로그 전송을 어떻게 자동화합니까?

목차

질문

로그 전송을 어떻게 자동화합니까?

환경

Cisco ESA(Email Security Appliance), WSA(Web Security Appliance), SMA(Security Management Appliance) 및 모든 버전의 AsyncOS입니다.

보안 어플라이언스에 다양한 유형의 로그가 생성됩니다.어플라이언스에서 자동으로 특정 로그를 다른 서버로 전송하도록 할 수 있습니다.

이 설정은 FTP 또는 SCP 프로토콜을 사용하여 GUI 또는 CLI를 통해 수행할 수 있습니다.아래에서 자세히 알아보십시오.

GUI

1. 시스템 관리 **-> 로그 서브스크립션으로 이동합니다**.
2. 수정할 로그의 로그 이름을 '로그 이름' 필드에서 클릭합니다.
3. '검색 방법'에서 '원격 서버의 FTP' 또는 '원격 서버의 SCP'를 선택할 수 있습니다.
4. 선택한 적절한 시나리오에 올바른 값을 입력합니다.올바른 값을 잘 모르는 경우 시스템/네트워크 관리자에게 문의하여 네트워크에서 사용 가능한 서버를 확인할 수 있도록 도움을 받으십시오.

CLI(명령줄 인터페이스)

다음 CLI 시퀀스를 참조하십시오.

```
S-Series> logconfig
```

```
[]> edit
[]> <appropriate number correlating to the log you wish to modify>

Please enter the name for the log:
[Log_name]> <enter for default>

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

[3]> <enter for the default>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
```

설정할 방법을 선택합니다.이 시점부터 CLI는 GUI에서 사용할 수 있는 동일한 연결 설정을 안내합니다.

이는 다음과 같습니다.

FTP

- 전송 사이의 최대 시간 간격:3600초
- FTP 호스트: FTP 서버의 호스트 이름/IP 주소
- 디렉터리: FTP 서버의 원격 디렉토리(FTP 로그온에 상대적)일반적으로 '/')
- 사용자 이름: FTP 사용자 이름
- 암호: FTP 암호

SCP

- 전송 사이의 최대 시간 간격:3600초
- 프로토콜: SSH1 또는 SSH2
- SCP 호스트: SCP 서버의 호스트 이름/IP 주소
- 디렉터리: SCP 서버의 원격 디렉터리(SCP 로그온에 상대적)일반적으로 '/')
- 사용자 이름: SCP 사용자 이름
- 호스트 키 확인 사용
- 자동 스캔
- 수동으로 입력

참고:FTP는 일반 텍스트 프로토콜로서, 네트워크 트래픽을 탐지하는 일부 사용자가 민감한 데이터를 읽을 수 있습니다.SCP는 암호화된 프로토콜이므로 스누핑 데이터에서 스니핑이 비효율적입니다.데이터가 민감하고 보안이 중요한 경우 FTP 대신 SCP를 사용하는 것이 좋습니다.