How are SMTP authentication events logged?

Document ID: 118570

Contributed by Cisco TAC Engineers.

Oct 14, 2014

Contents

Introduction

This document describes how SMTP authentication events are logged for inbound and outbound authentication.

How are SMTP authentication events logged?

Inbound SMTP Authentication

On the Cisco Email Security Appliance (ESA), authentication attempts made during inbound connections (in order to gain relay access) are logged in the mail_logs when successful and unsuccessful. All relevant entries will be associated with the ICID in question.

Successful:

```
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
```

Unsuccessful:

```
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
```

Outbound SMTP Authentication

From the ESA, when SMTP authentication is required for deliveries to a specific host (configured via an "Outgoing" SMTP authentication profile and an SMTP route referencing said profile), both successful and unsuccessful authentication attempts will be logged in the mail_logs. All entries will be associated with the

DCID in question.

Successful:

```
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
```

Unsuccessful:

```
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
```

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 14, 2014 Document ID: 118570