IKE アグレッシブ モードを開始するルータを使用する Router-to-Router LAN-to-LAN トンネルの設定

目次

はじめに
前提条件
要件
使用するコンポーネント
表記法
背景説明
設定
ネットワーク図
設定
確認
トラブルシューティング
トラブルシューティングのためのコマンド
ルータ A のデバッグ出力
関連情報

はじめに

Cisco IOS(R) ソフトウェア リリース 12.2(8)T では、アグレッシブ モードで Internet Key Exchange（IKE; インターネット鍵交換）を開始するルータの機能を導入しています。 詳細は、Bug Toolkit の Bug ID CSCdt30808（登録ユーザ専用）を参照してください。 そのリリース以前は、ルータはアグレッシブ モードのトンネル ネゴシエーション要求に応じることはできましたが、要求を出すことはできませんでした。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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くものです。

- Cisco IOS 12.2(8)T は、両側のルータで使用されてきましたが、受信側のルータには必ずしも導入される必要はありません。

注: この設定は、Cisco IOS ソフトウェア リリース12.2(13)T1 を使用してテストされました。 構成のすべての部分は同じままです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に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。

背景説明

注: 次に、新しいコマンドライン インターフェイス（CLI）コマンドを示します。

- **crypto isakmp peer < address <x.x.x.x> / hostname <名前> >**
- **set aggressive-mode client-endpoint < fqdn <名前> | ipv4-address <x.x.x.x> / user-fqdn <名前> >**
- **set aggressive-mode password <パスワード>**

次の設定例では、ルータ A と ルータ B との間に LAN 間トンネルが確立されています。 ルータ A は常にトンネルを開始するルータであり、この例ではアグレッシブ モードで開始するように設定されています。 ルータ B には、ルータ A からのトンネル パラメータ受信用のダイナミックな暗号化マップが存在するだけですが、標準的な LAN 間トンネルの設定も適用できます。

注: この例の場合、ルータ A からのトンネル パラメータを受け取るために、ルータ B で Cisco IOS ソフトウェア リリース 12.2(8)T が動作している必要はありません。 前述したように、ルータは今までも、アグレッシブ モードの要求を受け取ることはできました。ただし、要求を出すことはできませんでした。

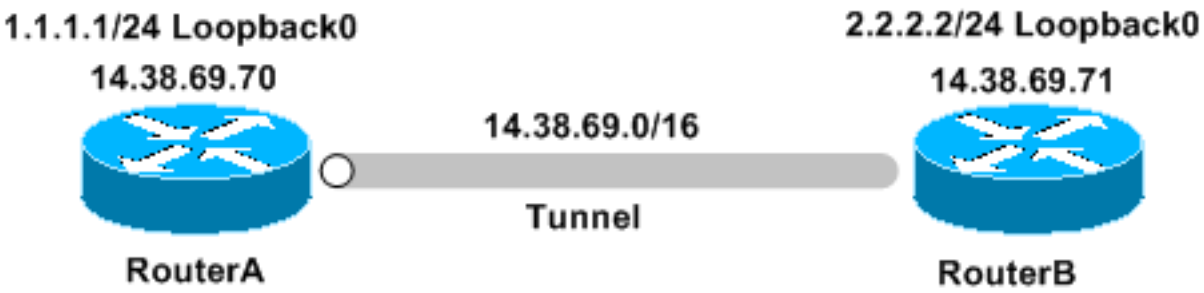
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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図に示すネットワーク



設定

このドキュメントでは、次の設定を使用します。

- RouterA
- RouterB

RouterA

```
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
```

RouterB

```

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
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **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。
- **show crypto isakmp sa**：フェーズ 1 のセキュリティ アソシエーションを表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『debug コマンドに関する重要な情報』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 isakmp**：フェーズ 1 の ISAKMP 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。

ルータ A のデバッグ出力

```
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
```

関連情報

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems