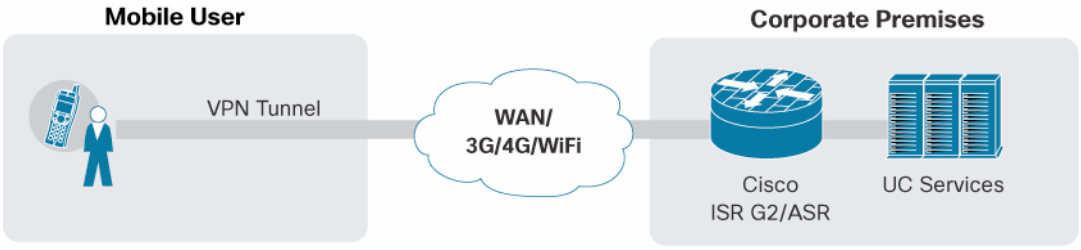
Mobile Workforce Architecture: VPN Deployment Guide for Microsoft Windows Mobile and Android Devices with Cisco Integrated Services Router Generation 2

This deployment guide explains the configuration of the Cisco IOS® VPN Integrated Services Router Generation 2 (ISR G2) head-end router for use with native VPN clients of Microsoft Windows Mobile and Android devices. This guide assumes that the basic Cisco IOS VPN head-end configuration is in place. The configurations discussed here include any network-related settings, such as inside and outside interface assignments, IP address configuration, hostname, domain, and default routes. Configurations are shown using the Cisco® command-line interface (CLI).

As shown in Figure 1, a smartphone user (using an Android or Windows Mobile device) can use the built-in VPN client or native VPN client of the device and terminate the secure, encrypted VPN tunnels on the Cisco ISR G2 router. Thus, Cisco IOS VPN effectively serves as a single point of convergence for multiple smartphones.

Figure 1. VPN Termination from Smartphone to Cisco ISR G2 Router



This deployment guide has two main parts:

- Part 1 discusses the configurations required on Cisco IOS VPN head-end routers to support Android and Windows Mobile. Note that both Windows Mobile and Android use native Layer 2 Tunnel Protocol (L2TP) and IP Security (IPsec) for connectivity. Windows Mobile works with both the preshared key (PSK) and public key infrastructure (PKI) options, but Android works only with PSK. Android cannot yet use L2TP or IPsec with PKI.
- Part 2 consists of Appendixes A and B, which discuss manual installation of VPN settings on Windows Mobile and Android devices.

Part 1: Cisco IOS VPN Head-End Configuration

Following are the steps to configure the VPN gateway to work with Android and Windows Mobile devices. Authentication is based on PKI and certificates either from a Microsoft or Cisco IOS Software certificate authority (CA). This document assumes a Microsoft CA.

Table 1 lists the high-level steps required to configure Cisco IOS Software to support Android and Windows Mobile devices.

Table 1. Steps for Configuring Cisco IOS Software Android and Windows Mobile Devices

Steps	Description
1	Define authentication, authorization, and accounting (AAA) settings.
2	Define the PKI trustpoint.
3	Authenticate and enroll with the CA.
4	Define L2TP settings.
5	Define Internet Security Association and Key Management Protocol (ISAKMP) policy.
6	Define a pool from which the client is assigned an IP address.
7	Define the username and password for the L2TP user.
8	Define the transform set.
9	Define the IPsec profile.
10	Define the virtual template.

Step 1: Define AAA Settings

This step defines the AAA settings. Here, local is used as the default method of authentication and authorization. You could also set up your IT AAA account here.

```
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa session-id common
```

Step 2: Define the PKI Trustpoint

This step defines the PKI trustpoint and the CA server to be used. Because of some strict requirements set by the device operating systems, some of the settings shown here are mandatory.

```
crypto pki trustpoint <trustpoint name>
enrollment mode ra
enrollment url http://<CA server url>
```

```
! e.g. http://ca.cisco.com:80/certsrv/mscep/mscep.dll
serial-number
fqdn <IP Address of WAN Interface>
ip-address none
subject-name CN=<IP Address of WAN Interface>
revocation-check none
```

Step 3: Authenticate and Enroll with the CA

This step helps ensure that the router uses the Simple Certificate Enrollment Protocol (SCEP) enrollment process, so you need a Microsoft CA with an SCEP client.

```
crypto pki authenticate <CA server name>
crypto pki enroll <CA server name>
```

Step 4: Define L2TP Settings

Define L2TP settings as shown here. Define a virtual template (template 10 here) and use the same virtual template later.

```
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 10
 source-ip <IP address of WAN Interface>
 source vpdn-template 10
 l2tp security crypto-profile l2tp keep-sa
 l2tp tunnel hello 15
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session 5000
```

Step 5: Define ISAKMP Policy

This step defines ISAKMP policy and settings. Windows Mobile can use PKI policy: for example, policy 2. Android cannot yet use PKI. PSK-based policies (such as policies 5 and 7, shown here) can be used by both Windows Mobile and Android devices.

```
crypto isakmp policy 2
 encr 3des
 group 2
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
crypto isakmp policy 7
 encr aes
 authentication pre-share
 group 2
```

```
Create the ISAKMP pre-shared key using below command. Note below we are using
test as the PSK
```

```
crypto isakmp key test address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
```

Step 6: Define a Pool from Which the Client Is Assigned an IP Address

This step defines the pool used to assign an IP address to the client.

```
ip local pool l2tp-pool <first_ip_addrlast_ip_addr>
```

Step 7: Define the Username and Password for the L2TP User

Define the username and password for the user. You can also use AAA for this task.

```
username cisco password cisco
```

Step 8: Define the Transform Set

This step defines the IPsec settings.

```
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec transform-set t3 esp-aes 256 esp-sha-hmac
 mode transport require
crypto ipsec transform-set t4 esp-3des esp-sha-hmac
 mode transport require
```

Step 9: Define the IPsec Profile

This profile links all transform sets under a single profile.

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
 set transform-set t3 t4 t1
```

Step 10: Define the Virtual Template

This step associates the physical interface with the virtual interface and applies the IPsec profile to the virtual interface.

```
interface Virtual-Template10
   ip unnumbered <WAN interface>(i.e. Fa4 etc)
   ip mtu 1400
   ip tcp adjust-mss 1200
   peer default ip address pool l2tp-pool
   ppp mtu adaptive
   ppp authentication ms-chap ms-chap-v2
   ppp timeout idle <define time out>


interface FastEthernet4
   no ip dhcp client request tftp-server-address
   ip address dhcp
   load-interval 30
   duplex auto
   speed auto
   crypto map l2tpsec
   !
```

Note: If you are using Loopback 1 as the WAN interface here, the configuration would be:

```
Interface Loopback 1
ip address <routable WAN IP><subnet mask>
```

Part 2: Appendixes

This section describes the step-by-step installation and management of VPN settings on mobile phones, including VPN policy, VPN settings, and VPN connectivity.

Appendix A: Windows Mobile Manual Step-by-Step VPN Configuration with Certificates

Note that these steps are for a Microsoft Windows Mobile Professional device. Some steps may vary from platform to platform.

1. From the Microsoft website, install Windows Mobile Device Center for Windows Vista or Windows 7, or install Microsoft ActiveSync for Windows XP. Microsoft ActiveSync 4.5.0 was used for testing. You can also use any other tool that can synchronize certificates from your device to your computer.
2. Connect your Windows Mobile device to the PC using the USB cable provided.
3. Upgrade your Windows Mobile software, if needed, using iTunes.
4. Request a certificate for the phone from RA-CA-SERVER at IP of CA server>/certsrv.
5. Install the certificate on your local computer.
6. Export the certificate.
   a. For Export the Private Keys, click Yes.
   b. Select Include All the Certificates in the Certification Path If Possible.
   c. Type a password.
   d. Provide a name for the certificate, such as Winmobile.p12. Complete the export. The certificate is exported to the desktop.
   e. Push this certificate from your local machine to your phone. Check your IT policy to email the certificate to yourself and open it on your phone, or use the Windows Mobile Device Center to push the certificate to your phone.
7. After the certificate has been installed on your device, you need to be sure that the network configuration is correctly defined on the phone. If the main connection is not configured as an Internet connection, but instead is configured as a work connection, the device will not dial the VPN.
   a. Choose Start > Settings > Connections > Connections. You should see two connections listed: My ISP and My Work Network. If you do not see these connections listed, choose Start > Settings > Connections > Connections > Advanced > Select Networks and make sure that you have two networks defined: an internal network called My ISP and an intranet network called My Work Network.
   b. You can add exceptions under Start > Settings > Connections > Connections > Advanced > Exceptions – Add URL. You can add *.*/* to launch VPN when browsing to any website. You can customize this option based on your domain name: for example, *. cisco.com. VPN will be launched on demand only when you browse to any website ending with cisco.com.

8. Define the L2TP and IPsec settings.
    a. Choose Start > Settings > Connectivity > Edit my VPN Settings > Add New.
    b. Define the name and hostname. Specify the IP address of the VPN gateway and VPN Type = l2tp/ipsec.
    c. Choose the authentication mechanism. Select Certificate Based (you can also choose PSK if you want to use the **test** key defined in the sample configuration here).
    d. Define the username and password from your AAA configuration. Specify cisco/cisco as shown in the sample configuration here.
    e. Click Finish to save the VPN profile.
    f. To connect to VPN using this profile, select this VPN profile and click Connect.

Appendix B: Android Manual Step-by-Step VPN Configuration with PSK

1. Choose Settings > Wireless and Networks >VPN Settings > Add VPN > Add L2TP/IPSecPSKVPN.
2. Use the following settings:
    a. Define VPN Name: Enter a name here.
    b. Set VPN Server: Define the IP address here.
    c. Set IPSec Pre-Shared Key: Define the key here; the sample configurations here used test.
    d. Enable L2TP Secret: Keep this option disabled.
    e. DNS Search Domains: Do not set this option.
3. Save this profile. Try connecting to this profile. Upon connection, you will be prompted for the username and password. Choose cisco/cisco based on the configuration set up here. If you use an AAA server, make sure to use those credentials. Your VPN should connect using this VPN profile.

For More Information

Read more about the Cisco Mobile Workforce Architecture, or contact your local account representative.

Read more about Cisco ISR G2.

Read more about Cisco Unified Communications Manager Business Edition.

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 C07-677829-00 06/11