Contents

Introduction

This document describes how to troubleshoot delivery and connection problems when centralized policiy, virus and outbreak quarnatine is enabled.

Components Used

The information in this document is based on these software and hardware versions:

- Email Security Appliance (ESA) with AsyncOS 8.1 or later
- Security Management Appliance (SMA) with AsyncOS 8.0 or later

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.

Background Information

The Centralized Policy, Virus and Outbreak (PVO) Quarantines feature was introduced in AsyncOS 8.0 (ESA) / 8.1 (SMA). This feature has additional network connectivity requirements, and poses some new challenges for troubleshooting.

Understand the communication

- CPQ communication uses SMTP, but with some extra commands for transferring metadata
- The SMA will listen for connections on the interface and port defined under Centralized Services -> Policy, Virus and Outbreak Quarantines. By default, the port is 7025, but this may have been changed by the admin user!
- The ESA will listen for connections on the interface and port defined under Security Services -> Policy, Virus and Outbreak Quarantines. Again, by default, the port is 7025, but this may have been changed by the admin user!
- The SMA also uses SSH (via command client) to get configuration information from the ESAs. In particular, this is used when the SMA delivers released emails to the ESA. The

SMA will use SSH to query the ESA configuration and determine which interface / port to deliver the released email to.

Listeners

- Both the ESA and the SMA will have a hidden listener called 'cpq_listener' that will listen on the specified port.
- These listeners can be seen in the configuration file. For example:

- These listeners will be suspended if the admin user uses 'suspendlisteners all' or 'suspend'. If the port is not accepting connections, you should check if the system status is 'offline' and resume if needed.

Troubleshoot delivery from ESA to SMA

- Check that the ESA can connect to the SMA on the configured port and interface. This can be done using telnet. You should get a 220 banner if the communication is successful.
- The ESA will have a destination object called 'the.cpq.host', which contains messages while they are queued for delivery to the SMA. You can see this using 'tophosts' or Monitor -> Delivery Status.   You cannot use 'hoststatus' with it, but you can use 'showrecipients' and 'deleterecipients' if necessary.

Troubleshoot delivery from SMA to ESA

- Check that the SMA can connect to the ESA on the configured port and interface. Again, you can use telnet and will see the 220 banner if succesful.
- When using clusters, it is important that the interface defined at cluster level under Security Services -> Policy, Virus and Outbreak Quarantines exists for all appliances at machine level. (check Network -> IP Interfaces).
- The SMA wil have a destination object called 'the.cpq.release.host' which contains released messages while they are queued for delivery to the ESA. You can see this using 'tophosts'. This does not appear to work with 'hoststatus' or 'showrecipients', and I have not tested 'deleterecipients' with it, but this probably does not work either.
- There may also be problems with SSH communication between the SMA and the ESA. These issues are not always necessarily network based, for example in CSCus29647 an internal component of the SMA goes out of operation. Issues such as these will typically show up as application faults in the mail logs, and can usually be resolved by rebooting the SMA.

TLS/Certificates

- All CPQ connections in either direction rely on TLS, and as a result cipher configuration can play a role.
- In order for the TLS connection to succeed, the device opening the connection must be able to verify that the receiving device is using our hiddent CPQ certificate. It is possible for this to fail if the appliance negotiates an anonymous cipher. This would appear in the logs as something like this:

- You can fix these issues by simply removing anonymous ciphers from the outgoing delivery cipher list, which is done by adding '`:-aNULL` `HIGH:MEDIUM:`**`-aNULL`**

Log File

- If the SMA has a mail logs subscription (it does by default), you can review the mail logs to gather additional insight.
- CPQ receiving events will look like this for both messages being quarantined to the SMA and messages released to ESA

- You can search for these events using grep, example: `grep "CPQ ICID" mail_logs`
- CPQ delivery events, both quarantining from ESA and release from quarantine from SMA, look similar to any other delivery, with the exception that the custom port is listed and a few lines include the verbiage 'Centralized Policy Quarantine'. Example below:

- You can find these events by using grep to seach for the port, example: `grep "port 7025" mail_logs`

ESA 'Enable' button disabled

When attempting to enable PVO on the ESA, you may find that the 'Enable' button is grayed out, despite all pre-requisite configuration being completed. When the ESA displays the PVO page, it communicates with the SMA over port 7025 to verify that the configuration is ready to be enabled. If this communication fails, the 'Enable' button will be disabled. You can troubleshoot this just like any ESA -> SMA port 7025 communication by grepping for "port 7025" on the ESA. For more information refer to the TechNote listed in Related Information.

Related Information

- **Requirements for the PVO Migration Wizard when ESA is clustered**
- **ESA Centralizing Policy, Virus, and Outbreak Quarantine (PVO) Cannot be Enabled**