

TechNote on High CPU Utilization on C170

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[High CPU Utilization on C170](#)

[Related Information](#)

Introduction

This document describes the CPU utilization and operation for a Cisco Email Security Appliance (ESA) C170 model.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Status detail and system utilization, with regard to ESA operation

Components Used

The information in this document is based on only the ESA C170 model.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

High CPU Utilization on C170

For an ESA C170, to get CPU load at 40% is not generally a cause for concern and it is normal under certain circumstances.

The appliance is not totally idle. The appliance is performing service level actions even while not processing email. Based on CPU load, these are some examples which can contribute to the CPU usage:

- Processing service updates (Anti-Spam, Anti-Virus, etc.)
- Accepting Secure Shell (SSH) connections from an Security Management Appliance (SMA)
- Processing reporting data

Note: The C170 only has two CPU. The relatively minor CPU usage of things like service updates and SSH connections has a greater impact on the CPU load calculation on appliances with less CPU onboard.

On the C170, one of the top reasons of CPU utilization is service updates. When the ESA processes service updates, the relevant processes are stopped and restarted as updates occur. This can take significant CPU. For example, when running the CLI command **antispamupdate ironport force**, the Cisco Anti-Spam Engine (CASE) is updated and restarted. The service itself compiles the rules and updates for faster overall performance. This momentary restart reflects in the seen CPU churn.

Note: CPU load, as computed by the OS is a rolling calculation. Thus, previous high CPU can affect the current reported CPU load even if CPU usage currently is not very high. This means that despite the service updates only occurring every 5 minutes, their CPU usage can impact the CPU load computed in the interval between the updates as well.

A second reason of high CPU utilization is SSH connections. If an ESA is configured to use an SMA for centralized reporting, quarantines, etc., there is CPU overhead which accepts SSH connections from the SMA when the ESA is initially connected to it. The rate at which the ESA is receiving SSH connections from the SMA varies but generally the ESA receives a connection around every 30 seconds or so. You may view this from the authentication logs and see the **smaduser** connecting:

```
myesa.local> tail authentication
```

```
Press Ctrl-C to stop.
```

```
Wed Apr 12 13:41:06 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:41:26 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:41:44 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:42:01 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

A final reason to consider when reviewing high CPU utilization is the appliance processing reporting data. The ESA continues to process reporting data while it is not processing email. For example, system load metrics are being processed for the System Capacity report. Furthermore, the ESA performs reporting **rollups** to allow the reporting database to remain at a reasonable size. These reporting rollups are most significant at the beginning of the month when the monthly rollup occurs.

The bottom line is that CPU utilization of 40% is not abnormal for the C170, even if the appliance is idle with no email messages processing. An ESA administrator should only be concerned if the CPU load is pegged at 100% for an extended period of time. Review the output of **status detail**, as shown in the image, for the **Gauges** of system resources and the log output of the status log.

Example from **status detail**:

Gauges:	Current
System	
RAM Utilization	1%
Overall CPU load average	5%
CPU Utilization	
MGA	0%
Anti-Spam	0%
Anti-Virus	0%
Reporting	0%
Quarantine	0%
Disk I/O Utilization	0%
Resource Conservation	0
Logging Disk Usage	2%
Logging Disk Available	182G
Connections	
Current Inbound Conn.	0
Current Outbound Conn.	0
Queue	
Active Recipients	0
Unattempted Recipients	0
Attempted Recipients	0
Messages In Work Queue	0
Destinations In Memory	3
Kilobytes Used	0
Kilobytes Free	8,388,608
Messages In Quarantine	
Policy, Virus and Outbreak	0
Kilobytes In Quarantine	
Policy, Virus and Outbreak	0

Example from status logs:

```
myesa.local> tail status
```

Press Ctrl-C to stop.

```
Wed Apr 12 14:03:06 2017 Info: Status: CPULd 0 DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvtnt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382176 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 7
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891
```

```
Wed Apr 12 14:04:06 2017 Info: Status: CPULd 0 DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvtnt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382236 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 5
```

LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Wed Apr 12 14:05:06 2017 Info: Status: **CPULd 45** DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID
23 CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382296 MaxIO 350 RAMUsd 74632122 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 5
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Wed Apr 12 14:06:06 2017 Info: Status: **CPULd 0** DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382356 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 15
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Related Information

- [Cisco Email Security Appliance C170](#)
- [Technical Support & Documentation - Cisco Systems](#)