ESA에서 아웃바운드 메일 SMTP 세션 추적

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 전체 이메일 대화를 추적하고 보는 방법에 대해 설명합니다.

수신자 도메인당 아웃바운드 메일 SMTP 세션 추적

도메인 디버그 로그를 사용하여 ESA와 대상 도메인/호스트 간에 전체 SMTP(Simple Mail Transfer Protocol) 대화를 추적할 수 있습니다. 도메인 디버그 로그의 각 행은 SMTP 대화 중에 전송(전송) 및 수신(Rcvd)된 데이터를 간략하게 설명합니다.

ESA에서 관심 있는 수신자 도메인에 대한 도메인 디버그 로그를 기록하도록 로깅을 구성하려면 ESA CLI에 logconfig 명령을 입력합니다.

```
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> new

Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
```

```
16. URL Filtering Logs
17. Graymail Engine Logs
18. Anti-Spam Archive
19. Anti-Virus Logs
20. Anti-Virus Archive
21. Scanning Logs
22. Spam Quarantine Logs
23. Spam Quarantine GUI Logs
24. Reporting Logs
25. Reporting Query Logs
26. Updater Logs
27. SNMP Logs
28. Tracking Logs
29. Safe/Block Lists Logs
30. Authentication Logs
31. FIPS Logs
32. Upgrade Logs
33. Configuration History Logs
34. Reputation Engine Logs
35. AMP Engine Logs
36. AMP Archive
37. API Logs
38. Graymail Archive
[1]> 6

Please enter the name for the log:
[]> example.com.domain.debug

Enter the name of the domain for which you want to record
debug information.
[]> example.com

Please enter the number of SMTP sessions you want to record
for this domain.
[1]> 10000

Choose the method to retrieve the logs.
1. Download Manually: FTP/HTTP(S)/SCP
2. FTP Push
3. SCP Push
4. Syslog Push
[1]>

Filename to use for log files:
[example.com.text]>

Would you like to append system based unique identifiers
like $hostname, $serialnumber to the log filename? [N]>

Please enter the maximum file size. You can specify suffixes:
"m" for megabytes, "k" for kilobytes. Suffixes are
case-insensitive:
[10485760]>

Please enter the maximum number of files:
[10]>

Should an alert be sent when files are removed due to the
maximum number of files allowed? [N]>

Do you want to configure time-based log files rollover? [N]>
```

참고:도메인 디버그 로그가 **구성된** 후 모든 변경 사항을 커밋해야 합니다.

도메인에 대해 구성한 세션 수에 대해 로그가 활성화됩니다.라이브 이메일 대화의 추적을 보려면 **tail example.com.domain.debug** 명령을 ESA CLI에 입력합니다.

다음은 ESA가 수신자 도메인 example.*com*에 메시지를 전달할 때 생성되는 도메인 디버그 로그의 예입니다.

```
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '220 ESmtp mail.example.com ESMTP service
ready'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'EHLO example.com'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-mail.example.com'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-8BITMIME'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-SIZE 31981568'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 PIPELINING'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'MAIL FROM:<user@example.com>'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 sender <user@exmple.com> ok'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'RCPT TO:<test@example.com>'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 recipient <test@example.com> ok'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'DATA'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '354 go ahead'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'Received: from unknown (HELO)(10.250.7.164)
\r\n by example.com with SMTP; 22 Mar 2005 16:52:08 -0800\r\n'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'Message-ID:
<000d01c52f43$48dacba0$a407fa0a@example.com>\r\nFrom: "User"
<user@example.com>\r\nTo:<test@example.com>\r\n Subject:Test\r\nDate:
Tue,22Mar200516:57:28-0800\r\nMIME-Version:1.0\r\n
Content-Type:multipart/alternative;\r\n\tboundary="----=_Next
Part_000_000A_01C52F00.3AA3B580"\r\nX-Priority: 3\r\nX-MSMail-Priority: Normal\r\n
X-Mailer: Microsoft Outlook Express 6.00.2900.2180\r\nX-MimeOLE: Produced ByMicrosoft
MimeOLEV6.00.2900.2180\r\n\r\nThis is a multi-part messageinMIMEformat.\r\n\r\
n------=_NextPart_000_000A_01C52F00.3AA3B580\r\nContent-Type:text/plain;\r\n\
tcharset= "iso-8859-1"\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\nThis
is the body of the mail.\r\nThis isadisclaimer.\r\n\r\n------=
_NextPart_000_000A_01C52F00.3AA3B580\r\nContent-Type:text/html;\r\n\tcharset=
"iso-8859-1"\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n<!DOCTYPE HTML
PUBLIC"-//W3C//DTDHTML4.0Transitional//EN">\r\n<HTML><HEAD>\r\n<METAhttp-equiv=
3DContent-Typecontent= 3D"text/html;charset= 3Diso-8859-1">\r\n<METAcontent=3D"
MSHTML6.00.2900.2523"name= 3DGENERATOR>\r\n<STYLE></STYLE>\r\n</HEAD>\r\n
<BODYbgColor= 3D#ffffff>\r\n<DIV><FONTface= 3DArialsize= 3D2>This is the body of
the\r\nmail.</FONT></DIV><pre> This is a disclaimer.\r\n </pre></BODY></HTML>\r\n\r\
n------=_NextPart_000_000A_01C52F00.3AA3B580--\r\n'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: '.\r\n'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 ok dirdel'
Tue Mar 22 16:52:12 2005 Info: 411 Sent: 'QUIT'
Tue Mar 22 16:52:12 2005 Info: 411 Rcvd: '221 mail.example.com'
```

관련 정보

- Cisco Email Security Appliance 최종 사용자 설명서
- ESA 도메인 디버그 로그 컨피그레이션 예
- ESA FAQ:ESA에서 간헐적인 메일 전달 문제를 어떻게 분석합니까?
- 기술 지원 및 문서 Cisco Systems