使用发件人验证的欺骗保护

目录

简介

默认情况下，思科邮件安全设备(ESA)不会阻止从同一域“发送”到同一域的邮件的入站传送。这允许与客户进行合法业务的外部公司“欺骗”消息。有些公司依靠第三方组织代表公司发送电子邮件，如医疗保健、旅行社等。

使用发件人验证的欺骗保护

配置邮件流策略(MFP)

1. 从 GUI：**邮件策略>邮件流策略>添加策略……**
2. 使用与SPOOF_ALLOW相关的名称创建新MFP
3. 在“*发件人验证*”部分，将“使用发件人*验证例外表*”*配置从“使用默认值”*更改为“*关闭*”。
4. 在邮**件策略>邮件流策略>默认策略参数**中，将*使用发件人验证例外表*配置设**置为On**。

配置HAT

1. 从GUI: Mail **Policies > HAT Overview > Add Sender Group...**
2. 相应地将名称设置为之前创建的MFP，即SPOOF_ALLOW。
3. 设置顺序，使其位于ALLOWLIST和BLOCKLIST发件人组之上。
4. 将SPOOF_**ALLOW策略**分配给此发件人组设置。
5. 单击**提交并添加发件人……**
6. 为要允许欺骗内部域的任何外部方添加IP或域。

配置异常表

1. 从 GUI： **邮件策略>异常表>添加发件人验证异常……**
2.
3.

验证

此时，除非发件人组SPOOF_ALLOW中列出该发件人，否则从*your.domain*发送到*your.domain*的邮件将被拒绝，因为该发件人将与不使用发件人验证例外表的MFP关联。

通过完成到侦听程序的手动telnet会话，可以看到以下示例：

```
$ 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响应是上述步骤中在ESA上配置的异常表的直接响应结果。

从邮件日志中，您可以看到IP地址192.168.0.9不在正确发件人组的有效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
```

与上述步骤中的配置示例匹配的允许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
```

相关信息

- ESA、SMA和WSA Grep，带Regex以搜索日志
- ESA消息处置确定
- 技术支持和文档 - Cisco Systems