CHAPTER 17

バーチャル プライベート ネットワークの設定

Cisco Unified IP Phone の Cisco VPN クライアントはシスコの他の在宅勤務用製品を補完するもので、お客様が在宅勤務者に関連する問題を解決するのに役立ちます。

- 導入しやすい : すべての設定を CUCM の管理で設定できます。
- 使いやすい : 企業内で電話機を設定した後、その電話機を家に持ち帰ってブロードバンド ルータに差し込むだけで、難しい設定メニューを使用せずに即座に接続できます。
- 管理しやすい : 電話機は、ファームウェア アップデートおよび設定変更をリモートで受け取ることができます。
- 安全 : VPN トンネルは、音声および Cisco Unified IP Phone サービスだけに適用されます。PC ポートに接続されている PC により、VPN クライアント ソフトウェアを使用して専用のトンネルが認証および確立されます。

サポートされるデバイス

Cisco Unified Reporting を使用すると、Cisco Unified IP Phone でサポートされる VPN クライアントを確認できます。Cisco Unified Reporting で、[Unified CM Phone Feature List] をクリックします。[Feature] のプルダウン メニューから [Virtual Private Network Client] を選択します。その機能をサポートしている製品のリストが表示されます。

Cisco Unified Reporting の使用方法の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

VPN 機能の設定

サポートされている Cisco Unified IP Phone の VPN 機能を設定するには、次に示す手順を実行します。

表 17-1　VPN の設定用チェックリスト

設定手順		注意および関連手順
ステップ 1	VPN ゲートウェイごとに VPN コンセントレータをセットアップします。	設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』 http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008071c428.shtml **（注）** ASA ソフトウェアはバージョン 8.0.4 以降である必要があります。また、「AnyConnect Cisco VPN Phone」ライセンスがインストールされている必要があります。 **（注）** ユーザがリモート電話機でファームウェアまたは設定情報をアップグレードする際の長時間にわたる遅延を回避するために、VPN コンセントレータをネットワーク内の TFTP または Cisco Unified Communications Manager サーバの近くにセットアップすることをお勧めします。ネットワークでこのような設定を実現できない場合は、VPN コンセントレータの隣にある代替の TFTP またはロード サーバをセットアップできます。 • 『*SSL VPN Client (WebVPN) on IOS with SDM Configuration Example*』 http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa61.shtml **（注）** IOS ソフトウェアはバージョン 15.1(2)T 以降である必要があります。フィーチャ セット/ライセンス：2900 モデルの場合は「Universal (Data & Security & UC)」、SSL VPN ライセンスがアクティブになっている 2800 モデルの場合は「Advanced Security」。 **（注）** ユーザがリモート電話機でファームウェアまたは設定情報をアップグレードする際の長時間にわたる遅延を回避するために、VPN コンセントレータをネットワーク内の TFTP または Cisco Unified Communications Manager サーバの近くにセットアップすることを推奨します。ネットワークでこのような設定を実現できない場合は、VPN コンセントレータの隣にある代替の TFTP またはロード サーバをセットアップできます。
ステップ 2	VPN コンセントレータの証明書をアップロードします。	第 18 章「VPN ゲートウェイの設定」
ステップ 3	VPN ゲートウェイを設定します。	第 18 章「VPN ゲートウェイの設定」
ステップ 4	VPN　ゲートウェイを使用して VPN グループを作成します。	第 19 章「VPN グループの設定」
ステップ 5	VPN プロファイルを設定します。	第 20 章「VPN プロファイルの設定」

表 17-1　VPN の設定用チェックリスト（続き）

設定手順		注意および関連手順
ステップ 6	VPN グループおよび VPN プロファイルを共通の電話プロファイルに追加します。	Cisco Unified Communications Manager の管理ページで、[デバイス(Device)] > [デバイスの設定(Device Settings)] > [共通の電話プロファイル(Common Phone Profile)] の順に選択します。詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「共通電話プロファイルの設定」の章を参照してください。 **（注）** VPN プロファイルを共通の電話プロファイルに関連付けていない場合、VPN は [VPN 機能設定(VPN Feature Configuration)] ウィンドウで定義されているデフォルト設定を使用します。
ステップ 7	Cisco Unified IP Phone のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	Cisco VPN クライアントを実行するには、サポートされている Cisco Unified IP Phone でファームウェア リリース 9.0(2) 以降が稼動している必要があります。ファームウェアのアップグレード方法の詳細については、使用している Cisco Unified IP Phone モデルの『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。 **（注）** ファームウェア リリース 9.0(2) にアップグレードする前に、サポートされている Cisco Unified IP Phone でファームウェア リリース 8.4(4) 以降が稼動している必要があります。
ステップ 8	サポートされている Cisco Unified IP Phone を使用して、VPN 接続を確立します。	Cisco Unified IP Phone の設定および VPN 接続の確立の詳細については、使用している Cisco Unified IP Phone モデルの『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

IOS の設定要件

IP Phone で VPN クライアントの IOS 設定を作成する場合は、次の手順を実行します。

ステップ 1　IOS ソフトウェア バージョン 15.1(2)T 以降をインストールします。

フィーチャ セット / ライセンス：Universal (Data & Security & UC) for IOS ISR-G2

フィーチャ セット / ライセンス：Advanced Security for IOS ISR

ステップ 2　SSL VPN ライセンスをアクティブにします。

IP Phone での VPN クライアントの IOS の設定

IP Phone で VPN クライアントの IOS を設定するには、次の手順を実行します。

ステップ 1　IOS をローカルで設定します。

a.　ネットワーク インターフェイスを設定します。

例：

```
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. スタティック ルートとデフォルト ルートを設定します。

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

例：

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

ステップ 2　Cisco Unified Communications Manager と IOS に必要な証明書を生成および登録します。

次の証明書を Cisco Unified Communications Manager からインポートする必要があります。

- CallManager：TLS ハンドシェイク時に Cisco UCM を認証します（混合モードのクラスタでのみ必要）。
- Cisco_Manufacturing_CA：Manufacturer Installed Certificate（MIC; 製造元でインストールされる証明書）を使用して IP Phone を認証します。
- CAPF：LSC を使用して IP Phone を認証します。

これらの Cisco Unified Communications Manager 証明書をインポートするには、次の手順を実行します。

a. Cisco Unified Communications Manager OS の管理 Web ページで次を選択します。

b. [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します（注意：この場所は、UCM のバージョンによって異なる場合があります）。

c. Cisco_Manufacturing_CA と CAPF の証明書を見つけます。.pem ファイルをダウンロードし、.txt ファイルで保存します。

d. IOS でトラストポイントを作成します。

例：

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

Base 64 で暗号化された CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行から END 行までコピーし、貼り付けます。他の証明書でこの手順を繰り返します。

e. 次の IOS 自己署名証明書を生成して Cisco Unified Communications Manager に登録するか、または CA からインポートする証明書と置き換えます。

- 自己署名証明書を生成します。

例：

```
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
```

- Cisco Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして自己署名証明書を生成します。

  例：

```
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
```

- 生成した証明書を Cisco Unified Communications Manager に登録します。

  例：

  Router(config)# **crypto pki export <name> pem terminal**
  端末からテキストをコピーして .pem ファイルとして保存し、これを CUCM の証明書の管理にアップロードします。

ステップ 3　AnyConnect を IOS にインストールします。

AnyConnect パッケージを cisco.com からダウンロードし、flash にインストールします。

例：

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

ステップ 4　VPN 機能を設定します。設定の参考として、次に示すサンプル IOS 設定を利用できます。

（注）　電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つユーザを作成します。ユーザ名では大文字と小文字が区別されます。次の例を参考にしてください。

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

サンプル IOS 設定

IP Phone で VPN クライアントの IOS 設定を独自に行う場合の一般的なガイドラインとして、次に示すサンプル設定を利用できます。設定の各エントリは変更される場合があります。

```
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 の設定要件

IP Phone で VPN クライアントの ASA 設定を作成する場合は、次の手順を実行します。

ステップ 1　ASA ソフトウェア（バージョン 8.0.4 以降）および互換性のある ASDM をインストールします。

ステップ 2　互換性のある AnyConnect パッケージをインストールします。

ステップ 3　ライセンスをアクティブにします。

a. 現行ライセンスの機能を表示します。
show activation-key detail

b. 追加の SSL VPN セッションと Linksys 電話機が有効になっている新しいライセンスについては、http://www.cisco.com/go/license を参照してください。VPN 機能をサポートする場合は、「Any Connect Cisco VPN phone」ライセンスを選択します。

IP Phone での VPN クライアントの ASA の設定

IP Phone で VPN クライアントの ASA を設定するには、次の手順を実行します。

ステップ 1　次のローカル設定を行います。

a. ネットワーク インターフェイスを設定します。

例：

```
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. スタティック ルートとデフォルト ルートを設定します。

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

例：

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

c. DNS を設定します。

例：

```
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
```

ステップ 2　Cisco Unified Communications Manager と IOS に必要な証明書を生成および登録します。

次の証明書を Cisco Unified Communications Manager からインポートする必要があります。

- CallManager : TLS ハンドシェイク時に Cisco UCM を認証します（混合モードのクラスタでのみ必要）。
- Cisco_Manufacturing_CA : Manufacturer Installed Certificate（MIC; 製造元でインストールされる証明書）を使用して IP Phone を認証します。
- CAPF : LSC を使用して IP Phone を認証します。

これらの Cisco Unified Communications Manager 証明書をインポートするには、次の手順を実行します。

a. Cisco Unified Communications Manager OS の管理 Web ページで次を選択します。

b. [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します（注意 : この場所は、UCM のバージョンによって異なる場合があります）。

c. Cisco_Manufacturing_CA と CAPF の証明書を見つけます。.pem ファイルをダウンロードし、.txt ファイルで保存します。

d. IOS でトラストポイントを作成します。

例 :

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

Base 64 で暗号化された CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行から END 行までコピーし、貼り付けます。他の証明書でこの手順を繰り返します。

e. 次の IOS 自己署名証明書を生成して Cisco Unified Communications Manager に登録するか、または CA からインポートする証明書と置き換えます。

- 自己署名証明書を生成します。

例 :

```
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
```

- Cisco Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして自己署名証明書を生成します。

例 :

```
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
```

- 生成した証明書を Cisco Unified Communications Manager に登録します。

  例：

  Router(config)# **crypto pki export <name> pem terminal**
  端末からテキストをコピーして .pem ファイルとして保存し、これを CUCM の証明書の管理にアップロードします。

ステップ 3　VPN 機能を設定します。設定の参考として、次に示すサンプル IOS 設定を利用できます。

（注） 電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つユーザを作成します。ユーザ名では大文字と小文字が区別されます。次の例を参考にしてください。

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

サンプル ASA 設定

IP Phone で VPN クライアントの ASA 設定を独自に行う場合の一般的なガイドラインとして、次に示すサンプル設定を利用できます。設定の各エントリは変更される場合があります。

```
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
```