라우터 간 IPSec 수동 키 지정 컨피그레이션 예

목차

소개

이 샘플 컨피그레이션을 사용하면 IPsec 수동 키잉의 도움을 받아 12.12.12.x와 14.14.14.x 네트워크 간의 트래픽을 암호화할 수 있습니다. 테스트용으로 호스트 12.12.12.12에서 14.14.14.14으로 확장된 ping과 ACL(Access Control List)이 사용되었습니다.

수동 키 지정은 일반적으로 Cisco 장치가 IKE(Internet Key Exchange)를 지원하지 않는 다른 공급업체의 장치에 대한 트래픽을 암호화하도록 구성된 경우에만 필요합니다. 두 디바이스에서 IKE를 구성할 경우 자동 키를 사용하는 것이 좋습니다. Cisco SPI(Device Security Parameter Index)는 10진수로 표시되지만 일부 공급업체는 16진수로 SPI를 수행합니다. 이 경우 변환이 필요할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 3640 및 1605 라우터
- Cisco IOS® 소프트웨어 릴리스 12.3.3.a

참고: 하드웨어 암호화 어댑터를 포함하는 모든 플랫폼에서는 하드웨어 암호화 어댑터가 활성화된 경우 수동 암호화가 지원되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

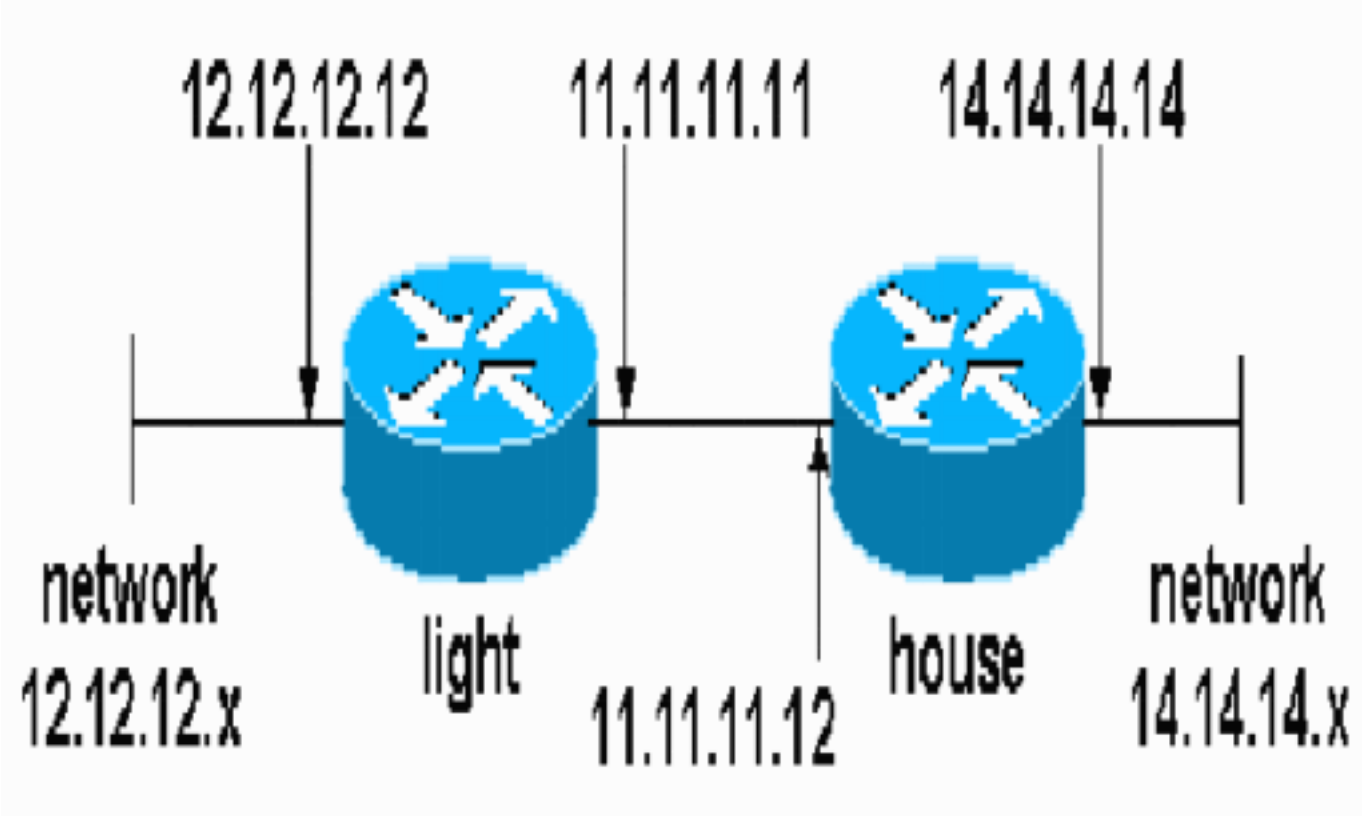
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

라이트 컨피그레이션

```
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
```

```
!
!
!
```

집 구성

```
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
```

다음을 확인합니다.

이 섹션에서는 구성 기능을 올바르게 확인하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.

변형 집합이 일치하지 않음

라이트에는 아-샤-맥이 있고 하우스에는 esp-des가 있습니다.

```
*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.....
```

ACL이 일치하지 않음

side_A("light" 라우터)에는 내부 host-to-inside-host가 있으며 side_B("house" 라우터)에는 interface-to-interface가 있습니다. ACL은 항상 대칭이어야 합니다(대칭은 아님).

```
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
```

이 출력은 side_A 시작 ping에서 가져옵니다.

```
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
```

이 출력은 side_A가 ping을 시작할 때 side_B에서 가져옵니다.

```
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
```

이 출력은 Ping을 시작하는 side_B에서 가져옵니다.

```
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
```

한쪽에는 암호화 맵이 있고 다른 한쪽에는 암호화 맵이 없음

```
%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
```

이 출력은 암호화 맵이 있는 side_B에서 가져옵니다.

```
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
```

암호화 엔진 가속기 카드가 활성화되었습니다.

```
1d05h: %HW_VPN-1-HPRXERR: Hardware VPN0/13: Packet
```

```
Encryption/Decryption error, status=4098.....
```

관련 정보

- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems