

TCPREFUSE 또는 REJECT 액세스 규칙이 작동하는지 확인하려면 어떻게 해야 하나요?

목차

[TCPREFUSE 또는 REJECT 액세스 규칙이 작동하는지 확인하려면 어떻게 해야 하나요?](#)

TCPREFUSE 또는 REJECT 액세스 규칙이 작동하는지 확인하려면 어떻게 해야 하나요?

환경: Cisco ESA (Email Security Appliance), 모든 버전의 AsyncOS

TCPREFUSE 및 REJECT는 일반적으로 BLOCKED Mail Flow Policy와 연결된 두 연결 동작입니다. 이러한 액세스 규칙을 사용하면 알림(하드 바운스)이 있는 원격 호스트의 메시지를 차단할지 아니면 단순히 연결을 삭제할지를 선택할 수 있습니다. [REJECT 와 TCPREFUSE의 차이점은 무엇입니까? 를 참조하십시오.](#)

TCPREFUSE 또는 REJECT(거부)로 인해 원격 호스트가 삭제되는지 여부를 확인하려면 메일 로그에서 항목을 볼 수 있습니다. 자세한 정보 연결 로깅이 활성화된 경우 메일 로그에 TCPREFUSE에 대한 항목만 포함됩니다. 또한 tcpdump와 같은 프로토콜 분석기를 사용하여 패킷 레벨에서 대화를 모니터링할 수 있습니다. 프로토콜 분석기를 사용할 때 TCPREFUSE와 REJECT에 대한 서로 다른 대화를 확인할 수 있습니다.

거부 연결을 위한 ESA와 원격 MTA(Message Transfer Agent) 간의 TCP 연결 흐름은 다음과 같습니다.

```

Remote MTA -----> SYN
Remote MTA -----> ESA
Remote MTA -----> SYN, ACK
ESA -----> Remote MTA
ESA -----> ACK
Remote MTA -----> ESA
Remote MTA -----> 5XX Code
ESA -----> Remote MTA
Remote MTA -----> FIN, ACK
ESA -----> Remote MTA
Remote MTA -----> ACK
Remote MTA -----> ESA
Remote MTA -----> FIN, ACK
Remote MTA -----> ESA
Remote MTA -----> ACK
ESA -----> Remote MTA
```

TCP 거부 연결을 위한 ESA와 원격 MTA 간의 TCP 연결 흐름은 다음과 같습니다.

SYN

```
Remote MTA -----> ESA
                    SYN, ACK
ESA -----> Remote MTA
                    ACK
Remote MTA -----> ESA
                    RST, ACK
ESA -----> Remote MTA
```