Configuratievoorbeeld van IPSec handmatig toetsen tussen routers

Inhoud

Inleiding

Met deze voorbeeldconfiguratie kunt u met behulp van IPsec handmatige vastlegging het verkeer tussen de 12.12.12.x en de 14.14.x-netwerken versleutelen. Voor testdoeleinden werd een toegangscontrolelijst (ACL) gebruikt, die is uitgebreid van host 12.12.12.12 tot 14.14.14.14.

Het handmatig vastzetten is meestal alleen nodig wanneer een Cisco-apparaat is geconfigureerd om het verkeer naar het apparaat van een andere verkoper te versleutelen, dat geen Internet Key Exchange (IKE) ondersteunt. Als IKE op beide apparaten configureerbaar is, is het beter om automatisch te controleren. Cisco device security parameter-indexen (SPI's) zijn in decimale volgorde, maar sommige verkopers doen SPI's in hexadecimaal. Als dit het geval is, is soms conversie nodig.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 3640 en 1605 routers
- Cisco IOS® softwarerelease 12.3.3.a

Opmerking: Op alle platforms die hardwareencryptie-adapters bevatten, wordt handmatige codering niet ondersteund als de hardwareencryptie-adapter is ingeschakeld.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk leeft, zorg ervoor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens u het gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

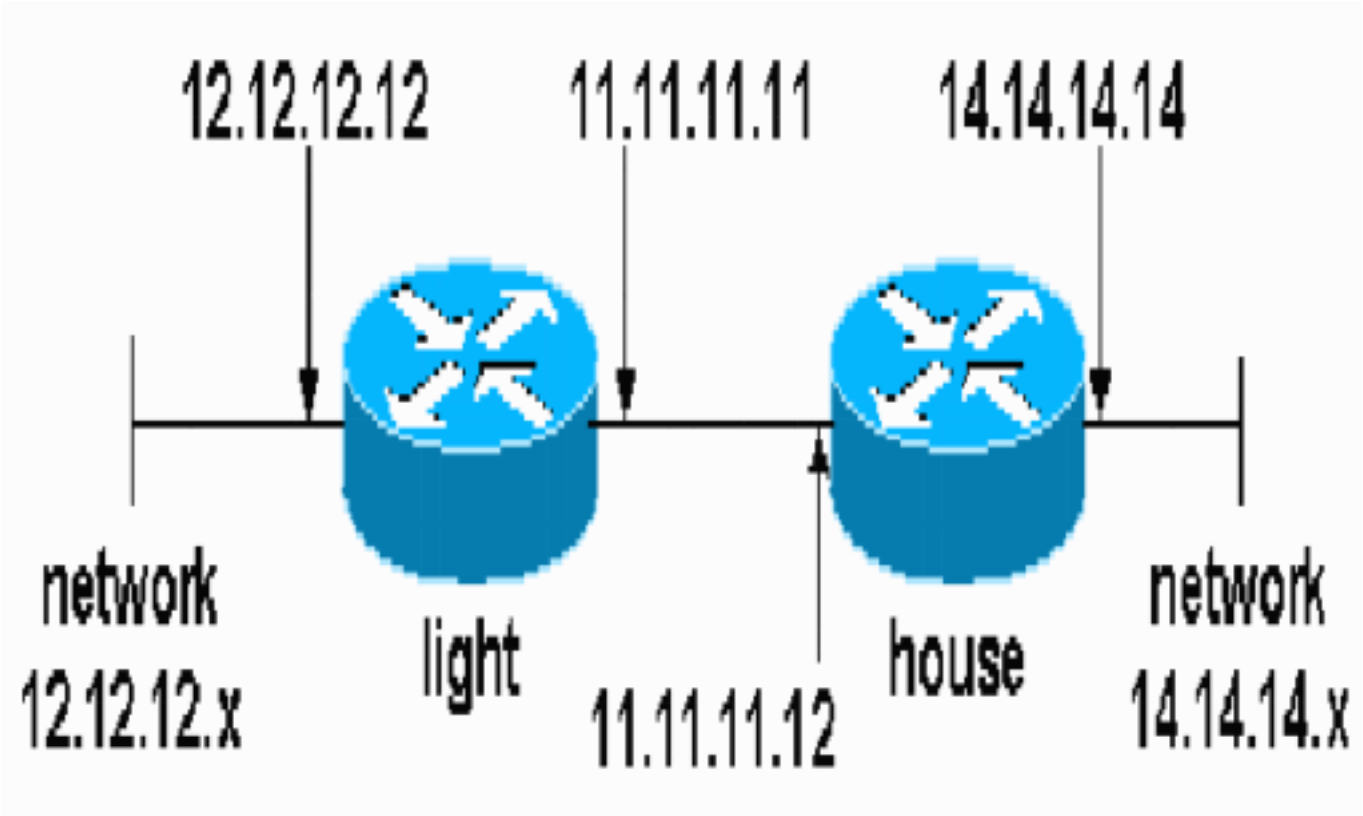
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- Lichtconfiguratie
- Configuratie thuis

Lichtconfiguratie

```
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
!
!
!
```

Configuratie thuis

```
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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om de configuratiefuncties correct te bevestigen.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon crypto ipsec sa**-shows the fase twee security associaties.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec**-displays de IPsec-onderhandelingen van fase twee.
- **debug van crypto motor**-displays het verkeer dat versleuteld wordt.

Transformeer reeksen komen niet overeen

Licht heeft ah-sha-hmac en House heeft 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.....
```

ACL's komen niet overeen

Aan side_A (de "lichtrouter") is er een binnen host-to-interne-host en aan side_B (de "huis" router) is er een interface-to-interface. ACL's moeten altijd symmetrisch zijn (dit is niet het geval).

```
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
```

Deze output wordt overgenomen van side_A die pingelt:

```
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
```

Deze output wordt van side_B gehaald wanneer side_A begint met 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
```

Deze output wordt overgenomen van side_B initierend 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
```

De ene kant heeft crypto kaart en de andere niet

```
%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
```

Deze output wordt afgeleid van side_B die een crypto kaart heeft:

```
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
```

De Crypto Engine Accelerator-kaart is ingeschakeld

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

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems