

SunScreen, Part One: An Overview of the Sun Microsystem Firewall

Ido Dubrawsky 2003-01-24

SunScreen is Sun Microsystem's firewall that runs under the Solaris operating system. It is the latest version of Sun's long line of firewall software that allows administrators to provide firewall capabilities to the Solaris operating system. [SunScreen 3.1](#) is available in a full version which can be purchased from Sun Microsystems or a "lite" version which could be downloaded from Sun's Web site. With the release of Solaris 9, Sun has now bundled the SunScreen software with the OS.

SunScreen provides for packet filtering as well as authentication and data encryption. The SunScreen software provides for both a packet filter as well as the capability to create IPsec-based VPNs. Administration of the SunScreen system is provided through a GUI or a command-line interface. The SunScreen system is composed of two parts: the screening system and the administration system. The administration can be either local (that is on SunScreen itself) or remote (a separate host running the SunScreen administration software and communicating with the firewall through a secure, encrypted channel).

Interface Modes

One of the nice features of SunScreen is the capability to choose how each of the system interfaces will be utilized. There are two modes for each physical interface: routing mode and stealth mode. In routing mode the interface has a TCP/IP stack and an IP address associated with the interface. This provides for routing of packets from one interface to another as well as filtering between interfaces. The second mode, stealth mode, does not associate a TCP/IP stack or an IP address to the interface. Because SunScreen operates in between Layer 3 and Layer 2 of the network stack it is able to operate in this mode where it acts as a bridge between interfaces. When an interface is operating in stealth mode, SunScreen is able to filter traffic but the host appears as a "bump" in the flow of packets.

The choice of either a routing interface or a stealth interface can be made on a case-by-case basis. A system could effectively have five 10/100Mb interfaces - one built-in 10/100Mb (hme0) and four on a quad fast Ethernet card (qfe0 - qfe4) - and have two in stealth mode and the other three in routing mode. An example is shown in Figure 1.

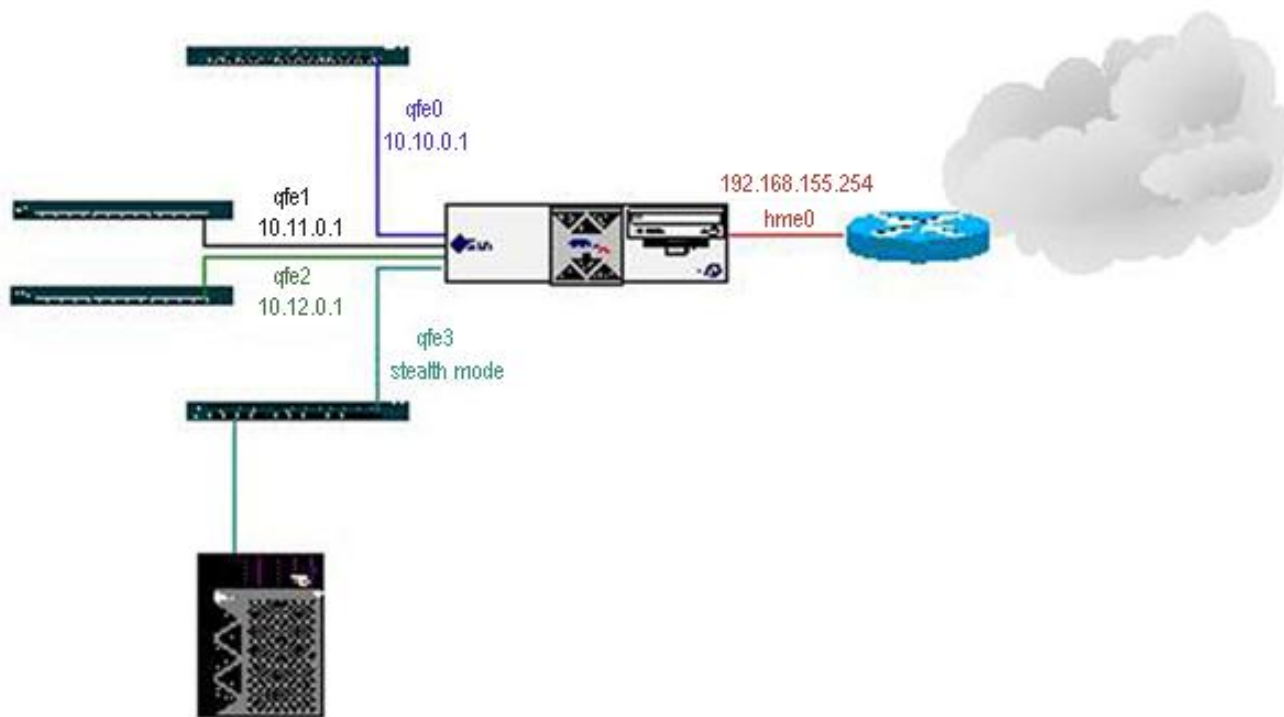


Figure 1: Interface Modes in SunScreen

In the above example the SunScreen system has an external interface (hme0) with an IP address of 192.168.155.254. The system also has a quad Fast Ethernet card installed with all four interfaces configured in the SunScreen software. The interfaces qfe0 - qfe2 are in routing mode and have the IP addresses 10.10.0.1, 10.11.0.1, and 10.12.0.1 respectively. However, interface qfe3 is operating in stealth mode; therefore, the system behind the SunScreen does not appear to reside behind a firewall. The hosts behind a SunScreen with an interface in stealth mode may have private IP addresses (which are then translated by SunScreen) or they may have public, routable IP addresses. The benefit of being behind a stealth interface lies in the fact that an IP address is not taken up by the firewall's interface, as well as the fact that SunScreen is harder to detect.

SunScreen Functions

SunScreen provides several functions when analyzing packets and, subsequently, determining if any action is required. The packet flow within SunScreen is shown in Figure 2. Packets destined for a host behind SunScreen or on the firewall itself are received from the network interface. Packets are first decrypted if they have been encrypted with SunScreen's public key. Decryption is either done by the Simple Key management for Internet protocols (SKIP) key manager or the Solaris Internet Key Exchange (IKE) facilities. Once decrypted, the packets are then translated if necessary. For inbound packets, the destination address is translated. Once these two functions have processed the packet, SunScreen applies the filtering rules. If the packets matches a rule then the corresponding action is taken.

Like many other firewall systems the SunScreen filter is a "first match" system, in which the first rule that matches the packet characteristics is the rule applied to the packet. Other firewall systems use a "best match"

concept wherein a packet may match a rule at the beginning of the ruleset but then match another rule more precisely later on. The second rule would then be applied to the packet as the "best match" rule. SunScreen uses the "first match" concept.

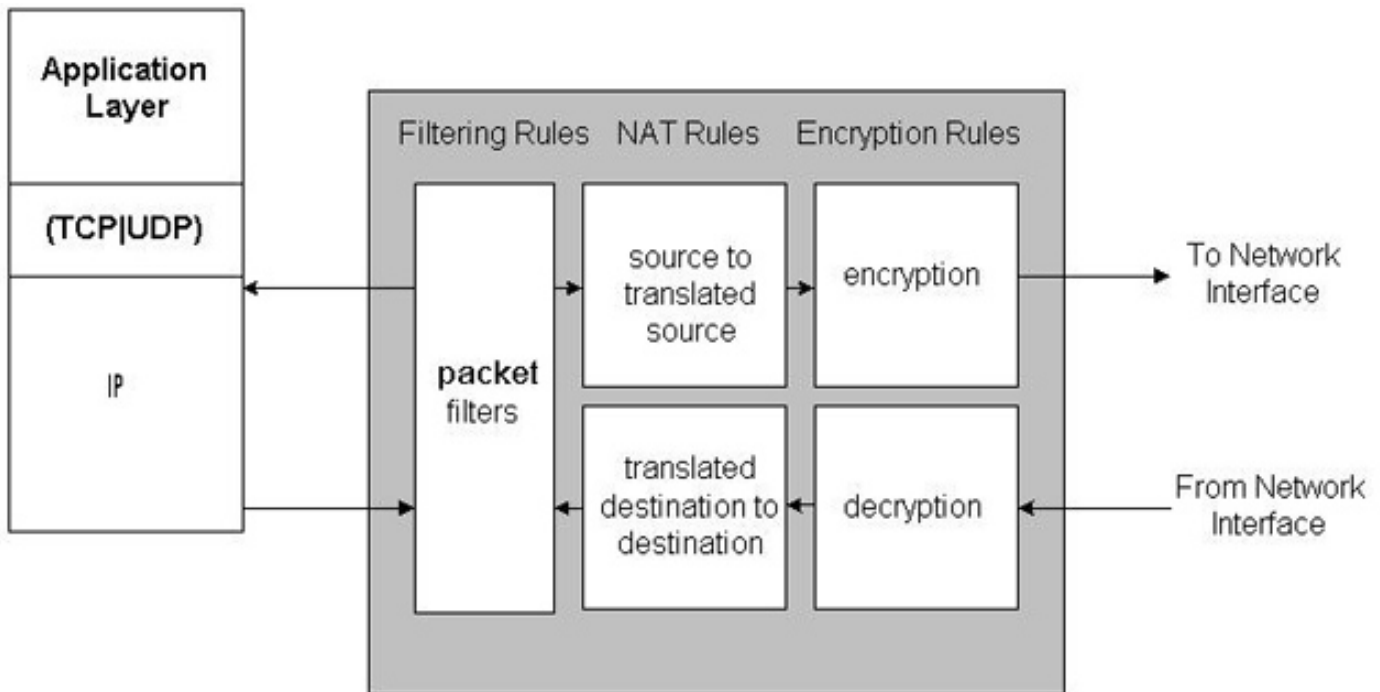


Figure 2: SunScreen Packet Functions

Once the packets have passed through the filter - if they haven't been denied - they are then passed to higher layers in the network stack for possible routing. If the packets are destined for a remote host, they are passed to the local application on SunScreen itself. Packets leaving SunScreen are treated in reverse order. After the network interface receives the packets, it applies the outbound filter rules to it. If the packets pass the filters, they are then translated and, if necessary, encrypted before being sent to the network interface.

Installing SunScreen

Bundling SunScreen with the Solaris 9 operating system distribution was a very smart move on Sun's part. CheckPoint's Firewall-1 software firewall is one of the more popular software firewalls to be used on Solaris systems. By bundling SunScreen with Solaris 9, Sun will allow many administrators the capability to try their software firewall and replace their CheckPoint Firewall-1 firewalls with SunScreen.

While combining SunScreen with Solaris 9 was shrewd, Sun's placement of the software on the CD distribution was not. It is not easy to find and requires a fair amount of poking about to locate it. SunScreen can be found on the second CD-ROM in the Solaris 9 distribution under the directory:

```
/cdrom/sol_9_sparc_2/Solaris_9/ExtraValue/CoBundled/SunScreen_3.2
```

Placing it so far down in the directory structure makes one wonder if Sun intended to release SunScreen 3.2 with Solaris 9 or whether it was an afterthought. Nevertheless, once the software has been found, installing it is

relatively straightforward. It is clear from the documentation that Sun is providing SunScreen with the OS as a way of displacing CheckPoint's FireWall-1, as the installation document clearly describes how to upgrade a system from FireWall-1 to SunScreen 3.2.

The install program is a java-based application and is found at the top-level directory of the SunScreen software. To start the install program simply use the install script. The installer guides the installation, allowing the administrator to choose whether to install the system with **local** administration or **remote** administration. Before installing the software, the installation script checks for the existence of various packages. If these packages are not installed, it will note this fact as a failure and provide a list of the missing packages. Installing any missing packages is not a problem as they exist on the Solaris CDs.

Perhaps the easiest way to do a SunScreen installation is to perform a complete install of Solaris and then use a provided script, *harden_os*, to lock down the system. Sun recommends that this only be done if all interfaces on the Screen (as SunScreen is also known as) run in stealth mode. If any interface is being used in routing mode then this is not recommended. The script can be found in

```
/usr/lib/sunscreen/lib
```

and removes packages and files that are not used by SunScreen from the operating system. This script is based on the best practices for Solaris security that are defined in [Sun's Blueprints](#).

Once the SunScreen software is installed the system must be rebooted in order for SunScreen to start up.

Administration

As mentioned above there are two ways in which a SunScreen system can be administered: **local** or **remote**. With **local** administration the Screen administrator logs into the SunScreen host and can either administer the system using a Command Line Interface (CLI) or a Graphical Interface (GUI). The CLI consists of various SunScreen command programs and requires that the user have *root* privileges on the SunScreen host. The GUI however allows the user to log in (for **local** administration) without requiring *root* privileges. The default account on SunScreen is the *admin* account which has a default password of *admin*. When logging into the SunScreen management GUI for the first time the best order of action to take is to 1) change the *admin* password and 2) create accounts for other administrators who will be managing the firewall.

Local Administration

Administering a SunScreen system locally through the GUI requires a Web browser...that's it. Start up a browser and point it to the URL `http://localhost:3852`. This brings up the login screen shown in Figure 3. Logging in as the *admin* account allows the administrator to modify Screen policies as well as add hosts or networks (Sun's documentation refers to the components of a Screen rule as "objects". So there are service objects, and address objects, and interface objects, and so forth).



Figure 3: SunScreen Login Page

Remote Administration

One of the nice features of SunScreen is the capability to designate one host as a remote administration host, which can then be used as a central point to manage other Screen hosts. This allows administrators to ease the process of maintaining multiple firewalls. All communications between the remote administration host and the Screen hosts are encrypted using either Simple Key management for Internet Protocols (SKIP) or Internet Key Exchange (IKE).

SKIP is a key distribution protocol that uses hybrid encryption to convey session keys. These session keys are used to encrypt data in IP packets. SKIP uses the [Diffie-Hellman algorithm](#) to take the public keys of two systems and derive a unique session key from the public keys. All traffic is then encrypted using a symmetric encryption algorithm with the session key as the encrypting key.

IKE is a key distribution protocol that is currently the standard that is used for setting up IPsec VPN tunnels. IKE is a protocol designed to provide mutual authentication of systems as well as the establishment of a shared secret key to create in IPsec Security Association (SA). Once a shared secret has been established, the two parties can use that secret to encrypt all communications.

SunScreen allows the administrator to choose whether to use SKIP or IKE as the key exchange scheme between the remote administration station and the Screen system. Once configured for remote administration the Screen system appears as simply another object in the administration web interface.

Conclusion

SunScreen is a powerful software package that can be used to set up enterprise-level firewalls on Solaris systems. By bundling SunScreen with Solaris 9, Sun has taken a significant step towards expanding the traditional role of Solaris in the enterprise network. With the addition of IPsec and SunScreen, Sun has created two more roles for Solaris: VPN gateway and Enterprise Firewall.

While Solaris has had these capabilities for quite some time with CheckPoint's Firewall-1 and the older Gauntlet Firewall software, by bundling SunScreen in with Solaris 9, Sun has clearly taken steps to make it much easier for administrators to deploy Solaris in new roles. The second article in this series will discuss how to configure a remote administration host to communicate securely with a Screen host, as well as how to add and remove rules from the Screen.

[Privacy Statement](#)

Copyright 2006, SecurityFocus