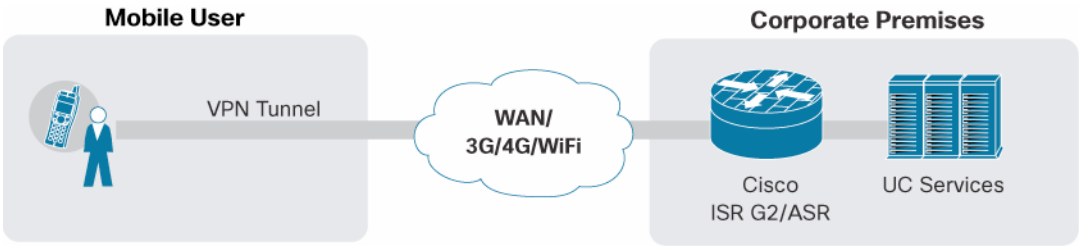
Mobile Workforce Architecture: VPN Deployment Guide for Nokia, iPhone, and RIM Devices with Cisco Integrated Services Router Generation 2

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 Nokia, Apple iPhone, and RIM devices. This guide assumes that the basic Cisco IOS VPN head-end configuration is in place. The configurations discussed here include any network-related configurations, 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 a Nokia, iPhone, or RIM 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 Nokia, iPhone, and RIM devices. Cisco IOS Software Release 151-3.T.bin was the version tested. Note that unlike Nokia and iPhone devices, which work over 3G, 4G, and WiFi networks, RIM IP Security (IPsec) VPN works only over WiFi hotspots. Also note that RIM devices with public key infrastructure (PKI) work only when xAuth with PKI is enabled on the RIM device.
- Part 2 consists of Appendixes A, B, and C, which discuss manual installation of VPN settings on iPhone, Nokia, and RIM devices.

Part 1: Cisco IOS VPN Head-End Configuration

Following are the steps to configure the VPN gateway to work with iPhone, Nokia, and RIM devices. Authentication is based on PKI and certificates either from a Microsoft or Cisco IOS Software certificate authority (CA). This guide assumes a Microsoft CA. This guide also assumes that there is not a split tunnel and that profile matching is based on the OU or department field in the certificate.

Table 1 lists the high-level steps required to configure Cisco IOS Software to support Nokia, iPhone, and RIM devices.

Table 1. Steps for Configuring Cisco IOS Software for Nokia, iPhone, and RIM 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 the certificate map.
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 mode configuration parameters.
8	Define the ISAKMP profile.
9	Define the transform set.
10	Define the IPsec profile.
11	Define the virtual template.

Step1: Define AAA Settings

This step defines the AAA settings. Here, **local** is used as the default method of authentication and authorization.

```
aaa new-model
aaa authentication login default local none
aaa authorization network default local none
```

Step 2: Define the PKI Trustpoint

This step defines the PKI trustpoint and the CA server to be used. Note that depending on the phone OS type—Nokia, iPhone, or RIM—some settings inside the trustpoint, such as fqdn/subjecname/ip-address, must exactly match the configuration shown here.

```
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 <IP Address of WAN Interface>
subject-name CN=<IP Address of WAN Interface>
revocation-check none
authorization username subjectname commonname
```

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 the Certificate Map

Define a certificate map for smartphones. Note that two certificate maps are created. RIM and Nokia use only the phonepki certificate map. iPhones use two certificate maps (phonepki and dummy) because of certain restrictions in Apple iOS.

```
Crypto pki certificate map phonepki 10
   subject-name co phonepki

crypto pki certificate map DUMMY 20
   subject-name co dummy
```

Step 5: Define ISAKMP Policy

This step defines the ISAKMP policy and settings.

```
Crypto isakmp policy 1
Encryption 3des
group 2

crypto isakmp keepalive 10 10
crypto isakmp nat keepalive 50
crypto isakmp xauth timeout 90
```

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 easyvpn-pool <first_ip_addrlast_ip_addr>
```

Step 7: Define the Mode Configuration Parameters

This step defines the parameters that an Easy VPN client receives from the server. The dummy profile is used only for iPhone devices.

```
Crypto isakmp client configuration group phonepki
   dns<dns server IP>
   domain<domain name>
   pooleasyvpn-pool
```

save-password -----⟶ forces the client to save the password

```
crypto isakmp client configuration group dummy
   dns <dns server IP>
   domain <domain name>
   pool easyvpn-pool
```

Step 8: Define the ISAKMP Profile

This step defines an ISAKMP profile that links the CA server, maps, AAA settings, and mode configuration parameters defined here in a single profile.

```
Crypto isakmp profile phonepki
   ca trust-point <trustpoint name>
   match identity group phonepki
   match identity user-fqdn domain cisco.com
   client authentication list local !! needed only if doing xauth
   isakmp authorization list local
   client configuration address
   respond virtual-template 6
cryptoisakmp profile dummy – need a dummy profile for iPhone
   self-identity address
   match identity group dummy
   client authentication list local
   isakmp authorization list local
   client configuration address respond
   virtual-template 6
```

Step 9: Define the Transform Set

This step defines the IPsec settings.

```
Crypto ipsec transform-set t1esp-3desesp-sha-hmac
Crypto ipsec transform-set t3esp-aes 256 esp-sha-hmac
 mode transport require
crypto ipsec transform-set t4esp-3desesp-sha-hmac
 mode transport require
```

Step 10: Define the IPsec Profile

This profile links all transform sets under a single profile.

```
Crypto ipsec profile stealth
 set transform-set t3 t4 t1
```

Step 11: 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-Template6 type tunnel
   ip unnumbered <WAN interface>
   ip mtu 1400
```

```
    iptcp adjust-mss 1200
    tunnel mode ipsecipv4
    tunnel path-mtu-discovery
    tunnel protection ipsec profile stealth shared

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

Note

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

  Interface `Loopback1`
  `ip address <`**`routable WAN IP><subnet mask`**`>`

- For RIM, you need to define a username and password along with the certificates:
  `username xyz password xyz`

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: Nokia E Series Manual Step-by-Step VPN Configuration with Certificates

This section provides step-by-step instructions for the installation and management of VPN settings on the Nokia E Series devices.

The Nokia E Series phone needs to be activated and associated with a phone number, and Internet access must be operational.

1. From nokia.com, install Nokia PC Suite on your PC.
2. Use Nokia PC Suite to upgrade the Nokia firmware, connecting through USB, Bluetooth, or infrared.
   Open a browser on your computer and request a certificate for the phone from the CA server at http://<IP of CA server>/certsrv. Note that the department field is the same as that defined in the configuration of the Cisco IOS VPN head-end router (for example, phonepki). Install the certificate on your computer.
3. 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 Mobile E72Certificate.p12. Complete the export. The certificate is exported to the desktop.
4. Create a VPN policy using the Nokia Mobile VPN Client Policy Tool. Match the VPN configurations based on the VPN configurations made on the Cisco IOS Software and create a .vpn file.
   Use Nokia PC Suite to connect the phone to the PC with USB or Bluetooth.

a. Copy the TEST11.vpn policy to any of the folders of the Nokia E72.

5. Disconnect the phone from USB.
6. Choose E72 > Menu > Office > File Manager and find the new VPN client. Install the VPN client.
7. Choose Menu > Office > File Manager and find the new VPN policy. Click and install the policy. Provide the P12 password (used in Step 3) and then a phone store password (the new password must contain no fewer then six characters).
8. Choose Menu >Tools > Settings > General > Security > Certificate Management > Authority Certificates and make sure that the RA-CA-SERVER certificate is installed.
9. Choose Menu > Tools > Settings > General > Security > Certificate Management > Phone Certificate and make sure that Mobile E72Certificate.p12 is installed.
10. Choose Menu > Tools > Settings > Connectivity > Destinations > Internet and make sure that your service provider's 3G or 4G network is listed. Add an access point if you are using a public hotspot.
11. Choose Menu > Tools > Settings > Connectivity > Destinations > Intranent > VPN > Edit VPN and make sure that VPN internally is using the Internet destination group. Choose Automatically Connect in the VPN settings.
12. Launch a browser and use the intranet access point configured earlier and make sure that you can access corporate resources. You can also choose Applications > Office > Intranet and manually connect to the intranet.

Appendix B: iPhone Manual Step-by-Step VPN Configuration with Certificates

The iPhone must be activated and associated with a phone number, and Internet access must be operational.

1. Install the iPhone Configuration Utility and iTunes from www.apple.com. The iPhone Configuration Utility Version 3.2.0.267 was used for testing.
2. Connect your iPhone to the PC using the USB cable provided.
3. Upgrade your iPhone software, if needed, using iTunes.
4. Open the iPhone Configuration Utility.
5. Request a certificate for the phone from RA-CA-SERVER at http://<IP of CA server>/certsrv. Note that the department field should be the same as that defined in the configuration of the Cisco IOS VPN gateway: for example, phonepki.
6. Install the certificate on your local computer.
7. 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: for example, iPhone.p12.
   e. Complete the export. The certificate is exported to the desktop.
8. Use the iPhone Configuration Utility to create a VPN policy according to the Cisco IOS Software configurations shown earlier.
   a. Define the General Settings: You can name your profile whatever you want and define a corresponding identifier.

b. Define the PKSC 12 certificate. Choose Credentials and click Configure. This process will automatically guide you to select the certificate you want to use for VPN connectivity.

c. Define the VPN settings. For the connection type, use iPsec. Also use the identity certificate configured in Step b.

9. Install this profile on the phone. Then choose Settings > VPN on your iPhone. Manually select the certificate on the phone if you did not select the certificate in Step 8. Turn on VPN connectivity on your iPhone.

Appendix C: RIM Manual Step-by-Step VPN Configuration with Certificates

1. Download the certificate to your computer as described in Appendix A or B.
2. Synchronize the certificates on your computer with your RIM device using the Blackberry Desktop Manager Certificate Synchronization Tool. Version 5.0.1 was used here.
3. In Version 6.0, you need a custom installation to get this option: http://docs.blackberry.com/tr-tr/admin/deliverables/14334/Users_cant_find_cert_synch_tool_602750_11.jsp.
4. Choose Options > Security > Advanced Security Options > VPN > Add a New VPN Profile. Change or define the parameters as shown here.

Note: RIM VPN works only with WiFi. Make sure to select the VPN profile under the RIM WiFi settings.

```
Name: <define any name>
Gateway Typ: Cisco IOSWith Easy VPN Server
Concentrator address: 128.x.x.x.
Group name:phonepki
Group Password:
User Name:cisco
User Password: cisco
 Save Password: Select This option
Client Certificate          <Select certificate>
CA Certificate <Select certificate>
Select button “Dynamically Determine DNS>
IP Address:
Subnet Mask:
Primary DNS:
Secondary DNS:
Domain Name:
IKE DH Group:  <Select Group>
IKE Cipher: Select 3DES (168-bit Key)
IKE Hash : Select HMACSHA1 (160 bitys)
Select button <Perfect Forward Secrecy>
IPSec Crypto and has suite : Select 3DES-SHA1
NAT timeout (in minutes):1
Unselect <use hard token>
Software token Serial Number <None Available>
Select <Disable VPN banner>
```

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 C07-677813-00 06/11