshooting

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

Comandos para Troubleshooting

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

Nota: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

- **debug crypto ipsec sa** — Usado para ver as negociações de IPSEC de fase 2.
- **debug crypto isakmp sa** — Usado para ver as negociações de ISAKMP de fase 1.
- **motor do debug crypto** — Usado para indicar as sessões de criptografia.

Informações Relacionadas

- Ordem de Operação NAT
- Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug
- Página de suporte do IPSec
- Página de suporte de NAT
- Suporte Técnico - Cisco Systems