Configuration d'IPSec de routeur à routeur, avec clé pré-partagée et surcharge NAT entre un réseau privé et un réseau public

Contenu

Introduction

Cet exemple de configuration montre comment chiffrer le trafic entre un réseau privé (10.103.1.x) et un réseau public (98.98.98.x) grâce à IPSec. Le réseau 98.98.98.x connaît le réseau 10.103.1.x grâce aux adresses privées. Le réseau 10.103.1.x connaît le réseau 98.98.98.x grâce aux adresses publiques.

Conditions préalables

Conditions requises

Ce document exige une compréhension de base de protocole IPsec. Pour se renseigner plus sur IPSec, référez-vous s'il vous plaît à une introduction au cryptage de sécurité IP (IPSec).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 12.3(5) de Cisco IOS®
- Routeurs de Cisco 3640

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

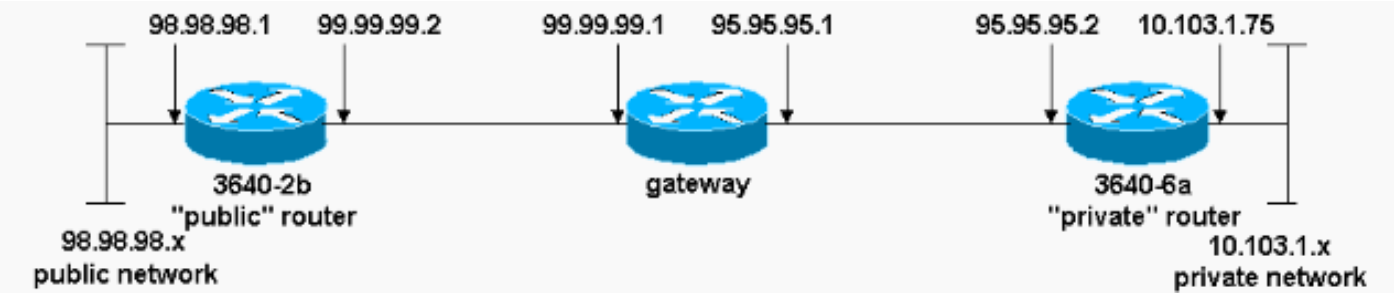
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Configurations

Ce document utilise les configurations suivantes :

- routeur 3640-2b « public »
- routeur 3640-6a « privé »

routeur 3640-2b « public »

```
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
```

routeur 3640-6a « privé »

```
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
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Pour vérifier cette configuration, essayez une commande ping étendue originaire de l'interface Ethernet sur le routeur privé 10.103.1.75, destiné à l'interface Ethernet sur le routeur public 98.98.98.1

- ping — Utilisé pour diagnostiquer la connexion réseau de base.`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`
- show crypto ipsec sa — Affiche les configurations utilisées par le courant (IPSec) SAS.
- show crypto isakmp sa — Affiche toutes les SA IKE en cours au niveau d'un homologue.
- show crypto engine — Affiche un résumé des informations de configuration pour les moteurs de chiffrement. Utilisez la commande de **show crypto engine** dans le mode d'exécution

privilégié.

Exemple de sortie avec show

Cette sortie est de la commande émise de **show crypto ipsec sa** sur le routeur concentrateur.

```
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:
```

Cette commande montre les SA IPsec créées entre homologues. Le tunnel chiffré est établi entre 95.95.95.2 et 99.99.99.2 pour le trafic qui va entre les réseaux 98.98.98.0 et 10.103.1.0. Vous pouvez voir les deux SA ESP (Encapsulating Security Payload) en entrée et en sortie. L'En-tête d'authentification (AH) SAS ne sont pas utilisés puisqu'il n'y a aucun AHs.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug crypto ipsec SA** — Utilisé pour voir les négociations IPSecs de la phase 2.
- **debug crypto isakmp SA** — Utilisé pour voir les négociations ISAKMP de la phase 1.
- **debug crypto engine** — Utilisé pour afficher les sessions chiffrées.

Informations connexes

- Ordre des opérations NAT
- Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage
- Page d'assistance IPsec
- Page de support NAT
- Support technique - Cisco Systems