

SMTP验证事件如何被记录？

目录

[简介](#)

[SMTP验证事件如何被记录？](#)

[入站SMTP验证](#)

[出站SMTP验证](#)

[相关信息](#)

简介

本文描述SMTP验证事件如何为入站和出局验证被记录。

SMTP验证事件如何被记录？

入站SMTP验证

在思科电子邮件安全工具(ESA)上，在Inbound连接期间被做的认证尝试(为了获得中继使用)登陆mail_logs，当成功和不成功。所有相关条目将关联与有问题的ICID。

成功：

```
Wed Apr 22 11:43:59 2009 Info: New SMTP ICID 450 interface IncomingMail (172.16.155.16)
address 172.16.155.102 reverse dns host unknown verified no
Wed Apr 22 11:43:59 2009 Info: ICID 450 ACCEPT SG None match ALL SBRS None
Wed Apr 22 11:44:48 2009 Info: SMTP Auth: (ICID 450) succeeded for user: ironport
using AUTH mechanism: PLAIN with profile: IncomingAuthentication
Wed Apr 22 11:46:14 2009 Info: ICID 450 close
```

不成功：

```
Wed Apr 22 11:47:30 2009 Info: New SMTP ICID 451 interface mail (172.16.155.16)
address 172.16.155.102 reverse dns host unknown verified no
Wed Apr 22 11:47:30 2009 Info: ICID 451 ACCEPT SG None match ALL SBRS None
Wed Apr 22 11:47:47 2009 Info: SMTP Auth: (ICID 451) failed for user: ironport
using AUTH mechanism: PLAIN with profile: IncomingAuthentication
Wed Apr 22 11:47:56 2009 Info: ICID 451 close
```

出站SMTP验证

从ESA，当SMTP验证为对一台特定主机的交付要求(配置通过“流出的”时SMTP验证配置文件和SMTP路由参考说配置文件)，成功，并且不成功验证尝试将登陆mail_logs。所有条目将关联与有问题的DCID。

成功：

```
Wed Apr 22 11:06:20 2009 Info: New SMTP DCID 5633 interface 172.16.155.16
address 172.16.155.102 port 25
Wed Apr 22 11:06:20 2009 Info: DCID: 5633 IP: 172.16.155.102 SMTP authentication using
the profile OutboundAuthentication succeeded.
Wed Apr 22 11:06:20 2009 Info: Delivery start DCID 5633 MID 441 to RID [0]
Wed Apr 22 11:06:20 2009 Info: Message done DCID 5633 MID 441 to RID [0]
Wed Apr 22 11:06:25 2009 Info: DCID 5633 close
```

不成功：

```
Wed Apr 22 11:19:39 2009 Info: New SMTP DCID 5640 interface 172.16.155.16
address 172.16.155.102 port 25
Wed Apr 22 11:19:41 2009 Info: DCID: 5640 IP: 172.16.155.102 SMTP authentication
using the profile OutboundAuthentication failed: ('535', ['5.7.8 Error: authentication
failed: authentication failure'])
Wed Apr 22 11:19:41 2009 Info: Delivery start DCID 5640 MID 448 to RID [0]
Wed Apr 22 11:19:41 2009 Info: Bounced: DCID 5640 MID 448 to RID 0 - Bounced by
destination server with response: 5.1.0 - Unknown address error
('554', ['5.7.1 <postmaster@example.com>: Relay access denied'])
Wed Apr 22 11:19:46 2009 Info: DCID 5640 close
```

相关信息

- [思科电子邮件安全工具-最终用户指南](#)
- [技术支持和文档 - Cisco Systems](#)