

***Check Point Software Technologies
LTD.TM***

***Migration from Enterprise Management
To
Multi Domain Management***

Provider-1

3.0/4.0 Enterprise Migration

The typical management model for Check Point customers revolves around a GUI Client that connects to a Management Console (MC) that may or may not exist on the Firewall. For this demonstration, the Firewall and MC will exist on the same system. (Note: The process is the same regardless of MC location)

The MC maintains all the files that define corporate policy, users, and objects for the corporate Intranet. (Figure 1)

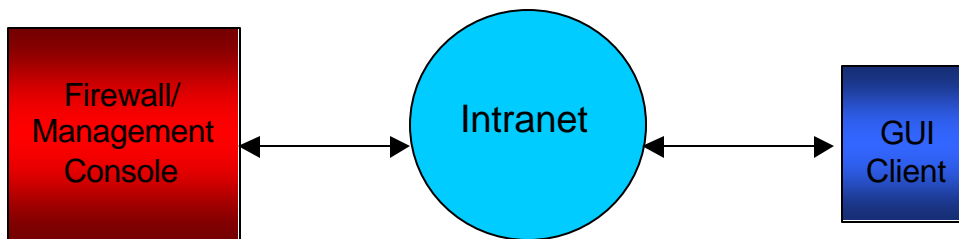


Figure 1

With Internet connectivity costs falling, global corporations are moving from costly backbone connections to conducting day to day business across the Internet. Changes in Internet Standard Operating Procedure (SOP) for connectivity have also driven change in Security SOP. Figure 2 demonstrates how corporate server access has changed from backbone to Internet access. The change in access also drives changes in security. With typical management, figure 1, the corporate management team is responsible for policy creation, user access control, and bandwidth management for all Firewalls, remote and local.

Check Point Provider-1 integrates multiple remote FireWalled networks within a management framework. Network Security, responsible for several FireWalled Networks can configure and monitor a Remote Location Security Policy and network activity from a single Network Operation Center.

Provider-1 maintains multiple FireWall-1 Management Servers on a single server, known as the Multi Domain Server. Each Management Server receives a virtual IP address and controls any number of FireWall Modules located at a Remote Corporate site. Each Site receives one Management Server. In this way, FireWall-1 databases for many Sites are maintained at a single administrative station, while preserving distinctions between specific locations

A simple user interface enables centralized Remote location management. FireWall-1 Remote Location, Management Servers and FireWall Modules are displayed in a hierarchical tree, providing a graphical overview of all system objects. Remote properties are easily configured and updated, simplifying management tasks.

Flexible client/server architecture enables the remote execution of FireWall-1 Management commands. The Management team can launch the FireWall-1 Graphical User Interface for any Remote Location, enabling remote configuration and management of the enterprise Security Policy. The GUI displays alert and status information for all FireWall Modules, allowing Corporate Administrators to monitor multiple networks from a single site.

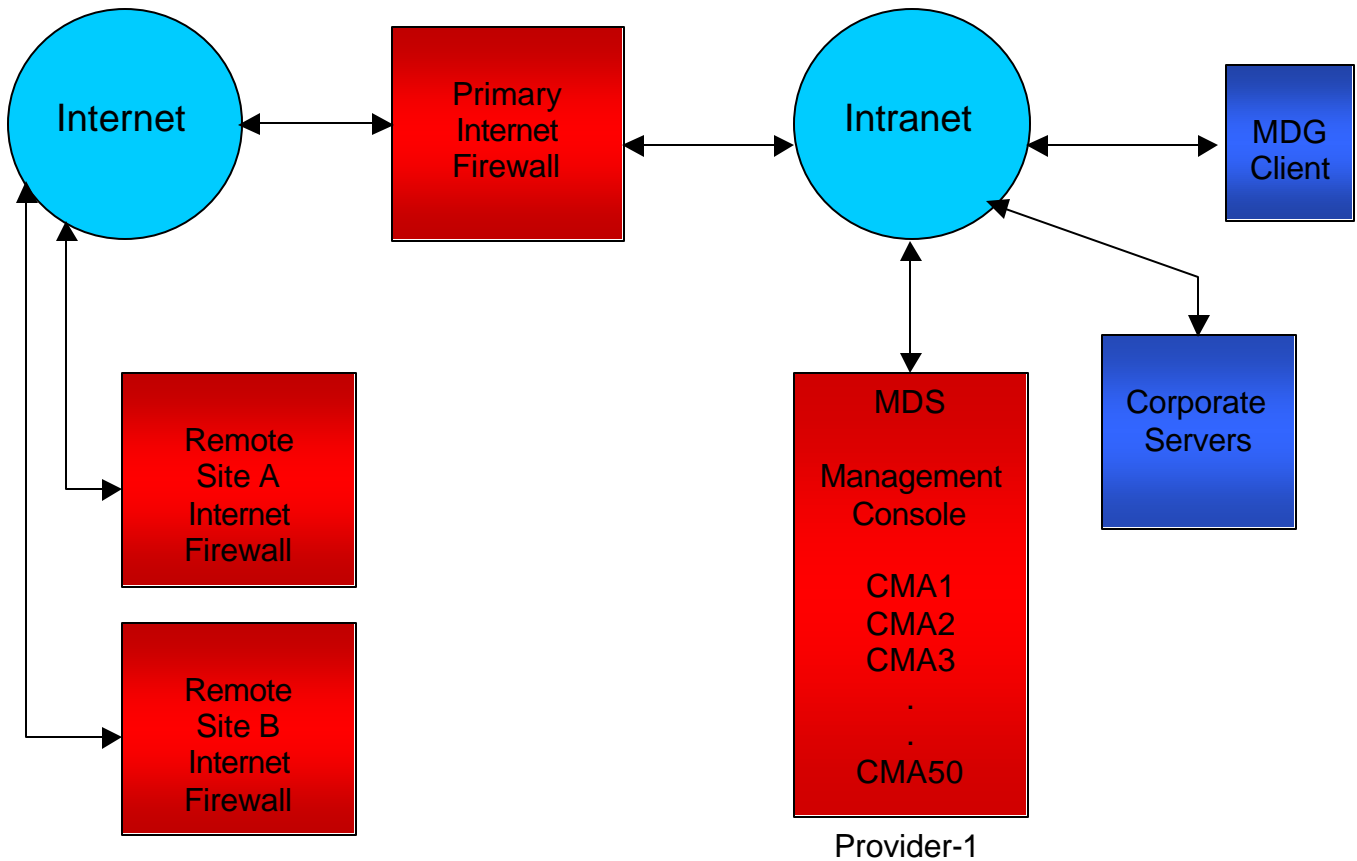


Figure 2

Provider-1 Architecture

Components

The Provider-1 system consists of four components:

- * Graphical User Interface (GUI)
- * Multi Domain Server (MDS)
- * Customer Management Add-on (CMA)
- * Remote Modules

Graphical User Interface

The GUI enables the remote management of multiple FireWall-1 customers. Provider-1 GUI Administrators assign and configure a FireWall-1 Management Server for each Customer. Customer properties are configured in terms of FireWall-1 Management Server properties, Licenses, Certificate Authority Keys, FireWall-1 GUI Clients, and FireWall Modules. The Management Server can be activated using the standard FireWall-1 Management commands. Administrators can launch the FireWall-1 Security Policy, Log and Status views to modify the Security Policy of a specific Customer. The GUI provides an overall view of Customer status and configuration. Customer properties are configured and maintained on the GUI. Customers and their respective Management Servers and FireWall Modules are represented as a tree, enabling simple, centralized management of any number of Customers. All alerts from a FireWall-1 Management Station can be viewed and managed through the GUI.

Multi Domain Server (MDS)

The Multi Domain Server is a single machine hosting multiple FireWall-1 Management Servers, known in Provider-1 as Customer Management Add-ons. Each Management Server is assigned a virtual IP address. All FireWall-1 components, such as the FireWall-1 GUI, communicate through the virtual IP address as if it is a standard standalone FireWall-1 version 4.0 Management Server.

The MDS resides at the Network Operation Center, and retrieves Customer status and alert information from the Management Servers. Customer properties are defined on the GUI and saved to the MDS.

Customer Management Add-on (CMA)

The Customer Management Add-on is a FireWall-1 version 4.0 Management Server. The CMA resides on the Multi Domain Server, and is designated by a virtual IP address. One CMA controls any number of FireWall Modules for a single FireWall-1 Customer. Each CMA maintains the Security Policy, User Database, Certificate Authority for the FireWall Modules it controls. The FireWall Modules are located on the Customer's site, while the CMAs reside on the Multi Domain Server, located at the Network Operation Center.

Remote Module

A Remote Module is a network object on which the FireWall Module is installed. Remote Modules are located at the Customer's site. Each CMA receives alert and status information from the Remote Modules it controls. The Provider-1 GUI displays detailed alert data for all Remote Modules.

The FireWall-1 Security Policy, Log and System Status views can be launched from the Provider-1 GUI to enable remote security configuration and management. The FireWall-1 Security Policy can be defined and modified through the Provider-1 GUI. The FireWall-1 Rule Base, User Database, and Certificate Authority are maintained on the CMA. The CMA downloads the Security Policy to its Remote Modules, which protect the Customer's network.

Migration

Existing on a Sun Solaris System, the heart of Provider-1 is the Multi Domain Server (MDS). The MDS is the central host for many dedicated & isolated Firewall-1 Management Servers (CMA). Currently MDS's provide support for 100 CMA's per MDS with the ability to cascade MDS's together for unlimited virtual customer support.

Customer data is stored in \$FWDIR/customers directory. The CMA, Customer Managed Add-on, is the functional management server for customers. Each CMA can manage up to 1, 4, or an unlimited number of firewall-1 modules. Communication between the GUI, firewall module, and SR client act as if the CMA is a standalone FW-1 management console.

This demonstration will utilize the network referenced in figure 3.

Equipment necessary for Multi Domain Management:

Multi Domain Server:	Sun Sparc XX
Firewall: CLM (Customer Log Module):	Any system currently supporting FW-1 FW CLM
Reporting Module:	Any system currently supporting FW-1 MC
GUI Client:	Windows NT system (current release) Any system currently supporting FW-1 GUI

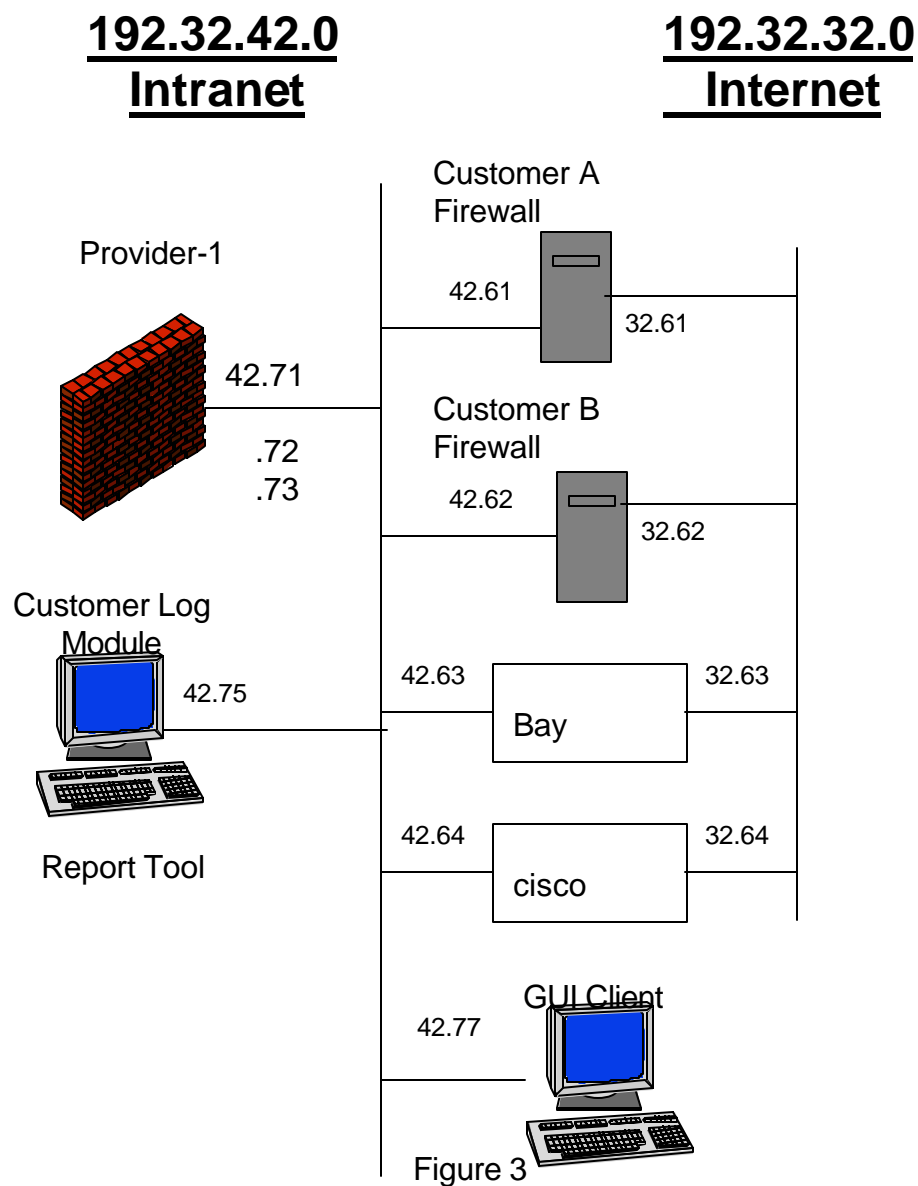
Configuration Overview:

1. Install Provider-1
2. Install Firewall GUI (Necessary if management is to be done on MC/MDS)
3. Create/Configure CMA's within MDS for Remote Firewalls
4. Copy required files from existing Management Console to MDS
5. Import/Confmerge data into MDS
6. Verify Policy for Remote Locations
7. Install policy from CMA to Remote Firewall
8. Convert/Remove old configuration files from Remote Modules

/etc/mds/customers/192.32.32.72 (management console address for customer A)
/etc/mds/customers/192.32.32.73 (management console address for customer B)

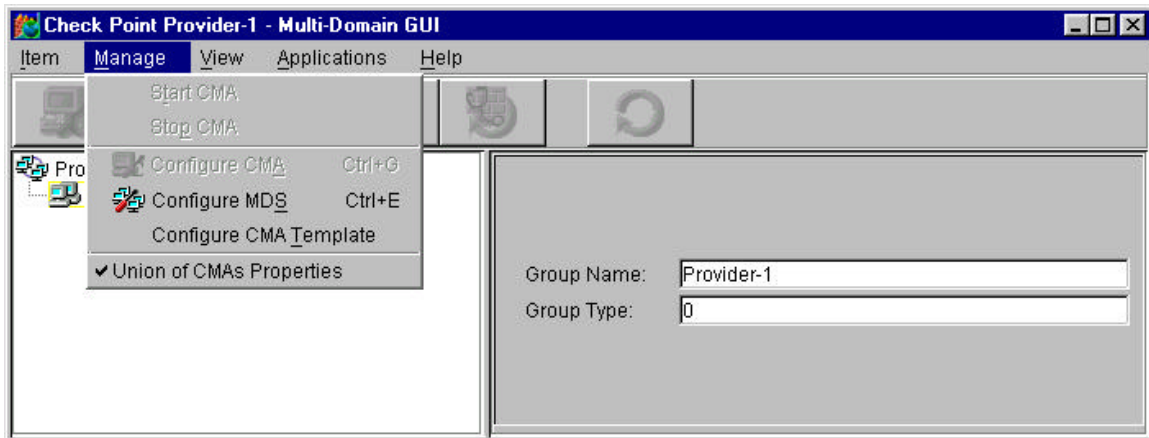
Where .72, and .73 represent the IP addresses of the management consoles for the customer firewalls on the Internet segment 192.32.32.0.

192.32.32.61 would have 192.32.42.72 as its management console.

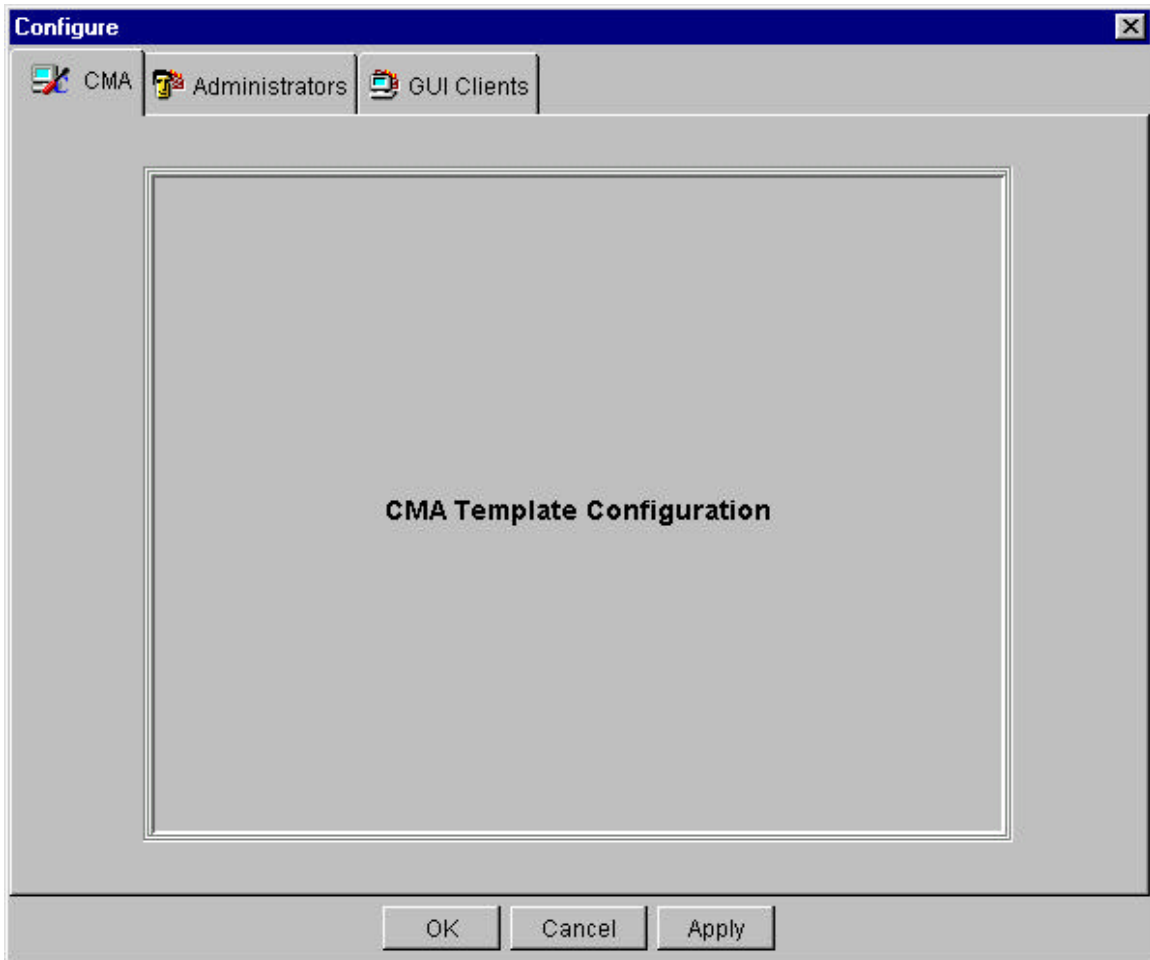
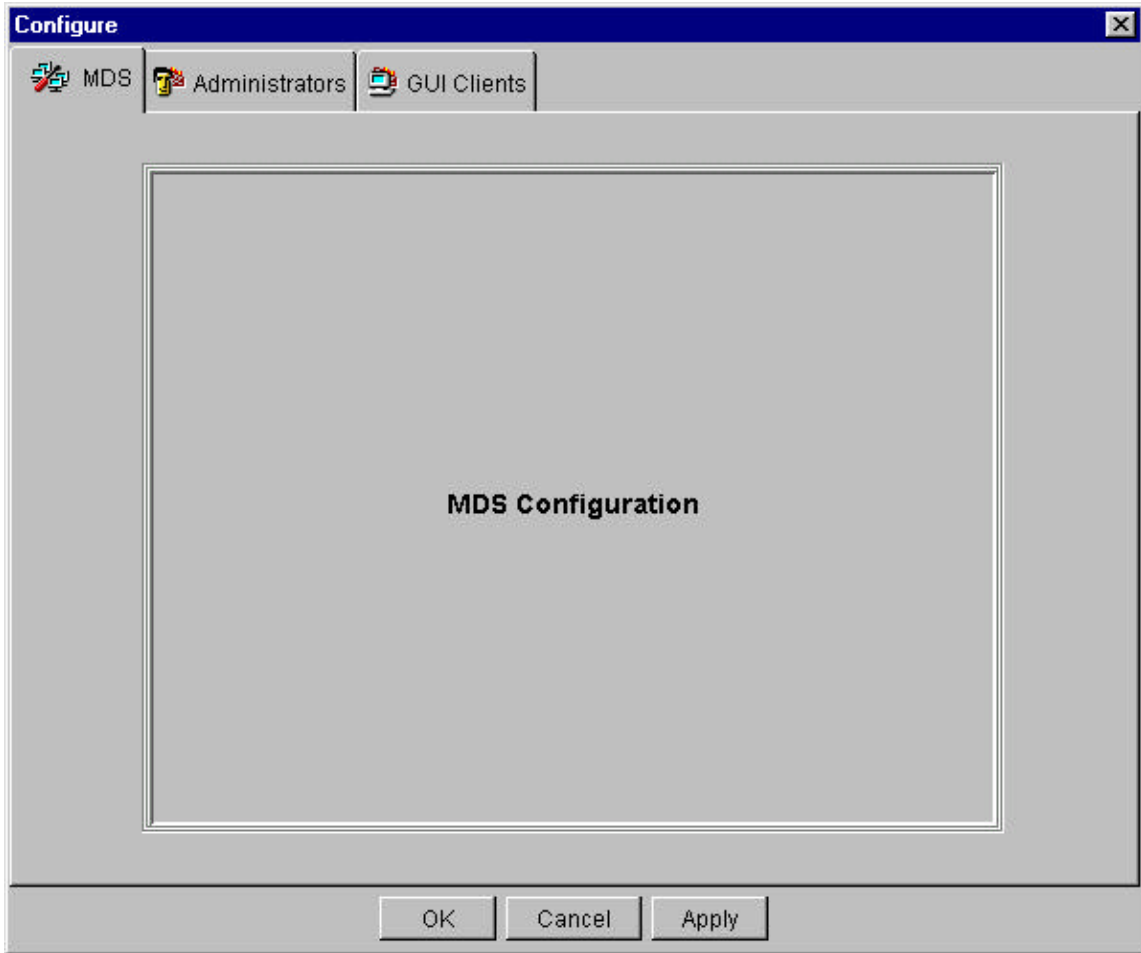


MDS Configuration

Before we can begin the migration process we must configure the MDS with both Customer A, which will be a new installation, and Customer B which will be a migration.

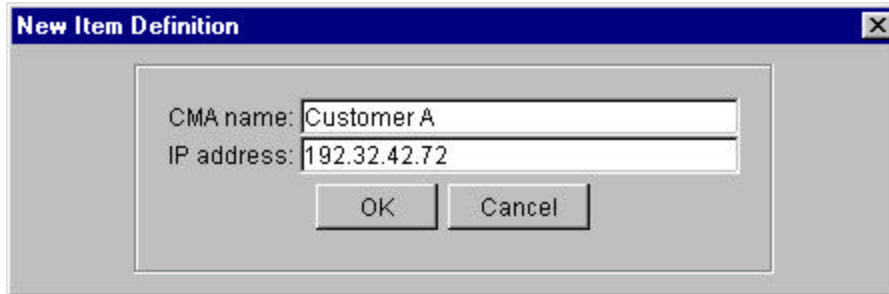


Starting with the Multi Domain GUI above we must configure the MDS and the CMA templates. MDS configuration sets the login parameters for administrators where CMA configuration templates set the login privileges for administrators within each CMA.



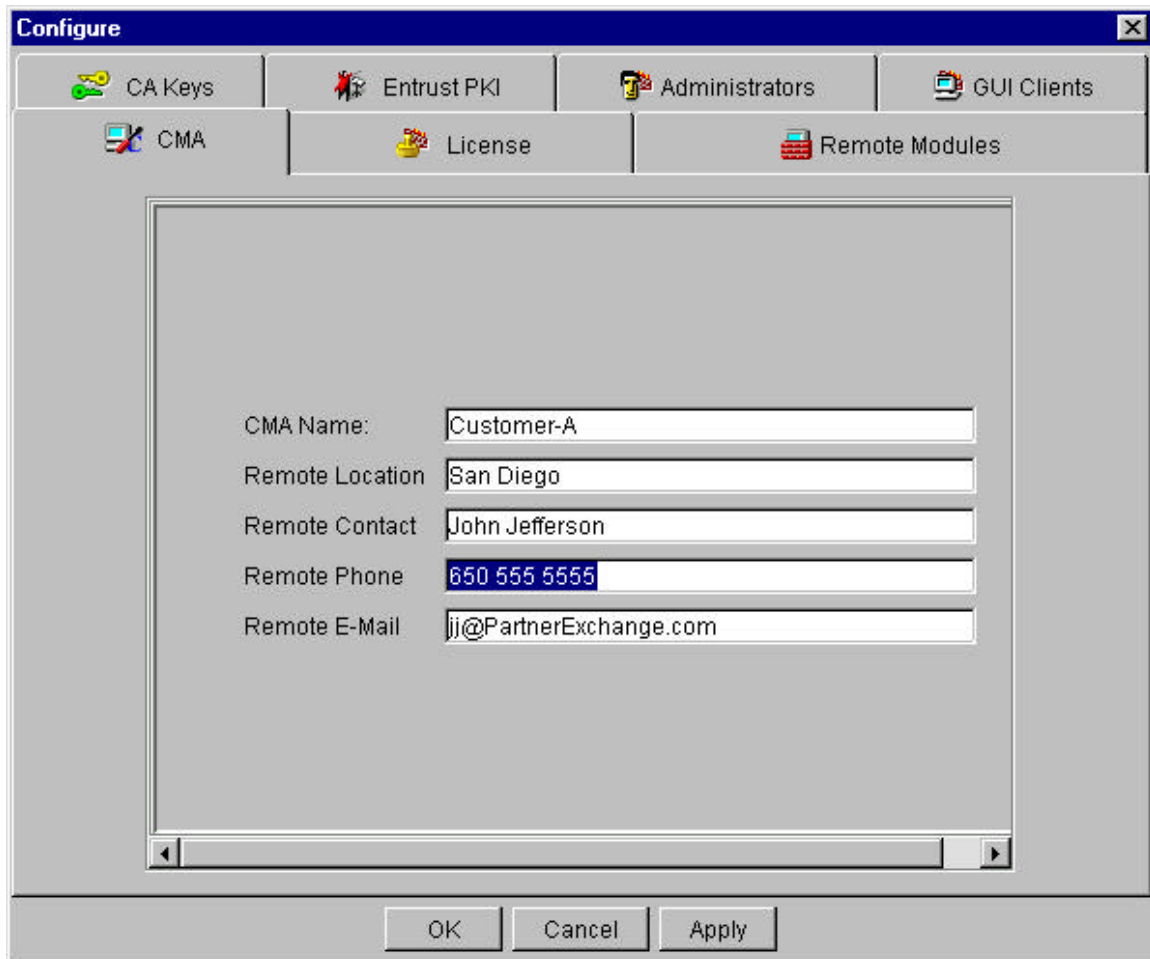
CMA Creation

We start by defining a new CMA. Where the IP Address is the MC address the firewall will use to communicate.



A dialog box titled "New Item Definition" with a close button (X) in the top right corner. It contains two text input fields: "CMA name:" with the value "Customer A" and "IP address:" with the value "192.32.42.72". Below the fields are two buttons: "OK" and "Cancel".

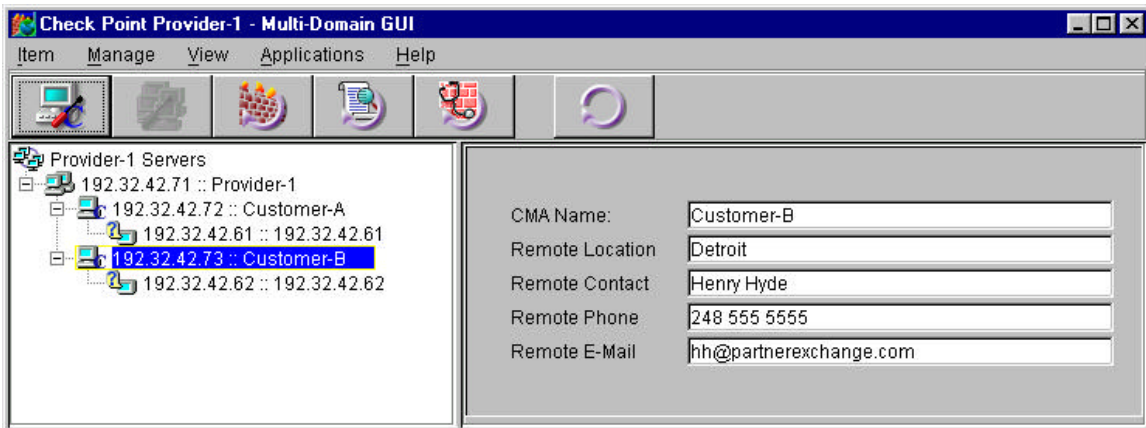
Once created, we now have to configure the properties for each CMA.



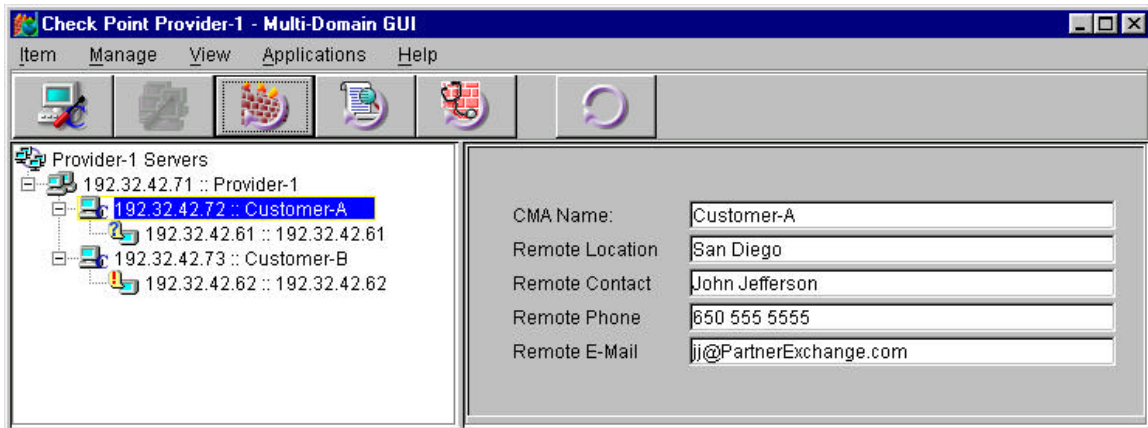
A "Configure" dialog box with a close button (X) in the top right corner. It features a tabbed interface with tabs for "CA Keys", "Entrust PKI", "Administrators", "GUI Clients", "CMA", "License", and "Remote Modules". The "CMA" tab is selected. The main area contains five text input fields: "CMA Name:" (Customer-A), "Remote Location:" (San Diego), "Remote Contact:" (John Jefferson), "Remote Phone:" (650 555 5555), and "Remote E-Mail:" (jj@PartnerExchange.com). At the bottom are three buttons: "OK", "Cancel", and "Apply".

The configuration is not really different than that used in standard FW-1 configuration. The major difference is the license for the customer firewall is entered here versus using FWCONFIG.

Once configured the Provider-1 MDG will show the following:

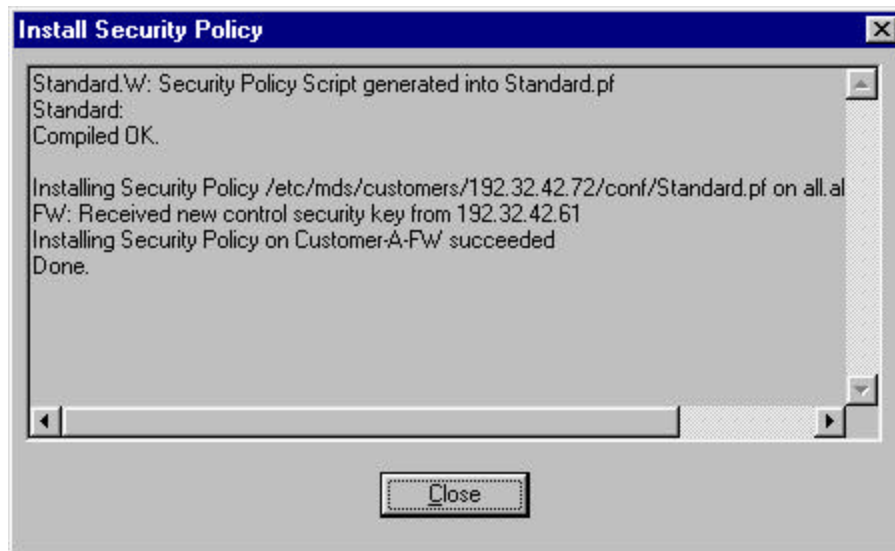


The Multi Domain Server is now ready to create and push policy to Customer A. (Remember Customer A is a new customer) By selecting Launch FW-1 Security Policy we can launch the Firewall-1 GUI and will be connected with the CMA running on IP 192.32.42.72.



At this point for Customer A, it is standard policy management. Creating Objects, Creating rules, and pushing these rules to the firewall.

No	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Customer-A-FW	Any	Any	accept	Long	Customer-A-FW	Any	
2	Net-42	Any	Any	accept	Long	Customer-A-FW	Any	
3	Net-32	Any	Any	accept	Long	Customer-A-FW	Any	
4	Any	Any	Any	reject	Long	Customer-A-FW	Any	



Customer B Migration

Now that Customer A's policy has been established, we are ready to start the migration of Customer B to a managed service. We currently have a policy installed on Cust-B-Firewall. This policy has been created, managed, and installed from the MC, which co-exists on Cust-B-Firewall. The process started when we created a CMA for Customer B. (shown previously).

Each customer environment has it's own conf, lib, bin, directory existing in the /etc/mds directory. Migration of the customer to the P-1 requires the following:

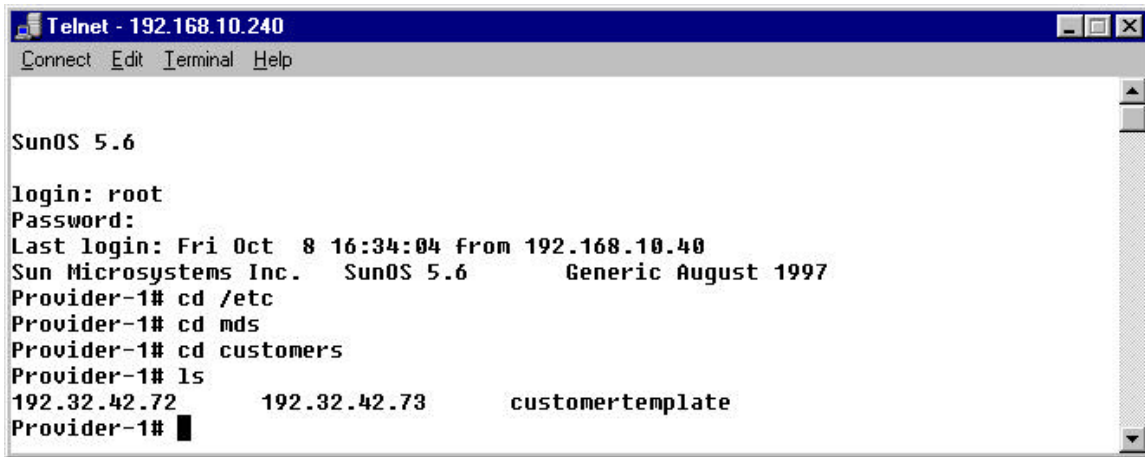
1. Create CMA's (completed above)
2. Configure old Firewall for Migration to P-1
3. Copy the necessary files from the FW/MC to the P-1/FW. (Objects.C, fwauth.NDB and *.W)
4. Set environmental parameters that will tell the firewall that it is dealing with a specific CMA and not the MDS.
5. Import OLD Management Console Files into CMA
6. Reset the environmental parameters to the default.

7. Push policy to the firewall that is being converted.

The MDS works with a variable FWDIR. This variable is normally set to FWDIR /etc/fw for standard implementations. (firewall/management console) When moving to a managed environment, this variable is set to /etc/mds, the directory where Provider-1 defaults its installation.

ON the new management console:

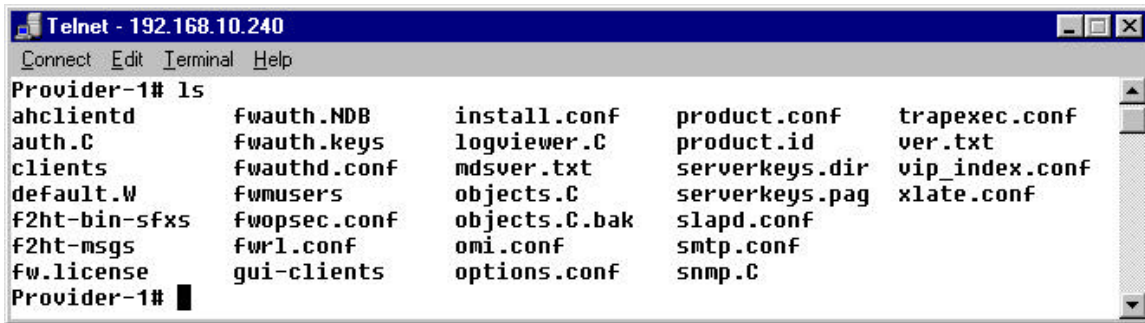
cd \$FWDIR/customers/192.32.42.73/conf



```
Telnet - 192.168.10.240
Connect Edit Terminal Help

SunOS 5.6

login: root
Password:
Last login: Fri Oct  8 16:34:04 from 192.168.10.40
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
Provider-1# cd /etc
Provider-1# cd mds
Provider-1# cd customers
Provider-1# ls
192.32.42.72      192.32.42.73      customertemplate
Provider-1#
```



```
Telnet - 192.168.10.240
Connect Edit Terminal Help

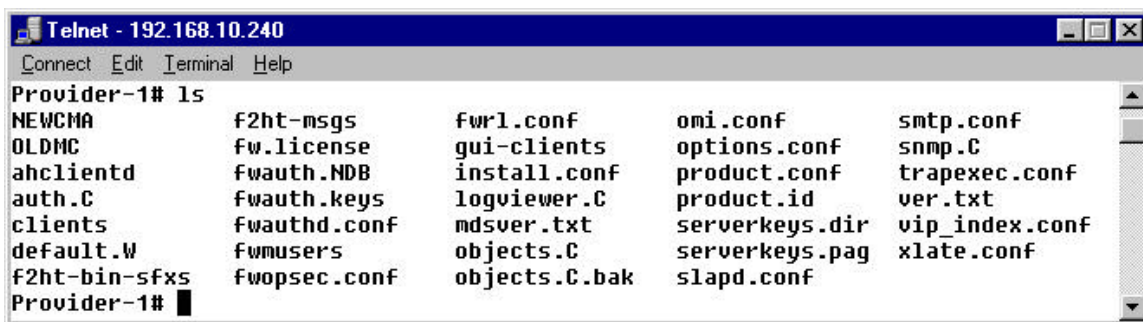
Provider-1# ls
ahclientd      fwauth.NDB      install.conf    product.conf    trapexec.conf
auth.C         fwauth.keys     logviewer.C     product.id      ver.txt
clients        fwauthd.conf   mdsver.txt     serverkeys.dir  vip_index.conf
default.W      fwmusers        objects.C       serverkeys.pag  xlate.conf
f2ht-bin-sfxs  fwopsec.conf   objects.C.bak  slapd.conf
f2ht-msgs      fwrl.conf       omi.conf        smtp.conf
fw.license     gui-clients     options.conf    snmp.C
Provider-1#
```

CREATE WORKING DIRECTORIES

```
mkdir $FWDIR/customers/192.32.42.73/conf/OLDMC
mkdir $FWDIR/customers/192.32.42.73/conf/NEWCMA
```

BACKUP EXISTING FILES

```
cp $FWDIR/customers/192.32.42.73/conf/objects.C
   $FWDIR/customers/192.32.42.73/conf/NEWCMA/objects.C
cp $FWDIR/customers/192.32.42.73/conf/fwauth.NDB*
   $FWDIR/customers/192.32.42.73/conf/NEWCMA/fwauth.NDB
```



The screenshot shows a Telnet session with the title bar 'Telnet - 192.168.10.240'. The terminal prompt is 'Provider-1#'. The user has entered the command 'ls', and the output is a directory listing of files in the /conf directory. The files are listed in five columns:

NEWMA	f2ht-msgs	fwrl.conf	omi.conf	smtp.conf
OLDMC	fw.license	gui-clients	options.conf	snmp.C
ahclientd	fwauth.NDB	install.conf	product.conf	trapexec.conf
auth.C	fwauth.keys	logviewer.C	product.id	ver.txt
clients	fwauthd.conf	mdsver.txt	serverkeys.dir	vip_index.conf
default.W	fwmusers	objects.C	serverkeys.pag	xlate.conf
f2ht-bin-sfxs	fwopsec.conf	objects.C.bak	slapd.conf	

The terminal prompt is 'Provider-1#'.

From the old firewall/management console copy the following files:

(192.32.42.71 real IP
192.32.42.73 Virtual Management IP)

```
/$FWDIR/conf/objects.C
/$FWDIR/conf/fwauth.NDB
/$FWDIR/conf/*.W
```

to the MDS in the following directory:

(\$FWDIR/customers/192.32.42.73/conf/OLDMC: where 192.32.42.73 is the address of the customer management add-on console)

```
/$FWDIR/conf/OLDMC/objects.C.cust.B
/$FWDIR/conf/OLDMC/fwauth.NDB.cust.B
/$FWDIR/conf/OLDMC/*.W
```

Excute the following commands:

CSH

```
setenv FWDIR /etc/mds/customers/192.32.42.73
setenv MSP_SOMEIP_ADDR 192.32.42.73
```

KSH

```
export FWDIR=/etc/mds/customers/192.32.42.73
export MSP_SOMEIP_ADDR=192.32.42.73
```

RUN the following commands:

```
cd $FWDIR/bin
./fwstop
./fw confmerge $FWDIR/conf/OLDMC/objects.C
    $FWDIR/conf/NEWCMA/objects.C > $FWDIR/conf/objects.C
cp $FWDIR/conf/OLDMC/fwauth.NDB* $FWDIR/conf
cp $FWDIR/conf/OLDMC/*.W $FWDIR/conf
./fwm -g $FWDIR/conf/*.W
fwstart
```



```
Telnet - 192.168.10.240
Connect Edit Terminal Help
Provider-1# setenv FWDIR /etc/mds/customers/192.32.42.73
Provider-1# setenv MSP_SOMEIP_ADDR 192.32.42.73
Provider-1# cd $FWDIR/bin
Provider-1# ./fwstop
fwm: Firewall-1 Management Server going to die on sig 15
Provider-1# ./fw confmerge $FWDIR/conf/OLDMC/objects.C $FWDIR/conf/NEWCMA/object
s.C > $FWDIR/conf/objects.C
Provider-1# cp $FWDIR/conf/OLDMC/fwauth.NDB* $FWDIR/conf
Provider-1# cp $FWDIR/conf/OLDMC/*.W $FWDIR/conf
Provider-1# ./fwm -g $FWDIR/conf/*.W
Converting File 'Cust-B-Policy.W'...
Converting File 'default.W'...
Total of 2 files converted successfully.
Provider-1# ./fwstart
FireWall-1: Starting fwd
FireWall-1: Starting fwm (Remote Management Server)
fwm: FireWall-1 Management Server is running

FireWall-1: This is a Management Station. No Security Policy will be Loaded
FireWall-1 started
Provider-1# █
```

UNSET ENVIRONMENTAL PARAMETERS.

CSH

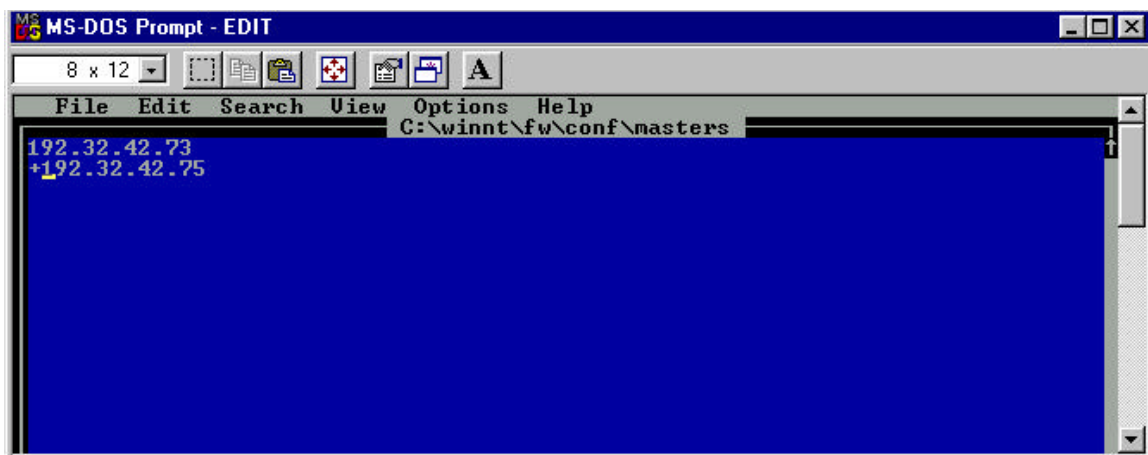
```
setenv FWDIR /etc/mds  
unsetenv MSP_SOMEIP_ADDR
```

KSH

```
export FWDIR=/etc/mds  
unset MSP_SOMEIP_ADDR.
```

ON THE SYSTEM TO BE MIGRATED (192.32.42.62)

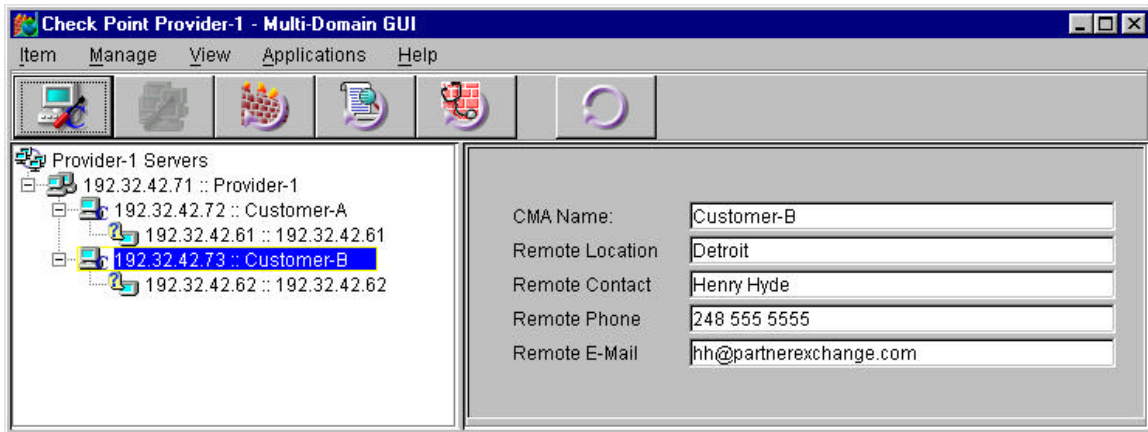
```
cd $FWDIR/conf  
create a masters file:  
vi masters or edit masters
```



SYNC KEYS

```
fw putkey 192.32.42.73  
Enter secret key: xxxxxxx  
Again secret key: xxxxxxx  
fwstop  
fwstart
```

The old management console has now been transferred to the Provider-1 environment. From the Provider-1 management console,



Selecting the “Launch FW-1 Security Policy” icon or “Applications/ Launch FW-1 Security Policy” will bring up the policy editor. At this point we can confirm that the rules and users have been import and can move forward with policy installation.

NOTE: In the installation process, our keys may or may not be sync’ed. If we receive “Authentication for command load failed” we simply need to re-sync our putkeys.

