ASA: Smart Tunnel mit ASDM-Konfigurationsbeispiel

Inhalt

Einführung

Ein intelligenter Tunnel ist eine Verbindung zwischen einer TCP-basierten Anwendung und einer privaten Site, die eine clientlose (browserbasierte) SSL VPN-Sitzung mit der Sicherheits-Appliance als Pfad und der Sicherheits-Appliance als Proxy-Server verwendet. Sie können Anwendungen identifizieren, für die Sie Smart Tunnel-Zugriff gewähren möchten, und für jede Anwendung den lokalen Pfad angeben. Für Anwendungen, die unter Microsoft Windows ausgeführt werden, können Sie auch eine Übereinstimmung des SHA-1-Hashs der Prüfsumme als Bedingung für die Gewährung des Zugriffs auf intelligente Tunnel benötigen.

Lotus SameTime und *Microsoft Outlook Express* sind Beispiele für Anwendungen, für die Sie möglicherweise Smart Tunnel-Zugriff gewähren möchten.

Je nachdem, ob es sich bei der Anwendung um einen Client oder um eine webfähige Anwendung handelt, ist für die Smart Tunnel-Konfiguration eine der folgenden Verfahren erforderlich:

- Erstellen Sie eine oder mehrere Smart Tunnel-Listen der Client-Anwendungen, und weisen Sie diese Liste dann den Gruppenrichtlinien oder lokalen Benutzerrichtlinien zu, für die Sie Smart Tunnel-Zugriff bereitstellen möchten.

- Erstellen Sie einen oder mehrere Lesezeichenlisteneinträge, die die URLs der für den Smart Tunnel-Zugriff berechtigten webfähigen Anwendungen angeben, und weisen Sie die Liste dann den DAPs, Gruppenrichtlinien oder lokalen Benutzerrichtlinien zu, für die Sie den Zugriff auf Smart Tunnel bereitstellen möchten.Sie können auch webaktivierte Anwendungen auflisten, mit denen die Übermittlung von Anmeldeinformationen bei Smart-Tunnel-Verbindungen über clientlose SSL VPN-Sitzungen automatisiert werden kann.

In diesem Dokument wird davon ausgegangen, dass die Konfiguration des Cisco AnyConnect SSL VPN Client bereits vorgenommen wurde und ordnungsgemäß funktioniert, sodass die Smart Tunnel-Funktion in der vorhandenen Konfiguration konfiguriert werden kann. Weitere Informationen zur Konfiguration des Cisco AnyConnect SSL VPN-Clients finden Sie unter ASA 8.x: Zulassen von Split Tunneling für den AnyConnect VPN-Client im ASA-Konfigurationsbeispiel.

Hinweis: Stellen Sie sicher, dass die Schritte *4.b bis 4.l* im Abschnitt "ASA-Konfiguration mit ASDM 6.0(2)" der *ASA 8.x* beschrieben sind*: Split Tunneling für AnyConnect VPN-Client zulassen im ASA-Konfigurationsbeispiel* wird nicht ausgeführt, um die Smart-Tunnel-Funktion zu konfigurieren.

Dieses Dokument beschreibt die Konfiguration von Smart Tunnels auf Adaptive Security Appliances der Serie Cisco ASA 5500.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Softwareversion 8.0(2)
- PC, auf dem Microsoft Vista, Windows XP SP2 oder Windows 2000 Professional SP4 mit Microsoft Installer Version 3.1 ausgeführt wird
- Cisco Adaptive Security Device Manager (ASDM) Version 6.0(2)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Hintergrundinformationen

Konfiguration des Smart Tunnel-Zugriffs

Die Smart Tunnel-Tabelle zeigt die Smart Tunnel-Listen an, die jeweils eine oder mehrere für den Smart Tunnel-Zugriff berechtigte Anwendungen und das zugehörige Betriebssystem (OS) identifizieren. Da jede Gruppenrichtlinie oder lokale Benutzerrichtlinie eine Smart Tunnel-Liste unterstützt, müssen Sie die nicht browserbasierten Anwendungen, die unterstützt werden sollen, in einer Smart Tunnel-Liste gruppieren. Nach der Konfiguration einer Liste können Sie diese einer oder mehreren Gruppenrichtlinien oder lokalen Benutzerrichtlinien zuweisen.

Im Fenster "Smart Tunnels" (**Konfiguration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**) können Sie folgende Schritte ausführen:

- **Hinzufügen einer Smart Tunnel-Liste und Hinzufügen von Anwendungen zur Liste**Gehen Sie wie folgt vor, um eine Smart-Tunnel-Liste hinzuzufügen und Anwendungen zur Liste hinzuzufügen:Klicken Sie auf **Hinzufügen**.Das Dialogfeld "Smart Tunnel-Liste hinzufügen" wird angezeigt.Geben Sie einen Namen für die Liste ein, und klicken Sie auf **Hinzufügen**.ASDM öffnet das Dialogfeld Add Smart Tunnel Entry (Smart-Tunnel-Eintrag hinzufügen), in dem Sie der Liste die Attribute eines Smart-Tunnels zuweisen können.Nachdem Sie die gewünschten Attribute für den Smart Tunnel zugewiesen haben, klicken Sie auf **OK**.ASDM zeigt diese Attribute in der Liste an.Wiederholen Sie diese Schritte, um die Liste abzuschließen, und klicken Sie dann im Dialogfeld "Smart Tunnel-Liste hinzufügen" auf **OK**.
- **Smart Tunnel-Liste ändern**Gehen Sie wie folgt vor, um eine Smart Tunnel-Liste zu ändern:Doppelklicken Sie auf die Liste, oder wählen Sie die Liste in der Tabelle aus, und klicken Sie auf **Bearbeiten**.Klicken Sie auf **Hinzufügen**, um eine neue Gruppe von Smart Tunnel-Attributen in die Liste einzufügen, oder wählen Sie einen Eintrag in der Liste aus, und klicken Sie dann auf **Bearbeiten** oder **Löschen**.
- **Liste entfernen**Um eine Liste zu entfernen, wählen Sie die Liste in der Tabelle aus, und klicken Sie auf **Löschen**.
- **Lesezeichen hinzufügen**Nach der Konfiguration und Zuweisung einer Smart-Tunnel-Liste können Sie einen Smart-Tunnel leicht verwenden, indem Sie ein Lesezeichen für den Dienst hinzufügen und im Dialogfeld Lesezeichen hinzufügen oder bearbeiten auf die Option **Smart-Tunnel aktivieren** klicken.

Beim Zugriff über einen Smart Tunnel kann eine TCP-basierte Client-Anwendung eine browserbasierte VPN-Verbindung verwenden, um eine Verbindung zu einem Dienst herzustellen. Im Vergleich zu Plug-Ins und der Legacy-Technologie bietet sie den Benutzern die folgenden Vorteile: Port Forwarding:

- Smart Tunnel bietet eine bessere Leistung als Plug-Ins.
- Anders als bei der Port-Weiterleitung vereinfacht Smart Tunnel die Benutzererfahrung, da keine Benutzerverbindung der lokalen Anwendung mit dem lokalen Port erforderlich ist.
- Im Gegensatz zur Port Forwarding benötigen Benutzer für Smart Tunnel keine Administratorrechte.

Anforderungen, Einschränkungen und Einschränkungen für Smart Tunnel

Allgemeine Anforderungen und Einschränkungen

Für Smart Tunnel gelten die folgenden allgemeinen Anforderungen und Einschränkungen:

- Der Remotehost, der den Smart Tunnel auslöst, muss eine 32-Bit-Version von Microsoft Windows Vista, Windows XP oder Windows 2000 ausführen. oder Mac OS 10.4 oder 10.5.
- Die automatische Smart Tunnel-Anmeldung unterstützt nur Microsoft Internet Explorer unter Windows.
- Der Browser muss mit Java, Microsoft ActiveX oder mit beiden aktiviert sein.
- Smart Tunnel unterstützt nur Proxys zwischen Computern, auf denen Microsoft Windows ausgeführt wird, und der Sicherheits-Appliance. Smart Tunnel verwendet die Internet Explorer-Konfiguration (d. h. die Konfiguration, die für die systemweite Verwendung in Windows vorgesehen ist). Wenn der Remote-Computer einen Proxyserver benötigt, um die Sicherheits-Appliance zu erreichen, muss die URL des terminierenden Endes der Verbindung in der Liste der URLs enthalten sein, die von den Proxydiensten ausgeschlossen sind. Wenn die Proxy-Konfiguration angibt, dass der für die ASA bestimmte Datenverkehr einen Proxy durchläuft, durchläuft der gesamte Smart Tunnel-Datenverkehr den Proxy.In einem HTTP-basierten Remote-Zugriffsszenario bietet ein Subnetz manchmal keinen Benutzerzugriff auf das VPN-Gateway. In diesem Fall stellt ein Proxy, der vor der ASA platziert wird, um Datenverkehr zwischen dem Internet und dem Standort des Endbenutzers zu routen, den Webzugriff bereit. Jedoch können nur VPN-Benutzer Proxys konfigurieren, die vor der ASA angeordnet sind. Dabei müssen sie sicherstellen, dass diese Proxys die CONNECT-Methode unterstützen. Für Proxys, die eine Authentifizierung erfordern, unterstützt Smart Tunnel nur den Standardauthentifizierungstyp Digest.
- Beim Start des Smart Tunnels tunnelt die Sicherheits-Appliance den gesamten Datenverkehr aus dem Browserprozess, den der Benutzer zum Initiieren der clientlosen Sitzung verwendet hat. Wenn der Benutzer eine andere Instanz des Browserprozesses startet, wird der gesamte Datenverkehr an den Tunnel weitergeleitet. Wenn der Browserprozess derselbe ist und die Sicherheits-Appliance keinen Zugriff auf eine bestimmte URL bietet, kann der Benutzer diese nicht öffnen. Als Problemumgehung kann der Benutzer einen anderen Browser verwenden als den, der zum Einrichten der clientlosen Sitzung verwendet wird.
- Ein Stateful Failover behält keine Smart Tunnel-Verbindungen bei. Nach einem Failover muss die Verbindung wieder hergestellt werden.

Windows-Anforderungen und -Einschränkungen

Die folgenden Anforderungen und Einschränkungen gelten nur für Windows:

- Nur Winsock 2-, TCP-basierte Anwendungen sind für den Zugriff auf Smart Tunnels qualifiziert.
- Die Sicherheits-Appliance unterstützt den Microsoft Outlook Exchange-Proxy (MAPI) nicht. Weder Port Forwarding noch Smart Tunnel unterstützen MAPI. Für die Kommunikation mit Microsoft Outlook Exchange mithilfe des MAPI-Protokolls müssen Remote-Benutzer AnyConnect verwenden.
- Benutzer von Microsoft Windows Vista, die Smart Tunnel oder Port Forwarding verwenden, müssen die URL der ASA zur Zone für vertrauenswürdige Standorte hinzufügen. Um auf die Zone Vertrauenswürdige Site zuzugreifen, starten Sie Internet Explorer, wählen **Extras > Internetoptionen**, und klicken Sie auf die Registerkarte **Sicherheit**. Vista-Benutzer können den geschützten Modus auch deaktivieren, um den Zugriff über Smart Tunnel zu vereinfachen. Cisco empfiehlt jedoch, diese Methode zu verwerfen, da sie die Anfälligkeit für Angriffe erhöht.

Mac OS - Anforderungen und Einschränkungen

Diese Anforderungen und Einschränkungen gelten nur für Mac OS:

- Safari 3.1.1 oder höher oder Firefox 3.0 oder höher
- Sun JRE 1.5 oder höher
- Nur Anwendungen, die von der Portalseite gestartet wurden, können Smart-Tunnel-Verbindungen herstellen. Diese Anforderung beinhaltet die Unterstützung von Smart Tunnels für Firefox. Wenn Sie Firefox verwenden, um während der ersten Verwendung eines Smart Tunnels eine andere Instanz von Firefox zu starten, ist das Benutzerprofil csco_st erforderlich. Wenn dieses Benutzerprofil nicht vorhanden ist, wird der Benutzer in der Sitzung aufgefordert, ein Benutzerprofil zu erstellen.
- Anwendungen, die TCP verwenden und dynamisch mit der SSL-Bibliothek verbunden sind, können über einen Smart Tunnel arbeiten.
- Smart Tunnel unterstützt diese Funktionen und Anwendungen unter Mac OS nicht:Proxy-ServicesAutomatische AnmeldungAnwendungen, die zweistufige Namensräume verwendenKonsolenbasierte Anwendungen wie Telnet, SSH und cURLAnwendungen, die dlopen oder dlsym zum Auffinden von Libsocket-Anrufen verwendenStatisch verknüpfte Anwendungen zum Auffinden von Socket-Anrufen

Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Smart Tunnel-Liste hinzufügen oder bearbeiten

Im Dialogfeld "Smart Tunnel-Liste hinzufügen" können Sie der Sicherheitsappliance-Konfiguration eine Liste mit Smart Tunnel-Einträgen hinzufügen. Im Dialogfeld "Smart Tunnel-Liste bearbeiten" können Sie den Inhalt der Liste ändern.

Feld

Listenname: Geben Sie einen eindeutigen Namen für die Liste der Anwendungen oder Programme ein. Die Anzahl der Zeichen im Namen ist nicht beschränkt. Verwenden Sie keine Leerzeichen. Nach der Konfiguration der Smart-Tunnel-Liste wird der Listenname neben dem Smart Tunnel List-Attribut in den Clientless-SSL-VPN-Gruppenrichtlinien und den lokalen Benutzerrichtlinien angezeigt. Weisen Sie einen Namen zu, der Ihnen hilft, seinen Inhalt oder Zweck von anderen Listen zu unterscheiden, die Sie wahrscheinlich konfigurieren werden.

Smart Tunnel-Eintrag hinzufügen oder bearbeiten

Im Dialogfeld Smart Tunnel-Eintrag hinzufügen oder bearbeiten können Sie die Attribute einer Anwendung in einer Smart Tunnel-Liste angeben.

- **Anwendungs-ID** - Geben Sie eine Zeichenfolge ein, um den Eintrag in der Smart Tunnel-Liste zu benennen. Die Zeichenfolge ist für das Betriebssystem eindeutig. In der Regel wird die Anwendung benannt, der der Zugriff auf Smart Tunnels gewährt werden soll. Um mehrere Versionen einer Anwendung zu unterstützen, für die Sie verschiedene Pfade oder Hashwerte angeben möchten, können Sie mithilfe dieses Attributs Einträge differenzieren und das Betriebssystem sowie den Namen und die Version der Anwendung angeben, die von jedem

Listeneintrag unterstützt werden. Die Zeichenfolge kann bis zu 64 Zeichen enthalten.

- **Prozessname**: Geben Sie den Dateinamen oder den Pfad der Anwendung ein. Die Zeichenfolge kann bis zu 128 Zeichen enthalten.Windows benötigt eine genaue Übereinstimmung dieses Werts mit der rechten Seite des Anwendungspfads auf dem Remotehost, um die Anwendung für den intelligenten Tunnelzugriff zu qualifizieren. Wenn Sie nur den Dateinamen für Windows angeben, erzwingt SSL VPN keine Standortbeschränkung für den Remotehost, um die Anwendung für den Zugriff über Smart Tunnel zu qualifizieren.Wenn Sie einen Pfad angeben und der Benutzer die Anwendung an einem anderen Speicherort installiert hat, ist diese Anwendung nicht qualifiziert. Die Anwendung kann sich auf einem beliebigen Pfad befinden, solange die rechte Seite der Zeichenfolge mit dem von Ihnen eingegebenen Wert übereinstimmt.Um eine Anwendung für den Zugriff über Smart Tunnel zu autorisieren, wenn sie auf einem von mehreren Pfaden auf dem Remotehost vorhanden ist, geben Sie entweder nur den Namen und die Erweiterung der Anwendung in diesem Feld an, oder erstellen Sie einen eindeutigen Smart Tunnel-Eintrag für jeden Pfad.Wenn Sie unter Windows Smart Tunnel-Zugriff auf eine Anwendung hinzufügen möchten, die von der Eingabeaufforderung gestartet wurde, müssen Sie im Prozessnamen eines Eintrags in der Smart Tunnel-Liste "cmd.exe" angeben und den Pfad zur Anwendung selbst in einem anderen Eintrag angeben, da "cmd.exe" das übergeordnete Element der Anwendung ist.Mac OS benötigt den vollständigen Pfad zum Prozess und ist auf Groß- und Kleinschreibung bezogen. Um zu vermeiden, einen Pfad für jeden Benutzernamen anzugeben, fügen Sie vor dem partiellen Pfad eine Tilde (~) ein (z. B. ~/bin/vnc).
- **OS** - Klicken Sie auf Windows oder Mac, um das Host-Betriebssystem der Anwendung anzugeben.
- **Hash** (*optional und nur für Windows verfügbar*) Um diesen Wert zu erhalten, geben Sie die Prüfsumme der ausführbaren Datei in ein Dienstprogramm ein, das einen Hash mithilfe des SHA-1-Algorithmus berechnet. Ein Beispiel für ein solches Dienstprogramm ist der Microsoft File Checksum Integrity Verifier (FCIV), der bei Verfügbarkeit und Beschreibung des File Checksum Integrity Verifier-Dienstprogramms verfügbar ist. Nachdem Sie FCIV installiert haben, legen Sie eine temporäre Kopie der Anwendung auf einem Pfad ab, der keine Leerzeichen enthält (z. B. c:/fciv.exe), und geben Sie dann die Anwendung fciv.exe -sha1 in der Befehlszeile ein (z. B. fciv.exe -sha1 c:\msimn.exe), um den SHA-1-Hash anzuzeigen.Der SHA-1-Hash hat immer 40 Hexadezimalzeichen.Vor der Autorisierung einer Anwendung für den Zugriff über Smart Tunnel berechnet das clientlose SSL VPN den Hash der Anwendung, der mit der Anwendungs-ID übereinstimmt. Sie qualifiziert die Anwendung für den Zugriff über Smart Tunnel, wenn das Ergebnis dem Hash-Wert entspricht.Die Eingabe eines Hashs bietet eine angemessene Sicherheit, dass SSL VPN keine unzulässige Datei qualifiziert, die mit der in der Anwendungs-ID angegebenen Zeichenfolge übereinstimmt. Da die Prüfsumme je nach Version oder Patch einer Anwendung variiert, kann der von Ihnen eingegebene Hash nur einer Version oder einem Patch auf dem Remotehost entsprechen. Um einen Hash für mehrere Versionen einer Anwendung anzugeben, erstellen Sie für jeden Hashwert einen eindeutigen Smart Tunnel-Eintrag.**Hinweis:** Wenn Sie Hash-Werte eingeben und künftige Versionen oder Patches einer Anwendung mit Smart Tunnel-Zugriff unterstützen möchten, müssen Sie die Smart Tunnel-Liste zukünftig aktualisieren. Ein plötzliches Problem beim Zugriff auf Smart Tunnels kann darauf hindeuten, dass die Anwendung, die Hash-Werte enthält, bei einem Anwendungs-Upgrade nicht auf dem neuesten Stand ist. Sie können dieses Problem vermeiden, indem Sie keinen Hash eingeben.
- Wenn Sie die Smart Tunnel-Liste konfigurieren, müssen Sie sie einer Gruppenrichtlinie oder einer lokalen Benutzerrichtlinie zuweisen, damit sie wie folgt aktiviert wird:Um die Liste einer

Gruppenrichtlinie zuzuordnen, wählen Sie **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal**, und wählen Sie in der Dropdown-Liste neben dem Smart Tunnel List-Attribut den Namen des Smart Tunnels aus.Um die Liste einer lokalen Benutzerrichtlinie zuzuweisen, wählen Sie **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**, und wählen Sie in der Dropdown-Liste neben dem Smart Tunnel List-Attribut den Namen des Smart Tunnels aus.

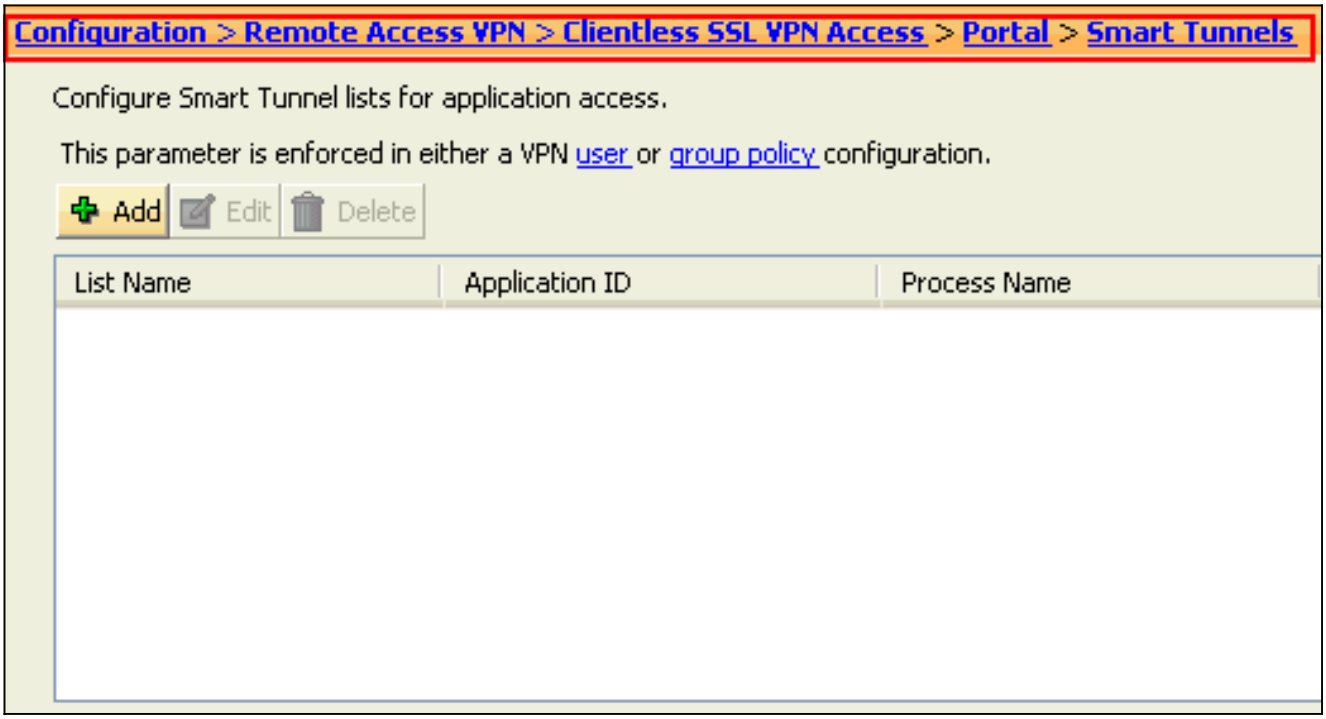
ASA Smart Tunnel (Lotus Example)-Konfiguration mit ASDM 6.0(2)

In diesem Dokument wird davon ausgegangen, dass die Basiskonfiguration, z. B. die Schnittstellenkonfiguration, vollständig ist und ordnungsgemäß funktioniert.

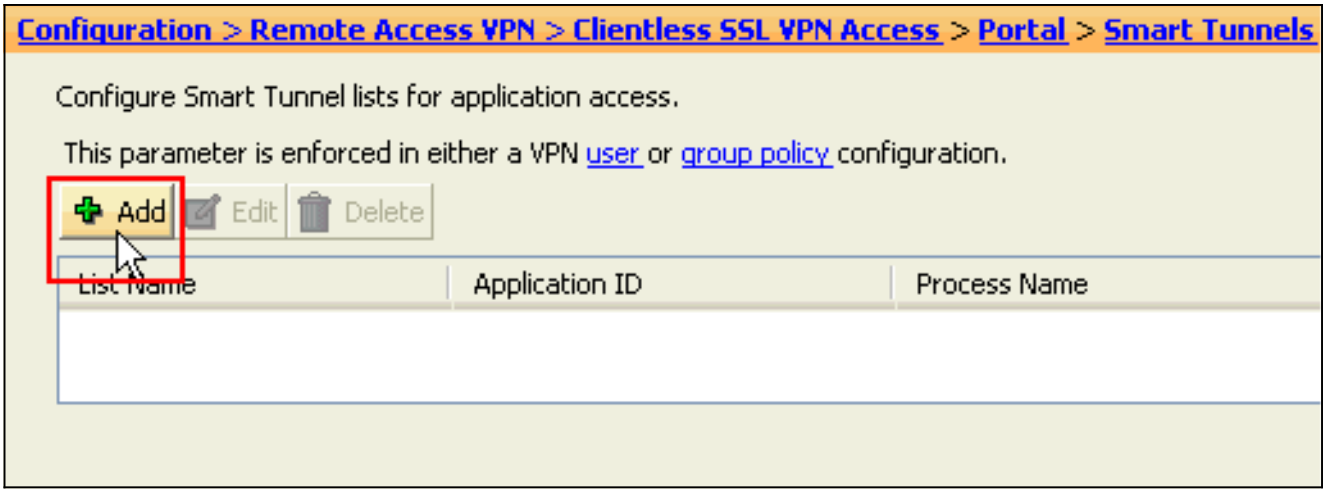
Gehen Sie wie folgt vor, um einen Smart Tunnel zu konfigurieren:

Hinweis: In diesem Konfigurationsbeispiel wird der Smart Tunnel für die Lotus-Anwendung konfiguriert.

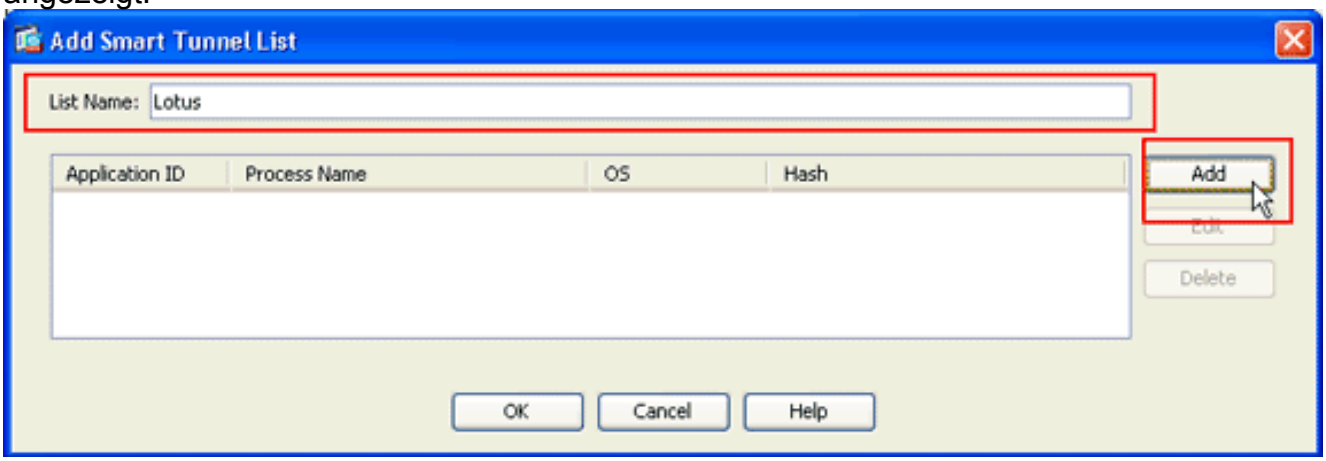
1. Wählen Sie **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**, um die Smart Tunnel-Konfiguration zu starten.



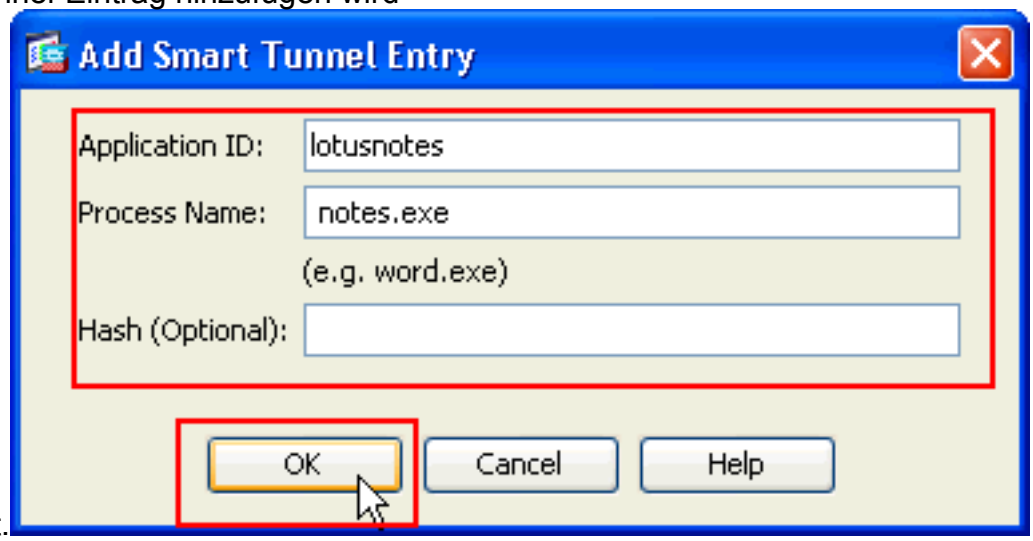
2. Klicken Sie auf **Hinzufügen**.



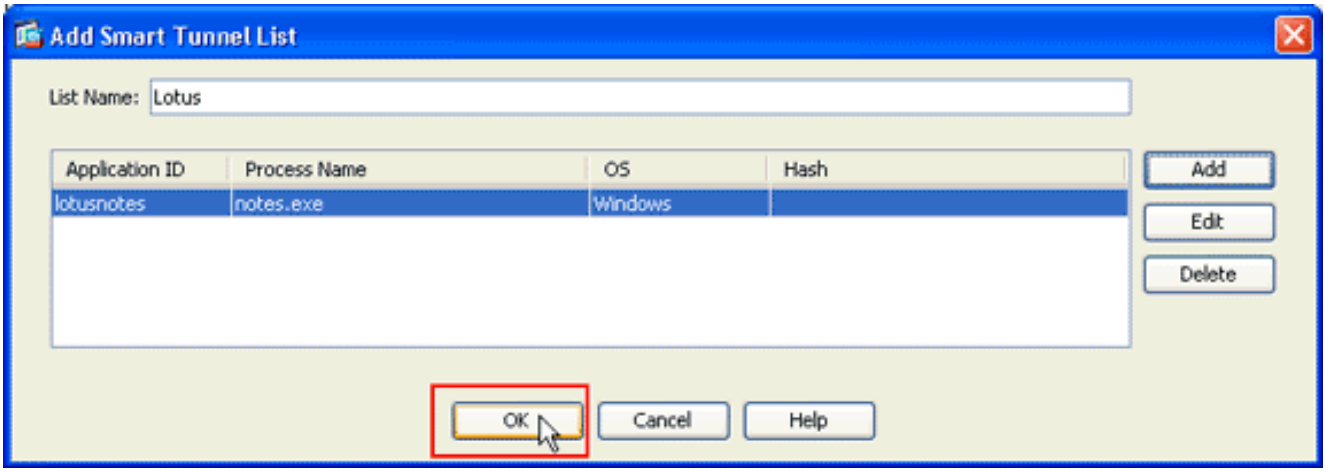
Das Dialogfeld "Smart Tunnel-Liste hinzufügen" wird angezeigt.



3. Klicken Sie im Dialogfeld Smart Tunnel-Liste hinzufügen auf **Hinzufügen**.Das Dialogfeld Smart Tunnel-Eintrag hinzufügen wird angezeigt.

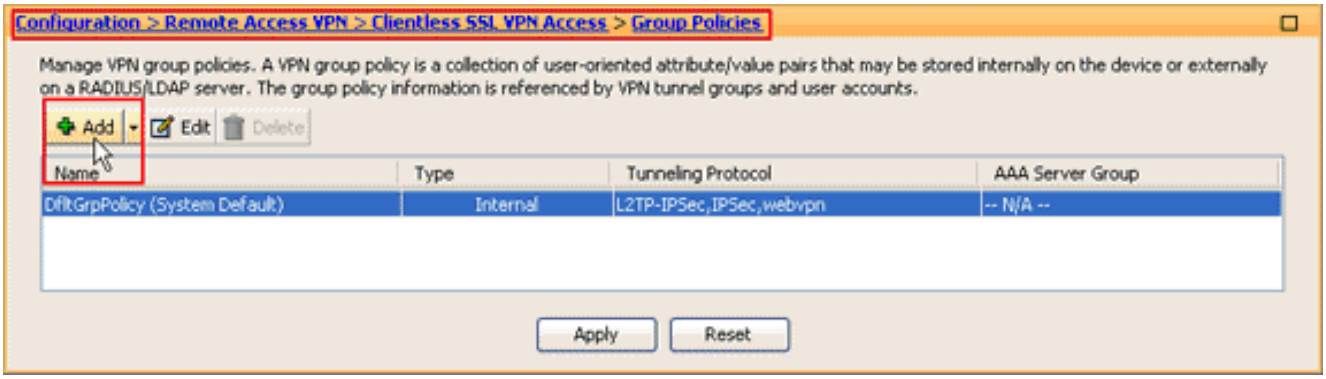


4. Geben Sie im Feld Application ID (Anwendungs-ID) eine Zeichenfolge ein, um den Eintrag in der Smart Tunnel-Liste zu identifizieren.
5. Geben Sie einen Dateinamen und eine Dateierweiterung für die Anwendung ein, und klicken Sie auf **OK**.
6. Klicken Sie im Dialogfeld Smart Tunnel-Liste hinzufügen auf **OK**.

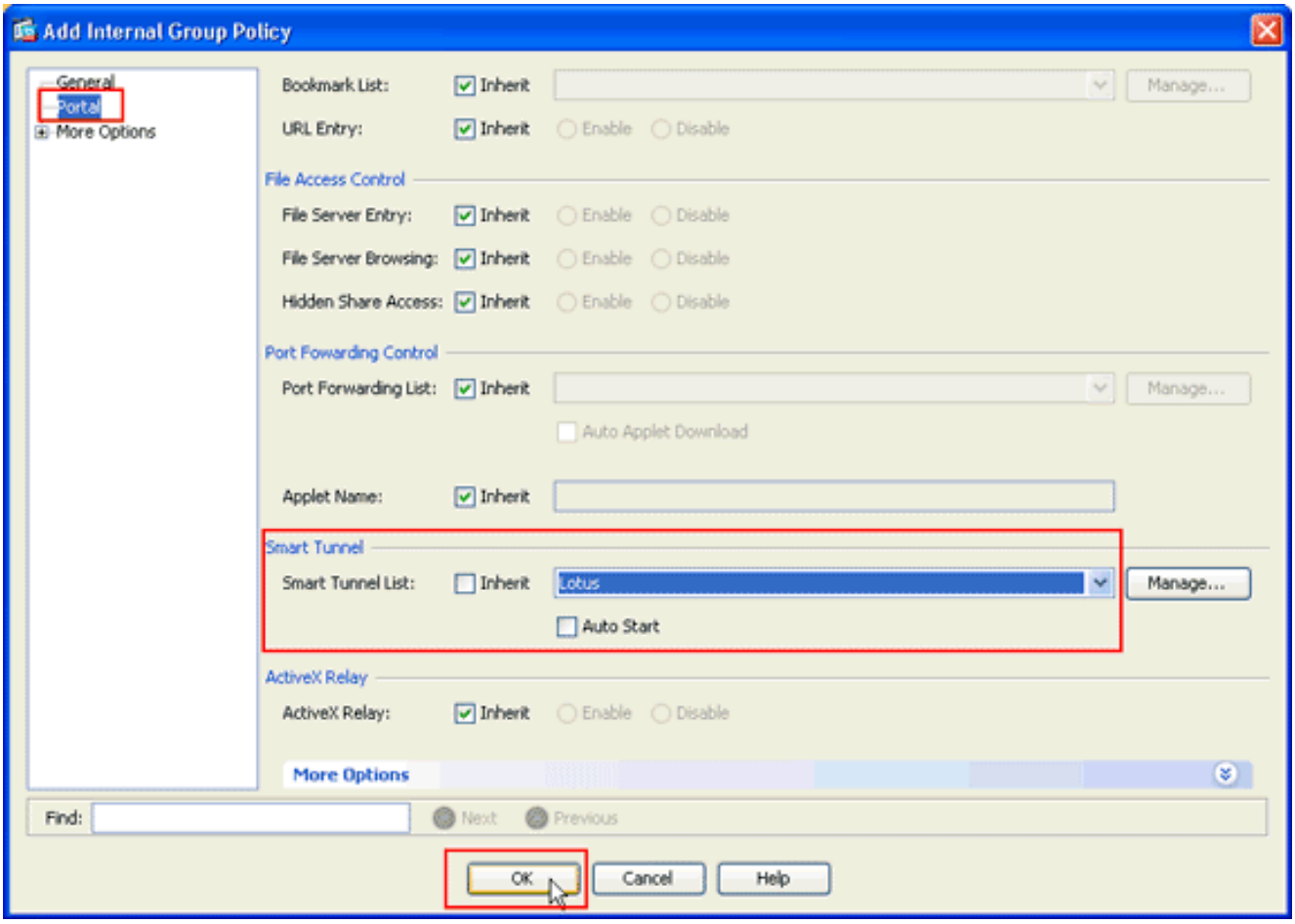


Hinweis: Hier ist der entsprechende CLI-Konfigurationsbefehl:

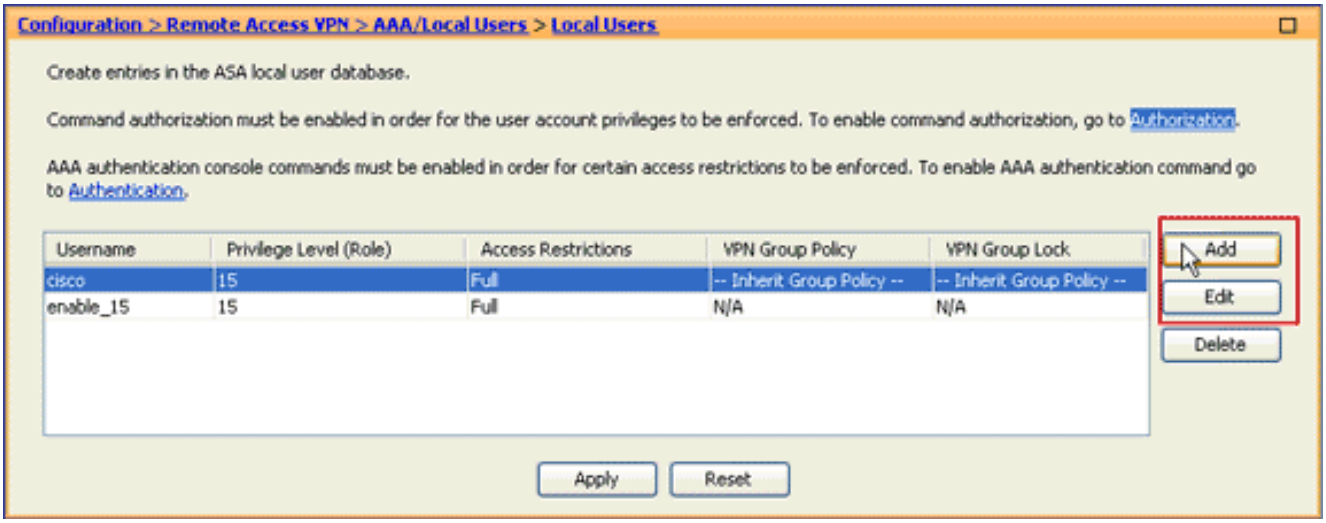
7. Weisen Sie die Liste den Gruppenrichtlinien und lokalen Benutzerrichtlinien zu, denen Sie Smart Tunnel-Zugriff auf die zugehörigen Anwendungen bereitstellen möchten:Um die Liste einer Gruppenrichtlinie zuzuordnen, wählen Sie **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies (Konfiguration > Remote-Access-VPN > Clientless-SSL-VPN-Zugriff > Gruppenrichtlinien) aus**, und klicken Sie auf **Add** oder **Edit.**



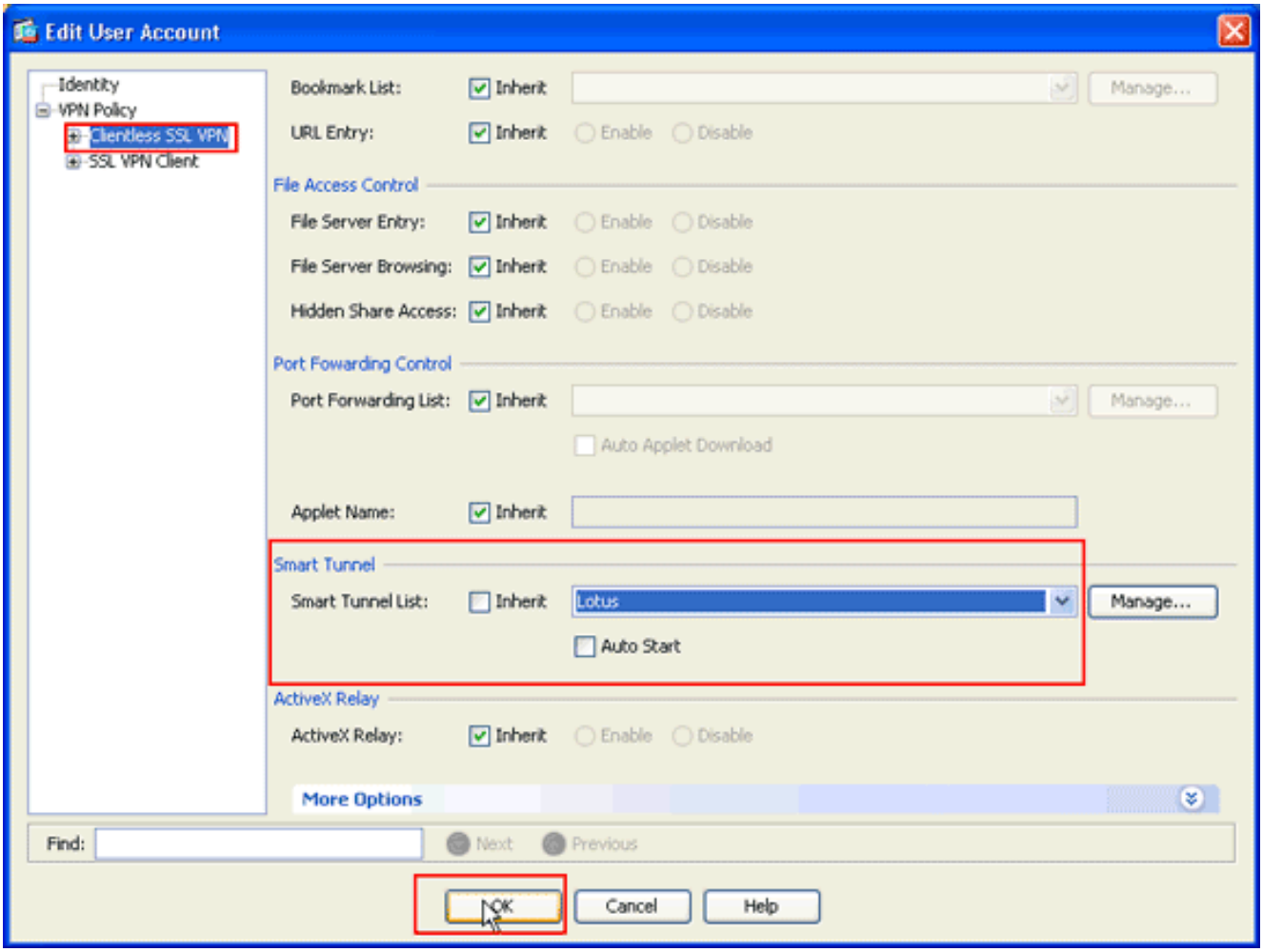
Das Dialogfeld Interne Gruppenrichtlinie hinzufügen wird angezeigt.



8. Klicken Sie im Dialogfeld Richtlinie für interne Gruppe hinzufügen auf **Portal**, wählen Sie in der Dropdown-Liste Smart Tunnel Name aus, und klicken Sie auf **OK**.**Hinweis:** In diesem Beispiel wird *Lotus* als Smart-Tunnel-Listenname verwendet.
9. Um die Liste einer lokalen Benutzerrichtlinie zuzuweisen, wählen Sie **Configuration > Remote Access VPN> AAA Setup > Local Users aus**, und klicken Sie auf **Add**, um einen neuen Benutzer zu konfigurieren, oder klicken Sie auf **Edit**, um einen vorhandenen Benutzer zu
bearbeiten.



Das Dialogfeld Benutzerkonto bearbeiten wird angezeigt.



10. Klicken Sie im Dialogfeld Benutzerkonto bearbeiten auf **Clientless SSL VPN**, wählen Sie in der Dropdown-Liste Smart Tunnel den Namen des Smart Tunnels aus, und klicken Sie auf **OK**.**Hinweis:** In diesem Beispiel wird *Lotus* als Smart-Tunnel-Listenname verwendet.

Die Smart Tunnel-Konfiguration ist abgeschlossen.

Fehlerbehebung

Ich kann keine Verbindung über eine als Lesezeichen gespeicherte Smart Tunnel-URL im Clientless-Portal herstellen. Warum tritt dieses Problem auf, und wie kann ich es beheben?

Dieses Problem wird durch das in Cisco Bug ID CSCsx05766 beschriebene Problem verursacht (nur registrierte **Kunden)** . Um dieses Problem zu beheben, müssen Sie das Java Runtime-Plugin auf eine ältere Version herabstufen.

Kann ich die URL einer in WebVPN konfigurierten Smart-Tunnel-Verbindung übernehmen?

Wenn auf der ASA Smart Tunnel verwendet wird, können Sie die URL nicht löschen oder die Adressleiste des Browsers nicht ausblenden. Benutzer können die URLs der in WebVPN konfigurierten Links anzeigen, die Smart Tunnel verwenden. Als Ergebnis können sie den Port ändern und für einen anderen Service auf den Server zugreifen.

Um dieses Problem zu beheben, verwenden Sie WebType-ACLs. Weitere Informationen finden

Sie unter WebType-Zugriffssteuerungslisten.

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- SSL VPN Client (SVC) auf ASA mit ASDM - Konfigurationsbeispiel
- Technischer Support und Dokumentation für Cisco Systeme