ESA FAQ:ESA에서 간헐적인 메일 전달 문제를 어떻게 분석합니까?

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 간헐적인 메일 전달 문제를 분석하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS

사용되는 구성 요소

이 문서의 정보는 모든 버전의 AsyncOS를 기반으로 합니다.

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

ESA에서 간헐적인 메일 전달 문제를 어떻게 분석합니까?

ESA와 인바운드 서버 연결 간의 전체 SMTP(Simple Mail Transfer Protocol) 대화를 추적하기 위해 수신 디버그 로그를 사용할 수 있습니다.Injection Debug Logs(수신 디버그 로그) 내의 각 행은 SMTP 대화 중에 전송 및 수신된 데이터를 간략하게 설명합니다.

GUI에서 수신 디버그 로그를 활성화하려면 다음 단계를 완료하십시오.

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

2. **로그 구독 추가...를 선택합니다.**.

3. Log Type(로그 유형) 필드에서 **Injection Debug Logs(수신 디버그 로그**)를 선택하고 적절한 데이터를 입력합니다.

주입 디버그 로그 데이터&콜론을 입력할 때 고려해야 할 몇 가지 중요한 사항은 다음과 같습니다.

- **10.1.1.0/24**과 같은 CIDR 주소가 허용됩니다.
- **10.1.1.10-20**과 같은 IP 주소 범위가 허용됩니다.
- **10.2.3**과 같은 IP 서브넷이 허용됩니다.
- 호스트 이름 및 와일드카드(예: **crm.example.com**)가 허용됩니다(**example.com**은 제외).
- 와일드카드는 **.example.com**(별표 없음)으로 표시되어야 합니다.
- 인바운드 이메일을 추적할 때 호스트 이름은 발신자 호스트와 일치해야 합니다.
- 아웃바운드 이메일을 추적할 때 호스트 이름이 내부 호스트 이름과 일치해야 합니다.
- SMTP 세션 수는 1에서 25 사이여야 합니다.

CLI에서 수신 디버그 로그를 활성화하려면 다음 단계를 완료하십시오.

1. CLI에 logconfig **> new** 명령을 입력합니다.

2. Injection **Debug Logs를 선택합니다**.

3. debugging_**example**과 같은 로그 이름을 **입력합니다**.

4. **mail1.example.com**과 같이 주입 디버그 정보를 기록할 IP 주소의 호스트 이름, IP 주소 또는 블록**을 입력합니다**.

5. 이 도메인에 대해 기록할 SMTP 세션 수를 입력합니다.값이 1에서 25 사이여야 합니다.

6. 로그를 검색하는 데 사용할 방법(예: **FTP 폴링)을 입력합니다**.

7. 파일 이름을 입력합니다.원하는 경우 기본 파일 이름을 사용할 수 있습니다.

8. 남아 있는 기본값을 선택합니다.

이 예에서는 ESA가 서버의 메일을 수락하는 경우 수신 디버그 로그를 보여줍니다.

> **참고:**수신 디버그 로그 및 도메인 디버그 로그는 mail_logs와 유사하므로 grep 및 **tail** 명령을 사용할 수 있습니다.

```
Sent to '10.251.21.203': '220 ironportappliance ESMTP\r\n'
Rcvd from '10.251.21.203': 'EHLO outgoing.example.com\r\n'
Sent to '10.251.21.203': '250-nibbles.run\r\n250-8BITMIME\r\n250
 SIZE 104857600\r\n'
Rcvd from '10.251.21.203': 'MAIL FROM:<jsmith@example.com>\r\n'
Sent to '10.251.21.203': '250 sender <jsmith@example.com> ok\r\n'
Rcvd from '10.251.21.203': 'RCPT TO:<test@example.org>\r\n'
Sent to '10.251.21.203': '250 recipient <test@example.org>ok\r\n'
Rcvd from '10.251.21.203': 'DATA\r\n'
Sent to '10.251.21.203': '354 go ahead\r\n'
Rcvd from '10.251.21.203': 'To: "test@example.org" <test@example.org>
 \r\nSubject: 12:14pm - test\r\nFrom: Hotel_Users <jsmith@example.com>
 \r\nContent-Type: text/plain; format=flowed; delsp=yes;
 charset=iso-8859-15\r\nMIME-Version: 1.0\r\nContent-Transfer-Encoding:
 7bit\r\nDate: Tue, 09 Jan 2007 12:14:35 -0800\r\nMessage-ID:
 <op.tlwk6lvgwomlp4@outgoing.example.com>\r\nUser-Agent: Opera Mail/9.10
 (Win32)\r\n\r\ntest\r\n'
Rcvd from '10.251.21.203': '\r\n.\r\n'
Sent to '10.251.21.203': '250 ok: Message 270 accepted\r\n'
Rcvd from '10.251.21.203': 'QUIT\r\n'
Sent to '10.251.21.203': '221 nibbles.run\r\n'
```