FORSCHUNGSZENTRUM JÜLICH GmbH
Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Technical Report

High-speed Firewalls: A Market Analysis

Markus Meier, Egon Grünter, Ralph Niederberger,
Thomas Eickermann

FZJ-JSC-IB-2008-06

September 2008

(last change: 25.09.2008)

D-Grid Integration project (DGI)

D-Grid Integration report for Area 3-5

High-speed Firewalls:
A Market Analysis
(August 2006)

Authors
Markus Meier, Egon Grünter, Ralph Niederberger, Thomas Eickermann (JSC, Forschungszentrum Jülich)

This report has been financed in part by the Federal ministry of Education and Research under grant number 01AK800B. The authors of this report are responsible for its content.

Content

1. Introduction

A (network) firewall is a system that separates two networks and controls access between them. Most firewalls are used to protect an internal network from access from the public Internet. A firewall prohibits unauthorised access to systems and networking resources by analysing incoming packets and comparing these to a locally defined access list. Current firewall systems go beyond processing packets on a per-packet basis, which restricts access according to ports and IP addresses only, and can be configured to process packets as part of a network session. Often VPN functionality and/or content-based filtering are provided by also examining the packet data. With these techniques, it is possible to filter ActiveX or JavaScript from requested HTML pages. These „deep inspection"-properties may, however, lead to a performance degradation of the firewall system.

A short market analysis has been initiated to give recommendations to D-Grid partners concerning firewall systems. The analysis has been done based solely on information from developer web-sites and advertisement pages. The analysis has concentrated on requirements for high-speed firewalls, because these are considered to be important according to a questionnaire done within the D-Grid community.

1.1 Core-D-Grid questionnaire

The Core-D-Grid questionnaire concerning firewall systems shows that more than 70 % of the interviewed institutions require an aggregated throughput of 10 Gbit/s (Figure 1). The throughput per interface port is less important. Only 25 % of those questioned reported that 10 Gbit/s per interface would be needed.

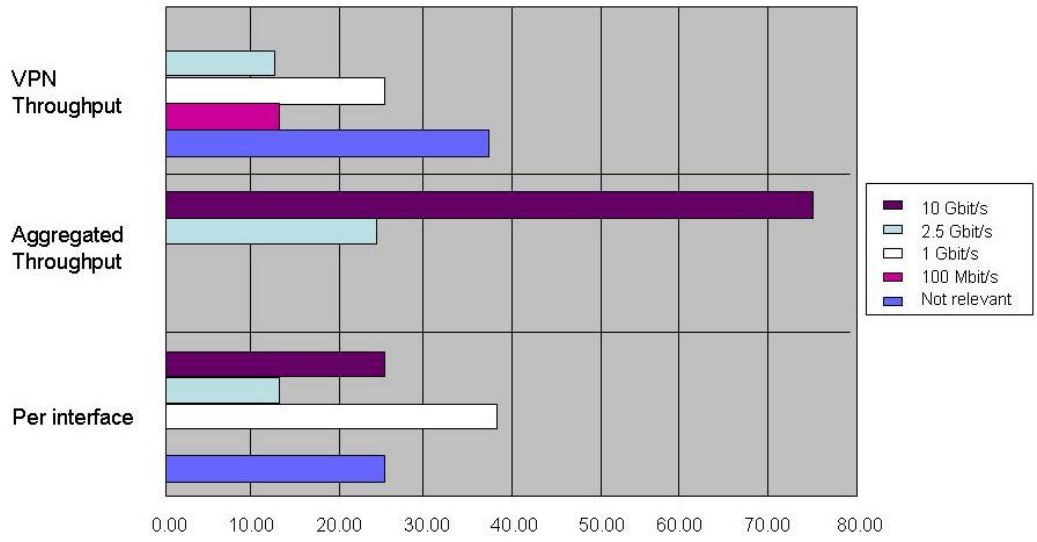

Figure 1: Throughput requirements

Furthermore, some additional features that the system must provide have been named by some D-Grid partners. Figure 2 shows that a „hot-standby"-solution is strongly required. Nearly 90 % rated high availability as being highly essential when ordering a

new system. Other techniques such as VPN-functionality or intrusion detection are not viewed as being necessary, but would nevertheless be appreciated.

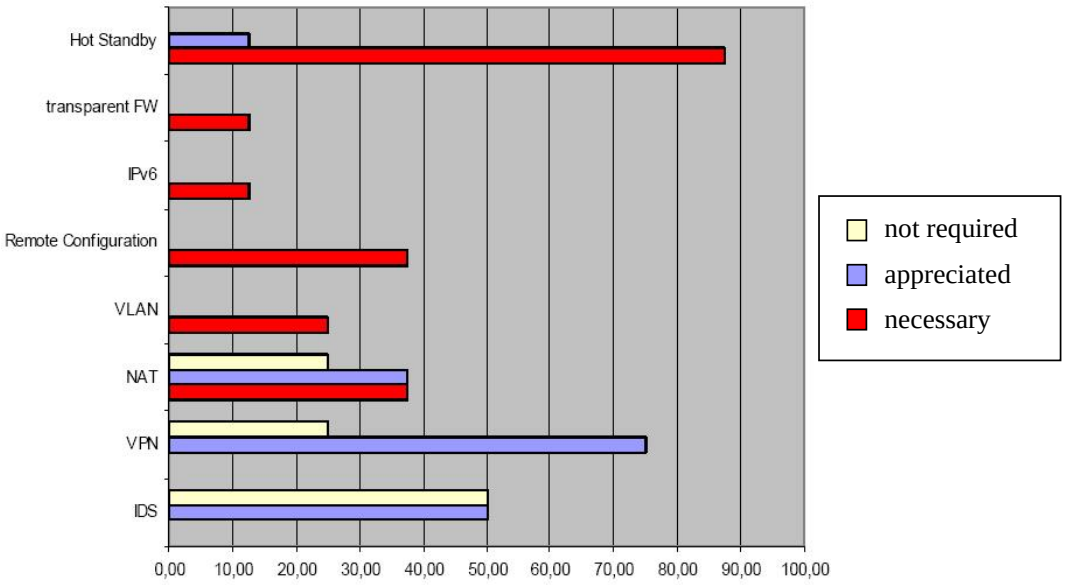

Figure 2: Additional functionalities

Figure 3 provides information about which protocols (above layer 4) the system has to support. Furthermore, multicast support has been included, since this protocol is often used within grid environments.

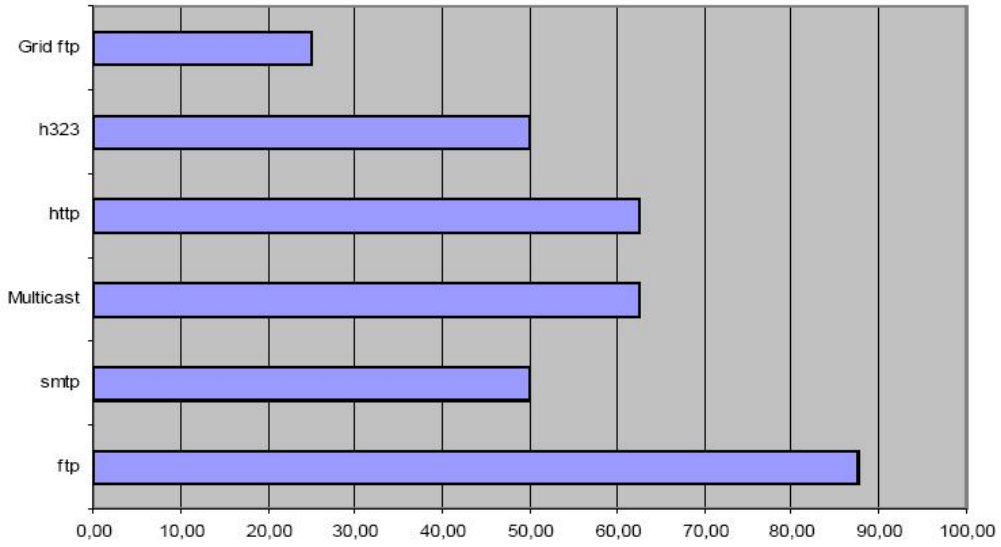

Figure 3: Application protocols to be supported

2 Market Analysis

Some D-Grid applications require high bandwidth (up to 10 Gbit/s) and thus high firewall throughput. Currently only a few systems are available that can deal with this aggregated throughput and even fewer can provide a 10 Gbit/s interface. Most systems only provide data rates above 3 Gbit/s by load-balancing traffic on several interfaces. The following pages give a short overview of the appliances available today. Products not applicable for D-Grid applications, e.g., those not providing adequate throughput, will not be covered by this study.

2.1 Astaro AG

Astaro AG was founded in 2000 to develop highly integrated network security solutions. The product line Astaro Security Gateway provides protection from many security risks and can be ordered as software solution or hardware appliance. The top product of the Astaro Security Gateway series, the model 525, can be used in environments having 1,000-2,000 users.

2.1.1 Astaro Security Gateway 525 / 525F

The Astaro Security Gateway 525 appliance is equipped with two Intel Xeon processors running at 3.2 GHz, 4GB DDRII main memory, two 120 GByte Serial-ATA discs and a RAID-Controller. The discs are hot-swappable and are used for storage of suspicious data as well as log data. The appliance securing the network against viruses, spam, and internet attacks is equipped with 10 GigE copper ports. Furthermore, a management port and two USB-Ports are available. The system throughput is given as 3 Gbit/s for uncompressed data. 400 Mbit/s can be processed if data is encrypted, e.g., VPN connections. It is possible to have 1,000,000 open connections in parallel, independent of the VPN tunnels assigned. A data base of 60 categories is provided to identify internet attacks. Due to a hardware accelerator card, security functions such as decompression and pattern recognition are executed very quickly. A web interface allows fast and easy installation and administration. Support of virtual LANs (VLANs) has been announced for smaller versions of the ASG, but this feature is not available for the 525 system. A QoS-management for providing reserved bandwidth or filtering at layer 2 is integrated. A second appliance type, ASG525F, has equal performance metrics and security functions and can be ordered with four copper ports and six SFP-Gbic fibre ports.

2.2 Check Point (Nokia Appliance)

Nokia firewall/VPN-appliances are based on security-optimized, custom hardware developments using Check Point's firewall software.

2.2.1 Nokia IP2255

The Nokia IP2255 appliance is a flash-ROM-based high-speed firewall that is optimised for the Check Point firewall software. It supports a firewall throughput of up to 8.9 Gbit/s. Up to 87,000 connections per second can be established or torn down. The VPN performance is about 2.3 Gbit/s. The appliance provides four slots for optical connections. Additionally to the four already available GigE ports, eight-port FE, four-port GigE or single-port 10 GigE interface cards can be installed. VLANs are supported, but functionality options are not described in more detail.

Kommentar [dw1]: richting?

Two hot-swappable power supplies and fans as well as the flash-ROM-based design provide a high operational availability and resilience. A statefull failover-mode can be realised by using two IP2255 firewall systems. The IP2255 system can be administered through a Web interface or a command-line interface (CLI). SNMP up to version 3 can be used for reporting and monitoring.

Kommentar [RRN2]: Siehe oben

2.3 Cisco Systems

The Cisco PIX Security Appliance is a phased-out model and therefore will not be considered here.

2.3.1 ASA 5500 Serie (Adaptive Security Appliance)

The Cisco Systems ASA product-line systems provide only up to 1.2 Gbit/s throughput (ASA 5550) and will not be applicable for transmission speeds greater than 1 Gbit/s. Load balancing with this system would be possible, but would result in a degraded performance of the systems, so that the throughput would not generally be much better. The VPN throughput is about 360 Mbit/s (ASA 5550), again assuming load-balancing of multiple systems. The largest model has eight GigE interfaces. There is also the possibility of using an IPS module with up to 450 Mbit/s throughput in all these models, except for the ASA 5550.

2.3.2 Catalyst Firewall Service Module

The Firewall Service Module (FWSM) is an integrated firewall for the Cisco Catalyst 6500 switches and the Cisco 7600 router Series. Up to four modules can be used within one Catalyst switch/router, each having a throughput of up to 5.5 Gbit/s or 2.8 million packets per second (Mpps). A theoretical performance of up to 20 Gbit/s can be reached using four such modules. Setup and teardown of up to 100,000 connections per second having 1,000,000 sessions running in parallel is possible. It is possible to protect each port of a switch or router after having installed one FWSM into the system. The FWSM can be used in a Failover Mode when combined with a second FWSM installed in the same or another switch / router system. Up to 1,000 VLANs can be supported per FWSM. The FWSM can be used either in a layer-2 transparent mode or as a typical layer-3 firewall in routed mode. It allows a web-based configuration (Cisco Device Manager) or configuration via CLI. Logging and monitoring can be configured for syslog messages, SNMP or via Cisco proprietary monitoring tools.

2.3.3 Application Control Engine Module (ACE)

Cisco Systems provides another chassis-based solution with the Application Control Engine Module (ACE). The ACE module is used inside the Catalyst 6500 switch series and allows 4 Gbit/s, 8 Gbit/s or 16 Gbit/s throughout, dependent on the licences ordered. This throughput rate will be reached when processing 6.5 million packets per second. Throughput can be increased by using up to 4 ACE modules per Catalyst switch. The ACE module is able to handle 345,000 connections per second having 4,000,000 parallel connections open. Up to 4,000 virtual networks can be handled. Security can be enhanced by configuring different security levels (e.g., deep inspection), but this leads to decreased performance. Additionally, the module can be used as load balancer for multiple Firewall-Service-Modules. This allows integrating the ACE module into an already existing firewall environment in order to enhance the data throughput.

Formatiert: Tabstopps: 10,16 cm, Links

2.4 Clavister

Clavister provides proprietary, technology-based firewall, security gateway and VPN-solutions. A main goal of the Clavister products is the provision of a comprehensive security solution.

2.4.1 Clavister Security Gateway 4400 Series

The Clavister Security Gateway 4400 Series has been designed as a central gateway for VPN networks and computer centres. The SG 4400 can be ordered as four different models having various performances. We consider only the largest appliance, the SG-4470. This supports functionality as an application-layer firewall and as an IDS/IPS in parallel. It delivers a 4 Gbit/s throughput on unencrypted connections and 1 Gbps VPN throughput with AES and 3DES encryption. Up to 1,000,000 simultaneous connections with 10,000 VPN tunnels in parallel are possible. An integrated bandwidth management allows setting the guaranteed and maximum bandwidth levels. Ten physical interfaces (eight SFP, two 1000BASE-TX) are available and can be used for up to 4,096 virtual LANs. Hot-swappable power supplies and fans guarantee the maximum availability. A clustering of multiple appliances is also possible. Lastly, the SG4470 can be used in the “routed” as well as in the “transparent” mode.

2.5 Fortinet

Fortinet was established in 2000 and focuses on the development of security solutions for networks. The Fortigate product family uses a hardware-accelerated, ASIC-based architecture and supports both network services such as firewall, VPN, and IDS, and services at the application layer such as virus protection, anti spam and content filtering.

2.5.1 FortiGate 3600

The Fortigate 3600 firewall is the largest appliance in the Fortinet portfolio. The firewall throughput of the FortiGate 3600 systems is about 4 Gbit/s using clustering techniques. 25,000 new connections per second can be processed, having up to 1,000,000 connections open in parallel. The system allows up to 5,000 dedicated VPN tunnels processing traffic at a throughput of 600 Mbit/s (128-bit 3DES encryption). One management port with FE as well as six GigE interfaces (two copper, four fibre) are available. A hot-swappable functionality with redundant fans and power supplies is integrated. Furthermore, it is possible to run the system in two stateful-failover modes: active/active or active/passive. Log data can be stored on an internal 20 GB disc. Syslog messages, E-Mail, SNMP as well as graphical monitoring in real time for operational purposes can be generated and used. The configuration of the system takes place with a CLI at the serial port or via a WebUI.

2.5.2 FortiGate 5000 Serie

Compared with the FortiGate 3600, the FortiGate 5000 product line is not an independent appliance, but instead a chassis-based security system. Three different types of system are available. The FortiGate 5020 offers two slots, the FortiGate 5050 allows five slots, and the FortiGate 5140 has 14 slots. Included in

the FortiGate 5000 product line are the FortiGate 5001 and FortiGate 5005 antivirus firewall module and the FortiGate 5003 switch blade. Advanced connectivity possibilities can be used by including a plug-in-module. This module can be equipped with two 10 GigE or eight GigE interface ports. The controller supports furthermore switch-based connections for traffic distribution onto multiple firewall blades, allowing load balancing. The firewall throughput capacity of one blade is 4 Gbit/s for the FortiGate 5001 model and 5 Gbit/s for the FortiGate 5005 model; the latter provides a VPN throughput of 600 Mbit/s as well. 2,000,000 parallel open connections can exist (1,000,000 for the FortiGate 5001) and 5,000 VPN tunnels. The FortiGate 5001 blade has four SFP ports and four 10/100/1000 Base-T ports; the FortiGate-5005 has eight SFP ports onboard. In addition to firewall and VPN functionality, the Fortinet 5000 product line also offers virus and spam protection, web filtering and intrusion prevention. Additionally, all FortiGate systems automatically download current signatures from vendor-specific anti-virus and intrusion-detection data bases. Administration and configuration can be done by a WebUI (multi-language), a CLI or from a proprietary management system. A transparent mode configuration and operation allows easy integration into an already existing infrastructure.

2.6 Juniper Networks

Juniper Networks is one of the leading developers of network solutions. Their main experience has been in designing professional routers and IP security. Through the acquisition of NetScreen, Juniper has become known for high-speed firewall systems as well.

2.6.1 NetScreen-5000 product line

The Netscreen product line offers firewall solutions for any company. The Netscreen-5400, with its 30 Gbit/s firewall throughput (18 Mpps), can be classified as one of the most powerful systems within the high-performance firewall market. The smaller system Netscreen 5200 also offers at least 10 Gbit/s throughput. The systems are designed modularly with four (5400) or two (5200) free slots. These slots accept management modules or interface modules with up to six 10 GigE ports or 24 GigE ports. Both systems offer integrated VPN and traffic management functionality and protect the network against DoS and DDoS attacks. The VPN throughput is rated at 15 Gbit/s (3DES encryption) for the Netscreen 5400 and 5 Gbit/s for the Netscreen 5200. The appliance is able to support up to 25,000 tunnels and/or 1,000,000 TCP sessions in parallel. Both systems support 4000 VLANs and up to 500 virtual firewalls. The NetScreen-5000 product line is based on a GigaScreen-II ASIC processor. This processor, custom-developed by NetScreen, is specified to offer better performance and more scalability, functionality, and programmability compared to commonly used silicon chipsets. Each GigaScreen-II ASIC can handle a firewall throughput of more than 1.7 million data packets per second and up to 2 Gbit/s, as well as a 3DES IPSec VPN throughput of more than 1 million data packets per second at 1 Gbit/s. The appliance can be used in active/active- as well as active/passive-mode with stateful-failover functionality. For monitoring purposes, SNMP (v1 and v2), E-Mail and syslog are offered.

2.7 Secure Computing

Secure Computing has in business for about 20 years. At the end of 2005 it acquired its competitor Cyberguard, which had specialised on proxy/deep-inspection firewalls. The Cyberguard TSP 7300 system is designed for midsize companies and is the biggest appliance offered by Secure Computing.

2.7.1 Cyberguard TSP 7300

The Cyberguard TSP 7300 appliance has been designed for the high-end sector and offers multiple security applications. The hardware is built around a dual-core AMD multiprocessor. The overall performance for packet filtering is about 10.2 Gbit/s (UDP) and 3.9 Gbit/s (TCP). The application-layer inspection throughput is rated at 2.1 Gbit/s. The protocols scanned are, e.g., ftp, h.323, http, https and smtp. The appliance protects against DoS attacks. URL filtering is also supported. Starting with release TSP 6.4, an anti virus software and spam filtering can be optionally activated. 32,000 connections can be established / toren down, having a maximum of 2,000,000 open sessions. Up to 25,000 encrypted VPN tunnels with a data rate of 1.2 Gbit/s can be established using 3DES and 1.4 Gbits/s using AES encryption. The standard configuration comes with 14 GigE copper ports and 24 GigE fibre ports. Virtual LANs are also supported. The system can be managed and configured using a web-based GUI (via https) or a CLI (using SSH). Redundant fans, power supplies and discs are integrated to ensure high availability. The TSP 7300 system can be used in active/passive failover mode without interrupting any running sessions. Additionally, clustering of multiple appliances is supported. For logging purposes syslog, E-mail and SNMP can be used.

2.8 Stonesoft

Stonesoft Corporation was founded in 1990 and is a corporation acting worldwide with a focus on network security. Stonesoft offers comprehensive solutions for security, high reliability and network management.

2.8.1 StoneGate-4000

The model SG-4000, built on a hardened Linux operating system, is a firewall appliance offering VPN concentrator functionality. Being the most powerful Stonesoft appliance, it can process a maximum of 3.1 Gbit/s firewall throughput. The VPN data rate is about 500 Mbit/s. The 22 GigE copper interface ports allow up to 500,000 sessions in parallel. Each port supports up to 4,096 virtual LANs. An integrated load balancing technology allows a constant availability and resiliency of all sessions. The patented multilink functionality offers a parallel connection to different ISPs for Internet connectivity and VPN, which provides optimal network performance. Clustering several SG-4000 systems ensures a high availability. Stonesoft offers a central management instance to allow secure remote management as well as remote update facilities and alarming (syslog, file logging). Defective hardware modules such as power supplies, fans or discs are hot swappable.

3 Overview

The following table gives an overview of the systems investigated in this study

System	Astaro ASG 525	Nokia IP2255	Cisco ASA 5550	Cisco FWSM	Cisco ACE	Clavister SG 4470	FortiGate 3600	Fortgate 5005	NetScreen 5400	Cyberguard TSP7300	StoneGate-4000
Throughput (Gbit/s)	3	8.9	1.2	5.5	4, 8, 16	4.0	4.0	5.0	30.0	10.2 UDP; 3.9 TCP	3.1
VPN throughput (Gbit/s)	0.4	2.3	0.42	-	-	1.0	0.6	0.6	15.0	1.4 AES; 1.2 3DES	0.5
Interfaces Gbit / 10 Gbit	10 / 0	4 (20) / 0 (4)	8 / 0	-	-	10 / 0	6 / 0	8 (16, 24) / 0 (2, 4)	24 / 0 ; 0 / 6	14 (24) / 0	22 / 0
Maximum sessions supported	1.000.000	-	650.000	1.000.000	4.000.000	5.000.000	1.000.000	2.000.000	1.000.000	2.000.000	500.000
Sessions per second	-	87	28.000	100.000	345.000	-	25.000	-	19.000	32.000	n.i.a.
max. VPN tunnels	1.000.000	-	5.000	-	-	10.000	5.000	5.000	25.000	25.000	n.i.a.
max. VLANs	-	j (n.i.a.)	200	1.000	4.000	4.096	-	-	4.000	n.i.a.	4096
Load Balancing / Clustering	-	- / j	j / j	j / j	J / j	-	- / j	j / j	j / j	- / j	j / j
Redundance / Failover	j / -	j / j	- / j	j / j	J / j	- / j	j / j	j / j	j / j	j / j	j / j
IDS / Virus / Spam	j / j / j	n	n	n	n	n	j / j / j	- / j / j	n	- / j / j	n
Layer 2 / 3	j	-	j	j	-	j	j	j	j	-	j
Management	web	web / cli	web / cli	web / cli	web / cli	web / cli	web / cli	web / cli	web / cli	web / cli	java-gui

4 Load balancing

This report has shown that most currently available firewall systems offer a throughput between 3 and 6 Gbit/s. (Appliances with higher traffic throughput use load-balancing techniques.) Requirements for throughput greater than 10 Gbit/s can be fulfilled by using specialised solutions only.

Typically, firewalls are positioned on the campus edge and secure the whole internal infrastructure. A single system can be seen as a single point of failure, i.e. failure of the firewall removes the organisation from the public Internet. Therefore, most firewalls are configured in a so-called failover constellation.

This design uses two identical systems, one system in active mode working as the firewall and the other working in standby mode, only becoming active in case of failure of the first one. Having two identical systems installed, it makes sense to use both in parallel with load balancing. Load balancing can be realised in different ways.

Multiple firewalls can be clustered as a firewall farm. One becomes the master firewall, delegating traffic to the others. The following figure illustrates this.

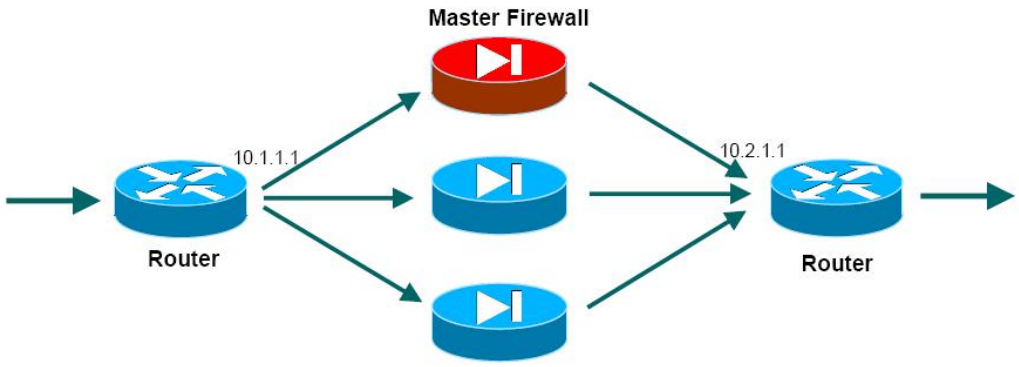

Figure: A firewall farm with a master firewall and two routers

The load balancing will be described in detail below. The router 10.1.1.1 sends incoming traffic to the master firewall. The master firewall now decides which firewall will deal with this session traffic by using the IP address and port information of the protocol header as the key for a hash algorithm. Then the master firewall sends an ICMP-redirect to the router, so that the accompanying traffic will be automatically sent to the defined firewall. The same procedure applies to the router 10.2.1.1, which has to forward the outgoing packets back to the source. This procedure assures that the incoming and outgoing traffic of a single session are using always the same firewall.

Unfortunately, this algorithm does not provide genuine load balancing, as only sessions will be distributed; these may vary extremely in their capacity and potential throughput. A session requiring a throughput capacity exceeding that of any available firewall interface cannot be load balanced. A further handling would be possible only if all firewalls have the same status information about ongoing sessions at any time.

A “round robin” algorithm would be useful. The routers on the network path before and after the firewall are used as load balancers. Routing protocols can distribute information concerning possible paths and used capacity.

Unfortunately, there is a problem with this approach. Parallel firewall systems can work in synchronised and unsynchronised modes. Synchronous firewalls distribute status information on all data connections among themselves, which cannot be done by asynchronous firewalls. Status information has to be distributed in a fast and secure manner. Because of the large amount of status information that is needed, a “round robin” scenario seems impractical. Communicating the required status information is a great challenge. Using TCP is assumed to be to slow, because of the overhead of the three-way handshake and the required acknowledgements. Thus, current solutions are based on multicast. Status information is forwarded within a multicast group, whereby it must be verified that the information has been distributed to all systems. Unfortunately, IP multicast does not provide this option.

Current load-balancing solutions are based on a load balancer before and after the clustered firewalls, using a hash algorithm to distribute traffic. This technique can be described as stream-based load balancing, which does not comply with the requirements for high speed data connections.

The currently available firewall systems use diverse solutions. Stonesoft offers a clustered load-balancing solution with a master firewall as load balancer, as described above. This solution is currently being tested and evaluated at the Technical University of Aachen. Load-balancing solutions of other companies often support any kind of firewall system. Cisco Systems, Foundry, and BIG-IP all offer these kinds of solutions. The load-balancing systems of Cisco Systems and Foundry are able to support application streams of several GBit/s.