Exemple de configuration de génération de clé manuelle IPSec entre routeurs

Contenu

Introduction

Cet exemple de configuration vous permet de chiffrer le trafic entre les réseaux 12.12.12.x et 14.14.14.x à l'aide de la saisie manuelle de la clé IPsec. Aux fins du test, une liste de contrôle d'accès (ACL) et un ping étendu envoyé de l'hôte du réseau 12.12.12.12 au réseau 14.14.14.14 ont été utilisés.

L'introduction de manuel est habituellement seulement nécessaire quand un périphérique de Cisco est configuré pour chiffrer le trafic au périphérique d'un autre constructeur qui ne prend en charge pas l'Échange de clés Internet (IKE). Si l'IKE est configurable sur les deux périphériques, il est préférable d'utiliser l'introduction automatique. Les index de paramètre de sécurité des périphériques de Cisco (SPI) sont dans la décimale cependant que quelques constructeurs font des SPI dans l'hexadécimal. Si c'est le cas, alors parfois la conversion est nécessaire.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique 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 :

- Cisco 3640 et 1605 Routeurs
- Version de logiciel 12.3.3.a de Cisco IOS®

Remarque: Sur toutes les Plateformes qui contiennent des adaptateurs de chiffrement matériel, le cryptage manuel n'est pas pris en charge quand l'adaptateur de chiffrement matériel est activé.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est actif, assurez-vous de bien comprendre l'incidence potentielle de chaque commande avant de l'utiliser.

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 légère
- Configuration de Chambre

Configuration légère

```
light#show running-config Building configuration...
Current configuration : 1177 bytes ! version 12.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname light ! boot-start-marker boot-
end-marker ! enable password cisco ! no aaa new-model ip
subnet-zero ! no crypto isakmp enable ! !--- IPsec
configuration crypto ipsec transform-set encrypt-des
esp-des esp-sha-hmac ! ! crypto map testcase 8 ipsec-
manual set peer 11.11.11.12 set session-key inbound esp
1001 cipher 1234abcd1234abcd authenticator 20 set
```

```
session-key outbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set transform-set encrypt-des !---
Traffic to encrypt match address 100 ! ! interface
Ethernet2/0 ip address 12.12.12.12 255.255.255.0 half-
duplex<br>! interface Ethernet2/1 ip address 11.11.11.11
255.255.255.0 half-duplex !--- Apply crypto map. crypto
map testcase ! ip http server no ip http secure-server
ip classless ip route 0.0.0.0 0.0.0.0 11.11.11.12 ! ! !-
-- Traffic to encrypt access-list 100 permit ip host
12.12.12.12 host 14.14.14.14 ! ! ! ! line con 0 line aux
0 line vty 0 4 login ! ! !
```

Configuration de Chambre

```
house#show running-config Current configuration : 1194
bytes ! version 12.3 service timestamps debug uptime
service timestamps log uptime no service password-
encryption ! hostname house ! ! logging buffered 50000
debugging enable password cisco ! no aaa new-model ip
subnet-zero ip domain name cisco.com ! ip cef ! ! no
crypto isakmp enable ! ! !--- IPsec configuration crypto
ipsec transform-set encrypt-des esp-des esp-sha-hmac !
crypto map testcase 8 ipsec-manual set peer 11.11.11.11
set session-key inbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set session-key outbound esp 1001
cipher 1234abcd1234abcd authenticator 20 set transform-
set encrypt-des !--- Traffic to encrypt match address
100 ! ! interface Ethernet0 ip address 11.11.11.12
255.255.255.0 !--- Apply crypto map. crypto map testcase
! interface Ethernet1 ip address 14.14.14.14
255.255.255.0 ! ip classless ip route 0.0.0.0 0.0.0.0
11.11.11.11 no ip http server no ip http secure-server !
! !--- Traffic to encrypt access-list 100 permit ip host
14.14.14.14 host 12.12.12.12 ! ! line con 0 exec-timeout
0 0 transport preferred none transport output none line
vty 0 4 exec-timeout 0 0 password cisco login transport
preferred none transport input none transport output
none ! ! end
```

Vérifiez

Cette section fournit des informations que vous pouvez employer pour confirmer vos fonctions de configuration 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 ipsec sa** — Affiche à la phase deux associations de sécurité.

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 deux.
- **debug crypto engine** — Affiche le trafic qui est chiffré.

Les jeux de transformations ne s'assortissent pas

La lumière a l'oh-SHA-hmac et la Chambre a l'ESP-DES.

```
*Mar  2 01:16:09.849: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 11.11.11.11, remote= 11.11.11.12,
    local_proxy= 12.12.12.12/255.255.255.255/0/0 (type=1),
    remote_proxy= 14.14.14.14/255.255.255.255/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xACD76816(2899798038), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  2 01:16:09.849: IPSEC(manual_key_stuffing):
keys missing for addr 11.11.11.12/prot 51/spi 0.....
```

ACLs ne s'assortissent pas

Sur le side_A (routeur) « léger » il y a un hôte-à-à l'intérieur-hôte intérieur et sur le side_B (le routeur de « maison ») il y a une interface-à-interface. ACLs doit toujours être symétrique (ceux-ci ne sont pas).

```
hostname house
match address 101
access-list 101 permit ip host 11.11.11.12 host 11.11.11.11
!

hostname light
match address 100
access-list 100 permit ip host 12.12.12.12 host 14.14.14.14
```

Cette sortie est prise du side_A initiant le ping :

```
nothing

light#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet2/1 11.11.11.11 set DES_56_CBC 5 0 2001 Ethernet2/1 11.11.11.11 set
DES_56_CBC 0 0
```

Cette sortie est prise du side_B quand le side_A initie le ping :

```
house#
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check


house#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet0 11.11.11.12 set DES_56_CBC 0 0 2001 Ethernet0 11.11.11.12 set DES_56_CBC
0 5
```

Cette sortie est prise du side_B initiant le ping :

```
side_ B
```

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
        (ip) vrf/dest_addr= /12.12.12.12, src_addr= 14.14.14.14, prot= 1
```

Un côté a le crypto map et l'autre ne fait pas

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
        (ip) vrf/dest_addr= /14.14.14.14, src_addr= 12.12.12.12, prot= 1
```

Cette sortie est prise du side_B qui a un crypto map :

```
house#show crypto engine connections active
 ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
2000 Ethernet0       11.11.11.12     set    DES_56_CBC                5        0
2001 Ethernet0       11.11.11.12     set    DES_56_CBC                0        0
```

La carte de crypto engine accelerator est activée

```
1d05h: %HW_VPN-1-HPRXERR: Hardware VPN0/13: Packet
 Encryption/Decryption error, status=4098.....
```

Informations connexes

- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems