# ASA: Smart Tunnel met ASDM-configuratievoorbeeld

## Inhoud



## Inleiding

Een slimme tunnel is een verbinding tussen een TCP-gebaseerde toepassing en een privésite, waarbij een clientloze (op browser gebaseerde) SSL VPN-sessie met het security apparaat wordt gebruikt als route en het security apparaat als een proxy-server. U kunt toepassingen identificeren waarop u slimme tunneltoegang wilt verlenen en het lokale pad naar elke toepassing specificeren. Voor toepassingen die op Microsoft Windows lopen, kunt u ook een match van de SHA-1 hash van de checksum nodig hebben als voorwaarde voor het verlenen van slimme tunneltoegang.

*Lotus ZelfdeTime* en *Microsoft Outlook Express* zijn voorbeelden van toepassingen waaraan u slimme tunneltoegang wilt verlenen.

Afhankelijk van of de toepassing een client is of een web-enabled toepassing is, vereist slimme tunnelconfiguratie één van deze procedures:

- Maak een of meer slimme tunnellijsten van de clienttoepassingen en verdeel dan de lijst met groepsbeleid of lokaal gebruikersbeleid waarvoor u slimme tunneltoegang wilt bieden.
- Maak een of meer favoriet lijstingangen die de URLs van web-enabled toepassingen voor slimme tunneltoegang specificeren, en dan de lijst aan de DAP's, groepsbeleid, of lokaal

gebruikersbeleid toewijzen voor wie u slimme tunneltoegang wilt verlenen.U kunt ook een lijst maken van web-enabled toepassingen waarvoor de inlogaanmeldingsgegevens in slimme tunnelverbindingen via clientloze SSL VPN-sessies moeten worden geautomatiseerd.

Dit document gaat ervan uit dat de Cisco AnyConnect SSL VPN-clientconfiguratie al is gemaakt en correct werkt, zodat de slimme tunnelfunctie op de bestaande configuratie kan worden geconfigureerd. Raadpleeg ASA 8.x voor meer informatie over de manier waarop u Cisco AnyConnect SSL VPN-client kunt configureren: Split-tunneling voor AnyConnect VPN-client toestaan in het ASA Configuration-voorbeeld.

**Opmerking:** Controleer of de stappen *4.b t/m 4.l* die in het ASA-configuratie met ASDM 6.0(2) van de *ASA 8.x zijn* beschreven. *Toestaan dat Split Tunneling voor AnyConnect VPN-client wordt uitgevoerd in het ASA Configuration Voorbeeld* om de slimme tunnelfunctie te configureren.

Dit document beschrijft hoe u een slimme tunnel kunt configureren op Cisco ASA 5500 Series adaptieve 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 applicaties die softwareversie 8.0(2) uitvoeren
- PC die Microsoft Vista, Windows XP SP2 of Windows 2000 Professional SP4 met Microsoft Installer versie 3.1 uitvoert
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.0(2)

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.

# Achtergrondinformatie

## Smart Tunnel-toegangsconfiguratie

De slimme tunneltabel toont de slimme tunnellijsten, die elk een of meer toepassingen identificeren die in aanmerking komen voor slimme tunneltoegang en het bijbehorende besturingssysteem. Omdat elk groepsbeleid of lokaal gebruikersbeleid één slimme tunnellijst ondersteunt, moet u de niet-browser-gebaseerde toepassingen groeperen die in een slimme tunnellijst worden ondersteund. Na de configuratie van een lijst, kunt u deze toewijzen aan een of

meer groepsposten of lokaal gebruikersbeleid.

Met het **venster** Smart tunnels (**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnel**) kunt u deze procedures voltooien:

- **Voeg een slimme tunnellijst toe en voeg toepassingen toe aan de lijst**Voltooi deze stappen om een slimme tunnellijst toe te voegen en toepassingen aan de lijst toe te voegen:Klik op **Add** (Toevoegen).Het dialoogvenster Smart Tunnel lijst toevoegen verschijnt.Voer een naam in voor de lijst en klik op **Toevoegen**.ASDM opent het dialoogvenster Smart Tunnel-ingang toevoegen, waarmee u de eigenschappen van een slimme tunnel aan de lijst kunt toewijzen.Nadat u de gewenste eigenschappen voor de slimme tunnel toewijst, klik op **OK**.ASDM geeft deze eigenschappen in de lijst weer.Herhaal deze stappen zo nodig om de lijst te voltooien en klik vervolgens op **OK** in het dialoogvenster Smart Tunnel lijst toevoegen.
- **Een slimme tunnellijst wijzigen**Voltooi deze stappen om een slimme tunnellijst te wijzigen:Dubbelklik op de lijst of kies de lijst in de tabel en klik op **Bewerken**.Klik op **Add** om een nieuwe set slimme tunneleigenschappen in de lijst toe te voegen of een ingang in de lijst te kiezen en klik op **Bewerken** of **Verwijderen**.
- **Een lijst verwijderen**Selecteer de lijst in de tabel en klik op **Verwijderen** om een lijst te verwijderen.
- **Een favoriet toevoegen**Na het configureren en toewijzen van een slimme tunnellijst kunt u een slimme tunnel makkelijk gebruiken maken door een favoriet voor de service toe te voegen en op de optie **Smart Tunnel** inschakelen in het dialoogvenster Woordenboek toevoegen of bewerken te klikken.

Smart tunnel toegang geeft een client-TCP-gebaseerde toepassing om een browser-gebaseerde VPN verbinding te gebruiken om verbinding te maken met een service. Het biedt de volgende voordelen voor de gebruikers, in vergelijking met de stekkers en de erfenis technologie, het doorsturen van havens:

- Smart-tunnel biedt betere prestaties dan plug-ins.
- In tegenstelling tot port expediteur, vereenvoudigt slimme tunnel de gebruikerservaring door niet de gebruikersverbinding van de lokale toepassing naar de lokale poort te vereisen.
- In tegenstelling tot poorttransport, vereist slimme tunnel geen gebruikers om beheerrechten te hebben.

# Smart Tunnel-vereisten, beperkingen en beperkingen

## Algemene vereisten en beperkingen

Smart-tunnel heeft de volgende algemene vereisten en beperkingen:

- De afstandsbediening van de slimme tunnel moet een 32-bits versie van Microsoft Windows Vista, Windows XP of Windows 2000 uitvoeren. of Mac OS 10.4 of 10.5.
- Smart tunnel auto-aanmelding ondersteunt alleen Microsoft Internet Explorer op Windows.
- De browser moet zijn ingeschakeld met Java, Microsoft ActiveX of beide.
- Smart tunnel ondersteunt alleen proxy's die worden geplaatst tussen computers die Microsoft Windows en het security apparaat besturen. Smart-tunnel gebruikt de configuratie van Internet Explorer (dat wil zeggen, de configuratie die is bedoeld voor systeembreed gebruik in Windows). Als de externe computer een proxy-server nodig heeft om het security apparaat te

bereiken, moet de URL van het einde van de verbinding voorkomen in de lijst met URL's die van proxy-services zijn uitgesloten. Als de proxy-configuratie aangeeft dat het voor de ASA bestemde verkeer door een proxy gaat, gaat al het slimme tunnelverkeer door de proxy.In een op HTTP gebaseerd ver-toegangsscenario, soms geeft een netwerk geen gebruikers toegang tot de VPN gateway. In dit geval biedt een proxy die voor de ASA is geplaatst om verkeer tussen het web en de locatie van de eindgebruiker te routeren, toegang tot het web. Alleen VPN-gebruikers kunnen echter proxy's configureren die voor de ASA zijn geplaatst. Wanneer u dit doet, moeten ze ervoor zorgen dat deze proxy's de CONNECT-methode ondersteunen. Voor proxy's die verificatie vereisen, ondersteunt slimme tunnel alleen het basistype van grootste authenticatie.
- Wanneer een slimme tunnel begint, tunnels de veiligheidsmachine al verkeer van de browser het proces dat de gebruiker gebruikt om de clientloze sessie te initiëren. Als de gebruiker een ander exemplaar van het zoekproces start, geeft het al het verkeer door naar de tunnel. Als het zoekproces hetzelfde is en het beveiligingsapparaat geen toegang geeft tot een bepaalde URL, kan de gebruiker het niet openen. Als een werkruimte kan de gebruiker een andere browser gebruiken dan die gebruikt wordt om de clientloze sessie te maken.
- Een stateful failover behoudt geen slimme tunnelverbindingen. De gebruikers moeten na een failover opnieuw verbinden.

## Windows-vereisten en -beperkingen

De volgende vereisten en beperkingen gelden alleen voor Windows:

- Alleen Winsock 2, TCP-gebaseerde toepassingen komen in aanmerking voor slimme tunneltoegang.
- Het security apparaat ondersteunt de Microsoft Outlook Exchange (MAPI)-proxy niet. Noch havenverzending noch de slimme tunnel ondersteunt MAPI. Voor Microsoft Outlook Exchange-communicatie met het MAPI-protocol moeten externe gebruikers AnyConnect gebruiken.
- Gebruikers van Microsoft Windows Vista die slimme tunnels of poortverzending gebruiken moeten de URL van de ASA aan de Trusted Site zone toevoegen. Om toegang tot de Trusted Site-zone te krijgen, start u Internet Explorer en kies **Gereedschappen > Internet-opties** en klik vervolgens op het tabblad **Beveiliging**. Vista-gebruikers kunnen de beschermde modus ook uitschakelen om slimme tunneltoegang te vergemakkelijken; echter, adviseert Cisco tegen deze methode omdat het kwetsbaarheid voor aanvallen verhoogt.

## Mac OS-vereisten en -beperkingen

Deze vereisten en beperkingen gelden alleen voor Mac OS:

- Safari 3.1.1 of hoger of Firefox 3.0 of hoger
- Sun JRE 1.5 of hoger
- Alleen toepassingen die vanaf de portal-pagina zijn gestart, kunnen slimme tunnelverbindingen maken. Dit vereiste omvat slimme tunnelondersteuning voor Firefox. Het gebruik van Firefox om een ander exemplaar van Firefox te starten tijdens het eerste gebruik van een slimme tunnel vereist het gebruikersprofiel dat csco_st heet. Als dit gebruikersprofiel niet aanwezig is, wordt de gebruiker gevraagd er een te maken.
- Toepassingen die TCP gebruiken die dynamisch verbonden zijn met de SSL bibliotheek

kunnen werken via een slimme tunnel.
- Smart tunnel ondersteunt deze functies en toepassingen niet op Mac OS:ProxyservicesAutomatische aanmeldingToepassingen die naamruimtes van twee niveaus gebruikenOp console gebaseerde toepassingen, zoals telnet, SSH en cURLToepassingen die gebruik maken van lopen of slymsystemen om libsocket-oproepen te vindenStatisch verbonden toepassingen om libsocket-oproepen te vinden

# Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

## Smart Tunnel lijst toevoegen of bewerken

Met het dialoogvenster Smart Tunnel lijst toevoegen kunt u een lijst met slimme tunnelitems toevoegen aan de configuratie van het security apparaat. Met het dialoogvenster Smart Tunnel lijst bewerken kunt u de inhoud van de lijst wijzigen.

**Veld**

**Lijstnaam** - Voer een unieke naam in voor de lijst met toepassingen of programma's. Er is geen beperking op het aantal tekens in de naam. Gebruik geen spaties. Na de configuratie van de slimme tunnellijst verschijnt de lijstnaam naast de eigenschap Smart Tunnel List in het groepsbeleid van Clientless SSL VPN en het lokale gebruikersbeleid. Wijs een naam toe die u zal helpen om zijn inhoud of doel van andere lijsten te onderscheiden die u waarschijnlijk zult vormen.

## Smart Tunnel-ingang toevoegen of bewerken

Met het dialoogvenster Smart Tunnel-invoer toevoegen of bewerken kunt u de eigenschappen van een toepassing in een slimme tunnellijst specificeren.

- **Application ID** - Voer een string in om de ingang in de slimme tunnellijst te noemen. De string is uniek voor het OS. Meestal noemt het de toepassing die slimme tunneltoegang krijgt. Om meerdere versies van een toepassing te ondersteunen waarvoor u kiest om verschillende paden of haswaarden te specificeren, kunt u deze eigenschap gebruiken om items te differentiëren, terwijl u het besturingssysteem en de naam en versie van de toepassing specificeert die door elke lijstingang worden ondersteund. De string kan maximaal 64 tekens bevatten.
- **Procesnaam** - Voer de bestandsnaam of het pad naar de toepassing in. De string kan maximaal 128 tekens bevattenWindows vereist een exacte match van deze waarde aan de rechterkant van het toepassingspad op de afstandshost om de toepassing voor slimme tunneltoegang in aanmerking te nemen. Als u alleen de bestandsnaam voor Windows specificeert, dwingt SSL VPN geen locatiebeperking op de externe host om de toepassing voor slimme tunneltoegang te kwalificeren.Als u een pad hebt opgegeven en de gebruiker de toepassing op een andere locatie heeft geïnstalleerd, kwalificeert die toepassing niet. De toepassing kan op elk pad blijven staan zolang de rechterkant van de string overeenkomt met de waarde die u ingeeft.Om een toepassing voor slimme tunneltoegang toe te staan indien deze op één van meerdere paden op de afstandsbediening aanwezig is, specificeert u alleen

de naam en de uitbreiding van de toepassing in dit veld of creëert u een unieke slimme tunnelingang voor elk pad.Als u voor Windows slimme tunneltoegang wilt toevoegen aan een toepassing die vanaf de opdrachtmelding is gestart, moet u "cmd.exe" in de procesnaam van een ingang in de lijst van slimme tunnels specificeren en het pad naar de toepassing zelf in een andere ingang specificeren, omdat "cmd.exe" de ouder van de toepassing is.Mac OS vereist het volledige pad naar het proces en is hoofdlettergevoelig. Om te voorkomen dat een pad voor elke gebruikersnaam wordt opgegeven, invoegt u een tilde (~) vóór het gedeeltelijke pad (bijvoorbeeld ~/bin/vnc).

- **OS**-Klik op Windows of Mac om het host OS van de toepassing te specificeren.
- **Hassen** — (*Optioneel en alleen van toepassing voor Windows*) Om deze waarde te verkrijgen, voert u de checksum van het uitvoerbare bestand in een voorziening die een hash berekent met het SHA-1 algoritme. Een voorbeeld van een dergelijke toepassing is de Microsoft File Checksum Integrity Verifier (FCIV), die beschikbaar is bij Beschikbaarheid en beschrijving van het File Checksum Integrity Verifier-hulpprogramma. Nadat u FCIV hebt geïnstalleerd, plaatst u een tijdelijk exemplaar van de toepassing die op een pad wordt gehashed dat geen spaties bevat (bijvoorbeeld c:/fciv.exe), en voert u fciv.exe-sha1 toepassing in op de opdrachtregel (bijvoorbeeld fciv.exe-sha1 c:\msimn.exe) om de SHA-1 hash weer te geven.De SHA-1 hash is altijd 40 hexadecimale tekens.Alvorens een toepassing voor slimme tunneltoegang toe te staan, berekent clientloze SSL VPN de hash van de toepassing die de toepassing-ID aansluit. Het kwalificeert de toepassing voor slimme tunneltoegang als het resultaat overeenkomt met de waarde van hash.Het invoeren van een hash geeft een redelijke garantie dat SSL VPN geen ongeldig bestand kwalificeert dat overeenkomt met de string die u in de applicatie-ID hebt gespecificeerd. Omdat de checksum varieert met elke versie of elk onderdeel van een toepassing, kan de hash die u ingeeft, slechts één versie of een pleister op de afstandsbediening overeenkomen. Om een hash voor meer dan één versie van een toepassing te specificeren, kunt u een unieke slimme tunnelingang maken voor elke hashwaarde.**Opmerking:** U moet de lijst met slimme tunnels in de toekomst bijwerken als u haswaarden invoert en u toekomstige versies of patches van een toepassing wilt ondersteunen met slimme tunneltoegang. Een plotseling probleem met slimme tunneltoegang kan een indicatie zijn dat de toepassing die haswaarden bevat niet up-to-date is met een applicatie upgrade. U kunt dit probleem voorkomen door geen hash in te voeren.
- Zodra u de lijst met slimme tunnels configureren moet u deze toewijzen aan een groepsbeleid of een lokaal gebruikersbeleid zodat deze als volgt actief wordt:Als u de lijst aan een groepsbeleid wilt toewijzen, kiest u **Config > Remote Access VPN > Clientloze SSL VPN-toegang > Groepsbeleid > Add of Bewerken > Portal**, en kiest u de slimme tunnelnaam uit de vervolgkeuzelijst naast het kenmerk Smart Tunnel List.Als u de lijst aan een lokaal gebruikersbeleid wilt toewijzen, kiest u **Config > Remote Access VPN> AAA-instellingen > Local Gebruikers > Add of werken > VPN-beleid > Clientless SSL VPN** en kiest u de naam van de slimme tunnel uit de vervolgkeuzelijst naast het kenmerk Smart Tunnel List.

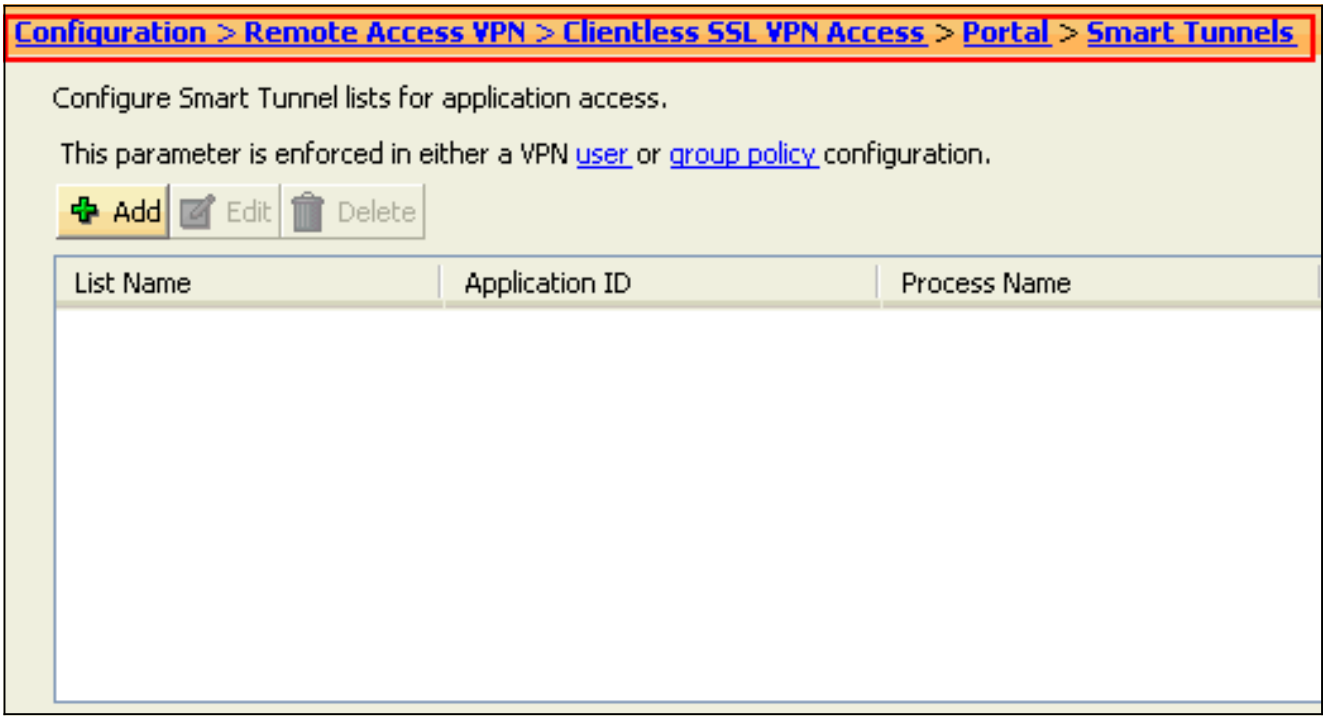
## ASA Smart Tunnel (Lotus Voorbeeld) configuratie met ASDM 6.0(2)

Dit document is gebaseerd op de veronderstelling dat de basisconfiguratie, zoals de interfaceconfiguratie, volledig is en correct werkt.

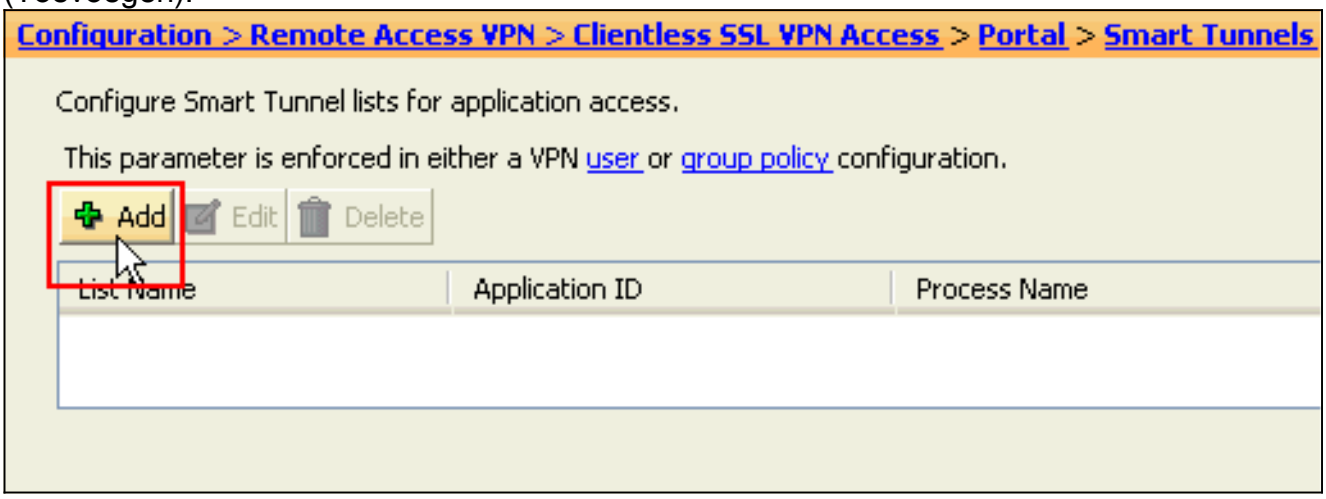
Voltooi deze stappen om een slimme tunnel te configureren:

**Opmerking:** In dit configuratievoorbeeld is de slimme tunnel ingesteld voor de Lotus applicatie.

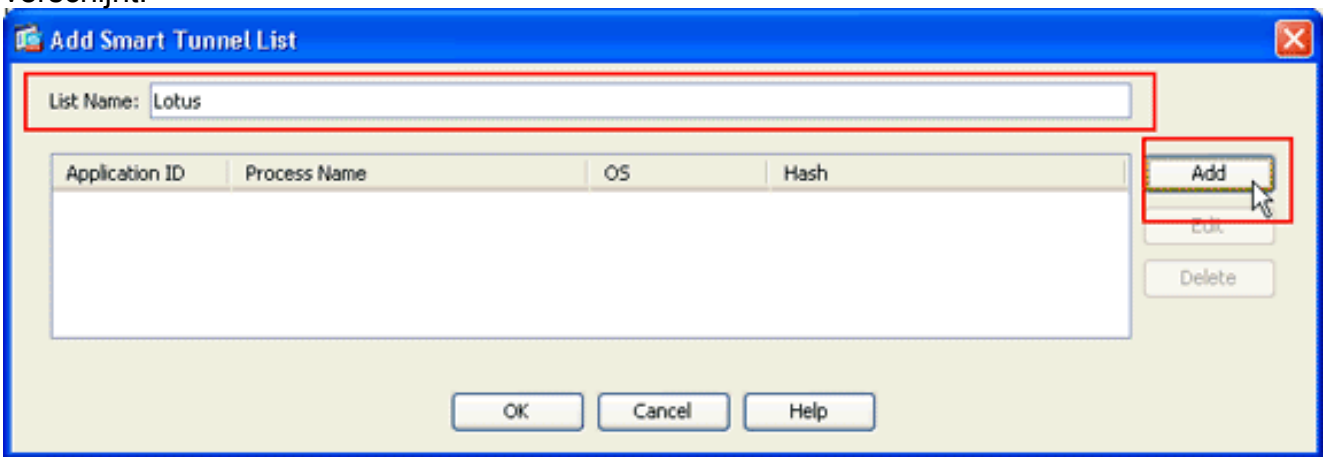
1. Kies **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnel** om de Smart Tunnel-configuratie te starten.



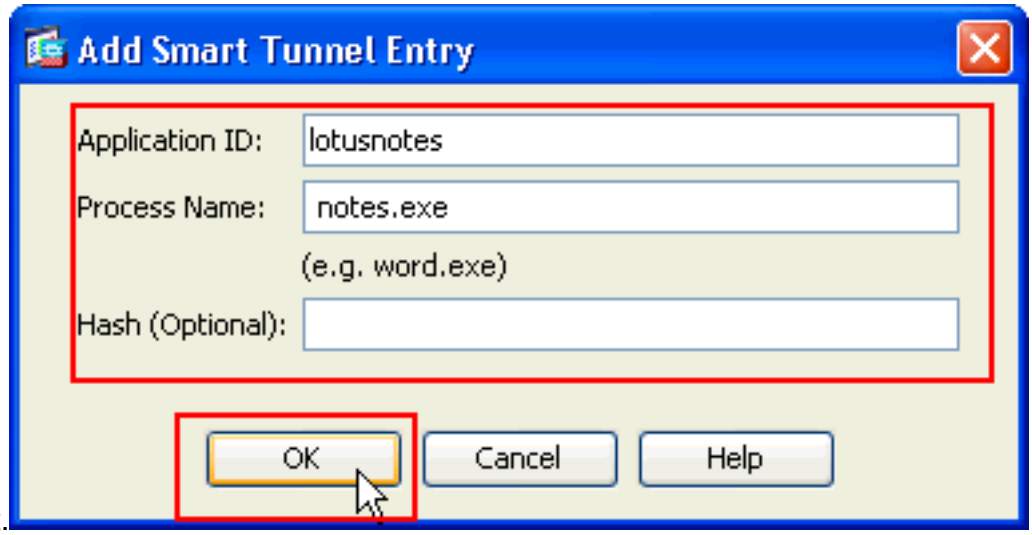

2. Klik op **Add** (Toevoegen).




Het dialoogvenster Smart Tunnel lijst toevoegen verschijnt.

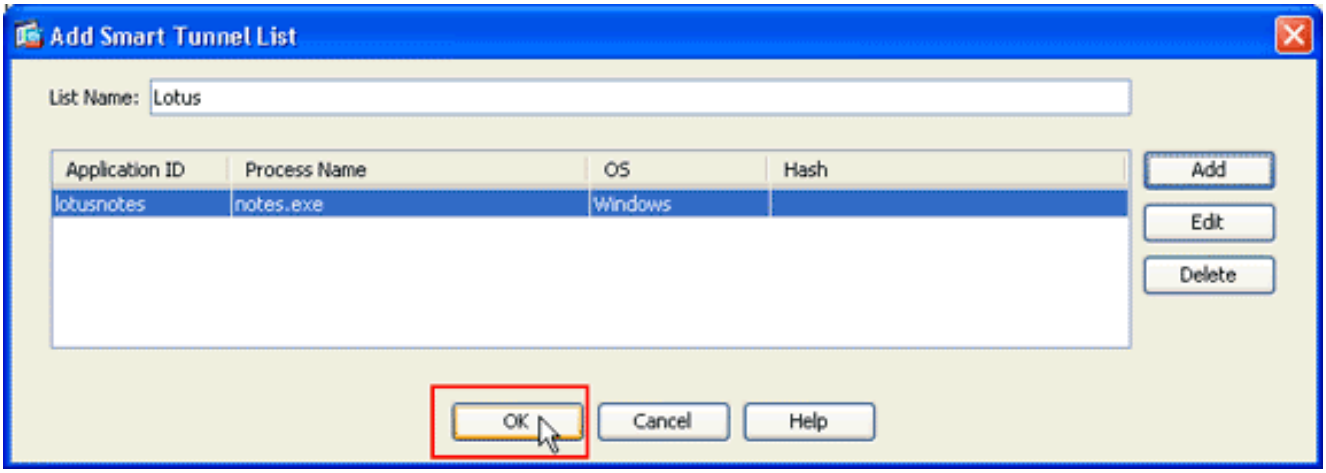



3. Klik in het dialoogvenster Smart Tunnel lijst toevoegen op **Toevoegen**.Het dialoogvenster Smart Tunnel invoeren



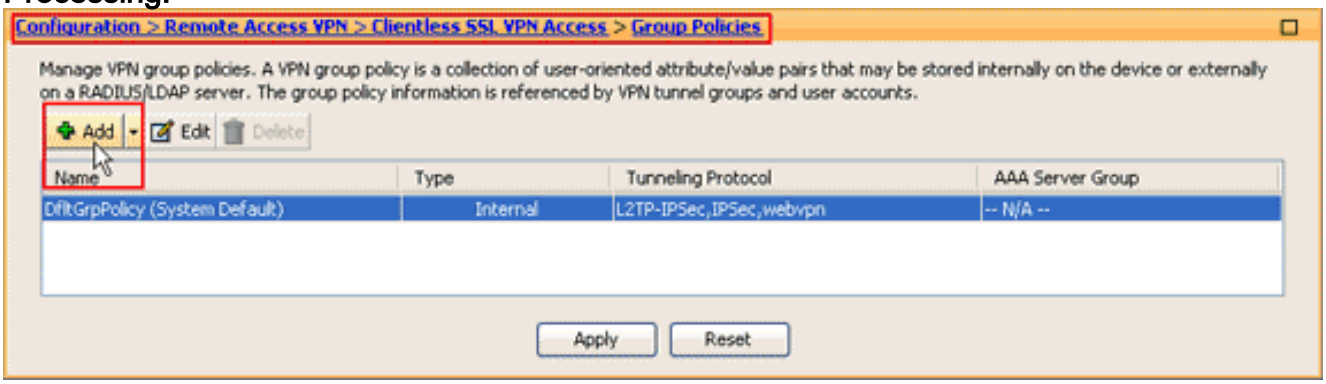

verschijnt.

4. Voer in het veld Application ID een string in om de vermelding in de lijst met slimme tunnels te identificeren.
5. Voer een bestandsnaam en -uitbreiding voor de toepassing in en klik op **OK**.
6. Klik in het dialoogvenster Smart Tunnel lijst toevoegen op **OK**.

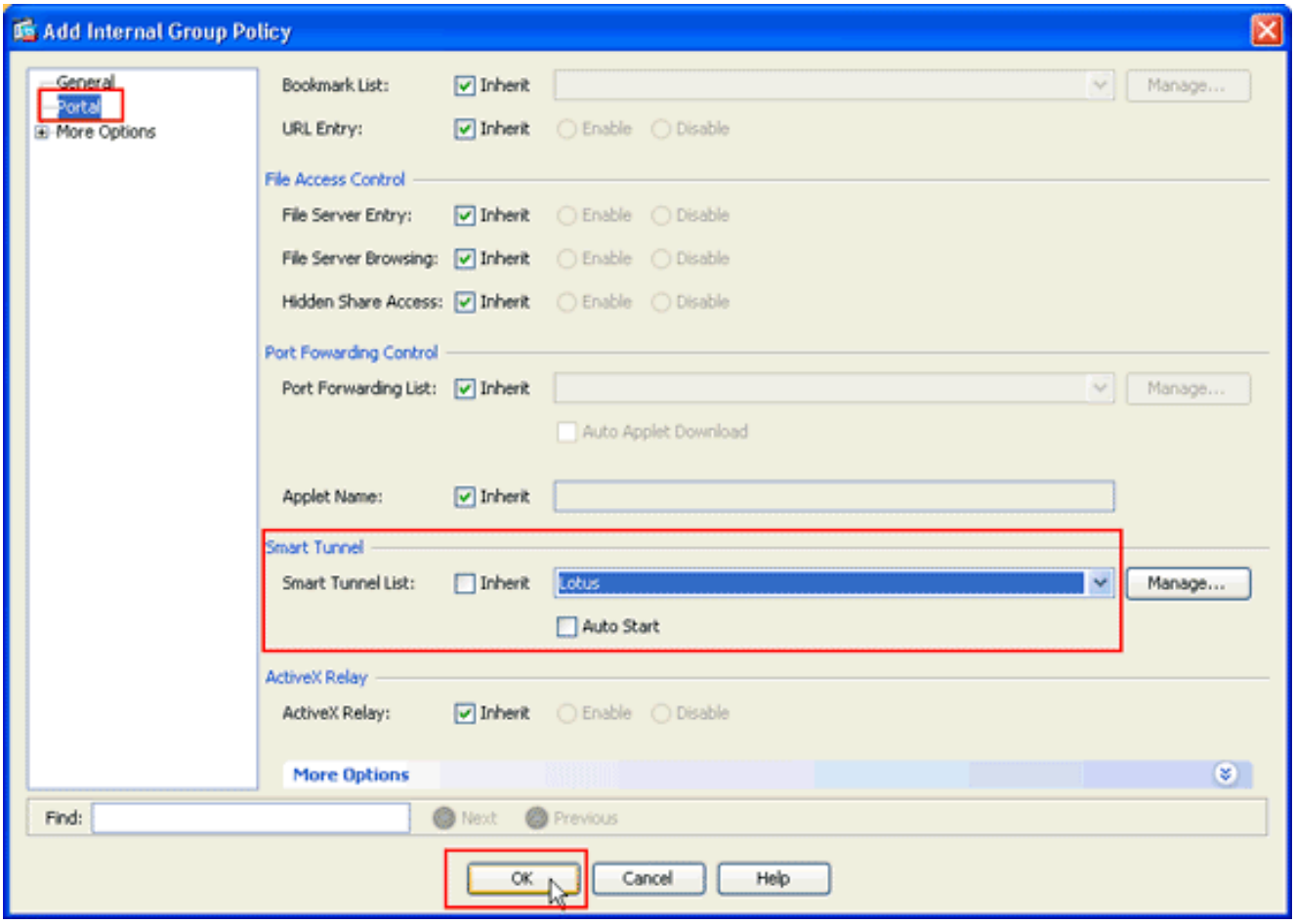



**Opmerking:** Hier is de equivalente CLI configuratie opdracht:

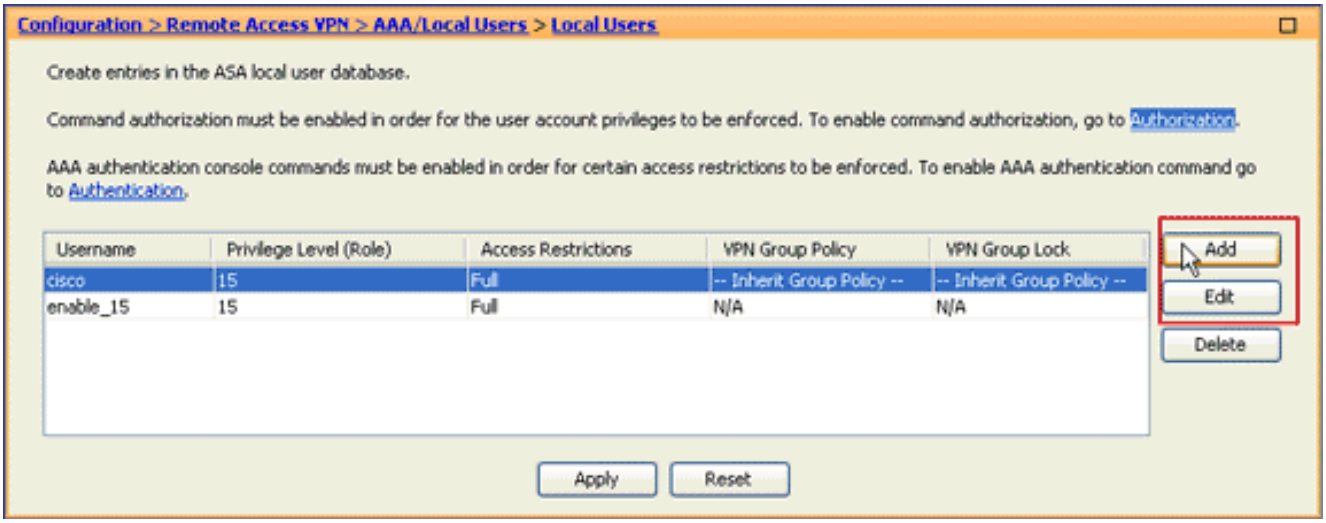
7. Pas de lijst aan het groepsbeleid en het lokale gebruikersbeleid toe waaraan u slimme tunneltoegang tot de bijbehorende toepassingen wilt verlenen:Als u de lijst aan een groepsbeleid wilt toewijzen, kiest u **Configuration > Remote Access VPN> Clientloze SSL VPN Access > Group Policy** en vervolgens klikt u op **Add** of **Processing.**



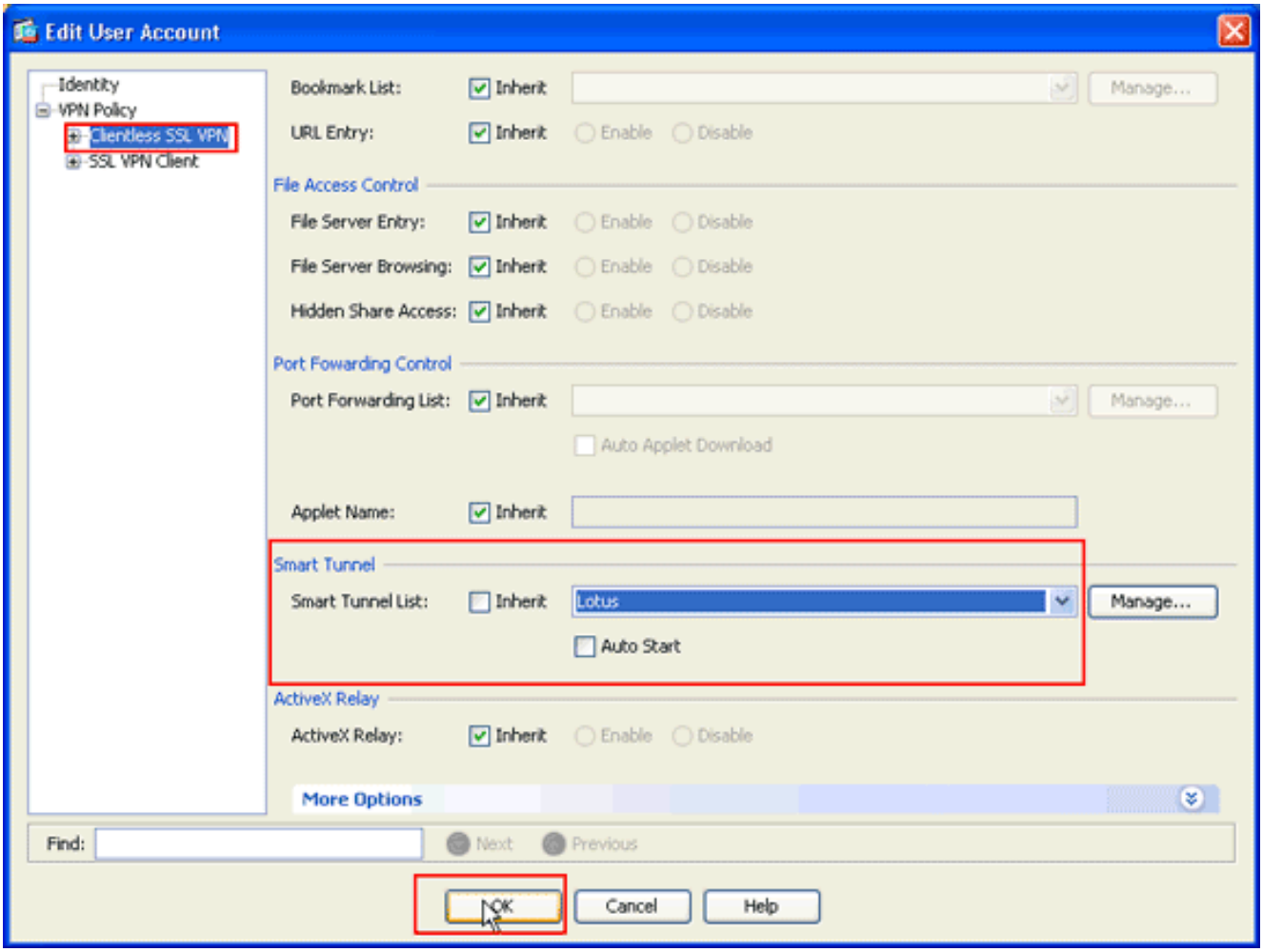

Het dialoogvenster Intern groepsbeleid toevoegen verschijnt.




8. In het dialoogvenster Intern groepsbeleid toevoegen klikt u op **Portal**, kiest u de naam van de slimme tunnel uit de vervolgkeuzelijst Smart Tunnel Lijst en vervolgens klikt u op **OK**.**Toelichting:** Dit voorbeeld gebruikt *Lotus* als de naam van de slimme tunnellijst.
9. Als u de lijst aan een lokaal gebruikersbeleid wilt toewijzen, kiest u **Configuration > Remote Access VPN> AAA-instelling > Local Gebruikers** en klikt u op **Add** om een nieuwe gebruiker te configureren of klikt u op **Bewerken** om een bestaande gebruiker te bewerken.




Het dialoogvenster Gebruikersaccount bewerken verschijnt.




10. In het dialoogvenster Gebruikersaccount bewerken klikt u op **Clientless SSL VPN**, kiest u de naam van de slimme tunnellijst in de vervolgkeuzelijst Smart Tunnel List en vervolgens klikt u op **OK**.**Toelichting:** Dit voorbeeld gebruikt *Lotus* als de naam van de slimme tunnellijst.

De slimme tunnelconfiguratie is compleet.

# Problemen oplossen

## Ik kan geen verbinding maken met een gemarkeerde Smart Tunnel URL in het clientloze portaal. Waarom gebeurt dit probleem en hoe kan ik het oplossen?

Dit probleem is een gevolg van het probleem dat in Cisco Bug ID CSCsx05766 **(alleen** geregistreerde **klanten)** is beschreven. Om dit probleem op te lossen, dient u de Java-Runtime plug-in te downloaden naar een oudere versie.

## Kan ik de URL van een slimme tunnellink in WebVPN vergarderen?

Wanneer een slimme tunnel op de ASA wordt gebruikt, kunt u de URL niet verven of de adresbalk van de browser verbergen. Gebruikers kunnen de URL's bekijken van links die in WebVPN zijn geconfigureerd die slimme tunnel gebruiken. Als resultaat hiervan kunnen ze de poort wijzigen en toegang krijgen tot de server voor een andere service.

Gebruik WebType ACL’s om dit probleem op te lossen. Raadpleeg Webex Access Control Lists voor meer informatie.

## Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- SSL VPN-client (SVC) op ASA met ASDM Configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems