Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=16101
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R75.40 home page (sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 May 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Data Loss Prevention R75.40 Hotfix Getting Started Guide).
Introduction

The Check Point R75.40 Data Loss Prevention Hotfix lets DLP use Monitor Mode on Gaia or SPAN port scanning on SecurePlatform.

After you install the DLP hotfix, the gateway can run scans simultaneously. SMTP scan on SPAN ports and on emails from Outlook clients sent to the gateway with an add-in.

You can enable the Anti-Bot, IPS and Application Control Software Blades with the Hotfix, for demonstration purposes only.

**Note** - SMTP or HTTP Tap Mode can be deployed as a supportable configuration on DLP-1 appliances. For other gateways (and appliances), after this hotfix is applied and Tap mode enabled, it can only serve as a demo. The gateway cannot replace a production firewall.

When you uninstall the hotfix, the gateway reverts to the state it was in before the hotfix installation.

Installation

If you have a DLP Security Gateway with an earlier hotfix installed, you must uninstall it before you upgrade to R75.40 and install this hotfix. See the uninstall instructions below.

Make sure the Security Gateway is on a version R75.40 SecurePlatform or Gaia Open Server, or UTM-1 or Power-1 appliance.

**Note** - During installation or uninstallation, the dlp.conf file is restored to its default state. If you changed this file, keep a copy. After installation, review which changes to carry over.

To install this hotfix:

1. Open a shell on the gateway.
2. Run the installation executable: `fw1_wrapper_HOTFIX_FIBER_DLP_HF_001_986026001_2`
   The Welcome text shows.
3. Press Y.
   Check Point services are stopped (`cpstop`) automatically.
4. Wait for installation to finish and then reboot the Security Gateway.

To uninstall the DLP Hotfix:

1. Run the uninstall script:
   - To uninstall the hotfix on R75.20, before upgrading to R75.40:
     `/opt/CPsuite-R75.20/uninstall_fw1_wrapper_HOTFIX_FLOW_DEMOTOOLS_HF_001`
   - To uninstall this hotfix to upgrade to a higher version:
     `/opt/CPsuite-R75.40/uninstall_fw1_wrapper_HOTFIX_FIBER_HF_001`
   Check Point services are stopped automatically (`cpstop`).
   All hotfix-related files are removed, and the Security Gateway is reverted.
2. Wait for uninstallation to finish and then reboot the Security Gateway.

Configuring Monitor Mode on Gaia

Monitor Mode lets a Security Gateway listen to traffic from a Mirror port or Span port on a switch. To configure Monitor Mode on the Gaia operating system, use the instructions in sk70900
(http://supportcontent.checkpoint.com/solutions?id=sk70900)
Configuring SPAN Port on SecurePlatform

DLP Tap mode for SMTP scanning scans traffic only on interfaces that are defined as SPAN ports on SecurePlatform, or use Monitor Mode on Gaia.

**To configure on Tap mode:**
1. Open a shell on the gateway.
2. Run: `sysconfig`
3. Enter the number for **Network Connections**.
4. Enter the number for **Configure Connection**.
5. Select the interface to connect to the SPAN port on the switch, .
6. Press 5 (Define interface as connected to a mirror port).
   If the interface has an IP address, remove it.
7. Finish the sysconfig options.
8. Install policy.

TAP Mode Traffic Scanning

This DLP hotfix lets the Security Gateway scan SMTP and HTTP traffic in TAP mode on SPAN ports. The DLP Software Blade is usually deployed Inline, as part of a Security Gateway or as a dedicated DLP gateway. With the DLP hotfix, you can connect a DLP gateway to a SPAN port of a switch.

The DLP gateway scans for DLP incidents in SMTP traffic (emails) and HTTP passing through this switch, with minimal deployment risks. This lets you run a full data leak assessment of all outgoing SMTP traffic of your organization.

How It Works

The DLP Security Gateway is connected to a SPAN port of the switch. The gateway gets a copy of all packets that go through the switch. The DLP tap mechanism builds TCP streams of SMTP traffic. These are scanned by the DLP engine, according to the installed DLP policy.

**Known Limitations:**
- HTTPS connections cannot be scanned.
- Exchange Agent cannot use the TAP interface during the TAP mode traffic scan. It requires a different interface.
- Sometimes large emails are not scanned. This is usually a result of switch mirror port that fails to transmit all packets to the DLP gateway. That occurs because the mirror port usually gets the lowest priority (compared to other switch ports).

**To configure and deploy:**
1. Configure the gateway:
   - Gaia: Configure Monitor Mode ("Configuring Monitor Mode on Gaia" on page 5)
   - SecurePlatform: Configure SPAN port
2. Set up network environment ("Network Environment" on page 7).
3. Configure the gateway.
Network Environment

Connect the mirror port interface of the Security Gateway to a SPAN port on the switch where the SMTP and HTTP traffic passes.

If necessary, configure the port on the switch to be a SPAN port and duplicate the incoming and outgoing packets.

**Example 1:** Configure Cisco switch to duplicate packets from 0/2 fast eth interface to 0/3 fast eth interface:

```
C2950(config)#monitor session 1 source interface fastethernet 0/2
C2950(config)#monitor session 1 destination interface fastethernet 0/3
```

**Example 2 (Virtualization):** In Virtualization environments, enable **Promiscuous** mode in the virtual switch network.

- **Note** - The Security Gateway must have network access for DLP to be able to function (for example, SSH Shell connections, LDAP access, UserCheck access, mail relay access to send emails to data owners).

Gateway Configuration

Configure DLP as usual: turn on the DLP Software Blade for SMTP, HTTP, or SMTP and HTTP traffic. We recommend that you review the DLP data types. Add relevant data types to the DLP rule base and create new data types. Do these procedures in the SmartDashboard.

**DLP Rule Base:**

Tap mode is a passive mode, so Prevent and Ask User actions are not supported. If the action of a rule is Prevent or Ask User, it is internally converted to Inform.

- **Important** - In Tap mode, you must not use Watermark.

**My Organization Network Definition:**

- If you define My Organization as **These networks and hosts only**, it works as expected.
- If you define it as **Anything behind the internal interfaces of my DLP gateway**, all emails that pass through the mirror port are scanned. This does not include emails coming from hosts or networks defined in the exclusion list.

To have better control of the scanned traffic, define the network according to **networks and hosts**, and not according to topology.

**My Organization Email Domain Configurations:**

Make sure that all the organization email domains are defined in the **Email addresses or Domains** section of My Organization. Only these domains are scanned by DLP.
SmartView Tracker:

After you install and activate the DLP hotfix, launch SmartView Tracker to see the DLP logs for scanned emails.

Security Policy:

When using the DLP hotfix for TAP mode, the gateway cannot function as a production firewall, and it must be deployed behind the production firewall. We recommend an Any-Any-Any-Accept policy. Packets are not dropped or rejected as a result of the rule base of TAP mode computers.
SmartEvent and Reporter Suite:
You can deploy the DLP hotfix for Tap mode in a standalone configuration. If you do, you can activate SmartEvent and use it to see DLP events. You can configure SmartReporter to generate DLP reports.

To activate SmartEvent and Reporter Suite in sysconfig:
1. Launch shell access to the gateway.
2. Run: `evconfig`
3. Enable SmartEvent, SmartEvent Correlation Unit, and SmartReporter.
4. Save and exit.

To activate SmartEvent and Reporter Suite in SmartDashboard:
1. Launch SmartDashboard and edit the gateway object.
2. In General Properties > Management, select SmartEvent, SmartEvent Correlation Unit, and SmartReporter.
3. Follow the on-screen instructions.

Enable or disable Tap mode scanning of SMTP traffic for DLP:
After you install the DLP hotfix, Tap mode is enabled by default. Do these steps in the command line (not the SmartDashboard).

To disable Tap mode:
1. Open `$DLPDIR/config/dlpt_policy.conf`
2. Change the enabled value to 0 (zero).
3. Install Policy.

Scanning Microsoft Outlook Emails

With the new Check Point Outlook Add-in, you can easily see how DLP works for SMTP. You can easily show the potential great value of DLP by finding incidents in already-sent emails.

How It Works

The Check Point Outlook add-in has online and offline scanning. In these modes, you can configure the add-in to scan only emails destined for external recipients, or to scan all emails.

Online scan intercepts an email when the user clicks the Send button. Before the email is actually sent to its destination, it goes to the configured DLP gateway. The gateway scans the email according to the policy and sends the action to the add-in. If the action is Prevent or Ask User, the email is moved to the Sent Items folder, without actually being sent.

Offline scan opens a Search window, which lets you select the folder you want to scan (Sent Items, by default) and the period of time. After you click the scan button, the folder is searched for matching emails. These emails are sent to the gateway for inspection.

A new Outlook folder, Check Point Outlook Add-In, is created. Emails with DLP violations are copied there with categories for the action. Ask actions are converted to Inform (the mail is already sent and there is no reason to send it again).

Known Limitations:
When Outlook is offline, or the gateway is unreachable, the user gets a message, asking whether to send the email without scanning it. Emails are not scanned after leaving the Outbox folder.

To configure and deploy:
1. Install the Add-in.
2. Configure Microsoft Outlook Scanning.
Installing the Add-in

The add-in is packaged in an MSI file. Double-click this file and follow the wizard. The wizard asks you to give the name or IP address of the Check Point DLP gateway. You can enter it, or leave it empty and specify it later from the Outlook add-in settings. If Outlook was running during the installation, restart it to see the add-in.


Configuring Microsoft Outlook Scanning

Make sure the firewall rule base on the gateway allows a connection on port 25 from the Outlook machine to the gateway.

The Add-in Toolbar:

- In Outlook 2003, the add-in is added as a toolbar.
- In Outlook 2010, the toolbar is added to the Add-Ins ribbon. To keep the toolbar always visible, right-click it and select Add Group to Quick Access Toolbar.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>About</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Enable realtime scan</td>
<td>Start online scan of emails.</td>
</tr>
<tr>
<td>3</td>
<td>Disable realtime scan</td>
<td>Stop online scan of emails.</td>
</tr>
<tr>
<td>4</td>
<td>Scan Folder</td>
<td>Start offline scan of emails.</td>
</tr>
<tr>
<td>5</td>
<td>Settings</td>
<td>Configure the gateway and type of emails to scan.</td>
</tr>
</tbody>
</table>

Configuring the add-in:

If you did not configure the IP address or name of the Security Gateway during installation, you must do it before starting the real-time scan.

To configure the Check Point Outlook Add-in settings:
1. Click Settings in the Check Point Add-in toolbar.
2. Enter the IP address or name of the Security Gateway.
3. Select which messages to scan:
   - External only
• External and Internal

4. Click OK.

Starting the scans:

After you click **Enable realtime scan**, each message you send is scanned once, when you click **Send**.

To start an offline scan:

1. Click **Scan folder** in the Check Point toolbar.

   In the window that opens, you can override the gateway configurations (gateway name and external/internal messages option).

2. Select the period of time to match emails to scan.

3. Browse to the folder to scan.

4. Click **Scan Folder**.

5. If the DLP Security Gateway finds emails with violations, they are copied to the new **Check Point Outlook Add-In** folder. The results show in the result pane. Each email gets a new category, for the action taken and the most restrictive rule name.

You can delete this folder at any time. It will be created again only if you run the Offline scan again.