Introduction

This document provides a sample configuration for how to allow VPN users access to the Internet while connected via an IPsec LAN-to-LAN (L2L) tunnel to another router. This configuration is achieved when you enable split tunneling. Split tunneling allows the VPN users to access corporate resources via the IPsec tunnel while still permitting access to the Internet.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on a Cisco 3640 Router with Cisco IOS® Software Release 12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure
In this section, you are presented with the information to configure the features described in this document.

**Network Diagram**

This document uses this network setup:

![Network Diagram](image)

**Note:** The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

**Configurations**

This document uses these configurations:

- **Router A**
- **Router B**

**Router A**

RouterA#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R9
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!

--- Create an ISAKMP policy for Phase 1
--- negotiations for the L2L tunnels. crypto isakmp policy 10 hash md5 authentication pre-share ---
the pre-shared key and the remote peer address
!---- to match for the L2L tunnel. crypto isakmp key vpnuser address 10.0.0.2 !---- Create the Phase 2 policy for actual data encryption. crypto ipsec transform-set myset esp-des esp-md5-hmac !---- Create the actual crypto map. Specify
!---- the peer IP address, transform
!---- set, and an access control list (ACL) for the split tunneling. crypto map mymap 10 ipsec-isakmp set peer 10.0.0.2 set transform-set myset match address 100 !---- Apply the crypto map on the outside interface. interface Ethernet0/0 ip address 10.1.1.2 255.255.255.0 half-duplex !---- Create the ACL for the traffic to
!---- be encrypted. In this example,
!---- the traffic from 10.1.1.0/24 to 172.16.2.0/24
!---- is encrypted. The traffic which does not match the access list
!---- is unencrypted for the Internet. access-list 100 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!---- interface Ethernet1 ip address 10.0.0.2 255.255.255.0 crypto map mymap !---- Create an ACL for the traffic to
!---- be encrypted. In this example,
!---- the traffic from 172.16.2.0/24 to 10.1.1.0/24
!---- is encrypted. The traffic which does not match the access list
!---- is unencrypted for the Internet. access-list 100 permit ip 172.16.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!

Router B
RouterB# show running-config
Building configuration...

Current configuration : 835 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
!
ip subnet-zero
!
!
!---- Create an ISAKMP policy for Phase 1
!---- negotiations for the L2L tunnels. crypto isakmp policy 10 hash md5 authentication pre-share !---- Specify the pre-shared key and the remote peer address
!---- to match for the L2L tunnel. crypto isakmp key vpnuser address 172.16.1.1 !---- Create the Phase 2 policy for actual data encryption. crypto ipsec transform-set myset esp-des esp-md5-hmac !---- Create the actual crypto map. Specify
!---- the peer IP address, transform
!---- set, and an ACL for the split tunneling. ! crypto map mymap 10 ipsec-isakmp set peer 172.16.1.1 set transform-set myset match address 100 !---- Apply the crypto map on the outside interface. interface Ethernet1 ip address 10.0.0.2 255.255.255.0 crypto map mymap ! interface Serial0 no ip address shutdown no fair-queue ! interface Serial1 no ip address shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 10.0.0.1 ip http server !---- Create an ACL for the traffic to
!---- be encrypted. In this example,
!---- the traffic from 172.16.2.0/24 to 10.1.1.0/24
!---- is encrypted. The traffic which does not match the access list
!---- is unencrypted for the Internet. access-list 100 permit ip 172.16.2.0 0.0.0.255 10.1.1.0 0.0.0.255 line con 0 line aux 0 line vty 0 4 ! end

Verify

This section provides information you can use to confirm your configuration is working properly.

The Cisco CLI Analyzer (registered customers only) supports certain show commands. Use the Cisco CLI Analyzer to view an analysis of show command output.

- show crypto ipsec sa - Shows the settings used by current Security Associations
RouterA#show crypto ipsec sa

interface: Serial2/0
Crypto map tag: mymap, local addr 172.16.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 43, #pkts encrypt: 43, #pkts digest: 43
#pkts decaps: 43, #pkts decrypt: 43, #pkts verify: 43
pkts compressed: 0, pkts decompressed: 0
pkts not compressed: 0, pkts compr. failed: 0
pkts not decompressed: 0, pkts decompress failed: 0
#send errors 4, #recv errors 0
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x267BC43(40352835)
inbound esp sas:
    spi: 0xD9F4BC76(3656694902)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4558868/3550)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
    spi: 0x267BC43(40352835)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4558868/3548)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

outbound ah sas:

outbound pcp sas:

- show crypto isakmp sa - Shows all current IKE SAs at a peer.

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>1</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

Troubleshoot

This section provides information you can use to troubleshoot your configuration. Sample debug output is also shown.

Troubleshooting Commands
The Cisco CLI Analyzer (registered customers only) supports certain show commands. Use the Cisco CLI Analyzer to view an analysis of show command output.

**Note:** Refer to Important Information on Debug Commands before you use debug commands.

- **debug crypto isakmp** - Displays the ISAKMP negotiations of Phase 1.
- **debug crypto ipsec** - Displays the IPsec negotiations of Phase 2.

### Sample debug Output

**Router**

**RouterA# debug crypto isakmp**

* Sep 29 22:50:35.511: ISAKMP: received ke message (1/1)
* Sep 29 22:50:35.511: ISAKMP: (0:0:N/A:0): SA request profile is (NULL)
* Sep 29 22:50:35.511: ISAKMP: Created a peer struct for 10.0.0.2, peer port 500
* Sep 29 22:50:35.511: ISAKMP: New peer created peer = 0x64C0EF54 peer_handle = 0 x8000000C
* Sep 29 22:50:35.515: ISAKMP: Locking peer struct 0x64C0EF54, IKE refcount 1 for isakmp_initiator
* Sep 29 22:50:35.515: ISAKMP: local port 500, remote port 500
* Sep 29 22:50:35.515: ISAKMP: set new node 0 to QM_IDLE
* Sep 29 22:50:35.515: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 64CDBF3C
* Sep 29 22:50:35.515: ISAKMP: (0:0:N/A:0): Can not start Aggressive mode, trying Main mode.
* Sep 29 22:50:35.515: ISAKMP: (0:0:N/A:0): found peer pre-shared key matching 10.0.0.2
* Sep 29 22:50:35.515: ISAKMP: (0:0:N/A:0): constructed NAT-T vendor-07 ID
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): constructed NAT-T vendor-03 ID
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): constructed NAT-T vendor-02 ID
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): Old State = IKE_READY New State = IKE_I_MM1
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): beginning Main Mode exchange
* Sep 29 22:50:35.519: ISAKMP: (0:0:N/A:0): sending packet to 10.0.0.2 my_port 500 peer_port 500 (1) MM_NO_STATE
* Sep 29 22:50:38.451: ISAKMP (0:0): received packet from 10.0.0.2 dport 500 sport 500 Global (1) MM_NO_STATE
* Sep 29 22:50:38.451: ISAKMP: (0:0:N/A:0): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
* Sep 29 22:50:38.451: ISAKMP: (0:0:N/A:0): Old State = IKE_I_MM1 New State = IKE_I_MM2
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): processing SA payload. message ID = 0
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): found peer pre-shared key matching 10.0.0.2
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): local preshared key found
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): Checking ISAKMP transform 1 against priority 10 policy
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): encryption DES-CBC
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): hash MD5
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): default group 1
* Sep 29 22:50:38.455: ISAKMP: (0:0:N/A:0): auth pre-share
* Sep 29 22:50:38.459: ISAKMP: (0:0:N/A:0): life type in seconds
* Sep 29 22:50:38.459: ISAKMP: (0:0:N/A:0): life duration (VPI) of 0x0 0x1 0x51 0x80
* Sep 29 22:50:38.459: ISAKMP: (0:0:N/A:0): atts are acceptable. Next payload is 0
* Sep 29 22:50:38.547: ISAKMP: (0:4:SW:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_M

*Sep 29 22:50:38.551: ISAKMP:(0:4:SW:1): sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) MM_SA_SETUP

*Sep 29 22:50:42.091: ISAKMP (0:134217732): received packet from 10.0.0.2 dport 500 sport 500 Global (I) MM_SA_SETUP
*Sep 29 22:50:42.095: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 29 22:50:42.095: ISAKMP:(0:4:SW:1): Old State = IKE_I_MM3  New State =IKE_I_MM4

*Sep 29 22:50:42.095: ISAKMP:(0:4:SW:1): processing KE payload. message ID = 0
*Sep 29 22:50:42.203: ISAKMP:(0:4:SW:1): processing NONCE payload. message ID = 0
*Sep 29 22:50:42.203: ISAKMP:(0:4:SW:1): found peer pre-shared key matching 10.0.0.2
*Sep 29 22:50:42.207: ISAKMP:(0:4:SW:1): SKEYID state generated
*Sep 29 22:50:42.207: ISAKMP:(0:4:SW:1): processing vendor id payload
*Sep 29 22:50:42.207: ISAKMP:(0:4:SW:1): speaking to another IOS box!
*Sep 29 22:50:42.207: ISAKMP:(0:4:SW:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Sep 29 22:50:42.207: ISAKMP:(0:4:SW:1): Old State = IKE_I_MM4  New State =IKE_I_MM4

*Sep 29 22:50:42.211: ISAKMP:(0:4:SW:1): Send initial contact
*Sep 29 22:50:42.215: ISAKMP:(0:4:SW:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
*Sep 29 22:50:42.215: ISAKMP (0:134217732): ID payload
  next-payload : 8
type : 1
address : 172.16.1.1
protocol : 17
port : 500
length : 12
*Sep 29 22:50:42.215: ISAKMP:(0:4:SW:1): Total payload length: 12
*Sep 29 22:50:42.215: ISAKMP:(0:4:SW:1): sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) MM_KEY_EXCH
*Sep 29 22:50:42.219: ISAKMP:(0:4:SW:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Sep 29 22:50:42.783: ISAKMP (0:134217732): received packet from 10.0.0.2 dport 500 sport 500 Global (I) MM_KEY_EXCH
*Sep 29 22:50:42.783: ISAKMP:(0:4:SW:1): processing ID payload. message ID = 0
*Sep 29 22:50:42.783: ISAKMP (0:134217732): ID payload
  next-payload : 8
type : 1
address : 10.0.0.2
protocol : 17
port : 500
length : 12
*Sep 29 22:50:42.783: ISAKMP:(0:4:SW:1): peer matches *none* of the profiles
*Sep 29 22:50:42.787: ISAKMP:(0:4:SW:1): processing HASH payload. message ID = 0
*Sep 29 22:50:42.787: ISAKMP:(0:4:SW:1): SA has been authenticated with 10.0.0.2
*Sep 29 22:50:42.787: ISAKMP: Trying to insert a peer 172.16.1.1/10.0.0.2/500/,
and inserted successfully 64C0EF54.

*Sep 29 22:50:42.787: ISAKMP:(0:4:SW:1):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 29 22:50:42.787: ISAKMP:(0:4:SW:1):Old State = IKE_I_MM5  New State = IKE_I_MM6

*Sep 29 22:50:42.791: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Sep 29 22:50:42.791: ISAKMP:(0:4:SW:1):Old State = IKE_I_MM6  New State = IKE_I_MM6

*Sep 29 22:50:42.795: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Sep 29 22:50:42.795: ISAKMP:(0:4:SW:1):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE

*Sep 29 22:50:42.799: ISAKMP:(0:4:SW:1):beginning Quick Mode exchange, M-ID of -966196463
*Sep 29 22:50:42.803: ISAKMP:(0:4:SW:1): sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) QM_IDLE
*Sep 29 22:50:42.803: ISAKMP:(0:4:SW:1):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1

--- IKE Phase 1 is completed successfully. *Sep 29 22:50:42.803: ISAKMP:(0:4:SW:1):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Sep 29 22:50:43.907: ISAKMP (0:134217732): received packet from 10.0.0.2 dport 500 sport 500 Global (I) QM_IDLE
*Sep 29 22:50:43.911: ISAKMP:(0:4:SW:1): processing HASH payload. message ID = -966196463
*Sep 29 22:50:43.911: ISAKMP:(0:4:SW:1): processing SA payload. message ID = -966196463
*Sep 29 22:50:43.911: ISAKMP:(0:4:SW:1):Checking IPSec proposal 1
*Sep 29 22:50:43.911: ISAKMP: transform 1, ESP_DES
*Sep 29 22:50:43.911: ISAKMP: attributes in transform:
*Sep 29 22:50:43.915: ISAKMP:   encaps is 1 (Tunnel)
*Sep 29 22:50:43.915: ISAKMP:   SA life type in seconds
*Sep 29 22:50:43.915: ISAKMP:   SA life duration (basic) of 3600
*Sep 29 22:50:43.915: ISAKMP:   SA life type in kilobytes
*Sep 29 22:50:43.915: ISAKMP:   SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 29 22:50:43.915: ISAKMP:   authenticator is HMAC-MD5
*Sep 29 22:50:43.915: ISAKMP:(0:4:SW:1):ats are acceptable.
*Sep 29 22:50:43.915: ISAKMP:(0:4:SW:1): processing NONCE payload. message ID = -966196463
*Sep 29 22:50:43.919: ISAKMP:(0:4:SW:1): processing ID payload. message ID = -966196463
*Sep 29 22:50:43.919: ISAKMP:(0:4:SW:1): processing ID payload. message ID = -966196463
*Sep 29 22:50:43.923: ISAKMP: Locking peer struct 0x64C0EF54, IPSEC refcount 1 for stuff_key
*Sep 29 22:50:43.923: ISAKMP:(0:4:SW:1): Creating IPSec SAs
*Sep 29 22:50:43.923: inbound SA from 10.0.0.2 to 172.16.1.1 (f/i) 0/0 (proxy 172.16.2.0 to 10.1.1.0)
*Sep 29 22:50:43.923: has spi 0x84E11317 and conn_id 0 and flags 2
*Sep 29 22:50:43.923: lifetime of 3600 seconds
*Sep 29 22:50:43.923: lifetime of 4608000 kilobytes
*Sep 29 22:50:43.923: has client flags 0x0
*Sep 29 22:50:43.923: outbound SA from 172.16.1.1 to 10.0.0.2 (f/i) 0/0 (proxy 10.1.1.0 to 172.16.2.0)
*Sep 29 22:50:43.923: has spi -65483228 and conn_id 0 and flags A
*Sep 29 22:50:43.923: lifetime of 3600 seconds
*Sep 29 22:50:43.923: lifetime of 4608000 bytes
*Sep 29 22:50:43.923: has client flags 0x0
*Sep 29 22:50:43.927: ISAKMP:(0:4:SW:1): sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) QM_IDLE
*Sep 29 22:50:43.927: ISAKMP:(0:4:SW:1):deleting node -966196463 error FALSE reason "No Error"


*Sep 29 22:50:43.931: ISAKMP: Locking peer struct 0x64C0EF54, IPSEC refcount 2 from create_transforms
*Sep 29 22:50:43.931: ISAKMP: Unlocking IPSEC struct 0x64C0EF54 from create_transforms, count 1

RouterA#debug crypto ipsec

*Sep 29 22:46:06.699: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 172.16.1.1, remote= 10.0.0.2,
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0xD9F4BC76(3656694902), conn_id= 0, keysize= 0, flags= 0x400A
*Sep 29 22:46:12.631: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 172.16.1.1, remote= 10.0.0.2,
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Sep 29 22:46:12.631: Crypto mapdb : proxy_match
src addr : 10.1.1.0
dst addr : 172.16.2.0
protocol : 0
src port : 0
dst port : 0
*Sep 29 22:46:12.639: IPSEC(key_engine): got a queue event with 2 kei messages
*Sep 29 22:46:12.639: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 172.16.1.1, remote= 10.0.0.2,
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0xD9F4BC76(3656694902), conn_id= 0, keysize= 0, flags= 0x2
*Sep 29 22:46:12.639: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 172.16.1.1, remote= 10.0.0.2,
local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 172.16.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x267BC43(40352835), conn_id= 0, keysize= 0, flags= 0xA
*Sep 29 22:46:12.639: Crypto mapdb : proxy_match
src addr : 10.1.1.0
dst addr : 172.16.2.0
protocol : 0
src port : 0
dst port : 0
*Sep 29 22:46:12.643: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and 10.0.0.2
*Sep 29 22:46:12.643: IPSEC(policy_db_add_ident): src 10.1.1.0, dest 172.16.2.0
dest_port 0

*Sep 29 22:46:12.643: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.1, sa_proto= 50,
  sa_spi= 0xD9F4BC76(3656694902),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
*Sep 29 22:46:12.643: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.2, sa_proto= 50,
  sa_spi= 0x267BC43(40352835),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002

Related Information

- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation - Cisco Systems](#)