Secure Web Appliance 액세스 로그 이해

목차

소개

이 문서에서는 SWA(Secure Web Appliance) 액세스 로그의 구조에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 CLI(Command Line Interface)에 액세스합니다.

- SWA에 대한 관리 액세스.
- SWA 워크플로에 대한 기본 이해

사용되는 구성 요소

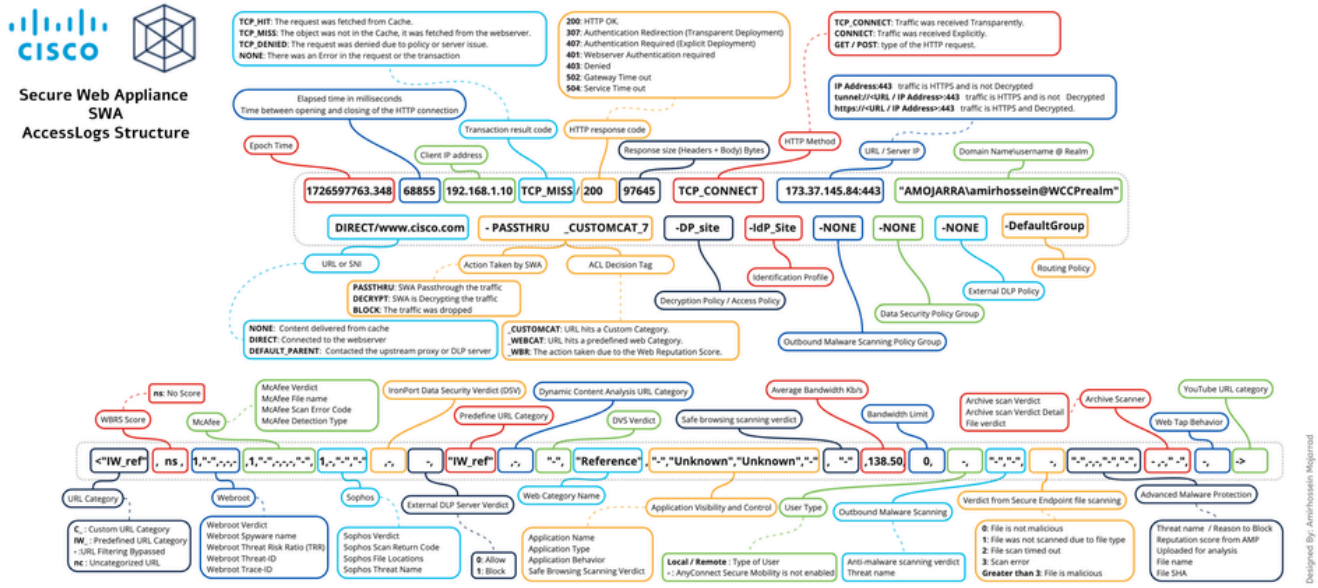
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

액세스 로그 구조

이 문서에서는 Accesslog 구조에 대해 다음 샘플을 통해 설명합니다.

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```



이미지 - 액세스 로그 구조

참고: 액세스 로그의 구조는 SWA의 버전에 따라 달라집니다. 각 Accesslog 파일의 시작 부분에는 해당 구조와 형식 지정자의 순서를 보여 주는 줄이 있습니다.

섹션	액세스 로그의 샘플	형식 지정자	세부사항
에포크 타임	1726597763.348	%t	에포크 시간(Unix 시간 또는 POSIX 시 1월 1일(UTC 00:00:00) 이후 경과된 총 크로초)를 계산하여 시간을 추적하기 위 트랜잭션이 완료된 에포크 시간입니다. 온라인 Epoch 시간 변환기 또는 모든 li 여 이 값을 변환할 수 있습니다.

경과 시간	68855	%e	요청이 완료/중단되고 연결이 닫히기 전 니다.
소스 IP 주소	192.168.1.10	%a	클라이언트/소스 IP 주소입니다.
트랜잭션 결과 코드	TCP_MISS	%w	Transaction Result Code(트랜잭션 결과 언트 요청을 확인하는 방법을 나타냅니 다음은 트랜잭션 결과 코드의 목록입니

TCP_HIT
TCP_IMS_HIT
TCP_MEM_HIT
TCP_MISS
TCP_REFRESH_HIT

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS</td></tr>
<tr><td>TCP_거부됨</td></tr>
<tr><td>TCP_DENIED_SSL HTTPS</td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS_SSL</td></tr>
<tr><td>TCP_MISS_SSL HTTPS</td></tr>
</table>
</td></tr>
<tr><td>HTTP 응답 코드</td><td>/200</td><td>%h</td><td>HTTP 응답 코드는 클라이언트 HTTP 요
서버에서 반환한 상태 코드를 나타냅니

다음은 가장 중요한 HTTP 응답 코드 목
이 문서의 HTTP 응답 코드 섹션을 참조
<table>
<tr><td>상태 코드</td><td>의미</td></tr>
<tr><td>000</td><td>000은 데이터 전송 중 TLS 단
통신 중단이 발생한 경우 비표</td></tr>
<tr><td>2xx 성공</td><td></td></tr>
</table>
</td></tr>
</table>

			200	확인
			204	콘텐츠 없음
			206	부분 콘텐츠(범위 요청이라고
			3xx 리디렉션	
			301	영구 리디렉션.
			302	임시 리디렉션
			304	수정되지 않음
			307	인증을 위한 임시 리디렉션 (일반적으로 SWA가 사용자를 포에서 표시됨)
			4xx 클라이언트 오류	
			400	잘못된 요청
			401	웹 서버 인증 필요(일반적으로 하는 동안 투명 배포에 표시됨
			403	금지됨
			404	찾을 수 없음
			407	명시적 프록시 인증 필요
			5xx 서버 오류	
			500	내부 서버 오류
			502	잘못된 게이트웨이
			503	서비스를 사용할 수 없음
			504	게이트웨이 시간 초과
전송된 총 크기	97645	%s	요청에 대해 전송된 총 바이트 수입니다	

<table>
<tr><td>HTTP 메서드</td><td>TCP_CONNECT</td><td>%1r</td><td>HTTP 메서드는 클라이언트가 GET을 사
하거나 POST를 사용하여 데이터를 제
가 리소스에 대해 수행할 작업을 지정하
<table><tr><td>가져오기</td><td>HTTP GET 메
를 요청하는 데
만을 위해 설계
포함해서는 안
GET은 다운로</td></tr><tr><td>POST</td><td>HTTP POST 메
본문에 포함된
데 사용됩니다
하거나, 파일을
태를 변경하는
용됩니다.</td></tr><tr><td>연결</td><td>HTTP CONNE
대상 서버에 대
성할 수 있도록
널을 설정하는
록시를 통한 임
기 위해 HTTPS
니다.

트래픽이 SWA
되었음을 나타
프록시를 직접
니다.</td></tr><tr><td>TCP_CONNECT</td><td>WCCP 또는 리
WSA에 의해 트
었음을 나타냅</td></tr></table></td></tr>
<tr><td>대상</td><td>10.37.145.84:443</td><td>%2r</td><td>이 섹션에서는 대상 서버 URL 및 TCP

투명 리디렉션에서 트래픽이 해독되기
주소 및 포트 번호를 표시합니다.

URL이 tunnel:// 으로 시작하는 경우 SW
하지 않았음을 의미합니다.

URL이 https://으로 시작하면 SWA가 트
입니다.</td></tr>
</table>

<table>
<tr><td>사용자 이름 및 인증 영역</td><td>"AMOJARRA\amirhossein@WCCPrealm"</td><td>%A</td><td>이 연결에 사용된 자격 증명입니다.

요청이 인증되면 SWA는 사용자 이름 및
이 기록합니다.

<Domain Name> \ <User Name> @ <A
Name>

요청이 아직 인증되지 않았거나 인증에
이픈 "-"이 표시됩니다.</td></tr>
<tr><td>액세스 유형</td><td>DIRECT/</td><td>%H</td><td>요청 콘텐츠를 검색하기 위해 접속된 서
입니다.

가장 일반적인 값은 다음과 같습니다.

<table><tr><td>없음</td><td>웹 프록시에 콘텐츠
색하기 위해 다른 서
다.</td></tr><tr><td>DIRECT</td><td>웹 프록시가 콘텐츠를
서 명명된 서버로 이</td></tr><tr><td>기본값_상위</td><td>웹 프록시가 콘텐츠를
위 프록시 또는 외부
다.</td></tr></table></td></tr>
<tr><td>서버 주소</td><td>www.cisco.com</td><td>%d</td><td>데이터 소스 또는 서버 IP 주소입니다.</td></tr>
<tr><td>MIME content-type/subtype</td><td>-</td><td>%c</td><td>MIME 문서, 파일 또는 바이트 집합의
다. MIME 유형은 IETF RFC 6838에서

기본 유형의 역할에는 두 가지 기본 MI

• text/plain은 텍스트 파일의 기본값
사람이 읽을 수 있어야 하며 이진
야 합니다.
• application/octet-stream은 다른 모
. 알 수 없는 파일 형식은 이 형식을
우저에서는 이러한 파일을 조작할
및 가능한 위험한 동작으로부터 사
특별히 주의를 기울입니다.</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>MIME 유형의 전체 목록을 가져오려면
문하십시오.</td></tr>
<tr><td>ACL 결정 태그</td><td>PASSTHRU_CUSTOMCAT_7-</td><td>%D</td><td>ACL 결정 태그는 웹 프록시에서 트랜잭
내는 액세스 로그 항목의 필드입니다.
URL 카테고리, 스캐닝 엔진의 정보가

참고: ACL 결정 태그의 끝에는 성
에서 내부적으로 사용하는 동적으
니다. 이 번호는 무시할 수 있습니

다음은 가장 중요한 ACL 결정 태그 목
이 문서의 ACL Decision Tag 섹션을 참
<table><tr><td>ACL 결정 태그</td><td>설명</td></tr><tr><td>허용(_C)</td><td>웹 프
룹에
리 필
션을</td></tr><tr><td>WBRS 허용(_W)</td><td>웹 프
룹의
트랜</td></tr><tr><td rowspan="4">AMP_FILE_VERDICT</td><td>파일
판정</td></tr><tr><td>1 - 알</td></tr><tr><td>2 - 정</td></tr><tr><td>3 - 악</td></tr><tr><td>4 - 검</td></tr><tr><td>차단_관리자</td><td>액세스
설정
되었</td></tr><tr><td>BLOCK_ADMIN_CONNECT</td><td>액세스
HTTP
정의
에 따
습니</td></tr><tr><td>BLOCK_ADMIN_CUSTOM_사용자_에이전트</td><td>액세스
자 지
설정
트에
었습</td></tr><tr><td>블록 관리자 터널링</td><td>웹 프</td></tr></table></td></tr>
</table>

	룹의 I 트래픽 트랜잭
BLOCK_ADMIN_파일_유형	액세스 일 유형 단되었
BLOCK_ADMIN_PROTOCOL	액세스 Proto 토콜에 되었습
차단_AMP_RESP	웹 프 룹의 A Prote 차단했
블록_AVC	액세스 된 애 트랜잭
BLOCK_CONTENT_UNSAFE	액세스 텐츠 분 션이 차 언트 요 한 요청 츠를 차 습니다
차단_사용자 지정	액세스 자 지정 에 따라 습니다
차단(_I)	웹 프 그룹에 템의 구 차단했
차단(_W)	액세스 터 설정 단되었
차단_웹캣	액세스 고리 구 잭션에
차단(_Y)	웹 프 룹에 I YouTu 정에 I 습니다
DECRYPT_ADMIN	웹 프 그룹의 트랜잭

				다.
			DECRYPT_EUN_CUSTOMCAT	웹 프 그룹에 범주 : 잭션의 EUN(이 삭
			DECRYPT_EUN_WBRS	웹 프 그룹의 라 트 습니다 트래픽
			DECRYPT_EUN_WEBCAT	웹 프 그룹의 설정에 를 해 화된 : 다.
			DECRYPT_WEBCAT	웹 프 그룹의 설정에 를 해
			DECRYPT_WBRS	웹 프 그룹의 라 트 습니다
			DROP_ADMIN	웹 프 그룹의 트랜잭
			DROP_WEBCAT	웹 프 그룹의 설정에 했습니
			DROP_WBRS	웹 프 그룹의 라 트
			PASSTHRU_ADMIN	암호 : 본 설정 랜잭션
			PASSTHRU_WEBCAT	암호 : 테고리 프록시 니다.
			PASSTHRU_WBRS	암호 : 필터 : 트랜잭

			기타	권한 기 또 과 같 에서 니다.
정책 이름	DP_site-	해당 없음	트래픽 유형에 따라 다음 항목이 표시됩 • 암호 해독 정책 이름: 트래픽이 H 않은 경우 • 액세스 정책 이름: 트래픽이 HTTI
ID 정책	IdP_사이트-	해당 없음	식별 프로필 이름을 표시합니다.
아웃바운드 악성코드 스캐닝 정책 그룹	NONE-	해당 없음	아웃바운드 악성코드 스캐닝 정책 그룹 정책 그룹 이름의 공백은 밑줄(_)로 바
데이터 보안 정책 그룹	NONE-	해당 없음	Cisco 데이터 보안 정책 그룹 이름입니 Cisco 데이터 보안 정책과 일치하는 경 DefaultGroup입니다. 이 정책 그룹 이름 터가 활성화된 경우에만 나타납니다. 더 지 않은 경우 "NONE"이 나타납니다. 정책 그룹 이름의 공백은 밑줄(_)로 바
외부 DLP 정책 그룹	NONE-	해당 없음	트랜잭션이 전역 외부 DLP 정책과 일치 DefaultGroup입니다. 외부 DLP 정책이 "NONE"이 나타납니다. 정책 그룹 이름의 공백은 밑줄(_)로 바
라우팅 정책 그룹	기본 그룹-	해당 없음	라우팅 정책 그룹 이름을 ProxyGroupName/ProxyServerName으 트랜잭션이 전역 라우팅 정책과 일치하 DefaultRouting입니다. 업스트림 프록시 경우 이 값은 DIRECT입니다 정책 그룹 이름의 공백은 밑줄(_)로 대
웹 트래픽 탭	없음	해당 없	웹 트래픽 탭 정책 이름

<table>
<tr><td></td><td></td><td>음</td><td></td></tr>
<tr><td>URL 범주 약어</td><td><"C_Cisco",</td><td>%XC</td><td>요청이 일치하는 URL 범주입니다.<table><tr><td>-</td><td>우회된 URL 필터링</td></tr><tr><td>nc</td><td>분류되지 않은 URL</td></tr><tr><td>오류</td><td>우회된 URL 필터링</td></tr><tr><td>꼬마 도깨비</td><td>불가능해</td></tr><tr><td>IW_</td><td>카테고리 이름이 IW_로 시
우 요청이 Cisco Predefine
Category(URL 카테고리 미
)에 도달했음을 의미합니다</td></tr><tr><td>C_</td><td>카테고리 이름이 IC_로 시
우 요청이 Custom URL
Category(맞춤형 URL 카테
적중했음을 의미합니다.</td></tr></table></td></tr>
<tr><td>웹 평판 점수</td><td>-,</td><td>%XW</td><td>이 필드는 WBRS(Web Reputation) 점수
ns는 URL에 점수가 없음을 의미합니다</td></tr>
<tr><td>Webroot 스캐닝</td><td>-,"-",-,-,-,</td><td></td><td>이 5개 필드는 Webroot 스캐닝과 관련<table><tr><td>Webroot 판정,</td><td>%Xv</td><td>Webro
악성코
Webro
적용됩
판정에
문서의
Verdic
.</td></tr><tr><td>Webroot</td><td>"%Xn"</td><td>개체의</td></tr></table></td></tr>
</table>

			Spyname,		름입니 응답에
			Webroot TRR,	%Xt	악성코 하는 T 값과 연 니다. V 에만 적
			Webroot 위협 ID,	%X	Webro 용하는 원에서 값을 사 Webro 적용됩
			Webroot TraceID,	%Xi	Webro 용하는 원에서 값을 사 Webro 적용됩
McAfee 스캐닝	-,"-",-,-,-,"-",		이 6개 필드는 McAfee 스캐닝과 관련이		
			맥아피 판정,	%Xd	McAfe 악성코 McAfe 적용됩 판정에 문서의 Verdic .
			McAfee 파일 이름,	"%Xe"	McAfe 입니다 답에만
			McAfee 스캔 오류 코드,	%Xf	McAfe 하는 값

					에서는 을 사용 McAfe 적용됩
			McAfee 탐지 유형, ,	%Xg	McAfe 용하는 원에서 값을 사 McAfe 적용됩
			McAfee 바이러스 유형,	%Xh	McAfe 로 사용 객 지원 때 이 값 McAfe 적용됩
			McAfee 바이러스 이름,	"%Xj"	McAfe 의 이름 지된 응
Sophos 스캐닝	-,-,"-","-",		이 4개의 필드는 Sophos 스캐닝과 관련		
			Sophos 판정,	%XY	Sopho 악성코 Sopho 적용됩 판정에 문서의 Verdic .
			Sophos 스캔 반환 코드,	%Xx	Sopho 사용하 지원어 이 값을 Sopho 적용됩

			Sophos 파일 위치 ,	"%Xy"	Sopho 은 파일 Sopho 적용됩
			Sophos 위협 이름 ,	"%Xz"	Sopho 용하는 원에서 값을 사 Sopho 적용됩
Cisco 데이터 보안 검사 판정	-,	%Xl	Cisco Data Security Policy의 Content(기반으로 하는 Cisco Data Security 스캔 이 목록에서는 이 필드에 사용할 수 있는 0.허용 1.블록 - (하이픈).Cisco 데이터 보안 필터에서 습니다. 이 값은 Cisco Data Security Fi 또는 URL 카테고리 작업이 Allow로 설정		
외부 DLP 검사 판정	-,	%Xp	ICAP 응답에서 제공된 결과를 기반으로 정. 이 목록에서는 이 필드에 사용할 수 있는 0.허용 1.블록 - (하이픈). 외부 DLP 서버에서 검사를 값은 외부 DLP 검사가 비활성화된 경우 Policies(외부 DLP 정책) > Destinations URL 카테고리로 인해 콘텐츠가 검사되 다.		
미리 정의된 URL 범주 판정	"-",	%XQ	요청 측 스캐닝 중에 결정된 약식 사전 URL 필터링이 비활성화되면 이 필드에 . 요청이 Custom URL Category(맞춤형		

			경우에도 Accesslog에서 사전 정의된 U 수 있지만, 결정은 맞춤형 URL 카테고리 . URL 범주 약어 목록은 URL 범주 설명을
URL 범주 판정	-,	%XA	응답 측 스캐닝 중에 DCA(Dynamic Co 정한 약식 URL 카테고리 판정. Cisco Web Usage Controls URL 필터링 nc: 이 값은 DCA(Dynamic Content Ana 설정되고 요청 시 URL 카테고리가 할당 스캐닝 판정에 표시되며, 이는 응답 측 기 전에 초기 요청 단계 중에 URL이 분 니다
Unified Inbound DVS 판정	"-",	%XZ	활성화된 스캐닝 엔진과 상관없이 악성 는 통합된 응답 측 Anti-Malware 스캐닝 으로 인해 차단되거나 모니터링되는 트
웹 신뢰도 필터 위협 유형	"-",	%Xk	Category Name(카테고리 이름) 또는 T 웹 평판 필터에 의해 반환됩니다. Categ)은 웹 평판이 높을 때 반환되고 Threat 이 낮을 때 반환됩니다. 일반적으로 이 필드는 평판 -4 이하의 사 .
Google Translate 캡슐화된 URL	"-",	%X#10#	Google translate engine에 캡슐화된 UR URL이 없는 경우 필드 값은 "-"입니다.
애플리케이션 제어 (AVC/ADC)	"-","-","-",		이 3개 필드에는 AVC(Application Visib ADC(Application Discovery and Control

AVC/ADC 애플리케이션 이름	"%XO"	AVC 또는 AD 리케이션 이름 또는 ADC 엔 적용됩니다.

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>AVC/ADC 애플리케이션 유형</td><td>"%Xu"</td><td>AVC 또는 AD
리케이션 유형
또는 ADC 엔
적용됩니다.</td></tr>
<tr><td>AVC/ADC 애플리케이션 동작</td><td>"%Xb"</td><td>AVC 또는 AD
리케이션 동작
또는 ADC 엔
적용됩니다.

AVC의 경우
수 없음"입니</td></tr>
</table>
</td></tr>
<tr><td>안전 검색 판정</td><td>"-",</td><td>%XS</td><td>이 값은 안전 검색 또는 사이트 콘텐츠
적용되었는지 여부를 나타냅니다.
<table>
<tr><td>구조</td><td>원래 클라이언트 요청이 안
색 기능이 적용되었습니다.</td></tr>
<tr><td>앙크르</td><td>원래 클라이언트 요청이 안
콘텐츠 등급 기능이 적용되</td></tr>
<tr><td>unsupp(지원 취소)</td><td>지원되지 않는 검색 엔진에
청입니다.</td></tr>
<tr><td>오류</td><td>원래 클라이언트 요청이 안
인해 안전 검색 및 사이트 콘
수 없습니다.</td></tr>
<tr><td>-</td><td>안전 검색 또는 사이트 콘텐
트 요청에 적용되지 않았습
나(예: 트랜잭션이 사용자 지
허용됨) 지원되지 않는 응용
행되었기 때문입니다.</td></tr>
</table>
</td></tr>
<tr><td>평균 대역폭</td><td>11.35,</td><td>%XB</td><td>요청을 처리하는 데 사용된 평균 대역폭</td></tr>
<tr><td>대역폭 제한 제어</td><td>0,</td><td>%XT</td><td>대역폭 제한 제어 설정으로 인해 요청이
타내는 값입니다.</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>"1"은 요청이 제한되었음을 나타냅니다
"0"은 요청이 제한되지 않았음을 나타냅</td></tr>
<tr><td>사용자 유형</td><td>-,</td><td>%l</td><td>요청을 하는 사용자의 유형("[Local]" 또
AnyConnect Secure Mobility가 활성화
활성화되지 않은 경우 값은 하이픈(-)입</td></tr>
<tr><td>아웃바운드 악성코드 스캐닝</td><td>"-","-",</td><td></td><td>이 두 필드는 아웃바운드 악성코드 스캐
라이언트 요청 스캐닝으로 인해 차단되
잭션에 적용됩니다.
<table>
<tr><td>Unified Outbound DVS 판정</td><td>"%X3"</td><td>어떤 스캐
는지에 관
안티멀웨
운드 악성
용될 때
으로 인해
되는 트랜</td></tr>
<tr><td>아웃바운드 위협 이름</td><td>"%X4"</td><td>적용 가능
드 스캐닝
거나 모니
요청에 할
이 위협
스캐닝 엔
상관없습</td></tr>
</table></td></tr>
<tr><td>Advanced Malware Protection</td><td>-"-",-,-,"-","-",</td><td></td><td>이 6개 필드는 Secure Endpoint(Advanc
Protection이라고도 함)와 관련이 있습니
<table>
<tr><td>파일 판정</td><td>%X#1#</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td></td></tr>
<tr><td>위협 이름</td><td>%X#2#</td></tr>
<tr><td>평판 점수</td><td>%X#3#</td></tr>
<tr><td>분석을 위한 업로드 작업</td><td>%X#4#</td></tr>
<tr><td>파일 이름</td><td>%X#5#</td></tr>
<tr><td>파일 SHA</td><td>%X#6#</td></tr>
</table>
</td></tr>
<tr><td>아카이브 스캔</td><td>-,-,"-",</td><td></td><td>다음 3개 필드는 아카이브 파일 검사의
<table>
<tr><td>보관 스캔</td><td>%X#8#</td><td>관 스캔 판정.</td></tr>
</table>
</td></tr>
</table>

			판정		아카이브SCAN_ALLCLEAR
					ARCHIVESCAN_BLOCKED
					아카이브SCAN_NESTEDTC

					아카이브SCAN_UNKNOWN
					아카이브 스캔 불가(_U)
					아카이브SCAN_FILETOOB
			보관 스캔 판정 세부	%X0	보관 스캔 판정 세부 정보. 검 일이 액세스 정책에 따라 차 (ARCHIVESCAN_BLOCKE Objects Blocking(사용자 지

			정보		Verdict Detail(판정 세부사항 의 유형 및 차단된 파일의 이 "UnScanable Archive-Block 에 차단된 파일 유형이 없음
			파일 판정	%Xm	아카이브 스캐너별 파일 판정
웹 탭	-,	%XU	웹 탭 동작		
YouTube URL 카테고리	->	%X#29#	트랜잭션에 할당된 YouTube URL 카테 할당되지 않은 경우 이 필드에 "nc"가 포		

HTTP 응답 코드

다음은 HTTP 응답 코드의 전체 목록입니다

상태 코드	의미
1xx 정보	
100	계속
101	프로토콜 스위칭
102	처리 중
103	초기 힌트
2xx 성공	
200	확인
201	생성됨
202	수락됨
203	신뢰할 수 없는 정보
204	콘텐츠 없음
205	콘텐츠 다시 설정
206	부분 콘텐츠

207	다중 상태
208	이미 보고됨
226	사용된 IM
3xx 리디렉션	
300	다양한 선택 사항
301	영구적으로 이동됨
302	발견(이전 "임시로 이동")
303	기타 참조
304	수정되지 않음
305	프록시 사용
306	스위치 프록시
307	인증을 위한 임시 리디렉션 (일반적으로 SWA가 사용자를 인증하는 동안 투명 배포에서 표시됨)
308	영구 리디렉션
4xx 클라이언트 오류	
400	잘못된 요청
401	웹 서버 인증 필요(일반적으로 SWA가 사용자를 인증하는 동안 투명 배포에 표시됨)
402	지급 필요
403	금지됨
404	찾을 수 없음
405	허용되지 않는 메서드
406	허용되지 않음
407	명시적 프록시 인증 필요
408	요청 시간 초과
409	충돌
410	사라짐
411	길이 필요

412	전제 조건 실패
413	페이로드가 너무 큼
414	URI가 너무 김
415	지원되지 않는 미디어 유형
416	범위를 충족할 수 없음
417	예상 실패
418	저는 찻주전자입니다
421	잘못 전달된 요청
422	처리할 수 없는 엔터티
423	잠김
424	실패한 종속성
425	너무 일러
426	업그레이드 필요
428	전제 조건 필요
429	요청이 너무 많음
431	요청 헤더 필드가 너무 큼
451	법적 이유로 사용 불가
5xx 서버 오류	
500	내부 서버 오류
501	구현되지 않음
502	잘못된 게이트웨이
503	서비스를 사용할 수 없음
504	게이트웨이 시간 초과
505	HTTP 버전이 지원되지 않음
506	Variant도 협상합니다
507	스토리지 부족
508	루프 감지
510	확장되지 않음
511	네트워크 인증 필요

ACL 결정 태그

다음은 ACL 결정 태그의 전체 목록입니다.

ACL 결정 태그	설명
허용_관리자_오류_페이지	웹 프록시에서 알림 페이지 및 해당 페이지에 사용된 로고에 대한 트랜잭션을 허용했습니다.
허용(_C)	웹 프록시에서 액세스 정책 그룹에 대한 맞춤형 URL 카테고리 필터링 설정에 따라 트랜잭션을 허용했습니다.
ALLOW_REFERER	웹 프록시에서 포함/참조된 콘텐츠 제외에 따라 트랜잭션을 허용했습니다.
WBRS 허용(_W)	웹 프록시에서 액세스 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션을 허용했습니다.
AMP_FILE_VERDICT	파일에 대한 AMP 평판 서버의 판정을 나타내는 값:
	1 - 알 수 없음
	2 - 정상
	3 - 악의적
	4 - 검사 불가
아카이브SCAN_ALLCLEAR	보관 스캔 판정
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR - 검사된 아카이브에 차단된 파일 유형이 없습니다.
아카이브SCAN_NESTEDTODEEP	ARCHIVESCAN_BLOCKEDFILETYPE - 검사된 아카이브에 차단된 파일 유형이 있습니다. 로그 항목의 다음 필드(Verdict Detail)에는 세부사항, 특히 차단된 파일의 유형 및 차단된 파일의 이름이 표시됩니다.
아카이브SCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP - 구성된 최대값보다 많은 "캡슐화된" 또는 중첩된 아카이브가 포함되어 있으므로 아카이브가 차단됩니다. Verdict Detail(판정 세부사항) 필드에는 "Un-Scanable Archive-Blocked"가 포함됩니다.
아카이브 스캔 불가(_U)	ARCHIVESCAN_UNKNOWNFMT - 아카이브가 알 수 없는 형식의 파일 형식을

	포함하므로 차단됩니다. 판정 세부사항은 "검사 불가 아카이브-차단됨"입니다.
아카이브SCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE - 아카이브에 검사할 수 없는 파일이 포함되어 있어 차단됩니다. 판정 세부사항은 "검사 불가 아카이브-차단됨"입니다.
	ARCHIVESCAN_FILETOOBIG - 아카이브의 크기가 구성된 최대값보다 크기 때문에 아카이브가 차단됩니다. 판정 세부사항은 "검사 불가 아카이브-차단됨"입니다.
	보관 스캔 판정 세부 정보
	로그 항목의 Verdict 필드와 Verdict 필드는 Verdict에 대한 추가 정보(예: 차단된 파일 유형 및 차단된 파일의 이름, "Un-Scannable Archive-Blocked" 또는 "-"가 아카이브에 차단된 파일 유형이 없음을 나타냅니다.
	예를 들어, 검사 가능한 아카이브 파일이 액세스 정책에 따라 차단된 경우 (ARCHIVESCAN_BLOCKEDFILETYPE) Custom Objects Blocking(사용자 지정 개체 차단) 설정, Verdict Detail(판정 세부사항) 항목에는 차단된 파일의 유형 및 차단된 파일의 이름이 포함됩니다.
	액세스 정책을 참조하십시오. 아카이브 검사에 대한 자세한 내용은 개체 차단 및 아카이브 검사 설정 을 참조하십시오.
차단_관리자	액세스 정책 그룹의 일부 기본 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_CONNECT	액세스 정책 그룹에 대한 HTTP CONNECT 포트 설정에 정의된 대로 대상의 TCP 포트에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_CUSTOM_사용자_에이전트	액세스 정책 그룹에 대한 사용자 지정 사용자 에이전트 차단 설정에 정의된 사용자 에이전트에 따라 트랜잭션이 차단되었습니다.
블록 관리자 터널링	웹 프록시에서 액세스 정책 그룹의 HTTP 포트에서 비 HTTP 트래픽의 터널링을 기반으로 트랜잭션을 차단했습니다.
BLOCK_ADMIN_HTTPS_NonLocalTarget	트랜잭션이 차단되었습니다. 클라이언트가 SSL 포트를 명시적 프록시로 사용하여 인증을 우회하려고 했습니다. 이를 방

	지하기 위해 SSL 연결이 WSA 자체에 연결되는 경우, 실제 WSA 리디렉션 호스트 이름에 대한 요청만 허용됩니다.
BLOCK_ADMIN_IDS	데이터 보안 정책 그룹에 정의된 요청 본문 콘텐츠의 MIME 유형에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_파일_유형	액세스 정책 그룹에 정의된 파일 유형에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_PROTOCOL	액세스 정책 그룹의 Block Protocols 설정에 정의된 프로토콜에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_SIZE	액세스 정책 그룹의 개체 크기 설정에 정의된 응답 크기에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_SIZE_IDS	데이터 보안 정책 그룹에 정의된 요청 본문 콘텐츠의 크기에 따라 트랜잭션이 차단되었습니다.
차단_AMP_RESP	웹 프록시에서 액세스 정책 그룹의 Advanced Malware Protection 설정에 따라 응답을 차단했습니다.
블록_AMW_REQ	웹 프록시에서 아웃바운드 악성코드 스캐닝 정책 그룹의 안티멀웨어 설정에 따라 요청을 차단했습니다. 요청 본문에서 긍정적인 악성코드 판정을 생성했습니다.
블록_AMW_응답	웹 프록시에서 액세스 정책 그룹의 안티멀웨어 설정에 따라 응답을 차단했습니다.
BLOCK_AMW_REQ_URL	웹 프록시는 HTTP 요청의 URL이 안전하지 않을 수 있다고 의심하므로 액세스 정책 그룹에 대한 안티멀웨어 설정에 따라 요청 시 트랜잭션을 차단했습니다.
블록_AVC	액세스 정책 그룹에 대해 구성된 애플리케이션 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_CONTENT_UNSAFE	액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션이 차단되었습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이며 정책이 성인 콘텐츠를 차단하도록 구성되어 있습니다.
BLOCK_CONTINUE_CONTENT_UNSAFE	액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션이 차단되고 Warn and Continue 페이지가 표시되었습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이었으며 성인 콘텐츠에 액세스하는 사용자에게 경고를 제공하도록 정책이

	구성되었습니다.
BLOCK_CONTINUE_CUSTOMCAT	"경고"로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션이 차단되고 Warn and Continue(경고 후 계속) 페이지가 표시되었습니다.
BLOCK_CONTINUE_웹캣	"경고"로 구성된 액세스 정책 그룹의 사전 정의된 URL 카테고리에 따라 트랜잭션이 차단되고 Warn and Continue(경고 후 계속) 페이지가 표시되었습니다.
차단_사용자 지정	액세스 정책 그룹에 대한 사용자 지정 URL 범주 필터링 설정에 따라 트랜잭션이 차단되었습니다.
차단(_I)	웹 프록시에서 외부 DLP 정책 그룹에 정의된 외부 DLP 시스템의 판정을 기반으로 요청을 차단했습니다.
BLOCK_SEARCH_UNSAFE	클라이언트 요청에 안전하지 않은 검색 쿼리가 포함되었으며 액세스 정책이 안전 검색을 적용하도록 구성되어 원래 클라이언트 요청이 차단되었습니다.
BLOCK_SUSPECT_USER_AGENT	액세스 정책 그룹의 의심되는 사용자 에이전트 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_UNSUPPORTED_SEARCH_APP	액세스 정책 그룹의 안전 검색 설정에 따라 트랜잭션이 차단되었습니다. 트랜잭션이 지원되지 않는 검색 엔진에 대한 것이었으며 정책이 지원되지 않는 검색 엔진을 차단하도록 구성되었습니다.
차단(_W)	액세스 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션이 차단되었습니다.
블록_WBRS_IDS	웹 프록시에서 데이터 보안 정책 그룹의 웹 평판 필터 설정에 따라 업로드 요청을 차단했습니다.
차단_웹캣	액세스 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_WEBCAT_IDS	웹 프록시에서 데이터 보안 정책 그룹의 URL 카테고리 필터링 설정에 따라 업로드 요청을 차단했습니다.
차단(_Y)	웹 프록시에서 액세스 정책 그룹에 대한 미리 정의된 YouTube 카테고리 필터링 설정에 따라 트랜잭션을 차단했습니다.
BLOCK_CONTINUE_TYCAT	웹 프록시에서 '경고'로 구성된 액세스 정책 그룹의 사전 정의된 YouTube 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue 페이지를 표시했습니다.

DECRYPT_ADMIN	웹 프록시에서 암호 해독 정책 그룹의 일부 기본 설정에 따라 트랜잭션의 암호를 해독했습니다.
DECRYPT_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었지만 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	EUN이 활성화된 경우 웹 프록시에서 암호 해독 정책 그룹에 대한 연결 삭제로 기본 설정에 따라 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_EXPIRED_CERT	HTTPS 프록시 설정이 EUN이 활성화된 만료된 인증서를 삭제할 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	HTTPS 프록시 설정이 EUN이 활성화된 유효하지 않은 리프 인증서를 삭제할 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_MISMATCH_HOSTNAME	HTTPS 프록시 설정이 EUN이 활성화된 불일치 호스트 이름을 삭제하는 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	HTTPS 프록시 설정이 EUN이 활성화된 다른 오류가 있는 OCSP를 삭제할 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	HTTPS 프록시 설정에서 EUN이 활성화된 OCSP 폐기 인증서를 삭제할 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	HTTPS 프록시 설정이 인식할 수 없는 루트 인증 기관 또는 EUN이 활성화된 발급자 인증서를 삭제하는 경우 웹 프록시에서 트랜잭션의 암호를 해독했습니다.
DECRYPT_EUN_CUSTOMCAT	웹 프록시에서 암호 해독 정책 그룹에 대한 사용자 지정 URL 범주 필터링 설정에 따라 트랜잭션의 암호를 해독했습니다. EUN이 활성화된 경우 트래픽이 삭제됩니다.
DECRYPT_EUN_WBRS	웹 프록시에서 암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션의 암호를 해독했습니다. EUN이 활성화된 경우 트래픽이 삭제됩니다.
DECRYPT_EUN_WBRS_NO_SCORE	웹 프록시에서 암호 해독 정책 그룹의 점수 없는 URL에 대한 웹 평판 필터 설정에 따라 트랜잭션의 암호를 해독했습니다. EUN이 활성화된 경우 트래픽이 삭제됩니다.

DECRYPT_EUN_WEBCAT	웹 프록시에서 암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션의 암호를 해독했습니다. EUN이 활성화된 경우 트래픽이 삭제됩니다.
DECRYPT_WEBCAT	웹 프록시에서 암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션의 암호를 해독했습니다.
DECRYPT_WBRS	웹 프록시에서 암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션의 암호를 해독했습니다.
기본_케이스	웹 평판 또는 안티멀웨어 스캐닝과 같은 AsyncOS 서비스가 트랜잭션에 대해 어떤 작업도 수행하지 않았으므로 웹 프록시에서 클라이언트가 서버에 액세스하도록 허용했습니다.
DENY_ADMIN	웹 프록시에서 트랜잭션을 거부했습니다. 이는 인증이 필요하고 HTTPS 프록시 설정에서 Decrypt for Authentication이 비활성화된 경우 HTTPS 요청에 대해 발생합니다.
DROP_ADMIN	웹 프록시에서 암호 해독 정책 그룹의 일부 기본 설정에 따라 트랜잭션을 삭제했습니다.
DROP_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었기 때문에 웹 프록시에서 트랜잭션을 삭제했습니다.
DROP_WEBCAT	웹 프록시에서 암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션을 삭제했습니다.
DROP_WBRS	웹 프록시에서 암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션을 삭제했습니다.
MONITOR_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었기 때문에 웹 프록시에서 서버 응답을 모니터링했습니다.
모니터_AMP_RESP	웹 프록시에서 액세스 정책 그룹의 Advanced Malware Protection 설정에 따라 서버 응답을 모니터링했습니다.
모니터_AMW_RESP	웹 프록시에서 액세스 정책 그룹의 안티멀웨어 설정에 따라 서버 응답을 모니터링했습니다.
MONITOR_AMW_RESP_URL	웹 프록시는 HTTP 요청의 URL이 안전하지 않을 수 있다고 의심하지만 액세스 정책 그룹의 안티멀웨어 설정에 따라 트랜잭션을 모니터링했습니다.
모니터_AVC	웹 프록시에서 액세스 정책 그룹의 애플

	리케이션 설정에 따라 트랜잭션을 모니터링했습니다.
MONITOR_CONTINUE_CONTENT_UNSAFE	원래 웹 프록시에서 액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션을 차단하고 Warn and Continue(경고 및 계속) 페이지를 표시했습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이었으며 성인 콘텐츠에 액세스하는 사용자에게 경고를 제공하도록 정책이 구성되었습니다. 사용자가 경고를 수락하고 원래 요청한 사이트로 계속 이동했으며, 다른 검사 엔진에서 요청을 차단하지 않았습니다.
MONITOR_CONTINUE_CUSTOMCAT	원래 웹 프록시에서 "경고"로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 사용자가 경고를 수락하고 원래 요청한 사이트로 계속 이동했으며, 다른 검사 엔진에서 요청을 차단하지 않았습니다.
MONITOR_CONTINUE_WEBCAT	원래 웹 프록시에서 "경고"로 구성된 액세스 정책 그룹의 사전 정의된 URL 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 사용자가 경고를 수락하고 원래 요청한 사이트로 계속 이동했으며, 다른 검사 엔진에서 요청을 차단하지 않았습니다.
MONITOR_CONTINUE_TYCAT	원래 웹 프록시에서 '경고'로 구성된 액세스 정책 그룹의 사전 정의된 YouTube 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 사용자가 경고를 수락하고 원래 요청한 사이트로 계속 이동했으며, 다른 검사 엔진에서 요청을 차단하지 않았습니다.
모니터_IDS	웹 프록시에서 데이터 보안 정책 또는 외부 DLP 정책을 사용하여 업로드 요청을 검사했지만 요청을 차단하지는 않았습니다. 액세스 정책과 비교하여 요청을 평가했습니다.
MONITOR_SUSPECT_USER_AGENT	웹 프록시에서 액세스 정책 그룹의 의심되는 사용자 에이전트 설정에 따라 트랜잭션을 모니터링했습니다.
모니터_WBRS	웹 프록시에서 액세스 정책 그룹의 웹 평

	판 필터 설정에 따라 트랜잭션을 모니터링했습니다.
NO_AUTHORIZATION	사용자가 이미 인증 영역에 대해 인증되었지만 애플리케이션 인증 정책에 구성된 인증 영역에 대해서는 인증되지 않았으므로 웹 프록시에서 애플리케이션에 대한 사용자 액세스를 허용하지 않았습니다.
암호 없음(_P)	사용자가 인증에 실패했습니다.
PASSTHRU_ADMIN	암호 해독 정책 그룹의 일부 기본 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었지만 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_WEBCAT	암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_WBRS	암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
리디렉션_CUSTOMCAT	웹 프록시에서 "리디렉션"으로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션을 다른 URL로 리디렉션했습니다.
SAAS_AUTH	사용자가 애플리케이션 인증 정책에 구성된 인증 영역에 대해 투명하게 인증되었으므로 웹 프록시에서 사용자가 애플리케이션에 액세스할 수 있도록 허용했습니다.
기타	권한 부여 실패, 서버 연결 끊기 또는 클라이언트에서 중단과 같은 오류로 인해 웹 프록시에서 요청을 완료하지 못했습니다.

악성코드 스캐닝 판정 값

악성코드 스캐닝 판정은 URL 요청 또는 서버 응답에 할당된 값으로, 악성코드가 포함되어 있을 가능성을 결정합니다. Webroot, McAfee 및 Sophos 스캐닝 엔진은 DVS 엔진이 스캐닝된 개체를 모니터링하거나 차단할지를 결정할 수 있도록 DVS 엔진에 악성코드 스캐닝 판정을 반환합니다. 각 악성코드 스캐닝 판정은 특정 액세스 정책에 대한 Anti-Malware 설정을 편집할 때 Access Policies(액세스 정책) > Reputation and Anti-Malware Settings(평판 및 안티멀웨어 설정) 페이지에 나열된 악성코드 카테고리에 해당합니다.

이 목록에는 서로 다른 악성코드 스캐닝 판정 값과 각 해당 악성코드 카테고리가 표시됩니다.

악성코드 스캐닝 판정 값	악성코드 범주
-	설정되지 않음
0	알 수 없음
1	검사되지 않음
2	Timeout(시간 초과)
3	오류
4	검색할 수 없음
10	일반 스파이웨어
12	브라우저 도우미 개체
13	애드웨어
14	시스템 모니터
18	상용 시스템 모니터
19	전화 걸기
20	납치범
21	피싱 URL
22	트로이 다운로더
23	트로이 목마

악성코드 스캐닝 판정 값	악성코드 범주
24	트로이 피셔
25	웜
26	암호화된 파일
27	바이러스
33	기타 악성코드
34	푸아
35	중단됨
36	발생 휴리스틱
37	알려진 악성 및 고위험 파일

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Secure Web Appliance 모범 사례 사용
- VMware 환경에서 적절한 가상 WSA HA 그룹 기능 확인
- 액세스 로그의 성능 매개변수 구성
- Secure Web Appliance의 HTTPS 액세스 로그 형식 이해
- 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.