피싱 교육 테스트를 위한 Cisco ESA에 화이트리스트 정책 생성

목차

소개

이 문서에서는 피싱 교육 테스트/캠페인을 허용하기 위해 Cisco ESA(Email Security Appliance) 또는 CES(Cloud Email Security) 인스턴스에 화이트리스트 정책을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WebUI의 Cisco ESA/CES에서 규칙 탐색 및 구성
- CLI(Command Line Interface)에서 Cisco ESA/CES에서 메시지 필터 생성
- 피싱 캠페인/테스트에 사용된 리소스에 대한 지식

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

피싱 교육 테스트 또는 캠페인을 실행하는 관리자는 Anti-Spam 및/또는 Outbreak Filter 규칙 집합의 현재 Talos 규칙과 일치하는 정보를 사용하여 이메일을 생성합니다.이러한 경우 피싱 캠페인 이메일은 최종 사용자에게 전달되지 않으며 Cisco ESA/CES 자체에서 작업을 수행하므로 테스트가 중단됩니다.관리자는 ESA/CES에서 이러한 이메일을 통해 캠페인/테스트를 수행할 수 있도록 해야 합니다.

구성

경고:전 세계적으로 허용 목록 피싱 시뮬레이션 및 교육 공급업체에 대한 Cisco의 입장은 허용되지 않습니다.관리자에게 피싱 시뮬레이터 서비스를 사용하도록 권장합니다*(예 :PhishMe)*를 사용하여 IP를 가져온 다음 Whitelist에 로컬로 추가합니다.Cisco는 ESA/CES 고객이 손을 바꾸거나 실제로 위협이 될 경우 이러한 IP로부터 고객을 보호해야 합니다.

주의:관리자는 테스트를 수행하는 동안 이러한 IP를 화이트리스트에 보관해야 하며, 외부 IP는 사후 테스트를 오랜 시간 동안 화이트리스트에 남겨두면 이러한 IP가 감염되면 원치 않거나 악의적인 이메일이 최종 사용자에게 전송될 수 있습니다.

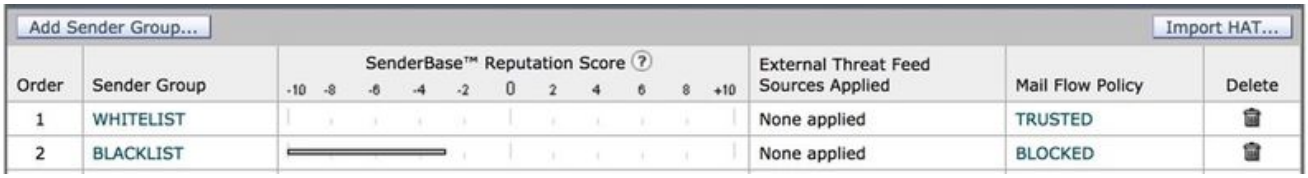
Cisco ESA(Email Security Appliance)에서 피싱 시뮬레이션을 위한 새 Sender Group을 생성하고 이를 $TRUSTED 메일 플로우 정책에 할당합니다.그러면 모든 피싱 시뮬레이션 이메일이 최종 사용자에게 전달될 수 있습니다.이 새 발신자 그룹의 구성원은 속도 제한 대상이 아니며, 이러한 발신자의 콘텐츠는 Cisco IronPort Anti-Spam 엔진에서 검사되지 않지만 안티바이러스 소프트웨어에서 스캔합니다.

참고:기본적으로 $TRUSTED 메일 흐름 정책에는 안티바이러스가 활성화되었지만 안티스팸이 꺼져 있습니다.

발신자 그룹 생성

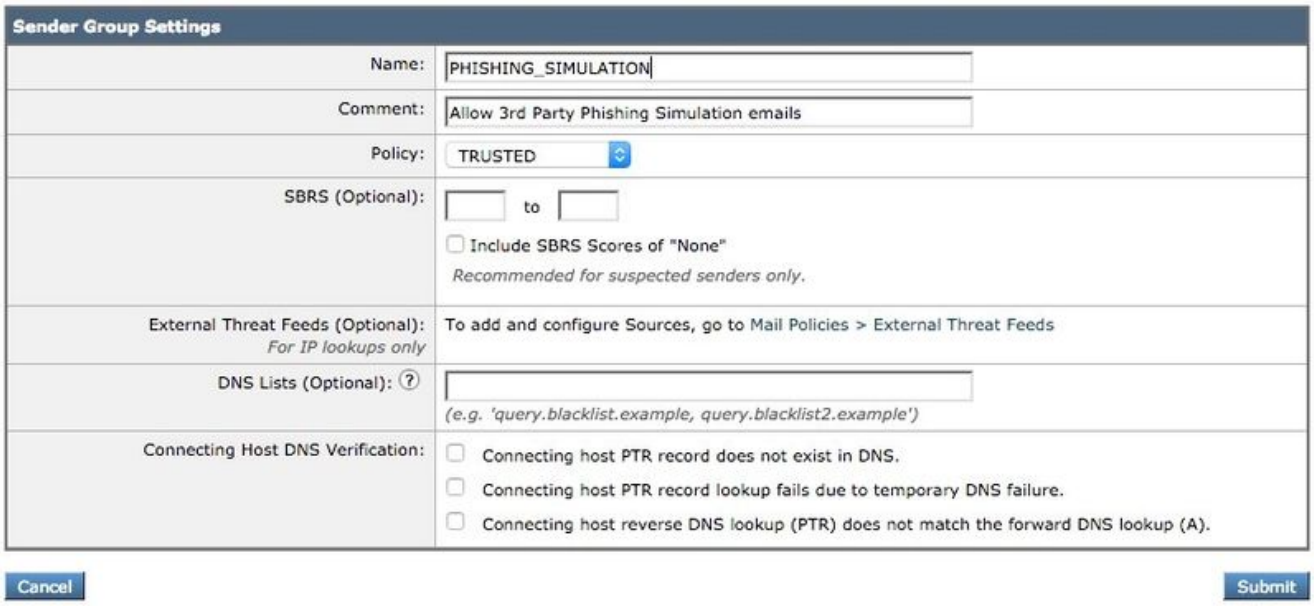
1. ***메일 정책 탭을 클릭합니다.***
2. ***Host Access Table 섹션에서 HAT Overview를 선택합니다.***

3. 오른쪽의 InboundMail ***Listener가*** 현재 선택되어 있는지 확인합니다.
4. 아래 ***Sender Group*** 열에서 Add ***Sender Group..,***

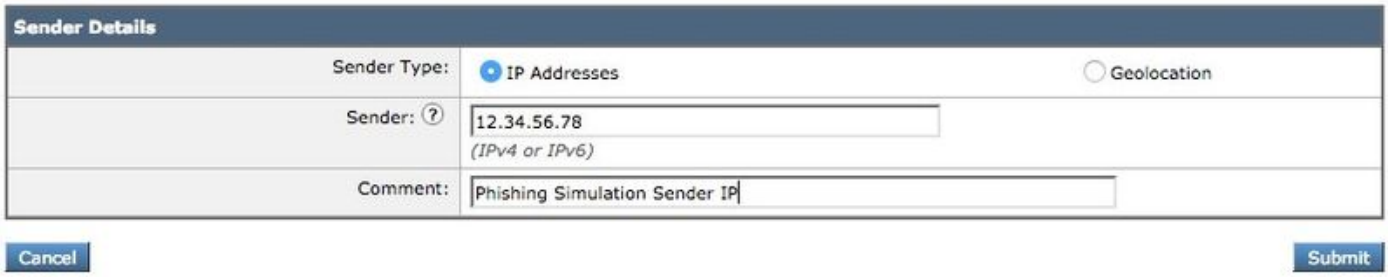


5. Name(*이름)* 및 *Comment(의견)* 필드를 입력합니다. Policy(*정책)* 드롭다운에서 '**$TRUSTED**'를 선택한 다음 Submit and *Add Senders >>를 클릭합니다*

.



6. 화이트리스트에 추가할 IP 또는 호스트 이름을 첫 번째 필드에 입력합니다. 피싱 시뮬레이션 파트너는 발신자 IP 정보를 제공합니다.



항목 추가를 완료하면 ***Submit(제출)*** 버튼을 클릭합니다.Commit Changes(변경 사항 ***커밋)*** 버튼을 클릭하여 변경 사항을 저장합니다.

메시지 필터 생성

Anti-Spam 및 Anti-Virus 우회를 허용하기 위해 Sender Group을 생성한 후, 피싱 캠페인/테스트와 일치할 수 있는 다른 보안 엔진을 건너뛰려면 메시지 필터가 필요합니다.

1. ESA의 CLI에 연결합니다.
2. 명령 ***필터****를* ***실행합니다***.
3. ***new*** 명령을 실행하여 새 메시지 필터를 생성합니다.
4. 필요한 경우 실제 발신자 그룹 이름을 수정하여 다음 필터 예를 복사하여 붙여넣습니다.

```
skip_amp_graymail_vof_for_phishing_campaigns:
```

```
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. 기본 CLI 프롬프트로 돌아가 Enter 키를 누릅니다.
6. commit를 실행하여 컨피그레이션을 저장합니다.

다음을 확인합니다.

서드파티 리소스를 사용하여 피싱 캠페인/테스트를 보내고 메시지 추적 로그의 결과를 확인하여 모든 엔진을 건너뛰고 이메일이 전달되었는지 확인합니다.