Configuration d'un tunnel IPSec entre un routeur Cisco et un Checkpoint NG

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Diagramme du réseau
Conventions
Configurez le routeur VPN de Cisco 1751
Configurez Checkpoint NG
Vérifiez
Vérifiez le routeur de Cisco
Vérifiez Checkpoint NG
Dépannez
Routeur de Cisco
Informations connexes

Introduction

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés :

- Le réseau 172.16.15.x privé à l'intérieur du routeur.
- Le réseau 192.168.10.x privé à l'intérieur de la nouvelle génération du$^{TM\ de}$ point de reprise (NG).

Conditions préalables

Conditions requises

Les procédures tracées les grandes lignes dans ce document sont fondées sur ces hypothèses.

- La stratégie de base NG du$^{TM\ de}$ point de reprise est installée.
- Tous les accès, Traduction d'adresses de réseau (NAT), et installations de routage sont configurés.
- Trafiquez de l'intérieur du routeur et intérieur que le NG du$^{TM\ de}$ point de reprise à l'Internet circule.

Composants utilisés

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

- Routeur Cisco 1751
- Logiciel de Cisco IOS® (C1700-K9O3SY7-M), version 12.2(8)T4, LOGICIEL de VERSION (fc1)
- Construction 50027 NG du TM de point de reprise

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Conventions

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

Configurez le routeur VPN de Cisco 1751

Routeur de Cisco VPN 1751

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1 encr 3des hash md5 authentication pre-
share group 2 lifetime 1800 !--- IPSec configuration.
crypto isakmp key aptrules address 209.165.202.129 !
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
! crypto map aptmap 1 ipsec-isakmp set peer
209.165.202.129 set transform-set aptset match address
110 ! interface Ethernet0/0 ip address 209.165.202.226
255.255.255.224 ip nat outside half-duplex crypto map
aptmap ! interface FastEthernet0/0 ip address
172.16.15.1 255.255.255.0 ip nat inside speed auto !---
NAT configuration. ip nat inside source route-map nonat
interface Ethernet0/0 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.202.225 no ip http server ip pim
```

```
bidir-enable !--- Encryption match address access list.
access-list 110 permit ip 172.16.15.0 0.0.0.255
192.168.10.0 0.0.0.255 !--- NAT access list. access-list
120 deny ip 172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10 match ip address 120 line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 password
cisco login end
```

Configurez Checkpoint NG

Le NG du TM de point de reprise est une configuration orientée objets. Des objets de réseau et les règles sont définis de composer la stratégie qui concerne la configuration du VPN à installer. Cette stratégie est alors installée utilisant l'éditeur de stratégie NG du TM de point de reprise pour se terminer le côté NG du TM de point de reprise de la configuration du VPN.

1. Créez le sous-réseau de réseau de Cisco et le sous-réseau de réseau NG du TM de point de reprise comme objets de réseau. C'est ce qui est chiffré. Pour créer les objets, choisis **gérez > des objets de réseau**, puis sélectionnez **nouveau > réseau**. Écrivez l'information réseau appropriée, puis cliquez sur OK.Ces exemples affichent une installation des objets appelés CP_Network et Cisco_Network.
2. Créez les objets de Cisco_Router et de Checkpoint_NG comme objets de poste de travail. Ce sont les périphériques VPN. Pour créer les objets, choisis **gérez > des objets de réseau**, puis sélectionnez **nouveau > poste de travail**.Notez que vous pouvez utiliser l'objet de poste de travail NG du TM de point de reprise créé pendant l'installation initiale NG du TM de point de reprise. Sélectionnez les options de placer le poste de travail comme **passerelle** et **périphérique VPN interopérable**.Ces exemples affichent une installation des objets appelés chef et Cisco_Router.
3. Configurez l'IKE sur l'onglet VPN, puis cliquez sur Edit.
4. Configurez la politique de change principale, et cliquez sur Edit les **secrets**.
5. Placez les clés pré-partagées à utiliser, puis cliquez sur OK plusieurs fois jusqu'à ce que les fenêtres de configuration disparaissent.
6. **Les règles** choisies **> ajoutent les règles > le dessus** pour configurer les règles de cryptage pour la stratégie.La règle sur le dessus est la première règle exécutée avant n'importe quelle autre règle qui peut sauter le cryptage. Configurez la source et la destination pour inclure le CP_Network et le Cisco_Network, comme affiché ici. Une fois que vous avez ajouté la section d'action de chiffrer de la règle, cliquez avec le bouton droit l'**action** et choisi **éditez Properties**.
7. L'IKE sélectionné et étant mis en valeur, cliquez sur Edit.
8. Confirmez la configuration d'IKE.
9. Un des problèmes principaux avec exécuter le VPN entre les périphériques de Cisco et d'autres périphériques d'IPSec est la renégociation de Key Exchange. Assurez-vous que la configuration pour l'échange d'IKE sur le routeur de Cisco est exactement identique que cela configurée sur le NG du TM de point de reprise.**Remarque:** La valeur réelle de ce paramètre dépend de votre stratégie de sécurité entreprise particulière.Dans cet exemple, la configuration d'IKE sur le routeur a été placée à 30 minutes avec la commande de la **vie 1800**. La même valeur doit être placée sur le NG du TM de point de reprise.Pour placer cette valeur sur le NG du TM de point de reprise, choisi **gérez l'objet de réseau**, puis sélectionnez l'objet NG du TM de point de reprise et cliquez sur Edit. Sélectionnez alors le **VPN**, et éditez

l'IKE. Sélectionnez l'**avance** et configurez les paramètres de nouvelle saisie. Après que vous configuriez l'échange clé pour l'objet de réseau NG du$^{TM\ de}$ point de reprise, exécutez la même configuration de la renégociation de Key Exchange pour l'objet de réseau de Cisco_Router.**Remarque:** Assurez-vous que vous faites sélectionner le groupe correct de Diffie-Hellman pour apparier cela configuré sur le routeur.

10. La configuration de politique est complète. Sauvegardez la stratégie et la **stratégie** choisie **> installent** pour l'activer.La fenêtre d'installation affiche des notes en progression pendant que la stratégie est compilée.Quand la fenêtre d'installation indique que l'installation de stratégie est complète, cliquez sur **près de la** finition la procédure.

Vérifiez

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

Vérifiez le routeur de Cisco

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 isakmp sa** - Affiche toutes les associations de sécurité actuelles d'IKE (SA) sur un pair.
- **show crypto ipsec sa—Affiche** les paramètres utilisés par les SA.

Vérifiez Checkpoint NG

Pour visualiser les logs, **fenêtre > visualiseur** choisis de **log**.

Pour visualiser l'état du système, **fenêtre** choisie **> état du système**.

Dépannez

Routeur de Cisco

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

Pour l'information de dépannage supplémentaire, référez-vous s'il vous plaît au dépannage de sécurité IP - en comprenant et en utilisant des commandes de débogage.

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

- **debug crypto engine** — Affiche des messages de débogage au sujet des moteurs de chiffrement, qui exécutent le cryptage et le déchiffrement.
- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug crypto ipsec** — Affiche des événements IPsec.
- **clear crypto isakmp** — Efface toutes les connexions actives d'IKE.
- **clear crypto sa** — Efface tout l'IPSec SAS.

Réussi mettez au point la sortie de log

```
18:05:32: ISAKMP (0:0): received packet from
   209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
   but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
   against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
```

```
   with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PHASE1_COMPLETE
```
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): processing HASH payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing SA payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): Checking IPSec proposal 1 18:05:33: ISAKMP: transform 1, ESP_3DES 18:05:33: ISAKMP: attributes in transform: 18:05:33: ISAKMP: SA life type in seconds 18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10 18:05:33: ISAKMP: authenticator is HMAC-MD5 18:05:33: ISAKMP: encaps is 1 18:05:33: ISAKMP (0:1): atts are acceptable. 18:05:33: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 18:05:33: ISAKMP (0:1): processing NONCE payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA from 209.165.202.226 to 209.165.202.129 for prot 3 18:05:33: ISAKMP: received ke message (2/1) 18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Creating IPSec SAs 18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226 (proxy 192.168.10.0 to 172.16.15.0) 18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4 18:05:33: lifetime of 3600 seconds 18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129 (proxy 172.16.15.0 to 192.168.10.0) 18:05:33: has spi -2006413528 and conn_id 201 and flags C 18:05:33: lifetime of 3600 seconds 18:05:33: ISAKMP (0:1): deleting node -1335371103 error FALSE reason "quick mode done (await()" 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE** 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0, flags= 0x4 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0, flags= 0xC 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.226, sa_prot= 50, sa_spi= 0x800022D3(2147492563), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.129, sa_prot= 50, sa_spi= 0x88688F28(2288553768), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201 18:05:34: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 18:05:34: ISAKMP (0:1): received packet from
```
```

209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 sv1-6#**show crypto isakmp sa** dst src state conn-id slot 209.165.202.226 209.165.202.129 QM_IDLE 1 0 sv1-6#**show crypto ipsec sa** interface: Ethernet0/0 Crypto map tag: aptmap, local addr. 209.165.202.226 local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) current_peer: 209.165.202.129 PERMIT, flags={origin_is_acl,} **#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21 #pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24** #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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129 path mtu 1500, media mtu 1500 current outbound spi: 88688F28 inbound esp sas: spi: 0x800022D3(2147492563) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3559) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x88688F28(2288553768) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3550) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: sv1-6#**show crypto engine conn act** ID Interface IP- Address State Algorithm Encrypt Decrypt 1 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0 200 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 **24** 201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C **21** 0

Informations connexes

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