使用發件人驗證進行欺騙保護

目錄

簡介

預設情況下，思科郵件安全裝置(ESA)不會阻止從同一域「傳送」到同一域的郵件的入站傳輸。這使得與客戶開展合法業務的外部公司可以「偽裝」郵件。一些公司依靠第三方組織代表公司（如醫療機構、旅行社等）傳送電子郵件。

使用發件人驗證進行欺騙保護

配置郵件流策略(MFP)

1. 在 GUI 上：**郵件策略>郵件流策略>新增策略……**
2. 使用與SPOOF_ALLOW相關的名稱建立新的MFP
3. 在「*Sender Verification*」部分，將*Use Sender Verification Exception Table*配置從*Use Default*更改為**OFF**。
4. 在**Mail Policies > Mail Flow Policies > Default Policy Parameters**中，將*Use Sender Verification Exception Table* configuration設定為**On**。

配置HAT

1. 在GUI中：郵**件策略> HAT概述>新增發件人組……**
2. 將名稱相應地設定為先前建立的MFP，即SPOOF_ALLOW。
3. 設定順序，使其位於ALLOWLIST和BLOCKLIST發件人組之上。
4. 將**SPOOF_ALLOW**策略分配給此發件人組設定。
5. 按一下**提交並新增發件人……**
6. 為要允許欺騙內部域的任何外部方新增IP或域。

配置異常表

1. 在 GUI 上： **郵件策略>異常表>新增發件人驗證異常……**
2.
3.

驗證

此時，從*.domain*到*.domain*的郵件將被拒絕，除非發件人列在發件人組SPOOF_ALLOW中，因為它將關聯到不使用發件人驗證例外表的MFP。

完成到監聽程式的手動telnet會話即可看到一個示例：

```
$ 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響應是來自異常表的直接響應，該異常表是以上步驟中在ESA上配置的。

從郵件日誌中可以看到，IP地址192.168.0.9不在正確發件人組的有效IP地址中：

```
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
```

與以上步驟中的配置示例匹配的允許的IP地址如下所示：

```
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
```

相關資訊

- ESA、SMA和WSA Grep，帶Regex以搜尋日誌

- ESA報文處置確定
- 技術支援與文件 - Cisco Systems