

PIX/ASA: Configuratievoorbeeld van IPsec VPN-client voor automatisch bijwerken

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Hoe clientupdate voor Windows instellen met CLI](#)

[Hoe clientupdate voor Windows instellen met ASDM](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u de Cisco VPN-clientfunctie Auto-Update kunt configureren in Cisco ASA 5500 Series adaptieve security applicatie en Cisco PIX 500 Series security applicaties.

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series adaptieve security applicatie, versie 7.x en hoger
- Cisco PIX 500 Series security applicaties, versie 7.x en hoger
- Cisco Adaptieve Security Devices Manager (ASDM) versie 5.x en hoger
- Cisco VPN-client 4.x en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Hoe clientupdate voor Windows instellen met CLI

Met de client update optie kunnen beheerders op een centrale locatie VPN-clientgebruikers automatisch op de hoogte stellen als het tijd is om de VPN-clientsoftware en het VPN 3002 hardware-clientbeeld bij te werken.

Geef de **client-update** opdracht uit in de `tunnel-groep ipsec-eigenschappen` configuratie modus om client-update te configureren. Als de client al een softwareversie in de lijst met revisienummers heeft uitgevoerd, hoeft deze niet bij te werken. Als de client geen softwareversie in de lijst gebruikt, moet deze worden bijgewerkt. U kunt maximaal vier client-update-items instellen.

De opdrachtsyntaxis volgt:

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

- Specificeert de software of firmware beelden voor deze client. Voer maximaal vier in, gescheiden door komma's.
- *type*-Specificeert de besturingssystemen om van een client update op de hoogte te stellen. De lijst van besturingssystemen bestaat uit:Microsoft Windows: alle op ramen gebaseerde platformsWIN9X: Windows 95, Windows 98 en Windows ME-platformsWinNT: Windows NT 4.0, Windows 2000 en Windows XP-platformsVPN3002: VPN 3002 hardwareclient
- *url-string*-Specificeert de URL voor de software/firmware-afbeelding. Deze URL moet naar een bestand wijzen dat geschikt is voor de client.

Dit voorbeeld vormt client update parameters voor de afstandstoegangstunnel-groep genaamd remointegration. Het wijst het herzieningsnummer 4.6.1 en de URL aan voor het ophalen van de update, dat is `https://support/updates`.

ASA
<pre>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</pre>

Hoe clientupdate voor Windows instellen met ASDM

Dit document gaat ervan uit dat de basisconfiguratie, zoals de interfaceconfiguratie, al is gemaakt en correct werkt.

Raadpleeg [HTTPS-toegang voor ASDM toestaan](#) om de ASA te kunnen configureren door de ASDM

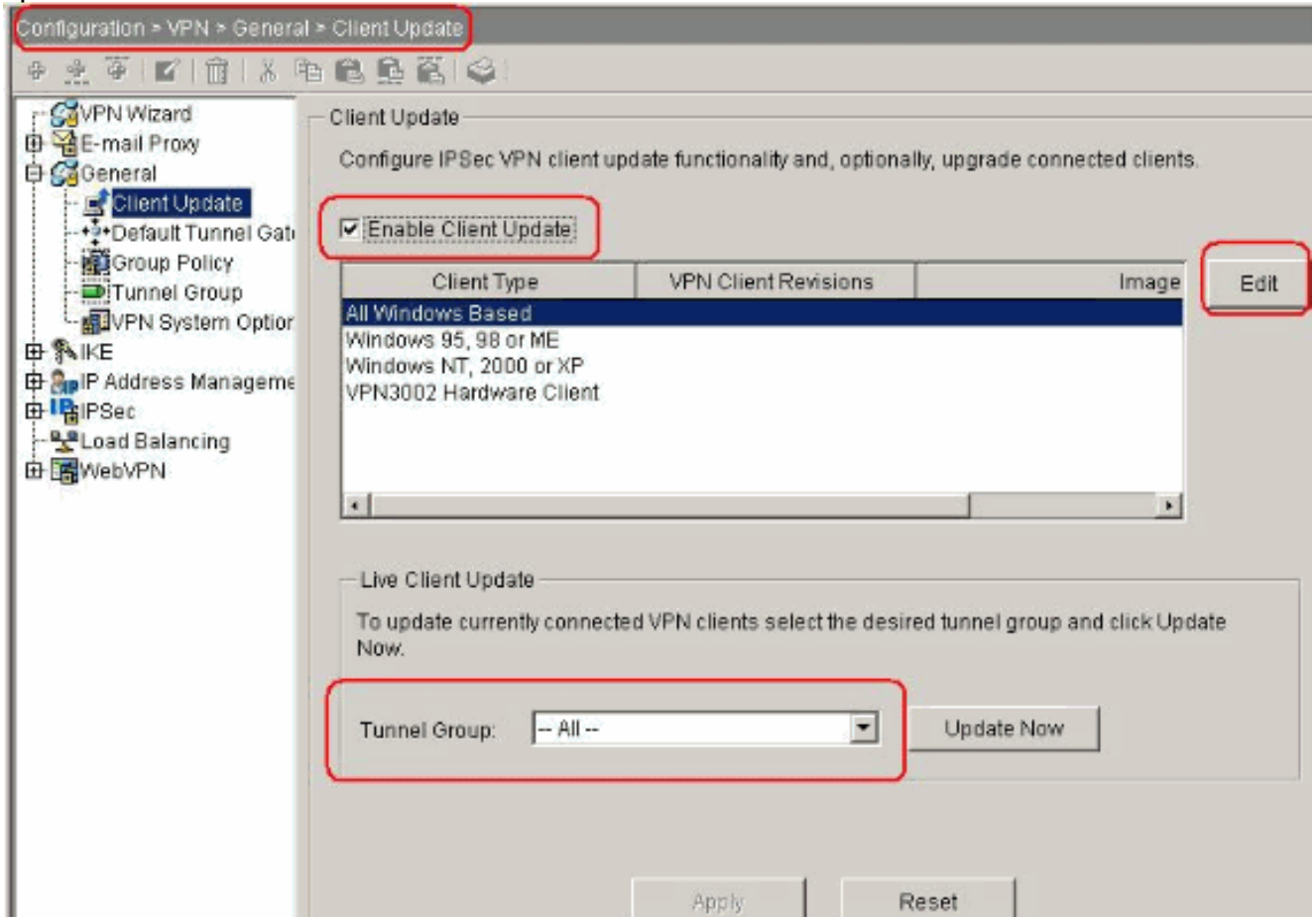
ASDM omvat twee soorten client-update: een die Windows klanten en VPN 3002 hardwarecliënten door een tunnelgroep ondersteunt, en de andere die ASA apparaten ondersteunt die fungeren als auto-update server.

Afstandsgebruikers kunnen verouderde VPN-software of hardwareclientversies gebruiken. U kunt op elk moment een client-update uitvoeren om deze functies te vervullen:

- Aanpassen van klantherzelingen inschakelen.
- Specificeer de types en revisienummers van de cliënten waarop de update van toepassing is.
- Geef een URL of IP adres op waaruit u de update wilt halen.
- Licht Windows client gebruikers op de hoogte dat ze hun VPN-clientversie zouden moeten bijwerken.
- Voor Windows clients kunt u een mechanisme voor gebruikers instellen om de update te realiseren.
- Voor VPN 3002 gebruikers van hardwareclients wordt de update automatisch doorgegeven, zonder dat er een melding wordt gedaan.

Voltooi deze stappen om een client-update te configureren:

1. Kies **Configuration > VPN > General > Client Update** om naar het client-update venster te gaan. Het venster Clientupdate wordt geopend. Controleer het aanvinkvakje **Clientupdate inschakelen** om de update van de client mogelijk te maken. Kies het type client waarop u de client-update wilt toepassen. De beschikbare clienttypen zijn **Alle Windows-gebaseerde, Windows 95, 98 of ME, Windows NT 4.0, 2000 of XP en VPN 3002-hardwareclient**. Als de client al een softwareversie in de lijst met revisienummers heeft uitgevoerd, hoeft deze niet bij te werken. Als de client geen softwareversie in de lijst heeft, moet deze worden bijgewerkt. U kunt maximaal drie van deze client-update-items instellen. De selectie Alle Windows gebaseerde opties bestrijkt alle toegestane Windows-platforms. Als u dit selecteert, specificeert u niet de afzonderlijke Windows-clienttypen. Klik op **Bewerken** om de acceptabele client-herzelingen en de bron voor de aangepaste software of firmware-afbeelding voor de client-update te specificeren.



2. Het venster Toegang tot client bewerken verschijnt en toont de selectie van het

clienttype.

3. Specificeer de client-update die u wilt toepassen op alle clients van het geselecteerde type in het gehele beveiligingsapparaat. Specificeer dan het type client, de URL of IP-adres waar u de geüpdatete afbeelding kunt verkrijgen, en het acceptabele nummer of de juiste nummers voor die client. U kunt maximaal vier herzieningsnummers instellen, gescheiden door komma's. Uw ingangen verschijnen in de juiste kolommen in de tabel in het venster Clientupgrade nadat u op **OK** klikt. Als het nummer van de klantbeoordeling overeenkomt met een van de gespecificeerde revisienummers, hoeft de client niet te worden bijgewerkt. **Opmerking:** Voor alle Windows-clients moet u het protocol `http://` of `https://` gebruiken als voorvoegsel voor de URL. Voor de VPN 3002 hardwareclient moet u in plaats daarvan protocol `tftp://` specificeren. Het initieert een client-update voor alle Windows clients voor een tunnelgroep met afstandsbediening ouder dan 4.6.1 en specificeert de URL voor het ophalen van de update als

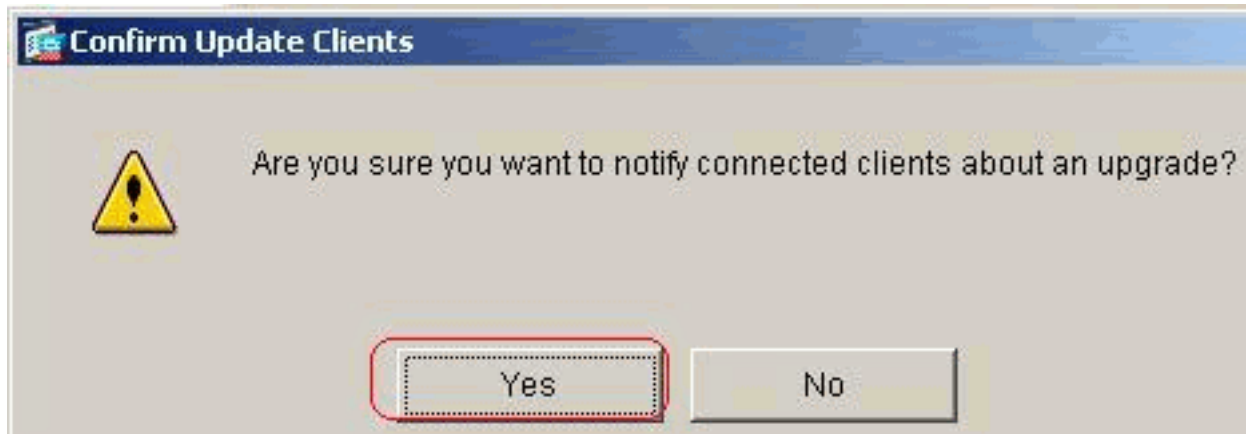
`https://support/updates.`

In plaats

hiervan kunt u ook client-update instellen voor afzonderlijke clienttypen, in plaats van voor alle Windows-clients, die u kunt zien als stap 1-c. VPN 3002-klienten werken bij zonder tussenkomst van de gebruiker en gebruikers ontvangen geen in kennisstellingsbericht. U kunt

de browser automatisch een toepassing laten starten als u de toepassingsnaam aan het eind van de URL opneemt; bijvoorbeeld : <https://support/updates/vpnclient.exe>.

4. Optioneel, kunt u een bericht naar actieve gebruikers met verouderde cliënten van Windows verzenden die hun client moeten bijwerken. Gebruik het gedeelte Live Client Update van het venster Client Update om deze kennisgeving te verzenden. Kies de tunnelgroep (of Alle) en klik op **Nu bijwerken**. Een dialoogvenster verschijnt in figuur en vraagt u te bevestigen dat u verbonden klanten over de upgrade wilt informeren.



De

aangewezen gebruikers zien een pop-up venster, dat hen de mogelijkheid biedt om een browser te lanceren en de bijgewerkte software te downloaden van de site die u in de URL hebt opgegeven. Het enige deel van dit bericht dat u kunt configureren is de URL. (Zie stappen 1-b of 1-c.) Gebruikers die niet actief zijn, krijgen de volgende keer dat ze inloggen een melding. Je kunt deze boodschap naar alle actieve klanten sturen op alle tunnelgroepen, of je kunt ze naar klanten sturen op een bepaalde tunnelgroep. Als het klant revisienummer overeenkomt met een van de gespecificeerde revisienummers, hoeft de client niet te worden bijgewerkt en wordt er geen melding naar de gebruiker verzonden. VPN 3002-klanten werken bij zonder tussenkomst van de gebruiker en gebruikers ontvangen geen in kennisstellingsbericht.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)