VPN 모니터링 및 문제 해결

이 장에서는 Firepower Threat Defense VPN 모니터링 툴, 파라미터 및 통계 정보와 문제 해결에 대해 설명합니다.

VPN 요약 대시보드

Firepower System 대시보드는 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공합니다. VPN 대시보드를 사용하여 현재 사용자 상태, 디바이스 유형, 클라이언트 애플리케이션, 사용자 위치 정보 및 연결 기간을 포함하여 VPN 사용자에 대한 통합 정보를 볼 수 있습니다.

VPN 요약 대시보드 보기

Remote Access VPN은 원격 사용자(예: 휴대폰 사용자 또는 재택 근무자)에 대한 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 얻을 수 있습니다.

이 작업을 수행하려면 리프 도메인의 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Access Controlled User Statistics(**액세스 제어 사용자 통계**)** > **VPN**을 선택합니다.

단계 **2** 다음과 같은 Remote Access VPN 정보 위젯을 확인합니다.

- 지속기간별 현재 VPN 사용자
- 클라이언트 애플리케이션별 현재 VPN 사용자

- 디바이스별 현재 VPN 사용자
- 전송된 데이터별 VPN 사용자
- 지속기간별 VPN 사용자
- 클라이언트 애플리케이션별 VPN 사용자
- 클라이언트 국가별 VPN 사용자

VPN 세션 및 사용자 정보

Firepower System은 네트워크에서 VPN 관련 활동을 포함한 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. Firepower System 모니터링 기능을 통해 Remote Access VPN 문제가 있는지 여부와 존재 여부를 신속하게 확인할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요한 경우 Remote Access VPN 사용자를 로그아웃할 수도 있습니다(선택 사항).

Remote Access VPN 활성 세션 보기

Analysis(분석**)** > **Users(**사용자**)** > **Active Sessions(**활성 세션**)**

사용자 이름, 로그인 기간, 인증 유형, 할당/공용 IP 주소, 디바이스 상세정보, 클라이언트 버전, 엔드포인트 정보, 처리량, 대역폭 소비 그룹 정책, 터널 그룹 등과 같은 지원 정보를 사용하여 현재 로그인한 VPN 사용자를 특정 시점에서 볼 수 있습니다. 또한 시스템은 현재 사용자 정보를 필터링하고 사용자를 로그아웃하며 요약 목록에서 사용자를 삭제하는 기능을 제공합니다.

참고 고가용성 구축에서 VPN을 구성한 경우 활성 VPN 세션에 대해 표시되는 디바이스 이름은 사용자 세션을 식별한 기본 또는 보조 디바이스일 수 있습니다.

Remote Access VPN 사용자 활동 보기

Analysis(분석**)** > **Users(**사용자**)** > **User Activity(**사용자 활동**)**

네트워크에서 사용자 활동의 상세정보를 볼 수 있습니다. 시스템은 기록 이벤트를 기록하고 연결 프로파일 정보, IP 주소, 지오로케이션 정보, 연결 기간, 처리량 및 디바이스 정보와 같은 VPN 관련 정보를 포함합니다.

VPN 상태 이벤트

Health Events(상태 이벤트) 페이지에서는 irepower Management Center의 상태 모니터에서 기록한 VPN 상태 이벤트를 볼 수 있습니다. Firepower System 디바이스 간에 하나 이상의 VPN 터널이 다운되면 다음 이벤트가 추적됩니다.

- Site-to-Site VPN Firepower Threat Defense
- 원격 액세스 VPN Firepower Threat Defense

VPN 상태 이벤트 보기

Firepower Management Center의 Health Events(상태 이벤트) 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다. 확인하려는 상태 이벤트를 생성한 모듈을 지정하여 이벤트 범위를 좁힐 수 있습니다.

이 작업을 수행하려면 관리자, 유지 보수 사용자 또는 보안 분석가여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** **Module Name(**모듈 이름**)** 열에서 **VPN Status(VPN** 상태**)**를 선택합니다.

VPN 문제 해결

이 섹션에서는 VPN 문제 해결 도구 및 디버그 정보에 대해 설명합니다.

시스템 메시지

Message Center는 문제 해결을 시작할 수있는 장소입니다. 이 기능을 사용하면 지속적으로 생성되는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다. Message Center를 열려면 메인 메뉴의 **Deploy(**구축**)** 버튼 오른쪽의 **System Status(**시스템 상태**)**를 클릭합니다.

VPN 시스템 로그

FTD 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. VPN 기록을 활성화하면 이러한 시스템 로그가 분석 및 보관을 위해 FTD 디바이스에서 Firepower Management Center로 전송됩니다.

표시되는 VPN 시스템 로그의 기본 심각도는 'ERROR' 이상입니다(변경되지 않은 경우). VPN 기록은 FTD 플랫폼 설정을 통해 관리됩니다. 대상 디바이스(**Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**에 대한 FTD 플랫폼 설정 정책에서 **VPN Logging Settings(VPN** 기록 설정**)**를 편집하여 메시지 심각도 수준을 조정할 수 있습니다. VPN 기록 활성화, 시스템 로그 서버 구성 및 시스템 로그 보기에 대한 자세한 내용은 시스템 로그 구성 관련 정보 섹션을 참조하십시오.

참고 디바이스가 Site-to-Site VPN 또는 Remote Access VPN으로 구성될 때마다 기본적으로 VPN 시스템 로그가 Firepower Management Center에 자동으로 전송되도록 설정됩니다.

VPN 시스템 이벤트 로그 보기

시스템은 VPN 문제의 소스에 대한 추가 정보를 수집하는 데 도움이 되는 이벤트 정보를 수집합니다. 표시되는 VPN 시스템 로그의 기본 심각도는 'ERROR' 이상입니다(변경되지 않은 경우). 기본적으로 행은 **Time(**시간**)** 열에 따라 정렬됩니다.

이 작업을 수행하려면 리프 도메인의 관리자 사용자여야 합니다.

시작하기 전에

FTD 플랫폼 설정(**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**))**에서 **Enable Logging to FMC(FMC**에 대한 기록 활성화**)** 확인란을 선택하여 VPN 기록을 활성화합니다. VPN 기록 활성화, 시스템 로그 서버 구성 및 시스템 로그 보기에 대한 자세한 내용은 시스템 로그 구성 관련 정보 섹션을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **VPN** > **Troubleshooting(**문제 해결**)**을 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Search(검색) - 현재 메시지 정보를 필터링하려면 **Edit Search(**검색 편집**)**를 클릭합니다.
- View(보기) - 보기에서 선택된 메시지와 관련된 VPN 상세정보를 보려면 **View(**보기**)**를 클릭합니다.
- View All(모두 보기) - 보기에서 모든 메시지에 대한 VPN 상세정보를 보려면 **View All(**모두 보기**)**을 클릭합니다.
- Delete(삭제) - 데이터베이스에서 선택한 메시지를 삭제하려면 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 모든 메시지를 삭제합니다.

디버그 명령

이 섹션에서는 디버그 명령을 사용하여 VPN 관련 문제점을 진단하고 해결하는 방법을 설명합니다. 이 섹션에서 사용 가능한 모든 디버그 명령을 설명하지는 않습니다. 여기에 있는 명령은 VPN 관련 문제점을 진단하는 데 도움이 되는 유용성에 따라 포함되어 있습니다.

사용 가이드라인

디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되기 때문에 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 **debug** 명령은 특정 문제를 해결하는 경우나 Cisco TAC(Technical Assistance Center)를 통한 문제 해결 세션 중에만 사용해야 합니다. 또한, 네트워크 트래픽과 사용자 수가 적은 기간에

debug 명령을 사용하는 것이 가장 좋습니다. 그러한 기간에 디버깅하면 **debug** 명령의 처리 오버헤드 증가로 인해 시스템 사용에 지장이 생길 가능성이 줄어듭니다.

디버그 출력은 CLI 세션에서만 확인할 수 있습니다. 콘솔 포트에 연결하거나 **system support diagnostic-cli**를 입력하여 진단 CLI를 사용할 때는 출력을 직접 사용할 수 있습니다. **show console-output** 명령을 사용하여 일반 Firepower Threat Defense CLI에서 출력을 확인할 수도 있습니다.

지정된 기능에 대한 디버깅 메시지를 표시하려면 **debug** 명령을 사용합니다. 디버그 메시지의 표시를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. **no debug all**은 모든 디버깅 명령을 끄는 데 사용합니다.

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	디버깅을 활성화하려는 기능을 지정합니다. 사용 가능한 기능을 보려면 CLI 도움말에 대한 **debug ?** 명령을 사용합니다.
subfeature	(선택 사항) 기능에 따라 하나 이상의 하위 기능에 대한 디버그 메시지를 활성화할 수 있습니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
level	(선택 사항) 디버깅 레벨을 지정합니다. 모든 기능에서 이 레벨을 사용할 수 있는 것은 아닙니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

예

원격 액세스 VPN에서 실행 중인 다중 세션에서는 지정된 로그의 크기 때문에 문제 해결이 어려울 수 있습니다. **debug webvpn condition** 명령을 사용하여 더 정확하게 디버그 프로세스를 대상으로 필터를 설정할 수 있습니다.

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

여기서 각 항목은 다음을 나타냅니다.

- 그룹 정책(터널 그룹 또는 연결 프로파일 이외)의 **group** *name* 필터.
- 클라이언트의 공용 IP 주소에 대한 **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] 필터. 서브넷 마스크(IPv4용) 또는 접두사(IPv6용)는 선택 사항입니다.
- **reset** 모든 필터 재설정. **no debug webvpn condition** 명령을 사용하여 특정 필터를 끌 수 있습니다.
- 사용자 이름을 기준으로 하는 **user** *name* 필터.

조건을 여러 개 구성하는 경우 조건이 결합되어(AND로 처리되어) 모든 조건이 충족될 경우에만 디버그가 표시됩니다.

조건 필터를 설정한 후 기본 **debug webvpn** 명령을 사용하여 디버그를 켭니다. 조건을 설정하는 것만으로 디버그가 활성화되지는 않습니다. 현재 디버깅 상태를 보려면 **show debug** 및 **show webvpn debug-condition** 명령을 사용합니다.

다음은 사용자 jdoe에 대해 조건부 디버그를 활성화하는 예를 보여줍니다.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands

Command(명령)	설명
show debug	현재 활성 디버그 설정을 표시합니다.
undebug	기능에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug**에 대한 동의어입니다.

debug aaa

인증, 권한 부여 및 계정(AAA, "트리플 A"로 발음)과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description

aaa	AAA 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
accounting	(선택 사항) AAA 계정 디버깅을 활성화합니다.
authentication	(선택 사항) AAA 인증 디버깅을 활성화합니다.
authorization	(선택 사항) AAA 권한 부여 디버깅을 활성화 합니다.
common	(선택 사항) 일반적인 AAA 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
internal	(선택 사항) AAA 내부 디버깅을 활성화합니다.

shim	(선택 사항) AAA shim 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
url-redirect	(선택 사항) AAA url-redirect 디버깅을 활성화합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug aaa	AAA의 현재 활성 디버그 설정을 표시합니다.
undebug aaa	AAA 디버깅을 비활성화합니다. 이 명령은 **no debug aaa**에 대한 동의어입니다.

debug crypto

암호화와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description

crypto	*crypto* 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
ca	(선택 사항) PKI 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
condition	(선택 사항) IPsec/ISAKMP 디버그 필터를 지정합니다. ?를 사용하여 사용 가능한 필터를 확인합니다.
engine	(선택 사항) Crypto engine 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ike-common	(선택 사항) 일반적인 IKE 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ikev1	(선택 사항) IKE 버전 1 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ikev2	(선택 사항) IKE 버전 2 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
ipsec	(선택 사항) IPsec 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
condition	(선택 사항) Crypto Secure Socket API 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

vpnclient	(선택 사항) EasyVPN 클라이언트 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto	crypto ca의 현재 활성 디버그 설정을 표시합니다.
undebug crypto	crypto ca 디버깅을 비활성화합니다. 이 명령은 **no debug crypto**에 대한 동의어입니다.

debug crypto ca

crypto ca와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description

crypto ca	*crypto ca*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
cluster	(선택 사항) PKI 클러스터 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cmp	(선택 사항) CMP 트랜잭션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
messages	(선택 사항) PKI 입/출력 메시지 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
periodic-authentication	(선택 사항) PKI periodic-authentication 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
scep-proxy	(선택 사항) SCEP 프록시 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
server	(선택 사항) 로컬 CA 서버 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
transactions	(선택 사항) PKI 트랜잭션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
trustpool	(선택 사항) 신뢰 풀 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

명령	설명
show debug crypto ca	crypto ca의 현재 활성 디버그 설정을 표시합니다.
undebug	crypto ca에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ca**에 대한 동의어입니다.

debug crypto ikev1

Internet Key Exchange 버전 1(IKEv1)과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ikev1* [*timers*] [*1-255*]

Syntax Description

ikev1	*ikev1*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
timers	(선택 사항) IKEv1 타이머에 대한 디버깅을 활성화합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ikev1	IKEv1에 대한 현재 활성 디버그 설정을 표시합니다.
undebug crypto ikev1	IKEv1에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ikev1**에 대한 동의어입니다.

debug crypto ikev2

Internet Key Exchange 버전 2(IKEv2)와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Syntax Description

ikev2	*ikev2* 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
ha	(선택 사항) IKEv2 HA 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
platform	(선택 사항) IKEv2 플랫폼 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

protocol	(선택 사항) IKEv2 프로토콜 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
timers	(선택 사항) IKEv2 타이머에 대한 디버깅을 활성화합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ikev2	IKEv2에 대한 현재 활성 디버그 설정을 표시합니다.
undebugcrypto ikev2	IKEv2에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ikev2**에 대한 동의어입니다.

debug crypto ipsec

IPsec과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *crypto ipsec* [*1-255*]

Syntax Description

ipsec	*ipsec*에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug crypto ipsec	IPsec에 대한 현재 활성 디버그 설정을 표시합니다.
undebugcrypto ipsec	IPsec에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug crypto ipsec**에 대한 동의어입니다.

ldap 디버그

LDAP(Lightweight Directory Access Protocol)와 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *ldap* [*1-255*]

Syntax Description

ldap	LDAP에 대한 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug ldap	LDAP에 대한 현재 활성 디버그 설정을 표시합니다.
undebugldap	LDAP에 대한 디버깅을 비활성화합니다. 이 명령은 **no debug ldap**에 대한 동의어입니다.

debug ssl

SSL 세션과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description

ssl	SSL 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.
cipher	(선택 사항) SSL 암호 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
device	(선택 사항) SSL 디바이스 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
1-255	(선택 사항) 디버깅 레벨을 지정합니다.

Command Default 기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug ssl	SSL의 현재 활성 디버그 설정을 표시합니다.
undebug ssl	SSL 디버깅을 비활성화합니다. 이 명령은 **no debug ssl**에 대한 동의어입니다.

debug webvpn

WebVPN과 관련된 구성 또는 설정을 디버깅하려면 다음 명령을 참조하십시오.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description

webvpn	WebVPN 디버깅을 활성화합니다. ?를 사용하여 사용 가능한 하위 기능을 확인합니다.

anyconnect	(선택 사항) WebVPN AnyConnect 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
chunk	(선택 사항) WebVPN chunk 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cifs	(선택 사항) WebVPN CIFS 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
citrix	(선택 사항) WebVPN Citrix 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
compression	(선택 사항) WebVPN 압축 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
condition	(선택 사항) WebVPN 필터 조건 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
cstp-auth	(선택 사항) WebVPN CSTP 인증 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
customization	(선택 사항) WebVPN customization 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
failover	(선택 사항) WebVPN 페일오버 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
html	(선택 사항) WebVPN HTML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
javascript	(선택 사항) WebVPN Javascript 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
kcd	(선택 사항) WebVPN KCD 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
listener	(선택 사항) WebVPN 리스너 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
mus	(선택 사항) WebVPN MUS 디버그 레벨을 지정 합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
nfs	(선택 사항) WebVPN NFS 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
request	(선택 사항) WebVPN 요청 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
response	(선택 사항) WebVPN 응답 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

saml	(선택 사항) WebVPN SAML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
session	(선택 사항) WebVPN 세션 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
task	(선택 사항) WebVPN 작업 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
transformation	(선택 사항) WebVPN 변환 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
url	(선택 사항) WebVPN URL 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
util	(선택 사항) WebVPN 유틸리티 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.
xml	(선택 사항) WebVPN XML 디버그 레벨을 지정합니다. ?를 사용하여 사용 가능한 레벨을 확인합니다.

Command Default

기본 디버깅 레벨은 1입니다.

Related Commands

Command(명령)	설명
show debug webvpn	WebVPN의 현재 활성 디버그 설정을 표시합니다.
undebug webvpn	WebVPN 디버깅을 비활성화합니다. 이 명령은 **no debug webvpn**에 대한 동의어입니다.