ASA: Esempio di configurazione di Smart Tunnel con ASDM

Sommario

Introduzione

Uno smart tunnel è una connessione tra un'applicazione basata su TCP e un sito privato che utilizza una sessione VPN SSL senza client (basata su browser) con l'appliance di sicurezza come percorso e l'appliance di sicurezza come server proxy. È possibile identificare le applicazioni a cui si desidera concedere l'accesso allo smart tunnel e specificare il percorso locale di ciascuna applicazione. Per le applicazioni eseguite in Microsoft Windows, è inoltre possibile richiedere una corrispondenza dell'hash SHA-1 del checksum come condizione per concedere l'accesso allo smart tunnel.

Lotus SameTime e *Microsoft Outlook Express* sono esempi di applicazioni per le quali è possibile concedere l'accesso allo smart tunnel.

A seconda che l'applicazione sia un client o un'applicazione abilitata per il Web, la configurazione dello smart tunnel richiede una delle procedure seguenti:

- Creare uno o più elenchi di smart tunnel delle applicazioni client, quindi assegnare l'elenco ai criteri di gruppo o ai criteri utente locali per i quali si desidera fornire l'accesso smart tunnel.
- Creare una o più voci dell'elenco dei segnalibri che specificano gli URL delle applicazioni

abilitate per il Web idonee per l'accesso allo smart tunnel, quindi assegnare l'elenco ai DAP, ai Criteri di gruppo o ai Criteri utente locali per i quali si desidera fornire l'accesso allo smart tunnel.Èinoltre possibile elencare le applicazioni abilitate per il Web per le quali automatizzare l'invio delle credenziali di accesso nelle connessioni smart tunnel su sessioni VPN SSL senza client.

In questo documento si presume che la configurazione del client VPN Cisco AnyConnect SSL sia già stata creata e funzioni correttamente in modo che la funzionalità smart tunnel possa essere configurata sulla configurazione esistente. Per ulteriori informazioni su come configurare il client VPN SSL di Cisco AnyConnect, fare riferimento alla sezione ASA 8.x: Esempio di configurazione dell'ASA che consente il tunneling ripartito per il client VPN AnyConnect.

Nota: verificare che i punti da *4.b a 4.l* descritti nella sezione Configurazione dell'ASA con ASDM 6.0(2) di *ASA 8.x: Nell'esempio di configurazione dell'ASA,* non *si* esegue *l'opzione Allow Split Tunneling for AnyConnect VPN Client* per configurare la funzione smart tunnel.

In questo documento viene descritto come configurare smart tunnel su Cisco ASA serie 5500 Adaptive Security Appliance.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.0(2)
- PC con Microsoft Vista, Windows XP SP2 o Windows 2000 Professional SP4 e Microsoft Installer versione 3.1
- Cisco Adaptive Security Device Manager (ASDM) versione 6.0(2)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Configurazione di Smart Tunnel Access

La tabella del tunnel intelligente visualizza gli elenchi dei tunnel intelligenti, ciascuno dei quali

identifica una o più applicazioni idonee per l'accesso al tunnel intelligente e il sistema operativo associato. Poiché ogni criterio di gruppo o criterio utente locale supporta un elenco di smart tunnel, è necessario raggruppare le applicazioni non basate su browser da supportare in un elenco di smart tunnel. Dopo aver configurato un elenco, è possibile assegnarlo a uno o più criteri di gruppo o criteri utente locali.

La finestra Smart Tunnel (**Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Portale > Smart Tunnel**) consente di completare le seguenti procedure:

- **Aggiungere un elenco di smart tunnel e aggiungere applicazioni all'elenco**Per aggiungere un elenco di smart tunnel e aggiungere applicazioni all'elenco, completare la procedura seguente:Fare clic su **Add**.Viene visualizzata la finestra di dialogo Aggiungi elenco smart tunnel.Immettere un nome per l'elenco e fare clic su **Aggiungi**.ASDM apre la finestra di dialogo Aggiungi voce di Smart Tunnel, che consente di assegnare gli attributi di uno smart tunnel all'elenco.Dopo aver assegnato gli attributi desiderati per lo smart tunnel, fare clic su **OK**.ASDM visualizza tali attributi nell'elenco.Ripetere questi passaggi per completare l'elenco e quindi fare clic su **OK** nella finestra di dialogo Aggiungi elenco smart tunnel.
- **Modifica di un elenco di smart tunnel**Per modificare un elenco di tunnel intelligenti, completare i seguenti passaggi:Fare doppio clic sull'elenco o scegliere l'elenco nella tabella e fare clic su **Modifica**.Fare clic su **Aggiungi** per inserire un nuovo set di attributi di smart tunnel nell'elenco o scegliere una voce nell'elenco e fare clic su **Modifica** o su **Elimina**.
- **Rimuovi elenco**Per rimuovere un elenco, sceglierlo nella tabella e fare clic su **Elimina**.
- **Aggiungi segnalibro**In seguito alla configurazione e all'assegnazione di un elenco di smart tunnel, è possibile semplificare l'utilizzo di uno smart tunnel aggiungendo un segnalibro per il servizio e facendo clic sull'opzione **Abilita smart tunnel** nella finestra di dialogo Aggiungi o modifica segnalibro.

Smart Tunnel Access consente a un'applicazione client basata su TCP di utilizzare una connessione VPN basata su browser per connettersi a un servizio. Offre i seguenti vantaggi agli utenti, rispetto ai plug-in e alla tecnologia legacy, all'inoltro delle porte:

- Il tunnel intelligente offre prestazioni migliori rispetto ai plug-in.
- A differenza dell'inoltro delle porte, lo smart tunnel semplifica l'esperienza utente in quanto non richiede la connessione dell'applicazione locale alla porta locale.
- A differenza dell'inoltro delle porte, lo smart tunnel non richiede privilegi di amministratore per gli utenti.

Requisiti, restrizioni e limitazioni dello Smart Tunnel

Requisiti e limitazioni generali

Lo Smart Tunnel presenta i seguenti requisiti e limitazioni generali:

- L'host remoto da cui ha origine lo smart tunnel deve eseguire una versione a 32 bit di Microsoft Windows Vista, Windows XP o Windows 2000; o Mac OS 10.4 o 10.5.
- Smart tunnel auto sign-on supporta solo Microsoft Internet Explorer su Windows.
- Il browser deve essere abilitato con Java, Microsoft ActiveX o entrambi.
- Smart Tunnel supporta solo proxy posizionati tra computer che eseguono Microsoft Windows e l'appliance di sicurezza. Smart tunnel utilizza la configurazione di Internet Explorer, ovvero

quella destinata all'utilizzo a livello di sistema in Windows. Se il computer remoto richiede un server proxy per raggiungere l'appliance di sicurezza, l'URL dell'estremità finale della connessione deve essere incluso nell'elenco degli URL esclusi dai servizi proxy. Se la configurazione del proxy specifica che il traffico destinato all'ASA deve passare attraverso un proxy, tutto il traffico dello smart tunnel deve passare attraverso il proxy.In uno scenario di accesso remoto basato su HTTP, a volte una subnet non fornisce l'accesso utente al gateway VPN. In questo caso, l'accesso Web è garantito da un proxy posizionato davanti all'appliance ASA per indirizzare il traffico tra il Web e la posizione dell'utente finale. Tuttavia, solo gli utenti VPN possono configurare i proxy davanti all'appliance ASA. In questo caso, devono verificare che i proxy supportino il metodo CONNECT. Per i proxy che richiedono l'autenticazione, smart tunnel supporta solo il tipo di autenticazione digest di base.

- All'avvio di Smart Tunnel, l'appliance di sicurezza esegue il tunneling di tutto il traffico proveniente dal browser, che viene elaborato dall'utente per avviare la sessione senza client. Se l'utente avvia un'altra istanza del processo del browser, passa tutto il traffico al tunnel. Se il processo del browser è lo stesso e l'accessorio di protezione non consente l'accesso a un determinato URL, l'utente non potrà aprirlo. Per risolvere il problema, l'utente può utilizzare un browser diverso da quello utilizzato per stabilire la sessione senza client.
- Un failover con stato non mantiene le connessioni smart tunnel. Gli utenti devono riconnettersi dopo un failover.

Requisiti e limitazioni di Windows

I requisiti e le limitazioni seguenti si applicano solo a Windows:

- Solo le applicazioni basate su TCP Winsock 2 sono idonee per l'accesso al tunnel intelligente.
- L'accessorio di protezione non supporta il proxy MAPI (Microsoft Outlook Exchange). L'inoltro delle porte e lo smart tunnel non supportano MAPI. Per le comunicazioni di Microsoft Outlook Exchange tramite il protocollo MAPI, gli utenti remoti devono utilizzare AnyConnect.
- Gli utenti di Microsoft Windows Vista che usano l'inoltro smart tunnel o porta devono aggiungere l'URL dell'ASA all'area dei siti attendibili. Per accedere all'area Sito attendibile, avviare Internet Explorer e scegliere **Strumenti > Opzioni Internet**, quindi fare clic sulla scheda **Protezione**. Gli utenti di Vista possono anche disabilitare la modalità protetta per facilitare l'accesso al tunnel intelligente; tuttavia, Cisco consiglia di utilizzare questo metodo perché aumenta la vulnerabilità agli attacchi.

Requisiti e limitazioni di Mac OS

Questi requisiti e limitazioni si applicano solo a Mac OS:

- Safari 3.1.1 o successivo o Firefox 3.0 o successivo
- Sun JRE 1.5 o versioni successive
- Solo le applicazioni avviate dalla pagina del portale possono stabilire connessioni smart tunnel. Questo requisito include il supporto di smart tunnel per Firefox. Se si utilizza Firefox per avviare un'altra istanza di Firefox durante il primo utilizzo di uno smart tunnel, è necessario il profilo utente cisco_st. Se questo profilo utente non è presente, la sessione richiede all'utente di crearne uno.
- Le applicazioni che utilizzano TCP e sono collegate dinamicamente alla libreria SSL possono funzionare su un tunnel intelligente.

- Smart tunnel non supporta queste funzionalità e applicazioni su Mac OS:Servizi proxyAccesso automaticoApplicazioni che utilizzano spazi dei nomi a due livelliApplicazioni basate su console, quali Telnet, SSH e cURLApplicazioni che utilizzano dlopen o dlsym per individuare le chiamate libsocketApplicazioni collegate staticamente per individuare le chiamate libsocket

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Aggiungi o modifica elenco smart tunnel

La finestra di dialogo Aggiungi elenco smart tunnel consente di aggiungere un elenco di voci di smart tunnel alla configurazione dell'appliance di sicurezza. La finestra di dialogo Modifica elenco smart tunnel consente di modificare il contenuto dell'elenco.

Campo

Nome elenco: immettere un nome univoco per l'elenco delle applicazioni o dei programmi. Non esistono restrizioni al numero di caratteri nel nome. Non utilizzare spazi. Dopo la configurazione dell'elenco di smart tunnel, il nome dell'elenco viene visualizzato accanto all'attributo Elenco smart tunnel nei criteri di gruppo VPN SSL senza client e nei criteri utente locali. Assegnare un nome che consenta di distinguerne il contenuto o lo scopo dagli altri elenchi che è probabile configurare.

Aggiungi o modifica voce di Smart Tunnel

La finestra di dialogo Aggiungi o modifica voce di Smart Tunnel consente di specificare gli attributi di un'applicazione in un elenco di smart tunnel.

- **ID applicazione**: immettere una stringa per assegnare un nome alla voce nell'elenco di smart tunnel. La stringa è univoca per il sistema operativo. In genere, assegna all'applicazione il nome per cui si desidera concedere l'accesso allo smart tunnel. Per supportare più versioni di un'applicazione per la quale si sceglie di specificare percorsi o valori hash diversi, è possibile utilizzare questo attributo per differenziare le voci, specificando il sistema operativo e il nome e la versione dell'applicazione supportata da ciascuna voce di elenco. La stringa può contenere un massimo di 64 caratteri.
- **Nome processo (Process Name)** - Immettete il nome o il percorso del file dell'applicazione. La stringa può contenere un massimo di 128 caratteriWindows richiede una corrispondenza esatta di questo valore con il lato destro del percorso dell'applicazione sull'host remoto per qualificare l'applicazione per l'accesso allo smart tunnel. Se si specifica solo il nome del file per Windows, la VPN SSL non applica una restrizione della posizione sull'host remoto per qualificare l'applicazione per l'accesso allo smart tunnel.Se si specifica un percorso e l'utente ha installato l'applicazione in un'altra posizione, tale applicazione non è qualificata. L'applicazione può risiedere in qualsiasi percorso purché il lato destro della stringa corrisponda al valore immesso.Per autorizzare un'applicazione per l'accesso allo smart tunnel se è presente in uno dei diversi percorsi dell'host remoto, specificare solo il nome e l'estensione dell'applicazione in questo campo o creare una voce smart tunnel univoca per

ciascun percorso.Per Windows, se si desidera aggiungere l'accesso allo smart tunnel a un'applicazione avviata dal prompt dei comandi, è necessario specificare "cmd.exe" nel nome del processo di una voce dell'elenco dello smart tunnel e specificare il percorso dell'applicazione stessa in un'altra voce, in quanto "cmd.exe" è l'elemento padre dell'applicazione.Mac OS richiede il percorso completo del processo e fa distinzione tra maiuscole e minuscole. Per evitare di specificare un percorso per ogni nome utente, inserire una tilde (~) prima del percorso parziale (ad esempio, ~/bin/vnc).

- **OS** - Fate clic su Windows o Mac per specificare il sistema operativo host dell'applicazione.
- **Hash**: (*facoltativo e applicabile solo a Windows*) per ottenere questo valore, immettere il checksum del file eseguibile in un'utilità che calcola un hash utilizzando l'algoritmo SHA-1. Un esempio di tale utilità è Microsoft File Checksum Integrity Verifier (FCIV), disponibile all'indirizzo Disponibilità e descrizione dell'utilità File Checksum Integrity Verifier. Dopo l'installazione di FCIV, inserire una copia temporanea dell'applicazione di cui eseguire l'hash in un percorso che non contenga spazi (ad esempio, c:/fciv.exe), quindi immettere fciv.exe -sha1 application nella riga di comando (ad esempio, fciv.exe -sha1 c:\msimn.exe) per visualizzare l'hash SHA-1.L'hash SHA-1 è sempre composto da 40 caratteri esadecimali.Prima di autorizzare un'applicazione per l'accesso allo smart tunnel, la VPN SSL senza client calcola l'hash dell'applicazione corrispondente all'ID applicazione. Qualifica l'applicazione per l'accesso allo smart tunnel se il risultato corrisponde al valore di hash.L'immissione di un hash garantisce che SSL VPN non qualifichi un file non valido corrispondente alla stringa specificata nell'ID applicazione. Poiché il checksum varia a seconda della versione o della patch di un'applicazione, l'hash immesso può corrispondere a una sola versione o patch sull'host remoto. Per specificare un hash per più versioni di un'applicazione, creare una voce di smart tunnel univoca per ogni valore hash.**Nota:** se si immettono valori hash e si desidera supportare versioni o patch future di un'applicazione con accesso a smart tunnel, sarà necessario aggiornare l'elenco di smart tunnel in futuro. Un problema improvviso con l'accesso al tunnel intelligente potrebbe indicare che l'applicazione che contiene i valori hash non è aggiornata con un aggiornamento dell'applicazione. È possibile evitare questo problema non immettendo un hash.
- Dopo aver configurato l'elenco di smart tunnel, è necessario assegnarlo a un criterio di gruppo o a un criterio utente locale affinché diventi attivo nel modo seguente:Per assegnare l'elenco a un criterio di gruppo, scegliere **Configura > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di gruppo > Aggiungi o Modifica > Portale**, quindi scegliere il nome dello smart tunnel dall'elenco a discesa accanto all'attributo Elenco smart tunnel.Per assegnare l'elenco a un criterio utente locale, scegliere **Configurazione > VPN ad accesso remoto > Impostazione AAA > Utenti locali > Aggiungi o Modifica > Criterio VPN > VPN SSL senza client**, quindi scegliere il nome dello smart tunnel dall'elenco a discesa accanto all'attributo Elenco smart tunnel.

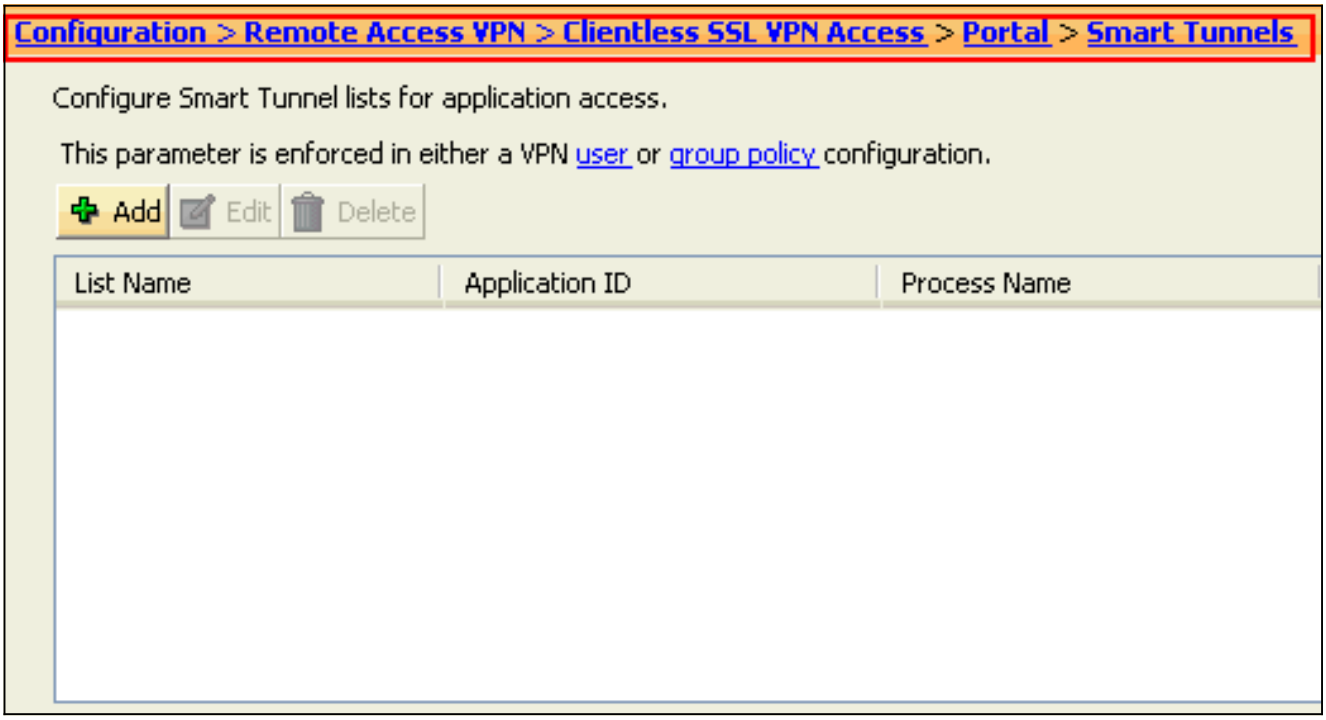
Configurazione di ASA Smart Tunnel (esempio con Lotus) con ASDM 6.0(2)

in questo documento si presume che la configurazione di base, ad esempio la configurazione dell'interfaccia, sia completa e funzioni correttamente.

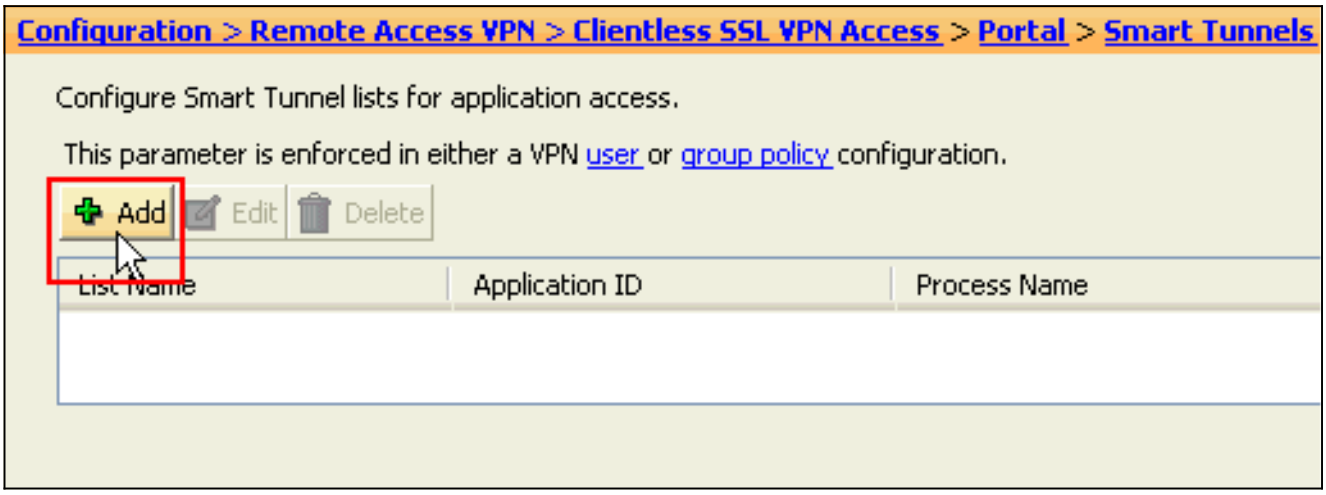
Per configurare un tunnel intelligente, completare la procedura seguente:

Nota: in questo esempio di configurazione, lo smart tunnel è configurato per l'applicazione Lotus.

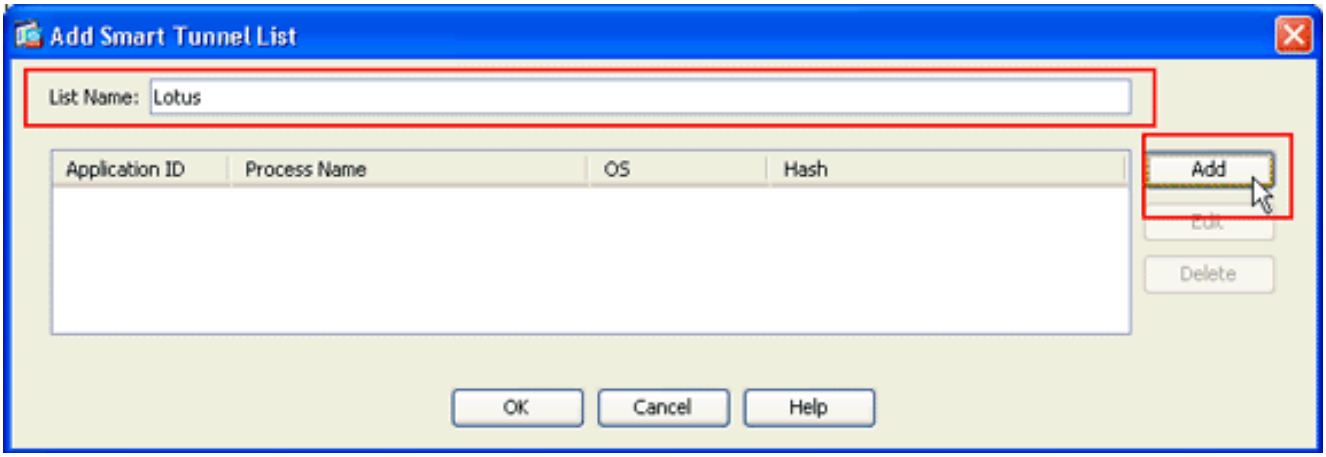
1. Per avviare la configurazione di Smart Tunnel, scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Portale > Smart Tunnel**.



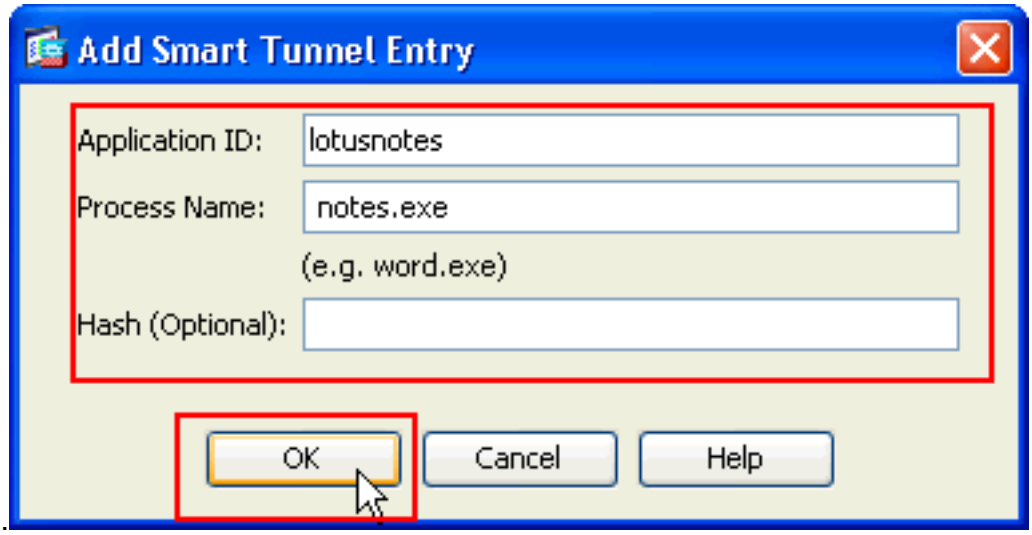
2. Fare clic su **Add**.



Viene visualizzata la finestra di dialogo Aggiungi elenco smart tunnel.

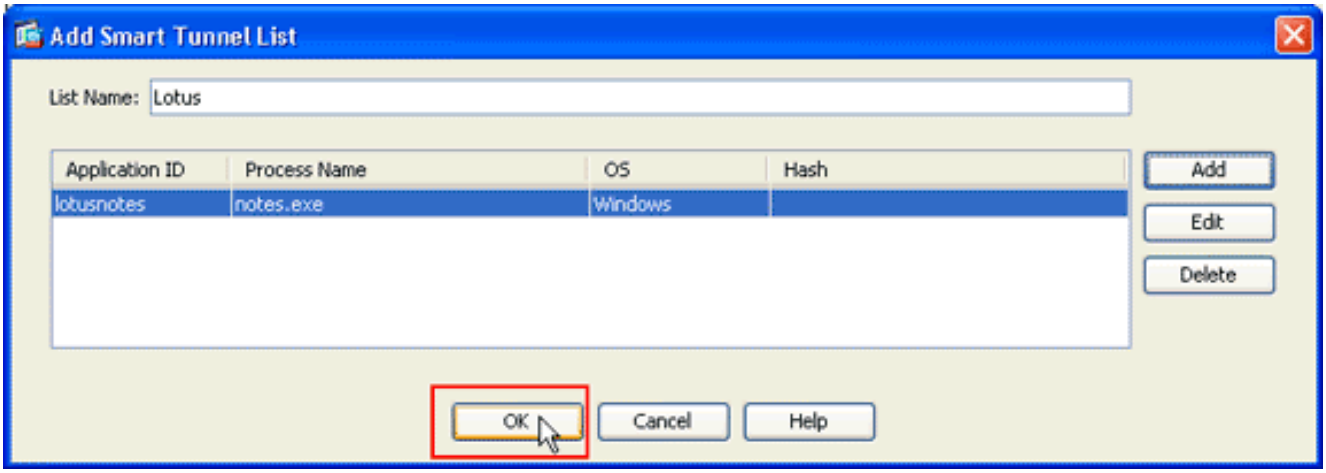


3. Nella finestra di dialogo Aggiungi elenco smart tunnel fare clic su **Aggiungi**.Viene visualizzata la finestra di dialogo Aggiungi voce tunnel



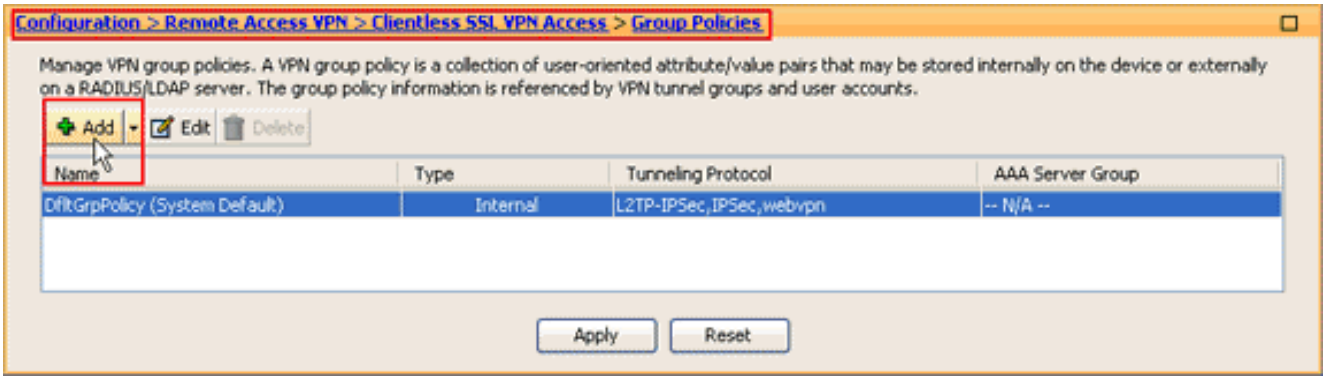
intelligente.

4. Nel campo ID applicazione immettere una stringa per identificare la voce nell'elenco di smart tunnel.
5. Immettere un nome file e un'estensione per l'applicazione, quindi fare clic su **OK**.
6. Nella finestra di dialogo Aggiungi elenco smart tunnel fare clic su **OK**.

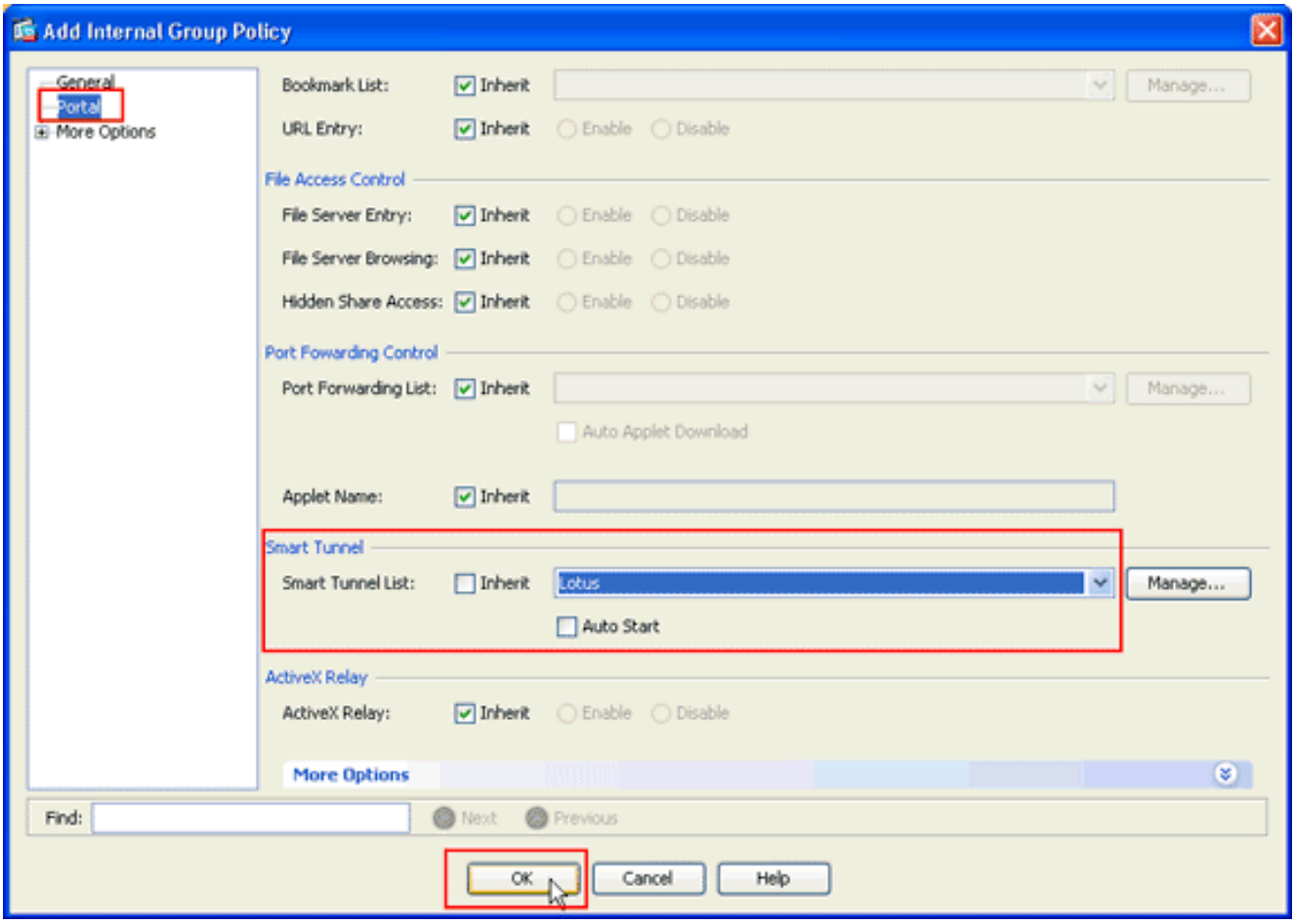


Nota: di seguito è riportato il comando di configurazione CLI equivalente:

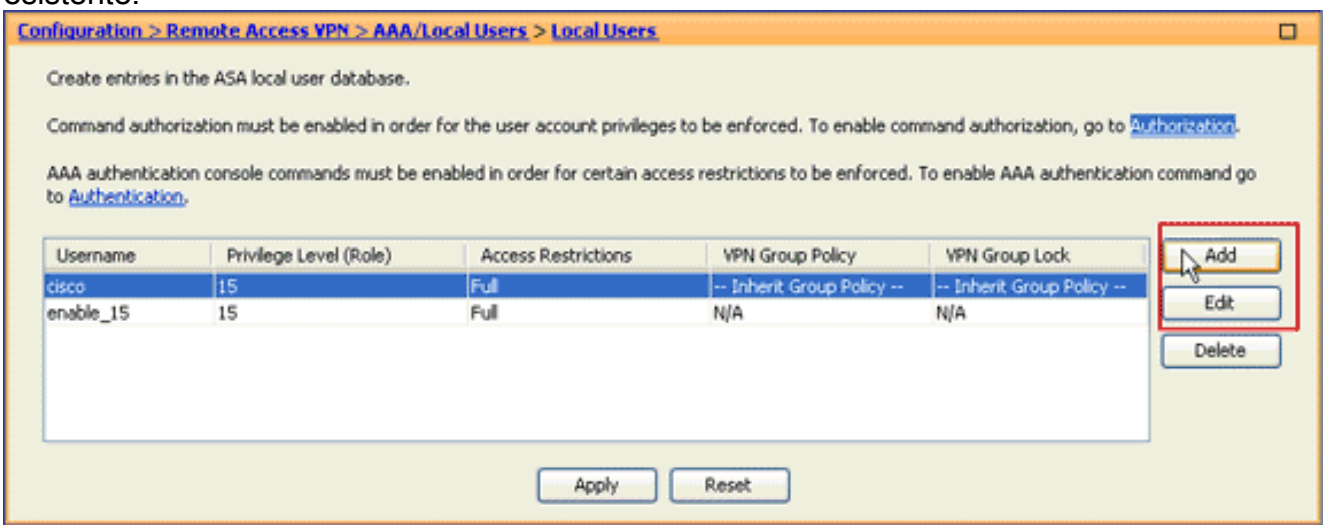
7. Assegnare l'elenco ai criteri di gruppo e ai criteri utente locali a cui si desidera fornire l'accesso smart tunnel alle applicazioni associate nel modo seguente:Per assegnare l'elenco a un criterio di gruppo, scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di gruppo**, quindi fare clic su **Aggiungi** o **Modifica.**



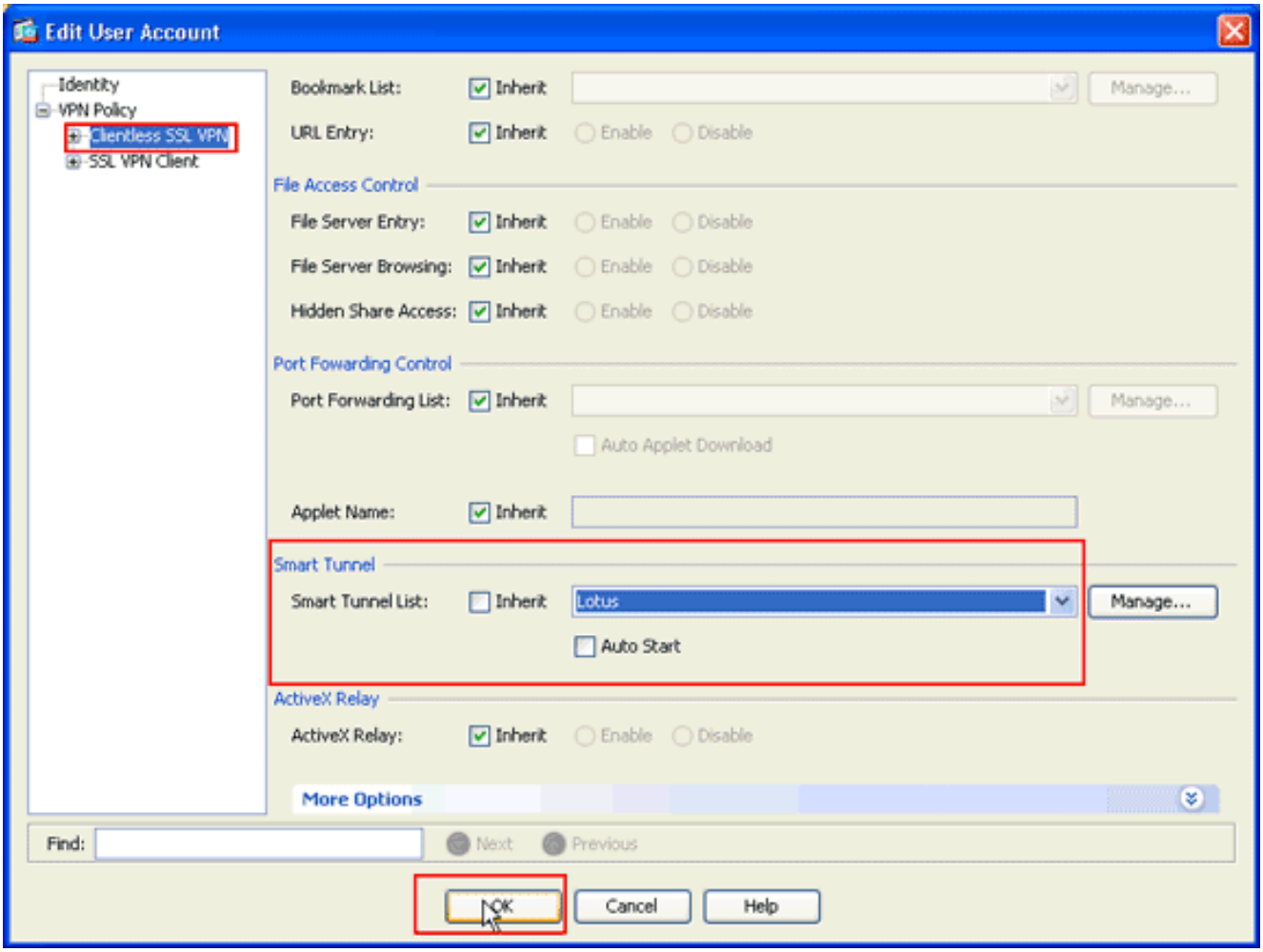
Verrà visualizzata la finestra di dialogo Aggiungi Criteri di gruppo interni.



8. Nella finestra di dialogo Aggiungi criteri di gruppo interni fare clic su **Portale**, scegliere il nome dello smart tunnel dall'elenco a discesa Elenco smart tunnel e fare clic su **OK**.**Nota:** in questo esempio viene utilizzato *Lotus* come nome dell'elenco di smart tunnel.
9. Per assegnare l'elenco a un criterio utente locale, scegliere **Configurazione > VPN ad accesso remoto> Configurazione AAA > Utenti locali** e fare clic su **Aggiungi** per configurare un nuovo utente oppure fare clic su **Modifica** per modificare un utente esistente.



Verrà visualizzata la finestra di dialogo Modifica account utente.



10. Nella finestra di dialogo Modifica account utente, fare clic su **VPN SSL senza client**, scegliere il nome dello smart tunnel dall'elenco a discesa Elenco smart tunnel e fare clic su **OK**.**Nota:** in questo esempio viene utilizzato *Lotus* come nome dell'elenco di smart tunnel.

Configurazione dello smart tunnel completata.

Risoluzione dei problemi

Impossibile connettersi utilizzando un URL dello Smart Tunnel con segnalibro nel portale senza client. Perché si verifica questo problema e come è possibile risolverlo?

Il problema è dovuto al problema descritto nell'ID bug Cisco CSCsx05766 (solo utenti registrati). Per risolvere il problema, eseguire il downgrade del plug-in Java Runtime a una versione precedente.

È possibile modificare l'URL di un collegamento allo smart tunnel configurato in WebVPN?

Quando si usa lo smart tunnel sull'appliance ASA, non è possibile nascondere l'URL o nascondere la barra degli indirizzi del browser. Gli utenti possono visualizzare gli URL dei collegamenti configurati in WebVPN che utilizzano smart tunnel. Di conseguenza, possono modificare la porta e accedere al server per altri servizi.

Per risolvere il problema, utilizzare ACL WebType. Per ulteriori informazioni, fare riferimento a

Access Control List WebType.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Documentazione e supporto tecnico – Cisco Systems