

다중 컨텍스트 ASA 9.x의 Site-To-Site VPN 컨피그레이션에서 오류 메시지 수신

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[배경 정보](#)

[권장 작업](#)

[솔루션](#)

[관련 정보](#)

소개

이 문서에서는 ASA(Multiple Context Adaptive Security Appliances) 9.x에서 Site-To-Site VPN을 구성할 때 오류 메시지, "허용되는 최대 터널 수에 도달했습니다"라는 오류 메시지의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

사용되는 구성 요소

이 문서의 정보는 ASA Software Version 9.0 이상을 기반으로 합니다. 이 버전은 다중 컨텍스트 모드에서 Site-To-Site VPN 컨피그레이션을 도입했습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

문제

ASA에서 여러 Site-To-Site VPN 터널을 가져오려고 하면 오류가 발생하고 syslog 메시지 "The maximum tunnel count has been reached"가 생성됩니다.

특정 syslog 메시지는 다음과 같습니다.

%ASA-4-751019: Local:<LocalAddr> Remote:<RemoteAddr> Username:<username> Failed to obtain a <licenseType> license.

- <LocalAddr> - 이 연결 시도에 대한 로컬 주소
- <RemoteAddr> - 이 연결 시도에 대한 원격 피어 주소
- <username> - 연결을 시도하는 피어의 사용자 이름
- <licenseType> - 초과한 라이선스 유형(기타 VPN 또는 AnyConnect Premium/Essentials)

배경 정보

로그는 VPN 터널에 대한 최대 라이선스 제한을 초과했기 때문에 세션을 생성하지 못했음을 나타내며, 이로 인해 터널 요청을 시작하거나 응답하지 못합니다.

다중 모드에서 VPN을 구현하려면 구성된 컨텍스트 중에서 사용 가능한 총 VPN 라이선스를 분할해야 합니다. ASA 관리자는 각 컨텍스트가 할당되는 라이선스 수를 구성할 수 있습니다.

기본적으로 VPN 터널 라이선스는 컨텍스트에 할당되지 않으며 관리자가 라이선스 유형을 수동으로 할당해야 합니다.

권장 작업

허용된 모든 사용자에게 충분한 라이선스가 제공되는지 확인하고 거부된 연결을 허용하기 위해 추가 라이선스를 얻습니다. 다중 컨텍스트의 경우 가능한 경우 오류를 보고한 컨텍스트에 추가 라이선스를 할당합니다.

솔루션

컨텍스트 간에 라이선스를 나누는 작업은 구성된 컨텍스트 사이에서 사이트 간 VPN에 사용되는 '기타 VPN' 라이선스 풀의 분리를 관리하는 'VPN other' 리소스로 리소스 관리자의 확대로 수행됩니다.

아래의 limit-resource CLI에서는 리소스 'class' 모드 내에서 이 컨피그레이션을 허용합니다.

```
Limit-resource vpn [burst] other <value> | <value>%
```

여기서 <value> 범위는 다음과 같습니다. 1- 플랫폼 라이선스 제한 또는 설치된 라이선스의 1-100%

버스트의 경우 범위는 1에서 할당되지 않은 라이선스 또는 할당되지 않은 라이선스의 1~100%입니다.

기본값:0;클래스에 할당된 VPN 리소스가 없습니다.

설치된 라이선스의 10%에 컨텍스트를 할당하려면 리소스 클래스를 정의해야 합니다. 그런 다음 시스템 컨텍스트 컨피그레이션 내에서 이 리소스를 가져오는 데 필요한 컨텍스트에 클래스를 적용합니다.

```
ciscoasa(config)# class vpn  
ciscoasa(config-class)# limit-resource vpn other 10%
```

설치된 라이선스의 VPN 피어 250개의 컨텍스트를 할당하려면 리소스 'class'를 정의해야 합니다. 그런 다음 시스템 컨텍스트 컨피그레이션 내에서 이 리소스를 가져올 수 있는 컨텍스트에 클래스를

적용합니다.

```
ciscoasa(config)# class vpn  
ciscoasa(config-class)# limit-resource vpn other 250
```

위의 클래스 "vpn"을 "administrator"라는 컨텍스트에 적용하려면 다음 단계를 수행합니다.

1. 시스템 컨텍스트로 변경/전환 및 "관리자" 컨텍스트에 대한 클래스 VPN을 적용합니다. 이 작업은 시스템 컨텍스트 내에서만 수행할 수 있습니다.
2. 다음은 "administrator" 컨텍스트에 "vpn" 클래스를 할당하는 컨피그레이션 조각입니다.

```
ciscoasa(config)# context administrator  
ciscoasa(config-ctx)# member vpn
```

관련 정보

- [Cisco ASA 5500 Series Next Generation Firewalls 참조 설명서](#)
- [Cisco ASA 5500 Series Next Generation Firewalls 컨피그레이션 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)