Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

OpenGridForum
OPEN FORUM | OPEN STANDARDS

High Speed and Loadbalancing Firewalls
-
A status overview

R.Niederberger@fz-juelich.de

GGF 19 - FI-RG - 30.01.2007

Introduction

As seen from first FI-RG document within Grid environments fast (high speed) as well as dynamic configurable firewalls are needed.

To discuss these … a definition of the term firewall is needed first.

Definition of the term firewall

- **packet filters/packet screens** -

  block transmissions of predefined traffic classes. Each packet is handled independendly.
- **stateful packet filter** -

  special form of a packet filter which stores information concering a stream of packets (TCP-stream, session, UDP-“stream“…)
- **circuit level firewall / gateway** -

  devides sessions into external sessions and internal sessions. From outside only the gateway is seen.
- **application firewall / application gateway** -

  one or more machines which handle individual applications. Examples are mail gateways, ftp gateways, ssh gateways

Definition of the term firewall

- **Loadbalancing firewalls** -

  # of firewalls at the edge of an organisation which process packets concerning access lists. The incoming and outgoing traffic is divided dependend on services, addresses, load … in an RoundRobin, hash or any other fashion

- **Distributed Firewalls**

  # of firewalls securing only parts of a network or different entries to a network, but interchanging information between each other

- **Firewall clusters and firewall farms**

  can be Load-Balancing and/or distributed firewalls

Firewall Architekturen

- **firewall appliances** or **stand-alone firewalls**
  - Special kind of hardware or pc with special software or hardware extension,
    dependend on this
    → cheap, but slow **or**
    → expensive and fast
- **firewall blades** (service modules within switches)
- **virtual firewalls** (often many parallel ones) implemented on one physical hardware

Firewall Architekturen (2)

security appliances

- Combining firewall, intrusion detection/prevention system, VPN concentrator, NAT Device and/or virus filter

- Security within a box
  - Small footprint, global management, internal interaction, simple network connection
- More cost effective than many single systems
- Slower than single systems
- Not usable for high throughput

Firewalls and Grids

- Grid Computing
  - → Vision of applications to have high throughput, on-demand access to distributed ressources like cpus, discs, visualization devices, and network
- Grid application
  - → access across boarders of own organization
- Different kinds of traffic classes
  - → many parallel small streams
  - → few big pipes (data intensive and high performance)
  - → any kind of mixed traffic classes of both above

Firewalls und Grids

Generall problem

- routers/switches combine many parallel streams at the boarder of the organization into one big pipe to the outside internet
- firewalls have to act in real time without adding additional delays
- Often this will lead to bottlenecks (many to one problem)

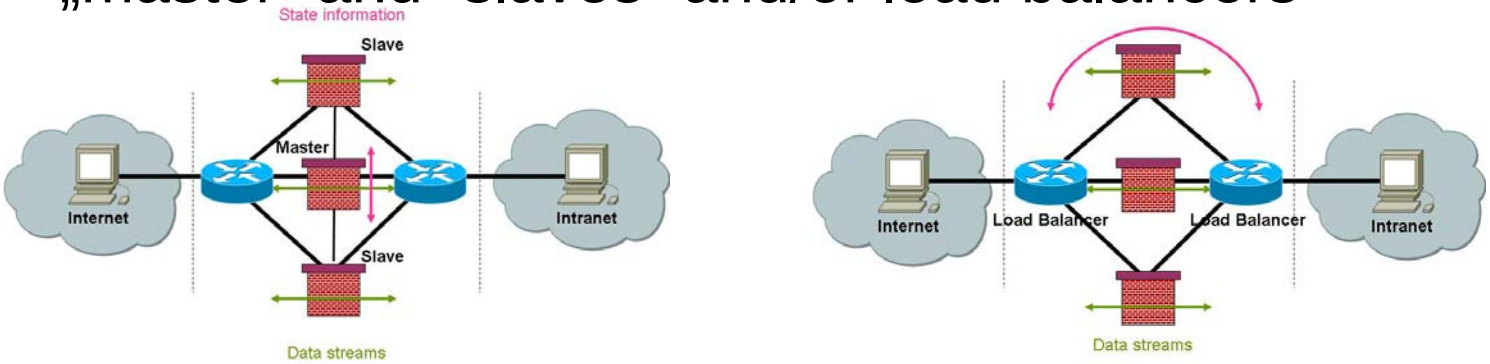
Loadbalancing Firewalls

Can be used as high speed firewalls, but problems in dividing traffic load. Load will be

- assigned by services,
- assigned by source/destination addresses,
- divided by load in a RoundRobin or hash fashion.

It is dependend on bandwidths requirements of streams.

We face problems transmitting state information between „master" and "slaves" and/or load balancers



Status: not yet really completly solved

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Maximum throughput reached today with high speed firewalls

OpenGridForum

Aggregated throughput*1:	10 Gbps
VPN throughput:	1 Gbps
# parallel sessions:	4.000.000
# connection setup per second:	100.000
# VPN tunnels:	10.000
# VLANs:	4.000

***1 !!! Aggregation of streams and interfaces !!!**

Packet screens may be faster.

Market overview
Status August 2006

Performance in Gbit/s:

Type	Throughput	VPN
Astaro Security GW 525	3	0.4
Nokia IP2255	8.9	2.3
Cisco Catalyst FW Modul	5.5	0.3
Clavister Security GW 4400	4	1
Fortinet Fortigate 3600	4	0.6
Juniper Netscreen 5400	30	15
Cyberguard TSP 7300	3.9-10.2	1.3-1.4
Stonesoft SG-4000	3.1	0.5

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Summary

OpenGridForum

- Current high speed firewalls can handle most of the Grid traffic needed today.
- Loadbalancing can enhance things quite well
- But organizations having multiple high speed connections to external partners will need expensive firewall solutions to deal with security concerns
- Modern technologies like DWDM links, which could be come standard in the near future, cannot be handled by current firewall solutions because of the high data rates (e.g. 32 times 10 Gb/s, current networking technologies allow up to 160 parallel wavelengths on a single fiber)

Questions and discussion

Questions
and
discussion