ASDM을 사용하는 ASA의 SVC(SSL VPN Client) 컨피그레이션 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[네트워크 다이어그램](#)
[사전 컨피그레이션 작업](#)
[표기 규칙](#)
[ASA에서 SSL VPN 클라이언트 구성](#)
[1단계. ASA에서 WebVPN 액세스 활성화](#)
[2단계. ASA에 SSL VPN 클라이언트 설치 및 활성화](#)
[3단계. 클라이언트에 SVC 설치 사용](#)
[4단계. Rekey 매개 변수 사용](#)
[결과](#)
[컨피그레이션 사용자 지정](#)
[1단계. 사용자 지정 그룹 정책 생성](#)
[2단계. 사용자 지정 터널 그룹 생성](#)
[3단계. 사용자를 생성하고 사용자 지정 그룹 정책에 해당 사용자를 추가합니다](#)
[다음을 확인합니다.](#)
[인증](#)
[설정](#)
[명령](#)
[문제 해결](#)
[SVC 오류](#)
[SVC에서 ASA와의 보안 세션을 설정했습니까?](#)
[보안 세션이 설정 및 종료되었습니까?](#)
[WebVPN 프로필에서 IP 풀 확인](#)
[팁](#)
[명령](#)
[관련 정보](#)

소개

SSL(Secure Socket Layer) VPN(Virtual Private Network) 기술을 사용하면 다음 방법 중 하나를 사용하여 모든 위치에서 내부 기업 네트워크에 안전하게 연결할 수 있습니다.

- Clientless SSL VPN (WebVPN)(클라이언트리스 SSL VPN(WebVPN)) - 기업 LAN(Local-Area Network)에서 HTTP 또는 HTTPS 웹 서버에 액세스하려면 SSL 사용 웹 브라우저가 필

요한 원격 클라이언트를 제공합니다. 또한 클라이언트리스 SSL VPN은 CIFS(Common Internet File System) 프로토콜을 통해 Windows 파일 브라우징에 대한 액세스를 제공합니다. OWA(Outlook Web Access)는 HTTP 액세스의 예입니다.

클라이언트리스 SSL VPN에 대한 자세한 내용은 ASA 컨피그레이션 예의 클라이언트리스 SSL VPN(WebVPN)을 참조하십시오.

- Thin-Client SSL VPN(Port Forwarding)(씬 클라이언트 SSL VPN(포트 전달)) - 작은 Java 기반 애플릿을 다운로드하고 고정 포트 번호를 사용하는 TCP(Transmission Control Protocol) 애플리케이션에 대한 보안 액세스를 허용하는 원격 클라이언트를 제공합니다. 보안 액세스의 예로는 POP3(Post Office Protocol), SMTP(Simple Mail Transfer Protocol), IMAP(Internet Message Access Protocol), ssh(Secure Shell), 텔넷 등이 있습니다. 로컬 시스템의 파일이 변경되므로 이 방법을 사용하려면 사용자에게 로컬 관리 권한이 있어야 합니다. 일부 FTP(File Transfer Protocol) 애플리케이션과 같이 동적 포트 할당을 사용하는 애플리케이션에서는 이 SSL VPN 방법이 작동하지 않습니다.

  씬 클라이언트 SSL VPN에 대한 자세한 내용은 ASDM을 사용하는 ASA의 씬 클라이언트 SSL VPN(WebVPN) 컨피그레이션 예를 참조하십시오.

  참고: UDP(User Datagram Protocol)는 지원되지 않습니다.

- SSL VPN Client(터널 모드) - 소규모 클라이언트를 원격 워크스테이션에 다운로드하고 내부 기업 네트워크의 리소스에 대한 완전한 보안 액세스를 허용합니다. SVC(SSL VPN Client)를 원격 워크스테이션에 영구적으로 다운로드하거나, 보안 세션이 닫힌 후 클라이언트를 제거할 수 있습니다.

이 문서에서는 ASDM(Adaptive Security Device Manager)을 사용하여 ASA(Adaptive Security Appliance)에서 SVC를 구성하는 방법에 대해 설명합니다. 이 컨피그레이션의 결과 명령줄은 Results 섹션에 나열되어 있습니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- SVC가 Cisco Adaptive Security Appliance Software Version 7.1 이상에서 지원 시작
- 모든 원격 워크스테이션에 대한 로컬 관리 권한
- 원격 워크스테이션의 Java 및 ActiveX 컨트롤
- 포트 443은 연결 경로를 따라 어느 곳에서도 차단되지 않습니다

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- Cisco Adaptive Security Appliance 5510 시리즈
- Microsoft Windows XP Professional SP 2

이 문서의 정보는 랩 환경에서 개발되었습니다. 이 문서에서 시작된 모든 장치가 기본 구성으로 재설정되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다. 이 구성에 사용된 모든 IP 주소는 랩 환경의 RFC 1918 주소에서 선택되었습니다. 이러한 IP 주소는 인터넷에서 라우팅할 수 없으며 테스트 목적으로만 사용됩니다.

네트워크 다이어그램

이 문서에서는 이 섹션에 설명된 네트워크 컨피그레이션을 사용합니다.

원격 사용자는 SSL 지원 웹 브라우저를 사용하여 ASA의 IP 주소에 연결합니다. 인증에 성공하면 SVC가 클라이언트 컴퓨터에 다운로드되고 사용자는 암호화된 보안 세션을 사용하여 기업 네트워크에서 허용된 모든 리소스에 액세스할 수 있습니다.

사전 컨피그레이션 작업

시작하기 전에 다음 작업을 완료하십시오.

- ASDM에서 ASA를 구성하도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

  ASDM 애플리케이션에 액세스하려면 관리 스테이션에서 SSL 지원 웹 브라우저를 사용하고 ASA 디바이스의 IP 주소를 입력합니다. 예: https:// inside_ip_address 여기서 inside_ip_address는 ASA의 주소입니다. ASDM이 로드되면 SVC 컨피그레이션을 시작할 수 있습니다.

- Cisco Software Download(등록된 고객만 해당) 웹 사이트에서 ASDM 애플리케이션에 액세스하는 관리 스테이션의 로컬 하드 드라이브로 SSL VPN 클라이언트 패키지(sslclient-win*.pkg)를 다운로드합니다.

포트 번호를 변경하지 않는 한 동일한 ASA 인터페이스에서 WebVPN 및 ASDM을 활성화할 수 없습니다. 두 기술이 동일한 디바이스에서 동일한 포트(포트 443)를 사용하도록 하려면 내부 인터페이스에서 ASDM을 활성화하고 외부 인터페이스에서 WebVPN을 활성화할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco Technical Tips Conventions를 참조하십시오.

ASA에서 SSL VPN 클라이언트 구성

ASA에서 SSL VPN 클라이언트를 구성하는 절차는 다음과 같습니다.

1. ASA에서 WebVPN 액세스 활성화
2. ASA에 SSL VPN 클라이언트 설치 및 활성화
3. 클라이언트에 SVC 설치 사용
4. 키 재설정 매개변수 활성화

1단계. ASA에서 WebVPN 액세스 활성화

ASA에서 WebVPN 액세스를 활성화하는 절차는 다음과 같습니다.

1. ASDM 애플리케이션 내에서 Configuration(컨피그레이션)을 클릭한 다음 VPN(VPN)을 클릭합니다.
2. WebVPN을 확장하고 WebVPN Access를 선택합니다.
3. WebVPN을 활성화할 인터페이스를 선택하고 Enable(활성화)을 클릭합니다.

2단계. ASA에 SSL VPN 클라이언트 설치 및 활성화

ASA에 SSL VPN 클라이언트를 설치하고 활성화하는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션)을 클릭한 다음 VPN(VPN)을 클릭합니다.
2. 탐색 창에서 WebVPN을 확장하고 SSL VPN Client(SSL VPN 클라이언트)를 선택합니다.
3. Add(추가)를 클릭합니다.

   Add SSL VPN Client Image(SSL VPN 클라이언트 이미지 추가) 대화 상자가 나타납니다.
4. Upload(업로드) 버튼을 클릭합니다.

   Upload Image(이미지 업로드) 대화 상자가 나타납니다.
5. [로컬 파일 찾아보기] 단추를 클릭하여 로컬 컴퓨터에서 파일을 찾거나 [플래시 찾아보기] 단추를 클릭하여 플래시 파일 시스템에서 파일을 찾습니다.
6. 업로드할 클라이언트 이미지 파일을 찾은 다음 OK(확인)를 클릭합니다.
7. Upload File(파일 업로드)을 클릭한 다음 Close(닫기)를 클릭합니다.
8. 클라이언트 이미지가 플래시에 로드되면 Enable SSL VPN Client(SSL VPN 클라이언트 활성화) 확인란을 선택한 다음 Apply(적용)를 클릭합니다.

   참고: 오류 메시지가 표시되면 WebVPN 액세스가 활성화되어 있는지 확인합니다. 탐색 창에서 WebVPN을 확장하고 WebVPN Access(WebVPN 액세스)를 선택합니다. 액세스를 구성할 인터페이스를 선택하고 Enable을 클릭합니다.
9. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

3단계. 클라이언트에 SVC 설치 사용

클라이언트에서 SVC 설치를 활성화하는 절차는 다음과 같습니다.

1. 탐색 창에서 IP Address Management(IP 주소 관리)를 확장하고 IP Pools(IP 풀)를 선택합니다.
2. Add(추가)를 클릭하고 Name(이름), Starting IP Address(시작 IP 주소), Ending IP Address(종료 IP 주소) 및 Subnet Mask(서브넷 마스크) 필드에 값을 입력합니다. Starting IP Address(시작 IP 주소) 및 Ending IP Address(종료 IP 주소) 필드에 입력하는 IP 주소는 내부 네트워크의 서브넷에서 가져와야 합니다.
3. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.
4. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.
5. 탐색 창에서 IP Address Management(IP 주소 관리)를 확장하고 Assignment(할당)를 선택합니다.
6. Use internal address pools(내부 주소 풀 사용) 확인란을 선택한 다음 Use authentication server(인증 서버 사용) 및 Use DHCP(DHCP 사용) 확인란의 선택을 취소합니다.
7. 적용을 클릭합니다.
8. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.
9. 탐색 창에서 General(일반)을 확장하고 Tunnel Group(터널 그룹)을 선택합니다.
10. 관리할 터널 그룹을 선택하고 Edit를 클릭합니다.
11. Client Address Assignment(클라이언트 주소 할당) 탭을 클릭하고 Available Pools(사용 가능한 풀) 목록에서 새로 생성된 IP 주소 풀을 선택합니다.
12. Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.
13. ASDM 애플리케이션 창에서 Apply를 클릭합니다.
14. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

4단계. Rekey 매개 변수 사용

rekey 매개변수를 활성화하려면

1. 탐색 창에서 General(일반)을 확장하고 Group Policy(그룹 정책)를 선택합니다.
2. 이 클라이언트 그룹에 적용할 정책을 선택하고 Edit를 클릭합니다.
3. General(일반) 탭에서 Tunneling Protocols Inherit(터널링 프로토콜 상속) 확인란의 선택을 취소하고 WebVPN 확인란을 선택합니다.

4. WebVPN 탭을 클릭하고 SSLVPN Client 탭을 클릭한 다음 다음 옵션을 선택합니다.

    a. Use SSL VPN Client(SSL VPN 클라이언트 사용) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 Optional(선택 사항) 라디오 버튼을 클릭합니다.

    이 옵션을 사용하면 원격 클라이언트가 SVC를 다운로드할지 여부를 선택할 수 있습니다. Always(항상) 선택을 선택하면 각 SSL VPN 연결 중에 SVC가 원격 워크스테이션에 다운로드됩니다.

    b. Keep Installer on Client System(클라이언트 시스템에 설치 프로그램 유지) 옵션의 경우 Inherit(상속) 확인란의 선택을 취소하고 Yes(예) 라디오 버튼을 클릭합니다.

    이 작업을 수행하면 SVC 소프트웨어가 클라이언트 컴퓨터에 남아 있을 수 있습니다. 따라서 ASA는 연결이 설정될 때마다 SVC 소프트웨어를 클라이언트에 다운로드할 필요가 없습니다. 이 옵션은 기업 네트워크에 자주 액세스하는 원격 사용자에게 적합합니다.

    c. Renegotiation Interval(재협상 간격) 옵션의 경우 Inherit(상속) 상자의 선택을 취소하고 Unlimited(무제한) 확인란의 선택을 취소한 후 재키가 발생할 때까지의 시간(분)을 입력합니다.

    키의 유효 기간에 제한을 설정하여 보안을 강화합니다.

    d. Renegotiation Method(재협상 방법) 옵션에서 Inherit(상속) 확인란의 선택을 취소하고 SSL 라디오 버튼을 클릭합니다. 재협상에서는 재협상을 위해 명시적으로 생성된 새 터널 또는 현재 SSL 터널을 사용할 수 있습니다.

    이 이미지에 표시된 대로 SSL VPN 클라이언트 특성을 구성해야 합니다.

5. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.

6. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

결과

ASDM에서는 다음과 같은 명령줄 컨피그레이션을 생성합니다.

시스코아사
<#root> ciscoasa(config)# **show run** ASA Version 7.2(1) ! hostname ciscoasa domain-name cisco.com enable password 9jNfZuG3TC5tCVH0 encrypted names dns-guard !

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!

!--- Group Policy Statements

group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

!--- Enable the SVC for WebVPN

 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable
http 10.2.2.0 255.255.255.0 inside
!
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Tunnel Group and Group Policy using the defaults here

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool CorporateNet
```

```
 default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
!
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global

!--- Enable webvpn and the select the SVC client

webvpn
 enable outside
 svc image disk0:/sslclient-win-1.1.1.164.pkg 1
 svc enable

!--- Provide list for access to resources

 url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
 url-list ServerList "BrowseServer" cifs://10.2.2.2 2
 tunnel-group-list enable

prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

컨피그레이션 사용자 지정

Configure the SSL VPN Client on an ASA(ASA에서 SSL VPN 클라이언트 구성)에 설명된 절차는 이 이미지에 표시된 대로 그룹 정책(GroupPolicy1) 및 터널 그룹(DefaultWebVPNGroup)에 ASA 기본 이름을 사용합니다.

이 절차에서는 사용자 지정 그룹 정책 및 터널 그룹을 만들고 조직의 보안 정책에 따라 함께 연결하는 방법에 대해 설명합니다.

구성을 사용자 지정하는 절차는 다음과 같습니다.

1. 사용자 지정 그룹 정책 생성
2. 사용자 지정 터널 그룹 생성
3. 사용자를 생성하고 사용자 지정 그룹 정책에 해당 사용자를 추가합니다

1단계. 사용자 지정 그룹 정책 생성

사용자 지정 그룹 정책을 만드는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션)을 클릭한 다음 VPN(VPN)을 클릭합니다.
2. General(일반)을 확장하고 Group Policy(그룹 정책)를 선택합니다.
3. Add(추가)를 클릭하고 Internal Group Policy(내부 그룹 정책)를 선택합니다.
4. Name 필드에 그룹 정책의 이름을 입력합니다.

   이 예에서는 그룹 정책 이름이 SalesGroupPolicy로 변경되었습니다.
5. General(일반) 탭에서 Tunneling Protocols Inherit(터널링 프로토콜 상속) 확인란의 선택을 취소하고 WebVPN 확인란을 선택합니다.
6. WebVPN 탭을 클릭한 다음 SSLVPN 클라이언트 탭을 클릭합니다.

   이 대화 상자에서는 SSL VPN 클라이언트의 동작을 선택할 수도 있습니다.
7. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.
8. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

2단계. 사용자 지정 터널 그룹 생성

사용자 지정 터널 그룹을 생성하는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션) 버튼을 클릭한 다음 VPN(VPN)을 클릭합니다.
2. General(일반)을 확장하고 Tunnel Group(터널 그룹)을 선택합니다.
3. Add(추가)를 클릭하고 WebVPN Access(웹 VPN 액세스)를 선택합니다.
4. Name 필드에 터널 그룹의 이름을 입력합니다.

   이 예에서는 터널 그룹 이름이 SalesForceGroup으로 변경되었습니다.
5. Group Policy(그룹 정책) 드롭다운 화살표를 클릭하고 새로 만든 그룹 정책을 선택합니다.

이제 그룹 정책 및 터널 그룹이 연결됩니다.

6. Client Address Assignment(클라이언트 주소 할당) 탭을 클릭하고 DHCP Server(DHCP 서버) 정보를 입력하거나 로컬에서 생성된 IP 풀에서 선택합니다.
7. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.
8. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

3단계. 사용자를 생성하고 사용자 지정 그룹 정책에 해당 사용자를 추가합니다

사용자를 생성하고 해당 사용자를 사용자 지정 그룹 정책에 추가하는 절차는 다음과 같습니다.

1. Configuration(컨피그레이션)을 클릭한 다음 VPN(VPN)을 클릭합니다.
2. General(일반)을 확장하고 Users(사용자)를 선택합니다.
3. Add(추가)를 클릭하고 사용자 이름 및 암호 정보를 입력합니다.
4. VPN Policy(VPN 정책) 탭을 클릭합니다. 새로 생성한 그룹 정책이 Group Policy(그룹 정책) 필드에 표시되는지 확인합니다.

   이 사용자는 새 그룹 정책의 모든 특성을 상속합니다.
5. OK(확인)를 클릭한 다음 Apply(적용)를 클릭합니다.
6. Save(저장)를 클릭한 다음 Yes(예)를 클릭하여 변경 사항을 적용합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

인증

SSL VPN 클라이언트에 대한 인증은 다음 방법 중 하나를 사용하여 수행됩니다.

- Cisco Secure ACS Server(Radius)
- NT 도메인
- 액티브 디렉토리
- 일회용 비밀번호
- 디지털 인증서
- 스마트 카드
- 로컬 AAA 인증

이 문서에서는 ASA 디바이스에서 생성된 로컬 계정을 사용합니다.

참고: Adaptive Security Appliance에 동일한 CA를 공유하는 여러 신뢰 지점이 있는 경우 CA를 공유하는 이러한 신뢰 지점 중 하나만 사용자 인증서의 유효성 검사에 사용할 수 있습니다.

설정

원격 클라이언트를 사용하여 ASA에 연결하려면 SSL 활성화 웹 브라우저의 주소 필드에 https://ASA_outside_address을 입력합니다. ASA_outside_address는 ASA의 외부 IP 주소입니다. 컨피그레이션에 성공하면 Cisco Systems SSL VPN Client(Cisco Systems SSL VPN 클라이언트) 창이 나타납니다.

참고: Cisco Systems SSL VPN Client(Cisco Systems SSL VPN 클라이언트) 창은 ASA에서 인증서를 승인하고 SSL VPN 클라이언트를 원격 스테이션에 다운로드한 후에만 나타납니다. 창이 표시되지 않으면 최소화되지 않았는지 확인합니다.

명령

여러 show 명령이 WebVPN과 연결됩니다. CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 표시할 수 있습니다. show 명령에 대한 자세한 내용은 WebVPN 구성 확인을 참조하십시오.

참고: Output Interpreter Tool(등록된 고객만 해당)(OIT)은 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결합니다.

SVC 오류

문제

인증 중에 다음과 같은 오류 메시지가 표시될 수 있습니다.

```
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires
re-authentication and must be restarted manually. Close all sensitive networked
applications."
```

솔루션

방화벽 서비스가 PC에서 실행 중이면 인증이 중단될 수 있습니다. 서비스를 중지하고 클라이언트를 다시 연결합니다.

SVC에서 ASA와의 보안 세션을 설정했습니까?

SSL VPN 클라이언트가 ASA와 보안 세션을 설정했는지 확인하려면 다음을 수행합니다.

1. Monitoring을 클릭합니다.
2. VPN Statistics(VPN 통계)를 확장하고 Sessions(세션)를 선택합니다.
3. Filter By(필터링 기준) 드롭다운 메뉴에서 SSL VPN Client(SSL VPN 클라이언트)를 선택하고 Filter(필터) 버튼을 클릭합니다.

   컨피그레이션이 세션 목록에 나타나야 합니다.

보안 세션이 설정 및 종료되었습니까?

세션이 성공적으로 설정 및 종료되고 있는지 확인하기 위해 실시간 로그를 볼 수 있습니다. 세션 로그를 보려면

1. Monitoring(모니터링)을 클릭한 다음 Logging(로깅)을 클릭합니다.
2. 실시간 로그 뷰어 또는 로그 버퍼를 선택한 다음 보기를 클릭합니다.

   참고: 특정 주소의 세션만 표시하려면 주소로 필터링합니다.

WebVPN 프로필에서 IP 풀 확인

```
%ASA-3-722020: Group group User user-name IP IP_address  No address
available for SVC connection
```

SVC 연결에 할당할 수 있는 주소가 없습니다. 따라서 프로필에서 IP 풀 주소를 할당합니다.

새 연결 프로파일을 생성하는 경우 이 연결 프로파일에 액세스하기 위해 별칭 또는 그룹 URL을 구성합니다. 그렇지 않은 경우 모든 SSL 시도가 IP 풀이 연결되지 않은 기본 WebVPN 연결 프로파일에 도달합니다. 기본 연결 프로파일을 사용하도록 설정하고 그 위에 IP 풀을 둡니다.

팁

- 원격 클라이언트에 할당한 IP 주소 풀에서 라우팅이 제대로 작동하는지 확인합니다. 이 IP 주소 풀은 LAN의 서브넷에서 가져와야 합니다. DHCP 서버 또는 인증 서버를 사용하여 IP 주소를 할당할 수도 있습니다.
- ASA는 기본 터널 그룹(DefaultWebVPNGroup) 및 기본 그룹 정책(GroupPolicy1)을 생성합니다. 새 그룹 및 정책을 생성하는 경우 네트워크의 보안 정책에 따라 값을 적용해야 합니다.
- CIFS를 통한 Windows 파일 브라우징을 활성화하려면 Configuration(구성) > VPN > WebVPN > Servers and URLs(서버 및 URL) 아래에 WINS(NBNS) 서버를 입력합니다. 이 기술은 CIFS

선택을 사용합니다.

명령

여러 debug 명령이 WebVPN과 연결됩니다. 이러한 명령에 대한 자세한 내용은 WebVPN 디버그 명령 사용을 참조하십시오.

참고: debug 명령을 사용하면 Cisco 디바이스에 악영향을 미칠 수 있습니다. debug 명령을 사용하기 전에 debug 명령에 대한 중요한 정보를 참조하십시오.

관련 정보

- ASA의 클라이언트리스 SSL VPN(WebVPN) 컨피그레이션 예
- ASDM을 사용하는 ASA의 씬 클라이언트 SSL VPN(WebVPN) 컨피그레이션 예
- ASDM 및 NTLMv1 컨피그레이션 예를 사용한 WebVPN 및 Single Sign-on을 사용하는 ASA
- Cisco ASA 5500 Series Adaptive Security Appliance
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.