Barbarians in the Gate : An Experimental Validation of NIC-based Distributed Firewall Performance and Flood Tolerance

Michael Ihde and William H. Sanders
Information Trust Institute and
Coordinated Science Laboratory,
University of Illinois at Urbana-Champaign
Urbana, IL

What are NIC-based Distributed Firewalls?

- First proposed by Steven Bellovin in 1994.
  - Pushes protection to the network edge with centralized policy management.
    - Helps reduce the threat of insider attacks.
    - May reduce global performance bottlenecks.
- NIC-based distributed firewalls place the firewall functionality on the NIC.
  - By placing the firewall functionality on the NIC the firewall cannot be circumvented by the host. Software firewalls can be disabled by malicious users and programs.
  - Allows least-privilege policy for network on a per-host basis.
- Our experiments focused on the Embedded Firewall (EFW) and the Autonomic Distributed Firewall (ADF)
  - The EFW provides stateless packet filtering on incoming and outgoing traffic.
  - The ADF provides Virtual Private Groups, that encrypt packets send between ADF NICs in the same group using a shared key.
  - Protects confidentiality, restricts communication to authorized members, and prevents spoofing.

Questions to be Answered

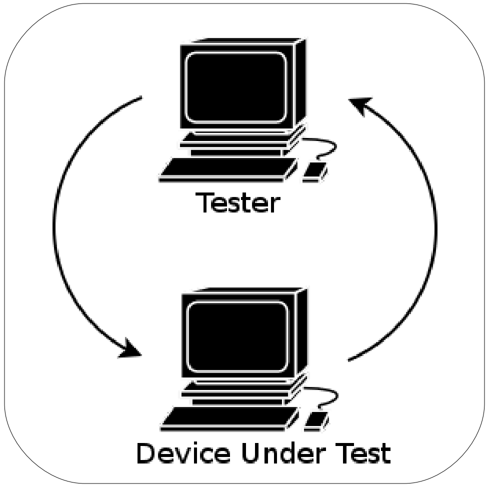
- Can low-cost embedded firewalls provide adequate performance and flood-tolerance?
  - We evaluated the performance of a commercially available distributed, NIC-based firewall
    - Mis-conception that NIC-based firewalls will *always* provide full network bandwidth
    - Began to develop a useful methodology for testing distributed firewalls.
- What is the performance cost of encrypting traffic in a VPG?
- Can rule-sets be tailored for maximum performance and flood-tolerance?
  - Provide experimental performance and denial-of-service data
    - Without accurate data it is difficult to safely and effectively deploy the firewalls.
- Does the additional firewall security create a “barbarian in the gate”?
  - RFC2647 explicitly warns against DoS attacks on firewalls, we performed packet flood attacks on both the ADF and EFW.

EFW (3CRFW200B) and ADF Details

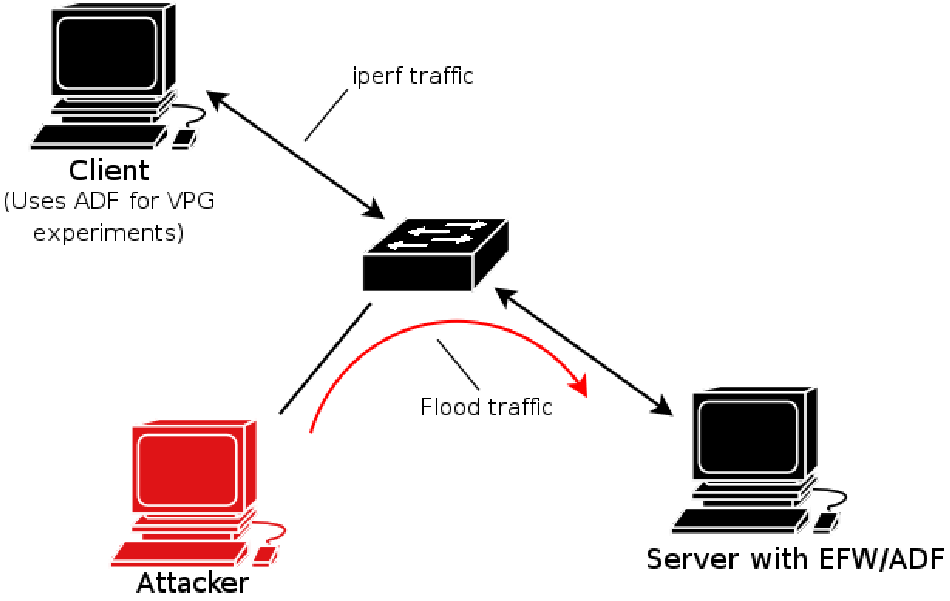
- Implemented using the 3CR990 hardware
  - Originally designed to provide IPSEC/Encryption offload.
  - Uses a 100 MHz ARM9 processor.
  - Supports 100 Mbps network connection, 64 stateless rules, and 4 VPGs (ADF)
- Original EFW model discontinued as of June 1st 2006
  - Replacement is 3CR990B-97 with software upgrade to add firewall support.
  - Possibly the same card as before.
- ADF is a firmware modification to the EFW
  - Developed by Secure Computing under DARPA effort
  - Provide Virtual Private Group to enable secure, authenticated group communication.
- Both the EFW and ADF are built on hardware designed for encryption offloading <u>not</u> packet filtering.

Experimental Setup

- The standard configuration for throughput tests is not suited to “attacker-oriented” embedded firewall experiments.
- The flood is generated as well-formed TCP packets filled with arbitrary data. It is only a naïve packet flood, it does not attempt to attack any other vulnerabilities (i.e. SYN floods, mal-formed packets).
  - Maximum theoretical rate:
    - 14881 packets/sec (10 Mbps), 148810 packets/sec (100 Mbps)



Recommended Setup from RFC2544



Rule Sets Used for Experiments

The attackers flood packets traverse the rule-set until reaching the "action rule", at which point they are accepted or denied.

The "test" traffic always falls through to the default allow rule.

We found that additional rules beyond the "action rule" did not affect the performance or flood tolerance.

A VPG minimally uses two rule-slots per VPG.

	Protocol	Src. IP	Src. Port	Dst. IP	Dst. Port	Action
1	any	130.126.141.14	any	*.*.*.*	any	deny
2	any	130.126.141.15	any	*.*.*.*	any	deny
3	any	130.126.141.16	any	*.*.*.*	any	deny
4	any	130.126.141.17	any	*.*.*.*	any	deny
5	default allow					

Flood packet is allowed.

	Protocol	Src. IP	Src. Port	Dst. IP	Dst. Port	Action
1	any	130.126.141.14	any	*.*.*.*	any	deny
2	any	130.126.141.15	any	*.*.*.*	any	deny
3	any	130.126.141.16	any	*.*.*.*	any	deny
4	any	130.126.141.17	any	*.*.*.*	any	deny
5	any	ATTACKER_IP	any	*.*.*.*	any	deny
6	default allow					

Flood packet is denied.

An attacker can **always** reach the deepest rule by spoofing the flood packets.

Experiments Performed

- Available bandwidth as rule-set size increases.
  - Can be used to indirectly measure throughput (if there is bandwidth loss)

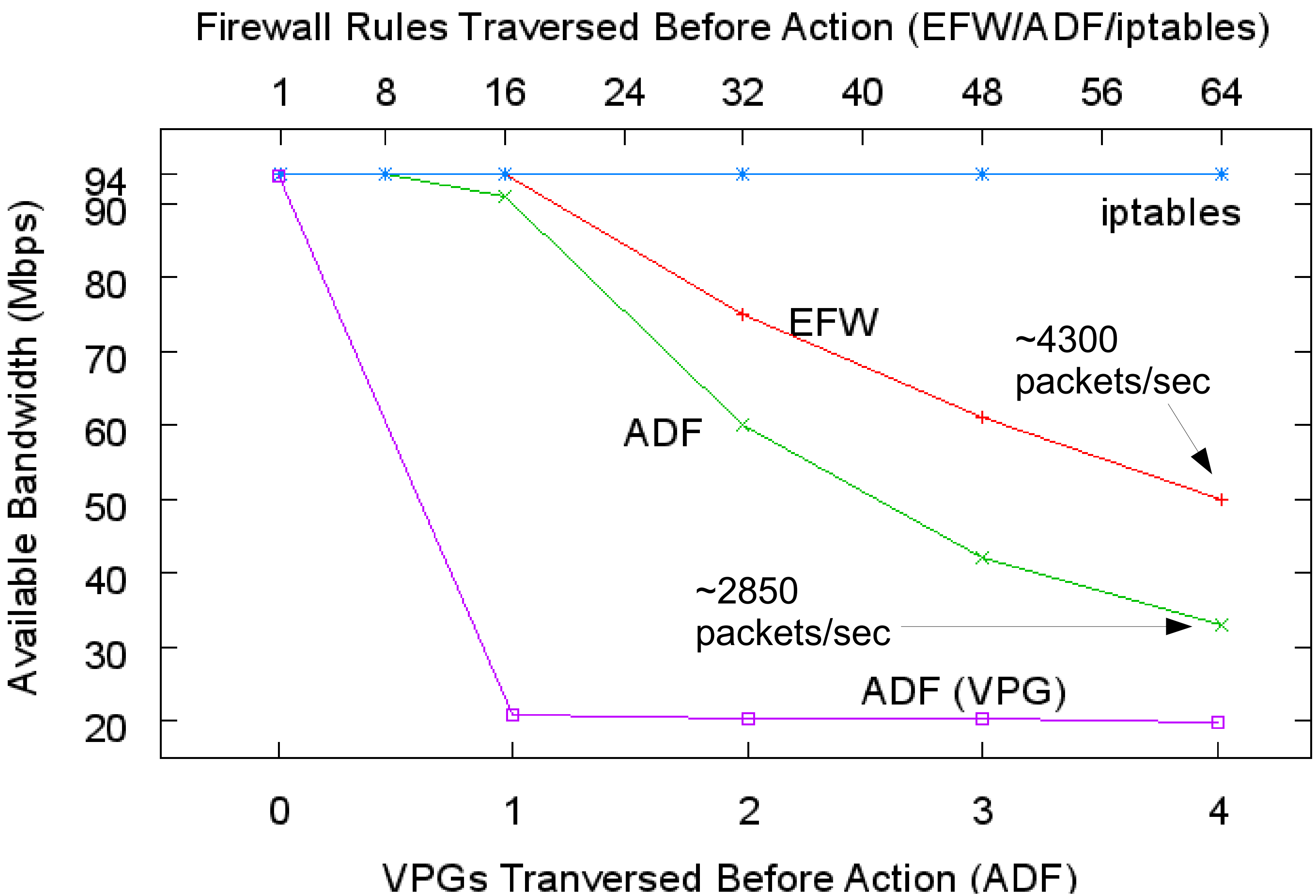
$$Throughput = BW / FrameSize$$

  - Uses iperf to measure bandwidth using maximum Ethernet frame-size (1518 bytes per frame)
- HTTP Performance
- Impact of packet floods on available bandwidth
  - With no firewall rules (best possible condition) we measure the flood rate required to reduce available bandwidth to 0 Mbps.
  - Another indirect measure of throughput (if bandwidth can be reduced to 0)

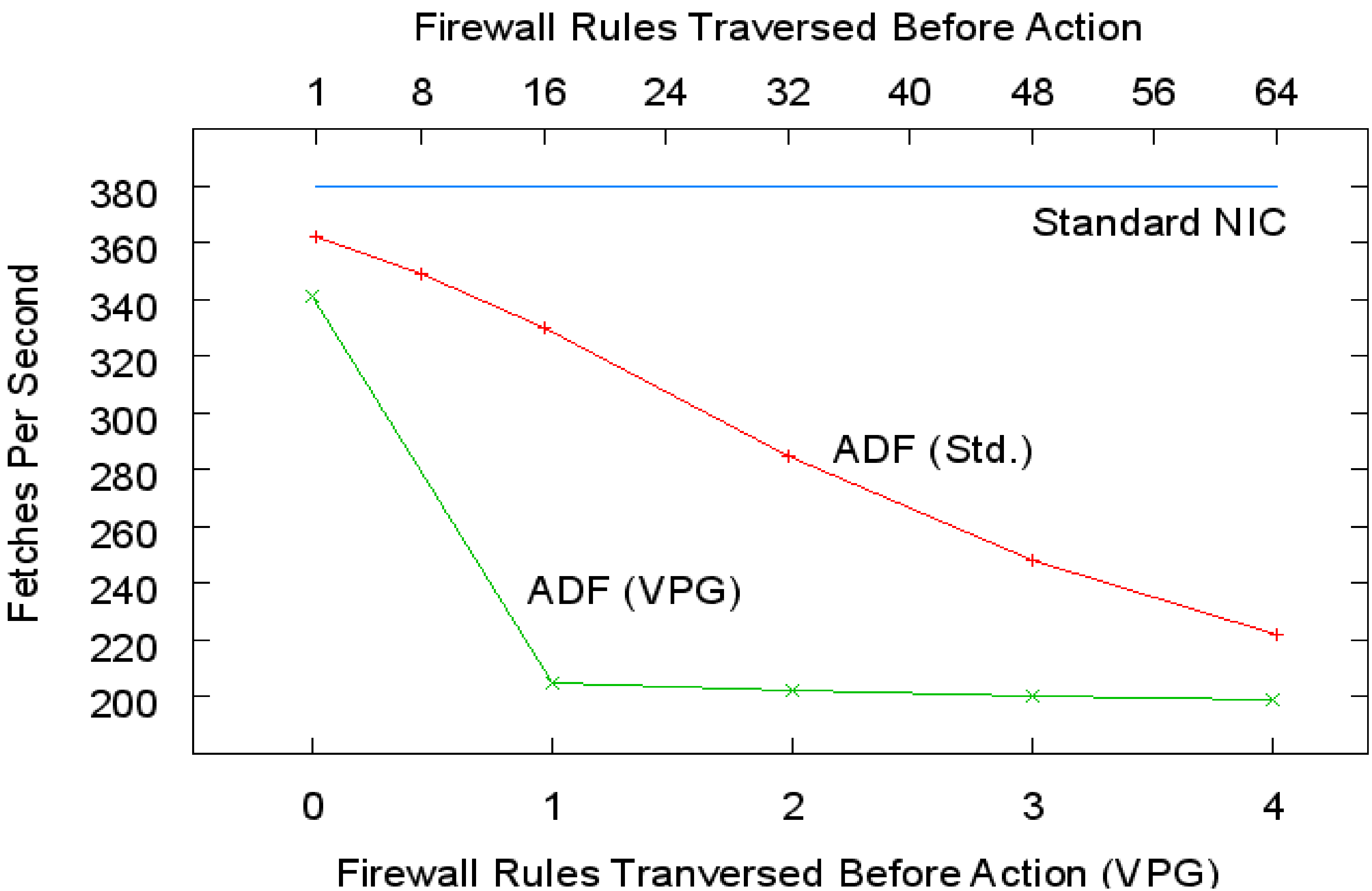
$$Throughput = FloodRate$$

  - Uses iperf to measure bandwidth during packet flood of minimum Ethernet frame-size packets (64 bytes per frame)
- Minimum flood-rate required for D.O.S. as rule-set size increases
  - For a particular rule-set configuration, how many packets per second are required for a successful denial-of-service attack.

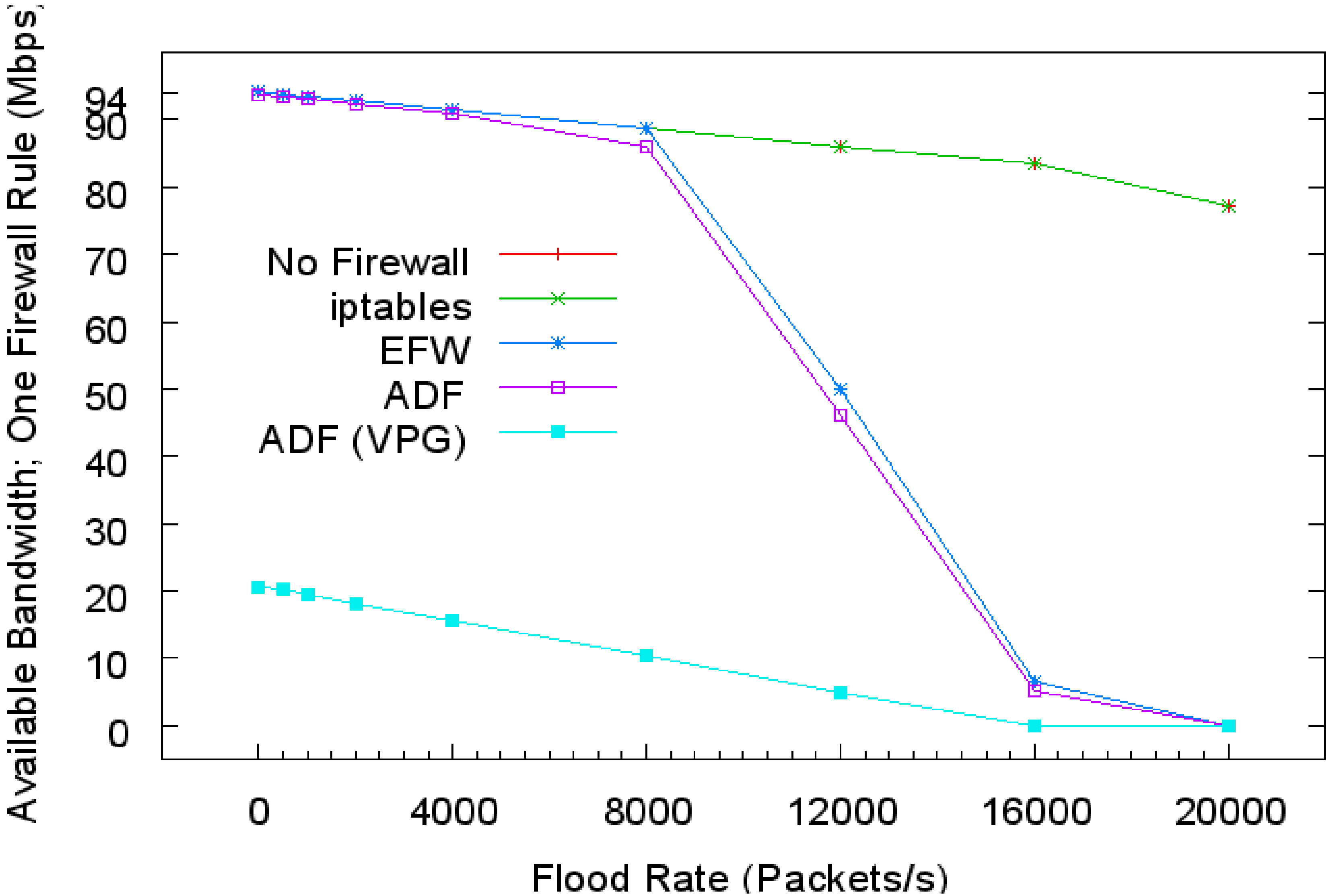
Measuring the Performance Cost of Firewall Rules



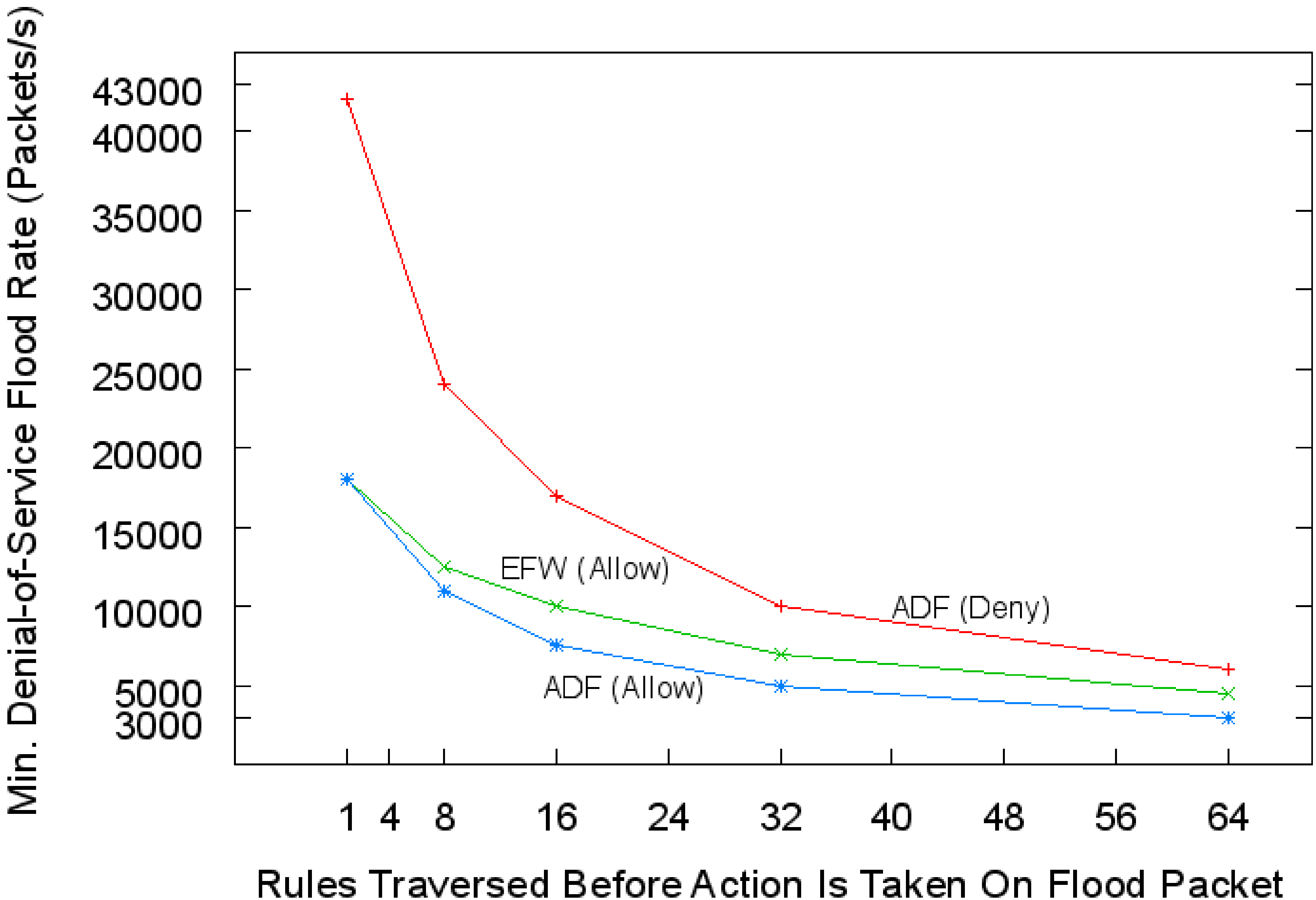
HTTP Performance



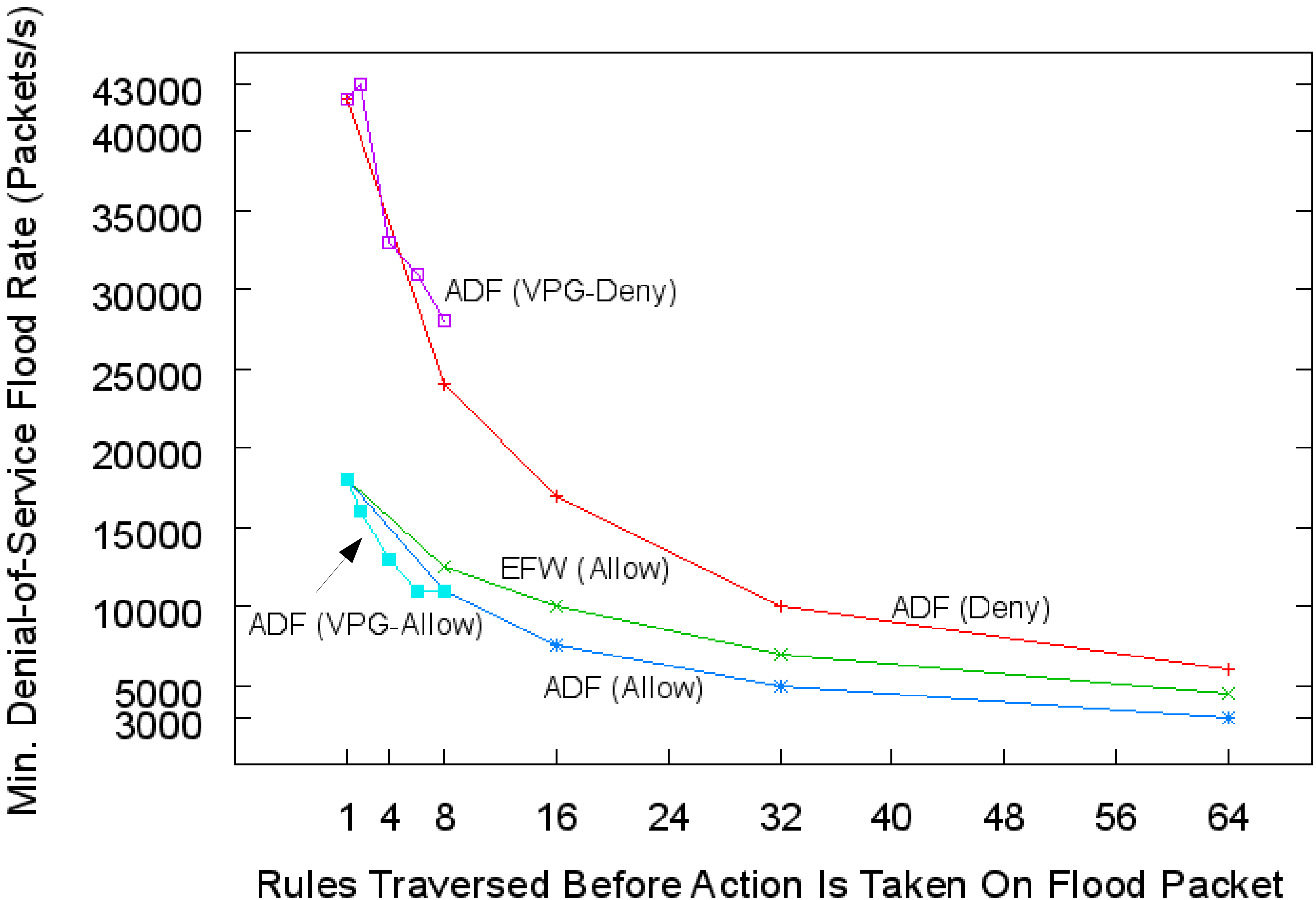
Impact of packet floods on available bandwidth



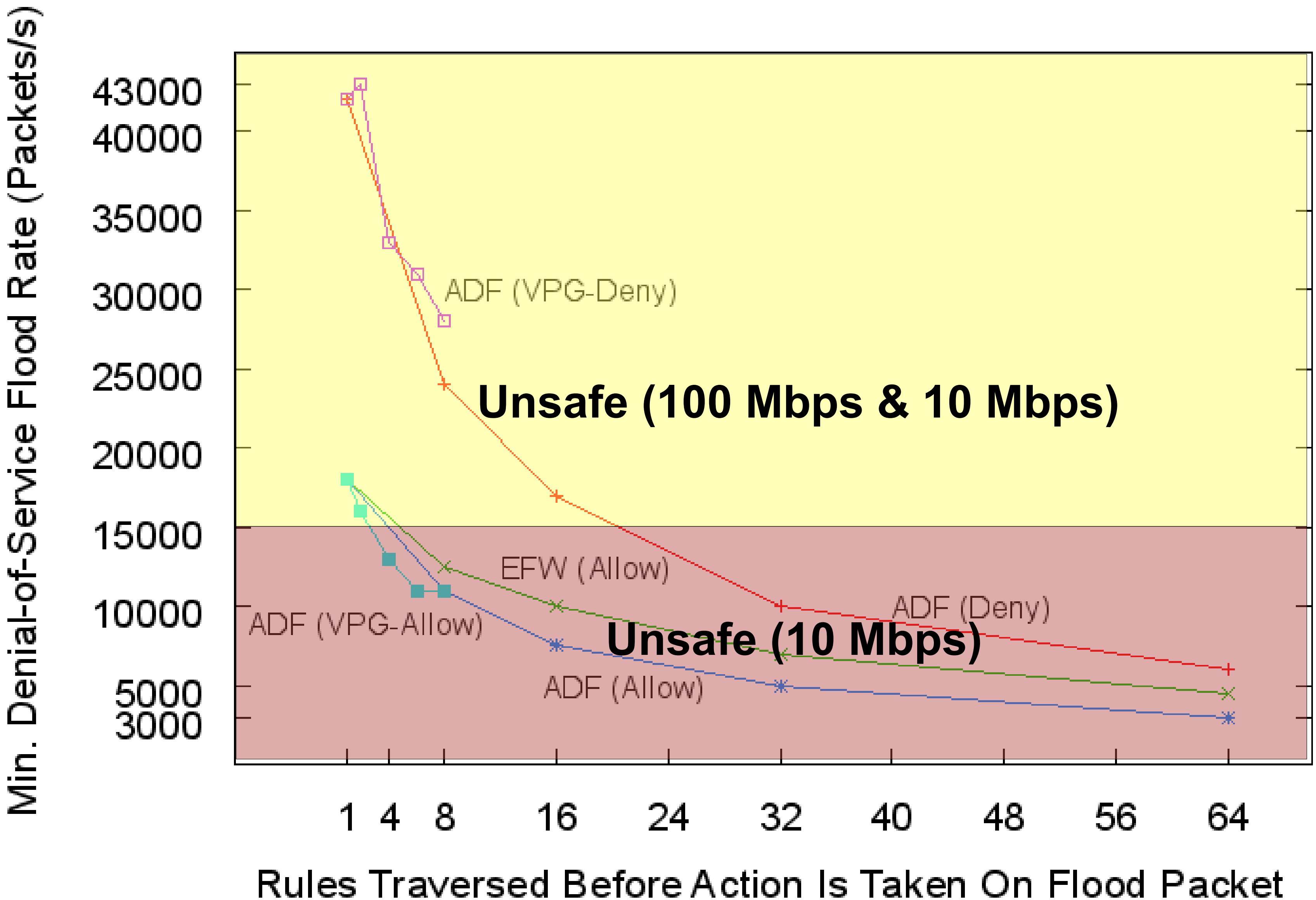
Minimum Flood Rate as Rules are Added



Minimum Flood Rate when using VPGs



...Is It Safe?



Min. Denial-of-Service Flood Rate (Packets/s)
43000
40000
35000
30000
25000
20000
15000
10000
5000
3000
ADF (VPG-Deny)
Unsafe (100 Mbps & 10 Mbps)
EFW (Allow)
ADF (VPG-Allow)
ADF (Deny)
Unsafe (10 Mbps)
ADF (Allow)
1
4
8
16
24
32
40
48
56
64
Rules Traversed Before Action Is Taken On Flood Packet

Preventing Attacks

- Only use the EFW/ADF on 10 Mbps networks
  - This is unrealistic for modern networks, but was utilized during the DPASA experiment.
  - Only works if the rule-sets are kept shorter than 8-rules (2 VPG rules); short rule-sets are usually less “strict”, and therefore less useful.
- Protect the EFW/ADF from malicious outside attacks with upstream firewalls
  - Cisco PIX firewalls were used upstream of all ADF protected hosts during the DPASA experiment.
  - This prevents from outsider flood attacks, but not insider attacks.
- Use switches with ingress/egress rate-limiting
  - With rate-limiting the EFW/ADF can be protected at the potential cost of performance.
- Order rules “deny first, then accept”
  - By denying attack packets first, their effectiveness for attacks is reduce. Spoofing can bypass this mitigation. This may also make rule-sets more difficult to write.

Future Work

- EFW/ADF specific
  - Perform identical experiments on the new revision of EFW/ADF.
    - Does it have the same flaws?
  - Search for other vulnerabilities in the EFW/ADF.
    - Can we bypass the rule-set, or change the rule-set remotely?
- In-General
  - Refine and augment the experimental methodology.
    - Can we create better tools and methods?
  - Explore the feasibility of low-cost, high-performance distributed firewalls.
    - Can we create new algorithms or hardware?

Barbarians in the Gate : An Experimental Validation of NIC-based Distributed Firewall Performance and Flood Tolerance

Michael Ihde and William H. Sanders
{ihde,whs}@crhc.uiuc.edu
Information Trust Institute and
Coordinated Science Laboratory,
University of Illinois at Urbana-Champaign
Urbana, IL