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

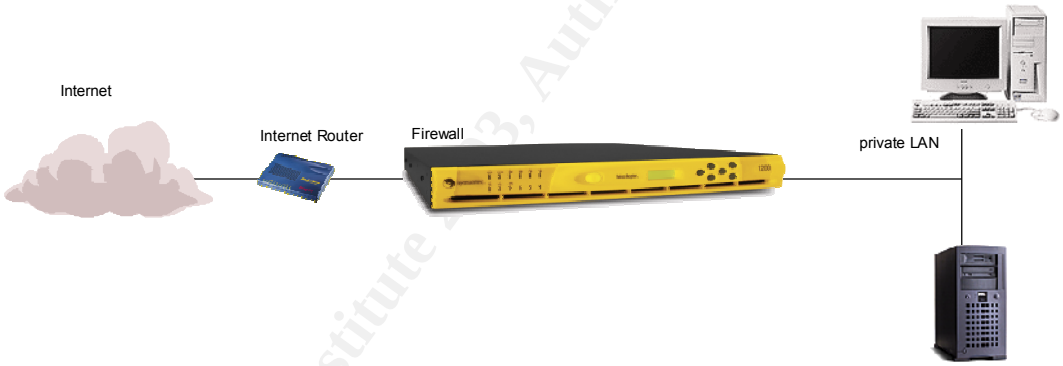
DNS and Proxy performance tuning of a Symantec Enterprise Firewall installation in an enterprise network

Content

In my five years of work with the Eagle, Raptor and now the Symantec Enterprise Firewall I repeatedly found typical mistakes in the configurati on of DNS services and Memory Management. I would like to pick up some of those features and further explain them. Information and facts that are used here ground on the base of my personal experience gained at installations in Germany, Austria and Switzer land. Furthermore, they are based on dialogues with the support teams and last but not least on researches in the Internet. For reasons of clearness I invented a fictive domain dreamland.de and the corresponding IP's.

Veloci Raptor

The Veloci Raptor is an appliance of the Symantec Enterprise Firewall. Axent created the first appliance generation on basis of the Cobalt platform. Today we are about to enter the third generation of appliances. Regarding the management of memory this paper will deal with applia nces 1100, 1300, 5100 and 5300 but comments on DNS can be generalised for all Firewall systems. In this paper a Symantec Veloci Raptor 1300 with the following installations will be used as an example:



These will be the technica l specifications of our Symantec Veloci Firewall [1]:

Hardware

- Intel-compatible processor
- LCD panel for easy set -up and administration
- 512 KB L2 cache
- 1 GB RAM
- UPS support
- Internal Ultra ATA hard drive
- Four 10/100 Base -T Ethernet network interfaces
- Serial con sole interface

1

http://enterprisesecurity.symantec.com/products/products.cfm?productID=49&pageID=820&EID=0
http://enterprisesecurity.symantec.com/content/promotions.cfm?PDFID=47 .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appliance Software (Version 1.5)

- Hardened Linux 2.2 multi -tasking operating system
- Symantec Enterprise Firewall Version 7.0
- Symantec Enterprise VPN Version 7.0

Performance

• Maximum throughput	65 Mbps
• Stateful throughput	>100Mbps
• Recommended network size	up to 2000 nodes

Overview DNS

One of the best sources of information for DNS services of the Symantec Enterprise Firewall can be found in the Internet under http://www.firetower.com/faqs/dns/. People of the development might have writte n this page as they already hint at great problems with DNS configurations. The situation has not changed a lot as talks with the Symantec support in Dublin reveal. DNS was one of the first services that TCP/IP provided and the question is why those proble ms could not be fixed till today. To answer this question we have to go back into the history of DNS and DNS implementation of the Symantec Enterprise Firewall.

As is known the Internet developed from the Advanced Research Projects Agency (ARPA, and later DARPA) created by an US department. The ARPA net used a centrally administered file that held all name -to-address mappings for each host computer connected to ARPA net. The name of this file was `hosts.txt`. This was possible because several computers were connected to the network. When the APRSA net was transformed into the Transmission Control Protocol/ Internet Protocol (TCP/IP) – the Internet we know today – the problems of high traffic, name collisions, consistency etc. lying in this file could not be r esolved. In 1984 Paul Mockapetries released Request For Comments (RFCs) 882 and 883 on a new system called the Domain Name System (DNS). The concept behind DNS was a distributed database architecture. DNS service replaced the `hosts.txt` file in the same year.

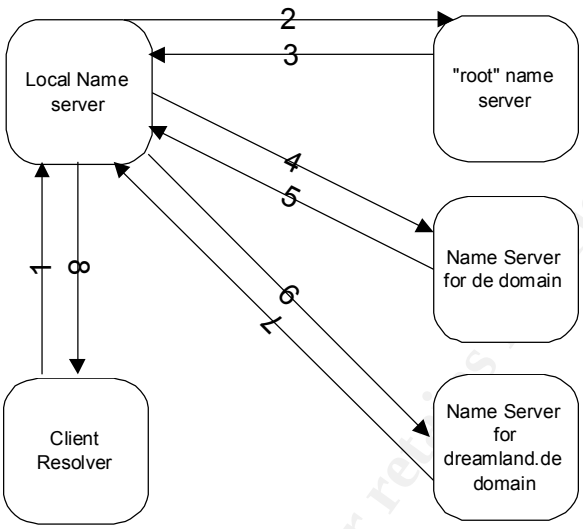
The heart of DNS is the root name server. Currently, the 13 root servers, managed by the Internet Engineering Task Force (IETF), are used as the starting point for the database. Each root server is responsible for keeping track of information on domain names and IP address spaces. Individual entities, called registrars, are organizations that have been given permission to register domain names and update information in the root servers.

But why do we need DNS? Apparently, man can remember names much be tter than numbers but computer can only work with numbers. The transformation of names into numbers is the task of DNS record, for instance the name www.dreamland.de would be transformed into an IP address like 10.1.2.3. The record file can also

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

transform numbers into names and therefore is able to assign the IP address 10.1.2.3 to the name www.dreamland.de. This is called a reverse name resolution. [2]

In short, these are important steps of a DNS resolution:



1.) Query for www.dream land.de
2.) Query for www.dreamland.de
3.) Answer, go to de name server (IP address)
4.) Query for www.dreamland.de
5.) Answer, go to dreamland.de server (IP address)
6.) Query, www.dreamland.de
7.) Answer, go to www.dreamland.de (IP address)
8.) Answer, go to www.dreamland.de (IP ad dress)

Recursive – This form of resolution places the burden on the queried name server receiving the request. The queried name server has to respond with the date or an error indicating the data does not exist. The queried name server cannot respond with a "referral" to another possible source information. Client resolvers issue this type of query.

Iterative – This enables the queried name server to respond by identifying another name server, if it does not have the requested information. A referral respon se provides the name and IP addresses of one or more name servers that should be contacted.

[2] http://www.uspntech.com/dns/ http://www.howstuffworks.c om/dns.htm/printable .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Symantec Enterprise Firewall DNS service

The Symantec Enterprise Firewall is decisively different from other Firewalls in its DNS service. But this is also the cruc ial point where many mistakes in configuration are made. One has to occupy oneself with the setting up of the DNS configuration of the Symantec Enterprise Firewall to come to an understanding how it works. The first thing that needs to be said is that this system can be used for the administration of several hundred zones although it is proprietarily constructed; yet this leads to limitations in the Remote Management Console (RMC as plug in of the Microsoft Management Console (MMC)).

Despite all presumption s one can read in the aforementioned DNS Firetower article that in 1997 an own DNS service was developed in the configuration files of the Windows system. The support teams constituted that Windows NT users with the EagleNT version brought forward most of the DNS inquiries at that time. This is not surprising as Microsoft only started using DNS service for transformation of names internally from Windows 2000 onwards. Before that, Windows worked with the Windows Information Name Service (WINS) and the NetBIO S protocol. Interestingly, many administrators today still do not know how the transformation of names in their Windows networks work. I would like to mention the NetBIOS Broadcast reports here; without this mechanism many networks in Germany would not be able to transform names. Microsoft operating systems use the `hosts` file for name resolution and this is the very file on which the internal DNS service of the Symantec Enterprise Firewall is built on.[3]

The Symantec Enterprise Firewall DNS service is a full y functional DNS name service and proxy. Furthermore, its characteristics as DNS proxy make it very save. Intrusion tools such as teardrop (overlapping fragmentation attacks) that can communicate on UDP port 53 (DNS) can cause much damage in a company and packet filter will not be able to ward of such attacks.

Objectives of the Symantec DNS services

The main tasks of DNS servers are name resolution, reverse name resolution and mail exchange information.

Name Resolution

One feature of DNS service most often used is the transformation of name inquiries into IP addresses. With that IP address the computer can set up a communication.

Reverse Name Resolution

This is the reverse process to name resolution. The DNS service assigns a name to an IP address.

---

[3] http://www.firetower.com/faqs/dns/ .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Mail Exchange Information

Mail server use DNS service to find the correct mail exchange server of a domain. They ask the mail server which belongs to the domain for the corresponding MX records. The DNS server then will send back to the enquirer the appropriate IPs , and the SMTP server sets up a communication with the server via TCP port 25 (default smtp port).

The DNS service of the Symantec Enterprise Firewall - as fully qualified name server - has the feature to cache the received results. You can set the Time to Life (TTL) value in the DNSd configuration of the Symantec Enterprise Firewall. The TTL value is identical with the TTL configuration in a BIND.

Security features of the Symantec Enterprise Firewall

A quite remarkable security feature is the **Split DNS ability** of DNSd networks with connection to the Internet that uses two separate DNS servers. The internal or private DNS server is responsible for name resolution within the internal network. Usually, companies use a manageable amount of domains here. For reasons of security a company will use an external or public DNS server for external communication. The only task of this server is to answer name inquiries from the Internet. Companies use much more domain names for public communication than they do for private, either for themselves or they might also administrate names for partner companies. The DNS proxy of the Symantec Enterprise Firewall unites the dual DNS configuration in one system. I will come back to details of the Split DNS configuration later (page 8).

Another security feature is **Checks the Consistency of all DNS Responses** . When a DNS service makes a reverse lookup on a host, it will verify this result with another inquiry by resolving the name internally and then compare the results. In case that the DNS service answers with a different IP address the server will refuse that answer. In that way documents delivered to the wrong address or wrong configurations are avoided, but also attacks like the cache poisoning attack can be repulsed.

A further security feature is the **refusal of recursive inquiries on the public interface**. The picture on page 3 shows the difference between the iterative and recursive process in a DNS inquiry. DNSd will only accept recursive inquiries of clients to interfaces that are denoted private. All recursive inquiries to the public interface (usually the external interface to the Internet) are refused. That mechanism protects the DNS service from attacks that flood the server with requests and consequently use up system time (DNS service runs in the Userspace). [4]

A last feature to deal with here is the **difference between private and public domains**. As this feature is significant of the DNS service it will be dealt with in detail later on. The use of DNS proxies in the Symantec Enterprise Firewall leads to the fact that all internal inquiries (inquiries to private interfaces) to external name servers are **non transparent**.

[4] dito.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

All those security features can only work when there is no forward record defined on the DNS service. When there is a forward record in the Symantec Enterprise Firewall DNS configuration, data is no longer cached. The DNS service trusts all answers of the DNS server configured as forwarder and will not check them again. For this reason, forwarders should be used very careful and only with correct configurations.

DNS Proxy Files

It has been mentioned before that the Symantec Enterprise Firewall does use the `hosts` and `hosts.pub` files out of historical reasons. Firewall systems that base on OS Windows contain the following files:

```
%SystemRoot%\system32\drivers\etc\hosts
%SystemRoot%\system32\drivers\etc\hosts.pub
```
(where `%SystemRoot%` is typically `c:\WINNT`)

Appliances or Firewall systems based on Solaris:

```
/etc/hosts
/etc/hosts.pub
```

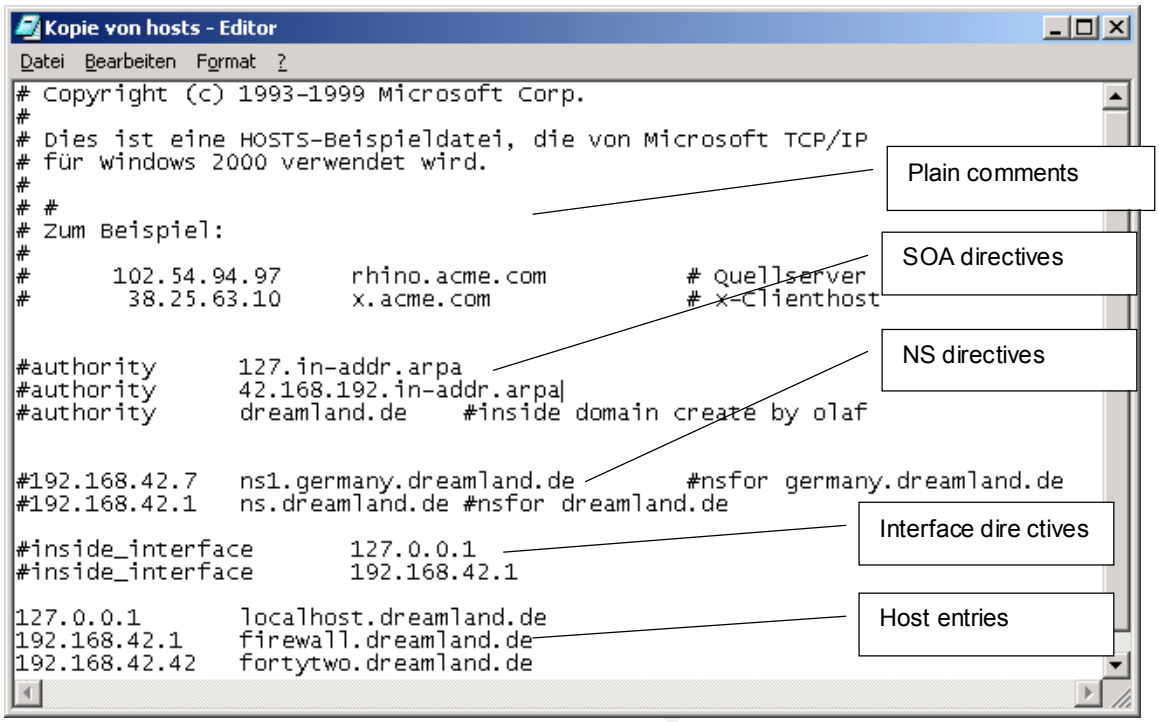
A Firewall differentiates between private DNS service (`hosts` file) and public DNS Service (`hosts.pub`). In the chapter about Split DNS we will look at how those two files work.

Developer of the Firewall had to find a format that could work with both the operating system Microsoft with the *hosts* file and the Symantec Enterprise Firewall. They defined keywords to solve that problem. All words occurring after # are written as comment statements because otherwise the system would interpret them (which would be a mistake). That mechanism assures that the operating system ignores all lines.

On the other hand, Symantec Enterprise Firewall DNS service can interpret those keywords.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



DNS service interprets a Reco rd line automatically as a PTR Record, for example:

192.168.42.42 fortytwo.dreamland.de fortytwo (hosts file entry)

The equivalent to this is

fortytwo.dreamland.de	IN	A	192.168.42.42
42.42.168.192.in-addr.arpa	IN	PTR	fortytwo.dreamland.de

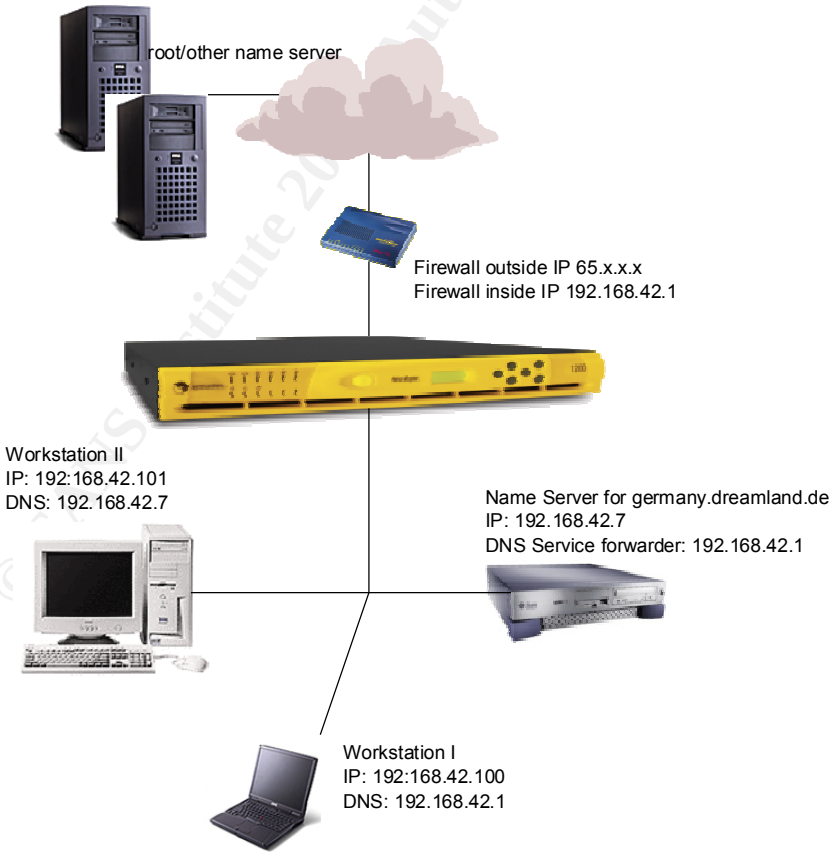
In this case, DNS service would ignore the first 12 lines (# characters!). In the 13th and 14th line it will set up an inverse zone in each line: 127.in-addr.arpa and 42.168.192.in-addr.arpa. The 15th line will be interpreted as forward zone dreamland.de. In the 18th and 19th lines it will set up the name server for the domain germany.dreamland.de, namely ns1.germany.dreamland.de (192.168.42.7), and the name server for the domain dreamland.de, which is ns.dreamland.de and, at the same time the firewall. In the 21st and 22nd lines you can find all interface which are private (important for the dual level DNS) and in the 24th, 25th and 26th lines will set up some A record (with PTR records).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Employed Keywords

Keyword	Description
inside_interface	Determines which interfac e belongs to the private Lan. This is important for the function Split DNS.
forward_to	Determines the next name server. You can only use three forwards as there is a bind v4.9 integrated.
root_server	Overwrites the default root server of the OS TCP/IP stacks.
recurse_for	Tells DNS service for which network segment it works as recursive name server.
Authority	Defines the SOA Record.
subnet_map	Allows the definition of non octet boundary inverse zones (also see CIDR [5]).
Mxfor	Defines the mail exchange se rver (MX record).
Nsfor	Defines the name server for one or more that one domains.

The following picture shows a typical DNS case in a medium -seized company, which is based on the aforementioned `hosts` file:



[5] http://www.spiritone.com/~nabil/netmask.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Workstation I wants to resolve a name. The Firewall is defined as DNS server in the TCP/IP configuration. When Workstation I has an inquiry for the domain dreamland.de the Firewall DNS service will answer. But if Workstation I has a request for the domain germany.dreamland. de, the name server 192.168.42.7 will answer. Yet if the workstation inquiries www.sans.org DNS split concept comes into force (we will look at that in detail in the following chapter) and the DNS service of the Firewall will answer the inquiry.

Workstation II puts all DNS inquiries forward to the internal DNS server ns1.germany.dreamland.de, which can answer all inquiries for the domain germany.dreamland.de. All other inquiries either for dreamland.de or www.sans.org will be delegated directly to the Firew all by the forward definition. The Firewall will answer directly or through an iterative process.

Dual-level DNS or Split DNS

One security feature of the Symantec Enterprise Firewall is the fact that the DNS service works as dual-level DNS. But what exactl y is a dual-level DNS? It simply means that the DNS contains two DNS processes, namely the public and the private process. The public DNS process receives its data from the `hosts.pub` file, whereas the private DNS process receives its data from the `hosts` file. Only systems that send their inquiries via private interfaces are allowed to use the private DNS process. The most important difference between both is how they run DNS inquiries.

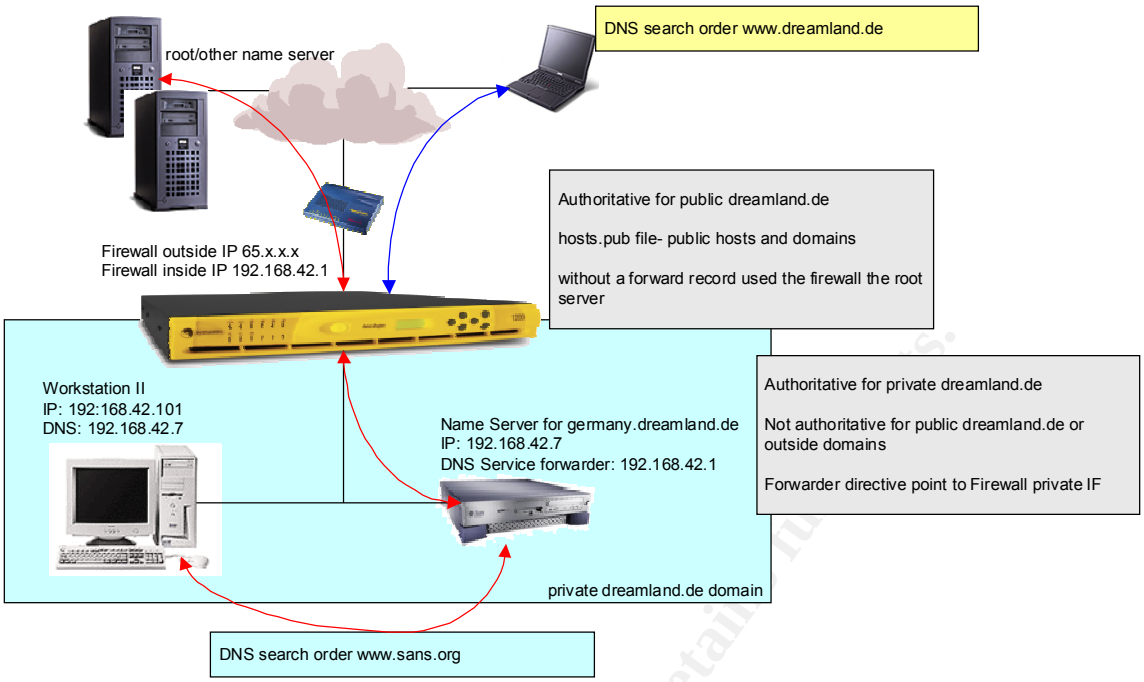
Public DNS or the `hosts.pub` (queries in blue)

Requests from the Internet will be answered when the Firewall is defined as DNS server. The public DNS service can only answer queries with information contained in the *hosts.pub* file (A record, MX record, PTR record, etc.) or information obtained from other name servers for this d omain (NS record).

Private DNS or the `hosts` file(queries in red)

Requests will go to private interfaces. Is this DNS server not able to answer them, for instance because it requested www.sans.org, the query will be forw arded to the public DNS service. If even the public DNS service cannot answer, it uses a forward record (if there is one defined) or tries to contact root server (default). If there is still no answer, the name or the IP cannot be resolved.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Disable the DNSd and use the udp_gsp 53

In some cases you must disable the DNSd if you work with your own DNS service. A name server has to be defined in the `/etc/resolv.conf` file and to be checked for its functions because services of the Symantec Enterprise Firewall also use name resolution. The place for this system is in your DMZ and service network. In an Enterprise solution you have different problems with this option:

1.) In the Symantec Enterprise Firewall 7.0. (build 1 and 2) version y ou can't enable the server to server (port 53 to port 53) udp_gsp and client to server (port 1024-65535 to port 53) udp_gsp. With this setting you will find a typical error message from the best-fit daemon in your logfile. A possible solution for this scenario is that you define a udp_gsp port 0-65535 to port 53 and use only this gsp without the server to server protocol.

2.) In a network with heavy load you must define new network parameters in your Symantec Enterprise Firewall/Veloci/SGS `config.cf`. The problem of DNS is the very short request time (typical) for a DNS question from your DNS server to your ISP and in a short time the firewall has a lot of UDP connection. These connections consume more and more memory. The variable `udp-gsp.timeout` controls the time-out for UDP connections using the Generic Service Passer (GSP). If no data flows for this period of time, the connection is closed. The default value is 3600 seconds. This is too long for a DNS request. In this case you can use the variable `usp-gsp.53.timeout=30` (or 15) seconds which overrides the general UDP GSP time-out. But you must check all your settings with `nslookup` if your timeout value is not too short. With `vmstat` you check your memory management. In this case please increase this value![6]

[6] http://service1.symantec.com/SUPPORT/ent-gate.nsf (please search to dns)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Performance tuning

Typical for a heavy load firewall are performance problems. In the following I would like to discuss some solutions.

Symantec Enterprise Firewall performance issues are traditionally found in CPU utilization and/or memory consumption. Link utilization is of some concern, but is not considered a function on the Symantec Enterprise Firewall, rather a function of the network topology.

On application servers, disk utilization is a potential issue, but not likely on the Symantec Enterprise Firew all. The disk on the Symantec Enterprise Firewall is used for logging and virtual memory management. High disk utilization only results when the system lacks sufficient memory and starts thrashing due to high paging and eventual swapping rates.

If the system is performing poorly, it is typically due to the queue delay for CPU and memory. You will see the results in poor response times.

Any process running at full utilization may potentially freeze. The system freeze occurs when resource consumption exceed s the operating system's ability to keep its many processings.

The general objectives of tuning proxies are to reduce memory consumption and to reduce the path length for packet processing. Path length is the amount of instruction required to process a pa cket. Path length reduction is usually accomplished by minimizing the instructions executed in the application. The primary ways to reduce path length are:

- Run selected proxies in the kernel instead of the application space.
  - Disable application data scann ing for HTTP, FTP, TCP GSP and Telnet
- Filter packets to minimize packet flow to the proxies.

Other considerations for tuning proxies are related to high memory consumption. On Solaris and Linux systems, the Firewall optimises proxy execution by spawning temporary proxies (child processes) when the activity on a proxy reaches a particular level. This level is the number of threads allocated to the proxy.

By default, the maximum number of threads a proxy instance can use is 32. If you have memory problems, you can increase the number of threads available to a proxy to reduce the memory consumption that would otherwise be incurred due to the spawned child processes. Please use these settings in the `config.cf` file to control child processes:

`httpd.csvr.max_co nnections_served=10000`
(Maximum number of connections served by a child processes before it is terminated. The default setting is 1,000,000)
`httpd.csvr.max_procs=72`
(Specifies maximum number of child processes allowed in the system for the HTTP proxy. The default setting is 32)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

`httpd.csvr.forced_death=1`
(Force a child process to terminate even if a thread is active. If this value is true, the default setting for this parameter is 60 seconds)

To continue with these settings you can use the following variabl es.
`driver.Global.Max_Memory=33554432`
(increases the Symantec driver memory from 16 MB to 32 MB)
`driver.Global.Tcp_Idle_Timeout=120`
(defines the idle timeout, in seconds, for TCP connections with no activity.)

Turning off DNS reverse lookups can also help to reduce the performance load. Please note that the SMTP proxy performs reverse lookups, regardless of the configuration setting for DNS reverse lookups.

Please check all your changes with `vmstat` and `netstat`, for example:

```
vmstat -n 5 10[7]

netstat -an | grep tcp | awk {'print $6'} | sort | uniq -c[8]
```

No application Data Scanning

The Symantec Enterprise Firewall allows you to disable the proxy's default operation of scanning of application data. This can be done to increase overall system performance. This feature is effectively implemented in two kernel -level routines called Fastpath and kernel proxy. Fastpath and kernel proxy are program execution facilities that run in the kernel. Eliminating process -level data scanning, but also context switching betwe en kernel mode and user mode reduced improve performance. The option of using no application data scanning is available for a limited number of proxies.

The Fastpath support can be used for:
- HTTP

The Kernel proxy support can be used for:
- HTTPS
- FTP
- Telnet
- TCP single port GSP
- TCP all ports GSP

Also other proxies can use the feature disable "application data scanning". The Symantec driver manages all subsequent data flow for the connection. In general, the Symantec driver is responsible for all data fl ow until the connection ends or times out. The disabling of the application data -scanning component of the Symantec

---

[7] http://www.canberra.edu.au/~sam/whp/awk -guide.html.

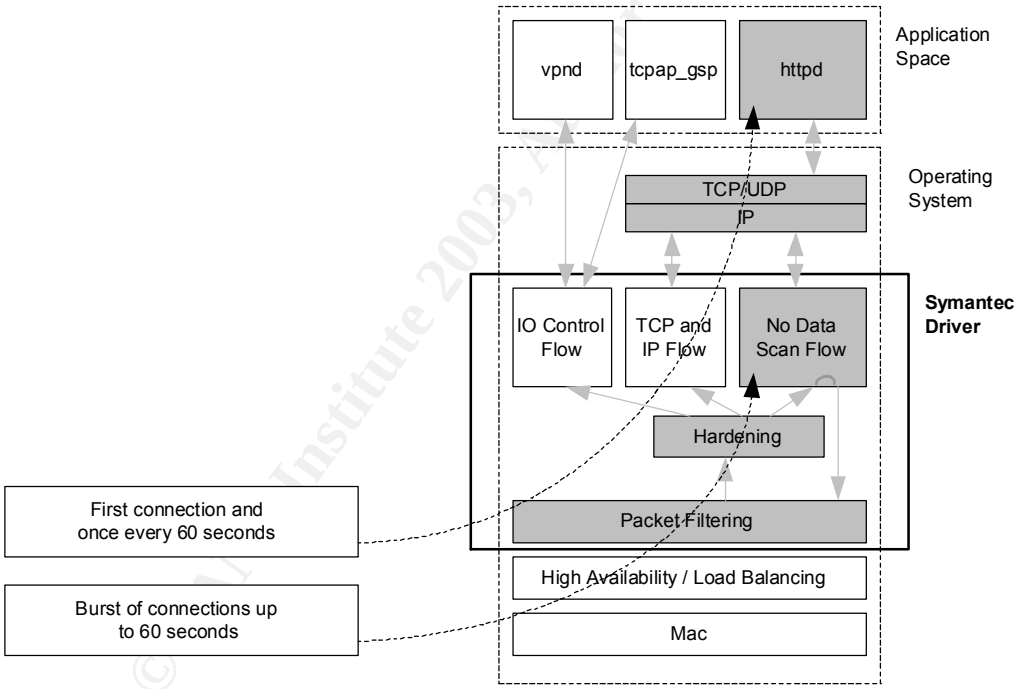
[8] http://snowhite.cis.uoguelph.ca/course_info/27420/netstat.html .
http://maclux-rz.uibk.ac.at/~maillists/sec urity-basics/msg03098.shtml .
http://www.canberra.edu.au/~sam/whp/awk -guide.html.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

driver uses the cache information of the connection to detect data packets that are to be serviced by the Fastpath and kernel proxy routines . After a packet has successfully passed through system hardening the packet is evaluated to determine whether it will progress to VPN processing, proxy processing or no data scanning processing. The source and destination IP addresses are compared against the no data scanning cache and if there is a match, then the destination port number is checked. If the destination port also matches, then the packet is considered either a Fastpath or kernel proxy packet. Which kernel -level routine is used depends on th e specific protocol type. The Symantec driver then forwards the packet without any additional analysis. The Symantec driver uses a cached copy of the routing table to determine the next hop address for the packet and then queues the packet to the appropriate interface for transmission. [9]

HTTP Fastpath

If you use this feature, please note that many HTTP data security checks are eliminated, but system hardening still occurs. The SYMANTEC ENTERPRISE FIREWALL clears the cache after a short period of time (60 s econds by default), so the HTTP proxy will re-evaluate connection attempts for allowed source and destination entities.



FTP Kernel Proxy

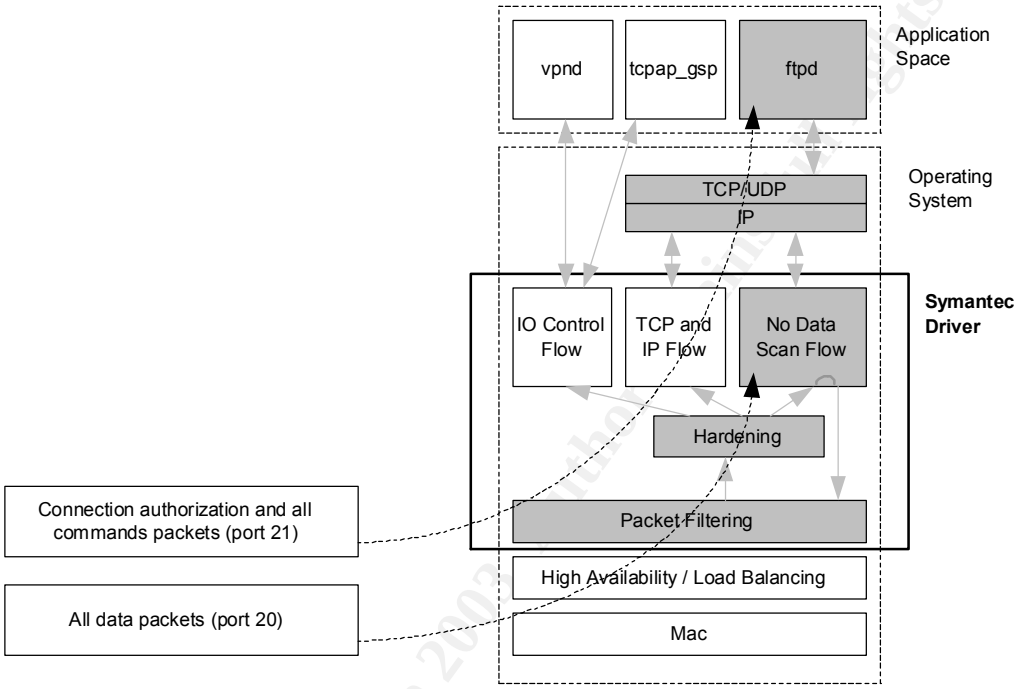
The kernel proxy for FTP recognizes the two different port numbers used in FTP communications. FTP uses port number 21 for commands and port 20 for data transfer. Once a no data scanning connection has been established, the following events occur:

[9] http://maclux-rz.uibk.ac.at/~maillists/security -basics/msg03098.shtml .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Packets containing a destination port number if 21 are always sent up to the process-level FTP proxy.
- Packets containing a destination port number of 20 are managed by the kernel proxy routine.

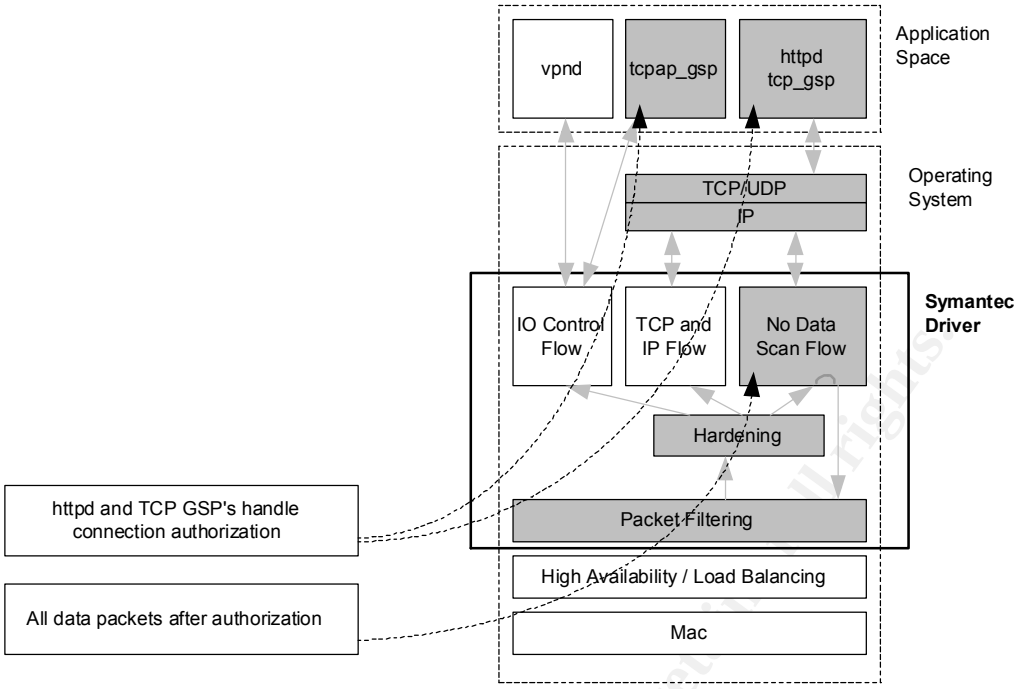
Please note that the FTP kernel proxy is secure. All FTP commands are still serviced by the process-level proxy. File transfer data is the only type of FT P traffic using the kernel proxy.



HTTPS and TCP GSP Kernel Proxy

HTTPS and TCP GSP protocols are similar in how application data scanning is implemented and in that application data scanning does not need to be applicated. By the nature of these protocols, data scanning makes no sense for either protocol: In the case of the TCP GSPs (tcp_gsp and tcpap_gsp), they have no knowledge of the application headers of the protocols they are managing. In the case of HTTPS, since an SSL connection implies the data encrypted, the HTTP proxy cannot perform data scanning. Therefore, using the kernel proxy feature for HTTPS and TCP GSPs does not introduce additional security compromises. For HTTPS (SSL) and TCP GSP protocols, the process-level proxy manages the initial connection request. Any subsequent packets are managed by the kernel proxy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Please note that HTTPS uses kernel proxy by default. If y ou are experiencing reduced firewall performance when processin g HTTPS (SSL) traffic is used and you also see a log message similar to the following: "message 630: component:kernel critical memory purge which started with xxxxxxx bytes and ended with xxxxxxx bytes will cause lost packets.“ then define in the `config.cf`[10]:

```
httpd.tls_kernelproxy=0
```

☺

[10] http://maclux-rz.uibk.ac.at/~maillists/security -basics/msg03098.shtml

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

List of references

Veloci Raptor
http://enterprisesecurity.symantec.com/products/products.cfm?productID=49&pageID=820&EID=0
http://enterprisesecurity.symantec.com/content/promotions.cfm?PDFID=47 .

Overview DNS
http://www.uspntech.com/d ns/
http://www.howstuffworks.com/dns.htm/printable

Symantec Enterprise Firewall DNS service
http://www.firetower.com/faqs/dns/ .

Objectives of the Symantec DNS service
http://www.firetower.com/faqs/dns/ .

DNS Proxy Files
http://www.accs-net.com/hosts/how_to_use_hosts.html
http://www.spiritone.com/~nabil/netmask.htm

Disable the DNSd and use the udp_gsp 53
http://service1.symantec.com/SUPPORT/ent-gate.nsf

Performance tuning
http://www.canberra.edu.au/~sam/whp/awk-guide.html
http://snowhite.cis.uoguelph.ca/course_info/27420/netstat.html
http://maclux-rz.uibk.ac.at/~maillists/security-basics/msg03098.shtml
http://www.canberra.edu.au/~sam/whp/awk-guide.html

No application Data Scanning
http://maclux-rz.uibk.ac.at/~maillists/security-basics/msg03098.shtml

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.