ASA:다중 컨텍스트 모드 AnyConnect(원격 액세스) VPN

소개

이 문서에서는 CLI를 사용하여 다중 컨텍스트(MC) 모드의 Cisco ASA(Adaptive Security Appliance) 방화벽에서 RA(Remote Access) VPN(Virtual Private Network)을 구성하는 방법에 대해 설명합니다.RA VPN과 관련하여 Cisco ASA가 지원되는 다중 컨텍스트 모드/지원되지 않는 기능 및 라이센싱 요구 사항을 보여줍니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA AnyConnect SSL 컨피그레이션
- ASA 다중 컨텍스트 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AnyConnect Secure Mobility Client 버전 4.4.00243
- ASA5525 with ASA Software 버전 9.6(2) 2개

참고: Cisco 소프트웨어 다운로드에서 AnyConnect VPN 클라이언트 패키지를 다운로드합니다(등록된 고객만 해당).

참고:이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

다중 컨텍스트는 동일한 하드웨어에서 여러 개의 독립적인 애플리케이션 복제본을 동시에 실행할 수 있도록 하는 가상화 형태이며, 각 복제본(또는 가상 디바이스)은 사용자에게 별도의 물리적 디바이스로 표시됩니다.이를 통해 단일 ASA가 여러 개별 사용자에게 여러 ASA로 표시될 수 있습니다.ASA 제품군은 최초 릴리스 이후 가상 방화벽을 지원합니다.그러나 ASA에서는 원격 액세스에 대한 가상화 지원이 없었습니다.9.0 릴리스에는 다중 컨텍스트에 대한 VPN LAN2LAN(L2L) 지원이 추가되었습니다.

참고:9.5.2에서 ASA에 대한 VPN RA(Remote Access) 연결을 위한 멀티 컨텍스트 기반 가상화 지원

9.6.2부터 Flash 가상화 지원이 있으므로 상황당 Anyconnect 이미지를 사용할 수 있습니다.

다중 컨텍스트의 기능 기록

ASA 9.6(2)에 추가된 새로운 기능

기능	설명
다중 컨텍스트 모드의 사전 채우기/사용자 이름-인증서 기능	AnyConnect SSL 지원이 확장되어 이전에는 단일 모드에서만 사용할 수 있었 전 채우기/사용자 이름-인증서 기능 CLI도 다중 컨텍스트 모드에서도 활성화 있습니다.
원격 액세스 VPN을 위한 플래시 가상화	다중 상황 모드의 원격 액세스 VPN은 이제 플래시 가상화를 지원합니다.각 컨 트에는 사용 가능한 전체 플래시를 기반으로 전용 스토리지 공간과 공유 스토 공간이 있을 수 있습니다.
멀티 컨텍스트 디바이스에서 지원되는 AnyConnect 클라이언트 프로파일	AnyConnect 클라이언트 프로파일은 멀티 컨텍스트 디바이스에서 지원됩니다 .ASDM을 사용하여 새 프로필을 추가하려면 AnyConnect Secure Mobility Clie 리스 4.2.00748 또는 4.3.03013 이상이 있어야 합니다.
다중 컨텍스트 모드에서 AnyConnect 연결을 위한 스테이트풀 장애 조치	이제 다중 컨텍스트 모드의 AnyConnect 연결에 대해 스테이트풀 장애 조치가 됩니다.
다중 컨텍스트 모드에서 원격 액세스 VPN DAP(Dynamic Access Policy)가 지원됩니다.	이제 다중 컨텍스트 모드에서 컨텍스트당 DAP를 구성할 수 있습니다.
원격 액세스 VPN CoA(Change of Authorization)는 다중 컨텍스트 모드에서 지원됩니다.	이제 다중 컨텍스트 모드에서 컨텍스트당 CoA를 구성할 수 있습니다.
다중 컨텍스트 모드에서 원격 액세스 VPN 현지화가 지원됩니다.	로컬라이제이션은 전역적으로 지원됩니다.서로 다른 컨텍스트에서 공유되는 라이제이션 파일 세트는 하나만 있습니다.
컨텍스트당 패킷 캡처 스토리지가 지원됩니다.	이 기능의 목적은 사용자가 캡처를 컨텍스트에서 직접 외부 스토리지로 또는 시의 컨텍스트 전용 스토리지로 복사할 수 있도록 하는 것입니다.이 기능을 사 면 컨텍스트 내에서 와이어-샤크와 같은 외부 패킷 캡처 툴에 원시 캡처를 복사 수도 있습니다.

ASA 9.5(2)의 기능

기능	설명
AnyConnect 4.x 이상(SSL VPN만 해당 ;IKEv2 지원 없음)	ASA에 대한 VPN RA(Remote Access) 연결을 위한 멀티 컨텍스트 기반 가상화 지
중앙 집중식 AnyConnect 이미지 컨피그레이션	• 플래시 스토리지는 가상화되지 않습니다. • AnyConnect 이미지는 관리 컨텍스트에서 전역적으로 구성되며 컨피그레이션 든 컨텍스트에 적용됩니다
AnyConnect 이미지 업그레이드	AnyConnect 클라이언트 프로파일은 멀티 컨텍스트 디바이스에서 지원됩니다.ASD 사용하여 새 프로필을 추가하려면 AnyConnect Secure Mobility Client 릴리스 4.2.0 또는 4.3.03013 이상이 있어야 합니다.
AnyConnect 연결을 위한 컨텍스트 리소스 관리	• 컨텍스트당 최대 라이센스 사용을 제어하는 구성 가능 • 컨텍스트당 라이센스 버스팅을 허용하는 구성 가능

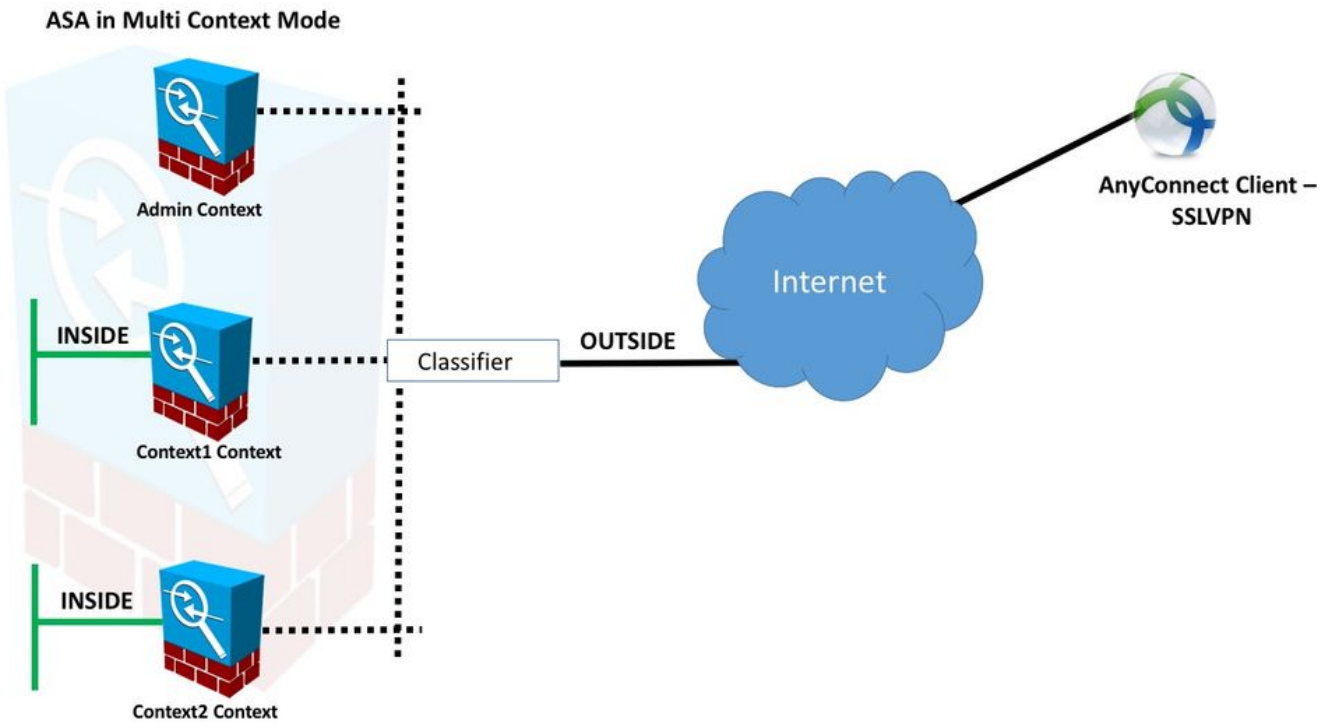
라이센싱

- AnyConnect Apex 라이센스 필요
- Essentials 라이센스가 무시되었거나 허용되지 않음
- 컨텍스트당 최대 라이센스 사용을 제어하는 구성 가능
- 컨텍스트당 라이센스 버스팅을 허용하는 구성 가능

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



> **참고:** 이 예의 다중 컨텍스트는 인터페이스(OUTSIDE)를 공유한 다음 분류자는 인터페이스 고유(자동 또는 수동) MAC 주소를 사용하여 패킷을 전달합니다.보안 어플라이언스가 여러 컨텍스트에서 패킷을 분류하는 방법에 대한 자세한 내용은 ASA에서 패킷을 분류하는 방법을 참조하십시오.

다음 컨피그레이션 절차는 ASA 9.6.2 버전 이상과 함께 제공되며, 여기에는 사용 가능한 새로운 기능 중 일부가 나와 있습니다.9.6.2 이전(9.5.2 이상) ASA 버전에 대한 컨피그레이션 절차의 차이점은 문서 부록 A에 설명되어 있습니다.

원격 액세스 VPN을 설정하기 위해 시스템 컨텍스트 및 사용자 지정 컨텍스트에서 필요한 컨피그레이션은 다음과 같습니다.

시스템 컨텍스트의 초기 컨피그레이션

먼저, System Context에서 장애 조치, VPN 리소스 할당, 사용자 지정 컨텍스트 및 Apex 라이센스 확인을 구성합니다.절차 및 컨피그레이션은 이 섹션과 다음 섹션에서 설명합니다.

1단계. 장애 조치 구성.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

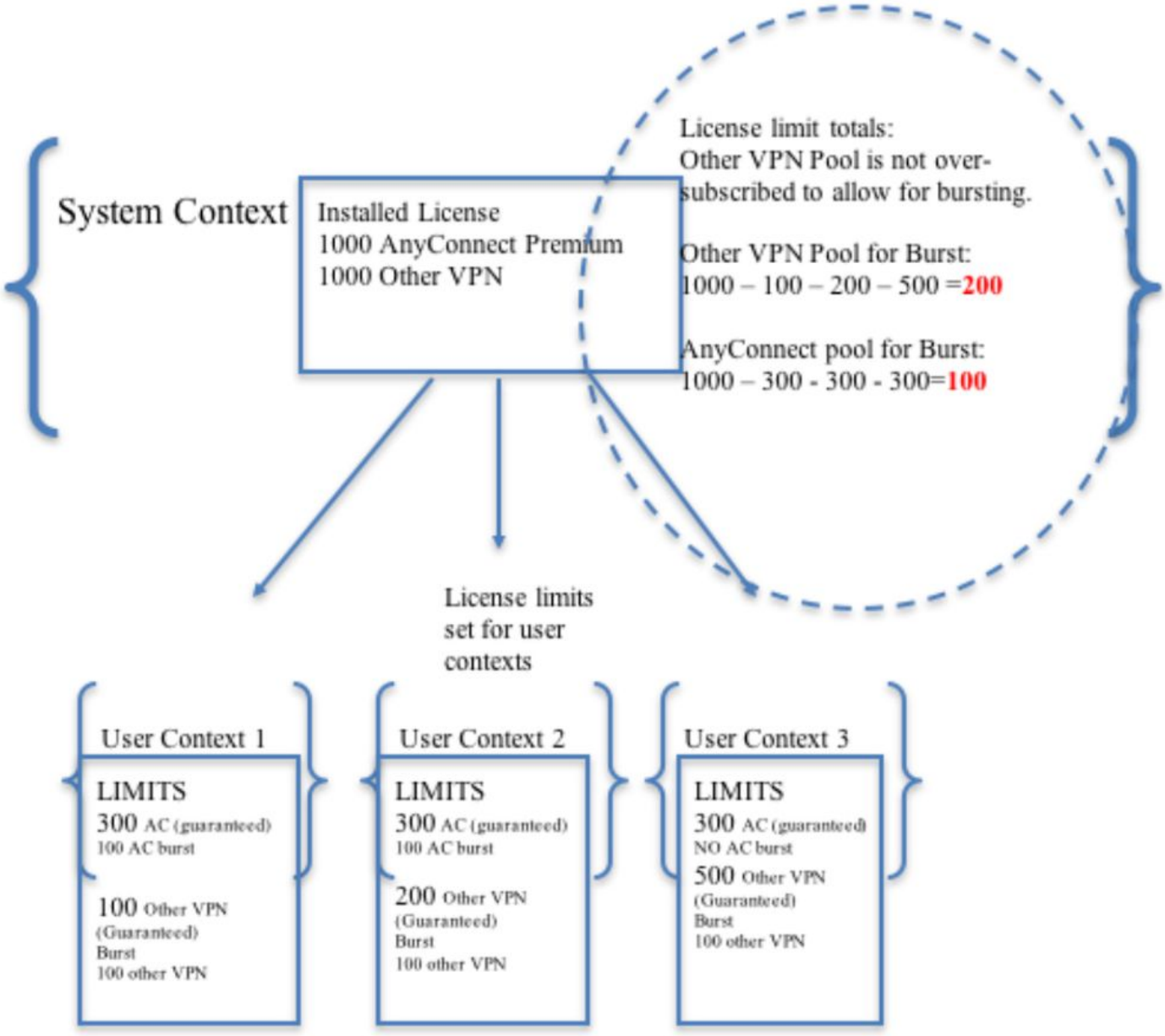
2단계. VPN 리소스를 할당합니다.

기존 클래스 컨피그레이션을 통해 구성되었습니다.라이센스는 라이센스 수 또는 컨텍스트당 총 라이센스 수의 %로 허용됩니다.

MC RAVPN을 위한 새로운 리소스 유형:

- VPN AnyConnect:컨텍스트에 보장되며 초과 가입할 수 없습니다.
- VPN 버스트 AnyConnect:보장 한도를 초과하는 컨텍스트 추가 라이센스를 허용합니다.버스트 풀은 컨텍스트에 보장되지 않는 라이센스로 구성되며 선착순으로 버스트 컨텍스트가 허용됩니다.

VPN 라이센스 프로비저닝 모델:



참고:ASA5585는 최대 10,000개의 Cisco AnyConnect 사용자 세션을 제공하며, 이 예에서는 4,000개의 Cisco AnyConnect 사용자 세션이 컨텍스트당 할당됩니다.

```
class resource02
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000

class resource01
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000
```

3단계. 컨텍스트를 구성하고 리소스를 할당합니다.

참고: 이 예에서 GigabitEthernet0/0은 모든 컨텍스트 간에 공유됩니다.

```
admin-context admin
```

```
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

4단계. ASA에 Apex 라이센스가 설치되어 있는지 확인하고 자세한 내용은 아래 링크를 참조하십시오.

활성화 키 활성화 또는 비활성화

5단계. Anyconnect 이미지 패키지를 구성합니다.사용 중인 ASA 버전에 따라 AnyConnect 이미지를 로드하고 RA VPN에 대해 구성하는 두 가지 방법이 있습니다.버전이 9.6.2 이상이면 Flash 가상화를 사용할 수 있습니다.9.6.2보다 이전 버전은 부록 A를 참조하십시오.

> **참고:**9.6.2 이상에서는 Flash Virtualization을 지원하므로 컨텍스트당 AnyConnect 이미지를 사용할 수 있습니다.

플래시 가상화

원격 액세스 VPN에는 AnyConnect 패키지, 호스트 스캔 패키지, DAP 컨피그레이션, 플러그인, 사용자 지정 및 현지화 등의 다양한 구성 및 이미지를 위한 플래시 스토리지가 필요합니다.9.6.2 이전의 다중 컨텍스트 모드에서는 사용자 컨텍스트가 플래시의 어느 부분에도 액세스할 수 없으며 시스템 컨텍스트만 통해 플래시를 관리하고 시스템 관리자가 액세스할 수 있습니다.

이 제한을 해결하기 위해 플래시에 있는 파일의 보안 및 개인 정보를 유지하면서 컨텍스트 간에 플래시를 적절하게 공유할 수 있도록 가상 파일 시스템이 멀티 컨텍스트 모드에서 플래시에 대해 생성됩니다. 이 기능의 목적은 AnyConnect 이미지가 전역으로 구성된 것이 아니라 컨텍스트별로 구성되도록 하는 것입니다.이렇게 하면 여러 사용자가 서로 다른 AnyConnect 이미지를 설치할 수 있습니다.또한 AnyConnect 이미지를 공유하도록 허용하면 이러한 이미지에 사용된 메모리 양을 줄일 수 있습니다. 공유 저장소는 모든 컨텍스트에 공통된 파일 및 패키지를 저장하는 데 사용됩니다.

> **참고:** 시스템 컨텍스트 관리자는 전체 플래시 및 전용 및 공유 스토리지 파일 시스템에 대한 전체 읽기-쓰기 액세스를 계속 가집니다.시스템 관리자는 디렉토리 구조를 작성하고 모든 개인 파일 및 공유 파일을 서로 다른 디렉토리로 구성하여 컨텍스트가 공유 스토리지 및 전용 스토리지로 액세스하도록 구성할 수 있습니다.

모든 컨텍스트는 자체 전용 스토리지에 대한 읽기/쓰기/삭제 권한을 가지며 공유 스토리지에 대한 읽기 전용 액세스를 갖게 됩니다.시스템 컨텍스트만 공유 스토리지에 대한 쓰기 액세스 권한을 갖습니다..

아래 구성에서는 프라이빗 스토리지를 설명하기 위해 사용자 지정 컨텍스트 1이 구성되고, 공유 스토리지를 설명하기 위해 사용자 지정 컨텍스트 2가 구성됩니다.

전용 스토리지

컨텍스트당 하나의 전용 스토리지 공간을 지정할 수 있습니다.컨텍스트 내의 이 디렉토리뿐 아니라 시스템 실행 영역에서도 읽기/쓰기/삭제할 수 있습니다. 지정된 경로 아래에서 ASA는 컨텍스트 이름을 딴 하위 디렉토리를 생성합니다.

예를 들어 context1에서 경로에 대해 disk0:/private-storage를 지정하면 ASA는 disk0:/private-storage/context1/에서 이 컨텍스트에 대한 하위 디렉토리를 생성합니다.

공유 스토리지

컨텍스트당 하나의 읽기 전용 공유 스토리지 공간을 지정할 수 있습니다.모든 컨텍스트(예: AnyConnect 패키지)에서 공유할 수 있는 일반 대용량 파일의 중복을 줄이기 위해 공유 저장 공간을 사용할 수 있습니다.

전용 스토리지 공간을 사용할 구성

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

공유 저장소 공간을 사용할 구성

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

각 컨텍스트에서 이미지를 확인합니다.

```
!! Custom Context 1 configured for private storage.

ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

!! Custom Context 2 configured for shared storage.

ciscoasa(config)#changeto context context2
```

```
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

6단계. 다음은 위에서 설명한 플래시 가상화 컨피그레이션을 포함하는 시스템 Context의 컨피그레이션 요약입니다.

시스템 컨텍스트

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
 storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

7단계:아래에 표시된 대로 두 개의 사용자 지정 컨텍스트를 구성합니다.

사용자 지정 컨텍스트 1

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
```

사용자 지정 컨텍스트 2

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
!
!
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Apex 라이센스가 설치되어 있는지 확인

ASA는 AnyConnect Apex 라이센스를 구체적으로 인식하지는 않지만 다음과 같은 Apex 라이센스의 라이센스 특성을 적용합니다.

- AnyConnect Premium은 플랫폼 제한에 라이센스 부여
- 모바일용 AnyConnect
- Cisco VPN Phone용 AnyConnect
- 고급 엔드포인트 평가

AnyConnect Apex 라이센스가 설치되지 않았기 때문에 연결이 차단되면 syslog가 생성됩니다.

사용자 지정 컨텍스트(9.6.2 이상)에서 AnyConnect 패키지를 사용할 수 있는지 확인

```
! AnyConnect package is available in context1
```

```
 ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

사용자 지정 컨텍스트 아래에 이미지가 없는 경우 Anyconnect [이미지 컨피그레이션(9.6.2 이상)을 참조하십시오.](#)

사용자가 사용자 지정 컨텍스트에서 AnyConnect를 통해 연결할 수 있는지 확인

팁: 전체 화면에서 비디오 아래에 더 잘 동영상을 표시할 수 있습니다.

```
!! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 5
Assigned IP : 192.168.1.1 Public IP : 10.142.168.102
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 3186 Bytes Rx : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time : 15:33:25 UTC Thu Dec 3 2015
Duration : 0h:00m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 1
Assigned IP : 192.168.51.1 Public IP : 10.142.168.94
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 10550 Bytes Rx : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
```

```
Login Time : 15:34:16 UTC Thu Dec 3 2015
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
Status : Capacity : Installed : Limit
---------------------------------------
AnyConnect Premium : ENABLED : 10000 : 10000 : NONE
Other VPN (Available by Default) : ENABLED : 10000 : 10000 : NONE
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone : ENABLED
VPN-3DES-AES : ENABLED
VPN-DES : ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
Local : Shared : All : Peak : Eff. :
In Use : In Use : In Use : In Use : Limit : Usage
-------------------------------------------------
AnyConnect Premium : 2 : 0 : 2 : 2 : 10000 : 0%
AnyConnect Client : : 2 : 2 : 0%
AnyConnect Mobile : : 2 : 2 : 0%
Other VPN : : 0 : 0 : 10000 : 0%
Site-to-Site VPN : : 0 : 0 : 0%
----------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource Current Peak Limit Denied Context
AnyConnect 1 1 4000 0 context1
AnyConnect 1 1 4000 0 context2
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

AnyConnect 문제 해결

> **팁:**ASA에 Apex 라이센스가 설치되어 있지 않은 경우 AnyConnect 세션이 syslog 아래에 있는 상태로 종료됩니다.
>
> %ASA-6-725002:디바이스가 TLSv1 세션에 대해 클라이언트 OUTSIDE:10.142.168.86/51577에서 10.106.44.38/443으로 SSL 핸드셰이크를 완료했습니다 .

%ASA-6-113012:AAA 사용자 인증 성공:로컬 데이터베이스:사용자 = cisco
%ASA-6-113009:AAA가 사용자 = cisco에 대한 기본 그룹 정책 (GroupPolicy_MC_RAVPN_1)을 검색했습니다.
%ASA-6-113008:AAA 트랜잭션 상태 수락:사용자 = cisco
%ASA-3-716057:그룹 사용자 IP <10.142.168.86> 세션이 종료됨, 사용 가능한 AnyConnect Apex 라이센스가 없음
%ASA-4-113038:그룹 사용자 IP <10.142.168.86> AnyConnect 상위 세션을 만들 수 없습니다.

부록 A - 9.6.2 이전 버전에 대한 AnyConnect 이미지 컨피그레이션

AnyConnect 이미지는 9.6.2 이전 ASA 버전의 관리 컨텍스트에서 전역적으로 구성됩니다(이 기능은 9.5.2에서 사용 가능). 플래시 스토리지는 가상화되지 않으며 시스템 컨텍스트에서만 액세스할 수 있기 때문입니다.

5단계.1. 시스템 컨텍스트에서 플래시에 AnyConnect 패키지 파일을 복사합니다.

시스템 컨텍스트:

```
ciscoasa(config)# show flash:

195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

5.2단계. Anyconnect 이미지 구성 Admin(관리) 컨텍스트로 이동합니다.

관리 컨텍스트:

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

참고: AnyConnect 이미지는 관리 컨텍스트에서만 구성할 수 있습니다.모든 컨텍스트는 자동으로 이 전역 Anyconnect 이미지 컨피그레이션을 참조합니다.

사용자 지정 컨텍스트 1:

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.38 255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
```

```
username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
group-url https://10.106.44.38/context1 enable
```

사용자 지정 컨텍스트 2:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.36 255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
group-url https://10.106.44.36/context2 enable
```

AnyConnect 패키지가 관리 컨텍스트에 설치되어 있고 사용자 지정 컨텍스트에서 사용 가능한지(9.6.2 이전) 확인

```
!! AnyConnect package is installed in Admin Context

ciscoasa/pri/admin/act# show run webvpn
webvpn
anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1

ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable OUTSIDE
anyconnect enable
tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

참조

릴리스 정보:9.5(2)

릴리스 정보:9.6(2)

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- AnyConnect VPN 클라이언트 문제 해결 가이드 - 일반적인 문제
- AnyConnect 세션 관리, 모니터링 및 문제 해결
- 기술 지원 및 문서 – Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf