目录

简介

在邮件期间，收据和交付本文描述如何排除故障断断续续问题和中止的连接。

先决条件

Cisco 建议您了解以下主题：

- Cisco专用互联网交换(PIX)或可适应安全工具(ASA)版本7.x和以上
- 思科电子邮件安全工具(ESA)

背景信息

思科ESA电子邮件网关固有地是电子邮件防火墙。这否定需要对于一上行防火墙，例如思科PIX或ASA，到/从ESA检查邮件流量。被建议禁用在防火墙的Extended Simple Mail Transfer Protocol (ESMTP)应用检查功能所有安全工具主机地址的。默认情况下， ESMTP协议检测为穿过思科防火墙的所有连接启用。这意味着，分析所有命令发出在邮件网关之间通过TCP端口25，以及各自的信息标题严格地坚持包括RFC的821， 1123和1870的请求注释(RFC)规格。有也许到/从您的ESA导致与交付的问题收件人和消息大小的最大的定义的默认值。这些特定配置默认概述得此处(采取从cisco命令查找工具)。

inspect esmtp命令包括**修正smtp**命令以前提供的功能，并且为一些ESMTP命令提供其他支持。ESMTP应用检查添加八ESMTP命令的支持，包括**验证**、**EHLO**、**ETRN**、**帮助**、**SAML**、**发送**、**SOML**和**VRFY**。与七RFC 821命令的支持一起(**DATA**，**直升机**， **MAIL**， **NOOP**，**离开**， **RCPT**，**R装置**)，安全工具支持总共15 SMTP命令。其他ESMTP发出命令，例如**ATRN**， **STARTLS**、**ONEX**、**动词**、**多级组块**和专用扩展和不支持。不支持的命令翻译到Xs，由内部服务器拒绝。这导致一个消息例如**500命令未知：XXX**.不完全的命令丢弃。

inspect esmtp命令更改在服务器SMTP标语的字符对星号除了"2"， "0"， "0"字符。回车(CR)和换行符(LF)字符忽略。使用SMTP检查，用于交互SMTP的会话等待有效命令，并且防火墙esmtp状态机保持会话的正确状态，如果这些规则没有遵守：

- SMTP命令必须是长度至少四个字符。
- 必须终止SMTP命令与回车和换行。
- SMTP命令必须在发出下回复前等待答复。

SMTP服务器回答与数字回复代码和可选人类易读的字符串的客户端的要求。SMTP应用检查控制并且减少用户能使用的命令，以及服务器返回的消息。SMTP检查执行三主要的任务：

- 限制SMTP请求对七基本SMTP命令和八扩展的命令。
- 监控SMTP命令响应顺序。
- 生成审计追踪。当在邮件地址嵌入的无效的字符替换时，审计记录108002生成。欲知更多信息，请参阅RFC 821。

SMTP检查监控以下异常签名的命令和答复顺序：

- 被削的命令。
- 不正确命令终端(没终止与<CR><LR>)。
- 如果找到PCI Express (管道)签名的PHY接口，当对一发出命令的**MAIL**从或**RCPT**的一个参数，会话关闭。它由用户不是可配置。
- 由SMTP服务器的意外的转换。
- 对于未知命令，安全工具在这种情况下更改在数据包的所有字符对**X.**，服务器将生成错误代码给客户端。由于在数据包上的变化， TCP校验和必须重新计算或调节。
- TCP数据流编辑。

show service策略Inspect ESMTP输出提供默认检查值和他们的对应的动作。

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

问题

偶然地，消息不能由思科ESA正确地传送或接收。一个或很多这些消息在思科ESA设备mail_logs被看到：

- 消息中止的MID XXX
- 接收21916丢失的中止的ICID
- ICID 21916 close
- 连接错误：DCID ：XXX域：example.com IP:10.1.2.3端口：25详细信息：[错误60] 计时的操作建立接口：10.10.10.1原因：网络错误

解决方案

其中一些默认设置可能影响事类似传输层安全(TLS)加密的消息、邮件列表市场活动和故障排除交付。一项更加好的策略也许让您使用防火墙检查首先不穿过安全工具，当豁免所有流量时有的所有剩余的电子邮件流量。此示例说明如何调整默认配置(以前注释)豁免单个安全主机地址的ESMTP应用检查。

您能到/从思科定义所有流量ESAs的内部地址供在模块化政策架构(MPF)类映射的参考：

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

这创建新的类映射特别地配比或将不同地对待的挑选流量：

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
```

```
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

此部分连接新的思科类映射并且禁用ESMTP协议检测功能：

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

并且请注释可帮助控制流入和半打开的地址转换语句(胚胎)连接数量对地址的。这为对付拒绝服务攻击(DoS)是有用的，但是可能干涉交付速率。

格式化落后**NAT**和**静态**命令… [tcp (max_conns)]参数 [max_embryonic]。
此示例指定50总TCP连接和100半打开或初期连接尝试限额：

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
```

noted in the RFCs (such as STARTTLS)
mask, packet 2555