Best Practices for Centralized Policy, Virus and Outbreak Quarantines Setup and Migration from ESA to SMA

Contents

Introduction

The following quarantines can now be collectively centralized on a Cisco Security Management Appliance (SMA):

- Anti-Virus
- Outbreak
- Policy quarantines used for messages that are caught by:
  Message filtersContent filtersData loss prevention policies

Centralizing these quarantines offers the following benefits:

- Administrators can manage quarantined messages from multiple Email Security Appliances (ESA) in one location.
- Quarantined messages are stored behind the firewall instead of in the DMZ, reducing the security risk.
- Centralized quarantines can be backed up as part of the standard backup functionality on the SMA.

Prerequisites

- SMA running 8.1 (SMA User Guide, Chapter 8, Centralized Policy, Virus, and Outbreak Quarantines)
- ESA running 8.0.1 (ESA User Guide, Chapter 27, Quarantines)
- Firewall - port 7025 / TCP (In and Out) / Hostname use: AsyncOS IPs / Description: Pass policy, virus, and outbreak quarantine data between Email Security appliances and the Security Management appliance when this feature is centralized

Configure

Starting with the ESA, in an existing Policy Quarantine, there are active messages in the Policy Quarantine:

In order to migrate these messages and then rely on the SMA to be the active appliance owning the Policy Quarantine, complete the following directions.

On the SMA, navigate to **Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines**. If not enabled already, click **Enable:**

Select the interface, if applicable, that is intended to handle traffic from the ESA to the SMA.

> **Note**: The Quarantine Port may be changed, but this will need to be opened if there is a firewall/network ACL in place.

Click **Submit**. The screen will refresh to show the ?Service enabled? message, seen below:

Navigate to **Management Appliance > Centralized Services > Security Appliances** and add the ESA communication to the SMA:

Click **Add Email Appliance**.

> **Note**: You only need to add the IP address that the SMA will use to communicate with the ESA. The appliance name is used only as an administrative reference.

Be sure to **Establish Connection** and **Test Connection**. Upon establishing connection from the SMA to the ESA, the administrator user name and password will be requested. This is the administrative user and password of the ESA that is being added. Based on what is already active vs. what is being added, the results of the test may vary, but should be similar to:

Be sure to **Submit** and **Commit Changes** at this point on the SMA.

At this time, if you were to revisit the ESA and attempt to configure the Centralized Services section of the Policy Quarantine, it would be similar to the following:

The migration steps must still be completed on the SMA. Return to the SMA and continue with the following section.

Once the **Commit Changes** is completed, the **Launch Migration Wizard?** of step 2 will become active:

Select **Launch Migration Wizard** and continue as follows:

If only a particular quarantine is to be migrated, choose **Custom**. In this example, we will continue with **Automatic**, which will migrate ANY/ALL Policy Quarantines from the ESA to SMA. Please note that you will see the specified name chosen during the ESA add earlier mentioned, followed by the IP address used in communication:

Click **Next**, and continue:

Finally, click **Submit**, and the "Success" notification is presented:

Commit your changes on the SMA.

Returning to the ESA, navigate to **Security Services > Policy, Virus and Outbreak Quarantines**. The prerequisite steps on the SMA are now recognized:

Click **Enable?**, and continue:

Notice, that here again the proper port used for communication is noted. These **must** match, and if firewall/network ACL is in use, must be opened in order to allow proper migration between the ESA and SMA.

> **Note**: If you have policy, virus, and outbreak quarantines configured on an ESA, migration of quarantines and all their messages begins as soon as you commit this change.

> **Note**: Only one migration process can be in progress at any time. Do not enable centralized policy, virus, and outbreak quarantines on another Email Security appliance until the previous migration is complete.

Click **Submit**, and finally click **Commit**. The info notification should be similar. If there are a large number of messages already in local quarantine, these may take time to process from ESA to SMA:

Revisit the SMA, and navigate to **Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines**. The migration steps will now be completed:

Verification

At this time, the migration of the Policy Quarantine from the ESA to the SMA is complete. For final verification, check the Policy Quarantine on the SMA:

You should see the same messages that were originally listed on the ESA. Select the # hyperlink in the messages column, and verify:

If you look at the mail_logs on the ESA, migration of the actual messages will be presented:

> **Note**: Note the use of communication between the ESA (XX.X.XX.XXX) and SMA (YY.Y.YY.YYY) via port 7025.

```
Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
```

```
Wed Mar  5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar  5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok:  Message 1 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar  5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok:  Message 2 accepted'
```

```
Wed Mar  5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar  5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok:  Message 3 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar  5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:07 2014 Info: DCID 12 close
```

Revisit the ESA, and the following is now presented when viewing the Policy, Virus, Outbreak Quarantines:

The next step of verification is sending a new test message through the ESA that will be caught for policy quarantine. Looking at mail_logs on the ESA, notice the highlighted line indicating the transfer from ESA to SMA via 7025, indicating the Policy Quarantine:

```
Wed Mar  5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar  5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
Wed Mar  5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar  5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar  5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar  5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok:  Message 4 accepted'
Wed Mar  5 02:57:47 2014 Info: Message finished MID 4 done
Wed Mar  5 02:57:52 2014 Info: DCID 16 close
```

Revisit the previously mentioned Policy Quarantine on the SMA, the new test message is now in quarantine as well:

Related Information

- **ESA Centralizing Policy, Virus, and Outbreak Quarantine (PVO) Cannot be Enabled**
- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**