발신자 확인을 사용한 스푸핑 보호

목차

소개

기본적으로 Cisco ESA(Email Security Appliance)는 동일한 도메인에서 동일한 도메인으로 향하는 "보낸" 메시지의 인바운드 전달을 방지하지 않습니다.이를 통해 고객과 합법적인 비즈니스를 수행하는 외부 기업이 메시지를 "스푸핑"할 수 있습니다.일부 기업은 Health Care, Travel Agents 등의 회사를 대신하여 이메일을 발송하기 위해 타사 조직에 의존합니다.

발신자 확인을 사용한 스푸핑 보호

MFP(메일 플로우 정책) 구성

1. GUI에서 다음과 같이 표시되어야 합니다.**메일 정책 > 메일 플로우 정책 > 정책 추가...**
2. SPOOF_ALLOW와 관련된 이름을 사용하여 새 MFP를 생성합니다.
3. Sender Verification(*발신자 확인*) 섹션에서 Use Sender Verification Exception Table(발신자 확인 *예외 테이블 사용) 구성을 Use Default(기본값 사용)*에서 **OFF(끄기)**로 **변경합니다**.
4. Mail **Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책) > Default Policy Parameters(기본 정책 매개변수)에서 Use Sender Verification Exception Table configuration(발신자 확인 예외 테이블** 구성 사용)을 On(**켜기)으로** 설정합니다.

HAT 구성

1. GUI: Mail Policies(**메일 정책) > HAT Overview(HAT 개요) > Add Sender Group(발신자 그룹 추가)...**
2. 이에 따라 SPOOF_ALLOW와 같이 이전에 생성한 MFP로 이름을 설정합니다.
3. ALLOWLIST 및 BLOCKLIST 발신자 그룹 위에 표시되도록 순서를 설정합니다.
4. SPOOF_**ALLOW** 정책을 이 Sender Group 설정에 할당합니다.
5. Submit **and Add Senders..(발신자 제출 및 추가...)를 클릭합니다.**
6. 내부 도메인을 스푸핑할 수 있도록 허용할 외부 대상의 IP 또는 도메인을 추가합니다.

예외 테이블 구성

1. GUI에서 다음과 같이 표시되어야 합니다. **메일 정책 > 예외 테이블 > 발송인 확인 예외 추가...**
2. Sender Verification Exception Table
3.

다음을 확인합니다.

이때 발신자가 발신자 확인 예외 테이블을 사용하지 않는 MFP에 연결되어 있는 경우 발신자가 Sender Group SPOOF_ALLOW에 나열되지 않는 한 your.domain에서 your.domain으로 보내는 메일이 거부됩니다.

이 예제는 리스너에 대한 수동 텔넷 세션을 완료하면 표시됩니다.

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

553 SMTP 응답은 위의 단계에서 ESA에 구성된 예외 테이블의 직접 응답 결과입니다.

메일 로그에서 올바른 발신자 그룹의 유효한 IP 주소에 192.168.0.9의 IP 주소가 없음을 확인할 수 있습니다.

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

위 단계의 컨피그레이션 샘플과 일치하는 허용된 IP 주소는 다음과 같습니다.

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

관련 정보

- ESA, SMA 및 WSA Grep with Regex to Search 로그
- ESA 메시지 처리 결정
- 기술 지원 및 문서 – Cisco Systems