How To Enable DLP on a Gateway
Objective

This will show you how to enable the DLP (Data Loss Prevention) Software Blade on your Check Point Security Gateway.

Supported Versions

- R71 up to R77

Supported OS

- Gaia
- IPSO
- SecurePlatform
- Windows 32 bit / 64 bit

Supported Appliances

The dedicated DLP Gateway is supported on:

- DLP-1 9571
- DLP-1 2571

SecurePlatform Open Server, with these minimum requirements:
- Intel® Xeon® processor 5100 series CPU equivalent or higher, at least 2 cores
- 4GB RAM
- 250 GB Hard disk

The UserCheck client application is supported on these Microsoft Windows platforms:
- XP Pro (SP3)
- Server 2003 (SP1-2)
- Vista (SP1) 32-bit
- Server 2008 (SP1)
- Windows 7 32-bit and 64-bit
Related Documentation

sk73660: ATRG: Data Loss Prevention (DLP)

Impact on the Environment and Warnings

The port for the DLP gateway on SecurePlatform, for the HTTP WebUI Management, is HTTPS 4434. You must open this port in the policy installed on the gateway.

Enabling DLP on Your Gateway

Requirements

- Security Management Server
- SmartDashboard
- Check Point Security Gateway or a DLP-1 appliance
  In a dedicated DLP gateway deployment, we recommend that you have a protecting Security Gateway in front of the DLP gateway. In this example, we are using an integrated gateway.
- DNS Server

Enabling DLP

1. In the gateway properties window, click Network Security > Data Loss Prevention.

The Data Loss Prevention Wizard opens.
2. Click **Next**.
   The Email Domain step lets you give your domain. This lets the DLP gateway distinguish between internal and external email addresses.
3. Enter the domain of your organization.
   The Organization Name step lets you identify your organization in different ways. These names are used by the DLP feature to accurately detect incidents of data loss.
4. Enter different names and phrases used to identify your organization.

In the Portal and Mail Server step, activate the portal to get messages from the DLP gateway, through the Mail server.
5. Select **Activate DLP Portal for Self Incident Handling**.
   The default URL is: https://<Gateway IP>/dlp

6. Select **Mail Server** and enter the DNS name or IP address of your organization's mail server.
   In the Protocols step, select the services to be scanned by DLP.
7. Select **Email**.
   This is the minimum for DLP protection.
   You can also select **Web** or **File Transfer**, or both. DLP scanning on HTTP posts and FTP can impact performance.
8. Click **Finish**.