

ASA 8.x:사용자가 그룹 별칭 및 그룹-URL 방법을 통해 WebVPN 로그인 시 그룹을 선택할 수 있도록 허용

목차

[소개](#)

[사전 요구 사항](#)

[별칭 구성 및 드롭다운 활성화](#)

[ASDM](#)

[CLI](#)

[URL 구성 및 드롭다운 활성화](#)

[ASDM](#)

[CLI](#)

[Q 및 A](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

SSL VPN 사용자(AnyConnect/SVC 및 클라이언트리스 모두)는 다음 다양한 방법을 사용하여 액세스할 터널 그룹[ASDM(Adaptive Security Device Manager) 링에서 연결 프로파일]을 선택할 수 있습니다.

- 그룹 URL
- group-alias(로그인 페이지의 터널 그룹 드롭다운 목록)
- 인증서 맵(인증서를 사용하는 경우)

이 문서에서는 사용자가 WebVPN 서비스에 로그인할 때 드롭다운 메뉴를 통해 그룹을 선택할 수 있도록 ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다. 메뉴에 표시되는 그룹은 ASA에 구성된 실제 연결 프로파일(터널 그룹)의 별칭 또는 URL입니다. 이 문서에서는 연결 프로파일(터널 그룹)에 대한 별칭 및 URL을 생성한 다음 드롭다운을 표시하도록 구성하는 방법을 설명합니다. 이 컨피그레이션은 소프트웨어 버전 8.0(2)을 실행하는 ASA에서 ASDM 6.0(2)을 사용하여 수행됩니다.

참고: ASA 버전 7.2.x는 두 가지 방법을 지원합니다.group-url 및 group-alias 목록

참고: ASA 버전 8.0.x는 다음 세 가지 방법을 지원합니다.group-url, group-alias 및 certificate-maps입니다.

[사전 요구 사항](#)

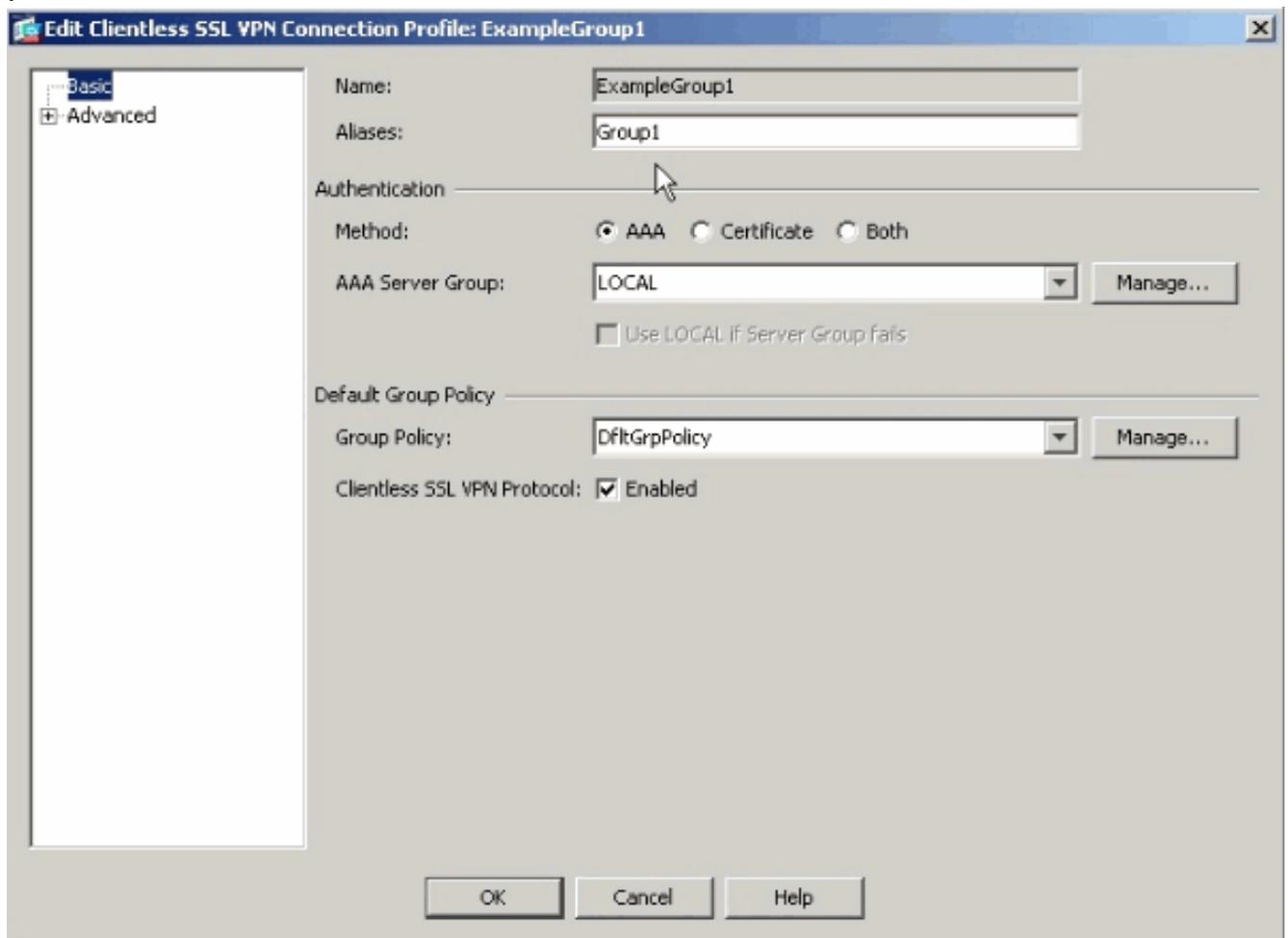
별칭 구성 및 드롭다운 활성화

이 섹션에서는 연결 프로파일(터널 그룹)에 대한 별칭을 구성한 다음 WebVPN 로그인 페이지의 Group(그룹) 드롭다운 메뉴에 해당 별칭을 표시하도록 구성하는 정보를 제공합니다.

ASDM

ASDM에서 연결 프로파일(터널 그룹)에 대한 별칭을 구성하려면 다음 단계를 완료합니다. 별칭을 구성하려는 각 그룹에 대해 필요에 따라 반복합니다.

1. Configuration(구성) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Connection Profiles(연결 프로파일)를 선택합니다.
2. 연결 프로파일을 선택하고 Edit를 클릭합니다.
3. 별칭 필드에 별칭을 입력합니다



4. 확인을 클릭하고 변경 사항을 적용합니다.
5. Connection Profiles(연결 프로파일) 창에서 Allow user to select connection(사용자 선택 허용)(위의 테이블에서 별칭으로 식별됨, 로그인 페이지)을 선택합니다

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Configure Clientless SSL VPN access parameters.

Access Interfaces
Enable interfaces for clientless SSL VPN access, and indicate whether to require a certificate for access.

Interface	Allow Access	Require Client Certificate
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

Click here to [Assign Certificate to Interface](#).

Connection Profiles
Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	Clientless SSL VPN Protocol	Group Policy
DefaultRAGroup		Enabled	DfltGrpPolicy
DefaultWEBVPGGroup		Enabled	DfltGrpPolicy
ExampleGroup1	Group1	Enabled	DfltGrpPolicy
ExampleGroup2	Group2	Enabled	DfltGrpPolicy

Allow user to select connection, identified by alias in the table above, at login page
 Allow user to enter internal password at login page

CLI

연결 프로파일(터널 그룹)에 대한 별칭을 구성하고 터널 그룹 드롭다운을 활성화하려면 명령줄에서 이 명령을 사용합니다. 별칭을 구성하려는 각 그룹에 대해 필요에 따라 반복합니다.

```
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
```

URL 구성 및 드롭다운 활성화

이 섹션에서는 연결 프로파일(터널 그룹)에 대한 URL을 구성한 다음 WebVPN 로그인 페이지의 Group(그룹) 드롭다운 메뉴에 해당 URL이 나타나도록 구성하는 정보를 제공합니다. group-url over group-alias(group 드롭다운)를 사용할 때의 한 가지 장점은 후자의 방법처럼 그룹 이름을 노출하지 않는다는 것입니다.

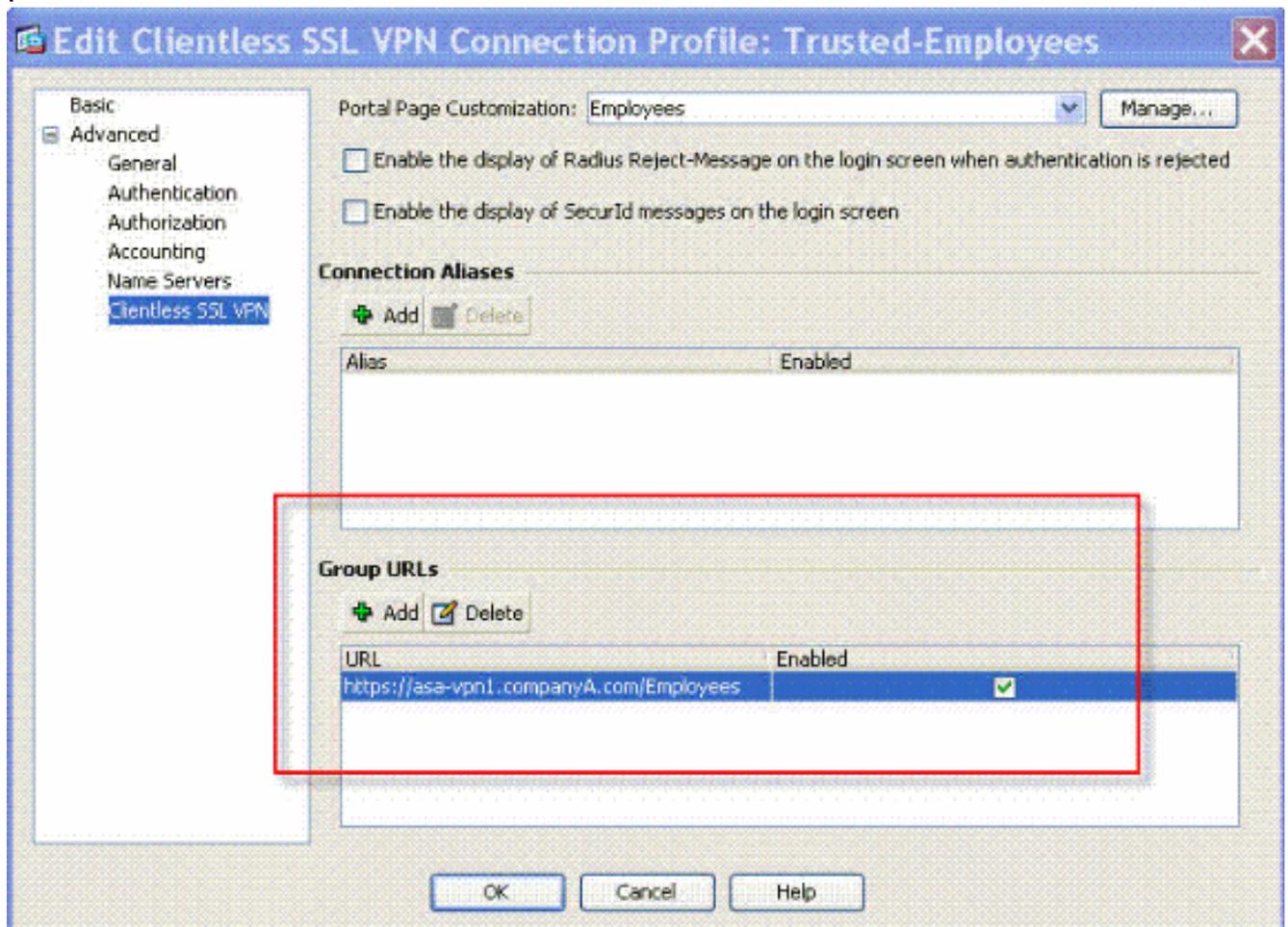
ASDM

ASDM에서 Group-URL을 지정하는 데 사용되는 두 가지 방법이 있습니다.

- 프로파일 방법 - 완전한 작동AC Profile(AC 프로필)을 수정하고 <HostAddress> 필드를 수정합니다.Windows 2000/XP에서 기본 프로파일 파일(예: CiscoAnyConnectProfile.xml)은 다음 디렉토리에 있습니다.C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile을 참조하십시오.Vista의 위치는 약간 다릅니다 .C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile을 참조하십시오.
- 연결 대상 필드에 그룹 URL 문자열을 입력합니다.그룹 URL 문자열의 3가지 형식이 지원됩니다.https://asa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com(도메인 전용, 경로 없음)

ASDM에서 연결 프로파일(터널 그룹)에 대한 URL을 구성하려면 다음 단계를 완료합니다.URL을 구성하려는 각 그룹에 대해 필요에 따라 반복합니다.

1. Configuration(구성) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Connection Profiles(연결 프로파일)>Advanced(고급)>Clientless SSL VPN(클라이언트리스 SSL VPN) 패널을 선택합니다.
2. 연결 프로파일을 선택하고 Edit를 클릭합니다.
3. Group URLs(그룹 URL) 필드에 URL을 입력합니다



4. 확인을 클릭하고 변경 사항을 적용합니다.

CLI

연결 프로파일(터널 그룹)에 대한 URL을 구성하고 터널 그룹 드롭다운을 활성화하려면 명령줄에서 다음 명령을 사용합니다.URL을 구성하려는 각 그룹에 대해 필요에 따라 반복합니다.

```
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
```

Q 및 A

질문:

ASA VPN 게이트웨이가 NAT 디바이스 뒤에 있는 경우 group-url을 어떻게 구성합니까?

답변:

사용자가 입력하는 호스트/URL은 그룹 매핑에 사용됩니다. 따라서 ASA의 외부 인터페이스에서 실제 주소가 아니라 NAT 주소를 사용해야 합니다. 가장 좋은 방법은 그룹 URL 매핑에 IP 주소 대신 FQDN을 사용하는 것입니다.

모든 매핑은 HTTP 프로토콜 레벨(브라우저에서 전송하는 정보에 따라)에 구현되며, URL은 수신 HTTP 헤더의 정보로부터 매핑되도록 구성됩니다. 호스트 이름 또는 IP는 호스트 헤더에서, 나머지 URL은 HTTP 요청 라인에서 가져옵니다. 즉, 사용자가 입력하는 호스트/URL이 그룹 매핑에 사용됩니다.

다음을 확인합니다.

ASA의 WebVPN 로그인 페이지로 이동하여 드롭다운이 활성화되었고 별칭이 표시되는지 확인합니다.



Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP:

- Group1
- Group2

ASA의 WebVPN 로그인 페이지로 이동하여 드롭다운이 활성화되었고 URL이 나타나는지 확인합니다.



문제 해결

- 드롭다운 목록이 나타나지 않으면 해당 목록을 활성화했으며 해당 별칭이 구성되었는지 확인하십시오. 사용자는 이러한 작업 중 하나를 수행하지만 다른 작업은 수행하지 않습니다.
- ASA의 기본 URL에 연결하고 있는지 확인합니다. group-url의 목적은 그룹 선택을 수행하기 위

한 것이므로 group-url을 사용하여 ASA에 연결하는 경우 드롭다운 목록이 나타나지 않습니다.

관련 정보

- [Cisco ASA 5500 Series Adaptive Security Appliance](#)
- [기술 지원 및 문서 - Cisco Systems](#)