Configuration d'un tunnel IPsec entre un routeur Cisco et un pare-feu Checkpoint Firewall 4.1

Contenu

Introduction

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés : le réseau privé 192.168.1.x interne au routeur Cisco et le réseau privé 10.32.50.x interne au Pare-feu checkpoint.

Conditions préalables

Conditions requises

Cette configuration d'échantillon suppose que le trafic de l'intérieur du routeur et de l'intérieur que le point de reprise à l'Internet (représenté ici par les réseaux 172.18.124.x) circule avant que vous commenciez la configuration.

Composants utilisés

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

- Routeur de Cisco 3600

- Logiciel de Cisco IOS® (C3640-JO3S56I-M), version 12.1(5)T, LOGICIEL de RELEASE (fc1)
- Pare-feu checkpoint 4.1

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.

- Configuration du routeur
- Configuration de pare-feu checkpoint

Configuration du routeur

Configuration de routeur de Cisco 3600

```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
```

```
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1 authentication pre-share crypto isakmp
key ciscorules address 172.18.124.157 ! !--- IPsec
configuration crypto ipsec transform-set rtpset esp-des
esp-sha-hmac ! crypto map rtp 1 ipsec-isakmp set peer
172.18.124.157 set transform-set rtpset match address
115 ! call rsvp-sync cns event-service server !
controller T1 1/0 ! controller T1 1/1 ! interface
Ethernet0/0 ip address 172.18.124.35 255.255.255.240 ip
nat outside no ip mroute-cache half-duplex crypto map
rtp ! interface Ethernet0/1 ip address 192.168.1.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet1/0 no ip address shutdown duplex auto speed
auto ! ip kerberos source-interface any ip nat pool
INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240 ip nat inside source route-map nonat
pool INTERNET ip classless ip route 0.0.0.0 0.0.0.0
172.18.124.34 no ip http server ! access-list 101 deny
ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 access-
list 101 permit ip 192.168.1.0 0.0.0.255 any access-list
115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any route-
map nonat permit 10 match ip address 101 ! dial-peer cor
custom ! line con 0 transport input none line aux 0 line
vty 0 4 login ! end
```

Configuration de pare-feu checkpoint

Terminez-vous ces étapes pour configurer le pare-feu checkpoint.

1. Puisque l'IKE et les vies par défaut d'IPsec diffèrent entre les constructeurs, **Properties** choisi **> cryptage** pour placer les durées de vie du point de contrôle pour être d'accord avec les valeurs par défaut de Cisco.La vie d'IKE de valeur par défaut de Cisco est de 86400 secondes (= 1440 minutes), et elle peut être modifiée par ces commandes :**crypto isakmp policy #vie #**La vie configurable d'IKE de Cisco a lieu de 60-86400 secondes. La vie d'IPsec de valeur par défaut de Cisco est de 3600 secondes, et elle peut être modifiée par le **crypto ipsec security-association lifetime seconde #** commande.La vie configurable de Cisco IPsec a lieu de 120-86400 secondes.
2. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour le réseau interne (appelé le « cpinside ») derrière le point de reprise.Ceci devrait être conforme au réseau de destination (en second lieu) dans la commande de **192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 d'IP d'autorisation de la liste d'accès 115 de** Cisco.Emplacement de dessous **interne** choisi.
3. Choisi **gérez > des objets de réseau > éditent** pour éditer l'objet pour le point final de point de reprise RTPCPVPN (passerelle) ce les points de routeur de Cisco à dans la commande de **172.18.124.157 de pair de positionnement**.Emplacement de dessous **interne** choisi. Pour le type, **passerelle** choisie. Sous des modules installés, sélectionnez la case **VPN-1 et FireWall-1**, et sélectionnez également la **case à cocher Station de gestion** :
4. Choisi **gérez > des objets de réseau > nouveau > réseau** pour configurer l'objet pour le réseau externe (appelé le « inside_cisco ») derrière le routeur de Cisco.Ceci devrait être conforme au premier) réseau de source (dans la commande de **192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 d'IP d'autorisation de la liste d'accès 115 de** Cisco.Emplacement de dessous **externe** choisi.

5. Choisi **gérez > des objets de réseau > nouveau > poste de travail** pour ajouter un objet pour la passerelle externe de routeur de Cisco (appelée le « cisco_endpoint »). C'est l'interface Cisco à laquelle la commande de **nom de carte de chiffrement** est appliquée.Emplacement de dessous **externe** choisi. Pour le type, **passerelle** choisie.**Remarque:** Ne sélectionnez pas la case VPN-1/FireWall-1.
6. Choisi **gérez > des objets de réseau > éditent** pour éditer onglet VPN de point d'extrémité de passerelle avec point de contrôle (appelé le le « RTPCPVPN »). Sous le domaine, sélectionnez **autre** et puis sélectionnez l'intérieur du réseau de points de contrôle (appelé le « cpinside ») de la liste déroulante. Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit alors.
7. Changez les propriétés IKE pour le chiffrement DES pour être d'accord avec ces commandes :**crypto isakmp policy #DES de cryptageRemarque:** Le chiffrement DES est le par défaut ainsi il n'est pas visible dans la configuration de Cisco.
8. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec ces commandes :**crypto isakmp policy #SHA d'informations parasitesRemarque:** L'algorithme de hachage de SHA est le par défaut ainsi il n'est pas visible dans la configuration de Cisco.Changez ces configurations :Retirez le **mode agressif**.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à ces commandes :**crypto isakmp policy #authentication pre-share**
9. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la commande d'**address address de** *clé de* **crypto isakmp key de** Cisco :
10. Choisi **gérez > des objets de réseau > éditent** pour éditer l'onglet VPN de « cisco_endpoint ». Sous le domaine, sélectionnez **autre**, et puis sélectionnez l'intérieur du réseau de Cisco (appelé le « inside_cisco »). Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit alors.
11. Changez le chiffrement DES de propriétés IKE pour être d'accord avec ces commandes :**crypto isakmp policy #DES de cryptageRemarque:** Le chiffrement DES est le par défaut ainsi il n'est pas visible dans la configuration de Cisco.
12. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec ces commandes :**crypto isakmp policy #SHA d'informations parasitesRemarque:** L'algorithme de hachage de SHA est le par défaut ainsi il n'est pas visible dans la configuration de Cisco.Changez ces configurations :Retirez le **mode agressif**.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à ces commandes :**crypto isakmp policy #authentication pre-share**
13. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la commande Cisco d'**address address de** *clé de* **crypto isakmp key**.
14. Dans la fenêtre de l'éditeur de stratégie, insérez une règle avec la source et la destination en tant que le « inside_cisco » et « cpinside » (bidirectionnel). Placez **Service=Any**, **Action=Encrypt**, et **Track=Long**.
15. Cliquez sur l'icône verte chiffrement et choisi **éditez les propriétés** pour configurer des stratégies de chiffrement sous le titre d'action.
16. **L'IKE** choisi, et cliquent sur Edit alors.
17. Sur la fenêtre de propriétés IKE, changez ces propriétés pour être d'accord avec Cisco IPsec transforme dans la commande d'ESP-**SHA-hmac ESP-DES de rtpset de crypto ipsec transform-set** :Sous transformez, **cryptage + intégrité des données** choisis **(ESP)**. L'algorithme de chiffrement devrait être **DES**, intégrité des données devrait être **SHA1**, et la passerelle homologue permise devrait être la passerelle de routeur externe (appelée le « cisco_endpoint »). Cliquez sur **OK**.

18. Après que vous configuriez le point de reprise, la **stratégie** choisie **> installent** sur le menu du point de contrôle pour faire les prendre effet les modifications.

Vérifiez

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

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** .

- **show crypto isakmp sa** — Visualisez toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** — Visualisez les configurations utilisées par le courant SAS.

Dépannez

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

Dépannage des commandes

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

- **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.

Récapitulation de réseau

Quand des réseaux intérieurs adjacents de multiple sont configurés dans le domaine de cryptage sur le point de reprise, le périphérique pourrait automatiquement les récapituler en ce qui concerne le trafic intéressant. Si le routeur n'est pas configuré pour être assorti, le tunnel est susceptible d'échouer. Par exemple, si les réseaux intérieurs de 10.0.0.0 /24 et de 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ils pourraient être récapitulés à 10.0.0.0 /23.

Point de reprise

Puisque le cheminement a été placé pour long dans la fenêtre de l'éditeur de stratégie, refusé le trafic devrait apparaître en rouge dans le visualiseur de log. Plus bavard mettez au point peut être obtenu avec :

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

et dans une autre fenêtre :

```
C:\WINNT\FW1\4.1\fwstart
```

Remarque: C'était une installation de NT de Microsoft Windows.

Émettez ces commandes d'effacer SAS sur le point de reprise :

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

La réponse **oui au** sont vous sure ? demande.

Exemple de sortie de débogage

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp Crypto ISAKMP debugging is on cisco_endpoint#debug crypto
isakmp Crypto IPSEC debugging is on cisco_endpoint#debug crypto engine Crypto Engine debugging
is on cisco_endpoint# 20:54:06: IPSEC(sa_request): , (key eng. msg.) src= 172.18.124.35, dest=
172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1) 20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_NO_STATE 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_NO_STATE 20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0 20:54:06: ISAKMP
(0:1): found peer pre-shared key matching 172.18.124.157 20:54:06: ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy 20:54:06: ISAKMP: encryption DES-CBC 20:54:06: ISAKMP:
hash SHA 20:54:06: ISAKMP: default group 1 20:54:06: ISAKMP: auth pre-share 20:54:06: ISAKMP
(0:1): atts are acceptable. Next payload is 0 20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0 20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1):
received packet from 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1): processing KE
payload. message ID = 0 20:54:06: CryptoEngine0: generate alg parameter 20:54:06: ISAKMP (0:1):
processing NONCE payload. message ID = 0 20:54:06: ISAKMP (0:1): found peer pre-shared key
matching 172.18.124.157 20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1 20:54:06:
ISAKMP (0:1): SKEYID state generated 20:54:06: ISAKMP (1): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 20:54:06: ISAKMP (1): Total payload length: 12 20:54:06:
CryptoEngine0: generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_KEY_EXCH 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_KEY_EXCH 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0 20:54:06: ISAKMP
(0:1): processing HASH payload. message ID = 0 20:54:06: CryptoEngine0: generate hmac context
for conn id 1 20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157 20:54:06:
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 20:54:06: CryptoEngine0:
generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I)
QM_IDLE 20:54:06: CryptoEngine0: clear dh number for conn id 1 20:54:06: ISAKMP (0:1): received
packet from 172.18.124.157 (I) QM_IDLE 20:54:06: CryptoEngine0: generate hmac context for conn
id 1 20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267 20:54:06: ISAKMP
(0:1): processing SA payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): Checking IPSec
proposal 1 20:54:06: ISAKMP: transform 1, ESP_DES 20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1 20:54:06: ISAKMP: SA life type in seconds 20:54:06: ISAKMP: SA
life duration (basic) of 3600 20:54:06: ISAKMP: SA life type in kilobytes 20:54:06: ISAKMP: SA
life duration (VPI) of 0x0 0x46 0x50 0x0 20:54:06: ISAKMP: authenticator is HMAC-SHA 20:54:06:
validate proposal 0 20:54:06: ISAKMP (0:1): atts are acceptable. 20:54:06:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src=
172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 20:54:06: validate proposal
request 0 20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 20:54:06:
ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing
ID payload. message ID = 1855173267 20:54:06: CryptoEngine0: generate hmac context for conn id 1
```

```
20:54:06: ipsec allocate flow 0 20:54:06: ipsec allocate flow 0 20:54:06: ISAKMP (0:1): Creating
IPSec SAs 20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to
192.168.1.0) 20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4 20:54:06: lifetime of
3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: outbound SA from 172.18.124.35 to
172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) 20:54:06: has spi 404516441 and conn_id 2001
and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06:
ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE 20:54:06: ISAKMP (0:1): deleting node
1855173267 error FALSE reason "" 20:54:06: IPSEC(key_engine): got a queue event... 20:54:06:
IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157, dest_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4 20:54:06: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4 20:54:06: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0xA29984CA(2727969994), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 2000 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest=
172.18.124.157, sa_prot= 50, sa_spi= 0x181C6E59(404516441), sa_trans= esp-des esp-sha-hmac ,
sa_conn_id= 2001 cisco_endpoint#sho cry ips sa interface: Ethernet0/0 Crypto map tag: rtp, local
addr. 172.18.124.35 local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote
ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT,
flags={origin_is_acl,} #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14 #pkts decaps: 14,
#pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 1, #recv errors
0 local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, media
mtu 1500 current outbound spi: 181C6E59 inbound esp sas: spi: 0xA29984CA(2727969994) transform:
esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: rtp --More-- sa timing: remaining key lifetime (k/sec): (4607998/3447) IV size: 8 bytes
replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x181C6E59(404516441) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key lifetime (k/sec):
(4607997/3447) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
cisco_endpoint#show crypto isakmp sa dst src state conn-id slot 172.18.124.157 172.18.124.35
QM_IDLE 1 0 cisco_endpoint#exit
```

Informations connexes

- Négociation IPSec/Protocoles IKE
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Support et documentation techniques - Cisco Systems