Avaya Solution & Interoperability Test Lab

Configuring the Avaya VPNremote Phone for Certificate Authentication using the Cisco Adaptive Security Appliance (ASA) and the Microsoft Certificate Authority – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Avaya VPNremote Phone and the Cisco Adaptive Security Appliance (ASA) to use digital certificate based authentication of the IPSec VPN in a Public-Key Infrastructure (PKI). The Cisco ASA is deployed as an enterprise network perimeter security device and terminates IPSec VPN tunnel requests from the Avaya VPNremote Phone. The Microsoft Certificate Authority server is used as the trusted authority for both the Cisco ASA and Avaya VPNremote Phones. The Avaya VPNremote Phones and the Cisco ASA communicate with the Microsoft Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

©2007 Avaya Inc. All Rights Reserved.

TABLE OF CONTENTS

1. INTRODUCTION 3

2. EQUIPMENT AND SOFTWARE VALIDATED 5

3. MICROSOFT CERTIFICATE AUTHORITY CONFIGURATION 5

3.1. REQUESTING AN SCEP CHALLENGE PHRASE FROM THE MICROSOFT CA 8
3.2. EXPORTING THE CERTIFICATE FROM THE MICROSOFT CA 9

4. CISCO ASA CONFIGURATION 13

4.1. CERTIFICATE IMPORT AND ENROLLMENT 13
4.2. VPN WIZARD 21
4.3. CERTIFICATE GROUP MATCHING 28
4.4. DEFAULT ROUTE 31
4.5. VPNREMOTE PHONE TO VPNREMOTE PHONE DIRECT AUDIO 32

5. AVAYA VPNREMOTE PHONE CONFIGURATION 32

5.1. 46VPNSETTINGS.TXT FILE 33
5.2. DOWNLOADING THE DIGITAL CERTIFICATE 35

6. VERIFICATION 36

6.1. VERIFY THE INSTALLATION OF THE MICROSOFT SCEP ADD-ON 36
6.2. ASA ACTIVE VPN SESSIONS 37

7. CONCLUSION 39

8. ADDITIONAL REFERENCES 39

APPENDIX A: CISCO ASA COMMAND LINE CONFIGURATION 40

APPENDIX B: 46VPNSETTING.TXT 45

©2007 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure the Avaya VPNremote Phone to use digital certificate based authentication of the IPSec VPN (Virtual Private Network) to the enterprise network. The focus of these Application Notes is on the Avaya VPNremote Phone, the Cisco Adaptive Security Appliance, and the Microsoft Windows 2003 Server Certificate Authority.

The Avaya VPNremote Phone is a software based IPSec VPN client integrated into the firmware of an Avaya 4600 Series IP Telephone. This capability allows the Avaya IP Telephone to be used over a secure IPSec VPN from any broadband Internet connection. The end user experiences the same IP telephone features as if the phone were being used in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Digital certificate based authentication was introduced as a new feature in Release 2.1 of the Avaya VPNremote Phone. Digital certificate authentication is an alternative to using the pre-shared key, a.k.a. shared secret, method for the VPNremote Phone to identify and authenticate itself with the enterprise network during the IPSec tunnel setup. Certificate based authentication offers a more scalable and manageable authentication method to using pre-shared keys.

The sample network implemented in these Application Notes is presented in **Figure 1**. Avaya VPNremote Phones are deployed with broadband Internet access. A Cisco Adaptive Security Appliance, referred to as "Cisco ASA" throughout the remainder of these Application Notes, is deployed as a perimeter security device. The Cisco ASA supports the IPSec VPN tunnel termination from the Avaya VPNremote Phone. The Cisco Adaptive Security Device Manager (ASDM) graphical user interface application is used to configure the Cisco ASA. The final Cisco ASA command line configuration used in the sample configuration is provided in **Appendix A**. The configuration steps utilize a Cisco ASA model 5520. However, these configuration steps can be applied to other ASA models using the software version specified in **Table 1**.

A Microsoft Windows 2003 Server Certificate Authority (CA) is used to generate and host the digital certificate used by both the Avaya VPNremote Phone and the Cisco ASA. The Microsoft CA in the sample configuration is deployed in the enterprise network as a private certificate server for internal use by the enterprise.

The Cisco ASA, as well as all Avaya VPNremote Phones that use digital certificate authentication, must first obtain the digital certificate from the Microsoft CA through a certificate enrollment method. The Cisco ASA is configured for automatic certificate enrollment. The Avaya VPNremote Phones utilize the 46vpnsetting.txt configuration file for instruction on how to enroll and download the digital certificate from the Microsoft CA. The 46vpnsetting.txt variables, specifically related to digital certificate authentication, are included in **Section 5.** The full 46vpnsetting.txt file used in the sample configuration is included in **Appendix B**.

©2007 Avaya Inc. All Rights Reserved.

The Avaya VPNremote Phone must import the digital certificate from the Microsoft CA prior to the phone being deployed remotely. This is accomplished by connecting the Avaya VPNremote Phone directly to the corporate network and downloading the certificate from the Microsoft CA. When deploying large numbers of Avaya VPNremote Phones, Avaya recommends the download of the certificate be done at the same time the Avaya VPNremote Phone firmware is loaded on the phones as part of an Avaya VPNremote Phone preparation, or staging, process.

The Simple Certificate Enrollment Protocol (SCEP) is the protocol used by the Microsoft CA to securely transport key information and digital certificates to network devices, such as the Avaya VPNremote Phone and Cisco ASA. For the Microsoft CA to support SCEP, the Microsoft SCEP add-on for Certificate Services must be installed. Information on how to obtain and install the SCEP add-on is included in the **Section 3** of these Application Notes.

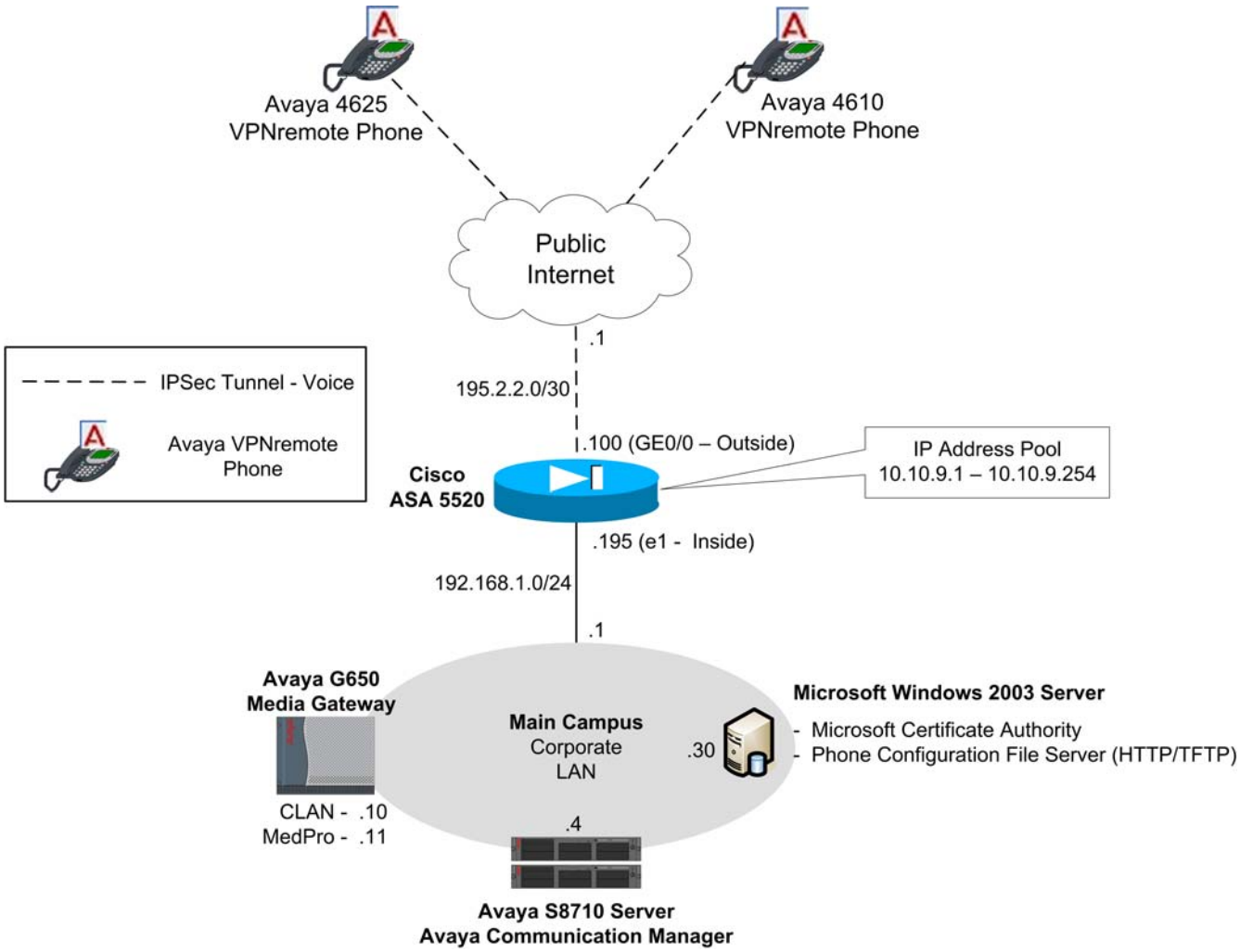


Figure 1: Network Diagram

©2007 Avaya Inc. All Rights Reserved.

2. Equipment and Software Validated

The information in these Application Notes is based on the software and hardware versions list in **Table 1** below.

Equipment	Software Version
Avaya S8710 Server	Avaya Communication Manager 4.0 Build 730.5
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	 FW 040 (HW10) FW 024 (HW017) FW 108 (HW12)
Avaya 4610SW IP Telephone	R2.3.2_4 – (a10bVPN232_4.bin)
Avaya 4625SW IP Telephone	R2.5.2_4 – (a25VPN252_4.bin)
Cisco ASA model 5520	7.2(1)
Cisco Adaptive Security Device Mgr.	5.2(1)

Table 1 – Software/Hardware Version Information

3. Microsoft Certificate Authority Configuration

The Avaya VPNremote Phones and the Cisco ASA use the Simple Certificate Enrollment Protocol (SCEP) when communicating with the Microsoft CA for Certificate Enrollment and Certificate Import. Therefore, the Microsoft CA must support SCEP. Microsoft provides an SCEP add-on to the Windows 2003 Certificate Authority. The SCEP add-on is available from the Windows Server 2003 Resource Kit or by downloading directly from the Microsoft Download Center at the following URL.

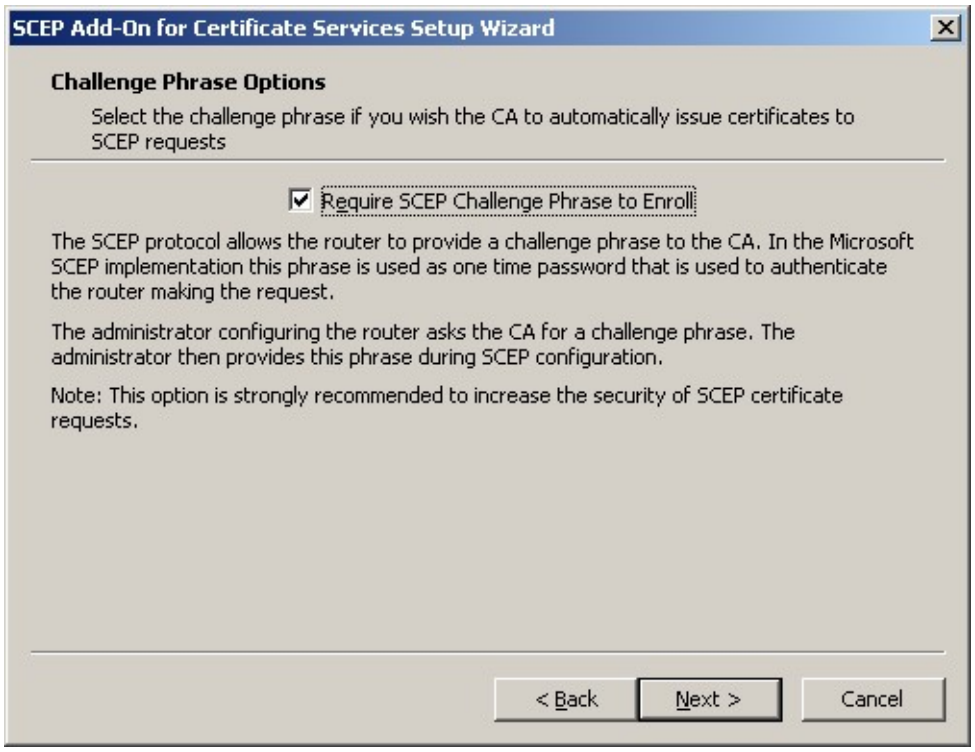
http://www.microsoft.com/downloads/details.aspx?familyid=9f306763-d036-41d8-8860-1636411b2d01&displaylang=en

The following steps describe how to install the SCEP add-on on an existing Microsoft CA.

1. Execute the SCEP add-on installation file, **cepsetup.exe**, from the Windows Server 2003 Resource Kit or the location downloaded from Microsoft.com. A confirmation window appears followed by the license agreement acceptance window then the “SCEP Add-On for Certificate Services Setup Wizard”. Select the appropriate Wizard options for the environment being installed. The following screens show relevant SCEP Wizard screens and options using for the sample configuration.

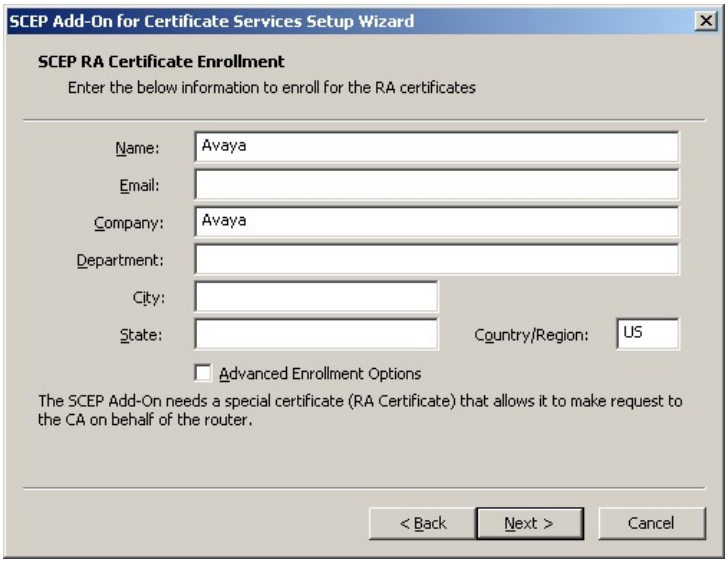
©2007 Avaya Inc. All Rights Reserved.

2. As recommended by Microsoft, the Challenge Phrase option is enabled in the sample configuration. The Challenge Phrase is a one time password generated by the Microsoft CA at the request of an administrator. Once the Challenge Phrase is used, it becomes invalid and a new challenge phrase request must be sent to the Microsoft CA to generate a password. This ensures certificates will not be downloaded from the Microsoft CA by unwanted devices. The process of requesting a Challenge Phrase from the Microsoft CA is described in **Section 3.1**. Because the Challenge Phrase is only valid for one time use, a new request must be made for each Avaya VPNremote Phone to import the digital certificate to the phone. The Avaya VPNremote Phone prompts for the Challenge Phrase to be entered when accessing the Microsoft CA to download the certificate. When deploying large numbers of Avaya VPNremote Phones this processes can become tedious. Consider deploying a Microsoft CA server with limited connectivity and the SCEP add-on Challenge Phrase option disabled when staging large numbers of Avaya VPNremote Phones. This eliminates the need to request a one-time password for each Avaya VPNremote Phone.

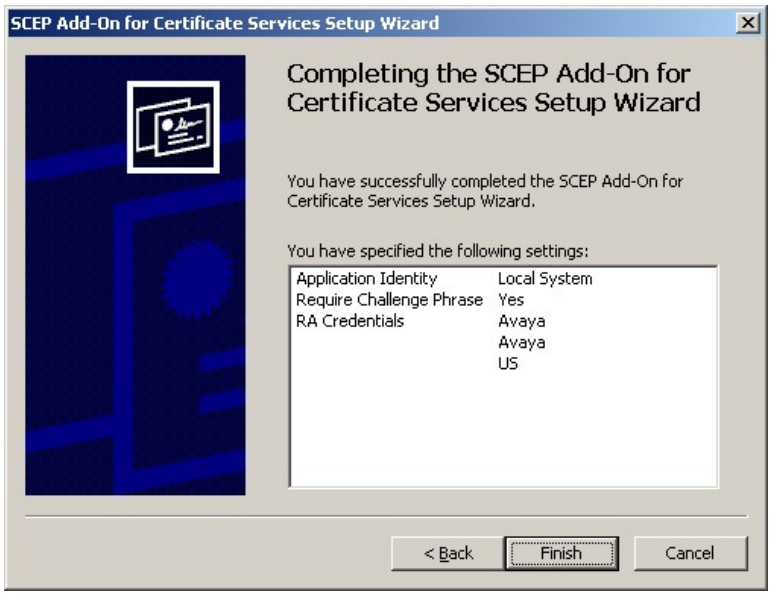


©2007 Avaya Inc. All Rights Reserved.

3. The SCEP add-on functions as a Registration Authority (RA) which makes requests to the Microsoft CA on behalf of network devices e.g., Avaya VPNremote Phones and Cisco ASA. An RA certificate must be associated with the SCEP add-on. The follow information is collected to create the RA certificate.



4. The following screen summarizes the selected options.



5. The following screen confirms the SCEP add-on was successfully installed and provides the URL used to access the SCEP enrollment page and generate the Challenge Phrase discussed in **Step 2**. "Avaya-iywd507jk" in the URL shown is the host name of the Microsoft CA used in the sample configuration. Alternatively, the IP address of the Microsoft CA can be used (http://192.168.1.30/certsrv/mscep/mscep.dll).

©2007 Avaya Inc. All Rights Reserved.

Once installed, see the SCEP add-on help page at the following URL for additional information: http://192.168.1.30/certsrv/mscep/mscephlp.htm

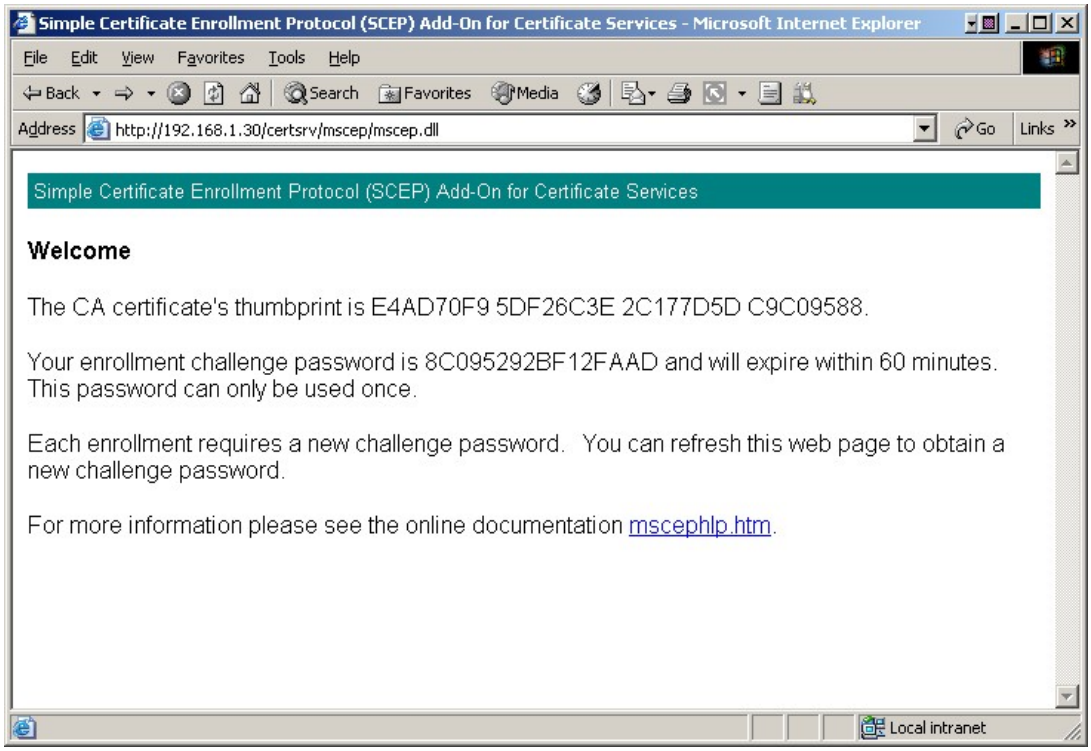


3.1. Requesting an SCEP Challenge Phrase from the Microsoft CA

If the "Require SCEP Challenge Phrase to Enroll" option was enabled during the SCEP add-on installation (**Section 3, Step 2**), a request for a new Challenge Phrase must be made for each device requiring enrollment to the Microsoft CA for import of a certificate. This includes the Cisco ASA and all Avaya VPNremote Phones using certificate authentication. The following steps describe how to generate a new Challenge Phrase.

1. From a web browser go to the URL displayed in the SCEP add-on installation dialog box shown in **Step 5** of **Section 3.0**. For example, using the IP address of the Microsoft CA in the sample configuration, the URL is "http://192.168.1.30/certsrv/mscep/mscep.dll".

2. The following page is displayed. The enrollment challenge password is generated, **8C095292BF12FAAD** in the example below. The password will expire after 60 minutes from the time it was generated and is only able to be used once.



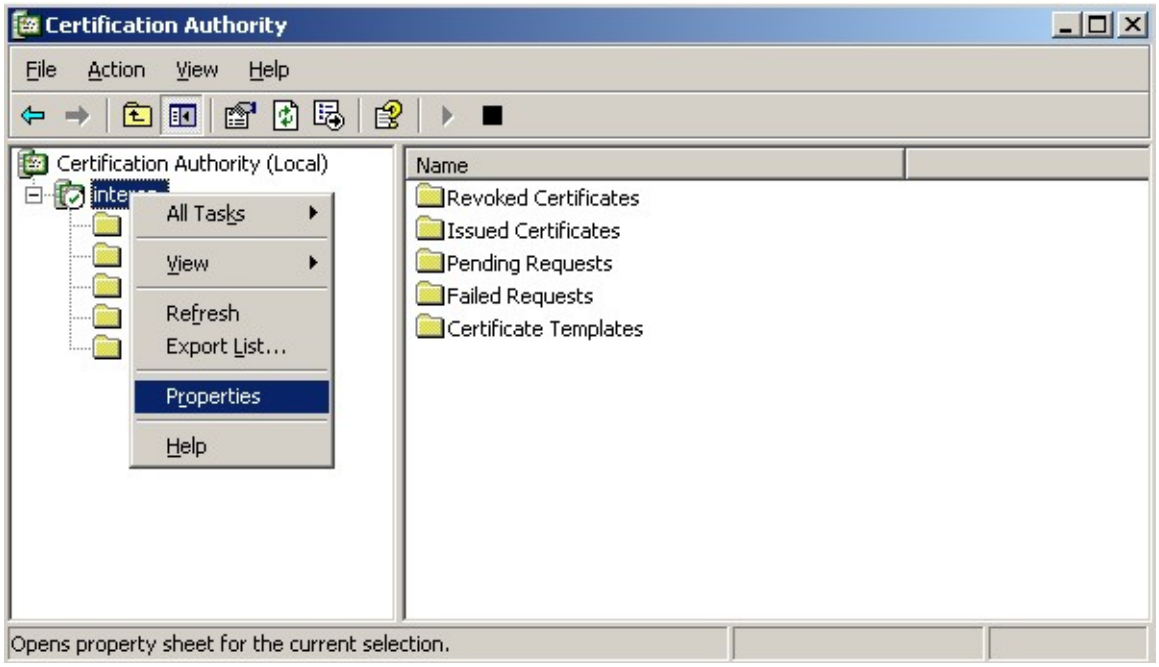
©2007 Avaya Inc. All Rights Reserved.

3.2. Exporting the Certificate from the Microsoft CA

For the Avaya VPNremote Phone to download the digital certificate, the certificate must first be exported from the Microsoft CA to a file with a ".cer" extension. Microsoft Windows associates files containing a ".cer" extension with a file type of "Security Certificate". The ".cer" file is then copied to the HTTP or TFTP phone configuration file server. The sample configuration uses Microsoft IIS as the HTTP phone configuration file server.

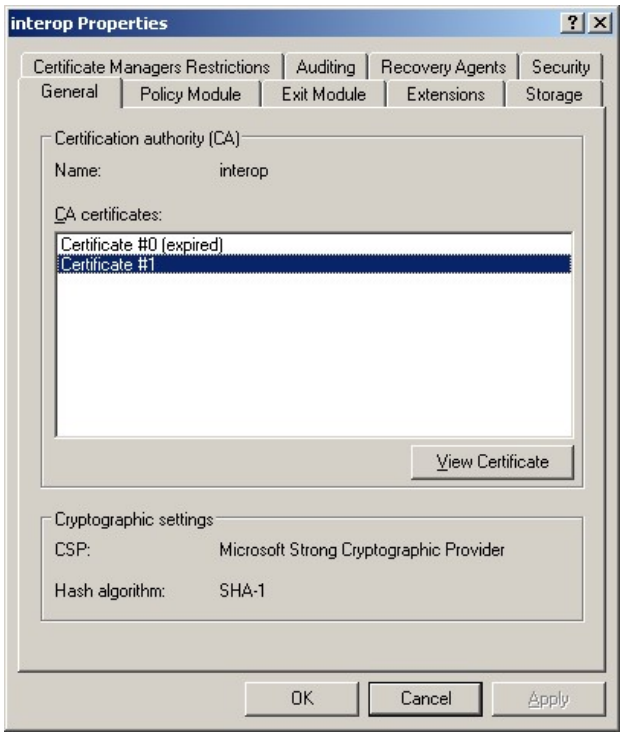
The following steps describe how to export the digital certificate from the Microsoft CA and copy to the Microsoft IIS root directory.

1. From the Microsoft CA management window, right click on the CA name in the left navigation window and select **Properties** from the drop-down window.

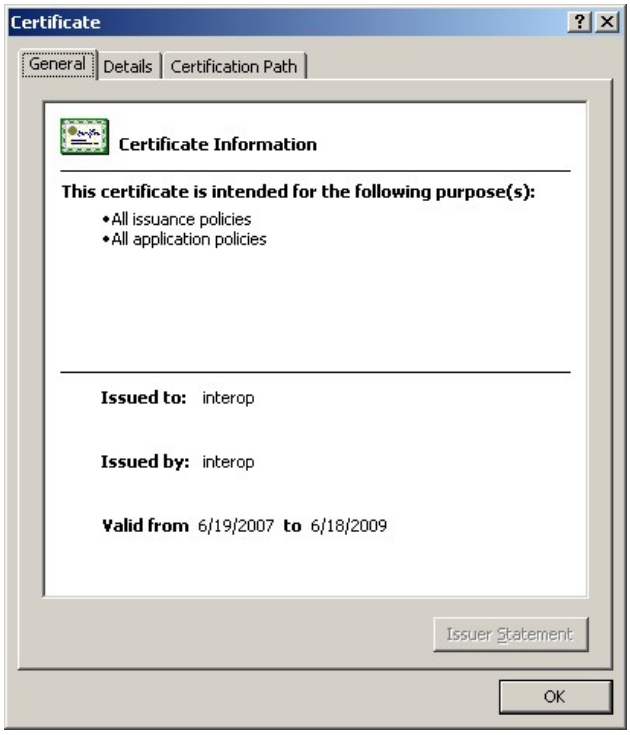


©2007 Avaya Inc. All Rights Reserved.

2. From the Properties window. Select the active certificate then click the **View Certificate** button.

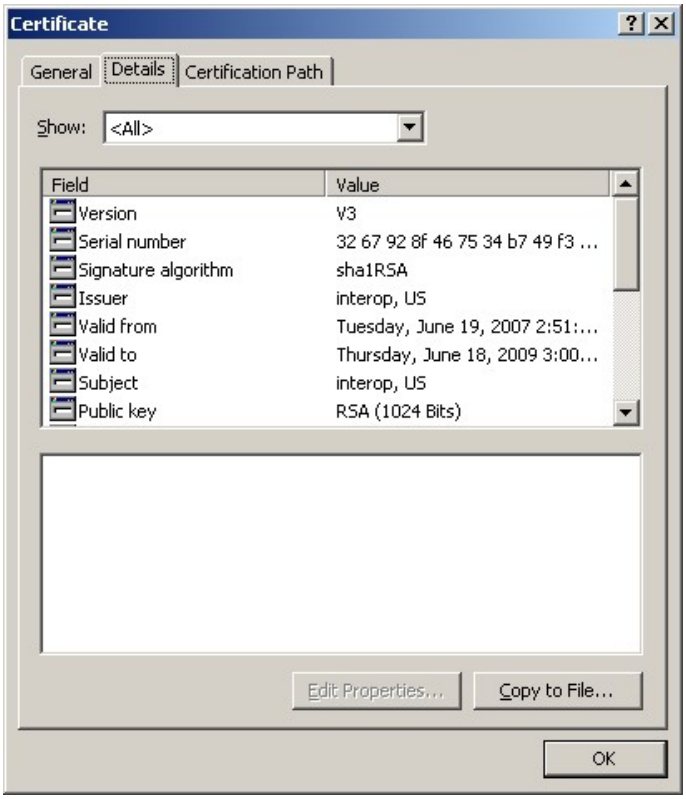


3. From the Certificate window, click the **Details** tab.



©2007 Avaya Inc. All Rights Reserved.

4. Click the **Copy to File** button.



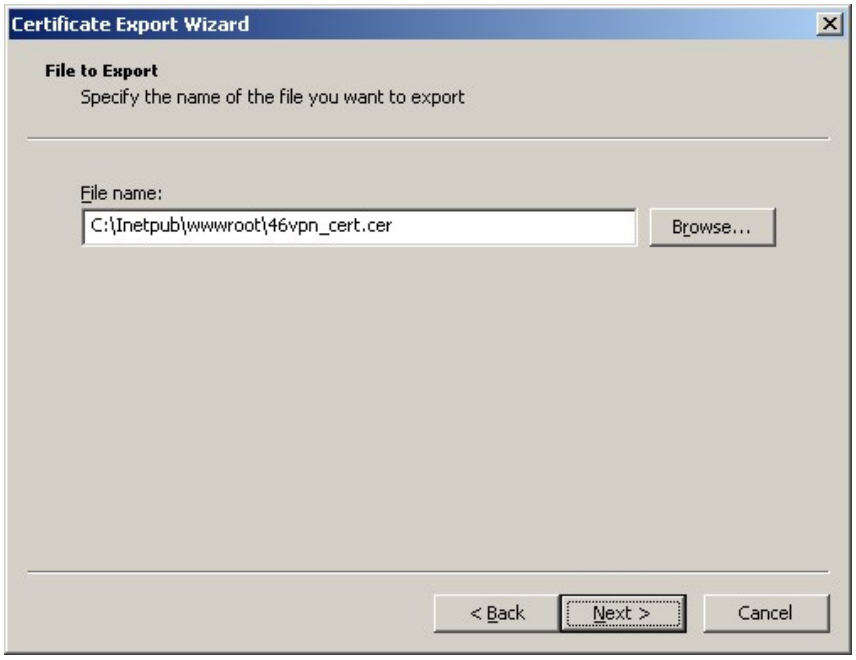
5. The **Certificate Export Wizard** starts. Click **Next** to continue.



©2007 Avaya Inc. All Rights Reserved.

6. Enter a name for the exported certificate file. Because Microsoft IIS is being used in the sample configuration, the path shown below is to the Microsoft IIS default web. Ensure the ".cer" file extension is used.

   Note: The file name length, excluding the ".cer" extension, can not be greater then 12 characters in length.



7. Click **Finish** to complete the Export Wizard.



©2007 Avaya Inc. All Rights Reserved.

8. A final status dialog box is displayed on the certificate export.



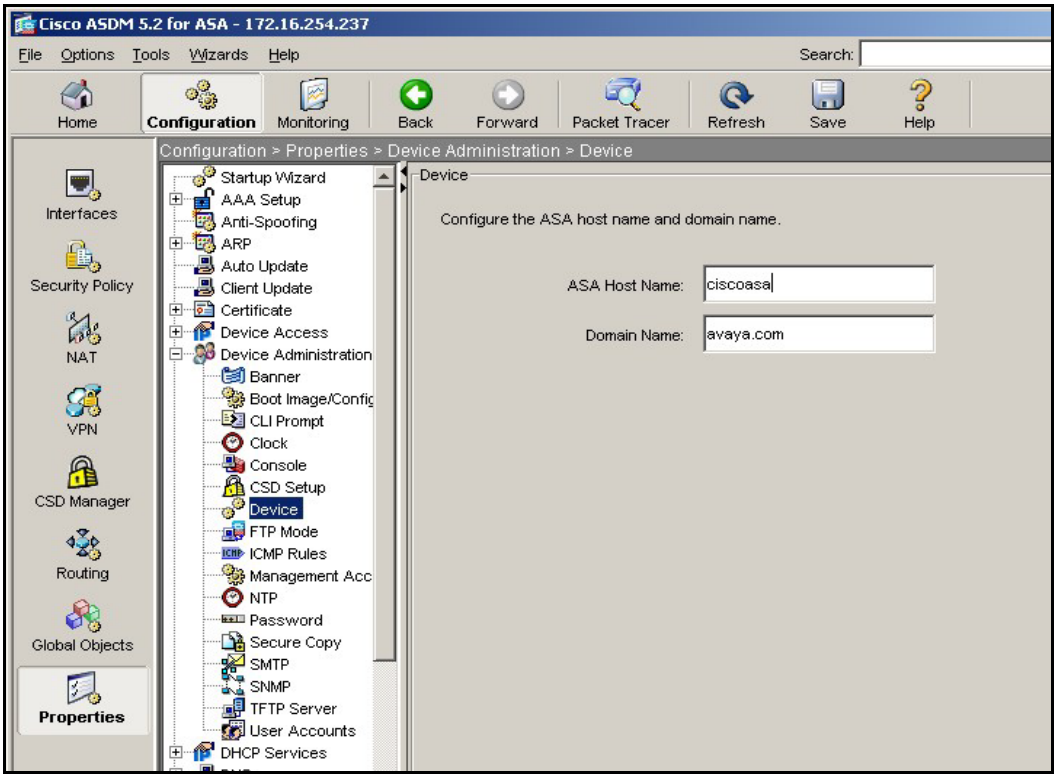
4. Cisco ASA Configuration

These Application Notes assume that the Cisco ASA is fully operational and configured to allow the Cisco ASDM to make configuration changes.

4.1. Certificate Import and Enrollment

The following steps describe how to import a digital certificate from and enroll with a Microsoft CA.

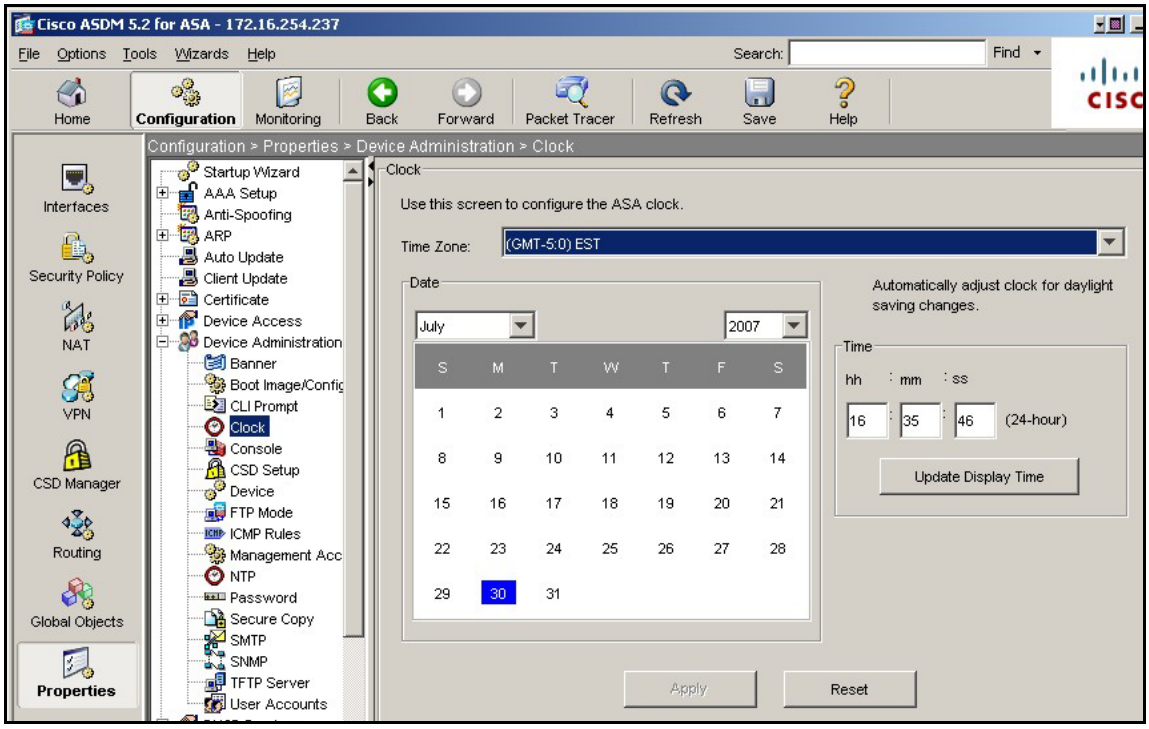
1. Verify the both CiscoASA Host and Domain names are set.
   - **a.** Open the ASDM application and click the **Configuration** button.
   - **b.** From the left menu, click the **Properties** button.
   - **c.** From the navigation pane, click **Device Administration > Device**.
   - **d.** Enter a Host Name and Domain Name for the Cisco ASA. Click the **Apply** button.



©2007 Avaya Inc. All Rights Reserved.

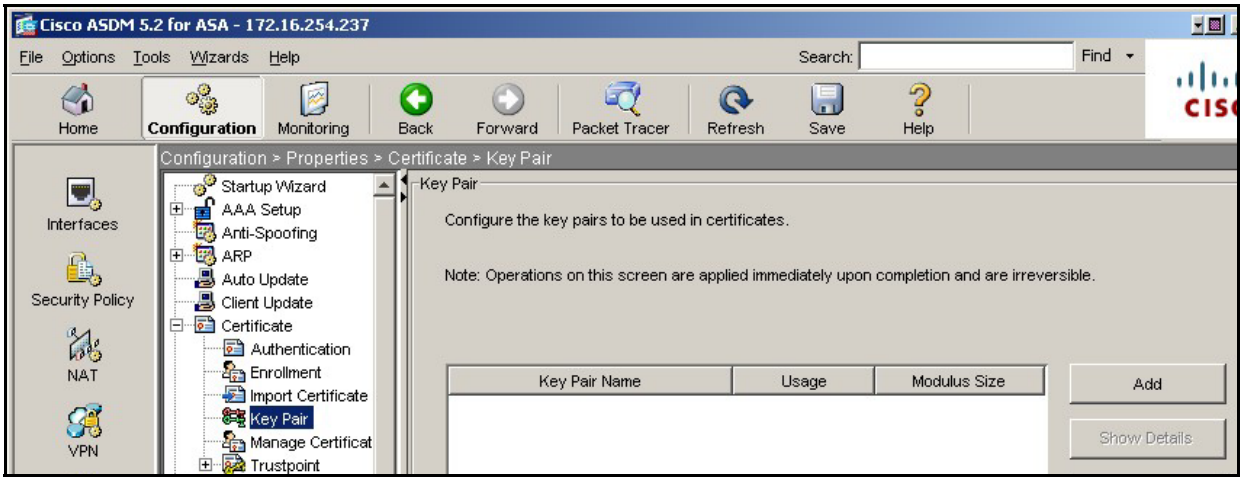
2. Configure the Cisco ASA with the correct date, time, and time zone. This is important for certificate generation of the device. Use of an NTP server is recommended.

   a. In the Clock window, use the fields and drop-down arrows to set the correct date, time, and time zone. Click **Apply**.



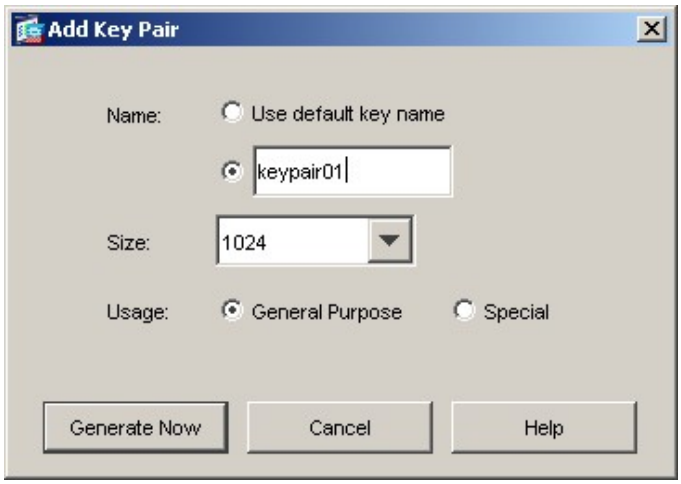
3. Configure the Cisco ASA key pair. The Cisco ASA must have its own private and public keys. The public key will be sent to the Microsoft CA during enrollment.

   a. From the navigation pane, click **Certificate > Key Pair**. The Key Pair window is displayed. Click the **Add** button.



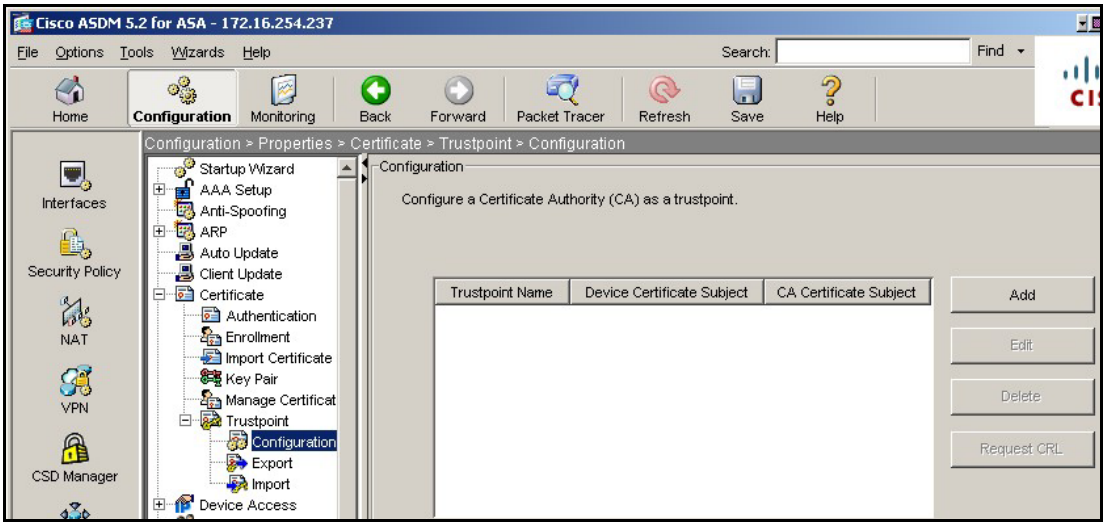
©2007 Avaya Inc. All Rights Reserved.

b. The Add Key Pair dialogue box is displayed. Check the radio button beside the blank field and enter a unique **Name** for the key pair. All remaining fields can be left at default values. Click the **Generate Now** button to generate the new key pair.



4. Configure the Microsoft CA to be a trusted device. From the navigation pane, click **Certificate > Trustpoint > Configuration**.

a. From the Configuration window, click the **Add** button.



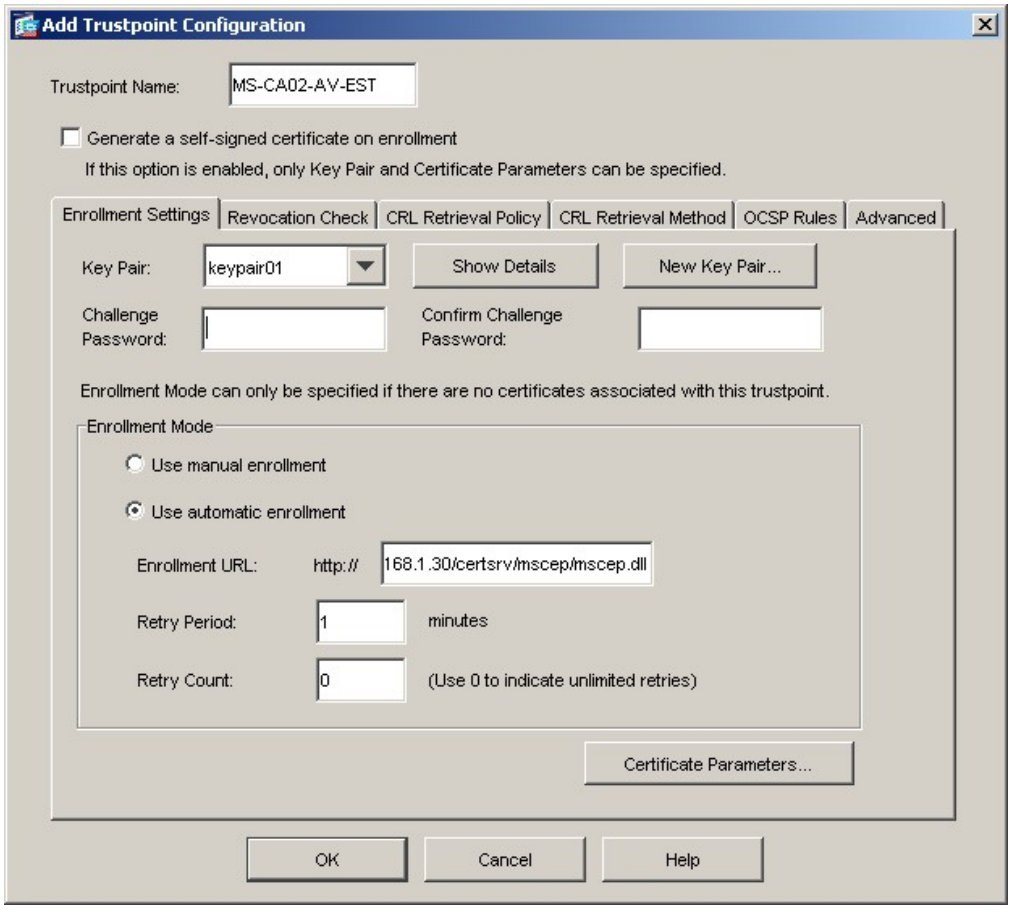
©2007 Avaya Inc. All Rights Reserved.

b. On the Add Trustpoint Configuration window, enter a name for the Trustpoint in the **Trustpoint Name** field.

c. From the **Key Pair** dropdown list, select the Key Pair created in **Step 3**.

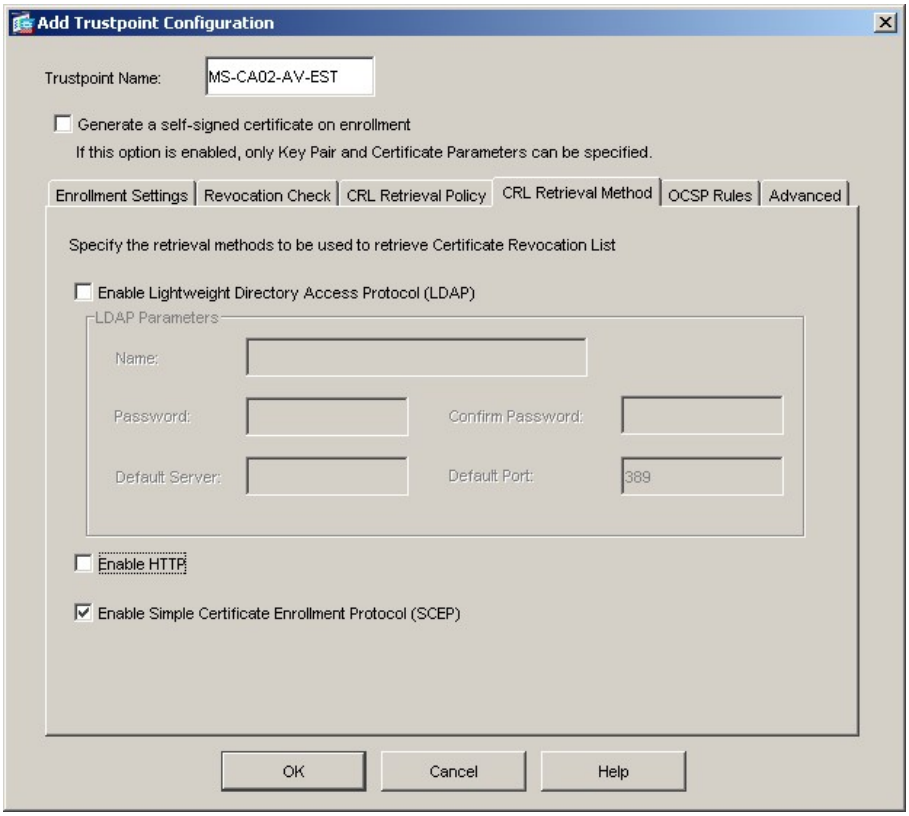
d. Generate a new Challenge Password, as described in **Section 3.1**, and enter the new password in the **Challenge Password** and **Confirm Challenge Password** fields.

e. Check the **Use automatic enrollment** radio button and enter the URL for the Microsoft CA: **<Microsoft CA IP Address>/certsrv/mscep/mscep.dll**. For the sample configuration, "192.168.1.30/certsrv/mscep/mscep.dll" was entered.



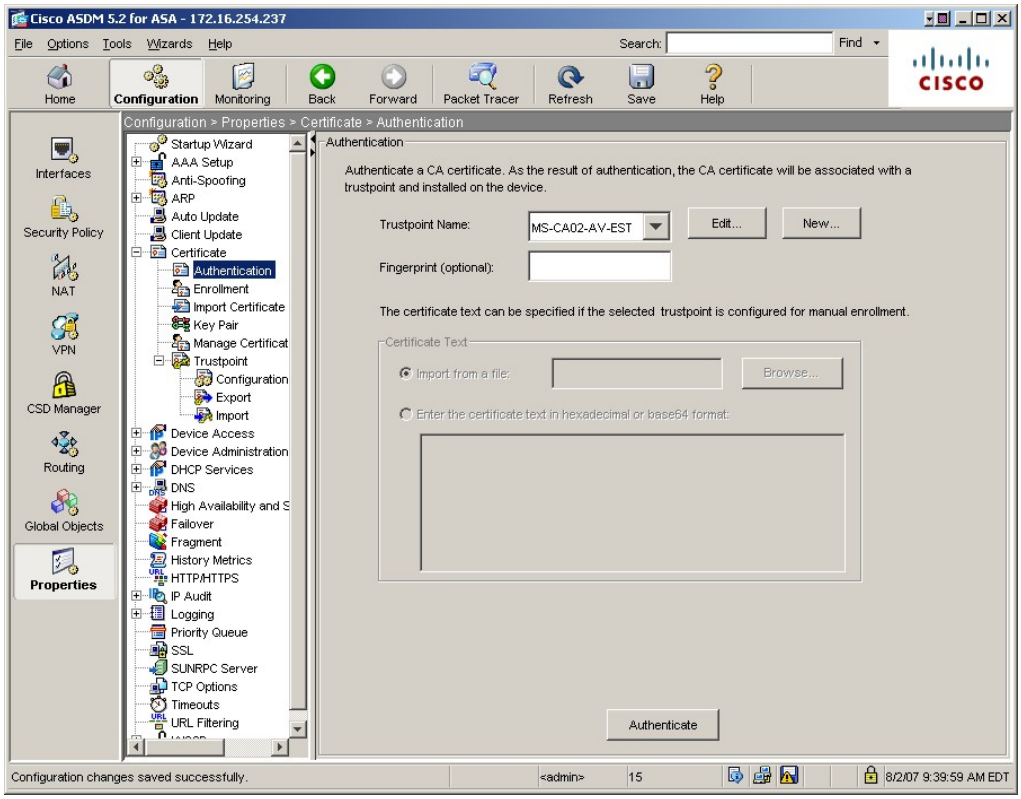
©2007 Avaya Inc. All Rights Reserved.

5. Click the **CRL Retrieval Method** tab.
    a. Uncheck the **Enable Lightweight Directory Access Protocol (LDAP)** and **Enable HTTP** check boxes.
    b. Leave the **Enable Simple Certificate Enrollment Protocol (SCEP)** check box checked. Leave all remaining fields default values.
    c. Click the **OK** button.

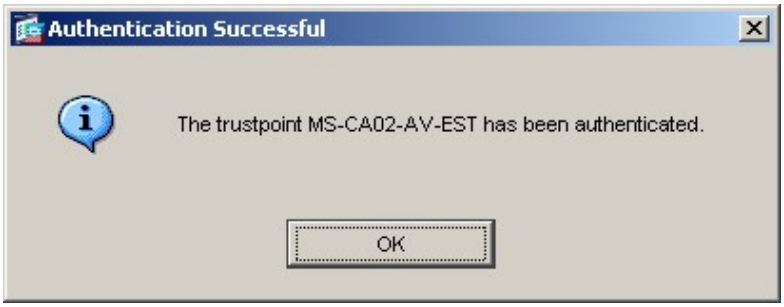


©2007 Avaya Inc. All Rights Reserved.

6. Authenticate with the Microsoft CA. From the navigation pane, click **Certificate > Authentication**. Select the Trustpoint created in **Step 4** from the **Trustpoint Name** drop-down list. Click the **Authenticate** button.

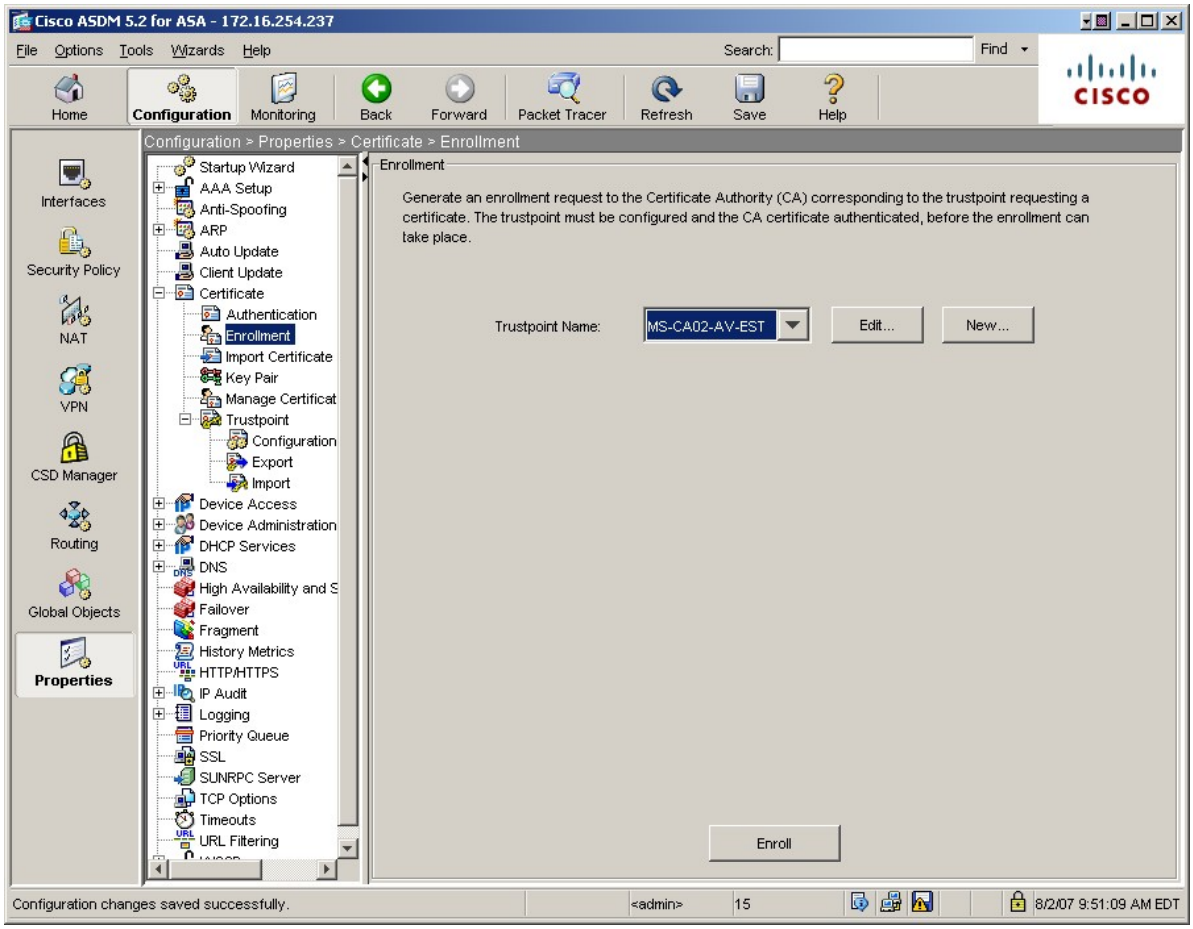


a. A dialogue box displays with status of the authentication request. Click the **OK** button.



©2007 Avaya Inc. All Rights Reserved.

7. Enroll with the Microsoft CA. From the navigation pane, click **Certificate > Enrollment**. Select the Trustpoint created in **Step 4** from the **Trustpoint Name** drop-down list. Click the **Enroll** button.

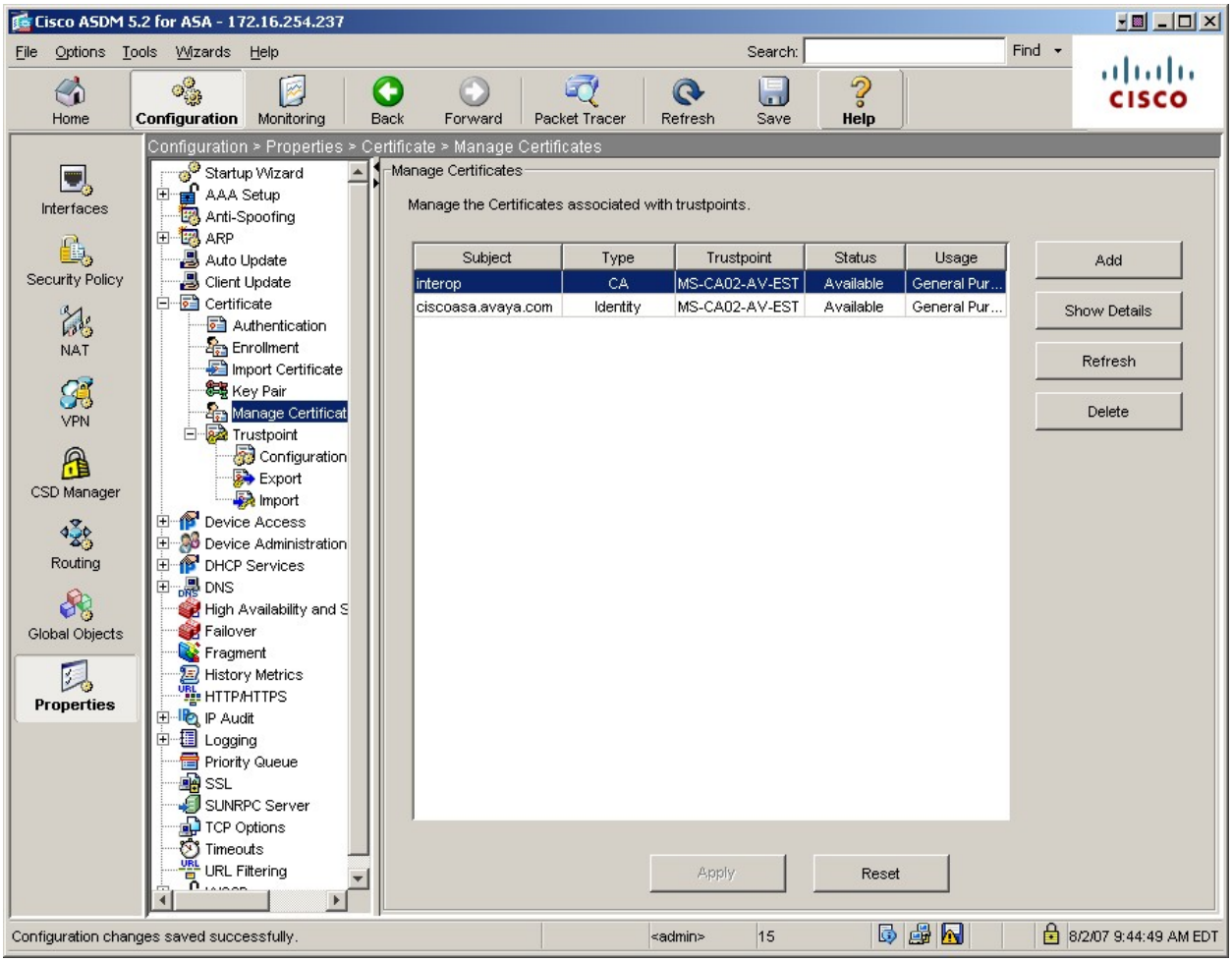


a. A dialogue box displays with status of the enroll request. Click the **OK** button.



©2007 Avaya Inc. All Rights Reserved.

8. The enrollment shown below to the Microsoft CA, named “interop” has a status of **Available**. This completes the steps required on the Cisco ASA for certificate import and enrollment with a Microsoft CA.

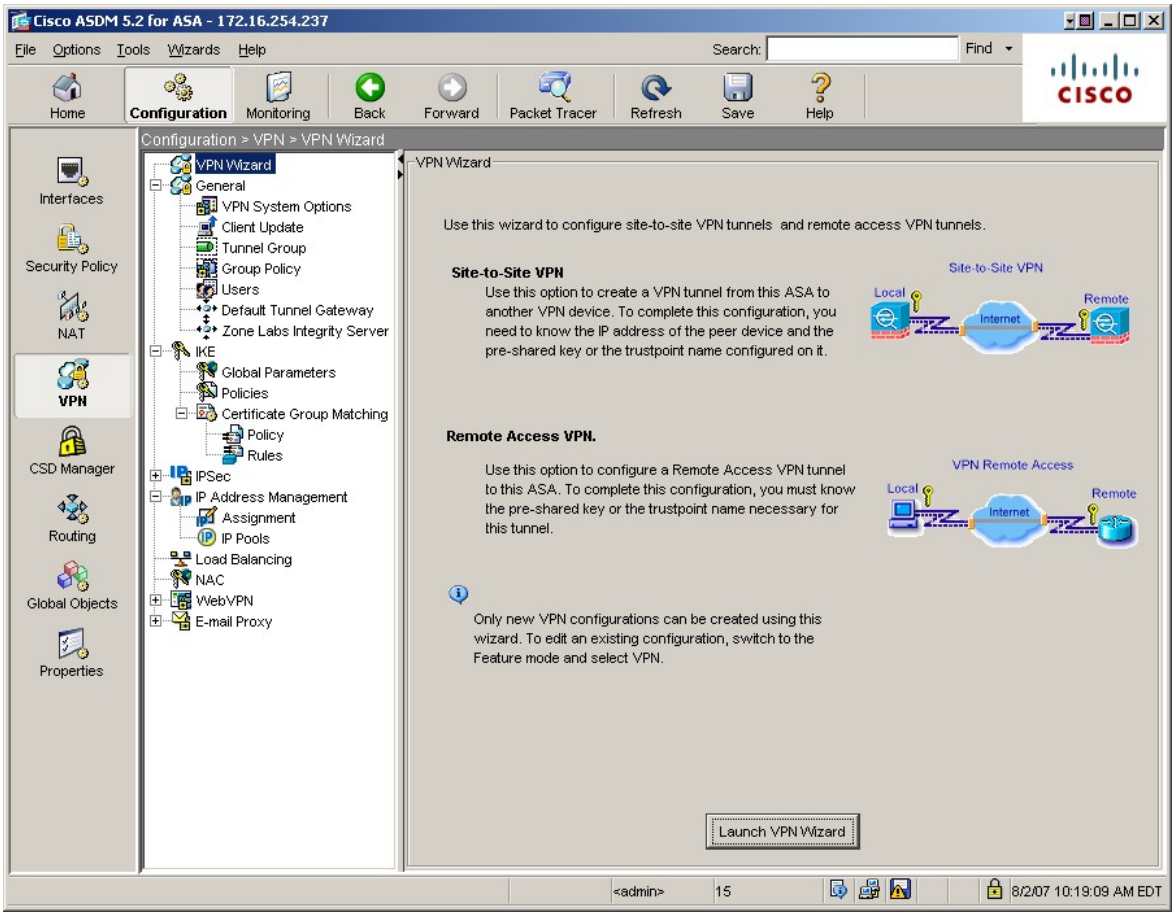


©2007 Avaya Inc. All Rights Reserved.

4.2. VPN Wizard

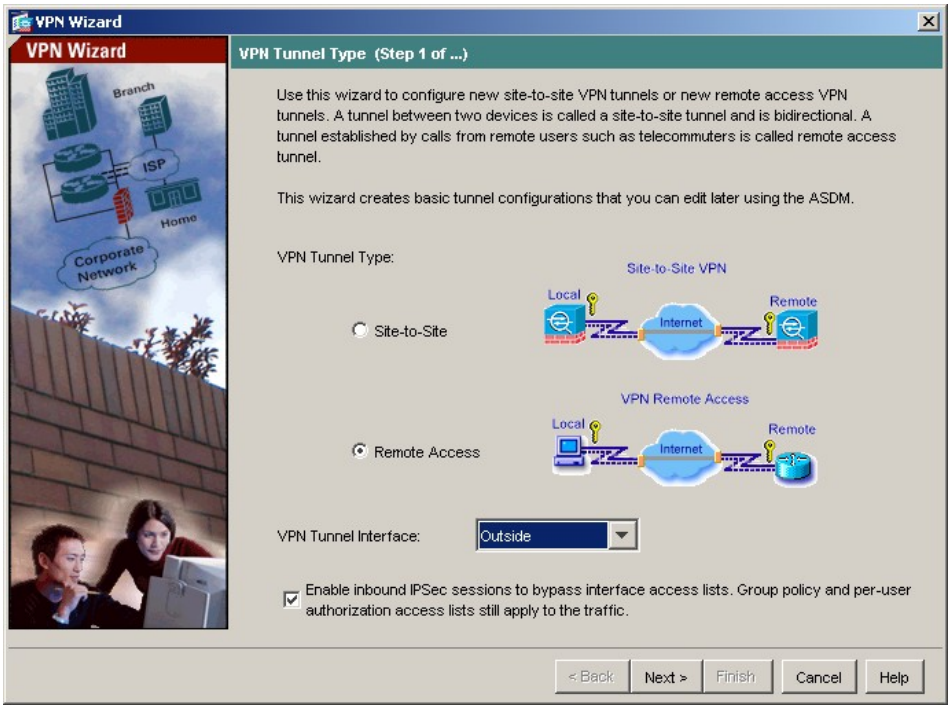
This section describes the steps to create the IPSec VPN and VPN user accounts using the ASDM VPN Wizard of the ASDM application. The user accounts are created in the user authentication database local to the Cisco ASA.

1. To start the VPN Wizard from the ASDM application:
    a. Click the **Configuration** button.
    b. From the left menu, click the **VPN** button.
    c. From the navigation pane, click **VPN Wizard**.
    d. Click the **Launch VPN Wizard** button.

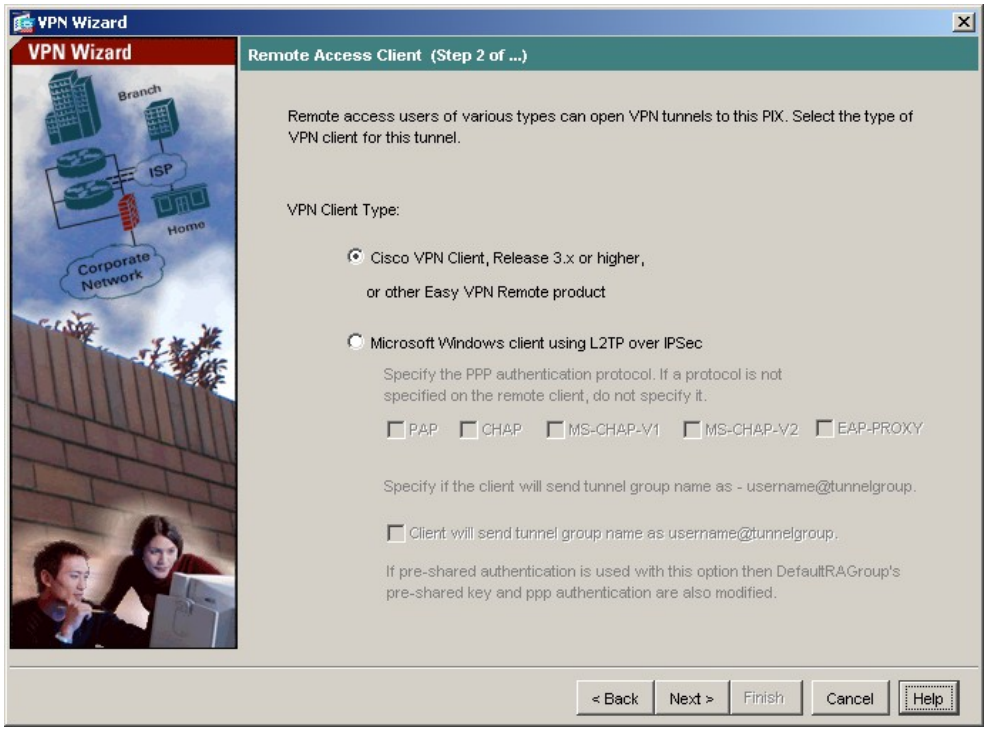


©2007 Avaya Inc. All Rights Reserved.

2. For the VPN Tunnel Type, select the **Remote Access** radio button. For the VPN Tunnel Interface, select **Outside** from the drop-down list. All remaining fields can be left at default values. Click **Next** to continue.

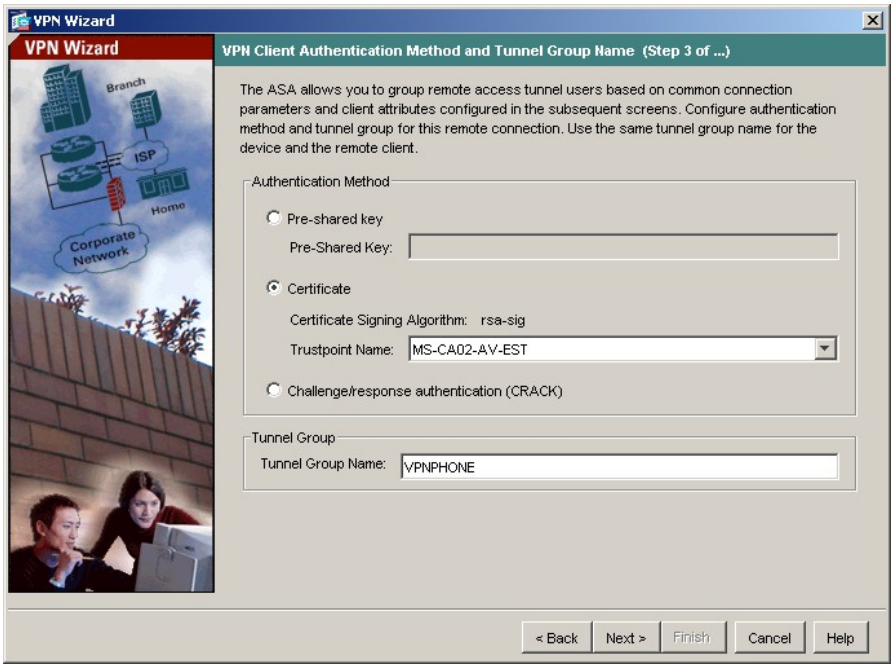


3. Maintain the default selection of **Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product**. Click **Next** to continue.

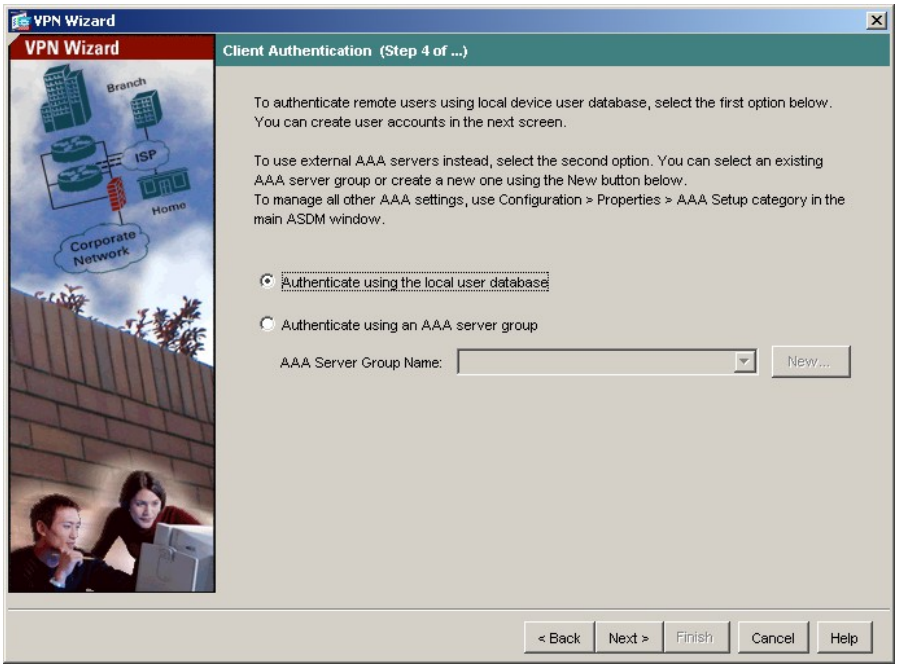


©2007 Avaya Inc. All Rights Reserved.

4. For the Authentication Method, select the **Certificate** radio button and the Trustpoint Name from the drop-down list created in **Step 4** of **Section 4.1**. For the Tunnel Group Name, any name can be entered. The Avaya VPNremote Phones default to the group name of **VPNPHONE**. Click **Next** to continue.

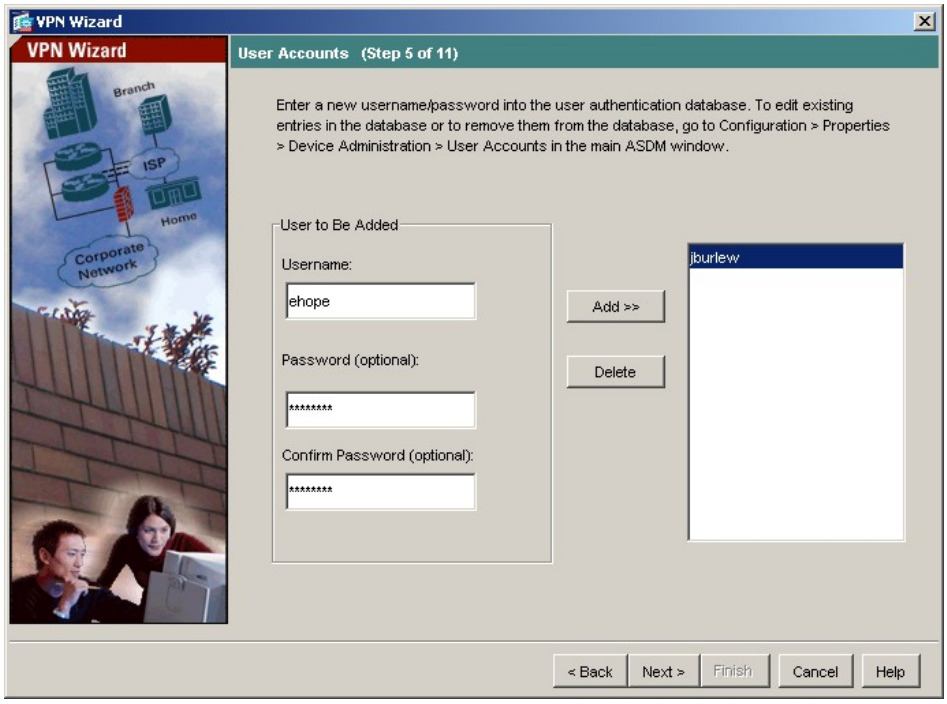


5. The internal ASA user authentication database is used in the sample configuration. However, an external authentication server can be used. Maintain the default **Authenticate using the local user database** and click **Next** to continue.

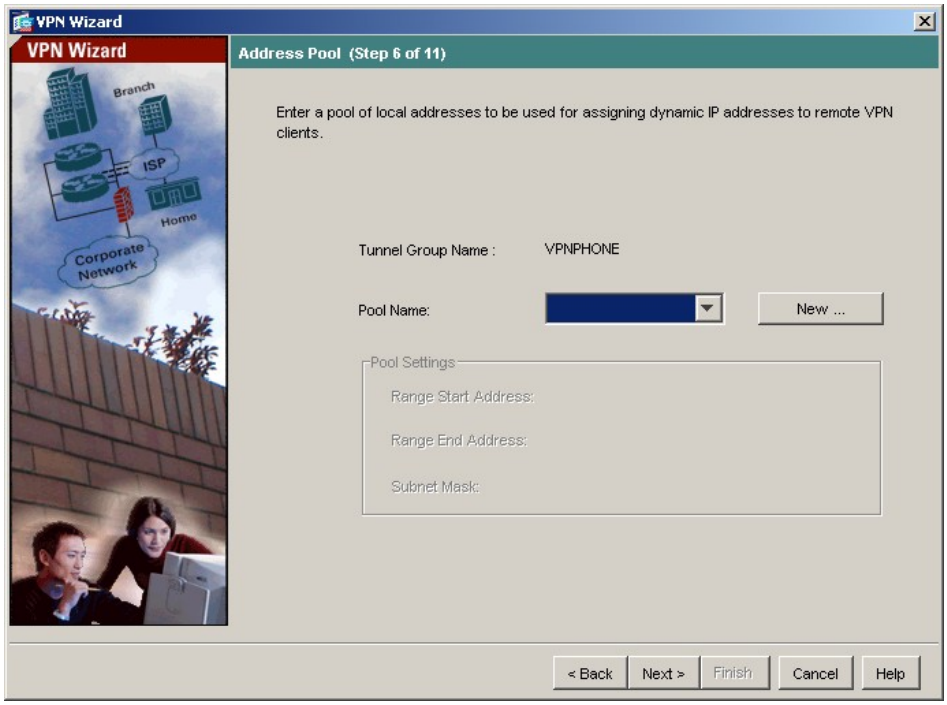


©2007 Avaya Inc. All Rights Reserved.

6. Enter the username and password of an Avaya VPNremote Phone user and click **Add**. Two user accounts, ehope and jburlew, are created in the sample configuration. When all Avaya VPNremote Phone user accounts have been entered, click **Next** to continue.

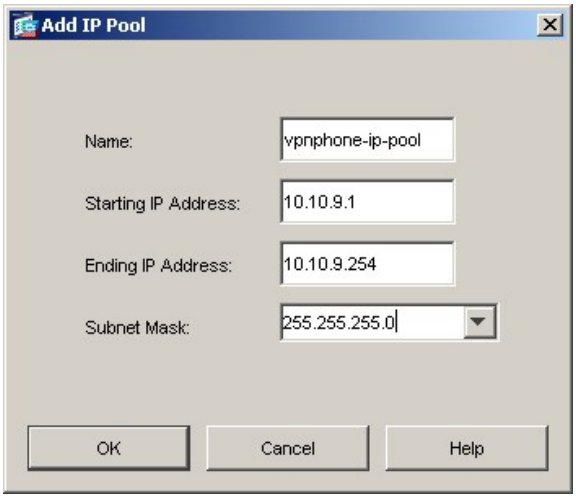


7. Click the **New** button to create a new IP address pool.

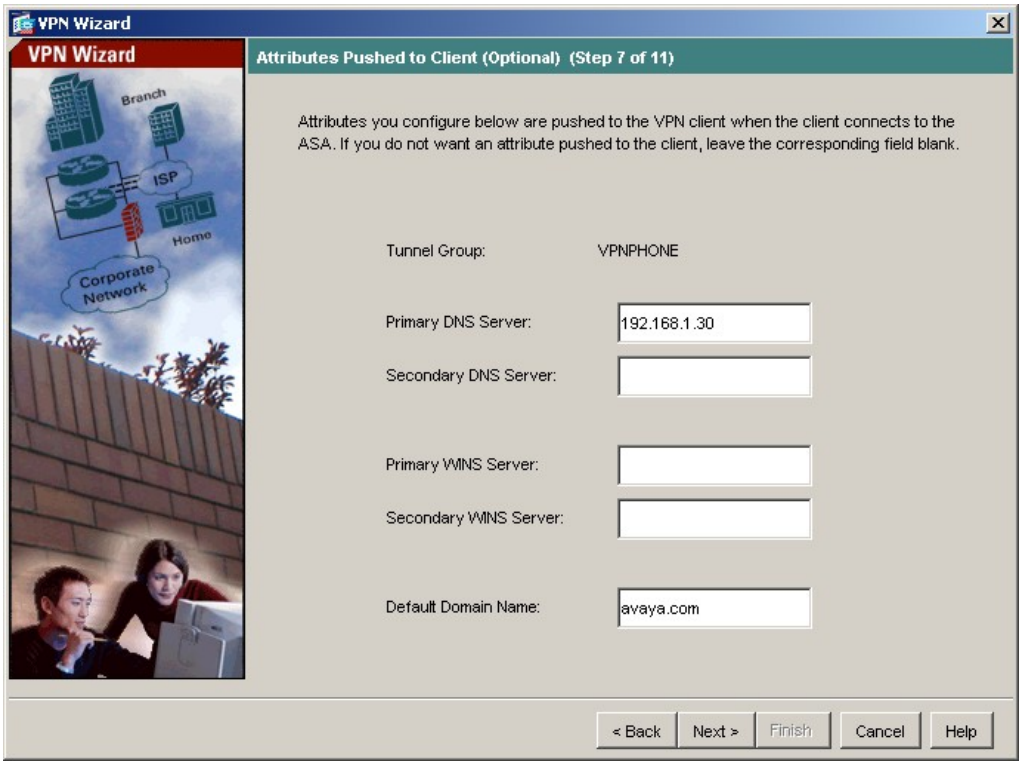


©2007 Avaya Inc. All Rights Reserved.

8. Enter a descriptive name and the IP address range to be assigned to Avaya VPNremote Phones as the “inner address”. This address range must not overlap with any addresses on the private enterprise network and must be routable within the enterprise network. Click **OK** and then click **Next** at the Address Pool window to continue.

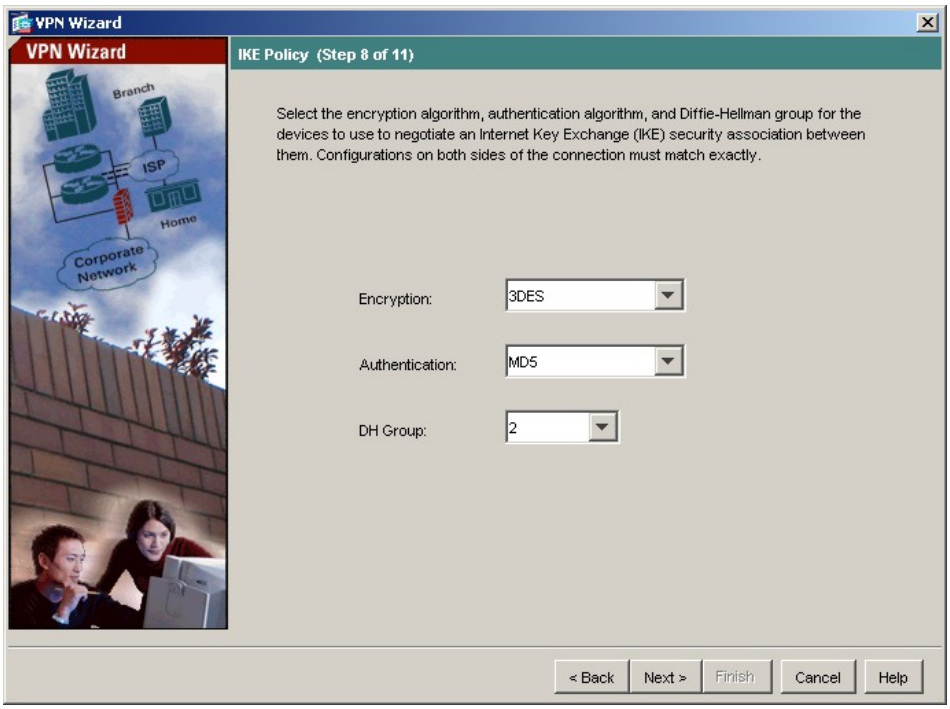


9. Enter the DNS, WINS and Domain information to be used by the Avaya VPNremote Phone while accessing enterprise network through the IPSec tunnel. Values entered below are specific to the sample network used for these Application Notes. Click **Next** when complete.

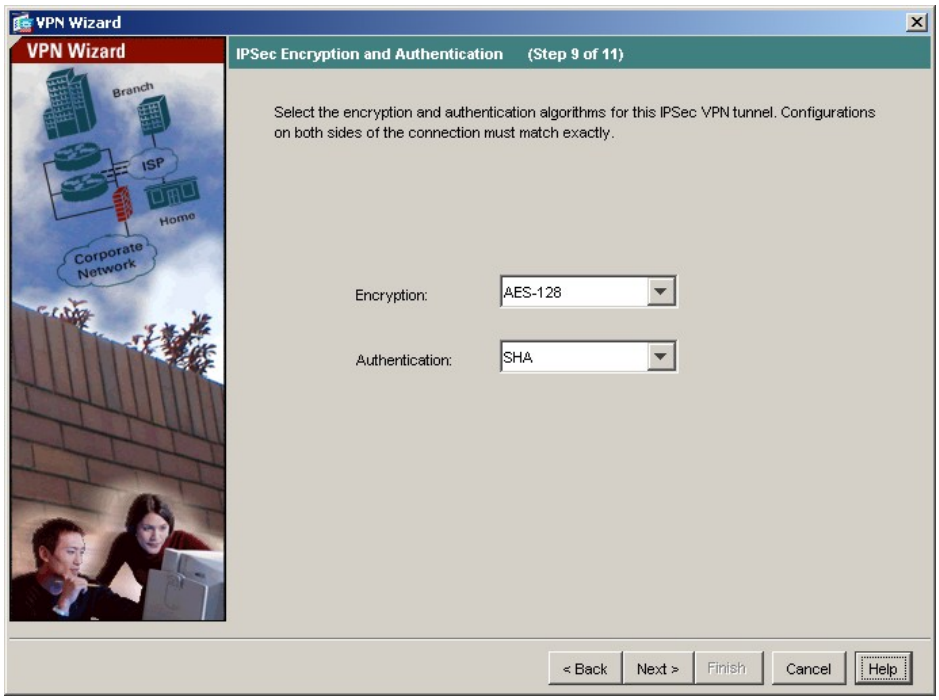


©2007 Avaya Inc. All Rights Reserved.

10. Select the IKE security association parameters from the drop-down lists. Click **Next** to continue.

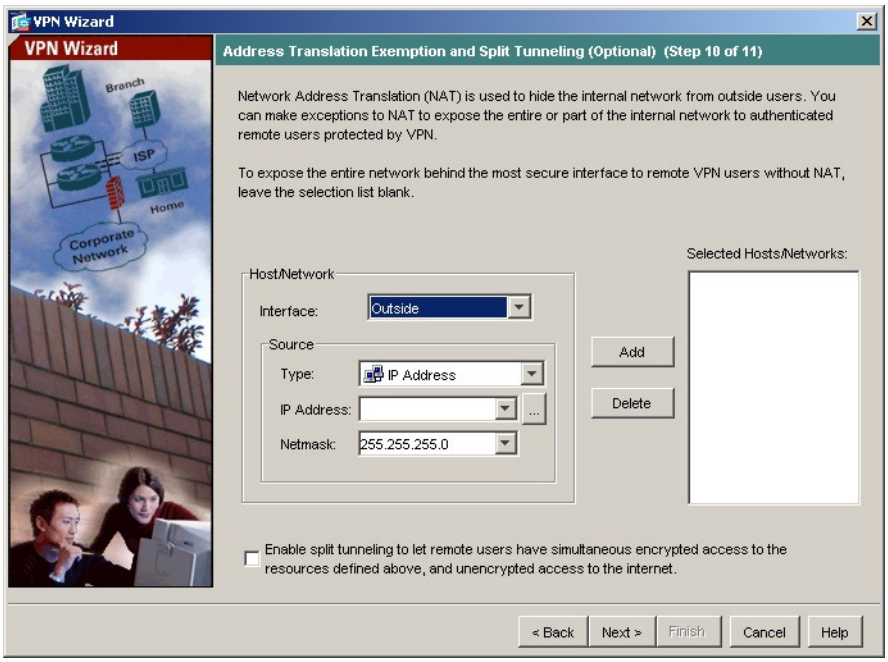


11. Select the appropriate IPSec VPN encryption and authentication parameters from the drop-down lists. Click **Next** to continue.

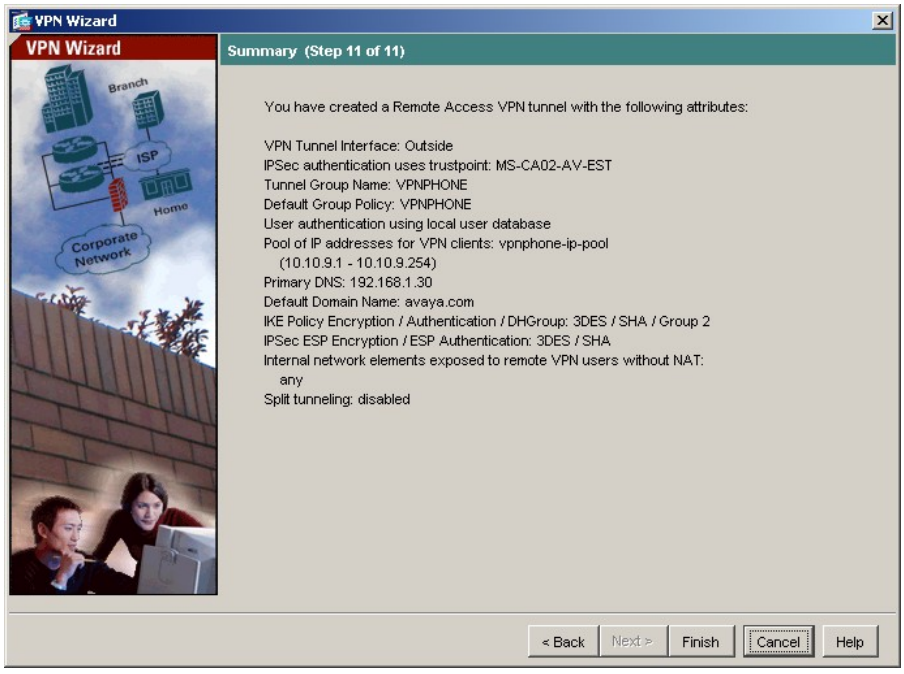


©2007 Avaya Inc. All Rights Reserved.

12. Maintain the default **Address Translation Exemption and Split Tunneling** options and click **Next** to continue.



13. Verify the VPN Tunnel options and click **Finish** to complete.



©2007 Avaya Inc. All Rights Reserved.

4.3. Certificate Group Matching

For an added layer of security when using certificate based authentication, the Certificate Group Matching feature of the Cisco ASA can be used with the Avaya VPNremote Phones. Certificate Group Matching allows a rule to be created to match an Avaya VPNremote Phone certificate based on fields of the certificate.

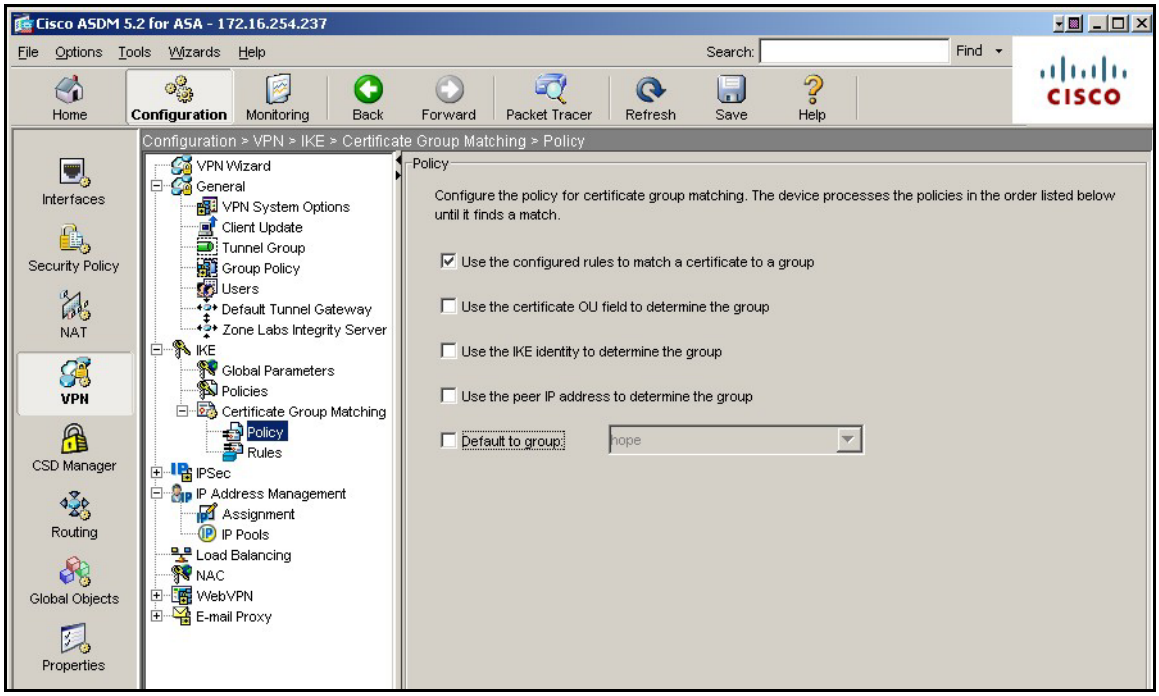
The rule created in the sample configuration requires the **Common Name** attribute of the certificate to contain a specified string value. The string value used is the first three octets of the MAC address of the Avaya 4600 Series IP Telephones, 00-04-0d. These first three octets of a MAC address are designated as the Organizationally Unique Identifier (OUI) and common across all 4600 Series IP Telephones. This rule verifies that the device the certificate is associated with is an Avaya Telephone.

To populate the Common Name attribute of the certificate with the MAC address of the Avaya VPNremote Phone, the variable "`MYCERTCN`" must be set to "`$MACADDR`" in the 46vpnsetting.txt file. See **Section 6.2** for additional information on this variable and the 46vpnsetting.txt file.

The following steps describe how to create a Certificate Group Match Policy and Rule.

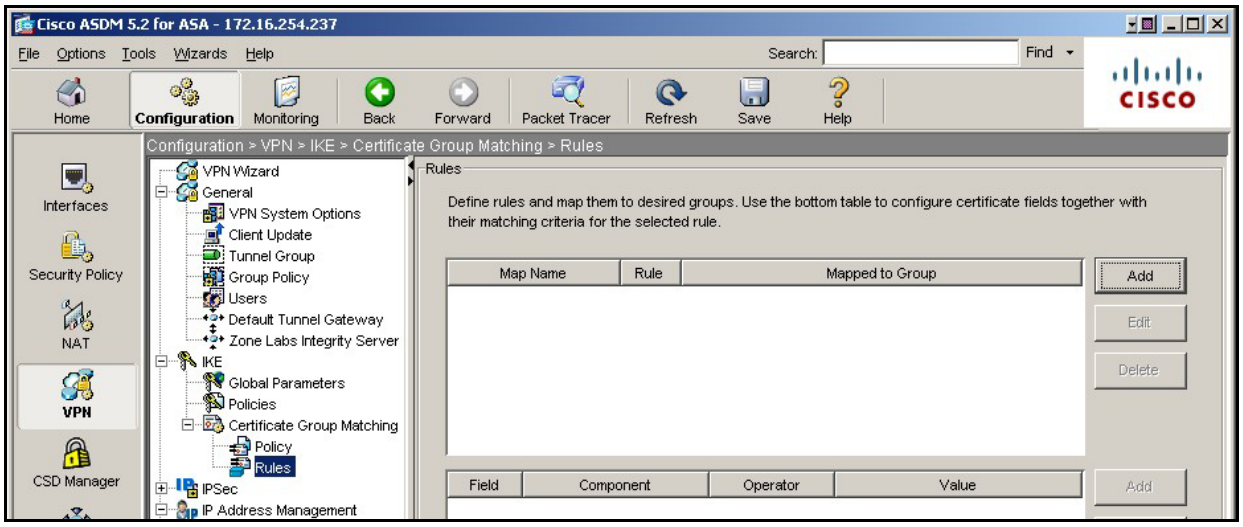
1. To create a certificate Group Match Policy:

    a. Click the **Configuration** button.
    b. From the left menu, click the **VPN** button.
    c. From the navigation pane, click **IKE > Certificate Group Matching > Policy**
    d. Check the **Use the configured rule to match a certificate to a group** check box
    e. Click the **Apply** button.

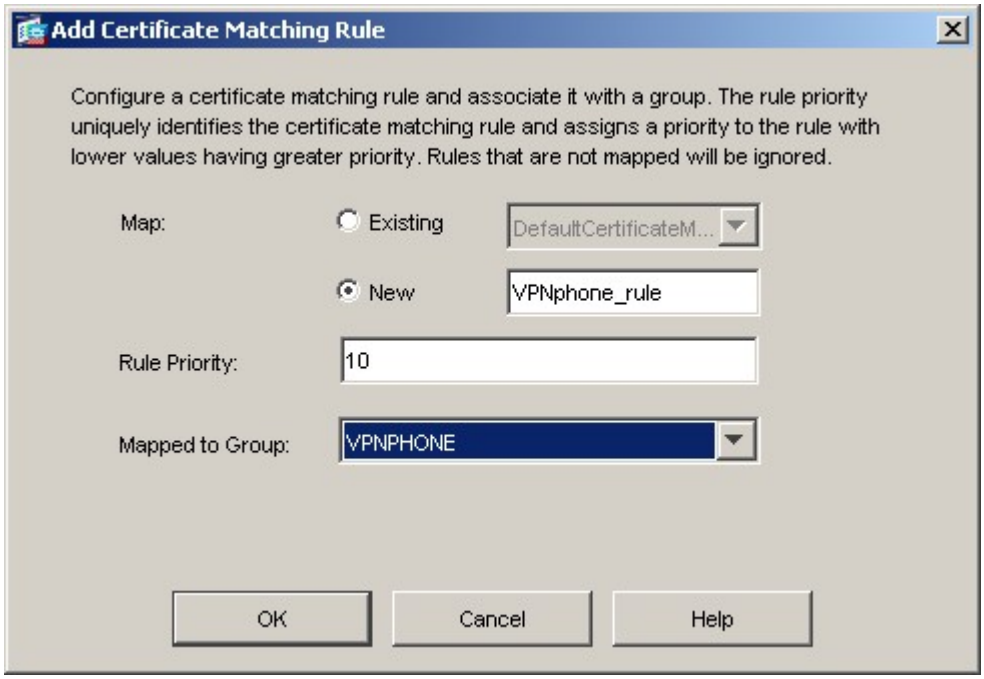


©2007 Avaya Inc. All Rights Reserved.

2. To create the Rule, click **Certificate Group Matching > Rules**. Click the **Add** button.

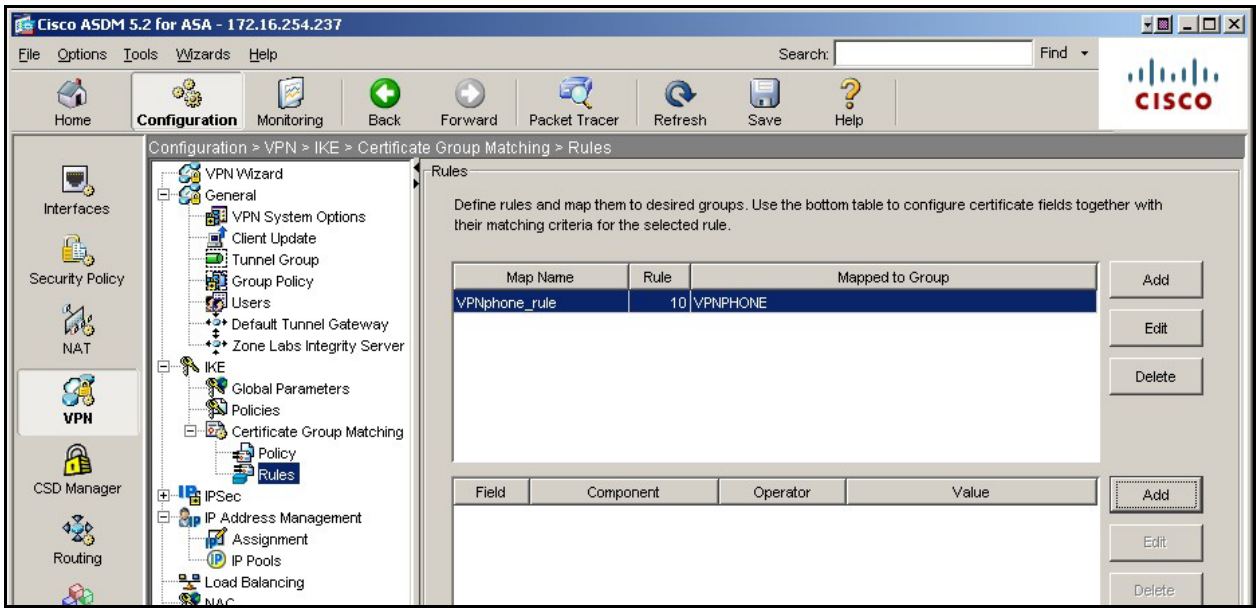


3. Select the **New** radio button and enter a descriptive name for this rule. Select the appropriate **Rule Priority**, 10 is the default. From the **Mapped to Group** drop-down list, select the Tunnel Group name created in **Step 4** of **Section 4.2**. Click the **OK** button to continue.

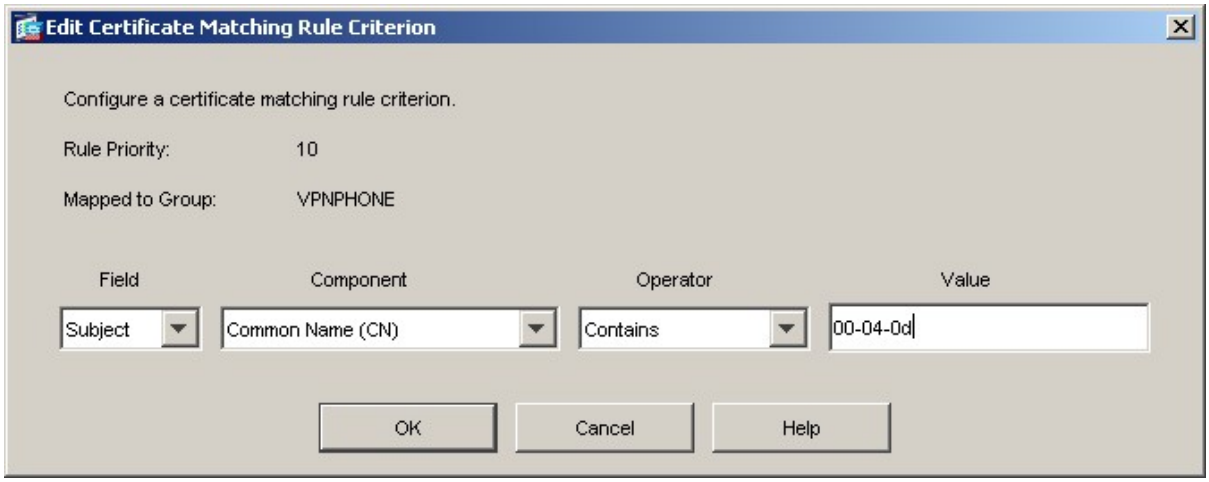


©2007 Avaya Inc. All Rights Reserved.

4. Click the bottom **Add** button to create the matching criteria for the rule.



5. Select the values shown below from the available drop-down lists. Enter the OUI of 00-04-0d for the Avaya 4600 Series IP Telephones in the **Value** field.

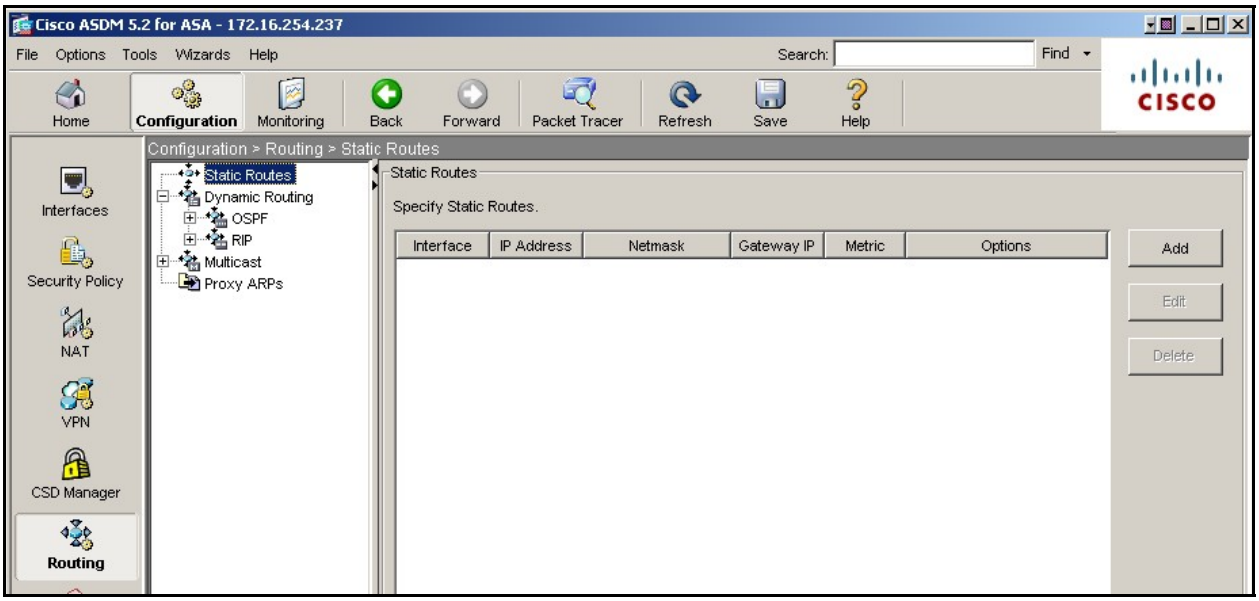


©2007 Avaya Inc. All Rights Reserved.

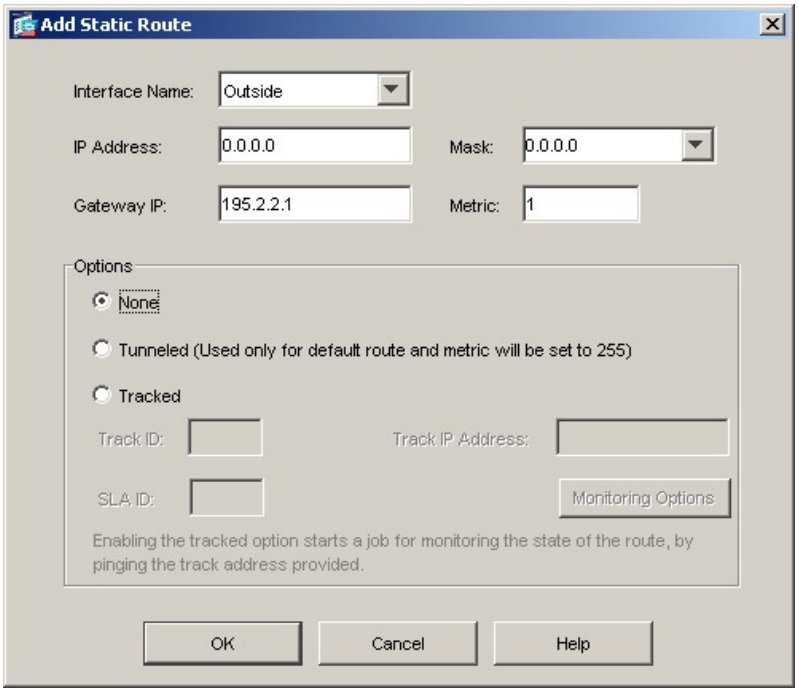
4.4. Default Route

The default route must be set on the Cisco ASA. The default route was set to the outside (public) interface for the sample configuration.

1. Navigate to **Configuration > Routing > Static Routes** and click the **Add** button.



2. The IP Address of 0.0.0.0 with a Mask of 0.0.0.0 signifies the default route. The IP address of 195.2.2.1 is the ISP next hop router as shown in **Figure 1**. Click the **OK** button.

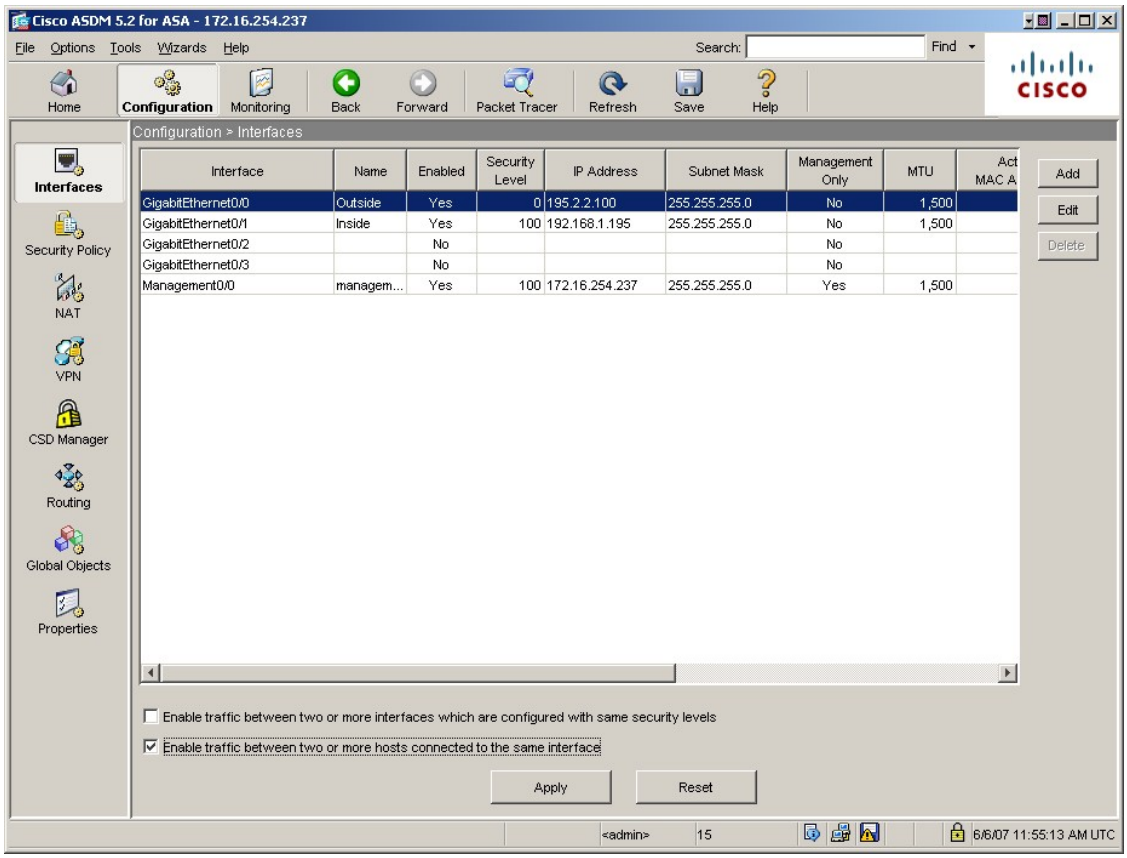


©2007 Avaya Inc. All Rights Reserved.

4.5. Avaya VPNremote Phone to Avaya VPNremote Phone Direct Audio

The path taken by the RTP audio packets of an Avaya VPNremote Phone can be controlled in the same way as a traditional Avaya IP Telephone using the IP-IP Direct Audio features of Avaya Communication Manager. If it is desirable for the RTP audio packets to go directly between two Avaya VPNremote Phones with VPN tunnels to the same Cisco ASA, the **Enable traffic between two or more hosts connected to the same interface** Cisco ASA configuration option must be enabled. This is in addition to configuring the proper IP-IP Direct Audio options on Avaya Communication Manager.

Navigate to **Configuration > Interfaces** and select the check box towards the bottom of the screen next to **Enable traffic between two or more hosts connected to the same interface**. Click the **Apply** button to save.



5. Avaya VPNremote Phone Configuration

The Avaya VPNremote Phone must download the digital certificate and enroll with the Microsoft CA prior to the phone being used remotely. This section describes the variables of the 46vpnsetting.txt configuration file specific to digital certificates and the steps to download the certificate to the Avaya VPNremote Phone.

©2007 Avaya Inc. All Rights Reserved.

This section assume the Avaya VPNremote Phone firmware has already been loaded on the phone. See **Section 8** for addition documentation on installed the Avaya VPNremote Phone firmware.

5.1. 46vpnsettings.txt File

The 46vpnsetting.txt file contains VPN specific variables for the Avaya VPNremote Phone to use during the setup of the IPSec VPN tunnel. The full 46vpnsettings.txt file used in the sample configuration is shown in **Appendix B**. The variables specific to digital certificate authentication and the Cisco ASA are listed below. Descriptions of each variable and the values used in the sample configuration are shown.

46vpnsetting.txt: Certificate Related Variables used in the Sample Configuration:

```
## Variable Name : TRUSTCERTS
## Valid Values
##     Name of a file containing CA certificate
##     in PEM format. Length of the file name
##     cannot be more than 16 characters.
## Description
##     Use this variable to import CA
##     certificates. The certificate presented
##     by peer is validated against the list of
##     CAs imported through this command. Maximum
##     number of CAs that can be imported is limited
##     to 5.
## Example
##    SET TRUSTCERTS CA1.CER,CA2.CER,CA3.CER
##
SET TRUSTCERTS 46vpn_cert.cer


## Variable Name : MYCERTURL
## Valid Values
##     URL for enrolling with a SCEP fronted Certificate Authority.
##
## Description
##     If this information is supplied, phone generates a RSA key pair
##     and sends the enrollment request using SCEP protocol to the
##     server pointed by this URL. Consult your CA administrator guide
##     for further information regarding SCEP support.
##
SET MYCERTURL http://192.168.1.30/certsrv/mscep/mscep.dll


## Variable Name : MYCERTCN
## Valid values
##     $MACADDR
##     $SERIALNO
##
## Description
##     If value of this variable is set to $MACADDR, phone uses it's
##        MAC Address as the CN component of the certificate request
##     If value of this variable is set to $SERIALNO, phone uses it's
##        Serial Number as the CN component of the certificate request.
##
SET MYCERTCN $MACADDR
```


©2007 Avaya Inc. All Rights Reserved.

```
## Variable Name : SCEPPASSWORDREQ
## Valid values
##      0
##      1
## Description
##      If value of this variable is set to 1, phone user is prompted to
##        enter challenge pass phrase during SCEP certificate enrollment.
##      If value of this variable is set to 0, phone uses the challenge
##        pass phrase as indicated by SCEPPASSWORD variable.
##
## Note
##      Consult your Certificate Authority administrator guide for HOWTO
##      configure pass phrase for SCEP certificate enrollment.
##
SET SCEPPASSWORDREQ 0


## Variable Name : SCEPPASSWORD
## Valid values
##      String
## Description
##      The string specified here is used by phone as the SCEP challenge pass
##      phrase for SCEP certificate enrollment. If left unspecified and
##      SCEPPASSWORDREQ is SET to 0, phone uses it's SERIAL number as the challenge
##      pass phrase.
## Note
##      Consult your Certificate Authority administrator guide for HOWTO
##      configure pass phrase for SCEP certificate enrollment.
##
SET SCEPPASSWORD "E676148554572C61"
```

46vpnsetting.txt: Cisco ASA with Certificates Related Variables used in the Sample Configuration:

```
## Variable Name : NVVPNCFGPROF
## Valid Values
##    1  Avaya Security Gateway
##    2  Checkpoint
##    3  Cisco Xauth with Preshared Key
##    5  Juniper/Netscreen Xauth with Preshared Key
##    6  Generic Preshared key
##    8  Cisco xauth with certificates
##    9  Juniper Xauth with certificates.
##    11 Nortel contivity
##
SET NVVPNCFGPROF 8


## Variable Name : NVIKEIDTYPE
## Valid Values
##    1    IP Address
##    2    FQDN
##    3    User-FQDN (E-Mail)
##    9    Directory-Name
##    11    KEY-ID (Opaque)
## Description
##    Phone uses this variable as the IKE Identifier type for the
##    IKE-ID specified via NVIKEID variable.
##
SET NVIKEIDTYPE   11
```


©2007 Avaya Inc. All Rights Reserved.

```
## Variable Name : NVIKEXCHMODE
## Valid Values
##    1    Aggressive
##    2    Identity protect
## Description
##    Aggressive – In Aggressive mode, there is no identity protection
##    for the negotiating nodes, because both nodes must transmit their
##    identities before establishing a negotiated secure channel.
##
##    Identity protect – In Identity protect mode, the exchange of ID
##    information occurs in the fifth and sixth messages exchanged during
##    Phase 1 negotiations, after a secure channel has been established
##    by the first four messages.
##
SET NVIKEXCHGMODE 2
```

5.2. Downloading the Digital Certificate

1. Generate a new Challenge Password, as described in **Section 3.1,** and enter the new password for the **SCEPPASSWORD** variable of the 46vpnsetting.txt file.
2. Connect the Avaya VPNremote Phone to the enterprise network.
3. Set the VPN Start Mode to DISABLED. This allows the phone to boot up as a "regular" IP phone.
4. Using HTTP or TFTP, the phone will download the following files: 46vpnupgrade.scr, 46vpnsetting.txt and the certificate file defined by the SET TRUSTCERTS variable of the 46vpnsetting.txt file (46vpn_cert.cer in the sample configuration). The download activity of these files is shown on the phones display.
5. Once the certificate is downloaded, the phone will enroll with the Microsoft CA. The phone will display status messages similar to the following during the download and enrollment process:

Screen 1:	**SCEP Download CA Cert…**
Screen 2:	**Generating Keys, Please Wait** **URL: http://192.168.1.30/certsrv/scep/mscep.dll**
Screen 3:	**Sending Enrollment Request**

Note: The phone obtains the Challenge Password to use during enrollment with the Microsoft CA from the SCEPPASSWORD variable of the 46vpnsetting.txt file. This variable must be set for each new enrollment with a new password, as described in

©2007 Avaya Inc. All Rights Reserved.

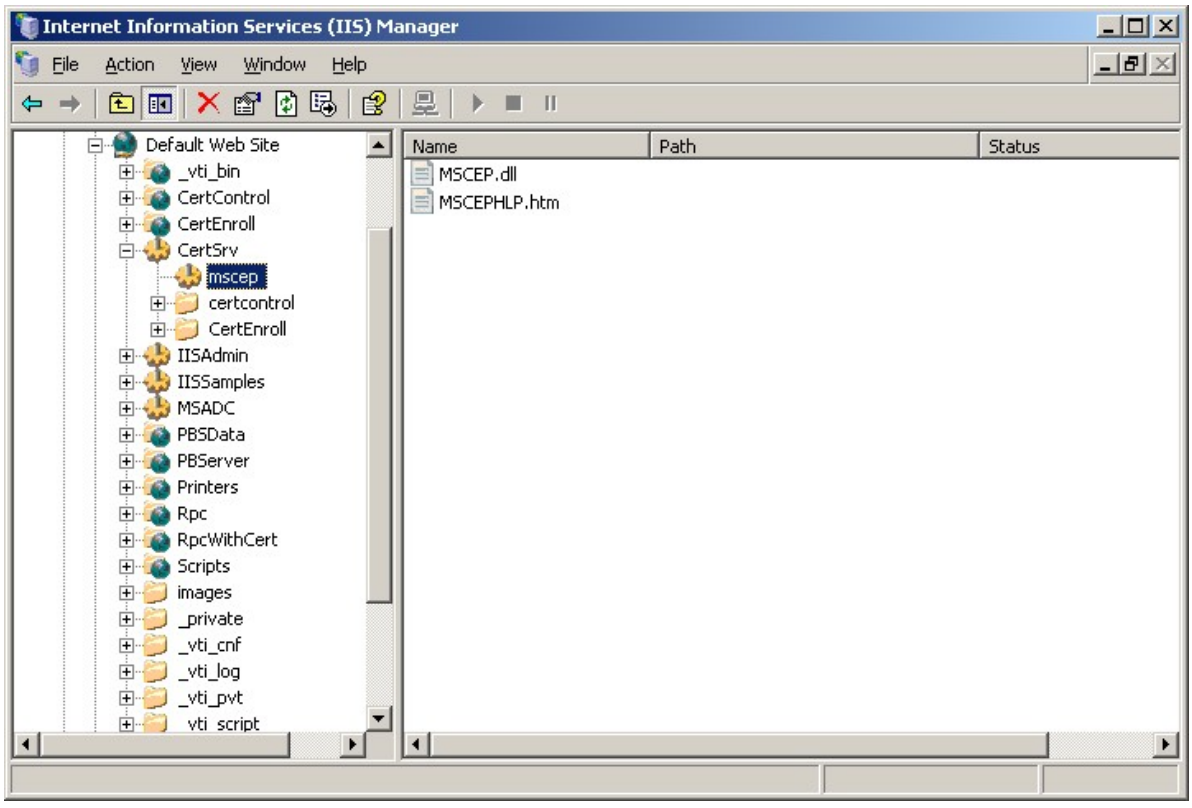
Section 3.1, and must be used within one hour of being generated. The phone will display the following error if there is a problem with the Challenge Password.

SCEP Failure 104:587

6. Verification

6.1. Verify the Installation of the Microsoft SCEP add-on

1. On the Microsoft Windows 2003 Server navigate to the IIS Manager by going to **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**. From the navigation pane click **Default Web Site > CertSrv**. The SCEP add-on is installed if **mscep** is installed under **CertSrv**.

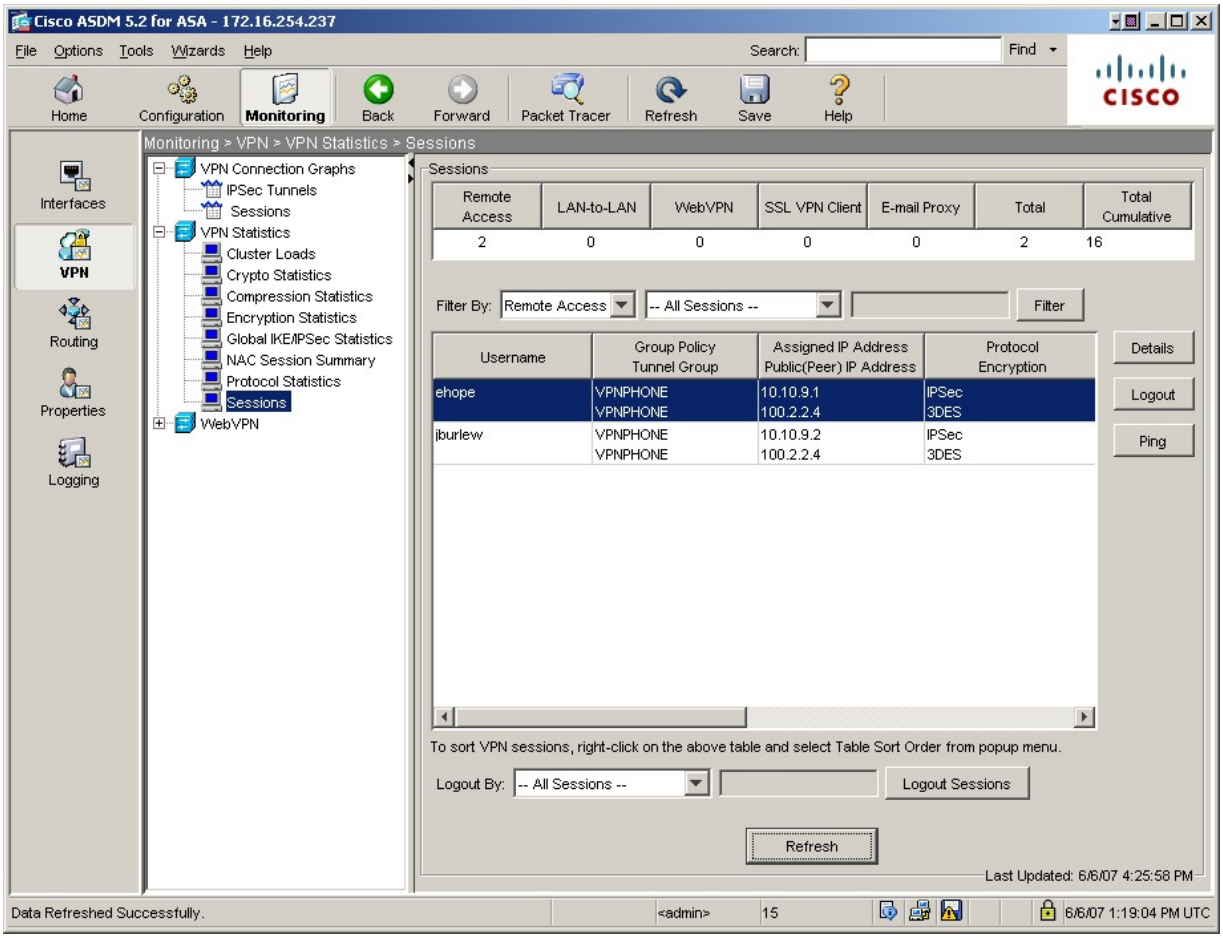


©2007 Avaya Inc. All Rights Reserved.

6.2. ASA Active VPN Sessions

6.2.1. VPN Session Statistics

The active VPN sessions to the Cisco ASA can be viewed by selecting **Monitoring > VPN > VPN Statistics > Sessions**. The screen shot below shows sessions of two Avaya VPNremote Phones with active tunnels to the Cisco ASA.



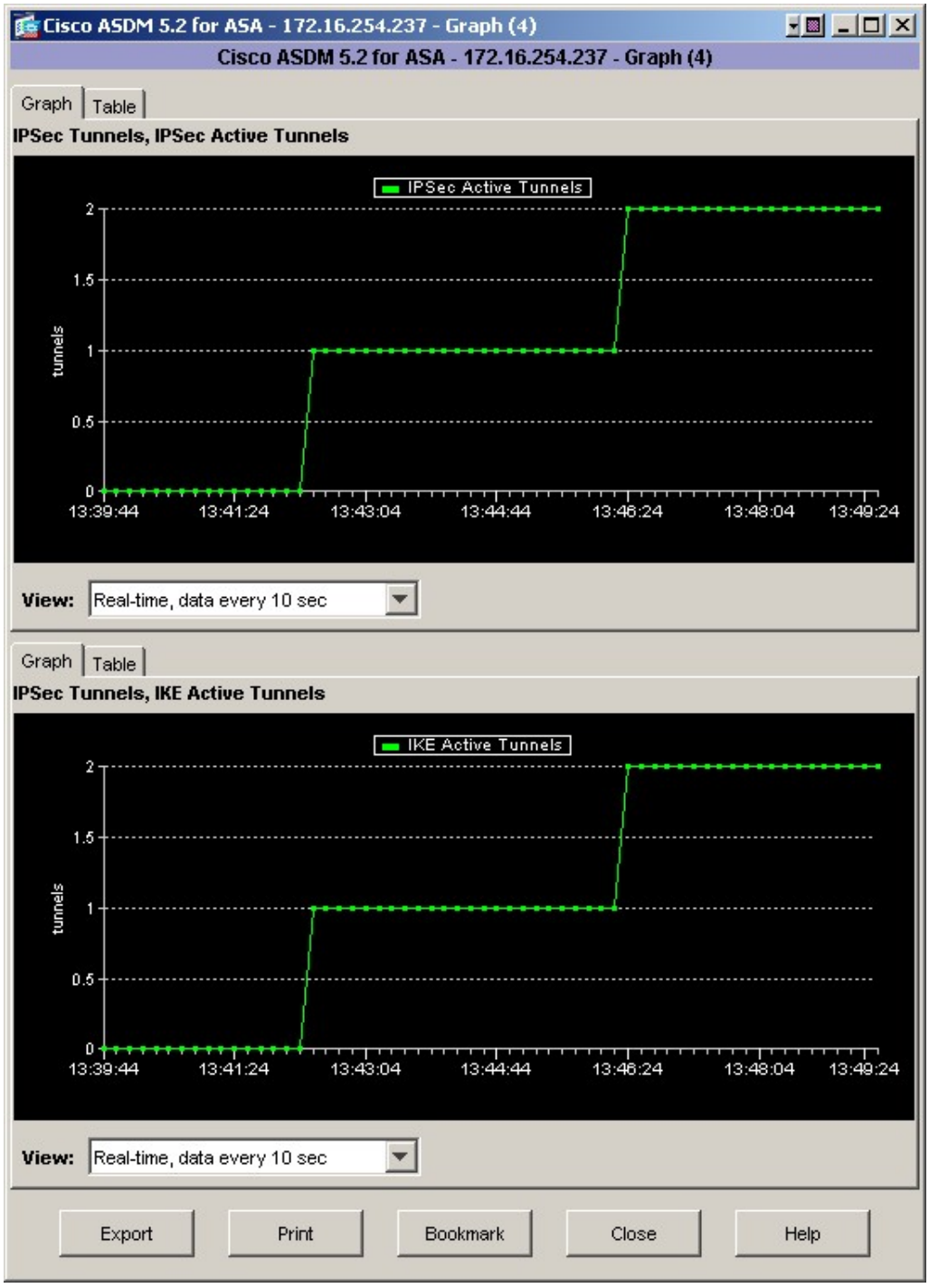
The Cisco ASDM Home page also provides some basic VPN Tunnel statistics as shown below.



©2007 Avaya Inc. All Rights Reserved.

6.2.2. VPN Session Graph

The active VPN sessions to the Cisco ASA can be shown in a graph by selecting **Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels**. Add **IPSec Active Tunnels** and **IKE Active Tunnels** to the Selected Graphs list and click the **Show Graphs** button to display the graph. The screen shot below shows the IPSec and IKE sessions of two Avaya VPNremote Phones with active tunnels to the Cisco ASA.



©2007 Avaya Inc. All Rights Reserved.

7. Conclusion

Customers using a Public Key Infrastructure can now take advantage of the digital certificate authentication feature of the Avaya VPNremote Phone. This feature offers customers an alternative to using the pre-shared key method of authentication. These Application Notes demonstrate the interoperability of the Avaya VPNremote Phone with the Cisco Adaptive Security Appliance and the Microsoft Certificate Authority using digital certificate authentication.

8. Additional References

Avaya Application Notes and additional resources can be found at the following web address http://www.avaya.com/gcm/master-usa/en-us/resource/. Avaya Product Support web site can be found at the following web address http://support.avaya.com/.

[1] **VPNremote for 46xx Series IP Telephone Installation and Deployment Guide,** Doc ID: 1022006

[2] **Configuring Cisco Adaptive Security Appliance (ASA) using Cisco Adaptive Security Device Manager (ASDM) VPN Wizard to Support Avaya VPNremote Phones – Issue 1.0,** Avaya Application Note

[3] **Application Notes for Converting an Avaya 4600 Series IP Telephone to an Avaya VPNremote Phone – Issue 1.0,** Avaya Application Note

[4] **Cisco ASA Security Appliance Command Reference, Version 7.2**

[5] **Public Key Infrastructure for Microsoft Windows Server 2003** http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx#EEF

[6] **Download Simple Certificate Enrollment Protocol (SCEP) Add-on for Microsoft Certificate Services** http://www.microsoft.com/downloads/details.aspx?familyid=9f306763-d036-41d8-8860-1636411b2d01&displaylang=en

[7] **Cisco Systems' Simple Certificate Enrollment Protocol (SCEP):** http://www.ietf.org/internet-drafts/draft-nourse-scep-15.txt

©2007 Avaya Inc. All Rights Reserved.

Appendix A: Cisco ASA Command Line Configuration

The command line configuration of the Cisco ASA used in the sample configuration is provided below.

```
ASA Version 7.2(2)
!
hostname ciscoasa
domain-name avaya.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface GigabitEthernet0/0
 description Public ISP connection
 nameif Outside
 security-level 0
 ip address 195.2.2.100 255.255.255.0
!
interface GigabitEthernet0/1
 description Corporate Network connection
 nameif Inside
 security-level 100
 ip address 192.168.1.195 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 172.16.254.237 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa722-k8.bin
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns server-group DefaultDNS
 domain-name avaya.com
same-security-traffic permit intra-interface
access-list Inside_nat0_outbound extended permit ip any 10.10.9.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu Outside 1500
mtu Inside 1500
mtu management 1500
ip local pool vpnphone-ip-pool 10.10.9.1-10.10.9.254 mask 255.255.255.0
no failover
```


©2007 Avaya Inc. All Rights Reserved.

```
monitor-interface Outside
monitor-interface Inside
monitor-interface management
icmp unreachable rate-limit 1 burst-size 1
icmp permit any Outside
icmp permit any management
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
nat (Inside) 0 access-list Inside_nat0_outbound
route Outside 0.0.0.0 0.0.0.0 195.2.2.1 1
route Inside 10.10.8.0 255.255.255.0 192.168.1.197 1
route management 135.0.0.0 255.0.0.0 172.16.254.4 1
route management 148.147.0.0 255.255.0.0 172.16.254.4 1
route management 198.152.0.0 255.255.0.0 172.16.254.4 1
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 uauth 0:05:00 absolute
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 3
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 msie-proxy server none
 msie-proxy method no-modify
 msie-proxy except-list none
 msie-proxy local-bypass disable
 nac disable
 nac-sq-period 300
 nac-reval-period 36000
 nac-default-acl none
 address-pools none
 client-firewall none
 client-access-rule none
 webvpn
```


©2007 Avaya Inc. All Rights Reserved.

```
  functions url-entry
  html-content-filter none
  homepage none
  keep-alive-ignore 4
  http-comp gzip
  filter none
  url-list none
  customization value DfltCustomization
  port-forward none
  port-forward-name value Application Access
  sso-server none
  deny-message value Login was successful, but because certain criteria have not been
met or due to some specific group policy, you do not have permission to use any of the
VPN features. Contact your IT administrator for more information
  svc none
  svc keep-installer installed
  svc keepalive none
  svc rekey time none
  svc rekey method none
  svc dpd-interval client none
  svc dpd-interval gateway none
  svc compression deflate
group-policy VPNPHONE internal
group-policy VPNPHONE attributes
 dns-server value 192.168.1.30
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-tunnel-protocol IPSec
 default-domain value avaya.com
username jburlew password skd9B6PomUq9nD/D encrypted
username jburlew attributes
 vpn-group-policy VPNPHONE
username ehope password 0SvLxMEfKe7LGJKH encrypted
username ehope attributes
 vpn-group-policy VPNPHONE
http server enable
http 192.168.1.0 255.255.255.0 management
http 172.16.254.0 255.255.255.0 management
http 135.0.0.0 255.0.0.0 management
http 148.147.0.0 255.255.0.0 management
http 198.152.0.0 255.255.0.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 40 set pfs
crypto dynamic-map Outside_dyn_map 40 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 60 set pfs
crypto dynamic-map Outside_dyn_map 60 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 80 set pfs
crypto dynamic-map Outside_dyn_map 80 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 100 set pfs
crypto dynamic-map Outside_dyn_map 100 set transform-set ESP-3DES-SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map
crypto map Outside_map interface Outside
crypto ca trustpoint MS-CA02-AV-EST
 enrollment url http://192.168.1.30:80/certsrv/mscep/mscep.dll
 password *
```


©2007 Avaya Inc. All Rights Reserved.

```
 keypair keypair01
 crl configure
  no protocol http
  no protocol ldap
crypto ca certificate map VPNphone_rule 10
 subject-name attr cn co 00-04-0d
crypto ca certificate chain MS-CA02-AV-EST
 certificate 18e46bac000100000019
    308204d1 3082043a a0030201 02020a18 e46bac00 01000000 19300d06 092a8648
    86f70d01 01050500 301f310b 30090603 55040613 02555331 10300e06 03550403
    1307696e 7465726f 70301e17 0d303730 38303231 33333534 375a170d 30393036
    31383139 30303332 5a302331 21301f06 092a8648 86f70d01 09021312 63697363
    6f617361 2e617661 79612e63 6f6d3081 9f300d06 092a8648 86f70d01 01010500
    03818d00 30818902 818100b4 f7298739 b5e5a46c 94011c9d f1c1bb8f ce839918
    0a18a8e0 1d732197 b10dab76 8e4168f6 e0733a0e 531fbf3f 540deb19 a40e383f
    7ca5eaeb 481c39d9 b82fcef5 f6447a71 30743312 8baf9157 46843845 f57bda4f
    c69b5dec e8efcc5d 7f3c736d 8c0d0eb1 6668fce4 3838cde7 cad8ea97 5d57fa3c
    d0f55705 78aeb82f 93b7a102 03010001 a382030e 3082030a 300b0603 551d0f04
    04030205 a0301d06 03551d11 04163014 82126369 73636f61 73612e61 76617961
    2e636f6d 301d0603 551d0e04 16041485 37d6a77e 26e09236 5ed256d4 f625e921
    2fdd6830 1f060355 1d230418 30168014 e872da8a 3834f0cc 1b111243 e21b9b30
    be5bcc24 30820111 0603551d 1f048201 08308201 04308201 00a081fd a081fa86
    81b96c64 61703a2f 2f2f434e 3d696e74 65726f70 2831292c 434e3d61 76617961
    2d697977 64353037 6a6b2c43 4e3d4344 502c434e 3d507562 6c696325 32304b65
    79253230 53657276 69636573 2c434e3d 53657276 69636573 2c434e3d 436f6e66
    69677572 6174696f 6e2c4443 3d696e74 65726f70 2c44433d 6c61623f 63657274
    69666963 61746552 65766f63 6174696f 6e4c6973 743f6261 73653f6f 626a6563
    74436c61 73733d63 524c4469 73747269 62757469 6f6e506f 696e7486 3c687474
    703a2f2f 61766179 612d6979 77643530 376a6b2e 696e7465 726f702e 6c61622f
    43657274 456e726f 6c6c2f69 6e746572 6f702831 292e6372 6c308201 2106082b
    06010505 07010104 82011330 82010f30 81a60608 2b060105 05073002 8681996c
    6461703a 2f2f2f43 4e3d696e 7465726f 702c434e 3d414941 2c434e3d 5075626c
    69632532 304b6579 25323053 65727669 6365732c 434e3d53 65727669 6365732c
    434e3d43 6f6e6669 67757261 74696f6e 2c44433d 696e7465 726f702c 44433d6c
    61623f63 41436572 74696669 63617465 3f626173 653f6f62 6a656374 436c6173
    733d6365 72746966 69636174 696f6e41 7574686f 72697479 30640608 2b060105
    05073002 86586874 74703a2f 2f617661 79612d69 79776435 30376a6b 2e696e74
    65726f70 2e6c6162 2f436572 74456e72 6f6c6c2f 61766179 612d6979 77643530
    376a6b2e 696e7465 726f702e 6c61625f 696e7465 726f7028 31292e63 7274303f
    06092b06 01040182 37140204 321e3000 49005000 53004500 43004900 6e007400
    65007200 6d006500 64006900 61007400 65004f00 66006600 6c006900 6e006530
    0c060355 1d130101 ff040230 00301306 03551d25 040c300a 06082b06 01050508
    0202300d 06092a86 4886f70d 01010505 00038181 004ea84c 35989b53 0b64e7e6
    89c8b6d8 938ba17e c8db4e37 c3aebdf6 f5c3c623 391a5c4f 87dd3cf4 1d59a79c
    81f0f112 8a3150f2 0224facb 2ce60191 2f7f7eaf d1b6f6da ccd4899a 967b785e
    20bb1944 71299b6f d3fdedf3 238b4bf2 674a7a26 dc47d465 8c76b563 ed0433ad
    c388c84a 6ab35c0b b3a62478 03ff4a0a b4024288 7a
  quit
 certificate ca 3267928f467534b749f33b1819648b30
    30820369 308202d2 a0030201 02021032 67928f46 7534b749 f33b1819 648b3030
    0d06092a 864886f7 0d010105 0500301f 310b3009 06035504 06130255 53311030
    0e060355 04031307 696e7465 726f7030 1e170d30 37303631 39313835 3130355a
    170d3039 30363138 31393030 33325a30 1f310b30 09060355 04061302 55533110
    300e0603 55040313 07696e74 65726f70 30819f30 0d06092a 864886f7 0d010101
    05000381 8d003081 89028181 00d25942 7cd15b16 9ba45c32 ded0a76a 8d853e09
    3f6d746a a884b645 744c0b97 e0269a32 041f0d8a 76da8d2f 170e2a71 4e8b9c0c
    1bdef20b 0609fe55 f13c0a2f 50aec807 74745306 d9bbef12 ec22726f 115c67ec
    e4bb2e3f f4710c50 f806a6cd 69611773 c9bb1dc5 77845167 2323b2a7 fb69aedf
    5a802b78 01832bd0 55dc29db 33020301 0001a382 01a43082 01a03013 06092b06
    01040182 37140204 061e0400 43004130 0b060355 1d0f0404 03020146 300f0603
    551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 e872da8a 3834f0cc
    1b111243 e21b9b30 be5bcc24 30820111 0603551d 1f048201 08308201 04308201
```


©2007 Avaya Inc. All Rights Reserved.

```
    00a081fd a081fa86 81b96c64 61703a2f 2f2f434e 3d696e74 65726f70 2831292c
    434e3d61 76617961 2d697977 64353037 6a6b2c43 4e3d4344 502c434e 3d507562
    6c696325 32304b65 79253230 53657276 69636573 2c434e3d 53657276 69636573
    2c434e3d 436f6e66 69677572 6174696f 6e2c4443 3d696e74 65726f70 2c44433d
    6c61623f 63657274 69666963 61746552 65766f63 6174696f 6e4c6973 743f6261
    73653f6f 626a6563 74436c61 73733d63 524c4469 73747269 62757469 6f6e506f
    696e7486 3c687474 703a2f2f 61766179 612d6979 77643530 376a6b2e 696e7465
    726f702e 6c61622f 43657274 456e726f 6c6c2f69 6e746572 6f702831 292e6372
    6c301206 092b0601 04018237 15010405 02030100 01302306 092b0601 04018237
    15020416 0414c68f 33916a51 0255822f 4fb798c9 bc51d2b0 cfa2300d 06092a86
    4886f70d 01010505 00038181 00bd27bc ac7d713c 9a215996 10f20ac4 8d600747
    f35e4f09 a97e1d5b f984ea50 092541f8 baf8691c 26e2c22f f380df90 efef0125
    b5e3f901 1feec3f6 27777c56 266f239c e6aa549f c683612c 23bece18 6d6dc861
    ff9de6ea 555c9359 450b383e d93f535f 0aca50ae 5b93f6a7 500e2edd 43d1f5df
    a30b8ba6 e61876c8 b9075898 de
  quit
crypto isakmp enable Outside
crypto isakmp policy 1
 authentication rsa-sig
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group DefaultRAGroup general-attributes
 address-pool vpnphone-ip-pool
tunnel-group DefaultRAGroup ipsec-attributes
 trust-point hope_tp
tunnel-group VPNPHONE type ipsec-ra
tunnel-group VPNPHONE general-attributes
 address-pool vpnphone-ip-pool
 default-group-policy VPNPHONE
tunnel-group VPNPHONE ipsec-attributes
 peer-id-validate nocheck
 trust-point MS-CA02-AV-EST
 isakmp keepalive disable
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
tunnel-group-map VPNphone_rule 10 VPNPHONE
telnet 192.168.1.0 255.255.255.0 Inside
telnet timeout 5
ssh timeout 5
console timeout 0
!
!
prompt hostname context
Cryptochecksum:1e7ba46728d1abd9e5c19bfec517681e
: end
```


©2007 Avaya Inc. All Rights Reserved.

Appendix B: 46vpnsetting.txt

The 46vpnsetting.txt file used in the sample configuration is provided below.

```
############################################################
## Avaya 46VPN IP Telephone Settings Script
## File Created on: 05/21/2007
## See the LAN Administrators Guide for
## more details on using this file.


## Use "##" without quotes to comment out a line.
## To activate a setting below, set the parameter
## to the appropriate value for your network and
## remove the "## " from the beginning of the line.

## To include whitespaces in a value,
## the entire value must be enclosed in double quotes.
## example:
## SET PARAM "value1 value2"

## To set different set types to different values, use
## the "IF" keyword statement.
## See the LAN Administrators Guide for more details.

## Some of the values listed below have default settings which
## are used by the IP Telephones even if they are commented out
## in this file. For a list of those settings and their default
## values, see the LAN Administrators Guide.
##
##

#############################################################################
## NOTE : It is highly recommended to use the 46vpnsetting_template.txt
## for building the customized 46vpnsetting.txt file for your VPN environment.
#############################################################################


## Variable Name : NVVPNMODE
## Valid Values
##    0  DISABLE
##    1  BOOT
##    2  SCRIPT
## Description
##    This variable dictates when the VPN Client is started. If it's value is
##    1, VPN Client is started immediately after TCP/IP stack is initialized,
##    If it's value is 2, VPN Client is started after downloading and processing
##    script file(s) from file server.
##
SET NVVPNMODE 1


## Variable Name : NVVPNCFGPROF
## Valid Values
##    1  Avaya Security Gateway
##    2  Checkpoint
##    3  Cisco Xauth with Preshared Key
##    5  Juniper/Netscreen Xauth with Preshared Key
##    6  Generic Preshared key
##    8  Cisco xauth with certificates
##    9  Juniper Xauth with certificates.
```


©2007 Avaya Inc. All Rights Reserved.

```
##    11 Nortel contivity
##
SET NVVPNCFGPROF 8


## Variable Name : NVSGIP
## Valid Values
##    String. Length of the string cannot exceed 30 characters.
## Description
##   This variable contains the IP address or fully qualified domain name of
##   the primary security gateway.
## Example : Setting primarysg.mycompany.com as the primary security gateway's FQDN.
## SET NVSGIP primarysg.mycompany.com
##
##
## Example : Setting 10.1.1.1 as the primary security gateway's IP address.
## SET NVSGIP 10.1.1.1
##
SET NVSGIP 195.2.2.100


## Variable Name : NVVPNPSWDTYPE
## Valid Values
##    1  Save in Flash.
##    2  Erase on power-off.
##    3  Numeric One Time Password.
##    4  Alpha-Numeric One Time Password.
## Description
##    This variables determines how password should be treated. By default
##    password type is set to 1. You must set this variable to 3 or 4 if
##    using One Time Password such as SecureID from RSA.
##
SET NVVPNPSWDTYPE 1

## Variable Name : NVVPNFILESRVR
## Valid Values
##    String. Length of the string cannot exceed 30 characters.
## Description
##    This variable contains the URL of the file server. A file server URL
##    consist of following components
##       (1) Download Method (HTTP,HTTPS,TFTP).
##       (2) FQDN or actual IP address of the file server.
##       (3) Service port (80 for HTTP and 411 for HTTPS).
##       (4) Path (NONE).
##    All the components specified above except for the FQDN/IP Address has a
##    default value. If download method is omitted from the URL, Phone attempts
##    to download the script file using all the methods.
## Example
## (1) SET NVVPNFILESRVR tftp://srv.domain.com/phone/
## (2) SET NVVPNFILESRVR tftp://10.1.1.1/phone/
## (3) SET NVVPNFILESRVR http://10.1.1.1:8080/phone
## (4) SET NVVPNFILESRVR https://10.1.1.1/phone
## (5) SET NVVPNFILESRVR 10.1.1.1
## The 1st Example above will set the download method to TFTP,
##    TFTPDIR to phone and TFTP Server FQDN to srv.domain.com
## The 2nd Example above will set the download method to TFTP,
##    TFTPDIR to phone and TFTP Server IP Address to 10.1.1.1
## The 3rd Example above will set the download method to HTTP,
##    HTTP Server port to 8080,HTTPDIR to phone and HTTP Server
##    IP Address to 10.1.1.1
## The 4th Example above will set the download method to HTTPS,
##    HTTP Server port to 1443, HTTPDIR to phone and HTTP Server
```


©2007 Avaya Inc. All Rights Reserved.

```
##    IP Address to 10.1.1.1
## The 5th Example above will set the download method to ALL.
##    In this example phone will first attempt HTTPS if that fails
##    it tries HTTP and finally TFTP.
##
## Note : 4625 models do not support HTTPS or HTTP download method. If phone
##    population consist of mix of 4620SW and 4625 phones use IF command to
##    conditionally deliver File Server URLs.
##
## Note : Service port is ignored if download method is HTTPS or TFTP.
##
## Example : Delivering TFTP url to 4625 models and HTTP to 4620SW and 4610
##    models. In this example we assume that TFTP and HTTP service is running
##    on the same machine.
##
##    IF $MODEL4 SEQ 4625 goto tftpmethod
##    SET NVVPNFILESRVR http://10.1.1.1
##    goto flsrvrend
##    # tftpmethod
##    SET NVVPNFILESRVR tftp://10.1.1.1
##    # flsrvrend
##
SET NVVPNFILESRVR http://192.168.1.30


## Variable Name : NVVPNCOPYTOS
## Valid Values
##    1  YES
##    2  NO
## Description
##    Value of this variable decides whether TOS bits should be copied from
##    inner header to outer header or not. If it's value is 1, TOS bits are
##    copied otherwise not. By default TOS bits are not copied from inner
##    header to outer header. Some Internet Service Provider don't route the
##    IP packets properly if TOS bits are set to anything other than 0.
##
SET NVVPNCOPYTOS 1


## Variable Name : NVVPNENCAPS
## Valid Values
##    0  4500-4500
##    1  Disable
##    2  2070-500
##    4  RFC (As per RFC 3947 and 3948)
## Description
##    Type of UDP encapsulation method to use if there is a NAT device between
##    phone and the security gateway. By default UDP Encapsulation 4500-4500
##    is used.
##    If NVVPNENCAPS is 0, ike negotiation starts with source port of 2070
##       and destination port 500. Negotiation switches to port source port
##       4500 and destination port 4500 if peer supports port floating (Ref
##       RFC 3947,3948). Finally IPSec traffic is send inside UDP packets
##       from/to port 4500 if supported by peer or port 2070<->500 if port
##       floating is not supported but UDP encapsulation is supported as
##       published in the initial draft versions of RFC 3947 and 3948.
##     If NVVPNENCAPS is 1, ike nat traversal is completely disabled.
##     If NVVPNENCAPS is 2, Port floating is disabled during IKE nat traversal.
##     If NVVPNENCAPS is 4, ike negotiation starts with source port of 500 and
##       destination port 500. Negotiation switches to port source port 4500
##       and destination port 4500 if peer supports port floating (Ref RFC 3947
##       and 3948). Finally IPSec traffic is send inside UDP packets from/to
```


©2007 Avaya Inc. All Rights Reserved.

```
##       port 4500 if supported by peer or port 500<->500 if port floating is
##       not supported but UDP encapsulation is supported as published in the
##       initial draft versions of RFC 3947 and 3948.
##
SET NVVPNENCAPS 0


## Variable Name : NVVPNCONCHECK
## Valid Values
##    1  First time
##    2  Never
##    3  Always
## Description
##    A tunnel connectivity check is performed after tunnel is setup. If
##    connectivity check fails, tunnel is setup with a different encapsulation
##    method until all the available encapsulation method are attempted or
##    connectivity check is successful. This variable decides if this check
##    should be performed at the end of tunnel setup process and if it has to
##    be performed, how it should behave in the event of connectivity check
##    failure. By default it's value is 1 which means that tunnel connectivity
##    check is performed the very first time only and it's value is changed
##    to 2 after completion of connectivity check (success or failure).
##    If this variable's value is 3 tunnel connectivity check is always
##    performed after tunnel is setup.
##
SET  NVVPNCONCHECK 3


## Variable Name : NVIKEID
## Valid Values
##     String. Length of the string cannot exceed 30 characters.
## Description
##     Phone uses this string as IKE Identifier during phase 1 negotiation.
##     Some XAuth documentation refer to this variable as group name because
##     same    IKE Id is shared among a group of user and individual user
##     authentication is done using XAuth after establishing IKE phase 1
##     security association.
## Note
##     If this variable is left uninitialized, phone uses "VPNPHONE" as the IKE
##     Identifier.
##
SET NVIKEID VPNPHONE


## Variable Name : NVIKEIDTYPE
## Valid Values
##    1    IP Address
##    2    FQDN
##    3    User-FQDN (E-Mail)
##    9    Directory-Name
##    11    KEY-ID (Opaque)
## Description
##    Phone uses this variable as the IKE Identifier type for the
##    IKE-ID specified via NVIKEID variable.
##
SET NVIKEIDTYPE   11


## Variable Name : NVIKEXCHMODE
## Valid Values
##    1    Aggressive
##    2    Identity protect
```


©2007 Avaya Inc. All Rights Reserved.

```
## Description
##    Aggressive – In Aggressive mode, there is no identity protection
##    for the negotiating nodes, because both nodes must transmit their
##    identities before establishing a negotiated secure channel.
##
##    Identity protect – In Identity protect mode, the exchange of ID
##    information occurs in the fifth and sixth messages exchanged during
##    Phase 1 negotiations, after a secure channel has been established
##    by the first four messages.
##
SET NVIKEXCHGMODE 2


## Variable Name : NVIKEDHGRP
## Valid Values
##    1    Diffie-Hellman Group 1
##    2    Diffie-Hellman Group 2
##    5    Diffie-Hellman Group 5
## Description
##    This variable contains the value of DH group to use during phase 1
##    negotiation. By default phone uses Group 2.
##
SET NVIKEDHGRP 2


## Variable Name : NVPFSDHGRP
## Valid Values
##    0    No-PFS
##    1    Diffie-Hellman Group 1
##    2    Diffie-Hellman Group 2
##    5    Diffie-Hellman Group 5
## Description
##    This variable contains the value of DH group to use during phase 2
##    negotiation for establishing IPSec security associations also known
##    as perfect forward secrecy (PFS).
##    By default PFS is disabled.
##
SET NVPFSDHGRP 2


## Variable Name : NVIKEP1ENCALG
## Valid Values
##    0    ANY
##    1    AES-128
##    2    3DES
##    3    DES
##    4    AES-192
##    5    AES-256
## Description
##    Encryption Algorithms to propose for IKE Phase 1 Security Association.
##
SET NVIKEP1ENCALG 2


## Variable Name : NVIKEP2ENCALG
## Valid Values
##     0    ANY
##     1    AES-128
##     2    3DES
##     3    DES
##     4    AES-192
##     5    AES-256
```


©2007 Avaya Inc. All Rights Reserved.

```
## Description
##     Encryption Algorithm(s) to propose for IKE Phase 2 Security
##     Association.
##
SET NVIKEP2ENCALG 1


## Variable Name : NVIKEP1AUTHALG
## Valid Values
##    0    ANY
##    1    MD5
##    2    SHA1
## Description
##    Authentication Algorithm(s) to propose for IKE phase 1 Security
##    Association.
##
SET NVIKEP1AUTHALG 1


## Variable Name : NVIKEP2AUTHALG
## Valid Values
##    0    ANY
##    1    MD5
##    2    SHA1
## Description
##    Authentication Algorithm(s) to propose for IKE phase 2 Security
##    Association
##
SET NVIKEP2AUTHALG 2



##########################################
## Certificate Related Variables Below    #
##########################################


## Variable Name : TRUSTCERTS
## Valid Values
##     Name of a file containing CA certificate
##     in PEM format. Length of the file name
##     cannot be more than 16 characters.
## Description
##     Use this variable to import CA
##     certificates. The certificate presented
##     by peer is validated against the list of
##     CAs imported through this command. Maximum
##     number of CAs that can be imported is limited
##     to 5.
## Example
##    SET TRUSTCERTS CA1.CER,CA2.CER,CA3.CER
##
SET TRUSTCERTS 46vpn_cert.cer



## Variable Name : MYCERTURL
## Valid Values
##     URL for enrolling with a SCEP fronted Certificate Authority.
##
## Description
##     If this information is supplied, phone generates a RSA key pair
```


©2007 Avaya Inc. All Rights Reserved.

```
##     and sends the enrollment request using SCEP protocol to the
##     server pointed by this URL. Consult your CA administrator guide
##     for further information regarding SCEP support.
##
SET MYCERTURL http://192.168.1.30/certsrv/mscep/mscep.dll



## Variable Name : MYCERTCN
## Valid values
##     $MACADDR
##     $SERIALNO
##
## Description
##     If value of this variable is set to $MACADDR, phone uses it's
##        MAC Address as the CN component of the certificate request
##     If value of this variable is set to $SERIALNO, phone uses it's
##        Serial Number as the CN component of the certificate request.
##
SET MYCERTCN $MACADDR


## Variable Name : SCEPPASSWORDREQ
## Valid values
##      0
##      1
##
## Description
##      If value of this variable is set to 1, phone user is prompted to
##        enter challenge pass phrase during SCEP certificate enrollment.
##      If value of this variable is set to 0, phone uses the challenge
##        pass phrase as indicated by SCEPPASSWORD variable.
##
## Note
##      Consult your Certificate Authority administrator guide for HOWTO
##      configure pass phrase for SCEP certificate enrollment.
##
SET SCEPPASSWORDREQ 0


## Variable Name : SCEPPASSWORD
## Valid values
##      String
##
## Description
##      The string specified here is used by phone as the SCEP challenge pass
##      phrase for SCEP certificate enrollment. If left unspecified and
##      SCEPPASSWORDREQ is SET to 0, phone uses it's SERIAL number as the challenge
##      pass phrase.
## Note
##      Consult your Certificate Authority administrator guide for HOWTO
##      configure pass phrase for SCEP certificate enrollment.
##
SET SCEPPASSWORD "E676148554572C61"
```


©2007 Avaya Inc. All Rights Reserved.

©2007 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com