Secure Web Appliance 레이턴시 트러블슈팅

목차

소개

이 문서에서는 Cisco SWA(Secure Web Appliance)에서 높은 레이턴시, 높은 디스크, 높은 CPU를 해결하기 위한 트러블슈팅 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SWA 관리
- 프록시 구축 방법(명시적 및 투명)
- SWA CLI(Command Line Interface) 명령

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

배경 정보

Cisco 기술 지원에 문의할 때 SWA 아웃바운드 및 인바운드 네트워크 활동에 대한 세부 정보를 제공하라는 메시지가 표시됩니다. 이는 디버깅 또는 확인을 위해 트래픽을 수집하기 위해 패킷 캡처를 실행하여 모니터링할 수 있습니다.

SWA에서 높은 레이턴시의 빈번한 원인

일반적으로 SWA에서는 높은 레이턴시에 대한 세 가지 주요 범주가 있습니다.

1. 부적절한 SWA 크기 조정 또는 리소스 과부하
2. 복잡한 구성
3. 네트워크 관련 지연 문제

SWA에서 레이턴시가 높은 가장 일반적인 원인 중 하나는 솔루션의 부적절한 크기 조정입니다. SWA 시스템에 현재 및 예상 워크로드를 처리할 수 있는 충분한 리소스가 있는지 확인하려면 적절한 크기 조정이 중요합니다. 시스템의 크기가 작아지면 요청을 효율적으로 처리하는 데 어려움을 겪게 되어 운영이 지연되고 성능이 저하될 수 있습니다. 사용자 수, 암호 해독 볼륨, 특정 검색 요구 등의 요인은 리소스 제한을 피하기 위해 구축 과정에서 신중하게 평가해야 합니다. SWA 용량을 조직의 요구 사항에 맞게 조정하지 못하면 지속적인 레이턴시가 발생하고 사용자 환경이 저하될 수 있습니다.

복잡한 컨피그레이션은 성능을 저하시키고 특히 로드가 높은 SWA의 레이턴시를 야기할 수 있습니다. 각 요청은 다양한 조건을 통해 처리되어야 하기 때문입니다.

네트워크 관련 레이턴시는 SWA 자체, Active Directory, DLP, DNS 같은 서드파티 서비스 또는 클라이언트, SWA 및 업스트림 서버 간의 네트워크 지연에서 비롯될 수 있습니다.

상위 사용자 및 가장 많이 액세스한 URL을 포함하여 SWA로 전송된 요청을 분석하면 잠재적인 오동작을 찾아내고 레이턴시의 근본 원인을 정확하게 찾아낼 수 있습니다. 이 정보는 성능 문제를 진단하고 대역폭 소비를 관리하며 시스템의 적절한 사용을 보장하는 데 매우 유용합니다.

SWA 레이턴시 트러블슈팅 툴

시스템 상태

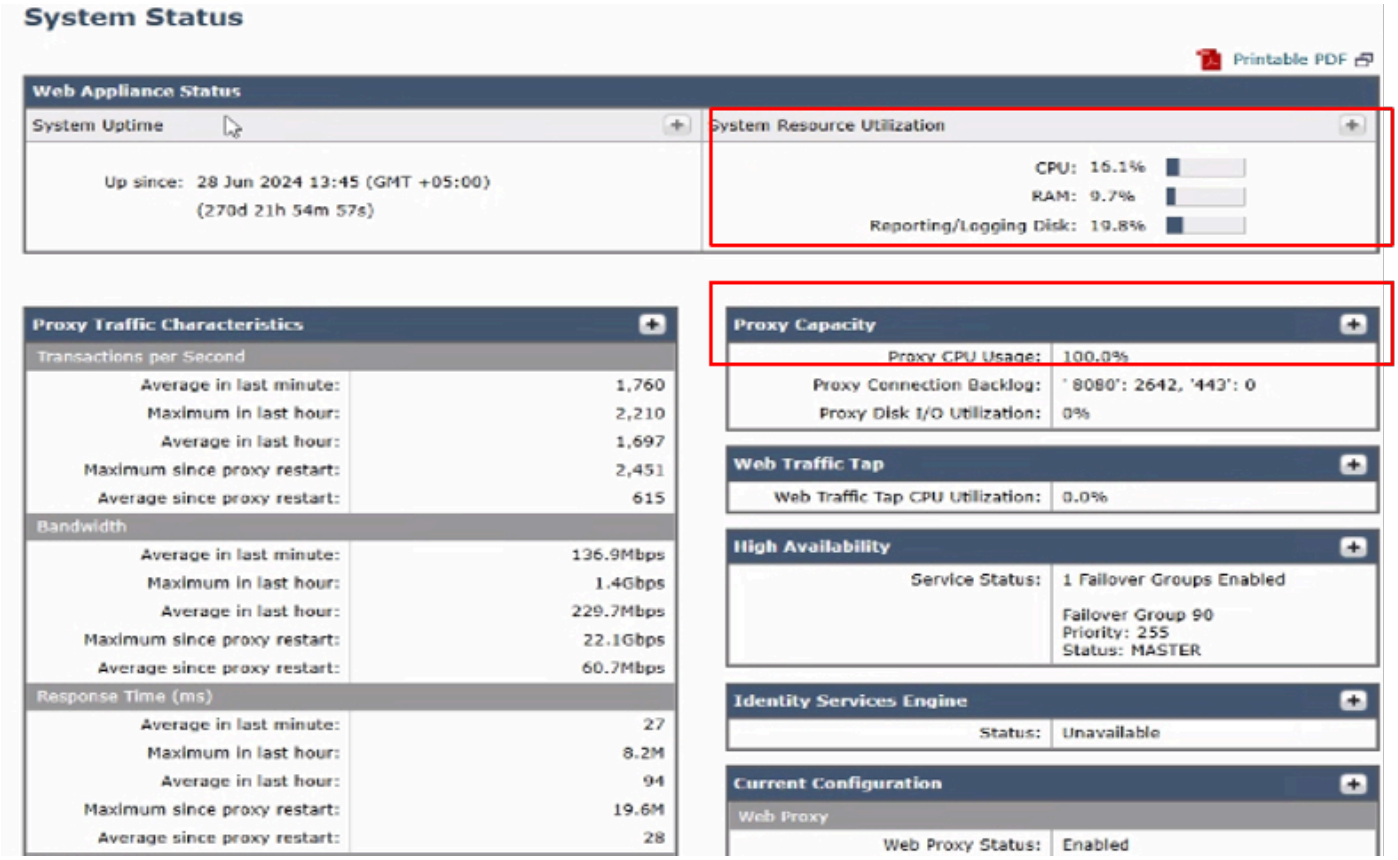
다음 단계를 사용하여 SWA의 현재 리소스 사용량을 확인합니다.

1단계. SWA GUI(Graphical User Interface)에 액세스합니다.

2단계. Reporting(보고) > System Information(시스템 정보) > System Status(시스템 상태)로 이동합니다.

3단계. 시스템 성능을 평가하려면 다음 중요 메트릭스를 확인합니다.

- CPU 사용량(%): 현재 CPU 로드를 나타냅니다.
- RAM 사용량(%): 메모리 사용률을 반영합니다.
- 보고/로깅 사용량(%): 보고 및 로깅에 사용되는 디스크 공간의 비율을 표시합니다
- 시스템 가동 시간: 시스템을 다시 시작하지 않고 실행한 총 시간을 표시합니다



이미지 - 시스템 상태

이 페이지에서는 RAM, CPU 및 디스크 사용량의 현재 상태에 대한 개요를 제공합니다. 시간에 따른 리소스 사용량을 보려면 SWA GUI에서 Reporting(보고)으로 이동하고 System Capacity(시스템 용량)를 선택합니다.

시스템 용량

SWA의 [시스템 용량] 페이지는 지정된 시간 범위에 걸친 리소스 사용률 및 성능 측정 단위의 포괄적인 보기를 제공합니다. 이 페이지에서는 시스템 동작을 모니터링 및 분석하여 최적의 성능을 보장하고 잠재적인 병목 지점을 파악하는 데 도움이 되는 자세한 그래프를 제공합니다.

System Capacity(시스템 용량) 페이지에서 사용 가능한 그래프 및 메트릭은 다음과 같습니다.

1. 전체 CPU 사용량: 총 CPU 사용량을 표시하여 시스템 성능을 개괄적으로 보여 줍니다.
2. 기능별 CPU 사용량: 다음을 비롯한 특정 기능에 따라 CPU 사용량을 세분화합니다.

- 웹 프록시
- 로깅
- 보고
- 맥아피
- 소포스
- 웹루트
- 허용 가능한 사용 및 평판

3. 응답 시간/대기 시간(밀리초): 처리 요청의 지연을 식별하기 위한 응답 시간을 추적합니다.

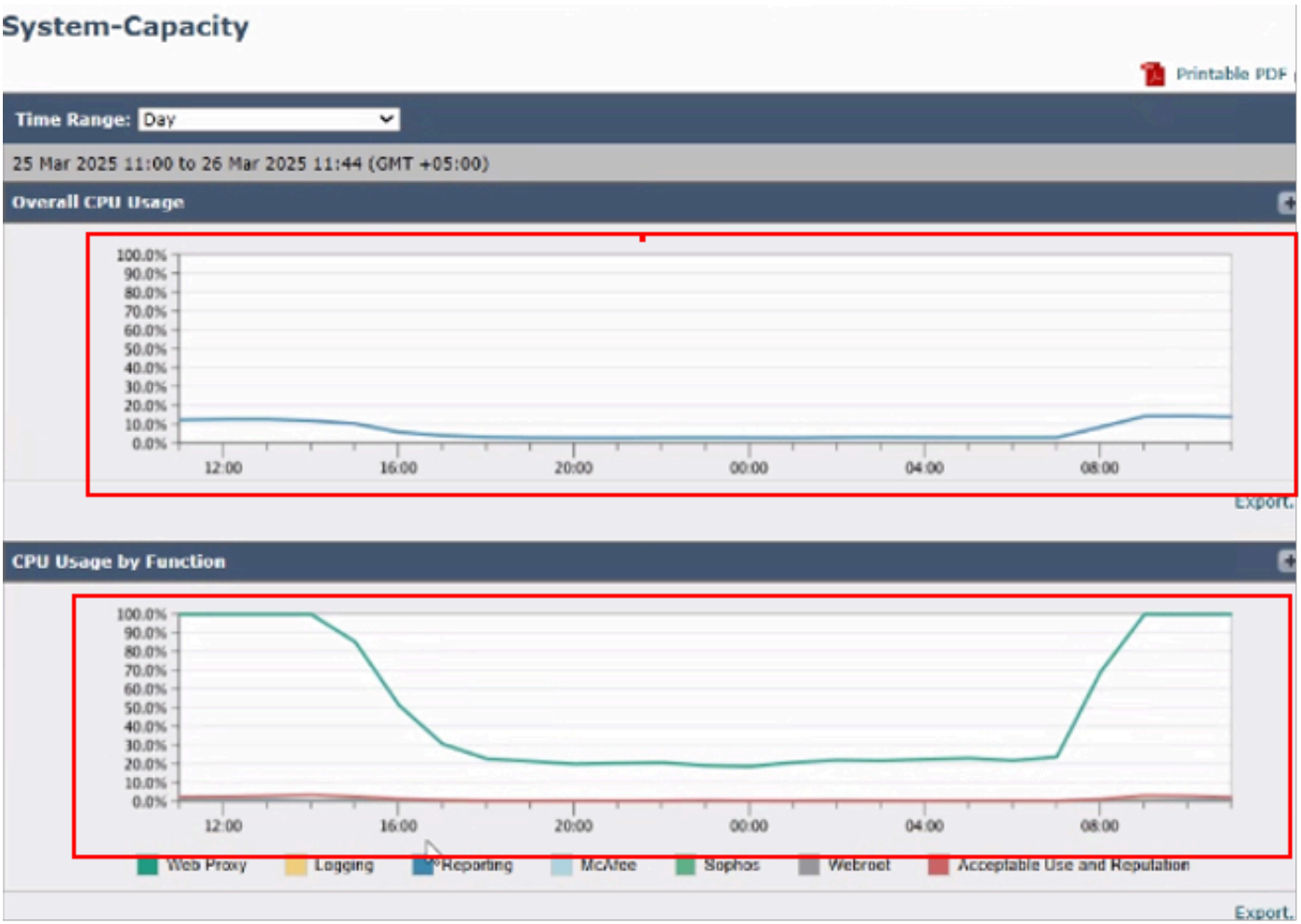
4. 초당 거래 건수 SWA에서 초당 처리하는 트랜잭션 수를 표시합니다.

5. 접속발신 설정 중인 아웃바운드 연결 수를 모니터링합니다.

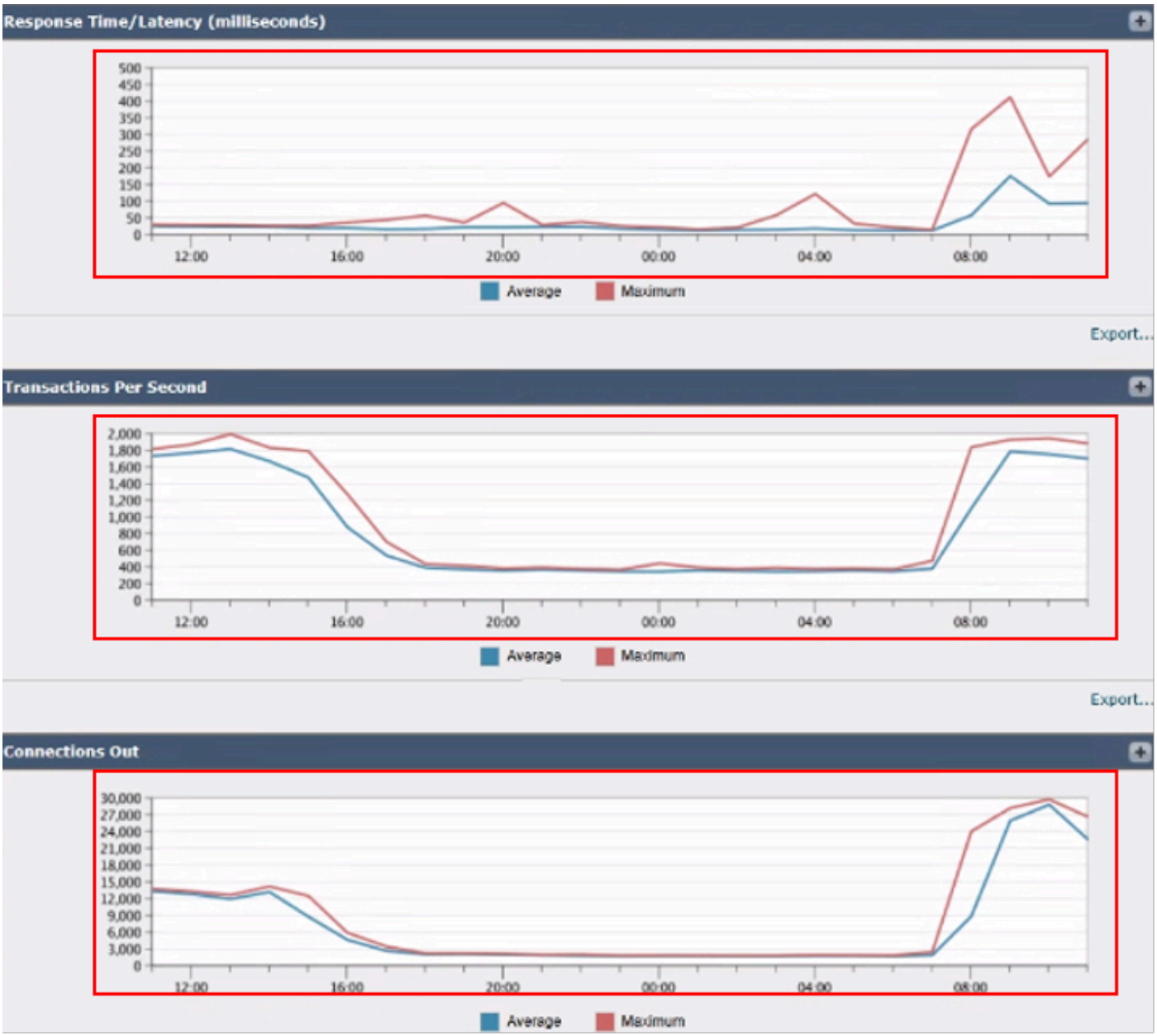
6. 대역폭 Out(바이트) 사용 중인 아웃바운드 대역폭의 양을 측정합니다.

7. 프록시 버퍼 메모리(%): 프록시 프로세스에서 사용하는 메모리의 백분율을 표시합니다.

이 대시보드에서 높은 리소스 사용량의 징후가 있는지 메트릭을 확인합니다.


System-Capacity
Printable PDF
Time Range: Day
25 Mar 2025 11:00 to 26 Mar 2025 11:44 (GMT +05:00)
Overall CPU Usage
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0.0%
12:00
16:00
20:00
00:00
04:00
08:00
Export...
CPU Usage by Function
Web Proxy
Logging
Reporting
McAfee
Sophos
Webroot
Acceptable Use and Reputation
Export...

이미지 - 시스템 용량



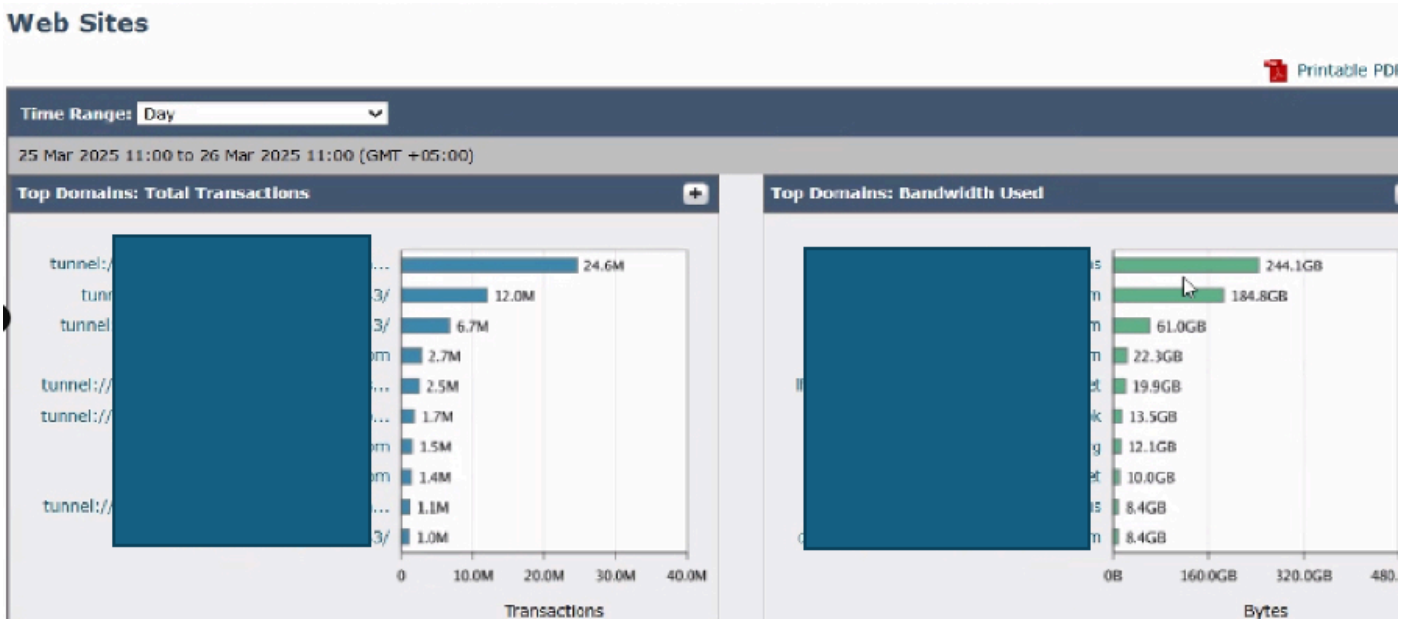
이미지 - 초당 SWA 트랜잭션 및 연결 출력

이미지 - SWA 메모리 사용량

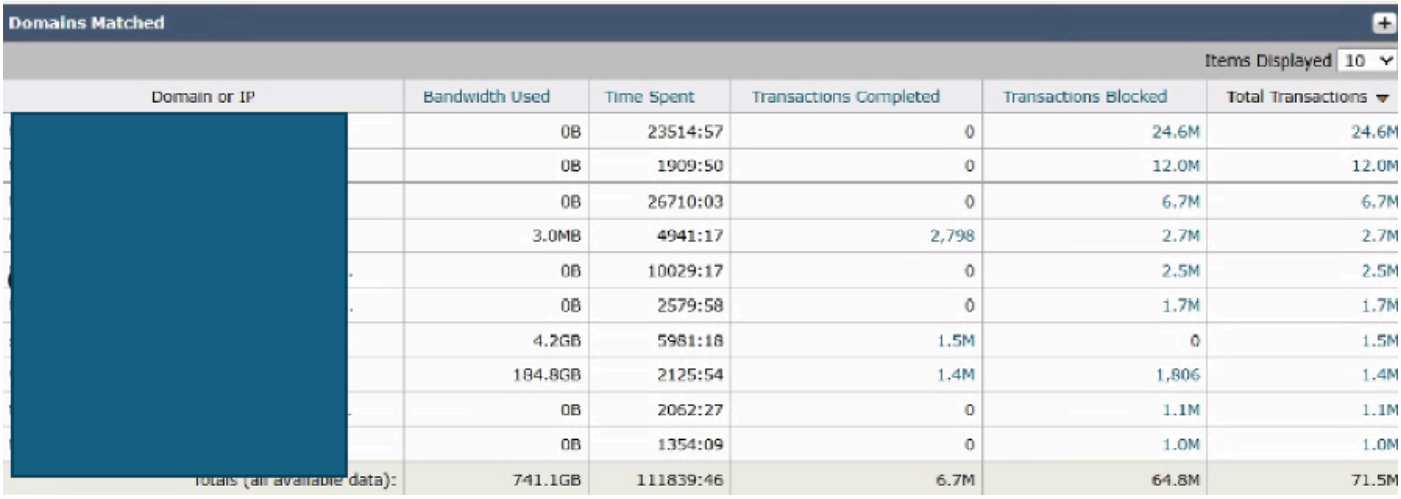
상위 대상 분석

상위 대상을 분석하려면 SWA GUI로 이동하고 Reporting(보고)으로 이동한 다음 Websites(웹 사이트)를 선택합니다. 상위 HTTP/HTTPS 웹 사이트 목록을 검토하고 트래픽이 많거나 자주 액세스하는 도메인을 식별합니다.

검색 결과에 따라 Microsoft Updates, Adobe, Office365 및 온라인 회의 플랫폼과 같은 일반 URL을 무시하거나 제외하는 것이 좋습니다. 이러한 접근 방식은 SWA의 트래픽을 줄여 지연 시간을 줄이고 프록시 처리 로드를 줄이는 데 도움이 됩니다.



이미지 - SWA 상위 웹 사이트 대시보드



Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted]	0B	23514:57	0	24.6M	24.6M
	0B	1909:50	0	12.0M	12.0M
	0B	26710:03	0	6.7M	6.7M
	3.0MB	4941:17	2,798	2.7M	2.7M
	0B	10029:17	0	2.5M	2.5M
	0B	2579:58	0	1.7M	1.7M
	4.2GB	5981:18	1.5M	0	1.5M
	184.8GB	2125:54	1.4M	1,806	1.4M
	0B	2062:27	0	1.1M	1.1M
	0B	1354:09	0	1.0M	1.0M
Totals (all available data):	741.1GB	111839:46	6.7M	64.8M	71.5M

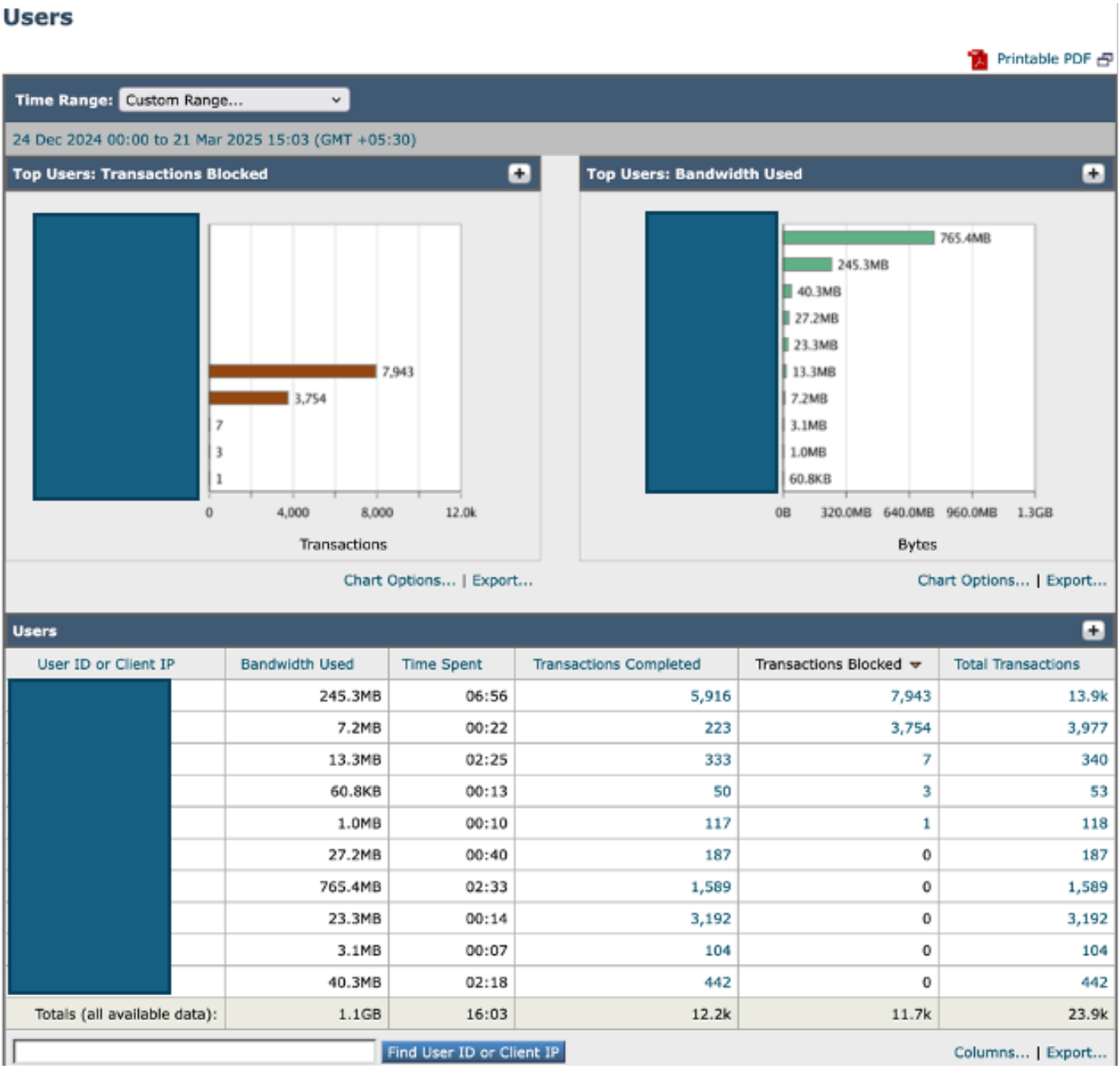
이미지 - SWA 상위 도메인 대시보드

상위 사용자 분석

과도한 트래픽의 잠재적 소스를 식별하려면 Reporting(보고)에서 SWA GUI(SWA GUI)로 이동하여 Users(사용자)를 선택합니다.

목록을 검토하여 어떤 사용자가 SWA에 가장 많은 트랜잭션을 생성하는지 확인합니다. 또한 SWA에 대해 가장 많은 트랜잭션을 생성하고 최대 대역폭을 소비하는 사용자 머신을 확인합니다.

이 분석을 통해 상당한 트래픽 부하를 담당하는 사용자 또는 디바이스를 정확하게 찾아내 표적 작업을 통해 전반적인 시스템 부담을 줄일 수 있습니다.



이미지-SWA 상위 사용자 대시보드

SHD 로그

SHD_log를 검토하여 사용자의 SWA(CliConn) 세션 수, SWA의 인터넷 세션 수(SrvConn), 초당 평균 요청 수(Req) 등의 일부 성능 메트릭을 분석할 수 있습니다.

SHD 로그에 대한 자세한 내용은 Troubleshoot Secure [Web Appliance Performance with SHD Logs(SHD 로그로 Secure Web Appliance 성능 문제 해결)](),

SHD 로그에서 검토할 몇 가지 주요 매개변수는 다음과 같습니다.

- 클라이언트 Conn: 활성 클라이언트 연결 수
- 서버콘: 활성 서버 연결 수

- ProxLd: 평균 프록시 프로세스 로드
- CPULD: 평균 전체 CPU 로드
- RAMUTIL: RAM 사용률
- 레이턴시: 평균 서비스 시간(1분)
- DiskUtil: 디스크 사용량 및 I/O 성능

이 예와 같이 초당 요청 수가 약 1,600개이므로 프록시 프로세스 로드가 높습니다.

```
Wed Mar 26 11:09:30 2025 Info: Status: CPULd 16.3 DskUtil 19.9 RAMUtil 9.3 Reqs 1661 Band 152966 Latenc
Wed Mar 26 11:10:31 2025 Info: Status: CPULd 13.6 DskUtil 19.9 RAMUtil 9.5 Reqs 1699 Band 107048 Latenc
Wed Mar 26 11:11:31 2025 Info: Status: CPULd 15.0 DskUtil 19.9 RAMUtil 9.5 Reqs 1669 Band 178803 Latenc
Wed Mar 26 11:12:31 2025 Info: Status: CPULd 17.6 DskUtil 19.9 RAMUtil 9.2 Reqs 1785 Band 143721 Latenc
```

액세스 로그를 사용하여 레이턴시 문제 해결

SWA를 통해 프록시되는 트래픽에 대해 레이턴시 문제가 발생할 경우, 액세스 로그는 가능한 근본 원인을 파악하는 데 유용한 툴이 될 수 있습니다. 문제 해결 노력을 개선하기 위해 기존 액세스 로그 설정을 수정하거나 새 액세스 로그를 만들 수 있습니다. Custom Field(맞춤형 필드)에 Performance Parameters(성능 매개변수)를 포함하면 레이턴시에 기여하는 요인에 대한 심층적인 통찰력을 얻을 수 있으므로, 더욱 효과적인 분석 및 해결이 가능합니다.

성능 매개변수 및 컨피그레이션 단계에 대한 자세한 내용은 액세스 로그에서 성능 매개변수 구성 링크를 참조하십시오

SWA에서 로그를 수집하는 자세한 지침은 다음과 같습니다. Secure Web Appliance 로그 액세스

클라이언트와 SWA 사이, SWA 내부 프로세스 사이 또는 SWA와 웹 서버 사이에 지연이 발생하는지 여부를 판별하는 데 도움이 되는 주요 매개변수를 검사하여 레이턴시 소스를 분석할 수 있습니다. 고려해야 할 중요한 지표로는 DNS 확인, 인증 시간, 서버 또는 클라이언트 응답 시간 등의 네트워크 기반 서비스가 있습니다. 또한 AMP, Sophos, AVC와 같은 스캔 엔진으로 인해 발생하는 지연은 전체 레이턴시에 미치는 영향을 파악하기 위해 평가되어야 합니다.

```
1750344193.093  272  10.10.20.30  TCP_MISS_SSL/200  39  CONNECT  tunnel://cisco.com:443/  "cisco\user@cisco.com"
DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-Authentication_Profile-DefaultGroup-NONE-NONE-DefaultGroup-
NONE<"C_Cis",6.3,1,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","IW_Com",-,"-","Computer","-","Unknown","Unknown","-","-
",0.06,0,-,"-","-",-,"-",-,-,"-","-",-,-,"-",-,-> - - [ Request Details: ID = 169121930, User Agent = "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36", AD Group Memberships = ( NTLMSSP )
"Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request Header = 0, Request to Server = 0, 1st byte to client = 3
Response Header = 0, Client Body = 9 ] [ Rx Wait Times (in ms): 1st request byte = 0, Request Header = 0,Client Body = 0,1st response
byte = 0,Response header = 0 Server response = 13, Disk Cache = 0; Auth response = 0, Auth total = 3; DNS response = 0, DNS total = 0
WBRS response = 0, WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0 McAfee
total = 0, Sophos response = 0, Sophos total = 0, Webroot response = 0, Webroot total = 0,Anti-Spyware response=0 , Anti-Spyware total
= 0; AMP response = 0, AMP total = 0; Latency = 143; "19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP = 10.20.30.40,
Server Port = 443]
```

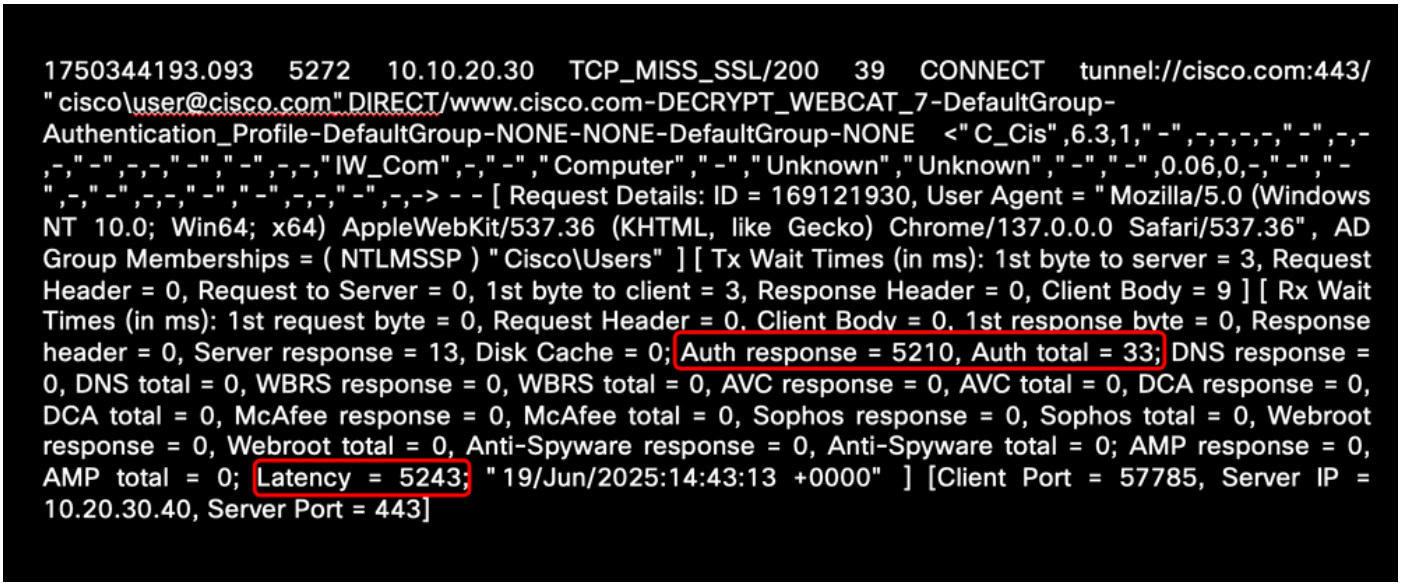
이미지 - AccessLog의 성능 매개변수

높은 인증 시간

인증 응답 시간이 길면 TAC에서 인증 지연 시간을 보다 빠르고 효율적으로 트러블슈팅하는 데 이 정보가 필요합니다.

- 현재 SWA 컨피그레이션
- 디버그 또는 추적 모드에서 인증 로그
- 패킷 캡처 위치
    - 클라이언트 시스템.
    - SWA(영역 설정에 구성된 모든 활성 디렉토리에 대한 클라이언트 트래픽 및 SWA 트래픽을 캡처하는 필터 포함)
- 액세스 로그에 인증 메커니즘 및 그룹을 식별하기 위한 사용자 지정 필드 %m 및 %g이(가) 모두 있는지 확인하십시오
- 문제를 재현하는 동안 클라이언트의 HAR 파일
- CLI의 testauthconfig 명령 출력

다음 예에서는 인증과 관련된 높은 레이턴시 시간을 보여줍니다.



이미지 - 높은 인증 지연 시간 샘플

높은 DNS 시간

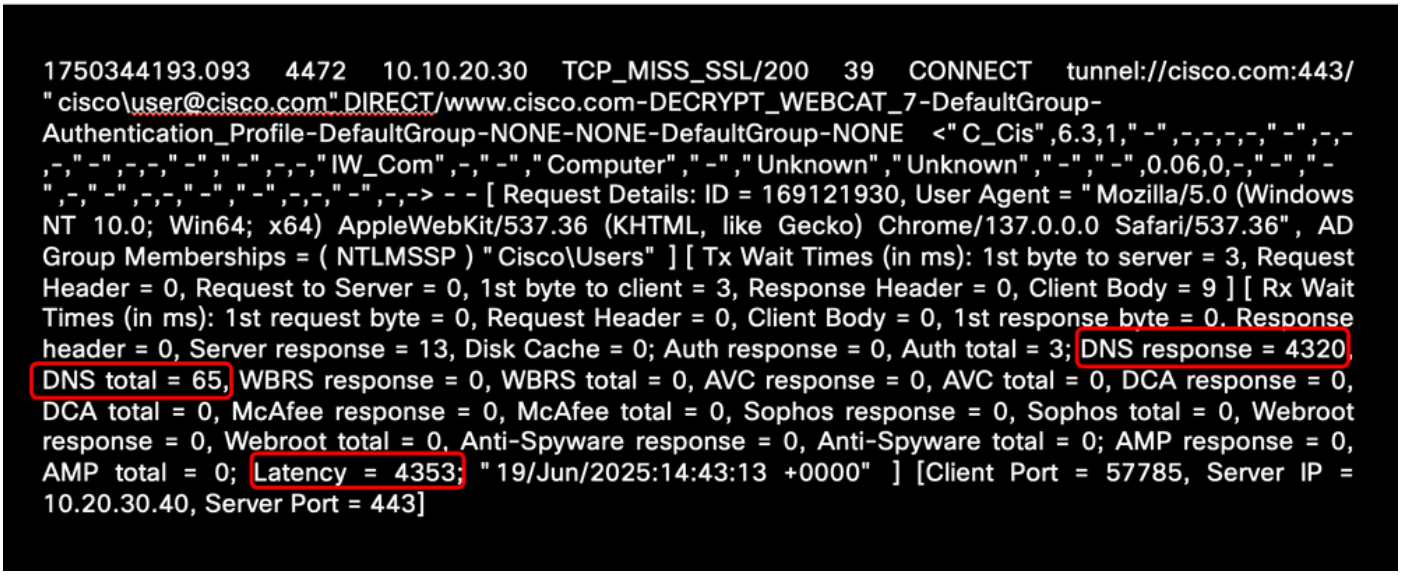
DNS 응답 시간이 길면 TAC에서 DNS 레이턴시 문제를 해결하는 데 이 정보가 필요합니다.

- 현재 SWA 컨피그레이션

- 추적 모드에서 시스템 로그
- DNS 서버 IP 주소
- 패킷 캡처 위치
    - 클라이언트 시스템
    - SWA(DNS 서버 IP 주소로 필터링)
- 사용자 지정 필드에 액세스 로그에 %:<d 및 %:>d가 모두 있는지 확인하십시오
- 문제를 재현하는 동안 클라이언트의 HAR 파일

DNS 컨피그레이션 및 트러블슈팅에 대한 자세한 내용은 Troubleshoot Secure Web Appliance DNS Service 링크를 참조하십시오

다음 예에서는 DNS 이름 확인과 관련된 높은 레이턴시 시간을 보여줍니다.



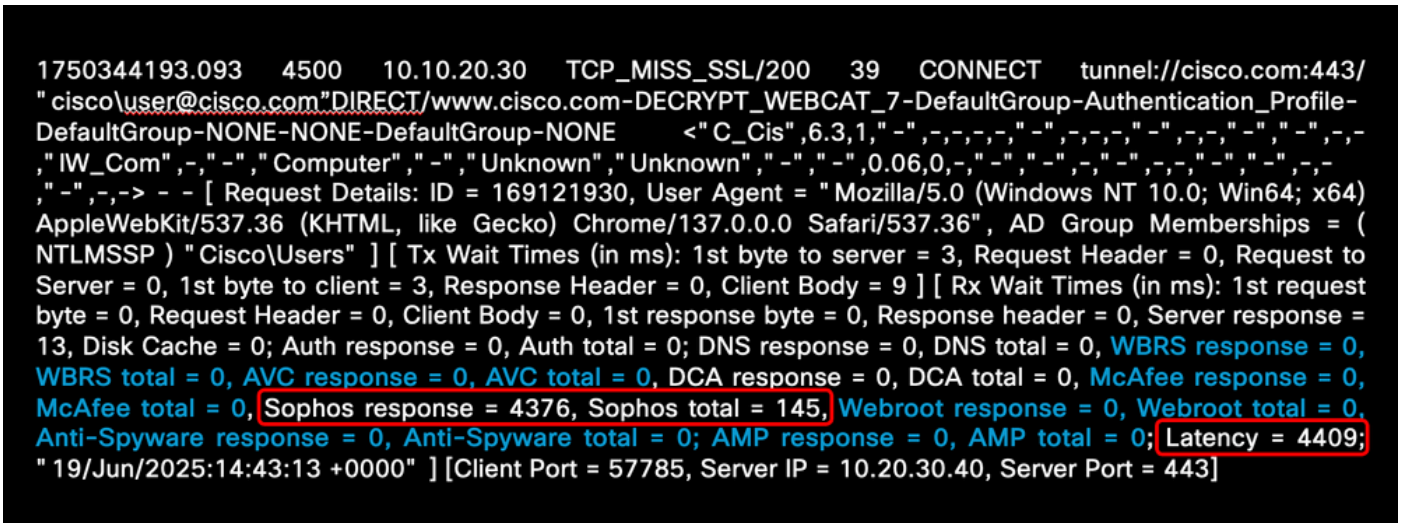
이미지 - 높은 DNS 확인 대기 시간의 샘플

높은 검사 엔진 시간

WBRS(Web Reputation Score), AVC(Application and Visibility Control), 악성코드 스캐닝 엔진에 대한 응답 시간이 긴 경우, TAC에서 스캐닝 엔진의 높은 응답 시간을 트러블슈팅하는 데 이 정보가 필요합니다.

- 현재 SWA 컨피그레이션.
- 응답 시간이 높은 엔진에 따라 로깅 레벨을 debug로 변경합니다.

다음 예에서는 Sophos 엔진과 관련된 높은 대기 시간을 보여 줍니다.



이미지 - 악성코드 스캐닝 엔진 높은 레이턴시

스캐닝 엔진이 높은 응답을 보이는 경우 즉시 복구하려면 다음 단계를 사용하여 CLI에서 스캐닝 서비스를 다시 시작할 수 있습니다.

1단계. diagnostic을 입력하고 Enter를 누릅니다. 이 명령은 숨겨진 명령이며 정확한 명령을 입력해야 합니다.

2단계. 서비스를 선택합니다.

3단계. WBRS 서비스를 다시 시작하려면 WBRS를 선택하거나 6단계로 건너뜁니다.

4단계. 재시작을 선택합니다.

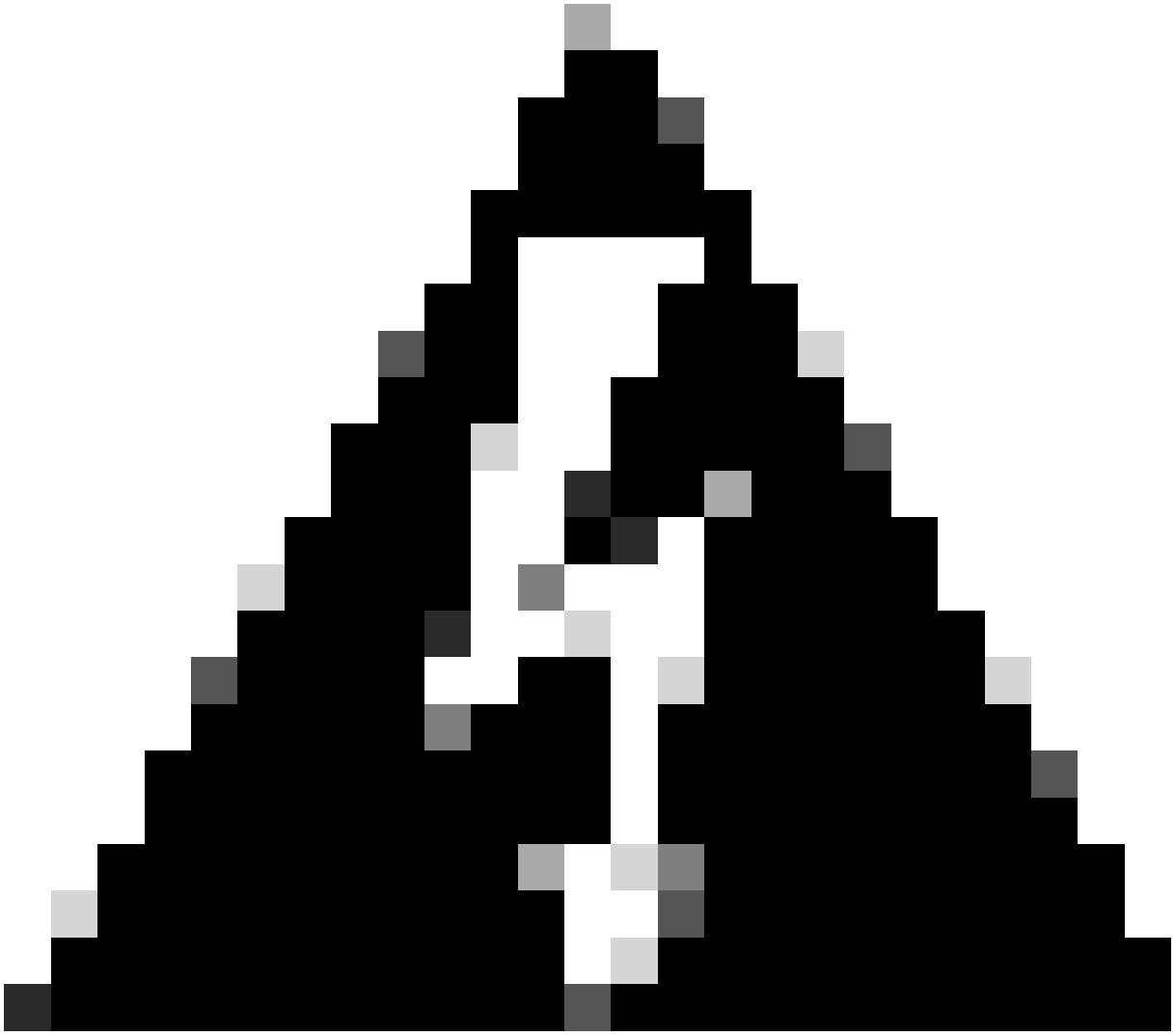
5단계. 마법사를 종료하려면 Enter 키를 계속 누릅니다.

6단계. 악성코드 스캐닝 엔진을 다시 시작할 계획인 경우 ANTIVIRUS를 선택합니다.

7단계. 스캐너를 선택합니다.

8단계. 재시작을 선택합니다.

9단계. 마법사를 종료하려면 Enter 키를 계속 누릅니다.



경고: 내부 서비스를 다시 시작하면 서비스가 중단됩니다. 비생산 시간 또는 주의로 이 작업을 수행하는 것이 좋습니다.

패킷 캡처 연결 시 모범 사례

패킷 캡처를 수행하는 동안 이 정보를 수집하여 Cisco TAC에 공유하십시오.

- 클라이언트 IP 주소입니다.
- 액세스하려는 URL.
- 클라이언트 PC 및 SWA에서 해당 URL에 대해 확인된 IP 주소입니다.
- 사용자 환경(예: 페이지가 로드되지 않았거나 부분적으로 로드되었으며 오류 메시지가 있는 경우 스크린샷을 찍어주십시오.)
- 테스트의 타임스탬프.
- 클라이언트 컴퓨터에서 다른 모든 브라우저 및 앱을 닫습니다. 웹 사이트에 액세스하여 한 번의 성공/실패 시도를 위해 메모장에서 로그를 캡처하고 Cisco Support에 공유합니다.

SWA에서 패킷 캡처를 수행하는 방법에 대한 자세한 내용은 Content Security Appliance에서 패킷

캡처 구성 링크를 참조하십시오

컨피그레이션 복잡성

레이턴시가 높고 성능이 떨어지는 또 다른 일반적인 원인은 컨피그레이션 복잡성입니다. 이는 SWA가 과도한 수의 조건, 프로파일 및 정책으로 구성된 경우 발생합니다. 이러한 복잡성은 응답 시간을 크게 증가시키고 프록시 프로세스에 큰 부담을 줄 수 있습니다. 이 문제는 트래픽이 가장 많은 피크 시간대에 더욱 두드러지는 경향이 있습니다.

다음은 구성을 최적화하는 몇 가지 팁입니다.

1. HTTPS 암호 해독 제한: 보안 정책에 필수적인 트래픽만 해독합니다. 가능하면 보안을 유지하면서 처리 오버헤드를 줄이십시오.
2. 효율성을 위해 정책의 우선 순위 지정: 정책 목록의 맨 위에 가장 자주 사용되는 정책을 정렬합니다. 이렇게 하면 가장 까다로운 트래픽을 먼저 해결하여 처리 속도를 높일 수 있습니다.
3. 효율적인 정책 설계: 최대한 수를 최소화하여 정책을 간소화합니다. 따라서 불필요한 처리가 줄어들고 전반적인 시스템 성능이 향상됩니다.
4. Optimize Anti-Malware and Anti-Virus Scanning(안티멀웨어 및 안티바이러스 검사 최적화): 안티멀웨어 및 안티바이러스 프로세스에 대한 검사 구성을 검토합니다. CPU를 많이 사용할 수 있으므로 이를 세부적으로 조정하면 보안에 영향을 주지 않고 리소스 소비를 크게 줄일 수 있습니다.
5. 경량 정규식 사용: 복잡한 정규식이나 리소스 사용량이 많은 정규식은 사용하지 마십시오. 점(.) 및 별표(*)와 같은 문자를 적절하게 이스케이프하여 처리 부담을 줄이고 비효율성을 방지합니다.

SWA 모범 사례에 대한 자세한 내용은 Use Secure Web Appliance 모범 사례를 참조하십시오

CLI 명령

버전

version 명령을 사용하여 하드웨어 할당(가상 SWA의 경우) 및 RAID 상태(물리적 SWA의 경우)를 확인합니다. 하드웨어 구성을 확인합니다. CPU 코어 수, 메모리 및 하드 디스크가 예상대로 할당되었는지 확인합니다. 가상 모델에서 RAID 상태가 알 수 없음으로 표시되고 물리적 어플라이언스에서 RAID 상태가 저하됨 또는 실패인 경우 Cisco TAC에 문의하여 백 엔드에서 디스크 상태를 검토하십시오.

다음은 SWA에 더 많은 CPU를 할당하여 오동작을 일으킬 수 있는 샘플입니다.

```
SWA Lab> version
Current Version
===============
Product: Cisco S100V Secure Web Appliance
Model: S100V
BIOS: 6.00
CPUs: 3 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
```

```
Hard disk: 200 GB, or 250 GB expected; 200 GB allocated
RAID: NA
RAID Status: Optimal
```

경고 표시

근본 원인을 나타낼 수 있는 SWA 네트워크 관련 알림 메시지를 확인하려면 displayalerts 명령을 사용합니다.

이 예에서는 IP 주소 10.10.10.10의 DNS 서버가 응답하지 않았으며 "The File Reputation service is not reachable" 메시지가 네트워크 연결 문제를 나타낼 수 있습니다.

```
SWA LAB> displayalerts
Date and Time Stamp           Description
--------------------------------------------------------------------------------
26 Mar 2025 11:20:07 +0500 The File Reputation service is not reachable.
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 10:16:18 +0500 Warning: Communication with the File Reputation service has been established
```

프로세스 상태

SWA 내부 서비스의 프로세스 및 메모리 사용량을 보려면 process_status 명령을 사용합니다.

트래픽 프록시를 처리하는 기본 프로세스인 Prox 프로세스가 몇 분 동안 지속적으로 100% 사용량을 초과하면 프로세스에 지속적으로 높은 로드가 발생함을 나타냅니다. 그러나 Prox 또는 기타 프로세스에서 CPU 사용량이 일시적으로 급증하는 것은 정상이며 예상된 현상입니다.

<#root>

```
SWA LAB> process_status
USER     PID
```

%CPU

%MEM

```
   VSZ     RSS TT  STAT STARTED           TIME
```

COMMAND

```
root      11 2805.4  0.0       0     512  -  RNL  28Jun24 11863204:12.63 idle
root   71189
```

102.0

19.5

```
 6670700 6478032  -  R    23Feb25    18076:32.80
```

prox

```
root   91880   99.0  0.6  369564  214832  -  R    28Jun24    58854:51.78 counterd
root   91267   76.0  0.9  379804  292324  -  R    28Jun24    59371:01.26 counterd
root      12   25.9  0.0       0    1600  -  WL   28Jun24    30899:57.88 intr
root   46955   25.0  0.2   91260   59336  -  S    23Jan25     7547:02.96 wbnpd
root   95056   23.0 11.2 5369332 3710348  -  I    28Jun24    31719:23.99 java
root   93190   12.0  1.4 3118384  456088  -  S    01:15         29:57.05 beakerd
root   64579   11.0  0.2  101336   71204  -  S     6Aug24    12074:55.55 coeuslogd
```

상태 세부사항

status detail 명령은 시스템 리소스 사용량, 네트워크 트래픽 메트릭 및 연결 통계에 대한 실시간 요약을 제공하며, 이는 SWA의 전반적인 상태 및 성능을 반영합니다. 빠른 모니터링과 문제 해결을 위해 GUI의 System Status(시스템 상태) 보기를 미러링합니다.

<#root>

```
SWA LAB> Status detail

Status as of:                  Wed Mar 26 11:51:27 2025 PKT


Up since:                      Fri Jun 28 13:45:43 2024 PKT (270d 22h 5m 43s)


System Resource Utilization:

CPU                                    16.0%


  RAM                                  10.3%


  Reporting/Logging Disk               19.8%


Transactions per Second:
  Average in last minute                1745
  Maximum in last hour                  2210
  Average in last hour                  1708
  Maximum since proxy restart           2451
  Average since proxy restart            615
Bandwidth (Mbps):
  Average in last minute             149.699
  Maximum in last hour              1356.387
  Average in last hour               229.634
  Maximum since proxy restart      22075.244
  Average since proxy restart         60.689
Response Time (ms):
  Average in last minute                 99
  Maximum in last hour              8194128
  Average in last hour                   87
```

```
  Maximum since proxy restart         19608632
  Average since proxy restart               28
Cache Hit Rate:
  Average in last minute                     3
  Maximum in last hour                       6
  Average in last hour                       2
  Maximum since proxy restart               89
  Average since proxy restart                2
Connections:
  Idle client connections                 3481
  Idle server connections                  754


Total client connections                21866


  Total server connections               19049


SSLJobs:
  In queue Avg in last minute                0
  Average in last minute                 12050
  SSLInfo Average in last min                0
Network Events:
  Average in last minute                  16.0
  Maximum in last minute                   171
  Network events in last min            151918
```

Ipcheck

ipcheck 명령은 하드웨어 사양, 디스크 사용량, 네트워크 인터페이스, 설치된 소프트웨어 키, 버전 세부 정보 등 Secure Web Appliance에 대한 자세한 시스템 정보를 표시하여 어플라이언스의 현재 상태에 대한 포괄적인 스냅샷을 제공합니다.

<#root>

```
SWA LAB > ipcheck
  Ipcheck Rev           1
  Date                  Fri Mar 21 16:34:56 2025
  Model                 S100V
  Platform              vmware (VMware Virtual Platform)
  Secure Web Appliance Version  Version: 15.2.1-011
  Build Date            2024-10-03
  Install Date          2025-02-13 17:49:24
  Burn-in Date          Unknown
  BIOS Version          6.00
  RAID Version          NA
  RAID Status           Unknown
  RAID Type             NA
  RAID Chunk            Unknown
  BMC Version           NA
  Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            200GB

  Root                  4GB 64%
```

Nextroot	**4GB 65%**
Var	**400MB 38%**
Log	**130GB 24%**
DB	**2GB 0%**
Swap	8GB
Proxy Cache	50GB
RAM Total	8192M

속도

rate 명령은 10초마다 연결 속도 및 초당 요청 수를 인쇄합니다.

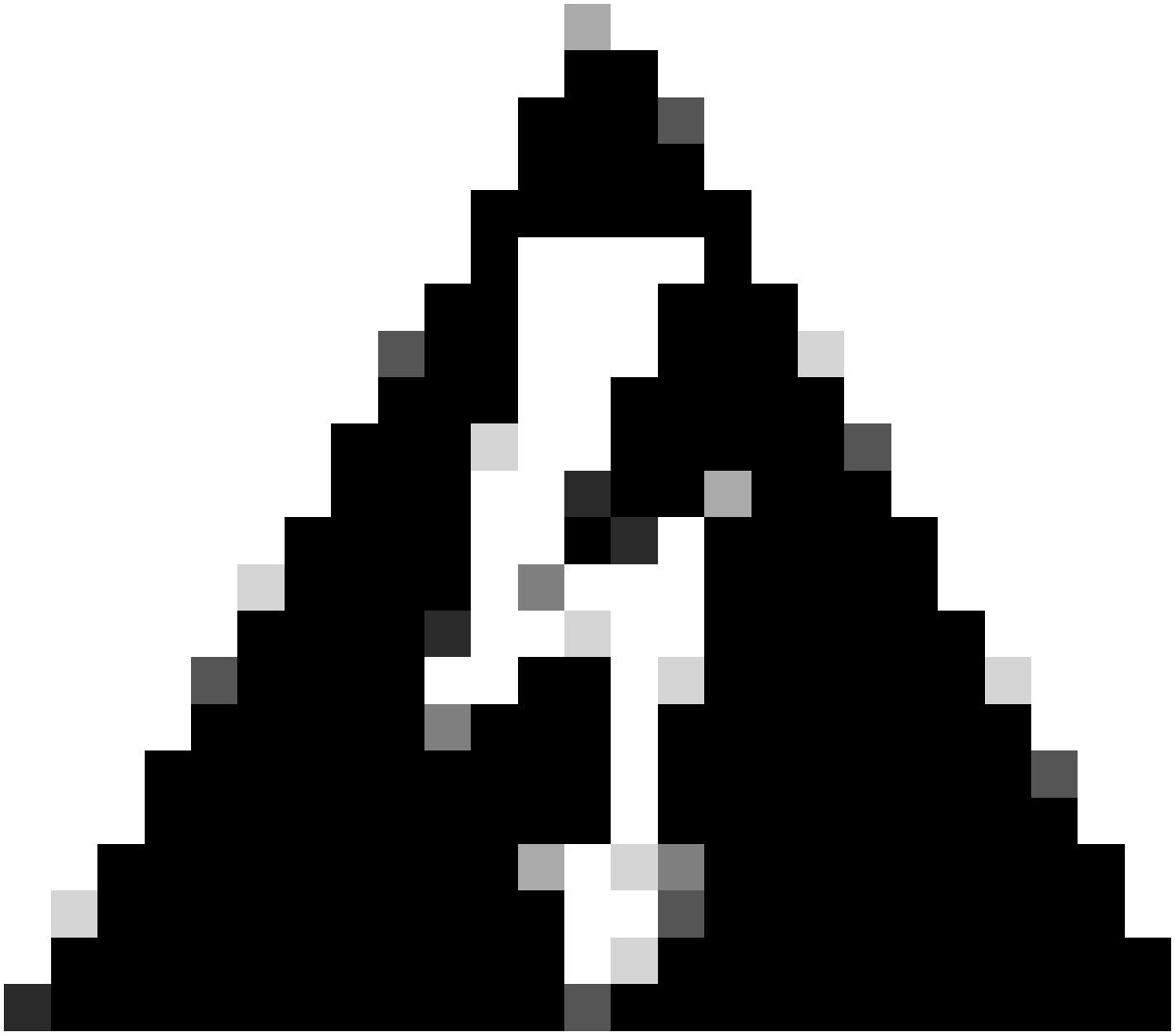
<#root>

```
SWA LAB> rate
Press Ctrl-C to stop.
```

%proxy	reqs				client	server	%bw	disk	disk
CPU	/sec	hits	blocks	misses	kb/sec	kb/sec	saved	wrs	rds
100.00	1800	17	16352	1626	178551	178551	0.0	2366	0
100.00	1813	18	16453	1659	226301	224952	0.6	3008	0
99.00	1799	10	16338	1645	206234	206234	0.0	3430	1

높은 레이턴시를 위한 로그 수집

액세스 로그에서 높은 응답 시간 또는 SHD 로그에서 높은 프로세스 로드가 표시되는 섹션에 따라 추가 트러블슈팅을 위해 해당 로그 서브스크립션을 Debug로 변경하는 것이 가장 좋습니다.



경고: 로그 레벨을 디버그 또는 추적으로 설정하면 리소스 사용량이 증가하고 로그 파일이 빠르게 회전하거나 덮어쓰게 될 수 있습니다.

액세스 로그 필드	SHD 로그 필드	해당 로그 서브스크립션
인증 응답, 인증 합계	—	인증 로그
DNS 응답, DNS 합계	—	시스템 로그
WBRS 응답, WBRS 합계	Wbrs_WucLd	Cisco TAC에 문의
AVC 응답, AVC 합계	—	avc_로그

McAfee 응답, McAfee 합계	McafeeLd	mcafee_logs
Sophos 응답, Sophos 합계	SophosLd	sophos_logs
Webroot 응답, Webroot 합계	WebrootLd	웹루트로그
AMP 응답, AMP 합계	AMPLd	amp_logs

관련 정보

SHD 로그로 Secure Web Appliance 성능 문제 해결

Secure Web Appliance 로그 액세스

Content Security Appliance에서 패킷 캡처 구성

Secure Web Appliance 모범 사례 사용

액세스 로그의 성능 매개변수 구성

SWA의 비정상적인 프로세스 상태 트러블슈팅

SWA에서 암호 해독 속도 확인

Secure Web Appliance DNS 서비스 문제 해결

Secure Web Appliance 로그 액세스

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.