

SecurityFocus SUN: Re: ipf, SunScreen or ?

## Re: ipf, SunScreen or ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2003-10/0038.html>

---

**From:** Eric Forgette ([4jet\\_at\\_overnite.com](mailto:4jet_at_overnite.com))

**Date:** 10/22/03

Date: Wed, 22 Oct 2003 12:55:18 -0400

To: [focus-sun@securityfocus.com](mailto:focus-sun@securityfocus.com)

> *I would really like to get a software firewall running on some of my  
> sun boxes*

I like SunScreen. Its free with Solaris 8 and 9, its a binary install,  
and I think patches are on SunSolve.

I was in the process of creating a 'HOW TO' for SunScreen on Solaris 9.

Similar steps can be taken for SunScreen-lite on Solaris 8. So I've  
done a quick brain dump below...

>> *I started reading the documentation on SunScreen from sun docs and  
>> wasn't horribly excited about it – I most definitely wouldn't run  
>> apache just to get a GUI.*

You don't need it. In my recipe below I turn it off!

> *Did you see the Sun BluePrint article describing how host-based  
> firewalls could be configured using SunScreen?*

This is a very good article, but they install everything but the  
kitchen sink!

What I was looking for was a locally, command line administered, host  
based firewall.

Here is what I've boiled it down to (still working on it though)...

Quick and dirty:

```
pkgadd -d . SUNWeuluf SUNWeulux SUNWeu8os SUNWeu8ox SUNWsfwau SUNWsfwr  
SUNWsfwu SUNWsfwf SUNWsfwm
```

Take note of /etc/sunscreen/AdminSetup.readme

In many cases I also run  
/usr/lib/sunscreen/lib/harden\_os

Re: ipf, SunScreen or ?

## SecurityFocus SUN: Re: ipf, Sunscreen or ?

From the console run:  
sudo ssadm configure

I don't remember the exact questions, but choose routing not stealth and local not remote. I seem to remember answering '1' to most questions. ;-)

edit /usr/lib/sunscreen/lib/ss\_boot  
and comment out the following lines:

```
$LIB_DIR/ssadmserver start >/dev/console 2>&1  
$LIB_DIR/run_httpd start
```

You should be up and running after a reboot.

The default policy is called Initial. I usually create a new one under a different name (see man ssadm).

To create your rules in this policy run:  
sudo ssadm edit Initial

some edit commands are:

delete rule <rule number>

add rule ...  
add address ...

list services  
list rules  
list addresses

So, here is a quick set of rules (localhost = all of my hosts's interfaces (not 127.0.0.1):  
add SERVICE ssh SINGLE FORWARD "tcp" PORT 22  
add rule "\*" "localhost" "\*" ALLOW COMMENT "allow everything from this host"  
add rule "www" "\*" "localhost" ALLOW COMMENT "http access"  
add rule "ssl" "\*" "localhost" ALLOW COMMENT "https access"  
add rule "ping" "\*" "localhost" ALLOW  
add rule "netbios" "\*" "\*" DENY COMMENT "silently drop netbios broadcasts"  
add rule "\*" "\*" "localhost" DENY LOG DETAIL COMMENT "drop and log everything else"

Then save it and exit:

```
save  
verify  
quit
```

Re: ipf, Sunscreen or ?

## SecurityFocus SUN: Re: ipf, Sunscreen or ?

Then make it active:  
ssadm activate Initial

I use this in an alias to dump out the 'denys' from the log  
ssadm log get | ssadm logdump -i - logwhy 256

I also add a cron job to rotate the logs out every day  
0 0 \* \* \* ssadm log get\_and\_clear > /var/tmp/sunscreen.bin.'date  
“+%Y%m%d”

and of course a quick find to remove the files after they've been  
around awhile...

/etc/sunscreen/.active can be moved or deleted to disable the firewall.  
SunScreen doesn't like nodename changes very much. I tend to rerun  
'sudo ssadm configure' and add my rules back to a fresh policy.

I've been using this type of setup for awhile. I actually lock down  
the source address in my rules by creating address groups (again see  
man ssadm). I also use this to lock folks onto a server (contractors,  
etc) obviously with a different rule set...

No gui, no apache, just good old cli. I don't have a lot of  
performance impact data yet, but nobody's complaining yet... =)

-Eric

-----  
Eric P. Forgette  
Unix Systems Administrator  
<http://homepage.mac.com/e4jet/sysadm/>