IKE Aggressive 모드를 시작하는 라우터를 사용하여 라우터 간 LAN-to-LAN 터널 구성

목차

소개

Cisco IOS® Software Release 12.2(8)T는 적극적인 모드에서 IKE(Internet Key Exchange)를 시작하는 라우터의 기능을 소개합니다.자세한 내용은 버그 툴킷의 버그 ID CSCdt30808(등록된 고객만 해당)을 참조하십시오.이전에는 라우터가 적극적인 모드의 터널 협상 요청에 응답할 수 있었지만 시작할 수 없었습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS 12.2(8)T는 두 라우터 모두에서 사용되었지만, 수신 라우터에 사용할 필요는 없습니다.

참고: 이 구성은 Cisco IOS Software Release12.2(13)T1에서 테스트되었습니다. 구성의 모든 측면은 동일하게 유지됩니다.

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

표기 규칙

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

배경 정보

참고: 새로운 CLI(Command Line Interface) 명령은 다음과 같습니다.

- **crypto isakmp peer < address <*x.x.x*> | 호스트 이름 <*이름*> >**
- **aggressive-mode client-endpoint 설정 < fqdn <*name*> | ipv4-address <*x.x.x*> | user-fqdn <*name*> >**
- **aggressive-mode 비밀번호 설정 <*password*>**

아래 샘플 컨피그레이션에서는 RouterA와 RouterB가 LAN-to-LAN 터널을 사용합니다.RouterA는 항상 터널 시작 라우터이며 이 예에서는 적극적인 모드에서 시작하도록 구성되었습니다.RouterB에는 표준 LAN-to-LAN 터널 컨피그레이션이 적용되었을 수도 있지만 RouterA의 터널 매개변수를 수락하기 위한 동적 암호화 맵만 있습니다.

참고: 이 예에서 RouterB는 RouterA의 터널 매개변수를 수락하기 위해 Cisco IOS Software Release 12.2(8)T를 실행할 필요가 없습니다.위에서 언급한 대로 라우터는 항상 적극적인 모드 요청을 수락했으며, 아직 시작할 수 없었습니다.

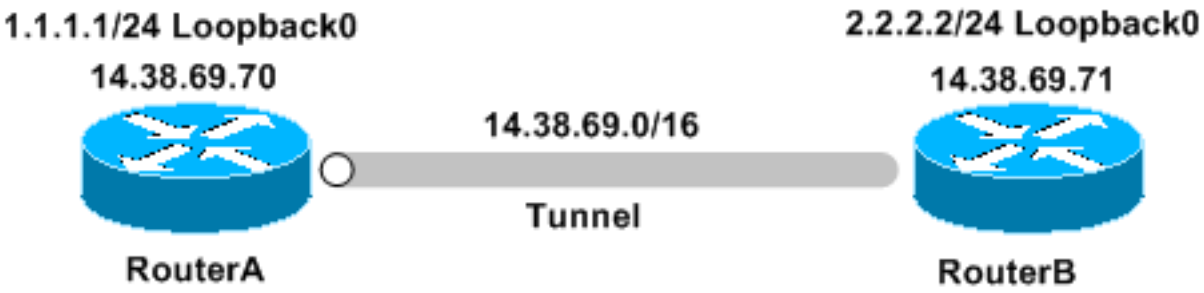
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 라우터A
- 라우터B

라우터A

```
Building configuration...

Current configuration : 1253 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp keepalive 30 5
!
crypto isakmp peer address 14.38.69.71
 set aggressive-mode password cisco123
 set aggressive-mode client-endpoint ipv4-address
14.38.69.70
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map mymap 1 ipsec-isakmp
 set peer 14.38.69.71
 set transform-set myset
 match address 100
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 14.38.69.70 255.255.0.0
 half-duplex
 crypto map mymap
!
interface BRI0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.69.71
```

```
ip http server
!
!
access-list 100 permit ip 1.1.1.0 0.0.0.255 2.2.2.0
0.0.0.255
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

라우터B

```
Building configuration...

Current configuration : 1147 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
!
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 14.38.69.70
crypto isakmp keepalive 30 5
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto dynamic-map mymap 10
 set transform-set myset
!
!
crypto map mainmap 1 ipsec-isakmp dynamic mymap
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!
interface FastEthernet0/0
```

```
 ip address 14.38.69.71 255.255.0.0
 duplex auto
 speed auto
 crypto map mainmap
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.69.70
no ip http server
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 speed 115200
line aux 0
line vty 0 4
 login
!
!
end
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.

문제 해결

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

문제 해결 명령

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.

RouterA 디버그 출력

```
00:08:26: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71,
    local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x4B68058A(1265108362), conn_id= 0, keysize= 0, flags= 0x400C
00:08:26: ISAKMP: received ke message (1/1)
00:08:26: ISAKMP: local port 500, remote port 500
00:08:26: ISAKMP (0:1): SA has tunnel attributes set.
00:08:26: ISAKMP (0:1): SA is doing unknown authentication!
00:08:26: ISAKMP (1): ID payload
        next-payload : 13
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
00:08:26: ISAKMP (1): Total payload length: 12
00:08:26: ISAKMP (0:1): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
Old State = IKE_READY  New State = IKE_I_AM1

00:08:26: ISAKMP (0:1): beginning Aggressive Mode exchange
00:08:26: ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_E.XCH....
Success rate is 0 percent (0/5)
vpn-2611a1#
00:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH...
00:08:36: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1
00:08:36: ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH
00:08:36: ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) AG_INIT_EXCH
00:08:37: ISAKMP (0:1): processing SA payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:08:37: ISAKMP:      encryption DES-CBC
00:08:37: ISAKMP:      hash MD5
00:08:37: ISAKMP:      default group 1
00:08:37: ISAKMP:      auth pre-share
00:08:37: ISAKMP:      life type in seconds
00:08:37: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
00:08:37: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is Unity
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): vendor ID is DPD
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): speaking to another IOS box!
00:08:37: ISAKMP (0:1): processing vendor id payload
00:08:37: ISAKMP (0:1): processing KE payload. message ID = 0
00:08:37: ISAKMP (0:1): processing ID payload. message ID = 0
00:08:37: ISAKMP (0:1): processing NONCE payload. message ID = 0
00:08:37: ISAKMP (0:1): SA using tunnel password as pre-shared key.
00:08:37: ISAKMP (0:1): SKEYID state generated
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 0
00:08:37: ISAKMP (0:1): SA has been authenticated with 14.38.69.71
```

```
00:08:37: ISAKMP (0:1): IKE_DPD is enabled, initializing timers
00:08:37: ISAKMP: Locking DPD struct 0x82702444
    from crypto_ikmp_dpd_ike_init, count 1
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1  New State = IKE_P1_COMPLETE

00:08:37: IPSEC(key_engine): got a queue event...
00:08:37: IPSec: Key engine got KEYENG_IKMP_MORE_SAS message
00:08:37: ISAKMP: received ke message (6/1)
00:08:37: ISAKMP: received KEYENG_IKMP_MORE_SAS message
00:08:37: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): purging node -1844394438
00:08:37: ISAKMP (0:1): Sending initial contact.

00:08:37: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE
00:08:37: ISAKMP (0:1): processing HASH payload. message ID = 133381228
00:08:37: ISAKMP (0:1): processing NOTIFY RESPONDER_LIFETIME protocol 1
        spi 0, message ID = 133381228, sa = 82701CDC
00:08:37: ISAKMP (0:1): processing responder lifetime
00:08:37: ISAKMP (0:1): deleting node 133381228 error
    FALSE reason "informational (in) state 1"
00:08:37: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

00:08:38: ISAKMP: quick mode timer expired.
00:08:38: ISAKMP (0:1): src 14.38.69.70 dst 14.38.69.71
00:08:38: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -1119238561
00:08:38: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE_MESG_INTERNAL,
    IKE_INIT_QM Old State = IKE_QM_READY  New State = IKE_QM_I_QM1

00:08:38: ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): processing HASH payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing SA payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): Checking IPSec proposal 1
00:08:38: ISAKMP: transform 1, ESP_3DES
00:08:38: ISAKMP:   attributes in transform:
00:08:38: ISAKMP:      encaps is 1
00:08:38: ISAKMP:      SA life type in seconds
00:08:38: ISAKMP:      SA life duration (basic) of 3600
00:08:38: ISAKMP:      SA life type in kilobytes
00:08:38: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
00:08:38: ISAKMP:      authenticator is HMAC-MD5
00:08:38: ISAKMP (0:1): atts are acceptable.
00:08:38: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71,
    local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
00:08:38: ISAKMP (0:1): processing NONCE payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): processing ID payload. message ID = -1119238561
00:08:38: ISAKMP (0:1): Creating IPSec SAs
00:08:38:         inbound SA from 14.38.69.71 to 14.38.69.70
        (proxy 2.2.2.0 to 1.1.1.0)
00:08:38:         has spi 0x4B68058A and conn_id 2000 and flags 4
00:08:38:         lifetime of 3600 seconds
00:08:38:         lifetime of 4608000 kilobytes
00:08:38:         outbound SA from 14.38.69.70 to 14.38.69.71
        (proxy 1.1.1.0 to 2.2.2.0)
00:08:38:         has spi 1503230765 and conn_id 2001 and flags C
```

```
00:08:38:         lifetime of 3600 seconds
00:08:38:         lifetime of 4608000 kilobytes
00:08:38: ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE
00:08:38: ISAKMP (0:1): deleting node -1119238561 error FALSE reason ""
00:08:38: ISAKMP (0:1): Node -1119238561, Input = IKE_MESG_FROM_PEER,
    IKE_QM_EXCH Old State = IKE_QM_I_QM1
    New State = IKE_QM_PHASE2_COMPLETE

00:08:38: IPSEC(key_engine): got a queue event...
00:08:38: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71,
    local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x4B68058A(1265108362), conn_id= 2000, keysize= 0, flags= 0x4
00:08:38: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71,
    local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x59997B2D(1503230765), conn_id= 2001, keysize= 0, flags= 0xC
00:08:38: IPSEC(create_sa): sa created,
  (sa) sa_dest= 14.38.69.70, sa_prot= 50,
    sa_spi= 0x4B68058A(1265108362),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000
00:08:38: IPSEC(create_sa): sa created,
  (sa) sa_dest= 14.38.69.71, sa_prot= 50,
    sa_spi= 0x59997B2D(1503230765),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
00:08:38: ISAKMP: received ke message (7/1)
00:08:38: ISAKMP: DPD received kei with flags 0x10
00:08:38: ISAKMP: Locking DPD struct 0x82702444 from
    crypto_ikmp_dpd_handle_kei_mess, count 2
```

관련 정보

- IPSec 지원 페이지
- Technical Support - Cisco Systems