Configuration d'un tunnel IPSec dynamique en statique entre deux routeurs, avec NAT

Contenu

Introduction

Dans cet exemple de configuration, un routeur distant reçoit une adresse IP par une partie du protocole PPP appelée protocole de contrôle IP (IPCP). Le routeur distant utilise l'adresse IP pour se connecter à un routeur central. Cette configuration permet au routeur central d'accepter des connexions IPSec dynamiques. Le routeur distant utilise la traduction d'adresses de réseau (NAT) pour « joindre » les périphériques adressés en privé derrière lui au réseau adressé en privé derrière le routeur central. Le routeur distant connaît le point d'extrémité et peut amorcer des connexions avec le routeur central. Par contre, le routeur central ne connaît pas le point d'extrémité; il ne peut donc pas amorcer de connexion avec le routeur distant.

Dans cet exemple, le dr_whoovie est le routeur distant et Sam-je-est est le routeur concentrateur. Une liste d'accès spécifie quel trafic doit être chiffré, ainsi le dr_whoovie connaît quel trafic à chiffrer et où Sam-je-suis le point final se trouve. Le routeur distant doit initier la connexion. Les deux côtés font la surcharge NAT.

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 12.2(24a) de Cisco IOS®
- Routeurs de la gamme Cisco 2500

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 à Conventions relatives aux conseils techniques Cisco.

Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- Sam-je-suis
- dr_whoovie

Sam-je-suis

```
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
```

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.

- ping — Utilisé pour diagnostiquer la connexion réseau de baseCet exemple affiche qu'un ping de l'interface Ethernet de 10.1.1.1 sur le dr_whoovie à l'interface Ethernet de 10.2.2.3 Sam-je-suis en fonction.`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`
- show crypto ipsec sa — Affiche à la phase 2 associations de sécurité (SA).
- show crypto isakmp sa — Affiche à la phase 1 SAS.

Exemple de sortie

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

```
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:
```

Cette commande montre IPSec SAS qui sont construits entre les périphériques de pair. Le tunnel chiffré connecte l'interface de 100.100.100.1 sur le dr_whoovie et l'interface de 99.99.99.1 Sam-je-suis en fonction. Ce tunnel porte le trafic allant entre les réseaux 10.2.2.3 et 10.1.1.1. Deux Protocole ESP (Encapsulating Security Payload) SAS sont d'arrivée et sortants construits. Le tunnel est établi quoique Sam-je-sois ne connaisse pas l'adresse IP de pair (100.100.100.1). L'En-tête d'authentification (AH) SAS ne sont pas utilisés puisqu'il y a d'aucun OH configuré.

Ces échantillons de sorties prouvent que l'interface série 0 sur le dr_whoovie reçoit une adresse IP de 100.100.100.1 par IPCP.

- Avant l'adresse IP est négocié :`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`
- Après l'adresse IP est négocié :`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`

Cet exemple a été installé dans un laboratoire avec la commande de **peer default ip address** d'assigner une adresse IP à l'extrémité distante de l'interface de l'interface série 0 sur le dr_whoovie. Le pool d'IP est défini avec la commande d'**ip local pool à l'**extrémité distante.

Dépannez

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

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- debug crypto ipsec — Affiche les négociations IPSecs de la phase 2.
- debug crypto isakmp — Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- debug crypto engine - Montre le trafic crypté.
- debug ip nat détaillé — (facultatif) vérifie l'exécution de la caractéristique NAT en affichant des informations sur chaque paquet que le routeur traduit.**Attention :** Cette commande génère un grand nombre de sortie. Utilisez cette commande seulement quand le trafic sur le réseau IP est bas.
- clear crypto isakmp — Efface SAS liée à la phase 1.
- clear crypto sa — Efface SAS liée à la phase 2.
- clear ip nat translation — Efface les traductions NAT dynamiques de la table de traduction.

Informations connexes

- Page d'assistance IPsec
- Support technique - Cisco Systems