PIX/ASA: Konfigurationsbeispiel für die IPsec VPN-Client-Funktion zur automatischen Aktualisierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco VPN Client Auto-Update-Funktion in den Cisco Adaptive Security Appliances der Serie ASA 5500 und den Cisco Security Appliances der Serie PIX 500 konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance der Serie ASA 5500 mit Version 7.x und höher
- Cisco PIX Security Appliances der Serie 500 führen Version 7.x und höher aus
- Cisco Adaptive Security Device Manager (ASDM) Version 5.x und höher
- Cisco VPN Client 4.x oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren von Client Update für Windows mit CLI

Mit der Client-Update-Funktion können Administratoren an einem zentralen Standort VPN-Client-Benutzer automatisch benachrichtigen, wenn die VPN-Client-Software und das VPN 3002-Hardware-Client-Image aktualisiert werden sollen.

Führen Sie den Befehl **client-update** im `tunnel-group ipsec-attribute-`Konfigurationsmodus aus, um die Client-Aktualisierung zu konfigurieren. Wenn der Client bereits eine Softwareversion auf der Liste der Revisionsnummern ausführt, muss er die Software nicht aktualisieren. Wenn der Client keine Softwareversion in der Liste ausführt, sollte er aktualisiert werden. Sie können bis zu vier Clientaktualisierungseinträge angeben.

Die Befehlssyntax folgt:

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

- **rev-nums** *rev-nums*: Gibt die Software- oder Firmware-Images für diesen Client an. Geben Sie bis zu vier durch Kommas getrennte Felder ein.
- *type*: Gibt die Betriebssysteme an, die über ein Clientupdate benachrichtigt werden sollen. Die Liste der Betriebssysteme umfasst folgende Komponenten:Microsoft Windows: alle Windows-basierten PlattformenWIN9X: Windows 95-, Windows 98- und Windows ME-PlattformenWinNT: Plattformen Windows NT 4.0, Windows 2000 und Windows XPVPN3002: VPN 3002 Hardware-Client
- **url** *url-string*: Gibt die URL für das Software-/Firmware-Image an. Diese URL muss auf eine für den Client geeignete Datei verweisen.

In diesem Beispiel werden die Clientaktualisierungsparameter für die Remote-Zugriffstunnel-Gruppe namens remotegrp konfiguriert. Sie gibt die Versionsnummer 4.6.1 und die URL für den Abruf der Aktualisierung an, die lautet `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**

Konfigurieren von Client Update für Windows mit ASDM

In diesem Dokument wird davon ausgegangen, dass die Basiskonfiguration, z. B. die Schnittstellenkonfiguration, bereits erstellt wurde und ordnungsgemäß funktioniert.

Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

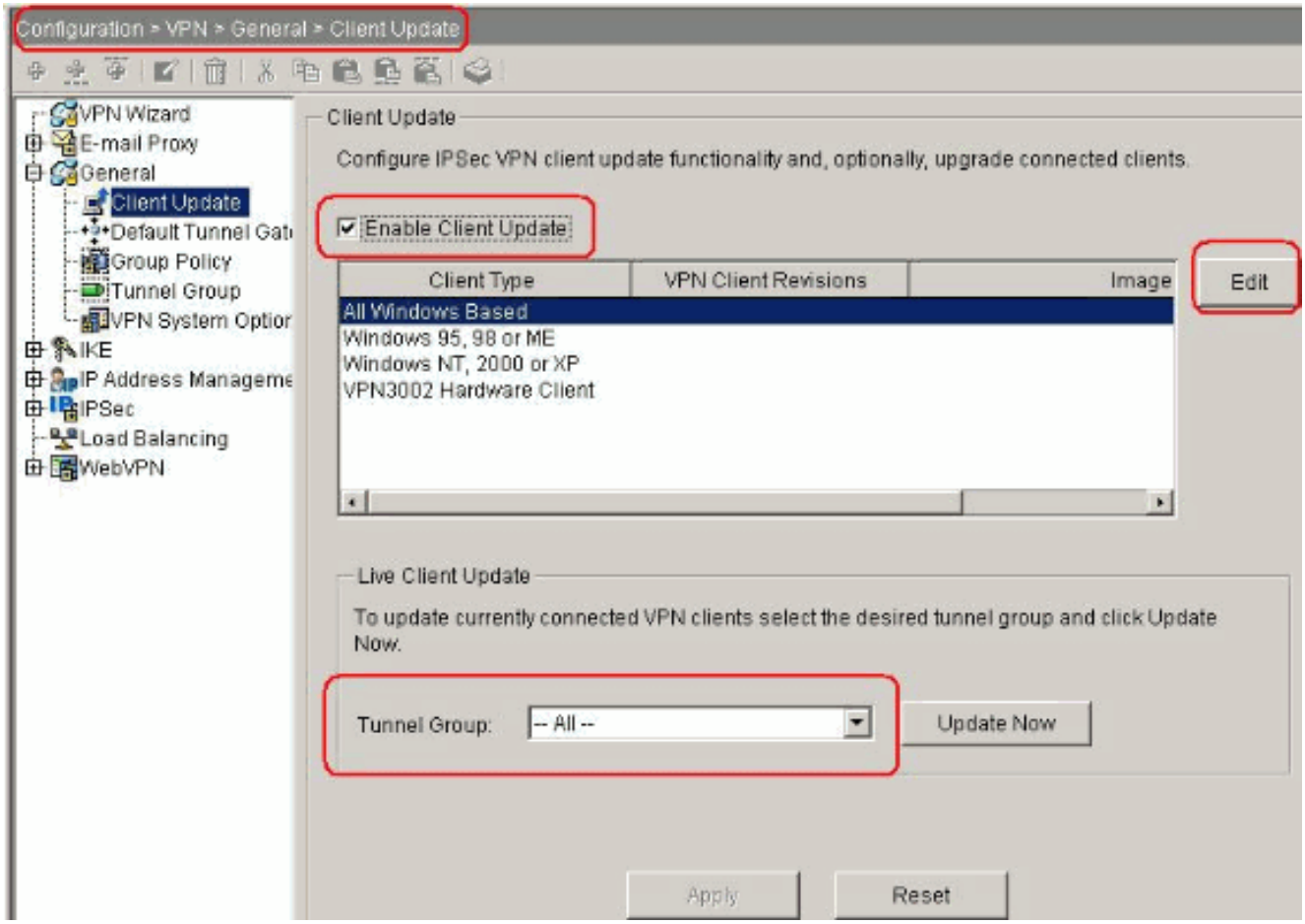
ASDM umfasst zwei Arten von Client-Updates: einer unterstützt Windows-Clients und VPN 3002-Hardware-Clients über eine Tunnelgruppe, der andere unterstützt ASA-Geräte, die als Auto-Update-Server fungieren.

Remote-Benutzer können veraltete VPN-Software- oder Hardware-Client-Versionen verwenden. Sie können jederzeit eine Client-Aktualisierung durchführen, um folgende Funktionen auszuführen:

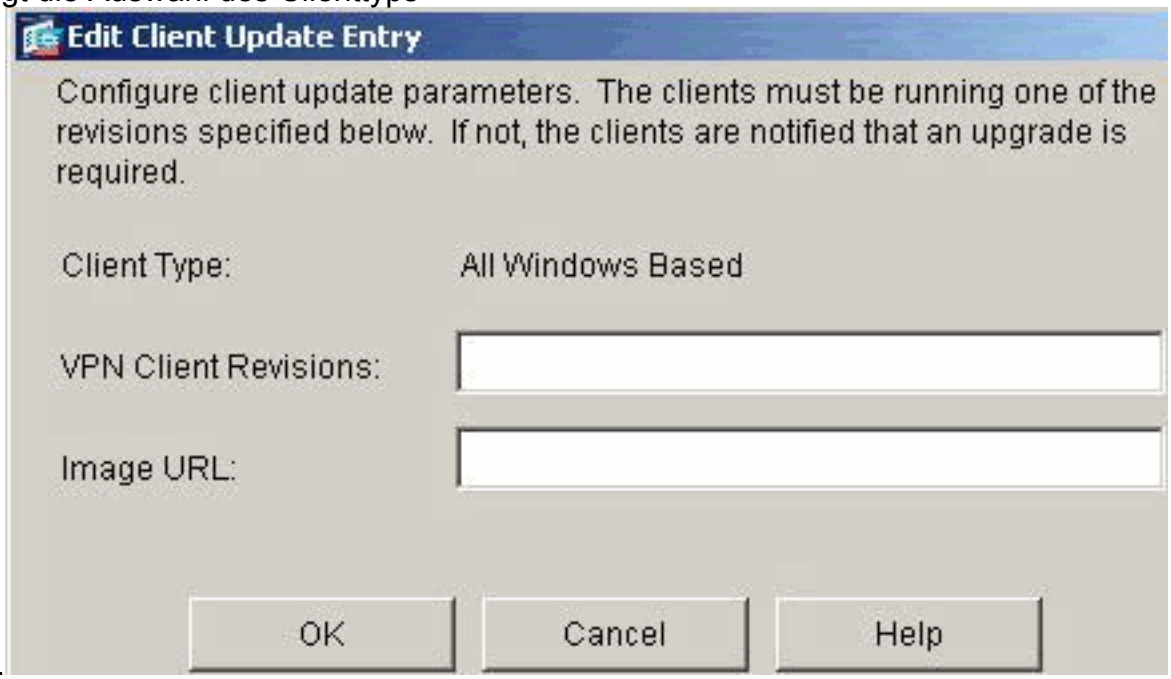
- Aktivieren Sie die Aktualisierung von Client-Versionen.
- Geben Sie die Typen und Revisionsnummern von Clients an, auf die das Update angewendet wird.
- Geben Sie eine URL oder IP-Adresse an, von der die Aktualisierung abgerufen werden soll.
- Benutzer von Windows-Clients können optional darüber informieren, dass sie ihre VPN-Clientversion aktualisieren sollen.
- Für Windows-Clients können Sie einen Mechanismus bereitstellen, mit dem Benutzer die Aktualisierung durchführen können.
- Bei Benutzern von VPN 3002-Hardware-Clients erfolgt die Aktualisierung automatisch und ohne Benachrichtigung.

Gehen Sie wie folgt vor, um eine Client-Aktualisierung zu konfigurieren:

1. Wählen Sie **Configuration > VPN > General > Client Update (Konfiguration > VPN > Allgemein > Client-Update)**, um zum Fenster für die Client-Aktualisierung zu gelangen. Das Fenster Client Update (Client-Aktualisierung) wird geöffnet.Aktivieren Sie das Kontrollkästchen **Client-Aktualisierung aktivieren**, um die Client-Aktualisierung zu aktivieren.Wählen Sie den Client-Typ aus, auf den Sie das Client-Update anwenden möchten. Verfügbare Client-Typen sind **All Windows-Based, Windows 95, 98 oder ME, Windows NT 4.0, 2000 oder XP und VPN 3002 Hardware Client.**Wenn der Client bereits eine Softwareversion auf der Liste der Revisionsnummern ausführt, muss er die Software nicht aktualisieren. Wenn der Client keine Softwareversion in der Liste ausführt, sollte er aktualisiert werden. Sie können bis zu drei dieser Clientaktualisierungseinträge angeben. Die Auswahl All Windows Based (Alle Windows-basierten Plattformen) deckt alle zulässigen Windows-Plattformen ab. Wenn Sie diese Option auswählen, geben Sie nicht die einzelnen Windows-Clienttypen an.Klicken Sie auf **Bearbeiten**, um die zulässigen Client-Versionen und die Quelle für das aktualisierte Software- oder Firmware-Image für das Client-Update anzugeben.

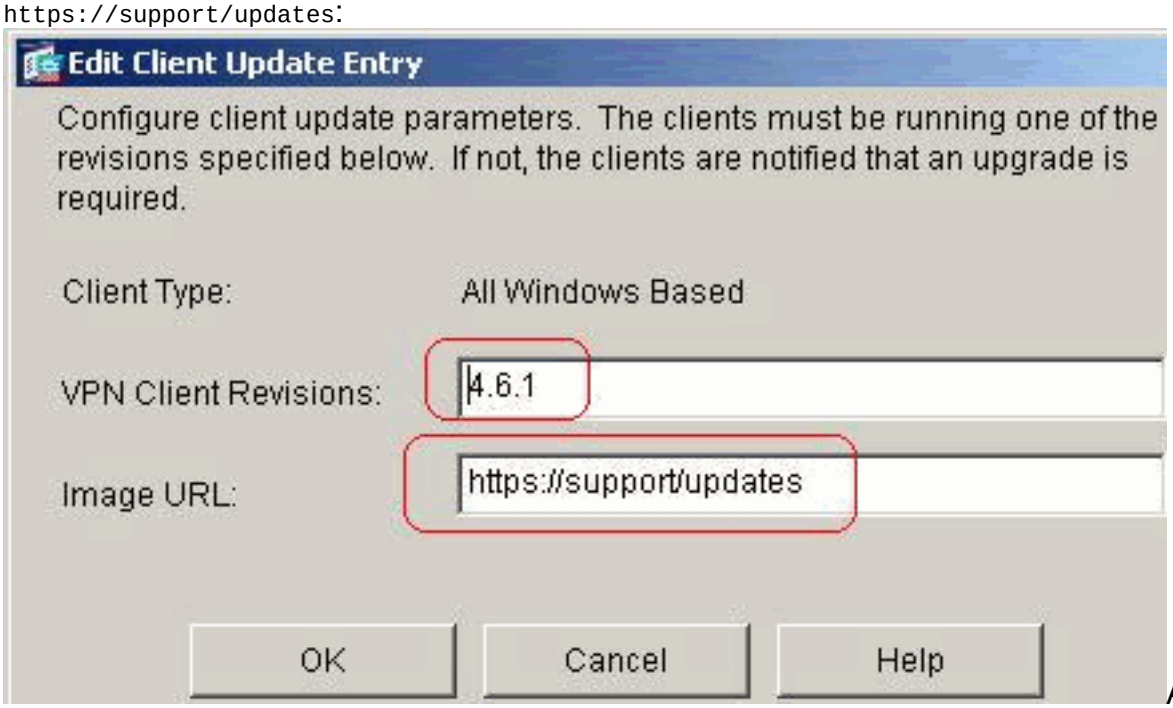


2. Das Fenster Edit Client Update Entry (Client-Update-Eintrag bearbeiten) wird angezeigt und zeigt die Auswahl des Clienttyps an.



3. Geben Sie das Client-Update an, das auf alle Clients des ausgewählten Typs in der gesamten Sicherheits-Appliance angewendet werden soll. Das heißt, geben Sie den Client-Typ, die URL oder die IP-Adresse an, von der das aktualisierte Image abgerufen werden soll, und die akzeptable(n) Revisionsnummer(n) für diesen Client. Sie können bis zu vier durch Kommas getrennte Revisionsnummern angeben. Ihre Einträge werden in den entsprechenden Spalten in der Tabelle im Fenster Client Upgrade angezeigt, nachdem Sie auf **OK** klicken.Wenn die Client-Revisionsnummer mit einer der angegebenen Revisionsnummern übereinstimmt, muss der Client nicht aktualisiert werden.**Hinweis:** Für

alle Windows-Clients müssen Sie das Protokoll http:// oder https:// als Präfix für die URL verwenden. Für den VPN 3002-Hardware-Client müssen Sie stattdessen das Protokoll tftp:// angeben.Es initiiert ein Client-Update für alle Windows-Clients für eine Tunnel-Gruppe mit Remotezugriff, in der Versionen ausgeführt werden, die älter als 4.6.1 sind, und gibt die URL für den Abruf der Aktualisierung an als `https://support/updates`:



Alternativ können Sie die Clientaktualisierung nur für einzelne Clienttypen und nicht für alle Windows-Clients konfigurieren, die Sie sehen können, wenn Sie Schritt 1-c ausführen.VPN 3002-Clients werden ohne Benutzereingriff aktualisiert, und die Benutzer erhalten keine Benachrichtigung.Sie können festlegen, dass der Browser eine Anwendung automatisch startet, wenn Sie den Anwendungsnamen am Ende der URL angeben. Beispiel: **https://support/updates/vpnclient.exe**

4. Optional können Sie eine Benachrichtigung an aktive Benutzer mit veralteten Windows-Clients senden, die ihren Client aktualisieren müssen. Verwenden Sie den Bereich Live Client Update (Live-Client-Update) im Fenster Client Update (Client-Update), um diese Benachrichtigung zu senden. Wählen Sie die Tunnelgruppe (oder Alle) aus, und klicken Sie auf **Jetzt aktualisieren**. In der Abbildung wird ein Dialogfeld angezeigt, in dem Sie bestätigen müssen, dass Sie die angeschlossenen Clients über die Aktualisierung informieren möchten.

Die designierten Benutzer sehen ein Popup-Fenster, das ihnen die Möglichkeit bietet, einen Browser zu starten und die aktualisierte Software von der Website herunterzuladen, die Sie

in der URL angegeben haben. Der einzige Teil dieser Meldung, den Sie konfigurieren können, ist die URL. (Siehe Schritte 1-b oder 1-c.) Benutzer, die nicht aktiv sind, erhalten bei der nächsten Anmeldung eine Benachrichtigung. Sie können diese Benachrichtigung an alle aktiven Clients in allen Tunnelgruppen senden oder an Clients in einer bestimmten Tunnelgruppe senden.Wenn die Client-Revisionsnummer mit einer der angegebenen Revisionsnummern übereinstimmt, muss der Client nicht aktualisiert werden, und es wird keine Benachrichtigung an den Benutzer gesendet. VPN 3002-Clients werden ohne Benutzereingriff aktualisiert, und die Benutzer erhalten keine Benachrichtigung.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems