Securing Your Network with pfSense

ILTA-U

Dale Qualls

Pattishall, McAuliffe, Newbury, Hilliard & Geraldson LLP

dqualls@pattishall.com

PATTISHALL
McAULIFFE
DEFENDING YOUR BRAND

Housekeeping

- Please turn off cell phones or put them on silent
- We're recording this session to share with those that were unable to attend… If you have a question please wait for the microphone to make it to you.
- Please fill out the survey after the session

Housekeeping

- 2 Hyper-V virtual machines
  - To release the mouse the right ALT, CTRL and Left Arrow simultaneously
- Helpers are here for you

What is pfSense

- Firewall
- Router
- Load balancer (bi-directional)
- VPN solution
- Internet filter
- Usage monitor
- Provides a Captive portal capabilities

- Based on FreeBSD PF (Packet Filter) project, ported from OpenBSD to FreeBSD in 2004
- Forked from the m0n0wall project in 2004 by Chris Buechler and Scott Ullrich
- Focus is not running on embedded systems but an embedded offering is available.

Beastie the Daemon

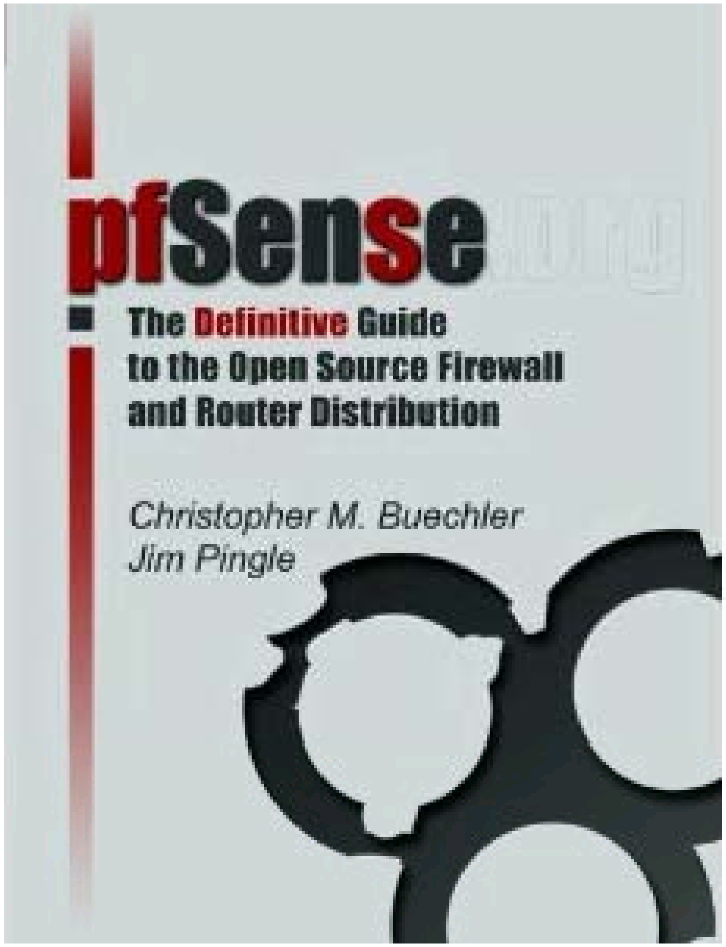
iX
MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK

Microsoft
Windows

What’s in a name?

- pfSense
  - pf (from the original project name)
  - Sense, as in making sense of pf
- Domain name availability, or lack thereof, helped dictate the name.
  - was though by some to stand for “Plain F...... Sense”.

$35 at Amazon
I will be giving one away today!


pfSense

The Definitive Guide to the Open Source Firewall and Router Distribution

Christopher M. Buechler
Jim Pingle

FreeBSD is used as a platform for devices and products from many of the world's largest IT companies, including:

JUNIPER
NETWORKS

FreeBSD runs some of the busiest sites on the Internet!

YAHOO!®

APACHE

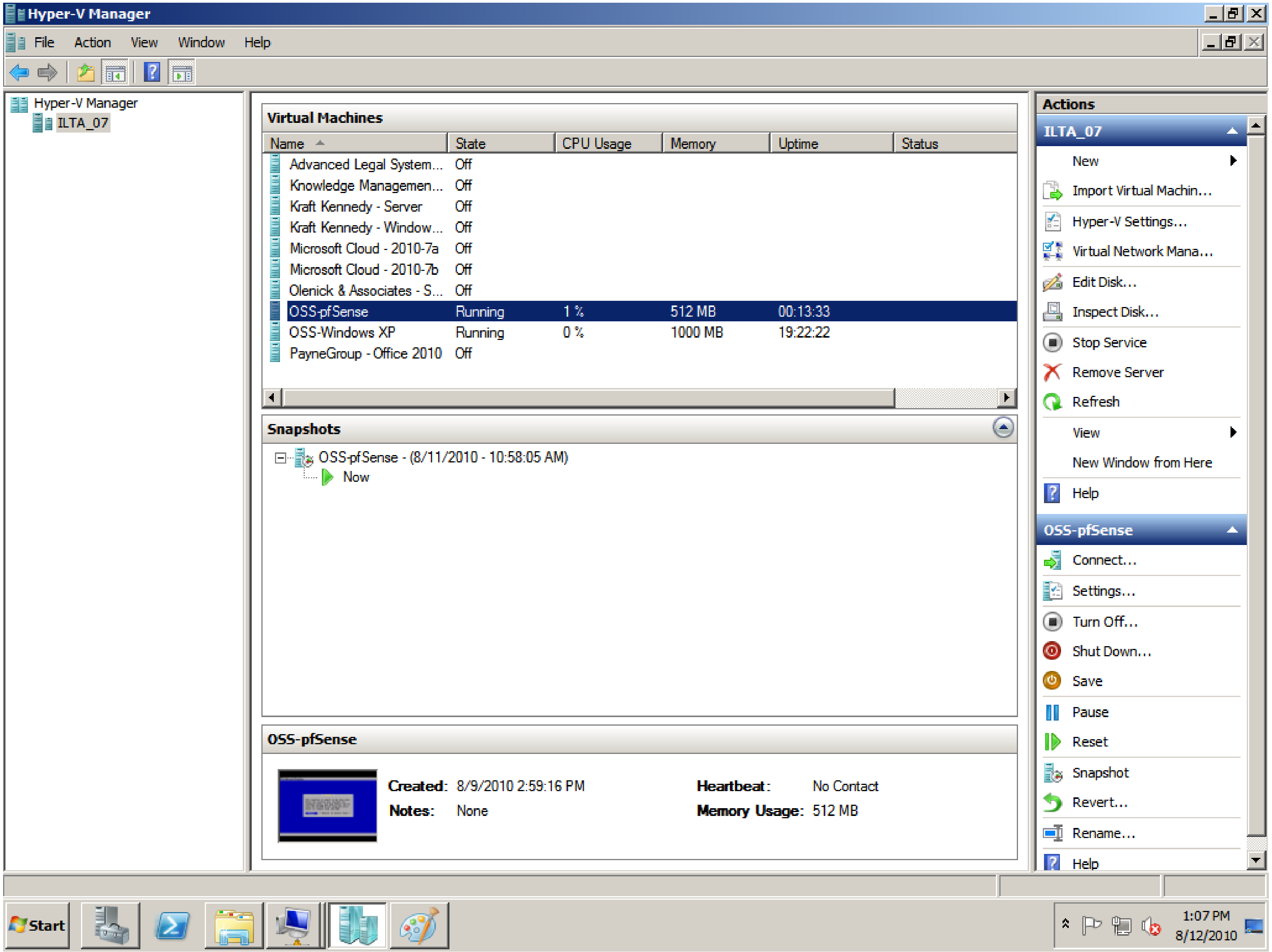
EXPERTS EXCHANGE

How do I get started? What do I need

- Properly sized hardware:
  - 100MHz Pentium CPU
  - 128 MB of RAM
- Requirements specific to individual platforms follow.
  - **Live CD**
CD-ROM drive
USB flash drive or floppy drive to hold configuration file
  - **Hard drive installation**
CD-ROM for initial installation
1 GB hard drive
  - **Embedded**
128 MB Compact Flash card
Serial port for console

Let’s Get Started!

Open Hyper-V



Virtual Machines

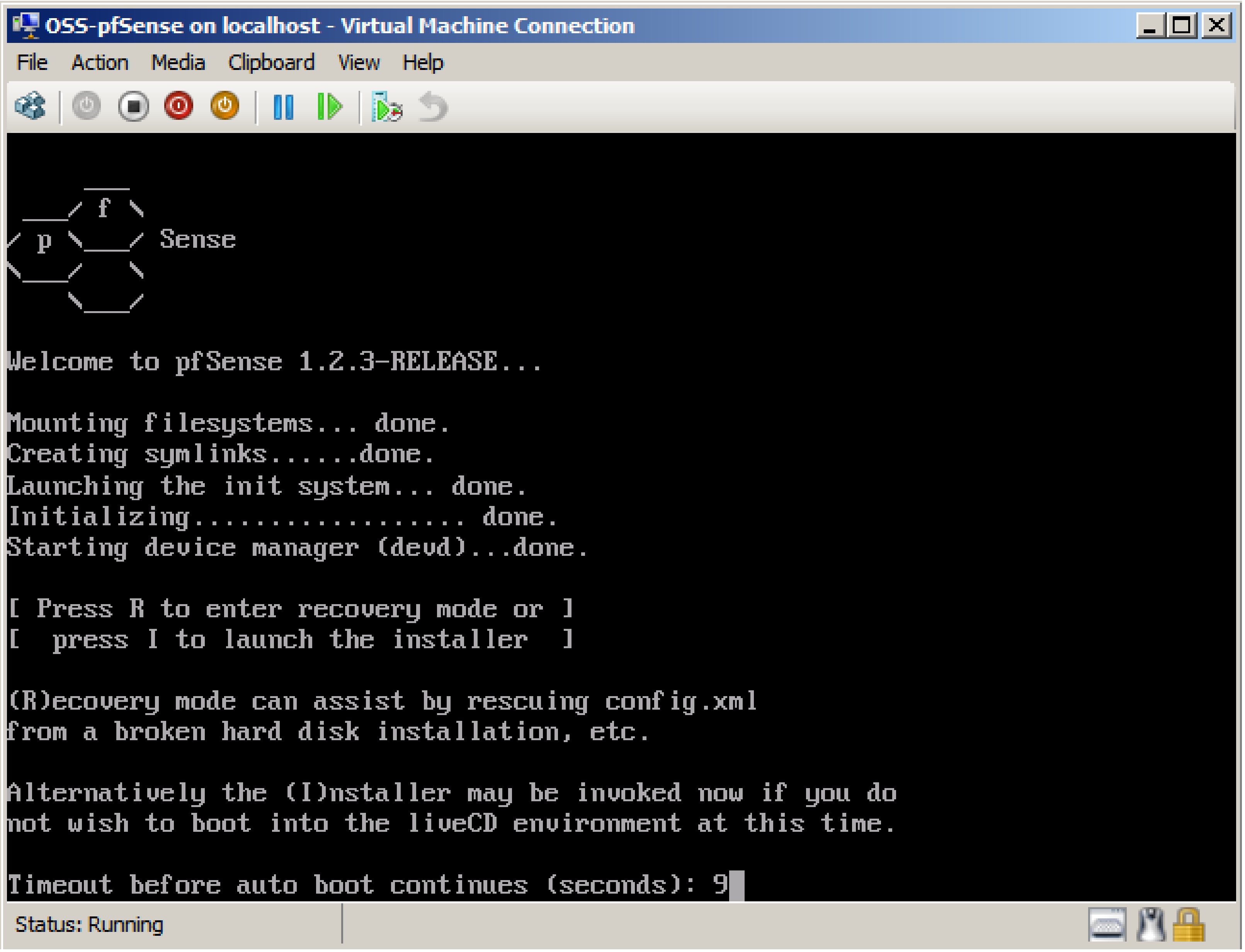
Name	State	CPU Usage	Memory	Uptime	Status
Advanced Legal System...	Off				
Knowledge Managemen...	Off				
Kraft Kennedy - Server	Off				
Kraft Kennedy - Window...	Off				
Microsoft Cloud - 2010-7a	Off				
Microsoft Cloud - 2010-7b	Off				
Olenick & Associates - S...	Off				
OSS-pfSense	Running	1 %	512 MB	00:13:33	
OSS-Windows XP	Running	0 %	1000 MB	19:22:22	
PayneGroup - Office 2010	Off				

Snapshots

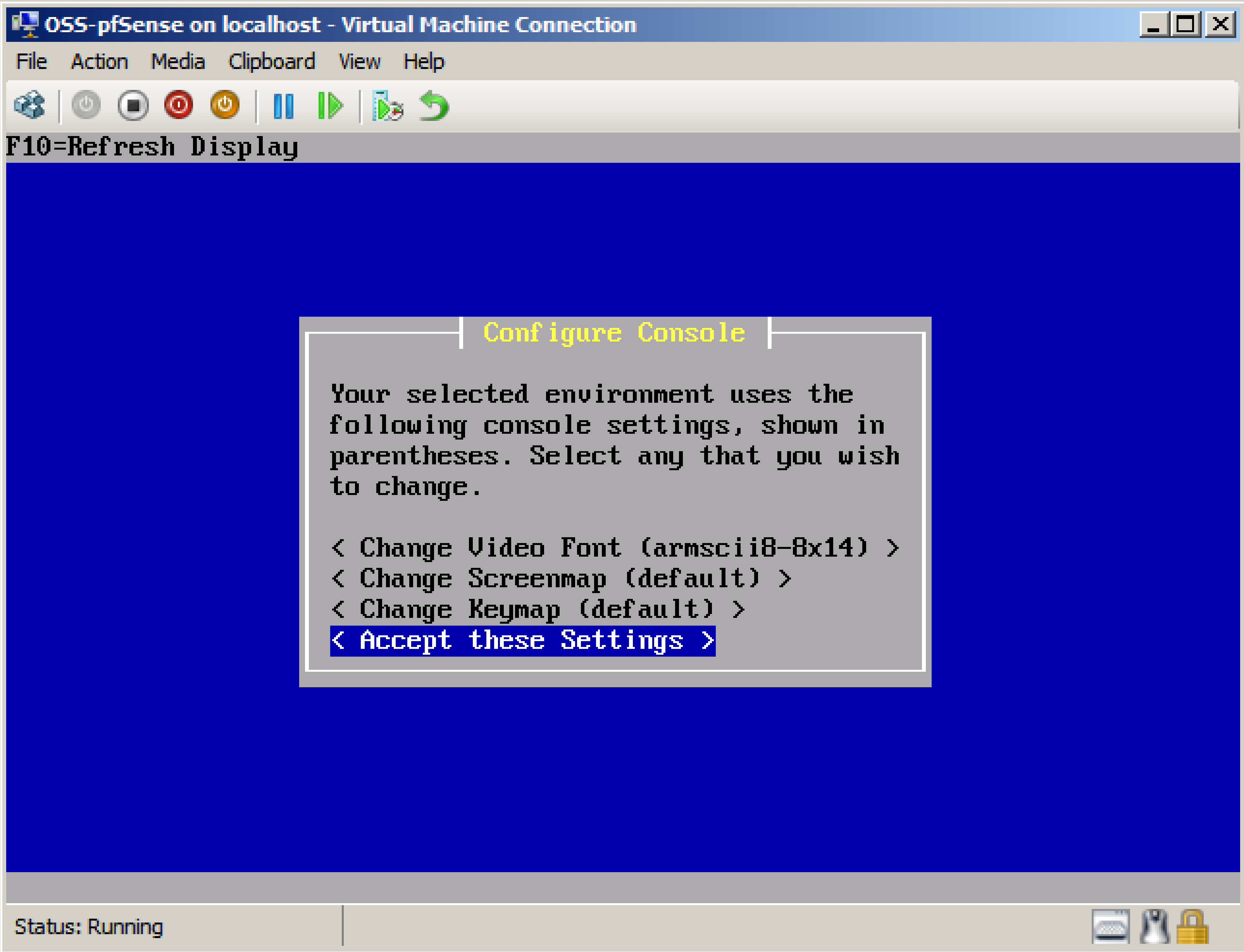
OSS-pfSense - (8/11/2010 - 10:58:05 AM)
Now

OSS-pfSense

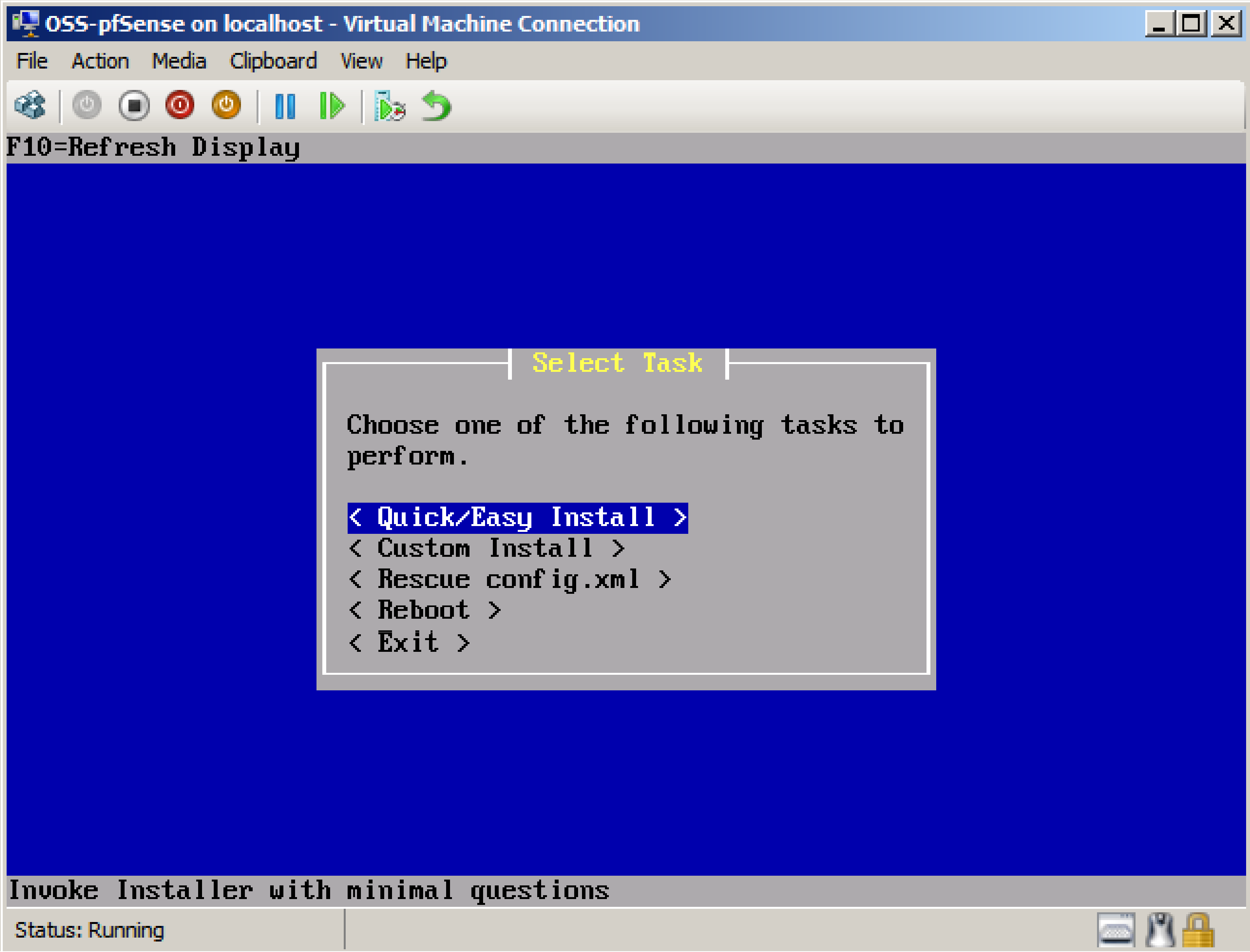
Created: 8/9/2010 2:59:16 PM
Notes: None
Heartbeat: No Contact
Memory Usage: 512 MB



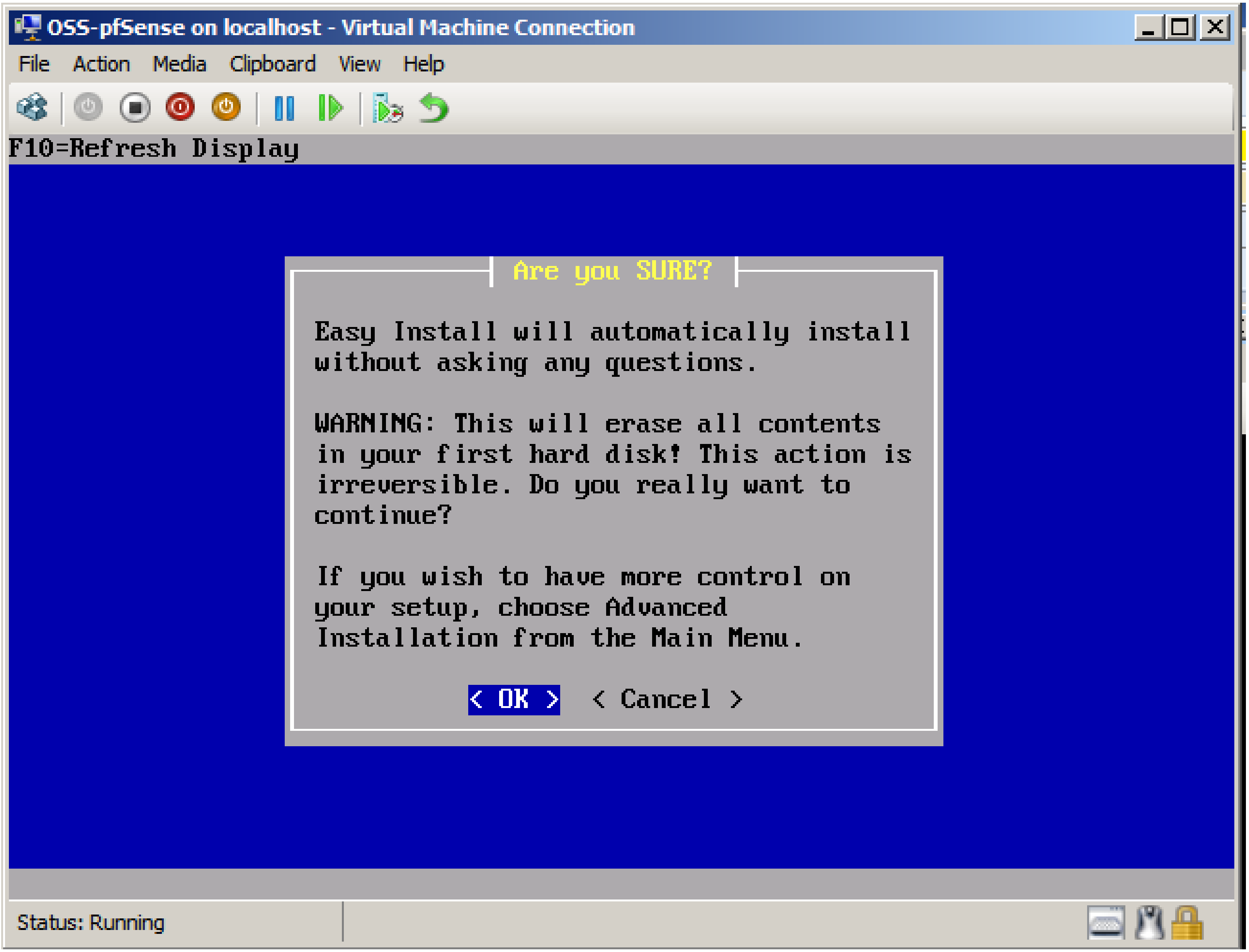
```
     ___
 ___/ f \
/ p \___/ Sense
\___/   \
    \___/

Welcome to pfSense 1.2.3-RELEASE...

Mounting filesystems... done.
Creating symlinks......done.
Launching the init system... done.
Initializing.................. done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[  press I to launch the installer  ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

Alternatively the (I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

Timeout before auto boot continues (seconds): 9
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

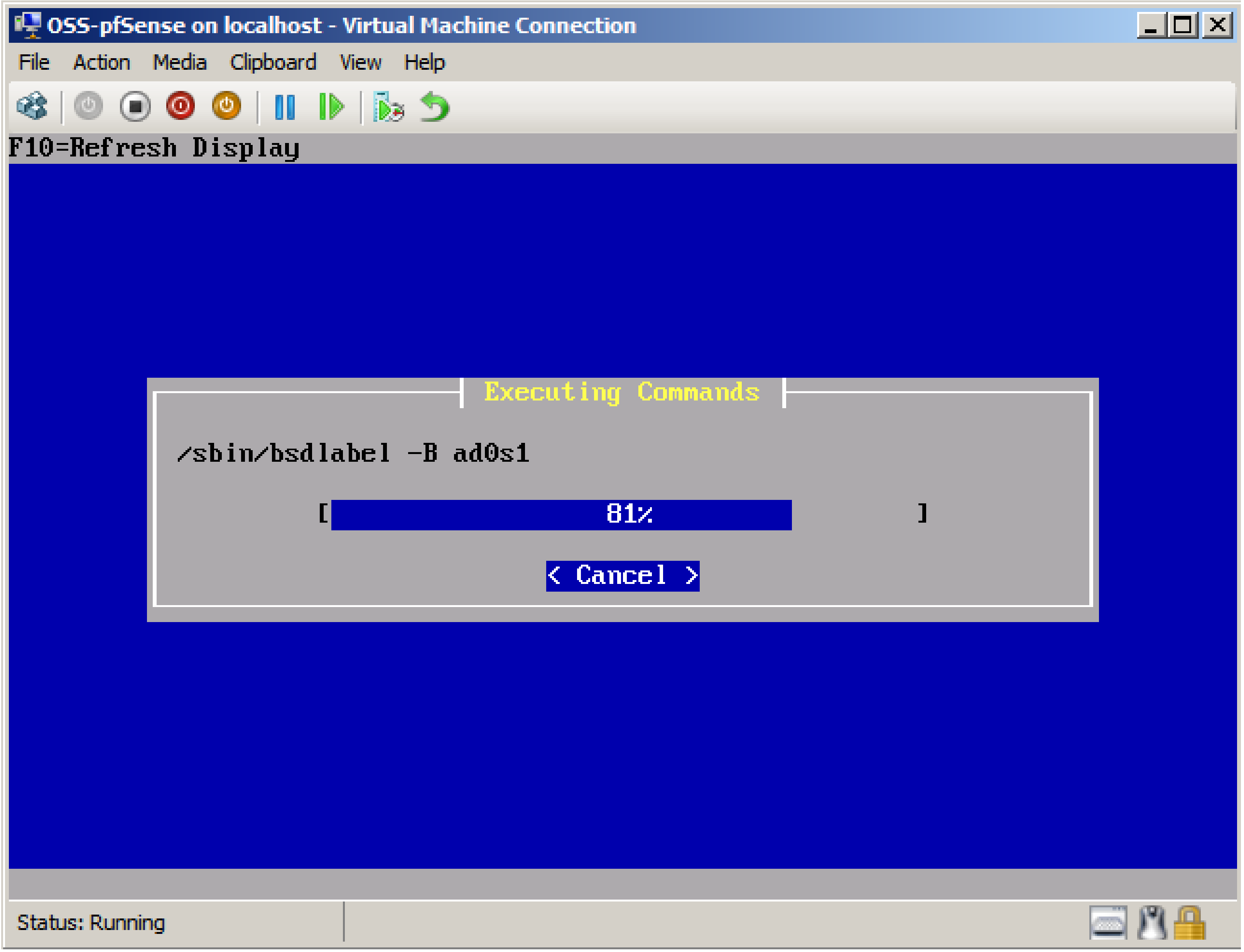
```
F10=Refresh Display

                    Configure Console

 Your selected environment uses the
 following console settings, shown in
 parentheses. Select any that you wish
 to change.

 < Change Video Font (armscii8-8x14) >
 < Change Screenmap (default) >
 < Change Keymap (default) >
 < Accept these Settings >
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

```
F10=Refresh Display

                    Select Task

   Choose one of the following tasks to
   perform.

   < Quick/Easy Install >
   < Custom Install >
   < Rescue config.xml >
   < Reboot >
   < Exit >

Invoke Installer with minimal questions
```

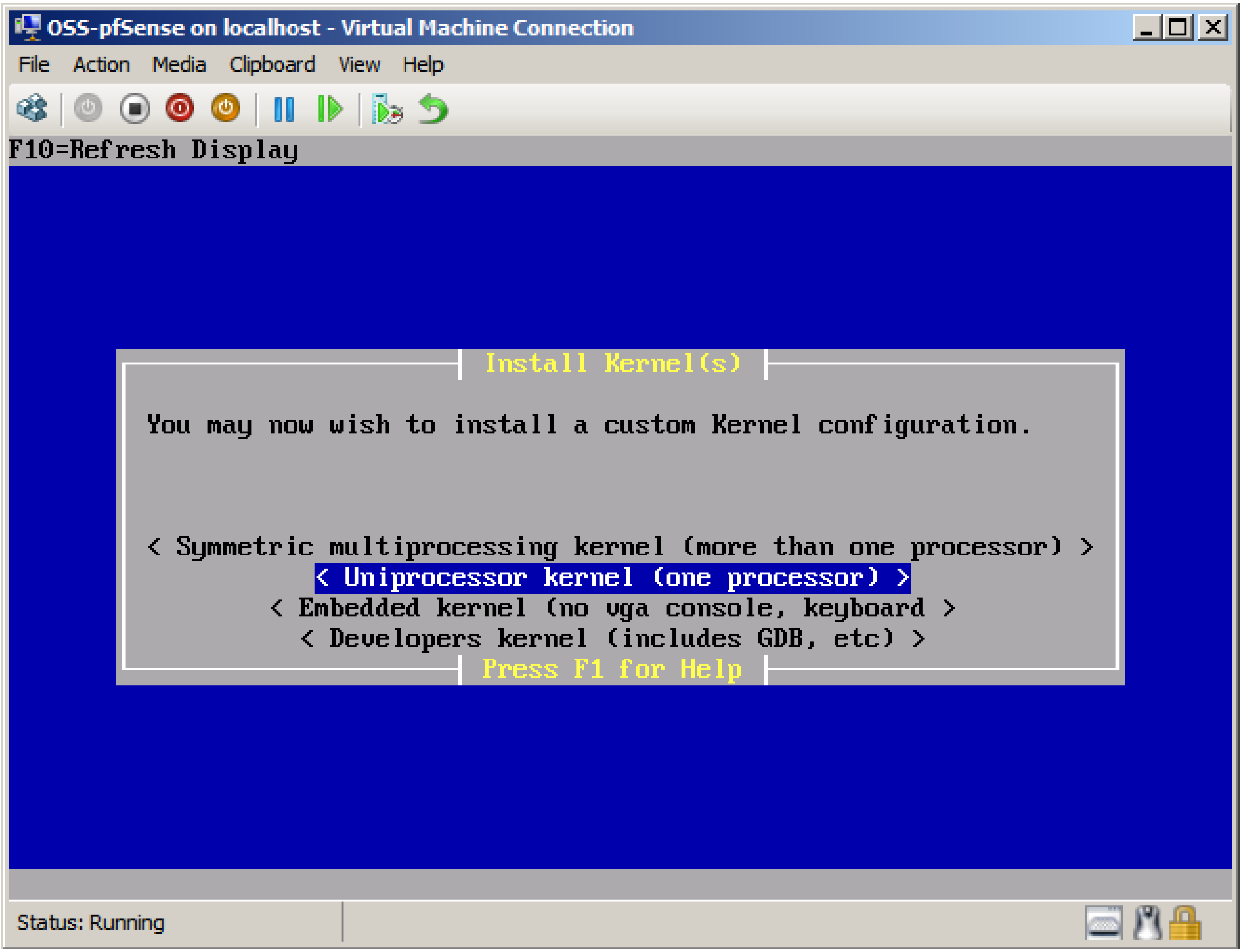

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
F10=Refresh Display

```
Are you SURE?

Easy Install will automatically install
without asking any questions.

WARNING: This will erase all contents
in your first hard disk! This action is
irreversible. Do you really want to
continue?

If you wish to have more control on
your setup, choose Advanced
Installation from the Main Menu.

           < OK >  < Cancel >
```

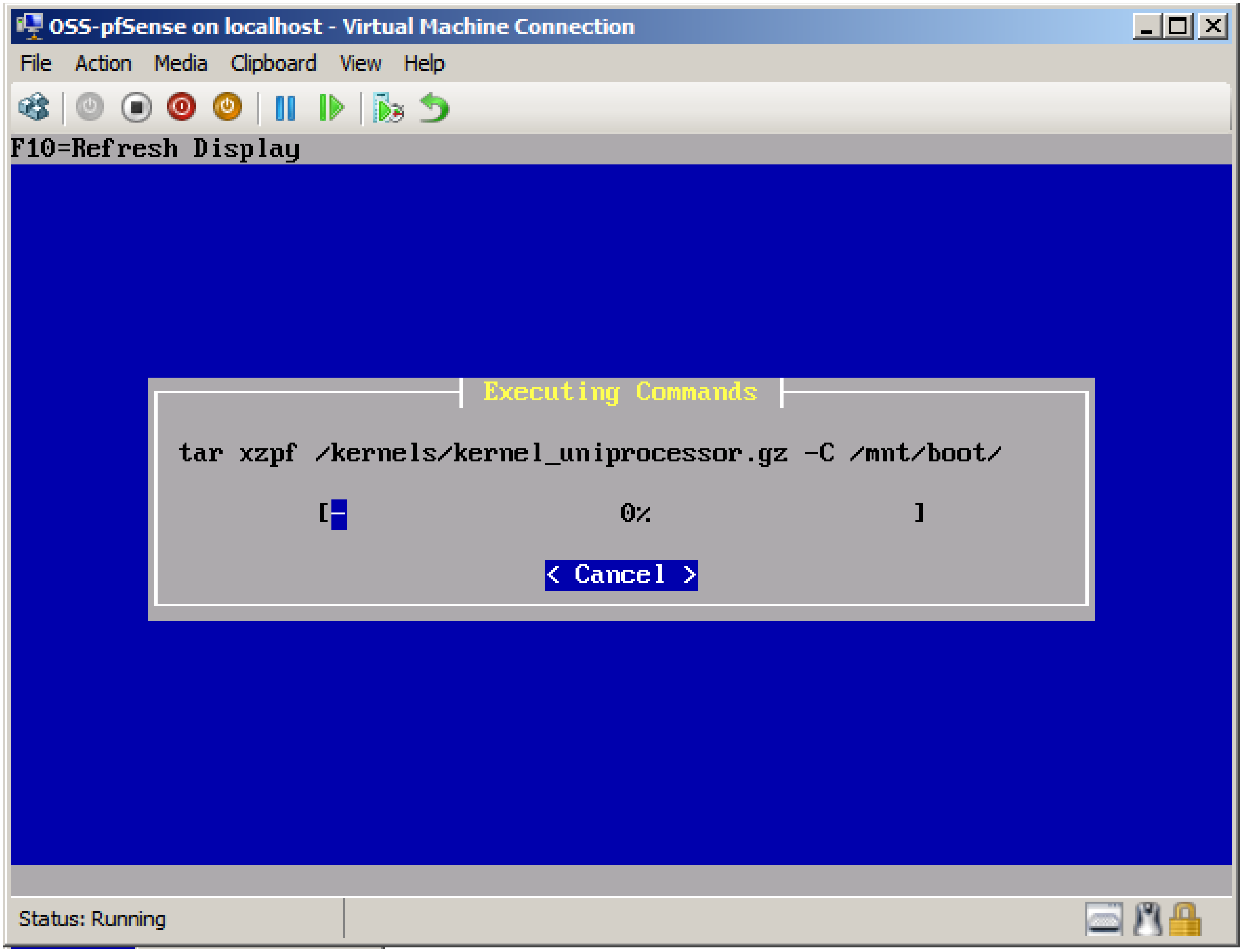


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

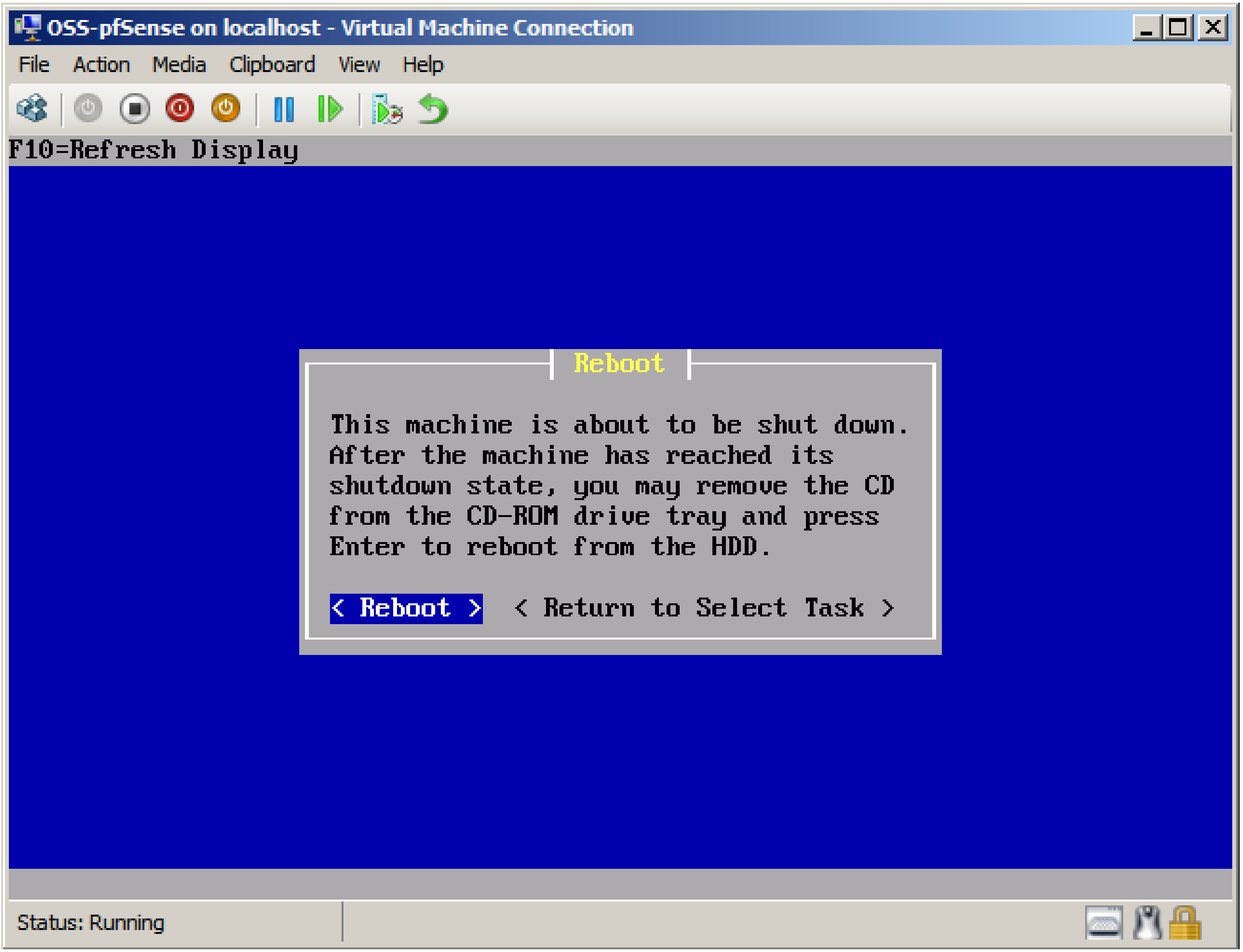
```
F10=Refresh Display

Executing Commands

/sbin/bsdlabel -B ad0s1

[                81%                    ]

< Cancel >
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

```
F10=Refresh Display

                    Install Kernel(s)

You may now wish to install a custom Kernel configuration.


< Symmetric multiprocessing kernel (more than one processor) >
          < Uniprocessor kernel (one processor) >
        < Embedded kernel (no vga console, keyboard >
          < Developers kernel (includes GDB, etc) >
                    Press F1 for Help
```

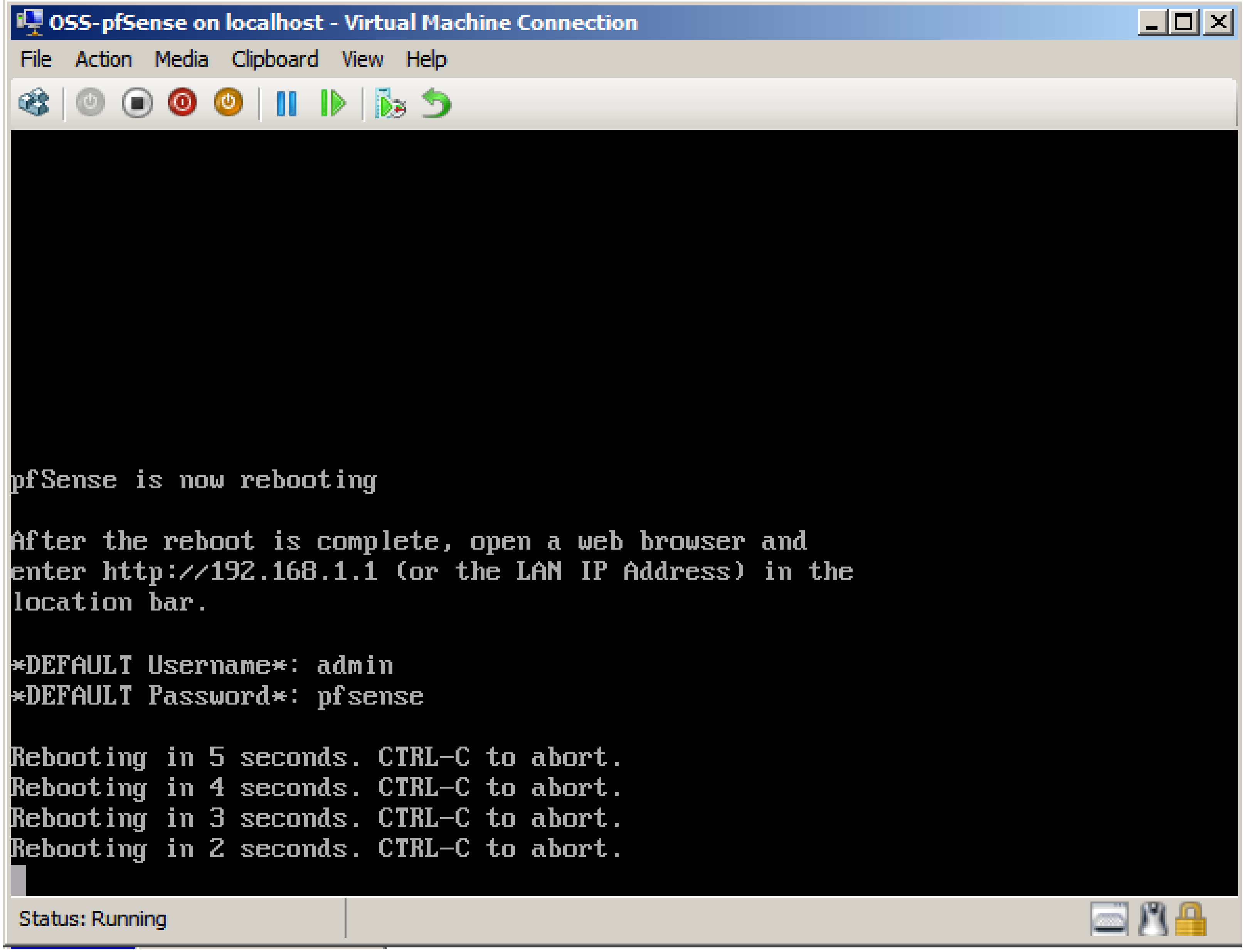

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
F10=Refresh Display

```
Executing Commands

tar xzpf /kernels/kernel_uniprocessor.gz -C /mnt/boot/

[-                  0%                  ]

< Cancel >
```

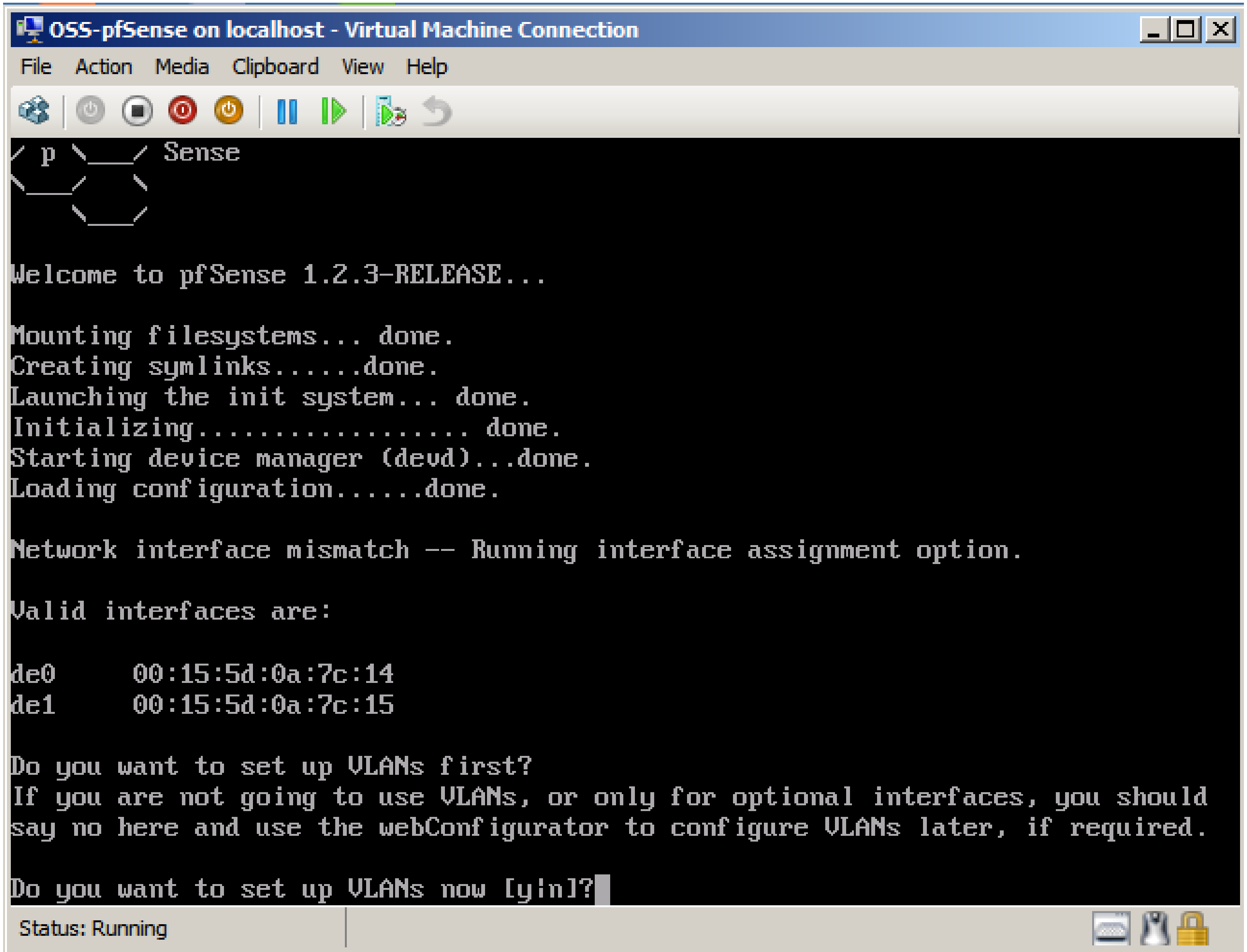

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

```
F10=Refresh Display

Reboot

This machine is about to be shut down.
After the machine has reached its
shutdown state, you may remove the CD
from the CD-ROM drive tray and press
Enter to reboot from the HDD.

< Reboot >   < Return to Select Task >
```

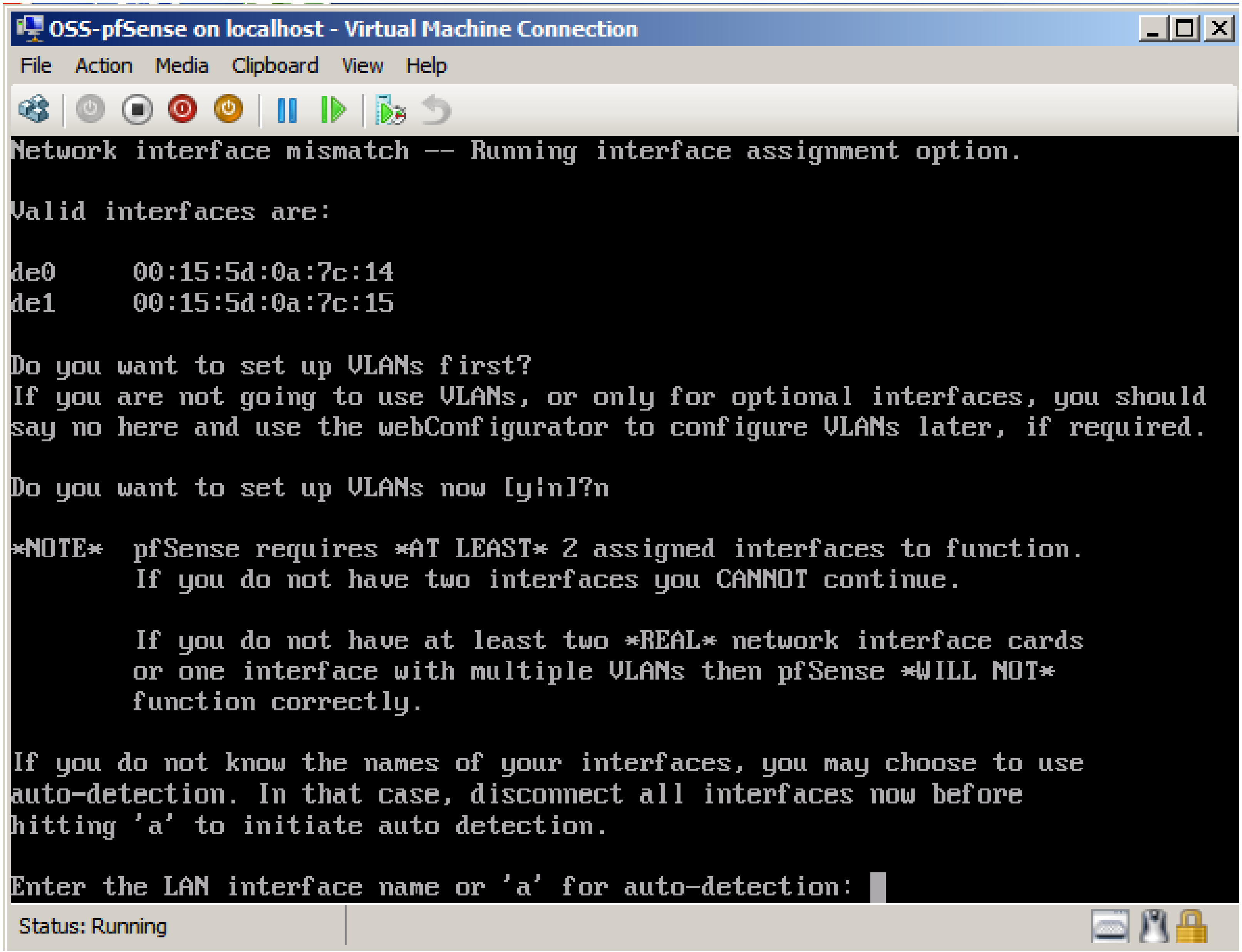
Status: Running



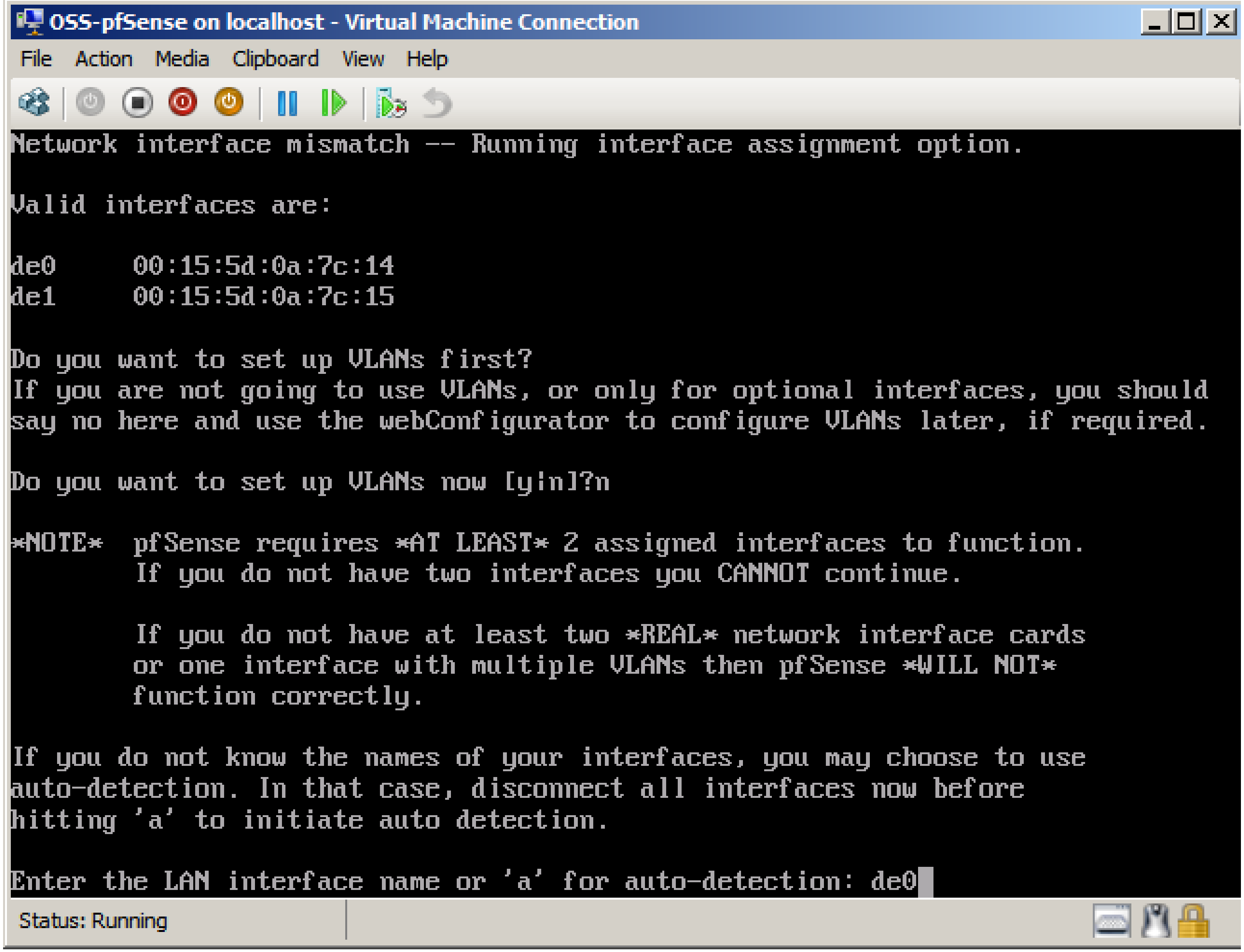
```
pfSense is now rebooting

After the reboot is complete, open a web browser and
enter http://192.168.1.1 (or the LAN IP Address) in the
location bar.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.
Rebooting in 2 seconds. CTRL-C to abort.
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

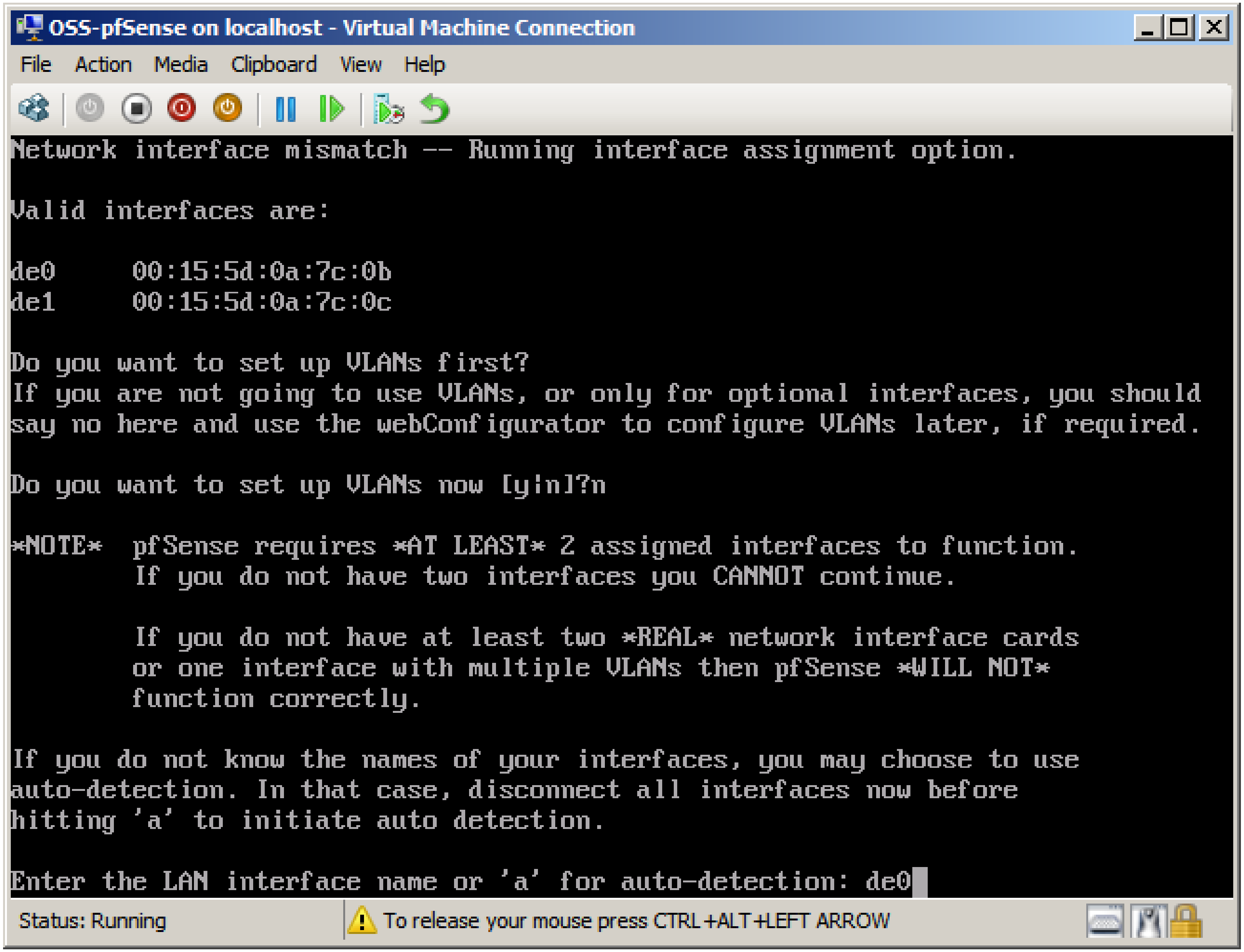
```
/ p \___/ Sense
\___/   \
    \___/

Welcome to pfSense 1.2.3-RELEASE...

Mounting filesystems... done.
Creating symlinks......done.
Launching the init system... done.
Initializing.................. done.
Starting device manager (devd)...done.
Loading configuration......done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0     00:15:5d:0a:7c:14
de1     00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

```
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0     00:15:5d:0a:7c:14
de1     00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection:
```

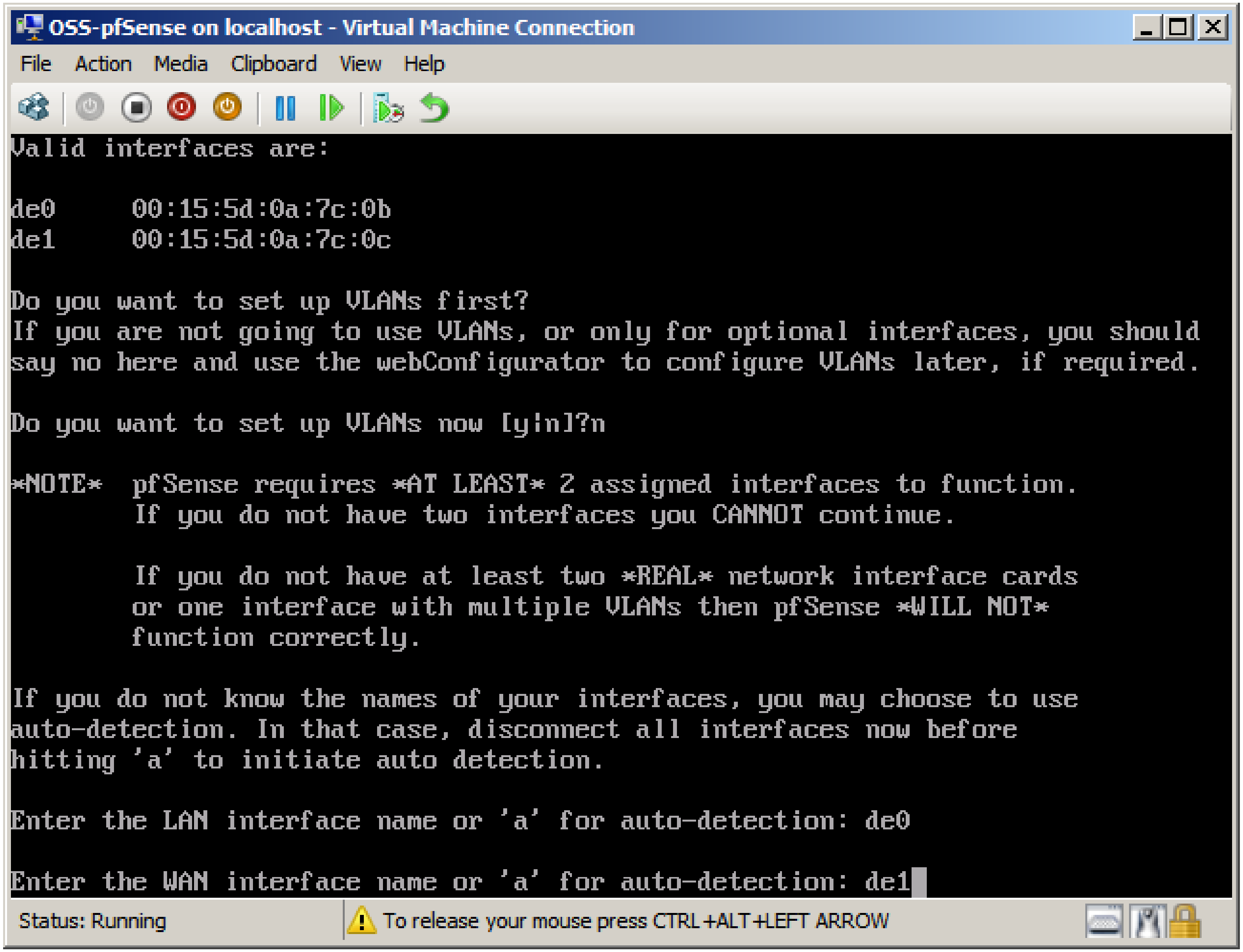

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

```
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0     00:15:5d:0a:7c:14
de1     00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0
```

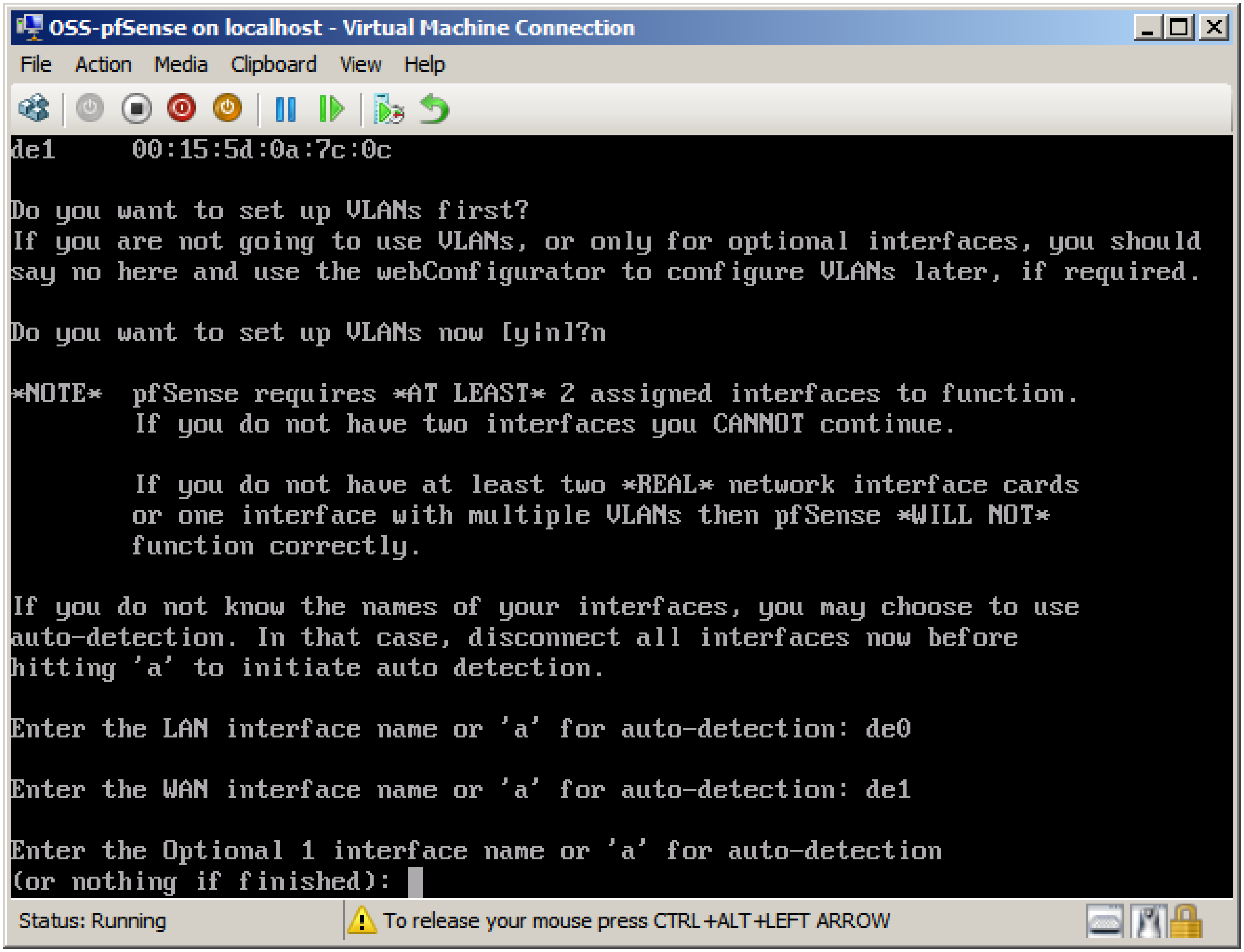


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

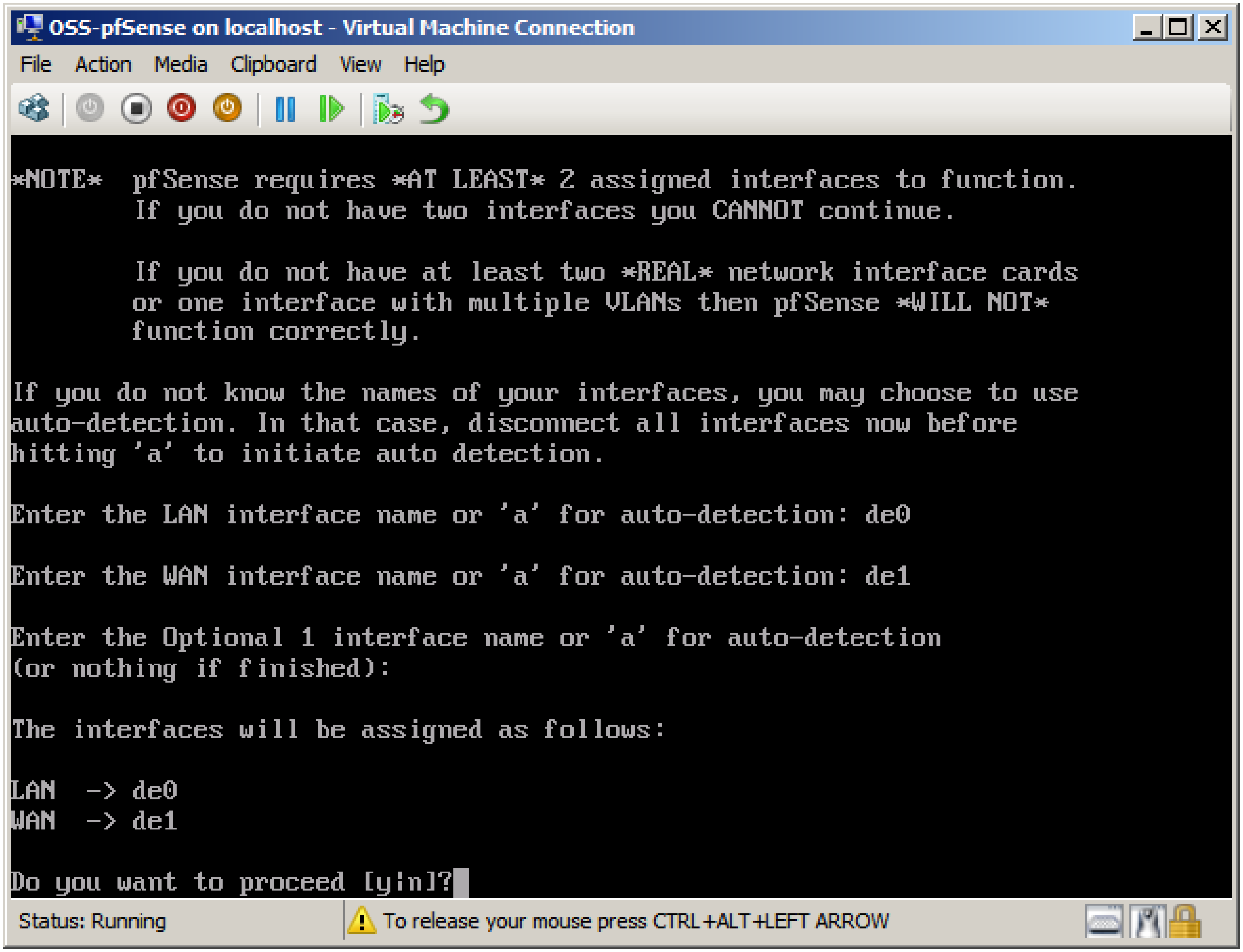
```
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0     00:15:5d:0a:7c:0b
de1     00:15:5d:0a:7c:0c

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0
```


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

```
Valid interfaces are:

de0     00:15:5d:0a:7c:0b
de1     00:15:5d:0a:7c:0c

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1
```

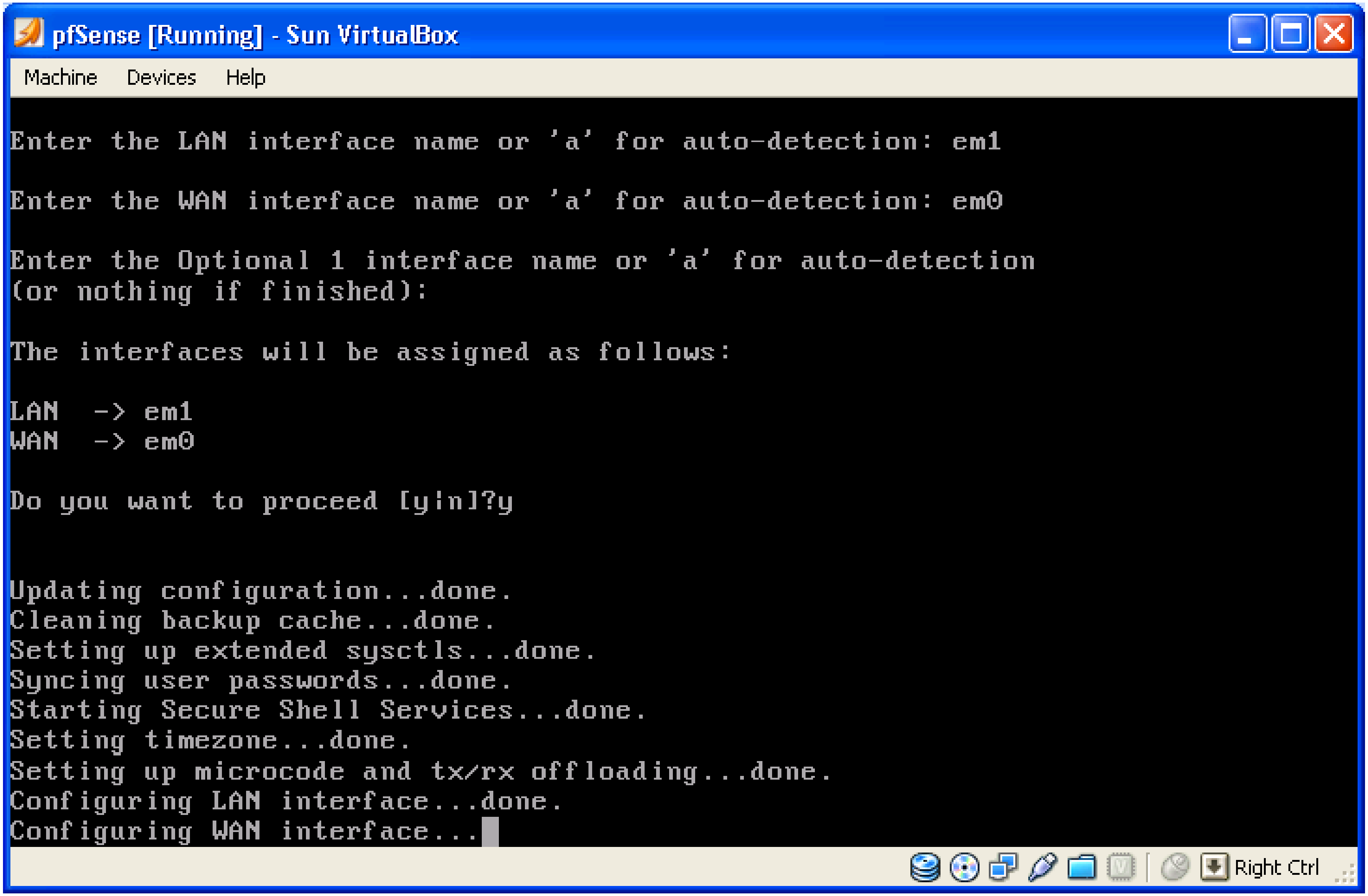

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running
To release your mouse press CTRL+ALT+LEFT ARROW

```
de1      00:15:5d:0a:7c:0c

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):
```

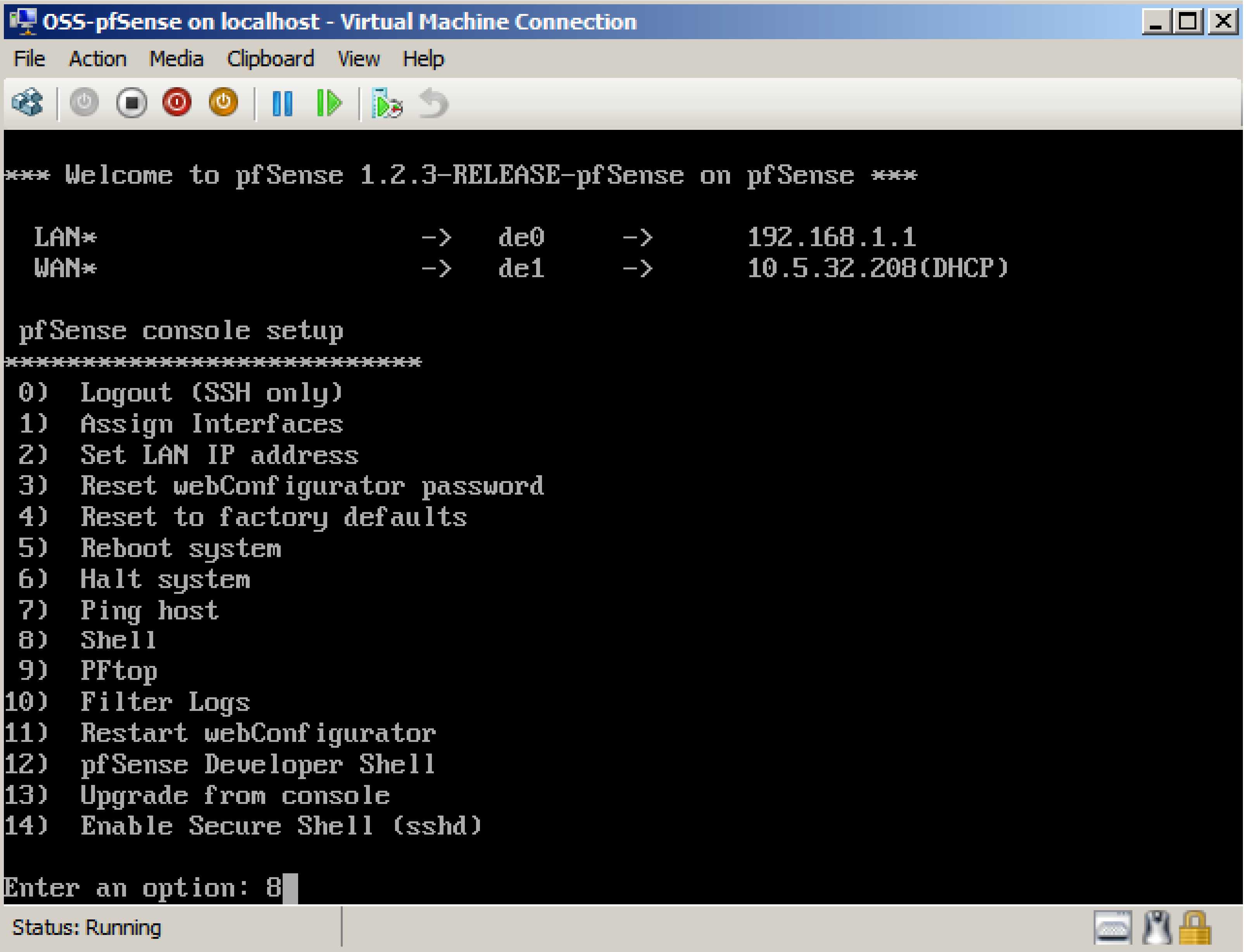


OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help

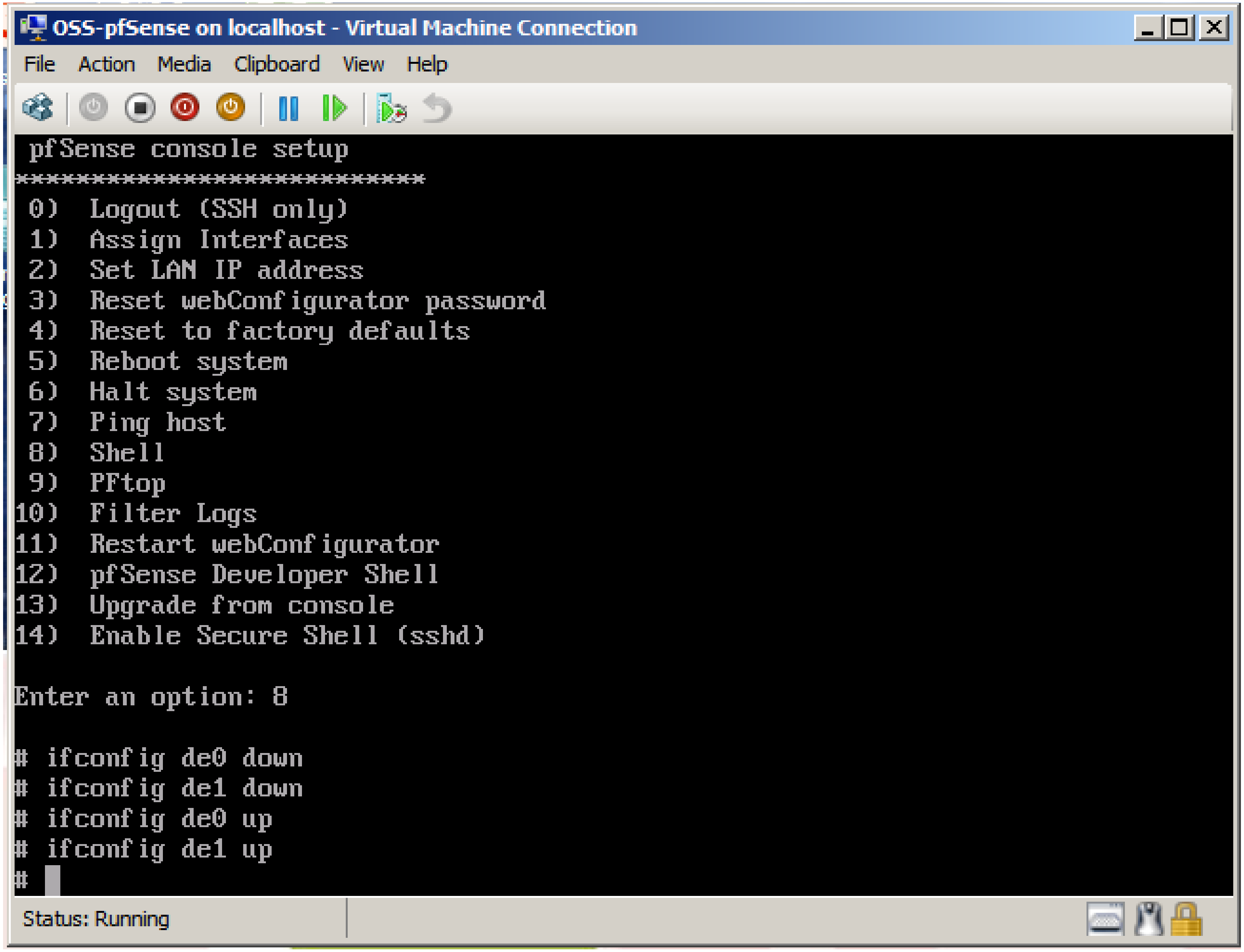
```
*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> de0
WAN  -> de1

Do you want to proceed [y|n]?
```



```
Enter the LAN interface name or 'a' for auto-detection: em1

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> em1
WAN  -> em0

Do you want to proceed [y|n]?y


Updating configuration...done.
Cleaning backup cache...done.
Setting up extended sysctls...done.
Syncing user passwords...done.
Starting Secure Shell Services...done.
Setting timezone...done.
Setting up microcode and tx/rx offloading...done.
Configuring LAN interface...done.
Configuring WAN interface...
```

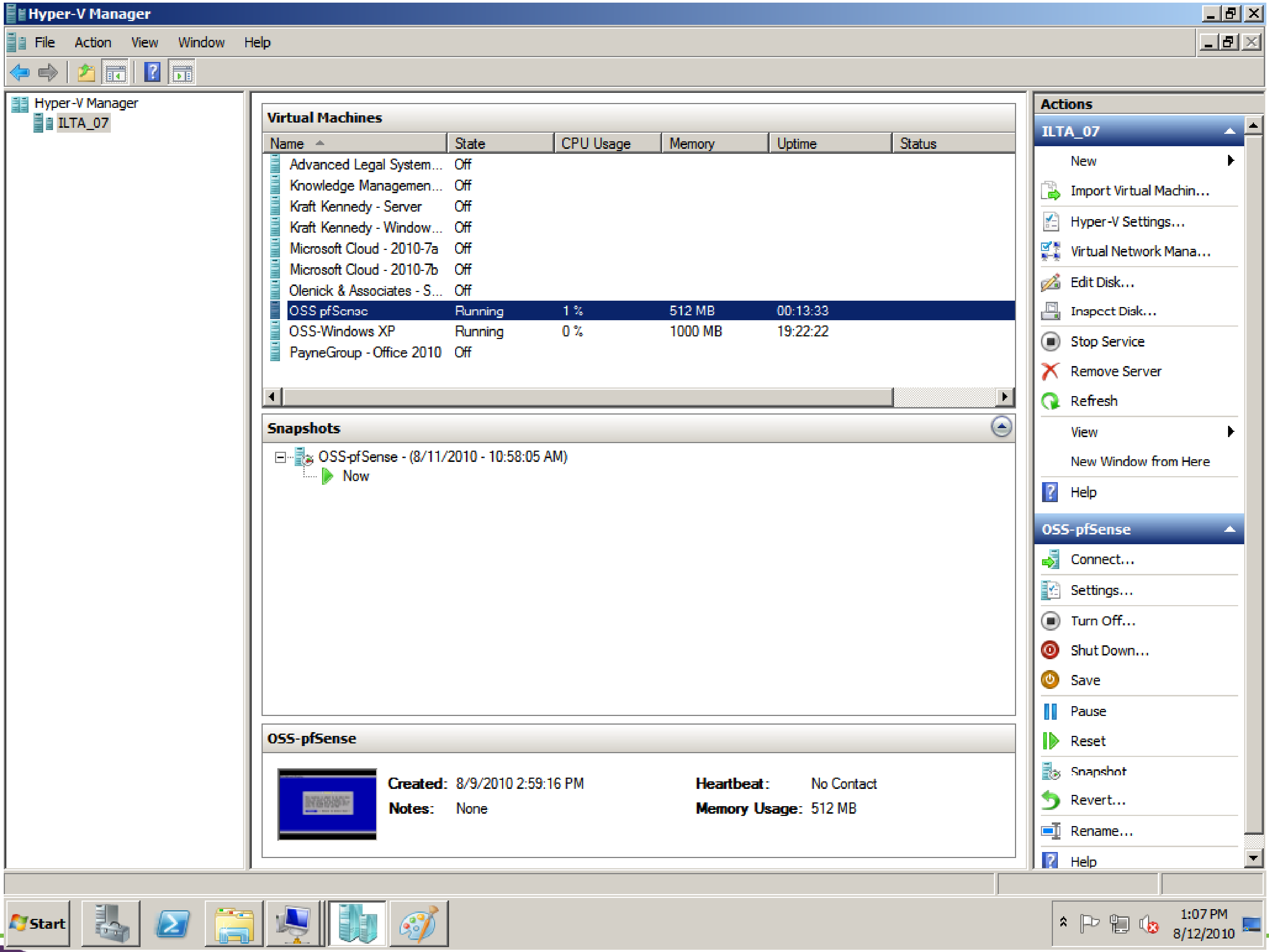

OSS-pfSense on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

```
*** Welcome to pfSense 1.2.3-RELEASE-pfSense on pfSense ***

  LAN*                          ->   de0     ->      192.168.1.1
  WAN*                          ->   de1     ->      10.5.32.208(DHCP)

 pfSense console setup
***************************
 0)  Logout (SSH only)
 1)  Assign Interfaces
 2)  Set LAN IP address
 3)  Reset webConfigurator password
 4)  Reset to factory defaults
 5)  Reboot system
 6)  Halt system
 7)  Ping host
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense Developer Shell
13)  Upgrade from console
14)  Enable Secure Shell (sshd)

Enter an option: 8
```



```
 pfSense console setup
***************************
 0)  Logout (SSH only)
 1)  Assign Interfaces
 2)  Set LAN IP address
 3)  Reset webConfigurator password
 4)  Reset to factory defaults
 5)  Reboot system
 6)  Halt system
 7)  Ping host
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense Developer Shell
13)  Upgrade from console
14)  Enable Secure Shell (sshd)

Enter an option: 8

# ifconfig de0 down
# ifconfig de1 down
# ifconfig de0 up
# ifconfig de1 up
#
```

```
ifconfig de0 down
ifconfig de0 up
ifconfig de1 down
ifconfig de1 up
```



Virtual Machines

Name	State	CPU Usage	Memory	Uptime	Status
Advanced Legal System...	Off				
Knowledge Managemen...	Off				
Kraft Kennedy - Server	Off				
Kraft Kennedy - Window...	Off				
Microsoft Cloud - 2010-7a	Off				
Microsoft Cloud - 2010-7b	Off				
Olenick & Associates - S...	Off				
OSS pfSense	Running	1 %	512 MB	00:13:33	
OSS-Windows XP	Running	0 %	1000 MB	19:22:22	
PayneGroup - Office 2010	Off				

Snapshots

OSS-pfSense - (8/11/2010 - 10:58:05 AM)
Now

OSS-pfSense

Created: 8/9/2010 2:59:16 PM
Notes: None
Heartbeat: No Contact
Memory Usage: 512 MB

Hardware Sizing

- When sizing hardware for use with pfSense, two main factors need to be considered.
  - Throughput required
  - Features that will be used

- Throughput Considerations
  - If you require less than 10 Mbps of throughput, you can get by with the minimum requirements. For higher throughput requirements we recommend following these guidelines, based on our extensive testing and deployment experience. These guidelines offer a bit of breathing room because you never want to run your hardware to its full capacity.

Hardware Sizing

- 10-20 Mbps - No less than 266 MHz CPU
- 21-50 Mbps - No less than 500 MHz CPU
- 51-200 Mbps - No less than 1.0 GHz CPU
- 201-500 Mbps - server class hardware with PCI-X or PCI-e network adapters, or newer desktop hardware with PCI-e network adapters. No less than 2.0 GHz CPU.
- 501+ Mbps - server class hardware with PCI-X or PCI-e network adapters. No less than 3.0 GHz CPU.

Hardware Sizing

- **Feature Considerations**
  - Most features do not factor into hardware sizing, though a few have significant impact on hardware utilization.
  - **VPN** - Heavy use of any of the VPN services included in pfSense will increase CPU requirements. Encrypting and decrypting traffic is CPU intensive. The number of connections is much less of a concern than the throughput required. A 266 MHz CPU will max out at around 4 Mbps of IPsec throughput, a 500 MHz CPU can push 10-15 Mbps of IPsec, and relatively new server hardware (Xeon 800 FSB and newer) deployments are pushing over 100 Mbps with plenty of capacity to spare. Supported encryption cards, such as several from Hifn, are capable of significantly reducing CPU requirements.

Hardware Sizing

- **Captive portal** - While the primary concern is typically throughput, environments with hundreds of simultaneous captive portal users (of which there are many) will require slightly more CPU power than recommended above.
- **Large state tables** - State table entries require about 1 KB of RAM each. The default state table, when full at 10,000 entries, takes up a little less than 10 MB RAM. For large environments requiring state tables with hundreds of thousands of connections, ensure adequate RAM is available.
- **Packages** - Some of the packages increase RAM requirements significantly. Snort and ntop are two that should not be installed on a system with less than 512 MB RAM.

Hardware Compatibility List

- pfSense 1.2.3 is based on FreeBSD 7.2, its hardware compatibility list is the same as FreeBSD's.
- The pfSense kernel includes all FreeBSD drivers.
- Visit freebsd.org for the HCL.
  - http://www.freebsd.org/releases/7.2R/hardware.html

Firewall Features

- Firewall
  - Filtering by source and destination IP, IP protocol, source and destination port for TCP and UDP traffic
  - Able to limit simultaneous connections on a per-rule basis
  - pfSense utilizes p0f, an advanced passive OS/network fingerprinting utility, to allow you to filter by the Operating System initiating the connection. Want to allow FreeBSD and Linux machines to the Internet, but block Windows machines? pfSense can do so (amongst many other possibilities) by passively detecting the Operating System in use.
  - Option to log or not log traffic matching each rule.

Firewall Features

– Highly flexible policy routing possible by selecting gateway on a per-rule basis (for load balancing, failover, multiple WAN, etc.)

– Aliases allow grouping and naming of IPs, networks and ports. This helps keep your firewall ruleset clean and easy to understand, especially in environments with multiple public IPs and numerous servers.

– Transparent layer 2 firewalling capable - can bridge interfaces and filter traffic between them, even allowing for an IP-less firewall (though you probably want an IP for management purposes).

Firewall Features

- Packet normalization
  - 'Scrubbing' is the normalization of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembles fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations.
  - Enabled in pfSense by default
  - Can disable if necessary. This option causes problems for some NFS implementations, but is safe and should be left enabled on most installations.
  - Disable filter - you can turn off the firewall filter entirely if you wish to turn pfSense into a pure router.

VPN

- pfSense offers three options for VPN connectivity:
  - IPsec
  - OpenVPN
  - PPTP

Captive Portal

- Captive Portal
  - Captive portal allows you to force authentication, or redirection to a click through page for network access. This is commonly used on hot spot networks (like the Aria), but is also widely used in corporate networks for an additional layer of security on guest wireless or Internet access.

Load Balancing

Load Balancing

- Outbound Load Balancing
  - Outbound load balancing is used with multiple WAN connections to provide load balancing and failover capabilities. Traffic is directed to the desired gateway or load balancing pool on a per-firewall rule basis.
- Inbound Load Balancing
  - Inbound load balancing is used to distribute load between multiple servers. This is commonly used with web servers, mail servers, and others. Servers that fail to respond to ping requests or TCP port connections are removed from the pool.

Reporting and Monitoring

- **RRD Graphs**
- The RRD graphs in pfSense maintain historical information on the following.
- CPU utilization
- Total throughput
- Firewall states
- Individual throughput for all interfaces
- Packets per second rates for all interfaces
- WAN interface gateway(s) ping response times
- Traffic shaper queues on systems with traffic shaping enable

Reporting and Monitoring

- Real Time Information
- Historical information is important, but sometimes it's more important to see real time information.
- SVG graphs are available that show real time throughput for each interface.
- For traffic shaper users, the Status -> Queues screen provides a real time display of queue usage using AJAX updated gauges.
- The front page includes AJAX gauges for display of real time CPU, memory, swap and disk usage, and state table size.

Redundancy/High Availability

- CARP
  - Common Address Redundancy Protocol

Redundancy/High Availability

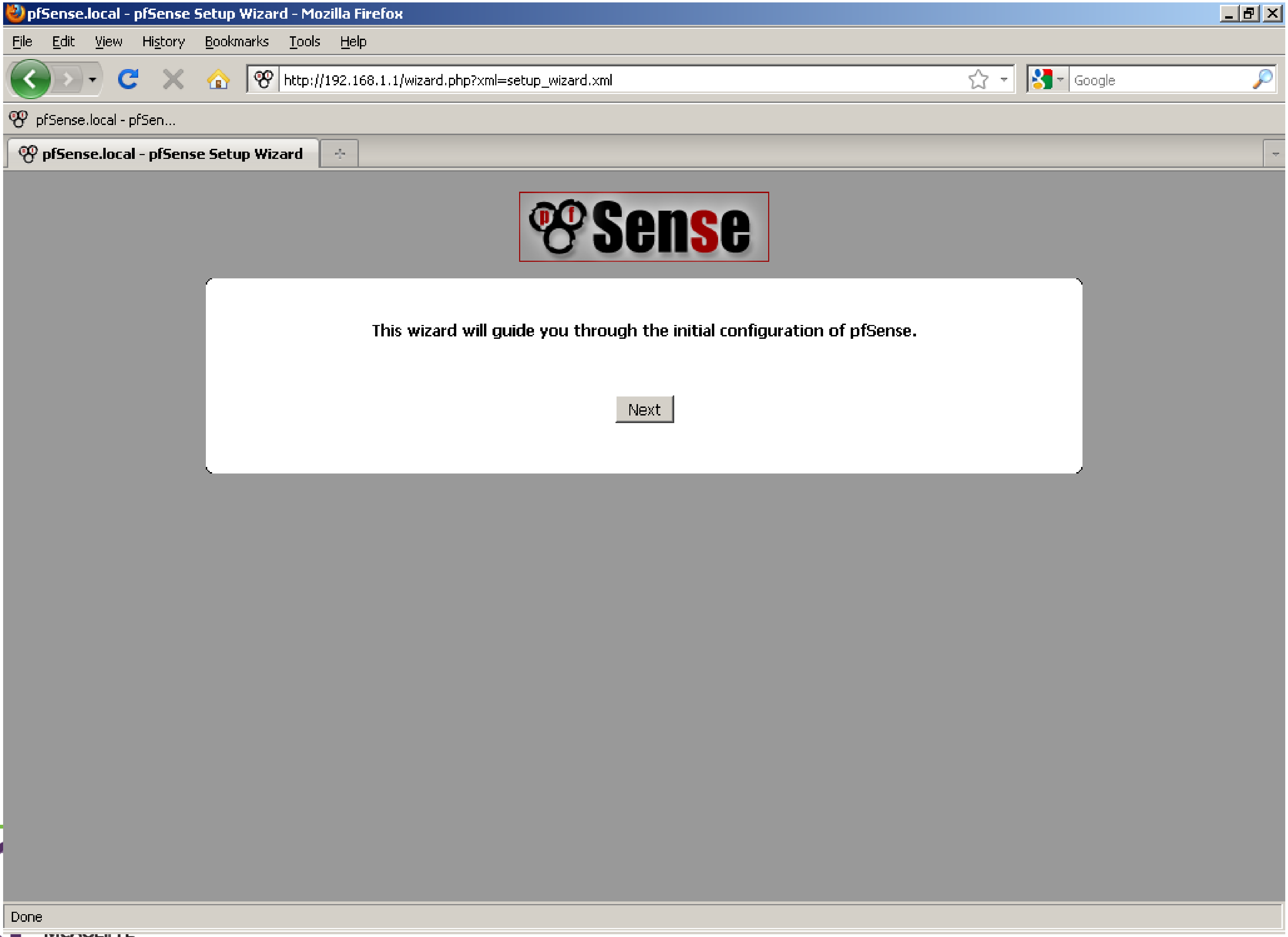
- Two or more firewalls can be configured as a failover group.
- If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.
- pfSynch ensures that state tables are also synchronized so that in the even of a failure seamless failover can occur.

Network Address Translation

- Port forwards including ranges and the use of multiple public IPs
- 1:1 NAT for individual IPs or entire subnets.
- Outbound NAT
  - Default settings NAT all outbound traffic to the WAN IP. In multiple WAN scenarios, the default settings NAT outbound traffic to the IP of the WAN interface being used.
  - Advanced Outbound NAT allows this default behavior to be disabled, and enables the creation of very flexible NAT (or no NAT) rules.
- NAT Reflection - in some configurations, NAT reflection is possible so services can be accessed by public IP from internal networks.

192.168.1.1

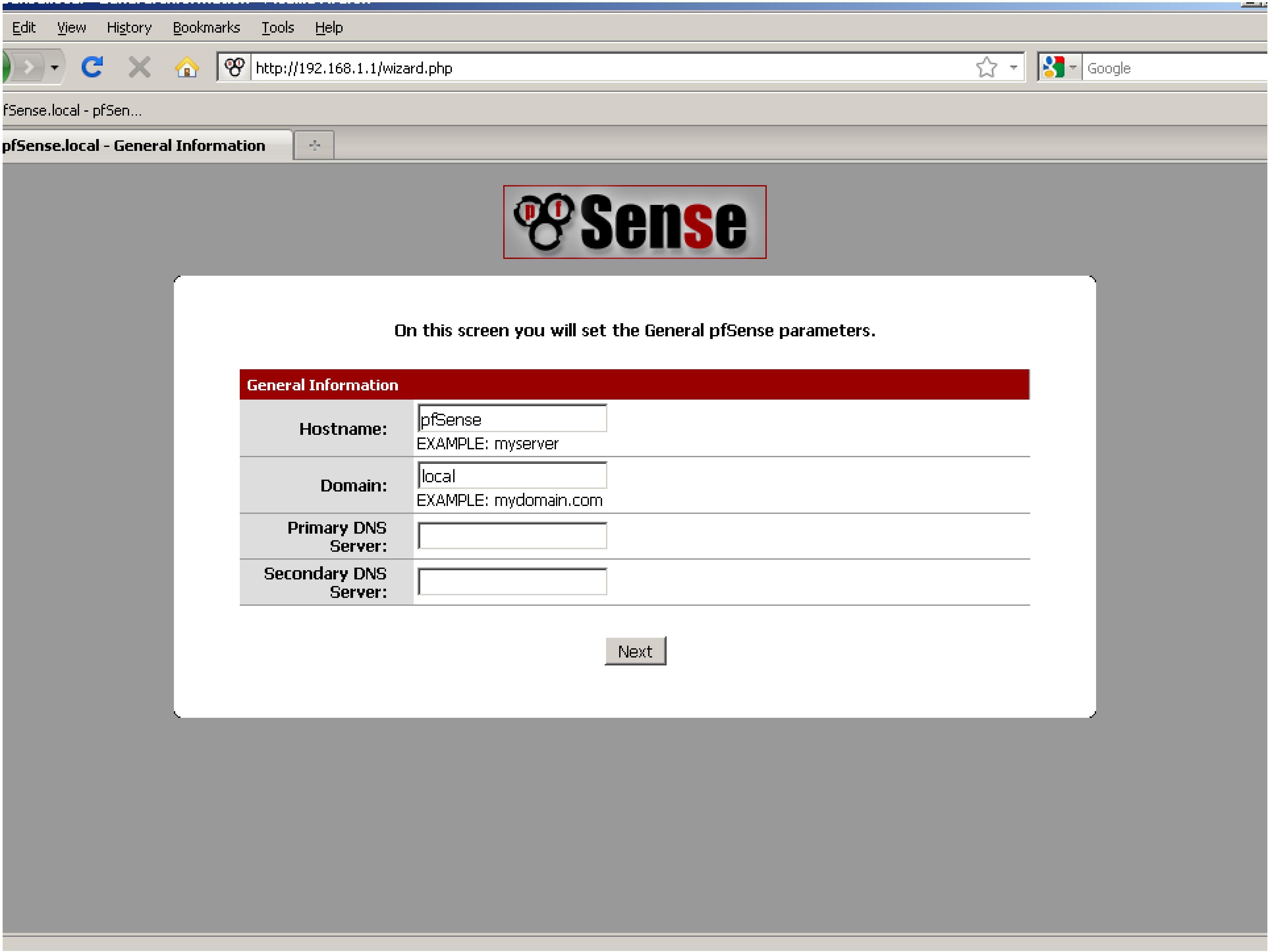
admin
pfsense



pfSense.local - pfSense Setup Wizard - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Google
pfSense.local - pfSen...
pfSense.local - pfSense Setup Wizard
pf Sense
Next
Done

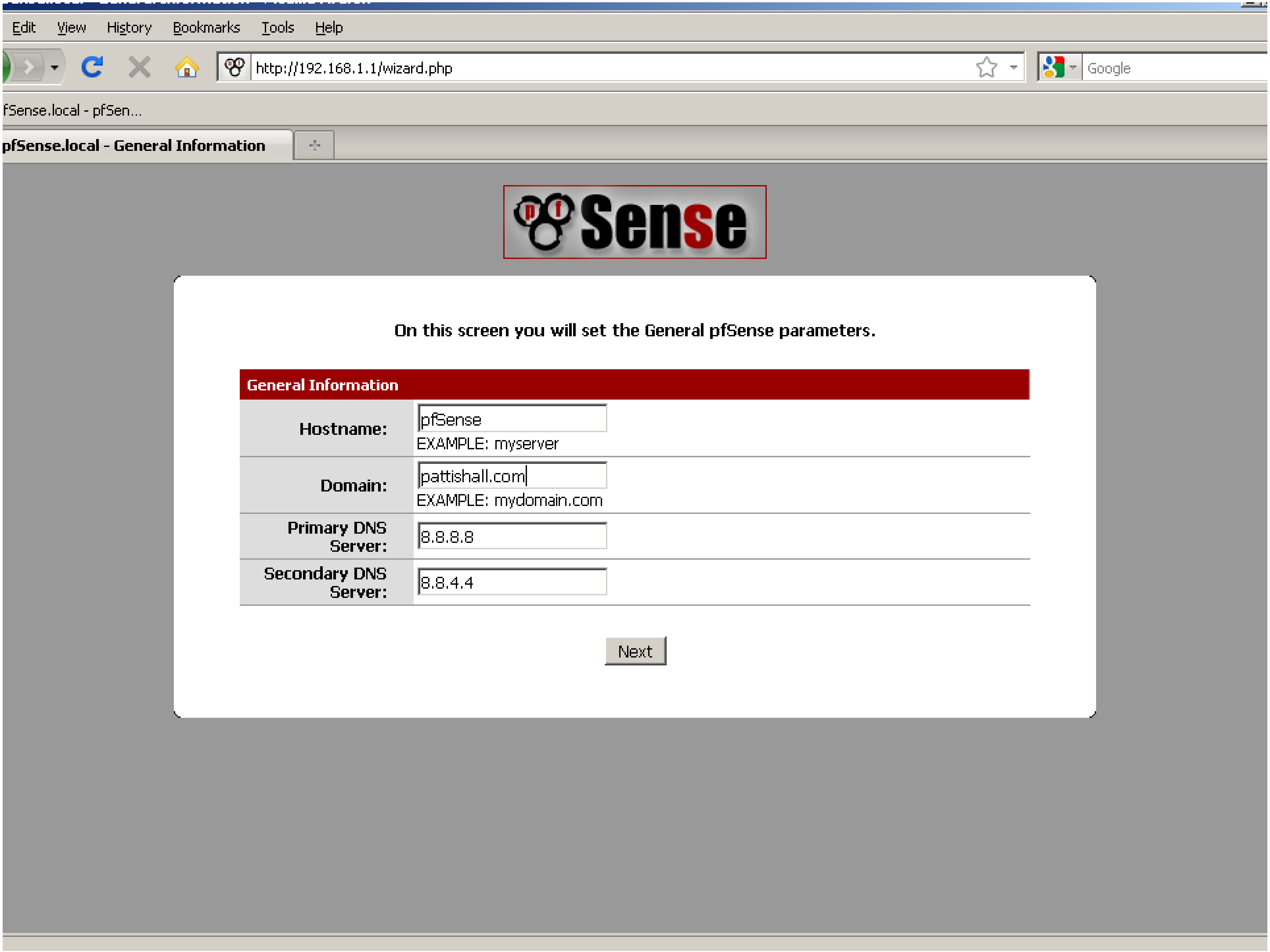
http://192.168.1.1/wizard.php?xml=setup_wizard.xml

This wizard will guide you through the initial configuration of pfSense.


Edit View History Bookmarks Tools Help
http://192.168.1.1/wizard.php
Google
fSense.local - pfSen...
pfSense.local - General Information
pfSense

On this screen you will set the General pfSense parameters.

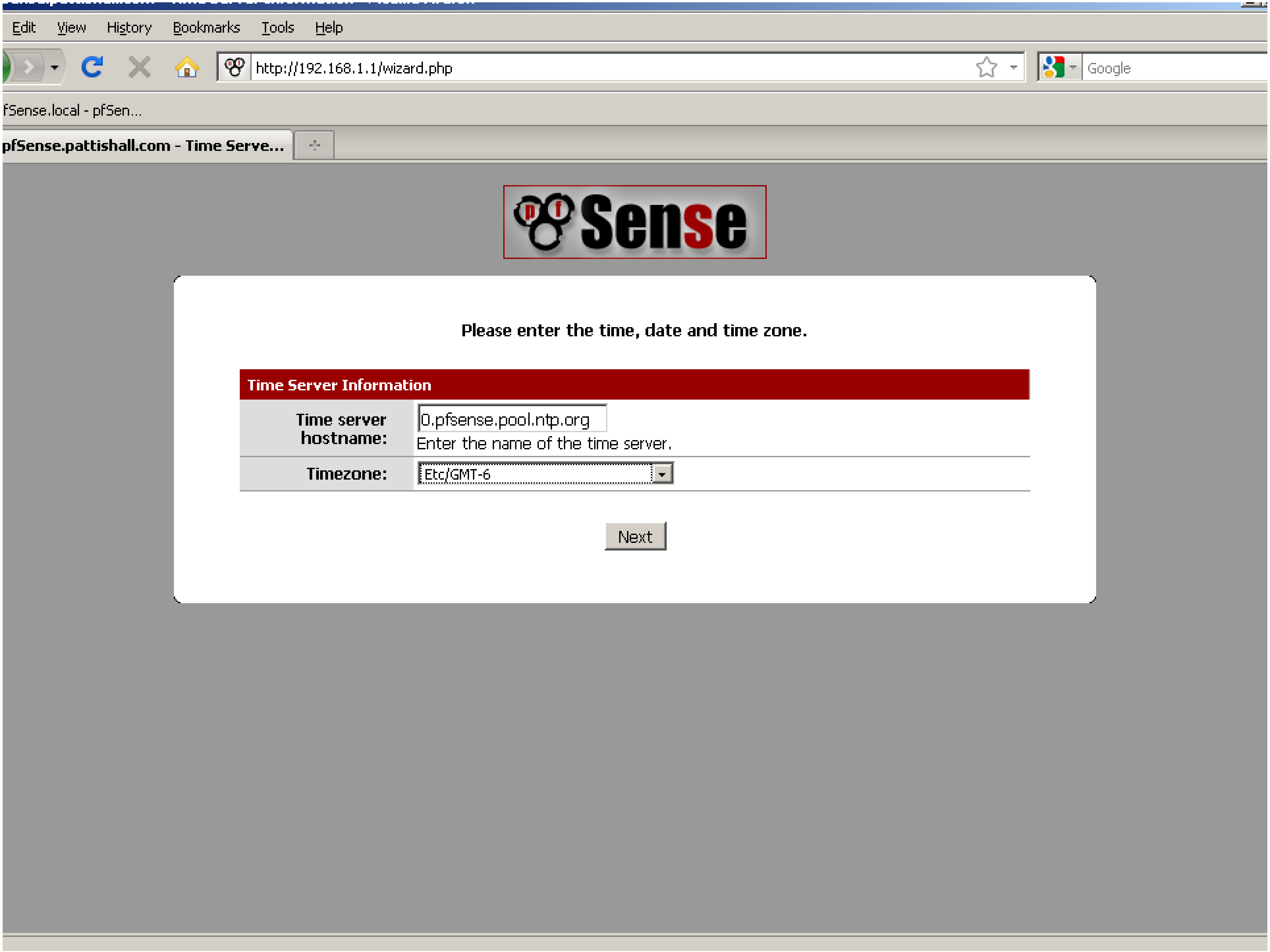
General Information	
Hostname:	pfSense EXAMPLE: myserver
Domain:	local EXAMPLE: mydomain.com
Primary DNS Server:	
Secondary DNS Server:	



On this screen you will set the General pfSense parameters.

General Information

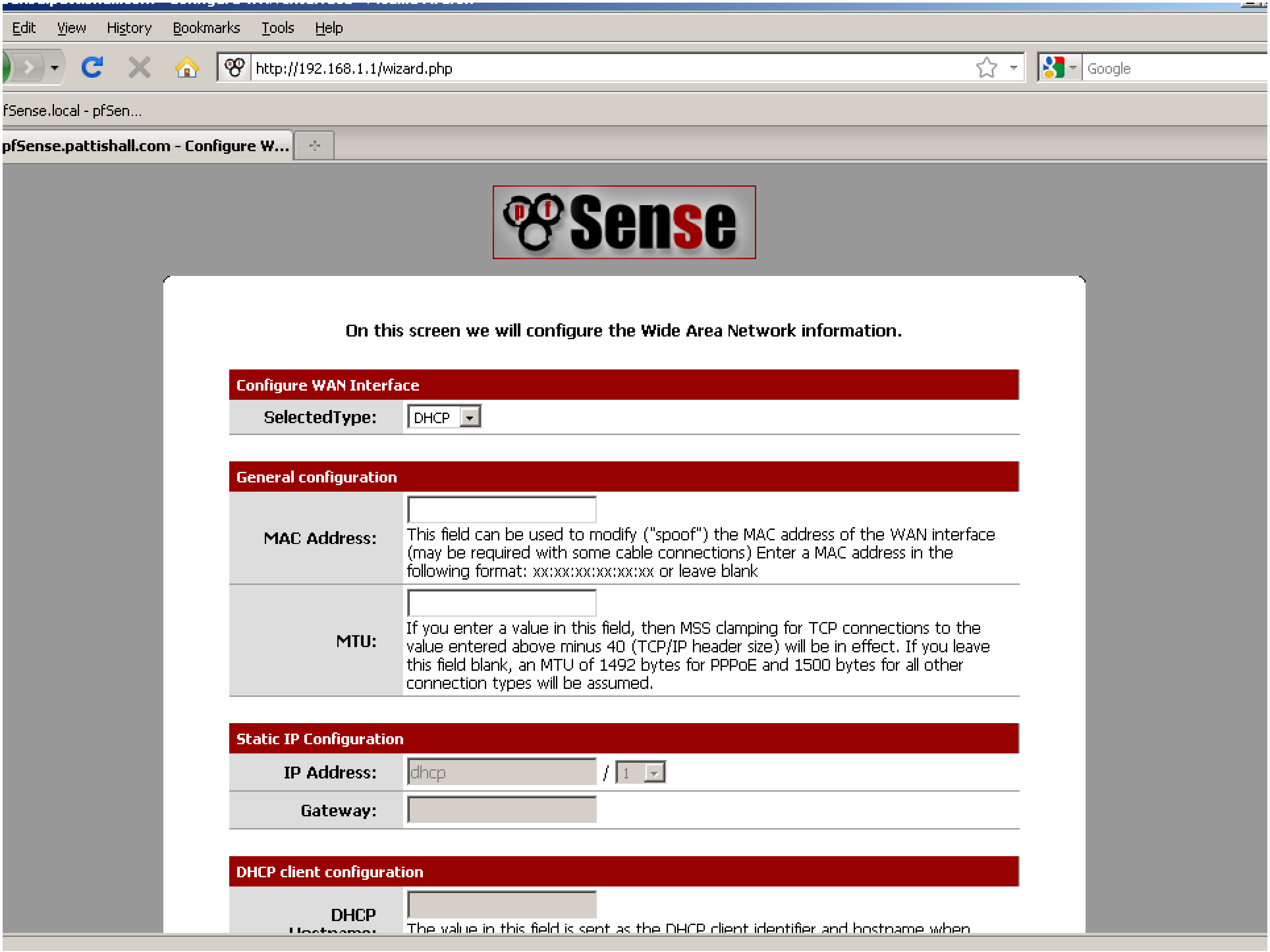
Hostname:	pfSense EXAMPLE: myserver
Domain:	pattishall.com EXAMPLE: mydomain.com
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	8.8.4.4



http://192.168.1.1/wizard.php

Please enter the time, date and time zone.

Time Server Information	
Time server hostname:	0.pfsense.pool.ntp.org Enter the name of the time server.
Timezone:	Etc/GMT-6



On this screen we will configure the Wide Area Network information.

Configure WAN Interface

SelectedType: DHCP

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU:

If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP Configuration

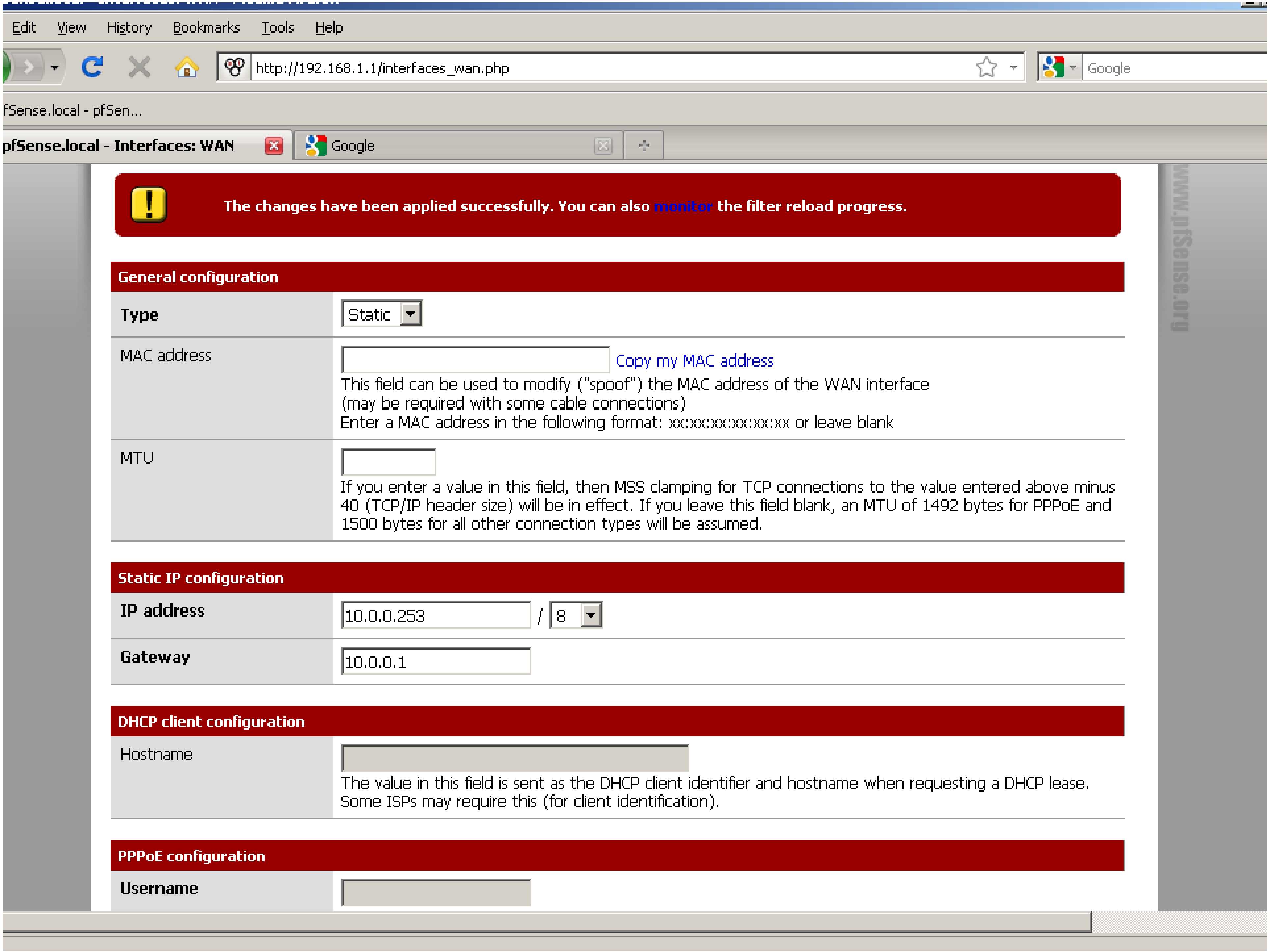
IP Address: dhcp / 1

Gateway:

DHCP client configuration

DHCP Hostname:

The value in this field is sent as the DHCP client identifier and hostname when



The changes have been applied successfully. You can also monitor the filter reload progress.

General configuration

Type	Static
MAC address	Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP configuration

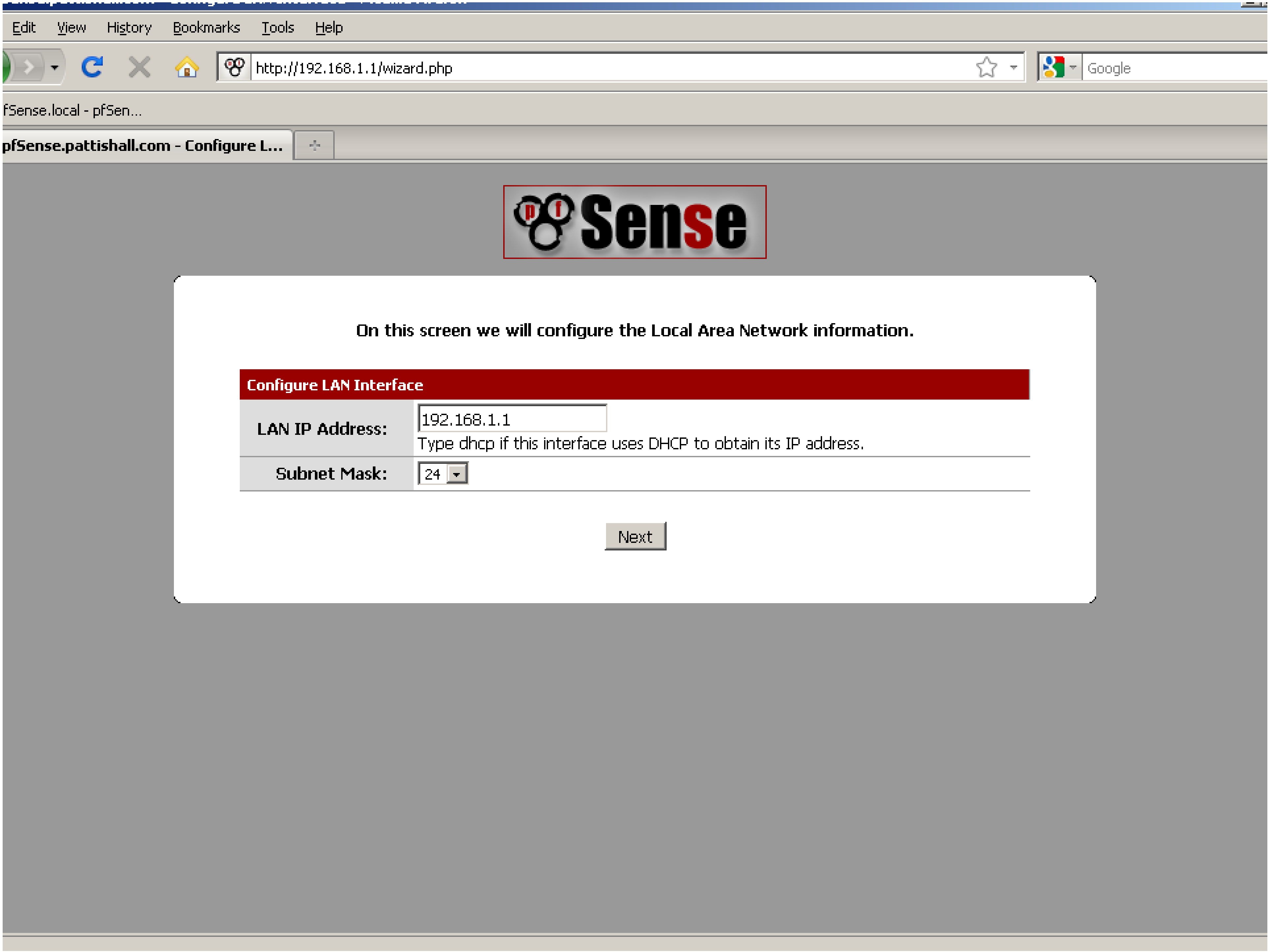
IP address	10.0.0.253 / 8
Gateway	10.0.0.1

DHCP client configuration

Hostname	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

Username	



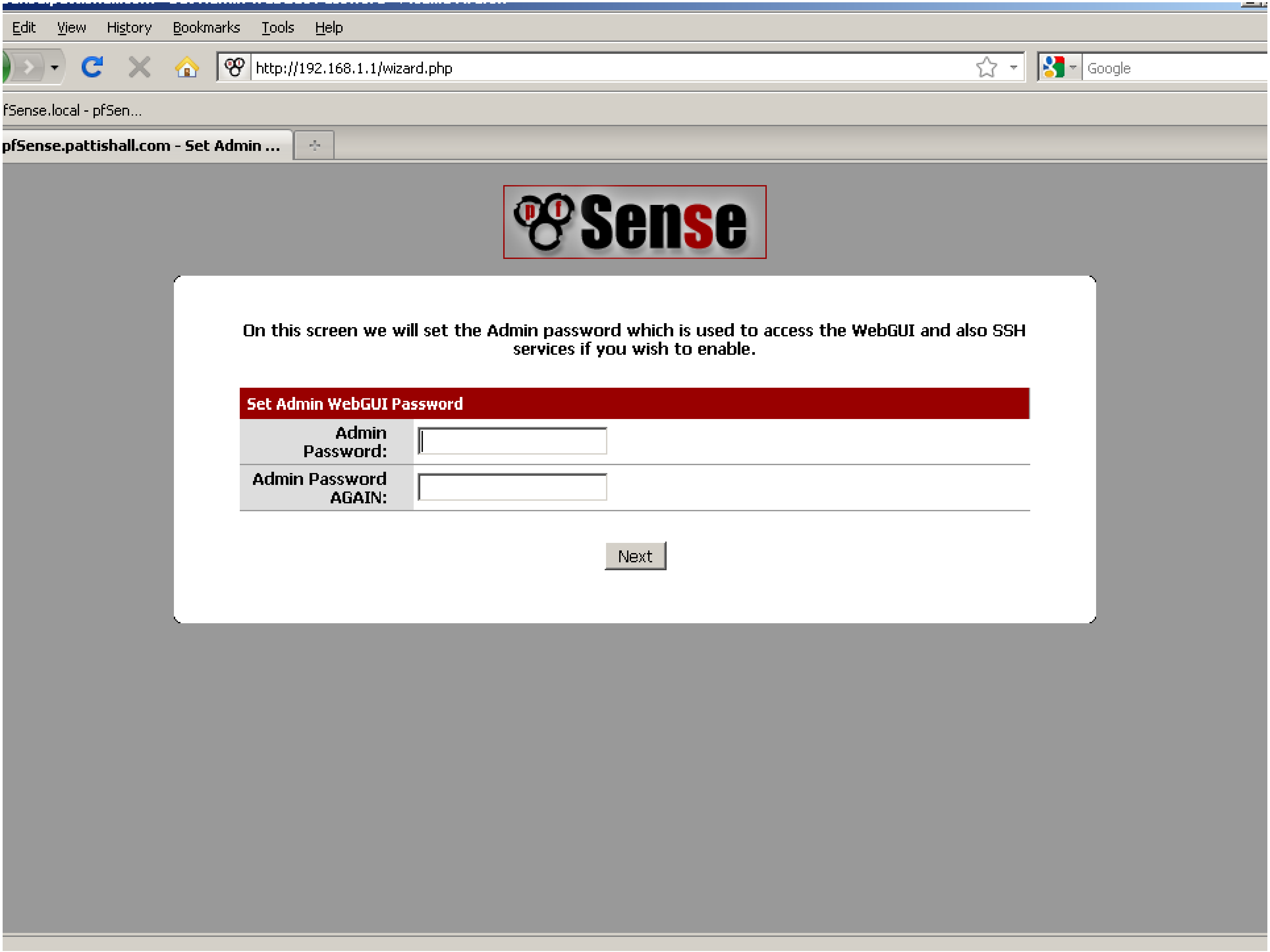
http://192.168.1.1/wizard.php

On this screen we will configure the Local Area Network information.

Configure LAN Interface

LAN IP Address:	192.168.1.1 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask:	24

Next


Edit View History Bookmarks Tools Help
http://192.168.1.1/wizard.php
Google
fSense.local - pfSen...
pfSense.pattishall.com - Set Admin ...
Sense

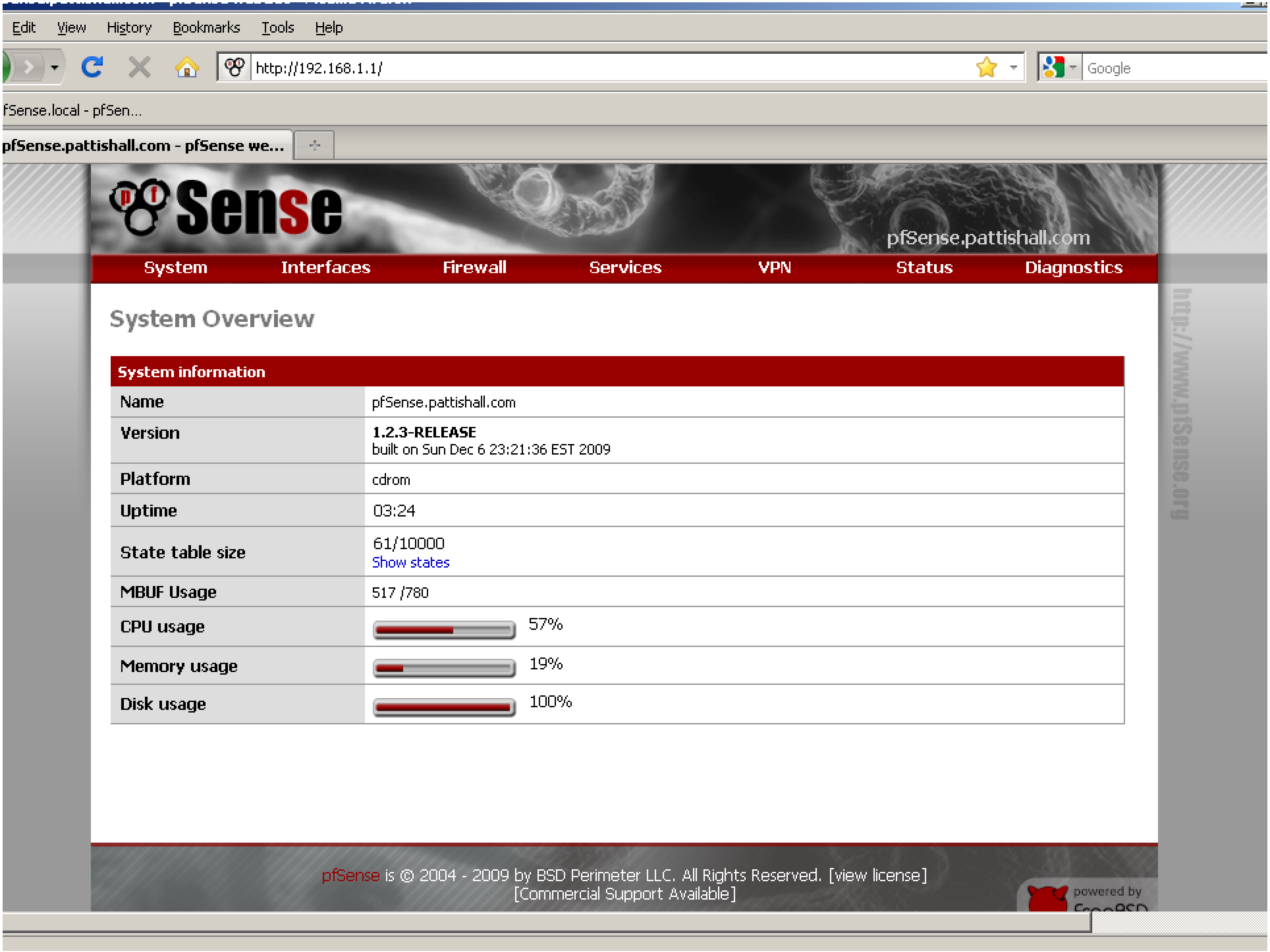
On this screen we will set the Admin password which is used to access the WebGUI and also SSH services if you wish to enable.

Set Admin WebGUI Password

Admin Password:	
Admin Password AGAIN:	

Next

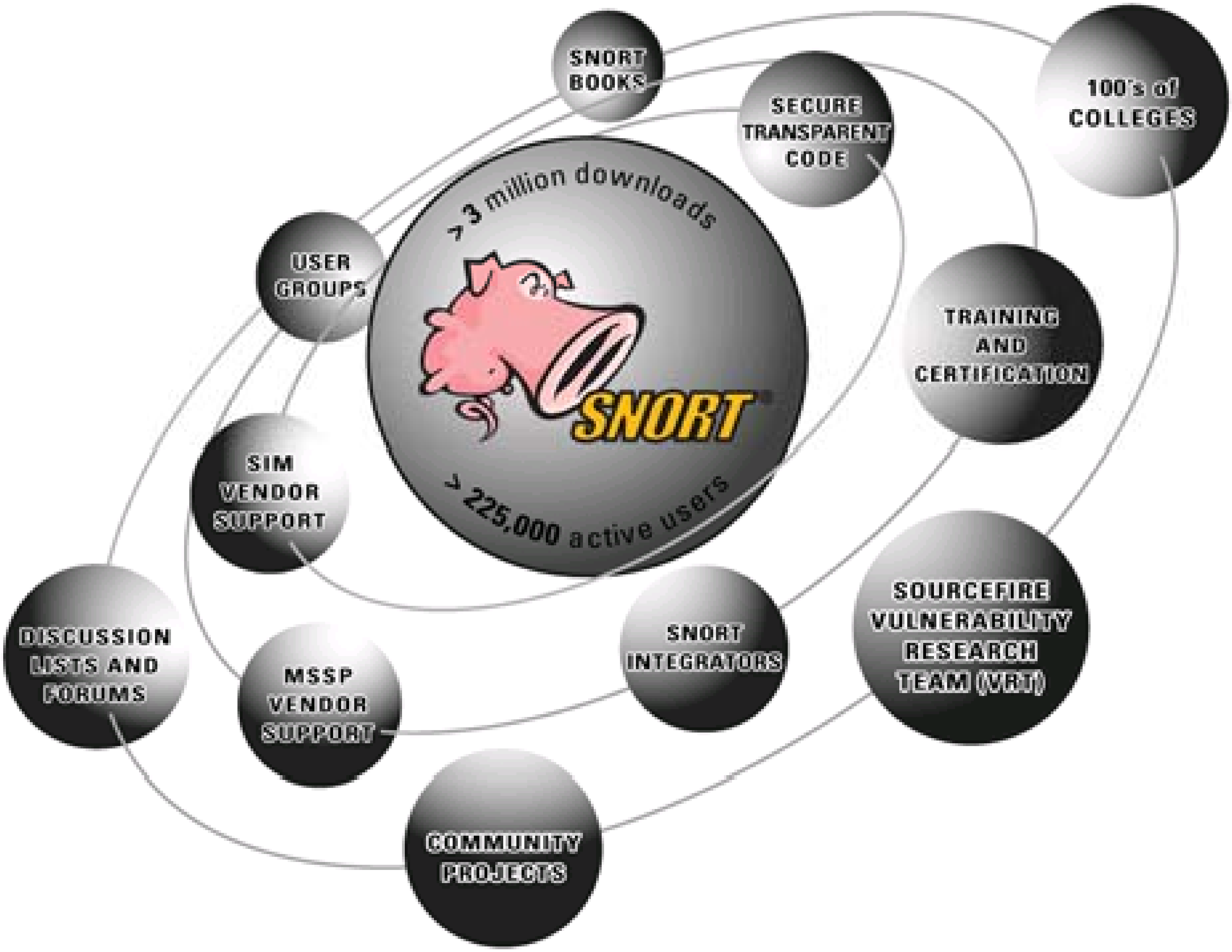
pfsense

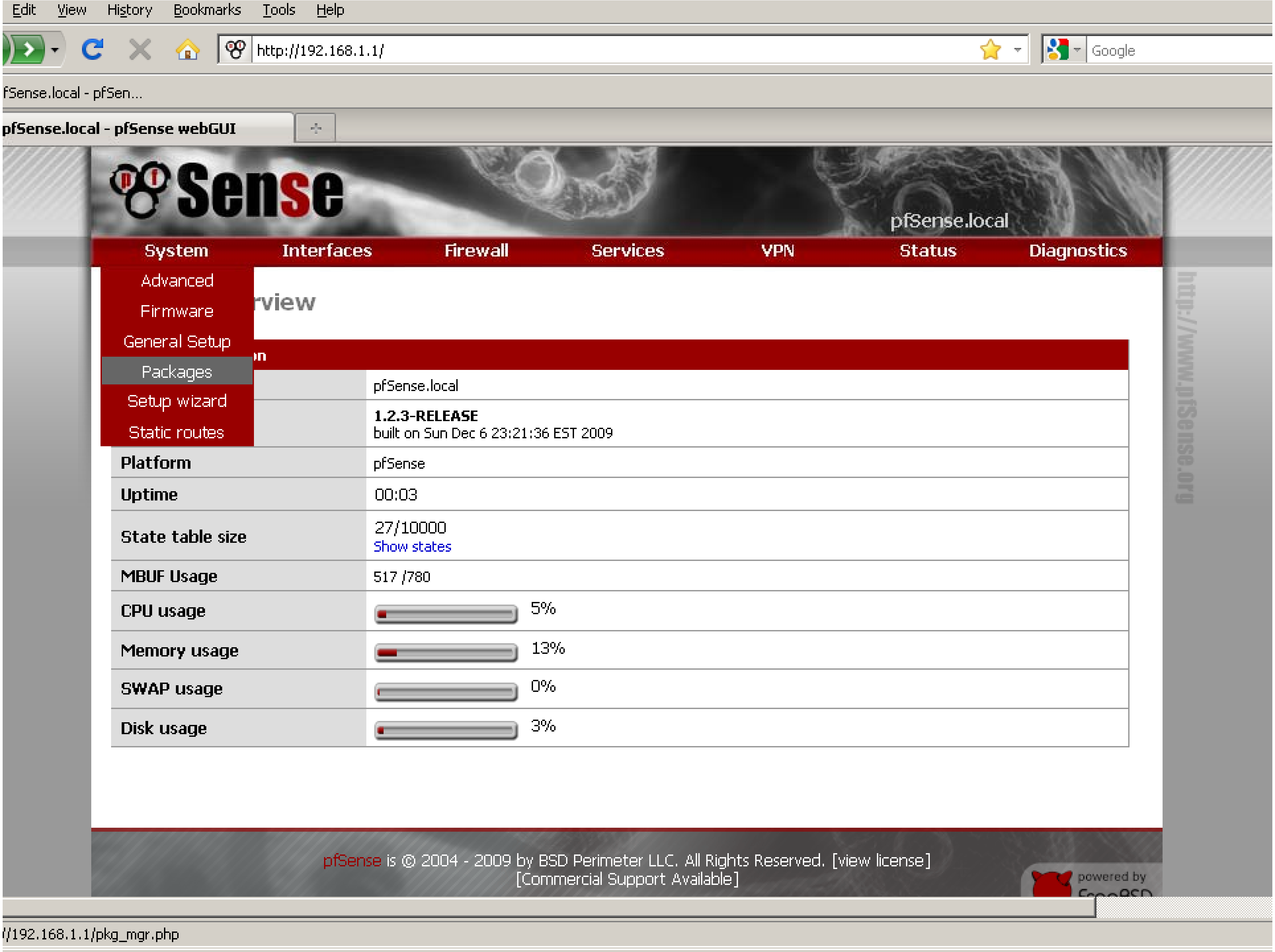


System Overview

System information	
Name	pfSense.pattishall.com
Version	**1.2.3-RELEASE** built on Sun Dec 6 23:21:36 EST 2009
Platform	cdrom
Uptime	03:24
State table size	61/10000 Show states
MBUF Usage	517 /780
CPU usage	57%
Memory usage	19%
Disk usage	100%

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]


> 3 million downloads
SNORT
> 225,000 active users
SNORT BOOKS
SECURE TRANSPARENT CODE
100's of COLLEGES
USER GROUPS
TRAINING AND CERTIFICATION
SIM VENDOR SUPPORT
DISCUSSION LISTS AND FORUMS
MSSP VENDOR SUPPORT
SNORT INTEGRATORS
SOURCEFIRE VULNERABILITY RESEARCH TEAM (VRT)
COMMUNITY PROJECTS



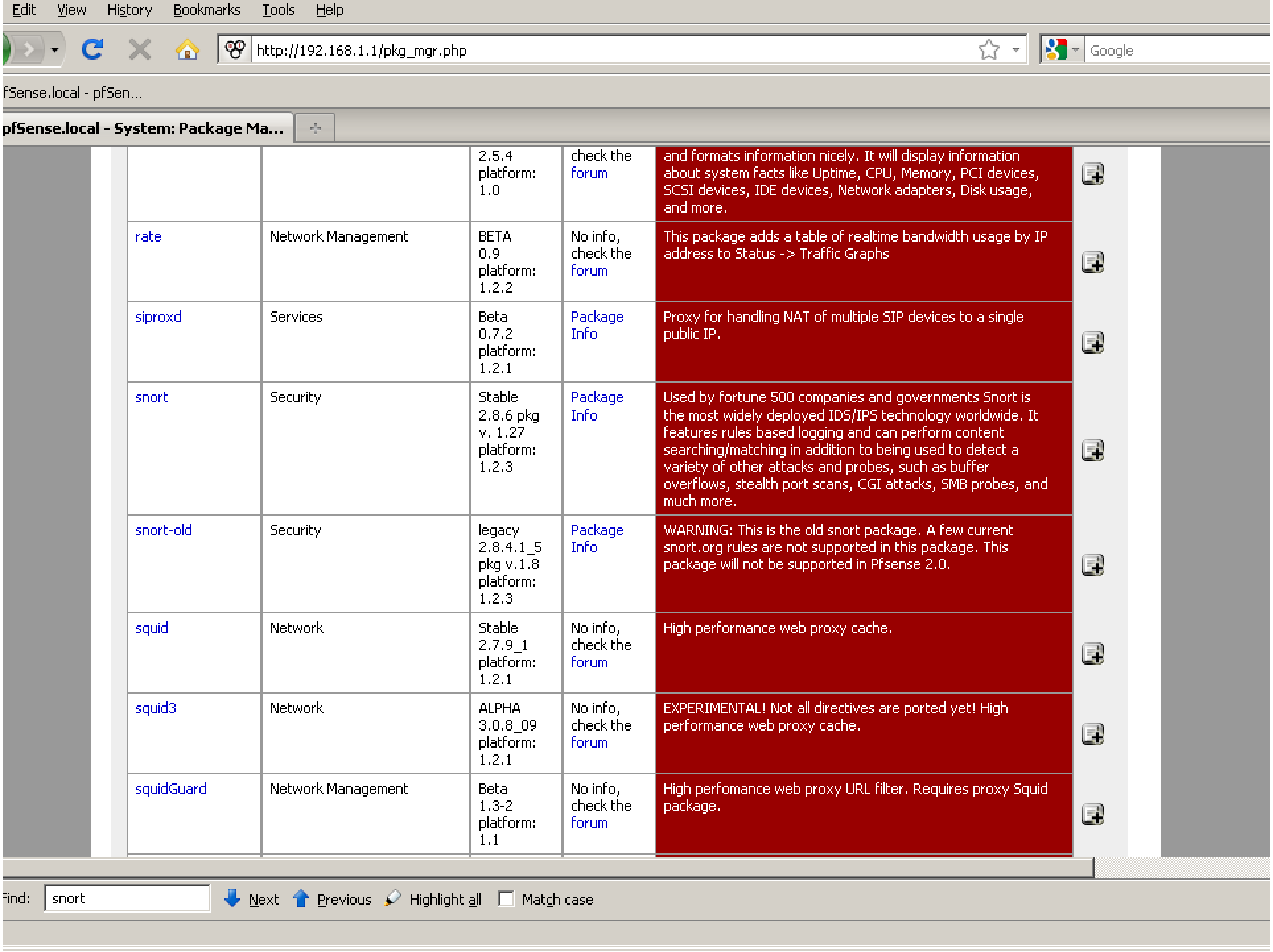
rview

n

	pfSense.local
	1.2.3-RELEASE built on Sun Dec 6 23:21:36 EST 2009
Platform	pfSense
Uptime	00:03
State table size	27/10000 Show states
MBUF Usage	517 /780
CPU usage	5%
Memory usage	13%
SWAP usage	0%
Disk usage	3%

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

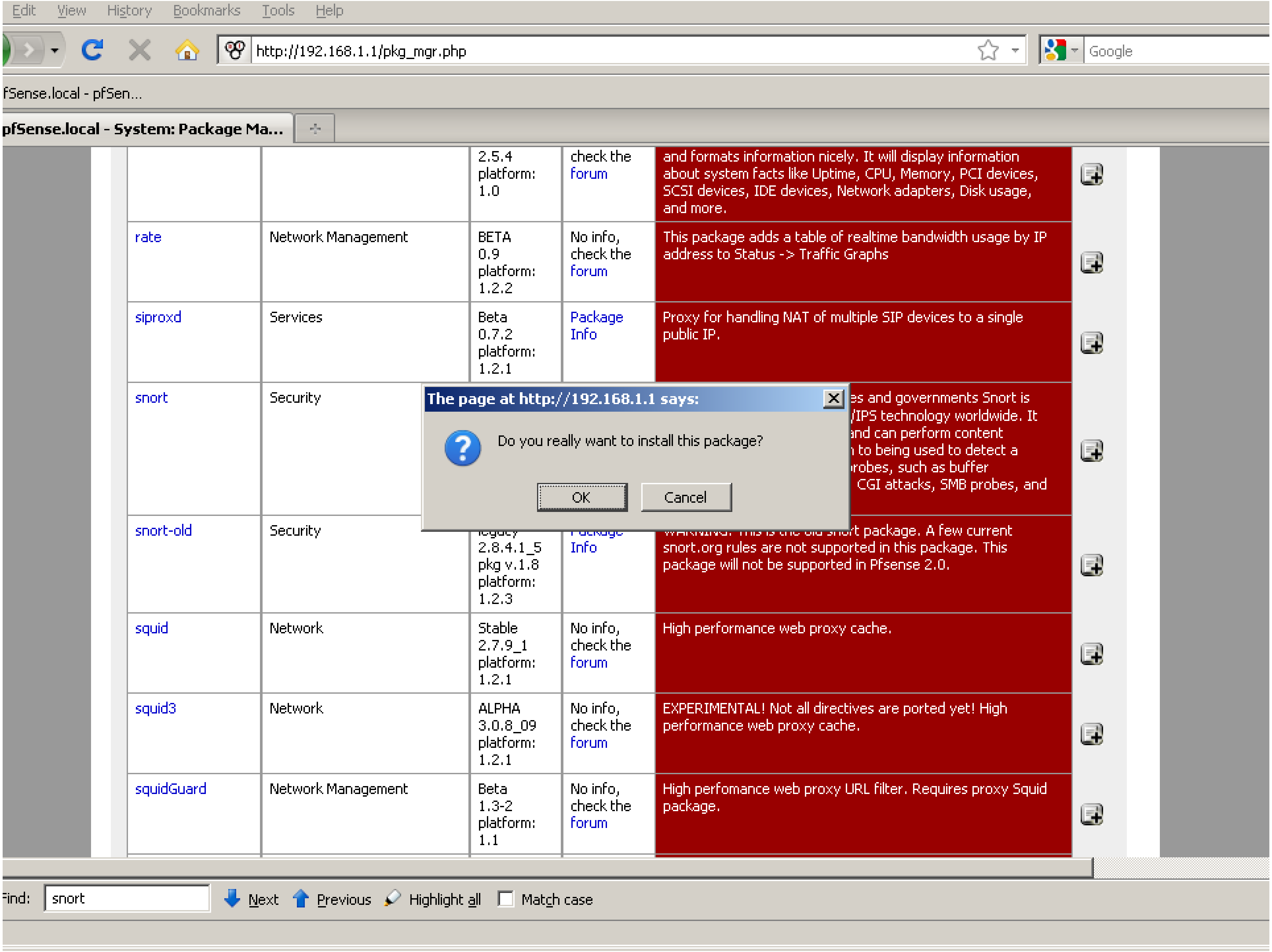
//192.168.1.1/pkg_mgr.php



http://192.168.1.1/pkg_mgr.php

		2.5.4 platform: 1.0	check the forum	and formats information nicely. It will display information about system facts like Uptime, CPU, Memory, PCI devices, SCSI devices, IDE devices, Network adapters, Disk usage, and more.	⊞
rate	Network Management	BETA 0.9 platform: 1.2.2	No info, check the forum	This package adds a table of realtime bandwidth usage by IP address to Status -> Traffic Graphs	⊞
siproxd	Services	Beta 0.7.2 platform: 1.2.1	Package Info	Proxy for handling NAT of multiple SIP devices to a single public IP.	⊞
snort	Security	Stable 2.8.6 pkg v. 1.27 platform: 1.2.3	Package Info	Used by fortune 500 companies and governments Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.	⊞
snort-old	Security	legacy 2.8.4.1_5 pkg v.1.8 platform: 1.2.3	Package Info	WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in Pfsense 2.0.	⊞
squid	Network	Stable 2.7.9_1 platform: 1.2.1	No info, check the forum	High performance web proxy cache.	⊞
squid3	Network	ALPHA 3.0.8_09 platform: 1.2.1	No info, check the forum	EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.	⊞
squidGuard	Network Management	Beta 1.3-2 platform: 1.1	No info, check the forum	High perfomance web proxy URL filter. Requires proxy Squid package.	⊞

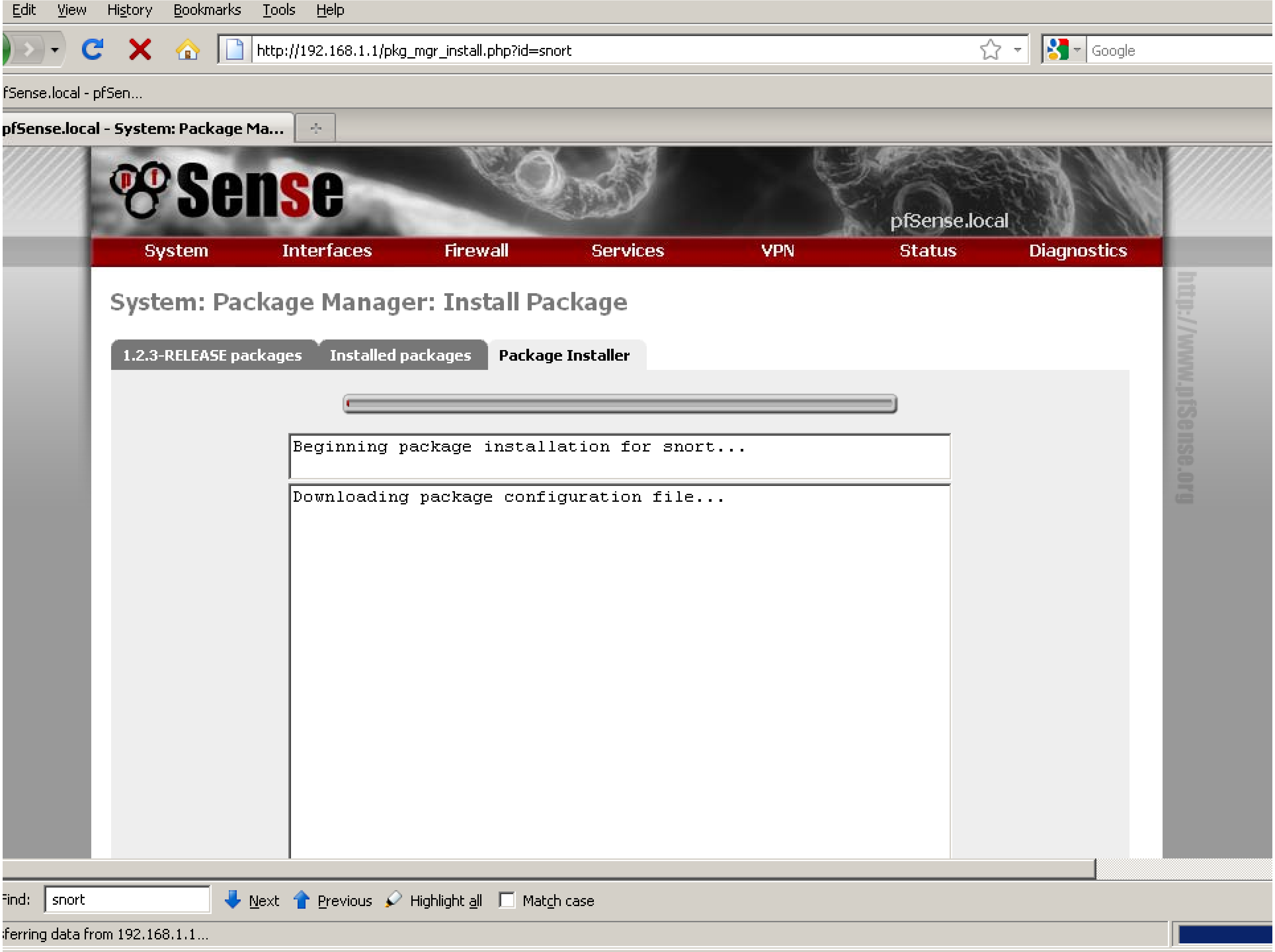
Find: snort


Edit
View
History
Bookmarks
Tools
Help
http://192.168.1.1/pkg_mgr.php
Google
fSense.local - pfSen...
pfSense.local - System: Package Ma...

The page at http://192.168.1.1 says:

Do you really want to install this package?

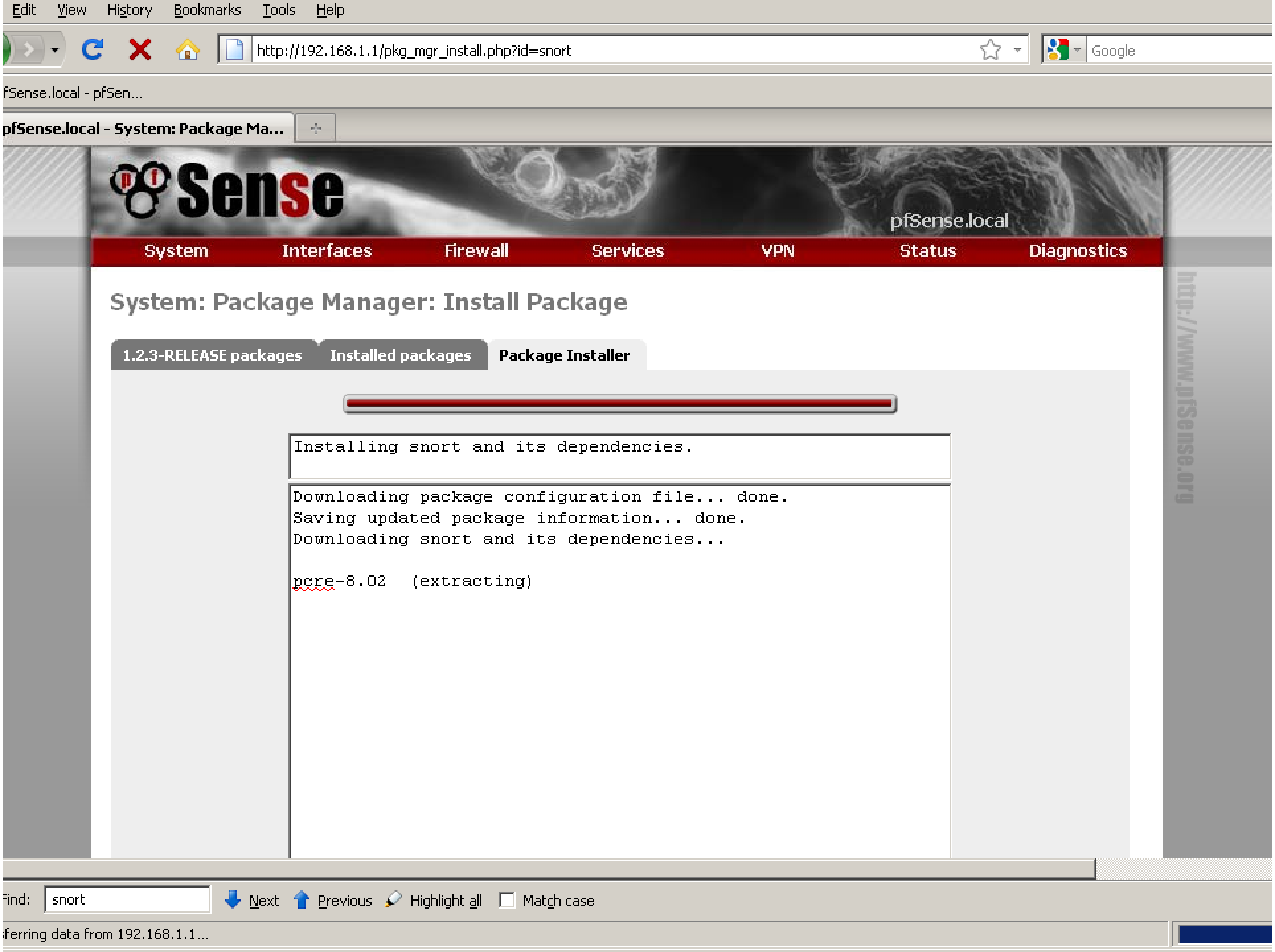
		2.5.4 platform: 1.0	check the forum	and formats information nicely. It will display information about system facts like Uptime, CPU, Memory, PCI devices, SCSI devices, IDE devices, Network adapters, Disk usage, and more.
rate	Network Management	BETA 0.9 platform: 1.2.2	No info, check the forum	This package adds a table of realtime bandwidth usage by IP address to Status -> Traffic Graphs
siproxd	Services	Beta 0.7.2 platform: 1.2.1	Package Info	Proxy for handling NAT of multiple SIP devices to a single public IP.
snort	Security			es and governments Snort is /IPS technology worldwide. It nd can perform content to being used to detect a robes, such as buffer CGI attacks, SMB probes, and
snort-old	Security	legacy 2.8.4.1_5 pkg v.1.8 platform: 1.2.3	Package Info	WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in Pfsense 2.0.
squid	Network	Stable 2.7.9_1 platform: 1.2.1	No info, check the forum	High performance web proxy cache.
squid3	Network	ALPHA 3.0.8_09 platform: 1.2.1	No info, check the forum	EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.
squidGuard	Network Management	Beta 1.3-2 platform: 1.1	No info, check the forum	High perfomance web proxy URL filter. Requires proxy Squid package.


Edit View History Bookmarks Tools Help
http://192.168.1.1/pkg_mgr_install.php?id=snort
Google
fSense.local - pfSen...
pfSense.local - System: Package Ma...
Sense
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
http://www.pfSense.org

System: Package Manager: Install Package

```
Beginning package installation for snort...
```

```
Downloading package configuration file...
```

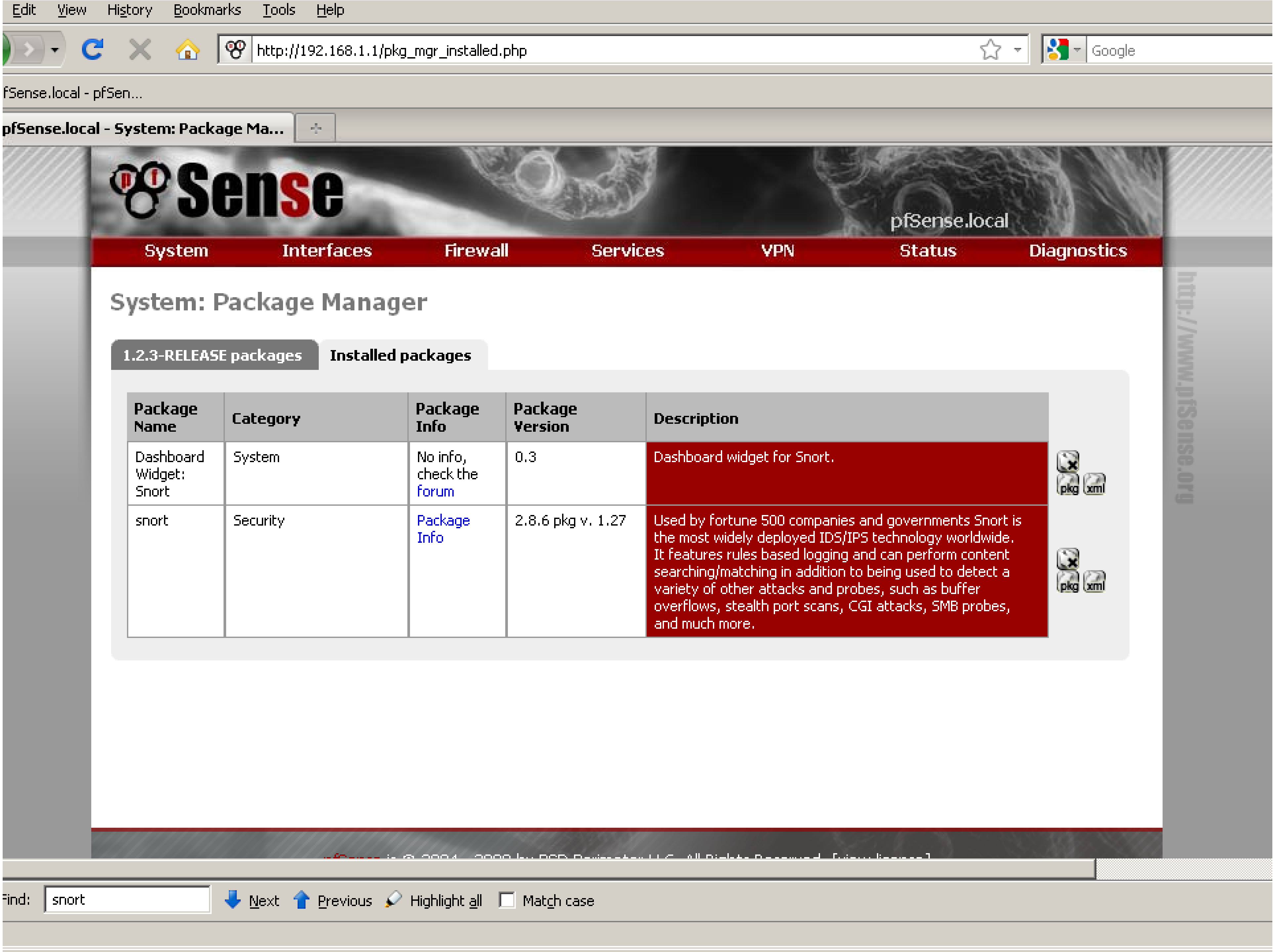


Edit View History Bookmarks Tools Help
http://192.168.1.1/pkg_mgr_install.php?id=snort
Google
fSense.local - pfSen...
pfSense.local - System: Package Ma...
Sense
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
http://www.pfSense.org

System: Package Manager: Install Package

```
Installing snort and its dependencies.
```

```
Downloading package configuration file... done.
Saving updated package information... done.
Downloading snort and its dependencies...

pcre-8.02  (extracting)
```

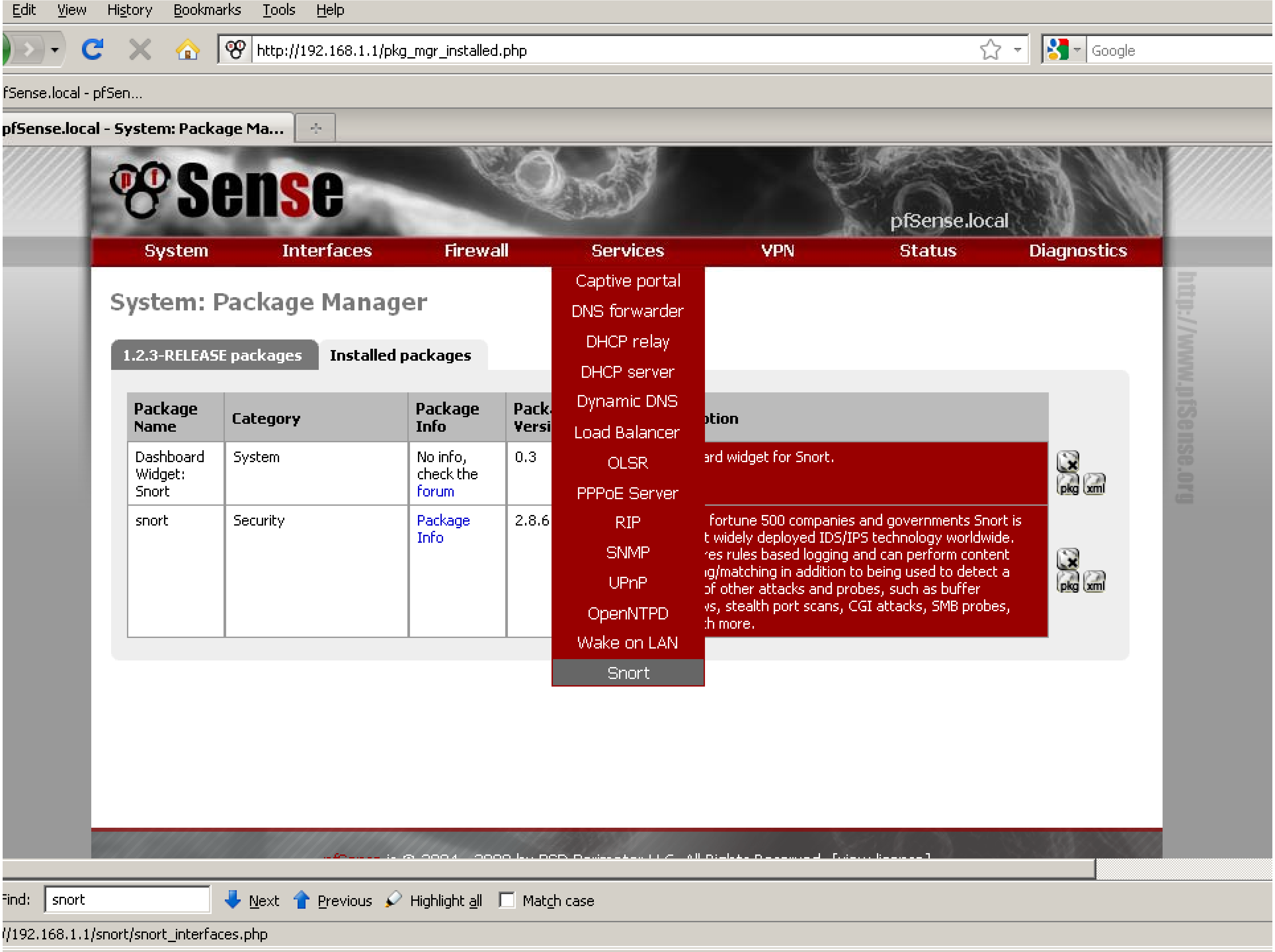


System: Package Manager

1.2.3-RELEASE packages | Installed packages

Package Name	Category	Package Info	Package Version	Description	
Dashboard Widget: Snort	System	No info, check the forum	0.3	Dashboard widget for Snort.	pkg xml
snort	Security	Package Info	2.8.6 pkg v. 1.27	Used by fortune 500 companies and governments Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.	pkg xml

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]



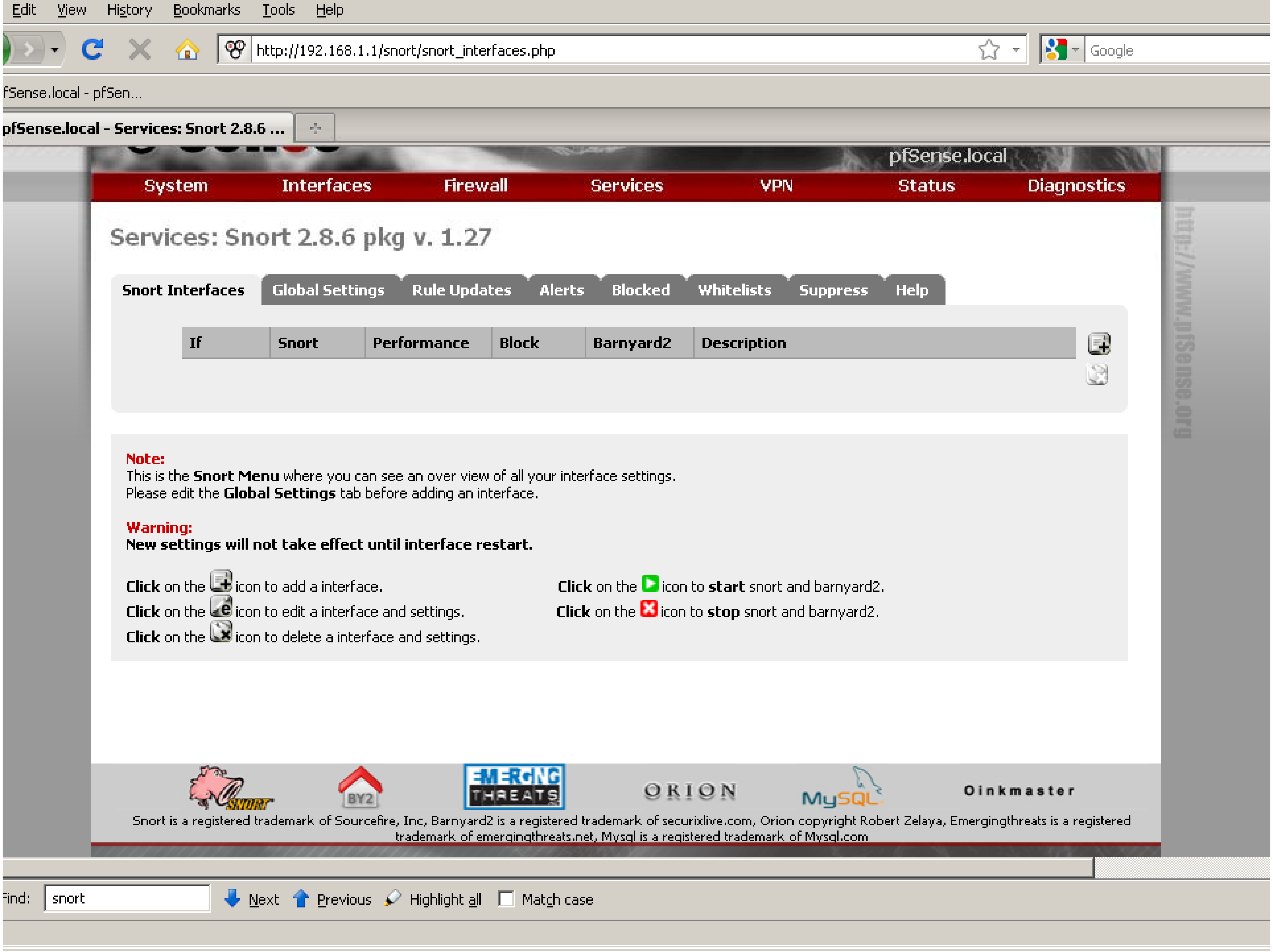
System: Package Manager

Package Name	Category	Package Info	Pack. Versi	ption
Dashboard Widget: Snort	System	No info, check the forum	0.3	ard widget for Snort.
snort	Security	Package Info	2.8.6	fortune 500 companies and governments Snort is t widely deployed IDS/IPS technology worldwide. res rules based logging and can perform content g/matching in addition to being used to detect a of other attacks and probes, such as buffer ws, stealth port scans, CGI attacks, SMB probes, h more.

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]

Find: snort Next Previous Highlight all □ Match case

//192.168.1.1/snort/snort_interfaces.php



Services: Snort 2.8.6 pkg v. 1.27

If	Snort	Performance	Block	Barnyard2	Description

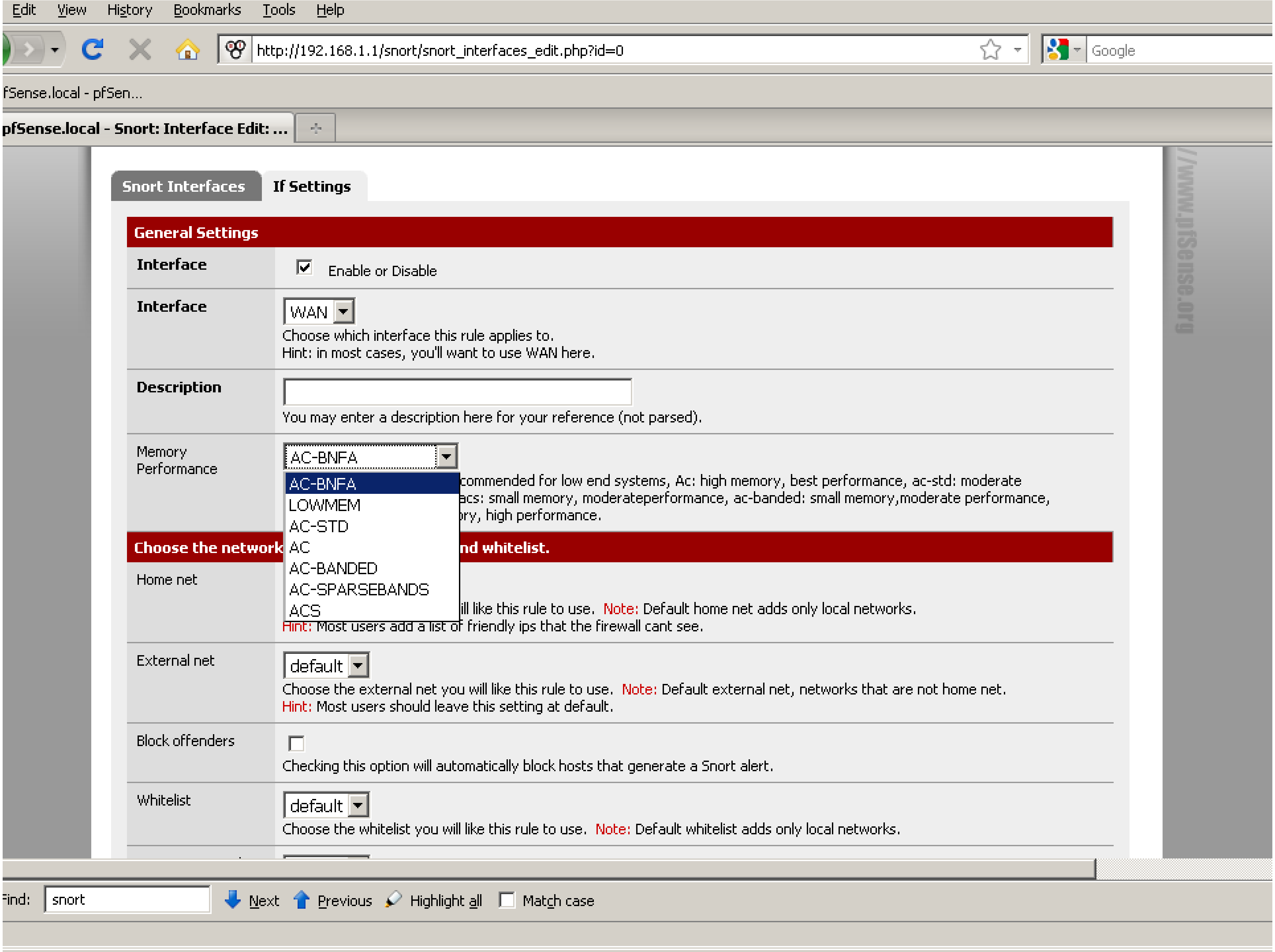
Note:
This is the **Snort Menu** where you can see an over view of all your interface settings.
Please edit the **Global Settings** tab before adding an interface.

Warning:
New settings will not take effect until interface restart.

Click on the ⊞ icon to add a interface.
Click on the ⓔ icon to edit a interface and settings.
Click on the ☒ icon to delete a interface and settings.

Click on the ▶ icon to **start** snort and barnyard2.
Click on the ☒ icon to **stop** snort and barnyard2.

Snort is a registered trademark of Sourcefire, Inc, Barnyard2 is a registered trademark of securixlive.com, Orion copyright Robert Zelaya, Emergingthreats is a registered trademark of emergingthreats.net, Mysql is a registered trademark of Mysql.com



Snort Interfaces | If Settings

General Settings

Interface ☑ Enable or Disable

Interface WAN

Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Description

You may enter a description here for your reference (not parsed).

Memory Performance AC-BNFA

AC-BNFA
LOWMEM
AC-STD
AC
AC-BANDED
AC-SPARSEBANDS
ACS

commended for low end systems, Ac: high memory, best performance, ac-std: moderate
acs: small memory, moderateperformance, ac-banded: small memory,moderate performance,
ory, high performance.

Choose the network **nd whitelist.**

Home net

ill like this rule to use. Note: Default home net adds only local networks.
Hint: Most users add a list of friendly ips that the firewall cant see.

External net default

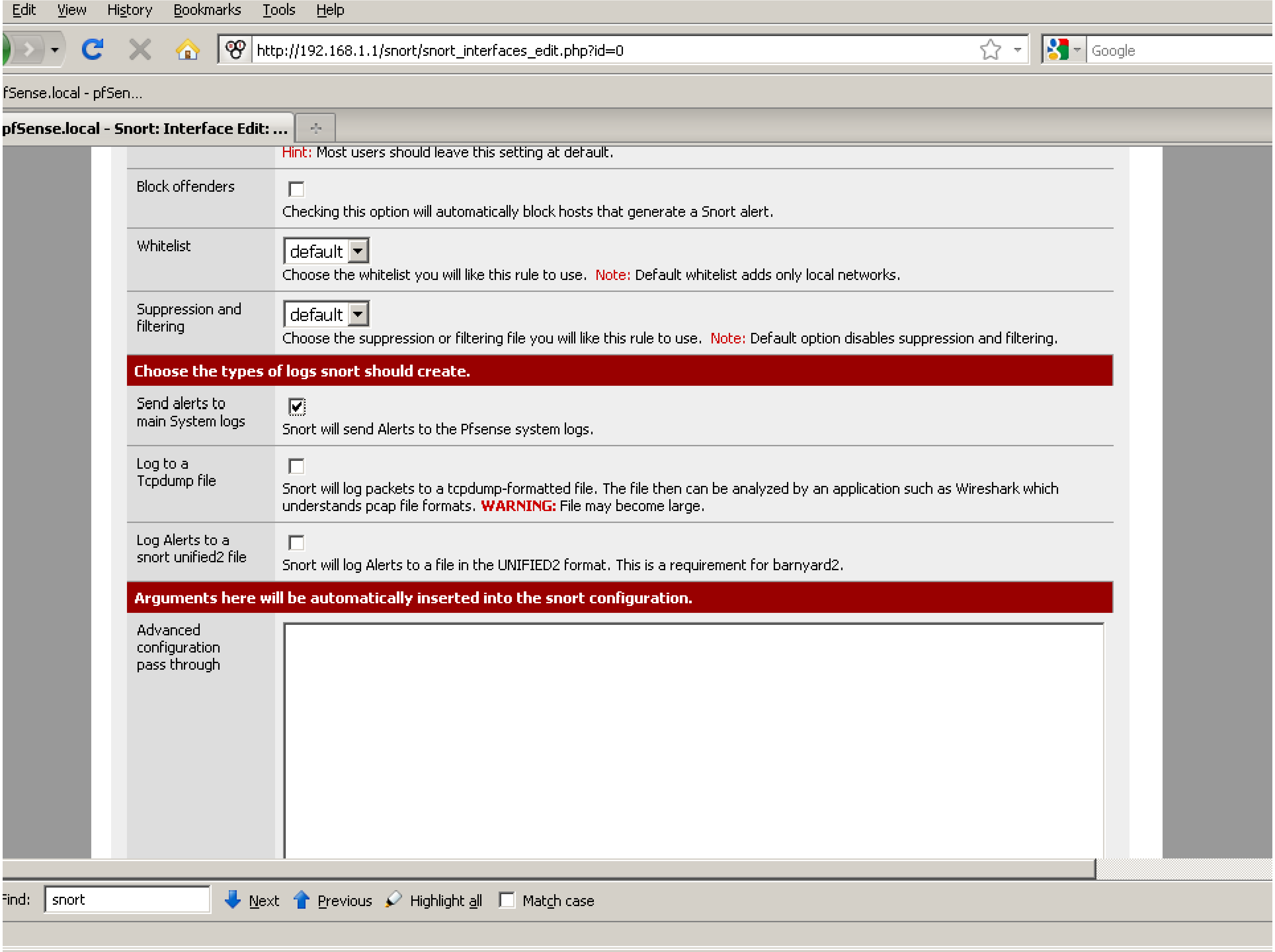
Choose the external net you will like this rule to use. Note: Default external net, networks that are not home net.
Hint: Most users should leave this setting at default.

Block offenders □

Checking this option will automatically block hosts that generate a Snort alert.

Whitelist default

Choose the whitelist you will like this rule to use. Note: Default whitelist adds only local networks.



Edit View History Bookmarks Tools Help
http://192.168.1.1/snort/snort_interfaces_edit.php?id=0
Google
fSense.local - pfSen...
pfSense.local - Snort: Interface Edit: ...

Hint: Most users should leave this setting at default.

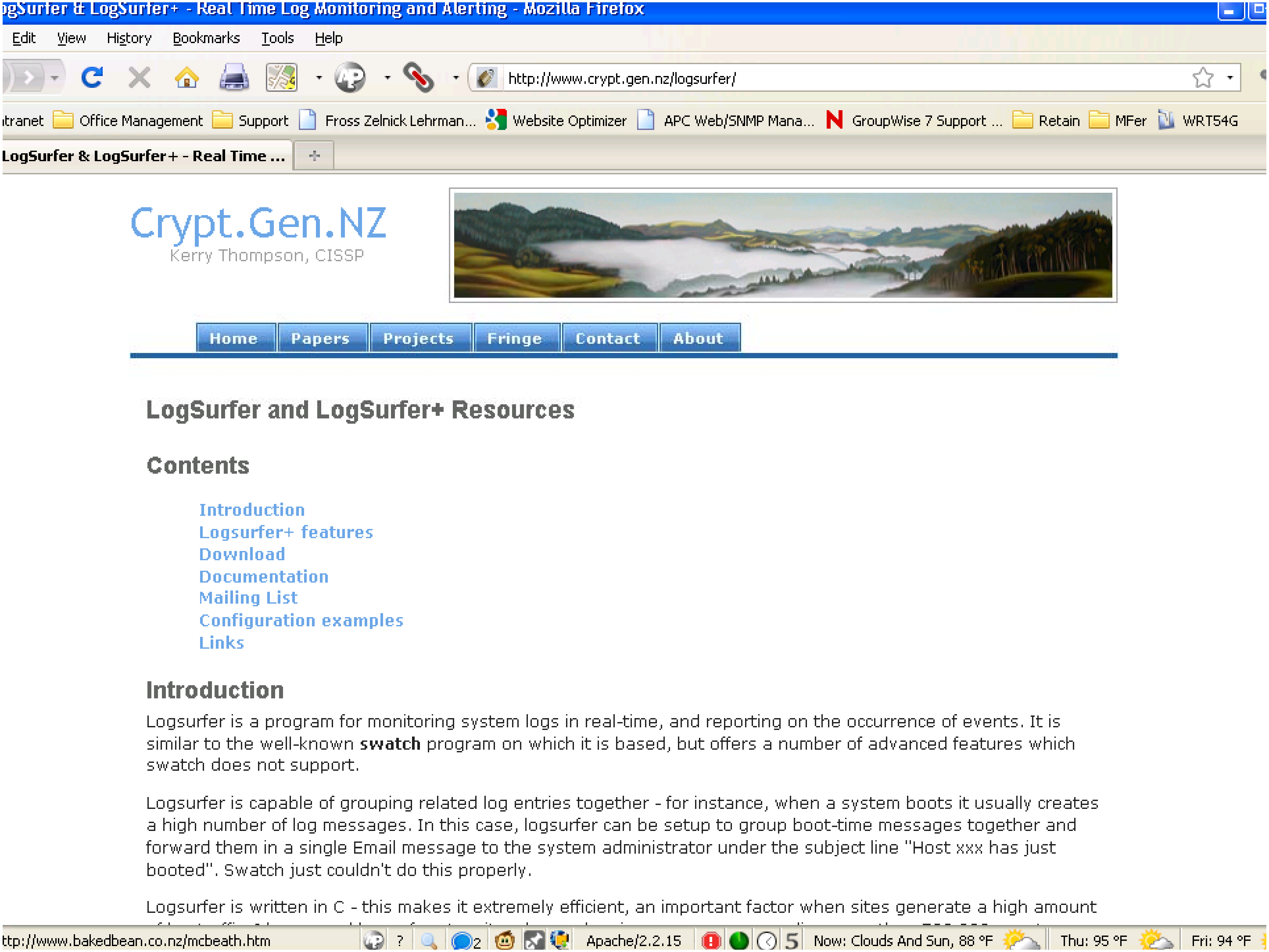
Block offenders	□ Checking this option will automatically block hosts that generate a Snort alert.
Whitelist	default Choose the whitelist you will like this rule to use. Note: Default whitelist adds only local networks.
Suppression and filtering	default Choose the suppression or filtering file you will like this rule to use. Note: Default option disables suppression and filtering.

Choose the types of logs snort should create.

Send alerts to main System logs	☑ Snort will send Alerts to the Pfsense system logs.
Log to a Tcpdump file	□ Snort will log packets to a tcpdump-formatted file. The file then can be analyzed by an application such as Wireshark which understands pcap file formats. **WARNING:** File may become large.
Log Alerts to a snort unified2 file	□ Snort will log Alerts to a file in the UNIFIED2 format. This is a requirement for barnyard2.

Arguments here will be automatically inserted into the snort configuration.

Advanced configuration pass through


ogSurfer & LogSurfer+ - Real Time Log Monitoring and Alerting - Mozilla Firefox
Edit View History Bookmarks Tools Help
http://www.crypt.gen.nz/logsurfer/
tranet Office Management Support Fross Zelnick Lehrman... Website Optimizer APC Web/SNMP Mana... GroupWise 7 Support ... Retain MFer WRT54G
LogSurfer & LogSurfer+ - Real Time ...
Crypt.Gen.NZ
Kerry Thompson, CISSP
Home Papers Projects Fringe Contact About
ttp://www.bakedbean.co.nz/mcbeath.htm ? 2 Apache/2.2.15 5 Now: Clouds And Sun, 88 °F Thu: 95 °F Fri: 94 °F

LogSurfer and LogSurfer+ Resources

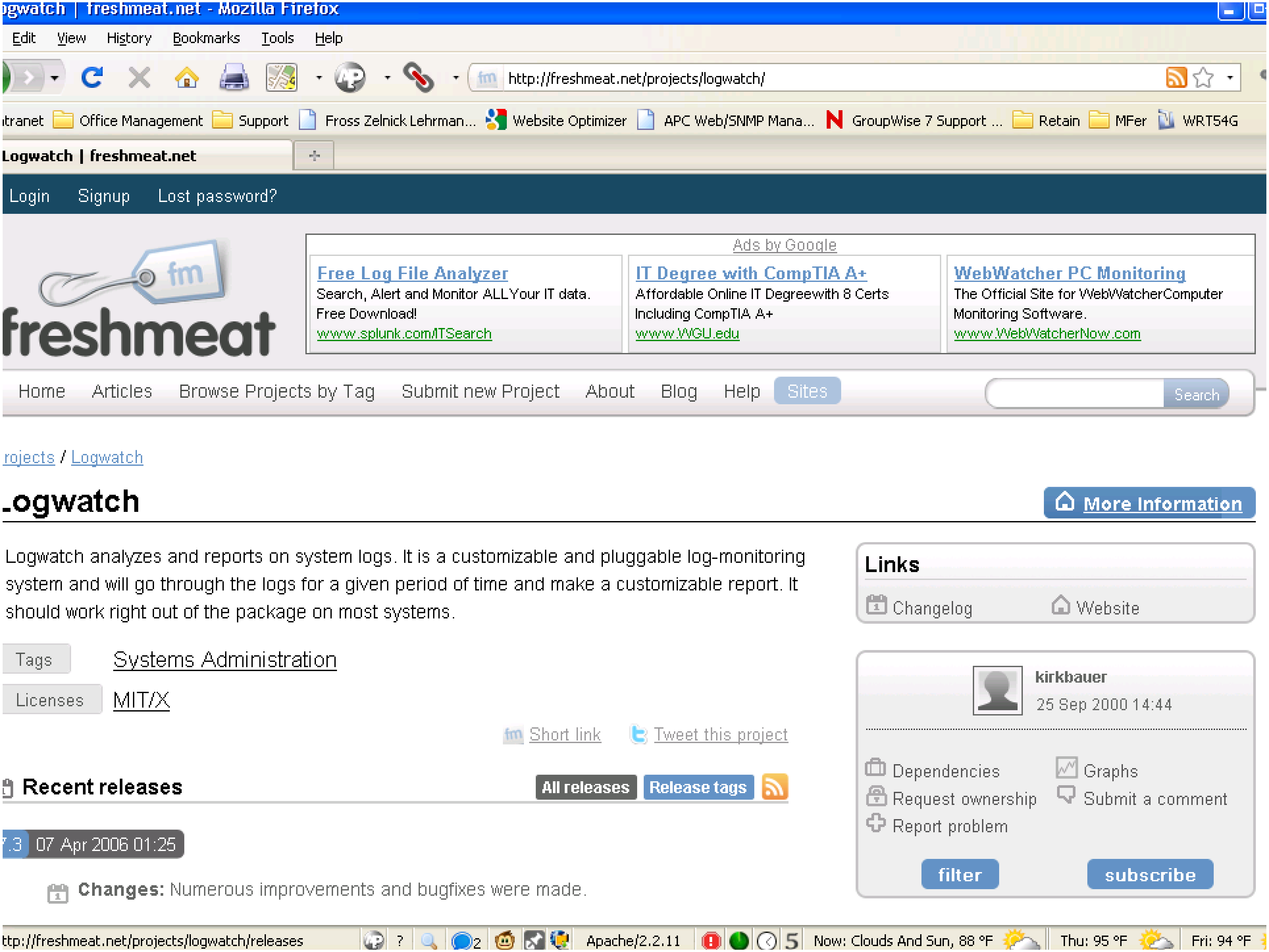
Contents

Introduction

Logsurfer is a program for monitoring system logs in real-time, and reporting on the occurrence of events. It is similar to the well-known **swatch** program on which it is based, but offers a number of advanced features which swatch does not support.

Logsurfer is capable of grouping related log entries together - for instance, when a system boots it usually creates a high number of log messages. In this case, logsurfer can be setup to group boot-time messages together and forward them in a single Email message to the system administrator under the subject line "Host xxx has just booted". Swatch just couldn't do this properly.

Logsurfer is written in C - this makes it extremely efficient, an important factor when sites generate a high amount


ogwatch | freshmeat.net - Mozilla Firefox
Edit View History Bookmarks Tools Help
http://freshmeat.net/projects/logwatch/
tranet Office Management Support Fross Zelnick Lehrman... Website Optimizer APC Web/SNMP Mana... GroupWise 7 Support ... Retain MFer WRT54G
Logwatch | freshmeat.net
Login Signup Lost password?
fm freshmeat
Home Articles Browse Projects by Tag Submit new Project About Blog Help Sites
Search
More Information
Short link
Tweet this project
All releases
Release tags
filter
subscribe
ttp://freshmeat.net/projects/logwatch/releases
Apache/2.2.11
5
Now: Clouds And Sun, 88 °F
Thu: 95 °F
Fri: 94 °F

rojects / Logwatch

.ogwatch

Logwatch analyzes and reports on system logs. It is a customizable and pluggable log-monitoring system and will go through the logs for a given period of time and make a customizable report. It should work right out of the package on most systems.

Tags	Systems Administration
Licenses	MIT/X

Links

Changelog Website

kirkbauer
25 Sep 2000 14:44

Dependencies Graphs
Request ownership Submit a comment
Report problem

Recent releases

.3 07 Apr 2006 01:25

Changes: Numerous improvements and bugfixes were made.

Support Options

- Community Forum
- Mailing List
- IRC
- Local Support is available in these areas:
    - Louisville, Kentucky
    - Nashville, Tennessee
    - Southeast Idaho
    - Northern Utah
    - Jackson, Wyoming
    - San Diego, California

Sounds great, but…

- How much does it cost?
  - – Nothing, nada, diddly squat, bupkis. It's FREE!
- Is it secure?
  - – Absolutely! However, a firewalls level of security is based entirely on how YOU configure it.

Paid Support Subscription

The base 5 hour annual subscription is $600 USD. Additional blocks of hours can be purchased if needed, at the following rates (all prices USD).

Additional Hours

Available to customers with an active support subscription

5 hours - $400

10 hours - $750

50 hours - $3500

Thank you!
Questions?