CHAPTER 4

# Fulfilling Other Administrative Requirements for AnyConnect

This chapter provides the following instructions:



## Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users

An Active Directory Domain Administrator can push a group policy to domain users that adds the security appliance to the list of trusted sites in Internet Explorer. Note that this differs from the procedure to add the security appliance to the list of trusted sites by individual users. This procedure applies only to Internet Explorer on Windows machines that are managed by a domain administrator.

**Note** Adding a security appliance to the list of trusted sites for Internet Explorer is required for those running Windows Vista who want to use WebLaunch.

To create a policy to add the Security Appliance to the Trusted Sites security zone in Internet Explorer by Group Policy using Active Directory, perform the following steps:

**Step 1** Log on as a member of the Domain Admins group.

**Step 2** Open the Active Directory Users and Computers MMC snap-in.

**Step 3** Right-click the Domain or Organizational Unit where you want to create the Group Policy Object and click Properties.

**Step 4** Select the Group Policy tab and click New.

**Step 5** Type a name for the new Group Policy Object and press Enter.

**Step 6** To prevent this new policy from being applied to some users or groups, click Properties. Select the Security tab. Add the user or group that you want to *prevent* from having this policy, then clear the Read and the Apply Group Policy check boxes in the Allow column. Click OK.

**Step 7** Click Edit and choose User Configuration > Windows Settings > Internet Explorer Maintenance > Security.

**Step 8** Right-click Security Zones and Content Ratings in the right-hand pane, then click Properties.

**Step 9** Select Import the current security zones and privacy settings. If prompted, click Continue.

**Step 10** Click Modify Settings, select Trusted Sites, and click Sites.

**Step 11** Type the URL for the Security Appliance that you want to add to the list of Trusted Sites and click Add. The format can contain a hostname (https://vpn.mycompany.com) or IP address (https://192.168.1.100). It can be an exact match (https://vpn.mycompany.com) or a wildcard (https://*.mycompany.com).

**Step 12** Click Close and click OK continually until all dialog boxes close.

**Step 13** Allow sufficient time for the policy to propagate throughout the domain or forest.

**Step 14** Click OK in the Internet Options window.

# Configuring CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

**Step 1** Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:

- The CD shipped with the security appliance.
- The software download page for the ASA 5500 Series Adaptive Security Appliance at http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip

**Step 2** Extract the .export files from the .zip package files.

**Step 3** Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.

**Step 4** Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

**Step 5** Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations.*