ESA 및 SMA에서 중앙 집중식 PVO 격리 문제 해결

목차

소개

이 문서에서는 중앙 집중식 정책, 바이러스 및 Outbreak 격리 기능이 활성화된 경우 전달 및 연결 문제를 해결하는 방법에 대해 설명합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ESA(Email Security Appliance) with AsyncOS 8.1 이상
- SMA(Security Management Appliance) with AsyncOS 8.0 이상

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.

배경 정보

PVO(Centralized Policy, Virus and Outbreak) 격리 기능은 AsyncOS 8.0(ESA) / 8.1(SMA)에 도입되었습니다. 이 기능에는 추가적인 네트워크 연결 요구 사항이 있으며, 트러블슈팅에 몇 가지 새로운 문제가 발생합니다.

커뮤니케이션 이해

- CPQ 통신에서는 SMTP를 사용하지만, 메타데이터 전송을 위한 일부 추가 명령이 있습니다.
- SMA는 Centralized Services(중앙 집중식 서비스) -> Policy(정책), Virus and Outbreak Quarantines(정책, 바이러스 및 Outbreak 격리)에 정의된 인터페이스 및 포트에서 연결을 수신합니다. 기본적으로 포트는 7025이지만 관리자 사용자가 이 포트를 변경했을 수 있습니다!

- ESA는 Security Services(보안 서비스) -> Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(Outbreak 격리)에 정의된 인터페이스 및 포트에서 연결을 수신합니다. 기본적으로 포트는 7025이지만 관리자 사용자가 이 포트를 변경했을 수 있습니다!
- 또한 SMA는 SSH(명령 클라이언트를 통해)를 사용하여 ESA에서 컨피그레이션 정보를 가져옵니다. 특히 SMA가 ESA에 릴리스된 이메일을 전달할 때 사용됩니다. SMA는 SSH를 사용하여 ESA 컨피그레이션을 쿼리하고 릴리스된 이메일을 전송할 인터페이스/포트를 결정합니다.

리스너

- ESA와 SMA 모두 지정된 포트에서 수신할 'cpq_listener'라는 숨겨진 리스너를 갖게 됩니다.
- 이러한 리스너는 컨피그레이션 파일에서 볼 수 있습니다. 예:

```
<listener>
     <listener_name>cpq_listener</listener_name>
     <protocol>CPQ</protocol>
     <interface_name>Incoming Mail</interface_name>
     <port>7025</port>
     <listen_queue_size>50</listen_queue_size>
     <type>private</type>
     <hat>
$RELAYED
   RELAY {}
$BLOCKED
   REJECT {}
RELAYLIST:
   10.1.2.3
       $RELAYED (Only select hosts can relay from this box)
ALL
   $BLOCKED (Everyone else)
     </hat>
     <rat>
       <rat_entry>
         <rat_address>ALL</rat_address>
         <access>ACCEPT</access>
       </rat_entry>
     </rat>
```

- 관리자 사용자가 'suspendlisteners all' 또는 'suspend'를 사용하는 경우 이러한 리스너는 일시 중단됩니다. 포트가 연결을 수락하지 않는 경우 시스템 상태가 '오프라인'인지 확인하고 필요한 경우 다시 시작해야 합니다.

ESA에서 SMA로의 전송 문제 해결

- ESA가 구성된 포트 및 인터페이스의 SMA에 연결할 수 있는지 확인합니다. 텔넷을 사용하여 이 작업을 수행할 수 있습니다. 통신이 성공하려면 220개의 배너를 받아야 합니다.
- ESA에는 'the.cpq.host'라는 목적지 객체가 있는데, 이 객체에는 SMA로 전달을 위해 대기하는 동안 메시지가 포함됩니다. 'tophosts' 또는 Monitor(모니터) -> Delivery Status(전달 상태)를 사용하여 이를 확인할 수 있습니다. 'hoststatus'를 함께 사용할 수는 없지만 필요한 경우 'showrecipients' 및 'deleterecipients'를 사용할 수 있습니다.

SMA에서 ESA로의 전송 문제 해결

- SMA가 구성된 포트 및 인터페이스에서 ESA에 연결할 수 있는지 확인합니다. 다시 텔넷을 사용할 수 있으며 성공할 경우 220 배너가 표시됩니다.

- 클러스터를 사용할 때는 Security Services(보안 서비스) -> Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(신종 바이러스 격리)의 클러스터 레벨에서 정의된 인터페이스가 시스템 레벨의 모든 어플라이언스에 대해 존재해야 합니다. (네트워크 -> IP 인터페이스 선택)
- SMA에는 ESA로 전달을 위해 대기열에 있는 동안 릴리스된 메시지를 포함하는 'the.cpq.release.host'라는 대상 객체가 있습니다. 'tophosts'를 사용하여 이를 확인할 수 있습니다. 이는 'hoststatus' 또는 'showrecipients'와 함께 작동하는 것으로 보이지 않으며, 'deleterecipients'와 함께 테스트한 적이 없지만, 이 역시 작동하지 않을 수 있습니다.
- SMA와 ESA 간의 SSH 통신에도 문제가 있을 수 있습니다. 이러한 문제가 항상 네트워크 기반일 필요는 없습니다. 예를 들어 CSCus29647에서 SMA의 내부 구성 요소가 작동하지 않습니다. 이러한 문제는 일반적으로 메일 로그에 애플리케이션 장애로 표시되며, SMA를 재부팅하여 해결할 수 있습니다.

TLS/인증서

- 어느 방향이든 모든 CPQ 연결은 TLS를 사용하며, 따라서 암호화 컨피그레이션이 역할을 수행할 수 있습니다.
- TLS 연결이 성공하려면 연결을 여는 디바이스가 수신 디바이스에서 Cisco의 기존 CPQ 인증서를 사용하고 있는지 확인할 수 있어야 합니다. 어플라이언스가 익명 암호를 협상하는 경우 이 오류가 발생할 수 있습니다. 로그에 다음과 같이 표시됩니다.

```
Mon Apr  1 12:00:00 2014 Info: New SMTP DCID 123456 interface 10.0.0.2 address 10.0.0.1 port
7025
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS failed: verify error: no certificate from
server
Mon Apr  1 12:00:00 2014 Info: DCID 123456 TLS was required but could not be successfully
negotiated
```

- 이 문제는 보내는 배달 암호 목록에서 익명 암호를 제거하기만 하면 해결할 수 있습니다. 암호 목록 끝에 ':-aNULL'을 추가하면 됩니다. 예:높음:보통:**-aNULL**

로그 파일

- SMA에 메일 로그 서브스크립션이 있는 경우(기본적으로 해당) 메일 로그를 검토하여 추가 정보를 수집할 수 있습니다.
- CPQ 수신 이벤트는 SMA로 격리되는 메시지와 ESA로 릴리스되는 메시지 모두에 대해 이렇게 표시됩니다.

```
New CPQ ICID 12345 interface Management (10.10.10.1) address 10.10.20.1 reverse dns host
unknown verified no
```

- grep를 사용하여 이러한 이벤트를 검색할 수 있습니다. 예:grep "CPQ ICID" mail_logs
- ESA에서 격리를 수행하고 SMA에서 격리를 해제하는 CPQ 전달 이벤트는 사용자 지정 포트가 나열되고 일부 라인에는 '중앙 집중식 정책 격리'라는 버전이 포함되어 있다는 점을 제외하고 다른 모든 전달과 유사합니다. 아래 예:

```
Fri Sep 13 15:08:02 2013 Info: New SMTP DCID 12345 interface 10.10.20.1 address 10.10.10.1
port 7025
```

```
Fri Sep 13 15:08:02 2013 Info: DCID 12345 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Fri Sep 13 15:08:02 2013 Info: Delivery start DCID 12345 MID 23456 to RID [0] to Centralized
Policy Quarantine
Fri Sep 13 15:08:02 2013 Info: Message done DCID 12345 MID 23456 to RID [0] (centralized
policy quarantine)
Fri Sep 13 15:08:07 2013 Info: DCID 12345 close
```

- 다음과 같이 grep를 사용하여 포트에 대한 검색을 사용하여 이러한 이벤트를 찾을 수 있습니다 .grep "port 7025" mail_logs

ESA 'Enable' 버튼 사용 안 함

ESA에서 PVO를 활성화하려고 할 때 모든 필수 구성 요소가 완료되었지만 'Enable' 버튼이 회색으로 표시될 수 있습니다.ESA에 PVO 페이지가 표시되면 SMA over port 7025와 통신하여 컨피그레이션을 활성화할 준비가 되었는지 확인합니다. 이 통신이 실패하면 'Enable' 버튼이 비활성화됩니다. ESA의 "포트 7025"에 대한 연결을 통해 ESA -> SMA 포트 7025 통신과 마찬가지로 이 문제를 해결할 수 있습니다.자세한 내용은 관련 정보에 나열된 TechNote를 참조하십시오.

관련 정보

- ESA가 클러스터링된 경우 PVO 마이그레이션 마법사의 요구 사항
- ESA 중앙 집중화 정책, 바이러스 및 PVO(Outbreak Quarantine)를 활성화할 수 없음