Secured Network Performance:
Firewalls put to test

Networks 2005, Geneva, 22 June 2005

Markus Berg
Herbert Guist
Matthias Hammer
IRT/Broadcast Networks and Servers

Agenda

- Introduction
- Motivation
- Firewalls in Broadcaster's Networks
- Test build-up
- Tested Firewalls
- Measurements (Extract)
- Results
- Conclusion

Introduction

- >6 years experience with soft- and hardware firewalls
  - Internal network security (www, research and office networks)
  - Trade fairs (security of the booth)
  - Requests from broadcasters
- Broadcast and IT world come together
  - Networks in production…
  - Separation and interconnection of broadcast “islands”
  - Applications like Video Filetransfer
  - External contributions (video journalist…)

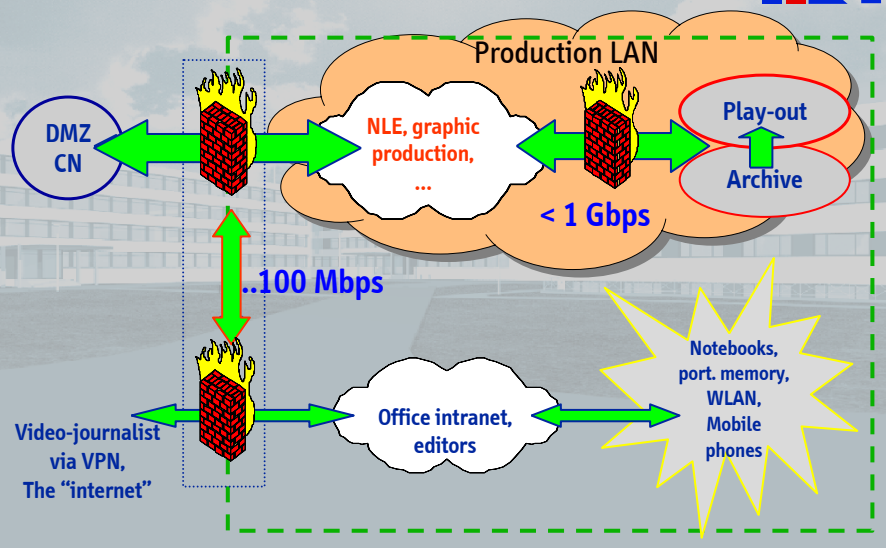
Motivation

- Need for more network security…
- Market situation not straightforward
  - Suppliers are changing
  - New changing solutions (HW, SW, combinations)
  - Big differences in price/performance ratio
- Internal IRT security project since *2003*
  - Security in contribution and distribution networks of broadcasters
  - Firewall-performance measurements (focus on high speed filetransfer)
  - Identification, documentation, communication of security risks (in broadcaster’s networks)
- Close cooperation with working groups of our affiliates and the EBU

Firewalls in broadcast networks

- Internet connections
  - Secured by “classical” firewall configuration (incl. VPN)
- Intranet and production
  - Securing critical internal departments like: archives, production, play out, administration...
- Corporate Network (CN), regional networks, connections to partners
- Separation of “office”- traffic and for example video-filetransfer

Firewalls in broadcast networks (example)



Broadcast specific requirements (video filetransfer)

- "small number" of data streams at very high speed
  - Copying files in a production LAN
  - Video filetransfer in the corporate network (CN)
  - Requirement: data streams up to 600 Mbit/s
- Due to the huge file size (200-400 MByte/ minute), proyxs with virus protection are no solution
- IPsec VPN-connections
  - ... are considered secure today. The broadcasters requirements are also valid for VPN traffic (i.e. filetransfer from external organisations)

Firewall tests

- Why?
  - "normal" usage scenarios not so interesting for broadcasters... (perhaps to validate the promises of the manufacturers)

  But:
  - Broadcast specific applications are unusual in the internet community
    - No references available
    - Manufacturers often do not know what to expect here
- Goal:
  - Gather experiences with different FW concepts
  - Knowledge base and market overview
  - Build a flexible high performance test bed including reference data
- Value:
  - Optimisation of FW concepts for broadcasters
  - Verification and comparison of "real" performances
  - Reference measurements (before implementation at broadcaster's premises)

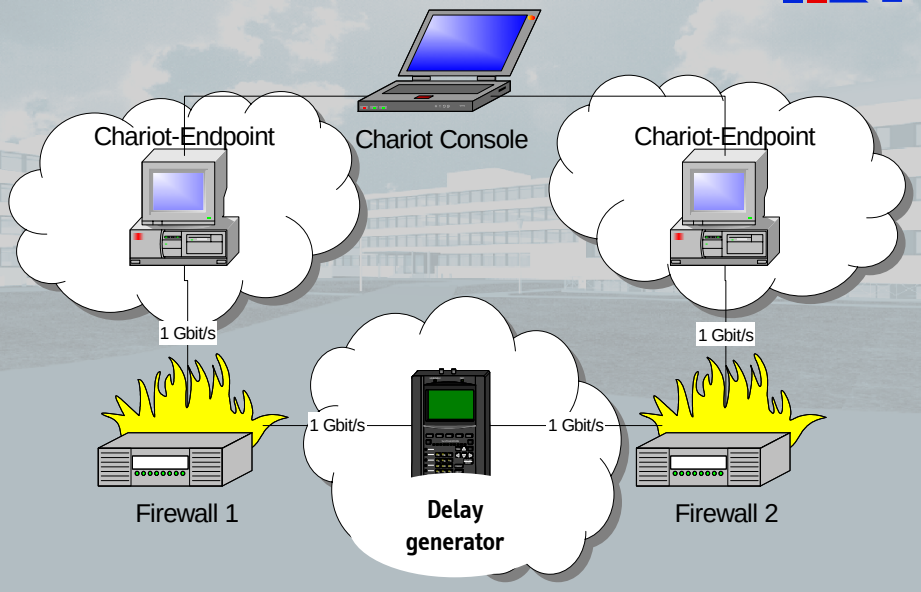
Measurement equipment

- Measurement software “Chariot” (NetIQ)
  - Traffic generation between so called “end points” (SW on PCs, any operating system). Data rates depends on PC capacities.
- Hardware-measurement system (IXIA)
  - 1 Gbit/s per Port on application level
  - “Chariot” acquired by “IXIA” and ported on Hardware -> Results are comparable.
- Video Filetransfer applicarion in the lab and a real WAN
  - Real and simulated TCP/IP-video filetransfer (VFT) by the DAVID-Replikator-Software
  - Use of 3 VFT-clients in the lab

Measurement procedures

- A single TCP connection between endpoints (Script: “High Performance- Throughput”, data rate up to 940 Mbit/s)
- 1 Parallel connection in both directions
- 50 parallel TCP connections
- VPN tests

Measurement build-up



Firewalls under test

4 different types of firewalls:

- Commercial, Linux based software:
  "Astaro Security Linux V5.2"
- Hardware based firewall by Juniper/NetScreen :
  Internet Security Gateway "ISG 2000"
- PC based firewall by Secure Computing :
  Sidewinder G2 Security Appliance 2150
- Non commercial public solution:
  Debian linux

Astaro Security Linux V5.2 (1)

- Based on Linux with high functionality
- Stateful Packet Inspection
- Application Level Filtering (Proxy)
- NAT (Network Address Translation)
- VPN (AES, DES, 3DES)
- Virus protection for web und email traffic
- URL- and content filtering
- Web based management interface
- High availability

NetScreen ISG2000

- Hardware based
- Up to 8 GE ports
- Throughput 2 GBit/s in packet filter mode (Stateful Inspection)
- 1 GBit/s in VPN-mode (3DES with 168 bit encryption)
- Up to 512.000 simultaneous and 30.000 new connections/s
- “Deep Inspection Modus” for selected protocols (300 Mbit/s)
- Up to 10.000 VPN-tunnelc
- SNMP-capable
- High availability
- Administration via management-SW, console/ssh and web interface

Sidewinder G2 Security Appliance 2150

- Multi-protocol content filtering, from layer 3 to layer 7
- Both stateful inspection and simple packet filtering engines
- Protocol anomaly detection; traffic anomaly protection
- Advanced network cloaking techniques
- Application and stateful inspection firewall
- Secure MAIL, Web, and DNS gateway services
- Embedded anti-spam and anti-virus engines
- Hardware accelerated HTTPS/SSL termination
- Both IPSec and clientless SSL VPN services
- Integrated IDS with real-time alerts and automated Strikeback® response
- High-speed, intrusion preventing application proxies
- Outbound Web access controls with IM & P2P blocking, as well as SmartFilter® URL filtering

Debian Linux

- Free of charge Linux distribution
- Version: AMD64 Sarge Distribution, 64 Bit Kernel 2.6.10 SMP
- Stateful inspection support integrated in kernel
- Filter rules: “iptables”
- No graphical administration interface. Needs time to learn working with the sytem
- Proyx (Squid)
- VPN (tested: AES-tunnel,192 Bit)

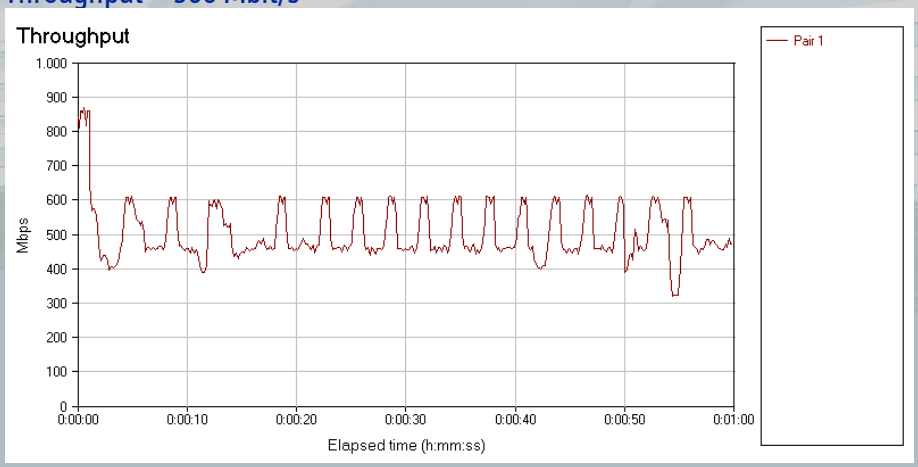
Test PCs (Astaro and Debian):

- Dual-Opteron 248, 2 GB RAM, Tyan Server Motherboard
- 2x GE-interfaces onboard via hypertransport (Broadcom)

Test results (snapshot examples)

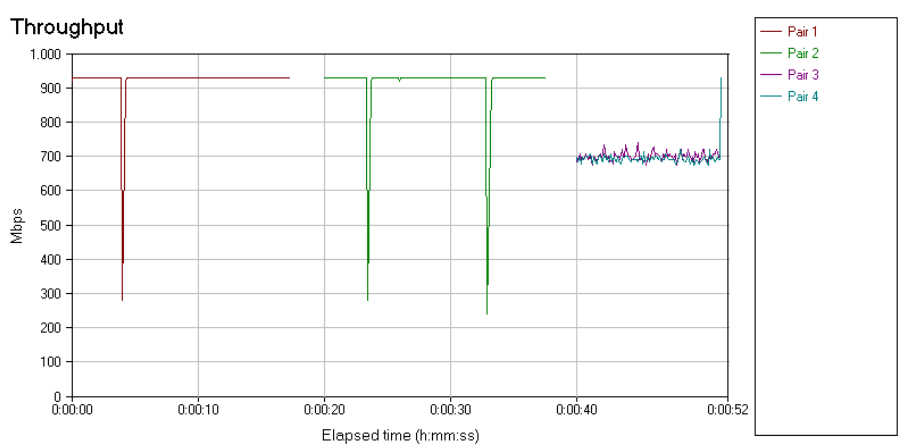
Test (Astaro)

Astaro: High-Performance-Throughput (1 connection through 2 FW), Throughput ~ 500 Mbit/s



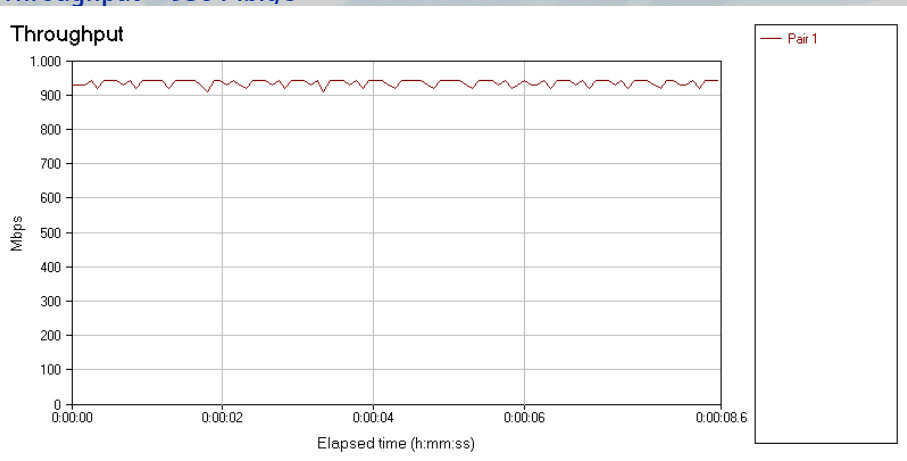
Test (ISG 2000)

ISG2000: Packet Filter Mode, 1 connection per direction, then bidirectional, Throughput ~ 930 Mbit/s unidirektional, 700 Mbit/s each bidirektional



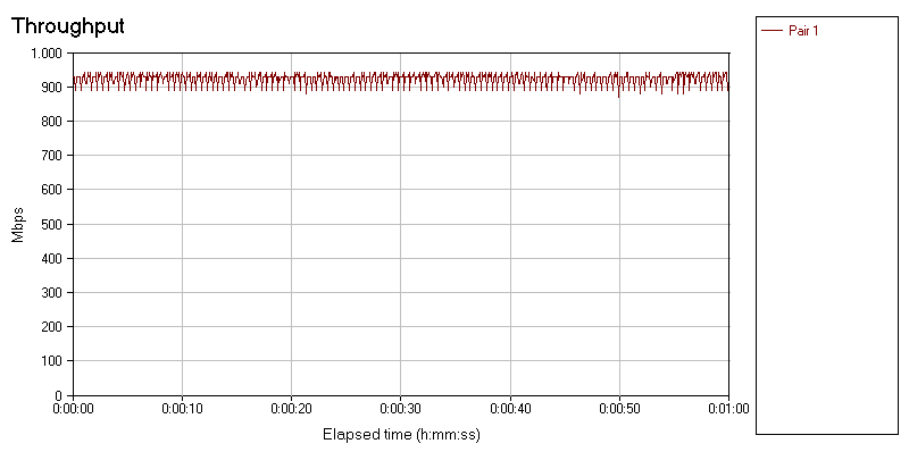
Test (Debian)

Debian: High-Performance-Throughput (1 connection through 2 FW), Throughput ~ 930 Mbit/s



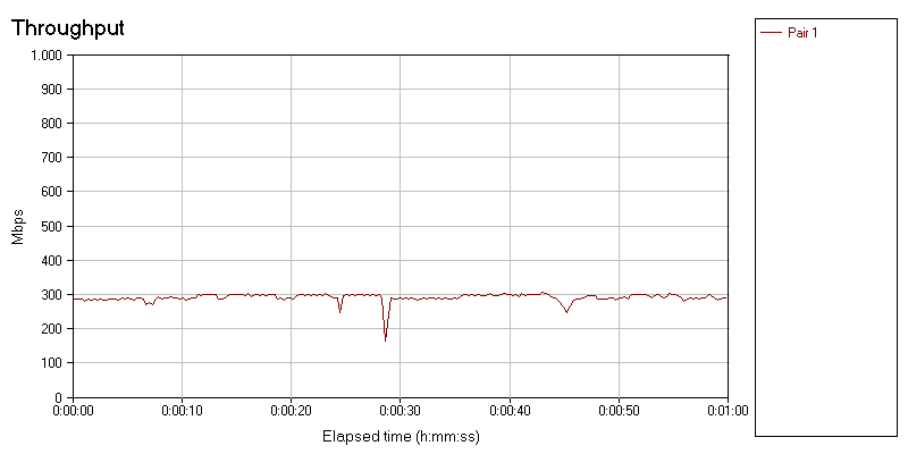
Test (Sidewinder)

Sidewinder: High-Performance-Throughput (1 connection through 1 FW), Throughput ~ 925 Mbit/s



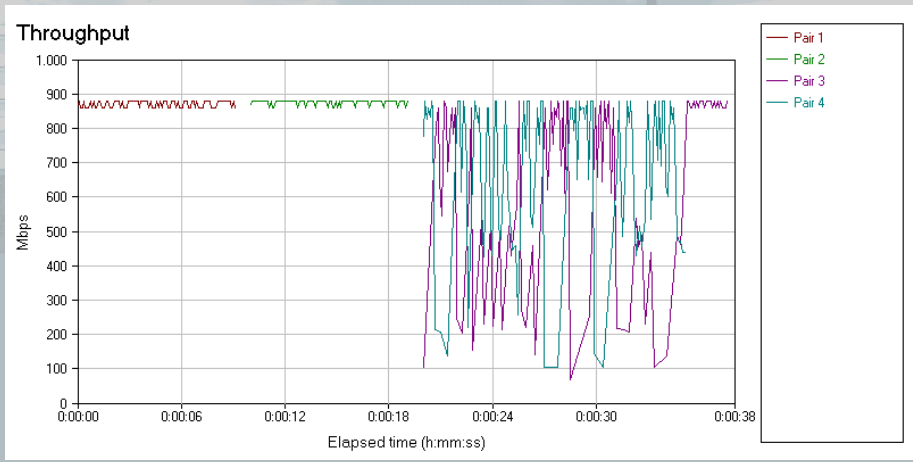
Test (Astaro, VPN)

Astaro: High-Performance-Throughput (1 connection through 2 FW), VPN, Throughput ~ 290 Mbit/s



Test (ISG 200, VPN)

ISG2000: **VPN mode, 1 connection per direction, then bidirectional, Throughput ~ 870 Mbit/s unidirectional, 890 Mbit/s bidirectional**



Results (1)

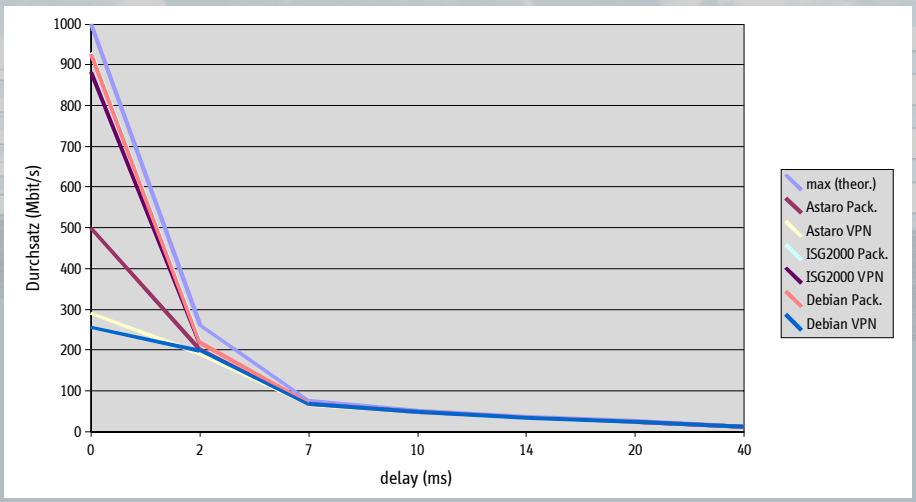
Table 1: Overview measurement 1x High-Performance-Throughput through 2 Firewalls in Packet-Filter and VPN-Mode. (Mbit/s.)

DUT	max (theor.)	Astaro Pack.	Astaro VPN	ISG2000 Pack.	ISG2000 VPN	Debian Pack.	Debian VPN	G2-2150	G2-2150 VPN
Throughput	1000	500	290	930	882	927	256	925	*

***** No VPN test possible, due to current new implementation of AES encryption, tests will be performed later.

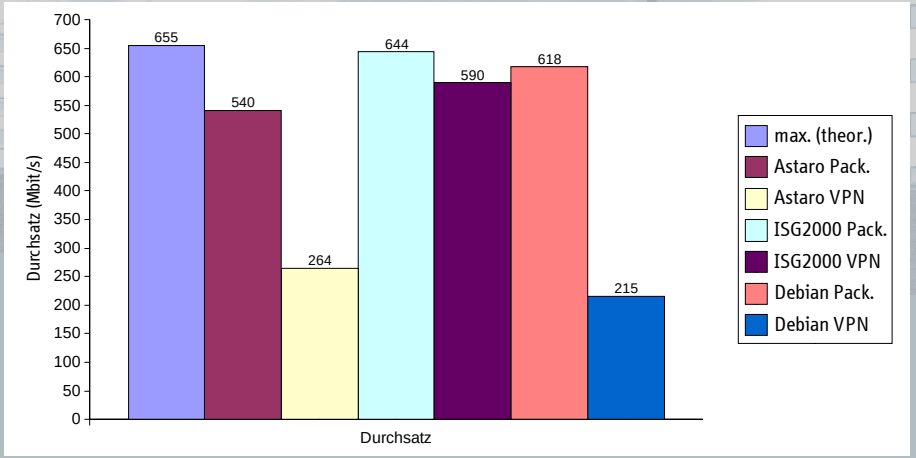
Results (2)

Figure 1: measurement 1x High-Performance-Throughput through 2 Firewalls in Packet-Filter and VPN-Mode



Results (3)

Figure 2: measurement 50 parallel connections High-Performance-Throughput through 2 Firewalls in Packet-Filter and VPN-Mode at 40 ms Delay



Results (4)

Table 2: measurements with VFT-Tool David Replikator (transfer rate test)

Direction	Debian			ASTARO		
	Delay	Packet Filter	VPN	Delay	Packet Filter	VPN
Client1 -> Client2	0	400	258	0	381	260[2]
	7	254	247	7	254	239[2]
	14	138	135	14	136	134[2]
	20	115	98	20	98	98
Client1 <- Client2	0	398	243	0	402	259
	7	252	233	7	252	233[2]
	14	136	135	14	135	134[2]
	20	114	96	20	97	97
Client1 <-> Client2	0	220 – 195	106 – 104	0	216 – 196	*
	7	223 – 215	*	7	240 – 180	*
	14	125 – 123	*	14	132 – 130[1]	*

[1] Transmission very symmetric and stable

[2] Transmission with constant interruptions

* A large number of interruptions, no useful measurement possible

Conclusion (1)

- FW: Astaro Security Linux V5.2
  - Moderate performance with single, very good performance with multiple parallel connections
  - Acceptable and stable VPN-performance (300 Mbit/s), also with parallel connections (265 Mbit/s with 50 connections)
- NetScreen ISG2000:
  - Behaves almost like a router in packet filter mode
  - VPN-performance: ~ 900 Mbit/s per tunnel (!). Combination of multiple tunnels on multiple ports to increase the performance
- Debian Linux:
  - With AMD 64-Bit architecture and kernel 2.6 very good performance in packet filter mode (~930 Mbit/s) with single and multiple connections
  - Moderate performance in VPN-mode (265 Mbit/s), even worst with 50 parallel connections (215 Mbit/s)
- Sidewinder G2 Security Appliance 2150
  - Excellent performance in packet filter mode
  - VPN mode to be tested in the future due to current new implementation of AES encryption

Conclusion (2)

- All tested firewalls fulfilled the basic expectations
  - Nevertheless there are significant differences. A lot of potential money savings possible...
  - Further tests are actually under development
- Packet filter mode
  - A delay > 7 ms is a stop block for TCP, not the firewall at these delays
  - Parallelisation of connections can cope with the delay problem
- VPN Gateway
  - Encrypted transmission is the worst case scenario for a firewall
  - But the performance is for example sufficient for several SDSL connections (video-journalist)
  - Encryption in a CN or DMZ not necessarily mandatory
- The expensive firewalls show a higher performance in critical conditions. The “cheap” and free of charge firewalls also showed to be flexible and performing and could be used for some use cases
- The measurements displayed represent only a small extract of the test program
- Comparisons are interesting for both vendors and customers

Contact

Markus Berg
Institut für Rundfunktechnik GmbH
Floriansmühlstr. 60
80939 München

Tel.: +49 89 / 32399 – 279
Fax: +49 89 / 32399 – 354
E-Mail: berg@irt.de
web:http://www.irt.de

The folio / documents are protected by the copyright.
A copy is only permitted with permission of the author.
The copyright reference must not be removed.