



DEPLOYMENT GUIDE

INTEGRATED EASY VPN AND DYNAMIC MULTIPOINT VPN

This guide describes how the combination of Easy VPN and Dynamic Multipoint VPN (DMVPN) has been deployed in the Enterprise-Class Teleworker (ECT) solution.

INTRODUCTION

This document describes how Easy VPN can be combined with DMVPN for the deployment of the ECT solution. ECT is an end-to-end secure VPN solution currently deployed within Cisco Systems®. It uses DMVPN as the base architecture. For more details on the solution and the various features, technologies, and applications that it supports, please go to:

http://www.cisco.com/application/pdf/en/us/guest/tech/tk372/c1550/cdecont_0900aecd801dc5b2.pdf

PURPOSE AND SCOPE

Integration of Easy VPN and DMVPN is desirable in two main scenarios:

- When an existing Easy VPN deployment is based on Cisco IOS® Software and the customer wants to add DMVPN to the same hub. DMVPN configuration can be added to the same hub without impacting the existing Easy VPN setup. If the existing Easy VPN setup has clients based on Cisco IOS Software routers, this setup can be converted into DMVPN spokes if needed.
- When an ECT solution deployment to provide full-scale integrated access to both small office or home office (SOHO) teleworkers and mobile users using the same end-to-end secure solution setup is desired:
 - For SOHO users, Easy VPN or DMVPN can run on a home router, providing corporate access to the computers and IP phones connected to the home network.
 - For mobile users, the Easy VPN client (software VPN client) installed on a laptop provides the desired connectivity, because that client can work from any location and will integrate well with the same solution.

Currently the DMVPN deployment supports up to 700 spokes being terminated on the same hub (in this case, a Cisco 7206 VXR Router). At this load, the same hub router can still terminate more IP Security (IPsec)–based tunnels such as Easy VPN tunnels or even plain IPsec tunnels.

With Easy VPN, as well as with DMVPN, secure tunnel access to the corporate network can be provided using preshared keys (PSKs) as well as a public key infrastructure (PKI) setup. Cisco recommends the use of PKI because it is more secure and provides enhanced user management capabilities.

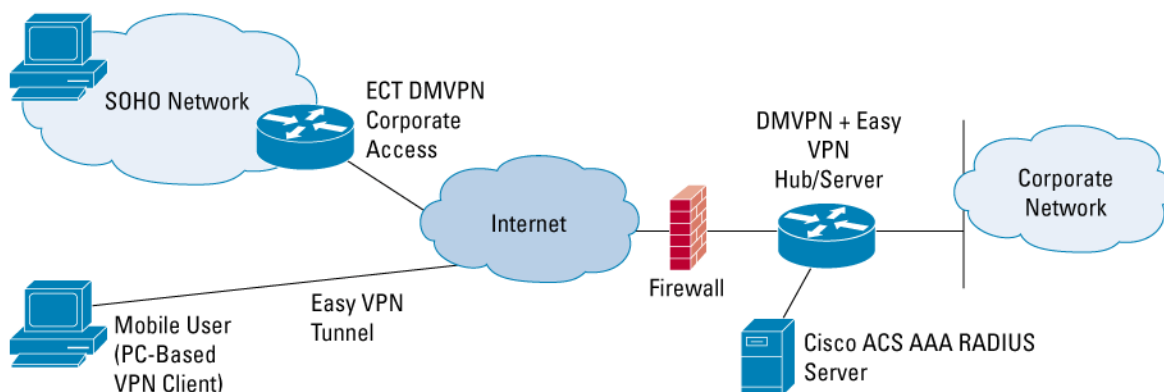
Access to and intranet and the Internet can be provided in two modes:

- Nonsplit tunnel mode, meaning that once a tunnel is up, all traffic flows through the tunnel.
- Split tunnel mode, in which only corporate traffic is routed through the tunnel. In this case, all other traffic is sent directly to the Internet, thereby lightening the load for the VPN headend.

TOPOLOGY

Figure 1 shows how Easy VPN is combined with an existing ECT deployment. The Easy VPN tunnel can start either from a software VPN client running on a laptop or from a Cisco IOS Software router acting as an Easy VPN client.

Figure 1. ECT Solution with Integrated Easy VPN Support



CONFIGURATION

This section describes configuration examples for both the Easy VPN server and the Easy VPN client. The Easy VPN server can be any of the larger platforms—for example, Cisco 3800 Series Integrated Services Routers or Cisco 7200 Series Routers. The client can be any Cisco IOS Software platform. Recommended Cisco IOS Software releases that have been tested out are Release 12.3(8)T5 and above.

Easy VPN can be provisioned in several modes. The various combinations (for server and client side) that have been showcased in this guide are as follows:

- PSKs
- PKI
- Split tunneling and nonsplit tunneling
- Client mode and network extension mode

Easy VPN with Preshared Keys

The Easy VPN server configuration is shown below. Extended Authentication (XAUTH) is used for session authentication and is tightly integrated to a back-end Cisco Access Control Server (ACS).

Server Configuration

Cisco IOS Software Router---Easy VPN Server

```
aaa new-model
aaa group server radius EzVPN
server-private <ACS AAA server ip address> auth-port 1812 acct-port 1813 key <key>
aaa authentication login easyVPN local group EzVPN
aaa authorization network easyVPN local group EzVPN
```

```
crypto keyring ezvpn-spokes
!!! This is where the EzVPN PSK is set for the corresponding spokes.
pre-shared-key address 0.0.0.0 0.0.0.0 key <ezvpn-preshared-key>
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2

crypto isakmp xauth timeout 20

crypto isakmp client configuration group easyvpn-group
  key <ezvpn-preshared-key>
  pool easyvpn-pool
  dns 172.16.226.120 172.16.168.183
  domain cisco.com
  save-password

crypto isakmp profile easyvpn-group
!!! Use the EzVPN pre-shared key provided in the keyring
  keyring ezvpn-spokes
  match identity group easyvpn-group
!!! Client will need to XAUTH with the AAA
  client authentication list easyVPN
  isakmp authorization list easyVPN
  client configuration address respond

crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
crypto dynamic-map dmap 10
  set transform-set ts1
!!! We associate the ezvpn isakmp profile to a dynamic crypto map.
  set isakmp-profile easyvpn
!!! Reverse-route is used to allow the ezvpn assigned ip address to be injected into the corporate
network. This used when a remote device will be visible from the corporate, which is needed for IP
telephony, etc.
  reverse-route

crypto map ezvpn-map 1 ipsec-isakmp dynamic dmap

interface GigabitEthernet0/0
  ip address 192.169.123.83 255.255.255.240
  crypto map ezvpn-map
```

!!! The client will be assigned one ip address from this pool. If client mode is used, the remote PC/IOS router will NAT all traffic through the EZVPN assigned ip address, other wise the end device will be directly routed to the corporate.

```
ip local pool easyvpn-pool 192.168.111.2 192.168.111.254
```

Note that the pre-shared key is provided in this configuration via a crypto keyring command. This way these keys are associated only with the respective Easy VPN crypto isakmp profile. A global crypto isakmp pre-shared key does not have to be defined in the box (that would allow any spoke to connect). Only Easy VPN spokes with the right pre-shared key, the right group name, and after authenticated using XAUTH to connect should be allowed.

With this configuration DMVPN spokes can use PKI and Easy VPN spokes will be able to use PSK. In fact, all combinations are allowed: DMVPN with PKI and/or PSK and Easy VPN with PKI and/or PSK. DMVPN and Easy VPN spokes are totally independent from each other.

Client Configuration

Software VPN Client---Easy VPN Client (Client Mode)

When using a Software VPN Client (on an end host device---or Laptop) with PSKs, start by creating a new connection entry and set the group name to the same group that has been defined in the server. In the example above it is the “easyvpn-group”. For the password, use the pre-shared one defined above in the crypto keyring command and in the crypto ezvpn client profile. Set the peer to the Easy VPN server’s ip address.

Cisco IOS Software Router---Easy VPN Client (Network extension Mode)

```
crypto ipsec client ezvpn easyvpn-group
```

```
connect auto
```

!!! the group name and key must match what is defined in the EzVPN server

```
group easyvpn-group key <ezvpn-preshared-key>
```

```
mode <client | network-extension>
```

```
peer 192.169.123.83
```

!!! these username/password are the ones define on the AAA for XAUTH. It can also be configured with a local user database in the EzVPN server.

```
username <ezvpn-user> password <ezvpn-password>
```

```
interface Ethernet0
```

```
description inside/private interface
```

!!! This is an example of the case where network-extension is used and we want the client to assigned ip addresses of this pool to connected devices.

```
ip address 10.32.247.65 255.255.255.240
```

```
crypto ipsec client ezvpn easyvpn-group inside
```

```
interface Ethernet1
```

```
description outside/public interface
```

!!! Use any possible way to connect to the Internet

```
ip address dhcp
```

```
crypto ipsec client ezvpn easyvpn-group
```

This configuration can either be applied manually to the router or the same can be achieved using Security Device Manager (SDM) packaged by default with latest Release 12.3 crypto images. In this case the user only needs to enter the group name, peer, username/password and mode of access. SDM will generate this configuration and apply to the router.

Easy VPN with Public Key Infrastructure

Easy VPN can also be configured to use PKI. This deployment mode is actually more secure, and hence the recommended mode in this guide.

To begin using PKI, the first setup which is needed is a Certificate Authority (CA) or Certificate Server (CS). Easy VPN with PKI example uses Cisco IOS Software based CS. Summary steps to configure Cisco IOS CS are given out in the next section.

Cisco IOS Certificate Setup

This setup example uses a Cisco 2811 Integrated Services Router with an appropriate Cisco IOS Software image containing the Cisco IOS Certificate code, available in all images supporting crypto. The router is configured for IP connectivity with a default route to the public network and the resources it will need to reach namely NTP and TFTP servers. This will effectively make the router a Cisco IOS Software “CS on a stick”. The “ip http server” must be enabled for service enrollment requests.

Cisco IOS CS Configuration is completely covered in the Cisco Connection Online documentation. The following configuration represents the snippet of the full configuration, needed to facilitate the Easy VPN with PKI deployment example:

Cisco IOS CS configuration:

```
!!! Set the CS name -> name must match the keypair name.
crypto pki server ezvpn-certificate-server
database level names
!!! When only generating a few certificates, the router can store the database in flash. This
example shows an external tftp server.
database url tftp://172.16.1.10/ezvpn-certificates
issuer-name CN=ezvpn-certificate-server, OU=pki-group, O=Cisco System, L=San Francisco, ST=CA, C=US
!!! Set "grant auto" only if you do not want to manually approve enrollment requests
grant auto
!!! CDP location embedded in certificate. If using CRL checking, routers will pick up CRL from this
location. Make sure that your remote routers are able to reach this URL. Otherwise do 'revocation-
check none' for the remote devices.
cdp-url http://172.16.1.10/ezvpn-certificates/ezvpn-certificate-server.crl
```

After configuring the Cisco IOS CS commands, issue the “no shutdown” command to start the Cisco IOS Certificate .

Easy VPN Server and Client Enrollment with Cisco IOS Certificate

Steps involved in setting up Easy VPN server and client routers to enroll with Cisco IOS CS:

- For both server and client routers start by setting up the hostname and an accessible NTP server.
- Generate RSA keys:

```
ezvpn-certificate-server (config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: ezvpn-certificate-server.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
ezvpn-certificate-server (config)#
```

Configure a new PKI trustpoint as shown below:

```
ip host ezvpn-certificate-server 192.168.123.123
crypto pki trustpoint ezvpn-certificate-server
enrollment url http://ezvpn-certificate-server:80
serial-number
!!! The OU field MUST match the EzVPN server group name
subject-name OU=pki-group
!!! Configure CRL checking. Remotes might not need to check the CRL. If not, configure "revocation-
check none".
revocation-check crl
```

- Authenticate the router with the Cisco IOS CS. This will download the CS root certificate so that the router will encrypt the enrollment request with the CS's public key:

```
"crypto pki authenticate ezvpn-certificate-server"
```

- Now enroll with the Cisco IOS CS:

!!! The "Serial number", "include the ip address in the subject name" and "password" fields are optional.

```
crypto pki enroll ezvpn-certificate-server
```

- Once the certificate is received, this message will pop up in the console:
"%PKI-6-CERTRET: Certificate received from Certificate Authority"

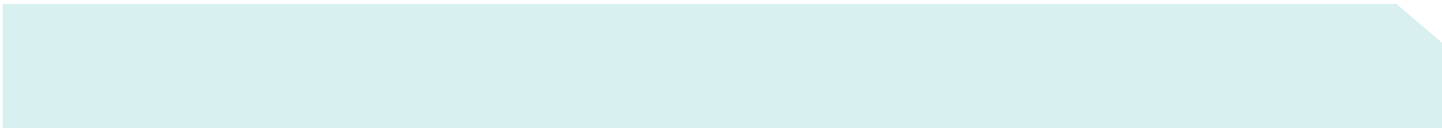
- After that save the configuration to make sure the certificate is stored.

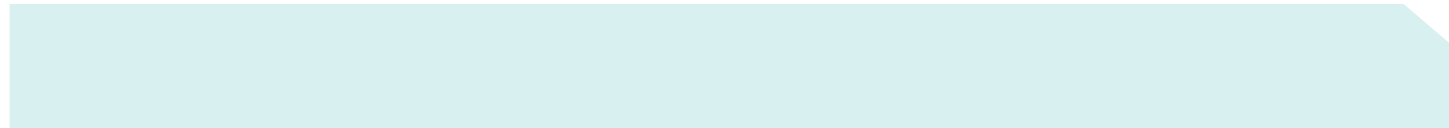
Server Configuration

This example shows how to configure an Easy VPN server to use PKI for authenticating ISAKMP tunnels, and do XAUTH based client authentication.

Cisco IOS Software Router---Easy VPN Server

```
aaa new-model
aaa group server radius EzVPN
server-private <acs AAA server ip address> auth-port 1812 acct-port 1813 key <key>
aaa authentication login easyVPN local group EzVPN
aaa authorization network easyVPN local group EzVPN
```





```
crypto pki trustpoint ezvpn-certificate-server
  enrollment url http://ezvpn-certificate-server:80
  serial-number
  revocation-check crl
```

```
crypto pki certificate map map1 10
!!! The certificate map will be used to find a match for the ezvpn profile group.
  subject-name co pki-group
```

```
crypto pki certificate chain ezvpn-certificate-server
  certificate 00BE
  certificate ca 01
```

```
crypto isakmp policy 20
  encr 3des
  group 2
crypto isakmp xauth timeout 20
```

```
crypto isakmp client configuration group pki-group
  dns 172.16.226.120 172.16.168.183
  wins 172.16.235.228 172.16.2.87
  domain cisco.com
  pool easyvpn-pool
  save-password
```

```
crypto isakmp profile ezvpn-pki
!!! The group name is the OU group field in the pki trustpoint definition
  match identity group pki-group
  match certificate map1
  client authentication list easyVPN
  isakmp authorization list easyVPN
  client configuration address respond
```

```
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
```

```
crypto dynamic-map dmap 20
  set transform-set ts1
  set isakmp-profile ezvpn-pki
  reverse-route
```

```
crypto map ezvpn-map 1 ipsec-isakmp dynamic dmap
```



```
interface GigabitEthernet0/0
 ip address 192.169.123.83 255.255.255.240
 crypto map ezvpn-map
 ip local pool easyvpn-pool 192.168.111.2 192.168.111.254
```

Client Configuration

Software VPN Client - Easy VPN Client (Client Mode)

When using Software VPN Client with PKI start by enrolling the end host device (we have used a PC in our setup) with the same Cisco IOS CS as the Easy VPN server:

- Get the CS's server root certificate. Go to the CS and export the root certificate using base 64 encoding.
- In the PC where the VPN client is installed, start by opening "Import from File" on the VPN client and select the 'Certificates -> Import'. Use the previously saved base 64 encoded certificate.
- Go to the 'Certificate -> Enroll' menu option. Enter the CA URL. In the example above it is: `http://ezvpn-certificate-server:80`. Other fields are optional. Click next to go to the next screen. Enter the CN name; in this example use: `ezvpn-certificate-server`. Enter the OU (group) field name. This one **MUST** match the Easy VPN group name defined in the server. In this example the group is the "pki-group" group.
- Click enroll.
- Now add a new connection entry. In the "Authentication" tab select the option "certificate authentication" and pick up the one just created.
- Set the peer to the Easy VPN server's ip address.

Cisco IOS Software Router---Easy VPN Client (Network extension Mode)

```
crypto pki trustpoint ezvpn-certificate-server
 enrollment url http://ezvpn-certificate-server:80
 serial-number
```

!!! The OU field MUST be set to the same ezvpn group name.

```
subject-name OU=pki-group
 revocation-check none
```

```
crypto pki certificate chain ezvpn-certificate-server
 certificate 00BF
 certificate ca 01
```

```
crypto ipsec client ezvpn easyvpn-group
```

!!! You don't need to configure the group name here. It is set in the pki trustpoint.

```
connect auto
 mode <client | network-extension>
 peer 192.169.123.83
```

!!! This username/password is the one defined on the AAA for XAUTH. It can also be configured with a local user database in the EzVPN server.

```
username <ezvpn-user> password <ezvpn-password>
 interface Ethernet0
 description inside/private interface
 ip address 10.32.247.65 255.255.255.240
 crypto ipsec client ezvpn easyvpn-group inside
```

```
interface Ethernet1
  description outside/public interface
  ip address dhcp
  crypto ipsec client ezvpn easyvpn-group
```

Easy VPN Setup with Split and Nonsplit Tunneling Modes

The examples above show how Easy VPN is deployed with non-split tunnel. This means that once the tunnel is established between client and server, all traffic flows through the tunnel, including traffic addressed to the Internet. However, it is not required to route all traffic through the corporate; this will in fact cause an unnecessary load in the corporate servers and Internet access.

The decision between split and non-split tunneling should be made according to the corporation security policies.

In any of the above cases, it is possible to apply split-tunneling mode. The only change needed is the use of access control lists (ACLs) in the “crypto isakmp client profile”.

If split-tunneling is used, the Easy VPN server will dynamically create crypto map entries for each remote/corporate subnet defined here.

The below example shows how it can be configured:

```
ip access-list extended ezvpn_split_tunnel_acl
  permit ip 10.0.0.0 0.255.255.255 any
  permit ip 192.168.0.0 0.0.255.255 any
  permit ip 172.16.0.0 0.31.255.255 any
!!! Add all the corporate internal/public subnets that the client will be able to reach
crypto isakmp client configuration group easyvpn-group
!!! Add the respective access-list to the crypto isakmp client configuration
acl ezvpn_split_tunnel_acl
```

Easy VPN Client Mode Versus Network Extension Mode

In client mode, the entire LAN behind the Easy VPN Client undergoes NAT to the mode config ip address that is pushed down by the Easy VPN Server. This is used when there is no need to assign more than one ip address to end devices, or those devices can work behind NAT. When this mode is configured, once the IPsec tunnel is established a loopback interface is dynamically configured and assigned to one ip address defined in the Easy VPN server’s pool.

In a Cisco IOS Software router, Easy VPN can also be configured for network extension mode. In this case, this client can have its own DHCP pool of ip addresses that are available to devices connecting to the client router. These devices will get an ip address of this DHCP pool which in turn will be routable all the way to the VPN Server. NAT is not used in this situation as the connection is directly provided end-to-end.

Both client and network extension modes can be either configured for split and non-split tunnel modalities. Again ISAKMP authentication can be achieved using either PSK or PKI.

Easy VPN Server Integrated with Dynamic Multipoint VPN Hub Using a Combination of Preshared Keys and Public Key Infrastructure

Below is shown the full Easy VPN Server configuration, which includes Easy VPN with all the modes described above and the DMVPN Hub configuration.

Since one of the DMVPN deployment scenarios uses “crypto profiles” instead of “crypto maps”, the physical interface is free for supporting other technologies such as Easy VPN. In the below example, we have applied a “dynamic crypto map” for Easy VPN setup on the physical interface and used “crypto profiles” for DMVPN on the tunnel interface.

Full Configuration

```
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname dmvpn_ezvpn_server
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
enable secret 5 $1$0FKZ$WDLs7U.zJkav8B.tocviN1
!
clock timezone pst -8
clock summer-time pdt recurring
aaa new-model
!
!
aaa group server radius EzVPN
!!! This is the Cisco ACS (AAA Radius server) for XAUTH authentication for remote ezvpn users.
server-private 192.168.111.106 auth-port 1812 acct-port 1813 key <key>
!
aaa authentication login easyVPN local group EzVPN
aaa authorization network easyVPN local group EzVPN
aaa session-id common
ip subnet-zero
no ip source-route
ip cef
!
!
ip domain name cisco.com
```

```
ip host ezvpn-certificate-server.cisco.com 192.168.123.123

ip multicast-routing
!
!

crypto pki trustpoint ezvpn-certificate-server
  enrollment url http://ezvpn-certificate-server:80
  serial-number
  revocation-check crl
!
crypto pki certificate map map1 10
!!! The certificate map will be used to find a match for the ezvpn profile group.
  subject-name co pki-group
!
crypto pki certificate chain ezvpn-certificate-server
  certificate 00BE
  certificate ca 01
!
!
crypto keyring ezvpn-spokes
!!! This is for ezvpn clients that use pre-shared keys
  pre-shared-key address 0.0.0.0 0.0.0.0 key <key>
!
crypto isakmp policy 10
  encr 3des
  group 2
!
crypto isakmp policy 20
  encr 3des
  authentication pre-share
  group 2
crypto isakmp keepalive 30 5
crypto isakmp xauth timeout 10
!
crypto isakmp client configuration group pki-group
  dns 172.16.226.120 172.16.168.183
  wins 172.16.235.228 172.16.2.87
  domain cisco.com
  pool easyvpn-pool
  save-password
!!! Only add this line only if split-tunnel is wanted
```

```

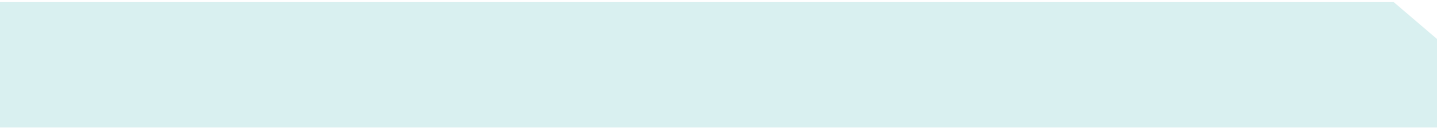
acl ezvpn_split_tunnel_acl
!
crypto isakmp client configuration group easyvpn-group
  key <ezvpn-preshare-key>
  dns 172.16.226.120 172.16.168.183
  wins 172.16.235.228 172.16.2.87
  domain cisco.com
  pool easyvpn-pool
  save-password
!!! Only add this line only if split-tunnel is wanted
acl ezvpn_split_tunnel_acl
crypto isakmp profile easyvpn-group
  description PSK group
  keyring ezvpn-spokes
  match identity group easyvpn-group
  client authentication list easyVPN
  isakmp authorization list easyVPN
  client configuration address respond
crypto isakmp profile ezvpn-pki
  description PKI group
  match identity group pki-group
  match certificate map1
  client authentication list easyVPN
  isakmp authorization list easyVPN
  client configuration address respond
!
!
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
crypto ipsec transform-set ts2 esp-3des esp-sha-hmac
  mode transport require
!
!!! This is for DMVPN
crypto ipsec profile dmvpn-profile
  set transform-set ts2
!
!
crypto dynamic-map dmap 10
set transform-set ts1
  set isakmp-profile ezvpn-pki
  reverse-route
crypto dynamic-map dmap 20
  set transform-set ts1

```

```

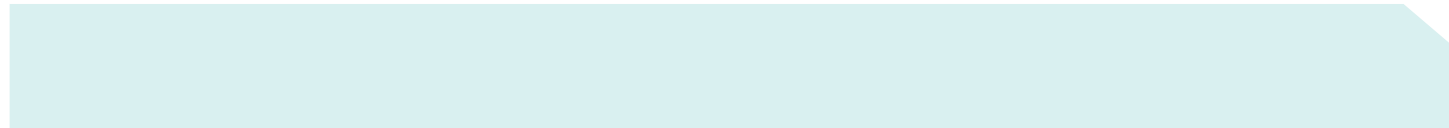
set isakmp-profile easyvpn-group
reverse-route
!
!
!!! This is the dynamic crypto map for the EzVPN server
crypto map ezvpn-map 1 ipsec-isakmp dynamic dmap
!
!
!!! This is the DMVPN mGRE interface
interface Tunnel200
description DMVPN - EIGRP network
bandwidth 2000
ip address 192.168.222.4 255.255.255.0
no ip redirects
ip mtu 1400
no ip next-hop-self eigrp 7
ip pim nbma-mode
ip pim sparse-dense-mode
ip multicast rate-limit out 768
ip nhrp map multicast dynamic
ip nhrp network-id 3686232
ip nhrp holdtime 600
ip nhrp server-only
ip tcp adjust-mss 1360
no ip split-horizon eigrp 7
no ip mroute-cache
delay 1500
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 123456
tunnel protection ipsec profile dmvpn-profile
!
!
interface GigabitEthernet0/0
!!! Here can go the public ip address of the Head end
ip address 192.169.123.83 255.255.255.240
ip pim sparse-dense-mode
duplex auto
crypto map ezvpn-map
!
router eigrp 7
network 192.168.222.0 0.0.0.255

```



```
network 192.169.123.83 0.0.0.15
```

```
default-metric 1900 1000 255 1 1500
  distribute-list split_out in Tunnel200
  no auto-summary
  no eigrp log-neighbor-changes
!
ip local pool easyvpn-pool 192.168.111.2 192.168.111.254
ip classless
ip route 0.0.0.0 0.0.0.0 192.169.123.1
!
!
no ip http server
no ip http secure-server
ip pim bidir-enable
ip pim ssm range multicast_ssm_range
!
ip access-list standard split_out
  !!! List all the subnets allowed for DMVPN spokes
  permit 10.199.224.0 0.0.0.255
  permit 10.199.225.0 0.0.0.255
!
ip access-list extended ezvpn_split_tunnel
  !!! This is the split-tunnel access list, which should contain all the corporate subnets that the
zvpn client spoke is allowed to connect to
  permit ip 10.0.0.0 0.255.255.255 any
  permit ip 172.16.0.0 0.15.255.255 any
  permit ip 192.168.0.0 0.0.255.255 any
!
route-map split_out permit 10
  match ip address static split_out
!
!
line con 0
  transport output all
  stopbits 1
line aux 0
  transport output all
  stopbits 1
line vty 0 4
  exec-timeout 120 0
!
scheduler allocate 20000 1000
ntp clock-period 17179531
```

```
ntp server 192.5.41.40
ntp server 192.5.41.41
!
end
dmvpn_ezvpn_server#
```

VERIFYING THE EASY VPN SETUP

In the Cisco IOS Software Router as Easy VPN client, the status of the connection is seen using:

Cisco IOS VPN Client side

```
ezvpn-client#show crypto ipsec ezvpn client
Easy VPN Remote Phase: 4
Tunnel name : easyvpn-group
Inside interface list: Ethernet0,
Outside interface: Ethernet1
Current State: CONNECT_REQUIRED
Last Event: TUNNEL_HAS_PUBLIC_IP_ADD
Save Password: Disallowed
Current EzVPN Peer: 192.169.123.83
```

After connecting (manually can be achieved by issuing: “crypto ipsec client ezvpn connect”) the status of the client will be this one (Note that here XAUTH will still be required):

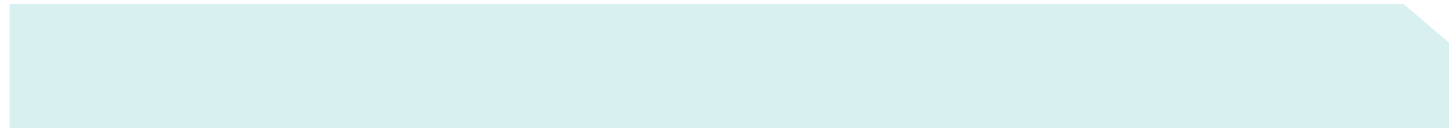
```
ezvpn-client#show crypto ipsec ezvpn client
Easy VPN Remote Phase: 4
Tunnel name : easyvpn-group
Inside interface list: Ethernet0,
Outside interface: Ethernet1
Current State: XAUTH_REQ
Last Event: XAUTH_REQUEST
Save Password: Disallowed
Current EzVPN Peer: 192.169.123.83
```

After XAUTH authentication:

```
ezvpn-client#crypto ipsec client ezvpn xauth
username:<enter AAA username>
password:<enter AAA password>
```

```
ezvpn-client#show crypto ipsec ezvpn client
Easy VPN Remote Phase: 4

Tunnel name : easyvpn-group
Inside interface list: Ethernet0,
Outside interface: Ethernet1
```



```
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.111.20
Mask: 255.255.255.255
DNS Primary: 172.16.226.120
DNS Secondary: 172.16.168.183
NBMS/WINS Primary: 172.16.235.228
NBMS/WINS Secondary: 172.16.2.87
Default Domain: cisco.com
Save Password: Allowed
Current EzVPN Peer: 192.169.123.83
```

Cisco IOS Router VPN Server side

Here we show a server with both PKI and PSK authentication methods configured:

```
ezvpn_server#show crypto isakmp profile
```

```
ISAKMP PROFILE easyvpn-group
```

```
Identities matched are:
```

```
group easyvpn-group
```

```
Certificate maps matched are:
```

```
keyring(s): ezvpn-spokes
```

!!! If you have multiple trustpoint configured in your server, you might want to restrict the ones that can connect using EzVPN using a "ca trust-point <trustpoint-name>" in the crypto isakmp profile <name>

```
trustpoint(s): <all>
```

```
ISAKMP PROFILE ezvpn-pki (PKI group)
```

```
Identities matched are:
```

```
group pki-group
```

```
Certificate maps matched are:
```

```
map1
```

```
keyring(s): <none>
```

```
trustpoint(s): <all>
```

After some Easy VPN clients are connected, their public ip address can be seen by doing:

```
ezvpn_server#show crypto isakmp peer
```

```
Peer: 192.168.33.21 Port: 1024 Local: 192.169.123.83
```

```
Phase1 id: easyvpn-group
```

```
Peer: 192.168.22.33 Port: 4500 Local: 192.169.123.83
```

!!! This example shows one client coming from a PC based VPN client using PSK and another one connecting from a router using PKI

```
Phase1 id: cn= ezvpn-certificate-server,ou=pki-group,hostname=ezvpn-client.cisco.com
```

The “show crypto map” will show the dynamic map associated with each client:

```
ezvpn_server#show crypto map
Crypto Map "ezvpn-map" 65536 ipsec-isakmp
    Peer = 192.168.22.33
    !!! This is the ezvpn group name for the PKI clients
ISAKMP Profile: pki-group
    Extended IP access list
        access-list permit ip any host 192.168.111.20
        dynamic (created from dynamic map dmap/2)
    Current peer: 192.168.22.33
    Security association lifetime: 4608000 kilobytes/3600 seconds
    PFS (Y/N): N

    Transform sets={
        t1,
    }

!!! Note the reverse route injection that will allow the ezvpn assigned ip address to be injected
into the corporate network
    Reverse Route Injection Enabled
        Interfaces using crypto map test:
            GigabitEthernet0/0
```

TROUBLESHOOTING

For Easy VPN these are the commands used to verify the connection/configuration:

- **debug crypto isakmp**---Displays errors during Phase 1.
- **debug crypto ipsec**---Displays errors during Phase 2.
- **debug crypto engine**---Displays information from the crypto engine.
- **debug crypto ipsec client ezvpn**---displays Easy VPN client related debugs
- **clear crypto isakmp**---Clears the Phase 1 security associations.
- **clear crypto sa**---Clears the Phase 2 security associations.
- **clear crypto ipsec client ezvpn**---Clears the Easy VPN client connection.

REFERENCES

Links for Additional Information

Configuring the Software VPN Client:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008009468a.shtml

Cisco IOS Certification Authority Server Configuration---TAC Tech Tip:

- VPN Client User Guide for Windows, Release 4.0

http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_book09186a008015cdf2.html



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packer*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

204026.d_ETMG_AE_3.05

