CHAPTER 17

Configuring Virtual Private Networks

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

The Cisco VPN Client for Cisco Unified IP Phones adds another option for customers attempting to solve the remote telecommuter problem by complementing other Cisco remote telecommuting offerings.

- Easy to Deploy—All settings configured via CUCM administration.
- Easy to Use—After configuring the phone within the Enterprise, the user can take it home and plug it into their broadband router for instant connectivity, without any difficult menus to configure.
- Easy to Manage—Phone can receive firmware updates and configuration changes remotely.
- Secure—VPN tunnel only applies to voice and Cisco Unified IP Phone services. A PC connected to the PC port is responsible for authenticating and establishing it own tunnel with VPN client software.

Supported Devices

You can use Cisco Unified Reporting to determine which Cisco Unified IP Phones support the VPN client. From Cisco Unified Reporting, click **Unified CM Phone Feature List**. For the Feature, choose **Virtual Private Network Client** from the pull-down menu. The system displays a list of products that support the feature.

For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

Configuring the VPN Feature

To configure the VPN feature for supported Cisco Unified IP Phones, follow the steps in the following table.

Table 17-1 VPN Configuration Checklist

Configuration Steps		Notes and Related Procedures
Step 1	Set up the VPN concentrators for each VPN Gateway.	For configuration information, refer to the documentation for the VPN concentrator; such the following: • *SSL VPN Client (SVC) on ASA with ASDM Configuration Example* http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008071c428.shtml **Note** The ASA software must be version 8.0.4 or later, and the "AnyConnect Cisco VPN Phone" license must be installed. **Note** To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, Cisco recommends that you set up the VPN concentrator close in the network to the TFTP or Cisco Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TPTP or load server that is next to the VPN concentrator. • *SSL VPN Client (WebVPN) on IOS with SDM Configuration Example* http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa61.shtml **Note** The IOS software must be versions 15.1(2)T or later. Feature Set/License:" Universal (Data & Security & UC)" for the 2900 models and "Advanced Security" for the 2800 models with SSL VPN licenses activated. **Note** To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, Cisco recommends that you set up the VPN concentrator close in the network to the TFTP or Cisco Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TPTP or load server that is next to the VPN concentrator.
Step 2	Upload the VPN concentrator certificates.	Chapter 18, "Configuring a VPN Gateway"
Step 3	Configure the VPN Gateways.	Chapter 18, "Configuring a VPN Gateway"
Step 4	Create a VPN Group using the VPN Gateways.	Chapter 19, "Configuring a VPN Group"
Step 5	Configure the VPN Profile	Chapter 20, "Configuring a VPN Profile"

Table 17-1 VPN Configuration Checklist

Configuration Steps		Notes and Related Procedures
Step 6	Add the VPN Group and VPN Profile to a Common Phone Profile.	In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Phone Profile**. For more information, see the "Common Phone Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. **Note** If you do not associate a VPN Profile with the Common Phone Profile, VPN uses the default settings defined in the VPN Feature Configuration window.
Step 7	Upgrade the firmware for Cisco Unified IP Phones to a version that supports VPN.	To run the Cisco VPN client, a supported Cisco Unified IP Phone must be running firmware release 9.0(2) or higher. For more information about upgrading firmware, see the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* for your Cisco Unified IP Phone model. **Note** Before you can upgrade to firmware release 9.0(2), supported Cisco Unified IP Phones must be running firmware release 8.4(4) or later.
Step 8	Using a supported Cisco Unified IP Phone, establish a VPN connection.	For more information about configuring a Cisco Unified IP Phone and establishing a VPN connection, see the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* for your Cisco Unified IP Phone model.

IOS configuration requirements

Before you create an ISO configuration for VPN client on IP phone, complete the following steps:

Step 1 Install IOS Software version 15.1(2)T or later

Feature Set/License: Universal (Data & Security & UC) for IOS ISR-G2

Feature Set/License: Advanced Security for IOS ISR

Step 2 Activate the SSL VPN License

Configuring IOS for VPN client on IP phone

Perform the following steps to configure IOS for VPN client on IP phone.

Step 1 Configure IOS locally.

a. Configure the Network Interface

Example:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b. Configure static and default routes.

router(config)# **ip route <***dest_ip***> < *mask*> < *gateway_ip*>**

Example:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

Step 2 Generate and register the necessary certificates for Cisco Unified Communications Manager and IOS.

The following certificates need to be imported from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters)
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Cisco Unified Communications Manager certificates

a. From the Cisco Unified Communications Manager OS Administration web page.

b. Choose **Security** > **Certificate Management**. (Note: This location may change based on the UCM version)

c. Find the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as .txt file

d. Create trustpoint on the IOS

Example:

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates

e. You should generate the following IOS self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 1024 1024
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.

Example:

```
Router> enable
Router# configure terminal
```

```
Router(config)# crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain name>
Router(config-ca-trustpoint)# subject-name CN=<full domain name>, CN=<IP>
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

  Router(config)# **crypto pki export <name> pem terminal**
  Copy the text from the terminal and save it as a .pem file and upload it to the Managing Certificate part of the CUCM.

Step 3 Install Anyconnect on IOS.

Download anyconnect package from cisco.com and install to flash

Example:

```
router(config)#webvpn install svc flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

Step 4 Configure the VPN feature. You can use the Sample IOS configuration summary bellow to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:
`username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted`

Sample IOS configuration summary

You can use the following sample IOS configuration for VPN client on IP phone as a general guideline to creating your own configurations. The configuration entries can change over time.

```
Current configuration: 4648 bytes
!
! Last configuration change at 13:48:28 CDT Fri Mar 19 2010 by test
!
version 15.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
! hostname of the IOS
hostname vpnios
!
boot-start-marker

! Specifying the image to be used by IOS - boot image
boot system flash c2800nm-advsecurityk9-mz.152-1.4.T
boot-end-marker
!
!
logging buffered 21474836
!
```

```
aaa new-model
!
!
 aaa authentication login default local
 aaa authentication login webvpn local
 aaa authorization exec default local
 !
 aaa session-id common
 !
 clock timezone CST -6
 clock summer-time CDT recurring
 !
 crypto pki token default removal timeout 0
 !

! Define trustpoints
 crypto pki trustpoint iosrcdnvpn-cert
  enrollment selfsigned
  serial-number
  subject-name cn=iosrcdnvpn-cert
  revocation-check none
  rsakeypair iosrcdnvpn-key 1024
 !
 crypto pki trustpoint CiscoMfgCert
  enrollment terminal
  revocation-check none
  authorization username subjectname commonname
 !
 crypto pki trustpoint CiscoRootCA
  enrollment terminal
  revocation-check crl
  authorization username subjectname commonname
 !
 !
! Certificates
 crypto pki certificate chain iosrcdnvpn-cert
  certificate self-signed 04
 crypto pki certificate chain CiscoMfgCert
  certificate ca 6A6967B3000000000003
 crypto pki certificate chain CiscoRootCA
  certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
 crypto pki certificate chain test
  certificate ca 00
 dot11 syslog
 ip source-route
 !
 !
 ip cef
 !
 !
 !
 ip domain name nw048b.cisco.com
 no ipv6 cef
 !
 multilink bundle-name authenticated
 !
!
 voice-card 0
 !
 !
 !
 license udi pid CISCO2821 sn FTX1344AH76
 archive
  log config
```

```
  hidekeys
 username admin privilege 15 password 0 vpnios
 username test privilege 15 password 0 adgjm
 username usr+ privilege 15 password 0 adgjm
 username usr# privilege 15 password 0 adgjm
 username test2 privilege 15 password 0 adg+jm
 username CP-7962G-SEP001B0CDB38FE privilege 15 password 0 adgjm
 !
 redundancy
 !
!
!--- Configure interface. Generally one interface to internal network and one outside
 interface GigabitEthernet0/0
  description "outside interface"
  ip address 10.89.79.140 255.255.255.240
  duplex auto
  speed auto
 !
 interface GigabitEthernet0/1
  description "Inside Interface"
  ip address dhcp
  duplex auto
  speed auto
 !
!--- Define IP local address pool
 ip local pool webvpn-pool 10.8.40.200 10.8.40.225
 ip default-gateway 10.89.79.129
 ip forward-protocol nd
 ip http server
 ip http authentication local
 ip http secure-server
 ip http timeout-policy idle 60 life 86400 requests 10000
 !
 !
!--- Define static IP routes
ip route 0.0.0.0 0.0.0.0 10.89.79.129
ip route 10.89.0.0 255.255.0.0 10.8.40.1
 !
 no logging trap
 access-list 23 permit 10.10.10.0 0.0.0.7
!
 control-plane
 !
line con 0
  exec-timeout 15 0
 line aux 0
! telnet access
 line vty 0 4
  exec-timeout 30 0
  privilege level 15
  password vpnios
  transport input telnet
 line vty 5 15
  access-class 23 in
  privilege level 15
  transport input all
 !
 exception data-corruption buffer truncate
 scheduler allocate 20000 1000
 !

! webvpn gateway configuration
 webvpn gateway VPN_RCDN_IOS
  hostname vpnios
```

```
  ip address 10.89.79.140 port 443
! ssl configuration
  ssl encryption aes128-sha1
  ssl trustpoint iosrcdnvpn-cert
  inservice
  !
! webvpn context for User and Password authentication
 webvpn context UserPasswordContext
  title "User-Password authentication"
  ssl authenticate verify all
  !
  !
  policy group UserPasswordGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
    svc default-domain "nw048b.cisco.com"
    svc split include 10.89.75.0 255.255.255.0
    svc dns-server primary 64.101.128.56
    svc dtls
  default-group-policy UserPasswordGroup
  gateway VPN_RCDN_IOS domain UserPasswordVPN
  inservice
 !
 !
! webvpn context for Certificate (username pre-filled) and Password authentication
 webvpn context CertPasswordContext
  title "certificate plus password"
  ssl authenticate verify all
  !
  !
  policy group CertPasswordGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
    svc default-domain "nw048b.cisco.com"
    svc dns-server primary 64.101.128.56
    svc dtls
  default-group-policy CertPasswordGroup
  gateway VPN_RCDN_IOS domain CertPasswordVPN
  authentication certificate aaa
  username-prefill
  ca trustpoint CiscoMfgCert
  inservice
 !
 !
! webvpn context for certificate only authentication
 webvpn context CertOnlyContext
  title "Certificate only authentication"
  ssl authenticate verify all
  !
  !
  policy group CertOnlyGroup
    functions svc-enabled
    hide-url-bar
    timeout idle 3600
    svc address-pool "webvpn-pool"
    svc default-domain "nw048b.cisco.com"
    svc dns-server primary 64.101.128.56
    svc dtls
  default-group-policy CertOnlyGroup
  gateway VPN_RCDN_IOS domain CertOnlyVPN
```

```
 authentication certificate
 ca trustpoint CiscoMfgCert
 inservice
!
end
```

ASA configuration requirements

Before you create an ASA configuration for VPN client on IP phone, complete the following steps:

Step 1 Install ASA software (version 8.0.4 or later) and compatible ASDM

Step 2 Install a compatible anyconnect package

Step 3 Activate License

a. Show features of the current license.
show activation-key detail

b. For a new license with additional SSL VPN sessions and Linksys phone enabled, visit http://www.cisco.com/go/license. Select “Any Connect Cisco VPN phone” license to support the VPN feature.

Configuring ASA for VPN client on IP phone

Perform the following steps to configure ASA for VPN client on IP phone.

Step 1 Local configuration

a. Configure network interface.

Example:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b. Configure static routes and default routes.

router(config)# ip route <dest_ip> <mask> <gateway_ip>

Example:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

c. Configure the DNS.

Example:

```
hostname(config)# dns domain-lookup inside
hostname(config)# dns server-group DefaultDNS
hostname(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

Step 2 Generate and register the necessary certificates for Cisco Unified Communications Manager and IOS.

The following certificates need to be imported from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters)
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

  To import these Cisco Unified Communications Manager certificates

a. From the Cisco Unified Communications Manager OS Administration web page.

b. Choose **Security** > **Certificate Management**. (Note: This location may change based on the UCM version)

c. Find the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as .txt file

d. Create trustpoint on the IOS

Example:

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates

e. You should generate the following IOS self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 1024 1024
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.

  Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name> <exportable
-optional>
Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain name>
Router(config-ca-trustpoint)# subject-name CN=<full domain name>, CN=<IP>
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

```
Router(config)# crypto pki export <name> pem terminal
```

Copy the text from the terminal and save it as a .pem file and upload it to the Managing Certificate part of the CUCM.

Step 3 Configure the VPN feature. You can use the Sample IOS configuration summary bellow to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes vpn-group-policy GroupPhoneWebvpn
service-type remote-access
```

Sample ASA configuration summary

You can use the following sample ASA configuration for VPN client on IP phone as a general guideline to creating your own configurations. The configuration entries can change over time.

```
ciscoasa(config)# show running-config
: Saved
:

!--- ASA version
ASA Version 8.2(1)
!
!--- Basic local config on ASA
hostname ciscoasa
domain-name nw048b.cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard

!--- Configure interface. Generally one interface to internal network and one outside
!--- Ethernet0/0 is outside interface with security level 0
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.89.79.135 255.255.255.0

!--- Ethernet0/1 is inside interface with security level 100
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address dhcp
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
```

```
 no nameif
 security-level 100
 no ip address
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!

!--- Boot image of ASA
boot system disk0:/asa821-k8.bin
ftp mode passive

!--- Clock settings
clock timezone CST -6
clock summer-time CDT recurring

!--- DNS configuration
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 64.101.128.56
 domain-name nw048b.cisco.com


!--- Enable interface on the same security level so that they can communicate to each
other
same-security-traffic permit inter-interface
!--- Enable communication between hosts connected to same interface
same-security-traffic permit intra-interface
pager lines 24

!--- Logging options
logging enable
logging timestamp
logging console debugging
no logging message 710005
mtu outside 1500
mtu inside 1500
mtu management 1500

!--- Define IP local address pool
ip local pool Webvpn_POOL 10.8.40.150-10.8.40.170 mask 255.255.255.192
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside

!--- ASDM image
asdm image disk0:/asdm-623.bin
no asdm history enable
arp timeout 14400

!--- Static routing
route outside 0.0.0.0 0.0.0.0 10.89.79.129 1
route inside 10.89.0.0 255.255.0.0 10.8.40.1 1
route inside 0.0.0.0 0.0.0.0 10.8.40.1 tunneled

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
```

```
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 inside
http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

!--- ASA certs
!--- trustpoints and certificates
crypto ca trustpoint ASA_VPN_Cert
 enrollment self
 keypair ASA_VPN_Cert_key
 crl configure
crypto ca trustpoint CiscoMfgCert
 enrollment terminal
 crl configure
crypto ca trustpoint UCM_CAPF_Cert
 enrollment terminal
 no client-types
 crl configure
crypto ca certificate chain ASA_VPN_Cert
 certificate 02d5054b
  quit

crypto ca certificate chain CiscoMfgCert
 certificate ca 6a6967b3000000000003
  quit

crypto ca certificate chain UCM_CAPF_Cert
 certificate ca 6a6967b3000000000003
  quit
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0

!--- configure client to send packets with broadcast flag set
dhcp-client broadcast-flag
!--- specifies use of mac-addr for client identifier to outside interface
dhcp-client client-id interface outside
!
tls-proxy maximum-session 200
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!--- configure ssl
ssl encryption aes128-sha1
ssl trust-point ASA_VPN_Cert
ssl certificate-authentication interface outside port 443

!--- VPN config
!--- Configure webvpn
webvpn
 enable outside
 default-idle-timeout 3600
 svc image disk0:/anyconnect-win-2.1.0148-k9.pkg 1
 svc enable
```

```
!--- Group-policy
group-policy GroupPhoneWebvpn internal
group-policy GroupPhoneWebvpn attributes
 banner none
 vpn-simultaneous-logins 10
 vpn-idle-timeout none
 vpn-session-timeout none
 vpn-tunnel-protocol IPSec svc webvpn
 default-domain value nw048b.cisco.com
 address-pools value Webvpn_POOL
 webvpn
  svc dtls enable
  svc keep-installer installed
  svc keepalive 120
  svc rekey time 4
  svc rekey method new-tunnel
  svc dpd-interval client none
  svc dpd-interval gateway 300
  svc compression deflate
  svc ask none default webvpn

!--- Configure user attributes
username test password S.eA5Qq5kwJqZ3QK encrypted
username test attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!—Configure username with Phone MAC address for certificate+password method
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!--- Configure tunnel group for username-password authentication
tunnel-group VPNphone type remote-access
tunnel-group VPNphone general-attributes
 address-pool Webvpn_POOL
 default-group-policy GroupPhoneWebvpn
tunnel-group VPNphone webvpn-attributes
 group-url https://10.89.79.135/VPNphone enable

!--- Configure tunnel group with certificate only authentication
tunnel-group CertOnlyTunnelGroup type remote-access
tunnel-group CertOnlyTunnelGroup general-attributes
 default-group-policy GroupPhoneWebvpn
tunnel-group CertOnlyTunnelGroup webvpn-attributes
 authentication certificate
 group-url https://10.89.79.135/CertOnly enable

!--- Configure tunnel group with certificate + password authentication
tunnel-group CertPassTunnelGroup type remote-access
tunnel-group CertPassTunnelGroup general-attributes
 authorization-server-group LOCAL
 default-group-policy GroupPhoneWebvpn
 username-from-certificate CN
tunnel-group CertPassTunnelGroup webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client
 group-url https://10.89.79.135/CertPass enable

!
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 ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:cd28d46a4f627ed0fbc82ba7d2fee98e
: end
```