Configuration d'IPSec en mode Hub and Spoke entre deux routeurs

Contenu

Introduction

Ce document montre le cryptage d'un réseau en étoile; d'un routeur (le « hub ») à trois autres routeurs (les sites en étoile). Une cryptocarte dans le routeur central indique les réseaux utilisés par chacun de ses trois pairs. Les cryptocartes dans chaque routeur en étoile indiquent le réseau utilisé par le routeur central.

Le cryptage est fait entre ces réseaux :

- réseau 160.160.160.x au réseau 170.170.170.x
- réseau 160.160.160.x au réseau 180.180.180.x
- réseau 160.160.160.x au réseau 190.190.190.x

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version de logiciel 12.0.7.T ou ultérieures de Cisco IOS®
- Routeurs de 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 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 suivante :

Configurations

Ce document utilise les configurations suivantes :

- configuration de dr_whoovie
- Sam-JE-suis la configuration
- configuration de thidwick
- configuration de yertle

configuration de dr_whoovie

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!--- Configure the Internet Key Exchange (IKE) !---
policy and preshared key for each peer: !--- IKE policy
defined for peers. crypto isakmp policy 1 authentication
```

```
pre-share !--- Preshared keys for different peers.
crypto isakmp key cisco170 address 150.150.150.2 crypto
isakmp key cisco180 address 150.150.150.3 crypto isakmp
key cisco190 address 150.150.150.4 !--- Configure the
IPSec parameters: !--- IPSec transform sets. crypto
ipsec transform-set 170cisco esp-des esp-md5-hmac crypto
ipsec transform-set 180cisco esp-des esp-md5-hmac crypto
ipsec transform-set 190cisco esp-des esp-md5-hmac !
crypto map ETH0 17 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.2 !--- The IPSec transform set is used
for this tunnel. set transform-set 170cisco !---
Interesting traffic for peer 150.150.150.2. match
address 170 crypto map ETH0 18 ipsec-isakmp !--- Set the
peer. set peer 150.150.150.3 !--- The IPSec transform
set is used for this tunnel. set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.3. match
address 180 crypto map ETH0 19 ipsec-isakmp !--- Set the
peer. set peer 150.150.150.4 !--- The IPSec transform
set is used for this tunnel. set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.4. match
address 190 ! interface Ethernet0 ip address
150.150.150.1 255.255.255.0 no ip directed-broadcast no
ip route-cache no ip mroute-cache no mop enabled !---
Apply crypto map on the interface. crypto map ETH0 !
interface Serial0 ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast no ip mroute-cache no fair-
queue ! ip classless ip route 170.170.170.0
255.255.255.0 150.150.150.2 ip route 180.180.180.0
255.255.255.0 150.150.150.3 ip route 190.190.190.0
255.255.255.0 150.150.150.4 no ip http server ! !---
Access list that shows traffic to encryption from
yertle. access-list 170 permit ip 160.160.160.0
0.0.0.255 170.170.170.0 0.0.0.255 !--- Access list that
shows traffic to encryption from thidwick. access-list
180 permit ip 160.160.160.0 0.0.0.255 180.180.180.0
0.0.0.255 !--- Access list that shows traffic to
encryption from sam-i-am. access-list 190 permit ip
160.160.160.0 0.0.0.255 190.190.190.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login end
```

Sam-JE-suis la configuration

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sam-I-am
!
enable secret 5 $1$HDyw$qubSJdqfIC0f1VLvHmg/P0
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco190 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
```

```
set. crypto ipsec transform-set 190cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 19 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 190cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 190 ! interface
Ethernet0 ip address 150.150.150.4 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled !--- Apply crypto map on the interface.
crypto map ETH0 ! interface Serial0 ip address
190.190.190.1 255.255.255.0 no ip directed-broadcast no
ip mroute-cache no fair-queue ! ip classless ip route
160.160.160.0 255.255.255.0 150.150.150.1 no ip http
server !--- Access list that shows traffic to encryption
!--- for the hub site (dr_whoovie). access-list 190
permit ip 190.190.190.0 0.0.0.255 160.160.160.0
0.0.0.255 dialer-list 1 protocol ip permit dialer-list 1
protocol ipx permit ! line con 0 transport input none
line aux 0 line vty 0 4 password ww login ! end
```

configuration de thidwick

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco180 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
set. crypto ipsec transform-set 180cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 18 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 180cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 180 ! interface
Ethernet0 ip address 150.150.150.3 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled !--- Apply crypto map on the interface.
crypto map ETH0 ! interface Serial1 ip address
180.180.180.1 255.255.255.0 no ip directed-broadcast
clockrate 4000000 ! interface BRI0 no ip address no ip
directed-broadcast shutdown isdn switch-type basic-5ess
! ip classless ip route 160.160.160.0 255.255.255.0
150.150.150.1 no ip http server !--- Access list that
shows traffic to encryption !--- for the hub site
(dr_whoovie). access-list 180 permit ip 180.180.180.0
0.0.0.255 160.160.160.0 0.0.0.255 dialer-list 1 protocol
ip permit dialer-list 1 protocol ipx permit ! line con 0
transport input none line aux 0 line vty 0 4 password ww
login ! end
```

configuration de yertle

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco170 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
set. crypto ipsec transform-set 170cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 17 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 170cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 170 ! interface
Ethernet0 ip address 150.150.150.2 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled !--- Apply crypto map on the interface.
crypto map ETH0 ! interface Serial0 no ip address no ip
directed-broadcast no ip mroute-cache shutdown no fair-
queue ! interface Serial1 ip address 170.170.170.1
255.255.255.0 no ip directed-broadcast ! ip classless ip
route 160.160.160.0 255.255.255.0 150.150.150.1 no ip
http server !--- Access list that shows traffic to
encryption for !--- the hub site (dr_whoovie). access-
list 170 permit ip 170.170.170.0 0.0.0.255 160.160.160.0
0.0.0.255 dialer-list 1 protocol ip permit dialer-list 1
protocol ipx permit ! tftp-server flash:/c2500-jos56i-
l.120-7.T tftp-server flash:c2500-jos56i-l.120-7.T tftp-
server flash: ! 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.

- **show crypto ipsec sa** - Montre les associations de sécurisation de phase 2.
- **show crypto isakmp sa** - Montre les associations de sécurisation de phase 1.

Dépannez

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

Dépannage des commandes

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** — Affiche le trafic qui est chiffré.
- **clear crypto isakmp** — Autorise les associations de sécurité liées à la phase 1.
- **clear crypto sa** — Autorise les associations de sécurité liées à la phase 2.

Informations connexes

- Configurez la Sécurité de réseau IPSec
- Configurez le protocole de sécurité IKE
- Page d'assistance IPsec
- Support technique - Cisco Systems