GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Sidewinder 5.1 Split DNS Architecture

Charlene Keltz

July 8, 2001

This paper provides an operating system overview of Sidewinder, a short overview of a Generic Split DNS Architecture, and explains Sidewinder's Secure Split DNS Architecture. It also outlines two (2) important additional DNS security statements that should be included in all Name Server configuration files.

Sidewinder Overview

Sidewinder is an application-level gateway firewall designed and developed by Secure Computing Corporation (SCC), which is headquartered in San Jose, California. Sidewinder has been in existence since 1995 and has been touted as the strongest firewall in the security industry. In fact, Sidewinder has never been compromised. The core of Sidewinder's technology is SecureOS™, which is Sidewinder's own operating system. SecureOS™ is based on BSD, but has been hardened by a team of SCC engineers and optimized by SCC's patented technology called Type Enforcement™. Unlike other UNIX and NT firewalls, there is no separation between Sidewinder and SecureOS™ – one installation process installs both on a hardware platform.

Type Enforcement™ divides SecureOS™ into individual sections not unlike watertight compartments in a submarine. These sections are called "domains". Every process, file and access role (such as the admin role) is contained within a domain, and assigned a label that consists of two (2) security attributes:

Domain	assigned to active processes
Type	assigned to files that active processes use to perform certain functions

Type Enforcement™ technology is "Mandatory". Its rules regarding domains cannot be bypassed and cannot be disabled. Every security policy decision made in SecureOS™ is checked against the Type Enforcement™ policy engine for an ALLOW/DENY action. Sidewinder's Split DNS Architecture is also governed by the Type Enforcement™ policy engine.

Generic Split DNS Overview

Many Generic Split DNS configurations are integrated into networks today. Normally a Split DNS architecture means that one or more Name Servers usually reside behind a firewall, and contain "inside" hostname and IP address information. If the firewall has Network Address Translation (NAT) enabled, the Network Administrator has the choice to assign reserved network addresses to all hosts. These network addresses are outlined in RFC1918, Section 3, and have been permanently designated as "reserved" by the Internet Assigned Numbers Authority (IANA). The Network Administrator can also decide to assign registered addresses to his inside systems, however, this makes a network more vulnerable because these addresses are routable on

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

the Internet, where reserved addresses are not.

On the external side of a firewall, this same organization has one or more Name Server(s) hosting zone files that contain minimal information. NS, MX, PTR and A zone records can either reference the firewall's fully-qualified hostname and IP address, or can point to the actual system's hostname and IP address. CNAME records, such as www and ftp, can also be included.

Two scenarios can take place regarding inside user queries:

1) Any queries that are generated by internal users are forwarded to the inside Name Server(s), and any queries this server cannot answer are forwarded directly to the external Name Server(s) for resolution. If the external Name Server(s) cannot answer, it forwards the queries to the Internet root servers.

2) Any queries that are generated by internal users are forwarded to the inside Name Server(s), and any queries it cannot answer are forwarded directly to the Internet root servers.

If any of these Name Servers are located on a standard UNIX system, they are vulnerable to BIND DNS attacks. As listed in the SANS Institute's Consensus List of The Top Ten Internet Security Threats, BIND Weaknesses is #1.

Sidewinder Split DNS Architecture

A Sidewinder firewall can be configured to incorporate up to nine (9) separate networks, or "burbs". Eight of these burbs must have at least one (1) physical interface – the ninth burb is a "Virtual" burb used in certain VPN configurations. Each of the burbs that contain a physical interface requires different network IP address. Whether a site configures two, three, or all nine burbs, only one (1) burb is configured as the Internet burb. All others are considered non-Internet, or trusted.

Each burb also has an Index Number assigned to it. This Index Number is very important because it is used by Sidewinder to reference Type Enforcement™ domain names, directories, filenames, filename extensions, and statements within individual files. The Index Number is also part of each burb's localhost number. For example:

Burb Index Number	Burb Name	Localhost Number	TE Domain
1	External	127.1.0.1	DNS1
2	Inside	127.2.0.1	DNSu

Sidewinder's Split DNS consists of (2) Name Servers. One is called the Unbound Name Server because it handles queries from all non-Internet burbs. The other is called the Internet Name Server because it is "bound" to the Internet Burb. This Name Server handles queries from the

© SANS Institute 2000 - 2005 Author retains full rights.

Internet, and directly from the Unbound Name Server.

Sidewinder's Name Servers can be configured as either Master or Slave to another Name Server on a separate system, which provides redundancy for both internal "whole story" and external "small snapshot" zone files. The most common configuration is the Unbound Name Server configured as Slave to an existing Master Name Server residing in a non-Internet burb, and the Internet Name Server configured as Master with an outside Slave Name Server usually located at the ISP site. The Type Enforcement™ policy engine prohibits these Name Servers from acting as Master/Slave to each other.

Sidewinder's Split DNS Architecture has a named.conf file for each Name Server, and a separate /etc/namedb directory containing that Name Server's zone files as outlined below:

Internet Name Server

The Internet Name Server resides in the Type Enforcement™ domain called DNS# (where # is the Index Number assigned to this burb at initial configuration). Its configuration file is called named.conf.i, resides in Sidewinder's /etc directory and can contain many forward and reverse-lookup zone statements. This configuration file also contains one (1) localhost zone statement, i.e., 0.x.127.in-addr-arpa, where x is the Index Number chosen to represent the Internet burb.

The named.conf.i configuration file, the /etc/namedb.i directory, and all zone files stored in /etc/namedb.i must also reside in the DNS# domain. This means that all files referenced by the Internet Name Server must have the correct Type Enforcement™ security attributes assigned. For example:

File Name	TE Domain:Type
/etc/named.conf.i	DNS1:conf
/etc/namedb.i	DNS1:diry
/etc/namedb.i/yourdomain.com.db	DNS1:conf
/etc/namedb.i/otherdomain.com.bak	DNS1:conf
/etc/namedb.i/68.168.192.db*	DNS1:conf
/etc/namedb.u/0.1.127.db**	DNS1:conf

* this address would normally be registered; used reserved for purpose of example
** this localhost address indicates that Index Number 1 was assigned to the Internet Burb

Unbound Name Server

The Unbound Name Server resides in the Type Enforcement™ domain called DNSu. Its configuration file is called named.conf.u, resides in Sidewinder's /etc directory. This configuration file contains zone statements for all the non-Internet (trusted) forward and reverse-lookup zones created at Sidewinder's initial configuration (up to seven (7) reverse-lookup zone statements). It also can contain up to seven (7) localhost statements, as well as many other

© SANS Institute 2000 - 2005 Author retains full rights.

forward and reverse-lookup zone statements.

The configuration file and all zone files stored in the /etc/namedb.u directory must also reside in the DNSu domain. This means that all files referenced by the Unbound Name Server must have the correct Type Enforcement™ security attributes assigned. For example:

File Name	TE Domain:Type
/etc/named.conf.u	DNSu:conf
/etc/namedb.u	DNSu:diry
/etc/namedb.u/yourdomain.com.db	DNSu:conf
/etc/namedb.u/otherdomain.com.bak	DNSu:conf
/etc/namedb.u/1.16.172.db	DNSu:conf
/etc/namedb.u/10.10.db	DNSu:conf
/etc/namedb.u/0.2.127.db*	DNSu:conf
/etc/namedb.u/0.3.127.db*	DNSu:conf

* these localhost numbers indicate that Index Numbers 2 & 3 were assigned to non-Internet (trusted) burbs.

Importance of correct Type Enforcement™ Security Attributes

To display Type Enforcement™ security attributes, enter 'ls –ly | more' at Sidewinder's command line. Because all the files listed in the above examples have the correct security attributes, both Name Servers will be able to read its configuration file and load all its zones (providing that there are no syntax errors). If you enter the 'ls –ly | more' command and any DNS file or directory does not list either DNSu or DNS#, the Name Server will not be able to see that file or directory.

For example, the Firewall Administrator has been tasked to create a new internal subdomain zone. He/she will perform the following steps:

1) Enter a new zone statement into /etc/named.conf.u
2) Create a new zone file, or copy an existing zone file and edit
3) Restart the Unbound Name Server with the command 'ndc restart'
4) Check for new records using 'nslookup'
5) The lookup fails. Why?

The Firewall Administrator had to be in the 'admin' role in order to create or copy an existing DNS zone file. This 'admin' role is contained in the Type Enforcement™ domain called Admn; therefore, the newly created zone file will have security attributes of Admn:file. The Unbound Name Server now has a problem because it resides in the DNSu domain, and all files that it is expected to load also need to be in DNSu domain. Type Enforcement™ prohibits this process from looking to other domains to locate this new zone file.

© SANS Institute 2000 - 2005 Author retains full rights.

The Firewall Administrator needs to perform the following additional steps in order for the Unbound Name Server to load the new zone file and be able to answer queries:

1) Enter 'ls –ly | more' to see that the new zone file is owned by the Admn domain and currently has security attributes of Admn:file
2) Enter 'chtype' to change the attributes to DNSu:conf. The correct syntax is 'chtype DNSu:conf *filename*'
3) Enter 'ls –ly | more' to confirm that the new zone file have been moved to the DNSu domain and now has security attributes of DNSu:conf
4) Restart the Unbound Name Server with the command 'ndc restart'
5) Check new records using 'nslookup'
6) The lookup will now be successful (unless you have syntax errors in the configuration or zone files)

Internal Name Servers and Client Workstations located on the Inside Network

Internal client workstations should be configured to send queries to the Internal Name Server IP address and to Sidewinder's internal NIC IP address. This can provide load balancing and redundancy. The Internal Name Server(s) should be configured with a 'forward only' forwarders statement that points to Sidewinder internal NIC IP address. All internal queries will first go to the Internal Name Server. This name server will then answer if it is authoritative for that query, i.e., hostname.yourdomain.com. Any queries that it cannot answer will then be forwarded to Sidewinder's Unbound Name Server listening on the internal NIC address.

If the Unbound Name Server cannot answer the queries, it will forward to the Internet Name Server based on the 'forward only' forwarders statement in its configuration file. If the Internet Name Server cannot answer the query, it will forward to the root servers. The Internal Name Server(s) on the inside network, and the Unbound Name Server are never configured to send directly to the Internet

Add restrictive statements to all Name Server configuration files

You have separated your DNS information into "small snapshot" and "whole story" zone files by incorporating Sidewinder's Split DNS Architecture. Only the Internet Name Server sends queries to the Internet root servers. Type Enforcement™ prohibits the Internet Name Server from sending any queries for zone information to the Unbound Name Server. But what about unauthorized zone transfers? By default, BIND will still allow zone transfers to any system configured as a Slave, whether those systems are considered "authorized" or not.

The 'allow-transfer' statement should be added to all Master and Slave Name Server(s) configuration files. It can be added to the 'options' statement so all zones are protected against unauthorized transfers, or to each individual zone statement. The examples show the 'allow-transfer' statement included in the 'options' statement because this will protect <u>all</u> zone files.

© SANS Institute 2000 - 2005 Author retains full rights.

On the Master Name Server (192.168.68.1):

```
options {
   allow-transfer { 192.168.68.2;  192.168.68.3; };
};
```

On Slave Name Servers (192.168.68.2 and 192.168.68.3):

```
options {
   allow-transfer { none; };
};
```

The "On Master Name Server" example indicates that only two (2) systems are "authorized" Slave Name Servers and can successfully receive a copy of any zone file listed in the configuration file

The "On Slave Name Servers" example indicates that no system configured as a Slave can get a transfer of any zone file listed in the configuration file

The 'allow-query' statement can be used to restrict queries for zone information, and can be added in the 'options' statement so all zones are protected against unauthorized queries, or to each individual 'zone' statement. A site may choose not to include this statement to the Internet Name Server's configuration file because such a minimal amount of information is contained in these zone files. However, depending on how your internal Name Server(s) hierarchy is configured, you may want:

1) The Unbound Name Server to only accept zone queries from the Internal Name Server (172.16.1.2), and the Internal Name Server to accept zone queries from any internal client workstation, or

2) Both the Unbound Name Server (172.16.1.1) and the Internal Name Server to accept zone queries from any internal network system

For Item 1) include the following allow-query statement in the Unbound Name Server's configuration file:

```
options {
   allow-query { 172.16.1.2;  127.x.0.1; };
};
```

For Item 1) include the following allow-query statement in the Internal Name Server's configuration file:

```
options {
   allow-query { any; 127.x.0.1; };
};
```


© SANS Institute 2000 - 2005 Author retains full rights.

For Item 2) include the following allow-query statement in the Unbound Name Server and the Internal Name Server's configuration files:

```
options {
   allow-query { any; 127.x.0.1; };
};
```

References

1) Network Security Product Solutions; Sidewinder (Online, accessed on July 3, 2001) Available: http://www.securecomputing.com/index.cfm?sKey=2

2) Minear, Space "SecureOS™ A Working Example of a Secure BSD OS" (Online, accessed on July 3, 2001) Available: http://securecomputing.com/index.cfm?sKey=575

3) Secure Computing Corporation, Sidewinder Administration Guide, November, 2000, Chapters 1 and 8.

4) RFC1918, Section 3 (Online, accessed on July 3, 2001) Available: http://www.faqs.org

5) Consensus List of The Top Ten Internet Security Threats (Online, accessed on July 3, 2001) Available: http://www.sans.org/topten.htm

6) Liu, Cricket "Securing an Internet Name Server" (Online, accessed on July 3, 2001) Available: http://www.acmebw.com/resources/papers/securing.pdf

7) Albitz, Paul and Liu, Cricket, DNS and BIND, Third Edition, Sebastopol, CA, O'Reilly & Associates, Inc., September, 1998, Pages 249-253.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.