Global Information Assurance Certification Paper

Stealth Firewalls

Brandon Gillespie
April 10, 2001

Stealth firewalls are the little known but powerful gem of firewall architectures. The first step of any attack is to "know your enemy" [4]. An attacker first probes, scans and enumerates all of the network's visible resources. Stealth firewalls are hard to see on the network, and thus it is harder for an attacker to learn your network topology.

There are a few distinct types of behaviors currently considered by the industry as "Stealth." The first type locks down a system--either workstation or server--in its presence on the network. It accomplishes this by restricting its services to the minimum necessary and using a packet filter to control which network resources it communicates with. Another type is a network firewall which does not respond to restricted resource requests with a "resource denied" or "resource restricted" message, but instead simply ignores the request. The final type is also a network firewall, but it does not route network traffic in the conventional manner. This is the type of firewall we will scrutinize.

I consider the following two prerequisites as requirements for full qualification as a true Stealth Firewall. First, a Stealth Firewall has no addresses or other Layer 3 presence on any network for which it is providing access control. Instead it behaves as a bridge or switch, connecting multiple network segments, but also provides access control mechanisms at that point. The second requirement is implied from the first: Stealth Firewalls do not decrement the Time To Live (TTL) on packets being managed. Because of this, anybody scrutinizing the packet's path will not see the Stealth Firewall as a hop.

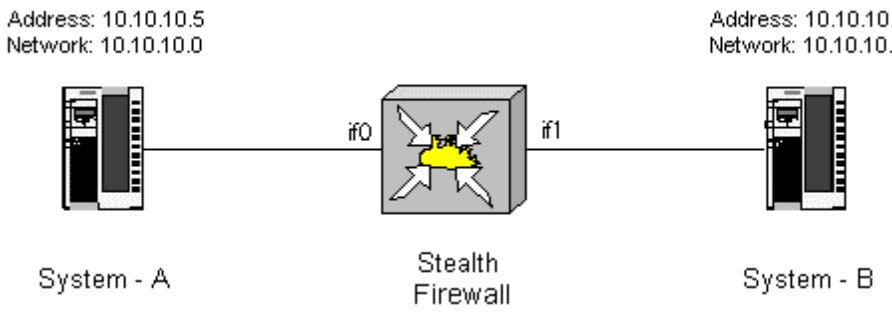
As of this writing there are only a few common products capable of running as stealth network firewalls: FreeBSD, Linux and Sun Microsystem's Sunscreen Firewall. FreeBSD and Linux both combine a bridging mode with their packet filter to become a Stealth Firewall. Sunscreen accomplishes it through a special stealth-mode, which can be enabled in their product. Of these, Sunscreen is by far the most mature product. However, when considering costs FreeBSD and Linux are both available open-sourced for free, and Sunscreen is approximately $4500. This does not include the administrative costs, as FreeBSD and Linux both require more management and expertise to build, where Sunscreen is a fully bundled and completed product.

Stealth Firewall Architecture

Stealth Firewalls can handle multiple network interfaces, however they are not network routers. They split a single subnet into distinct segments (or zones) with the firewall at the center, joining them in a manner similar to a bridge or switch. Stealth Firewalls do this at a layer lower than routing, and instead examine each IP packet in a manner similar to network sniffers, moving them between interfaces as is appropriate based on the given access control lists. To accomplish this the firewall must be configured to know which

hosts are on which interface, and firewall access control lists must be defined describing what traffic is allowed to and from different segments.

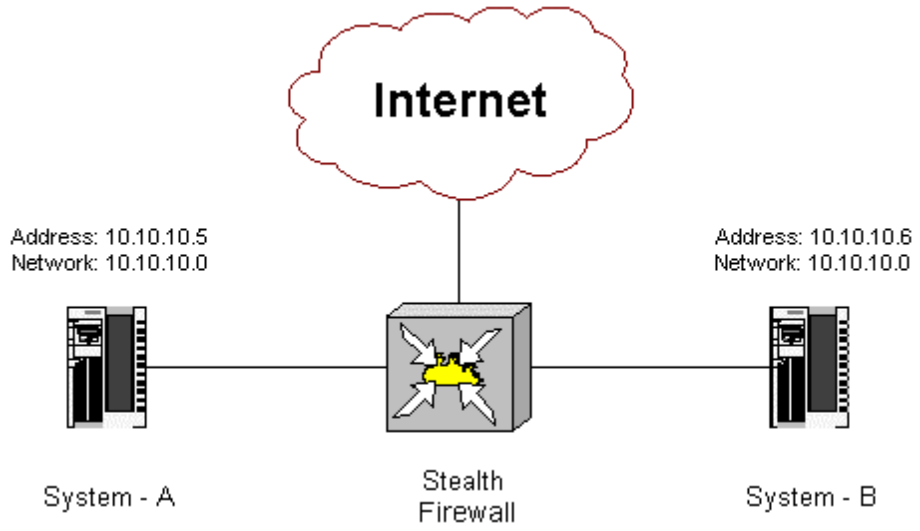
Diagram #1



This example shows a simple network (10.1.1.0/25) split into two segments, separated by a Stealth Firewall

Diagram #1 shows a simple Stealth firewall splitting subnet 10.1.1.0/24. In this example you have a system on each side of the Stealth Firewall. This example is not a real-world example, rather it demonstrates how the systems exist on the same IP network, but on different segments of the firewall. The configuration for this example would include a definition for System-A on interface zero (if0) and a definition for System-B on interface one (if1)

Diagram #2



This example shows two servers protected from themselves and from an external network.

Diagram #2 is a little closer to the real world. This time you have System-A and System-B, but they are both protected from the external network, as well as each other. In this example System-A could be a web server for public access and System-B could be a web

server for private access. Access Control Lists could be defined to manage relationships between the external network and each individual system, as well as relationships between each system.

Merits of Stealth Firewalls

Stealth firewalls have a few merits over routing firewalls:

- All attacks are restricted to Layer 2, since the firewall does not have an OSI layer 3 presence on the network it is protecting.
- It is more difficult to determine which firewall product is being used and which version.
- It is more difficult to externally enumerate and map topology of a network.
- Existing networks can be firewalled without subnetting them.

One way to defeat a firewall is to target it directly. It is usually a network device like any other, and has an IP address. You can often probe and query against this address to learn useful information, such as what firewall product it is, what patch level it is at and even what services it may be running. When running in stealth mode this is not possible.

By not having a Layer 3 presence on the network, it is not possible to target and/or probe the firewall. This limits attacks directly against the firewall to those which use layer 2. In addition to being a hard target, it also means it is difficult to determine which firewall product is being used and which version is being run.

Additionally, you can place a Stealth Firewall into a single network subnet, joining separate network segments together with relationships between segments yet on the same subnet. It is then more difficult to enumerate and map the topology of the network, because externally it is hard to determine where the firewall is sitting in relation to the systems it is protecting. With a routing firewall you can easily determine this by discerning which subnets the firewall is protecting.

The ability to firewall a network without subnetting it can also be useful during implementation of an existing network, as you do not have to change any subnets from the way they are currently implemented.

Drawbacks of Stealth Firewalls

Stealth firewalls do have drawbacks:

- They are difficult to architect.
- They are difficult to install.
- It is more difficult to trouble shoot networking problems when they are present.

Stealth firewalls are much harder to architect and install. They do require more indepth knowledge of networking, since you have to be more cautious with each segment being built, and the relationships required between systems in different segments.

Troubleshooting networking issues is more difficult once the stealth firewall is in place. Because Stealth Firewalls have no presence it is very difficult to trace traffic behavior and relationships between systems.

Implementation Summary in Sunscreen

Sun Microsystem's Sunscreen Firewall is the pioneer for Stealth Firewall behavior. It is currently available in two forms: a limited version is available free with Solaris 8 as Sunscreen-Lite (by download for Solaris 8 x86 or on the Software 2 CD for Solaris 8 sparc), and a full release edition is available for purchase. Unfortunately the lite edition does not have stealth capabilities. Sunscreen has additional features including an easy to use administration interface with both a Graphical User Interface (GUI) and Command Line Interface (CLI), which work synchronously. It also comes with Remote Administration, NAT, VPN, proxies and more.

Installing Sunscreen is done in two parts. First you define an administration station, and then you install the screen (the actual firewall). If you are evaluating sunscreen it is best to select "Local Administration" and not to define remote administration. Remote administration is more work to get functioning properly.

The easiest way to install sunscreen is to load the CD and run the `installer` script. Unfortunately this loads a java GUI. It is also possible to install sunscreen from the CLI, by simply running `pkgadd` on the relevant packages (refer to the appendix in the *Sunscreen Installation* manual).

During the GUI install it will ask you several questions, including whether or not you want Remote or Local administration, and whether or not you want to run in Stealth Mode or Routing Mode. If you are doing a CLI installation, after the *pkgadd* has completed you must run the *ss_install* command.

After the software is installed and the server is rebooted, you can access the configuration through the GUI by pointing a web browser at: *`http://localhost:3852`*. It will load a java applet.

> **note:** if you are running Netscape for this, you should also look in the manual for a new java library, as the stock Netscape java library will not allow an applet to store files, which you may want to do if you wish to backup your configuration to disk.

The default user is `admin` with a password of admin. From the command line you can access sunscreen by typing `ssadm edit` *`policy`*. By default your policy is *Initial*.

To define the simplest sunscreen installation allowing all traffic between systems you must create a rule allowing * from * to *. The most important thing you must do is to define address groups for each interface, and associate them with the interface. The address group should be inclusive of all systems on each network interface segment.

References

Boran, Seán "Checking out Sun's Stealth Firewall" Security Portal April 3, 2000
URL: http://www.securityportal.com/cover/coverstory20000403.html March 28, 2001

Conoboy, Brendan & Fitchner, Erik "IP Filter Based Firewalls HOWTO" obfuscation.org March 10, 2001
URL:http://www.obfuscation.org/ipf/ipf-howto.html March 28, 2001

Peterson, Steve "Bridging" FreeBSD Handbook March 28, 2001
URL: http://www.freebsd.org/handbook/bridging.html March 28, 2001

Sun Tzu "The Art of War"
URL: http://www.ccs.neu.edu/home/thigpen/html/art_of_war.html March 28, 2001

Breuer, Peter "Linux Bridge+Firewall Mini-HOWTO version 1.2.0" December 19, 1997
URL: http://www.linuxdoc.org/HOWTO/mini/Bridge+Firewall.html March 28, 2001

Sun Microsystems "SunScreen Secure Net 3.1" March 28, 2001
URL: http://www.sun.com/software/securenet/index.html March 28, 2001

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS