로그 파일을 CTA 시스템에 업로드하도록 WSA 구성

최종 업데이트: 2016년 4월 18일

목차

표기 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표시
굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은** 글꼴로 표시합니다.
기울임꼴 글꼴	문서 제목, 새로운 용어 또는 강조된 용어 및 사용자가 값을 제공해야 하는 인수는 *기울임꼴* 글꼴로 표시됩니다.
[ ]	대괄호로 묶인 요소는 선택적 요소입니다.
{x | y | z }	필수 대체 키워드는 중괄호로 묶고 세로 선으로 구분합니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶고 세로 선으로 구분합니다.
문자열	따옴표 없는 문자의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그렇지 않으면 따옴표도 문자열에 포함됩니다.
courier 글꼴	시스템에서 표시되는 터미널 세션 및 정보는 courier 글꼴로 표시합니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 행을 나타냅니다.

참고: *독자가 참고해야 하는 내용*을 의미합니다. 참고에는 유용한 제안이나 해당 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.

주의: ***독자가 주의해야 하는 항목*을 의미합니다. 이 경우, 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 합니다.**

경고: 중요한 안전상의 지침

위험을 의미합니다. 부상이 발생할 수 있는 상황입니다. 장비를 작동하기 전에 전기 관련 재해에 유의하고 사고 예방을 위해 표준 절차를 숙지하십시오. 각 경고의 끝에는 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾을 수 있도록 명령문 번호가 제공됩니다.

이 지침을 반드시 숙지하십시오.

규정: 추가 정보가 제공되어 있으며 규정 및 고객 요구 사항을 준수해야 합니다.

소개

이 문서는 로그 파일을 Cisco CTA(Cognitive Threat Analytics) 시스템에 업로드할 수 있도록 Cisco WSA(Web Security Appliance)를 구성하는 방법에 대해 설명합니다. 로그 파일을 시스템에 업로드하면 CTA에서 해당 데이터를 분석하고 CTA 포털에 결과를 보고합니다.

사전 요구 사항

요구 사항

Cisco ScanCenter는 Cisco Cloud Web Security의 관리 포털입니다. 먼저 Cisco ScanCenter에서 WSA에 대한 디바이스 어카운트를 만들어야 합니다.

- Cisco ScanCenter에 로그인합니다.
- **Threats(위협)** 탭을 클릭합니다.
- 페이지의 오른쪽 상단 모서리에 있는 Global Settings(전역 설정) 메뉴 아이콘을 클릭합니다.
- **Device Accounts(디바이스 어카운트)**를 클릭합니다.
- 업로드 방법으로 **Automatic(자동)**을 선택합니다.

자세한 내용은 Cisco ScanCenter 관리자 가이드의 "Proxy Device Uploads(프록시 디바이스 업로드)" 섹션을 참조하십시오.

디바이스 어카운트가 생성되면 Cisco ScanCenter의 Add Device Account(디바이스 어카운트 추가) 페이지에서 이 정보를 복사하여 WSA 컨피그레이션에 붙여넣습니다.

- SCP 호스트: `etr.cloudsec.sco.cisco.com`
- 프록시 디바이스에 대해 생성된 디바이스 사용자 이름은 대/소문자를 구분하며, 프록시 디바이스마다 다릅니다.

WSA의 경우 다음이 필요합니다.

- WSA의 호스트 이름 또는 IP 주소
- WSA의 관리자 사용자 비밀번호(기본 비밀번호는 `ironport`)

- WSA는 추가 프록시 업스트림 없이 인터넷에 직접 연결해야 합니다.
- 포트 22를 사용하여 WSA 관리 인터페이스와 SCP 호스트 etr.cloudsec.sco.cisco.com 사이의 네트워크 연결이 이루어져야 합니다. 이 연결을 허용하려면 방화벽 규칙을 조정해야 할 수 있습니다.

주의: 이 설명서에 있는 정보는 랩 환경의 디바이스를 바탕으로 작성한 것입니다. 네트워크가 실행 중인 경우, 모든 컨피그레이션 명령으로 인한 잠재적 영향을 미리 숙지하시기 바랍니다.

사용된 구성 요소

이 문서의 정보는 다음 소프트웨어 버전에서 테스트되었습니다.

- WSA 8.5.1 GD
- WSA 8.0.8
- WSA 7.7.5

이 문서의 정보는 다음 하드웨어에서 테스트되었습니다.

- WSA S100V
- WSA S160
- WSA S300V

구성

프록시 구성

1. 웹 브라우저에서 WSA(http://wsa_*hostname*:8080/)를 가리키도록 합니다.
2. 필요한 경우, 비보안 HTTPS 인증서를 수락하여 계속 진행합니다.
3. admin으로 로그인합니다.
4. **System Administration(시스템 관리)** > **Log Subscriptions(로그 서브스크립션)**로 이동합니다.
5. **Add Log Subscription(로그 서브스크립션 추가)**을 클릭합니다.
6. **Log Type(로그 유형)** 풀다운 메뉴에서 **W3C Logs(W3C 로그)**를 선택합니다.
7. **Log Name(로그 이름)** 필드에 로그 디렉토리를 설명하는 이름을 입력합니다.
8. **Selected Log Fields(선택한 로그 필드)** 상자의 모든 항목을 선택하고 **Remove(제거)**를 클릭하여 선택한 Log Fields(로그 필드)를 제거합니다.

9. **Custom Fields(맞춤설정 필드)** 상자에 다음 항목을 입력하되, 줄바꿈을 사용하여 각 항목을 구분합니다.

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

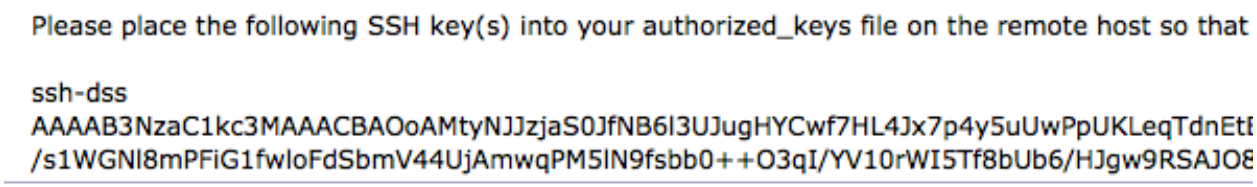
   참고: WSA 버전 7.7.5에서는 AMP가 지원되지 않으므로, "`x-amp`" 필드 4개를 추가하지 마십시오.

10. 모든 항목을 입력한 후 **Add >>(추가 >>)**를 클릭합니다.
11. **Rollover by File Size(파일 크기별로 롤오버)** 필드에 `500M`를 입력합니다.
12. **Rollover by Time(시간별로 롤오버)** 풀다운 메뉴에서 **Custom Time Interval(시간 간격 맞춤설정)**을 선택합니다.
13. **Rollover every(롤오버 간격)** 필드에서 예로 `55m`를 입력합니다.

프록시 뒤의 사용자 수	권장 업로드 기간
알 수 없음 또는 2000 미만	55분
2000 ~ 4000	30분
4000 ~ 6000	20분
6000 이상	10분

14. **File Name(파일 이름)** 필드에 `w3c_log`를 입력합니다.
15. **Log Compression(로그 압축)**을 선택하여 압축을 사용합니다.
16. **Retrieval Method(검색 방법)**로 **SCP on Remote Server(원격 서버에서 SCP)**를 선택합니다.

17. **SCP Host(SCP 호스트)** 필드에 Cisco ScanCenter에 제공된 SCP 호스트를 다음 예처럼 입력합니다. `etr.cloudsec.sco.cisco.com`
18. **SCP Port(SCP 포트)** 필드에 `22`를 입력합니다.
19. **Directory(디렉토리)** 필드에 `/upload`를 입력합니다.
20. **Username(사용자 이름)** 필드에 Cisco ScanCenter의 디바이스에 대해 생성된 사용자 이름을 입력합니다. 디바이스 사용자 이름은 대/소문자를 구분하며 각 프록시 디바이스마다 다릅니다.
21. **Enable Host Key Checking(호스트 키 확인 활성화)** 체크 박스를 선택하고 **Automatically Scan(자동으로 검사)** 라디오 버튼을 선택합니다.
22. **Submit(제출)**를 클릭합니다.
23. WSA Management Console에 공용 SSH 키가 표시됩니다. 맨 앞의 "ssh-dss"를 포함한 전체 키를 복사하여 Cisco ScanCenter의 디바이스 어카운트에 붙여넣습니다. 프록시 디바이스와 CTA 시스템 간에 인증이 성공하면 프록시 디바이스의 로그 파일을 CTA 시스템에 업로드하여 분석할 수 있습니다.



24. **Commit Changes(변경 커밋)**를 클릭합니다.

    주의: 이러한 변경 사항을 처리하려면 변경 사항을 커밋한 후 프록시 프로세스를 재시작해야 합니다. 이렇게 하면 서비스가 잠시 중단될 수 있습니다. 또한 인증 캐시가 지워지며, 사용자에 따라서는 재인증이 필요할 수 있습니다. 업무 시간에 사용자에게 영향을 주지 않으려면 근무 외 시간인 유지 관리 기간에 WSA를 구성하는 것이 좋습니다.

New Log Subscription

Log Subscription

Log Type: W3C Logs

Log Name: w3clogs

(will be used to name the log directory)

Log Fields:

Available Log Fields

CMF
DCF
bytes
c-ip
c-port
cs(Cookie)
cs(Referer)
cs(User-Agent)
cs(X-Forwarded-For)
cs-auth-group
cs-auth-mechanism
cs-bytes
cs-method
cs-mime-type
cs-uri
cs-url

Add >>

Selected Log Fields

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

Custom Fields

(Use line breaks to separate multiple entries)

Rollover by File Size: 500M Maximum

(Add a trailing K or M to indicate size units)

Rollover by Time: Custom Time Interval

Rollover every: 55m

(Example: 120s, 5m 30s, 4h, 2d)

File Name: w3c_log

Log Compression: Enable

Log Exclusions (Optional):

(Enter the HTTP status codes of transactions that should not be included in the W3C Log)

Retrieval Method:

FTP on prg5-wsa-s160.cisco.com

Maximum Number of Files: 100

FTP on Remote Server

FTP Host:

Directory:

Username:

Password:

SCP on Remote Server

SCP Host: etr.cloudsec.sco.cisco.com SCP Port: 22

Directory: /upload

Username: d111...

Enable Host Key Checking

Automatically Scan

Enter Manually

Active Directory에 연결하여 사용자 이름 확인

로그 서브스크립션을 만들기 위해 Active Directory를 설정할 필요는 없으며, 이미 구성되어 있을 수 있습니다. 그러나 이러한 설정은 영향을 받은 디바이스를 파악하는 데 도움이 됩니다. CTA 시스템에서 사용자 이름을 보려면 WSA에서 모든 사용자를 인증할 수 있어야 합니다. 이는 Transparent User Identification(투명한 사용자 식별) 기능을 사용하여 구현할 수 있습니다. 자세한 내용은 Cisco Web Security Appliances 사용 설명서의 5장 "Acquire End-User Credentials(최종 사용자 자격 증명 얻기)"를 참조하십시오.

1. **Network(네트워크)** > **Authentication(인증)**으로 이동합니다.
2. Active Directory에 연결하는 Realm(영역)을 추가합니다.
    a. **Active Directory Server(Active Directory 서버)**는 호스트 이름이 아닌 도메인의 이름입니다.
    b. **Active Directory Domain(Active Directory 도메인)**은 대문자로 표시되는 도메인 이름입니다.
    c. **Join Domain(도메인 참여)**을 클릭한 후 도메인 관리자 권한을 보유한 사용자의 자격 증명을 입력하면 WSA에서 Active Directory에 고유한 사용자를 만듭니다.
    d. **Enable Transparent User Identification using Active Directory(Active Directory 에이전트를 사용하여 투명한 사용자 식별 활성화)** 에이전트를 클릭합니다. 실행 중인 Cisco Active Directory 에이전트가 있어야 하며, Active Directory에 연결할 수 있어야 합니다. 해당 서버 호스트 이름 및 공유 암호를 입력합니다.
3. **Web Security Manager** > **Identities(ID)**로 이동합니다.
4. **Global Identity Policy(전역 ID 정책)**를 수정합니다. **Identification and Authentication to Identify Users Transparently(사용자를 투명하게 식별하기 위한 식별 및 인증)**를 설정하고 이전 단계에서 만든 영역을 선택합니다.
5. **Network Authentication Global Authentication Settings(네트워크 인증 전역 인증 설정)**에서 **Edit Global Settings(전역 설정 수정)**를 클릭하고 **Action if Authentication Service Unavailable(인증 서비스를 사용할 수 없는 경우 취할 조치)**을 **Block all traffic if authentication fails(인증이 실패할 경우 모든 트래픽 차단)**로 설정합니다. 이렇게 하면 인증되지 않은 사용자에게 추가되는 "⋆" 표시가 **userid access** 로그 필드에 추가되지 않습니다.

SMA를 사용하여 여러 WSA 구성

Cisco Content SMA(Security Management Appliance)는 여러 WSA 전체의 관리 기능을 중앙 집중화합니다. 그러나 SMA는 로그 업로드를 설정하는 데에는 도움이 되지 않습니다. 컨피그레이션 설정이 WSA마다 다르고 SMA는 W3C 로그를 지원하지 않으므로, 각 WSA를 개별적으로 구성해야 합니다.

배포 시나리오

단일 WSA, 명시적 또는 투명 모드, 단일 라우팅 테이블

- 포트 22에서 CTA 서버에 연결할 수 있는지 확인합니다.
- 라우팅 테이블에서 로그에 사용할 인터페이스를 제어합니다.

단일 WSA, 명시적 모드, 데이터 및 관리 트래픽에 대한 개별 라우팅 테이블

- 포트 22에서 관리 인터페이스를 통해 CTA 서버에 연결할 수 있는지 확인합니다.
- SCP 트래픽은 관리 트래픽으로 간주되며 관리 포트 외부로 나갑니다. 관리 포트가 포트 22에서 CTA 서버에 연결되는지 확인합니다.

업스트림 및 다운스트림 프록시

일반 컨피그레이션:

- 다운스트림 프록시 필수 기능: 인증, URL 필터링
- 업스트림 프록시 필수 기능: 안티 멀웨어 스캐닝
- 클라이언트 → 다운스트림 → 업스트림 → 인터넷
- 데이터 및 관리 트래픽에 대한 개별 라우팅 테이블

이 시나리오에서 다운스트림 프록시에는 사용자 이름과 클라이언트 IP 주소가 있습니다. 단, 필수 필드인 대상 IP 주소는 없습니다. 대상 IP 주소는 항상 업스트림 프록시로 인식되지만, 사용자 이름은 다운스트림 프록시로만 표시됩니다.

이 경우, 다운스트림 프록시의 XFF(X-Forwarded-For) 헤더를 활성화하고 이를 업스트림 프록시에서 평가합니다. 이렇게 하면 업스트림 프록시가 클라이언트 IP 주소로 인식됩니다. 관리 인터페이스를 통해 CTA 서버에 HTTP 로그를 전송하도록 업스트림 프록시를 구성합니다.

다음 단계

Cisco ScanCenter 내에서 디바이스 어카운트를 선택하고 공용 SSH 키를 입력합니다. 자세한 내용은 Cisco ScanCenter 사용 설명서, 릴리스 5.2의 32장 "Proxy Device Uploads(프록시 디바이스 업로드)" 섹션을 참조하십시오.

Q&A

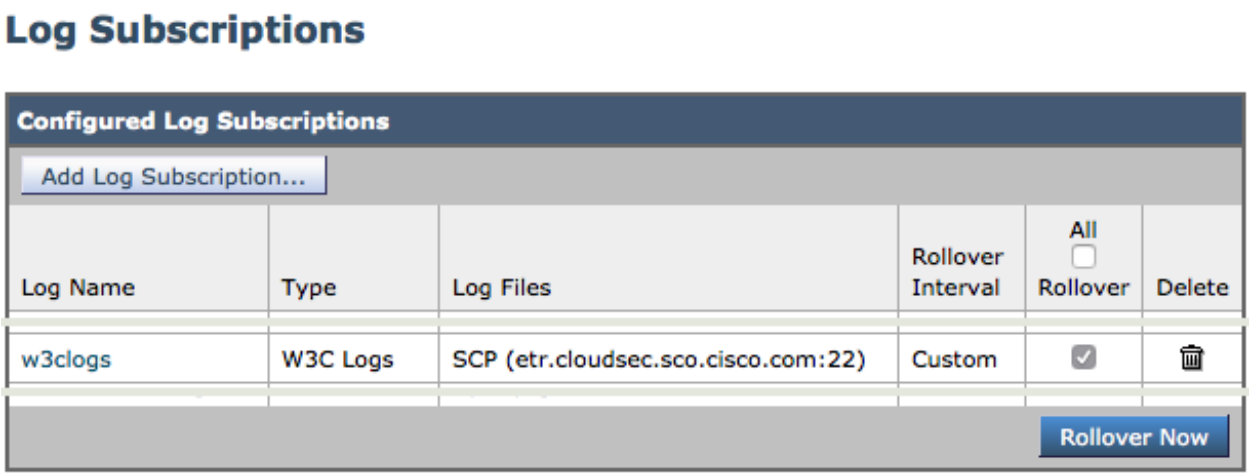
로그를 CTA로 전송하기 전에 익명화할 수 있습니까?

예. 사용자 이름 및 클라이언트 IP는 필수 필드이며 익명화할 수 있습니다. 사용자 이름은 해시 처리되며 향후 참조를 위해 변환 테이블에 매핑이 저장됩니다. 올바른 IP 주소(클라이언트 전용)도 익명화할 수 있습니다.

트러블슈팅

연결을 테스트하려면, WSA에서 즉시 업로드를 시도하도록 실행합니다.

1. **Log Subscriptions(로그 서브스크립션)** 페이지로 이동합니다.
2. 테스트할 서브스크립션에서 **Rollover(롤오버)** 체크 박스를 선택합니다.
3. **Rollover Now(지금 롤오버)** 버튼을 클릭합니다.



연결 확인

다음 단계에 따라 연결을 확인합니다.

1. WSA의 CLI에 로그인합니다.
2. **logconfig** 명령을 입력합니다.
3. **hostkeyconfig** 명령을 입력합니다.
4. **scan** 명령을 입력합니다.
5. CTA 서버 호스트 이름 `etr.cloudsec.sco.cisco.com`을 입력합니다.
6. SSH 프로토콜 유형을 묻는 메시지가 표시되면 **All(모두)**을 선택합니다.
7. CTA 호스트 키를 추가해야 하는지 묻는 메시지가 표시되면 **Y**를 입력합니다.

etr.cloudsec.sco.cisco.com에 대한 RSA 호스트 키를 알 수 없는 경우

텔레메트리 데이터를 업로드하지 않은 경우, WSA 로그를 확인합니다. 다음과 같은 메시지를 받은 경우

"No RSA host key is known for etr.cloudsec.sco.cisco.com and you have requested strict checking. Host key verification failed. Lost connection."

다음 단계에 따라 문제를 해결합니다.

1. WSA의 CLI에 로그인합니다.
2. **logconfig** 명령을 입력합니다.
3. **hostkeyconfig** 명령을 입력합니다.

4. 호스트 키를 삭제합니다.
5. Enter 키를 눌러 메인 CLI로 돌아갑니다.
6. **commit** 명령을 입력합니다.
7. 로그 서브스크립션을 추가하려면 컨피그레이션 단계를 반복합니다. **Enable Host Key Checking(호스트 키 확인 활성화)** 체크 박스를 선택하고 **Automatically Scan(자동으로 검사)** 라디오 버튼을 선택합니다.

문서 가져오기 및 서비스 요청 제출

설명서 받기, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출 및 추가 정보 수집에 대한 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html에서 *What's New in Cisco Product Documentation(Cisco 제품 설명서의 새로운 사항)*을 참조하십시오.

새로 개정된 Cisco 기술 문서를 모두 보여주는 *What's New in Cisco Product Documentation(Cisco 제품 설명서의 새로운 사항)*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 전달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.