Interoperability Guidelines and Requirements

This chapter provides the following instructions:

Using Quarantine to Restrict Non-Compliant Clients

Through the use of quarantine, you can restrict a particular client that is attempting to initiate a VPN connection. The ASA applies restricted ACLs to a session to form a restricted group, based on the dynamic access policies configured in Configuration > Remote Access VPN > Network (Client) Access or Clientless SSL VPN Access > Dynamic Access Policies. When an endpoint is not compliant with an administratively defined policy, the user can still access services for remediation (such as updating an antivirus application), but restrictions are placed upon the user. After the remediation occurs, the user can reconnect, which invokes a new posture assessment. If this assessment passes, the user connects without any restrictions.

Quarantine Requirements

Quarantine requires an AnyConnect Premium license activated on the adaptive security appliance. The advanced endpoint assessment remediates endpoints that do not comply with dynamic policy requirements for antivirus, antispyware, and firewall applications, and any associated application definition file requirements. Advanced endpoint assessment is a Cisco Secure Desktop Host Scan feature, so AnyConnect supports quarantine on all OSs supported by AnyConnect.

ASA Release 8.3(1) or later features dynamic access policies and group policies that support a user message to display on the AnyConnect GUI when the user is first notified of the quarantine. Other quarantine messages (such as “Quarantined - Remediation Required” and “To attempt a normal connection, please reconnect”) are reported, but these messages cannot be defined by the administrator to show the users. Quarantine does not require the ASA upgrade; only the user message requires it.

If you upgrade the ASA software, we recommend that you also upgrade ASDM to Release 6.3(1) or later so that you can use it to configure the new features.

AnyConnect supports quarantine on all OSs supported by AnyConnect. The client supports the quarantine user message on Windows 7, Vista, XP and Mac OS and Linux.

Configuring Quarantine

To configure quarantine:

Step 1 (Optional) Choose **Configuration** > **Remote Access VPN** > **Secure Desktop Manager** > **Host Scan** > **Advanced Endpoint Assessment** if you want to configure Host Scan to remediate noncompliant computers.

Step 2 Choose > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies**, click **Add**, create a DAP that uses endpoint attributes that identify noncompliant computers, click the **Action** tab, and click **Quarantine**.

Step 3 (Optional) Enter a message to display for the user in a quarantined session.

Use the ASDM help if you need more information with configuring dynamic access policies.

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.

A security appliance uses data that is stored in filtering tables to evaluate and match URL request attributes such as domain names and IP address path segments with locally maintained database records. If a match occurs, access policy settings determine an action to block or monitor the traffic. If no match occurs, processing continues.

Note Adding a security appliance to the list of trusted sites for Internet Explorer is required for those running Windows Vista or Windows 7 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 AnyConnect 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 AnyConnect and Cisco Secure Desktop to interoperate with the ASA.

To do this, follow these steps:

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

- The CD shipped with the ASA.
- 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.*

Port Information for AnyConnect and the Legacy VPN Client

Table 10-1and Table 10-2 provide port information that may help you migrate users from the legacy Cisco VPN client to the Cisco AnyConnect Secure Mobility client:

Table 10-1 Ports Used by the AnyConnect Client

Protocol	Cisco AnyConnect Client Port
TLS (SSL)	TCP 443
SSL Redirection	TCP 80 (optional)
DTLS	UDP 443 (optional, but *highly* recommended)
IPsec/IKEv2	UDP 500, UDP 4500

Table 10-2 Ports Used by the Cisco VPN (IPsec) Client

Protocol	Cisco VPN Client (IPsec) Port
IPsec/NATT	UDP 500, UDP 4500
IPsec/NATT	UDP 500, UDP 4500
IPsec/TCP	TCP (configurable)
IPsec/UDP	UDP 500, UDP X (configurable)

Differences in Client Split Tunneling Behavior for Traffic within the Subnet

The AnyConnect client and the legacy Cisco VPN client (the IPsec/IKEv1 client) behave differently when passing traffic to sites within the same subnet as the IP address assigned by the ASA. With AnyConnect, the client passes traffic to all sites specified in the split tunneling policy you configured, and to all sites that fall within the same subnet as the IP address assigned by the ASA. For example, if the IP address assigned by the ASA is 10.1.1.1 with a mask of 255.0.0.0, the endpoint device passes all traffic destined to 10.0.0.0/8, regardless of the split tunneling policy.

By contrast, the legacy Cisco VPN client only passes traffic to addresses specified by the split-tunneling policy, regardless of the subnet assigned to the client.

Therefore, use a netmask for the assigned IP address that properly references the expected local subnet.