PIX/ASA: IPsec VPN Client Auto-Update Feature Configuration Example

Contents

Introduction

This document describes how to configure the Cisco VPN Client Auto-Update feature in the Cisco ASA 5500 Series Adaptive Security Appliance and Cisco PIX 500 Series Security Appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Adaptive Security Appliance runs Version 7.x and later
- Cisco PIX 500 Series Security Appliances runs Version 7.x and later
- Cisco Adaptive Security Device Manager (ASDM) version 5.x and later
- Cisco VPN Client 4.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

How to Configure Client Update for Windows with CLI

The client update feature lets administrators at a central location automatically notify VPN client users when it is time to update the VPN client software and the VPN 3002 hardware client image.

Issue the **client-update** command in `tunnel-group ipsec-attributes` configuration mode in order to configure client update. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client does not run a software version on the list, it should update. You can specify up to four client update entries.

The command syntax follows:

```
client-update type type {url url-string} {rev-nums rev-nums} no client-update [type]
```

- **rev-nums** *rev-nums*—Specifies the software or firmware images for this client. Enter up to four, separated by commas.
- *type*—Specifies the operating systems to notify of a client update. The list of operating systems comprises of these:Microsoft Windows: all windows-based platformsWIN9X: Windows 95, Windows 98, and Windows ME platformsWinNT: Windows NT 4.0, Windows 2000, and Windows XP platformsvpn3002: VPN 3002 hardware client
- **url** *url-string*—Specifies the URL for the software/firmware image. This URL must point to a file appropriate for the client.

This example configures client update parameters for the remote-access tunnel-group called remotegrp. It designates the revision number 4.6.1 and the URL for the retrieval of the update, which is `https://support/updates`.

ASA

```
hostname(config)#tunnel-group remotegrp type ipsec_ra
hostname(config)#tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)#client-update type windows url
https://support/updates/rev-nums 4.6.1
```

How to Configure Client Update for Windows with ASDM

This document assumes that the basic configuration, such as interface configuration, is already made and works properly.

Refer to Allowing HTTPS Access for ASDM in order to allow the ASA to be configured by the ASDM

ASDM encompasses two kinds of client update: one that supports Windows clients and VPN 3002 hardware clients through a tunnel group, and the other that supports ASA devices acting as an auto-update server.

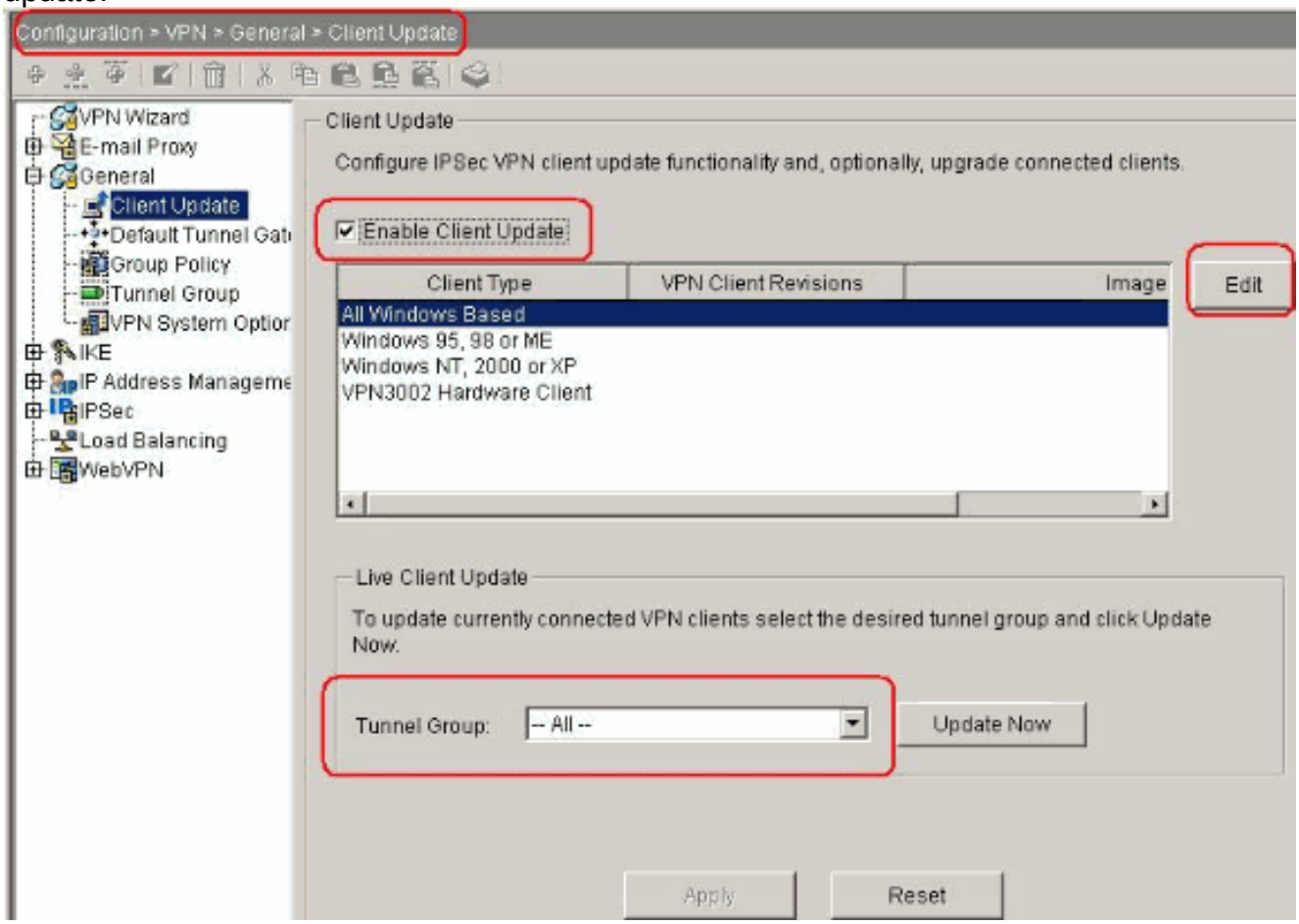
Remote users can use outdated VPN software or hardware client versions. You can perform a client-update at any time to do these functions:

- Enable updating client revisions.
- Specify the types and revision numbers of clients to which the update applies.
- Provide a URL or IP address from which to get the update.
- Optionally notify Windows client users that they should update their VPN client version.
- For Windows clients, you can provide a mechanism for users to accomplish the update.

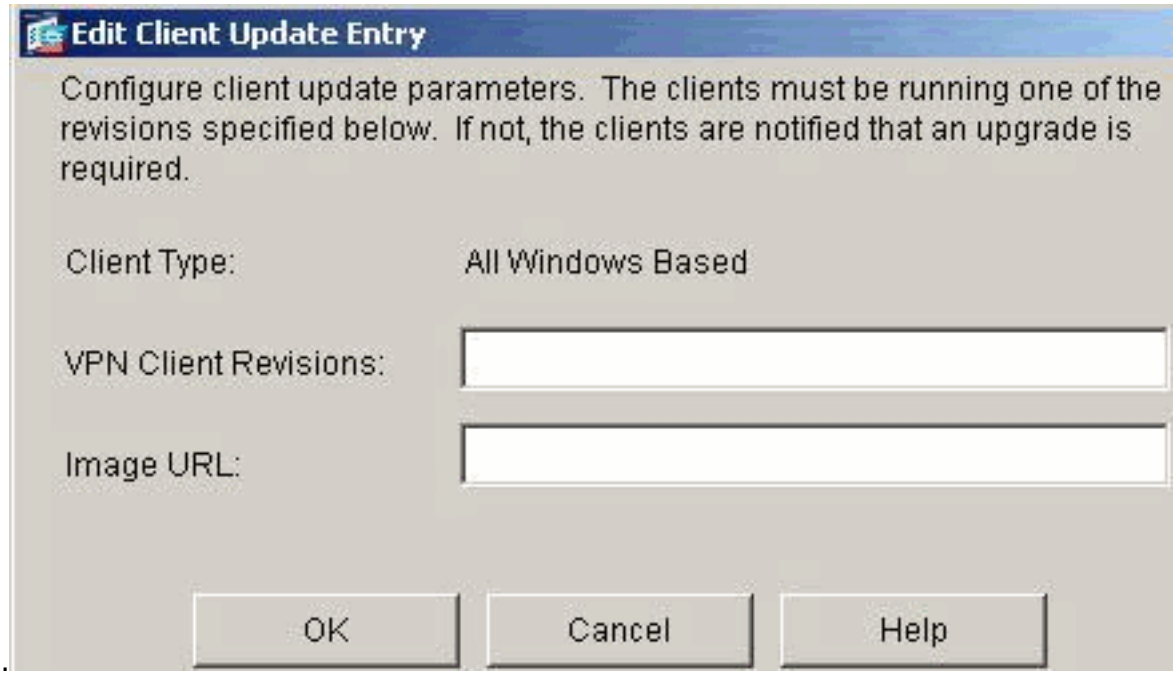
- For VPN 3002 hardware client users, the update occurs automatically, with no notification.

Complete these steps in order to configure a client-update:

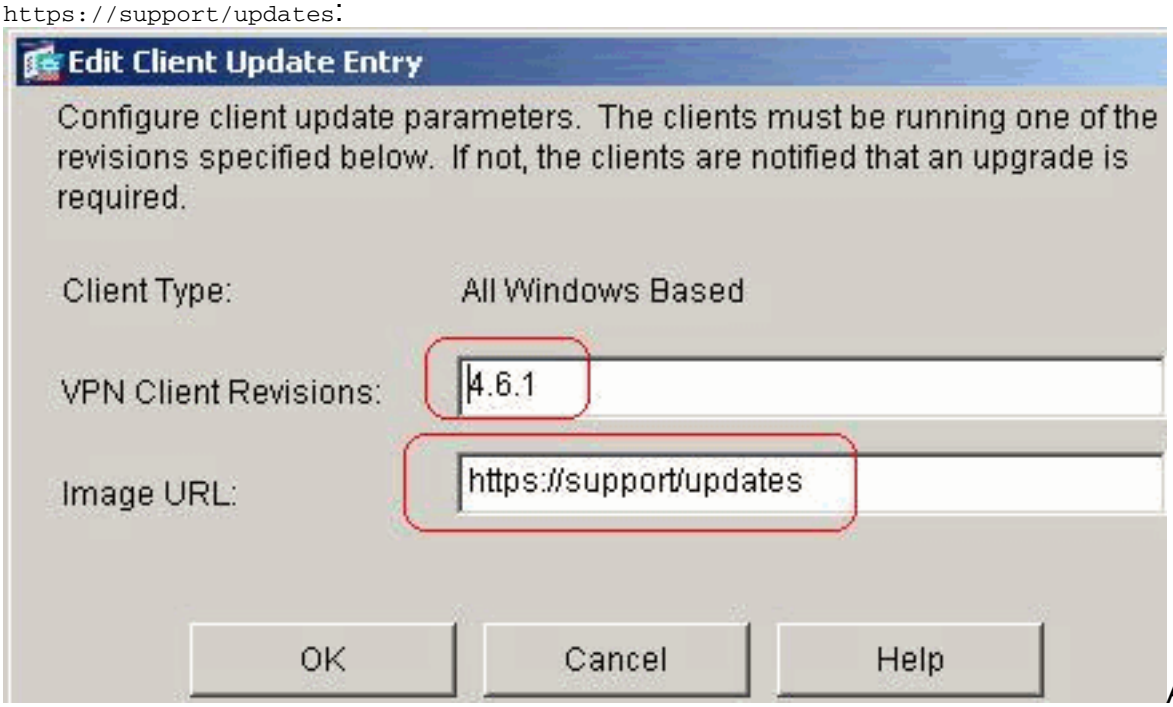
1. Choose **Configuration > VPN > General > Client Update** in order to go to the client update window. The Client Update window opens.Check the **Enable Client Update** check box in order to enable client update.Choose the type of client to which you want to apply the client update. The available client types are **All Windows-Based, Windows 95, 98 or ME, Windows NT 4.0, 2000 or XP, and VPN 3002 Hardware Client.**If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update. You can specify up to three of these client update entries. The All Windows Based selection covers all of the allowable Windows platforms. If you select this, do not specify the individual Windows client types.Click **Edit** in order to specify the acceptable client revisions and the source for the updated software or firmware image for the client update.



2. The Edit Client Update Entry window appears and shows the client type

selection. 

3. Specify the client update that you want to apply to all clients of the selected type across the entire security appliance. That is, specify the type of client, the URL or IP address from which to get the updated image, and the acceptable revision number or numbers for that client. You can specify up to four revision numbers, separated by commas. Your entries appear in the appropriate columns the table on the Client Upgrade window after you click **OK**.If the client revision number matches one of the specified revision numbers, there is no need to update the client.**Note:** For all Windows clients, you must use the protocol http:// or https:// as the prefix for the URL. For the VPN 3002 hardware client, you must specify protocol tftp:// instead.It initiates a client update for all Windows clients for a remote-access tunnel-group running revisions older than 4.6.1 and specifies the URL for the retrieval of the update as `https://support/updates`:



Alternatively, you can configure client update just for individual client types, rather than for all Windows clients, which you can see if step 1-c.VPN 3002 clients update without user intervention and users receive no notification message.You can have the browser automatically start an application if you include the application name at the end of the URL; for example: **https://support/updates/vpnclient.exe.**

4. Optionally, you can send a notice to active users with outdated Windows clients who need to update their client. Use the Live Client Update area of the Client Update window in order to send this notice. Choose the tunnel group (or All) and click **Update Now**. A dialog box appears in figure and asks you to confirm that you want to notify connected clients about the upgrade.

The designated users see a pop-up window, which offers them the opportunity to launch a browser and download the updated software from the site that you specified in the URL. The only part of this message that you can configure is the URL. (See steps 1-b or 1-c.) Users who are not active get a notification message the next time they log on. You can send this notice to all active clients on all tunnel groups, or you can send it to clients on a particular tunnel group.If the client revision number matches one of the specified revision numbers, there is no need to update the client, and no notification message is sent to the user. VPN 3002 clients update without user intervention and users receive no notification message.

Verify

There is currently no verification procedure available for this configuration.

Related Information

- **Technical Support & Documentation - Cisco Systems**