Cisco Virtual Office: Easy VPN Deployment Guide

This guide provides detailed design and implementation information for deployment of Easy VPN in client mode with the Cisco® Virtual Office.

Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for more information about the solution, its architecture, and all of its components.

Introduction

This document describes deployment of Cisco Virtual Office with Easy VPN in client mode using firewall, Network Address Translation (NAT), Quality of Service (QoS), and IEEE 802.1x.

With Cisco Easy VPN in client mode configuration, the entire LAN behind the Easy VPN client undergoes NAT translation to the IP address that is pushed down by the Easy VPN server. In this mode, there is no need to manage the IP address space in the local LAN behind the remote-access router—the same local IP Dynamic Host Configuration Protocol (DHCP) server pool can be configured on all routers. When Easy VPN runs in client mode, after the IP Security (IPsec) tunnel is established, a loopback interface is dynamically configured on the spoke and assigned an IP address defined in the Easy VPN server's pool. This pool must be routable to the corporate network.

Optionally, you can enable split tunneling on the Easy VPN server, meaning that all noncorporate traffic is sent directly to the Internet. In this case only corporate traffic is routed through the tunnel, thereby lightening the load for the VPN headend.

Platforms and Images

This document provides configuration samples corresponding to the following platforms and images:

- Easy VPN client: Cisco 881w Integrated Services Router
- Easy VPN server: Cisco 3845 Integrated Services Router with a VPN encryption module (AIM-VPN/SSL-3)
- Cisco IOS® Software Release 12.4(20)T or higher

Configuration of the Remote-Access Cisco 881W Integrated Services Router

The Easy VPN client configuration provided in this guide is a sample configuration and should be customized to your correct corporate servers.

QoS is necessary to provide a good end-user experience, because it guarantees quality for voice and video while simultaneously sending and receiving email messages, sharing applications, and browsing the web.

Dynamic Virtual Tunnel Interface

Cisco Enhanced Easy VPN is a new method for configuring Easy VPN using Dynamic Virtual Tunnel Interface (DVTI) instead of a cryptography map, which is used by traditional Easy VPN. You can use DVTI on both the Easy VPN server and Easy VPN remote routers. DVTI relies on the

virtual tunnel interface to create a virtual access interface for every new Easy VPN tunnel. The configuration of the virtual access interface is cloned from a virtual template configuration. The cloned configuration includes the IPsec configuration and any Cisco IOS Software feature configured on the virtual template interface, such as QoS, NAT, stateful firewall, NetFlow, or access control lists (ACLs).

Using DVTI simplifies the VPN configuration and supports per-session features; in addition, you can apply tunnel-specific features with this protocol, so the deployment and management of the solution is simple.

Please note the following regarding configuration of Easy VPN on the Cisco 881W Cisco Integrated Services Router:

- To add wireless support to the Cisco 881W, refer to the Cisco Virtual Office–Secure Wireless.
- The four Cisco 881W switch ports—FastEthernet0 through FastEthernet3—are configured such that hosts with an 802.1x supplicant (client) gain corporate network access only if they provide proper credentials. Cisco IP phones are automatically detected; they bypass the 802.1x authentication and are put in the voice VLAN. You can use the MAC bypass feature to manually bypass other IP phones. Other devices, with no 802.1x supplicant for guests or spouse and kids, are put in the guest VLAN; these devices have only Internet connectivity.
- For QoS, replace the end-user Internet service provider (ISP) uplink speed in the corresponding configuration line. (You can determine the ISP uplink speed by running a public Internet speed testing tool.)
- The client is configured with a default peer and a backup peer. If the default peer goes down, the backup peer becomes the active one. When the default peer comes back up, it becomes the active server again. If you do not use the default keyword, the backup peer will remain the active server.

```
!!! Create VLANs
Vlan 20
Vlan 30
!
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service linenumber
service sequence-numbers
!
!!!! **** Encrypt the easyvpn passwords and keys with AES for extra
security
key config password-encrypt <your-own-password>
service password-encryption
password encryption aes
!
hostname EasyVPN-client-vpn
```

```
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 0 <secretpassword>
!
aaa new-model
!
aaa group server radius dot1x-aaa
 server-private <rad-ip> auth-port 1812 acct-port 1813 key <rad-key>
 ip radius source-interface Vlan20
!
aaa authentication login default local
aaa authentication dot1x default group dot1x-aaa
aaa authorization exec default local
aaa authorization network default group dot1x-aaa
!
aaa session-id common
!
no ip source-route
no ip gratuitous-arps
ip cef
!
ip dhcp pool CORPORATE_Pool
   import all
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
   option 150 ip <corporate-tftpserver-for-callManager>
   netbios-name-server <corporate-netbios>
   dns-server <corporate-dns-servers>
   lease 33
!
ip dhcp pool GUEST_Pool
   import all
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
   lease 33
!
!
ip tftp source-interface Vlan20
no ip bootp server
!!! use your company domain name
ip domain name cisco.com
no ip domain lookup
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall realaudio
ip inspect name firewall rtsp
```

```
ip inspect name firewall tftp
ip inspect name firewall ftp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall streamworks
ip inspect name firewall esmtp
ip inspect name firewall sip
ip inspect name firewall skinny
!
!! Enable 802.1x globally
dot1x system-auth-control
!
username debuguser secret 0 debugonly
!
!! These are the QoS matching classes
class-map match-any call-setup
 match ip dscp af31
 match ip dscp af32
 match ip dscp cs3
 match ip precedence 3
class-map match-any internetwork-control
 match ip dscp cs6
 match access-group name control_acl
class-map match-any voice
 match ip dscp ef
 match ip dscp cs5
 match ip precedence 5
!
class-map match-any call-setup
 match ip dscp cs3
 match ip precedence 3
class-map match-any internetwork-control
 match access-group name isakmp_acl
 match ip precedence 6
 match ip precedence 7
class-map match-any voice
 match access-group name voice_acl
 match ip precedence 5
class-map match-all discover_signaling
 match protocol skinny
class-map match-all discover_video
 match protocol rtp video
class-map match-all discover_voip
 match protocol rtp audio
class-map match-any video
 match access-group name video_acl
 match ip dscp af41
 match ip precedence 4
class-map match-all non_voip
```

```
 match access-group name non_voip_traffic_acl
!
!!! Marking traffic with correct DSCP values – after the discovery is done with NBAR
policy-map mark_incoming_traffic
 class discover_signaling
  set dscp cs3
 class discover_video
  set dscp af41
 class discover_voip
  set dscp ef
 class non_voip
  set dscp default
!
policy-map voice_and_video
 class voice
  bandwidth 128
 class call-setup
  priority percent 5
 class internetwork-control
  priority percent 5
class video
!!! Video set for 384kbps – this is set on the call manager
  priority 384
 class class-default
  fair-queue
  random-detect
policy-map shaper
  class class-default
!!! enter here the user ISP uplink speed for shaping
    shape average 600000 6000
    service-policy voice_and_video
!
ip access-list extended isakmp_acl
 permit udp any any eq isakmp

ip access-list extended voice_acl
 permit udp any any range 24576 24656

ip access-list extended non_voip_traffic_acl
 permit ip any any

ip access-list extended video_acl
 permit udp any any eq 5445
 permit udp any any range 2326 2373
!
crypto ipsec client ezvpn vpnserver
 connect auto
 group <easyvpn-group> key <EzVPNkey>
```

```
 mode client
 peer <easyvpn-server-ip> default
 peer <backup-peer>
 virtual-interface 1
 username <EzVPNuser> password <EzVPNpassword>
 xauth userid mode local
!
interface FastEthernet0
 switchport access vlan 20
 switchport voice vlan 1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 30
 spanning-tree portfast
!
interface FastEthernet1
 switchport access vlan 20
 switchport voice vlan 1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 30
 spanning-tree portfast
!
interface FastEthernet2
 switchport access vlan 20
 switchport voice vlan 1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 30
 spanning-tree portfast
!
interface FastEthernet3
 switchport access vlan 20
 switchport voice vlan 1
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x guest-vlan 30
 spanning-tree portfast
!
interface FastEthernet4
 description *** Outside – WAN side - Interface
!!! enter here the correct ISP ip address if not using dhcp
 ip address dhcp
 ip access-group firewall_acl in
 no ip redirects
```

```
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 fair-queue
 no cdp enable
 crypto ipsec client ezvpn vpnserver
!
interface Vlan1
 description *** Corporate-access Voice Vlan Interface ***
 ip unnumbered vlan 20
 ip access-group allow_skinny_acl in
 no ip redirects
 no ip unreachables
 ip pim sparse-dense-mode
 ip nat inside
 ip inspect firewall in
 ip virtual-reassembly
 ip tcp adjust-mss 1360
 no autostate
 crypto ipsec client ezvpn vpnserver inside
!
interface Vlan20
 description *** Corporate-access Data Vlan Interface ***
 ip address 192.168.20.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip pim sparse-dense-mode
 ip nat inside
 ip inspect firewall in
 ip virtual-reassembly
 ip tcp adjust-mss 1360
 no autostate
 crypto ipsec client ezvpn vpnserver inside
 service-policy input mark_incoming_traffic
!
interface Vlan30
 description *** Guest/Family Vlan Interface ***
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat inside
 ip inspect firewall in
 ip virtual-reassembly
!
interface Virtual-Template1 type tunnel
```

```
 no ip address
 tunnel mode ipsec ipv4
 service-policy output shaper
!
no ip http server
no ip http secure-server
!
ip nat inside source list nat_acl interface FastEthernet4 overload
!
ip access-list extended allow_skinny_acl
 permit udp any any eq bootps
 permit udp any any range bootps bootpc
 permit udp any host <corporate-tftpserver-for-callManager> eq tftp
 permit udp any host <corporate-tftpserver-backup> eq tftp
 permit udp any host <corporate-dns-server> eq domain
 permit tcp any any eq 2000
 permit udp any any range 24576 24656
 permit udp any any eq 5445
 permit udp any any range 2326 2373
 permit tcp any host <directory-services-server> eq www
 permit tcp any host <phone-services-server> eq www
 deny   ip any any
!
ip access-list extended control_acl
 permit udp any eq isakmp any eq isakmp
!
ip access-list extended firewall_acl
 permit esp any any
 permit udp any any eq isakmp
 permit udp any eq isakmp any
 permit udp any eq non500-isakmp any
 permit udp any any eq bootpc
 deny   ip any any
!
ip access-list extended nat_acl
 permit ip 192.168.1.0 0.0.0.255 any
 permit ip 192.168.20.0 0.0.0.255 any
 permit ip 192.168.30.0 0.0.0.255 any
!
End
```

Configuration of the Server

The Easy VPN server configuration using DVTI follows. The example shows Easy VPN configured with split tunneling. The ezvpn_split_tunnel ACL gets pushed to the client when it establishes a tunnel, allowing only corporate traffic through the tunnel, while other traffic goes directly to the internet.

Following is a sample configuration, so you must customize it to your correct corporate servers.

```
aaa new-model
!
aaa group server radius EzVPN
 server-private <radius-server> auth-port 1812 acct-port 1813 key
<key>
!
aaa authentication login easyVPN local group EzVPN
aaa authorization network easyVPN local group EzVPN
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
crypto isakmp xauth timeout 10
!
crypto isakmp client configuration group easyvpn-group
 key <ezvpn-preshared-key>
 dns <dns-server>
 wins <wins-server>
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn_split_tunnel
 save-password
!
crypto isakmp profile easyvpn-group
   description PSK group
   match identity group easyvpn-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec profile prof
 set transform-set t1
!
interface GigabitEthernet0/0
 ip address 10.20.20.20 255.255.255.0
!
interface Virtual-Template1 type tunnel
 description EasyVPN for PSK users
 ip unnumbered GigabitEthernet0/0
 ip pim sparse-mode
 tunnel mode ipsec ipv4
```

```
 tunnel protection ipsec profile prof
!
ip local pool easyvpn-pool 10.10.10.130 10.10.10.254
!
ip access-list extended ezvpn_split_tunnel
 permit ip 10.0.0.0 0.255.255.255 any
 permit ip <corporate-network> 0.255.255.255 any
```

Deployment Enhancements Recommendations

This section describes the recommended enhancements to the existing configuration.

Public Key Infrastructure

Easy VPN secure tunnel access to the corporate network can be provided using preshared keys (PSKs) as well as a public key infrastructure (PKI) setup. We recommend PKI because it is more secure and provides enhanced device management capabilities.

Use the following configuration to implement PKI on the server side:

```
     crypto isakmp client configuration group easyvpn-group
 key <ezvpn-preshared-key>
 dns <dns-server>
 wins <wins-server>
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn_split_tunnel
 save-password
!
crypto isakmp profile easyvpn-group
   description PSK group
   match identity group easyvpn-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 1
```

to this:

```
crypto isakmp client configuration group easyvpn-group
 dns <dns-server>
 wins <wins-server>
 domain cisco.com
 pool easyvpn-pool
 acl ezvpn_split_tunnel
 save-password
!
crypto isakmp profile easyvpn-group
   description PKI group
   ca trust-point <ezvpn-certificate-server>
```

```
   match identity group easyvpn-group
   client authentication list easyVPN
   isakmp authorization list easyVPN
   client configuration address respond
   virtual-template 1
```

This change removes the configured preshared key from the client configuration group, and adds the Certificate Authority trustpoint and certificate matching statements in the profile.

You must also configure a PKI trustpoint, as well as a certificate map:

```
crypto pki trustpoint ezvpn-certificate-server
 enrollment mode ra
 enrollment url http://ezvpn-certificate-server:80
 serial-number
 ip-address none
 password 7 1107160B
 revocation-check none
!
```

The crypto isakmp policy must be modified to allow authentication other than preshare:

```
crypto isakmp policy 2
 encr 3des
 group 2
```

On the client side, remove the “group <easyvpn-group> key <EzVPNkey>” line from the crypto ipsec client configuration:

```
crypto ipsec client EasyVPN vpnserver
 connect auto
 group <easyvpn-group> key <EzVPNkey>
 mode client
 peer <enter-you-easyvpn-server-ip-here>
 username <EzVPNuser> password <EzVPNpassword>
 xauth userid mode local
```

and add an RSA digital certificate where the OU field of the subject name matches the Easy VPN server certificate map:

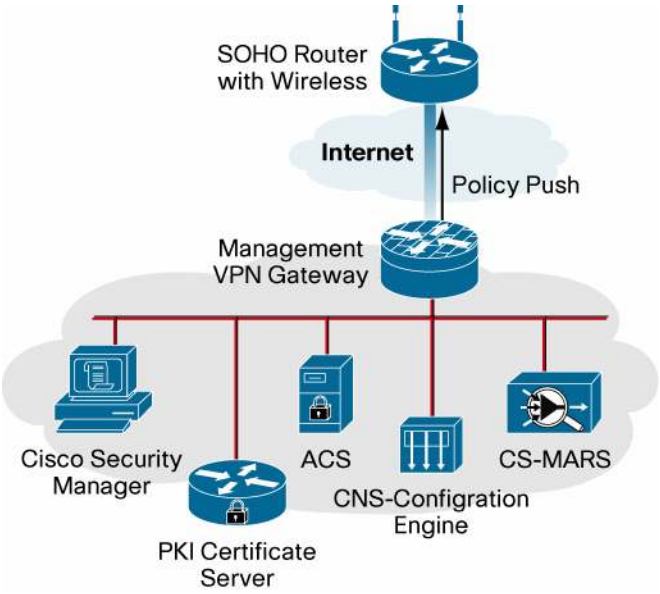
```
crypto pki trustpoint ezvpn-certificate-server
  enrollment url http://ezvpn-certificate-server:80
  serial-number
  !!! The OU field MUST be set to the same ezvpn group name.
  subject-name OU=easyvpn-group
  revocation-check crl
```

Then all you need to do is enroll the Easy VPN client with the same PKI server as the Easy VPN server.

Management Tunnel

We recommend that you dedicate one tunnel specifically for management, which should be completely separate from the corporate data access tunnels (Figure 1). The main objective is to always have a secure link to the remote device for policy update, image management, and device and user authentication—this setup also prevents the situation where connectivity is lost if policies are changed over the data channel.

Figure 1. Management Network



You need to have DVTI configured instead of traditional Easy VPN—because only DVTI can provide dual-tunnel configuration.

You can establish the management tunnel by adding the following configuration, with preshared keys. You can introduce the same modifications discussed earlier to use PKI instead.

```
crypto ipsec client ezvpn smg-psk
connect auto
group <group> key <key>
mode client
peer <easyvpn management server>
virtual-interface 1
username <ezvpn-user> password <ezyvpn-password>
xauth userid mode local
```

Wireless Access

Wireless access greatly enhances the end-user experience by providing freedom of mobility while maintaining the same performance as a wired connection. Extensible Authentication Protocol (EAP) provides a secure two-way centralized authentication between the client and the Cisco

Secure Access Control Server (ACS). EAP-Protected EAP (EAP-PEAP) is the recommended, widely used EAP authentication method.

To configure wireless access on the Cisco 881W, refer to the Cisco Virtual Office—Secure Wireless.

Authentication Proxy

Cisco IOS Firewall Authentication Proxy (AuthProxy) is a powerful way to provide an extra level of security by doing a layer 3 end-user authentication. It is useful in many situations such as:

- If a home PC has saved 802.1x credentials, anyone who uses that PC will be able to connect. If AuthProxy is enabled, the end user needs to enter an authorization, authorization, and accounting (AAA) username and password to access corporate servers. By default an ACL is configured on the LAN side interface that blocks all corporate traffic.
- If the router or PC is stolen, then the AuthProxy provides an extra level of authentication.
- If the home network is extended with a switch or hub, all PCs need to authenticate separately, so AuthProxy is effective in this situation.

Troubleshooting

For Easy VPN, use the following commands to verify the connection or configuration:

- debug crypto isakmp: Displays errors during phase 1
- debug crypto ipsec: Displays errors during phase 2
- debug crypto engine: Displays information from the cryptography 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

For user authentication for 802.1x and wireless, use:

- debug radius: Displays errors or failures during authentication

Note: You should also check the Cisco Secure ACS RADIUS logs for failed authentications.

References

- Cisco Virtual Office solution guides and information: http://www.cisco.com/go/cvo
- Cisco Feature Navigator: http://www.cisco.com/go/fn
- Cisco Security Manager: http://cisco.com/go/csmanager
- Easy VPN: http://cisco.com/go/easyvpn

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-458259-01 09/08