

***Check Point Software Technologies  
LTD.<sup>TM</sup>***

***Customer Log Module,  
Remote Logging  
Utility***

***Efficient Network  
Utilization***

## **Customer Log Module**

The Customer Log Module (CLM) was designed to allow customers or remote locations to view logs that recorded from their Internet/Intranet/Extranet Firewall. Typical management revolves around a Management Console/Customer Managed Add-on (CMA/MC) managing a number of firewalls. These firewalls inspect traffic, accept or reject based on the installed rulebase, and log the event to its corresponding CMA/MC.

When existing connections, R1 shown in Figure1, are T-1 through DS3 connections, there generally is not a problem with the typical management model. There is plenty of bandwidth available allowing the customer to use a log viewer to connect to the CMA/MC and view the existing logs. However, when a 56k Internet Connection is tasked with logs and log viewer requests, the remote site A or B typically experiences bottleneaking or network congestion.

The CLM, a scaled down Management Console, allows the customer to connect to a management console located at their facility. Logs may be sent to any of the following:

- \* Management Console/Customer Managed Add-on
  - \* Logs are sent to the MC/CMA by default.
- \* Customer Log Module
  - \* FW-1 V4.0 SP5 allows for a "\$FWDIR/conf/loggers" file to be created. This file will control where logs will be sent when the firewall system boots.
- \* Maintained on the Firewall (Logs are stored on the local firewall for off-hour processing)

Any one or all of the above may be utilized at the same time.

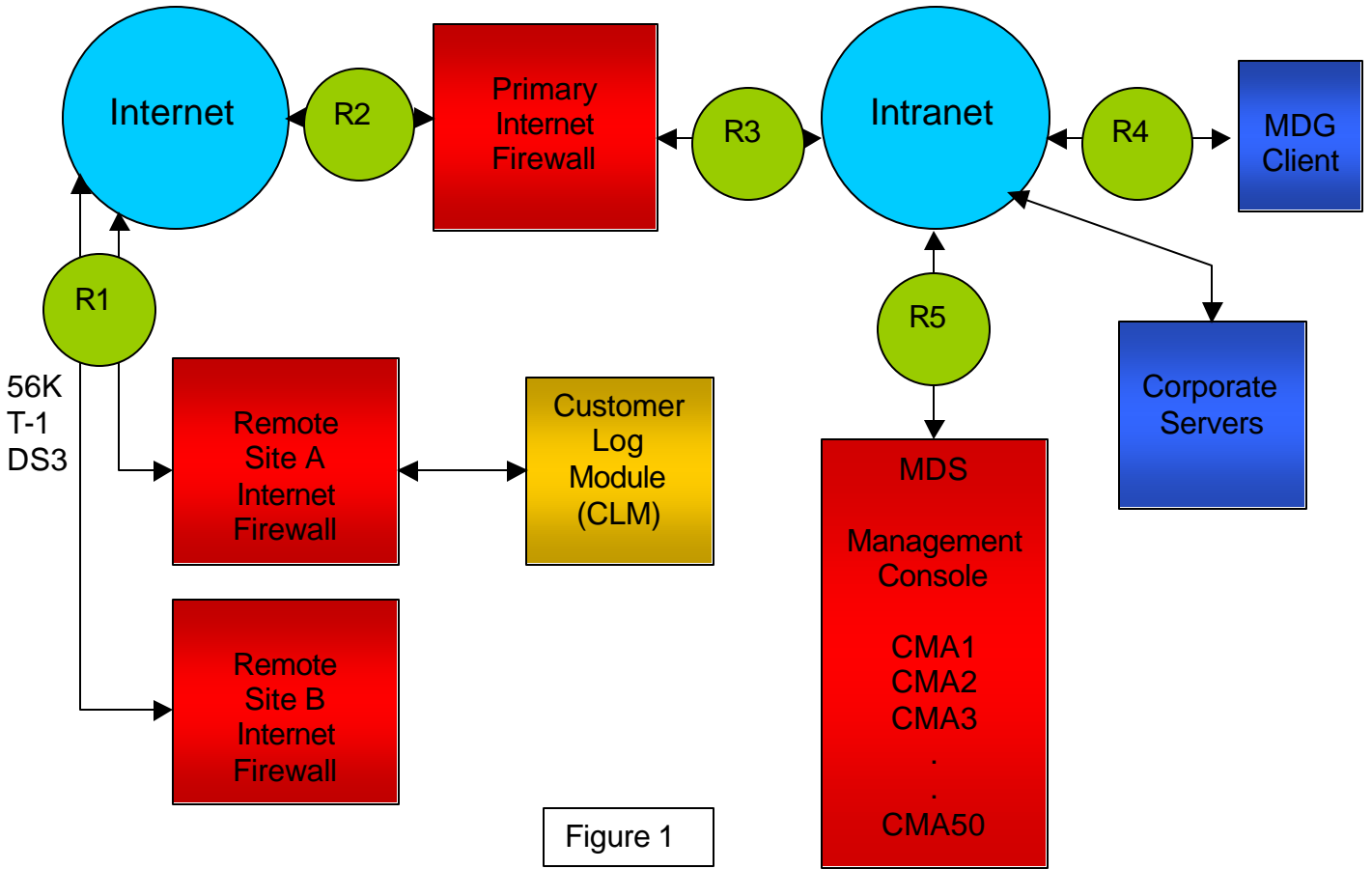


Figure 1

# Customer Log Module Architecture

The CLM exists today on any system that runs a Management Console. (AIX, HPUX, Solaris, NT, ...) Figure 2 shows a CLM residing on an NT system. Both Customer A and Customer B firewalls report logs back to the respective CMA and the CLM.

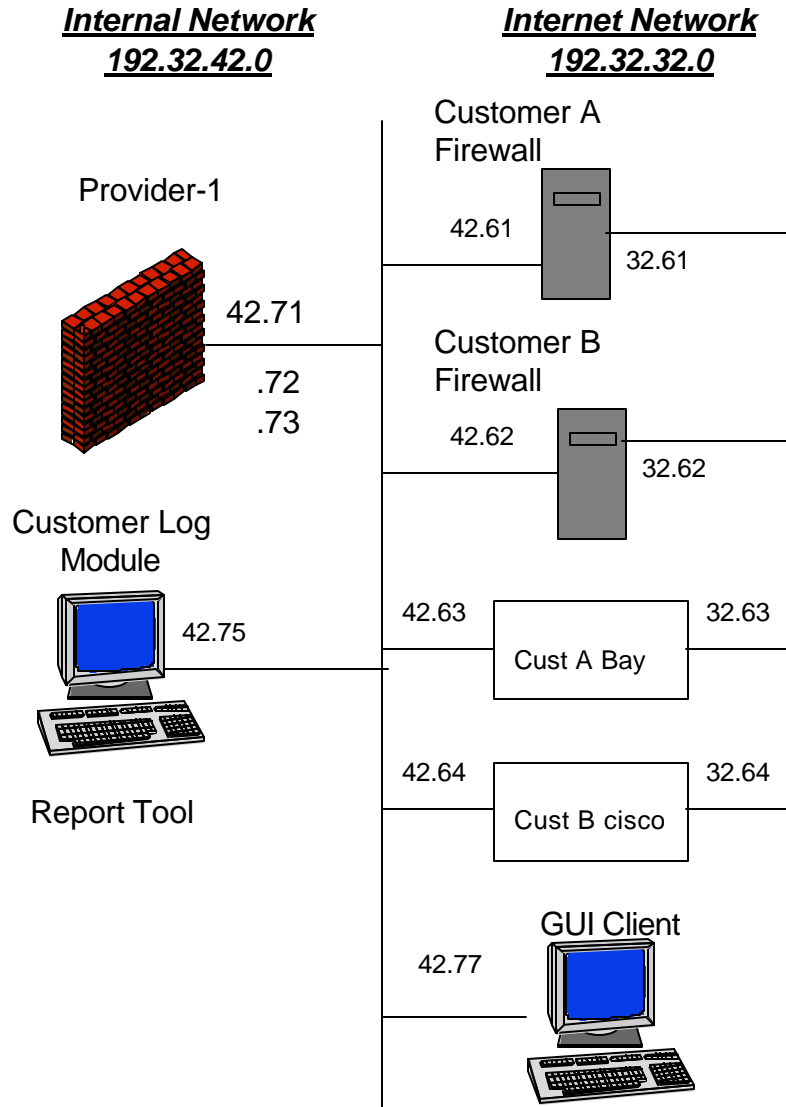
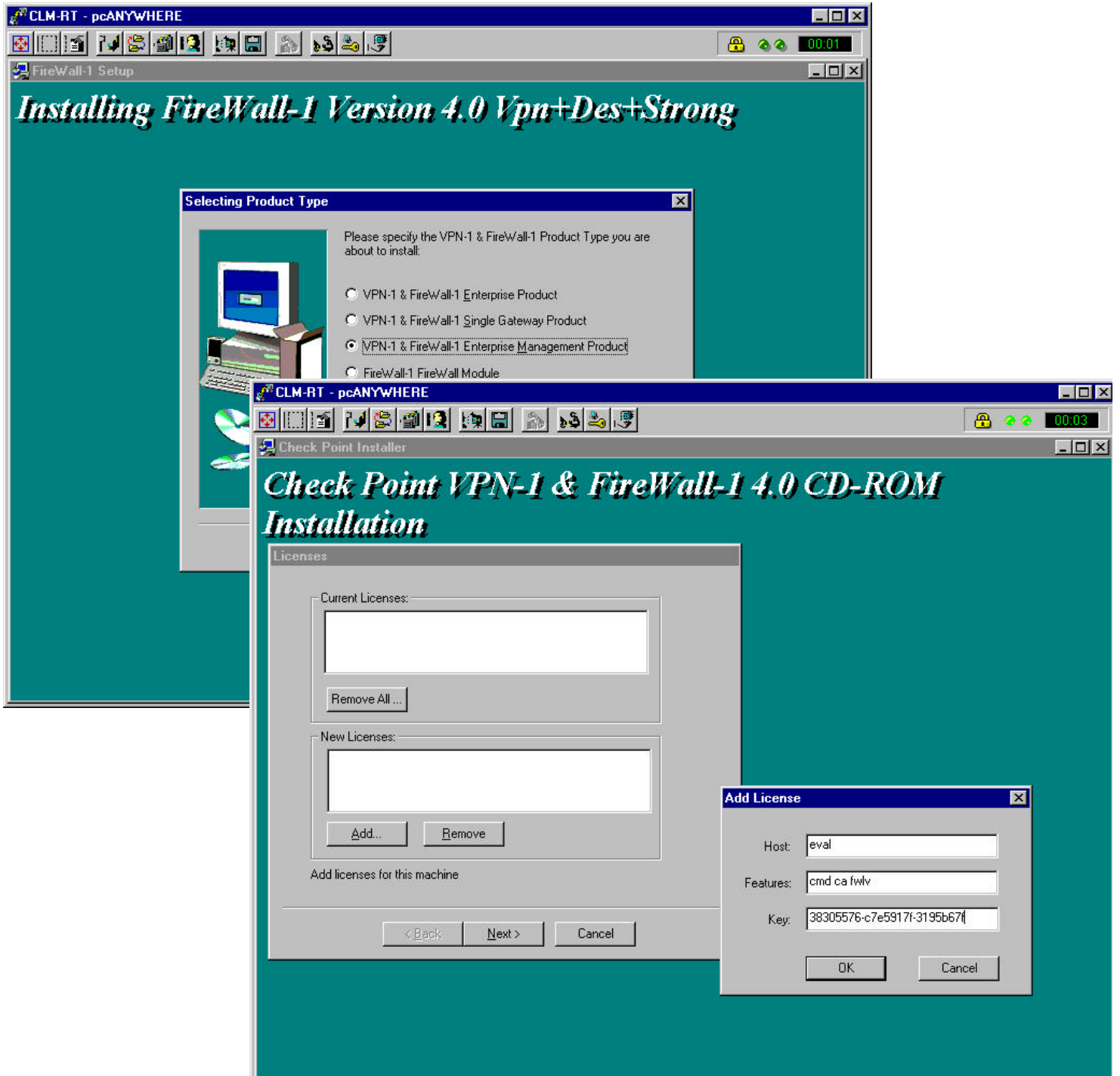


Figure 2

# Installation

The installation process is no different than installing a management console.

1. Install Firewall-1
2. Install Service Packs
3. Configure Licenses, GUI Clients, Remote Modules, Administrators
4. Login to the CLM



**fw.log - VPN-1 & FireWall-1 Log Viewer**

File Edit View Select Window Help

Log

No.	Date	Time	Inter.	Origin	Type	Action
0	11Oct1999	12:45:33	dae...	CLM-RT	control	ctl
1	11Oct1999	13:18:49	dae...	CLM-RT	control	ctl
2	11Oct1999	13:18:55	dae...	CLM-RT	control	ctl
3	11Oct1999	12:52:53	N10...	192.32.42.62	control	ctl
4	11Oct1999	12:52:53	N10...	192.32.42.62	log	accept
5	11Oct1999	12:52:53	N10...	192.32.42.62	control	ctl
6	11Oct1999	12:52:54	N10...	192.32.42.62	log	accept
7	11Oct1999	12:54:34	N10...	192.32.42.62	log	accept
8	11Oct1999	12:54:34	N10...	192.32.42.62	log	accept
9	11Oct1999	13:21:06	dae...	CLM-RT	control	ctl
10	11Oct1999	13:21:24	N10...	192.32.42.61	control	ctl
11	11Oct1999	13:21:24	N10...	192.32.42.61	log	accept
12	11Oct1999	13:21:24	N10...	192.32.42.61	log	accept
13	11Oct1999	13:21:24	N10...	192.32.42.61	log	accept
14	11Oct1999	13:21:25	N10...	192.32.42.61	control	ctl
15	11Oct1999	13:21:26	N10...	192.32.42.61	log	accept
16	11Oct1999	13:21:26	N10...	192.32.42.61	log	accept
17	11Oct1999	13:21:26	N10...	192.32.42.61	log	accept
18	11Oct1999	13:26:26	N10...	192.32.42.62	log	accept
19	11Oct1999	13:26:26	N10...	192.32.42.62	log	accept
20	11Oct1999	13:26:26	N10...	192.32.42.62	log	accept

For Help, press F1

logview.fw 192.32.42.75 NUM

**VPN-1 & FireWall-1 Login**

Welcome to  
**Check Point VPN-1 & FireWall-1**  
 Log Viewer  
 version 4.0

User Name:

Password:

Management Server: