

SunScreen, Part Two: Policies, Rules, and NAT

Ido Dubrawsky 2003-02-06

The [first article](#) in this series introduced SunScreen 3.2, which is available as part of the Solaris 9 distribution. SunScreen is Sun Microsystems's firewall product and provides a variety of features that allow system and network administrators to secure their networks as well as provide for remote access capabilities. This article will cover the some of the rudimentary facilities in SunScreen such as adding and removing rules, setting up a remote management station, and network address translation.

Policies

SunScreen uses the concept of policies as a way of defining the rules that the SunScreen firewall implements. Policy rules consist of a variety of items, which Sun terms as "Common Objects". Common objects include such items as the following:

- IP Addresses
- SunScreen Screens
- Services
- Certificates
- Time

This is not an exhaustive list by any means. There are many more common objects that can define the rules used to implement SunScreen policies. Common objects provide a significant flexibility, which allows SunScreen policies to be very powerful. Figure 1 shows the example network configuration that will be used to provide some simple examples of how to manage SunScreen firewalls.

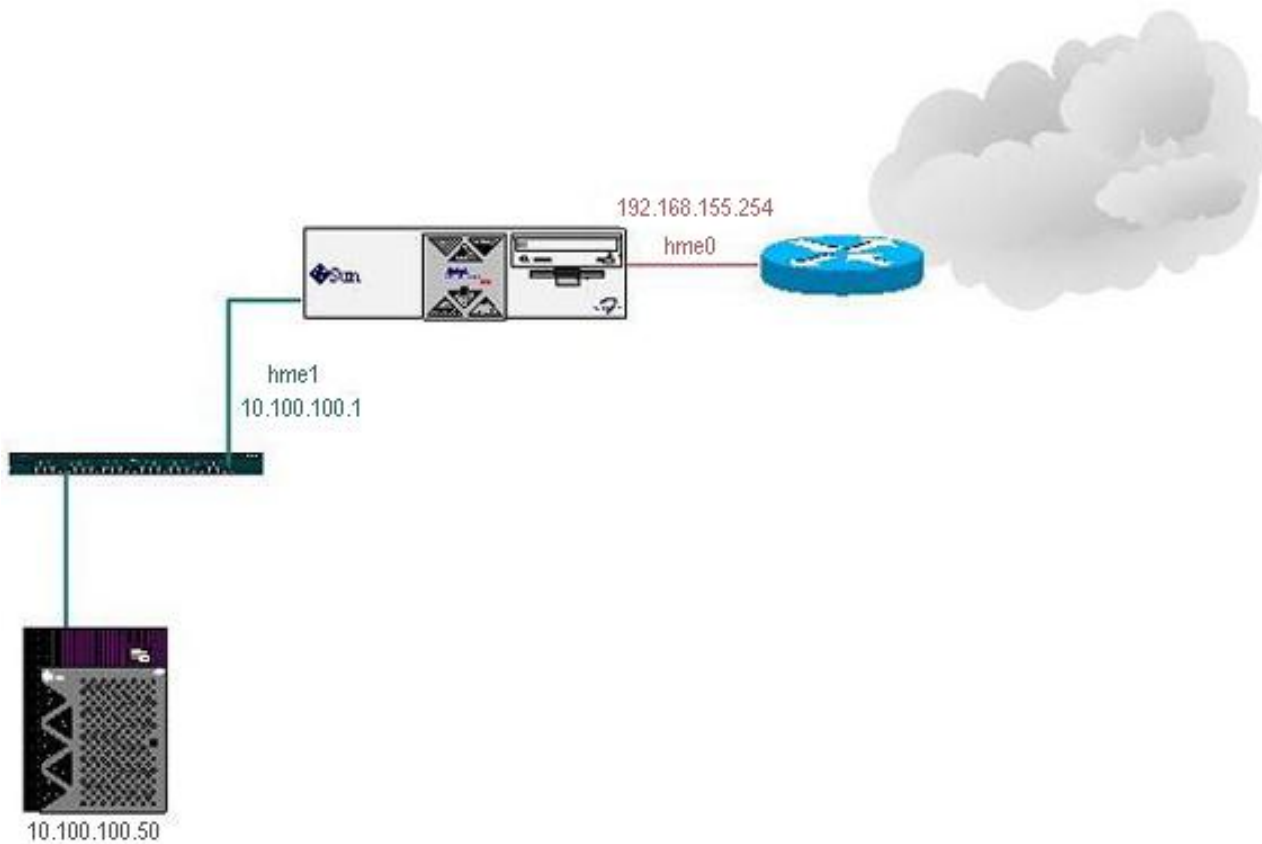


Figure 1: Example SunScreen Network

In this network, the SunScreen host has two 10/100 interfaces with a public interface IP address of 192.168.155.254 and a private interface address of 10.100.100.1. Both interfaces are routing interfaces, as was discussed in the previous article.

Adding Rules to a Policy

This first example involves adding a rule to a policy. When SunScreen is first installed, it has an initial policy that is completely open. The only access that is restricted by default is access to the SunScreen administrative GUI interface, as shown in Figure 2. This can be verified by scanning the SunScreen host with a tool such as [Nmap](#) or [Nessus](#) as shown in Figure 3.

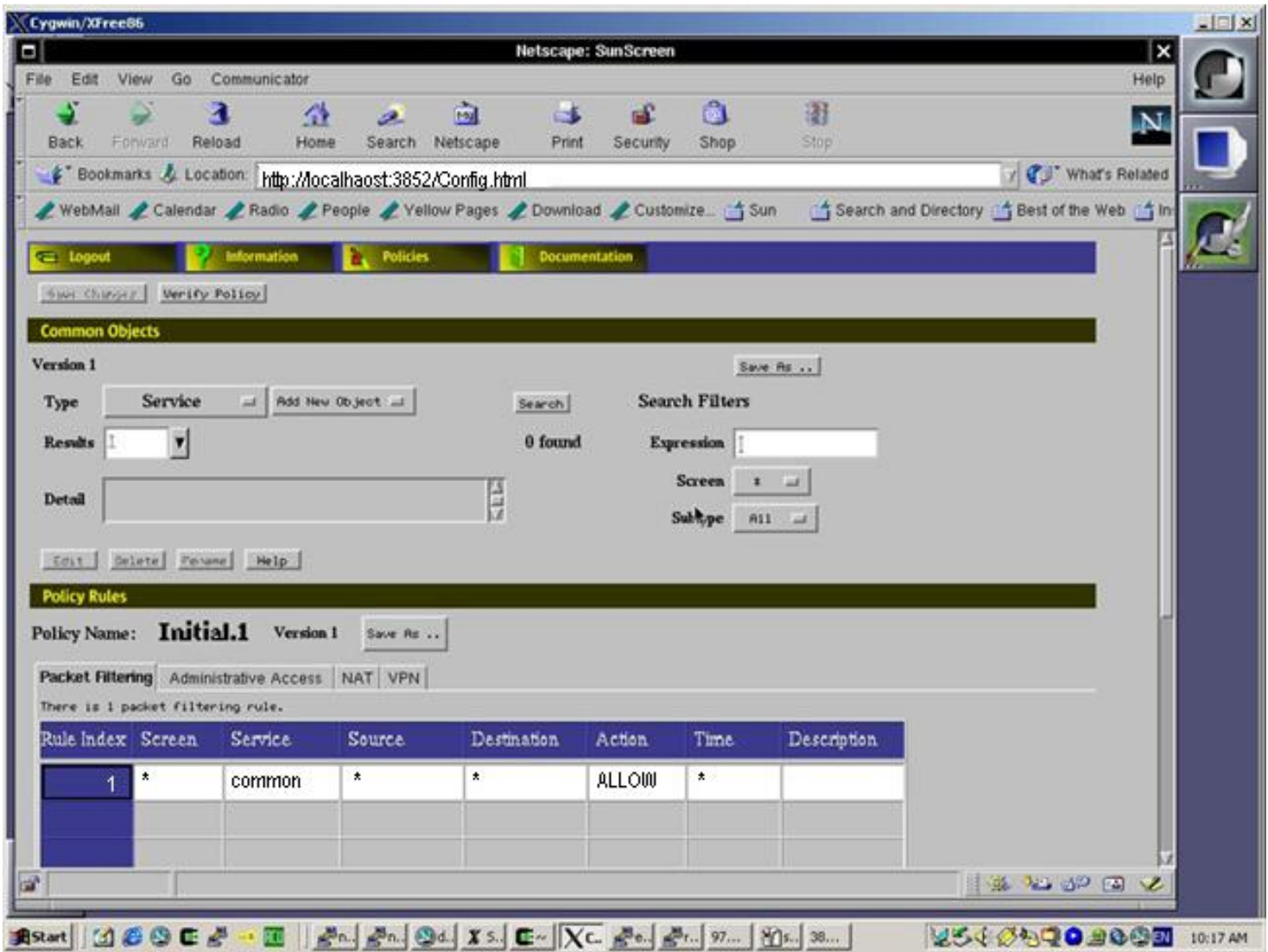
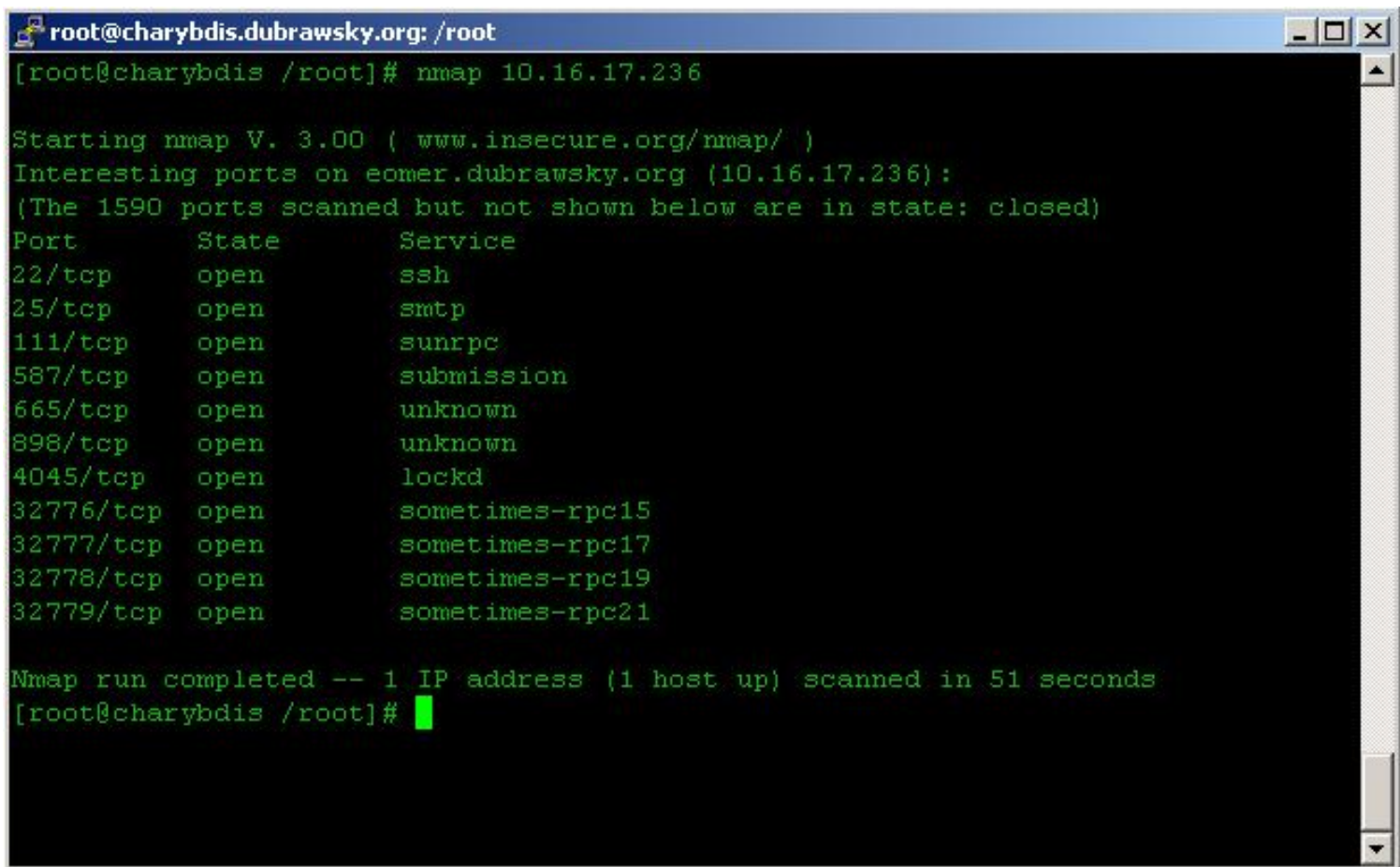


Figure 2: SunScreen Initial Policy Information



```
root@charybdis.dubrawsky.org: /root
[root@charybdis /root]# nmap 10.16.17.236

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on eomer.dubrawsky.org (10.16.17.236):
(The 1590 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open      ssh
25/tcp    open      smtp
111/tcp   open      sunrpc
587/tcp   open      submission
665/tcp   open      unknown
898/tcp   open      unknown
4045/tcp  open      lockd
32776/tcp open      sometimes-rpc15
32777/tcp open      sometimes-rpc17
32778/tcp open      sometimes-rpc19
32779/tcp open      sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 51 seconds
[root@charybdis /root]#
```

Figure 3: Initial Nmap Scan of SunScreen

Adding a rule to a SunScreen policy is fairly simple. In the main SunScreen policy page, highlight the policy to be edited. Be sure not to highlight one of the policy revisions. (These are visible on that page and have a name format such as [policy_name].[rev]. For example, Figure 4 shows that the SunScreen Policy "Initial" has three revisions - Initial.1, Initial.2, and Initial.3). Once the policy is highlighted, select "edit" from the bottom of the window as shown in Figure 4.

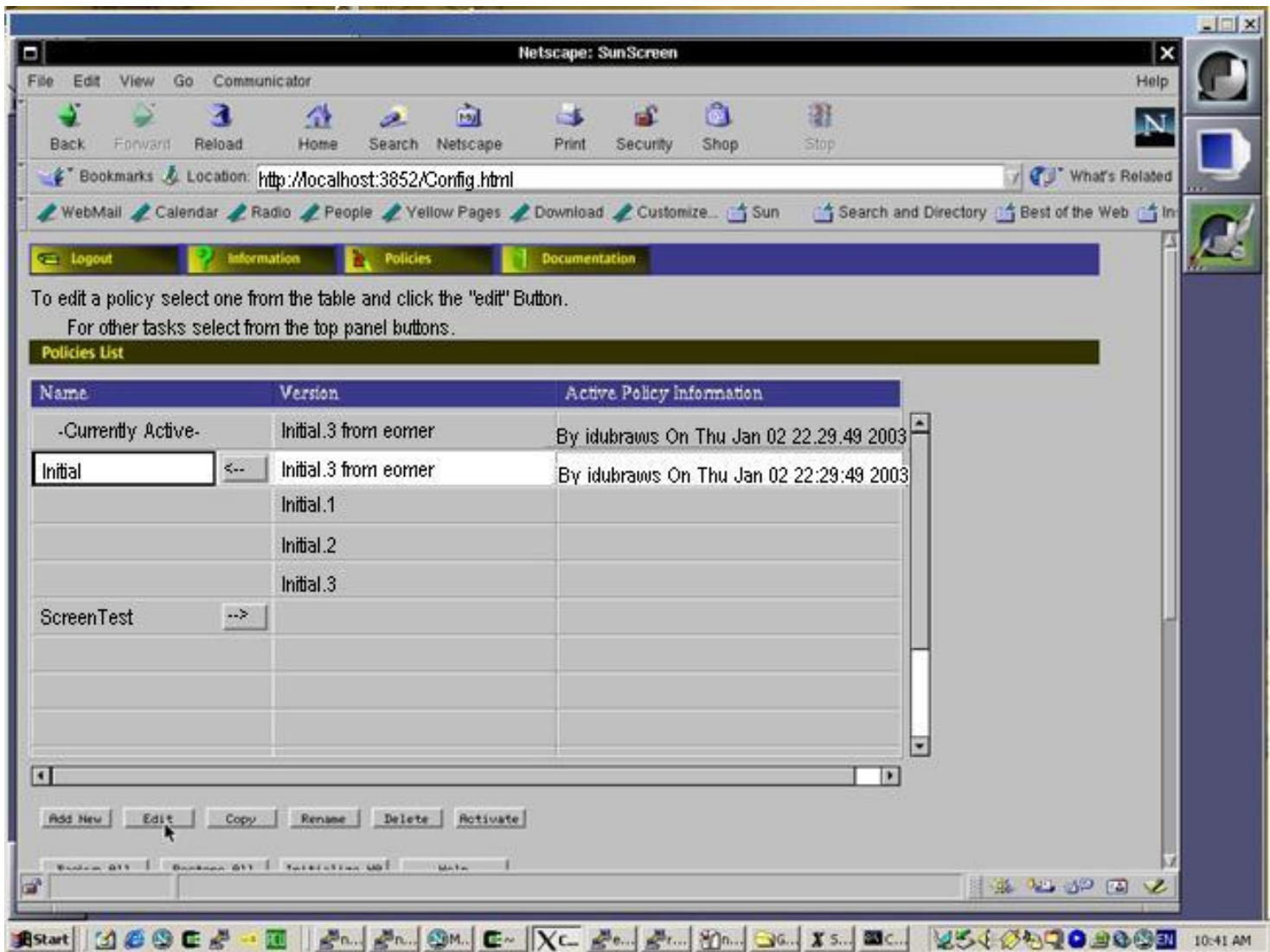


Figure 4: Editing the Initial Policy

To add a rule simply click the button "Add New Rule" at the bottom of the "Policy Rules" section as shown below.

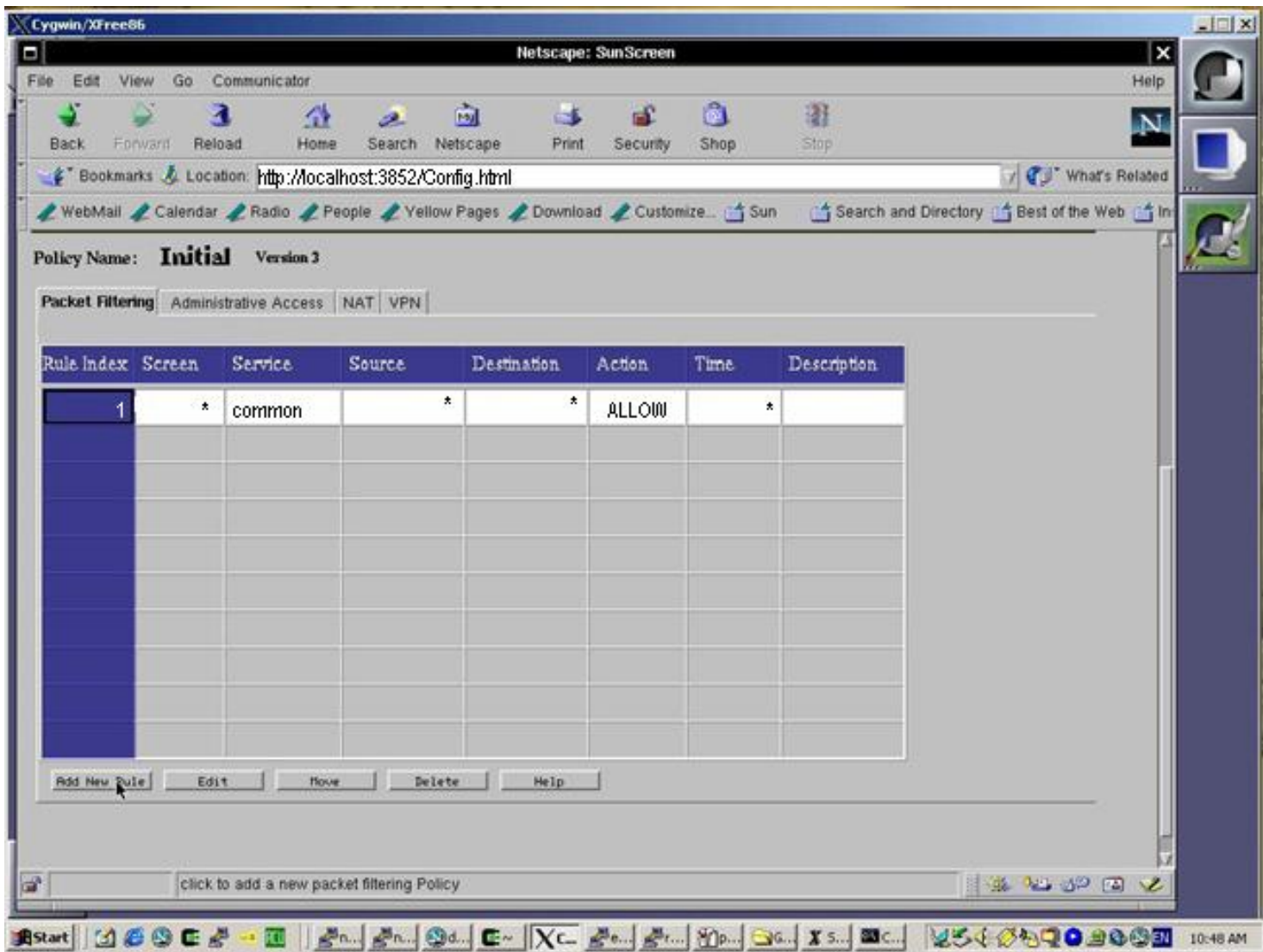


Figure 5: Adding a New Rule to a Policy

This brings up the rule definition dialog box shown in Figure 6a. Filling in the pertinent information in this dialog box will create the rule to be implemented in the SunScreen policy. One of the more important items to define is the action to be taken by the SunScreen firewall when a packet which matches this rule is intercepted. By selecting "DENY" a new dialog box appears which allows the administrator to select a how the SunScreen logs and responds to the offending packet. A log entry can be generated as well as an SNMP trap. It is also possible to define what type of ICMP error message, if any, should be sent to the source address of the packet as shown in Figure 6b.

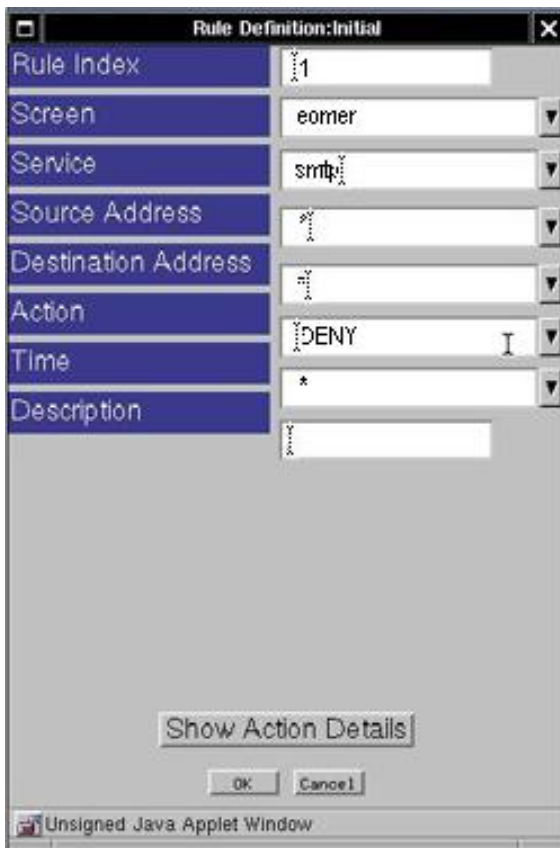


Figure 6a: New Rule Definition - **Figure 6b:** Rule Action Detail

The order of the rules is important because SunScreen works on a "first match" principle for its rules: the first rule to match a packet is the rule applied to that packet. The "Move" button can be used to move a rule from one index in a policy to another.

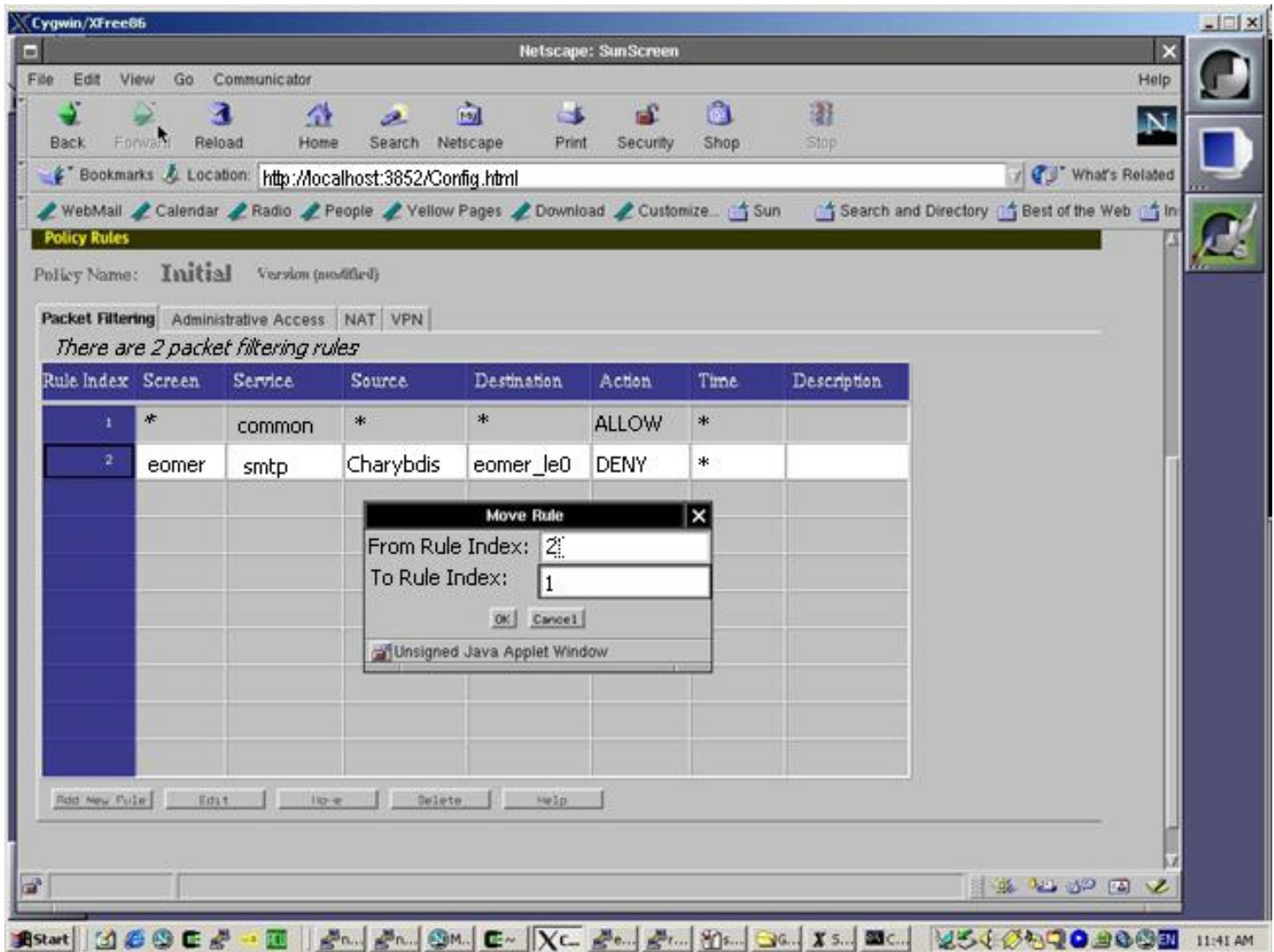


Figure 7: Moving a Rule

Once the new rule has been added to the policy the changes need to be saved and the policy verified. The buttons for these actions are at the top of the Policy Rules page as shown below.

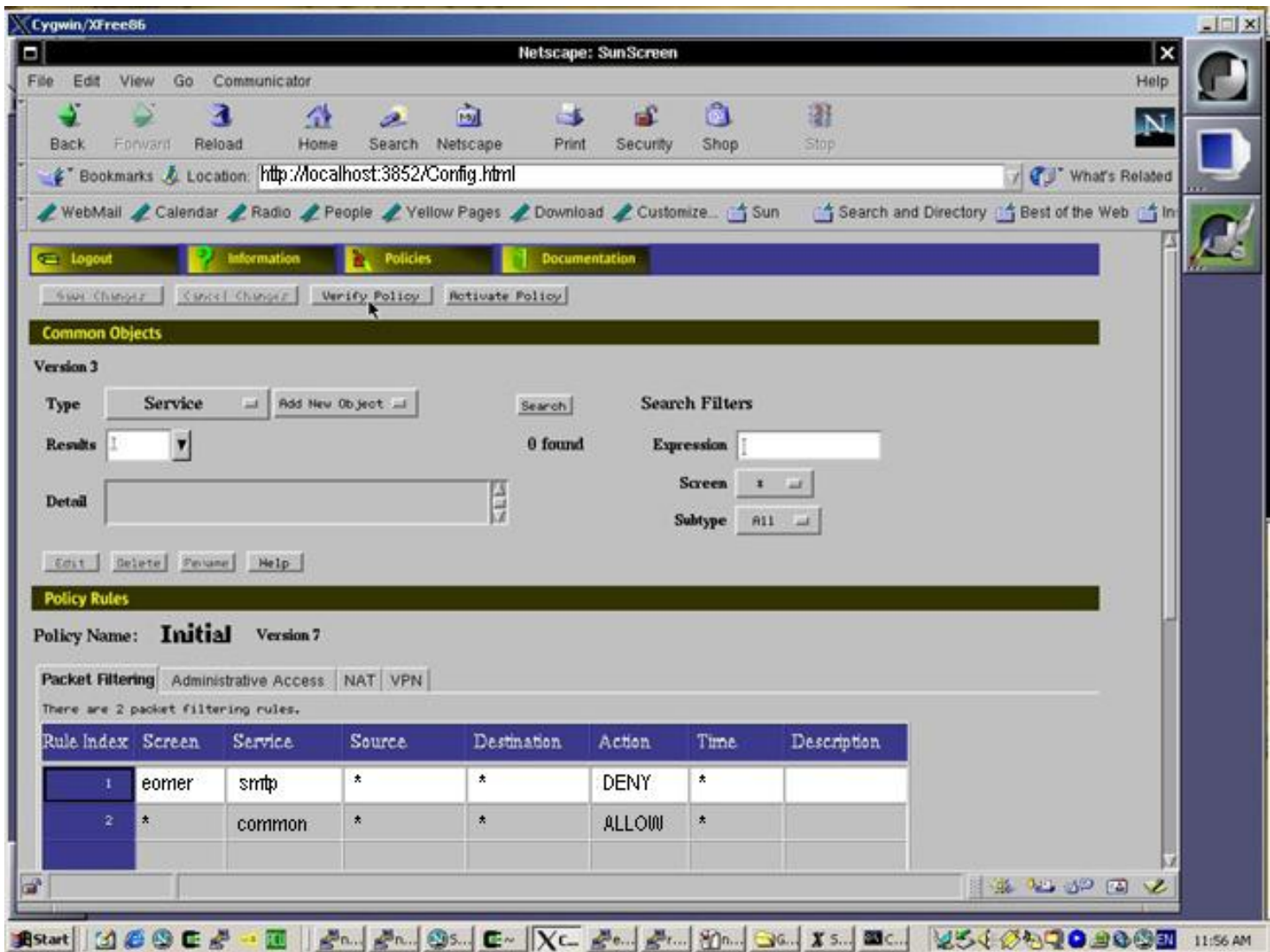
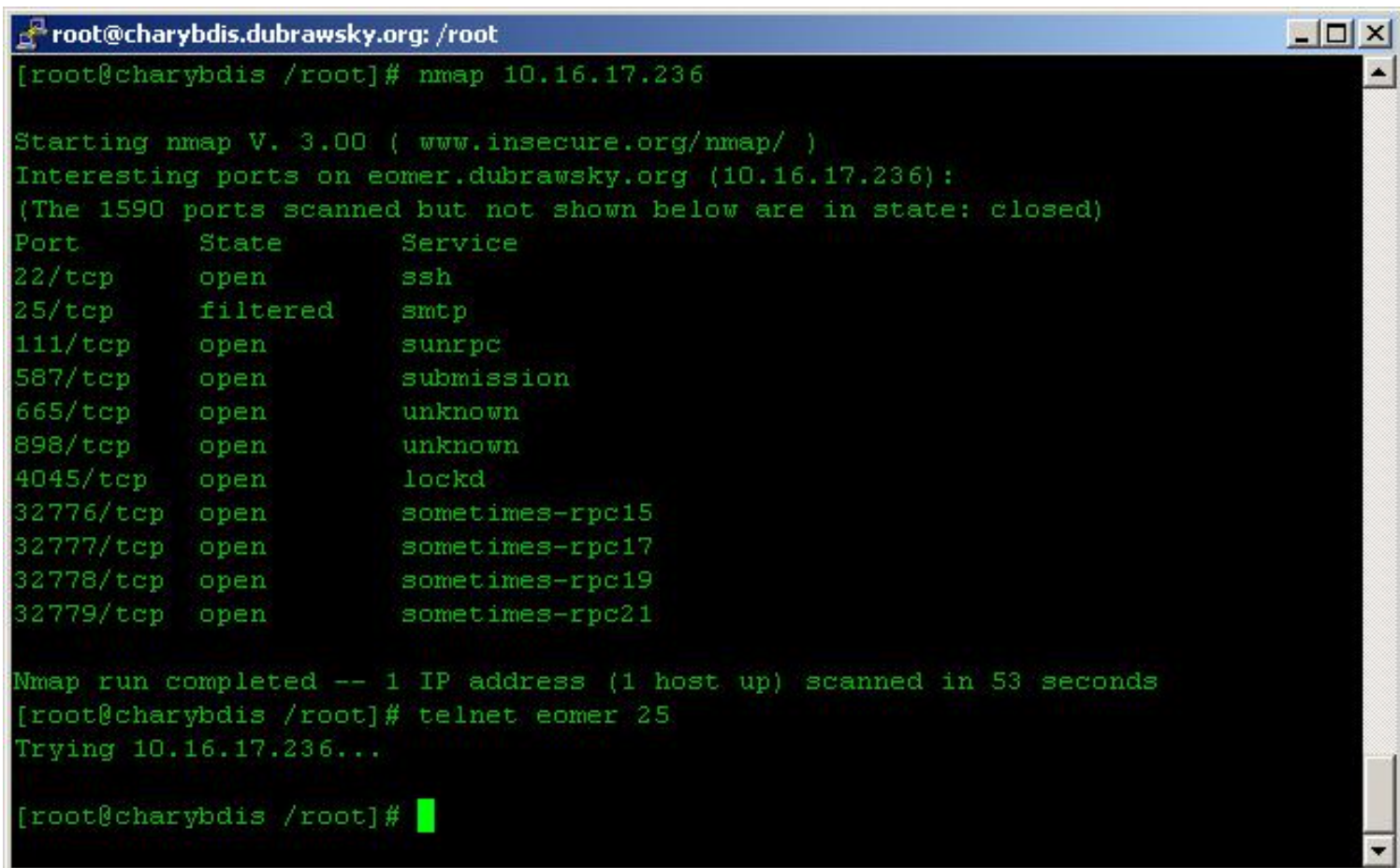


Figure 8: Saving and Verifying Policies

With the new rule verified, the policy needs to be activated. Normally, the act of verifying a policy initiates a dialog box asking if the new policy should be activated. A policy can also be manually activated by selecting the "Activate Policy" button on the page. Once a policy is activated, SunScreen uses the rules in that policy to filter packets. In the case of the example shown above, the SMTP port is now blocked on the SunScreen host as shown in Figure 9 below.



```
root@charybdis.dubrawsky.org: /root
[root@charybdis /root]# nmap 10.16.17.236

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on eomer.dubrawsky.org (10.16.17.236):
(The 1590 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
25/tcp    filtered   smtp
111/tcp   open       sunrpc
587/tcp   open       submission
665/tcp   open       unknown
898/tcp   open       unknown
4045/tcp  open       lockd
32776/tcp open       sometimes-rpc15
32777/tcp open       sometimes-rpc17
32778/tcp open       sometimes-rpc19
32779/tcp open       sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 53 seconds
[root@charybdis /root]# telnet eomer 25
Trying 10.16.17.236...

[root@charybdis /root]# █
```

Figure 9: Blocking the SMTP Port

Deleting a Rule

Deleting a SunScreen policy rule is much less complicated than adding one. To delete a rule in a policy involves simply selecting the rule to be deleted from the rules in the policy list, saving the changes, verifying the policy and activating it. To delete the SMTP filter rule added above to the initial policy in SunScreen, simply highlight the rule in the policy list and select the delete button at the bottom. Answer "yes" to the dialog box that pops up after selecting the delete button and the rule is deleted.

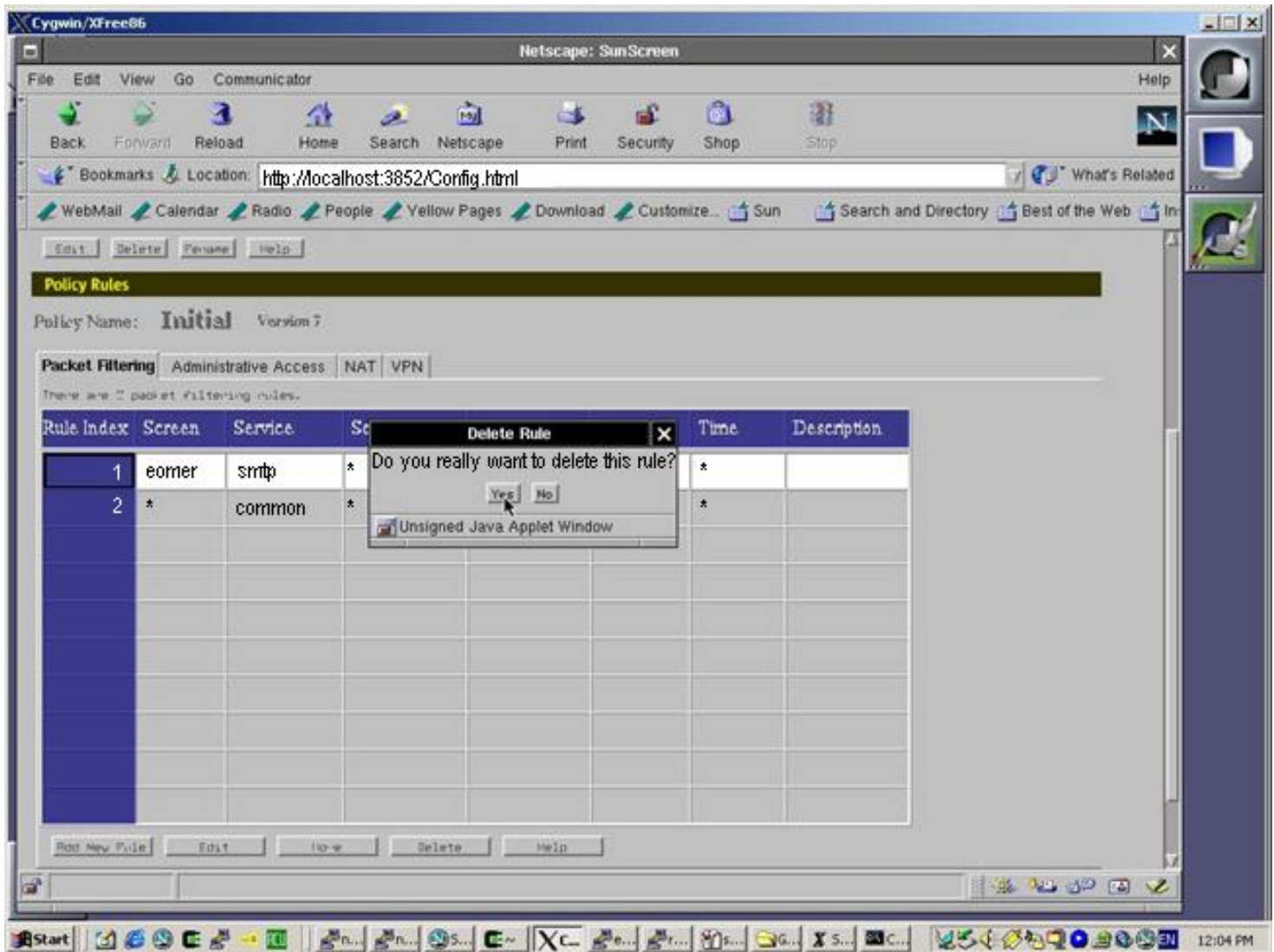
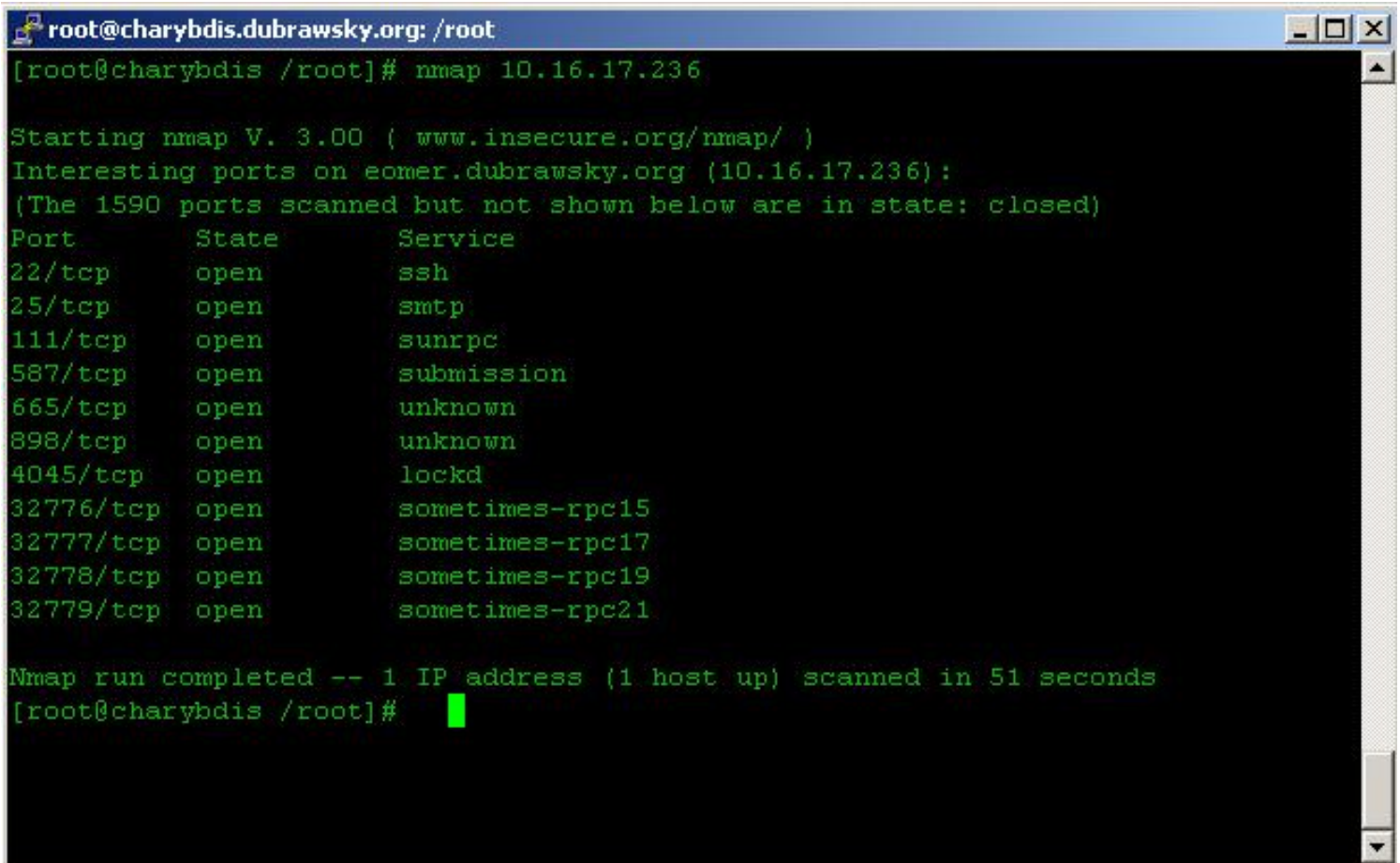


Figure 10: Deleting a Rule

Once the rule has been deleted and the new policy verified and activated the port is once again open for traffic as shown below.

A terminal window titled 'root@charybdis.dubrawsky.org: /root' showing the output of an nmap scan. The scan was performed on 10.16.17.236. The output lists several open ports and their corresponding services. The terminal text is as follows:

```
root@charybdis.dubrawsky.org: /root
[root@charybdis /root]# nmap 10.16.17.236

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on eomer.dubrawsky.org (10.16.17.236):
(The 1590 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
25/tcp    open       smtp
111/tcp   open       sunrpc
587/tcp   open       submission
665/tcp   open       unknown
898/tcp   open       unknown
4045/tcp  open       lockd
32776/tcp open       sometimes-rpc15
32777/tcp open       sometimes-rpc17
32778/tcp open       sometimes-rpc19
32779/tcp open       sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 51 seconds
[root@charybdis /root]#
```

Figure 11: Unblocking the SMTP Port

Creating a Static Network Address Translation (NAT) Mapping

NAT capabilities on the SunScreen firewall allow the firewall to map external, publicly routable addresses for systems or networks behind the firewall that may either have private [RFC 1918](#) addresses or other address ranges. SunScreen supports both static and dynamic NAT mappings. To NAT a host behind the firewall, simply select the "NAT" tab in the "Policy Rules" page of the administrative GUI and add a new NAT rule.

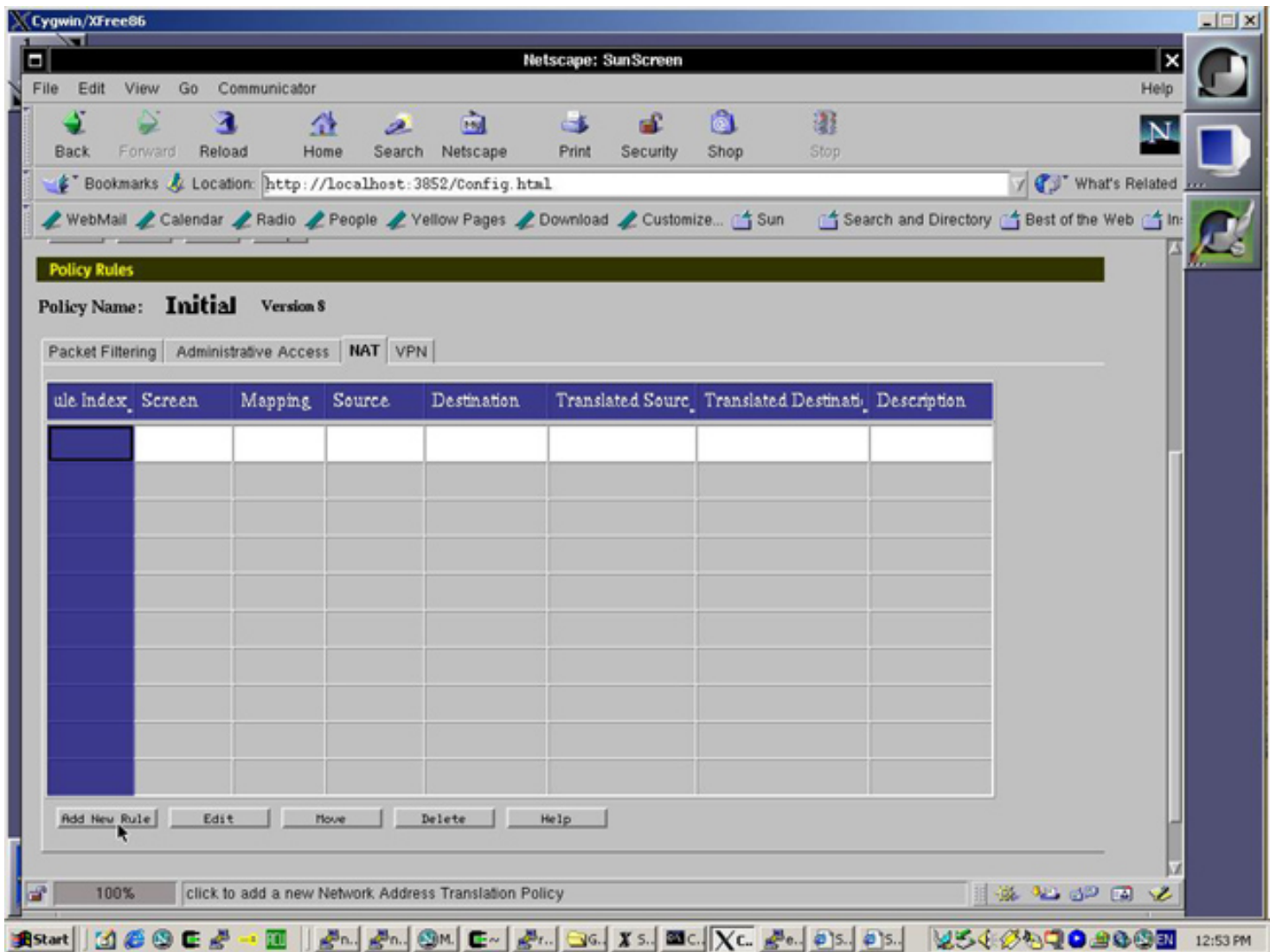


Figure 12: Adding a NAT rule

Selecting "Add New Rule" will bring up a NAT definition dialog box. This dialog box is where all relevant information in the NAT mapping is entered. The Screen name is selected as well as the type of mapping (static or dynamic). The source field contains the host IP address or the network range and the destination field contains the destination address. The translated source and destination are where the values for the NAT addresses are entered. Finally, the description field allows administrator to put in a descriptive text message as a reminder of the purpose of this rule.



Figure 13: Static NAT Mapping

Remote Administration

One of the nicest features of SunScreen is the capability of setting up a remote administration station to provide a central location to administer deployed SunScreen systems. This example assumes that IKE will be used to provide a session key for use in encrypting the communications between the SunScreen system and the remote administration system.

Certificates must be generated in order to use IKE between the administration station and the SunScreen firewall. These certificates can be truly valid (that is, signed by a certificate authority) or self-signed. This example assumes that they are self-signed. To generate a self-signed IKE certificate on a Solaris 9 host running as a remote administration station:

```
[root@eowyn /]
# ikecert certlocal -ks -m 512 -t rsa-md5 -D "C=US, O=DUBRAWSKY_ORG, OU=IT, CN=idubraws"

[root@eowyn /]
# ikecert certdb -e "C=US, O=DUBRAWSKY_ORG, OU=IT, CN=idubraws" > /tmp/eowyn_ike_cert.txt
```

Similarly, the SunScreen IKE certificate needs to be created and copied over to the remote administration station. Once the administration station's certificate has been transferred to the SunScreen firewall (and the SunScreen firewall IKE certificate has been transferred to the administration station) it must be imported into the SunScreen database. Importing a certificate can also be done through the command line interface for

SunScreen using ssadm:

```
[root@eomer /]
# ssadm certdb -I -a < /tmp/eowyn_ike_cert.txt
```

With the certificates now imported into the SunScreen databases, the common objects for the certificates need to be created. An object must be created both for the administration station's IKE certificate as well as the SunScreen IKE certificate.

```
[root@eomer /]
# ssadm edit Initial
edit> add certificate eowyn_ike_cert SINGLE IKE "C=US, O=DUBRAWASKY_ORG, OU=IT, CN=eowyn"
edit> add certificate eomer_ike_cert SINGLE IKE "C=US, O=DUBRAWASKY_ORG, OU=IT, CN=eomer"
edit> add member certificate "IKE manually verified certificates" "eowyn_ike_cert"
```

Once the administration station's IKE certificate has been added to the SunScreen database, the administration station's IP address should be added as an "address" common object and the station itself should be added as a "screen" common object.

With that information added to the SunScreen database, the next step is to create an administrative access rule in the policy to allow for the administration station to communicate with the SunScreen firewall. Selecting the "Administrative Access" tab in the Policies page and clicking on the "Add New Rule" button opens the "Remote Access Rules" dialog box shown below:

Remote Access Rules

Rule Index: 1

Description: Admin access from eowyn

Screen: *

Address Object: eowyn_le0

User: admin

Access Level: ALL

Encryption: IPSEC IKE

Algorithms | Options

ESP [EDIT]

BLOWFISH MD5

AH [EDIT]

NONE

IKE

Encryption Algorithm: BLOWFISH

Hash Algorithm: MD5

Oakley Group: 1

Authentication Method: RSA-SIGNATURES

Preshared Key: []

Source Certificate: eowyn_ike

Figure 14: Remote Access Configuration

Once the remote access rules have been configured, the policy should be saved, verified, and activated. The SunScreen firewall can now be administered by a remote system. The configuration on the remote administration station depends on whether it is a Solaris 8 or Solaris 9 host.

Solaris 8 Remote Administration Station

On a Solaris 8 host acting as the remote administration station, the procedure for configuring it to communicate with the SunScreen firewall is very similar to the procedure on the firewall itself:

```
[root@elrond /]
# ssadm certdb -I -a < /tmp/eomer_ike_cert.txt

[root@elrond /]
# ssadm edit Initial
edit> add certificate elrond_ike_cert SINGLE IKE "C=US, O=DUBRAWSKY_ORG, OU=IT, CN=elrond"
edit> add certificate eomer_ike_cert SINGLE IKE "C=US, O=DUBRAWSKY_ORG, OU=IT, CN=eomer"
edit>add member certificate "IKE manually verified certificates" "eomer_ike_cert"
```

Once the certificates have been added to the SunScreen database on the remote administration host, the GUI can be used to add a filter rule to allow communication between the SunScreen firewall and remote administration station.

Solaris 9 Remote Administration Station

Solaris 9 natively supports IKE, which makes importing the IKE certificate of the SunScreen firewall much easier:

```
[root@eowyn /]
# ikecert certdb -a < /tmp/eomer_ike_cert.txt
```

The next step is to edit the ipsecinit.conf file in /etc/inet to allow communication between the SunScreen firewall and the administration station:

```
[root@eowyn inet]
# cat ipsecinit.conf
{sport 500} bypass {dir out}
{dport 500} bypass {dir in}
{saddr 10.16.17.237 daddr 10.16.17.236} apply {encr_algs 3des encr_auth_algs md5 sa shared}
{saddr 10.16.17.236 daddr 10.16.17.237} permit {encr_algs 3des encr_auth_algs md5 sa shared}

[root@eowyn inet]
#
```

Once that is complete, the /etc/inet/ike/config should be edited to mark the SunScreen certificate as trusted as well as to define various encryption parameters:

```
[root@eowyn ike]
# cat config
#
#ident "@(#)config.sample      1.2      01/12/06 SMI"
#
# Copyright (c) 2001 by Sun Microsystems, Inc.
# All rights reserved.

##
## This file should be copied into /etc/inet/ike/config to enable the
## launch of the IKE daemon, in.iked(1m), at boot time.  You can also
## launch the IKE daemon after creating this file without rebooting by
## invoking /usr/lib/inet/in.iked with a root shell.
##

# Consult the ike.config(4) man page for further details.  Here is a small
# example from the man page.

### BEGINNING OF FILE

### First some global parameters...

## Phase 1 transform defaults
p1_lifetime_secs 14400
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2

# Remote SunScreen Administration using IKE manually verified self-signed certificates
cert_trust "SUBJECT=CN=DNofScreensCert-rsa-sha1-4096, O=Sun, C=US"
# Outgoing IKE rule for remote admin
{label "ike_outbound"
local_id_type DN
local_id "SUBJECT=CN=RemoteAdminCert-blowfish-md5-1024, C=US, O=DUBRAWSKY_ORG, OU=IT, CN=eowyn"
remote_id "SUBJECT=CN=ScreenCert-blowfish-md5-1024, C=US, O=DUBRAWSKY_ORG, OU=IT, CN=eomer"
local_addr 10.16.17.237
remote_addr 10.16.17.236
p1_xform {auth_method rsa_sig oakley_group 1 auth_alg md5 encr_alg blowfish }
}
```

```
[root@eowyn ike]
```

```
#
```

Once the config file has been updated to allow for communication with the remote SunScreen host the IKE daemon, `in.iked`, needs to be restarted and the IPsec configuration reloaded:

```
[root@eowyn ike]
```

```
# ps -ef | grep in.iked
```

```
root    292      1  0   Jan 29  ?           0:00 /usr/lib/inet/in.iked
root    4082    3979  0 15:52:49 pts/1    0:00 grep in.iked
```

```
[root@eowyn ike]
```

```
# kill -SIGTERM 292
```

```
[root@eowyn ike]
```

```
# ipsecconf -f
```

```
[root@eowyn ike]
```

```
# ipseckey flush
```

```
[root@eowyn ike]
```

```
# ipsecconf -a /etc/inet/ipsecinit.conf
```

```
[root@eowyn ike]
```

```
# /usr/lib/inet/in.iked -f ./config
```

With the configuration complete, the SunScreen firewall can now be managed remotely through the Web GUI.

Conclusion

SunScreen is a very powerful firewall software package with many features. This series has only described a small fraction of the capabilities that SunScreen features. Its availability with the Solaris 9 CDs appears to indicate Sun's commitment to expanding the roles that Solaris is capable of performing and to making Solaris a serious competitor of other firewall systems such as CheckPoint FW-1, iptables, and ipfilter.

Relevant Links

[SunScreen, Part One: An Overview of the Sun Microsystem Firewall](#)

Ido Dubrawsky

[Privacy Statement](#)

Copyright 2006, SecurityFocus