# Konfigurationsbeispiel für das manuelle Keying von IPSec zwischen Routern

## Inhalt



## Einführung

Mit dieser Beispielkonfiguration können Sie den Datenverkehr zwischen den Netzwerken 12.12.12.x und 14.14.14.x mithilfe der manuellen IPsec-Keying verschlüsseln. Zu Testzwecken wurden eine Zugriffskontrollliste (ACL) und ein erweiterter Ping von Host 12.12.12 bis 14.14.14.14 verwendet.

Eine manuelle Keying ist in der Regel nur erforderlich, wenn ein Cisco Gerät so konfiguriert ist, dass der Datenverkehr auf dem Gerät eines anderen Anbieters verschlüsselt wird, das Internet Key Exchange (IKE) nicht unterstützt. Wenn IKE auf beiden Geräten konfiguriert werden kann, empfiehlt es sich, die automatische Keying-Funktion zu verwenden. Die Cisco Device Security Parameter Indixes (SPIs) sind dezimal, einige Anbieter verwenden SPIs jedoch hexadezimal. In diesem Fall ist manchmal eine Konvertierung erforderlich.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router 3640 und 1605
- Cisco IOS® Softwareversion 12.3.3.a

**Hinweis:** Auf allen Plattformen, die Hardware-Verschlüsselungsadapter enthalten, wird die manuelle Verschlüsselung nicht unterstützt, wenn der Hardware-Verschlüsselungsadapter aktiviert ist.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

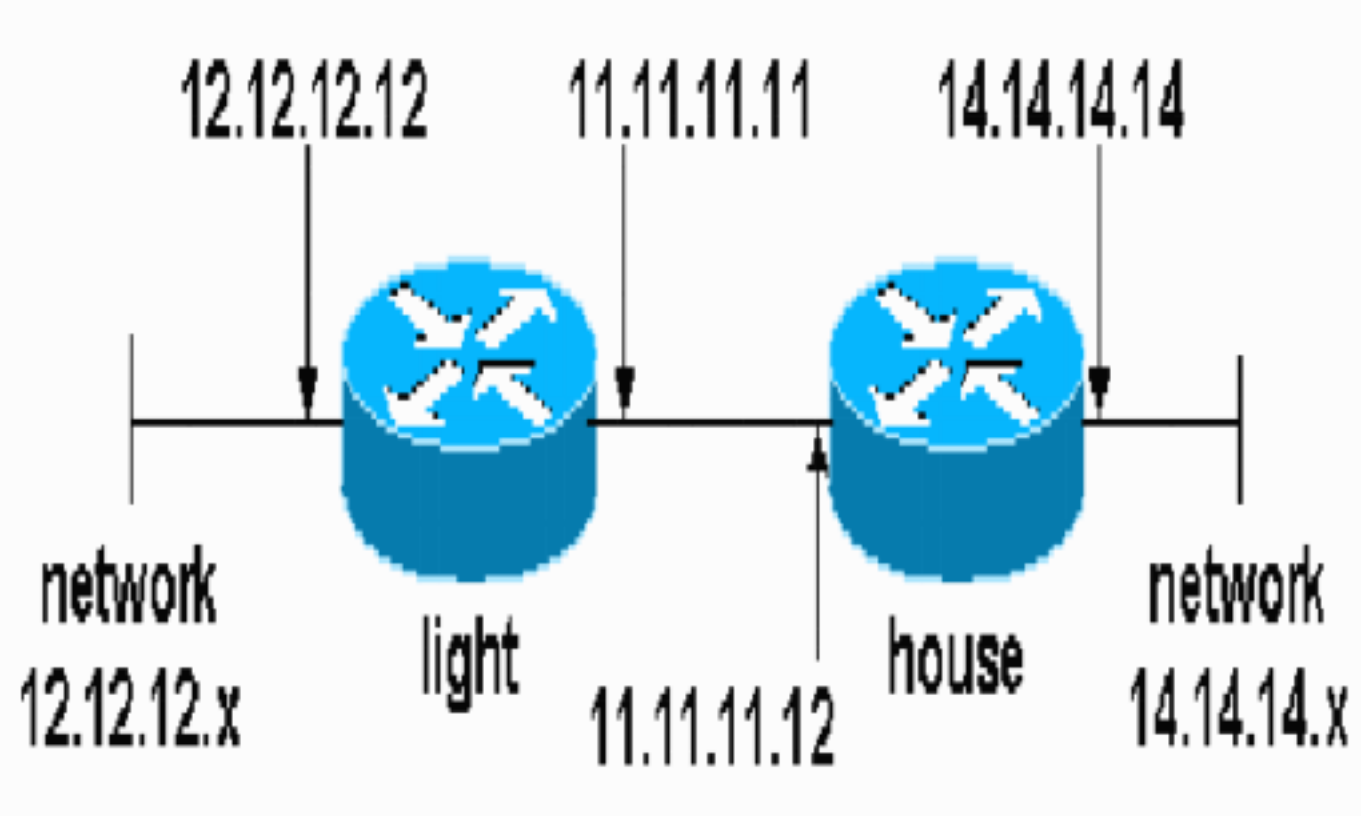
# Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Lichtkonfiguration
- Hauskonfiguration

**Lichtkonfiguration**

```
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
!
!
!
```

## Hauskonfiguration

```
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
```

# Überprüfen

In diesem Abschnitt finden Sie Informationen zur Bestätigung Ihrer Konfigurationsfunktionen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen in Phase 2 an.

# Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

## Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

**Hinweis:** Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an.

## Transform-Sets stimmen nicht überein

Licht hat ah-sha-hmac und House hat 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 stimmen nicht überein

Auf side_A (dem "leichten" Router) befindet sich ein interner Host-zu-Host-Router, und auf side_B (dem "Haus-Router") gibt es eine Schnittstelle zur Schnittstelle. ACLs müssen immer symmetrisch sein (dies ist nicht der Fall).

```
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
```

Diese Ausgabe stammt vom initiierenden Ping side_A:

```
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
```

Diese Ausgabe wird von side_B übernommen, wenn side_A den Ping-Befehl initiiert:

```
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
```

Diese Ausgabe stammt von der Seite_B, die den Ping initiiert:

```
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
```

## Eine Seite verfügt über eine Crypto Map, die andere nicht.

```
%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
```

Diese Ausgabe stammt von der side_B-Karte, die über eine Crypto Map verfügt:

```
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
```

## Die Crypto Engine Accelerator-Karte ist aktiviert.

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

# Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems