ASA 8.x: Consenti agli utenti di selezionare un gruppo all'accesso WebVPN tramite Group-Alias e Group-URL

Sommario

Introduzione

Gli utenti VPN SSL (sia AnyConnect/SVC che Client) possono scegliere il gruppo di tunnel a cui accedere [Connection Profile in Adaptive Security Device Manager (ASDM) lingo] tramite i seguenti metodi:

- url-gruppo
- group-alias (elenco a discesa gruppo tunnel nella pagina di accesso)
- mapping dei certificati, se si utilizzano i certificati

In questo documento viene illustrato come configurare Adaptive Security Appliance (ASA) in modo che gli utenti possano selezionare un gruppo tramite un menu a discesa quando accedono al servizio WebVPN. I gruppi visualizzati nel menu sono alias o URL di profili di connessione reali (gruppi di tunnel) configurati sull'appliance ASA. In questo documento viene spiegato come creare alias e URL per i profili di connessione (gruppi di tunnel) e quindi configurare la visualizzazione dell'elenco a discesa. Questa configurazione viene eseguita utilizzando ASDM 6.0(2) su un'ASA con software versione 8.0(2).

Nota: ASA versione 7.2.x supporta due metodi: elenco group-url e group-alias.

Nota: ASA versione 8.0.x supporta tre metodi: group-url, group-alias e certificate-map.

Prerequisiti

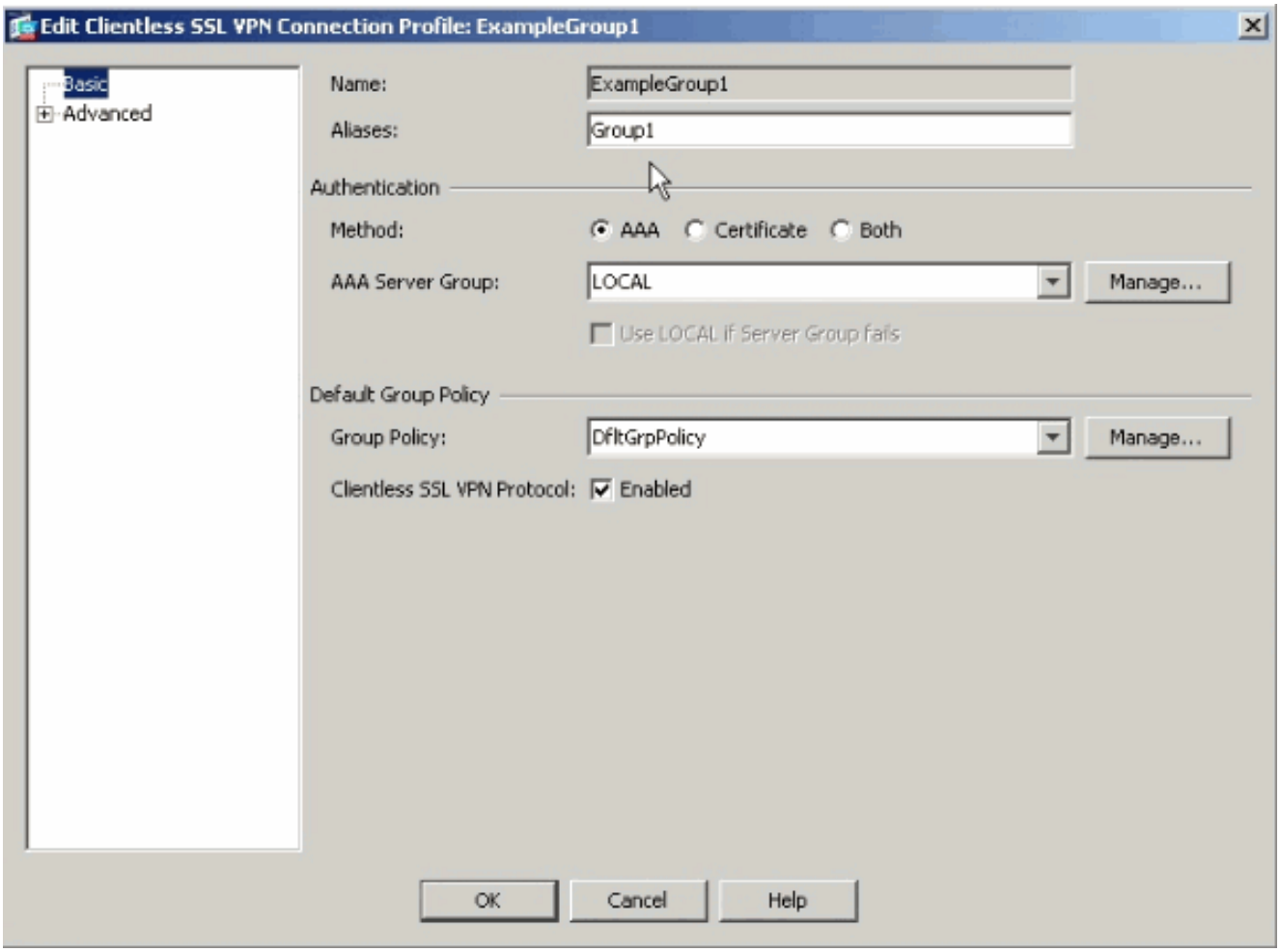
Configurare un alias e abilitare l'elenco a discesa

In questa sezione vengono presentate le informazioni necessarie per configurare un alias per un profilo di connessione (gruppo tunnel) e quindi configurare gli alias in modo che vengano visualizzati nel menu a discesa Gruppo della pagina di accesso di WebVPN.

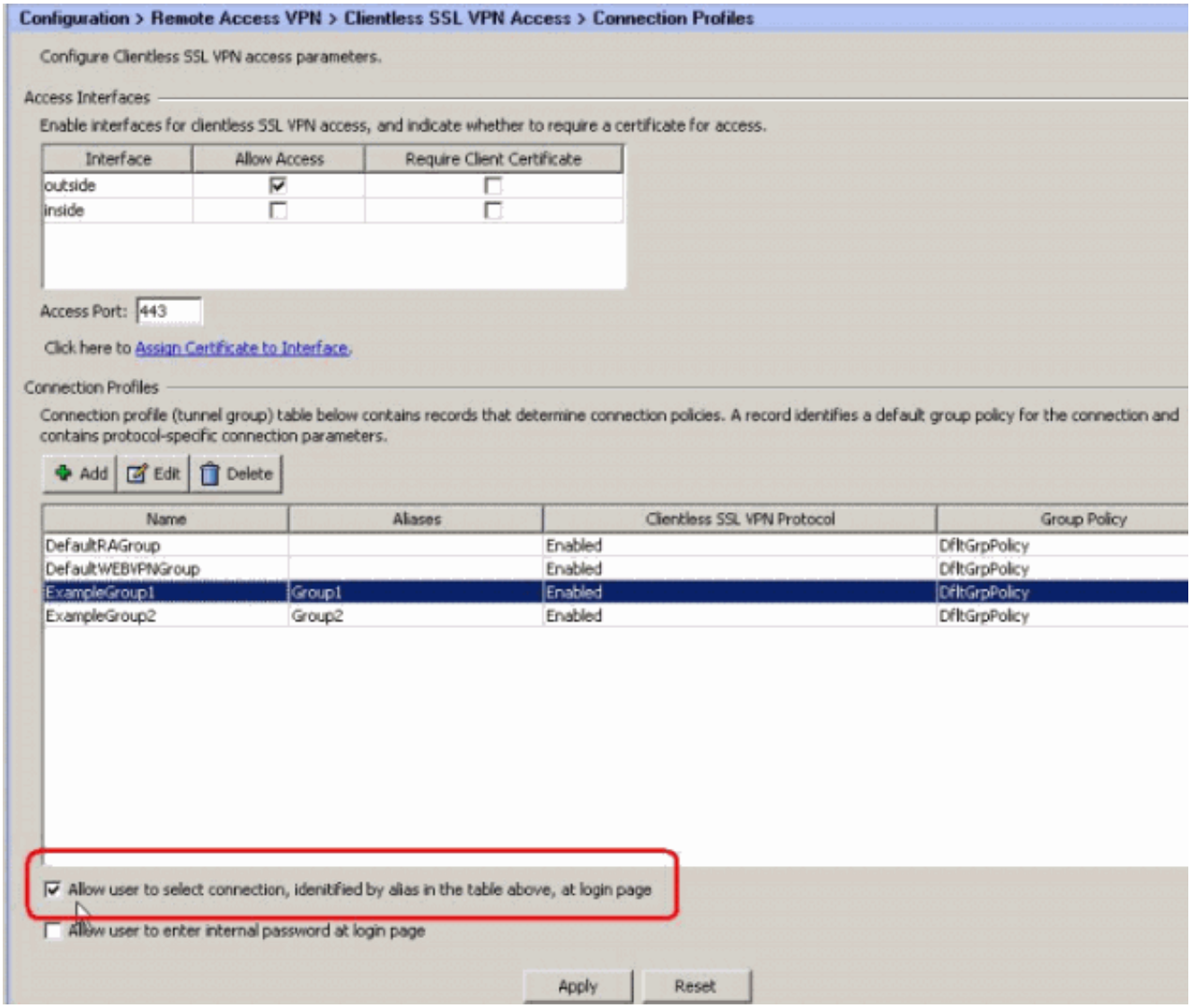
ASDM

Completare questa procedura per configurare un alias per un profilo di connessione (gruppo di tunnel) in ASDM. Ripetere l'operazione per ogni gruppo per il quale si desidera configurare un alias.

1. Scegliere **Configurazione > Accesso VPN SSL senza client > Profili di connessione**.
2. Selezionare un profilo di connessione e fare clic su **Modifica**.
3. Immettere un alias nel campo Alias.



4. Fare clic su **OK** e **Applicare** la modifica.
5. Nella finestra Profili di connessione, selezionare **Consenti all'utente di selezionare la connessione, identificata dall'alias nella tabella precedente, nella pagina di accesso**.



CLI

Utilizzare questi comandi dalla riga di comando per configurare un alias per un profilo di connessione (gruppo tunnel) e abilitare l'elenco a discesa del gruppo tunnel. Ripetere l'operazione per ogni gruppo per il quale si desidera configurare un alias.

```
ciscoasa#configure terminal
ciscoasa(config)#tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)#group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)#exit
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

Configurare un URL e abilitare l'elenco a discesa

In questa sezione vengono presentate le informazioni necessarie per configurare un URL per un profilo di connessione (gruppo tunnel) e quindi configurare gli URL in modo che vengano visualizzati nel menu a discesa Gruppo della pagina di accesso di WebVPN. Uno dei vantaggi dell'utilizzo di group-url rispetto a group-alias (elenco a discesa dei gruppi) consiste nel fatto che i nomi dei gruppi non vengono esposti come nel secondo metodo.

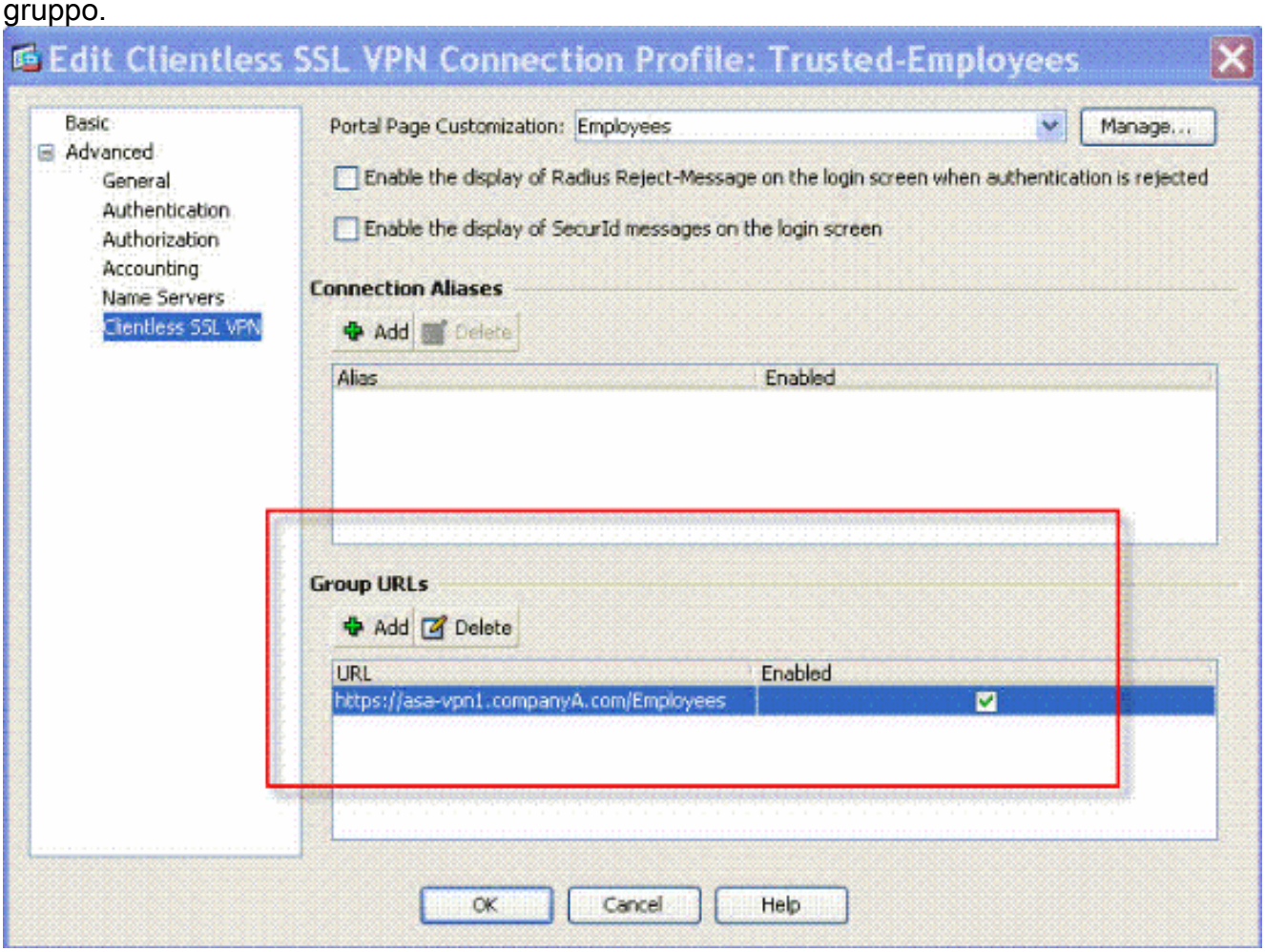
ASDM

Per specificare l'URL del gruppo in ASDM, è possibile procedere in due modi:

- Metodo di profilo - completamente operativoModificare il profilo AC e il campo <IndirizzoHost>.In Windows 2000/XP, il file del profilo predefinito (ad esempio, CiscoAnyConnectProfile.xml) si trova nella directory: C:\Documents and Settings\All Users\Dati applicazioni\Cisco\Cisco AnyConnect VPN Client\Profile.La posizione di Vista è leggermente diversa: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile.
- Immettere la stringa dell'URL del gruppo nel campo Connetti a.Sono supportati tre formati di stringhe URL di gruppo:https://asa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com (solo dominio, nessun percorso)

Completare questa procedura per configurare un URL per un profilo di connessione (gruppo di tunnel) in ASDM. Ripetere l'operazione per ciascun gruppo per il quale si desidera configurare un URL.

1. Scegliere **Configurazione > Accesso VPN SSL senza client > Profili di connessione>Avanzate>Pannello VPN SSL senza client**.
2. Selezionare un profilo di connessione e fare clic su **Modifica**.
3. Immettere un URL nel campo URL gruppo.



4. Fare clic su **OK** e **Applicare** la modifica.

CLI

Utilizzare questi comandi dalla riga di comando per configurare un URL per un profilo di connessione (gruppo tunnel) e abilitare l'elenco a discesa del gruppo tunnel. Ripetere l'operazione per ciascun gruppo per il quale si desidera configurare un URL.

```
ciscoasa#configure terminal

ciscoasa(config)#tunnel-group Trusted-Employees type remote-access

ciscoasa(config)#tunnel-group Trusted-Employees general-attributes

ciscoasa(config)#authentication-server-group (inside) LDAP-AD11

ciscoasa(config)#accounting-server-group RadiusACS12

ciscoasa(config)#default-group-policy Employees

ciscoasa(config)#tunnel-group Trusted-Employees webvpn-attributes

ciscoasa(config)#group-url https://asa-vpn1.companyA.com/Employees enable
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

Domande e risposte

Domanda:

Come configurare l'URL del gruppo se il gateway VPN ASA è dietro un dispositivo NAT?

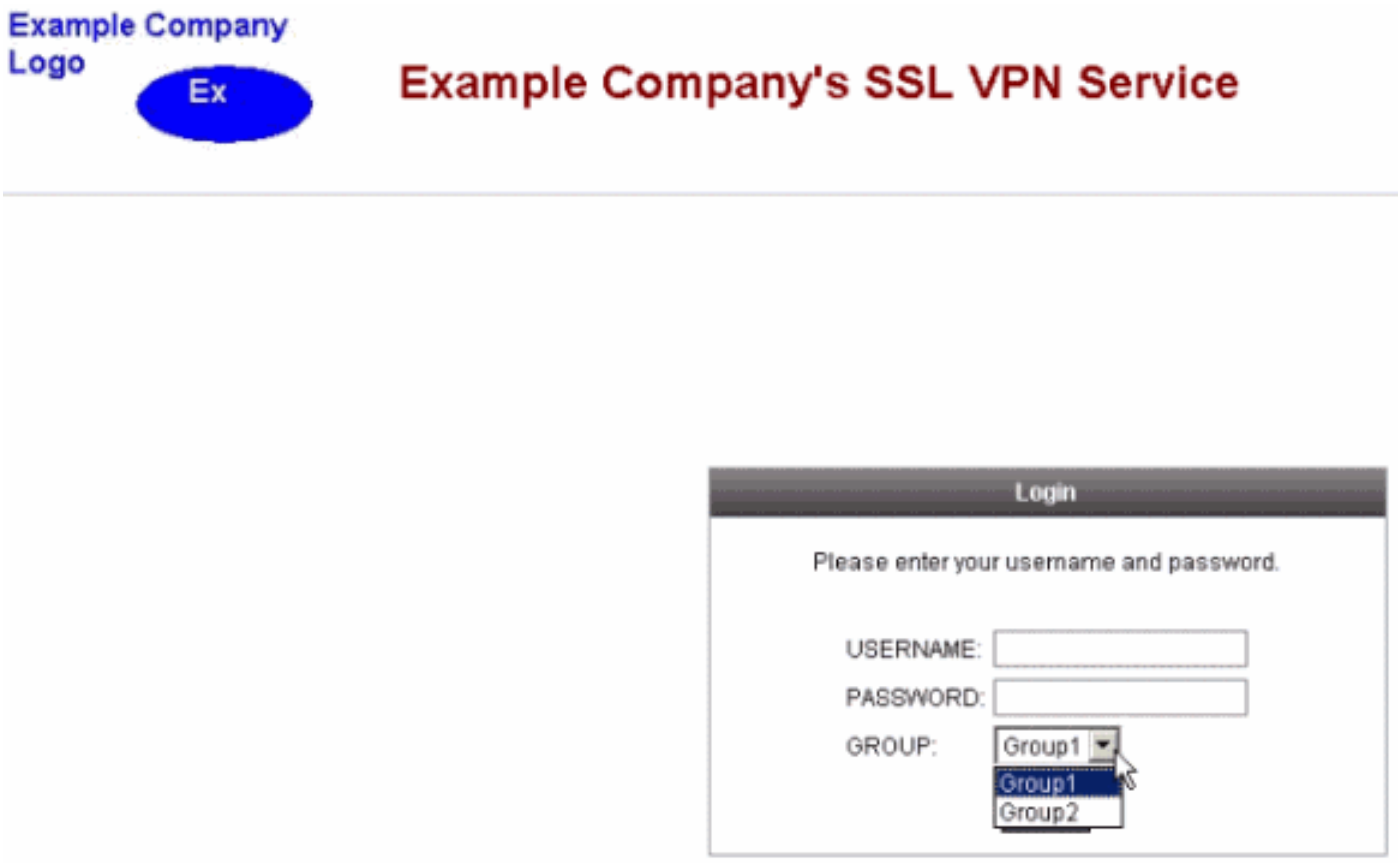
Risposta.

L'host o l'URL immesso dall'utente verrà utilizzato per il mapping del gruppo. Pertanto, è necessario usare l'indirizzo NAT e non l'indirizzo effettivo sull'interfaccia esterna dell'ASA. L'alternativa migliore è utilizzare il nome di dominio completo (FQDN) anziché l'indirizzo IP per il mapping di URL di gruppo.

Tutti i mapping vengono implementati a livello di protocollo HTTP (in base alle informazioni inviate dal browser) e un URL viene composto per eseguire il mapping dalle informazioni nelle intestazioni HTTP in ingresso. Il nome host o l'indirizzo IP vengono ricavati dall'intestazione host e il resto dell'URL dalla riga della richiesta HTTP. Ciò significa che l'host/URL immesso dall'utente verrà utilizzato per il mapping del gruppo.

Verifica

Andare alla pagina di accesso di WebVPN sull'appliance ASA per verificare che l'elenco a discesa sia abilitato e che gli alias vengano visualizzati.



Andare alla pagina di accesso di WebVPN sull'appliance ASA per verificare che l'elenco a discesa sia abilitato e che l'URL venga visualizzato.

Risoluzione dei problemi

- Se l'elenco a discesa non viene visualizzato, assicurarsi di averlo abilitato e che gli alias siano configurati. Gli utenti spesso eseguono una di queste operazioni, ma non l'altra.
- Accertarsi di connettersi all'URL di base dell'appliance ASA. L'elenco a discesa **non viene**

visualizzato se si esegue la connessione all'appliance ASA con un URL di gruppo, in quanto lo scopo dell'URL di gruppo è quello di eseguire la selezione del gruppo.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems