如何記錄SMTP身份驗證事件？

目錄

簡介

本文檔介紹如何為入站和出站身份驗證記錄SMTP身份驗證事件。

如何記錄SMTP身份驗證事件？

入站SMTP身份驗證

在思科電子郵件安全裝置(ESA)上，在入站連線期間進行的身份驗證嘗試（以獲取中繼訪問許可權）成功和不成功時記錄在mail_logs中。所有相關條目將與所涉ICID關聯。

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
```

未成功：

```
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身份驗證

從ESA中，當向特定主機傳輸資料時需要SMTP身份驗證（通過「傳出」SMTP身份驗證配置檔案和引用該配置檔案的SMTP路由配置），則在mail_logs中記錄身份驗證嘗試的成功和不成功。所有條目將與所討論的DCID關聯。

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
```

未成功：

```
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
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems