VPN 모니터링 및 문제 해결

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

VPN 요약 대시보드

시스템 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 인터페이스, 터널 상태 등 구성된 VPN 토폴로지의 세부 정보를 볼 수 있습니다.

모든 VPN 토폴로지에서 편집 및 삭제 버튼을 사용하여 토폴로지를 편집하거나 삭제할 수 있습니다. SASE 토폴로지 VPN의 경우 토폴로지를 구축, 편집 및 삭제할 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

원격 액세스 VPN 대시보드

RA VPN(Remote Access Virtual Private Network)을 사용하면 원격 사용자가 네트워크에 안전하게 연결할 수 있습니다. RA VPN 대시보드를 사용하면 디바이스의 활성 RA VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 사용자 세션과 관련된 문제를 신속하게 확인하고 네트워크 및 사용자의 문제를 완화할 수 있습니다.

RA VPN 대시보드(**Overview(**개요**)** > **Dashboards(**대시보드**)** > **Remote Access VPN(**원격 액세스 **VPN)**)는 management center에서 관리하는 Threat Defense 디바이스에서 활성 RA VPN 세션의 스냅샷을 제공합니다.

대시보드에는 다음과 같은 위젯이 있습니다.

- 활성 세션(표 보기)
- 활성 세션(맵 보기)
- Sessions
- 디바이스 ID 인증서

활성 세션**(**표 보기**)**

이 위젯은 연결된 활성 RA VPN 사용자의 테이블 보기를 제공합니다. 사용자 이름, 할당된 IP, 공용 IP, 로그인 시간, VPN 게이트웨이(위협 방어 디바이스), 클라이언트 애플리케이션, 클라이언트 운영 체제, 연결 프로파일 및 그룹 정책과 같은 활성 RA VPN 세션의 세부 정보를 볼 수 있습니다. 필터를 사용하여 다른 기준에 따라 검색 범위를 좁힐 수 있습니다. 개별 세션에서 다음 작업을 수행할 수도 있습니다.

- 특정 사용자의 세션을 종료합니다.

- 특정 VPN 게이트웨이에 연결된 특정 사용자의 모든 세션을 종료합니다.
- 특정 VPN 게이트웨이에 연결된 모든 세션을 종료합니다.

활성 세션(맵 보기)

이 위젯에서는 디바이스의 RA VPN 세션을 통해 연결된 사용자의 위치를 시각화하는 대화형 열 지도를 보여줍니다.

- 사용자 세션이 있는 국가는 파란색 음영으로 표시됩니다.
- 맵의 범례는 국가의 세션 수와 해당 국가의 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.
- 맵 위에 마우스 포인터를 올려놓으면 국가 이름 및 총 활성 사용자 세션 수를 확인할 수 있습니다.
- 확대, 축소 및 재설정 옵션을 사용할 수 있습니다.

Sessions

이 위젯을 사용하면 디바이스의 활성 RA VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 다음에 따라 활성 RA VPN 세션의 분포를 필터링하고 볼 수 있습니다.

- Device(디바이스): 디바이스당 세션 수를 표시합니다.
- Encryption Type(암호화 유형): Secure Client SSL 또는 IPsec 세션의 수를 표시합니다.
- Secure ClientVersion(버전): Secure Client 버전별 세션을 표시합니다.
- Operating System(운영 체제): 운영 체제별 세션을 표시합니다. 예를 들면 Windows, Linux, Mac, Mobile OS 등이 있습니다.
- Connection Profile(연결 프로파일): 연결 프로파일당 세션을 표시합니다.

디바이스 **ID** 인증서

이 위젯은 RA VPN 게이트웨이의 ID 인증서 만료에 대한 정보를 제공합니다. 만료된 인증서 및 한 달 이내에 만료되는 인증서를 볼 수 있습니다. **Device(**디바이스**) > Certificates(**인증서**)** 페이지에서 인증서를 보려면 **View Details(**세부 정보 보기**)**를 클릭합니다.

SD-WAN 요약 대시보드

SD-WAN 요약 대시보드(**Overview(**개요**) > Dashboards(**대시보드**) > SD-WAN Summary(SD-WAN** 요약**)**)에서는 WAN 디바이스 및 인터페이스의 스냅샷을 제공합니다. 이 대시보드를 통해 수행할 수 있는 작업은 다음과 같습니다.

- 언더레이 및 오버레이 (VPN) 토폴로지의 문제를 식별합니다.

- 기존의 **Health Monitoring(**상태 모니터링**)**, **Device Management(**디바이스 관리**)** 및 **Site-to-Site Monitoring(**사이트 간 모니터링**)** 페이지를 사용하여 VPN 문제 해결을 수행합니다.
- WAN 인터페이스의 애플리케이션 성능 메트릭을 모니터링합니다. Threat Defense는 이러한 메트릭을 기반으로 애플리케이션 트래픽을 조정합니다.

WAN 디바이스는 다음 기준 중 하나를 충족해야 합니다.

- 디바이스가 VPN 피어여야 합니다.
- 디바이스에 WAN 인터페이스가 있어야 합니다.

WAN 인터페이스는 다음 기준 중 하나를 충족해야 합니다.

- 인터페이스에 IP 주소 기반 경로 모니터링이 활성화되어 있습니다.
- 인터페이스에 PBR(정책 기반 라우팅) 정책이 있으며, 이 정책을 모니터링하도록 구성된 애플리케이션이 하나 이상 있습니다.

PBR 정책 및 경로 모니터링에 대한 자세한 내용은 정책 기반 라우팅를 참조하십시오.

Uplink Decisions(업링크 결정**)**를 클릭하여 **VPN Troubleshooting(VPN** 문제 해결**)** 페이지를 확인합니다. ID가 880001인 시스템 로그를 볼 수 있습니다. 이러한 시스템 로그에는 구성된 PBR 정책에 따라 트래픽을 처리하는 Threat Defense 인터페이스가 표시됩니다.

SD-WAN 요약 대시보드를 사용하기 위한 사전 요건

- 이 대시보드를 보려면 관리자, 보안 분석가 또는 유지 관리 사용자여야 합니다.
- Threat Defense 디바이스는 버전 7.2 이상이어야 합니다.
- WAN 인터페이스에서 IP 기반 경로 모니터링 및 HTTP 기반 애플리케이션 모니터링을 활성화합니다.
  1. **Devices(**디바이스**) > Device Management(**디바이스 관리**) >**를 선택합니다.
  2. 편집할 디바이스 옆에 있는 편집 아이콘을 클릭합니다.
  3. 편집할 인터페이스 옆에 있는 편집 아이콘을 클릭합니다.
  4. **Path Monitoring(**경로 모니터링**)** 탭을 클릭합니다.
  5. **Enable IP based Monitoring(IP** 기반 모니터링 활성화**)** 체크 박스를 선택합니다.
  6. **Enable HTTP based Application Monitoring(HTTP** 기반 애플리케이션 모니터링 활성화**)** 체크 박스를 선택합니다.
  7. **OK(**확인**)**를 클릭합니다.
- PBR 정책을 모니터링하도록 구성된 하나 이상의 애플리케이션으로 PBR 정책을 구성합니다.
  1. **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.

2. 편집할 디바이스 옆에 있는 편집 아이콘을 클릭합니다.
3. **Routing(**라우팅**)**을 클릭합니다.
4. 왼쪽 창에서 **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.
5. **Add(**추가**)**를 클릭합니다.
6. **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 인터페이스를 선택합니다.
7. **Add(**추가**)**를 클릭하여 전달 작업을 구성합니다.
8. 매개변수를 구성합니다.
9. **Save(**저장**)**를 클릭합니다.

- WAN 인터페이스에 대한 애플리케이션 성능 메트릭을 보려면 다음을 수행해야 합니다.
  - Threat Defense 디바이스는 버전 7.4.1이어야 합니다.
  - 상태 정책에서 SD-WAN 모듈의 데이터 수집을 활성화합니다.
    1. **System(**시스템**) > Policy(**정책**)**를 선택합니다.
    2. **Edit health policy(**상태 정책 편집**)** 아이콘을 클릭합니다.
    3. **Health Modules(**상태 모듈**)** 탭의 **SD-WAN**에서 **SD-WAN Monitoring(SD-WAN** 모니터링**)** 토글 버튼을 클릭합니다.
  - PBR 정책에 대한 애플리케이션을 구성합니다.
    1. **Objects(**개체**) > Object Management(**개체 관리**) > Access List(**액세스 목록**) > Extended(**확장**)**를 선택합니다.
    2. 액세스 목록 옆의 편집 아이콘을 클릭하고 PBR 정책에 사용할 애플리케이션을 추가합니다.
  - 네 가지 애플리케이션 메트릭 중 하나를 사용하여 정책에 대한 전달 작업을 구성합니다.
    1. **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.
    2. 편집할 디바이스 옆에 있는 편집 아이콘을 클릭합니다.
    3. **Routing(**라우팅**)**을 클릭합니다.
    4. 왼쪽 창에서 **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.
    5. 편집할 정책 옆에 있는 편집 아이콘을 클릭합니다.
    6. **Edit Policy Based Route(**정책 기반 경로 편집**)** 대화 상자에서 해당 ACL 옆에 있는 편집 아이콘을 클릭합니다.
    7. **Edit Forwarding Actions(**전달 작업 편집**)** 대화 상자에 있는 **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
       - 최소 지터

- 최대 평균 의견 점수
- 최소 왕복 시간
- 최소 패킷 손실

Interface Priority(인터페이스 우선순위**)** 또는 **Order(**순서**)**를 선택하면 인터페이스에서 애플리케이션 모니터링이 활성화되지 않습니다.

- WAN 인터페이스에 ECMP를 구성합니다.
  1. **Devices(**디바이스**) > Device Management(**디바이스 관리**)**를 선택합니다.
  2. 편집할 디바이스 옆에 있는 편집 아이콘을 클릭합니다.
  3. **Routing(**라우팅**)**을 클릭합니다.
  4. 왼쪽 창에서 **ECMP**를 클릭합니다.
  5. **Add(**추가**)**를 클릭하고 ECMP 영역의 이름을 지정합니다.
  6. **Add(**추가**)**를 클릭하여 **Available Interfaces(**사용 가능한 인터페이스**)**에서 **Selected Interfaces(**선택한 인터페이스**)**로 인터페이스를 이동합니다.
  7. **OK(**확인**)**를 클릭합니다.
- 트래픽이 인터페이스를 통과하는지 확인합니다.
- Threat Defense 디바이스가 DNS 스누핑을 수행하고 신뢰할 수 있는 DNS 서버를 구성할 수 있도록 각 WAN 디바이스에서 DNS 검사를 활성화합니다.
  1. **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 선택합니다.
  2. 편집할 Threat Defense 정책 옆에 있는 편집 아이콘을 클릭합니다.
  3. 왼쪽 창에서 **DNS**를 클릭합니다.
  4. **DNS Settings(DNS** 설정**)** 탭을 클릭합니다.
  5. **Enable DNS name resolution by device(**디바이스로 **DNS** 이름 확인 활성화**)** 체크 박스를 선택합니다.
  6. **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 탭을 클릭합니다.
  7. 다음 중 하나를 수행합니다.
     - **Trust Any DNS server(**모든 **DNS** 서버 신뢰**)** 토글 버튼을 클릭합니다.
     - **Specify DNS Servers(DNS** 서버 지정**)**에서 **Edit(**편집**)**을 클릭하여 신뢰할 수 있는 DNS 서버를 추가합니다.

SD-WAN 요약 대시보드를 사용하여 WAN 디바이스 및 인터페이스 모니터링

SD-WAN 요약 대시보드에는 **Overview(**개요**)** 탭 아래에 다음 위젯이 있습니다.

최상위 애플리케이션

이 위젯은 처리량에 따라 순위가 지정된 상위 10개 애플리케이션을 표시합니다.

Show Last(마지막 선택 표시**)** 드롭다운 목록에서 위젯 데이터에 대한 시간 범위를 선택할 수 있습니다. 범위는 15분~2주입니다.

WAN 연결성

이 위젯은 WAN 인터페이스 상태의 요약을 제공합니다. **Online(**온라인**)**, **Offline(**오프라인**)** 또는 **No Data(**데이터 없음**)** 상태인 WAN 인터페이스의 수가 표시됩니다. 이 위젯을 사용하여 하위 인터페이스를 모니터링할 수는 없습니다.

View All Interfaces(모든 인터페이스 보기**)**를 클릭하여 Health Monitor(상태 모니터) 페이지에서 인터페이스에 대한 자세한 정보를 확인합니다.

WAN 인터페이스가 **Offline(**오프라인**)** 또는 **No Data(**데이터 없음**)** 상태인 경우 Health Monitor(상태 모니터) 페이지에서 문제를 해결할 수 있습니다.

1. **Monitoring(**모니터링**)** 창에서 **Devices(**디바이스**)**를 확장합니다.
2. 디바이스별 상태 세부 정보를 보려면 해당 WAN 디바이스를 클릭합니다.
3. 특정 시간 동안의 인터페이스 상태와 집계 트래픽 통계를 보려면 **Interface(**인터페이스**)** 탭을 클릭합니다.

   View System and Troubleshoot Details(시스템 및 문제 해결 세부 정보 보기**)**를 클릭할 수도 있습니다. 모든 필요한 세부 정보가 포함된 Health Monitor(상태 모니터) 페이지가 표시됩니다.

VPN 토폴로지

이 위젯은 사이트 간 VPN 터널 상태의 요약을 제공합니다. **Active(**활성**)**, **Inactive(**비활성**)**, **No Active Data(**활성 데이터 없음**)** VPN 터널의 수가 표시됩니다.

사이트 간 **VPN** 모니터링 대시보드에서 VPN 터널 세부 정보를 보려면 **View All Connections(**모든 연결 보기**)**를 클릭합니다.

터널이 **Inactive(**비활성**)** 또는 **No Active Data(**활성 데이터 없음**)** 상태인 경우 사이트 간 **VPN** 모니터링 대시보드를 사용하여 문제를 해결할 수 있습니다. **Tunnel Status(**터널 상태**)** 위젯에서 토폴로지 위에 커서를 올려놓고 보기 아이콘을 클릭한 후 다음 중 하나를 수행합니다.

- VPN 터널의 세부 정보를 보려면 **CLI Details(CLI** 세부 정보**)** 탭을 클릭합니다.
- **Packet Tracer(**패킷 트레이서**)** 탭을 클릭하여 토폴로지에 패킷 트레이서 도구를 사용합니다.

인터페이스 처리량

이 위젯은 WAN 인터페이스의 처리량 사용률을 모니터링합니다.

인터페이스 처리량은 4개의 대역으로 분류됩니다. 이러한 세부 정보는 비용 계획 및 리소스에 도움이 됩니다. **Show Last(**마지막 선택 표시**)** 드롭다운 목록에서 위젯 데이터에 대한 시간 범위를 선택할 수 있습니다. 범위는 15분~2주입니다.

View Health Monitoring(상태 모니터링 보기**)**을 클릭하여 Health Monitor(상태 모니터) 페이지에서 인터페이스에 대한 자세한 정보를 확인합니다.

디바이스 인벤토리

이 위젯은 관리되는 모든 WAN 디바이스를 나열하고 모델에 따라 그룹화합니다.

View Device Management(디바이스 관리 보기**)**를 클릭하여 **Device Management(**디바이스 관리**)** 페이지에서 디바이스에 대한 자세한 정보를 확인합니다.

WAN 디바이스 상태

이 위젯은 WAN 디바이스의 상태에 따라 디바이스 수를 표시합니다. 오류/경고가 있거나 **Disabled(**비활성화**)** 상태인 디바이스의 수를 볼 수 있습니다.

View Health Monitoring(상태 모니터링 보기**)**을 클릭하여 알람을 확인하고 문제를 신속하게 식별, 격리 및 해결합니다.

디바이스의 상태가 영향을 받는 경우 Health Monitor(상태 모니터) 페이지에서 문제를 해결할 수 있습니다.

1. **Monitoring(**모니터링**)** 창에서 **Devices(**디바이스**)**를 확장합니다.
2. 디바이스별 상태 세부 정보를 보려면 해당 WAN 디바이스를 클릭합니다.
3. **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**)**를 클릭합니다. 모든 필요한 세부 정보가 포함된 Health Monitor(상태 모니터) 페이지가 표시됩니다.

디바이스는 다음을 포함한 여러 가지 이유로 **Disabled(**비활성화**)** 상태가 될 수 있습니다.

- 관리 인터페이스가 비활성화됩니다.
- 디바이스의 전원이 꺼져 있습니다.

• 디바이스가 업그레이드 중입니다.

SD-WAN 요약 대시보드를 사용하여 WAN 인터페이스의 애플리케이션 성능 메트릭 모니터링

Application Monitoring(애플리케이션 모니터링**)** 탭에서 WAN 디바이스를 선택하고 해당하는 WAN 인터페이스에 대한 애플리케이션 성능 메트릭을 볼 수 있습니다. 이러한 메트릭에는 지터, RTT(Round Trip Time), MOS(Mean Opinion Score) 및 패킷 손실이 포함됩니다.

기본적으로 메트릭 데이터는 5분마다 새로 고쳐집니다. 새로 고침 시간을 변경할 수 있습니다. 범위는 5~30분입니다. 메트릭을 테이블 및 그래픽 형식으로 볼 수 있습니다. 각 WAN 인터페이스에 대한 최신 메트릭 값이 테이블에 나열됩니다. 그래픽 데이터의 경우 최대 24시간까지의 시간 간격을 선택하여 해당하는 WAN 인터페이스에 대한 메트릭 데이터를 확인할 수 있습니다.

VPN 세션 및 사용자 정보

시스템은 네트워크에서 VPN 관련 활동을 포함한 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. 시스템 모니터링 기능을 통해 원격 액세스 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 원격 액세스 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/공개 IP 주소, 디바이스 세부 정보, 클라이언트 버전, 엔드포인트 정보, 처리량, 대역폭 소비 그룹 정책, 터널 그룹 등과 같은 지원 정보를 사용하여 지정된 시점에 현재 로그인한 VPN 사용자를 볼 수 있습니다. 시스템에서 현재 사용자 정보를 필터링하고, 사용자를 로그아웃하고, 요약 목록에서 사용자를 삭제할 수 있습니다.

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.

사이트 간 VPN 연결 이벤트 모니터링

사이트 간 VPN 연결 이벤트를 통해 VPN이 연결을 암호화하는지 또는 암호화하지 않는지 알 수 있으며, 특히 멀티 홉 VPN 구축에서 연결 문제를 해결하는 데 도움이 됩니다. management center의 이벤트 대시보드에는 트래픽을 암호화하거나 해독하는 VPN 피어(피어의 IKE 주소)의 IP 주소가 표시되며 VPN 작업이 다음과 같이 표시됩니다.

- VPN에 의해 연결이 암호 해독된 경우 **Decrypt Peer(**피어 암호 해독**)** 열에 트래픽을 암호 해독하는 VPN 피어의 IP 주소가 표시되며 VPN 작업으로 **Decrypt(**암호 해독**)**가 표시됩니다.
- 연결이 VPN에 의해 암호화된 경우 **Encrypt Peer(**피어 암호화**)** 열에 트래픽을 암호화하는 VPN 피어의 IP 주소가 표시되고 VPN 작업으로 암호화가 표시됩니다.
- VPN 서버가 연결을 캐스케이딩하는 경우 한 터널에서 암호 해독되고 다른 터널에서 다시 암호화됩니다. 이 경우 **Encrypt Peer(**피어 암호화**)** 및 **Decrypt Peer IP addresses get(**피어 **IP** 주소 암호 해독**)**이 모두 이벤트에 나타납니다. **VPN Action(VPN** 작업**)** 열에는 VPN 서버를 통해 연결이 전송됨을 나타내는 작업으로 **VPN** 라우팅이 표시됩니다.

암호 해독된 트래픽에 대해 액세스 제어 정책 우회(sysopt permit-vpn) 옵션을 활성화하는 경우 시스템이 액세스 제어 정책을 우회하고 암호 해독된 트래픽의 이벤트를 기록하지 않습니다. 이 옵션은 기본적으로 비활성화되어 있으며 VPN 터널의 암호 해독된 모든 트래픽은 ACL 검사를 받습니다.

사이트 간 VPN 연결 이벤트 보기

management center의 연결 이벤트 뷰어에 액세스하여 VPN이 연결 트래픽을 암호화하는지 여부를 확인하고 VPN 피어 세부 정보를 검색합니다.

시작하기 전에

액세스 제어 규칙에서 연결을 시작할 때와 종료할 때 연결 이벤트 로깅을 활성화해야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** **Table View of Connection Events(**연결 이벤트 테이블 보기**)** 탭으로 이동합니다.

단계 **3** 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 표시되는 필드를 변경하려면 임의의 열 이름에서 **x** 아이콘을 클릭하여 필드 선택기를 표시합니다.

단계 **4** 다음 열을 선택합니다.

- 피어 암호 해독
- 피어 암호화
- VPN 작업

단계 5 **Apply(**적용**)**를 클릭합니다.

연결 이벤트에 대한 자세한 내용은 Secure Firewall Management Center 관리 가이드의 연결 및 보안 관련 연결 이벤트를 참조하십시오.

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

threat defense 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. VPN 로깅을 활성화하면 threat defense 디바이스는 분석 및 보관을 위해 VPN 시스템 로그를 Secure Firewall Management Center에 보냅니다.

모든 VPN 시스템 로그가 기본 심각도 수준 'ERROR' 이상으로 나타납니다(변경되지 않은 경우). threat defense 플랫폼 설정을 통해 VPN 로깅을 관리할 수 있습니다. 대상 디바이스(**Platform Settings(**플랫폼 설정**)** > **Syslog(**시스템 로그**)** > **Logging Setup(**기록 설정**)**에 대한 threat defense 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 Syslog 섹션을 참조하십시오.

참고 사이트 간 또는 원격 액세스 VPN을 사용하여 디바이스를 구성하면 기본적으로 management center에 VPN 시스템 로그를 자동으로 전송할 수 있습니다.

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

threat defense 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 Syslog 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. 여기에 설명된 명령은 전체가 아니며, 이 섹션에는 VPN 관련 문제를 진단하는 데 도움이 되는 명령이 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. ?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 나타납니다.

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

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

debug aaa

디버깅 구성 또는 AAA(인증, 권한 부여 및 계정) 설정은 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

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

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

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

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

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

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

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 Secure Client 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

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