

Tru64 UNIX Best Practice

Configuring FireScreen Using Internet Express

July 2002

Product Version: **Internet Express Version 5.9**

This Best Practice describes how to use the HP Internet Express installation procedure and Administration utility to set up and configure FireScreen for the HP *Tru64*TM UNIX operating system.

Hewlett-Packard Company
Palo Alto, California

Contents

Configuring FireScreen

Is This Best Practice Right for You?	1
Before You Begin	1
Applying the Best Practice	2
Obtain the Internet Express Kit	3
Install the Web Server and Administration Utility	3
Install FireScreen	3
Configure FireScreen	4
Set FireScreen Options	5
Add Screening Rules	5
Setting Screening Mode	6
Manage FireScreen	6
Use FireScreen To Implement TCP/IP Security Policies ...	6
Tune the System to Improve FireScreen Performance	7
Verifying Success	7
Troubleshooting	9
Alternative Practices	11
Comments and Questions	11
Legal Notice	11

Configuring FireScreen

See the Tru64 UNIX Best Practices Web page for more information about Best Practices documentation.

Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that it is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Hardware	An Alpha system acting as an IP router or Internet gateway (two or more network cards)
Operating System	Tru64 UNIX Version 5.0A or higher
Product Version	Internet Express Version 5.9 or higher
Network	IPv4

If you do not meet the previous requirements, see *Alternative Practices* for information.

Before You Begin

Before you apply the Best Practice for installing and configuring FireScreen, you must understand some background information and perform some preliminary tasks to configure the system software.

Internet Express is a collection of popular Open Source and HP software contained on CD-ROM. FireScreen is a component of the Administration utility provided with Internet Express. You can use FireScreen to configure and manage the screening router (or firewall) called `screend`. FireScreen uses screening rules stored in its configuration file to filter routed packets by inhibiting the IP-forwarding functionality built into the kernel. This kernel feature is called the "Gateway packet screening facility". It is described in detail in `screen(2)`.

You can use the `setld` command and a Tru64 UNIX operating system CD-ROM to install a prebuilt `screend` binary. Install the `OSFINETxxx` subset (where `xxx` is the Tru64 UNIX operating system version). The binary is placed in `/usr/sbin/screend`. Reference pages for `screend` can also be installed if you install the `OSFDCFTxxx`, `OSFMANOSxxx`, and `OSFMANOPxxx` subsets.

Note

Do not install the `OSFINETxxx` subset on a system that already has AltaVista Firewall software installed (the `DFWBASExxx` subset, where `xxx` is the AltaVista Firewall product version number). The subsets are incompatible.

If you have not already done so, register the IP address and any IP aliases for the system's interfaces. The system must be configured as an IP router or a gateway. Use the `setup` or `sysman network` commands to run either the `routed` or `gated` daemons; or to configure static routes on the system. Ensure that you are broadcasting RIP packets.

Once you have completed the system software configuration, you must install the Internet Express Administration utility to access the FireScreen installation. See *Applying the Best Practice* for more information.

Applying the Best Practice

Before you configure the FireScreen firewall, be sure to follow the recommendations in *Before You Begin*.

The Internet Express CD-ROM labeled "Installation and Documentation" contains the Administration utility, as well as other Internet software. To configure your system as a firewall using FireScreen, you should:

1. *Obtain the Internet Express Kit.*
2. *Install the Web Server and Administration Utility.*
3. *Install FireScreen.*
4. *Configure FireScreen.*
5. *Manage FireScreen.*
6. *Use FireScreen To Implement TCP/IP Security Policies.*
7. *Tune the System to Improve FireScreen Performance.*

Obtain the Internet Express Kit

HP includes the Internet Express CD-ROMs with Tru64 UNIX AlphaServer systems. If you need the Internet Express CD-ROMs, you can contact your HP representative. The part number for the Internet Express Kit is QB-3NCAA-SA.

Install the Web Server and Administration Utility

To install the Administration utility, follow the instructions in the *Internet Express for Tru64 UNIX Installation Guide* for mounting the Internet Express CD-ROMs and running the `ix_install` installation script.

During the installation, choose the Administration utility and the Secure Web Server subsets (`IAEADMxxx` and `IAEAPCHxxx`, respectively, where `xxx` is the Internet Express version number). These choices will implicitly select prerequisite subsets from the Internet Express kit.

When the installation has completed, the Administration Web server is set up on your system with default configuration settings and permissions.

Use a Web browser on the local host to connect to the Administration utility Web server running on port 8081. Use the following URL:

`http://hostname:8081`

Log in to the Administration utility by specifying the user name `admin` and the password you selected at the beginning of the Internet Express installation.

Install FireScreen

To access the Internet Express Administration utility, enter the URL, **`http://hostname:8081`**, in your Web browser after the Internet Express installation has completed.

Click on FireScreen in the Security components list under Manage Components in the Administration utility main menu to access the Install FireScreen option. You must click on Install FireScreen, perform the FireScreen installation, and reboot the system before additional FireScreen options will appear under the FireScreen component.

The Install FireScreen option verifies all FireScreen prerequisites have been met, installs the FireScreen configuration file, `/etc/firescreen.conf`, and then prompts you for your system configuration file and the path to

the system's kernel. It uses this information to rebuild the system's kernel with the `gwscreen` (gateway screen) option necessary to run the `screend` daemon.

Backup files for the files modified by the Install FireScreen option (including the kernel) are created with a file name extension of `.bck` in the same directory as the original file. When the default settings are used, these files include:

```
/etc/firescreen.conf.bck
/etc/inittab.bck
/sbin/init.d/firescreen.bck
/sys/conf/system configuration file name.bck
/vmunix.bck
```

You should move or copy these files to a backup area before performing an update installation of Internet Express Administration utility or the Tru64 UNIX operating system.

When the system reboots, the FireScreen firewall will be installed and the `screend` daemon will be running on the system. By default, any IP packet routed by the system will be denied. This behavior is controlled by the default screening rule in the FireScreen configuration file.

Configure FireScreen

Use the options under Configure FireScreen menu to configure your system as a FireScreen firewall. This option and others will appear on the Administration utility after the Install FireScreen option has finished.

To configure your system using FireScreen, follow these steps:

1. Choose FireScreen under Network Security on the Manage Components menu.
2. Click on Configure FireScreen on the FireScreen Administration menu.
3. Set the FireScreen Options. See *Set FireScreen Options*.
4. Add screening rules to the FireScreen configuration file. See *Add Screening Rules*.
5. Set the current and boot-time screening mode. See *Setting Screening Mode*.

With the exception of setting the screening mode, you must restart the `screend` process for changes to the FireScreen configuration to take

effect. To restart `screend`, click on Start/Stop FireScreen option under FireScreen.

Set FireScreen Options

Use the Set Screening Mode option under Configure FireScreen to set the Screening Mode of the `screend` process. When the Screening Mode is on, `screend` is actively filtering forwarded packets. When the Screening mode is off, forwarded packets are not filtered. This feature allows you to temporarily disable the firewall (perhaps to perform some administration or allow some IP traffic through) without having to shut down the `screend` process. You can also choose the Screening Mode you want in affect just prior to when your system's network interface is activated when the system is booted.

See the FireScreen chapter in the *Internet Express Administration Guide* and the `firescreend(8)` reference page for further information.

Add Screening Rules

You can add screening rules to the FireScreen configuration file to allow or deny IP-based protocols with packet destination addresses bound for networks, subnets, or hosts linked by the gateway. You can also control which packets of a protocol are allowed or denied access to a port on a host in a network.

You can use the Add New Screening Rule and Delete Screening Rules options to add and remove screening rules from the FireScreen configuration file. After adding new rules, you should check their syntax using the Check Screening Rules option before starting FireScreen.

The FireScreen installation creates a default screening rule in the configuration file that rejects all packets. The default rule is recreated if you select the New Screening Rule option after deleting all the Screening Rules from the configuration file. You can change the default rule to accept all packets by deleting it and adding the following line to the configuration file:

```
default accept;
```

IP packets are screened based on the first matching rule in the configuration file. Screening rules that are specific should appear in the file before general rules (except for the default rule, which can appear anywhere in the file).

Setting Screening Mode

Use the Set Screening Mode option under Configure FireScreen to set the Screening Mode of the `screend` process. When the Screening Mode is on, `screend` is actively filtering forwarded packets. When the screening mode is off, forwarded packets are not filtered. This feature allows you to temporarily disable the firewall (perhaps to perform some administrative task or allow some IP traffic through) without having to shut down the `screend` process. You can also choose the Screening Mode you want in effect just prior to when your system's network interface is activated when the system is booted.

Manage FireScreen

Use the Start/Stop FireScreen option to start, stop, or restart the `screend` daemon. During a restart, this form ensures the firewall remains enabled by shutting down the old `screend` process only after the new process has started.

Use the View FireScreen Status options to monitor the status of FireScreen. You can view the current screening rules, view the FireScreen log file, and get current FireScreen statistics about the IP packets processed. The statistics include total packets screened, total accepted, total rejected, the packets dropped, and the total packets dropped.

Use FireScreen To Implement TCP/IP Security Policies

Use screening rules to implement the TCP/IP security policies for your network. Security policies describe the access control to and from hosts on the upstream and downstream networks associated with your firewall. When creating a security policy for your network, you should consider the trustworthiness of any individual system or network and understand its vulnerabilities and any potential threat to other systems or networks.

Use some best practices of Internet security when implementing your Security policy, for example:

- a. Minimize direct communication between hosts by employing proxies or relays for network services.
- b. Separate services among several firewalls. If one becomes compromised the others remain secure.
- c. By default, completely deny access to services unless access is explicitly granted.

Tune the System to Improve FireScreen Performance

The following kernel subsystem attributes can be tuned to improve the performance of the `screend` daemon used by FireScreen.

Kernel Attribute	Default Value	Recommended Value
<code>screen_cachewidth</code>	8	2048
<code>screen_cachedepth</code>	8	16
<code>screen_maxpend</code>	32	8192

Tuning the `screening_cachewidth` and `screening_cachedepth` attributes reduces the number of screening cache misses generated by `screend`. A screening cache miss occurs every time an outgoing packet has an address/port pair that does not already exist in the kernel screening table or when the table is filled and new entries are required. Tuning the `screen_maxpend` attribute to the recommended value will help reduce the number of dropped packets when `screend` is experiencing heavy network load.

Verifying Success

After you apply the Best Practice for Setting Up and Configuring FireScreen, you can use the following criteria to verify whether it was successful:

- The `IAEADMxxx` subset is installed correctly (where `xxx` is the Internet Express version number).
- `OSFINETxxx` subset is installed correctly (where `xxx` is the Tru64 UNIX operating system version number).
- The `gwscreen` option is included in the running kernel.
- The FireScreen startup file (`/sbin/init.d/firescreen`) and configuration file (`/etc/firescreen.conf`) are installed.
- The `screenmode (sm)` entry is correctly installed in `/etc/inittab`.
- The services (or systems) you want to deny or allow are correctly denied or allowed access through the firewall.

To verify that the `IAEADMxxx` subset is installed correctly when you installed Internet Express, run the `setld` command as `root` and look for the word “installed” next to the subset name in the list of subsets displayed:

```

$ su root
$ setld -i | grep IAEADM
IAEADMxxx installed Internet Express Administration Utility
(Administration Utility)

```

To verify that the gwscreen option is included in the running kernel, reboot the system and use the nm command to list the gwscreen symbols in the kernel file from which you booted:

```

$ su root
$ nm -a /vmunix | grep gwscreen
gwscreen_li      |-004398040898216|Global |struct lockinfo* |0000000000000008|86060|SBss
gwscreen_rt      |-004398040093872|Global | |0000000000000000|92769|Bss
gwscreen_lock    |-004398040898224|Global | |0000000000000000|92774|SBss

```

To verify that the FireScreen startup file (/sbin/init.d/firescreen) and FireScreen configuration file (/etc/firescreen.conf) are installed correctly, try stopping and starting FireScreen using the S11 firescreen link in the /sbin/rc3.d directory:

```

$ su root
$ /sbin/rc3.d/S11firescreen stop
$ ps ax | grep screend
$ /sbin/rc3.d/S11firescreen start
FireScreen mode on
No forwarding until FireScreen starts...
FireScreen started
$ ps ax | grep screend
8227 ??      S          0:02.88  /usr/sbin/screend -f /etc/firescreen.conf

```

To verify that the screenmode (sm) entry in /etc/inittab is correctly installed, use the grep command to confirm it exists in the file and get the value of the entry. Then try running the screenmode command from the command line to confirm that it works:

```

$ su root
$ grep sm /etc/inittab
sm:23:wait:/usr/sbin/screenmode on < /dev/console > /dev/console 2>&1
$ /usr/sbin/screenmode on
$ /usr/sbin/screenmode
screening is on

```

To verify that the services (or systems) you allowed or denied access through the firewall are correctly allowed or denied access, test the service. For example, if you have allowed ftp access only to host 16.141.42.60, log in to any host on the other side of the firewall and try to ftp to host 16.141.42.60, then try to ftp to another host on the 16.141.42.0 network.

```

$ su root
$ cat /etc/firescreen.conf
for 16.141.0.0 netmask is 255.255.255.0;
between host 16.141.42.60 tcp port ftp and any accept;
between host 16.141.42.60 and any tcp port ftp accept;
default reject;
$ telnet 16.141.0.110
$ ftp 16.141.42.60
Connected to 16.141.42.60.
220 16.141.42.60 FTP server (Tru64 UNIX Version 5.0) ready.
Name (16.141.42.60:username):
$ ftp 16.141.42.110

```

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that the Best Practice was not successful as described in *Verifying Success*, use the following table to identify and solve problems.

Problem	Possible Solutions
The IAEADM subset is not installed.	<ul style="list-style-type: none">Review the installation steps described in the <i>Internet Express for Tru64 UNIX Installation Guide</i>.
The OSFINET subset is not installed.	<ul style="list-style-type: none">Mount the Tru64 UNIX operating system CD in the CD-ROM drive and use the <code>setld</code> command to reinstall the OSFINETxxx subset, as follows: <pre data-bbox="649 808 1120 903">\$ su root \$ setld -l path to kit on CD-ROM OSFINETxxx</pre>

Problem	Possible Solutions
FireScreen will not start.	<ul style="list-style-type: none"> • Rerun the Install FireScreen option located under the FireScreen component in Manage Components. Add the <code>gwscreen</code> option to the system configuration file and rebuild the kernel using the <code>doconfig</code> command, as follows: <pre data-bbox="654 453 1487 537"> \$ su root \$ echo "pseudo-device gwscreen" >> /sys/conf/system configuration file name \$ doconfig -m -c system configuration file name </pre> • Click on the Check Screening Rules option under the Configure FireScreen menu in FireScreen Administration and submit the form to check for syntax errors in your screening rules. • Use Delete Screening Rule and Add Screening Rule options to fix any syntax errors. • Reinstall the OSFINET_{xxx} subset from the Tru64 UNIX operating system CD-ROM (where <i>xxx</i> is the operating system version). Use the following commands: <pre data-bbox="654 947 1133 1010"> \$ su root \$ setld -d OSFINETxxx \$ setld -l path to kit on CD-ROM OSFINETxxx </pre>
Services (or systems) are denied (or allowed) access through the firewall	<ul style="list-style-type: none"> • Ensure FireScreen is running. Use the Start/Stop FireScreen option to start (or restart) FireScreen • Ensure FireScreen's screening mode is on using the Set Screening Mode form under Configure FireScreen. • Verify the path to the FireScreen configuration file is correct in the Set Options option under the Configure FireScreen menu. • Check your screening rules for logical errors that might result in a service (or system) losing or gaining access. • Use the <code>netconfig</code> or <code>sysman</code> command to verify the system's routing daemon (<code>gated</code> or <code>routed</code>) is broadcasting routes (RIP)

Alternative Practices

Although this Best Practice is the recommended method for configuring FireScreen, you can use an alternative method.

The `screend` daemon is an Open Source program. You could download, build, install, and configure a firewall yourself using just `screend`. FireScreen provides no additional functionality. However, the operating system kernel must support the `gwscreen` pseudodevice option to successfully run the `screend` daemon. This support is available on Tru64 UNIX Version 4.0B or later operating systems.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

`best_practices@zk3.dec.com`

Legal Notice

Compaq, AlphaServer, and Tru64 are trademarks of Compaq Information Technologies Group, L.P. in the U.S. and/or other countries.

Microsoft, Windows, and FrontPage are trademarks of Microsoft Corporation in the U.S. and/or other countries. UNIX and The Open Group are trademarks of The Open Group in the U.S. and/or other countries. HP and HEWLETT PACKARD are trademarks of Hewlett-Packard Company. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.