메일 수신 및 전달 중 간헐적인 문제 및 중단된 연결 문제 해결

목차

소개

이 문서에서는 메일을 수신하고 전달하는 동안 간헐적인 문제 및 중단된 연결을 해결하는 방법에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco PIX(Private Internet eXchange) 또는 ASA(Adaptive Security Appliance) 버전 7.x 이상
- Cisco ESA(Email Security Appliance)

배경 정보

Cisco ESA 이메일 게이트웨이는 기본적으로 이메일 방화벽입니다.따라서 Cisco PIX 또는 ASA와 같은 업스트림 방화벽이 ESA에서 주고받는 메일 트래픽을 검사할 필요가 없습니다.모든 보안 어플라이언스 호스트 주소에 대해 방화벽에서 ESMTP(Extended Simple Mail Transfer Protocol) 애플리케이션 검사 기능을 비활성화하는 것이 좋습니다.기본적으로 ESMTP 프로토콜 검사는 Cisco 방화벽을 통과하는 모든 연결에 대해 활성화됩니다.즉, TCP 포트 25와 개별 메시지 헤더를 통해 메일 게이트웨이 간에 실행된 모든 명령이 RFC의 821, 1123 및 1870을 포함하는 RFC(Request for Comments) 사양을 엄격하게 준수하도록 분석됩니다.ESA로 송수신되는 문제를 일으킬 수 있는 최대 수신자 수 및 메시지 크기에 대한 기본값이 정의되어 있습니다.이러한 특정 컨피그레이션 기본값은 여기에 설명되어 있습니다(Cisco Command Lookup Tool에서 가져옴).

inspect **esmtp** 명령은 이전에 fixup smtp 명령에서 제공한 기능을 포함하며 일부 ESMTP 명령에 대한 추가 지원을 제공합니다.ESMTP 애플리케이션 검사는 AUTH, EHLO, ETRN, HELP, SAML,

SEND, **SOML** 및 VRFY를 포함한 8개의 ESMTP 명령에 대한 지원을 추가합니다.7개의 RFC 821 명령(**DATA**, **HELO**, **MAIL**, **NOOP**, **QUIT, RCPT, RSET)을** 지원하는 **동시에 보안 어플라이언스는 총 15개의 SMTP 명령을 지원합니다.**ATRN, **STARTLS**, **ONEX**, **VERB**, CHUNKING **및 전용 확장과** 같은 기타 ESMTP 명령은 **지원되지 않으며 지원되지 않습니다.**지원되지 않는 명령은 Xs로 변환되며 내부 서버에서 이를 거부합니다.이렇게 하면 **500 명령 알 수 없음**과 같은 메시지가 **표시됩니다 .XXX**.불완전한 명령은 삭제됩니다.

inspect **esmtp** 명령은 서버 SMTP 배너의 문자를 별표로 변경합니다. 단, "2", "0", "0" 문자는 예외입니다.캐리지 리턴(CR) 및 LF(linefeed) 문자는 무시됩니다.SMTP 검사가 활성화되면 인터랙티브 SMTP에 사용되는 세션이 유효한 명령을 기다리고 방화벽 esmtp 상태 시스템은 이러한 규칙이 관찰되지 않을 경우 세션에 대한 올바른 상태를 유지합니다.

- SMTP 명령의 길이는 4자 이상이어야 합니다.
- SMTP 명령은 캐리지 리턴 및 라인 피드로 종료해야 합니다.
- SMTP 명령은 다음 응답을 실행하기 전에 응답을 기다려야 합니다.

SMTP 서버는 숫자 응답 코드 및 사용자가 읽을 수 있는 문자열(선택 사항)을 사용하여 클라이언트 요청에 응답합니다.SMTP 애플리케이션 검사는 사용자가 사용할 수 있는 명령 및 서버가 반환하는 메시지를 제어하고 줄입니다.SMTP 검사는 3가지 기본 작업을 수행합니다.

- SMTP 요청을 7개의 기본 SMTP 명령과 8개의 확장 명령으로 제한합니다.
- SMTP 명령 응답 시퀀스를 모니터링합니다.
- 감사 추적을 생성합니다.메일 주소에 포함된 잘못된 문자가 교체될 때 감사 레코드 108002가 생성됩니다.자세한 내용은 RFC 821을 참조하십시오.

SMTP 검사는 다음과 같은 비정상적인 서명에 대한 명령 및 응답 시퀀스를 모니터링합니다.

- 잘린 명령입니다.
- 잘못된 명령 종료(<CR><LR>으로 종료되지 않음).
- PCI Express(PIPE) 서명에 대한 PHY 인터페이스가 **MAIL** from 또는 RCPT to 명령의 매개변수로 발견되면 세션이 닫힙니다.사용자가 구성할 수 없습니다.
- SMTP 서버에 의한 예기치 않은 전환.
- 알 수 없는 명령의 경우 보안 어플라이언스는 패킷의 모든 문자를 **X**로 변경합니다. 이 경우 서버는 클라이언트에 오류 코드를 생성합니다.패킷의 변경 때문에 TCP 체크섬을 다시 계산하거나 조정해야 합니다.
- TCP 스트림 편집.

show service-policy inspect ESMTP의 출력은 기본 검사 값과 해당 작업을 제공합니다.

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
```

```
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

문제

Cisco ESA에서 메시지를 올바르게 전달하거나 수신하지 못하는 경우가 있습니다.다음 메시지 중 하나 이상이 Cisco ESA 디바이스 mail_logs에 표시됩니다.

- 메시지 중단 MID XXX
- 수신 중단된 ICID 21916이 손실됨
- ICID 21916 닫기
- 연결 오류:DCID:XXX 도메인:example.com IP:10.1.2.3 포트:25 세부 정보:[오류 60] 작업 시간 초과 인터페이스:10.10.10.1 이유:네트워크 오류

솔루션

이러한 기본 설정 중 일부는 TLS(Transport Layer Security) 암호화 메시지 전달, 메일 목록 캠페인, 문제 해결과 같은 항목에 영향을 줄 수 있습니다.더 나은 정책에서는 방화벽을 사용하여 먼저 보안 어플라이언스를 통과하지 않는 나머지 이메일 트래픽을 모두 검사하는 동시에, 있는 모든 트래픽을 제외시키는 것입니다.이 예에서는 단일 보안 호스트 주소에 대해 ESMTP 애플리케이션 검사를 제외하도록(앞에서 설명한) 기본 컨피그레이션을 조정하는 방법을 보여 줍니다.

MPF(Modular Policy Framework) 클래스 맵에서 참조할 수 있도록 Cisco ESA의 내부 주소를 오가는 모든 트래픽을 정의할 수 있습니다.

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

이렇게 하면 다르게 처리할 트래픽을 구체적으로 매칭하거나 선택하는 새로운 클래스 맵이 생성됩니다.

```
class-map ironport_esa
match address ironport_esa_internal
```

이 섹션에서는 새 Cisco 클래스 맵을 링크하고 ESMTP 프로토콜 검사 기능을 비활성화합니다.

```
policy-map global_policy
class ironport_esa
no inspect esmtp
```

또한 주소에 대한 수신 및 절반이 열린(원시) 연결 수를 제어하는 데 도움이 되는 주소 변환 명령문을 참고하십시오.이는 DoS(Denial of Service) 공격을 차단하는 데 유용하지만, 전송 속도를 방해할 수 있습니다.

NAT 및 **STATIC** 명령의 매개 변수를 추적하기 위한 형식 ... [tcp (max_conns)] [max_embryonic]. 이 예에서는 총 TCP 연결 50개 및 100개의 절반이 열린 연결 또는 미발달 연결 시도의 제한을 지정합니다.

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```