IPsec Manual Keying Between Routers Configuration Example

Document ID: 14140

Contents

Introduction

This sample configuration allows you to encrypt traffic between the 12.12.12.x and the 14.14.14.x networks with the help of IPsec manual keying. For test purposes, an access control list (ACL) and extended ping from host 12.12.12.12 to 14.14.14.14 were used.

Manual keying is usually only necessary when a Cisco device is configured to encrypt traffic to another vendor's device which does not support Internet Key Exchange (IKE). If IKE is configurable on both devices, it is preferable to use automatic keying. Cisco device security parameter indexes (SPIs) are in decimal however some vendors do SPIs in hexadecimal. If this is the case, then sometimes conversion is needed.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 3640 and 1605 routers
- Cisco IOS® Software Release 12.3.3.a

Note: On all platforms that contain hardware encryption adapters, manual encryption is not supported when the hardware encryption adapter is enabled.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command before you use it.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

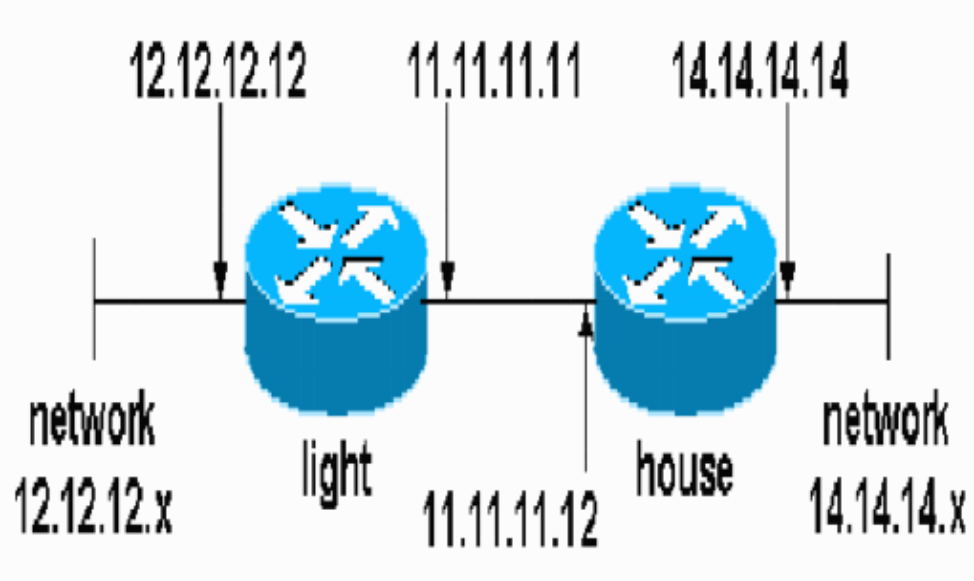
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Light Configuration
- House Configuration

Light Configuration

```
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 Configuration

```
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
```

Verify

This section provides information you can use to confirm your configuration functions properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto ipsec sa** Shows the phase two security associations.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays the IPsec negotiations of phase two.
- **debug crypto engine** Displays the traffic that is encrypted.

Transform Sets Do Not Match

Light has ah-sha-hmac and House has 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 Do Not Match

On side_A (the "light" router) there is an inside host-to-inside-host and on side_B (the "house" router) there is an interface-to-interface. ACLs must always be symmetric (these are not).

```
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
```

This output is taken from the side_A initiating 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
```

This output is taken from the side_B when side_A is initiating 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
```

This output is taken from the side_B initiating 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
```

One Side has crypto map and the Other Does Not

```
%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
```

This output is taken from the side_B that has a 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
```

The Crypto Engine Accelerator Card is Enabled

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

Related Information

- **IPsec Negotiation/IKE Protocols**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 29, 2006 Document ID: 14140