Network Working Group
INTERNET-DRAFT
Expires in May 1998

D. Newman
Data Communications
H. Holzbaur, J. Hurd, and S. Platt
National Software Testing Laboratories

Benchmarking Terminology for Firewall Performance
<draft-ietf-bmwg-secperf-01.txt>

Status of This Memo

1. Introduction

This document defines terms used in measuring the performance of firewalls. It extends the terminology already used for benchmarking routers and switches and adds terminology specific to firewalls. The primary metrics defined in this document are maximum forwarding rate and maximum number of connections.

Why are firewall performance measurements needed? First, despite the rapid rise in deployment of firewalls, there is no standard method for benchmarking their performance. Second, implementations vary widely, making it difficult to do direct performance comparisons. Finally, more and more organizations are deploying firewalls on internal networks operating at relatively high speeds, while most firewall implementations remain optimized for use over low-speed wide-area connections. As a result, users are often unsure whether the products they buy will stand up to relatively heavy loads.

We may also create additional terminology and methodology documents to define other types of network security products such as virtual private network (VPN) and encryption devices. This document, however, focuses solely on firewall terminology.

2. Existing definitions

This document uses the conceptual framework established in RFCs 1242 and 1944 (for routers) and draft-ietf-bmwg-lanswitch-07.txt (for switches). The router and switch documents contain discussions of several terms relevant to benchmarking the performance of firewalls. Readers should consult the router and switch documents before making use of this document.

This document uses the definition format described in RFC 1242, Section 2. The sections in each definition are: definition, discussion, measurement units (optional), issues (optional), and cross-references.

3. Term definitions

3.1 Allowed traffic

Definition:
Packets forwarded as a result of the rule set of the DUT/SUT.

Discussion:
Firewalls typically are configured to forward only those packets

explicitly permitted in the rule set. Forwarded packets MUST be included in calculating the forwarding rate or maximum forwarding rate of the DUT/SUT. All other packets MUST NOT be included in forwarding rate calculations.

Measurement units:
Not applicable

Issues:

See also:
policy (3.12)
rule set (3.15)

3.2 Authentication

Definition:
The process of verifying that a client user or machine requesting a network resource is who he, she, or it claims to be, and vice versa.

Discussion:
Trust is a critical concept in network security. Any network resource (such as a file server or printer) with restricted access MUST require authentication before granting access.

Authentication takes many forms, including but not limited to IP addresses; TCP or UDP port numbers; passwords; external token authentication cards; and biometric identification such as signature, speech, or retina recognition systems.

Authentication MAY work either by client machine (for example, by proving that a given IP source address really is that address, and not a rogue machine spoofing that address) or by user (by proving that the user really is who he or she claims to be). Servers SHOULD also authenticate themselves to clients.

Measurement units:
Not applicable

Issues:

Testers should be aware that in an increasingly mobile society, authentication based on machine-specific criteria such as an IP address or port number is not equivalent to verifying that a given individual is making an access request. At this writing systems that verify the identity of persons are typically external to the firewall, and may introduce additional latency to the overall SUT.

See also:
user (3.20)

3.3 Data source

Definition:
A station capable of generating traffic to the DUT/SUT.

Discussion:
One data source MAY emulate multiple users or stations. In addition, one data source MAY offer traffic to multiple network interfaces on the DUT/SUT.

Measurement units:
Not applicable

Issues:

The term "data source" is deliberately independent of any number of users. It is useful to think of data sources simply as traffic generators, and not as a given number of users.

See also:
data connection (3.4)

3.4 Data connection

Definition:
A logical link established between two hosts, or between a host and the DUT/SUT.

Discussion:
The number of concurrent data connections a firewall can field may be just as important a metric for some users as the rate at which it can

forward traffic. Data connections MAY be TCP sessions, but they don't have to be. Users of other connection-oriented protocols such as ATM may wish to measure these, either instead of or in addition to TCP connections.

Measurement units:
Number of connections

Issues:
A firewall's architecture dictates where the connection is terminated. In the case of proxy-based systems, a connection by definition terminates at the DUT/SUT. But firewalls using packet filtering or stateful inspection designs act only as passthrough devices, in that they reside between two connection endpoints. Regardless of firewall architecture, the number of data connections is still relevant, since all firewalls perform some form of connection maintenance; at the very least, all check connection requests against their rule sets.

See also:
data source (3.3)

3.5 Demilitarized zone (DMZ)

Definition:
A network segment or segments located between protected and external networks. DMZ networks are sometimes called perimeter networks.

Discussion:
As an extra security measure, networks are often designed such that protected and external segments are never directly connected. Instead, firewalls (and possibly public resources such as WWW or FTP servers) often reside on the so-called DMZ network. To connect protected, DMZ, and external networks with one device, the device MUST have at least three network interfaces.

Multiple firewalls MAY bound the DMZ. In this case, the firewalls connecting the protected network with the DMZ and the DMZ with the external network MUST each have at least two network interfaces.

Measurement units:

Not applicable

Issues:
Dual-homed
Homed

See also:
external network (3.8)
perimeter network (3.11)
protected network (3.13)

3.6 Dual-homed

Definition:
A firewall with at least two network interfaces.

Discussion:
Dual-homed firewalls connect two segments with different network addresses.

Measurement units:
Not applicable

Issues:
Typically the differentiator between one segment and another is its IP address. However, firewalls may connect different networks of other types, such as ATM or Netware segments.

See also:
Homed (3.9)
Tri-homed (3.19)

3.7 Dynamic proxy

Definition:
A proxy service that is set up and torn down in response to a client request, rather than existing on a static basis.

Discussion:
Proxy services (see section 3.14) typically "listen" on a given TCP port number for client requests. With static proxies, a firewall always forwards packets containing a given TCP port number if that port number is permitted by the rule set. Dynamic proxies, in contrast, forward TCP packets only once an authenticated connection has been established. When the connection closes, a firewall using dynamic proxies rejects individual packets, even if they contain port numbers allowed by a rule set.

Measurement units:
Not applicable

Issues:

rule sets

See also:
allowed traffic (3.1)
proxy (3.14)
rejected traffic (3.15)
rule set (3.16)

3.8 External network

Definition:
The segment or segments not protected by the network security DUT/SUT.

Discussion:
Firewalls are deployed between protected and unprotected segments. The external network is not protected by the DUT/SUT.

Measurement units:
Not applicable

Issues:

See also:
demilitarized zone (DMZ) (3.5)
protected network (3.13)

3.9 Homed

Definition:
The number of logical interfaces a DUT/SUT contains.

Discussion:
Firewalls MUST contain at least two interfaces, using a dual-homed configuration. In network topologies where a DMZ is used, the firewall contains at least three interfaces and is said to be tri-homed. Additional interfaces would make a firewall quad-homed, quint-homed, and so on.

Issues:

It is theoretically possible for a firewall to contain one physical interface and multiple logical interfaces. This configuration is strongly discouraged for testing purposes because of the possibility of leakage between protected and unprotected segments.

See also:
Dual-homed (3.6)
Tri-homed (3.19)

3.10 Packet filtering

Definition:
The process of controlling access by examining packets based on packet header content.

Discussion:
Packet-filtering devices forward or deny packets based on information in each packet's header, such as IP address or TCP port number. A packet-filtering firewall uses a rule set (see section 3.16) to determine which traffic should be forwarded and which should be blocked.

Measurement units:
Not applicable

Issues:

See also:
dynamic proxy (3.7)
proxy (3.14)
rule set (3.16)
stateful inspection (3.18)

3.11 Perimeter network

Definition:
A network segment or segments located between protected and external networks. Perimeter networks are often called DMZ networks.

Discussion:
See the definition of DMZ for a discussion.

Measurement units:
Not applicable

Issues:
Dual-homed
Tri-homed

See also:
Demilitarized zone (DMZ) (3.5)
external network (3.8)
protected network (3.13)

3.12 Policy

Definition:
A document defining acceptable use of protected, DMZ, and external networks.

Discussion:
Security policies generally do not spell out specific configurations for firewalls; rather, they set general guidelines for what it and is not acceptable network behavior.

The actual mechanism for controlling access is usually the rule set (see section 3.16) implemented in the DUT/SUT.

Measurement units:
Not applicable

Issues:

See also:
Rule set (3.16)

3.13 Protected network

Definition:
A network segment or segments to which access is controlled by the DUT/SUT.

Discussion:
Firewalls are intended to prevent unauthorized access either to or from the protected network. Depending on the configuration specified by the policy and rule set, the DUT/SUT may allow stations on the protected segment to act as clients for servers on either the DMZ or the external network, or both.

Protected networks are often called "internal networks." That term is not used here because firewalls increasingly are deployed within an organization, where all segments are by definition internal.

Measurement units:
Not applicable

Issues:

See also:
Demilitarized zone (DMZ) (3.5)
external network (3.8)
policy (3.12)
rule set (3.16)

3.14 Proxy

Definition:
A request for a connection made on behalf of a host.

Discussion:
Proxy-based firewalls never allow direct connections between hosts. Instead, two connections are established: one between the client host and the DUT/SUT, and another between the DUT/SUT and server host.

As with packet-filtering firewalls, proxy-based devices use a rule set to determine which traffic should be forwarded and which should be rejected.

Measurement units:
Not applicable

Issues:

See also:

dynamic proxy (3.7)
packet filtering (3.10)
stateful inspection (3.18)

3.15 Rejected traffic

Definition:
Packets dropped as a result of the rule set of the DUT/SUT.

Discussion:
Firewalls MUST reject any traffic not explicitly permitted in the rule set. Dropped packets MUST NOT be included in calculating the forwarding rate or maximum forwarding rate of the DUT/SUT.

Measurement units:
Not applicable

Issues:

See also:
policy (3.12)
rule set (3.16)

3.16 Rule set

Definition:
The collection of access control rules that determines which packets the DUT/SUT will forward and which it will reject.

Discussion:
Rule sets control access to and from the network interfaces of the DUT/SUT. By definition, rule sets MUST NOT apply equally to all network interfaces; otherwise there would be no need for the firewall. Therefore, a specific rule set MUST be applied to each network interface in the DUT/SUT.

The order of rules within the rule set is critical. Firewalls generally scan rule sets in a "top down" fashion, which is to say that the device compares each packet received with each rule in the rule set until it finds a rule that applies to the packet. Once the device finds an applicable rule, it applies the actions defined in that rule (such as forwarding or rejecting the packet) and ignores all subsequent rules. For testing purposes, the rule set MUST conclude with a rule denying all access.

Measurement units:
Not applicable

Issues:

See also:
Demilitarized zone (DMZ) (3.5)
external network (3.8)
policy (3.12)

protected network (3.13)
rejected traffic (3.15)

3.17 Session

Definition:
A logical connection established between two stations using a known protocol.

Discussion:
Because of the application-layer focus of many firewalls, sessions are a more useful metric than the packet-based measurements used in benchmarking routers and switches. Although firewall rule sets generally work on a per-packet basis, it is ultimately sessions that a firewall must handle. For example, the number of file transfer protocol (ftp) sessions a DUT/SUT can handle concurrently is a more meaningful measurement in benchmarking performance than the number of ftp "open" packets it can reject. Further, a stateful inspection firewall will not forward individual packets if those packets' headers conflict with state information maintained by the firewall.

For purposes of this document, a session MUST be established using a known protocol such as TCP. A traffic pattern is not considered a session until it successfully completes the establishment procedures defined by that protocol.

Also for purposes of this document, a session constitutes the logical connection between two end-stations and not the intermediate connections that proxy-based firewalls may use.

Issues:

See also:
policy (3.12)

proxy (3.14)
rule set (3.16)
stateful inspection (3.18)

3.18 Stateful inspection

Definition:
The process of forwarding or rejecting traffic based on the contents of a state table maintained by a firewall.

Discussion:
Packet filtering and proxy firewalls are essentially static, in that they always forward or reject packets based on the contents of the rule set.

In contrast, devices using stateful inspection will only forward packets if they correspond with state information maintained by the device about each session. For example, a stateful inspection device will reject a packet on port 20 (ftp-data) if no session has been established over the ftp control port (usually port 21).

Measurement units:
Not applicable

Issues:

See also:
dynamic proxy (3.7)
packet filter (3.10)
proxy (3.14)

3.19 Tri-homed

Definition:
A firewall with three network interfaces.

Discussion:
Tri-homed firewalls connect three network segments with different network addresses. Typically, these would be protected, DMZ, and external segments.

Measurement units:
Not applicable

Issues:
Usually the differentiator between one segment and another is its IP address. However, firewalls may connect different networks of other types, such as ATM or Netware segments.

See also:
Dual-homed (3.6)
Homed (3.9)

3.20 User

Definition:
The person or machine requesting access to resources protected by the DUT/SUT.

Discussion:
"User" is a problematic term in the context of firewall performance testing, for several reasons. First, a user may in fact be a machine or machines requesting services through the DUT/SUT. Second, different "user" requests may require radically different amounts of DUT/SUT resources. Third, traffic profiles vary widely from one organization to another, making it difficult to characterize the load offered by a typical users.

For these reasons, we prefer not to measure DUT/SUT performance in terms of users supported. Instead, we describe performance in terms of maximum forwarding rate and maximum number of sessions sustained. Further, we use the term "data source" rather than user to describe the traffic generator(s).

Measurement units:
Not applicable

Issues:

See also:

data source (3.3)

4. Security considerations

Security considerations are explicitly excluded from this memo. The authors plan to address security and management concerns in a separate proposal brought to the IETF's security directorate.

5. References

Bradner, S., editor. "Benchmarking Terminology for Network Interconnection Devices." RFC 1242.

Bradner, S., and McQuaid, J. "Benchmarking Methodology for Network Interconnect Devices." RFC 1944.

Mandeville, B. "Benchmarking Terminology for LAN Switching Devices." ftp://ietf.org/internet-drafts/draft-ietf-bmwg-lanswitch-07.txt

Newman, D., and Melson, B. "Can Firewalls Take the Heat?" Data Communications, November 21, 1995. http://www.data.com/Lab_Tests/Firewalls.html

Newman, D., Holzbaur, H., and Bishop, K. "Firewalls: Don't Get Burned," Data Communications, March 21, 1997. http://www.data.com/lab_tests/firewalls97.html

Ranum, M. "Firewall Performance Measurement Techniques: A Scientific Approach." http://www.clark.net/pub/mjr/pubs/fwperf/intro.htm

Shannon, G. "Profile of Corporate Internet Application Traffic." http://www.milkyway.com/libr/prof.html

6. Acknowledgments

The authors wish to thank the IETF Benchmarking Working Group for agreeing to review this document. Ted Doty (Internet Security Systems), Shlomo Kramer (Check Point Software Technologies), Bob Mandeville (European Network Laboratories), Brent Melson (National Software Testing Laboratories), Marcus Ranum (Network Flight Recorder Inc.), Greg Shannon (Ascend Communications), Rick Siebenaler (Cyberguard), and Greg Smith (Check Point Software Technologies) offered valuable contributions and critiques during this project.

7. Contact Information

David Newman
Data Communications magazine
1221 Avenue of the Americas, 41st Floor
New York, NY 10020
USA

212-512-6182 voice
212-512-6833 fax
dnewman@data.com

Helen Holzbaur
National Software Testing Laboratories Inc.
625 Ridge Pike
Conshohocken, PA 19428
USA
helen@nstl.com

Jim Hurd
National Software Testing Laboratories Inc.
625 Ridge Pike
Conshohocken, PA 19428
USA
jimh@nstl.com

Steven Platt
National Software Testing Laboratories Inc.
625 Ridge Pike
Conshohocken, PA 19428
USA
steve@nstl.com