Benchmarking Working Group D. Newman
INTERNET-DRAFT Data Communications
Expires in January 1998 H. Holzbaur, J. Hurd, and S. Platt
National Software Testing Laboratories

Benchmarking Terminology for Network Security Devices

<draft-ietf-bmwg-secperf-00.txt>

Status of This Memo

1. Introduction

Despite the rapid rise in deployment of network security devices such as firewalls and authentication/encryption products, there is no standard method for evaluating the performance of these devices.

The lack of a standard is troubling for two reasons. First, hardware and software implementations vary widely, making it difficult to do direct performance comparisons. Second, a growing number of organizations are deploying these devices on internal networks that operate at relatively high data rates, while many network security devices are optimized for use over relatively low-speed wide-area connections. As a result, users are often unsure whether the products they buy will stand up to the relatively heavy loads found on internal networks.

This document defines terms used in measuring the performance of network security devices. It extends the terminology already used for benchmarking routers and switches to network security devices.

The primary metrics defined in this document are maximum forwarding rate and maximum number of connections.

Depending on the outcome of discussions within the BMWG, we may also attempt to classify devices using various architectural considerations (proxy, packet filter) or offered load levels

(high, medium, low) as criteria. Additionally, new metrics may need to be defined to evaluate application-level issues.

2. Existing definitions

This document uses the conceptual framework established in RFCs 1242 and 1944 and draft-ietf-bmwg-lanswitch-05.txt, which describes benchmarking of LAN
switch performance. In addition to defining basic practices, these documents
contain discussions of several terms relevant to benchmarking performance of network security devices. This document uses the definition format described in RFC 1242, Section 2. Readers should consult these documents before making use of this document.

3. Term definitions

3.1 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. Obviously, 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 pattern matching based on human characteristics such as signature, speech, or retina patterns.

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:

See also:
forwarding rate (3.9)
user (3.25)
virtual client (3.26)

3.2 Bidirectional traffic

Definition:

Packets presented to a DUT/SUT such that the network interfaces of the DUT/SUT both receive and transmit traffic.

Discussion:
Traffic patterns offered to the DUT/SUT MUST be bidirectional or fully meshed. See forwarding rate (3.9) for a more complete discussion of issues with traffic patterns.

Measurement units:
Not applicable

Issues:
truncated binary exponential back-off algorithm

See Also:
forwarding rate (3.9)
fully meshed traffic (3.10)
unidirectional traffic (3.24)

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. However, each virtual client MUST offer traffic to only one interface.

Measurement units:
Not applicable

Issues:

See also:
user (3.25)
virtual client (3.26)

3.4 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, security devices (and possibly other public resources such as WWW or FTP servers) often reside in 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 devices MAY constitute the DMZ, in which case the devices connected the protected network with the DMZ and the DMZ with the external network MUST have two network interfaces.

Measurement units:
Not applicable

Issues:
Dual-homed
Multihomed

See also:
external network (3.8)

perimeter network (3.15)
protected network (3.17)

3.5 Device under test (DUT)

Definition:
The network security device to which traffic is offered and response measured.

Discussion:
A single station, generally equipped with at least two network interfaces.

Measurement units:
Not applicable

Issues:

See also:
system under test (SUT) (3.23)

3.6 Dual-homed

Definition:
A station with at least two network interfaces.

Discussion:
Dual-homed network security devices connect two segments with different network-layer addresses.

Measurement units:
Not applicable

Issues:

See also:
multihomed (3.12)

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 3.18) typically are configured to "listen" on a given port number for client requests. However, some devices set up a proxy service only when a client requests the service.

Measurement units:
Not applicable

Issues:
rule sets

See also:
proxy (3.18)
rule sets (3.20)

3.8 External network

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

Discussion:
Network security devices 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) (3.4)
protected network (3.17)

3.9 Forwarding rate

Definition: The number of bits per second a DUT/SUT can transmit to the correct destination network interface in response to a specified offered load.

Discussion:
Network security devices are by definition session-oriented: They will only grant access to a desired resource once authentication occurs and a session has been established.

Because application-layer sessions are always involved, unidirectional packet-per-second metrics are not meaningful in the

context of testing network security devices. Instead, this

definition MUST measure application-layer performance once a session has been established.

Forwarding rate refers to the number of bits per second observed on the output side of the network interface under test. Forwarding rate can be measured with different traffic orientations and distributions. When multiple network interfaces are measured, measurements MUST be observed from the interface with the highest forwarding rate.

Measurement units:
bits per second (bit/s)
kilobits per second (kbit/s)
Megabits per second (Mbit/s)

Issues:
truncated binary exponential back-off algorithm
unidirectional vs. bidirectional

See Also:
authentication (3.1)
maximum forwarding rate (3.11)
offered load (3.13)
unidirectional traffic (3.24)

3.10 Fully meshed traffic

Definition:
Packets forwarded simultaneously among all of a designated number of network interfaces of a DUT/SUT such that each of the interfaces under test will both forward packets to and receive packets from all of the other interfaces.

Discussion:
Fully meshed traffic is the most thorough method of exercising the transmitting and receiving capabilities of the DUT/SUT.

Unlike past definitions for router or switch testing, it should be noted that fully meshed traffic in this context is not necessarily symmetrical. While all of a designated group of network interfaces

MUST simultaneously send and receive traffic, the type and amount of traffic offered MAY differ on each interface. For example, a network security device may see more traffic from the protected network bound for the external network than the opposite (although the inverse could be true during an attack on the DUT/SUT).

Measurement units:
Not applicable

Issues:
Half duplex
Full duplex

See also:

bidirectional traffic (3.2)
unidirectional traffic (3.24)

3.11 Maximum forwarding rate

Definition:
The highest forwarding rate of a network security device taken from a set of iterative measurements.

Discussion:
Maximum forwarding rate may degrade before maximum load is offered.

Unlike benchmarks for evaluating router and switch performance, this definition MUST involve measurement of application-layer performance rather than network-layer packet-per-second metrics.

Measurement units:
Megabits per second
kbytes per second
bytes per second

Issues:
full duplex vs. half duplex
truncated binary exponential back-off algorithm

See also:
bidirectional traffic (3.2)

partially meshed traffic (3.24)
unidirectional traffic

3.12 Multihomed

Definition:
A network security device with more than two network interfaces.

Discussion:
Multihoming is a way to connect three or more networks-protected, DMZ, and external-with a single network security device. However, this configuration is not mandatory if multiple network security devices are used. For example, one device could secure the connection between an external and DMZ network, while another could secure the connection between a DMZ and protected network; the two stations collectively form the SUT.

Because of the differences in traffic patterns between dual-homed and multihomed devices, direct performance comparisons should be avoided. However, it is acceptable to compare results between a dual-homed device and a DUT/SUT in which only two network interfaces are used.

Measurement units:
Not applicable

Issues:
truncated binary exponential back-off algorithm

See also:
bidirectional traffic (3.2)
dual-homed (3.6)
fully meshed traffic (3.10)

3.13 Offered load

Definition:
The number of bits per second that an external source can transmit to a DUT/SUT for forwarding to a specified network interface or interfaces.

Discussion:

The load that an external source actually applies to a DUT/SUT may be lower than the external source attempts to apply because of collisions on the wire. The transmission capabilities of the external source SHOULD be verified without the DUT/SUT by transmitting unidirectional traffic.

Measurement units:
bits per second
kilobits per second (kbit/s)
Megabits per second (Mbit/s)

Issues:
truncated binary exponential back-off algorithm

See also:
forwarding rate (3.9)
maximum forwarding rate (3.11)

3.14 Packet filtering

Definition:
The process of controlling access by examining packets based on network-layer or transport-layer criteria.

Discussion:
Packet-filtering devices forward or deny packets based on information in each packet's header. A packet-filtering network security device uses a rule set (see section 3.20) to determine which traffic should be forwarded and which should be blocked. Packet filtering may be used in a dual-homed or multihomed device.

Measurement units:
Not applicable

Issues:

See also:
dynamic proxy (3.7)

proxy (3.18)
rule set (3.20)
stateful inspection (3.22)

3.15 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 (which see) for a discussion.

Measurement units:
Not applicable

Issues:
Dual-homed
Multihomed

See also:
Demilitarized zone (DMZ) (3.4)
external network (3.8)
protected network (3.17)

3.16 Policy

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

Discussion:
Security policies generally do not spell out specific configurations for network security devices; 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 3.20) implemented in the DUT/SUT.

Measurement units:
Not applicable

Issues:

See also:
Rule set (3.20)

3.17 Protected network

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

Discussion:
Network security devices 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 network security devices increasingly are deployed within an organization, where all segments are by definition internal.

Measurement units:
Not applicable

Issues:

See also:
Demilitarized zone (DMZ) (3.4)
external network (3.8)
policy (3.16)
rule set (3.20)

3.18 Proxy

Definition:
The process of requesting sessions with servers on behalf of clients.

Discussion:
Proxy-based network security devices never involve direct connections between client and server. Instead, two sessions are established: one between the client and the DUT/SUT, and another between the DUT/SUT and server.

As with packet-filtering network security devices, proxy-based devices use a rule set (which see) to determine which traffic should be forwarded and which should be blocked.

Measurement units:
Not applicable

Issues:

See also:
dynamic proxy (3.7)
packet filtering (3.14)
stateful inspection (3.22)

3.19 Rejected traffic

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

Discussion:
Network security devices typically are configured to drop any traffic not explicitly permitted in the rule set (which see). 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:
forwarding rate (3.9)
maximum forwarding rate (3.11)
policy (3.16)
rule set (3.20)

3.20 Rule set

Definition:
The collection of definitions 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 network security device. Therefore, a specific rule set MUST be applied to each network device used in the DUT/SUT.

The order of rules within the rule set is critical. Network security devices 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 purposes of this document, the rule set MUST conclude with a rule denying all access except that which is permitted in the rule set.

Measurement units:
Not applicable

Issues:

See also:
Demilitarized zone (DMZ) (3.4)
external network (3.8)
policy (3.17)
protected network (3.18)
rejected traffic (3.19)

3.21 Session

Definition:
A logical connection established between two stations using a known protocol. For purposes of this document, a session MUST be conducted over either TCP (RFC 793) or UDP (RFC 768).

Discussion:
Because of the application-layer focus of many network security devices, sessions are a more useful metric than the packet-based measurements used in benchmarking routers and switches. Although network security device rule sets generally work on a per-packet basis, it is ultimately sessions that a network security device 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 device (which see) will not forward individual packets if those packets' headers conflict with state information maintained in the device's rule set.

For purposes of this document, a session MUST be established using a known protocol. 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 network security devices may use.

Issues:

See also:
policy (3.16)
proxy (3.18)
rule set (3.20)
stateful inspection (3.22)

3.22 Stateful inspection

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

Discussion:
Packet filtering and proxy devices are essentially static, in that they always forward or reject traffic based on the contents of the rule set. Devices using stateful inspection, in contrast, will only forward traffic if it corresponds with state information maintained by the device about each session. For example, a stateful inspection device will reject a packet on TCP port 21 (ftp DATA) if no ftp session has been established.

Measurement units:
Not applicable

Issues:

See also:
dynamic proxy (3.7)

packet filter (3.14)
proxy (3.18)

3.23 System under test (SUT)

Definition:
The collective set of network security devices to which traffic is offered as a single entity and response measured.

Discussion:
A system under test may comprise multiple network security devices. A typical configuration involves two or more devices, with at least one located between the protected network and DMZ and at least one other located between the DMZ and external network. Some devices may be active, such as firewalls or authentication products; other devices, such as systems for logging, may be passive.

Measurement units:
Not applicable

Issues:

See also:
demilitarized zone (DMZ) (3.4)
device under test (3.5)
external network (3.8)
protected network (3.17)

3.24 Unidirectional traffic

Definition:
Packets offered to the DUT/SUT such that the sending and receiving network interface or interfaces are mutually exclusive.

Discussion:
This definition is included mainly for purposes of completeness; it is not particularly meaningful in the context of network security device performance. As noted in the discussion of forwarding rate (see section 3.9), network security devices almost invariably involve sessions with bidirectional traffic flow.

However, unidirectional traffic is appropriate for evaluating the maximum forwarding rate of data sources (absent the DUT/SUT), and for evaluating the maximum forwarding rate of certain connectionless protocols.

Measurement units:
Not applicable

Issues:
half duplex vs. full duplex

See also:
bidirectional traffic (3.2)
forwarding rate (3.9)
maximum forwarding rate (3.11)

3.25 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 security device 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.

Measurement units:
Not applicable

Issues:

See also:
data source (3.3)
virtual client (3.26)

3.26 Virtual client

Definition:
A subset of a data source that represents one individual user.

Discussion:
In offering traffic to the DUT/SUT it may be useful for one data source to emulate multiple users, machines, or networks. For

purposes of this document, each emulated user should be considered a virtual client.

One data source MAY offer traffic from multiple virtual clients to multiple network interfaces on the DUT/SUT. However, each virtual client MUST offer traffic to just one network interface.

Measurement units:
Not applicable

Issues:

See also:
data source (3.3)
user (3.25)

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-05.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 (Network 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 (Milkyway Networks), 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

Newman et al [Page 15]

INTERNET-DRAFT Terminology for Network Security Devices July 1997

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, PhD.
National Software Testing Laboratories Inc.

625 Ridge Pike
Conshohocken, PA 19428
USA
steve@nstl.com