Tuning of Iptables v1.2.11
Fedora Core Release 3
Using Test Equipments
Avalanche 2500 / Reflector 2500

by
Gregory FRESNAIS
EMEA Business Development
Spirent Communications

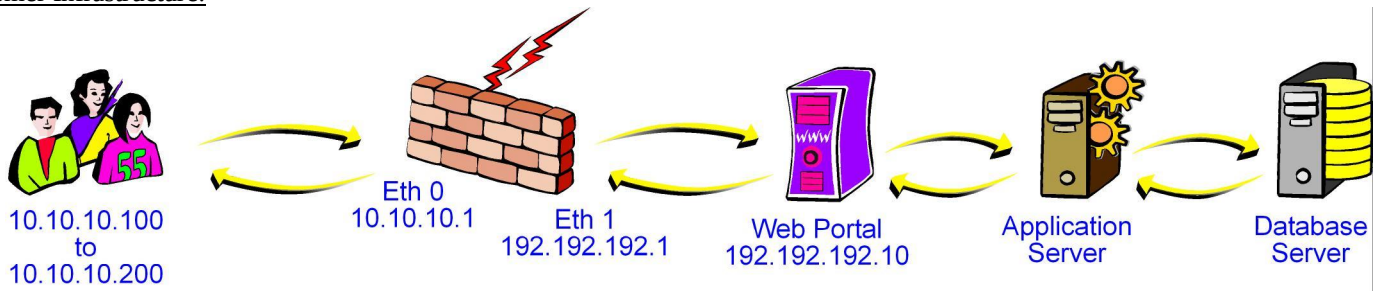
The proliferation of network attacks and security issues has had a significant effect on network designs and architectures. Network security continues to be a hot topic among networks, with firewalls playing a central role in a network's security. Because of the increasing sophistication of attacks, firewall vendors have responded with ever increasing features and complexity that attempt to mitigate these attacks. However, this complexity comes at a cost: performance, stability and reliability can often take unexpected turns by these changes. Deploying firewalls, and indeed, any security infrastructure, will undoubtedly reduce performance, a risk that may be important to consider during firewall deployments.

Spirent Communications provide solution to run performance, scalability and security tests on firewalls.
The testing will benefit from Avalanche's ability to simulate highly realistic clients and Reflector's robust server emulation.

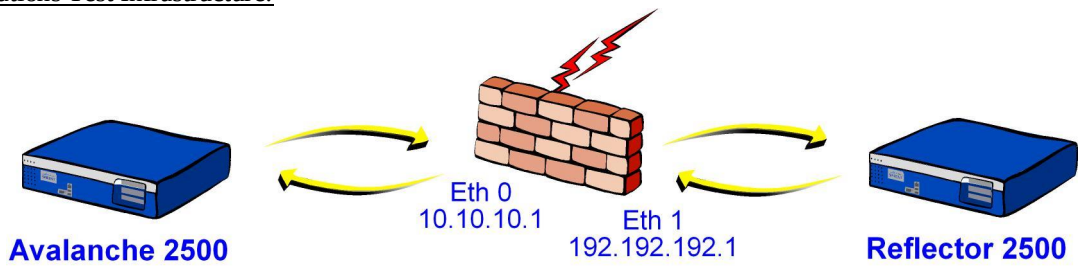
Firewall Platform under evaluation is:

Athlon 2.6 Ghz
512 Mo of Ram
HD 40 Go
2 NICS 3COM
Iptable v1.2.11 on Fedora Core Release 3

Customer Infrastructure:



Spirent Communications Test Infrastructure:



Iptables configuration:

#!/bin/bash

```
#!/bin/bash
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_nat
iptables -F
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t nat -F
iptables -A OUTPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT  -i lo -p ALL -j ACCEPT
iptables -A OUTPUT -o lo -p ALL -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -i eth0 -d 10.10.10.1 --dport 80 -j DNAT --to 192.192.192.10:80
iptables -A FORWARD -p tcp -i eth0 -d 192.92.192.10 --dport 80 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.192.192.0/24 -o eth1 -j MASQUERADE
iptables -A INPUT   -p icmp -j ACCEPT
iptables -A OUTPUT  -p icmp -j ACCEPT
iptables -A FORWARD -p icmp -j ACCEPT
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -A INPUT -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -A FORWARD -j ACCEPT
```

Iptables configuration with Tuning:

#!/bin/bash

```
#!/bin/bash
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_nat
iptables -F
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t nat -F
iptables -A OUTPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT  -i lo -p ALL -j ACCEPT
iptables -A OUTPUT -o lo -p ALL -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -i eth0 -d 10.10.10.1 --dport 80 -j DNAT --to 192.192.192.10:80
iptables -A FORWARD -p tcp -i eth0 -d 192.92.192.10 --dport 80 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.192.192.0/24 -o eth1 -j MASQUERADE
iptables -A INPUT   -p icmp -j ACCEPT
iptables -A OUTPUT  -p icmp -j ACCEPT
iptables -A FORWARD -p icmp -j ACCEPT
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -A INPUT -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -A FORWARD -j ACCEPT

# Tuning Iptables by Gregory FRESNAIS (EMEA Business Development at Spirent Communications)

echo 5 > /proc/sys/net/ipv4/tcp_keepalive_intvl &&
echo 3 > /proc/sys/net/ipv4/tcp_keepalive_probes &&
echo 180 > /proc/sys/net/ipv4/tcp_keepalive_time &&
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout &&
echo 4096 > /proc/sys/net/ipv4/tcp_max_syn_backlog &&
echo 500000 > /proc/sys/net/ipv4/netfilter/ip_conntrack_max &&
echo 500000 > /proc/sys/net/ipv4/ip_conntrack_max
```

Validation of maximum bandwidth – 1 Test

Spirent Communications Performance Level Ranking:

- No unsuccessful HTTP Transaction

Validation of maximum new TCP connections per second – 6 Tests

Spirent Communications Performance Level Ranking:

- Number of concurrent TCP connections must be under 200
- Maximum response time must be under 100 ms
- No unsuccessful HTTP Transaction

Validation of maximum concurrent TCP connections – 6 Tests

Spirent Communications Performance Level Ranking:

- Maximum response time must be under 100 ms
- No unsuccessful HTTP Transaction

Validation of maximum new HTTP transactions per second – 6 Tests

Spirent Communications Performance Level Ranking:

- Number of concurrent TCP connections must be under 200
- Maximum response time must be under 100 ms
- No unsuccessful HTTP Transaction

Detail about different test:

T01: Maximum HTTP Transactions per Second to download file of 512 Bytes
T02: Maximum HTTP Transactions per Second to download file of 1KB
T03: Maximum HTTP Transactions per Second to download file of 5KB
T04: Maximum HTTP Transactions per Second to download file of 10KB
T05: Maximum HTTP Transactions per Second to download file of 50KB
T06: Maximum HTTP Transactions per Second to download file of 100KB

Comparison for maximum Bandwidth using Avalanche 2500 and Reflector 2500 from Spirent Communications

SPIRENT TEST CODE	Fedora R3 without Tuning	Fedora R3 with Tuning
FW_BANDWIDTH_T01	95.4 Mbps	95.4 Mbps

Comparison for maximum Concurrent TCP Connection using Avalanche 2500 and Reflector 2500 from Spirent Communications

SPIRENT TEST CODE	Fedora R3 without Tuning	Fedora R3 with Tuning
FW_TCP_OPEN_T01	30712	500000
FW_TCP_OPEN_T02	30712	500000
FW_TCP_OPEN_T03	30712	500000
FW_TCP_OPEN_T04	30712	500000
FW_TCP_OPEN_T05	29350	500000
FW_TCP_OPEN_T06	28995	500000

Comparison for maximum TCP Connection per Second using Avalanche 2500 and Reflector 2500 from Spirent Communications

SPIRENT TEST CODE	Fedora R3 without Tuning	Fedora R3 with Tuning
FW_TCP_SEC_T01	290	3200
FW_TCP_SEC_T02	290	3100
FW_TCP_SEC_T03	290	2000
FW_TCP_SEC_T04	290	1100
FW_TCP_SEC_T05	200	210
FW_TCP_SEC_T06	110	110

Comparison for maximum HTTP Transaction per Second using Avalanche 2500 and Reflector 2500 from Spirent Communications

SPIRENT TEST CODE	Fedora R3 without Tuning	Fedora R3 with Tuning
FW_HTTP_SEC_T01	2900	15000
FW_HTTP_SEC_T02	2900	10000
FW_HTTP_SEC_T03	2100	2200
FW_ HTTP_SEC_T04	1100	1100
FW_ HTTP_SEC_T05	200	200
FW_ HTTP_SEC_T06	110	110

Other Test possibility with Spirent Communication Solution:

Device under Test Possibility	Spirent Configuration	
Firewall	Avalanche/Reflector	Yes
Load Balancer	Avalanche/Reflector	Yes
Proxy	Avalanche/Reflector	Yes
Reverse-Proxy	Avalanche/Reflector	
Cache	Avalanche/Reflector	Yes
Anti-Virus	Avalanche/Reflector	Yes
Content Filter	Avalanche/Reflector	Yes
URL Filter	Avalanche/Reflector	Yes
Packet Shaper	Avalanche/Reflector	Yes
SSL Accelerator	Avalanche/Reflector	Yes
HTTP Accelerator	Avalanche/Reflector	Yes
HTTPS Accelerator	Avalanche/Reflector	Yes
SMTP Relay	Avalanche/Reflector	Yes
IDS/IPS	Avalanche/Reflector	Yes
IPSec VPN Gateway	Avalanche/Reflector	Yes
SSL VPN Gateway	Avalanche/Reflector	Yes

Server under Test Possibility	Spirent Configuration	
HTTP/HTPS Server	Avalanche	Yes
2-Tier Infrastructure	Avalanche	Yes
3-Tier Infrastructure	Avalanche	Yes
SMTP Server	Avalanche	Yes
POP3 Server	Avalanche	Yes
FTP Server	Avalanche	Yes
Telnet Server	Avalanche	Yes
Streaming QuickTime Server	Avalanche	Yes
Streaming Real Network Server	Avalanche	Yes
Streaming Microsoft Server	Avalanche	Yes
Streaming Multicast	Avalanche	Yes

Contact Information:

Gregory Fresnais EMEA Business Development
Spirent Communications
gregory.fresnais@spirencom.com
Mobile: +33630916508
http://www.spirentcom.com/analysis/product_line.cfm?PL=32&wt=2