Manipulating objects and rules on Provider-1/SiteManager-1 with Object Filler and Object Dumper

Martín Humberto Hoz Salvador, CISA, CISSP

mhoz at mexico dot com
martinhoz at gmail dot com

Created on July 2005

Revision 20061229

Table of Contents

1. Introduction

Provider-1/SiteManager-1 are solutions for maintaining multiple SmartCenters in a single piece of hardware. This is, the SmartCenters are virtualized. There is one entity which works as a container (the Multi-Domain Server or simply MDS) that hold and has control over all the virtual SmartCenters (called Customer Management Add-Ons or simply CMAs), which are independent from each other in configuration, environment, disk space, etc..

You may find more information on Provider-1/SiteManager-1 here:
http://www.checkpoint.com – Products and Technologies – Provider-1

Object Dumper and Object Filler are tools that allow to import and export objects from SmartCenters, either physical (regular SmartCenters) or virtual (CMAs).

You may find more information on Object Filler and Object Dumper here:
http://ofiller.chatscope.com/   (main download site with Beta versions, Bug tracker, forums, FAQs and other nice resources)
http://www.lindercentral.com/ofiller/ - always the latest stable version
http://www.cpug.org/ - always the latest stable version

1.1 Typographic convention

The regular text of the document will be written in regular Arial font..
```
Text seen in the screen or output shown as result of some command, will be shown on
Courier font, like this.
```
`Text that the user has to type-in and is normally shown to the screen will be on Courier bold, as this example`
`Text that the user has to type-in but is not shown to the screen will be printed in Courier bold and italic font, as in this example`
Whenever a new term is introduced, some specific name is used or there is a buzzword, it will be printed in italic format. Italics may be used as well to highlight something under special circumstances
<u>Whenever it is needed to highlight something, it will be underlined</u>.

2. Disclaimer

Object Filler and Object Dumper are tools not officially supported. This is, even though they work, nobody is in the obligation of helping you, and if you call Check Point Support they won't be able to assist you. Please read the Object Filler and Object Dumper documentation (such as the *User's Manual* and *Object Filler and Object Dumper Tutorial*) before you proceed.

Even though the procedures described here have been tested by the author of this document and some others, they are not guaranteed to be error-free. The only responsible entity for the results of using the procedures and techniques described on this document, is the person implementing them and the person that approves the use of this on her/his infrastructure. Check Point, Check Point employees and affiliates in any way and the document's author; are not liable nor responsible by any good or bad thing resulted of any direct or indirect use, abuse or misuse of the contents of this document, either express or implicit.

3. Environment Description

The software version used on the first version of this document was **Provider-1/SiteManager-1 NGX (Build 244) installed on SecurePlatform NGX.** The latest revision of the document was done using version **NGX R62** on SecurePlatform. Details below:

```
[Expert@p1ngxr62]# ver
This is Provider-1/SiteManager-1 NGX R62 Build 031
[Expert@p1ngxr62]# fw ver
This is Check Point VPN-1(TM) & FireWall-1(R) NGX (R62) - Build 120
[Expert@p1ngxr62]#
```

The *expert mode* of SecurePlatform was the working environment for most of the operations done. This is needed because you need to interact with files and do operations that the restricted *cpshell,* which SecurePlatform puts to all the defined users by default, normally doesn't allow.

The tools version used for writing this document was **Object Dumper and Object Filler 2.4 running on Windows XP**. The output screens of another version may be a little different than the ones shown here. As a general rule, use at minimum Object Dumper and Object Filler <u>version 2.4</u> and for sure what you see here will work for you.

```
D:\Stuff\OFiller\v2.4>ver

Microsoft Windows XP [Version 5.1.2600]

D:\Stuff\OFiller\v2.4>ofiller -V
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
===============================================================================

*******************************************************************************
This is Object Filler Version v2.4
This is Object Filler Build Number Thu_211206_1229
*******************************************************************************

===============================================================================
No valid objects were processed! - Thank you for using Object Filler v2.4!
```

We'll assume that the objects that are going to be manipulated are exclusively host and network objects. Any other type of objects, such as service objects was not tested but there are reasons to believe they will work fine as well.

For this scenario, we'll assume we have 2 CMAs and 1 MDS Manager and Container. The IP Addresses are 10.20.30.200 for the MDS, CMA named *cma1* has 10.20.30.201 and *cma2*, which is the second CMA has 10.20.30.202

The setup was done using evaluation licenses. The CMAs and the MDS have *AnyHost* assigned as GUI Client for the MDS and both CMAs, and only one Provider-1 Super User administrator. This administrator was named admin

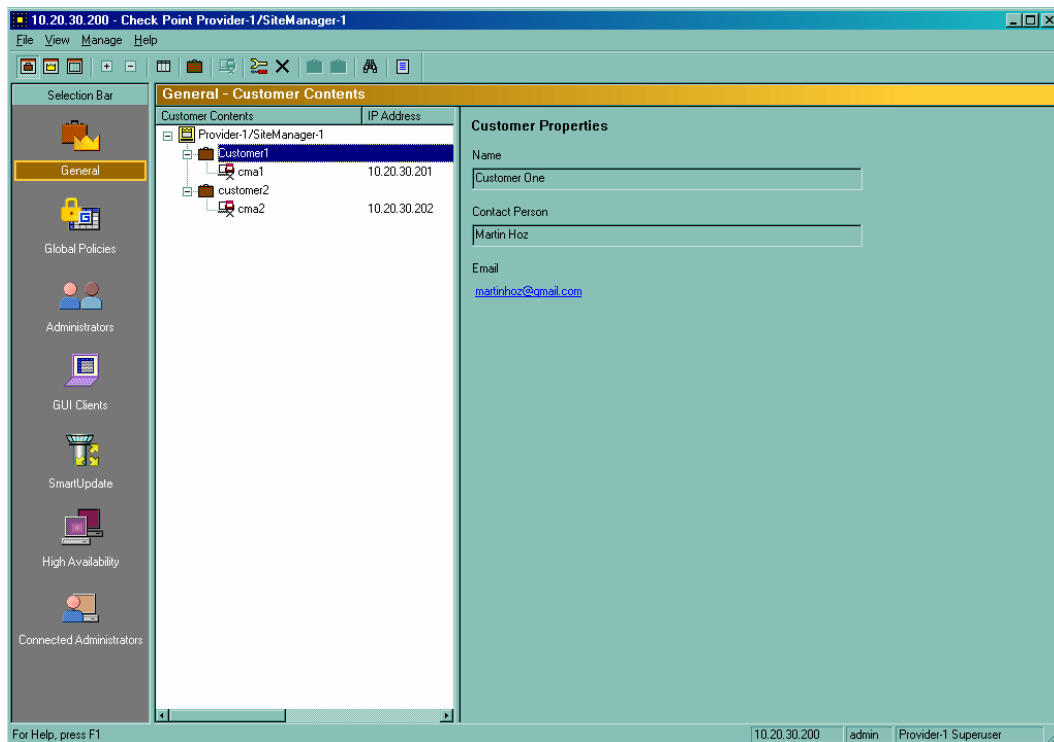The following screenshots will tell you more about the environment:
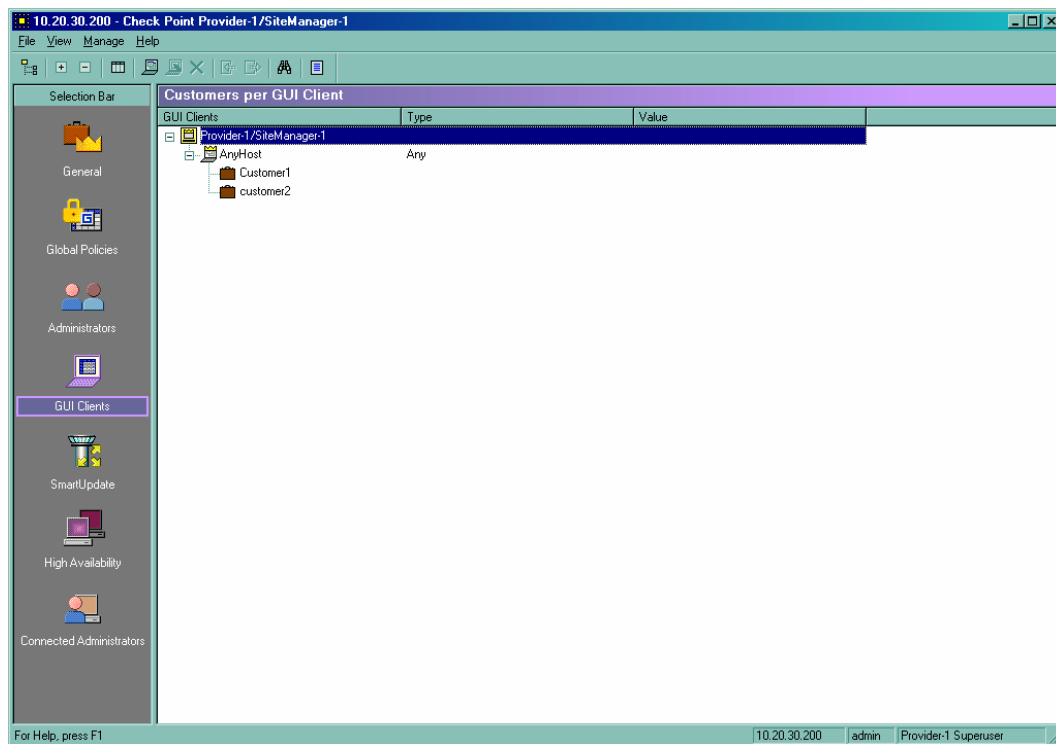

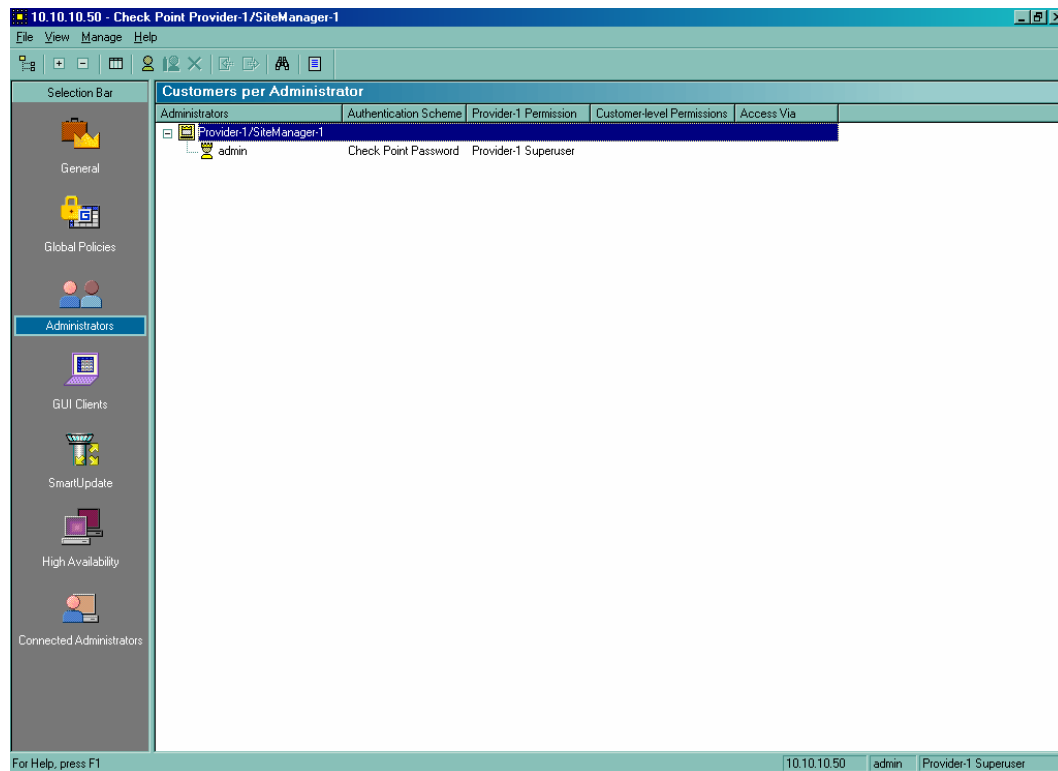*Figure 1 - Customer Contents View*

Figure 2 – GUI Clients View

Figure 3 – Administrators View
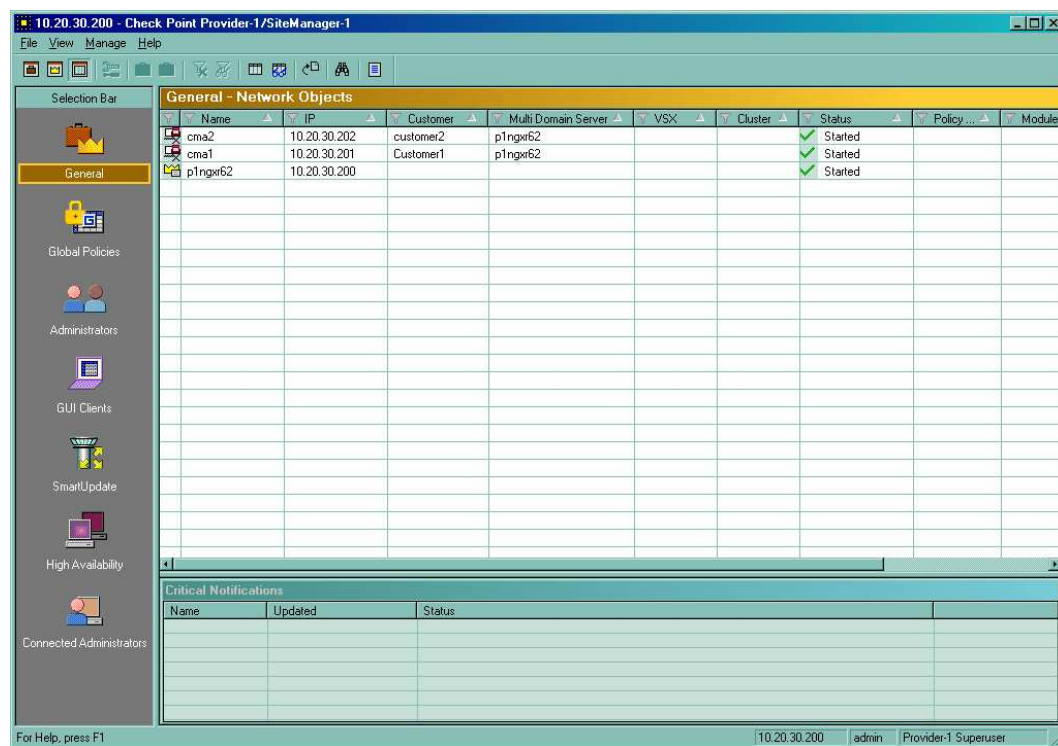
Figure 4 – SmartView Status View

The following parts deal with creating objects and performing import operations. This assumes you have previous experience working with Provider-1/SiteManager-1 and you are familiar with the product's terminology.

This document also assumes you already did read the Object Dumper and Object Filler Manual - or at least the Object Filler and Object Dumper Tutorial (which is shorter, goes to the point and it is more fun to read) and you are aware on how the tools work in conjunction with DBedit.

If you don't have such background, it is strongly recommended at this point to review such documentation (again, at least the Tutorial), prior to any other step.

4. Importing Objects into CMAs and the Global Database

4.1 Creating Objects to Import into **cma1**

Before going any ahead, let's remember that the document was written using Provider-1/Site-Manager-1 NGX over SecurePlatform, and the tools Object Filler and Object Dumper were running on Windows.

We'll use Object Filler to automatically generate a script to create 100 hosts. We'll import them into the first CMA (named *cma1* in this case). The objects will be created on the range of the 10.1.1.0/24 address space, going from 1 to 100.

The Object Filler syntax to do it is:

```
D:\Stuff\OFiller\v2.4>ofiller -s 10.1.1.1 -d 10.1.1.100 -m 24 -t host -o cma1.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
=============================================================================
...................................
=============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 100 possible objects and/or rules.
Found 100 total valid (or successfully processed) objects/rules.
-----------------------------------------------------------------------------
Total successfully processed Hosts = 100
-----------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
=============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Now, we transfer to the MDS machine the *cma1.dbedit* file created as a result of the above steps. This has to be done using FTP in ASCII mode, copy-pasting it from notepad to vi, or any other reliable ASCII file transfer mechanism.

Let's check the CMA we are going to use to import the object to (*cma1* on this case) is up and running. We will use *mdsstat* to check this out:

```
[Expert@p1ngxr62]# mdsstat
+---------------------------------------------------------------------------------+
|                       Processes status checking                                 |
+-----+----------------+----------------+----------+----------+----------+---------+
| Type| Name           | IP address     | FWM      | FWD      | CPD      | CPCA    |
+-----+----------------+----------------+----------+----------+----------+---------+
| MDS |        -       | 10.20.30.200   | up 1213  | up 1212  | up 1211  | up 1460 |
+-----+----------------+----------------+----------+----------+----------+---------+
| CMA | cma1           | 10.20.30.201   | up 2966  | up 2965  | up 2940  | up 2978 |
| CMA | cma2           | 10.20.30.202   | up 3562  | up 3561  | up 3536  | up 3576 |
+-----+----------------+----------------+----------+----------+----------+---------+
```

```
| Total customer add-ons checked: 2      2 up    0 down                               |
| Tip: Run mdsstat -h for legend                                                      |
+-------------------------------------------------------------------------------------+
[Expert@p1ngxr62]#
```

Now that we know *cma1* is up and running, we have to make sure the CMA is not locked by an administrator using a GUI or something. First we use *mdsenv* to set the environment to the proper CMA and then *cpstat* to review for any connected GUIs.

```
[Expert@p1ngxr62]# mdsenv cma1
[Expert@p1ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK


Connected clients
-----------------------------------------------
|Client type|Administrator|Host|Database lock|
-----------------------------------------------
-----------------------------------------------
```

What you have to check on the above is that you don't see something like this:

```
Connected clients
--------------------------------------------------
|Client type    |Administrator|Host |Database lock|
--------------------------------------------------
|SmartDashboard|admin         |mhoz1|true         |
--------------------------------------------------
```

The above indicated the Database for such CMA is locked by *admin* from the *mhoz1* host. You cannot use DBedit on a CMA that has the database locked.

Once you do that, we need to set the environment to the CMA *cma1* using *mdsenv* to do so, and then run DBedit over this file. All this in expert mode:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la
total 48
drwx------    2 root     root         4096 Dec 21 12:43 .
drwxr-xr-x    4 root     root         4096 Dec 21 06:32 ..
-rw-------    1 root     root            0 Dec 21 12:27 .bash_history
-rw-r--r--    1 root     root           24 Dec 21 06:32 .bash_logout
-rw-r--r--    1 root     root          191 Dec 21 06:32 .bash_profile
-rw-r--r--    1 root     root          124 Dec 21 06:32 .bashrc
-rw-rw----    1 root     root        25252 Dec 21 12:43 cma1.dbedit
[Expert@p1ngxr62]# mdsenv cma1
[Expert@p1ngxr62]# dbedit -s localhost -u admin -f cma1.dbedit
```

```
Enter Administrator Password: secret
Host_10.1.1.1 updated successfully.
Host_10.1.1.2 updated successfully.
Host_10.1.1.3 updated successfully.
      .
      .
      .
Host_10.1.1.99 updated successfully.
Host_10.1.1.100 updated successfully.
[Expert@p1ngxr62]#
```

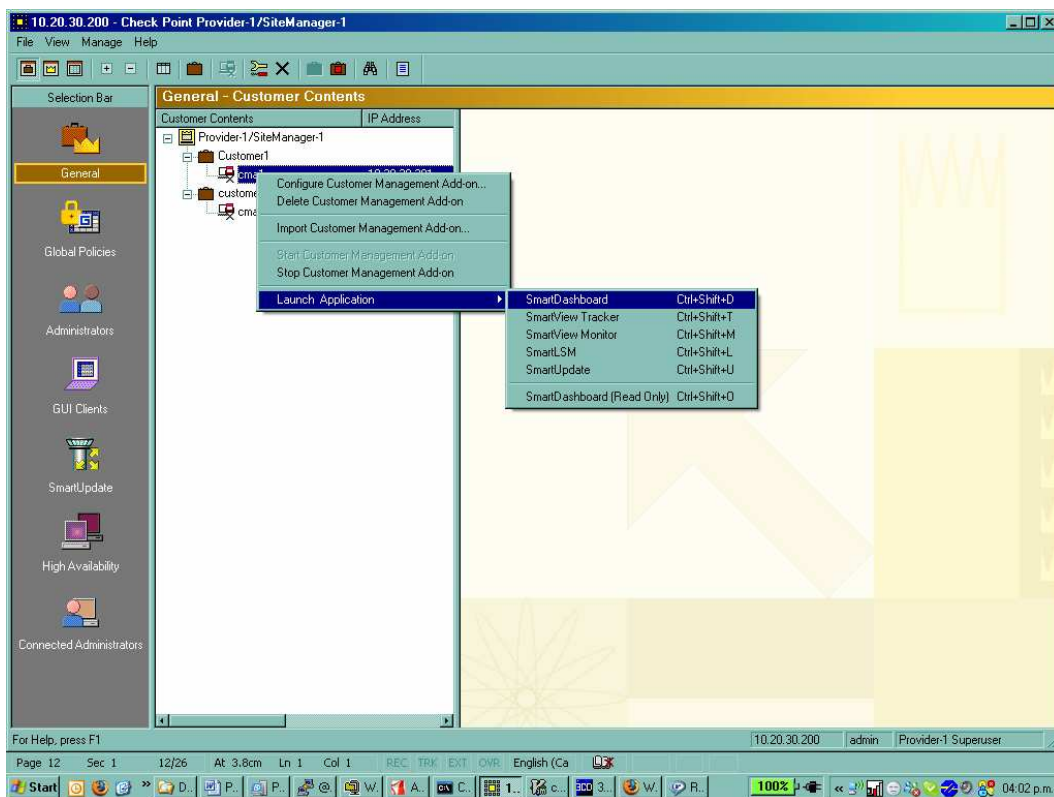Then we go to the MDG, open the SmartDashboard over CMA1 and make sure the objects were created there:

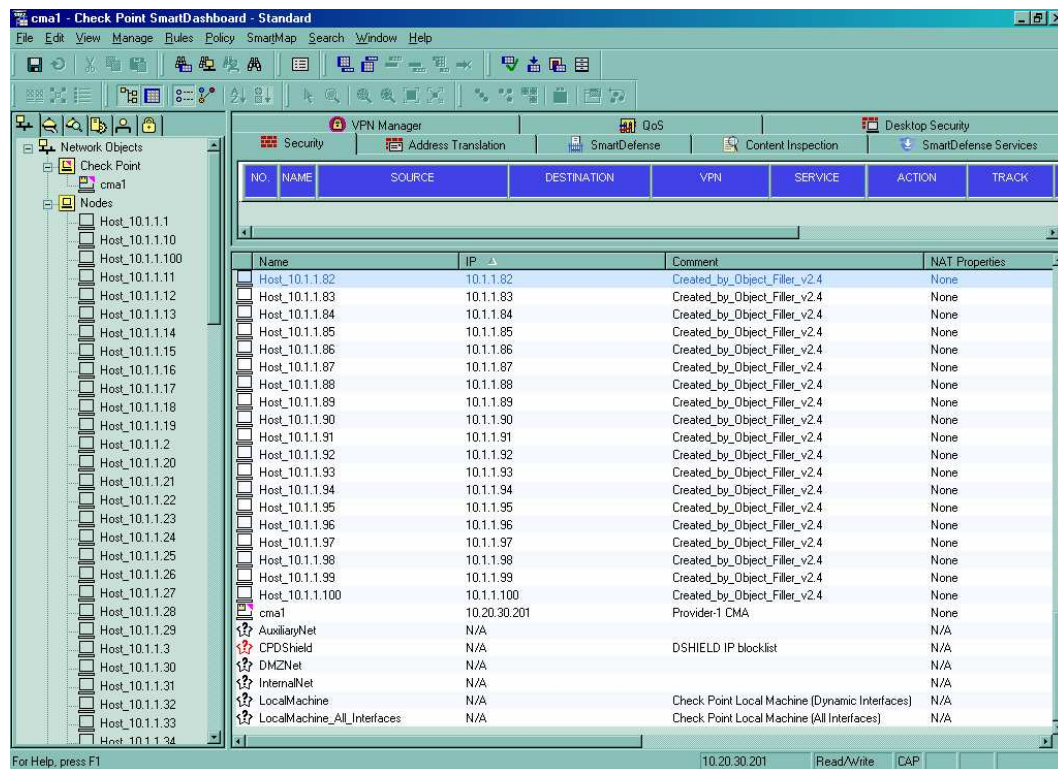*Figure 5.a – Launching SmartDashboard over cma1 from the MDG*

Figure 5.b – SmartDashboard open over cma1

4.2 Creating Objects to Import into CMA2

Now, we'll create 101 networks within the 192.168.0.0/16 address space so we can import them into *cma2*, and do the same procedure there as we did with *cma1*.

First creating the objects with Object Filler:
```
D:\Stuff\OFiller\v2.4>ofiller -s 192.168.0.0 -d 192.168.100.0 -m 24 -t net -o
cma2.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
==============================================================================
.................................
==============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 25601 possible objects and/or rules.
Found 101 total valid (or successfully processed) objects/rules.
------------------------------------------------------------------------------
Total successfully processed Networks = 101
------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
==============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Page 13

```
D:\Stuff\OFiller\v2.4>
```

Then, after transferring the resulting file *cma2.dbedit* to the MDS machine, we need to import the objects into *cma2*.

Remember the file has to be transferred in an **ASCII** format: using FTP in ASCII mode, copy-pasting it from notepad to vi, or any other reliable ASCII file transfer mechanism. The following is an example using FTP.

```
[Expert@p1ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> get cma2.dbedit
local: cma2.dbedit remote: cma2.dbedit
227 Entering passive mode (10,20,30,76,8,147)
125 Using existing data connection
################################
226 Closing data connection; File transfer successful.
33368 bytes received in 0.0269 secs (1.2e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la
total 96
drwx------     2 root     root         4096 Dec 21 13:11 .
drwxr-xr-x     4 root     root         4096 Dec 21 06:32 ..
-rw-------     1 root     root            0 Dec 21 12:27 .bash_history
-rw-r--r--     1 root     root           24 Dec 21 06:32 .bash_logout
-rw-r--r--     1 root     root          191 Dec 21 06:32 .bash_profile
-rw-r--r--     1 root     root          124 Dec 21 06:32 .bashrc
-rw-rw----     1 root     root        25252 Dec 21 12:43 cma1.dbedit
-rw-rw----     1 root     root        32762 Dec 21 13:11 cma2.dbedit
[Expert@p1ngxr62]# file cma2.dbedit
cma2.dbedit: ASCII text
```

Now we check *cma2* is up and running

```
[Expert@p1ngxr62]# mdsstat cma2
Checking status of CMA 'cma2'
+--------------------------------------------------------------------------------------+
|                           Processes status checking                                  |
+-----+----------------+----------------+----------+----------+----------+---------+
```

```
| Type| Name           | IP address      | FWM      | FWD      | CPD      | CPCA     |
+-----+----------------+-----------------+----------+----------+----------+----------+
| MDS |       -        | 10.20.30.200    | up 1213  | up 1212  | up 1211  | up 1460  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| CMA | cma2           | 10.20.30.202    | up 3562  | up 3561  | up 3536  | up 3576  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 1     1 up   0 down                                |
| Tip: Run mdsstat -h for legend                                                     |
+-----------------------------------------------------------------------------------+
```

and there is nobody locking the database

```
[Expert@p1ngxr62]# mdsenv cma2
[Expert@p1ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK


Connected clients
-------------------------------------------------
|Client type|Administrator|Host|Database lock|
-------------------------------------------------
-------------------------------------------------
```

Please notice that before running DBedit, we set the environment to *cma2* using the *mdsenv* command:

```
[Expert@p1ngxr62]# mdsenv cma2
[Expert@p1ngxr62]# dbedit -s localhost -u admin -f cma2.dbedit
Enter Administrator Password: secret
Net_192.168.0.0 updated successfully.
Net_192.168.1.0 updated successfully.
Net_192.168.2.0 updated successfully.
     .
     .
     .
Net_192.168.99.0 updated successfully.
Net_192.168.100.0 updated successfully.
[Expert@p1ngxr62]#
```

Then we go to the MDG, open the SmartDashboard over CMA2 and make sure the objects were created there:
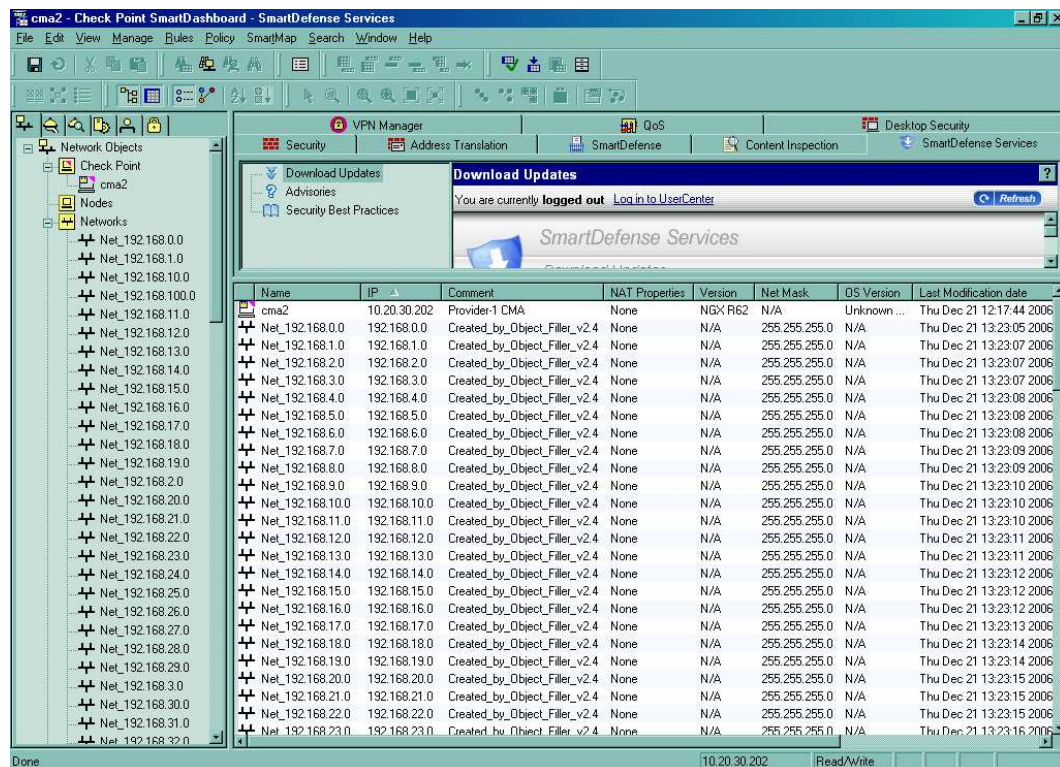
Figure 6 – SmartDashboard open over cma2

4.3 Creating Objects to Import them into the Provider-1/SiteManager-1 Global Database

Now, we'll create some hosts in the network 172.16.10.0/24 to import them to the global database :

```
D:\Stuff\OFiller\v2.4>ofiller -s 172.16.10.0 -d 172.16.10.10 -m 24 -t host -o
global.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
==============================================================================
....
==============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 11 possible objects and/or rules.
Found 10 total valid (or successfully processed) objects/rules.
------------------------------------------------------------------------------
Total successfully processed Hosts = 10
------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
==============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

```
D:\Stuff\OFiller\v2.4>
```

Once they are created and the file is transferred to the MDS machine (remember, in an ASCII format), we'll need to import them into the Global database. Since we're doing this at the MDS level, we use *mdsenv* with no arguments to set the environment to the MDS.

Please notice the difference in the *DBedit* syntax when you are using it to import objects into the Global Database. Also notice that no password is required:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la
total 100
drwx------    2 root     root         4096 Dec 21 13:33 .
drwxr-xr-x    4 root     root         4096 Dec 21 06:32 ..
-rw-------    1 root     root            0 Dec 21 12:27 .bash_history
-rw-r--r--    1 root     root           24 Dec 21 06:32 .bash_logout
-rw-r--r--    1 root     root          191 Dec 21 06:32 .bash_profile
-rw-r--r--    1 root     root          124 Dec 21 06:32 .bashrc
-rw-rw----    1 root     root        25252 Dec 21 12:43 cma1.dbedit
-rw-rw----    1 root     root        32762 Dec 21 13:11 cma2.dbedit
-rw-rw----    1 root     root         2656 Dec 21 13:33 global.dbedit
[Expert@p1ngxr62]# mdsenv
[Expert@p1ngxr62]# dbedit -mds -s localhost -u admin -f global.dbedit
Host_172.16.10.1 updated successfully.
Host_172.16.10.2 updated successfully.
      .
      .
      .
Host_172.16.10.9 updated successfully.
Host_172.16.10.10 updated successfully.
[Expert@p1ngxr62]#
```

We'll make sure that the objects were created, by opening the Global SmartDashboard. Please notice that the created objects have a purple the capital G, indicating those are recognized as Global Objects:
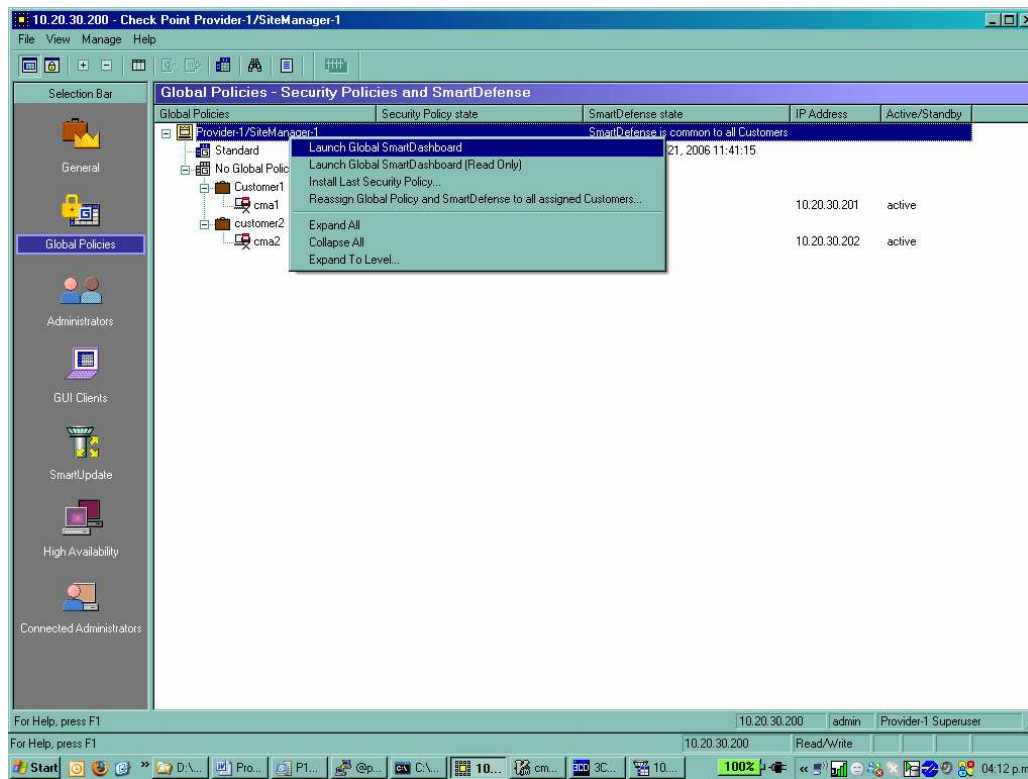
Figure 7.a – Launching Global SmartDashboard from the MDG
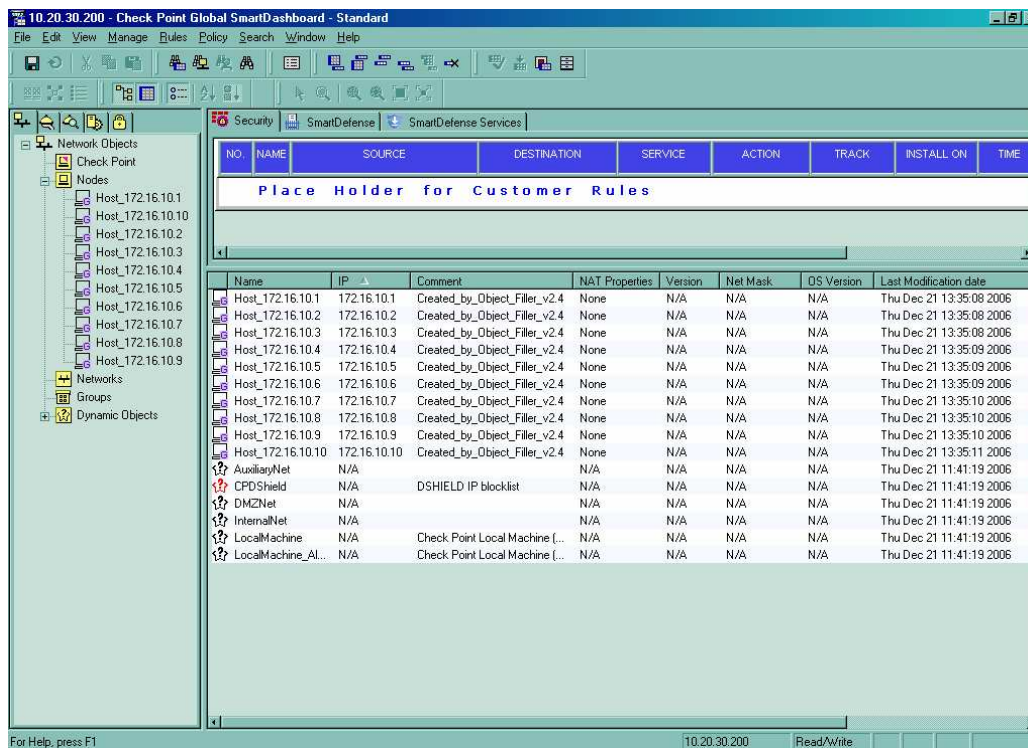
Figure 7.b – Global SmartDashboard open over the Provider-1/SiteManager-1 Global Database

5. Exporting and Importing Objects back between the Global Objects Database and CMAs

All the objects database is hold in a file named *objects_5_0.C* always present in the *$FWDIR/conf* directory of any regular SmartCenter. In a Provider-1 environment, this file is also present in the CMAs and is used to hold the CMA's object database. The file is present as well in the MDS itself and in that case contains the Global Objects database.

Object Dumper can process the *objects_5_0.C* file and dump it to a *Comma Separated Values* (*CSV*) format file, from which Object Filler can be used to build such exported objects again into another place: another SmartCenter, another CMA or the MDS Global Database.

5.1 Exporting Objects from a CMA (or SmartCenter) and Importing into the Global Objects Database

As a note: even though this procedure was done for this document using a CMA's objects database, it is possible to follow the same steps and perform this very procedure with an SmartCenter, with the only exception that in a regular **SmartCenter** you **don't need** to set the environment with *mdsenv* before gathering the *objects_5_0.C* file. Remember *mdsenv* is only needed in Provider-1 to set the proper environment in the shell, so the variables and directories point to one specific CMA.

The following procedure shows how the Objects database from the CMA named *cma2* is exported. First we have to copy the database file to the Windows machine where Object Dumper is running. In this case, an FTP Server was placed in the Windows machine where the tools are running, and the FTP Client available in SecurePlatform was used. Notice that ASCII file transfer was used

Please notice that previous to any operation, we set the environment to *cma2* with *mdsenv*, so we can copy the appropriate files.

```
[Expert@p1ngxr62]# mdsenv cma2
[Expert@p1ngxr62]# cd $FWDIR/conf
[Expert@p1ngxr62]# pwd
/opt/CPmds-R62/customers/cma2/CPsuite-R62/fw1/conf
[Expert@p1ngxr62]# ls -la objects_5_0.C
-rw-rw-r--    1 root     root       651841 Dec 21 13:23 objects_5_0.C
[Expert@p1ngxr62]# file objects_5_0.C
objects_5_0.C: ASCII text
[Expert@p1ngxr62]# ftp 10.20.30.76
```
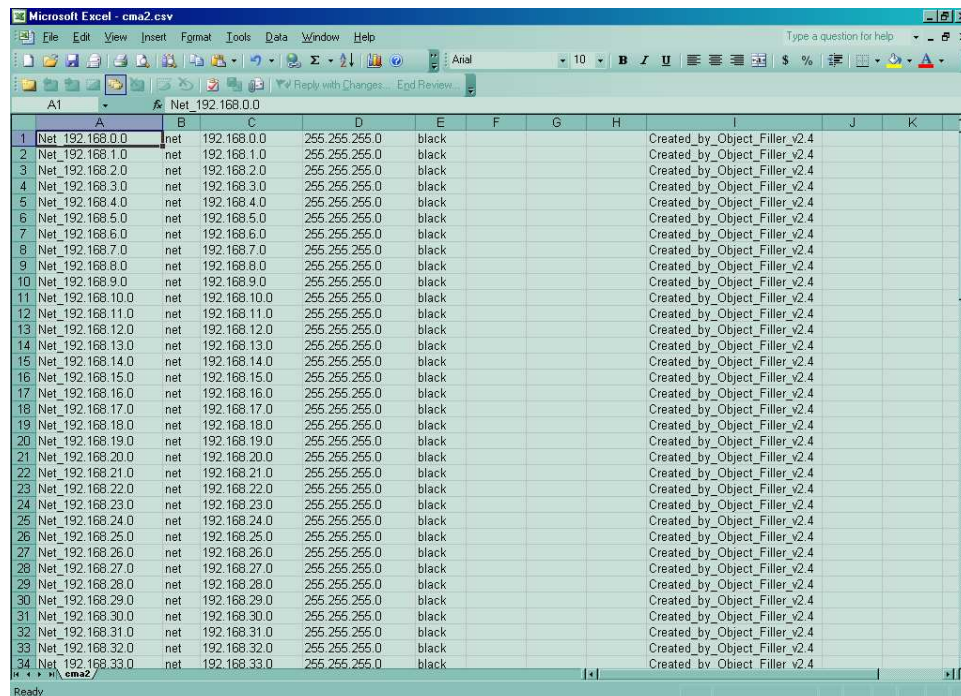
```
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> put objects_5_0.C objects_5_0_cma2.C
local: objects_5_0.C remote: objects_5_0_cma2.C
227 Entering passive mode (10,20,30,76,4,157)
125 Using existing data connection
################################################################################
################################################################################
############################################################
226 Closing data connection; File transfer successful.
678483 bytes sent in 0.725 secs (9.1e+02 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]#
```

Then we'll export the objects from *cma2* using Object Dumper and the file we just transferred.

```
D:\Stuff\OFiller\v2.4>odumper -f objects_5_0_cma2.c -o cma2.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
================================================================================

================================================================================
 * Processing objects...
--------------------------------------------------------------------------------
................................................................................
.....................


================================================================================
Processed 26642 possible objects and found 150 valid ones.
It took 3.0 seconds on quiet mode.
Total successfully processed CP Hosts (Secure Servers/SmartCenters) = 1
Total successfully processed Networks = 101
================================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

Now you have to edit the *cma2.csv* file, which in this case is the file that results from running Object Dumper over the *objects_5_0.C* we got from *CMA2*; and remove the lines that represent objects you don't want to transfer to the Global Database, such as services, as usually they already exist in the other side; and extra hosts objects like the CMA object itself, which is useless in the Global Objects Database.
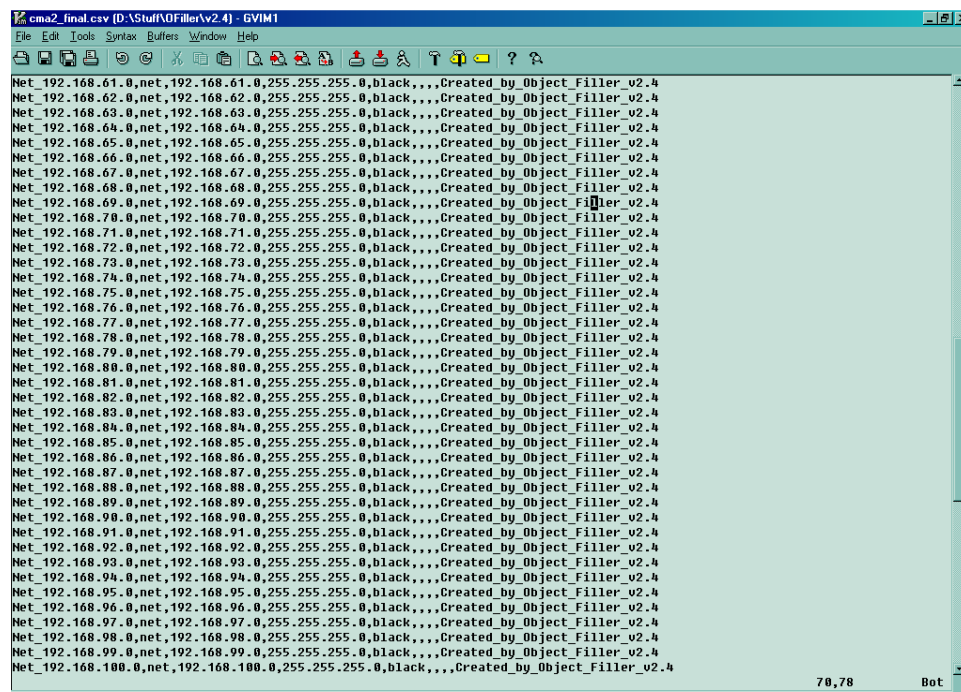
You may do this editing work using any text editor (Notepad or vi for example) or spreadsheet program (Microsoft Excel for example).

Figure 9a – A preview (using Microsoft Excel) of the final file that resulted from exporting objects from CMA2, and used to feed Object Filler later.

Figure 9b – A preview (using a Text Editor) of the final file that resulted from exporting objects from CMA2, and used to feed Object Filler later.

Once you have the file with only the objects you need, run Object Filler over it:

```
D:\Stuff\OFiller\v2.4>ofiller -f cma2_final.csv -i csv -o import_global.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
=============================================================================
Processing objects...
................................
=============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 202 possible objects and/or rules.
Found 101 total valid (or successfully processed) objects/rules.
-----------------------------------------------------------------------------
Total successfully processed Networks = 101
-----------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
=============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Now that the *import_global.dbedit* was created as a result, transfer it to the MDS machine and import it into the Global Database using DBedit. Let's remember that the file is an ASCII (text) file and should be treated as such. Don't forget as well to set the environment accordingly using *mdsenv*. Also, remember the special DBedit syntax when running it over the Global Objects Database:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la
total 136
drwx------    2 root     root           4096 Dec 21 14:27 .
drwxr-xr-x    4 root     root           4096 Dec 21 06:32 ..
-rw-------    1 root     root              0 Dec 21 12:27 .bash_history
-rw-r--r--    1 root     root             24 Dec 21 06:32 .bash_logout
-rw-r--r--    1 root     root            191 Dec 21 06:32 .bash_profile
-rw-r--r--    1 root     root            124 Dec 21 06:32 .bashrc
-rw-rw----    1 root     root          25252 Dec 21 12:43 cma1.dbedit
-rw-rw----    1 root     root          32762 Dec 21 13:11 cma2.dbedit
-rw-rw----    1 root     root           2656 Dec 21 13:33 global.dbedit
-rw-rw----    1 root     root          32964 Dec 21 14:27 import_global.dbedit
[Expert@p1ngxr62]# mdsenv
[Expert@p1ngxr62]# dbedit -mds -s localhost -u admin -f import_global.dbedit
Net_192.168.0.0 updated successfully.
Net_192.168.1.0 updated successfully.
       .
       .
       .
Net_192.168.99.0 updated successfully.
Net_192.168.100.0 updated successfully.
[Expert@p1ngxr62]#
```

You may see that the objects (Networks in the 192.168.0.0/16 range) were imported into the Global Objects Database using the Global SmartDashboard
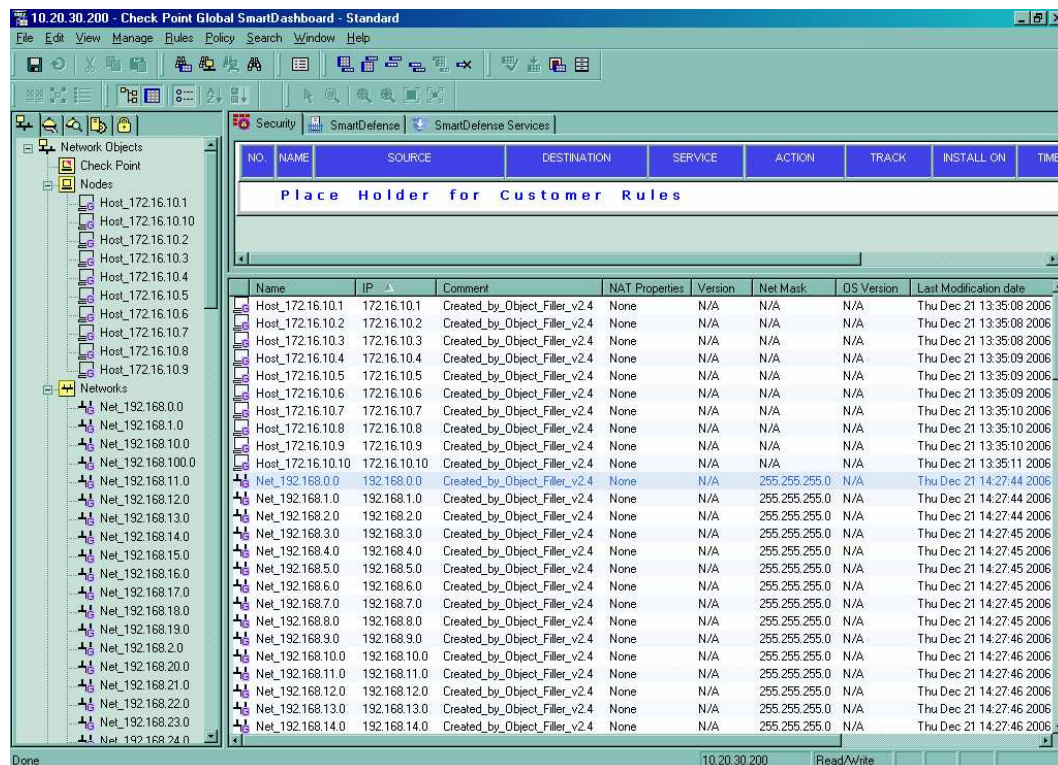
Figure 10 – Global SmartDashboard open over the Provider-1/SiteManager-1 Global Database after successfully importing objects from cma2 into it.

5.2 Exporting the Global Database and importing it into a CMA (or SmartCenter)

Again as a note: even though this procedure was done for this document using a CMA as the target, it is possible to follow the same steps and perform this very procedure with a regular SmartCenter. The only exception is that in a regular SmartCenter you **don't need** to set the environment with *mdsenv* before running DBedit. Remember *mdsenv* is only needed in Provider-1 to set the proper environment in the shell, so the variables and directories point to one specific CMA (which usually is a customer).

The following lines will show how to export objects from the Global Database, so they can be imported into a CMA (*cma1*). First we need to transfer the Global Objects database file to the machine where Object Dumper is running. Remember that this is the *objects_5_0.C* file in the MDS, so we have to set the environment accordingly using *mdsenv*.

```
[Expert@p1ngxr62]# mdsenv
[Expert@p1ngxr62]# cd $FWDIR/conf
```

```
[Expert@p1ngxr62]# ls -la objects_5_0.C
-rw-rw-r--    1 root      root         662458 Dec 21 14:28 objects_5_0.C
[Expert@p1ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> put objects_5_0.C objects_5_0_global.C
local: objects_5_0.C remote: objects_5_0_global.C
227 Entering passive mode (10,20,30,76,6,239)
125 Using existing data connection
################################################################################
################################################################################
#############################################################################
226 Closing data connection; File transfer successful.
689622 bytes sent in 0.621 secs (1.1e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]#
```

Now the file is transferred. Let's use Object Dumper to export the objects to a CSV file:

```
D:\Stuff\OFiller\v2.4>odumper -f objects_5_0_global.C -o global_export.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
================================================================================

================================================================================
 * Processing objects...
--------------------------------------------------------------------------------
.................................................................................
.............................

================================================================================
Processed 27164 possible objects and found 159 valid ones.
It took 2.0 seconds on quiet mode.
Total successfully processed Hosts = 10
Total successfully processed Networks = 101
================================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

Before importing the objects list into the CMA *cma1*, is necessary to edit the output file (*global_export.csv* in this example) and remove the objects you don't need to import, such as services and extra objects – as we previously saw. Then use Object Filler to convert the edited file to a DBedit script:

```
D:\Stuff\OFiller\v2.4>ofiller -f global_export_final.csv -i csv -o cma1_import.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
===============================================================================
Processing objects...
......................................
===============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 223 possible objects and/or rules.
Found 111 total valid (or successfully processed) objects/rules.
-------------------------------------------------------------------------------
Total successfully processed Hosts = 10
Total successfully processed Networks = 101
-------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
===============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Then you need to transfer the output file (*cma1_import.dbedit* in this example), to the MDS machine and perform the import procedure. Remember to set the environment appropriately using *mdsenv*

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la
total 172
drwx------    2 root     root            4096 Dec 21 15:20 .
drwxr-xr-x    4 root     root            4096 Dec 21 06:32 ..
-rw-------    1 root     root               0 Dec 21 15:17 .bash_history
-rw-r--r--    1 root     root              24 Dec 21 06:32 .bash_logout
-rw-r--r--    1 root     root             191 Dec 21 06:32 .bash_profile
-rw-r--r--    1 root     root             124 Dec 21 06:32 .bashrc
-rw-rw----    1 root     root           25252 Dec 21 12:43 cma1.dbedit
-rw-rw----    1 root     root           35640 Dec 21 15:20 cma1_import.dbedit
-rw-rw----    1 root     root           32762 Dec 21 13:11 cma2.dbedit
-rw-rw----    1 root     root            2656 Dec 21 13:33 global.dbedit
-rw-rw----    1 root     root           32964 Dec 21 14:27 import_global.dbedit
[Expert@p1ngxr62]# mdsenv cma1
[Expert@p1ngxr62]# dbedit -s localhost -u admin -f cma1_import.dbedit
Enter Administrator Password: secret
Host_172.16.10.1 updated successfully.
Host_172.16.10.2 updated successfully.
   .
   .
   .
Host_172.16.10.10 updated successfully.
Net_192.168.0.0 updated successfully.
   .
   .
   .
Net_192.168.99.0 updated successfully.
Net_192.168.100.0 updated successfully.
[Expert@p1ngxr62]#
```

You can see that the objects imported from the Global Objects database (Networks within the 192.168.0.0/16 address space and Hosts from the 172.16.10.0/24 network) appear now within the *cma1* context. Launch SmartDashboard over *cma1* to verify this
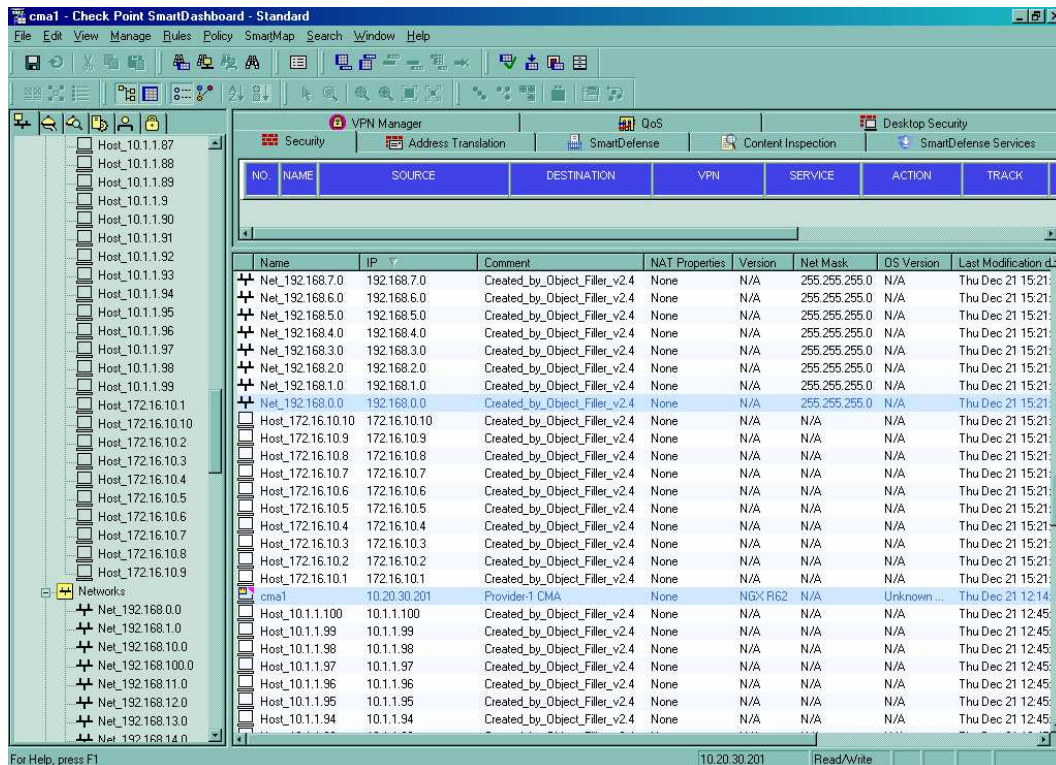

Figure 11 –SmartDashboard open over cma1 after successfully importing objects from the Global Database into it

Now you have the objects combined in one CMA (*cma1* on this case), as it was intended from the beginning…

6. Special operations involving objects and rules

Here we will discuss special operations that can be done with Object Filler and Object Dumper and involve both objects and rules. Even though the usage of rules has not been explained up to now, since the sections will be divided in objects and rules, you can skip to the proper section if you want to pass just one part of the configuration.

For this section we won't explain on detail the objects part, since that was explained in the previous chapters of this document. The objects section is shown here so the document can be used as a quick reference when needed, but it is assumed that if details are needed, the proper section needs to be read.

6.1 Cautions before performing any operation

The following points are valid for all the operations explained on the sections below. So, reading this section will save you headaches later.

a) Backup everything. Include a full backup (using the *backup* facility on *Nokia IPSO* or *Check Point SecurePlatform* will save as well operating system information) and then a Database Revision Control entry. If possible (on IPSO and SecurePlatform) take as well a *snapshot* entry, just to be on the safe side. I know it sounds basic, but most of the times (let's admit it) we forget or believe it's easy to skip it, just to find out later we would need to recover. So, always backup. Even if you are running a partially damaged configuration, at least you know the state of the environment before performing any procedure. You might need to recover later to a known point, and this is the chance

b) Not all objects or parameters are moved/merged. Remember Object Filler and Object Dumper (the tools) only deal with objects and rules:
b.1- Users are not passed. You may need to take a look at *fwm dbimport* and *fwm dbexport* to pass users and groups. References to such commands appear on the Command Line Interface (CLI) User Guide manual (part of the standard set of Check Point manuals). If you have any RADIUS, Secure ID, LDAP or any other user database configured, you might need to reconfigure as well. In all the cases, if the configuration you are passing involves User Groups, make sure such User Groups exist as well on the target environment.
b.2- Check Point Gateways or Host properties such as Products Installed or Log Settings are not passed.
b.3- VPN Communities are not passed. This includes any configuration related to VPN Communities and associated gateways, such as configuration type, pre-shared secrets, etc.
b.4- SmartDefense settings are not passed. Those would need to be reconfigured manually if they were manually changed. However, remember that host settings for DNS, Web and Mail servers are objects properties that can be handled with the tools.

b.5- Resources are partially supported. If you are going to pass resources, make sure you pass them manually. If you let the tools to handle them, they will create a resource with the same name of the appropriate type (URI, SMTP, FTP, etc.) but the properties for the resource itself will not be passed.

b.6- Global properties are not passed. If there are global properties different from the defaults, those must be manually passed.

b.7- Certificates (from ICA or any other CA) are not passed. This means all the certificates must be manually passed, or revoked and created again (depending on how your CA handles situations when you move the configuration).

b.8- SIC trust relationships are not passed. Since when you install a new CMA (or SmartCenter) a new ICA root certificate is created, automatically you need to establish trust again with any managed device (establish SIC between the gateway and the new CMA/SmartCenter)

b.9- Points b.1, b.7 and b.8 are as well relevant if you have deployed internal certificates for VPN users. As the new CMA will have a new root ICA certificate, such certificates become invalid, and you will need to issue certificates for all your users again.

b.10 Just to make sure, sections 9.4 and 9.5 of the *User's Manual* will tell you the objects supported by the tools. Take a look on these tables to be sure you are using the tools to process the right kind of objects.

b.11 Time Objects do not pass automatically. They have to be manually copied over as well.

b.12 Object Filler and Object Dumper (the tools) can deal with Automatic NAT rules, but they can NOT deal with Manual NAT rules.

b.13 The tools do NOT support QoS policies.

b.14 The tools do NOT support Desktop Security policies.

b.15 If you have User, Client or Session Authentication rules, the authentication properties (the ones you have access to when you double-click on the *Action* item of the rule) are NOT processed by the tools.

b.16 The tools don't take care of any third-party device (Including OPSEC servers)

b.17 The tools don't take care of any Content Inspection settings.

As a reminder, all of the points above can be saved if you use the *migrate_assist* and *cma_migrate* supported scripts, when this option is available (such as when moving from SmartCenter to a CMA). Those are as well not needed to be considered if you are using *upgrade_export*/*upgrade_import* when this option is available (such as when moving from SmartCenter to SmartCenter). So, if you can workaround and NOT use Object Filler and Object Dumper, then do…

All of the above are reasons of why you should use Object Filler and Object Dumper as your very last resort: when there is no other supported way to do whatever you are trying to do.

c) Always use the –v (*verbose*) switch of the tools. Especially with Object Filler, since this is the part where you prepare the configuration to be imported. Using this option will

give you a detailed view on how the processing is done line by line, will give you indication of any potential problems (look for the **WARNING** and **Failed** messages), and will give you as well a report on objects, services and groups processed. As an advice, it's easier to redirect the –v output to a file, and then editing the file with a text editor.

d) Always audit and compare the results of the imported configuration before taking it to production. One way to do it is using Object Dumper to dump the configuration again and compare it with the original dump from the source, and compare. You have to manually review the configuration you passed manually. By experience (and per best-practice), it is better if a different person from the one that passed the configuration performs the audit.

e) After you are absolutely sure everything went fine, backup everything (again). At this point, you are backing-up a new configuration that is ok. This time, include as well a Database Revision Control entry, just in case.

f) If possible, have the new configuration with no additional changes, under testing (*staging* if you want to look at it this way) on the production environment, for at least one week. If one week is not possible, have it the more time you can and document the changes done for at least one month. If issues arise later (such as a rule you forgot to pass) or there is a conflict later, you know you can go back to this known state.

6.2 Moving a configuration from a SmartCenter to a CMA

There is an official and supported way to import object from a SmartCenter Server into a CMA: you have the *migrate_assist* and *cma_migrate* scripts to help you on this task. These tools are extensively covered on *SecureKnowledge*, the Provider-1 documentation and the *Upgrade Guide* that comes with every version of the Check Point Software. The *Upgrade Guide* is great document all along. Don't miss it.

So, if you are trying to migrate from a SmartCenter to a CMA, it is better to follow such path, which is supported.

There might be special reasons of why you want to pass the configuration using Object Filler and Object Dumper: perhaps you want to take a look on the objects you are about to move on a CSV format first and then delete some of the objects you don't need anymore. Perhaps you have a partially damaged configuration and you want to rebuilt most of it as if you were doing it for the scratch. In any case, whatever the reason you have, it is better for you to consider that using Object Filler and Object Dumper to move configuration from a SmartCenter to a CMA is NOT the officially supported procedure, and you are going to perform additional steps that if you do it automatically. If you reached to this point and still want to do it, let's continue…
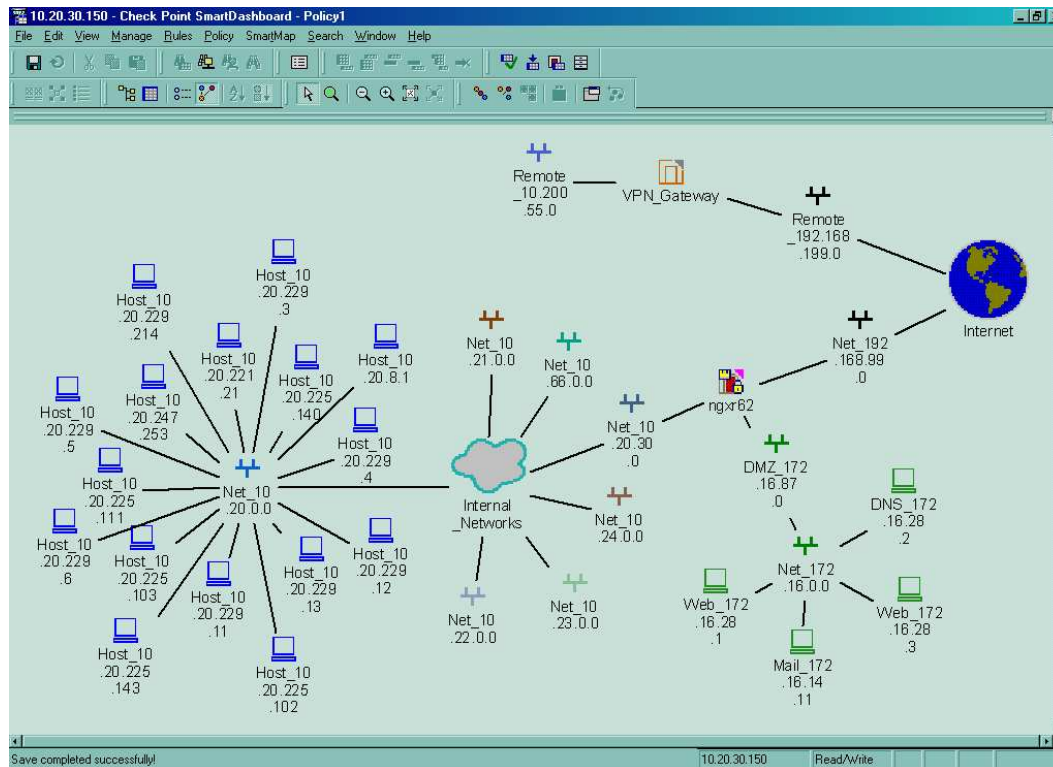
6.2.1 Scenario (environment) for the operations

In order to move a configuration from a SmartCenter to a CMA, one configured SmartCenter must exist and one configured CMA must exist. We will say the CMA is named *cma3* and the SmartCenter lives on a StandAlone installation and is named *ngxr62*

Let's assume we have the SmartCenter with the following rules:

The network topology perhaps looks like this:

Check section 6.1 before going ahead.

6.2.2 Cautions before performing any operation

Again, check section 6.1 before going ahead.

Especially, make sure the Check Point objects (gateways, SmartCenters, etc.), users, user groups, VPNs and resources have been created manually first.

You need to check them on the SmartCenter first:
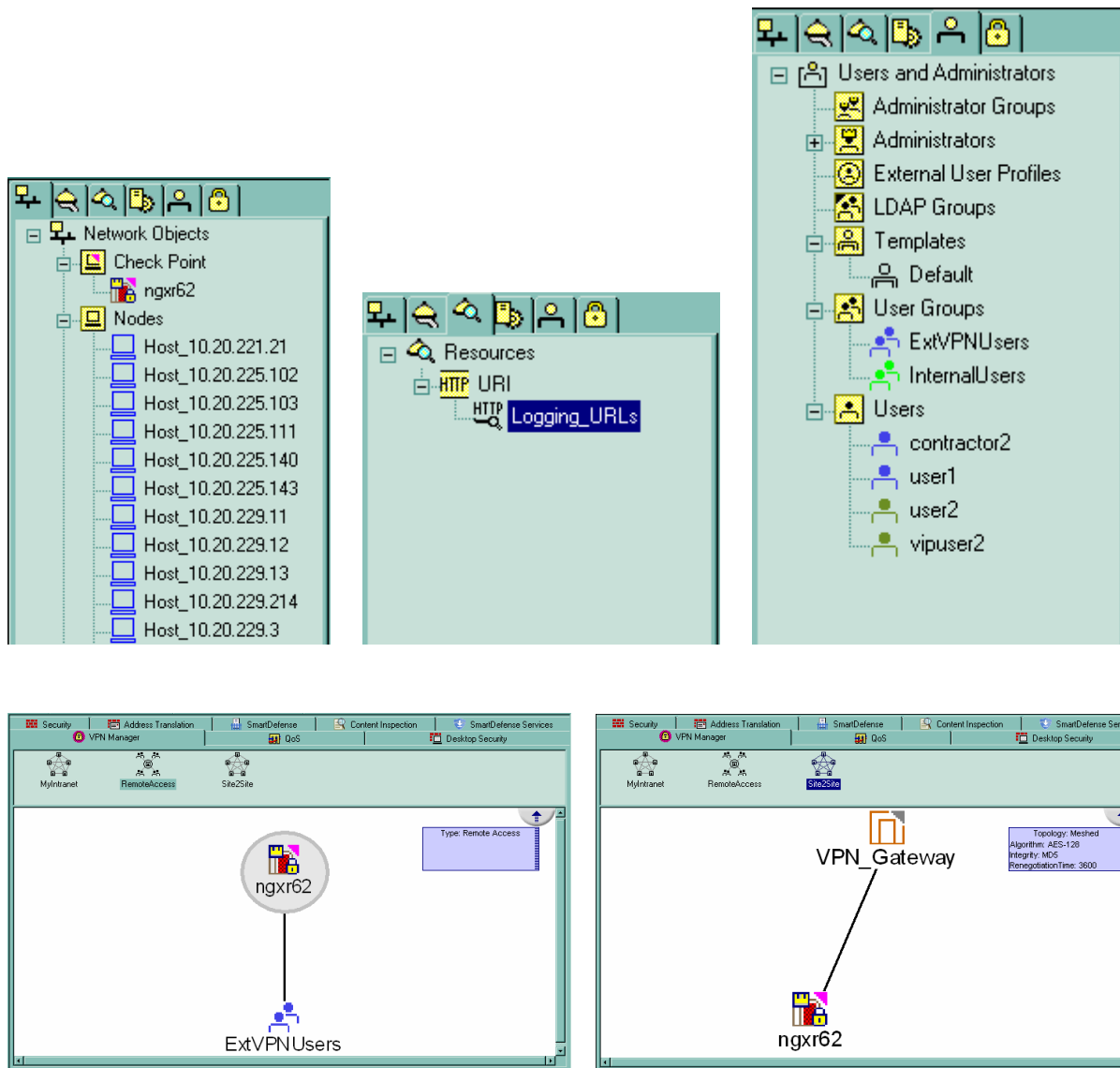
So, let's go to the CMA and make sure you have passed all the above mentioned elements.

- **Users and User Groups**

We will use *fwm dbexport* and *fwm dbimport* for this. Both are documented on the *Command Line Interface (CLI)* Manual, and you can check the full syntax there. On this case, both systems are NGX R62 and that's why this works. Most of the times, doing this even with different versions should work, but you better test it first.

On the original SmartCenter server (*ngxr62* on this case), make sure there is no GUI connected so it doesn't affect our operations:

```
[Expert@ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------
|Client type|Administrator|Host|Database lock|
-----------------------------------------------
-----------------------------------------------
```

Now do the following to export the groups:

```
[Expert@ngxr62]# fwm dbexport -v  -g  -f /home/admin/groups.db
 DBExport> db_exp_main(): Start of execution
Done.
[Expert@ngxr62]# pwd
/home/admin
[Expert@ngxr62]# ls -l groups.db
-rw-rw----    1 root     root            117 Dec 20 10:31 groups.db
```

As a catch, groups cannot be automatically imported. We will have to re-create them manually anyway, but having them exported is good for backup purposes. You never know.

Now, do the following to export the users:

```
[Expert@ngxr62]# fwm dbexport -v -f /home/admin/users.db
 DBExport> db_exp_main(): Start of execution
Done.
[Expert@ngxr62]# pwd
/home/admin
[Expert@ngxr62]# ls -l users.db
-rw-rw----    1 root     root           1449 Dec 20 10:32 users.db
```

As you can see, both files are ASCII files:
```
[Expert@ngxr62]# pwd

/home/admin
[Expert@ngxr62]# file *.db
groups.db: ASCII text
users.db:  ASCII text, with very long lines
```

So, transfer those files (remember, as ASCII files) to the target CM, and check they are there:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la *.db
-rw-rw----    1 root     root            117 Dec 21 17:36 groups.db
```

```
-rw-rw----   1 root    root          1449 Dec 21 17:36 users.db
[Expert@p1ngxr62]# file *
groups.db: ASCII text
users.db:  ASCII text, with very long lines
```

Once you verified they are on the target system, let's check *cma3* (our target CMA) is up and running.

```
[Expert@p1ngxr62]# mdsstat
+------------------------------------------------------------------------------+
|                       Processes status checking                              |
+-----+----------------+----------------+----------+----------+----------+----------+
| Type| Name           | IP address     | FWM      | FWD      | CPD      | CPCA     |
+-----+----------------+----------------+----------+----------+----------+----------+
| MDS |       -        | 10.20.30.200   | up 1213  | up 1212  | up 1497  | up 1460  |
+-----+----------------+----------------+----------+----------+----------+----------+
| CMA | cma1           | 10.20.30.201   | up 2966  | up 2965  | up 2940  | up 2978  |
| CMA | cma2           | 10.20.30.202   | up 3562  | up 3561  | up 3536  | up 3576  |
| CMA | cma3           | 10.20.30.203   | up 6228  | up 6227  | up 6209  | up 6249  |
+-----+----------------+----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3     3 up   0 down                           |
| Tip: Run mdsstat -h for legend                                               |
+------------------------------------------------------------------------------+
```

Now, let's put ourselves into the environment of *cma3* (our target CMA) and check no GUI is connected:

```
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK

Connected clients
-------------------------------------------------
|Client type|Administrator|Host|Database lock|
-------------------------------------------------
-------------------------------------------------
```

Now, let's recreate the groups first. Remember that groups cannot be automatically imported, so just create them on the *SmartDashboard*. (You can and should create a *Database Revision Control* entry at this point, before doing anything, so you have a "backup" to be on the safe side of a known state). You can view the groups.db file to see what User Group names you had and need to recreate and have copy-paste to give you hand

```
[Expert@p1ngxr62]# cat groups.db
name;   groups; color;  comments;        is_administrator_group;
ExtVPNUsers;    ;       blue1;  ;        ;
```

```
InternalUsers;  ;        olive drab;      ;          ;
```

After the re-creation of the groups, you should have something like this:
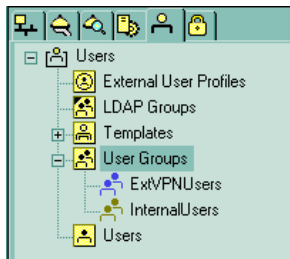
Then, exit from SmartDashboard and finally, let's import the users, which can be done automatically

```
[Expert@p1ngxr62]# fwm dbimport -v -f /home/admin/users.db
 Trying to import file /home/admin/users.db. Import_mode is: add
 Connecting to database
 writing the new users to database...
 creating user user1...
 creating user user2...
 creating user contractor2...
 creating user vipuser2...
 4 users were written to database
 Done
[Expert@p1ngxr62]#
```

If for some reason you didn't create all the groups, on this phase will have errors. If you passed all this successfully, you will end up with something like the following:
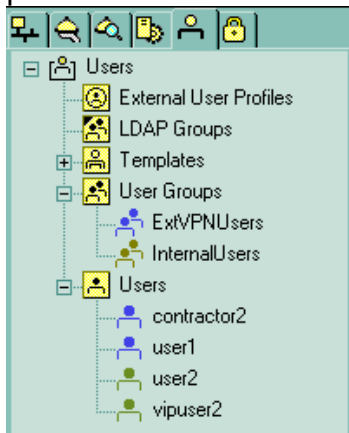
If you are getting a versions conflict at this point, you would need to pass manually the users, and handle their passwords according to what you have on your password management policy to notify them on password changes.

- **Resources**

The resources (URI, SMTP, TCP, etc.) must be manually passed, so… just open the resource on the original SmartCenter and check the properties. Then create one just exactly like it on the CMA. Below an example for a URI resource
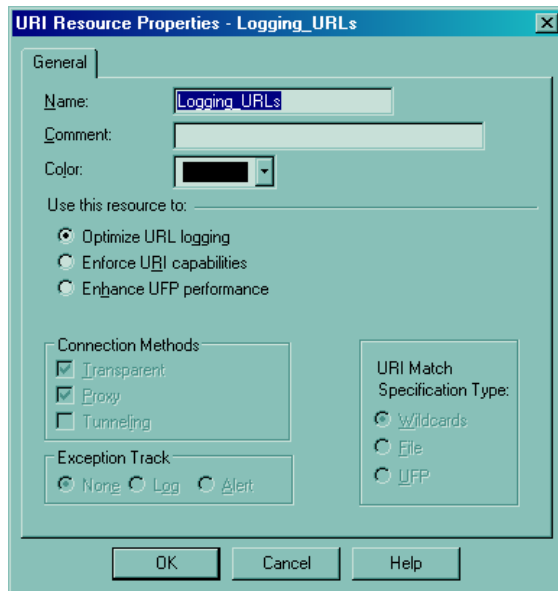

- **VPN Communities**

Even though you will NOT have any members yet on the VPN Communities, at least make sure all the communities are created with the exactly same names you have on the original SmartCenter. They will be on default by now. That's OK:
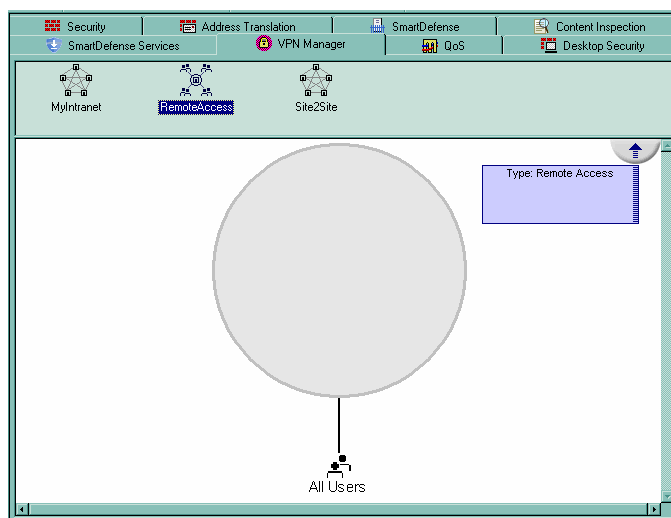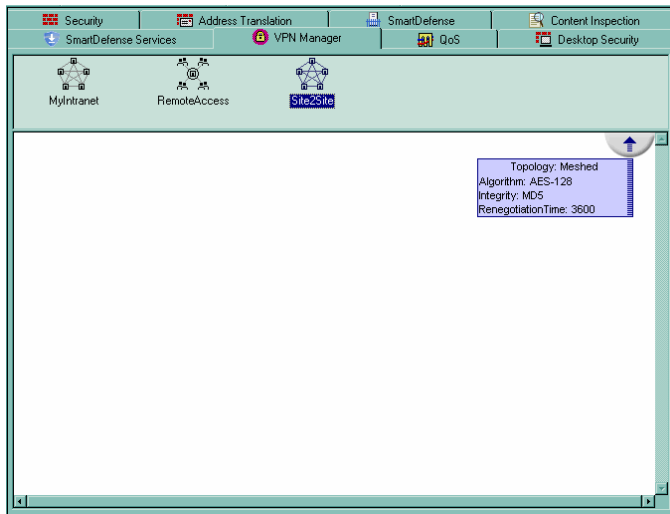
- **Check Point Gateway objects**

Create them with the <u>exactly</u> same name you used for them originally. The IP doesn't need to match, so you may change the IP address if that is needed, but the name has to be the same. Preferably establish SIC with them, but if that it is not possible, at least create them. This is important because some of the objects (such as Automatic NATs or protection properties for Web, DNS and Mail Servers) and the rules, may reference to such objects. On this case, since the original gateway has as name *ngxr62*, we will create an object with this name and at least *Firewall* marked under *Check Point Products*:
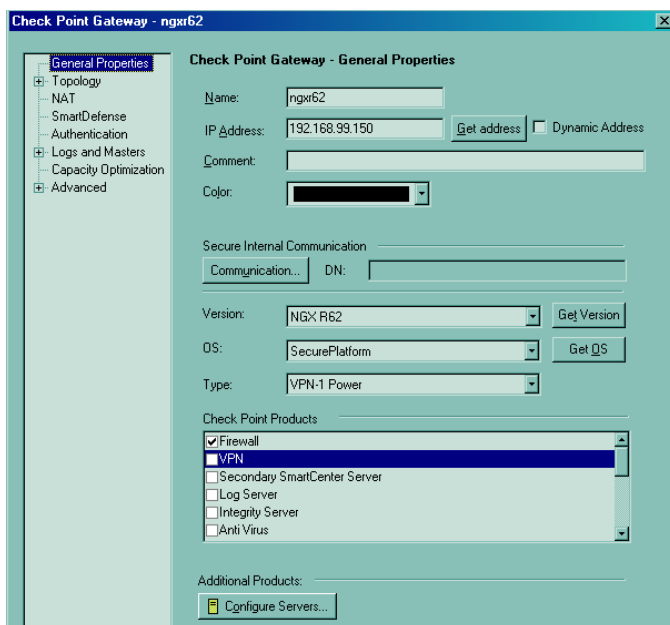
Your objects list should look like this:
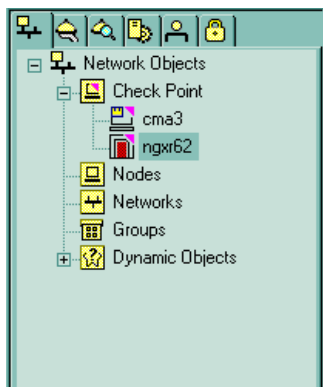
Now you are ready for the next step.

6.2.3 Moving the objects

Obtain the *$FWDIR/conf/objects_5_0.C* file from your original SmartCenter and transfer it to the machine where you have Object Dumper and Object Filler:

```
[Expert@ngxr62]# cd $FWDIR/conf
[Expert@ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> put objects_5_0.C objects_5_0_SmartCenter.C
local: objects_5_0.C remote: objects_5_0_SmartCenter.C
227 Entering passive mode (10,20,30,76,16,103)
125 Using existing data connection
##############################################################################
##############################################################################
##############################################################################
##########################################################################
226 Closing data connection; File transfer successful.
786164 bytes sent in 0.654 secs (1.2e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@ngxr62]#
```

Now, run Object Dumper over it to get a CSV file with the objects listed:

```
D:\Stuff\OFiller\v2.4>dir obj*.C
```

```
 Volume in drive D is Data
 Volume Serial Number is 88AE-1253

 Directory of D:\Stuff\OFiller\v2.4

28/12/2006  10:57 p.m.          786,164 objects_5_0_SmartCenter.C
                1 File(s)       786,164 bytes
                0 Dir(s)     862,584,832 bytes free

D:\Stuff\OFiller\v2.4>odumper -f objects_5_0_SmartCenter.C -o objssmc.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
===============================================================================

===============================================================================
 * Processing objects...
-------------------------------------------------------------------------------
...............................................

===============================================================================
Processed 30823 possible objects and found 97 valid ones.
From these, 7 were NATted records. It took 3.0 seconds on quiet mode.
Total successfully processed CP Gateways = 1
Total successfully processed Hosts = 20
Total successfully processed Interoperable Devices = 1
Total successfully processed Networks = 12
Total successfully processed Interfaces = 5
Total successfully processed Groups = 1
Total successfully processed Group Elements = 10
Total successfully processed TCP Services = 6
Total successfully processed UDP Services = 6
Total successfully processed URI Resources = 1
===============================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

Then edit the CSV file to remove the objects that you won't need. Those include the resources (which you manually passed) and the Check Point Gateways and its associated interfaces, for which you will take care manually (Which is the best anyways for this kind of cases).

Over the resulting file (the one that doesn't have the objects above mentioned), let's run Object Filler this way:

```
D:\Stuff\OFiller\v2.4>ofiller -f objssmc_final.csv -i csv -o objssmc.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
===============================================================================
Processing objects...
...............
===============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 99 possible objects and/or rules.
Found 49 total valid (or successfully processed) objects/rules.
Found 7 total NATted records.
-------------------------------------------------------------------------------
Total successfully processed Hosts = 20
 - Total successfully processed Web Server Hosts = 2
   WARNING: These objects are only valid on NG+AI R55 or higher
 - Total successfully processed DNS Server Hosts = 1
   WARNING: These objects are only valid on NG+AI R55W or higher
 - Total successfully processed Mail Server Hosts = 1
   WARNING: These objects are only valid on NG+AI R55W or higher
Total successfully processed Interoperable Devices = 1
Total successfully processed Networks = 12
Total successfully processed Groups = 2
Total successfully processed Group Elements = 10
Total successfully processed TCP Service objects = 6
Total successfully processed UDP Service objects = 6
Total successfully processed Interface entities = 2
```

```
--------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
================================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Transfer the resulting DBedit file to the MDS system, where we will import it under the environment of the target CMA (*cma3* in out case). Remember the usual cautions when doing this:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> get objssmc.dbedit
local: objssmc.dbedit remote: objssmc.dbedit
227 Entering passive mode (10,20,30,76,16,104)
125 Using existing data connection
####################
226 Closing data connection; File transfer successful.
19475 bytes received in 0.0602 secs (3.2e+02 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -la objssmc.dbedit
-rw-rw----    1 root     root        19120 Dec 21 18:28 objssmc.dbedit
[Expert@p1ngxr62]# mdsstat
+--------------------------------------------------------------------------------+
|                        Processes status checking                               |
+-----+----------------+----------------+----------+----------+----------+----------+
| Type| Name           | IP address     | FWM      | FWD      | CPD      | CPCA     |
+-----+----------------+----------------+----------+----------+----------+----------+
| MDS |       -        | 10.20.30.200   | up 1213  | up 1212  | up 1497  | up 1460  |
+-----+----------------+----------------+----------+----------+----------+----------+
| CMA | cma1           | 10.20.30.201   | up 2966  | up 2965  | up 2940  | up 2978  |
| CMA | cma2           | 10.20.30.202   | up 3562  | up 3561  | up 3536  | up 3576  |
| CMA | cma3           | 10.20.30.203   | up 6228  | up 6227  | up 6209  | up 6249  |
+-----+----------------+----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3     3 up   0 down                             |
| Tip: Run mdsstat -h for legend                                                  |
+--------------------------------------------------------------------------------+
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# cpstat mg
```

```
Product Name:   Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK


Connected clients
------------------------------------------------
|Client type|Administrator|Host|Database lock|
------------------------------------------------
------------------------------------------------
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ls -l objssmc.dbedit
-rw-rw----    1 root     root         19120 Dec 21 18:28 objssmc.dbedit
 [Expert@p1ngxr62]# dbedit -s localhost -u admin -f objssmc.dbedit
Enter Administrator Password: secret
Net_172.16.0.0 updated successfully.
Net_10.20.0.0 updated successfully.
    .
    .
    .
UDP_Port_135 updated successfully.
UDP_Port_137 updated successfully.
    .
    .
    .
Mail_Services updated successfully.
Mail_Services updated successfully.
[Expert@p1ngxr62]#
```

At this point, you should have your objects passed.

6.2.4 Moving the rules

The process of moving the rules is somewhat similar to moving the objects.

First, gather the $FWDIR/conf/rulebases_5_0.fws from the original SmartCenter and transfer it to the machine where you have Object Dumper and Object Filler:

```
[Expert@ngxr62]# cd $FWDIR/conf
[Expert@ngxr62]# ls -l rulebases_5_0.fws
-rw-rw----    1 root     root         37037 Dec 20 10:55 rulebases_5_0.fws
[Expert@ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
```

Page 42

```
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> put rulebases_5_0.fws rulebases_5_0_SmartCenter.fws
local: rulebases_5_0.fws remote: rulebases_5_0_SmartCenter.fws
227 Entering passive mode (10,20,30,76,16,123)
125 Using existing data connection
####################################
226 Closing data connection; File transfer successful.
38731 bytes sent in 0.00808 secs (4.7e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@ngxr62]#
```

Now, run Object Dumper over this file, using the following syntax:

```
D:\Stuff\OFiller\v2.4>odumper -p rulebases_5_0_SmartCenter.fws -o policysmc.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
================================================================================

================================================================================
 * Processing rules...
--------------------------------------------------------------------------------
.............

================================================================================
Processed 1694 possible objects and found 16 valid ones.
It took 2.0 seconds on quiet mode.
Total successfully processed Rules = 16
================================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

Now we have all the rules on this CSV file. You may take a look at it if you want:

In reality, the original CSV file looks uglier, but the format is quite helpful:

The next step is running Object Filler over this file with a special syntax, to make it process the rules:

```
D:\Stuff\OFiller\v2.4>ofiller -f policysmc.csv -i csv -p policy -nopv -o
policysmc.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
============================================================================
```

```
Processing objects...

==============================================================================
Rules processing requested: Processing rules now!!!
.......................................
==============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 49 possible objects and/or rules.
Found 11 total valid (or successfully processed) objects/rules.
Rules processing was requested and done for Policy "Policy1".
------------------------------------------------------------------------------
Total successfully processed Rules = 16
------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
==============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Then transfer the DBedit File to the MDS, enter the proper environment and import the file. Remember the usual cautions to make of this a success:

```
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> get policysmc.dbedit
local: policysmc.dbedit remote: policysmc.dbedit
227 Entering passive mode (10,20,30,76,16,128)
125 Using existing data connection
##########
226 Closing data connection; File transfer successful.
10779 bytes received in 0.0111 secs (9.5e+02 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]# ls -la policysmc.dbedit
-rw-rw----    1 root     root        10608 Dec 21 19:03 policysmc.dbedit
[Expert@p1ngxr62]# mdsstat
+------------------------------------------------------------------------------+
|                        Processes status checking                             |
+-----+----------------+----------------+---------+---------+---------+---------+
| Type| Name           | IP address     | FWM     | FWD     | CPD     | CPCA    |
+-----+----------------+----------------+---------+---------+---------+---------+
| MDS |       -        | 10.20.30.200   | up 1213 | up 1212 | up 1497 | up 1460 |
+-----+----------------+----------------+---------+---------+---------+---------+
```

```
| CMA  | cma1          | 10.20.30.201    | up 2966  | up 2965  | up 2940  | up 2978  |
| CMA  | cma2          | 10.20.30.202    | up 3562  | up 3561  | up 3536  | up 3576  |
| CMA  | cma3          | 10.20.30.203    | up 6228  | up 6227  | up 6209  | up 6249  |
+-----+---------------+-----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3      3 up    0 down                              |
| Tip: Run mdsstat -h for legend                                                    |
+-----------------------------------------------------------------------------------+
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK


Connected clients
------------------------------------------------
|Client type|Administrator|Host|Database lock|
------------------------------------------------
------------------------------------------------

[Expert@p1ngxr62]# dbedit -s localhost -u admin -f policysmc.dbedit
Enter Administrator Password:
Policy1 updated successfully.
##Policy1 updated successfully.
##Policy1 updated successfully.
   .
   .
   .
##Policy1 updated successfully.
##Policy1 updated successfully.
[Expert@p1ngxr62]#
```
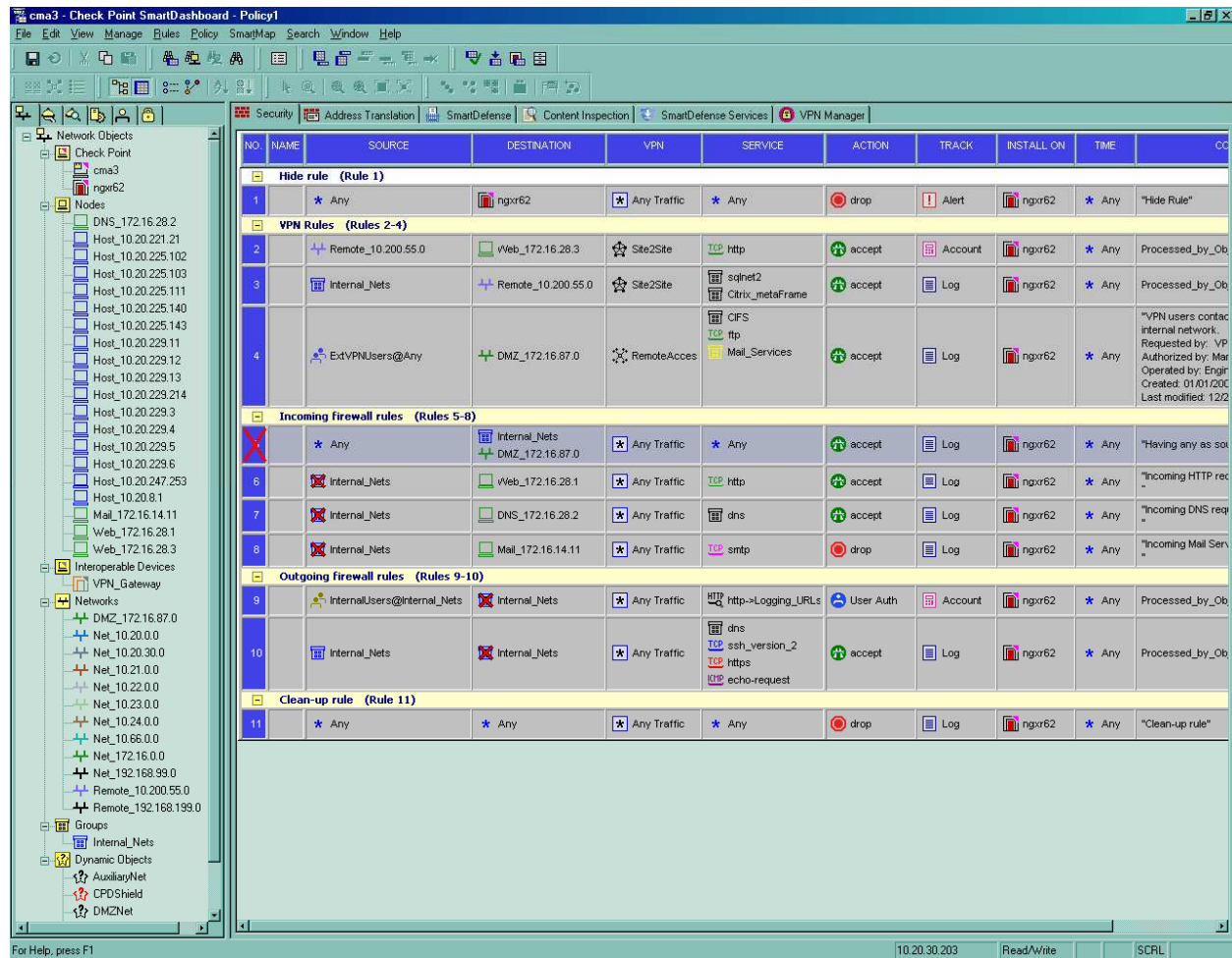
This should have your rules successfully imported. Let's open the SmartDashboard and take a look:
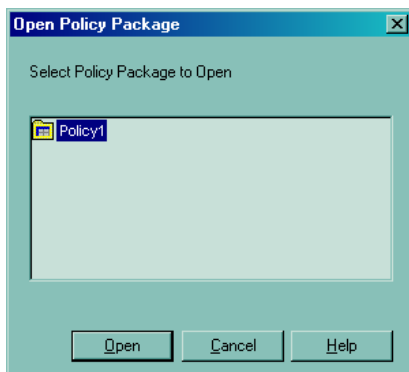
6.2.5 Completing and verifying the configuration

In short, review that all the manual items you need to pass, passed fine. The following is NOT an exhaustive list, but it marks some of the important items that your list should include:
- Configure properly the VPN communities. Add members to them, change properties as required
- Modify the Global properties accordingly
- Modify the Authentication properties on the Security Rules
- Recreate the Manual NAT rules, Desktop Security rules and/or QoS rules as needed
- Modify the SmartDefense settings as required.
- Finish configuring the gateway properties (such as Log Servers, Concurrent Connections, Products installed on the gateway, etc.)
- Set the proper policy targets to the relevant policy packages
- Install Policy to the relevant gateways.

## *6.3 Moving a configuration from a CMA to a SmartCenter*

This section of the document covers the opposite procedure as of what we discussed on the section 6.2 of this document. The steps are pretty much the same, so I would repeat them here, with the necessary modifications to make it from a CMA to a SmartCenter.

The steps would be the same as well if you need to move configuration from one CMA to another, with the exception that you would need to be changing environments (using *mdsenv*) all the time. But the same procedure should work.

To give you an idea on what we will do here, reading section 6.1 of this document is strongly suggested, if you have not done so yet; because (Again) the steps will be pretty much the same, and is important to understand the differences when moving a configuration from a CMA to a SmartCenter with regards to moving the configuration from a SmartCenter to a CMA.

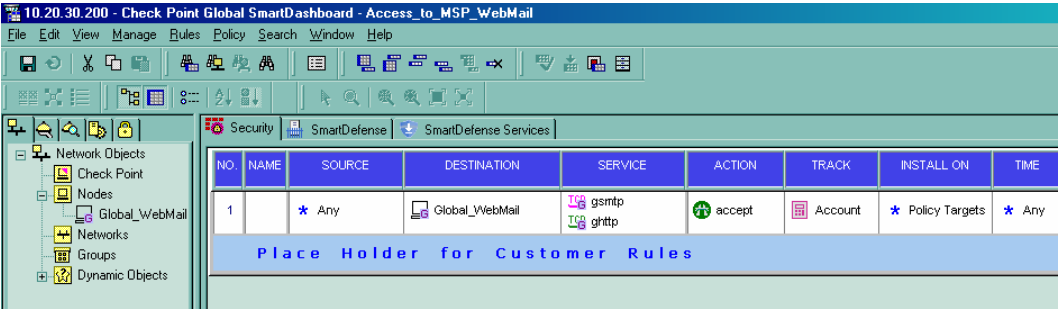### 6.3.1 Scenario (environment) for the operations

The view on the Multi Domain GUI for the relevant CMA is as follows:
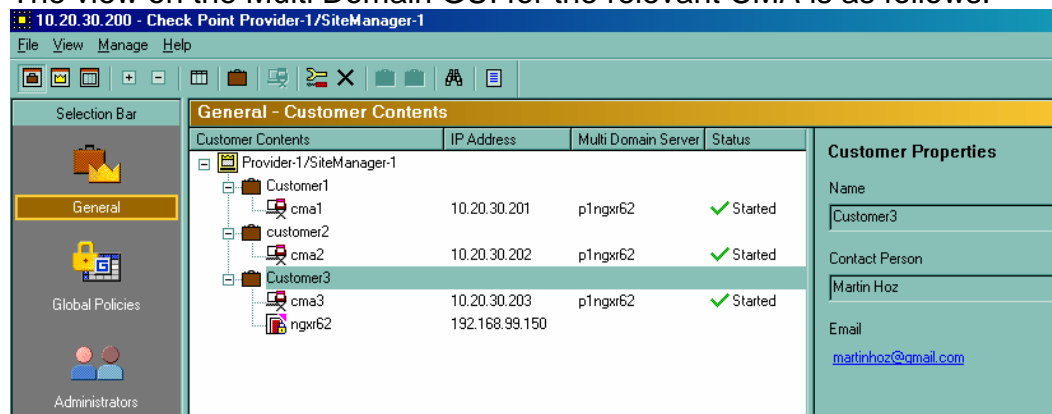
The following is a screenshot of the assigned Global policies window. Please note the CMA we are trying to deal with has a Global Policy Assigned
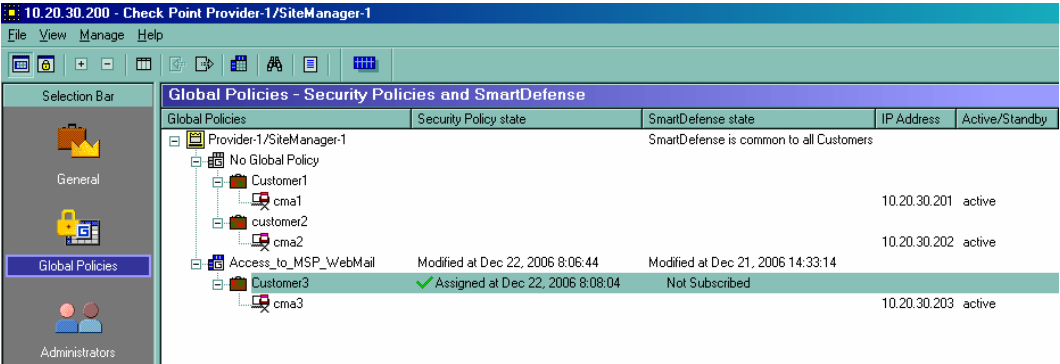
The following is a screenshot of the Global SmartDashboard on the global policy that *cma3* has assigned

The following is a screenshot of the rulebase as it appears on the CMA

The following is a SmartMAP screenshot with the topology for the Network we are dealing with:
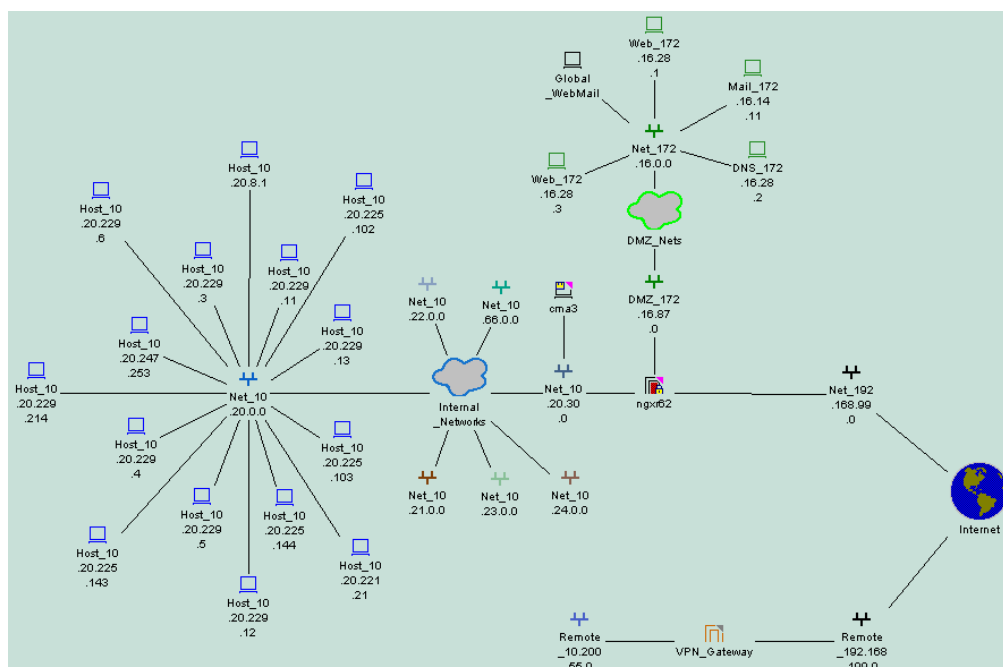
The Check Point Objects, Users Groups, VPN Communities, OPSEC objects, Servers and Resources are as follows:
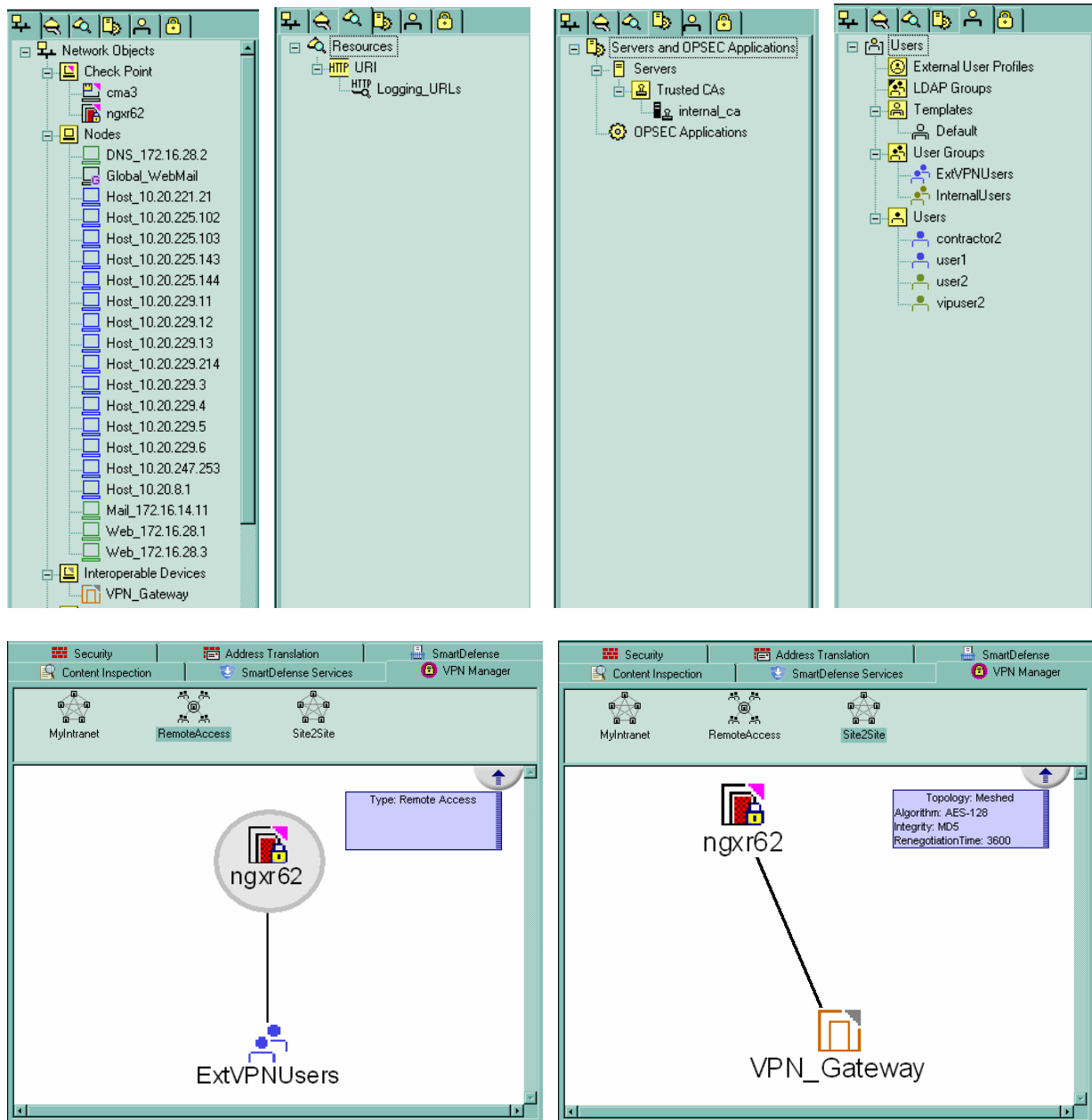
Notice that by definition, since it's a CMA, the installation is distributed. The CMA's name is *cma3* and the gateway name is *ngxr62*.

Now, let's assume we want to move this environment to a StandAlone configuration (SmartCenter + Gateway on the same machine). Let's say the new machine has as

name *newngxr62*. This impacts a lot on the references we have on rules, Automatic NAT rules (NATted objects), Servers (objects marked as Web or DNS servers).

Below a screenshot for the initial configuration for the target StandAlone System
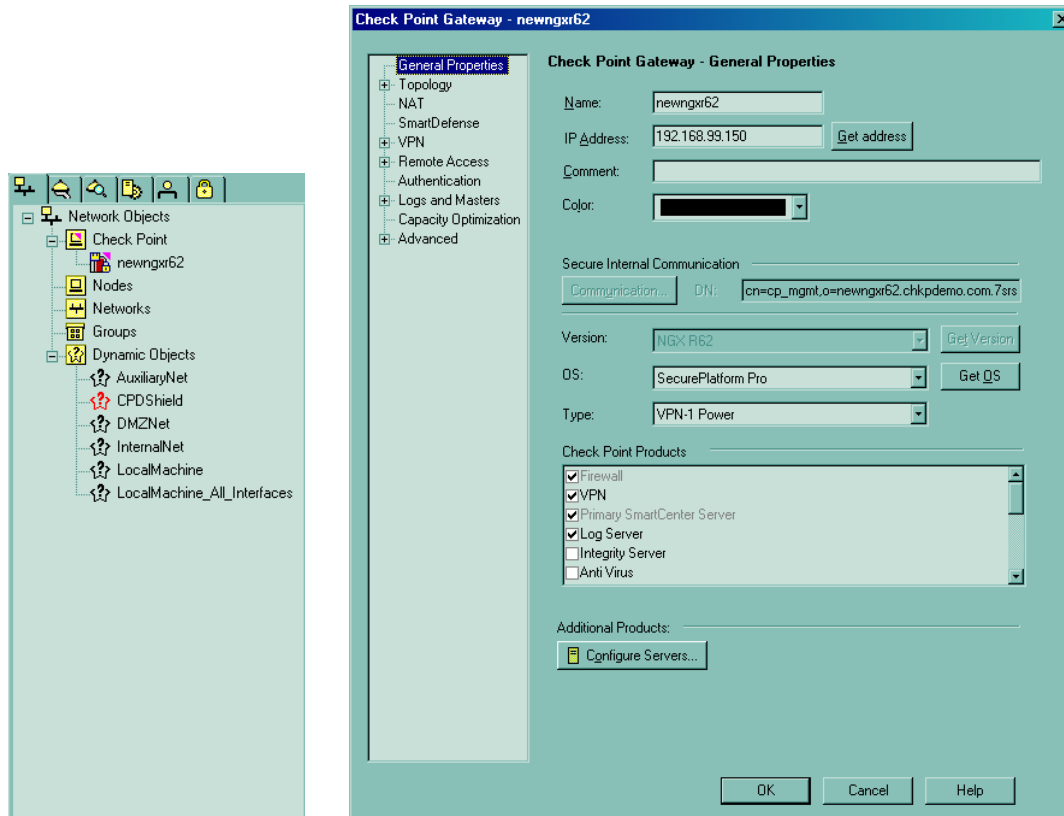
We will deal with the fact of different names for the gateway in the following sections.

6.3.2 Cautions before performing any operation

Again, check section 6.1 before going ahead. The 5 minutes (or less) you will use to read it are worth your time.

Especially, make sure the Check Point objects (gateways, SmartCenters, etc.), users, user groups, VPNs and resources have been created manually first in the new SmartCenter.

- **Users and User Groups**
We will use the *fwm dbexport* command to export the users information from the CMA, and then *fwm dbimport* to import such users into the SmartCenter

```
[Expert@p1ngxr62]# mdsstat
```

```
+--------------------------------------------------------------------------------+
|                          Processes status checking                             |
+-----+----------------+-----------------+----------+----------+----------+----------+
| Type| Name           | IP address      | FWM      | FWD      | CPD      | CPCA     |
+-----+----------------+-----------------+----------+----------+----------+----------+
| MDS |       -        | 10.20.30.200    | up 1364  | up 1363  | up 1362  | up 1635  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| CMA | cma1           | 10.20.30.201    | up 1340  | up 1335  | up 1290  | up 1637  |
| CMA | cma2           | 10.20.30.202    | up 1336  | up 1333  | up 1277  | up 1631  |
| CMA | cma3           | 10.20.30.203    | up 1338  | up 1334  | up 1279  | up 1632  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3      3 up    0 down                           |
| Tip: Run mdsstat -h for legend                                                 |
+--------------------------------------------------------------------------------+
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# pwd
/home/admin
[Expert@p1ngxr62]# fwm dbexport -v -g -f /home/admin/groups_cma.db
 DBExport> db_exp_main(): Start of execution
Done.
[Expert@p1ngxr62]# fwm dbexport -v  -f /home/admin/users_cma.db
 DBExport> db_exp_main(): Start of execution
Done.
[Expert@p1ngxr62]# ls -l *.db
-rw-rw----    1 root      root              117 Dec 22 07:22 groups_cma.db
-rw-rw----    1 root      root             1449 Dec 22 07:22 users_cma.db
[Expert@p1ngxr62]# file *.db
groups_cma.db: ASCII text
users_cma.db:  ASCII text, with very long lines
[Expert@p1ngxr62]#
```

We need to pass the *users_cma.db* file to the SmartCenter, and via SmartDashboard create the groups contained in the file *groups_cma.db* – Groups <u>must</u> be created before you can import users due the internal references.

```
[Expert@p1ngxr62]# cat groups_cma.db
name;   groups; color;  comments;          is_administrator_group;
ExtVPNUsers;    ;       blue1;  ;          ;
InternalUsers;  ;       dark green;     ;          ;
```
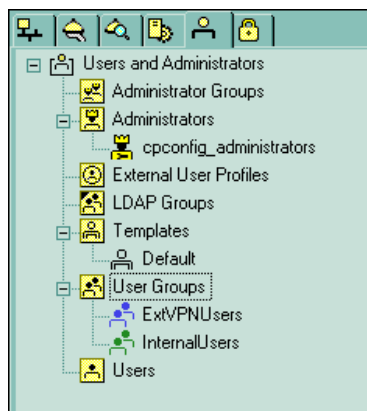

Now let's import the users into the SmartCenter using *fwm dbimport*:

```
[Expert@newngxr62]# pwd
/home/admin
[Expert@newngxr62]# ls -l
total 8
-rw-rw----    1 root     root          117 Dec 29 11:55 groups_cma.db
-rw-rw----    1 root     root         1449 Dec 29 11:55 users_cma.db
[Expert@newngxr62]# file *.db
groups_cma.db: ASCII text
users_cma.db:  ASCII text, with very long lines
[Expert@newngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK

Connected clients
-----------------------------------------------
|Client type|Administrator|Host|Database lock|
-----------------------------------------------
-----------------------------------------------

[Expert@newngxr62]# fwm dbimport -v -f /home/admin/users_cma.db
 Trying to import file /home/admin/users_cma.db. Import_mode is: add
 Connecting to database
 writing the new users to database...
 creating user contractor2...
 creating user user1...
 creating user user2...
 creating user vipuser2...
 4 users were written to database
 Done
[Expert@newngxr62]#
```

- **Resources**

Resources must be manually recreated. So, take a look on the ones from the CMA and recreate them into the SmartCenter. Below an example:
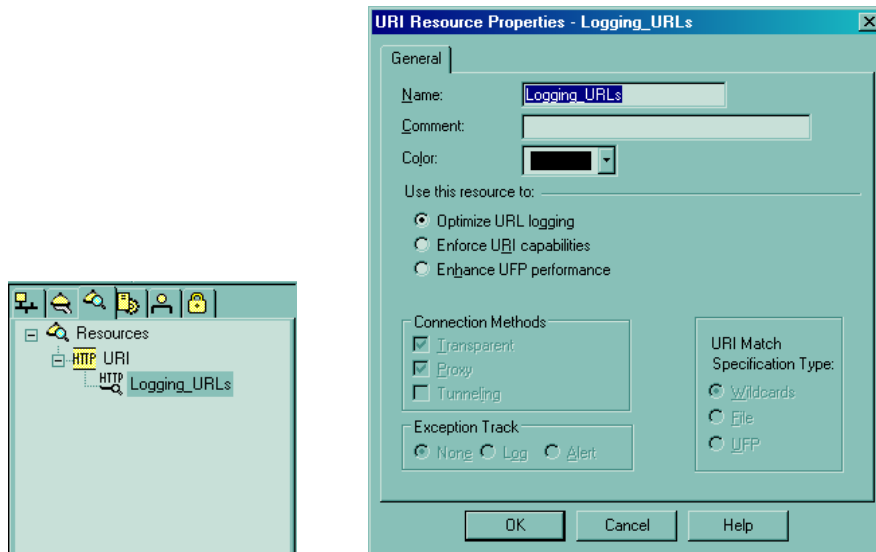
- **VPN Communities**

You need to create the VPN communities that exist on the source CMA, on the target SmartCenter. Even if they are empty and left to the defaults, they need to be created before you attempt to import rules and objects
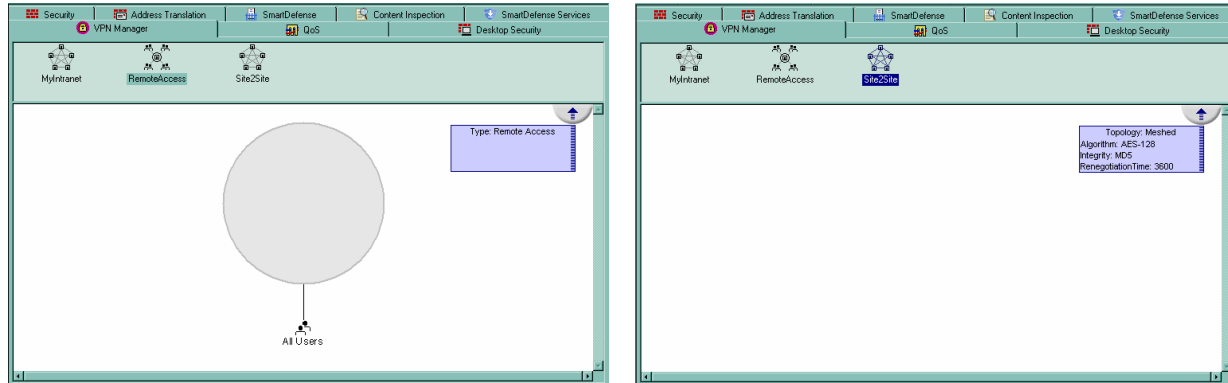
- **Global Objects**

The global objects that are used on the Security Policy currently assigned to the CMA will be moved with the other local objects. As well, the global rulebase assigned to the CMA at the moment you do the export, will pass along with the rules locally defined. You don't need to worry on those by now.

- **Check Point Gateway objects**

If you have more than one Check Point gateway created on the CMA that is referenced by the rulebase, VPNs or objects, you must create them first on your new configuration. This includes any global Check Point object used locally.

For our example, since the firewall will be the same machine as the SmartCenter, we don't need to create any additional objects.

6.3.3 Moving the objects

First let's export the *$FWDIR/conf/objects_5_0.C* file from the source CMA to the machine where Object Filler and Object Dumper are running. Remember to take the usual cautions to make sure the file contains the lastest updates:

```
[Expert@p1ngxr62]# mdsstat
+-------------------------------------------------------------------------------+
|                        Processes status checking                              |
+-----+----------------+-----------------+----------+----------+----------+----------+
| Type| Name           | IP address      | FWM      | FWD      | CPD      | CPCA     |
+-----+----------------+-----------------+----------+----------+----------+----------+
| MDS |       -        | 10.20.30.200    | up 1364  | up 1363  | up 1362  | up 1635  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| CMA | cma1           | 10.20.30.201    | up 1340  | up 1335  | up 1290  | up 1637  |
| CMA | cma2           | 10.20.30.202    | up 1336  | up 1333  | up 1277  | up 1631  |
| CMA | cma3           | 10.20.30.203    | up 1338  | up 1334  | up 1279  | up 1632  |
+-----+----------------+-----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3      3 up   0 down                           |
| Tip: Run mdsstat -h for legend                                                |
+-------------------------------------------------------------------------------+
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK

Connected clients
------------------------------------------------
|Client type|Administrator|Host|Database lock|
------------------------------------------------
------------------------------------------------

[Expert@p1ngxr62]# cd $FWDIR/conf
[Expert@p1ngxr62]# ls -l objects_5_0.C
-rw-rw-r--   1 root     root       768775 Dec 22 08:44 objects_5_0.C
[Expert@p1ngxr62]# ftp 10.20.30.76
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
```

```
Interactive mode off.
ftp> put objects_5_0.C put objects_5_0_cma3.C

local: objects_5_0.C remote: objects_5_0_cma3.C
227 Entering passive mode (10,20,30,76,5,58)
125 Using existing data connection
##############################################################################
##############################################################################
##############################################################################
############################################################
226 Closing data connection; File transfer successful.
800118 bytes sent in 0.323 secs (2.4e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]#
```

Now, let's run Object Dumper over the file to get the list of objects on CSV format

```
D:\Stuff\OFiller\v2.4>odumper -f objects_5_0_cma3.C -o objscma3.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
==============================================================================

==============================================================================
 * Processing objects...
------------------------------------------------------------------------------
.........................................

==============================================================================
Processed 31491 possible objects and found 96 valid ones.
From these, 7 were NATted records. It took 2.0 seconds on quiet mode.
Total successfully processed CP Gateways = 1
Total successfully processed CP Hosts (Secure Servers/SmartCenters) = 1
Total successfully processed Hosts = 20
Total successfully processed Interoperable Devices = 1
Total successfully processed Networks = 12
Total successfully processed Interfaces = 5
Total successfully processed Groups = 1
Total successfully processed Group Elements = 10
Total successfully processed TCP Services = 5
Total successfully processed UDP Services = 5
Total successfully processed URI Resources = 1
==============================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

Good. Now, let's open the list and do two things. First we need to delete the objects we don't want to import into the new SmartCenter. These include Resources, the object that represents the CMA and the object representing the Check Point Gateway. All those were manually addressed and this is the reason.

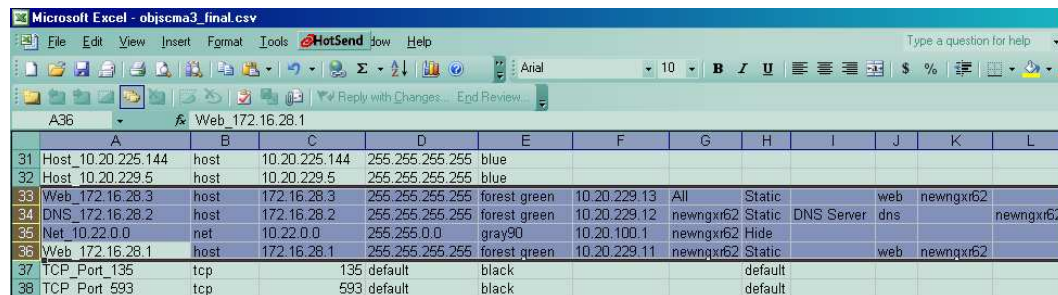On the following screenshots such objects are highlighted

Once the unnecessary objects get deleted, the second thing we need to do is to change any reference to ngxr62 to newngxr62 – this is important since newngrx62 is the name of the new gateway, and if the name still refers to the old one, the references will break with DBEdit. For our example, those references appear as the gateways protecting the DNS and Web Servers, and on some automatic NAT rules.

Search and replace is a good helper for doing the job. Once replaced, the objects should look like this:

Good. Now, let's run Object Filler over this resulting file and get the DBedit commands we need to import the objects into the new SmartCenter

```
D:\Stuff\OFiller\v2.4>ofiller -f objscma3_final.csv -i csv -o objscma3.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
===============================================================================
Processing objects...
..............
===============================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 96 possible objects and/or rules.
Found 46 total valid (or successfully processed) objects/rules.
Found 7 total NATted records.
-------------------------------------------------------------------------------
Total successfully processed Hosts = 20
 - Total successfully processed Web Server Hosts = 2
   WARNING: These objects are only valid on NG+AI R55 or higher
 - Total successfully processed DNS Server Hosts = 1
   WARNING: These objects are only valid on NG+AI R55W or higher
 - Total successfully processed Mail Server Hosts = 1
   WARNING: These objects are only valid on NG+AI R55W or higher
Total successfully processed Interoperable Devices = 1
Total successfully processed Networks = 12
Total successfully processed Groups = 2
Total successfully processed Group Elements = 10
Total successfully processed TCP Service objects = 4
Total successfully processed UDP Service objects = 5
Total successfully processed Interface entities = 2
-------------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
===============================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Let's pass the file to the SmartCenter, check the file is there, no GUI is connected and import the objects.

```
[Expert@newngxr62]# pwd
/home/admin
[Expert@newngxr62]# ls -l objscma3.dbedit
-rw-rw----    1 root     root         18943 Dec 29 14:19 objscma3.dbedit
[Expert@newngxr62]# file objscma3.dbedit
objscma3.dbedit: ASCII text
```

```
[Expert@newngxr62]# cpstat mg

Product Name:   Check Point SmartCenter Server
Major version:  6
Minor version:  0
Build number:   618000021
Is started:     1
Active status: active
Status:         OK


Connected clients
----------------------------------------------
|Client type|Administrator|Host|Database lock|
----------------------------------------------
----------------------------------------------


[Expert@newngxr62]# dbedit -s localhost -u admin -f objscma3.dbedit
Enter Administrator Password:
Host_10.20.229.3 updated successfully.
Host_10.20.229.4 updated successfully.
     .
     .
     .
Net_10.22.0.0 updated successfully.
Web_172.16.28.1 updated successfully.
TCP_Port_135 updated successfully.
     .
     .
     .
UDP_Port_8998 updated successfully.
Internal_Nets updated successfully.
     .
     .
     .
Mail_Services updated successfully.
Mail_Services updated successfully.
[Expert@newngxr62]#
```

At this point you should have the objects created:
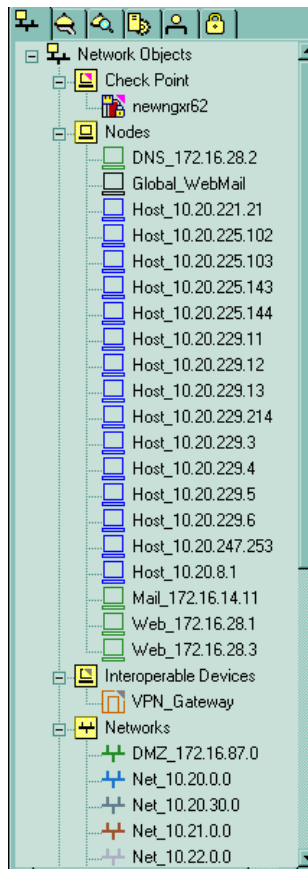
6.3.4 Moving the rules

Let's gather the $FWDIR/conf/rulebases_5_0.fws from the source CMA to the machine where we have Object Filler and Object Dumper

```
[Expert@p1ngxr62]# mdsstat
+--------------------------------------------------------------------------------+
|                          Processes status checking                             |
+-----+---------------+-----------------+----------+----------+----------+----------+
| Type| Name          | IP address      | FWM      | FWD      | CPD      | CPCA     |
+-----+---------------+-----------------+----------+----------+----------+----------+
| MDS |      -        | 10.20.30.200    | up 1364  | up 1363  | up 1362  | up 1635  |
+-----+---------------+-----------------+----------+----------+----------+----------+
| CMA | cma1          | 10.20.30.201    | up 1340  | up 1335  | up 1290  | up 1637  |
| CMA | cma2          | 10.20.30.202    | up 1336  | up 1333  | up 1277  | up 1631  |
| CMA | cma3          | 10.20.30.203    | up 1338  | up 1334  | up 1279  | up 1632  |
+-----+---------------+-----------------+----------+----------+----------+----------+
| Total customer add-ons checked: 3     3 up   0 down                             |
| Tip: Run mdsstat -h for legend                                                  |
+--------------------------------------------------------------------------------+
[Expert@p1ngxr62]# mdsenv cma3
[Expert@p1ngxr62]# cd $FWDIR/conf
[Expert@p1ngxr62]# pwd
/opt/CPmds-R62/customers/cma3/CPsuite-R62/fw1/conf
[Expert@p1ngxr62]# ls -l rulebases_5_0.fws
-rw-rw-r--    1 root     root        42176 Dec 22 08:08 rulebases_5_0.fws
[Expert@p1ngxr62]# ftp 10.20.30.76
```

Page 61

```
Connected to 10.20.30.76 (10.20.30.76).
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.20.30.76:admin): ofiller
331 User name ok, need password
Password: secret
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii
200 Type set to A.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Interactive mode off.
ftp> put rulebases_5_0.fws rulebases_5_0_cma3.fws
local: rulebases_5_0.fws remote: rulebases_5_0_cma3.fws
227 Entering passive mode (10,20,30,76,5,153)
125 Using existing data connection
#########################################
226 Closing data connection; File transfer successful.
44101 bytes sent in 0.0387 secs (1.1e+03 Kbytes/sec)
ftp> bye
221 Service closing control connection
[Expert@p1ngxr62]#
```

Once the file is there, let's extract the CSV format with Object Dumper, so we can work more easily with it.

```
D:\Stuff\OFiller\v2.4>odumper -p rulebases_5_0_cma3.fws -o rules_cma3.csv
Unofficial/Unsupported Object Dumper v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
================================================================================

================================================================================
 * Processing rules...
--------------------------------------------------------------------------------
................

================================================================================
Processed 1925 possible objects and found 18 valid ones.
It took 2.0 seconds on quiet mode.
Total successfully processed Rules = 18
================================================================================
Task done successfully! - Thank you for using Object Dumper v2.4!
```

The result of this operation appears on the next screenshot:

#RULE_TYPE	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL_ON	TIME	COMMENT
rulebase_header	Policy1								
security_rule	Any	Global_WebMail	Any	gsmtp;ghttp	Accept	Account	Any	Any	
section_header	Hide rule								
security_rule	Any	ngxr62	Any	Any	Drop	Alert	ngxr62	Any	Hide Rule
section_header	VPN Rules								
security_rule	Remote_10.200.55.0	Web_172.16.28.3	Site2Site	http	Accept	Account	ngxr62	Any	VPN from the remote site
security_rule	Internal_Nets	Remote_10.200.55.0	Site2Site	sqlnet2;Citrix_metaFrame	Accept	Log	ngxr62	Any	Access to the remote VPN sit
security_rule	ExtVPNUsers@Any	DMZ_172.16.87.0	RemoteAccess	CIFS;ftp;Mail_Services	Accept	Log	ngxr62	Any	VPN users contact services o
section_header	Incoming firewall rules								
disabled_sec_rule	Any	Internal_Nets;DMZ_172.16.87.0	Any	Any	Accept	Log	ngxr62	Any	Having any as source is a bac
security_rule	!Internal_Nets	Web_172.16.28.1	Any	http	Accept	Log	ngxr62	Any	Incoming HTTP requests
security_rule	!Internal_Nets	DNS_172.16.28.2	Any	dns	Accept	Log	ngxr62	Any	Incoming DNS requests
security_rule	!Internal_Nets	Mail_172.16.14.11	Any	smtp	Drop	Log	ngxr62	Any	Incoming Mail Service
section_header	Outgoing firewall rules								
security_rule	InternalUsers@Internal_Nets	!Internal_Nets	Any	http->Logging_URLs	UserAuth	Account	ngxr62	Any	Authentication for outgoing we
security_rule	Internal_Nets	!Internal_Nets	Any	dns;ssh_version_2;https;echo-request	Accept	Log	ngxr62	Any	Access from the Internal Net t
section_header	Clean-up rule								
security_rule	Any	Any	Any	Any	Drop	Log	ngxr62	Any	Clean-up rule
rulebase_header	Standard								
security_rule	Any	Global_WebMail	Any	gsmtp;ghttp	Accept	Account	Any	Any	

For the policies we have to take caution with some items as well:

a) **Change references to the names of old gateways**. On our case, we need to search and replace the old name *ngxr62* with the new name *newngxr62*. This may appear as *source*, *destination* or *installation target* for the rules.

b) **Policy names**. Check specifically for default policy names such as Standard. As a caution change the policy names to something slightly different and you will avoid potential conflicts.

c) **References to global services**. Global services would be dumped as well with regular services when you are passing objects, EXCEPT if the services are default ones. Default Global Services do NOT exist on the SmartCenter, so you will need to either create them manually or reference the names on the policy to the names of the regular default services.

So, let's open the CSV file, search and replace any reference to the elements above mentioned. The following screenshot highlights the changes required/suggested for our example.

#RULE_TYPE	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL_ON	TIME	COMMENT
rulebase_header	Policy1_2								
security_rule	Any	Global_WebMail	Any	smtp;http	Accept	Account	Any	Any	
section_header	Hide rule								
security_rule	Any	newngxrf62	Any	Any	Drop	Alert	newngxrf62	Any	Hide Rule
section_header	VPN Rules								
security_rule	Remote_10.200.55.0	Web_172.16.28.3	Site2Site	http	Accept	Account	newngxrf62	Any	VPN from the remote site
security_rule	Internal_Nets	Remote_10.200.55.0	Site2Site	sqlnet2;Citrix_metaFrame	Accept	Log	newngxrf62	Any	Access to the remote VPN si
security_rule	ExtVPNUsers@Any	DMZ_172.16.87.0	RemoteAccess	CIFS;ftp;Mail_Services	Accept	Log	newngxrf62	Any	VPN users contact services o
section_header	Incoming firewall rules								
disabled_sec_rule	Any	Internal_Nets;DMZ_172.16.87.0	Any	Any	Accept	Log	newngxrf62	Any	Having any as source is a bac
security_rule	!Internal_Nets	Web_172.16.28.1	Any	http	Accept	Log	newngxrf62	Any	Incoming HTTP requests
security_rule	!Internal_Nets	DNS_172.16.28.2	Any	dns	Accept	Log	newngxrf62	Any	Incoming DNS requests
security_rule	!Internal_Nets	Mail_172.16.14.11	Any	smtp	Drop	Log	newngxrf62	Any	Incoming Mail Service
section_header	Outgoing firewall rules								
security_rule	InternalUsers@Internal_Nets	!Internal_Nets	Any	http->Logging_URLs	UserAuth	Account	newngxrf62	Any	Authentication for outgoing we
security_rule	Internal_Nets	!Internal_Nets	Any	dns;ssh_version_2;https;echo-request	Accept	Log	newngxrf62	Any	Access from the Internal Net t
section_header	Clean-up rule								
security_rule	Any	Any	Any	Any	Drop	Log	newngxrf62	Any	Clean-up rule
rulebase_header	Standard_2								
security_rule	Any	Global_WebMail	Any	smtp;http	Accept	Account	Any	Any	

Once the required/suggested changes are complete, we need to use Object Filler to convert from the CSV format to DBedit commands. The syntax is as follows:

```
D:\Stuff\OFiller\v2.4>ofiller -i csv -nopv -p policy -f rules_cma3_final.csv -o
rules_cma3.dbedit
Unofficial/Unsupported Object Filler v2.4  -  Developed by Martin Hoz
(c) 2003-2006 by Check Point Software Technologies, Inc.
==========================================================================
Processing objects...


==========================================================================
Rules processing requested: Processing rules now!!!
..............................................
==========================================================================
It took 3.0 seconds of total processing time on QUIET Mode.
Processed 55 possible objects and/or rules.
Found 13 total valid (or successfully processed) objects/rules.
Rules processing was requested and done for Policy "Standard_2".
--------------------------------------------------------------------------
Total successfully processed Rules = 18
--------------------------------------------------------------------------
Please review that all DBedit output commands were written correctly.
Please remember DBedit commands are imported into SmartCenter directly.
If you wish to review first, the use of CSV mode (-a switch) is suggested.
==========================================================================
Task done successfully! - Thank you for using Object Filler v2.4!
```

Note we are using the *–p policy* and *–nopv* options. Those are important for the correct processing of rules.

Now, pass the output file of this operation to the SmartCenter, and use DBedit to process the commands:

```
[Expert@newngxr62]# pwd
/home/admin
[Expert@newngxr62]# ls -l rules_cma3.dbedit
```

```
-rw-rw----    1 root      root           12655 Dec 29 14:58 rules_cma3.dbedit
[Expert@newngxr62]# file rules_cma3.dbedit
rules_cma3.dbedit: ASCII English text
[Expert@newngxr62]# cpstat mg

Product Name:  Check Point SmartCenter Server
Major version: 6
Minor version: 0
Build number:  618000021
Is started:    1
Active status: active
Status:        OK


Connected clients
-----------------------------------------------
|Client type|Administrator|Host|Database lock|
-----------------------------------------------
-----------------------------------------------


[Expert@newngxr62]# dbedit -s localhost -u admin -f rules_cma3.dbedit
Enter Administrator Password:
Policy1_2 updated successfully.
##Policy1_2 updated successfully.
##Policy1_2 updated successfully.
    .
    .
    .
##Policy1_2 updated successfully.
Standard_2 updated successfully.
##Standard_2 updated successfully.
```
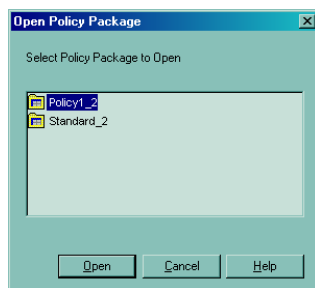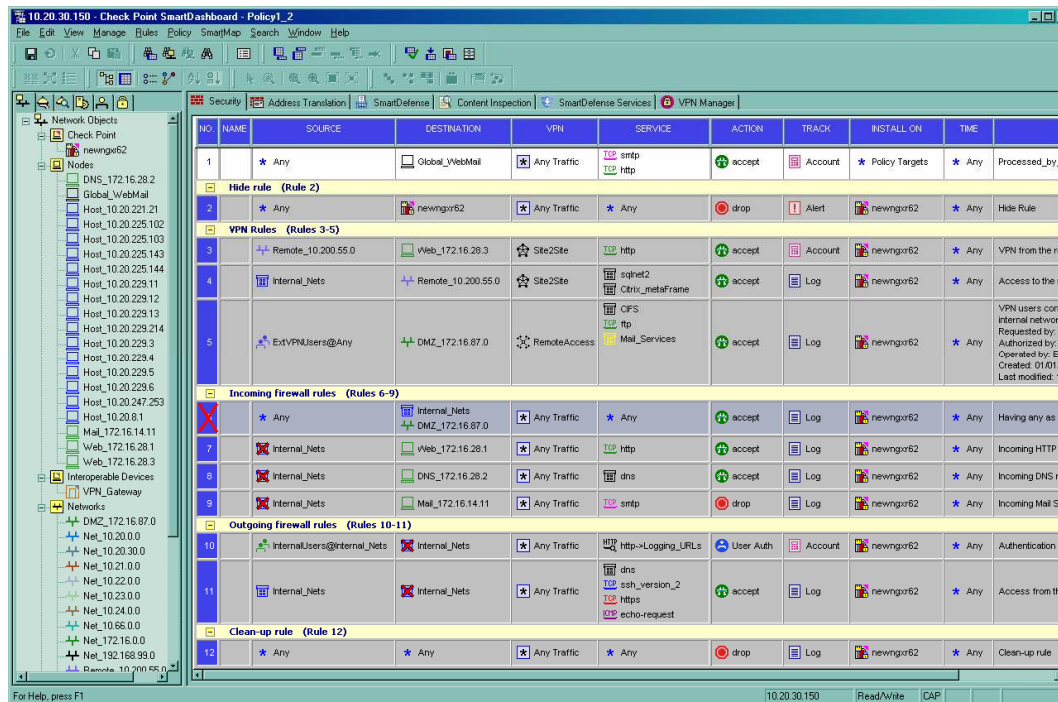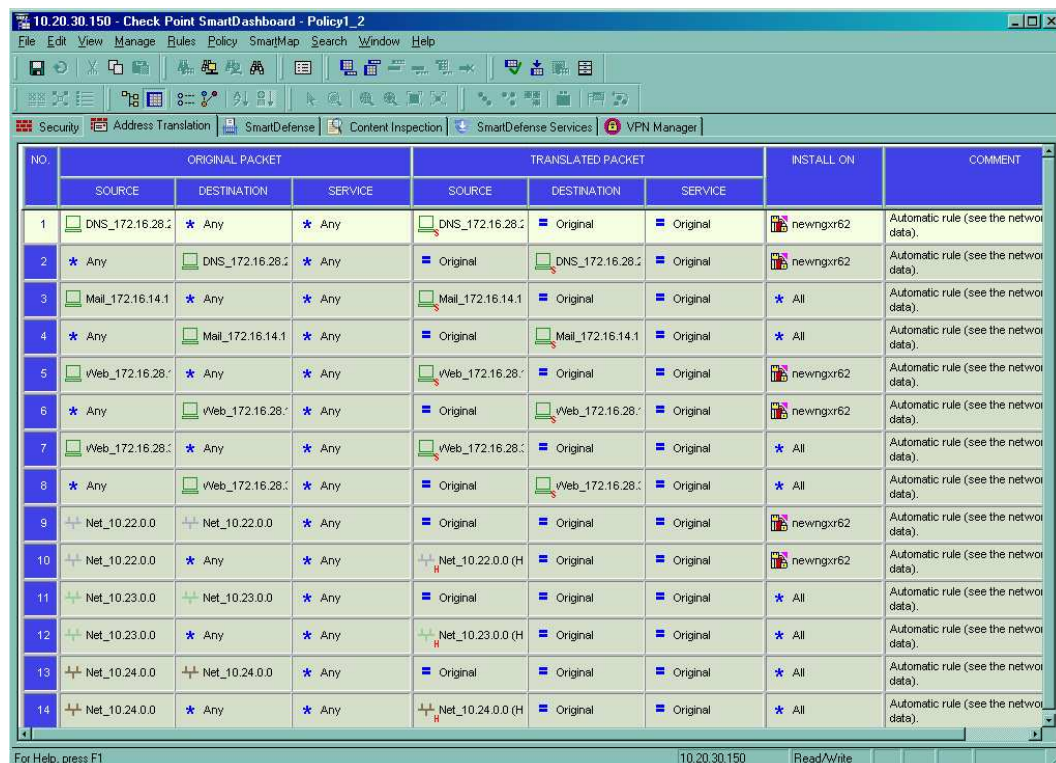
Now, open the *SmartDashboard* on the *SmartCenter*. Go to the *File* menu, use the option *Open*, then choose the Policy you just imported (*Policy1_2*)

Check as well the references on Server objects and Automatic NAT rules. Those should be fine as well.

6.3.5 Completing and verifying the configuration

In short, after passing the objects and the rules (Which is what you can automate with Object Filler and Object Dumper) review that all the manual items you need to pass, passed fine. The following is NOT an exhaustive list, but it marks some of the important items that your list should include:

- Create the administrator accounts to the new SmartCenter, especially if granular access to the configuration is needed (such as having read-only administrators).
- Add the relevant GUI entries to the new SmartCenter, to match what you previously had on the CMA, or to match the new environment.
- Configure properly the VPN communities. Add members to them, change properties as required
- Modify the Global properties accordingly
- Modify the Authentication properties on the Security Rules
- Recreate the Manual NAT rules, Desktop Security rules and/or QoS rules as needed
- Modify the SmartDefense settings as required.
- Finish configuring the gateway properties (such as Log Servers, Concurrent Connections, Products installed on the gateway, etc.)
- Set the proper policy targets to the relevant policy packages
- Install Policy to the relevant gateways.

6.4 Advises on merging configurations from 2 CMAs (or 2 SmartCenters, or 1 SmartCenter + 1 CMA)

As you saw from previous exercises, since you can export the configuration to a text format, this gives great flexibility to the manipulation of objects and policies.

One of the uses that such format may have is when you are trying to merge the configurations from 2 different sources (CMAs or SmartCenters). Below are some general recommendations on how to deal with this situation the best possible way.

6.4.1 Merging objects

a) It is better if you export all the objects from both sources using Object Dumper. Remove any objects you want to exclude on the merge (such as Check Point Objects, or resources) from each individual file
b) Put all the them both in 2 files: one for network objects and the other for services.
c) Once all the objects are in one file (for each class), sort them by IP address/Port. This is better than by name, as it reveals duplicates. Find out if the duplicates have any reason to be there (such as services with different timeouts or Host objects representing different entities on different networks). In case there is no reason for the duplicates to be there, delete them. Make sure you know to document each object you delete. You will need to track these objects down later when dealing with the policies.

d) Make a "*diff*" of this resulting file with the original files. You may use *diff* from GNU (http://www.gnu.org/software/diffutils/) if you are on any UN*X version. You may use CSDiff from Component Software (http://www.componentsoftware.com/Products/CSDiff/download.htm) for Windows. It is free and the output is very good.

e) Once you know what the different objects are, then put them into a separate file and import them using Object Filler and DBedit. Document the list of objects added on this step.

6.4.2 Merging rules

a) Dump the rules from both sources using Object Dumper and put them into a single CSV file.

b) Make sure you NEVER sort the rules. If you sort the rules in any form, you will lose the order of them, and that leads to disaster.

c) Check the list of policy names from both sources. If there are policies that have the same name, change the name for one of them.

d) Review the list of the objects you had to add or delete as part of the process of merging the objects. Look for any references to them in the rules and change them for the new equivalent. The search and replace of the spreadsheet should be of great help here.

e) Delete from the CSV file the Policies (rulebases) that are already present in the target system where you will import the *difference*, in case such policies didn't suffer any modification. If the rules inside any of these policies suffered a change (as a consequence of the objects merger) then rename the policy and leave it in the file

f) Use Object Filler over the resulting CSV File and then DBedit to import the rules that remained on the file.