

CHAPTER 6: PROVIDER-1 LOGGING FEATURES

.....

Provider-1 enables real-time event tracking and management for an expanding customer base. A centralized logging system provides detailed information on network activity for all customer sites. An Administrator can configure logging for each customer, or for each individual CMA.

This section describes how to set up a Customer Log Module (CLM) for log management, using Provider-1.

Objectives

1. Define a CLM.
2. Describe the steps needed to configure a CLM in a Provider-1 environment.
3. Describe the steps needed to install and configure an MDS MLM in a Provider-1 environment.



Key Terms

- Customer Log Module
- Multi-Domain Log Module



LOG MANAGEMENT

By default, all Security Gateway logs are sent to the CMA. Log management can also be performed by the following modules:

Customer Log Module (CLM) — A CLM collects log data for managed Security Gateways. It can be deployed on customer premises and at the NOC.

MDS Multi-Domain Log Module (MDS MLM) — The MDS MLM is configured similarly to the primary MDS. Multiple CLMs can be configured on each MDS MLM so that each CMA has a separate log repository.

Provider-1 logging deployment is dependent upon site-specific considerations, such as:

- NOC network layout.
- Bandwidth conditions.
- Machine-load status.
- Desired log manageability.

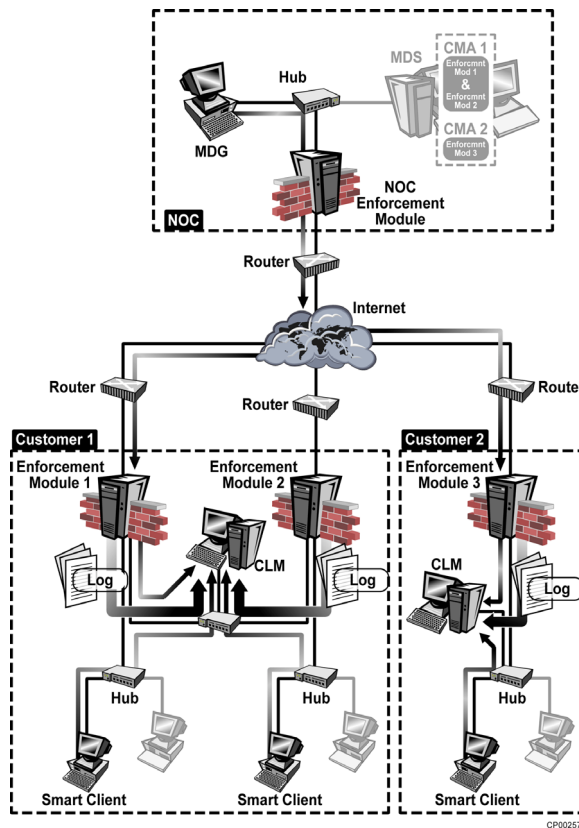
The SmartView Tracker can connect to any log server, including the individual CLMs or CLMs loaded on an MDS MLM, and display information about logged traffic events and Security Policy installations.

Logs can be sorted to identify events of interest, or can be exported to other applications. The standard NGX log commands are available for efficient management.

CUSTOMER LOG MODULE

CLMs located at remote customer sites collect logs from the remote Security Gateways, allowing real-time event tracking and management. The MDG SmartView Tracker allows Administrators to view network activity for remote sites.

In the figure, a CLM is installed at each customer site. The SmartView Tracker is also installed at the NOC, on the MDG. From the NOC, the SmartView Tracker is used to manage log files retrieved by the CLM. Client SmartView Trackers can also be installed to let clients view their logs locally.



CLM Deployment



If the CLM is installed outside the NOC, CLM data is not separated by CMA or Customer. All logs sent to the CLM display together when viewed by the customer or the MDG SmartView Tracker.



The CLM maintains NGX log files *only*. It does *not* install the Security Policy on a customer's remote Security Gateways.

Check Point recommends each customer have at least one CLM for each CMA managed by Provider-1. If the CLMs are separate Management Servers installed on the customer site, or if the CLMs reside at the NOC, all CMA specific data should be kept separate.

MULTI-DOMAIN LOG MODULE SYSTEM

The MDS MLM is installed at the NOC to collect logs for each managed CMA. Unlike the CLM installed at the customer site, CLMs loaded on the MLM separate logs from each managed CMA. Although multiple Security Gateways can be logging to a single log repository, all logs are kept in distinct, CMA-specific databases. Not only is a customer's sensitive data protected, keeping the logs separated by CMA enhances the Administrator's ability to troubleshoot potential issues identified in the logs.

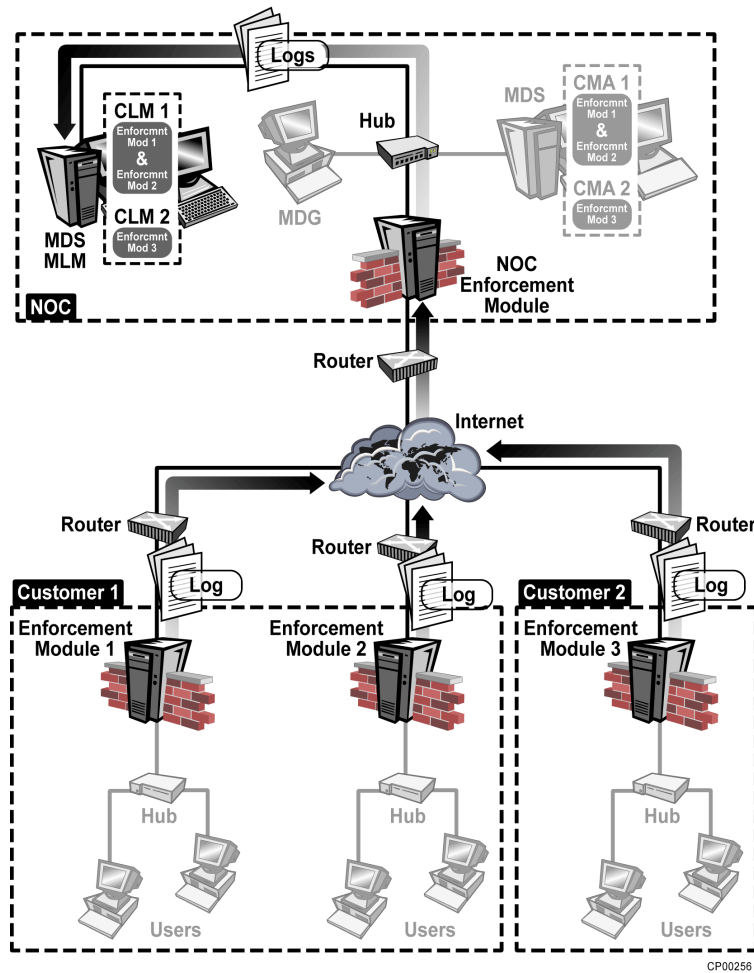


Each Customer must have at least one CMA configured before a CLM can added. The CLM must also reside on a different MDS as the CMA.



MLM Deployment

Each MDS MLM can manage up to 250 CLMs. The MLM is only limited by the number of CLMs. An unlimited number of CMA managed Security Gateways can be configured to log to the CLMs loaded on the MLM.



MLM Deployment

The purpose of the MLM is to separate all logging traffic from system-critical traffic, while allowing the Administrator greater flexibility in configuring logging for customer CMAs. The process of adding new CLMs to the configuration is similar to the process of adding CMAs to an MDS.



Provider-1 supports Eventia Reporter Reports. An Eventia Reporter Server is installed on a separate machine and then configured in the Provider-1 environment.

Using Eventia Reporter

Eventia Reporter can produce both Log Based reports and Express reports for modules managed by Provider-1 CMAs. Use Eventia Reporter to create selected reports for specified customers and modules.

The Eventia Reporter delivers a user-friendly solution for auditing traffic and generating detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for events logged by CMA-managed gateways that are running SmartView Monitor. Eventia Reporter produces reports for these modules.

Reports can be scheduled at any time, and can be sent by e-mail or uploaded to an FTP site. Eventia Reporter needs to be properly configured to work with Provider-1, see the *Getting Started* chapter of the *Eventia Reporter User Guide* for further details.

REPORTING SERVER PROCESSES

The Eventia Reporter Add-on for Provider-1 doesn't have its own package. It is installed, removed, enabled and disabled using the `SVRSetup` script provided with MDS installation. When the Eventia Reporter Add-on for Provider-1 one is used, the Eventia Reporter Server maintains a connection to the MDS. Whenever reports are generated, another component called Eventia Reporter Generator opens a connection to the MDS as well.