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

Table des matières

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, dr_whoovie est le routeur distant et sam-i-am est le routeur concentrateur. Une liste de contrôle d’accès spécifie le trafic à chiffrer, de sorte que dr_whoovie sache quel trafic chiffrer et où se trouve le point d’extrémité sam-i-am. Le routeur distant doit initier la connexion. Les deux côtés effectuent une surcharge NAT.

Conditions préalables

Exigences

Ce document exige une connaissance de base du protocole IPSec. Pour en savoir plus sur IPSec, veuillez vous reporter à Une introduction au cryptage IPSec (IP Security).

Composants utilisés

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

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Configurer

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

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- sam-sam
- dr_whoovie

<#root>

```
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 !--

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

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation r

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 whic

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 NA
 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

<#root>

```
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 !--


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

!
crypto map rtp 1 ipsec-isakmp


!--- Creates a crypto map and indicates that IKE will be used !--- to establish the IPSec SAs for prot

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 NA

 no mop enabled
!
interface Serial0
 ip address negotiated

 !--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiati

 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
```

Vérifier

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 connectivité réseau de base

  Cet exemple montre une requête ping de l'interface Ethernet 10.1.1.1 sur dr_whoovie à l'interface Ethernet 10.2.2.3 sur sam-i-am.

  <#root>

  ```
  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 les associations de sécurité (SA) de phase 2.
- show crypto isakmp sa : affiche les SA de phase 1.

Exemple de sortie

Ce résultat provient de la commande show crypto ipsec sa émise sur le routeur concentrateur.

<#root>

```
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 affiche les associations de sécurité IPSec qui sont créées entre les périphériques homologues. Le tunnel chiffré connecte l'interface 100.100.100.1 sur dr_whoovie et l'interface 99.99.99.1 sur sam-i-am. Ce tunnel transporte le trafic entre les réseaux 10.2.2.3 et 10.1.1.1. Deux SA ESP (Encapsulating Security Payload) sont créées en entrée et en sortie. Le tunnel est établi même si sam-i-am ne connaît pas l'adresse IP de l'homologue (100.100.100.1). Les SA d'en-tête d'authentification (AH) ne sont pas utilisées car aucun AH n'est configuré.

Ces exemples de sortie montrent que l'interface série 0 sur dr_whoovie reçoit une adresse IP de 100.100.100.1 via IPCP.

- Avant la négociation de l’adresse IP :

```
<#root>

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
```

- Une fois l'adresse IP négociée :

```
<#root>

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 configuré dans un TP avec la commande peer default ip address pour attribuer une adresse IP à l'extrémité distante de l'interface Serial 0 sur dr_whoovie. Le pool d'adresses IP est défini avec la commande ip local pool à l'extrémité distante.

Dépannage

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 : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

- debug crypto ipsec : Cette commande affiche les négociations IPSec de la phase 2.

- debug crypto isakmp : Cette commande affiche les négociations ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- debug crypto engine - Montre le trafic crypté.
- debug ip nat detailed -(Facultatif) Vérifie le fonctionnement de la fonctionnalité NAT en affichant des informations sur chaque paquet que le routeur traduit.

  Attention : cette commande génère une grande quantité de résultats. Utilisez cette commande uniquement lorsque le trafic sur le réseau IP est faible.
- clear crypto isakmp - Efface les SA liées à la phase 1.
- clear crypto sa : efface les SA liées 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.