Secure Web Appliance에서 요청 디버그 로그 구성

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 디버그 로그를 요청하는 단계에 대해 설명합니다 .

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 CLI(Command Line Interface)에 대한 관리 액세스.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

디버그 로그 요청

SWA의 요청 디버그 로그는 단일 특정 HTTP 또는 HTTPS 트랜잭션 또는 클라이언트 머신에 대한 매우 자세한 엔드 투 엔드 디버그 및 추적 레벨 정보를 캡처하도록 설계된 특수 로그 유형입니다. 여러 요청 전반에 걸쳐 요약된 이벤트를 기록하는 표준 프록시 로그와 달리, 요청 디버그 로그는 특정 요청(예: 인증, URL 필터링, 암호 해독, 악성코드 검사 및 평판 서비스) 처리와 관련된 모든 웹 프록시 모듈의 디버그 출력을 하나의 상관관계가 있는 로그 스트림으로 집계합니다. 이 로그 유형은 심층 진단을 위한 것이며 GUI가 아닌 CLI를 통해서만 생성할 수 있습니다

요청 디버그 로그는 표준 로그에 충분한 세부사항이 없는 복잡한 또는 간헐적인 프록시 문제를 해결할 때 필수적입니다. 관리자와 Cisco TAC는 모든 처리 단계에서 단일 요청이 처리된 방식을 정확하게 추적할 수 있으므로 예기치 않은 정책 일치, 검사 지연, 인증 실패 또는 엔진 간 판정 불일치와 같은 근본 원인을 정확하게 찾아낼 수 있습니다. 로그는 하나의 트랜잭션에 초점을 맞추므로 시스템 전체에 걸쳐 모든 프록시 모듈에서 디버그 로깅을 활성화하여 운영 오버헤드와 성능에 영향을 미치지 않고 최대 가시성을 제공합니다. 그러면 고급 조사 중에 디버그 로그 요청이 정확하고 효율적이며 위험이 낮은 진단 툴이 됩니다.

요청 디버그 로그 구성

1단계. CLI에 로그인하고 logconfig를 실행한 후 new(새로 만들기)를 선택합니다.

2단계. 요청 디버그 로그와 관련된 번호를 선택하고 Enter 키를 누릅니다.

3단계. 로그 이름을 입력합니다.

4단계. 로깅 레벨로 Trace(추적)를 선택합니다.

5단계. 향상된 로깅을 수집하도록 요청한 모듈을 선택합니다. 쉼표로 구분된 목록 또는 범위 목록(예: 1,3,4 또는 3-7)으로 여러 개의 항목을 선택할 수 있습니다.

팁: TAC에서 요청한 특정 모듈이 없는 경우 모든 모듈(예: 1~30)을 선택하는 것이 좋습니다.

6단계. 고급 로깅을 활성화할 요청 수를 지정합니다. 이 수의 요청이 캡처되면 로깅이 자동으로 중지됩니다.

참고: 트러블슈팅 과정에서 트래픽 조건을 기준으로 적절한 값을 선택하는 것이 중요합니다. 예를 들어, 전용 테스트 머신을 사용 중이고 백그라운드 트래픽이 최소화되는 경우, 요청 수가 적으면 충분합니다. 그러나 백그라운드 작업(예: 운영 체제 업데이트, 브라우저 백그라운드 요청 또는 Webex와 같은 애플리케이션)이 더 높은 환경에서는 더 높은 값을 선택하면 관련 트랜

잭션이 캡처됩니다.

7단계. 클라이언트 IP 주소, 대상 IP 주소 또는 대상 도메인을 선택하여 향상된 로깅을 위한 요청 일치 기준을 정의합니다.

참고: 대부분의 경우 클라이언트 IP 주소를 선택하는 것이 좋습니다. 단일 웹 사이트에 대한 액세스를 트러블슈팅하는 경우에도 이 접근 방식은 페이지 로드 중에 생성된 모든 웹 요청을 캡처하며, 추가 URL에 대한 백그라운드 요청은 즉시 표시되지 않을 수 있습니다. 그러나 이 방법은 백그라운드 인터넷 트래픽을 최소화한 전용 테스트 시스템을 사용할 때 가장 효과적입니다. 클라이언트가 상당한 추가 트래픽(예: 운영 체제 업데이트, 브라우저 백그라운드 서비스 또는 Webex와 같은 애플리케이션)을 생성하는 환경에서는 대상 도메인 또는 대상 IP 주소로 필터링하는 것이 좋습니다.

팁: 정확한 오류 지점을 알 수 없는 경우 브라우저 HAR 로그를 수집하여 문제가 있는 특정 URL 또는 도메인(예: 페이지 로드 실패 또는 높은 레이턴시)을 식별하고 디버그 로그 요청 기준에 해당 도메인을 구성할 수 있습니다.

8단계. 로그를 검색할 방법을 선택합니다. FTP Poll을 선택하면 로그가 SWA에 저장됩니다.

9단계. 로그 파일에 사용할 파일 이름을 정의하거나 Enter 키를 눌러 현재 생성된 파일 이름을 적용합니다.

10단계. 정의된 요청 수가 충족된 후 로깅이 중지되므로 시간 기반 로그 파일 롤오버에 대해 No를 선택합니다.

11단계. 최대 파일 크기(바이트)를 정의하거나 Enter 키를 눌러 현재 값을 적용합니다.

팁: 로그 파일 크기를 더 크게 정의하면 로그를 다운로드하고 검토하기가 더 어려워질 수 있습니다. 개별 로그 파일의 크기를 늘리는 대신 로그 파일 수를 늘리는 것이 좋습니다(다음 단계). 이 접근 방식을 사용하면 관리 용이성이 향상되는 동시에 너무 큰 파일을 만들지 않고도 필요한 모든 디버그 정보를 캡처할 수 있습니다.

12단계. 5단계에서 로깅하기 위해 선택한 프록시 모듈의 수 및 7단계에서 정의한 요청 일치 기준에 따라 최대 로그 파일 수를 구성합니다. 적절한 파일 제한을 선택하는 것은 모든 관련 디버그 정보가 로깅을 섣불리 중지하지 않고 캡처되어 로그가 불완전하거나 누락될 수 있음을 보장하기 위해 중요합니다.

13단계. 허용되는 최대 파일 수로 인해 파일이 제거될 때 경고를 보내야 합니까?라는 메시지가 표시되면 No(아니요)를 선택합니다. 이렇게 하면 정상적인 로그 회전 중에 불필요한 경고가 표시되지 않

습니다. 특히 문제 해결을 위해 디버그 로그 요청을 의도적으로 생성할 때 이러한 경고가 표시되지 않습니다.

14단계. Do you want to compress logs (yes/no)?(로그를 압축하시겠습니까(예/아니요)?) 메시지가 표시되면 No(아니요)를 선택합니다. 이렇게 하면 로그 파일의 압축이 해제되어 문제 해결 중에 더 쉽게 검토하고 분석할 수 있습니다.

15단계. Enter를 눌러 마법사를 종료합니다

16단계. commit을 입력하고 Enter를 눌러 변경 사항을 저장합니다

```
SWA_CLI> logconfig

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
55. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[]> new

Choose the log file type for this subscription:
1. ADC Engine Framework Logs
2. ADC Engine Logs
...
[Output removed to simplify readability]
...
53. Request Debug Logs
...
[Output removed to simplify readability]
...
[1]> 53

Please enter the name for the log:
[]> Request_Debug_Logs

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 5

Choose modules where enhanced request logging is to be performed.
Multiple selections can be made in the form of a comma separated or range list (e.g. 1,3,4 or 3-7)
```

```
Choosing the Default Proxy will enable enhanced logging across modules:
1. Default Proxy
2. Access Control Engine
3. Proxy Configuration
4. Disk Manager
5. Memory Manager
6. McAfee Integration Framework
7. Sophos Integration Framework
8. Webroot Integration Framework
9. Webcat Integration Framework
10. Connection Management
11. Authentication Framework
12. HTTPS
13. FTP proxy
14. WCCP Module
15. License Module
16. SNMP Module
17. WBRS Integration Framework
18. Logging Framework
19. Data Security Module
20. Miscellaneous Proxy Modules
21. DCA Engine Framework
22. AVC Engine Framework
23. Cloud Connector
24. SOCKS Proxy
25. Advanced Malware Protection
26. ArchiveScan module in proxy
27. Web Traffic Tap module in proxy
28. Bandwidth Control
29. Http2 proxy
30. ADC Engine Framework
[1]> 1-30

Please enter the number of requests for which to perform enhanced logging:
[1]> 100

Choose the request criteria for logging:
1. Client IP Address
2. Destination Domain
3. Destination IP Address
[1]> 1

Specify source IP address
[]> 10.20.3.15

Choose the method to retrieve the logs:
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 1

Filename to use for log files:
[Request_Debug_Logs.text]>

Do you want to configure time-based log files rollover? [N]>

Please enter the maximum file size:
[10485760]>

Please enter the maximum number of files:
[10]> 50
```

```
Should an alert be sent when files are removed due to the maximum number of files allowed? [N]>

Do you want to compress logs (yes/no)
[n]>

Currently configured logs:
1. "Request_Debug_Logs" Type: "Request Debug Logs" Retrieval: FTP Poll
2. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
3. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
[Output removed to simplify readability]
...
56. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll


SWA_LIC> commit

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
```

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Secure Web Appliance 모범 사례 사용
- Secure Web Appliance 로그 액세스
- Microsoft Server를 사용하여 SWA에서 SCP 푸시 로그 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.