Wie werden SMTP-Authentifizierungsereignisse protokolliert?

Inhalt

Einführung

Dieses Dokument beschreibt, wie SMTP-Authentifizierungsereignisse für die eingehende und ausgehende Authentifizierung protokolliert werden.

Wie werden SMTP-Authentifizierungsereignisse protokolliert?

Eingehende SMTP-Authentifizierung

Auf der Cisco E-Mail Security Appliance (ESA) werden Authentifizierungsversuche, die bei eingehenden Verbindungen (um Relay-Zugriff zu erhalten) durchgeführt werden, im mail_logs protokolliert, wenn sie erfolgreich und erfolglos sind. Alle relevanten Einträge werden mit der betreffenden ICID verknüpft.

Erfolgreich:

```
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
```

Fehlgeschlagen:

```
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
```

Ausgehende SMTP-Authentifizierung

Wenn für Lieferungen an einen bestimmten Host eine SMTP-Authentifizierung erforderlich ist (konfiguriert über ein "ausgehendes" SMTP-Authentifizierungsprofil und eine SMTP-Route, auf die dieses Profil verweist), werden von der ESA sowohl erfolgreiche als auch erfolglose Authentifizierungsversuche in den mail_logs protokolliert. Alle Einträge werden der betreffenden DCID zugeordnet.

Erfolgreich:

```
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
```

Fehlgeschlagen:

```
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
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems