VPN 문제 해결을 위한 플랫폼 설정 구현

목차

소개

이 문서에서는 Secure Firewall Management Center 및 Secure Firewall Threat Defense를 사용하여 VPN 디버그 로그를 쉽게 구성하고 식별하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(보안 방화벽 위협 방어)
- FMC(Secure Firewall Management Center)

- FMC GUI 및 FTD CLI 탐색에 대한 기본 이해
- 플랫폼 설정에 대한 기존 정책 할당

사용되는 구성 요소

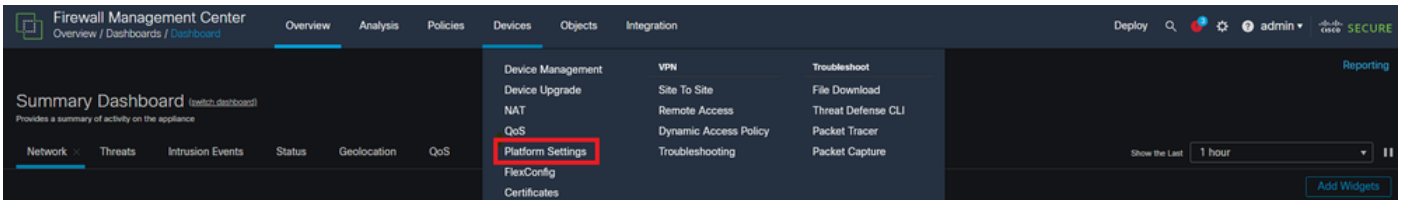
이 문서의 정보는 다음 소프트웨어 버전 및 하드웨어 버전을 기반으로 합니다.

- Firewall Management Center 버전 7.3
- Firewall Threat Defence 버전 7.3

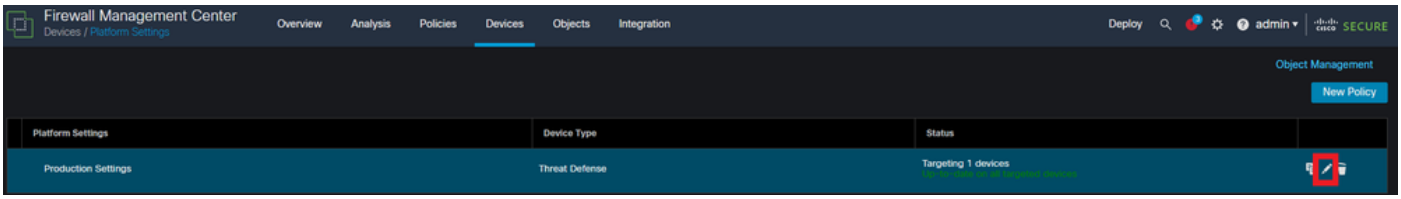
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

방화벽 관리 센터

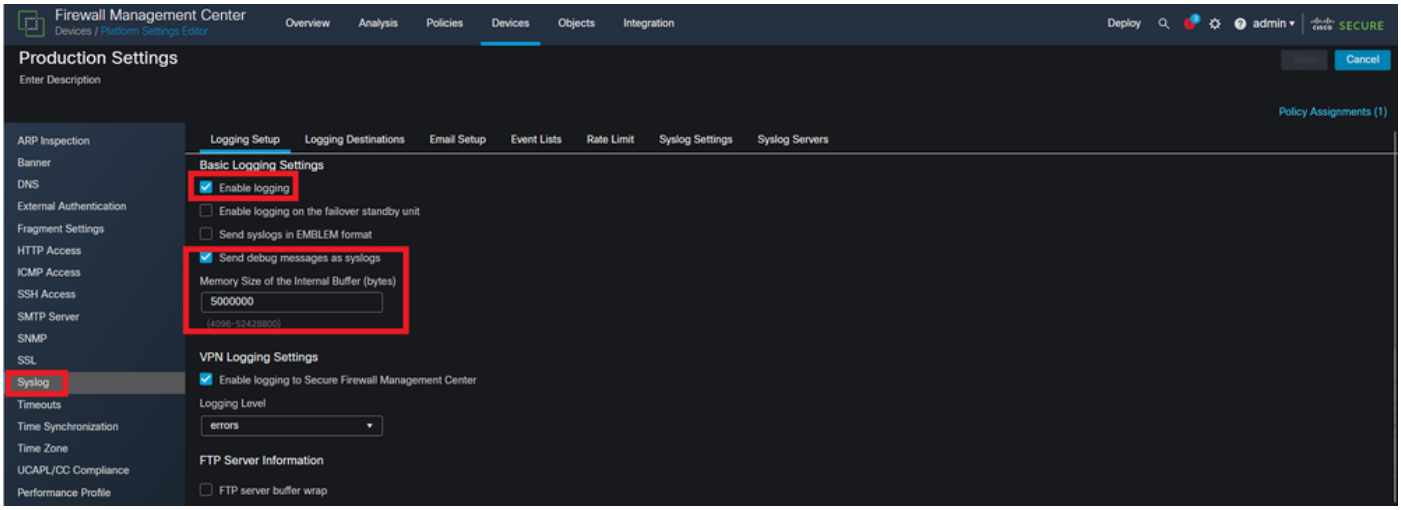
로 이동합니다.Devices > Platform Settings



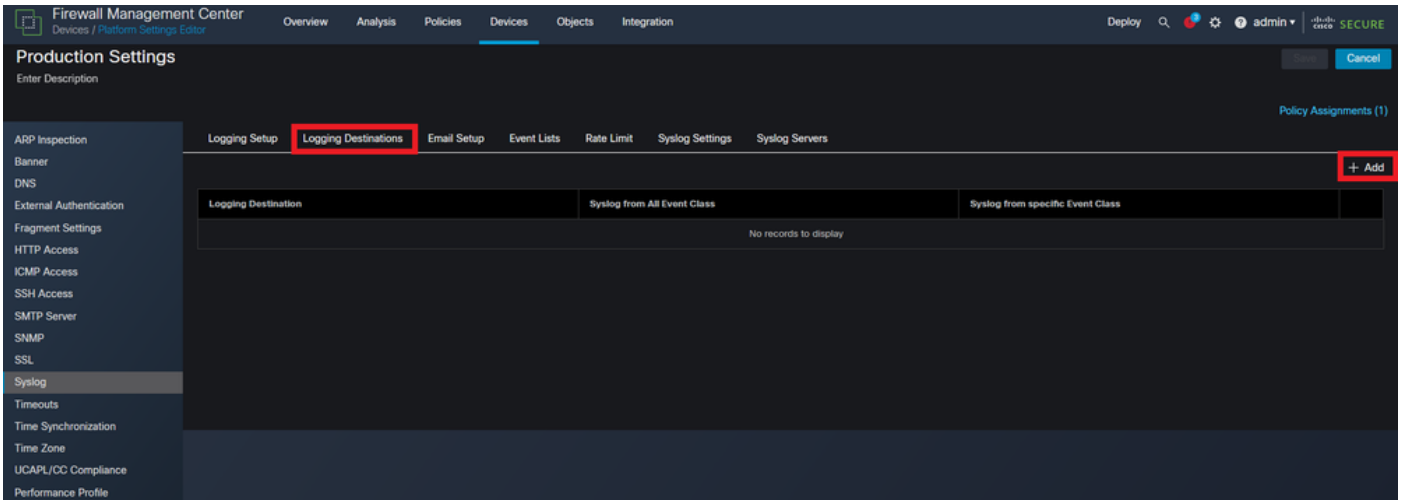
와 **pencil** 삭제 사이의copy를icon클릭합니다.



옵션Syslog의 왼쪽 열로 이동하여 및 이 **Enable Logging**활성화되었는지 **Send debug messages as syslog** 확인합니다. 또한Memory Size of the Internal Buffer, 가 문제 해결에 적합한 값으로 설정되어 있는지 확인합니다.

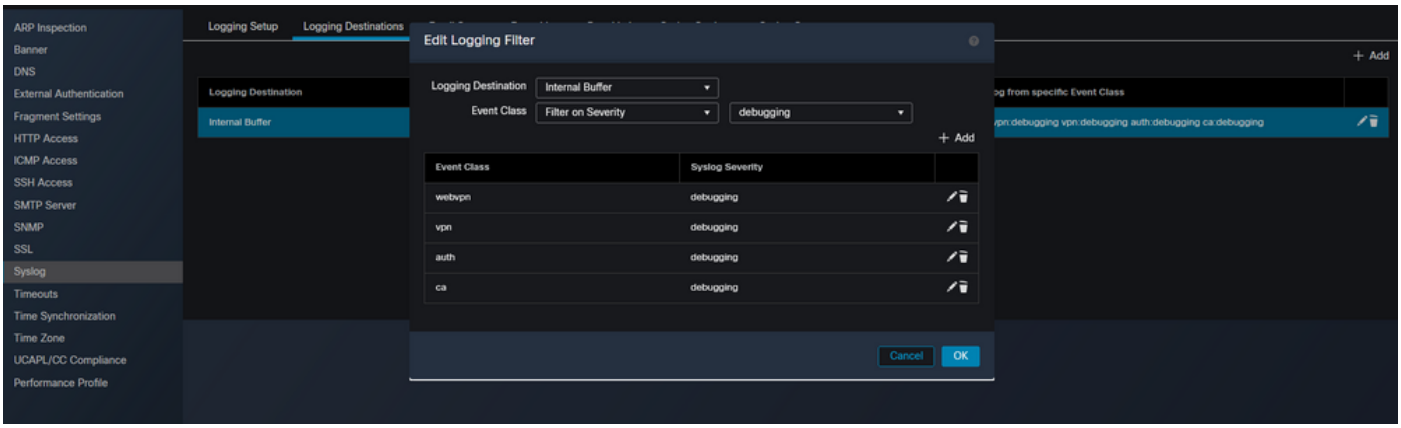


을 클릭한 **Logging Destinations** 다음 을 클릭합니다. **+Add**.



이 섹션에서는 로깅 대상이 관리자의 기본 설정이며 **Internal Buffer** 사용됩니다. 이**Event Class**가 **Filter on Severity and debugging**. 완료되면 을 클릭하고 ,+Addwebvpn,vpn,authca및 모두를 선택하여 Syslog 심각도를 debugging선택합니다. 이 단계를 통해 관리자는 특정 syslog 메시지(711001)로 이러한 디버그 출력을 필터링할 수 있습니다. 문제 해결 유형에 따라 이러한 출력을 수정할 수 있습니다. 그러나 이 예에서

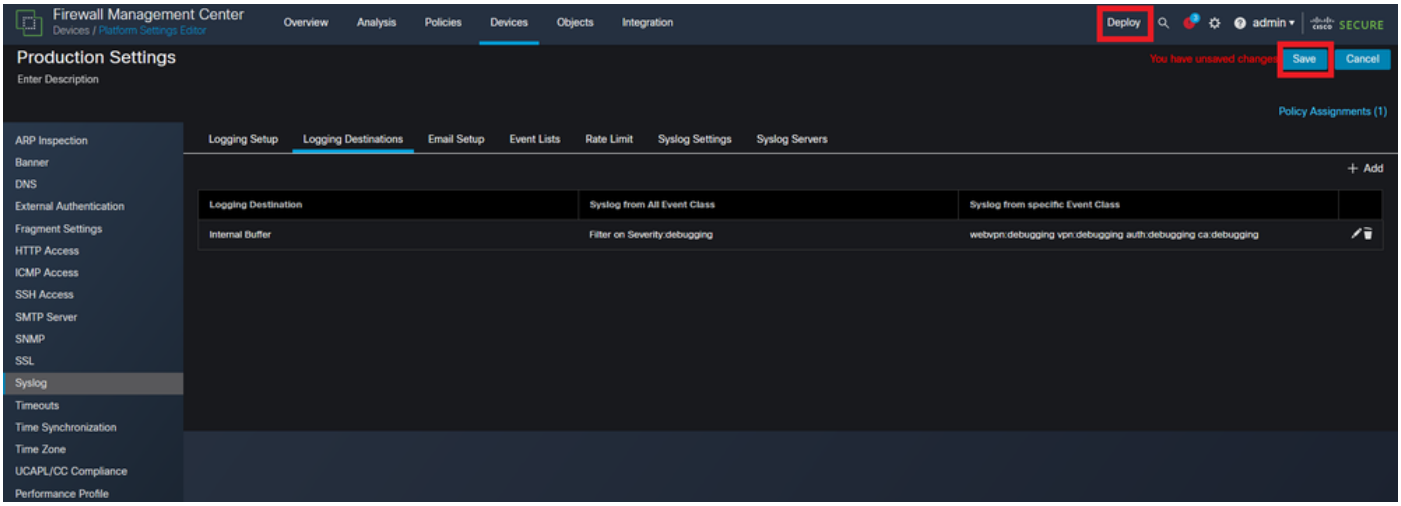
선택한 항목에서는 가장 일반적으로 발생하는 Site-to-Site, Remote Access 및 AAA VPN 관련 문제를 다룹니다.



디버그에 대한 이벤트 클래스 및 필터를 만듭니다.

경고: 그러면 Buffer Logging Level(버퍼 로깅 수준)이 디버깅으로 변경되고 내부 버퍼에 지정된 클래스에 대한 디버깅 이벤트가 로깅됩니다. 이 로깅 방법은 문제 해결을 위해 사용하는 것이 좋으며 장기간 사용하는 것은 아닙니다.

Choose Save 오른쪽 상단에서 컨피그레이션Deploy이 변경됩니다.



방화벽 위협 방어

FTD CLI로 이동하고 명령을 실행합니다show logging setting. 여기의 설정은 FMC의 변경 사항을 반영합니다. debug-trace 로깅이 활성화되어 있고 버퍼 로깅이 지정된 클래스 및 로깅 레벨과 일치하는지 확인합니다.

```
FTD72# show logging setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled (persistent)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, class auth vpn webvpn ca, 362685 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, class auth vpn webvpn ca, 27 messages logged
```

FTD CLI의 로깅 설정을 표시합니다.

마지막으로, 로그를 syslog:711001으로 리디렉션하도록 디버그를 적용합니다. 이 예에서debug webvpn anyconnect 255를 적용합니다. 그러면 관리자가 이러한 디버그가 리디렉션되었음을 알 수 있도록 디버그 추적 로깅 알림이 트리거됩니다. 이러한 디버그를 보려면 명령을 실행하십시오show log | in 711001. 이제 이 syslog ID에는 관리자가 적용한 관련 VPN 디버깅만 포함됩니다. 기존 로그는 지우기 로깅 버퍼로 지울 수 있습니다.

```
FTD72# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and will not appear in any monitor session
INFO: debug webvpn anyconnect enabled at level 255.
FTD72# show log | in 711001
```

모든 VPN 디버그가 syslog 서버로 리디렉션되고 있음을 711001.

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.