

在路由器配置示例之间的IPSec手工密钥

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[转换集不匹配](#)

[ACL 不匹配](#)

[一端有加密映射，另一端没有](#)

[Crypto 引擎加速卡启用](#)

[相关信息](#)

简介

此示例配置允许您在 IPSec 手动密钥设置的帮助下加密 12.12.12.x 和 14.14.14.x 网络之间的数据流。出于测试目的，使用主机 12.12.12.12 至 14.14.14.14 的访问控制列表 (ACL) 和扩展 ping。

仅当 Cisco 设备配置为将数据流加密至不支持 Internet 密钥交换 (IKE) 的另一供应商设备时，才需要手动密钥设置。如果 IKE 在两个设备上均可配置，则最好使用自动密钥设置。Cisco 设备安全参数索引 (SPI) 采用十进制，但某些供应商的 SPI 采用十六进制。在这种情况下，有时需要进行转换。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 3640 及 1605 路由器

- Cisco IOS® 软件版本 12.3.3.a

注意： 在所有包含硬件加密适配器的平台上，当硬件加密适配器启用时，不支持手动加密。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络是活的，在您使用指令前请切记您了解所有指令潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用 [命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- [Light 配置](#)
- [House 配置](#)

Light 配置

```
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 ! ! !
```

House 配置

```
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
```

验证

此部分提供您能使用的确认您的配置功能的信息。

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa** - 显示第 2 阶段的安全关联。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto engine** - 显示已加密的流量。

转换集不匹配

Light 具有 ah-sha-hmac，而 House 具有 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 不匹配

在 side_A (“light”路由器) 端为内部主机到内部主机，而在 side_B (“house”路由器) 端为接口到接口。ACL 必须始终对称 (而这些不对称) 。

```
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
```

此输出来自 side_A 启动 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
```

当 side_A 启动 ping 时，此输出来自 side_B :

```
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
```

此输出来自 side_B 启动 ping :

```
side_ B
```

```
%CRYPTO-4-RECV_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
```

一端有加密映射，另一端没有

```
%CRYPTO-4-RECV_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
```

此输出来自具有加密映射的 side_B :

```
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
```

Crypto 引擎加速卡启用

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

相关信息

- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)