

Secure Web Appliance 모범 사례 사용

목차

[소개](#)

[배경 정보](#)

[네트워크 환경](#)

[ICMP](#)

[방화벽](#)

[유니캐스트 역방향 경로 전달](#)

[WCCP를 사용한 IP 스푸핑](#)

[SWA 네트워크 컨피그레이션](#)

[인터페이스](#)

[관리 네트워크 라우팅](#)

[TALOS 텔레메트리](#)

[DNS](#)

[로드 밸런싱](#)

[활성 인증](#)

[수동 인증](#)

[서비스 컨피그레이션](#)

[웹 프록시](#)

[HTTPS 프록시](#)

[레이어 4 트래픽 모니터\(L4TM\)](#)

[정책 컨피그레이션](#)

[복잡성](#)

[식별 프로필](#)

[암호 해독 정책](#)

[액세스 정책](#)

[맞춤형 및 외부 URL 범주](#)

[모니터링 및 알림](#)

[CLI 모니터](#)

[로그](#)

[AWSR\(Advanced Web Security Reporting\)](#)

[이메일 알림](#)

[가용성 모니터링](#)

[SNMP 모니터링](#)

[결론](#)

소개

이 문서에서는 Cisco SWA(Secure Web Appliance)를 구성하는 방법의 모범 사례에 대해 설명합니다.

배경 정보

이 가이드는 모범 사례 컨피그레이션에 대한 참조로 제공되며 지원되는 네트워크 환경, 정책 컨피그레이션, 모니터링 및 트러블슈팅을 비롯한 SWA 구축의 여러 측면을 다룹니다. 여기에 문서화된 모범 사례는 모든 관리자, 설계자 및 운영자가 이해하는 데 중요하지만, 이는 지침일 뿐이며 그와 같이 취급되어야 합니다. 각 네트워크에는 고유한 특정 요구 사항 및 과제가 있습니다.

보안 디바이스로서 SWA는 여러 가지 고유한 방식으로 네트워크와 상호 작용합니다. 이는 웹 트래픽의 소스 및 목적지 둘 다입니다. 웹 서버 및 웹 클라이언트와 동시에 작동합니다. 최소한 서버 측 IP 주소 스푸핑과 중간자(man-in-the-middle) 기술을 사용하여 HTTPS 트랜잭션을 검사합니다. 또한 클라이언트 IP 주소를 스푸핑할 수 있으므로 구축에 또 다른 복잡성이 추가되고 지원 네트워크 컨피그레이션에 추가 요구 사항이 부과됩니다. 이 설명서는 관련 네트워크 디바이스 컨피그레이션과 관련된 가장 일반적인 문제를 다룹니다.

SWA 정책 컨피그레이션은 보안 효율성 및 시행뿐 아니라 어플라이언스의 성능에도 영향을 미칩니다. 이 설명서는 구성의 복잡성이 시스템 리소스에 미치는 영향에 대해 설명합니다. 이러한 맥락에서 복잡성을 정의하고 정책 설계에서 이를 최소화하는 방법을 설명한다. 또한 보안, 확장성 및 효율성을 높이기 위해 특정 기능과 이러한 기능을 어떻게 구성해야 하는지도 고려해야 합니다.

이 문서의 Monitoring and Alerting 섹션에서는 어플라이언스를 모니터링하는 가장 효과적인 방법을 설명하고, 성능 및 가용성과 시스템 리소스 사용의 모니터링에 대해서도 다룹니다. 또한 기본 문제 해결에 유용한 정보도 제공합니다.

네트워크 환경

ICMP

경로 MTU 검색(RFC [1191](#)에 정의됨)에서 메커니즘은 임의의 경로를 따라 패킷의 최대 크기를 결정합니다. IPv4의 경우 디바이스는 패킷의 IP 헤더에 DF(Don't Fragment) 비트를 설정하여 경로를 따라 패킷의 MTU(Maximum Transmission Unit)를 결정할 수 있습니다. 경로를 따라 일부 링크에서 디바이스가 패킷을 프래그먼트화하지 않고 전달할 수 없는 경우 ICMP(Internet Control Message Protocol) 프래그먼트화 필요(Type 3, Code 4) 메시지가 다시 소스로 전송됩니다. 그런 다음 클라이언트는 더 작은 패킷을 다시 보냅니다. 이는 전체 경로에 대한 MTU가 검색될 때까지 계속됩니다. IPv6는 프래그먼트화를 지원하지 않으며, 지정된 링크를 통해 패킷을 맞출 수 없음을 나타내기 위해 Packet Too Big(Type 2) ICMPv6 메시지를 사용합니다.

패킷 단편화 프로세스는 TCP 흐름의 성능에 심각한 영향을 미칠 수 있으므로, SWA는 경로 MTU 검색을 사용합니다. 언급된 ICMP 메시지는 SWA가 네트워크를 통과하는 경로에 대한 MTU를 결정할 수 있도록 관련 네트워크 디바이스에서 활성화되어야 합니다. SWA에서 pathmtudiscovery CLI(command-line interface) 명령을 사용하면 이 동작을 비활성화할 수 있습니다. 이렇게 하면 기본 MTU가 576바이트(RFC 879에 따라)로 떨어지며 성능에 심각한 영향을 미칩니다. 관리자는 etherconfig CLI 명령에서 SWA의 MTU를 수동으로 구성하는 추가 단계를 수행해야 합니다.

WCCP(Web Cache Communication Protocol)의 경우, 웹 트래픽은 인터넷으로 연결되는 클라이언트 경로를 따라 다른 네트워크 디바이스에서 SWA로 리디렉션됩니다. 이 경우 ICMP와 같은 다른 프로토콜은 SWA로 리디렉션되지 않습니다. SWA가 네트워크의 라우터에서 ICMP Fragmentation Needed(ICMP 조각화 필요) 메시지를 트리거할 수 있지만 메시지가 SWA에 전달되지 않을 가능성이 있습니다. 네트워크에서 이 문제가 발생할 수 있는 경우 경로 MTU 검색을 비활성화해야 합니다. 앞서 언급했듯이 이 컨피그레이션에서는 etherconfig CLI 명령을 사용하여 SWA에서 MTU를 수동으로 설정하는 추가 단계가 필요합니다.

방화벽

기본 컨피그레이션에서 SWA는 연결을 프록시할 때 클라이언트 IP 주소를 스푸핑하지 않습니다. 즉, 모든 아웃바운드 웹 트래픽은 SWA IP 주소에서 소싱됩니다. NAT(Network Address Translation) 디바이스가 이를 수용할 수 있는 충분한 외부 주소 및 포트 풀을 가지고 있는지 확인해야 합니다. 이를 위해 특정 주소를 지정하는 것이 좋습니다.

일부 방화벽은 단일 클라이언트 IP 주소에서 수많은 동시 연결이 소싱될 때 트리거되는 DoS(Denial-of-Service) 보호 또는 기타 보안 기능을 사용합니다. 클라이언트 IP 스푸핑이 활성화되지 않은 경우 SWA IP 주소를 이러한 보호에서 제외해야 합니다.

유니캐스트 역방향 경로 전달

SWA는 클라이언트와 통신할 때 서버 IP 주소를 스푸핑하며, 선택적으로 업스트림 서버와 통신할 때 클라이언트 IP 주소를 스푸핑하도록 구성할 수 있습니다. 수신 패킷이 예상 인그레스 포트와 일치하는지 확인하기 위해 스위치에서 uRPF(Unicast Reverse Path Forwarding)와 같은 보호를 활성화할 수 있습니다. 이러한 보호는 라우팅 테이블을 기준으로 패킷의 소스 인터페이스를 검사하여 패킷이 예상 포트에 도착했는지 확인합니다. SWA는 적절한 경우 이러한 보호에서 면제되어야 합니다.

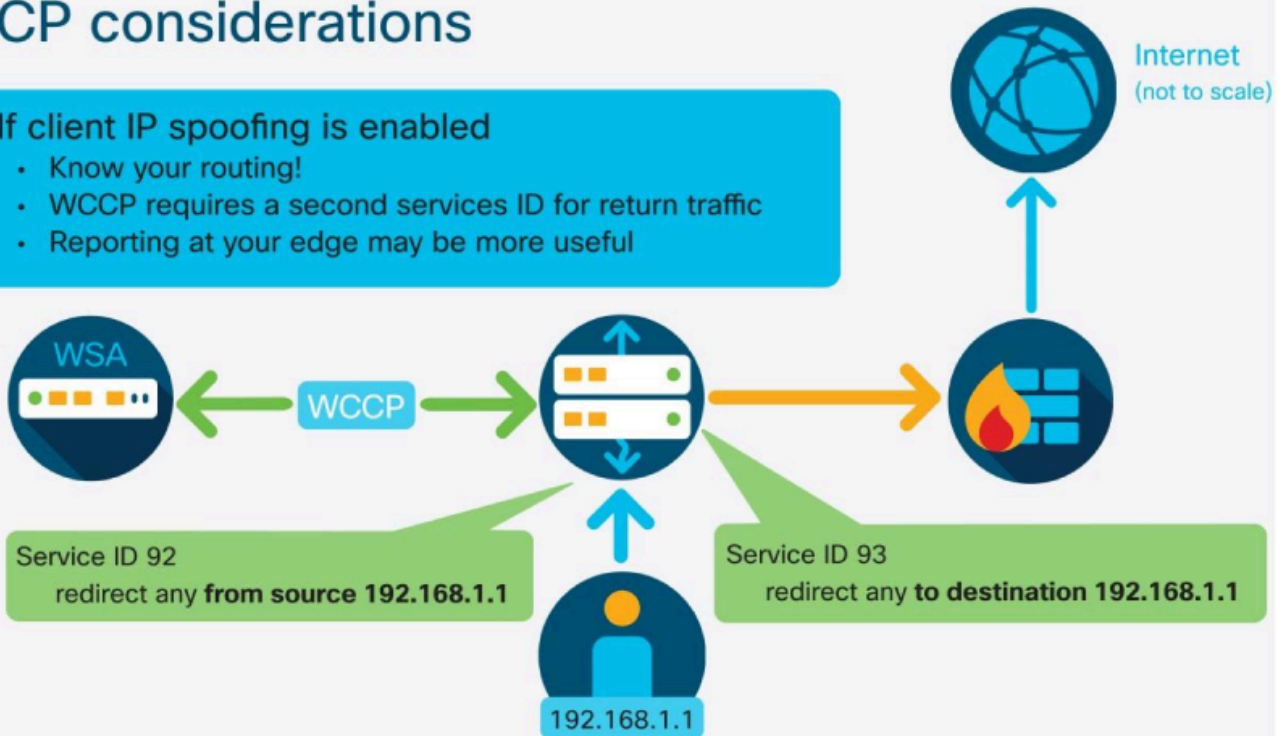
WCCP를 사용한 IP 스푸핑

IP 스푸핑 기능이 SWA에서 활성화되면 아웃바운드 요청은 원래 클라이언트 요청의 소스 주소를 사용하여 어플라이언스를 떠납니다. 이를 위해서는 반환 패킷이 요청을 시작한 클라이언트 대신 SWA 아웃바운드 인터페이스로 라우팅되도록 관련 네트워크 인프라의 추가 컨피그레이션이 필요합니다.

WCCP가 네트워크 디바이스(라우터, 스위치 또는 방화벽)에 구현된 경우, ACL(Access Control List)을 기준으로 트래픽과 매칭하는 서비스 ID가 정의됩니다. 그런 다음 서비스 ID가 인터페이스에 적용되고 리디렉션을 위해 트래픽을 확인하는 데 사용됩니다. IP 스푸핑이 활성화된 경우 반환 트래픽도 SWA로 리디렉션되도록 두 번째 서비스 ID를 생성해야 합니다.

WCCP considerations

- If client IP spoofing is enabled
 - Know your routing!
 - WCCP requires a second services ID for return traffic
 - Reporting at your edge may be more useful



SWA 네트워크 컨피그레이션

인터페이스

SWA에는 5개의 사용 가능한 네트워크 인터페이스(M1, P1, P2, T1 및 T2)가 있습니다. 가능한 경우 이러한 각각을 특정 목적에 활용해야 합니다. 각각의 포트를 사용하는 것은 고유의 이유로 유익합니다. M1 인터페이스는 전용 관리 네트워크에 연결해야 하며, 분할 라우팅을 활성화하여 관리 서비스 노출을 제한해야 합니다. P1은 클라이언트 요청 트래픽으로 제한할 수 있지만, P2는 명시적 프록시 요청을 수락할 수 없습니다. 이렇게 하면 각 인터페이스의 트래픽 양이 줄고 네트워크 설계에서 더 나은 세그멘테이션이 가능합니다.

T1 및 T2 포트는 L4TM(Layer 4 Traffic Monitor) 기능에 사용할 수 있습니다. 이 기능은 미러링된 레이어 2 포트를 모니터링하고 알려진 악성 IP 주소 및 도메인 이름의 차단된 목록을 기반으로 트래픽을 차단하는 기능을 추가합니다. 이를 위해 트래픽의 소스 및 목적지 IP 주소를 확인하고 차단된 목록이 일치하는 경우 TCP 재설정 패킷 또는 Port Unreachable 메시지를 전송합니다. 모든 프로토콜로 전송된 트래픽은 이 기능으로 차단할 수 있습니다.

L4TM 기능이 활성화되지 않은 경우에도 T1 및 T2 포트가 미러링된 포트에 연결되어 있으면 투명한 우회가 향상될 수 있습니다. WCCP의 경우 SWA는 수신 패킷의 소스 및 대상 IP 주소만 알고 있으므로 프록시를 수행하거나 해당 정보를 기반으로 우회하도록 결정해야 합니다. SWA는 레코드의 TTL(Time to Live)에 관계없이 30분마다 우회 설정 목록의 모든 항목을 확인합니다. 그러나 L4TM 기능이 활성화된 경우 SWA는 스누핑된 DNS 쿼리를 사용하여 이러한 레코드를 더 자주 업데이트할 수 있습니다. 이렇게 하면 클라이언트가 SWA와 다른 주소를 확인한 시나리오에서 오탐의 위험이 줄어듭니다.

관리 네트워크 라우팅

전용 관리 네트워크에 인터넷 액세스가 없는 경우 각 서비스가 데이터 라우팅 테이블을 사용하도록 구성할 수 있습니다. 이는 네트워크 토폴로지에 맞게 조정할 수 있으나, 일반적으로 모든 시스템 서비스에는 관리 네트워크를, 클라이언트 트래픽에는 데이터 네트워크를 사용하는 것이 좋습니다. AsyncOS 버전 11.0부터 라우팅을 설정할 수 있는 서비스는 다음과 같습니다.

- 외부 URL 피드
- AMP(Advanced Malware Protection) 파일 평판 및 분석
- 업데이트 및 업그레이드
- DNS
- 액티브 디렉토리

관리 트래픽의 추가 이그레스 필터링을 위해 고정 주소를 다음 서비스에 사용하도록 구성할 수 있습니다.

- 외부 URL 피드:
 1. 사용자 지정은 호스트되는 위치에 따라 다릅니다
 2. AMP 파일 평판 및 분석
 3. cloud-sa.amp.cisco.com(북미)
 4. cloud-sa.eu.amp.cisco.com(유럽)
 5. cloud-sa.apjc.amp.cisco.com(아시아 태평양)
- 업데이트 및 업그레이드:
 1. downloads-static.ironport.com
 2. updates-static.ironport.com

TALOS 텔레메트리

Cisco Talos 그룹은 새로운 위협을 식별하는 것으로 잘 알려져 있습니다. Talos로 전송되는 모든 데이터는 익명화되고 미국 데이터 센터에 저장됩니다. SensorBase에 참여하면 웹 위협의 범주화 및 식별이 향상되고 SWA는 물론 다른 Cisco 보안 솔루션으로부터 더 효과적으로 보호됩니다.

DNS

DNS(Domain Name Server) 보안 모범 사례에 따르면 모든 네트워크는 두 개의 DNS 리졸버를 호스팅해야 합니다. 하나는 로컬 도메인 내의 권한 있는 레코드용이고 다른 하나는 인터넷 도메인의 재귀적 확인용입니다. 이를 수용하기 위해 SWA는 DNS 서버가 특정 도메인에 대해 구성되도록 허용합니다. 로컬 및 재귀 쿼리 둘 다에 대해 하나의 DNS 서버만 사용할 수 있는 경우 모든 SWA 쿼리에 사용할 때 추가되는 로드를 고려하십시오. 로컬 도메인에는 내부 확인기를 사용하고 외부 도메인에는 루트 인터넷 확인기를 사용하는 것이 더 좋습니다. 이는 관리자 위협 프로필 및 허용 한도에 따라 달라집니다.

기본적으로 SWA는 레코드의 TTL과 상관없이 최소 30분 동안 DNS 레코드를 캐시합니다. CDN(Content Delivery Network)을 많이 사용하는 최신 웹 사이트는 IP 주소가 자주 변경되므로 TTL 기록이 낮습니다. 그러면 클라이언트가 특정 서버에 대해 하나의 IP 주소를 캐싱하고 SWA가 동일한 서버에 대해 다른 주소를 캐싱할 수 있습니다. 이에 대응하기 위해 다음 CLI 명령에서 SWA

기본 TTL을 5분으로 낮출 수 있습니다.

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[ ]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

기본 DNS를 사용할 수 없는 경우 보조 DNS 서버를 구성해야 합니다. 모든 서버가 동일한 우선 순위로 구성된 경우 서버 IP가 임의로 선택됩니다. 구성된 서버 수에 따라 지정된 서버에 대한 시간 초과가 달라질 수 있습니다. 테이블은 최대 6개의 DNS 서버에 대한 쿼리 시간 제한입니다.

DNS 서버 수	쿼리 시간 초과(시퀀스)
1	60
2	5, 45
3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

CLI를 통해서만 사용할 수 있는 고급 DNS 옵션도 있습니다. 이러한 옵션은 CLI에서 `advancedproxyconfig > DNS` 명령을 사용하여 사용할 수 있습니다.

다음 옵션 중 하나를 선택합니다.

- 0—항상 DNS 응답을 순서대로 사용
- 1 - 클라이언트 제공 주소를 사용 한 다음 DNS
- 2 - 제한된 DNS 사용
- 3 - 매우 제한적인 DNS 사용

옵션 1과 2에서는 웹 평판이 활성화된 경우 DNS가 사용됩니다.

옵션 2 및 3의 경우, 업스트림 프록시가 없거나 구성된 업스트림 프록시가 실패한 경우 명시적 프록시 요청에 DNS가 사용됩니다.

모든 옵션에서 DNS는 대상 IP 주소가 정책 구성원 자격에 사용될 때 사용됩니다.

이 옵션은 SWA가 클라이언트 요청을 평가할 때 연결할 IP 주소를 결정하는 방법을 제어합니다. 요청이 수신되면 SWA는 대상 IP 주소 및 호스트 이름을 확인합니다. SWA는 TCP 연결을 위해 원래 목적지 IP 주소를 신뢰할지 아니면 자체 DNS 확인을 수행하고 확인된 주소를 사용할지 결정해야 합니다. 기본값은 "0 = Always use DNS answers in order"이며, 이는 SWA가 IP 주소를 제공하도록 클라이언트를 신뢰하지 않음을 의미합니다.

- 옵션 1 — SWA는 클라이언트가 제공한 IP 주소를 연결에 대해 시도하지만, 실패한 경우 확인된 주소로 폴백합니다. 확인된 주소는 정책 평가(웹 카테고리, 웹 평판 등)에 사용됩니다.
- 옵션 2 — SWA는 연결을 위해 클라이언트가 제공한 주소만 사용하며 폴백되지 않습니다. 확인된 주소는 정책 평가(웹 카테고리, 웹 평판 등)에 사용됩니다.
- 옵션 3 — SWA는 연결을 위해 클라이언트가 제공한 주소만 사용하며 폴백되지 않습니다. 클라이언트 제공 IP 주소는 정책 평가에 사용됩니다(웹 카테고리, 웹 평판 등).

선택한 옵션은 지정된 호스트 이름에 대해 확인된 주소를 확인할 때 관리자가 클라이언트에 어느 정도의 신뢰도를 두어야 하는지에 따라 달라집니다. 클라이언트가 다운스트림 프록시인 경우 옵션 3을 선택하여 불필요한 DNS 조회가 추가로 지연되는 것을 방지합니다.

로드 밸런싱

WCCP는 최대 8개의 어플라이언스를 사용할 때 투명한 트래픽 로드 밸런싱을 지원합니다. 해시 또는 마스크를 기준으로 트래픽 흐름의 균형을 맞출 수 있으며, 네트워크에 어플라이언스 모델이 혼용되는 경우 가중치가 적용될 수 있으며, 다운타임 없이 서비스 풀에서 디바이스를 추가 및 제거할 수 있습니다. 8개의 SWA로 처리할 수 있는 것보다 요구 사항이 많으면 전용 로드 밸런서를 사용하는 것이 좋습니다.

WCCP 컨피그레이션의 구체적인 모범 사례는 사용된 플랫폼에 따라 다릅니다. Cisco Catalyst® 스위치의 모범 사례는 [Cisco Catalyst Instant Access Solution](#) 백서에 문서화되어 있습니다.

WCCP는 Cisco ASA(Adaptive Security Appliance)와 함께 사용할 경우 제한이 있습니다. 즉, 클라이언트 IP 스푸핑은 지원되지 않습니다. 또한 클라이언트와 SWA는 동일한 인터페이스 뒤에 있어야 합니다. 따라서 레이어 4 스위치 또는 라우터를 사용하여 트래픽을 리디렉션하는 것이 더 유연합니다. ASA 플랫폼의 WCCP 컨피그레이션은 WCCP [on ASA: Concepts, Limitations, and Configuration](#)에 설명되어 있습니다.

명시적 구축의 경우 PAC(Proxy Autoconfiguration) 파일이 가장 널리 배포되는 방법이지만, 이 문서의 범위를 벗어나는 여러 가지 단점과 보안 문제가 있습니다. PAC 파일이 배포된 경우, 공격자의 공통 대상인 WPAD(Web Proxy Autodiscover Protocol)에 의존하지 않고 GPO(Group Policy Objects)를 사용하여 위치를 구성하는 것이 좋으며 잘못 구성하면 쉽게 악용될 수 있습니다. SWA는 여러 PAC 파일을 호스팅하고 브라우저의 캐시에서 파일의 만료일을 제어할 수 있습니다.

PAC 파일은 구성 가능한 TCP 포트 번호(기본적으로 9001)에서 SWA에서 직접 요청할 수 있습니다. . 포트를 지정하지 않으면 아웃바운드 웹 요청인 것처럼 프록시 프로세스 자체에 요청을 보낼 수 있습니다. 이 경우 요청에 있는 HTTP 호스트 헤더를 기반으로 특정 PAC 파일을 제공할 수 있습니다.

Hostnames for Serving PAC Files Directly ?		
To serve PAC files for PAC file requests that do not include the PAC server port, enter one or more hosts here and choose a default PAC file name. You can specify hosts using hostnames or IP addresses.		
<input type="text"/>	Default PAC File for "Get/" Request through Proxy Port <input type="text"/>	<input type="button" value="Add Row"/>
<input type="text"/>	<input type="button" value="Select a PAC File..."/>	<input type="button" value="X"/>

고가용성 환경에서 사용할 경우 Kerberos를 다르게 구성해야 합니다. SWA는 여러 호스트 이름을 SPN(서비스 원칙 이름)과 연결할 수 있도록 하는 keytab 파일을 지원합니다. 자세한 내용은 [고가용성 구축에서 Kerberos 인증을 위해 Windows Active Directory에서 서비스 계정 생성을 참조하십시오](#).

활성 인증

Kerberos는 NTLMSSP(NT LAN Manager Security Support Provider)보다 안전하며 널리 지원되는 인증 프로토콜입니다. Apple OS X 운영 체제는 NTLMSSP를 지원하지 않지만 도메인이 가입된 경우 Kerberos를 사용하여 인증할 수 있습니다. 기본 인증은 HTTP 헤더에서 암호화되지 않은 자격 증명을 전송하고 네트워크에서 공격자가 쉽게 스니핑할 수 있으므로 사용하지 않아야 합니다. 기본 인증을 사용해야 하는 경우 자격 증명에 암호화된 터널을 통해 전송되도록 하려면 자격 증명 암호화를 활성화해야 합니다.

가용성을 보장하려면 둘 이상의 도메인 컨트롤러를 컨피그레이션에 추가해야 하지만, 이 트래픽에는 고유한 로드 밸런싱이 없습니다. SWA는 구성된 모든 도메인 컨트롤러로 TCP SYN 패킷을 전송하며, 첫 번째 응답 패킷이 인증에 사용됩니다.

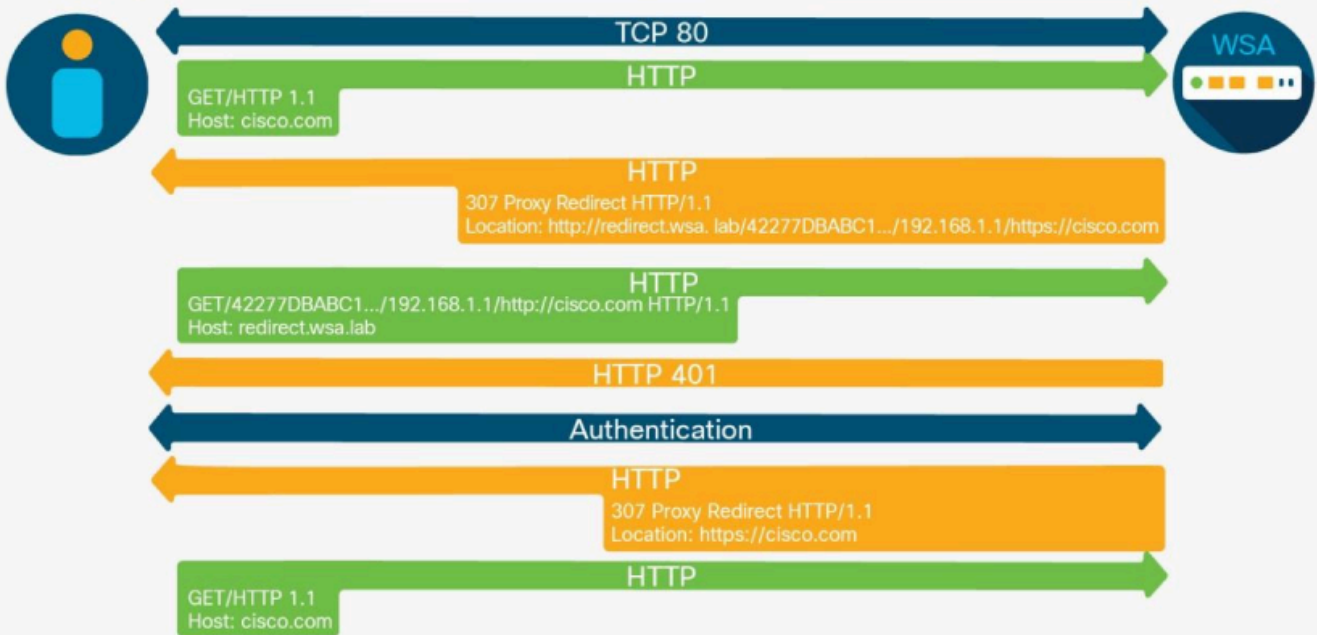
인증 설정 페이지에 구성된 리디렉션 호스트 이름은 인증을 완료하기 위해 투명 클라이언트가 전송되는 위치를 결정합니다. Windows 클라이언트가 통합 인증을 완료하고 SSO(Single Sign-On)를 달성하려면 리디렉션 호스트 이름이 인터넷 옵션 제어판의 신뢰할 수 있는 사이트 영역에 있어야 합니다. Kerberos 프로토콜에서는 FQDN(Fully Qualified Domain Name)을 사용하여 리소스를 지정해야 합니다. 즉, Kerberos가 의도된 인증 메커니즘인 경우 "shortname"(또는 "NETBIOS" 이름)을 사용할 수 없습니다. FQDN을 신뢰할 수 있는 사이트에 수동으로 추가해야 합니다(예: 그룹 정책을 통해). 또한 인터넷 옵션 컨트롤 패널에서 사용자 이름과 비밀번호로 자동 로그인을 설정해야 합니다.

브라우저가 네트워크 프록시를 사용하여 인증을 완료하려면 Firefox에서 추가 설정도 필요합니다. 이러한 설정은 about:config 페이지에서 구성할 수 있습니다. Kerberos가 성공적으로 완료되려면 리디렉션 호스트 이름을 network.negotiate-auth.trusted-uris 옵션에 추가해야 합니다. NTLMSSP의 경우 network.automatic-ntlm-auth.trusted-uris 옵션에 추가해야 합니다.

인증 서로게이트는 인증이 완료된 후 설정된 기간 동안 인증된 사용자를 기억하는 데 사용됩니다. 발생하는 활성 인증 이벤트의 수를 제한하려면 가능하면 항상 IP 서로게이트를 사용해야 합니다. 클라이언트를 적극적으로 인증하는 작업은 리소스 집약적인 작업이며, 특히 Kerberos가 사용되는 경우 더욱 그렇습니다. 서로게이트 시간 제한은 기본적으로 3600초(1시간)이며 낮출 수 있지만 가장 낮은 권장 값은 900초(15분)입니다.

이 이미지는 "redirect.WSA.lab"이 리디렉션 호스트 이름으로 사용되는 방법을 보여줍니다.

Transparent authentication packet flow



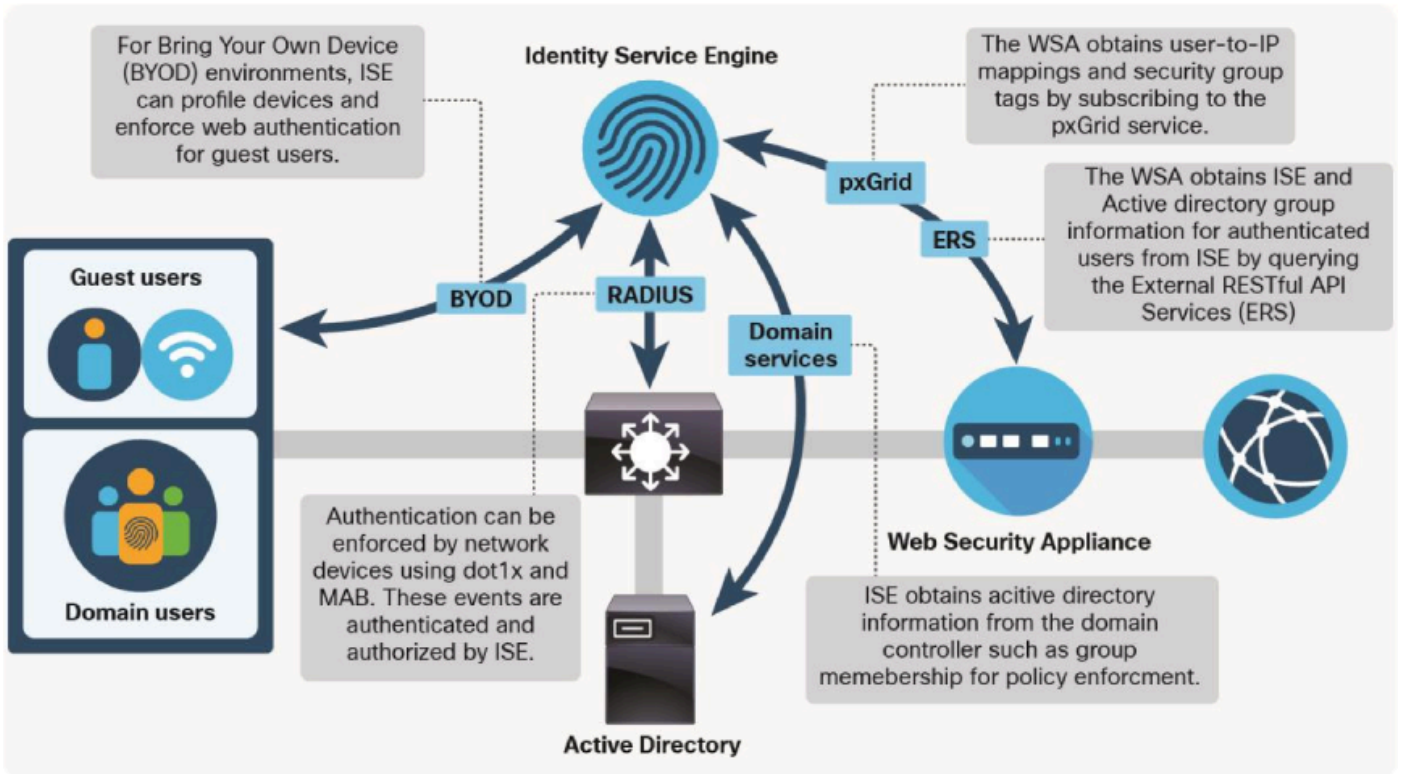
수동 인증

SWA는 다른 Cisco 보안 플랫폼을 활용하여 프록시 사용자를 수동적으로 식별할 수 있습니다. 수동적으로 사용자를 식별하면 직접 인증 챌린지 및 SWA의 모든 Active Directory 통신이 필요하지 않으므로 어플라이언스에서 지연 및 리소스 사용량이 줄어듭니다. 현재 수동 인증에 사용 가능한 메커니즘은 CDA(Context Directory Agent), ISE(Identity Services Engine) 및 ISE-PIC(Identity Services Connector Passive Identity Connector)를 통해 이루어집니다.

ISE는 풍부한 기능을 갖춘 제품으로, 관리자가 인증 서비스를 중앙 집중화하고 광범위한 네트워크 액세스 제어 기능을 활용할 수 있도록 지원합니다. ISE가 사용자 인증 이벤트에 대해 알게 되면 (Dot1x 인증 또는 웹 인증 리디렉션을 통해) 인증에 포함된 사용자 및 디바이스에 대한 정보가 포함된 세션 데이터베이스를 채웁니다. SWA는 pxGrid(Platform Exchange Grid)를 통해 ISE에 연결하고 프록시 연결과 연결된 사용자 이름, IP 주소 및 SGT(Security Group Tag)를 가져옵니다. AsyncOS 버전 11.7부터 SWA는 그룹 정보를 얻기 위해 ISE의 ERS(External Restful Service)에 쿼리할 수도 있습니다.

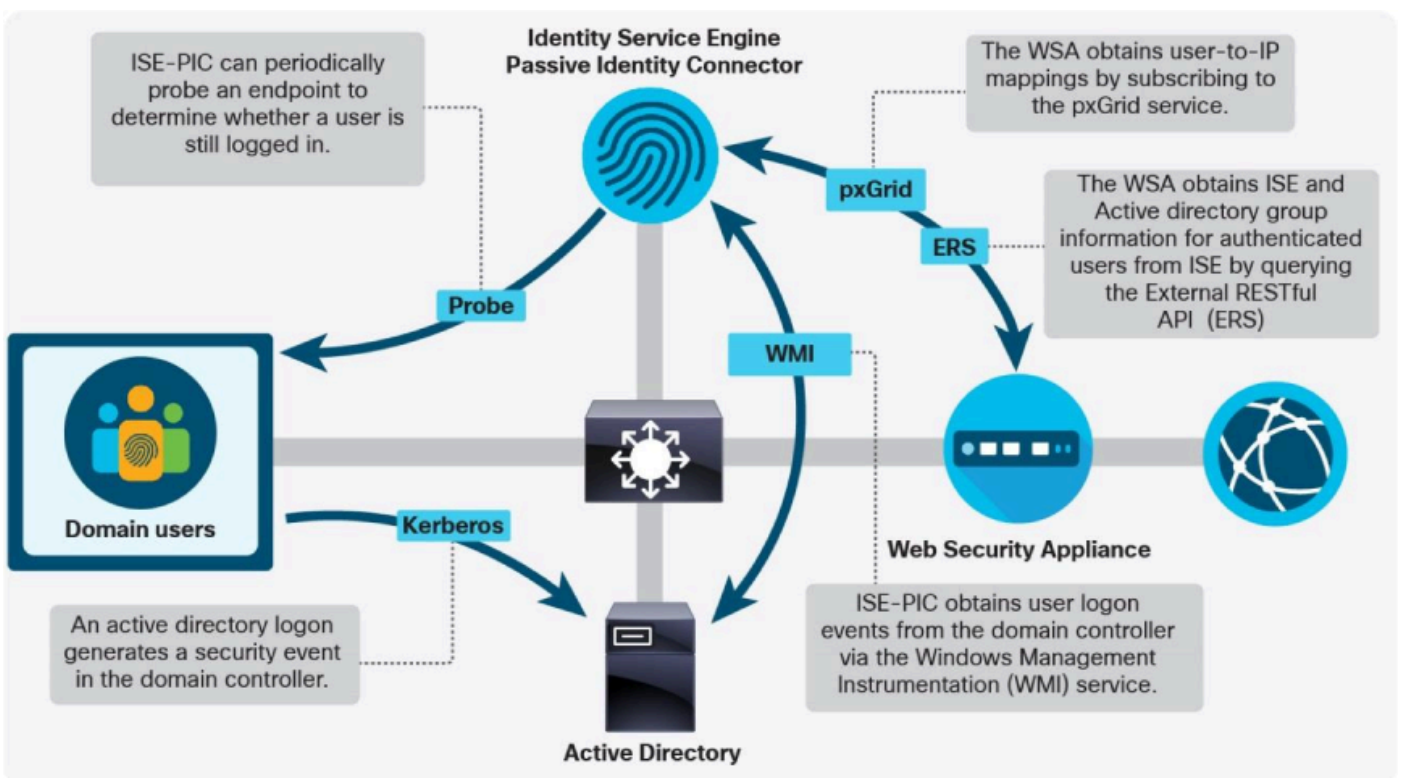
권장되는 버전은 ISE 3.1 및 SWA 14.0.2-X 이상입니다. SWA용 ISE 호환성 매트릭스에 대한 자세한 내용은 [Secure Web Appliance용 ISE 호환성 매트릭스를 참조하십시오](#).

전체 통합 단계에 대한 자세한 내용은 [Web Security Appliance 최종 사용자 가이드를 참조하십시오](#).



Cisco에서 Cisco CDA(Context Directory Agent) 소프트웨어의 단종을 발표합니다. [Cisco CDA\(Context Directory Agent\)](#)를 참조하십시오.

CDA 패치 6부터는 Microsoft Server 2016과 호환됩니다. 그러나 관리자는 CDA 구축을 ISE-PIC로 마이그레이션하는 것이 좋습니다. 두 솔루션 모두 WMI를 사용하여 Windows 보안 이벤트 로그를 구독하여 사용자-IP 매핑("세션"이라고 함)을 생성합니다. CDA의 경우 SWA는 RADIUS를 사용하여 이러한 매핑을 쿼리합니다. ISE-PIC의 경우 전체 ISE 구축에서와 동일한 pxGrid 및 ERS 연결이 사용됩니다. ISE-PIC 기능은 전체 ISE 설치와 독립형 가상 어플라이언스에서 사용할 수 있습니다.



서비스 컨피그레이션

웹 프록시

대역폭을 절약하고 성능을 높이려면 웹 프록시 컨피그레이션에서 캐싱을 활성화해야 합니다. 이는 SWA가 기본적으로 HTTPS 트랜잭션을 캐시하지 않기 때문에 HTTPS 트래픽의 비율이 증가함에 따라 덜 중요해지고 있습니다. 프록시가 명시적 클라이언트만 지원하도록 구축된 경우, 프록시 서비스로 특별히 지정되지 않은 트래픽을 거부하려면 전달 모드를 지정해야 합니다. 이렇게 하면 어플라이언스 공격 표면이 줄어들고 적절한 보안 원칙이 적용됩니다. 즉, 필요하지 않을 경우 이를 끕니다.

범위 요청 헤더는 다운로드할 파일의 바이트 범위를 지정하기 위해 HTTP 요청에 사용됩니다. 운영 체제 및 애플리케이션 업데이트 데몬에서 한 번에 파일의 작은 부분을 전송하는 데 일반적으로 사용됩니다. 기본적으로 SWA는 AV(Antivirus) 스캐닝, 파일 평판 및 분석, AVC(Application Visibility Control)를 위해 전체 파일을 가져올 수 있도록 이러한 헤더를 스트립합니다. 프록시 설정에서 전역적으로 범위 요청 헤더의 전달을 활성화하면 관리자가 해당 헤더를 전달하거나 제거하는 개별 액세스 정책을 생성할 수 있습니다. 이 컨피그레이션에 대한 자세한 내용은 액세스 정책, 섹션에서 설명합니다.



HTTPS 프록시

보안 모범 사례에서는 개인 키가 사용되는 어플라이언스에 개인 키를 생성해야 하며 다른 곳으로 전송해서는 안 됩니다. HTTPS 프록시 마법사를 사용하면 TLS(Transport Layer Security) 연결의 암호 해독에 사용되는 키 쌍 및 인증서를 생성할 수 있습니다. 그러면 CSR(Certificate Signing Request)을 다운로드하여 사내 CA(Certificate Authority)에 의해 서명할 수 있습니다. AD(Active Directory) 환경에서 이 방법은 AD 통합 CA가 도메인의 모든 구성원이 자동으로 신뢰하며 인증서를 배포하는 데 추가 단계가 필요하지 않기 때문에 가장 좋습니다.

HTTPS 프록시의 한 가지 보안 기능은 서버 인증서를 검증하는 것입니다. 모범 사례에서는 유효하지 않은 인증서의 경우 연결을 삭제해야 한다고 제안합니다. Decrypt for EUN을 활성화하면 SWA가 차단 이유를 설명하는 차단 페이지를 표시할 수 있습니다. 이 옵션을 활성화하지 않으면 차단된 모든 HTTPS 사이트가 브라우저 오류를 발생시킵니다. 이는 헬프 데스크 티켓 증가와 SWA가 연결을 차단했다는 지식이 아니라, 사용자의 입장에서 어떤 것이 끊겼다는 가정으로 이어집니다. 유효하지 않은 모든 인증서 옵션은 최소 Decrypt로 설정해야 합니다. 이러한 옵션 중 하나를 Monitor(모니터링)로 남겨두면 인증서 문제로 인해 사이트가 로드되지 않을 경우 유용한 오류 메시지를 로깅할 수 있습니다.

Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Monitor
	Mismatched Hostname: Monitor
	Unrecognized Root Authority / Issuer: Monitor
	Invalid Signing Certificate: Monitor
	Invalid Leaf Certificate: Monitor
	All other error types: Monitor
Online Certificate Status Protocol Options	
OCSP Result Handling:	Revoked Certificate: Monitor
	Unknown Certificate: Monitor
	OCSP Error: Monitor

마찬가지로, OCSP(Online Certificate Services Protocol) 검사는 활성화 상태로 유지해야 하며 어떤 옵션에서도 모니터를 사용하지 않아야 합니다. 관련 오류 메시지의 로깅을 허용하려면 폐기된 인증서를 삭제하고 다른 모든 인증서를 최소한 Decrypt로 설정해야 합니다. AIA 체이싱(Authority Information Access Chasing)은 클라이언트가 인증서의 서명자를 스캔할 수 있는 수단이며 추가 인증서를 가져올 수 있는 URL입니다. 예를 들어, 서버에서 받은 인증서 체인이 완전하지 않은 경우(중간 또는 루트 인증서 누락) SWA는 AIA 필드를 확인하여 누락 인증서를 가져오고 신뢰성을 확인하는 데 사용할 수 있습니다. 이 설정은 CLI에서 다음 명령에서만 사용할 수 있습니다.

```
SWA_CLI> advancedproxyconfig
```

```
Choose a parameter group:
```

- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters


```
[ ]> HTTPS
```

```
...
```

```
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
```

```
[Y]>
```

```
...
```

 **참고:** 많은 최신 서버가 클라이언트에 전체 신뢰 체인을 제공하기 위해 이 메커니즘을 사용하므로 이 설정은 기본적으로 활성화되어 있으며 비활성화되어서는 안 됩니다.

레이어 4 트래픽 모니터(L4TM)

L4TM은 프록시를 통과하지 않는 악의적인 트래픽을 포함할 뿐만 아니라 모든 TCP 및 UDP 포트의

트래픽을 포함하도록 SWA의 범위를 확장하는 매우 효과적인 방법입니다. T1 및 T2 포트는 네트워크 탭 또는 스위치 모니터 세션에 연결하기 위한 것입니다. 이를 통해 SWA는 클라이언트의 모든 트래픽을 수동적으로 모니터링할 수 있습니다. 악성 IP 주소로 향하는 트래픽이 발견되면 SWA는 서버 IP 주소를 스누핑하는 동안 RST를 전송하여 TCP 세션을 종료할 수 있습니다. UDP 트래픽의 경우 Port Unreachable 메시지를 전송할 수 있습니다. 모니터 세션을 구성할 때 SWA의 관리 인터페이스로 향하는 모든 트래픽을 제외하여 해당 기능이 디바이스에 대한 액세스를 잠재적으로 방해하지 않도록 하는 것이 좋습니다.

L4TM은 악성 트래픽을 모니터링하는 것 외에도 우회 설정 목록을 업데이트하기 위해 DNS 쿼리를 스누핑합니다. 이 목록은 WCCP 구축에서 웹 서버로의 직접 라우팅을 위해 특정 요청을 WCCP 라우터로 되돌리는 데 사용됩니다. 우회 설정 목록과 일치하는 패킷은 프록시에서 처리되지 않습니다. 목록에는 IP 주소 또는 서버 이름이 포함될 수 있습니다. SWA는 레코드의 TTL에 관계없이 30분마다 우회 설정 목록의 모든 항목을 확인합니다. 그러나 L4TM 기능이 활성화된 경우 SWA는 스누핑된 DNS 쿼리를 사용하여 이러한 레코드를 더 자주 업데이트할 수 있습니다. 이렇게 하면 클라이언트가 SWA와 다른 주소를 확인한 시나리오에서 오탐의 위험이 줄어듭니다.

정책 컨피그레이션

올바른 정책 컨피그레이션은 SWA의 성능 및 확장성의 핵심입니다. 이는 고객 보호와 회사 요구 사항 시행에 있어서 정책 자체의 효과뿐만 아니라, 어떤 정책이 구성되는지가 리소스 사용과 SWA의 전반적인 상태 및 성과에 직접적인 영향을 주기 때문입니다. 정책 집합이 지나치게 복잡하거나 잘못 설계되면 어플라이언스에서 불안정하고 대응성이 저하될 수 있습니다.

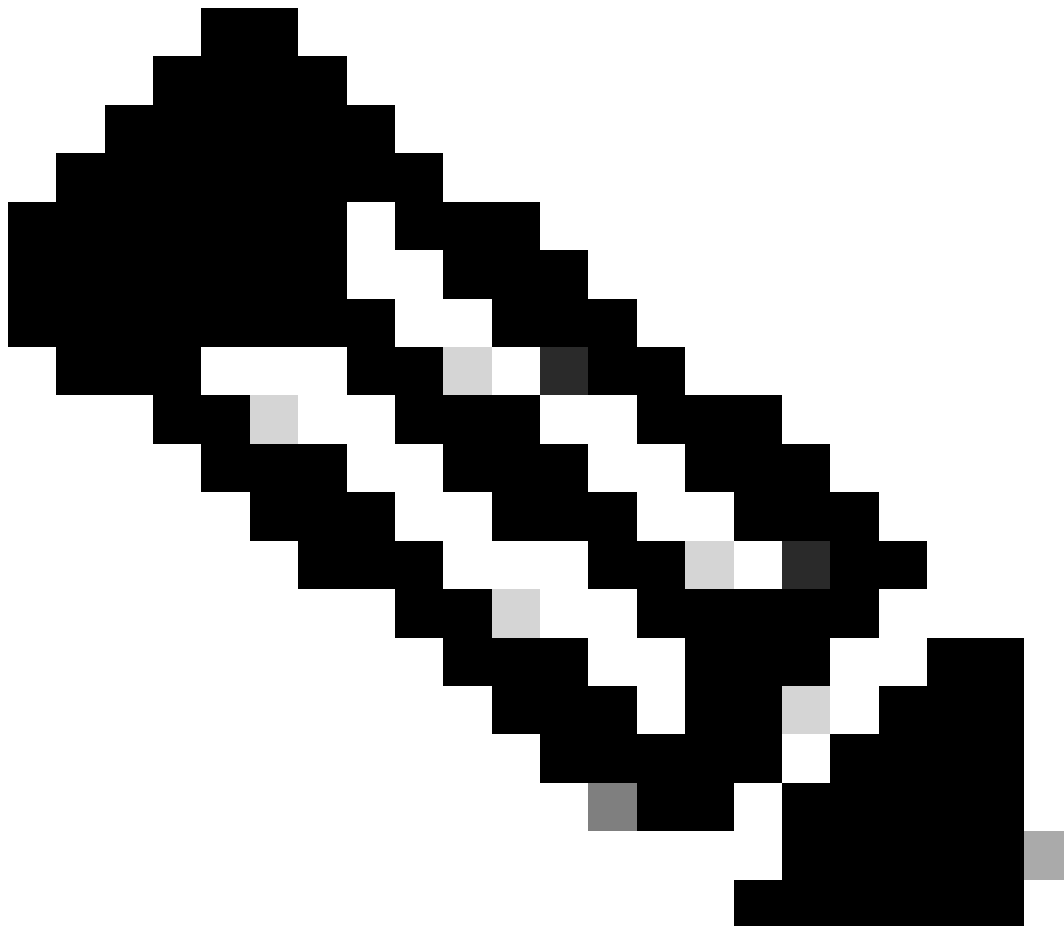
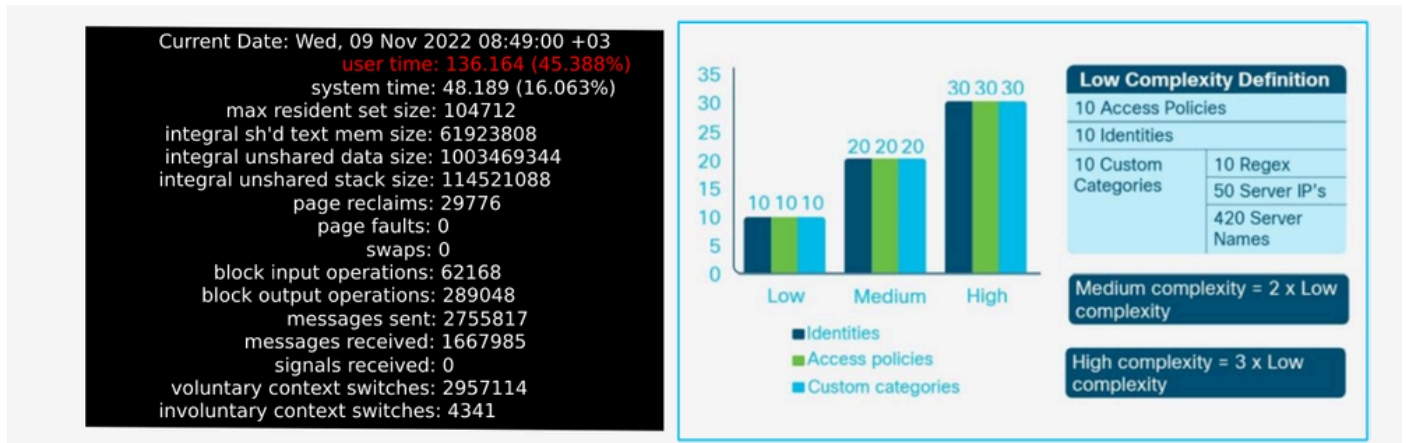
복잡성

SWA 정책의 구축에는 다양한 정책적 요소가 사용되고 있다. 컨피그레이션에서 생성된 XML 파일은 여러 백엔드 컨피그레이션 파일 및 액세스 규칙을 생성하는 데 사용됩니다. 구성이 복잡할수록 프록시 프로세스가 각 트랜잭션에 대한 다양한 규칙 집합을 평가하는 데 더 많은 시간을 소비해야 합니다. SWA의 벤치마킹 및 크기 조정에서는 3단계 컨피그레이션 복잡성을 나타내는 기본 정책 요소 집합이 생성됩니다. 10개의 ID 프로필, 암호 해독 정책, 액세스 정책, 10개의 regex 항목, 50개의 서버 IP 주소, 420개의 서버 호스트 이름을 포함하는 10개의 사용자 지정 카테고리는 낮은 복잡성 구성으로 간주됩니다. 각 수치에 2와 3을 곱하면 각각 중간 복잡성 및 높은 복잡성 컨피그레이션이 생성됩니다.

컨피그레이션이 너무 복잡해지면 첫 번째 증상은 일반적으로 웹 인터페이스 및 CLI에서 느린 응답을 포함합니다. 처음에는 사용자에게 큰 영향을 미칠 수 없습니다. 그러나 컨피그레이션이 복잡할수록 프록시 프로세스가 사용자 모드에서 더 많은 시간을 보내야 합니다. 따라서 이 모드에서 소요된 시간의 백분율을 확인하는 것은 너무 복잡한 컨피그레이션을 느린 SWA의 원인으로 진단하는 유용한 방법이 될 수 있습니다.

CPU 시간(초)은 track_stats 로그에 5분마다 기록됩니다. 이는 사용자 시간 백분율을 (사용자 시간 + 시스템 시간)/300으로 계산할 수 있음을 의미한다. 사용자 시간이 270에 가까워지면 프로세스가 사용자 모드에서 너무 많은 CPU 사이클을 소비하고 있으며, 이는 구성이 너무 복잡하여 효율적으

로 구문 분석할 수 없기 때문에 거의 항상 발생합니다.



참고: 지금까지 SWA의 최대 동시 클라이언트 연결 수는 60,000개이고 동시 서버 연결 수는 60,000개입니다.

식별 프로필

ID(식별) 프로필은 새 요청을 받을 때 평가되는 첫 번째 정책 요소입니다. ID 프로필의 첫 번째 섹션에서 구성된 모든 정보는 논리적 AND로 평가됩니다. 즉, 요청과 프로필이 일치하려면 모든 기준이 일치해야 합니다. 정책을 생성할 때는 반드시 필요한 만큼만 구체적이어야 합니다. 개별 호스트 주소를 포함하는 프로필은 거의 필요하지 않으며, 불규칙한 컨피그레이션으로 이어질 수 있습니다. 일반적으로 HTTP 헤더, 사용자 지정 범주 목록 또는 서버넷에 있는 사용자 에이전트 문자열을 활용하는 것이 프로필의 범위를 제한하는 더 나은 전략입니다.

일반적으로 인증이 필요한 정책은 맨 아래에 구성되며 그 위에 예외가 추가됩니다. 인증이 필요하지 않은 정책을 주문할 경우 가장 많이 사용되는 정책이 가능한 한 가장 상위 정책과 가장 가까운 것이어야 합니다. 액세스를 제한하기 위해 실패한 인증에 의존하지 마십시오. 네트워크의 클라이언트가 프록시에 대해 인증할 수 없는 것으로 알려진 경우 인증에서 제외되고 액세스 정책에서 차단되어야 합니다. 반복적으로 인증할 수 없는 클라이언트는 SWA에 인증되지 않은 요청을 보냅니다. SWA는 리소스를 사용하며 과도한 CPU 및 메모리 사용을 일으킬 수 있습니다.

관리자에게 흔히 발생하는 오해는 고유한 ID 프로필과 해당 암호 해독 정책 및 액세스 정책이 있어야 한다는 것입니다. 이는 정책 구성에 비효율적인 전략입니다. 가능한 경우 단일 ID 프로필을 여러 암호 해독 및 액세스 정책과 연결할 수 있도록 정책을 "축소"해야 합니다. 이는 트래픽이 정책과 일치하려면 지정된 정책의 모든 기준이 일치해야 하기 때문에 가능합니다. 인증 정책에서 더 일반적이고 결과 정책에서 더 구체적이므로 전체적으로 더 적은 정책을 적용할 수 있습니다.

Client / User Identification Profiles
Managed by: ngsma.chclassen.lab - local changes will be overwritten.

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	AD Auth Subnets: 192.168.10.50, 192.168.0.40 Protocols: HTTP/HTTPS	Authenticate: Realm: AD (Scheme: Basic, NTLMSSP, Kerberos)	(global profile)	

Global Identification Profile
Managed by: ngsma.chclassen.lab - local changes will be overwritten.

Edit Order...

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects
1	Github Identification Profile: AD Auth All identified users URL Categories: Github	(global policy)	Monitor: 1	(global policy)	(global policy)
2	Contractors Identification Profile: AD Auth 1 groups (AD\CHCLASEN\Contractors)	(global policy)	(global policy)	(global policy)	(global policy)
3	Domain Users AP Identification Profile: AD Auth All identified users	(global policy)	(global policy)	(global policy)	(global policy)
Global Policy Identification Profile: All		No blocked items	Monitor: 85	Monitor: 356	No blocked items

Edit Policy Order...

- Policies do not require a 1:1 flow!
- Reduce complexity by collapsing where possible.

암호 해독 정책

ID 프로필과 마찬가지로, 암호 해독 정책에 설정된 기준도 논리적 AND로 평가되며, ISE의 정보가 사용되는 경우 한 가지 중요한 예외가 있습니다. 구성된 요소(AD 그룹, 사용자 또는 SGT)에 따라 정책 일치가 작동하는 방식은 다음과 같습니다.

- AD 그룹 및 사용자 - 이전 동작에 대한 변경 사항이 없습니다. 사용자가 그룹의 멤버이거나 사

용자가 정책에 지정된 경우 정책이 일치합니다.

- SGT 및 AD 그룹 및 사용자 - 사용자가 SGT와 연결되고 AD 그룹의 멤버이거나 사용자가 정책에 지정된 경우 정책이 일치됩니다.
- SGT and users(SGT 및 사용자) - 사용자가 SGT와 연결되거나 사용자가 정책에 지정된 경우 정책이 일치됩니다.

SWA에서 수행하는 모든 서비스 중에서 성능 측면에서 HTTPS 트래픽의 평가가 가장 중요합니다. 해독된 트래픽의 비율은 어플라이언스의 크기를 조정하는 방법에 직접적인 영향을 미칩니다. 관리자는 웹 트래픽의 75% 이상을 HTTPS로 간주할 수 있습니다.

초기 설치 후 해독된 트래픽의 비율을 결정해야 향후 성장에 대한 기대치가 정확하게 설정됩니다. 구축 후에는 분기별로 한 번씩 이 번호를 확인해야 합니다. SWA에서 해독된 HTTPS 트래픽의 비율을 찾는 것은 추가 로그 관리 소프트웨어가 없어도 access_logs의 복사본으로 쉽게 할 수 있습니다. Simple Bash 또는 PowerShell 명령을 사용하여 이 숫자를 얻을 수 있습니다. 각 환경에 대해 설명된 단계는 다음과 같습니다.

1. Linux 명령:

```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

2. Powershell 명령:

```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

암호 해독 정책을 설계할 때 정책에 나열된 다양한 작업으로 인해 어플라이언스가 HTTPS 연결을 평가하는 방법을 이해하는 것이 중요합니다. SWA가 모든 패킷을 해독하지 않고 클라이언트와 서버가 TLS 세션의 각 끝을 종료하도록 허용해야 하는 경우 passthrough 작업이 사용됩니다. 사이트가 passthrough로 설정된 경우에도 SWA는 서버와의 TLS 핸드셰이크 하나를 완료해야 합니다. 이는 SWA가 인증서 유효성을 기준으로 연결을 차단하도록 선택해야 하며, 인증서를 얻기 위해 서버와의 TLS 연결을 시작해야 하기 때문입니다. 인증서가 유효하면 SWA는 연결을 닫고 클라이언트가 서버와 직접 세션을 계속 설정할 수 있도록 합니다.

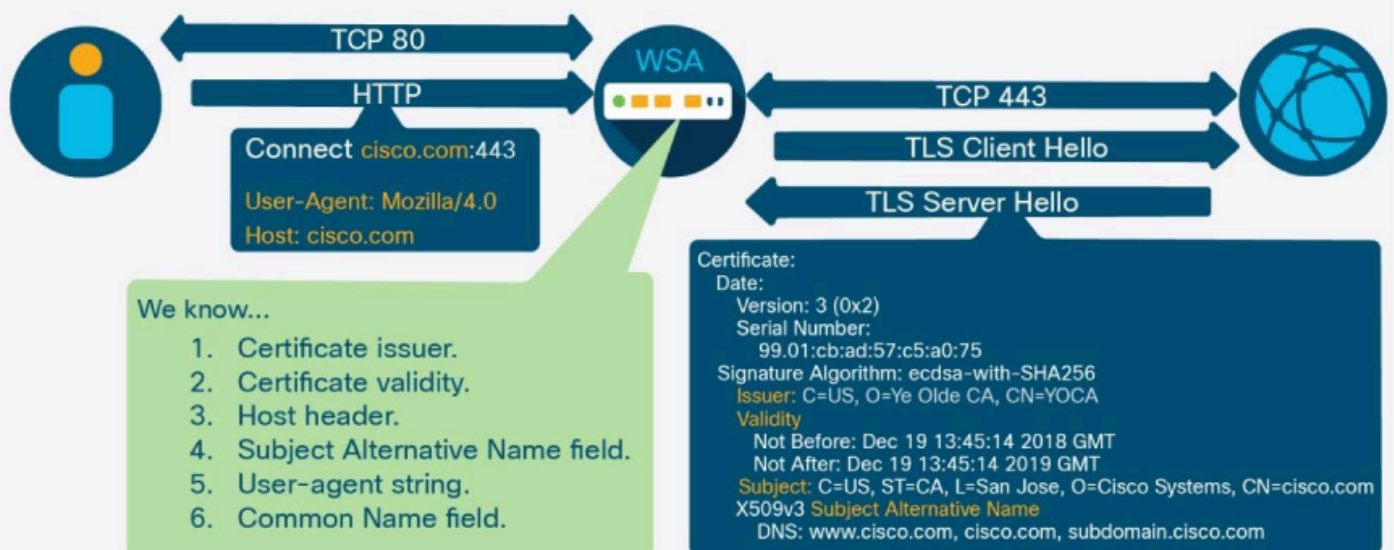
HTTPS policy operations

- **Drop**
 - Connection is closed.
- **Decrypt**
 - Traffic is decrypted and evaluated by access policies.
- **Passthrough**
 - Transaction is not decrypted.
 - Client negotiates directly with server.
- **Monitor**
 - No action taken.
 - Move to the next column on the policy.

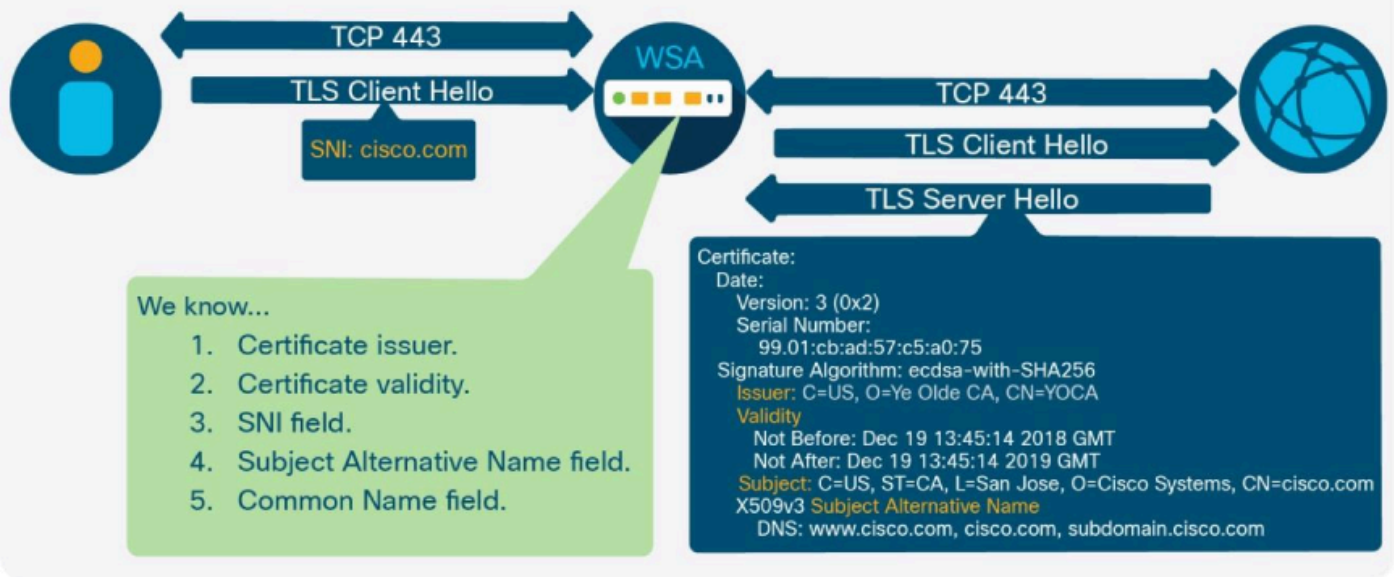
SWA가 TLS 핸드셰이크를 수행하지 않는 유일한 경우는 서버 이름 또는 IP 주소가 passthrough로 설정된 사용자 지정 범주에 있고 서버 이름이 HTTP CONNECT 또는 TLS Client Hello에서 사용 가능한 경우입니다. 명시적 시나리오에서 클라이언트는 TLS 세션 시작(호스트 헤더)에 앞서 서버의 호스트 이름을 프록시에 제공하므로 이 필드는 사용자 지정 범주에 대해 선택됩니다. 투명 구축에서 SWA는 TLS Client Hello 메시지의 Server Name Indication(SNI) 필드를 확인하고 사용자 지정 범주에 따라 평가합니다. 호스트 헤더 또는 SNI가 없는 경우, SWA는 인증서의 주체 대체 이름(SAN)과 공통 이름(CN) 필드를 순서대로 확인하기 위해 서버와 핸드셰이크를 계속해야 합니다.

이 동작이 정책 설계에 미치는 영향은 잘 알려져 있고 내부적으로 신뢰할 수 있는 서버를 결정하고 사용자 지정 범주 목록에서 통과하도록 설정함으로써 TLS 핸드셰이크 수를 줄일 수 있다는 것입니다. 웹 범주 및 평판 점수에 의존하지 않고 이 경우에도 SWA가 서버와 TLS 핸드셰이크를 완료해야 합니다. 그러나 이 경우 인증서 유효성 검사도 방지됩니다.

Explicit HTTPS-What do we know?



Transparent HTTPS-What do we know?



새로운 사이트가 웹에 나타나는 속도를 고려할 때, SWA에서 사용하는 웹 평판 및 분류 데이터베이스에 의해 분류되지 않은 사이트가 다수 발견될 가능성이 높습니다. 이는 사이트가 반드시 악의적일 가능성이 더 높다는 것을 의미하지는 않으며, 또한 이러한 모든 사이트는 여전히 AV 스캐닝, AMP 파일 평판 및 분석, 구성된 모든 객체 차단 또는 스캐닝의 대상이 됩니다. 이러한 이유로 인해 대부분의 상황에서 분류되지 않은 사이트를 삭제하는 것은 권장되지 않습니다. AV 엔진에서 암호 해독하고 검사하며 AVC, AMP, 액세스 정책 등으로 평가하도록 설정하는 것이 가장 좋습니다. 분류되지 않은 사이트에 대한 자세한 내용은 Access Policies(액세스 정책) 섹션을 참조하십시오.

액세스 정책

ID 프로필과 마찬가지로, 암호 해독 정책에 설정된 기준도 ISE의 정보가 사용될 때 한 가지 중요한 예외를 제외하고 논리적 AND로 평가됩니다. 다음은 구성된 요소(AD 그룹, 사용자 또는 SGT)에 따라 정책 일치 동작에 대해 설명합니다.

- AD 그룹 및 사용자 - 이전 동작에 대한 변경 사항이 없습니다. 사용자가 그룹의 멤버이거나 사용자가 정책에 지정된 경우 정책이 일치합니다.
- SGT 및 AD 그룹 및 사용자 - 사용자가 SGT와 연결되고 AD 그룹의 멤버이거나 사용자가 정책에 지정된 경우 정책이 일치됩니다.
- SGT and users(SGT 및 사용자) - 사용자가 SGT와 연결되거나 사용자가 정책에 지정된 경우 정책이 일치됩니다.

HTTP 트래픽은 인증된 직후 액세스 정책과 비교하여 평가됩니다. HTTPS 트래픽은 인증된 후 평가되며, 일치하는 암호 해독 정책에 따라 암호 해독 작업이 적용되는 경우 평가됩니다. 해독된 요청의 경우 access_log 항목이 2개 있습니다. 첫 번째 로그 항목은 초기 TLS 연결(암호 해독)에 적용된 작업을 표시하고, 두 번째 로그 항목은 액세스 정책이 암호 해독된 HTTP 요청에 적용한 작업을 표시합니다.

웹 프록시 섹션에서 설명한 것처럼 범위 요청 헤더는 파일의 특정 바이트 범위를 요청하는 데 사용되며 일반적으로 OS 및 애플리케이션 업데이트 서비스에서 사용됩니다. SWA는 기본적으로 아웃

바운드 요청에서 이러한 헤더를 제거합니다. 전체 파일이 없으면 악성코드 스캐닝을 수행하거나 AVC 기능을 활용할 수 없기 때문입니다. 네트워크의 많은 호스트가 업데이트를 검색하기 위해 작은 바이트 범위를 자주 요청하는 경우, 이는 SWA가 전체 파일을 동시에 여러 번 다운로드하도록 트리거할 수 있습니다. 따라서 사용 가능한 인터넷 대역폭이 빠르게 소진되고 서비스 중단이 발생할 수 있습니다. 이 실패 시나리오의 가장 일반적인 원인은 Microsoft Windows 업데이트 및 Adobe 소프트웨어 업데이트 데몬입니다.

이를 완화하려면 SWA를 중심으로 이 트래픽을 모두 전달하는 것이 가장 좋은 방법입니다. 이는 투명하게 구축된 환경에서 항상 실행 가능한 것은 아니며, 이러한 경우 차선책은 트래픽에 대한 전용 액세스 정책을 생성하고 이러한 정책에서 범위 요청 헤더 전달을 활성화하는 것입니다. 이러한 요청에 대해서는 AV 스캐닝 및 AVC가 가능하지 않은 것으로 간주되어야 하며, 따라서 정책은 의도한 트래픽만을 대상으로 하도록 신중하게 설계되어야 합니다. 대개 이를 수행하는 가장 좋은 방법은 요청 헤더에 있는 사용자 에이전트 문자열을 확인하는 것입니다. 일반 업데이트 데몬의 사용자 에이전트 문자열은 온라인으로 찾을 수 있으며, 관리자가 요청을 캡처하여 검사할 수도 있습니다. Microsoft Windows 및 Adobe 소프트웨어 업데이트를 포함한 대부분의 업데이트 서비스는 HTTPS를 사용하지 않습니다.

Decryption Policies(해독 정책) 섹션에서 설명한 것처럼, 해독 정책에서 분류되지 않은 사이트를 삭제하는 것은 권장되지 않습니다. 동일한 이유로 액세스 정책에서 이를 차단하지 않는 것이 좋습니다. DCA(Dynamic Content Analysis) 엔진은 URL 데이터베이스 조회를 통해 분류되지 않은 것으로 표시될 수 있는 분류된 사이트에 대해 지정된 사이트의 콘텐츠와 기타 휴리스틱 데이터를 사용할 수 있습니다. 이 기능을 활성화하면 SWA에서 분류되지 않은 판정의 수가 줄어듭니다.

액세스 정책의 Object Scanning(개체 검사) 설정은 여러 유형의 아카이브 파일을 검사할 수 있는 기능을 제공합니다. 네트워크가 애플리케이션 업데이트의 일환으로 아카이브 파일을 정기적으로 다운로드하는 경우, 아카이브 파일 검사를 활성화하면 CPU 사용량이 크게 증가할 수 있습니다. 이 트래픽은 모든 아카이브 파일을 검사하려는 경우 미리 식별해야 하며 면제되어야 합니다. 이 트래픽을 식별하기 위해 가능한 방법을 조사하는 첫 번째 위치는 사용자 에이전트 문자열입니다. 이렇게 하면 유지 관리가 번거로워질 수 있는 IP 허용 목록을 피할 수 있습니다.

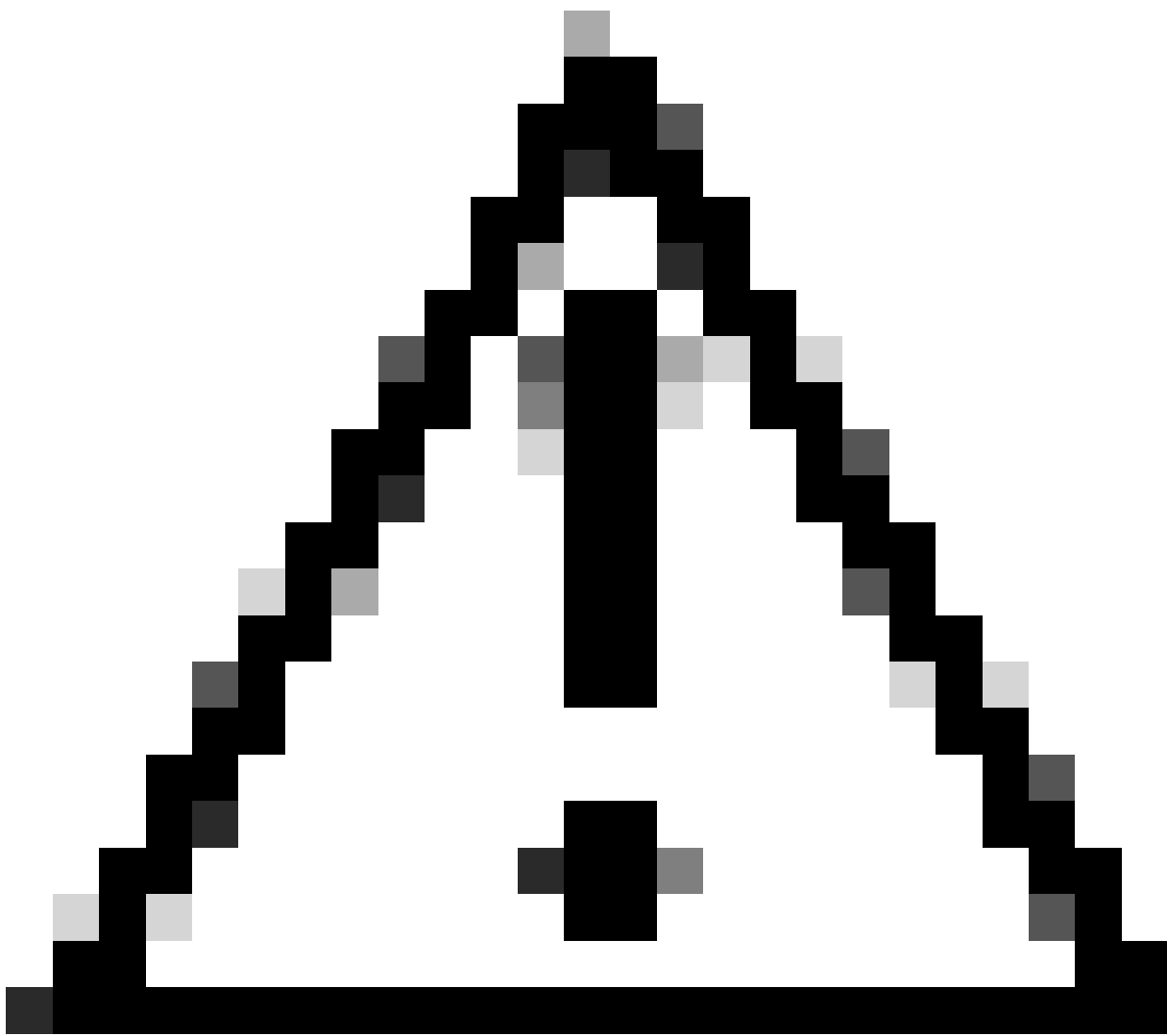
맞춤형 및 외부 URL 범주

Custom(맞춤형) 범주 목록은 IP 주소 또는 호스트 이름으로 서버를 식별하는 데 사용됩니다. 정규식(regex)을 사용하여 서버 이름을 확인할 수 있는 패턴을 지정할 수 있습니다. regex 패턴을 사용하여 서버 이름을 일치시키는 것은 하위 문자열 일치를 사용하는 것보다 훨씬 리소스가 많이 소모되므로 반드시 필요한 경우에만 사용해야 합니다. regex를 사용하지 않고 하위 도메인과 일치시키기 위해 도메인 이름의 시작 부분에 "."를 추가할 수 있습니다. 예를 들어 ".cisco.com"은 "www.cisco.com"과도 [일치합니다](#).

복잡성 섹션에서 설명한 것처럼, 낮은 복잡성은 10개의 사용자 지정 범주 목록으로, 중간 복잡성은 20개로, 높은 복잡성은 30개로 정의됩니다. 특히 목록에서 regex 패턴을 사용하거나 항목이 많은 경우 이 숫자를 20보다 작게 유지하는 것이 좋습니다. 각 유형에 대한 항목 수에 대한 자세한 내용은 액세스 정책 섹션을 참조하십시오.

외부 URL 피드는 정적 사용자 지정 범주 목록보다 훨씬 유연하며, 관리자가 수동으로 URL을 유지 관리할 필요가 없기 때문에 이를 활용하면 보안에 직접적인 영향을 줄 수 있습니다. 이 기능은 SWA 관리자가 유지 관리하거나 제어하지 않는 목록을 검색하는 데 사용할 수 있으므로 다운로드한 주소에 대한 개별 예외를 추가하는 기능은 AsyncOS 버전 11.8에 추가되었습니다.

Office365 API는 일반적으로 배포되는 이 서비스에 대한 정책 결정을 내리는 데 특히 유용하며 개별 응용 프로그램(PowerPoint, Skype, Word 등)에 사용할 수 있습니다. Microsoft에서는 성능을 최적화하기 위해 모든 Office365 트래픽에 대해 프록시를 우회할 것을 권장합니다. Microsoft 문서에는 다음과 같은 내용이 있습니다.



주의: "SSL Break and Inspect는 가장 큰 레이턴시를 생성하지만 프록시 인증 및 평판 조회와 같은 다른 서비스는 성능 저하 및 사용자 경험 저하를 초래할 수 있습니다. 또한 이러한 경계 네트워크 디바이스에는 모든 네트워크 연결 요청을 처리할 수 있는 충분한 용량이 필요합니다. 직접 Office 365 네트워크 요청에 대해서는 프록시 또는 검사 장치를 우회하는 것이 좋습니다." - <https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide>

투명한 프록시 환경에서 이 지침을 사용하는 것은 어려울 수 있습니다. AsyncOS 버전 11.8부터는 Office365 API에서 검색된 동적 범주 목록을 사용하여 우회 설정 목록을 채울 수 있습니다. 이 목록은 직접 라우팅을 위해 투명하게 리디렉션된 트래픽을 WCCP 디바이스로 다시 전송하는 데 사용됩니다.

모든 Office365 트래픽을 우회하면 이 트래픽에 대한 몇 가지 기본 보안 제어 및 보고 기능이 필요한 관리자에게 사각지대가 발생합니다. Office365 트래픽이 SWA에서 우회되지 않는 경우 발생할 수 있는 구체적인 기술적 문제를 이해하는 것이 중요합니다. 그중 하나는 애플리케이션에 필요한 연결 수입니다. Office365 응용 프로그램에 필요한 추가적인 영구 TCP 연결을 수용하려면 크기를 적절하게 조정해야 합니다. 이렇게 하면 사용자당 10개에서 15개의 영구 TCP 세션이 증가하여 총 연결 수가 증가할 수 있습니다.

HTTPS 프록시에서 수행하는 해독 및 재암호화 작업은 연결에 적은 레이턴시를 초래합니다. Office365 응용 프로그램은 레이턴시에 매우 민감할 수 있으며, 느린 WAN 연결 및 분산된 지리적 위치와 같은 다른 요인으로 인해 이러한 문제가 심화될 경우 사용자 환경이 악화될 수 있습니다.

일부 Office365 응용 프로그램에서는 HTTPS 프록시가 응용 프로그램 서버와의 핸드셰이크를 완료하지 못하도록 독점적인 TLS 매개 변수를 사용합니다. 이는 인증서를 검증하거나 호스트 이름을 검색하는 데 필요합니다. TLS 클라이언트 Hello 메시지에서 SNI(Server Name Indication) 필드를 전송하지 않는 비즈니스용 Skype와 같은 애플리케이션과 이를 결합하면 이 트래픽을 완전히 우회해야 합니다. AsyncOS 11.8에서는 이 시나리오를 해결하기 위해 인증서 확인 없이 목적지 IP 주소만을 기반으로 트래픽을 우회하는 기능을 도입했습니다.

모니터링 및 알림

CLI 모니터

SWA CLI는 중요한 프로세스의 실시간 모니터링을 위한 명령을 제공합니다. prox 프로세스와 관련된 통계를 표시하는 명령이 가장 유용합니다. status detail 명령은 가동 시간, 사용된 대역폭, 응답 대기 시간, 연결 수 등을 비롯한 리소스 사용량 및 성능 메트릭을 요약할 수 있는 좋은 소스입니다. 다음은 이 명령의 출력 예입니다.

```
SWA_CLI> status detail
```

```
Status as of:                Fri Nov 11 14:06:52 2022 +03
Up since:                  Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                       3.3%
  RAM                       6.2%
  Reporting/Logging Disk    45.6%
Transactions per Second:
  Average in last minute    55
  Maximum in last hour      201
  Average in last hour      65
  Maximum since proxy restart 1031
  Average since proxy restart 51
```

```

Bandwidth (Mbps):
  Average in last minute      4.676
  Maximum in last hour       327.258
  Average in last hour       10.845
  Maximum since proxy restart 1581.297
  Average since proxy restart 11.167
Response Time (ms):
  Average in last minute      635
  Maximum in last hour       376209
  Average in last hour       605
  Maximum since proxy restart 2602943
  Average since proxy restart 701
Cache Hit Rate:
  Average in last minute      0
  Maximum in last hour       2
  Average in last hour       0
  Maximum since proxy restart 15
  Average since proxy restart 0
Connections:
  Idle client connections     186
  Idle server connections     184
  Total client connections    3499
  Total server connections    3632
SSLJobs:
  In queue Avg in last minute 4
  Average in last minute     45214
  SSLInfo Average in last min 94
Network Events:
  Average in last minute     0.0
  Maximum in last minute     35
  Network events in last min 124502

```

rate 명령은 prox 프로세스에서 사용하는 CPU 백분율에 대한 실시간 정보와 RPS(초당 요청 수) 및 캐시 통계를 표시합니다. 이 명령은 중단될 때까지 계속해서 새 출력을 폴링하고 표시합니다. 다음은 이 명령의 출력 예입니다.

```
SWA_CLI> rate
```

Press Ctrl-C to stop.

%proxy CPU	reqs /sec	hits	blocks	misses	client kb/sec	server kb/sec	%bw saved	disk wrs	disk rds
5.00	51	1	147	370	2283	2268	0.6	48	37
4.00	36	0	128	237	21695	21687	0.0	47	38
4.00	48	2	179	307	8168	8154	0.2	65	33
5.00	53	0	161	372	2894	2880	0.5	48	32
6.00	52	0	198	328	15110	15100	0.1	63	33
6.00	77	0	415	363	4695	4684	0.2	48	34
7.00	85	1	417	433	5270	5251	0.4	49	35
7.00	67	1	443	228	2242	2232	0.5	85	44

tcpsservices 명령은 선택한 프로세스 수신 대기 포트에 대한 정보를 표시합니다. 각 프로세스 및 주소와 포트 조합에 대한 설명도 표시됩니다.

SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)

- ftpd.main - The FTP daemon
- ginetd - The INET daemon
- interface - The interface controller for inter-process communication
- ipfw - The IP firewall
- slapd - The Standalone LDAP daemon
- sntpd - The SNTP daemon
- sshd - The SSH daemon
- syslogd - The system logging daemon
- winbindd - The Samba Name Service Switch daemon

Feature Processes

- coeuslogd - Main WSA controller
- gui - GUI process
- hermes - Mail server for sending alerts, etc.
- java - Processes for storing and querying Web Tracking data
- musd - AnyConnect Secure Mobility server
- pacd - PAC file hosting daemon
- prox - WSA proxy
- trafmon - L4 Traffic Monitor
- uds - User Discovery System (Transparent Auth)
- wccpd - WCCP daemon

COMMAND	USER	TYPE	NODE	NAME
connector	root	IPv4	TCP	127.0.0.1:8823
java	root	IPv6	TCP	:::127.0.0.1]:18081
hybridd	root	IPv4	TCP	127.0.0.1:8833
gui	root	IPv4	TCP	172.16.40.80:8443
ginetd	root	IPv4	TCP	172.16.40.80:ssh
nginx	root	IPv6	TCP	*:4431
nginx	root	IPv4	TCP	127.0.0.1:8843
nginx	nobody	IPv6	TCP	*:4431
nginx	nobody	IPv4	TCP	127.0.0.1:8843
nginx	nobody	IPv6	TCP	*:4431
nginx	nobody	IPv4	TCP	127.0.0.1:8843
api_serve	root	IPv4	TCP	172.16.40.80:6080
api_serve	root	IPv4	TCP	127.0.0.1:60001
api_serve	root	IPv4	TCP	172.16.40.80:6443
chimera	root	IPv4	TCP	127.0.0.1:6380
nectar	root	IPv4	TCP	127.0.0.1:6382
redis-ser	root	IPv4	TCP	127.0.0.1:6383
redis-ser	root	IPv4	TCP	127.0.0.1:6379
prox	root	IPv4	TCP	127.0.0.1:http
prox	root	IPv6	TCP	:::1]:http
prox	root	IPv4	TCP	172.16.11.69:http
prox	root	IPv4	TCP	172.16.11.68:http
prox	root	IPv4	TCP	172.16.11.252:http
prox	root	IPv4	TCP	127.0.0.1:3128
prox	root	IPv6	TCP	:::1]:3128
prox	root	IPv4	TCP	172.16.11.69:3128
prox	root	IPv4	TCP	172.16.11.68:3128
prox	root	IPv4	TCP	172.16.11.252:3128
prox	root	IPv4	TCP	127.0.0.1:https
prox	root	IPv6	TCP	:::1]:https
prox	root	IPv4	TCP	172.16.11.69:https
prox	root	IPv4	TCP	172.16.11.68:https
prox	root	IPv4	TCP	172.16.11.252:https
prox	root	IPv4	TCP	127.0.0.1:http
prox	root	IPv6	TCP	:::1]:http
prox	root	IPv4	TCP	172.16.11.69:http

prox	root	IPv4 TCP	172.16.11.68:http
prox	root	IPv4 TCP	172.16.11.252:http
prox	root	IPv4 TCP	127.0.0.1:3128
prox	root	IPv6 TCP	[::1]:3128
prox	root	IPv4 TCP	172.16.11.69:3128
prox	root	IPv4 TCP	172.16.11.68:3128
prox	root	IPv4 TCP	172.16.11.252:3128
prox	root	IPv4 TCP	127.0.0.1:https
prox	root	IPv6 TCP	[::1]:https
prox	root	IPv4 TCP	172.16.11.69:https
prox	root	IPv4 TCP	172.16.11.68:https
prox	root	IPv4 TCP	172.16.11.252:https
prox	root	IPv4 TCP	127.0.0.1:25255
prox	root	IPv4 TCP	127.0.0.1:socks
prox	root	IPv6 TCP	[::1]:socks
prox	root	IPv4 TCP	172.16.11.69:socks
prox	root	IPv4 TCP	172.16.11.68:socks
prox	root	IPv4 TCP	172.16.11.252:socks
prox	root	IPv4 TCP	127.0.0.1:ftp-proxy
prox	root	IPv6 TCP	[::1]:ftp-proxy
prox	root	IPv4 TCP	172.16.11.69:ftp-proxy
prox	root	IPv4 TCP	172.16.11.68:ftp-proxy
prox	root	IPv4 TCP	172.16.11.252:ftp-proxy
prox	root	IPv4 TCP	127.0.0.1:http
prox	root	IPv6 TCP	[::1]:http
prox	root	IPv4 TCP	172.16.11.69:http
prox	root	IPv4 TCP	172.16.11.68:http
prox	root	IPv4 TCP	172.16.11.252:http
prox	root	IPv4 TCP	127.0.0.1:3128
prox	root	IPv6 TCP	[::1]:3128
prox	root	IPv4 TCP	172.16.11.69:3128
prox	root	IPv4 TCP	172.16.11.68:3128
prox	root	IPv4 TCP	172.16.11.252:3128
prox	root	IPv4 TCP	127.0.0.1:https
prox	root	IPv6 TCP	[::1]:https
prox	root	IPv4 TCP	172.16.11.69:https
prox	root	IPv4 TCP	172.16.11.68:https
prox	root	IPv4 TCP	172.16.11.252:https
prox	root	IPv4 TCP	127.0.0.1:25256
prox	root	IPv4 TCP	127.0.0.1:http
prox	root	IPv6 TCP	[::1]:http
prox	root	IPv4 TCP	172.16.11.69:http
prox	root	IPv4 TCP	172.16.11.68:http
prox	root	IPv4 TCP	172.16.11.252:http
prox	root	IPv4 TCP	127.0.0.1:3128
prox	root	IPv6 TCP	[::1]:3128
prox	root	IPv4 TCP	172.16.11.69:3128
prox	root	IPv4 TCP	172.16.11.68:3128
prox	root	IPv4 TCP	172.16.11.252:3128
prox	root	IPv4 TCP	127.0.0.1:https
prox	root	IPv6 TCP	[::1]:https
prox	root	IPv4 TCP	172.21.11.69:https
prox	root	IPv4 TCP	172.21.11.68:https
prox	root	IPv4 TCP	172.21.11.252:https
prox	root	IPv4 TCP	127.0.0.1:25257
smart_age	root	IPv6 TCP	[::127.0.0.1]:65501
smart_age	root	IPv6 TCP	[::127.0.0.1]:28073
interface	root	IPv4 TCP	127.0.0.1:domain
stunnel	root	IPv4 TCP	127.0.0.1:32137

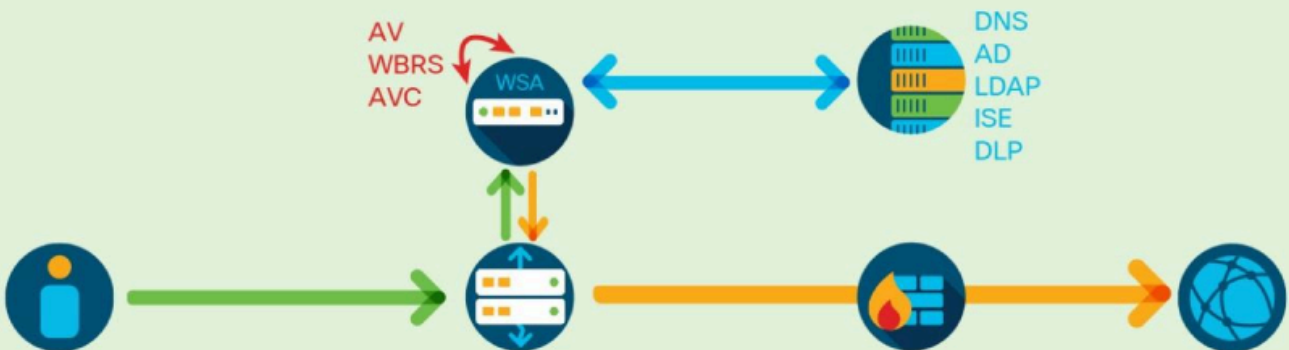
로깅

웹 트래픽은 매우 동적이고 다양합니다. 프록시 구축이 완료되면 어플라이언스를 통과하는 트래픽의 양과 구성을 정기적으로 재평가하는 것이 중요합니다. 크기가 초기 설치의 기대와 사양에 맞게 조정되도록 정기적으로(분기마다 한 번) 암호 해독된 트래픽의 백분율을 확인해야 합니다. 이 작업은 AWSR(Advanced Web Security Reporting)과 같은 로그 관리 제품이나 액세스 로그와 함께 간단한 Bash 또는 PowerShell 명령을 사용하여 수행할 수 있습니다. 또한 RPS 수를 정기적으로 재평가하여 고가용성, 로드 밸런싱 컨피그레이션에서 어플라이언스의 트래픽 급증 및 장애 조치 가능성을 고려할 수 있는 오버헤드가 충분한지 확인해야 합니다.

track_stats 로그는 5분마다 추가되며 prox 프로세스 및 메모리에 있는 해당 객체와 직접 관련된 몇 개의 출력 섹션을 포함합니다. 성능 모니터링에서 가장 유용한 섹션은 다양한 요청 프로세스에 대한 평균 대기 시간, DNS 조회 시간, AV 엔진 스캔 시간 및 더 많은 유용한 필드를 보여주는 섹션입니다. 이 로그는 GUI 또는 CLI에서 구성할 수 없으며 SCP(Secure Copy Protocol) 또는 FTP(File Transfer Protocol)를 통해서만 액세스할 수 있습니다. 이 로그는 성능 문제를 해결할 때 가장 중요한 로그이므로 자주 폴링해야 합니다.

Where can latency be introduced?

- Client Side
- External Services
- Internal Services
- Server Side



Client side latency

```

Client Time 1.0 ms 15575
Client Time 1.6 ms 185
Client Time 2.5 ms 855
Client Time 4.0 ms 573
Client Time 6.3 ms 180
Client Time 10.0 ms 264
Client Time 15.8 ms 580
Client Time 25.1 ms 924
Client Time 39.8 ms 1330
Client Time 63.1 ms 4936
Client Time 100.0 ms 5278
Client Time 159.5 ms 10
Client Time 251.2 ms 13
Client Time 398.1 ms 0
Client Time 631.0 ms 0
Client Time 1000.0 ms 0
Client Time 1584.9 ms 0
Client Time 2511.9 ms 0
Client Time 3981.1 ms 0
Client Time 6309.6 ms 30328
    
```

- “Client Time” in track_stats log.
- The amount of time in milliseconds that the client was waiting for a response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field % : 1 >

%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client
------	-----------------------	--



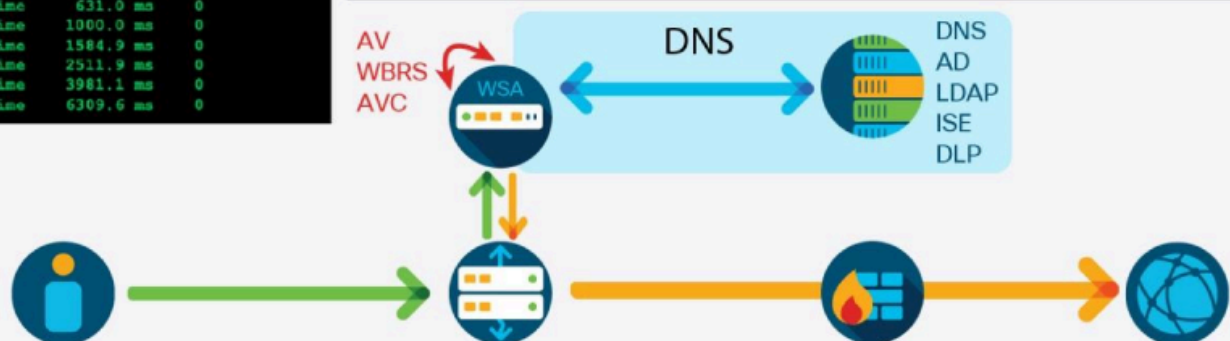
DNS latency

```

DNS Time 1.0 ms 51
DNS Time 1.6 ms 347
DNS Time 2.5 ms 152
DNS Time 4.0 ms 71
DNS Time 6.3 ms 98
DNS Time 10.0 ms 7
DNS Time 15.8 ms 11
DNS Time 25.1 ms 13
DNS Time 39.8 ms 2
DNS Time 63.1 ms 3
DNS Time 100.0 ms 7
DNS Time 159.5 ms 16
DNS Time 251.2 ms 4
DNS Time 398.1 ms 1
DNS Time 631.0 ms 0
DNS Time 1000.0 ms 0
DNS Time 1584.9 ms 0
DNS Time 2511.9 ms 0
DNS Time 3981.1 ms 0
DNS Time 6309.6 ms 0
    
```

- The amount of time in milliseconds that the WSA waited for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field % : >d

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS Process to send a DNS result to the Web proxy.
------	--------------------	--



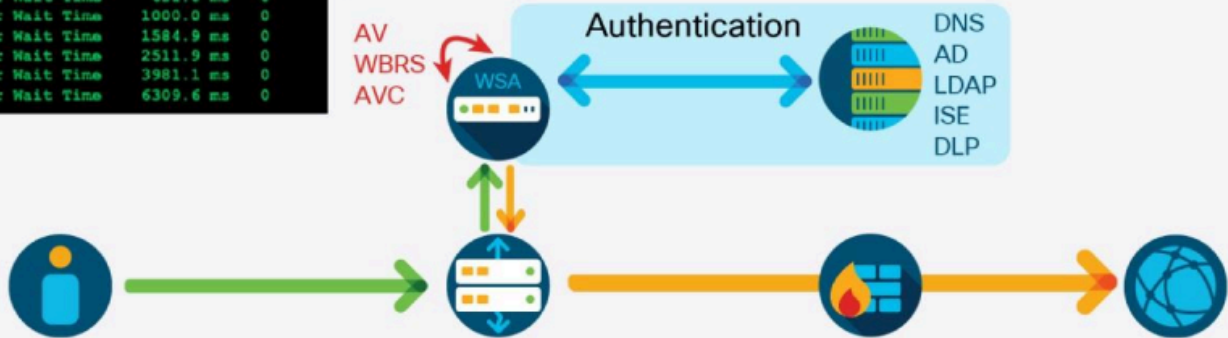
Authentication latency

```

Server Wait Time 1.0 ms 0
Server Wait Time 1.6 ms 0
Server Wait Time 2.5 ms 0
Server Wait Time 4.0 ms 0
Server Wait Time 6.3 ms 0
Server Wait Time 10.0 ms 0
Server Wait Time 15.8 ms 0
Server Wait Time 25.1 ms 0
Server Wait Time 39.8 ms 0
Server Wait Time 63.1 ms 0
Server Wait Time 100.0 ms 0
Server Wait Time 158.5 ms 1
Server Wait Time 251.2 ms 1
Server Wait Time 398.1 ms 0
Server Wait Time 631.0 ms 0
Server Wait Time 1000.0 ms 0
Server Wait Time 1584.9 ms 0
Server Wait Time 2511.9 ms 0
Server Wait Time 3981.1 ms 0
Server Wait Time 6309.6 ms 0
    
```

- There are two metrics: “Auth Helper Wait Time” and “Auth Helper Service Wait Time.”
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field % : >a

%;<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.
------	----------------------	--



Server latency-wait time

```

Server Wait Time 1.0 ms 0
Server Wait Time 1.6 ms 0
Server Wait Time 2.5 ms 0
Server Wait Time 4.0 ms 0
Server Wait Time 6.3 ms 0
Server Wait Time 10.0 ms 0
Server Wait Time 15.8 ms 0
Server Wait Time 25.1 ms 0
Server Wait Time 39.8 ms 0
Server Wait Time 63.1 ms 0
Server Wait Time 100.0 ms 0
Server Wait Time 158.5 ms 1
Server Wait Time 251.2 ms 1
Server Wait Time 398.1 ms 0
Server Wait Time 631.0 ms 0
Server Wait Time 1000.0 ms 0
Server Wait Time 1584.9 ms 0
Server Wait Time 2511.9 ms 0
Server Wait Time 3981.1 ms 0
Server Wait Time 6309.6 ms 0
    
```

- The amount of time in milliseconds that the WSA waited for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field % : >1

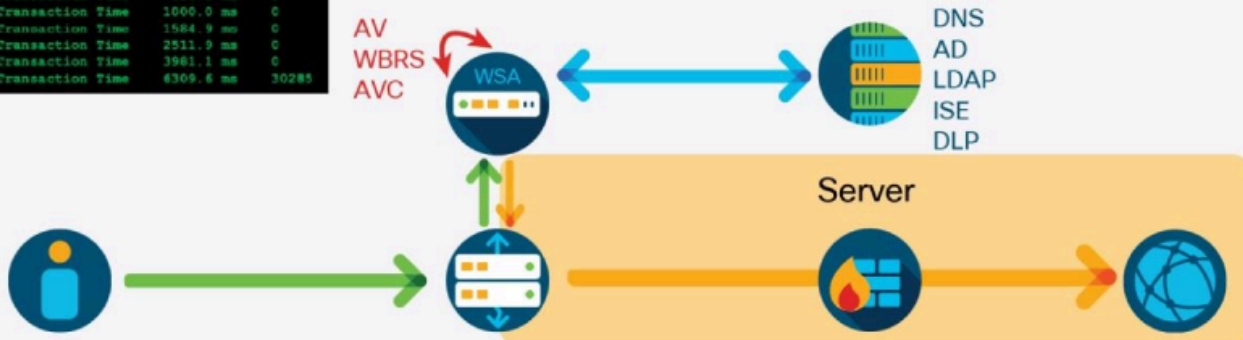
%;>1	x-s2p-first-byte-time	Wait-time for first response byte from server
------	-----------------------	---



Server latency-transaction time

Server Transaction Time	1.0 ms	1422
Server Transaction Time	1.6 ms	858
Server Transaction Time	2.5 ms	1835
Server Transaction Time	4.0 ms	1106
Server Transaction Time	6.3 ms	758
Server Transaction Time	10.0 ms	810
Server Transaction Time	15.8 ms	788
Server Transaction Time	25.1 ms	45
Server Transaction Time	39.8 ms	73
Server Transaction Time	63.1 ms	4221
Server Transaction Time	100.0 ms	8897
Server Transaction Time	156.5 ms	3
Server Transaction Time	251.2 ms	0
Server Transaction Time	398.1 ms	2
Server Transaction Time	631.0 ms	0
Server Transaction Time	1000.0 ms	0
Server Transaction Time	1584.9 ms	0
Server Transaction Time	2511.9 ms	0
Server Transaction Time	3961.1 ms	0
Server Transaction Time	4309.6 ms	30285

- The amount of time in milliseconds for the entire server-side transaction to complete.
- Calls for investigation of your upstream devices and WAN connection.
- No **access logs** custom field, but can be determined by a combination of them.



Internal services latency-not exhaustive

Sophos Response Body Service Time	10.0 ms	0	Adaptive Scanning Service Time	1.0 ms	2
Sophos Response Body Service Time	17.3 ms	0	Adaptive Scanning Service Time	1.6 ms	0
Sophos Response Body Service Time	30.0 ms	0	Adaptive Scanning Service Time	2.5 ms	0
Sophos Response Body Service Time	52.1 ms	0	Adaptive Scanning Service Time	4.0 ms	0
Sophos Response Body Service Time	90.3 ms	0	Adaptive Scanning Service Time	6.3 ms	0
Sophos Response Body Service Time	156.5 ms	0	Adaptive Scanning Service Time	10.0 ms	0
McAfee Response Body Service Time	10.0 ms	0	AVC Header Scan Service Time	10.0 ms	8398
McAfee Response Body Service Time	17.3 ms	0	AVC Header Scan Service Time	17.3 ms	11
McAfee Response Body Service Time	30.0 ms	0	AVC Header Scan Service Time	30.0 ms	3
McAfee Response Body Service Time	52.1 ms	0	AVC Header Scan Service Time	52.1 ms	0
McAfee Response Body Service Time	90.3 ms	0	AVC Header Scan Service Time	90.3 ms	0
McAfee Response Body Service Time	156.5 ms	0	AVC Header Scan Service Time	156.5 ms	0
Webroot Response Body Service Time	10.0 ms	0	Ironport Data Security Service Time	10.0 ms	0
Webroot Response Body Service Time	14.6 ms	0	Ironport Data Security Service Time	17.3 ms	0
Webroot Response Body Service Time	21.4 ms	0	Ironport Data Security Service Time	30.0 ms	0
Webroot Response Body Service Time	31.3 ms	0	Ironport Data Security Service Time	52.1 ms	0
Webroot Response Body Service Time	45.7 ms	0	Ironport Data Security Service Time	90.3 ms	0
Webroot Response Body Service Time	66.9 ms	0	Ironport Data Security Service Time	156.5 ms	0
WBRS Service Time	1.0 ms	3917	<p>See the user guide for all custom fields associated with these values.</p>		
WBRS Service Time	1.6 ms	198			
WBRS Service Time	2.5 ms	60			
WBRS Service Time	4.0 ms	16			
WBRS Service Time	6.3 ms	6			



개별 SHD 로그 라인은 60초마다 기록되며 지연, RPS, 총 클라이언트 및 서버 측 연결을 포함하여 성능 모니터링에 중요한 많은 필드가 포함되어 있습니다. 다음은 SHD 로그 라인의 예입니다.

```

Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 79
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 140
    
```

```
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

개별 요청에 대한 레이턴시 정보를 나타내는 추가 사용자 지정 필드를 access_logs에 추가할 수 있습니다. 이러한 필드에는 서버 응답, DNS 확인 및 AV 스캐너 레이턴시가 포함됩니다. 문제 해결에 사용할 중요한 정보를 수집하려면 필드를 로그에 추가해야 합니다. 다음은 권장되는 사용자 지정 필드 문자열입니다.

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,
```

```
a; DNS response = %:
```

```
d, WBRs response = %:
```

```
r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respon
```

```
s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k
```

이 값에서 파생된 성능 정보는 다음과 같습니다.

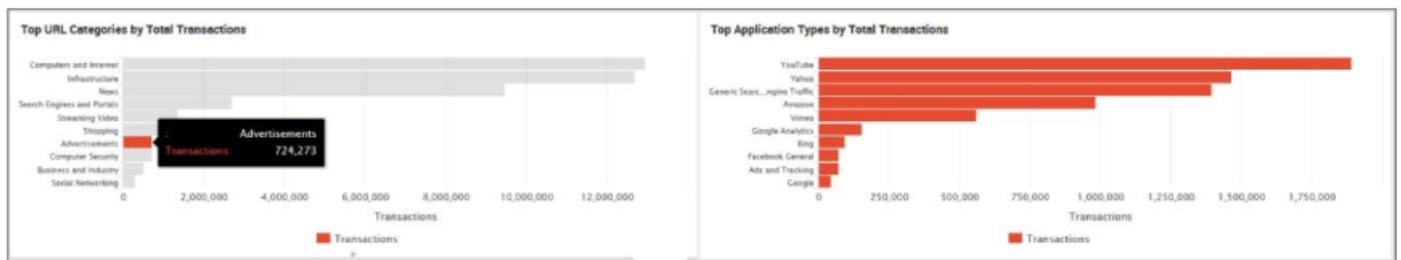
사용자 지정 필드	설명
%:<a	웹 프록시가 요청을 전송한 후 웹 프록시 인증 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:<b	헤더 후 요청 본문을 서버에 쓸 때까지 기다리는 시간.
%:<d	웹 프록시가 요청을 전송한 후 웹 프록시 DNS 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:<h	첫 번째 바이트 이후 요청 헤더를 서버에 쓰는 데 걸리는 대기 시간입니다.
%:<r	웹 프록시가 요청을 전송한 후 웹 평판 필터에서 응답을 수신할 때까지 대기하는 시간.
%:<s	웹 프록시에서 요청을 보낸 후 웹 프록시 안티스파이웨어 프로세스에서 판정을 수신할 때까지 대기하는 시간.
%:>	서버의 첫 번째 응답 바이트에 대한 대기 시간입니다.
%:>a	웹 프록시 인증 프로세스로부터 응답을 수신할 때까지 대기하는 시간. 웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함합니다.
%:>b	헤더를 수신한 후 전체 응답 본문을 기다리는 시간.
%:>c	웹 프록시가 디스크 캐시에서 응답을 읽는 데 필요한 시간입니다.
%:>d	웹 프록시 DNS 프로세스에서 응답을 수신할 때까지 대기하는 시간. 웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함합니다.
%:>h	첫 번째 응답 바이트 이후 서버 헤더의 대기 시간입니다.
%:>r	웹 평판 필터에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다.
%:>s	웹 프록시 안티스파이웨어 프로세스에서 판정을 수신할 때까지 대기하는 시간. 여기에는 웹 프록시가 요청을 전송하는 데 필요한 시간이 포함됩니다.
%:1<	새 클라이언트 연결에서 첫 번째 요청 바이트에 대한 대기 시간입니다.
%:1>	첫 번째 바이트가 클라이언트에 기록될 때까지 기다리는 시간입니다.
%:b<	전체 클라이언트 본문을 기다리는 시간입니다.
%:b>	클라이언트에 전체 본문이 쓰여질 때까지 기다리는 시간입니다.
%:e>	웹 프록시에서 요청을 전송한 후 AMP 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.
%:e<	AMP 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다.
%:h<	첫 번째 바이트 이후 전체 클라이언트 헤더를 기다리는 시간.
%:h>	클라이언트에 작성된 전체 헤더를 기다리는 시간입니다.
%:m<	McAfee 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간에는 웹 프록시에서 요청을 전송하는 데 필요한 시간이 포함됩니다.

%:m>	웹 프록시에서 요청을 전송한 후 McAfee 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.
%F	클라이언트 소스 포트.
%p	웹 서버 포트.
%k	데이터 원본 IP 주소(웹 서버 IP 주소)
%:w<	Webroot 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간(웹 프록시에서 요청을 전송하는 데 필요한 시간 포함)입니다.
%:w>	웹 프록시가 요청을 전송한 후 Webroot 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.

SWA 라이선싱 모델에서는 가상 어플라이언스에 물리적 어플라이언스 라이선스를 재사용할 수 있습니다. 이를 활용하여 랩 환경에서 사용할 테스트 SWAv 어플라이언스를 구축할 수 있습니다. 새로운 기능 및 구성은 라이선싱 조건을 위반하지 않으면서 안정성과 신뢰성을 보장하기 위해 이러한 방식으로 시범 적용될 수 있습니다.

AWSR(Advanced Web Security Reporting)

SWA의 보고 데이터를 최대한 활용하려면 AWSR을 활용해야 합니다. 특히 많은 SWA가 구축된 환경에서 이 솔루션은 SMA(Security Management Appliance)에서 중앙 집중식 보고 기능을 활용하는 것보다 확장성이 훨씬 뛰어나며 데이터에 엄청난 깊이와 사용자 지정 기능을 추가하는 사용자 지정 보고 특성을 제공합니다. 모든 조직의 필요에 맞게 보고서를 그룹화하고 사용자 지정할 수 있습니다. Cisco Advanced Services 그룹은 AWSR의 크기 조정에 활용해야 합니다.



이메일 알림

SWA에 내장된 이메일 알림 시스템은 기본 알림 시스템으로 활용되는 것이 가장 좋습니다. 모든 정보 이벤트가 활성화된 경우 매우 시끄러울 수 있으므로 관리자의 요구를 충족하기 위해 적절하게 조정해야 합니다. 모든 것을 알리고 스팸으로 무시하는 것보다 알림을 제한하고 능동적으로 모니터링하는 것이 더 중요합니다.

경고 설정	설정
경보를 전송할 때 사용할 발신 주소	자동 생성
중복 알림을 전송하기 전 초기 대기 시간(초)	300초
중복 알림을 전송하기 전 최대 대기 시간(초)	3600초

가용성 모니터링

웹 프록시의 가용성을 모니터링하는 데 사용할 수 있는 두 가지 방법이 있습니다.

1. 첫 번째는 L3(Layer 3) 모니터링으로, 어플라이언스 IP 주소가 네트워크에 연결 가능한지 테스트합니다. 이를 테스트하는 가장 간단한 방법은 일정한 간격으로 주소에 ICMP 에코(ping) 요청을 보내고 응답 패킷을 확인하는 것입니다. TTL 및 레이턴시와 같은 응답의 특성을 구분 분석하여 네트워크 레이어의 상태를 확인할 수 있습니다.
2. 디바이스가 ping에 응답할 수 있지만 프록시 프로세스가 응답하지 않거나 간헐적일 수 있습니다. 따라서 어플라이언스에 명시적 프록시 요청을 보내고 200 OK HTTP 응답 코드를 예상하는 L7(Layer 7) 모니터를 사용하는 것이 좋습니다. 이는 네트워크 인터페이스의 연결성뿐만 아니라 프록시 서비스의 응답성과 외부 리소스가 요청될 경우 업스트림 서비스의 실행 가능성을 테스트합니다. 이러한 유형의 모니터링은 일반적으로 프록시에 리소스에 연결하라는 명시적 HTTP HEAD 요청 형식을 취합니다. HEAD 메서드는 반환될 헤더를 요청하지만, 클라이언트가 GET 요청을 전송해야 하지만 응답 헤더만 포함하고 데이터는 포함하지 않습니다.
 - L7 모니터링 툴 또는 스크립트를 사용할 경우 트래픽이 인증에서 제외되도록 하는 것이 중요합니다. 그렇지 않으면 정기적인 인증 실패 및 리소스 소비가 발생합니다. 모니터링 툴에서 사용자 지정 user-agent 문자열을 사용하는 경우 트래픽을 식별하기 위해 사용해야 합니다. 트래픽이 인증에서 제외되더라도 액세스 정책을 통해 불필요한 인터넷 액세스에서 여전히 제한될 수 있습니다.

이러한 방법 중 하나 이상을 사용하는 경우 관리자는 프록시 응답 주변에서 허용 가능한 측정 단위의 기준을 설정하고 이를 사용하여 경고 임계값을 작성해야 합니다. 이러한 검사의 응답을 수집하는 데 시간을 할애해야 하며 임계값 및 알림을 구성하는 방법을 결정하기 전에 시간을 할애해야 합니다.

SNMP 모니터링

SNMP(Simple Network Management Protocol)는 어플라이언스의 상태를 모니터링하기 위한 기본 방법입니다. 어플라이언스(트랩)에서 알림을 수신하거나 다양한 OID(Object Identifier)를 폴링하여 정보를 수집하는 데 사용할 수 있습니다. SWA에는 하드웨어에서 리소스 사용량, 개별 프로세스 정보 및 요청 통계에 이르는 모든 것을 포괄하는 많은 OID가 있습니다.

하드웨어 및 성능 관련 이유로 모두 모니터링해야 하는 여러 특정 MIB(Machine Information Base)가 있습니다. MIB의 전체 목록은 <https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt>에서 확인할 수 있습니다.

다음은 전체 목록이 아니라 모니터링해야 할 권장 MIB 목록입니다.

하드웨어 OID	이름
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raid상태
1.3.6.1.4.1.15497.1.1.1.18.1.4	raid마지막 오류
1.3.6.1.4.1.15497.1.1.1.10	팬 테이블
1.3.6.1.4.1.15497.1.1.1.9.1.2	섭씨 온도

OID는 status detail CLI 명령의 출력에 직접 매핑됩니다.

OID	이름	상태 세부사항 필드
시스템 리소스		
1.3.6.1.4.1.15497.1.1.1.2.0	PerCentCPU사용화	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	perCentMemory사용률	램
초당 트랜잭션		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	캐시처리	최근 1분 동안의 초당 평균 트랜잭션입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	지난 1시간 동안의 초당 최대 트랜잭션 수입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hr평균	지난 1시간 동안의 초당 평균 트랜잭션입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	프록시 재시작 이후 초당 최대 트랜잭션 수입니다.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	프록시 재시작 이후 초당 평균 트랜잭션 수입니다.
Bandwidth		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	캐시현재 너비	지난 1분 동안의 평균 대역폭.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	지난 1시간 동안의 최대 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hr평균	지난 1시간의 평균 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	캐시너비TotalLifePeak	프록시 재시작 이후 최대 대역폭입니다.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	캐시너비 총 수명 평균	프록시 재시작 이후의 평균 대역폭입니다.
응답 시간		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	캐시 적중률	마지막 순간에 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hr최대	지난 1시간 동안의 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hr평균	지난 1시간의 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	캐시적중수명의	프록시 재시작 이후 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	캐시 적중수명 평균	프록시 재시작 이후의 평균 캐시 적중률입니다.
캐시 적중률		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	캐시 적중률	마지막 순간에 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hr최대	지난 1시간 동안의 최대 캐시 적중률입니다.

1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hr평균	지난 1시간의 평균 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	캐시적중수명의	프록시 재시작 이후 최대 캐시 적중률입니다.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	캐시 적중수명 평균	프록시 재시작 이후의 평균 캐시 적중률입니다.
연결		
1.3.6.1.4.1.15497.1.2.3.2.7.0	캐시클라이언트유휴 통화	유휴 클라이언트 연결
1.3.6.1.4.1.15497.1.2.3.3.7.0	캐시서버유휴 연결	유휴 서버 연결.
1.3.6.1.4.1.15497.1.2.3.2.8.0	캐시클라이언트총연결	총 클라이언트 연결 수
1.3.6.1.4.1.15497.1.2.3.3.8.0	캐시서버총연결	총 서버 연결 수

결론

이 가이드에서는 SWA 컨피그레이션, 구축 및 모니터링의 가장 중요한 측면에 대해 설명합니다. 참조 가이드로서, SWA의 가장 효과적인 사용을 보장하고자 하는 사람에게 유용한 정보를 제공하는 것이 목표입니다. 여기에 설명된 모범 사례는 보안 툴로서 디바이스의 안정성, 확장성 및 효율성에 중요합니다. 또한 관련 리소스가 계속 사용되므로 네트워크 환경 및 제품 기능 집합의 변경 사항을 반영하기 위해 자주 업데이트해야 합니다.

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.