메시지 헤더를 로깅하는 방법

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)를 통해 처리된 메시지 헤더를 기록하는 방법에 대해 설명합니다.

메시지 헤더를 로깅하는 방법

경우에 따라 메시지 헤더가 어플라이언스를 통과할 때 해당 헤더의 현재 상태 및 내용을 기록하는 것이 유용합니다.logconfig > logheaders를 통해 기록할 헤더를 **지정합니다**.ESA는 지정된 메시지 헤더를 IronPort 텍스트 메일 로그, IronPort 전달 로그 및 IronPort 바운스 로그에 기록합니다.헤더가 있는 경우 헤더의 이름과 값이 기록됩니다. 헤더 정보는 납품 정보 뒤에 기록됩니다.

다음은 헤더 X-IPAS-Result 및 X-IronPort-AV로 메시지를 기록하기 위해 로깅을 활성화하는 방법의 예입니다.

```
my_esa.local> logconfig

Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. amp AMP Engine Logs Manual Download None
2. amparchive AMP Archive Manual Download None
3. antispam Anti-Spam Logs Manual Download None
4. antivirus Anti-Virus Logs Manual Download None
5. asarchive Anti-Spam Archive Manual Download None
6. authentication Authentication Logs Manual Download None
7. avarchive Anti-Virus Archive Manual Download None
8. bounces Bounce Logs Manual Download None
9. cli_logs CLI Audit Logs Manual Download None
10. encryption Encryption Logs Manual Download None
11. error_logs IronPort Text Mail Logs Manual Download None
12. euq_logs Spam Quarantine Logs Manual Download None
13. euqgui_logs Spam Quarantine GUI Logs Manual Download None
14. ftpd_logs FTP Server Logs Manual Download None
15. gui_logs HTTP Logs Manual Download None
16. mail_logs IronPort Text Mail Logs Manual Download None
17. mail_logs_copy IronPort Text Mail Logs SCP Push - Host
192.168.0.200: Port 22None
18. repeng Reputation Engine Logs Manual Download None
19. reportd_logs Reporting Logs Manual Download None
```

```
20. reportqueryd_logs Reporting Query Logs Manual Download None
21. scanning Scanning Logs Manual Download None
22. slbld_logs Safe/Block Lists Logs Manual Download None
23. snmp_logs SNMP Logs Manual Download None
24. sntpd_logs NTP logs Manual Download None
25. status Status Logs Manual Download None
26. system_logs System Logs Manual Download None
27. trackerd_logs Tracking Logs Manual Download None
28. updater_logs Updater Logs Manual Download None
29. upgrade_logs Upgrade Logs Manual Download None

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.
[]> logheaders

Please enter the list of headers you wish to record in the
log files.
Separate multiple headers with commas.
[]> X-IPAS-Result, X-IronPort-AV
```

기본 CLI 프롬프트로 돌아가서 모든 변경 사항을 커밋합니다.

mail_logs를 검토할 때 구성된 대로 로그에 삽입된 헤더의 결과가 표시됩니다.

```
Thu Aug 14 08:40:18 2014 Info: New SMTP ICID 10282 interface Management
(192.168.0.199) address 192.168.0.200 reverse dns host ns.domain.com verified no
Thu Aug 14 08:40:18 2014 Info: ICID 10282 RELAY SG RELAY_SG match 192.168.0.200
SBRS not enabled
Thu Aug 14 08:40:18 2014 Info: Start MID 1403 ICID 10282
Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 From: <orig_user@domain.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 RID 0 To: <end_user@example.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: SPF Verdict Cache cache status: hits = 7, misses = 12,
expires = 0, adds = 12, seconds saved = 0.06, total seconds = 0.56
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: helo identity postmaster@domain.com None
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: mailfrom identity orig_user@domain.com
Pass (v=spf1)
Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
cached verdict
Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: pra identity orig_user@domain.com None
headers from
Thu Aug 14 08:40:18 2014 Info: MID 1403 Message-ID '<20140814124103.GC6764@domain.com>'
Thu Aug 14 08:40:18 2014 Info: MID 1403 Subject 'Hello - this is the morning report...'
Thu Aug 14 08:40:18 2014 Info: MID 1403 ready 611 bytes from <orig_user@domain.com>
Thu Aug 14 08:40:18 2014 Info: MID 1403 matched all recipients for per-recipient policy
DEFAULT in the outbound table
Thu Aug 14 08:40:18 2014 Info: ICID 10282 close
Thu Aug 14 08:40:20 2014 Info: MID 1403 interim verdict using engine: CASE spam negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 using engine: CASE spam negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 interim AV verdict using Sophos CLEAN
Thu Aug 14 08:40:20 2014 Info: MID 1403 antivirus negative
Thu Aug 14 08:40:20 2014 Info: MID 1403 Outbreak Filters: verdict negative
```

```
Thu Aug 14 08:40:20 2014 Info: MID 1403 DLP no violation
Thu Aug 14 08:40:20 2014 Info: MID 1403 queued for delivery
Thu Aug 14 08:40:20 2014 Info: New SMTP DCID 173 interface 192.168.0.199 address
111.22.111.22 port 25
Thu Aug 14 08:40:20 2014 Info: DCID 173 STARTTLS command not supported
Thu Aug 14 08:40:20 2014 Info: Delivery start DCID 173 MID 1403 to RID [0]
Thu Aug 14 08:40:20 2014 Info: Message done DCID 173 MID 1403 to RID [0]
[('X-IPAS-Result', 'AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRi
JC8VuF4wKg1+DGYEdAQSPCoMNiiEBmHaDHwEBAQ'), ('X-IronPort-AV', 'E=Sophos;i=
"5.01,863,1400040000"; \r\n d="scan\'208";a="1403"')]
Thu Aug 14 08:40:20 2014 Info: MID 1403 RID [0] Response '2.0.0 OK
F6/FE-18769-93EACE35'
Thu Aug 14 08:40:20 2014 Info: Message finished MID 1403 done
Thu Aug 14 08:40:25 2014 Info: DCID 173 close
```

수신된 이메일에서 해당 이메일의 헤더를 직접 확인하려는 경우 첫 번째 홉이 수신되기 전에 원본 헤더에 강조 표시된 X-IPAS-Result 및 X-IronPort-AV 헤더가 표시됩니다.

```
X-IronPort-Anti-Spam-Filtered: true
X-IPAS-Result: AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRiJC8VuF4wKg1+
DGYEdAQSPCoMNiiEBmHaDHwEBAQ
X-IronPort-AV: E=Sophos;i="5.01,863,1400040000";
  d="scan'208";a="1403"
Received: from ns.domain.com (HELO mail.domain.com) ([192.168.0.200])  by
 myesa_local.domain.com with ESMTP; 14 Aug 2014 08:40:18 -0400
Received: by mail.domain.com (Postfix, from userid 1000)id 29F4E8033E; Thu,
 14 Aug 2014 08:41:03 -0400 (EDT)
Date: Thu, 14 Aug 2014 08:41:03 -0400
From: robert <orig_user@domain.com.com>
To: <end_user@example.com>
Subject: Hello - this is the morning report...
Message-ID: <20140814124103.GC6764@domain.com>
MIME-Version: 1.0
User-Agent: Mutt/1.5.21 (2010-09-15)
X-RR-Connecting-IP: 111.22.111.222:25
X-Cloudmark-Score: 0
Return-Path: orig_user@domain.com.com
X-MS-Exchange-Organization-AuthSource: xhc-aln-x10.example.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 10
Content-type: text/plain;
charset="US-ASCII"
Content-transfer-encoding: 7bit

No info this morning.

-Joe
```

참고: SMTP 프로토콜에 대한 RFC는 http://www.faqs.org/rfcs/rfc2821.html에 있으며 사용자 정의 헤더를 정의합니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems