

# IOS VPN(Router): Add a New L2L Tunnel or Remote Access to an Existing L2L VPN

Document ID: 107553

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions
- Network Diagram

### Background Information

#### Add an Additional L2L Tunnel to the Configuration

- Step-by-Step Instructions
- Example Configuration

#### Add a Remote Access VPN to the Configuration

- Step-by-Step Instructions
- Example Configuration

### Verify

### Troubleshoot

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document provides the steps required to add a new L2L VPN tunnel or a remote access VPN to a L2L VPN configuration that already exists in an IOS router.

## Prerequisites

## Requirements

Ensure that you correctly configure the L2L IPSec VPN tunnel that is currently operational before you attempt this configuration.

## Components Used

The information in this document is based on these software and hardware versions:

- Two IOS routers that run software versions 12.4 and 12.2
- One Cisco Adaptive Security Appliance (ASA) that runs software version 8.0

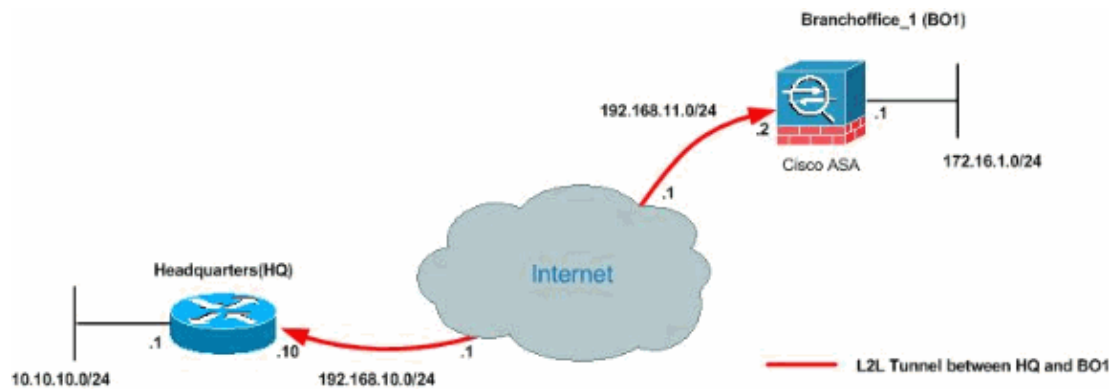
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

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

# Network Diagram

This document uses this network setup:



These outputs are the current running configurations of the HQ (HUB) Router and the Branch Office 1 (BO1) ASA. In this configuration, there is an IPsec L2L tunnel configured between HQ and BO1 ASA.

## Current HQ (HUB) Router Configuration

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!

!--- Output is suppressed.

!
ip cef
!
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
  set peer 192.168.11.2
  set transform-set newset
  match address VPN_BO1
!
```

```

!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
 ip http server
 no ip http secure-server
!
 ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
 ip nat inside source route-map nonat interface Serial2/0 overload
!
 ip access-list extended NAT_Exempt
  deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
  permit ip 10.10.10.0 0.0.0.255 any
 ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
 route-map nonat permit 10
  match ip address NAT_Exempt
!
!
 control-plane
!
 line con 0
 line aux 0
 line vty 0 4
!
!
 end
HQ_HUB#

```

### BO1 ASA Configuration

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0

```

```
ip address 192.168.11.2 255.255.255.0
!
!--- Output is suppressed.
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list 100 extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list nonat extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
crypto isakmp policy 65535
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
```

```

inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
  pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#

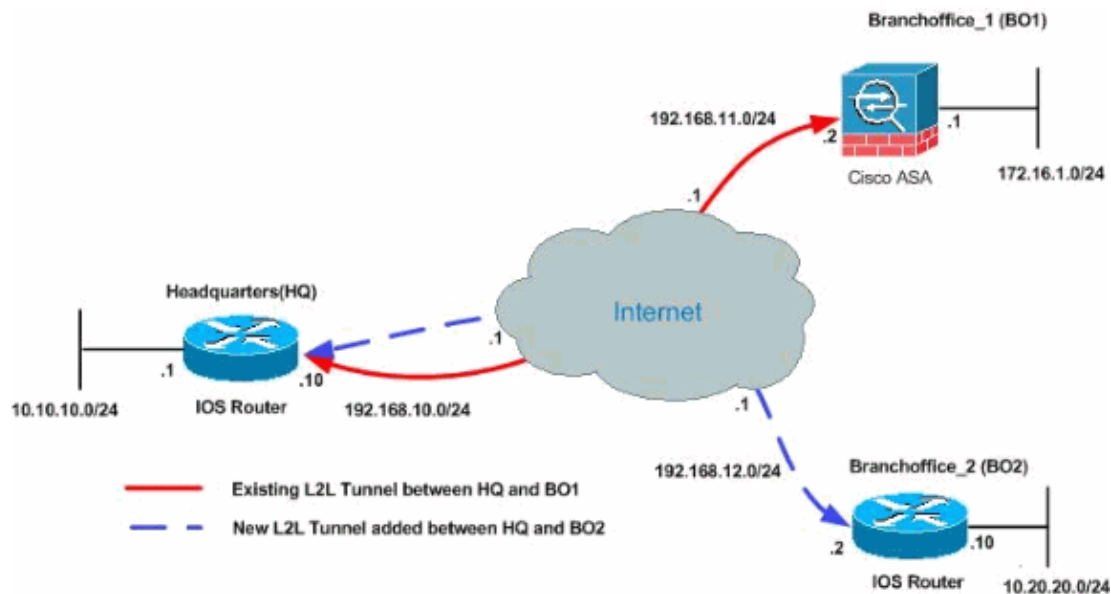
```

## Background Information

Currently, there is an existing L2L tunnel set up between the HQ office and BO1 office. Your company has recently opened a new branch office (BO2). This new office requires connectivity to local resources that are located in the HQ office. In addition, there is an additional requirement to allow employees the opportunity to work from home and securely access resources that are located on the internal network remotely. In this example, a new VPN tunnel is configured as well as a remote access VPN server that is located in the the HQ office.

## Add an Additional L2L Tunnel to the Configuration

This is the network diagram for this configuration:



## Step-by-Step Instructions

This section provides the required procedures that must be performed on the HUB HQ router.

Complete these steps:

1. Create this new access-list to be used by the crypto map in order to define interesting traffic:

```
HQ_HUB(config)#ip access-list extended VPN_BO2
```

```
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```



**Warning:** In order for the communication to take place, the other side of the tunnel must have

the opposite of this access control list (ACL) entry for that particular network.

2. Add these entries to the no nat statement in order to exempt the nating between these networks:

```
HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
```

Add these ACLs to the existing route map **nonat**:

```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```



**Warning:** In order for the communication to take place, the other side of the tunnel must have

the opposite of this ACL entry for that particular network.

3. Specify the peer address in the phase 1 configuration as shown:

```
HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
```

**Note:** The pre-shared-key must match exactly on both sides of the tunnel.

4. Create the crypto map configuration for the new VPN tunnel. Use the same transform set that was used in the first VPN configuration, as all the phase 2 settings are the same.

```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
HQ_HUB(config-crypto-map)#set peer 192.168.12.2
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#match address VPN_BO2
```

5. Now that you have configured the new tunnel, you must send interesting traffic across the tunnel in order to bring it up. In order to perform this, issue the extended **ping** command to ping a host on the inside network of the remote tunnel.

In this example, a workstation on the other side of the tunnel with the address 10.20.20.16 is pinged. This brings the tunnel up between HQ and BO2. Now, there are two tunnels connected to the HQ office. If you do not have access to a system behind the tunnel, refer to Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions to find an alternate solution using `management-access`.

## Example Configuration

### HUB\_HQ – Added a New L2L VPN Tunnel Configuration

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
```

```
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
!  
resource policy  
!  
ip cef  
!  
crypto isakmp policy 10  
  authentication pre-share  
  encryption 3des  
  group 2  
crypto isakmp key cisco123 address 192.168.11.2  
crypto isakmp key cisco123 address 192.168.12.2  
!  
!  
crypto ipsec transform-set newset esp-3des esp-md5-hmac  
!  
crypto map map1 5 ipsec-isakmp  
  set peer 192.168.11.2  
  set transform-set newset  
  match address VPN_BO1  
crypto map map1 10 ipsec-isakmp  
  set peer 192.168.12.2  
  set transform-set newset  
  match address VPN_BO2  
!  
!  
interface Ethernet0/0  
  ip address 10.10.10.1 255.255.255.0  
  ip nat inside  
  ip virtual-reassembly  
!  
  
interface Serial2/0  
  ip address 192.168.10.10 255.255.255.0  
  ip nat outside  
  ip virtual-reassembly  
  clock rate 64000  
  crypto map map1  
!  
!  
ip http server  
no ip http secure-server  
!  
ip route 0.0.0.0 0.0.0.0 192.168.10.1  
!  
ip nat inside source route-map nonat interface Serial2/0 overload  
!  
  
ip access-list extended NAT_Exempt  
  deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255  
  deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255  
  permit ip 10.10.10.0 0.0.0.255 any  
ip access-list extended VPN_BO1  
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255  
ip access-list extended VPN_BO2  
  permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255  
!  
!
```

```
route-map nonat permit 10
  match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

### BO2 L2L VPN Tunnel Configuration

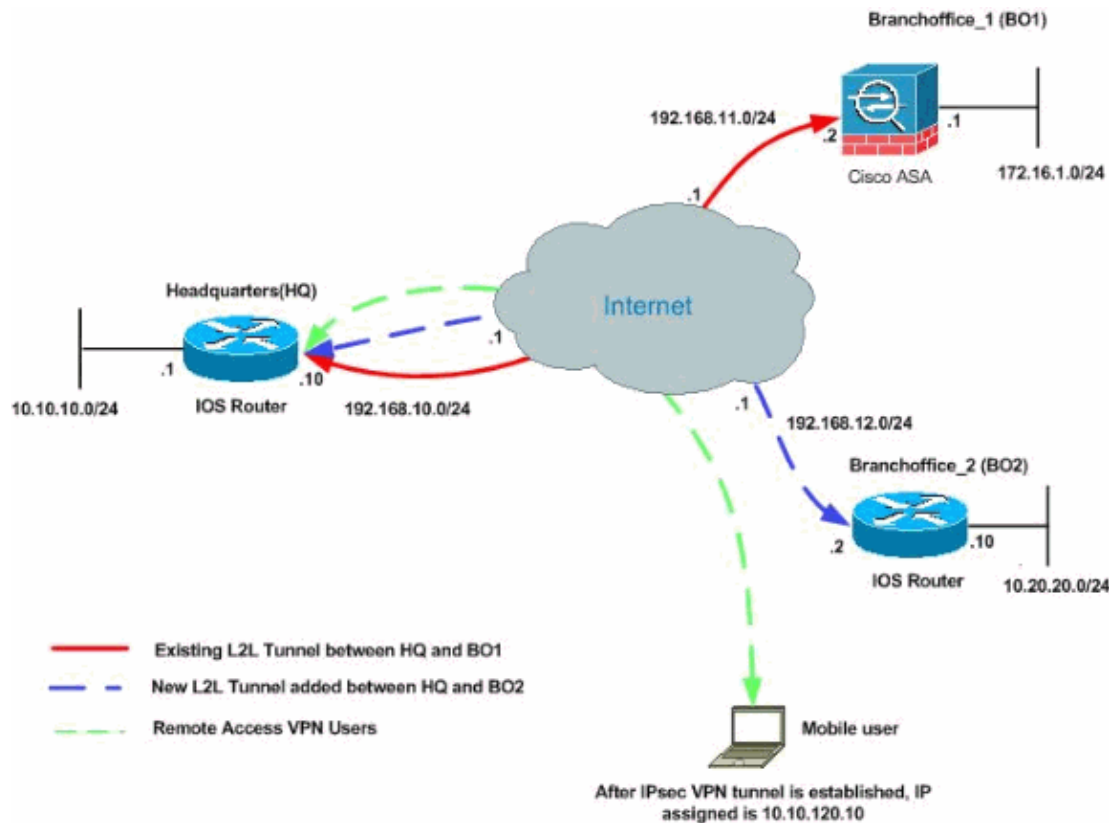
```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
  set peer 192.168.10.10
  set transform-set newset
  match address 100
!
!
!
!
interface Ethernet0
  ip address 10.20.20.10 255.255.255.0
  ip nat inside
!
!
interface Ethernet1
```

```
ip address 192.168.12.2 255.255.255.0
ip nat outside
crypto map map1
!
interface Serial0
no ip address
no fair-queue
!
interface Serial1
no ip address
shutdown
!
ip nat inside source route-map nonat interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
end
BO2#
```

## Add a Remote Access VPN to the Configuration

This is the network diagram for this configuration:



In this example, the feature called **split-tunneling** is used. This feature allows a remote-access IPsec client to conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the IPsec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. This concept applies the split tunneling policy to a specified network. The default is to tunnel all traffic. In order to set a split tunneling policy, specify an ACL where the traffic meant for the internet can be mentioned.

## Step-by-Step Instructions

This section provides the required procedures to add remote access capability and to allow remote users to access all sites.

Complete these steps:

1. Create an IP address pool to be used for clients that connect via the VPN tunnel. Also, create a basic user in order to access the VPN once the configuration is completed.

```

◆ HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50
◆ HQ_HUB(config)#username vpnuser password 0 vpnuser123

```

2. Exempt specific traffic from being nated.

```

HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit

```

Add these ACLs to the existing route map **nonat**:

```

HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt

```

```
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

Notice that the nat communication between VPN tunnels is exempted in this example.

3. Allow communication between the existing L2L tunnels and remote access VPN users.

```
HQ_HUB(config)#ip access-list extended VPN_BO1
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

This allows remote access users the ability to communicate with networks behind the specified tunnels.



**Warning:** In order for the communication to take place, the other side of the tunnel must have the opposite of this ACL entry for that particular network.

4. Configure split-tunneling

In order to enable split tunneling for the VPN connections, make sure you configure an ACL on the router. In this example, the **access-list split\_tunnel** command is associated with the group for split-tunneling purposes, and the tunnel is formed to the 10.10.10.0 /24 and 10.20.20.0/24 and 172.16.1.0/24 networks. Traffic flows unencrypted to devices not in ACL split tunnel (for example, the Internet).

```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

5. Configure local authentication, authorization and client configuration information, such as wins, dns, interesting traffic acl and ip pool, for the VPN clients.

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthen local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```

6. Configure the dynamic map and crypto map information required to the VPN tunnel creation.

```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthen
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

## Example Configuration

### Example Configuration 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!
!--- Output is suppressed
!
username vpnuser password 0 vpnuser123
!
!
!
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
crypto isakmp client configuration group vpngroup
  key cisco123
  dns 10.10.10.10
  wins 10.10.10.20
  domain cisco.com
  pool ippool
  acl split_tunnel
crypto isakmp profile vpnclient
  match identity group vpngroup
  client authentication list userauthen
  isakmp authorization list groupauthor
  client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
```

```
crypto ipsec transform-set remote-set esp-3des esp-md5-hmac
!
crypto dynamic-map dynmap 10
  set transform-set remote-set
  set isakmp-profile vpnclient
  reverse-route
!
!
crypto map map1 5 ipsec-isakmp
  set peer 192.168.11.2
  set transform-set newset
  match address VPN_BO1
crypto map map1 10 ipsec-isakmp
  set peer 192.168.12.2
  set transform-set newset
  match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
!

interface Serial2/0
  ip address 192.168.10.10 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  clock rate 64000
  crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0 overload
!
ip access-list extended NAT_Exempt
  deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
  deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
  deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
  deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
  deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
  permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
  permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
  permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
  permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
  permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
  permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
  permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255

!
route-map nonat permit 10
  match ip address NAT_Exempt
!
!
```

```
control-plane
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end  
HQ_HUB#
```

## Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **ping** This command allows you to initiate the L2L VPN tunnel as shown.

Extended Ping
<pre>HQ_HUB#ping  <i>!--- In order to make the L2L VPN tunnel with B01 !--- to be established.</i>  Protocol [ip]: Target IP address: <b>172.16.1.2</b> Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: <b>y</b> Source address or interface: <b>10.10.10.1</b> Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: Packet sent with a source address of 10.10.10.1 <b>.!!!!</b> Success rate is 80 percent (4/5), round-trip min/avg/max = 132/160/172 ms  HQ_HUB#ping  <i>!--- In order to make the L2L VPN tunnel with B02 !--- to be established.</i>  Protocol [ip]: Target IP address: 10.20.20.10 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: <b>y</b> Source address or interface: <b>10.10.10.1</b> Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:</pre>

```

Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.10, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
....!
Success rate is 20 percent (1/5), round-trip min/avg/max = 64/64/64 ms

```

### show crypto isakmp sa

```

HQ_HUB#show crypto isakmp sa
dst          src          state         conn-id slot status
192.168.12.2 192.168.10.10 QM_IDLE      2      0 ACTIVE
192.168.11.2 192.168.10.10 QM_IDLE      1      0 ACTIVE

```

### show crypto ipsec sa

```

HQ_HUB#show crypto ipsec sa

interface: Serial2/0
  Crypto map tag: map1, local addr 192.168.10.10

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.120.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
  current_peer 192.168.11.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.11.22
    path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
    current outbound spi: 0x0(0)

    inbound esp sas:

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:

    outbound ah sas:

    outbound pcp sas:

    local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
    current outbound spi: 0x0(0)

    inbound esp sas:

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:

    outbound ah sas:

    outbound pcp sas:

```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer 192.168.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
#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.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0xF1328(987944)

inbound esp sas:
  spi: 0xAD07C262(2902966882)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2004, flow_id: SW:4, crypto map: map1
    sa timing: remaining key lifetime (k/sec): (4601612/3292)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xF1328(987944)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: SW:3, crypto map: map1
    sa timing: remaining key lifetime (k/sec): (4601612/3291)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.120.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer 192.168.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:
```

outbound esp sas:

outbound ah sas:

outbound pcp sas:

protected vrf: (none)

local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)

current\_peer 192.168.11.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 11, #recv errors 0

local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.11.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0

current outbound spi: 0x978B3F93(2542485395)

inbound esp sas:

spi: 0x2884F32(42487602)

transform: esp-3des esp-md5-hmac ,

in use settings = {Tunnel, }

conn id: 2002, flow\_id: SW:2, crypto map: map1

sa timing: remaining key lifetime (k/sec): (4421529/3261)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x978B3F93(2542485395)

transform: esp-3des esp-md5-hmac ,

in use settings = {Tunnel, }

conn id: 2001, flow\_id: SW:1, crypto map: map1

sa timing: remaining key lifetime (k/sec): (4421529/3261)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0

current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
current_peer 192.168.12.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)
```

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer 192.168.11.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.11.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)
```

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

```
local crypto endpt.: 192.168.10.10, remote crypto endpt.: 192.168.12.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
current outbound spi: 0x0(0)
```

inbound esp sas:

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
outbound ah sas:
outbound pcp sas:
HQ_HUB#
```

## Troubleshoot

Refer to these documents for information you can use in order to troubleshoot your configuration:

- Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions
- IP Security Troubleshooting – Understanding and Using debug Commands

**Tip:** When you clear security associations, and it does not resolve an IPsec VPN issue, then remove and reapply the relevant crypto map in order to resolve a wide variety of issues.



**Warning:** If you remove a crypto map from an interface, it brings down any IPsec tunnels associated with that crypto map. Follow these steps with caution and consider the change control policy of your organization before you proceed.

### Example

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

## Related Information

- [An Introduction to IP Security \(IPsec\) Encryption](#)
- [IPsec Negotiation/IKE Protocols Support Page](#)
- [Configuring an IPsec Router Dynamic LAN-to-LAN Peer and VPN Clients](#)
- [Technical Support & Documentation – Cisco Systems](#)

