ルータ間での IPSec キーの手入力による設定例

内容

概要

この設定例では、IPSec キーの手入力により 12.12.12.x と 14.14.14.x のネットワーク間のトラフィックを暗号化することができます。ここでは、Access Control List（ACL; アクセス コントロール リスト）と、ホスト 12.12.12.12 からホスト 14.14.14.14 への拡張 ping を、テストの目的で使用しています

通常、キーの手入力が必要となるのは、Internet Key Exchange（IKE; インターネット鍵交換）をサポートしていない他ベンダーのデバイスへのトラフィックを暗号化するようにシスコのデバイスを設定する場合だけです。 両方のデバイスで IKE が設定できる場合は、自動キーを使用することをお勧めします。シスコ デバイスのセキュリティ パラメータ インデックス（SPI）は 10 進数ですが、一部のベンダーは 16 進数の SPI を採用しています。その場合、変換が必要なことがあります。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 3640 および 1605 ルータ
- Cisco IOS® ソフトウェア リリース 12.3.3.a

注：ハードウェア暗号化アダプタを含むすべてのプラットフォームでは、ハードウェア暗号化アダプタが有効になっている場合は、手動暗号化はサポートされません。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが実稼働中である場合は、コマンドを使用する前に、コマンドによる潜在的な影響について理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

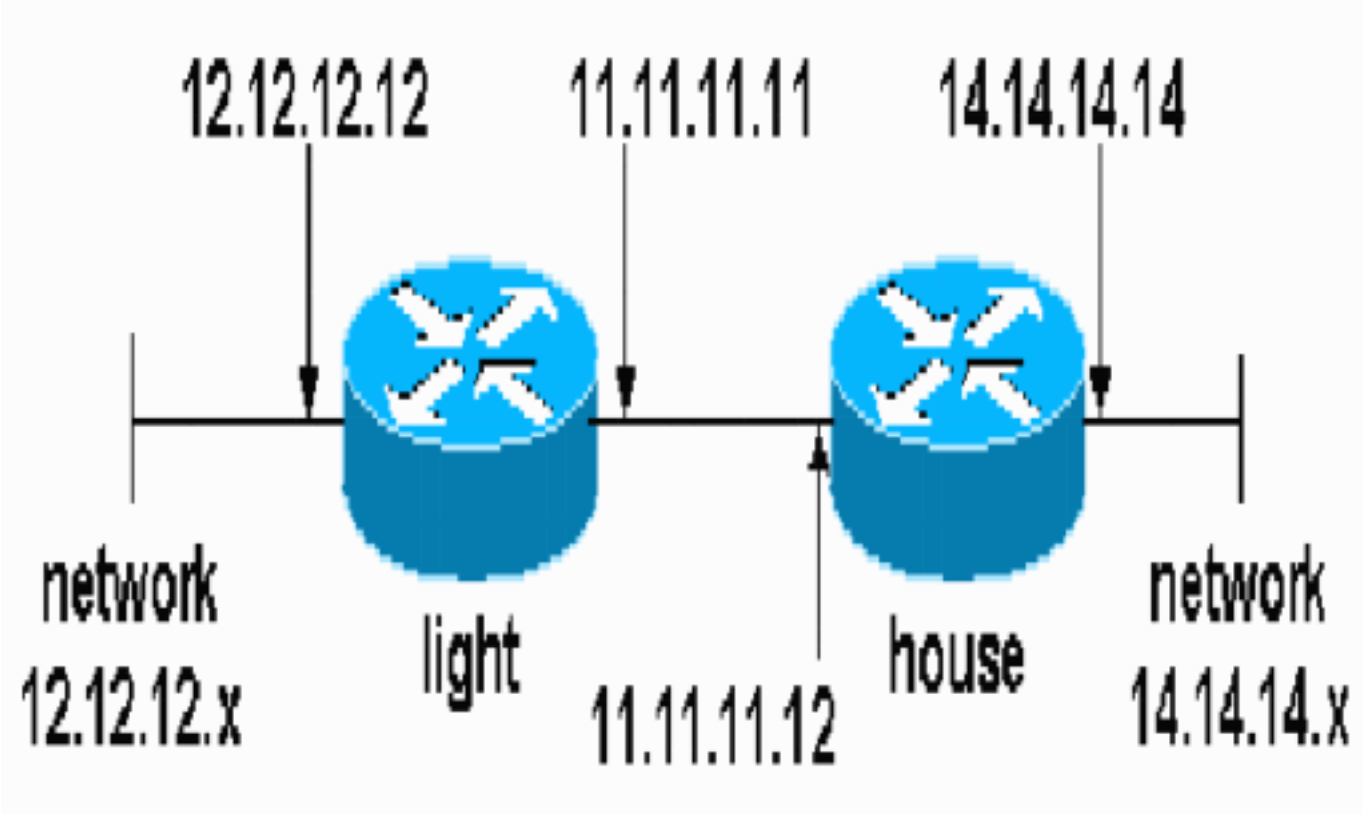
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- Light の設定
- House の設定

Light の設定

```
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 の設定

```
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
```

確認

このセクションでは、設定が正常に機能するかどうかを確認する際に役立つ情報を示しています。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show crypto ipsec sa**：フェーズ2のセキュリティアソシエーションを表示します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec**：フェーズ2のIPSecネゴシエーションを表示します。
- **debug crypto engine - 暗号化されたトラフィックを表示します。**

トランスフォーム セットが一致しない

Light では ah-sha-hmac、House では 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 が一致しない

side_A（「light」ルータ）では、内側のホストから内側のホストへの ACL が、side_B（「house」ルータ）では、インターフェイスからインターフェイスへの ACL が設定されています。ACL は常に対称である必要があります（この場合は対称ではありません）。

```
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
```

これは、ping を開始する side_A の出力です。

```
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
```

これは、side_A が ping を開始した場合の side_B の出力です。

```
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
```

これは、ping を開始する side_B の出力です。

```
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
```

一方には暗号マップがあるが、もう一方にはない

```
%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
```

これは、暗号マップがある side_B の出力です。

```
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 エンジンのアクセラレータ カードがイネーブルになっている

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

関連情報

- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems