# Web Security Appliance 실습 v1

최종 업데이트: 2017년 4월 28일

## 실습 정보

본 실습은 참가자가 Web Security Appliance를 구축하는 방법을 이해하고 ASyncOS v10.1의 최신 기능 집합을 살펴보는 데 도움을 주기 위해 설계되었습니다. 본 실습은 Cisco Web Security Appliance의 다양한 기능을 제어하는 정책의 컨피그레이션, 관리 및 보고에 대해 다룹니다. 연습 문제에서는 가장 일반적인 컨피그레이션, 문제 해결과 고객 설치 시 일반적으로 나타나는 보고 작업을 시뮬레이션합니다. 제한적 사용, 웹 보안, 애플리케이션 가시성 및 온박스(On-Box) 보고 등의 기능을 다룰 예정입니다. 실습 참가자는 3시간의 할당된 실습 시간 이내에 실습을 완료할 수 있어야 합니다. 이 실습에 포함된 모든 작업은 시나리오 11을 제외하고 **WSA-HQ1**에서 수행됩니다.

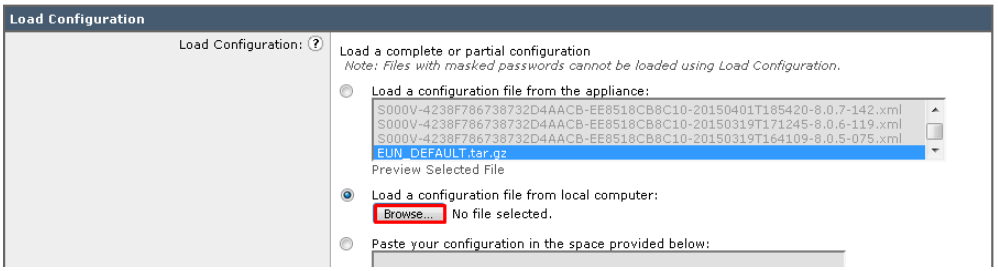
Web Security Appliance 데모에 대한 본 가이드는 다음 내용으로 구성되어 있습니다.

## 맞춤형 옵션

WSA 기본 설정 및 컨피그레이션에 친숙한 고급 사용자의 경우 다음 단계에 따라 컨피그레이션을 로드하여 시나리오 3으로 바로 이동할 수 있습니다. 시나리오 1과 2에서는 다음 작업을 완료합니다.

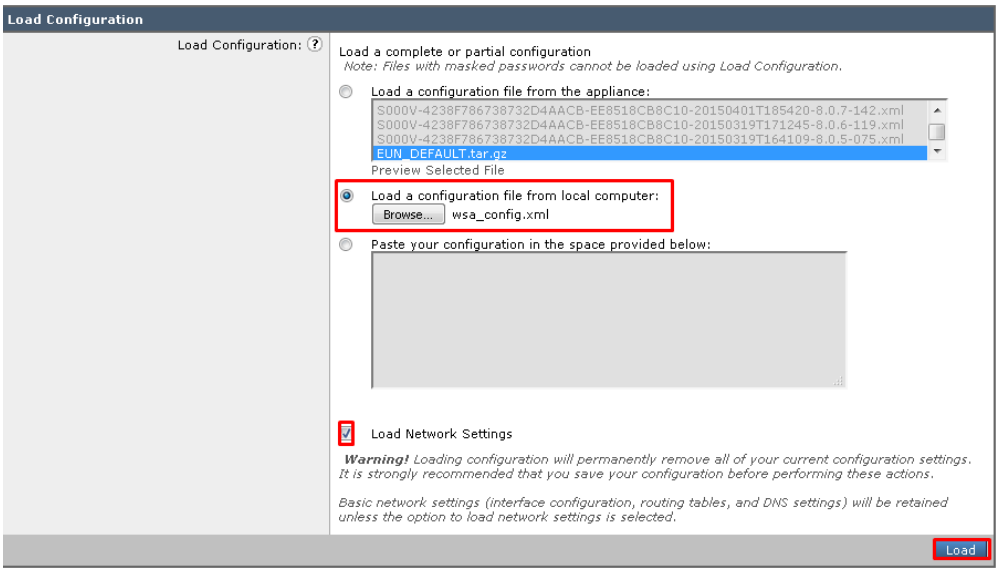
- 네트워크 구성정보
- 인증 영역 생성
- 기본 인증 및 NTLMSSP에 사용되는 ID 프로파일 생성
- 범주를 차단하는 액세스 정책 컨피그레이션
- HTTPS 검사

- 기본 클라이언트 머신(wkst1)에 로그인합니다.
- Firefox를 열고 기본 WSA(WSA-HQ1)(https://198.19.10.51)에 액세스합니다.
- 사용자 이름 admin과 비밀번호 ironport를 사용하여 로그인합니다.
- System Administration(시스템 관리) > Configuration File(컨피그레이션 파일)로 이동합니다.
- Load Configuration(컨피그레이션 로드)에서 **Load a configuration file from your local computer(로컬 컴퓨터에서 컨피그레이션 파일 로드)**를 선택하고 Browse(찾아보기)를 클릭합니다.




- 데스크톱에서 **wsa_config.xml**을 선택합니다.

- Load Network Settings(네트워크 설정 로드) 확인란이 선택되었는지 확인하고 Load(로드)를 클릭합니다.




- 팝업에서 Continue(계속)를 클릭한 다음 성공 메시지를 받으면 오른쪽 상단에서 Commit Changes(변경사항 커밋)를 클릭합니다.
- 컨피그레이션이 이제 로드됩니다.
- 로그인 접속 정보는 사용자 이름이 **admin**이고 비밀번호가 **ironport**입니다.

# 필요조건

다음 표에는 사전 구성된 데모의 필요조건이 요약되어 있습니다.

**표 1.** 필요조건

| 필수 | 옵션 |
|---|---|
| • 노트북 컴퓨터 | • Cisco AnyConnect |

# 솔루션 정보

지능형 웹 보안 위협에 맞서기 위해서는 모든 엔드포인트와 그 사이의 모든 영역에 강력한 보호와 일관성 있는 제어가 이루어져야 합니다. 여기에는 모바일 디바이스, 웹 및 모바일 애플리케이션, 웹 브라우저가 포함됩니다. Cisco® Web Security Appliance가 필요한 이유입니다. 이 제품을 통해 웹 트래픽의 보안 및 제어 문제를 쉽고 빠르게 해결할 수 있습니다.

Cisco WSA는 고도로 보안된 일체형(all-in-one) 웹 게이트웨이로서 강력한 보호, 완벽한 제어, 투자 가치라는 이점을 제공합니다. 또한 경쟁력 있는 웹 보안 구축 옵션을 다양하게 제공하며, 각 옵션에는 Cisco의 업계 최고 글로벌 위협 정보 인프라가 포함되어 있습니다.

Web Security Appliance는 AMP(Advanced Malware Protection), CTA(Cognitive Threat Analytics), AVC(Application Visibility and Contro), AUP(Acceptable-use policies), 인사이트 보고, 고도의 보안 모빌리티를 통합하여 제공합니다(그림 1). 사용하기 쉬운 단일 플랫폼을 제공합니다. 물리적 어플라이언스인 Web Security Appliance는 레이턴시 감소와 더불어 낮은 운용 비용 등 유지보수에

대한 요구사항이 적습니다. 고도로 분산된 네트워크의 경우 Cisco Web Security Virtual Appliance를 통해 필요할 때 언제, 어디서든 가상 버전으로 동일한 웹 보안을 구축할 수 있습니다.

http://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html

# 토폴로지

이 콘텐츠에는 데모 시나리오의 솔루션 기능을 설명하기 위해 사전 설정된 사용자 및 구성 요소가 포함되어 있습니다. 대부분의 구성 요소는 사전 정의된 관리자 계정으로 충분히 설정할 수 있습니다. 활성 세션의 **Topology(토폴로지)** 메뉴 또는 활용할 시나리오 단계에서 구성 요소 아이콘을 클릭하면 해당 구성 요소에 액세스하는 데 사용할 IP 주소 및 사용자 계정 접속 정보를 볼 수 있습니다.

**그림 1.** dCloud 토폴로지

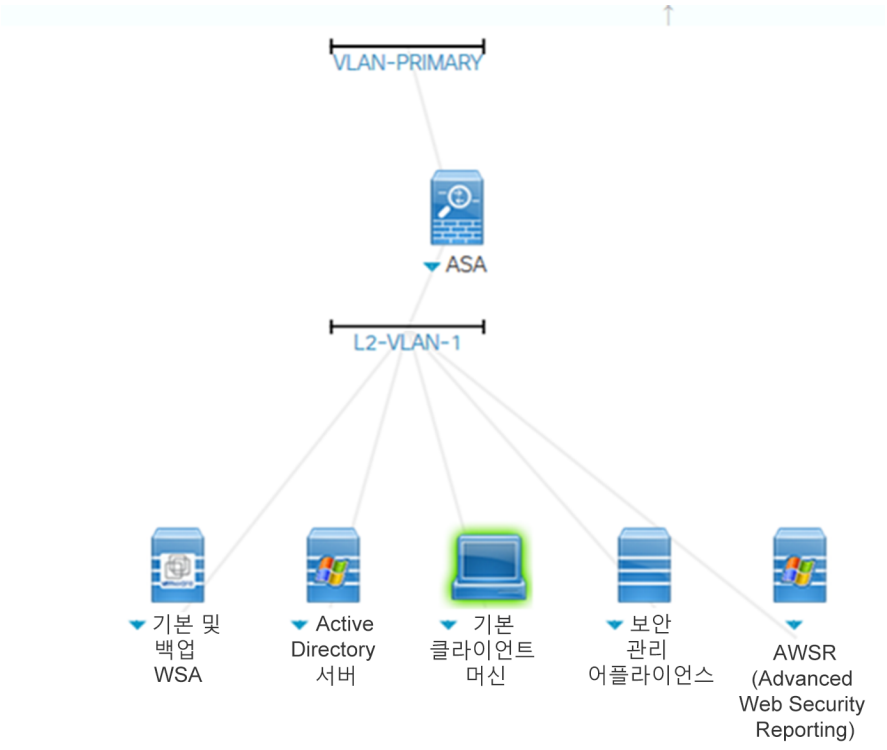



**표 2.** 장비 세부 사항

| 이름 | 설명 | 호스트 이름(FQDN) | IP 주소 | 사용자 이름 | 비밀번호 |
|---|---|---|---|---|---|
| WSA 1 | 기본 WSA(v. 10.1) | wsa-hq1.dcloud.cisco.com | 198.19.10.51 | admin | ironport |
| WSA 2 | 보조 WSA(v. 10.1) | wsa-hq2.dcloud.cisco.com | 198.19.10.52 | admin | C1sco12345 |
| Workstation 1 | 기본 클라이언트 머신 | wkst1.dcloud.cisco.com | 198.19.10.36 | dCloud\wsaproxy | C1sco12345 |
| Workstation 2 | 보조 클라이언트 머신 | wkst3.dcloud.cisco.com | 198.18.133.36 | dcloud\connector | C1sco12345 |
| AD Server | Active Directory 서버 | ad1.dcloud.cisco.com | 198.19.10.1 | dcloud\administrator | C1sco12345 |
| AWSR | AWSR(Advanced Web Security Reporting) | | 198.19.10.56 | admin | C1sco12345 |
| SMA | 보안 관리 어플라이언스 | sma.dcloud.cisco.com | 198.19.10.55 | admin | C1sco12345 |
| ESXi Server | ESXi 호스팅 서버 | | 198.19.10.31 | root | C1sco12345 |

# 시작하기

다음 단계에 따라 세션을 예약하고 환경을 설정하시기 바랍니다.

1. dCloud 세션을 시작합니다. [방법 보기]

**참고:** 세션이 활성화되기까지 최대 10분이 소요될 수 있습니다.

2. 최적의 환경으로 데모를 진행하기 위해 **Cisco AnyConnect VPN**과[방법 보기] **노트북 컴퓨터의 로컬 RDP 클라이언트**[방법 보기]를 이용하여 워크스테이션에 연결하십시오.
   - 워크스테이션 1: **198.19.10.36**, 사용자 이름: **dCloud\wsaproxy**, 비밀번호: **C1sco12345**

**참고:** Cisco dCloud Remote Desktop 클라이언트를 사용하여[방법 보기] 워크스테이션에 연결할 수도 있습니다. dCloud Remote Desktop 클라이언트는 데모 세션을 유지하기 위한 인터액션을 최소한으로 발생시키기 때문에 리모트 접속에 최적화된 환경을 제공합니다. 단, dcloud RDP 활용시 많은 사용자들이 연결 및 성능 관련한 문제를 겪기도 합니다.

# 시나리오 1. 기본 WSA 컨피그레이션 및 테스트

## 서론

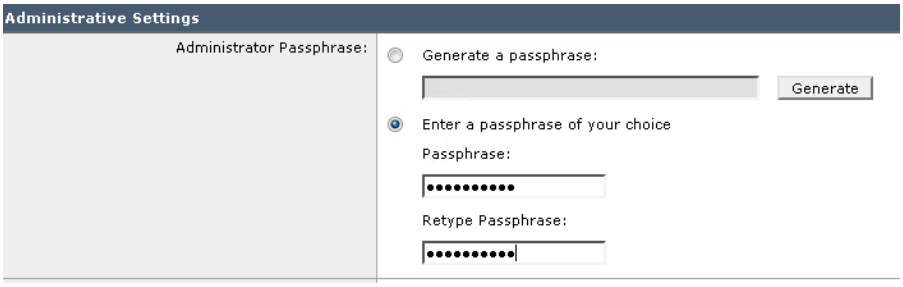
이 시나리오는 WSA의 기본 컨피그레이션 및 테스트를 다루며 본 실습에서 추가적인 시나리오를 진행하기 위해 **필수**로 진행해야 합니다. 본 실습은 여러 작업으로 구성되어 있습니다. 고급 사용자와 WAS 기본 컨피그레이션에 친숙한 사용자는 본 시나리오의 콘텐츠를 VMWare 스냅샷에서 로드할 수 있습니다. 맞춤형 옵션 섹션에서 지침이 제공됩니다.

## 작업 A: 시스템 설정

## 단계

1. **기본 클라이언트 머신**에서 Firefox를 열고 다음의 방법을 이용하여 WSA 관리 GUI에 접속합니다.
    a. https://198.19.10.51:8443를 입력하거나 북마크 툴바에서 WSA-HQ1 바로가기를 클릭합니다.
    b. 사용자 이름 **admin**과 비밀번호 **ironport**로 로그인합니다.
2. WSA GUI에서 **System Administration(시스템 관리) > System Setup Wizard(시스템 설정 마법사)**로 이동합니다.
3. 기본 시스템 호스트 이름이 **wsa-hq1.dcloud.cisco.com**인지 확인합니다.
4. DNS 서버가 **198.19.10.1**로 설정되었는지 확인합니다.
5. NTP 서버가 **time.sco.cisco.com**인지 확인합니다.
6. 표준 시간대를 지역 – 아메리카, 국가 – 미국, 표준 시간대/GMT 오프셋 - 태평양(Los_Angeles)으로 설정합니다.
7. Appliance Mode of Operation(작업 어플라이언스 모드)로 **Standard(표준)**가 선택되었는지 확인하고 **Next(다음)**를 클릭합니다.
8. Network Context(네트워크 상황) 메뉴에서 다시 Next(다음)를 클릭합니다.
9. Network Interfaces and Wiring(네트워크 인터페이스 및 연결) 메뉴에서 IPv4 Address(IPv4 주소)로 **198.19.10.51/24**가 입력되었는지 확인합니다. **Next(다음)**를 클릭합니다.
10. Layer 4 Traffic Monitor Wiring(레이어 4 트래픽 모니터 연결) 메뉴에서 Duplex TAP(이중 TAP)을 선택했는지 확인합니다. **Next(다음)**를 클릭합니다.
11. 기본 게이트웨이로 **198.19.10.254**가 설정되었는지 확인합니다. **Next(다음)**를 클릭합니다.
12. Layer 4 Switch(레이어 4 스위치) 또는 No Device(디바이스 없음)가 선택되었는지 확인하고 **Next(다음)**를 클릭합니다.

13. Administrative Setting(관리 설정)에서 **Enter a passphrase of your choice(선택한 암호 입력)**를 선택하고 **Cisco123$**를 입력합니다.




14. 이메일 주소로 operator@wsalab.com을 설정합니다.
15. AutoSupport 및 NetworkParticipation을 선택 취소하거나 **Next(다음)**를 클릭합니다.
16. Malware and Spyware Scanning(악성코드 및 스파이웨어 스캐닝)의 **Action for Detected Malware(탐지된 악성코드에 대한 조치)**에서 Block(차단) 라디오 버튼(나머지는 기본값으로 유지)을 선택하고 **Next(다음)**를 클릭합니다.
17. 설정을 살펴보고 오른쪽에 있는 Edit(편집)을 클릭하여 권장 설정과 비교하여 잘못된 내용을 수정합니다. **Install This Configuration(이 컨피그레이션 설치)**을 클릭하여 초기 컨피그레이션을 설치합니다.
18. 이때 WSA는 새로운 FQDN으로 리디렉션됩니다. 인증서 오류를 받고 액세스가 허용된 이후에 **System Setup Next Steps(시스템 설정 다음 단계)** 창으로 이동합니다. 또한 IP https://198.19.10.51:8443을 통해 WSA UI에 다시 액세스할 수도 있습니다.

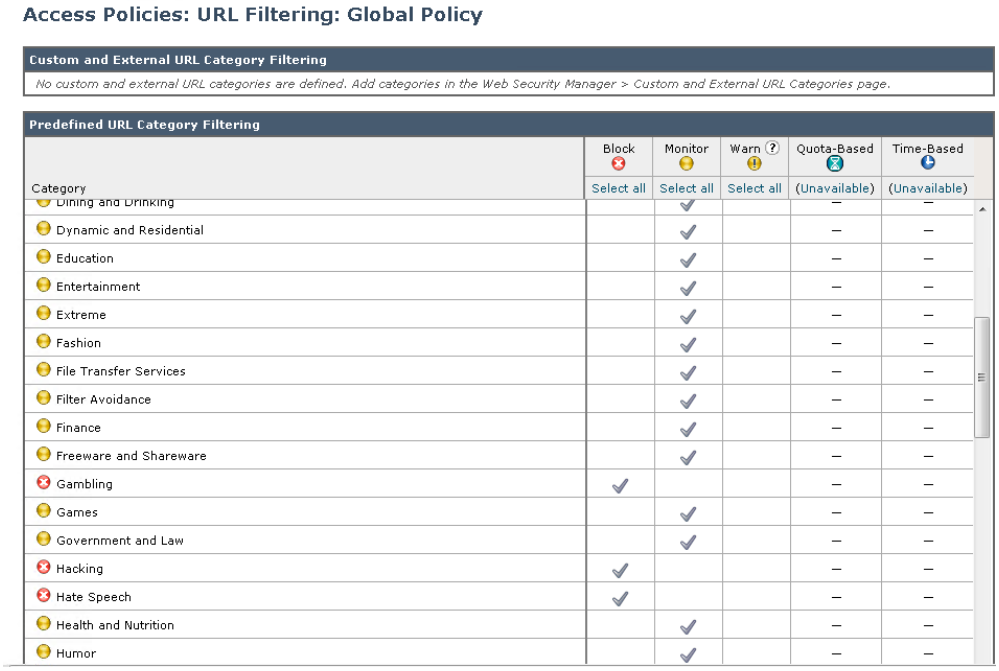
**참고:** 시스템 설정 마법사가 제대로 실행되었으며 컨피그레이션이 적용되었는지 확인하려면 WSA GUI > Security Services(보안 서비스) > Web Proxy(웹 프록시) > Basic Settings(기본 설정)으로 이동하여 프록시에 대한 HTTP 포트가 80, 3128이며 프록시가 활성화되었는지 확인하십시오. 프록시가 비활성화되어 있는 경우, 시스템 설정 마법사를 재실행해야 합니다.

## 작업 B: 제한적 사용 시행

## 단계

1. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)를 선택합니다.
2. URL Filtering(URL 필터링) 열에서 **Monitor: 79** 텍스트를 클릭합니다.

3. Block(차단) 열을 클릭하여 부적절하다고 생각하는 범주를 차단합니다.




4. Gambling(도박)이 차단되었는지 확인합니다. 이 용어는 본 실습에서 제한적 사용을 테스트하기 위해 사용합니다.

5. 페이지 하단에 있는 Submit(제출) 버튼을 클릭합니다. [변경 사항을 제출하면 이후에 커밋 또는 취소될 수 있는 비활성 컨피그레이션이 구성됩니다.]

6. WSA GUI 오른쪽 상단에서 노란색 버튼을 클릭합니다.

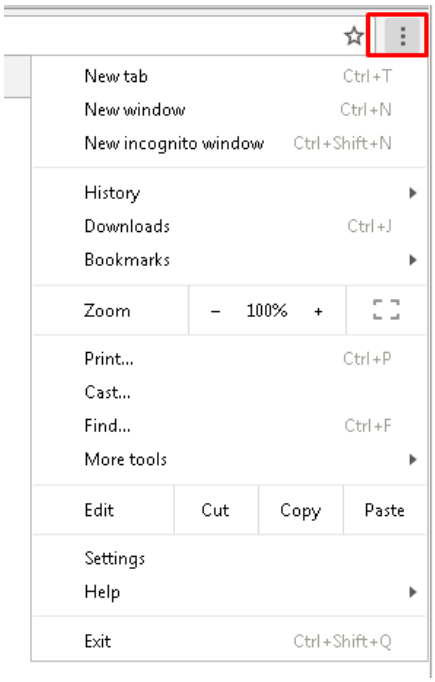

7. 중요한 코멘트를 입력한 다음 Commit Changes(변경 사항 커밋)를 클릭합니다.


# 작업 C: 프록시 기능 확인

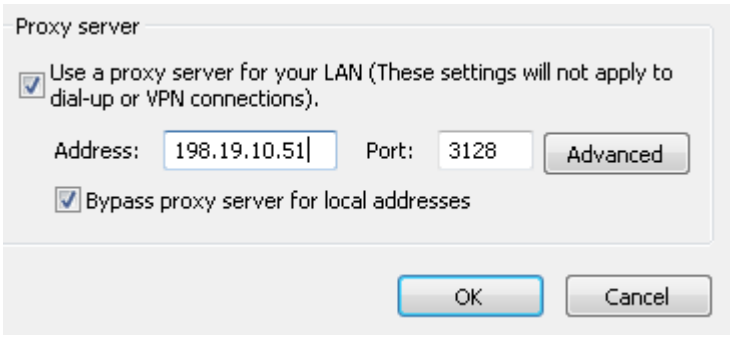
## 단계

1. Chrome 브라우저를 열고 프록시가 WSA로 설정되었는지 확인합니다.

2. 옵션 버튼을 클릭합니다(오른쪽 상단에 있는 세로로 놓인 3개의 점)

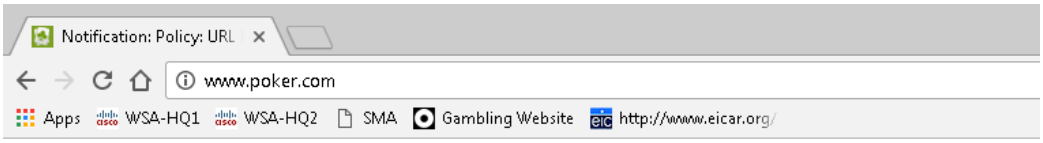


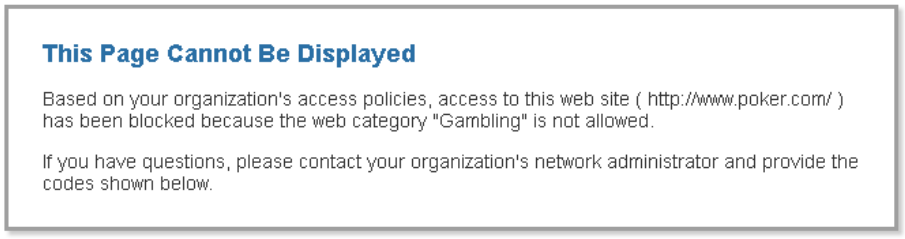

3. Settings(설정)를 클릭한 다음 아래로 스크롤하여 하이퍼링크 **Show advanced settings...(고급 설정 표시...)**를 클릭합니다.
4. Network(네트워크)에서 Change proxy settings...(프록시 설정 변경...)를 클릭합니다.
5. Connections(연결) > LAN Settings(LAN 설정)에서 프록시 설정이 다음과 같은지 확인합니다.




6. OK(확인)를 클릭하고 다시 한번 OK(확인)를 클릭합니다.
7. http://www.yahoo.com 같이 허용되는 웹 사이트에 액세스합니다. 액세스에 성공해야 합니다.

8. 이제 http://poker.com 같이 허용되지 않는 웹 사이트에 액세스합니다. 액세스가 차단되어야 합니다.

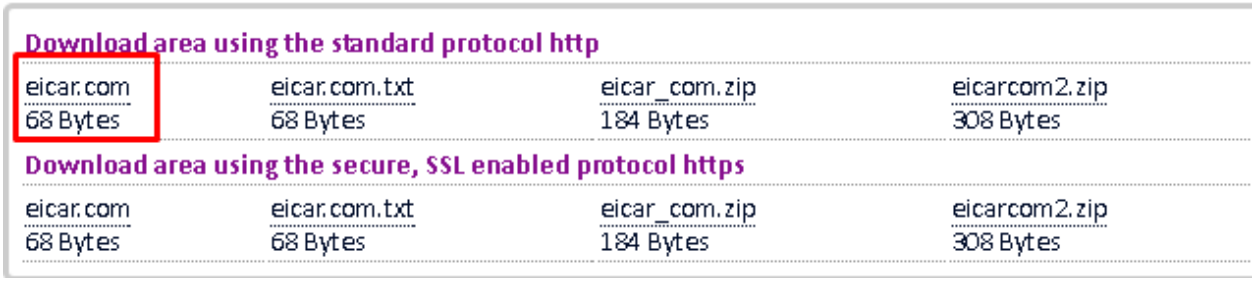



Date: Sat, 01 Apr 2017 17:17:31 PDT
Username:
Source IP: 198.19.10.36
URL: GET http://www.poker.com/
Category: Gambling
Reason: BLOCK-WEBCAT
Notification: WEBCAT

9. 북마크 툴바에서 eicar.org를 선택합니다.


10. Download(다운로드) 영역이 보일 때까지 아래로 스크롤하고 표준 http에 대해 **eicar.com** 테스트 파일을 클릭합니다. 해당 페이지가 차단되어야 합니다.




11. 이제 www.ihaveabadreputation.com으로 이동합니다. 액세스가 차단되어야 하며 최종 사용자 통지 페이지가 표시되어야 합니다.

# 작업 D: CLI를 사용하여 프록시 액세스 로그 읽기

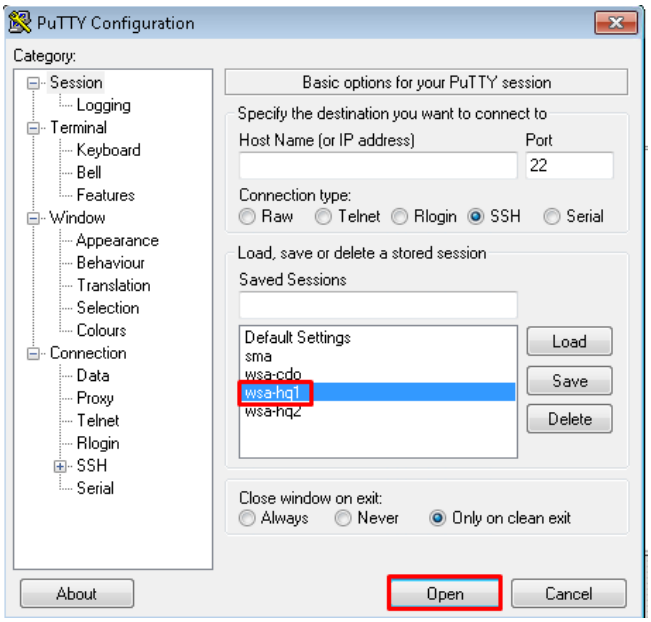
## 단계

정책 컨피그레이션의 문제 해결에서 가장 중요한 로그가 프록시 액세스 로그입니다. 본 실습 전반에서 이 액세스 로그를 확인할 수 있습니다. 이제 실시간으로 이 로그를 확인하는 방법을 학습하겠습니다.

1. SSH를 통해 S-Series에 접속합니다.

   a. putty.exe라는 데스크톱 아이콘을 더블 클릭합니다. 

   b. **wsa-hq1**이라는 사전 정의된 세션이 있습니다. 이 세션은 SSH를 통해 사용자를 WSA에 연결합니다.




   c. WSA에 로그인합니다.

2. WSA CLI를 사용하여 로그를 확인하는 두 가지 방법이 있습니다.

   a. WSA CLI에 **tail accesslogs**를 입력합니다. 종료하려면 **ctrl + C**를 누릅니다.

   b. 구성된 로그 목록을 표시하려면 tail을 입력합니다. 여기에서 추적하려는 로그에 해당하는 숫자를 입력할 수 있습니다. **1**을 선택하여 액세스 로그를 찾습니다.

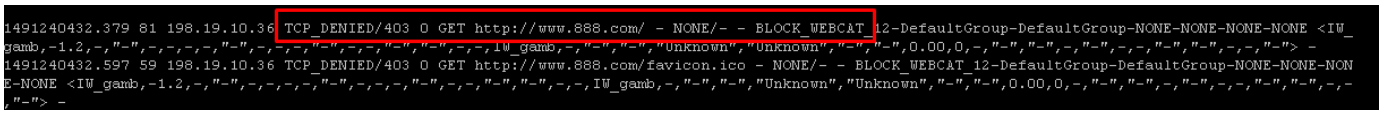
**참고:** 경우에 따라 tail accesslogs 명령의 출력에 10초~30초의 지연이 발생할 수 있습니다. WSA는 실시간으로 로그를 기록하지만, 출력만 약간 늦게 표시되는 것입니다.

3. Chrome을 사용하여 http://poker.com에 방문하고 액세스 로그와 HTTP 헤더를 모두 살펴봅니다. 이전 실습에서 생성한 액세스 정책으로 인해 액세스가 차단됩니다. 액세스 로그 tail 엔트리에서 다음 문자열을 찾습니다.

   a. **TCP_DENIED** – 동작 코드 또는 캐시 결과 코드

b. **403 –** HTTP 응답 코드

c. **BLOCK_WEBCAT** – ACL 결정 태그

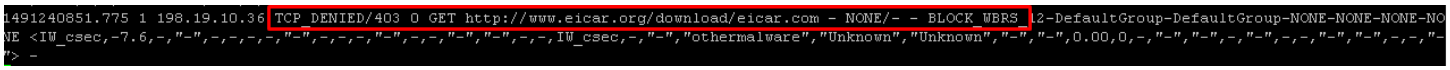



4. Chrome을 사용하여 eicar 테스트 바이러스 다운로드를 다시 시도합니다. 액세스 로그 및 HTTP 헤더를 모두 확인합니다. WSA의 액세스 로그 엔트리에서 다음 문자열을 찾습니다.

   a. TCP_DENIED – 동작 코드 또는 캐시 결과 코드

   b. 403 – HTTP 응답 코드

   c. BLOCK_WEBCAT – ACL 결정 태그




## 작업 E: 프록시 인증

## 단계

1. WSA GUI에서 Network(네트워크) > Authentication(인증)으로 이동하여 **Add Realm...(영역 추가...)**을 클릭합니다.

   a. Realm Name(영역 이름)에 ADrealmDC1을 입력합니다.

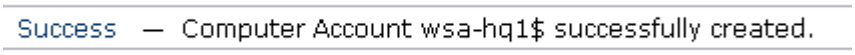
   b. Authentication Server Type and Scheme(인증 서버 유형 및 스키마)에서 **Active Directory (Kerberos, NTLMSSP or Basic Authentication)(Active Directory(Kerberos, NTLMSSP 또는 기본 인증)**를 선택합니다.

   c. Active Directory 서버에 **198.19.10.1**을 입력합니다.

   d. Active Directory 도메인에 **dcloud.cisco.com**을 입력합니다.

   e. Join Domain(도메인 조인)을 클릭하고 접속 정보로 사용자 이름 **Administrator**, 비밀번호 **C1sco12345**를 사용합니다.

   f. 모든 단계가 성공하면 "Success – Computer Account gold$ successfully created" 메시지가 표시됩니다.




2. **Start Test(테스트 시작)** 버튼을 클릭합니다.

   a. 테스트가 성공적으로 완료된 후 Submit(제출) 버튼을 클릭합니다.

   b. 오류 메시지가 나타나면 문제를 해결하고 호스트 이름과 AD 서버 등을 확인하십시오.

   c. 변경 사항을 커밋하고 Comments(코멘트) 섹션에 "AD Realm created"를 추가합니다.

3. WSA 도메인의 새로운 ID를 생성합니다.

    a. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Identification Profiles(식별 프로파일)로 이동합니다.

    b. Add Identification Profile...(식별 프로파일 추가...)을 클릭합니다.

    c. Name(이름) 필드에 **dCloud**를 입력합니다. Description(설명) 텍스트 상자에 적절한 설명을 입력합니다.

    d. Identification and Authentication(식별 및 인증)에서 드롭다운을 클릭하고 **Authenticate Users(사용자 인증)**를 선택합니다.

    e. Select a Realm or Sequence(영역 또는 순서 선택)에는 ADrealmDC1이 이미 선택되어 있습니다.

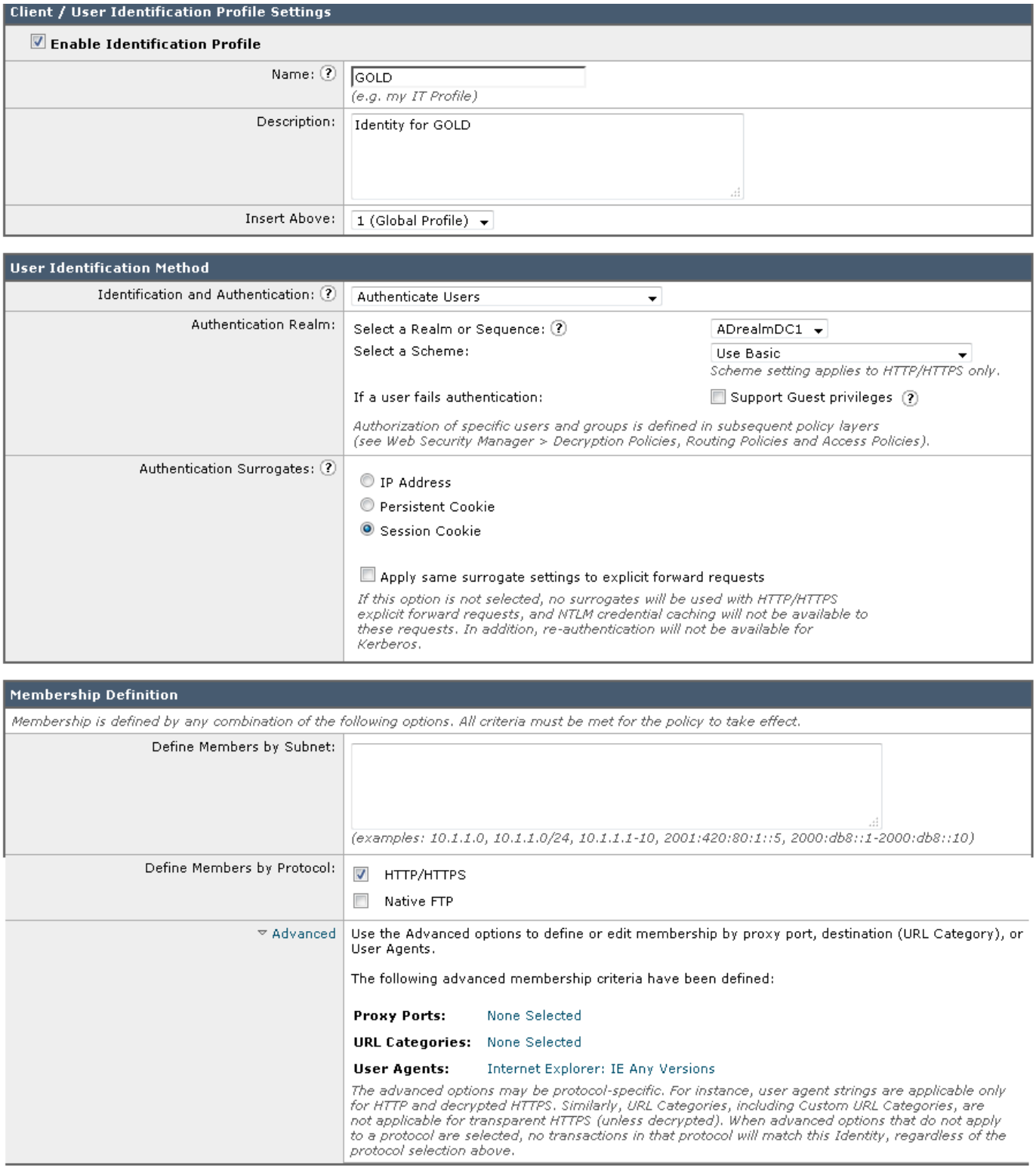
    f. Select a Scheme(스키마 선택)에서 **Use Basic(기본 사용)**을 선택하고 Authentication Surrogates(인증 서로게이트)에서 **Session Cookie(세션 쿠키)**를 선택합니다.

    g. **Apply same surrogate settings to explicit forward requests(명시적 전달 요청에 동일한 서로게이트 설정을 적용)**를 선택합니다.

    h. **Advanced(고급)**을 클릭하고 **None Selected(선택한 항목 없음)**를 클릭합니다.

    i. Common User Agents(일반 사용자 에이전트)에서 브라우저를 클릭하고 **IE Any Versions(임의의 IE 버전)**를 선택합니다. 아래로 스크롤하고 Done(완료)을 클릭합니다.

    j. 컨피그레이션이 아래 스크린샷과 같이 보여야 합니다. 마무리되면 Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.



**Client / User Identification Profile Settings**

Enable Identification Profile

Name: GOLD
*(e.g. my IT Profile)*

Description: Identity for GOLD

Insert Above: 1 (Global Profile)

**User Identification Method**

Identification and Authentication: Authenticate Users

Authentication Realm:
Select a Realm or Sequence: ADrealmDC1
Select a Scheme: Use Basic
*Scheme setting applies to HTTP/HTTPS only.*
If a user fails authentication: Support Guest privileges
*Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).*

Authentication Surrogates:
IP Address
Persistent Cookie
Session Cookie
Apply same surrogate settings to explicit forward requests
*If this option is not selected, no surrogates will be used with HTTP/HTTPS explicit forward requests, and NTLM credential caching will not be available to these requests. In addition, re-authentication will not be available for Kerberos.*

**Membership Definition**

*Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.*

Define Members by Subnet:
*(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)*

Define Members by Protocol:
HTTP/HTTPS
Native FTP

Advanced
Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Proxy Ports:** None Selected
**URL Categories:** None Selected
**User Agents:** Internet Explorer: IE Any Versions

*The advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories, are not applicable for transparent HTTPS (unless decrypted). When advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.*

**참고:** Submit(제출)을 클릭한 후에 경고 메시지를 받습니다. 아이디어 ID 프로파일 순서 관련 메시지를 확인합니다.

4. 글로벌 ID에 대한 인증을 활성화합니다.

    a. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Identification Profiles(식별 프로파일)로 이동합니다. Global Identification Profile(글로벌 식별 프로파일)을 클릭합니다.

    b. Identification and Authentication(식별 및 인증) 드롭다운 메뉴에서 **Authenticate Users(사용자 인증)**를 선택합니다.

    c. Select a Realm or Sequence(영역 또는 순서 선택) 드롭다운 메뉴에서 **All Realms(모든 영역)**를 선택합니다.

    d. Select a Scheme(스키마 선택) 드롭다운 메뉴에서 **Use NTLMSSP or Basic(NTLMSSP 또는 기본 사용)**을 선택합니다.

    e. Authentication Surrogates(인증 서로게이트)로 **Session Cookie(세션 쿠키)**를 선택합니다.

    f. 페이지 우측 하단의 Submit(제출) 버튼을 클릭합니다. 경고를 무시합니다.

    g. 오른쪽 상단에서 Commit Changes(변경 사항 커밋) >>로 나타나는 노란색 버튼을 클릭합니다.

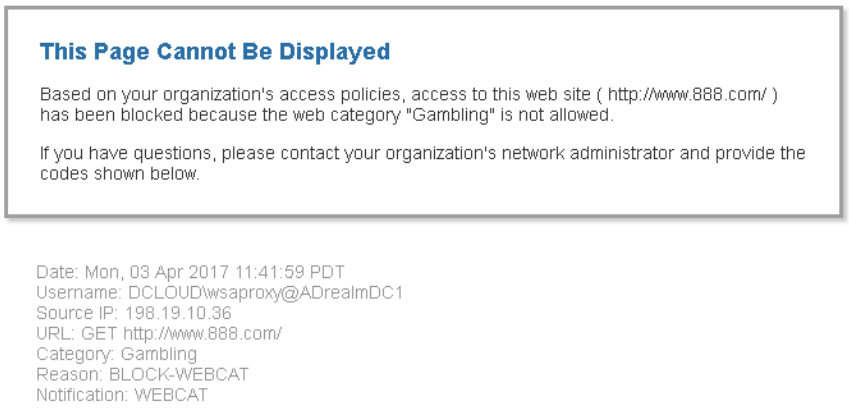
    h. Configured proxy authentication 같이 중요한 코멘트를 입력합니다.

    i. Commit Changes(변경사항 커밋)를 클릭합니다.

# 작업 E: 테스트 인증 컨피그레이션

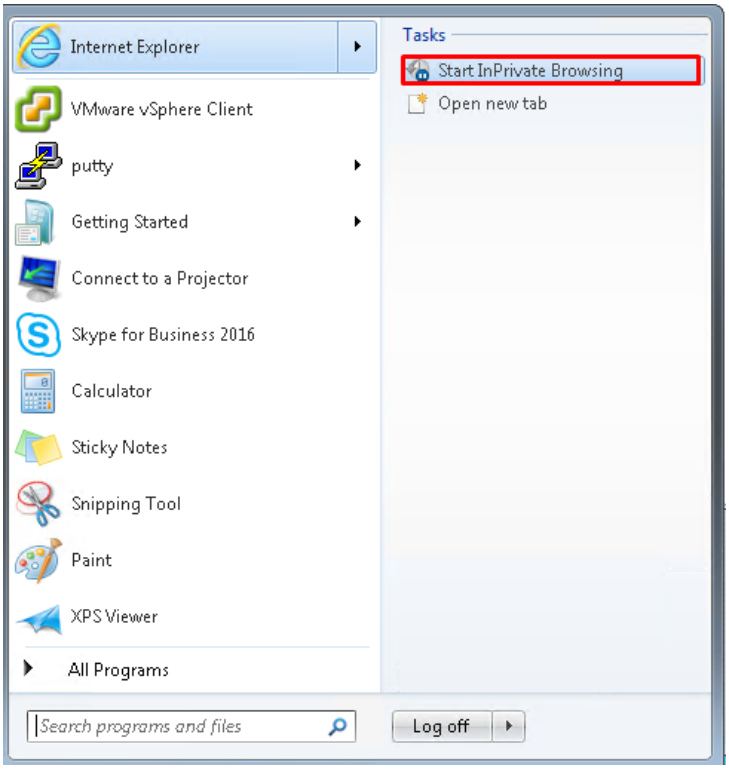
## 단계

1. Chrome을 엽니다. 선택한 몇 개의 URL을 테스트합니다.
2. www.poker.com을 검색합니다. 로그인하는 데 사용한 AD 사용자 이름이 다음과 같이 표시되어야 합니다.




3. 인증된 사용자의 ID가 액세스 로그에 나타나는지 CLI를 통해 확인합니다.

4. 시작 메뉴에서 개인 브라우징 모드로 Internet Explorer를 엽니다.




5. www.poker.com으로 이동합니다. 사용자 이름 **wsaproxy**, 비밀번호 **C1sco12345**를 입력합니다. 액세스가 차단되어야 합니다.

6. Gambling(도박) 사이트를 방문하면 사용자 이름이 나타나야 합니다.

**참고:** 다음은 WSA에서 수행하는 두 가지 인증 방법을 보여줍니다. NTLMSSP를 사용하도록 글로벌 정책을 설정했으므로 인증이 투명하게 수행됩니다. GOLD ID 프로파일이 Basic(기본)으로 설정되어 있고 Internet Explore에만 적용되도록 설정되어 있기 때문에 IE가 열리면 로그인 메시지가 표시됩니다.

# 시나리오 2. HTTPS 검사 활용

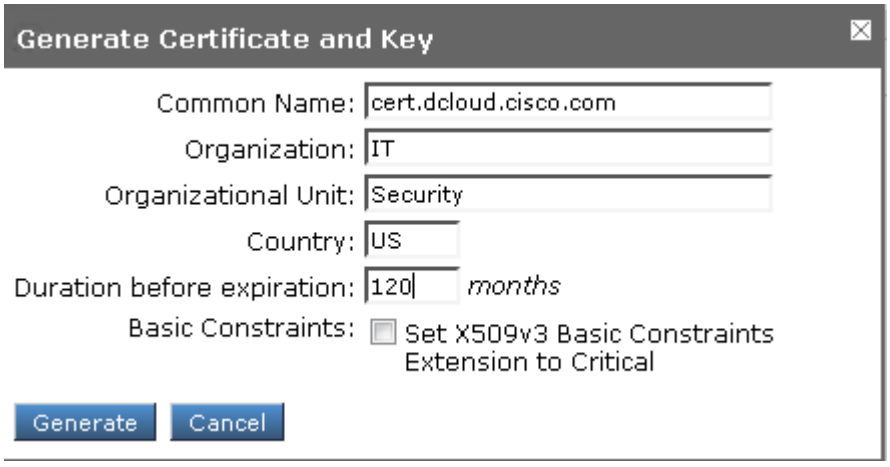
## 작업 A: HTTPS 프록시 컨피그레이션

### 서론

HTTPS 프록시 구성은 웹 트래픽을 캡처하고 제어하기 위해 매우 중요한 과정입니다. 이 기능은 더 많은 웹 사이트가 암호화될수록 더 많은 고객 환경에서 필수적인 기능으로 자리 잡고 있습니다.

### 단계

1. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)에서 URL Filtering(URL 필터링)에 있는 링크를 클릭합니다. 차단할 소셜 네트워킹 범주를 설정합니다. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.
2. HTTPS 검사가 필요한 이유를 설명합니다. HTTPS를 사용하여 다운로드된 파일이 검사되고 있지 않은지 확인합니다.
    a. Chrome을 사용하여 **https://www.facebook.com**으로 이동합니다.
    b. 이 페이지의 로드에 실패해야 합니다. 그 이유는 초기 HTTPS 요청이 암호화되지 않았기 때문에 WSA가 이 초기 연결을 차단하기 때문입니다. 그러나 적절한 차단 페이지는 완전히 암호화되었으므로 표시되지 않습니다. HTTPS 차단을 제대로 활용하기 위해서는 HTTPS 검사를 활성화해야 합니다.
3. HTTPS 프록시를 활성화하고 구성합니다.
    a. Security Services(보안 서비스)> HTTPS Proxy(HTTPS 프록시)로 이동합니다. Enable and Edit Settings...(설정 사용 및 편집...)를 클릭합니다.
    b. HTTPS 프록시 라이선스 계약서를 수락합니다.
    c. HTTPS Proxy Settings(HTTPS 프록시 설정)에서 **Use Generated Certificate and Key(생성된 인증서 및 키 사용)**를 선택하고 Generate New Certificate and Key(새로운 인증서 및 키 생성) 버튼을 클릭합니다. 다음과 같이 파라미터를 추가하고 작업이 완료되면 Generate(생성)를 클릭합니다.

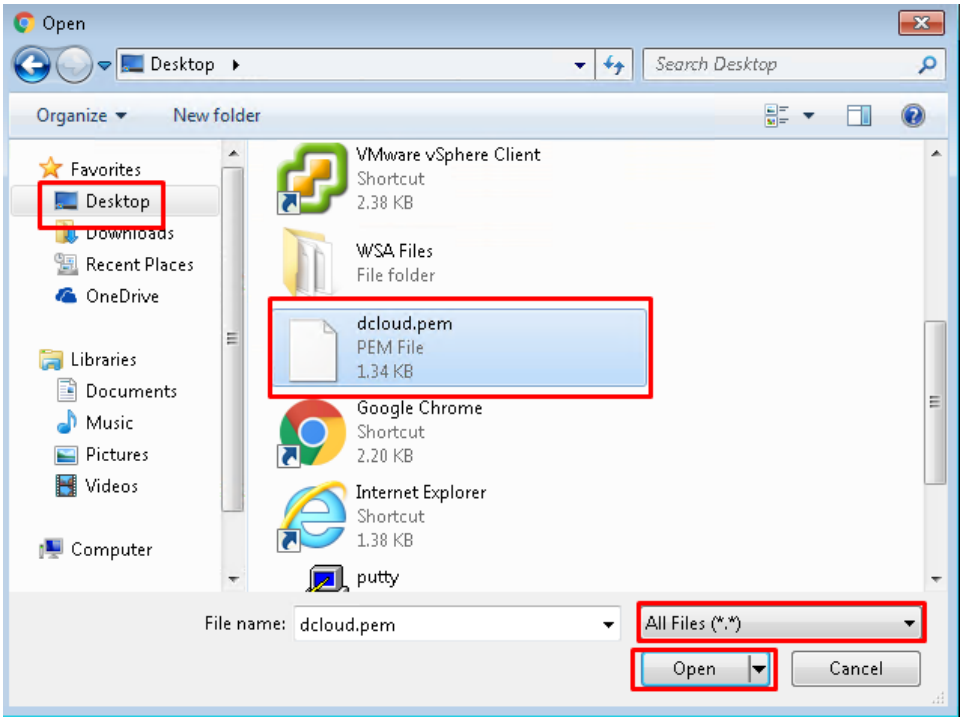


d. **Download Certificate(인증서 다운로드)** 링크를 마우스 오른쪽 버튼으로 클릭하고 Save Link As...(다른 이름으로 링크 저장)를 선택하고 .pem 파일 이름을 **dcloud**로 지정합니다. 데스크톱에 저장합니다.

e. 새 탭을 열고 **chrome://settings**를 입력합니다. 아래로 스크롤하고 Show advanced settings...(고급 설정 표시...)를 클릭합니다.

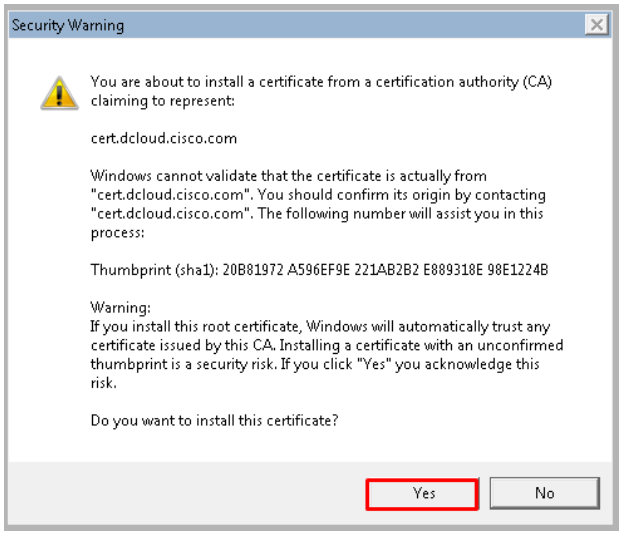
f. 아래로 스크롤하여 HTTPS/SSL로 이동하고 **Manage Certificates...(인증서 관리...)**를 클릭합니다.

g. Certificates(인증서) 창에서 **Import(가져오기) > Next(다음)**를 클릭합니다. Certificate Import Wizard(인증서 가져오기 마법사) 창에서 **Browse(찾아보기)**를 클릭합니다. Desktop(데스크톱)을 선택하고 드롭다운에서 **All files(모든 파일)**를 선택합니다. 마지막으로 dcloud.pem 파일을 선택하고 **Open(열기)**을 클릭합니다.




h. 다음 창에서 **Next(다음)**를 다시 클릭합니다. Certificate Store(인증서 저장소) 창에서 **Place all certificates in the following store(모든 인증서를 다음 저장소에 저장)**를 선택하고 **Browse(찾아보기)**를 클릭합니다. Select Certificate Store(인증서 저장소 선택) 창에서 **Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)**를 선택합니다. **OK(확인)**를 클릭합니다.

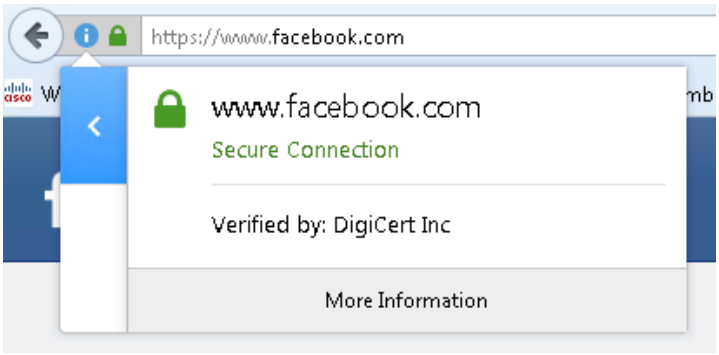
i. **Next(다음)**를 클릭하고 **Finish(마침)**를 클릭합니다. 보안 경고가 나타나면 **Yes(예)**를 클릭합니다.




j. WSA UI로 돌아가서 아래로 스크롤하고 HTTPS Proxy Settings(HTTPS 프록시 설정) 메뉴에서 **Submit(제출)**을 클릭합니다. 변경 사항을 커밋합니다.

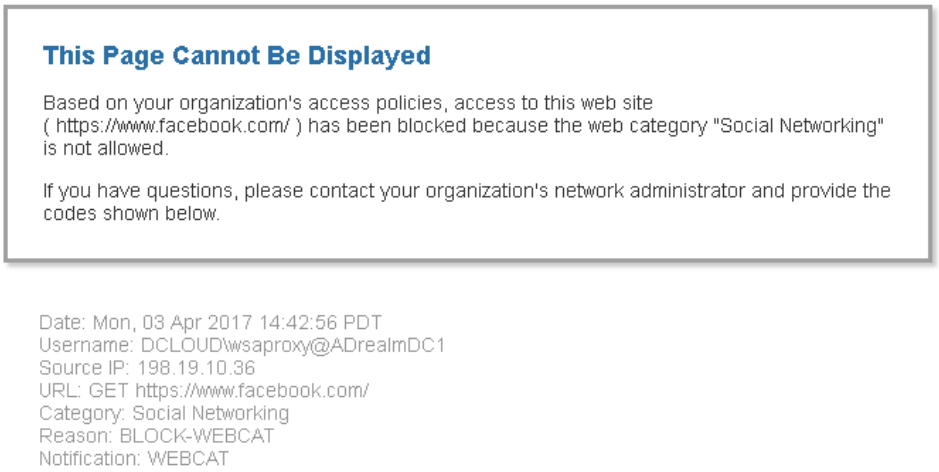
4. 복호화를 테스트합니다.

a. Firefox에서www.facebook.com으로 이동합니다. URL 필드에 녹색 자물쇠 아이콘을 클릭합니다. > 화살표를 클릭하고 인증서 세부 정보를 참조합니다.

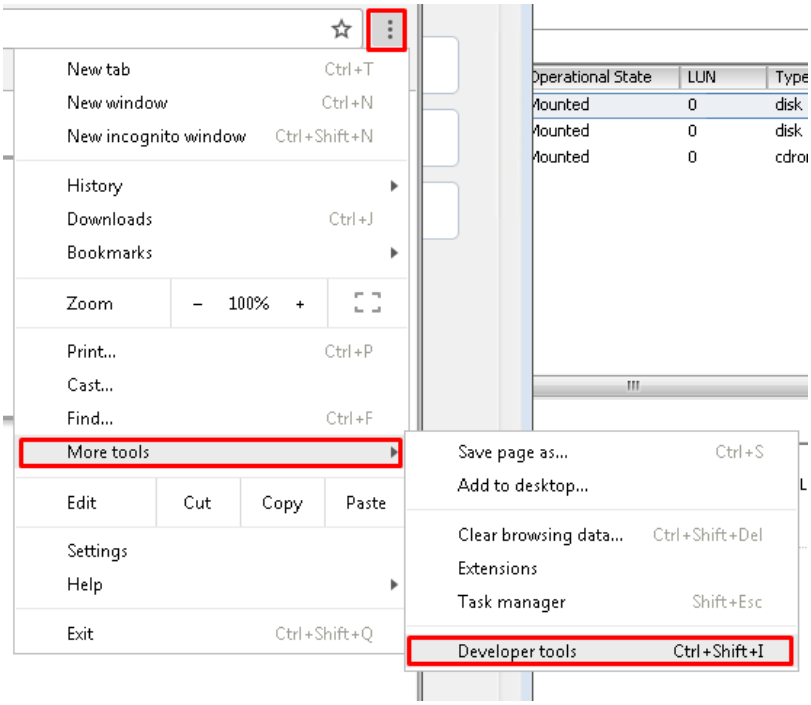



b. 상단에는 DigiCert에서 인증서를 제공한다고 표시됩니다.

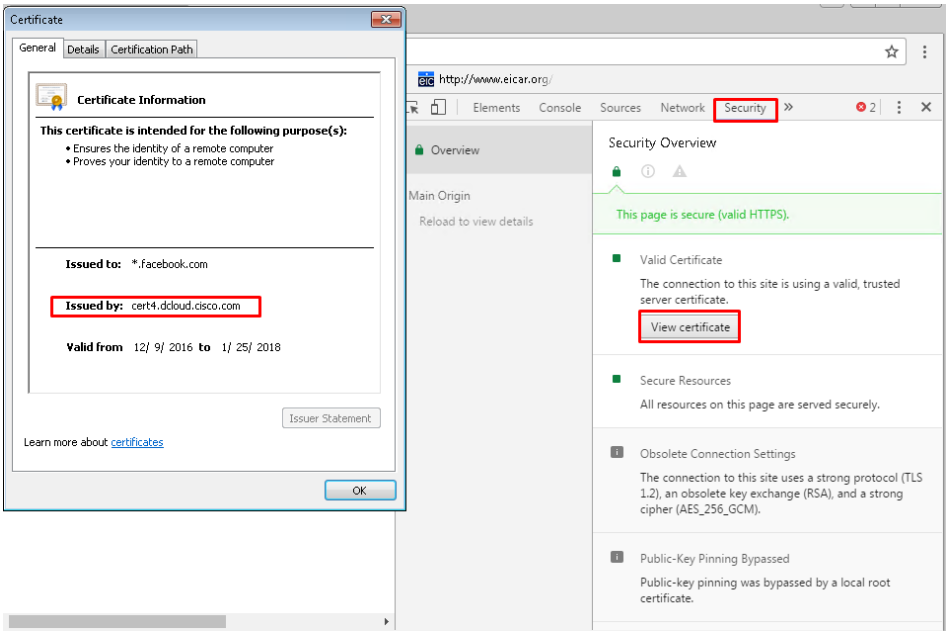
c. Chrome에서, facebook.com으로 다시 이동합니다. 이번에는 차단 페이지가 나타나야 합니다.




d. Chrome 설정에서 More tools(도구 더보기) > Developer tools(개발자 도구)를 선택합니다.



e. 다음으로, Security(보안) > View certificate(인증서 보기)를 클릭합니다.




f. 발급 중인 인증서에 WSA에서 생성한 인증서가 표시되어야 합니다. 이는 WSA가 HTTPS 트래픽을 올바르게 복호화하고 있음을 나타냅니다.

# 시나리오 3: 제한적 사용 시행

## 서론

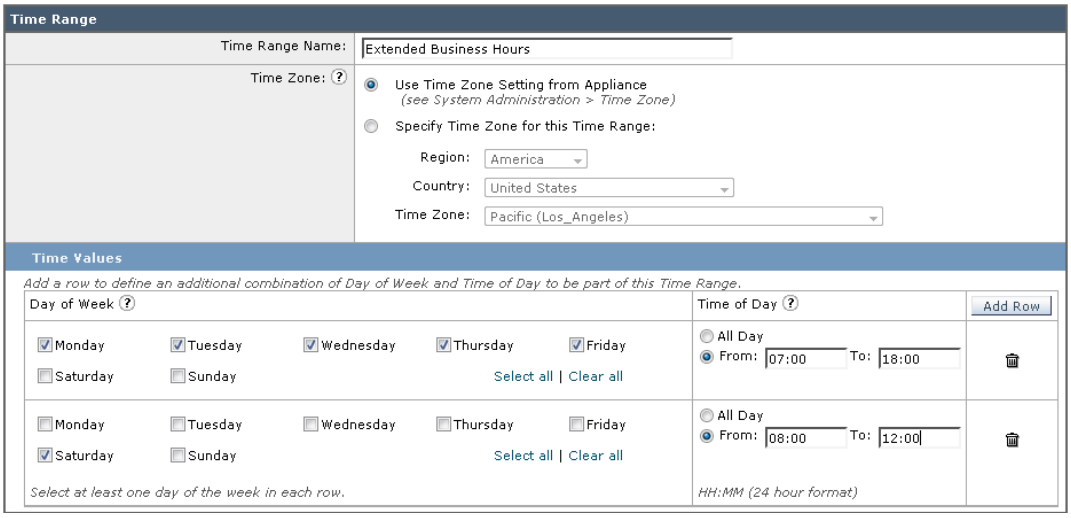
이 연습 문제의 목표는 제한적 사용 정책을 올바르게 구축하는 방법을 이해하는 것입니다. 이 시나리오는 5가지 작업으로 구성되어 있습니다.

1. 불법적이거나 불건전한 자료를 표시하는 범주를 차단합니다.
2. 특정 파일 유형을 차단하기 위한 아카이브 검사를 구성합니다.
3. Filter Avoidance(필터 회피) 및 Peer File Transfer(피어 파일 전송) 범주를 Warn(경고)으로 설정합니다.
4. 가장 바쁜 업무 시간(이외에는 모니터링) 동안 소셜 네트워킹을 차단합니다.
5. IP 기반 URL을 차단합니다.

## 작업 A: 적절한 글로벌 제한적 사용 정책 생성

## 단계

1. 두 가지 시간 범위, 즉 연장된 업무 시간 및 가장 바쁜 업무 시간을 생성합니다.
    a. WSA GUI에서 **Web Security Manager(웹 보안 관리자) > Define Time Ranges and Quotas(시간 범위 및 할당량 정의)**로 이동합니다.
    b. Add Time Range(시간 범위 추가)를 클릭합니다.
    c. Time Range Name(시간 범위 이름)에 Extended Business Hours(연장된 업무 시간)를 입력합니다.
    d. 어플라이언스의 시간대 설정을 사용합니다.
    e. Time Values(시간 값)에서 월요일부터 금요일까지의 상자를 선택합니다.
    f. Time of Day(시간)에서 07:00와 18:00를 입력합니다.
    g. Add Row(행 추가)를 클릭합니다.
    h. 새로운 행에서 토요일 확인란을 선택합니다.
    i. 새로운 행에 08:00와 12:00를 입력합니다.




j. 페이지 우측 하단의 Submit(제출) 버튼을 클릭합니다.

k. Add Time Range(시간 범위 추가)를 클릭합니다.

l. Time Range Name(시간 범위 이름)에 Peak Business 이름을 입력합니다.

m. 어플라이언스의 시간대 설정을 사용합니다.

n. Time Values(시간 값)에서 월요일부터 금요일까지의 상자를 선택합니다.

o. Time of Day(시간)에서 10:00와 14:00를 입력합니다.

p. Submit(제출) 버튼을 클릭하고 변경 사항을 커밋합니다.

2. 글로벌 정책(액세스 정책 그룹)의 URL 필터를 구성합니다.

a. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다.

b. Global Policy(글로벌 정책) 행의 URL Filtering(URL 필터링) 열에서 텍스트를 클릭합니다.

c. 불법적이거나 불건전한 자료를 나타내는 범주를 차단합니다. 여러 범주가 있습니다.

d. Filter Avoidance(필터 회피) 및 Peer File Transfer(피어 파일 전송) 범주를 Warn(경고)으로 설정합니다.

e. Social Networking(소셜 네트워킹) 범주에서 Time-Based(시간 기반)를 선택합니다.

f. 가장 바쁜 업무 시간(이외에는 모니터링) 동안 소셜 네트워킹을 차단합니다.

g. Shopping(쇼핑) 범주에서 Time Range(시간 범위)를 선택합니다.

h. 연장된 업무 시간 동안 쇼핑을 차단합니다(이외에는 경고 표시됨).

i. 페이지 우측 하단의 Submit(제출) 버튼을 클릭합니다.

j. 오른쪽 상단에서 Commit Changes(변경 사항 커밋)로 나타나는 노란색 버튼을 클릭합니다.

k. 글로벌 AUP 생성 같이 중요한 코멘트를 입력합니다.

l. Commit Changes(변경사항 커밋)를 클릭합니다.

m. 다음 URL를 방문하여 결과를 확인합니다.

i. www.proxify.com(필터 회피)

ii. www.facebook.com(소셜 네트워킹)

iii. www.amazon.com(쇼핑)

3. Social Networking(소셜 네트워킹) 및 Gambling(도박)에 대한 시간 기반 정책을 테스트하려면 정책 추적 툴을 사용합니다.

   a. WSA GUI에서 System Administration(시스템 관리) > Policy Trace(정책 추적)로 이동합니다.

   b. URL에 www.cisco.com 같이 유효한 URL을 입력합니다.

   c. Authentication Realm(인증 영역)에서 기존에 생성한 영역을 선택합니다.

   d. User Name(사용자 이름)에 DCLOUD\wsaproxy를 입력합니다.

   e. Advanced(고급) 텍스트를 클릭하여 고급 설정에 액세스합니다.

   f. Request Details(요청 정보)의 Time of Request(요청 시간)에서 Peak Business Hours(가장 바쁜 영업 시간)에 날짜와 시간을 입력합니다.

   g. Response Detail Overrides(응답 정보 재정의)의 URL 범주에서 Social Networking(소셜 네트워킹)을 선택합니다.

   h. Find Policy Match(정책 일치 찾기) 버튼을 클릭합니다.

   i. 결과가 정책 컨피그레이션과 일치하는지 확인합니다. 일치하지 않는 경우, 문제를 해결하고 모든 오류를 수정합니다. 다음의 스크린샷을 참조합니다.

## Policy Trace

**Destination**

URL: www.cisco.com

**Transaction**

Client or User: *To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through an authentication realm, choose the authentication realm and enter the user name.*

Authentication / Identification: ADrealmDC1

Client IP Address:

User Name: DCLOUD\wsaproxy

Advanced

**Request Details**

Proxy Port:

User Agent:

Time of Request: Date: 04/03/2017 Time: 11:00 (GMT -07:00)

Upload File: Browse... No file selected.

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

**Response Detail Overrides**

URL Category: Social Networking

Application: Do not override application

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Web Reputation Score: *(from -10.0 to 10.0)*

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

**Response Detail Overrides**

URL Category: Social Networking

Application: Do not override application

Object Size: *(Add a trailing K, M, or G to indicate size unit)*

MIME Type: Object and MIME Type Reference

Web Reputation Score: *(from -10.0 to 10.0)*

Webroot Verdict: Do not override malware verdict

McAfee Verdict: Do not override malware verdict

Sophos Verdict: Do not override malware verdict

Find Policy Match

**Results**

**User Information**

User Name: DCLOUD\wsaproxy
Authentication Realm Group Membership: DCLOUD\wsaproxy, DCLOUD\Group Policy Creator Owners, DCLOUD\Domain Users, DCLOUD\Domain Admins, DCLOUD\Enterprise Admins, DCLOUD\Schema Admins, DCLOUD\Organization Management
Secure Group Tag Membership: None
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0

**URL Check**

WBRS Score: 8.7
URL Category: Social Networking

**Policy Match**

Cisco Data Security policy: None
Decryption policy: None
Routing policy: None
Identification Profile: DefaultIdentification
Access policy: Global Access Policy

**Final Result**

**Request blocked**

Details: Request blocked based on URL category

Trace session complete

4. 3a~3i 단계를 반복하여 이전에 생성한 2개의 시간 할당량에 따라 요청 시간과 URL 범주를 다양하게 조합합니다.
5. IP 기반 URL 차단: http://67.20.81.143으로 이동할 수 있는지 확인합니다.

**참고:** 정규식을 사용하여 IP 주소를 연결하는 작업은 쉬운 일이 아닙니다. 이 작업이 복잡한 이유는 IP 주소가 여러 가지 방식으로 인코딩될 수 있기 때문입니다(예: 16진법, 8진법, 정수 또는 점으로 구분되는 4개의 정수). 또한 정규식이 구성되는 방식으로 인해 WSA에서 성능 문제가 발생할 수 있습니다. 이 연습 문제에서 제대로 수행되는 다음의 간단한 정규식을 활용할 수 있습니다. **http://[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+**

6. IP 주소 기반의 URL을 차단하려면 Custom URL(맞춤형 URL) 범주를 생성하고 구축합니다.
    a. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Custom Policy Element(맞춤형 정책 요소) > Custom and External URL Categories(맞춤형 및 외부 URL 범주)로 이동합니다.
    b. Add Category(범주 추가)를 클릭합니다.
    c. Category Name(범주 이름)에 예를 들어, IP 기반 URL을 입력합니다.
    d. Regular Expression(정규식) 텍스트 상자가 표시되지 않는 경우 Advanced(고급) 화살표를 클릭합니다.
    e. Regular Expression(정규식) 상자에 http://[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+를 입력합니다.
    f. 페이지 우측 하단의 Submit(제출) 버튼을 클릭하고 Commit Changes(변경 사항 커밋)를 클릭합니다.
7. 방금 생성한 Custom URL(맞춤형 URL) 범주를 차단하려면 글로벌 정책 URL 범주를 설정합니다.
    a. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Web Policies(웹 정책) > Access Policies(액세스 정책)로 이동합니다.
    b. Global Policy(글로벌 정책) 그룹의 URL Filtering(URL 필터링) 상자에서 텍스트를 클릭합니다.
    c. Select Custom Categories(맞춤형 범주 선택) 버튼을 클릭합니다.
    d. 방금 생성한 맞춤형 범주에서 Setting Selection(설정 선택) 드롭다운 메뉴에서 **Include in policy(정책에 포함)**를 선택합니다.
    e. 페이지 우측 하단의 Apply(적용) 버튼을 클릭합니다.
    f. 맞춤형 범주(IP 기반 URL)의 오른쪽에 있는 Block(차단) 열을 선택합니다.
    g. 변경 사항을 제출 및 커밋합니다.
8. http://67.20.81.143에 액세스할 수 없는지 확인합니다(사이트가 처음에 차단되지 않은 경우 모든 브라우저 캐시를 지워야 함). 액세스 로그에서 맞춤형 URL 범주의 첫 번째 4글자를 찾으십시오. 로그는 CLI에서 accesslogs에 다음과 같이 표시될 수 있습니다.

```
1491264101.340 6 198.19.10.36 TCP_DENIED/403 0 GET http://67.20.81.143/ "DCLOUD\wsaproxy@ADrealmDC1"
NONE/- - BLOCK_CUSTOMCAT_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-NONE <C_IP_b,-,-,"-",-,-,-,-,"-",-
,-,-,"-",-,-,"-","-",-,-,-,-,"-","-","-","-","-","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-",-,-,"-"> -
```

# 작업 B: 아카이브 검사

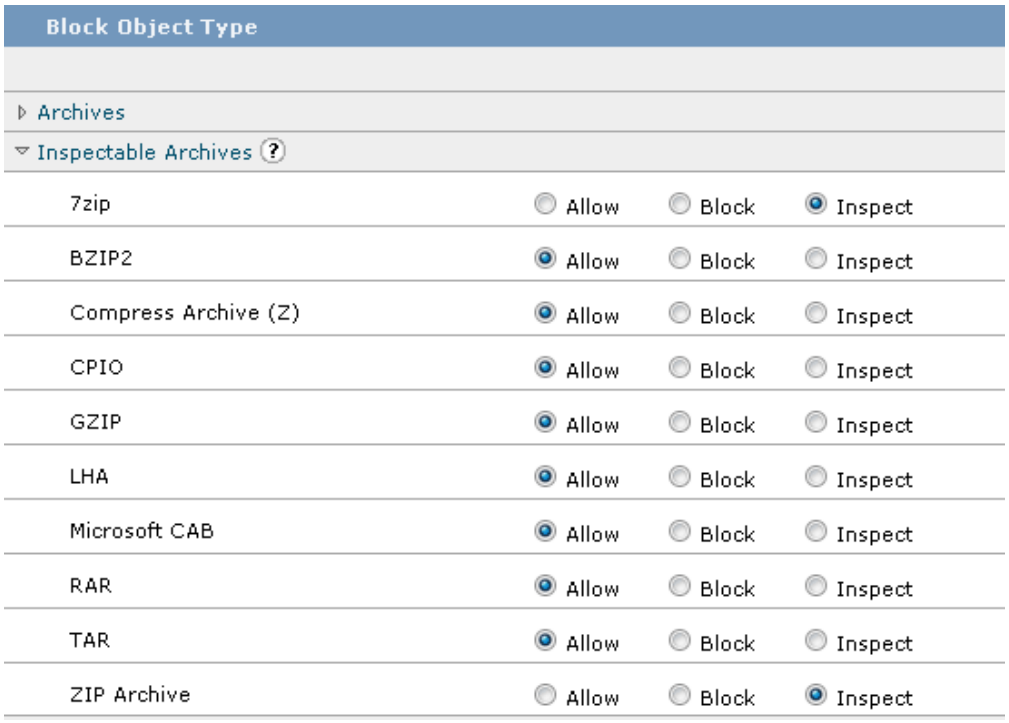
## 서론

개별 액세스 정책의 Inspectable Archives(검사 가능한 아카이브)에 대해 Allow(허용), Block(차단) 또는 Inspect(검사) 유형을 선택할 수 있습니다. Inspectable Archives(검사 가능한 아카이브)는 WSA에서 파일 유형 차단 정책을 적용하기 위해 포함된 파일을 하나씩 검사하도록 확장할 수 있는 아카이브 또는 압축된 파일입니다.

## 단계

1. Inspectable Archives(검사 가능한 아카이브) 설정을 구성합니다.
    a. Security Services(보안 서비스) > Acceptable Use Controls(제한적 사용 제어)로 이동합니다.
    b. 아래로 스크롤하여 Inspectable Archives(검사 가능한 아카이브) 설정으로 이동하고 Edit Archives Settings(아카이브 설정 편집)를 클릭합니다.
    c. Maximum Encapsulated Archive Extractions(캡슐화된 아카이브의 최대 추출 값)의 기본값은 2입니다. 이 값을 5로 설정합니다.
    d. Block Uninspectable Archives(검사 불가능한 아카이브 차단) 확인란을 선택합니다.
    e. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.
2. 아카이브 파일의 액세스 정책을 구성합니다.
    a. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다.
    b. Global Policy(글로벌 정책)에서 Objects(개체) 열의 **No blocked items(차단된 항목 없음)**를 클릭합니다.

c. Inspectable Archives(검사 가능한 아카이브) 옵션을 확장합니다. **ZIP Archive(ZIP 아카이브)**를 **Inspect(검사)**로 설정합니다.

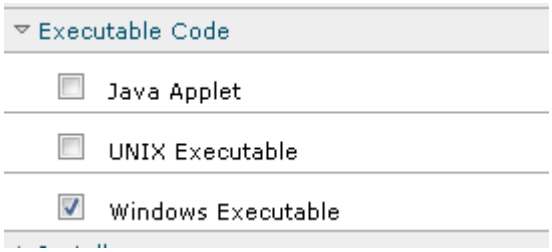



d. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.

e. Chrome에서 https://cisco.box.com/s/mfr48alu4jtgz0dtwpc6w0b808x4zgwx로 이동합니다. **testsetup.zip** 파일을 다운로드하라는 메시지가 표시되어야 합니다. Download를 클릭합니다. 파일을 성공적으로 다운로드해야 합니다.

f. Global Policy(글로벌 정책) > Objects(개체)로 돌아갑니다. 다시 한번 No blocked items(차단된 항목 없음)를 클릭합니다.

g. Executable Code(실행 코드)를 확장하고 Windows Executable(Windows 실행 파일)을 선택합니다.




h. 변경 사항을 제출 및 커밋합니다.

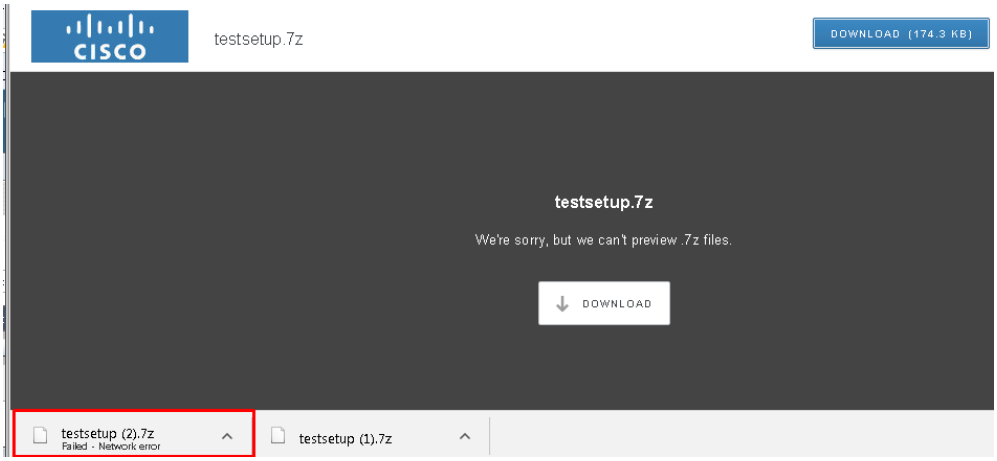
3. 변경 사항을 테스트하고 추적합니다.

   a. Putty를 열고 WSA CLI에 접속합니다.

   b. **tail**을 실행하고 **3**(archiveinspect_logs)을 선택합니다.

4. Chrome에서 이 상자 페이지를 새로 고치거나 https://cisco.box.com/s/mfr48alu4jtgz0dtwpc6w0b808x4zgwx로 다시 이동합니다.

5. **testsetup.zip** 파일 다운로드를 다시 시도합니다. 이번에는 다운로드에 실패해야 합니다. 파일이 즉시 차단되지 않으면 이 파일 내부의 .exe 파일이 차단됩니다.




6. 다음 출력이 표시됩니다. Blocked MIME 및 Inspect MIME 유형과 Verdict 및 차단된 파일을 확인합니다.

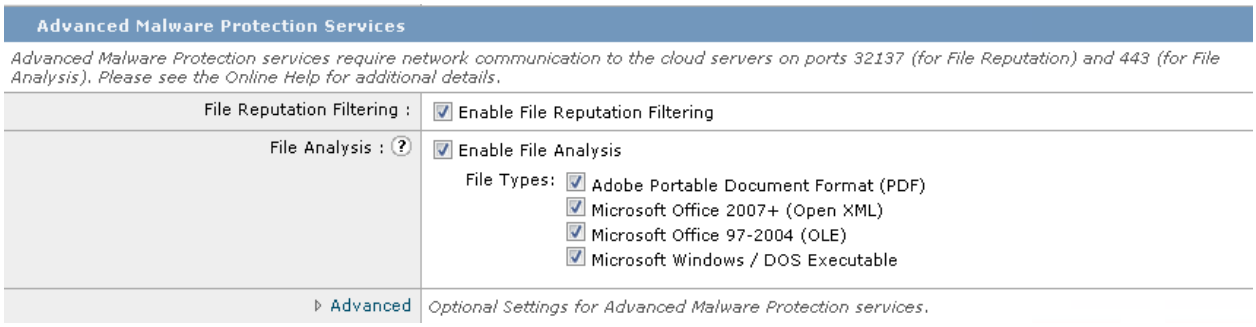
```
05 Apr 2017 19:18:46 (GMT -0700) Info: Request Message from PROX:
05 Apr 2017 19:18:46 (GMT -0700) Info: SoProxId: 152, Method: [Req] RespBodyMimeType: [application/zip; charset=binary]
05 Apr 2017 19:18:46 (GMT -0700) Info: FileName: [download] ResponseBodySize: [178332]Bytes
05 Apr 2017 19:18:46 (GMT -0700) Info: BlockedMimeTypes: [text/x-msdos-batch application/x-dosexec]
05 Apr 2017 19:18:46 (GMT -0700) Info: InspectMimeTypes: [application/zip application/x-7z-compressed]
05 Apr 2017 19:18:46 (GMT -0700) Info: NestLevel: 5, MaxScanSize: [33554432], MaxDiskUse: [1000]MB
05 Apr 2017 19:18:47 (GMT -0700) Info: ------Start of JOBSTATS FileName:[download]------
05 Apr 2017 19:18:47 (GMT -0700) Info: JobID: [5], FileName: [download] JobSize: [178332]
05 Apr 2017 19:18:47 (GMT -0700) Info: Verdict: VERDICT_BLOCKEDMIME  Total Extracted Size [2200]
05 Apr 2017 19:18:47 (GMT -0700) Info: Blocked Mime: [application/x-dosexec], Blocked Filename: [setup.exe]
05 Apr 2017 19:18:47 (GMT -0700) Info: Inspected Nestlevel: [0], Total Nested Archives [0]
05 Apr 2017 19:18:47 (GMT -0700) Info: Num of DataRequests: [11], Files Inspected: [1]
05 Apr 2017 19:18:47 (GMT -0700) Info: Total Job Time: [1094] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: Total Data Download Time: [1088] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: Total UnArchive and Inspection Time: [6] ms
05 Apr 2017 19:18:47 (GMT -0700) Info: ------End of JOBSTATS FileName:[download]------
05 Apr 2017 19:18:47 (GMT -0700) Info: Malloc stats : alloc bytes : 681296, mmap bytes 6174280
```

# 시나리오 4: Advanced Malware Protection

## 작업 A: AMP 파일 평판 및 파일 분석 활성화

### 단계

1. WSA GUI에서 Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판)으로 이동합니다.
    a. Edit Global Settings(전역 설정 편집)를 클릭합니다. (기본적으로 활성화되어 있지 않은 경우 AMP를 활성화하기 위해 다음 작업을 수행하십시오.)
    b. Advanced Malware Protection Services에서 Enable File Reputation Filtering(파일 평판 필터링 활성화) 확인란을 선택합니다. 다음 화면에서 동의를 수락합니다.
    c. 다시 Edit Global Settings(전역 설정 편집)를 클릭합니다.
    d. Advanced Malware Protection Services에서 File Analysis(파일 분석) 확인란을 선택합니다. 다음 화면에서 동의를 수락합니다.
    e. Edit Global Settings(전역 설정 편집)를 다시 클릭합니다.
    f. File Analysis(파일 분석)에서 4개의 파일 유형을 모두 선택합니다.




    g. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.

## 작업 B: 액세스 정책에서 AMP 제어 구성

### 단계

1. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다.
    a. 표의 하단에 있는 Global Policy(글로벌 정책) 행에서 Anti-Malware and Reputation(악성코드 차단 및 평판) 열에 있는 텍스트를 클릭합니다.

b. Advanced Malware Protection 설정에서 Enable File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석 활성화) 확인란을 선택합니다.

c. Known Malicious and High-Risk Files(알려진 악성 고위험 파일)에서 확인 표시를 Block(차단)으로 설정합니다.

d. 페이지 맨 아래에서 Submit(제출)을 클릭합니다.

e. 계속해서 변경 사항을 커밋합니다. (2개의 개별 페이지에서 Commit Changes(변경 사항 커밋)를 클릭합니다.)

# 작업 C: 테스트 파일 평판 필터링

## 단계

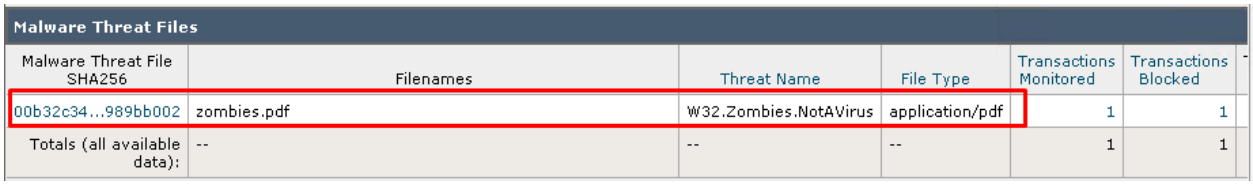
1. 개별 Putty 창에서 실행 중인 accesslogs가 없는 경우, 이 단계에서 실행할 수 있습니다. accesslogs를 추적하는 방법에 대한 자세한 내용은 시나리오 1을 참조하십시오.
2. Chrome을 엽니다.
   a. 다음 웹 사이트로 이동합니다. http://mysite.science.uottawa.ca/rsmith43/zombies.pdf
   b. PDF는 AMP에 의해 차단되어야 합니다. accesslogs에 다음 엔트리가 표시되어야 합니다.

```
1491270162.869 1230 198.19.10.36 TCP_DENIED/403 172449 GET
http://mysite.science.uottawa.ca/rsmith43/zombies.pdf "DCLOUD\wsaproxy@ADrealmDC1"
DIRECT/mysite.science.uottawa.ca application/pdf BLOCK_AMP_RESP_12-DefaultGroup-DefaultGroup-NONE-NONE-
NONE-DefaultGroup <IW_edu,-3.0,0,"-",0,0,0,0,"-",-1,0,-1,"-",0,0,"-","-",-,-,IW_edu,-,"AMP High Risk","-
","Unknown","Unknown","-","-",1121.62,0,-,"Unknown","-
",37,"W32.Zombies.NotAVirus",100,0,"zombies.pdf","00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f
96989bb002",3,-,"-"> -
```

# 작업 D: AMP 파일 평판 보고서

## 단계

1. WSA GUI에서 Reporting(보고) > Advanced Malware Protection으로 이동합니다.
   a. Time Range(시간 범위)를 Hour(시간)로 변경하고 zombie.pdf에 대해 트랜잭션이 차단되었는지 확인합니다. 다음 스크린샷은 출력 예시입니다.



Malware Threat Files

| Malware Threat File SHA256 | Filenames | Threat Name | File Type | Transactions Monitored | Transactions Blocked |
|---|---|---|---|---|---|
| 00b32c34...989bb002 | zombies.pdf | W32.Zombies.NotAVirus | application/pdf | 1 | 1 |
| Totals (all available data): | -- | -- | -- | 1 | 1 |

b. 차단된 파일/모니터링된 파일에 대해 각기 다른 보고 위젯을 선택합니다. Malware Threat Files(악성코드 위협 파일) 표에서 표에 있는 첫 번째 SHA를 클릭합니다.

c. 특정 SHA에 대한 보고서는 선택한 SHA와 일치하는 파일의 다운로드를 시도한 모든 사용자에게 제공됩니다.

d. 페이지 하단의 Files Matched(일치된 파일) 표는 선택한 SHA와 일치하며 다운로드를 시도했던 파일을 보여줍니다. 해당 파일과 일치하는 각각의 트랜잭션으로 구성된 자세한 웹 추적 보고서에 나와 있는 파일 중 하나에 대해 차단된 트랜잭션을 클릭합니다.

## 작업 E: AMP 파일 분석

## 단계

1. WSA GUI에서 Reporting(보고) > File Analysis(파일 분석)로 이동합니다.
2. 파일 이름은 분석된 각 SHA 옆에 나타나며, 이 기능은 새롭게 추가된 기능입니다. 각 결과 옆에 있는 Details(세부 사항)를 클릭하면 Web Tracking(웹 추적)에 액세스할 수 있으며 Results(결과)에 소스 정보가 제공됩니다.
3. 이전으로 돌아가 개별 SHA를 클릭하면 Classification(분류)/Threat Score(위협 점수) 및 Matching(일치) 서명 등의 파일 분석 정보가 제공됩니다. 하단에는 분석한 파일에 대한 모든 상세 정보를 확인할 수 있는 Cisco AMP Threat Grid의 링크가 있습니다.
4. 새로운 기능이 많이 추가되었으므로 이 섹션을 마음껏 살펴보시기 바랍니다.

# 시나리오 5: Cognitive Threat Analytics

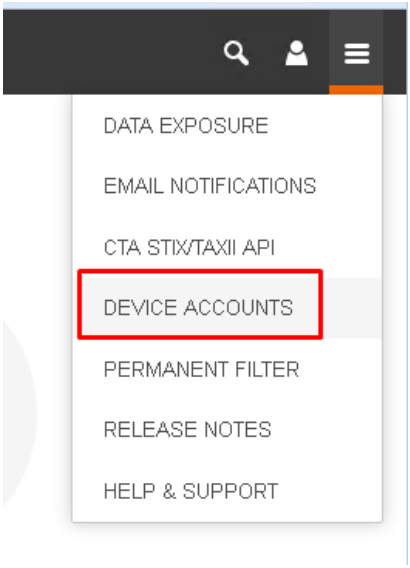
## 서론

Cisco WSA와 CTA가 통합됨으로써 행동 기반 위협 탐지를 통해 공격 확산을 발견하는 시간을 줄일 수 있게 되었습니다. 이 통합을 통해 동작 이상 징후 탐지 알고리즘과 신뢰 모델링을 이용하여 감염 징후를 찾아낼 수 있습니다. 또한 머신 러닝을 사용하여 계속해서 적응해 가므로 자체적으로 위협을 찾아내기 위한 규칙 집합이 필요하지 않습니다.

## 작업 A: CTA 컨피그레이션

## 단계

1. Firefox에서 **https://cognitive.cisco.com**으로 이동합니다.
2. 오른쪽 상단에서 **Customer Login(고객 로그인)**을 클릭합니다.
3. 로그인 접속 정보로 **Web Security(웹 보안)**를 선택합니다.
4. 사용자 이름 **ismeet.singh@gmail.com**, 비밀번호 **Cisco1234%**로 로그인합니다.
5. **Options(옵션)** 탭을 클릭하고 **Device Accounts(디바이스 계정)**를 클릭합니다.




6. Add Device Account(디바이스 계정 추가) 페이지로 이동되면 **Automatic(자동)**을 선택합니다.
7. SCP 또는 HTTPS를 통해 디바이스를 추가하는 옵션이 나타납니다. **SCP**를 선택합니다.

8. WSA[POD NUMBER]-SEVTLAB 규칙을 사용하여 의미 있는 디바이스 이름을 입력하고 ADD ACCOUNT(계정 추가)를 클릭합니다. 예를 들어, 포드 번호가 5인 경우 이름은 WSA5- SEVTLAB이 됩니다.

**참고:** 이름이 사용 중인 경우, 다른 고유한 이름을 선택하십시오.

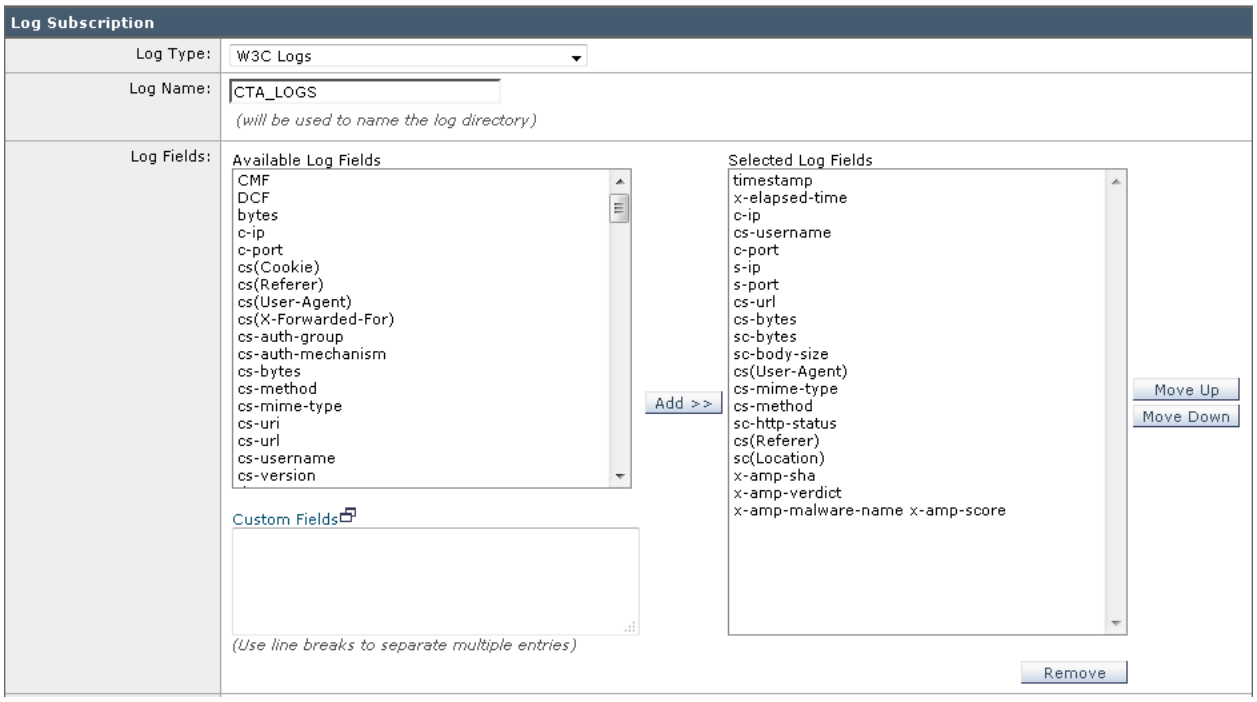
9. 제공된 정보를 참조하고 **이 창을 닫지 마십시오**. 연습 문제를 완료하면 이 페이지로 돌아오게 됩니다.

# 작업 B: WSA 컨피그레이션

## 단계

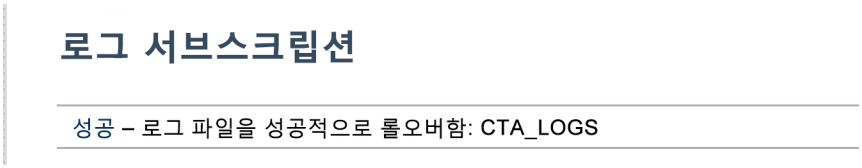
1. WSA UI에서 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**로 이동합니다.
2. **Add Log Subscription(로그 서브스크립션 추가)**을 클릭합니다.
3. Log Type(로그 유형) 풀다운 메뉴에서 **W3C Logs(W3C 로그)**를 선택합니다.
4. Log Name(로그 이름) 필드에 **CTA_LOGS** 같이 로그 디렉토리를 설명하는 이름을 입력합니다.
5. "Selected Log Fields(선택한 로그 필드)" 상자의 모든 항목을 선택하고 **Remove(제거)**를 클릭하여(타임스탬프는 유지) 미리 선택한 Log Fields(로그 필드)를 제거합니다.
6. Custom Fields(맞춤형 필드) 상자에 다음 표에 나와 있는 항목을 입력합니다. 모든 항목을 입력한 후 **Add(추가)**를 클릭합니다. 이 섹션의 예시가 다음의 로그 서브스크립션 그림에 표시됩니다.

| |
|---|
| x-elapsed-time |
| c-ip |
| cs-username |
| c-port |
| s-ip |
| s-port |
| cs-url |
| cs-bytes |
| sc-bytes |
| sc-body-size |
| cs(User-Agent) |
| cs-mime-type |
| cs-method |
| sc-http-status |
| cs(Referer) |
| sc(Location) |
| x-amp-sha |
| x-amp-verdict |
| x-amp-malware-name |
| x-amp-score |

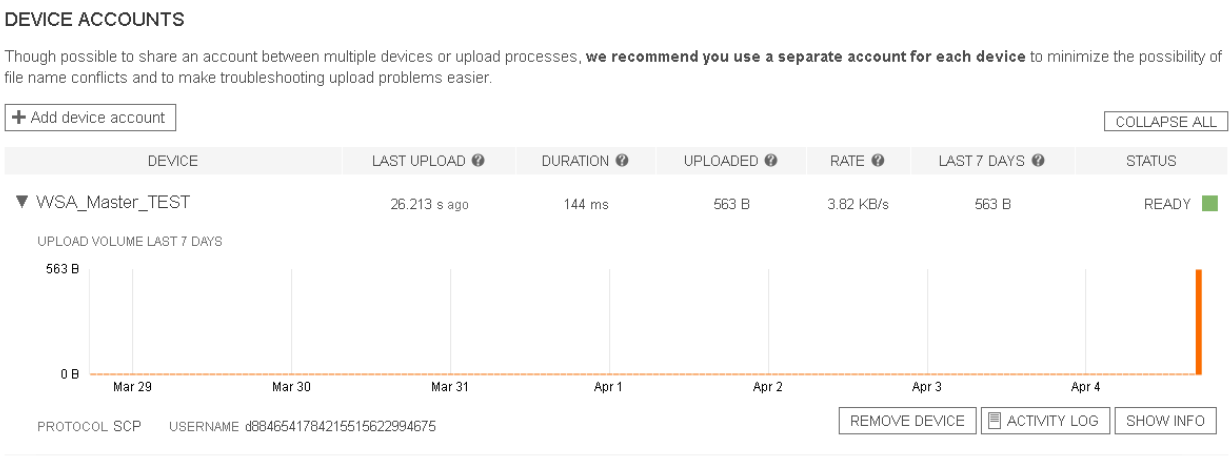



7. 다음 값을 추가합니다.
    a. 파일 크기별 롤오버: 500M
    b. 시간별 롤오버: 맞춤형 시간 간격
    c. 매일 롤오버: 55m
    d. 파일 이름: w3c_log
    e. 로그 압축: 활성화
    f. 검색 방법: 원격 서버에서 SCP
        i. SCP 호스트: etr.cloudsec.sco.cisco.com
        ii. SCP 포트: 22
        iii. 디렉토리: /upload
    g. 사용자 이름: Cisco CTA 포털에서 디바이스에 대해 생성된 사용자 이름을 입력합니다. 디바이스 사용자 이름은 대/소문자를 구분하며 각 프록시 디바이스마다 다릅니다.
    h. Enable Host Key Checking(호스트 키 검사 활성화) 확인란을 선택합니다.
    i. Automatically Scan(자동 스캔) 라디오 버튼을 선택합니다.
8. **Submit(제출)**을 클릭합니다.
9. 워크스테이션에서 메모장을 열고 SSH 키를 복사합니다.
10. **Commit Changes(변경 사항 커밋)**를 클릭합니다. **Commit Changes(변경 사항 커밋)** 버튼을 클릭하기 전에 중요한 설명을 입력했는지 확인합니다.

11. SSH 키를 복사했으면 CTA 포털로 다시 이동하여 **Finish(마침)**를 클릭합니다.
12. 생성된 새로운 디바이스 인스턴스 옆에 있는 **Provide SSH Key(SSH 키 입력)**를 클릭합니다. 키를 붙여 넣고 **Save SSH Key(SSH 키 저장)**를 클릭합니다.
13. 1~2분 후에 **Option(옵션) > Device Accounts(디바이스 계정)**를 클릭합니다. WSA가 등록되면 상태가 Provisioning(프로비저닝)에서 Ready(준비)로 변경됩니다.
14. 연결이 성공적인지 검증하려면 WSA로 다시 이동하여 **Log Subscriptions(로그 서브스크립션)**를 클릭합니다.
15. 생성한 로그 서브스크립션 옆에 있는 Rollover(롤오버) 확인란을 클릭합니다. 아래로 스크롤하여 **Rollover Now(지금 롤오버)**를 클릭합니다.
16. 성공 메시지가 반환되어야 합니다.




17. CTA 포털으로 다시 이동합니다. **Options(옵션)**을 클릭하고 **Device Accounts(디바이스 계정)**를 다시 클릭합니다. 이제 WSA에 로드가 CTA에 성공적으로 업로드되었음을 의미하는 데이터 세부 정보가 표시됩니다.

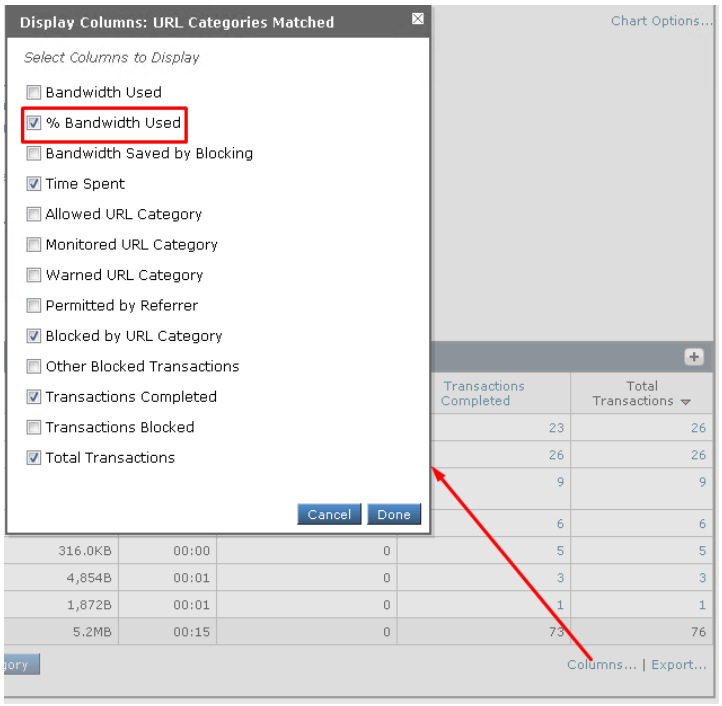


# 시나리오 6:  보고 및 웹 추적

## 작업 A: 보고서 활용

## 단계

1. WSA GUI에서 Reporting(보고) > URL Categories(URL 범주)로 이동합니다.
    a. 총 트랜잭션을 기준으로 최상위 URL 범주를 확인합니다.
    b. 차단 및 경고가 있는 트랜잭션을 기준으로 최상위 URL 범주를 확인합니다.
    c. URL Categories Matched(일치된 URL 범주) 표의 경우, Bandwidth Used(사용된 대역폭)를 %Bandwidth Used(사용된 대역폭 %)로 바꿉니다.
        i. 표의 오른쪽 하단 열에서 Columns(열)... 텍스트를 클릭합니다.
        ii. Bandwidth Used(사용된 대역폭) 상자의 선택을 취소합니다. **%Bandwidth Used(사용된 대역폭 %)** 상자를 선택합니다.
        iii. Done(완료)을 클릭합니다.




    d. 적절한 열의 헤더를 클릭하여 %Bandwidth Used(사용된 대역폭 %)를 기준으로 표를 정렬합니다.
    e. URL 범주를 기준으로 차단된 표를 정렬하고 왼쪽 열에서 범주 이름(Gambling(도박)일 수 있음)을 클릭합니다.

f. 이 범주에서 최상위 사이트와 최상위 사용자를 확인합니다(총 트랜잭션 기준).

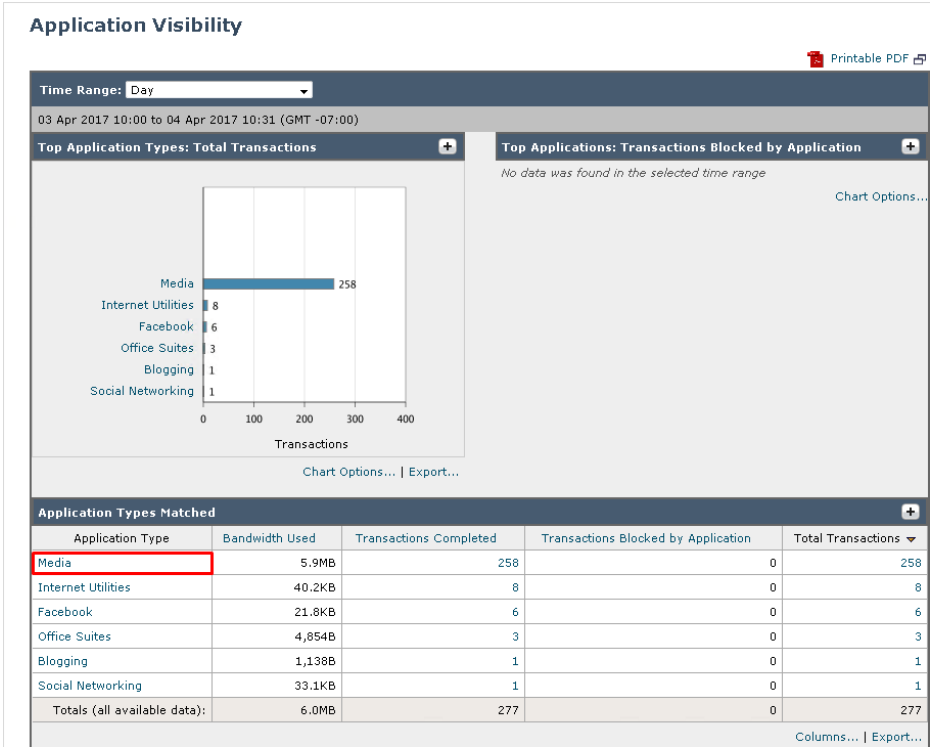
g. Web Users(웹 사용자) 표에서 최상위 사용자 이름을 클릭합니다. 이 사용자에 대한 자세한 정보를 확인합니다.

2. 애플리케이션 가시성

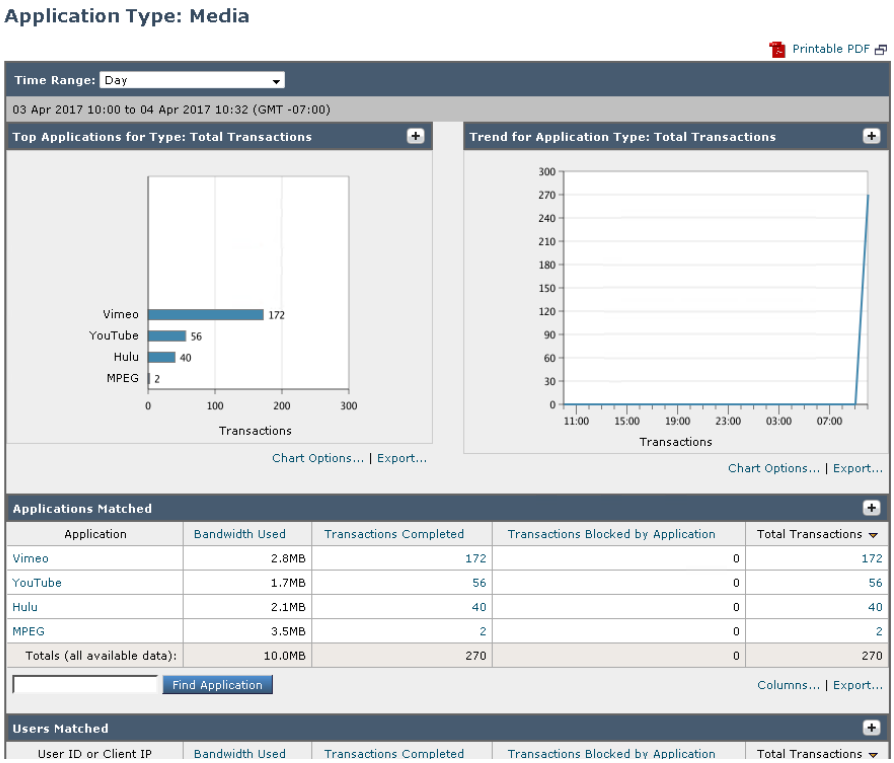
a. Chrome으로 이동하여 다양한 비디오 웹 사이트(예: youtbe.com, hulu.com, vimeo.com, order.hbonow.com)를 둘러봅니다.

b. WSA GUI에서 Reporting(보고) > Application Visibility(애플리케이션 가시성)로 이동합니다.

c. Application Types Matched(일치한 애플리케이션 유형) 표에 Media(미디어)가 표시되는지 확인합니다.



d. Media(미디어)를 클릭합니다. 스트리밍 비디오 사이트의 트랜잭션 세부 정보가 표시되어야 합니다.




3. WSA GUI에서 Reporting(보고) > Anti Malware(악성코드 차단)로 이동합니다.

**참고:** EICAR 테스트 파일이 Malware Threats(악성코드 위협) 표에 나와 있습니다. 이는 eicar.com 테스트 파일 다운로드를 시도했기 때문입니다.

4. 다음과 같은 기타 보고서도 간단하게 살펴봅니다.

   a. 보고 > 클라이언트 악성코드

   b. 보고 > 사용자

   c. 보고 > 웹 사이트

   d. 보고 > 웹 평판 필터

## 작업 B: 웹 추적 활용

## 단계

1. WSA GUI에서 Reporting(보고) > Web Tracking(웹 추적)으로 이동합니다. Search(검색) 상자에서 다음 작업을 수행합니다.

   a. Time Range(시간 범위)의 경우, Day(하루)를 선택합니다.

   b. 사용자/클라이언트 IP는 비워 둡니다.

c. Website(웹 사이트)에는 cisco.com 또는 앞에서 검색한 웹사이트를 입력합니다.

d. Transaction Type(트랜잭션 유형)에는 All Transactions(모든 트랜잭션)를 선택합니다.

e. 검색 버튼을 클릭합니다.

f. Results(결과) 표에서 표에서 Display Details(세부 정보 표시)... 텍스트를 클릭합니다.

g. 1개 이상의 트랜잭션에 대해 RELATED TRANSACTIONS(관련 트랜잭션) 텍스트를 클릭합니다.

h. 페이지와 관련된 HTML 구성 요소(이미지, JavaScript 등)가 표시되는지 확인합니다.


2. 웹 추적 검색을 다음과 같이 수정합니다. Search(검색) 상자에서 다음 작업을 수행합니다.

a. 웹 사이트를 비워 둡니다.

b. Transaction Type(트랜잭션 유형)을 Blocked(차단됨)로 변경합니다.

c. 검색 버튼을 클릭합니다.

d. Results(결과) 표에서 트랜잭션 중 하나를 클릭합니다.

e. 트랜잭션이 차단된 이유와 위협에 대한 상세 정보도 확인합니다.

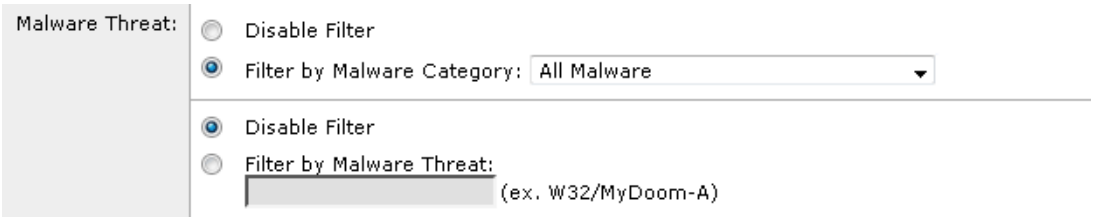
3. 웹 추적 검색을 다음과 같이 수정합니다. Search(검색) 상자에서 다음 작업을 수행합니다.

a. Transaction Type(트랜잭션 유형)을 All Transactions(모든 트랜잭션)로 다시 변경합니다.

b. Advanced(고급)를 클릭하여 고급 기준을 사용하여 트랜잭션을 검색합니다.

i. Malware Threat(악성코드 위협)에서 Filter by Malware Category(악성코드 범주별 필터링) 라디오 버튼을 선택합니다.

ii. 드롭다운 메뉴에서 "All Malware(모든 악성코드)"를 선택합니다.




c. 검색 버튼을 클릭합니다.

d. Results(결과) 상자에서 다양한 사용자의 트랜잭션이 차단된 것을 확인할 수 있어야 합니다.

3. 웹 추적 검색을 다음과 같이 수정합니다.

4. 검색 상자에서 고급 기준을 사용하여 트랜잭션을 검색하려면 **Advanced(고급)**를 클릭합니다.

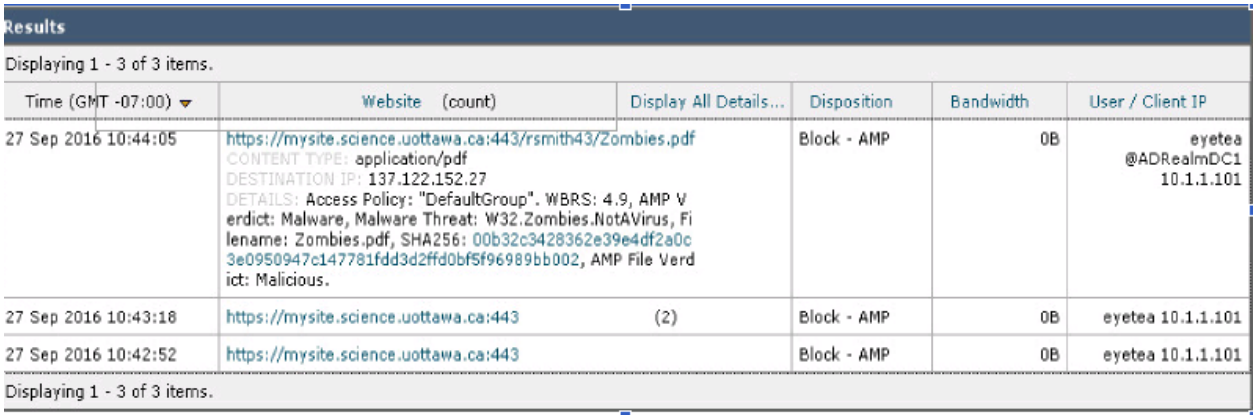
a. Advance Malware Protection에서 Filter by Filename(파일 이름별 필터링) 라디오 버튼을 선택합니다.

b. Filename(파일 이름) 텍스트 필드에 "Zombies.pdf"를 입력합니다.

c. Time Range(시간 범위)로 "Day(하루)"를 선택합니다.

d. 검색 버튼을 클릭합니다.

e. Results(결과) 상자에 다음과 유사한 화면이 표시됩니다.



Results

Displaying 1 - 3 of 3 items.

| Time (GMT -07:00) | Website (count) | Display All Details... | Disposition | Bandwidth | User / Client IP |
|---|---|---|---|---|---|
| 27 Sep 2016 10:44:05 | https://mysite.science.uottawa.ca:443/rsmith43/Zombies.pdf<br>CONTENT TYPE: application/pdf<br>DESTINATION IP: 137.122.152.27<br>DETAILS: Access Policy: "DefaultGroup". WBRS: 4.9, AMP Verdict: Malware, Malware Threat: W32.Zombies.NotAVirus, Filename: Zombies.pdf, SHA256: 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002, AMP File Verdict: Malicious. | | Block - AMP | 0B | eyetea @ADRealmDC1 10.1.1.101 |
| 27 Sep 2016 10:43:18 | https://mysite.science.uottawa.ca:443 | (2) | Block - AMP | 0B | eyetea 10.1.1.101 |
| 27 Sep 2016 10:42:52 | https://mysite.science.uottawa.ca:443 | | Block - AMP | 0B | eyetea 10.1.1.101 |

Displaying 1 - 3 of 3 items.

# 시나리오 7: 리퍼러(Referrer) 헤더

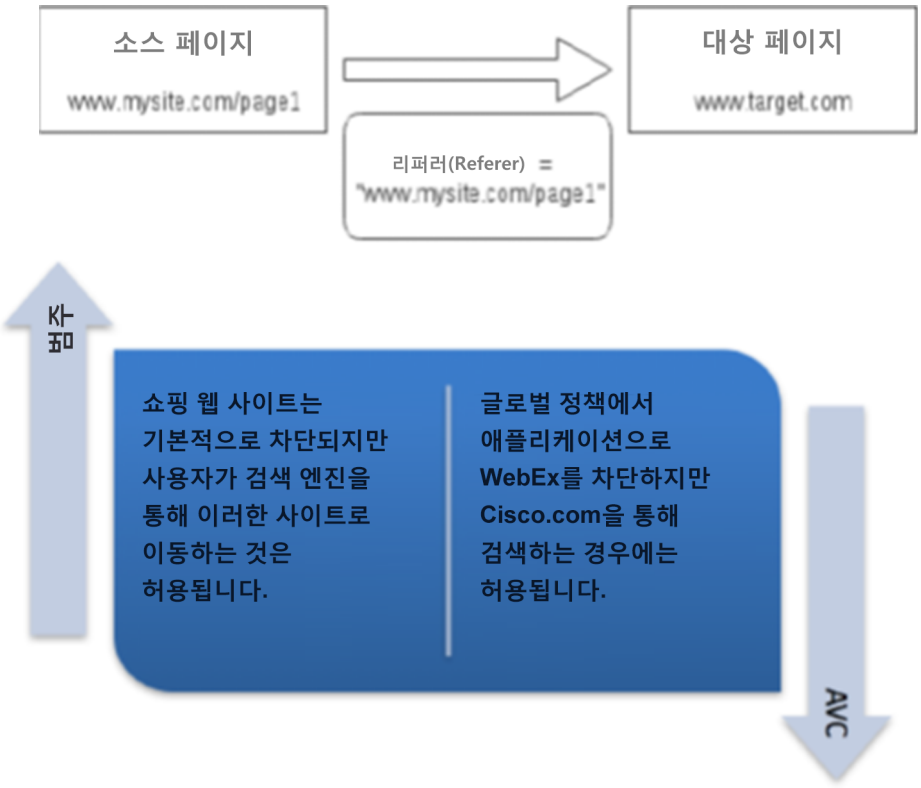
## 서론

리퍼러(Referrer)는 현재 웹 페이지를 요청한 웹 페이지를 식별하는 HTTP 헤더 필드입니다. 리퍼러(Referrer) 필드를 사용하여 웹 사이트를 검색한 URL을 찾아내고 이를 사용하여 액세스 정책을 정의합니다.

본 실습에서는 다음의 리퍼러(Referrer) 헤더를 사용하는 2개의 활용 사례를 다룹니다.

1: **범주** - 사전 정의된/맞춤형 차단 범주에 포함되지만 특정 범주에서 참조되는 URL에 대한 액세스를 활성화합니다.

2: **AVC**- 차단되어 있지만 특정 범주에서 참조되는 애플리케이션에 대한 액세스를 활성화합니다.




## 작업 A: 범주

## 단계

1. WSA GUI에서 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**로 이동합니다.

2. **Add Policy(정책 추가)**를 클릭합니다.
3. Policy Name(정책 이름)에 Referrer Header 이름을 입력합니다.
4. Identification Profiles and Users(ID 프로파일 및 사용자)에서 그룹 및 사용자를 선택하고 **No Group Entered(입력된 그룹 없음)**를 클릭합니다.
5. Directory Search(디렉토리 검색)에서 **DCLOUD\Nurses**를 선택하고 **Add(추가)**를 클릭합니다.
6. **Done(완료)**을 클릭합니다.
7. **Submit(제출)**을 클릭합니다.
8. 이제 Referrer Header Policy(리퍼러 헤더 정책)에서 **URL Filtering(URL 필터링)**을 클릭합니다.
9. 아래로 스크롤하여 Shopping(쇼핑) > Block(차단)으로 이동합니다.
10. **Submit(제출)**을 클릭하고 코멘트를 입력한 후 **Commit Changes(변경 사항 커밋)**를 클릭합니다.
11. WSA CLI에서 다음 명령을 실행합니다(**authcache**를 먼저 실행하고 **flushall** 실행).

```
wsa-hq1.dcloud.cisco.com> authcache


Choose the operation you want to perform:
- FLUSHALL - Flush all entries from auth cache
- FLUSHUSER - Flush specific user entry from auth cache
- LIST - List all entries from auth cache
- SEARCH - Search all entries from auth cache
[]> flushall

Are you sure that you want to flush all entries? [Y]> Y

2 entries in authentication cache flushed
```

12. IE에서 쿠키와 사용자 접속 정보를 지우고 브라우저를 재시작합니다.
13. 사용자 이름 **aroberts**, 비밀번호 **C1sco12345**로 로그인합니다.
14. www.bestbuy.com 또는 www.Amazon.com을 찾습니다. 해당 사이트는 차단되며 EUN을 받습니다(원하는 대로 작동).
15. 이제 Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책) > Referrer Header(리퍼러 헤더) > URL Filtering(URL 필터링)으로 다시 돌아갑니다. 아래로 스크롤하여 Check and Enable Referrer Exceptions(리퍼러 예외 확인 및 활성화)로 이동합니다.
16. **Set Exception for content Referred by these categories(이러한 범주에서 참조하는 콘텐츠에 대한 예외 설정)**에서 **Select Categories(범주 선택)**를 선택합니다.
17. **Search Engines and Portals(검색 엔진 및 포털)**를 선택하고 Done(완료)을 클릭합니다.
18. 아래로 스크롤하여 **Set Exception for This Referred Content(이 참조 콘텐츠에 대한 예외 설정)**에서 **Embedded/Referred content(임베드/참조 콘텐츠)**를 선택합니다.
19. **Select Categories(범주 선택) > Shopping(쇼핑)**을 클릭한 다음 **Done(완료)**를 클릭합니다(참고: 이 범주가 유일하게 차단된 경우에만 강조 표시됨).

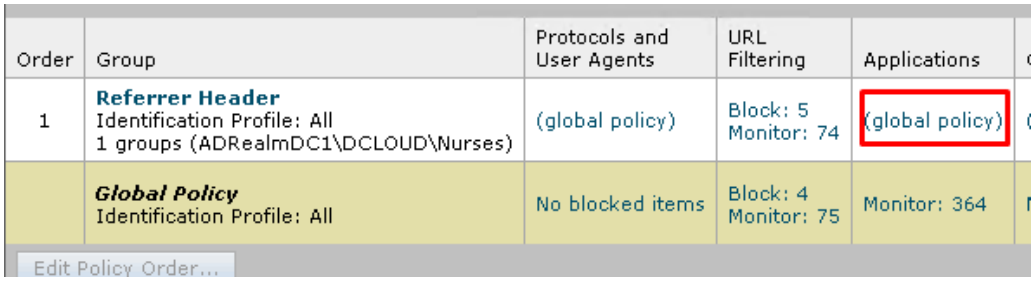
20. **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.
21. www.amazon.com으로 다시 이동합니다. 이 사이트는 차단되어야 합니다.
22. 이제 www.google.com으로 이동하고 "amazon"을 검색합니다.
23. 첫 번째 결과(www.amazon.com)를 클릭하면 www.amazon.com로 리디렉션됩니다. (www.google.com을 통해 이동하므로 이제 www.amazon.com을 통해 검색할 수 있습니다.)
24. 이제, 해당 리퍼러 헤더의 보고서를 찾으려면 다음 경로에서 보고서를 선택합니다.
    a. WSA GUI > Reporting(보고) > Web Sites(웹 사이트)
    b. Time Range(시간 범위) > Day(하루)를 선택합니다.
    c. Top Domains(상위 도메인) > Chart Option(차트 옵션)에서 Permitted by Referrer(리퍼러에서 허용됨)를 선택하고 Save(저장)를 클릭합니다.
    d. 이렇게 하면 리퍼러에서 허용되는 상위 도메인이 표시됩니다.
    e. 또한 URL 범주에 대한 리퍼러 보고서를 보려면 WSA GUI > Reporting(보고) > URL Categories(URL 범주)로 이동합니다.

**참고:** 보고서 결과가 즉시 나타나지 않을 경우 다음 시나리오를 완료한 이후에 다시 확인하십시오. 이 보고서가 나타나는 데 다소 시간이 걸릴 수 있습니다,

## 작업 B: AVC

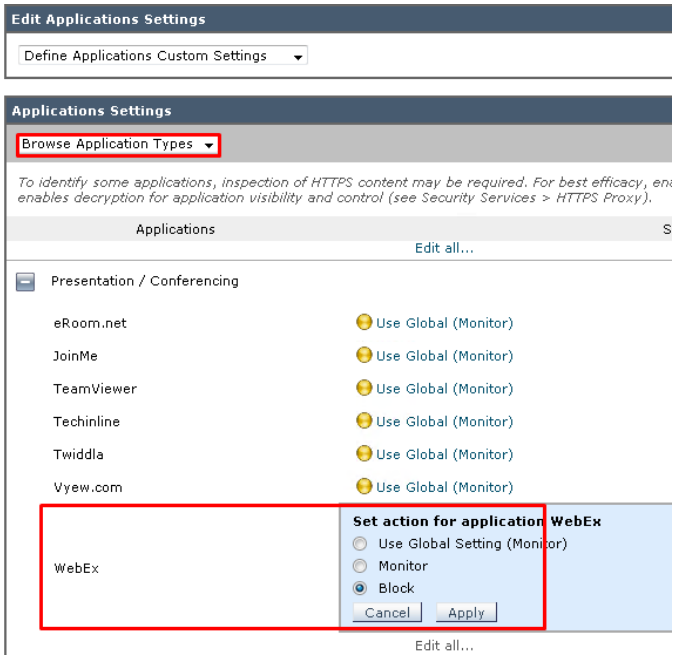
## 단계

1. 애플리케이션으로 WebEx를 차단합니다.
    a. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책) > "Referrer Header" Policy("리퍼러 헤더" 정책)로 이동하여 Applications(애플리케이션)의 링크를 클릭합니다.




    b. Edit Application Settings(애플리케이션 설정 편집) > Define Application Custom Settings(애플리케이션 맞춤형 설정 정의) > Presentation/Conferencing (+)(프레젠테이션/컨퍼런싱 (+))

c. WebEx > Use Global(Monitor)(글로벌 사용(모니터)) > Block(차단) > Apply(적용) > Submit(제출) > Commit Changes(변경 사항 커밋)(2)

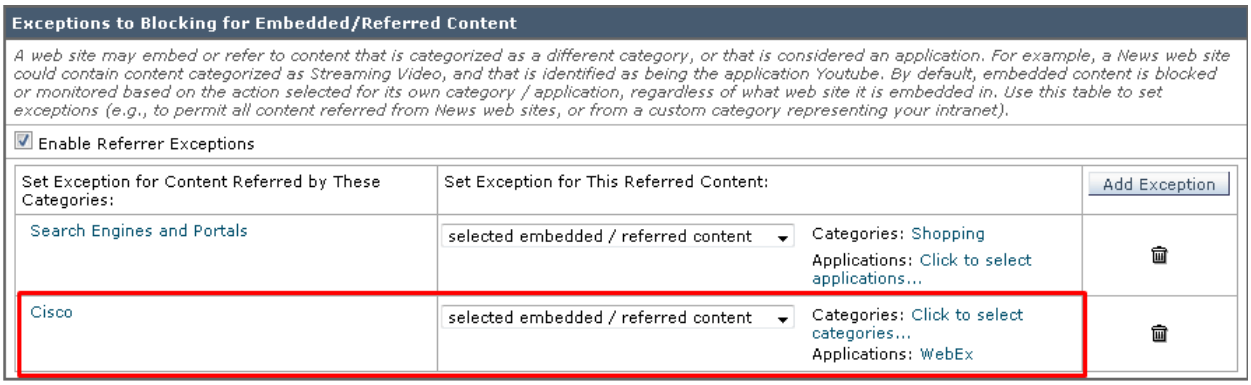



d. www.WebEx.com을 검색합니다. 이 URL은 AVC에 의해 차단되어야 합니다.

2. WSA GUI로 다시 이동하여 Web Security Manager(웹 보안 관리자) > Custom & External URL Categories(맞춤형 및 외부 URL 범주)로 이동합니다. Add Category(범주 추가)를 클릭합니다.
3. Category Name(범주 이름)을 "Cisco"로 지정하고 Category Type(범주 유형)을 **Local Custom Category(로컬 맞춤형 범주)**로 선택합니다.
4. Sites(사이트)에서 **.cisco.com** 및 **www.webex.com**을 선택합니다(참고: WebEx가 자체 리퍼러로 추가됨).

**참고:** .cisco와 www.cisco.com이 아닌 항목이 여기에 추가되었는지 확인합니다. 이렇게 하면 Cisco.com 아래의 모든 하위 도메인도 이해됩니다.

5. **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.
6. 다음으로, Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책) > Referrer Header(리퍼러 헤더) > URL Filtering(URL 필터링)으로 이동합니다.
7. 아래로 스크롤하여 Referrer Exceptions(리퍼러 예외)로 이동합니다.
8. **Add Exception(예외 추가)**을 클릭합니다.
9. **Select Categories(범주 선택)**를 클릭하고 Cisco를 추가합니다. **Done(완료)**을 클릭합니다.
10. **Set Exception for This Referred Content(이 참조 콘텐츠에 대한 예외 설정)**에서 **Embedded/Referred content(임베드/참조 콘텐츠)**를 선택합니다.
11. 이제 Application(애플리케이션)에서 **Applications: WebEx(애플리케이션: WebEx)**를 추가합니다. Done(완료)을 클릭합니다.



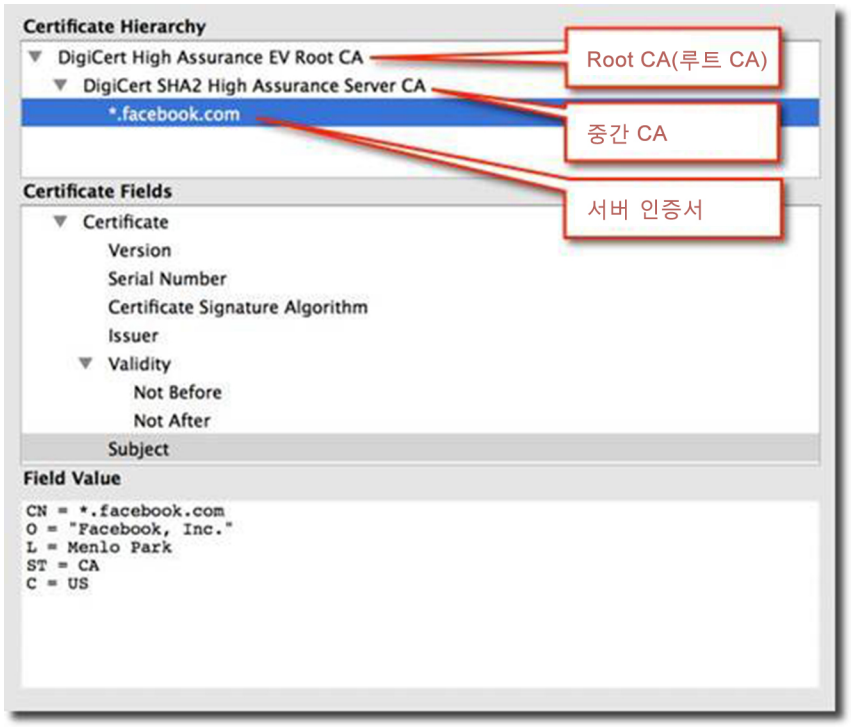

12. **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.
13. IE에서 www.cisco.com을 찾고 검색 유형 키워드에 "webexwebex"를 사용합니다.
14. 이렇게 하면 www.webex.com이 첫 번째 검색 URL로 나타납니다.
15. 이 URL을 클릭하면 webex.com 웹 사이트가 열립니다.
16. 이제, 해당 리퍼러 헤더의 보고서를 찾으려면 WSA GUI > Reporting(보고) > Web Sites(웹 사이트)에서 다음 보고서를 클릭합니다.
17. Time Range(시간 범위) > Day(하루)를 선택하고 Top Domains(상위 도메인) > Chart Option(차트 옵션)에서 Permitted by Referrer(리퍼러에서 허용됨)를 선택합니다. 이렇게 하면 리퍼러에서 허용되는 상위 도메인이 표시됩니다.
18. 또한 URL 범주에 대한 리퍼러 보고서를 보려면 Reporting(보고) > URL Categories(URL 범주)로 이동합니다.

# 시나리오 8: 중간 인증서

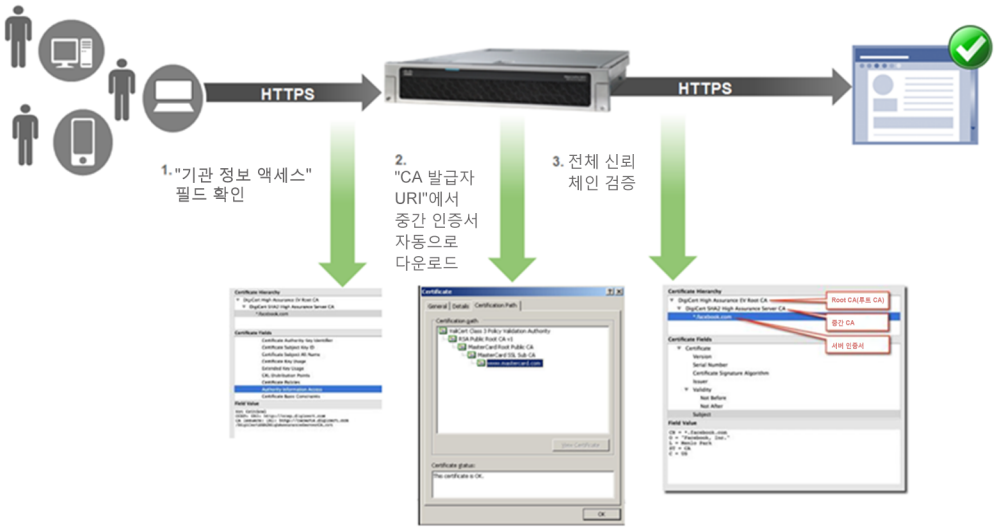
## 서론

HTTPS 웹 사이트에 연결할 경우 웹 서버는 SSL 인증서를 제출할 때 전체 신뢰 체인을 보낼 수 있습니다. 어떤 경우에는 신뢰 체인 완료에 실패하고 서버 인증서만 전송합니다. 이 경우 클라이언트에는 신뢰 체인을 완료할 수 없다는 오류가 표시됩니다.

**예상 신뢰 체인**




**WSA가 누락된 인증서를 위해 수행하는 작업:**



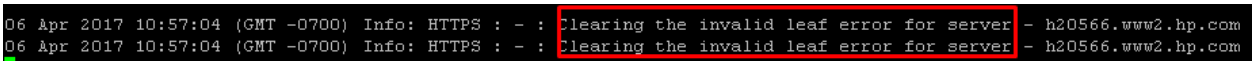
# 단계

1. Firefox 브라우저를 엽니다.
2. URL > **https://www.sslshopper.com/ssl-checker.html**로 이동하여 링크가 깨지지 않았는지 테스트합니다.
3. 링크가 깨지지 않았는지 테스트하기 위해 위의 사이트에서 다음 링크를 입력합니다.

| |
|---|
| https://businessportal.alcatel-lucent.com |
| https://h20566.www2.hp.com/hpsc/wc/public/home |

4. 아래 스크린샷과 유사한 결과를 확인해야 합니다.


5. Putty 클라이언트를 열고 wsa-hq1에 로그인합니다.
6. **tail httpslog**를 실행합니다.
7. Chrome를 열고 위에 나와 있는 웹 사이트로 이동합니다. 두 페이지를 성공적으로 로드해야 합니다.
8. 중간 인증서가 유효하지 않거나 누락된 경우, CLI 명령에서 "Clearing the Invalid leaf error for server - <URL>" 오류 메시지를 받게 됩니다.



# 시나리오 9:  서드파티 피드

## 서론

이 기능은 정책을 WSA에서 생성할 수 있는 기반이 되는 데이터를 획득하기 위해 WSA가 외부(또는 서드파티) 피드와 통신할 수 있도록 지원합니다. 이 데이터는 피드 콘텐츠가 변경되므로 주기적으로 동적 업데이트가 수행됩니다.

외부 피드 서버에서 가져온 데이터는 WSA의 맞춤형 URL 범주에 추가됩니다. 새로운 데이터가 있을 때마다 이 데이터를 가져오게 되고 그 결과 일치하는 맞춤형 URL 범주가 업데이트됩니다.

WSA 관리자는 URL 범주를 기반으로 적절한 정책을 생성할 수 있습니다. 예를 들어, 특정 URL 범주(블랙리스트)와 일치하는 트래픽을 차단하는 정책을 생성하고 특정 URL 범주(화이트리스트)와 일치하는 트래픽에 대한 서비스를 우회하는 정책을 생성할 수 있습니다.

WSA는 최대 5개의 외부 피드 서버를 지원합니다. 피드 서버에서 획득한 데이터와 WSA 컨피그레이션에 저장된 데이터는 WSA가 재시작되어도 지속됩니다.

이 연습 문제에서 Microsoft Office 365 서비스와 관련된 IP와 URL 목록을 포함하는 공식 Microsoft Office 365 피드를 사용합니다.

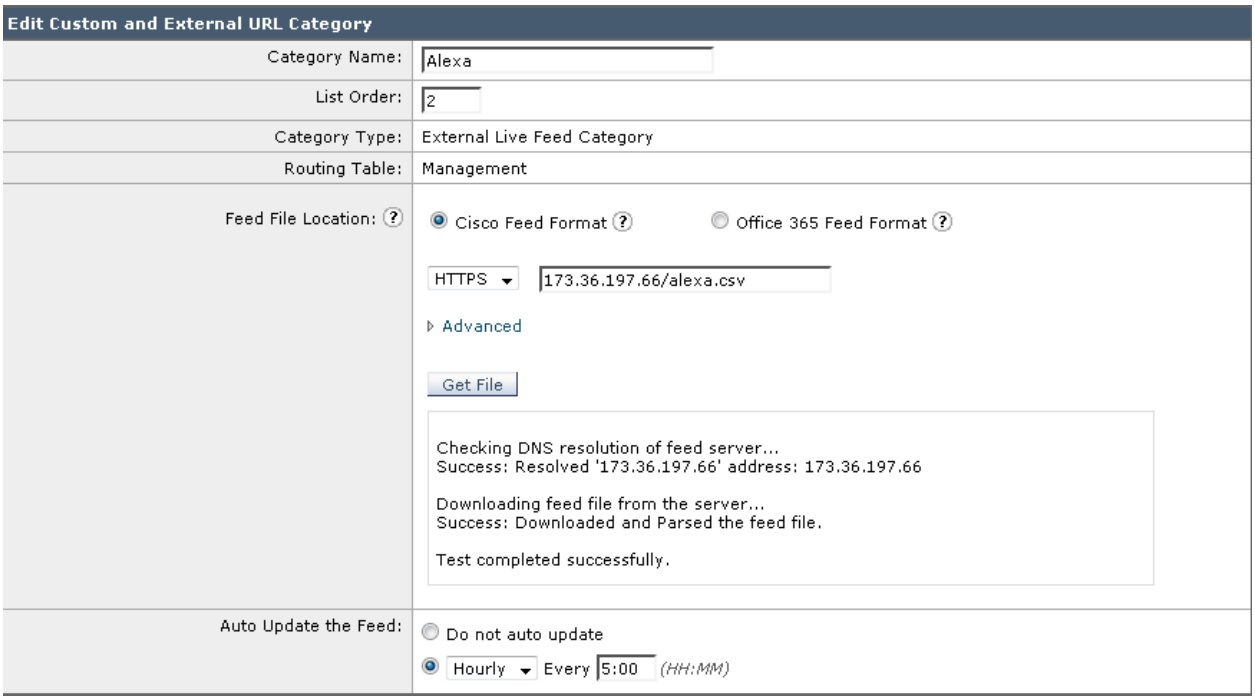
맞춤형 및 외부 URL 범주


# 작업 A: 서드파티 피드 통합

## 단계

1. Web Security Manager(웹 보안 관리자) > Custom and External URL Categories(맞춤형 및 외부 URL 범주)로 이동합니다.
2. Add Category(범주 추가) > Category Name(범주 이름) > Alexa를 클릭합니다.

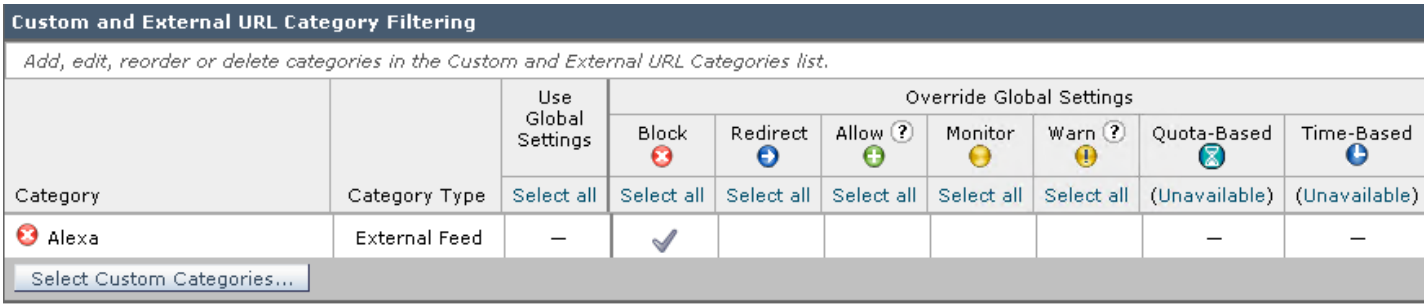
3. 그런 다음 Category Type(범주 유형)을 External Live Feed Category(외부 라이브 피드 범주) > Cisco Feed(Cisco 피드) > HTTPS > 링크로 변경합니다.
4. Get File(파일 다운로드)를 클릭합니다(참고: 인증 필요 없음).
5. Auto Update the Feed(피드 자동 업데이트) > 5시간 마다를 선택합니다.




6. **Submit**을 클릭합니다.
7. 제출 후 Feed Content(피드 콘텐츠) > View(보기)를 확인하고(외부 피드에서 가져온 모든 URL을 표시) 변경 사항을 커밋합니다.
8. 변경 사항을 커밋한 후 Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다. Referrer Header(리퍼러 헤더)가 목록 상단에 있는지 확인합니다. 그렇지 않으면, Group(그룹)에서 Referrer Header(리퍼러 헤더) 텍스트를 클릭합니다. 이 정책 또한 목록 상단으로 이동되었는지 확인합니다.


9. 다시 Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책) > Referrer Header(리퍼러 헤더) > URL Filtering(URL 필터링)으로 이동합니다.
10. Select Custom Categories(맞춤형 범주 선택) > Alexa > Include in Policy (정책에 포함) > Apply(적용)를 클릭합니다.

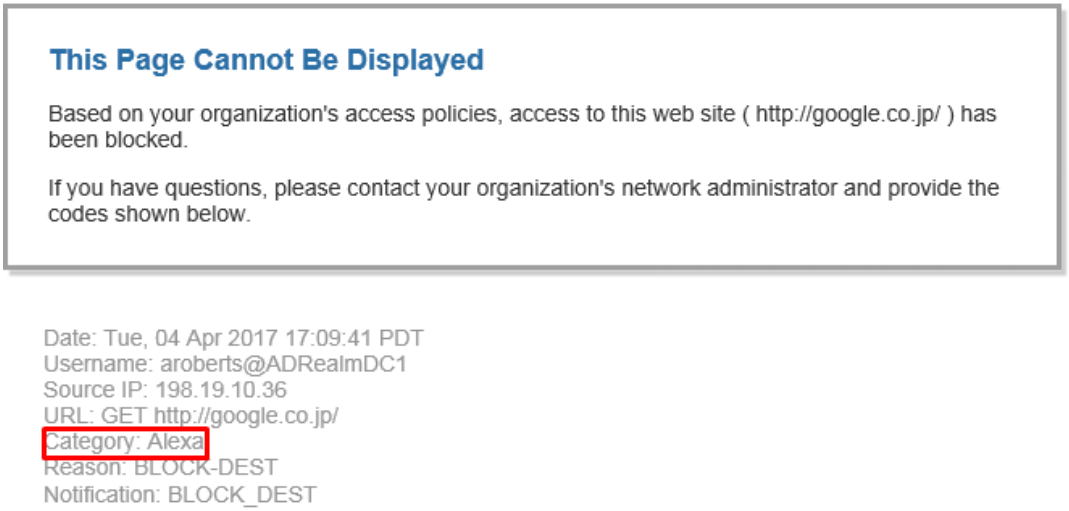
11. Override Global Settings(글로벌 설정 재정의) 창에서 Block(차단)을 선택하여 제출을 클릭하고 변경 사항을 커밋합니다.




12. 이제 IE에서 Web Security Appliance에서 자동으로 차단되는 다음 웹 사이트를 찾아보십시오.

| |
|---|
| taobao.com |
| msn.com |
| yahoo.co.jp |
| linkedin.com |
| google.co.jp |
| sina.com.cn |
| weibo.com |
| Wikipedia.org |
| yandex.ru |

13. 이 사이트는 맞춤형 범주에 따라 차단되어야 합니다.

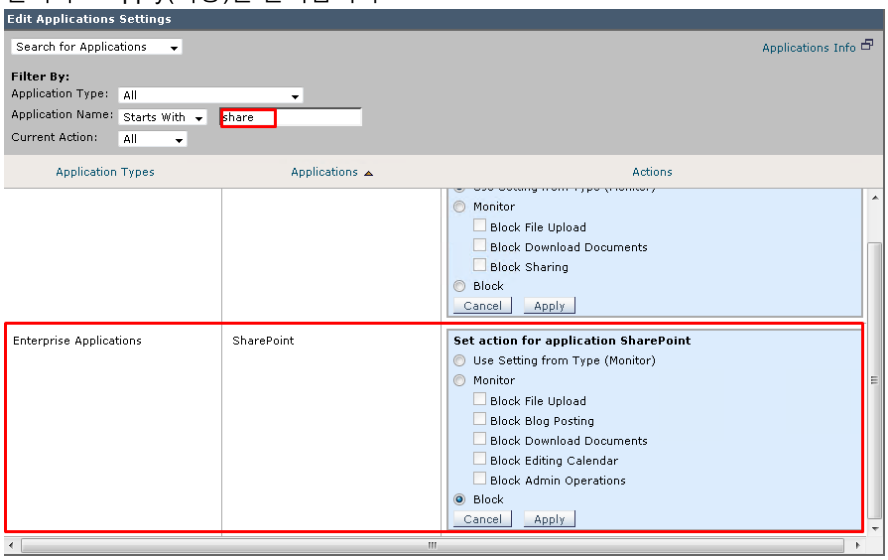



**참고:** 이 피드는 지속적으로 업데이트되므로 위 사이트 중 일부는 대부분 차단되어야 할 대상이지만 차단되지 않을 수 있습니다.

# 작업 B: Office 365 호환성

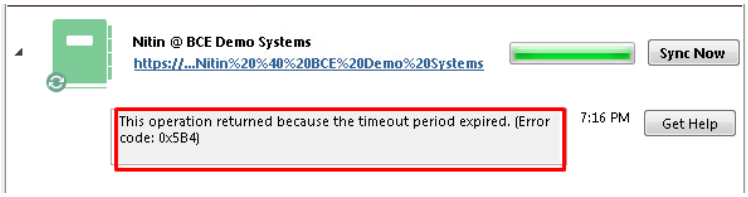
## 단계

1. Office 365 애플리케이션의 AVC 차단을 설정합니다.
    a. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다.
    b. Global Policy(글로벌 정책)에서 Applications(애플리케이션) 열을 클릭합니다.
    c. 아래로 스크롤하여 Edit Application Settings(애플리케이션 설정 편집)로 이동하고 Search for Applications(애플리케이션 검색)를 선택합니다.
    d. 텍스트 필드에 **Sharepoint**를 입력합니다.
    e. 두 가지 애플리케이션 유형에 나타납니다. Enterprise Applications(엔터프라이즈 애플리케이션)에서 **Block(차단)**을 선택하고 Apply(적용)를 클릭합니다.



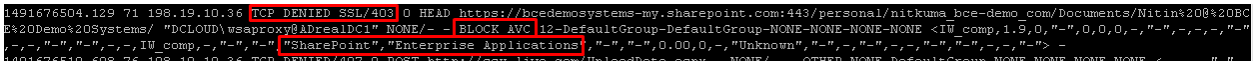

    f. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.
    g. 다음으로, 작업 표시줄에서 OneNote 애플리케이션을 클릭합니다. 
    h. 페이지의 아무 곳에나 메모를 입력합니다.
    i. File(파일)로 이동하여 View Sync Status(동기화 상태 보기)를 클릭합니다.
    j. 라디오 버튼을 Sync manually(수동 동기화)로 설정하고 Sync Now(지금 동기화) 버튼을 클릭합니다.

k. 다음 오류가 표시되어야 합니다.




l. Close(닫기)를 클릭합니다.

m. 또는 WSA CLI에서 **tail accesslogs**를 실행할 수 있습니다. 다음 엔트리를 참조하십시오.




**참고:** OneNote를 비롯한 여러 Office 365 애플리케이션은 Sharepoint 서비스를 활용하여 클라우드에 동기화됩니다. 이로 인해 Sharepoint가 액세스 정책에서 차단된 경우 동기화 프로세스가 중단됩니다.

2. 서드파티 피드를 구성합니다.

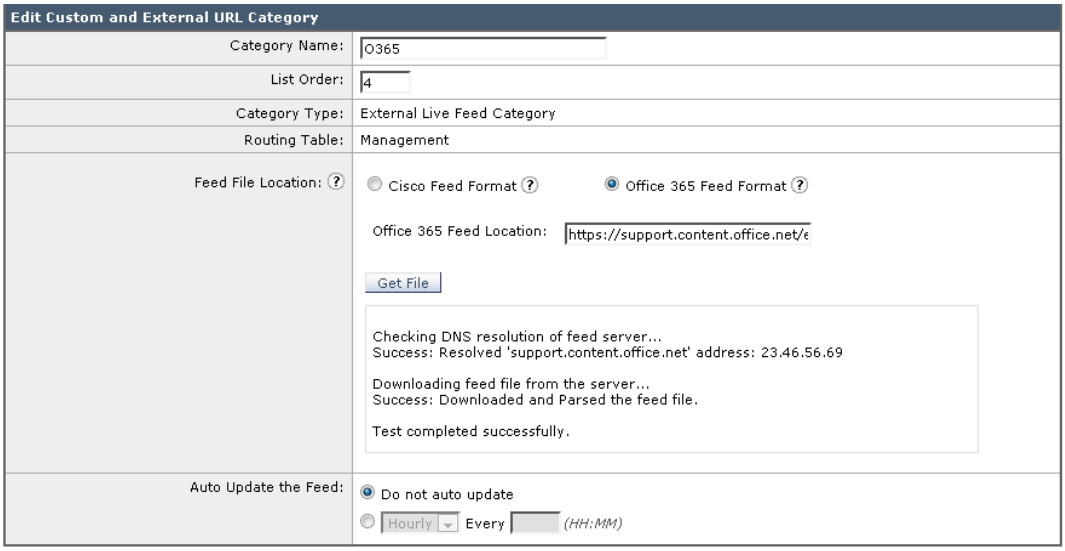
a. Web Security Manager(웹 보안 관리자) > Custom and External URL Categories(맞춤형 및 외부 URL 범주)로 이동합니다.

b. **Add Category(범주 추가)...**를 클릭합니다.

c. Category Name(범주 이름)에 **O365**를 입력하고 Category Type(범주 유형)을 **External Live Feed Category(외부 라이브 피드 범주)**로 선택합니다.

d. Feed File Location(피드 파일 위치)에 Office 365 Feed Format(Office 365 피드 형식)을 선택하고 다음 URL을 입력합니다. https://support.content.office.net/en-us/static/O365IPAddresses.xml

e. **Get File(파일 다운로드)**을 클릭합니다. 성공 메시지를 수신해야 합니다.




f. **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

3. 액세스 정책을 생성합니다.

   a. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)로 이동합니다.

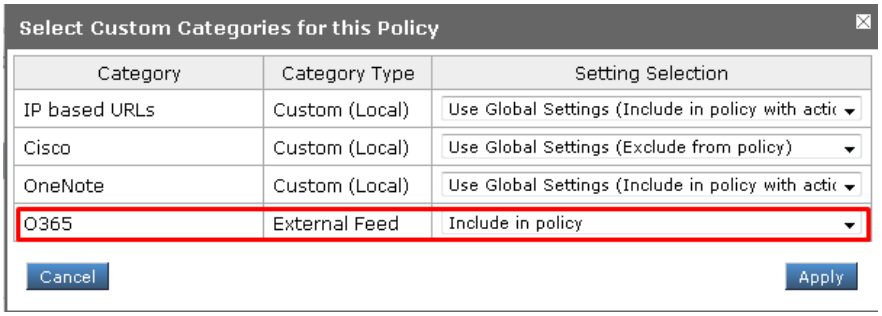
   b. **Add Policy(정책 추가)**를 클릭합니다.

   c. 정책 이름을 **O365**로 입력합니다.

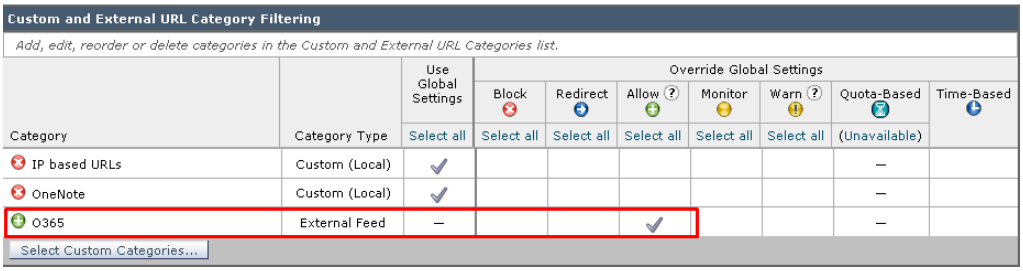
   d. **All Authenticated Users(모든 인증된 사용자)**가 선택되었는지 확인하고 **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

   e. 방금 생성한 새 정책의 URL Filtering(URL 필터링) 열을 클릭합니다.

   f. Select Custom Categories(맞춤형 범주 선택)를 클릭하고 O365 범주에 대해 Include in policy(정책에 포함)를 선택하고 Apply(적용)를 클릭합니다.




   g. Override Global Settings(글로벌 설정 재정의)에서 옵션을 **Allow(허용)**로 설정합니다.




   h. **Submit(제출)**과 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

   i. OneNote로 돌아가서 **File(파일)**을 클릭합니다.

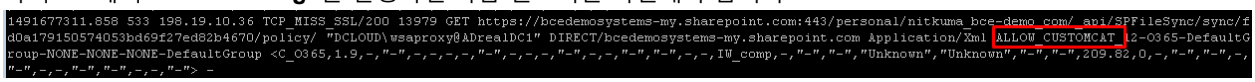
   j. **View Sync Status(동기화 상태 보기)**를 클릭합니다.

   k. 다시 한번 Sync manually(수동 동기화)를 선택했는지 확인하고 **Sync Now(지금 동기화)**를 클릭합니다.

   l. 더 이상 원래 오류가 표시되지 않고 다음 메시지가 표시되어야 합니다.


   m. **Last sync(지난 동기화)**는 클라이언트 머신에서의 로컬 시간과 일치해야 합니다. 이는 동기화가 성공했음을 나타냅니다.

   n. 다시 CLI에서 **tail accesslogs**를 실행하면 다음 엔트리를 확인해야 합니다.




   o. 이는 sharepoint에 대한 요청이 허용하도록 설정된 맞춤형 범주에 따라 허용되었음을 나타냅니다(이는 외부 피드에서 확인 가능).

# 시나리오 10:  AWSR(Advanced Web Security Reporting)

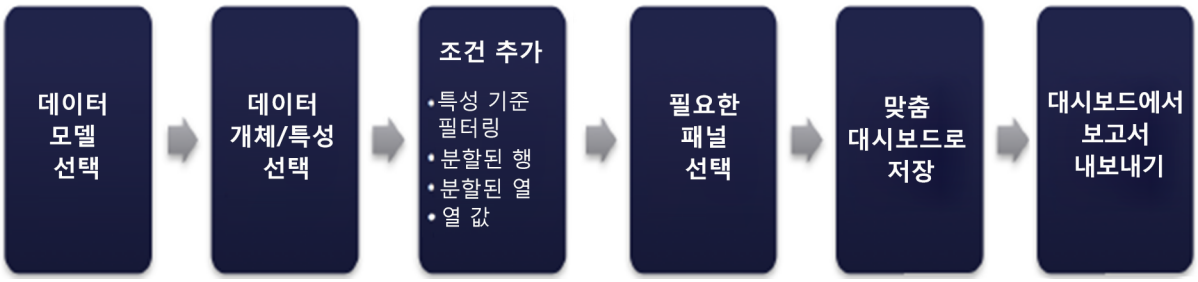
## 서론

### AWSR 소개


- 단일 플레인에서 여러 WSA 어플라이언스에서 보낸 보고서를 확인하고 개별 어플라이언스별로 보고서를 확인할 수도 있습니다.
- SMA는 WSA가 일정 수가 넘도록 확장하지 않으므로 더 많은 WSA 기존 고객을 위해서는 AWSR을 이용하는 것이 좋습니다.
- AD 그룹 기반 보고
- WSA 및 CWS를 위한 하이브리드 보고
- 기록 데이터를 가져오는 데에도 사용됨
- 포렌식 목적으로 데이터 보존

이제 AWSR 6.0의 맞춤형 필터를 구성하는 방법에 대한 프로세스를 살펴보겠습니다.

**맞춤형 필터를 사용하는 방법에 대한 프로세스**

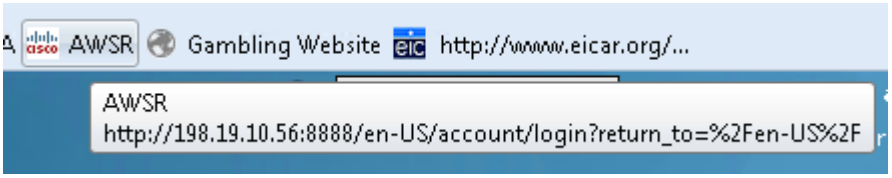



**참고:** 본 실습은 AWSR에 로그를 전송하기 위해 WSA를 구성하는 방법은 다루지 않습니다. 이 지침에 대해서는 AWSR 사용 설명서를 참조하십시오. http://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/Advanced_Web_Security_Reporting_6.pdf. 지침은 섹션 1~12에서 시작됩니다.

# 작업 A: AWSR의 기본 보고서

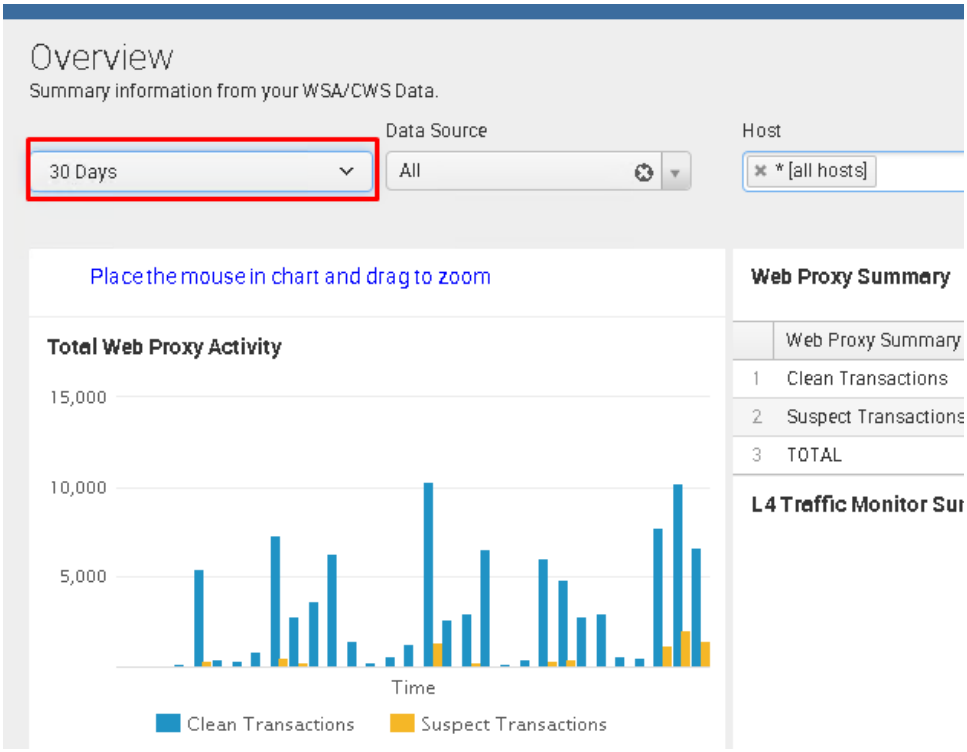
## 단계

1. Advanced Web Security 보고 애플리케이션에 로그인합니다.




2. 사용자 이름 **admin**, 비밀번호 **C1sco12345**로 로그인합니다.

3. 로그인하면 AWSR 개요 페이지가 표시됩니다. 기본 시간 프레임으로 **30 Days(30일)**를 선택합니다.



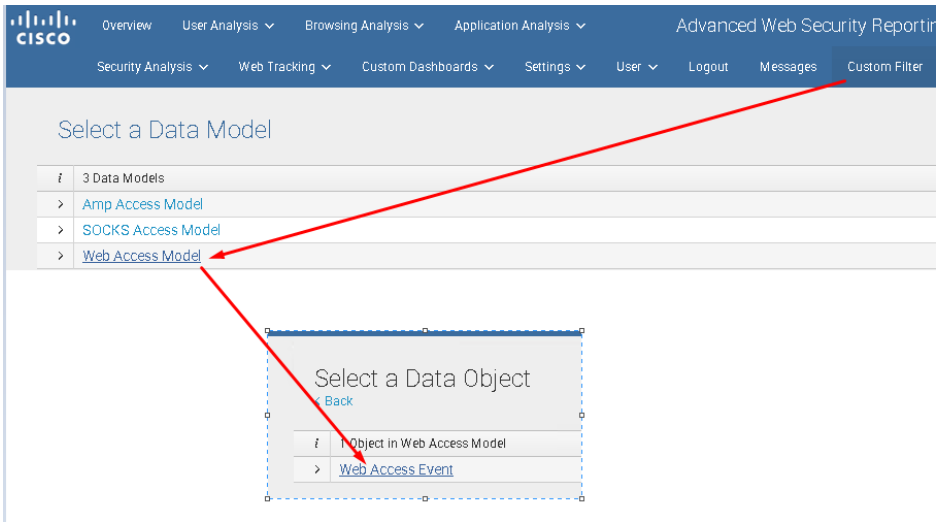

4. 사용자 분석, 브라우징 분석, 애플리케이션 분석, 보안 분석 및 웹 추적 등 다양한 보고서를 찾습니다.

**참고:** 이 모든 보고서는 WSA의 유사한 패턴/추적에 대한 내용입니다.

# 작업 B: 맞춤형 필터: 일반 보고서

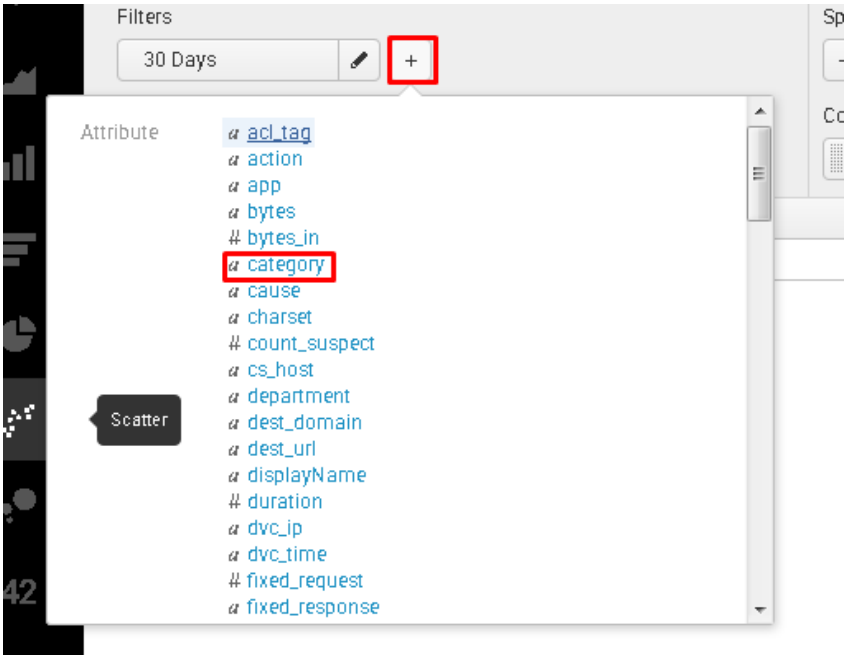
## 단계

1. Custom Filter(맞춤형 필터) > Web Access Model(웹 액세스 모델) > Web Access Event(웹 액세스 이벤트)를 클릭합니다.

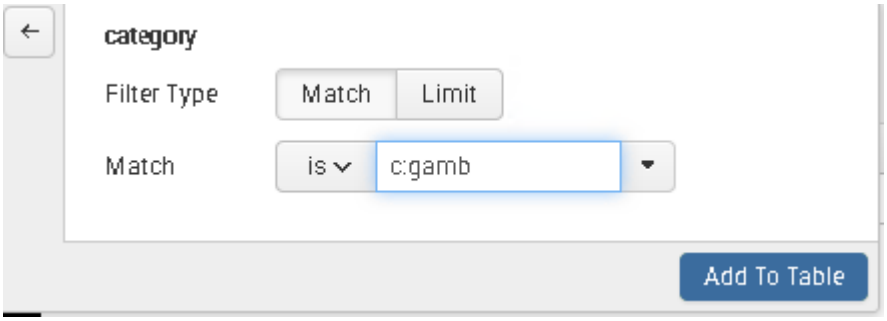



2. New Custom Filter(새 맞춤형 필터) 창에서 Filters(필터)를 All time(항상)에서 30 Days(30일)로 변경합니다.

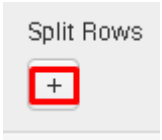
3. 필터 + 기호 아이콘을 클릭하고 **category(범주)**를 선택합니다.



4. Filter Type(필터 유형)을 Match(일치)로 설정하고 Match(일치)가 **is**이며 **c:gamb** 문자열인지 확인합니다. 그런 다음 Add To Table(표에 추가)을 클릭합니다. 이 필터는 Gambling(도박) 범주에만 결과를 표시합니다.




5. Split Rows(분할된 행)의 + 기호 아이콘을 클릭합니다.




6. 다음 속성을 추가합니다.
    a. dest_domain
    b. dvc_ip
    c. user_id_fixed
    d. 능력

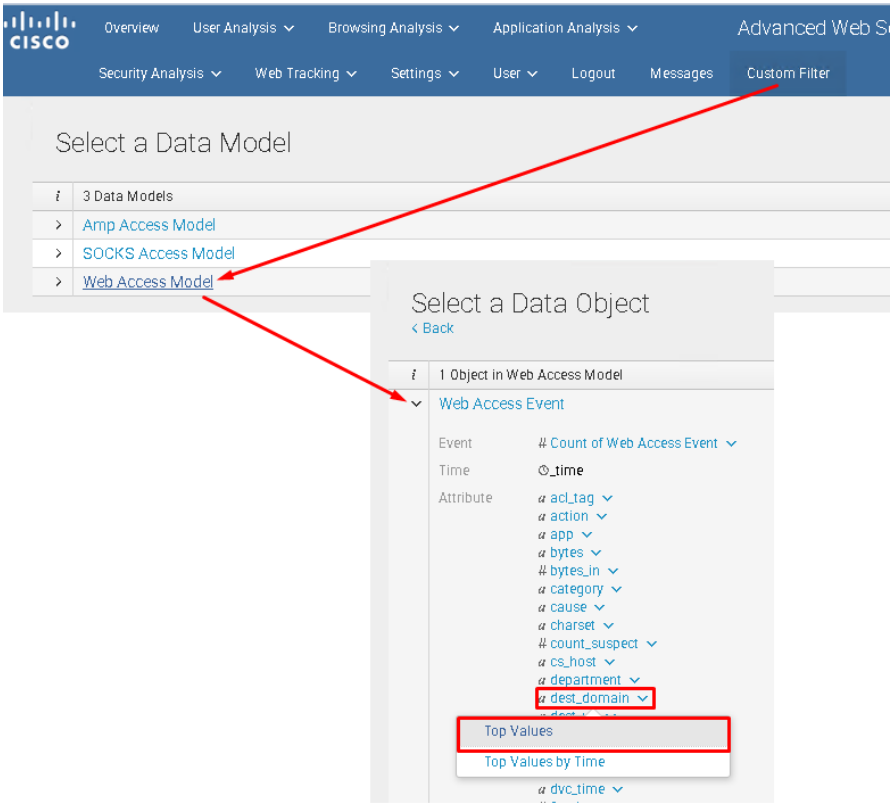
7. 순서가 **dvc_ip, user_id_fixed, dest_domain, action**이 되도록 행을 이동시킵니다.


8. 결과를 참고합니다. 이 보고서는 디바이스 IP, 사용자 이름, 대상 도메인 및 작업을 보여줍니다.

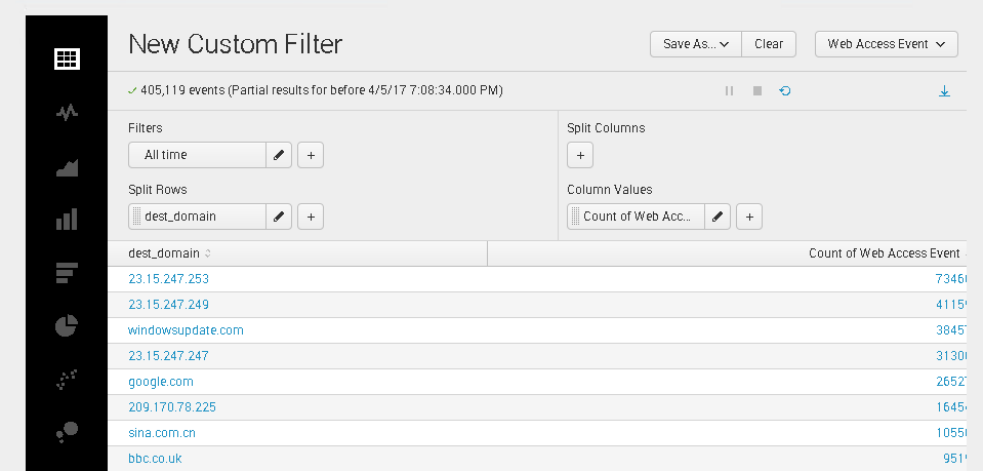
# 작업 C: 맞춤형 필터: 시간을 낭비하는 웹 사이트

## 단계

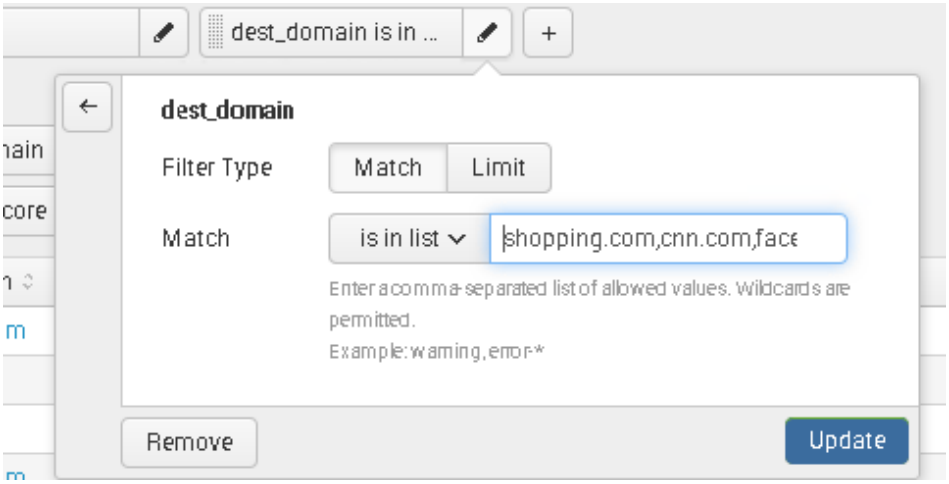
1. 이 연습 문제에서는 관리자가 시간을 낭비하는 특정 웹 사이트(맞춤형 사이트/도메인)에 따른 보고서를 얻으려고 할 때의 활용 사례를 다룹니다.
2. **Custom Filter(맞춤형 필터)**를 클릭합니다.
3. Data Model(데이터 모델) > Web Access Model(웹 액세스 모델)을 선택합니다.
4. 모든 필드/특성을 나열하는 목록 보기를 클릭합니다.
5. **dest_domain**를 **Top Values(최상위 값)**로 선택하면 최상위 도메인이 모두 나열됩니다.



6. 이제 **New Custom Filter(새 맞춤형 필터)** 창이 표시됩니다.

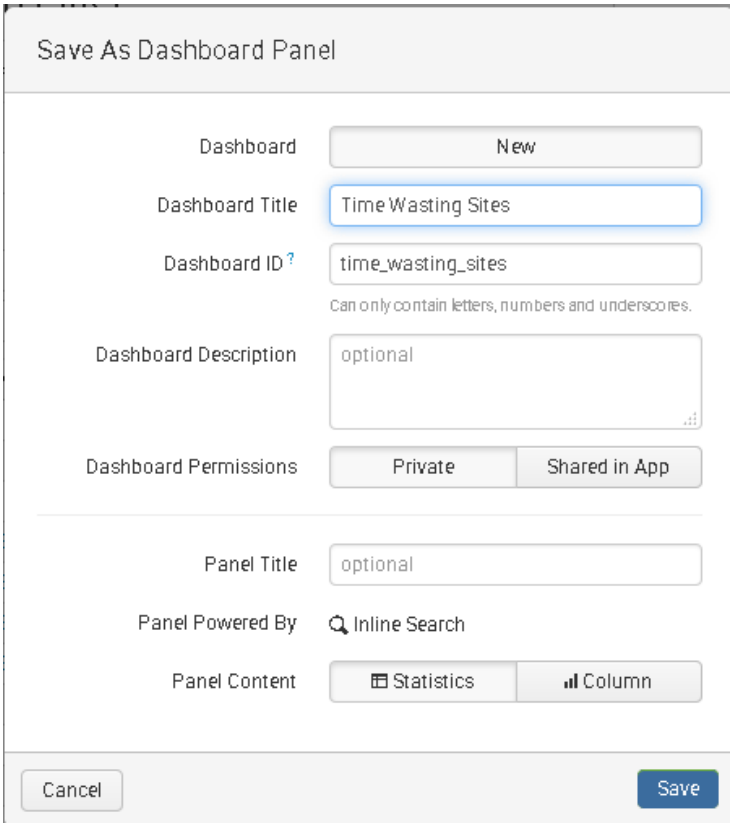



7. **Filters(필터)**를 All Time(항상)에서 **30 Days(30일)**로 설정합니다.
8. 최상위 도메인을 더 확인하려면 왼쪽 하단에서 "페이지당 50개"를 변경합니다.
9. Split Rows(분할된 행)에서 행(+)을 추가합니다.
    a. user_id_fixed
    b. dvc_ip
    c. dest_domain
    d. bytes
10. **Filters(필터)**의 (+)를 클릭하여 **dest_domain**을 선택합니다.
11. **facebook.com,cnn.com,youtube.com,amazon.com,netflix.com** 도메인을 추가하고 Match(일치)에 **is in list**를 선택합니다. 마지막으로 **Add To Table(표에 추가)**을 클릭합니다.

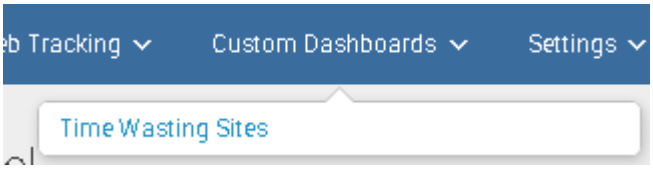



12. 이제 **Save As(다른 이름으로 저장) > Dashboard Panel(대시보드 패널)**을 클릭합니다.

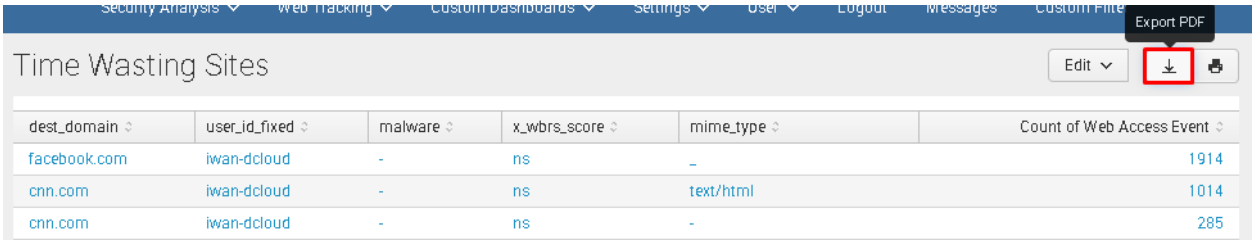
13. **Time Wasting Sites**와 같이 의미 있는 이름을 입력합니다.




14. 저장하면 Custom Dashboards(맞춤형 대시보드) 탭이 나타납니다.




15. Time Wasting Sites(시간을 낭비하는 사이트)를 클릭합니다. 다운로드 버튼이 표시됩니다. 이 보고서를 PDF로 내보냅니다.

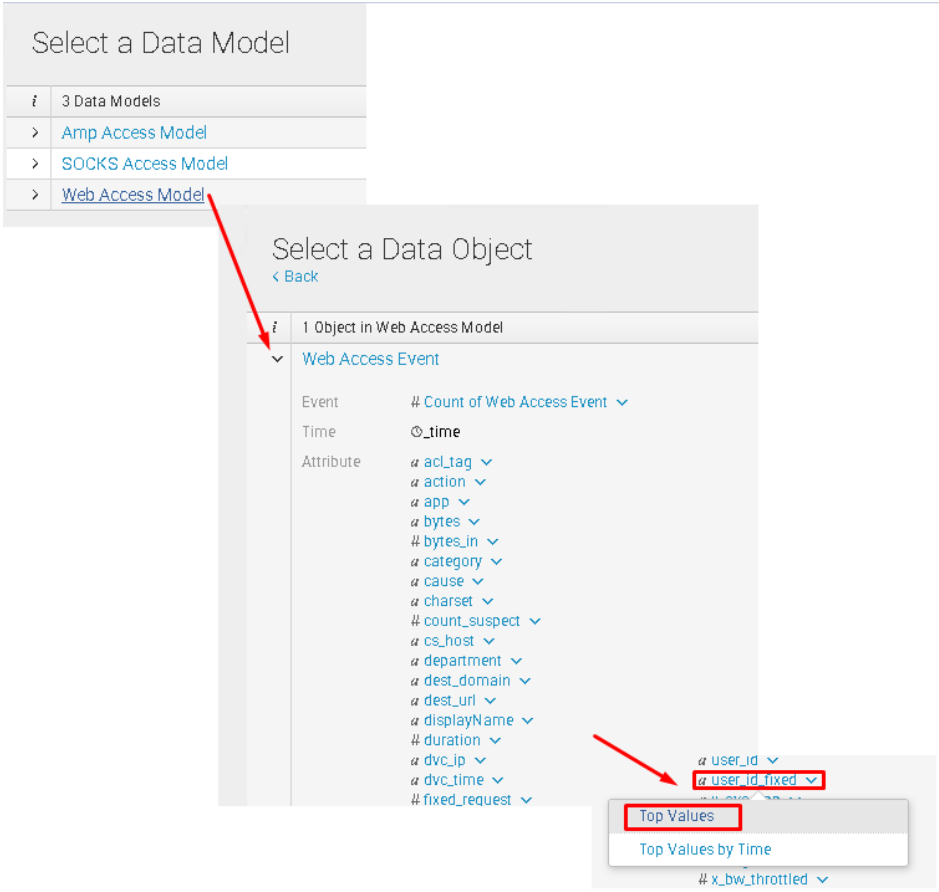



## 작업 D: 맞춤형 필터: 파이 차트 패널

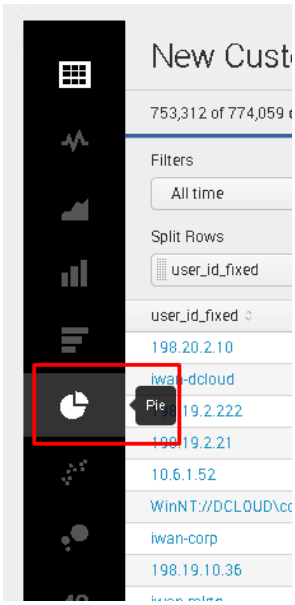
## 단계

1. Custom Filter(맞춤형 필터)를 클릭합니다.

2. Data Model(데이터 모델)을 **Web Access Model(웹 액세스 모델)**로 선택합니다.
3. user_id_fixed를 Top Values(최상위 값)로 선택합니다. 이렇게 하면 모든 최상위 사용자/IP 주소가 나열됩니다.

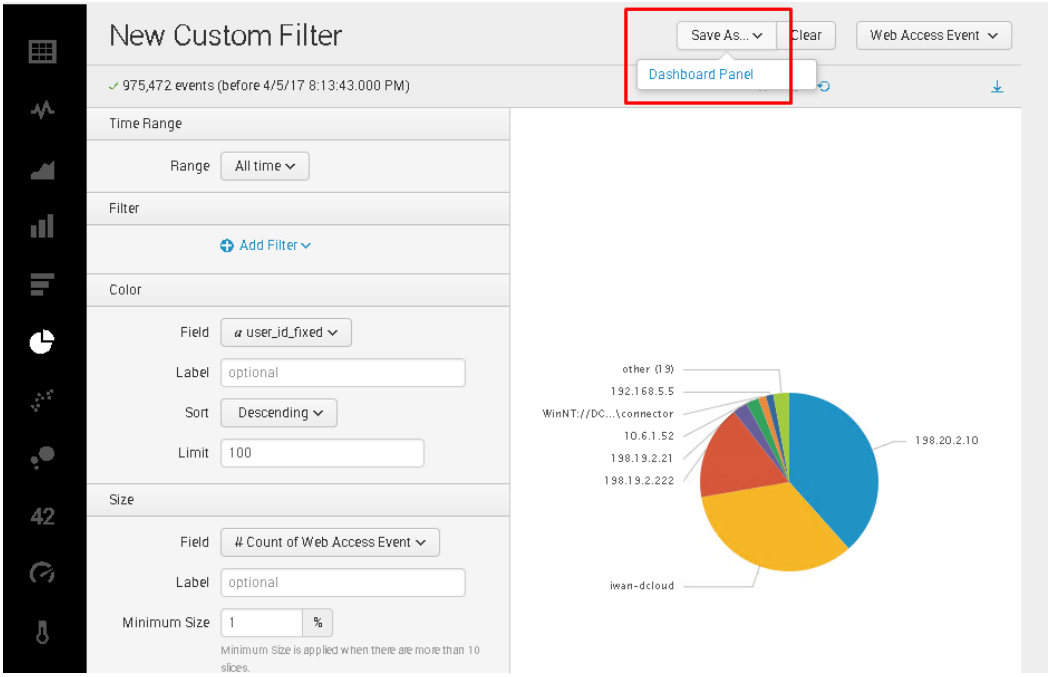



4. 왼쪽 패널에서 파이 차트 아이콘을 선택합니다.




5. 이 아이콘을 클릭하면 파이 차트 형식으로 데이터가 표시됩니다.

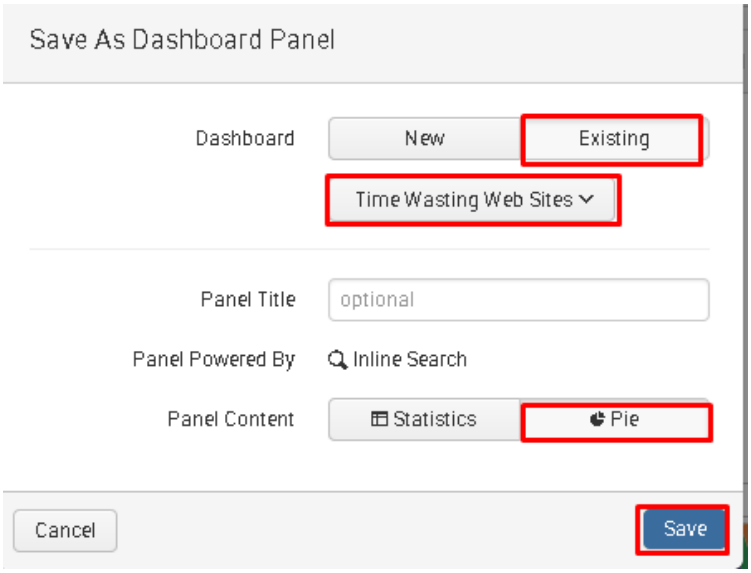
6. 오른쪽 상단에서 Save As(다른 이름으로 저장)... > Dashboard Panel(대시보드 패널)을 선택합니다.



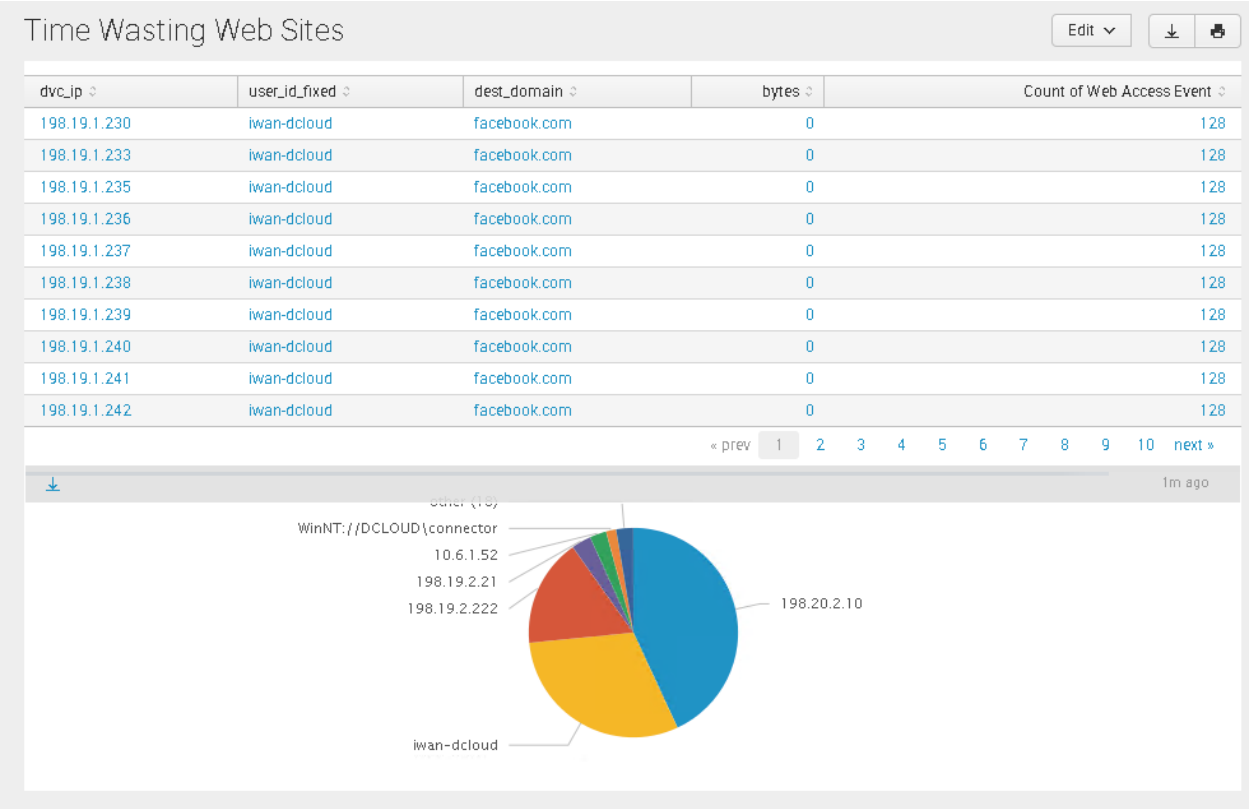

7. **Exisiting(기존 항목)**을 선택하고 **Time Wasting Sites(시간을 낭비하는 사이트)**를 선택합니다.

8. Panel Content(패널 콘텐츠) > Pie(파이)를 선택합니다.

9. **Save(저장)**를 클릭한 다음 **OK(확인)**를 클릭합니다.



10. Custom Dashboards(맞춤형 대시보드)를 다시 클릭하고 **Time Wasting Sites(시간을 낭비하는 사이트)**를 선택합니다. 이제 파이 차트와 테이블 형식의 보고서가 표시되어야 합니다.



# 시나리오 11: 중앙 집중식 소프트웨어 업그레이드

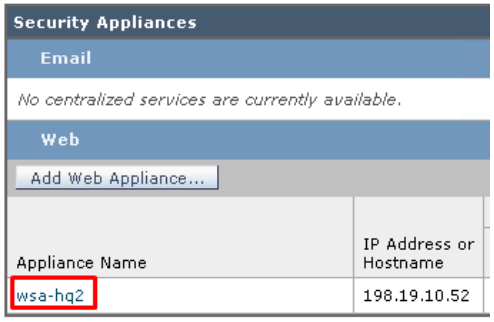
## 서론

WSA 및 ESA를 관리하기 위해 SMA(Security Management Appliance)를 구축하는 고객은 디바이스별로 업그레이드 절차를 수행해야 합니다. 버전 10.1 관리자에서 시작하면 동시에 여러 디바이스에서 업그레이드를 푸시할 수 있습니다.

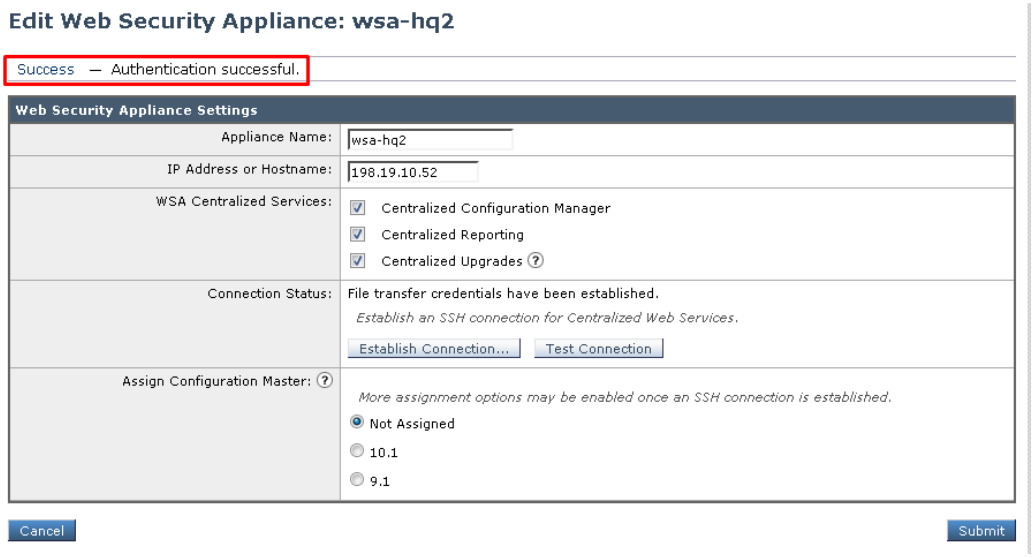
## 작업 A: 시스템 설정

## 단계

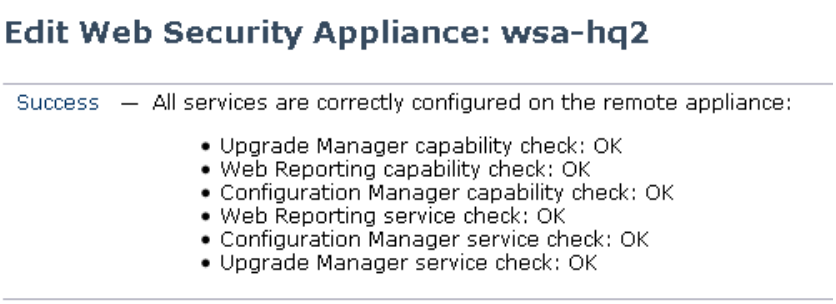
1. 연결되어 있는지 확인합니다.
    a. 북마크 링크를 통해 SMA에 로그인하거나 https://sma.dcloud.cisco.com으로 이동합니다.
    b. Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)로 이동합니다.
    c. Security Appliances(보안 어플라이언스)에 wsa-hq2가 표시됩니다. 어플라이언스 이름을 클릭합니다.



d. Establish Connection(연결 설정) 버튼을 클릭합니다. 사용자 이름 **admin**, 비밀번호 **ironport**를 입력합니다. Establish Connection(연결 설정)을 다시 클릭합니다. 성공 메시지를 수신해야 합니다.




e. 다음으로 Test Connection(연결 테스트)을 클릭합니다. 다시 성공 메시지를 수신해야 합니다.

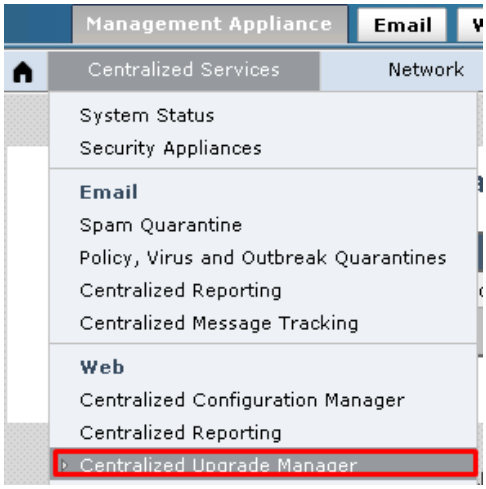



f. Submit(제출)을 클릭한 다음 Commit Changes(변경 사항 커밋)를 클릭합니다.

g. 이제 **Connection Established(연결 설정됨)**에 Yes(예)가 표시되어야 합니다.

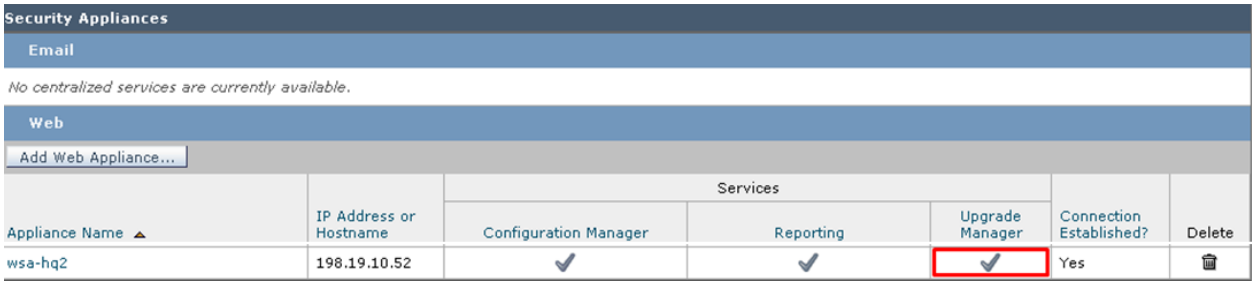

2. SMA를 중앙 집중식 업그레이드로 구성합니다.

a. Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Centralized Upgrade Manager(중앙 집중식 업그레이드 관리자)로 이동합니다.



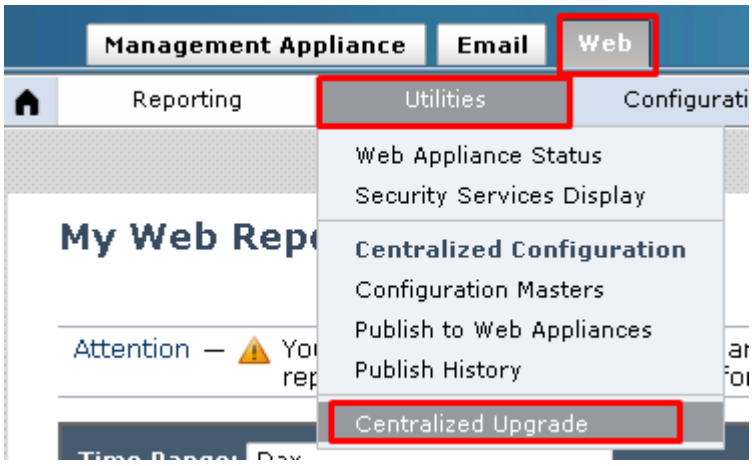

b. 중앙 집중식 업그레이드가 활성화되어 있는지 확인합니다. 활성화된 경우, 2c단계로 이동합니다. 활성화되어 있지 않은 경우 Edit Settings(설정 편집)를 클릭하고 **Enable Centralized upgrade Service(중앙 집중식 업그레이드 서비스 활성화)** 확인란을 선택합니다. Submit(제출)과 Commit Changes(변경 사항 커밋)를 클릭합니다.

c. 마지막으로 Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)로 이동하여 wsa-hq2의 Upgrade Manager(업그레이드 관리자)가 선택되어 있는지 확인합니다.



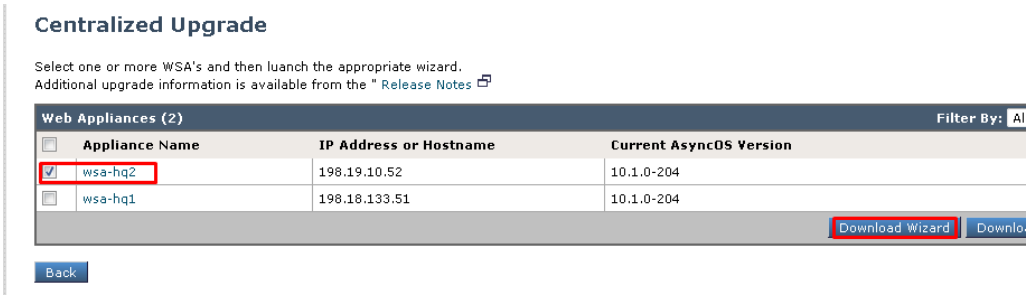

3. WSA 업그레이드를 다운로드합니다.

a. Web(웹) > Utilities(유틸리티) > Centralized Upgrade(중앙 집중식 업그레이드)로 이동합니다.

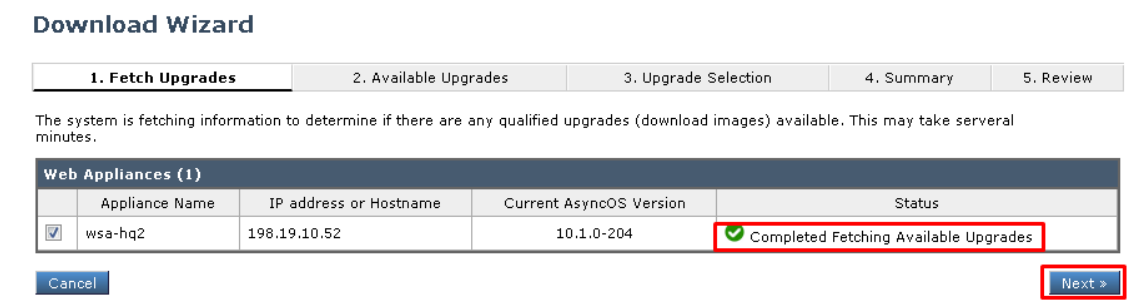



b. Upgrade Appliances(어플라이언스 업그레이드) 버튼을 클릭합니다. 이제 wsa-hq2와 wsa-hq1이 모두 나타나야 합니다.

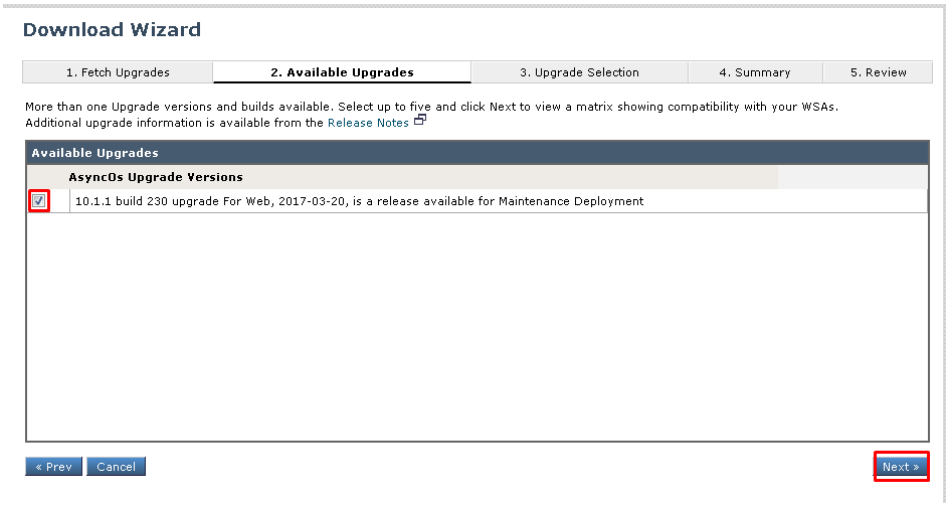
c. wsa-hq2를 선택하고 Download Wizard(다운로드 마법사) 버튼을 클릭합니다.



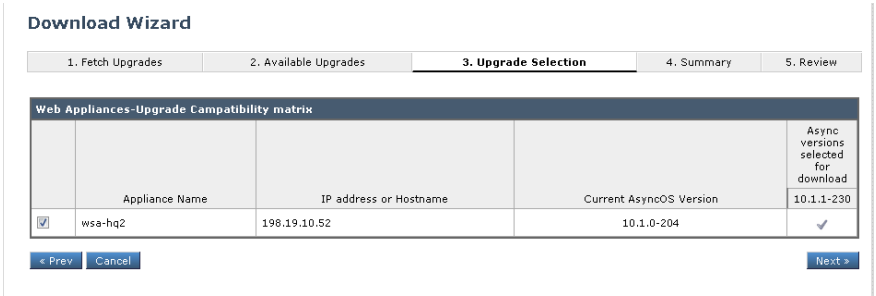

d. 이제 업그레이드 가져오기 화면이 표시되어야 합니다. 작업을 성공적으로 완료한 경우 Next(다음)를 클릭합니다.




e. 사용 가능한 AsyncOS 버전을 선택하고 Next(다음)를 클릭합니다.

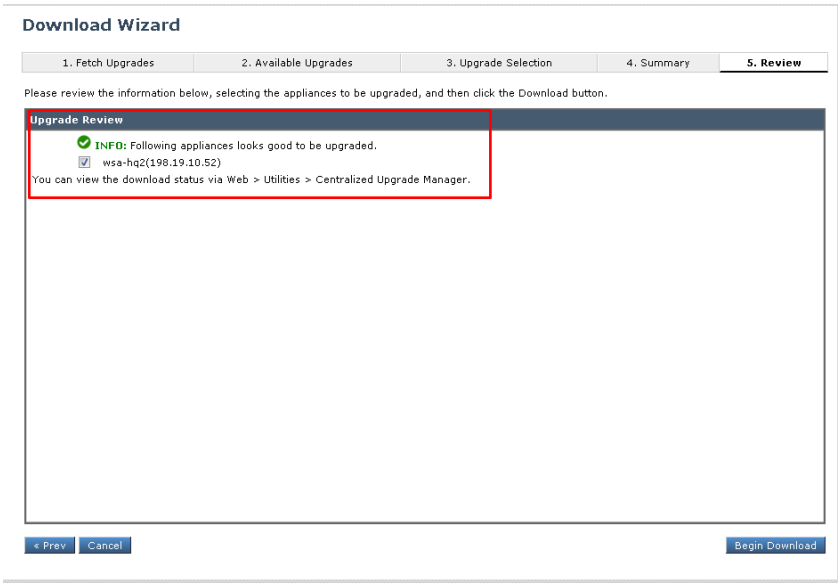



f. 올바른 WSA가 IP 주소 및 현재 AsyncOS 버전과 함께 표시되는지 확인한 후 Next(다음)를 클릭합니다.




g. Summary(요약) 탭에서 정보를 확인하고 Next(다음)를 클릭합니다.

h. 이제 Begin Download(다운로드를 시작) 옵션이 표시되어야 합니다.




i. 다운로드는 WSA를 시작하면서 시작되어야 합니다. Cancel(취소)과 Confirm Cancel(취소 확인)을 클릭하여 실습 인프라용 대역폭을 유지합니다.

**참고:** 일반적인 상황에서 중앙 집중식 업그레이드를 통해 여러 WSA가 업그레이드될 수 있습니다.

축하합니다. 실습을 성공적으로 완료하셨습니다.

# 감사합니다.

이 평가 인증서는

Cisco Web Security Appliance AsyncOS 10.0 교육 이수

시 제공됩니다.

서명 날짜

**SEVT, 2017년 5월**

**미주 지역 본부**
Cisco Systems, Inc.
San Jose CA

**아시아 태평양 지역 본부**
Cisco Systems (USA) Pte. Ltd.
싱가포르

**유럽 지역 본부**
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.