Secure Firewall Management Center 상태 모니터, 버전 7.2에서 수집한 Secure Firewall Threat Defense 디바이스 메트릭

초판: 2023년 6월 20일

최종 변경: 2023년 12월 29일

Secure Firewall Management Center 상태 모니터가 수집하는 Secure Firewall Threat Defense 디바이스 메트릭

디바이스 상태 모니터에는 시스템 이벤트를 예측하고 응답하는 데 사용되는 주요 threat defense 디바이스 메트릭 어레이가 포함되어 있습니다. 보고된 메트릭을 통해 모든 threat defense 디바이스의 상태를 확인할 수 있습니다. 이 문서에서는 모든 상태 모니터 대시보드 및 보고된 메트릭의 목록을 제공합니다.

CPU 그룹 메트릭

상태 모니터는 프로세스 및 물리적 코어별 CPU 사용률을 포함하여 CPU 이용률과 관련된 통계를 추적합니다.

표 *1: CPU* 그룹 메트릭

메트릭	설명	형식
컨트롤 플레인	지난 1분 동안 제어 플레인의 평균 CPU 사용률입니다.	백분율
데이터 플레인	지난 1분 동안 데이터 플레인의 평균 CPU 사용률입니다.	백분율
Snort	지난 1분 동안 Snort 프로세스의 평균 CPU 사용률입니다.	백분율
시스템	지난 1분 동안 시스템 프로세스의 평균 CPU 사용률입니다.	백분율
물리적 코어	지난 1분 동안의 모든 코어에 대한 평균 CPU 사용률입니다.	백분율

메모리 그룹 메트릭

상태 모니터는 데이터 플레인 및 Snort 메모리 사용량을 포함하여 디바이스 메모리 사용률과 관련된 통계를 추적합니다.

표 *2:* 메모리 그룹 메트릭

메트릭	설명	형식
버퍼 캐시	버퍼 캐시입니다.	바이트
여유 공간	사용 가능한 총 메모리입니다.	바이트
최대 데이터 플레인	데이터 플레인에서 사용하는 최대 메모리입니다.	바이트
최대 Snort	Snort 프로세스에서 사용하는 최대 메모리입니다.	바이트
Snort에 대한 최대 스왑	Snort 프로세스에서 사용하는 최대 스왑 메모리입니다.	바이트
남은 메모리 블록(1550)	1550 바이트 블록의 사용 가능한 메모리입니다.	숫자
남은 메모리 블록(256)	256 바이트 블록의 사용 가능한 메모리입니다.	숫자
사용된 시스템	시스템에서 사용한 총 메모리입니다.	바이트
합계	사용 가능한 총 메모리입니다.	바이트
총 스왑	스왑에 사용 가능한 총 메모리입니다.	바이트
데이터 플레인	데이터 플레인에서 사용된 총 메모리입니다.	바이트
데이터 플레인에서 사용된 비율	데이터 플레인에 사용된 메모리의 비율입니다.	백분율
Snort에서 사용된 비율	Snort 프로세스에 사용된 메모리의 비율입니다.	백분율
스왑에서 사용된 비율	스왑에 사용된 메모리의 비율입니다.	백분율
시스템에서 사용된 비율	시스템에 사용된 메모리의 비율입니다.	백분율
시스템 및 스왑에서 사용된 비율	시스템 및 스왑에 사용된 메모리의 비율입니다.	백분율
Snort	Snort 프로세스에 사용된 총 메모리입니다.	바이트
사용된 스왑	스왑에 사용된 총 메모리입니다.	바이트
Snort에서 사용된 스왑	Snort 프로세스에 사용된 총 스왑 메모리입니다.	바이트

인터페이스 그룹 메트릭

상태 모니터는 인터페이스 상태 및 집계 트래픽 통계를 포함하여 디바이스 인터페이스와 관련된 통계를 추적합니다.

표 ***3:*** 인터페이스 그룹 메트릭

메트릭	설명	형식
패킷 삭제	드롭된 패킷 수입니다.	숫자
평균 입력 패킷 크기	수신 패킷의 평균 크기입니다.	바이트
입력 속도	총 수신 바이트 수입니다.	바이트
입력 패킷	총 수신 패킷 수입니다.	숫자
평균 출력 패킷 크기	발신 패킷의 평균 크기입니다.	바이트
출력 속도	총 발신 바이트 수입니다.	바이트
출력 패킷	총 발신 패킷 수입니다.	숫자
상태	인터페이스의 상태로, 1은 up(가동), 0은 down(중지)입니다.	1 또는 0
CRC 오류	CRC(Cyclic Redundancy Check) 오류가 발생한 총 패킷 수입니다.	숫자
입력 오류	입력 오류 수입니다.	숫자
출력 오류	출력 오류 수입니다.	숫자
오버런 오류	입력 속도가 수신 데이터를 처리하는 수신기의 기능을 초과하여 삭제된 패킷 수입니다.	숫자
언더런 오류	송신기가 라우터가 처리할 수 있는 속도보다 빠르게 실행되어 삭제된 패킷 수입니다.	숫자
L2 디코드 삭제	이름이 구성되지 않았거나(nameif command) VLAN ID가 잘못된 프레임이 수신되어 삭제된 패킷 수입니다.	숫자
Jitter(지터)	패킷 플로우의 레이턴시 변화	마이크로초
MOS(평균 의견 점수)	연결의 품질 측정 단위는 0~5이며, 5가 가장 뛰어납니다.	0~5
패킷 손실	대상에 도달하지 않은 전송된 패킷의 백분율입니다.	백분율

메트릭	설명	형식
왕복 시간	ICMP 에코 요청과 응답 사이의 평균 지속 시간.	마이크로초

연결 그룹 메트릭

상태 모니터는 연결 및 NAT 변환 수와 관련된 통계를 추적합니다.

표 *4:* 연결 그룹 메트릭

메트릭	설명	형식
활성 엘리펀트 플로우	활성 엘리펀트 플로우 수를 보여줍니다. 엘리펀트 플로우는 전체 시스템 성능에 영향을 줄 수 있을 만큼 큰 연결입니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큰 상태입니다. **system support elephant-flow-detection** 명령을 사용하여 threat defense CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다. 참고 바이트 및 시간 임계값이 모두 초과되는 경우에만 플로우가 Elephant 플로우로 간주됩니다.	숫자
활성 연결	활성 연결 수를 표시합니다.	숫자
최대 연결 수	최대 동시 연결 수를 표시합니다.	숫자
초당 전체 연결 수	모든 연결 유형에 대한 초당 연결 수입니다.	숫자
초당 TCP 연결 수	TCP 연결 유형의 초당 연결 수입니다.	숫자
초당 UDP 연결 수	UDP 연결 유형의 초당 연결 수입니다.	숫자
활성화된 연결 유지	Snort 프로세스가 중단될 경우 라우팅 및 투명 인터페이스에서 기존 TCP/UDP 연결을 유지합니다.	숫자
유지되는 연결	현재 유지되는 연결이 활성화된 연결 수입니다.	숫자
가장 활성화된 연결 유지	지금까지 유지되는 가장 많은 연결 수입니다.	숫자
유지되는 최대 연결 수	지금까지 유지되는 가장 많은 최대 연결 수입니다.	숫자
NAT 변환	변환 수를 표시합니다.	숫자
최대 NAT 변환	동시 변환의 기록 최대 값을 한 번에 표시합니다.	숫자

Snort 그룹 메트릭

상태 모니터는 Snort 프로세스와 관련된 통계를 추적합니다.

표 *5: Snort* 그룹 메트릭

메트릭	설명	형식
차단된 목록 플로우	Snort에서 삭제한 정책 설정의 플로우 수입니다.	숫자
차단된 패킷	차단된 패킷 수입니다.	숫자
거부된 플로우	거부된 플로우 이벤트 수입니다. 데이터 플레인은 Snort로 전송하기 전에 플로우를 삭제하기로 결정하면 거부된 플로우 이벤트를 Snort로 전송합니다.	숫자
플로우 종료	데이터 플레인은 빠른 경로 플로우가 종료되면 Snort에 플로우 종료 이벤트를 전송합니다.	숫자
빠른 전달 플로우	정책에 의해 빨리 전달되어 검사되지 않은 플로우 수입니다.	숫자
데이터 플레인에서 전달된 삭제된 프레임	데이터 플레인에서 전달된 삭제된 프레임 수입니다.	숫자
삽입된 패킷 삭제됨	Snort가 삭제된 트래픽 스트림에 추가한 패킷 수입니다.	숫자
삽입된 패킷	Snort가 생성하여 트래픽 스트림에 추가한 패킷 수입니다. 예를 들어 재설정 작업으로 파단을 구성하는 경우, Snort는 연결을 재설정할 패킷을 생성합니다.	숫자
인스턴스	Snort 인스턴스(프로세스) 수입니다.	숫자
패킷 수신 대기열 사용률	데이터 플레인 수신 대기열의 대기열 사용률입니다.	백분율
Snort가 사용 중이어서 패킷 우회됨	Snort 사용량이 너무 많아 패킷을 처리할 수 없을 때 검사를 우회한 패킷 수입니다.	숫자
Snort 다운으로 인해 패킷 우회됨	Snort가 중단되었을 때 검사를 우회한 패킷 수입니다.	숫자
RX 대기열이 꽉 차서 패킷 우회됨	수신 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자

메트릭	설명	형식
TX 대기열이 꽉 차서 패킷 우회됨	전송 대기열이 꽉 차서 우회된 패킷 수입니다.	숫자
통과된 패킷	데이터 플레인에서 Snort로 전송된 패킷 수입니다.	숫자
플로우 시작	플로우 시작 이벤트 수입니다. 이러한 이벤트는 Snort가 연결을 추적하고 연결 이벤트를 보고하는 데 도움이 됩니다.	숫자

ASP 삭제 메트릭

상태 모니터는 ASP(Accelerated Security Path) 삭제된 패킷 또는 연결과 관련된 통계를 추적합니다.

표 ***6: ASP*** 삭제 메트릭

메트릭	설명	형식
연결 제한이 초과됨	연결 제한이 초과되었을 때 닫히는 플로우 수를 계산합니다.	숫자
연결 제한에 도달함	연결 제한 또는 호스트 연결 제한을 초과했을 때 손실된 패킷 수를 계산합니다.	숫자
액세스 규칙에 의해 거부된 플로우	액세스 규칙에 의해 거부된 연결 수입니다.	숫자
구성된 규칙에 의해 거부된 플로우	구성된 규칙에 의해 거부된 연결 수입니다.	숫자
L2 규칙 삭제	레이어 2 ACL로 인해 거부된 패킷 수를 계산합니다.	숫자
L2 규칙 VXLAN 삭제	레이어 2 ACL 검사를 적용할 때 VXLAN out_tag를 찾지 못하여 거부된 패킷 수를 계산합니다.	숫자
NAT 역방향 경로 실패	변환된 호스트의 실제 주소를 사용하여 변환된 호스트에 연결하는 거부된 시도 횟수를 계산합니다.	숫자
NAT 실패	IP 또는 전송 헤더를 변환하는 xlate를 생성하려고 시도했지만 실패한 횟수를 계산합니다.	숫자
유효한 v4 인접성 없음	보안 어플라이언스가 인접 항목을 가져오려고 했지만 다음 홉(IPv4)에 대한 MAC 주소를 가져올 수 없는 경우 손실된 패킷 수를 계산합니다.	숫자

메트릭	설명	형식
유효한 v6 인접성 없음	보안 어플라이언스가 인접성을 가져오려고 했는데 다음 홉의 MAC 주소를 가져올 수 없으면 이 카운터의 값이 증가합니다.	숫자
Snort에 의해 차단 목록에 나열된 패킷; Snort에 의해 차단된 패킷	Snort 모듈의 요청에 따라 삭제된 패킷 수를 계산합니다.	숫자
프레임 삭제 - Snort 사용 중; 프레임 삭제 - Snort 다운; 프레임 삭제 – Snort 삭제	Snort 모듈이 사용 중이며 프레임을 처리할 수 없으므로 삭제된 프레임 수를 계산합니다. Snort 모듈이 중단되었습니다. Snort 모듈은 삭제를 요청합니다.	숫자
디스패치 대기열 제한에 도달함	디바이스의 로드 밸런싱 ASP 디스패처가 큐 제한에 도달하는 횟수를 계산합니다. 이보다 더 많은 패킷을 포함하려고 하면 tail drop이 수행되며 이 카운터의 값이 증가합니다.	숫자
대상 MAC L2 조회에 실패함	실패한 레이어 2 대상 MAC 주소 조회 수를 계산합니다. 조회 장애 시 어플라이언스는 대상 MAC 검색 프로세스를 시작하여 ARP 및/또는 ICMP 메시지를 통해 호스트 위치를 찾으려고 합니다.	숫자
검사 실패	네트워크 프로세서가 연결에 대해 수행하는 프로토콜 검사를 실행하지 못하는 횟수를 계산합니다. 메모리 할당 장애가 원인일 수도 있고, ICMP 오류 메시지의 경우에는 ICMP 오류 메시지에 임베드된 프레임과 관련하여 설정된 연결을 어플라이언스가 찾을 수 없는 것일 수도 있습니다.	숫자
NAT PAT 풀에 대한 xlate 없음	PAT 풀의 매핑된 주소와 일치하는 대상이 있는 연결에 대해 기존의 xlate를 찾을 수 없습니다.	숫자
호스트로의 경로 없음	보안 어플라이언스가 인터페이스 외부로 패킷을 전송하려고 하지만 라우팅 테이블에서 패킷을 찾을 수 없는 횟수입니다.	숫자
PDTS 펀트 제한 초과됨	데이터 경로에서 패킷을 검사기로 펀트하는데 Snort에 대기된 패킷 수가 최대 제한을 초과한 경우 삭제된 패킷 수입니다.	숫자
펀트 제한	제한에 도달한 검사에 대기된 패킷으로 인해 삭제된 패킷 수입니다.	숫자
Snort 자동 삭제	Snort 모듈의 요청에 따라 패킷이 자동으로 삭제되는 횟수입니다.	숫자

메트릭	설명	형식
SYN에 없는 첫 번째 TCP 패킷	비 SYN 패킷이 비가로채기/비고정 연결의 첫 번째 패킷으로 수신되는 횟수입니다.	숫자

하드웨어/환경 상태 메트릭

하드웨어/환경 상태 모니터는 위협 방어 하드웨어 엔터티와 관련된 통계를 추적하고 메트릭 값을 수집합니다.

표 *7:* 하드웨어/환경 상태 메트릭

메트릭	설명	형식
팬 속도	섀시 팬 속도입니다.	RPM
입구 온도	흡입구 센서의 온도입니다.	섭씨
내부 온도	내부 센서의 온도입니다.	섭씨
출구 온도	출구 센서의 온도입니다.	섭씨
SSD1	SSD1의 상태입니다.	숫자
시스템 업타임	시스템이 활성 상태인 기간입니다.	초

하드웨어 / 환경 상태 메트릭의 가용성은 threat defense 디바이스의 모델에 따라 달라질 수 있습니다. 다음 표에서는 각 디바이스 모델에 사용할 수 있는 메트릭에 대해 설명합니다.

표 *8:* 디바이스 모델별 하드웨어/환경 상태 메트릭

메트릭	**1000** 시리즈	**2100** 시리즈	**3100** 시리즈	**4100** 시리즈	**9300** 시리즈	**SSP**
시스템 업타임	예	예	예	예	예	예
팬 속도	예	예	예	아니요	아니요	아니요
내부 온도	예	예	예	아니요	아니요	아니요
입구 온도	아니요	아니요	아니요	아니요	아니요	아니요
출구 온도	아니요	아니요	아니요	아니요	아니요	아니요
SSD1 상태	예	예	예	아니요	아니요	아니요

구축된 컨피그레이션 그룹 메트릭

상태 모니터는 구축된 설정과 관련된 통계(예: IPS 규칙 수 및 ACE 수)를 추적합니다.

표 ***9:*** 구축된 설정 그룹 메트릭

메트릭	설명	형식
ACE의 수	ACE(Access Control Entry) 또는 규칙의 수입니다. ACL(액세스 제어 목록)은 하나 이상의 ACE 또는 규칙으로 구성됩니다.	숫자
규칙의 수	침입 정책에 있는 규칙의 수입니다.	숫자

디스크 그룹 메트릭

상태 모니터는 디스크 크기 및 파티션별 디스크 사용률을 포함하여 디바이스 디스크 사용과 관련된 통계를 추적합니다.

표 ***10:*** 디스크 그룹 메트릭

메트릭	설명	형식
합계	디바이스 디스크의 총 크기입니다.	바이트
사용됨	디바이스 디스크에서 사용된 총 공간입니다.	바이트
/ngfw에서 사용된 비율	/ngfw 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/ngfw/Volume에서 사용된 비율	/ngfw/Volume 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/dev/cgroups에서 사용된 비율	/dev/cgroups 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/mnt/disk0에서 사용된 비율	/mnt/disk0 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율
/var/volatile에서 사용된 비율	/var/volatile 파티션에서 사용하는 디스크 공간의 백분율입니다.	백분율

중요 프로세스 그룹 메트릭

상태 모니터는 관리되는 프로세스의 프로세스 재시작과 관련된 통계를 추적합니다. 또한 각 중요 프로세스에 대해 상태 모니터는 CPU 사용률, 메모리 사용률, 업타임 및 상태를 추적합니다.

표 ***11:*** 중요 프로세스 그룹 메트릭

메트릭	설명	형식
CPU 사용률	프로세스 시작 이후 프로세스의 CPU 사용률입니다.	백분율
재시작 횟수	threat defense 디바이스 부팅 이후 프로세스가 다시 시작된 횟수입니다. 프로세스가 너무 자주 재시작되는 경우 이 메트릭이 1분마다 실행되므로 재시작 횟수 메트릭은 정확한 숫자를 반영하지 않을 수 있습니다.	숫자
예기치 않은 재시작 횟수	threat defense 디바이스가 부팅된 이후 프로세스가 예기치 않게 재시작된 시간입니다.	숫자
상태	프로세스의 상태입니다.	다음 중 하나에 해당합니다. • 시작됨 • 실행 중 • 중단 • 대기 중 • 잠김 • 비활성화 비활성화된 사용자
실행 시간	프로세스가 실행 중인 기간입니다.	초
사용된 메모리	프로세스에서 사용된 RSS 메모리입니다.	바이트

NTP 서버 그룹 메트릭

상태 모니터는 매니지드 디바이스의 NTP 시계 동기화 상태와 관련된 통계를 추적합니다.

표 12: NTP 서버 그룹 메트릭

메트릭	설명	형식
Delay(연기)	NTP 서버 연결이 지연되고 있습니다.	밀리초
Jitter(지터)	디바이스와 NTP 서버 간의 네트워크 지연입니다.	밀리초
마지막으로 폴링됨	디바이스가 NTP 서버에 대한 마지막 폴링 이후의 시간입니다.	초
오프셋	로컬 시계와 NTP 서버의 시계 사이의 차이입니다.	초
지원 범위	8진수로 최신 8개의 NTP 업데이트입니다. 예를 들어, 8개의 성공적인 시도는 377로 표시됩니다.	숫자

플로우 오프로드 통계 그룹 메트릭

상태 모니터링은 Threat Defense 9300 및 4100 플랫폼에서 하드웨어 플로우 오프로드 통계를 추적합니다.

표 13: 플로우 오프로드 통계 그룹 메트릭

메트릭	설명	형식
사용 중	현재 오프로드된 플로우 수입니다.	숫자
가장 많이 사용됨	지금까지 확인된 오프로드된 최대 플로우 수입니다.	숫자
충돌 플로우 수	동시에 동일한 하드웨어 오프로드 위치와 일치하는 여러 플로우의 수입니다.	숫자
오프로드 비율	현재 하드웨어로 오프로드된 총 플로우의 백분율입니다.	백분율

경로 통계 그룹 메트릭

상태 모니터는 threat defense 디바이스에서 IPv4 및 IPv6 경로 정보를 모두 추적합니다.

표 14: 경로 통계 그룹 메트릭

메트릭	설명	형식
현재 IPv4 및 IPv6 경로	현재 IPv4 및 IPv6 경로의 수입니다.	숫자

메트릭	설명	형식
전역 IPv4 경로	전역 IPv4 경로입니다.	숫자
전역 IPv6 경로	전역 IPv6 경로입니다.	숫자
최대 IPv4 및 IPv6 경로	IPv4 및 IPv6의 최대 경로 수입니다.	숫자
VRF 당 총 IPv4 경로 수	VRF 당 총 IPv4 경로 수입니다.	숫자
VRF 당 총 IPv6 경로 수	VRF 당 총 IPv6 경로 수입니다.	숫자

VPN 그룹 메트릭

상태 모니터링은 사이트 간 및 원격 액세스 VPN 터널 통계를 추적합니다.

표 ***15: VPN*** 그룹 메트릭

메트릭	설명	형식
활성 RA VPN 터널	활성 원격 액세스 VPN 터널 수입니다.	숫자
활성 S2S VPN 터널	활성 사이트간 VPN 터널 수입니다.	숫자
누적 RA VPN 세션	지금까지 활성 상태였던 원격 액세스 VPN 터널의 총 수입니다.	숫자
누적 S2S VPN 세션	지금까지 활성 상태였던 사이트 간 VPN 터널의 총 수입니다.	숫자
비활성 RA VPN 터널	비활성 원격 액세스 VPN 터널 수입니다.	숫자
최대 동시 RA VPN 터널	지금까지 동시에 활성이었던 원격 액세스 VPN 터널의 최대 수입니다.	숫자
최대 동시 S2S VPN 터널	지금까지 동시에 활성이었던 사이트 간 VPN 터널의 최대 수입니다.	숫자

AMP 연결 그룹 메트릭

상태 모니터링은 threat defense 디바이스에서 AMP 클라우드 연결 상태를 추적합니다.

표 *16:*

메트릭	설명	형식
연결 상태	AMP 클라우드 연결 상태입니다.	0~5의 숫자로 구성됩니다. • 0은 비활성화됨을 나타냅니다. • 1은 대기 중을 나타냅니다. • 2는 실행 중을 나타냅니다. • 3은 구성되지 않음을 나타냅니다. • 4는 AMP 클라우드 연결이 켜져 있음을 나타냅니다. • 5는 AMP 클라우드 연결이 꺼져 있음을 나타냅니다.

AMP Threat Grid 연결 그룹 메트릭

상태 모니터링은 threat defense 디바이스에서 AMP Threat Grid 클라우드 연결 상태를 추적합니다.

표 *17:*

메트릭	설명	형식
연결 상태	AMP Threat Grid 클라우드 연결 상태입니다.	0~5의 숫자로 구성됩니다. • 0은 비활성화됨을 나타냅니다. • 1은 대기 중을 나타냅니다. • 2는 실행 중을 나타냅니다. • 3은 구성되지 않음을 나타냅니다. • 4는 AMP Threat Grid 클라우드 연결이 켜져 있음을 나타냅니다. • 5는 AMP Threat Grid 클라우드 연결이 꺼져 있음을 나타냅니다.

디바이스 상태 메트릭 내역

기능	버전	세부정보
엘리펀트 플로우 탐지	7.1	상태 모니터에는 다음과 같은 향상된 기능이 포함됩니다. • 연결 통계에는 활성 엘리펀트 플로우가 포함됩니다. • Connection Group Metrics(연결 그룹 메트릭)에는 활성 엘리펀트 플로우의 수가 포함됩니다.
새 상태 모듈	7.0	다음 상태 모듈을 추가했습니다. • AMP Connection Status(AMP 연결 상태): threat defense에서 AMP 클라우드 연결을 모니터링합니다. • AMP Threat Grid Status(AMP Threat Grid 상태): threat defense에서 AMP Threat Grid 클라우드 연결을 모니터링합니다. • ASP Drop(ASP 삭제): 데이터 플레인 가속 보안 경로에 의해 삭제된 연결을 모니터링합니다. • Advanced Snort Statistics(고급 Snort 통계): 패킷 성능, 흐름 카운터 및 흐름 이벤트와 관련된 Snort 통계를 모니터링합니다. • Hardware and Environment Status(하드웨어 및 환경 상태): threat defense 디바이스 하드웨어 및 환경 메트릭을 모니터링합니다. • Flow Offload(플로우 오프로드): threat defense 9300 및 4100 플랫폼에서 하드웨어 플로우 오프로드 통계를 모니터링합니다. • NTP Status(NTP 상태): 매니지드 디바이스의 NTP 클럭 동기화 상태를 모니터링합니다. • Routing Statistics(라우팅 통계): 에서 IPv4 및 IPv6 경로 정보를 모두 모니터링합니다.threat defense • SSE Connection Status(SSE 연결 상태): threat defense에서 SSE 클라우드 연결을 모니터링합니다. • VPN Statistics(VPN 통계): 사이트 간 및 원격 액세스 VPN 터널 통계를 모니터링합니다. • TLS Counters(TLS 카운터): xTLS/SSL 플로우, 메모리 및 캐시 효율성을 모니터링합니다.

기능	버전	세부정보
새 상태 모듈	6.7	다음 메트릭이 CPU 사용량을 추적하기 위해 추가되었습니다. • CPU 사용(코어 당): 모든 코어의 CPU 사용을 모니터링합니다. • CPU 사용 데이터 플레인: 디바이스에서 모든 데이터 플레인 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용 데이터 Snort: 디바이스에서 Snort 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용량 시스템: 디바이스에 있는 모든 시스템 프로세스의 평균 CPU 사용량을 모니터링합니다. 다음 메트릭 그룹은 디바이스 상태 통계를 추적하기 위해 추가됩니다. • 연결 통계: 연결 통계 및 NAT 변환 수를 모니터링합니다. • 중요 프로세스 통계: 이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다. • 구축된 구성 통계: 구축 된 구성에 대한 통계(예: ACE 및 IPS 규칙 수)를 모니터링합니다. • Snort 통계: 이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다. 다음 메트릭이 메모리 사용량을 추적하기 위해 추가되었습니다. • 메모리 사용 데이터 플레인: 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다. • 메모리 사용량 Snort: Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다.