欺骗保护使用发送方验证

目录

[简介](#)
[欺骗保护使用发送方验证](#)
[配置帽子](#)
[配置例外表](#)
[验证](#)
[相关信息](#)
[相关的思科支持社区讨论](#)

简介

默认情况下思科电子邮件安全工具(ESA)不防止从"去同一个的域寻址"对同一个域消息的入站交付。这允许使与客户的事务合法的外部公司"伪装的"消息。一些公司依靠第三方组织代表公司发送电子邮件例如卫生保健、旅行社等等。

欺骗保护使用发送方验证

配置邮件流量策略(MFP)

1. 从 GUI：**邮寄策略>邮件流量策略>Add策略…**
2. 创建一新的MFP使用是相关的类似SPOOF_ALLOW的名称
3. 在*发送方验证*部分，请更改*使用发送方验证例外表*配置从**使用默认**到**OFF**。
4. 在**邮件策略>邮件流量策略>默认策略参数**，设置*使用发送方验证例外表*配置至**开**。

配置帽子

1. 从 GUI： **邮寄策略>帽子概述>Add发送方组…**
2. 相应地设置名称为创建的MFP前，即SPOOF_ALLOW。
3. 设置命令，因此在WHITELIST和黑名单发送方上组。
4. 分配**SPOOF_ALLOW**策略到此发送方组设置。
5. 单击**提交并且添加发送方…**
6. 添加IP或域您要允许伪装内部域的所有外部当事人的。

配置例外表

1. 从 GUI：**邮寄策略>例外表>Add发送方验证例外…**
2.
3.

验证

这时，来自*your.domain的*邮件*到*your.domainwould拒绝，除非发送方在发送方组SPOOF_ALLOW中列出，因为不使用发送方验证例外表的将关联对MFP。

此的示例将通过完成监听程序的一手工的远程登录会话看到：

```
$ 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答复是从例外表的直接响应结果如配置在从上面步骤的ESA。

从邮件日志，您能看到192.168.0.9的IP地址不在正确发送方组的有效IP地址：

```
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
```

匹配与从以上的步骤的配置示例的一个允许IP地址被看到如下：

```
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

- 与搜索日志的REGEX的ESA、SMA和WSA Grep

- ESA消息处理确定
- 技术支持和文档 - Cisco Systems