Ejemplo de Configuración de Clave Manual IPSec entre Routers

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshoot](#)
[Comandos para resolución de problemas](#)
[Los comandos transform set no coinciden](#)
[Los ACL no coinciden](#)
[Un lado tiene cripto map (correspondencia de criptografía) y el otro no](#)
[Está habilitada la tarjeta del acelerador del motor de criptografía](#)
[Información Relacionada](#)

Introducción

Esta configuración de ejemplo permite que cifrar el tráfico entre las redes 12.12.12.x y 14.14.14.x con la ayuda de claves IPsec generadas manualmente. Con fines de prueba, se utilizaron una lista de control de acceso (ACL) y ping extendido desde el host 12.12.12.12 al 14.14.14.14.

Normalmente, la clave manual solo es necesaria cuando un dispositivo de Cisco está configurado para cifrar el tráfico al dispositivo de otro proveedor que no es compatible con el intercambio de claves de Internet (IKE). Si IKE se puede configurar en ambos dispositivos, es preferible utilizar la clave automática. Los índices de parámetros de seguridad de dispositivos (SPI) de Cisco se expresan en números decimales; sin embargo, algunos proveedores utilizan SPI en números hexadecimales. Si este es el caso, entonces a veces la conversión es necesaria.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers 3640 y 1605 de Cisco
- Software Cisco IOS® versión 12.3.3.a

Nota: En todas las plataformas que contienen adaptadores de cifrado de hardware, el cifrado manual no se admite cuando el adaptador de cifrado de hardware está habilitado.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando antes de utilizarla.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

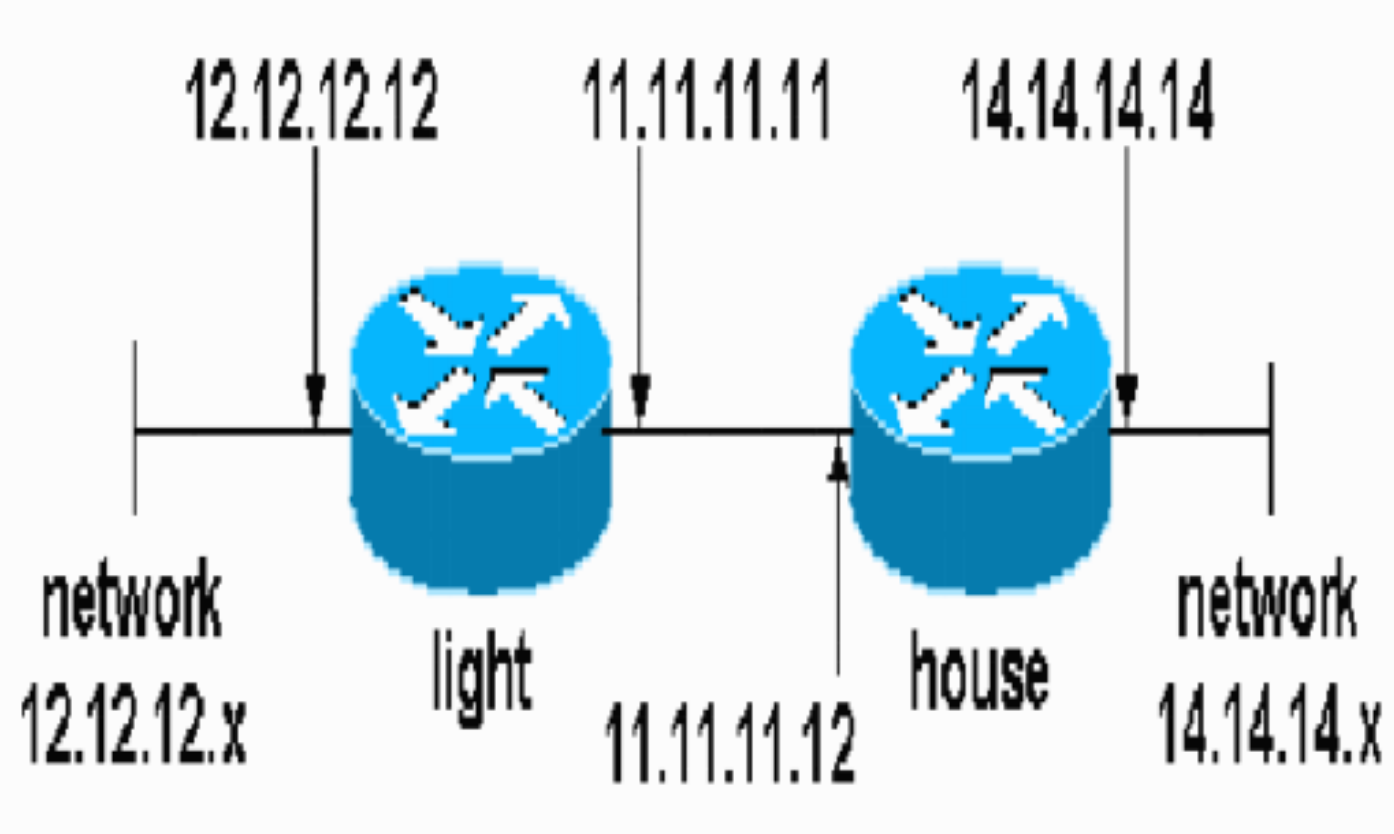
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta de búsqueda de comandos (solo para clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de luz
- Configuración base

Configuración de luz

<#root>

```
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
!
!
!
```

Configuración base

<#root>

```
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
```

Verificación

Esta sección proporciona información que puede utilizar para confirmar las funciones de configuración correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto ipsec sa—Muestra las asociaciones de seguridad de la fase dos.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

- debug crypto ipsec—Muestra las negociaciones IPSec de la fase dos.
- debug crypto engine: muestra el tráfico que está cifrado.

Los comandos transform set no coinciden

light tiene ah-sha-hmac y house tiene 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.....
```

Los ACL no coinciden

En side_A (el router “light”) existe un host a host interior y en side_B (el router “house”) existe una interfaz a interfaz. Las ACL deben ser siempre simétricas (no lo son).

```
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
```

Este resultado se toma del ping de inicio side_A:

<#root>

```
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
```

Esta salida se toma del side_B cuando side_A está iniciando el ping:

<#root>

```
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
```

Este resultado se toma del ping de inicio side_B:

```
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 lado tiene cripto map (correspondencia de criptografía) y el otro no

```
%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
```

Este resultado se toma del side_B que tiene un mapa criptográfico:

```
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
```

Está habilitada la tarjeta del acelerador del motor de criptografía

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

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).