AsyncOS 9.0.1 for Cisco Web Security Appliances 사용 설명서

게시: 2016년 1월 27일
수정: 2016년 8월 12일

Cisco Systems, Inc.
www.cisco.com

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NNOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED **"AS IS"** WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

AsyncOS 9.0.1 for Cisco Web Security Appliances User Guide
© 2016 Cisco Systems, Inc. All rights reserved.

목 차

1장 **제품 및 릴리스 소개** 1-1

Web Security Appliance 소개 1-1

새로운 기능 1-1

Cisco AsyncOS 9.0.1의 새로운 기능 1-1

Cisco AsyncOS 9.0.1-162(GD)의 새로운 기능 1-2

Cisco AsyncOS 9.0.1-161(GD-물리적 어플라이언스만)의 새로운 기능 1-2

Cisco AsyncOS 9.0.1-135(ED)의 새로운 기능 1-2

Cisco AsyncOS 9.2의 새로운 기능 1-2

Cisco AsyncOS 9.2.0-082의 새로운 기능 1-2

Cisco AsyncOS 9.2.0-075의 새로운 기능 1-3

관련 주제 1-3

어플라이언스 웹 인터페이스 사용 1-3

웹 인터페이스 브라우저 요건 1-3

가상 어플라이언스에서 웹 인터페이스에 대한 액세스 사용 1-4

어플라이언스 웹 인터페이스 액세스 1-4

웹 인터페이스 변경 사항 커밋 1-5

웹 인터페이스 변경 사항 지우기 1-5

Cisco SensorBase 네트워크 1-5

SensorBase 혜택 및 개인 정보 보호 1-5

Cisco SensorBase 네트워크에 참여 사용 1-6

2장 **연결, 설치 및 구성** 2-1

연결, 설치 및 구성 개요 2-1

가상 어플라이언스 구축 2-2

물리적 어플라이언스에서 가상 어플라이언스로 마이그레이션 2-2

운영 모드 비교 2-2

연결, 설치 및 구성 작업 개요 2-2

어플라이언스 연결 2-3

설정 정보 수집 2-6

시스템 설정 마법사 2-7

시스템 설정 마법사 참조 정보 2-8

네트워크/시스템 설정 2-8

네트워크/네트워크 상황 2-9
네트워크/네트워크 인터페이스 및 와이어링 2-10
네트워크/레이어 4 트래픽 모니터 와이어링 2-10
네트워크/관리 및 데이터 트래픽에 대한 경로 2-11
네트워크/투명 연결 설정 2-11
네트워크/관리 설정 2-12
보안/보안 설정 2-12
업스트림 프록시 2-13
업스트림 프록시 작업 개요 2-13
업스트림 프록시에 대한 프록시 그룹 생성 2-13
네트워크 인터페이스 2-14
IP 주소 버전 2-15
네트워크 인터페이스 사용 또는 변경 2-15
고가용성을 위한 페일오버 그룹 구성 2-17
페일오버 그룹 추가 2-17
고가용성 전역 설정 편집 2-18
페일오버 그룹의 상태 보기 2-18
웹 프록시 데이터용 P2 데이터 인터페이스 사용 2-19
TCP/IP 트래픽 경로 구성 2-20
기본 경로 수정 2-21
경로 추가 2-21
라우팅 테이블 저장 및 로드 2-21
경로 삭제 2-21
투명 리디렉션 구성 2-22
투명 리디렉션 디바이스 지정 2-22
WCCP 서비스 구성 2-22
VLAN을 사용하여 인터페이스 용량 늘리기 2-25
VLAN 구성 및 관리 2-25
리디렉션 호스트 이름 및 시스템 호스트 이름 2-28
리디렉션 호스트 이름 변경 2-28
시스템 호스트 이름 변경 2-28
SMTP 릴레이 호스트 설정 구성 2-29
SMTP 릴레이 호스트 구성 2-29
DNS 설정 2-29
분할 DNS 2-30
DNS 캐시 지우기 2-30
DNS 설정 편집 2-30
연결, 설치 및 구성 트러블슈팅 2-31

3장 **어플라이언스를 Cisco Cloud Web Security 프록시에 연결** 3-1
클라우드 커넥터 모드에서 기능을 구성 및 사용하는 방법 3-1
클라우드 커넥터 모드에서 구축 3-2
클라우드 커넥터 구성 3-2
클라우드에서 디렉토리 그룹을 사용하여 웹 액세스 제어 3-5
클라우드 프록시 서버 우회 3-5
클라우드 커넥터 모드에서 FTP 및 HTTPS 부분 지원 3-6
보안 데이터 유출 방지 3-6
그룹 및 사용자 이름과 IP 주소 보기 3-6
클라우드 커넥터 로그 구독 3-7
Cloud Web Security Connector를 사용하는 식별 프로필 및 인증 3-7
정책 적용을 위한 머신 식별 3-8
인증되지 않은 사용자에 대한 게스트 액세스 3-8

4장 **웹 요청 가로채기** 4-1
웹 요청 가로채기 개요 4-1
웹 요청 가로채기 작업 4-2
웹 요청 가로채기 모범 사례 4-2
웹 요청 가로채기를 위한 웹 프록시 옵션 4-3
웹 프록시 설정 구성 4-3
웹 프록시 캐시 4-5
웹 프록시 캐시 지우기 4-6
웹 프록시 캐시에서 URL 제거 4-6
웹 프록시에서 캐시하지 않는 도메인 또는 URL 지정 4-6
웹 프록시 캐시 모드 선택 4-7
웹 프록시 IP 스푸핑 4-8
웹 프록시 맞춤형 헤더 4-9
웹 요청에 맞춤형 헤더 추가 4-9
웹 프록시 우회 4-10
웹 요청에 대한 웹 프록시 우회 4-10
웹 요청에 대한 웹 프록시 우회 구성 4-11
애플리케이션에 대한 웹 프록시 우회 구성 4-11
웹 프록시 사용 계약 4-11
웹 요청을 리디렉션하기 위한 클라이언트 옵션 4-11
클라이언트 애플리케이션에 PAC 파일 사용 4-12
PAC(Proxy Auto-Config) 파일을 게시하기 위한 옵션 4-12
PAC(Proxy Auto-Config) 파일을 찾기 위한 클라이언트 옵션 4-12
자동 PAC 파일 탐지 4-12

웹 보안 어플라이언스에서 PAC 파일 호스팅 4-13
클라이언트 애플리케이션에서 PAC 파일 지정 4-14
클라이언트에서 수동으로 PAC 파일 위치 구성 4-14
클라이언트에서 자동으로 PAC 파일 탐지 4-14
FTP 프록시 서비스 4-15
FTP 프록시 서비스 개요 4-15
FTP 프록시 사용 및 구성 4-15
SOCKS 프록시 서비스 4-17
SOCKS 프록시 서비스 개요 4-17
SOCKS 트래픽의 처리 사용 4-17
SOCKS 프록시 구성 4-17
SOCKS 정책 생성 4-18
요청 가로채기 트러블슈팅 4-19

5장 **최종 사용자 자격 증명 확보 5-1**
최종 사용자 자격 증명 확보 개요 5-1
인증 작업 개요 5-2
인증 모범 사례 5-2
인증 계획 5-2
Active Directory/Kerberos 5-3
Active Directory/기본 5-4
Active Directory/NTLMSSP 5-4
LDAP/기본 5-5
투명하게 사용자 식별 5-5
투명한 사용자 식별 이해 5-6
투명한 사용자 식별에 대한 규칙 및 지침 5-8
투명한 사용자 식별 구성 5-9
CLI를 사용하여 고급 투명한 사용자 식별 설정 구성 5-9
단일 로그인 구성 5-10
인증 영역 5-10
외부 인증 5-10
LDAP 서버를 통한 외부 인증 구성 5-10
RADIUS 외부 인증 사용 5-11
Kerberos 인증 체계에 대한 Active Directory 영역 생성 5-11
Active Directory 인증 영역(NTLMSSP 및 기본)을 생성하는 방법 5-13
Active Directory 인증 영역(NTLMSSP 및 기본) 생성에 대한 사전 요구 사항 5-13
다중 NTLM 영역 및 도메인 사용에 대한 정보 5-14
Active Directory 인증 영역 생성(NTLMSSP 및 기본) 5-14

LDAP 인증 영역 생성 5-15
인증 영역 삭제 정보 5-20
전역 인증 설정 구성 5-20
인증 시퀀스 5-25
인증 시퀀스 정보 5-25
인증 시퀀스 생성 5-26
인증 시퀀스 편집 및 다시 정렬 5-27
인증 시퀀스 삭제 5-27
실패한 인증 5-27
실패한 인증 정보 5-28
문제가 되는 사용자 에이전트에 대한 인증 우회 5-28
인증 우회 5-30
인증 서비스가 사용 불가능한 동안 인증되지 않은 트래픽 허용 5-30
인증 실패 후 게스트 액세스 권한 부여 5-31
게스트 액세스를 지원하는 식별 프로필 정의 5-31
정책에서 게스트 액세스를 지원하는 식별 프로필 사용 5-31
게스트 사용자 세부 정보가 기록되는 방식 구성 5-32
권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용 5-32
다른 자격 증명을 사용한 재인증 허용 정보 5-32
다른 자격 증명을 사용한 재인증 허용 5-32
식별된 사용자 추적 5-33
명시적 요청에 대해 지원되는 인증 서로게이트 5-33
투명 요청에 대해 지원되는 인증 서로게이트 5-33
재인증된 사용자 추적 5-34
자격 증명 5-34
세션 중에 재사용할 자격 증명 추적 5-34
인증 및 권한 부여 실패 5-35
자격 증명 형식 5-35
기본 인증을 위한 자격 증명 암호화 5-35
기본 인증을 위한 자격 증명 암호화 정보 5-35
자격 증명 암호화 구성 5-36
인증 트러블슈팅 5-36

6장 **최종 사용자 및 클라이언트 소프트웨어 분류 6-1**
사용자 및 클라이언트 소프트웨어 분류 개요 6-1
사용자 및 클라이언트 소프트웨어 분류: 모범 사례 6-2
식별 프로필 기준 6-2
사용자 및 클라이언트 소프트웨어 분류 6-3
ID 사용/사용 안 함 6-8

식별 프로필 및 인증 6-8
식별 프로필 트러블슈팅 6-10

7장 **SaaS 액세스 제어 7-1**
SaaS 액세스 제어 개요 7-1
어플라이언스를 ID 공급자로 구성 7-2
SaaS 액세스 제어 및 여러 어플라이언스 사용 7-3
SaaS 애플리케이션 인증 정책 생성 7-4
단일 로그인 URL에 대한 최종 사용자 액세스 구성 7-7

8장 **Cisco Identity Services Engine 통합 8-1**
ISE(Identity Services Engine) 서비스 개요 8-1
pxGrid 정보 8-1
ISE 서버 구축 및 페일오버 정보 8-2
ISE(Identity Services Engine) 인증서 8-2
자체 서명된 인증서 사용 8-3
CA 서명 인증서 사용 8-3
ISE 서비스를 인증하고 통합하기 위한 작업 8-3
ISE 서비스에 연결 8-6
ISE(Identity Services Engine) 트러블슈팅 8-8

9장 **정책 애플리케이션을 위한 URL 분류 9-1**
URL 트랜잭션 분류 개요 9-1
실패한 URL 트랜잭션 분류 9-2
DCA(Dynamic Content Analysis) 엔진 사용 9-2
분류되지 않은 URL 9-3
URL과 URL 카테고리 일치 9-3
분류되지 않은 URL 또는 잘못 분류된 URL 보고 9-3
URL 카테고리 데이터베이스 9-4
URL 필터링 엔진 구성 9-4
URL 카테고리 집합에 대한 업데이트 관리 9-4
URL 카테고리 집합 업데이트의 영향 이해 9-5
URL 카테고리 집합 변경이 정책 그룹 구성원 자격에 미치는 영향 9-5
URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향 9-5
병합된 카테고리 - 예 9-6
URL 카테고리 집합에 대한 업데이트 제어 9-7
수동으로 URL 카테고리 집합 업데이트 9-8

새 카테고리 및 변경된 카테고리에 대한 기본 설정 9-8
기존 설정 확인 및/또는 변경 9-8
카테고리 및 정책 변경에 대한 경고 수신 9-8
URL 카테고리 집합 업데이트에 대한 경고에 응답 9-9
URL 카테고리를 사용하여 트랜잭션 필터링 9-9
액세스 정책 그룹에 대한 URL 필터 구성 9-9
암호 해독 정책 그룹에 대한 URL 필터 구성 9-11
데이터 보안 정책 그룹에 대한 URL 필터 구성 9-12
맞춤형 URL 카테고리 생성 및 편집 9-14
성인 콘텐츠 필터링 9-15
안전 검색 및 사이트 콘텐츠 등급 시행 9-15
성인 콘텐츠 액세스 기록 9-16
액세스 정책의 트래픽 리디렉션 9-17
기록 및 보고 9-17
사용자에게 경고하고 계속하도록 허용 9-18
최종 사용자 필터링 경고 페이지에 대한 설정 구성 9-18
시간 기반 URL 필터 생성 9-19
URL 필터링 활동 보기 9-19
필터링되지 않고 분류되지 않은 데이터 이해 9-20
액세스 로그의 URL 카테고리 기록 9-20
정규식 9-20
정규식 형성 9-21
검증 실패를 방지하기 위한 지침 9-21
정규식 문자 표 9-22
URL 카테고리 설명 9-23

10장 **인터넷 요청을 제어하기 위한 정책 생성 10-1**
정책 개요: 가로챈 인터넷 요청 제어 10-1
정책을 통한 웹 요청 관리 작업 개요 10-2
정책을 통한 웹 요청 관리 모범 사례 10-2
정책 10-2
정책 유형 10-2
정책 순서 10-5
정책 생성 10-5
정책에 대한 SGT(Secure Group Tag) 추가 및 편집 10-8
정책 컨피그레이션 10-8
트랜잭션 요청 차단, 허용 또는 리디렉션 10-10

클라이언트 애플리케이션 10-10
클라이언트 애플리케이션 정보 10-10
정책에서 클라이언트 애플리케이션 사용 10-11
인증에서 클라이언트 애플리케이션 제외 10-12
시간 범위 및 할당량 10-12
정책 및 제한적 사용 제어에 대한 시간 범위 10-12
시간 범위 생성 10-12
시간 및 볼륨 할당량 10-13
볼륨 할당량 계산 10-14
시간 할당량 계산 10-14
시간 및 볼륨 할당량 정의 10-14
URL 카테고리별로 액세스 제어 10-15
맞춤형 URL 카테고리 생성 10-15
URL 카테고리를 사용하여 웹 요청 식별 10-16
URL 카테고리를 사용하여 웹 요청에 대한 조치 수행 10-17
원격 사용자 10-18
원격 사용자 정보 10-18
원격 사용자의 식별 구성 방법 10-18
원격 사용자의 식별 구성 10-19
ASA에 대한 원격 사용자 상태 및 통계 표시 10-20
정책 트러블슈팅 10-20

11장 **HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성 11-1**
HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성 개요 11-1
암호 해독 정책을 통한 HTTPS 트래픽 관리 작업 개요 11-2
암호 해독 정책을 통한 HTTPS 트래픽 관리 모범 사례 11-2
암호 해독 정책 11-2
HTTPS 프록시 사용 11-3
HTTPS 트래픽 제어 11-4
암호 해독 옵션 구성 11-5
인증 및 HTTPS 연결 11-5
루트 인증서 11-6
HTTPS에 대한 인증서 검증 및 암호 해독 관리 11-6
유효한 인증서 11-6
유효하지 않은 인증서 처리 11-7
루트 인증서 및 키 업로드 11-7
HTTPS 프록시에 대한 인증서 및 키 생성 11-8
유효하지 않은 인증서 처리 구성 11-9
인증서 폐기 상태 확인 옵션 11-9

실시간 폐기 상태 확인 사용 11-10
신뢰할 수 있는 루트 인증서 11-11
신뢰할 수 있는 목록에 인증서 추가 11-11
신뢰할 수 있는 목록에서 인증서 제거 11-11
HTTPS 트래픽 라우팅 11-12
암호 해독/HTTPS/인증서 트러블슈팅 11-12

12장 **기존 감염에 대한 아웃바운드 트래픽 스캐닝 12-1**
아웃바운드 트래픽 스캐닝 개요 12-1
요청이 DVS 엔진에서 차단된 경우 사용자 경험 12-1
업로드 요청 이해 12-2
그룹 구성원 자격에 대한 기준 12-2
클라이언트 요청을 아웃바운드 악성프로그램 검색 정책 그룹과 일치 12-2
아웃바운드 악성프로그램 검색 정책 생성 12-3
업로드 요청 제어 12-4
DVS 스캐닝 기록 12-5

13장 **보안 서비스 구성 13-1**
보안 서비스 구성 개요 13-1
웹 평판 필터 개요 13-2
웹 평판 점수 13-2
웹 평판 필터링의 작동 방식 이해 13-3
액세스 정책의 웹 평판 13-3
암호 해독 정책의 웹 평판 13-4
Cisco IronPort 데이터 보안 정책의 웹 평판 13-4
안티멀웨어 스캐닝 개요 13-4
DVS 엔진 작동 방식 이해 13-5
다중 악성코드 판정에 대한 작업 13-5
Webroot 스캐닝 13-6
McAfee 스캐닝 13-6
바이러스 시그니처 패턴 일치 13-6
휴리스틱 분석 13-6
McAfee 카테고리 13-6
Sophos 스캐닝 13-7
적응형 스캐닝 이해 13-7
적응형 스캐닝 및 액세스 정책 13-7
안티멀웨어 및 평판 필터 사용 13-8

정책에서 안티멀웨어 및 평판 구성 13-9
액세스 정책에서 안티멀웨어 및 평판 설정 13-9
적응형 스캐닝이 사용하도록 설정된 안티멀웨어 및 평판 설정 구성 13-10
적응형 스캐닝이 사용하지 않도록 설정된 안티멀웨어 및 평판 설정 구성 13-11
웹 평판 점수 구성 13-12
액세스 정책에 대한 웹 평판 점수 임계값 구성 13-12
암호 해독 정책 그룹에 대한 웹 평판 필터 설정 구성 13-13
데이터 보안 정책 그룹에 대한 웹 평판 필터 설정 구성 13-13
데이터베이스 테이블 유지 관리 13-13
웹 평판 데이터베이스 13-13
웹 평판 필터링 활동 및 DVS 스캐닝 기록 13-14
적응형 스캐닝 기록 13-14
캐싱 13-14
악성코드 카테고리 설명 13-14

14장 **파일 평판 필터링 및 파일 분석 14-1**
파일 평판 필터링 및 파일 분석의 개요 14-1
파일 위협 판정 업데이트 14-1
파일 처리 개요 14-2
파일 평판 및 분석 서비스에 대해 지원되는 파일 14-3
아카이브 또는 압축 파일 처리 14-4
클라우드에 전송된 정보의 개인 정보 보호 14-4
파일 평판 및 분석 기능 구성 14-5
파일 평판 및 분석 서비스와의 통신을 위한 요건 14-5
데이터 인터페이스를 통해 파일 평판 및 파일 분석 서버에 트래픽 라우팅 14-6
온프레미스 파일 분석 서버 구성 14-6
파일 평판 및 분석 서비스 사용 및 구성 14-7
(퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성 14-9
분석 그룹에 어떤 어플라이언스가 있습니까? 14-9
액세스 정책에 따라 파일 평판 및 분석 서비스 조치 구성 14-10
Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인 14-10
Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성 14-11
파일 평판 및 파일 분석 보고 및 추적 14-11
SHA-256 해시로 파일 식별 14-11
파일 평판 및 파일 분석 보고서 페이지 14-12
다른 보고서의 파일 평판 필터링 데이터 보기 14-13
웹 추적 및 Advanced Malware Protection 기능 정보 14-13
파일 위협 판정 변경 시 조치 수행 14-14

파일 평판 및 분석 트러블슈팅 14-14
로그 파일 14-14
파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고 14-15
API 키 오류(온프레미스 파일 분석) 14-15
파일이 예상대로 업로드되지 않음 14-15
클라우드의 파일 분석 세부사항이 불완전함 14-16
분석을 위해 전송할 수 있는 파일 유형에 대한 경고 14-16

15장 **웹 애플리케이션에 대한 액세스 관리 15-1**
웹 애플리케이션에 대한 액세스 관리의 개요 15-1
AVC 엔진 사용 15-2
AVC 엔진 업데이트 및 기본 조치 15-2
요청이 AVC 엔진에서 차단된 경우 사용자 경험 15-3
정책 애플리케이션 제어 설정 15-3
범위 요청 설정 15-4
애플리케이션 제어 구성에 대한 규칙 및 지침 15-4
액세스 정책 그룹에서 애플리케이션 제어 설정 구성 15-5
대역폭 제어 15-6
전체 대역폭 제한 구성 15-6
사용자 대역폭 제한 구성 15-6
애플리케이션 유형에 대한 기본 대역폭 제한 구성 15-7
애플리케이션 유형에 대한 기본 대역폭 제한 재지정 15-7
애플리케이션에 대한 대역폭 제어 구성 15-8
인스턴트 메시징 트래픽 제어 15-8
AVC 활동 보기 15-9
액세스 로그 파일의 AVC 정보 15-9

16장 **민감한 데이터의 유출 방지 16-1**
민감한 데이터의 유출 방지 개요 16-1
최소 크기 미만의 업로드 요청 우회 16-2
요청이 민감한 데이터로 차단된 경우 사용자 경험 16-2
업로드 요청 관리 16-3
외부 DLP 시스템에서 업로드 요청 관리 16-3
데이터 보안 및 외부 DLP 정책 그룹 구성원 자격 평가 16-4
클라이언트 요청을 데이터 보안 및 외부 DLP 정책 그룹과 매칭 16-4
데이터 보안 및 외부 DLP 정책 생성 16-5
업로드 요청에 대한 설정 관리 16-7
URL 카테고리 16-7

웹 평판 16-8
콘텐츠 차단 16-8
외부 DLP 시스템 정의 16-9
외부 DLP 서버 구성 16-9
외부 DLP 정책을 사용하여 업로드 요청 제어 16-11
데이터 유출 방지 검사 기록 16-12

17장 **최종 사용자에게 프록시 조치 알림 17-1**
최종 사용자 알림 개요 17-1
알림 페이지에 대한 일반 설정 구성 17-2
최종 사용자 승인 페이지 17-2
최종 사용자 승인 페이지를 사용하여 HTTPS 및 FTP 사이트에 액세스 17-3
최종 사용자 승인 페이지 정보 17-3
최종 사용자 승인 페이지 구성 17-3
최종 사용자 알림 페이지 17-5
온박스 최종 사용자 알림 페이지 구성 17-5
오프박스 최종 사용자 알림 페이지 17-6
액세스 차단 이유에 따라 올바른 오프박스 페이지 표시 17-6
오프박스 알림 페이지에 대한 URL 기준 17-7
오프박스 최종 사용자 알림 페이지 매개변수 17-7
최종 사용자 알림 페이지를 맞춤형 URL로 리디렉션(오프박스) 17-8
최종 사용자 URL 필터링 경고 페이지 구성 17-9
FTP 알림 메시지 구성 17-9
알림 페이지의 맞춤형 메시지 17-10
알림 페이지의 맞춤형 메시지에서 지원되는 HTML 태그 17-10
알림 페이지의 URL 및 로그 주의 사항 17-11
알림 페이지 HTML 파일을 직접 편집 17-11
알림 HTML 파일을 직접 편집하기 위한 요건 17-12
알림 HTML 파일을 직접 편집 17-12
알림 HTML 파일에서 변수 사용 17-13
알림 HTML 파일을 맞춤화하기 위한 변수 17-13
알림 페이지 유형 17-15

18장 **최종 사용자 활동을 모니터링하기 위한 보고서 생성 18-1**
보고 개요 18-1
보고서의 사용자 이름에 대한 작업 18-1
Report(보고서) 페이지 18-2

Reporting(보고) 탭 사용 18-2
시간 범위 변경 18-3
데이터 검색 18-3
차트에 표시할 데이터 선택 18-4
맞춤형 보고서 18-4
맞춤형 보고서에 추가될 수 없는 모듈 18-5
맞춤형 보고서 페이지 생성 18-5
보고 및 추적의 하위 도메인과 두 번째 레벨 도메인 비교 18-5
보고서 페이지에서 보고서 인쇄 및 내보내기 18-6
보고서 데이터 내보내기 18-6
중앙 집중식 보고 사용 18-7
보고서 예약 18-7
예약된 보고서 추가 18-8
예약된 보고서 편집 18-8
예약된 보고서 삭제 18-8
온디맨드 보고서 생성 18-9
아카이브된 보고서 18-9

19장 **Web Security Appliance 보고서** 19-1
Overview(개요) 페이지 19-2
Users(사용자) 페이지 19-3
User Details(사용자 세부사항) 페이지 19-3
Web Sites(웹 사이트) 페이지 19-4
URL Categories(URL 카테고리) 페이지 19-4
URL 카테고리 집합 업데이트 및 보고 19-5
Application Visibility(애플리케이션 가시성) 페이지 19-5
Anti-Malware(안티멀웨어) 페이지 19-5
Malware Category Report(악성코드 카테고리 보고서) 페이지 19-6
Malware Threat Report(멀웨어 위협 보고서) 페이지 19-6
Advanced Malware Protection 페이지 19-6
File Analysis(파일 분석) 페이지 19-6
AMP Verdict Updates(AMP 판정 업데이트) 페이지 19-6
Client Malware Risk(클라이언트 악성코드 위험) 페이지 19-6
Web Proxy - Clients by Malware Risk(웹 프록시 - 악성코드 위험별 클라이언트)에 대한 Client Detail(클라이언트 세부사항) 페이지 19-7
Web Reputation Filters(웹 평판 필터) 페이지 19-7
L4 Traffic Monitor(L4 트래픽 모니터) 페이지 19-8
SOCKS Proxy(SOCKS 프록시) 페이지 19-8

Reports by User Location(사용자 위치별 보고서) 페이지 19-8
Web Tracking(웹 추적) 페이지 19-9
웹 프록시에서 처리되는 트랜잭션 검색 19-9
L4 트래픽 모니터에서 처리되는 트랜잭션 검색 19-12
SOCKS 프록시에서 처리되는 트랜잭션 검색 19-12
System Capacity(시스템 용량) 페이지 19-12
System Status(시스템 상태) 페이지 19-13

20장 **비표준 포트에서 비인가 트래픽 탐지** 20-1
비인가 트래픽 탐지 개요 20-1
L4 트래픽 모니터 구성 20-1
알려진 사이트 목록 20-2
L4 트래픽 모니터 전역 설정 구성 20-2
L4 트래픽 모니터 안티멀웨어 규칙 업데이트 20-3
비인가 트래픽을 탐지하기 위한 정책 생성 20-3
유효한 형식 20-4
L4 트래픽 모니터 활동 보기 20-5
활동 모니터링 및 요약 통계 보기 20-5
L4 트래픽 모니터 로그 파일 항목 20-5

21장 **로그를 통해 시스템 활동 모니터링** 21-1
로깅 개요 21-1
로깅에 대한 공통 작업 21-2
로깅에 대한 모범 사례 21-2
로그를 사용하여 웹 프록시 문제 트러블슈팅 21-2
로그 파일 유형 21-3
로그 서브스크립션 추가 및 편집 21-7
로그 파일을 다른 서버에 푸시 21-11
로그 파일 아카이브 21-12
로그 파일 이름 및 어플라이언스 디렉토리 구조 21-12
로그 파일 읽기 및 해석 21-13
로그 파일 보기 21-13
액세스 로그 파일의 웹 프록시 정보 21-14
트랜잭션 결과 코드 21-16
ACL 결정 태그 21-17
액세스 로그 스캐닝 판정 항목 해석 21-20

W3C 호환 액세스 로그 파일 21-24
W3C 필드 유형 21-24
W3C 액세스 로그 해석 21-25
W3C 로그 파일 헤더 21-25
W3C 필드 접두사 21-26
액세스 로그 맞춤화 21-26
액세스 로그 사용자 정의 필드 21-26
일반 액세스 로그 맞춤화 21-27
W3C 액세스 로그 맞춤화 21-28
CTA 특정 맞춤형 W3C 로그 구성 21-28
트래픽 모니터 로그 파일 21-30
트래픽 모니터 로그 해석 21-30
로그 파일 필드 및 태그 21-31
액세스 로그 형식 지정자 및 W3C 로그 파일 필드 21-31
악성코드 스캐닝 판정 값 21-40
로깅 트러블슈팅 21-41

22장 **시스템 관리 작업 수행** 22-1
시스템 관리 개요 22-1
어플라이언스 컨피그레이션 저장, 로드 및 재설정 22-2
어플라이언스 컨피그레이션 보기 및 인쇄 22-2
어플라이언스 컨피그레이션 파일 저장 22-2
어플라이언스 컨피그레이션 파일 로드 22-3
어플라이언스 컨피그레이션을 공장 기본값으로 재설정 22-3
기능 키에 대한 작업 22-4
기능 키 표시 및 업데이트 22-4
기능 키 업데이트 설정 변경 22-4
가상 어플라이언스 라이센스 22-5
가상 어플라이언스 라이센스 설치 22-5
원격 전원 관리 활성화 22-5
사용자 계정 관리 22-6
로컬 사용자 계정 관리 22-7
로컬 사용자 계정 추가 22-7
사용자 계정 삭제 22-8
사용자 계정 편집 22-8
암호 변경 22-8
RADIUS 사용자 인증 22-9
Radius 인증의 이벤트 순서 22-9

RADIUS를 사용하여 외부 인증 사용 22-9
사용자 환경 설정 정의 22-11
관리자 설정 구성 22-11
관리자의 암호 요건 설정 22-11
어플라이언스에 액세스하기 위한 추가 보안 설정 22-12
관리자 암호 재설정 22-13
생성된 메시지에 대한 반환 주소 구성 22-13
경고 관리 22-14
경고 분류 및 심각도 22-14
경고 수신자 관리 22-14
경고 수신자 추가 및 편집 22-14
경고 수신자 삭제 22-15
경고 설정 구성 22-15
경고 목록 22-16
기능 키 경고 22-16
하드웨어 알림 22-16
기록 경고 22-16
보고 경고 22-17
시스템 경보 22-19
업데이트 프로그램 경고 22-20
안티멀웨어 경고 22-20
FIPS 컴플라이언스 22-21
FIPS 인증서 요건 22-21
FIPS 모드 사용 또는 사용 안 함 22-21
시스템 날짜 및 시간 관리 22-22
시간대 설정 22-22
시스템 클록을 NTP 서버와 동기화 22-22
SSL 컨피그레이션 22-23
인증서 관리 22-24
인증서 및 키 정보 22-24
신뢰할 수 있는 루트 인증서 관리 22-24
인증서 업데이트 22-25
차단된 인증서 보기 22-25
인증서 및 키 업로드 또는 생성 22-25
인증서 및 키 업로드 22-25
인증서 및 키 생성 22-26
인증서 서명 요청 22-27
중간 인증서 22-27

AsyncOS for Web 업그레이드 및 업데이트 22-27
AsyncOS for Web 업그레이드 모범 사례 22-27
AsyncOS 및 보안 서비스 구성 요소 업그레이드 및 업데이트 22-28
AsyncOS for Web 업그레이드 22-28
자동 및 수동 업데이트 및 업그레이드 쿼리 22-28
수동으로 보안 서비스 구성 요소 업데이트 22-29
로컬 및 원격 업데이트 서버 22-29
Cisco 업데이트 서버에서 업데이트 및 업그레이드 22-30
로컬 서버에서 업그레이드 22-30
로컬 및 원격 업그레이드 방법 간의 차이점 22-31
업그레이드 및 서비스 업데이트 설정 구성 22-32
이전 버전의 AsyncOS for Web으로 되돌리기 22-33
가상 어플라이언스에서 AsyncOS를 되돌리면 라이센스에 영향을 미칠 수 있음 22-33
되돌리기 프로세스에서 컨피그레이션 파일 사용 22-33
SMA에서 관리되는 어플라이언스에 대한 AsyncOS 되돌리기 22-33
AsyncOS for Web을 이전 버전으로 되돌리기 22-34
SNMP를 사용하여 시스템 상태 모니터링 22-35
MIB 파일 22-35
SNMP 모니터링 사용 및 구성 22-36
하드웨어 개체 22-36
SNMP 트랩 22-36
connectivityFailure SNMP 트랩 정보 22-36
CLI 예: snmpconfig 22-37

부록 A
문제 해결 A-1
일반 트러블슈팅 모범 사례 A-2
인증 문제 A-2
인증 문제에 대한 트러블슈팅 툴 A-2
실패한 인증이 정상적인 작업에 영향을 미침 A-2
LDAP 문제 A-3
NTLMSSP로 인해 LDAP 사용자가 인증에 실패함 A-3
LDAP 참조로 인해 LDAP 인증 실패 A-3
기본 인증 문제 A-3
기본 인증 실패 A-3
단일 로그인 문제 A-4
사용자에게 자격 증명 프롬프트가 잘못 표시됨 A-4
브라우저 문제 A-4
WPAD가 Firefox에서 작동하지 않음 A-4

DNS 문제 A-5
경고: DNS 캐시를 부트스트랩하는 데 실패함 A-5
기능 키가 만료됨 A-5
페일오버 문제 A-5
잘못된 페일오버 구성 A-5
가상 어플라이언스에 대한 페일오버 문제 A-6
FTP 문제 A-6
URL 카테고리가 일부 FTP 사이트를 차단하지 않음 A-6
대용량 FTP 전송 연결 끊기 A-6
파일 업로드 후 FTP 서버에 0바이트 파일이 표시됨 A-6
FTP-over-HTTP 요청에서 Chrome 브라우저가 사용자 에이전트로 탐지되지 않음 A-6
하드웨어 문제 A-7
어플라이언스 전원 주기 A-7
어플라이언스 상태 표시기 A-7
경고: 380 또는 680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트) A-7
HTTPS/암호 해독/인증서 문제 A-7
URL 카테고리 기준을 사용하는 라우팅 정책을 통해 HTTPS 사이트에 액세스 A-8
HTTPS 요청 실패 A-8
IP 기반 서로게이트 및 투명 요청을 사용하는 HTTPS A-8
특정 웹 사이트에 대한 암호 해독 우회 A-8
경고: 보안 인증서 문제 A-9
ISE(Identity Services Engine) 문제 A-9
ISE 문제 트러블슈팅 툴 A-9
ISE 서버 연결 문제 A-10
인증서 문제 A-10
네트워크 문제 A-11
기타 ISE 서버 연결 문제 A-11
ISE 관련 위험 로그 메시지 A-11
기록 문제 A-12
맞춤형 URL 카테고리가 액세스 로그 항목에 표시되지 않음 A-12
HTTPS 트랜잭션 기록 A-12
경고: 생성되는 데이터의 비율을 유지할 수 없음 A-13
서드파티 로그 분석기 툴을 통한 W3C 액세스 로그 사용 문제 A-13
정책 문제 A-13
HTTPS에 대한 액세스 정책을 구성할 수 없음 A-13
차단된 개체 문제 A-14
일부 Microsoft Office 파일이 차단되지 않음 A-14
DOS 실행 가능 개체 유형을 차단하면 Windows OneCare에 대한 업데이트도 차단됨 A-14

식별 프로필이 정책에서 사라짐 A-14
정책 일치 실패 A-14
정책이 적용되지 않음 A-14
HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨 A-15
사용자가 HTTPS 및 FTP over HTTP 요청에 대한 전역 정책과 일치함 A-15
사용자가 잘못된 액세스 정책에 할당됨 A-15
정책 트러블슈팅 툴: 정책 추적 A-16
정책 추적 툴 정보 A-16
클라이언트 요청 추적 A-16
고급: 요청 세부 정보 A-17
고급: 응답 세부 정보 재지정 A-18
파일 평판 및 파일 분석 문제 A-18
재부팅 문제 A-19
재부팅 시 KVM에서 실행 중인 가상 어플라이언스가 정지됨 A-19
하드웨어 어플라이언스: 원격으로 어플라이언스 전원 재설정 A-19
사이트 액세스 문제 A-20
인증을 지원하지 않는 URL에 액세스할 수 없음 A-20
POST 요청을 사용하는 사이트에 액세스할 수 없음 A-20
업스트림 프록시 문제 A-21
업스트림 프록시가 기본 자격 증명을 수신하지 않음 A-21
업스트림 프록시에서 클라이언트 요청 실패 A-21
업스트림 프록시를 통해 FTP 요청을 라우팅할 수 없음 A-21
가상 어플라이언스 A-21
AsyncOS 시작 중에 강제 재설정, 전원 끄기 또는 재설정 옵션을 사용하지 않음 A-22
KVM 구축의 네트워크 연결이 처음에 작동한 후 실패함 A-22
KVM 구축 시 성능 저하, Watchdog 문제 및 높은 CPU 사용률 A-22
Linux 호스트에서 실행 중인 가상 어플라이언스에 대한 일반 트러블슈팅 A-22
WCCP 문제 A-22
최대 포트 항목 수 A-22
패킷 캡처 A-23
패킷 캡처 시작 A-23
패킷 캡처 파일 관리 A-24
패킷 캡처 파일 다운로드 또는 삭제 A-24
지원에 대한 작업 A-24
효율적인 서비스를 위해 정보 수집 A-24
기술 지원 요청 열기 A-25
가상 어플라이언스에 대한 지원 받기 A-25
어플라이언스에 대한 원격 액세스 사용 A-26

부록 B

CLI(Command Line Interface) B-1

CLI(Command Line Interface) 개요 B-1
CLI(Command Line Interface) 액세스 B-1
첫 번째 액세스 B-1
후속 액세스 B-2
명령 프롬프트에 대한 작업 B-2
명령 구문 B-2
선택 목록 B-3
예/아니요 쿼리 B-3
하위 명령 B-3
하위 명령 이스케이프 B-4
명령 기록 B-4
명령 완성 B-4
CLI를 사용하여 컨피그레이션 변경 사항 커밋 B-4
범용 CLI 명령 B-4
CLI 예: 컨피그레이션 변경 사항 커밋 B-5
CLI 예: 컨피그레이션 변경 사항 지우기 B-5
CLI 예: CLI(Command Line Interface) 세션 종료 B-5
CLI 예: CLI(Command Line Interface)에서 도움말 찾기 B-5
Web Security Appliance CLI 명령 B-6

부록 C

추가 리소스 C-1

Cisco 알림 서비스 C-1
문서 집합 C-1
교육 C-2
기술 자료(TechNotes) C-2
Cisco 지원 커뮤니티 C-2
고객 지원 C-2
리소스에 액세스하기 위해 Cisco 계정 등록 C-3
서드파티 기여자 C-3
Cisco에 의견 보내기 C-3

부록 D

최종 사용자 라이센스 계약 D-1

Cisco Systems 최종 사용자 라이센스 계약 D-1
Cisco Systems Content Security 소프트웨어에 대한 보충 최종 사용자 라이센스 계약 D-6

제품 및 릴리스 소개

- Web Security Appliance 소개, 1-1페이지
- 새로운 기능, 1-1페이지
- 어플라이언스 웹 인터페이스 사용, 1-3페이지
- Cisco SensorBase 네트워크, 1-5페이지

Web Security Appliance 소개

Cisco Web Security Appliance는 인터넷 트래픽을 가로채고 모니터링하며 정책을 적용하여 악성 코드, 민감한 데이터 손실, 생산성 손실 및 기타 인터넷 기반 위협으로부터 내부 네트워크를 지속적으로 보호합니다.

새로운 기능

- Cisco AsyncOS 9.0.1의 새로운 기능, 1-1페이지

Cisco AsyncOS 9.0.1의 새로운 기능

- Cisco AsyncOS 9.0.1-162(GD)의 새로운 기능, 1-2페이지
- Cisco AsyncOS 9.0.1-161(GD-물리적 어플라이언스만)의 새로운 기능, 1-2페이지
- Cisco AsyncOS 9.0.1-135(ED)의 새로운 기능, 1-2페이지

Cisco AsyncOS 9.0.1-162(GD)의 새로운 기능

기능	설명
ISE(Identity Services Engine) 버전	최대 2.0까지의 모든 ISE 버전이 지원됩니다.
최대 HTTP 헤더 크기	CLI 명령 `maxhttpheadersize`를 사용하여 프록시 요청에 대한 최대 HTTP 헤더 크기를 변경할 수 있습니다. 이 값을 늘리면 지정된 사용자가 다수의 인증 그룹에 속해 있거나 응답 헤더가 현재 최대 헤더 크기보다 큰 경우에 발생할 수 있는 정책 추적 실패를 완화할 수 있습니다. **참고** 이 명령은 AsyncOS 9.0에서 실제로 도입되었습니다.

Cisco AsyncOS 9.0.1-161(GD-물리적 어플라이언스만)의 새로운 기능

이 빌드는 물리적 어플라이언스에만 설치할 수 있습니다.

기능	설명
ISE(Identity Services Engine) 버전	최대 2.0까지의 모든 ISE 버전이 지원됩니다.
최대 HTTP 헤더 크기	CLI 명령 maxhttpheadersize를 사용하여 프록시 요청에 대한 최대 HTTP 헤더 크기를 변경할 수 있습니다. 이 값을 늘리면 지정된 사용자가 다수의 인증 그룹에 속해 있거나 응답 헤더가 현재 최대 헤더 크기보다 큰 경우에 발생할 수 있는 정책 추적 실패를 완화할 수 있습니다. **참고** 이 명령은 AsyncOS 9.0에서 실제로 도입되었습니다.

Cisco AsyncOS 9.0.1-135(ED)의 새로운 기능

이는 유지 관리 릴리스이므로 새 기능이 추가되지 않았습니다.

Cisco AsyncOS 9.2의 새로운 기능

참고 이 릴리스는 주로 구성되지 않은 디바이스에 하이브리드 웹 보안을 설치하기 위해 사용됩니다. 하이브리드 모드에서 어플라이언스를 작동하려는 계획이 아니면 이 버전을 설치하거나 이 버전으로 업그레이드하지 마십시오.

- Cisco AsyncOS 9.2.0-082의 새로운 기능, 1-2페이지
- Cisco AsyncOS 9.2.0-075의 새로운 기능, 1-3페이지

Cisco AsyncOS 9.2.0-082의 새로운 기능

이는 유지 관리 릴리스이므로 새 기능이 추가되지 않았습니다.

Cisco AsyncOS 9.2.0-075의 새로운 기능

하이브리드 웹 보안 모드는 Web Security appliance에 자동으로 다운로드되는 Cisco ScanCenter(Cloud Web Security에 대한 관리 포털)에 정의된 정책을 사용하여 통합 클라우드 및 온프레미스 정책 시행과 위협 방어를 제공합니다.

관련 주제

- 제품 릴리스 노트: http://www.cisco.com/en/US/partner/products/ps10164/prod_release_notes_list.html

어플라이언스 웹 인터페이스 사용

- 웹 인터페이스 브라우저 요건, 1-3페이지
- 가상 어플라이언스에서 웹 인터페이스에 대한 액세스 사용, 1-4페이지
- 어플라이언스 웹 인터페이스 액세스, 1-4페이지
- 웹 인터페이스 변경 사항 커밋, 1-5페이지
- 웹 인터페이스 변경 사항 지우기, 1-5페이지

웹 인터페이스 브라우저 요건

웹 인터페이스에 액세스하려면 브라우저가 JavaScript 및 쿠키를 지원하고, 허용하도록 설정되어 있어야 합니다. 또한 CSS(Cascading Style Sheet)가 포함된 HTML 페이지를 렌더링할 수 있어야 합니다.

Cisco Web Security Appliance는 YUI(http://yuilibrary.com/yui/environments/)에서 설정된 대상 환경을 따릅니다.

30분 동안 아무 작업도 수행하지 않으면 세션이 자동으로 시간 초과됩니다.

웹 인터페이스의 일부 버튼 및 링크를 클릭하면 추가 창이 열립니다. 따라서 웹 인터페이스를 사용하려면 브라우저의 팝업 차단 설정을 구성해야 할 수 있습니다.

참고 한 번에 하나의 브라우저 창 또는 탭만 사용하여 어플라이언스 컨피그레이션을 편집하십시오. 또한 웹 인터페이스 및 CLI를 동시에 사용하여 어플라이언스를 편집하지 마십시오. 동시에 여러 위치에서 어플라이언스를 편집하면 예기치 않은 동작이 발생하므로 이는 지원되지 않습니다.

가상 어플라이언스에서 웹 인터페이스에 대한 액세스 사용

기본적으로 HTTP 및 HTTPS 인터페이스는 가상 어플라이언스에서 사용하도록 설정되지 않습니다. 이러한 프로토콜을 사용하도록 설정하려면 CLI(Command Line Interface)를 사용해야 합니다.

1단계 CLI(Command Line Interface)에 액세스합니다. CLI(Command Line Interface) 액세스, B-1페이지를 참조하십시오.

2단계 `interfaceconfig` 명령을 실행합니다.

프롬프트에서 Enter를 누르면 기본값이 승인됩니다.

HTTP 및 HTTPS에 대한 프롬프트를 찾고 사용할 프로토콜을 사용하도록 설정합니다.

어플라이언스 웹 인터페이스 액세스

시작하기 전에

가상 어플라이언스를 사용하는 경우 가상 어플라이언스에서 웹 인터페이스에 대한 액세스 사용, 1-4페이지를 참조하십시오.

1단계 브라우저를 열고 웹 보안 어플라이언스의 IP 주소(또는 호스트 이름)를 입력합니다. 어플라이언스가 이전에 구성되지 않은 경우 기본 설정을 사용합니다.

`https://192.168.42.42:8443`

-또는-

`http://192.168.42.42:8080`

여기서 `192.168.42.42`는 기본 IP 주소이고, `8080`은 HTTP의 기본 관리 포트 설정이며, `8443`은 HTTPS의 기본 관리 포트입니다.

그렇지 않으면, 어플라이언스가 현재 구성되어 있는 경우 M1 포트의 IP 주소(또는 호스트 이름)를 사용합니다.

참고 어플라이언스에 연결할 때 포트 번호를 사용해야 합니다(기본적으로 포트 8080). 웹 인터페이스에 액세스할 때 포트 번호를 지정하지 못하면 기본 포트 80, Proxy Unlicensed(프록시 사용이 허가되지 않음) 오류 페이지가 표시됩니다.

2단계 어플라이언스 로그인 화면이 표시되면 사용자 이름과 암호를 입력하여 어플라이언스에 액세스합니다.

기본적으로 어플라이언스는 다음 사용자 이름 및 암호로 제공됩니다.

- 사용자 이름: **admin**
- 암호: **ironport**

기본 **admin** 사용자 이름으로 처음 로그인한 경우 즉시 암호를 변경하라는 프롬프트가 표시됩니다.

3단계 사용자 이름에 대한 최근 어플라이언스 액세스 시도(성공 또는 실패 모두) 목록을 보려면 애플리케이션 창의 오른쪽 위 모서리에 있는 "Logged in as(로그인된 계정)" 항목 앞의 최근 활동 아이콘(성공 또는 실패의 경우 각각 **i** 또는 **!**)을 클릭합니다.

웹 인터페이스 변경 사항 커밋

참고 모든 변경 사항을 커밋하기 전에 여러 컨피그레이션 변경 사항을 작성할 수 있습니다.

1단계 **Commit Changes(변경 사항 커밋)** 버튼을 클릭합니다.

2단계 선택한 경우 Comment(의견) 필드에 의견을 입력합니다.

3단계 **Commit Changes(변경 커밋)**를 클릭합니다.

웹 인터페이스 변경 사항 지우기

1단계 **Commit Changes(변경 사항 커밋)** 버튼을 클릭합니다.

2단계 **Abandon Changes(변경 사항 취소)**를 클릭합니다.

Cisco SensorBase 네트워크

Cisco SensorBase 네트워크는 전 세계적으로 수백만 개의 도메인을 추적하고 인터넷 트래픽에 대한 전역 관찰 목록을 유지 관리하는 위협 관리 데이터베이스입니다. SensorBase는 Cisco에 알려진 인터넷 도메인의 신뢰도 평가를 제공합니다. 웹 보안 어플라이언스는 SensorBase 데이터 피드를 사용하여 웹 평판 점수의 정확성을 향상시킵니다.

SensorBase 혜택 및 개인 정보 보호

Cisco SensorBase 네트워크에 참여한다는 것은 Cisco에서 데이터를 수집하고 해당 정보를 SensorBase 위협 관리 데이터베이스와 공유하는 것을 의미합니다. 이 데이터에는 요청 특성 및 어플라이언스에서 요청을 처리하는 방법에 대한 정보가 포함됩니다.

Cisco에서는 개인 정보 유지 관리의 중요성을 인식하고 사용자 이름 및 암호와 같은 개인 또는 기밀 정보를 수집하거나 사용하지 않습니다. 또한 기밀성을 보장하기 위해 호스트 이름 다음에 오는 파일 이름 및 URL 특성이 난독 처리됩니다. 암호 해독된 HTTPS 트랜잭션의 경우 SensorBase 네트워크가 인증서에 있는 서버 이름의 IP 주소, 웹 평판 점수 및 URL 카테고리만 수신합니다.

SenderBase 네트워크에 참여하는 데 동의하면 어플라이언스에서 전송된 데이터가 HTTPS를 사용하여 안전하게 전송됩니다. 데이터를 공유하면 웹 기반 위협에 대응하고 악의적인 활동으로부터 회사 환경을 보호하는 Cisco의 기능이 향상됩니다.

Cisco SensorBase 네트워크에 참여 사용

참고 표준 SensorBase 네트워크 참여는 시스템 설정 중에 기본적으로 사용하도록 설정됩니다.

1단계 **Security Services(보안 서비스) > SensorBase**를 선택합니다.

2단계 SensorBase 네트워크 참여가 사용하도록 설정되었는지 확인합니다.

사용하지 않도록 설정된 경우 어플라이언스에서 수집하는 데이터가 SensorBase 네트워크 서버로 다시 전송되지 않습니다.

3단계 Participation Level(참여 레벨) 섹션에서 다음 레벨 중 하나를 선택합니다.

- **Limited(제한적).** 기본 참여는 서버 이름 정보를 요약하고 MD5 해시 경로 세그먼트를 SensorBase 네트워크 서버에 전송합니다.
- **Standard(표준).** 향상된 참여는 모호하지 않은 경로 세그먼트가 포함된 전체 URL을 SensorBase 네트워크 서버에 전송합니다. 이 옵션은 더 강력한 데이터베이스를 제공하도록 지원하고 웹 평판 점수의 무결성을 지속적으로 향상시킵니다.

4단계 AnyConnect Network Participation(AnyConnect 네트워크 참여) 필드에서 Cisco AnyConnect 클라이언트를 사용하여 웹 보안 어플라이언스에 연결하는 클라이언트에서 수집된 정보를 포함할지 여부를 선택합니다.

AnyConnect 클라이언트가 보안 모빌리티 기능을 사용하여 어플라이언스에 웹 트래픽을 전송합니다.

5단계 Excluded Domains and IP Addresses(제외된 도메인 및 IP 주소) 필드에서 선택적으로 SensorBase 서버에 전송되는 트래픽에서 제외할 도메인 또는 IP 주소를 입력합니다.

6단계 변경 사항을 제출 및 커밋합니다.

연결, 설치 및 구성

- 연결, 설치 및 구성 개요, 2-1페이지
- 가상 어플라이언스 구축, 2-2페이지
- 운영 모드 비교, 2-2페이지
- 연결, 설치 및 구성 작업 개요, 2-2페이지
- 어플라이언스 연결, 2-3페이지
- 설정 정보 수집, 2-6페이지
- 시스템 설정 마법사, 2-7페이지
- 업스트림 프록시, 2-13페이지
- 네트워크 인터페이스, 2-14페이지
- 고가용성을 위한 페일오버 그룹 구성, 2-17페이지
- 웹 프록시 데이터용 P2 데이터 인터페이스 사용, 2-19페이지
- 리디렉션 호스트 이름 및 시스템 호스트 이름, 2-28페이지
- DNS 설정, 2-29페이지
- 연결, 설치 및 구성 트러블슈팅, 2-31페이지

연결, 설치 및 구성 개요

웹 보안 어플라이언스에서는 3가지 운영 모드(표준, Cloud Web Security Connector 및 하이브리드 웹 보안)를 제공합니다.

웹 보안 어플라이언스 작업의 표준 모드에는 Cloud Web Security Connector 모드에서 사용할 수 없는 온사이트 웹 프록시 서비스와 하이브리드 웹 보안 또는 Cloud Web Security Connector 모드에서 사용할 수 없는 레이어-4 트래픽 모니터링이 포함됩니다.

Cloud Web Security Connector 모드에서는 어플라이언스가 Cisco CWS(Cloud Web Security) 프록시에 연결하여 트래픽을 라우팅합니다. 여기서 웹 보안 정책이 시행됩니다.

하이브리드 웹 보안 모드는 웹 보안 어플라이언스에 자동으로 다운로드되는 Cisco ScanCenter(Cloud Web Security에 대한 관리 포털)에 정의된 정책을 사용하여 통합 클라우드 및 온프레미스 정책 시행과 위협 방어를 제공합니다.

어플라이언스에는 여러 네트워크 포트가 있으며 각 포트는 하나 이상의 특정 데이터 유형을 관리하도록 지정됩니다.

어플라이언스는 네트워크 경로, DNS, VLAN 및 기타 설정과 서비스를 사용하여 네트워크 연결성 및 트래픽 가로채기를 관리합니다. 시스템 설치 마법사를 사용하면 기본 서비스 및 설정을 지정할 수 있으며, 어플라이언스의 웹 인터페이스에서는 설정을 수정하고 추가 옵션을 구성할 수 있습니다.

가상 어플라이언스 구축

가상 Web Security Appliance를 구축하려면 *Cisco Content Security Virtual Appliance 설치 설명서* (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html)를 참조하십시오.

물리적 어플라이언스에서 가상 어플라이언스로 마이그레이션

물리적 어플라이언스에서 가상 어플라이언스로 구축을 마이그레이션하려면 이전 주제와 사용 중인 AsyncOS 버전의 릴리스 노트에서 참조되는 가상 어플라이언스 설치 설명서를 참조하십시오.

운영 모드 비교

Web Security Appliance 작업의 표준 모드에는 Cloud Web Security Connector 모드에서 사용할 수 없는 온사이트 웹 프록시 서비스와 하이브리드 웹 보안 또는 Cloud Web Security Connector 모드에서 사용할 수 없는 레이어-4 트래픽 모니터링이 포함됩니다.

Cloud Web Security Connector 모드에서는 어플라이언스가 Cisco Cloud Web Security 프록시에 연결하여 트래픽을 라우팅합니다. 여기서 웹 보안 정책이 적용됩니다.

하이브리드 웹 보안 모드에서는 Cisco Cloud Web Security 프록시에 대한 연결을 통합하여 클라우드 및 온프레미스 정책 시행과 위협 방어를 모두 제공합니다.

다음 표에는 각 모드에서 사용할 수 있는 다양한 메뉴 명령을 제시하여 각 모드에서 사용할 수 있는 다양한 기능을 표시합니다.

연결, 설치 및 구성 작업 개요

작업	추가 정보
1. 어플라이언스를 인터넷 트래픽에 연결합니다.	어플라이언스 연결, 2-3페이지
2. 설정 정보를 수집하여 기록합니다.	설정 정보 수집, 2-6페이지
3. 시스템 설정 마법사를 실행합니다.	시스템 설정 마법사, 2-7페이지
4. HTTPS 프록시 설정, 인증 영역 및 식별 프로필을 구성합니다. **하이브리드 웹 보안 모드의 경우 이 단계를 완료해야 합니다.**	HTTPS 프록시 사용, 11-3페이지 인증 영역, 5-10페이지 식별 프로필 및 인증, 6-8페이지
5. (선택 사항) 업스트림 프록시를 연결합니다.	업스트림 프록시, 2-13페이지

어플라이언스 연결

시작하기 전에

- 어플라이언스를 마운트하려면 관리를 위해 어플라이언스에 케이블을 연결하고 어플라이언스를 전원에 연결한 후 사용 중인 어플라이언스에 해당하는 하드웨어 설명서의 지침에 따릅니다. 해당 모델에 대한 이 문서의 위치는 문서 집합, C-1페이지를 참조하십시오.
- 투명 리디렉션을 위해 어플라이언스를 WCCP v2 라우터에 물리적으로 연결하려는 경우 먼저 WCCP 라우터가 레이어 2 리디렉션을 지원하는지 확인합니다.
- Cisco 컨피그레이션 권장 사항에 주의하십시오.
  - 향상된 성능과 보안을 위해 가능하면 심플렉스 케이블링을 사용합니다(수신 및 발신 트래픽에 별도의 케이블 사용).

1단계 아직 수행하지 않은 경우 관리 인터페이스를 연결합니다.

Ethernet 포트	참고
M1	다음을 수행할 수 있는 위치에 M1을 연결합니다. • 관리 트래픽을 전송하고 수신합니다. • (선택 사항) 웹 프록시 데이터 트래픽을 전송하고 수신합니다. M1에 직접 랩톱을 연결하여 어플라이언스를 관리할 수 있습니다. 호스트 이름(http://hostname:8080)을 사용하여 관리 인터페이스에 연결하려면 DNS 서버 데이터베이스에 어플라이언스 호스트 이름 및 IP 주소를 추가합니다.
P1 및 P2 (선택 사항)	• 아웃바운드 관리 서비스 트래픽에 사용할 수 있지만 관리용으로는 사용할 수 없습니다. • **Use M1 port for management only(M1 포트를 관리용으로만 사용)**(Network(네트워크) > Interfaces(인터페이스) 페이지)를 사용하도록 설정합니다. • 데이터 인터페이스를 사용하도록 서비스에 대한 라우팅을 설정합니다.

2단계 (선택 사항) 어플라이언스를 데이터 트래픽에 직접 연결하거나 투명 리디렉션 디바이스를 통해 연결합니다.

Ethernet 포트	명시적 전달	투명 리디렉션
P1/P2	P1 전용: • **Use M1 port for management only(M1 포트를 관리용으로만 사용)**를 사용하도록 설정합니다. • P1과 M1을 서로 다른 서브넷에 연결합니다. • 인바운드 및 아웃바운드 트래픽을 모두 수신할 수 있도록 듀플렉스 케이블을 사용하여 P1을 내부 네트워크와 인터넷에 연결합니다. P1 및 P2 • P1을 사용하도록 설정합니다. • M1, P1 및 P2를 서로 다른 서브넷에 연결합니다. • 인바운드 인터넷 트래픽을 수신하도록 P2를 인터넷에 연결합니다. 시스템 설정 마법사를 실행한 후 P2를 사용하도록 설정합니다.	디바이스: WCCP v2 라우터: • 레이어 2 리디렉션의 경우 라우터를 물리적으로 P1/P2에 연결합니다. • 레이어 3 리디렉션의 경우 GRE(Generic Routing Encapsulation)에 성능 문제가 발생할 수 있습니다. • 어플라이언스에서 WCCP 서비스를 생성합니다. 디바이스: 레이어-4 스위치: • 레이어 2 리디렉션의 경우 물리적으로 스위치를 P1/P2에 연결합니다. • 레이어 3 리디렉션의 경우 GRE(Generic Routing Encapsulation)에 성능 문제가 발생할 수 있습니다. **참고** 어플라이언스에서 인라인 모드를 지원하지 않습니다.
M1(선택 사항)	**Use M1 port for management only(M1 포트를 관리용으로만 사용)**가 사용하지 않도록 설정된 경우 M1이 데이터 트래픽에 대한 기본 포트입니다.	해당 없음

단계 3 (선택 사항) 레이어-4 트래픽을 모니터링하려면 프록시 포트 뒤와 클라이언트 IP 주소에 대한 NAT(Network Address Translation)를 수행하는 디바이스 앞의 TAP, 스위치 또는 허브에 어플라이언스를 연결합니다.

Ethernet 포트	참고
T1/T2	레이어 4 트래픽 모니터 차단을 허용하려면 레이어 4 트래픽 모니터를 Web Security Appliance와 동일한 네트워크에 배치합니다. **권장 컨피그레이션:** **디바이스: 네트워크 TAP:** • **아웃바운드 클라이언트 트래픽을 수신하기 위해 T1을 네트워크 TAP에 연결합니다.** • **인바운드 인터넷 트래픽을 수신하기 위해 T2를 네트워크 TAP에 연결합니다.** 기타 옵션: 디바이스: 네트워크 TAP: • 인바운드 및 아웃바운드 트래픽을 수신하기 위해 T1에서 듀플렉스 케이블을 사용합니다. 디바이스: 스위치의 스팬 또는 미러링 포트 • 아웃바운드 클라이언트 트래픽을 수신하기 위해 T1을 연결하고 인바운드 인터넷 트래픽을 수신하기 위해 T2를 연결합니다. • (덜 선호됨) 인바운드 및 아웃바운드 트래픽을 모두 수신하기 위해 하프 듀플렉스(half duplex) 또는 풀 듀플렉스(full-duplex) 케이블을 사용하여 T1을 연결합니다. 디바이스: 허브: • (가장 선호되지 않음) 인바운드 및 아웃바운드 트래픽을 모두 수신하기 위해 듀플렉스 케이블을 사용하여 T1을 연결합니다. 어플라이언스가 이러한 인터페이스의 모든 TCP 포트에서 트래픽을 수신합니다.

4단계 외부 프록시가 어플라이언스에서 데이터를 수신하도록 허용하려면 어플라이언스의 업스트림에 외부 프록시를 연결합니다.

다음 작업

- 설정 정보 수집, 2-6페이지

관련 주제

- 네트워크 인터페이스 사용 또는 변경, 2-15페이지
- 웹 프록시 데이터용 P2 데이터 인터페이스 사용, 2-19페이지
- WCCP 서비스 추가 및 편집, 2-22페이지
- 투명 리디렉션 구성, 2-22페이지
- 업스트림 프록시, 2-13페이지

설정 정보 수집

아래 워크시트를 사용하여 시스템 설치 마법사를 실행하는 동안 필요한 컨피그레이션 값을 기록할 수 있습니다. 각 속성에 대한 자세한 내용은 시스템 설정 마법사 참조 정보, 2-8페이지를 참조하십시오.

시스템 설정 마법사 워크시트

속성	값	속성	값
애플리케이션 세부 정보		**Routes**	
기본 시스템 호스트 이름		**관리 트래픽**	
로컬 DNS 서버 **(인터넷 루트 서버를 사용하지 않는 경우 필요함)**		Default Gateway	
DNS 서버 1		(선택 사항) 정적 경로 테이블 이름	
(선택 사항) DNS 서버 2		(선택 사항) 정적 경로 테이블 대상 네트워크	
(선택 사항) DNS 서버 3		(선택 사항) 표준 서비스 라우터 주소	
(선택 사항) 시간 설정		**(선택 사항) 데이터 트래픽**	
NTP(Network Time Protocol) 서버		Default Gateway	
(선택 사항) 외부 프록시 세부 정보		정적 경로 테이블 이름	
프록시 그룹 이름		정적 경로 테이블 대상 네트워크	
프록시 서버 주소		(선택 사항) **WCCP 설정**	
프록시 포트 번호		WCCP 라우터 주소	
인터페이스 세부 정보		WCCP 라우터 암호	
관리(M1) 포트		**관리 설정**	
IPv4 주소(필수) IPv6 주소(선택 사항)		관리자 암호	
네트워크 마스크		다음 사용자에게 이메일로 시스템 경고 보내기	
호스트 이름		(선택 사항) SMTP 릴레이 호스트	
(선택 사항) 데이터(P1) 포트			
IPv4(선택 사항) IPv6 주소(선택 사항)			
네트워크 마스크			
호스트 이름			

시스템 설정 마법사

시작하기 전에

- 어플라이언스를 네트워크 및 디바이스에 연결합니다. 어플라이언스 연결, 2-3페이지를 참조하십시오.
- System Setup Wizard 워크시트를 완료합니다. 설정 정보 수집, 2-6페이지를 참조하십시오.
- 가상 어플라이언스를 설정하는 경우:
  - `loadlicense` 명령을 사용하여 가상 어플라이언스 라이센스를 로드합니다. 자세한 내용은 *Cisco Content Security Virtual Appliance 설치 설명서* (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html)를 참조하십시오.
  - HTTP 및/또는 HTTPS 인터페이스 사용: CLI(Command Line Interface)에서 `interfaceconfig` 명령을 실행합니다.
- 시스템 설치 마법사에서 사용되는 각 컨피그레이션 항목에 대한 참조 정보는 시스템 설정 마법사 참조 정보, 2-8페이지에 있습니다.

경고 **어플라이언스를 처음 설치하거나 기존 컨피그레이션을 완전히 덮어쓰려는 경우에만 시스템 설치 마법사를 사용하십시오.**

1단계 브라우저를 열고 웹 보안 어플라이언스의 IP 주소를 입력합니다. 처음으로 시스템 설치 마법사를 실행하는 경우 기본 IP 주소를 사용합니다.

`https://192.168.42.42:8443`

-또는-

`http://192.168.42.42:8080`

여기서 `192.168.42.42`는 기본 IP 주소이고, `8080`은 HTTP의 기본 관리 포트 설정이며, `8443`은 HTTPS의 기본 관리 포트입니다.

그렇지 않으면, 어플라이언스가 현재 구성된 경우 M1 포트의 IP 주소를 사용합니다.

2단계 어플라이언스 로그인 화면이 표시되면 사용자 이름과 암호를 입력하여 어플라이언스에 액세스합니다. 기본적으로 어플라이언스는 다음 사용자 이름 및 암호와 함께 제공됩니다.

- 사용자 이름: **admin**
- 암호: **ironport**

3단계 즉시 암호를 변경해야 합니다.

4단계 어플라이언스가 이미 구성된 경우, **System Administration(시스템 관리) > System Setup Wizard(시스템 설정 마법사)**를 선택합니다.

어플라이언스가 이미 구성된 경우, 컨피그레이션을 재설정하려고 한다는 경고 메시지가 표시됩니다. 시스템 설치 마법사를 계속 진행하려면 **Reset Configuration(컨피그레이션 재설정)** 버튼을 클릭합니다. 어플라이언스가 재설정되고 브라우저가 어플라이언스 홈 화면으로 새로 고침됩니다.

5단계 최종 사용자 라이센스 계약의 약관을 읽고 동의합니다.

6단계 **Begin Setup(설정 시작)**을 클릭하여 계속 진행합니다.

7단계 필요에 따라 다음 섹션에 제공된 참조표를 사용하여 모든 설정을 구성합니다. 시스템 설정 마법사 참조 정보, 2-8페이지를 참조하십시오.

8단계 컨피그레이션 정보를 검토합니다. 옵션을 변경해야 할 경우 해당 섹션의 **Edit(편집)** 버튼을 클릭합니다.

9단계 **Install This Configuration(이 컨피그레이션 설치)**을 클릭합니다.

컨피그레이션이 설치되면 *Next Steps(다음 단계)* 페이지가 표시되어야 합니다. 그러나 설정 과정 동안 구성한 IP, 호스트 이름 또는 DNS 설정에 따라 이 단계에서 어플라이언스의 연결이 끊어질 수 있습니다. 브라우저에 "page not found(페이지를 찾을 수 없음)" 오류가 표시되는 경우 URL을 변경하여 새 주소 설정을 반영하고 페이지를 다시 로드합니다. 그런 다음, 수행하려는 모든 후속 설정 작업을 계속 진행합니다.

시스템 설정 마법사 참조 정보

- 네트워크/시스템 설정, 2-8페이지
- 네트워크/네트워크 인터페이스 및 와이어링, 2-10페이지
- 네트워크/관리 및 데이터 트래픽에 대한 경로, 2-11페이지
- 네트워크/투명 연결 설정, 2-11페이지
- 네트워크/관리 설정, 2-12페이지

네트워크/시스템 설정

속성	설명
기본 시스템 호스트 이름	시스템 호스트 이름은 다음 영역에서 어플라이언스를 식별하는 데 사용되는 정규화된 호스트 이름입니다. • CLI(Command Line Interface) • 시스템 경고 • 최종 사용자 알림 및 승인 페이지 • 웹 보안 어플라이언스가 Active Directory 도메인에 조인하는 경우 머신 NetBIOS 이름을 형성할 때 시스템 호스트 이름은 인터페이스 호스트 이름과 직접 대응되지 않으며 클라이언트에서 어플라이언스에 연결하는 데 사용되지 않습니다.
DNS 서버	• **인터넷 루트 DNS 서버 사용** – 어플라이언스에서 네트워크에 있는 DNS 서버에 액세스할 수 없는 경우 도메인 이름 서비스 조회를 위해 인터넷 루트 DNS 서버를 사용하도록 선택할 수 있습니다. **참고** 인터넷 루트 DNS 서버는 로컬 호스트 이름을 확인하지 않습니다. 어플라이언스에서 로컬 호스트 이름을 확인해야 하는 경우 로컬 DNS 서버를 사용하거나 CLI를 사용하여 로컬 DNS에 적절한 정적 항목을 추가해야 합니다. **이 DNS 서버 사용** – 어플라이언스에서 호스트 이름을 확인하는 데 사용할 수 있는 로컬 DNS 서버의 주소를 제공합니다. 이러한 설정에 대한 자세한 내용은 DNS 설정, 2-29페이지를 참조하십시오.

속성	설명
NTP 서버	시스템 클록을 네트워크 또는 인터넷에 있는 다른 서버와 동기화하는 데 사용되는 NTP(Network Time Protocol) 서버입니다. 기본값은 time.sco.cisco.com입니다.
Time Zone	어플라이언스의 위치에 대한 시간대 정보를 제공합니다. 메시지 헤더와 로그 파일의 타임스탬프에 영향을 줍니다.
어플라이언스 운영 모드	• 표준 – 표준 온프레미스 정책 시행에 사용됩니다. • Cloud Web Security Connector – 주로 정책 시행 및 위협 방어를 위해 Cisco Cloud Web Security 서비스에 트래픽을 전달하는 데 사용됩니다. 이러한 운영 모드에 대한 자세한 내용은 운영 모드 비교, 2-2페이지를 참조하십시오.

네트워크/네트워크 상황

참고 다른 프록시 서버가 포함된 네트워크에서 웹 보안 어플라이언스를 사용하는 경우 웹 보안 어플라이언스를 클라이언트와 더 가깝게 프록시 서버로부터 다운스트림에 배치하는 것이 좋습니다.

속성	설명
네트워크에 다른 웹 프록시가 있습니까?	네트워크에 다음과 같은 다른 프록시가 있습니까? **a.** 트래픽이 해당 프록시를 통과해야 합니다. **b.** 웹 보안 어플라이언스의 업스트림입니다. 두 가지 사항에 모두 해당하는 경우 이 확인란을 선택합니다. 이렇게 하면 하나의 업스트림 프록시에 대한 프록시 그룹을 생성할 수 있습니다. 나중에 업스트림 프록시를 더 추가할 수 있습니다.
프록시 그룹 이름	어플라이언스에서 프록시 그룹을 식별하는 데 사용되는 이름입니다.
주소	업스트림 프록시 서버의 호스트 이름 또는 IP 주소입니다.
포트	업스트림 프록시 서버의 포트 번호입니다.

관련 주제

- 업스트림 프록시, 2-13페이지

네트워크/네트워크 인터페이스 및 와이어링

웹 보안 어플라이언스를 관리하는 데 사용할 IP 주소, 네트워크 마스크 및 호스트 이름이며, 기본적으로 프록시(데이터) 트래픽에 사용됩니다.

어플라이언스 관리 인터페이스에 연결할 때 여기에 지정된 호스트 이름을 사용할 수 있지만(또는 M1이 프록시 데이터용으로 사용되는 경우 브라우저 프록시 설정에서) 해당 호스트 이름을 조직의 DNS에 등록해야 합니다.

설정	설명
Ethernet 포트	(선택 사항) 데이터 트래픽용으로 별도의 포트를 사용하려면 **Use M1 port for management only(M1 포트를 관리용으로만 사용)**를 선택합니다. M1 인터페이스를 관리 트래픽용으로만 구성하는 경우 데이터 트래픽용 P1 인터페이스를 구성해야 합니다. 또한 관리 및 데이터 트래픽에 대해 다른 경로를 정의해야 합니다. 그러나 M1 인터페이스가 관리 및 데이터 트래픽 모두에 사용되는 경우에도 P1 인터페이스를 구성할 수 있습니다. 시스템 설치 마법사에서는 P1 포트만 사용하도록 설정하고 구성할 수 있습니다. P2 인터페이스를 사용하도록 설정하려면 시스템 설치 마법사 완료 후 이를 수행해야 합니다.
IP 주소/넷마스크	이 네트워크 인터페이스에서 Web Security Appliance를 관리할 때 사용할 IP 주소 및 네트워크 마스크입니다.
호스트 이름	이 네트워크 인터페이스에서 Web Security Appliance를 관리할 때 사용할 호스트 이름입니다.

네트워크/레이어 4 트래픽 모니터 와이어링

속성	설명
레이어-4 트래픽 모니터	"T" 인터페이스에 플러그된 유선 연결의 유형입니다. • **듀플렉스 TAP.** T1 포트가 수신 및 발신 트래픽을 모두 수신합니다. • **심플렉스 TAP.** T1 포트는 발신 트래픽(클라이언트에서 인터넷으로)을 수신하고 T2 포트는 수신 트래픽(인터넷에서 클라이언트로)을 수신합니다. Cisco에서는 성능과 보안이 향상될 수 있으므로 가능하면 심플렉스(Simplex)를 사용하는 것을 권장합니다.

네트워크/관리 및 데이터 트래픽에 대한 경로

참고 "Use M1 port for management only(M1 포트를 관리용으로만 사용)"를 사용하도록 설정하면 이 섹션에 관리 및 데이터 트래픽에 대한 별도의 섹션이 표시됩니다. 그렇지 않으면 하나의 공동 섹션이 표시됩니다.

속성	설명
기본 게이트웨이	관리 및 데이터 인터페이스를 통한 트래픽에 사용할 기본 게이트웨이 IP 주소입니다.
정적 경로 테이블	관리 및 데이터 트래픽에 대한 선택적인 정적 경로입니다. 여러 경로를 추가할 수 있습니다. • **Name(이름)** – 정적 경로를 식별하는 데 사용되는 이름입니다. • **Internal Network(내부 네트워크)** – 네트워크에 있는 이 경로의 대상에 대한 IPv4 주소입니다. • **Internal Gateway(내부 게이트웨이)** – 이 경로에 대한 게이트웨이 IPv4 주소입니다. 경로 게이트웨이는 구성된 관리 또는 데이터 인터페이스와 동일한 서브넷에 있어야 합니다.

네트워크/투명 연결 설정

속성	설명
레이어-4 스위치 또는 디바이스 없음	웹 보안 어플라이언스가 투명 리디렉션을 위해 레이어-4 스위치에 연결되거나 투명 리디렉션 디바이스가 사용되지 않고 클라이언트가 명시적으로 요청을 어플라이언스에 전달하도록 지정합니다.
WCCP v2 라우터	웹 보안 어플라이언스가 버전 2 WCCP 지원 라우터에 연결되도록 지정합니다. 어플라이언스를 버전 2 WCCP 라우터에 연결하는 경우 하나 이상의 WCCP 서비스를 생성해야 합니다. 이 화면에서 또는 시스템 설치 마법사가 완료된 후 표준 서비스를 사용하도록 설정할 수 있습니다. 여기서 여러 동적 서비스를 생성할 수도 있습니다. 표준 서비스를 사용하도록 설정하는 경우 라우터 보안을 사용하도록 설정하고 암호를 입력할 수도 있습니다. 여기에서 사용된 암호는 동일한 서비스 그룹에 있는 모든 어플라이언스와 WCCP 라우터에 사용되어야 합니다. 표준 서비스 유형("웹 캐시" 서비스라고도 함)에는 고정된 ID 0, 고정된 리디렉션 방법(대상 포트를 통해) 및 고정된 대상 포트 80이 할당됩니다. 동적 서비스 유형을 사용하여 맞춤형 ID, 포트 번호, 리디렉션 및 로드 밸런싱 옵션을 정의할 수 있습니다.

네트워크/관리 설정

속성	설명
관리자 암호	관리 목적으로 웹 보안 어플라이언스에 액세스하는 데 사용되는 암호입니다.
다음 사용자에게 이메일로 시스템 경고 보내기	어플라이언스가 시스템 경고를 전송하는 이메일 주소입니다.
SMTP 릴레이 호스트로 이메일 전송(선택 사항)	AsyncOS가 시스템에서 생성된 이메일 메시지를 전송하는 데 사용할 수 있는 SMTP 릴레이 호스트의 주소 및 포트입니다. 정의된 SMTP 릴레이 호스트가 없는 경우 AsyncOS에서는 MX 레코드에 나열된 메일 서버를 사용합니다.
자동지원	어플라이언스에서 Cisco 고객 지원에 시스템 경고와 주별 상태 보고서를 전송할지 여부를 지정합니다.
SensorBase 네트워크 참여	Cisco SensorBase 네트워크에 참여할지 여부를 지정합니다. 참여하는 경우 Limited 또는 Standard(전체) 참여를 구성할 수 있습니다. 기본값은 Standard입니다. SensorBase 네트워크는 전 세계적으로 수백만 개의 도메인을 추적하고 인터넷 트래픽에 대한 전역 관찰 목록을 유지 관리하는 위협 관리 데이터베이스입니다. SensorBase 네트워크 참여를 사용하도록 설정하면 웹 보안 어플라이언스가 HTTP 요청에 대한 익명 통계를 Cisco에 전송하여 SensorBase 네트워크 데이터값을 증가시킵니다.

보안/보안 설정

옵션	설명
전역 정책 기본 조치	시스템 설치 마법사가 완료된 후 기본적으로 모든 웹 트래픽을 차단하거나 모니터링할지를 지정합니다. 전역 액세스 정책에 대한 프로토콜 및 사용자 에이전트 설정을 편집하여 나중에 이 동작을 변경할 수 있습니다. 기본 설정은 트래픽을 모니터링하는 것입니다.
L4 트래픽 모니터	시스템 설치 마법사가 완료된 후 레이어-4 트래픽 모니터에서 의심되는 악성코드를 기본적으로 모니터링해야 할지 또는 차단해야 할지를 지정합니다. 나중에 이 동작을 변경할 수 있습니다. 기본 설정은 트래픽을 모니터링하는 것입니다.
허용 가능한 사용 컨트롤	제한적 사용 제어를 사용하도록 설정할지 여부를 지정합니다. 사용하도록 설정된 경우 제한적 사용 제어를 사용하여 URL 필터링을 기반으로 정책을 구성할 수 있습니다. 또한 애플리케이션 가시성 및 제어와 안전한 검색 시행 등의 관련 옵션을 제공합니다. 기본적으로 사용하도록 설정되어 있습니다.
평판 필터링	전역 정책 그룹에 대한 웹 평판 필터링을 사용하도록 설정할지 여부를 지정합니다. 웹 평판 필터는 웹 서버 동작을 분석하고 URL에 평판 점수를 할당하여 URL 기반의 악성코드를 포함할 가능성을 판별하는 보안 기능입니다. 기본적으로 사용하도록 설정되어 있습니다.

옵션	설명
악성코드 및 스파이웨어 스캐닝	Webroot, McAfee 또는 Sophos를 사용하여 악성코드 및 스파이웨어 스캐닝을 사용하도록 설정할지 여부를 지정합니다. 기본적으로 3개 옵션 모두 사용하도록 설정되어 있습니다. 옵션이 사용하도록 설정된 경우 탐지된 악성코드를 모니터링하거나 차단할지도 선택합니다. 기본 설정은 악성코드를 모니터링하는 것입니다. 시스템 설치 마법사를 완료한 후 악성코드 스캐닝을 추가로 구성할 수 있습니다.
Cisco 데이터 보안 필터링	Cisco 데이터 보안 필터를 사용하도록 설정할지 여부를 지정합니다. 사용하도록 설정된 경우 Cisco 데이터 보안 필터가 네트워크에서 나가는 데이터를 평가하고 특정 유형의 업로드 요청을 차단하기 위한 Cisco 데이터 보안 정책을 생성할 수 있도록 합니다. 기본적으로 사용하도록 설정되어 있습니다.

업스트림 프록시

웹 프록시는 대상 웹 서버로 직접 웹 트래픽을 전달하거나 라우팅 정책을 사용하여 외부 업스트림 프록시로 리디렉션할 수 있습니다.

- 업스트림 프록시 작업 개요, 2-13페이지
- 업스트림 프록시에 대한 프록시 그룹 생성, 2-13페이지

업스트림 프록시 작업 개요

작업	추가 정보
1. Cisco Web Security Appliance의 외부 프록시 업스트림에 연결합니다.	어플라이언스 연결, 2-3페이지
2. 업스트림 프록시에 대한 프록시 그룹을 생성하고 구성합니다.	업스트림 프록시에 대한 프록시 그룹 생성, 2-13페이지
3. 업스트림 프록시로 라우팅되는 트래픽을 관리하기 위한 프록시 그룹의 라우팅 정책을 생성합니다.	인터넷 요청을 제어하기 위한 정책 생성

업스트림 프록시에 대한 프록시 그룹 생성

1단계 **Network(네트워크) > Upstream Proxies(업스트림 프록시)**를 선택합니다.

2단계 **Add Group(그룹 추가)**을 클릭합니다.

3단계 프록시 그룹 설정을 완료합니다.

속성	설명
이름	어플라이언스에서 프록시 그룹을 식별하는 데 사용되는 이름입니다(예: 라우팅 정책에서).

속성	설명
프록시 서버	그룹에 있는 프록시 서버에 대한 주소, 포트 및 다시 연결 시도 횟수(프록시가 응답하지 않는 경우)입니다. 필요에 따라 각 프록시 서버에 대한 행을 추가하거나 삭제할 수 있습니다. **참고** 동일한 프록시 서버를 여러 번 입력하여 프록시 그룹에 있는 프록시 간에 동등하지 않은 부하 분산을 허용할 수 있습니다.
부하 균형	웹 프록시가 여러 업스트림 프록시 간에 요청의 부하를 분산하는 데 사용하는 전략입니다. 다음 중에서 선택합니다. • **없음(페일오버)**. 웹 프록시가 그룹에 있는 하나의 외부 프록시에 트랜잭션을 전달합니다. 프록시가 나열된 순서대로 프록시에 연결하려고 시도합니다. 하나의 프록시에 연결할 수 없는 경우 웹 프록시가 목록에 있는 다음 프록시에 연결하려고 시도합니다. • **최소 연결**. 웹 프록시가 그룹에 있는 여러 프록시를 사용하는 활성 요청의 수를 추적하고 현재 가장 적은 수의 연결을 서비스하는 프록시에 트랜잭션을 전달합니다. • **해시 기반. 가장 오래전에 사용**. 모든 프록시가 현재 활성 상태인 경우 웹 프록시는 최근 가장 적은 트랜잭션을 수신한 프록시에 트랜잭션을 전달합니다. 웹 프록시에서 프록시가 다른 프록시 그룹의 구성원이 되어 수신한 트랜잭션도 고려한다는 점을 제외하고 이 설정은 라운드 로빈과 유사합니다. 즉, 프록시가 여러 프록시 그룹에 나열된 경우 "least recently used(가장 오래전에 사용)" 옵션을 사용하면 해당 프록시가 과부하될 가능성이 낮아집니다. • **라운드 로빈**. 웹 프록시가 나열된 순서대로 그룹에 있는 모든 프록시 간에 동등하게 트랜잭션을 순환합니다. **참고** 2개 이상의 프록시가 정의될 때까지 로드 밸런싱 옵션은 흐리게 표시됩니다.
오류 처리	이 그룹의 모든 프록시가 실패할 경우 수행할 기본 조치를 지정합니다. 다음 중에서 선택합니다. • **직접 연결.** 요청을 목적지 서버에 직접 전송합니다. • **요청 삭제.** 요청을 전달하지 않고 무시합니다.

4단계 변경 사항을 제출 및 커밋합니다.

다음 작업.

- 정책 생성, 10-5페이지

네트워크 인터페이스

- IP 주소 버전, 2-15페이지
- 네트워크 인터페이스 사용 또는 변경, 2-15페이지

IP 주소 버전

표준 모드에서는 대부분의 경우에 Cisco Web Security Appliance가 IPv4 및 IPv6 주소를 지원합니다.

참고 클라우드 커넥터 모드에서는 Cisco Web Security Appliance가 IPv4만 지원합니다.

DNS 서버는 IPv4 및 IPv6 주소가 모두 포함된 결과를 반환할 수 있습니다. 이러한 상황에서 AsyncOS 동작을 구성할 수 있도록 DNS 설정에 IP 주소 버전 환경 설정이 포함됩니다.

인터페이스/서비스	IPv4	IPv6	참고
M1 인터페이스	필수	선택 사항	IPv6 주소를 사용하려면 기본 IPv6 게이트웨이를 정의하는 IPv6 라우팅 테이블이 필요합니다. 네트워크에 따라 라우팅 테이블에 정적 IPv6 경로를 지정해야 할 수도 있습니다.
P1 인터페이스	선택 사항	선택 사항	P1 인터페이스에 IPv6 주소가 구성되어 있으며 어플라이언스에서 분할 라우팅(별도의 관리 및 데이터 경로)을 사용하는 경우 P1 인터페이스가 관리 경로에 구성된 IPv6 게이트웨이를 사용할 수 없습니다. 대신 데이터 라우팅 테이블용 IPv6 게이트웨이를 지정합니다.
P2 인터페이스	선택 사항	선택 사항	—
데이터 서비스	지원	지원	—
제어 및 관리 서비스	지원	부분적으로 지원됨	이미지(예: 최종 사용자 알림 페이지의 맞춤형 로고)에는 IPv4가 필요합니다.
AnyConnect Secure Mobility(MUS)	지원	지원되지 않음	—

관련 주제

- 네트워크 인터페이스 사용 또는 변경, 2-15페이지
- DNS 설정, 2-29페이지

네트워크 인터페이스 사용 또는 변경

- 인터페이스 IP 주소 추가 또는 수정
- 레이어-4 트래픽 모니터 와이어링 유형 변경
- 관리 및 데이터 트래픽의 분할 라우팅 사용

1단계 **Network(네트워크) > Interfaces(인터페이스)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 인터페이스 옵션을 구성합니다.

옵션	설명
인터페이스	필요에 따라 M1, P1 또는 P2 인터페이스에 대한 새로운 IPv4 또는 IPv6 주소, 넷마스크 및 호스트 이름 세부 정보를 수정하거나 추가합니다. • **M1** – AsyncOS에는 M1(관리) 포트에 IPv4 주소가 필요합니다. IPv4 주소 이외에 IPv6 주소를 지정할 수 있습니다. 기본적으로 관리 인터페이스는 어플라이언스 및 웹 프록시 (데이터) 모니터링을 관리하는 데 사용됩니다. 그러나 M1 포트를 관리 전용으로 구성할 수 있습니다. • **P1** 및 **P2** – IPv4 주소, IPv6 주소 또는 두 버전 모두를 데이터 포트에 사용합니다. 데이터 인터페이스는 웹 프록시 모니터링 및 레이어-4 트래픽 모니터 차단(선택 사항)에 사용됩니다. DNS, 소프트웨어 업그레이드, NTP 및 트레이스라우트(traceroute) 데이터 트래픽과 같은 아웃바운드 서비스를 지원하도록 이러한 인터페이스를 구성할 수도 있습니다. **참고** 관리 및 데이터 인터페이스가 모두 구성된 경우 각각에 다른 서브넷의 IP 주소가 지정되어야 합니다.
관리 서비스에 대한 개별 라우팅	데이터 트래픽용으로 별도의 포트를 사용하도록 하여 M1을 관리 트래픽 전용으로 제한하려면 **Restrict M1 port to appliance management services only(M1 포트를 어플라이언스 관리 서비스로만 제한)**를 확인합니다. **참고** M1을 관리 트래픽용으로만 사용하는 경우 다른 서브넷에 프록시 트래픽용 데이터 인터페이스를 하나 이상 구성합니다. 관리 및 데이터 트래픽에 대해 다른 경로를 정의합니다.
어플라이언스 관리 서비스	다음 네트워크 프로토콜의 사용을 사용하도록 설정/사용하지 않도록 설정하고 이에 대한 기본 포트 번호를 지정합니다. • **FTP** – 기본적으로 사용하지 않도록 설정되어 있습니다. • **SSH** • **HTTP** • **HTTPS** 또한 HTTP 트래픽의 HTTPS로의 리디렉션을 사용하도록 설정/사용하지 않도록 설정할 수 있습니다.

4단계 변경 사항을 제출 및 커밋합니다.

다음 작업

- IPv6 주소를 추가한 후 IPv6 라우팅 테이블을 추가합니다.

관련 주제

- 어플라이언스 연결, 2-3페이지
- IP 주소 버전, 2-15페이지
- TCP/IP 트래픽 경로 구성, 2-20페이지

고가용성을 위한 페일오버 그룹 구성

CARP(Common Address Redundancy Protocol)를 사용하면 WSA가 네트워크에 있는 여러 호스트에서 IP 주소를 공유할 수 있도록 하여 해당 호스트에서 제공되는 서비스의 고가용성을 보장하기 위한 IP 이중화를 제공합니다. CARP에는 3가지 호스트 상태가 있습니다.

- master
- backup
- init

서비스를 제공할 수 있는 각 페일오버 그룹마다 하나의 마스터 호스트만 존재할 수 있습니다.

페일오버 그룹 추가

시작하기 전에

- 이 페일오버 그룹에 독점적으로 사용될 가상 IP 주소를 식별합니다. 클라이언트가 이 IP 주소를 사용하여 명시적 전달 프록시 모드에서 페일오버 그룹에 연결합니다.
- 다음 매개변수에 대해 동일한 값을 사용하여 페일오버 그룹의 모든 어플라이언스를 구성합니다.
  - 페일오버 그룹 ID
  - 호스트 이름
  - 가상 IP 주소
- 가상 어플라이언스에서 이 기능을 구성할 경우 각 어플라이언스에 특정한 가상 스위치 및 가상 인터페이스가 혼합 모드를 사용하도록 구성되었는지 확인합니다. 자세한 내용은 가상 하이퍼바이저 설명서를 참조하십시오.

1단계 **Network(네트워크)** > **High Availability(고가용성)**를 선택합니다.

2단계 **Add Failover Group(페일오버 그룹 추가)**을 클릭합니다.

3단계 1에서 255 범위의 **Failover Group ID(페일오버 그룹 ID)**를 입력합니다.

4단계 (선택 사항) **Description(설명)**을 입력합니다.

5단계 **Hostname(호스트 이름)**을 입력합니다(예: *www.example.com*).

6단계 **Virtual IP Address and Netmask(가상 IP 주소 및 넷마스크)**를 입력합니다(예: *10.0.0.3/24*(IPv4) 또는 *2001:420:80:1::5/32*(IPv6)).

7단계 **Interface(인터페이스)** 메뉴에서 옵션을 선택합니다. **Select Interface Automatically(자동으로 인터페이스 선택)** 옵션은 사용자가 제공한 IP 주소를 기반으로 인터페이스를 선택합니다.

참고 **Select Interface Automatically(자동으로 인터페이스 선택)** 옵션을 선택하지 않은 경우에는 사용자가 제공한 가상 IP 주소와 동일한 서브넷에 있는 인터페이스를 선택해야 합니다.

8단계 우선순위를 선택합니다. **Master(마스터)**를 클릭하여 우선순위를 255로 설정합니다. 또는 **Backup(백업)**을 선택하고 **Priority(우선순위)** 필드에 1(최저)에서 254 사이의 우선순위를 입력합니다.

9단계 (선택 사항) 서비스에 대한 보안을 사용하도록 설정하려면 **Enable Security for Service(서비스에 대한 보안 사용)** 확인란을 선택하고 **Shared Secret(공유 암호)** 및 **Retype Shared Secret(공유 암호 다시 입력)** 필드에 공유 암호로 사용될 문자열을 입력합니다.

참고 페일오버 그룹의 모든 어플라이언스에 대한 공유 암호, 가상 IP 및 페일오버 그룹 ID가 동일해야 합니다.

10단계 **Advertisement Interval(알림 간격)** 필드에 사용 가능성에 대해 알리는 호스트 간의 지연 시간(1~255초)을 입력합니다.

11단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 페일오버 문제, A-5페이지

고가용성 전역 설정 편집

1단계 **Network(네트워크)** > **High Availability(고가용성)**를 선택합니다.

2단계 High Availability Global Settings(고가용성 전역 설정) 영역에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **Failover Handling(페일오버 처리)** 메뉴에서 옵션을 선택합니다.

- **Preemptive(선점형)** - 사용 가능한 경우 우선순위가 가장 높은 호스트가 제어를 담당합니다.
- **Non-preemptive(비선점형)** - 우선순위가 더 높은 호스트가 사용 가능하게 되더라도 제어 중인 호스트가 계속 제어합니다.

4단계 **Submit(제출)**를 클릭합니다. 또는 변경을 취소하려면 **Cancel(취소)**을 클릭합니다.

페일오버 그룹의 상태 보기

Network(네트워크) > **High Availability(고가용성)**를 선택합니다. **Failover Groups(페일오버 그룹)** 영역에 현재 페일오버 그룹이 표시됩니다. **Refresh Status(상태 새로 고침)**를 클릭하여 표시를 업데이트할 수 있습니다. **Network(네트워크)** > **Interfaces(인터페이스)** 또는 **Report(보고서)** > **System Status(시스템 상태)**를 선택하여 페일오버 세부 정보를 볼 수도 있습니다.

웹 프록시 데이터용 P2 데이터 인터페이스 사용

기본적으로 웹 프록시는 P2가 사용하도록 설정되어 있는 경우에도 P2에서 요청을 수신하지 않습니다. 그러나 웹 프록시 데이터를 수신하도록 P2를 구성할 수 있습니다.

참고 `advancedproxyconfig > miscellaneous` CLI 명령을 사용하여 P2에서 클라이언트 요청을 수신하도록 설정하는 경우 P1 또는 P2를 발신 트래픽용으로 사용할지를 선택할 수 있습니다. P1을 발신 트래픽용으로 사용하려면 데이터 트래픽에 대한 기본 경로를 변경하여 P1 인터페이스가 연결된 다음 IP 주소를 지정합니다.

시작하기 전에

- P2를 사용하도록 설정합니다. P1이 아직 사용하도록 설정되지 않은 경우 P1도 사용하도록 설정해야 합니다(네트워크 인터페이스 사용 또는 변경, 2-15페이지 참조).

1단계 CLI에 액세스합니다.

2단계 `advancedproxyconfig` **->** `miscellaneous` 명령을 사용하여 필요한 영역에 액세스합니다.

```
example.com> 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
```

3단계 **[]> miscellaneous**

4단계 다음 질문이 표시될 때까지 각 질문 다음에 **Enter** 를 누릅니다.

```
Do you want proxy to listen on P2?
```

이 질문에 대해 '**y**'를 입력합니다.

5단계 나머지 질문 다음에 **Enter**를 누릅니다.

6단계 변경 사항을 커밋합니다.

관련 주제

- 어플라이언스 연결, 2-3페이지.
- TCP/IP 트래픽 경로 구성, 2-20페이지.

TCP/IP 트래픽 경로 구성

경로는 네트워크 트래픽을 전송하거나 라우팅할 위치를 결정하는 데 사용됩니다. 웹 보안 어플라이언스에서 다음과 같은 유형의 트래픽을 라우팅합니다.

- **데이터 트래픽.** 웹 프록시가 웹을 탐색하는 최종 사용자로부터 처리하는 트래픽입니다.
- **관리 트래픽.** 웹 인터페이스를 통해 어플라이언스를 관리하여 생성된 트래픽과 어플라이언스에서 AsyncOS 업그레이드, 구성 요소 업데이트, DNS, 인증 등과 같은 관리 서비스용으로 생성하는 트래픽입니다.

기본적으로 두 유형의 트래픽은 구성된 모든 네트워크 인터페이스에 대해 정의된 경로를 사용합니다. 그러나 관리 트래픽은 관리 라우팅 테이블을 사용하고 데이터 트래픽은 데이터 라우팅 테이블을 사용하도록 라우팅 분할하기를 선택할 수 있습니다. 다음과 같이 두 가지 유형의 분할된 트래픽으로 나뉩니다.

관리 트래픽	트래픽의 증가
• WebUI • SSH • SNMP • NTLM 인증(도메인 컨트롤러 사용) • 외부 DLP 서버를 사용하는 ICAP 요청 • 시스템 로그 • FTP 푸시 • DNS(구성 가능) • 업데이트/업그레이드/기능 키(구성 가능)	• HTTP • HTTPS • FTP • WCCP 협상 • DNS(구성 가능) • 업데이트/업그레이드/기능 키(구성 가능)

Network(네트워크) > Routes(경로) 페이지의 섹션 수는 분할 라우팅을 사용하도록 설정되었는지 여부에 따라 결정됩니다.

- **관리 및 데이터 트래픽에 대한 별도의 경로 컨피그레이션 섹션**(분할 라우팅이 사용됨). 관리 인터페이스를 관리 트래픽용으로만 사용하는 경우(**Restrict M1 port to appliance management services only(M1 포트를 어플라이언스 관리 서비스로만 제한)**가 사용하도록 설정됨) 이 페이지에는 경로를 입력할 수 있는 2개의 섹션(1개는 관리 트래픽용, 1개는 데이터 트래픽용)이 포함됩니다.
- **모든 트래픽에 대한 하나의 경로 컨피그레이션 섹션**(분할 라우팅이 사용되지 않음). 관리 인터페이스를 관리 및 데이터 트래픽 모두에 사용하는 경우(**Restrict M1 port to appliance management services only(M1 포트를 어플라이언스 관리 서비스로만 제한)**가 사용하지 않도록 설정됨) 이 페이지에는 웹 보안 어플라이언스에서 나가는 모든 트래픽(관리 및 데이터 트래픽 모두)에 대한 경로를 입력할 수 있는 하나의 섹션이 포함됩니다.

참고 경로 게이트웨이는 구성된 관리 또는 데이터 인터페이스와 동일한 서브넷에 있어야 합니다. 여러 데이터 포트가 사용하도록 설정된 경우 웹 프록시는 데이터 트래픽용으로 구성된 기본 게이트웨이와 동일한 네트워크에 있는 데이터 인터페이스에 트랜잭션을 전송합니다.

관련 주제

- 관리 및 데이터 트래픽에 대한 분할 라우팅을 사용하도록 설정하려면 네트워크 인터페이스 사용 또는 변경, 2-15페이지를 참조하십시오.

기본 경로 수정

1단계 **Network(네트워크) > Routes(경로)**를 선택합니다.

2단계 필요에 따라 관리 또는 데이터 테이블(또는 분할 라우팅이 사용하도록 설정되지 않은 경우 결합된 관리/데이터 테이블)에서 **Default Route(기본 경로)**를 클릭합니다.

3단계 Gateway(게이트웨이) 열에서 편집할 네트워크 인터페이스에 연결된 네트워크의 다음 홉에 컴퓨터 시스템의 IP 주소를 입력합니다.

4단계 변경 사항을 제출 및 커밋합니다.

경로 추가

1단계 **Network(네트워크) > Routes(경로)**를 선택합니다.

2단계 경로를 생성할 인터페이스에 해당하는 **Add Route(경로 추가)** 버튼을 클릭합니다.

3단계 이름, 대상 네트워크 및 게이트웨이를 입력합니다.

4단계 변경 사항을 제출 및 커밋합니다.

라우팅 테이블 저장 및 로드

1단계 **Network(네트워크) > Routes(경로)**를 선택합니다.

경로 테이블을 저장하려면 **Save Route Table(경로 테이블 저장)**을 클릭하고 파일을 저장할 위치를 지정합니다.

저장된 경로 테이블을 로드하려면 **Load Route Table(경로 테이블 로드)**을 클릭한 후 파일을 탐색하여 열고 변경 사항을 제출 및 커밋합니다.

참고 대상 주소가 물리적 네트워크 인터페이스 중 하나와 동일한 서브넷에 있는 경우 AsyncOS는 동일한 서브넷을 사용하는 네트워크 인터페이스를 통해 데이터를 전송합니다. 라우팅 테이블을 참고하지 않습니다.

경로 삭제

1단계 **Network(네트워크) > Routes(경로)**를 선택합니다.

2단계 Delete(삭제) 열에서 해당 경로에 대한 확인란을 선택합니다.

3단계 **Delete(삭제)**를 클릭하고 확인합니다**.**

4단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 네트워크 인터페이스 사용 또는 변경, 2-15페이지.

투명 리디렉션 구성

투명 리디렉션 디바이스 지정

시작하기 전에

- 어플라이언스를 레이어-4 스위치 또는 WCCP v2 라우터에 연결합니다.

1단계 **Network(네트워크) > Transparent Redirection(투명 리디렉션)**을 선택합니다.

2단계 **Edit Device(디바이스 편집)**를 클릭합니다.

3단계 Type(유형) 드롭다운 목록에서 트래픽을 어플라이언스에 투명하게 리디렉션하는 디바이스의 유형을 선택합니다.

4단계 변경 사항을 제출 및 커밋합니다.

5단계 WCCP v2 디바이스의 경우 다음 추가 단계를 완료합니다.

a. 디바이스 설명서를 사용하여 WCCP 디바이스를 구성합니다.

b. WCCP 서비스를 추가합니다.

c. 어플라이언스에서 IP 스푸핑이 사용하도록 설정된 경우 두 번째 WCCP 서비스를 생성합니다.

관련 주제

- 어플라이언스 연결, 2-3페이지.
- WCCP 서비스 구성, 2-22페이지.

WCCP 서비스 구성

WCCP 서비스는 WCCP v2 라우터에 서비스 그룹을 정의하는 어플라이언스 컨피그레이션입니다. 여기에는 사용된 서비스 ID 및 포트와 같은 정보가 포함됩니다. 서비스 그룹을 사용하면 웹 프록시가 WCCP 라우터와의 연결을 설정하고 라우터에서 리디렉션된 트래픽을 처리할 수 있습니다.

WCCP 서비스 추가 및 편집

시작하기 전에

- WCCP v2 라우터를 사용하도록 어플라이언스를 구성합니다(투명 리디렉션 디바이스 지정, 2-22페이지 참조).

1단계 **Network(네트워크) > Transparent Redirection(투명 리디렉션)**을 선택합니다.

2단계 **Add Service(서비스 추가)**를 클릭하거나 WCCP 서비스를 편집하려면 Service Profile Name(서비스 프로필 이름) 열에서 WCCP 서비스의 이름을 클릭합니다.

3단계 설명된 대로 WCCP 옵션을 구성합니다.

WCCP 서비스 옵션	설명
서비스 프로파일 이름	WCCP 서비스의 이름입니다. **참고** 이 옵션을 비워 두고 표준 서비스(아래 참조)를 선택하면 'web_cache'라는 이름이 자동으로 여기에 할당됩니다.
서비스	라우터의 서비스 그룹 유형입니다. 다음 중에서 선택합니다. **표준 서비스.** 이 서비스 유형에는 고정된 ID 0, 고정된 리디렉션 방법(*대상 포트를 통해*) 및 고정된 대상 포트 80이 할당됩니다. 하나의 표준 서비스만 생성할 수 있습니다. 표준 서비스가 어플라이언스에 이미 존재하는 경우 이 옵션이 흐리게 표시됩니다. **동적 서비스.** 이 서비스 유형을 사용하여 맞춤형 ID, 포트 번호, 리디렉션 및 로드 밸런싱 옵션을 정의할 수 있습니다. WCCP 라우터에 서비스를 생성할 때 동적 서비스에 대해 입력한 것과 동일한 매개변수를 입력합니다. 동적 서비스를 생성하는 경우 다음 정보를 입력합니다. • **서비스 ID.** Dynamic Service ID(동적 서비스 ID) 필드에 0에서 255 사이의 숫자를 입력합니다. • **포트 번호.** Port Numbers(포트 번호) 필드에 트래픽이 리디렉션될 최대 8개의 포트 번호를 입력합니다. • **리디렉션 기반.** 소스 또는 목적지 포트를 기반으로 트래픽을 리디렉션하도록 선택합니다. 기본값은 목적지 포트입니다. **참고** 투명 리디렉션과 IP 스푸핑을 사용하여 네이티브 FTP를 구성하려면 소스 포트(반환 경로)에 따라 리디렉션하도록 선택하고 소스 포트를 13007로 설정합니다. • **로드 밸런싱 기반.** 네트워크가 여러 Web Security Appliance를 사용하는 경우 어플라이언스 간에 패킷을 분산하는 방법을 선택할 수 있습니다. 서버 또는 클라이언트 주소를 기반으로 패킷을 분산할 수 있습니다. 클라이언트 주소를 선택하면 클라이언트에서 오는 패킷이 항상 동일한 어플라이언스로 분산됩니다. 기본값은 서버 주소입니다.
라우터 IP 주소	하나 이상의 WCCP 지원 라우터에 대한 IPv4 또는 IPv6 주소입니다. 각 라우터의 고유한 IP를 사용합니다. 멀티캐스트 주소를 입력할 수 없습니다. 서비스 그룹 내에서 IPv4 및 IPv6 주소를 혼합할 수 없습니다.
라우터 보안	이 서비스 그룹에 대한 암호가 필요한지 여부를 지정합니다. 사용하도록 설정된 경우 서비스 그룹을 사용하는 모든 어플라이언스 및 WCCP 라우터에서 동일한 암호를 사용해야 합니다.

WCCP 서비스 옵션	설명
고급	**로드 밸런싱 방법.** 이 옵션은 라우터가 여러 웹 보안 어플라이언스 사이에서 패킷의 로드 밸런싱을 수행하는 방법을 결정합니다. 다음 중에서 선택합니다. • **마스크만 허용.** WCCP 라우터가 라우터의 하드웨어를 사용하여 결정합니다. 이 방법을 사용하면 해시 방법에 비해 라우터 성능이 향상될 수 있습니다. 그러나 모든 WCCP 라우터에서 마스크 할당을 지원하지는 않습니다. • **해시만 허용.** 이 방법은 해시 기능에 의존하여 리디렉션 결정을 내립니다. 이 방법은 마스크 방법보다 덜 효율적일 수 있지만 라우터에서 이 옵션만 지원할 수 있습니다. • **해시 또는 마스크 허용**. AsyncOS에서 라우터와 방법을 협상할 수 있도록 허용합니다. 라우터에서 마스크를 지원하는 경우에는 AsyncOS에서 마스킹을 사용하고, 그렇지 않은 경우에는 해싱이 사용됩니다. **마스크 맞춤화.** Allow Mask Only(마스크만 허용)나 Allow Hash or Mask(해시 또는 마스크 허용)를 선택하는 경우 마스크를 맞춤화하거나 비트 수를 지정할 수 있습니다. • **맞춤형 마스크(최대 5비트)**. 마스크를 지정할 수 있습니다. 사용자가 제공하는 마스크와 연결된 비트 수가 웹 인터페이스에 표시됩니다. • **시스템 생성 마스크.** 시스템에서 마스크를 생성하도록 할 수 있습니다. 선택적으로 시스템 생성 마스크의 비트 수(최대 5비트)를 지정할 수 있습니다. **전달 방법.** 리디렉션된 패킷이 라우터에서 웹 프록시로 전송되는 방법입니다. **반환 방법.** 리디렉션된 패킷이 웹 프록시에서 라우터로 전송되는 방법입니다. 전달 및 반환 방법 모두 다음 방법 유형 중 하나를 사용합니다. • **레이어 2(L2)**. 패킷의 목적지 MAC 주소를 대상 웹 프록시의 MAC 주소로 교체하여 레이어 2에서 트래픽을 리디렉션합니다. L2 방법은 하드웨어 레벨에서 작동하며 일반적으로 최적의 성능을 제공합니다. 그러나 일부 WCCP 라우터는 L2 전달을 지원하지 않습니다. 또한 WCCP 라우터는 직접 (물리적으로) 연결된 웹 보안 어플라이언스와의 L2 협상만 허용합니다. • **GRE(Generic Routing Encapsulation)**. 이 방법은 GRE 헤더 및 리디렉션 헤더로 IP 패킷을 캡슐화하여 레이어 3에서 트래픽을 리디렉션합니다. GRE는 소프트웨어 레벨에서 작동하므로 성능에 영향을 줄 수 있습니다. • **L2 또는 GRE**. 이 옵션을 사용하면 라우터에서 지원한다고 표시하는 방법을 어플라이언스에서 사용합니다. 라우터 및 어플라이언스 모두가 L2와 GRE를 지원하는 경우 어플라이언스에서 L2를 사용합니다. 라우터가 어플라이언스에 직접 연결되지 않은 경우 GRE를 선택해야 합니다.

4단계 변경 사항을 제출 및 커밋합니다.

IP 스푸핑을 위한 WCCP 서비스 생성

1단계 웹 프록시에서 IP 스푸핑을 사용하도록 설정한 경우 2개의 WCCP 서비스를 생성합니다. 표준 WCCP 서비스를 생성하거나 목적지 포트를 기반으로 트래픽을 리디렉션하는 동적 WCCP 서비스를 생성합니다.

2단계 소스 포트를 기반으로 트래픽을 리디렉션하는 동적 WCCP 서비스를 생성합니다.

1단계에서 생성된 서비스에 사용되는 것과 동일한 포트 번호, 라우터 IP 주소 및 라우터 보안 설정을 사용합니다.

참고 Cisco에서는 반환 경로에 사용되는 WCCP 서비스에 90에서 97까지의 서비스 ID 번호를 사용하도록 제안합니다(소스 포트를 기반으로).

관련 주제

- 웹 프록시 캐시, 4-5페이지.

VLAN을 사용하여 인터페이스 용량 늘리기

Cisco Web Security Appliance에서 연결할 수 있는 네트워크 수가 포함된 물리적 인터페이스 수를 초과하도록 하나 이상의 VLAN을 구성할 수 있습니다.

VLAN은 "VLAN DDDD" 형식의 동적 "데이터 포트"로 표시됩니다. 여기서 "DDDD"는 ID이고 최대 4자리 정수입니다(예: VLAN 2 또는 VLAN 4094). AsyncOS는 최대 30개의 VLAN을 지원합니다.

VLAN에 두기 위해 물리적 포트에 IP 주소가 구성되어 있을 필요는 없습니다. VLAN을 만든 물리적 포트는 비 VLAN 트래픽을 수신할 IP를 가질 수 있습니다. 따라서 동일한 인터페이스에서 VLAN과 비 VLAN 트래픽이 모두 있을 수 있습니다.

VLAN은 관리 및 P1 데이터 포트에서만 생성할 수 있습니다.

VLAN 구성 및 관리

`etherconfig` 명령을 통해 VLAN을 만들고 수정하고 삭제할 수 있습니다. VLAN이 생성되면 CLI에서 `interfaceconfig` 명령을 통해 구성할 수 있습니다.

예 1: 새 VLAN 생성

이 예에서는 P1 포트에 2개의 VLAN(VLAN 31 및 VLAN 34)을 생성합니다.

1단계 T1 또는 T2 인터페이스에 VLAN을 생성하지 마십시오. CLI에 액세스합니다.

2단계 표시되는 단계에 따릅니다.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan

VLAN interfaces:
```

```
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 34

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2.
[1]> 2

VLAN interfaces:
1. VLAN   34 (P1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 31

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2.
[1]> 2

VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

3단계 변경 사항을 커밋합니다.

예 2: VLAN에 IP 인터페이스 생성

이 예에서는 VLAN 34 이더넷 인터페이스에 새 IP 인터페이스가 생성됩니다.

참고 인터페이스를 변경하면 어플라이언스에 대한 연결이 닫힐 수 있습니다.

1단계 CLI에 액세스합니다.

2단계 표시되는 단계에 따릅니다.

```
example.com> interfaceconfig

Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new

IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10

Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>

Hostname:
[]> v.example.com


Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>

example.com> commit
```

3단계 변경 사항을 커밋합니다.

관련 주제

- 네트워크 인터페이스 사용 또는 변경, 2-15페이지.
- TCP/IP 트래픽 경로 구성, 2-20페이지.

리디렉션 호스트 이름 및 시스템 호스트 이름

시스템 설정 마법사를 실행한 후 시스템 호스트 이름과 리디렉션 호스트 이름은 동일합니다. 그러나 sethostnam 명령을 사용하여 시스템 호스트 이름을 변경해도 리디렉션 호스트 이름은 변경되지 않습니다. 따라서 설정된 값이 서로 다를 수 있습니다.

AsyncOS에서는 최종 사용자 알림 및 승인을 위해 리디렉션 호스트 이름을 사용합니다.

시스템 호스트 이름은 다음 영역에서 어플라이언스를 식별하는 데 사용되는 정규화된 호스트 이름입니다.

- CLI(Command Line Interface)
- 시스템 경고
- 웹 보안 어플라이언스가 Active Directory 도메인에 조인하는 경우 머신 NetBIOS 이름을 형성할 때

시스템 호스트 이름은 인터페이스 호스트 이름과 직접 대응되지 않으며 클라이언트에서 어플라이언스에 연결하는 데 사용되지 않습니다.

리디렉션 호스트 이름 변경

1단계 웹 사용자 인터페이스에서 **Network(네트워크)>Authentication(인증)**으로 이동합니다.

2단계 Edit Global Settings(전역 설정 편집)를 클릭합니다.

3단계 리디렉션 호스트 이름에 새 값을 입력합니다.

시스템 호스트 이름 변경

1단계 CLI에 액세스합니다.

2단계 `sethostname` 명령을 사용하여 웹 보안 어플라이언스의 이름을 변경합니다.

```
example.com> sethostname
example.com> hostname.com
example.com> commit
...
hostname.com>
```

3단계 변경 사항을 커밋합니다.

SMTP 릴레이 호스트 설정 구성

AsyncOS는 알림, 경고 및 Cisco 고객 지원 요청과 같은 시스템 생성 이메일 메시지를 주기적으로 전송합니다. 기본적으로 AsyncOS는 도메인의 MX 레코드에 나열된 정보를 사용하여 이메일을 전송합니다. 그러나 어플라이언스가 MX 레코드에 나열된 메일 서버에 직접 연결할 수 없는 경우에는 어플라이언스에서 하나 이상의 SMTP 릴레이 호스트를 구성해야 합니다.

참고 웹 보안 어플라이언스가 MX 레코드에 나열된 메일 서버 또는 구성된 SMTP 릴레이 호스트와 통신할 수 없는 경우, 이메일 메시지를 전송할 수 없으며 로그 파일에 메시지를 기록합니다.

하나 이상의 SMTP 릴레이 호스트를 구성할 수 있습니다. 여러 SMTP 릴레이 호스트를 구성하는 경우 AsyncOS에서 사용 가능성이 가장 높은 SMPT 릴레이 호스트를 사용합니다. SMTP 릴레이 호스트를 사용할 수 없는 경우 목록에서 해당 릴레이 호스트 아래에 있는 릴레이 호스트를 사용하려고 시도합니다.

SMTP 릴레이 호스트 구성

1단계 **Network(네트워크) > Internal SMTP Relay(내부 SMTP 릴레이)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 내부 SMTP 릴레이 설정을 완료합니다.

속성	설명
릴레이 호스트 이름 또는 IP 주소	SMTP 릴레이에 사용할 호스트 이름 또는 IP 주소입니다.
포트	SMTP 릴레이에 연결하기 위한 포트입니다. 이 속성을 비워 두면 어플라이언스에서 포트 25를 사용합니다.
SMTP에 사용할 라우팅 테이블	SMTP 릴레이에 연결하는 데 사용할 어플라이언스 네트워크 인터페이스(관리 또는 데이터)와 연결된 라우팅 테이블입니다. 릴레이 시스템과 동일한 네트워크에 있는 원하는 인터페이스를 선택합니다.

4단계 (선택 사항) **Add Row(행 추가)**를 클릭하여 SMTP 릴레이 호스트를 더 추가합니다.

5단계 변경 사항을 제출 및 커밋합니다.

DNS 설정

AsyncOS for Web은 인터넷 루트 DNS 서버 또는 사용자의 고유 DNS 서버를 사용할 수 있습니다. 인터넷 루트 서버를 사용할 경우 특정 도메인에 사용할 대체 서버를 지정할 수 있습니다. 대체 DNS 서버는 단일 도메인에 적용되므로, 해당 도메인에 대해 신뢰할 수 있는 서버여야 합니다(확정된 DNS 레코드 제공).

- 분할 DNS, 2-30페이지
- DNS 캐시 지우기, 2-30페이지
- DNS 설정 편집, 2-30페이지

분할 DNS

AsyncOS에서는 내부 서버가 특정 도메인용으로 구성되고 외부 또는 루트 DNS 서버가 다른 도메인용으로 구성된 분할 DNS를 지원합니다. 자체 내부 서버를 사용 중인 경우 예외 도메인 및 관련된 DNS 서버를 지정할 수 있습니다.

DNS 캐시 지우기

시작하기 전에

- 이 명령을 사용하면 캐시가 다시 채워지는 동안 일시적으로 성능이 저하될 수 있습니다.

1단계 **Network(네트워크) > DNS**를 선택합니다.

2단계 **Clear DNS Cache(DNS 캐시 지우기)**를 클릭합니다.

DNS 설정 편집

1단계 **Network(네트워크) > DNS**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 필요에 따라 DNS 설정을 구성합니다.

속성	설명
DNS 서버	**이 DNS 서버 사용.** 어플라이언스에서 호스트 이름을 확인하는 데 사용할 수 있는 로컬 DNS 서버입니다. **인터넷 루트 DNS 서버 사용.** 어플라이언스에서 네트워크에 있는 DNS 서버에 액세스할 수 없는 경우 도메인 이름 서비스 조회를 위해 인터넷 루트 DNS 서버를 사용하도록 선택할 수 있습니다. **참고** 인터넷 루트 DNS 서버는 로컬 호스트 이름을 확인하지 않습니다. 어플라이언스에서 로컬 호스트 이름을 확인해야 하는 경우 로컬 DNS 서버를 사용하거나 CLI(Command Line Interface)를 사용하여 로컬 DNS에 적절한 정적 항목을 추가해야 합니다. **대체 DNS 서버 재지정(선택 사항)**. 특정 도메인에 대한 신뢰할 수 있는 DNS 서버.
DNS 트래픽용 라우팅 테이블	DNS 서비스가 트래픽을 라우팅하는 인터페이스를 지정합니다.
IP 주소 버전 환경 설정	DNS 서버가 IPv4 및 IPv6 주소를 모두 제공하는 경우 AsyncOS에서 이 환경 설정을 사용하여 IP 주소 버전을 선택합니다. **참고** AsyncOS는 투명 FTP 요청에 대한 버전 환경 설정을 준수하지 않습니다.

속성	설명
역 DNS 조회가 시간 초과될 때까지 대기	응답하지 않는 역 DNS 조회가 시간 초과되기 전의 대기 시간(초)입니다.
도메인 검색 목록	DNS 도메인 검색 목록은 요청이 기본 호스트 이름('.' 문자가 없음)에 전송되는 경우에 사용됩니다. 각각의 지정된 도메인을 입력한 순서에 따라 차례로 시도하여 호스트 이름 및 도메인의 DNS 일치 항목을 찾을 수 있는지 확인합니다.

4단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- TCP/IP 트래픽 경로 구성, 2-20페이지
- IP 주소 버전, 2-15페이지

연결, 설치 및 구성 트러블슈팅

- 페일오버 문제, A-5페이지
- 업스트림 프록시가 기본 자격 증명을 수신하지 않음, A-21페이지
- 업스트림 프록시에서 클라이언트 요청 실패, A-21페이지
- 최대 포트 항목 수, A-22페이지

3장 어플라이언스를 Cisco Cloud Web Security 프록시에 연결

- 클라우드 커넥터 모드에서 기능을 구성 및 사용하는 방법, 3-1페이지
- 클라우드 커넥터 모드에서 구축, 3-2페이지
- 클라우드 커넥터 구성, 3-2페이지
- 클라우드에서 디렉토리 그룹을 사용하여 웹 액세스 제어, 3-5페이지
- 클라우드 프록시 서버 우회, 3-5페이지
- 클라우드 커넥터 모드에서 FTP 및 HTTPS 부분 지원, 3-6페이지
- 보안 데이터 유출 방지, 3-6페이지
- 그룹 및 사용자 이름과 IP 주소 보기, 3-6페이지
- 클라우드 커넥터 로그 구독, 3-7페이지
- Cloud Web Security Connector를 사용하는 식별 프로필 및 인증, 3-7페이지

클라우드 커넥터 모드에서 기능을 구성 및 사용하는 방법

따로 언급된 경우를 제외하고 클라우드 커넥터 하위 집합에 포함된 기능의 사용은 표준 모드와 동일합니다. 자세한 내용은 운영 모드 비교, 2-2페이지 섹션을 참조하십시오.

이 장에서는 표준 모드 및 Cloud Web Security Connector 모드에 공통적으로 해당되는 Web Security Appliance의 일부 주요 기능에 대한 정보를 제공하는 곳으로 이동할 수 있도록 문서내 링크를 제공합니다. 클라우드 커넥터 컨피그레이션 설정 및 디렉토리 그룹을 클라우드에 전송하는 방법에 대한 정보를 제외하고, 이 설명서의 여러 다른 곳에서 관련 정보를 찾을 수 있습니다.

이 장에는 표준 모드에서 적용할 수 없는 Cloud Web Security Connector 구성에 대한 정보가 포함되어 있습니다.

이 설명서는 Cisco Cloud Web Security 제품에 대한 정보를 제공하지 않습니다. Cisco Cloud Web Security 설명서는 http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html에서 구할 수 있습니다.

클라우드 커넥터 모드에서 구축

어플라이언스를 처음 설정하는 경우 클라우드 커넥터 모드와 표준 모드 중 어디서 구축할지 선택합니다. 필요한 라이센스가 있는 경우에는 현재 표준 모드로 구축된 어플라이언스에서 시스템 설정 마법사를 실행하여 클라우드 커넥터 모드에서 다시 구축할 수도 있습니다. 시스템 설정 마법사를 실행하면 기존 컨피그레이션을 덮어쓰고 기존 데이터를 모두 삭제합니다.

어플라이언스 구축은 표준 모드와 클라우드 보안 모드에서 동일합니다. 단, 온사이트 웹 프록시 서비스 및 레이어 4 트래픽 모니터 서비스는 Cloud Web Security Connector 모드에서 사용할 수 없습니다.

Cloud Web Security Connector는 명시적 전달 모드 또는 투명 모드 중 하나에서 구축할 수 있습니다.

초기 설정 후 클라우드 커넥터 설정을 수정하려면 **Network(네트워크) > Cloud Connector(클라우드 커넥터)**를 선택합니다.

관련 주제

- 2장, "연결, 설치 및 구성"

클라우드 커넥터 구성

시작하기 전에

가상 어플라이언스에서 웹 인터페이스에 대한 액세스 사용, 1-4페이지를 참조하십시오.

1단계 Web Security Appliance용 웹 인터페이스에 액세스합니다.

인터넷 브라우저에서 웹 보안 어플라이언스의 IPv4 주소를 입력합니다.

시스템 설치 마법사를 처음 실행하는 경우 기본 IPv4 주소를 사용합니다.

`https://192.168.42.42:8443`

-또는-

`http://192.168.42.42:8080`

여기서 `192.168.42.42`는 기본 IPv4 주소이고, `8080`은 HTTP의 기본 관리 포트 설정이며, `8443`은 HTTPS의 기본 관리 포트입니다.

2단계 **System Administration(시스템 관리) > System Setup Wizard(시스템 설정 마법사)**를 선택합니다.

3단계 라이센스 계약서의 약관에 동의합니다.

4단계 **Begin Setup(설정 시작)**을 클릭합니다.

5단계 시스템 설정 구성:

설정	설명
기본 시스템 호스트 이름	Web Security Appliance의 정규화된 호스트 이름입니다.
DNS 서버	도메인 이름 서비스 조회를 위한 인터넷 루트 DNS 서버입니다. DNS 설정, 2-29페이지도 참조하십시오.

설정	설명
NTP 서버	시스템 시간을 동기화할 서버입니다. 기본값은 time.ironport.com 입니다.
표준 시간대	메시지 헤더와 로그 파일의 타임스탬프가 정확하도록 어플라이언스에서 표준 시간대를 설정합니다.

6단계 어플라이언스 모드에 대한 **Cloud Web Security Connector**를 선택합니다.

7단계 클라우드 커넥터 설정 구성:

설정	설명
클라우드 웹 보안 프록시 서버	CPS(Cloud Proxy Server)의 주소. 예: proxy1743.scansafe.net
장애 처리	AsyncOS에서 클라우드 웹 보안 프록시에 연결하지 못할 경우 인터넷에 **직접 연결**하거나 **요청을 삭제**합니다.
클라우드 웹 보안 권한 부여 체계	트랜잭션 권한 부여 방법: • Web Security Appliance 공개 IPv4 주소 • 각 트랜잭션에 포함되는 권한 부여 키. Cisco Cloud Web Security 포털에서 권한 부여 키를 생성할 수 있습니다.

8단계 네트워크 인터페이스 및 와이어링 구성:

설정	설명
이더넷 포트	M1 인터페이스를 관리 트래픽용으로만 구성하는 경우 데이터 트래픽을 위한 P1 인터페이스를 구성해야 합니다. 그러나 M1 인터페이스가 관리 및 데이터 트래픽 모두에 사용되는 경우에도 P1 인터페이스를 구성할 수 있습니다.
IP 주소	Web Security Appliance 관리에 사용할 IPv4 주소입니다.
네트워크 마스크	이 네트워크 인터페이스에서 Web Security Appliance를 관리할 때 사용할 네트워크 마스크입니다.
호스트 이름	이 네트워크 인터페이스에서 Web Security Appliance를 관리할 때 사용할 호스트 이름입니다.

9단계 관리 및 데이터 트래픽을 위한 경로 구성:

설정	설명
기본 게이트웨이	관리 및/또는 데이터 인터페이스를 지나는 트래픽에 사용할 기본 게이트웨이 IPv4 주소입니다.
이름	정적 경로를 식별하는 데 사용되는 이름입니다.
내부 네트워크	네트워크에서 이 경로의 대상에 대한 IPv4 주소입니다.
내부 게이트웨이	이 경로에 대한 게이트웨이 IPv4 주소입니다. 경로 게이트웨이는 구성된 관리 또는 데이터 인터페이스와 동일한 서브넷에 있어야 합니다.

10단계 투명 연결 설정 구성:

참고 기본적으로 클라우드 커넥터는 투명 모드에서 구축됩니다. 그러면, 레이어 4 스위치 또는 버전 2 WCCP 라우터와의 연결이 필요합니다.

설정	설명
레이어 4 스위치 또는 디바이스 없음	• Web Security Appliance가 레이어 4 스위치에 연결됩니다. 또는 • 명시적 전달 모드에서 클라우드 커넥터를 구축합니다.
WCCP v2 라우터	Web Security Appliance가 버전 2 WCCP 지원 라우터에 연결되어 있습니다. 참고: 암호는 최대 7자를 포함할 수 있으며 선택 사항입니다.

11단계 관리 설정 구성:

설정	설명
관리자 암호	Web Security Appliance에 액세스하기 위한 암호입니다. 암호는 6자 이상이어야 합니다.
이메일로 시스템 경고를 받을 대상	어플라이언스에서 경고를 전송할 이메일 주소입니다.
SMTP 릴레이 호스트로 이메일 전송	(선택 사항) AsyncOS가 시스템에서 생성된 이메일 메시지를 전송하는 데 사용하는 SMTP 릴레이 호스트의 호스트 이름 또는 주소입니다. 기본 SMTP 릴레이 호스트는 MX 레코드에 나열된 메일 서버입니다. 기본 포트 번호는 25입니다.
자동지원	어플라이언스가 Cisco 고객 지원에 시스템 경고와 주별 상태 보고서를 전송할 수 있습니다.

12단계 검토 및 설치:

a. 설치를 검토합니다.

b. 뒤로 이동하여 변경 사항을 작성하려면 **Previous(이전)**를 클릭합니다.

c. 제공한 정보로 계속 진행하려면 **Install This Configuration(이 컨피그레이션 설치)**을 클릭합니다.

관련 주제

- 보안 데이터 유출 방지, 3-6페이지
- 네트워크 인터페이스, 2-14페이지
- TCP/IP 트래픽 경로 구성, 2-20페이지
- 투명 리디렉션 구성, 2-22페이지
- 경고 관리, 22-14페이지
- SMTP 릴레이 호스트 설정 구성, 2-29페이지

클라우드에서 디렉토리 그룹을 사용하여 웹 액세스 제어

Cisco Cloud Web Security를 사용하여 디렉토리 그룹을 기반으로 웹 액세스를 제어할 수 있습니다. Cisco Cloud Web Security에 대한 트래픽이 클라우드 커넥터 모드의 Web Security Appliance을 통해 라우팅되는 경우 Cisco Cloud Web Security는 클라우드 커넥터로부터 디렉토리 그룹 정보를 트랜잭션과 함께 받아야 그룹 기반의 클라우드 정책을 적용할 수 있습니다.

시작하기 전에

- Web Security Appliance 컨피그레이션에 인증 영역을 추가합니다.

1단계 **Network(네트워크)** > **Cloud Connector(클라우드 커넥터)**로 이동합니다.

2단계 **Cloud Policy Directory Groups(클라우드 정책 디렉토리 그룹)** 영역에서 **Edit Groups(그룹 수정)**를 클릭합니다.

3단계 Cisco Cloud Web Security 내에서 클라우드 정책을 생성한 **User Groups(사용자 그룹)** 및 **Machine Groups(머신 그룹)**를 선택합니다.

4단계 **Add(추가)**를 클릭합니다.

5단계 **Done(완료)**을 클릭하고 변경 사항을 커밋합니다.

관련 정보

- 인증 영역, 5-10페이지

클라우드 프록시 서버 우회

클라우드 라우팅 정책을 사용하면 다음 특성을 기반으로 웹 트래픽을 Cisco Cloud Web Security 프록시에 라우팅하거나 직접 인터넷으로 라우팅할 수 있습니다.

- **ID 프로필**
- 프록시 포트
- 서브넷
- URL 카테고리
- 사용자 에이전트

클라우드 커넥터 모드에서 클라우드 라우팅 정책을 생성하는 프로세스는 표준 모드를 사용하여 라우팅 정책을 생성하는 프로세스와 동일합니다.

관련 주제

- 정책 생성, 10-5페이지

클라우드 커넥터 모드에서 FTP 및 HTTPS 부분 지원

클라우드 커넥터 모드의 웹 보안 어플라이언스는 FTP 또는 HTTPS를 완전히 지원하지 않습니다.

FTP

FTP는 클라우드 커넥터에서 지원되지 않습니다. 어플라이언스가 클라우드 커넥터용으로 구성된 경우 AsyncOS는 네이티브 FTP 트래픽을 삭제합니다.

FTP over HTTP는 클라우드 커넥터 모드에서 지원됩니다.

HTTPS

클라우드 커넥터는 암호 해독을 지원하지 않습니다. 암호 해독 없이 HTTPS 트래픽을 통과시킵니다.

클라우드 커넥터가 암호 해독을 지원하지 않으므로 일반적으로 AsyncOS는 HTTPS 트래픽의 클라이언트 헤더에 있는 정보에 액세스할 수 없습니다. 따라서, 대개의 경우 AsyncOS는 암호화된 헤더의 정보에 의존하는 라우팅 정책을 적용할 수 없습니다. 투명 HTTPS 트랜잭션의 경우 항상 이에 해당합니다. 예를 들어, 투명 HTTPS 트랜잭션의 경우 AsyncOS는 HTTPS 클라이언트 헤더에 있는 포트 번호에 액세스할 수 없으므로 포트 번호를 기반으로 라우팅 정책을 매칭할 수 없습니다. 그러한 경우 AsyncOS에서 기본 라우팅 정책을 사용합니다.

명시적 HTTPS 트랜잭션에는 두 가지 예외가 있습니다. AsyncOS는 명시적 HTTPS 트랜잭션에 대한 다음 정보에 액세스할 수 있습니다.

- URL
- 대상 포트 번호

명시적 HTTPS 트랜잭션의 경우 URL 또는 포트 번호에 따라 라우팅 정책을 매칭할 수 있습니다.

보안 데이터 유출 방지

Network(네트워크) > **External DLP Servers(외부 DLP 서버)**를 통해 클라우드 커넥터를 외부 DLP(Data Loss Prevention) 서버와 통합할 수 있습니다.

관련 주제

- 16장, "민감한 데이터의 유출 방지"

그룹 및 사용자 이름과 IP 주소 보기

구성된 그룹 이름, 사용자 이름 및 IP 주소를 보려면 whoami.scansafe.net으로 이동합니다.

클라우드 커넥터 로그 구독

클라우드 커넥터 로그는 클라우드 커넥터에 대한 문제를 트러블슈팅하는 데 유용한 정보(예: 인증된 사용자 및 그룹, 클라우드 헤더 및 인증 키)를 제공합니다.

1단계 **System Administration(시스템 관리)** > **Log Subscriptions(로그 서브스크립션)**로 이동합니다.

2단계 **Log Type(로그 유형)** 메뉴에서 **Cloud Connector Logs(클라우드 커넥터 로그)**를 선택합니다.

3단계 **Log Name(로그 이름)** 필드에 이름을 입력합니다.

4단계 로그 레벨을 설정합니다.

5단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 21장, "로그를 통해 시스템 활동 모니터링"

Cloud Web Security Connector를 사용하는 식별 프로필 및 인증

Cloud Web Security Connector는 기본 인증과 NTLM을 지원합니다. 특정 대상에 대한 인증을 우회할 수도 있습니다.

클라우드 커넥터 모드에서 Active Directory 영역을 사용하여 특정 머신에서 생성되는 트랜잭션 요청을 식별할 수 있습니다. 표준 모드에서는 머신 ID 서비스를 사용할 수 없습니다.

두 가지를 제외하고 표준 컨피그레이션 또는 클라우드 커넥터 컨피그레이션에 관계없이 인증이 Web Security Appliance 전체에서 동일하게 작동합니다. 예외

- 표준 모드에서는 머신 ID 서비스를 사용할 수 없습니다.
- 어플라이언스가 클라우드 커넥터 모드에서 구성되는 경우 AsyncOS가 Kerberos를 지원하지 않습니다.

참고 HTTPS 트래픽에 대한 사용자 에이전트 또는 대상 URL 기반의 식별 프로필은 지원되지 않습니다.

관련 주제

- 정책 적용을 위한 머신 식별, 3-8페이지
- 인증되지 않은 사용자에 대한 게스트 액세스, 3-8페이지
- 6장, "최종 사용자 및 클라이언트 소프트웨어 분류"
- 5장, "최종 사용자 자격 증명 확보"

정책 적용을 위한 머신 식별

머신 ID 서비스를 사용하도록 설정하면 AsyncOS가 인증된 사용자 또는 IP 주소나 일부 다른 식별자 대신에 트랜잭션 요청을 작성한 머신을 기반으로 정책을 적용할 수 있습니다. AsyncOS는 NetBIOS를 사용하여 머신 ID를 확보합니다.

시작하기 전에

- 머신 ID 서비스는 Active Directory 영역을 통해서만 사용할 수 있습니다. Active Directory 영역이 구성되지 않은 경우에는 이 서비스가 사용하지 않도록 설정됩니다.

1단계 **Network(네트워크) > Machine ID Service(머신 ID 서비스)**를 선택합니다.

2단계 **Enable and Edit Settings(설정 사용 및 편집)**를 클릭합니다.

3단계 머신 식별 설정을 구성합니다.

설정	설명
머신 식별을 위해 NetBIOS 사용	머신 식별 서비스를 사용하도록 선택합니다.
영역	트랜잭션 요청을 시작하는 머신을 식별하는 데 사용할 Active Directory 영역입니다.
오류 처리	AsyncOS에서 머신을 식별할 수 없는 경우 트랜잭션을 삭제해야 하는지 아니면 정책 일치를 계속 진행해야 하는지 결정합니다.

4단계 변경 사항을 제출하고 커밋합니다.

인증되지 않은 사용자에 대한 게스트 액세스

웹 보안 어플라이언스가 클라우드 커넥터 모드에서 인증되지 않은 사용자에 대한 게스트 액세스를 제공하도록 구성된 경우, AsyncOS는 게스트 사용자에게 __GUEST_GROUP__ 그룹을 할당하고 해당 정보를 Cisco Cloud Web Security에 전송합니다. ID를 사용하여 인증되지 않은 사용자에 대한 게스트 액세스를 제공합니다. Cisco Cloud Web Security 정책을 사용하여 이러한 게스트 사용자를 제어합니다.

관련 주제

- 인증 실패 후 게스트 액세스 권한 부여, 5-31페이지

웹 요청 가로채기

- 웹 요청 가로채기 개요, 4-1페이지.
- 웹 요청 가로채기 작업, 4-2페이지.
- 웹 요청 가로채기 모범 사례, 4-2페이지.
- 웹 요청 가로채기를 위한 웹 프록시 옵션, 4-3페이지.
- 웹 요청을 리디렉션하기 위한 클라이언트 옵션, 4-11페이지.
- 클라이언트 애플리케이션에 PAC 파일 사용, 4-12페이지.
- FTP 프록시 서비스, 4-15페이지.
- SOCKS 프록시 서비스, 4-17페이지

웹 요청 가로채기 개요

Web Security Appliance는 네트워크를 통해 클라이언트 또는 다른 디바이스에서 전달된 요청을 가로챕니다.

어플라이언스는 다른 네트워크 디바이스와 함께 작동하여 트래픽을 가로챕니다. 이러한 디바이스에는 스위치, 투명 리디렉션 디바이스, 네트워크 탭 및 기타 프록시 서버 또는 Web Security Appliance가 포함될 수 있습니다.

웹 요청 가로채기 작업

단계	작업	관련 주제 및 절차에 대한 링크
1.	모범 사례를 검토합니다.	• 웹 요청 가로채기 모범 사례, 4-2페이지
2.	(선택 사항) 후속 네트워킹 작업을 수행합니다. • 업스트림 프록시에 연결하여 구성합니다. • 네트워크 인터페이스 포트를 구성합니다. • 투명 리디렉션 디바이스를 구성합니다. • TCP/IP 경로를 구성합니다. • VLAN을 구성합니다.	• 업스트림 프록시, 2-13페이지 • 네트워크 인터페이스, 2-14페이지 • 투명 리디렉션 구성, 2-22페이지 • TCP/IP 트래픽 경로 구성, 2-20페이지 • VLAN을 사용하여 인터페이스 용량 늘리기, 2-25페이지
3.	(선택 사항) 후속 웹 프록시 작업을 수행합니다. • 전달 또는 투명 모드에서 작동하도록 웹 프록시를 구성합니다. • 가로챌 프로토콜 유형에 추가 서비스가 필요한지 여부를 결정합니다. • IP 스푸핑을 구성합니다. • 웹 프록시 캐시를 관리합니다. • 맞춤형 웹 요청 헤더를 사용합니다. • 일부 요청에 대한 프록시를 우회합니다.	• 웹 요청 가로채기를 위한 웹 프록시 옵션, 4-3페이지 • 웹 프록시 설정 구성, 4-3페이지 • 웹 요청 가로채기를 위한 웹 프록시 옵션, 4-3페이지 • 웹 프록시 캐시, 4-5페이지 • 웹 프록시 IP 스푸핑, 4-8페이지 • 웹 프록시 우회, 4-10페이지
4.	클라이언트 작업을 수행합니다. • 클라이언트가 요청을 웹 프록시에 리디렉션해야 하는 방법을 결정합니다. • 클라이언트 및 클라이언트 리소스를 구성합니다.	• 웹 요청을 리디렉션하기 위한 클라이언트 옵션, 4-11페이지 • 클라이언트 애플리케이션에 PAC 파일 사용, 4-12페이지
5.	(선택 사항) FTP 프록시를 사용하도록 설정하고 구성합니다.	• FTP 프록시 서비스, 4-15페이지

웹 요청 가로채기 모범 사례

- 필요한 프록시 서비스만 사용하도록 설정합니다.
- Web Security Appliance에 정의된 모든 WCCP 서비스에 대해 동일한 전달 및 반환 방법(L2 또는 GRE)을 사용합니다. 이를 통해 프록시 우회 목록이 일관되게 작동합니다.
- 사용자가 회사 네트워크 외부에서 PAC 파일에 액세스할 수 없는지 확인합니다. 이렇게 하면 모바일 근무자가 회사 네트워크에 있는 경우에는 웹 프록시를 사용하고 그렇지 않은 경우에는 웹 서버에 직접 연결할 수 있습니다.
- 웹 프록시가 신뢰할 수 있는 다운스트림 프록시 또는 로드 밸런서의 X-Forwarded-For 헤더만 수락하도록 합니다.
- 처음에 명시적 전달만 사용한 경우에도 웹 프록시를 기본 투명 모드로 유지합니다. 투명 모드도 명시적으로 전달된 요청을 수락합니다.

웹 요청 가로채기를 위한 웹 프록시 옵션

웹 프록시는 자체적으로 HTTP(FTP over HTTP 포함) 및 HTTPS를 사용하는 웹 요청을 가로챌 수 있습니다. 프로토콜 관리를 개선하기 위해 추가 프록시 모듈을 사용할 수 있습니다.

- **FTP 프록시.** FTP 프록시는 HTTP 내에서 인코딩된 FTP 트래픽만이 아니라 네이티브 FTP 트래픽의 가로채기를 허용합니다.
- **HTTPS 프록시.** HTTPS 프록시는 HTTPS 트래픽의 암호 해독을 지원하며 웹 프록시가 암호화되지 않은 HTTPS 요청을 콘텐츠 분석 정책에 전달할 수 있도록 합니다.

참고 투명 모드에서는 HTTPS 프록시가 사용하도록 설정되지 않은 경우 웹 프록시가 투명하게 리디렉션된 모든 HTTPS 요청을 삭제합니다. 삭제된 투명하게 리디렉션된 HTTPS 요청에 대한 로그 항목은 생성되지 않습니다.

- **SOCKS 프록시.** SOCKS 프록시는 SOCKS 트래픽의 가로채기를 허용합니다.

이러한 각 추가 프록시가 작동하려면 웹 프록시가 필요합니다. 웹 프록시를 사용하지 않도록 설정하는 경우에는 추가 프록시를 사용하도록 설정할 수 없습니다.

참고 웹 프록시는 기본적으로 사용하도록 설정되어 있습니다. 기타 모든 프록시는 기본적으로 사용하지 않도록 설정되어 있습니다.

관련 주제

- FTP 프록시 서비스, 4-15페이지.
- SOCKS 프록시 서비스, 4-17페이지

웹 프록시 설정 구성

시작하기 전에

- 웹 프록시를 사용하도록 설정합니다.

1단계 **Security Services(보안 서비스)** > **Web Proxy(웹 프록시)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 필요에 따라 기본 웹 프록시 설정을 구성합니다.

속성	설명
프록시에 대한 HTTP 포트	웹 프록시가 HTTP 연결을 수신 대기할 포트입니다.
HTTP CONNECT 포트	포트 애플리케이션이 HTTP를 통해 아웃바운드 트래픽을 터널링하는 데 사용될 수 있습니다.
캐싱	웹 프록시 캐싱을 사용하거나 사용하지 않도록 설정할지를 지정합니다. 웹 프록시는 성능 향상을 위해 데이터를 캐시합니다.

속성	설명
프록시 모드	• **전달** - 클라이언트 브라우저에서 인터넷 대상의 이름을 지정할 수 있습니다. 웹 프록시를 사용하려면 각 웹 브라우저의 개별 컨피그레이션이 필요합니다. 이 모드에서는 웹 프록시가 명시적으로 전달된 웹 요청만 가로챌 수 있습니다. • **투명**(권장) - 웹 프록시에서 인터넷 대상의 이름을 지정할 수 있습니다. 이 모드에서는 웹 프록시가 투명 웹 요청 및 명시적으로 전달된 웹 요청 모두를 가로챌 수 있습니다.
IP 스푸핑	• **IP 스푸핑이 사용됨** - 웹 프록시가 보안 향상을 위해 고유한 주소와 일치하도록 요청 소스 IP 주소를 변경합니다. • **IP 스푸핑이 사용되지 않음** - 웹 프록시가 Web Security Appliance 대신 소스 클라이언트에서 생성된 것으로 보이도록 소스 주소를 유지합니다.

4단계 필요한 경우 고급 웹 프록시 설정을 완료합니다.

속성	설명
영구 연결 시간 초과	트랜잭션이 완료되고 추가 활동이 탐지되지 않은 후 웹 프록시가 클라이언트 또는 서버에 대한 연결을 열린 상태로 유지하는 최대 시간(초)입니다. • **클라이언트 측.** 클라이언트에 대한 연결의 시간 초과 값입니다. • **서버 측.** 서버에 대한 연결의 시간 초과 값입니다. 이러한 값을 늘리면 연결이 더 오랫동안 열린 상태를 유지하므로 반복해서 연결을 열고 닫는 데 사용되는 오버헤드를 줄여줍니다. 그러나 최대 동시 영구 연결 수에 도달하면 새 연결을 열 수 있는 웹 프록시의 기능이 저하됩니다. Cisco에서는 기본값을 유지하는 것을 권장합니다.
사용 중 연결 시간 초과	현재 트랜잭션이 아직 완료되지 않은 경우 웹 프록시가 유휴 클라이언트 또는 서버의 추가 데이터를 기다리는 최대 시간(초)입니다. • **클라이언트 측.** 클라이언트에 대한 연결의 시간 초과 값입니다. • **서버 측.** 서버에 대한 연결의 시간 초과 값입니다.
동시 영구 연결 수(서버 최대 수)	웹 프록시가 열린 상태로 유지하는 서버와의 최대 연결(소켓) 수입니다.

헤더 생성	요청에 대한 정보를 인코딩하는 헤더를 생성하여 추가합니다. • **X-Forwarded-For** 헤더는 HTTP 요청이 생성된 클라이언트의 IP 주소를 인코딩합니다. **참고** 헤더 전달을 설정하거나 해제하려면 CLI `advancedproxyconfig` 명령, 기타 옵션, "Do you want to pass HTTP X-Forwarded-For headers?(HTTP X-Forwarded-For 헤더를 전달하시겠습니까?)"를 사용합니다. **참고** 명시적 전달 업스트림 프록시를 사용하여 사용자 인증이나 프록시 인증을 통한 액세스 제어를 관리하려면 이러한 헤더를 전달해야 합니다. • **Request Side VIA** 헤더는 요청이 클라이언트에서 서버로 전달될 때 통과하는 프록시를 인코딩합니다. • **Response Side VIA** 헤더는 요청이 서버에서 클라이언트로 전달될 때 통과하는 프록시를 인코딩합니다.
수신된 헤더 사용	업스트림 프록시로 구축된 웹 프록시가 다운스트림 프록시에서 전송된 X-Forwarded-For 헤더를 사용하여 클라이언트를 식별하도록 합니다. 웹 프록시는 이 목록에 포함되지 않은 소스의 X-Forwarded-For 헤더에 있는 IP 주소를 수락하지 않습니다. 사용하도록 설정된 경우 다운스트림 프록시 또는 로드 밸런서의 IP 주소가 필요합니다(서브넷 또는 호스트 이름을 입력할 수 없음).
범위 요청 전달	범위 요청 전달을 사용하거나 사용하지 않도록 설정하려면 **Enable Range Request Forwarding(범위 요청 전달 사용)** 확인란을 사용합니다. 자세한 내용은 범위 요청 설정, 15-4페이지를 참조하십시오.

단계 5 변경 사항을 제출 및 커밋합니다.

관련 항목

- 웹 프록시 캐시, 4-5페이지.
- 투명 리디렉션 구성, 2-22페이지

웹 프록시 캐시

웹 프록시는 성능 향상을 위해 데이터를 캐시합니다. AsyncOS는 안전 모드에서 적극적 모드까지 정의된 캐싱 모드를 포함하며 맞춤화된 캐싱도 허용합니다. 또한 캐시에서 URL을 제거하거나 URL을 무시하도록 캐시를 구성하여 특정 URL이 캐시되지 않도록 제외할 수 있습니다.

웹 프록시 캐시 지우기

1단계 **Security Services(보안 서비스)** > **Web Proxy(웹 프록시)**를 선택합니다.

2단계 **Clear Cache(캐시 지우기)**를 클릭하고 조치를 확인합니다.

웹 프록시 캐시에서 URL 제거

1단계 CLI에 액세스합니다.

2단계 `webcache` > `evict` 명령을 사용하여 필요한 캐싱 영역에 액세스합니다.

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict

Enter the URL to be removed from the cache.
[]>
```

3단계 Enter the URL to be removed from the cache.

참고 URL에 프로토콜이 포함되지 않은 경우 `http://`가 앞에 추가됩니다(예: `www.cisco.com`은 `http://www.cisco.com`이 됨).

웹 프록시에서 캐시하지 않는 도메인 또는 URL 지정

1단계 CLI에 액세스합니다.

2단계 `webcache` **->** `ignore` 명령을 사용하여 필요한 하위 메뉴에 액세스합니다.

```
example.com> webcache

Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore

Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

3단계 DOMAINS 또는 URLS 중에서 관리할 주소 유형을 입력합니다.

```
[]> urls

Manage url entries:

Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

4단계 새 항목을 추가하려면 **add**를 입력합니다.

```
[]> add

Enter new url values; one on each line; an empty line to finish
[]>
```

5단계 도메인 또는 URL을 행당 하나씩 입력합니다. 예를 들어, 다음과 같습니다.

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com

Enter new url values; one on each line; an empty line to finish
[]>
```

도메인 또는 URL을 지정할 때 특정 정규식(regex) 문자를 포함할 수 있습니다. DOMAINS 옵션에서는 선행 점 문자를 사용하여 전체 도메인과 해당 하위 도메인을 캐싱에서 제외할 수 있습니다. 예를 들어, www.google.com, docs.google.com 등을 제외하려면 google.com이 아니라. google.com을 입력할 수 있습니다.

URLS 옵션에서는 전체 정규식 문자 모음을 사용할 수 있습니다. 정규식 사용에 대한 자세한 내용은 정규식, 9-20페이지를 참조하십시오.

6단계 값을 모두 입력한 후 기본 CLI(Command Line Interface)로 돌아갈 때까지 Enter를 누릅니다.

7단계 변경 사항을 커밋합니다.

웹 프록시 캐시 모드 선택

1단계 CLI에 액세스합니다.

2단계 advancedproxyconfig -> caching 명령을 사용하여 필요한 하위 메뉴에 액세스합니다.

```
example.com> 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
[]> caching
```

```
Enter values for the caching options:

The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

3단계 필요한 웹 프록시 캐시 설정에 해당하는 번호를 입력합니다.

엔트리	모드	설명
1	보안	다른 모드에 비해 가장 적게 캐시하며 RFC #2616을 가장 잘 준수합니다.
2	최적화 됨	중간 정도로 캐시하며 중간 정도로 RFC #2616을 준수합니다. 안전 모드에 비해 최적화 모드에서는 Last-Modified 헤더가 있으며 캐싱 시간이 지정되지 않은 경우에 웹 프록시가 개체를 캐시합니다. 웹 프록시가 부정 응답을 캐시합니다.
3	적극적	가장 많이 캐시하며 RFC #2616을 가장 덜 준수합니다. 최적화 모드에 비해 적극적 모드에서는 인증된 콘텐츠, ETag 불일치 및 Last-Modified 헤더가 없는 콘텐츠를 캐시합니다. 웹 프록시가 no-cache 매개변수를 무시합니다.
4	맞춤화된 모드	각 매개변수를 개별적으로 구성합니다.

4단계 옵션 4(맞춤화 모드)를 선택한 경우 각 맞춤형 설정에 대한 값을 입력합니다(또는 기본값으로 유지).

5단계 기본 명령 인터페이스로 돌아갈 때까지 **Enter**를 누릅니다.

6단계 변경 사항을 커밋합니다.

관련 주제

- 웹 프록시 캐시, 4-5페이지.

웹 프록시 IP 스푸핑

웹 프록시가 요청을 전달할 때 기본적으로 자체 주소와 일치하도록 요청 소스 IP 주소를 변경합니다. 이렇게 하면 보안이 향상되지만, 요청이 해당 소스 주소를 유지하고 Web Security Appliance가 아니라 소스 클라이언트에서 생성된 것으로 보이도록 IP 스푸핑을 구현하여 이 동작을 변경할 수 있습니다.

IP 스푸핑은 투명 트래픽 및 명시적으로 전달된 트래픽에 대해 작동합니다. 웹 프록시가 투명 모드에서 구축된 경우 투명하게 리디렉션된 연결에 대해서만 IP 스푸핑을 사용하도록 설정하거나 모든 연결(투명하게 리디렉션된 연결 및 명시적으로 전달된 연결)에 대해 IP 스푸핑을 사용하도록 설정할 것인지 선택할 수 있습니다. 명시적으로 전달된 연결에서 IP 스푸핑을 사용하는 경우 반환 패킷을 다시 Web Security Appliance로 라우팅하기 위한 적절한 네트워크 디바이스가 있는지 확인해야 합니다.

IP 스푸핑이 사용하도록 설정되고 어플라이언스가 WCCP 라우터에 연결된 경우 2개의 WCCP 서비스(소스 포트 기반 WCCP 서비스 및 목적지 포트 기반 WCCP 서비스)를 구성해야 합니다.

관련 주제

- 웹 프록시 설정 구성, 4-3페이지.
- WCCP 서비스 구성, 2-22페이지.

웹 프록시 맞춤형 헤더

목적지 서버의 특별한 처리를 요청하기 위해 특정 발신 트랜잭션에 맞춤형 헤더를 추가할 수 있습니다. 예를 들어, YouTube for Schools와 관계가 있는 경우 맞춤형 헤더를 사용하여 YouTube.com에 대한 트랜잭션 요청을 사용자 네트워크에서 가져오고 특별한 처리가 필요한 것으로 식별할 수 있습니다.

웹 요청에 맞춤형 헤더 추가

1단계 CLI에 액세스합니다.

2단계 `advancedproxyconfig -> customheaders` 명령을 사용하여 필요한 하위 메뉴에 액세스합니다.

```
example.com> 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
[]> customheaders

Currently defined custom headers:

Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

3단계 다음과 같은 필요한 하위 명령을 입력합니다.

옵션	설명
Delete	사용자가 식별하는 맞춤형 헤더를 삭제합니다. 헤더를 식별하여 명령에서 반환된 목록에 있는 헤더와 연결된 번호를 통해 삭제합니다.
New	사용자가 지정하는 도메인에 사용할 수 있도록 제공하는 헤더를 생성합니다. 헤더 예: X-YouTube-Edu-Filter: ABCD1234567890abcdef (이 경우에는 값이 YouTube에서 제공하는 고유 키입니다.) 도메인 예: youtube.com
Edit	기존 헤더를 사용자가 지정하는 헤더로 대체합니다. 헤더를 식별하여 명령에서 반환된 목록에 있는 헤더와 연결된 번호를 통해 삭제합니다.

4단계 기본 명령 인터페이스로 돌아갈 때까지 **Enter**를 누릅니다.

5단계 변경 사항을 커밋합니다.

웹 프록시 우회

- 웹 요청에 대한 웹 프록시 우회, 4-10페이지
- 웹 요청에 대한 웹 프록시 우회 구성, 4-11페이지
- 애플리케이션에 대한 웹 프록시 우회 구성, 4-11페이지

웹 요청에 대한 웹 프록시 우회

특정 클라이언트로부터 또는 특정 대상으로의 투명 요청이 웹 프록시를 우회하도록 Web Security Appliance를 구성할 수 있습니다.

웹 프록시를 우회하면 다음이 가능합니다.

- HTTP 포트를 사용하지만 프록시 서버에 연결할 때 제대로 작동하지 않는 비HTTP 호환(또는 전용) 프로토콜의 방해를 방지합니다.
- 네트워크 내부에 있는 특정 머신(예: 악성코드 테스트 머신)으로부터의 트래픽이 웹 프록시 및 모든 기본 제공 보안 보호를 우회하는지 확인합니다.

우회는 웹 프록시에 투명하게 리디렉션된 요청에 대해서만 작동합니다. 웹 프록시가 투명 모드이거나 전달 모드인지에 관계없이 웹 프록시는 클라이언트에서 명시적으로 전달하는 모든 요청을 처리합니다.

웹 요청에 대한 웹 프록시 우회 구성

1단계 **Web Security Manager(웹 보안 관리자) > Bypass Settings(우회 설정)**를 선택합니다.

2단계 **Edit Bypass Settings(우회 설정 편집)**를 클릭합니다.

3단계 웹 프록시를 우회할 주소를 입력합니다.

4단계 변경 사항을 제출 및 커밋합니다.

애플리케이션에 대한 웹 프록시 우회 구성

1단계 **Web Security Manager(웹 보안 관리자) > Bypass Settings(우회 설정)**를 선택합니다.

2단계 **Edit Application Bypass Settings(애플리케이션 우회 설정 편집)**를 클릭합니다.

3단계 스캐닝을 우회할 애플리케이션을 선택합니다.

4단계 변경 사항을 제출 및 커밋합니다.

웹 프록시 사용 계약

웹 활동을 필터링 및 모니터링 중임을 사용자에게 알리도록 Web Security Appliance를 구성할 수 있습니다. 특정 기간 이후 사용자가 처음으로 브라우저에 액세스하면 어플라이언스에서 최종 사용자 승인 페이지를 표시하여 이를 수행합니다. 최종 사용자 승인 페이지가 표시되면 사용자가 링크를 클릭하여 요청된 원래 사이트 또는 다른 웹 사이트에 액세스해야 합니다.

관련 주제

- 최종 사용자에게 프록시 조치 알림

웹 요청을 리디렉션하기 위한 클라이언트 옵션

클라이언트가 명시적으로 웹 프록시에 요청을 전달하도록 선택하는 경우 이를 수행하기 위한 클라이언트 구성 방법도 결정해야 합니다. 다음 방법 중에서 선택합니다.

- **명시적 설정을 사용하여 클라이언트 구성.** 웹 프록시 호스트 이름 및 포트 번호를 사용하여 클라이언트를 구성합니다. 이를 수행하는 방법에 대한 자세한 내용은 개별 클라이언트 문서를 참조하십시오.

참고 기본적으로 웹 프록시 포트는 포트 번호 80 및 3128을 사용합니다. 클라이언트는 어느 포트라도 사용할 수 있습니다.

- **PAC(Proxy Auto-Config) 파일을 사용하여 클라이언트 구성.** PAC 파일은 웹 요청을 전달할 위치에 대한 지침을 클라이언트에 제공합니다. 이 옵션을 사용하면 프록시 세부 정보에 대한 후속 변경 사항을 중앙에서 관리할 수 있습니다.

PAC 파일을 사용하도록 선택하는 경우 해당 파일을 저장할 위치와 클라이언트가 해당 파일을 찾는 방법도 선택해야 합니다.

관련 주제

- 클라이언트 애플리케이션에 PAC 파일 사용, 4-12페이지.

클라이언트 애플리케이션에 PAC 파일 사용

PAC(Proxy Auto-Config) 파일을 게시하기 위한 옵션

클라이언트가 액세스할 수 있는 위치에 PAC 파일을 게시해야 합니다. 유효한 위치는 다음과 같습니다.

- **웹 서버.**
- **Web Security Appliance.** 클라이언트에 웹 브라우저로 표시되는 Web Security Appliance에 PAC 파일을 배치할 수 있습니다. 또한 어플라이언스가 여러 호스트 이름, 포트 및 파일 이름을 사용하는 요청을 제공할 수 있는 기능을 포함하여 PAC 파일을 관리하기 위한 추가 옵션을 제공합니다.
- **로컬 머신.** 클라이언트의 하드 디스크에 로컬로 PAC 파일을 배치할 수 있습니다. Cisco에서는 이를 일반 솔루션으로 권장하지 않으며, 이는 자동 PAC 파일 탐지 방법에는 적합하지 않지만 테스트용으로는 유용할 수 있습니다.

관련 주제

- 웹 보안 어플라이언스에서 PAC 파일 호스팅, 4-13페이지.
- 클라이언트 애플리케이션에서 PAC 파일 지정, 4-14페이지.

PAC(Proxy Auto-Config) 파일을 찾기 위한 클라이언트 옵션

클라이언트에 PAC 파일을 사용하도록 선택하는 경우 클라이언트가 PAC 파일을 찾는 방법도 선택해야 합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- **PAC 파일 위치를 사용하여 클라이언트 구성.** 명확하게 PAC 파일을 가리키는 URL을 사용하여 클라이언트를 구성합니다.
- **PAC 파일 위치를 자동으로 탐지하도록 클라이언트 구성.** WPAD 프로토콜을 DHCP 또는 DNS와 함께 사용하여 자동으로 PAC 파일을 찾도록 클라이언트를 구성합니다.

자동 PAC 파일 탐지

WPAD는 브라우저에서 DHCP 및 DNS를 사용하여 PAC 파일의 위치를 확인할 수 있도록 하는 프로토콜입니다.

- **WPAD를 DHCP와 함께 사용하려면** PAC 파일 위치의 URL을 사용하여 DHCP 서버에 옵션 252를 설정해야 합니다. 그러나 모든 브라우저가 DHCP를 지원하지는 않습니다.
- **WPAD를 DNS와 함께 사용하려면** DNS 레코드가 PAC 파일의 호스트 서버를 가리키도록 구성해야 합니다.

둘 중 하나 또는 두 옵션을 모두 구성할 수 있습니다. WPAD는 먼저 DHCP를 사용하여 PAC 파일을 찾으려고 시도합니다. 찾지 못한 경우 DNS를 시도합니다.

관련 주제

- 클라이언트에서 자동으로 PAC 파일 탐지, 4-14페이지

웹 보안 어플라이언스에서 PAC 파일 호스팅

1단계 **Security Services(보안 서비스) > PAC File Hosting(PAC 파일 호스팅)**을 선택합니다.

2단계 **Enable and Edit Settings(설정 사용 및 편집)**를 클릭합니다.

3단계 (선택 사항) 다음 기본 설정을 완료합니다.

옵션	설명
PAC 서버 포트	Web Security Appliance에서 PAC 파일 요청을 수신 대기하는 데 사용할 포트입니다.
PAC 파일 만료	PAC 파일이 지정된 시간(분) 이후 브라우저의 캐시에서 만료되도록 합니다.

4단계 PAC Files(PAC 파일) 섹션에서 **Browse(찾아보기)**를 클릭하고 로컬 머신에서 Web Security Appliance에 업로드할 PAC 파일을 선택합니다.

참고 선택한 파일이 `default.pac`이면 브라우저에서 해당 위치를 구성할 때 파일 이름을 지정할 필요가 없습니다. 이름이 지정되지 않으면 Web Security Appliance에서 `default.pac`라는 파일을 찾습니다.

5단계 **Upload(업로드)**를 클릭하여 4단계에서 선택한 PAC 파일을 Web Security Appliance에 업로드합니다.

6단계 (선택 사항) Hostnames for Serving PAC Files Directly(직접 PAC 파일을 제공하기 위한 호스트 이름) 섹션에서 포트 번호가 포함되지 않은 PAC 파일 요청의 호스트 이름 및 연결된 파일 이름을 구성합니다(BS: 예를 들어, DNS WPAD 요청?).

옵션	설명
호스트 이름	Web Security Appliance가 요청을 제공할 경우 PAC 파일 요청에 포함되어야 하는 호스트 이름입니다. 요청에 포트 번호가 포함되지 않으므로 웹 프록시 HTTP 포트(예: 포트 80)를 통해 처리되며 이 호스트 이름 값을 통해 PAC 파일 요청으로 구별할 수 있어야 합니다.
프록시 포트를 통한 "Get/" 요청의 기본 PAC 파일	동일한 행의 호스트 이름과 연결될 PAC 파일 이름입니다. 호스트 이름에 대한 요청이 여기에 지정된 PAC 파일을 반환합니다. 업로드된 PAC 파일만 선택할 수 있습니다.
행 추가	추가 호스트 이름 및 PAC 파일 이름을 지정하려면 다른 행을 추가합니다.

7단계 변경 사항을 제출 및 커밋합니다.

클라이언트 애플리케이션에서 PAC 파일 지정

- 클라이언트에서 수동으로 PAC 파일 위치 구성, 4-14페이지
- 클라이언트에서 자동으로 PAC 파일 탐지, 4-14페이지

클라이언트에서 수동으로 PAC 파일 위치 구성

1단계 PAC 파일을 생성하여 게시합니다.

2단계 브라우저의 PAC 파일 컨피그레이션 영역에 PAC 파일 위치를 가리키는 URL을 입력합니다.

Web Security Appliance에서 PAC 파일을 호스팅하는 경우 유효한 URL 형식은 다음과 같습니다.

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

여기서 *WSAHostname*은 Web Security Appliance에서 PAC 파일을 호스팅하는 경우 구성된 **hostname(호스트 이름)** 값입니다. 그렇지 않으면 URL 형식이 스토리지 위치 및 클라이언트(일부 경우)에 따라 달라집니다.

관련 주제

- 웹 보안 어플라이언스에서 PAC 파일 호스팅, 4-13페이지.

클라이언트에서 자동으로 PAC 파일 탐지

1단계 `wpad.dat`라는 PAC 파일을 생성하여 웹 서버 또는 Web Security Appliance에 게시합니다(WPAD를 DNS와 함께 사용하려는 경우 파일이 웹 서버의 루트 폴더에 있어야 함).

2단계 다음 MIME 유형을 사용하여 `.dat` 파일을 설정하도록 웹 서버를 구성합니다.

```
application/x-ns-proxy-autoconfig
```

참고 Web Security Appliance에서 자동으로 이를 수행합니다.

3단계 DNS 조회를 지원하려면 '`wpad`'로 시작하는 내부적으로 해석 가능한 DNS 이름(예: `wpad.example.com`)을 생성하여 `wpad.dat` 파일을 호스팅하는 서버의 IP 주소와 연결합니다.

4단계 DHCP 조회를 지원하려면 wpad.dat 파일 위치의 URL(예: "`http://wpad.example.com/wpad.dat`")을 사용하여 DHCP 서버의 옵션 252를 구성합니다. URL은 IP 주소를 포함하여 유효한 호스트 주소를 사용할 수 있으며 특정 DNS 항목이 필요하지 않습니다.

관련 주제

- 클라이언트 애플리케이션에 PAC 파일 사용, 4-12페이지.
- 웹 보안 어플라이언스에서 PAC 파일 호스팅, 4-13페이지.
- WPAD가 Firefox에서 작동하지 않음, A-4페이지

FTP 프록시 서비스

- FTP 프록시 서비스 개요, 4-15페이지
- FTP 프록시 사용 및 구성, 4-15페이지

FTP 프록시 서비스 개요

웹 프록시는 두 가지 유형의 FTP 요청을 가로챌 수 있습니다.

- **네이티브 FTP.** 네이티브 FTP 요청은 전용 FTP 클라이언트 또는 내장 FTP 클라이언트를 사용하는 브라우저에서 생성됩니다. FTP 프록시가 필요합니다.
- **FTP over HTTP.** 경우에 따라 브라우저에서 네이티브 FTP를 사용하는 대신 HTTP 요청 내부의 FTP 요청을 인코딩합니다. FTP 프록시가 필요하지 않습니다.

관련 주제

- FTP 프록시 사용 및 구성, 4-15페이지.
- FTP 알림 메시지 구성, 17-9페이지.

FTP 프록시 사용 및 구성

참고 FTP over HTTP 연결에 적용되는 프록시 설정을 구성하려면 웹 프록시 설정 구성, 4-3페이지를 참조하십시오.

1단계 **Security Services(보안 서비스) > FTP Proxy(FTP 프록시)**를 선택합니다.

2단계 **Enable and Edit Settings(설정 사용 및 편집)**를 클릭합니다(**Edit Settings(설정 편집)** 옵션만 사용 가능한 경우 FTP 프록시가 이미 사용하도록 설정됨).

3단계 (선택 사항)기본 FTP 프록시 설정을 구성합니다.

속성	설명
프록시 수신 대기 포트	FTP 프록시가 FTP 제어 연결을 수신 대기할 포트입니다. FTP 프록시를 구성할 때 클라이언트에서 이 포트를 사용해야 합니다(일반적으로 포트 21을 사용하는 FTP 서버에 연결하기 위한 포트가 아님).
캐싱	익명 사용자로부터의 데이터 연결이 캐시되는지 여부입니다. **참고** 익명이 아닌 사용자의 데이터는 캐시되지 않습니다.
서버 측 IP 스푸핑	FTP 프록시가 FTP 서버의 IP 주소를 모방하도록 허용합니다. 이는 제어 및 데이터 연결에 대한 IP 주소가 서로 다른 경우 트랜잭션을 허용하지 않는 FTP 클라이언트를 지원합니다.
인증 형식	FTP 클라이언트와 통신할 때 FTP 프록시에서 사용할 수 있는 인증 형식을 선택할 수 있습니다.
수동 모드 데이터 포트 범위	FTP 클라이언트에서 수동 모드 연결을 위해 FTP 프록시와의 데이터 연결을 설정하는 데 사용해야 하는 TCP 포트의 범위입니다.

속성	설명
활성 모드 데이터 포트 범위	FTP 서버에서 활성 모드 연결을 위해 FTP 프록시와의 데이터 연결을 설정하는 데 사용해야 하는 TCP 포트의 범위입니다. 이 설정은 네이티브 FTP 및 FTP over HTTP 연결 모두에 적용됩니다. 포트 범위를 늘리면 동일한 FTP 서버의 요청이 더 많이 수용됩니다. TCP 세션 TIME-WAIT 지연(일반적으로 몇 분)으로 인해 포트가 사용된 직후 *동일한* FTP 서버에 대해 다시 사용 가능하게 되지 않습니다. 따라서 지정된 FTP 서버가 짧은 기간에 *n*번보다 많이 활성 모드로 FTP 프록시에 연결할 수 없습니다. 여기서 *n*은 이 필드에 지정된 포트의 수입니다.
시작 배너	연결 중에 FTP 클라이언트에 표시되는 시작 배너입니다. 다음 중에서 선택합니다. • **FTP 서버 메시지.** 목적지 FTP 서버에서 메시지를 제공합니다. 이 옵션은 웹 프록시가 투명 모드로 구성된 경우에만 사용할 수 있으며 투명 연결에 대해서만 적용됩니다. • **맞춤형 메시지.** 선택된 경우 모든 네이티브 FTP 연결에 대해 이 맞춤형 메시지가 표시됩니다. 선택되지 않은 경우 여전히 명시적 전달 네이티브 FTP 연결에 사용됩니다.

4단계 (선택 사항) 고급 FTP 프록시 설정을 구성합니다.

속성	설명
제어 연결 시간 초과	현재 트랜잭션이 완료되지 않은 경우 FTP 프록시가 유휴 FTP 클라이언트 또는 FTP 서버로부터 제어 연결의 추가 통신을 기다리는 최대 시간(초)입니다. • **클라이언트 측.** 유휴 FTP 클라이언트에 대한 제어 연결의 시간 초과 값입니다. • **서버 측.** 유휴 FTP 서버에 대한 제어 연결의 시간 초과 값입니다.
데이터 연결 시간 초과	현재 트랜잭션이 아직 완료되지 않은 경우 FTP 프록시가 유휴 FTP 클라이언트 또는 FTP 서버로부터 데이터 연결의 추가 통신을 기다리는 기간입니다. • **클라이언트 측.** 유휴 FTP 클라이언트에 대한 데이터 연결의 시간 초과 값입니다. • **서버 측.** 유휴 FTP 서버에 대한 데이터 연결의 시간 초과 값입니다.

5단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- FTP 프록시 서비스 개요, 4-15페이지.

SOCKS 프록시 서비스

- SOCKS 프록시 서비스 개요, 4-17페이지
- SOCKS 트래픽의 처리 사용, 4-17페이지
- SOCKS 프록시 구성, 4-17페이지
- SOCKS 정책 생성, 4-18페이지

SOCKS 프록시 서비스 개요

Web Security Appliance에는 SOCKS 트래픽을 처리하기 위한 SOCKS 프록시가 포함되어 있습니다. SOCKS 정책은 SOCKS 트래픽을 제어하는 액세스 정책과 동등합니다. 액세스 정책과 유사하게, 식별 프로필을 사용하여 각 SOCKS 정책에서 어떤 트랜잭션을 제어하는지 지정할 수 있습니다. SOCKS 정책이 트랜잭션에 적용되면 라우팅 정책이 트래픽의 라우팅을 제어할 수 있습니다.

SOCKS 프록시에 대해 다음에 유의하십시오.

- SOCKS 프로토콜은 직접 전달 연결만 지원합니다.
- SOCKS 프록시는 업스트림 프록시를 지원하지 않습니다(업스트림 프록시에 전달하지 않음).
- SOCKS 프록시는 AVC(Application Visibility and Control), DLP(Data Loss Prevention) 및 악성코드 탐지에서 사용되는 스캐닝 서비스를 지원하지 않습니다.
- SOCKS 프록시는 정책 추적을 지원하지 않습니다.
- SOCKS 트래픽은 SSL 트래픽의 암호를 해독하지 않습니다. 클라이언트에서 서버로 터널링합니다.

SOCKS 트래픽의 처리 사용

시작하기 전에

- 웹 프록시를 사용하도록 설정합니다.

1단계 **Security Services(보안 서비스)** > **SOCKS Proxy(SOCKS 프록시)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable SOCKS Proxy(SOCKS 프록시 사용)**를 선택합니다.

4단계 **변경 사항**을 **제출** 및 **커밋합니다**.

SOCKS 프록시 구성

1단계 **Security Services(보안 서비스)** > **SOCKS Proxy(SOCKS 프록시)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable SOCKS Proxy(SOCKS 프록시 사용)**를 선택합니다.

4단계 기본 및 고급 SOCKS 프록시 설정을 구성합니다.

속성	설명
SOCKS 프록시	사용하도록 설정됩니다.
SOCKS 제어 포트	SOCKS 요청을 수락하는 포트입니다. 기본값은 1080입니다.
UDP 요청 포트	SOCKS 서버가 수신 대기해야 하는 UDP 포트입니다. 기본값은 16000~16100입니다.
프록시 협상 시간 초과	협상 단계에서 SOCKS 클라이언트로부터 데이터를 전송하거나 수신할 때까지 기다리는 시간(초)입니다. 기본값은 60입니다.
UDP 터널 시간 초과	UDP 터널을 닫기 전에 UDP 클라이언트 또는 서버의 데이터를 기다리는 시간(초)입니다. 기본값은 60입니다.

SOCKS 정책 생성

1단계 **Web Security Manager(웹 보안 관리자)** > **SOCKS Policies(SOCKS 정책)**를 선택합니다.

2단계 **Add Policy(정책 추가)**를 클릭합니다.

3단계 **Policy Name(정책 이름)** 필드에 이름을 지정합니다.

참고 각 정책 그룹 이름은 고유해야 하며 영숫자 또는 공백 문자만 포함해야 합니다.

4단계 (선택 사항) 설명을 추가합니다.

5단계 **Insert Above Policy(정책 위에 삽입)** 필드에서 이 SOCKS 정책을 삽입할 SOCKS 정책 테이블의 위치를 선택합니다.

참고 여러 SOCKS 정책을 구성하는 경우 각 정책의 논리적 순서를 결정합니다. 올바르게 일치될 수 있도록 정책의 순서를 지정합니다.

6단계 **Identities and Users(ID 및 사용자)** 섹션에서 이 정책 그룹에 적용할 하나 이상의 ID를 선택합니다.

7단계 (선택 사항) 추가 구성원 자격 요건을 정의하려면 Advanced(고급) 섹션을 확장합니다.

고급 옵션	설명
프록시 포트	브라우저에 구성된 포트입니다. (선택 사항) 웹 프록시에 액세스하는 데 사용되는 프록시 포트별로 정책 그룹 구성원 자격을 정의합니다. Proxy Ports(프록시 포트) 필드에 하나 이상의 포트 번호를 입력합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오. 하나의 포트에서 명시적으로 요청을 전달하도록 구성된 하나의 클라이언트 집합과 다른 포트에서 명시적으로 요청을 전달하도록 구성된 다른 클라이언트 집합이 있는 경우 프록시 포트에 정책 그룹 구성원 자격을 정의할 수 있습니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정으로 ID 구성원 자격을 정의하는 경우 SOCKS 정책 그룹 레벨에서 설정을 구성할 수 없습니다.
서브넷	(선택 사항) 서브넷 또는 기타 주소로 정책 그룹 구성원 자격을 정의합니다. 연결된 ID로 정의될 수 있는 주소를 사용하도록 선택하거나 여기에 특정 주소를 입력할 수 있습니다. **참고** 이 정책 그룹과 연결된 ID가 주소를 통해 구성원 자격을 정의하는 경우 이 정책 그룹에서 ID 주소의 하위 집합인 주소를 입력해야 합니다. 정책 그룹에 주소를 추가하면 이 정책 그룹과 일치하는 트랜잭션 목록이 더 줄어듭니다.
시간 범위	(선택 사항) 시간 범위로 정책 그룹 구성원 자격을 정의합니다. 1. **Time Range(시간 범위)** 필드에서 시간 범위를 선택합니다. 2. 이 정책 그룹이 선택한 시간 범위 내부 또는 외부의 시간에 적용되어야 하는지를 지정합니다.

8단계 **변경 사항**을 **제출** 및 **커밋합니다**.

다음 작업

- (선택 사항) SOCKS 정책에서 사용할 ID를 추가합니다.
- SOCKS 트래픽을 관리할 하나 이상의 SOCKS 정책을 추가합니다.

요청 가로채기 트러블슈팅

- URL 카테고리가 일부 FTP 사이트를 차단하지 않음, A-6페이지
- 대용량 FTP 전송 연결 끊기, A-6페이지
- 파일 업로드 후 FTP 서버에 0바이트 파일이 표시됨, A-6페이지
- 업스트림 프록시를 통해 FTP 요청을 라우팅할 수 없음, A-21페이지
- HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨, A-15페이지
- 사용자가 HTTPS 및 FTP over HTTP 요청에 대한 전역 정책과 일치함, A-15페이지

5장

최종 사용자 자격 증명 확보

- 최종 사용자 자격 증명 확보 개요, 5-1페이지
- 인증 모범 사례, 5-2페이지
- 인증 영역, 5-10페이지
- 실패한 인증, 5-27페이지
- 자격 증명, 5-34페이지
- 인증 트러블슈팅, 5-36페이지

최종 사용자 자격 증명 확보 개요

서버 유형/영역	인증 체계	지원되는 네트워크 프로토콜	참고
Active Directory	Kerberos NTLMSSP 기본	HTTP, HTTPS 네이티브 FTP, FTP over HTTP SOCKS(기본 인증)	Kerberos는 표준 모드에서만 지원됩니다. 클라우드 커넥터 모드에서는 지원되지 않습니다.
LDAP	기본	HTTP, HTTPS 네이티브 FTP, FTP over HTTP SOCKS	—

인증 작업 개요

단계	작업	관련 주제 및 절차에 대한 링크
1.	인증 영역을 생성합니다.	• Active Directory 인증 영역(NTLMSSP 및 기본)을 생성하는 방법, 5-13페이지 • LDAP 인증 영역 생성, 5-15페이지
2.	전역 인증 설정을 구성합니다.	• 전역 인증 설정 구성, 5-20페이지
3.	외부 인증을 구성합니다. 외부 LDAP 또는 RADIUS 서버를 통해 사용자를 인증할 수 있습니다.	• 외부 인증, 5-10페이지
4.	(선택 사항) 추가 인증 영역을 생성하고 순서를 지정합니다. 사용하려는 각 인증 프로토콜 및 체계 조합에 대한 하나 이상의 인증 영역을 생성합니다.	• 인증 시퀀스 생성, 5-26페이지
5.	(선택 사항) 자격 증명 암호화를 구성합니다.	• 자격 증명 암호화 구성, 5-36페이지
6.	인증 요건에 따라 사용자 및 클라이언트 소프트웨어를 분류하기 위한 ID를 생성합니다.	• 사용자 및 클라이언트 소프트웨어 분류, 6-3페이지
7.	ID를 생성한 사용자 및 사용자 그룹의 웹 요청을 관리하기 위한 정책을 생성합니다.	• 정책을 통한 웹 요청 관리 모범 사례, 10-2페이지

인증 모범 사례

- 가능한 적은 Active Directory 영역을 생성하는 것이 좋습니다. 다중 Active Directory 영역에는 인증을 위해 추가 메모리 사용량이 필요합니다.
- NTLMSSP를 사용하는 경우 웹 보안 어플라이언스 또는 업스트림 프록시 서버 중 하나를 사용하여(둘 다가 아님) 사용자를 인증합니다 (웹 보안 어플라이언스 권장).
- Kerberos를 사용 중인 경우 웹 보안 어플라이언스를 사용하여 인증합니다.
- 최적의 성능을 위해 동일한 서브넷의 클라이언트는 단일 영역을 사용하여 인증합니다.
- 일부 사용자 에이전트는 컴퓨터 자격 증명 문제 또는 인증 실패가 발생하여 정상적인 작업에 부정적인 영향을 미칠 수 있는 것으로 알려져 있습니다. 이러한 사용자 에이전트에 대한 인증을 우회해야 합니다. 문제가 되는 사용자 에이전트에 대한 인증 우회, 5-28페이지를 참조하십시오.

인증 계획

- Active Directory/Kerberos, 5-3페이지
- Active Directory/기본, 5-4페이지
- Active Directory/NTLMSSP, 5-4페이지
- LDAP/기본, 5-5페이지
- 투명하게 사용자 식별, 5-5페이지

Active Directory/Kerberos

명시적 전달	투명, IP 기반 캐싱	투명, 쿠키 기반 캐싱
장점: • NTLM에 비해 더 뛰어난 성능과 상호운용성 • 도메인에 조인한 Windows 및 Windows가 아닌 클라이언트 모두에 대해 작동함 • 모든 브라우저와 대부분의 다른 애플리케이션에서 지원됨 • RFC 기반 • 최소 오버헤드 • HTTPS(CONNECT) 요청에 대해 작동함 • 암호가 인증 서버에 전송되지 않으므로 더 안전함 • 호스트 또는 IP 주소가 아니라 연결이 인증됨 • 클라이언트 애플리케이션이 웹 보안 어플라이언스를 신뢰하도록 구성된 경우 Active Directory 환경에서 실제 단일 로그인 수행	**장점:** • NTLM에 비해 더 뛰어난 성능과 상호운용성 • 도메인에 조인한 Windows 및 Windows가 아닌 클라이언트 모두에 대해 작동함 • 모든 주요 브라우저에서 작동함 • 인증을 지원하지 않는 사용자 에이전트를 사용하는 경우 사용자가 먼저 지원되는 브라우저에서 인증하기만 하면 됨 • 비교적 낮은 오버헤드 • 사용자가 이전에 HTTP 요청으로 인증된 경우 HTTPS 요청에 대해 작동함	**장점**: • NTLM에 비해 더 뛰어난 성능과 상호운용성 • 도메인에 조인한 Windows 및 Windows가 아닌 클라이언트 모두에 대해 작동함 • 모든 주요 브라우저에서 작동함 • 인증이 호스트 또는 IP 주소가 아닌 사용자와 연결됨 **단점**: • 쿠키가 도메인에 특정하기 때문에 각각의 새 웹 도메인에 전체 인증 프로세스가 필요함 • 쿠키를 사용하도록 설정해야 함 • HTTPS 요청에 대해 작동하지 않음

Active Directory/기본

명시적 전달	투명, IP 기반 캐싱	투명, 쿠키 기반 캐싱
장점: • 모든 브라우저와 대부분의 다른 애플리케이션에서 지원됨 • RFC 기반 • 최소 오버헤드 • HTTPS(CONNECT) 요청에 대해 작동함 • 암호가 인증 서버에 전송되지 않으므로 더 안전함 • 호스트 또는 IP 주소가 아니라 연결이 인증됨 • 클라이언트 애플리케이션이 웹 보안 어플라이언스를 신뢰하도록 구성된 경우 Active Directory 환경에서 실제 단일 로그인 수행 **단점**: • 모든 요청에 대해 암호가 일반 텍스트(Base64)로 전송됨 • 단일 로그인 없음 • 중간 오버헤드: 새 연결마다 재인증되어야 함 • 주로 Windows 및 주요 브라우저에서만 지원됨	**장점:** • 모든 주요 브라우저에서 작동함 • 인증을 지원하지 않는 사용자 에이전트를 사용하는 경우 사용자가 먼저 지원되는 브라우저에서 인증하기만 하면 됨 • 비교적 낮은 오버헤드 • 사용자가 이전에 HTTP 요청으로 인증된 경우 HTTPS 요청에 대해 작동함 **단점**: • 인증 자격 증명이 사용자가 아니라 IP 주소와 연결됨(Citrix 및 RDP 환경에서 또는 사용자가 IP 주소를 변경하는 경우 작동하지 않음) • 단일 로그인 없음 • 암호가 일반 텍스트(Base64)로 전송됨	**장점**: • 모든 주요 브라우저에서 작동함 • 인증이 호스트 또는 IP 주소가 아닌 사용자와 연결됨 **단점**: • 쿠키가 도메인에 특정하기 때문에 각각의 새 웹 도메인에 전체 인증 프로세스가 필요함 • 쿠키를 사용하도록 설정해야 함 • HTTPS 요청에 대해 작동하지 않음 • 단일 로그인 없음 • 암호가 일반 텍스트(Base64)로 전송됨

Active Directory/NTLMSSP

명시적 전달	투명
장점: • 암호가 인증 서버에 전송되지 않으므로 더 안전함 • 호스트 또는 IP 주소가 아니라 연결이 인증됨 • 클라이언트 애플리케이션이 웹 보안 어플라이언스를 신뢰하도록 구성된 경우 Active Directory 환경에서 실제 단일 로그인 수행 **단점:** • 중간 오버헤드: 새 연결마다 재인증되어야 함 • 주로 Windows 및 주요 브라우저에서만 지원됨	**장점:** • 더 유연함 투명한 NTLMSSP 인증은 웹 프록시가 기본적인 일반 텍스트 사용자 이름 및 암호 대신에 인증 질문 및 응답을 사용하여 클라이언트와 통신한다는 점을 제외하고 투명한 기본 인증과 유사합니다. 투명한 NTLM 인증 사용의 장점 및 단점은 **투명한 NTLM 인증에는 인증 서버에 암호를 전송하지 않는다는 장점이 추가되었고 클라이언트 애플리케이션이 웹 보안 어플라이언스를 신뢰하도록 구성된 경우 단일 로그인을 수행할 수 있다는 점**을 제외하고 투명한 기본 인증 사용의 장점 및 단점과 동일합니다.

LDAP/기본

명시적 전달	투명
장점: • RFC 기반 • NTLM보다 더 많은 브라우저 지원 • 최소 오버헤드 • HTTPS(CONNECT) 요청에 대해 작동함 **단점:** • 단일 로그인 없음 • 모든 요청에 대해 암호가 일반 텍스트(Base64)로 전송됨 **해결 방법:** • 실패한 인증, 5-27페이지	**장점:** • 명시적 전달보다 더 유연함 • NTLM보다 더 많은 브라우저 지원 • 인증을 지원하지 않는 사용자 에이전트를 사용하는 경우 사용자가 먼저 지원되는 브라우저에서 인증하기만 하면 됨 • 비교적 낮은 오버헤드 • 사용자가 이전에 HTTP 요청으로 인증된 경우 HTTPS 요청에 대해 작동함 **단점:** • 단일 로그인 없음 • 암호가 일반 텍스트(Base64)로 전송됨 • 인증 자격 증명이 사용자가 아니라 IP 주소와 연결됨(Citrix 및 RDP 환경에서 또는 사용자가 IP 주소를 변경하는 경우 작동하지 않음) **해결 방법:** • 실패한 인증, 5-27페이지

투명하게 사용자 식별

일반적으로 사용자에게 사용자 이름 및 암호를 입력하라는 프롬프트를 표시하여 사용자를 식별하고 인증합니다. 이러한 자격 증명이 인증 서버에 대해 검증된 후 웹 프록시가 인증된 사용자 이름에 따라 트랜잭션에 적절한 정책을 적용합니다.

그러나 최종 사용자에게 자격 증명에 대한 프롬프트를 표시하지 않고 사용자를 투명하게 인증하도록 웹 보안 어플라이언스를 구성할 수 있습니다. 투명한 식별은 사용자가 다른 신뢰된 소스에서 이미 인증되었다고 가정하여 해당 신뢰된 소스에서 가져온 자격 증명을 사용하여 사용자를 인증한 후 적절한 정책을 적용합니다.

다음을 수행하기 위해 사용자를 투명하게 식별할 수 있습니다.

- 사용자가 네트워크에 프록시가 존재하는지 인식하지 못하도록 단일 로그인 환경을 생성합니다.
- 최종 사용자에게 인증 프롬프트를 표시할 수 없는 클라이언트 애플리케이션에서 생성된 트랜잭션에 인증 기반 정책을 적용합니다.

투명하게 사용자를 식별하면 웹 프록시가 사용자 이름을 가져오고 식별 프로필을 할당하는 방법에만 영향을 미칩니다. 사용자 이름을 가져오고 식별 프로필을 할당한 후에는 식별 프로필 할당 방법에 관계없이 다른 모든 정책을 정상적으로 적용합니다.

투명 인증에 실패하는 경우 트랜잭션을 처리하는 방법을 구성할 수 있습니다. 즉, 사용자에게 게스트 액세스 권한을 부여하거나 강제로 사용자에게 인증 프롬프트를 표시할 수 있습니다.

투명한 사용자 식별에 실패하여 최종 사용자에게 인증 프롬프트가 표시되고 유효하지 않은 자격 증명으로 인해 사용자가 인증에 실패하면 사용자 게스트 액세스를 허용할지 여부를 선택할 수 있습니다.

참고 재인증을 사용하도록 설정하고 트랜잭션이 URL 필터링으로 인해 차단된 경우 최종 사용자 알림 페이지가 다른 사용자로 로그인할 수 있는 옵션과 함께 표시됩니다. 링크를 클릭하는 사용자에게 인증 프롬프트가 표시됩니다. 자세한 내용은 권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용, 5-32페이지를 참고하십시오.

투명한 사용자 식별 이해

사용 가능한 투명한 사용자 식별 방법은 다음과 같습니다.

- **Transparently identify users with ISE(ISE로 투명하게 사용자 식별)** – ISE(Identity Services Engine) 서비스가 사용하도록 설정된 경우(Network(네트워크) > ISE(Identity Services Engine)) 사용할 수 있습니다. 이러한 트랜잭션의 경우 ISE(Identity Services Engine) 서버에서 사용자 이름 및 연결된 SGT(Secure Group Tag)를 가져옵니다. ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지를 참조하십시오.
- **Transparently identify users with ASA(ASA로 투명하게 사용자 식별)** – Cisco Adaptive Security Appliance에서 받은 현재 IP 주소-사용자 이름 매핑으로 사용자를 식별합니다(원격 사용자 전용). 이 옵션은 AnyConnect Secure Mobility가 사용하도록 설정되고 ASA와 통합된 경우에 사용할 수 있습니다. 사용자 이름은 ASA에서 가져오고 연결된 디렉토리 그룹은 웹 보안 어플라이언스에 지정된 인증 영역 또는 시퀀스에서 가져옵니다. 원격 사용자, 10-18페이지를 참조하십시오.
- **Transparently identify users with authentication realms(인증 영역으로 투명하게 사용자 식별)** – 이 옵션은 하나 이상의 인증 영역이 다음 인증 서버 중 하나를 사용하여 투명한 식별을 지원하도록 구성된 경우에 사용할 수 있습니다.
  - **Active Directory** – NTLM 또는 Kerberos 인증 영역을 생성하고 투명한 사용자 식별을 사용하도록 설정합니다. 또한 Cisco Context Directory Agent와 같은 별도의 Active Directory 에이전트를 구축해야 합니다. 자세한 내용은 Active Directory를 사용한 투명한 사용자 식별, 5-6페이지를 참고하십시오.
  - **LDAP** – eDirectory로 구성된 LDAP 인증 영역을 생성하고 투명한 사용자 식별을 사용하도록 설정합니다. 자세한 내용은 LDAP를 사용한 투명한 사용자 식별, 5-8페이지를 참고하십시오.

  AsyncOS for Web은 일정한 간격으로 eDirectory 또는 Active Directory 에이전트와 통신하여 인증된 사용자 이름을 현재 IP 주소와 일치시키는 매핑을 유지합니다.

Active Directory를 사용한 투명한 사용자 식별

Active Directory는 웹 보안 어플라이언스와 같은 다른 시스템에서 쉽게 쿼리하는 형식으로 사용자 로그인 정보를 기록하지 않습니다. Cisco CDA(Context Directory Agent)와 같은 Active Directory 에이전트는 Active Directory 보안 이벤트 로그에서 인증된 사용자에 대한 정보를 쿼리하는 데 필요합니다.

AsyncOS for Web은 Active Directory 에이전트와 통신하여 IP 주소와 사용자 이름 간 매핑의 로컬 사본을 유지 관리합니다. AsyncOS for Web이 IP 주소를 사용자 이름과 연결해야 하는 경우 먼저 매핑의 로컬 사본을 확인합니다. 일치 항목이 발견되지 않으면 일치 항목을 찾기 위해 Active Directory 에이전트에 쿼리합니다.

Active Directory 에이전트 설치 및 구성에 대한 자세한 내용은 Web Security appliance에 정보를 제공하도록 Active Directory 에이전트 설정, 5-7페이지를 참조하십시오.

Active Directory를 사용하여 투명하게 사용자를 식별하는 경우 다음을 고려하십시오.

- Active Directory를 사용한 투명한 사용자 식별은 NTLM 또는 Kerberos 인증 체계에서만 작동합니다. Active Directory 인스턴스에 해당하는 LDAP 인증 영역과 함께 사용할 수 없습니다.
- 투명한 사용자 식별은 Active Directory 에이전트에서 지원되는 Active Directory 버전에서 작동합니다.
- 고가용성을 위해 다른 머신에 Active Directory 에이전트의 두 번째 인스턴스를 설치할 수 있습니다. 이를 수행하면 각 Active Directory 에이전트가 다른 에이전트와 독립적으로 IP 주소와 사용자 이름 간 매핑을 유지 관리합니다. 기본 에이전트에 대한 ping 시도에 3번 실패하면 AsyncOS for Web에서 백업 Active Directory 에이전트를 사용합니다.
- Active Directory 에이전트는 웹 보안 어플라이언스와 통신할 때 온디맨드 모드를 사용합니다.
- Active Directory 에이전트가 사용자 로그아웃 정보를 웹 보안 어플라이언스에 푸시합니다. 경우에 따라 일부 사용자 로그아웃 정보가 Active Directory 보안 로그에 기록되지 않습니다. 이는 클라이언트 머신의 작동이 중단되거나 사용자가 로그아웃하지 않고 머신을 종료하는 경우 발생할 수 있습니다. 보안 로그에 사용자 로그아웃 정보가 없는 경우 Active Directory 에이전트에서 IP 주소가 더 이상 해당 사용자에 할당되지 않음을 어플라이언스에 알릴 수 없습니다. 이러한 가능성을 없애기 위해 Active Directory 에이전트의 업데이트가 없을 때 AsyncOS에서 IP 주소와 사용자 간 매핑을 캐시하는 기간을 정의할 수 있습니다. 자세한 내용은 CLI를 사용하여 고급 투명한 사용자 식별 설정 구성, 5-9페이지를 참고하십시오.
- Active Directory 에이전트는 특정 IP 주소에서 로그인하는 각 사용자에 대한 `sAMAccountName`을 기록하여 사용자 이름이 고유하도록 합니다.
- 클라이언트 머신에서 Active Directory 서버 및 웹 보안 어플라이언스에 표시하는 클라이언트 IP 주소는 동일해야 합니다.
- AsyncOS for Web은 직계 상위 그룹에서만 사용자를 검색합니다. 중첩된 그룹은 검색하지 않습니다.

Web Security appliance에 정보를 제공하도록 Active Directory 에이전트 설정

AsyncOS for Web은 Active Directory에서 직접 클라이언트 IP 주소를 가져올 수 없으므로 Active Directory 에이전트에서 IP 주소와 사용자 이름 간의 매핑 정보를 가져와야 합니다.

웹 보안 어플라이언스에 액세스할 수 있으며 표시된 모든 Windows 도메인 컨트롤러와 통신할 수 있는 네트워크의 머신에 Active Directory 에이전트를 설치합니다. 최상의 성능을 위해 이 에이전트는 가능한 한 웹 보안 어플라이언스와 물리적으로 가까운 위치에 있어야 합니다. 작은 규모의 네트워크 환경에서는 Active Directory 서버에 직접 Active Directory 에이전트를 설치할 수 있습니다.

참고 웹 보안 어플라이언스와 통신하는 데 사용되는 Active Directory 에이전트 인스턴스가 Cisco Adaptive Security Appliance 및 기타 웹 보안 어플라이언스를 포함하여 다른 어플라이언스를 지원할 수도 있습니다.

Cisco Context Directory Agent 가져오기, 설치 및 구성

다음에서 Cisco Context Directory Agent 다운로드, 설치 및 구성에 대한 정보를 찾을 수 있습니다. http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html

참고 웹 보안 어플라이언스 및 Active Directory 에이전트는 RADIUS 프로토콜을 사용하여 서로 통신합니다. 어플라이언스와 에이전트는 동일한 공유 암호를 사용하여 사용자 암호를 난독 처리하도록 구성되어야 합니다. 다른 사용자 특성은 난독 처리되지 않습니다.

LDAP를 사용한 투명한 사용자 식별

AsyncOS for Web은 IP 주소와 사용자 이름 간의 매핑을 유지 관리하는 LDAP(Lightweight Directory Access Protocol) 영역으로 구성된 eDirectory 서버와 통신할 수 있습니다. 사용자가 eDirectory 클라이언트를 통해 로그인할 경우 사용자가 eDirectory 서버에 대해 인증됩니다. 인증에 성공하면 클라이언트 IP 주소가 로그인한 사용자의 특성(`NetworkAddress`)으로 eDirectory 서버에 기록됩니다.

LDAP(eDirectory)를 사용하여 투명하게 사용자를 식별하는 경우 다음을 고려하십시오.

- eDirectory 클라이언트가 각 클라이언트 워크스테이션에 설치되어야 하고 최종 사용자가 이를 사용하여 eDirectory 서버에 대해 인증해야 합니다.
- eDirectory 클라이언트 로그인에서 사용되는 LDAP 트리는 인증 영역에 구성된 LDAP 트리와 동일해야 합니다.
- eDirectory 클라이언트에서 여러 LDAP 트리를 사용하는 경우 각 트리에 대한 인증 영역을 생성한 후 각 LDAP 인증 영역을 사용하는 인증 시퀀스를 생성합니다.
- LDAP 인증 영역을 eDirectory로 구성할 때 쿼리 자격 증명에 대한 바인드 DN을 지정해야 합니다.
- 사용자가 로그인할 때 사용자 개체의 `NetworkAddress` 특성을 업데이트하도록 eDirectory 서버를 구성해야 합니다.
- AsyncOS for Web은 직계 상위 그룹에서만 사용자를 검색합니다. 중첩된 그룹은 검색하지 않습니다.
- eDirectory 사용자의 `NetworkAddress` 특성을 사용하여 사용자의 최근 로그인 IP 주소를 확인할 수 있습니다.

투명한 사용자 식별에 대한 규칙 및 지침

인증 서버를 사용한 투명한 사용자 식별을 사용할 때는 다음 규칙 및 지침을 고려하십시오.

- DHCP를 사용하여 클라이언트 머신에 IP 주소를 할당하는 경우 웹 보안 어플라이언스에서 IP 주소와 사용자 이름 간의 매핑이 DHCP 리스보다 더 자주 업데이트되는지 확인하십시오. `tuiconfig` CLI 명령을 사용하여 매핑 업데이트 간격을 업데이트합니다. 자세한 내용은 CLI를 사용하여 고급 투명한 사용자 식별 설정 구성, 5-9페이지를 참고하십시오.
- 사용자가 머신에서 로그아웃하고 웹 보안 어플라이언스에서 IP 주소와 사용자 이름 간 매핑이 업데이트되기 전에 다른 사용자가 동일한 머신에 로그인하는 경우 웹 프록시가 클라이언트를 이전 사용자로 기록합니다.
- 투명한 사용자 식별이 실패하는 경우 웹 프록시에서 트랜잭션을 처리하는 방법을 구성할 수 있습니다. 사용자에게 게스트 액세스 권한을 부여하거나 최종 사용자에게 인증 프롬프트가 강제로 표시되도록 할 수 있습니다.
- 투명한 사용자 식별에 실패하여 사용자에게 인증 프롬프트가 표시되고 유효하지 않은 자격 증명으로 인해 사용자가 인증에 실패하면 사용자 게스트 액세스를 허용할지 여부를 선택할 수 있습니다.
- 할당된 식별 프로필에서 사용자가 존재하는 여러 영역을 포함하는 인증 시퀀스를 사용하는 경우 AsyncOS for Web이 시퀀스에 표시되는 순서대로 영역에서 사용자 그룹을 가져옵니다.
- 투명하게 사용자를 식별하도록 식별 프로필을 구성하는 경우 인증 서로게이트가 IP 주소여야 합니다. 다른 서로게이트 유형을 선택할 수 없습니다.
- 사용자에 대한 세부 트랜잭션을 볼 때 Web Tracking(웹 추적) 페이지에 투명하게 식별된 사용자가 표시됩니다.

- %m 및 x-auth-mechanism 맞춤형 필드를 사용하여 액세스 및 WC3 로그에 어떤 사용자가 투명하게 식별되었는지 기록할 수 있습니다. SSO_TUI의 로그 항목은 투명한 사용자 식별을 사용하여 클라이언트 IP 주소를 인증된 사용자 이름과 일치시켜서 사용자 이름을 가져왔음을 나타냅니다. (마찬가지로, SSO_ASA 값은 사용자가 원격 사용자이고 AnyConnect Secure Mobility를 사용하여 Cisco ASA에서 사용자 이름을 가져왔음을 나타냅니다.)

투명한 사용자 식별 구성

투명한 사용자 식별 및 권한 부여 구성은 최종 사용자 자격 증명 확보, 5-1페이지에 자세히 설명되어 있습니다. 기본 단계는 다음과 같습니다.

- 인증 영역을 생성하고 순서를 지정합니다.
- 사용자 및 클라이언트 소프트웨어를 분류하기 위한 식별 프로필을 생성합니다.
- 식별된 사용자 및 사용자 그룹의 웹 요청을 관리하기 위한 정책을 생성합니다.

CLI를 사용하여 고급 투명한 사용자 식별 설정 구성

AsyncOS for Web은 다음과 같은 TUI 관련 CLI 명령을 제공합니다.

- **tuiconfig** – 투명한 사용자 식별과 연관된 고급 설정을 구성합니다. 배치 모드를 사용하여 여러 매개변수를 동시에 구성할 수 있습니다.
  - **Active Directory 에이전트에 대한 매핑 시간 초과 구성** – 에이전트의 업데이트가 없는 경우 AD 에이전트에서 검색된 IP 주소에 대한 IP 주소-사용자 매핑이 캐시되는 시간(분)입니다.
  - **Active Directory 에이전트에 대한 프록시 캐시 시간 초과 구성** – 프록시별 IP 주소-사용자 매핑이 캐시되는 시간(초)이며, 유효한 값의 범위는 5 ~ 1200초입니다. 기본값 및 권장되는 값은 120초입니다. 하한값을 지정하면 프록시 성능에 부정적인 영향이 미칠 수 있습니다.
  - **Novell eDirectory에 대한 매핑 시간 초과 구성** – 서버의 업데이트가 없는 경우 eDirectory 서버에서 검색된 IP 주소에 대한 IP 주소-사용자 매핑이 캐시되는 시간(분)입니다.
  - **Active Directory 에이전트에 대한 쿼리 대기 시간 구성** – Active Directory 에이전트의 응답을 대기하는 시간(초)입니다. 쿼리에 이 값보다 더 오랜 시간이 소요되는 경우 투명한 사용자 식별이 실패한 것으로 간주됩니다. 이를 통해 최종 사용자가 경험하는 인증 지연을 제한합니다.
  - **Novell eDirectory에 대한 쿼리 대기 시간 구성** – eDirectory 서버의 응답을 대기하는 시간(초)입니다. 쿼리에 이 값보다 더 오랜 시간이 소요되는 경우 투명한 사용자 식별이 실패한 것으로 간주됩니다. 이를 통해 최종 사용자가 경험하는 인증 지연을 제한합니다.

  Active Directory 설정은 투명한 사용자 식별을 위해 AD 에이전트를 사용하는 모든 AD 영역에 적용됩니다. eDirectory 설정은 투명한 사용자 식별을 위해 eDirectory를 사용하는 모든 LDAP 영역에 적용됩니다.

  하나의 매개변수에 대한 검증이 실패하면 값이 변경되지 않습니다.
- **tuistatus** – 이 명령은 다음과 같은 AD 관련 하위 명령을 제공합니다.
  - **adagentstatus** – 모든 AD 에이전트의 현재 상태와 Windows 도메인 컨트롤러와의 연결에 대한 정보를 표시합니다.
  - **listlocalmappings** – AD 에이전트에서 검색되는 웹 보안 어플라이언스에 저장된 모든 IP 주소-사용자 이름 매핑을 나열합니다. 에이전트에 저장된 항목을 나열하지 않으며 현재 진행 중인 쿼리에 대한 매핑도 나열하지 않습니다.

단일 로그인 구성

자격 증명을 투명하게 가져오면 단일 로그인 환경을 손쉽게 만들 수 있습니다. 투명한 사용자 식별은 인증 영역 설정입니다.

Internet Explorer의 경우 리디렉션 호스트 이름은 정규화된 도메인이 아니라 간단한 호스트 이름(점을 포함하지 않음) 또는 NetBIOS 이름이어야 합니다. 또는 Internet Explorer의 로컬 인트라넷 영역에 어플라이언스 호스트 이름을 추가할 수 있지만(Tools(도구) > Internet options(인터넷 옵션) > Security(보안) 탭) 모든 클라이언트에서 이를 수행해야 합니다. 이에 대한 자세한 내용은 How do I properly set up NTLM with SSO (credentials sent transparently)?를 참조하십시오.

Firefox 및 기타 비Microsoft 브라우저의 경우 **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** 및 **network.automatic-ntlm-auth.trusted-uris** 매개변수를 투명 모드 리디렉션 호스트 이름으로 설정해야 합니다. Firefox is not sending authentication credentials transparently (SSO)를 참조할 수도 있습니다. 이 자료에서는 Firefox 매개변수 변경에 대한 일반 정보를 제공합니다.

리디렉션 호스트 이름에 대한 자세한 내용은 전역 인증 설정 구성 또는 CLI 명령 sethostname을 참조하십시오.

인증 영역

인증 영역은 인증 서버에 접속하는 데 필요한 세부 정보를 정의하고 클라이언트와 통신할 때 사용할 인증 체계를 지정합니다. AsyncOS는 여러 인증 영역을 지원합니다. 영역을 인증 시퀀스로 그룹화하여 여러 인증 요건이 있는 사용자를 동일한 정책을 통해 관리할 수도 있습니다.

- 외부 인증, 5-10페이지
- Kerberos 인증 체계에 대한 Active Directory 영역 생성, 5-11페이지
- Active Directory 인증 영역(NTLMSSP 및 기본)을 생성하는 방법, 5-13페이지
- LDAP 인증 영역 생성, 5-15페이지
- 인증 영역 삭제 정보, 5-20페이지
- 전역 인증 설정 구성, 5-20페이지

관련 주제

- RADIUS 사용자 인증, 22-9페이지
- 인증 시퀀스, 5-25페이지

외부 인증

외부 LDAP 또는 RADIUS 서버를 통해 사용자를 인증할 수 있습니다.

LDAP 서버를 통한 외부 인증 구성

시작하기 전에

- LDAP 인증 영역을 생성하여 하나 이상의 외부 인증 쿼리로 구성합니다. LDAP 인증 영역 생성, 5-15페이지

1단계 어플라이언스에서 외부 인증을 사용하도록 설정합니다.

a. **System Administration(시스템 관리)** > **Users(사용자)**로 이동합니다.

b. External Authentication(외부 인증) 섹션에서 **Enable(사용)**을 클릭합니다.

c. 옵션을 구성합니다.

옵션	설명
외부 인증 사용:	—
인증 유형	LDAP를 선택합니다.
외부 인증 캐시 시간 제한	재인증을 위해 LDAP 서버에 다시 연결하기 전까지 AsyncOS가 외부 인증 자격 증명을 저장하는 시간(초)입니다. 기본값은 영(0)입니다.
LDAP 외부 인증 쿼리	LDAP 영역으로 구성된 쿼리입니다.
서버의 유효한 응답을 대기하는 시간 초과	AsyncOS가 서버로부터 쿼리에 대한 응답을 대기하는 시간(초)입니다.
그룹 매핑	디렉토리에 있는 각 그룹 이름에 대해 역할을 할당합니다.

2단계 변경 사항을 제출 및 커밋합니다.

RADIUS 외부 인증 사용

RADIUS를 사용하여 외부 인증 사용, 22-9페이지를 참조하십시오.

Kerberos 인증 체계에 대한 Active Directory 영역 생성

시작하기 전에

- 어플라이언스가 표준 모드(클라우드 커넥터 모드 아님)에서 구성되었는지 확인합니다.
- Active Directory 서버를 준비합니다.
  - Windows Server 2003, 2008, 2008R2 또는 2012 중 하나에 Active Directory를 설치합니다.
  - Active Directory 서버에 도메인 관리자의 구성원인 사용자를 생성합니다.
  - 클라이언트를 도메인에 조인합니다. 지원되는 클라이언트는 Windows XP, Windows 7 및 Mac OS 10.5+입니다.
  - 다음 사이트에서 Windows Resource Kit의 kerbtray 툴을 사용하여 클라이언트의 Kerberos 티켓을 확인합니다. http://www.microsoft.com/en-us/download/details.aspx?id=17657
  - 주 메뉴 > KeyChain Access(키체인 접근) 아래에서 Mac 클라이언트의 티켓 뷰어 애플리케이션을 사용하여 Kerberos 티켓을 볼 수 있습니다.
- 인증하려는 Active Directory 도메인에 Web Security appliance에 조인하는 데 필요한 권한 및 도메인 정보가 있는지 확인합니다.
- 웹 보안 어플라이언스의 현재 시간을 Active Directory 서버의 현재 시간과 비교하여 차이가 Active Directory 서버의 "Maximum tolerance for computer clock synchronization(컴퓨터 시계 동기화 최대 허용 오차)" 옵션에 지정된 시간보다 크지 않은지 확인합니다.

- 웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 여러 웹 보안 어플라이언스에 있는 동일한 이름의 인증 영역에서 각 어플라이언스에 동일한 속성이 정의되었는지 확인하여 준비합니다.
- 웹 보안 어플라이언스 컨피그레이션:
  - 명시적 모드에서는 WSA 호스트 이름(CLI 명령 sethostname)과 브라우저에 구성된 프록시 이름이 동일해야 합니다.
  - 투명 모드에서는 WSA 호스트 이름이 리디렉션 호스트 이름(전역 인증 설정 구성, 5-20페이지 참조)과 동일해야 합니다. 또한 Kerberos 영역을 생성하기 전에 WSA 호스트 이름과 리디렉션 호스트 이름을 구성해야 합니다.
- 새 영역을 커밋하면 영역의 인증 프로토콜을 변경할 수 없습니다.
- 클라이언트 브라우저에서 단일 로그인을 구성해야 합니다. 단일 로그인 구성, 5-10페이지를 참조하십시오.
- 로그 사용을 간소화하려면 `%m` 맞춤형 필드 매개변수를 사용하도록 액세스 로그를 맞춤 설정합니다. 액세스 로그 맞춤화, 21-26페이지를 참조하십시오.

1단계 Cisco Web Security Appliance 웹 인터페이스에서 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Add Realm(영역 추가)**을 클릭합니다.

3단계 영숫자 및 공백 문자만 사용하여 인증 영역에 고유한 이름을 지정합니다.

4단계 Authentication Protocol(인증 프로토콜) 필드에서 **Active Directory**를 선택합니다.

5단계 Active Directory 서버의 정규화된 도메인 이름 또는 IP 주소를 최대 3개 입력합니다.

예: `ntlm.example.com`.

어플라이언스에 구성된 DNS 서버가 Active Directory 서버 호스트 이름을 확인할 수 없는 경우에만 IP 주소가 필요합니다.

영역에 여러 인증 서버가 구성된 경우 이 영역 내에서 트랜잭션을 인증하는 데 실패하기 전에 어플라이언스가 최대 3개의 인증 서버로 인증하려고 시도합니다.

6단계 어플라이언스를 도메인에 조인합니다.

a. Active Directory 계정을 구성합니다.

설정	설명
Active Directory 도메인	Active Directory 서버 도메인 이름입니다. DNS 도메인 또는 영역이라고도 합니다.
NetBIOS 도메인 이름	네트워크에서 NetBIOS를 사용하는 경우 도메인 이름을 제공합니다. **정보** 이 옵션이 사용 불가능하면 setntlmsecuritymode CLI 명령을 사용하여 NTLM 보안 모드가 "domain"으로 설정되어 있는지 확인합니다.
컴퓨터 계정	AsyncOS가 도메인에서 컴퓨터를 고유하게 식별하기 위해 "머신 신뢰 계정"이라고도 하는 Active Directory 컴퓨터 계정을 생성할 Active Directory 도메인에서 위치를 지정합니다. Active Directory 환경에서 특정 간격으로 컴퓨터 개체를 자동으로 삭제하는 경우 자동 삭제에서 보호되는 컨테이너에 있는 컴퓨터 계정의 위치를 지정합니다.

b. **Join Domain(도메인에 조인)**을 클릭합니다.

c. Active Directory의 계정에 대한 로그인 자격 증명(사용자 이름 및 암호)을 제공하고 Create Account(계정 생성)를 클릭합니다.

7단계 (선택 사항) 투명한 사용자 식별을 구성합니다.

설정	설명
Active Directory 에이전트를 사용하여 투명한 사용자 식별 사용	기본 Context Directory Agent가 설치된 머신의 서버 이름과 액세스하는 데 사용된 공유 암호를 모두 입력합니다. (선택 사항) 백업 Context Directory Agent가 설치된 머신의 서버 이름과 해당 공유 암호를 입력합니다.

8단계 네트워크 보안을 구성합니다.

설정	설명
클라이언트 서명 필요	클라이언트 서명이 필요하도록 Active Directory 서버가 구성된 경우 이 옵션을 선택합니다. 이 옵션을 선택한 경우 AsyncOS가 Active Directory 서버와 통신할 때 TLS(Transport Layer Security)를 사용합니다.

9단계 (선택 사항) **Start Test(테스트 시작)**를 클릭합니다. 그러면 사용자가 입력한 설정이 테스트되어 실제 사용자가 인증하는 데 사용하기 전에 설정이 올바른지 확인합니다. 수행되는 테스트에 대한 자세한 내용은 •기존 NTLM 영역에서 신뢰할 수 없는 도메인의 사용자를 인증하기 위한 추가 NTLM 영역을 생성합니다., 5-20페이지를 참조하십시오.

10단계 테스트 중에 발견된 문제를 트러블슈팅합니다. 인증 문제에 대한 트러블슈팅 툴을 참고하십시오.

11단계 변경 사항을 제출 및 커밋합니다.

다음 작업

- Kerberos 인증 체계를 사용하는 식별 프로필을 생성합니다. 사용자 및 클라이언트 소프트웨어 분류, 6-3페이지.

Active Directory 인증 영역(NTLMSSP 및 기본)을 생성하는 방법

Active Directory 인증 영역(NTLMSSP 및 기본) 생성에 대한 사전 요구 사항

- 인증하려는 Active Directory 도메인에 Web Security appliance에 조인하는 데 필요한 권한 및 도메인 정보가 있는지 확인합니다.
- "domain"을 NTLM 보안 모드로 사용하려는 경우 중첩된 Active Directory 그룹만 사용합니다. Active Directory 그룹이 중첩되지 않은 경우 기본값 "ads"를 사용합니다. 이 설명서의 CLI(Command Line Interface) 부록에서 setntlmsecuritymode를 참조하십시오.
- 웹 보안 어플라이언스의 현재 시간을 Active Directory 서버의 현재 시간과 비교하여 차이가 Active Directory 서버의 "Maximum tolerance for computer clock synchronization(컴퓨터 시계 동기화 최대 허용 오차)" 옵션에 지정된 시간보다 크지 않은지 확인합니다.

- 웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 여러 웹 보안 어플라이언스에 있는 동일한 이름의 인증 영역에서 각 어플라이언스에 동일한 속성이 정의되었는지 확인하여 준비합니다.
- 새 영역을 커밋하면 영역의 인증 프로토콜을 변경할 수 없습니다.
- NTLMSSP의 경우 클라이언트 브라우저에서 단일 로그인을 구성할 수 있습니다. 단일 로그인 구성, 5-10페이지를 참조하십시오.

다중 NTLM 영역 및 도메인 사용에 대한 정보

다음 규칙은 다중 NTLM 영역 및 도메인 사용에 대해 적용됩니다.

- 최대 10개의 NTLM 인증 영역을 생성할 수 있습니다.
- 한 NTLM 영역의 클라이언트 IP 주소가 다른 NTLM 영역의 클라이언트 IP 주소와 중복되어서는 안 됩니다.
- 각 NTLM 영역은 하나의 Active Directory 도메인에만 조인할 수 있지만 해당 도메인에서 신뢰할 수 있는 모든 도메인의 사용자를 인증할 수 있습니다. 이 신뢰는 기본적으로 동일한 포리스트에 있는 다른 도메인에 적용되고 하나 이상의 단방향 신뢰가 존재하는 포리스트 외부의 도메인에 적용됩니다.
- 기존 NTLM 영역에서 신뢰할 수 없는 도메인의 사용자를 인증하기 위한 추가 NTLM 영역을 생성합니다.

Active Directory 인증 영역 생성(NTLMSSP 및 기본)

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Add Realm(영역 추가)**을 클릭합니다.

3단계 영숫자 및 공백 문자만 사용하여 인증 영역에 고유한 이름을 지정합니다.

4단계 Authentication Protocol and Scheme(s)(인증 프로토콜 및 체계) 필드에서 **Active Directory**를 선택합니다.

5단계 Active Directory 서버의 정규화된 도메인 이름 또는 IP 주소를 최대 3개 입력합니다.

예: `active.example.com`.

어플라이언스에 구성된 DNS 서버가 Active Directory 서버 호스트 이름을 확인할 수 없는 경우에만 IP 주소가 필요합니다.

영역에 여러 인증 서버가 구성된 경우 이 영역 내에서 트랜잭션을 인증하는 데 실패하기 전에 어플라이언스가 최대 3개의 인증 서버로 인증하려고 시도합니다.

6단계 어플라이언스를 도메인에 조인합니다.

a. Active Directory 계정을 구성합니다.

설정	설명
Active Directory 도메인	Active Directory 서버 도메인 이름입니다. DNS 도메인 또는 영역이라고도 합니다.
NetBIOS 도메인 이름	네트워크에서 NetBIOS를 사용하는 경우 도메인 이름을 제공합니다.

설정	설명
컴퓨터 계정	AsyncOS가 도메인에서 컴퓨터를 고유하게 식별하기 위해 "머신 신뢰 계정"이라고도 하는 Active Directory 컴퓨터 계정을 생성할 Active Directory 도메인에서 위치를 지정합니다. Active Directory 환경에서 특정 간격으로 컴퓨터 개체를 자동으로 삭제하는 경우 자동 삭제에서 보호되는 컨테이너에 있는 컴퓨터 계정의 위치를 지정합니다.

b. **Join Domain(도메인에 조인)**을 클릭합니다.

c. 도메인에서 컴퓨터 계정을 생성할 권한이 있는 기존 Active Directory 사용자의 sAMAccountName 사용자 이름 및 암호를 입력합니다.

   예를 들어, "jazzdoe"입니다. "DOMAIN\jazzdoe" 또는 "jazzdoe@domain"은 사용하지 마십시오.

   이 정보는 컴퓨터 계정을 설정하는 데 한 번 사용되고 저장되지 않습니다.

d. **Create Account(계정 생성)**를 클릭합니다.

7단계 (선택 사항) 투명 인증을 구성합니다.

설정	설명
Active Directory 에이전트를 사용하여 투명한 사용자 식별 사용	기본 Context Directory Agent가 설치된 머신의 서버 이름과 액세스하는 데 사용된 공유 암호를 모두 입력합니다. (선택 사항) 백업 Context Directory Agent가 설치된 머신의 서버 이름과 해당 공유 암호를 입력합니다.

8단계 네트워크 보안을 구성합니다.

설정	설명
클라이언트 서명 필요	클라이언트 서명이 필요하도록 Active Directory 서버가 구성된 경우 이 옵션을 선택합니다. 이 옵션을 선택한 경우 AsyncOS가 Active Directory 서버와 통신할 때 TLS(Transport Layer Security)를 사용합니다.

9단계 (선택 사항) **Start Test(테스트 시작)**를 클릭합니다. 그러면 사용자가 입력한 설정이 테스트되어 실제 사용자가 인증하는 데 사용하기 전에 설정이 올바른지 확인합니다.

10단계 변경 사항을 제출 및 커밋합니다.

LDAP 인증 영역 생성

시작하기 전에

- 사용자 조직의 LDAP에 대한 다음 정보를 확보합니다.
  - LDAP 버전
  - 서버 주소
  - LDAP 포트

- 웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 여러 웹 보안 어플라이언스에 있는 동일한 이름의 인증 영역에서 각 어플라이언스에 동일한 속성이 정의되었는지 확인합니다.

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Add Realm(영역 추가)**을 클릭합니다.

3단계 영숫자 및 공백 문자만 사용하여 인증 영역에 고유한 이름을 지정합니다.

4단계 Authentication Protocol and Scheme(s)(인증 프로토콜 및 체계) 필드에서 **LDAP**를 선택합니다.

5단계 LDAP 인증 설정을 입력합니다.

설정	설명
LDAP 버전	LDAP 버전을 선택하고 보안 LDAP를 사용할지 여부를 선택합니다. 어플라이언스는 LDAP 버전 2 및 3을 지원합니다. 보안 LDAP에는 LDAP 버전 3이 필요합니다. 이 LDAP 서버가 Novell eDirectory를 투명한 사용자 식별에 사용하도록 지원하는지 여부를 선택합니다.
LDAP 서버	LDAP 서버 IP 주소 또는 호스트 이름과 해당 포트 번호를 입력합니다. 최대 3개의 서버를 지정할 수 있습니다. 호스트 이름은 정규화된 도메인 이름이어야 합니다. 예를 들어, `ldap.example.com`입니다. 어플라이언스에 구성된 DNS 서버가 LDAP 서버 호스트 이름을 확인할 수 없는 경우에만 IP 주소가 필요합니다. 표준 LDAP의 기본 포트 번호는 389입니다. 보안 LDAP의 기본 번호는 636입니다. LDAP 서버가 Active Directory 서버인 경우, 여기에 도메인 컨트롤러의 호스트 이름 또는 IP 주소와 포트를 입력합니다. 가능한 경우 전역 카탈로그 서버의 이름을 입력하고 포트 3268을 사용합니다. 그러나 전역 카탈로그 서버가 물리적으로 멀리 떨어져 있고 로컬 도메인 컨트롤러의 사용자만 인증해야 한다는 것을 알고 있는 경우 로컬 도메인 컨트롤러를 사용할 수 있습니다. **참고:** 영역에서 여러 인증 서버를 구성할 때 해당 영역 내의 트랜잭션을 인증하는 데 실패하기 전에 어플라이언스가 최대 3개의 인증 서버로 인증하려고 시도합니다.
LDAP 영구 연결 (Advanced(고급) 섹션 아래)	다음 값 중 하나를 선택합니다. • **영구 연결 사용(무제한)**. 기존 연결을 사용합니다. 사용 가능한 연결이 없는 경우 새 연결이 열립니다. • **영구 연결 사용.** 기존 연결을 사용하여 지정된 수의 요청을 제공합니다. 최대값에 도달하면 LDAP 서버에 대한 새 연결을 설정합니다. • **영구 연결을 사용하지 않음.** 항상 LDAP 서버에 대한 새 연결을 생성합니다.

설정	설명
사용자 인증	다음 필드에 값을 입력합니다. **기본 고유 이름(기본 DN)** LDAP 데이터베이스가 트리 유형 디렉토리 구조이며 어플라이언스가 기본 DN을 사용하여 LDAP 디렉토리 트리의 올바른 위치로 이동한 후 검색을 시작합니다. 유효한 기본 DN 필터 문자열은 `object-value` 형식의 하나 이상의 구성 요소로 이루어집니다. 예를 들어, `dc=companyname, dc=com`입니다. **사용자 이름 특성** 다음 값 중 하나를 선택합니다. • **uid**, **cn** 및 **sAMAccountName.** 사용자 이름을 지정하는 LDAP 디렉토리의 고유 식별자입니다. • **맞춤형.** `UserAccount`와 같은 맞춤형 식별자입니다. **사용자 필터 쿼리** 사용자 필터 쿼리는 사용자 기본 DN을 찾는 LDAP 검색 필터입니다. 사용자 디렉토리가 기본 DN 아래의 계층 구조에 있거나 로그인 이름이 해당 사용자 기본 DN의 사용자별 구성 요소에 포함되지 않은 경우에 필요합니다. 다음 값 중 하나를 선택합니다. • **없음.** 모든 사용자를 필터링합니다. • **맞춤형.** 특정 사용자 그룹을 필터링합니다.
쿼리 자격 증명	인증 서버가 익명 쿼리를 수락하는지 여부를 선택합니다. 인증 서버가 익명 쿼리를 수락하는 경우 **Server Accepts Anonymous Queries(서버가 익명 쿼리를 수락함)**를 선택합니다. 인증 서버가 익명 쿼리를 수락하지 않는 경우 **Use Bind DN(바인드 DN 사용)**을 선택한 후 다음 정보를 입력합니다. • **바인드 DN.** LDAP 디렉토리를 검색하도록 허용된 외부 LDAP 서버의 사용자입니다. 일반적으로 바인드 DN은 전체 디렉토리를 검색하도록 허용되어야 합니다. • **암호.** Bind DN(바인드 DN) 필드에 입력하는 사용자와 연관된 암호입니다. 다음 텍스트는 Bind DN(바인드 DN) 필드의 몇 가지 사용자 예입니다. cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. LDAP 서버가 Active Directory 서버인 경우 바인드 DN 사용자 이름을 "DOMAIN\username"으로 입력할 수도 있습니다.

6단계 (선택 사항) 그룹 개체 또는 사용자 개체를 통해 그룹 권한 부여를 사용하도록 설정하고 선택한 옵션에 대한 설정을 적절히 완료합니다.

그룹 개체 설정	설명
그룹 개체 내의 그룹 구성원 자격 특성	이 그룹에 속하는 모든 사용자를 나열하는 LDAP 특성을 선택합니다. 다음 값 중 하나를 선택합니다. • **member** 및 **uniquemember.** 그룹 구성원을 지정하는 LDAP 디렉토리의 고유 식별자입니다. • **맞춤형.** `UserInGroup`과 같은 맞춤형 식별자입니다.
그룹 이름을 포함하는 특성	정책 그룹 컨피그레이션에서 사용할 수 있는 그룹 이름을 지정하는 LDAP 특성을 선택합니다. 다음 값 중 하나를 선택합니다. • **cn.** 그룹의 이름을 지정하는 LDAP 디렉토리의 고유 식별자입니다. • **맞춤형.** `FinanceGroup`과 같은 맞춤형 식별자입니다.
개체가 그룹인지 여부를 결정하는 쿼리 문자열	LDAP 개체가 사용자 그룹을 나타내는지 여부를 결정하는 LDAP 검색 필터를 선택합니다. 다음 값 중 하나를 선택합니다. • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** `objectclass=person`과 같은 맞춤형 필터입니다. **참고:** 이 쿼리에서는 정책 그룹에서 사용할 수 있는 인증 그룹 집합을 정의합니다.

사용자 개체 설정	설명
사용자 개체 내의 그룹 구성원 자격 특성	이 사용자가 속하는 모든 그룹을 나열하는 특성을 선택합니다. 다음 값 중 하나를 선택합니다. • **memberOf.** 사용자 구성원을 지정하는 LDAP 디렉토리의 고유 식별자입니다. • **custom.** `UserInGroup`과 같은 맞춤형 식별자입니다.
그룹 구성원 자격 특성이 DN임	그룹 구성원 자격 특성이 LDAP 개체를 참조하는 DN(Distinguished Name)인지 여부를 지정합니다. Active Directory 서버의 경우 이 옵션을 사용하도록 설정합니다. 이 옵션이 사용하도록 설정된 경우 후속 설정을 구성해야 합니다.
그룹 이름을 포함하는 특성	그룹 구성원 자격 특성이 DN인 경우 이 옵션은 정책 그룹 컨피그레이션에서 그룹 이름으로 사용할 수 있는 특성을 지정합니다. 다음 값 중 하나를 선택합니다. • **cn.** 그룹의 이름을 지정하는 LDAP 디렉토리의 고유 식별자입니다. • **custom.** `FinanceGroup`과 같은 맞춤형 식별자입니다.

사용자 개체 설정	설명
개체가 그룹인지 여부를 결정하는 쿼리 문자열	LDAP 개체가 사용자 그룹을 나타내는지 여부를 결정하는 LDAP 검색 필터를 선택합니다. 다음 값 중 하나를 선택합니다. • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** `objectclass=person`과 같은 맞춤형 필터입니다. **참고:** 이 쿼리는 웹 보안 관리자 정책에서 사용될 수 있는 인증 그룹 집합을 정의합니다.

7단계 (선택 사항) 사용자의 외부 LDAP 인증 구성

a. **External Authentication Queries(외부 인증 쿼리)**를 선택합니다.

b. 사용자 계정을 식별합니다.

기본 DN	기본 DN을 사용하여 LDAP 디렉토리 트리의 올바른 위치로 이동한 후 검색을 시작합니다.

Query String(쿼리 문자열)	인증 그룹 집합을 반환하기 위한 쿼리입니다. 예를 들어, 다음과 같습니다.
	`(&(objectClass=posixAccount)(uid={u}))`
	또는
	`(&(objectClass=user)(sAMAccountName={u}))`

사용자의 전체 이름을 포함하는 특성	LDAP 특성(예: `displayName` 또는 `gecos`)입니다.

c. (선택 사항) RFC 2307 계정 만료 LDAP 특성에 따라 만료된 계정에 대한 로그인을 거부합니다.

d. 사용자에게 그룹 정보를 검색하기 위한 쿼리를 제공합니다.

한 사용자가 다양한 사용자 역할의 여러 LDAP 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 가장 제한적인 역할에 대한 권한을 부여합니다.

기본 DN	기본 DN을 사용하여 LDAP 디렉토리 트리의 올바른 위치로 이동한 후 검색을 시작합니다.
쿼리 문자열	`(&(objectClass=posixAccount)(uid={u}))`
사용자의 전체 이름을 포함하는 특성	`gecos`

8단계 (선택 사항) **Start Test(테스트 시작)**를 클릭합니다. 그러면 사용자가 입력한 설정이 테스트되어 실제 사용자가 인증하는 데 사용하기 전에 설정이 올바른지 확인합니다. 수행되는 테스트에 대한 자세한 내용은 •기존 NTLM 영역에서 신뢰할 수 없는 도메인의 사용자를 인증하기 위한 추가 NTLM 영역을 생성합니다., 5-20페이지를 참조하십시오.

참고 변경 사항을 제출하고 커밋하면 나중에 영역의 인증 프로토콜을 변경할 수 없습니다.

9단계 변경 사항을 제출 및 커밋합니다.

다음 작업

- Kerberos 인증 체계를 사용하는 식별 프로필을 생성합니다. 사용자 및 클라이언트 소프트웨어 분류, 6-3페이지.

관련 주제

- 외부 인증, 5-10페이지

다중 NTLM 영역 및 도메인 사용

다음 규칙은 다중 NTLM 영역 및 도메인 사용에 대해 적용됩니다.

- 최대 10개의 NTLM 인증 영역을 생성할 수 있습니다.
- 한 NTLM 영역의 클라이언트 IP 주소가 다른 NTLM 영역의 클라이언트 IP 주소와 중복되어서는 안 됩니다.
- 각 NTLM 영역은 하나의 Active Directory 도메인에만 조인할 수 있지만 해당 도메인에서 신뢰할 수 있는 모든 도메인의 사용자를 인증할 수 있습니다. 이 신뢰는 기본적으로 동일한 포리스트에 있는 다른 도메인에 적용되고 하나 이상의 단방향 신뢰가 존재하는 포리스트 외부의 도메인에 적용됩니다.
- 기존 NTLM 영역에서 신뢰할 수 없는 도메인의 사용자를 인증하기 위한 추가 NTLM 영역을 생성합니다.

인증 영역 삭제 정보

인증 영역을 삭제하면 연결된 ID가 사용하지 않도록 설정되고 해당 ID가 연결된 정책에서 제거됩니다.

인증 영역을 삭제하면 시퀀스에서 제거됩니다.

전역 인증 설정 구성

인증 프로토콜에 관계없이 모든 인증 영역에 설정을 적용하도록 전역 인증 설정을 구성합니다.

웹 프록시 구축 모드는 구성할 수 있는 전역 인증 설정에 영향을 미칩니다. 명시적 전달 모드가 아니라 투명 모드에서 구축되는 경우 더 많은 설정을 사용할 수 있습니다.

시작하기 전에

- 다음 개념을 숙지하십시오.
  - 실패한 인증, 5-27페이지
  - 권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용, 5-32페이지

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

3단계 Global Authentication Settings(전역 인증 설정) 섹션에서 설정을 편집합니다.

설정	설명
인증 서비스가 사용 불가능한 경우의 조치	다음 값 중 하나를 선택합니다. • **트래픽을 인증 없이 처리하도록 허용.** 사용자가 인증된 것처럼 계속 처리합니다. • **사용자 인증이 실패한 경우 모든 트래픽 차단.** 처리가 중단되고 모든 트래픽이 차단됩니다.
실패한 인증 처리	식별 프로필 정책에서 사용자에게 게스트 액세스 권한을 부여하는 경우 이 설정에 따라 웹 프록시가 액세스 로그에서 사용자를 게스트로 식별하고 기록하는 방법이 결정됩니다. 사용자에게 게스트 액세스 권한을 부여하는 방법에 대한 자세한 내용은 인증 실패 후 게스트 액세스 권한 부여, 5-31페이지를 참조하십시오.
재인증 (최종 사용자가 URL 카테고리 또는 사용자 세션 제한으로 인해 차단된 경우 재인증 프롬프트 사용)	제한적 URL 필터링 정책 또는 다른 IP 주소에 로그인하지 못하도록 제한되기 때문에 사용자가 웹 사이트에서 차단된 경우 이 설정을 통해 사용자가 다시 인증할 수 있습니다. 새 인증 자격 증명을 입력할 수 있는 링크가 포함된 차단 페이지가 사용자에게 표시됩니다. 사용자가 액세스를 확대할 수 있는 자격 증명을 입력하면 요청된 페이지가 브라우저에 표시됩니다. **참고:** 이 설정은 제한적인 URL 필터링 정책 또는 사용자 세션 제한으로 인해 차단된 인증된 사용자에만 적용됩니다. 인증이 없는 서브넷으로 인해 차단된 트랜잭션에는 적용되지 않습니다. 자세한 내용은 권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용, 5-32페이지를 참고하십시오.
기본 인증 토큰 TTL	인증 서버로 재검증하기 전에 사용자 자격 증명이 캐시에 저장되는 시간을 제어합니다. 여기에는 사용자 이름과 암호 및 사용자와 연관된 디렉토리 그룹이 포함됩니다. 기본값은 권장 설정입니다. 서로게이트 시간 초과 설정이 구성되고 기본 인증 토큰 TTL보다 큰 경우에는 서로게이트 시간 초과 값이 우선하며 서로게이트 시간 초과가 만료된 후 웹 프록시가 인증 서버에 접속합니다.

구성할 수 있는 나머지 인증 설정은 웹 프록시가 투명 모드 또는 명시적 전달 모드에서 구축되었는지에 따라 다릅니다.

4단계 웹 프록시가 투명 모드에서 구축된 경우 다음과 같이 설정을 편집합니다.

설정	설명
자격 증명 암호화	이 설정은 클라이언트가 암호화된 HTTPS 연결을 통해 웹 프록시에 로그인 자격 증명을 전송할지 여부를 지정합니다. 이 설정은 기본 및 NTLMSSP 인증 체계 모두에 적용되지만 사용자 자격 증명이 일반 텍스트로 전송되기 때문에 기본 인증 체계에 특히 유용합니다. 자세한 내용은 실패한 인증, 5-27페이지를 참고하십시오.

설정	설명
HTTPS 리디렉션 포트	HTTPS 연결을 통해 사용자를 인증하기 위해 요청을 리디렉션하는 데 사용할 TCP 포트를 지정합니다. 이 설정은 클라이언트가 HTTPS를 사용하여 웹 프록시에 대한 연결을 여는 포트를 지정합니다. 이는 자격 증명 암호화가 사용하도록 설정되거나 액세스 제어를 사용하고 사용자에게 인증 프롬프트가 표시되는 경우에 발생합니다.
리디렉션 호스트 이름	웹 프록시가 들어오는 연결을 수신 대기하는 네트워크 인터페이스의 간단한 호스트 이름을 입력합니다. 투명 모드에서 구축된 어플라이언스에서 인증을 구성하는 경우 웹 프록시가 사용자를 인증하기 위해 클라이언트에 전송된 리디렉션 URL에서 이 호스트 이름을 사용합니다. 다음 값 중 하나를 입력할 수 있습니다. • **단일 단어 호스트 이름.** 클라이언트 및 웹 보안 어플라이언스에서 DNS로 확인 가능한 단일 단어 호스트 이름을 입력할 수 있습니다. 이를 통해 클라이언트가 추가 브라우저 측 설정 없이 Internet Explorer에서 실제 단일 로그인을 수행할 수 있습니다. 클라이언트 및 웹 보안 어플라이언스에서 DNS로 확인 가능한 단일 단어 호스트 이름을 입력해야 합니다. 예를 들어, 클라이언트가 `mycompany.com` 도메인에 있고 웹 프록시가 수신 대기 중인 인터페이스의 전체 호스트 이름이 `proxy.mycompany.com`인 경우 이 필드에 `proxy`를 입력해야 합니다. 클라이언트가 `프록시`에 대한 조회를 수행하고 `proxy.mycompany.com`을 확인할 수 있어야 합니다. • **FQDN(Fully Qualified Domain Name).** 이 필드에 FQDN 또는 IP 주소를 입력할 수도 있습니다. 그러나 이를 수행하고 Internet Explorer 및 Firefox 브라우저에 대해 실제 단일 로그인을 원하는 경우 클라이언트 브라우저에서 FQDN 또는 IP 주소가 클라이언트의 신뢰할 수 있는 사이트 목록에 추가되었는지 확인해야 합니다. 기본값은 프록시 트래픽에 사용되는 인터페이스에 따라 M1 또는 P1 인터페이스의 FQDN입니다.
자격 증명 캐시 옵션: Surrogate 시간 초과	이 설정은 클라이언트에 인증 자격 증명을 다시 요청하기 전에 웹 프록시가 대기하는 시간을 지정합니다. 웹 프록시가 자격 증명을 다시 요청할 때까지 서로게이트(IP 주소 또는 쿠키)에 저장된 값을 사용합니다. 일반적으로 사용자 에이전트(예: 브라우저)에서 인증 자격 증명을 캐시하므로 매번 사용자에게 자격 증명을 입력하라는 프롬프트를 표시하지 않습니다.
자격 증명 캐시 옵션: 클라이언트 IP 유휴 제한 시간	IP 주소가 인증 서로게이트로 사용되는 경우, 이 설정은 클라이언트가 유휴 상태일 때 클라이언트에 인증 자격 증명을 다시 요청하기 전에 웹 프록시가 대기하는 시간을 지정합니다. 이 값이 서로게이트 시간 초과 값보다 큰 경우 이 설정은 적용되지 않으며 서로게이트 시간 초과에 도달한 후 클라이언트에 인증 프롬프트를 표시합니다. 이 설정을 사용하여 컴퓨터에서 나가는 사용자의 취약성을 줄일 수 있습니다.
자격 증명 캐시 옵션: 캐시 크기	인증 캐시에 저장되는 항목의 수를 지정합니다. 실제로 이 디바이스를 사용 중인 사용자의 수를 충분히 수용할 수 있도록 이 값을 설정합니다. 기본값은 권장 설정입니다.

설정	설명
사용자 세션 제한	이 설정은 인증된 사용자가 여러 IP 주소에서 동시에 인터넷에 액세스할 수 있는지 여부를 지정합니다. 사용자가 인증되지 않은 사용자와 인증 자격 증명을 공유하지 못하도록 한 대의 머신으로 액세스를 제한할 수 있습니다. 사용자가 다른 머신에서 로그인할 수 없는 경우 최종 사용자 알림 페이지가 표시됩니다. 사용자가 버튼을 클릭하여 이 페이지의 재인증 설정을 통해 다른 사용자 이름으로 로그인할 수 있는지 여부를 선택할 수 있습니다. 이 설정을 사용하도록 설정하는 경우 사용자가 다른 IP 주소로 머신에 로그인할 수 있을 때까지 대기해야 하는 시간을 결정하는 제한 시간 초과 값을 입력합니다. 제한 시간 초과 값은 서로게이트 시간 초과 값보다 커야 합니다. `authcache` CLI 명령을 사용하여 특정 사용자 또는 모든 사용자를 인증 캐시에서 제거할 수 있습니다.
고급	자격 증명 암호화 또는 액세스 제어를 사용할 경우 어플라이언스에서 어플라이언스와 함께 제공되는 디지털 인증서 및 키(Cisco Web Security Appliance 데모 인증서)를 사용할지 또는 여기서 업로드하는 디지털 인증서 및 키를 사용할지를 선택할 수 있습니다.

5단계 웹 프록시가 명시적 전달 모드에서 구축된 경우 다음과 같이 설정을 편집합니다.

설정	설명
자격 증명 암호화	이 설정은 클라이언트가 암호화된 HTTPS 연결을 통해 웹 프록시에 로그인 자격 증명을 전송할지 여부를 지정합니다. 자격 증명 암호화를 사용하도록 설정하려면 "HTTPS Redirect (Secure)(HTTPS 리디렉션(보안)"를 선택합니다. 자격 증명 암호화를 사용하도록 설정하는 경우 인증을 위해 클라이언트를 웹 프록시로 리디렉션하는 방법을 구성하기 위한 추가 필드가 표시됩니다. 이 설정은 기본 및 NTLMSSP 인증 체계 모두에 적용되지만 사용자 자격 증명이 일반 텍스트로 전송되기 때문에 기본 인증 체계에 특히 유용합니다. 자세한 내용은 실패한 인증, 5-27페이지를 참고하십시오.
HTTPS 리디렉션 포트	HTTPS 연결을 통해 사용자를 인증하기 위해 요청을 리디렉션하는 데 사용할 TCP 포트를 지정합니다. 이 설정은 클라이언트가 HTTPS를 사용하여 웹 프록시에 대한 연결을 여는 포트를 지정합니다. 이는 자격 증명 암호화가 사용하도록 설정되거나 액세스 제어를 사용하고 사용자에게 인증 프롬프트가 표시되는 경우에 발생합니다.

설정	설명
리디렉션 호스트 이름	웹 프록시가 들어오는 연결을 수신 대기하는 네트워크 인터페이스의 간단한 호스트 이름을 입력합니다. 위에서 인증 모드를 사용하도록 설정하는 경우 웹 프록시가 사용자를 인증하기 위해 클라이언트에 전송되는 리디렉션 URL에서 이 호스트 이름을 사용합니다. 다음 값 중 하나를 입력할 수 있습니다. • **단일 단어 호스트 이름.** 클라이언트 및 웹 보안 어플라이언스에서 DNS로 확인 가능한 단일 단어 호스트 이름을 입력할 수 있습니다. 이를 통해 클라이언트가 추가 브라우저 측 설정 없이 Internet Explorer에서 실제 단일 로그인을 수행할 수 있습니다. 클라이언트 및 웹 보안 어플라이언스에서 DNS로 확인 가능한 단일 단어 호스트 이름을 입력해야 합니다. 예를 들어, 클라이언트가 `mycompany.com` 도메인에 있고 웹 프록시가 수신 대기 중인 인터페이스의 전체 호스트 이름이 `proxy.mycompany.com`인 경우 이 필드에 `proxy`를 입력해야 합니다. 클라이언트가 `프록시`에 대한 조회를 수행하고 `proxy.mycompany.com`을 확인할 수 있어야 합니다. • **FQDN(Fully Qualified Domain Name).** 이 필드에 FQDN 또는 IP 주소를 입력할 수도 있습니다. 그러나 이를 수행하고 Internet Explorer 및 Firefox 브라우저에 대해 실제 단일 로그인을 원하는 경우 클라이언트 브라우저에서 FQDN 또는 IP 주소가 클라이언트의 신뢰할 수 있는 사이트 목록에 추가되었는지 확인해야 합니다. 기본값은 프록시 트래픽에 사용되는 인터페이스에 따라 M1 또는 P1 인터페이스의 FQDN입니다.
자격 증명 캐시 옵션: Surrogate 시간 초과	이 설정은 클라이언트에 인증 자격 증명을 다시 요청하기 전에 웹 프록시가 대기하는 시간을 지정합니다. 웹 프록시가 자격 증명을 다시 요청할 때까지 서로게이트(IP 주소 또는 쿠키)에 저장된 값을 사용합니다. 일반적으로 사용자 에이전트(예: 브라우저)에서 인증 자격 증명을 캐시하므로 매번 사용자에게 자격 증명을 입력하라는 프롬프트를 표시하지 않습니다.
자격 증명 캐시 옵션: 클라이언트 IP 유휴 제한 시간	IP 주소가 인증 서로게이트로 사용되는 경우, 이 설정은 클라이언트가 유휴 상태일 때 클라이언트에 인증 자격 증명을 다시 요청하기 전에 웹 프록시가 대기하는 시간을 지정합니다. 이 값이 서로게이트 시간 초과 값보다 큰 경우 이 설정은 적용되지 않으며 서로게이트 시간 초과에 도달한 후 클라이언트에 인증 프롬프트를 표시합니다. 이 설정을 사용하여 컴퓨터에서 나가는 사용자의 취약성을 줄일 수 있습니다.
자격 증명 캐시 옵션: 캐시 크기	인증 캐시에 저장되는 항목의 수를 지정합니다. 실제로 이 디바이스를 사용 중인 사용자의 수를 충분히 수용할 수 있도록 이 값을 설정합니다. 기본값은 권장 설정입니다.

설정	설명
사용자 세션 제한	이 설정은 인증된 사용자가 여러 IP 주소에서 동시에 인터넷에 액세스할 수 있는지 여부를 지정합니다. 사용자가 인증되지 않은 사용자와 인증 자격 증명을 공유하지 못하도록 한 대의 머신으로 액세스를 제한할 수 있습니다. 사용자가 다른 머신에서 로그인할 수 없는 경우 최종 사용자 알림 페이지가 표시됩니다. 사용자가 버튼을 클릭하여 이 페이지의 재인증 설정을 통해 다른 사용자 이름으로 로그인할 수 있는지 여부를 선택할 수 있습니다. 이 설정을 사용하도록 설정하는 경우 사용자가 다른 IP 주소로 머신에 로그인할 수 있을 때까지 대기해야 하는 시간을 결정하는 제한 시간 초과 값을 입력합니다. 제한 시간 초과 값은 서로게이트 시간 초과 값보다 커야 합니다. `authcache` CLI 명령을 사용하여 특정 사용자 또는 모든 사용자를 인증 캐시에서 제거할 수 있습니다.
고급	자격 증명 암호화 또는 액세스 제어를 사용할 경우 어플라이언스에서 어플라이언스와 함께 제공되는 디지털 인증서 및 키(Cisco Web Security Appliance 데모 인증서)를 사용할지 또는 여기서 업로드하는 디지털 인증서 및 키를 사용할지를 선택할 수 있습니다. 디지털 인증서 및 키를 업로드하려면 **Browse(찾아보기)**를 클릭하고 로컬 머신의 필요한 파일로 이동합니다. 원하는 파일을 선택한 후 **Upload Files(파일 업로드)**를 클릭합니다.

6단계 변경 사항을 제출 및 커밋합니다.

인증 시퀀스

- 인증 시퀀스 정보, 5-25페이지
- 인증 시퀀스 생성, 5-26페이지
- 인증 시퀀스 편집 및 다시 정렬, 5-27페이지
- 인증 시퀀스 편집 및 다시 정렬, 5-27페이지

인증 시퀀스 정보

인증 시퀀스를 사용하면 단일 ID로 여러 인증 서버나 프로토콜을 통해 사용자를 인증할 수 있습니다. 또한 인증 시퀀스는 기본 인증 옵션이 사용 불가능한 경우 백업 옵션을 제공하는 데 유용합니다.

인증 시퀀스는 둘 이상의 인증 영역 컬렉션입니다. 사용된 영역에 여러 인증 서버와 여러 인증 프로토콜이 있을 수 있습니다. 인증 영역에 대한 자세한 내용은 인증 영역, 5-10페이지를 참조하십시오.

두 번째 인증 영역을 생성한 후 어플라이언스가 자동으로 Network(네트워크) > Authentication(인증) 아래에 Realm Sequences(영역 시퀀스) 섹션을 표시하고 All Realms(모든 영역)라는 기본 인증 시퀀스를 포함합니다. All Realms(모든 영역) 시퀀스는 사용자가 정의하는 각 영역을 자동으로 포함합니다. All Realms(모든 영역) 시퀀스 내의 영역의 순서를 변경할 수 있지만 All Realms(모든 영역) 시퀀스를 삭제하거나 이 시퀀스에서 영역을 제거할 수는 없습니다.

여러 NTLM 인증 영역이 정의된 경우 웹 보안 어플라이언스에서는 시퀀스당 하나의 NTLM 인증 영역만 포함하는 NTLMSSP 인증 체계를 사용합니다. All Realms(모든 영역) 시퀀스를 포함하여 각 시퀀스 내의 NTLMSSP에 사용할 NTLM 인증 영역을 선택할 수 있습니다. 여러 NTLM 영역이 포함된 NTLMSSP를 사용하려면 각 영역에 대한 별도의 식별 프로필을 정의합니다.

인증 중에 시퀀스 내의 어떤 인증 영역이 사용되는지는 다음에 따라 결정됩니다.

- 사용되는 인증 체계. 일반적으로 클라이언트에서 입력한 자격 증명의 유형에 따라 지정됩니다.
- 영역이 시퀀스 내에 나열된 순서(하나의 NTLMSSP 영역만 가능하므로 기본 영역에만 해당).

정보 최적의 성능을 위해 동일한 서브넷의 클라이언트는 단일 영역을 사용하여 인증합니다.

인증 시퀀스 생성

시작하기 전에

- 둘 이상의 인증 영역을 생성합니다(인증 영역, 5-10페이지 참조).
- 웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 여러 웹 보안 어플라이언스에 있는 동일한 이름의 인증 영역에서 각 어플라이언스에 동일한 속성이 정의되었는지 확인합니다. AsyncOS는 영역을 사용하여 목록에 있는 첫 번째 영역부터 순차적으로 인증을 처리합니다.

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Add Sequence(시퀀스 추가)**를 클릭합니다.

3단계 영숫자 및 공백 문자를 사용하여 시퀀스의 고유한 이름을 입력합니다.

4단계 Realm Sequence for Basic Scheme(기본 체계에 대한 영역 시퀀스) 영역의 첫 번째 행에서 시퀀스에 포함할 첫 번째 인증 영역을 선택합니다.

5단계 Realm Sequence for Basic Scheme(기본 체계에 대한 영역 시퀀스) 영역의 두 번째 행에서 시퀀스에 포함할 다음 영역을 선택합니다.

6단계 (선택 사항) 기본 자격 증명을 사용하는 다른 영역을 포함하려면 **Add Row(행 추가)**를 클릭합니다.

7단계 NTLM 영역이 정의되면 Realm for NTLMSSP Scheme(NTLMSSP 체계에 대한 영역) 필드에서 NTLM 영역을 선택합니다.

클라이언트가 NTLMSSP 인증 자격 증명을 전송할 때 웹 프록시에서 이 NTLM 영역을 사용합니다.

8단계 변경 사항을 제출 및 커밋합니다.

인증 시퀀스 편집 및 다시 정렬

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 편집하거나 다시 정렬할 시퀀스의 이름을 클릭합니다.

3단계 영역이 시퀀스에서 차지할 위치 번호에 해당하는 행의 Realms(영역) 드롭다운 목록에서 영역 이름을 선택합니다.

참고 All Realms(모든 영역) 시퀀스의 경우 해당 영역의 순서만 변경할 수 있으며 영역 자체를 변경할 수는 없습니다. All Realms(모든 영역) 시퀀스 내의 영역 순서를 변경하려면 Order(순서) 열의 화살표를 클릭하여 해당 영역을 재배치합니다.

4단계 필요에 따라 모든 영역이 나열되고 정렬될 때까지 3단계를 반복하여 각 영역 이름이 한 행에만 표시되도록 합니다.

5단계 변경 사항을 제출 및 커밋합니다.

인증 시퀀스 삭제

시작하기 전에

- 인증 시퀀스를 삭제하면 연결된 ID가 사용되지 않도록 설정되고, 이후 해당 ID가 연결된 정책에서 제거됩니다.

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 시퀀스 이름에 대한 휴지통 아이콘을 클릭합니다.

3단계 **Delete(삭제)**를 클릭하여 시퀀스를 삭제할 것임을 확인합니다.

4단계 변경 사항을 커밋합니다.

실패한 인증

- 실패한 인증 정보, 5-28페이지
- 문제가 되는 사용자 에이전트에 대한 인증 우회, 5-28페이지
- 인증 우회, 5-30페이지
- 인증 서비스가 사용 불가능한 동안 인증되지 않은 트래픽 허용, 5-30페이지
- 인증 실패 후 게스트 액세스 권한 부여, 5-31페이지
- 권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용, 5-32페이지

실패한 인증 정보

다음과 같은 이유로 인증에 실패하여 사용자가 웹에서 차단될 수 있습니다.

- **클라이언트/사용자 에이전트 제한.** 일부 클라이언트 애플리케이션이 인증을 적절히 지원하지 않을 수 있습니다. 권한 부여가 필요하지 않은 식별 프로필을 구성하고 클라이언트를 기반으로(선택적으로, 액세스해야 하는 URL을 기반으로) 해당 기준을 지정하여 이러한 클라이언트에 대한 인증을 우회할 수 있습니다.
- **인증 서비스가 사용 불가능함.** 네트워크 또는 서버 문제로 인해 인증 서비스가 사용 불가능할 수 있습니다. 이 경우에 인증되지 않은 트래픽을 허용하도록 선택할 수 있습니다.
- **유효하지 않은 자격 증명.** 일부 사용자는 적절한 인증을 위해 유효한 자격 증명을 제공하지 못할 수 있습니다(예: 자격 증명을 대기 중인 사용자 또는 방문자). 이러한 사용자에게 웹에 대한 제한된 액세스 권한을 부여하도록 선택할 수 있습니다.

관련 주제

- 문제가 되는 사용자 에이전트에 대한 인증 우회, 5-28페이지
- 인증 우회, 5-30페이지
- 인증 서비스가 사용 불가능한 동안 인증되지 않은 트래픽 허용, 5-30페이지
- 인증 실패 후 게스트 액세스 권한 부여, 5-31페이지

문제가 되는 사용자 에이전트에 대한 인증 우회

일부 사용자 에이전트에는 정상적인 작업에 영향을 미칠 수 있는 인증 문제가 있는 것으로 알려져 있습니다.

다음 사용자 에이전트를 통해 인증을 우회해야 합니다.

- Windows-Update-Agent
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft-CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Google Update

참고 액세스 정책이 계속 필터링되고(URL 카테고리 기반) 액세스 정책 설정에 따라 트래픽을 스캐닝합니다(McAfee, Webroot).

1단계 지정된 사용자 에이전트에 대한 인증을 우회하도록 식별 프로필을 구성합니다.

a. **Web Security Manager(웹 보안 관리자) > Identification Profile(식별 프로필)**을 선택합니다.

b. **Add Identification Profile(식별 프로필 추가)**을 클릭합니다.

c. 다음 정보를 입력합니다.

옵션	값
이름	사용자 에이전트 AuthExempt 식별 프로필
위에 삽입	처리 순서에서 첫 번째 프로필로 설정합니다.
서브넷별 구성원 정의	비워 둡니다.
인증별 구성원 정의	인증이 필요하지 않습니다.

d. **Advanced(고급) > User Agents(사용자 에이전트)**를 클릭합니다.

e. **None Selected(선택된 항목 없음)**를 클릭합니다.

f. 맞춤형 사용자 에이전트 아래에 문제가 되는 사용자 에이전트 문자열을 지정합니다.

2단계 액세스 정책을 구성합니다.

a. **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

b. **Add Policy(정책 추가)**를 클릭합니다.

c. 다음 정보를 입력합니다.

옵션	값
정책 이름	사용자 에이전트에 대한 인증 제외
정책 위에 삽입	처리 순서에서 첫 번째 정책으로 설정합니다.
식별 프로필 정책	사용자 에이전트 AuthExempt 식별 프로필
고급	None

3단계 변경 사항을 제출 및 커밋합니다.

인증 우회

단계	추가 정보
1. 고급 속성을 구성하여 영향을 받는 웹 사이트를 포함하는 맞춤형 URL 카테고리를 생성합니다.	
2. 다음 특성을 가지는 식별 프로필을 생성합니다. – 인증이 필요한 모든 ID 위에 배치됩니다. – 맞춤형 URL 카테고리를 포함합니다. – 영향을 받는 클라이언트 애플리케이션을 포함합니다. – 인증이 필요하지 않습니다.	사용자 및 클라이언트 소프트웨어 분류, 6-3페이지
3. 식별 프로필에 대한 정책을 생성합니다.	정책 생성, 10-5페이지

관련 주제

- 웹 프록시 우회

인증 서비스가 사용 불가능한 동안 인증되지 않은 트래픽 허용

참고 이 컨피그레이션은 인증 서비스가 사용 불가능한 경우에만 적용됩니다. 영구적으로 인증을 우회하지는 않습니다. 대체 옵션은 실패한 인증 정보, 5-28페이지를 참조하십시오.

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

3단계 Action If Authentication Service Unavailable(인증 서비스가 사용 불가능한 경우의 조치) 필드에서 **Permit Traffic To Proceed Without Authentication(트래픽을 인증 없이 처리하도록 허용)**을 클릭합니다.

4단계 변경 사항을 제출 및 커밋합니다.

인증 실패 후 게스트 액세스 권한 부여

게스트 액세스 권한을 부여하려면 다음 절차를 완료해야 합니다.

1. 게스트 액세스를 지원하는 식별 프로필 정의, 5-31페이지
2. 정책에서 게스트 액세스를 지원하는 식별 프로필 사용, 5-31페이지
3. (선택사항) 게스트 사용자 세부 정보가 기록되는 방식 구성, 5-32페이지

참고 식별 프로필에서 게스트 액세스를 허용하고 식별 프로필을 사용하는 사용자 정의 정책이 없는 경우, 인증에 실패한 사용자는 적용 가능한 정책 유형의 전역 정책과 일치됩니다. 예를 들어, MyIdentificationProfile이 게스트 액세스를 허용하고 MyIdentificationProfile을 사용하는 사용자 정의 액세스 정책이 없는 경우 인증에 실패한 사용자는 전역 액세스 정책과 일치됩니다. 게스트 사용자를 전역 정책과 일치시키지 않으려면 게스트 사용자에게 적용되고 모든 액세스를 차단하는 정책을 전역 정책 위에 생성합니다.

게스트 액세스를 지원하는 식별 프로필 정의

1단계 **Web Security Manager(웹 보안 관리자) > Identification Profiles(식별 프로필)**를 선택합니다.

2단계 **Add Identification Profile(식별 프로필 추가)**을 클릭하여 새 ID를 추가하거나 사용할 기존 ID의 이름을 클릭합니다.

3단계 **Support Guest Privileges(게스트 권한 지원)** 확인란을 선택합니다.

4단계 변경 사항을 제출 및 커밋합니다.

정책에서 게스트 액세스를 지원하는 식별 프로필 사용

1단계 Web Security Manager(웹 보안 관리자) 메뉴에서 정책 유형을 선택합니다.

2단계 정책 테이블에서 정책 이름을 클릭합니다.

3단계 Identification Profiles And Users(식별 프로필 및 사용자) 드롭다운 목록에서 **Select One Or More Identification Profiles(하나 이상의 식별 프로필 선택)**를 선택합니다(아직 선택하지 않은 경우).

4단계 Identification Profile(식별 프로필) 열의 드롭다운 목록에서 게스트 액세스를 지원하는 **프로필**을 선택합니다.

5단계 **Guests (Users Failing Authentication)(게스트(인증에 실패한 사용자))** 라디오 버튼을 클릭합니다.

참고 이 옵션이 사용 불가능한 경우 선택한 **프로필**이 게스트 액세스를 지원하도록 구성되지 않았음을 의미합니다. 4단계단계로 돌아가서 다른 프로필을 선택하거나 게스트 액세스를 지원하는 식별 프로필 정의, 5-31페이지를 참조하여 새 프로필을 정의합니다.

6단계 변경 사항을 제출 및 커밋합니다.

게스트 사용자 세부 정보가 기록되는 방식 구성

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

3단계 아래 설명된 대로 Failed Authentication Handling(실패한 인증 처리) 필드에서 Log Guest User By(게스트 사용자 로그 기준) 라디오 버튼을 클릭합니다.

라디오 버튼	설명
IP 주소	게스트 사용자의 클라이언트 IP 주소가 액세스 로그에 기록됩니다.
최종 사용자가 입력한 사용자 이름	원래 인증에 실패한 사용자 이름이 액세스 로그에 기록됩니다.

4단계 변경 사항을 제출 및 커밋합니다.

권한 부여 실패: 다른 자격 증명을 사용한 재인증 허용

- 다른 자격 증명을 사용한 재인증 허용 정보, 5-32페이지
- 다른 자격 증명을 사용한 재인증 허용, 5-32페이지

다른 자격 증명을 사용한 재인증 허용 정보

재인증을 사용하면 이전에 사용한 자격 증명이 권한 부여에 실패한 경우 사용자가 다른 자격 증명을 사용하여 다시 인증할 수 있습니다. 사용자가 성공적으로 인증할 수 있지만, 이를 수행하도록 권한이 부여되지 않은 경우에는 여전히 웹 리소스에 액세스하지 못합니다. 인증은 확인된 자격 증명을 정책에 전달할 목적으로 단순히 사용자를 식별하는 것이지만 권한 부여는 해당 사용자가 리소스에 액세스할 수 있도록(또는 액세스할 수 없도록) 권한을 부여하는 정책이기 때문입니다.

재인증이 허용되려면 사용자가 성공적으로 인증되어야 합니다.

- 사용자 정의된 최종 사용자 알림 페이지를 통해 재인증 기능을 사용하려면 리디렉션 URL을 구문 분석하는 CGI 스크립트가 Reauth_URL 매개변수를 구문 분석하고 사용해야 합니다.

다른 자격 증명을 사용한 재인증 허용

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

3단계 **Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction(최종 사용자가 URL 카테고리 또는 사용자 세션 제한으로 인해 차단된 경우 재인증 프롬프트)** 확인란을 선택합니다.

4단계 **Submit(제출)**를 클릭합니다.

식별된 사용자 추적

참고 어플라이언스가 쿠키 기반 인증 서로게이트를 사용하도록 구성된 경우 클라이언트에서 HTTPS 및 FTP over HTTP 요청에 대한 쿠키 정보를 가져오지 않습니다. 따라서 쿠키에서 사용자 이름을 가져올 수 없습니다.

명시적 요청에 대해 지원되는 인증 서로게이트

서로게이트 유형	자격 증명 암호화가 사용되지 않음			자격 증명 암호화가 사용됨		
Protocol:	**HTTP**	**HTTPS 및 HTTP 상의 FTP**	**네이티브 FTP**	**HTTP**	**HTTPS 및 HTTP 상의 FTP**	**네이티브 FTP**
서로게이트 없음	예	예	예	해당 없음	해당 없음	해당 없음
IP 기반	예	예	예	예	예	예
쿠키 기반	예	예***	예***	예	아니요/예**	예***

투명 요청에 대해 지원되는 인증 서로게이트

참고 사용자 및 클라이언트 소프트웨어 분류, 6-3페이지에서 인증 서로게이트 옵션에 대한 설명을 참조하십시오.

서로게이트 유형	자격 증명 암호화가 사용되지 않음			자격 증명 암호화가 사용됨		
Protocol:	**HTTP**	**HTTPS**	**네이티브 FTP**	**HTTP**	**HTTPS**	**네이티브 FTP**
서로게이트 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
IP 기반	예	아니요/예*	아니요/예*	예	아니요/예*	아니요/예*
쿠키 기반	예	아니요/예**	아니요/예**	예	아니요/예**	아니요/예**

* 클라이언트가 HTTP 사이트에 대한 요청을 작성하고 인증된 후 작동합니다. 발생하기 전의 동작은 트랜잭션 유형에 따라 다릅니다.

- **네이티브 FTP 트랜잭션.** 트랜잭션이 인증을 우회합니다.
- **HTTPS 트랜잭션.** 트랜잭션이 삭제됩니다. 그러나 인증 목적으로 첫 번째 HTTPS 요청의 암호를 해독하도록 HTTPS 프록시를 구성할 수 있습니다.

** 쿠키 기반 인증이 사용되는 경우 웹 프록시가 HTTPS, 네이티브 FTP 및 FTP over HTTP 트랜잭션을 위해 사용자를 인증할 수 없습니다. 이 제한으로 인해 모든 HTTPS, 네이티브 FTP 및 FTP over HTTP 요청이 인증을 우회하므로 인증이 요청되지 않습니다.

*** 쿠키 기반 서로게이트가 구성된 경우에도 이 경우에는 서로게이트가 사용되지 않습니다.

관련 주제

- 식별 프로필 및 인증, 6-8페이지

재인증된 사용자 추적

재인증을 사용하면 더 많은 권한이 있는 사용자가 인증되고 권한이 부여되는 경우 웹 프록시에서 구성된 인증 서로게이트에 따라 다른 시간 동안 이 사용자 ID를 캐시합니다.

- **세션 쿠키.** 권한 있는 사용자 ID는 브라우저가 닫히거나 세션이 시간 초과될 때까지 사용됩니다.
- **영구 쿠키.** 권한 있는 사용자 ID는 서로게이트가 시간 초과될 때까지 사용됩니다.
- **IP 주소.** 권한 있는 사용자 ID는 서로게이트가 시간 초과될 때까지 사용됩니다.
- **서로게이트 없음.** 기본적으로 웹 프록시는 새 연결마다 인증을 요청하지만 재인증이 사용하도록 설정된 경우에는 웹 프록시가 새 요청마다 인증을 요청하므로 NTLMSSP 사용 시 인증 서버의 로드가 증가합니다. 그러나 대부분의 브라우저는 브라우저가 닫힐 때까지 권한 있는 사용자 자격 증명을 캐시하고 프롬프트를 표시하지 않은 상태로 인증하기 때문에 인증 활동의 증가가 사용자에게 명백하게 나타나지 않을 수 있습니다. 또한 웹 프록시가 투명 모드에서 구축되고 "명시적 전달 요청에 동일한 서로게이트 설정 적용" 옵션이 사용하도록 설정되지 않은 경우 명시적 전달 요청에 대한 인증 서로게이트가 사용되지 않으며 재인증으로 인해 로드가 증가합니다.

참고 웹 보안 어플라이언스에서 쿠키를 인증 서로게이트로 사용하는 경우 Cisco에서는 자격 증명 암호화를 사용하도록 설정하는 것을 권장합니다.

자격 증명

사용자에게 브라우저 또는 다른 클라이언트 애플리케이션을 통해 자격 증명을 입력하라는 프롬프트를 표시하거나 다른 소스에서 투명하게 자격 증명을 가져와서 사용자로부터 인증 자격 증명을 가져옵니다.

- 세션 중에 재사용할 자격 증명 추적, 5-34페이지
- 인증 및 권한 부여 실패, 5-35페이지
- 자격 증명 형식, 5-35페이지
- 기본 인증을 위한 자격 증명 암호화, 5-35페이지

세션 중에 재사용할 자격 증명 추적

인증 서로게이트를 사용하면 사용자가 세션 중에 한 번 인증한 후 새 요청마다 사용자가 인증하도록 하지 않고 해당 세션 전체에서 재사용할 자격 증명을 추적할 수 있습니다. 인증 서로게이트는 사용자 워크스테이션의 IP 주소 또는 세션에 할당된 쿠키를 기반으로 할 수 있습니다.

Internet Explorer의 경우 리디렉션 호스트 이름은 정규화된 도메인이 아니라 간단한 호스트 이름(점을 포함하지 않음) 또는 NetBIOS 이름이어야 합니다. 또는 Internet Explorer의 로컬 인트라넷 영역에 어플라이언스 호스트 이름을 추가할 수 있지만(Tools(도구) > Internet options(인터넷 옵션) > Security(보안) 탭) 모든 클라이언트에서 이를 수행해야 합니다. 이에 대한 자세한 내용은 How do I properly set up NTLM with SSO (credentials sent transparently)?를 참조하십시오.

Firefox 및 기타 비Microsoft 브라우저의 경우 **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** 및 **network.automatic-ntlm-auth.trusted-uris** 매개변수를 투명 모드 리디렉션 호스트 이름으로 설정해야 합니다. Firefox is not sending authentication credentials transparently (SSO)를 참조할 수도 있습니다. 이 자료에서는 Firefox 매개변수 변경에 대한 일반 정보를 제공합니다.

리디렉션 호스트 이름에 대한 자세한 내용은 전역 인증 설정 구성 또는 CLI 명령 sethostname을 참조하십시오.

인증 및 권한 부여 실패

호환되지 않는 클라이언트 애플리케이션과 같이 일반적으로 인정된 이유로 인증에 실패하는 경우 게스트 액세스 권한을 부여할 수 있습니다.

인증에 성공했지만 권한 부여에는 실패한 경우 요청된 리소스에 액세스할 권한이 있는 다른 자격 증명 집합을 사용하여 재인증을 허용할 수 있습니다.

관련 주제

- 인증 실패 후 게스트 액세스 권한 부여, 5-31페이지
- 다른 자격 증명을 사용한 재인증 허용, 5-32페이지

자격 증명 형식

인증 체계	자격 증명 형식
NTLMSSP	`MyDomain\jsmith`

기본	`jsmith`
	`MyDomain\jsmith`
	참고 사용자가 Windows 도메인을 입력하지 않으면 웹 프록시에서 기본 Windows 도메인을 앞에 추가합니다.

기본 인증을 위한 자격 증명 암호화

기본 인증을 위한 자격 증명 암호화 정보

암호화된 양식으로 HTTPS를 통해 자격 증명을 전송하도록 자격 증명 암호화를 사용하도록 설정합니다. 이렇게 하면 기본 인증 프로세스의 보안이 향상됩니다.

웹 보안 어플라이언스는 기본적으로 고유한 인증서 및 개인 키를 사용하여 보안 인증을 위해 클라이언트와의 HTTPS 연결을 생성합니다. 그러나 대부분의 브라우저에서는 이 인증서가 유효하지 않다고 사용자에게 경고합니다. 사용자가 유효하지 않은 인증서 메시지를 보지 못하도록 사용자 조직에서 사용하는 유효한 인증서 및 키 쌍을 업로드할 수 있습니다.

자격 증명 암호화 구성

시작하기 전에

- IP 서로게이트를 사용하도록 어플라이언스를 구성합니다.
- (선택 사항) 인증서 및 암호화되지 않은 개인 키를 확보합니다. 여기에서 구성된 인증서와 키는 액세스 제어에서도 사용됩니다.

1단계 **Network(네트워크) > Authentication(인증)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

3단계 Credential Encryption(자격 증명 암호화) 필드에서 **Use Encrypted HTTPS Connection For Authentication(인증을 위해 암호화된 HTTPS 연결 사용)** 확인란을 선택합니다.

4단계 (선택 사항) 인증 중에 HTTPS Redirect Port(HTTPS 리디렉션 포트) 필드에서 클라이언트 HTTP 연결에 대한 기본 포트 번호(443)를 편집합니다.

5단계 (선택 사항) 인증서 및 키를 업로드합니다.

a. Advanced(고급) 섹션을 확장합니다.

b. Certificate(인증서) 필드에서 **Browse(찾아보기)**를 클릭하여 업로드할 인증서 파일을 찾습니다.

c. Key(키) 필드에서 **Browse(찾아보기)**를 클릭하여 업로드할 개인 키 파일을 찾습니다.

d. **Upload Files(파일 업로드)**를 클릭합니다.

6단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 인증서 관리, 22-24페이지.

인증 트러블슈팅

- NTLMSSP로 인해 LDAP 사용자가 인증에 실패함, A-3페이지
- LDAP 참조로 인해 LDAP 인증 실패, A-3페이지
- 기본 인증 실패, A-3페이지
- 사용자에게 자격 증명 프롬프트가 잘못 표시됨, A-4페이지
- HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨, A-15페이지
- 인증을 지원하지 않는 URL에 액세스할 수 없음, A-20페이지
- 업스트림 프록시에서 클라이언트 요청 실패, A-21페이지

6장 최종 사용자 및 클라이언트 소프트웨어 분류

- 사용자 및 클라이언트 소프트웨어 분류 개요, 6-1페이지
- 사용자 및 클라이언트 소프트웨어 분류: 모범 사례, 6-2페이지
- 식별 프로필 기준, 6-2페이지
- 사용자 및 클라이언트 소프트웨어 분류, 6-3페이지
- 식별 프로필 및 인증, 6-8페이지
- 식별 프로필 트러블슈팅, 6-10페이지

사용자 및 클라이언트 소프트웨어 분류 개요

식별 프로필을 사용하여 다음과 같은 목적으로 사용자 및 사용자 에이전트(클라이언트 소프트웨어)를 분류할 수 있습니다.

- 정책 애플리케이션(SaaS 제외)
- 식별 및 인증 요건의 사양

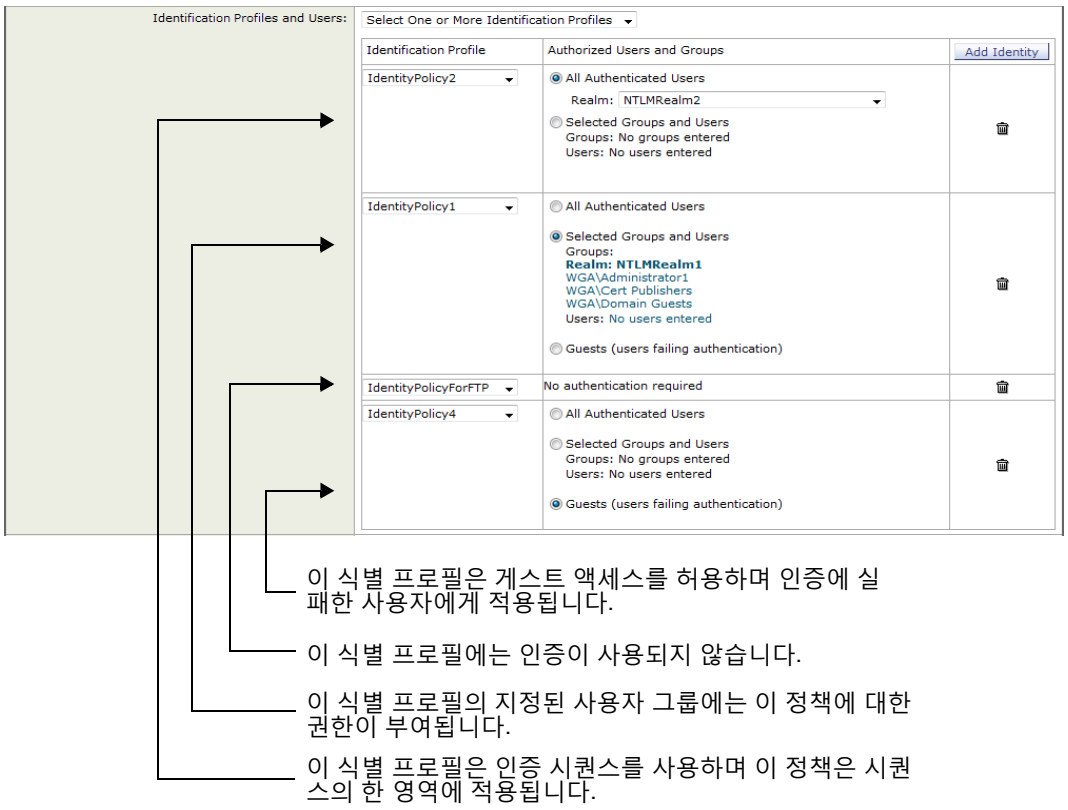
AsyncOS에서는 모든 트랜잭션에 식별 프로필을 할당합니다.

- 맞춤형 식별 프로필 - AsyncOS에서는 해당 ID의 기준에 따라 맞춤형 프로필을 할당합니다.
- 전역 식별 프로필 - AsyncOS가 맞춤형 프로필의 기준을 충족하지 않는 트랜잭션에 전역 프로필을 할당합니다. 기본적으로 전역 프로필에는 인증이 필요하지 않습니다.

AsyncOS에서는 첫 번째 ID부터 순차적으로 식별 프로필을 처리합니다. 전역 프로필이 마지막 프로필입니다.

식별 프로필에는 하나의 기준만 포함할 수 있습니다. 또는 여러 기준을 포함하는 프로필에서는 모든 기준이 충족되어야 합니다.

하나의 정책으로 여러 식별 프로필을 호출할 수 있습니다.



사용자 및 클라이언트 소프트웨어 분류: 모범 사례

- 모든 사용자에게 적용되거나 더 적은 수의 큰 사용자 그룹에 적용되는 일반적인 ID 프로필을 더 적은 수로 생성합니다. 더 세부적으로 관리하려면 프로필 대신 정책을 사용하십시오.
- 고유 기준을 포함하는 식별 프로필을 생성합니다.
- 투명 모드에서 구축된 경우 인증을 지원하지 않는 사이트에 대한 식별 프로필을 생성합니다. 인증 우회, 5-30페이지를 참조하십시오.

식별 프로필 기준

옵션	설명
서브넷	클라이언트 서브넷이 정책의 서브넷 목록과 일치해야 합니다.
프로토콜	트랜잭션에서 사용되는 프로토콜(HTTP, HTTPS, SOCKS 또는 네이티브 FTP)입니다.
포트	요청의 프록시 포트가 식별 프로필의 포트 목록에 있어야 합니다(나열된 항목이 있는 경우). 명시적 전달 연결의 경우에는 브라우저에 구성된 포트입니다. 투명한 연결의 경우에는 목적지 포트와 동일합니다.

옵션	설명
사용자 에이전트	요청하는 사용자 에이전트(클라이언트 소프트웨어)가 식별 프로필의 사용자 에이전트 목록에 있어야 합니다(나열된 항목이 있는 경우). 일부 사용자 에이전트는 인증을 처리할 수 없으므로 인증이 필요하지 않은 프로필을 생성해야 합니다.
URL Category (URL 범주)	요청 URL의 URL 카테고리가 식별 프로필의 URL 카테고리 목록에 있어야 합니다(나열된 항목이 있는 경우).
인증 요건	식별 프로필에 인증이 필요한 경우 클라이언트 인증 자격 증명이 식별 프로필의 인증 요건과 일치해야 합니다.

사용자 및 클라이언트 소프트웨어 분류

시작하기 전에

- 인증 영역을 생성합니다. Active Directory 인증 영역(NTLMSSP 및 기본)을 생성하는 방법, 5-13페이지 또는 LDAP 인증 영역 생성, 5-15페이지를 참조하십시오.
- 식별 프로필에 변경 사항을 커밋하는 경우에는 최종 사용자를 다시 인증해야 합니다.
- Cloud Connector 모드인 경우 추가 식별 프로필 옵션인 머신 ID를 사용할 수 있습니다. 정책 적용을 위한 머신 식별, 3-8페이지를 참조하십시오.
- (선택 사항) 인증 시퀀스를 생성합니다. 인증 시퀀스 생성, 5-26페이지를 참고하십시오.
- (선택 사항) 식별 프로필에 모바일 사용자가 포함될 경우 보안 모빌리티를 사용하도록 설정합니다.
- (선택 사항) 인증 서로게이트를 이해합니다. 식별된 사용자 추적, 5-33페이지를 참조하십시오.

1단계 **Web Security Manager(웹 보안 관리자) > Identification Profiles(식별 프로필)**를 선택합니다.

2단계 프로필을 추가하려면 **Add Profile(프로필 추가)**을 클릭합니다.

3단계 이 프로필을 사용하도록 설정하거나 삭제하지 않고 빠르게 사용하지 않도록 설정하려면 **Enable Identification Profile(식별 프로필 사용)** 확인란을 사용합니다.

4단계 고유한 프로필 **Name(이름)**을 지정합니다.

5단계 **Description(설명)**은 선택 사항입니다.

6단계 **Insert Above(위에 삽입)** 드롭다운 목록에서 이 프로필이 표시될 표의 위치를 선택합니다.

참고 인증이 필요한 첫 번째 식별 프로필 위에 인증이 필요하지 않은 식별 프로필을 배치합니다.

7단계 **User Identification Method(사용자 식별 방법)** 섹션에서 식별 방법을 선택한 후 관련 매개변수를 제공합니다. 표시되는 옵션은 선택한 방법에 따라 다릅니다.

인증/식별에서 제외, 사용자 인증 및 사용자를 식별하는 세 가지 방법(ISE, ASA(AnyConnect Secure Mobility를 통해) 또는 적절하게 구성된 인증 영역) 등 세 가지 유형의 방법이 있습니다. 마지막 방법에는 Active Directory 영역 또는 Novell eDirectory로 구성된 LDAP 영역이 포함됩니다.

a. **User Identification Method(사용자 식별 방법)**드롭다운 목록에서 식별 방법을 선택합니다.

옵션	설명
인증/식별에서 제외	기본적으로 IP 주소로 사용자를 식별합니다. 추가 매개변수가 필요하지 않습니다.
사용자 인증	사용자가 입력하는 인증 자격 증명으로 사용자를 식별합니다.
ISE로 투명하게 사용자 식별	ISE 서비스가 사용하도록 설정된 경우(Network(네트워크) > ISE(Identity Services Engine)) 사용할 수 있습니다. 이러한 트랜잭션의 경우 ISE(Identity Services Engine)에서 사용자 이름 및 연결된 SGT(Secure Group Tag)를 가져옵니다. 자세한 내용은 ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지를 참고하십시오.
ASA로 투명하게 사용자 식별	Cisco Adaptive Security Appliance에서 받은 현재 IP 주소-사용자 이름 매핑으로 사용자를 식별합니다(원격 사용자만 해당). 이 옵션은 보안 모빌리티가 사용하도록 설정되고 ASA와 통합된 경우에 표시됩니다. 사용자 이름은 ASA에서 가져오고 연결된 디렉토리 그룹은 선택한 인증 영역 또는 시퀀스에서 가져옵니다.
인증 영역으로 투명하게 사용자 식별	하나 이상의 인증 영역이 투명 식별을 지원하도록 구성된 경우 이 옵션을 사용할 수 있습니다.

참고 인증 또는 투명 식별을 사용하는 하나 이상의 식별 프로필이 구성된 경우 정책 테이블이 사용자 이름, 디렉토리 그룹 및 SGT(Secure Group Tag)를 사용하여 정책 구성원 자격을 정의하도록 지원합니다.

b. 선택한 방법에 적합한 매개변수를 제공합니다. 이 표에 설명된 모든 섹션이 각 선택 항목에 표시되지는 않습니다.

Fallback to Authentication Realm or Guest Privileges	사용자 인증이 ISE에서 제공되지 않는 경우: • **게스트 권한 지원** – 트랜잭션이 계속될 수 있으며 모든 식별 프로필에서 게스트 사용자에 대한 후속 정책을 일치시킵니다. • **트랜잭션 차단** – ISE로 식별될 수 없는 사용자에 대한 인터넷 액세스를 허용하지 않습니다. • **게스트 권한 지원** – 유효하지 않은 자격 증명으로 인해 인증에 실패한 사용자에게 게스트 액세스 권한을 부여하려면 이 확인란을 선택합니다.

인증 영역	**영역 또는 시퀀스 선택** – 정의된 인증 영역 또는 시퀀스를 선택합니다. **체계 선택** – 인증 체계를 선택합니다. • **Kerberos** – 클라이언트가 Kerberos 티켓을 사용하여 투명하게 인증됩니다. • **기본** – 클라이언트가 항상 사용자에게 자격 증명에 대한 프롬프트를 표시합니다. 사용자가 자격 증명을 입력하면 일반적으로 브라우저에서 제공된 자격 증명을 기억할지 묻는 확인란을 제공합니다. 사용자가 브라우저를 열 때마다 클라이언트가 자격 증명에 대한 프롬프트를 표시하고 이전에 저장된 자격 증명을 다시 전송합니다. 자격 증명은 안전하지 않은 상태의 일반 텍스트(Base64)로 전송됩니다. 클라이언트와 Web Security Appliance 간의 패킷 캡처에 사용자 이름 및 암호가 표시될 수 있습니다. • **NTLMSSP** – 클라이언트가 해당 Windows 로그인 자격 증명을 사용하여 투명하게 인증합니다. 사용자에게 자격 증명에 대한 프롬프트를 표시하지 않습니다. 그러나 다음 상황에서는 클라이언트가 사용자에게 자격 증명에 대한 프롬프트를 표시합니다. – Windows 자격 증명에 실패했습니다. – 브라우저 보안 설정으로 인해 클라이언트가 Web Security Appliance를 신뢰하지 않습니다. 자격 증명이 3방향 핸드셰이크(다이제스트 스타일 인증)를 사용하여 안전하게 전송됩니다. 암호는 연결을 통해 전송되지 않습니다. • **게스트 권한 지원** – 유효하지 않은 자격 증명으로 인해 인증에 실패한 사용자에게 게스트 액세스 권한을 부여하려면 이 확인란을 선택합니다.
그룹 인증을 위한 영역	• **인증 또는 시퀀스 선택** – 정의된 인증 영역 또는 시퀀스를 선택합니다.

인증 서로게이트	인증에 성공한 후 트랜잭션을 사용자와 연결할 방법을 지정합니다(옵션은 웹 프록시 구축 모드에 따라 다름). • **IP 주소** – 웹 프록시가 특정 IP 주소의 인증된 사용자를 추적합니다. 투명 사용자 식별의 경우 이 옵션을 선택합니다. • **영구적 쿠키** – 웹 프록시가 애플리케이션별로 각 사용자에 대한 영구적 쿠키를 생성하여 특정 애플리케이션의 인증된 사용자를 추적합니다. 애플리케이션을 종료해도 쿠키는 제거되지 않습니다. • **세션 쿠키** – 웹 프록시는 애플리케이션별로 도메인의 각 사용자에 대한 세션 쿠키를 생성하여 특정 애플리케이션의 인증된 사용자를 추적합니다. (그러나 사용자가 동일한 애플리케이션에서 같은 도메인에 대해 다른 자격 증명을 제공할 경우, 쿠키를 덮어씁니다.) 애플리케이션을 종료하면 쿠키도 제거됩니다. • **서로게이트 없음** – 웹 프록시가 서로게이트를 사용하여 자격 증명을 캐시하지 않으며 새 TCP 연결마다 인증된 사용자를 추적합니다. 이 옵션을 선택하면 웹 인터페이스가 더 이상 적용되지 않은 다른 설정을 사용하지 않도록 설정합니다. 이 옵션은 명시적 전달 모드에서와 Network(네트워크) > Authentication(인증) 페이지에서 자격 증명 암호화를 사용하지 않도록 설정하는 경우에만 사용할 수 있습니다. • **명시적 전달 요청에 동일한 서로게이트 설정 적용** – 투명 요청에 사용되는 서로게이트를 명시적 요청에 적용하려는 경우 선택합니다. 자동으로 자격 증명 암호화를 사용하도록 설정합니다. 이 옵션은 웹 프록시가 투명 모드에서 구축된 경우에만 표시됩니다. **참고** 전역 인증 설정에서 모든 요청에 대한 인증 서로게이트의 시간 초과 값을 정의할 수 있습니다.

8단계 **구성원 자격 정의** 섹션에서 선택한 식별 방법에 적합한 구성원 자격 매개변수를 제공합니다. 이 표에 설명된 모든 옵션을 모든 사용자 식별 방법에 사용할 수는 없습니다.

구성원 정의	
사용자 위치별 구성원 정의	**로컬 사용자만**, **원격 사용자만** 또는 **모두**에 적용하도록 이 식별 프로필을 구성합니다. 이 선택은 이 식별 프로필에 대해 사용 가능한 인증 설정에 영향을 줍니다.
서브넷별 구성원 정의	이 식별 프로필이 적용되어야 하는 주소를 입력합니다. IP 주소, CIDR 블록 및 서브넷을 사용할 수 있습니다. **참고** 어떤 항목도 입력하지 않으면 식별 프로필이 *모든* IP 주소에 적용됩니다.
프로토콜별 구성원 정의	이 식별 프로필이 적용되어야 하는 프로토콜을 선택합니다. 적용되는 모든 프로토콜을 선택합니다. • **HTTP/HTTPS** – FTP over HTTP를 포함하여 HTTP 또는 HTTPS를 기본 프로토콜로 사용하고 HTTP CONNECT를 사용하여 터널링되는 다른 모든 프로토콜을 사용하는 모든 요청에 적용됩니다. • **네이티브 FTP** – 네이티브 FTP 요청에만 적용됩니다. • **SOCKS** – SOCKS 정책에만 적용됩니다.

머신 ID별 구성원 정의	• **이 정책에서 머신 ID를 사용하지 않음** – 사용자가 머신 ID로 식별되지 않습니다. • **머신 ID를 기반으로 사용자 인증 정책 정의** – 주로 사용자가 머신 ID로 식별됩니다. Authorized Machine Groups(인증된 머신 그룹) 페이지를 표시하려면 Machine Groups(머신 그룹) 영역을 클릭합니다. 추가할 각 그룹에 대해 Directory Search(디렉토리 검색) 필드에 추가할 그룹의 이름을 입력한 후 Add(추가)를 클릭합니다. 그룹을 선택하고 Remove(제거)를 클릭하여 목록에서 제거할 수 있습니다. Done(완료)을 클릭하여 이전 페이지로 돌아갑니다. Authorized Machines(인증된 머신) 페이지를 표시하려면 Machine IDs(머신 ID) 영역을 클릭합니다. Authorized Machines(인증된 머신) 필드에 정책과 연결할 머신 ID를 입력한 후 Done(완료)을 클릭합니다. **참고** 머신 ID를 사용하는 인증은 커넥터 모드에서만 지원되며 Active Directory가 필요합니다.
고급	추가 구성원 자격 요건을 정의하려면 이 섹션을 확장합니다. • **프록시 포트** – 웹 프록시에 액세스하는 데 사용되는 하나 이상의 프록시 포트를 지정합니다. 쉼표로 구분된 포트 번호를 입력합니다. 명시적 전달 연결의 경우 프록시 포트는 브라우저에서 구성됩니다. 투명한 연결의 경우에는 목적지 포트와 동일합니다. 포트별 ID 정의는 어플라이언스가 명시적 전달 모드에서 구축되거나 클라이언트가 요청을 명시적으로 어플라이언스에 전달하는 경우에 가장 적합합니다. 클라이언트 요청이 어플라이언스에 투명하게 리디렉션되는 경우 포트별로 ID를 정의하면 일부 요청이 거부될 수 있습니다. • **URL 카테고리** – 사용자 정의 또는 미리 정의된 URL 카테고리를 선택합니다. 이러한 URL 카테고리에 대한 구성원 자격은 기본적으로 제외됩니다. 즉, Add(추가) 열에서 선택하지 않으면 웹 프록시에서 모든 카테고리를 무시합니다. URL 카테고리별로 구성원 자격을 정의해야 하는 경우, 해당 카테고리에 대한 인증 요청에서 제외해야 할 때만 ID 그룹에 이를 정의합니다. • **사용자 에이전트** – 클라이언트 요청에서 사용되는 사용자 에이전트(Firefox 또는 Chrome 웹 브라우저와 같은 애플리케이션)별로 정책 그룹 구성원 자격을 정의합니다. 일반적으로 정의된 일부 브라우저를 선택하거나 정규식을 사용하여 고유한 브라우저를 정의할 수 있습니다. 이 정책 그룹이 선택한 사용자 에이전트에만 적용되어야 하는지 또는 선택한 에이전트 목록에 없는 모든 사용자 에이전트에 적용되어야 하는지를 선택합니다.

9단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 최종 사용자 자격 증명 확보 개요, 5-1페이지
- 정책을 통한 웹 요청 관리 작업 개요, 10-2페이지

ID 사용/사용 안 함

시작하기 전에

- 식별 프로필을 사용하지 않도록 설정하면 연결된 정책에서 제거됩니다.
- 식별 프로필을 다시 사용하도록 설정하면 어떤 정책과도 다시 연결되지 않습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Identification Profiles(식별 프로필)**를 선택합니다.

2단계 Identification Profiles(식별 프로필) 테이블에서 프로필을 클릭하여 해당 프로필의 Identification Profile(식별 프로필) 페이지를 엽니다.

3단계 Client/User Identification Profile Settings(클라이언트/사용자 식별 프로필 설정) 바로 아래의 **Enable Identity(ID 사용)**를 선택하거나 지웁니다.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

식별 프로필 및 인증

그림 6-1 페이지 6-9에서는 프로필이 다음을 사용하도록 구성된 경우 웹 프록시가 클라이언트 요청을 식별 프로필과 비교하여 평가하는 방법을 보여줍니다.

- 인증 서로게이트 없음
- IP 주소를 인증 서로게이트로 사용
- 쿠키를 투명 요청을 통한 인증 서로게이트로 사용
- 쿠키를 명시적 요청을 통한 인증 서로게이트로 사용하고 자격 증명 암호화가 사용하도록 설정됨

그림 6-1 트랜잭션 요청 플로우: 식별 프로필 및 인증 - 서로게이트 없음 및 IP 기반 서로게이트

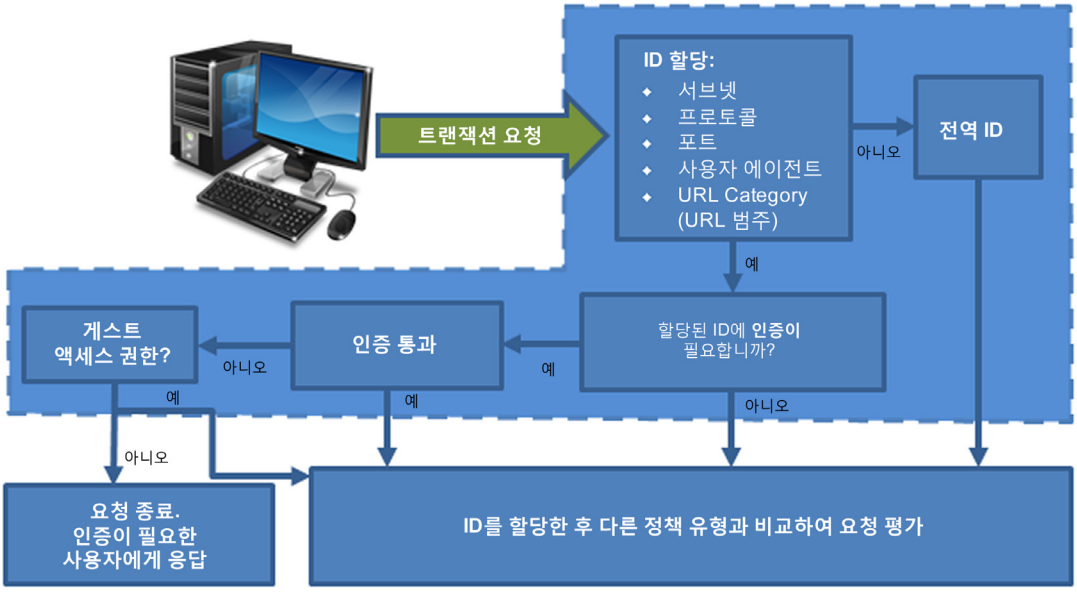
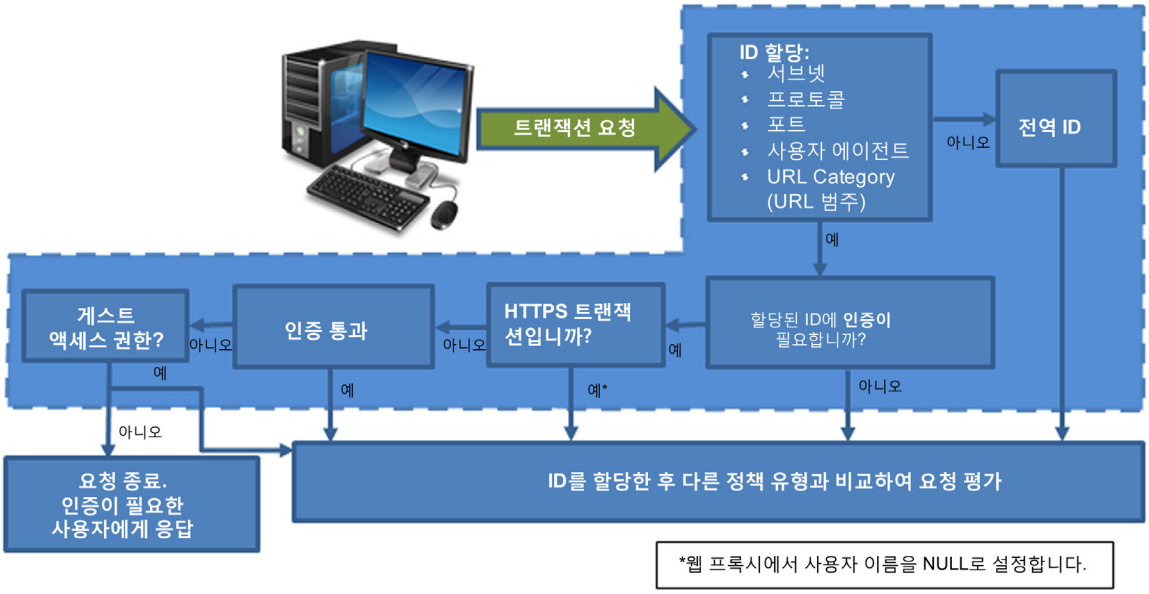


그림 6-2 트랜잭션 요청 플로우: 식별 프로필 및 인증 - TranCookie 기반 서로게이트



식별 프로필 트러블슈팅

- 기본 인증 문제, A-3페이지
- 정책 문제, A-13페이지
- 정책이 적용되지 않음, A-14페이지
- 정책 트러블슈팅 툴: 정책 추적, A-16페이지
- 업스트림 프록시 문제, A-21페이지

SaaS 액세스 제어

- SaaS 액세스 제어 개요, 7-1페이지
- 어플라이언스를 ID 공급자로 구성, 7-2페이지
- SaaS 액세스 제어 및 여러 어플라이언스 사용, 7-3페이지
- SaaS 애플리케이션 인증 정책 생성, 7-4페이지
- 단일 로그인 URL에 대한 최종 사용자 액세스 구성, 7-7페이지

SaaS 액세스 제어 개요

Web Security Appliance는 SAML(Security Assertion Markup Language)을 사용하여 SaaS 애플리케이션에 액세스 권한을 부여합니다. SAML 버전 2.0과 엄격하게 호환되는 SaaS 애플리케이션에서 작동합니다.

Cisco SaaS 액세스 제어를 사용하여 다음을 수행할 수 있습니다.

- SaaS 애플리케이션에 액세스할 수 있는 사용자와 액세스하는 위치를 제어합니다.
- 사용자가 조직에 더 이상 고용되지 않은 경우 모든 SaaS 애플리케이션에 대한 액세스를 빠르게 사용하지 않도록 설정합니다.
- 사용자에게 SaaS 사용자 자격 증명을 입력하도록 요구하는 피싱 공격의 위험을 줄입니다.
- 사용자가 투명하게 로그인되는지(단일 로그인 기능) 아니면 인증 사용자 이름과 암호를 입력하라는 프롬프트가 표시되는지를 선택합니다.

SaaS 액세스 제어는 웹 보안 어플라이언스에서 지원되는 인증 메커니즘이 필요한 SaaS 애플리케이션에서만 작동합니다. 현재 웹 프록시는 "PasswordProtectedTransport" 인증 메커니즘을 사용합니다.

SaaS 액세스 제어를 사용하도록 설정하려면 웹 보안 어플라이언스 및 SaaS 애플리케이션 모두에서 설정을 구성해야 합니다.

1단계	웹 보안 어플라이언스를 ID 공급자로 구성합니다.	어플라이언스를 ID 공급자로 구성, 7-2페이지
2단계	SaaS 애플리케이션에 대한 인증 정책을 생성합니다.	SaaS 애플리케이션 인증 정책 생성, 7-4페이지
3단계	단일 로그인을 위해 SaaS 애플리케이션을 구성합니다.	단일 로그인 URL에 대한 최종 사용자 액세스 구성, 7-7페이지
4단계	(선택 사항) 여러 웹 보안 어플라이언스를 구성합니다.	SaaS 액세스 제어 및 여러 어플라이언스 사용, 7-3페이지

어플라이언스를 ID 공급자로 구성

웹 보안 어플라이언스를 ID 공급자로 구성할 때 사용자가 정의하는 설정이 통신하는 모든 SaaS 애플리케이션에 적용됩니다. 웹 보안 어플라이언스가 인증서 및 키를 사용하여 생성하는 각 SAML 어설션에 서명합니다.

시작하기 전에

- (선택 사항) SAML 어설션에 서명하기 위한 인증서(PEM 형식) 및 키를 찾습니다.
- 인증서를 각 SaaS 애플리케이션에 업로드합니다.

1단계 **Network(네트워크) > Identity Provider for SaaS(SaaS용 ID 공급자)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable SaaS Single Sign-on Service(SaaS 단일 로그인 서비스 사용)**를 선택합니다.

4단계 **Identity Provider Domain Name(ID 공급자 도메인 이름)** 필드에 가상 도메인 이름을 입력합니다.

5단계 **Identity Provider Entity ID(ID 공급자 엔티티 ID)** 필드에 고유한 텍스트 ID를 입력합니다(URI 형식의 문자열이 권장됨).

6단계 인증서 및 키를 업로드하거나 생성합니다.

방법	추가 단계
인증서 및 키 업로드	1. **Use Uploaded Certificate and Key(업로드된 인증서 및 키 사용)**를 선택합니다. 2. **Certificate(인증서)** 필드에서 Browse(찾아보기)를 클릭하여 업로드할 파일을 찾습니다. **참고** 웹 프록시에서 파일에 있는 첫 번째 인증서 또는 키를 사용합니다. 인증서 파일은 PEM 형식이어야 합니다. DER 형식은 지원되지 않습니다. 3. **Key(키)** 필드에서 Browse(찾아보기)를 클릭하여 업로드할 파일을 찾습니다. 키가 암호화된 경우 **Key is Encrypted(키가 암호화됨)**를 선택합니다. **참고** 키 길이는 512, 1024 또는 2048비트여야 합니다. 개인 키 파일은 PEM 형식이어야 합니다. DER 형식은 지원되지 않습니다. 4. **Upload Files(파일 업로드)**를 클릭합니다. 5. **Download Certificate(인증서 다운로드)**를 클릭하여 Web Security appliance가 통신할 SaaS 애플리케이션에 전송할 수 있도록 인증서의 사본을 다운로드합니다.

방법	추가 단계
인증서 및 키 생성	1. **Use Generated Certificate and Key(생성된 인증서 및 키 사용)**를 선택합니다. 2. **Generate New Certificate and Key(새 인증서 및 키 생성)**를 클릭합니다. a. Generate Certificate and Key(인증서 및 키 생성) 대화 상자에서 서명 인증서에 표시할 정보를 입력합니다. **참고** Common Name(공용 이름) 필드에 슬래시(/)를 제외한 모든 ASCII 문자를 입력할 수 있습니다. b. **Generate(생성)**를 클릭합니다. 3. **Download Certificate(인증서 다운로드)**를 클릭하여 웹 보안 어플라이언스와 통신할 SaaS 애플리케이션에 인증서를 전송합니다. 4. (선택 사항) 서명된 인증서를 사용하려면 DCSR(**Download Certificate Signing Request**) 링크를 클릭하여 CA(Certificate Authority)에 요청을 제출합니다. CA에서 서명된 인증서를 받은 후에는 **Browse**를 클릭하고 서명된 인증서 위치로 이동합니다. **파일 업로드**를 클릭합니다.

참고 어플라이언스에 업로드된 인증서 및 키 쌍과 생성된 인증서 및 키 쌍이 모두 있는 경우 Signing Certificate(서명 인증서) 섹션에서 현재 선택한 인증서 및 키 쌍만을 사용합니다.

7단계 어플라이언스를 ID 공급자로 구성하는 경우 설정을 기록하십시오. 이러한 설정 중 일부는 단일 로그인을 위해 SaaS 애플리케이션을 구성할 때 사용되어야 합니다.

8단계 변경 사항을 제출 및 커밋합니다.

다음 단계

- SAML 어설션에 서명하는 데 사용할 인증서 및 키를 지정한 후 인증서를 각 SaaS 애플리케이션에 업로드합니다.

관련 주제

- 단일 로그인 URL에 대한 최종 사용자 액세스 구성, 7-7페이지

SaaS 액세스 제어 및 여러 어플라이언스 사용

시작하기 전에

- 어플라이언스를 ID 공급자로 구성, 15-2페이지

1단계 각 웹 보안 어플라이언스에 대해 동일한 ID 공급자 도메인 이름을 구성합니다.

2단계 각 웹 보안 어플라이언스에 대해 동일한 ID 공급자 엔티티 ID를 구성합니다.

3단계 **Network(네트워크) > Identity Provider for SaaS(SaaS용 ID 공급자)** 페이지에서 동일한 인증서 및 개인 키를 각 어플라이언스에 업로드합니다.

4단계 사용자가 구성하는 각 SaaS 애플리케이션에 이 인증서를 업로드합니다.

SaaS 애플리케이션 인증 정책 생성

시작하기 전에

- 연결된 ID를 생성합니다.
- ID 공급자를 구성합니다. 어플라이언스를 ID 공급자로 구성, 7-2페이지를 참조하십시오.
- Network(네트워크) > Identity Provider for SaaS(SaaS용 ID 공급자) > Enable and Edit Settings(설정 사용 및 편집)에서 ID 공급자 서명 인증서 및 키를 제공합니다.
- 인증 영역을 생성합니다. 인증 영역, 5-10페이지를 참조하십시오.

1단계 **Web Security Manager(웹 보안 관리자) > SaaS Policies(SaaS 정책)**를 선택합니다.

2단계 **Add Application(애플리케이션 추가)**을 클릭합니다.

3단계 설정을 구성합니다.

속성	설명
애플리케이션 이름	이 정책에 대한 SaaS 애플리케이션을 식별하기 위한 이름을 입력합니다. 각 애플리케이션 이름은 고유해야 합니다. Web Security appliance에서 애플리케이션 이름을 사용하여 단일 로그인 URL을 생성합니다.
설명	(선택 사항) 이 SaaS 정책에 대한 설명을 입력합니다.

속성	설명
서비스 공급자용 메타데이터	이 정책에서 참조되는 서비스 공급자에 대해 설명하는 메타데이터를 구성합니다. 수동으로 서비스 공급자 속성에 대해 설명하거나 SaaS 애플리케이션에서 제공된 메타데이터 파일을 업로드할 수 있습니다. Web Security appliance에서 메타데이터를 사용하여 SAML을 통해 SaaS 애플리케이션(서비스 공급자)과 통신하는 방법을 결정합니다. 메타데이터를 구성하기 위한 올바른 설정에 대해 알아보려면 SaaS 애플리케이션에 문의하십시오. **Configure Keys Manually(수동으로 키 구성)** – 이 옵션을 선택하는 경우 다음을 제공합니다. • **Service Provider Entity ID(서비스 공급자 엔티티 ID)**. SaaS 애플리케이션에서 자체를 서비스 공급자로 식별하는 데 사용하는 텍스트(일반적으로 URI 형식)를 입력합니다. • **Name ID Format(이름 ID 형식)**. 드롭다운 목록에서 어플라이언스가 서비스 공급자에게 전송하는 SAML 어설션에서 사용자를 식별하는 데 사용해야 하는 형식을 선택합니다. 여기에 입력하는 값은 SaaS 애플리케이션에 구성된 해당 설정과 일치해야 합니다. • **Assertion Consumer Service URL(어설션 고객 서비스 URL)**. Web Security appliance에서 생성하는 SAML 어설션을 전송할 URL을 입력합니다. 사용할 올바른 URL(로그인 URL이라고도 함)을 결정하려면 SaaS 애플리케이션 문서를 읽으십시오. **Import File from Hard Disk(하드 디스크에서 파일 가져오기)** – 이 옵션을 선택하는 경우 Browse(찾아보기)를 클릭하여 파일을 찾은 후 **Import(가져오기)**를 클릭합니다. **참고** 이 메타데이터 파일은 SAML 표준에 따라 서비스 공급자 인스턴스에 대해 설명하는 XML 문서입니다. 모든 SaaS 애플리케이션에서 메타데이터 파일을 사용하지는 않지만 이 파일을 사용하는 SaaS 애플리케이션의 경우 SaaS 애플리케이션 공급자에게 파일에 대해 문의하십시오.
SaaS SSO를 위한 사용자 식별/인증	SaaS 단일 로그인을 위해 사용자를 식별/인증하는 방법을 지정합니다. • 사용자에게 항상 로컬 인증 자격 증명 프롬프트를 표시합니다. • 웹 프록시가 투명하게 사용자 이름을 가져온 경우 사용자에게 로컬 인증 자격 증명에 대한 프롬프트를 표시합니다. • 로컬 인증 자격 증명을 사용하여 자동으로 SaaS 사용자를 로그인합니다. 웹 프록시가 이 SaaS 애플리케이션에 액세스하는 사용자를 인증하는 데 사용해야 하는 인증 영역 또는 시퀀스를 선택합니다. 사용자가 SaaS 애플리케이션에 성공적으로 액세스하려면 인증 영역 또는 인증 시퀀스의 구성원이어야 합니다. ISE(Identity Services Engine)가 인증에 사용되고 LDAP가 선택된 경우 SAML 사용자 이름과 특성 매핑을 위한 영역이 사용됩니다.

속성	설명
SAML 사용자 이름 매핑	웹 프록시가 SAML 어설션에서 사용자 이름을 서비스 공급자에게 표시하는 방법을 지정합니다. 네트워크 내부에서 사용되는 그대로 사용자 이름을 전달하거나(**매핑 없음**) 다음 방법 중 하나를 사용하여 내부 사용자 이름을 다른 형식으로 변경할 수 있습니다. • **LDAP 쿼리.** 서비스 공급자에게 전송되는 사용자 이름이 하나 이상의 LDAP 쿼리 특성을 기반으로 합니다. LDAP 특성 필드와 선택적인 맞춤형 텍스트를 포함하는 식을 입력합니다. 특성 이름은 꺾쇠괄호로 묶어야 합니다. 여러 특성을 포함할 수 있습니다. 예를 들어, LDAP 특성 "user" 및 "domain"의 경우 <user>@<domain>.com을 입력할 수 있습니다. • **고정된 규칙 매핑.** 서비스 공급자에게 전송되는 사용자 이름은 내부 사용자 이름 앞이나 뒤에 고정된 문자열이 추가된 내부 사용자 이름을 기반으로 합니다. 내부 사용자 이름에서 해당 위치를 표시하기 위해 문자열 앞이나 뒤에 %s가 포함된 고정 문자열을 **Expression Name(식 이름)** 필드에 입력합니다.
SAML 속성 매핑	(선택 사항) SaaS 애플리케이션에 필요한 경우 LDAP 인증 서버의 내부 사용자에 대한 추가 정보를 SaaS 애플리케이션에 제공할 수 있습니다. 각 LDAP 서버 특성을 SAML 특성에 매핑합니다.
인증 컨텍스트	웹 프록시에서 내부 사용자를 인증하는 데 사용하는 인증 메커니즘을 선택합니다. **참고** 인증 상황 인식에서는 ID 공급자가 내부 사용자를 인증하는 데 어떤 인증 메커니즘을 사용했는지 서비스 공급자에게 알립니다. 일부 서비스 공급자의 경우 사용자가 SaaS 애플리케이션에 액세스하도록 허용하려면 특정 인증 메커니즘이 필요합니다. ID 공급자가 지원하지 않는 인증 상황 인식이 서비스 공급자에게 필요한 경우 사용자는 ID 공급자의 단일 로그인을 사용하여 서비스 공급자에 액세스할 수 없습니다.

4단계 변경 사항을 제출 및 커밋합니다.

다음 작업

- 동일한 매개변수를 통해 애플리케이션을 구성하여 SaaS 애플리케이션 측에서 단일 로그인 설정을 지정합니다.

단일 로그인 URL에 대한 최종 사용자 액세스 구성

웹 보안 어플라이언스를 ID 공급자로 구성하고 SaaS 애플리케이션에 대한 SaaS 애플리케이션 인증 정책을 생성한 후 어플라이언스에서 SSO URL(Single Sign-On URL)을 생성합니다. 웹 보안 어플라이언스는 SaaS 애플리케이션 인증 정책에 구성된 애플리케이션 이름을 사용하여 단일 로그인 URL을 생성합니다. SSO URL 형식은 다음과 같습니다.

http:///*IdentityProviderDomainName*/SSOURL/*ApplicationName*

1단계 **Web Security Manager(웹 보안 관리자) > SaaS Policies(SaaS 정책)** 페이지에서 단일 로그인 URL을 가져옵니다.

2단계 플로우 유형에 따라 최종 사용자가 URL을 사용할 수 있도록 합니다.

3단계 ID 공급자가 시작한 플로우를 선택하는 경우 어플라이언스에서 사용자를 SaaS 애플리케이션으로 리디렉션합니다.

4단계 서비스 공급자가 시작한 플로우를 선택하는 경우 SaaS 애플리케이션에서 이 URL을 구성해야 합니다.

- SaaS 사용자에게 항상 프록시 인증 확인. 유효한 자격 증명을 입력하면 사용자가 SaaS 애플리케이션에 로그인됩니다.
- 투명하게 SaaS 사용자 로그인. 사용자가 자동으로 SaaS 애플리케이션에 로그인됩니다.

참고 어플라이언스가 투명 모드에서 구축된 경우 인증된 모든 사용자에 대해 명시적 전달 요청을 사용하여 단일 로그인 동작을 수행하려면 ID 그룹을 구성할 때 "**Apply same surrogate settings to explicit forward requests(명시적 전달 요청에 동일한 서로게이트 설정 적용)**"를 선택합니다.

Cisco Identity Services Engine 통합

- ISE(Identity Services Engine) 서비스 개요, 8-1페이지
- ISE(Identity Services Engine) 인증서, 8-2페이지
- ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지
- ISE 서비스에 연결, 8-6페이지
- ISE(Identity Services Engine) 트러블슈팅, 8-8페이지

ISE(Identity Services Engine) 서비스 개요

Cisco의 ISE(Identity Services Engine)는 향상된 ID 관리를 제공하기 위해 네트워크의 개별 서버에서 실행되는 애플리케이션입니다. AsyncOS는 ISE 서버에서 사용자 ID 정보에 액세스할 수 있습니다. 구성된 경우, 적절하게 구성된 식별 프로필에 대한 ISE(Identity Services Engine)에서 사용자 이름 및 연관된 SGT(Secure Group Tag)를 가져와서 해당 프로필을 사용하도록 구성된 정책에서 투명한 사용자 식별을 허용합니다.

참고 커넥터 모드에서는 ISE 서비스를 사용할 수 없습니다.

관련 주제

- pxGrid 정보, 8-1페이지
- ISE 서버 구축 및 페일오버 정보, 8-2페이지

pxGrid 정보

Cisco pxGrid(Platform Exchange Grid)를 사용하면 보안 모니터링 및 네트워크 탐지 시스템, ID 및 액세스 관리 플랫폼 등과 같은 네트워크 인프라 구성 요소 간에 협업할 수 있습니다. 이러한 구성 요소는 pxGrid를 사용하여 게시/구독 방법을 통해 정보를 교환할 수 있습니다.

기본적으로 pxGrid 게시자, pxGrid 클라이언트 및 pxGrid 컨트롤러의 3가지 pxGrid 구성 요소가 있습니다.

- pxGrid 게시자 – pxGrid 클라이언트에 대한 정보를 제공합니다.
- pxGrid 클라이언트 – 게시된 정보를 구독하는 임의의 시스템(예: 웹 보안 어플라이언스)입니다. 이 경우 SGT(Security Group Tag)와 사용자 그룹 및 프로필 정보를 구독합니다.
- pxGrid 컨트롤러 – 이 경우 클라이언트 등록/관리 및 토픽/서브스크립션 프로세스를 제어하는 ISE pxGrid 노드입니다.

각 구성 요소에는 신뢰할 수 있는 인증서가 필요하며 이러한 인증서가 각 호스트 플랫폼에 설치되어야 합니다.

ISE 서버 구축 및 페일오버 정보

단일 ISE 노드 설치를 "독립형 구축"이라고 하며, 이 단일 노드는 관리, 정책 서비스 및 모니터링 페르소나에서 실행됩니다. 페일오버를 지원하고 성능을 향상시키려면 여러 ISE 노드를 "분산형 구축"으로 설치해야 합니다. 웹 보안 어플라이언스에서 ISE 페일오버를 지원하기 위해 필요한 최소 분산형 ISE 컨피그레이션은 다음과 같습니다.

- 2개의 pxGrid 노드
- 2개의 모니터링 노드
- 2개의 관리 노드
- 1개의 정책 서비스 노드

이 컨피그레이션은 *Cisco Identity Services Engine 하드웨어 설치 설명서*에서 "중간 규모의 네트워크 구축"으로 참조됩니다. 추가 정보는 설치 설명서의 해당 네트워크 구축 섹션을 참조하십시오.

관련 주제

- ISE(Identity Services Engine) 인증서, 8-2페이지
- ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지
- ISE 서비스에 연결, 8-6페이지
- ISE(Identity Services Engine) 트러블슈팅, 8-8페이지

ISE(Identity Services Engine) 인증서

참고 이 섹션에서는 ISE 연결에 필요한 인증서에 대해 설명합니다. ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지에서는 이러한 인증서에 대한 자세한 정보를 제공합니다. 인증서 관리, 22-24페이지에서는 AsyncOS에 대한 일반 인증서 관리 정보를 제공합니다.

웹 보안 어플라이언스와 각 ISE 서버 간의 상호 인증과 보안 통신에는 3개의 인증서 세트가 필요합니다.

- **WSA 클라이언트 인증서** – ISE 서버에서 웹 보안 어플라이언스를 인증하는 데 사용됩니다.
- **ISE 관리 인증서** – 웹 보안 어플라이언스에서 ISE 사용자 프로필 데이터의 벌크 다운로드를 위해 포트 443에서 ISE 서버를 인증하는 데 사용됩니다.
- **ISE pxGrid 인증서** – 웹 보안 어플라이언스에서 WSA-ISE 데이터 서브스크립션(ISE 서버에 대한 지속적인 쿼리 게시/구독)을 위해 포트 5222에서 ISE 서버를 인증하는 데 사용됩니다.

이러한 3개의 인증서는 CA(Certificate Authority) 서명 또는 자체 서명된 인증서일 수 있습니다. AsyncOS는 자체 서명된 WSA 클라이언트 인증서를 생성하거나, CA 서명 인증서가 필요한 경우에는 대신 CSR(Certificate Signing Request)을 생성하기 위한 옵션을 제공합니다. 마찬가지로, ISE 서버는 자체 서명된 ISE 관리 및 pxGrid 인증서를 생성하거나 CA 서명 인증서가 필요한 경우에는 대신 CSR을 생성하기 위한 옵션을 제공합니다.

관련 주제

- 자체 서명된 인증서 사용, 8-3페이지
- CA 서명 인증서 사용, 8-3페이지
- ISE(Identity Services Engine) 서비스 개요, 8-1페이지
- ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지
- ISE 서비스에 연결, 8-6페이지

자체 서명된 인증서 사용

자체 서명된 인증서가 ISE 서버에서 사용되는 경우 3개의 인증서(ISE 서버에서 개발된 ISE pxGrid 및 관리 인증서와 WSA에서 개발된 WSA 클라이언트 인증서)가 모두 ISE 서버의 신뢰할 수 있는 인증서 저장소에 추가되어야 합니다(Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서) > Import(가져오기)).

CA 서명 인증서 사용

CA 서명 인증서의 경우:

- ISE 서버에서 WSA 클라이언트 인증서에 대한 적절한 CA 루트 인증서가 신뢰할 수 있는 인증서 저장소(Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서))에 있는지 확인합니다.
- WSA에서 적절한 CA 루트 인증서가 신뢰할 수 있는 인증서 목록에 있는지 확인하십시오(Network(네트워크) > Certificate Management(인증서 관리) > Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)). ISE(Identity Services Engine) 페이지(Network(네트워크) > Identity Services Engine))에서 ISE 관리 및 pxGrid 인증서에 대한 CA 루트 인증서를 업로드해야 합니다.

ISE 서비스를 인증하고 통합하기 위한 작업

단계	작업	관련 주제 및 절차에 대한 링크
1a	WSA에서 WSA 클라이언트 인증서를 추가합니다.	• WSA에서 CA 서명 또는 자체 서명된 WSA 클라이언트 인증서를 생성하거나 업로드합니다. ISE 서비스에 연결, 8-6페이지 및 인증서 관리, 22-24페이지 섹션을 참조해 주십시오.
1b	WSA에서 ISE 서버에 업로드하도록 이 WSA 클라이언트 인증서를 다운로드합니다.	• WSA 클라이언트 인증서를 다운로드하여 저장한 후 ISE 서버에 전송합니다. ISE 서비스에 연결, 8-6페이지를 참조하십시오.

단계	작업	관련 주제 및 절차에 대한 링크
2	WSA 클라이언트 인증서가 자체 서명된 경우 이 인증서와 해당 서명 인증서를 ISE 서버에 업로드합니다.	• 이전 단계의 WSA에서 다운로드된 WSA 클라이언트 인증서를 가져와서 ISE 서버의 신뢰할 수 있는 인증서 저장소에 추가합니다. (Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서) > Import(가져오기)) • 또한 자체 서명된 인증서 사용, 8-3페이지에 논의된 대로 이 WSA 클라이언트 인증서에 대한 적절한 서명 인증서를 ISE 서버의 신뢰할 수 있는 인증서 저장소에 추가해야 합니다.
3	ISE 서버에서 ISE 관리 pxGrid 인증서를 추가합니다.	• Administration(관리) > Certificates(인증서) 페이지로 이동하여 ISE 관리 및 pxGrid 인증서를 생성하거나 업로드합니다. – CA 서명 인증서의 경우 2개의 인증서 서명 요청(관리 및 pxGrid 사용을 위해 하나씩)을 생성한 후 인증서가 서명되도록 합니다. 서명된 인증서를 수신하면 2개 인증서를 ISE 서버에 업로드합니다. 2개 인증서에 대해 "CA 서명 인증서 바인드" 작업을 수행합니다. CA 루트 인증서를 ISE 서버의 신뢰할 수 있는 인증서 저장소에 추가해야 합니다. ISE 서버를 재시작합니다. – 자체 서명된 인증서의 경우 Administration(관리) > Certificates(인증서) > System Certificates(시스템 인증서)로 이동하여 2개의 자체 서명된 인증서(관리 및 pxGrid에 하나씩)를 생성합니다. (모두에 대해 하나의 공통 인증서를 생성하도록 선택할 수도 있습니다.) 두 인증서를 모두 신뢰할 수 있는 인증서 저장소에 추가합니다. WSA에서 가져올 수 있도록 자체 서명된 인증서를 내보냅니다. **참고** ISE(Identity Services Engine) 인증서, 8-2페이지에서 논의된 대로 이러한 ISE 관리 및 pxGrid 인증서에 대한 적절한 자체 서명된 인증서 또는 CA 루트 인증서가 신뢰할 수 있는 인증서 저장소에 추가되었는지 확인합니다.

단계	작업	관련 주제 및 절차에 대한 링크
4	ISE 서버가 WSA 액세스에 대해 적절하게 구성되었는지 확인합니다.	각 ISE 서버는 ID 토픽 구독자(예: WSA)가 실시간으로 세션 상황을 가져올 수 있도록 구성되어야 합니다. 기본 단계는 다음과 같습니다. • "Enable Auto Registration(자동 등록 사용)"이 켜져 있는지 확인합니다(Administration(관리) > pxGrid Services(pxGrid 서비스) > 오른쪽 상단). • 기존 WSA 클라이언트를 모두 ISE 서버에서 삭제합니다(Administration(관리) > pxGrid Services(pxGrid 서비스) > Clients(클라이언트)). • ISE 서버 바닥글(Administration(관리) > pxGrid Services(pxGrid 서비스))에 "Connected to pxGrid(pxGrid에 연결됨)"라고 표시되는지 확인합니다. • ISE 서버에 SGT 그룹을 구성합니다(Policy(정책) > Results(결과) > TrustSec > Security Groups(보안 그룹)). • SGT 그룹을 사용자와 연결하는 정책을 구성합니다. 자세한 내용은 Cisco Identity Services Engine 설명서를 참조하십시오.
5	WSA에서 내보낸 ISE 관리 및 pxGrid 인증서를 추가합니다.	• 이 WSA에서 구성 중인 각 ISE 서버에 대한 ISE 관리 및 pxGrid 인증서를 업로드합니다. ISE 서비스에 연결, 8-6페이지를 참조하십시오. – ISE 관리 및 pxGrid 모두에 단일 자체 서명된 인증서를 사용하는 경우 ISE Admin Certificate(ISE 관리 인증서) 및 ISE pxGrid Certificate(ISE pxGrid 인증서) 필드에서 각각 한 번씩, 두 번 파일을 업로드합니다. ISE 서비스에 연결, 8-6페이지를 참조하십시오. – CA 서명 인증서를 사용하는 경우 각 쌍의 ISE 인증서에 서명한 인증 기관이 WSA의 Trusted Root Certificates(신뢰할 수 있는 루트 인증서) 목록에 나열되어 있는지 확인합니다. 그렇지 않은 경우 CA 루트 인증서를 가져옵니다. 신뢰할 수 있는 루트 인증서 관리, 22-24페이지를 참조하십시오. **참고** ISE 관리 및 pxGrid 인증서가 루트 CA 인증서에서 서명된 경우 루트 CA 인증서 자체를 WSA의 ISE Admin Certificate(ISE 관리 인증서) 및 ISE pxGrid Certificate(ISE pxGrid 인증서) 필드에 업로드해야 합니다(Network(네트워크) > Identity Services Engine).

단계	작업	관련 주제 및 절차에 대한 링크
6	ISE 액세스 및 기록을 위해 WSA 컨피그레이션을 완료합니다.	• ISE 서비스에 연결, 8-6페이지. • 인증 메커니즘을 기록하기 위해 액세스 로그에 맞춤형 필드 %m을(를) 추가합니다(액세스 로그 맞춤화, 21-26페이지). • ISE 서비스 로그가 생성되었는지 확인합니다. 그렇지 않은 경우 이 로그를 생성합니다(로그 서브스크립션 추가 및 편집, 21-7페이지). • ISE 서비스 로그가 생성되었는지 확인합니다. 그렇지 않은 경우 이 로그를 추가합니다(로그 서브스크립션 추가 및 편집, 21-7페이지). • 사용자 식별 및 인증을 위해 ISE에 액세스하는 식별 프로필을 정의합니다(사용자 및 클라이언트 소프트웨어 분류, 6-3페이지). • ISE 식별을 활용하여 사용자 요청에 대한 기준 및 조치를 정의하는 액세스 정책을 구성합니다(정책 컨피그레이션, 10-8페이지).

참고 ISE 서버에서 인증서를 업로드하거나 변경할 때마다 ISE 서비스를 재시작해야 합니다. 또한 서비스 및 연결이 복원되기 전에 몇 분 정도가 필요할 수 있습니다.

관련 주제

- ISE(Identity Services Engine) 서비스 개요, 8-1페이지
- ISE(Identity Services Engine) 인증서, 8-2페이지
- ISE(Identity Services Engine) 트러블슈팅, 8-8페이지

ISE 서비스에 연결

시작하기 전에

- 각 ISE 서버가 WSA 액세스에 대해 적절하게 구성되어 있어야 합니다. ISE 서비스를 인증하고 통합하기 위한 작업, 8-3페이지를 참조하십시오.
- ISE 서버 연결 정보를 확보합니다.
- 유효한 ISE 관련 인증서(클라이언트, 포털 및 pxGrid) 및 키를 확보합니다. 관련 정보는 ISE(Identity Services Engine) 인증서, 8-2페이지를 참조하십시오.

1단계 **Network(네트워크) > Identification Service Engine**을 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable ISE Service(ISE 서비스 사용)**를 선택합니다.

4단계 해당 호스트 이름 또는 IPv4 주소를 사용하여 **기본 ISE pxGrid 노드**를 식별합니다.

a. WSA-ISE 데이터 서브스크립션(ISE 서버에 대한 지속적인 쿼리)을 위한 **ISE pxGrid 노드 인증서**를 제공합니다.

인증서 파일을 찾아 선택한 후 **Upload File(파일 업로드)**을 클릭합니다. 자세한 내용은 인증서 및 키 업로드, 22-25페이지를 참조하십시오.

5단계 페일오버를 위해 두 번째 ISE 서버를 사용하는 경우 해당 호스트 이름 또는 IPv4 주소를 사용하여 **보조 ISE pxGrid 노드**를 식별합니다.

a. 보조 **ISE pxGrid 노드 인증서**를 제공합니다.

인증서 파일을 찾아 선택한 후 **Upload File(파일 업로드)**을 클릭합니다. 자세한 내용은 인증서 및 키 업로드, 22-25페이지를 참조하십시오.

참고 기본 ISE 서버에서 보조 ISE 서버로 페일오버되는 동안 WSA 컨피그레이션에 따라 기존 ISE SGT 캐시에 없는 사용자는 인증되어야 하거나 게스트 권한이 지정됩니다. ISE 페일오버가 완료된 후 정상적인 ISE 인증이 재개됩니다.

6단계 **ISE 모니터링 노드 관리 인증서**를 업로드합니다.

a. ISE 사용자 프로필 데이터를 WSA에 벌크로 다운로드하는 데 사용할 **기본 ISE 모니터링 노드 관리 인증서**를 제공합니다.

인증서 파일을 찾아 선택한 후 **Upload File(파일 업로드)**을 클릭합니다. 자세한 내용은 인증서 및 키 업로드, 22-25페이지를 참조하십시오.

b. 페일오버를 위해 두 번째 ISE 서버를 사용하는 경우 **보조 ISE 모니터링 노드 관리 인증서**를 제공합니다.

7단계 WSA-ISE 서버 상호 인증을 위해 **WSA 클라이언트 인증서**를 제공합니다.

참고 이 인증서는 CA 신뢰 루트 인증서여야 합니다. 관련 정보는 ISE(Identity Services Engine) 인증서, 8-2페이지를 참조하십시오.

- **업로드된 인증서 및 키 사용**

  인증서 및 키 모두에 대해 Choose(선택)를 클릭하여 각 파일을 찾아봅니다.

  키가 암호화된 경우 이 확인란을 선택합니다.

  Upload Files(파일 업로드)를 클릭합니다. (이 옵션에 대한 자세한 내용은 인증서 및 키 업로드, 22-25페이지를 참조하십시오.)

- **생성된 인증서 및 키 사용**

  Generate New Certificate and Key(새 인증서 및 키 생성)를 클릭합니다. (이 옵션에 대한 자세한 내용은 인증서 및 키 생성, 22-26페이지를 참조하십시오.)

8단계 WSA 클라이언트 인증서를 다운로드하여 저장한 후 ISE 서버 호스트에 업로드합니다(지정된 서버에서 Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서) > Import(가져오기)).

9단계 (선택 사항) **Start Test(테스트 시작)**를 클릭하여 ISE pxGrid 노드에 대한 연결을 테스트합니다.

10단계 **Submit(제출)**를 클릭합니다.

다음 작업

- 최종 사용자 및 클라이언트 소프트웨어 분류, 6-1페이지
- 인터넷 요청을 제어하기 위한 정책 생성, 10-1페이지

관련 정보

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html, 특히 "How To Integrate Cisco WSA using ISE and TrustSec through pxGrid"

ISE(Identity Services Engine) 트러블슈팅

- ISE(Identity Services Engine) 문제, A-9페이지
  - ISE 문제 트러블슈팅 툴, A-9페이지
  - ISE 서버 연결 문제, A-10페이지
  - ISE 관련 위험 로그 메시지, A-11페이지

9장 정책 애플리케이션을 위한 URL 분류

- URL 트랜잭션 분류 개요, 9-1페이지
- URL 필터링 엔진 구성, 9-4페이지
- URL 카테고리 집합에 대한 업데이트 관리, 9-4페이지
- URL 카테고리를 사용하여 트랜잭션 필터링, 9-9페이지
- 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지
- 성인 콘텐츠 필터링, 9-15페이지
- 액세스 정책의 트래픽 리디렉션, 9-17페이지
- 사용자에게 경고하고 계속하도록 허용, 9-18페이지
- 시간 기반 URL 필터 생성, 9-19페이지
- URL 필터링 활동 보기, 9-19페이지
- 정규식, 9-20페이지
- URL 카테고리 설명, 9-23페이지

URL 트랜잭션 분류 개요

정책 그룹을 사용하여 불확실한 콘텐츠를 포함하는 웹 사이트에 대한 액세스를 제어하는 보안 정책을 생성할 수 있습니다. 차단, 허용 또는 암호 해독되는 사이트는 각 정책 그룹에 대한 카테고리 차단을 설정할 때 선택하는 카테고리에 따라 결정됩니다. URL 카테고리에 따라 사용자 액세스를 제어하려면 Cisco Web Usage Controls를 사용하도록 설정해야 합니다. 이는 도메인 접두사 및 키워드 분석을 사용하여 URL을 분류하는 멀티 레이어 URL 필터링 엔진입니다.

다음 작업을 수행할 때 URL 카테고리를 사용할 수 있습니다.

옵션	방법
정책 그룹 구성원 자격 정의	URL과 URL 카테고리 일치, 9-3페이지
HTTP, HTTPS 및 FTP 요청에 대한 액세스 제어	URL 카테고리를 사용하여 트랜잭션 필터링, 9-9페이지
특정 호스트 이름 및 IP 주소를 지정하는 사용자 정의 맞춤형 URL 카테고리 생성	맞춤형 URL 카테고리 생성 및 편집, 9-14페이지

실패한 URL 트랜잭션 분류

DCA(Dynamic Content Analysis) 엔진은 액세스 정책의 웹 사이트에 대한 액세스를 제어하는 경우에만 URL을 분류합니다. 정책 그룹 구성원 자격을 결정하거나 암호 해독 또는 Cisco 데이터 보안 정책을 사용하여 웹 사이트에 대한 액세스를 제어하는 경우에는 URL을 분류하지 않습니다. 이 엔진은 목적지 서버의 응답 콘텐츠를 분석하여 작동하므로 서버로부터 응답이 다운로드되기 전에 요청 시 이루어져야 하는 결정에는 사용될 수 없기 때문입니다.

분류되지 않은 URL에 대한 웹 평판 점수가 WBRS ALLOW 범위 내에 있는 경우 AsyncOS에서 DCA(Dynamic Content Analysis)를 수행하지 않고 요청을 허용합니다.

DCA(Dynamic Content Analysis) 엔진이 URL을 분류한 후 카테고리 판정과 URL을 임시 캐시에 저장합니다. 이를 통해 향후 트랜잭션이 이전 응답 스캐닝을 활용하고 응답 시간이 아니라 요청 시간에 분류될 수 있습니다.

DCA(Dynamic Content Analysis) 엔진을 사용하도록 설정하면 트랜잭션 성능에 영향을 줄 수 있습니다. 그러나 대부분의 트랜잭션은 Cisco Web Usage Controls URL 카테고리 데이터베이스를 사용하여 분류되므로 일반적으로 적은 비율의 트랜잭션에 대해서만 DCA(Dynamic Content Analysis) 엔진이 호출됩니다.

DCA(Dynamic Content Analysis) 엔진 사용

참고 액세스 정책 또는 액세스 정책에서 사용된 ID가 미리 정의된 URL 카테고리로 정책 구성원 자격을 정의하고 액세스 정책이 동일한 URL 카테고리에 대해 조치를 수행할 수 있습니다. ID 및 액세스 정책 그룹 구성원 자격을 결정할 때 요청의 URL이 분류되지 않을 수 있지만 서버 응답을 수신한 후 DCA(Dynamic Content Analysis) 엔진에서 분류되어야 합니다. Cisco Web Usage Controls는 DCA(Dynamic Content Analysis) 엔진의 카테고리 판정을 무시하며 나머지 트랜잭션에 대한 URL은 "분류되지 않음" 판정으로 유지됩니다. 향후 트랜잭션은 계속 새 카테고리 판정을 활용합니다.

1단계 **Security Services(보안 서비스) > Acceptable Use Controls(제한적 사용 제어)**를 선택합니다.

2단계 Cisco Web Usage Controls를 사용하도록 설정합니다.

3단계 DCA(Dynamic Content Analysis) 엔진을 사용하도록 설정하려면 **클릭**합니다.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

분류되지 않은 URL

분류되지 않은 URL은 미리 정의된 URL 카테고리 또는 *포함된* 맞춤형 URL 카테고리와 일치하지 않는 URL입니다.

참고 정책 그룹 구성원 자격을 결정할 때 맞춤형 URL 카테고리는 정책 그룹 구성원 자격에 대해 선택되는 경우에만 포함된 것으로 간주됩니다.

카테고리가 일치하지 않는 모든 트랜잭션은 Reporting(보고)> URL Categories(URL 카테고리) 페이지에서 "Uncategorized URLs(분류되지 않은 URL)"로 보고됩니다. 내부 네트워크 내의 웹 사이트에 대한 요청에서 다수의 분류되지 않은 URL이 생성됩니다. Cisco에서는 맞춤형 URL 카테고리를 사용하여 내부 URL을 그룹화하고 내부 웹 사이트에 대한 모든 요청을 허용하도록 권장합니다. 이렇게 하면 "분류되지 않은 URL"로 보고되는 웹 트랜잭션의 수가 감소하고, 대신 내부 트랜잭션이 "무시된 URL 필터링" 통계의 일부로 보고됩니다.

관련 주제

- 필터링되지 않고 분류되지 않은 데이터 이해, 9-20페이지.
- 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지.

URL과 URL 카테고리 일치

URL 필터링 엔진에서 URL 카테고리를 클라이언트 요청의 URL과 일치시킬 때 먼저 정책 그룹에 *포함된* 맞춤형 URL 카테고리와 비교하여 URL을 평가합니다. 요청의 URL이 포함된 맞춤형 카테고리와 일치하지 않는 경우 URL 필터링 엔진이 이를 미리 정의된 URL 카테고리와 비교합니다. URL이 포함된 맞춤형 또는 미리 정의된 URL 카테고리와 일치하지 않는 경우 요청이 분류되지 않습니다.

참고 정책 그룹 구성원 자격을 결정할 때 맞춤형 URL 카테고리는 정책 그룹 구성원 자격에 대해 선택되는 경우에만 포함된 것으로 간주됩니다.

정보 특정 웹 사이트가 할당된 카테고리를 보려면 분류되지 않은 URL 또는 잘못 분류된 URL 보고, 9-3페이지의 URL로 이동하십시오.

관련 주제

- 분류되지 않은 URL, 9-3페이지.

분류되지 않은 URL 또는 잘못 분류된 URL 보고

분류되지 않은 URL 및 잘못 분류된 URL을 Cisco에 보고할 수 있습니다. Cisco에서는 해당 웹 사이트에서 여러 URL을 동시에 제출할 수 있는 URL 제출 툴을 제공합니다.

`https://securityhub.cisco.com/web/submit_urls`

제출된 URL의 상태를 확인하려면 이 페이지에 있는 **Status on Submitted URLs(제출된 URL의 상태)** 탭을 클릭합니다. 또한 URL 제출 툴을 사용하여 URL에 대해 할당된 URL 카테고리를 조회할 수 있습니다.

URL 카테고리 데이터베이스

URL이 속하는 카테고리는 필터링 카테고리 데이터베이스에서 결정됩니다. 웹 보안 어플라이언스는 정보를 수집하고 각 URL 필터링 엔진마다 별도의 데이터베이스를 유지 관리합니다. 필터링 카테고리 데이터베이스는 Cisco 업데이트 서버에서 주기적으로 업데이트를 수신합니다.

URL 카테고리 데이터베이스에는 Cisco 내부에서 사용되거나 인터넷에서 가져온 여러 가지 다양한 데이터 요소와 소스가 포함됩니다. 경우에 따라 고려되고 원본으로부터 크게 수정되는 요소 중 하나는 오픈 디렉토리 프로젝트의 정보입니다.

정보 특정 웹 사이트가 할당된 카테고리를 보려면 분류되지 않은 URL 또는 잘못 분류된 URL 보고, 9-3페이지의 URL로 이동하십시오.

관련 주제

- 수동으로 보안 서비스 구성 요소 업데이트, 22-29페이지.

URL 필터링 엔진 구성

기본적으로 Cisco Web Usage Controls URL 필터링 엔진은 시스템 설정 마법사에서 사용하도록 설정됩니다.

1단계 **Security Services(보안 서비스) > Acceptable Use Controls(제한적 사용 제어)**를 선택합니다.

2단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 **Enable Acceptable Use Controls(제한적 사용 제어 사용)** 속성이 사용하도록 설정되었는지 확인합니다.

4단계 DCA(Dynamic Content Analysis) 엔진을 사용하도록 설정할지 여부를 선택합니다.

5단계 URL 필터링 엔진이 사용 불가능한 경우 웹 프록시에서 사용해야 하는 기본 조치(모니터링 또는 차단)를 선택합니다. 기본값은 Monitor(모니터링)입니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

URL 카테고리 집합에 대한 업데이트 관리

새로운 웹 트렌드와 발전된 사용 패턴에 맞게 경우에 따라 미리 정의된 URL 카테고리 집합이 업데이트될 수도 있습니다. URL 카테고리 집합에 대한 업데이트는 새 URL을 추가하고 잘못 분류된 URL을 다시 매핑하는 변경 작업과 다릅니다. 카테고리 집합 업데이트는 기존 정책의 컨피그레이션을 변경할 수 있으므로 조치가 필요합니다. URL 카테고리 집합 업데이트는 제품 릴리스 간에 발생할 수 있으며 AsyncOS 업그레이드가 필요하지 않습니다.

다음에서 정보를 볼 수 있습니다.
http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html

다음 조치를 수행합니다.

조치 수행 시기	방법
업데이트 발생 전 (이러한 작업을 초기 설정의 일부로 수행)	URL 카테고리 집합 업데이트의 영향 이해, 9-5페이지 URL 카테고리 집합에 대한 업데이트 제어, 9-7페이지 새 카테고리 및 변경된 카테고리에 대한 기본 설정, 9-8페이지 카테고리 및 정책 변경에 대한 경고 수신, 9-8페이지
업데이트 발생 후	URL 카테고리 집합 업데이트에 대한 경고에 응답, 9-9페이지

URL 카테고리 집합 업데이트의 영향 이해

URL 카테고리 집합 업데이트는 기존 액세스 정책, 암호 해독 정책 및 Cisco 데이터 보안 정책과 ID에 다음과 같은 영향을 줄 수 있습니다.

- URL 카테고리 집합 변경이 정책 그룹 구성원 자격에 미치는 영향, 9-5페이지
- URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향, 9-5페이지

URL 카테고리 집합 변경이 정책 그룹 구성원 자격에 미치는 영향

이 섹션은 URL 카테고리로 정의될 수 있는 구성원 자격이 있는 모든 정책 유형과 ID에 적용됩니다. 정책 그룹 구성원 자격이 URL 카테고리로 정의되는 경우 카테고리 집합을 변경하면 다음과 같은 영향이 있을 수 있습니다.

- 삭제된 카테고리가 구성원 자격에 대한 단 하나의 조건인 경우에는 정책 또는 ID가 사용하지 않도록 설정됩니다.

정책의 구성원 자격이 변경된 URL 카테고리에 따라 정의되고 이로 인해 ACL 목록이 변경된 경우 웹 프록시가 재시작됩니다.

URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향

URL 카테고리 집합 업데이트로 인해 다음 방식으로 정책 동작이 변경될 수 있습니다.

변경	정책 및 ID의 영향
새 카테고리가 추가될 수 있음	각 정책에 대해 새로 추가된 카테고리의 기본 조치는 해당 정책의 분류되지 않은 URL에 대해 지정된 조치입니다.
카테고리가 삭제될 수 있음	삭제된 카테고리와 연관된 조치가 삭제됩니다. 정책이 삭제된 카테고리에만 종속된 경우 정책이 사용하지 않도록 설정됩니다. 정책이 삭제된 카테고리에만 종속된 ID에 종속되는 경우 정책이 사용하지 않도록 설정됩니다.
카테고리의 이름이 변경될 수 있음	기존 정책의 동작이 변경되지 않습니다.
카테고리가 분할될 수 있음	단일 카테고리가 여러 개의 새 카테고리가 될 수 있습니다. 두 개의 새 카테고리 모두에는 원래 카테고리와 연관된 조치가 있습니다.

변경	정책 및 ID의 영향
둘 이상의 기존 카테고리를 병합할 수 있음	정책의 원래 카테고리에 동일한 조치가 할당된 경우 병합된 카테고리에 원래 카테고리와 동일한 조치가 포함됩니다. 원래 카테고리가 "Use Global Setting(전역 설정 사용)"으로 설정된 경우 병합된 카테고리도 "Use Global Setting(전역 설정 사용)"으로 설정됩니다. 정책에 원래 카테고리에 할당된 여러 조치가 포함된 경우 병합된 카테고리에 할당되는 조치는 해당 정책의 분류되지 않은 URL 설정에 따라 달라집니다. • 분류되지 않은 URL이 Block(차단)(또는 전역 설정이 Block(차단)인 경우 "Use Global Setting(전역 설정 사용)")으로 설정되면 원래 카테고리 중에서 가장 제한적인 조치가 병합된 카테고리에 적용됩니다. • 분류되지 않은 URL이 Block(차단) 이외의 조치(또는 전역 설정이 Block(차단) 이외의 조치인 경우 "Use Global Setting(전역 설정 사용)")로 설정되면 원래 카테고리 중에서 가장 덜 제한적인 조치가 병합된 카테고리에 적용됩니다. 이 경우, 사용자가 이전에 차단되었던 사이트에 액세스할 수 있습니다. 정책 구성원 자격이 URL 카테고리로 정의되고 병합 또는 분류되지 않은 URL 조치와 관련된 카테고리 중 일부가 정책 구성원 자격 정의에 포함되지 않은 경우 전역 정책의 값이 누락된 항목에 사용됩니다. • 제한 순서는 다음과 같습니다(모든 조치를 모든 정책 유형에 사용할 수는 없음). 차단 • 삭제 • 암호 해독 • 경고 • 시간 기반 • 모니터링 • 통과 **참고** 병합된 카테고리를 기반으로 하는 시간 기반 정책은 원래 카테고리 중 하나와 연관된 조치를 채택합니다. (시간 기반 정책에는 확실히 가장 제한적인 조치와 가장 덜 제한적인 조치가 없을 수 있습니다.)

관련 주제

- 병합된 카테고리 - 예, 9-6페이지.

병합된 카테고리 - 예

다음은 정책에 대한 URL 필터링 페이지의 설정에 따른 병합된 카테고리의 몇 가지 예입니다.

원래 카테고리 1	원래 카테고리 2	분류되지 않은 URL	병합된 카테고리
모니터링	모니터링	(해당 없음)	모니터링
차단	차단	(해당 없음)	차단
전역 설정 사용	전역 설정 사용	(해당 없음)	전역 설정 사용
경고	차단	모니터링 원래 카테고리 중에서 가장 덜 제한적인 카테고리를 사용합니다.	경고

원래 카테고리 1	원래 카테고리 2	분류되지 않은 URL	병합된 카테고리
모니터링	• 차단 또는 • 전역 설정 사용, 전역이 차단으로 설정된 경우	• 차단 또는 • 전역이 차단으로 설정된 경우 전역 설정 사용 원래 카테고리 중에서 가장 제한적인 카테고리를 사용합니다.	차단
차단	• 모니터링 또는 • 전역 설정 사용, 전역이 모니터링으로 설정된 경우	• 모니터링 또는 • 전역이 모니터링으로 설정된 경우 전역 설정 사용 원래 카테고리 중에서 가장 덜 제한적인 카테고리를 사용합니다.	모니터링
구성원 자격이 URL 카테고리로 정의되는 정책의 경우: 모니터링	이 카테고리의 조치는 이 정책에 지정되지 않지만 이 카테고리에 대한 전역 정책의 값은 차단입니다.	분류되지 않은 URL의 조치는 이 정책에 지정되지 않지만 분류되지 않은 URL에 대한 전역 정책의 값은 모니터링입니다.	모니터링

URL 카테고리 집합에 대한 업데이트 제어

기본적으로 URL 카테고리 집합 업데이트는 자동으로 발생합니다. 이러한 업데이트는 기존 정책 컨피그레이션을 변경할 수 있으므로 모든 자동 업데이트를 사용하지 않도록 설정하는 것을 선호할 수도 있습니다.

옵션	방법
업데이트를 사용하지 않도록 설정하면 System Administration(시스템 관리) > Upgrade and Update Settings(업그레이드 및 업데이트 설정) 페이지의 Update Servers(업데이트 서버)(목록) 섹션에 나열된 모든 서비스를 수동으로 업데이트해야 합니다.	수동으로 URL 카테고리 집합 업데이트, 9-8페이지 및 수동으로 보안 서비스 구성 요소 업데이트, 22-29페이지
모든 자동 업데이트 사용 안 함	업그레이드 및 서비스 업데이트 설정 구성, 22-32페이지.

참고 CLI를 사용하는 경우 업데이트 간격을 영(0)으로 설정하여 업데이트를 사용하지 않도록 설정하십시오.

수동으로 URL 카테고리 집합 업데이트

참고 진행 중인 업데이트를 중단하지 마십시오.

자동 업데이트를 사용하지 않도록 설정한 경우 편의에 따라 수동으로 URL 카테고리 집합을 업데이트할 수 있습니다.

1단계 **Security Services(보안 서비스) > Acceptable Use Controls(제한적 사용 제어)**를 선택합니다.

2단계 다음을 수행하여 업데이트가 사용 가능한지 확인합니다.

Acceptable Use Controls Engine Updates(제한적 사용 제어 엔진 업데이트) 표의 "Cisco Web Usage Controls - Web Categorization Categories List(웹 분류 카테고리 목록)" 항목을 살펴봅니다.

3단계 업데이트하려면 **Update Now(지금 업데이트)**를 클릭합니다.

새 카테고리 및 변경된 카테고리에 대한 기본 설정

URL 카테고리 집합 업데이트로 인해 기존 정책의 동작이 변경될 수 있습니다. URL 카테고리 집합 업데이트가 발생할 때 준비가 될 수 있도록 정책 구성 시 특정 변경 사항의 기본 설정을 지정해야 합니다. 새 카테고리가 추가되거나 기존 카테고리가 새 카테고리로 병합되는 경우 각 정책에 대한 이러한 카테고리의 기본 조치는 해당 정책의 분류되지 않은 URL 설정에 의해 영향을 받습니다.

기존 설정 확인 및/또는 변경

1단계 **Web Security Manager(웹 보안 관리자)**를 선택합니다.

2단계 각 액세스 정책, 암호 해독 정책 및 Cisco 데이터 보안 정책의 경우 **URL Filtering(URL 필터링)** 링크를 클릭합니다.

3단계 분류되지 않은 URL에 대한 선택된 설정을 확인합니다.

관련 주제

- URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향, 17-6페이지.

카테고리 및 정책 변경에 대한 경고 수신

카테고리 집합 업데이트는 두 가지 유형의 경고를 트리거합니다.

- 카테고리 변경에 대한 경고
- 카테고리 집합 변경의 결과로 변경되거나 사용하지 않도록 설정된 정책에 대한 경고

1단계 **System Administration(시스템 관리)> Alerts(경고)**를 선택합니다.

2단계 **Add Recipient(수신자 추가)**를 클릭하고 이메일 주소(또는 여러 개의 이메일 주소)를 추가합니다.

3단계 수신할 **Alert Types(경고 유형)** 및 **Alert Severities(경고 심각도)**를 결정합니다.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

URL 카테고리 집합 업데이트에 대한 경고에 응답

카테고리 집합 변경에 대한 경고를 수신하는 경우 다음을 수행해야 합니다.

- 카테고리 병합, 추가 및 삭제 후에 정책과 ID가 여전히 정책 목표를 충족하는지 확인합니다.
- 새 카테고리와 추가된 분할 카테고리의 세분성을 활용하도록 정책 및 ID를 수정하는 것을 고려합니다.

관련 주제

- URL 카테고리 집합 업데이트의 영향 이해, 9-5페이지

URL 카테고리를 사용하여 트랜잭션 필터링

URL 필터링 엔진을 사용하여 액세스, 암호 해독 및 데이터 보안 정책의 트랜잭션을 필터링할 수 있습니다. 정책 그룹에 대한 URL 카테고리를 구성할 때 맞춤형 URL 카테고리(정의된 경우) 및 미리 정의된 URL 카테고리에 대한 조치를 구성할 수 있습니다.

구성할 수 있는 URL 필터링 조치는 정책 그룹의 유형에 따라 다릅니다.

옵션	방법
액세스 정책	액세스 정책 그룹에 대한 URL 필터 구성, 9-9페이지
암호 해독 정책	암호 해독 정책 그룹에 대한 URL 필터 구성, 9-11페이지
Cisco 데이터 보안 정책	데이터 보안 정책 그룹에 대한 URL 필터 구성, 9-12페이지

관련 주제

- 액세스 정책의 트래픽 리디렉션, 9-17페이지.
- 사용자에게 경고하고 계속하도록 허용, 9-18페이지
- 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지
- URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향, 9-5페이지

액세스 정책 그룹에 대한 URL 필터 구성

사용자 정의 액세스 정책 그룹과 전역 정책 그룹에 대한 URL 필터링을 구성할 수 있습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 URL Filtering(URL 필터링) 열 아래의 링크를 클릭합니다.

3단계 (선택 사항) Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에서 조치를 수행할 맞춤형 URL 카테고리를 이 정책에 추가할 수 있습니다.

a. **Select Custom Categories(맞춤형 카테고리 선택)**를 클릭합니다.

b. 이 정책에 포함할 맞춤형 URL 카테고리를 선택하고 **Apply(적용)**를 클릭합니다.

URL 필터링 엔진이 클라이언트 요청과 비교해야 하는 맞춤형 URL 카테고리를 선택합니다. URL 필터링 엔진은 클라이언트 요청을 포함된 맞춤형 URL 카테고리와 비교하고 제외된 맞춤형 URL 카테고리는 무시합니다. URL 필터링 엔진은 클라이언트 요청의 URL을 미리 정의된 URL 카테고리와 비교하기 전에 포함된 맞춤형 URL 카테고리와 비교합니다.

정책에 포함된 맞춤형 URL 카테고리는 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에 표시됩니다.

4단계 **Custom URL Category Filtering(맞춤형 URL 카테고리 필터링)** 섹션에서 각각의 포함된 맞춤형 URL 카테고리에 대한 조치를 선택합니다.

작업	설명
전역 설정 사용	전역 정책 그룹의 이 카테고리에 대한 조치를 사용합니다. 이는 사용자 정의 정책 그룹에 대한 기본 조치입니다. 사용자 정의 정책 그룹에만 적용됩니다. **참고** 맞춤형 URL 카테고리가 전역 액세스 정책에서 제외되는 경우 사용자 정의 액세스 정책에 포함된 맞춤형 URL 카테고리에 대한 기본 조치는 Use Global Settings(전역 설정 사용)가 아니라 Monitor(모니터링)입니다. 맞춤형 URL 카테고리가 전역 액세스 정책에서 제외된 경우에는 Use Global Settings(전역 설정 사용)를 선택할 수 없습니다.
차단	웹 프록시가 이 설정과 일치하는 트랜잭션을 거부합니다.
리디렉션	원래 이 카테고리의 URL로 지정된 트래픽을 사용자가 지정하는 위치로 리디렉션합니다. 이 조치를 선택하면 Redirect To(리디렉션 대상) 필드가 표시됩니다. 모든 트래픽을 리디렉션할 URL을 입력합니다.
허용	이 카테고리의 웹 사이트에 대한 클라이언트 요청을 항상 허용합니다. 허용된 요청은 모든 추가 필터링 및 악성코드 스캐닝을 우회합니다. 신뢰할 수 있는 웹 사이트에만 이 설정을 사용하십시오. 내부 사이트에 이 설정을 사용할 수 있습니다.
모니터링	웹 프록시가 요청을 허용하거나 차단하지 않습니다. 대신, 계속해서 다른 정책 그룹 제어 설정(예: 웹 평판 필터링)과 비교하여 클라이언트 요청을 평가합니다.
경고	웹 프록시가 처음에는 요청을 차단하고 경고 페이지를 표시하지만 사용자가 경고 페이지의 하이퍼텍스트 링크를 클릭하여 계속할 수 있도록 합니다.
할당량 기반	개별 사용자가 지정한 볼륨 또는 시간 할당량에 접근하면 경고가 표시됩니다. 할당량이 충족된 경우 차단 페이지가 표시됩니다. 시간 범위 및 할당량, 10-12페이지를 참조하십시오.
시간 기반	사용자가 지정하는 시간 범위 동안 웹 프록시에서 요청을 차단하거나 모니터링합니다. 시간 범위 및 할당량, 10-12페이지를 참조하십시오.

5단계 Predefined URL Category Filtering(미리 정의된 URL 카테고리 필터링) 섹션에서 각 카테고리에 대해 다음 조치 중 하나를 선택합니다.

- 전역 설정 사용
- 모니터링
- 경고
- 차단
- 시간 기반
- 할당량 기반

6단계 Uncategorized URL(분류되지 않은 URL) 섹션에서 맞춤형 또는 미리 정의된 URL 카테고리에 해당하지 않는 웹 사이트에 대한 클라이언트 요청에 수행할 조치를 선택합니다. 또한 이 설정에 따라 URL 카테고리 집합 업데이트로 인해 발생하는 새 카테고리 및 병합된 카테고리의 기본 조치가 결정됩니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

암호 해독 정책 그룹에 대한 URL 필터 구성

사용자 정의 암호 해독 정책 그룹과 전역 암호 해독 정책 그룹에 대한 URL 필터링을 구성할 수 있습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 URL Categories(URL 카테고리) 열 아래의 링크를 클릭합니다.

3단계 (선택 사항) Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에서 조치를 수행할 맞춤형 URL 카테고리를 이 정책에 추가할 수 있습니다.

a. **Select Custom Categories(맞춤형 카테고리 선택)**를 클릭합니다.

b. 이 정책에 포함할 맞춤형 URL 카테고리를 선택하고 **Apply(적용)**를 클릭합니다.

URL 필터링 엔진이 클라이언트 요청과 비교해야 하는 맞춤형 URL 카테고리를 선택합니다. URL 필터링 엔진은 클라이언트 요청을 포함된 맞춤형 URL 카테고리와 비교하고 제외된 맞춤형 URL 카테고리는 무시합니다. URL 필터링 엔진은 클라이언트 요청의 URL을 미리 정의된 URL 카테고리와 비교하기 전에 포함된 맞춤형 URL 카테고리와 비교합니다.

정책에 포함된 맞춤형 URL 카테고리는 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에 표시됩니다.

4단계 각 맞춤형 및 미리 정의된 URL 카테고리에 대한 조치를 선택합니다.

작업	설명
전역 설정 사용	전역 암호 해독 정책 그룹의 이 카테고리에 대한 조치를 사용합니다. 이는 사용자 정의 정책 그룹에 대한 기본 조치입니다. 사용자 정의 정책 그룹에만 적용됩니다. 맞춤형 URL 카테고리가 전역 암호 해독 정책에서 제외되는 경우 사용자 정의 암호 해독 정책에 포함된 맞춤형 URL 카테고리에 대한 기본 조치는 Use Global Settings(전역 설정 사용)가 아니라 Monitor(모니터링)입니다. 맞춤형 URL 카테고리가 전역 암호 해독 정책에서 제외된 경우에는 Use Global Settings(전역 설정 사용)를 선택할 수 없습니다.
통과	트래픽 콘텐츠를 검사하지 않고 클라이언트와 서버 간의 연결을 통과합니다.
모니터링	웹 프록시가 요청을 허용하거나 차단하지 않습니다. 대신, 계속해서 다른 정책 그룹 제어 설정(예: 웹 평판 필터링)과 비교하여 클라이언트 요청을 평가합니다.
암호 해독	연결을 허용하지만 트래픽 콘텐츠를 검사합니다. 어플라이언스가 트래픽의 암호를 해독하고 일반 텍스트 HTTP 연결인 것처럼 암호 해독된 트래픽에 액세스 정책을 적용합니다. 연결 암호를 해독하고 액세스 정책을 적용하여 트래픽에서 악성코드를 스캐닝할 수 있습니다.
삭제	연결을 끊고 연결 요청을 서버로 전달하지 않습니다. 어플라이언스가 연결을 삭제했다고 사용자에게 알리지 않습니다.

참고 HTTPS 요청에 대해 특정 URL 카테고리를 *차단*하려는 경우 암호 해독 정책 그룹에서 해당 URL 카테고리를 암호 해독하도록 선택한 후 액세스 정책 그룹에서 동일한 URL 카테고리를 차단하도록 선택합니다.

5단계 Uncategorized URL(분류되지 않은 URL) 섹션에서 맞춤형 또는 미리 정의된 URL 카테고리에 해당하지 않는 웹 사이트에 대한 클라이언트 요청에 수행할 조치를 선택합니다.

또한 이 설정에 따라 URL 카테고리 집합 업데이트로 인해 발생하는 새 카테고리 및 병합된 카테고리의 기본 조치가 결정됩니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

데이터 보안 정책 그룹에 대한 URL 필터 구성

사용자 정의 데이터 보안 정책 그룹과 전역 정책 그룹에 대한 URL 필터링을 구성할 수 있습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Cisco Data Security(Cisco 데이터 보안)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 URL Categories(URL 카테고리) 열 아래의 링크를 클릭합니다.

3단계 (선택 사항) Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에서 조치를 수행할 맞춤형 URL 카테고리를 이 정책에 추가할 수 있습니다.

a. **Select Custom Categories(맞춤형 카테고리 선택)**를 클릭합니다.

b. 이 정책에 포함할 맞춤형 URL 카테고리를 선택하고 **Apply(적용)**를 클릭합니다.

URL 필터링 엔진이 클라이언트 요청과 비교해야 하는 맞춤형 URL 카테고리를 선택합니다. URL 필터링 엔진은 클라이언트 요청을 포함된 맞춤형 URL 카테고리와 비교하고 제외된 맞춤형 URL 카테고리는 무시합니다. URL 필터링 엔진은 클라이언트 요청의 URL을 미리 정의된 URL 카테고리와 비교하기 전에 포함된 맞춤형 URL 카테고리와 비교합니다.

정책에 포함된 맞춤형 URL 카테고리는 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에 표시됩니다.

4단계 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에서 각 맞춤형 URL 카테고리에 대한 조치를 선택합니다.

작업	설명
전역 설정 사용	전역 정책 그룹의 이 카테고리에 대한 조치를 사용합니다. 이는 사용자 정의 정책 그룹에 대한 기본 조치입니다. 사용자 정의 정책 그룹에만 적용됩니다. 맞춤형 URL 카테고리가 전역 Cisco 데이터 보안 정책에서 제외되는 경우 사용자 정의 Cisco 데이터 보안 정책에 포함된 맞춤형 URL 카테고리에 대한 기본 조치는 Use Global Settings(전역 설정 사용)가 아니라 Monitor(모니터링)입니다. 맞춤형 URL 카테고리가 전역 Cisco 데이터 보안 정책에서 제외된 경우에는 Use Global Settings(전역 설정 사용)를 선택할 수 없습니다.
허용	이 카테고리의 웹 사이트에 대한 업로드 요청을 항상 허용합니다. 맞춤형 URL 카테고리에만 적용됩니다. 허용된 요청은 모든 추가 데이터 보안 스캐닝을 우회하고 요청이 액세스 정책과 비교하여 평가됩니다. 신뢰할 수 있는 웹 사이트에만 이 설정을 사용하십시오. 내부 사이트에 이 설정을 사용할 수 있습니다.
모니터링	웹 프록시가 요청을 허용하거나 차단하지 않습니다. 대신, 계속해서 다른 정책 그룹 제어 설정(예: 웹 평판 필터링)에 대해 업로드 요청을 평가합니다.
차단	웹 프록시가 이 설정과 일치하는 트랜잭션을 거부합니다.

5단계 Predefined URL Category Filtering(미리 정의된 URL 카테고리 필터링) 섹션에서 각 카테고리에 대해 다음 조치 중 하나를 선택합니다.

- 전역 설정 사용
- 모니터링
- 차단

6단계 Uncategorized URL(분류되지 않은 URL) 섹션에서 맞춤형 또는 미리 정의된 URL 카테고리에 해당하지 않는 웹 사이트에 대한 업로드 요청에 수행할 조치를 선택합니다. 또한 이 설정에 따라 URL 카테고리 집합 업데이트로 인해 발생하는 새 카테고리 및 병합된 카테고리의 기본 조치가 결정됩니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- URL 카테고리 집합 업데이트가 정책의 필터링 조치에 미치는 영향, 9-5페이지.

맞춤형 URL 카테고리 생성 및 편집

특정 호스트 이름 및 IP 주소를 지정하는 사용자 정의 맞춤형 URL 카테고리를 생성할 수도 있습니다. 또한 기존 URL 카테고리를 편집하고 삭제할 수 있습니다. 이러한 맞춤형 URL 카테고리를 동일한 액세스, 암호 해독 또는 Cisco 데이터 보안 정책 그룹에 포함하고 각 카테고리에 다른 조치를 정의하는 경우 포함된 상위 맞춤형 URL 카테고리의 조치가 적용됩니다.

참고 웹 보안 어플라이언스는 액세스 로그에서 앞에 "c_"가 있는 맞춤형 URL 카테고리 이름의 처음 4개 문자를 사용합니다. Sawmill for를 사용하여 액세스 로그를 구문 분석하는 경우 맞춤형 URL 카테고리 이름을 고려하십시오. 맞춤형 URL 카테고리의 처음 4개 문자에 공백이 포함되어 있으면 Sawmill for에서 액세스 로그 항목을 적절히 구문 분석할 수 없습니다. 대신, Sawmill for를 사용하여 액세스 로그를 구문 분석할 경우에는 처음 4개 문자에 지원되는 문자만 사용하십시오. 맞춤형 URL 카테고리의 전체 이름을 액세스 로그에 포함하려면 %XF 형식 지정자를 액세스 로그에 추가합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Custom URL Categories(맞춤형 URL 카테고리)**를 선택합니다.

2단계 맞춤형 URL 카테고리를 생성하려면 **Add Custom Category(맞춤형 카테고리 추가)**를 클릭합니다. 기존 맞춤형 URL 카테고리를 편집하려면 URL 카테고리의 이름을 클릭합니다.

3단계 맞춤형 URL 카테고리에 대한 아래 표의 설정을 입력합니다.

설정	설명
카테고리 이름	URL 카테고리의 이름을 입력합니다. 이 이름은 정책 그룹에 대한 URL 필터링을 구성할 때 표시됩니다.
목록 순서	맞춤형 URL 카테고리 목록에서 이 카테고리를 배치할 순서를 선택합니다. 가장 높은 URL 카테고리의 경우 "1"을 입력합니다. URL 필터링 엔진은 지정된 순서로 맞춤형 URL 카테고리와 비교하여 클라이언트 요청을 평가합니다.
사이트	맞춤형 카테고리에 속하는 하나 이상의 주소를 입력합니다. 줄 바꿈 기호 또는 쉼표로 구분된 여러 주소를 입력할 수 있습니다.
고급: 정규식	정규식을 사용하여 사용자가 입력하는 패턴과 일치하는 여러 웹 서버를 지정할 수 있습니다. **참고** URL 필터링 엔진이 먼저 Sites(사이트) 필드에 입력된 주소와 URL을 비교합니다. 트랜잭션의 URL이 Sites(사이트) 필드의 항목과 일치하면 여기에 입력된 식과 비교되지 않습니다. 정규식 사용에 대한 자세한 내용은 정규식, 9-20페이지를 참조하십시오.

4단계 (선택 사항) Sites(사이트) 필드의 모든 주소를 정렬하려면 **Sort URLs(URL 정렬)**를 클릭합니다.

참고 주소를 정렬하면 원래 순서로 복원할 수 없습니다.

5단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 정규식, 9-20페이지.
- 액세스 로그 맞춤화, 21-26페이지.

성인 콘텐츠 필터링

일부 웹 검색 및 웹 사이트에서 성인 콘텐츠를 필터링하도록 웹 보안 어플라이언스를 구성할 수 있습니다. 안전 검색 및 사이트 콘텐츠 등급을 시행하기 위해 AVC 엔진은 안전 모드가 강제로 설정될 수 있도록 URL 및/또는 웹 쿠키를 재작성하여 특정 웹 사이트에 구현된 안전 모드 기능을 활용합니다.

다음 기능이 성인 콘텐츠를 필터링합니다.

옵션	설명
안전 검색 시행	발신 검색 요청이 검색 엔진에 안전한 검색 요청으로 표시되도록 웹 보안 어플라이언스를 구성할 수 있습니다. 이 기능은 사용자가 검색 엔진을 사용하여 사용 정책을 우회하지 못하도록 합니다.
사이트 콘텐츠 등급 시행	일부 콘텐츠 공유 사이트에서는 사용자가 고유한 안전 검색 기능을 적용하거나, 성인 콘텐츠에 대한 액세스를 차단하거나, 둘 다를 수행하여 이러한 사이트에 있는 성인 콘텐츠에 대한 자체 액세스를 제한할 수 있습니다. 이 분류 기능을 일반적으로 콘텐츠 등급이라고 합니다.

참고 안전 검색 또는 사이트 콘텐츠 등급 기능이 사용하도록 설정된 액세스 정책이 안전한 검색 액세스 정책으로 간주됩니다.

안전 검색 및 사이트 콘텐츠 등급 시행

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 URL Categories(URL 카테고리) 열 아래에서 액세스 정책 그룹 또는 전역 정책 그룹에 해당하는 링크를 클릭합니다.

3단계 사용자 정의 액세스 정책을 편집할 때 Content Filtering(콘텐츠 필터링) 섹션에서 **Define Content Filtering Custom Settings(콘텐츠 필터링 맞춤형 설정 정의)**를 선택합니다.

4단계 안전 검색 기능을 사용하도록 설정하려면 **Enable Safe Search(안전 검색 사용)** 확인란을 클릭합니다.

5단계 현재 웹 보안 어플라이언스 안전 검색 기능에서 지원되지 않는 사용자를 검색 엔진에서 차단할지 여부를 선택합니다.

6단계 사이트 콘텐츠 등급 기능을 사용하도록 설정하려면 **Enable Site Content Rating(사이트 콘텐츠 등급 사용)** 확인란을 클릭합니다.

7단계 지원되는 콘텐츠 등급 웹 사이트에서 모든 성인 콘텐츠를 차단하거나 최종 사용자 URL 필터링 경고 페이지를 표시할지 선택합니다.

참고 지원되는 검색 엔진 또는 지원되는 콘텐츠 등급 웹 사이트 중 하나의 URL이 허용 조치가 적용된 맞춤형 URL 카테고리에 포함된 경우에는 검색 결과가 차단되지 않고 모든 콘텐츠가 표시됩니다.

8단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 사용자에게 경고하고 계속하도록 허용, 9-18페이지
- 웹 애플리케이션에 대한 액세스 제어, 17-18페이지

성인 콘텐츠 액세스 기록

기본적으로 액세스 로그에는 각 항목의 안전 검색 스캐닝 판정이 꺾쇠괄호 안에 포함됩니다. 안전 검색 스캐닝 판정은 안전 검색 또는 사이트 콘텐츠 등급 기능이 트랜잭션에 적용되었는지 여부를 표시합니다. 또한 액세스 로그 또는 W3C 액세스 로그에 안전 검색 스캐닝 판정 변수를 추가할 수도 있습니다.

- 액세스 로그: %XS
- W3C 액세스 로그: x-request-rewrite

값	설명
ensrch	원래 클라이언트 요청이 안전하지 않았으며 안전 검색 기능이 적용되었습니다.
encrt	원래 클라이언트 요청이 안전하지 않았으며 사이트 콘텐츠 등급 기능이 적용되었습니다.
unsupp	원래 클라이언트 요청이 지원되지 않는 검색 엔진에 대한 것이었습니다.
err	원래 클라이언트 요청이 안전하지 않았지만 오류로 인해 안전 검색 및 사이트 콘텐츠 등급 기능을 모두 적용할 수 없었습니다.
-	기능이 무시되었거나(예를 들어, 트랜잭션이 맞춤형 URL 카테고리에서 허용됨) 지원되지 않는 애플리케이션에서 요청이 작성되었기 때문에 안전 검색 및 사이트 콘텐츠 등급 기능이 모두 클라이언트 요청에 적용되지 않았습니다.

안전 검색 또는 사이트 콘텐츠 등급 기능으로 인해 요청이 차단되면 액세스 로그에서 다음 ACL 결정 태그 중 하나를 사용합니다.

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

관련 주제

- ACL 결정 태그, 21-17페이지.

액세스 정책의 트래픽 리디렉션

원래 맞춤형 URL 카테고리의 URL로 대상이 지정된 트래픽을 사용자가 지정하는 위치로 리디렉션하도록 Web Security appliance를 구성할 수 있습니다. 이렇게 하면 목적지 서버 대신에 애플리케이션에서 트래픽을 리디렉션할 수 있습니다. 맞춤형 액세스 정책 그룹 또는 전역 정책 그룹에 대한 트래픽을 리디렉션할 수 있습니다.

시작하기 전에

- 트래픽을 리디렉션하려면 하나 이상의 맞춤형 URL 카테고리를 정의해야 합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 URL Categories(URL 카테고리) 열 아래에서 액세스 정책 그룹 또는 전역 정책 그룹에 해당하는 링크를 클릭합니다.

3단계 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에서 **Select Custom Categories(맞춤형 카테고리 선택)**를 클릭합니다.

4단계 **Select Custom Categories for this Policy(이 정책의 맞춤형 카테고리 선택)** 대화 상자에서 리디렉션할 맞춤형 URL 카테고리에 대한 **Include in policy(정책에 포함)**를 선택합니다.

5단계 **Apply(적용)**를 클릭합니다.

6단계 리디렉션할 맞춤형 카테고리에 대한 **Redirect(리디렉션)** 열을 클릭합니다.

7단계 맞춤형 카테고리에 대한 **Redirect To(리디렉션 대상)** 필드에 트래픽을 리디렉션할 대상 URL을 입력합니다.

8단계 **변경 사항을 제출** 및 **커밋합니다**.

참고 트래픽을 리디렉션하도록 어플라이언스를 구성할 때 무한 루프에 주의하십시오.

관련 주제

- 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지

기록 및 보고

트래픽을 리디렉션하는 경우 원래 요청된 웹 사이트에 대한 액세스 로그 항목에 REDIRECT_CUSTOMCAT으로 시작하는 ACL 태그가 있습니다. 이후 액세스 로그(일반적으로 다음 행)에 사용자가 리디렉션된 웹 사이트에 대한 항목이 표시됩니다.

Reporting(보고) 탭에 표시되는 보고서에 리디렉션된 트랜잭션이 "Allowed(허용됨)"로 표시됩니다.

사용자에게 경고하고 계속하도록 허용

사이트가 조직의 사용 정책을 충족하지 않는다고 사용자에게 경고할 수 있습니다. 인증을 통해 사용자 이름이 사용 가능하게 된 경우에는 액세스 로그에서 사용자 이름으로 사용자를 추적하고 사용자 이름이 사용 불가능한 경우에는 IP 주소로 추적합니다.

다음 방법 중 하나를 사용하여 사용자에게 경고하고 계속 진행하도록 허용할 수 있습니다.

- 액세스 정책 그룹의 URL 카테고리에 대해 경고 조치를 선택합니다. 또는
- 사이트 콘텐츠 등급 기능을 사용하도록 설정하고 사용자를 차단하는 대신 성인 콘텐츠에 액세스하는 사용자에게 경고를 표시합니다.

최종 사용자 필터링 경고 페이지에 대한 설정 구성

참고 경고 후 계속 기능은 HTTP 및 암호 해독된 HTTPS 트랜잭션에 대해서만 작동합니다. 네이티브 FTP 트랜잭션에서 대해서는 작동하지 않습니다.

참고 URL 필터링 엔진이 사용자에게 특정 요청에 대해 경고할 때 웹 프록시가 최종 사용자에게 전송하는 경고 페이지를 제공합니다. 그러나 모든 웹 사이트가 최종 사용자에게 경고 페이지를 표시하지는 않습니다. 이러한 경우에는 어떤 방식으로든 사이트에 계속 액세스할 수 있는 기회를 제공하지 않고 경고 옵션이 할당된 URL에서 사용자가 차단됩니다.

1단계 **Security Services(보안 서비스) > End-User Notification(최종 사용자 알림)**을 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **End-User Filtering Warning(최종 사용자 필터링 경고)** 페이지에서 다음 설정을 구성합니다.

옵션	방법
경고 간격	Time Between Warning(경고 간격)에 따라 사용자별로 웹 프록시가 각 URL 카테고리에 대한 최종 사용자 URL 필터링 경고 페이지를 표시하는 빈도가 결정됩니다. 이 설정은 사용자 이름으로 추적된 사용자와 IP 주소로 추적된 사용자에 적용됩니다. 30초에서 2678400초(1개월) 사이의 값을 지정합니다. 기본값은 1시간(3600초)입니다.
맞춤형 메시지	맞춤형 메시지는 모든 최종 사용자 URL 필터링 경고 페이지에 표시되는 사용자 입력 텍스트입니다. 텍스트 형식을 지정하기 위해 몇 가지 단순 HTML 태그를 포함합니다.

4단계 **Submit(제출)**를 클릭합니다.

관련 항목

- 성인 콘텐츠 필터링, 9-15페이지
- 알림 페이지의 맞춤형 메시지, 17-10페이지
- 최종 사용자 URL 필터링 경고 페이지 구성, 17-9페이지

시간 기반 URL 필터 생성

웹 보안 어플라이언스에서 특정 카테고리의 URL에 대한 요청을 시간 및 일에 따라 다르게 처리하는 방법을 구성할 수 있습니다.

시작하기 전에

Web Security Manager(웹 보안 관리자) > Defined Time Range(정의된 시간 범위) 페이지로 이동하여 하나 이상의 시간 범위를 정의합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 URL Categories(URL 카테고리) 열 아래의 링크를 클릭합니다.

3단계 시간 범위에 따라 구성하려는 맞춤형 또는 미리 정의된 URL 카테고리에 대한 **Time-Based(시간 기반)**를 선택합니다.

4단계 **Time Range(시간 범위)** 필드에서 URL 카테고리에 사용할 정의된 시간 범위를 선택합니다.

5단계 **Action(조치)** 필드에서 정의된 시간 범위 동안 이 URL 카테고리의 트랜잭션에 대해 수행할 조치를 선택합니다.

6단계 **Otherwise(기타 경우)** 필드에서 정의된 시간 범위 *외부에서* 이 URL 카테고리의 트랜잭션에 대해 수행할 조치를 선택합니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 시간 범위 및 할당량, 10-12페이지

URL 필터링 활동 보기

Reporting(보고) > URL Categories(URL 카테고리) 페이지는 일치하는 상위 URL 카테고리 및 차단된 상위 URL 카테고리에 대한 정보를 포함하는 URL 통계의 통합 표시를 제공합니다. 이 페이지에는 대역폭 절감 및 웹 트랜잭션에 대한 카테고리별 데이터가 표시됩니다.

관련 주제

- 최종 사용자 활동을 모니터링하기 위한 보고서 생성, 18-1페이지

필터링되지 않고 분류되지 않은 데이터 이해

Reporting(보고) > URL Categories(URL 카테고리) 페이지에서 URL 통계를 볼 때 다음 데이터를 해석하는 방법을 이해하는 것이 중요합니다.

데이터 유형	설명
무시된 URL 필터	URL 필터링 전에 발생하는 정책, 포트 및 관리 사용자 에이전트 차단을 나타냅니다.
분류되지 않은 URL	URL 필터링 엔진이 쿼리되었지만 카테고리가 일치되지 않은 모든 트랜잭션을 나타냅니다.

액세스 로그의 URL 카테고리 기록

액세스 로그 파일은 각 항목의 스캐닝 판정 정보 섹션에서 각 트랜잭션에 대한 URL 카테고리를 기록합니다.

관련 주제

- 로그를 통해 시스템 활동 모니터링, 21-1페이지.
- URL 카테고리 설명, 9-23페이지.

정규식

웹 보안 어플라이언스는 다른 속도 패턴 일치 엔진 구현에서 사용되는 정규식 구문과 약간 다른 정규식 구문을 사용합니다. 또한 어플라이언스에서는 백슬래시를 사용하여 슬래시를 이스케이프하도록 지원하지 않습니다. 정규식에서 슬래시를 사용해야 하는 경우 백슬래시 없이 슬래시를 입력하면 됩니다.

참고 기술적으로 AsyncOS for Web은 Flex 정규식 분석기를 사용합니다. Flex 정규식 분석기에서 정규식을 읽는 방법에 대한 자세한 내용은 http://flex.sourceforge.net/manual/Patterns.html을 참조하십시오.

다음 위치에서 정규식을 사용할 수 있습니다.

- **액세스 정책에 대한 맞춤형 URL 카테고리.** 액세스 정책 그룹에 사용할 맞춤형 URL 카테고리를 생성할 때 정규식을 사용하여 사용자가 입력하는 패턴과 일치하는 여러 웹 서버를 지정할 수 있습니다.
- **차단할 맞춤형 사용자 에이전트.** 액세스 정책 그룹에 대해 차단할 애플리케이션을 편집할 때 정규식을 사용하여 차단할 특정 사용자 에이전트를 입력할 수 있습니다.

참고 광범위한 문자 일치를 수행하는 정규식은 리소스를 사용하고 시스템 성능에 영향을 줄 수 있습니다. 이러한 이유로 정규식은 신중하게 적용되어야 합니다.

관련 주제

- 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지
- 정책: 프로토콜 및 사용자 에이전트, 9-13페이지

정규식 형성

정규식은 일반적으로 식에서 "일치"라는 단어를 사용하는 규칙입니다. 특정 URL 대상 또는 웹 서버를 일치시키기 위해 정규식을 적용할 수 있습니다. 예를 들어, 다음 정규식은 "`blocksite.com`"을 포함하는 모든 패턴과 일치합니다.

```
\.blocksite\.com
```

다음과 같은 정규식이 있다고 가정합니다.

```
server[0-9]\.example\.com
```

이 예에서 `server[0-9]`는 `example.com` 도메인의 `server0`, `server1`, `server2`, ..., `server9`와 일치합니다.

다음 예에서는 정규식이 `downloads` 디렉토리에 있는 `.exe`, `.zip` 및 `.bin`으로 끝나는 파일과 일치합니다.

```
/downloads/.*\.(exe|zip|bin)
```

참고 공백 문자 또는 영숫자가 아닌 문자를 포함하는 정규식은 ASCII 따옴표로 묶어야 합니다.

검증 실패를 방지하기 위한 지침

검증 실패를 최소화하려면 다음 지침에 따르십시오.

- 가능하면 와일드카드 및 대괄호를 사용하는 식보다는 리터럴 식을 사용하십시오. 리터럴 표현식은 기본적으로 직설적인 텍스트입니다(예: "`It's as easy as ABC123`"). "`It's as easy as [A-C]{3}[1-3]{3}`"를 사용하는 것보다 실패할 확률이 더 적습니다. 후자의 식은 NFA(Non-Deterministic Finite Automatons) 항목을 생성하여 처리 시간이 크게 증가할 수 있습니다.
- 가능하면 이스케이프되지 않은 마침표의 사용을 피하십시오. 마침표는 줄 바꿈 문자를 제외한 모든 문자와 일치하는 것을 의미하는 특수 정규식 문자입니다. 실제 마침표를 일치시키려면(예: "`url.com`") \ 문자를 사용하여 마침표를 이스케이프합니다(예: "`url\.com`"). 이스케이프된 마침표는 리터럴 항목으로 처리되므로 문제를 발생시키지 않습니다.

  마찬가지로, 가능하면 이스케이프되지 않은 마침표보다는 더 구체적인 일치를 사용하십시오. 예를 들어, 뒤에 단일 숫자가 있는 URL을 일치시키려면 "`url.`"보다는 "`url[0-9]`"를 사용하십시오.
- 특히 규모가 큰 정규식에서 이스케이프되지 않은 마침표를 사용하면 문제가 발생할 수 있으므로 피해야 합니다. 예를 들어, "`Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual`"을 사용하면 오류가 발생할 수 있습니다. "`.qual`"에서 마침표를 리터럴 "`equal`"로 바꾸면 문제가 해결됩니다.

  또한 마침표 다음에 63개를 초과하는 문자를 반환하는 패턴의 이스케이프되지 않은 마침표는 패턴 일치 엔진에 의해 사용하지 않도록 설정됩니다. 패턴을 정정하거나 바꾸십시오.
- "`.*`"를 사용하여 정규식을 시작하거나 종료할 수 없습니다. 또한 URL을 일치시키기 위한 정규식에서 "./"를 사용할 수 없으며 마침표로 이러한 정규식을 종료할 수 없습니다.

- 와일드카드와 대괄호 식을 조합하면 문제가 발생할 수 있습니다. 가능한 한 많은 조합을 제거하십시오. 예를 들어, "`id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$`"는 오류를 발생시키지만 "`Gecko/20100101 Firefox/9\.0\.1\$`"는 그렇지 않습니다. 후자의 식은 와일드카드 또는 대괄호 식을 포함하지 않으며 두 식 모두 이스케이프된 마침표만 사용합니다.

  와일드카드 및 대괄호 식을 제거할 수 없는 경우 식의 크기와 복잡도를 줄이십시오. 예를 들어 "`[0-9a-z]{64}`"는 오류를 발생시킬 수 있습니다. 이를 더 작거나 덜 복잡한 식으로 변경하면 문제가 해결될 수 있습니다(예: "`[0-9]{64}`" 또는 "`[0-9a-z]{40}`").

오류가 발생하는 경우 와일드카드(예: *, + .) 및 대괄호가 사용된 식에 이러한 규칙을 적용하여 해결하십시오.

정규식 문자 표

메타-문자	설명
.	줄 바꿈 문자(0x0A)를 제외한 모든 단일 문자와 일치합니다. 예를 들어, 정규식 `r.t`는 문자열 rat, rut, r t와 일치하지만 root와는 일치하지 않습니다. 긴 패턴에서(특히 긴 패턴의 중간에) 이스케이프된 문자를 사용할 때 주의하십시오. 자세한 내용은 검증 실패를 방지하기 위한 지침, 9-21페이지를 참조하십시오.
*	바로 앞의 문자가 0번 이상 연속으로 나열된 문자열과 일치합니다. 예를 들어, 정규식 `.*`는 임의의 문자열과 일치하며 `[0-9]*`는 임의의 숫자 문자열과 일치합니다. 특히 마침표 문자와 함께 이 메타 문자를 사용할 때 주의하십시오. 마침표 뒤에 63개를 초과하는 문자가 반환되는 이스케이프되지 않은 마침표를 포함하는 패턴은 사용하지 않도록 설정됩니다. 자세한 내용은 검증 실패를 방지하기 위한 지침, 9-21페이지를 참조하십시오.
\	다음에 오는 메타 문자를 일반 문자로 처리하는 이스케이프 문자입니다. 예를 들어, `\^`은 행의 시작이 아니라 캐럿 문자(^)를 일치시키는 데 사용됩니다. 마찬가지로, 식 `\.`는 단일 문자가 아니라 실제 마침표를 일치시키는 데 사용됩니다.
^	행의 시작과 일치합니다. 예를 들어, 정규식 `^When in`은 "When in the course of human events" 문자열의 시작과 일치하지만 "What and when in the" 문자열의 시작과는 일치하지 않습니다.
$	행 또는 문자열의 끝과 일치합니다. 예를 들어, `b$\.`는 "b."로 끝나는 모든 행 또는 문자열과 일치합니다.
+	바로 앞의 문자 또는 정규식이 1번 이상 연속으로 나열된 문자열과 일치합니다. 예를 들어, 정규식 `9+`는 9, 99 및 999와 일치합니다.
?	선행 패턴 요소가 0번 또는 1번 발생한 문자열과 일치합니다. 예를 들어, `colou?r`에서는 "u"가 선택 사항이므로 "colour" 및 "color" 모두와 일치합니다.
( )	왼쪽 괄호와 오른쪽 괄호 사이의 식을 그룹으로 처리하여 다른 메타 문자의 범위를 제한합니다. 예를 들어, `(abc)+`는 "abcabcabc" 또는 "abc123"과 같이 문자열 "abc"가 1번 이상 발생하는 문자열과 일치하지만 "abab" 또는 "ab123"과는 일치하지 않습니다.
|	논리적 OR는 선행 패턴 또는 다음 패턴과 일치합니다. 예를 들어, `(him|her)`는 "it belongs to him" 행 및 "it belongs to her" 행과 일치하지만 "it belongs to them" 행과는 일치하지 않습니다.

메타-문자	설명
[ ]	대괄호 사이의 문자 중 하나와 일치합니다. 예를 들어, 정규식 `r[aou]t`는 "rat", "rot" 및 "rut"와 일치하지만 "ret"와는 일치하지 않습니다. 문자의 범위는 시작 문자, 하이픈 및 끝 문자로 지정됩니다. 예를 들어, 패턴 `[0-9]`는 모든 숫자와 일치됨을 의미합니다. 여러 범위를 지정할 수도 있습니다. 패턴 `[A-Za-z]`는 모든 대문자 또는 소문자와 일치함을 의미합니다. 범위(즉, 보완 범위)에 있는 문자를 제외한 모든 문자와 일치하려면 여는 대괄호 다음에 첫 번째 문자로 캐럿을 사용합니다. 예를 들어, 정규식 `[^269A-Z]`는 2, 6, 9와 대문자를 제외한 모든 문자와 일치합니다.
{ }	이전 패턴과 일치하는 횟수를 지정합니다. 예를 들면 다음과 같습니다. D{1,3}는 문자 D가 1~3번 발생하는 것과 일치합니다. 특정 수 `{n}` 또는 선행 패턴 인스턴스의 최소 수 `{n,}`와 일치합니다. 예를 들어, 표현식 `A[0-9]{3}`는 "A" 다음에 정확히 3개의 숫자가 오는 경우와 일치합니다. 즉, "A123"과 일치하지만 "A1234"와는 일치하지 않습니다. 식 `[0-9]{4,}`는 임의 순서의 4개 이상 숫자와 일치합니다.
"..."	따옴표로 묶인 모든 문자는 문자 그대로 해석합니다.

URL 카테고리 설명

이 섹션에는 Cisco Web Usage Controls의 URL 카테고리가 나열되어 있습니다. 이 표에는 액세스 로그 파일 항목의 웹 평판 필터링 및 안티멀웨어 스캐닝 섹션에 표시될 수 있는 URL 카테고리 이름의 약어도 포함되어 있습니다.

참고 액세스 로그에서는 Cisco Web Usage Controls의 URL 카테고리 약어에는 각 약어 앞에 접두사 "IW_"가 포함됩니다. 따라서 "art" 카테고리는 "IW_art"가 됩니다.

URL 카테고리	약어	코드	설명	URL 예
성인	adlt	1006	성인을 대상으로 하지만 꼭 외설적인 게시물은 아닙니다. 성인 클럽(스트립 클럽, 스와핑 클럽, 사교모임 동반 서비스, 스트리퍼), 성에 대한 일반적인 정보, 실질적으로 외설 의도가 없는 콘텐츠, 생식기 피어싱, 성인용 제품 또는 축하 카드, 건강 또는 질병 이외의 성 관련 정보가 포함될 수 있습니다.	www.adultentertainmentexpo.com www.adultnetline.com
광고	adv	1027	종종 웹 페이지가 함께 열리는 배너 및 팝업 광고, 광고 콘텐츠를 제공하는 기타 광고 웹사이트입니다. 광고 서비스 및 세일즈는 "비즈니스 및 산업"으로 분류됩니다.	www.adforce.com www.doubleclick.com

URL 카테고리	약어	코드	설명	URL 예
주류	alc	1077	즐겁게 마시는 알코올, 맥주 및 와인 제조, 칵테일 제조법, 주류 판매업체, 와이너리, 포도원, 맥주 공장, 주류 유통회사가 해당됩니다. 알코올 중독은 "건강 및 영양"으로 분류됩니다. 술집과 식당은 "식당 및 주점"으로 분류됩니다.	www.samueladams.com www.whisky.com
아트	art	1002	갤러리 및 전시회, 예술가 및 예술, 사진, 문학 및 책, 공연 예술 및 극장, 뮤지컬, 발레, 박물관, 디자인, 건축이 해당됩니다. 영화 및 TV는 "엔터테인먼트"로 분류됩니다.	www.moma.org www.nga.gov
점성술	astr	1074	점성술, 별자리, 운세, 숫자점, 심령 상담, 타로 카드가 해당됩니다.	www.astro.com www.astrology.com
경매	auct	1088	온라인 및 오프라인 경매, 경매 주택 및 분류 광고가 해당됩니다.	www.craigslist.com www.ebay.com
비즈니스 및 산업	busi	1019	마케팅, 상거래, 기업, 비즈니스 관행, 인력, 인사, 수송, 급여, 보안 및 벤처 자금, 사무용품, 산업 장비(프로세스 장비), 기계 및 기계 관련 시스템, 난방 장비, 냉방 장비, 재료 처리 장비, 포장 장비, 제조: 고형물 처리, 금속 제조, 건설 및 건축, 승객 수송, 상거래, 산업 디자인, 건설, 건축 재료, 선적 및 운송(운송 서비스, 트럭 수송, 화물 운송업체, 전세화물 수송업체, 운송 및 수송 중개업자, 특송 서비스, 적재 및 운송 대조, 추적 및 기록, 철도 운송, 해운 배송, 복합 물류 서비스, 이송 및 보관)이 해당됩니다.	www.freightcenter.com www.staples.com
채팅 및 인스턴트 메시징	chat	1040	웹 기반 인스턴트 메시징 및 채팅방이 해당됩니다.	www.icq.com www.meebo.com
부정행위 및 표절	plag	1051	기말 리포트 같은 창작물을 표절할 수 있도록 창작 과제물의 부정 도용 및 판매를 조장	www.bestessays.com www.superiorpapers.com
아동 학대 콘텐츠	cprn	1064	전 세계의 불법 아동 성 학대 콘텐츠입니다.	—
컴퓨터 보안	csec	1065	기업 및 가정 사용자를 위한 보안 제품 및 서비스를 제공합니다.	www.computersecurity.com www.symantec.com
컴퓨터 및 인터넷	comp	1003	컴퓨터 및 소프트웨어에 대한 정보로 여기에는 하드웨어, 소프트웨어, 소프트웨어 지원, 소프트웨어 엔지니어를 위한 정보, 프로그래밍 및 네트워킹, 웹 사이트 디자인, 일반적인 웹 및 인터넷 정보, 컴퓨터 공학, 컴퓨터 그래픽 및 클립아트 등이 포함됩니다. "프리웨어 및 셰어웨어"는 별도의 범주에 속합니다.	www.xml.com www.w3.org
데이트	date	1055	데이트 업체, 온라인 개인 상담 업체, 결혼중개업체가 해당됩니다.	www.eharmony.com www.match.com
디지털 엽서	card	1082	디지털 엽서 및 e-카드를 보낼 수 있는 사이트입니다.	www.all-yours.net www.delivr.net

URL 카테고리	약어	코드	설명	URL 예
식당 및 주점	food	1061	식사와 음주가 가능한 시설, 레스토랑, 바, 소규모 주점 및 펍, 레스토랑 가이드 및 평가가 포함됩니다.	www.hideawaybrewpub.com www.restaurantrow.com
동적 및 주거용 링크	dyn	1091	일반적으로 홈 네트워크 액세스를 시도하는 사용자를 나타내는 광대역 링크의 IP 주소입니다. 가정용 컴퓨터에 대한 원격 세션을 예로 들 수 있습니다.	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
교육	edu	1001	학교, 전문대학, 대학교, 수업 자료, 교사 리소스, 기술 및 직업 교육, 온라인 교육, 교육 문제 및 정책, 재정 지원, 학교 기금, 표준 및 테스트 등 교육과 관련된 콘텐츠입니다.	www.education.com www.greatschools.org
엔터테인먼트	ent	1093	영화에 대한 자세한 정보 또는 토론, 음악 및 밴드, TV, 유명인 및 팬 웹사이트, 엔터테인먼트 뉴스, 유명인 가십, 유흥 장소 등이 해당됩니다. "예술" 범주와 비교해 보십시오.	www.eonline.com www.ew.com
극도	extr	1075	성폭력 또는 범죄 관련 자료, 폭력 및 폭력적인 행위, 유혈이 포함된 참혹한 사진(예: 부검 사진, 범죄 현장, 범죄 및 사고 희생자 사진, 과도하게 선정적인 자료), 충격적인 웹사이트가 해당됩니다.	www.car-accidents.com www.crime-scene-photos.com
패션	fash	1076	의상과 패션, 미용실, 화장품, 액세서리, 보석, 향수, 성형 관련 사진 및 텍스트, 문신 및 피어싱, 모델 에이전시가 해당됩니다. 피부과 제품은 "건강 및 영양"으로 분류됩니다.	www.fashion.net www.findabeautysalon.com
파일 전송 서비스	fts	1071	다운로드 서비스 및 호스팅된 파일 공유 제공을 기본적인 목적으로 하는 파일 전송 서비스입니다.	www.rapidshare.com www.yousendit.com
필터 회피	filt	1025	감지 불가능한 익명 웹 사용을 장려하고 지원하는 서비스로 여기에는 cgi, php, glype 익명 프록시 서비스가 포함됩니다.	www.bypassschoolfilter.com www.filterbypass.com
재무	fnnc	1015	회계 실무 및 회계사, 과세, 세금, 은행업무, 보험, 투자, 국가 경제, 모든 유형의 보험과 관련된 개인 금융, 신용카드, 퇴직 및 부동산 계획, 융자, 모기지 등의 재무 정보가 주로 해당됩니다. 증권 및 주식은 "온라인 거래"로 분류됩니다.	finance.yahoo.com www.bankofamerica.com
프리웨어 및 셰어웨어	free	1068	무료 및 셰어웨어 소프트웨어 다운로드를 제공합니다.	www.freewarehome.com www.shareware.com
도박	gamb	1049	카지노 및 온라인 도박, 마권업자 및 승률, 도박 정보, 도박 경주, 스포츠 예약, 스포츠 도박, 증권 및 주식 스프레드 베팅 서비스가 해당됩니다. 도박 중독을 다루는 웹사이트는 "건강 및 영양"으로 분류됩니다. 정부 운영 복권은 "복권"으로 분류됩니다.	www.888.com www.gambling.com
게임	game	1007	다양한 카드 게임, 보드 게임, 문자 게임, 비디오 게임, 전투 게임, 스포츠 게임, 다운로드 가능한 게임, 게임 평가, 치트시트, 컴퓨터 게임 및 인터넷 게임(예: 롤플레잉 게임)이 해당됩니다.	www.games.com www.shockwave.com

URL 카테고리	약어	코드	설명	URL 예
정부 및 법률	gov	1011	정부 웹사이트, 외교 문제, 정부/선거 관련 소식 및 정보, 법조계 관련 정보(예: 변호사, 로펌, 법률 공표, 법률 참조 자료, 법원, 사건 일람표, 법률 협회), 법령 및 법원 판결, 시민권 문제, 이민, 특허 및 저작권, 법 집행 및 교정 체계 관련 정보, 범죄 보고, 법 집행, 범죄 통계, 군사 정보(예: 군대, 군사 기지, 군사 조직), 대테러 관련 내용이 해당됩니다.	www.usa.gov www.law.com
해킹	hack	1050	웹사이트, 소프트웨어 및 컴퓨터의 보안을 우회하는 방법에 대해 모의하는 사이트입니다.	www.hackthissite.org www.gohacking.com
혐오 발언	hate	1016	사회 계층, 피부색, 종교, 성적 성향, 장애, 계급, 민족, 국적, 연령, 성별, 성 정체성을 기준으로 증오나 편견 또는 차별을 부추기는 웹사이트 그리고 인종차별, 성차별, 인종차별 신학, 인종차별 음악, 신나치주의 조직, 백인우월주의, 홀로코스트 부인론을 조장하는 사이트가 해당됩니다.	www.kkk.com www.nazi.org
건강 및 영양	hlth	1009	보건, 질병 및 장애, 의료 서비스, 병원, 의사, 의약품, 정신 건강, 정신 의학, 약리학, 운동 및 피트니스, 신체장애, 비타민 및 보충제, 성 건강(질병 및 보건), 흡연/음주/마약/도박 건강(질병 및 보건), 일반적인 식품 정보, 식음료, 요리 및 조리법, 식품 및 영양, 건강, 다이어트, 요리(조리법 및 조리 웹사이트 포함), 대체 의학이 해당됩니다.	www.health.com www.webmd.com
유머	lol	1079	농담, 촌극, 코미디 및 기타 재미있는 콘텐츠입니다. 불쾌감을 유발할 수 있는 성인 유머는 "성인"으로 분류됩니다.	www.humor.com www.jokes.com
불법 행위	ilac	1022	도난, 사기, 전화망 불법 액세스, 컴퓨터 바이러스, 테러, 폭탄, 무정부 상태 등의 범죄를 조장하는 사이트, 살인과 자살에 대한 설명뿐만 아니라 이를 실행하는 방법에 대한 내용이 서술된 웹사이트 등이 해당됩니다.	www.ekran.no www.thedisease.net
불법 다운로드	ildl	1084	저작권 계약을 위반하여 소프트웨어 보호 조치를 우회할 수 있도록 소프트웨어나 기타 자료, 시리얼 번호, 키 생성기 및 도구를 다운로드하는 기능을 제공합니다. 토렌트는 "피어 파일 전송"으로 분류됩니다.	www.keygenguru.com www.zcrack.com
불법 약물	drug	1047	환각제, 마약 용품, 마약 구매 및 제조에 대한 정보입니다.	www.cocaine.org www.hightimes.com
인프라 및 콘텐츠 전달 네트워크	infr	1018	콘텐츠 전달 인프라 및 동적으로 생성된 콘텐츠로, 현재 안전하거나 분류의 어려움으로 인해 보다 구체적으로 분류할 수 없는 웹사이트가 해당됩니다.	www.akamai.net www.webstat.net
인터넷 텔레포니	voip	1067	인터넷을 사용하는 전화 서비스입니다.	www.evaphone.com www.skype.com
채용 정보 검색	job	1004	경력 조언, 이력서 작성 및 면접 요령, 직무 적성 서비스, 일자리 데이터뱅크, 상근직 및 임시직 에이전시, 고용업체 웹사이트가 해당됩니다.	www.careerbuilder.com www.monster.com

URL 카테고리	약어	코드	설명	URL 예
란제리 및 수영복	ling	1031	주로 모델이 등장하는 속옷 및 수영복 콘텐츠입니다.	www.swimsuits.com www.victoriassecret.com
복권	lotr	1034	로또, 시합 및 정부에서 주관하는 복권 사업입니다.	www.calottery.com www.flalottery.com
휴대폰	cell	1070	SMS(문자 메시지 서비스), 전화 연결음 및 휴대 전화 다운로드가 해당됩니다. 이동통신 사업자 웹 사이트는 "비즈니스 및 산업" 범주에 포함됩니다.	www.cbfsms.com www.zedge.net
자연	natr	1013	천연 자원, 생태계 및 보존, 삼림, 황야, 식물, 화훼, 삼림 보존, 삼림, 황야, 임업 실무, 삼림 관리(재조림, 삼림 보호, 보존, 수확, 삼림 실태, 간벌, 계획 산불), 농업 실무(농업, 조원, 원예, 조경, 이식, 잡초 방제, 관개, 가지치기, 수확), 오염 문제(대기 청정도, 유해 폐기물, 오염 방지, 재활용, 폐기물 관리, 용수 품질, 환경 정화 산업), 동물, 애완동물, 가축, 동물학, 생물학, 식물학이 해당됩니다.	www.enature.com www.nature.org
뉴스	news	1058	뉴스, 헤드라인, 신문, TV 방송국, 잡지, 날씨, 기상 상태에 대한 콘텐츠입니다.	www.cnn.com news.bbc.co.uk
비정부 기구	ngo	1087	클럽, 압력 단체, 커뮤니티, 비영리 조직, 노동조합 같은 비정부 기구가 해당됩니다.	www.panda.org www.unions.org
나체주의	nsn	1060	나체주의 및 나체, 자연주의, 나체주의자 캠프, 예술적 누드가 해당됩니다.	www.artenuda.com www.naturistsociety.com
온라인 커뮤니티	comm	1024	동호회 단체, 특수한 관심사를 공유한 그룹, 웹 뉴스그룹, 게시판이 해당됩니다. "전문 네트워킹" 또는 "소셜 네트워킹"으로 분류된 웹사이트는 제외합니다.	www.igda.org www.ieee.org
온라인 스토리지 및 백업	osb	1066	백업, 공유, 호스팅을 지원하는 오프사이트 및 P2P(Peer-to-peer) 스토리지입니다.	www.adrive.com www.dropbox.com
온라인 거래	trad	1028	온라인 중개, 사용자가 온라인 주식 거래를 할 수 있는 웹사이트와 함께 주식 시장, 주식, 채권, 뮤추얼 펀드, 중개업자, 주식 분석 및 해석, 주식 선별, 주식 차트, IPO, 주식 분할과 관련된 정보가 해당됩니다. 증권 및 주식에 대한 스프레드 베팅 서비스는 "도박"으로 분류됩니다. 기타 금융 서비스는 "금융"으로 분류됩니다.	www.tdameritrade.com www.scottrade.com
조직 이메일	pem	1085	비즈니스 이메일에 액세스하는 데 사용되는 웹 사이트입니다(종종 Outlook Web Access를 통해 실행).	—
파킹된 도메인	park	1092	광고 네트워크의 유료 리스팅을 사용하는 도메인의 트래픽을 통해 수익을 창출하거나, 수익을 목적으로 도메인 이름을 판매하고자 하는 "도메인 선점자"가 소유하고 있는 웹사이트입니다. 이러한 사이트에는 유료 광고 링크를 반환하는 허위 검색 웹사이트도 포함됩니다.	www.domainzaar.com www.parked.com

URL 카테고리	약어	코드	설명	URL 예
피어 파일 전송	p2p	1056	P2P(Peer-to-Peer) 파일 전송 웹사이트입니다. 이 사이트에서는 파일 전송을 자체적으로 추적하지 않습니다.	www.bittorrent.com www.limewire.com
개인 사이트	pers	1081	개인에 대한 웹사이트, 개인 홈페이지 서버, 개인 콘텐츠가 포함된 웹사이트, 특정한 주제가 없는 개인 블로그가 해당됩니다.	www.karymullis.com www.stallman.org
사진 검색 및 이미지	img	1090	이미지, 사진, 클립아트의 저장 및 검색을 지원하는 사이트입니다.	www.flickr.com www.photobucket.com
정치	pol	1083	정치인, 정당, 정치/선거/민주주의/투표에 대한 뉴스 및 정보를 다루는 웹사이트입니다.	www.politics.com www.thisnation.com
음란물	porn	1054	노골적인 성적 표현 또는 묘사가 수반됩니다. 여기에는 노골적인 애니메이션 및 만화, 전반적으로 노골적인 묘사, 기타 페티시 자료, 노골적인 채팅방, 성관계 시뮬레이터, 스트립 포커, 성인 영화, 외설적인 작품, 노골적인 표현이 포함된 웹 기반 이메일이 포함됩니다.	www.redtube.com www.youporn.com
전문 네트워킹	pnet	1089	경력 또는 전문성 개발을 위한 소셜 네트워킹이 해당됩니다. "소셜 네트워킹" 항목도 참조해 주십시오.	www.linkedin.com www.europeanpwn.net
부동산	rest	1045	부동산, 사무실 및 상업용 공간, 부동산 리스트(예: 임대 시설, 아파트, 주택, 가옥) 검색을 지원하는 정보입니다.	www.realtor.com www.zillow.com
참조	ref	1017	시/도 가이드, 지도, 역사, 참조자료 출처, 사전, 라이브러리가 해당됩니다.	www.wikipedia.org www.yellowpages.com
종교	rel	1086	종교적 콘텐츠, 종교에 대한 정보, 종교 커뮤니티가 해당됩니다.	www.religionfacts.com www.religioustolerance.org
및 B2B	saas	1080	온라인 비즈니스 서비스, 온라인 회의를 지원하는 웹 포털입니다.	www.netsuite.com www.salesforce.com
어린이 안전	kids	1057	어린이의 액세스가 허용되며 어린이를 대상으로 하는 사이트입니다.	kids.discovery.com www.nickjr.com
과학 및 기술	sci	1012	과학 및 기술 분야에 대한 내용으로 항공우주, 전자, 공학, 수학, 기타 유사 학문, 우주 탐사, 기상학, 지리학, 환경학, 에너지학(화석연료, 핵연료, 재생연료), 통신학(전화, 통신) 등이 포함됩니다.	www.physorg.com www.science.gov
검색 엔진 및 포털	srch	1020	검색 엔진 및 인터넷의 정보에 처음 액세스하는 기타 지점입니다.	www.bing.com www.google.com
성교육	sxed	1052	성, 성 건강, 피임, 임신에 대한 내용을 사실적으로 알려주는 웹사이트입니다.	www.avert.org www.scarleteen.com
쇼핑	shop	1005	물물교환, 온라인 구매, 쿠폰 및 무료 서비스, 일반적인 사무용품, 온라인 카탈로그, 온라인 몰이 해당됩니다.	www.amazon.com www.shopping.com

URL 카테고리	약어	코드	설명	URL 예
소셜 네트워킹	snet	1069	소셜 네트워킹. "전문 네트워킹" 항목도 참조해 주십시오.	www.facebook.com www.twitter.com
사회과학	socs	1014	사회, 고고학, 인류학, 문화 연구, 역사, 언어, 지리, 철학, 심리학, 여성학 연구와 관련된 과학 및 사학입니다.	www.archaeology.org www.anthropology.net
사회 및 문화	scty	2010년	가족 및 관계, 민족, 사회 조직, 계보학, 노인, 보육이 해당됩니다.	www.childcare.gov www.familysearch.org
소프트웨어 업데이트	swup	1053	소프트웨어 패키지의 업데이트를 호스팅하는 웹 사이트입니다.	www.softwarepatch.com www.versiontracker.com
스포츠 및 레크리에이션	sprt	1008	모든 스포츠, 전문가와 아마추어, 레크리에이션 활동, 낚시, 판타지 스포츠, 공원, 놀이공원, 워터파크, 테마파크, 동물원, 아쿠아리움, 스파가 해당됩니다.	www.espn.com www.recreation.gov
스트리밍 오디오	aud	1073	인터넷 라디오 및 오디오 피드를 비롯한 실시간 스트리밍 오디오 콘텐츠입니다.	www.live-radio.net www.shoutcast.com
스트리밍 비디오	vid	1072	인터넷 TV, 웹 캐스트, 비디오 공유를 비롯한 실시간 스트리밍 비디오입니다.	www.hulu.com www.youtube.com
담배	tob	1078	애연가 웹사이트, 담배 제조사, 파이프 및 흡연 제품(불법 약물 흡입을 위한 제품이 아님)이 해당됩니다. 담배 중독은 "건강 및 영양"으로 분류됩니다.	www.bat.com www.tobacco.org
운송	trns	1044	개인 운송 수단, 자동차 및 오토바이에 대한 정보, 신형 및 중고 자동차/오토바이 구매 정보, 자동차 동호회, 보트/항공기/RV(레크리에이션용 차량) 및 기타 유사 제품이 해당됩니다. 참고로, 자동차 및 오토바이 경주는 "스포츠 및 레크리에이션"으로 분류됩니다.	www.cars.com www.motorcycles.com
여행	trvl	1046	출장 및 개인 여행, 여행 정보, 여행 자료, 여행사, 휴가 패키지, 크루즈, 숙소 및 숙박시설, 여행 교통수단, 항공권 예약, 항공료, 자동차 렌트, 별장이 해당됩니다.	www.expedia.com www.lonelyplanet.com
미분류	—	—	Cisco 데이터베이스에 없는 웹사이트는 보고를 위해 미분류로 기록됩니다. This may include mistyped URLs.	—
무기	weap	1036	총포상, 총기 경매, 총기 분류 광고, 총 부속품, 총기류 전시회, 총기 교육, 총기 관련 일반 정보 등 재래식 무기를 구매하거나 사용하는 것과 관련된 정보가 해당되며, 여기에는 기타 무기류 및 사냥 지역 그래픽 정보가 포함될 수 있습니다. 정부 군사 웹사이트는 "정부 및 법률"로 분류됩니다.	www.coldsteel.com www.gunbroker.com
웹 호스팅	whst	1037	웹사이트 호스팅, 대역폭 서비스입니다.	www.bluehost.com www.godaddy.com

URL 카테고리	약어	코드	설명	URL 예
웹 페이지 번역	tran	1063	웹 페이지의 언어를 다른 언어로 번역해줍니다.	babelfish.yahoo.com translate.google.com
웹 기반 이메일	mail	1038	공용 웹 기반 이메일 서비스입니다. 개인이 소속 회사 또는 조직의 이메일 서비스에 액세스할 수 있는 웹사이트는 "조직 이메일"로 분류됩니다.	mail.yahoo.com www.hotmail.com

관련 주제

- URL 카테고리 집합에 대한 업데이트 관리, 9-4페이지
- 분류되지 않은 URL 또는 잘못 분류된 URL 보고, 9-3페이지

10장

인터넷 요청을 제어하기 위한 정책 생성

- 정책 개요: 가로챈 인터넷 요청 제어, 10-1페이지
- 정책을 통한 웹 요청 관리 작업 개요, 10-2페이지
- 정책을 통한 웹 요청 관리 모범 사례, 10-2페이지
- 정책, 10-2페이지
- 정책 컨피그레이션, 10-8페이지
- 트랜잭션 요청 차단, 허용 또는 리디렉션, 10-10페이지
- 클라이언트 애플리케이션, 10-10페이지
- 시간 범위 및 할당량, 10-12페이지
- URL 카테고리별로 액세스 제어, 10-15페이지
- 원격 사용자, 10-18페이지
- 정책 트러블슈팅, 10-20페이지

정책 개요: 가로챈 인터넷 요청 제어

사용자가 웹 요청을 생성할 때 구성된 Web Security Appliance에서 요청을 가로채고 요청이 특정 웹 사이트, 이메일 또는 온라인 애플리케이션에 액세스한다는 최종 결과에 도달하기 위해 이동하는 프로세스를 관리합니다. 구성 중에 사용자가 작성한 요청의 기준과 조치를 정의하기 위한 Web Security Appliance 정책이 생성됩니다.

정책은 Web Security Appliance에서 웹 요청을 식별하고 제어하는 방법입니다. 클라이언트가 웹 요청을 서버에 전송할 때 웹 프록시가 요청을 수신하고 평가하며 해당 웹 요청이 속해 있는 정책을 확인합니다. 그런 다음, 정책에 정의된 조치가 요청에 적용됩니다.

Web Security Appliance는 여러 정책 유형을 사용하여 다양한 측면의 웹 요청을 관리합니다. 정책 유형은 완전히 단독으로 트랜잭션을 관리하거나 추가 처리를 위해 다른 정책 유형으로 트랜잭션을 전달할 수 있습니다. 액세스, 라우팅 또는 보안과 같이 수행하는 기능에 따라 정책 유형을 그룹화할 수 있습니다.

AsyncOS는 어플라이언스에서 불필요한 외부 통신을 피하기 위해 외부 종속성을 평가하기 전에 정책을 기반으로 트랜잭션을 평가합니다. 예를 들어, 분류되지 않은 URL을 차단하는 정책에 따라 트랜잭션이 차단되는 경우 트랜잭션은 DNS 오류에 따라 실패하지 않습니다.

정책을 통한 웹 요청 관리 작업 개요

단계	정책을 통해 웹 요청을 관리하기 위한 작업 목록	관련 주제 및 절차에 대한 링크
1	인증 영역 설정 및 순서 지정	인증 영역, 5-10페이지
2	(업스트림 프록시의 경우) 프록시 그룹 생성	업스트림 프록시에 대한 프록시 그룹 생성, 2-13페이지
2	(선택 사항) 맞춤형 클라이언트 애플리케이션 생성	클라이언트 애플리케이션, 10-10페이지
3	(선택 사항) 맞춤형 URL 카테고리 생성	맞춤형 URL 카테고리 생성, 10-15페이지
4	식별 프로필 생성	사용자 및 클라이언트 소프트웨어 분류, 6-3페이지
5	(선택 사항) 시간별로 액세스를 제한하도록 시간 범위 생성	시간 범위 및 할당량, 10-12페이지
6	정책 생성 및 순서 지정	• 정책 생성, 10-5페이지 • 정책 순서, 10-5페이지

정책을 통한 웹 요청 관리 모범 사례

- Active Directory 사용자 개체를 사용하여 웹 요청을 관리하려면 기본 그룹을 기준으로 사용하지 마십시오. Active Directory 사용자 개체에는 기본 그룹이 포함되어 있지 않습니다.

정책

- 정책 유형, 10-2페이지
- 정책 순서, 10-5페이지
- 정책 생성, 10-5페이지

정책 유형

정책 유형	요청 유형	설명	작업 링크
액세스	• HTTP • 암호 해독된 HTTPS • FTP	인바운드 HTTP, FTP 및 암호 해독된 HTTPS 트래픽을 차단, 허용 또는 리디렉션합니다. HTTPS 프록시가 사용되지 않도록 설정된 경우 액세스 정책이 인바운드 암호화된 HTTPS 트래픽도 관리합니다.	정책 생성, 10-5페이지
SOCKS	• SOCKS	SOCKS 통신 요청을 허용하거나 차단합니다.	정책 생성, 10-5페이지

정책 유형	요청 유형	설명	작업 링크
애플리케이션 인증	• application	SaaS(Software as a Service) 애플리케이션에 대한 액세스를 허용하거나 거부합니다. 애플리케이션에 대한 액세스가 빠르게 사용되지 않도록 설정될 수 있도록 하여 단일 로그인을 통해 사용자를 인증하고 보안을 향상시킵니다. 정책의 단일 로그인 기능을 사용하려면 Web Security Appliance를 ID 공급자로 구성하고 SaaS에 대한 인증서 및 키를 업로드하거나 생성해야 합니다.	SaaS 애플리케이션 인증 정책 생성, 7-4페이지
암호화된 HTTPS 관리	• HTTPS	HTTP 연결을 암호 해독, 통과 또는 삭제합니다. AsyncOS가 향후 처리를 위해 암호 해독된 트래픽을 액세스 정책에 전달합니다.	정책 생성, 10-5페이지
데이터 보안	• HTTP • 암호 해독된 HTTPS • FTP	웹으로의 데이터 업로드를 관리합니다. 데이터 보안 정책은 아웃바운드 트래픽을 스캐닝하여 해당 대상 및 콘텐츠를 기반으로 데이터 업로드에 대한 회사 규칙을 준수하는지 확인합니다. 스캐닝을 위해 아웃바운드 트래픽을 외부 서버로 리디렉션하는 외부 DLP 정책과 다르게 데이터 보안 정책은 Web Security Appliance를 사용하여 트래픽을 스캐닝하고 평가합니다.	정책 생성, 10-5페이지
외부 DLP(데이터 유출 방지)	• HTTP • 암호 해독된 HTTPS • FTP	데이터 업로드에 대한 회사 규칙을 준수하는지를 스캐닝하는 서드파티 DLP 시스템을 실행 중인 서버로 아웃바운드 트래픽을 전송합니다. 데이터 업로드도 관리하는 데이터 보안 정책과 다르게 외부 DLP 정책은 웹 보안 어플라이언스에서 스캐닝 작업을 수행하지 않도록 하여 어플라이언스에서 리소스를 비우고 서드파티 소프트웨어에서 제공하는 추가 기능을 활용합니다.	정책 생성, 10-5페이지
아웃바운드 악성프로그램 검색	• HTTP • 암호 해독된 HTTPS • FTP	악의적인 데이터를 포함할 수 있는 데이터의 업로드 요청을 차단, 모니터링 또는 허용합니다. 이미 네트워크에 있는 악성코드가 외부 네트워크로 전송되지 않도록 합니다.	정책 생성, 10-5페이지

정책 유형	요청 유형	설명	작업 링크
라우팅	• HTTP • HTTPS • FTP	업스트림 프록시를 통해 웹 트래픽을 전달하거나 목적지 서버에 전달합니다. 기존 네트워크 설계를 유지하거나, Web Security Appliance에서 처리를 오프로드하거나, 서드파티 프록시 시스템에서 제공하는 추가 기능을 활용하기 위해 업스트림 프록시를 통해 트래픽을 리디렉션할 수 있습니다. 여러 업스트림 프록시가 사용 가능한 경우 Web Security Appliance는 로드 밸런싱 기술을 사용하여 데이터를 여러 업스트림 프록시에 분배할 수 있습니다.	정책 생성, 10-5페이지

각 정책 유형은 정책 테이블을 사용하여 해당 정책을 저장하고 관리합니다. 각 정책 테이블은 정책 유형에 대한 기본 조치를 유지 관리하는 미리 정의된 전역 정책과 함께 제공됩니다. 또한 필요에 따라 사용자 정의 정책을 생성하여 정책 테이블에 추가합니다. 정책은 정책 테이블에 나열된 순서대로 처리됩니다.

개별 정책은 관리하는 사용자 요청 유형과 해당 요청에 대해 수행하는 조치를 정의합니다. 각 정책 정의에는 두 가지 기본 섹션이 있습니다.

- **Identification Profiles and Users(식별 프로필 및 사용자)** – 식별 프로필은 정책 구성원 자격 기준에 사용되며, 특히 웹 트랜잭션을 식별하기 위한 여러 옵션이 포함되어 있으므로 중요합니다. 또한 여러 속성을 정책과 공유할 수 있습니다.
- **Advanced(고급)** – 정책이 적용되는 사용자를 식별하는 데 사용되는 기준입니다. 정책에 하나 이상의 기준을 지정할 수 있으며 기준이 충족되려면 모든 항목이 일치해야 합니다.
  - **Protocols(프로토콜)** – 다양한 네트워킹 디바이스 간의 데이터 전송을 허용합니다(예: http, https, ftp 등).
  - **Proxy Ports(프록시 포트)** – 요청이 웹 프록시에 액세스하는 데 사용하는 번호가 지정된 포트입니다.
  - **Subnets(서브넷)** – 연결된 네트워크 디바이스의 논리적 그룹(예: 지리적 위치 또는 LAN(Local Area Network))이며, 여기서 요청이 시작됩니다.
  - **Time Range(시간 범위)** – 정책에서 요청이 작성된 시간 또는 날짜에 따라 웹 요청을 식별하거나 웹 요청에 조치를 적용하는 데 사용하도록 시간 범위를 생성할 수 있습니다. 시간 범위는 개별 단위로 생성됩니다.
  - **URL Categories(URL 카테고리)** – URL 카테고리는 뉴스, 비즈니스, 소셜 미디어 등과 같은 웹 사이트의 미리 정의된 카테고리 또는 맞춤형 카테고리입니다.
  - **User Agents(사용자 에이전트)** – 요청을 작성하는 데 사용되는 클라이언트 애플리케이션(예: 웹 브라우저 Firefox 또는 Chrome)입니다. 사용자 에이전트를 기반으로 정책 기준을 정의할 수 있으며 사용자 에이전트를 기반으로 제어 설정을 지정할 수 있습니다. 또한 사용자 에이전트를 인증에서 제외할 수 있습니다. 이는 자격 증명에 대한 프롬프트를 표시할 수 없는 애플리케이션에 유용합니다. 맞춤형 클라이언트 애플리케이션을 정의할 수 있지만 이러한 정의를 다른 정책에 재사용할 수 없습니다.

참고 여러 구성원 자격 기준을 정의하는 경우 정책과 일치하려면 클라이언트 요청이 모든 기준을 충족해야 합니다.

정책 순서

정책이 정책 테이블에 나열된 순서에 따라 정책이 웹 요청에 적용되는 우선순위가 결정됩니다. 테이블의 맨 위부터 처음으로 일치하는 정책까지 웹 요청을 정책과 비교하여 확인합니다. 테이블의 해당 지점 아래에 있는 모든 정책은 처리되지 않습니다.

웹 요청과 일치되는 사용자 정의 정책이 없는 경우 해당 정책 유형에 대한 전역 정책이 적용됩니다. 전역 정책은 항상 정책 테이블의 마지막에 배치되며 다시 정렬할 수 없습니다.

정책 생성

시작하기 전에

- 적절한 프록시를 사용하도록 설정합니다.
  - 웹 프록시(HTTP, 암호 해독된 HTTPS 및 FTP용)
  - HTTPS 프록시
  - SOCKS 프록시
- 연결된 식별 프로필을 생성합니다.
- 정책 순서, 10-5페이지를 이해합니다.
- (암호화된 HTTPS 전용) 인증서 및 키를 업로드하거나 생성합니다.
- (데이터 보안 전용) Cisco 데이터 보안 필터 설정을 사용하도록 설정합니다.
- (외부 DLP 전용) 외부 DLP 서버를 정의합니다.
- (라우팅 전용) 웹 보안 어플라이언스에 연결된 업스트림 프록시를 정의합니다.
- (선택 사항) 연결된 클라이언트 애플리케이션을 생성합니다.
- (선택 사항) 연결된 시간 범위를 생성합니다. 시간 범위 및 할당량을 참조하십시오.
- (선택 사항) 연결된 URL 카테고리를 생성합니다. 맞춤형 URL 카테고리 생성을 참조하십시오.

1단계 **Policy Settings(정책 설정)** 섹션에서 **Enable Identity(ID 사용)** 확인란을 사용하여 이 정책을 사용하도록 설정하거나 삭제하지 않고 빠르게 사용하지 않도록 설정합니다.

2단계 고유한 정책 **Name(이름)**을 지정합니다.

3단계 **Description(설명)**은 선택 사항입니다.

4단계 **Insert Above(위에 삽입)** 드롭다운 목록에서 테이블에서 이 정책이 표시될 위치를 선택합니다.

참고 테이블의 위쪽에서 아래쪽으로 가장 제한적인 정책에서 가장 덜 제한적인 정책순으로 정렬합니다. 자세한 내용은 정책 순서, 10-5페이지를 참조하십시오.

5단계 **Policy Member Definition(정책 구성원 정의)** 섹션에서 사용자 및 그룹 구성원 자격이 정의되는 방법을 지정합니다. Identification Profiles and Users(식별 프로필 및 사용자) 목록에서 다음 중 하나를 선택합니다.

- **All Identification Profiles(모든 식별 프로필)** – 이 정책이 기존의 모든 프로필에 적용됩니다. 또한 하나 이상의 **Advanced(고급)** 옵션을 정의해야 합니다.
- **Select One or More Identification Profiles(하나 이상의 식별 프로필 선택)** – 개별 식별 프로필을 지정하는 테이블이 표시됩니다. 이 테이블에는 행당 하나의 프로필 구성원 자격 정의가 포함되어 있습니다.

6단계 **All Identification Profiles(모든 식별 프로필)**를 선택한 경우:

a. 다음 옵션 중 하나를 선택하여 이 정책이 적용되는 인증된 사용자 및 그룹을 지정합니다.

- **All Authenticated Users(인증된 모든 사용자)** – 인증 또는 투명 식별을 통해 식별되는 모든 사용자.
- **Selected Groups and Users(선택된 그룹 및 사용자)** – 지정된 사용자 및 그룹이 사용됩니다.

  지정된 ISE SGT(Secure Group Tag) 및 지정된 사용자를 추가하거나 편집하려면 적절한 레이블에 따라 링크를 클릭합니다. 예를 들어, 현재 지정된 사용자 목록을 클릭하여 해당 목록을 편집합니다. 자세한 내용은 정책에 대한 SGT(Secure Group Tag) 추가 및 편집, 10-8페이지를 참조하십시오.
- **Guests(게스트)** – 게스트로 연결된 사용자 및 인증에 실패한 사용자.
- **All Users(모든 사용자)** – 인증되었는지 여부에 관계없이 모든 클라이언트. 이 옵션이 선택된 경우 하나 이상의 **Advanced(고급)** 옵션도 제공해야 합니다.

7단계 **Select One or More Identification Profiles(하나 이상의 식별 프로필 선택)**를 선택한 경우 프로필 선택 테이블이 표시됩니다.

a. Identification Profiles(식별 프로필) 열의 Select Identification Profile(식별 프로필 선택) 드롭다운 목록에서 Identification Profile(식별 프로필)을 선택합니다.

b. 이 정책이 적용되는 인증된 사용자 및 그룹을 지정합니다.

- **All Authenticated Users(인증된 모든 사용자)** – 인증 또는 투명 식별을 통해 식별되는 모든 사용자.
- **Selected Groups and Users(선택된 그룹 및 사용자)** – 지정된 사용자 및 그룹이 사용됩니다.

  지정된 ISE SGT(Secure Group Tag) 및 지정된 사용자를 추가하거나 편집하려면 적절한 레이블에 따라 링크를 클릭합니다. 예를 들어, 현재 지정된 사용자 목록을 클릭하여 해당 목록을 편집합니다. 자세한 내용은 정책에 대한 SGT(Secure Group Tag) 추가 및 편집, 10-8페이지를 참조하십시오.
- **Guests(게스트)** – 게스트로 연결된 사용자 및 인증에 실패한 사용자.

c. 프로필 선택 테이블에 행을 추가하려면 **Add Identification Profile(식별 프로필 추가)**을 클릭합니다. 행을 삭제하려면 해당 행에서 휴지통 아이콘을 클릭합니다.

필요에 따라 (a)~(c)단계를 반복하여 원하는 모든 식별 프로필을 추가합니다.

8단계 추가 그룹 구성원 자격 기준을 정의하려면 **Advanced(고급)** 섹션을 확장합니다. (이 단계는 **Policy Member Definition(정책 구성원 정의)** 섹션의 선택에 따라 선택 사항이 될 수 있습니다. 또한 구성 중인 정책의 유형에 따라 다음 중 몇 가지 옵션은 사용할 수 없습니다.)

고급 옵션	설명
프로토콜	이 정책이 적용될 프로토콜을 선택합니다. **All others(기타 모두)**는 프로토콜이 선택되지 않음을 의미합니다. 연결된 식별 프로필이 특정 프로토콜에 적용되는 경우 이 정책은 동일한 프로토콜에 적용됩니다.
프록시 포트	특정 포트를 사용하여 웹 프록시에 액세스하는 트래픽에만 이 정책을 적용합니다. 여러 포트를 쉼표로 구분하여 하나 이상의 포트 번호를 입력합니다. 명시적 전달 연결의 경우에는 브라우저에 구성된 포트입니다. 투명한 연결의 경우에는 목적지 포트와 동일합니다. **참고** 연결된 식별 프로필이 특정 프록시 포트에만 적용되는 경우 여기에 프록시 포트를 입력할 수 없습니다.
서브넷	특정 서브넷의 트래픽에만 이 정책을 적용합니다. **Specify subnets(서브넷 지정)**를 선택하고 쉼표로 구분된 특정 서브넷을 입력합니다. 추가로 서브넷을 통해 필터링하지 않으려면 **Use subnets from selected Identities(선택된 ID의 서브넷 사용)**를 선택된 상태로 유지합니다. **참고** 연결된 ID가 특정 서브넷에 적용되는 경우 ID가 적용되는 주소의 하위 집합으로 이 정책의 적용을 추가로 제한할 수 있습니다.
시간 범위	정책 구성원 자격에 대한 시간 범위를 적용할 수 있습니다. • 시간 범위 – 이전에 정의된 시간 범위를 선택합니다(시간 범위 및 할당량, 10-12페이지). • 시간 범위 일치 - 이 옵션을 사용하여 이 시간 범위가 포함되거나 제외되는지를 표시합니다. 즉, 지정된 범위 중에만 일치시킬지 또는 지정된 범위를 제외하고 항상 일치시킬지를 표시합니다.
URL 범주	특정 대상(URL) 및 URL 카테고리별로 정책 구성원 자격을 제한할 수 있습니다. 원하는 모든 맞춤형 카테고리 및 미리 정의된 카테고리를 선택합니다. 맞춤형 카테고리에 대한 자세한 내용은 맞춤형 URL 카테고리 생성, 10-15페이지를 참조하십시오.
사용자 에이전트	이 정책에 대한 구성원 자격 정의의 일부로 특정 사용자 에이전트를 선택하고 정규식을 사용하여 맞춤형 에이전트를 정의할 수 있습니다. • 공통 사용자 에이전트 – **Browsers(브라우저)** – Internet Explorer 및 Firefox 버전을 선택하려면 이 섹션을 확장합니다. – **Others(기타)** – Microsoft Windows 및 Adobe Acrobat 등의 특정 애플리케이션 업데이트 에이전트를 선택하려면 이 섹션을 확장합니다. • 맞춤형 사용자 에이전트 - 행당 하나씩 하나 이상의 정규식을 입력하여 맞춤형 사용자 에이전트를 정의할 수 있습니다. • 사용자 에이전트 일치 - 이 옵션을 사용하여 이러한 사용자 에이전트 사양이 포함되거나 제외되는지를 표시합니다. 즉, 해당 정의만 일치시킬지 또는 여기에 지정된 정의를 제외한 모든 정의만 일치시킬지를 표시합니다.

정책에 대한 SGT(Secure Group Tag) 추가 및 편집

정책의 특정 식별 프로필에 할당된 SGT(Secure Group Tag) 목록을 변경하려면 Add/Edit Policy(정책 추가/편집) 페이지의 Selected Groups and Users(선택된 그룹 및 사용자) 목록에 있는 ISE SGT(Secure Group Tag) 레이블을 따라 링크를 클릭합니다. (정책 생성, 10-5페이지 참조) 이 링크는 "태그가 입력되지 않음"이거나 현재 할당된 태그 목록입니다. 이 링크를 통해 Add/Edit Secure Group Tags(SGT(Secure Group Tag) 추가/편집) 페이지가 열립니다.

현재 이 정책에 할당된 모든 SGT는 Authorized Secure Group Tags(권한 있는 SGT(Secure Group Tag)) 섹션에 나열됩니다. 연결된 ISE 서버에서 사용 가능한 모든 SGT는 Secure Group Tag Search(STG(Secure Group Tag) 검색) 섹션에 나열됩니다.

1단계 Authorized Secure Group Tags(인증된 STG(Secure Group Tag)) 목록에 하나 이상의 SGT를 추가하려면 Secure Group Tag Search(STG(Secure Group Tag) 검색) 섹션에서 원하는 항목을 선택한 후 **Add(추가)**를 클릭합니다.

이미 추가된 SGT는 녹색으로 강조 표시됩니다. 사용 가능한 SGT 목록에서 특정 SGT를 빠르게 찾으려면 **Search(검색)** 필드에 텍스트 문자열을 입력합니다.

2단계 Authorized Secure Group Tags(인증된 STG(Secure Group Tag)) 목록에서 하나 이상의 SGT를 제거하려면 해당 항목을 선택한 후 **Delete(삭제)**를 클릭합니다.

3단계 Done(완료)을 클릭하여 Add/Edit Group(그룹 추가/편집) 페이지로 돌아갑니다.

관련 주제

- 시간 범위 및 할당량
- 정책에서 클라이언트 애플리케이션 사용

정책 컨피그레이션

정책 테이블의 각 행은 정책 정의를 나타내고 각 열은 해당 정책 요소에 대한 컨피그레이션 페이지의 링크를 포함합니다.

참고 다음 정책 컨피그레이션 구성 요소에서 URL 필터링에서만 "경고" 옵션을 지정할 수 있습니다.

옵션	설명
프로토콜 및 사용자 에이전트	프로토콜에 대한 정책 액세스를 제어하고 특정 클라이언트 애플리케이션(예: 인스턴트 메시징 클라이언트, 웹 브라우저 및 인터넷 전화 서비스)에 대한 차단을 구성하는 데 사용됩니다. 특정 포트에서 HTTP CONNECT 요청을 터널링하도록 어플라이언스를 구성할 수도 있습니다. 터널링이 사용하도록 설정된 경우 어플라이언스는 HTTP 트래픽을 평가하지 않고 지정된 포트를 통해 전달합니다.

옵션	설명
URL 필터링	AsyncOS for Web을 사용하면 어플라이언스에서 특정 HTTP 또는 HTTPS 요청의 URL 카테고리에 따라 트랜잭션을 처리하는 방법을 구성할 수 있습니다. 미리 정의된 카테고리 목록을 사용하여 할당량 기반 또는 시간 기반 필터를 차단, 모니터링, 경고 또는 설정하도록 선택할 수 있습니다. 또한 맞춤형 URL 카테고리를 생성한 후 맞춤형 카테고리의 웹 사이트에 대한 할당량 기반 또는 시간 기반 필터를 차단, 리디렉션, 허용, 모니터링, 경고 또는 적용하도록 선택할 수 있습니다. 맞춤형 URL 카테고리 생성에 대한 자세한 내용은 맞춤형 URL 카테고리 생성 및 편집, 9-14페이지를 참조하십시오.
애플리케이션	애플리케이션 가시성 및 제어 엔진(AVC 엔진)은 애플리케이션에 사용되는 웹 트래픽을 심층적으로 이해하고 제어할 수 있도록 웹 트래픽을 검사하는 사용 정책 구성 요소입니다. 어플라이언스를 통해 애플리케이션 유형 및 개별 애플리케이션별로 애플리케이션을 차단하거나 허용하도록 웹 프록시를 구성할 수 있습니다. 또한 특정 애플리케이션 내에서 특정 애플리케이션 동작(예: 파일 전송)에 제어를 적용할 수 있습니다. 컨피그레이션 정보는 웹 애플리케이션에 대한 액세스 관리, 15-1페이지를 참조하십시오.
오브젝트	파일 특성(예: 파일 크기 및 파일 유형)을 기반으로 파일 다운로드를 차단하도록 웹 프록시를 구성할 수 있습니다. 일반적으로 개체는 개별적으로 선택, 업로드, 다운로드 및 조작할 수 있는 항목입니다. 예를 들어 다음과 같습니다. • 애플리케이션: pdf, xml, zip, exe • 텍스트: cmd, csv, html, javascript • 이미지: gif, jpeg, png, tiff • 비디오: mp4, Quicktime, avi, wmv • 오디오: mp4, wav, webm, mpeg • 메시지: http, xml, rfc822, partial • x-world: wrl, wrz, xof, 3dmf **참고** 개체 차단은 압축된 파일 내부에서 검사되지 않습니다.
안티멀웨어 및 평판	웹 평판 필터를 사용하면 URL에 웹 기반 평판 점수를 할당하여 URL 기반 악성코드를 포함할 가능성을 확인할 수 있습니다. 안티멀웨어 스캐닝은 웹 기반 멀웨어 위협을 식별하고 중지합니다. Advanced Malware Protection은 다운로드된 파일에서 악성코드를 식별합니다. 안티멀웨어 및 평판 정책은 각 구성 요소에 대한 전역 설정을 상속합니다. **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)** 내에서 악성코드 스캐닝 판정을 기반으로 모니터링하거나 차단하도록 악성코드 카테고리를 맞춤화할 수 있으며 웹 평판 점수 임계값을 맞춤화할 수 있습니다. 정책 내에서 악성코드 카테고리를 추가로 맞춤화할 수 있습니다. 또한 파일 평판 및 분석 서비스에 대한 전역 설정이 있습니다. 자세한 내용은 액세스 정책에서 안티멀웨어 및 평판 설정, 13-9페이지 및 파일 평판 및 분석 기능 구성, 14-5페이지를 참조하십시오.

트랜잭션 요청 차단, 허용 또는 리디렉션

웹 프록시는 사용자가 트랜잭션 요청 그룹에 대해 생성하는 정책을 기반으로 웹 트래픽을 제어합니다.

- **허용.** 웹 프록시가 중단 없이 연결을 허용합니다. 허용된 연결은 DVS 엔진에서 스캐닝되지 않았을 수 있습니다.
- **차단.** 웹 프록시가 연결을 허용하지 않으며, 대신 차단 이유를 설명하는 최종 사용자 알림 페이지를 표시합니다.
- **리디렉션.** 웹 프록시는 원래 요청된 목적지 서버에 대한 연결을 허용하지 않고, 대신 지정된 다른 URL에 연결합니다. 액세스 정책의 트래픽 리디렉션을 참조하십시오.

참고 선행 조치는 웹 프록시가 클라이언트 요청에 대해 수행하는 최종 조치입니다. 액세스 정책에 대해 구성할 수 있는 모니터링 조치는 최종 조치가 아닙니다.

일반적으로 여러 유형의 정책이 전송 프로토콜에 따라 트래픽을 제어합니다.

정책 유형	프로토콜				지원되는 조치			
	HTTP	HTTPS	FTP	SOCKS	Block	허용	리디렉션	모니터링
액세스	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
암호 해독	x	x						x
데이터 보안	x	x	x		x			x
외부 DLP	x	x	x				x	
아웃바운드 악성프로그램 검색	x	x	x		x			x
라우팅	x	x	x				x	

참고 암호 해독 정책이 액세스 정책보다 우선합니다.

클라이언트 애플리케이션

클라이언트 애플리케이션 정보

클라이언트 애플리케이션(예: 웹 브라우저)은 요청을 작성하는 데 사용됩니다. 클라이언트 애플리케이션을 기반으로 정책 구성원 자격을 정의할 수 있으며 제어 설정을 지정하고 클라이언트 애플리케이션을 인증에서 제외할 수 있습니다. 이는 자격 증명에 대한 프롬프트를 표시할 수 없는 애플리케이션에 유용합니다.

정책에서 클라이언트 애플리케이션 사용

클라이언트 애플리케이션을 사용하여 정책 구성원 자격 정의

1단계 Web Security Manager(웹 보안 관리자) 메뉴에서 정책 유형을 선택합니다.

2단계 정책 테이블에서 정책 이름을 클릭합니다.

3단계 Advanced(고급) 섹션을 확장하고 Client Applications(클라이언트 애플리케이션) 필드의 링크를 클릭합니다.

4단계 하나 이상의 클라이언트 애플리케이션을 정의합니다.

표 10-1

옵션	방법
미리 정의된 클라이언트 애플리케이션 선택	Browser and Other(브라우저 및 기타) 섹션을 확장하고 필요한 클라이언트 애플리케이션 확인란을 선택합니다. **정보** 가능한 경우 Any Version(모든 버전) 옵션만 선택합니다. 이렇게 하면 여러 항목을 선택하는 것보다 성능이 향상되기 때문입니다.
맞춤형 클라이언트 애플리케이션 정의	Custom Client Application(맞춤형 클라이언트 애플리케이션) 필드에 적절한 정규식을 입력합니다. 필요에 따라 새 행에 추가 정규식을 입력합니다. **정보** 정규식 예제를 보려면 **Example Client Applications Patterns(예제 클라이언트 애플리케이션 패턴)**를 클릭합니다.

5단계 (선택 사항) 정책 구성원 자격이 사용자가 정의한 클라이언트 애플리케이션을 **제외한** 모든 클라이언트 애플리케이션에 기반하도록 하려면 **Match All Except The Selected Client Applications Definitions(선택된 클라이언트 애플리케이션 정의를 제외하고 모두 일치)** 라디오 버튼을 클릭합니다.

6단계 **Done(완료)**을 클릭합니다.

클라이언트 애플리케이션을 사용하여 정책 제어 설정 정의

1단계 Web Security Manager(웹 보안 관리자) 메뉴에서 정책 유형을 선택합니다.

2단계 정책 테이블에서 필요한 정책 이름을 찾습니다.

3단계 동일한 행의 Protocols and Client Applications(프로토콜 및 클라이언트 애플리케이션) 열에 있는 셀 링크를 클릭합니다.

4단계 Edit Protocols and Client Applications Settings(프로토콜 및 클라이언트 애플리케이션 설정 편집) 창의 드롭다운 목록에서 **Define Custom Settings(맞춤형 설정 정의)**를 선택합니다(아직 설정되지 않은 경우).

5단계 Custom Client Applications(맞춤형 클라이언트 애플리케이션) 필드에 정의하려는 클라이언트 애플리케이션과 일치하는 정규식을 입력합니다. 필요에 따라 새 행에 추가 정규식을 입력합니다.

정보 정규식 예제를 보려면 **Example Client Application Patterns(예제 클라이언트 애플리케이션 패턴)**를 클릭합니다.

6단계 변경 사항을 제출 및 커밋합니다.

인증에서 클라이언트 애플리케이션 제외

단계	작업	링크
1단계	인증이 필요하지 않은 식별 프로필을 생성합니다.	사용자 및 클라이언트 소프트웨어 분류
2단계	식별 프로필 구성원 자격을 제외할 클라이언트 애플리케이션으로 설정합니다.	정책에서 클라이언트 애플리케이션 사용
3단계	정책 테이블에서 인증이 필요한 식별 프로필을 다른 모든 식별 프로필 위에 배치합니다.	정책 순서

시간 범위 및 할당량

액세스 정책 및 암호 해독 정책에 시간 범위와 시간 및 볼륨 할당량을 적용하여 사용자가 액세스할 수 있는 시간, 사용자의 최대 연결 시간 또는 데이터 볼륨("대역폭 할당량"이라고도 함)을 제한할 수 있습니다.

- 정책 및 제한적 사용 제어에 대한 시간 범위, 10-12페이지
- 시간 및 볼륨 할당량, 10-13페이지

정책 및 제한적 사용 제어에 대한 시간 범위

시간 범위는 정책 및 제한적 사용 제어가 적용되는 기간을 정의합니다.

참고 시간 범위를 사용하여 사용자가 인증되어야 하는 시간을 정의할 수 없습니다. 인증 요건은 시간 범위를 지원하지 않는 식별 프로필에 정의됩니다.

- 시간 범위 생성, 10-12페이지

시간 범위 생성

1단계 **Web Security Manager(웹 보안 관리자) > Define Time Ranges and Quotas(시간 범위 및 할당량 정의)**를 선택합니다.

2단계 **Add Time Range(시간 범위 추가)**를 클릭합니다.

3단계 시간 범위의 이름을 입력합니다.

4단계 **Time Zone(시간대)** 옵션을 선택합니다.

- **Time Zone Setting From Appliance(어플라이언스의 시간대 설정)** 사용 – Web Security Appliance와 동일한 시간대를 사용합니다.
- **Specify Time Zone for this Time Range(이 시간 범위에 대한 시간대 지정)** – GMT 차감 시간 또는 지역, 국가 및 해당 국가의 특정 시간대로 다른 시간대를 정의합니다.

5단계 하나 이상의 **Day of Week(요일)** 확인란을 선택합니다.

6단계 **Time of Day(시간)** 옵션을 선택합니다.

- **All Day(종일)** – 전체 24시간 기간을 사용합니다.
- **From(시작)** 및 **To(종료)** – 특정 시간 범위를 정의합니다. 시작 시간 및 종료 시간을 HH:MM(24시간 형식)으로 입력합니다.

정보 각 시간 범위는 시작 시간 및 종료 시간 경계를 정의합니다. 예를 들어, 8:00 - 17:00을 입력하면 8:00:00 - 16:59:59와 일치하지만 17:00:00과는 일치하지 않습니다. 자정은 00:00을 시작 시간으로 지정하고 24:00을 종료 시간으로 지정해야 합니다.

7단계 변경 사항을 제출 및 커밋합니다.

시간 및 볼륨 할당량

할당량을 사용하면 개별 사용자가 부과된 데이터 볼륨 또는 시간 제한이 소진될 때까지 계속해서 인터넷 리소스(또는 인터넷 리소스 클래스)에 액세스할 수 있습니다. AsyncOS는 HTTP, HTTPS 및 FTP 트래픽에 정의된 할당량을 적용합니다.

사용자가 시간 또는 볼륨 할당량에 도달하면 AsyncOS가 먼저 경고를 표시한 후 차단 페이지를 표시합니다.

시간 및 볼륨 할당량 사용에 대해 다음에 주의하십시오.

- AsyncOS가 투명 모드에서 구축되고 HTTPS 프록시가 사용하지 않도록 설정된 경우 포트 443에서 수신 대기하지 않으며 요청이 삭제됩니다. 이것이 표준 동작입니다. AsyncOS가 명시적 모드에서 구축된 경우 액세스 정책에 할당량을 설정할 수 있습니다.

  HTTPS 프록시가 사용하도록 설정된 경우 요청에 대한 가능한 조치는 통과, 암호 해독, 삭제 또는 모니터링입니다. 전반적으로 암호 해독 정책의 할당량은 통과 카테고리에만 적용할 수 있습니다.

  통과를 사용하는 경우 터널 트래픽에 대한 할당량을 설정할 수 있는 옵션도 있습니다. 암호 해독을 사용하는 경우 액세스 정책에 구성된 할당량이 암호 해독된 트래픽에 적용되므로 이 옵션을 사용할 수 없습니다.
- URL 필터링이 사용하지 않도록 설정되었거나 해당 기능 키를 사용할 수 없는 경우 AsyncOS가 URL의 카테고리를 식별할 수 없으며 Access Policy(액세스 정책) -> URL Filtering(URL 필터링) 페이지가 사용하지 않도록 설정됩니다. 따라서 할당량을 구성하려면 기능 키가 존재해야 하고 사용 정책이 사용하도록 설정되어야 합니다.
- Facebook 및 Gmail과 같은 많은 웹 사이트는 빈번히 자동 업데이트됩니다. 사용하지 않는 브라우저 창 또는 탭에서 이러한 웹 사이트가 열려 있으면 계속해서 사용자의 시간 및 볼륨 할당량을 사용합니다.
- 프록시를 재시작하면 할당량이 재설정되어, 계획된 것보다 잠재적으로 더 많은 액세스가 허용될 수 있습니다. 프록시 재시작은 컨피그레이션 변경, 크래시, 머신 재부팅 등으로 인해 발생할 수 있습니다. 관리자에게 프록시 재시작에 대해 명시적으로 알리지 않는 경우 약간의 혼란이 발생할 수 있습니다.
- decrypt-for-EUN 옵션이 사용하도록 설정된 경우에도 HTTPS에 대한 EUN 페이지(경고 및 차단)를 표시할 수 없습니다.

참고 둘 이상의 할당량이 지정된 사용자에게 적용되는 경우 항상 가장 제한적인 할당량이 적용됩니다.

- 볼륨 할당량 계산, 10-14페이지
- 시간 할당량 계산, 10-14페이지
- 시간 및 볼륨 할당량 정의, 10-14페이지

볼륨 할당량 계산

볼륨 할당량은 다음과 같이 계산됩니다.

- HTTP 및 암호 해독된 HTTPS 트래픽 – HTTP 요청 및 응답 본문이 할당량 제한에 포함됩니다. 요청 헤더 및 응답 헤더는 제한에 포함되지 않습니다.
- 터널 트래픽(터널링된 HTTPS 포함) - AsyncOS는 단순히 터널링된 트래픽을 클라이언트에서 서버로, 서버에서 클라이언트로 전달합니다. 터널 트래픽의 전체 데이터 볼륨이 할당량 제한에 포함됩니다.
- FTP – 제어 연결 트래픽은 계산되지 않습니다. 업로드 및 다운로드되는 파일의 크기는 할당량 제한에 포함됩니다.

참고 클라이언트 측 트래픽만 할당량 제한에 포함됩니다. 캐시에서 응답이 제공되는 경우에도 클라이언트 측 트래픽이 생성되기 때문에 캐시된 콘텐츠도 제한에 포함됩니다.

시간 할당량 계산

시간 할당량은 다음과 같이 계산됩니다.

- HTTP 및 암호 해독된 HTTPS 트래픽 – 동일한 URL 카테고리에 대한 각 연결의 지속시간(연결이 형성될 때부터 끊어질 때까지)에 1분을 더한 시간이 시간 할당량 제한에 포함됩니다. 상호 1분 이내에 동일한 URL 카테고리에 여러 요청이 작성된 경우 하나의 지속적인 세션으로 간주되고 이 세션의 끝에 1분만 추가됩니다(즉, 1분 이상 "정지" 이후).
- 터널 트래픽(터널링된 HTTPS 포함) – 터널의 실제 지속시간(연결이 형성될 때부터 끊어질 때까지)이 할당량 제한에 포함됩니다. 위에서 설명된 여러 요청에 대한 계산이 터널링된 트래픽에도 적용됩니다.
- FTP – FTP 제어 세션의 실제 지속시간(연결이 형성될 때부터 끊어질 때까지)이 할당량 제한에 포함됩니다. 위에서 설명된 여러 요청에 대한 계산이 FTP 트래픽에도 적용됩니다.

시간 및 볼륨 할당량 정의

시작하기 전에

- **Security Services(보안 서비스)** > **Acceptable Use Controls(제한적 사용 제어)**로 이동하여 제한적 사용 제어를 사용하도록 설정합니다.
- 할당량을 일별 제한으로 적용하지 않을 경우 시간 범위를 정의합니다. 시간 및 볼륨 할당량 정의를 참조하십시오.

1단계 **Web Security Manager(웹 보안 관리자)** > **Define Time Ranges and Quotas(시간 범위 및 할당량 정의)**로 이동합니다.

2단계 **Add Quota(할당량 추가)**를 클릭합니다.

3단계 필드에 고유한 **Quota Name(할당량 이름)**을 입력합니다.

4단계 매일 할당량을 재설정하려면 **Reset this quota daily at(매일 이 할당량을 재설정하는 시간)**을 선택하고 필드에 12시간 형식의 시간을 입력한 후 메뉴에서 **AM(오전)** 또는 **PM(오후)**을 선택합니다. 또는 **Select a predefined time range profile(미리 정의된 시간 범위 프로필 선택)**을 선택합니다.

5단계 시간 할당량을 설정하려면 **Time Quota(시간 할당량)** 확인란을 선택하고 **hrs(시간)** 메뉴에서 시간 수를 선택한 후 **mins(분)** 메뉴에서 분 수를 선택합니다. 0(항상 차단됨)부터 23시간 및 59분까지 선택할 수 있습니다.

6단계 볼륨 할당량을 설정하려면 필드에 숫자를 입력하고 메뉴에서 **KB**(킬로바이트), **MB**(메가바이트) 또는 **GB**(기가바이트)를 선택합니다.

7단계 **Submit(제출)**을 클릭한 후 **Commit Changes(변경 사항 커밋)**를 클릭하여 변경 사항을 적용합니다. 또는 변경을 취소하려면 **Cancel(취소)**을 클릭합니다.

다음 작업

- (선택 사항) **Security Services(보안 서비스)** > **End-User Notification(최종 사용자 알림)**으로 이동하여 할당량에 대한 최종 사용자 알림을 구성합니다.

URL 카테고리별로 액세스 제어

웹 요청이 지정하는 웹 사이트의 카테고리를 기준으로 웹 요청을 식별하고 조치를 수행할 수 있습니다. 기본적으로 Web Security Appliance는 여러 가지 미리 정의된 URL 카테고리(예: 웹 기반 이메일 및 기타)와 함께 제공됩니다.

미리 정의된 카테고리 및 이와 연결된 웹 사이트는 Web Security Appliance에 있는 필터링 데이터베이스 내에 정의됩니다. Cisco에서 자동으로 이러한 데이터베이스를 최신 상태로 유지합니다. 그러나 사용자가 지정하는 호스트 이름 및 IP 주소에 대해 사용자 정의 맞춤형 URL 카테고리를 생성할 수도 있습니다.

URL 카테고리는 요청을 식별하기 위한 정책을 제외한 모든 정책에서 사용될 수 있습니다. 또한 액세스, 암호화된 HTTPS 관리 및 데이터 보안 정책에서 요청에 조치를 적용하는 데 사용될 수도 있습니다.

맞춤형 URL 카테고리 생성

시작하기 전에

- **Security Services(보안 서비스)** > **Acceptable Use Controls(제한적 사용 제어)**로 이동하여 제한적 사용 제어를 사용하도록 설정합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Custom URL Categories(맞춤형 URL 카테고리)**를 선택합니다.

2단계 **Add Custom Category(맞춤형 카테고리 추가)**를 클릭합니다.

3단계 맞춤형 URL 카테고리에 대한 설정을 입력합니다.

설정	설명
범주 이름	URL 카테고리의 이름을 입력합니다. 이 이름은 정책에 대한 URL 필터링을 구성할 때 표시됩니다. **참고:** 보고용 Sawmill 툴은 URL 카테고리 이름의 처음 4개 문자에 공백이 포함되어 있는 경우 액세스 로그에서 맞춤형 URL 카테고리를 찾지 못합니다.

설정	설명
목록 순서	맞춤형 URL 카테고리 목록에서 이 카테고리를 배치할 순서를 선택합니다. 가장 높은 URL 카테고리의 경우 "1"을 입력합니다. URL 필터링 엔진은 지정된 순서로 맞춤형 URL 카테고리와 비교하여 클라이언트 요청을 평가합니다.
사이트	맞춤형 카테고리에 속하는 하나 이상의 주소를 입력합니다. 줄 바꿈 기호 또는 쉼표로 구분된 여러 주소를 입력할 수 있습니다. 다음 형식 중 하나를 사용하여 주소를 입력할 수 있습니다. • IP 주소(예: 10.1.1.0) • CIDR 주소(예: 10.1.1.0/24) • 도메인 이름(예: example.com) • 호스트 이름(예: crm.example.com) • 부분 호스트 이름(예: .example.com) **참고:** 부분 호스트 이름(예: .example.com)을 입력해도 www.example.com과 일치됩니다. **참고**: 여러 맞춤형 URL 카테고리에서 동일한 주소를 사용할 수 있지만 카테고리가 나열되는 순서와 관련됩니다. 이러한 카테고리를 동일한 정책에 포함하고 각각에 다른 조치를 정의하면 맞춤형 URL 카테고리 테이블에서 가장 높은 목록에 있는 카테고리의 조치가 적용됩니다.
고급: 정규식	정규식을 사용하여 사용자가 입력하는 패턴과 일치하는 여러 웹 서버를 지정할 수 있습니다. **참고:** URL 필터링 엔진은 먼저 Sites(사이트) 필드에 입력된 주소와 URL을 비교합니다. 트랜잭션의 URL이 Sites(사이트) 필드의 항목과 일치하면 여기에 입력된 식과 비교되지 않습니다.

4단계 (선택 사항) Sites(사이트) 필드의 모든 주소를 알파벳순으로 정렬하려면 **Sort URLs(URL 정렬)**를 클릭합니다.

참고 주소를 정렬하면 원래 순서로 복구할 수 없습니다.

5단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 정규식

URL 카테고리를 사용하여 웹 요청 식별

시작하기 전에

- 제한적 사용 제어를 사용하도록 설정합니다. URL 필터링 엔진 구성을 참조하십시오.
- (선택 사항) 맞춤형 URL 카테고리를 생성합니다. 맞춤형 URL 카테고리 생성을 참조하십시오.

1단계 Web Security Manager(웹 보안 관리자) 메뉴에서 정책 유형(SaaS 제외)을 선택합니다.

2단계 정책 테이블의 정책 이름을 클릭하거나 새 정책을 추가합니다.

3단계 **Advanced(고급)** 섹션을 확장하고 URL Categories(URL 카테고리) 필드의 링크를 클릭합니다.

4단계 웹 요청을 식별하려는 URL 카테고리에 해당하는 Add(추가) 열 셀을 클릭합니다. 필요에 따라 맞춤형 URL 카테고리 및 미리 정의된 URL 카테고리 목록에 대해서도 이를 수행합니다.

5단계 **Done(완료)**을 클릭합니다.

6단계 변경 사항을 제출 및 커밋합니다.

URL 카테고리를 사용하여 웹 요청에 대한 조치 수행

시작하기 전에

- 제한적 사용 제어를 사용하도록 설정합니다. URL 필터링 엔진 구성을 참조하십시오.
- (선택 사항) 맞춤형 URL 카테고리를 생성합니다. 맞춤형 URL 카테고리 생성을 참조하십시오.

참고 정책 내에서 URL 카테고리를 기준으로 사용한 경우 해당 카테고리만 사용하여 동일한 정책 내에 조치를 지정할 수 있습니다. 이로 인해 아래 설명된 옵션 중 일부는 다르거나 사용 불가능할 수 있습니다.

1단계 Web Security Manager(웹 보안 관리자) 메뉴에서 **Access Policies(액세스 정책)**, **Cisco Data Security Policies(Cisco 데이터 보안 정책)** 또는 **Encrypted HTTPS Management(암호화된 HTTPS 관리)** 중 하나를 선택합니다.

2단계 정책 테이블에서 필요한 정책 이름을 찾습니다.

3단계 동일한 행의 URL Filtering(URL 필터링) 열에 있는 셀 링크를 클릭합니다.

4단계 (선택 사항) 맞춤형 URL 카테고리를 선택합니다.

a. **Select Custom Categories(맞춤형 카테고리 선택)**를 클릭합니다.

b. 이 정책에 포함할 맞춤형 URL 카테고리를 선택하고 **Apply(적용)**를 클릭합니다.

URL 필터링 엔진이 클라이언트 요청과 비교해야 하는 맞춤형 URL 카테고리를 선택합니다. URL 필터링 엔진은 클라이언트 요청을 포함된 맞춤형 URL 카테고리와 비교하고 제외된 맞춤형 URL 카테고리는 무시합니다. URL 필터링 엔진은 클라이언트 요청의 URL을 미리 정의된 URL 카테고리와 비교하기 전에 포함된 맞춤형 URL 카테고리와 비교합니다.

정책에 포함된 맞춤형 URL 카테고리는 Custom URL Category Filtering(맞춤형 URL 카테고리 필터링) 섹션에 표시됩니다.

5단계 각 맞춤형 및 미리 정의된 URL 카테고리에 대한 조치를 선택합니다.

참고 사용 가능한 조치는 맞춤형 및 미리 정의된 카테고리와 정책 유형마다 다릅니다.

6단계 Uncategorized URL(분류되지 않은 URL) 섹션에서 맞춤형 또는 미리 정의된 URL 카테고리에 해당하지 않는 웹 사이트에 대한 클라이언트 요청에 수행할 조치를 선택합니다.

7단계 변경 사항을 제출 및 커밋합니다.

원격 사용자

- 원격 사용자 정보, 10-18페이지
- 원격 사용자의 식별 구성 방법, 10-18페이지
- ASA에 대한 원격 사용자 상태 및 통계 표시, 10-20페이지

원격 사용자 정보

Cisco AnyConnect 모빌리티 보안는 네트워크 경계를 원격 엔드포인트로 확장하여 Web Security Appliance에서 제공하는 웹 필터링 서비스를 통합합니다.

원격 및 모바일 사용자는 Cisco AnyConnect Secure VPN(Virtual Private Network) 클라이언트를 사용하여 ASA(Adaptive Security Appliance)와의 VPN 세션을 설정합니다. ASA가 IP 주소 및 사용자 이름으로 사용자를 식별하는 정보와 함께 웹 트래픽을 웹 보안 어플라이언스에 전송합니다. Web Security Appliance는 트래픽을 스캐닝하고 사용 정책을 적용하며 보안 위협으로부터 사용자를 보호합니다. 보안 어플라이언스는 안전하고 허용 가능한 것으로 간주되는 모든 트래픽을 사용자에게 반환합니다.

모빌리티 보안가 사용하도록 설정된 경우 해당 위치별로 사용자에게 적용할 ID 및 정책을 구성할 수 있습니다.

- **원격 사용자.** 이러한 사용자는 VPN을 사용하여 원격 위치에서 네트워크에 연결됩니다. Cisco ASA 및 Cisco AnyConnect 클라이언트가 모두 VPN 액세스에 사용되는 경우 Web Security Appliance에서 자동으로 원격 사용자를 식별합니다. 그렇지 않으면, Web Security Appliance 관리자가 IP 주소의 범위를 구성하여 원격 사용자를 지정해야 합니다.
- **로컬 사용자.** 이러한 사용자는 네트워크에 물리적으로 또는 무선으로 연결되어 있습니다.

Web Security Appliance가 Cisco ASA와 통합되는 경우 인증된 사용자 이름으로 투명하게 사용자를 식별하도록 구성하여 원격 사용자에 대한 단일 로그인을 수행할 수 있습니다.

원격 사용자의 식별 구성 방법

작업	추가 정보
1. 원격 사용자의 식별을 구성합니다.	원격 사용자의 식별 구성, 10-19페이지
2. 원격 사용자의 ID를 생성합니다.	사용자 및 클라이언트 소프트웨어 분류, 6-3페이지 a. "Define Members by User Location(사용자 위치별 구성원 정의)" 섹션에서 "Remote Users Only(원격 사용자만)"를 선택합니다. b. "Define Members by Authentication(인증별 구성원 정의)" 섹션에서 "Identify Users Transparently through Cisco ASA Integration(Cisco ASA 통합을 통해 투명하게 사용자 식별)"을 선택합니다.
3. 원격 사용자에 대한 정책을 생성합니다.	정책 생성, 10-5페이지

원격 사용자의 식별 구성

1단계 Security Services(보안 서비스) > AnyConnect Secure Mobility를 선택하고 **Enable(사용)**을 클릭합니다.

2단계 AnyConnect Secure Mobility 라이센스 계약서의 약관을 읽고 **Accept(동의)**를 클릭합니다.

3단계 원격 사용자를 식별하는 방법을 구성합니다.

옵션	설명	추가 단계
IP 주소	어플라이언스가 원격 디바이스에 할당된 것으로 간주되어야 하는 IP 주소의 범위를 지정합니다.	1. IP Range(IP 범위) 필드에 IP 주소의 범위를 입력합니다. 2. 4단계로 이동합니다.
Cisco ASA Integration	Web Security Appliance가 통신하는 하나 이상의 Cisco ASA를 지정합니다. Cisco ASA에서 IP 주소와 사용자 간의 매핑을 유지 관리하며 Web Security Appliance에 해당 정보를 전달합니다. 웹 프록시가 트랜잭션을 수신할 때 IP 주소를 가져오고 IP 주소와 사용자 간의 매핑을 확인하여 사용자를 확인합니다. Cisco ASA와 통합하여 사용자를 확인하는 경우 원격 사용자에 대한 단일 로그인을 사용하도록 설정할 수 있습니다.	1. Cisco ASA 호스트 이름 또는 IP 주소를 입력합니다. 2. ASA에 액세스하는 데 사용되는 포트 번호를 입력합니다. Cisco ASA의 기본 포트 번호는 11999입니다. 3. 클러스터에 여러 Cisco ASA가 구성되어 있는 경우 **Add Row(행 추가)**를 클릭하고 클러스터의 각 ASA를 구성합니다. **참고** 고가용성을 위해 2개의 Cisco ASA가 구성된 경우 *활성* Cisco ASA에 대한 하나의 호스트 이름 또는 IP 주소만 입력합니다. 4. Cisco ASA에 대한 액세스 암호를 입력합니다. **참고** 여기에 입력하는 암호는 지정된 Cisco ASA에 대해 구성된 액세스 암호와 일치해야 합니다. 5. 선택적으로 **Start Test(테스트 시작)**를 클릭하여 Web Security Appliance가 구성된 Cisco ASA에 연결할 수 있는지 확인합니다.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

ASA에 대한 원격 사용자 상태 및 통계 표시

Web Security Appliance가 ASA와 통합될 때 모빌리티 보안 관련 정보를 표시하려면 다음 명령을 사용합니다.

명령	설명
`musstatus`	이 명령은 다음 정보를 표시합니다. • 각 ASA와의 Web Security Appliance 연결 상태 • 각 ASA와의 Web Security Appliance 연결 지속시간(분) • 각 ASA의 원격 클라이언트 수 • 서비스되는 원격 클라이언트 수, Web Security Appliance를 통해 트래픽을 전달한 원격 클라이언트 수로 정의됩니다. • 전체 원격 클라이언트 수

정책 트러블슈팅

- HTTPS에 대한 액세스 정책을 구성할 수 없음, A-13페이지
- 일부 Microsoft Office 파일이 차단되지 않음, A-14페이지
- DOS 실행 가능 개체 유형을 차단하면 Windows OneCare에 대한 업데이트도 차단됨, A-14페이지
- 식별 프로필이 정책에서 사라짐, A-14페이지
- 정책이 적용되지 않음, A-14페이지
- HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨, A-15페이지
- 사용자가 HTTPS 및 FTP over HTTP 요청에 대한 전역 정책과 일치함, A-15페이지
- 사용자가 잘못된 액세스 정책에 할당됨, A-15페이지
- 정책 트러블슈팅 툴: 정책 추적, A-16페이지

11 장

HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성

- HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성 개요, 11-1페이지
- 암호 해독 정책을 통한 HTTPS 트래픽 관리 모범 사례, 11-2페이지
- 암호 해독 정책, 11-2페이지
- 루트 인증서, 11-6페이지
- HTTPS 트래픽 라우팅, 11-12페이지

HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성 개요

암호 해독 정책은 웹 프록시 내의 HTTPS 트래픽 처리를 정의합니다.

- HTTPS 트래픽의 암호를 해독하는 시기
- 유효하지 않거나 폐기된 보안 인증서를 사용하는 요청을 처리하는 방법

다음 방법으로 HTTPS 트래픽을 처리하기 위한 암호 해독 정책을 생성할 수 있습니다.

- 암호화된 트래픽 통과
- 트래픽의 암호를 해독하고 HTTP 트래픽에 대해 정의된 콘텐츠 기반 액세스 정책 적용. 또한 이를 통해 악성코드 스캐닝이 가능하게 됩니다.
- HTTPS 연결 삭제
- 웹 프록시가 정책과 비교하여 계속해서 요청을 평가할 때 요청 모니터링(최종 조치를 수행하지 않음). 최종 조치는 삭제, 통과 또는 암호 해독이 될 수 있습니다.

주의 **개인적으로 식별 가능한 정보를 주의하여 처리:** 최종 사용자의 HTTPS 세션 암호를 해독하도록 선택하면 웹 보안 어플라이언스 액세스 로그 및 보고서에 개인적으로 식별 가능한 정보가 포함될 수 있습니다. 관리자는 `advancedproxyconfig` CLI 명령 및 `HTTPS` 하위 명령을 사용하여 얼마나 많은 URI 텍스트가 로그에 저장되는지 구성할 수 있습니다. 전체 URI 또는 쿼리 부분이 제거된 일부 URI 양식을 기록할 수 있습니다. 그러나 URI에서 쿼리를 제거하도록 선택하는 경우에도 개인적으로 식별 가능한 정보가 여전히 남아 있을 수 있습니다.

암호 해독 정책을 통한 HTTPS 트래픽 관리 작업 개요

단계	암호 해독 정책을 통한 HTTPS 트래픽 관리 작업 목록	관련 주제 및 절차에 대한 링크
1	HTTPS 프록시 사용	HTTPS 프록시 사용, 11-3페이지
2	인증서 및 키 업로드 또는 생성	• 루트 인증서 및 키 업로드, 11-7페이지 • HTTPS 프록시에 대한 인증서 및 키 생성, 11-8페이지
3	암호 해독 옵션 구성	암호 해독 옵션 구성, 11-5페이지
5	(선택 사항) 유효하지 않은 인증서 처리 구성	유효하지 않은 인증서 처리 구성, 11-9페이지
6	(선택 사항) 실시간 폐기 상태 확인 사용	실시간 폐기 상태 확인 사용, 11-10페이지
7	(선택 사항) 신뢰할 수 있는 인증서 및 차단된 인증서 관리	신뢰할 수 있는 루트 인증서, 11-11페이지

암호 해독 정책을 통한 HTTPS 트래픽 관리 모범 사례

- 네트워크에 있는 모든 사용자 또는 더 적거나 더 많은 사용자 그룹에 적용되는 더 적고 일반적인 암호 해독 정책 그룹을 생성합니다. 그런 다음, 암호 해독된 HTTPS 트래픽에 더 세분화된 제어를 적용해야 하는 경우 더 구체적인 액세스 정책 그룹을 사용하십시오.

암호 해독 정책

어플라이언스는 HTTPS 연결 요청에 대해 다음 조치 중 하나를 수행할 수 있습니다.

옵션	설명
모니터링	모니터링은 웹 프록시가 계속해서 트랜잭션을 다른 제어 설정에 대해 평가하여 궁극적으로 적용할 최종 조치를 결정해야 함을 표시하는 중간 조치입니다.
삭제	어플라이언스가 연결을 삭제하고 연결 요청을 서버로 전달하지 않습니다. 어플라이언스가 연결을 삭제했다고 사용자에게 알리지 않습니다.
통과	어플라이언스가 트래픽 콘텐츠를 검사하지 않고 클라이언트와 서버 간의 연결을 통과합니다.
암호 해독	어플라이언스가 연결을 허용하지만 트래픽 콘텐츠를 검사합니다. 트래픽의 암호를 해독하고 일반 텍스트 HTTP 연결인 것처럼 암호 해독된 트래픽에 액세스 정책을 적용합니다. 연결 암호를 해독하고 액세스 정책을 적용하여 트래픽에서 악성코드를 스캐닝할 수 있습니다.

HTTPS 프록시 사용

HTTPS 트래픽을 모니터링하고 암호 해독하려면 HTTPS 프록시를 사용하도록 설정해야 합니다. HTTPS 프록시를 사용하도록 설정하는 경우 어플라이언스가 자체 서명된 서버 인증서를 네트워크의 클라이언트 애플리케이션으로 전송할 때 루트 인증서를 위해 사용할 내용을 구성해야 합니다. 이미 조직에 있는 루트 인증서 및 키를 업로드하거나 사용자가 입력하는 정보로 인증서 및 키를 생성하도록 어플라이언스를 구성할 수 있습니다.

HTTPS 프록시가 사용하도록 설정되면 모든 HTTPS 정책 결정이 암호 해독 정책에 따라 처리됩니다. 또한 이 페이지에서 서버 인증서가 유효하지 않은 경우 어플라이언스가 HTTPS 트래픽을 처리하는 방법을 구성할 수 있습니다.

시작하기 전에

- HTTPS 프록시가 사용하도록 설정되면 액세스 정책의 HTTPS 특정 규칙이 사용하지 않도록 설정되고 웹 프록시에서 HTTP에 대한 규칙을 사용하여 암호 해독된 HTTPS 트래픽을 처리합니다.

1단계 Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시)를 선택하고 **Enable and Edit Settings(설정 사용 및 편집)**를 클릭합니다.

HTTPS 프록시 라이센스 계약서가 표시됩니다.

2단계 HTTPS 프록시 라이센스 계약의 약관을 읽고 **Accept(동의)**를 클릭합니다.

3단계 Enable HTTPS Proxy(HTTPS 프록시 사용) 필드가 사용하도록 설정되었는지 확인합니다.

4단계 HTTPS Ports to Proxy(프록시에 대한 HTTPS 포트) 필드에 어플라이언스가 HTTPS 트래픽을 확인해야 하는 포트를 입력합니다. 포트 443이 기본 포트입니다.

참고 웹 보안 어플라이언스에서 프록시로 사용할 수 있는 최대 포트 수는 30개이며, 여기에는 HTTP 및 HTTPS가 모두 포함됩니다.

5단계 암호 해독에 사용할 루트/서명 인증서를 업로드 **또는** 생성합니다.

참고 업로드된 인증서 및 키 쌍과 생성된 인증서 및 키 쌍이 모두 어플라이언스에 있는 경우 Root Certificate for Signing(서명을 위한 루트 인증서) 섹션에서 현재 선택한 인증서 및 키 쌍만을 사용합니다.

6단계 HTTPS Transparent Request(HTTPS 투명 요청) 섹션에서 다음 옵션 중 하나를 선택합니다.

- HTTPS 요청 암호 해독 및 인증을 위해 리디렉션
- HTTPS 요청 거부

이 설정은 사용자가 아직 인증되지 않은 경우에 IP 주소를 인증 서로게이트로 사용하는 트랜잭션에만 적용됩니다.

참고 이 필드는 어플라이언스가 투명 모드에서 구축되는 경우에만 표시됩니다.

7단계 Applications that Use HTTPS(HTTPS를 사용하는 애플리케이션) 섹션에서 애플리케이션 가시성 및 제어를 향상시키기 위해 암호 해독을 사용하도록 설정할지 여부를 선택합니다.

참고 클라이언트에 서명을 위한 루트 인증서가 설치되어 있지 않으면 암호 해독 중에 일부 애플리케이션이 실패할 수 있습니다. 어플라이언스 루트 인증서에 대한 자세한 내용은 다음을 참조하십시오.

8단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- HTTPS에 대한 인증서 검증 및 암호 해독 관리, 11-6페이지

HTTPS 트래픽 제어

웹 보안 어플라이언스에서 암호 해독 정책 그룹에 HTTPS 연결 요청을 할당한 후에 연결 요청이 해당 정책 그룹의 제어 설정을 상속합니다. 암호 해독 정책 그룹의 제어 설정에 따라 어플라이언스에서 연결을 암호 해독하거나, 삭제하거나, 통과시키는지가 결정됩니다.

옵션	설명
URL 카테고리	각각의 미리 정의된 맞춤형 URL 카테고리에 대한 HTTPS 요청에 대해 수행할 조치를 구성할 수 있습니다. 구성할 정책 그룹에 해당하는 URL Categories(URL 카테고리) 열 아래의 링크를 클릭합니다. **참고** 삭제(최종 사용자에게 알리지 않음) 대신에 HTTPS 요청에 대해 특정 URL 카테고리를 *차단*(최종 사용자에게 알림)하려는 경우 암호 해독 정책 그룹에서 해당 URL 카테고리를 암호 해독하도록 선택한 후 액세스 정책 그룹에서 동일한 URL 카테고리를 차단하도록 선택합니다.
웹 평판	요청된 서버의 웹 평판 점수를 기준으로 HTTPS 요청에 대해 수행할 조치를 구성할 수 있습니다. 구성할 정책 그룹에 해당하는 Web Reputation(웹 평판) 열 아래의 링크를 클릭합니다.
기본 조치	다른 설정이 적용되지 않을 때 어플라이언스에서 수행해야 하는 조치를 구성할 수 있습니다. 구성할 정책 그룹에 해당하는 Default Action(기본 조치) 열 아래의 링크를 클릭합니다. **참고** 구성된 기본 조치는 URL 카테고리 또는 웹 평판 점수를 기준으로 결정을 내리지 않은 경우에만 트랜잭션에 영향을 미칩니다. 웹 평판 필터링이 사용하지 않도록 설정된 경우 URL 카테고리의 모니터링 조치와 일치하는 모든 트랜잭션에 기본 조치가 적용됩니다. 웹 평판 필터링이 사용하도록 설정된 경우 점수가 없는 사이트에 대해 모니터링 조치가 선택된 경우에만 기본 조치가 사용됩니다.

암호 해독 옵션 구성

시작하기 전에

- HTTPS 프록시 사용, 11-3페이지에 설명된 대로 HTTPS 프록시가 사용하도록 설정되었는지 확인합니다.

1단계 **Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 암호 해독 옵션을 사용하도록 설정합니다.

암호 해독 옵션	설명
인증을 위한 암호 해독	이 HTTPS 트랜잭션 이전에 인증되지 않은 사용자를 위해 인증을 위한 암호 해독을 허용합니다.
최종 사용자 알림을 위한 암호 해독	AsyncOS가 최종 사용자 알림을 표시할 수 있도록 암호 해독을 허용합니다. **참고** 인증서가 유효하지 않고 유효하지 않은 인증서를 삭제하도록 설정한 경우 정책 추적을 실행할 때 트랜잭션에 대해 처음으로 기록되는 조치는 "암호 해독"입니다.
최종 사용자 승인을 위한 암호 해독	이 HTTPS 트랜잭션 이전에 웹 프록시를 승인하지 않은 사용자를 위해 AsyncOS가 최종 사용자 승인을 표시할 수 있도록 암호 해독을 허용합니다.
애플리케이션 탐지를 위한 암호 해독	HTTPS 애플리케이션을 탐지하는 AsyncOS의 기능을 강화합니다.

인증 및 HTTPS 연결

HTTPS 연결 레이어의 인증은 다음과 같은 유형의 요청에 사용할 수 있습니다.

옵션	설명
명시적 요청	• 보안 클라이언트 인증이 사용되지 않음 또는 • 보안 클라이언트 인증이 사용됨 및 IP 기반 서로게이트
투명 요청	• IP 기반 서로게이트, 인증을 위한 암호 해독이 사용됨 또는 • IP 기반 서로게이트, 이전에 HTTP 요청을 사용하여 인증된 클라이언트

루트 인증서

HTTPS 프록시는 어플라이언스에 업로드하는 루트 인증서 및 개인 키 파일을 사용하여 트래픽의 암호를 해독합니다. 어플라이언스에 업로드하는 루트 인증서 및 개인 키 파일은 PEM 형식이어야 합니다. DER 형식은 지원되지 않습니다.

다음 방법으로 루트 인증서 정보를 입력할 수 있습니다.

- **생성.** 일부 기본 조직 정보를 입력한 후 버튼을 클릭하여 어플라이언스에서 나머지 인증서와 개인 키를 생성하도록 할 수 있습니다.
- **업로드.** 어플라이언스의 외부에서 생성된 인증서 파일 및 이와 일치하는 개인 키 파일을 업로드할 수 있습니다.

참고 또한 루트 인증 기관에서 서명된 중간 인증서를 업로드할 수도 있습니다. 웹 프록시가 서버 인증서를 모방하는 경우 업로드된 인증서를 모방된 인증서와 함께 클라이언트 애플리케이션에 전송합니다. 이러한 방식으로 중간 인증서가 클라이언트 애플리케이션에서 신뢰하는 루트 인증 기관에서 서명된 경우에는 애플리케이션이 모방된 서버 인증서도 신뢰합니다. 자세한 내용은 인증서 및 키 정보, 22-24페이지를 참조하십시오.

웹 보안 어플라이언스에서 발급된 루트 인증서를 처리하는 방법을 선택할 수 있습니다.

- **루트 인증서를 수락하도록 사용자에게 알립니다.** 조직의 사용자에게 회사의 새로운 정책에 대해 알리고 조직에서 제공하는 루트 인증서를 신뢰할 수 있는 소스로 수락하도록 통지할 수 있습니다.
- **루트 인증서를 클라이언트 머신에 추가합니다.** 신뢰할 수 있는 루트 인증 기관으로 네트워크에 있는 모든 클라이언트 머신에 루트 인증서를 추가할 수 있습니다. 이렇게 하면 클라이언트 애플리케이션이 루트 인증서를 포함하는 트랜잭션을 자동으로 수락합니다.

1단계 Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시).

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 생성되거나 업로드된 인증서에 대한 Download Certificate(인증서 다운로드) 링크를 클릭합니다.

참고 클라이언트 머신에서 인증서 오류가 발생할 수 있는 가능성을 줄이려면 루트 인증서를 생성하거나 웹 보안 어플라이언스에 업로드한 후 변경 사항을 제출하고 인증서를 클라이언트 머신에 배포한 다음 변경 사항을 어플라이언스에 커밋합니다.

HTTPS에 대한 인증서 검증 및 암호 해독 관리

Web Security Appliance는 콘텐츠를 검사하고 암호 해독하기 전에 인증서를 검증합니다.

유효한 인증서

유효한 인증서의 특성:

- **만료되지 않음.** 인증서의 유효 기간에 현재 날짜가 포함됩니다.
- **인식되는 인증 기관.** 발급 인증 기관은 Web Security Appliance에 저장된 신뢰할 수 있는 인증 기관 목록에 포함되어 있습니다.

- **유효한 시그니처.** 디지털 시그니처가 암호화 표준에 따라 적절하게 구현되었습니다.
- **일관된 이름 지정.** 공용 이름이 HTTP 헤더에 지정된 호스트 이름과 일치합니다.
- **폐기되지 않음.** 발급 인증 기관이 인증서를 폐기하지 않았습니다.

관련 주제

- HTTPS에 대한 인증서 검증 및 암호 해독 관리, 11-6페이지
- 유효하지 않은 인증서 처리 구성, 11-9페이지
- 인증서 폐기 상태 확인 옵션, 11-9페이지
- 실시간 폐기 상태 확인 사용, 11-10페이지

유효하지 않은 인증서 처리

어플라이언스에서는 유효하지 않은 서버 인증서에 대해 다음 조치 중 하나를 수행할 수 있습니다.

- **삭제**
- **암호 해독**
- **모니터링**

여러 가지 이유로 유효하지 않은 인증서

인식되지 않는 루트 인증 기관과 만료된 인증서로 인해 유효하지 않은 서버 인증서의 경우 HTTPS 프록시에서는 인식되지 않는 루트 인증 기관에 적용할 조치를 수행합니다.

다른 모든 경우에는 HTTPS 프록시가 동시에 여러 가지 이유로 인해 유효하지 않은 서버 인증서에 대해 가장 제한적인 조치에서 덜 제한적인 조치의 순서로 조치를 수행합니다.

암호 해독된 연결에 대한 신뢰할 수 없는 인증서 경고

웹 보안 어플라이언스가 유효하지 않은 인증서를 발견하고 연결의 암호를 해독하도록 구성된 경우 AsyncOS에서는 최종 사용자가 연결을 수락하거나 거부해야 하는 신뢰할 수 없는 인증서를 생성합니다. 인증서의 공용 이름은 "Untrusted Certificate Warning(신뢰할 수 없는 인증서 경고)"입니다.

이 신뢰할 수 없는 인증서를 신뢰할 수 있는 인증서 목록에 추가하면 연결을 수락하거나 거부할 수 있는 최종 사용자 옵션이 제거됩니다.

AsyncOS에서는 이러한 인증서 중 하나를 생성할 때 "Signing untrusted key(신뢰할 수 없는 키 서명)" 또는 "Signing untrusted cert(신뢰할 수 없는 인증서 서명)" 텍스트가 포함된 프록시 로그 항목을 생성합니다.

루트 인증서 및 키 업로드

시작하기 전에

- HTTPS 프록시를 사용하도록 설정합니다. HTTPS 프록시 사용, 11-3페이지.

1단계 **Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Use Uploaded Certificate and Key(업로드된 인증서 및 키 사용)**를 선택합니다.

4단계 Certificate(인증서) 필드에 대해 **Browse(찾아보기)**를 클릭하여 로컬 머신에 저장된 인증서 파일을 탐색합니다.

업로드하는 파일에 여러 인증서 또는 키가 포함되어 있는 경우 웹 프록시에서는 파일에 있는 첫 번째 인증서 또는 키를 사용합니다.

5단계 Key(키) 필드에 대해 **Browse(찾아보기)**를 클릭하여 개인 키 파일을 탐색합니다.

참고 키 길이는 512, 1024 또는 2048비트여야 합니다.

6단계 키가 암호화된 경우 **Key is Encrypted(키가 암호화됨)**를 선택합니다.

7단계 **Upload Files(파일 업로드)**를 클릭하여 웹 보안 어플라이언스에 인증서 및 키 파일을 전송합니다.

업로드된 인증서 정보가 Edit HTTPS Proxy Settings(HTTPS 프록시 설정 편집) 페이지에 표시됩니다.

8단계 (선택 사항) 네트워크에 있는 클라이언트 애플리케이션에 전송할 수 있도록 **Download Certificate(인증서 다운로드)**를 클릭합니다.

HTTPS 프록시에 대한 인증서 및 키 생성

시작하기 전에

- HTTPS 프록시를 사용하도록 설정합니다. HTTPS 프록시 사용, 11-3페이지.

1단계 **Security Services(보안 서비스)** > **HTTPS Proxy(HTTPS 프록시)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Use Generated Certificate and Key(생성된 인증서 및 키 사용)**를 선택합니다.

4단계 **Generate New Certificate and Key(새 인증서 및 키 생성)**를 클릭합니다.

5단계 Generate Certificate and Key(인증서 및 키 생성) 대화 상자에서 루트 인증서에 표시할 정보를 입력합니다.

Common Name(공용 이름) 필드에 슬래시(/)를 제외한 모든 ASCII 문자를 입력할 수 있습니다.

6단계 **Generate(생성)**를 클릭합니다.

7단계 생성된 인증서 정보가 Edit HTTPS Proxy Settings(HTTPS 프록시 설정 편집) 페이지에 표시됩니다.

8단계 (선택 사항) 네트워크에 있는 클라이언트 애플리케이션에 전송할 수 있도록 **Download Certificate(인증서 다운로드)**를 클릭합니다.

9단계 (선택 사항) CSR(Certificate Signing Request)을 CA(Certificate Authority)에 제출할 수 있도록 **Download Certificate Signing Request(인증서 서명 요청 다운로드)** 링크를 클릭합니다.

10단계 (선택 사항) 서명된 인증서를 CA에서 다시 수신한 후 웹 보안 어플라이언스에 업로드합니다. 어플라이언스에서 인증서를 생성한 후 언제든지 이를 수행할 수 있습니다.

11단계 **변경 사항을 제출** 및 **커밋합니다**.

유효하지 않은 인증서 처리 구성

시작하기 전에

- HTTPS 프록시 사용, 11-3페이지에 설명된 대로 HTTPS 프록시가 사용하도록 설정되었는지 확인합니다.

1단계 **Security Services(보안 서비스)** > **HTTPS Proxy(HTTPS 프록시)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 각 유형의 인증서 오류에 대한 프록시 응답(**삭제**, **암호 해독** 또는 **모니터링**)을 정의합니다.

인증서 오류 유형	설명
Expired	현재 날짜가 인증서의 유효 범위에서 벗어났습니다.
일치하지 않는 호스트 이름	인증서의 호스트 이름이 클라이언트가 액세스하려고 시도한 호스트 이름과 일치하지 않습니다. **참고** 웹 프록시가 명시적 전달 모드에 구축되는 경우에만 호스트 이름 일치를 수행할 수 있습니다. 투명 모드에서 구축되는 경우에는 목적지 서버의 호스트 이름을 알지 못하므로(IP 주소만 알고 있음) 서버 인증서의 호스트 이름과 비교할 수 없습니다.
인식되지 않는 루트 인증 기관/발급자	루트 인증 기관 또는 중간 인증 기관이 인식되지 않습니다.
유효하지 않은 서명 인증서	서명 인증서에 문제가 발생했습니다.
유효하지 않은 리프 인증서	리프 인증서에 문제가 발생했습니다(예: 거부, 복호화 또는 불일치 문제).
다른 모든 오류 유형	대부분의 기타 오류 유형은 어플라이언스가 HTTPS 서버와의 SSL 핸드셰이크를 완료할 수 없기 때문에 발생합니다. 서버 인증서의 추가 오류 시나리오에 대한 자세한 내용은 http://www.openssl.org/docs/apps/verify.html을 참조하십시오.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

인증서 폐기 상태 확인 옵션

발급 인증 기관이 인증서를 폐기했는지 여부를 확인하기 위해 웹 보안 어플라이언스에서 다음과 같은 방식으로 발급 인증 기관에 확인할 수 있습니다.

- **인증서 폐기 목록(Comodo 인증서 전용).** 웹 보안 어플라이언스에서 Comodo의 인증서 폐기 목록을 확인합니다. Comodo에서 자체 정책에 따라 이 목록을 업데이트하여 유지 관리합니다. 마지막으로 업데이트된 시간에 따라 웹 보안 어플라이언스에서 확인하는 시점에 인증서 폐기 목록이 최신 상태가 아닐 수 있습니다.
- **OCSP(Online Certificate Status Protocol).** 웹 보안 어플라이언스에서 실시간으로 발급 인증 기관에 폐기 상태를 확인합니다. 발급 인증 기관이 OCSP를 지원하는 경우 인증서에 실시간 상태 확인을 위한 URL이 포함됩니다. 신규 설치의 경우에는 이 기능이 기본적으로 사용하도록 설정되어 있고 업데이트의 경우에는 기본적으로 사용하지 않도록 설정되어 있습니다.

참고 Web Security Appliance는 다른 모든 측면에서 유효한 것으로 확인되고 OCSP URL을 포함하는 인증서에 대한 OCSP 쿼리만 수행합니다.

관련 주제

- 실시간 폐기 상태 확인 사용, 11-10페이지
- 유효하지 않은 인증서 처리 구성, 11-9페이지

실시간 폐기 상태 확인 사용

시작하기 전에

- HTTPS 프록시가 사용하도록 설정되었는지 확인합니다. HTTPS 프록시 사용, 11-3페이지를 참고하십시오.

1단계 **Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable Online Certificate Status Protocol(OCSP(Online Certificate Status Protocol) 사용)**을 선택합니다.

4단계 **OCSP Result Handling(OCSP 결과 처리)** 속성을 구성합니다.

Cisco에서는 OCSP Result Handling(OCSP 결과 처리) 옵션을 Invalid Certificate Handling(유효하지 않은 인증서 처리) 옵션과 동일한 조치로 구성하도록 권장합니다. 예를 들어, 만료된 인증서가 모니터링으로 설정된 경우 폐기된 인증서를 모니터링으로 구성합니다.

5단계 (선택 사항) Advanced(고급) 컨피그레이션 섹션을 확장한 후 아래 설명된 설정을 구성합니다.

필드 이름	설명
OCSP 유효한 응답 캐시 시간 초과	유효한 OCSP 응답을 다시 확인하기 전에 대기하는 시간이며, 초(s), 분(m), 시간(h) 또는 일(d) 단위를 사용합니다. 기본 단위는 초입니다. 유효한 범위는 1초에서 7일입니다.
OCSP 유효하지 않은 응답 캐시 시간 초과	유효하지 않은 OCSP 응답을 다시 확인하기 전에 대기하는 시간이며, 초(s), 분(m), 시간(h) 또는 일(d) 단위를 사용합니다. 기본 단위는 초입니다. 유효한 범위는 1초에서 7일입니다.
OCSP 네트워크 오류 캐시 시간 초과	응답을 얻는 데 실패한 후 OCSP 응답자와 연결하려고 시도하기 전에 대기하는 시간이며, 초(s), 분(m), 시간(h) 또는 일(d) 단위를 사용합니다. 유효한 범위는 1초에서 24시간입니다.
허용된 클록 스큐	웹 보안 어플라이언스와 OCSP 응답자 간의 시간 설정에서 허용되는 최대 차이이며, 초(s) 또는 분(m) 단위를 사용합니다. 유효한 범위는 1초에서 60분입니다.
OCSP 응답 최대 대기 시간	OCSP 응답자의 응답을 대기하는 최대 시간입니다. 유효한 범위는 1초에서 10분입니다. OCSP 응답자가 사용 불가능한 경우 HTTPS 요청에 대한 최종 사용자 액세스의 지연 시간을 줄이려면 더 짧은 지속시간을 지정합니다.
OCSP 검사에 업스트림 프록시 사용	업스트림 프록시의 그룹 이름입니다.
업스트림 프록시에서 서버 제외	제외할 서버의 IP 주소 또는 호스트 이름입니다. 비워 둘 수 있습니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

신뢰할 수 있는 루트 인증서

Web Security Appliance는 신뢰할 수 있는 루트 인증서 목록과 함께 제공되며 이 목록을 유지 관리합니다. 신뢰할 수 있는 인증서가 있는 웹 사이트에서는 암호 해독이 필요하지 않습니다.

인증서를 추가하고 기능적으로 인증서를 제거하여 신뢰할 수 있는 인증서 목록을 관리할 수 있습니다. Web Security Appliance는 인증서를 마스터 목록에서 삭제하지 않지만 인증서의 신뢰를 재지정하도록 허용하여 신뢰할 수 있는 목록에서 기능적으로 인증서를 제거합니다.

신뢰할 수 있는 목록에 인증서 추가

시작하기 전에

- HTTPS 프록시가 사용하도록 설정되었는지 확인합니다. HTTPS 프록시 사용, 11-3페이지를 참고하십시오.

1단계 **Security Services(보안 서비스)** > **HTTPS Proxy(HTTPS 프록시)**.

2단계 **Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)**를 클릭합니다.

3단계 **Import(가져오기)**를 클릭합니다.

4단계 **Browse(찾아보기)**를 클릭하고 인증서 파일로 이동합니다.

5단계 **변경 사항**을 **제출** 및 **커밋합니다**.

Custom Trusted Root Certificates(맞춤형 신뢰할 수 있는 루트 인증서) 목록에서 업로드한 인증서를 찾습니다.

신뢰할 수 있는 목록에서 인증서 제거

1단계 **Security Services(보안 서비스)**> **HTTPS Proxy(HTTPS 프록시)**를 선택합니다.

2단계 **Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)**를 클릭합니다.

3단계 목록에서 제거할 인증서에 해당하는 **Override Trust(신뢰 재지정)** 확인란을 선택합니다.

4단계 **변경 사항**을 **제출** 및 **커밋합니다**.

HTTPS 트래픽 라우팅

클라이언트 헤더에 저장된 정보를 기반으로 HTTPS 트랜잭션을 라우팅하는 AsyncOS의 기능이 제한되고 투명 및 명시적 HTTPS에 대해 서로 다릅니다.

옵션	설명
투명 HTTPS	투명 HTTPS의 경우 AsyncOS는 클라이언트 헤더에 있는 정보에 액세스할 수 없습니다. 따라서 AsyncOS는 클라이언트 헤더의 정보에 의존하는 라우팅 정책을 시행할 수 없습니다.
명시적 HTTPS	명시적 HTTPS의 경우 AsyncOS가 클라이언트 헤더에 있는 다음 정보에 액세스할 수 있습니다. • URL • 대상 포트 번호 따라서 명시적 HTTPS 트랜잭션의 경우 URL 또는 포트 번호에 따라 라우팅 정책을 일치시킬 수 있습니다.

암호 해독/HTTPS/인증서 트러블슈팅

- URL 카테고리 기준을 사용하는 라우팅 정책을 통해 HTTPS 사이트에 액세스, A-8페이지
- IP 기반 서로게이트 및 투명 요청을 사용하는 HTTPS, A-8페이지
- 특정 웹 사이트에 대한 암호 해독 우회, A-8페이지
- 경고: 보안 인증서 문제, A-9페이지

기존 감염에 대한 아웃바운드 트래픽 스캐닝

- 아웃바운드 트래픽 스캐닝 개요, 12-1페이지
- 업로드 요청 이해, 12-2페이지
- 아웃바운드 악성프로그램 검색 정책 생성, 12-3페이지
- 업로드 요청 제어, 12-4페이지
- DVS 스캐닝 기록, 12-5페이지

아웃바운드 트래픽 스캐닝 개요

악의적인 데이터가 네트워크에서 나가지 않도록 하기 위해 웹 보안 어플라이언스에서 아웃바운드 악성프로그램 검색 기능을 제공합니다. 정책 그룹을 사용하여 악성코드를 스캐닝할 업로드, 스캐닝에 사용할 안티멀웨어 스캐닝 엔진 및 차단할 악성코드 유형을 정의할 수 있습니다.

트랜잭션 요청이 네트워크에서 나갈 때 Cisco IronPort DVS(Dynamic Vectoring and Streaming) 엔진이 트랜잭션 요청을 스캐닝합니다. Cisco IronPort DVS 엔진을 사용하여 작업하면 웹 보안 어플라이언스를 통해 사용자가 의도하지 않게 악의적인 데이터를 업로드하지 못하도록 방지할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

작업	작업 링크
악성코드를 차단하기 위한 정책 생성	아웃바운드 악성코드 스캐닝 정책 생성, 12-4페이지
아웃바운드 악성코드 정책 그룹에 업로드 요청 할당	업로드 요청 제어, 12-6페이지

요청이 DVS 엔진에서 차단된 경우 사용자 경험

Cisco IronPort DVS 엔진이 업로드 요청을 차단하는 경우 웹 프록시가 최종 사용자에게 차단 페이지를 전송합니다. 그러나 모든 웹 사이트가 최종 사용자에게 차단 페이지를 표시하지는 않습니다. 일부 Web 2.0 웹 사이트는 정적 웹 페이지 대신에 javascript를 사용하여 동적 콘텐츠를 표시하고 차단 페이지를 표시하지 않을 수 있습니다. 계속해서 사용자가 악의적인 데이터를 업로드하지 못하도록 적절히 차단되지만 웹 사이트에서 항상 사용자에게 이에 대해 알리지 않을 수 있습니다.

업로드 요청 이해

아웃바운드 악성프로그램 검색 정책은 웹 프록시가 데이터를 서버에 업로드하는 트랜잭션(업로드 요청)에 대한 암호 해독된 HTTPS 연결 또는 HTTP 요청을 차단하는지 여부를 정의합니다. 업로드 요청은 요청 본문에 콘텐츠가 있는 HTTP 또는 암호 해독된 HTTPS 요청입니다.

웹 프록시가 업로드 요청을 수신하면 요청을 아웃바운드 악성프로그램 검색 정책 그룹과 비교하여 적용할 정책 그룹을 결정합니다. 요청을 정책 그룹에 할당한 후 요청을 정책 그룹의 구성된 제어 설정과 비교하여 요청을 차단할지 또는 요청을 모니터링할지를 결정합니다. 아웃바운드 악성프로그램 검색 정책이 요청을 모니터링하도록 결정하면 요청을 액세스 정책에 대해 평가하고 적용 가능한 액세스 정책에 따라 웹 프록시가 요청에 대해 수행하는 최종 조치를 결정합니다.

참고 파일 크기가 0바이트인 파일을 업로드하려고 시도하는 업로드 요청은 아웃바운드 악성프로그램 검색 정책에 대해 평가되지 않습니다.

그룹 구성원 자격에 대한 기준

각 클라이언트 요청이 ID에 할당된 후 다른 정책 유형에 대해 평가되어 각 유형마다 클라이언트 요청이 속해 있는 정책 그룹을 판별합니다. 웹 프록시가 클라이언트 요청의 정책 그룹 구성원 자격을 기반으로 구성된 정책 제어 설정을 클라이언트 요청에 적용합니다.

웹 프록시는 특정 프로세스에 따라 그룹 구성원 자격 기준을 일치시킵니다. 그룹 구성원 자격에 대해 다음 요인을 고려합니다.

기준	설명
ID	각 클라이언트 요청이 ID와 일치하고 인증에 실패하여 게스트 액세스가 부여되거나 인증에 실패하여 종료됩니다.
인증된 사용자	할당된 ID에 인증이 필요한 경우 정책 그룹과 일치하려면 사용자가 아웃바운드 악성프로그램 검색 정책 그룹의 인증된 사용자 목록에 있어야 합니다. 인증된 사용자 목록은 지정된 그룹 또는 사용자이거나, ID가 게스트 액세스를 허용하는 경우에는 게스트 사용자일 수 있습니다.
고급 옵션	아웃바운드 악성프로그램 검색 정책 그룹 구성원 자격에 대한 몇 가지 고급 옵션을 구성할 수 있습니다. ID 내에 프록시 포트 및 URL 카테고리와 같은 일부 옵션을 정의할 수도 있습니다. ID에 고급 옵션이 구성된 경우 아웃바운드 악성프로그램 검색 정책 그룹 레벨에서 구성할 수 없습니다.

클라이언트 요청을 아웃바운드 악성프로그램 검색 정책 그룹과 일치

웹 프록시가 업로드 요청 상태를 첫 번째 정책 그룹의 구성원 자격 기준과 비교합니다. 일치하는 경우 웹 프록시가 해당 정책 그룹의 정책 설정을 적용합니다.

일치하지 않는 경우 웹 프록시가 업로드 요청을 다음 정책 그룹과 비교합니다. 업로드 요청이 사용자 정의 정책 그룹과 일치할 때까지 이 프로세스를 계속 진행합니다. 사용자 정의 정책 그룹과 일치하지 않는 경우 전역 정책 그룹과 일치됩니다. 웹 프록시가 업로드 요청을 정책 그룹 또는 전역 정책 그룹과 일치시킬 때 해당 정책 그룹의 정책 설정을 적용합니다.

아웃바운드 악성프로그램 검색 정책 생성

하나 이상의 ID 또는 대상 사이트의 URL 카테고리와 같은 몇 가지 기준의 조합을 기반으로 아웃바운드 악성프로그램 검색 정책 그룹을 생성할 수 있습니다. 정책 그룹 구성원 자격에 대한 하나 이상의 기준을 정의해야 합니다. 여러 기준을 정의하는 경우 정책 그룹과 일치하려면 업로드 요청이 모든 기준을 충족해야 합니다. 그러나 업로드 요청은 구성된 ID 중 하나에만 일치해야 합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Outbound Malware Scanning(아웃바운드 악성코드 스캐닝)**을 선택합니다.

2단계 **Add Policy(정책 추가)**를 클릭합니다.

3단계 정책 그룹의 이름과 설명(선택 사항)을 입력합니다.

참고 각 정책 그룹 이름은 고유해야 하며 영숫자 또는 공백 문자만 포함해야 합니다.

4단계 Insert Above Policy(정책 위에 삽입) 필드에서 정책 그룹을 배치할 정책 테이블의 위치를 선택합니다.

여러 정책 그룹을 구성하는 경우 각 그룹의 논리적 순서를 지정해야 합니다.

5단계 **Identities and Users(ID 및 사용자)** 섹션에서 이 정책 그룹에 적용할 하나 이상의 ID 그룹을 선택합니다.

6단계 (선택 사항) 추가 구성원 자격 요건을 정의하려면 Advanced(고급) 섹션을 확장합니다.

7단계 고급 옵션을 사용하여 정책 그룹 구성원 자격을 정의하려면 고급 옵션에 대한 링크를 클릭하고 표시되는 페이지에서 옵션을 구성합니다.

고급 옵션	설명
프로토콜	클라이언트 요청에서 사용된 프로토콜별로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 포함할 프로토콜을 선택합니다. "All others(기타 모두)"는 프로토콜이 이 옵션 위에 나열되지 않음을 의미합니다. **참고** HTTPS 프록시가 사용하도록 설정되면 암호 해독 정책만 HTTPS 트랜잭션에 적용됩니다. 액세스, 라우팅, 아웃바운드 악성프로그램 검색, 데이터 보안 또는 외부 DLP 정책에 대한 정책 구성원 자격은 HTTPS 프로토콜로 정의할 수 없습니다.
프록시 포트	프록시 포트에서 웹 프록시에 액세스하는 데 사용되는 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. Proxy Ports(프록시 포트) 필드에 하나 이상의 포트 번호를 입력합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오. 명시적 전달 연결의 경우에는 브라우저에 구성된 포트입니다. 투명한 연결의 경우에는 목적지 포트와 동일합니다. 클라이언트 요청이 어플라이언스에 투명하게 리디렉션되는 경우 프록시 포트별로 정책 그룹 구성원 자격을 정의하면 일부 요청이 거부될 수 있습니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정을 사용하여 ID 구성원 자격을 정의하는 경우 비ID 정책 그룹 레벨에서 설정을 구성할 수 없습니다.

고급 옵션	설명
서브넷	서브넷 또는 기타 주소별로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 연결된 ID로 정의될 수 있는 주소를 사용하도록 선택하거나 여기에 특정 주소를 입력할 수 있습니다. **참고** 이 정책 그룹과 연결된 ID가 주소별로 구성원 자격을 정의하는 경우 이 정책 그룹에서 ID에 정의된 주소의 하위 집합인 주소를 입력해야 합니다. 정책 그룹에 주소를 추가하면 이 정책 그룹과 일치하는 트랜잭션 목록이 더 줄어듭니다.
URL 카테고리	URL 카테고리별로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 사용자 정의된 URL 카테고리 또는 미리 정의된 URL 카테고리를 선택합니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정을 사용하여 ID 구성원 자격을 정의하는 경우 비ID 정책 그룹 레벨에서 설정을 구성할 수 없습니다.
사용자 에이전트	클라이언트 요청에서 사용된 사용자 에이전트별로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 일반적으로 정의된 일부 브라우저를 선택하거나 정규식을 사용하여 고유한 브라우저를 정의할 수 있습니다. 이 정책 그룹이 선택한 사용자 에이전트에 적용되어야 하는지 또는 선택한 사용자 에이전트 목록에 없는 모든 사용자 에이전트에 적용되어야 하는지를 선택합니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정을 사용하여 ID 구성원 자격을 정의하는 경우 비ID 정책 그룹 레벨에서 설정을 구성할 수 없습니다.
사용자 위치	사용자 위치(원격 또는 로컬)별로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다.

8단계 변경 사항을 제출합니다.

9단계 아웃바운드 악성프로그램 검색 정책 그룹 제어 설정을 구성하여 웹 프록시에서 트랜잭션을 처리하는 방법을 정의합니다.

각 제어 설정에 대한 옵션을 구성할 때까지 새 아웃바운드 악성프로그램 검색 정책 그룹이 자동으로 전역 정책 그룹 설정을 상속합니다.

10단계 **변경 사항을 제출 및 커밋합니다.**

업로드 요청 제어

각 업로드 요청이 아웃바운드 악성프로그램 검색 정책 그룹에 할당되고 해당 정책 그룹의 제어 설정을 상속합니다. 웹 프록시가 업로드 요청 헤더를 수신하면 요청 본문을 스캐닝해야 하는지 여부를 결정하는 데 필요한 정보를 보유하게 됩니다. DVS 엔진이 요청을 스캐닝하고 웹 프록시에 판정을 반환합니다. 해당되는 경우 최종 사용자에게 차단 페이지가 표시됩니다.

1단계 **Web Security Manager(웹 보안 관리자) > Outbound Malware Scanning(아웃바운드 악성코드 스캐닝)**을 선택합니다.

2단계 Destinations(대상) 열에서 구성할 정책 그룹에 대한 링크를 클릭합니다.

3단계 **Edit Destination Settings(대상 설정 편집)** 섹션의 드롭다운 목록에서 "Define Destinations Scanning Custom Settings(대상 스캐닝 맞춤형 설정 정의)"를 선택합니다.

4단계 **Destinations to Scan(스캐닝 대상)** 섹션에서 다음 중 하나를 선택합니다.

옵션	설명
업로드를 검사하지 않음	DVS 엔진이 업로드 요청을 스캐닝하지 않습니다. 모든 업로드 요청이 액세스 정책과 비교하여 평가됩니다.
모든 업로드 검사	DVS 엔진이 모든 업로드 요청을 스캐닝합니다. DVS 엔진 스캐닝 판정에 따라 업로드 요청이 차단되거나 액세스 정책과 비교하여 평가됩니다.
지정된 맞춤형 URL 카테고리에 대한 업로드 스캐닝	DVS 엔진이 특정 맞춤형 URL 카테고리에 속하는 업로드 요청을 스캐닝합니다. DVS 엔진 스캐닝 판정에 따라 업로드 요청이 차단되거나 액세스 정책과 비교하여 평가됩니다. 스캐닝할 URL 카테고리를 선택하려면 **Edit custom categories list(맞춤형 카테고리 목록 편집)**를 클릭합니다.

5단계 변경 사항을 제출합니다.

6단계 Anti-Malware Filtering(안티멀웨어 필터링) 열에서 정책 그룹에 대한 열을 클릭합니다.

7단계 Anti-Malware Settings(안티멀웨어 설정) 섹션에서 "Define Anti-Malware Custom Settings(안티멀웨어 맞춤형 설정 정의)"를 선택합니다.

8단계 Cisco IronPort DVS Anti-Malware Settings(Cisco IronPort DVS 안티멀웨어 설정) 섹션에서 이 정책 그룹에 대해 사용하도록 설정할 안티멀웨어 스캐닝 엔진을 선택합니다.

9단계 Malware Categories(악성코드 카테고리) 섹션에서 다양한 악성코드 카테고리를 모니터링하거나 차단할지를 선택합니다.

이 섹션에 나열되는 카테고리는 사용하도록 설정하는 스캐닝 엔진에 따라 다릅니다.

참고 구성된 최대 시간 설정에 도달하거나 시스템에서 임시 오류 조건이 발생하는 경우 URL 트랜잭션이 스캐닝 불가능으로 분류됩니다. 예를 들어, 스캐닝 엔진 업데이트 또는 AsyncOS 업그레이드 중에 트랜잭션이 스캐닝 불가능으로 분류될 수 있습니다. 악성코드 스캐닝 판정 SV_TIMEOUT 및 SV_ERROR는 스캐닝 불가능 트랜잭션으로 간주됩니다.

10단계 **변경 사항을 제출** 및 **커밋합니다**.

DVS 스캐닝 기록

액세스 로그에는 DVS 엔진이 업로드 요청에서 악성코드를 스캐닝했는지 여부가 표시됩니다. 각 액세스 로그 항목의 스캐닝 판정 정보 섹션에는 스캐닝된 업로드에 대한 DVS 엔진 활동의 값이 포함됩니다. 또한 다음 필드 중 하나를 W3C 또는 액세스 로그에 추가하여 더 쉽게 이 DVS 엔진 활동을 찾을 수도 있습니다.

표 12-1 W3C 로그의 로그 필드 및 액세스 로그의 형식 지정자

W3C 로그 필드	액세스 로그의 형식 지정자
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

DVS 엔진이 업로드 요청을 악성코드로 표시하고 악성코드 업로드를 차단하도록 구성된 경우 액세스 로그의 ACL 결정 태그는 BLOCK_AMW_REQ입니다.

그러나 DVS 엔진이 업로드 요청을 악성코드로 표시하고 악성코드 업로드를 *모니터링*하도록 구성된 경우 액세스 로그의 ACL 결정 태그는 실제로 트랜잭션에 적용된 액세스 정책에 따라 결정됩니다.

DVS 엔진이 업로드 요청에서 악성코드를 스캐닝했는지 여부를 확인하려면 각 액세스 로그 항목의 스캐닝 판정 정보 섹션에서 DVS 엔진 활동의 결과를 보십시오.

13장

보안 서비스 구성

- 보안 서비스 구성 개요, 13-1페이지
- 웹 평판 필터 개요, 13-2페이지
- 안티멀웨어 스캐닝 개요, 13-4페이지
- 적응형 스캐닝 이해, 13-7페이지
- 안티멀웨어 및 평판 필터 사용, 13-8페이지
- 정책에서 안티멀웨어 및 평판 구성, 13-9페이지
- 데이터베이스 테이블 유지 관리, 13-13페이지
- 웹 평판 필터링 활동 및 DVS 스캐닝 기록, 13-14페이지
- 캐싱, 13-14페이지
- 악성코드 카테고리 설명, 13-14페이지

보안 서비스 구성 개요

Web Security Appliance는 보안 구성 요소를 사용하여 다양한 멀웨어 위협으로부터 최종 사용자를 보호합니다. 각 정책 그룹에 대한 안티멀웨어 및 웹 평판 설정을 구성할 수 있습니다. 액세스 정책을 구성하는 경우 AsyncOS for Web이 차단할 콘텐츠를 결정할 때 사용할 안티멀웨어 스캐닝 및 웹 평판 점수의 조합을 선택하도록 할 수도 있습니다.

최종 사용자를 악성코드로부터 보호하기 위해 어플라이언스에서 이러한 기능을 사용하도록 설정한 후 정책별로 안티멀웨어 및 웹 평판 설정을 구성합니다.

옵션	설명	링크
안티멀웨어 스캐닝	멀웨어 위협을 차단하기 위해 어플라이언스에 통합된 여러 안티멀웨어 스캐닝 엔진에 대해 작업합니다.	안티멀웨어 스캐닝 개요, 13-4페이지
웹 신뢰도 필터	웹 서버 동작을 분석하고 URL에 URL 기반 악성코드가 포함되어 있는지 여부를 확인합니다.	웹 평판 필터 개요, 13-2페이지
AMP(Advanced Malware Protection)	파일 평판을 평가하고 파일 특성을 분석하여 다운로드 파일의 위협으로부터 보호합니다.	파일 평판 필터링 및 파일 분석의 개요, 14-1페이지

관련 주제

- 안티멀웨어 및 평판 필터 사용, 13-8페이지
- 적응형 스캐닝 이해, 13-7페이지

웹 평판 필터 개요

웹 평판 필터는 URL에 WBRS(Web-Based Reputation Score)를 할당하여 URL 기반 악성코드를 포함할 가능성을 확인합니다. Web Security Appliance는 웹 평판 점수를 사용하여 악성코드 공격이 발생하기 전에 식별하여 중지합니다. 웹 평판 필터는 액세스, 암호 해독 및 Cisco IronPort 데이터 보안 정책과 함께 사용할 수 있습니다.

웹 평판 점수

웹 평판 필터는 데이터를 사용하여 인터넷 도메인의 신뢰성을 평가하고 URL의 평판 점수를 지정합니다. 웹 평판 계산은 URL을 네트워크 매개변수와 연결하여 악성코드가 존재할 확률을 결정합니다. 그런 다음, 악성코드가 존재할 확률 합계가 -10에서 +10 사이의 웹 평판 점수에 매핑됩니다. +10이 악성코드를 포함할 가능성이 가장 낮은 경우입니다.

예를 들어, 매개변수는 다음과 같습니다.

- URL 분류 데이터
- 다운로드 가능한 코드의 존재 여부
- 길고 애매한 EULA(End-User License Agreements)의 존재 여부
- 전역 볼륨 및 볼륨 변경
- 네트워크 소유자 정보
- URL 기록
- URL 유효 기간
- 차단 목록에 있는지 여부
- 허용 목록에 있는지 여부
- 인기 있는 도메인의 URL 오자
- 도메인 등록자 정보
- IP 주소 정보

참고 Cisco에서는 사용자 이름, 암호 또는 클라이언트 IP 주소와 같은 식별 가능한 정보를 수집하지 않습니다.

웹 평판 필터링의 작동 방식 이해

웹 평판 점수는 URL 요청에 대해 수행할 조치와 연결됩니다. 조치가 특정 웹 평판 점수와 연관되도록 각 정책 그룹을 구성할 수 있습니다. 사용 가능한 조치는 URL 요청에 할당된 정책 그룹 유형에 따라 다릅니다.

정책 유형	작업
액세스 정책	차단, 스캐닝 또는 허용하도록 선택할 수 있습니다.
암호 해독 정책	삭제, 암호 해독 또는 통과하도록 선택할 수 있습니다.
Cisco IronPort 데이터 보안 정책	차단하거나 모니터링하도록 선택할 수 있습니다.

액세스 정책의 웹 평판

액세스 정책에서 웹 평판 설정을 구성할 경우 수동으로 설정을 구성하거나 AsyncOS for Web에서 적응형 스캐닝을 사용하여 최적의 옵션을 선택하도록 선택할 수 있습니다. 적응형 스캐닝이 사용하도록 설정된 경우 각 액세스 정책의 웹 평판 필터링을 사용하거나 사용하지 않도록 설정할 수 있지만 웹 평판 점수를 편집할 수는 없습니다.

점수	작업	설명	예
-10 ~ -6.0	Block	불량 사이트. 요청이 차단되고 추가적인 악성코드 스캐닝이 발생하지 않습니다.	• URL이 사용자 승인 없이 정보를 다운로드합니다. • URL 볼륨이 급증합니다. • URL이 인기 있는 도메인의 오자입니다.
-5.9 ~ 5.9	Scan	결정되지 않은 사이트. 추가적인 악성코드 스캐닝을 위해 요청이 DVS 엔진에 전달됩니다. DVS 엔진이 요청 및 서버 응답 콘텐츠를 스캐닝합니다.	• 동적 IP 주소가 있고 다운로드 가능한 콘텐츠가 포함된 최근 생성된 URL. • 웹 평판 점수가 양수인 네트워크 소유자 IP 주소.
6.0 ~ 10.0	허용	양호한 사이트. 요청이 허용됩니다. 악성코드 스캐닝이 필요하지 않습니다.	• URL에 다운로드 가능한 콘텐츠가 없음. • 평판이 좋고 기록이 많은 대용량 도메인. • 여러 허용 목록에 있는 도메인. • 평판이 나쁜 URL에 대한 링크가 없음.

기본적으로, HTTP 요청에서 웹 평판 점수 +7이 할당된 URL이 허용되고 추가적인 스캐닝이 필요하지 않습니다. 그러나 HTTP 요청에 대한 점수가 더 취약한 경우(예: +3)에는 악성코드를 스캐닝하는 Cisco IronPort DVS 엔진에 자동으로 전달됩니다. 평판이 불량한 HTTP 요청의 URL은 차단됩니다.

관련 주제

- 적응형 스캐닝 이해, 13-7페이지

암호 해독 정책의 웹 평판

점수	작업	설명
-10 ~ -9.0	삭제	불량 사이트. 최종 사용자에게 알리지 않고 요청이 삭제됩니다. 이 설정은 신중하게 사용하십시오.
-8.9 ~ 5.9	암호 해독	결정되지 않은 사이트. 요청이 허용되지만 연결이 암호 해독되고 액세스 정책이 암호 해독된 트래픽에 적용됩니다.
6.0 ~ 10.0	통과	양호한 사이트. 요청이 검사 또는 암호 해독 없이 통과됩니다.

Cisco IronPort 데이터 보안 정책의 웹 평판

점수	작업	설명
-10 ~ -6.0	차단	불량 사이트. 트랜잭션이 차단되고 추가적인 스캐닝이 발생하지 않습니다.
-5.9 ~ 0.0	모니터링	트랜잭션이 웹 평판에 따라 차단되지 않으며 콘텐츠 확인(파일 유형 및 크기)을 진행합니다. **참고** 점수가 없는 사이트는 모니터링됩니다.

안티멀웨어 스캐닝 개요

Web Security Appliance 안티멀웨어 기능은 안티멀웨어 스캐닝 엔진과 함께 Cisco IronPort DVS™ 엔진을 사용하여 웹 기반 멀웨어 위협을 중지합니다. DVS 엔진은 Webroot™, McAfee 및 Sophos 안티멀웨어 스캐닝 엔진과 함께 작동합니다.

스캐닝 엔진은 트랜잭션을 검사하여 DVS 엔진에 전달할 악성코드 스캐닝 판정을 결정합니다. DVS 엔진은 악성코드 스캐닝 판정을 기반으로 요청을 모니터링하거나 차단할지를 결정합니다. 어플라이언스의 안티멀웨어 구성 요소를 사용하려면 안티멀웨어 스캐닝을 사용하도록 설정하고 전역 설정을 구성한 후 여러 정책에 특정 설정을 적용해야 합니다.

관련 주제

- 안티멀웨어 및 평판 필터 사용, 13-8페이지
- 관련 주제, 13-9페이지

DVS 엔진 작동 방식 이해

DVS 엔진은 웹 평판 필터에서 전달된 URL 트랜잭션에 대해 안티멀웨어 스캐닝을 수행합니다. 웹 평판 필터가 특정 URL에 악성코드가 포함될 확률을 계산하고, 트랜잭션을 차단, 스캐닝 또는 허용하는 조치와 연결되는 URL 점수를 할당합니다.

할당된 웹 평판 점수가 트랜잭션을 스캐닝하도록 표시하는 경우 DVS 엔진에서는 URL 요청 및 서버 응답 콘텐츠를 수신합니다. DVS 엔진이 Webroot 및/또는 Sophos 또는 McAfee 스캐닝 엔진과 함께 악성코드 스캐닝 판정을 반환합니다. DVS 엔진이 악성코드 스캐닝 판정 및 액세스 정책 설정의 정보를 사용하여 콘텐츠를 차단하거나 클라이언트에 전달할지를 결정합니다.

다중 악성코드 판정에 대한 작업

DVS 엔진이 단일 URL에 대해 다중 악성코드 판정을 결정할 수도 있습니다. 하나 또는 두 가지 사용하도록 설정된 스캐닝 엔진에서 다중 판정이 발생할 수 있습니다.

- **다른 스캐닝 엔진의 다양한 판정.** Webroot와 Sophos 또는 McAfee를 모두 사용하도록 설정하는 경우 각 스캐닝 엔진이 동일한 개체에 대해 다른 악성코드 판정을 반환할 수 있습니다. 사용하도록 설정된 모든 스캐닝 엔진에서 URL에 대해 다중 판정이 발생하면 어플라이언스가 가장 제한적인 조치를 수행합니다. 예를 들어, 하나의 스캐닝 엔진이 차단 판정을 반환하고 다른 스캐닝 엔진이 모니터링 판정을 반환하는 경우 DVS 엔진에서는 항상 요청을 차단합니다.
- **동일한 스캐닝 엔진의 다양한 판정.** 개체에 다중 감염이 포함되어 있는 경우에는 스캐닝 엔진이 단일 개체에 대해 다중 판정을 반환할 수 있습니다. 동일한 스캐닝 엔진에서 URL에 대해 다중 판정이 발생하면 어플라이언스는 우선순위가 가장 높은 판정에 따라 조치를 수행합니다. 다음 텍스트에는 가능한 악성코드 스캐닝 판정이 우선순위가 가장 높은 것부터 가장 낮은 것까지 나열되어 있습니다.
  - 바이러스
  - 트로이 목마 다운로더
  - 트로이 목마
  - 트로이 피셔
  - 하이잭커
  - 시스템 모니터
  - 상업용 시스템 모니터
  - 다이얼러
  - 웜
  - 브라우저 헬퍼 개체
  - 피싱 URL
  - 애드웨어
  - 암호화된 파일
  - Unscannable(검색할 수 없음)
  - 기타 악성 코드

Webroot 스캐닝

Webroot 스캐닝 엔진은 개체를 검사하여 DVS 엔진에 전송할 악성코드 스캐닝 판정을 결정합니다. Webroot 스캐닝 엔진은 다음 개체를 검사합니다.

- **URL 요청.** Webroot가 URL 요청을 평가하여 URL이 악성코드 의심 대상인지 여부를 결정합니다. Webroot에서 이 URL의 응답에 악성코드가 포함되어 있다고 의심하는 경우 어플라이언스에서는 구성된 방식에 따라 요청을 모니터링하거나 차단합니다. Webroot 평가로 인해 요청이 지워지는 경우 어플라이언스에서는 URL을 검색하고 서버 응답을 검사합니다.
- **서버 응답.** 어플라이언스가 URL을 검색할 때 Webroot에서는 서버 응답 콘텐츠를 스캐닝하고 Webroot 시그니처 데이터베이스와 비교합니다.

McAfee 스캐닝

McAfee 스캐닝 엔진은 HTTP 응답에서 웹 서버로부터 다운로드된 개체를 검사합니다. 개체를 검사한 후 악성코드 스캐닝 판정을 DVS 엔진에 전달하여 DVS 엔진에서 요청을 모니터링하거나 차단할지를 결정할 수 있도록 합니다.

McAfee 스캐닝 엔진은 다음 방법을 사용하여 악성코드 스캐닝 판정을 결정합니다.

- 바이러스 시그니처 패턴 일치
- 휴리스틱 분석

바이러스 시그니처 패턴 일치

McAfee는 스캐닝 엔진과 함께 데이터베이스의 바이러스 정의를 사용하여 특정 바이러스, 바이러스 유형 또는 기타 사용자 동의 없이 설치된 소프트웨어를 탐지합니다. 파일에서 바이러스 시그니처를 검색합니다. McAfee를 사용하도록 설정하면 McAfee 스캐닝 엔진이 이 방법을 사용하여 서버 응답 콘텐츠를 스캐닝합니다.

휴리스틱 분석

휴리스틱 분석은 특정 규칙이 아니라 일반 규칙을 사용하여 새로운 바이러스 및 악성코드를 탐지하는 기술입니다. McAfee 스캐닝 엔진이 휴리스틱 분석을 사용하는 경우 개체의 코드를 확인하고 일반 규칙을 적용하며 개체에 바이러스가 발생할 가능성을 판별합니다.

휴리스틱 분석을 사용하면 오탐(바이러스로 지정된 클린 콘텐츠)을 보고할 가능성이 증가하며 어플라이언스 성능에 영향을 줄 수 있습니다. McAfee를 사용하도록 설정한 경우 개체를 스캐닝할 때 휴리스틱 분석도 사용하도록 설정할지 여부를 선택할 수 있습니다.

McAfee 카테고리

McAfee 판정	악성코드 스캐닝 판정 카테고리
알려진 바이러스	바이러스
트로이 목마	트로이 목마
조크 파일	애드웨어
테스트 파일	바이러스

(계속)

McAfee 판정	악성코드 스캐닝 판정 카테고리
워너비(Wannabe)	바이러스
강제 종료됨	바이러스
상업용 애플리케이션	상업용 시스템 모니터
사용자 동의 없이 설치된 개체	애드웨어
사용자 동의 없이 설치된 소프트웨어 패키지	애드웨어
암호화된 파일	암호화된 파일

Sophos 스캐닝

Sophos 스캐닝 엔진은 HTTP 응답에서 웹 서버로부터 다운로드된 개체를 검사합니다. 개체를 검사한 후 악성코드 스캐닝 판정을 DVS 엔진에 전달하여 DVS 엔진에서 요청을 모니터링하거나 차단할지를 결정할 수 있도록 합니다. McAfee 안티멀웨어 소프트웨어가 설치된 경우 McAfee 스캐닝 엔진 대신에 Sophos 스캐닝 엔진을 사용하도록 설정할 수 있습니다.

적응형 스캐닝 이해

적응형 스캐닝은 어떤 안티멀웨어 스캐닝 엔진(다운로드된 파일을 위한 Advanced Malware Protection 스캐닝 포함)이 웹 요청을 처리할지를 결정합니다. 적응형 스캐닝은 스캐닝 엔진을 실행하기 전에 악성코드로 식별되는 트랜잭션에 '발생 휴리스틱' 안티멀웨어 카테고리를 적용합니다. 어플라이언스에서 안티멀웨어 설정을 구성할 때 이러한 트랜잭션을 차단할지 여부를 선택할 수 있습니다.

적응형 스캐닝 및 액세스 정책

적응형 스캐닝이 사용하도록 설정된 경우 액세스 정책에서 구성할 수 있는 안티멀웨어 및 평판 설정은 약간 다릅니다.

- 각 액세스 정책에서 웹 평판 필터링을 사용하거나 사용하지 않도록 설정할 수 있지만 웹 평판 점수를 편집할 수는 없습니다.
- 각 액세스 정책에서 안티멀웨어 스캐닝을 사용하도록 설정할 수 있지만 사용하도록 설정할 안티멀웨어 스캐닝 엔진을 선택할 수는 없습니다. 적응형 스캐닝은 각 웹 요청에 가장 적합한 엔진을 선택합니다.

참고 적응형 스캐닝이 사용하도록 설정되지 않고 액세스 정책에 특정 웹 평판 및 안티멀웨어 설정이 구성되어 있는 경우 적응형 스캐닝이 사용하도록 설정되고 기존 웹 평판 및 안티멀웨어 설정이 재지정됩니다.

적응형 스캐닝이 사용하도록 설정되었는지 여부에 관계없이 정책별 Advanced Malware Protection 설정은 동일합니다.

안티멀웨어 및 평판 필터 사용

시작하기 전에

- 웹 평판 필터, DVS 엔진, Webroot, McAfee 및 Sophos 스캐닝 엔진이 사용하도록 설정되었는지 확인합니다. 기본적으로 시스템 설정 중에 사용하도록 설정되어야 합니다.

1단계 **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 필요에 따라 설정을 구성합니다.

설정	설명
웹 평판 필터링	웹 평판 필터링을 사용하도록 설정할지 여부를 선택합니다.
적응형 스캐닝	적응형 스캐닝을 사용하도록 설정할지 여부를 선택합니다. 웹 평판 필터링이 사용하도록 설정된 경우에만 적응형 스캐닝을 사용하도록 설정할 수 있습니다.
파일 평판 필터링 및 파일 분석	파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지를 참조하십시오.
DVS 엔진 개체 스캐닝 제한	최대 요청/응답 크기를 지정합니다. 사용자가 지정하는 최대 개체 크기 값은 모든 안티멀웨어 및 안티바이러스 스캐닝 엔진과 Advanced Malware Protection 기능을 통해 스캐닝할 수 있는 요청 및 응답의 전체 크기에 적용됩니다. 업로드 또는 다운로드 크기가 이 크기를 초과하면 보안 구성 요소가 진행 중인 스캐닝을 중단할 수 있으며 스캐닝 판정을 웹 프록시에 제공하지 않을 수 있습니다.
Sophos	Sophos 스캐닝 엔진을 사용하도록 설정할지 여부를 선택합니다.
McAfee	McAfee 스캐닝 엔진을 사용하도록 설정할지 여부를 선택합니다. McAfee 스캐닝 엔진을 사용하도록 설정하는 경우 휴리스틱 스캐닝을 사용하도록 설정할지 여부를 선택할 수 있습니다. **참고** 휴리스틱 분석으로 인해 보안 보호가 강화되지만 오탐과 성능 감소가 발생할 수 있습니다.
Webroot	Webroot 스캐닝 엔진을 사용하도록 설정할지 여부를 선택합니다. Webroot 스캐닝 엔진을 사용하도록 설정할 때 TRT(Threat Risk Threshold)를 구성할 수 있습니다. TRT는 악성코드가 존재할 확률에 숫자 값을 할당합니다. 전용 알고리즘이 URL 일치 시퀀스의 결과를 평가하고 TRR(Threat Risk Rating)을 할당합니다. 이 값은 TRT(Threat Risk Threshold) 설정과 연결됩니다. TRR 값이 TRT보다 크거나 같으면 URL이 악성코드로 간주되고 추가 처리를 위해 전달됩니다. **참고** TRT(Threat Risk Threshold)를 90보다 낮은 값으로 설정하면 URL 차단 비율이 크게 증가하고 정당한 요청이 거부됩니다. Cisco에서는 TRT를 기본값 90으로 유지하도록 적극 권장합니다. TRT 설정의 최소값은 51입니다.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 적응형 스캐닝 이해, 13-7페이지
- McAfee 스캐닝, 13-6페이지

정책에서 안티멀웨어 및 평판 구성

어플라이언스에서 안티멀웨어 및 평판 필터가 사용하도록 설정된 경우 정책 그룹에서 다양한 설정을 구성할 수 있습니다. 악성코드 스캐닝 판정에 따라 악성코드 카테고리에 대한 모니터링 또는 차단을 사용하도록 설정할 수 있습니다.

다음 정책 그룹에서 안티멀웨어 설정을 구성할 수 있습니다.

정책 유형	작업 링크
액세스 정책	액세스 정책에서 안티멀웨어 및 평판 설정, 13-9페이지
아웃바운드 악성코드 스캐닝 정책	아웃바운드 악성코드 스캐닝 정책을 사용하여 업로드 요청 제어

다음 정책 그룹에서 웹 평판 설정을 구성할 수 있습니다.

정책 유형	작업 링크
액세스 정책	액세스 정책에서 안티멀웨어 및 평판 설정, 13-9페이지
암호 해독 정책	암호 해독 정책 그룹에 대한 웹 평판 필터 설정 구성, 13-13페이지
Cisco 데이터 보안 정책	암호 해독 정책 그룹에 대한 웹 평판 필터 설정 구성, 13-13페이지

액세스 정책에서 Advanced Malware Protection 설정을 구성할 수 있습니다. 파일 평판 및 분석 기능 구성, 14-5페이지를 참조하십시오.

액세스 정책에서 안티멀웨어 및 평판 설정

적응형 스캐닝이 사용하도록 설정된 경우 액세스 정책에 대해 구성할 수 있는 웹 평판 및 안티멀웨어 설정은 적응형 스캐닝이 해제된 경우와 약간 다릅니다.

참고 구축에 보안 관리 어플라이언스가 포함되고 컨피그레이션 마스터에서 이 기능을 구성할 경우 이 페이지의 옵션은 관련 컨피그레이션 마스터에 대한 적응형 보안이 사용하도록 설정되었는지 여부에 따라 달라집니다. **Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)** 페이지에서 보안 관리 어플라이언스에 대한 설정을 확인합니다.

관련 주제

- 적응형 스캐닝 이해, 13-7페이지

적응형 스캐닝이 사용하도록 설정된 안티멀웨어 및 평판 설정 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 구성할 액세스 정책에 대한 **Anti-Malware and Reputation(안티멀웨어 및 평판)** 링크를 클릭합니다.

3단계 **Web Reputation and Anti-Malware Settings(웹 평판 및 안티멀웨어 설정)** 섹션 아래에서 **Define Web Reputation and Anti-Malware Custom Settings(웹 평판 및 안티멀웨어 맞춤형 설정 정의)**를 선택합니다.

이를 통해 전역 정책과 다른 이 액세스 정책에 대한 웹 평판 및 안티멀웨어 설정을 구성할 수 있습니다.

4단계 **Web Reputation Settings(웹 평판 설정)** 섹션에서 웹 평판 필터링을 사용하도록 설정할지 여부를 선택합니다. 적응형 스캐닝은 각 웹 요청에 가장 적합한 웹 평판 점수 임계값을 선택합니다.

5단계 **Advanced Malware Protection Settings(Advanced Malware Protection 설정)** 섹션에서 설정을 구성합니다.

6단계 Cisco DVS Anti-Malware Settings(Cisco DVS 안티멀웨어 설정) 섹션으로 스크롤합니다.

7단계 필요에 따라 정책에 대한 안티멀웨어 설정을 구성합니다.

설정	설명
의심되는 사용자 에이전트 검사 사용	HTTP 요청 헤더에 지정된 사용자 에이전트 필드에 따라 트래픽을 스캐닝할지 여부를 선택합니다. 이 확인란을 선택하는 경우 페이지의 하단에 있는 Additional Scanning(추가 스캐닝) 섹션에서 의심되는 사용자 에이전트를 모니터링하거나 차단할지를 선택할 수 있습니다. **참고** Chrome 브라우저에는 FTP-over-HTTP 요청의 사용자 에이전트 문자열이 포함되어 있지 않으므로 Chrome은 해당 요청에서 사용자 에이전트로 탐지될 수 없습니다.
안티멀웨어 스캐닝 사용	DVS 엔진을 사용하여 트래픽에서 악성코드를 스캐닝할지 여부를 선택합니다. 적응형 스캐닝은 각 웹 요청에 가장 적합한 엔진을 선택합니다.
악성프로그램 범주	악성코드 스캐닝 판정에 따라 다양한 악성코드 카테고리를 모니터링하거나 차단할지를 선택합니다.
기타 범주	이 섹션에 나열된 유형의 개체 및 응답을 모니터링하거나 차단할지를 선택합니다. **참고** 발생 휴리스틱 카테고리는 스캐닝 엔진을 실행하기 전에 적응형 스캐닝을 통해 악성코드로 식별된 트랜잭션에 적용됩니다. **참고** 구성된 최대 시간 설정에 도달하거나 시스템에서 임시 오류 조건이 발생하는 경우 URL 트랜잭션이 스캐닝 불가능으로 분류됩니다. 예를 들어, 스캐닝 엔진 업데이트 또는 AsyncOS 업그레이드 중에 트랜잭션이 스캐닝 불가능으로 분류될 수 있습니다. 악성코드 스캐닝 판정 SV_TIMEOUT 및 SV_ERROR는 스캐닝 불가능 트랜잭션으로 간주됩니다.

8단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 악성코드 카테고리 설명, 13-14페이지

적응형 스캐닝이 사용하지 않도록 설정된 안티멀웨어 및 평판 설정 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 구성할 액세스 정책에 대한 **Anti-Malware and Reputation(안티멀웨어 및 평판)** 링크를 클릭합니다.

3단계 **Web Reputation and Anti-Malware Settings(웹 평판 및 안티멀웨어 설정)** 섹션 아래에서 **Define Web Reputation and Anti-Malware Custom Settings(웹 평판 및 안티멀웨어 맞춤형 설정 정의)**를 선택합니다.

이를 통해 전역 정책과 다른 이 액세스 정책에 대한 웹 평판 및 안티멀웨어 설정을 구성할 수 있습니다.

4단계 Web Reputation Settings(웹 평판 설정) 섹션에서 설정을 구성합니다.

5단계 **Advanced Malware Protection Settings(Advanced Malware Protection 설정)** 섹션에서 설정을 구성합니다.

6단계 Cisco DVS Anti-Malware Settings(Cisco DVS 안티멀웨어 설정) 섹션으로 스크롤합니다.

7단계 필요에 따라 정책에 대한 안티멀웨어 설정을 구성합니다.

참고 Webroot, Sophos 또는 McAfee 스캐닝을 사용하도록 설정하는 경우 이 페이지에서 악성코드 카테고리의 일부 추가 카테고리를 모니터링하거나 차단하도록 선택할 수 있습니다.

설정	설명
의심되는 사용자 에이전트 검사 사용	HTTP 요청 헤더에 지정된 사용자 에이전트 필드에 따라 어플라이언스에서 트래픽을 스캐닝하도록 할지 여부를 선택합니다. 이 확인란을 선택하는 경우 페이지의 하단에 있는 Additional Scanning(추가 스캐닝) 섹션에서 의심되는 사용자 에이전트를 모니터링하거나 차단할지를 선택할 수 있습니다. **참고** Chrome 브라우저에는 FTP-over-HTTP 요청의 사용자 에이전트 문자열이 포함되어 있지 않으므로 Chrome은 해당 요청에서 사용자 에이전트로 탐지될 수 없습니다.
Webroot 사용함	트래픽을 스캐닝할 때 어플라이언스에서 Webroot 스캐닝 엔진을 사용하도록 할지 여부를 선택합니다.
Sophos 또는 McAfee 사용	트래픽을 스캐닝할 때 어플라이언스에서 Sophos 또는 McAfee 스캐닝 엔진을 사용하도록 설정할지 여부를 선택합니다.
악성프로그램 범주	악성코드 스캐닝 판정에 따라 다양한 악성코드 카테고리를 모니터링하거나 차단할지를 선택합니다. 이 섹션에 나열된 카테고리는 위에서 사용하도록 설정하는 스캐닝 엔진에 따라 다릅니다.

설정	설명
기타 범주	이 섹션에 나열된 유형의 개체 및 응답을 모니터링하거나 차단할지를 선택합니다. **참고** 구성된 최대 시간 설정에 도달하거나 시스템에서 임시 오류 조건이 발생하는 경우 URL 트랜잭션이 스캐닝 불가능으로 분류됩니다. 예를 들어, 스캐닝 엔진 업데이트 또는 AsyncOS 업그레이드 중에 트랜잭션이 스캐닝 불가능으로 분류될 수 있습니다. 악성코드 스캐닝 판정 SV_TIMEOUT 및 SV_ERROR는 스캐닝 불가능 트랜잭션으로 간주됩니다.

8단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 액세스 정책에 대한 웹 평판 점수 임계값 구성, 13-12페이지
- 악성코드 카테고리 설명, 13-14페이지

웹 평판 점수 구성

Web Security Appliance를 설치 및 설정하면 웹 평판 점수에 대한 기본 설정이 생성됩니다. 그러나 조직의 요구 사항에 맞게 웹 평판 점수의 임계값 설정을 수정할 수 있습니다. 각 정책 그룹에 대한 웹 평판 임계값 필터 설정을 구성합니다.

액세스 정책에 대한 웹 평판 점수 임계값 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 편집할 액세스 정책 그룹에 해당하는 Anti-Malware and Reputation(안티멀웨어 및 평판) 열 아래의 링크를 클릭합니다.

3단계 Web Reputation and Anti-Malware Settings(웹 평판 및 안티멀웨어 설정) 섹션 아래에서 **Define Web Reputation and Anti-Malware Custom Settings(웹 평판 및 안티멀웨어 맞춤형 설정 정의)**를 선택합니다.

이를 통해 전역 정책과 다른 이 액세스 정책에 대한 웹 평판 및 안티멀웨어 설정을 구성할 수 있습니다.

4단계 Enable Web Reputation Filtering(웹 평판 필터링 사용) 필드가 사용하도록 설정되었는지 확인합니다.

5단계 URL 차단, 스캐닝 및 허용 조치에 대한 범위를 변경하려면 마커를 이동합니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

참고 적응형 스캐닝이 사용하지 않도록 설정된 경우 액세스 정책의 웹 평판 점수 임계값을 편집할 수 있습니다.

암호 해독 정책 그룹에 대한 웹 평판 필터 설정 구성

1단계 **Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책)**를 선택합니다.

2단계 편집할 암호 해독 정책 그룹에 해당하는 Web Reputation(웹 평판) 열 아래의 링크를 클릭합니다.

3단계 Web Reputation Settings(웹 평판 설정) 섹션 아래에서 **Define Web Reputation Custom Settings(웹 평판 맞춤형 설정 정의)**를 선택합니다. 이를 통해 전역 정책 그룹의 웹 평판 설정을 재지정할 수 있습니다.

4단계 Enable Web Reputation Filtering(웹 평판 필터링 사용) 필드가 선택되었는지 확인합니다.

5단계 URL 삭제, 암호 해독 및 통과 조치에 대한 범위를 변경하려면 마커를 이동합니다.

6단계 **Sites with No Score(점수 없는 사이트)** 필드에서 웹 평판 점수가 할당되지 않은 사이트에 대한 요청에 수행할 조치를 선택합니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

데이터 보안 정책 그룹에 대한 웹 평판 필터 설정 구성

1단계 **Web Security Manager(웹 보안 관리자) > Cisco IronPort Data Security(Cisco IronPort 데이터 보안)**를 선택합니다.

2단계 편집할 데이터 보안 정책 그룹에 해당하는 Web Reputation(웹 평판) 열 아래의 링크를 클릭합니다.

3단계 Web Reputation Settings(웹 평판 설정) 섹션 아래에서 **Define Web Reputation Custom Settings(웹 평판 맞춤형 설정 정의)**를 선택합니다.

이를 통해 전역 정책 그룹의 웹 평판 설정을 재지정할 수 있습니다.

4단계 URL 차단 및 모니터링 조치에 대한 범위를 변경하려면 마커를 이동합니다.

5단계 **변경 사항을 제출** 및 **커밋합니다**.

참고 Cisco IronPort 데이터 보안 정책의 웹 평판 임계값 설정에는 음수 및 0 값만 구성할 수 있습니다. 즉, 모든 양수 점수는 모니터링됩니다.

데이터베이스 테이블 유지 관리

웹 평판, Webroot, Sophos 및 McAfee 데이터베이스는 Cisco IronPort 업데이트 서버에서 주기적으로 업데이트를 수신합니다. 서버 업데이트가 자동화되었으며 서버에서 업데이트 간격을 설정합니다.

웹 평판 데이터베이스

Web Security Appliance는 다양한 유형의 요청이 처리되는 방식에 대한 정보 및 통계를 포함하는 필터링 데이터베이스를 유지 관리합니다. Cisco SensorBase 네트워크 서버에 웹 평판 통계를 전송하도록 어플라이언스를 구성할 수도 있습니다. SensorBase 서버 정보는 SensorBase 네트워크의 데이터 피드와 함께 활용되고 이 정보는 웹 평판 점수를 생성하는 데 사용됩니다.

웹 평판 필터링 활동 및 DVS 스캐닝 기록

액세스 로그 파일은 각 트랜잭션의 DVS 엔진 및 웹 평판 필터에서 반환된 정보를 기록합니다. 액세스 로그의 스캐닝 판정 정보 섹션에는 트랜잭션에 적용된 조치의 원인을 이해하는 데 도움이 되는 여러 필드가 포함되어 있습니다. 예를 들어, 일부 필드에는 DVS 엔진에 전달되는 웹 평판 점수 또는 악성코드 스캐닝 판정 Sophos가 표시됩니다.

적응형 스캐닝 기록

액세스로그의 맞춤형 필드	W3C 로그의 맞춤형 필드	설명
%X6	x-as-malware-threat-name	적응형 스캐닝에서 반환된 안티멀웨어 이름. 트랜잭션이 차단되지 않은 경우 이 필드는 하이픈("-")을 반환합니다. 이 변수는 스캐닝 판정 정보에 포함됩니다(각 액세스 로그 항목의 끝에 꺾쇠괄호 안에 포함됨).

적응형 스캐닝 엔진에서 차단 및 모니터링되는 트랜잭션은 다음과 같은 ACL 결정 태그를 사용합니다.

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

캐싱

다음 지침은 악성코드를 스캐닝하는 동안 AsyncOS에서 캐시를 사용하는 방법에 대해 설명합니다.

- AsyncOS는 전체 개체가 다운로드되는 경우에만 개체를 캐시합니다. 스캐닝 중에 악성코드가 차단되면 전체 개체가 다운로드되지 않기 때문에 캐시되지 않습니다.
- AsyncOS는 콘텐츠가 서버에서 검색되었는지 또는 웹 캐시에서 검색되었는지에 따라 콘텐츠를 스캐닝합니다.
- 콘텐츠가 캐시되는 시간은 여러 요인에 따라 달라집니다. 기본값은 없습니다.
- 시그니처가 업데이트되면 AsyncOS에서 콘텐츠를 다시 스캐닝합니다.

악성코드 카테고리 설명

악성코드 유형	설명
애드웨어	애드웨어는 사용자를 판매할 상품으로 이동시키는 모든 소프트웨어 실행 파일 및 플러그인을 포함합니다. 이러한 프로그램은 사용자가 시스템 설정을 변경할 수 없도록 보안 설정을 변경할 수도 있습니다.
브라우저 헬퍼 개체	브라우저 헬퍼 개체는 광고 제공 또는 사용자 설정 하이재킹과 관련된 다양한 기능을 수행할 수 있는 브라우저 플러그인입니다.
상업용 시스템 모니터	상업용 시스템 모니터는 법적인 수단을 통해 적법한 라이센스로 확보할 수 있는 시스템 모니터 특성이 포함된 소프트웨어 부분입니다.

악성코드 유형	설명
다이얼러	다이얼러는 모뎀 또는 다른 유형의 인터넷 액세스를 활용하여 전화선 또는 사용자가 완전히 동의하지 않은 장거리 요금이 발생하는 사이트에 연결하는 프로그램입니다.
일반 스파이웨어	스파이웨어는 컴퓨터에 설치되는 일종의 악성코드이며, 사용자가 모르는 사이에 사용자에 대한 작은 정보 조각을 수집합니다.
하이잭커	하이잭커는 시스템 설정을 수정하거나 사용자의 시스템을 원치 않게 변경하여 사용자를 웹 사이트로 이동시키거나 사용자 동의 없이 프로그램을 실행할 수 있습니다.
알려진 악성 및 고위험 파일	Advanced Malware Protection 파일 평판 서비스에서 위협으로 식별한 파일입니다.
기타 악성 코드	이 카테고리는 정의된 다른 카테고리 중 하나에 정확하게 맞지 않는 기타 모든 악성코드와 의심스러운 동작을 포착하는 데 사용됩니다.
피싱 URL	피싱 URL은 브라우저 주소 표시줄에 표시됩니다. 일부 경우에 도메인 이름의 사용을 포함하며 올바른 도메인의 이름과 유사합니다.
PUA	사용자 동의 없이 설치된 애플리케이션. PUA는 악의적이지는 않지만 원치 않는 것으로 간주될 수 있는 애플리케이션입니다.
시스템 모니터	시스템 모니터는 다음 중 하나를 수행하는 소프트웨어를 포함합니다. • 명백하게 또는 은밀히 시스템 프로세스 및/또는 사용자 조치를 기록합니다. • 나중에 이러한 레코드를 검색 및 검토할 수 있도록 합니다.
트로이 목마 다운로더	트로이 다운로더는 설치 후에 원격 호스트/사이트에 연결하여 원격 호스트에서 패키지 또는 관련 소프트웨어를 설치하는 트로이 목마입니다.
트로이 목마	트로이 목마는 무해한 애플리케이션으로 위장한 파괴적인 프로그램입니다. 바이러스와 달리 트로이 목마는 자체적으로 복제하지 않습니다.
트로이 피셔	트로이 피셔는 감염된 컴퓨터에서 특정 웹 페이지에 방문할 때까지 대기하거나 감염된 머신을 스캐닝하여 사용자 이름 및 암호를 찾을 수 있습니다.
바이러스	바이러스는 사용자가 모르는 사이에 컴퓨터에 로드되는 프로그램 또는 코드 조각입니다.
웜	웜은 컴퓨터 네트워크를 통해 자체를 복제하고 악의적인 조치를 수행하는 프로그램 또는 알고리즘입니다.

파일 평판 필터링 및 파일 분석

- 파일 평판 필터링 및 파일 분석의 개요, 14-1페이지
- 파일 평판 및 분석 기능 구성, 14-5페이지
- 파일 평판 및 파일 분석 보고 및 추적, 14-11페이지
- 파일 위협 판정 변경 시 조치 수행, 14-14페이지
- 파일 평판 및 분석 트러블슈팅, 14-14페이지

파일 평판 필터링 및 파일 분석의 개요

Advanced Malware Protection은 다음을 통해 제로 데이 및 대상이 지정된 파일 기반 위협으로부터 보호합니다.

- 알려진 파일의 평판 가져오기
- 아직 평판 서비스에 알려지지 특정 파일의 동작 분석
- 새로운 정보가 사용 가능하게 될 때 새로 발생하는 위협을 지속적으로 평가하고 네트워크에 들어온 후 위협으로 확인된 파일에 대해 알림

이러한 기능은 파일 다운로드에만 사용할 수 있습니다. 업로드된 파일은 평가되지 않습니다.

평판 서비스는 클라우드에 있습니다. 파일 분석 서비스에는 퍼블릭 또는 프라이빗 클라우드(온프레미스)에 대한 옵션이 있습니다.

파일 위협 판정 업데이트

새 정보가 나타나면 위협 판정이 변경될 수 있습니다. 파일이 처음에 알 수 없음 또는 클린으로 평가될 수 있으므로 사용자가 파일에 액세스할 수 있습니다. 새 정보가 사용 가능하게 될 때 위협 판정이 변경되면 사용자에게 경고가 전달되고 파일과 파일의 새로운 판정이 AMP 판정 업데이트 보고서에 표시됩니다. 위협의 영향을 해결할 수 있는 시작점으로 진입점 트랜잭션을 조사할 수 있습니다.

판정이 악성에서 클린으로 변경될 수도 있습니다.

어플라이언스가 동일한 파일의 후속 인스턴스를 처리할 경우 업데이트된 판정이 즉시 적용됩니다.

판정 업데이트 타이밍에 대한 정보는 파일 평판 및 분석 서비스에 대해 지원되는 파일, 14-3페이지에서 참조되는 파일 기준 문서에 포함되어 있습니다.

관련 주제

- 파일 평판 및 파일 분석 보고 및 추적, 14-11페이지
- 파일 위협 판정 변경 시 조치 수행, 14-14페이지

파일 처리 개요

먼저, 파일을 다운로드한 웹사이트는 WBRS(Web Based Reputation Service)에 따라 평가됩니다.

이 사이트의 웹 평판 점수가 "스캐닝"으로 구성된 범위에 있는 경우 어플라이언스가 동시에 악성 코드에 대한 트랜잭션을 스캐닝하고 해당 파일의 평판에 대한 클라우드 기반 서비스를 쿼리합니다. (사이트의 평판 점수가 "차단" 범위에 있는 경우 그에 따라 트랜잭션이 처리되므로 필터를 추가로 처리할 필요가 없습니다.) 검사 도중 맬웨어가 발견되면 파일의 평판에 관계없이 트랜잭션이 차단됩니다.

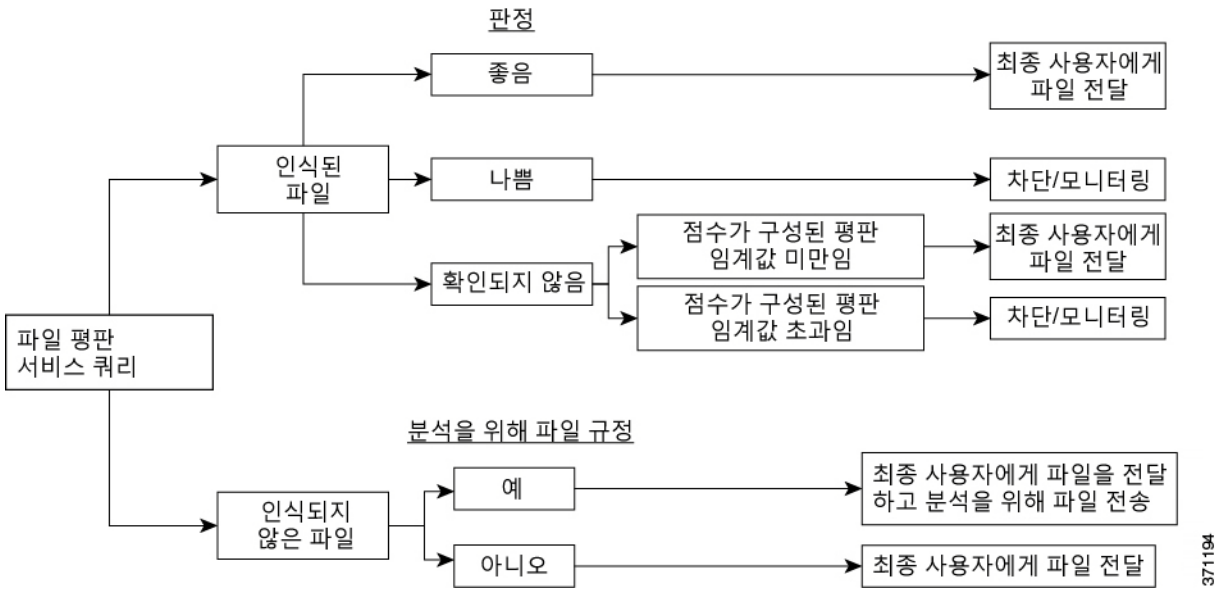
적응형 스캐닝도 사용하도록 설정된 경우 파일 평판 평가와 파일 분석이 적응형 스캐닝에 포함됩니다.

어플라이언스와 파일 평판 서비스 간의 통신은 암호화되어 변조로부터 보호됩니다.

파일의 평판이 평가된 후:

- 파일이 파일 평판 서비스에 알려지고 클린으로 확인되면 파일이 최종 사용자에게 릴리스됩니다.
- 파일 평판 서비스가 악성 판정을 반환하면 어플라이언스에서는 해당 파일에 대해 지정한 조치를 적용합니다.
- 파일이 평판 서비스에 알려졌지만 확정 판정을 위한 정보가 부족한 경우 평판 서비스에서 위협 핑거프린트 및 동작 분석과 같은 파일의 특성을 기반으로 위협 점수를 반환합니다. 이 점수가 구성된 평판 임계값을 충족하거나 초과할 경우 어플라이언스가 액세스 정책에서 악성 또는 고위험 파일에 대해 구성한 조치를 적용합니다.
- 평판 서비스에 파일에 대한 정보가 없고 파일이 분석 기준을 충족하지 않을 경우(파일 평판 및 분석 서비스에 대해 지원되는 파일, 14-3페이지 참조) 파일이 클린으로 간주되어 파일이 최종 사용자에게 릴리스됩니다.
- 클라우드 기반 파일 분석 서비스를 사용하도록 설정하고 평판 서비스에 파일에 대한 정보가 없으며 파일이 분석 가능한 파일에 대한 기준을 충족하면(파일 평판 및 분석 서비스에 대해 지원되는 파일, 14-3페이지 참조) 파일이 클린으로 간주되고 선택적으로 분석을 위해 전송됩니다.
- 온프레미스 파일 분석과 함께 구축할 경우 평판 평가와 파일 분석이 동시에 발생합니다. 평판 서비스에는 다양한 소스의 입력이 포함되므로 평판 서비스가 판정을 반환하면 해당 판정이 사용됩니다. 파일이 평판 서비스에 알려지지 않은 경우 파일이 사용자에게 릴리스되지만 파일 분석 결과가 로컬 캐시에서 업데이트되어 파일의 향후 인스턴스를 평가하는 데 사용됩니다.
- 서비스와의 연결 제한 시간이 초과되어 파일 평판 또는 파일 분석 판정 정보를 사용할 수 없는 경우 파일이 클린으로 간주되어 최종 사용자에게 릴리스됩니다.

그림 14-1 클라우드 파일 분석 구축을 위한 Advanced Malware Protection 워크플로우



파일이 분석을 위해 전송되는 경우:

- 파일이 분석을 위해 클라우드로 전송되는 경우: 파일이 HTTPS를 통해 전송됩니다.
- 분석은 일반적으로 몇 분이 소요되지만 더 오래 걸릴 수 있습니다.
- 파일 분석 후 악성으로 플래그가 지정된 파일이 평판 서비스에서 악성으로 식별되지 않을 수 있습니다. 파일 평판은 반드시 단일 파일 분석 판정만이 아니라 시간이 경과함에 따라 다양한 요인으로 결정됩니다.
- 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하여 분석된 파일에 대한 결과는 로컬로 캐시됩니다.

판정 업데이트에 대한 자세한 내용은 파일 위협 판정 업데이트, 14-1페이지를 참조하십시오.

파일 평판 및 분석 서비스에 대해 지원되는 파일

평판 서비스에서는 대부분의 파일 유형을 평가합니다. 파일 유형 ID는 파일 내용에 따라 결정되며 파일 이름 확장자에 종속되지 않습니다.

평판을 알 수 없는 일부 파일은 위협 특성을 분석할 수 있습니다. 파일 분석 기능을 구성할 때 분석할 파일 유형을 선택합니다. 새로운 유형이 동적으로 추가될 수 있으며 업로드 가능한 파일 유형의 목록이 변경되면 경고를 수신하게 되므로 업로드할 추가 파일 유형을 선택할 수 있습니다.

등록된 Cisco 고객만이 평판 및 분석 서비스에서 지원되는 파일에 대한 세부사항을 볼 수 있습니다. 평가 및 분석되는 파일에 대한 자세한 내용은 *Cisco 콘텐츠 보안 제품용 Advanced Malware Protection 서비스의 파일 기준* (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html)을 참조하십시오. 파일의 평판 평가 및 분석을 위한 파일 전송에 대한 기준은 언제든지 변경될 수 있습니다.

이 문서에 액세스하려면 지원 계약을 통해 제공된 Cisco 고객 어카운트가 있어야 합니다. 등록하려면 https://tools.cisco.com/RPF/register/register.do를 방문하십시오.

Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판) 페이지의 **DVS Engine Object Scanning Limits(DVS 엔진 개체 스캐닝 제한)**의 설정도 파일 평판 및 분석의 최대 파일 크기를 결정합니다.

Advanced Malware Protection에서 처리되지 않는 파일의 다운로드를 차단하도록 정책을 구성해야 합니다.

참고 분석을 위해 소스에서 이미 업로드된 파일은 다시 업로드되지 않습니다. 이러한 파일의 분석 결과를 보려면 File Analysis(파일 분석) 보고 페이지에서 SHA-256을 검색합니다.

관련 주제

- 파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지
- Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 14-10페이지
- 아카이브 또는 압축 파일 처리, 14-4페이지

아카이브 또는 압축 파일 처리

파일이 압축 또는 아카이브될 경우

- 압축 또는 아카이브 파일의 평판이 평가됩니다.
- 압축 또는 아카이브 파일의 압축이 해제되며 추출된 모든 파일의 평판이 평가됩니다.

파일 형식을 포함하여 검사되는 아카이브 및 압축 파일에 대한 내용은 파일 평판 및 분석 서비스에 대해 지원되는 파일, 14-3페이지에서 연결된 정보를 참조하십시오.

이 시나리오에서는

- 추출한 파일 중 하나가 악성인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환합니다.
- 압축 또는 아카이브 파일이 악성이고 추출된 모든 파일은 클린인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환합니다.
- 추출된 파일의 판정을 알 수 없는 경우 추출된 파일이 파일 분석을 위해 선택적으로 전송됩니다(구성되고 해당 파일 유형에 파일 분석이 지원되는 경우).
- 압축 또는 아카이브 파일의 압축을 푸는 동안 파일 추출에 실패할 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 스캐닝 불가능 판정을 반환합니다. 이 시나리오에서는 추출된 파일 중 하나가 악성인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환한다는 점에 유의하십시오(악성 판정이 스캐닝 불가능 판정보다 우선함).

참고 보안 MIME 유형(예: 텍스트/일반)으로 추출된 파일의 평판은 평가되지 않습니다.

클라우드에 전송된 정보의 개인 정보 보호

- 파일을 고유하게 식별하는 SHA만 클라우드의 평판 서비스에 전송됩니다. 파일 자체는 전송되지 않습니다.
- 클라우드에서 파일 분석 서비스를 사용 중이고 파일이 분석에 적합한 경우에는 파일 자체가 클라우드에 전송됩니다.
- 분석을 위해 클라우드로 전송되고 "악성" 판정을 받은 모든 파일에 대한 정보가 평판 데이터베이스에 추가됩니다. 이 정보를 다른 데이터와 함께 사용하여 평판 점수를 결정합니다.

온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하여 분석된 파일에 대한 정보는 평판 서비스와 공유되지 않습니다.

파일 평판 및 분석 기능 구성

- 파일 평판 및 분석 서비스와의 통신을 위한 요건, 14-5페이지
- 온프레미스 파일 분석 서버 구성, 14-6페이지
- 파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지
- (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성, 14-9페이지
- 액세스 정책에 따라 파일 평판 및 분석 서비스 조치 구성, 14-10페이지
- Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 14-10페이지
- Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성, 14-11페이지

파일 평판 및 분석 서비스와의 통신을 위한 요건

- 이러한 서비스를 사용하는 모든 Web Security appliance는 인터넷을 통해 직접 서비스에 연결할 수 있어야 합니다(온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하도록 구성된 파일 분석 서비스 제외).
- 기본적으로 파일 평판 및 분석 서비스 와의 통신은 어플라이언스의 관리 포트(M1)를 통해 라우팅됩니다. 어플라이언스가 관리 포트를 통해 데이터를 라우팅하지 않을 경우 데이터 인터페이스를 통해 파일 평판 및 파일 분석 서버에 트래픽 라우팅, 14-6페이지를 참조하십시오.
- 다음과 같은 방화벽 포트를 열어야 합니다.

방화벽 포트	설명	프로토콜	In/Out	호스트 이름	어플라이언스 인터페이스
32137 (기본) 또는 443	파일 평판을 얻기 위해 클라우드 서비스에 액세스합니다.	TCP	Out	Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판), Advanced(고급) 섹션: Advanced Settings for File Reputation(파일 평판 고급 설정)에 구성된 대로 클라우드 서버 풀 매개변수.	관리, 데이터 포트를 통해 이 트래픽을 라우팅하도록 구성되지 않은 경우.
443	파일 분석을 위해 클라우드 서비스에 액세스합니다.	TCP	Out	Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판), Advanced(고급) 섹션: Advanced Settings for File Analysis(파일 분석을 위한 고급 설정)에 구성된 대로.	

- 파일 평판 기능을 구성할 때 포트 443을 통해 SSL을 사용할지 여부를 선택합니다.

관련 주제

- 파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지

데이터 인터페이스를 통해 파일 평판 및 파일 분석 서버에 트래픽 라우팅

어플라이언스가 관리 포트를 어플라이언스 관리 서비스로만 제한하도록 구성된 경우(Network(네트워크) > Interfaces(인터페이스) 페이지에서) 그 대신 데이터 포트를 통해 파일 평판 및 분석 트래픽을 라우팅하도록 어플라이언스를 구성합니다.

Network(네트워크) > Routes(경로) 페이지에서 데이터 트래픽의 경로를 추가합니다. 일반 요건 및 지침은 TCP/IP 트래픽 경로 구성, 2-20페이지를 참조하십시오.

대상	대상 네트워크	게이트웨이
파일 평판 서비스	클라우드 서버 풀의 호스트 이름, Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판), Advanced(고급) 섹션: Advanced Settings for File Reputation(파일 평판 고급 설정)에 구성된 대로.	데이터 포트용 게이트웨이의 IP 주소
파일 분석 서비스	파일 분석 서버의 호스트 이름, Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판), Advanced(고급) 섹션: Advanced Settings for File Analysis(파일 분석을 위한 고급 설정)에 구성된 대로.	데이터 포트용 게이트웨이의 IP 주소

관련 주제

- TCP/IP 트래픽 경로 구성, 2-20페이지

온프레미스 파일 분석 서버 구성

Cisco AMP Threat Grid 어플라이언스를 프라이빗 클라우드 파일 분석 서버로 사용할 경우:

- Cisco AMP Threat Grid 어플라이언스 설정 및 환경 설정 가이드와 Cisco AMP Threat Grid 어플라이언스 관리 설명서를 얻습니다. Cisco AMP Threat Grid 어플라이언스 문서는 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html에서 사용할 수 있습니다.

  이 주제에 설명된 작업을 수행하려면 이 문서를 사용합니다.

  추가 설명서는 AMP Threat Grid 어플라이언스의 Help(도움말) 링크에서 사용할 수 있습니다.

  관리 설명서에서 다른 Cisco 어플라이언스, CSA, Cisco Sandbox API, WSA 및 Web Security Appliance와의 통합에 대한 모든 정보를 검색합니다.
- Cisco AMP Threat Grid 어플라이언스를 설정하고 구성합니다.
- 필요한 경우 Cisco AMP Threat Grid 어플라이언스 소프트웨어를 1.2.1 버전으로 업데이트하여 Cisco 웹 보안 어플라이언스와의 통합을 지원합니다.

  버전 번호를 확인하고 업데이트를 수행하는 방법에 대한 지침은 AMP Thread Grid 설명서를 참조하십시오.
- 어플라이언스가 네트워크를 통해 서로 통신할 수 있는지 확인합니다. Cisco 웹 보안 어플라이언스는 AMP Threat Grid 어플라이언스의 CLEAN 인터페이스에 연결할 수 있어야 합니다.

- 자체 서명 인증서를 배포할 경우: 웹 보안 어플라이언스에서 사용할 Cisco AMP Threat Grid 어플라이언스에서 자체 서명 SSL 인증서를 생성합니다. AMP Threat Grid 어플라이언스의 관리자 설명서에서 SSL 인증서 및 키 다운로드 지침을 참조하십시오. AMP Threat Grid 어플라이언스의 호스트 이름이 CN으로 지정된 인증서를 생성해야 합니다. AMP Threat Grid 어플라이언스의 기본 인증서는 작동하지 않습니다.
- 파일 분석 컨피그레이션을 제출하면 웹 보안 어플라이언스가 Threat Grid 어플라이언스에 자동으로 등록됩니다(파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지에 설명됨). 그러나 동일한 절차에 설명된 대로 등록을 활성화해야 합니다.

파일 평판 및 분석 서비스 사용 및 구성

시작하기 전에

- 파일 평판 서비스 및 파일 분석 서비스에 대한 기능 키를 얻습니다.
- 파일 평판 및 분석 서비스와의 통신을 위한 요건, 14-5페이지를 충족해야 합니다.
- 파일 평판 및 분석 서비스에 데이터 네트워크 인터페이스를 사용하려면 어플라이언스에서 데이터 네트워크 인터페이스를 사용하도록 설정해야 합니다. 네트워크 인터페이스 사용 또는 변경, 2-15페이지를 참조하십시오.
- 업그레이드 및 서비스 업데이트 설정 구성, 22-32페이지에서 구성된 업데이트 서버에 대한 연결을 확인하십시오.
- Cisco AMP Threat Grid 어플라이언스를 프라이빗 클라우드 파일 분석 서버로 사용할 경우 온프레미스 파일 분석 서버 구성, 14-6페이지를 참조하십시오.

1단계 **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)**을 선택합니다.

2단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 **Advanced Malware Protection Services(Advanced Malware Protection 서비스)** 섹션에서 **Enable File Reputation Filtering(파일 평판 필터링 사용)**을 선택합니다.

4단계 라이센스 계약이 표시되는 동의합니다.

5단계 **Advanced Malware Protection Services(Advanced Malware Protection 서비스)** 섹션에서 **Enable File Analysis(파일 분석 사용)**를 선택합니다.

6단계 **File Analysis(파일 분석)** 섹션에서 분석을 위해 클라우드에 전송할 파일 유형을 선택합니다.

7단계 필요에 따라 다음 **Advanced Settings for File Reputation(파일 평판 고급 설정)**을 조정합니다.

옵션	설명
라우팅 테이블	Advanced Malware Protection 서비스에 사용할 라우팅 테이블(어플라이언스 네트워크 인터페이스 유형인 관리 또는 데이터와 연결됨). 어플라이언스에서 관리 인터페이스와 하나 이상의 데이터 인터페이스가 활성화된 경우 관리 또는 데이터를 선택할 수 있습니다.

옵션	설명
파일 평판의 SSL 통신	기본 포트 32137이 아닌 포트 443에서 통신하려면 **Use SSL(Port 443)(SSL 사용(포트 443))**을 선택합니다. 이 옵션을 사용하여 파일 평판 서비스와의 통신에 사용할 업스트림 프록시를 구성할 수도 있습니다. **참고** 방화벽에서 포트를 열려면 포트 32137을 통한 SSL 통신이 필요할 수 있습니다.
평판 임계값 • 클라우드 서비스의 값 사용 • 사용자 지정 값 입력	허용되는 파일 평판 점수의 상한. 이 임계값 위의 점수는 해당 파일이 감염되었음을 나타냅니다.

참고 Cisco 지원의 지침 없이 이 섹션의 다른 설정을 변경하지 마십시오.

8단계 파일 분석을 위해 클라우드 서비스를 사용할 경우:

a. **Advanced Settings for File Analysis(파일 분석을 위한 고급 설정)**를 선택합니다.

b. 웹 보안 어플라이언스에 물리적으로 가장 가까운 클라우드 서버를 선택합니다.

새로 제공된 서버가 표준 업데이트 프로세스를 사용하여 이 목록에 주기적으로 추가됩니다.

9단계 파일 분석을 위해 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 경우:

Advanced Settings for File Analysis(파일 분석을 위한 고급 설정)를 구성합니다.

옵션	설명
파일 분석 서버 URL	**Private cloud(프라이빗 클라우드)**를 선택합니다.
서버	온프레미스 Cisco AMP Threat Grid 어플라이언스의 URL. 이 값과 인증서에 IP 주소가 아니라 호스트 이름을 사용합니다.
인증서	온프레미스 Cisco AMP Threat Grid 어플라이언스에서 생성한 자체 서명 인증서를 업로드합니다. 가장 최근에 업로드된 자체 서명 인증서가 사용됩니다. 가장 최근 인증서 이전에 업로드된 인증서에 액세스할 수 없습니다. 필요한 경우 원하는 인증서를 다시 업로드합니다.

10단계 변경 사항을 제출하고 커밋합니다.

11단계 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 경우 AMP Threat Grid 어플라이언스에서 이 어플라이언스에 대한 계정을 활성화합니다.

"사용자" 계정 활성화에 대한 자세한 지침은 AMP Threat Grid 문서에서 확인할 수 있습니다.

a. 섹션의 하단에 표시되는 파일 분석 클라이언트 ID를 메모합니다. 이를 통해 활성화할 "사용자" 식별합니다.

b. AMP Threat Grid 어플라이언스에 로그인합니다.

c. **Welcome...(시작...) > Manage Users(사용자 관리)**를 선택하고 User Details(사용자 세부사항)로 이동합니다.

d. 웹 보안 어플라이언스의 파일 분석 클라이언트 ID를 기준으로 "사용자" 계정을 찾습니다.

e. 어플라이언스의 이 "사용자" 계정을 활성화합니다.

(퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성

조직의 모든 콘텐츠 보안 어플라이언스가 조직의 어플라이언스에서 분석을 위해 전송한 파일에 대해 클라우드에서 파일 분석 결과 세부사항을 볼 수 있게 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹으로 묶어야 합니다.

1단계 **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)**을 선택합니다.

2단계 Appliance Grouping for File Analysis Cloud Reporting(파일 분석 클라우드 보고를 위한 어플라이언스 그룹화) 섹션에서 File Analysis Cloud Reporting Group ID(파일 분석 클라우드 보고 그룹 ID)를 입력합니다.

- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경 사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 이 값은 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다.
- 이 값에 CCOID를 사용하는 것이 좋습니다. 그러나 이 항목의 정확성은 검증되지 않습니다.
- 이 값은 대/소문자를 구분합니다.
- 그룹의 모든 어플라이언스가 클라우드에서 동일한 파일 분석 서버를 사용하도록 구성해야 합니다.
- 하나의 어플라이언스는 하나의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

3단계 **Add Appliance to Group(그룹에 어플라이언스 추가)**을 클릭합니다.

분석 그룹에 어떤 어플라이언스가 있습니까?

1단계 **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)**을 선택합니다.

2단계 Appliance Grouping for File Analysis Cloud Reporting(파일 분석 클라우드 보고를 위한 어플라이언스 그룹화) 섹션에서 **View Appliances in Group(그룹의 어플라이언스 보기)**을 클릭합니다.

3단계 특정 어플라이언스의 **파일 분석 클라이언트 ID**를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 ID의 위치
Email Security Appliance	**Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션.
웹 보안 어플라이언스	**Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션.
Security Management Appliance	**Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)** 페이지의 하단.

액세스 정책에 따라 파일 평판 및 분석 서비스 조치 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 표에서 정책에 대한 **Anti-Malware and Reputation(안티멀웨어 및 평판)** 열의 링크를 클릭합니다.

3단계 **Advanced Malware Protection Settings(Advanced Malware Protection 설정)** 섹션에서 **Enable File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석 사용)**를 선택합니다.

파일 분석이 전역적으로 활성화되지 않은 경우 파일 평판 필터링만 제공됩니다.

4단계 **Known Malicious and High-Risk Files(알려진 악성 및 고위험 파일)**에 대한 조치(**Monitor(모니터링)** 또는 **Block(차단)**)를 선택합니다.

기본값은 모니터링입니다.

5단계 변경 사항을 제출하고 커밋합니다.

Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인

Advanced Malware Protection과 관련된 경고를 보내도록 어플라이언스가 구성되었는지 확인합니다.

다음과 같은 경우에 경고를 수신하게 됩니다.

경고 설명	유형	심각도
기능 키 만료	(모든 기능에 기본으로 설정된 대로)	
파일 평판 또는 파일 분석 서비스에 연결할 수 없습니다.	안티맬웨어	경고
클라우드 서비스와의 통신이 구성되었습니다.	안티맬웨어	정보
파일 평판 판정이 변경됩니다.	안티맬웨어	정보
분석을 위해 전송할 수 있는 파일 유형이 변경되었습니다. 새 파일 유형의 업로드를 활성화할 수 있습니다.	안티맬웨어	정보

경고 설명	유형	심각도
일부 파일 유형에 대한 분석을 일시적으로 사용할 수 없습니다.	안티맬웨어	경고
지원되는 모든 파일 유형에 대한 분석이 일시적인 중단된 후 복원됩니다.	안티맬웨어	정보

관련 주제

- 파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고, 14-15페이지
- 파일 위협 판정 변경 시 조치 수행, 14-14페이지

Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성

Security Management Appliance에서 보고를 중앙 집중화할 경우 온라인 도움말의 웹 보고 장 또는 관리 어플라이언스의 사용 설명서에 있는 Advanced Malware Protection 섹션의 중요한 컨피그레이션 요건을 참조하십시오.

파일 평판 및 파일 분석 보고 및 추적

- SHA-256 해시로 파일 식별, 14-11페이지
- 파일 평판 및 파일 분석 보고서 페이지, 14-12페이지
- 다른 보고서의 파일 평판 필터링 데이터 보기, 14-13페이지
- 웹 추적 및 Advanced Malware Protection 기능 정보, 14-13페이지

SHA-256 해시로 파일 식별

파일 이름을 쉽게 변경할 수 있으므로 어플라이언스가 보안 해시 알고리즘(SHA-256)을 사용하여 각 파일에 대해 식별자를 생성합니다. 어플라이언스가 이름이 다른 동일한 파일을 처리할 경우 모든 인스턴스가 동일한 SHA-256으로 인식됩니다. 여러 어플라이언스가 동일한 파일을 처리하는 경우 해당 파일의 모든 인스턴스에 동일한 SHA-256 식별자가 있습니다.

대부분의 보고서에서는 파일이 SHA-256 값(단축 형식)으로 나열됩니다. 조직에서 악성코드 인스턴스와 관련된 파일 이름을 식별하려면 Reporting(보고) > Advanced Malware Protection을 선택하고 표에서 SHA-256 링크를 클릭합니다. 세부사항 페이지에 관련 파일 이름이 표시됩니다.

파일 평판 및 파일 분석 보고서 페이지

보고서	설명
AMP(Advanced Malware Protection)	파일 평판 서비스에서 식별된 파일 기반 위협을 표시합니다. 각 SHA에 액세스를 시도한 사용자와 해당 SHA-256과 관련된 파일 이름을 보려면 표에서 SHA-256을 클릭합니다. 맬웨어 위협 파일 세부사항 보고서 페이지의 하단에 있는 링크를 클릭하면 보고서에 대해 선택한 시간 범위와 관계없이 최대 가용 시간 범위 내에서 발생한 웹 추적의 파일의 모든 인스턴스가 표시됩니다. 판정이 변경된 파일은 AMP 판정 업데이트 보고서를 참조하십시오. 그러한 판정은 Advanced Malware Protection 보고서에 적용되지 않습니다. **참고** 압축 또는 아카이브 파일에서 추출된 파일 중 하나가 악성인 경우 압축 또는 아카이브 파일의 SHA 값만 Advanced Malware Protection 보고서에 포함됩니다.
파일 분석	분석을 위해 전송된 각 파일의 시간 및 판정(또는 임시 판정)을 표시합니다. Cisco AMP Threat Grid 어플라이언스의 허용 목록에 나열된 파일은 "클린"으로 표시됩니다. 허용 목록에 대한 내용은 AMP Threat Grid 온라인 도움말을 참조하십시오. 1,000개가 넘는 파일 분석 결과를 보려면 데이터를 .csv 파일로 내보냅니다. 각 파일의 위협 특성 및 점수 를 포함한 자세한 분석 결과를 보려면 드릴다운합니다. SHA를 검색하거나 파일 분석 세부사항 페이지의 하단에서 Cisco AMP Threat Grid 링크를 클릭하여 분석을 수행한 AMP Threat Grid 어플라이언스 또는 클라우드 서버에서 직접 SHA에 대한 추가 세부사항을 볼 수도 있습니다. **참고** 압축 또는 아카이브 파일에서 추출된 파일이 분석을 위해 전송된 경우 이러한 추출된 파일의 SHA 값만 파일 분석 보고서에 포함됩니다.
AMP 판정 업데이트	트랜잭션이 처리된 이후에 판정이 변경되어 이 어플라이언스에서 처리한 파일을 표시합니다. 이 상황에 대한 내용은 파일 위협 판정 업데이트, 14-1페이지를 참조하십시오. 1,000개가 넘는 판정 업데이트를 보려면 데이터를 .csv 파일로 내보냅니다. 단일 SHA-256에 대해 여러 판정이 변경된 경우 이 보고서에 판정 기록이 아닌 최신 판정만 표시됩니다. SHA-256 링크를 클릭하면 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 이 SHA-256이 포함된 모든 트랜잭션의 웹 추적 결과가 표시됩니다. 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 트랜잭션을 보려면 Malware Threat Files(멀웨어 위협 파일) 페이지의 하단에 있는 링크를 클릭합니다.

다른 보고서의 파일 평판 필터링 데이터 보기

파일 평판 및 분석 데이터는 관련이 있는 경우 다른 보고서에서도 볼 수 있습니다. "Blocked by Advanced Malware Protection(Advanced Malware Protection에 의해 차단됨)" 열은 해당 보고서에서 기본적으로 숨겨질 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

사용자 위치별 보고서에 Advanced Malware Protection 탭이 있습니다.

웹 추적 및 Advanced Malware Protection 기능 정보

웹 추적에서 파일 위협 정보를 검색할 경우 다음 사항에 유의하십시오.

- 파일 평판 서비스에서 발견된 악성 파일을 검색하려면 웹 추적의 Advanced(고급) 섹션에 있는 Malware Threat(멀웨어 위협) 영역에서 **Known Malicious and High-Risk Files(알려진 악성 및 고위험 파일)**를 **Filter by Malware Category(악성코드 카테고리별 필터링)** 옵션으로 선택합니다.
- 웹 추적에는 파일 평판 처리와 트랜잭션이 처리되었을 때 반환된 원래 파일 평판 판정에 대한 정보만 포함됩니다. 예를 들어, 파일이 처음에는 클린으로 확인되었으나 판정 업데이트에서는 파일이 악성으로 확인된 경우 클릭 판정만 추적 결과에 표시됩니다.

  검색 결과의 "차단 - AMP"는 파일의 평판 판정으로 인해 트랜잭션이 차단되었음을 의미합니다.

  추적 세부사항에서 "AMP 위협 점수"는 파일에 대한 클리어 판정을 결정할 수 없는 경우 클라우드 평판 서비스가 제공하는 최상의 점수입니다. 이 경우 점수는 1~100입니다. (AMP 판정이 반환되거나 점수가 0인 경우 AMP 위협 점수를 무시하십시오.) 어플라이언스가 이 점수를 임계값 점수(Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판) 페이지에서 구성됨)와 비교하여 수행할 조치를 결정합니다. 기본적으로 점수가 60~100인 파일은 악성으로 간주됩니다. Cisco에서는 기본 임계값 점수 변경을 권장하지 않습니다. WBRS 점수는 파일을 다운로드한 사이트의 평판이므로 이 점수는 파일 평판과 관련이 없습니다.
- 판정 업데이트는 AMP 판정 업데이트 보고서에서만 사용할 수 있습니다. 판정이 변경된 경우 웹 추적의 원래 트랜잭션 세부사항이 업데이트되지 않습니다. 특정 파일을 포함하는 트랜잭션을 보려면 판정 업데이트 보고서에서 SHA-256을 클릭합니다.
- 분석 결과 및 분석을 위해 파일이 전송되었는지 여부를 포함한 파일 분석에 대한 정보는 파일 분석 보고서에서만 사용할 수 있습니다.

  분석한 파일에 대한 추가 정보는 클라우드 또는 온프레미스 파일 분석 서버에서 사용할 수 있습니다. 파일에 대한 사용 가능한 파일 분석 정보를 보려면 **Reporting(보고) > File Analysis(파일 분석)**를 선택하고 SHA-256을 입력하여 파일을 검색하거나 웹 추적 세부사항에서 SHA-256 링크를 클릭합니다. 파일 분석 서비스가 임의의 소스에서 파일을 분석한 경우 세부사항을 볼 수 있습니다. 결과는 분석된 파일에 대해서만 표시됩니다.

  어플라이언스가 분석을 위해 전송된 파일의 후속 인스턴스를 처리한 경우 해당 인스턴스가 웹 추적 검색 결과에 표시됩니다.

파일 위협 판정 변경 시 조치 수행

1단계 AMP 판정 업데이트 보고서를 봅니다.

2단계 관련 SHA-256 링크를 클릭하여 최종 사용자가 액세스할 수 있었던 파일 관련 모든 트랜잭션에 대한 웹 추적 데이터를 확인합니다.

3단계 추적 데이터를 사용하여 위반에 포함된 파일 이름 및 파일을 다운로드한 웹 사이트와 같은 정보뿐 아니라 손상되었을 수 있는 사용자를 식별합니다.

4단계 파일 분석 보고서를 검토하여 이 SHA-256이 분석을 위해 전송되었는지 확인하고 파일의 위협 동작을 더 자세히 이해합니다.

관련 주제

- 파일 위협 판정 업데이트, 14-1페이지

파일 평판 및 분석 트러블슈팅

- 로그 파일, 14-14페이지
- 파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고, 14-15페이지
- API 키 오류(온프레미스 파일 분석), 14-15페이지
- 파일이 예상대로 업로드되지 않음, 14-15페이지
- 클라우드의 파일 분석 세부사항이 불완전함, 14-16페이지
- 분석을 위해 전송할 수 있는 파일 유형에 대한 경고, 14-16페이지

로그 파일

로그에서:

- `AMP` 및 `amp`는 파일 평판 서비스 또는 엔진을 나타냅니다.
- `Retrospective`는 판정 업데이트를 나타냅니다.
- `VRT` 및 `sandboxing`은 파일 분석 서비스를 나타냅니다.

파일 분석을 포함한 Advanced Malware Protection에 대한 정보가 액세스 로그 또는 AMP 엔진 로그에 기록됩니다. 자세한 내용은 로그를 통한 시스템 활동 모니터링에 대한 장을 참조하십시오.

로그 메시지 "Response received for file reputation query(파일 평판 쿼리에 대해 수신한 응답)"에서 "upload action(업로드 조치)"에 가능한 값은 다음과 같습니다.

- 0: 파일이 평판 서비스에 알려졌으므로 분석을 위해 전송하지 마십시오.
- 1: 전송
- 2: 파일이 평판 서비스에 알려졌으므로 분석을 위해 전송하지 마십시오.

파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고

문제 클라우드에서 파일 평판 또는 분석 서비스에 연결하지 못할 경우 이에 대한 여러 경고를 수신하게 됩니다. (단일 경고는 일시적인 문제만을 나타낼 수 있습니다.)

솔루션

- 파일 평판 및 분석 서비스와의 통신을 위한 요건, 14-5페이지에서 요건을 충족했는지 확인합니다.
- 어플라이언스가 클라우드 서비스와 통신하는 것을 차단할 수 있는 네트워크 문제를 확인합니다.
- 쿼리 시간 초과 값을 높입니다.

  Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)을 선택합니다. 쿼리 시간 초과 값은 **Advanced Malware Protection Services(Advanced Malware Protection 서비스)** 섹션의 Advanced(고급) 설정 영역에 있습니다.

API 키 오류(온프레미스 파일 분석)

문제 파일 분석 보고서 세부사항을 보려고 시도하거나 웹 보안 어플라이언스에서 AMP Threat Grid 서버에 연결하여 분석을 위해 파일을 업로드할 수 없는 경우 API 키 경고를 수신합니다.

솔루션 이 오류는 AMP Threat Grid 서버의 호스트 이름을 변경하고 AMP Threat Grid 서버에서 자체 서명 인증서를 사용할 경우에 발생할 수 있습니다(그 외의 상황에서도 발생할 수 있음). 문제를 해결하려면 다음을 수행합니다.

- 새로운 호스트 이름이 있는 AMP Threat Grid 어플라이언스에서 새 인증서를 생성합니다.
- 새 인증서를 웹 보안 어플라이언스에 업로드합니다.
- AMP Threat Grid 어플라이언스의 API 키를 재설정합니다. 지침은 AMP Threat Grid 어플라이언스에 대한 온라인 도움말을 참조하십시오.

관련 주제

- 파일 평판 및 분석 서비스 사용 및 구성, 14-7페이지

파일이 예상대로 업로드되지 않음

문제 파일이 예상대로 평가되거나 분석되지 않습니다. 경고나 명시적인 오류가 없습니다.

문제 다음과 같은 변화에 주목하십시오.

- 다른 어플라이언스에서 분석을 위해 파일을 전송하여 파일 분석 서버 또는 파일을 처리 중인 어플라이언스의 캐시에 파일이 이미 존재할 수 있습니다.
- **Security Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)** 페이지의 **DVS Engine Object Scanning Limits(DVS 엔진 개체 스캐닝 제한)**에 대해 구성된 최대 파일 크기 제한을 확인합니다. 이 제한은 Advanced Malware Protection 기능에 적용됩니다.

클라우드의 파일 분석 세부사항이 불완전함

문제 퍼블릭 클라우드의 완전한 파일 분석 결과는 조직의 다른 웹 보안 어플라이언스에서 업로드한 파일에 대해서는 사용할 수 없습니다.

솔루션 파일 분석 결과 데이터를 공유할 모든 어플라이언스를 그룹화해야 합니다. (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성, 14-9페이지를 참조하십시오. 그룹의 각 어플라이언스에서 이 컨피그레이션을 수행해야 합니다.

분석을 위해 전송할 수 있는 파일 유형에 대한 경고

문제 파일 분석을 위해 전송할 수 있는 파일 유형에 대한 심각도 정보 경고를 수신합니다.

솔루션 이 경고는 지원되는 파일 유형이 변경되거나 어플라이언스에서 지원되는 파일 유형을 알아보기 위해 확인할 때 전송됩니다. 이 문제는 다음과 같은 경우 발생할 수 있습니다.

- 사용자 또는 다른 관리자가 분석을 위해 선택한 파일 유형을 변경합니다.
- 지원되는 파일 유형은 클라우드 서비스의 사용 가능성에 따라 일시적으로 변경됩니다. 이 경우 어플라이언스에서 선택한 파일 유형에 대한 지원이 가능한 즉시 복원됩니다. 두 프로세스 모두 동적이며 사용자의 조치가 필요하지 않습니다.
- 예를 들어, AsyncOS 업그레이드의 일부로 어플라이언스가 재시작됩니다.

15장

웹 애플리케이션에 대한 액세스 관리

- 웹 애플리케이션에 대한 액세스 관리의 개요, 15-1페이지
- AVC 엔진 사용, 15-2페이지
- 정책 애플리케이션 제어 설정, 15-3페이지
- 대역폭 제어, 15-6페이지
- 인스턴트 메시징 트래픽 제어, 15-8페이지
- AVC 활동 보기, 15-9페이지

웹 애플리케이션에 대한 액세스 관리의 개요

AVC(Application Visibility and Control) 엔진을 사용하면 각 애플리케이션의 기반 기술을 완전히 이해할 필요 없이 네트워크의 애플리케이션 활동을 제어하기 위한 정책을 생성할 수 있습니다. 액세스 정책 그룹에서 애플리케이션 제어 설정을 구성할 수 있습니다. 개별적으로 또는 애플리케이션 유형에 따라 애플리케이션을 차단하거나 허용할 수 있습니다. 특정 애플리케이션 유형에 제어를 적용할 수도 있습니다.

액세스 정책을 사용하여 다음을 수행할 수 있습니다.

- 애플리케이션 동작 제어
- 특정 애플리케이션 유형에 사용되는 대역폭의 양 제어
- 최종 사용자가 차단된 경우 최종 사용자에게 알림
- 인스턴트 메시징, 블로그 및 소셜 미디어 애플리케이션에 제어 할당
- 범위 요청 설정 지정

AVC 엔진을 사용하여 애플리케이션을 제어하려면 다음 작업을 수행합니다.

작업	작업 링크
AVC 엔진 사용	AVC 엔진 사용, 15-2페이지
액세스 정책 그룹의 제어 설정	액세스 정책 그룹에서 애플리케이션 제어 설정 구성, 15-5페이지
혼잡을 제어하기 위해 일부 애플리케이션 유형에서 사용되는 대역폭 제한	대역폭 제어, 15-6페이지
인스턴트 메시징 트래픽을 허용하지만 인스턴트 메신저를 사용한 파일 공유는 허용하지 않음	인스턴트 메시징 트래픽 제어, 15-8페이지

AVC 엔진 사용

제한적 사용 제어를 사용하도록 설정한 경우 AVC 엔진을 사용하도록 설정합니다.

참고 **Reporting(보고) > Application Visibility(애플리케이션 가시성)** 페이지의 Application Visibility(애플리케이션 가시성) 보고서에서 AVC 엔진 스캐닝 활동을 볼 수 있습니다.

1단계 **Security Services(보안 서비스) > Acceptable Use Controls(제한적 사용 제어)**를 선택합니다.

2단계 현재 제한적 사용 제어 설정에 따라 **Enable(사용)** 또는 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 Enable Cisco Web Usage Controls(Cisco Web Usage Controls 사용)가 선택되어야 합니다.

4단계 Acceptable Use Controls Service(제한적 사용 제어 서비스) 패널에서 **Cisco Web Usage Controls**를 선택한 후 **Enable Application Visibility and Control(애플리케이션 가시성 및 제어 사용)**을 선택합니다.

5단계 **Default Action for Unreachable Service(연결할 수 없는 서비스에 대한 기본 조치)**: **Monitor(모니터링)** 또는 **Block(차단)**을 선택합니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- AVC 엔진 업데이트 및 기본 조치, 15-2페이지
- 요청이 AVC 엔진에서 차단된 경우 사용자 경험, 15-3페이지

AVC 엔진 업데이트 및 기본 조치

AsyncOS는 업데이트 서버에서 AVC 엔진을 포함하는 모든 보안 서비스 구성 요소에 대한 새로운 업데이트를 주기적으로 쿼리합니다. AVC 엔진 업데이트에는 새 애플리케이션 유형 및 애플리케이션에 대한 지원과 기존 애플리케이션에 대한 업데이트된 지원(애플리케이션 동작이 변경된 경우)이 포함될 수 있습니다. AsyncOS 버전 업데이트 간에 AVC 엔진을 업데이트하면 서버 업그레이드가 필요 없이 웹 보안 어플라이언스가 유연한 상태로 유지됩니다.

AsyncOS for Web은 전역 액세스 정책에 대해 다음과 같은 기본 조치를 할당합니다.

- 새 애플리케이션 유형의 기본값은 **Monitor(모니터링)**입니다.
- 새 애플리케이션 동작(예: 특정 애플리케이션 내에서 파일 전송 차단)의 기본값은 **Monitor(모니터링)**입니다.
- 기존 애플리케이션 유형에 대한 새 애플리케이션의 기본값은 애플리케이션 유형의 기본값입니다.

참고 전역 액세스 정책에서 각 애플리케이션 유형에 대한 기본 조치를 설정할 수 있으므로 AVC 엔진 업데이트에 도입된 새 애플리케이션이 자동으로 지정된 기본 조치를 상속합니다. 액세스 정책 그룹에서 애플리케이션 제어 설정 구성, 15-5페이지를 참조하십시오.

요청이 AVC 엔진에서 차단된 경우 사용자 경험

AVC 엔진이 트랜잭션을 차단하는 경우 웹 프록시가 최종 사용자에게 차단 페이지를 전송합니다. 그러나 모든 웹 사이트가 최종 사용자에게 차단 페이지를 표시하지는 않습니다. 많은 웹 사이트가 정적 웹 페이지 대신 JavaScript를 사용하여 동적 콘텐츠를 표시하며 차단 페이지를 표시하지 않을 수 있습니다. 계속해서 사용자가 악의적인 데이터를 다운로드하지 못하도록 적절히 차단되지만 웹 사이트에서 항상 사용자에게 이에 대해 알리지 않을 수 있습니다.

정책 애플리케이션 제어 설정

애플리케이션 제어에는 다음 요소의 구성이 포함됩니다.

옵션	설명
애플리케이션 유형	하나 이상의 애플리케이션을 포함하는 카테고리.
애플리케이션	애플리케이션 유형 내의 특정 애플리케이션.
애플리케이션 동작	관리자가 제어할 수 있는 애플리케이션 내에서 사용자가 수행할 수 있는 특정 조치 또는 동작. 모든 애플리케이션에 사용자가 구성할 수 있는 동작이 포함되어 있지는 않습니다.

액세스 정책 그룹에서 애플리케이션 제어 설정을 구성할 수 있습니다. Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책) 페이지에서 구성하려는 정책 그룹에 해당하는 Applications(애플리케이션) 링크를 클릭합니다. 애플리케이션을 구성할 때 다음 조치를 선택할 수 있습니다.

옵션	설명
차단	이 조치는 최종 조치입니다. 사용자가 웹 페이지를 볼 수 없으며 대신 최종 사용자 알림 페이지가 표시됩니다.
모니터링	이 조치는 중간 조치입니다. 웹 프록시가 계속해서 트랜잭션을 다른 제어 설정과 비교하여 적용할 최종 조치를 결정합니다.
제한	이 조치는 애플리케이션 동작이 차단되었음을 표시합니다. 예를 들어, 특정 인스턴트 메시징 애플리케이션에 대한 파일 전송을 차단하는 경우 해당 애플리케이션에 대한 조치는 제한입니다.
대역폭 제한	Media 및 Facebook과 같은 특정 애플리케이션의 경우 웹 트래픽에 사용 가능한 대역폭을 제한할 수 있습니다. 애플리케이션 자체와 해당 사용자에 대한 대역폭을 제한할 수 있습니다.

관련 주제

- 범위 요청 설정, 15-4페이지
- 애플리케이션 제어 구성에 대한 규칙 및 지침, 15-4페이지

범위 요청 설정

HTTP 범위 요청이 사용되지 않도록 설정되고 대용량 파일이 여러 스트림을 통해 다운로드되는 경우 통합된 패키지가 스캐닝됩니다. 이로 인해 대용량 개체를 다운로드하는 데 사용되는 다운로드 관리 유틸리티 및 애플리케이션의 성능 이점이 없어집니다.

또는 범위 요청 전달이 사용하도록 설정된 경우(웹 프록시 설정 구성, 4-3페이지 참조) 정책별로 수신 범위 요청이 처리되는 방법을 제어할 수 있습니다. 이 프로세스는 "바이트 제공"이라고도 하며 대용량 파일을 요청할 때 대역폭을 최적화하는 방법입니다.

그러나 범위 요청 전달을 사용하도록 설정하면 정책 기반의 AVC(Application Visibility and Control) 효율성에 방해가 되고 보안이 손상될 수 있습니다. 주의하여 사용하고 이점이 보안에 미치는 영향보다 더 큰 경우에만 HTTP 범위 요청 전달을 사용하도록 설정하십시오.

참고 범위 요청 전달이 사용하도록 설정되지 않은 경우와 사용하도록 설정되었지만 모든 애플리케이션이 Monitor(모니터링)로 설정된 경우에 범위 요청 설정은 읽기 전용입니다. 하나 이상의 애플리케이션이 Block(차단), Restrict(제한) 또는 Throttle(조절)로 설정된 경우 이 설정을 사용할 수 있습니다.

정책의 범위 요청 설정	
범위 요청 설정	• **Do not forward range requests(범위 요청을 전달하지 않음)** – 파일의 일부에 대한 요청이 전달되지 않으며 전체 파일이 반환됩니다. • **Forward range requests(범위 요청 전달)** – 요청된 범위가 유효한 경우에 전달되고 대상 서버에서 원하는 파일의 요청된 부분만 반환합니다.
예외 목록	현재 전달 선택 항목에서 제외되는 트래픽 대상을 지정할 수 있습니다. 즉, **Do not forward range requests(범위 요청을 전달하지 않음)**가 선택된 경우 요청이 전달되는 대상을 지정할 수 있습니다. 마찬가지로, **Forward range requests(범위 요청 전달)**가 선택된 경우 요청이 전달되지 않는 대상을 지정할 수 있습니다.

애플리케이션 제어 구성에 대한 규칙 및 지침

애플리케이션 제어 설정을 구성할 때 다음 규칙 및 지침을 고려합니다.

- 지원되는 애플리케이션 유형, 애플리케이션 및 애플리케이션 동작은 AsyncOS for Web 업그레이드 간이나 AVC 엔진 업데이트 후에 변경될 수 있습니다.
- Application Type(애플리케이션 유형) 목록에서 각 애플리케이션 유형에 대한 요약에 해당 애플리케이션의 최종 조치가 나열되지만 이러한 조치가 전역 정책에서 상속되었는지 또는 현재 액세스 정책에서 구성되었는지는 표시되지 않습니다. 특정 애플리케이션의 조치에 대해 자세히 알아보려면 애플리케이션 유형을 확장합니다.
- 전역 액세스 정책에서 각 애플리케이션 유형에 대한 기본 조치를 설정할 수 있으므로 AVC 엔진 업데이트에 도입된 새 애플리케이션이 자동으로 기본 조치를 상속합니다.
- 찾아보기 보기에서 애플리케이션 유형에 대한 "edit all(모두 편집)" 링크를 클릭하여 애플리케이션 유형의 모든 애플리케이션에 대해 동일한 조치를 빠르게 구성할 수 있습니다. 그러나 애플리케이션 동작 조치가 아니라 애플리케이션 조치만 구성할 수 있습니다. 애플리케이션 동작을 구성하려면 애플리케이션을 개별적으로 편집해야 합니다.

- Search(검색) 보기에서 조치 열을 기준으로 테이블을 정렬하면 최종 조치순으로 정렬됩니다. 예를 들어, "Use Global (Block)(전역 사용(차단))"은 정렬 순서에서 "Block(차단)" 다음에 나옵니다.
- 클라이언트에 서명을 위한 루트 인증서가 설치되어 있지 않으면 암호 해독 중에 일부 애플리케이션이 실패할 수 있습니다.

관련 주제

- 액세스 정책 그룹에서 애플리케이션 제어 설정 구성, 15-5페이지
- 전체 대역폭 제한 구성, 15-6페이지
- AVC 활동 보기, 15-9페이지

액세스 정책 그룹에서 애플리케이션 제어 설정 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 Policies(정책) 테이블에서 편집하려는 정책 그룹에 해당하는 Applications(애플리케이션) 열 아래의 링크를 클릭합니다.

3단계 전역 액세스 정책을 구성하는 경우:

a. **Default Actions for Application Types(애플리케이션 유형에 대한 기본 조치)** 섹션에서 각 애플리케이션 유형에 대한 기본 조치를 정의합니다.

b. 페이지의 Edit Applications Settings(애플리케이션 설정 편집) 섹션에서 그룹으로 또는 개별적으로 각 애플리케이션 유형의 개별 구성원에 대한 기본 조치를 편집할 수 있습니다. 개별 애플리케이션에 대한 기본 조치 편집은 다음 단계에 설명되어 있습니다.

4단계 사용자 정의 액세스 정책을 구성할 때 **Edit Applications Settings(애플리케이션 설정 편집)** 섹션에서 **Define Applications Custom Settings(애플리케이션 맞춤형 설정 정의)**를 선택합니다.

5단계 Application Settings(애플리케이션 설정) 영역의 드롭다운 메뉴에서 **Browse view(찾아보기 보기)** 또는 **Search view(검색 보기)**를 선택합니다.

- **Browse view(찾아보기 보기).** 애플리케이션 유형을 찾아볼 수 있습니다. Browse view(찾아보기 보기)를 사용하여 특정 유형의 모든 애플리케이션을 동시에 구성할 수 있습니다. Browse view(찾아보기 보기)에서 애플리케이션 유형이 축소되어 있는 경우, 애플리케이션 유형 요약에 해당 애플리케이션의 최종 조치가 나열되지만 조치가 전역 정책에서 상속되었는지 또는 현재 액세스 정책에서 구성되었는지는 표시되지 않습니다.
- **Search view(검색 보기).** 이름으로 애플리케이션을 검색할 수 있습니다. 전체 애플리케이션 목록이 길고 특정 애플리케이션을 빠르게 찾아서 구성해야 하는 경우에는 Search view(검색 보기)를 사용할 수 있습니다.

6단계 각 애플리케이션 및 애플리케이션 동작에 대한 조치를 구성합니다.

7단계 적용 가능한 각 애플리케이션에 대한 대역폭 제어를 구성합니다.

8단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 대역폭 제어, 15-6페이지

대역폭 제어

전체 제한 및 사용자 제한이 모두 트랜잭션에 적용되는 경우 가장 제한적인 옵션이 적용됩니다. URL 카테고리에 대한 ID 그룹을 정의하고 대역폭을 제한하는 액세스 정책에서 사용하여 특정 URL 카테고리에 대한 대역폭 제한을 정의할 수 있습니다.

다음과 같은 대역폭 제한을 정의할 수 있습니다.

대역폭 제한	설명	링크 작업
전체	지원되는 애플리케이션 유형에 대해 네트워크에 있는 모든 사용자의 전체 제한을 정의합니다. 전체 대역폭 제한은 웹 보안 어플라이언스와 웹 서버 간의 트래픽에 영향을 줍니다. 웹 캐시에서 제공되는 트래픽은 제한하지 않습니다.	전체 대역폭 제한 구성, 15-6페이지
사용자	애플리케이션 유형별로 네트워크에 있는 특정 사용자에 대한 제한을 정의합니다. 사용자 대역폭은 웹 서버로부터의 트래픽과 웹 캐시에서 제공되는 트래픽을 제한합니다.	사용자 대역폭 제한 구성, 15-6페이지

참고 대역폭 제한을 정의하면 사용자로 이동하는 데이터만 제한됩니다. 할당량에 도달하는 것에 따라 데이터를 차단하지는 않습니다. 웹 프록시가 각 애플리케이션 트랜잭션에 레이턴시를 도입하여 서버에 대한 링크의 속도가 더 느린 것처럼 보이게 합니다.

전체 대역폭 제한 구성

1단계 **Web Security Manager(웹 보안 관리자) > Overall Bandwidth Limits(전체 대역폭 제한)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Limit to(제한 범위)** 옵션을 선택합니다.

4단계 초당 메가비트(Mbps) 또는 초당 킬로비트(kbps) 단위로 제한할 트래픽의 양을 입력합니다.

5단계 **변경 사항을 제출** 및 **커밋합니다**.

사용자 대역폭 제한 구성

액세스 정책의 Applications Visibility and Control(애플리케이션 가시성 및 제어) 페이지에서 대역폭 제어 설정을 구성하여 사용자 대역폭 제한을 정의할 수 있습니다. 액세스 정책에서 사용자에 대해 다음 유형의 대역폭 제어를 정의할 수 있습니다.

옵션	설명	작업 링크
애플리케이션 유형에 대한 기본 대역폭 제한	전역 액세스 정책에서 애플리케이션 유형의 모든 애플리케이션에 대한 기본 대역폭 제한을 정의할 수 있습니다.	애플리케이션 유형에 대한 기본 대역폭 제한 구성, 15-7페이지

옵션	설명	작업 링크
애플리케이션 유형에 대한 대역폭 제한	사용자 정의 액세스 정책에서 전역 액세스 정책에 정의된 애플리케이션 유형에 대한 기본 대역폭 제한을 재지정할 수 있습니다.	애플리케이션 유형에 대한 기본 대역폭 제한 재지정, 15-7페이지
애플리케이션에 대한 대역폭 제한	사용자 정의 또는 전역 액세스 정책에서 애플리케이션 유형 대역폭 제한 또는 제한 없음(애플리케이션 유형 제한 제외)을 적용하도록 선택할 수 있습니다.	애플리케이션에 대한 대역폭 제어 구성, 15-8페이지

애플리케이션 유형에 대한 기본 대역폭 제한 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 전역 액세스 정책에 해당하는 Applications(애플리케이션) 열 아래의 링크를 클릭합니다.

3단계 **Default Actions for Application Types(애플리케이션 유형에 대한 기본 작업)** 섹션에서 편집할 애플리케이션 유형에 대한 "Bandwidth Limit(대역폭 제한)" 옆의 링크를 클릭합니다.

4단계 **Set Bandwidth Limit(대역폭 제한 설정)**를 선택하고 초당 메가비트(Mbps) 또는 초당 킬로비트(kbps) 단위로 제한할 트래픽의 양을 입력합니다.

5단계 **Apply(적용)**를 클릭합니다.

6단계 **변경 사항을 제출** 및 **커밋합니다**.

애플리케이션 유형에 대한 기본 대역폭 제한 재지정

전역 액세스 정책 그룹에서 정의된 기본 대역폭 제한을 사용자 정의 액세스 정책에서 재지정할 수 있습니다. Browse view(찾아보기 보기)에서만 이를 수행할 수 있습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 사용자 정의 정책 그룹에 해당하는 Applications(애플리케이션) 열 아래의 링크를 클릭합니다.

3단계 Edit Applications Settings(애플리케이션 설정 편집) 섹션에서 **Define Applications Custom Settings(애플리케이션 맞춤형 설정 정의)**를 선택합니다.

4단계 편집할 애플리케이션 유형에 대한 "Bandwidth Limit(대역폭 제한)" 옆의 링크를 클릭합니다.

5단계 다른 대역폭 제한 값을 선택하려면 **Set Bandwidth Limit(대역폭 제한 설정)**를 선택하고 초당 메가비트(Mbps) 또는 초당 킬로비트(kbps) 단위로 제한할 트래픽의 양을 입력합니다. 대역폭 제한이 없음을 지정하려면 **No Bandwidth Limit for Application Type(애플리케이션 유형에 대한 대역폭 제한 없음)**을 선택합니다.

6단계 **Apply(적용)**를 클릭합니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

애플리케이션에 대한 대역폭 제어 구성

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 Applications(애플리케이션) 열 아래의 링크를 클릭합니다.

3단계 정의하려는 애플리케이션이 포함된 애플리케이션 유형을 확장합니다.

4단계 구성할 애플리케이션에 대한 링크를 클릭합니다.

5단계 **Monitor(모니터링)**를 선택한 후 애플리케이션 유형에 대해 정의된 대역폭 제한 또는 제한 없음을 사용하도록 선택합니다.

참고 애플리케이션이 차단되었거나 애플리케이션 유형에 대한 대역폭 제한이 정의되지 않은 경우 대역폭 제한 설정을 적용할 수 없습니다.

6단계 **Done(완료)**을 클릭합니다.

7단계 **변경 사항을 제출** 및 **커밋합니다**.

인스턴트 메시징 트래픽 제어

IM 트래픽을 차단하거나 모니터링할 수 있으며 IM 서비스에 따라 IM 세션에서 특정 활동(애플리케이션 동작이라고도 함)을 차단할 수 있습니다.

1단계 **Web Security Manager(웹 보안 관리자) > Access Policies(액세스 정책)**를 선택합니다.

2단계 정책 테이블에서 편집하려는 정책 그룹에 해당하는 Applications(애플리케이션) 열 아래의 링크를 클릭합니다.

3단계 **Define Applications Custom Setting(애플리케이션 맞춤형 설정 정의)**을 클릭합니다.

4단계 인스턴트 메시징 애플리케이션 유형을 확장합니다.

5단계 구성하려는 IM 애플리케이션 옆에 있는 링크를 클릭합니다.

6단계 이 IM 애플리케이션에 대한 모든 트래픽을 차단하려면 **Block(차단)**을 선택합니다.

7단계 IM 애플리케이션을 모니터링하지만 애플리케이션 내의 특정 활동을 차단하려면 **Monitor(모니터링)**를 선택한 후 해당 애플리케이션 동작을 **Block(차단)**으로 선택합니다.

8단계 **Done(완료)**을 클릭합니다.

9단계 **변경 사항을 제출** 및 **커밋합니다**.

AVC 활동 보기

Reporting(보고) > Application Visibility(애플리케이션 가시성) 페이지에는 사용된 상위 애플리케이션 및 애플리케이션 유형에 대한 정보가 표시됩니다. 또한 차단된 상위 애플리케이션 및 애플리케이션 유형을 표시합니다.

액세스 로그 파일의 AVC 정보

액세스 로그 파일은 AVC(Application Visibility and Control) 엔진에서 각 트랜잭션에 대해 반환되는 정보를 기록합니다. 액세스 로그의 스캐닝 판정 정보 섹션에는 아래 나열된 필드가 포함됩니다.

설명	액세스 로그의 맞춤형 필드	W3C 로그의 맞춤형 필드
애플리케이션 이름	%XO	x-avc-app
애플리케이션 유형	%Xu	x-avc-type
애플리케이션 동작	%Xb	x-avc-behavior

16장

민감한 데이터의 유출 방지

- 데이터 보안 및 외부 DLP 정책 개요, 13-1페이지
- 업로드 요청 관리, 13-2페이지
- 외부 DLP 시스템에서 업로드 요청 관리, 16-3페이지
- 데이터 보안 및 외부 DLP 정책 그룹 구성원 자격 평가, 16-4페이지
- 데이터 보안 및 외부 DLP 정책 생성, 16-5페이지
- 업로드 요청에 대한 설정 관리, 16-7페이지
- 외부 DLP 시스템 정의, 16-9페이지
- 외부 DLP 정책을 사용하여 업로드 요청 제어, 16-11페이지
- 데이터 유출 방지 검사 기록, 16-12페이지

민감한 데이터의 유출 방지 개요

웹 보안 어플라이언스는 다음 기능을 제공하여 데이터를 보호합니다.

옵션	설명
Cisco IronPort 데이터 보안 필터	웹 보안 어플라이언스의 Cisco IronPort 데이터 보안 필터는 HTTP, HTTPS 및 FTP를 통해 네트워크에서 나가는 데이터를 평가합니다.
서드파티 DLP(Data Loss Prevention) 통합	웹 보안 어플라이언스는 민감한 데이터를 식별하고 보호하는 업계 선두의 서드파티 콘텐츠 인식 DLP 시스템과 통합됩니다. 웹 프록시에서는 ICAP(Internet Content Adaptation Protocol)를 사용하므로 콘텐츠 검사 작업을 프록시 서버에서 외부 시스템으로 이전할 수 있습니다.

웹 프록시가 업로드 요청을 수신하면 요청을 데이터 보안 및 외부 DLP 정책 그룹과 비교하여 적용할 정책 그룹을 결정합니다. 두 가지 유형의 정책이 모두 구성된 경우 외부 DLP 정책보다 먼저 Cisco IronPort 데이터 보안 정책과 요청을 비교합니다. 요청을 정책 그룹에 할당한 후 요청을 정책 그룹의 구성된 제어 설정과 비교하여 요청에 대해 수행할 작업을 결정합니다. 업로드 요청을 처리하도록 어플라이언스를 구성하는 방법은 정책 그룹 유형에 따라 다릅니다.

참고 크기가 영(0)바이트인 파일의 업로드 요청은 Cisco IronPort 데이터 보안 또는 외부 DLP 정책과 비교하여 평가되지 않습니다.

네트워크에서 나가는 데이터를 제한하고 제어하기 위해 다음 작업을 수행할 수 있습니다.

작업	작업 링크
Cisco IronPort 데이터 보안 정책 생성	업로드 요청 관리, 13-2페이지
외부 DLP 정책 생성	외부 DLP 시스템에서 업로드 요청 관리, 13-3페이지
데이터 보안 및 외부 DLP 정책 생성	데이터 보안 및 외부 DLP 정책 생성, 16-5페이지
Cisco IronPort 데이터 보안 정책을 사용하여 업로드 요청 제어	업로드 요청에 대한 설정 관리, 13-7페이지
외부 DLP 정책을 사용하여 업로드 요청 제어	외부 DLP 정책을 사용하여 업로드 요청 제어, 13-11페이지

최소 크기 미만의 업로드 요청 우회

로그 파일에 기록되는 업로드 요청 수를 줄이기 위해 최소 요청 본문 크기를 정의할 수 있습니다. 이보다 작은 업로드 요청은 Cisco IronPort 데이터 보안 필터 또는 외부 DLP 서버에서 검사하지 않습니다.

이를 위해 다음 CLI 명령을 사용합니다.

- **`datasecurityconfig`**. Cisco IronPort 데이터 보안 필터에 적용됩니다.
- **`externaldlpconfig`**. 구성된 외부 DLP 서버에 적용됩니다.

최소 요청 본문 크기의 기본값은 두 CLI 명령 모두 4KB(4096바이트)입니다. 유효한 값은 1~64KB입니다. 지정하는 크기는 업로드 요청 본문의 전체 크기에 적용됩니다.

참고 활성화된 경우 모든 대규모 인코딩 업로드 및 모든 네이티브 FTP 트랜잭션이 Cisco IronPort 데이터 보안 필터 또는 외부 DLP 서버의 검사를 받습니다. 그러나 맞춤형 URL 카테고리를 기반으로 우회할 수도 있습니다.

요청이 민감한 데이터로 차단된 경우 사용자 경험

Cisco IronPort 데이터 보안 필터 또는 외부 DLP 서버에서 업로드 요청을 차단하는 경우 웹 프록시가 최종 사용자에게 전송하는 차단 페이지를 제공합니다. 모든 웹 사이트에서 최종 사용자에게 차단 페이지를 표시하지는 않습니다. 예를 들어, 일부 Web 2.0 웹 사이트는 정적 웹 페이지 대신에 javascript를 사용하여 동적 콘텐츠를 표시하므로 차단 페이지를 표시할 가능성이 낮습니다. 사용자의 데이터 보안 위반 행위는 여전히 제대로 차단되지만, 웹 사이트에서 이런 상황을 사용자에게 알리지 않을 수도 있습니다.

업로드 요청 관리

시작하기 전에

- **Security Services(보안 서비스) > Data Security Filters(데이터 보안 필터)**로 이동하여 Cisco IronPort 데이터 보안 필터를 활성화합니다.

1단계 **데이터 보안 정책 그룹을 생성하고 구성합니다.** Cisco IronPort 데이터 보안 정책은 업로드 요청을 평가할 때 URL 필터링, 웹 평판 및 업로드 콘텐츠 정보를 사용합니다. 이러한 보안 구성 요소 각각을 구성하여 업로드 요청 차단 여부를 결정합니다.

웹 프록시에서 업로드 요청을 제어 설정과 비교할 경우 순서대로 설정을 평가합니다. 각 제어 설정을 구성하여 Cisco IronPort 데이터 보안 정책에 대한 다음 작업 중 하나를 수행할 수 있습니다.

작업	설명
차단	웹 프록시에서 연결을 허용하지 않으며, 대신 차단 이유를 설명하는 최종 사용자 알림 페이지를 표시합니다.
허용	웹 프록시에서 나머지 데이터 보안 정책 보안 서비스 검사를 우회한 후 액세스 정책과 비교하여 요청을 평가한 다음 최종 결정을 내립니다. Cisco IronPort 데이터 보안 정책의 경우 허용은 나머지 데이터 보안 검사를 우회하지만 외부 DLP 또는 액세스 정책 검사는 우회하지 않습니다. 웹 프록시가 요청에 대해 수행할 최종 조치는 적용 가능한 액세스 정책(또는 요청을 차단할 수 있는 적용 가능한 외부 DLP 정책)에 의해 결정됩니다.
모니터링	웹 프록시가 계속해서 트랜잭션을 다른 데이터 보안 정책 그룹 제어 설정과 비교하여 트랜잭션을 차단할지 또는 액세스 정책과 비교하여 평가할지 결정합니다.

Cisco IronPort 데이터 보안 정책의 경우, 웹 프록시에서 클라이언트 요청에 대해 수행하는 최종 조치는 차단 조치뿐입니다. 모니터링 및 허용 조치는 중간 조치입니다. 두 경우 모두 웹 프록시는 외부 DLP 정책(구성된 경우) 및 액세스 정책과 비교하여 트랜잭션을 평가합니다. 웹 프록시는 액세스 정책 그룹 제어 설정(또는 요청을 차단할 수 있는 적용 가능한 외부 DLP 정책)에 따라 적용할 최종 조치를 결정합니다.

관련 주제

- 외부 DLP 시스템에서 업로드 요청 관리, 13-3페이지
- 업로드 요청에 대한 설정 관리, 16-7페이지

외부 DLP 시스템에서 업로드 요청 관리

외부 DLP 시스템에서 업로드 요청을 처리하도록 웹 보안 어플라이언스를 구성하려면 다음 작업을 수행합니다.

1단계 **Network(네트워크) > External DLP Servers(외부 DLP 서버)**를 선택합니다. 외부 DLP 시스템을 정의합니다. 웹 보안 어플라이언스검사를 위해 업로드 요청을 외부 DLP 시스템에 전달하려면 에서 하나 이상의 ICAP 호환 DLP 시스템을 정의해야 합니다.

2단계 **외부 DLP 정책 그룹을 생성하고 구성합니다.** 외부 DLP 시스템이 정의되면 외부 DLP 정책 그룹을 생성하고 구성하여 검사를 위해 DLP 시스템에 보낼 업로드 요청을 결정합니다.

3단계 업로드 요청이 외부 DLP 정책과 매칭할 경우 웹 프록시는 검사를 위해 ICAP(Internet Content Adaptation Protocol)를 사용하여 DLP 시스템에 업로드 요청을 보냅니다. DLP 시스템은 요청 본문 콘텐츠를 검사하고 웹 프록시에 차단 또는 허용 판정을 반환합니다. 허용 판정은 업로드 요청을 액세스 정책과 비교한다는 점에서 Cisco IronPort 데이터 보안 정책에 대한 허용 조치와 유사합니다. 웹 프록시가 요청에 대해 수행할 최종 조치는 적용 가능한 액세스 정책에 의해 결정됩니다.

관련 주제

- 외부 DLP 정책을 사용하여 업로드 요청 제어, 16-11페이지
- 외부 DLP 시스템 정의, 16-9페이지

데이터 보안 및 외부 DLP 정책 그룹 구성원 자격 평가

각 클라이언트 요청이 ID에 할당된 후 다른 정책 유형에 대해 평가되어 각 유형마다 클라이언트 요청이 속해 있는 정책 그룹을 판별합니다. 웹 프록시는 *업로드 요청*을 데이터 보안 및 외부 DLP 정책과 비교하여 평가합니다. 웹 프록시가 클라이언트 요청의 정책 그룹 구성원 자격을 기반으로 구성된 정책 제어 설정을 클라이언트 요청에 적용합니다.

클라이언트 요청을 데이터 보안 및 외부 DLP 정책 그룹과 매칭

클라이언트 요청과 매칭하는 정책 그룹을 결정하기 위해 웹 프록시는 그룹 구성원 자격 기준과의 매칭에 특정 프로세스를 따릅니다. 그룹 구성원 자격에 대해 다음 요인을 고려합니다.

- **ID.** 각 클라이언트 요청은 ID와 매칭하고 인증에 실패하여 게스트 액세스 권한을 부여받거나 인증에 실패하여 종료됩니다.
- **인증된 사용자.** 할당된 ID에 인증이 필요한 경우 사용자가 데이터 보안 또는 외부 DLP 정책 그룹의 권한있는 사용자 목록에 포함되어야 정책 그룹과 매칭할 수 있습니다. 권한있는 사용자 목록은 임의의 지정된 그룹 또는 사용자이거나, ID가 게스트 액세스를 허용하는 경우에는 게스트 사용자일 수 있습니다.
- **고급 옵션.** 데이터 보안 및 외부 DLP 정책 그룹 구성원 자격에 대한 여러 고급 옵션을 구성할 수 있습니다. 일부 옵션(예: 프록시 포트 및 URL 카테고리)은 ID 내에서 정의될 수도 있습니다. ID에 고급 옵션이 구성된 경우 데이터 보안 또는 외부 DLP 정책 그룹 레벨에서는 구성할 수 없습니다.

이 섹션에서는 웹 프록시가 데이터 보안 및 외부 DLP 정책 그룹에 업로드 요청을 매칭하는 방식을 개괄적으로 소개합니다.

웹 프록시가 정책 테이블에 있는 각 정책 그룹을 순차적으로 읽습니다. 웹 프록시가 업로드 요청 상태를 첫 번째 정책 그룹의 구성원 자격 기준과 비교합니다. 매칭할 경우 웹 프록시는 해당 정책 그룹의 정책 설정을 적용합니다.

매칭하지 않는 경우 웹 프록시는 업로드 요청을 다음 정책 그룹과 비교합니다. 업로드 요청이 사용자 정의 정책 그룹과 매칭할 때까지 이 프로세스를 계속 진행합니다. 사용자 정의 정책 그룹과 매칭하지 않을 경우 전역 정책 그룹과 매칭합니다. 웹 프록시가 업로드 요청을 정책 그룹 또는 전역 정책 그룹과 매칭할 경우 해당 정책 그룹의 정책 설정을 적용합니다.

데이터 보안 및 외부 DLP 정책 생성

하나 이상의 ID 또는 대상 사이트의 URL 카테고리와 같은 여러 기준의 조합을 기반으로 데이터 보안 및 외부 DLP 정책 그룹을 생성할 수 있습니다. 정책 그룹 구성원 자격에 대한 하나 이상의 기준을 정의해야 합니다. 여러 기준을 정의할 경우 업로드 요청이 모든 기준에 부합해야 정책 그룹과 매칭합니다. 그러나 업로드 요청은 구성된 ID 중 단 하나와 매칭해야 합니다.

1단계 **Web Security Manager(웹 보안 관리자) > Cisco IronPort Data Security(Cisco IronPort 데이터 보안)**(데이터 보안 정책 그룹 구성원 자격을 정의하는 경우) 또는 **Web Security Manager(웹 보안 관리자) > External Data Loss Prevention(외부 데이터 유출 방지)**(외부 DLP 정책 그룹 구성원 자격을 정의하는 경우)을 선택합니다.

2단계 **Add Policy(정책 추가)**를 클릭합니다.

3단계 Policy Name(정책 이름) 필드에 정책 그룹의 이름을 입력하고 Description(설명) 필드(선택 사항)에 설명을 추가합니다.

참고 각 정책 그룹 이름은 고유해야 하며 영숫자 또는 공백 문자만 포함해야 합니다.

4단계 Insert Above Policy(정책 위에 삽입) 필드에서 정책 테이블의 어디에 정책 그룹을 배치할지 그 위치를 선택합니다.

여러 정책 그룹을 구성하는 경우 각 그룹에 대해 논리적 순서를 지정해야 합니다. 정확한 매칭이 이루어지도록 정책 그룹의 순서를 지정합니다.

5단계 Identities and Users(ID 및 사용자) 섹션에서 이 정책 그룹에 적용할 하나 이상의 ID 그룹을 선택합니다.

6단계 (선택 사항) 추가 구성원 자격 요건을 정의하려면 Advanced(고급) 섹션을 확장합니다.

7단계 고급 옵션 중 무엇이든 사용하여 정책 그룹 구성원 자격을 정의하려면 고급 옵션의 링크를 클릭하고 표시되는 페이지에서 옵션을 구성합니다.

고급 옵션	설명
프로토콜	클라이언트 요청에 사용된 프로토콜로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 포함할 프로토콜을 선택합니다. "All others(기타)"는 이 옵션 위에 나열되지 않은 임의의 프로토콜을 의미합니다. **참고** HTTPS 프록시가 활성화된 경우 암호 해독 정책만 HTTPS 트랜잭션에 적용됩니다. 액세스, 라우팅, 아웃바운드 악성프로그램 검색, 데이터 보안 또는 외부 DLP 정책에 대한 정책 구성원 자격은 HTTPS 프로토콜로 정의할 수 없습니다.

고급 옵션	설명
프록시 포트	웹 프록시 액세스에 사용된 프록시 포트로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. Proxy Ports(프록시 포트) 필드에 하나 이상의 포트 번호를 입력합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오. 명시적 전달 연결의 경우, 이는 브라우저에 구성된 포트입니다. 투명한 연결의 경우, 이는 대상 포트와 동일합니다. 한 포트에 명시적으로 요청을 전달하도록 구성된 클라이언트 세트가 있고 다른 포트에 명시적으로 요청을 전달하도록 구성된 또 다른 클라이언트 세트가 있을 경우 프록시 포트에서 정책 그룹 구성원 자격을 정의할 수 있습니다. Cisco는 어플라이언스가 명시적 전달 모드로 구축되거나 클라이언트가 어플라이언스에 명시적으로 요청을 전달하는 경우에만 프록시 포트로 정책 그룹 구성원 자격을 정의하도록 권장합니다. 클라이언트 요청이 투명하게 어플라이언스에 리디렉션될 경우 프록시 포트로 정책 그룹 구성원 자격을 정의한다면 일부 요청이 거부될 수도 있습니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정으로 ID 구성원 자격을 정의할 경우 이 설정은 비 ID 정책 그룹 레벨에서는 구성 불가합니다.
서브넷	서브넷 또는 기타 주소로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 연결된 ID로 정의될 수 있는 주소를 사용하도록 선택하거나 여기에 특정 주소를 입력할 수 있습니다. **참고** 이 정책 그룹과 연결된 ID가 주소로 ID 멤버십을 정의할 경우 ID에 정의된 주소의 일부인 주소를 이 정책 그룹에 입력해야 합니다. 정책 그룹에 주소를 추가하면 이 정책 그룹과 매칭하는 트랜잭션 목록이 더욱 좁혀집니다.
URL 카테고리	URL 카테고리로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 사용자 정의 또는 사전 정의 URL 카테고리를 선택합니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정으로 ID 구성원 자격을 정의할 경우 이 설정은 비 ID 정책 그룹 레벨에서는 구성 불가합니다.
사용자 에이전트	클라이언트 요청에서 사용된 사용자 에이전트로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 일반적으로 정의되는 일부 브라우저를 선택하거나 정규식을 사용하여 직접 정의할 수도 있습니다. 이 정책 그룹이 선택한 사용자 에이전트에 적용되어야 하는지 또는 선택한 사용자 에이전트 목록에 없는 모든 사용자 에이전트에 적용되어야 하는지를 선택합니다. **참고** 이 정책 그룹과 연결된 ID가 이 고급 설정으로 ID 구성원 자격을 정의할 경우 이 설정은 비 ID 정책 그룹 레벨에서는 구성 불가합니다.
사용자 위치	사용자 위치(원격 또는 로컬)로 정책 그룹 구성원 자격을 정의할지 여부를 선택합니다. 이 옵션은 모빌리티 보안가 활성화된 경우에만 표시됩니다.

8단계 변경 사항을 제출합니다.

9단계 데이터 보안 정책 그룹을 생성하는 경우 그 제어 설정을 구성하여 웹 프록시에서 업로드 요청을 처리하는 방법을 정의합니다.

새로운 데이터 보안 정책 그룹은 제어 설정별 옵션을 구성할 때까지 전역 정책 그룹 설정을 자동으로 상속합니다.

외부 DLP 정책 그룹을 생성하는 경우 그 제어 설정을 구성하여 웹 프록시에서 업로드 요청을 처리하는 방법을 정의합니다.

새 외부 DLP 정책 그룹은 맞춤형 설정을 구성할 때까지 자동으로 전역 정책 그룹 설정을 상속합니다.

10단계 변경 사항을 **Submit(제출)** 및 **Commit(커밋)**합니다.

관련 주제

- 데이터 보안 및 외부 DLP 정책 그룹 구성원 자격 평가, 16-4페이지
- 클라이언트 요청을 데이터 보안 및 외부 DLP 정책 그룹과 매칭, 16-4페이지
- 업로드 요청에 대한 설정 관리, 16-7페이지
- 외부 DLP 정책을 사용하여 업로드 요청 제어, 16-11페이지

업로드 요청에 대한 설정 관리

각 업로드 요청이 데이터 보안 정책 그룹에 할당되고 해당 정책 그룹의 제어 설정을 상속합니다. 데이터 보안 정책 그룹의 제어 설정에 따라 어플라이언스가 연결을 차단할지 아니면 액세스 정책과 비교하여 평가할지 결정됩니다.

Web Security Manager(웹 보안 관리자) > Cisco IronPort Data Security(Cisco IronPort 데이터 보안) 페이지에서 데이터 보안 정책 그룹에 대한 제어 설정을 구성합니다.

다음 설정을 구성하여 업로드 요청에 대해 수행할 조치를 결정할 수 있습니다.

옵션	링크
URL 카테고리	URL 카테고리, 13-8페이지
웹 평판	웹 평판, 13-8페이지
콘텐츠	콘텐츠 차단, 13-8페이지

데이터 보안 정책 그룹이 업로드 요청에 할당된 후 정책 그룹에 대한 제어 설정을 평가하여 요청을 차단할지 아니면 액세스 정책과 비교하여 평가할지 결정합니다.

URL 카테고리

AsyncOS for Web을 사용하면 특정 요청의 URL 카테고리를 기반으로 어플라이언스의 트랜잭션 처리 방법을 구성할 수 있습니다. 사전 정의 카테고리 목록을 사용하여 카테고리별로 콘텐츠를 모니터링할지 아니면 차단할지 선택할 수 있습니다. 또한 맞춤형 URL 카테고리를 생성하고 맞춤형 카테고리의 웹 사이트에 대한 트래픽을 허용, 모니터링 또는 차단할지 선택할 수 있습니다.

웹 평판

웹 평판 설정은 전역 설정을 상속합니다. 특정 정책 그룹에 대한 웹 평판 필터링을 맞춤화하기 위해 Web Reputation Settings(웹 평판 설정) 풀다운 메뉴를 사용하여 웹 평판 점수 임계값을 맞춤화할 수 있습니다.

Cisco IronPort 데이터 보안 정책에 대한 웹 평판 임계값 설정에는 음수 및 0 값만 구성할 수 있습니다. 당연히, 모든 양수 점수는 모니터링됩니다.

콘텐츠 차단

Cisco IronPort Data Security Policies(Cisco IronPort 데이터 보안 정책) > Content(콘텐츠) 페이지의 설정을 사용하여 웹 프록시에서 다음 파일 특성에 따라 데이터 업로드를 차단하도록 구성할 수 있습니다.

- **파일 크기.** 허용되는 최대 *업로드* 크기를 지정할 수 있습니다. 지정된 최대 크기와 같거나 더 큰 업로드는 모두 차단됩니다. HTTP/HTTPS 및 네이티브 FTP 요청에 대해 최대 파일 크기를 다르게 지정할 수 있습니다.

  업로드 요청 크기가 최대 업로드 크기 및 최대 검사 크기(Security Services(보안 서비스) > Anti-Malware(악성코드 차단) 페이지의 "DVS Engine Object Scanning Limits(DVS 엔진 개체 검사 제한)" 필드에 구성)보다 클 경우 업로드 요청은 차단되지만 데이터 보안 로그의 항목에서 파일 이름 및 콘텐츠 유형을 기록하지 않습니다. 액세스 로그의 항목은 변경되지 않습니다.

- **파일 유형.** 사전 정의 파일 유형 또는 사용자가 입력한 맞춤형 MIME 유형을 차단할 수 있습니다. 사전 정의 파일 유형을 차단할 경우 해당 유형의 모든 파일 또는 지정된 크기보다 큰 파일을 차단할 수 있습니다. 크기를 기준으로 파일 유형을 차단할 경우 지정 가능한 최대 파일 크기는 Security Services(보안 서비스) > Anti-Malware(악성코드 차단) 페이지의 "DVS Engine Object Scanning Limits(DVS 엔진 개체 검사 제한)" 필드의 값과 동일합니다. 기본적으로 이 값은 32MB입니다.

  Cisco IronPort 데이터 보안 필터는 파일 유형을 기준으로 차단할 경우 아카이브 파일의 콘텐츠를 검사하지 않습니다. 아카이브된 파일은 콘텐츠가 아니라 파일 유형 또는 파일 이름으로 차단될 수 있습니다.

참고 일부 MIME 유형 그룹에서는 한 유형을 차단하면 그룹에 있는 모든 MIME 유형이 차단됩니다. 예를 들어 application/x-java-applet을 차단하면 application/java, application/javascript 등과 같은 모든 java MIME 유형이 차단됩니다.

- **파일 이름.** 지정된 이름의 파일을 차단할 수 있습니다. 차단할 파일 이름을 지정하는 데 텍스트를 리터럴 문자열 또는 정규식으로 사용할 수 있습니다.

참고 8비트 ASCII 문자로만 파일 이름을 입력합니다. 웹 프록시는 8비트 ASCII 문자로 된 파일 이름만 매칭합니다.

외부 DLP 시스템 정의

웹 보안 어플라이언스는 어플라이언스에서 여러 DLP 서버를 정의하여 동일한 벤더의 여러 외부 DLP 서버와 통합할 수 있습니다. 웹 프록시에서 DLP 시스템에 연결할 때 사용하는 로드 밸런싱 기술을 정의할 수 있습니다. 이는 여러 DLP 시스템을 정의할 때 유용합니다. 외부 DLP 서버와의 통신 보호에 사용되는 프로토콜 지정에 대한 자세한 내용은 SSL 컨피그레이션, 22-23페이지를 참조하십시오.

참고 외부 DLP 서버가 웹 프록시에 수정된 콘텐츠를 전송하지 않는지 확인합니다. AsyncOS for Web은 업로드 요청 차단 또는 허용 기능만 지원합니다. 외부 DLP 서버에서 수정한 콘텐츠의 업로드는 지원하지 않습니다.

외부 DLP 서버 구성

1단계 **Network(네트워크) > External DLP Servers(외부 DLP 서버)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

설정	설명
외부 DLP 서버용 프로토콜	다음 중 하나를 선택합니다. • **ICAP** – DLP 클라이언트/서버 ICAP 통신이 암호화되지 않습니다. • **보안 ICAP** – DLP 클라이언트/서버 ICAP 통신이 암호화된 터널을 통해 이루어집니다. 추가 관련 옵션이 표시됩니다.

설정	설명
외부 DLP 서버	ICAP 호환 DLP 시스템에 액세스하려면 다음 정보를 입력합니다. • **서버 주소** 및 **포트** – DLP 시스템 액세스를 위한 호스트 이름 또는 IP 주소 및 TCP 포트. • **다시 연결 시도 횟수** – 실패하기 전에 웹 프록시가 DLP 시스템에 연결하려고 시도하는 횟수. • **서비스 URL** – 특정 DLP 서버와 관련된 ICAP 쿼리 URL. 웹 프록시는 여기에 입력된는 내용을 외부 DLP 서버에 전송하는 ICAP 요청에 포함합니다. URL은 ICAP 프로토콜로 시작해야 합니다. 예: icap:// • 인증서(선택 사항) - 각 외부 DLP 서버 연결을 보호하기 위해 제공되는 인증서는 CA(Certificate Authority)에서 서명되거나 자체 서명될 수 있습니다. 지정된 서버로부터 인증서를 확보한 다음 어플라이언스에 업로드합니다. – 인증서 파일을 찾아 선택한 후 **Upload File(파일 업로드)**을 클릭합니다. **참고** 이 단일 파일에는 클라이언트 인증서와 개인 키가 암호화되지 않은 양식으로 포함되어야 합니다. – **Use this certificate for all DLP servers using Secure ICAP(보안 ICAP를 사용하는 모든 DLP 서버에 이 인증서 사용)** – 여기에서 정의하는 모든 외부 DLP 서버에 동일한 인증서를 사용하려면 이 상자를 선택합니다. 각 서버에 다른 인증서를 입력하려면 이 옵션을 선택되지 않은 상태로 남겨 둡니다. • 테스트 시작 - **Start Test(테스트 시작)**를 클릭하여 웹 보안 어플라이언스와 정의된 외부 DLP 서버 간의 연결을 테스트할 수 있습니다.
로드 밸런싱	여러 DLP 서버가 정의된 경우 웹 프록시가 여러 DLP 서버에 업로드 요청을 분배하는 데 사용할 로드 밸런싱 기술을 선택합니다. 다음과 같은 로드 밸런싱 기술을 선택할 수 있습니다. • **없음(페일오버).** 웹 프록시가 업로드 요청을 하나의 DLP 서버에 전달합니다. 나열된 순서대로 DLP 서버에 연결하려고 시도합니다. 하나의 DLP 서버에 연결할 수 없는 경우 웹 프록시는 목록에 있는 다음 서버와 연결을 시도합니다. • **최소 연결.** 웹 프록시는 여러 DLP 서버에 대한 활성 요청 수를 계속 추적하면서 현재 가장 적은 수의 연결을 서비스하는 DLP 서버에 업로드 요청을 전달합니다. • **해시 기반.** 웹 프록시가 해시 함수를 사용하여 DLP 서버에 요청을 분배합니다. 해시 함수는 프록시 ID 및 URL을 입력으로 사용하여 동일한 URL에 대한 요청이 항상 동일한 DLP 서버로 전달되도록 합니다. • **라운드 로빈.** 웹 프록시가 나열된 순서대로 모든 DLP 서버에 고르게 업로드 요청을 순환합니다.
서비스 요청 시간 초과	웹 프록시가 DLP 서버의 응답을 기다리는 시간을 입력합니다. 이 시간을 초과한 경우 ICAP 요청이 실패한 것이며 오류 처리 설정에 따라 업로드 요청이 차단되거나 허용됩니다. 기본값은 60초입니다.

설정	설명
최대 동시 연결	웹 보안 어플라이언스에서 구성된 각 외부 DLP 서버까지 동시 ICAP 요청 연결 최대 수를 지정합니다. 이 페이지의 오류 처리 설정은 이 한도를 초과하는 모든 요청에 적용됩니다. 기본값은 25입니다.
오류 처리	DLP 서버가 적시에 응답하지 못할 경우 업로드 요청을 차단할지 아니면 허용할지(평가를 위해 액세스 정책에 전달됨) 선택합니다. 기본값은 허용("검사 없이 모든 데이터 전송 처리 허용") 입니다.
신뢰할 수 있는 루트 인증서	외부 DLP 서버와 함께 제공되는 인증서에 대한 신뢰할 수 있는 루트 인증서를 찾아 선택한 후 Upload File(파일 업로드)을 클릭합니다. 자세한 내용은 인증서 관리, 22-24페이지 섹션을 참조하십시오.
유효하지 않은 인증서 옵션	**Drop(삭제)** 또는 **Monitor(모니터링)** 중에서 다양한 유효하지 않은 인증서 처리 방법을 지정합니다.
서버 인증서	이 섹션에는 현재 어플라이언스에서 사용 가능한 모든 DLP 서버 인증서가 표시됩니다.

3단계 (선택 사항) **Add Row(행 추가)**를 클릭하고 새로 제공된 필드에 DLP 서버 정보를 입력하는 방법으로 다른 DLP 서버를 추가할 수 있습니다.

4단계 변경 사항을 **Submit(제출)** 및 **Commit(커밋)**합니다.

외부 DLP 정책을 사용하여 업로드 요청 제어

웹 프록시가 업로드 요청 헤더를 수신하면 검사를 위해 요청을 외부 DLP 시스템에 보낼지 여부를 결정하는 데 필요한 정보를 확보하게 됩니다. DLP 시스템은 요청을 검사하고 웹 프록시에 차단 또는 모니터링(액세스 정책과 비교하여 요청 평가) 판정을 반환합니다.

1단계 **Web Security Manager(웹 보안 관리자) > External Data Loss Prevention(외부 데이터 유출 방지)**을 선택합니다.

2단계 Destinations(대상) 열에서 구성할 정책 그룹에 해당하는 링크를 클릭합니다.

3단계 **Edit Destination Settings(대상 설정 수정** 섹션에서 **"Define Destinations Scanning Custom Settings(대상 검사 맞춤형 설정 정의"**를 선택합니다.

4단계 Destination to scan(검사 대상) 섹션에서 다음 옵션 중 하나를 선택합니다.

- **Do not scan any uploads(업로드를 검사하지 않음).** 구성된 DLP 시스템에 검사를 위해 어떤 업로드 요청도 보내지 않습니다. 모든 업로드 요청이 액세스 정책과 비교하여 평가됩니다.
- **Scan all uploads(모든 업로드 검사).** 구성된 DLP 시스템에 모든 업로드 요청을 보내 검사받습니다. DLP 시스템 검사 판정에 따라 업로드 요청이 차단되거나 액세스 정책과 비교하여 평가됩니다.
- **Scan uploads to specified custom URL categories only(지정된 맞춤형 URL 카테고리에 대한 업로드만 검사).** 특정 맞춤형 URL 카테고리에 속하는 업로드 요청은 검사를 위해 구성된 DLP 시스템에 전송됩니다. DLP 시스템 검사 판정에 따라 업로드 요청이 차단되거나 액세스 정책과 비교하여 평가됩니다. **Edit custom categories list(맞춤형 카테고리 목록 수정)**를 클릭하여 검사할 URL 카테고리를 선택합니다.

5단계 변경 사항을 **Submit(제출)** 및 **Commit Changes(커밋)**합니다.

데이터 유출 방지 검사 기록

액세스 로그는 Cisco IronPort 데이터 보안 필터 또는 외부 DLP 서버에서 업로드 요청을 검사했는지 여부를 나타냅니다. 액세스 로그 항목에는 Cisco IronPort 데이터 보안 검사 판정용 필드와 외부 DLP 검사 판정 기반 필드가 각각 포함되어 있습니다.

액세스 로그 이외에 웹 보안 어플라이언스는 다음과 같은 로그 파일 유형을 제공하여 Cisco IronPort 데이터 보안 및 외부 DLP 정책을 트러블슈팅 합니다.

- **데이터 보안 로그.** Cisco IronPort 데이터 보안 필터에서 평가하는 업로드 요청에 대한 클라이언트 내역을 기록합니다.
- **데이터 보안 모듈 로그.** Cisco IronPort 데이터 보안 필터와 관련된 메시지를 기록합니다.
- **기본 프록시 로그.** 기본 프록시 로그는 웹 프록시와 관련된 오류를 기록할 뿐 아니라 외부 DLP 서버와의 연결 관련 메시지를 포함합니다. 그러면 외부 DLP 서버와의 연결 또는 통합 문제를 트러블슈팅할 수 있습니다.

다음 텍스트는 데이터 보안 로그 항목의 예입니다.

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

필드 값	설명
`Mon Mar 30 03:02:13 2009 Info:`	타임스탬프 및 추적 레벨
`303`	거래 ID
`10.1.1.1`	소스 IP 주소
`-`	사용자 이름
`-`	권한 있는 그룹 이름
`<<bar,text/plain,5120><foo,text/plain,5120>>`	한꺼번에 업로드된 각 파일의 이름, 유형, 크기 **참고** 이 필드는 구성된 최소 요청 본문 크기(기본값은 4096바이트)보다 작은 텍스트/일반 파일을 포함하지 않습니다.
`BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting`	Cisco IronPort 데이터 보안 정책 및 조치
`ns`	웹 평판 점수
`server.com`	발신 URL
`nc`	URL 카테고리

참고 어떤 사이트에 대한 POST 요청과 같은 데이터 전송이 외부 DLP 서버에 의해 차단된 시간을 확인하려면 액세스 로그에서 DLP 서버의 IP 주소 또는 호스트 이름을 검색합니다.

17장

최종 사용자에게 프록시 조치 알림

- 최종 사용자 알림 개요, 17-1페이지
- 알림 페이지에 대한 일반 설정 구성, 17-2페이지
- 최종 사용자 승인 페이지, 17-2페이지
- 최종 사용자 알림 페이지, 17-5페이지
- 최종 사용자 URL 필터링 경고 페이지 구성, 17-9페이지
- FTP 알림 메시지 구성, 17-9페이지
- 알림 페이지의 맞춤형 메시지, 17-10페이지
- 알림 페이지 HTML 파일을 직접 편집, 17-11페이지
- 알림 페이지 유형, 17-15페이지

최종 사용자 알림 개요

최종 사용자에 대한 다음 유형의 알림을 구성할 수 있습니다.

옵션	설명	추가 정보
최종 사용자 승인 페이지	해당 웹 활동이 필터링 및 모니터링 되고 있음을 최종 사용자에게 알립니다. 일정한 기간 후에 사용자가 처음으로 브라우저에 액세스할 때 최종 사용자 승인 페이지가 표시됩니다.	최종 사용자 승인 페이지, 17-2페이지
최종 사용자 알림 페이지	특정 페이지에 대한 액세스가 차단되는 경우 최종 사용자에게 표시되는 페이지이며, 해당 액세스를 차단한 이유와 관련됩니다.	최종 사용자 알림 페이지, 17-5페이지
최종 사용자 URL 필터링 경고 페이지	액세스하는 사이트가 조직의 제한적 사용 정책을 충족하지 않는다고 최종 사용자에게 경고하고 선택하는 경우 계속 진행하도록 허용합니다.	최종 사용자 URL 필터링 경고 페이지 구성, 17-9페이지
FTP 알림 메시지	네이티브 FTP 트랜잭션이 차단된 이유를 최종 사용자에게 제공합니다.	FTP 알림 메시지 구성, 17-9페이지.

옵션	설명	추가 정보
시간 및 볼륨 할당량 만료 경고 페이지	구성된 데이터 볼륨 또는 시간 제한에 도달하여 액세스가 차단된 경우 최종 사용자에게 알립니다.	Security Services(보안 서비스) > End User Notification(최종 사용자 알림) 페이지, Time and Volume Quotas Expiry Warning Page(시간 및 볼륨 할당량 만료 경고 페이지) 섹션에서 이러한 설정을 구성합니다. 시간 범위 및 할당량, 10-12페이지도 참조하십시오.

알림 페이지에 대한 일반 설정 구성

알림 페이지에 대한 표시 언어 및 로고를 지정합니다. 제한 사항은 이 절차에 설명되어 있습니다.

1단계 **Security Services(보안 서비스) > End-User Notification(최종 사용자 알림)**을 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 General Settings(일반 설정) 섹션에서 웹 프록시가 알림 페이지를 표시할 때 사용해야 하는 언어를 선택합니다.

- HTTP 언어 설정은 모든 HTTP 알림 페이지(승인, 온박스 최종 사용자, 맞춤화된 최종 사용자 및 최종 사용자 URL 필터링 경고)에 적용됩니다.
- FTP 언어는 모든 FTP 알림 페이지에 적용됩니다.

4단계 각 알림 페이지에서 로고를 사용할지 여부를 선택합니다. Use Custom Logo(맞춤형 로고 사용) 필드에 입력하는 URL에서 참조되는 Cisco 로고 또는 그래픽 파일을 지정할 수 있습니다.

이 설정은 IPv4를 통해 제공되는 모든 HTTP 알림 페이지에 적용됩니다. AsyncOS는 IPv6을 통해 이미지를 지원하지 않습니다.

5단계 **변경 사항을 제출** 및 **커밋**합니다.

관련 주제

- 알림 페이지의 URL 및 로그 주의 사항, 17-11페이지

최종 사용자 승인 페이지

웹 활동을 필터링 및 모니터링 중임을 사용자에게 알리도록 웹 보안 어플라이언스를 구성할 수 있습니다. 구성된 경우 어플라이언스가 HTTP 또는 HTTPS를 사용하여 웹에 액세스하는 모든 사용자에게 최종 사용자 승인 페이지를 표시합니다. 사용자가 처음으로 웹 사이트에 액세스하려고 시도하는 경우나 구성된 시간 간격 이후 최종 사용자 승인 페이지를 표시합니다.

인증을 통해 사용자 이름이 사용 가능하게 된 경우 웹 프록시가 사용자 이름으로 사용자를 추적합니다. 사용자 이름이 사용 불가능한 경우 사용자를 추적하는 방법(IP 주소 또는 웹 브라우저 세션 쿠키로)을 선택할 수 있습니다.

참고 네이티브 FTP 트랜잭션은 최종 사용자 승인 페이지에서 제외됩니다.

최종 사용자 승인 페이지를 사용하여 HTTPS 및 FTP 사이트에 액세스

최종 사용자 승인 페이지는 강제로 사용 정책 계약을 클릭하도록 하는 HTML 페이지를 최종 사용자에게 표시하기 때문에 이 페이지가 작동합니다. 사용자가 링크를 클릭하면 웹 프록시가 클라이언트를 원래 요청된 웹 사이트로 리디렉션합니다. 사용자에 대한 사용자 이름을 사용할 수 없는 경우에는 서로게이트(IP 주소 또는 웹 브라우저 세션 쿠키)를 사용하여 사용자가 최종 사용자 승인 페이지를 수락한 시간을 추적합니다.

- **HTTPS.** 웹 프록시는 사용자가 쿠키를 사용하여 최종 사용자 승인 페이지를 승인했는지 여부를 추적하지만 트랜잭션의 암호를 해독하지 않으면 쿠키를 확보할 수 없습니다. 최종 사용자 승인 페이지가 사용하도록 설정되어 있고 세션 쿠키를 사용하여 사용자를 추적하는 경우 HTTPS 요청을 무시(통과)하거나 삭제할지를 선택할 수 있습니다. `advancedproxyconfig > EUN` CLI 명령을 사용하여 이를 수행하고 "세션 기반 EUA를 사용하는 HTTP 요청에 대해 수행될 조치("bypass" 또는 "drop")" 명령에 대해 bypass를 선택합니다.
- **FTP over HTTP.** 웹 브라우저가 FTP over HTTP 트랜잭션에 대한 쿠키를 전송하지 않으므로 웹 프록시가 쿠키를 확보할 수 없습니다. 이 문제를 해결하기 위해 FTP over HTTP 트랜잭션에 최종 사용자 승인 페이지가 필요하지 않도록 설정할 수 있습니다. "ftp://"를 정규식으로 사용하여(따옴표 없이) 맞춤형 URL 카테고리를 생성하고 이 맞춤형 URL 카테고리에 대한 최종 사용자 승인 페이지에서 사용자를 제외하는 ID 정책을 정의하여 이를 수행합니다.

최종 사용자 승인 페이지 정보

- IP 주소로 사용자를 추적하는 경우 어플라이언스가 최대 시간 간격 및 최대 IP 주소 유휴 시간 제한의 가장 짧은 값을 사용하여 최종 사용자 승인 페이지를 다시 표시할 시기를 결정합니다.
- 사용자가 세션 쿠키를 사용하여 추적되면 사용자가 웹 브라우저를 닫은 후 다시 열거나 두 번째 웹 브라우저 애플리케이션을 여는 경우 웹 프록시가 최종 사용자 승인 페이지를 다시 표시합니다.
- 클라이언트가 FTP over HTTP를 사용하여 HTTPS 사이트 또는 FTP 서버에 액세스할 때 세션 쿠키를 사용하여 사용자를 추적하는 작업은 작동하지 않습니다.
- 어플라이언스가 명시적 전달 모드에서 구축되고 사용자가 HTTPS 사이트로 이동하면 사용자를 원래 요청된 URL로 리디렉션하는 도메인 이름만 최종 사용자 승인 페이지의 링크에 포함됩니다. 원래 요청된 URL에 도메인 이름 다음에 텍스트를 포함하는 경우 해당 텍스트가 잘립니다.
- 최종 사용자 승인 페이지가 사용자에게 표시될 때 해당 트랜잭션에 대한 액세스 로그 항목이 OTHER를 ACL 결정 태그로 표시합니다. 원래 요청된 URL이 차단되고 대신 최종 사용자 승인 페이지가 사용자에게 표시되었기 때문입니다.

최종 사용자 승인 페이지 구성

웹 인터페이스 또는 CLI(Command Line Interface)에서 최종 사용자 승인 페이지를 사용하도록 설정하고 구성할 수 있습니다. 웹 인터페이스에서 최종 사용자 승인 페이지를 구성하는 경우 각 페이지에 표시되는 맞춤형 메시지를 포함할 수 있습니다.

CLI에서 `advancedproxyconfig > eun`을 사용합니다.

시작하기 전에

- 표시 언어를 구성하고 표시된 로고를 맞춤화하려면 알림 페이지에 대한 일반 설정 구성, 17-2페이지를 참조하십시오.

- 최종 사용자에게 표시되는 메시지를 맞춤화할 경우 알림 페이지의 맞춤형 메시지, 17-10페이지를 참조하십시오. Custom Message(맞춤형 메시지) 상자에서 허용하는 것보다 더 많은 맞춤화가 필요한 경우 알림 페이지 HTML 파일을 직접 편집, 17-11페이지를 참조하십시오.

1단계 **Security Services(보안 서비스) > End-User Notification(최종 사용자 알림)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 "**Require end-user to click through acknowledgment page(최종 사용자가 승인 페이지를 클릭해야 함)**" 필드를 사용하도록 설정합니다.

4단계 옵션을 입력합니다.

설정	설명
승인 간격	승인 간격은 웹 프록시가 각 사용자에게 최종 사용자 승인 페이지를 표시하는 빈도를 결정합니다. 이 설정은 사용자 이름으로 추적된 사용자와 IP 주소 또는 세션 쿠키로 추적된 사용자에 적용됩니다. 30초에서 2678400초(1개월) 사이의 값을 지정할 수 있습니다. 기본값은 1일(86400초)입니다. 승인 간격이 변경되고 커밋되면 웹 프록시를 이미 승인한 사용자의 경우에도 웹 프록시가 새 값을 사용합니다.
비활동 시간 제한	비활동 시간 제한은 IP 주소 또는 세션 쿠키(인증되지 않은 사용자만)로 추적 및 승인된 사용자가 사용 정책에 동의한 것으로 간주하는 동안에 유휴 상태일 수 있는 시간을 결정합니다. 30초에서 2678400초(1개월) 사이의 값을 지정할 수 있습니다. 기본값은 4시간(14400초)입니다.
대리 유형	웹 프록시에서 사용자를 추적하는 데 사용하는 방법을 결정합니다. • **IP 주소.** 사용자가 최종 사용자 승인 페이지에서 링크를 클릭하면 웹 프록시에서 해당 IP 주소의 사용자가 웹 브라우저 또는 브라우저에 기반하지 않는 HTTP 프로세스를 사용하여 웹에 액세스할 수 있도록 합니다. IP 주소로 사용자를 추적하면 비활성 또는 구성된 새 승인 시간 간격으로 인해 웹 프록시에서 새로운 최종 사용자 승인 페이지를 표시할 때까지 사용자가 웹에 액세스할 수 있습니다. 세션 쿠키를 통한 추적과 다르게 IP 주소로 추적하면 사용자가 여러 웹 브라우저 애플리케이션을 열 수 있으며 구성된 시간 간격이 만료된 경우가 아니면 최종 사용자 승인에 동의하지 않아도 됩니다. **참고** IP 주소가 구성되고 사용자가 인증된 경우 웹 프록시가 IP 주소 대신에 사용자 이름으로 사용자를 추적합니다. • **세션 쿠키.** 사용자가 최종 사용자 승인 페이지에서 링크를 클릭하고 쿠키를 사용하여 해당 세션을 추적하면 웹 프록시에서 사용자의 웹 브라우저에 쿠키를 전송합니다. 사용자는 승인 간격 값이 만료되거나, 할당 시간보다 더 오래 비활성 상태였거나, 웹 브라우저를 닫을 때까지 계속해서 웹 브라우저를 사용하여 웹에 액세스할 수 있습니다. 사용자가 브라우저에 기반하지 않는 HTTP 클라이언트 애플리케이션을 사용하는 경우 최종 사용자 승인 페이지의 링크를 클릭하여 웹에 액세스할 수 있어야 합니다. 사용자가 두 번째 웹 브라우저 애플리케이션을 여는 경우 웹 프록시에서 두 번째 웹 브라우저에 세션 쿠키를 전송하려면 사용자가 최종 사용자 승인 프로세스를 다시 통과해야 합니다. **참고** 클라이언트가 FTP over HTTP를 사용하여 HTTPS 사이트 또는 FTP 서버에 액세스할 때 세션 쿠키를 사용하여 사용자를 추적하는 것은 지원되지 않습니다.

설정	설명
맞춤형 메시지	모든 최종 사용자 승인 페이지에 표시되는 텍스트를 맞춤화합니다. 텍스트 형식을 지정하기 위해 몇 가지 단순 HTML 태그를 포함할 수 있습니다. **참고** CLI가 아니라 웹 인터페이스에서 최종 사용자 승인 페이지를 구성하는 경우에만 맞춤형 메시지를 포함할 수 있습니다. 알림 페이지의 맞춤형 메시지, 17-10페이지도 참조하십시오.

5단계 (선택 사항) 현재 최종 사용자 승인 페이지를 별도의 브라우저 창에서 보려면 **Preview Acknowledgment Page Customization(승인 페이지 맞춤화 미리보기)**을 클릭합니다.

참고 알림 HTML 파일이 편집된 경우 이 미리보기 기능을 사용할 수 없습니다.

6단계 **변경 사항을 제출** 및 **커밋**합니다.

최종 사용자 알림 페이지

정책으로 인해 사용자가 웹 사이트에서 차단된 경우 URL 요청을 차단한 이유를 사용자에게 알리도록 어플라이언스를 구성할 수 있습니다. 다음 몇 가지 방법으로 이 작업을 수행합니다.

하려는 작업	참조:
웹 보안 어플라이언스에서 호스팅되는 미리 정의된 맞춤화 가능 페이지를 표시합니다.	온박스 최종 사용자 알림 페이지 구성, 17-5페이지
사용자를 특정 URL의 HTTP 최종 사용자 알림 페이지로 리디렉션합니다.	오프박스 최종 사용자 알림 페이지, 17-6페이지

온박스 최종 사용자 알림 페이지 구성

온박스 페이지는 어플라이언스에 있는 미리 정의된 맞춤화 가능 알림 페이지입니다.

시작하기 전에

- 표시 언어를 구성하고 표시된 로고를 맞춤화하려면 알림 페이지에 대한 일반 설정 구성, 17-2페이지를 참조하십시오.
- 온박스 알림을 사용하여 표시되는 메시지를 맞춤화할 경우 알림 페이지의 맞춤형 메시지, 17-10페이지 아래의 주제를 검토하십시오. Custom Message(맞춤형 메시지) 상자에서 허용하는 것보다 더 많은 맞춤화가 필요한 경우 알림 페이지 HTML 파일을 직접 편집, 17-11페이지를 참조하십시오.

1단계 **Security Services(보안 서비스)** > **End-User Notification(최종 사용자 알림)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 Notification Type(알림 유형) 필드에서 **Use On Box End User Notification(온박스 최종 사용자 알림 사용)**을 선택합니다.

4단계 온박스 최종 사용자 알림 페이지 설정을 구성합니다.

설정	설명
사용자 지정 메시지	각 알림 페이지에 필요한 추가 텍스트를 포함합니다. 맞춤형 메시지를 입력하면 AsyncOS가 연락처 정보를 포함하는 알림 페이지의 마지막 문장 앞에 메시지를 배치합니다.
담당자 정보	각 알림 페이지에 나열되는 연락처 정보를 맞춤화합니다. AsyncOS는 사용자가 네트워크 관리자에게 제공할 수 있는 알림 코드를 제공하기 전에 연락처 정보 문장을 페이지의 마지막 문장으로 표시합니다.
최종 사용자 오분류 보고	사용하도록 설정된 경우 사용자가 Cisco에 잘못 분류된 URL을 보고할 수 있습니다. 의심되는 악성코드 또는 URL 필터로 인해 차단된 사이트에 대한 온박스 최종 사용자 알림 페이지에 추가 버튼이 표시됩니다. 사용자는 페이지가 잘못 분류되었다고 생각하는 경우에 이 버튼을 사용하여 보고할 수 있습니다. 다른 정책 설정으로 인해 차단된 페이지의 경우에는 이 버튼이 표시되지 않습니다.

5단계 (선택 사항) 현재 최종 사용자 알림 페이지를 별도의 브라우저 창에서 보려면 **Preview Notification Page Customization(알림 페이지 맞춤화 미리보기)** 링크를 클릭합니다.

참고 알림 HTML 파일이 편집된 경우 이 미리보기 기능을 사용할 수 없습니다.

6단계 **변경 사항을 제출** 및 **커밋**합니다.

오프박스 최종 사용자 알림 페이지

모든 HTTP 최종 사용자 알림 페이지를 사용자가 지정하는 특정 URL로 리디렉션하도록 웹 프록시를 구성할 수 있습니다.

액세스 차단 이유에 따라 올바른 오프박스 페이지 표시

기본적으로 AsyncOS는 원래 페이지를 차단한 이유와 관계없이 차단된 모든 웹 사이트를 해당 URL로 리디렉션합니다. 그러나 AsyncOS는 매개변수를 리디렉션 URL에 추가된 쿼리 문자열로 전달하므로 차단 이유를 설명하는 고유한 페이지가 사용자에게 표시되도록 할 수 있습니다. 포함된 매개변수에 대한 자세한 내용은 오프박스 최종 사용자 알림 페이지 매개변수, 17-7페이지를 참조하십시오.

사용자가 차단된 웹 사이트에 대한 이유에 따라 다른 페이지를 보도록 하려면 리디렉션 URL에서 쿼리 문자열을 구문 분석할 수 있는 CGI 스크립트를 웹 서버에 생성합니다. 그러면 서버에서 적절한 페이지로의 두 번째 리디렉션을 수행할 수 있습니다.

오프박스 알림 페이지에 대한 URL 기준

- 임의의 HTTP 또는 HTTPS URL을 사용할 수 있습니다.
- URL이 특정 포트 번호를 지정할 수 있습니다.
- URL에서 물음표 다음에 인수가 올 수 없습니다.
- URL에는 올바른 형식의 호스트 이름이 포함되어야 합니다.

예를 들어, Redirect to Custom URL(맞춤형 URL로 리디렉션) 필드에 다음 URL을 입력했다고 가정합니다.

```
http://www.example.com/eun.policy.html
```

또한 다음 액세스 로그 항목이 있는 경우:

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html
HTTP/1.1 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

AsyncOS에서 다음과 같은 리디렉션된 URL을 생성합니다.

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

오프박스 최종 사용자 알림 페이지 매개변수

AsyncOS는 매개변수를 HTTP GET 요청의 표준 URL 매개변수로 웹 서버에 전달합니다. 다음과 같은 형식을 사용합니다.

```
<notification_page_url>?param1=value1&param2=value2
```

다음 표에서는 AsyncOS가 쿼리 문자열에 포함하는 매개변수에 대해 설명합니다.

매개 변수 이름	설명
Time	트랜잭션의 날짜 및 시간입니다.
ID	트랜잭션 ID입니다.
Client_IP	클라이언트의 IP 주소입니다.
User	사용 가능한 경우 요청을 작성한 클라이언트의 사용자 이름입니다.
Site	HTTP 요청에 있는 대상의 호스트 이름입니다.
URI	HTTP 요청에 지정된 URL 경로입니다.
Status_Code	요청의 HTTP 상태 코드입니다.
Decision_Tag	DVS 엔진이 트랜잭션을 처리한 방법을 나타내는 액세스 로그 항목에 정의된 ACL 결정 태그입니다.
URL_Cat	URL 필터링 엔진이 트랜잭션 요청에 할당한 URL 카테고리입니다. **참고:** AsyncOS for Web에서는 미리 정의된 URL 카테고리와 사용자 정의 URL 카테고리 모두에 대한 전체 URL 카테고리 이름을 전송합니다. 카테고리 이름에 대해 URL 인코딩을 수행하므로 공백은 "%20"으로 기록됩니다.

매개 변수 이름	설명
WBRS	웹 평판 필터가 요청의 URL에 할당한 WBRS 점수입니다.
DVS_Verdict	DVS 엔진이 트랜잭션에 할당하는 악성코드 카테고리입니다.
DVS_ThreatName	DVS 엔진에서 발견한 악성코드의 이름입니다.
Reauth_URL	제한적 URL 필터링 정책으로 인해 사용자가 웹 사이트에서 차단된 경우 사용자가 클릭하여 다시 인증할 수 있는 URL입니다. "Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction(최종 사용자가 URL 카테고리 또는 사용자 세션 제한으로 차단된 경우 재인증 프롬프트 사용)" 전역 인증 설정이 사용하도록 설정되어 있고 사용자가 차단된 URL 카테고리로 인해 웹 사이트에서 차단된 경우 이 매개변수를 사용합니다. 이 매개변수를 사용하려면 CGI 스크립트에서 다음 단계를 수행하는지 확인합니다. 1. `Reauth_Url` 매개변수의 값을 가져옵니다. 2. 값을 URL로 디코딩합니다. 3. Base64가 값을 디코딩하고 실제 재인증 URL을 가져옵니다. 4. 링크를 클릭하고 액세스 권한을 확대할 수 있는 새로운 인증 자격 증명을 입력할 수 있음을 사용자에게 알리는 지침과 함께 최종 사용자 알림 페이지에 링크 또는 버튼과 같은 몇 가지 방식으로 디코딩된 URL을 포함합니다.

참고 AsyncOS는 항상 각 리디렉션된 URL에 모든 매개변수를 포함합니다. 특정 매개변수의 값이 없는 경우 AsyncOS가 하이픈(-)을 전달합니다.

최종 사용자 알림 페이지를 맞춤형 URL로 리디렉션(오프박스)

1단계 **Security Services(보안 서비스)** > **End-User Notification(최종 사용자 알림)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 End-User Notification Pages(최종 사용자 알림 페이지) 섹션에서 **Redirect to Custom URL(맞춤형 URL로 리디렉션)**을 선택합니다.

4단계 Notification Page URL(알림 페이지 URL) 필드에 차단된 웹 사이트를 리디렉션할 URL을 입력합니다.

5단계 (선택 사항) **Preview Custom URL(맞춤형 URL 미리보기)** 링크를 클릭합니다.

6단계 **변경 사항을 제출** 및 **커밋**합니다.

최종 사용자 URL 필터링 경고 페이지 구성

일정한 기간 후에 사용자가 특정 URL 카테고리의 웹 사이트에 처음으로 액세스할 때 최종 사용자 URL 필터링 경고 페이지가 표시됩니다. 사이트 콘텐츠 등급 기능이 사용하도록 설정된 경우 사용자가 성인 콘텐츠에 액세스할 때 표시할 경고 페이지를 구성할 수도 있습니다.

시작하기 전에

온박스 알림을 사용하여 표시되는 메시지를 맞춤화할 경우 알림 페이지의 맞춤형 메시지, 17-10페이지 아래의 주제를 검토하십시오. Custom Message(맞춤형 메시지) 상자에서 허용하는 것보다 더 많은 맞춤화가 필요한 경우 알림 페이지 HTML 파일을 직접 편집, 17-11페이지를 참조하십시오.

1단계 **Security Services(보안 서비스) > End-User Notification(최종 사용자 알림)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 화면을 스크롤하여 End-User URL Filtering Warning Page(최종 사용자 URL 필터링 경고 페이지) 섹션으로 이동합니다.

4단계 Time Between Warning(경고 간격) 필드에 웹 프록시에서 사용자별로 각 URL 카테고리에 대한 최종 사용자 URL 필터링 경고 페이지를 표시하는 간격으로 사용하는 시간 간격을 입력합니다.

30초에서 2678400초(1개월) 사이의 값을 지정할 수 있습니다. 기본값은 1시간(3600초)입니다. 초, 분 또는 일 단위로 값을 입력할 수 있습니다. 초에는 's', 분에는 'm', 일에는 'd'를 사용합니다.

5단계 Custom Message(맞춤형 메시지) 필드에 모든 최종 사용자 URL 필터링 경고 페이지에서 표시할 텍스트를 입력합니다.

6단계 (선택 사항) 현재 최종 사용자 URL 필터링 경고 페이지를 별도의 브라우저 창에서 보려면 **Preview URL Category Warning Page Customization(URL 카테고리 경고 페이지 맞춤화 미리보기)**을 클릭합니다.

참고 알림 HTML 파일이 편집된 경우 이 미리보기 기능을 사용할 수 없습니다.

7단계 **변경 사항을 제출** 및 **커밋**합니다.

FTP 알림 메시지 구성

FTP 프록시 인증 오류 또는 서버 도메인 이름에 대한 나쁜 평판 등 어떤 이유로든 FTP 프록시가 FTP 서버와의 연결을 설정할 수 없는 경우 FTP 프록시는 네이티브 FTP 클라이언트에 미리 정의된 맞춤화 가능 알림 메시지를 표시합니다. 알림은 연결이 차단된 이유와 관련됩니다.

시작하기 전에

온박스 알림을 사용하여 표시되는 메시지를 맞춤화할 경우 알림 페이지의 맞춤형 메시지, 17-10페이지 아래의 주제를 검토하십시오. Custom Message(맞춤형 메시지) 상자에서 허용하는 것보다 더 많은 맞춤화가 필요한 경우 알림 페이지 HTML 파일을 직접 편집, 17-11페이지를 참조하십시오.

1단계 **Security Services(보안 서비스) > End-User Notification(최종 사용자 알림)**.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 화면을 아래로 스크롤하여 네이티브 FTP 섹션으로 이동합니다.

4단계 Language(언어) 필드에서 네이티브 FTP 알림 메시지를 표시할 때 사용할 언어를 선택합니다.

5단계 Custom Message(맞춤형 메시지) 필드에 모든 네이티브 FTP 알림 메시지에서 표시할 텍스트를 입력합니다.

6단계 **변경 사항을 제출** 및 **커밋**합니다.

알림 페이지의 맞춤형 메시지

다음 섹션은 Edit End User Notification(최종 사용자 알림 편집) 페이지에서 구성된 알림 유형에 대해 "Custom Message(맞춤형 메시지)" 상자에 입력한 텍스트에 적용됩니다.

- 알림 페이지의 맞춤형 메시지에서 지원되는 HTML 태그, 17-10페이지
- 알림 페이지의 URL 및 로그 주의 사항, 17-11페이지

알림 페이지의 맞춤형 메시지에서 지원되는 HTML 태그

HTML 태그를 사용하여 "Custom Message(맞춤형 메시지)" 상자를 제공하는 Edit End User Notification(최종 사용자 알림 편집) 페이지의 알림에서 텍스트 형식을 지정할 수 있습니다. 태그는 소문자이고 표준 HTML 구문(예: 닫는 태그)을 따라야 합니다.

다음과 같은 HTML 태그를 사용할 수 있습니다.

- <a>
-
-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

예를 들어, 일부 텍스트를 기울임꼴로 설정할 수 있습니다.

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

 태그로 CSS 스타일을 사용하여 텍스트 형식을 지정할 수 있습니다. 예를 들어, 일부 텍스트를 빨간색으로 설정할 수 있습니다.

```
<span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

참고 유연성을 강화해야 하거나 알림 페이지에 JavaScript를 추가하려는 경우 HTML 알림 파일을 직접 편집해야 합니다. 웹 사용자 인터페이스의 알림에 대한 Custom Message(맞춤형 메시지) 상자에 입력한 JavaScript가 제거됩니다. 알림 페이지 HTML 파일을 직접 편집, 17-11페이지를 참조하십시오.

알림 페이지의 URL 및 로그 주의 사항

이 섹션은 다음과 같이 맞춤화할 경우에 적용됩니다.

- Edit End User Notification(최종 사용자 알림 편집) 페이지에서 알림에 대한 "Custom Message(맞춤형 메시지)" 상자에 텍스트 입력
- 온박스 알림에 대한 HTML 파일 직접 편집
- 맞춤형 로고 사용

온박스 알림의 경우 맞춤형 텍스트 내에 포함된 링크의 URL 경로 및 도메인 이름과 맞춤형 로고의 모든 조합이 다음에서 제외됩니다.

- 사용자 인증:
- 최종 사용자 승인
- 악성코드 스캐닝 및 웹 평판 점수와 같은 모든 스캐닝

예를 들어, 다음 URL이 맞춤형 텍스트에 포함되었다고 가정합니다.

`http://www.example.com/index.html`

`http://www.mycompany.com/logo.jpg`

그러면 다음 모든 URL도 모든 스캐닝에서 제외되는 것으로 처리됩니다.

`http://www.example.com/index.html`

`http://www.mycompany.com/logo.jpg`

`http://www.example.com/logo.jpg`

`http://www.mycompany.com/index.html`

또한 포함된 URL이 `<protocol>://<domain-name>/<directory path>/` 형식이면 호스트의 해당 디렉토리 경로 아래 모든 하위 파일과 하위 디렉토리도 모든 스캐닝에서 제외됩니다.

예를 들어, URL `http://www.example.com/gallery2/`가 포함된 경우 `http://www.example.com/gallery2/main.php` 등과 같은 URL도 제외로 처리됩니다.

이를 통해 포함된 콘텐츠가 초기 URL과 관련되는 경우 포함된 콘텐츠가 들어 있는 더 정교한 페이지를 생성할 수 있습니다. 그러나 링크 및 맞춤형 로고로 포함할 경로를 결정할 때 신중하게 처리해야 합니다.

알림 페이지 HTML 파일을 직접 편집

각 알림 페이지는 웹 보안 어플라이언스에 HTML 파일로 저장됩니다. 웹 기반 인터페이스의 "Custom Message(맞춤형 메시지)" 상자에서 허용하는 것보다 더 많은 맞춤화가 필요한 경우 이러한 HTML 파일을 직접 편집할 수 있습니다. 예를 들어, 표준 JavaScript를 포함하거나 각 페이지의 전체 룩앤드필(look and feel)을 편집할 수 있습니다.

다음 섹션의 정보는 End-User Acknowledgment(최종 사용자 승인) 페이지를 포함하여 어플라이언스에 있는 모든 유형의 최종 사용자 알림 HTML 파일에 적용됩니다.

알림 HTML 파일을 직접 편집하기 위한 요건

- 각 알림 페이지 파일은 유효한 HTML 파일이어야 합니다. 포함할 수 있는 HTML 태그 목록은 알림 페이지의 맞춤형 메시지에서 지원되는 HTML 태그, 17-10페이지를 참조하십시오.
- 맞춤화된 알림 페이지 파일 이름은 웹 보안 어플라이언스와 함께 제공되는 파일 이름과 정확히 일치해야 합니다.

  필요한 이름을 사용하는 특정 파일이 `configuration\eun` 디렉토리에 없는 경우 어플라이언스가 표준 온박스 최종 사용자 알림 페이지를 표시합니다.
- URL에 대한 링크는 HTML 파일에 포함하지 마십시오. 알림 페이지에 포함된 링크에는 액세스 정책에 정의된 액세스 제어 규칙이 적용되므로 사용자가 반복 루프에 빠지게 될 수 있습니다.
- 특히 JavaScript를 포함하는 경우 지원되는 클라이언트 브라우저에서 HTML 파일을 테스트하여 예상대로 작동하는지 확인하십시오.
- 맞춤화된 페이지를 적용하려면 `advancedproxyconfig > EUN > Refresh EUN Pages(EUN 페이지 새로고침)` CLI 명령을 사용하여 맞춤화된 파일을 사용하도록 설정해야 합니다.

알림 HTML 파일을 직접 편집

시작하기 전에

- 알림 HTML 파일을 직접 편집하기 위한 요건, 17-12페이지의 요건을 이해합니다.
- 알림 HTML 파일을 맞춤화하기 위한 변수 및 알림 HTML 파일에서 변수 사용, 17-13페이지를 참조하십시오.

1단계 FTP 클라이언트를 사용하여 웹 보안 어플라이언스에 연결합니다.

2단계 `configuration\eun` 디렉토리로 이동합니다.

3단계 편집하려는 알림 페이지에 대한 언어 디렉토리 파일을 다운로드합니다.

4단계 로컬 컴퓨터에서 텍스트 또는 HTML 편집기를 사용하여 HTML 파일을 편집합니다.

5단계 FTP 클라이언트를 사용하여 맞춤화된 HTML 파일을 3단계에서 다운로드한 디렉토리와 동일한 디렉토리에 업로드합니다.

6단계 SSH 클라이언트를 열고 웹 보안 어플라이언스에 연결합니다.

7단계 `advancedproxyconfig > EUN` CLI 명령을 실행합니다.

8단계 맞춤형 최종 사용자 알림 페이지를 사용하려면 `2`를 입력합니다.

9단계 HTML 파일을 업데이트할 때 맞춤형 최종 사용자 알림 페이지 옵션이 현재 사용하도록 설정된 경우 `1`을 입력하여 맞춤형 최종 사용자 알림 페이지를 새로 고칩니다.

이를 수행하지 않으면 웹 프록시가 재시작될 때까지 새 파일이 적용되지 않습니다.

10단계 변경 사항을 커밋합니다.

11단계 SSH 클라이언트를 닫습니다.

알림 HTML 파일에서 변수 사용

알림 HTML 파일을 편집할 때 조건 변수를 포함하여 현재 상태에 따라 다른 조치를 수행하기 위한 if-then 문을 생성할 수 있습니다.

다음 표에는 다양한 조건 변수 형식이 설명되어 있습니다.

조건 변수 형식	설명
%?*V*	이 조건 변수는 %*V* 변수의 출력이 비어 있지 않은 경우 TRUE로 평가됩니다.
%!*V*	다음 조건을 나타냅니다. `else` %?*V* 조건 변수와 함께 사용합니다.
%#*V*	다음 조건을 나타냅니다. `endif` %?*V* 조건 변수와 함께 사용합니다.

예를 들어, 다음 텍스트는 %R을 조건 변수로 사용하여 재인증이 제공되는지 여부를 확인하고 %r을 일반 변수로 사용하여 재인증 URL을 제공하는 HTML 코드의 일부입니다.

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'"
id="Reauth" value="Login as different user...">
  </form>
</div>
%#R
```

알림 HTML 파일을 맞춤화하기 위한 변수에 포함된 모든 변수를 조건 변수로 사용할 수 있습니다. 그러나 조건문에서 사용하기에 가장 적합한 변수는 서버 응답 대신에 *클라이언트 요청*과 관련된 변수와 항상 TRUE로 평가되는 변수 대신 TRUE로 평가될 수도 있고 그렇지 않을 수도 있는 변수입니다.

알림 HTML 파일을 맞춤화하기 위한 변수

알림 HTML 파일에서 변수를 사용하여 사용자에게 특정 정보를 표시할 수 있습니다. 또한 각 변수를 조건 변수로 변환하여 if-then 문을 생성할 수 있습니다. 자세한 내용은 알림 HTML 파일에서 변수 사용, 17-13페이지를 참고하십시오.

변수	설명	조건 변수로 사용된 경우 항상 TRUE로 평가되는지 여부
%a	FTP에 대한 인증 영역	아니요
%A	ARP 주소	예
%b	사용자 에이전트 이름	아니요
%B	BLOCK-SRC 또는 BLOCK-TYPE과 같은 차단 이유	아니요

변수	설명	조건 변수로 사용된 경우 항상 TRUE로 평가되는지 여부
%c	오류 페이지 담당자	예
%C	전체 Set-Cookie: 헤더 행 또는 빈 문자열	아니요
%d	클라이언트 IP 주소	예
%D	사용자 이름	아니요
%e	오류 페이지 이메일 주소	예
%E	오류 페이지 로고 URL	아니요
%f	사용자 피드백 섹션	아니요
%F	사용자 피드백 URL	아니요
%g	웹 카테고리 이름(사용 가능한 경우)	예
%G	허용되는 최대 파일 크기(MB)	아니요
%h	프록시의 호스트 이름	예
%H	URL의 서버 이름	예
%i	16진수로 된 트랜잭션 ID	예
%I	Management IP Address	예
%j	URL 카테고리 경고 페이지 맞춤형 텍스트	아니요
%k	최종 사용자 승인 페이지 및 최종 사용자 URL 필터링 경고 페이지에 대한 리디렉션 링크	아니요
%K	응답 파일 유형	아니요
%l	WWW-Authenticate: 헤더 행	아니요
%L	Proxy-Authenticate: 헤더 행	아니요
%M	요청 메서드(예: "GET" 또는 "POST")	예
%n	악성코드 카테고리 이름(사용 가능한 경우)	아니요
%N	멀웨어 위협 이름(사용 가능한 경우)	아니요
%o	웹 평판 위협 유형(사용 가능한 경우)	아니요
%O	웹 평판 위협 이유(사용 가능한 경우)	아니요
%p	Proxy-Connection HTTP 헤더 문자열	예
%P	프로토콜	예
%q	ID 정책 그룹 이름	예
%Q	비ID 정책의 정책 그룹 이름	예
%r	Redirect URL	아니요
%R	재인증이 제공됩니다. 이 변수는 false인 경우 비어 있는 문자열을 출력하고 true인 경우 공백을 출력하므로 단독으로 사용하기에 적합하지 않습니다. 대신 조건 변수로 사용합니다.	아니요
%S	프록시의 시그니처	아니요, 항상 FALSE로 평가됨
%t	UNIX 초 및 밀리초 단위의 타임스탬프	예
%T	날짜	예

변수	설명	조건 변수로 사용된 경우 항상 TRUE로 평가되는지 여부
%u	URL의 URI 부분(서버 이름을 제외한 URL)	예
%U	요청의 전체 URL	예
%v	HTTP 프로토콜 버전	예
%W	관리 WebUI 포트	예
%X	확장된 차단 코드. 액세스 로그에 기록된 대부분의 웹 평판 및 안티멀웨어 정보(예: ACL 결정 태그 및 WBRS 점수)를 인코딩하는 16바이트 base64 값입니다.	예
%Y	설정된 경우 관리자가 맞춤화한 텍스트 문자열, 그렇지 않으면 비어 있음	아니요
%y	최종 사용자 승인 페이지 맞춤형 텍스트	예
%z	웹 평판 점수	예
%Z	DLP 메타 데이터	예
%%	알림 페이지에 퍼센트 기호(%)를 인쇄합니다.	해당 없음

알림 페이지 유형

기본적으로 웹 프록시는 차단되었다는 사실과 차단 이유를 사용자에게 알리는 알림 페이지를 표시합니다.

대부분의 알림 페이지는 관리자 또는 Cisco 고객 지원에서 잠재적인 문제를 트러블슈팅하는 데 도움이 될 수 있는 다른 코드 집합을 표시합니다. 일부 코드는 Cisco 내부 전용입니다. 알림 페이지에 표시될 수 있는 다른 코드는 알림 HTML 파일을 맞춤화하기 위한 변수에 표시된 대로 맞춤화된 알림 페이지에 포함할 수 있는 변수와 동일합니다.

다음 표에는 사용자가 발견할 수 있는 여러 알림 페이지가 설명되어 있습니다.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_ACCEPTED 피드백이 수락되었습니다. 감사합니다	사용자가 "Report Misclassification(오분류 보고)" 옵션을 사용한 후 표시되는 알림 페이지입니다.	오분류 보고서를 전송했습니다. 소중한 의견에 감사드립니다.
ERR_ADAPTIVE_SECURITY 정책: 일반	적응형 스캐닝 기능으로 인해 사용자가 차단될 때 표시되는 차단 페이지입니다.	조직의 보안 정책에 따라 해당 콘텐츠가 보안 위협으로 판별되었기 때문에 이 웹 사이트 <*URL*>이(가) 차단되었습니다.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_ADULT_CONTENT 정책 승인	최종 사용자가 성인 콘텐츠로 분류된 페이지에 액세스할 때 표시되는 경고 페이지입니다. 사용자가 승인 링크를 클릭하여 원래 요청된 사이트로 계속 진행할 수 있습니다.	노골적이거나 성인 등급이 지정된 콘텐츠가 포함된 웹 페이지를 방문하려고 합니다. 아래 링크를 클릭하면 이러한 유형의 콘텐츠에 대한 인터넷 사용을 제어하는 조직의 정책을 읽었으며 해당 정책에 동의함을 승인하는 것이 됩니다. 탐색 행적에 대한 데이터가 모니터링 및 기록될 수 있습니다. 이러한 종류의 웹 페이지에 계속 접속하려면 주기적으로 이 내용을 승인하라는 요청을 받게 됩니다. 이 내용을 수락하고 인터넷에 접속하려면 여기를 클릭하십시오.
ERR_AVC 정책: 애플리케이션 제어	사용자가 AVC(Application Visibility and Control) 엔진으로 인해 차단된 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 %2 유형의 %1 애플리케이션에 대한 액세스가 차단되었습니다.
ERR_BAD_REQUEST 잘못된 요청	유효하지 않은 트랜잭션 요청으로 인해 발생하는 오류 페이지입니다.	시스템에서 이 요청을 처리할 수 없습니다. 비표준 브라우저에서 유효하지 않은 HTTP 요청을 생성했을 수 있습니다. 표준 브라우저를 사용하는 경우 요청을 다시 시도하십시오.
ERR_BLOCK_DEST 정책: 대상	사용자가 차단된 웹 사이트 주소에 액세스하려고 시도하는 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 이 웹 사이트 <*URL*>에 대한 액세스가 차단되었습니다.
ERR_BROWSER 보안: 브라우저	트랜잭션 요청이 악성코드 또는 스파이웨어로 인해 유해한 것으로 식별된 애플리케이션에서 생성되는 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 해당 컴퓨터의 요청이 조직의 네트워크에 대해 보안 위협으로 판별되었기 때문에 이 요청이 차단되었습니다. 브라우저가 "<*malware name*>"(으)로 식별된 악성코드/스파이웨어 에이전트에 의해 손상되었을 수 있습니다. <*contact name*> <*email address*>에 문의하고 아래 표시된 코드를 제공하십시오. 비표준 브라우저를 사용 중이고 분류가 잘못되었다고 판단되면 아래 버튼을 사용하여 이 오분류를 보고합니다.
ERR_BROWSER_CUSTOM 정책: 브라우저	트랜잭션 요청이 차단된 사용자 에이전트에서 생성되는 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 브라우저의 요청이 차단되었습니다. 이 브라우저 "<*browser type*>"이(가) 잠재적인 보안 위험으로 인해 허용되지 않습니다.
ERR_CERT_INVALID 유효하지 않은 인증서	요청된 HTTPS 사이트가 유효하지 않은 인증서를 사용하는 경우 표시되는 차단 페이지입니다.	사이트 <*hostname*>에서 유효하지 않은 인증서를 제공했으므로 보안 세션을 설정할 수 없습니다.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_CONTINUE_UNACKNOWLEDGED 정책 승인	사용자가 경고 조치가 할당된 맞춤형 URL 카테고리에 있는 사이트를 요청하는 경우 표시되는 경고 페이지입니다. 사용자가 승인 링크를 클릭하여 원래 요청된 사이트로 계속 진행할 수 있습니다.	URL 카테고리 <*URL category*>에 속하는 웹 페이지를 방문하려고 합니다. 아래 링크를 클릭하면 이러한 유형의 콘텐츠에 대한 인터넷 사용을 제어하는 조직의 정책을 읽었으며 해당 정책에 동의함을 승인하는 것이 됩니다. 탐색 행적에 대한 데이터가 모니터링 및 기록될 수 있습니다. 이러한 종류의 웹 페이지에 계속 접속하려면 주기적으로 이 내용을 승인하라는 요청을 받게 됩니다. 이 내용을 수락하고 인터넷에 접속하려면 여기를 클릭하십시오.
ERR_DNS_FAIL DNS 오류	요청된 URL에 유효하지 않은 도메인 이름이 포함된 경우 표시되는 오류 페이지입니다.	이 호스트 이름 <*hostname*>에 대한 호스트 이름 확인(DNS 검색)에 실패했습니다. 인터넷 주소가 잘못 입력되거나 더 이상 사용되지 않는 것이거나, 호스트 <*hostname*>이(가) 일시적으로 사용 불가능하거나, DNS 서버가 응답할 수 없는 상태일 수 있습니다. 인터넷 주소를 정확하게 입력했는지 확인하십시오. 주소가 정확한 경우 나중에 이 요청을 다시 시도하십시오.
ERR_EXPECTATION_FAILED 예상 실패	트랜잭션 요청이 HTTP 417 "예상 실패" 응답을 트리거하는 경우 표시되는 오류 페이지입니다.	시스템에서 이 사이트 <*URL*>에 대한 요청을 처리할 수 없습니다. 비표준 브라우저에서 유효하지 않은 HTTP 요청을 생성했을 수 있습니다. 표준 브라우저를 사용하는 경우 요청을 다시 시도하십시오.
ERR_FILE_SIZE 정책: 파일 크기	요청된 파일이 허용된 최대 파일 크기보다 큰 경우에 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 다운로드 크기가 허용되는 제한을 초과하므로 이 웹 사이트 또는 다운로드 <*URL*>에 대한 액세스가 차단되었습니다.
ERR_FILE_TYPE 정책: 파일 유형	요청된 파일이 차단된 파일 유형인 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 파일 유형 "<*file type*>"은(는) 허용되지 않으므로 이 웹 사이트 또는 다운로드 <*URL*>에 대한 액세스가 차단되었습니다.
ERR_FILTER_FAILURE 필터 오류	URL 필터링 엔진이 일시적으로 URL 필터링 응답을 전달할 수 없고 "연결할 수 없는 서비스에 대한 기본 조치" 옵션이 차단으로 설정된 경우 표시되는 오류 페이지입니다.	현재 내부 서버에 연결할 수 없거나 서버가 과부하 상태이므로 <*URL*> 페이지에 대한 요청이 거부되었습니다. 나중에 다시 요청을 시도하십시오.
ERR_FOUND 발견	일부 오류에 대한 내부 리디렉션 페이지입니다.	<*URL*> 페이지가 <*redirected URL*>(으)로 리디렉션되고 있습니다.
ERR_FTP_ABORTED FTP가 중단됨	FTP over HTTP 트랜잭션 요청이 HTTP 416 "요청된 범위를 충족할 수 없음" 응답을 트리거하는 경우 표시되는 오류 페이지입니다.	<*URL*> 파일에 대한 요청에 실패했습니다. FTP 서버 <*hostname*>에서 예기치 않게 연결을 종료했습니다. 나중에 다시 요청을 시도하십시오.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_FTP_AUTH_REQUIRED FTP 권한 필요	FTP over HTTP 트랜잭션 요청이 FTP 530 "로그인되지 않음" 응답을 트리거하는 경우 표시되는 오류 페이지입니다.	FTP 서버 <*hostname*>에서 인증해야 합니다. 프롬프트가 표시되면 유효한 사용자 ID와 암호를 입력해야 합니다. 경우에 따라 FTP 서버에서 익명 접속의 수를 제한할 수도 있습니다. 평소 이 서버에 익명 사용자로 접속했었다면 나중에 다시 시도하십시오.
ERR_FTP_CONNECTION_FAILED FTP 연결 실패	FTP over HTTP 트랜잭션 요청이 FTP 425 "데이터 연결을 열 수 없음" 응답을 트리거하는 경우 표시되는 오류 페이지입니다.	시스템이 FTP 서버 <*hostname*>와(과) 통신할 수 없습니다. FTP 서버가 일시적으로나 영구적으로 다운되었을 수도 있고, 네트워크 문제로 인해 서버에 연결하지 못하는 것일 수도 있습니다. 주소를 정확하게 입력했는지 확인하십시오. 주소가 정확한 경우 나중에 이 요청을 다시 시도하십시오.
ERR_FTP_FORBIDDEN FTP가 금지됨	FTP over HTTP 트랜잭션 요청이 사용자의 액세스가 허용되지 않는 개체에 해당하는 경우 표시되는 오류 페이지입니다.	FTP 서버 <*hostname*>에서 액세스를 거부했습니다. 사용자 ID는 이 문서에 접속할 수 있는 권한이 없습니다.
ERR_FTP_NOT_FOUND FTP를 찾을 수 없음	FTP over HTTP 트랜잭션 요청이 서버에 없는 개체에 해당하는 경우 표시되는 오류 페이지입니다.	<*URL*> 파일을 찾을 수 없습니다. 주소가 올바르지 않거나 더 이상 사용되지 않습니다.
ERR_FTP_SERVER_ERR FTP 서버 오류	FTP를 지원하는 서버에 액세스하려고 시도하는 FTP over HTTP 트랜잭션에 대해 표시되는 오류 페이지입니다. 일반적으로 서버에서 HTTP 501 "구현되지 않음" 응답을 반환합니다.	시스템이 FTP 서버 <*hostname*>와(과) 통신할 수 없습니다. FTP 서버가 일시적으로나 영구적으로 다운되었을 수도 있고 이 서비스를 제공하지 않을 수도 있습니다. 주소가 정확한지 확인하십시오. 주소가 정확한 경우 나중에 이 요청을 다시 시도하십시오.
ERR_FTP_SERVICE_UNAVAIL FTP 서비스 사용 불가능	사용 불가능한 FTP 서버에 액세스하려고 시도하는 FTP over HTTP 트랜잭션에 대해 표시되는 오류 페이지입니다.	시스템이 FTP 서버 <*hostname*>와(과) 통신할 수 없습니다. FTP 서버가 다른 작업으로 분주하거나 영구적으로 다운되었을 수도 있고 이 서비스를 제공하지 않을 수도 있습니다. 주소가 정확한지 확인하십시오. 주소가 정확한 경우 나중에 이 요청을 다시 시도하십시오.
ERR_GATEWAY_TIMEOUT 게이트웨이 시간 초과	요청된 서버가 적절한 시간 내에 응답하지 않은 경우 표시되는 오류 페이지입니다.	시스템이 외부 서버 <*hostname*>와(과) 통신할 수 없습니다. 인터넷 서버가 다른 작업으로 분주하거나 영구적으로 다운되었을 수도 있고 네트워크 문제로 인해 연결되지 못하는 것일 수도 있습니다. 인터넷 주소를 정확하게 입력했는지 확인하십시오. 주소가 정확한 경우 나중에 이 요청을 다시 시도하십시오.
ERR_IDS_ACCESS_FORBIDDEN IDS 액세스가 금지됨	사용자가 구성된 Cisco 데이터 보안 정책으로 인해 차단된 파일을 업로드하려고 시도할 때 표시되는 차단 페이지입니다.	조직의 데이터 전송 정책에 따라 업로드 요청이 차단되었습니다. 파일 세부사항: <*파일 세부사항*>

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_INTERNAL_ERROR Internal Error	내부 오류가 발생하는 경우 표시되는 오류 페이지입니다.	<*URL*> 페이지에 대한 요청을 처리할 때 내부 시스템 오류가 발생했습니다. 이 요청을 다시 시도하십시오. 이 상태가 지속되는 경우 <*contact name*> <*email address*>에 문의하여 아래 표시된 코드를 제공하십시오.
ERR_MALWARE_SPECIFIC 보안: 악성코드가 탐지됨	파일을 다운로드할 때 악성코드가 탐지된 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 이 웹 사이트 <*URL*>이(가) 컴퓨터 또는 조직의 네트워크에 대한 보안 위협으로 판별되었기 때문에 차단되었습니다. 이 사이트에서 <*malware category*> 카테고리의 악성코드 <*malware name*>이(가) 발견되었습니다.
ERR_MALWARE_SPECIFIC_OUTGOING 보안: 악성코드가 탐지됨	파일을 업로드할 때 악성코드가 탐지된 경우 표시되는 차단 페이지입니다.	조직의 정책에 따라 파일이 수신자의 네트워크 보안에 유해한 악성코드를 포함하는 것으로 탐지되었으므로 URL(<*URL*>)로의 파일 업로드가 차단되었습니다. 악성코드 이름: <*malware name*> 악성코드 카테고리: <*malware category*>
ERR_NATIVE_FTP_DENIED	네이티브 FTP 트랜잭션이 차단된 경우 네이티브 FTP 클라이언트에 표시되는 차단 메시지입니다.	530 로그인 거부됨
ERR_NO_MORE_FORWARDS 추가 전달 없음	어플라이언스가 웹 프록시와 네트워크의 다른 프록시 서버 간의 정방향 루프를 탐지한 경우 표시되는 오류 페이지입니다. 웹 프록시가 루프를 중단하고 이 메시지를 클라이언트에 표시합니다.	<*URL*> 페이지에 대한 요청에 실패했습니다. 서버 주소 <*hostname*>이(가) 유효하지 않을 수도 있고, 이 서버에 액세스하려면 포트 번호를 지정해야 할 수도 있습니다.
ERR_POLICY 정책: 일반	정책 설정으로 인해 요청이 차단된 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 이 웹 사이트 <*URL*>에 대한 액세스가 차단되었습니다.
ERR_PROTOCOL 정책: 프로토콜	사용된 프로토콜에 따라 요청이 차단된 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 데이터 전송 프로토콜 "<*protocol type*>"은(는) 허용되지 않으므로 이 요청이 차단되었습니다.
ERR_PROXY_AUTH_REQUIRED 프록시 권한 필요	계속하려면 사용자가 인증 자격 증명을 입력해야 하는 경우 표시되는 알림 페이지입니다. 이는 명시적 트랜잭션 요청에 사용됩니다.	이 시스템을 사용하여 인터넷에 접속하려면 인증이 필요합니다. 프롬프트가 표시되면 유효한 사용자 ID와 암호를 입력해야 합니다.
ERR_PROXY_PREVENT_MULTIPLE_LOGIN 다른 컴퓨터에서 이미 로그인됨	이미 다른 컴퓨터에서 웹 프록시에 인증된 사용자 이름과 동일한 사용자 이름을 사용하여 웹에 액세스하려고 시도할 때 표시되는 차단 페이지입니다. 사용자 세션 제한 전역 인증 옵션이 사용하도록 설정된 경우 사용됩니다.	다른 IP 주소에서 이 사용자 ID를 사용하여 활성화된 세션이 있으므로 조직의 정책에 따라 인터넷 액세스 요청이 거부되었습니다. 다른 사용자로 로그인하려면 아래 버튼을 클릭하고 다른 사용자 이름과 암호를 입력하십시오.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_PROXY_REDIRECT 리디렉션	리디렉션 페이지입니다.	이 요청은 리디렉션되고 있습니다. 이 페이지가 자동으로 리디렉션되지 않으면 여기를 클릭하여 계속 진행하십시오.
ERR_PROXY_UNACKNOWLEDGED 정책 승인	최종 사용자 승인 페이지입니다. 자세한 내용은 최종 사용자 알림 페이지, 17-5페이지를 참고하십시오.	인터넷에 액세스하기 전에 다음 내용을 승인하십시오. 위험한 콘텐츠를 탐지하고 조직의 정책을 적용하기 위해 웹 트랜잭션이 자동으로 모니터링 및 처리됩니다. 아래 링크를 클릭하면 이러한 모니터링을 승인하는 것은 물론, 방문하는 사이트에 대한 데이터가 기록될 수 있음을 인정하는 것입니다. 또한 주기적으로 모니터링 시스템의 존재를 승인하도록 요청받게 됩니다. 여러분은 다음과 같은 조직의 인터넷 액세스 정책에 대해 책임이 있습니다. 이 내용을 수락하고 인터넷에 접속하려면 여기를 클릭하십시오.
ERR_PROXY_UNLICENSED 프록시 라이센스가 없음	웹 보안 어플라이언스 웹 프록시에 대한 유효한 라이센스 키가 없는 경우 표시되는 차단 페이지입니다.	보안 장치에 대한 적절한 라이센스가 없어 인터넷에 접속할 수 없습니다. <*contact name*> <*email address*>에 문의하고 아래 표시된 코드를 제공하십시오. **참고** 보안 디바이스의 관리 인터페이스에 액세스하려면 구성된 IP 주소를 포트와 함께 입력하십시오.
ERR_RANGE_NOT_SATISFIABLE 범위를 충족할 수 없음	웹 서버에서 요청된 바이트 범위를 충족할 수 없는 경우 표시되는 오류 페이지입니다.	시스템에서 이 요청을 처리할 수 없습니다. 비표준 브라우저에서 유효하지 않은 HTTP 요청을 생성했을 수 있습니다. 표준 브라우저를 사용하는 경우 요청을 다시 시도하십시오.
ERR_REDIRECT_PERMANENT 영구 리디렉션	내부 리디렉션 페이지입니다.	<*URL*> 페이지가 <*redirected URL*>(으)로 리디렉션되고 있습니다.
ERR_REDIRECT_REPEAT_REQUEST 리디렉션	내부 리디렉션 페이지입니다.	요청을 반복하십시오.
ERR_SAAS_AUTHENTICATION 정책: 액세스 거부됨	계속하려면 사용자가 인증 자격 증명을 입력해야 하는 경우 표시되는 알림 페이지입니다. 이 페이지는 애플리케이션에 액세스하기 위해 사용됩니다.	조직의 정책에 따라 <*URL*> 액세스 요청이 사용자가 로그인 자격 증명을 입력해야 하는 페이지로 리디렉션되었습니다. 인증에 성공하고 적절한 권한이 있는 경우 애플리케이션에 액세스할 수 있습니다.

파일 이름 및 알림 제목	알림 설명	알림 텍스트
ERR_SAAS_AUTHORIZATION 정책: 액세스 거부됨	사용자가 액세스할 권한이 없는 애플리케이션에 액세스하려고 시도하는 경우 표시되는 차단 페이지입니다.	조직의 정책에 따라 권한 있는 사용자가 아니므로 애플리케이션 <*URL*>에 대한 액세스가 차단됩니다. 다른 사용자로 로그인하려면 이 애플리케이션에 액세스할 수 있는 권한이 있는 사용자의 다른 사용자 이름과 암호를 입력합니다.
ERR_SAML_PROCESSING 정책: 액세스 거부됨	내부 프로세스가 애플리케이션에 액세스하기 위해 단일 로그인 URL을 처리하려는 시도에 실패하는 경우 표시되는 오류 페이지입니다.	단일 로그인 요청 프로세스 중에 오류가 발견되었으므로 <*user name*> 액세스 요청이 진행되지 않았습니다.
ERR_SERVER_NAME_EXPANSION 서버 이름 확장	자동으로 URL을 확장하고 사용자를 업데이트된 URL로 리디렉션하는 내부 리디렉션 페이지입니다.	서버 이름 <*hostname*>이(가) 약어이므로 <*redirected URL*>(으)로 리디렉션되고 있습니다.
ERR_URI_TOO_LONG URL이 너무 김	URL 길이가 너무 긴 경우 표시되는 차단 페이지입니다.	요청한 URL이 너무 길어 처리하지 못했습니다. 네트워크에 대한 공격을 의미할 수도 있습니다. <*contact name*> <*email address*>에 문의하고 아래 표시된 코드를 제공하십시오.
ERR_WBRS 보안: 악성코드 위험	낮은 웹 평판 점수로 인해 웹 평판 필터에서 사이트를 차단할 때 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 웹 평판 필터에서 컴퓨터 또는 조직의 네트워크에 대한 보안 위협으로 판별되었기 때문에 이 웹 사이트 <*URL*>이(가) 차단되었습니다. 이 웹 사이트는 맬웨어/스파이웨어와 관련되어 있습니다. 위협 유형: %o 위협 사유: %O
ERR_WEBCAT 정책: URL 필터링	사용자가 차단된 URL 카테고리의 웹 사이트에 액세스하려고 시도하는 경우 표시되는 차단 페이지입니다.	조직의 액세스 정책에 따라 웹 카테고리 "<*category type*>"이(가) 허용되지 않으므로 이 웹 사이트 <*URL*>에 대한 액세스가 차단되었습니다.
ERR_WWW_AUTH_REQUIRED WWW 권한 필요	요청된 서버에서 계속하려면 사용자가 자격 증명을 입력해야 하는 경우 표시되는 알림 페이지입니다.	요청된 웹 사이트 <*hostname*>에 액세스하려면 인증이 필요합니다. 프롬프트가 표시되면 유효한 사용자 ID와 암호를 입력해야 합니다.

18장

최종 사용자 활동을 모니터링하기 위한 보고서 생성

- 보고 개요, 18-1페이지
- Reporting(보고) 탭 사용, 18-2페이지
- 중앙 집중식 보고 사용, 18-7페이지
- 보고서 예약, 18-7페이지
- 온디맨드 보고서 생성, 18-9페이지
- 아카이브된 보고서, 18-9페이지

보고 개요

웹 보안 어플라이언스는 네트워크에서 발생하는 상황을 이해하고 특정 도메인, 사용자 또는 카테고리에 대한 트래픽 세부사항을 볼 수 있는 높은 수준의 보고서를 생성합니다. 보고서를 실행하여 특정 기간 동안의 시스템 활동에 대한 대화형 표시를 볼 수도 있고 보고서를 예약하여 일정한 간격으로 실행할 수도 있습니다.

관련 주제

- 보고서 페이지에서 보고서 인쇄 및 내보내기, 18-6페이지

보고서의 사용자 이름에 대한 작업

인증을 사용하도록 설정하면 사용자가 웹 프록시에 인증할 때 보고서에 사용자 이름별로 사용자가 나열됩니다. 기본적으로 사용자 이름은 인증 서버에 표시되는 대로 작성됩니다. 그러나 모든 보고서에서 사용자 이름을 인식 불가능하게 설정하도록 선택할 수 있습니다.

참고 관리자는 항상 보고서에서 사용자 이름을 볼 수 있습니다.

1단계 **Security Services(보안 서비스) > Reporting(보고)**을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 Local Reporting(로컬 보고) 아래에서 **Anonymize usernames in reports(보고서에서 사용자 이름 익명 처리)**를 선택합니다.

3단계 **변경 사항을** 제출 및 **커밋합니다**.

Report(보고서) 페이지

웹 보안 어플라이언스에서는 다음과 같은 보고서를 제공합니다.

- 개요
- 사용자
- 웹 사이트
- URL 범주
- 애플리케이션 가시성
- 안티맬웨어
- 클라이언트 악성프로그램 위험
- 웹 신뢰도 필터
- 레이어-4 트래픽 모니터
- 사용자 위치별 보고서
- 웹 추적
- 시스템 용량
- 시스템 상태

Reporting(보고) 탭 사용

Reporting(보고) 탭은 시스템 데이터를 보기 위한 여러 옵션을 제공합니다. 보고서 페이지는 시스템 활동의 개요를 제공하고 시스템 데이터를 보기 위한 여러 옵션을 지원합니다. 각 페이지에서 웹 사이트 및 클라이언트별 데이터를 검색할 수도 있습니다.

Reporting(보고) 탭에서 대부분의 보고서에 대해 다음 작업을 수행할 수 있습니다.

옵션	작업 링크
보고서에 표시되는 시간 범위 변경	시간 범위 변경, 18-3페이지
특정 클라이언트 및 도메인 검색	데이터 검색, 18-3페이지
차트에 표시할 데이터 선택	차트에 표시할 데이터 선택, 18-4페이지
열 선택 및 정렬	관련 주제, 18-4페이지
보고서를 외부 파일로 내보내기	보고서 페이지에서 보고서 인쇄 및 내보내기, 18-6페이지

시간 범위 변경

Time Range(시간 범위) 필드를 사용하여 각 보안 구성 요소에 대해 표시되는 데이터를 업데이트할 수 있습니다. 이 옵션을 사용하여 미리 정의된 시간 범위에 대한 업데이트를 생성하고 특정 시작 시간에서 특정 종료 시간까지의 맞춤형 시간 범위를 정의할 수 있습니다.

참고 사용자가 선택하는 시간 범위는 Time Range(시간 범위) 메뉴에서 다른 값을 선택할 때까지 모든 보고서 페이지에서 사용됩니다.

시간 범위	데이터가 반환되는 시간
시	총 60분, 최대 추가 5분 포함
교육일	지난 24시간 동안 1시간 간격, 현재 부분 시간 포함
주	지난 7일 동안 1일 간격, 현재 1일 중 일부 포함
월(30일)	지난 30일 동안 1일 간격, 현재 1일 중 일부 포함
과거	웹 보안 어플라이언스에 정의된 시간대를 사용하는 지난 24시간(00:00 ~ 23:59)
사용자 지정 범위	사용자가 정의하는 맞춤형 시간 범위입니다. Custom Range(맞춤형 범위)를 선택하면 시작 및 종료 시간을 입력할 수 있는 대화 상자가 표시됩니다.

참고 모든 보고서는 GMT(Greenwich Mean Time) 차감 시간으로 표시되는 시스템에 구성된 시간대를 기준으로 날짜 및 시간 정보를 표시합니다. 그러나 데이터 내보내기에서는 전 세계의 여러 시간대로 된 여러 시스템을 수용할 수 있도록 GMT로 시간을 표시합니다.

데이터 검색

일부 보고서에는 특정 데이터 포인트를 검색할 수 있는 필드가 포함되어 있습니다. 데이터를 검색할 때 보고서에서 검색 중인 특정 데이터 집합에 대한 보고서 데이터를 세분화합니다. 입력하는 문자열과 정확히 일치하는 값 또는 입력하는 문자열로 시작하는 값을 검색할 수 있습니다. 다음 보고서 페이지에 검색 필드가 포함됩니다.

검색 필드	설명
사용자	사용자 이름 또는 클라이언트 IP 주소로 사용자 검색
웹 사이트	도메인 또는 서버 IP 주소로 서버 검색
URL 범주	URL 카테고리 검색
애플리케이션 가시성	AVC 엔진에서 모니터링하고 차단하는 애플리케이션 이름 검색
클라이언트 악성코드 위험	사용자 이름 또는 클라이언트 IP 주소로 사용자 검색

참고 클라이언트 사용자 ID 및 클라이언트 IP 주소를 보려면 인증을 구성해야 합니다.

차트에 표시할 데이터 선택

각 웹 보고 페이지의 기본 차트에는 자주 참조되는 데이터가 표시되지만 대신 다른 데이터를 차트에 표시하도록 선택할 수 있습니다. 페이지에 여러 차트가 있는 경우 각 차트를 변경할 수 있습니다. 차트 옵션은 보고서에 있는 표의 열 제목과 동일합니다.

1단계 차트 아래의 **Chart Options(차트 옵션)** 링크를 클릭합니다.

2단계 표시할 데이터를 선택합니다.

3단계 **Done(완료)**을 클릭합니다.

관련 주제

- 관련 주제, 18-4페이지

맞춤형 보고서

기존 보고서 페이지에서 차트(그래프)와 표를 조합하여 맞춤형 보고서 페이지를 생성할 수 있습니다.

하려는 작업	수행해야 할 작업
사용자 지정 보고서 페이지에 모듈 추가	참조: • 맞춤형 보고서에 추가될 수 없는 모듈, 18-5페이지. • 맞춤형 보고서 페이지 생성, 18-5페이지
사용자 지정 보고서 페이지 보기	1. **Reporting(보고) > My Reports(내 보고서)를 선택합니다.** 2. 보려는 시간 범위를 선택합니다. 선택한 시간 범위는 My Reports(내 보고서) 페이지의 모든 모듈을 포함하여 모든 보고서에 적용됩니다. 새로 추가된 모듈이 관련 섹션의 상단에 표시됩니다.
사용자 지정 보고서 페이지에서 모듈 정돈	모듈을 원하는 위치로 끌어다 놓습니다.
사용자 지정 보고서 페이지에서 모듈 삭제	모듈의 상단 우측에 있는 [X]를 클릭합니다.
PDF 또는 CSV 버전의 맞춤형 보고서를 생성합니다.	**Reporting(보고) > Archived Reports(아카이브된 보고서)**를 선택하고 **Generate Report Now(지금 보고서 생성)**를 클릭합니다.
주기적으로 PDF 또는 CSV 버전의 맞춤형 보고서를 생성합니다.	**Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택합니다.

맞춤형 보고서에 추가될 수 없는 모듈

- 웹 추적 검색 결과를 포함한 검색 결과

맞춤형 보고서 페이지 생성

시작하기 전에

- 추가하려는 모듈이 추가될 수 있는지 확인합니다. 맞춤형 보고서에 추가될 수 없는 모듈, 18-5 페이지를 참조하십시오.
- 모듈의 오른쪽 상단 모서리에 있는 **[X]**를 클릭하여 필요하지 않은 기본 모듈을 삭제합니다.

1단계 다음 방법 중 하나를 사용하여 맞춤형 보고서 페이지에 모듈을 추가합니다.

참고 일부 모듈은 이러한 방법 중 하나를 통해서만 사용할 수 있습니다. 한 가지 방법을 사용하여 모듈을 추가할 수 없는 경우 다른 방법을 시도하십시오.

- 추가하려는 모듈이 있는 보고서 페이지로 이동한 후 모듈의 상단에 있는 **[+]** 버튼을 클릭합니다.
- **Reporting(보고) > My Reports(내 보고서)**로 이동하여 섹션 중 하나의 상단에 있는 **[+]** 버튼을 클릭한 후 추가할 보고서 모듈을 선택합니다. 검색 중인 모듈을 찾기 위해 My Reports(내 보고서) 페이지의 각 섹션에서 **[+]** 버튼을 클릭해야 할 수 있습니다.

각 모듈을 한 번만 추가할 수 있습니다. 보고서에 특정 모듈을 이미 추가한 경우, 해당 추가 옵션은 사용할 수 없는 상태가 됩니다.

2단계 맞춤화한(예: 열을 추가, 삭제 또는 재정렬하거나 차트에 기본이 아닌 데이터를 표시하여) 모듈을 추가하는 경우 My Reports(내 보고서) 페이지에서 모듈을 맞춤화합니다.

모듈이 기본 설정으로 추가됩니다. 원래 모듈의 시간 범위는 유지되지 않습니다.

3단계 별도의 범례가 포함된 차트를 추가하는 경우(예: Overview(개요) 페이지의 그래프) 범례를 따로 추가합니다. 필요한 경우, 설명하는 데이터 옆으로 끌어다 놓습니다.

보고 및 추적의 하위 도메인과 두 번째 레벨 도메인 비교

보고 및 추적 검색에서 두 번째 레벨 도메인(http://george.surbl.org/two-level-tlds 에 나열된 지역 도메인)과 하위 도메인이 동일하게 표시될 수 있지만 두 도메인은 서로 다르게 처리됩니다. 예를 들면 다음과 같습니다.

- 보고서에 2-레벨 도메인(예: `co.uk`)에 대한 결과가 포함되지 않지만 `foo.co.uk`에 대한 결과는 포함됩니다. 보고서에 기본 회사 도메인(예: `cisco.com`) 아래의 하위 도메인이 포함됩니다.
- 지역 도메인 `co.uk`의 추적 검색 결과에는 `foo.co.uk`와 같은 도메인이 포함되지 않지만 `cisco.com`의 검색 결과에는 `subdomain.cisco.com`과 같은 하위 도메인이 포함됩니다.

보고서 페이지에서 보고서 인쇄 및 내보내기

페이지의 오른쪽 상단 모서리에서 **Printable PDF(인쇄 가능한 PDF)** 링크를 클릭하여 보고서 페이지의 인쇄용 PDF 버전을 생성할 수 있습니다. 또한 **Export(내보내기)** 링크를 클릭하여 원시 데이터를 CSV(Comma-Separated Value) 파일로 내보낼 수 있습니다.

CSV 내보내기에는 원시 데이터만 포함되기 때문에 백분율과 같은 계산된 데이터가 웹 기반 보고서에 표시되는 경우에도 웹 기반 보고서 페이지에서 내보낸 데이터에는 이러한 데이터가 포함되지 않을 수 있습니다.

보고서 데이터 내보내기

대부분의 보고서에는 원시 데이터를 CSV(Comma-Separated Values) 파일로 내보낼 수 있는 **Export(내보내기)** 링크가 포함되어 있습니다. 데이터를 CSV 파일로 내보낸 후 Microsoft Excel과 같은 애플리케이션을 사용하여 데이터에 액세스하여 조작할 수 있습니다.

내보낸 CSV 데이터는 웹 보안 어플라이언스의 설정과 상관없이 모든 메시지 추적 및 보고 데이터를 GMT(Greenwich Mean Time)로 표시합니다. GMT 시간 변환의 목적은 어플라이언스와 독립적으로 또는 여러 표준 시간대의 어플라이언스에서 데이터를 참조하는 시기와 독립적으로 데이터를 사용하도록 하려는 것입니다.

다음 예는 안티멀웨어 카테고리 보고서의 원시 데이터 내보내기 항목입니다. 여기서 PDT(Pacific Daylight Time)는 GMT 7시간으로 표시됩니다.

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored,
Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

카테고리 헤더	값	설명
시간 타임스탬프	1159772400.0	쿼리 시작 시간입니다(epoch 이후 초 수).
종료 타임스탬프	1159858799.0	쿼리 종료 시간입니다(epoch 이후 초 수).
시작 날짜	2006-10-02 07:00 GMT	쿼리가 시작된 날짜입니다.
종료 날짜	2006-10-03 오전 6:59 GMT	쿼리가 종료된 날짜입니다.
이름	애드웨어	악성코드 카테고리의 이름입니다.
모니터링된 트랜잭션	525	모니터링되는 트랜잭션 수입니다.
차단된 트랜잭션	2100	차단된 트랜잭션 수입니다.
발견된 트랜잭션	2625	총 트랜잭션 수: 탐지된 트랜잭션 수 + 차단된 트랜잭션 수.

참고 카테고리 헤더는 각 보고서 유형마다 다릅니다.

참고 현지화된 CSV 데이터를 내보낼 경우 일부 브라우저에서 제목이 제대로 표시되지 않을 수 있습니다. 이러한 문제는 일부 브라우저에서 현지화된 텍스트에 적절한 문자 집합을 사용하지 않기 때문에 발생할 수 있습니다. 이 문제를 해결하기 위해 파일을 로컬 머신에 저장하고 **File(파일) > Open(열기)**을 사용하여 웹 브라우저에서 파일을 열 수 있습니다. 파일을 열 때 현지화된 텍스트를 표시하기 위한 문자 집합을 선택합니다.

중앙 집중식 보고 사용

웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 웹 보안 어플라이언스에서 처리되는 웹 트래픽에 대한 보고서를 표시하는 어플라이언스를 선택할 수 있습니다. 보안 관리 어플라이언스에서 여러 웹 보안 어플라이언스를 관리하는 경우에는 중앙 집중식 보고를 사용하도록 설정할 수 있습니다.

참고 중앙 집중식 보고를 사용하도록 설정하면 시스템 용량 및 시스템 상태 보고서만 웹 보안 어플라이언스에서 사용할 수 있습니다. 다른 보고서를 보려면 보안 관리 어플라이언스에 연결합니다.

1단계 **Security Services(보안 서비스) > Reporting(보고)**을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 **Centralized Reporting(중앙 집중식 보고)**을 선택합니다.

3단계 **변경 사항을 제출** 및 **커밋합니다**.

보고서 예약

매일, 매주 또는 매월 실행되는 보고서를 예약할 수 있습니다. 전날, 지난 7일 또는 이전 달 동안의 데이터를 포함하도록 예약된 보고서를 구성할 수 있습니다.

다음 유형의 보고서에 대한 보고서를 예약할 수 있습니다.

- 개요
- 사용자
- 웹 사이트
- URL 범주
- 애플리케이션 가시성
- 안티맬웨어
- 클라이언트 악성프로그램 위험
- 웹 신뢰도 필터
- 레이어-4 트래픽 모니터
- SOCKS 프록시
- 사용자 위치별 보고서
- 시스템 용량
- My Reports(내 리포트)

예약된 보고서 추가

1단계 **Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택하고 **Add Scheduled Report(예약된 보고서 추가)**를 클릭합니다.

2단계 보고서 유형을 선택합니다.

3단계 보고서 제목을 입력합니다. 동일한 이름을 사용하는 여러 보고서를 생성하지 않으려면 설명이 포함된 제목을 사용합니다.

4단계 보고서에 포함된 데이터의 시간 범위를 선택합니다.

5단계 생성되는 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다. 또한 대부분의 보고서에서는 원시 데이터를 CSV 파일로 저장할 수 있습니다.

6단계 구성하는 보고서의 유형에 따라 포함할 행 수 및 데이터 정렬 기준 열 등의 여러 보고서 옵션을 지정할 수 있습니다. 필요에 따라 이러한 옵션을 구성합니다.

7단계 Schedule(일정) 섹션에서 매일, 매주 또는 매월 몇 시에 보고서를 실행할지를 선택합니다.

8단계 Email(이메일) 필드에 생성된 보고서를 전송할 이메일 주소를 입력합니다.

이메일 주소를 지정하지 않으면 보고서 아카이브만 실행됩니다.

9단계 **변경 사항을 제출** 및 **커밋합니다**.

예약된 보고서 편집

1단계 **Reporting(보고) > Scheduled Reports(예약된 보고서)를 선택합니다.**

2단계 목록에서 보고서 제목을 선택합니다.

3단계 설정을 수정합니다.

4단계 **변경 사항을** 제출 및 **커밋합니다**.

예약된 보고서 삭제

1단계 **Reporting(보고) > Scheduled Reports(예약된 보고서)**를 선택합니다.

2단계 삭제할 보고서에 해당하는 확인란을 선택합니다.

3단계 예약된 보고서를 모두 제거하려면 All(모두) 확인란을 선택합니다.

4단계 **변경 사항을** 삭제 **및 커밋합니다**.

참고 삭제된 보고서의 아카이브된 버전은 삭제되지 않습니다.

온디맨드 보고서 생성

1단계 **Reporting(보고) > Archived Reports(아카이브된 보고서)**를 선택합니다.

2단계 **Generate Report Now(지금 보고서 생성)**를 클릭합니다.

3단계 보고서 유형을 선택하고 제목을 편집합니다.

4단계 보고서에 포함된 데이터의 시간 범위를 선택합니다.

5단계 생성되는 보고서의 형식을 선택합니다.

기본 형식은 PDF입니다. 또한 대부분의 보고서에서는 원시 데이터를 CSV 파일로 저장할 수 있습니다.

6단계 구성하는 보고서의 유형에 따라 포함할 행 수 및 데이터 정렬 기준 열 등의 여러 보고서 옵션을 지정할 수 있습니다. 필요에 따라 이러한 옵션을 구성합니다.

7단계 보고서를 아카이브할지 여부를 선택합니다(아카이브할 경우 보고서가 Archived Reports(아카이브된 보고서) 페이지에 표시됨).

8단계 보고서를 이메일로 전송할지 여부를 지정하고 수신자의 이메일 주소를 나열합니다.

9단계 **Deliver this Report(이 보고서 전달)**를 클릭하여 보고서를 생성합니다.

10단계 **변경 사항을 커밋합니다**.

아카이브된 보고서

Reporting(보고) > Archived Reports(아카이브된 보고서) 페이지에는 사용 가능한 아카이브된 보고서가 나열됩니다. Report Title(보고서 제목) 열의 보고서 이름은 대화형이며 각 보고서의 보기에 대한 링크입니다. Show(표시) 메뉴는 나열되는 보고서의 유형을 필터링합니다. 대화형 열 제목을 사용하여 각 열의 데이터를 정렬할 수 있습니다.

어플라이언스는 각 예약된 보고서(최대 1000개의 보고서)의 인스턴스를 최대 12개 저장합니다. 아카이브된 보고서는 어플라이언스의 `/periodic_reports` 디렉토리에 저장됩니다. 아카이브된 보고서는 자동으로 삭제됩니다. 새 보고서가 추가되면 1000개 개수를 유지하기 위해 이전 보고서가 제거됩니다. 인스턴스를 12개로 제한하는 내용은 동일한 이름과 시간 범위를 사용하는 각 예약된 보고서에 적용됩니다.

19장

Web Security Appliance 보고서

- Overview(개요) 페이지, 19-2페이지
- Users(사용자) 페이지, 19-3페이지
- Web Sites(웹 사이트) 페이지, 19-4페이지
- URL Categories(URL 카테고리) 페이지, 19-4페이지
- Application Visibility(애플리케이션 가시성) 페이지, 19-5페이지
- Anti-Malware(안티멀웨어) 페이지, 19-5페이지
- Advanced Malware Protection 페이지, 19-6페이지
- File Analysis(파일 분석) 페이지, 19-6페이지
- AMP Verdict Updates(AMP 판정 업데이트) 페이지, 19-6페이지
- Client Malware Risk(클라이언트 악성코드 위험) 페이지, 19-6페이지
- Web Reputation Filters(웹 평판 필터) 페이지, 19-7페이지
- L4 Traffic Monitor(L4 트래픽 모니터) 페이지, 19-8페이지
- SOCKS Proxy(SOCKS 프록시) 페이지, 19-8페이지
- Reports by User Location(사용자 위치별 보고서) 페이지, 19-8페이지
- Web Tracking(웹 추적) 페이지, 19-9페이지
- System Capacity(시스템 용량) 페이지, 19-12페이지
- System Status(시스템 상태) 페이지, 19-13페이지

Overview(개요) 페이지

Reporting(보고) > Overview(개요) 페이지는 웹 보안 어플라이언스에 대한 활동의 개요를 제공합니다. 여기에는 웹 보안 어플라이언스에서 처리되는 웹 트래픽에 대한 그래프 및 요약 표가 포함됩니다.

시스템 개요

섹션	설명
웹 프록시 트래픽 특성	지난 1분 동안의 초당 평균 트랜잭션 수, 지난 1분 동안의 평균 대역폭(bps), 지난 1분 동안의 평균 응답 시간(ms) 및 총 현재 연결 수의 목록입니다.
시스템 리소스 사용률	현재 전체 CPU 로드, RAM 및 보고/로깅 디스크 사용률의 목록입니다. System Status(시스템 상태) 페이지로 전환하려면 System Status Details(시스템 상태 세부사항)를 클릭합니다(자세한 내용은 System Status(시스템 상태) 페이지, 19-13페이지 참조). **참고** 이 페이지에 표시된 CPU 사용률 값과 시스템 상태 페이지에 표시된 CPU 값은 다른 순간에 개별적으로 읽혀지므로 약간 다를 수 있습니다.

시간 범위 기반 카테고리 및 요약

섹션	설명
시간 범위: 다음 섹션에 표시되는 데이터에 대한 시간 범위를 선택합니다. 옵션은 Hour(시간), Day(일), Week(주), 30 Days(30일), Yesterday(어제) 또는 Custom Range(맞춤형 범위)입니다.	
총 웹 프록시 작업	(웹 프록시) 활동이 발생한 대략적인 날짜(가로 타임라인)와 실제 트랜잭션 수(세로 눈금)를 표시합니다.
웹 프록시 요약	의심되는 웹 프록시 활동 또는 클린 웹 프록시 활동의 백분율을 볼 수 있습니다.
L4 트래픽 모니터 요약	L4 트래픽 모니터에서 모니터링되고 차단된 트래픽에 대해 보고합니다.
의심되는 트랜잭션	다양한 보안 구성 요소에서 의심되는 것으로 레이블 지정된 웹 트랜잭션을 볼 수 있습니다. 활동이 발생한 대략적인 날짜와 실제 트랜잭션 수를 표시합니다.
의심되는 트랜잭션 요약	의심되어 차단되거나 경고가 표시된 트랜잭션의 백분율을 볼 수 있습니다.
상위 URL 카테고리: 전체 트랜잭션	차단된 상위 10개의 URL 카테고리를 표시합니다.
상위 애플리케이션 유형: 전체 트랜잭션	AVC 엔진에서 차단된 상위 애플리케이션 유형을 표시합니다.
상위 악성코드 카테고리: 모니터링됨 또는 차단됨	탐지된 모든 악성코드 카테고리를 표시합니다.
상위 사용자: 차단되거나 경고가 표시된 트랜잭션	차단되거나 경고가 표시된 트랜잭션을 생성하는 사용자를 표시합니다. 인증된 사용자는 사용자 이름으로 표시되고 인증되지 않은 사용자는 IP 주소로 표시됩니다.

Users(사용자) 페이지

Reporting(보고) > Users(사용자) 페이지는 개별 사용자에 대한 웹 트래픽 정보를 볼 수 있는 여러 링크를 제공합니다. 네트워크의 사용자가 인터넷이나 특정 웹 사이트 또는 URL에서 소요한 시간과 사용자가 사용한 대역폭의 양을 볼 수 있습니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
차단된 트랜잭션별 상위 사용자	차단된 트랜잭션(가로 눈금)의 수가 가장 큰 사용자(세로 눈금)를 나열합니다.
사용된 대역폭별 상위 사용자	시스템에서 가장 많은 대역폭(GB 사용량으로 표시되는 가로 눈금)을 사용 중인 사용자(세로 눈금)를 표시합니다.
사용자 표	개별 사용자를 나열하고 각 사용자에 대한 여러 통계를 표시합니다.

User Details(사용자 세부사항) 페이지

User Details(사용자 세부사항) 페이지는 **Reporting(보고) > Users(사용자)** 페이지의 Users Table(사용자 표)에서 선택한 특정 사용자에 대한 정보를 표시합니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
전체 트랜잭션별 URL 범주	특정 사용자가 사용 중인 특정 URL 카테고리를 나열합니다.
전체 트랜잭션별 추세	사용자가 웹에 액세스한 시간을 표시합니다.
일치하는 URL 범주	완료된 트랜잭션 및 차단된 트랜잭션 모두에 대해 지정된 시간 범위 동안 일치하는 모든 URL 카테고리를 표시합니다.
일치하는 도메인	이 사용자가 액세스한 특정 도메인 또는 IP 주소에 대한 정보를 표시합니다. **참고** 이 도메인 데이터를 `csv` 파일로 내보내는 경우 처음 300,000개 항목만 파일로 내보냅니다.
일치하는 애플리케이션	AVC 엔진에서 탐지된 대로 특정 사용자가 사용 중인 특정 애플리케이션을 표시합니다.
발견된 악성프로그램 위협	특정 사용자가 트리거하는 상위 멀웨어 위협을 표시합니다.
일치하는 정책	이 특정 사용자에 대해 적용되는 특정 정책을 표시합니다.

Web Sites(웹 사이트) 페이지

Reporting(보고) > Web Sites(웹 사이트) 페이지는 웹 보안 어플라이언스에서 발생하는 활동에 대한 전반적인 집계를 제공합니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
전체 트랜잭션별 상위 도메인	사이트에서 방문하는 상위 도메인을 그래프 형식으로 나열합니다.
차단된 트랜잭션별 상위 도메인	트랜잭션별로 차단 조치가 발생하도록 트리거한 상위 도메인을 그래프 형식으로 나열합니다.
일치하는 도메인	사이트에서 방문하는 도메인을 대화형 표로 나열합니다. **참고** 이 도메인 데이터를 csv 파일로 내보내는 경우 처음 300,000개 항목만 파일로 내보냅니다.

URL Categories(URL 카테고리) 페이지

Reporting(보고) > URL Categories(URL 카테고리) 페이지를 사용하여 네트워크에서 사용자가 방문하는 URL 카테고리를 볼 수 있습니다. URL 카테고리 페이지를 애플리케이션 가시성 페이지 및 사용자 페이지와 함께 사용하여 특정 사용자와 특정 사용자가 액세스하려고 시도하는 애플리케이션 또는 웹 사이트의 유형을 조사할 수 있습니다.

참고경우에 따라 미리 정의된 URL 카테고리 집합이 업데이트됩니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서의 시간 범위를 선택합니다.
전체 트랜잭션별 상위 URL 범주	이 섹션에서는 사이트에서 방문하는 상위 URL 카테고리를 그래프 형식으로 나열합니다.
차단 및 경고된 트랜잭션별 상위 URL 범주	트랜잭션별로 차단 또는 경고 조치가 발생하도록 트리거한 상위 URL을 그래프 형식으로 나열합니다.
일치하는 URL 범주	지정된 시간 범위 동안의 URL 카테고리별 트랜잭션 처리와 각 카테고리에서 사용된 대역폭 및 소요된 시간을 표시합니다. 분류되지 않은 URL의 백분율이 15-20%보다 높은 경우 다음 옵션을 고려합니다. • 특정 현지화된 URL의 경우 맞춤형 URL 카테고리를 생성하여 특정 사용자 또는 그룹 정책에 적용할 수 있습니다. • 평가 및 데이터베이스 업데이트를 위해 분류되지 않은 URL과 잘못 분류된 URL을 Cisco에 보고할 수 있습니다. • 웹 평판 필터링 및 안티멀웨어 필터링이 사용하도록 설정되었는지 확인합니다.

URL 카테고리 집합 업데이트 및 보고

미리 정의된 URL 카테고리 집합이 웹 보안 어플라이언스에서 주기적으로 자동 업데이트될 수 있습니다.

이러한 업데이트가 발생하면 더 오래된 카테고리와 연결된 데이터가 너무 오래되어서 보고서에 포함될 수 없을 때까지 이전 카테고리 이름이 보고서에 계속 표시됩니다. URL 카테고리 집합 업데이트 이후 생성되는 보고서 데이터는 새 카테고리를 사용하므로 이전 카테고리와 새 카테고리 모두가 동일한 보고서에 표시될 수 있습니다.

Application Visibility(애플리케이션 가시성) 페이지

Reporting(보고) > Application Visibility(애플리케이션 가시성) 페이지는 AVC(Application Visibility and Control) 엔진에서 탐지된 대로 사용되고 차단된 애플리케이션 및 애플리케이션 유형을 표시합니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
전체 트랜잭션별 상위 애플리케이션 유형	이 섹션에서는 사이트에서 방문하는 상위 애플리케이션 유형을 그래프 형식으로 나열합니다.
차단된 트랜잭션별 상위 애플리케이션	트랜잭션별로 차단 조치가 발생하도록 트리거한 상위 애플리케이션 유형을 그래프 형식으로 나열합니다.
일치하는 애플리케이션 유형	전체 트랜잭션별 상위 애플리케이션 유형 그래프에 나열된 애플리케이션 유형에 대한 세부 정보를 볼 수 있습니다.
일치하는 애플리케이션	지정된 시간 범위 동안의 모든 애플리케이션을 표시합니다.

Anti-Malware(안티멀웨어) 페이지

Reporting(보고) > Anti-Malware(안티멀웨어) 페이지를 사용하여 Cisco IronPort DVS 엔진에서 탐지된 악성코드를 모니터링하고 식별할 수 있습니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
발견된 전체 악성프로그램 범주	DVS 엔진에서 탐지된 상위 악성코드 카테고리를 표시합니다.
발견된 상위 악성프로그램 위협	DVS 엔진에서 탐지된 상위 악성코드 위협을 표시합니다.
악성프로그램 범주	Top Malware Categories Detected(탐지된 상위 악성코드 카테고리) 섹션에 표시된 특정 악성코드 카테고리에 대한 정보를 표시합니다.
악성프로그램 위협	Top Malware Threats(상위 멀웨어 위협) 섹션에 표시되는 특정 멀웨어 위협에 대한 정보를 표시합니다.

Malware Category Report(악성코드 카테고리 보고서) 페이지

1단계 **Reporting(보고) > Anti-Malware(안티멀웨어)**를 선택합니다.

2단계 Malware Categories(악성코드 카테고리) 대화형 표의 악성코드 카테고리(Malware Category) 열에서 카테고리를 클릭합니다.

Malware Threat Report(멀웨어 위협 보고서) 페이지

1단계 **Reporting(보고) > Anti-Malware(안티멀웨어)**를 선택합니다.

2단계 Malware Threat(멀웨어 위협) 표의 Malware Category(악성코드 카테고리) 열에서 카테고리를 클릭합니다.

Advanced Malware Protection 페이지

파일 평판 및 파일 분석 보고 및 추적, 14-11페이지를 참조하십시오.

File Analysis(파일 분석) 페이지

파일 평판 및 파일 분석 보고 및 추적, 14-11페이지를 참조하십시오.

AMP Verdict Updates(AMP 판정 업데이트) 페이지

파일 평판 및 파일 분석 보고 및 추적, 14-11페이지를 참조하십시오.

Client Malware Risk(클라이언트 악성코드 위험) 페이지

Reporting(보고) > Client Malware Risk(클라이언트 악성코드 위험) 페이지는 클라이언트 악성코드 위험 활동을 모니터링하는 데 사용될 수 있는 보안 관련 보고 페이지입니다. 또한 Client Malware Risk(클라이언트 악성코드 위험) 페이지에는 L4TM(L4 Traffic Monitor)에서 식별된 대로 자주 사용되는 악성코드 연결과 관련된 클라이언트 IP 주소가 나열됩니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
웹 프록시: 악성프로그램 위험별 상위 클라이언트	이 차트는 악성코드 위험을 발생시킨 상위 10명의 사용자를 표시합니다.

(계속)

섹션	설명
L4 트래픽 모니터: 탐지된 악성코드 연결	이 차트는 악성코드 사이트에 가장 자주 연결하는 사용자 조직에 있는 컴퓨터의 IP 주소를 표시합니다.
웹 프록시: 악성프로그램 위험별 클라이언트	웹 프록시: Clients by Malware Risk(악성코드 위험별 클라이언트) 표에는 Web Proxy: Top Clients by Malware Risk(웹 프록시: 악성코드 위험별 상위 클라이언트) 섹션에 표시되는 특정 클라이언트에 대한 자세한 정보가 표시됩니다.
L4 트래픽 모니터: 악성프로그램 위험별 클라이언트	이 표는 악성코드 사이트에 자주 연결하는 사용자 조직에 있는 컴퓨터의 IP 주소를 표시합니다.

Web Proxy - Clients by Malware Risk(웹 프록시 - 악성코드 위험별 클라이언트)에 대한 Client Detail(클라이언트 세부사항) 페이지

Client Details(클라이언트 세부사항) 페이지에는 지정된 시간 범위 동안 특정 클라이언트에 대한 모든 웹 활동 및 악성코드 위험 데이터가 표시됩니다.

1단계 **Reporting(보고) > Client Malware Risk(클라이언트 악성코드 위험)**를 선택합니다.

2단계 **Web Proxy - Client Malware Risk(웹 프록시 - 클라이언트 악성코드 위험)** 섹션의 "User ID / Client IP Address(사용자 ID/클라이언트 IP 주소)" 열에서 사용자 이름을 클릭합니다.

관련 주제

- User Details(사용자 세부사항) 페이지, 23-3페이지

Web Reputation Filters(웹 평판 필터) 페이지

Reporting(보고) > Web Reputation Filters(웹 평판 필터) 페이지는 지정된 시간 범위 동안 트랜잭션에 대해 설정된 웹 평판 필터의 결과를 볼 수 있는 보안 관련 보고 페이지입니다.

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
웹 평판 조치(추세)	지정된 시간(가로 타임라인)에 대한 총 웹 평판 조치 수(세로)를 표시합니다.
웹 신뢰도 작업(볼륨)	트랜잭션별 웹 평판 조치 볼륨(백분율)을 표시합니다.
차단된 트랜잭션별 웹 평판 위협 유형	낮은 평판 점수로 인해 차단된 위협 유형을 표시합니다.
검색된 추가 트랜잭션별 웹 신뢰도 위협 유형	트랜잭션을 스캐닝하도록 표시한 평판 점수를 발생시킨 위협 유형을 표시합니다.
웹 평판 조치(점수별 분석)	각 조치에 대해 분석된 웹 평판 점수를 표시합니다.

L4 Traffic Monitor(L4 트래픽 모니터) 페이지

Reporting(보고) > L4 Traffic Monitor(L4 트래픽 모니터) 페이지는 L4 트래픽 모니터에서 지정된 시간 범위 동안 탐지한 악성코드 포트 및 악성코드 사이트에 대한 정보를 표시하는 보안 관련 보고 페이지입니다. 또한 악성코드 사이트를 자주 발견하는 클라이언트의 IP 주소를 표시합니다.

L4 트래픽 모니터는 어플라이언스의 모든 포트를 통해 들어오는 네트워크 트래픽을 수신하고 도메인 이름과 IP 주소를 자체 데이터베이스 테이블의 항목과 일치시켜서 들어오는 트래픽과 나가는 트래픽을 허용할지 여부를 결정합니다.

섹션	설명
시간 범위(드롭다운 목록)	보고할 시간 범위를 선택할 수 있는 메뉴입니다.
상위 클라이언트 IP	악성코드 사이트에 가장 자주 연결하는 사용자 조직에 있는 컴퓨터의 IP 주소를 그래프 형식으로 표시합니다.
상위 악성코드 사이트	L4 트래픽 모니터에서 탐지된 상위 악성코드 도메인을 그래프 형식으로 표시합니다.
클라이언트 소스 IP	악성코드 사이트에 자주 연결하는 사용자 조직에 있는 컴퓨터의 IP 주소를 표시합니다.
악성코드 포트	L4 트래픽 모니터에서 가장 자주 악성코드를 탐지한 포트를 표시합니다.
발견된 악성프로그램 사이트	L4 트래픽 모니터에서 가장 자주 악성코드를 탐지하는 도메인을 표시합니다.

SOCKS Proxy(SOCKS 프록시) 페이지

Reporting(보고) > SOCKS Proxy(SOCKS 프록시) 페이지에서는 상위 대상 및 사용자에 대한 정보를 포함하여 SOCKS 프록시를 통해 처리되는 트랜잭션에 대한 데이터 및 추세를 볼 수 있습니다.

Reports by User Location(사용자 위치별 보고서) 페이지

Reporting(보고) > Reports by User Location(사용자 위치별 보고서) 페이지에서 로컬 및 원격 사용자가 수행하는 활동을 알아볼 수 있습니다.

활동에는 다음이 포함됩니다.

- 로컬 및 원격 사용자가 액세스하는 URL 카테고리
- 로컬 및 원격 사용자가 액세스하는 사이트에서 트리거되는 안티멀웨어 활동
- 로컬 및 원격 사용자가 액세스하는 사이트의 웹 평판
- 로컬 및 원격 사용자가 액세스하는 애플리케이션
- 사용자(로컬 및 원격)

- 로컬 및 원격 사용자가 액세스하는 도메인

섹션	설명
시간 범위(드롭다운 목록)	보고서에 포함된 데이터의 시간 범위를 선택할 수 있는 메뉴입니다.
총 웹 프록시 활동: 원격 사용자	지정된 시간(가로) 동안 원격 사용자(세로)의 활동을 표시합니다.
웹 프록시 요약	네트워크에 있는 로컬 및 원격 사용자의 활동에 대한 요약을 표시합니다.
총 웹 프록시 활동: 로컬 사용자	지정된 시간(가로) 동안 원격 사용자(세로)의 활동을 표시합니다.
탐지된 의심되는 트랜잭션: 원격 사용자	지정된 시간(가로) 동안 원격 사용자(세로)에 대해 정의된 액세스 정책으로 인해 탐지된 의심되는 트랜잭션을 표시합니다.
의심되는 트랜잭션 요약	네트워크에 있는 원격 사용자의 의심되는 트랜잭션에 대한 요약을 표시합니다.
탐지된 의심되는 트랜잭션: 로컬 사용자	지정된 시간(가로) 동안 사용자의 원격 사용자(세로)에 대해 정의된 액세스 정책으로 인해 탐지된 의심되는 트랜잭션을 표시합니다.
의심되는 트랜잭션 요약	네트워크에 있는 로컬 사용자의 의심되는 트랜잭션에 대한 요약을 표시합니다.

Web Tracking(웹 추적) 페이지

웹 추적 페이지를 사용하여 관심이 있는 개별 트랜잭션 또는 트랜잭션 패턴에 대한 세부사항을 검색하고 가져옵니다. 필요에 따라 다음 탭 중 하나를 검색합니다.

웹 추적 페이지	작업 링크
웹 프록시에서 처리되는 트랜잭션	웹 프록시에서 처리되는 트랜잭션 검색, 19-9페이지
L4 트래픽 모니터에서 처리되는 트랜잭션	L4 트래픽 모니터에서 처리되는 트랜잭션 검색, 19-12페이지
SOCKS 프록시에서 처리되는 트랜잭션	SOCKS 프록시에서 처리되는 트랜잭션 검색, 19-12페이지

웹 프록시에서 처리되는 트랜잭션 검색

Reporting(보고) > Web Tracking(웹 추적) 페이지의 **Proxy Services(프록시 서비스)** 탭을 사용하여 특정 사용자 또는 모든 사용자에 대한 웹 사용 현황을 추적하고 보고할 수 있습니다.

특정 기간 동안 기록된 트랜잭션 유형(차단됨, 모니터링됨, 경고가 표시됨 및 완료됨)에 대한 검색 결과를 볼 수 있습니다. 또한 URL 카테고리, 멀웨어 위협 및 애플리케이션과 같은 여러 조건을 사용하여 데이터 결과를 필터링할 수 있습니다.

참고 웹 프록시는 "OTHER-NONE" 이외의 ACL 결정 태그를 포함하는 트랜잭션에 대해서만 보고합니다.

1단계 **Reporting(보고) > Web Tracking(웹 추적)**을 선택합니다.

2단계 **Proxy Services(프록시 서비스)** 탭을 클릭합니다.

3단계 설정을 구성합니다.

설정	설명
시간 범위	보고할 시간 범위를 선택합니다.
사용자/클라이언트 IP	(선택 사항) 보고서에 표시되는 인증 사용자 이름 또는 추적할 클라이언트 IP 주소를 입력합니다. CIDR 형식의 IP 범위를 입력할 수도 있습니다. 이 필드를 비워 두면 검색 시 모든 사용자에 대한 결과가 반환됩니다.
웹사이트	(선택 사항) 추적할 웹 사이트를 입력합니다. 이 필드를 비워 두면 검색 시 모든 웹 사이트에 대한 결과가 반환됩니다.
거래 유형	All Transactions(모든 트랜잭션), Completed(완료됨), Blocked(차단됨), Monitored(모니터링됨) 또는 Warned(경고가 표시됨) 중에서 추적할 트랜잭션의 유형을 선택합니다.

4단계 (선택 사항) Advanced(고급) 섹션을 확장하고 웹 추적 결과를 더 상세한 조건으로 필터링하도록 필드를 구성합니다.

설정	설명
URL Category (URL 범주)	URL 카테고리별로 필터링하려면 **Filter by URL Category(URL 카테고리별 필터링)**를 선택하고 필터링 기준이 될 URL 카테고리의 첫 번째 문자를 입력합니다. 표시되는 목록에서 카테고리를 선택합니다.
애플리케이션	애플리케이션별로 필터링하려면 **Filter by Application(애플리케이션별 필터링)**을 선택하고 필터링 기준이 될 애플리케이션을 선택합니다. 애플리케이션 유형별로 필터링하려면 **Filter by Application Type(애플리케이션 유형별 필터링)**을 선택하고 필터링 기준이 될 애플리케이션 유형을 선택합니다.
정책	이 트랜잭션에 대한 최종 결정을 담당하는 정책의 이름별로 필터링하려면 **Filter by Action Policy(조치 정책별 필터링)**를 선택하고 필터링 기준이 될 정책 그룹 이름(액세스 정책, 암호 해독 정책 또는 데이터 보안 정책)을 입력합니다. 자세한 내용은 액세스 로그 파일의 웹 프록시 정보, 21-14페이지 섹션에서 `PolicyGroupName`에 대한 설명을 참조하십시오.
AMP(Advanced Malware Protection)	웹 추적 및 Advanced Malware Protection 기능 정보, 14-13페이지를 참조하십시오.
악성프로그램 위협	특정 멀웨어 위협별로 필터링하려면 **Filter by Malware Threat(멀웨어 위협별 필터링)**를 선택하고 필터링 기준이 될 멀웨어 위협 이름을 입력합니다. 악성코드 카테고리별로 필터링하려면 **Filter by Malware Category(악성코드 카테고리별 필터링)**를 선택하고 필터링 기준이 될 악성코드 카테고리를 선택합니다.

(계속)

설정	설명
WBRS	WBRS 섹션에서는 웹 평판 점수 및 특정 웹 평판 위협별로 필터링할 수 있습니다. • 웹 평판 점수별로 필터링하려면 **Score Range(점수 범위)**를 선택하고 필터링 기준이 될 상위 및 하위 값을 선택합니다. 또는 **No Score(점수 없음)**를 선택하여 점수가 없는 웹 사이트에 대해 필터링할 수 있습니다. • 웹 평판 위협별로 필터링하려면 **Filter by Reputation Threat(평판 위협별 필터링)**를 선택하고 필터링 기준이 될 웹 평판 위협을 입력합니다.
AnyConnect Secure Mobility	사용자 위치(원격 또는 로컬)별로 필터링하려면 **Filter by User Location(사용자 위치별 필터링)**을 선택하고 필터링 기준이 될 사용자 유형을 선택합니다.
사용자 요청	클라이언트가 시작한 트랜잭션별로 필터링하려면 **Filter by User-Requested Transactions(사용자 요청 트랜잭션별 필터링)**를 선택합니다. **참고** 이 필터를 사용하도록 설정하면 검색 결과에 일부 "추측" 트랜잭션이 포함됩니다.

5단계 **Search(검색)**를 클릭합니다.

결과는 타임스탬프를 기준으로 정렬되며, 최근 결과가 맨 위에 있습니다.

"Display Details(세부사항 표시)" 링크 아래의 괄호 안에 있는 숫자는 사용자가 시작한 트랜잭션에서 생성된 관련 트랜잭션의 수입니다(예: 로드된 이미지, 실행된 javascripts 및 액세스된 보조 사이트).

6단계 (선택 사항) 각 트랜잭션에 대한 자세한 정보를 보려면 Transactions(트랜잭션) 열에서 **Display Details(세부사항 표시)**를 클릭합니다.

참고 1000개보다 더 많은 결과를 확인해야 하는 경우 **Printable Download(인쇄 가능한 다운로드)** 링크를 클릭하여 관련 트랜잭션의 세부사항을 제외한 전체 원시 데이터 집합을 포함하는 CSV 파일을 확보합니다.

정보 결과의 URL이 잘린 경우 액세스 로그에서 전체 URL을 찾을 수 있습니다.

최대 500개의 관련 트랜잭션에 대한 세부사항을 보려면 **Related Transactions(관련 트랜잭션)** 링크를 클릭합니다.

관련 주제

- URL 카테고리 집합 업데이트 및 보고, 19-5페이지
- 악성코드 카테고리 설명, 13-14페이지
- 웹 추적 및 Advanced Malware Protection 기능 정보, 14-13페이지

L4 트래픽 모니터에서 처리되는 트랜잭션 검색

Reporting(보고) > Web Tracking(웹 추적) 페이지의 L4 Traffic Monitor(L4 트래픽 모니터) 탭에서는 악성코드 사이트 및 포트에 대한 연결과 관련된 세부사항을 제공합니다. 다음 유형의 정보를 사용하여 악성코드 사이트에 대한 연결을 검색할 수 있습니다.

- 시간 범위
- IP 주소 또는 도메인을 사용하는 사이트
- 포트
- 조직의 컴퓨터와 연결된 IP 주소
- 연결 유형

처음으로 일치한 1000개의 검색 결과가 표시됩니다.

SOCKS 프록시에서 처리되는 트랜잭션 검색

차단되거나 완료된 트랜잭션, 사용자 및 대상 도메인, IP 주소 또는 포트를 포함하여 다양한 기준을 충족하는 트랜잭션을 검색할 수 있습니다.

1단계 **Web(웹) > Reporting(보고) > Web Tracking(웹 추적)**을 선택합니다.

2단계 **SOCKS Proxy(SOCKS 프록시)** 탭을 클릭합니다.

3단계 결과를 필터링하려면 **Advanced(고급)**를 클릭합니다.

4단계 검색 기준을 입력합니다.

5단계 **Search(검색)**를 클릭합니다.

관련 주제

- SOCKS Proxy(SOCKS 프록시) 페이지, 19-8페이지

System Capacity(시스템 용량) 페이지

Reporting(보고) > System Capacity(시스템 용량) 페이지는 웹 보안 어플라이언스의 리소스 사용률에 대한 현재 정보 및 기록 정보를 표시합니다.

System Capacity(시스템 용량) 페이지에서 데이터를 보기 위해 시간 범위를 선택할 때 다음을 기억해야 합니다.

- **시간 보고서.** 시간 보고서는 분 표를 쿼리하고 60분 기간 동안 분 단위로 어플라이언스에서 기록된 정확한 항목 수(예: 바이트 및 연결)를 표시합니다.
- **일 보고서.** 일 보고서는 시간 표를 쿼리하고 24시간 기간 동안 시간 단위로 어플라이언스에서 기록된 정확한 항목 수(예: 바이트 및 연결)를 표시합니다. 이 정보는 시간 표에서 수집됩니다.

주 보고서 및 30일 보고서는 시간 및 일 보고서와 유사하게 작동합니다.

System Status(시스템 상태) 페이지

Reporting(보고) > System Status(시스템 상태) 페이지를 사용하여 시스템 상태를 모니터링합니다. 이 페이지는 웹 보안 어플라이언스의 현재 상태 및 컨피그레이션을 표시합니다.

섹션	표시되는 항목
Web Security Appliance 상태	• 시스템 가동 시간 • 시스템 리소스 사용률 - CPU 사용률, RAM 사용률, 보고 및 기록에 사용된 디스크 공간의 백분율 이 페이지에 표시된 CPU 사용률 값과 시스템 개요 페이지(Overview(개요) 페이지, 19-2페이지)에 표시된 CPU 값은 다른 순간에 개별적으로 읽혀지므로 약간 다를 수 있습니다. 효율적으로 작동하는 시스템의 RAM 사용률이 90%를 초과할 수 있습니다. 시스템에서 사용되지 않는 RAM은 웹 개체 캐시에서 사용되기 때문입니다. 시스템에서 심각한 성능 문제가 발생하지 않고 이 값이 지속적으로 100%를 나타내지 않으면 시스템이 정상적으로 작동하는 것입니다. **참고** 프록시 버퍼 메모리는 이 RAM을 사용하는 하나의 구성 요소입니다.
프록시 트래픽 특성	• 초당 트랜잭션 수 • 대역폭 • 대응시간 • 캐시 적중률 • 연결
고가용성	•
외부 서비스	• Identity Services Engine
현재 구성	웹 프록시 설정: • 웹 프록시 상태 - 사용됨 또는 사용 안 함 • 구축 토폴로지 • 웹 프록시 모드 - 전달 또는 투명 • IP 스푸핑 - 사용됨 또는 사용 안 함 L4 트래픽 모니터 설정: • L4 트래픽 모니터 상태 - 사용됨 또는 사용 안 함 • L4 트래픽 모니터 와이어링: • L4 트래픽 모니터 조치 - 모니터링 또는 차단 웹 보안 어플라이언스 버전 정보 하드웨어 정보

관련 주제

- System Capacity(시스템 용량) 페이지, 19-12페이지

비표준 포트에서 비인가 트래픽 탐지

- 비인가 트래픽 탐지 개요, 20-1페이지
- L4 트래픽 모니터 구성, 20-1페이지
- 알려진 사이트 목록, 20-2페이지
- L4 트래픽 모니터 전역 설정 구성, 20-2페이지
- L4 트래픽 모니터 안티멀웨어 규칙 업데이트, 20-3페이지
- 비인가 트래픽을 탐지하기 위한 정책 생성, 20-3페이지
- L4 트래픽 모니터 활동 보기, 20-5페이지

비인가 트래픽 탐지 개요

Web Security Appliance에는 모든 네트워크 포트에서 비인가 트래픽을 탐지하고 포트 80을 우회하려는 악성코드 시도를 중지하는 통합 레이어-4 트래픽 모니터가 있습니다. 내부 클라이언트가 악성코드에 감염되고 비표준 포트 및 프로토콜에서 phone-home을 시도하면 L4 트래픽 모니터에서 phone-home 활동이 회사 네트워크 외부에서 이동하지 못하도록 합니다. 기본적으로 L4 트래픽 모니터가 사용하도록 설정되어 있고 모든 포트의 트래픽을 모니터링하도록 설정됩니다. 여기에는 DNS 및 기타 서비스가 포함됩니다.

L4 트래픽 모니터는 고유한 내부 데이터베이스를 사용하고 유지 관리합니다. 이 데이터베이스는 IP 주소 및 도메인 이름에 일치하는 결과로 계속해서 업데이트됩니다.

L4 트래픽 모니터 구성

1단계	방화벽 내부에 L4 트래픽 모니터를 구성합니다.	
2단계	L4 트래픽 모니터가 프록시 포트 뒤와 클라이언트 IP 주소에 대한 NAT(Network Address Translation)를 수행하는 디바이스 앞에 '논리적으로' 연결되었는지 확인합니다.	
3단계	전역 설정 구성	L4 트래픽 모니터 전역 설정 구성, 20-2페이지를 참조하십시오.
4단계	L4 트래픽 모니터 정책 생성	비인가 트래픽을 탐지하기 위한 정책 생성, 20-3페이지를 참조하십시오.

알려진 사이트 목록

주소	설명
알려진 허용	Allow List(허용 목록) 속성에 나열된 IP 주소 또는 호스트 이름. 이러한 주소는 로그 파일에 "whitelist(화이트리스트)" 주소로 표시됩니다.
목록에 없음	악성코드 사이트로 알려지지 않았고 알려진 허용 주소가 아닌 모든 IP 주소. 이러한 주소는 Allow List(허용 목록), Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소) 속성 또는 L4 트래픽 모니터 데이터베이스에 나열되지 않습니다. 이러한 주소는 로그 파일에 표시되지 않습니다.
모호한	이러한 주소는 로그 파일에 "greylist(그레이리스트)" 주소로 표시되고 다음을 포함합니다. – 목록에 없는 *호스트 이름* 및 알려진 악성코드 *호스트 이름* 모두와 연결된 *IP 주소* – 목록에 없는 *호스트 이름* 및 Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소) 속성의 *호스트 이름* 모두와 연결된 *IP 주소*
알려진 악성코드	이러한 주소는 로그 파일에 "blacklist(블랙리스트)" 주소로 표시되고 다음을 포함합니다. – L4 트래픽 모니터 데이터베이스가 알려진 악성코드 사이트로 판별하고 허용 목록에 나열되지 *않은* IP 주소 또는 호스트 이름 – Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소) 속성에 나열되고 허용 목록에 나열되지 *않으며* 모호하지 *않은 IP 주소*

L4 트래픽 모니터 전역 설정 구성

1단계 **Security Services(보안 서비스) > L4 Traffic Monitor(L4 트래픽 모니터)**를 선택합니다.

2단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 L4 트래픽 모니터를 사용하도록 설정할지 여부를 선택합니다.

4단계 L4 트래픽 모니터를 사용하도록 설정한 경우 모니터링해야 하는 포트를 선택합니다.

- **모든 포트.** 65535개의 모든 TCP 포트에서 비인가 활동을 모니터링합니다.
- **프록시 포트를 제외한 모든 포트.** 다음 포트를 제외한 모든 TCP 포트에서 비인가 활동을 모니터링합니다.
  - **Security Services(보안 서비스) > Web Proxy(웹 프록시)** 페이지의 "HTTP Ports to Proxy(프록시에 대한 HTTP 포트)" 속성에서 구성된 포트(일반적으로 포트 80).
  - **Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시)** 페이지의 "Transparent HTTPS Ports to Proxy(프록시에 대한 투명 HTTPS 포트)" 속성에 구성된 포트(일반적으로 포트 443).

5단계 **변경 사항을 제출** 및 **커밋합니다**.

L4 트래픽 모니터 안티멀웨어 규칙 업데이트

1단계 **Security Services(보안 서비스) > L4 Traffic Monitor(L4 트래픽 모니터)**를 선택합니다.

2단계 **Update Now(지금 업데이트)**를 클릭합니다.

비인가 트래픽을 탐지하기 위한 정책 생성

L4 트래픽 모니터에서 수행하는 조치는 사용자가 구성하는 L4 트래픽 모니터 정책에 따라 다릅니다.

1단계 **Web Security Manager(웹 보안 관리자) > L4 Traffic Monitor(L4 트래픽 모니터)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Edit L4 Traffic Monitor Policies(L4 트래픽 모니터 정책 편집)** 페이지에서 L4 트래픽 모니터 정책을 구성합니다.

a. **허용 목록 정의**

b. 알려진 양호한 사이트를 **허용 목록**에 추가

참고 Web Security Appliance IP 주소 또는 호스트 이름을 **허용 목록**에 포함하지 마십시오. 그렇지 않으면 L4 트래픽 모니터가 트래픽을 차단하지 않습니다.

c. **의심되는 악성코드 주소**에 대해 수행할 조치를 결정합니다.

작업	설명
허용	알려진 허용 주소 및 목록에 없는 주소에 대한 트래픽을 항상 허용합니다.
모니터링	다음과 같은 경우에 트래픽을 모니터링합니다. – Action for Suspected Malware Addresses(의심되는 악성코드 주소에 대한 조치) 옵션이 Monitor(모니터링)로 설정된 경우 알려진 허용 주소에 대한 트래픽을 제외한 모든 트래픽을 항상 모니터링합니다. – Action for Suspected Malware Addresses(의심되는 악성코드 주소에 대한 조치) 옵션이 Block(차단)으로 설정된 경우 모호한 주소에 대한 트래픽을 모니터링합니다.
차단	Action for Suspected Malware Addresses(의심되는 악성코드 주소에 대한 조치) 옵션이 Block(차단)으로 설정된 경우 알려진 악성코드 주소에 대한 트래픽을 차단합니다.

참고 의심되는 악성코드 트래픽을 차단하도록 선택하는 경우 모호한 주소를 항상 차단할지 여부를 선택할 수도 있습니다. 기본적으로 모호한 주소가 모니터링됩니다.

참고 L4 트래픽 모니터가 차단으로 구성된 경우 L4 트래픽 모니터와 웹 프록시가 동일한 네트워크에서 구성되어야 합니다. **Network(네트워크) > Routes(경로)** 페이지를 사용하여 데이터 트래픽용으로 구성된 경로에서 모든 클라이언트에 액세스할 수 있는지 확인합니다.

d. **Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소)** 속성을 정의합니다.

참고 내부 IP 주소를 의심되는 추가 악성코드 주소 목록에 추가하면 정당한 대상 URL이 L4 트래픽 모니터 보고서에 악성코드로 표시됩니다. 이를 방지하려면 **Web Security Manager(웹 보안 관리자) > L4 Traffic Monitor Policies(L4 트래픽 모니터 정책)** 페이지의 "**Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소)**" 필드에 내부 IP 주소를 입력하지 마십시오.

4단계 **변경 사항을 제출** 및 **커밋합니다**.

관련 주제

- 비인가 트래픽 탐지 개요, 20-1페이지
- 유효한 형식, 20-4페이지

유효한 형식

Allow List(허용 목록) 또는 Additional Suspected Malware Addresses(의심되는 추가 악성코드 주소) 속성에 주소를 추가할 경우 공백이나 쉼표로 여러 항목을 구분합니다. 다음 형식으로 주소를 입력할 수 있습니다.

- **IPv4 IP 주소.** 예: IPv4 형식: 10.1.1.0. IPv6 형식: 2002:4559:1FE2::4559:1FE2
- **CIDR 주소.** 예: 10.1.1.0/24.
- **도메인 이름.** 예: example.com.
- **호스트 이름.** 예: crm.example.com.

L4 트래픽 모니터 활동 보기

S-Series 어플라이언스는 기능별 보고서 및 요약 통계의 인터랙티브 표시를 생성하기 위한 몇 가지 옵션을 지원합니다.

활동 모니터링 및 요약 통계 보기

Reporting(보고) > L4 Traffic Monitor(L4 트래픽 모니터) 페이지에서는 모니터링 활동의 통계 요약을 제공합니다. 다음 표시 및 보고 툴을 사용하여 L4 트래픽 모니터 활동의 결과를 볼 수 있습니다.

보려는 내용	참조
클라이언트 통계	Reporting(보고) > Client Activity(클라이언트 활동)
악성코드 통계 포트 통계	Reporting(보고) > L4 Traffic Monitor(L4 트래픽 모니터)
L4 트래픽 모니터 로그 파일	System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) • trafmon_errlogs • trafmonlogs

참고 웹 프록시가 전달 프록시로 구성되고 L4 트래픽 모니터가 모든 포트를 모니터링하도록 설정된 경우 프록시 데이터 포트의 IP 주소가 기록되고 **Reporting(보고) > Client Activity(클라이언트 활동)** 페이지의 클라이언트 활동 보고서에 클라이언트 IP 주소로 표시됩니다. 웹 프록시가 투명 프록시로 구성된 경우 클라이언트 IP 주소를 올바르게 기록하고 표시할 수 있도록 IP 스푸핑을 사용하도록 설정합니다.

L4 트래픽 모니터 로그 파일 항목

L4 트래픽 모니터 로그 파일은 모니터링 활동에 대한 자세한 레코드를 제공합니다.

21장

로그를 통해 시스템 활동 모니터링

- 로깅 개요, 21-1페이지
- 로깅에 대한 공통 작업, 21-2페이지
- 로깅에 대한 모범 사례, 21-2페이지
- 로그를 사용하여 웹 프록시 문제 트러블슈팅, 21-2페이지
- 로그 파일 유형, 21-3페이지
- 로그 서브스크립션 추가 및 편집, 21-7페이지
- 로그 파일을 다른 서버에 푸시, 21-11페이지
- 로그 파일 아카이브, 21-12페이지
- 로그 파일 이름 및 어플라이언스 디렉토리 구조, 21-12페이지
- 로그 파일 보기, 21-13페이지
- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지
- 액세스 로그 스캐닝 판정 항목 해석, 21-20페이지
- W3C 호환 액세스 로그 파일, 21-24페이지
- 액세스 로그 맞춤화, 21-26페이지
- 트래픽 모니터 로그 파일, 21-30페이지
- 로그 파일 필드 및 태그, 21-31페이지
- 로깅 트러블슈팅, 21-41페이지

로깅 개요

웹 보안 어플라이언스는 고유한 시스템 및 트래픽 관리 활동을 로그 파일에 작성하여 기록합니다. 관리자는 이러한 로그 파일을 참조하여 어플라이언스를 모니터링하고 트러블슈팅할 수 있습니다.

어플라이언스는 특정 활동에 대한 정보 찾기 작업을 간소화하기 위해 여러 유형의 활동을 다양한 로깅 유형으로 나눕니다. 기본적으로 이들 대부분이 자동으로 사용하도록 설정되지만 일부는 필요에 따라 수동으로 사용하도록 설정해야 합니다.

로그 파일 서브스크립션을 통해 로그 파일을 사용하도록 설정하고 관리합니다. 서브스크립션을 통해 로그 파일을 생성, 맞춤화 및 관리하기 위한 설정을 정의할 수 있습니다.

일반적으로 관리자가 사용하는 두 가지 기본 로그 파일 유형은 다음과 같습니다.

- **액세스 로그.** 이 로그는 모든 웹 프록시 필터링 및 스캐닝 활동을 기록합니다.
- **트래픽 모니터 로그.** 이 로그는 모든 레이어-4 트래픽 모니터 활동을 기록합니다.

이러한 로그 유형과 기타 로그 유형을 사용하여 현재 및 과거 어플라이언스 활동을 볼 수 있습니다. 참조표를 사용하여 로그 파일 항목을 해석하는 데 도움을 받을 수 있습니다.

관련 주제

- 로깅에 대한 공통 작업, 21-2페이지
- 로그 파일 유형, 21-3페이지

로깅에 대한 공통 작업

작업	관련 주제 및 절차에 대한 링크
로그를 사용하여 웹 프록시 문제 트러블슈팅	로그를 사용하여 웹 프록시 문제 트러블슈팅, 21-2페이지
로그 서브스크립션 추가 및 편집	로그 서브스크립션 추가 및 편집, 21-7페이지
로그 파일 보기	로그 파일 보기, 21-13페이지
로그 파일 해석	액세스 로그 스캐닝 판정 항목 해석, 21-20페이지
로그 파일 맞춤화	액세스 로그 맞춤화, 21-26페이지
로그 파일을 다른 서버에 푸시	로그 파일을 다른 서버에 푸시, 21-11페이지
로그 파일 아카이브	로그 파일 아카이브, 21-12페이지

로깅에 대한 모범 사례

- 로그 서브스크립션의 수를 최소화하면 시스템 성능이 향상됩니다.
- 더 적은 세부 정보를 기록하면 시스템 성능이 향상됩니다.

로그를 사용하여 웹 프록시 문제 트러블슈팅

기본적으로 웹 보안 어플라이언스에는 웹 프록시 로깅 메시지를 위해 생성된 "Default Proxy Logs(기본 프록시 로그)"라는 하나의 로그 서브스크립션이 있습니다. 이는 모든 웹 프록시 모듈에 대한 기본 정보를 캡처합니다. 또한 기본 프록시 로그를 복잡하게 하지 않고 각 모듈에 대한 더 구체적인 디버그 정보를 읽을 수 있도록 각 웹 프록시 모듈에 대한 로그 파일 유형이 어플라이언스에 포함되어 있습니다.

아래 단계에 따라 사용 가능한 여러 로그를 사용하여 웹 프록시 문제를 트러블슈팅합니다.

1단계 기본 프록시 로그를 읽습니다.

2단계 문제와 관련되었을 수 있지만 해결하기 위한 충분한 정보가 없는 항목이 표시된 경우 관련 특정 웹 프록시 모듈에 대한 로그 서브스크립션을 생성합니다. 다음 웹 프록시 모듈 로그 유형을 사용할 수 있습니다.

액세스 제어 엔진 로그
AVC 엔진 프레임워크 로그
컨피그레이션 로그
연결 관리 로그
데이터 보안 모듈 로그
DCA 엔진 프레임워크 로그
디스크 관리자 로그
FireAMP
FTP 프록시 로그
HTTPS 로그
라이센스 모듈 로그
로깅 프레임워크 로그
McAfee 통합 프레임워크 로그
메모리 관리자 로그
기타 프록시 모듈 로그
요청 디버그 로그
SNMP 모듈 로그
Sophos 통합 프레임워크 로그
WBRS 프레임워크 로그
WCCP 모듈 로그
Webcat 통합 프레임워크 로그
Webroot 통합 프레임워크 로그

3단계 문제를 다시 생성하고 관련 항목에 대한 새 웹 프록시 모듈 로그를 읽습니다.

4단계 필요에 따라 다른 웹 프록시 모듈 로그에 대해서도 반복합니다.

5단계 더 이상 필요하지 않은 서브스크립션을 제거합니다.

관련 주제

- 로그 파일 유형, 21-3페이지
- 로그 서브스크립션 추가 및 편집, 21-7페이지

로그 파일 유형

웹 프록시 구성 요소와 관련된 일부 로그 유형은 사용하도록 설정되어 있지 않습니다. "Default Proxy Logs(기본 프록시 로그)"라는 기본 웹 프록시 로그 유형이 기본적으로 사용하도록 설정되고 모든 웹 프록시 모듈에 대한 기본 정보를 캡처합니다. 또한 각 웹 프록시 모듈에는 필요에 따라 수동으로 사용하도록 설정할 수 있는 고유한 로그 유형이 있습니다.

다음 표에는 웹 보안 어플라이언스 로그 파일 유형이 설명되어 있습니다.

로그 파일 유형	설명	Syslog 푸시 지원 여부	기본적으로 사용하도록 설정되는지 여부
액세스 제어 엔진 로그	웹 프록시 ACL(Access Control List) 평가 엔진과 관련된 메시지를 기록합니다.	아니요	아니요
AMP 엔진 로그	파일 평판 스캐닝 및 파일 분석(Advanced Malware Protection)에 대한 정보를 기록합니다. 로그 파일, 14-14페이지도 참조하십시오.	예	예
감사 로그	AAA(Authentication, Authorization, and Accounting)를 기록합니다. 애플리케이션 및 CLI(Command Line Interface)와의 모든 사용자 상호 작용을 기록하고 커밋된 변경 사항을 캡처합니다.	예	예

로그 파일 유형	설명	Syslog 푸시 지원 여부	기본적으로 사용하도록 설정되는지 여부
액세스 로그	웹 프록시 클라이언트 기록을 기록합니다.	예	예
인증 프레임워크 로그	인증 내역 및 메시지를 기록합니다.	아니요	예
AVC 엔진 프레임워크 로그	웹 프록시와 AVC 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
AVC 엔진 로그	AVC 엔진의 디버그 메시지를 기록합니다.	예	예
CLI Audit Logs	CLI(Command Line Interface) 활동의 감사 내역을 기록합니다.	예	예
컨피그레이션 로그	웹 프록시 컨피그레이션 관리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
연결 관리 로그	웹 프록시 연결 관리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
데이터 보안 로그	Cisco 데이터 보안 필터로 평가되는 업로드 요청에 대한 클라이언트 내역을 기록합니다.	예	예
데이터 보안 모듈 로그	Cisco 데이터 보안 필터와 관련된 메시지를 기록합니다.	아니요	아니요
DCA 엔진 프레임워크 로그 (Dynamic Content Analysis)	웹 프록시와 Cisco Web Usage Controls DCA(Dynamic Content Analysis) 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
DCA 엔진 로그 (Dynamic Content Analysis)	Cisco Web Usage Controls DCA(Dynamic Content Analysis) 엔진과 관련된 메시지를 기록합니다.	예	예
기본 프록시 로그	웹 프록시와 관련된 오류를 기록합니다. 이는 모든 웹 프록시 관련 로그 중에서 가장 기본적인 기록입니다. 웹 프록시와 관련하여 더욱 구체적인 문제를 해결하려면, 해당 웹 프록시 모듈에 대한 로그 서브스크립션을 생성합니다.	예	예
디스크 관리자 로그	디스크에 있는 캐시에 쓰기와 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
외부 인증 로그	외부 인증 서버와의 통신 성공 또는 실패와 같은 외부 인증 기능 사용과 관련된 메시지를 기록합니다. 외부 인증이 사용하지 않도록 설정된 경우에도 이 로그에는 로그인에 성공하거나 실패한 로컬 사용자에 대한 메시지가 포함됩니다.	아니요	예
피드백 로그	잘못 분류된 페이지를 보고하는 웹 사용자를 기록합니다.	예	예
FTP 프록시 로그	FTP 프록시와 관련된 오류 및 경고 메시지를 기록합니다.	아니요	아니요

로그 파일 유형	설명	Syslog 푸시 지원 여부	기본적으로 사용하도록 설정되는지 여부
FTP Server Logs	FTP를 사용하여 웹 보안 어플라이언스에 업로드되고 이 어플라이언스에서 다운로드된 모든 파일을 기록합니다.	예	예
GUI 로그 (Graphical User Interface)	웹 인터페이스의 페이지 새로 고침 내역을 기록합니다. GUI 로그에는 SMTP 트랜잭션에 대한 정보가 포함됩니다(예: 어플라이언스에서 이메일로 전송된 예약된 보고서의 정보).	예	예
헤이스택 (Haystack) 로그	헤이스택(Haystack) 로그에는 웹 트랜잭션 추적 데이터 처리가 기록됩니다.	예	예
HTTPS 로그	HTTPS 프록시가 사용하도록 설정된 경우 HTTPS 프록시에 특정한 웹 프록시 메시지를 기록합니다.	아니요	아니요
ISE 서버 로그	ISE 서버 연결 및 작동 정보를 기록합니다.	예	예
라이센스 모듈 로그	웹 프록시의 라이센스 및 기능 키 처리 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
로깅 프레임워크 로그	웹 프록시의 로깅 시스템과 관련된 메시지를 기록합니다.	아니요	아니요
로깅 로그	로그 관리와 관련된 오류를 기록합니다.	예	예
McAfee 통합 프레임워크 로그	웹 프록시와 McAfee 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
McAfee 로그	McAfee 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
메모리 관리자 로그	웹 프록시 프로세스에 대한 메모리 내 캐시를 포함한 모든 메모리의 관리와 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
기타 프록시 모듈 로그	주로 개발자 또는 고객 지원에서 사용하는 웹 프록시 메시지를 기록합니다.	아니요	아니요
AnyConnect Secure Mobility 데몬 로그	상태 확인을 포함하여 Web Security Appliance와 AnyConnect 클라이언트 간의 상호작용을 기록합니다.	예	예
NTP 로그 (Network Time Protocol)	NTP(Network Time Protocol)를 통해 작성된 시스템 시간에 대한 변경 사항을 기록합니다.	예	예
PAC 파일 호스트 데몬 로그	클라이언트별 PAC(Proxy Auto-Config) 파일 사용을 기록합니다.	예	예
프록시 Bypass 로그	웹 프록시를 우회하는 트랜잭션을 기록합니다.	아니요	예
보고 로그	보고서 생성 내역을 기록합니다.	예	예
쿼리 보고 로그	보고서 생성과 관련된 오류를 기록합니다.	예	예

로그 파일 유형	설명	Syslog 푸시 지원 여부	기본적으로 사용하도록 설정되는지 여부
요청 디버그 로그	모든 웹 프록시 모듈 로그 유형의 특정 HTTP 트랜잭션에 대한 자세한 디버그 정보를 기록합니다. 다른 모든 프록시 로그 서브스크립션을 생성하지 않고 특정 트랜잭션에 대한 프록시 문제를 트러블슈팅하기 위해 이 로그 서브스크립션을 생성하려고 할 수 있습니다. **참고:** CLI에서만 이 로그 서브스크립션을 생성할 수 있습니다.	아니요	아니요
인증 로그	액세스 제어 기능과 관련된 메시지를 기록합니다.	예	예
SHD 로그 (System Health Daemon)	시스템 서비스 상태의 내역과 예기치 않은 데몬 재시작 내역을 기록합니다.	예	예
SNMP 로그	SNMP 네트워크 관리 엔진과 관련된 디버그 메시지를 기록합니다.	예	예
SNMP 모듈 로그	SNMP 모니터링 시스템과의 상호작용과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
Sophos 통합 프레임워크 로그	웹 프록시와 Sophos 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Sophos 로그	Sophos 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
Status Logs	기능 키 다운로드와 같이 시스템과 관련된 정보를 기록합니다.	예	예
시스템 로그	DNS, 오류 및 커밋 활동을 기록합니다.	예	예
트래픽 모니터 오류 로그	L4TM 인터페이스 및 캡처 오류를 기록합니다.	예	예
트래픽 모니터 로그	L4TM 차단 및 허용 목록에 추가된 사이트를 기록합니다.	아니요	예
UDS 로그 (User Discovery Service)	실제 인증을 수행하지 않고 웹 프록시에서 사용자 이름을 검색하는 방법에 대한 데이터를 기록합니다. 여기에는 투명한 사용자 식별을 위한 Novell eDirectory 서버와의 통합과 모빌리티 보안를 위한 Cisco Adaptive Security Appliance와의 상호작용에 대한 정보가 포함됩니다.	예	예
Updater Logs	WBRS 및 기타 업데이트 내역을 기록합니다.	예	예
W3C 로그	웹 프록시 클라이언트 기록을 W3C 호환 형식으로 기록합니다. 자세한 내용은 W3C 호환 액세스 로그 파일, 21-24페이지를 참고하십시오.	예	아니요

로그 파일 유형	설명	Syslog 푸시 지원 여부	기본적으로 사용하도록 설정되는지 여부
WBNP 로그 (SensorBase Network Participation)	SensorBase 네트워크에 대한 Cisco SensorBase 네트워크 참여 업로드 내역을 기록합니다.	아니요	예
WBRS 프레임워크 로그 (Web Reputation Score)	웹 프록시와 웹 평판 필터 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
WCCP 모듈 로그	WCCP 구현과 관련된 웹 프록시 메시지를 기록합니다.	아니요	아니요
Webcat 통합 프레임워크 로그	Cisco Web Usage Controls와 연결된 URL 필터링 엔진과 웹 프록시 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Webroot 통합 프레임워크 로그	웹 프록시와 Webroot 스캐닝 엔진 간의 통신과 관련된 메시지를 기록합니다.	아니요	아니요
Webroot 로그	Webroot 스캐닝 엔진의 안티멀웨어 스캐닝 활동 상태를 기록합니다.	예	예
시작 페이지 승인 로그	최종 사용자 승인 페이지에서 Accept(수락) 버튼을 클릭하는 웹 클라이언트의 내역을 기록합니다.	예	예

로그 서브스크립션 추가 및 편집

각 로그 파일 유형마다 여러 로그 서브스크립션을 생성할 수 있습니다. 서브스크립션에는 다음을 포함하여 아카이브 및 스토리지에 대한 컨피그레이션 세부 정보가 포함됩니다.

- 로그 파일이 아카이브되는 시기를 결정하는 롤오버 설정
- 아카이브된 로그에 대한 압축 설정
- 로그가 원격 서버에 아카이브되거나 어플라이언스에 저장되는지를 지정하는 아카이브 로그에 대한 검색 설정

1단계 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**를 선택합니다.

2단계 로그 서브스크립션을 추가하려면 **Add Log Subscription(로그 서브스크립션 추가)**을 클릭합니다. 또는 로그 서브스크립션을 편집하려면 Log Name(로그 이름) 필드에서 로그 파일의 이름을 클릭합니다.

3단계 서브스크립션을 구성합니다.

옵션	설명
로그 유형	구독할 수 있는 사용 가능한 로그 파일 유형의 목록입니다. 이 페이지의 다른 옵션은 선택하는 로그 파일 유형에 따라 변경될 수 있습니다. **참고** 요청 디버그 로그 로그 유형은 CLI를 통해서만 구독할 수 있으며 이 목록에 표시되지 않습니다.

옵션	설명
로그 이름	웹 보안 어플라이언스에서 서브스크립션을 참조하는 데 사용되는 이름입니다. 이 이름은 서브스크립션을 위해 로그 파일을 저장할 로그 디렉토리에도 사용됩니다.
Rollover by File Size (파일 크기별 롤오버)	현재 로그 파일이 아카이브되고 새 로그 파일이 시작되기 전에 현재 로그 파일이 증가할 수 있는 최대 파일 크기입니다. 100KB에서 10GB 사이의 숫자를 입력합니다.
Rollover by Time(시간별 롤오버)	현재 로그 파일이 아카이브되고 새 로그 파일이 시작되기 전의 최대 시간 간격입니다. 다음 간격 유형을 사용할 수 있습니다. • **없음.** AsyncOS는 로그 파일이 최대 파일 크기에 도달할 때만 롤오버를 수행합니다. • **Custom Time Interval(사용자 지정 시간 간격).** AsyncOS는 이전 롤오버 이후 지정된 시간이 지나면 롤오버를 수행합니다. `d`, `h`, `m` 및 `s`를 접미사로 사용하여 롤오버 간격을 일, 시간, 분 및 초 단위로 입력합니다. • **Daily Rollover(매일 롤오버).** AsyncOS는 지정된 시간에 매일 롤오버를 수행합니다. 시간이 여러 개인 경우 쉼표를 사용하여 구분합니다. 하루 중 매시간 롤오버가 발생하도록 하려면 시간에 별표(*)를 사용합니다. 별표를 사용하여 매분 롤오버할 수도 있습니다. • **Weekly Rollover(매주 롤오버).** AsyncOS는 매주 하루 이상 지정된 시간에 롤오버를 수행합니다.
로그 스타일 (액세스 로그)	사용할 로그 형식(Squid, Apache 또는 Squid Details)을 지정합니다.

Custom Fields
(액세스 로그)
	각 액세스 로그 항목에 맞춤형 정보를 포함할 수 있습니다.
	맞춤형 필드에 형식 지정자를 입력하는 구문은 다음과 같습니다.
	`<format_specifier_1> <format_specifier_2> ...`
	예: `%a %b %E`
	액세스 로그 파일에서 설명 텍스트를 표시하기 위해 형식 지정자 앞에 토큰을 추가할 수 있습니다. 예를 들면 다음과 같습니다.
	`client_IP %a body_bytes %b error_type %E`
	여기서 `client_IP`는 로그 형식 지정자 `%a`에 대한 설명 토큰입니다.

파일 이름	로그 파일의 이름입니다. 현재 로그 파일은 `.c` 확장자와 함께 추가되고 롤오버된 로그 파일은 파일 생성 타임스탬프 및 `.s` 확장자와 함께 추가됩니다.

옵션	설명
로그 필드 (W3C 액세스 로그)	W3C 액세스 로그에 포함할 필드를 선택할 수 있습니다. Available Fields(사용 가능한 필드) 목록에서 필드를 선택하거나 Custom Field(맞춤형 필드) 상자에 필드를 입력한 후 Add(추가)를 클릭합니다. 필드가 Selected Log Fields(선택한 로그 필드) 목록에 표시되는 순서에 따라 W3C 액세스 로그 파일의 필드 순서가 결정됩니다. **Move Up(위로 이동)** 및 **Move Down(아래로 이동)** 버튼을 사용하여 필드의 순서를 변경할 수 있습니다. Selected Log Fields(선택한 로그 필드) 목록에서 필드를 선택하고 **Remove(제거)**를 클릭하여 필드를 제거할 수 있습니다. Custom Fields(맞춤형 필드) 상자에 여러 사용자 정의 필드를 입력하고 각 항목을 줄 바꿈(Enter 클릭)으로 구분한 다음 **Add(추가)**를 클릭하여 동시에 추가할 수 있습니다. W3C 로그 서브스크립션에 포함된 로그 필드를 변경하면 로그 서브스크립션이 자동으로 롤오버됩니다. 이를 통해 최신 버전의 로그 파일이 올바른 새 필드 헤더에 포함될 수 있습니다.
로그 압축	롤오버된 파일이 압축되는지 여부를 지정합니다. AsyncOS가 gzip 압축 형식을 사용하여 로그 파일을 압축합니다.
로그 제외(선택 사항) (액세스 로그)	액세스 로그 또는 W3C 액세스 로그에서 연결된 트랜잭션을 제외할 HTTP 상태 코드(4xx 또는 5xx만 해당)를 지정할 수 있습니다. 예를 들어, 401을 입력하면 해당 트랜잭션 번호를 포함한 인증 실패 요청이 필터링됩니다.
로그 레벨	로그 항목에 대한 세부 정보 레벨을 지정합니다. 다음 중에서 선택합니다. • **Critical(위험)**. 오류만 포함합니다. 가장 덜 세부적인 설정이며 syslog 레벨 "Alert"와 같습니다. • **Warning(경고)**. 오류 및 경고를 포함합니다. 이 로그 레벨은 syslog 레벨 "Warning"과 같습니다. • **Information(정보)**. 오류, 경고 및 추가 시스템 작업을 포함합니다. 기본 세부 정보 레벨이며 syslog 레벨 "Info"와 같습니다. • **Debug(디버그)**. 시스템 문제를 디버그하는 데 유용한 데이터를 포함합니다. 오류의 원인을 찾으려는 경우 디버그 로그 레벨을 사용합니다. 이 설정은 임시로 사용한 다음 기본 레벨로 돌려놓으십시오. 이 로그 레벨은 syslog 레벨 "Debug"와 같습니다. • **Trace(추적)**. 가장 세부적인 설정입니다. 이 레벨은 전체 시스템 작업 및 활동 레코드를 포함합니다. 추적 로그 레벨은 개발자들에게만 권장됩니다. 이 레벨을 사용하면 시스템 성능이 심각하게 저하되므로 사용하지 않는 것이 좋습니다. 이 로그 레벨은 syslog 레벨 "Debug"와 같습니다. **참고** 더 세부적인 설정일수록 로그 파일 크기가 더 커질 수 있으며 시스템 성능에도 더 많은 영향을 미칩니다.
검색 방법	롤오버된 로그 파일이 저장되는 위치와 읽기 위해 이러한 파일을 검색하는 방법을 지정합니다. 사용 가능한 방법에 대한 설명은 아래를 참조하십시오.

옵션	설명
검색 방법: 어플라이언스의 FTP	어플라이언스의 FTP 방법(FTP 폴링과 같음)에서는 어플라이언스에 액세스하는 원격 FTP 클라이언트가 관리자 또는 운영자 사용자의 사용자 이름 및 암호를 사용하여 로그 파일을 검색해야 합니다. 이 방법을 선택하는 경우 어플라이언스에 저장할 최대 로그 파일의 수를 입력해야 합니다. 최대 수에 도달하면 시스템에서 가장 오래된 파일을 삭제합니다. 이것이 기본 검색 방법입니다.
검색 방법: 원격 서버의 FTP	원격 서버의 FTP 방법(FTP 푸시와 같음)은 원격 컴퓨터에 있는 FTP 서버에 로그 파일을 주기적으로 푸시합니다. 이 방법을 선택하는 경우 다음 정보를 입력해야 합니다. • FTP 서버 호스트 이름 • 로그 파일을 저장할 FTP 서버의 디렉토리 • FTP 서버에 연결할 권한이 있는 사용자의 사용자 이름 및 암호 **참고** AsyncOS for Web은 원격 FTP 서버에 대해 수동 모드만 지원합니다. 활성 모드에서는 FTP 서버에 로그 파일을 푸시할 수 없습니다.
검색 방법: 원격 서버의 SCP	원격 서버의 SCP 방법(SCP 푸시와 같음)은 보안 복사 프로토콜을 사용하여 원격 SCP 서버에 로그 파일을 주기적으로 푸시합니다. 이 방법을 사용하려면 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 필요합니다. 서브스크립션에는 원격 컴퓨터의 사용자 이름, SSH 키 및 대상 디렉토리가 필요합니다. 사용자가 설정한 롤오버 일정을 기반으로 로그 파일이 전송됩니다. 이 방법을 선택하는 경우 다음 정보를 입력해야 합니다. • SCP 서버 호스트 이름 • 로그 파일을 저장할 SCP 서버의 디렉토리 • SCP 서버에 연결할 권한이 있는 사용자의 사용자 이름
검색 방법: Syslog Push	텍스트 기반 로그의 경우에만 syslog를 선택 할 수 있습니다. Syslog 푸시 방법은 포트 514에서 원격 syslog 서버에 로그 메시지를 전송합니다. 이 방법은 RFC 3164를 준수합니다. 이 방법을 선택하는 경우 다음 정보를 입력해야 합니다. • Syslog 서버 호스트 이름 • 전송에 사용할 프로토콜(UDP 또는 TCP) • Maximum message size(최대 메시지 크기) UDP의 경우 유효한 값은 1024 ~ 9216입니다. TCP의 경우 유효한 값은 1024 ~ 65535입니다. 최대 메시지 크기는 syslog 서버 컨피그레이션에 따라 다릅니다. • 로그와 함께 사용할 기능

단계 4 변경 사항을 제출 및 커밋합니다.

다음 작업

- SCP를 검색 방법으로 선택한 경우 어플라이언스에서 SSH 키를 표시하며, 이 SSH 키를 SCP 서버 호스트에 추가합니다. 로그 파일을 다른 서버에 푸시, 21-11페이지를 참조하십시오.

관련 항목

- 로그 파일 유형, 21-3페이지
- 로그 파일 이름 및 어플라이언스 디렉토리 구조, 21-12페이지

로그 파일을 다른 서버에 푸시

시작하기 전에

- SCP를 복구 방법으로 선택하여 원하는 로그 서브스크립션을 생성하거나 편집합니다. 로그 서브스크립션 추가 및 편집, 21-7페이지

1단계 원격 시스템에 키를 추가합니다.

a. CLI에 액세스합니다.

b. `logconfig -> hostkeyconfig` 명령을 입력합니다.

c. 아래 명령을 사용하여 키를 표시합니다.

명령	설명
Host	시스템 호스트 키를 표시합니다. 이 값은 원격 시스템의 'known_hosts' 파일에 배치할 값입니다.
User	원격 머신에 로그를 푸시하는 시스템 계정의 공개 키를 표시합니다. 이것은 SCP 푸시 서브스크립션을 설정할 때 표시되는 것과 동일한 키입니다. 이 값은 원격 시스템의 'authorized_keys' 파일에 배치할 값입니다.

d. 이러한 키를 원격 시스템에 추가합니다.

2단계 CLI에 있는 동안 원격 서버의 SSH 공개 호스트 키를 어플라이언스에 추가합니다.

명령	설명
New	새 키를 추가합니다.
Fingerprint	시스템 호스트 키 지문을 표시합니다.

e. 변경 사항을 커밋합니다.

로그 파일 아카이브

마지막 롤오버 이후 현재 로그 파일이 사용자가 지정한 최대 파일 크기 또는 최대 시간 제한에 도달하면 AsyncOS에서 로그 서브스크립션을 아카이브(롤오버)합니다.

다음과 같은 아카이브 설정이 로그 서브스크립션에 포함됩니다.

- Rollover by File Size(파일 크기별 롤오버)
- Rollover by Time(시간별 롤오버)
- 로그 압축
- 검색 방법

수동으로 로그 파일을 아카이브(롤오버)할 수도 있습니다.

1단계 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**를 선택합니다.

2단계 아카이브할 로그 서브스크립션의 Rollover(롤오버) 열에서 확인란을 선택하거나 모든 서브스크립션을 선택하려면 **All(모두)** 확인란을 선택합니다.

3단계 **Rollover Now(지금 롤오버)**를 클릭하여 선택한 로그를 아카이브합니다.

관련 주제

- 로그 서브스크립션 추가 및 편집, 21-7페이지
- 로그 파일 이름 및 어플라이언스 디렉토리 구조, 21-12페이지

로그 파일 이름 및 어플라이언스 디렉토리 구조

어플라이언스는 로그 서브스크립션 이름에 따라 각 로그 서브스크립션에 대한 디렉토리를 생성합니다. 디렉토리의 로그 파일 이름은 다음 정보로 구성됩니다.

- 로그 서브스크립션에 지정된 로그 파일 이름
- 로그 파일이 시작된 타임스탬프
- 단일 문자 상태 코드, `.c`(현재를 나타냄) 또는 `.s`(저장됨을 나타냄)

로그의 파일 이름은 다음 공식을 사용하여 만들어집니다.

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

참고 저장된 상태의 로그 파일만 전송해야 합니다.

로그 파일 읽기 및 해석

웹 보안 어플라이언스를 모니터링하고 트러블슈팅하는 방법으로 현재 로그 파일 활동을 읽을 수 있습니다. 어플라이언스 인터페이스를 사용하여 이를 수행합니다.

또한 이전 활동 레코드의 아카이브된 파일을 읽을 수 있습니다. 아카이브된 파일이 어플라이언스에 저장된 경우 어플라이언스 인터페이스를 사용하여 이를 수행할 수 있습니다. 그렇지 않은 경우 적절한 방법을 사용하여 외부 스토리지 위치에서 읽어야 합니다.

로그 파일에 있는 정보의 각 항목은 필드 변수로 표시됩니다. 어떤 필드가 어떤 정보 항목을 나타내는지를 확인하여 필드 기능을 조회하고 로그 파일 콘텐츠를 해석할 수 있습니다. W3C 호환 액세스 로그의 경우 필드 이름이 로그 항목에 표시되는 순서대로 파일 헤더에 나열됩니다. 그러나 표준 액세스 로그의 경우 이 로그 유형 관련 문서에서 필드 순서에 대한 정보를 참조해야 합니다.

관련 주제

- 로그 파일 보기, 21-13페이지.
- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- W3C 액세스 로그 해석, 21-25페이지.
- 트래픽 모니터 로그 해석, 21-30페이지.
- 로그 파일 필드 및 태그, 21-31페이지.

로그 파일 보기

시작하기 전에

- 이 보기 방법은 어플라이언스에 저장된 로그 파일에 해당됩니다. 외부에 저장된 파일을 보는 프로세스는 이 문서의 범위를 벗어납니다.

1단계 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**를 선택합니다.

2단계 로그 서브스크립션 목록의 Log Files(로그 파일) 열에서 로그 서브스크립션의 이름을 클릭합니다.

3단계 프롬프트가 표시되면 어플라이언스에 액세스하기 위한 관리자의 사용자 이름 및 암호를 입력합니다.

4단계 로그인되면 로그 파일 중 하나를 클릭하여 브라우저에서 보거나 디스크에 저장합니다.

5단계 업데이트된 결과를 보려면 브라우저를 새로 고칩니다.

참고 로그 서브스크립션이 압축된 경우 다운로드하여 압축을 푼 다음 엽니다.

관련 주제

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- W3C 액세스 로그 해석, 21-25페이지.
- 트래픽 모니터 로그 해석, 21-30페이지.

액세스 로그 파일의 웹 프록시 정보

액세스 로그 파일은 모든 웹 프록시 필터링 및 스캐닝 활동의 설명 레코드를 제공합니다. 액세스 로그 파일 항목에 어플라이언스가 각 트랜잭션을 처리한 방법에 대한 레코드가 표시됩니다.

액세스 로그는 표준 및 W3C 호환의 두 가지 형식으로 사용할 수 있습니다. W3C 호환 로그 파일은 표준 액세스 로그보다 더 세부적으로 콘텐츠 및 레이아웃을 맞춤화할 수 있습니다.

다음 텍스트는 단일 트랜잭션의 액세스 로그 파일 항목 예제입니다.

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain
DEFAULT_CASE_11-PolicyGroupName-Identity-OutboundMalwareScanningPolicy-DataSecurityPolic
y-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Un
known","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.p
df","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

형식 지정자	필드 값	필드 설명
%t	`1278096903.150`	UNIX Epoch 이후 타임스탬프.
%e	`97`	밀리초 단위의 경과 시간(레이턴시).
%a	`172.xx.xx.xx`	클라이언트 IP 주소. **참고:** `advancedproxyconfig > authentication` CLI 명령을 사용하여 액세스 로그에서 IP 주소를 마스킹하도록 선택할 수 있습니다.
%w	`TCP_MISS`	트랜잭션 결과 코드. 자세한 내용은 W3C 호환 액세스 로그 파일, 21-24페이지를 참고하십시오.
%h	`200`	HTTP 응답 코드.
%s	`8187`	응답 크기(헤더 + 본문).
%2r	`GET http://my.site.com/`	요청의 첫 번째 행. **참고:** 요청의 첫 번째 행이 네이티브 FTP 트랜잭션에 해당하는 경우 파일 이름의 일부 특수 문자가 액세스 로그에서 URL로 인코딩됩니다. 예를 들어, "@" 기호는 액세스 로그에서 "%40"으로 작성됩니다. 다음 문자가 URL로 인코딩됩니다. `& # % + , : ; = @ ^ { } [ ]`
%A	`-`	인증된 사용자. **참고:** `advancedproxyconfig > authentication` CLI 명령을 사용하여 액세스 로그에서 사용자 이름을 마스킹하도록 선택할 수 있습니다.

형식 지정자	필드 값	필드 설명
%H	DIRECT	요청 콘텐츠를 검색하기 위해 접속된 서버에 대해 설명하는 코드. 가장 일반적인 값은 다음과 같습니다. • **NONE.** 웹 프록시에 콘텐츠가 있으므로 콘텐츠를 검색하기 위해 다른 서버에 접속하지 않았습니다. • **DIRECT.** 웹 프록시가 콘텐츠를 가져오기 위해 요청에 명명된 서버로 이동했습니다. • **DEFAULT_PARENT.** 웹 프록시가 콘텐츠를 가져오기 위해 1차 상위 프록시 또는 외부 DLP 서버로 이동했습니다.
%d	my.site.com	데이터 소스 또는 서버 IP 주소.
%c	text/plain	응답 본문 MIME 유형.
%D	DEFAULT_CASE_11	ACL 결정 태그. **참고:** 웹 프록시에서 내부적으로 사용하는 동적으로 생성된 번호가 ACL 결정 태그의 끝에 포함됩니다. 이 번호는 무시할 수 있습니다. 자세한 내용은 ACL 결정 태그, 21-17페이지를 참고하십시오.
해당 없음(ACL 결정 태그의 일부)	PolicyGroupName	이 트랜잭션에 대한 최종 결정을 담당하는 정책 그룹의 이름(액세스 정책, 암호 해독 정책 또는 데이터 보안 정책). 트랜잭션이 전역 정책과 일치하는 경우 이 값은 "DefaultGroup"입니다. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.
해당 없음(ACL 결정 태그의 일부)	ID	ID 정책 그룹 이름. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.
해당 없음(ACL 결정 태그의 일부)	OutboundMalwareScanning Policy	아웃바운드 악성코드 스캐닝 정책 그룹 이름. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.
해당 없음(ACL 결정 태그의 일부)	DataSecurityPolicy	Cisco IronPort 데이터 보안 정책 그룹 이름. 트랜잭션이 전역 Cisco IronPort 데이터 보안 정책과 일치하는 경우 이 값은 "DefaultGroup"입니다. 이 정책 그룹 이름은 Cisco IronPort 데이터 보안 필터가 사용하도록 설정된 경우에만 표시됩니다. 데이터 보안 정책이 적용되지 않은 경우 "NONE"이 표시됩니다. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.
해당 없음(ACL 결정 태그의 일부)	ExternalDLPPolicy	외부 DLP 정책 그룹 이름. 트랜잭션이 전역 외부 DLP 정책과 일치하는 경우 이 값은 "DefaultGroup"입니다. 외부 DLP 정책이 적용되지 않은 경우 "NONE"이 표시됩니다. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.

형식 지정자	필드 값	필드 설명
해당 없음(ACL 결정 태그의 일부)	`RoutingPolicy`	*ProxyGroupName/ProxyServerName*인 라우팅 정책 그룹 이름. 트랜잭션이 전역 라우팅 정책과 일치하는 경우 이 값은 "DefaultRouting"입니다. 업스트림 프록시 서버가 사용되지 않는 경우 이 값은 "DIRECT"입니다. 정책 그룹 이름에 있는 공백은 밑줄(_)로 대체됩니다.
%Xr	`<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">`	스캐닝 판정 정보. 액세스 로그에서 꺾쇠괄호 안에 다양한 스캐닝 엔진의 판정 정보가 포함됩니다. 꺾쇠괄호 안에 포함된 값에 대한 자세한 내용은 액세스 로그 스캐닝 판정 항목 해석, 21-20페이지 및 악성코드 스캐닝 판정 값, 21-40페이지를 참조하십시오.
%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%.	-	의심되는 사용자 에이전트.

트랜잭션 결과 코드

액세스 로그 파일의 트랜잭션 결과 코드는 어플라이언스가 클라이언트 요청을 해결하는 방법에 대해 설명합니다. 예를 들어, 개체에 대한 요청을 캐시에서 해결할 수 있는 경우 결과 코드는 `TCP_HIT`입니다. 그러나 개체가 캐시에 없고 어플라이언스가 원래 서버에서 개체를 가져오는 경우 결과 코드는 `TCP_MISS`입니다. 다음 표에는 트랜잭션 결과 코드가 설명되어 있습니다.

결과 코드	설명
`TCP_HIT`	요청된 개체를 디스크 캐시에서 가져왔습니다.
`TCP_IMS_HIT`	클라이언트가 개체에 대한 IMS(If-Modified-Since) 요청을 전송했으며 캐시에서 개체를 찾았습니다. 프록시가 304 응답으로 응답합니다.
`TCP_MEM_HIT`	요청된 개체를 메모리 캐시에서 가져왔습니다.
`TCP_MISS`	개체를 캐시에서 찾지 못했으므로 원래 서버에서 가져왔습니다.
`TCP_REFRESH_HIT`	개체가 캐시에 있었지만 만료되었습니다. 프록시가 IMS(If-Modified-Since) 요청을 원래 서버로 전송했으며 서버에서 개체가 수정되지 않았음을 확인했습니다. 따라서 어플라이언스가 디스크 또는 메모리 캐시에서 개체를 가져왔습니다.
`TCP_CLIENT_REFRESH_MISS`	클라이언트가 'Pragma: no-cache' 헤더를 발행하여 "캐시에서 응답을 가져오지 않음" 요청을 전송했습니다. 클라이언트의 이 헤더로 인해 어플라이언스가 원래 서버에서 개체를 가져왔습니다.
`TCP_DENIED`	액세스 정책으로 인해 클라이언트 요청이 거부되었습니다.
`UDP_MISS`	개체를 원래 서버에서 가져왔습니다.
`NONE`	트랜잭션에 오류가 발생했습니다. 예를 들어, DNS 실패 또는 게이트웨이 시간 초과.

ACL 결정 태그

ACL 결정 태그는 웹 프록시의 트랜잭션 처리 방법을 표시하는 액세스 로그 항목의 필드입니다. 여기에는 웹 평판 필터, URL 카테고리 및 스캐닝 엔진에 대한 정보가 포함됩니다.

참고 성능 향상을 위해 웹 프록시에서 내부적으로 사용하는 동적으로 생성된 번호가 ACL 결정 태그의 끝에 포함됩니다. 이 번호는 무시할 수 있습니다.

다음 표에는 ACL 결정 태그 값이 설명되어 있습니다.

ACL 결정 태그	설명
ALLOW_ADMIN_ERROR_PAGE	웹 프록시에서 알림 페이지와 해당 페이지에 사용된 모든 로고에 대해 트랜잭션을 허용했습니다.
ALLOW_CUSTOMCAT	웹 프록시에서 액세스 정책 그룹의 맞춤형 URL 카테고리 필터링 설정에 따라 트랜잭션을 허용했습니다.
ALLOW_WBRS	웹 프록시에서 액세스 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션을 허용했습니다.
BLOCK_ADMIN	액세스 정책 그룹의 일부 기본 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_CONNECT	액세스 정책 그룹의 HTTP CONNECT 포트 설정에 정의된 대로 목적지의 TCP 포트에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_CUSTOM_USER_AGENT	액세스 정책 그룹의 맞춤형 사용자 에이전트 차단 설정에 정의된 대로 사용자 에이전트에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_HTTPS_NonLocalDestination	트랜잭션이 차단되었습니다. 클라이언트가 SSL 포트를 명시적 프록시로 사용하여 인증을 우회하려고 시도했습니다. 이를 방지하기 위해 SSL 연결이 WSA 자체에 대한 것인 경우 실제 WSA 리디렉션 호스트 이름에 대한 요청만 허용됩니다.
BLOCK_ADMIN_IDS	데이터 보안 정책 그룹에 정의된 대로 요청 본문 콘텐츠의 MIME 유형에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_FILE_TYPE	액세스 정책 그룹에 정의된 대로 파일 유형에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_PROTOCOL	액세스 정책 그룹의 프로토콜 차단 설정에 정의된 대로 프로토콜에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_SIZE	액세스 정책 그룹의 개체 크기 설정에 정의된 대로 응답의 크기에 따라 트랜잭션이 차단되었습니다.
BLOCK_ADMIN_SIZE_IDS	데이터 보안 정책 그룹에 정의된 대로 요청 본문 콘텐츠의 크기에 따라 트랜잭션이 차단되었습니다.
BLOCK_AMP_RESP	웹 프록시에서 액세스 정책 그룹의 Advanced Malware Protection 설정에 따라 응답을 차단했습니다.
BLOCK_AMW_REQ	웹 프록시에서 아웃바운드 악성코드 스캐닝 정책 그룹의 안티멀웨어 설정에 따라 요청을 차단했습니다. 요청 본문이 양의 악성코드 판정을 생성했습니다.
BLOCK_AMW_RESP	웹 프록시에서 액세스 정책 그룹의 안티멀웨어 설정에 따라 응답을 차단했습니다.

ACL 결정 태그	설명
BLOCK_AMW_REQ_URL	웹 프록시에서 HTTP 요청의 URL이 안전하지 않은 것으로 의심하여 액세스 정책 그룹의 안티멀웨어 설정에 따라 요청 시 트랜잭션을 차단했습니다.
BLOCK_AVC	액세스 정책 그룹에 대해 구성된 애플리케이션 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_CONTENT_UNSAFE	액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션이 차단되었습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이었으며 정책이 성인 콘텐츠를 차단하도록 구성되어 있습니다.
BLOCK_CONTINUE_CONTENT_UNSAFE	액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션이 차단되고 Warn and Continue(경고 후 계속) 페이지가 표시되었습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이었으며 성인 콘텐츠에 액세스하는 사용자에게 경고를 제공하도록 정책이 구성되어 있습니다.
BLOCK_CONTINUE_CUSTOMCAT	"경고"로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션이 차단되고 Warn and Continue(경고 후 계속) 페이지가 표시되었습니다.
BLOCK_CONTINUE_WEBCAT	"경고"로 구성된 액세스 정책 그룹의 미리 정의된 URL 카테고리에 따라 트랜잭션이 차단되고 Warn and Continue(경고 후 계속) 페이지가 표시되었습니다.
BLOCK_CUSTOMCAT	액세스 정책 그룹의 맞춤형 URL 카테고리 필터링 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_ICAP	웹 프록시에서 외부 DLP 정책 그룹에 정의된 대로 외부 DLP 시스템의 판정에 따라 요청을 차단했습니다.
BLOCK_SEARCH_UNSAFE	클라이언트 요청에 안전하지 않은 검색 쿼리가 포함되었으며 액세스 정책이 안전 검색을 시행하도록 구성되었으므로 원래 클라이언트 요청이 차단되었습니다.
BLOCK_SUSPECT_USER_AGENT	액세스 정책 그룹의 의심되는 사용자 에이전트 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_UNSUPPORTED_SEARCH_APP	액세스 정책 그룹의 안전 검색 설정에 따라 트랜잭션이 차단되었습니다. 트랜잭션이 지원되지 않은 검색 엔진에 대한 것이었으며 정책이 지원되지 않는 검색 엔진을 차단하도록 구성되어 있습니다.
BLOCK_WBRS	액세스 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_WBRS_IDS	웹 프록시에서 데이터 보안 정책 그룹의 웹 평판 필터 설정에 따라 업로드 요청을 차단했습니다.
BLOCK_WEBCAT	액세스 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션이 차단되었습니다.
BLOCK_WEBCAT_IDS	웹 프록시에서 데이터 보안 정책 그룹의 URL 카테고리 필터링 설정에 따라 업로드 요청을 차단했습니다.
DECRYPT_ADMIN	웹 프록시에서 암호 해독 정책 그룹의 일부 기본 설정에 따라 트랜잭션의 암호를 해독했습니다.
DECRYPT_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었지만 웹 프록시에서 트랜잭션의 암호를 해독했습니다.

ACL 결정 태그	설명
DECRYPT_WEBCAT	웹 프록시에서 암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션의 암호를 해독했습니다.
DECRYPT_WBRS	웹 프록시에서 암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션의 암호를 해독했습니다.
DEFAULT_CASE	웹 평판 또는 안티멀웨어 스캐닝과 같은 AsyncOS 서비스가 트랜잭션에 대해 아무 조치도 수행하지 않았으므로 웹 프록시에서 클라이언트가 서버에 액세스하도록 허용했습니다.
DROP_ADMIN	웹 프록시에서 암호 해독 정책 그룹의 일부 기본 설정에 따라 트랜잭션을 삭제했습니다.
DROP_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었으므로 웹 프록시에서 트랜잭션을 삭제했습니다.
DROP_WEBCAT	웹 프록시에서 암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 트랜잭션을 삭제했습니다.
DROP_WBRS	웹 프록시에서 암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션을 삭제했습니다.
MONITOR_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었으므로 웹 프록시에서 서버 응답을 모니터링했습니다.
MONITOR_AMP_RESP	웹 프록시에서 액세스 정책 그룹의 Advanced Malware Protection 설정에 따라 서버 응답을 모니터링했습니다.
MONITOR_AMW_RESP	웹 프록시에서 액세스 정책 그룹의 안티멀웨어 설정에 따라 서버 응답을 모니터링했습니다.
MONITOR_AMW_RESP_URL	웹 프록시에서 HTTP 요청의 URL이 안전하지 않은 것으로 의심했지만 액세스 정책 그룹의 안티멀웨어 설정에 따라 트랜잭션을 모니터링했습니다.
MONITOR_AVC	웹 프록시에서 액세스 정책 그룹의 애플리케이션 설정에 따라 트랜잭션을 모니터링했습니다.
MONITOR_CONTINUE_CONTENT_UNSAFE	원래, 웹 프록시에서 액세스 정책 그룹의 사이트 콘텐츠 등급 설정에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 클라이언트 요청이 성인 콘텐츠에 대한 요청이었으며 성인 콘텐츠에 액세스하는 사용자에게 경고를 제공하도록 정책이 구성되어 있습니다. 사용자가 경고를 승인하고 원래 요청된 사이트를 계속 진행했으며 이후에 다른 스캐닝 엔진이 요청을 차단하지 않았습니다.
MONITOR_CONTINUE_CUSTOMCAT	원래, 웹 프록시에서 "경고"로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 사용자가 경고를 승인하고 원래 요청된 사이트를 계속 진행했으며 이후에 다른 스캐닝 엔진이 요청을 차단하지 않았습니다.
MONITOR_CONTINUE_WEBCAT	원래, 웹 프록시에서 "경고"로 구성된 액세스 정책 그룹의 미리 정의된 URL 카테고리에 따라 트랜잭션을 차단하고 Warn and Continue(경고 후 계속) 페이지를 표시했습니다. 사용자가 경고를 승인하고 원래 요청된 사이트를 계속 진행했으며 이후에 다른 스캐닝 엔진이 요청을 차단하지 않았습니다.

ACL 결정 태그	설명
MONITOR_IDS	웹 프록시에서 데이터 보안 정책 또는 외부 DLP 정책을 사용하여 업로드 요청을 스캐닝했지만 요청을 차단하지 않았습니다. 액세스 정책과 비교하여 요청을 평가했습니다.
MONITOR_SUSPECT_USER_AGENT	웹 프록시에서 액세스 정책 그룹의 의심되는 사용자 에이전트 설정에 따라 트랜잭션을 모니터링했습니다.
MONITOR_WBRS	웹 프록시에서 액세스 정책 그룹의 웹 평판 필터 설정에 따라 트랜잭션을 모니터링했습니다.
NO_AUTHORIZATION	사용자가 이미 인증 영역에 대해 인증되었지만 애플리케이션 인증 정책에 구성된 인증 영역에 대해서는 인증되지 않았으므로 웹 프록시에서 애플리케이션에 대한 사용자 액세스를 허용하지 않았습니다.
NO_PASSWORD	사용자가 인증에 실패했습니다.
PASSTHRU_ADMIN	암호 해독 정책 그룹의 일부 기본 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_ADMIN_EXPIRED_CERT	서버 인증서가 만료되었지만 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_WEBCAT	암호 해독 정책 그룹의 URL 카테고리 필터링 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
PASSTHRU_WBRS	암호 해독 정책 그룹의 웹 평판 필터 설정에 따라 웹 프록시가 트랜잭션을 통과했습니다.
REDIRECT_CUSTOMCAT	웹 프록시에서 "리디렉션"으로 구성된 액세스 정책 그룹의 맞춤형 URL 카테고리에 따라 트랜잭션을 다른 URL로 리디렉션했습니다.
SAAS_AUTH	사용자가 애플리케이션 인증 정책에 구성된 인증 영역에 대해 투명하게 인증되었으므로 웹 프록시에서 애플리케이션에 대한 사용자 액세스를 허용했습니다.
기타	인증 실패, 서버 연결 해제 또는 클라이언트로부터 중단 등의 오류로 인해 웹 프록시가 요청을 완료하지 않았습니다.

액세스 로그 스캐닝 판정 항목 해석

액세스 로그 파일 항목은 다양한 스캐닝 엔진(예: URL 필터링, 웹 평판 필터링 및 안티멀웨어 스캐닝)의 결과를 집계하여 표시합니다. 어플라이언스가 각 액세스 로그 항목 끝에 꺾쇠괄호 안에 이 정보를 표시합니다.

다음 텍스트는 액세스 로그 파일 항목의 스캐닝 판정 정보입니다. 이 예에서는 Webroot 스캐닝 엔진이 악성코드를 발견했습니다.

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,"-",-,-,-,"-",-,-,"-","-",-,-,
IW_infr,-,"Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,-,[Local],"-"
,37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d
85829614fba368a421d14e64c426da5e">
```

참고 전체 액세스 로그 항목의 예는 액세스 로그 파일의 웹 프록시 정보, 21-14페이지를 참조하십시오.

이 예의 각 요소는 다음 표에 표시된 대로 로그 파일 형식 지정자와 대응됩니다.

위치	필드 값	형식 지정자	설명
1	IW_infr	%XC	트랜잭션에 할당된 약식 URL 카테고리. 카테고리가 할당되지 않은 경우 이 필드에 "nc"가 표시됩니다. URL 카테고리 약어 목록은 URL 카테고리 설명, 9-23페이지를 참조하십시오.
2	ns	%XW	웹 평판 필터 점수. 이 필드는 점수를 숫자로 표시하거나 점수가 없는 경우 "ns" 또는 DNS 조회 오류가 발생한 경우 "dns"로 표시합니다.
3	24	%Xv	Webroot에서 DVS 엔진에 전달한 악성코드 스캐닝 판정. Webroot에서 탐지된 응답에만 적용됩니다. 자세한 내용은 악성코드 스캐닝 판정 값, 21-40페이지를 참고하십시오.
4	"Trojan-Phisher-Gamec"	"%Xn"	개체와 연결된 스파이웨어의 이름. Webroot에서 탐지된 응답에만 적용됩니다.
5	0	%Xt	악성코드가 존재할 확률을 결정하는 TRR(Threat Risk Ratio) 값과 연결된 Webroot 특정 값. Webroot에서 탐지된 응답에만 적용됩니다.
6	354385	%Xs	Webroot에서 위협 식별자로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. Webroot에서 탐지된 응답에만 적용됩니다.
7	12559	%Xi	Webroot에서 추적 식별자로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. Webroot에서 탐지된 응답에만 적용됩니다.
8	-	%Xd	McAfee에서 DVS 엔진에 전달한 악성코드 스캐닝 판정. McAfee에서 탐지된 응답에만 적용됩니다. 자세한 내용은 악성코드 스캐닝 판정 값, 21-40페이지를 참고하십시오.
9	"-"	"%Xe"	McAfee에서 스캐닝한 파일의 이름. McAfee에서 탐지된 응답에만 적용됩니다.
10	-	%Xf	McAfee에서 스캐닝 오류로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. McAfee에서 탐지된 응답에만 적용됩니다.
11	-	%Xg	McAfee에서 탐지 유형으로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. McAfee에서 탐지된 응답에만 적용됩니다.
12	-	%Xh	McAfee에서 바이러스 유형으로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. McAfee에서 탐지된 응답에만 적용됩니다.
13	"-"	"%Xj"	McAfee에서 스캐닝한 바이러스의 이름. McAfee에서 탐지된 응답에만 적용됩니다.
14	-	%XY	Sophos에서 DVS 엔진에 전달한 악성코드 스캐닝 판정. Sophos에서 탐지된 응답에만 적용됩니다. 자세한 내용은 악성코드 스캐닝 판정 값, 21-40페이지를 참고하십시오.

위치	필드 값	형식 지정자	설명
15	-	%Xx	Sophos에서 스캐닝 반환 코드로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. Sophos에서 탐지된 응답에만 적용됩니다.
16	"-"	"%Xy"	Sophos에서 유해한 콘텐츠를 발견한 파일 위치. 비아카이브 파일의 경우 이 값은 파일 이름 자체입니다. 아카이브 파일의 경우 아카이브의 개체입니다(예: `archive.zip/virus.exe`). Sophos에서 탐지된 응답에만 적용됩니다.
17	"-"	"%Xz"	Sophos에서 위협 이름으로 사용하는 값. Cisco 고객 지원에서 문제를 트러블슈팅할 때 이 값을 사용합니다. Sophos에서 탐지된 응답에만 적용됩니다.
18	-	%Xl	Cisco 데이터 보안 정책의 Content(콘텐츠) 열에 있는 조치를 기반으로 하는 Cisco 데이터 보안 스캐닝 판정. 다음 목록에서는 이 필드에 가능한 값에 대해 설명합니다. • **0.** 허용 • **1.** Block • **-(하이픈).** Cisco 데이터 보안 필터에서 스캐닝을 시작하지 않았습니다. 이 값은 Cisco 데이터 보안 필터가 사용되지 않도록 설정되었거나 URL 카테고리 조치가 허용으로 설정된 경우에 표시됩니다.
19	-	%Xp	ICAP 응답에 제공된 결과를 기반으로 하는 외부 DLP 스캐닝 판정. 다음 목록에서는 이 필드에 가능한 값에 대해 설명합니다. • **0.** 허용 • **1.** Block • **-(하이픈).** 외부 DLP 서버에서 스캐닝을 시작하지 않았습니다. 이 값은 외부 DLP 스캐닝이 사용되지 않도록 설정되어 있거나 External DLP Policies(외부 DLP 정책) > Destinations(대상) 페이지의 제외 URL 카테고리로 인해 콘텐츠가 스캐닝되지 않은 경우 표시됩니다.
20	IW_infr	%XQ	요청 측 스캐닝 중에 결정된 약식 URL 카테고리 판정. URL 필터링이 사용되지 않도록 설정된 경우 이 필드에 하이픈(-)이 나열됩니다. URL 카테고리 약어 목록은 URL 카테고리 설명, 9-23페이지를 참조하십시오.
21	-	%XA	응답 측 스캐닝 중에 DCA(Dynamic Content Analysis) 엔진에서 결정된 약식 URL 카테고리 판정. Cisco Web Usage Controls URL 필터링 엔진에만 적용됩니다. DCS(Dynamic Content Analysis) 엔진이 사용하도록 설정되고 요청 시 카테고리가 할당되지 않은 경우(요청 측 스캐닝 판정에 "nc" 값이 나열됨)에만 적용됩니다. URL 카테고리 약어 목록은 URL 카테고리 설명, 9-23페이지를 참조하십시오.
22	"Trojan Phisher"	"%XZ"	어떤 스캐닝 엔진이 사용하도록 설정되었는지에 관계없이 악성 코드 카테고리를 제공하는 통합된 응답 측 안티멀웨어 스캐닝 판정. 서버 응답 스캐닝으로 인해 차단되거나 모니터링되는 트랜잭션에 적용됩니다.

위치	필드 값	형식 지정자	설명
23	"-"	"%Xk"	대상 웹 사이트가 나쁜 평판을 받도록 한 웹 평판 필터에서 반환된 위협 유형. 이 필드는 일반적으로 평판이 4 이하인 사이트의 경우 채워집니다.
24	"Unknown"	"%XO"	해당되는 경우 AVC 엔진에서 반환된 애플리케이션 이름. AVC 엔진이 사용하도록 설정된 경우에만 적용됩니다.
25	"Unknown"	"%Xu"	해당되는 경우 AVC 엔진에서 반환된 애플리케이션 유형. AVC 엔진이 사용하도록 설정된 경우에만 적용됩니다.
26	"-"	"%Xb"	해당되는 경우 AVC 엔진에서 반환된 애플리케이션 동작. AVC 엔진이 사용하도록 설정된 경우에만 적용됩니다.
27	"-"	"%XS"	안전 검색 스캐닝 판정. 이 값은 안전 검색 또는 사이트 콘텐츠 등급 기능이 트랜잭션에 적용되었는지를 나타냅니다. 가능한 값 목록은 성인 콘텐츠 액세스 기록, 9-16페이지를 참조하십시오.
28	489.73	%XB	요청을 제공하는 데 사용된 평균 대역폭(Kb/초).
29	0	%XT	대역폭 제한 제어 설정으로 인해 요청이 제한되었는지 여부를 나타내는 값이며, 여기서 "1"은 요청이 제한되었음을 나타내고 "0"은 제한되지 않았음을 나타냅니다.
30	[Local]	%l	요청을 작성한 사용자 유형, "[Local]" 또는 "[Remote]". AnyConnect Secure Mobility가 사용하도록 설정된 경우에만 적용됩니다. 사용하도록 설정되지 않은 경우 이 값은 하이픈(-)입니다.
31	"-"	"%X3"	어떤 스캐닝 엔진이 사용하도록 설정되었는지에 관계없이 통합된 요청 측 안티멀웨어 스캐닝 판정. 아웃바운드 악성코드 스캐닝 정책이 적용될 때 클라이언트 요청 스캐닝으로 인해 차단되거나 모니터링되는 트랜잭션에 적용됩니다.
32	"-"	"%X4"	적용 가능한 아웃바운드 악성코드 스캐닝 정책으로 인해 차단되거나 모니터링된 클라이언트 요청에 할당된 위협 이름. 이 위협 이름은 어떤 안티멀웨어 스캐닝 엔진이 사용하도록 설정되었는지와 관계가 없습니다.
33	37	%X#1#	Advanced Malware Protection 파일 스캐닝의 판정: • 0: 파일이 악성이 아닙니다. • 1: 파일 유형으로 인해 파일이 스캐닝되지 않았습니다. • 2: 파일 스캐닝이 시간 초과되었습니다. • 3: 스캐닝 오류 • 3보다 큼: 파일이 악성입니다.
34	"W32.CiscoTestVector"	%X#2#	Advanced Malware Protection 파일 스캐닝으로 결정된 위협 이름. "-"은 위협이 없음을 나타냅니다.
35	33	%X#3#	Advanced Malware Protection 파일 스캐닝의 평판 점수. 이 점수는 클라우드 평판 서비스가 파일에 대한 명확한 판정을 결정할 수 없는 경우에만 사용됩니다. 자세한 내용은 14장, "파일 평판 필터링 및 파일 분석."에서 위협 점수 및 평판 임계값에 대한 정보를 참조하십시오.

위치	필드 값	형식 지정자	설명
36	0	%X#4#	업로드 및 분석 요청의 표시기: "0"은 Advanced Malware Protection에서 분석을 위해 파일의 업로드를 요청하지 않았음을 나타냅니다. "1"은 Advanced Malware Protection에서 분석을 위해 파일의 업로드를 요청했음을 나타냅니다.
37	"WSA-INFECTED-FILE.pdf"	%X#5#	다운로드되고 분석되는 파일의 이름.
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e	%X#6#	이 파일에 대한 SHA-256 식별자.

각 형식 지정자의 기능에 대한 설명은 로그 파일 필드 및 태그, 21-31페이지를 참조하십시오.

관련 주제

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지
- 액세스 로그 맞춤화, 21-26페이지
- W3C 호환 액세스 로그 파일, 21-24페이지
- 로그 파일 보기, 21-13페이지
- 로그 파일 필드 및 태그, 21-31페이지

W3C 호환 액세스 로그 파일

웹 보안 어플라이언스는 웹 프록시 트랜잭션 정보를 기록하기 위한 두 가지 다른 로그 유형(액세스 로그 및 W3C 형식 액세스 로그)을 제공합니다. W3C 액세스 로그는 W3C(World Wide Web Consortium)와 호환되며 W3C ELF(Extended Log File) 형식의 트랜잭션 내역을 기록합니다.

- W3C 필드 유형, 21-24페이지
- W3C 액세스 로그 해석, 21-25페이지

W3C 필드 유형

W3C 액세스 로그 서브스크립션을 정의할 때 포함할 로그 필드(예: ACL 결정 태그 또는 클라이언트 IP 주소)를 선택해야 합니다. 다음 로그 필드 유형 중 하나를 포함할 수 있습니다.

- **미리 정의됨.** 웹 인터페이스에 선택할 수 있는 필드 목록이 포함되어 있습니다.
- **사용자 정의됨.** 미리 정의된 목록에 포함되지 않은 로그 필드를 입력할 수 있습니다.

W3C 액세스 로그 해석

W3C 액세스 로그를 해석할 때 다음 규칙 및 지침을 고려합니다.

- 관리자가 각 W3C 액세스 로그 서브스크립션에 기록되는 데이터를 결정하기 때문에 W3C 액세스 로그에 설정된 필드 형식이 없습니다.
- W3C 로그는 자체 설명 로그입니다. 파일 형식(필드 목록)이 각 로그 파일의 시작 부분에 있는 헤더에 정의됩니다.
- W3C 액세스 로그의 필드는 공백으로 구분됩니다.
- 필드에 특정 항목의 데이터가 포함되지 않은 경우 대신 하이픈(-)이 로그 파일에 포함됩니다.
- W3C 액세스 로그 파일의 각 행은 하나의 트랜잭션과 관련되며 각 행은 LF 시퀀스로 종료됩니다.
- W3C 로그 파일 헤더, 21-25페이지
- W3C 필드 접두사, 21-26페이지

W3C 로그 파일 헤더

각 W3C 로그 파일에는 파일의 시작 부분에 헤더 텍스트가 포함되어 있습니다. 각 행은 # 문자로 시작하고 로그 파일을 생성한 웹 보안 어플라이언스에 대한 정보를 제공합니다. 또한 W3C 로그 파일 헤더에는 파일 형식(필드 목록)이 포함되어 있으므로 로그 파일은 자체 설명 특성을 가집니다.

다음 표에서는 각 W3C 로그 파일의 시작 부분에 나열되는 헤더 필드에 대해 설명합니다.

헤더 필드	설명
버전	사용된 W3C ELF 형식의 버전입니다.
Date(날짜)	헤더(및 로그 파일)가 생성된 날짜 및 시간입니다.
System	"Management_IP - Management_hostname" 형식의 로그 파일을 생성한 웹 보안 어플라이언스입니다.
소프트웨어	이러한 로그를 생성한 소프트웨어입니다.
필드	로그에 기록된 필드입니다.

W3C 로그 파일 예:

```
#Version: 1.0

#Date: 2009-06-15 13:55:20

#System: 10.1.1.1 - wsa.qa

#Software: AsyncOS for Web 6.3.0

#Fields: timestamp x-elapsed-time c-ip x-resultcode-httpstatus sc-bytes cs-method
cs-url cs-username x-hierarchy-origin cs-mime-type x-acltag x-result-code
x-suspect-user-agent
```

W3C 필드 접두사

대부분의 W3C 로그 필드 이름에는 값을 가져오는 헤더(클라이언트 또는 서버)를 식별하는 접두사가 포함됩니다. 접두사가 없는 로그 필드는 트랜잭션과 관련된 컴퓨터와 관계없는 값을 참조합니다. 다음 표에는 W3C 로그 필드 접두사가 설명되어 있습니다.

접두사 헤더	설명
c	클라이언트
s	서버
cs	클라이언트에서 서버로
sc	서버에서 클라이언트로
x	애플리케이션 특정 식별자.

예를 들어, W3C 로그 필드 "cs-method"는 클라이언트에서 서버로 전송된 요청의 방법을 나타내고 "c-ip"는 클라이언트의 IP 주소를 나타냅니다.

관련 주제

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- 액세스 로그 맞춤화, 21-26페이지.
- 트래픽 모니터 로그 파일, 21-30페이지.
- 로그 파일 필드 및 태그, 21-31페이지.
- 로그 파일 보기, 21-13페이지.

액세스 로그 맞춤화

미리 정의된 필드 또는 사용자 정의 필드를 사용하여 네트워크 내의 웹 트래픽에 대한 포괄적인 정보를 캡처하기 위한 여러 다른 필드를 포함하도록 일반 로그 및 W3C 액세스 로그를 맞춤화할 수 있습니다.

관련 주제

- 미리 정의된 필드 목록은 로그 파일 필드 및 태그, 21-31페이지를 참조하십시오.
- 사용자 정의 필드에 대한 자세한 내용은 액세스 로그 사용자 정의 필드, 21-26페이지를 참조하십시오.

액세스 로그 사용자 정의 필드

미리 정의된 액세스 로그 및 W3C 로그 필드 목록에 HTTP/HTTPS 트랜잭션에서 기록하려는 모든 헤더 정보가 포함되어 있지 않으면 액세스 및 W3C 로그 서브스크립션을 구성할 때 Custom Fields(맞춤형 필드) 텍스트 상자에 사용자 정의 로그 필드를 입력할 수 있습니다.

맞춤형 로그 필드는 클라이언트 또는 서버에서 전송된 임의 헤더의 임의 데이터일 수 있습니다. 로그 서브스크립션에 추가된 헤더가 요청 또는 응답에 포함되지 않은 경우 로그 파일에 로그 필드 값으로 하이픈이 포함됩니다.

다음 표에는 액세스 및 W3C 로그에 사용할 구문이 정의되어 있습니다.

헤더 유형	액세스 로그 형식 지정자 구문	W3C 로그 맞춤형 필드 구문
클라이언트 애플리케이션의 헤더	%<*ClientHeaderName*:	cs(*ClientHeaderName*)
서버의 헤더	%<*ServerHeaderName*:	sc(*ServerHeaderName*)

예를 들어, 클라이언트 요청에 If-Modified-Since 헤더 값을 기록하려면 W3C 로그 서브스크립션에 대한 Custom Fields(맞춤형 필드) 상자에 다음 텍스트를 입력합니다.

```
cs(If-Modified-Since)
```

관련 주제

- 일반 액세스 로그 맞춤화, 21-27페이지.
- W3C 액세스 로그 맞춤화, 21-28페이지.

일반 액세스 로그 맞춤화

1단계 System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)를 선택합니다.

2단계 액세스 로그 서브스크립션을 편집하려면 액세스 로그 파일 이름을 클릭합니다.

3단계 Custom Field(맞춤형 필드)에 필요한 형식 지정자를 입력합니다.

맞춤형 필드에 형식 지정자를 입력하는 구문은 다음과 같습니다.

```
<format_specifier_1> <format_specifier_2> ...
```

예: `%a %b %E`

액세스 로그 파일에서 설명 텍스트를 표시하기 위해 형식 지정자 앞에 토큰을 추가할 수 있습니다. 예:

```
client_IP %a body_bytes %b error_type %E
```

여기서 `client_IP`는 로그 형식 지정자 `%a`에 대한 설명 토큰입니다.

참고 클라이언트 요청 또는 서버 응답의 헤더에 대한 맞춤형 필드를 생성할 수 있습니다.

4단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- 로그 파일 필드 및 태그, 21-31페이지.
- 액세스 로그 사용자 정의 필드, 21-26페이지.

W3C 액세스 로그 맞춤화

1단계 **System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)**를 선택합니다.

2단계 W3C 로그 서브스크립션을 편집하려면 W3C 로그 파일 이름을 클릭합니다.

3단계 Custom Field(맞춤형 필드) 상자에 필드를 입력하고 **Add(추가)**를 클릭합니다.

필드가 Selected Log Fields(선택한 로그 필드) 목록에 표시되는 순서에 따라 W3C 액세스 로그 파일의 필드 순서가 결정됩니다. **Move Up(위로 이동)** 및 **Move Down(아래로 이동)** 버튼을 사용하여 필드의 순서를 변경할 수 있습니다. Selected Log Fields(선택한 로그 필드) 목록에서 필드를 선택하고 **Remove(제거)**를 클릭하여 필드를 제거할 수 있습니다.

Custom Fields(맞춤형 필드) 상자에 여러 사용자 정의 필드를 입력하고 각 항목을 줄 바꿈(Enter 클릭)으로 구분한 다음 **Add(추가)**를 클릭하여 동시에 추가할 수 있습니다.

W3C 로그 서브스크립션에 포함된 로그 필드를 변경하면 로그 서브스크립션이 자동으로 롤오버됩니다. 이를 통해 최신 버전의 로그 파일이 올바른 새 필드 헤더에 포함될 수 있습니다.

참고 클라이언트 요청 또는 서버 응답의 헤더에 대한 맞춤형 필드를 생성할 수 있습니다.

4단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- W3C 호환 액세스 로그 파일, 21-24페이지.
- 로그 파일 필드 및 태그, 21-31페이지.
- 액세스 로그 사용자 정의 필드, 21-26페이지.
- CTA 특정 맞춤형 W3C 로그 구성, 21-28페이지.

CTA 특정 맞춤형 W3C 로그 구성

분석 및 보고를 위해 Cisco Cloud Web Security 서비스에 CTA(Cognitive Threat Analytics) 특정 맞춤형 W3C 액세스 로그를 "푸시"하도록 WSA를 구성할 수 있습니다. Cisco ScanCenter는 CWS(Cloud Web Security)의 관리 포털입니다.

시작하기 전에

- **SCP**를 자동 업로드 프로토콜로 선택하여 Cisco ScanCenter에서 WSA에 대한 디바이스 계정을 생성합니다(자세한 내용은 *Cisco ScanCenter 관리자 설명서*의 "프록시 디바이스 업로드" 섹션 참조). SCP(Secure Copy Protocol) 호스트 이름 및 WSA에 대해 생성된 사용자 이름(대/소문자 구분, 각 디바이스마다 다름)을 메모합니다.

1단계 W3C 액세스 로그 맞춤화, 21-28페이지의 지침에 따라 **W3C Logs(W3C 로그)**를 **Log Type(로그 유형)**으로 선택하여 새 W3C 액세스 로그 서브스크립션을 추가합니다.

2단계 설명이 포함된 **Log Name(로그 이름)**을 제공합니다.

3단계 **Selected Log Fields(선택한 로그 필드)** 목록에서 항목을 삭제합니다(모두 선택하고 **Remove(제거)** 클릭).

4단계 **Selected Log Fields(선택한 로그 필드)** 목록에 다음 필드를 추가합니다.

a. 다음을 복사하여 **Custom Fields(맞춤형 필드)** 상자에 붙여넣은 후 **Add(추가)**를 클릭합니다.

```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
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
```

5단계 **Rollover by File Size(파일 크기별 롤오버)**를 제공합니다. 이 경우에는 `500M`가 권장됩니다.

6단계 **Rollover by Time(시간별 롤오버)** 옵션을 선택합니다.

이러한 지침에 따라 **Rollover every:(롤오버 간격:)** 시간 간격과 함께 **Custom Time Interval(맞춤형 시간 간격)**을 사용하는 것이 좋습니다.

프록시 뒤의 사용자 수	권장되는 롤오버 기간
알 수 없음 또는 2000 미만	55분
2000 ~ 4000	30분
4000 ~ 6000	20분
6000 이상	10분

7단계 **Retrieval Method(검색 방법)**로 **SCP on Remote Server(원격 서버의 SCP)**를 선택하고 CWS 계정에서 CTA 서버 정보를 입력합니다.

a. **SCP Host(SCP 호스트)** 필드에 Cisco ScanCenter에서 제공된 SCP 호스트를 입력합니다(예: `etr.cloudsec.sco.cisco.com`).

b. **SCP Port(SCP 포트)** 필드에 `22`를 입력합니다.

c. **Directory(디렉토리)** 필드에 `/upload`를 입력합니다.

d. **Username(사용자 이름)** 필드에 Cisco ScanCenter에서 디바이스에 대해 생성된 사용자 이름을 입력합니다. 디바이스 사용자 이름은 대/소문자를 구분하고 각 프록시 디바이스마다 다릅니다.

e. **Enable Host Key Checking(호스트 키 확인 사용)**을 선택하고 **Automatically Scan(자동으로 스캐닝)**을 선택합니다.

8단계 WSA에서 **Submit(제출)**을 클릭합니다.

공개 SSH 키가 WSA에서 생성되고 관리 콘솔에 표시됩니다.

9단계 WSA에서 생성된 공개 SSH 키를 클립보드에 복사합니다.

10단계 Cisco ScanCenter 포털로 전환하고 적절한 디바이스 계정을 선택한 후 공개 SSH 키를 CTA Device Provisioning(CTA 디바이스 프로비저닝) 페이지에 붙여넣습니다. (자세한 내용은 *Cisco ScanCenter 관리자 설명서*의 "프록시 디바이스 업로드" 섹션을 참조하십시오.)

프록시 디바이스와 CTA 시스템 간의 인증에 성공하면 분석을 위해 프록시 디바이스의 로그 파일을 CTA 시스템에 업로드할 수 있습니다.

Cisco ScanCenter는 Cisco Cloud Web Security의 관리 포털입니다. http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html을 참조하십시오.

11단계 WSA로 다시 전환하여 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

참고 컨피그레이션 변경 사항을 커밋하면 WSA가 재시작되므로 연결된 사용자의 연결이 일시적으로 끊길 수 있습니다.

트래픽 모니터 로그 파일

레이어-4 트래픽 모니터 로그 파일은 레이어-4 모니터링 활동에 대한 자세한 레코드를 제공합니다. 레이어-4 트래픽 모니터 로그 파일 항목을 확인하여 방화벽 차단 목록 및 방화벽 허용 목록에 대한 업데이트를 추적할 수 있습니다.

트래픽 모니터 로그 해석

아래 예를 사용하여 트래픽 모니터 로그에 포함된 다양한 항목 유형을 해석합니다.

예: 1:

```
172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.
```

이 예에서는 일치하는 항목이 차단 목록 방화벽 항목이 됩니다. 레이어-4 트래픽 모니터가 어플라이언스를 통과한 DNS 요청을 기반으로 차단 목록에 있는 도메인 이름과 IP 주소를 일치시켰습니다. 그런 다음, IP 주소가 방화벽의 차단 목록에 입력됩니다.

예: 2:

```
172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow
list.
```

이 예에서는 일치하는 항목이 허용 목록 방화벽 항목이 됩니다. 레이어-4 트래픽 모니터가 도메인 이름 항목을 일치시키고 어플라이언스 허용 목록에 추가했습니다. 그런 다음, IP 주소가 방화벽의 허용 목록에 입력됩니다.

예: 3:

```
Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.
```

이 예에서는 레이어-4 트래픽 모니터가 내부 IP 주소와 차단 목록에 있는 외부 IP 주소 간에 전달된 데이터의 레코드를 기록합니다. 또한 레이어-4 트래픽 모니터가 차단이 아닌 모니터링으로 설정됩니다.

관련 주제

- 로그 파일 보기, 21-13페이지

로그 파일 필드 및 태그

- 액세스 로그 형식 지정자 및 W3C 로그 파일 필드, 21-31페이지
- 트랜잭션 결과 코드, 21-16페이지
- ACL 결정 태그, 21-17페이지
- 악성코드 스캐닝 판정 값, 21-40페이지

액세스 로그 형식 지정자 및 W3C 로그 파일 필드

로그 파일은 변수를 사용하여 각 로그 파일 항목을 구성하는 정보의 개별 항목을 표시합니다. 액세스 로그에서는 이러한 변수를 형식 지정자라고 하고 W3C 로그에서는 로그 필드라고 합니다. 각 형식 지정자에는 대응하는 로그 필드가 있습니다.

이러한 값을 표시하도록 액세스 로그를 구성하려면 액세스 로그 맞춤화, 21-26페이지 및 로그 서브스크립션 추가 및 편집, 21-7페이지에서 맞춤형 필드에 대한 정보를 참조하십시오.

다음 표에서 이러한 변수에 대해 설명합니다.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%:<1	x-p2s-first-byte-time	웹 프록시가 서버에 연결하기 시작한 순간부터 처음으로 서버에 작성할 수 있는 시간까지 소요되는 시간. 트랜잭션을 완료하기 위해 웹 프록시에서 여러 서버에 연결해야 하는 경우 해당 시간의 합계입니다.
%:<a	x-p2p-auth-wait-time	웹 프록시가 요청을 전송한 후 웹 프록시 인증 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:<b	x-p2s-body-time	헤더 이후 서버에 요청 본문을 작성할 때까지 대기하는 시간.
%:<d	x-p2p-dns-wait-time	웹 프록시에서 웹 프록시 DNS 프로세스에 DNS 요청을 전송하는 데 소요된 시간.
%:<h	x-p2s-header-time	첫 번째 바이트 이후 서버에 요청 헤더를 작성할 때까지 대기하는 시간.
%:<r	x-p2p-reputation-wait-time	웹 프록시가 요청을 전송한 후 웹 평판 필터에서 응답을 수신할 때까지 대기하는 시간.
%:<s	x-p2p-asw-req-wait-time	웹 프록시가 요청을 전송한 후 웹 프록시 안티스파이웨어 프로세스에서 판정을 수신할 때까지 대기하는 시간.
%:>1	x-s2p-first-byte-time	서버의 첫 번째 바이트에 대한 응답 대기 시간.
%:>a	x-p2p-auth-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 웹 프록시 인증 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:>b	x-s2p-body-time	헤더가 수신된 후 전체 응답 본문을 대기하는 시간.
%:>c	x-p2p-fetch-time	웹 프록시가 디스크 캐시에서 응답을 읽는 데 필요한 시간.
%:>d	x-p2p-dns-svc-time	웹 프록시 DNS 프로세스가 웹 프록시에 DNS 결과를 다시 전송하는 데 소요된 시간.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%:>h	x-s2p-header-time	첫 번째 응답 바이트 이후 서버 헤더를 대기하는 시간.
%:>r	x-p2p-reputation-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 웹 평판 필터에서 판정을 수신할 때까지 대기하는 시간.
%:>s	x-p2p-asw-req-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 웹 프록시 안티스파이웨어 프로세스에서 판정을 수신할 때까지 대기하는 시간.
%:1<	x-c2p-first-byte-time	새 클라이언트 연결의 첫 번째 요청 바이트를 대기하는 시간.
%:1>	x-p2c-first-byte-time	첫 번째 바이트가 클라이언트에 작성될 때까지 대기하는 시간.
%:A<	x-p2p-avc-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 AVC 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:A>	x-p2p-avc-wait-time	웹 프록시가 요청을 전송한 후 AVC 프로세스에서 응답을 수신할 때까지 대기하는 시간.
%:b<	x-c2p-body-time	전체 클라이언트 본문을 대기하는 시간.
%:b>	x-p2c-body-time	전체 본문이 클라이언트에 작성될 때까지 대기하는 시간.
%:C<	x-p2p-dca-resp-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 DCA(Dynamic Content Analysis) 엔진에서 판정을 수신할 때까지 대기하는 시간.
%:C>	x-p2p-dca-resp-wait-time	웹 프록시가 요청을 전송한 후 DCA(Dynamic Content Analysis) 엔진에서 응답을 수신할 때까지 대기하는 시간.
%:h<	x-c2p-header-time	첫 번째 바이트 이후 전체 클라이언트 헤더를 대기하는 시간.
%:h>	x-s2p-header-time	전체 헤더가 클라이언트에 작성될 때까지 대기하는 시간.
%:m<	x-p2p-mcafee-resp-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 McAfee 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간.
%:m>	x-p2p-mcafee-resp-wait-time	웹 프록시가 요청을 전송한 후 McAfee 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.
%:p<	x-p2p-sophos-resp-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 Sophos 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간.
%:p>	x-p2p-sophos-resp-wait-time	웹 프록시가 요청을 전송한 후 Sophos 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.
%:w<	x-p2p-webroot-resp-svc-time	웹 프록시에서 요청을 전송하는 데 필요한 시간을 포함하여 Webroot 스캐닝 엔진에서 판정을 수신할 때까지 대기하는 시간.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%:w>	x-p2p-webroot-resp-wait-time	웹 프록시가 요청을 전송한 후 Webroot 스캐닝 엔진에서 응답을 수신할 때까지 대기하는 시간.
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:%!%-%.	x-suspect-user-agent	해당되는 경우 의심되는 사용자 에이전트. 웹 프록시에서 사용자 에이전트가 의심되는 것으로 판별하는 경우 이 필드에 사용자 에이전트를 기록합니다. 그렇지 않은 경우 하이픈을 기록합니다. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%<Referer:	cs(Referer)	참조자
%>Server:	sc(Server)	응답의 서버 헤더.
%a	c-ip	클라이언트 IP 주소.
%A	cs-username	인증된 사용자 이름. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%b	sc-body-size	웹 프록시에서 클라이언트에 전송된 본문 콘텐츠의 바이트 수.
%B	bytes	사용된 총 바이트 수(요청 크기 + 응답 크기, 즉 %q + %s).
%c	cs-mime-type	응답 본문 MIME 유형. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%C	cs(Cookie)	쿠키 헤더. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%d	s-hostname	데이터 소스 또는 서버 IP 주소.
%D	x-acltag	ACL 결정 태그.
%e	x-elapsed-time	밀리초 단위의 경과 시간. TCP 트래픽의 경우 HTTP 연결을 열고 닫은 시간 사이에 경과된 시간입니다. UDP 트래픽의 경우 첫 번째 데이터그램을 전송한 시간과 마지막 데이터그램이 승인될 수 있는 시간 사이에 경과된 시간입니다. UDP 트래픽의 경과 시간 값이 큰 경우 시간 초과 값이 크고 필요한 것보다 더 길게 데이터그램을 승인할 수 있는 수명이 긴 UDP 연관을 의미할 수 있습니다.
%E	x-error-code	고객 지원에서 실패한 트랜잭션의 이유를 트러블슈팅하는 데 도움이 될 수 있는 오류 코드 번호.
%f	cs(X-Forwarded-For)	X-Forwarded-For 헤더.
%F	c-port	클라이언트 소스 포트
%g	cs-auth-group	인증된 그룹 이름. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다. 이 필드는 정책/인증 문제 트러블슈팅을 위해 사용자가 올바른 그룹 또는 정책과 일치하는지 여부를 확인하는 데 사용됩니다.
%h	sc-http-status	HTTP 응답 코드.
%H	s-hierarchy	계층 구조 검색.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%i	x-icap-server	요청을 처리하는 동안 마지막으로 접속된 ICAP 서버의 IP 주소.
%I	x-transaction-id	트랜잭션 ID.
%j	DCF	응답 코드(DCF 플래그)를 캐시하지 않습니다. 응답 코드 설명: • 클라이언트 요청에 기반한 응답 코드: – 1 = 요청에 "no-cache" 헤더가 있습니다. – 2 = 요청에 대한 캐싱이 인증되지 않았습니다. – 4 = 요청에서 'Variant' 헤더가 누락되었습니다. – 8 = 사용자 요청에 대한 사용자 이름 또는 암호가 필요합니다. – 20 = 지정된 HTTP 메서드에 대한 응답입니다. • 어플라이언스에서 수신된 응답에 기반한 응답 코드: – 40 = 응답에 "Cache-Control: private" 헤더가 포함되어 있습니다. – 80 = 응답에 "Cache-Control: no-store" 헤더가 포함되어 있습니다. – 100 = 요청이 쿼리였음이 응답에 표시되어 있습니다. – 200 = 응답의 "Expires" 값이 작습니다(곧 만료됨). – 400 = 응답에 "Last Modified" 헤더가 없습니다. – 1000 = 응답이 즉시 만료됩니다. – 2000 = 응답 파일이 너무 커서 캐시할 수 없습니다. – 20000 = 파일의 새 사본이 존재합니다. – 40000 = 응답의 "Vary" 헤더에 잘못된/유효하지 않은 값이 있습니다. – 80000 = 응답에 쿠키 설정이 필요합니다. – 100000 = 캐시 불가능 HTTP STATUS 코드입니다. – 200000 = 어플라이언스에서 수신된 개체가 완전하지 않습니다(크기에 따라). – 800000 =응답 트레일러가 캐싱 안 함을 표시합니다. – 1000000 = 응답에 다시 쓰기가 필요합니다.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%k	s-ip	데이터 소스 IP 주소(서버 IP 주소) 이 값은 IP 주소가 네트워크에서 침입 탐지 디바이스로 플래그 지정된 경우 요청자를 확인하는 데 사용됩니다. 이와 같이 플래그가 지정된 IP 주소를 방문한 클라이언트를 찾을 수 있습니다.
%l	user-type	사용자 유형(로컬 또는 원격).
%L	x-local_time	사용자가 읽을 수 있는 DD/MMM/YYYY : hh:mm:ss +nnnn 형식의 요청 로컬 시간. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다. 이 필드를 사용하도록 설정하면 각 로그 항목에 대한 Epoch 시간으로부터 로컬 시간을 계산할 필요 없이 로그와 문제의 상관관계를 지정할 수 있습니다.
%m	cs-auth-mechanism	인증 문제를 트러블슈팅하는 데 사용됩니다. 트랜잭션에서 사용되는 인증 메커니즘. 가능한 값은 다음과 같습니다. • **BASIC.** 사용자 이름이 Basic 인증 체계를 사용하여 인증되었습니다. • **NTLMSSP.** 사용자 이름이 NTLMSSP 인증 체계를 사용하여 인증되었습니다. • **Kerberos.** 사용자 이름이 Kerberos 인증 체계를 사용하여 인증되었습니다. • **SSO_TUI.** 투명한 사용자 식별을 사용하여 클라이언트 IP 주소를 인증된 사용자 이름과 일치시켜서 사용자 이름을 가져왔습니다. • **SSO_ISE.** ISE 서버에서 사용자를 인증했습니다. (ISE 인증에 대한 대체 메커니즘으로 선택된 경우 로그에 GUEST가 표시됩니다.) • **SSO_ASA.** 사용자가 원격 사용자이고 모빌리티 보안를 사용하여 Cisco ASA에서 사용자 이름을 가져왔습니다. • **FORM_AUTH.** 애플리케이션에 액세스할 때 사용자가 웹 브라우저의 양식에 인증 자격 증명을 입력했습니다. • **GUEST.** 사용자가 인증에 실패하고 대신 게스트 액세스 권한이 부여되었습니다.
%M	CMF	캐시 누락 플래그: CMF 플래그.
%N	s-computerName	서버 이름 또는 대상 호스트 이름. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%p	s-port	대상 포트 번호.
%P	cs-version	프로토콜.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%q	cs-bytes	요청 크기(헤더 + 본문).
%r	x-req-first-line	요청 첫 번째 행 - 요청 메서드, URI.
%s	sc-bytes	응답 크기(헤더 + 본문).
%t	timestamp	UNIX Epoch의 타임스탬프. **참고:**서드파티 로그 분석기 툴을 사용하여 W3C 액세스 로그를 읽고 구문 분석하려는 경우 "timestamp(타임스탬프)" 필드를 포함해야 할 수 있습니다. 대부분의 로그 분석기는 이 필드에서 제공된 형식의 시간만 이해합니다.
%u	cs(User-Agent)	사용자 에이전트. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다. 이 필드는 애플리케이션이 인증에 실패하는지 여부 및/또는 다른 액세스 권한이 필요한지 여부를 확인하는 데 도움이 됩니다.
%U	cs-uri	요청 URI.
%v	date	YYYY-MM-DD 형식의 날짜.
%V	time	HH:MM:SS 형식의 시간.
%w	sc-result-code	결과 코드. 예: TCP_MISS, TCP_HIT.
%W	sc-result-code-denial	결과 코드 거부.
%x	x-latency	레이턴시.
%X0	x-resp-dvs-scanverdict	어떤 스캐닝 엔진이 사용하도록 설정되었는지에 관계없이 *악성코드 카테고리 번호*를 제공하는 통합된 응답 측 안티멀웨어 스캐닝 판정. 서버 응답 스캐닝으로 인해 차단되거나 모니터링되는 트랜잭션에 적용됩니다. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%X1	x-resp-dvs-threat-name	어떤 스캐닝 엔진이 사용하도록 설정되었는지에 관계없이 *멀웨어 위협 이름*을 제공하는 통합된 응답 측 안티멀웨어 스캐닝 판정. 서버 응답 스캐닝으로 인해 차단되거나 모니터링되는 트랜잭션에 적용됩니다. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%X2	x-req-dvs-scanverdict	요청 측 DVS 스캐닝 판정
%X3	x-req-dvs-verdictname	요청 측 DVS 판정 이름
%X4	x-req-dvs-threat-name	요청 측 DVS 위협 이름

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%X6	x-as-malware-threat-name	적응형 스캐닝이 안티멀웨어 스캐닝 엔진을 호출하지 않고 트랜잭션을 차단했는지 여부를 나타냅니다. 가능한 값은 다음과 같습니다. • **1.** 트랜잭션이 차단되었습니다. • **0.** 트랜잭션이 차단되지 않았습니다. 이 변수는 스캐닝 판정 정보에 포함됩니다(각 액세스 로그 항목의 끝에 꺾쇠괄호 안에 포함됨).
%XA	x-webcat-resp-code-abbr	응답 측 스캐닝 중에 결정된 약식 URL 카테고리 판정. Cisco Web Usage Controls URL 필터링 엔진에만 적용됩니다.
%Xb	x-avc-behavior	AVC 엔진에서 식별된 웹 애플리케이션 동작.
%XB	x-avg-bw	AVC 엔진에서 대역폭 제한을 정의하는 경우 사용자의 평균 대역폭.
%XC	x-webcat-code-abbr	트랜잭션에 할당된 URL 카테고리에 대한 URL 카테고리 약어.
%Xd	x-mcafee-scanverdict	McAfee 특정 식별자: (스캐닝 판정).
%Xe	x-mcafee-filename	McAfee 특정 식별자: (판정을 생성하는 파일 이름). 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%Xf	x-mcafee-av-scanerror	McAfee 특정 식별자: (스캐닝 오류).
%XF	x-webcat-code-full	트랜잭션에 할당된 URL 카테고리의 전체 이름. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%Xg	x-mcafee-av-detecttype	McAfee 특정 식별자: (탐지 유형).
%XG	x-avc-reqhead-scanverdict	AVC 요청 헤더 판정.
%Xh	x-mcafee-av-virustype	McAfee 특정 식별자: (바이러스 유형).
%XH	x-avc-reqbody-scanverdict	AVC 요청 본문 판정.
%Xi	x-webroot-trace-id	Webroot 특정 스캐닝 식별자: (추적 ID).
%Xj	x-mcafee-virus-name	McAfee 특정 식별자: (바이러스 이름). 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%Xk	x-wbrs-threat-type	웹 평판 위협 유형.
%XK	x-wbrs-threat-reason	웹 평판 위협 이유.
%Xl	x-ids-verdict	Cisco 데이터 보안 정책 스캐닝 판정. 이 필드가 포함된 경우 IDS 판정을 표시하거나, IDS가 활성화되었지만 문서가 클린 상태로 스캐닝된 경우 "0" 또는 요청에 대한 IDS 정책이 활성화되지 않은 경우 "-"을 표시합니다.
%XL	x-webcat-resp-code-full	응답 측 스캐닝 중에 결정된 URL 카테고리 판정의 전체 이름. Cisco Web Usage Controls URL 필터링 엔진에만 적용됩니다.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%XM	x-avc-resphead-scanverdict	AVC 응답 헤더 판정.
%Xn	x-webroot-threat-name	Webroot 특정 식별자: (위협 이름). 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%XN	x-avc-reqbody-scanverdict	AVC 응답 본문 판정.
%XO	x-avc-app	AVC 엔진에서 식별된 웹 애플리케이션.
%Xp	x-icap-verdict	외부 DLP 서버 스캐닝 판정.
%XP	x-acl-added-headers	인식되지 않은 헤더. 이 필드를 사용하여 클라이언트 요청에 추가 헤더를 기록합니다. 이는 클라이언트 요청을 인증하고 리디렉션하는 방법으로 해당 요청에 헤더를 추가하는 특수 시스템의 트러블슈팅을 지원합니다(예: YouTube for Schools).
%XQ	x-webcat-req-code-abbr	요청 측 스캐닝 중에 결정된 약식 URL 카테고리 판정.
%Xr	x-result-code	스캐닝 판정 정보.
%XR	x-webcat-req-code-full	요청 측 스캐닝 중에 결정된 URL 카테고리 판정의 전체 이름.
%Xs	x-webroot-spyid	Webroot 특정 식별자: (스파이 ID).
%XS	x-request-rewrite	안전 검색 스캐닝 판정. 안전 검색 또는 사이트 콘텐츠 등급 기능이 트랜잭션에 적용되었는지를 표시합니다.
%Xt	x-webroot-trr	Webroot 특정 식별자: (TRR(Threat Risk Ratio)).
%XT	x-bw-throttled	대역폭 제한이 트랜잭션에 적용되었는지 여부를 표시하는 플래그.
%Xu	x-avc-type	AVC 엔진에서 식별된 웹 애플리케이션 유형.
%Xv	x-webroot-scanverdict	Webroot의 악성코드 스캐닝 판정.
%XV	x-request-source-ip	웹 프록시 설정에 대한 "Enable Identification of Client IP Addresses using X-Forwarded-For (X-Forwarded-For를 사용하여 클라이언트 IP 주소의 식별 사용)" 확인란이 사용하도록 설정된 경우 다운스트림 IP 주소.
%XW	x-wbrs-score	디코딩된 WBRS 점수 <-10.0-10.0>.
%Xx	x-sophos-scanerror	Sophos 특정 식별자: (스캐닝 반환 코드).
%Xy	x-sophos-file-name	Sophos에서 유해한 콘텐츠를 발견한 파일 위치. 비아카이브 파일의 경우 이 값은 파일 이름 자체입니다. 아카이브 파일의 경우 아카이브의 개체입니다(예: `archive.zip/virus.exe`).
%XY	x-sophos-scanverdict	Sophos 특정 식별자: (스캐닝 판정).
%Xz	x-sophos-virus-name	Sophos 특정 식별자: (위협 이름).

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%XZ	x-resp-dvs-verdictname	어떤 스캐닝 엔진이 사용하도록 설정되었는지에 관계없이 *악성코드 카테고리*를 제공하는 통합된 응답 측 안티멀웨어 스캐닝 판정. 서버 응답 스캐닝으로 인해 차단되거나 모니터링되는 트랜잭션에 적용됩니다. 이 필드는 액세스 로그에 큰따옴표를 사용하여 기록됩니다.
%X#1#	x-amp-verdict	Advanced Malware Protection 파일 스캐닝의 판정: • 0: 파일이 악성이 아닙니다. • 1: 파일 유형으로 인해 파일이 스캐닝되지 않았습니다. • 2: 파일 스캐닝이 시간 초과되었습니다. • 3: 스캐닝 오류. • 3보다 큼: 파일이 악성입니다.
%X#2#	x-amp-malware-name	Advanced Malware Protection 파일 스캐닝으로 결정된 위협 이름. "-"은 위협이 없음을 나타냅니다.
%X#3#	x-amp-score	Advanced Malware Protection 파일 스캐닝의 평판 점수. 이 점수는 클라우드 평판 서비스가 파일에 대한 명확한 판정을 결정할 수 없는 경우에만 사용됩니다. 자세한 내용은 14장, "파일 평판 필터링 및 파일 분석."에서 위협 점수 및 평판 임계값에 대한 정보를 참조하십시오.
%X#4#	x-amp-upload	업로드 및 분석 요청의 표시기: "0"은 Advanced Malware Protection에서 분석을 위해 파일의 업로드를 요청하지 않았음을 나타냅니다. "1"은 Advanced Malware Protection에서 분석을 위해 파일의 업로드를 요청했음을 나타냅니다.
%X#5#	x-amp-filename	다운로드되고 분석되는 파일의 이름.
%X#6#	x-amp-sha	이 파일에 대한 SHA-256 식별자.
%y	cs-method	메서드.
%Y	cs-url	전체 URL.
해당 없음	x-hierarchy-origin	요청 콘텐츠를 검색하기 위해 접속된 서버에 대해 설명하는 코드(예: DIRECT/www.example.com).
해당 없음	x-resultcode-httpstatus	사이에 슬래시(/)가 있는 결과 코드 및 HTTP 응답 코드.

관련 주제

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- W3C 액세스 로그 해석, 21-25페이지.

악성코드 스캐닝 판정 값

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

다음 목록에는 여러 악성코드 스캐닝 판정 값과 각각에 해당하는 악성코드 카테고리가 나열되어 있습니다.

악성코드 스캐닝 판정 값	악성프로그램 범주
-	설정되지 않음
0	알 수 없음
1	검색되지 않음
2	시간 초과
3	오류
4	Unscannable(검색할 수 없음)
10	일반 스파이웨어
12	브라우저 헬퍼 개체
13	애드웨어
14	시스템 모니터
18	상업용 시스템 모니터
19	다이얼러
20	하이잭커
21	피싱 URL
22	트로이 목마 다운로더
23	트로이 목마
24	트로이 피셔
25	웜
26	암호화된 파일
27	바이러스
33	기타 악성 코드
34	PUA
35	중단됨
36	발생 휴리스틱
37	알려진 악성 및 고위험 파일

관련 주제

- 액세스 로그 파일의 웹 프록시 정보, 21-14페이지.
- W3C 액세스 로그 해석, 21-25페이지.

로깅 트러블슈팅

- 맞춤형 URL 카테고리가 액세스 로그 항목에 표시되지 않음, A-12페이지
- HTTPS 트랜잭션 기록, A-12페이지
- 경고: 생성되는 데이터의 비율을 유지할 수 없음, A-13페이지
- 서드파티 로그 분석기 툴을 통한 W3C 액세스 로그 사용 문제, A-13페이지

시스템 관리 작업 수행

- 시스템 관리 개요, 22-1페이지
- 어플라이언스 컨피그레이션 저장, 로드 및 재설정, 22-2페이지
- 기능 키에 대한 작업, 22-4페이지
- 가상 어플라이언스 라이센스, 22-5페이지
- 원격 전원 관리 활성화, 22-5페이지
- 사용자 계정 관리, 22-6페이지
- 사용자 환경 설정 정의, 22-11페이지
- 관리자 설정 구성, 22-11페이지
- 생성된 메시지에 대한 반환 주소 구성, 22-13페이지
- 경고 관리, 22-14페이지
- FIPS 컴플라이언스, 22-21페이지
- SSL 컨피그레이션, 22-23페이지
- 시스템 날짜 및 시간 관리, 22-22페이지
- 인증서 관리, 22-24페이지
- AsyncOS for Web 업그레이드 및 업데이트, 22-27페이지
- 이전 버전의 AsyncOS for Web으로 되돌리기, 22-33페이지
- SNMP를 사용하여 시스템 상태 모니터링, 22-35페이지

시스템 관리 개요

S-Series 어플라이언스는 시스템을 관리하기 위한 다양한 툴을 제공합니다. System Administration(시스템 관리) 탭의 기능을 통해 다음 작업을 관리할 수 있습니다.

- 어플라이언스 컨피그레이션
- 기능 키
- 사용자 계정 추가, 편집 및 제거
- AsyncOS 소프트웨어 업그레이드 및 업데이트
- 시스템 시간

어플라이언스 컨피그레이션 저장, 로드 및 재설정

웹 보안 어플라이언스 내의 모든 컨피그레이션 설정은 단일 XML 컨피그레이션 파일을 사용하여 관리합니다.

- 어플라이언스 컨피그레이션 보기 및 인쇄, 22-2페이지
- 어플라이언스 컨피그레이션 파일 저장, 22-2페이지
- 어플라이언스 컨피그레이션 파일 로드, 22-3페이지
- 어플라이언스 컨피그레이션을 공장 기본값으로 재설정, 22-3페이지

어플라이언스 컨피그레이션 보기 및 인쇄

1단계 **System Administration(시스템 관리) > Configuration Summary(컨피그레이션 요약)**를 선택합니다.

2단계 필요에 따라 Configuration Summary(컨피그레이션 요약) 페이지를 보거나 인쇄합니다.

어플라이언스 컨피그레이션 파일 저장

1단계 **System Administration(시스템 관리) > Configuration File(컨피그레이션 파일)**을 선택합니다.

2단계 컨피그레이션 파일 옵션을 완료합니다.

옵션	설명
다음 위치 옵션 중에서 선택합니다. • 파일을 로컬 컴퓨터로 다운로드하여 보거나 저장합니다. • 파일을 이 어플라이언스(example.com)에 저장 • 다음 사용자에게 이메일로 파일 보내기	파일을 저장할 위치를 선택할 수 있습니다.
컨피그레이션 파일에서 암호 마스크	사용하도록 설정된 경우 내보내거나 저장한 파일의 암호화된 원래 암호가 "*****"로 바뀝니다. 그러나 암호가 마스크 처리된 컨피그레이션 파일은 직접 AsyncOS for Web으로 다시 로드할 수 없습니다.
다음 파일 이름 옵션 중에서 선택합니다. • 시스템 생성 파일 이름 사용 • 사용자 정의 파일 이름 사용:	컨피그레이션 파일 이름 지정 방법을 선택할 수 있습니다.

3단계 **Submit(제출)**을 클릭합니다.

어플라이언스 컨피그레이션 파일 로드

주의 컨피그레이션을 로드하면 현재 컨피그레이션 설정이 모두 영구적으로 제거됩니다. 이러한 조치를 수행하기 전에 컨피그레이션을 저장하는 것이 좋습니다.

참고 호환되는 컨피그레이션 파일이 현재 어플라이언스에 설치된 버전보다 오래된 버전의 URL 카테고리 집합을 기반으로 하는 경우 컨피그레이션 파일의 정책 및 ID가 자동으로 수정될 수 있습니다.

1단계 **System Administration(시스템 관리) > Configuration File(컨피그레이션 파일)**을 선택합니다.

2단계 Load Configuration(컨피그레이션 로드) 옵션과 로드할 파일을 선택합니다. 참고:

암호가 마스크 처리된 파일은 로드할 수 없습니다.

파일에 다음과 같은 헤더가 있어야 합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

또한 올바르게 형식이 지정된 config 섹션이 있어야 합니다.

```
<config> ... your configuration information in valid XML </config>
```

3단계 **Load(로드)**를 클릭합니다.

4단계 표시된 경고를 읽어보십시오. 처리 결과를 이해하는 경우 **Continue(계속)**를 클릭합니다.

어플라이언스 컨피그레이션을 공장 기본값으로 재설정

어플라이언스 컨피그레이션을 재설정할 때 기존 네트워크 설정을 유지할지 여부를 선택할 수 있습니다.

이 조치에는 커밋이 필요하지 않습니다.

시작하기 전에

어플라이언스에서 떨어진 위치에 컨피그레이션을 저장합니다.

1단계 **System Administration(시스템 관리) > Configuration File(컨피그레이션 파일)**을 선택합니다.

2단계 **Reset Configuration(컨피그레이션 재설정)** 섹션을 보려면 아래로 스크롤합니다.

3단계 페이지의 정보를 읽고 옵션을 선택합니다.

4단계 **Reset**을 클릭합니다.

기능 키에 대한 작업

기능 키는 시스템에서 특정 기능을 사용하도록 설정합니다. 키는 어플라이언스의 일련번호에 따라 다릅니다(한 시스템의 키를 다른 시스템에서 다시 사용할 수 없음).

- 기능 키 표시 및 업데이트, 22-4페이지
- 기능 키 업데이트 설정 변경, 22-4페이지

기능 키 표시 및 업데이트

1단계 **System Administration(시스템 관리) > Feature Keys(기능 키)**를 선택합니다.

2단계 보류 중인 키 목록을 새로 고치려면 **Check for New Keys(새 키 확인)**를 클릭합니다.

3단계 수동으로 새 기능 키를 추가하려면 키를 Feature Key(기능 키) 필드에 붙여넣거나 입력하고 **Submit Key(키 제출)**를 클릭합니다. 기능 키가 유효한 경우 기능 키가 표시에 추가됩니다.

4단계 활성화 보류 중(Pending Activation) 목록에서 새 기능 키를 활성화하려면 해당 "Select(선택)" 확인란을 표시하고 **Activate Selected Keys(선택한 키 활성화)**를 클릭합니다.

새 키가 발급될 때 자동으로 새 키를 다운로드하여 설치하도록 어플라이언스를 구성할 수 있습니다. 이 경우 Pending Activation(활성화 보류 중) 목록은 항상 비어 있습니다. Feature Key Settings(기능 키 설정) 페이지를 통해 자동 확인을 사용하지 않도록 설정한 경우에도 언제든지 **Check for New Keys(새 키 확인)** 버튼을 클릭하여 AsyncOS에서 새 키를 찾도록 설정할 수 있습니다.

기능 키 업데이트 설정 변경

Feature Key Settings(기능 키 설정) 페이지는 어플라이언스가 새 기능 키를 확인하여 다운로드하는지 여부와 해당 키가 자동으로 활성화되는지 여부를 제어하는 데 사용됩니다.

1단계 **System Administration(시스템 관리) > Feature Key Settings(기능 키 설정)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 필요에 따라 기능 키를 변경합니다.

옵션	설명
기능 키 자동 제공	기능 키를 자동으로 확인 및 다운로드하고 다운로드된 기능 키를 자동으로 활성화하기 위한 옵션입니다. 자동 확인은 일반적으로 한 달에 한 번 수행되지만 기능 키의 만료 기한이 10일 미만인 경우 하루에 한 번으로 변경되고 키가 만료된 후에도 최대 한 달 동안 하루에 한 번으로 변경됩니다. 한 달 후에는 만료된 키가 만료 예정/만료된 키 목록에 더 이상 포함되지 않습니다.

4단계 변경 사항을 제출 및 커밋합니다.

가상 어플라이언스 라이센스

Cisco Web Security Virtual Appliance에서는 호스트에서 가상 어플라이언스를 실행하려면 추가 라이센스가 필요합니다.

가상 어플라이언스 라이센싱에 대한 자세한 내용은 *Cisco Content Security Virtual Appliance 설치 설명서* (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html)를 참조하십시오.

참고 가상 어플라이언스 라이센스를 설치하기 전에는 기술 지원 터널을 열 수 없습니다.

라이센스가 만료된 후에도 180일 동안에는 보안 서비스 없이 어플라이언스가 계속해서 웹 프록시 역할을 수행합니다. 이 기간에는 보안 서비스 업데이트가 발생하지 않습니다.

라이센스 만료에 대한 경고를 수신하도록 어플라이언스를 구성할 수 있습니다.

관련 주제

- 경고 관리, 22-14페이지

가상 어플라이언스 라이센스 설치

Cisco Content Security Virtual Appliance 설치 설명서 (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html)를 참조하십시오.

원격 전원 관리 활성화

어플라이언스 섀시에 대한 전원을 원격으로 재설정하는 기능은 S380 및 S680 하드웨어에서만 사용 가능합니다.

어플라이언스 전원을 원격으로 재설정하려면 이 섹션에 설명된 절차를 사용하여 미리 이 기능을 활성화 및 구성해야 합니다.

시작하기 전에

- 전용 원격 전원 관리 포트를 안전한 네트워크에 직접 연결합니다. 자세한 내용은 사용 중인 어플라이언스 모델의 하드웨어 설명서를 참조하십시오. 이 문서의 위치는 문서 집합, C-1페이지를 참조하십시오.
- 어플라이언스에 원격에서 액세스 가능한지 확인합니다. 예를 들어 방화벽을 통해 필요한 포트를 엽니다.
- 이 기능을 사용하려면 전용 원격 전원 관리 인터페이스에 대한 고유한 IPv4 주소가 필요합니다. 이 인터페이스는 이 섹션에 설명된 절차를 통해서만 구성 가능하며, `ipconfig` 명령을 사용하여 구성할 수 없습니다.
- 어플라이언스 전원을 껐다가 켜려면 IPMI(Intelligent Platform Management Interface) 버전 2.0을 지원하는 디바이스를 관리할 수 있는 서드파티 툴이 필요합니다. 그러한 툴을 사용할 준비가 되었는지 확인합니다.
- CLI(Command Line Interface)에 액세스하는 방법에 대한 자세한 내용은 를 참조하십시오. 부록 B, "CLI(Command Line Interface)"

1단계 SSH 또는 직렬 콘솔 포트를 사용하여 CLI에 액세스합니다.

2단계 Administrator 액세스 권한의 계정을 사용하여 로그인합니다.

3단계 다음과 같은 명령을 입력합니다.

```
remotepower
setup
```

4단계 프롬프트를 따라 다음을 지정합니다.

- 이 기능의 전용 IP 주소와 넷마스크 및 게이트웨이.
- power-cycle 명령을 실행하는 데 필요한 사용자 이름과 암호.

  이러한 자격 증명은 어플라이언스에 액세스하는 데 사용되는 다른 자격 증명과 다릅니다.

5단계 `commit`을 입력하여 변경 사항을 저장합니다.

6단계 컨피그레이션을 테스트하여 어플라이언스 전원을 원격으로 관리할 수 있는지 확인합니다.

7단계 입력한 자격 증명을 불확실한 미래에 사용할 수 있는지 확인합니다. 예를 들면 이 정보를 안전한 곳에 보관하고, 이 작업을 수행해야 하는 관리자가 필요한 자격 증명에 액세스할 수 있는지 확인합니다.

관련 항목

- 하드웨어 어플라이언스: 원격으로 어플라이언스 전원 재설정, A-19페이지

사용자 계정 관리

다음과 같은 유형의 사용자가 웹 보안 어플라이언스에 로그인하여 어플라이언스를 관리할 수 있습니다.

- **로컬 사용자.** 어플라이언스 자체에 로컬로 사용자를 정의할 수 있습니다.
- **외부 시스템에 정의된 사용자.** 외부 RADIUS 서버에 연결하여 어플라이언스에 로그인하는 사용자를 인증하도록 어플라이언스를 구성할 수 있습니다.

참고 정의하는 모든 사용자가 임의의 방법(예: 웹 인터페이스에 로그인 또는 SSH 사용)을 사용하여 어플라이언스에 로그인할 수 있습니다.

관련 주제

- 로컬 사용자 계정 관리, 22-7페이지.
- RADIUS 사용자 인증, 22-9페이지.

로컬 사용자 계정 관리

웹 보안 어플라이언스에 로컬로 임의 수의 사용자를 정의할 수 있습니다.

기본 시스템 admin 계정에는 모든 관리 권한이 있습니다. admin 계정 암호를 변경할 수 있지만 이 계정을 편집하거나 삭제할 수는 없습니다.

참고 admin 사용자 암호를 잊은 경우 Cisco 지원 공급업체에 문의하십시오.

로컬 사용자 계정 추가

시작하기 전에

모든 사용자 계정이 준수해야 하는 암호 요건을 정의합니다. 관리자의 암호 요건 설정, 22-11페이지를 참조하십시오.

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 **Add User(사용자 추가)**를 클릭합니다.

3단계 다음 규칙에 주의하여 사용자 이름을 입력합니다.

- 사용자 이름은 소문자, 숫자, 대시(-) 문자를 포함할 수 있지만 대시로 시작할 수는 없습니다.
- 사용자 이름은 16자보다 길 수 없습니다.
- 사용자 이름은 시스템에서 예약된 특수 이름(예: "operator" 또는 "root")일 수 없습니다.
- 또한 외부 인증을 사용하는 경우 사용자 이름이 외부적으로 인증된 사용자 이름과 중복되어서는 안 됩니다.

4단계 사용자의 전체 이름을 입력합니다.

5단계 사용자 유형을 선택합니다.

사용자 유형	설명
Administrator (관리자)	모든 시스템 컨피그레이션 설정에 대한 전체 액세스를 허용합니다. 그러나 `upgradecheck` 및 `upgradeinstall` CLI 명령은 시스템 정의 "admin" 계정에서만 실행할 수 있습니다.
Operator (운영자)	사용자가 사용자 계정을 생성, 편집 또는 제거하지 못하도록 제한합니다. 또한 운영자 그룹은 다음 CLI 명령의 사용을 제한합니다. • `resetconfig` • `upgradecheck` • `upgradeinstall` • `systemsetup` 또는 시스템 설정 마법사 실행

사용자 유형	설명
Read-Only Operator(읽기 전용 운영자)	이 역할이 있는 사용자 계정은 다음을 수행할 수 있습니다. • 컨피그레이션 정보를 볼 수 있습니다. • 변경 사항을 작성하고 제출하여 기능을 구성하는 방법을 확인할 수 있지만 커밋할 수는 없습니다. • 어플라이언스에 대한 다른 변경 사항(예: 캐시 지우기 또는 파일 저장)을 작성할 수 없습니다. • 파일 시스템, FTP 또는 SCP에 액세스할 수 없습니다.
Guest(게스트)	게스트 그룹 사용자는 보고 및 추적을 포함하여 시스템 상태 정보만 볼 수 있습니다.

6단계 암호를 입력하거나 생성합니다.

7단계 변경 사항을 제출 및 커밋합니다.

사용자 계정 삭제

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 목록에 있는 사용자 이름에 해당하는 휴지통 아이콘을 클릭하고 프롬프트가 표시되면 확인합니다.

3단계 변경 사항을 제출 및 커밋합니다.

사용자 계정 편집

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 사용자 이름을 클릭합니다.

3단계 필요한 경우 Edit User(사용자 편집) 페이지에서 사용자를 변경합니다.

4단계 변경 사항을 제출 및 커밋합니다.

암호 변경

현재 로그인된 계정의 암호를 변경하려면 창의 오른쪽 맨 위에서 **Options(옵션) > Change Passphrase(암호 변경)**를 선택합니다.

다른 계정의 경우 Local User Settings(로컬 사용자 설정) 페이지에서 계정을 편집하고 암호를 변경합니다.

관련 주제

- 사용자 계정 편집, 22-8페이지
- 관리자의 암호 요건 설정, 22-11페이지

RADIUS 사용자 인증

웹 보안 어플라이언스는 RADIUS 디렉토리 서비스를 사용하여 HTTP, HTTPS, SSH 및 FTP를 통해 어플라이언스에 로그인하는 사용자를 인증할 수 있습니다. PAP 또는 CHAP 인증을 사용하여 인증을 위해 여러 외부 서버에 연결하도록 어플라이언스를 구성할 수 있습니다. 외부 사용자 그룹을 여러 웹 보안 어플라이언스 사용자 역할 유형에 매핑할 수 있습니다.

Radius 인증의 이벤트 순서

외부 인증이 사용하도록 설정되어 있고 사용자가 웹 보안 어플라이언스에 로그인하면 어플라이언스에서 다음을 수행합니다.

1. 사용자가 시스템 정의 "admin" 계정인지 확인합니다.
2. 그렇지 않으면 사용자가 첫 번째로 구성된 외부 서버에 정의되어 있는지 확인합니다.
3. 어플라이언스에서 첫 번째 외부 서버에 연결할 수 없는 경우 목록에 있는 다음 외부 서버를 확인합니다.
4. 어플라이언스에서 외부 서버에 연결할 수 없는 경우 사용자를 웹 보안 어플라이언스에 정의된 로컬 사용자로 인증하려고 시도합니다.
5. 사용자가 외부 서버 또는 어플라이언스에 존재하지 않거나 잘못된 암호를 입력하면 어플라이언스에 대한 액세스가 거부됩니다.

RADIUS를 사용하여 외부 인증 사용

1단계 System Administration(시스템 관리) > Users(사용자) 페이지에서 **Enable External Authentication(외부 인증 사용)**을 클릭합니다.

2단계 **RADIUS**를 인증 유형으로 선택합니다.

3단계 RADIUS 서버에 대한 호스트 이름, 포트 이름 및 Shared Secret(공유 암호) 암호를 입력합니다. 기본 포트는 1812입니다.

4단계 어플라이언스가 시간 초과되기 전에 서버의 응답을 기다리는 시간(초)을 입력합니다.

5단계 RADIUS 서버에서 사용되는 인증 프로토콜을 선택합니다.

6단계 (선택 사항) 또 다른 RADIUS 서버를 추가하려면 **Add Row(행 추가)**를 클릭합니다. 각 RADIUS 서버에 대해 3단계–5단계를 반복합니다.

참고 최대 10대의 RADIUS 서버를 추가할 수 있습니다.

7단계 **External Authentication Cache Timeout(외부 인증 캐시 시간 초과)** 필드에 AsyncOS가 재인증하기 위해 RADIUS 서버에 다시 연결하기 전에 외부 인증 자격 증명을 저장하는 시간(초)을 입력합니다. 기본값은 영(0)입니다.

참고 RADIUS 서버에서 일회용 암호(예: 토큰에서 생성된 암호)를 사용하는 경우 영(0)을 입력합니다. 값이 영으로 설정되면 AsyncOS는 현재 세션 중에 인증을 위해 RADIUS 서버에 다시 연결하지 않습니다.

8단계 그룹 매핑 구성 - 외부에서 인증된 모든 사용자를 Administrator 역할에 매핑할지 다른 어플라이언스 사용자 역할 유형에 매핑할지를 선택합니다.

설정	설명
Map externally authenticated users to multiple local roles(외부에서 인증된 사용자를 다중 로컬 역할에 매핑)	RADIUS CLASS 특성에 정의된 대로 그룹 이름을 입력하고 어플라이언스 역할 유형을 선택합니다. Add Row(행 추가)를 클릭하여 역할 매핑을 더 추가할 수 있습니다. AsyncOS는 RADIUS CLASS 특성을 기반으로 RADIUS 사용자를 어플라이언스 역할에 할당합니다. CLASS 특성 요건: • 최소 3자 • 최대 253자 • 콜론, 쉼표 또는 줄 바꿈 문자 없음 • 각 RADIUS 사용자에 대한 하나 이상의 매핑된 CLASS 특성(이 설정에 따라, AsyncOS는 매핑된 CLASS 특성이 없는 RADIUS 사용자에 대한 액세스를 거부합니다.) 여러 CLASS 특성이 있는 RADIUS 사용자의 경우 AsyncOS는 가장 제한적인 역할을 할당합니다. 예를 들어 RADIUS 사용자가 Operator 및 Read-Only Operator 역할에 매핑되는 두 개의 CLASS 특성을 가지고 있는 경우 AsyncOS는 RADIUS 사용자를 Operator 역할보다 더 제한적인 Read-Only Operator 역할에 할당합니다. 다음은 가장 제한적인 역할에서 가장 덜 제한적인 역할 순서로 정렬된 어플라이언스 역할입니다. • Administrator(관리자) • Operator(운영자) • Read-Only Operator(읽기 전용 운영자) • Guest(게스트)
Map all externally authenticated users to the Administrator role(외부에서 인증된 모든 사용자를 Administrator 역할에 매핑)	AsyncOS는 모든 RADIUS 사용자를 Administrator(관리자) 역할에 할당합니다.

9단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 외부 인증, 5-10페이지
- 로컬 사용자 계정 추가, 22-7페이지.

사용자 환경 설정 정의

환경 설정(예: 보고 표시 형식)은 각 사용자에 대해 저장되며 사용자가 어플라이언스에 로그인하는 클라이언트 머신에 관계없이 동일합니다.

1단계 **Options(옵션) > Preferences(기본 설정)**를 선택합니다.

2단계 User Preferences(사용자 환경 설정) 페이지에서 **Edit Preferences(환경 설정 편집)**를 클릭합니다.

3단계 필요에 따라 환경 설정을 구성합니다.

기본 설정	설명
Language Display(언어 표시)	웹 인터페이스 및 CLI에서 AsyncOS for Web이 사용하는 언어
Landing Page	사용자가 어플라이언스에 로그인할 때 표시되는 페이지
Reporting Time Range Displayed(보고 시간 범위 표시)(기본값)	Reporting(보고) 탭의 보고서에 대해 표시되는 기본 시간 범위
Number of Reporting Rows Displayed(보고 행 수 표시)	기본적으로 각 보고서에 대해 표시되는 데이터 행의 수

4단계 변경 사항을 제출 및 커밋합니다.

관리자 설정 구성

관리자의 암호 요건 설정

로컬로 정의된 어플라이언스 관리자에 대한 암호 요건을 설정하려면 다음을 수행합니다.

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 **Passphrase Settings(암호 설정)** 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 옵션을 선택합니다.

옵션	설명
암호에서 허용되지 않는 단어 목록	개별 행에 각각 금지된 단어가 있는 .txt 파일을 생성한 후 업로드할 파일을 선택합니다. 후속 업로드가 이전 업로드를 덮어씁니다.
암호 강도	관리자가 새 암호를 입력할 때 암호 강도 표시기를 표시할 수 있습니다. 이 설정은 강력한 암호를 생성하도록 강제하는 것은 아니며 단순히 입력한 암호를 얼마나 쉽게 추측할 수 있는가를 보여줍니다. 표시기를 표시할 역할을 선택합니다. 그런 다음 선택한 각 역할에 대해 영(0)보다 큰 수를 입력합니다. 숫자가 더 크면 등록되는 암호의 강도를 획득하기가 더 어렵다는 의미입니다. 이 설정에는 최댓값이 없지만 너무 높은 수를 사용하면 "양호"한 것으로 평가되는 암호를 효과적으로 입력할 수 없게 됩니다. 시험하여 요건에 가장 적합한 숫자를 확인합니다. 암호 강도는 로그 눈금 간격으로 측정됩니다. 평가는 NIST SP 800-63, 부록 A에 정의된 미국 NIST(National Institute of Standards and Technology) 엔트로피 규칙을 기반으로 합니다. 일반적으로 다음과 같은 암호가 더 강력합니다. • 길이가 더 깁니다. • 대문자, 소문자, 숫자 및 특수 문자를 포함합니다. • 언어 사전에 나오는 단어를 포함하지 않습니다. 이러한 특성을 가지는 암호를 적용하려면 이 페이지의 다른 설정을 사용합니다.

단계 4 변경 사항을 제출 및 커밋합니다.

어플라이언스에 액세스하기 위한 추가 보안 설정

어플라이언스에 로그인하는 관리자에 대해 더 엄격한 액세스 요건을 가지도록 웹 보안 어플라이언스를 구성할 수 있습니다.

명령	설명
adminaccessconfig > banner	관리자가 로그인하려고 시도할 때 사용자가 지정한 텍스트를 표시하도록 어플라이언스를 구성합니다. 관리자가 모든 인터페이스(예: 웹 인터페이스) 또는 FTP를 통해 어플라이언스에 액세스하려고 시도할 때 맞춤형 배너 텍스트가 표시됩니다. CLI 프롬프트에 붙여넣거나 웹 보안 어플라이언스에 있는 파일에서 복사하여 맞춤형 텍스트를 로드할 수 있습니다. 파일에서 텍스트를 업로드하려면 먼저 FTP를 사용하여 어플라이언스의 컨피그레이션 디렉토리로 파일을 전송해야 합니다.

명령	설명
adminaccessconfig > ipaccess	관리자가 어떤 IP 주소에서 웹 보안 어플라이언스에 액세스하는지 제어합니다. 관리자는 임의의 머신 또는 사용자가 지정한 목록에 포함된 IP 주소를 사용하는 머신에서 어플라이언스에 액세스할 수 있습니다. 액세스를 허용 목록으로 제한하는 경우 IP 주소, 서브넷 또는 CIDR 주소를 지정할 수 있습니다. 기본적으로 어플라이언스에 액세스할 수 있는 주소를 나열할 때 현재 머신의 IP 주소가 허용 목록의 첫 번째 주소로 나열됩니다. 현재 머신의 IP 주소를 허용 목록에서 삭제할 수 없습니다.
adminaccessconfig > strictssl	관리자가 더 강력한 SSL 암호(56비트 이상 암호화)를 사용하여 포트 8443에서 웹 인터페이스에 로그인하도록 어플라이언스를 구성합니다. 더 강력한 SSL 암호가 필요하도록 어플라이언스를 구성하면 HTTPS를 통해 어플라이언스에 액세스하여 어플라이언스를 관리하는 관리자에게만 변경 사항이 적용됩니다. HTTPS를 사용하여 웹 프록시에 연결된 다른 네트워크 트래픽에는 적용되지 않습니다.

관리자 암호 재설정

관리자 레벨의 사용자가 "admin" 사용자의 암호를 변경할 수 있습니다.

시작하기 전에

- admin 계정의 암호를 알지 못하는 경우 암호를 재설정하려면 고객 지원 공급업체에 문의하십시오.
- 암호 변경 사항은 즉시 적용되므로 변경 사항을 커밋할 필요가 없습니다.

1단계 **Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 Users(사용자) 목록에서 **admin** 링크를 클릭합니다.

3단계 **Change the passphrase(암호 변경)**를 선택합니다.

4단계 새 암호를 생성하거나 입력합니다.

생성된 메시지에 대한 반환 주소 구성

보고 장에 대한 후보

보고서를 위해 AsyncOS에서 생성된 메일의 반환 주소를 구성할 수 있습니다.

1단계 **System Administration(시스템 관리) > Return Addresses(반환 주소)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 표시 이름, 사용자 이름 및 도메인 이름을 입력합니다.

4단계 변경 사항을 제출 및 커밋합니다.

경고 관리

경고는 Cisco Web Security Appliance 어플라이언스에서 발생하는 이벤트에 대한 정보를 포함하는 이메일 알림입니다. 이러한 이벤트는 중요도(또는 심각도) 레벨이 낮음(정보)에서 높음(위험)까지 다양할 수 있으며, 일반적으로 어플라이언스의 특정 구성 요소 또는 기능과 관련이 있습니다.

참고 경고 및 이메일 알림을 수신하려면 어플라이언스에서 이메일 메시지를 보내는 데 사용하는 SMTP 릴레이 호스트를 구성해야 합니다.

경고 분류 및 심각도

경고에 포함되는 정보는 경고 분류 및 심각도에 따라 결정됩니다. 경고 수신자에게 전송되는 경고 분류와 심각도를 지정할 수 있습니다.

경고 분류

AsyncOS는 다음 유형의 경고를 전송합니다.

- System
- 하드웨어
- Updater
- 웹 프록시
- 안티맬웨어
- L4 트래픽 모니터

경고 심각도

다음과 같은 심각도에 대해 알림을 전송할 수 있습니다.

- **Critical(위험)**: 즉각적인 조치가 필요합니다.
- **Warning(경고)**: 추가 모니터링 및 잠재적으로 즉각적인 조치가 필요한 문제 또는 오류.
- **Information(정보)**: 이 디바이스의 일상적인 작동 과정에서 생성된 정보.

경고 수신자 관리

참고 시스템 설정 중에 AutoSupport를 사용하도록 설정한 경우, 기본적으로 모든 심각도 및 클래스에 대한 경고가 지정한 이메일 주소로 전송됩니다. 언제든 이 컨피그레이션을 변경할 수 있습니다.

경고 수신자 추가 및 편집

1단계 **System Administration(시스템 관리) > Alerts(경고)**를 선택합니다.

2단계 Alert Recipients(경고 수신자) 목록에서 수신자를 클릭하여 편집하거나 **Add Recipient(수신자 추가)**를 클릭하여 새 수신자를 추가합니다.

3단계 수신자의 이메일 주소를 추가하거나 편집합니다. 여러 주소를 쉼표로 구분하여 입력할 수 있습니다.

4단계 각 경고 유형에 대해 수신할 경고 심각도를 선택합니다.

5단계 변경 사항을 제출 및 커밋합니다.

경고 수신자 삭제

1단계 **System Administration(시스템 관리) > Alerts(경고)**를 선택합니다.

2단계 Alert Recipient(경고 수신자) 목록에서 경고 수신자에 해당하는 휴지통 아이콘을 클릭하고 확인합니다.

3단계 변경 사항을 커밋합니다.

경고 설정 구성

경고 설정은 전역 설정이므로 모든 경고가 동작하는 방법에 영향을 미칩니다.

1단계 **System Administration(시스템 관리) > Alerts(경고)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 필요에 따라 경고 설정을 구성합니다.

옵션	설명
경고를 보내는 데 사용할 발신 주소	경고를 보낼 때 사용할 RFC 2822 준수 "Header From:(헤더 발신:)" 주소입니다. 시스템 호스트 이름에 따라 자동으로 주소("alert@<hostname>")를 생성하는 옵션이 제공됩니다.
중복 경고를 보내기 전에 대기	중복 경고에 대한 시간 간격을 지정합니다. 두 가지 설정이 있습니다. **중복 경고를 보내기 전에 대기할 초기 시간(초)** 중복 알림 요약이 전송되지 않고 대신 모든 중복 알림이 지연 없이 전송됩니다(이 경우 짧은 시간 동안 대량의 이메일이 전송될 수 있음). 중복 알림 전송 사이에 기다릴 시간(초)(알림 간격)은 각 알림이 전송된 후 늘어납니다. 대기 시간(초)에 마지막 간격의 두 배를 더한 값이 늘어납니다. 따라서 5초 대기의 경우 5초, 15초, 35초, 75초, 155초, 315초 등에 알림이 전송됩니다. **중복 경고를 보내기 전에 대기할 최대 시간(초)**. 중복 알림을 전송하기 전 기다릴 최대 시간(초) 필드를 통해 간격 사이에 기다릴 시간(초)의 최대값을 설정할 수 있습니다. 예를 들어, 초기값을 5초로 설정하고 최댓값을 60초로 설정하면 5초, 15초, 35초, 60초, 120초 등의 간격으로 경고가 전송됩니다.
Cisco AutoSupport	Cisco에 다음 지원 정보를 보낼지 여부를 지정합니다. • 시스템에서 생성한 모든 경고 메시지의 사본 • 시스템의 가동 시간, `status` 명령의 출력 및 사용된 AsyncOS 버전을 알려주는 주간 보고서 또한 Cisco에 보낸 모든 메시지의 사본을 내부 경고 수신자에게 전송할지 여부를 지정합니다. 이는 Information(정보) 심각도 레벨에서 System(시스템) 경고를 수신하도록 설정된 수신자에게만 적용됩니다.

4단계 변경 사항을 제출 및 커밋합니다.

경고 목록

다음 섹션에는 경고가 분류별로 나열되어 있습니다. 각 섹션의 표에는 경고 이름(내부적으로 사용되는 설명자), 경고의 실제 텍스트, 설명, 심각도(위험, 정보 또는 경고) 및 메시지 텍스트에 포함된 매개변수(있는 경우)가 있습니다.

기능 키 경고

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 기능 키 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
A "$feature" key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information(정보).	**$feature:** 기능의 이름.
Your "$feature" evaluation key has expired. Please contact your authorized sales representative.	Warning(경고).	**$feature:** 기능의 이름.
Your "$feature" evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	Warning(경고).	**$feature:** 기능의 이름. **$days:** 기능 키가 만료되기 전에 경과될 기간(일).

하드웨어 알림

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 하드웨어 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
A RAID-event has occurred: $error	경고	**$error:** RAID 오류의 텍스트.

기록 경고

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 기록 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
$error.	Information(정보).	**$error:** 오류의 역추적 문자열.
Log Error: Subscription $name: Log partition is full.	Critical(위험).	**$name:** 로그 서브스크립션 이름.
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$ip:** 원격 호스트의 IP 주소. **$reason:** 연결 오류에 대해 설명하는 텍스트.

Message	경고 심각도	매개변수
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$ip:** 원격 호스트의 IP 주소. **$reason:** 잘못된 문제에 대해 설명하는 텍스트.
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$ip:** 원격 호스트의 IP 주소. **$port:** 원격 호스트의 포트 번호. **$reason:** 잘못된 문제에 대해 설명하는 텍스트.
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$hostname:** Syslog 서버의 호스트 이름. **$ip:** Syslog 서버의 IP 주소. **$error:** 오류 메시지의 텍스트.
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$hostname:** Syslog 서버의 호스트 이름. **$ip:** Syslog 서버의 IP 주소. **$error:** 오류 메시지의 텍스트.
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$timeout:** 시간 초과(초). **$hostname:** Syslog 서버의 호스트 이름. **$ip:** Syslog 서버의 IP 주소.
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	Critical(위험).	**$name:** 로그 서브스크립션 이름. **$hostname:** Syslog 서버의 호스트 이름. **$ip:** Syslog 서버의 IP 주소.
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	Information(정보).	**$name:** 로그 서브스크립션 이름. **$max_num_files:** 로그 서브스크립션당 허용되는 최대 파일 수. **$files_removed:** 제거된 파일 목록.

보고 경고

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 보고 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	Critical(중대).	해당 없음
The reporting system is now able to handle new data.	Information(정보).	해당 없음

Message	경고 심각도	매개변수
A failure occurred while building periodic report '$report_title'. This subscription should be examined and deleted if its configuration details are no longer valid.	Critical(위험).	**$report_title:** 보고서의 제목.
A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	Critical(위험).	**$report_title:** 보고서의 제목.
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. 보고 이벤트 기록이 곧 제한되며, 오래된 로그 제거 등을 통해 디스크 공간을 확보하지 않을 경우 보고 데이터가 손실될 수 있습니다. Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning(경고)	**$threshold:** 임계값.
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent.	Critical(위험).	**$report_title:** 보고서의 제목. **$file_name:** 파일의 이름.
Counter group "$counter_group" does not exist.	Critical(위험).	**$counter_group:** counter_group의 이름.
PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent.	Critical(위험).	**$report_title:** 보고서의 제목. **$file_name:** 파일의 이름.
PERIODIC REPORTS: Errors were encountered while processing the domain specification file '$file_name' for the periodic report '$report_title'. Any line which has any reported problem had no report sent. $error_text	Critical(위험).	**$report_title:** 보고서의 제목. **$file_name:** 파일의 이름. **$error_text:** 발생한 오류 목록.

Message	경고 심각도	매개변수
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. 보고 이벤트 기록이 곧 제한되며, 오래된 로그 제거 등을 통해 디스크 공간을 확보하지 않을 경우 보고 데이터가 손실될 수 있습니다. Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning(경고)	**$threshold:** 임계값.
The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	Critical(위험).	**$err_msg:** 오류 메시지 텍스트.

시스템 경보

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 시스템 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
Startup script $name exited with error: $message	Critical(위험).	**$name:** 스크립트의 이름. **$message:** 오류 메시지 텍스트.
System halt failed: $exit_status: $output',	Critical(위험).	**$exit_status:** 명령의 종료 코드. **$output:** 명령의 출력.
System reboot failed: $exit_status: $output	Critical(위험).	**$exit_status:** 명령의 종료 코드. **$output:** 명령의 출력.
Process $name listed $dependency as a dependency, but it does not exist.	Critical(위험).	**$name:** 프로세스의 이름. **$dependency:** 목록에 있었던 종속성의 이름.
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	Critical(위험).	**$name:** 프로세스의 이름. **$dependency:** 목록에 있었던 종속성의 이름.
Process $name listed itself as a dependency.	Critical(위험).	**$name:** 프로세스의 이름.
Process $name listed $dependency as a dependency multiple times.	Critical(위험).	**$name:** 프로세스의 이름. **$dependency:** 목록에 있었던 종속성의 이름.
Dependency cycle detected: $cycle.	Critical(위험).	**$cycle:** 주기에 포함된 프로세스 이름의 목록.

Message	경고 심각도	매개변수
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	Warning(경고)	**$error:** 예외와 연관된 오류 메시지.
There is an error with "$name".	Critical(위험).	**$name:** 코어 파일을 생성한 프로세스의 이름.
An application fault occurred: "$error"	Critical(위험).	**$error:** 오류의 텍스트(일반적으로 역추적).
Tech support: Service tunnel has been enabled, port $port	Information(정보).	**$port:** 서비스 터널에 사용된 포트 번호.
Tech support: Service tunnel has been disabled.	Information(정보).	해당 없음
• The host at $ip has been added to the blacklist because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh whitelist. • The host at $ip has been removed from the blacklist	Warning(경고)	**$ip** - 로그인 시도가 발생한 IP 주소. **Description:** SSH를 통해 어플라이언스에 연결하려고 시도하지만 유효한 자격 증명을 제공하지 않는 IP 주소는 10분 내에 실패한 시도 수가 10을 넘으면 SSH 블랙리스트에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소는 화이트리스트에 추가됩니다. 화이트리스트의 주소는 블랙리스트에서도 발견되더라도 액세스가 허용됩니다. 약 하루가 지나면 항목이 자동으로 블랙리스트에서 제거됩니다.

업데이트 프로그램 경고

다음 표에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 업데이트 프로그램 경고의 목록이 포함되어 있습니다.

Message	경고 심각도	매개변수
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning(경고)	**$app:** 웹 보안 어플라이언스 보안 서비스 이름. **$attempts:** 시도한 횟수.
The updater has been unable to communicate with the update server for at least $threshold.	Warning(경고)	**$threshold:** 임계값 시간.
Unknown error occurred: $traceback.	Critical(위험).	**$traceback:** 역추적 정보.

안티멀웨어 경고

Advanced Malware Protection과 관련된 경고에 대한 자세한 내용은 Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 14-10페이지를 참조하십시오.

FIPS 컴플라이언스

FIPS(Federal Information Processing Standards)는 민감하지만 기밀사항으로 분류되지 않은 정보를 보호하기 위해 모든 정부 기관에서 사용하는 암호화 모듈에 대한 요건을 명시합니다. FIPS는 연방 보안 및 데이터 프라이버시 요건을 준수하도록 합니다. NIST(National Institute for Standards and Technology)에서 개발한 FIPS는 연방 요건을 충족하기 위한 임의 표준이 존재하지 않는 경우에 사용됩니다.

WSA는 C3M(Cisco Common Cryptographic Module)을 사용하여 FIPS 모드에서 FIPS 140-2 레벨 1 컴플라이언스를 달성합니다. 기본적으로 FIPS 모드는 사용하지 않도록 설정되어 있습니다.

FIPS 인증서 요건

FIPS 모드에서는 웹 보안 어플라이언스에서 사용하도록 설정된 모든 암호화 서비스가 FIPS 준수 인증서를 사용해야 합니다. 이는 다음 암호화 서비스에 적용됩니다.

- HTTPS 프록시
- 인증
- SaaS용 ID 공급자
- 어플라이언스 관리 HTTPS 서비스

참고 FIPS 모드를 사용하도록 설정하기 전에 먼저 어플라이언스 관리 HTTPS 서비스를 사용하도록 설정해야 합니다. 다른 암호화 서비스는 사용하도록 설정할 필요가 없습니다.

FIPS 준수 인증서는 다음 요건을 충족해야 합니다.

인증서	알고리즘	비트 키 크기	서명 알고리즘	참고
X509	RSA	1024, 2048, 3072 또는 4096	sha1WithRSAEncryption	Cisco에서는 최적의 암호 해독 성능과 충분한 보안을 위해 비트 키 크기 1024를 권장합니다. 비트 크기를 더 크게 설정하면 보안이 향상되지만 암호 해독 성능에 영향이 미칩니다.
	DSA	1024	dsaWithSHA1	

FIPS 모드 사용 또는 사용 안 함

시작하기 전에

- FIPS 모드에서 사용될 인증서가 FIPS 140-2 승인 공개 키 알고리즘을 사용하는지 확인합니다(FIPS 인증서 요건, 22-21페이지 참조).

참고 FIPS 모드를 변경하면 어플라이언스 재부팅이 시작됩니다.

1단계 **System Administration(시스템 관리) > FIPS Mode(FIPS 모드)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Enable FIPS Level 1 Compliance(FIPS 레벨 1 컴플라이언스 사용)** 확인란을 선택하거나 취소합니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 **Continue(계속)**를 클릭하여 어플라이언스가 재부팅되도록 합니다.

시스템 날짜 및 시간 관리

- 시간대 설정, 22-22페이지
- 시스템 클록을 NTP 서버와 동기화, 22-22페이지

시간대 설정

1단계 **System Administration(시스템 관리) > Time Zone(시간대)**을 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 지역, 국가 및 시간대를 선택하거나 GMT 차감 시간을 선택합니다.

4단계 변경 사항을 제출하고 커밋합니다.

시스템 클록을 NTP 서버와 동기화

Cisco에서는 어플라이언스에서 수동으로 시간을 설정하지 않고 NTP(Network Time Protocol) 서버를 쿼리하여 현재 날짜 및 시간을 추적하도록 Web Security appliance를 설정하는 것을 권장합니다. 이는 특히 어플라이언스가 다른 디바이스와 통합된 경우 권장되는 방법입니다. 모든 통합된 디바이스는 동일한 NTP 서버를 사용해야 합니다.

1단계 **System Administration(시스템 관리) > Time Settings(시간 설정)**를 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 **Use Network Time Protocol(NTP(Network Time Protocol) 사용)**을 시간 기록 방법으로 선택합니다.

4단계 서버를 추가하기 위해 필요에 따라 **Add Row(행 추가)**를 클릭하여 NTP 서버의 정규화된 호스트 이름 또는 IP 주소를 입력합니다.

5단계 (선택 사항) NTP 쿼리에 사용할 어플라이언스 네트워크 인터페이스 유형(관리 또는 데이터)과 연결된 라우팅 테이블을 선택합니다. 이것은 NTP 쿼리가 시작되는 IP 주소입니다.

참고 이 옵션은 어플라이언스가 데이터 및 관리 트래픽에 분할 라우팅을 사용하는 경우에만 편집할 수 있습니다.

6단계 변경 사항을 제출 및 커밋합니다.

SSL 컨피그레이션

보안 강화를 위해 여러 서비스에 대한 SSLv3 및 다양한 버전의 TLS를 사용하도록 설정하고 사용하지 않도록 설정할 수 있습니다. 최적의 보안을 위해서는 모든 서비스에 대해 SSL v3을 사용하지 않도록 설정하는 것이 좋습니다. 기본적으로 모든 버전의 TLS가 사용하도록 설정되어 있고 SSL이 사용하지 않도록 설정되어 있습니다.

참고 `sslconfig` CLI 명령을 사용하여 이러한 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다. Web Security Appliance CLI 명령, B-6페이지를 참조하십시오.

1단계 **System Administration(시스템 관리) > SSL Configuration(SSL 컨피그레이션)**을 선택합니다.

2단계 **Edit Settings(설정 수정)**를 클릭합니다.

3단계 다음 서비스에 대한 SSL v3 및 TLS v1.x를 사용하도록 설정하려면 해당 상자를 선택합니다.

- **Appliance Management Web User Interface(어플라이언스 관리 웹 사용자 인터페이스)** – 이 설정을 변경하면 모든 활성 사용자 연결이 끊어집니다.
- **Proxy Services(프록시 서비스)** – HTTPS 프록시 및 보안 클라이언트를 위한 자격 증명 암호화를 포함합니다. 또한 이 섹션에는 다음 내용이 포함됩니다.
  - **Cipher(s) to Use(사용할 암호)** – 프록시 서비스 통신에 사용될 추가 암호 그룹을 입력할 수 있습니다. 콜론(:)을 사용하여 암호 그룹을 구분합니다. 기본 암호는 `DEFAULT:+kEDH`이지만 ECDHE 암호 선택 사항에 따라 변경할 수 있습니다. 선택한 TLS/SSL 버전에 적합한 암호 그룹만 입력해야 합니다. 자세한 내용과 암호 목록은 https://www.openssl.org/docs/manmaster/apps/ciphers.html을 참조하십시오.

    특정 암호를 사용하지 못하도록 하려면 해당 문자열 앞에 느낌표(!)를 추가합니다. 예를 들어, `!EXP-DHE-RSA-DES-CBC-SHA`입니다.
  - **Disable TLS Compression(TLS 압축 사용 안 함)(권장)** – 이 상자를 선택하여 TLS 압축을 사용하지 않도록 설정할 수 있습니다. 최상의 보안을 위해 권장됩니다.
- **Secure LDAP Services(보안 LDAP 서비스)** – 인증, 외부 인증, SaaS SSO 및 보안 모빌리티를 포함합니다.
- **Secure ICAP Services (External DLP)(보안 ICAP 서비스(외부 DLP))** – 어플라이언스와 외부 DLP(Data Loss Prevention) 서버 간의 ICAP 통신 보안에 사용되는 프로토콜을 선택합니다. 자세한 내용은 외부 DLP 서버 구성, 16-9페이지를 참조하십시오.
- **Update Service(업데이트 서비스)** – 어플라이언스와 사용 가능한 업데이트 서버 간의 통신에 사용되는 프로토콜을 선택합니다. 업데이트 서비스에 대한 자세한 내용은 AsyncOS for Web 업그레이드 및 업데이트, 22-27페이지를 참조하십시오.

참고 Cisco의 업데이트 서버는 SSL v3을 지원하지 않으므로 Cisco 업데이트 서비스에 대해 TLS 1.0 이상을 사용하도록 설정해야 합니다. 그러나 이와 같이 구성된 경우 SSL v3을 계속해서 로컬 업데이트 서버에 사용할 수 있습니다. 해당 서버에서 지원되는 SSL/TLS 버전을 확인해야 합니다.

4단계 **Submit(제출)**을 클릭합니다.

인증서 관리

어플라이언스는 디지털 인증서를 사용하여 다양한 연결을 설정, 확인 및 보호합니다. Certificate Management(인증서 관리) 페이지에서 현재 인증서 목록을 보고 업데이트하며 신뢰할 수 있는 루트 인증서를 관리하고 차단된 인증서를 볼 수 있습니다.

관련 주제

- 인증서 및 키 정보, 22-24페이지
- 인증서 업데이트, 22-25페이지
- 신뢰할 수 있는 루트 인증서 관리, 22-24페이지
- 차단된 인증서 보기, 22-25페이지

인증서 및 키 정보

브라우저에서 사용자에게 인증하도록 프롬프트를 표시하는 경우 브라우저가 보안 HTTPS 연결을 사용하여 웹 프록시에 인증 자격 증명을 전송합니다. 기본적으로 웹 보안 어플라이언스는 함께 제공되는 "Cisco Web Security Appliance 데모 인증서"를 사용하여 클라이언트와의 HTTPS 연결을 생성합니다. 대부분의 브라우저에서 인증서가 유효하지 않다고 사용자에게 경고합니다. 사용자가 잘못된 인증서 메시지를 보지 못하도록 애플리케이션에서 자동으로 인식하는 인증서 및 키 쌍을 업로드할 수 있습니다.

관련 주제

- 인증서 및 키 업로드 또는 생성, 22-25페이지
- 인증서 서명 요청, 22-27페이지
- 중간 인증서, 22-27페이지

신뢰할 수 있는 루트 인증서 관리

Web Security appliance는 신뢰할 수 있는 루트 인증서 목록과 함께 제공되며 이 목록을 유지 관리합니다. 신뢰할 수 있는 인증서가 있는 웹 사이트에서는 암호 해독이 필요하지 않습니다.

인증서를 추가하고 기능적으로 인증서를 제거하여 신뢰할 수 있는 인증서 목록을 관리할 수 있습니다. 웹 보안 어플라이언스는 인증서를 마스터 목록에서 삭제하지 않지만 인증서의 신뢰를 재지정하도록 허용하여 신뢰할 수 있는 목록에서 기능적으로 인증서를 제거합니다.

신뢰할 수 있는 루트 인증서를 추가, 재지정 또는 다운로드하려면 다음을 수행합니다.

1단계 **Network(네트워크) > Certificate Management(인증서 관리)**를 선택합니다.

2단계 Certificate Management(인증서 관리) 페이지에서 **Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)**를 클릭합니다.

3단계 Cisco에서 인식하는 목록에 없는 서명 권한을 가지는 신뢰할 수 있는 맞춤형 루트 인증서를 추가하려면 다음을 수행합니다.

Import(가져오기)를 클릭한 후 인증서 파일을 찾아서 선택하고 **Submit(제출)**합니다.

4단계 하나 이상의 Cisco 인식 인증서에 대한 신뢰를 재지정하려면 다음을 수행합니다.

a. 재지정하려는 각 항목에 대한 **Override Trust(신뢰 재지정)** 확인란을 선택합니다.

b. **Submit(제출)**을 클릭합니다.

5단계 특정 인증서의 사본을 다운로드하려면 다음을 수행합니다.

a. Cisco Trusted Root Certificate List(Cisco의 신뢰할 수 있는 루트 인증서 목록)에서 인증서의 이름을 클릭하여 해당 항목을 확장합니다.

b. **Download Certificate(인증서 다운로드)**를 클릭합니다.

인증서 업데이트

Updates(업데이트) 섹션에는 어플라이언스에 있는 Cisco의 신뢰할 수 있는 루트 인증서 및 블랙리스트 번들에 대한 버전 및 최신 업데이트 정보가 나열되어 있습니다. 이러한 번들은 주기적으로 업데이트됩니다.

1단계 Certificate Management(인증서 관리) 페이지에서 **Update Now(지금 업데이트)**를 클릭하여 업데이트가 사용 가능한 모든 번들을 업데이트합니다.

차단된 인증서 보기

Cisco에서 유효하지 않은 것으로 확인하여 차단한 인증서 목록을 보려면 다음을 수행합니다.

1단계 **View Blocked Certificates(차단된 인증서 보기)**를 클릭합니다.

인증서 및 키 업로드 또는 생성

특정 AsyncOS 기능에는 연결을 설정, 확인 또는 보호하기 위한 인증서 및 키가 필요합니다(예: ISE(Identity Services Engine) 및 SaaS용 ID 공급자). 기존 인증서 및 키를 업로드하거나 기능을 구성할 때 인증서 및 키를 생성할 수 있습니다.

인증서 및 키 업로드

어플라이언스에 업로드하는 인증서는 다음 요건을 충족해야 합니다.

- X.509 표준을 사용해야 합니다.
- PEM 형식의 일치하는 개인 키를 포함해야 합니다. DER 형식은 지원되지 않습니다.

1단계 **Use Uploaded Certificate and Key(업로드된 인증서 및 키 사용)**를 선택합니다.

2단계 **Certificate(인증서)** 필드에서 Browse(찾아보기)를 클릭하여 업로드할 파일을 찾습니다.

참고 웹 프록시에서 파일에 있는 첫 번째 인증서 또는 키를 사용합니다. 인증서 파일은 PEM 형식이어야 합니다. DER 형식은 지원되지 않습니다.

3단계 **Key(키)** 필드에서 Browse(찾아보기)를 클릭하여 업로드할 파일을 찾습니다.

참고 키 길이는 512, 1024 또는 2048비트여야 합니다. 개인 키 파일은 PEM 형식이어야 합니다. DER 형식은 지원되지 않습니다.

4단계 키가 암호화된 경우 **Key is Encrypted(키가 암호화됨)**를 선택합니다.

5단계 **Upload Files(파일 업로드)**를 클릭합니다.

인증서 및 키 생성

1단계 **Use Generated Certificate and Key(생성된 인증서 및 키 사용)**를 선택합니다.

2단계 **Generate New Certificate and Key(새 인증서 및 키 생성)**를 클릭합니다.

a. Generate Certificate and Key(인증서 및 키 생성) 대화 상자에서 필요한 생성 정보를 입력합니다.

참고 Common Name(공용 이름) 필드에 슬래시(/)를 제외한 모든 ASCII 문자를 입력할 수 있습니다.

b. Generate Certificate and Key(인증서 및 키 생성) 대화 상자에서 **Generate(생성)**를 클릭합니다.

생성이 완료되면 **Download Certificate(인증서 다운로드)** 및 **Download Certificate Signing Request(인증서 서명 요청 다운로드)** 링크와 함께 인증서 정보가 Certificate(인증서) 섹션에 표시됩니다. 또한 CA(Certificate Authority)로부터 서명된 인증서를 수신하는 경우 이를 업로드하는 데 사용되는 Signed Certificate(서명된 인증서) 옵션이 있습니다.

3단계 어플라이언스에 업로드하기 위해 새 인증서를 다운로드하려면 **Download Certificate(인증서 다운로드)**를 클릭합니다.

4단계 서명을 위해 CA(Certificate Authority)에 전송할 새 인증서 파일을 다운로드하려면 **Download Certificate Signing Request(인증서 서명 요청 다운로드)**를 클릭합니다. 이 프로세스에 대한 자세한 내용은 인증서 서명 요청, 22-27페이지를 참조하십시오.

a. CA가 서명된 인증서를 반환하는 경우 Certificate(인증서) 필드의 Signed Certificate(서명된 인증서) 부분에서 Browse(찾아보기)를 클릭하여 서명된 인증서 파일을 찾은 후 Upload File(파일 업로드)을 클릭하여 어플라이언스에 업로드합니다.

b. CA의 루트 인증서가 어플라이언스의 신뢰할 수 있는 루트 인증서 목록에 있는지 확인합니다. 그렇지 않은 경우 해당 인증서를 추가합니다. 자세한 내용은 신뢰할 수 있는 루트 인증서 관리, 22-24페이지를 참조하십시오.

인증서 서명 요청

웹 보안 어플라이언스는 어플라이언스에 업로드되는 인증서에 대한 CSR(Certificate Signing Request)을 생성할 수 없습니다. 따라서 어플라이언스에 대한 인증서가 생성되도록 하려면 다른 시스템에서 서명 요청을 발행해야 합니다. 나중에 어플라이언스에 설치해야 하므로 이 시스템에서 PEM 형식의 키를 저장합니다.

최신 버전의 OpenSSL이 설치된 UNIX 시스템을 사용할 수 있습니다. CSR에 어플라이언스 호스트 이름을 입력해야 합니다. OpenSSL을 사용하여 CSR을 생성하는 방법에 대한 자세한 내용은 다음 위치의 지침을 참조하십시오.

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

CSR이 생성되면 CA(Certificate Authority)에 제출합니다. CA에서는 PEM 형식의 인증서를 반환합니다.

처음으로 인증서를 획득하는 경우 인터넷에서 "certificate authority services SSL server certificates(인증 기관 서비스 SSL 서버 인증서)"를 검색하고 조직의 요구에 가장 적합한 서비스를 선택합니다. SSL 인증서를 가져오려면 서비스 지침을 따르십시오.

참고 또한 자체 인증서를 생성하여 서명할 수도 있습니다. 이 작업을 수행하기 위한 툴은 OpenSSL에 포함되어 있으며 이는 `http://www.openssl.org`에서 무료로 받을 수 있는 소프트웨어입니다.

중간 인증서

루트 CA(Certificate Authority) 인증서 검증 이외에도 AsyncOS는 중간 인증서 검증 사용을 지원합니다. 중간 인증서는 신뢰할 수 있는 루트 CA에서 발급하는 인증서로서 추가 인증서를 생성하는 데 사용됩니다. 중간 인증서는 연결된 신뢰 라인을 생성합니다. 예를 들어, 신뢰할 수 있는 루트 CA에서 인증서 발급 권한을 부여받은 example.com에서 인증서를 발급할 수 있습니다. example.com에서 발급한 인증서와 관련하여 신뢰할 수 있는 루트 CA에서 얻은 개인 키뿐만 아니라 example.com에서 얻은 개인 키도 검증해야 합니다.

AsyncOS for Web 업그레이드 및 업데이트

Cisco에서는 AsyncOS for Web 및 해당 구성 요소에 대한 업그레이드(새 소프트웨어 버전) 및 업데이트(현재 소프트웨어 버전에 대한 변경 사항)를 정기적으로 릴리스합니다.

AsyncOS for Web 업그레이드 모범 사례

- 업그레이드를 시작하기 전에 System Administration(시스템 관리) > Configuration File(컨피그레이션 파일) 페이지에서 또는 `saveconfig` 명령을 사용하여 웹 보안 어플라이언스의 XML 컨피그레이션 파일을 저장합니다.
- PAC 파일 또는 맞춤화된 최종 사용자 알림 페이지와 같은 어플라이언스에 저장된 다른 파일을 저장합니다.
- 업그레이드할 때 다양한 프롬프트에서 오랜 시간 동안 일시정지하지 마십시오. 다운로드 중에 TCP 세션 시간이 초과되면 업그레이드에 실패할 수 있습니다.
- 업그레이드가 완료된 후 컨피그레이션 정보를 XML 파일에 저장합니다.

관련 주제

- 어플라이언스 컨피그레이션 저장, 로드 및 재설정, 22-2페이지.

AsyncOS 및 보안 서비스 구성 요소 업그레이드 및 업데이트

AsyncOS for Web 업그레이드

시작하기 전에

- 어플라이언스 컨피그레이션 파일을 저장합니다(어플라이언스 컨피그레이션 저장, 로드 및 재설정, 22-2페이지 참조).

1단계 **System Administration(시스템 관리) > System Upgrade(시스템 업그레이드)**를 선택합니다.

2단계 **Available Upgrades(사용 가능한 업그레이드)**를 클릭합니다.

3단계 사용 가능한 업그레이드 목록에서 업그레이드를 선택하고 **Begin Upgrade(업그레이드 시작)**를 클릭하여 업그레이드 프로세스를 시작합니다. 표시되는 질문에 응답합니다.

CLI 및 웹 애플리케이션 인터페이스가 업데이트 프로세스 중에 느려지거나 사용 불가능하게 될 수 있습니다.

4단계 업그레이드가 완료되면 **Reboot Now(지금 재부팅)**를 클릭하여 웹 보안 어플라이언스를 재부팅합니다.

관련 주제

- 로컬 및 원격 업데이트 서버, 22-29페이지.

자동 및 수동 업데이트 및 업그레이드 쿼리

AsyncOS는 업데이트 서버에서 모든 보안 서비스 구성 요소에 대한 새로운 업데이트를 주기적으로 쿼리하지만 새로운 AsyncOS 업그레이드에 대해서는 쿼리하지 않습니다. AsyncOS를 업그레이드하려면 사용 가능한 업그레이드를 쿼리하도록 수동으로 AsyncOS에 프롬프트를 표시해야 합니다. 또한 사용 가능한 보안 서비스 업데이트를 쿼리하도록 수동으로 AsyncOS에 프롬프트를 표시할 수도 있습니다. 자세한 내용은 이전 버전의 AsyncOS for Web으로 되돌리기, 22-33페이지를 참고하십시오.

AsyncOS가 업데이트 서버에서 업데이트 또는 업그레이드를 쿼리할 때 다음 단계를 수행합니다.

1. 업데이트 서버에 연결합니다.

   Cisco에서는 다음과 같은 업데이트 서버 소스를 허용합니다.

   - **Cisco 업데이트 서버.** 자세한 내용은 Cisco 업데이트 서버에서 업데이트 및 업그레이드, 22-30페이지를 참고하십시오.
   - **로컬 서버.** 자세한 내용은 로컬 서버에서 업그레이드, 22-30페이지를 참고하십시오.
2. 사용 가능한 업데이트 또는 AsyncOS 업그레이드 버전이 나열된 XML 파일을 수신합니다. 이 XML 파일을 "매니페스트"라고 합니다.
3. 업데이트 또는 업그레이드 이미지 파일을 다운로드합니다.

수동으로 보안 서비스 구성 요소 업데이트

기본적으로 각 보안 서비스 구성 요소는 주기적으로 Cisco 업데이트 서버에서 해당 데이터베이스 테이블로 업데이트를 수신합니다. 그러나 수동으로 데이터베이스 테이블을 업데이트할 수 있습니다.

참고 일부 업데이트는 기능과 관련된 GUI 페이지에서 온디맨드로 사용할 수 있습니다.

정보 업데이트 프로그램 로그 파일에서 업데이트 활동 레코드를 확인합니다. System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지에서 업데이트 프로그램 로그 파일을 구독합니다.

참고 진행 중인 업데이트를 중단할 수 없습니다. 새 변경 사항을 적용하려면 진행 중인 모든 업데이트가 완료되어야 합니다.

1단계 **System Administration(시스템 관리) > Upgrade and Update Settings(업그레이드 및 업데이트 설정)**를 선택합니다.

2단계 **Edit Update Settings(업데이트 설정 수정)**를 클릭합니다.

3단계 업데이트 파일의 위치를 지정합니다.

4단계 Security Services(보안 서비스) 탭에 있는 구성 요소 페이지의 Update Now(지금 업데이트) 기능 키를 사용하여 업데이트를 시작합니다. 예를 들어, Security Services(보안 서비스) > Web Reputation Filters(웹 평판 필터) 페이지입니다.

CLI 및 웹 애플리케이션 인터페이스가 업데이트 프로세스 중에 느려지거나 사용 불가능하게 될 수 있습니다.

로컬 및 원격 업데이트 서버

기본적으로 AsyncOS는 업데이트 및 업그레이드 이미지와 매니페스트 XML 파일 모두에 사용할 Cisco 업데이트 서버에 연결합니다. 그러나 업그레이드 및 업데이트 이미지와 매니페스트 파일을 다운로드할 위치를 선택할 수 있습니다. 다음 이유로 인해 이미지 또는 매니페스트 파일에 대해 로컬 업데이트 서버를 사용합니다.

- **동시에 업그레이드할 여러 어플라이언스가 있습니다.** 업그레이드 이미지를 네트워크 내부의 웹 서버에 다운로드하여 네트워크에 있는 모든 어플라이언스에 제공할 수 있습니다.
- **방화벽 설정에 Cisco 업데이트 서버의 고정 IP 주소가 필요합니다.** Cisco 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 업데이트 및 AsyncOS 업그레이드를 위한 고정 위치를 구성해야 할 수 있습니다. 자세한 내용은 Cisco 업데이트 서버에 대한 고정 주소 구성, 22-30페이지를 참고하십시오.

참고 로컬 업데이트 서버는 보안 서비스 업데이트가 아니라 AsyncOS 업그레이드만 자동으로 수신합니다. 로컬 업데이트 서버를 사용하여 AsyncOS를 업그레이드한 후 다시 보안 서비스가 자동으로 업데이트되도록 업데이트 및 업그레이드 설정을 Cisco 업데이트 서버 사용으로 다시 변경합니다.

Cisco 업데이트 서버에서 업데이트 및 업그레이드

웹 보안 어플라이언스는 Cisco 업데이트 서버에 직접 연결하여 업그레이드 이미지 및 보안 서비스 업데이트를 다운로드할 수 있습니다. 각 어플라이언스가 개별적으로 업데이트 및 업그레이드 이미지를 다운로드합니다.

Cisco 업데이트 서버에 대한 고정 주소 구성

Cisco 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 업데이트 및 AsyncOS 업그레이드를 위한 고정 위치를 구성해야 할 수 있습니다.

1단계 고정 URL 주소를 가져오려면 Cisco 고객 지원에 문의하십시오.

2단계 System Administration(시스템 관리) > Upgrade and Update Settings(업그레이드 및 업데이트 설정 페이지)로 이동하여 **Edit Update Settings(업데이트 설정 편집)**를 클릭합니다.

3단계 Edit Update Settings(업데이트 설정 편집) 페이지의 "Update Servers (images)(업데이트 서버(이미지))" 섹션에서 Local Update Servers(로컬 업데이트 서버)를 선택하고 1단계에서 수신된 고정 URL 주소를 입력합니다.

4단계 "Update Servers (list)(업데이트 서버(목록))" 섹션에 대해 Cisco 업데이트 서버가 선택되었는지 확인합니다.

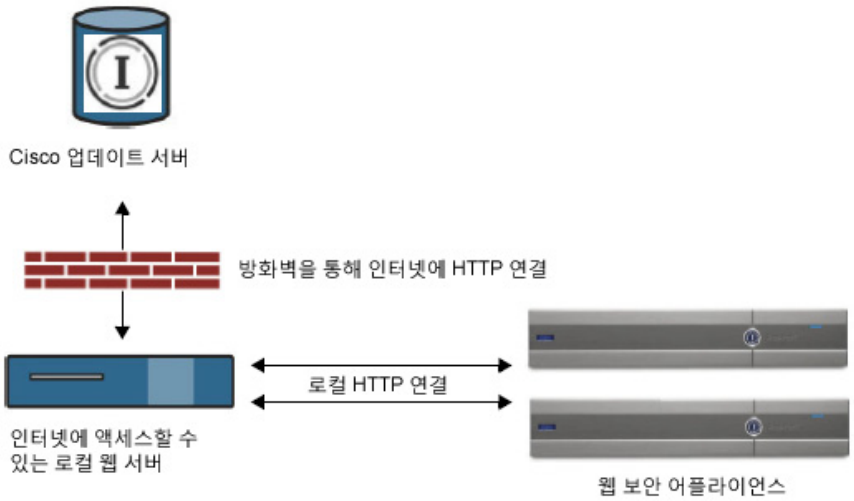
5단계 변경 사항을 제출 및 커밋합니다.

로컬 서버에서 업그레이드

웹 보안 어플라이언스는 Cisco 업데이트 서버에서 직접 업그레이드를 가져오지 않고 네트워크 내의 서버에서 AsyncOS 업그레이드를 다운로드할 수 있습니다. 이 기능을 사용하는 경우 업그레이드 이미지를 Cisco에서 한 번만 다운로드한 후 네트워크의 모든 웹 보안 어플라이언스에 제공합니다.

그림 22-1에서는 웹 보안 어플라이언스가 로컬 서버에서 업그레이드 이미지를 다운로드하는 방법을 보여줍니다.

그림 22-1 로컬 서버에서 업그레이드



로컬 업그레이드 서버에 대한 하드웨어 및 소프트웨어 요건

AsyncOS 업그레이드 파일을 *다운로드*하려면 웹 브라우저가 있으며 Cisco 업데이트 서버에 인터넷으로 액세스할 수 있는 시스템이 내부 네트워크에 있어야 합니다.

참고 이 주소에 대한 HTTP 액세스를 허용하도록 방화벽 설정을 구성해야 하는 경우, 특정 IP 주소가 아니라 DNS 이름을 사용하여 구성해야 합니다.

AsyncOS 업그레이드 파일을 *호스팅*하려면 내부 네트워크의 서버에 다음 기능이 포함된 웹 서버(Microsoft IIS(Internet Information Services) 또는 Apache 오픈 소스 서버)가 있어야 합니다.

- 24자를 초과하는 파일 이름 또는 디렉토리 표시를 지원합니다.
- 디렉토리 찾아보기가 가능합니다.
- 익명(인증 없음) 또는 기본("단순") 인증으로 구성됩니다.
- 각 AsyncOS 업그레이드 이미지에 대해 최소한 350MB의 여유 디스크 공간을 포함합니다.

로컬 서버에서 업그레이드 구성

참고 업그레이드가 완료된 후에는 보안 서비스 구성 요소가 계속해서 자동으로 업데이트되도록 Cisco 업데이트 서버를 사용하기 위한 업데이트 및 업그레이드 설정(동적 또는 고정 주소)을 변경하는 것이 좋습니다.

1단계 업그레이드 파일을 검색하여 제공하도록 로컬 서버를 구성합니다.

2단계 업그레이드 zip 파일을 다운로드합니다.

로컬 서버에서 브라우저를 통해 `http://updates.ironport.com/fetch_manifest.html` 로 이동하여 업그레이드 이미지의 zip 파일을 다운로드합니다. 이미지를 다운로드하려면 어플라이언스의 일련번호(물리적 어플라이언스용) 또는 VLN(가상 어플라이언스용) 및 버전 번호를 입력합니다. 그러면 사용 가능한 업그레이드 목록이 표시됩니다. 다운로드하려는 업그레이드 버전을 클릭합니다.

3단계 디렉토리 구조를 그대로 유지하고 로컬 서버의 루트 디렉토리에 zip 파일의 압축을 풉니다.

4단계 System Administration(시스템 관리) > Upgrade and Update Settings(업그레이드 및 업데이트 설정) 페이지 또는 `updateconfig` 명령을 사용하여 로컬 서버를 사용하도록 어플라이언스를 구성합니다.

5단계 System Administration(시스템 관리) > System Upgrade(시스템 업그레이드) 페이지에서 **Available Upgrades(사용 가능한 업그레이드)**를 클릭하거나 `upgrade` 명령을 실행합니다.

로컬 및 원격 업그레이드 방법 간의 차이점

Cisco 업데이트 서버가 아니라 로컬 서버에서 AsyncOS를 업그레이드하는 경우 다음 차이점이 적용됩니다.

- 업그레이드가 *다운로드되는 동안* 즉시 설치됩니다.
- 업그레이드 프로시스 시작 시 10초 동안 배너가 표시됩니다. 이 배너가 표시되어 있는 동안 Ctrl+C를 입력하면 다운로드가 시작되기 전에 업그레이드 프로세스를 종료할 수 있는 옵션이 있습니다.

업그레이드 및 서비스 업데이트 설정 구성

웹 보안 어플라이언스에서 보안 서비스 업데이트 및 AsyncOS for Web 업그레이드를 다운로드하는 방법을 구성할 수 있습니다. 예를 들어, 파일을 다운로드할 때 사용할 네트워크 인터페이스를 선택하거나 업데이트 간격을 구성하거나 자동 업데이트를 사용하지 않도록 설정할 수 있습니다.

1단계 **System Administration(시스템 관리) > Upgrade and Update Settings(업그레이드 및 업데이트 설정)**를 선택합니다.

2단계 **Edit Update Settings(업데이트 설정 수정)**를 클릭합니다.

3단계 다음 정보를 참조하여 설정을 구성합니다.

설정	설명
자동 업데이트	보안 구성 요소의 자동 업데이트를 사용하도록 설정할지 여부를 선택합니다. 자동 업데이트를 선택하는 경우 시간 간격을 입력합니다. 기본값이 사용하도록 설정되고 업데이트 간격은 5분입니다.
업그레이드 알림	AsyncOS에 대한 새로운 업그레이드가 사용 가능한 경우 웹 인터페이스의 상단에 알림을 표시할지 여부를 선택합니다. 어플라이언스는 관리자에게만 이 알림을 표시합니다. 자세한 내용은 AsyncOS for Web 업그레이드, 22-28페이지를 참고하십시오.
업데이트 서버(목록)	사용 가능한 업그레이드 및 업데이트 목록(매니페스트 XML 파일)을 Cisco 업데이트 서버에서 다운로드할지 아니면 로컬 웹 서버에서 다운로드할지를 선택합니다. 로컬 업데이트 서버를 선택할 경우 서버의 포트 번호 및 파일 이름을 포함하여 해당 목록의 매니페스트 XML 파일에 대한 전체 경로를 입력합니다. 포트 필드를 비워두면 AsyncOS에서는 포트 80을 사용합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력할 수도 있습니다. • 하드웨어 어플라이언스의 매니페스트를 얻기 위한 URL: https://update-manifests.ironport.com • 가상 어플라이언스에 대한 매니페스트를 얻기 위한 URL: https://update-manifests.sco.cisco.com
업데이트 서버(이미지)	업그레이드 및 업데이트 이미지를 Cisco 업데이트 서버에서 다운로드할지 아니면 로컬 웹 서버에서 다운로드할지 선택합니다. 로컬 업데이트 서버를 선택할 경우 서버의 기본 URL과 포트 번호를 입력합니다. 포트 필드를 비워두면 AsyncOS에서는 포트 80을 사용합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력할 수도 있습니다.
라우팅 테이블	업데이트 서버에 연결할 때 사용할 네트워크 인터페이스의 라우팅 테이블을 선택합니다.
프록시 서버(선택 사항)	업스트림 프록시 서버가 있고 인증을 요구하는 경우 여기에 서버 정보와 사용자 이름 및 암호를 입력합니다.

4단계 변경 사항을 제출 및 커밋합니다.

관련 항목

- 로컬 및 원격 업데이트 서버, 22-29페이지.
- 자동 및 수동 업데이트 및 업그레이드 쿼리, 22-28페이지.
- AsyncOS 및 보안 서비스 구성 요소 업그레이드 및 업데이트, 22-28페이지.

이전 버전의 AsyncOS for Web으로 되돌리기

AsyncOS for Web은 비상 시에 AsyncOS for Web 운영 체제를 이전의 정식 빌드로 되돌릴 수 있는 기능을 지원합니다.

참고 AsyncOS for Web 버전을 버전 7.5 이전으로 되돌릴 수 없습니다.

가상 어플라이언스에서 AsyncOS를 되돌리면 라이센스에 영향을 미칠 수 있음

AsyncOS 8.0으로 되돌리는 경우 어플라이언스가 보안 기능 없이 웹 트랜잭션을 처리하는 180일 유예 기간이 주어지지 않습니다. 라이센스 만료 날짜는 영향을 받지 않습니다.

되돌리기 프로세스에서 컨피그레이션 파일 사용

버전 7.5부터 이후 버전으로 업그레이드할 때 업그레이드 프로세스가 자동으로 현재 시스템 컨피그레이션을 웹 보안 어플라이언스의 파일에 저장합니다. (그러나 Cisco에서는 수동으로 컨피그레이션 파일을 로컬 머신에 백업으로 저장하도록 권장합니다.) 이렇게 하면 이전 버전으로 되돌린 후 AsyncOS for Web이 이전 버전과 연결된 컨피그레이션 파일을 로드할 수 있습니다. 그러나 되돌리기를 수행할 때 관리 인터페이스에 대한 현재 네트워크 설정을 사용합니다.

SMA에서 관리되는 어플라이언스에 대한 AsyncOS 되돌리기

웹 보안 어플라이언스에서 AsyncOS for Web을 되돌릴 수 있습니다. 그러나 웹 보안 어플라이언스가 보안 관리 어플라이언스에서 관리되는 경우 다음 규칙과 지침을 고려하십시오.

- 웹 보안 어플라이언스에서 중앙 집중식 보고가 사용하도록 설정된 경우 AsyncOS for Web이 되돌리기를 시작하기 전에 보고 데이터를 보안 관리 어플라이언스에 전송하는 작업을 완료합니다. 파일을 보안 관리 어플라이언스에 전송하는 데 40초보다 더 오랜 시간이 걸리는 경우 AsyncOS for Web에서 파일 전송을 계속 기다릴지 아니면 모든 파일을 전송하지 않고 되돌리기를 계속할지에 대한 프롬프트를 표시합니다.
- 되돌린 후 웹 보안 어플라이언스를 적절한 컨피그레이션 마스터와 연결해야 합니다. 그렇지 않으면, 컨피그레이션을 보안 관리 어플라이언스에서 웹 보안 어플라이언스로 푸시하는 데 실패할 수 있습니다.

AsyncOS for Web을 이전 버전으로 되돌리기

주의 웹 보안 어플라이언스에서 운영 체제를 되돌리는 작업은 매우 파괴적인 조치이며 모든 컨피그레이션 로그 및 데이터베이스를 삭제합니다. 또한 되돌리기를 수행하면 어플라이언스가 재구성될 때까지 웹 트래픽 처리가 중단됩니다. 초기 웹 보안 어플라이언스 컨피그레이션에 따라 이 조치로 네트워크 컨피그레이션이 파괴될 수 있습니다. 이러한 상황이 발생하는 경우 되돌리기를 수행한 후 로컬에서 물리적으로 어플라이언스에 액세스해야 합니다.

참고 URL 카테고리 집합에 대한 업데이트가 사용 가능한 경우 AsyncOS 되돌리기 후 적용됩니다.

시작하기 전에

- Cisco Quality Assurance에 문의하여 예정된 되돌리기를 수행할 수 있는지 확인합니다.
- 웹 보안 어플라이언스의 다음 정보를 별도의 머신에 백업합니다.
  - 시스템 컨피그레이션 파일(암호가 마스크 처리되지 않음)
  - 보존할 로그 파일
  - 보존할 보고서
  - 어플라이언스에 저장된 맞춤형 최종 사용자 알림 페이지
  - 어플라이언스에 저장된 PAC 파일

1단계 복귀할 어플라이언스의 CLI에 로그인합니다.

참고 다음 단계에서 `revert` 명령을 실행하면 몇 가지 경고 프롬프트가 표시됩니다. 이러한 경고 프롬프트에 동의하면 즉시 복귀 작업이 수행됩니다. 따라서 복귀 전 단계를 완료하기 전에는 복귀 프로세스를 시작하지 마십시오.

2단계 `revert` 명령을 입력합니다.

3단계 되돌리기를 계속할 것을 두 번 확인합니다.

4단계 되돌릴 사용 가능한 버전 중 하나를 선택합니다.

어플라이언스가 두 번 재부팅됩니다.

참고 복귀 프로세스는 시간이 많이 걸리는 작업입니다. 복귀가 완료될 때까지 15분에서 20분 정도 소요될 수 있으며, 어플라이언스에 대한 콘솔 액세스가 다시 사용 가능해집니다.

이제 선택한 AsyncOS for Web 버전을 사용하여 어플라이언스를 실행해야 합니다. 웹 브라우저에서 웹 인터페이스에 액세스할 수 있습니다.

SNMP를 사용하여 시스템 상태 모니터링

AsyncOS 운영 체제는 SNMP(Simple Network Management Protocol)를 통한 시스템 상태 모니터링을 지원합니다. (SNMP에 대한 자세한 내용은 RFC 1065, 1066 및 1067을 참조하십시오.)

참고:

- SNMP는 기본적으로 **off**입니다.
- SNMP SET 작업(컨피그레이션)은 구현되지 않습니다.
- AsyncOS는 SNMPv1, v2 및 v3을 지원합니다. SNMPv3에 대한 자세한 내용은 RFC 2571-2575를 참조하십시오.
- 메시지 인증 및 암호화는 SNMPv3을 사용하도록 설정하는 경우 필수 사항입니다. 인증과 암호화를 위한 암호는 서로 달라야 합니다. 암호화 알고리즘은 AES(권장) 또는 DES일 수 있습니다. 인증 알고리즘은 SHA-1(권장) 또는 MD5일 수 있습니다. `snmpconfig` 명령은 다음에 실행할 때 암호를 "기억"합니다.
- SNMPv3 사용자 이름: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- SNMPv1 또는 SNMPv2만 사용하는 경우 커뮤니티 문자열을 설정해야 합니다. 커뮤니티 문자열은 기본값이 `public`이 아닙니다.
- SNMPv1 및 SNMPv2에 대해 SNMP GET 요청을 수락할 네트워크를 지정해야 합니다.
- 트랩을 사용하려면 SNMP 관리자(AsyncOS에 포함되지 않음)를 실행하고 트랩 대상으로 해당 IP 주소를 입력해야 합니다. (호스트 이름을 사용할 수 있지만, 그럴 경우 DNS가 작동하는 경우에만 트랩이 작동합니다.)

MIB 파일

MIB 파일은 http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html에서 사용할 수 있습니다. 각 MIB 파일의 최신 버전을 사용합니다.

여러 MIB 파일이 있습니다.

- asyncoswebsecurityappliance-mib.txt - 웹 보안 어플라이언스용 엔터프라이즈 MIB의 SNMPv2 호환 설명입니다.
- ASYNCOS-MAIL-MIB.txt - 이메일 보안 어플라이언스용 엔터프라이즈 MIB의 SNMPv2 호환 설명입니다.
- IRONPORT-SMI.txt — 이 "SMI(Structure of Management Information)" 파일은 asyncoswebsecurityappliance-mib의 역할을 정의합니다.

이 릴리스는 RFC 1213 및 1907에 정의된 대로 MIB-II의 읽기 전용 하위 집합을 구현합니다.

SNMP 모니터링 사용 및 구성

어플라이언스에 대한 시스템 상태 정보를 수집하도록 SNMP를 구성하려면 CLI(Command Line Interface)에서 `snmpconfig` 명령을 사용합니다. 인터페이스에 대한 값의 선택 및 구성이 완료되면 어플라이언스는 SNMPv3 GET 요청에 응답합니다.

SNMP 모니터링을 사용할 때 다음 사항에 유의해야 합니다.

- 이러한 버전 3 요청에는 일치하는 암호가 포함되어야 합니다.
- 기본적으로 버전 1 및 2 요청은 거부됩니다.
- 활성화된 경우 버전 1 및 2 요청에 일치하는 커뮤니티 문자열을 포함해야 합니다.

하드웨어 개체

IPMI(Intelligent Platform Management Interface) 사양을 준수하는 하드웨어 센서는 온도, 팬 속도 및 전원 공급 장치 상태와 같은 정보를 보고합니다.

모니터링에 사용 가능한 하드웨어 관련 개체(예: 팬 수 또는 작동 온도 범위)를 확인하려면 사용 중인 어플라이언스 모델에 대한 하드웨어 설명서를 참조하십시오.

관련 주제

- 문서 집합, C-1페이지

SNMP 트랩

SNMP는 하나 이상의 조건이 충족되는 경우 관리 애플리케이션에 알리기 위해 트랩 또는 알림을 전송하는 기능을 제공합니다.트랩은 트랩을 전송하는 시스템의 구성 요소와 관련된 데이터를 포함하는 네트워크 패킷입니다.트랩은 SNMP 에이전트(이 경우 Cisco Web Security Appliance 어플라이언스)에서 조건이 충족될 때 생성됩니다. 조건이 충족되면 SNMP 에이전트가 SNMP 패킷을 만들어 SNMP 관리 콘솔 소프트웨어를 실행 중인 호스트에 전송합니다.

인터페이스에 대해 SNMP를 사용하도록 설정할 때 SNMP 트랩을 구성할 수 있습니다(특정 트랩 사용 또는 사용 안 함).

여러 트랩 대상을 지정하려면, 트랩 대상에 대한 프롬프트가 표시될 때 쉼표로 구분된 IP 주소를 최대 10개 입력할 수 있습니다.

관련 주제

- connectivityFailure SNMP 트랩 정보, 22-36페이지

connectivityFailure SNMP 트랩 정보

connectivityFailure 트랩은 어플라이언스의 인터넷 연결을 모니터링하기 위한 것입니다. 5~7초마다 단일 외부 서버에 연결하고 HTTP GET 요청을 전송하려고 시도하여 이를 수행합니다. 기본적으로 모니터링되는 URL은 포트 80의 `downloads.ironport.com`입니다.

모니터링되는 URL 또는 포트를 변경하려면 `snmpconfig` 명령을 실행하고 이미 사용하도록 설정된 경우에도 connecivityFailure 트랩을 사용하도록 설정합니다. URL을 변경하라는 프롬프트가 표시됩니다.

정보 connectivityFailure 트랩을 시뮬레이션하기 위해 `dnsconfig` CLI 명령을 사용하여 작동하지 않는 DNS 서버를 입력할 수 있습니다. downloads.ironport.com 검색에 실패하고 5~7초마다 트랩이 전송됩니다. 테스트를 완료한 후 DNS 서버를 작업 중인 서버로 다시 변경해야 합니다.

CLI 예: snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
```

```
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit
```

```
Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

문제 해결

- 일반 트러블슈팅 모범 사례
- 인증 문제
- 차단된 개체 문제
- 브라우저 문제
- DNS 문제
- 페일오버 문제
- 기능 키가 만료됨
- FTP 문제
- 하드웨어 문제
- HTTPS/암호 해독/인증서 문제
- ISE(Identity Services Engine) 문제
- 기록 문제
- 정책 문제
- 파일 평판 및 파일 분석 문제
- 재부팅 문제
- 사이트 액세스 문제
- 업스트림 프록시 문제
- 가상 어플라이언스
- WCCP 문제
- 패킷 캡처
- 지원에 대한 작업

일반 트러블슈팅 모범 사례

다음 맞춤형 필드를 포함하도록 액세스 로그를 구성합니다.

%u, %g, %m, %k, %L(이러한 값은 대/소문자를 구분함)

이러한 필드에 대한 설명은 액세스 로그 형식 지정자 및 W3C 로그 파일 필드, 21-31페이지를 참조하십시오.

컨피그레이션 지침은 액세스 로그 맞춤화, 21-26페이지 및 로그 서브스크립션 추가 및 편집, 21-7페이지를 참조하십시오.

인증 문제

- 인증 문제에 대한 트러블슈팅 툴
- 실패한 인증이 정상적인 작업에 영향을 미침
- LDAP 문제
- 기본 인증 문제
- 단일 로그인 문제
- 관련 주제:
  - 일반 트러블슈팅 모범 사례
  - HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨
  - 인증을 지원하지 않는 URL에 액세스할 수 없음
  - 업스트림 프록시에서 클라이언트 요청 실패

인증 문제에 대한 트러블슈팅 툴

Kerberos 티켓 캐시를 확인하고 비우기 위한 KerbTray 또는 klist(둘 다 Windows Server Resources Kit의 일부임). Active Directory를 보고 편집하기 위한 Active Directory Explorer. Wireshark는 네트워크 트러블슈팅에 사용할 수 있는 패킷 분석기입니다.

실패한 인증이 정상적인 작업에 영향을 미침

특정 사용자 에이전트 또는 애플리케이션이 인증하는 데 실패하고 액세스가 거부된 경우에는 웹 보안 어플라이언스에 반복적으로 요청을 전송하고, 차례로 머신 자격 증명이 있는 Active Directory 서버에 반복적으로 요청을 전송합니다. 경우에 따라 이는 정상적인 작업에 영향을 미칠 수 있습니다.

최상의 결과를 얻으려면 이러한 사용자 에이전트에 대한 인증을 우회합니다. 문제가 되는 사용자 에이전트에 대한 인증 우회, 5-28페이지를 참조하십시오.

LDAP 문제

- NTLMSSP로 인해 LDAP 사용자가 인증에 실패함
- LDAP 참조로 인해 LDAP 인증 실패

NTLMSSP로 인해 LDAP 사용자가 인증에 실패함

LDAP 서버는 NTLMSSP를 지원하지 않습니다. Internet Explorer와 같은 일부 클라이언트 애플리케이션은 NTLMSSP와 기본 중에서 선택해야 할 때 항상 NTLMSSP를 선택합니다. 다음 모든 조건에 해당하는 경우 사용자가 인증에 실패합니다.

- 사용자가 LDAP 영역에만 있습니다.
- 식별 프로필에서 LDAP 및 NTLM 영역을 모두 포함하는 시퀀스를 사용합니다.
- 식별 프로필에서 "기본 또는 NTLMSSP" 인증 체계를 사용합니다.
- 사용자가 기본이 아닌 NTLMSSP를 선택하는 애플리케이션에서 요청을 전송합니다.

식별 프로필 또는 인증 영역이나 위의 조건 중 하나 이상이 거짓인 애플리케이션을 재구성합니다.

LDAP 참조로 인해 LDAP 인증 실패

다음 모든 조건에 해당하는 경우 LDAP 인증이 실패합니다.

- LDAP 인증 영역에서 Active Directory 서버를 사용합니다.
- Active Directory 서버가 다른 인증 서버에 대한 LDAP 참조를 사용합니다.
- 참조된 인증 서버를 웹 보안 어플라이언스에 사용할 수 없습니다.

해결 방법:

- 어플라이언스에서 LDAP 인증 영역을 구성할 때 Active Directory 포리스트에 전역 카탈로그 서버(기본 포트는 3268)를 지정합니다.
- `advancedproxyconfig > authentication` CLI 명령을 사용하여 LDAP 참조를 사용하지 않도록 설정합니다. LDAP 참조는 기본적으로 사용하지 않도록 설정되어 있습니다.

기본 인증 문제

- 기본 인증 실패

관련 문제

- 업스트림 프록시가 기본 자격 증명을 수신하지 않음

기본 인증 실패

기본 인증 체계를 사용하는 경우 AsyncOS for Web에서는 암호에 7비트 ASCII 문자만 지원합니다. 암호에 7비트 ASCII가 아닌 문자가 포함되어 있는 경우 기본 인증이 실패합니다.

단일 로그인 문제

• 사용자에게 자격 증명 프롬프트가 잘못 표시됨

사용자에게 자격 증명 프롬프트가 잘못 표시됨

웹 보안 어플라이언스가 WCCP v2 지원 디바이스에 연결될 때 NTLM 인증이 작동하지 않는 경우가 있습니다. 사용자가 투명 NTLM 인증을 올바르게 수행하지 않는 매우 제한적인 버전의 Internet Explorer를 사용하여 요청을 작성하고 어플라이언스가 WCCP v2 지원 디바이스에 연결된 경우, 기본적으로 브라우저는 기본 인증을 사용합니다. 이로 인해 프롬프트가 표시되지 않아야 하는 경우에 사용자에게 인증 자격 증명 프롬프트가 표시됩니다.

해결 방법

Internet Explorer에서 웹 보안 어플라이언스 리디렉션 호스트 이름을 로컬 인트라넷 영역의 신뢰할 수 있는 사이트 목록에 추가합니다(Tools(도구) > Internet Options(인터넷 옵션) > Security(보안) 탭).

브라우저 문제

• WPAD가 Firefox에서 작동하지 않음

WPAD가 Firefox에서 작동하지 않음

Firefox 브라우저가 WPAD를 사용하는 DHCP 조회를 지원하지 않을 수 있습니다. 최신 정보는 `https://bugzilla.mozilla.org/show_bug.cgi?id=356831`을 참조하십시오.

PAC 파일이 웹 보안 어플라이언스에서 호스팅될 때 WPAD와 함께 Firefox(또는 DHCP를 지원하지 않는 다른 브라우저)를 사용하려면 포트 80을 통해 PAC 파일을 제공하도록 어플라이언스를 구성합니다.

1단계 **Security Services(보안 서비스) > Web Proxy(웹 프록시)**를 선택하고 **HTTP Ports to Proxy(프록시에 대한 HTTP 포트)** 필드에서 포트 80을 삭제합니다.

2단계 파일을 어플라이언스에 업로드할 때 포트 80을 PAC 서버 포트로 사용합니다.

3단계 브라우저가 수동으로 포트 80의 웹 프록시를 가리키도록 구성된 경우 HTTP Ports to Proxy(프록시에 대한 HTTP 포트) 필드에서 다른 포트를 가리키도록 해당 브라우저를 재구성합니다.

4단계 PAC 파일에서 포트 80에 대한 참조를 변경합니다.

DNS 문제

- 경고: DNS 캐시를 부트스트랩하는 데 실패함

경고: DNS 캐시를 부트스트랩하는 데 실패함

어플라이언스가 재부팅될 때 "DNS 캐시를 부트스트랩하는 데 실패함" 메시지를 포함하는 경고가 생성되는 경우, 이는 시스템에서 기본 DNS 서버에 연결할 수 없음을 나타냅니다. 이는 네트워크 연결이 설정되기 전에 DNS 하위 시스템이 온라인 상태가 된 경우 부팅 시에 발생할 수 있습니다. 이 메시지가 다른 때에 나타나면 네트워크 문제를 나타내거나 DNS 컨피그레이션이 유효한 서버를 가리키고 있지 않음을 나타낼 수 있습니다.

기능 키가 만료됨

웹 인터페이스를 통해 액세스하려고 시도하는 기능에 대한 기능 키가 만료된 경우 Cisco 담당자 또는 지원 조직에 문의하십시오.

페일오버 문제

- 잘못된 페일오버 구성
- 가상 어플라이언스에 대한 페일오버 문제

잘못된 페일오버 구성

페일오버 그룹을 잘못 구성하면 여러 마스터 어플라이언스 또는 기타 페일오버 문제가 발생할 수 있습니다. CLI `failoverconfig` 명령의 `testfailovergroup` 하위 명령을 사용하여 페일오버 문제를 진단합니다.

예를 들면 다음과 같습니다.

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: MASTER
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

가상 어플라이언스에 대한 페일오버 문제

가상 어플라이언스에서 구축하는 경우 하이퍼바이저에 인터페이스/가상 스위치가 혼합 모드를 사용하도록 구성되었는지 확인하십시오.

FTP 문제

- URL 카테고리가 일부 FTP 사이트를 차단하지 않음
- 대용량 FTP 전송 연결 끊기
- 파일 업로드 후 FTP 서버에 0바이트 파일이 표시됨
- FTP-over-HTTP 요청에서 Chrome 브라우저가 사용자 에이전트로 탐지되지 않음, A-6페이지
- 관련 주제:
  - 업스트림 프록시를 통해 FTP 요청을 라우팅할 수 없음
  - HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨

URL 카테고리가 일부 FTP 사이트를 차단하지 않음

네이티브 FTP 요청이 FTP 프록시에 투명하게 리디렉션될 때 FTP 서버에 대한 호스트 이름 정보를 포함하지 않으며 해당 IP 주소만 포함합니다. 따라서 호스트 이름 정보만 포함하는 일부 미리 정의된 URL 카테고리 및 웹 평판 필터는 요청의 대상이 해당 서버로 지정된 경우에도 네이티브 FTP 요청과 일치되지 않습니다. 이러한 사이트에 대한 액세스를 차단하려면 해당 IP 주소를 사용하여 맞춤형 URL 카테고리를 생성해야 합니다.

대용량 FTP 전송 연결 끊기

FTP 프록시와 FTP 서버 간의 연결 속도가 느리면 대용량 파일을 업로드하는 데 오랜 시간이 소요될 수 있습니다(특히 Cisco 데이터 보안 필터가 사용하도록 설정된 경우). 이로 인해 FTP 프록시가 전체 파일을 업로드하기 전에 FTP 클라이언트가 시간 초과될 수 있으며 실패한 트랜잭션 알림을 받을 수 있습니다. 그러나 트랜잭션이 실패하지 않고 백그라운드에서 계속 실행되며 FTP 프록시에서 트랜잭션을 완료합니다.

FTP 클라이언트에서 유휴 시간 초과 값을 적절하게 늘려서 이 문제를 해결할 수 있습니다.

파일 업로드 후 FTP 서버에 0바이트 파일이 표시됨

아웃바운드 안티멀웨어 스캐닝으로 인해 FTP 프록시가 업로드를 차단하는 경우 FTP 클라이언트에서 FTP 서버에 0바이트 파일을 생성합니다.

FTP-over-HTTP 요청에서 Chrome 브라우저가 사용자 에이전트로 탐지되지 않음

Chrome 브라우저에는 FTP-over-HTTP 요청의 사용자 에이전트 문자열이 포함되어 있지 않으므로 Chrome은 해당 요청에서 사용자 에이전트로 탐지될 수 없습니다.

하드웨어 문제

- 어플라이언스 전원 주기, A-7페이지
- 어플라이언스 상태 표시기, A-7페이지
- 경고: 380 또는 680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트), A-7페이지

어플라이언스 전원 주기

중요! x80 어플라이언스의 전원을 순환해야 하는 경우 전원 버튼을 누르기 전에 어플라이언스가 다시 표시될 때까지(모든 LED가 녹색) 20분 이상 기다립니다.

어플라이언스 상태 표시기

하드웨어 어플라이언스의 전면 및/또는 후면 패널에 있는 표시등은 어플라이언스의 상태를 나타냅니다. 이러한 표시기에 대한 설명은 하드웨어 설명서 (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html)를 참조하십시오.

어플라이언스 사양(예: 온도 범위)도 이러한 문서에서 확인할 수 있습니다.

경고: 380 또는 680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트)

이 경고문은 문제를 나타낼 수도 있고 그렇지 않을 수도 있습니다. 배터리 재인식 시간 초과 자체가 RAID 컨트롤러에 문제가 있음을 의미하지는 않습니다. 후속 재인식에서 컨트롤러가 복구될 수 있습니다. 이것이 다른 문제의 부작용이 아닌지 확인하려면 앞으로 48시간 동안 다른 RAID 경고문이 이메일로 전달되는지 모니터링하십시오. 시스템에서 다른 RAID 관련 경고가 표시되지 않으면 이 경고를 안전하게 무시할 수 있습니다.

HTTPS/암호 해독/인증서 문제

- URL 카테고리 기준을 사용하는 라우팅 정책을 통해 HTTPS 사이트에 액세스
- HTTPS 요청 실패
- 특정 웹 사이트에 대한 암호 해독 우회
- 경고: 보안 인증서 문제
- 관련 주제:
  - HTTPS 트랜잭션 기록
  - HTTPS에 대한 액세스 정책을 구성할 수 없음
  - HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨

URL 카테고리 기준을 사용하는 라우팅 정책을 통해 HTTPS 사이트에 액세스

투명하게 리디렉션된 HTTPS 요청의 경우 웹 프록시가 목적지 서버에 접속하여 서버 이름과 서버가 속한 URL 카테고리를 확인해야 합니다. 이로 인해 웹 프록시가 라우팅 정책 그룹 구성원 자격을 평가할 때는 아직 목적지 서버에 접속하지 않았으므로 HTTPS 요청의 URL 카테고리를 알 수 없습니다. 웹 프록시가 URL 카테고리를 알지 못하는 경우 URL 카테고리를 구성원 자격 기준으로 사용하는 라우팅 정책과 투명 HTTPS 요청을 일치시킬 수 없습니다.

따라서 투명하게 리디렉션된 HTTPS 트랜잭션은 URL 카테고리로 라우팅 정책 그룹 구성원 자격 기준을 정의하지 않는 라우팅 정책에만 일치됩니다. 모든 사용자 정의 라우팅 정책이 URL 카테고리로 구성원 자격을 정의하는 경우에는 투명 HTTPS 트랜잭션이 기본 라우팅 정책 그룹과 일치됩니다.

HTTPS 요청 실패

- IP 기반 서로게이트 및 투명 요청을 사용하는 HTTPS

IP 기반 서로게이트 및 투명 요청을 사용하는 HTTPS

이전 HTTP 요청에서 사용 가능한 인증 정보가 없는 클라이언트에서 HTTPS 요청을 가져오는 경우, HTTPS 프록시를 구성하는 방법에 따라 AsyncOS가 HTTPS 요청에 실패하거나 사용자를 인증하기 위해 HTTPS 요청을 암호 해독합니다. 이 동작을 정의하려면 Security Services(보안 서비스) > HTTPS Proxy(HTTPS 프록시) 페이지의 HTTPS Transparent Request(HTTPS 투명 요청) 설정을 사용합니다. 암호 해독 정책 장의 HTTPS 프록시 사용 섹션을 참조하십시오.

특정 웹 사이트에 대한 암호 해독 우회

프록시 서버(예: 웹 프록시)에서 트래픽의 암호를 해독할 때 일부 HTTPS 서버가 예상대로 작동하지 않습니다. 예를 들어, 일부 웹 사이트 및 이와 연결된 웹 애플리케이션과 애플릿(예: 보안 수준이 높은 뱅킹 사이트)은 운영 체제 인증서 저장소에 의존하는 대신에 신뢰할 수 있는 인증서의 하드 코딩된 목록을 유지 관리합니다.

모든 사용자가 이러한 유형의 사이트에 액세스할 수 있도록 이러한 서버에 대한 HTTPS 트래픽의 암호 해독을 우회할 수 있습니다.

1단계 고급 속성을 구성하여 영향을 받는 HTTPS 서버를 포함하는 맞춤형 URL 카테고리를 생성합니다.

2단계 1단계에서 구성원 자격의 일부로 생성된 맞춤형 URL 카테고리를 사용하는 암호 해독 정책을 생성하고 맞춤형 URL 카테고리에 대한 조치를 통과로 설정합니다.

경고: 보안 인증서 문제

일반적으로 어플라이언스에서 생성하거나 업로드하는 루트 인증서 정보는 클라이언트 애플리케이션에서 신뢰할 수 있는 루트 인증 기관으로 나열되지 않습니다. 기본적으로 대부분의 웹 브라우저에서는 사용자가 HTTPS 요청을 전송할 때 클라이언트 애플리케이션에서 웹 사이트의 보안 인증서에 문제가 있음을 알려주는 경고 메시지를 표시합니다. 일반적으로 이 오류 메시지는 웹 사이트의 보안 인증서가 신뢰할 수 있는 인증 기관에서 발급되지 않았거나 웹 사이트가 알 수 없는 인증 기관에서 인증되었음을 나타냅니다. 일부 다른 클라이언트 애플리케이션은 사용자에게 이 경고 메시지를 표시하지 않으며 사용자가 인식할 수 없는 인증서를 수락하도록 허용하지도 않습니다.

참고 **Mozilla Firefox 브라우저:** Mozilla Firefox 브라우저를 사용하여 작업하려면 업로드하는 인증서에 "basicConstraints=CA:TRUE"가 포함되어야 합니다. 이 제약을 통해 Firefox가 루트 인증서를 신뢰할 수 있는 루트 인증 기관으로 인식할 수 있습니다.

ISE(Identity Services Engine) 문제

- ISE 문제 트러블슈팅 툴
- ISE 서버 연결 문제
- ISE 관련 위험 로그 메시지

ISE 문제 트러블슈팅 툴

다음은 ISE 관련 문제를 트러블슈팅하는 데 유용할 수 있습니다.

- ISE 서버에 대한 연결을 테스트하는 데 사용되는 ISE 테스트 유틸리티가 중요한 연결 관련 정보를 제공합니다. 이는 ISE(Identity Services Engine) 페이지의 **Start Test(테스트 시작)** 옵션입니다. ISE 서비스에 연결을 참조하십시오.
- ISE 및 프록시 로그의 경우 로그를 통해 시스템 활동 모니터링을 참조하십시오.
- ISE 관련 CLI 명령 `iseconfig` 및 `isedata`, 특히 SGT(Security Group Tag) 다운로드를 확인하기 위한 `isedata`. 자세한 내용은 Web Security Appliance CLI 명령을 참조하십시오.
- 웹 추적 및 정책 추적 기능을 사용하여 정책 일치 문제를 디버그할 수 있습니다(예: 허용되어야 하는 사용자가 차단되었거나 그 반대의 경우). 자세한 내용은 Web Tracking(웹 추적) 페이지 및 정책 트러블슈팅 툴: 정책 추적을 참조하십시오.
- 패킷 캡처의 경우 지원에 대한 작업.
- 인증서 상태를 확인하기 위해 www.openssl.org에서 제공하는 `openssl ocsp`(Online Certificate Status Protocol) 유틸리티를 사용할 수 있습니다.

ISE 서버 연결 문제

인증서 문제

WSA 및 ISE 서버는 성공적인 연결을 위해 인증서를 사용하여 상호 인증합니다. 따라서 한 엔티티에서 제공하는 각 인증서를 다른 엔티티에서 인식할 수 있어야 합니다. 예를 들어, WSA의 클라이언트 인증서가 자체 서명된 인증서인 경우 동일한 인증서가 적절한 ISE 서버의 신뢰할 수 있는 인증서 목록에 있어야 합니다. 상대적으로, WSA 클라이언트 인증서가 CA 서명 인증서인 경우 CA 루트 인증서가 적절한 ISE 서버에 있어야 합니다. ISE 서버 관련 관리 및 pxGrid 인증서에 유사한 요건이 적용됩니다.

인증서 요건 및 설치는 Cisco Identity Services Engine 통합에 설명되어 있습니다. 인증서 관련 문제가 발생하는 경우 다음 사항을 확인합니다.

- CA 서명 인증서를 사용하는 경우:
  - 관리 및 pxGrid 인증서에 대한 루트 CA 서명 인증서가 WSA에 있는지 확인합니다.
  - WSA 클라이언트 인증서에 대한 루트 CA 서명 인증서가 ISE 서버의 신뢰할 수 있는 인증서 목록에 있는지 확인합니다.
- 자체 서명된 인증서를 사용하는 경우:
  - WSA에서 생성되고 다운로드된 WSA 클라이언트 인증서가 ISE 서버에 업로드되었으며 ISE 서버의 신뢰할 수 있는 인증서 목록에 있는지 확인합니다.
  - ISE 서버에서 생성되고 다운로드된 ISE 관리 및 pxGrid 인증서가 WSA에 업로드되었으며 해당 인증서 목록에 있는지 확인합니다.
- 만료된 인증서:
  - 업로드 시 유효했던 인증서가 만료되지 않았는지 확인합니다.

인증서 문제를 표시하는 로그 출력

다음 ISE 서비스 로그 부분은 누락되거나 유효하지 않은 인증서로 인한 클라이언트 연결 시간 초과를 보여줍니다.

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

이러한 WSA의 추적 레벨 로그 항목은 30초 후에 ISE 서버에 연결하려는 시도가 종료되었음을 나타냅니다.

네트워크 문제

- ISE(Identity Services Engine) 페이지(ISE 서비스에 연결)에서 **Start Test(테스트 시작)** 중에 ISE 서버에 대한 연결이 실패하는 경우 포트 443 및 5222에 구성된 ISE 서버에 대한 연결을 확인합니다.

  포트 5222는 공식적인 클라이언트-서버 XMPP(Extensible Messaging and Presence Protocol) 포트이며 ISE 서버에 연결하는 데 사용되고 Jabber 및 Google Talk와 같은 애플리케이션에서도 사용됩니다. 일부 방화벽은 포트 5222를 차단하도록 구성됩니다.

  연결을 확인하는 데 사용할 수 있는 툴에는 `telnet` 및 `tcpdump`가 있습니다.

기타 ISE 서버 연결 문제

WSA가 ISE 서버와 연결하려고 시도할 때 다음 문제로 인해 장애가 발생할 수 있습니다.

- ISE 서버의 라이센스가 만료되었습니다.
- ISE 서버의 Administration(관리) > pxGrid Services(pxGrid 서비스) 페이지에서 pxGrid 노드 상태가 "연결되지 않음"입니다. 이 페이지에서 "Enable Auto-Registration(자동 등록 사용)"이 선택되어야 합니다.
- ISE 서버에 오래된 WSA 클라이언트(특히 "test_client" 또는 "pxgrid_client")가 있습니다. 이러한 클라이언트는 삭제되어야 합니다. ISE 서버에서 Administration(관리) > pxGrid Services(pxGrid 서비스) > Clients(클라이언트)를 참조하십시오.
- 모든 서비스가 실행되기 전에 WSA가 ISE 서버에 연결하려고 시도하는 중입니다.

  ISE 서버의 일부 변경 사항(예: 인증서 업데이트)을 적용하려면 ISE 서버 또는 ISE 서버에서 실행 중인 서비스를 재시작해야 합니다. 이 시간 동안 ISE 서버에 연결하려는 시도는 실패하지만 결국 연결에 성공합니다.

ISE 관련 위험 로그 메시지

이 섹션에는 WSA의 ISE 관련 위험 로그 메시지에 대한 설명이 포함되어 있습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  WSA의 ISE 프로세스가 30초 동안 ISE 서버에 연결하는 데 실패했습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config`

  WSA의 ISE(Identity Service Engine) 컨피그레이션 페이지에서 WSA 클라이언트 인증서 및 키가 업로드되거나 생성되지 않았습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  WSA의 ISE 프로세스가 120초 동안 ISE 서버에 연결할 수 없었으며 종료되었습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed …`

  WSA의 ISE 프로세스가 업데이트를 위해 ISE 서버를 구독할 수 없습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: …`

  ISE 서버 연결을 위해 WSA의 ISE 클라이언트를 생성하는 동안 내부 오류가 발생했습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: …`

  연결 또는 다시 연결 중에 SGT의 벌크 다운로드에 실패했음을 나타내는 내부 오류가 발생했습니다.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: …`

  WSA의 ISE 서비스를 시작하는 데 실패했습니다.
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal …`

  WSA의 ISE 서비스가 `heimdall`에 준비 신호를 전송할 수 없습니다.
- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal …`

  WSA의 ISE 서비스가 `heimdall`에 재시작 신호를 전송할 수 없습니다.

기록 문제

- 맞춤형 URL 카테고리가 액세스 로그 항목에 표시되지 않음
- HTTPS 트랜잭션 기록
- 경고: 생성되는 데이터의 비율을 유지할 수 없음
- 서드파티 로그 분석기 툴을 통한 W3C 액세스 로그 사용 문제

맞춤형 URL 카테고리가 액세스 로그 항목에 표시되지 않음

웹 액세스 정책 그룹에 모니터링으로 설정된 맞춤형 URL 카테고리가 있으며 일부 다른 구성 요소(예: 웹 평판 필터 또는 DVS 엔진)가 맞춤형 URL 카테고리의 URL에 대한 요청을 허용하거나 차단하기로 최종 결정을 내린 경우에는 요청의 액세스 로그 항목에 맞춤형 URL 카테고리가 아닌 미리 정의된 URL 카테고리가 표시됩니다.

HTTPS 트랜잭션 기록

액세스 로그의 HTTPS 트랜잭션은 HTTP 트랜잭션과 유사하지만 약간 다른 특성을 가집니다. 기록되는 항목은 트랜잭션이 HTTPS 프록시에 명시적으로 전송되었는지 또는 투명하게 리디렉션되었는지에 따라 다릅니다.

- **TUNNEL.** HTTPS 요청이 HTTPS 프록시에 투명하게 리디렉션된 경우 액세스 로그에 기록됩니다.
- **CONNECT.** HTTPS 요청이 HTTPS 프록시에 명시적으로 전송된 경우에 액세스 로그에 기록됩니다.

HTTPS 트래픽이 암호 해독될 때 액세스 로그에는 트랜잭션에 대한 2개의 항목이 포함됩니다.

- 처리되는 요청의 유형에 따라 TUNNEL 또는 CONNECT.
- HTTP 메서드 및 암호 해독된 URL. 예를 들어, "GET https://ftp.example.com"입니다.

HTTPS 프록시가 트래픽을 암호 해독하는 경우에만 전체 URL이 표시됩니다.

경고: 생성되는 데이터의 비율을 유지할 수 없음

버퍼가 가득 차서 내부 기록 프로세스가 웹 트랜잭션 이벤트를 삭제하는 경우 AsyncOS for Web이 구성된 경고 수신자에게 위험 이메일 메시지를 전송합니다.

기본적으로 웹 프록시의 로드가 과도하게 많은 경우 나중에 웹 프록시 로드가 감소할 때 기록할 수 있도록 내부 기록 프로세스가 이벤트를 버퍼에 저장합니다. 기록 버퍼가 가득 차는 경우 웹 프록시에서는 계속해서 트래픽을 처리하지만 기록 프로세스가 액세스 로그 또는 웹 추적 보고서에 일부 이벤트를 기록하지 않습니다. 이는 웹 트래픽이 급증하는 동안 발생할 수 있습니다.

그러나 어플라이언스가 지속된 기간 동안 용량을 초과하는 경우에도 기록 버퍼가 가득 찰 수 있습니다. AsyncOS for Web은 기록 프로세스에서 더 이상 데이터를 삭제하지 않을 때까지 몇 분마다 계속해서 위험 이메일 메시지를 전송합니다.

위험 메시지에는 다음 텍스트가 포함되어 있습니다.

```
Reporting Client: The reporting system is unable to maintain the rate of data being
generated. Any new data generated will be lost.
```

AsyncOS for Web에서 이 위험 메시지를 지속적으로 또는 자주 전송하는 경우 어플라이언스의 용량이 초과되었을 수 있습니다. Cisco 고객 지원에 문의하여 추가 웹 보안 어플라이언스 용량이 필요한지 여부를 확인하십시오.

서드파티 로그 분석기 툴을 통한 W3C 액세스 로그 사용 문제

서드파티 로그 분석기 툴을 사용하여 W3C 액세스 로그를 읽고 구문 분석하려는 경우 "timestamp(타임스탬프)" 필드를 포함해야 할 수 있습니다. timestamp(타임스탬프) W3C 필드는 UNIX Epoch 이후의 시간을 표시하며 대부분의 로그 분석기는 이 형식의 시간만 이해합니다.

정책 문제

- HTTPS에 대한 액세스 정책을 구성할 수 없음
- 차단된 개체 문제
- 식별 프로필이 정책에서 사라짐
- 정책 일치 실패
- 정책 트러블슈팅 툴: 정책 추적
- 관련 주제: URL 카테고리 기준을 사용하는 라우팅 정책을 통해 HTTPS 사이트에 액세스

HTTPS에 대한 액세스 정책을 구성할 수 없음

(버그 38046, 40843, 41282)

원래 7장 웹 프록시에 있던 트랜잭션 요청 차단, 허용 또는 리디렉션 장의 프로토콜 및 사용자 에이전트(표 다음), 9-7페이지에서 가져온 참고 사항

HTTPS 프록시가 사용하도록 설정된 경우 암호 해독 정책이 모든 HTTPS 정책 결정을 처리합니다. 더 이상 HTTPS로 액세스 및 라우팅 정책 그룹 구성원 자격을 정의할 수 없으며 HTTPS 트랜잭션을 차단하도록 액세스 정책을 구성할 수 없습니다.

일부 액세스 및 라우팅 정책 그룹 구성원 자격이 HTTPS로 정의되고 일부 액세스 정책이 HTTPS를 차단하는 경우에 HTTPS 프록시를 사용하도록 설정하면 해당 액세스 및 라우팅 정책 그룹이 사용하지 않도록 설정됩니다. 언제든지 정책을 사용하도록 선택할 수 있지만 모든 HTTPS 관련 컨피그레이션이 제거됩니다. (버그 38046, 40843, 41282)

차단된 개체 문제

- 일부 Microsoft Office 파일이 차단되지 않음
- DOS 실행 가능 개체 유형을 차단하면 Windows OneCare에 대한 업데이트도 차단됨

일부 Microsoft Office 파일이 차단되지 않음

Block Object Type(개체 유형 차단) 섹션에서 Microsoft Office 파일을 차단할 때 일부 Microsoft Office 파일이 차단되지 않을 수 있습니다.

모든 Microsoft Office 파일을 차단해야 하는 경우 Block Custom MIME Types(맞춤형 MIME 유형 차단) 필드에서 **`application/x-ole`**를 추가합니다. 그러나 이 맞춤형 MIME 유형을 차단하면 Visio 파일 및 일부 서드파티 애플리케이션과 같은 모든 Microsoft 복합 개체 형식 유형도 차단됩니다.

DOS 실행 가능 개체 유형을 차단하면 Windows OneCare에 대한 업데이트도 차단됨

DOS 실행 가능 개체 유형을 차단하도록 웹 보안 어플라이언스를 구성하면 어플라이언스가 Windows OneCare에 대한 업데이트도 차단합니다.

식별 프로필이 정책에서 사라짐

식별 프로필을 사용하지 않도록 설정하면 연결된 정책에서 식별 프로필이 제거됩니다. 식별 프로필이 사용하도록 설정되어 있는지 확인한 후 정책에 식별 프로필을 다시 추가합니다.

정책 일치 실패

- 정책이 적용되지 않음
- HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨
- 사용자가 HTTPS 및 FTP over HTTP 요청에 대한 전역 정책과 일치함
- 사용자가 잘못된 액세스 정책에 할당됨

정책이 적용되지 않음

여러 식별 프로필의 기준이 동일한 경우 AsyncOS가 일치하는 첫 번째 식별 프로필에 트랜잭션을 할당합니다. 따라서 트랜잭션이 추가적으로 동일한 식별 프로필에 일치되지 않으며 다음에 나오는 동일한 식별 프로필에 적용된 정책이 일치되거나 적용되지 않습니다.

HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됨

자격 증명 암호화가 사용하도록 설정된 경우 IP 주소를 서로게이트로 사용하도록 어플라이언스를 구성합니다.

자격 증명 암호화가 사용하도록 설정되고 쿠키를 서로게이트 유형으로 사용하도록 구성된 경우 HTTPS 및 FTP over HTTP 요청에 대해 인증이 작동하지 않습니다. 이는 자격 증명 암호화가 사용하도록 설정된 경우에 웹 프록시가 인증을 위해 HTTPS 연결을 사용하여 클라이언트를 웹 프록시 자체로 리디렉션하기 때문입니다. 인증이 완료된 후 웹 프록시가 클라이언트를 다시 원래 웹 사이트로 리디렉션합니다. 웹 프록시가 계속해서 사용자를 식별하려면 서로게이트(IP 주소 또는 쿠키)를 사용해야 합니다. 그러나 요청이 HTTPS 또는 FTP over HTTP를 사용하는 경우에 쿠키를 사용하여 사용자를 추적하면 다음과 같은 동작이 발생합니다.

- **HTTPS.** 웹 프록시가 암호 해독 정책을 할당하기 전에 사용자 ID를 확인하고 트랜잭션의 암호를 해독해야 하지만 웹 프록시에서 트랜잭션의 암호를 해독하지 않는 경우 사용자를 식별하기 위한 쿠키를 확보할 수 없습니다.
- **FTP over HTTP.** FTP over HTTP를 사용하여 FTP에 액세스할 때의 딜레마는 HTTPS 사이트에 액세스하는 경우와 유사합니다. 웹 프록시가 액세스 정책을 할당하기 전에 사용자 ID를 확인해야 하지만 FTP 트랜잭션에서 쿠키를 설정할 수 없습니다.

따라서 HTTPS 및 FTP over HTTP 요청은 인증이 필요하지 않은 액세스 정책에만 일치됩니다. 일반적으로 전역 액세스 정책에는 인증이 필요하지 않으므로 전역 액세스 정책과 일치됩니다.

사용자가 HTTPS 및 FTP over HTTP 요청에 대한 전역 정책과 일치함

어플라이언스가 쿠키 기반 인증을 사용하는 경우 웹 프록시가 클라이언트에서 HTTPS 및 FTP over HTTP 요청에 대한 쿠키 정보를 가져오지 않습니다. 따라서 쿠키에서 사용자 이름을 가져올 수 없습니다.

HTTPS 및 FTP over HTTP 요청이 다른 구성원 자격 기준에 따라 여전히 식별 프로필과 일치하지만 식별 프로필에 인증이 필요한 경우에도 웹 프록시가 클라이언트에 인증 프롬프트를 표시하지 않습니다. 대신, 웹 프록시가 사용자 이름을 NULL로 설정하고 사용자가 인증되지 않은 것으로 간주합니다.

인증되지 않은 요청이 정책과 비교하여 평가될 때 "모든 ID"를 지정하고 "모든 사용자"에 적용되는 정책에만 일치됩니다. 일반적으로 이러한 정책은 전역 액세스 정책과 같은 전역 정책입니다.

사용자가 잘못된 액세스 정책에 할당됨

- 네트워크의 클라이언트에서는 NCSI(Network Connectivity Status Indicator)를 사용합니다.
- 웹 보안 어플라이언스에서는 NTLMSSP 인증을 사용합니다.
- 식별 프로필에서는 IP 기반 서로게이트를 사용합니다.

사용자는 사용자 고유의 자격 증명 대신에 머신 자격 증명을 사용하여 식별될 수 있으므로 잘못된 액세스 정책에 할당될 수 있습니다.

해결 방법:

- 머신 자격 증명에 대한 서로게이트 시간 초과 값을 줄입니다.

1단계 advancedproxyconfig > authentication CLI 명령을 사용합니다.

2단계 머신 자격 증명에 대한 서로게이트 시간 초과를 입력합니다.

정책 트러블슈팅 툴: 정책 추적

- 정책 추적 툴 정보
- 클라이언트 요청 추적
- 고급: 요청 세부 정보
- 고급: 응답 세부 정보 재지정

정책 추적 툴 정보

정책 추적 툴은 클라이언트 요청을 에뮬레이트한 후 웹 프록시가 해당 요청을 처리하는 방식에 대해 자세히 설명합니다. 웹 프록시 문제를 트러블슈팅할 때 클라이언트 요청을 추적하고 정책 처리를 디버그하는 데 사용될 수 있습니다. 기본 추적을 수행하거나 고급 추적 설정을 입력하고 옵션을 재지정할 수 있습니다.

참고 정책 추적 툴을 사용할 때 웹 프록시가 액세스 로그 또는 보고 데이터베이스에 요청을 기록하지 않습니다.

정책 추적 툴은 웹 프록시에서 사용되는 정책에 대해서만 요청을 평가합니다. 이러한 정책은 액세스, 암호화된 HTTPS 관리, 라우팅, 데이터 보안 및 아웃바운드 악성코드 스캐닝 정책입니다.

참고 SOCKS 및 외부 DLP 정책은 정책 추적 툴로 평가되지 않습니다.

클라이언트 요청 추적

참고 CLI 명령 `maxhttpheadersize`를 사용하여 프록시 요청에 대한 최대 HTTP 헤더 크기를 변경할 수 있습니다. 이 값을 늘리면 지정된 사용자가 다수의 인증 그룹에 속해 있거나 응답 헤더가 현재 최대 헤더 크기보다 큰 경우에 발생할 수 있는 정책 추적 실패를 완화할 수 있습니다. 이 명령에 대한 자세한 내용은 Web Security Appliance CLI 명령, B-6페이지를 참조하십시오.

1단계 **System Administration(시스템 관리) > Policy Trace(정책 추적)**를 선택합니다.

2단계 Destination URL(대상 URL) 필드에 추적할 URL을 입력합니다.

3단계 (선택 사항) 추가 에뮬레이션 매개변수를 입력합니다.

에뮬레이션 대상...	입력...
요청을 작성하는 데 사용되는 클라이언트 소스 IP.	Client IP Address(클라이언트 IP 주소) 필드에 IP 주소를 입력합니다. **참고** IP 주소를 지정하지 않으면 AsyncOS에서 localhost를 사용합니다. 또한 SGT(Security Group Tag)를 가져올 수 없으며 SGT 기반의 정책이 일치되지 않습니다.

에뮬레이션 대상...	입력...
요청을 작성하는 데 사용되는 인증/식별 자격 증명.	User Name(사용자 이름) 필드에 사용자 이름을 입력한 후 Authentication/Identification(인증/식별) 드롭다운 목록에서 ISE(Identity Services Engine) 또는 인증 영역을 선택합니다. **참고** 사용하도록 설정된 옵션만 사용할 수 있습니다. 즉, 인증 옵션 및 ISE 옵션이 모두 사용하도록 설정된 경우에만 사용할 수 있습니다. 여기에 입력하는 사용자의 인증을 위해서는 사용자가 Web Security appliance를 통해 이미 인증되어 있어야 합니다.

4단계 **Find Policy Match(정책 일치 찾기)**를 클릭합니다.

정책 추적 결과가 Results(결과) 창에 표시됩니다.

참고 HTTPS 트랜잭션 통과의 경우 정책 추적 툴이 추가적인 스캐닝을 무시하고 액세스 정책이 트랜잭션과 연결되지 않습니다. 마찬가지로, HTTPS 트랜잭션 암호 해독의 경우 이 툴이 실제로 트랜잭션의 암호를 해독하여 적용된 액세스 정책을 확인할 수 없습니다. 두 경우 모두와 트랜잭션 삭제의 경우에 추적 결과에 "Access policy: Not Applicable(액세스 정책: 적용할 수 없음)"이 표시됩니다.

관련 주제

- 고급: 요청 세부 정보, A-17페이지
- 고급: 응답 세부 정보 재지정, A-18페이지

고급: 요청 세부 정보

Policy Trace(정책 추적) 페이지, Advanced(고급) 섹션에 있는 Request Details(요청 세부 정보) 창의 설정을 사용하여 이 정책 추적에 대한 아웃바운드 악성코드 스캐닝 요청을 조정할 수 있습니다.

1단계 Policy Trace(정책 추적) 페이지의 **Advanced(고급)** 섹션을 확장합니다.

2단계 필요에 따라 Request Details(요청 세부 정보) 창의 필드를 완성합니다.

설정	설명
프록시 포트	추적 요청이 프록시 포트를 기반으로 정책 구성원 자격을 테스트하는 데 사용할 특정 프록시 포트를 선택합니다.
사용자 에이전트	요청에서 시뮬레이션할 사용자 에이전트를 지정합니다.
요청 시간	요청에서 시뮬레이션할 날짜 및 시간을 지정합니다.
파일 업로드	요청에서 업로드를 시뮬레이션할 로컬 파일을 선택합니다. 여기에서 업로드할 파일을 지정하면 웹 프록시가 GET 요청 대신에 HTTP POST 요청을 시뮬레이션합니다.

설정	설명
오브젝트 크기	요청 개체의 크기(바이트)를 입력합니다. K, M 또는 G를 입력하여 킬로바이트, 메가바이트 또는 기가바이트를 표시할 수 있습니다.
MIME 유형	MIME 유형을 입력합니다.
안티멀웨어 스캐닝 판정	Webroot, McAfee 또는 Sophos 스캐닝 판정을 재지정하려면 재지정할 특정 유형의 판정을 선택합니다.

3단계 **Find Policy Match(정책 일치 찾기)**를 클릭합니다.

정책 추적 결과가 Results(결과) 창에 표시됩니다.

고급: 응답 세부 정보 재지정

Policy Trace(정책 추적) 페이지, Advanced(고급) 섹션에 있는 Response Detail Overrides(응답 세부 정보 재지정) 창의 설정을 사용하여 이 추적에 대한 웹 액세스 정책 응답의 요소를 "수정"할 수 있습니다.

1단계 Policy Trace(정책 추적) 페이지의 **Advanced(고급)** 섹션을 확장합니다.

2단계 필요에 따라 Response Detail Overrides(응답 세부 정보 재지정) 창의 필드를 완성합니다.

설정	설명
URL Category(URL 범주)	이 설정을 사용하여 추적 응답의 URL 트랜잭션 카테고리를 재지정합니다. 응답 결과에서 URL 카테고리를 대체할 카테고리를 선택합니다.
애플리케이션	마찬가지로, 이 설정을 사용하여 추적 응답의 애플리케이션 카테고리를 재지정합니다. 응답 결과에서 애플리케이션 카테고리를 대체할 카테고리를 선택합니다.
오브젝트 크기	응답 개체의 크기(바이트)를 입력합니다. K, M 또는 G를 입력하여 킬로바이트, 메가바이트 또는 기가바이트를 표시할 수 있습니다.
MIME 유형	MIME 유형을 입력합니다.
웹 신뢰도 점수	-10.0에서 10.0까지의 웹 평판 점수를 입력합니다.
안티멀웨어 스캐닝 판정	이러한 옵션을 사용하여 추적 응답에 제공된 특정 안티멀웨어 스캐닝 판정을 재지정합니다. 응답 결과에서 Webroot, McAfee 및 Sophos 스캐닝 판정을 대체할 판정을 선택합니다.

3단계 **Find Policy Match(정책 일치 찾기)**를 클릭합니다.

정책 추적 결과가 Results(결과) 창에 표시됩니다.

파일 평판 및 파일 분석 문제

파일 평판 및 분석 트러블슈팅, 14-14페이지를 참조하십시오.

재부팅 문제

- 재부팅 시 KVM에서 실행 중인 가상 어플라이언스가 정지됨
- 하드웨어 어플라이언스: 원격으로 어플라이언스 전원 재설정

재부팅 시 KVM에서 실행 중인 가상 어플라이언스가 정지됨

참고 이는 KVM 문제이며 언제든지 변경될 수 있습니다.

자세한 내용은 https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html 및 https://bugs.launchpad.net/qemu/+bug/1329956을 참조하십시오.

1단계 다음을 확인합니다.

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

2단계 위의 값이 Y로 설정된 경우:

a. 가상 어플라이언스를 중지하고 KVM 커널 모듈을 다시 설치합니다.

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b. 가상 어플라이언스를 재시작합니다.

하드웨어 어플라이언스: 원격으로 어플라이언스 전원 재설정

하드웨어 어플라이언스를 하드 초기화해야 하는 경우 서드파티 IPMI(Intelligent Platform Management Interface) 툴을 사용하여 어플라이언스 섀시를 원격으로 재부팅할 수 있습니다.

제한 사항

- 원격 전원 관리는 특정 하드웨어에서만 이용할 수 있습니다. 세부 정보는 원격 전원 관리 사용, 21-4페이지를 참조하십시오.
- 이 기능을 사용하려면 먼저 활성화해야 합니다. 세부 정보는 원격 전원 관리 사용, 21-4페이지를 참조하십시오.
- IPMI 명령 status, on, off, cycle, reset, diag, soft만 지원됩니다. 지원되지 않는 명령을 실행하면 "insufficient privileges(권한 부족)" 오류가 표시됩니다.

시작하기 전에

- IPMI 버전 2.0을 사용하여 장비를 관리할 수 있는 유틸리티를 구해 설치합니다.
- 지원되는 IPMI 명령 사용 방법을 이해합니다. IPMI 툴에 대한 문서를 참조해 주십시오.

1단계 IPMI를 사용하여, 필요한 자격 증명과 함께 앞서 구성한 원격 전원 관리 포트에 할당된 IP 주소로 지원되는 전원 사이클링 명령을 실행합니다.

예를 들어 IPMI가 지원되는 UNIX 유형의 시스템에서는 다음 명령을 실행할 수 있습니다.

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

여기서 192.0.2.1은 원격 전원 관리 포트에 할당된 IP 주소이고 remoteresetuser 및 passphrase는 이 기능을 사용하도록 설정하는 동안 입력한 자격 증명입니다.

2단계 어플라이언스가 재부팅될 때까지 최소 5분 정도 기다립니다.

사이트 액세스 문제

- 인증을 지원하지 않는 URL에 액세스할 수 없음
- POST 요청을 사용하는 사이트에 액세스할 수 없음
- 관련 주제: 특정 웹 사이트에 대한 암호 해독 우회

인증을 지원하지 않는 URL에 액세스할 수 없음

다음은 인증을 지원하지 않으므로 웹 보안 어플라이언스가 투명 모드에서 구축된 경우 사용할 수 없는 일부 애플리케이션 목록입니다.

- Mozilla Thunderbird
- Adobe Acrobat 업데이트
- HttpBridge
- CollabNet의 Subversion
- Microsoft Windows 업데이트
- Microsoft Visual Studio

해결 방법: 인증이 필요하지 않은 URL에 대한 사용자 클래스를 생성합니다.

관련 주제

- 인증 우회, 5-30페이지

POST 요청을 사용하는 사이트에 액세스할 수 없음

사용자의 첫 번째 클라이언트 요청이 POST 요청이고 사용자가 여전히 인증되어야 하는 경우 POST 본문 콘텐츠가 손실됩니다. 이 문제는 POST 요청이 액세스 제어 단일 로그인을 사용 중인 애플리케이션에 해당하는 경우 발생할 수 있습니다.

해결 방법:

- POST를 첫 번째 요청으로 사용하는 URL에 연결하기 전에 브라우저를 통해 다른 URL을 요청하여 사용자가 먼저 웹 프록시에 인증하도록 합니다.
- POST를 첫 번째 요청으로 사용하는 URL의 경우에는 인증을 우회합니다.

참고 액세스 제어에 대해 작업할 때 애플리케이션 인증 정책에 구성된 ACS(Assertion Consumer Service) URL에 대한 인증을 우회할 수 있습니다.

관련 주제

- 인증 우회, 5-30페이지.

업스트림 프록시 문제

- 업스트림 프록시가 기본 자격 증명을 수신하지 않음
- 업스트림 프록시에서 클라이언트 요청 실패

업스트림 프록시가 기본 자격 증명을 수신하지 않음

어플라이언스와 업스트림 프록시가 모두 NTLMSSP를 통한 인증을 사용하는 경우, 컨피그레이션에 따라 어플라이언스와 업스트림 프록시가 인증 자격 증명을 요청하는 무한 루프에 빠질 수 있습니다. 예를 들어, 업스트림 프록시에 기본 인증이 필요하지만 어플라이언스에는 NTLMSSP 인증이 필요한 경우 어플라이언스가 업스트림 프록시에 기본 자격 증명을 성공적으로 전달할 수 없습니다. 이는 인증 프로토콜의 제한 사항 때문입니다.

업스트림 프록시에서 클라이언트 요청 실패

컨피그레이션:

- 웹 보안 어플라이언스 및 업스트림 프록시 서버는 기본 인증을 사용합니다.
- 자격 증명 암호화는 다운스트림 웹 보안 어플라이언스에서 사용하도록 설정됩니다.

웹 프록시가 클라이언트에서 "Authorization" HTTP 헤더를 수신하지만 업스트림 프록시 서버에 "Proxy-Authorization" HTTP 헤더가 필요하기 때문에 업스트림 프록시에서 클라이언트 요청이 실패합니다.

업스트림 프록시를 통해 FTP 요청을 라우팅할 수 없음

네트워크에 FTP 연결을 지원하지 않는 업스트림 프록시가 포함되어 있는 경우 모든 ID 및 FTP 요청에만 적용되는 라우팅 정책을 생성해야 합니다. 직접 FTP 서버에 연결하거나 프록시가 모두 FTP 연결을 지원하는 프록시 그룹에 연결하도록 해당 라우팅 정책을 구성합니다.

가상 어플라이언스

- AsyncOS 시작 중에 강제 재설정, 전원 끄기 또는 재설정 옵션을 사용하지 않음
- KVM 구축의 네트워크 연결이 처음에 작동한 후 실패함
- KVM 구축 시 성능 저하, Watchdog 문제 및 높은 CPU 사용률
- Linux 호스트에서 실행 중인 가상 어플라이언스에 대한 일반 트러블슈팅

AsyncOS 시작 중에 강제 재설정, 전원 끄기 또는 재설정 옵션을 사용하지 않음

가상 호스트의 다음 조치는 하드웨어 어플라이언스에서 플러그를 빼는 것과 동일하며 특히 AsyncOS 시작 중에 지원되지 않습니다.

- KVM에서는 강제 재설정 옵션.
- VMWare에서는 전원 끄기 및 재설정 옵션 (이러한 옵션은 어플라이언스가 완전히 부팅된 후 사용하는 것이 안전합니다.)

KVM 구축의 네트워크 연결이 처음에 작동한 후 실패함

문제 이전에 작동 중이던 네트워크 연결이 끊어집니다.

솔루션 이는 KVM 문제입니다. 다음 사이트의 OpenStack 문서에서 "KVM: Network connectivity works initially, then fails" 섹션을 참조하십시오.
http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html

KVM 구축 시 성능 저하, Watchdog 문제 및 높은 CPU 사용률

문제 Ubuntu 가상 머신에서 실행할 때 어플라이언스 성능이 저하되고 watchdog 문제가 발생하며 어플라이언스에 비정상적으로 높은 CPU 사용률이 표시됩니다.

솔루션 Ubuntu에서 최신 호스트 OS 업데이트를 설치합니다.

Linux 호스트에서 실행 중인 가상 어플라이언스에 대한 일반 트러블슈팅

문제 KVM 구축에서 실행 중인 가상 어플라이언스에 대한 문제는 호스트 OS 컨피그레이션 문제와 관련될 수 있습니다.

솔루션 다음 사이트에 있는 *Virtualization Deployment and Administration Guide*에서 트러블슈팅 섹션 및 기타 정보를 참조하십시오.
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf

WCCP 문제

- 최대 포트 항목 수

최대 포트 항목 수

WCCP를 사용하여 구축하는 경우 최대 포트 항목 수는 HTTP, HTTPS 및 FTP 포트를 합해서 30개입니다.

패킷 캡처

- 패킷 캡처 시작
- 패킷 캡처 파일 관리

어플라이언스는 어플라이언스가 어태치된 네트워크를 통해 전송되거나 수신된 TCP/IP 및 기타 패킷을 캡처하고 표시할 수 있는 기능을 제공합니다.

참고 패킷 캡처 기능은 UNIX tcpdump 명령과 유사합니다.

패킷 캡처 시작

1단계 **Support and Help(지원 및 도움말) > Packet Capture(패킷 캡처)**를 선택합니다.

2단계 (선택 사항) 패킷 캡처 설정을 변경하려면 **Edit Settings(설정 편집)**를 클릭합니다.

옵션	설명
캡처 파일 크기 제한	캡처 파일이 도달할 수 있는 최대 크기를 지정합니다. 캡처 기간 설정이 "파일 크기 제한점까지 캡처 실행"이 아닌 경우 제한에 도달하면 데이터가 무시되고 새 파일이 시작됩니다.
캡처 기간	캡처가 자동으로 중지되는 경우를 위한 옵션입니다. 다음 중에서 선택합니다. • **파일 크기 제한점까지 캡처 실행.** 위에서 설정된 파일 제한에 도달할 때까지 캡처가 실행됩니다. • **경과 시간 제한점까지 캡처 실행.** 지정된 기간 동안 캡처가 실행됩니다. 단위를 지정하지 않고 시간을 입력하면 AsyncOS가 기본적으로 초 단위를 사용합니다. • **캡처 무한 실행.** 수동으로 중지할 때까지 패킷 캡처가 실행됩니다. **참고** 언제든지 수동으로 캡처를 종료할 수 있습니다.
인터페이스	트래픽이 캡처될 인터페이스입니다.
필터	패킷을 캡처할 때 적용할 필터링 옵션입니다. 필터링을 사용하면 필요한 패킷만 캡처할 수 있습니다. 다음 중에서 선택합니다. • **필터 없음.** 모든 패킷이 캡처됩니다. • **미리 정의된 필터.** 미리 정의된 필터는 포트 및/또는 IP 주소별 필터링을 제공합니다. 비워 두면 모든 트래픽이 캡처됩니다. • **맞춤형 필터.** 필요한 패킷 캡처 옵션의 정확한 구문을 이미 알고 있는 경우 이 옵션을 사용합니다. 표준 tcpdump 구문을 사용합니다.

(선택 사항) 패킷 캡처 변경 사항을 제출하고 커밋합니다.

참고 변경 사항을 커밋하지 않고 패킷 캡처 설정을 변경한 후 패킷 캡처를 시작하면 AsyncOS에서 새로운 설정을 사용합니다. 이렇게 하면 향후 패킷 캡처 실행을 위해 설정을 적용하지 않고 현재 세션에서 새로운 설정을 사용할 수 있습니다. 설정은 지울 때까지 계속 유지됩니다.

3단계 **Start Capture(캡처 시작)**를 클릭합니다. 실행 중인 캡처를 수동으로 중지하려면 **Stop Capture(캡처 중지)**를 클릭합니다.

패킷 캡처 파일 관리

어플라이언스는 캡처된 패킷 활동을 파일에 저장하고 이 파일을 로컬에 저장합니다. 디버깅 및 트러블슈팅을 위해 FTP를 사용하여 패킷 캡처 파일을 Cisco 고객 지원에 전송할 수 있습니다.

- 패킷 캡처 파일 다운로드 또는 삭제

패킷 캡처 파일 다운로드 또는 삭제

참고 FTP를 사용하고 캡처 디렉토리에서 패킷 캡처 파일을 검색하여 어플라이언스에 연결할 수도 있습니다.

1단계 **Support and Help(지원 및 도움말) > Packet Capture(패킷 캡처)**를 선택합니다.

2단계 Manage Packet Capture Files(패킷 캡처 파일 관리) 창에서 사용할 패킷 캡처 파일을 선택합니다. 패킷 캡처 파일이 어플라이언스에 저장되지 않은 경우 이 창이 표시되지 않습니다.

3단계 필요에 따라 **Download File(파일 다운로드)** 또는 **Delete Selected Files(선택한 파일 삭제)**를 클릭합니다.

지원에 대한 작업

- 효율적인 서비스를 위해 정보 수집, A-24페이지
- 기술 지원 요청 열기, A-25페이지
- 가상 어플라이언스에 대한 지원 받기, A-25페이지
- 어플라이언스에 대한 원격 액세스 사용, A-26페이지

효율적인 서비스를 위해 정보 수집

지원 센터에 문의하기 전에 다음을 수행합니다.

- 일반 트러블슈팅 모범 사례, A-2페이지에 설명된 대로 맞춤형 기록 필드를 사용하도록 설정합니다.
- 패킷 캡처 수행을 고려합니다. 패킷 캡처, A-23페이지를 참조하십시오.

기술 지원 요청 열기

어플라이언스를 사용하여 지원을 위해 긴급하지 않은 요청을 Cisco 고객 지원에 전송할 수 있습니다. 어플라이언스가 요청을 전송할 때 어플라이언스의 컨피그레이션도 전송합니다. 지원 요청을 전송하려면 어플라이언스가 인터넷에 메일을 전송할 수 있어야 합니다.

참고 긴급한 문제가 있는 경우 Cisco Worldwide Support Center에 문의하십시오.

시작하기 전에

- Cisco.com 사용자 ID가 이 어플라이언스의 서비스 계약과 연관되어 있는지 확인합니다. 현재 Cisco.com 프로필과 연결된 서비스 계약의 목록을 보려면 Cisco.com 프로필 관리자(https://sso.cisco.com/autho/forms/CDClogin.html)를 방문하십시오. Cisco.com 사용자 ID가 없는 경우, 등록하고 받으십시오.

1단계 **Support And Help(지원 및 도움말) > Contact Technical Support(기술 지원에 문의)**를 선택합니다.

2단계 (선택 사항) 추가 요청 수신자를 선택합니다. 기본적으로 지원 요청 및 컨피그레이션 파일이 Cisco 고객 지원에 전송됩니다.

3단계 연락처 정보를 입력합니다.

4단계 문제 세부 정보를 입력합니다.

- 이 문제에 대한 고객 지원 티켓이 이미 있는 경우 해당 티켓을 입력합니다.

5단계 **Send(보내기)**를 클릭합니다. Cisco와 함께 장애 처리를 생성합니다.

가상 어플라이언스에 대한 지원 받기

Cisco 콘텐츠 보안 가상 어플라이언스에 대한 지원 사례를 보관하려면 VLN(Virtual License Number), 계약 번호 및 PID(Product Identifier) 코드를 제공해야 합니다.

구매 주문을 참조하거나 다음 표를 통해 가상 어플라이언스에서 실행되는 소프트웨어 라이센스를 기반으로 PID를 식별할 수 있습니다.

기능	PID	설명
Web Security Essentials	WSA-WSE-LIC=	구성: • 웹 사용 제어 • 웹 평판
Web Security Premium	WSA-WSP-LIC=	구성: • 웹 사용 제어 • 웹 평판 • Sophos 및 Webroot 안티멀웨어 시그니처
웹 보안 안티멀웨어	WSA-WSM-LIC=	Sophos 및 Webroot 안티멀웨어 시그니처 포함

기능	PID	설명
McAfee Anti-Malware	WSA-AMM-LIC=	—
AMP(Advanced Malware Protection)	WSA-AMP-LIC=	—

어플라이언스에 대한 원격 액세스 사용

원격 액세스 옵션을 사용하면 Cisco 고객 지원에서 지원 목적으로 여러분의 어플라이언스에 원격으로 액세스할 수 있습니다.

1단계 **Support And Help(지원 및 도움말) > Remote Access(원격 액세스)**를 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 Customer Support Remote Access(고객 지원 원격 액세스) 옵션을 완료합니다.

옵션	설명
시드 문자열	문자열을 입력하는 경우 문자열이 기존 또는 향후 암호와 일치하지 않아야 합니다. Submit(제출)을 클릭하면 이 문자열이 페이지의 상단 근처에 표시됩니다. 지원 담당자에게 이 문자열을 제공합니다.
보안 터널(권장)	원격 액세스 연결을 위해 보안 터널을 사용할지 여부를 지정합니다. 사용하도록 설정된 경우 어플라이언스가 지정된 포트를 통해 upgrades.ironport.com 서버에 대한 SSH 터널을 생성합니다(기본적으로 포트 443을 통해). 연결되면 Cisco 고객 지원에서 SSH 터널을 사용하여 어플라이언스에 액세스할 수 있습니다. 기술 지원 터널이 사용되도록 설정되면 7일 동안 upgrades.ironport.com에 계속 연결됩니다. 7일 후에는 기존 연결이 계속 존재하고 작동하는 경우에도 기술 지원 터널을 사용하여 새 연결을 작성할 수 없습니다. 특별히 비활성화하지 않으면 원격 액세스 계정이 활성 상태로 유지됩니다.

4단계 변경 사항을 제출 및 커밋합니다.

5단계 페이지 상단 근처의 성공 메시지에서 시드 문자열을 찾아 기록합니다.

보안상의 이유로 이 문자열은 어플라이언스에 저장되지 않으며 나중에 이 문자열을 찾을 수 있는 방법은 없습니다.

이 시드 문자열을 안전한 위치에 보관합니다.

6단계 시드 문자열을 지원 담당자에게 제공합니다.

CLI(Command Line Interface)

- CLI(Command Line Interface) 개요, 27-1페이지
- CLI(Command Line Interface) 액세스, 27-1페이지
- 범용 CLI 명령, 27-4페이지
- Web Security Appliance CLI 명령, 27-6페이지

CLI(Command Line Interface) 개요

AsyncOS CLI(Command Line Interface)를 사용하면 Web Security Appliance를 구성하고 모니터링할 수 있습니다. CLI(Command Line Interface)는 이러한 서비스가 사용하도록 설정된 상태로 구성된 IP 인터페이스의 SSH 또는 시리얼 포트의 터미널 에뮬레이션 소프트웨어를 사용하여 액세스할 수 있습니다. 기본적으로 SSH는 관리 포트에 구성됩니다.

인수를 포함하거나 포함하지 않고 명령 이름을 입력하여 명령을 호출합니다. 인수 없이 명령을 입력하면 명령에서 필요한 정보를 입력하라는 프롬프트를 표시합니다.

CLI(Command Line Interface) 액세스

다음 방법 중 하나를 사용하여 연결할 수 있습니다.

- **이더넷.** Web Security Appliance의 IP 주소를 사용하여 SSH 세션을 시작합니다. 공장 기본값 IP 주소는 192.168.42.42입니다. SSH는 포트 22를 사용하도록 구성되어 있습니다.
- **시리얼 연결.** 시리얼 케이블이 연결된 PC의 통신 포트로 터미널 세션을 시작합니다.

첫 번째 액세스

admin 계정을 사용하여 처음으로 CLI에 액세스한 후 다른 레벨의 권한이 있는 다른 사용자를 추가할 수 있습니다. 기본 **admin** 사용자 이름 및 암호를 입력하여 어플라이언스에 로그인합니다.

- 사용자 이름: **admin**
- 암호: **ironport**

처음으로 기본 암호를 사용하여 로그인하면 시스템 설정 마법사에서 **admin** 계정의 암호를 변경하라는 프롬프트를 표시합니다.

언제라도 `passwd` 명령을 사용하여 **admin** 계정 암호를 재설정할 수도 있습니다.

후속 액세스

유효한 사용자 이름 및 암호를 사용하여 언제라도 어플라이언스에 연결하고 로그인할 수 있습니다. 로그인되면 현재 사용자 이름에 대한 최근 어플라이언스 액세스 시도 목록(성공 및 실패 모두)이 자동으로 표시됩니다.

추가 사용자 구성에 대한 자세한 내용은 다음 `userconfig` 명령 설명 또는 사용자 계정 관리, 22-6페이지를 참조하십시오.

명령 프롬프트에 대한 작업

최상위 명령 프롬프트는 정규화된 호스트 이름, > 기호, 공백 순으로 구성됩니다. 예를 들면 다음과 같습니다.

```
example.com>
```

명령을 실행하면 CLI는 사용자 입력을 요청합니다. CLI에서 입력을 요청할 때 프롬프트에는 대괄호([])로 묶인 기본값과 보다 큼(>) 기호가 표시됩니다. 기본값이 없는 경우 대괄호 안이 비어 있습니다.

예를 들면 다음과 같습니다.

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

기본 설정이 있는 경우 해당 설정이 명령 프롬프트 대괄호 안에 표시됩니다. 예를 들면 다음과 같습니다.

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

기본 설정이 표시될 때 Return을 입력하는 것은 기본값을 승인하는 것과 동일합니다.

명령 구문

인터랙티브 모드에서 작동하는 경우 CLI 명령 구문은 공백이 없고 인수 또는 매개변수가 없는 단일 명령으로 구성됩니다. 예를 들면 다음과 같습니다.

```
example.com> logconfig
```

선택 목록

입력에 대해 여러 선택 항목이 제공될 경우 숫자가 지정된 목록을 사용하는 명령도 있습니다. 프롬프트에 선택할 번호를 입력합니다.

예를 들면 다음과 같습니다.

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

예/아니요 쿼리

예 또는 아니요 옵션이 있을 경우 질문은 괄호로 묶인 기본값과 함께 제시됩니다. **Y**, **N** 또는 **Yes**, **No**로 답할 수 있습니다. 대소문자는 구분하지 않습니다.

예를 들면 다음과 같습니다.

```
Do you want to enable the proxy? [Y]> Y
```

하위 명령

일부 명령에서는 NEW, EDIT 및 DELETE와 같은 하위 명령 지시문을 사용할 수 있습니다. EDIT 및 DELETE 함수는 이전에 구성된 값 목록을 제공합니다.

예를 들면 다음과 같습니다.

```
example.com> interfaceconfig

Currently configured interfaces:

1. Management (172.xxx.xx.xx/xx: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- DELETE - Remove an interface.

[]>
```

하위 명령에서 빈 프롬프트에 Enter 또는 Return을 입력하면 기본 명령으로 돌아갑니다.

하위 명령 이스케이프

하위 명령에서 언제든지 Ctrl+C 키보드 바로가기를 사용하여 해당 명령을 종료한 후 즉시 CLI의 최상위 레벨로 돌아갈 수 있습니다.

명령 기록

CLI는 세션 중에 입력한 모든 명령의 기록을 보관합니다. 키보드의 위쪽 및 아래쪽 화살표 키를 사용하거나 Ctrl+P 및 Ctrl+N 키 조합을 사용하여 최근 사용된 명령의 실행 중인 목록을 스크롤할 수 있습니다.

명령 완성

AsyncOS CLI는 명령 완성 기능을 지원합니다. 일부 명령의 처음 몇 개 문자를 입력하고 Tab 키를 누르면 CLI에서 해당 문자열을 완성합니다. 입력하는 글자가 명령과 일치하지 않는 경우, CLI는 범위를 "줄입니다". 예를 들면 다음과 같습니다.

```
example.com> set(Tab 키를 누름)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth(Tab을 다시 누르면 sethostname이 포함된 항목이 완성됨)
```

CLI를 사용하여 컨피그레이션 변경 사항 커밋

- 대부분의 컨피그레이션 변경 사항은 커밋할 때까지 적용되지 않습니다.
- `commit` 명령을 사용하면 다른 작업이 정상적으로 진행되는 동안 컨피그레이션 설정을 변경할 수 있습니다.
- 변경사항을 성공적으로 커밋하려면 최상위 명령 프롬프트에서 수행해야 합니다. 빈 프롬프트에서 **Return**을 입력하면 명령행 계층 구조에서 한 레벨 위로 이동합니다.
- 커밋되지 않은 컨피그레이션 변경 사항은 기록되지만 `commit` 명령을 실행할 때까지 적용되지 않습니다. 그러나 모든 명령에 `commit` 명령을 실행할 필요는 없습니다. CLI 세션을 종료하거나 시스템을 종료하거나, 재부팅을 하거나 오류가 발생하거나 `clear` 명령을 실행하면 아직 커밋되지 않은 변경사항은 지워집니다.
- 확인 및 타임스탬프를 수신할 때까지 변경 사항이 실제로 커밋되지 않습니다.

범용 CLI 명령

이 섹션에서는 변경 사항 커밋 및 지우기와 같이 일반 CLI 세션에서 사용할 수 있는 일부 기본 명령에 대해 설명합니다.

CLI 예: 컨피그레이션 변경 사항 커밋

commit 명령 다음에 주석을 입력하는 것은 선택 사항입니다.

```
example.com> commit


Please enter some comments describing your changes:

[]> Changed "psinet" IP Interface to a different IP address

Changes committed: Wed Jan 01 12:00:01 2007
```

CLI 예: 컨피그레이션 변경 사항 지우기

clear 명령은 마지막 commit 또는 clear 명령이 실행된 후 어플라이언스 컨피그레이션에 작성된 모든 변경 사항을 지웁니다.

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y

Changes cleared: Wed Jan 01 12:00:01 2007

example.com>
```

CLI 예: CLI(Command Line Interface) 세션 종료

exit 명령을 실행하면 CLI 애플리케이션에서 로그아웃됩니다. 커밋되지 않은 구성 변경사항은 지워집니다.

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.

Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

CLI 예: CLI(Command Line Interface)에서 도움말 찾기

help 명령은 사용 가능한 모든 CLI 명령을 나열하고 각 명령에 대한 간략한 설명을 제공합니다. help 명령은 명령 프롬프트에 help 또는 단일 물음표(?)를 입력하여 호출할 수 있습니다.

```
example.com> help
```

또한 **help** *commandname*을 입력하여 특정 명령에 대한 도움말에 액세스할 수 있습니다.

관련 주제

- Web Security Appliance CLI 명령, 27-6페이지

Web Security Appliance CLI 명령

Web Security Appliance CLI는 시스템 액세스, 업그레이드 및 관리를 수행하기 위한 프록시 및 UNIX 명령 집합을 지원합니다.

참고 모든 CLI 명령이 모든 작동 모드(표준 및 Cloud Web Security Connector)에서 적용 가능/사용 가능하지는 않습니다.

명령	설명
advancedproxyconfig	고급 웹 프록시 컨피그레이션을 구성합니다. 하위 명령은 다음과 같습니다. **AUTHENTICATION** – 인증 컨피그레이션 옵션: • 인증 요청 헤더를 상위 프록시로 언제 전달하시겠습니까? • 최종 사용자 인증 대화상자에 표시할 프록시 인증 영역 입력 • 요청 URI에 나타나는 사용자 이름을 기록하시겠습니까? • 웹 UI의 디렉토리 조회에 그룹 구성원 자격 특성을 사용해야 합니까(사용되지 않을 경우, 빈 그룹 및 다른 구성원 자격 특성을 가지는 그룹이 표시됩니다)? • 고급 Active Directory 연결성 검사를 사용하시겠습니까? • 정책에서 대소문자를 구분하지 않는 사용자 이름 일치를 허용하시겠습니까? • LDAP 그룹 이름에 대해 * 문자를 사용한 와일드카드 일치를 허용하시겠습니까? • 클라이언트에서 기본 인증에 사용하는 문자 집합을 입력합니다 [ISO-8859-1/UTF-8]. • LDAP에 대한 조회를 사용하도록 설정하시겠습니까? • 보안 인증을 사용하도록 설정하시겠습니까? • 인증을 위해 클라이언트를 리디렉션하는 호스트 이름 입력 • 사용자 자격 증명에 대한 서로게이트 시간 초과 입력 • 머신 자격 증명에 대한 서로게이트 시간 초과 입력 • 인증 서비스를 사용할 수 없으므로 트래픽이 허용된 경우 서로게이트 시간 초과 입력 • 요청 거부 시 재인증 옵션 [disabled / embedlinkinblockpage] 입력 • NTLMSSP 인증을 위해 NTLM 헤더와 함께 Negotiate 헤더를 보내시겠습니까? • 로그 및 보고서의 사용자 이름과 IP 주소 마스킹 구성

advancedproxyconfig (계속)	**CACHING** – 프록시 캐싱 모드: 다음 중에서 하나를 선택합니다. • 안전 모드 • 최적화된 모드 • 적극적인 모드 • 맞춤화된 모드 웹 프록시 캐시 모드 선택, 4-7페이지도 참조하십시오. **DNS** – DNS 컨피그레이션 옵션: • DNS 조회 실패 시 HTTP 307 리디렉션의 URL 형식 입력 • DNS 조회 실패 시 프록시에서 HTTP 307 리디렉션을 실행하시겠습니까? • 업스트림 프록시(피어)에서 응답이 없을 경우 DNS 결과에 대해 프록시에서 자동으로 페일오버를 수행하지 않도록 설정하시겠습니까? • 다음을 사용하여 웹 서버를 찾습니다. 0 = 항상 DNS 응답을 순차적으로 사용 1 = 클라이언트 제공 주소 다음에 DNS 사용 2 = 제한적인 DNS 사용 3 = 매우 제한적인 DNS 사용 옵션 1 및 2에서는 웹 평판이 사용하도록 설정된 경우 DNS가 사용됩니다. 옵션 2 및 3에서는 업스트림 프록시가 없거나 구성된 업스트림 프록시가 실패한 경우 명시적 프록시 요청에 대해 DNS가 사용됩니다. 모든 옵션에서 대상 IP 주소가 정책 구성원 자격에 사용되는 경우 DNS가 사용됩니다. **EUN** – 최종 사용자 알림 매개변수: • 선택: 1. EUN 페이지 새로 고침 2. 맞춤형 EUN 페이지 사용 3. 표준 EUN 페이지 사용 • '사용자 승인' 페이지 표시를 설정하시겠습니까? 웹 프록시 사용 계약, 4-11페이지 및 최종 사용자 알림 개요, 17-1페이지도 참조하십시오. **NATIVEFTP** – 네이티브 FTP 컨피그레이션: • FTP 프록시를 사용하도록 설정하시겠습니까? • FTP 프록시가 수신하는 포트 입력 • 수동 FTP 연결에 대해 프록시가 수신할 포트 번호의 범위 입력 • 활성 FTP 연결에 대해 수신할 프록시에 대한 포트 번호의 범위 입력 • 인증 형식 입력: 1. Check Point 2. 프록시 인증 없음 3. 랩터 • 캐싱을 사용하도록 설정하시겠습니까? • 서버 IP 스푸핑을 사용하도록 설정하시겠습니까? • FTP 서버 시작 메시지를 클라이언트에 전달하시겠습니까? • ftp 서버 디렉토리에 대한 최대 경로 크기 입력 FTP 프록시 서비스 개요, 4-15페이지도 참조하십시오.

advancedproxyconfig (계속)	**FTPOVERHTTP** – FTP Over HTTP 옵션: • 익명 FTP 액세스에서 사용할 로그인 이름 입력 • 익명 FTP 액세스에서 사용할 비밀번호 입력 FTP 프록시 서비스 개요, 4-15페이지도 참조하십시오. **HTTPS** – HTTPS 관련 옵션: • HTTPS URI 로깅 스타일 • 인증 목적으로 인증되지 않은 투명 HTTPS 요청의 암호를 해독하시겠습니까? • 최종 사용자 알림 목적으로 HTTPS 요청의 암호를 해독하시겠습니까? • 핸드셰이크 중 HTTPS 서버에서 클라이언트 인증서를 요청할 때 수행할 조치: 1. 트랜잭션 통과 2. 사용 불가능한 인증서로 응답 • SNI(Server Name Indication) 확장 기능을 사용하도록 설정하시겠습니까? • 세션 재개를 사용하도록 설정하시겠습니까? HTTPS 트래픽을 제어하기 위한 암호 해독 정책 생성 개요, 11-1페이지도 참조하십시오. **SCANNING** – 스캐닝 옵션: • 콘텐츠 유형에 관계없이 프록시에서 모든 콘텐츠에 대해 악성코드 스캐닝을 수행하시겠습니까? • 안티멀웨어 스캐닝 엔진(Sophos, McAfee 또는 Webroot)의 응답을 기다리는 시간(초) 입력 • Webroot 본문 스캐닝을 사용하지 않도록 설정하시겠습니까? 안티멀웨어 스캐닝 개요, 13-4페이지 및 아웃바운드 트래픽 스캐닝 개요, 12-1페이지도 참조하십시오. **PROXYCONN** – 프록시 연결 헤더를 수락할 수 없는 사용자 에이전트 목록을 관리합니다. 이 목록 항목은 Flex(Fast Lexical Analyzer) 언어에서 정규식으로 해석됩니다. 하위 문자열이 목록에 있는 정규식과 일치하는 경우 사용자 에이전트가 일치됩니다. • Choose the operation you want to perform: NEW - 사용자 에이전트 목록에 항목 추가 DELETE - 목록에서 항목 제거 **CUSTOMHEADERS** – 특정 도메인에 대한 맞춤형 요청 헤더를 관리합니다. • Choose the operation you want to perform: DELETE - 항목 삭제 NEW - 새 항목 추가 EDIT - 항목 편집 웹 요청에 맞춤형 헤더 추가, 4-9페이지도 참조하십시오.

advancedproxyconfig (계속)	**MISCELLANEOUS** – 기타 프록시 관련 매개변수: • 프록시에서 L4 스위치의 상태 검사에 응답하도록 하시겠습니까(WSA가 L4 투명 모드에 있을 경우 항상 사용하도록 설정됨)? • 프록시에서 TCP 수신 창 크기를 동적으로 조정하도록 하시겠습니까? • 프록시에서 TCP 전송 창 크기를 동적으로 조정하도록 하시겠습니까? • HTTPS 응답 캐시 사용 • 무응답 업스트림 프록시를 확인하기 위한 최소 유휴 제한 시간 입력(초) • 무응답 업스트림 프록시를 확인하기 위한 최대 유휴 제한 시간 입력(초) • 프록시 모드: 1. 명시적 전달 모드만 2. L4 스위치가 있거나 리디렉션을 위한 디바이스가 없는 투명 모드 3. 리디렉션을 위한 WCCP v2 라우터가 있는 투명 모드 • 프록시에 의한 클라이언트 IP 스푸핑 1. 비활성화 2. 모든 요청에 사용 3. 투명 요청에만 사용 • HTTP X-Forwarded-For 헤더를 전달하시겠습니까? • HTTP 포트에서 HTTP가 아닌 요청의 터널링을 허용하시겠습니까? • SSL 포트에서 SSL이 아닌 트랜잭션의 터널링을 차단하시겠습니까? • 프록시에서 수신 연결 IP 주소 대신 X-Forwarded-For 헤더의 값을 로그에 기록하도록 허용하시겠습니까? • 프록시가 캐시에서 제공되는 컨텐트를 제한하도록 허용하시겠습니까? • 프록시에서 X-Forwarded-For 헤더의 클라이언트 IP 주소를 사용하도록 설정하시겠습니까? 웹 프록시 데이터용 P2 데이터 인터페이스 사용, 2-19페이지 및 웹 프록시 설정 구성, 4-3페이지도 참조하십시오. **SOCKS** – SOCKS 프록시 옵션: • SOCKS 프록시를 사용하도록 설정하시겠습니까? • 프록시 협상 시간 초과 • UDP 터널 시간 초과 • SOCKS 제어 포트 • UDP 요청 포트 웹 프록시 데이터용 P2 데이터 인터페이스 사용, 2-19페이지 및 SOCKS 프록시 서비스, 4-17페이지도 참조하십시오.
adminaccessconfig	어플라이언스에 로그인하는 관리자에 대해 더 엄격한 액세스 요건을 가지도록 Web Security Appliance를 구성할 수 있습니다.
alertconfig	경고 수신자를 지정하고 시스템 경고를 보내기 위한 매개변수를 설정합니다.
authcache	인증 캐시에서 하나 또는 모든 항목(사용자)을 삭제할 수 있습니다. 또한 현재 인증 캐시에 포함된 모든 사용자를 나열할 수 있습니다.
bwcontrol	기본 프록시 로그 파일에서 대역폭 제어 디버그 메시지를 사용하도록 설정합니다.
certconfig	보안 인증서 및 키를 구성합니다.
clear	마지막 커밋 이후 보류 중인 컨피그레이션 변경 사항을 지웁니다.
commit	보류 중인 변경 사항을 시스템 컨피그레이션에 커밋합니다.
createcomputerobject	사용자가 지정하는 위치에 컴퓨터 개체를 생성합니다.

datasecurityconfig	최소 요청 본문 크기를 정의합니다. 이 크기 미만의 업로드 요청은 Cisco IronPort 데이터 보안 필터에서 스캐닝하지 않습니다.
date	현재 날짜를 표시합니다. 예: `Thu Jan 10 23:13:40 2013 GMT`
dnsconfig	DNS 서버 매개변수를 구성합니다.
dnsflush	어플라이언스에서 DNS 항목을 플러시합니다.
etherconfig	이더넷 포트 연결을 구성합니다.
externaldlpconfig	최소 요청 본문 크기를 정의합니다. 이 크기 미만의 업로드 요청은 외부 DLP 서버에서 스캐닝하지 않습니다.
featurekey	라이센스가 있는 기능을 활성화하기 위해 유효한 키를 제출합니다.
featurekeyconfig	자동으로 기능 키를 확인하고 업데이트합니다.
grep	명명된 입력 파일에서 지정된 패턴과 일치하는 항목을 포함하는 행을 검색합니다.
help	명령 목록을 반환합니다.
iccm_message	보안 관리 어플라이언스(M-Series)에서 이 Web Security Appliance를 관리하는 경우 표시되는 웹 인터페이스 및 CLI의 메시지를 지웁니다.
ifconfig 또는 interfaceconfig	M1, P1 및 P2를 포함하여 네트워크 인터페이스를 구성하고 관리합니다. 현재 구성된 인터페이스를 표시하고 인터페이스를 생성, 편집 또는 삭제할 수 있는 작업 메뉴를 제공합니다.
iseconfig	현재 ISE 컨피그레이션 매개변수를 표시하고 수행할 ISE 컨피그레이션 작업을 지정합니다. • `setup` – 사용/사용 안 함, ISE 서버 이름 또는 IPv4 주소, 프록시 캐시 시간 초과, 통계 백업 간격 등의 ISE 설정을 구성합니다.
isedata	ISE 데이터 관련 작업을 지정합니다. `statistics` – ISE 서버 상태 및 ISE 통계를 표시합니다. `cache` – ISE 캐시를 표시하거나 IP 주소를 표시합니다. `show` – ISE ID 캐시를 표시합니다. `checkip` – 로컬 ISE 캐시에서 IP 주소를 쿼리합니다. `sgts` – ISE SGT(Secure Group Tag) 테이블을 표시합니다.
last	tty 및 호스트를 포함하는 사용자별 사용자 정보를 역시간순으로 나열하거나 지정된 날짜 및 시간에 로그인되어 있는 사용자를 나열합니다.
loadconfig	시스템 컨피그레이션 파일을 로드합니다.
logconfig	로그 파일에 대한 액세스를 구성합니다.
mailconfig	현재 컨피그레이션 파일을 지정된 주소로 발송합니다.
musconfig	모빌리티 보안를 사용하도록 설정하고 IP 주소를 사용하거나 하나 이상의 Cisco Adaptive Security Appliance와 통합하여 원격 사용자를 식별하는 방법을 구성하려면 이 명령을 사용합니다. **참고** 이 명령을 사용하여 변경 사항을 작성하면 웹 프록시가 재시작됩니다.

musstatus	Web Security Appliance가 Adaptive Security Appliance와 통합된 경우 모빌리티 보안 관련 정보를 표시하려면 이 명령을 사용합니다. 이 명령은 다음 정보를 표시합니다. • 각 Adaptive Security Appliance와의 Web Security Appliance 연결 상태 • 각 Adaptive Security Appliance와의 Web Security Appliance 연결 지속시간(분) • 각 Adaptive Security Appliance의 원격 클라이언트 수 • 서비스되는 원격 클라이언트 수, Web Security Appliance를 통해 트래픽을 전달한 원격 클라이언트 수로 정의됩니다. • 전체 원격 클라이언트 수
nslookup	인터넷 도메인 이름 서버에서 지정된 호스트 및 도메인에 대한 정보를 쿼리하거나 도메인에 있는 호스트 목록을 인쇄합니다.
ntpconfig	NTP 서버를 구성합니다. 현재 구성된 인터페이스를 표시하고 IP 주소에서 NTP 쿼리가 시작되어야 하는 인터페이스를 추가, 제거 또는 설정할 수 있는 작업 메뉴를 제공합니다.
packetcapture	어플라이언스가 어태치된 네트워크를 통해 전송되거나 수신된 TCP/IP 및 기타 패킷을 가로채고 표시합니다.
passwd	암호를 설정합니다.
pathmtudiscovery	경로 MTU 검색을 사용하거나 사용하지 않도록 설정합니다. 패킷 프래그멘테이션이 필요한 경우 경로 MTU 검색을 사용하지 않도록 설정할 수 있습니다.
ping	지정된 호스트 또는 게이트웨이에 ICMP ECHO REQUEST를 전송합니다.
maxhttpheadersize	프록시 요청에 대한 최대 HTTP 헤더 크기를 설정합니다. 값(바이트 수)을 입력하거나 킬로바이트를 표시하려면 숫자에 K를 추가합니다. 다수의 인증 그룹에 속해 있는 사용자의 경우 정책 추적이 실패할 수 있습니다. 또한 HTTP 응답 헤더 크기가 현재 "최대 헤더 크기"보다 큰 경우에도 실패할 수 있습니다. 이 값을 늘리면 이러한 실패를 줄일 수 있습니다. 최소값은 32KB이고 기본값은 32KB이며 최대값은 1024KB입니다.
proxyconfig <enable | disable>	웹 프록시를 사용하거나 사용하지 않도록 설정합니다.
proxystat	웹 프록시 통계를 표시합니다.
quit, q, exit	활성 프로세스 또는 세션을 종료합니다.
reboot	파일 시스템 캐시를 디스크에 플러시하고 실행 중인 모든 프로세스를 정지한 후 시스템을 재시작합니다.
reportingconfig	보고 시스템을 구성합니다.
resetconfig	컨피그레이션을 공장 기본값으로 복원합니다.
rollovernow	로그 파일을 롤오버합니다.
routeconfig	트래픽에 대한 목적지 IP 주소 및 게이트웨이를 구성합니다. 현재 구성된 경로를 표시하고 항목을 생성, 편집 또는 삭제하거나 지울 수 있는 작업 메뉴를 제공합니다.
saveconfig	현재 컨피그레이션 설정의 사본을 파일에 저장합니다. 필요한 경우 이 파일을 사용하여 기본값을 복원할 수 있습니다.

setgateway	머신에 대한 기본 게이트웨이를 구성합니다.
sethostname	호스트 이름 매개변수를 설정합니다.
setntlmsecuritymode	NTLM 인증 영역에 대한 보안 설정을 "ads" 또는 "domain"으로 변경합니다. • domain - AsyncOS가 도메인 보안 신뢰 계정을 사용하여 Active Directory 도메인에 조인합니다. 이 모드에서는 AsyncOS에서 Active Directory가 중첩된 Active Directory 그룹만 사용해야 합니다. • ads - AsyncOS가 네이티브 Active Directory 구성원으로 도메인에 조인합니다. 기본값은 ads입니다.
settime	시스템 시간을 설정합니다.
settz	현재 시간대 및 시간대 버전을 표시합니다. 로컬 시간대를 설정하기 위한 작업 메뉴를 제공합니다.
showconfig	모든 컨피그레이션 값을 표시합니다. **참고** 사용자 암호는 암호화됩니다.
shutdown	연결을 종료하고 시스템을 종료합니다.
smtprelay	내부적으로 생성된 이메일에 대한 SMTP 릴레이 호스트를 구성합니다. SMTP 릴레이 호스트는 시스템에서 생성된 이메일 및 경고를 수신하는 데 필요합니다.
snmpconfig	SNMP 쿼리를 수신하고 SNMP 요청을 허용하도록 로컬 호스트를 구성합니다.
sshconfig	신뢰할 수 있는 서버에 대한 호스트 이름 및 호스트 키 옵션을 구성합니다.

sslconfig	어플라이언스 관리 웹 사용자 인터페이스, 프록시 서비스(HTTPS 프록시 및 보안 클라이언트를 위한 자격 증명 암호화 포함), 보안 LDAP 서비스(인증, 외부 인증, SaaS SSO 및 보안 모빌리티 포함) 및 업데이트 서비스에 통신 프로토콜 TLS v1.x 및 SSL v3을 사용하기 위한 명령입니다. VERSIONS - 특정 서비스에 대해 사용하도록 설정된 프로토콜을 확인하고 변경합니다. COMPRESS – TLS 압축을 사용하도록 설정/사용하지 않도록 설정합니다. 최적의 보안을 위해서는 사용하지 않도록 설정하는 것이 좋습니다. CIPHERS – 선택한 프로토콜에 사용 가능한 암호 그룹을 추가/업데이트합니다. 기본 암호는 DEFAULT:+kEDH이지만 ECDHE 암호 선택 사항에 따라 변경할 수 있습니다. FALLBACK – SSL/TLS 폴백 옵션을 사용하도록 설정/사용하지 않도록 설정합니다. 사용하도록 설정된 경우 핸드셰이크 실패 후 원격 서버와의 통신이 구성된 가장 낮은 프로토콜로 폴백합니다. 클라이언트와 서버 간에 프로토콜 버전이 협상된 후 구현 문제로 인해 핸드셰이크 실패가 발생할 수 있습니다. 이 옵션이 사용하도록 설정된 경우 프록시는 현재 구성된 TLS/SSL 프로토콜 중 가장 낮은 버전을 사용하여 연결하려고 시도합니다. **참고** 새 AsyncOS 9.x 설치에서는 기본적으로 폴백이 사용하지 않도록 설정되어 있습니다. 폴백 옵션이 있는 이전 버전에서 업그레이드하는 경우 현재 설정이 유지됩니다. 그렇지 않으면, 옵션이 존재하지 않는 버전에서 업그레이드하는 경우에는 기본적으로 폴백이 사용하도록 설정됩니다. ECDHE– LDAP에 대한 ECDHE 암호의 사용을 사용하도록 설정/사용하지 않도록 설정합니다. 추가 ECDH 암호가 연속적인 릴리스에서 지원되지만 명명된 특정 곡선이 일부 추가 암호와 함께 제공되면 보안 LDAP 인증 및 HTTPS 트래픽 암호 해독 중에 어플라이언스에서 연결을 닫습니다. 추가 암호 지정에 대한 자세한 내용은 SSL 컨피그레이션, 22-23페이지를 참조하십시오. 이러한 문제가 발생하는 경우 이 옵션을 사용하여 하나 또는 두 개의 기능에 대해 ECDHE 암호 사용을 사용하지 않거나 사용하도록 설정합니다.
status	시스템 상태를 표시합니다.
supportrequest	Cisco IronPort 고객 지원에 지원 요청 이메일을 보냅니다. 이 이메일에는 시스템 정보와 마스터 컨피그레이션 사본이 포함됩니다.

tail	로그 파일의 끝을 표시합니다. 이 명령은 로그 파일 이름 또는 숫자를 매개변수로 허용합니다.
	`example.com> tail system_logs`
	`example.com> tail 9`

tcpservices	개방형 TCP/IP 서비스에 대한 정보를 표시합니다.
techsupport	Cisco IronPort 고객 지원에서 시스템에 액세스하여 트러블슈팅을 지원할 수 있도록 임시 연결을 제공합니다.
텔넷(telnet)	TELNET 프로토콜을 사용하여 다른 호스트와 통신합니다.

testauthconfig	영역에 정의된 인증 서버에 대해 지정된 인증 영역의 인증 설정을 테스트합니다. `testauthconfig [-d level] [realm name]` 옵션 없이 명령을 실행하면 어플라이언스에서 사용자가 선택할 수 있는 구성된 인증 영역을 나열합니다. 디버그 플래그(-d)는 디버그 정보의 레벨을 제어합니다. 레벨의 범위는 0 ~ 10일 수 있습니다. 지정되지 않으면 어플라이언스에서 레벨 0을 사용합니다. 레벨 0을 사용하면 명령이 성공 또는 실패를 반환합니다. 테스트 설정이 실패하는 경우 명령이 실패의 원인을 나열합니다. **참고** 레벨 0을 사용하는 것이 좋습니다. 트러블슈팅을 위해 자세한 정보가 필요한 경우에만 다른 디버그 레벨을 사용하십시오.
traceroute	게이트웨이를 통하거나 대상 호스트에 대한 경로를 따라 IP 패킷을 추적합니다.
tuiconfig tuistatus	이러한 두 명령은 CLI를 사용하여 고급 투명한 사용자 식별 설정 구성, 5-9페이지에 문서화되어 있습니다.
updateconfig	업데이트 및 업그레이드 설정을 구성합니다.
updatenow	모든 구성 요소를 업데이트합니다.
upgrade	AsyncOS 소프트웨어 업그레이드를 설치합니다.
userconfig	시스템 관리자를 구성합니다.
version	일반 시스템 정보, 설치된 시스템 소프트웨어 버전 및 규칙 정의를 표시합니다.
webcache	프록시 캐시의 콘텐츠를 검사 또는 수정하거나 어플라이언스에서 캐시하지 않는 도메인 및 URL을 구성합니다. 관리자가 특정 URL을 프록시 캐시에서 제거하거나 프록시 캐시에 저장하지 않을 도메인 또는 URL을 지정할 수 있습니다.
who	CLI 및 웹 인터페이스 세션 모두에 대해 시스템에 로그인된 사용자를 표시합니다. **참고** 각 사용자당 최대 10개의 동시 세션이 허용됩니다.
whoami	사용자 정보를 표시합니다.

추가 리소스

- Cisco 알림 서비스, C-1페이지
- 문서 집합, C-1페이지
- 교육, C-2페이지
- 기술 자료(TechNotes), C-2페이지
- Cisco 지원 커뮤니티, C-2페이지
- 고객 지원, C-2페이지
- 리소스에 액세스하기 위해 Cisco 계정 등록, C-3페이지
- 서드파티 기여자, C-3페이지
- Cisco에 의견 보내기, C-3페이지

Cisco 알림 서비스

보안 자문, 현장 통지, 판매 중단 및 지원 종료 안내문, 소프트웨어 업데이트 및 알려진 문제에 대한 정보 등 Cisco Content Security Appliance와 관련된 알림을 수신하려면 신청하십시오.

알림 빈도, 수신할 정보 유형 등의 옵션을 지정할 수 있습니다. 사용하는 각 제품에 대한 알림을 받으려면 개별적으로 신청해야 합니다.

신청하려면 http://www.cisco.com/cisco/support/notifications.html을 방문해 주십시오.

Cisco.com 계정이 필요합니다. 계정이 없으면 리소스에 액세스하기 위해 Cisco 계정 등록, C-3페이지 섹션을 참조해 주십시오.

문서 집합

Cisco Web Security Appliance 관련 문서를 다음 위치에서 볼 수 있습니다.

제품	링크
웹 보안 어플라이언스 (하드웨어 설명서 포함)	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

제품	링크
Content Security Management Appliance (하드웨어 설명서 포함)	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Cloud Web Security (하드웨어 설명서 포함)	http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

교육

Cisco 이메일 및 웹 보안 제품에 대한 교육:

http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

기술 자료(TechNotes)

1단계 기본 제품 페이지로 이동합니다 (http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html).

2단계 **TechNotes**라는 이름의 링크를 찾습니다.

Cisco 지원 커뮤니티

다음 URL에서 웹 보안 및 연관된 관리를 위한 Cisco 지원 커뮤니티에 액세스하십시오.

https://supportforums.cisco.com/community/5786/web-security

Cisco 지원 커뮤니티에서는 일반적인 웹 보안 문제에 대해 논의하고 특정 Cisco 제품에 대한 기술 정보를 얻을 수 있습니다. 예를 들어, 게시물에 트러블슈팅 비디오가 포함될 수 있습니다.

고객 지원

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

레거시 IronPort에 대한 지원 사이트:
http://www.cisco.com/web/services/acquisitions/ironport.html

가상 어플라이언스에 대한 지침은 *Cisco Content Security Virtual Appliance 설치 설명서*를 참조하십시오.

심각하지 않은 문제의 경우 어플라이언스에서 지원 사례를 열 수도 있습니다.

관련 주제

- 지원에 대한 작업, A-24페이지.

리소스에 액세스하기 위해 Cisco 계정 등록

Cisco.com의 많은 리소스에 액세스하려면 Cisco 계정이 필요합니다.

Cisco.com 사용자 ID가 없는 경우 다음에서 등록할 수 있습니다.
https://tools.cisco.com/RPF/register/register.do

서드파티 기여자

AsyncOS에 포함된 일부 소프트웨어는 FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc. 및 기타 서드파티 지원업체의 소프트웨어 라이센스 계약의 약관, 통지 및 조건에 따라 배포되며 이러한 모든 약관과 조건은 라이센스 계약에 통합되어 있습니다. 이러한 계약의 전문은 다음에서 찾아볼 수 있습니다.

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

AsyncOS에 포함된 소프트웨어의 일부는 Tobi Oetiker가 명시적으로 서면 동의한 RRDtool을 기반으로 합니다.

이 문서의 일부는 Dell Computer Corporation의 허가로 다시 작성되었습니다. 이 문서의 일부는 McAfee, Inc.의 허가로 다시 작성되었습니다. 이 문서의 일부는 Sophos Plc.의 허가로 다시 작성되었습니다.

Cisco에 의견 보내기

Cisco Technical Publications 팀은 더 우수한 제품 설명서를 제공하기 위해 최선을 다하고 있습니다. 소중한 의견과 제안을 언제라도 보내주십시오. 다음 이메일 주소로 의견을 보내실 수 있습니다. contentsecuritydocs@cisco.com

메시지의 제목 행에 이 책의 제목 및 제목 페이지에 표시된 발행일을 기재해 주십시오.

최종 사용자 라이센스 계약

- Cisco Systems 최종 사용자 라이센스 계약, D-1페이지
- Cisco Systems Content Security 소프트웨어에 대한 보충 최종 사용자 라이센스 계약, D-6페이지

Cisco Systems 최종 사용자 라이센스 계약

중요: 본 최종 사용자 라이센스 계약을 주의 깊게 읽으십시오. 귀하가 CISCO 소프트웨어 또는 장비를 승인된 소스로부터 구매하고 있는지, 그리고 귀하 또는 귀하가 대표하는 실체("고객"으로 통칭)가 본 CISCO 최종 사용자 라이센스 계약의 목적에 맞게 최종 사용자로 등록되었는지를 확인하는 것이 매우 중요합니다. 귀하는 최종 사용자로 등록되어 있지 않은 경우 소프트웨어를 사용할 라이센스가 없으며 본 최종 사용자 라이센스 계약의 제한된 보증이 적용되지 않습니다. CISCO 또는 CISCO 제공 소프트웨어를 승인된 소스로부터 구매하고 다운로드, 설치 또는 사용하는 경우 귀하는 본 계약에 동의하는 것입니다.

Cisco Systems, Inc. 또는 CISCO SYSTEMS, INC. 대신 소프트웨어를 라이센싱하는 자회사("CISCO")는 귀하가 소프트웨어를 승인된 소스로부터 구매한 경우 그리고 본 최종 사용자 라이센스 계약에 포함된 모든 약관 및 제품에 수반되거나 주문 시 사용 가능한 보충 라이센스 계약("계약"으로 통칭)에 명시된 모든 추가 제한 사항에 동의하는 경우에만 본 소프트웨어의 라이센스를 부여합니다. 본 최종 사용자 라이센스 계약 및 보충 라이센스 계약의 조건이 상충하는 경우 보충 라이센스 계약이 적용됩니다. 소프트웨어를 다운로드, 설치 또는 사용함으로써 귀하는 소프트웨어를 승인된 소스로부터 구매하였으며 계약을 준수할 것임을 나타내는 것입니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 승인된 소스로부터 구매한 지 30일 후에 만료되며, 귀하가 등록되어 있는 원래 최종 사용자 구매자인 경우에만 적용됩니다. 본 최종 사용자 라이센스 계약에서 "승인된 소스"란 (A) CISCO 또는 (B) 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포하도록 CISCO에서 승인한 총판사 또는 시스템 통합업체 또는 (C) 그러한 총판사 또는 시스템 통합업체에서 CISCO와 총판사의 계약 조건에 따라 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포/판매하도록 승인한 리셀러를 의미합니다.

다음의 계약 조건은 고객의 소프트웨어 사용(아래에 정의)을 제어하되, (A) 고객과 고객의 소프트웨어 사용을 제어하는 CISCO 간에 별도의 서명된 계약이 있는 경우 또는 (B) 고객의 소프트웨어 사용을 제어하는 설치 또는 다운로드 프로세스의 일부로서 소프트웨어에 별도의 "클릭-동의" 라이센스 계약 또는 서드파티 라이센스 계약이 포함된 경우는 예외입니다. 앞서 언급한 문서의 조항이 상충하는 경우 우선순위는 (1) 서명된 계약, (2) 클릭-동의 계약 또는 서드파티 라이센스 계약, (3) 본 계약입니다. 본 계약에서 "소프트웨어"란 컴퓨터 프로그램(승인된 소스에서 고객에게 제공된 CISCO 장비에 내장된 펌웨어 및 컴퓨터 프로그램 포함), 업그레이드, 업데이트, 버그 픽스 또는 이에 따른 수정 버전("업그레이드"로 통칭), CISCO 소프트웨어 양도 및 재라이센싱 정책(CISCO에서 수시로 수정 가능)에 따라 재라이센스된 것 또는 그러한 것의 백업 사본을 의미합니다.

라이센스. 본 계약의 약관을 준수하는 범위에서 Cisco는 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 소프트웨어 및 문서를 고객의 내부 비즈니스 목적으로 사용할 비독점적이고 양도 불가능한 라이센스를 부여합니다. "문서"란 소프트웨어에 관해 작성되어 승인된 소스에서 어떤 방식으로든(CD-ROM 또는 온라인) 소프트웨어와 함께 사용하도록 제공하는 정보(사용자 또는 기술 매뉴얼, 교육 자료, 사양 등)를 의미합니다. 소프트웨어를 사용하려면 고객은 등록 번호나 제품 인증 키를 입력하고 Cisco 웹사이트에서 소프트웨어의 고객 사본을 온라인으로 등록하여 필요한 라이센스 키 또는 라이센스 파일을 얻어야 할 수 있습니다.

고객의 소프트웨어 사용 라이센스 및 소프트웨어 사용 범위는 단일 하드웨어 섀시나 카드로 제한되거나, 해당 보충 라이센스 계약에 명시되거나 승인된 소스가 동의했고 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 해당 구매 발주서("구매 발주서")에 명시된 기타 제한 사항으로 제한됩니다.

문서 또는 해당되는 보충 라이센스 계약에 달리 명시하지 않는 한 고객은 소프트웨어를 내장된 대로 실행에 사용하거나, (해당 문서에서 비 Cisco 장비에 설치를 허용한 경우) 고객이 소유하거나 임대한 Cisco 장비와의 통신 및 고객의 내부 비즈니스 용도로 사용할 수 있습니다. 암시, 금반언 등에 의해 다른 어떤 라이센스도 부여되지 않습니다.

Cisco에서 라이센스 요금을 부과하지 않는 평가판 또는 베타 사본의 경우 위의 라이센스 요금 지불 요건이 적용되지 않습니다.

일반 제한 사항. 타이틀의 양도가 아니라 소프트웨어 및 문서에 대한 라이센스이므로 Cisco는 소프트웨어 및 문서의 모든 사본에 대한 소유권을 보유합니다. 소프트웨어 및 문서에는 개별 프로그램의 특정 내부 설계와 구조 및 관련 인터페이스 정보를 포함하여(이에 제한되지 않음) Cisco 또는 공급업체나 라이센스 허가업체의 영업 비밀이 포함되어 있음을 고객은 인지합니다. 계약에 달리 명시하지 않는 한 고객은 승인된 소스로부터 구매한 Cisco 장비의 사용과 연결해서만 소프트웨어를 사용하며, 고객은 다음에 대해 권리가 없고 다음을 수행하지 않을 것에 특별히 동의합니다.

(i) 타인 또는 다른 실체에 라이센스 권리를 양도하거나 하위 라이센스를 부여하거나(Cisco 재라이센싱/양도 정책 적용의 준수 외), 고객이 승인된 소스로부터 구매하지 않은 Cisco 장비 또는 중고 Cisco 장비에서 소프트웨어를 사용하는 행위. 고객은 양도, 하위 라이센스 부여 또는 사용을 시도하는 행위가 무효임을 인지합니다.

(ii) 오류를 고치거나 소프트웨어를 달리 수정 또는 각색하거나 소프트웨어를 기반으로 파생물을 만들거나 서드파티에 동일한 일을 하도록 허용하는 행위.

(iii) 소프트웨어를 리버스 엔지니어링 또는 디컴파일, 해독, 디스어셈블하거나 인간이 읽을 수 있는 형식으로 축소하는 행위. 단, 이러한 제한에도 불구하고 적용법에 따라 명시적으로 허가되거나 적용되는 오픈 소스 라이센스에 따라 Cisco가 특정 활동을 허가해야 하는 경우는 예외입니다.

(iv) 소프트웨어에서 실행되는 벤치마크 테스트의 결과를 게시하는 행위.

(v) Cisco의 명시적인 서면 인증 없이 서비스 사무소에서 또는 시간 공유 기반으로 서드파티의 서비스를 수행하는 데 소프트웨어를 사용하거나 사용하도록 허가하는 행위.

(vi) Cisco의 사전 서면 승인 없이 소프트웨어 및 문서 내에 포함된 영업 비밀을 서드파티에서 사용할 수 있도록 공개, 제공 또는 달리 조작하는 행위. 고객은 그러한 영업 비밀을 보호하기 위해 합당한 보안 조치를 취해야 합니다.

적용법의 요구에 따라 그리고 고객의 서면 요청에 따라 Cisco는 해당 요금을 Cisco에 지불하는 경우 소프트웨어와 다른 독립적으로 생성된 프로그램 간 상호 운용성을 위해 필요한 인터페이스 정보를 고객에게 제공합니다. 고객은 그러한 정보와 관련된 기밀 유지의 책임을 엄격히 준수해야 하며, Cisco에서 그러한 정보를 사용 가능하게 하는 해당 약관에 따라 그러한 정보를 사용해야 합니다.

소프트웨어, 업그레이드 및 추가 사본. 계약의 다른 조항에도 불구하고: (1) 사본이나 업그레이드를 만들거나 얻은 시점에 고객이 이미 원본 소프트웨어에 대한 유효한 라이센스를 보유하고 있으며 업그레이드 또는 추가 사본에 대해 승인된 소스에 해당 요금을 이미 지불한 경우가 아닌 한, 고객은 추가 사본 또는 업그레이드를 만들거나 사용할 라이센스 또는 권리가 없습니다. (2) 업그레이드 사용은 고객이 원래 최종 사용자 구매자 또는 임차인이거나 업그레이드할 소프트웨어 사용에 대한 유효한 라이센스를 보유하고 있는, 승인된 소스가 제공한 CISCO 장비로 제한됩니다. (3) 추가 사본을 만들고 사용하는 것은 필요한 백업용으로만 제한됩니다.

소유 자산 통지. 고객은 어떤 형식이든 모든 저작권, 소유 자산 및 기타 통지를, 그러한 저작권 및 기타 소유 자산 통지가 소프트웨어에 포함되어 있는 것과 동일한 형식과 방법으로, 소프트웨어의 모든 사본에서 유지 및 재현할 것에 동의합니다. 계약에 명시적으로 승인된 경우를 제외하고, 고객은 Cisco의 사전 서면 승인 없이 소프트웨어의 사본이나 복제본을 만들지 않습니다.

기간 및 종료. 계약 및 여기에 부여된 라이센스는 종료될 때까지 유효합니다. 고객은 소프트웨어와 문서의 모든 사본을 폐기함으로써 언제든지 계약과 라이센스를 종료할 수 있습니다. 고객이 계약의 조항을 준수하지 않으면 계약에 따른 고객의 권리는 Cisco에서의 통보 없이 즉시 종료됩니다. 종료 시 고객은 소유 또는 제어하는 모든 소프트웨어 및 문서의 사본을 폐기해야 합니다. 고객의 모든 기밀 유지 책임, "일반 제한 사항" 섹션에서 고객에게 부여된 모든 제약 조건과 제한 사항 그리고 모든 책임과 면책조항과 보증의 제한과 제약은 계약의 종료 이후에도 유지됩니다. 또한 "미국 정부 최종 사용자 구매자" 및 "제한된 보증 안내문 및 최종 사용자 라이센스 계약에 적용되는 일반 약관" 섹션의 조항은 계약 종료 이후에도 유지됩니다.

고객 레코드. 고객은 본 계약의 준수 여부를 확인하기 위해 정상 영업시간에 고객의 장부, 레코드 및 회계를 검토할 권리를 Cisco 및 해당 독립 회계업체에 부여합니다. 그러한 감사에서 본 계약의 위반이 발견되면 고객은 적절한 라이센스 요금 및 감사에 따른 합당한 비용을 즉시 Cisco에 지불해야 합니다.

수출, 재수출, 양도 및 규제 사용. 계약에 따라 Cisco에서 제공하는 소프트웨어, 문서와 기술 또는 그에 따른 직접 제품(이후 "소프트웨어 및 기술")은 미국의 법률과 규정 및 기타 해당 국가의 법률과 규정에 따라 수출 규제의 대상이 됩니다. 고객은 Cisco 소프트웨어 및 기술의 수출, 재수출, 양도, 사용을 관장하는 관련 법률과 규정을 준수해야 하며 미국 및 현지의 모든 필요한 승인, 허가 또는 라이센스를 얻어야 합니다. Cisco와 고객은 권한 또는 라이센스의 보호와 관련하여 상대방에 합리적으로 요구할 수 있는 기타 정보, 지원 문서 및 지원을 제공할 것에 각각 동의합니다. 수출, 재수출, 양도 및 사용의 규정준수와 관련된 정보는 다음 URL에서 찾을 수 있습니다.

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

미국 정부 최종 사용자 구매자 소프트웨어 및 문서는 Federal Acquisition Regulation("FAR") (48 C.F.R.) 2.101에 정의된 대로 "상용 품목"이며, FAR 12.212에 사용된 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서" 같은 용어로 구성되어 있습니다. FAR 12.212 및 DoD FAR Supp. 227.7202-1~227.7202-4와 일치하고 계약에 통합되어 있을 수 있는 다른 계약에 반하는 FAR 또는 기타 계약 조항이 있더라도, 고객은 정부 최종 사용자에게 소프트웨어 및 문서를 제공할 수 있으며, 계약이 직접적인 경우 정부 최종 사용자는 계약에 명시된 권리만으로 소프트웨어 및 문서를 취득하게 됩니다. 소프트웨어나 문서 또는 둘을 모두 사용하는 경우 소프트웨어 및 문서는 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서"라는 정부와의 계약이 성립되고, 여기에 명시된 권리와 제약 조건을 따르는 것으로 간주됩니다.

식별된 구성 요소: 추가 용어. 소프트웨어는 하나 이상의 구성 요소를 포함하거나 그러한 구성 요소와 함께 제공될 수 있으며, 그러한 구성 요소에는 Cisco가 문서, readme.txt 파일, 서드파티 클릭-동의 또는 다른 곳(예: www.cisco.com)에서 식별한 서드파티 구성 요소("식별된 구성 요소")가 포함될 수 있고, 여기에 명시된 것과 다른 라이센스 계약 조건, 보증의 면책조항, 제한된 보증 또는 기타 약관("추가 조건"으로 통칭)이 적용될 수 있습니다. 귀하는 그러한 식별된 구성 요소에 적용되는 추가 조건에 동의합니다.

제한된 보증

여기에 명시된 제한 사항과 조건에 따라 Cisco는 (a) 소프트웨어를 담아 제공하는 미디어는 정상적으로 사용할 경우 재질 및 제조상 결함이 없으며, (b) 소프트웨어는 실제로 문서와 일치한다는 점을, 고객에게 배송된 날짜부터 시작(Cisco 이외의 승인된 소스에 의해 재판매되는 경우 Cisco의 원래 배송일 이후 90일 기간에 시작)하여 (a) 90일 동안 또는 (b) 소프트웨어가 포함된 제품("제품")에 동봉된 보증 카드에 소프트웨어에 대해 특별히 명시된 보증 기간(있는 경우) 동안 보증합니다. Cisco 제품 배송 날짜는 제품이 배송되는 포장 재료에 명시됩니다. 상기 내용을 제외하고 소프트웨어는 "있는 그대로" 제공됩니다. 본 제한된 보증은 처음 등록된 최종 사용자인 고객이 승인된 소스로부터 구매한 소프트웨어에만 적용됩니다. 본 제한된 보증에 따라 고객의 유일한 보상 및 Cisco와 공급업체의 전체 책임은 (i) 결함 있는 미디어의 교체 및/또는 (ii) Cisco의 선택에 따른 수리, 교체 또는 소프트웨어 구매 가격의 환불이며, 두 경우 모두 본 제한된 보증의 위반을 구성하는 오류나 결함은 보증된 기간 내에 고객에게 소프트웨어를 제공한 승인된 소스로 보고된 것이어야 합니다. Cisco 또는 고객에게 소프트웨어를 제공하는 승인된 소스는 보상의 조건으로서 선택적으로 소프트웨어 및/또는 문서의 반환을 요구할 수 있습니다. 어떤 경우에도 Cisco는 소프트웨어에 오류가 없음과 고객이 문제 또는 중단 없이 소프트웨어를 작동할 수 있을 것임을 보증합니다. 또한 네트워크 침입과 공격을 위한 지속적인 신기술 개발 때문에 Cisco는 소프트웨어 또는 소프트웨어가 사용되는 장비, 시스템 또는 네트워크가 침입이나 공격에 취약하지 않을 것이라고 보증하지 않습니다.

제약 조건. 소프트웨어, 제품 또는 소프트웨어 사용이 인증된 기타 장비가 (a) 변경된 경우(Cisco 또는 공인 대리점에서 변경한 경우 제외), (b) Cisco에서 제공한 지침에 따라 설치, 작동, 수리 또는 유지 관리된 경우, (c) 비정상적인 물리적 또는 전기적 스트레스, 비정상적인 환경 조건, 오용, 부주의, 사고를 겪은 경우 또는 (d) 베타, 평가, 테스트 또는 데모 목적으로 라이센스가 부여된 경우에는 본 보증이 적용되지 않습니다. 또한 (e) 임시 소프트웨어 모듈, (f) Cisco 소프트웨어 센터에 게시되지 않은 소프트웨어, (g) Cisco가 Cisco 소프트웨어 센터에 "있는 그대로" 기반으로 명시적으로 제공하는 소프트웨어, (h) 승인된 소스에서 라이센스 요금을 받지 않는 소프트웨어, (i) 승인된 소스가 아닌 서드파티에서 제공하는 소프트웨어에도 소프트웨어 보증이 적용되지 않습니다.

보증의 면책조항

본 보증 섹션에 지정된 내용을 제외하고, 상업성, 특정 목적에의 적합성, 비위반, 만족스런 품질, 비간섭, 정보 내용의 정확성을 포함하여(이에 제한되지 않음) 또는 거래, 법률, 사용 또는 무역 관행에서 발생하는 모든 명시적 또는 암시적 조건, 표현 및 보증은 적용법에서 허용하는 한도까지 제외되며 CISCO, 공급업체 또는 라이센스 허가업체에 의해 명시적으로 부인됩니다. 동일한 것 중 어떤 것도 제외할 수 없는 경우, 그러한 암시적 조건, 표현 및/또는 보증은 위의 "제한적 보증" 섹션에 나와 있는 명시적 보증 기간까지로 제한됩니다. 일부 국가나 관할 지역에서는 암시적 보증의 지속 기간에 대한 제한을 허용하지 않으므로 위의 제한 사항이 적용되지 않을 수 있습니다. 본 보증은 고객에게 특별한 법적 권리를 제공하며, 고객은 관할 지역에 따라 다른 권리를 보유할 수 있습니다. 위에 기술한 명시적 보증이 본질적 목적에 맞지 않는 경우에도 본 면책조항 및 예외는 적용됩니다.

책임의 면책조항 - 책임의 제한 사항. 미국, 라틴아메리카, 캐나다, 일본 및 카리브해에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 보증 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 승인된 소스에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다).

유럽, 중동, 아프리카, 아시아 및 오세아니아에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 보증 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 CISCO에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다). 계약의 어떤 내용도 (I) 과실로 인한 개인 상해 또는 사망에 대해 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 책임을 제한하지 않고, (II) CISCO의 기만적 허위진술에 대한 책임을 제한하지 않으며, 또는 (III) 적용법에 따라 제외할 수 없는 CISCO의 책임을 제한하지 않습니다.

책임의 면책조항 - 결과적 손해 및 기타 손실의 면제. 미국, 라틴아메리카, 카리브해 또는 캐나다에서 소프트웨어를 구매한 경우 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 어떤 경우에도, CISCO 및 공급업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO와 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 적용되지 않을 수 있습니다.

일본에서 소프트웨어를 구매한 경우 사망이나 개인 상해, 기만적 허위진술로 인해 발생하거나 이와 관련된 책임을 제외하고, 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO, 승인된 소스, 해당 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다.

유럽, 중동, 아프리카, 아시아 또는 오세아니아에서 소프트웨어를 구매한 경우 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 계약, 불법 행위(태만 포함)로 인해 발생하든 소프트웨어의 사용 또는 사용 불가로 인해 발생하든 상관없이 그리고 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 충분히 적용되지 않을 수 있습니다. 위의 예외는 다음과 관련하여 발생하는 책임에는 적용되지 않습니다. (I) 사망 또는 개인 상해, (II) 기만적 허위진술, 또는 (III) 적용법에서 제외할 수 없는 조건과 관련된 CISCO의 책임.

고객은 Cisco가 여기에 명시된 보증의 면책조항 및 책임의 제한 사항에 의존하여 가격을 책정하고 계약을 체결했으며, 동일한 내용이 양방 간 위험의 할당을 반영하며(계약 보상이 본질적 목적에 맞지 않고 결과적 손해를 초래할 위험 포함), 동일한 내용이 쌍방 간 거래의 필수적인 기초를 형성함을 인지하고 이에 동의합니다.

규제 법률, 관할지. 승인된 소스에서 수락한 구매 발주서의 주소를 참조하여 미국, 라틴아메리카 또는 카리브해에서 소프트웨어를 취득한 경우 계약 및 보증("보증")은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 캐나다에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 캐나다 온타리오 주의 법에 따라 제어되고 해석됩니다. 온타리오 주 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 유럽, 중동, 아프리카, 아시아 또는 오세아니아(오스트레일리아 제외)에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 영국의 법에 따라 제어되고 해석됩니다. 영국 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 또한 계약이 영국 법에 의해 제어되는 경우 계약 당사자가 아닌 사람은 Contracts(Rights of Third Parties) Act 1999 조건의 적용 또는 혜택을 받을 수 없습니다. 소프트웨어를 일본에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 일

본 법에 따라 제어되고 해석됩니다. 일본 도쿄 지방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 오스트레일리아에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 오스트레일리아 뉴 사우스 웨일스 주의 법에 따라 제어되고 해석됩니다. 뉴 사우스 웨일스 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 기타 국가에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다.

위에서 언급한 모든 국가에서 당사자들은 국제물품매매계약에 관한 국제연합협약(UN Convention on Contracts for the International Sale of Goods)을 부인합니다. 위의 내용에도 불구하고, 당사자는 자신의 지적 재산권 또는 소유권의 위반 혐의와 관련하여 해당 관할 지역의 법원에 임시 금지 명령 구제를 요청할 수 있습니다. 계약 및 보증의 일부가 무효이거나 집행 불가능한 것으로 판명되는 경우 나머지 조항은 완전한 효력을 유지합니다. 명시적으로 기술된 경우를 제외하고, 본 계약은 소프트웨어 및 문서의 라이센스에 대한 양방 간 완전한 합의를 구성하며, 구매 발주서 등에 포함된 충돌하는 조건 또는 추가 조건에 우선하며, 그러한 모든 조건은 제외됩니다. 본 계약은 영어로 작성되었으며, 양방은 영어 버전이 적용됨에 동의합니다.

Cisco 제품에 적용되는 제품 보증 조항 및 기타 정보는 다음 URL에서 확인할 수 있습니다.

http://www.cisco.com/go/warranty

Cisco Systems Content Security 소프트웨어에 대한 보충 최종 사용자 라이센스 계약

중요: 신중하게 읽어보십시오.

본 보충 최종 사용자 라이센스 계약("SEULA")에는 귀하(여기에서 "귀하"란 귀하 및 귀하가 대표하는 기업체 또는 "회사"를 의미함)와 Cisco 간 최종 사용자 라이센스 계약("EULA")("계약"으로 통칭)에 따라 라이센스가 부여된 소프트웨어에 대한 추가 약관이 포함되어 있습니다. 본 SEULA에 사용되었지만 정의되지 않은 대문자로 표시된 용어는 EULA에서 정의된 의미로 사용됩니다. EULA와 본 SEULA의 약관 사이에 충돌이 있는 경우 본 SEULA의 약관이 우선 적용됩니다.

소프트웨어의 액세스 및 사용에 대해 EULA에 명시된 제한 사항 외에도 귀하는 언제나 본 SEULA에 제공된 약관을 준수할 것에 동의합니다.

소프트웨어를 다운로드, 설치 또는 사용하는 것은 계약에 대한 동의를 의미하며, 귀하 및 귀하가 대표하는 사업체는 계약을 준수해야 합니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 CISCO 또는 승인된 CISCO 리셀러로부터 구매한 지 30일 후에 만료되며, 귀하가 원래 최종 사용자 구매자인 경우에만 적용됩니다.

본 SEULA에서, 귀하가 주문한 제품 이름 및 제품 설명은 Cisco Systems Email Security Appliance("ESA"), Cisco Systems Web Security Appliance("WSA") 및 Cisco Systems Security Management Application("SMA")("Content Security"로 통칭) 및 가상 어플라이언스 해당 제품("소프트웨어") 중 하나입니다.

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

정의

본 SEULA에서는 다음과 같은 의미로 용어가 사용되었습니다.

"회사 서비스"란 회사의 내부 비즈니스 수행을 위해 최종 사용자에게 제공되는 회사의 이메일, 인터넷, 보안 관리 서비스를 의미합니다.

"최종 사용자"란 (1) WSA와 SMA의 경우, 회사에서 회사 서비스를 통해 인터넷 및 SMA에 액세스하도록 승인한 직원, 계약직원 및 기타 에이전트를 의미하고, (2) ESA의 경우, 회사에서 회사 서비스를 통해 이메일 서비스에 액세스하고 사용하도록 승인한 직원, 계약직원 또는 기타 에이전트의 이메일 편지함을 의미합니다.

주문 문서란 회사와 Cisco 또는 회사와 Cisco 리셀러 간 구매 계약, 평가 계약, 베타, 사전 릴리스 계약 또는 유사한 계약, 또는 본 계약에서 허용한 소프트웨어 라이센스에 대한 구매 조건을 포함하여 이와 따라 Cisco에서 수락하는 모든 구매 발주서의 유효한 조건을 의미합니다.

"개인 식별 가능 정보"란 개인의 이름, 사용자 이름, 이메일 주소 및 기타 개인 식별이 가능한 정보를 포함하여(이에 제한되지 않음) 개인을 식별하는 데 사용할 수 있는 정보를 의미합니다.

"서버"란 여러 사용자를 위한 네트워크 리소스를 관리 또는 제공하는 네트워크상의 단일 물리적 컴퓨터 또는 디바이스를 의미합니다.

"서비스"란 Cisco 소프트웨어 구독 서비스를 의미합니다.

"서비스 설명"이란 http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html에 있는 소프트웨어 구독 지원 서비스의 설명을 의미합니다.

"텔레메트리 데이터"란 회사 이메일 및 웹 트래픽의 샘플을 의미합니다. 여기에는 이메일 메시지 및 웹 요청 특성에 대한 데이터, 그리고 회사의 Cisco 하드웨어 제품에서 서로 다른 유형의 이메일 메시지 및 웹 요청이 처리된 방식에 대한 정보가 포함됩니다. 텔레메트리 데이터에 포함된 이메일 메시지 메타데이터 및 웹 요청은 개인 식별 가능 정보를 제거하기 위해 알아볼 수 없도록 익명으로 처리됩니다.

"기간"이란 주문 문서에 표시된 대로 귀하가 주문한 소프트웨어 구독의 기간을 의미합니다.

"가상 어플라이언스"란 Cisco Email Security Appliance, Web Security Appliance 및 Security Management Appliance의 가상 버전을 의미합니다.

"가상 머신"이란 자체 운영 체제를 실행할 수 있고 서버처럼 애플리케이션을 실행할 수 있는 소프트웨어 컨테이너를 의미합니다.

추가 라이센스 약관

데이터 수집 조건에 대한 라이센스 허가 및 승낙

소프트웨어 라이센스.

소프트웨어 및 문서를 사용함으로써 회사는 본 계약의 조건을 준수할 것에 동의하며, 회사가 본 계약을 준수하는 한 Cisco는 Cisco 하드웨어 제품에서만, 또는 가상 어플라이언스의 경우 최종 사용자에 대한 회사 서비스의 조항과 관련하여 가상 머신에서만 지정된 기간 동안 소프트웨어를 사용하도록, 하위 라이센스 부여나 양도가 불가능한 비배타적이며 세계적인 라이센스를 회사에 부여합니다. 소프트웨어를 사용할 수 있는 라이센스가 부여되는 최종 사용자의 수는 주문 문서에 지정된 최종 사용자의 수로 제한됩니다. 회사 서비스 조항과 관련된 최종 사용자의 수가 주문 문서에 지정된 최종 사용자의 수를 초과하면 회사는 승인된 소스에 연락하여 소프트웨어의 추가 라이센스를 구매해야 합니다. 본 라이센스의 기간과 범위는 주문 문서에 자세히 정의되어 있습니다. 주문 문서는 소프트웨어 라이센스의 조건과 관련하여 EULA에 우선합니다. 여기에서 부여된 라이센스 권리 외에 Cisco, Cisco의 리셀러 또는 개별 라이센스 허가업체는 회사에 어떤 권리, 타이틀 또는 이권도 부여하지 않습니다. 귀하의 소프트웨어 업그레이드 자격은 서비스 설명의 적용을 받습니다. 본 계약과 서비스는 동시에 종료됩니다.

데이터 사용에 대한 동의 및 라이센스.

Cisco 개인정보 보호정책(http://www.cisco.com/web/siteassets/legal/privacy.html)에 따라 회사는 Cisco가 회사에서 텔레메트리 데이터를 수집하고 사용하도록 허락하며 해당 권한을 부여합니다. Cisco는 텔레메트리 데이터에서 개인 식별 가능 정보를 수집하거나 사용하지 않습니다. 사용자 환경과 소프트웨어, 그리고 기타 Cisco 보안 제품 및 서비스의 개선을 위해 Cisco는 집계된 익명의 텔레메트리 데이터를 서드파티와 공유할 수 있습니다. 회사는 소프트웨어에서 SenderBase 네트워크 참여를 비활성화하여 언제든지 Cisco의 텔레메트리 데이터 수집 권리를 종료할 수 있습니다. SenderBase 네트워크 참여의 활성화 또는 비활성화에 대한 지침은 소프트웨어 컨피그레이션 가이드에서 찾아볼 수 있습니다.

기타 권리 및 의무에 대한 설명

Cisco Systems, Inc. 최종 사용자 라이센스 계약, 개인정보 취급방침 및 소프트웨어 구독 지원 서비스의 서비스 설명을 참조하십시오.

색 인

A

ACL 결정 태그
  액세스 로그 파일 21-17
Active Directory 5-1
adminaccessconfig 명령
  개요 22-11
Advanced Malware Protection 14-1
  MONITOR_AMP_RESP 21-19
AMP. Advanced Malware Protection 참조.
AMP(Advanced Malware Protection) 14-1
AMW
  안티멀웨어 참조
AsyncOS 복귀 22-33
AVC 엔진
  사용 15-2
  업데이트 15-2

C

Cisco ASA 통합
  개요 10-19
Cisco Cloud Web Security
  게스트 사용자 3-8
Cisco IronPort 데이터 보안 정책
  데이터 보안 정책 참조
  요청의 사용자 위치 16-6
Cisco Web Usage Controls
  개요 9-1
Cisco 데이터 보안 정책
  및 URL 카테고리 변경 9-5
CLI
  SSH B-1
  개요 B-1
  대소문자 구분 B-3
  언어 구성 22-11
  호스트 키 구성 21-14
Cloud Web Security Connector
  FTP 3-6
  Cloud Web Security Connector
    HTTPS 3-6
  구성 3-2
  기록 3-7
  데이터 유출 방지 3-6
  디렉토리 그룹 정책 3-5
  문서 3-1
  사용자 인증 3-7
  클라우드 라우팅 정책 3-5
  클라우드 커넥터 설정 3-3
  표준 모드와 비교 2-2
commit 명령 B-4
CSR(Certificate Signing Request)
  HTTPS 프록시용 11-8
  SaaS용 ID 공급자 7-3
  웹 인터페이스용 22-27
CSS
  최종 사용자 알림 페이지에서 17-10

D

datasecurityconfig
  CLI 명령 16-2
DCA(Dynamic Content Analysis) 엔진
  사용 9-4
DLP 서버
  정의 16-9

페일오버 16-10
DNS
구성 2-29
분할 2-30
신뢰할 수 있는 이름 서버 2-29
DNS 캐시
플러싱 2-30
DVS(Dynamic Vectoring and Streaming) 엔진
DVS 엔진 참조
DVS 엔진
다중 악성코드 판정에 대한 작업 13-5
작동 방식 13-5

E

`etherconfig` 명령
VLAN 2-25
`externaldlpconfig`
CLI 명령 16-2

F

Federal Information Processing Standards 22-21
FIPS
모드 22-21
인증서 요건 22-21
컴플라이언스 22-21
FIPS(Federal Information Processing Standards) 22-21
FTP
알림 메시지 구성 17-9
최종 사용자 승인 페이지 17-3

G

GUI
언어 구성 22-11

H

`hostkeyconfig` 명령 21-14
HTTPS
기록 A-12
라우팅 11-10
암호 해독 우회 A-8
최종 사용자 승인 페이지 17-3
HTTPS 트래픽 암호 해독
암호 해독 정책 구성 11-1
HTTPS 프록시
구성 11-3
프록시에 대한 포트 11-3

I

ID 9-5
및 URL 카테고리 변경 9-5
`interfaceconfig` 명령
VLAN 2-27
IPv4 2-16
IPv4/IPv6 2-15
IPv6 2-16
IP 스푸핑
WCCP 서비스 2-25

K

Kerberos 5-1

L

L2
전달 방법 2-24
L4 트래픽 모니터
로그 파일 21-30
모호한 주소 20-2
보고서 19-8

안티멀웨어 규칙 20-2
알려진 악성코드 주소 20-2
알려진 허용 주소 20-2
인터페이스 2-5
활동 보기 20-5
L4 트래픽 모니터 인터페이스
개요 2-5
LDAP 5-1

M

MAIL FROM
알림 구성 22-13
McAfee 스캐닝 엔진
개요 13-6
데이터베이스 13-13
카테고리 13-6
휴리스틱 분석 13-6
MIB 파일
SNMP 22-35
MONITOR_AMP_RESP 21-19

N

nc(no category) 21-21
ns(no score) 21-21
NTLMSSP 5-1

O

OCSP 11-9

P

PDF
보고서 18-6

R

RFC
1065 22-35
1066 22-35
1067 22-35
1213 22-35
1907 22-35
2571-2575 22-35

S

SaaS 액세스 제어
개요 7-1
여러 어플라이언스 7-3
제로 데이 폐기 7-1
SensorBase Network 1-5
`sethostname` 명령
개요 2-28
SMI 파일
SNMP 22-35
SMTP 트랜잭션
로깅 21-5
SNMP
MIB 파일 22-35
SMI 파일 22-35
SNMPv1 22-35
SNMPv2 22-35
개요 22-35
여러 트랩 대상 지정 22-36
커뮤니티 문자열 22-35
트랩 22-36
SNMP(Simple Network Management Protocol)
SNMP 참조
SOCKS
개요 4-17
구성 4-17
사용 4-17
정책 4-18

Sophos 스캐닝 엔진
개요 13-7
SSH
CLI에 사용 B-1
supportrequest 명령 A-25

T

T1 및 T2 인터페이스
개요 2-5
TRT(Threat Risk Threshold)
Webroot 13-8

U

UDP_MISS 21-16
URL
Cisco IronPort 데이터 보안 정책 16-6
아웃바운드 악성코드 스캐닝 정책 12-4
외부 DLP 정책 16-6
URL 제출 툴
사용 9-3
URL 카테고리 9-18
분류되지 않은 URL 19-4
설명 9-23
약어 9-23
차단 16-7
URL 카테고리 보고서 19-4
URL 카테고리 집합
업데이트 9-4, 19-5, 22-3
URL 필터
URL 카테고리 설명 9-23
구성 9-9
데이터베이스 9-4
맞춤형 카테고리 9-14
사용 9-4
시간 기반 9-19
정규식 9-20
카테고리 없음 9-3
필터링 활동 보기 9-19

V

VLAN
etherconfig 명령 2-25
interfaceconfig 명령 2-27
레이블 2-25
VRT. 파일 분석을 참조하십시오.

W

W3C 액세스 로그
개요 21-24
WBRS
*웹 평판 필터*도 참조
WCCP 라우터
WCCP 서비스 2-22
WCCP 서비스
IP 스푸핑 2-25
개요 2-22
추가 2-22
편집 2-22
Webroot 스캐닝 엔진
TRT(Threat Risk Threshold) 13-8
개요 13-6
데이터베이스 13-13

Y

YouTube
헤더 21-38
YouTube, 다음에 대해 추가된 헤더 기록 21-38

ㄱ

개요 보고서 19-2
개체
  차단 16-8
검증
  인증서 11-6
결과 코드 21-16
경고
  경고 분류 22-14
경고 목록 22-16
경고 유형 22-14
경고 페이지
  최종 사용자 URL 카테고리 페이지 17-9
경로
  개요 2-20
  기본 경로 2-21
  분할 라우팅 2-20
구성 2-21
  HTTPS 프록시 11-3
  URL 필터 9-9
  관리자 설정 22-11
  반환 주소 22-13
  애플리케이션 제어 설정 15-3
  웹 평판 필터 13-12
구성원 자격 다이어그램
  Cisco IronPort 데이터 보안 정책 16-4
  아웃바운드 악성코드 스캐닝 정책 12-2
  외부 DLP 정책 16-4
그레이리스트 주소
  모호한 주소 참조
기능 키
  개요 22-4
  만료된 키 A-5
  설정 22-4
  수동으로 추가 22-4
기록
  HTTPS 요청 A-12
  리디렉션된 트래픽 9-17
기본 ID 6-1
기본 게이트웨이 2-21
기본 경로
  구성 2-21
기본 설정
  사용자에 대해 정의 22-11

ㄴ

내보내기
  보고서 18-6
네이티브 FTP
  알림 메시지 구성 17-9
  투명 리디렉션 및 IP 스푸핑 사용 2-23
네트워크 인터페이스 2-15
  T1 및 T2 2-5
네트워크 패킷 캡처
  개요 A-23

ㄷ

대소문자 구분
  CLI B-3
대역폭
  사용자 제한 구성 15-6
  전체 제한 구성 15-6
  제한 15-6
대역폭 제어
  개요 15-6
  사용자 제한 15-6
  전체 제한 15-6
대역폭 제한
  개요 15-6
  사용자당 15-6
  애플리케이션에 대해 구성 15-8
  애플리케이션 유형에 대해 구성 15-7
  애플리케이션 유형에 대해 재지정 15-7
  전체 15-6

데이터 보안 로그
개요 16-12
데이터 보안 정책
URL 필터 16-7
구성 16-7
구성원 자격 16-4
기록 16-12
생성 16-5
요청의 URL 카테고리 16-6
요청의 사용자 에이전트 16-6
요청의 서브넷 16-6
요청의 프로토콜 16-5
요청의 프록시 포트 16-6
웹 평판 16-8
최소 요청 크기 16-2
콘텐츠 16-8
흐름도 16-7
데이터 보안 정책, Cisco 9-5
데이터 보안 정책 구성원 자격 평가
클라이언트 요청 매칭 16-4
데이터 유출 방지
아웃바운드 악성코드 스캐닝 정책 참조
데이터 유출 방지 정책, 외부 9-5

ㄹ

라우팅
HTTPS 11-10
라우팅 정책 9-5
및 URL 카테고리 변경 9-5
로그 서브스크립션
추가 21-7
편집 21-7
로그 파일
L4 트래픽 모니터 21-30
명명 규칙 21-12
유형 21-3
최신 버전 보기 21-13
로그 파일 롤오버 21-12
로깅
SMTP 트랜잭션 21-5
YouTube 헤더 21-38
로드 밸런싱
외부 DLP 서버에 대한 트래픽 16-10
로드 밸런싱 방법 2-24
로드 밸런싱을 위한 마스크 맞춤화 2-24
로드 밸런싱을 위한 마스크와 해시 비교 2-24
로드 밸런싱을 위한 맞춤형 마스크 2-24
로드 밸런싱을 위한 해시와 마스크 비교 2-24
루트 인증서
생성 11-3
업로드 11-3

ㅁ

만료된 키
개요 A-5
맞춤형
URL 카테고리 9-14
트래픽 리디렉션 9-17
날짜 범위 18-3
최종 사용자 알림 페이지 17-12
헤더 21-38
매니페스트 XML 파일 22-32
머신 ID 서비스 3-8
모니터링
보고서 예약 18-7
시스템 활동 19-2
암호 해독 정책 11-2
요약 데이터 18-1
모호한 주소
정의됨 20-2

ㅂ

반환 주소
구성 22-13

범주
SaaS 및 B2B 9-28
개인 사이트 9-28
건강 및 영양 9-26
검색 엔진 및 포털 9-28
게임 9-25
경매 9-24
과학 및 기술 9-28
광고 9-23
교육 9-25
극도 9-25
나체주의 9-27
뉴스 9-27
담배 9-29
데이트 9-24
도박 9-25
동적 및 주거용 링크 9-25
디지털 엽서 9-24
란제리 및 수영복 9-27
무기 9-30
미분류 9-29
복권 9-27
부동산 9-28
부정행위 및 표절 9-24
불법 다운로드 9-26
불법 약물 9-26
불법 행위 9-26
비정부 기구 9-27
비즈니스 및 산업 9-24
사진 검색 및 이미지 9-28
사회과학 9-29
사회 및 문화 9-29
성교육 9-29
성인 9-23
소셜 네트워킹 9-29
소프트웨어 업데이트 9-29
쇼핑 9-29
스트리밍 비디오 9-29
스트리밍 오디오 9-29
스포츠 및 레크리에이션 9-29
식당 및 주점 9-25
아동 학대 콘텐츠 9-24
아트 9-24
어린이 안전 9-28
엔터테인먼트 9-25
여행 9-29
온라인 거래 9-27
온라인 스토리지 및 백업 9-27
온라인 커뮤니티 9-27
운송 9-29
웹 기반 이메일 9-30
웹 페이지 번역 9-30
웹 호스팅 9-30
유머 9-26
음란물 9-28
인터넷 텔레포니 9-26
인프라 및 콘텐츠 전달 네트워크 9-26
자연 9-27
재무 9-25
전문 네트워킹 9-28
점성술 9-24
정부 및 법률 9-26
정치 9-28
조직 이메일 9-27
종교 9-28
주류 9-24
참조 9-28
채용 정보 검색 9-27
채팅 및 인스턴트 메시징 9-24
컴퓨터 및 인터넷 9-24
컴퓨터 보안 9-24
파일 전송 서비스 9-25
파킹된 도메인 9-28
패션 9-25
프리웨어 및 셰어웨어 9-25
피어 파일 전송 9-28
필터 회피 9-25
해킹 9-26

혐오 발언 9-26
휴대폰 9-27
변수
최종 사용자 알림 페이지 17-12
보고
리디렉션된 트래픽 9-17
보고서
L4 트래픽 모니터 19-8
PDF로 인쇄 18-6
URL 카테고리 19-4
개요 19-2
검색 옵션 18-3
그래프 18-4
대화형 표시 18-1
데이터 내보내기 18-6
맞춤형 날짜 범위 18-3
멀웨어 위협 19-6
반환 주소 22-13
분류되지 않은 URL 19-4
사용자 위치별 보고서 19-8
사용자 이름을 인식 불가능하게 설정 18-1
사용자 이름 익명 처리 18-1
시간 범위 18-3
시스템 상태 19-13
시스템 용량 19-12
아카이브 18-9
악성코드 카테고리 19-5
안티멀웨어 19-5
애플리케이션 가시성 19-5
예약 18-7
예약된 보고서의 시간 범위 18-7
웹 사이트 19-4
웹 평판 필터 19-7
차트 18-4
클라이언트 세부사항 19-7
클라이언트 악성코드 위험 19-6
클라이언트 악성코드 위험 페이지 19-6
보안 모빌리티
보고서 19-8
복귀
설치 22-33
분류되지 않은 URL
URL 제출 툴 9-3
보고서에서 19-4
정의됨 9-3
분할 라우팅
정의됨 2-20
브라우저
웹 브라우저 참조
블랙리스트 주소
알려진 악성코드 주소 참조
비밀번호
변경 22-8
비밀번호 변경 22-8
비밀번호 변경 링크 22-8

ㅅ

사용
HTTPS 프록시 11-3
사용 가능한 업그레이드 22-28
사용자 계정
관리 22-7
정보 22-6
사용자 기본 설정
정의 22-11
사용자 비밀번호 22-8
사용자에게 경고 9-18
URL 카테고리 사용 9-18
최종 사용자 경고 페이지 구성 17-9
사용자 에이전트
Cisco IronPort 데이터 보안 정책 16-6
아웃바운드 악성코드 스캐닝 정책 12-4
외부 DLP 정책 16-6
사용자 위치
Cisco IronPort 데이터 보안 정책 16-6
아웃바운드 악성코드 스캐닝 정책 12-4
외부 DLP 정책 16-6

사용자 위치별 보고서 보고서
개요 19-8
사용자 이름
보고서에서 인식 불가능하게 설정 18-1
사용자 정의 알림 페이지
개요 17-6
매개변수 17-7
예 17-7
사이트 콘텐츠 등급
시행 9-15
샌드박싱. 파일 분석 참조
생성
Cisco IronPort 데이터 보안 정책 16-5
로그 서브스크립션 21-7
루트 인증서 11-3
아웃바운드 악성코드 스캐닝 정책 12-3
외부 DLP 정책 16-5
서브넷
Cisco IronPort 데이터 보안 정책 16-6
아웃바운드 악성코드 스캐닝 정책 12-4
액세스 정책 4-19
외부 DLP 정책 16-6
설치
복귀 22-33
성인 콘텐츠
사용 기록 9-16
필터링 9-15

부호

스캐닝 판정
안티멀웨어 21-40
시간 기반 정책
URL 필터 9-19
시간 및 볼륨 할당량 17-2
시간 범위
액세스 정책 4-19
시스템 상태 보고서 19-13
시스템 설정 마법사
보안 페이지 2-12
시스템 용량 보고서
개요 19-12

o

아웃바운드 악성코드 스캐닝
개요 12-1
아웃바운드 악성코드 스캐닝 구성원 자격 평가
클라이언트 요청 일치 12-2
아웃바운드 악성코드 스캐닝 정책 9-5
구성 12-4
구성원 자격 12-2
기록 12-5
및 URL 카테고리 변경 9-5
생성 12-3
요청의 URL 카테고리 12-4
요청의 사용자 에이전트 12-4
요청의 사용자 위치 12-4
요청의 서브넷 12-4
요청의 프로토콜 12-3
요청의 프록시 포트 12-3
아카이브
로그 파일 압축 21-9, 21-12
롤오버 설정 21-8, 21-12
보고서 18-9
악성코드
스캐닝 구성 13-8
*안티멀웨어*도 참조
악성코드 판정
다중 13-5
안전 검색
시행 9-15
안티멀웨어
L4 트래픽 모니터에 대한 규칙 20-2
개요 13-4
구성 13-8
데이터베이스 13-13
스캐닝 판정 21-40

아웃바운드 스캐닝 12-1
액세스 로그 파일 13-14
안티멀웨어 규칙
L4 트래픽 모니터 20-2
안티멀웨어 보고서 19-5
안티멀웨어 스캐닝
아웃바운드 12-1
알려진 악성코드 주소
정의됨 20-2
알려진 허용 주소
정의됨 20-2
알림
심각도 22-14
암호 해독
HTTPS 트래픽 11-2
우회 A-8
암호 해독 정책 9-5
개요 11-2
기록 A-12
모니터링 조치 11-2
및 URL 카테고리 변경 9-5
사용 11-3
암호 해독 우회 A-8
제어 설정 11-4
차단 11-9
트래픽 삭제 11-1
트래픽 암호 해독 11-1
트래픽 제어 11-4
트래픽 통과 11-1
암호 해독 정책 그룹
정책 그룹도 참조
압축
로그 파일 아카이브 21-9, 21-12
애플리케이션
대역폭 제한 구성 15-8
정의됨 15-3
차단 15-5
애플리케이션 가시성 보고서
개요 19-5
애플리케이션 동작
정의됨 15-3
애플리케이션 유형
대역폭 제한 구성 15-7
대역폭 제한 재지정 15-7
정의됨 15-3
애플리케이션 제어
개요 15-1
구성 15-3, 15-5
기록 15-9
대역폭 15-6
보고 15-9
보고서 19-5
애플리케이션 15-3
애플리케이션 동작 15-3
애플리케이션 유형 15-3
인스턴트 메시징 트래픽 15-8
액세스 로그
헤더 형식 지정자 21-38
액세스 로그 파일
*W3C 액세스 로그*도 참조
ACL 결정 태그 21-17
nc(no category) 21-21
ns(no score) 21-21
URL 카테고리 약어 9-23
개요 21-14
결과 코드 21-16
액세스 정책 9-5
URL 필터 10-9
및 URL 카테고리 변경 9-5
요청의 서브넷 4-19
요청의 시간 4-19
요청의 프록시 포트 4-19
웹 평판 구성 13-12
어플라이언스 구성
기능 사용 22-4
네트워크 인터페이스 2-15
보고 18-1
보고서 예약 18-7

브라우저 요건 1-3
안티멀웨어 13-8
어플라이언스 설치
워크시트 설정 2-6
어플라이언스 편집
동시 편집 1-3
언어
사용자 기본 설정 22-11
사용자당 기본값 정의 22-11
업그레이드
로컬 업그레이드 서버에 대한 요건 22-31
사용 가능 22-28
업그레이드 설정 구성 22-32
원격 22-30, 22-31
업데이트
개요 22-32
수동 업데이트 22-28, 22-29
업로드
루트 인증서 11-3
인증서 파일 11-7
업스트림 프록시
파일 평판 14-8
온박스 알림 페이지
개요 17-5
외부 DLP 서버
DLP 서버 참조
외부 DLP 정책
구성 16-11
구성원 자격 16-4
기록 16-12
로드 밸런싱 16-10
생성 16-5
외부 DLP 서버 정의 16-9
요청의 URL 카테고리 16-6
요청의 사용자 에이전트 16-6
요청의 사용자 위치 16-6
요청의 서브넷 16-6
요청의 프로토콜 16-5
요청의 프록시 포트 16-6
최소 요청 크기 16-2
외부 DLP 정책 구성원 자격 평가
클라이언트 요청 매칭 16-4
외부 데이터 유출 방지
및 URL 카테고리 변경 9-5
우회
암호 해독 A-8
우회검사에서 업로드 요청 16-2
원격 업그레이드 22-30, 22-31
웹 브라우저
지원됨 1-3
웹 사이트 보고서 19-4
웹 인터페이스
브라우저 요건 1-3
탐색 1-3
웹 평판 필터
데이터베이스 13-13
보고서 19-7
액세스 로그 파일 13-14
액세스 정책 구성 13-12
작동 방식 13-3
점수 13-2
정보 13-2
웹 프록시
개요 4-17
유효하지 않은 인증서
처리 11-9
유효하지 않음
서명, 리프 인증서 11-9
이 문서에 대한 피드백, 보내기 C-3
익명 처리
보고서에서 사용자 18-1
인스턴트 메시징 트래픽
제어 15-8
인식되지 않는 루트 인증 기관
유효하지 않은 인증서 11-9
인식되지 않음
루트 인증 기관/발급자 11-9

인증서
FIPS 22-21
HTTPS 프록시용 CSR 11-8
SaaS용 ID 공급자의 CSR 7-3
검증 11-6
웹 인터페이스용 CSR 22-27
유효하지 않음 11-9
자체적으로 생성 및 서명 22-27
인증서 파일
업로드 11-7
지원되는 형식 11-6
일치하는 클라이언트 요청
아웃바운드 악성코드 스캐닝 정책 12-2

ㅈ

잘못 분류된 URL
URL 제출 툴 9-3
보고 17-6
잘못 분류된 URL 보고 17-6
전달 방법
L2 2-24
전역 ID 6-1
정규식
URL 필터에서 사용 9-20
개요 9-20
정의
사용자 기본 설정 22-11
정책 그룹
맞춤형 URL 카테고리 9-14
암호 해독 정책 11-1
정책 그룹 구성원 자격 정의
아웃바운드 악성코드 스캐닝 정책 12-2
정책 그룹 구성원 정의
Cisco IronPort 데이터 보안 정책 16-4
외부 DLP 정책 16-4
제로 데이 폐기
정의됨 7-1
제어 설정
암호 해독 정책 11-4
주소
모호한 주소 20-2
알려진 악성코드 주소 20-2
알려진 허용 주소 20-2
지원되는 언어
기본값 구성 22-11

ㅊ

차단
AVC 엔진으로 인한 업로드 요청 15-3
HTTPS 트래픽 11-9
URL 카테고리 16-7
개체 16-8
기본적으로 모든 트래픽 2-12
사용자 경험 12-1, 15-3, 16-2
성인 콘텐츠 9-15
악성코드로 인한 업로드 요청 12-1
애플리케이션 15-5
업로드 요청 16-2
최종 사용자 URL 카테고리 페이지
구성 17-9
사용자에게 경고 9-18
최종 사용자 승인 페이지
FTP 요청 17-3
HTTPS 요청 17-3
개요 17-2
구성 17-3
최종 사용자 알림 페이지
HTML 태그 17-10
네이티브 FTP 17-9
맞춤화 17-12
변수 17-12
사용자 정의 알림 페이지 17-6
온박스 알림 페이지 17-5
텍스트 형식 지정 17-10
토큰 17-12

추가
WCCP 서비스 2-22
로그 서브스크립션 21-7

ㅋ

카테고리 필터링
데이터베이스 9-4
캐싱 13-14
커뮤니티 문자열
SNMP 22-35
콘텐츠 필터링
Cisco IronPort 데이터 보안 정책 16-8
쿼리
외부 인증 5-19
클라우드의 파일 분석 결과 세부사항에 대한 어플라이언스의 그룹화 14-9
클라우드 커넥터
인증 실패 3-8
클라이언트 서명 필요 5-13, 5-15
클라이언트 악성코드 위험 19-6
클라이언트 악성코드 위험 보고서 19-6
클라이언트 악성코드 위험 보고서 페이지 19-6
클라이언트 요청 매칭
Cisco IronPort 데이터 보안 정책 16-4
외부 DLP 정책 16-4
키
개요 22-4
키 파일
지원되는 형식 11-6

ㅌ

탐색
웹 인터페이스 1-3
토큰
변수 참조
투명 리디렉션 2-24
L2 전달 방법 2-24
WCCP 서비스 2-22
WCCP 서비스 추가 2-22
개요 2-22
투명 모드
투명 리디렉션 2-22
트래픽 리디렉션
기록 및 보고 9-17
트래픽 삭제
암호 해독 정책 11-1
트래픽 차단
기본적으로 시스템 설정 마법사에서 2-12
트래픽 통과
암호 해독 정책 11-1
트랜잭션 결과 코드 21-16

ㅍ

파일 분석 14-1
파일 평판 필터링 14-1
패킷 캡처
개요 A-23
시작 A-23
페일오버
DLP 서버 16-10
편집
WCCP 서비스 2-22
평판 필터링
파일 14-1
포트
Cisco IronPort 데이터 보안 정책 16-6
아웃바운드 악성코드 스캐닝 정책 12-3
액세스 정책 4-19
외부 DLP 정책 16-6
프로토콜
Cisco IronPort 데이터 보안 정책 16-5
아웃바운드 악성코드 스캐닝 정책 12-3
외부 DLP 정책 16-5
프록시
웹 프록시 참조

프록시 버퍼 메모리 19-13
프록시에 대한 포트
HTTPS 11-3
필터링
Cisco IronPort 데이터 보안 정책의 데이터 16-8
성인 콘텐츠 9-15
웹 평판 16-8
카테고리 10-9, 16-7

ㅎ

하드웨어 문제, 트러블슈팅 A-7
하드 전원 초기화 22-5
헤더
맞춤형 21-38
형식 지정
최종 사용자 승인 페이지 17-10
최종 사용자 알림 페이지 17-10
호스트 이름
변경 2-28
화이트리스트 주소
알려진 허용 주소 참조
회귀 판정 14-14
휴리스틱 분석
McAfee 스캐닝 엔진 13-6