Hillstone · Fortinet · Juniper
高端防火墙产品测评报告

亓亚烜　薛一波
清华大学信息技术研究院网络安全实验室

测试产品: Hillstone SA-5050 防火墙
报告版本: V1.0
测试日期: 2008年2 月2 日

测试结果摘要

1. SA-5050 防火墙在双向、零丢包率下的吞吐量，无论网包大小，性能均高于比较测评的FortiGate 3600A和NetScreen 5200。

2. SA-5050 防火墙达到了每秒24.5 万的TCP 新建连接速率。

3. SA-5050 防火墙对64-Byte 小包的转发速率达到3Gbps。

4. SA-5050 防火墙在复杂防火墙规则下，性能稳定，且不受网络流量变化影响。

1. 测试对象和测试仪器

本测试为山石网科 (Hillstone Networks Inc.) 委托清华大学信息技术研究院网络安全实验室 (NSLab, RIIT, Tsinghua Univ.) 进行的防火墙性能比对测试。

1.1. 本测试的测试对象

- Hillstone公司: SA-5050防火墙(图例: SA-5050)
  软件版本: SA5000-1.1R1d4。

用作性能对比的测试对象为:

- Juniper公司:NetScreen5200防火墙(图例: NS5200)
  软件版本: NS5000-5.0R8
- Fortinet公司: Fortigate3600A防火墙(图例:FG3600A)
  软件版本: FortiOS3.0build559

测试对象的主要性能标称见表1。

1.2. 本测试使用的测试仪器

- 防火墙网络层测试设备:
  硬件: SmartBits 6000C （SMB6000C）
  软件: Smartflow version 5.00
- 防火墙应用层测试设备:
  硬件: IXIA 1600T（IXIA1600T）
  软件: Ixload version 3.30
- 流汇聚交换机:
  H3C S5100-24P-EI 24 口千兆交换机 (H3C5100)
- 管理交换机:
  H3C S2126 24 口百兆交换机（H3C2126）

测试仪器见图1。

1.3. 本测试的主要测试依据

- RFC2544
- RFC2647
- RFC3511

表1. 测试对象主要性能参数标称

防火墙	吞吐量	最大并发连接数	新建连接速率	主要接口
SA-5050	8Gbps	5,000,000	200,000	12 GE, 6 GE/SFP
NS5200	4Gbps	1,000,000	20,000	8 mini-GBIC
FG3600A	4Gbps	1,000,000	25,000	8 GE, 2 GE/SFP

图1. 测试对象和测试仪器

1.4.测试平台拓扑

本测试被测防火墙、测试仪器、交换设备以及控制台连接拓扑见图2 和图3。

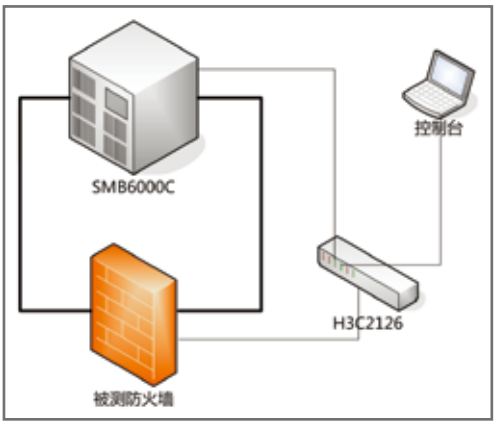


图2. 测试仪器配置方案1

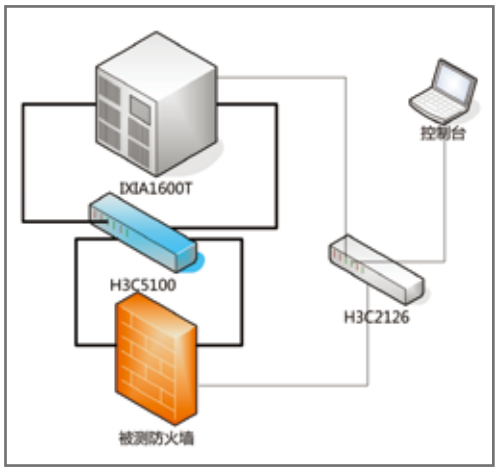


图3. 测试仪器配置方案2

2. 防火墙吞吐量测试

2.1. 测试目的

吞吐量是指防火墙在不丢包情况下能转发的最大网包数量。防火墙作为内外网之间的唯一数据通道，吞吐量的大小将直接影响到网络的整体性能。

2.2. 测试方法

防火墙的每一端口均直接连接到SmartBit6000C上。防火墙配置1 条规则，即所有端口的流量全部允许通过。测试分别对64 字节、128 字节、512 字节、1024 字节和1518 字节的网包流量吞吐量分别测试。测试仪器配置方案见图2。为了精确考察防火墙的双向处理能力，被测试防火墙的端口被均匀分配到trust 和untrust 两个域，测试使用双向流量。为了精确考察防火墙的吞吐量，依据RFC2544，测试中丢包率被严格设置为0。

2.3. 测试结果

吞吐量测试结果见图4、表2。

图4. 吞吐量测试结果

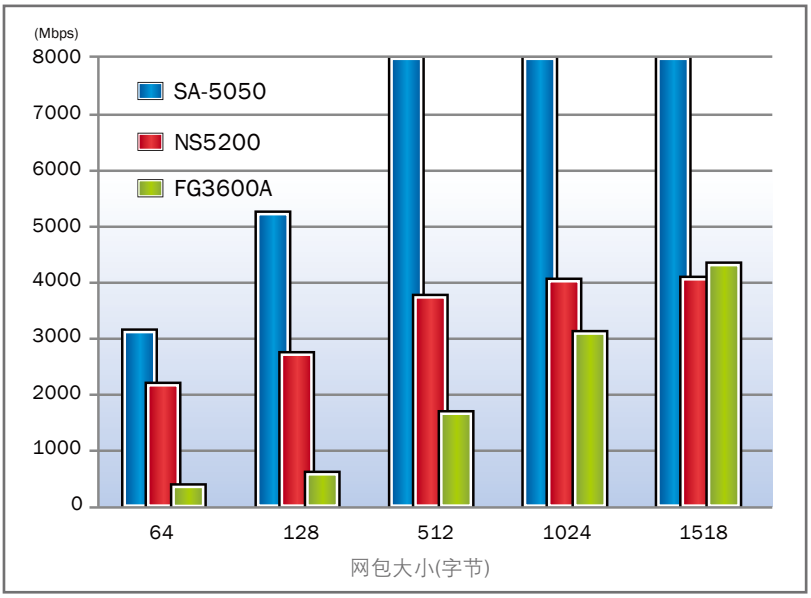


表2. 吞吐量测试结果

Throughput					
Packet size(bytes) / Throughput(Mbps)	64	128	512	1024	1518
SA-5050 (8GE)	2929.69	5125	7882.81	7960.94	7968.75
NS5200 (7GE)	1825.88	2287.3	3216.31	3450.1	3505.47
	2086.72	2614.06	3675.78	3942.97	4006.25
FG3600A (8GE)	250	445.313	1546.88	3015.63	4289.06

3. 防火墙平均时延测试

3.1. 测试目的

防火墙的时延是指测试仪器发送端口发出网包经过防火墙后到接收端口收到该网包的时间间隔。防火墙的平均时延是防火墙存储转发性能的重要指标。

3.2. 测试方法

测试中，被测防火墙的每一端口均直接连接到SmartBit6000C 上。被测防火墙配置1 条规则，即所有端口的流量全部允许通过。测试分别对64 字节、128字节、512 字节、1024 字节和1518 字节的网包流量时延分别测试。测试仪器配置方案见图2。

为了精确考察防火墙的双向处理能力，被测防火墙的端口被均匀分配到trust和untrust 两个域，测试使用双向流量，50%的流量从trust 到untrust 域，50%的流量从untrust 到trust 域。为了精确考察防火墙在高负荷运载下的平均处理时延，测试中使用了被测防火墙的所有端口并以95%的最高吞吐量（由测试1 得出）作为测试流量负载。

3.3. 测试结果：

平均时延测试结果见图5、表3。

图5. 平均时延测试结果

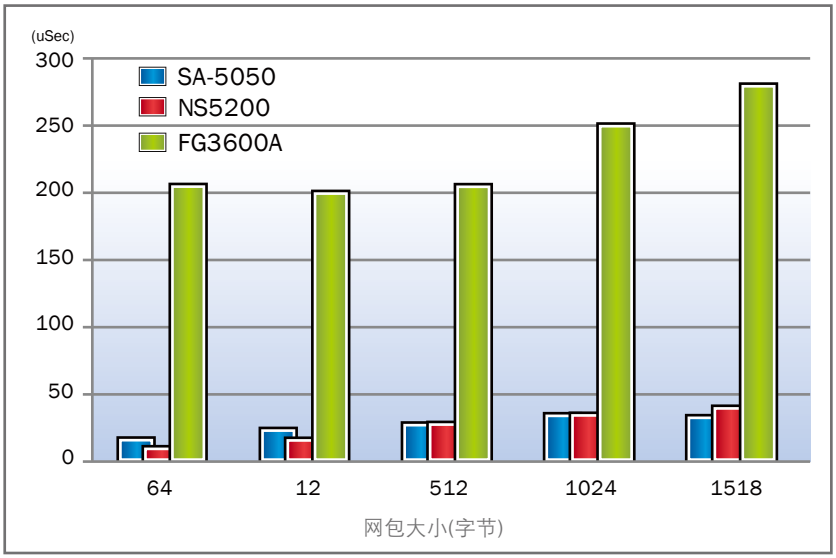


表3. 平均时延测试结果

Average Latency					
Latency(uSec) \ Packet size(bytes)	64	128	512	1024	1518
SA-5050 (8GE)	8.628	11.29	16.036	25.157	32.159
NS5200 (7GE)	5.095	6.911	16.205	25.713	35.413
FG3600A (8GE)	199.633	196.422	200.793	243.274	280.755

4. 防火墙最大并发连接数测试

4.1. 测试目的

最大TCP 并发连接数是防火墙能同时维护的网络连接数量，它反映了被测防火墙设备对多个连接的访问控制能力和连接状态跟踪能力。

4.2. 测试方法

测试中，被测防火墙配置1 条规则，即所有端口的流量全部允许通过。选取被测防火墙的两个端口分别作为连接内网用户和外网服务器的接口。测试仪IXIA1600T 用来产生TCP 三次握手的流量。

测试仪器配置方案见图3。

为了考察被测防火墙的极限性能，我们使用了IXIA1600T 的全部22 个端口，通过24 口的H3C5100交换机将流量汇聚到防火墙（防火墙的内网和外网使用交换机剩余的两个端口）。

4.3. 测试结果

最大连接数测试结果见表4。

表4. 最大连接数测试结果

Concurrent TCP Connecion Capacity	
SA-5050	4999325
NS5200	999937
FG3600A	4865454

5. 防火墙最大新建连接速率测试

5.1. 测试目的

防火墙最大新建连接速率测试分别使用TCP 和HTTP 进行测试。

防火墙最大新建连接速率TCP 测试是指防火墙在单位时间内所能建立TCP连接的数量，即防火墙处理TCP 三次握手的能力。

与TCP 新建连接不同，防火墙最大新建连接速率HTTP 测试不仅仅考察被测防火墙对TCP 三次握手的处理，同时还要考察被测防火墙对TCP 连接关闭时的四次握手处理。测试中还添加了1 字节的HTTP 通信流量，即三次握手之后，用户从服务器端GET 1 字节的流量，然后进行四次握手的连接关闭处理。

5.2. 测试方法

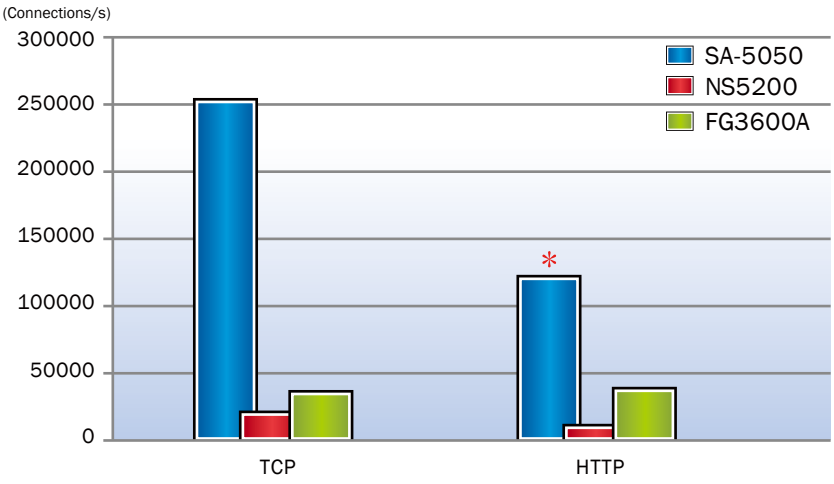
测试中，被测防火墙配置1 条规则，即所有端口的流量全部允许通过。选取被测防火墙的两个端口分别作为连接内网用户和外网服务器的接口。测试仪IXIA1600T 用来产生500 个内网用户访问5 个外HTTP服务器的流量。测试仪器配置方案见图3。

为了考察被测防火墙的极限性能，我们使用了IXIA1600T 的全部22 个端口，通过24 口的SR-550 交换机将流量汇聚到防火墙（防火墙的内网和外网使用交换机剩余的两个端口）。

5.3. 测试结果

新建连接速率测试结果见图6、表5。注意：由于IXIA 测试仪的全部三块板卡只能提供每秒约12 万的HTTP 连接流量（使用短接测试得出），而测试中SA-5050的HTTP 连接处理能力达到了11.5 万（此时其处理器平均利用率约为70%），因此测试中的结果仅是其真实HTTP 新建连接速率的一个下界。

图6. 新建连接速率测试结果



* 由于IXIA测试仪的全部三块板卡的极限只能提供每秒约12万的HTTP新建连接

表5. 新建连接速率测试结果

Maximum TCP Connection Estblishment Rate (TCP)	
SA-5050	246863
NS5200	17385
FG3600A	33828

Maximum TCP Connection Estblishment Rate (HTTP)	
SA-5050	*115000
NS5200	5779
FG3600A	33295

* 受测试仪限制，CPU 70%

6. 网包分类性能

6.1. 测试目的

网包分类性能考察防火墙对每一个网流的第一个网包的处理能力。本测试中所指网流为具有相同五元组（源IP、目标IP、源端口、目标端口、传输层协议）的一系列网包。网包分类性能对防火墙的影响体现在多个方面，这里从流量的角度进行来分析：首先，对合法流量，虽然防火墙通常为合法流量建立连接状态，并通过快速通道的精确匹配进行高速转发，但新建连接都需要对网流的首包进行分类，因此网包分类直接影响新建连接的速率；其次，对非法流量，由于防火墙通常不为非法流量建立连接状态，所以非法流量的网包即使属于同一网流，都需要进行分类，因此网包分类的性能也反映了防火墙处理大量非法流量的能力。

6.2. 测试方法

测试中， 被测防火墙的所有端口均配置在一个域中并分别连接到SmartBit6000C 上。测试主要考察防火墙在大规模防火墙规则（即网包分类规则）下，对不同比例的合法、非法流量的总体处理能力。输入流量选取1518 字节的网包。测试仪器配置方案见图2。

为了考察合法、非法流量对网包分类性能的不同影响，测试流量包括不同比例的合法流量（防火墙允许通过的流量,GOOD_TRAFIC）和非法流量（防火墙拒绝通过的流量,BAD_TRAFFIC ）。定义非法流量占总流量的比例（BAD_TRAFFIC_RATE）为：BAD_TRAFFIC_RATE =（BAD_TRAFFIC）/（BAD_TRAFFIC+GOOD_TRAFFIC）*100%

为了考察防火墙规则变化对网包分类性能的影响，防火墙规则分别采用两组复杂度不同的规则。两组规则数量均为2000 条，但第一组规则（SET1）可以从数学上简化为8 条范围匹配（range-match）的规则或24 条最长前缀匹配（prefix-match）的规则，而第二组规则（SET2）则只能简化为80 条范围匹配的规则或400 条最长前缀匹配的规则。测试中，合法流量与第1999 条规则匹配，并允许通过；非法流量与第2000 条匹配，不允许通过。

6.3. 测试结果

网包分类性能测试结果见图7、表6和图8、表7。从测试中可以看出：SA-5050 防火墙的性能稳定，无论非法流量所占比例大小，无论输入规则复杂程度，均保持转发时处理能力的93%以上；NS5200 防火墙性能不受规则复杂程度影响，但当非法流量达到80%时，其整体处理能力下降到30%；FG3600A 防火墙的性能随规则复杂程度增加及非法流量所占比例增大而明显下降，尤其是在使用SET2规则时，FG3600A 无法通过0 丢包率的测试。

图7. 网包分类性能（规则集合SET1）

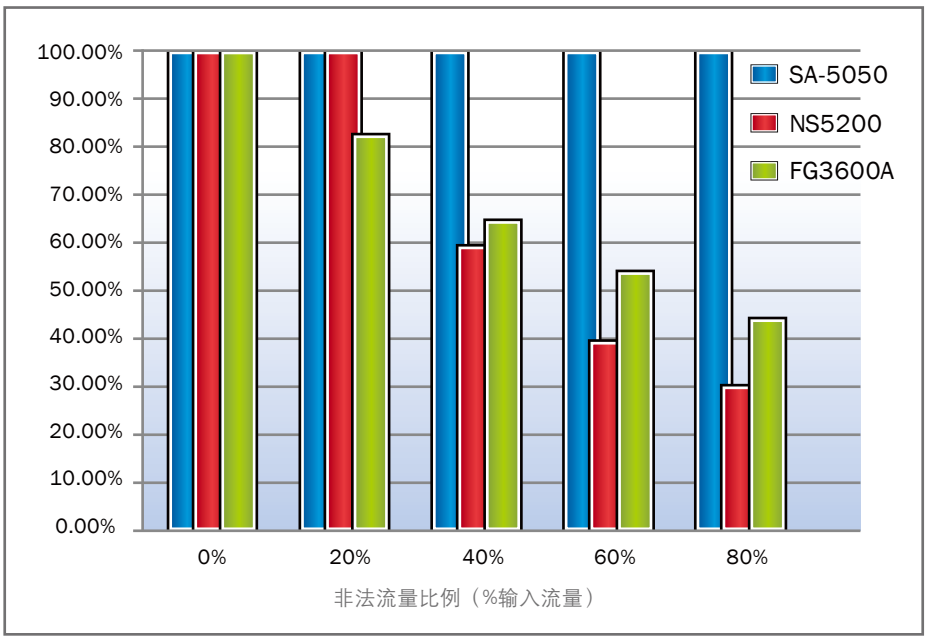


表6 网包分类性能（规则集合SET1）

RuleSet 1					
performance \ bad traffic rate (%)	0%	20%	40%	60%	80%
SA-5050 (8GE)	7968.75	7968.75	7968.75	7968.75	7968.75
NS5200 (7GE)	3469.238	3596.56	2049.76	1366.85	1023.85
FG3600A (8GE)	4000	3264	2574	2123	1748

图8. 网包分类性能、（规则集合SET2）

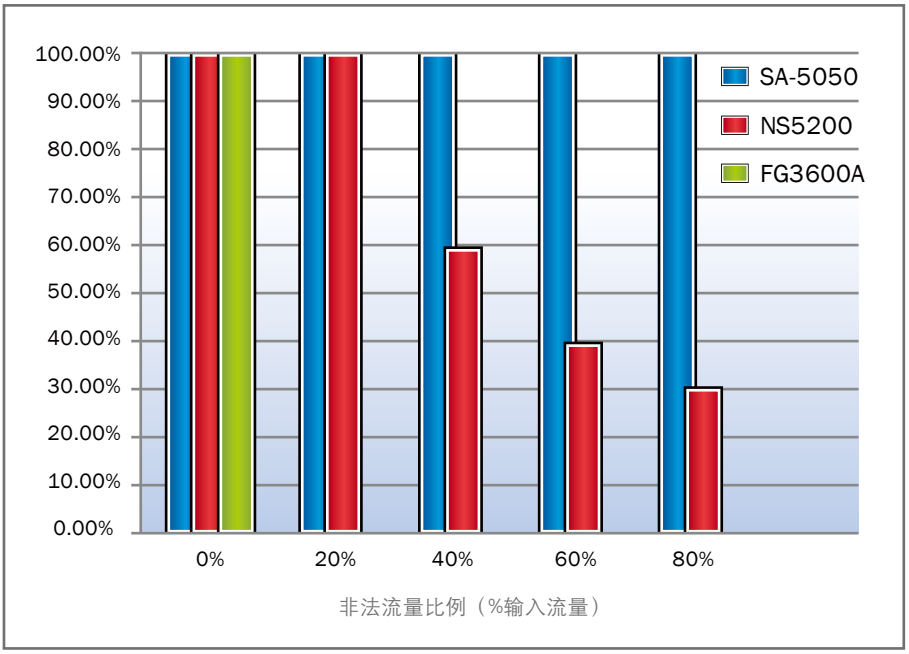


表7. 网包分类性能（规则集合SET2）

RuleSet 2					
performance \ bad traffic rate (%)	0%	20%	40%	60%	80%
SA-5050 (8GE)	7968.75	7968.75	7968.75	7968.75	7492.19
NS5200 (7GE)	3469.238	3596.56	2049.76	1366.85	1023.85
FG3600A (8GE)	4000	0	0	0	0

清华大学 信息技术研究院
网络安全实验室, FIT 3-419, 100084
Tel: 86-10-62797765 Fax: 86-10-62772393