Contents

Introduction

This document describes when a virtual Email Security Appliance (vESA) does not download and apply updates for the Cisco antispam engine (CASE) or Sophos and/or McAfee antivirus, even though the virtual appliance is licensed correctly.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Email Security Appliance (ESA)
- vESA, virtual Web Security appliance (vWSA), virtual Security Management Appliance (vSMA)
- AysncOS

Components Used

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

- vESA, that runs AsyncOS 8.0.0 and later
- vWSA, that runs AsyncOS 7.7.5 and later
- vSMA, that runs AsyncOS 9.0.0 and 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.

vESA Is Not Able to Download and Apply Updates for Antispam or Antivirus

When you update antispam or antivirus, the processes are not able to reach out and update the

service engine or rulesets, even if you enter the **update force** command.

One of these commands might have been entered directly from the CLI on the vESA:

```
> antispamupdate ironport
>antispamupdate ironport force
>antivirusupdate force
>updatenow force
```

When you run **tail updater_logs**, the errors seen are similar to these:

```
Mon Oct 21 17:48:43 2013 Info: Dynamic manifest fetch failure: Received invalid
update manifest response
```

This indicates that the dynamic host URL associated to the update configuration is not able to reach the proper updater manifest correctly. The dynamic host URL is set within the **updateconfig** command. The subcommand, **dynamichost,** is a hidden command within **updateconfig**, as highlighted here:

```
myesa.local> updateconfig
Service (images): Update URL:
-------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
IMS Secondary Service rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]> dynamichost

Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]>
```

Set the Appliance to Use the Correct Dynamic Host URL

There are two different dynamic host URLs that are used for customers based on how they are associated through Cisco:

- update-manifests.sco.cisco.com:443

- Usage: Customer vESA, vWSA, vSMA

  Note: Hardware appliances (C1x0, C3x0, C6x0, and X10x0) should ONLY use the dynamic host URL of*update-manifests.ironport.com:443*. If there is a cluster configuration with both ESA and vESA, **updateconfig** must be configured at the machine level and then confirm that **dynamichost** is set accordingly.

- stage-stg-updates.ironport.com:443
- Usage: Friendlies, Beta virtual and hardware appliances

  Note: Customers should only use the staging update server URLs if they have gained access to preprovisioning through Cisco for Beta usage only. If you do not have a valid license applied for Beta use, your appliance will not receive updates from the staging update servers.

As a continuation from **updateconfig** and the **dynamichost** subcommand, enter the dynamic host URL as needed, return to the main CLI prompt, and commit the changes:

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]> stage-stg-updates.ironport.com:443
[]> <<<HIT RETURN TO GO BACK TO THE MAIN CLI PROMPT>>>

myesa.local> commit
```

Verify

In order to verify that the appliance now reaches out to the proper dynamic host URL and updates are successful, complete these steps:

1. Increase the **updater_logs** to **debug**. `Currently configured logs:> logconfig`

   ```
   Log Name Log Type Retrieval Interval
   -------------------------------------------------------------------------------
   1. antispam Anti-Spam Logs Manual Download None
   [SNIP FOR BREVITY]
   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.
   []> edit
   Enter the number of the log you wish to edit.
   []> 28 [NOTE, log # will be different on a per/appliance basis]
   Please enter the name for the log:
   [updater_logs]>
   Log level:
   1. Critical
   2. Warning
   3. Information
   4. Debug
   5. Trace
   [3]> 4
   [SNIP FOR BREVITY]
   ```

```
myesa_2.local> commit
```

2. Run a force update on either antispam (**antispamupdate force**) or antivirus (**antivirusupdate force**). `myesa.local> antivirusupdate force`

```
Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```

3. Finally, **tail updater_logs** and ensure that the appliance is able to reach the dynamichost as indicated: `Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-updates.ironport.com:443`

Troubleshoot

Complete these steps in order to troubleshoot any issues:

1. Ensure that the default **updateconfig** is used. If the vESA or host is behind a firewall, ensure that updates with a static server are in use.
2. Ensure that you can **telnet** to the dynamic host URL as chosen: `> telnet`

```
Please select which interface you want to telnet from.
1. Auto
2. Management (172.16.6.165/24: myesa_2.local)
3. new_data (192.168.1.10/24: myesa.local_data1)
[1]>
Enter the remote hostname or IP address.
[]> stage-stg-updates.ironport.com
Enter the remote port.
[25]> 443
Trying 208.90.58.24...
Connected to stage-stg-updates.ironport.com.
Escape character is '^]'.
^] ["CTRL + ]"]
telnet> quit
Connection closed.
```

Related Information

- **Content Security Appliance Upgrades or Updates with a Static Server**
- **Technical Support & Documentation - Cisco Systems**