Securing the Open-Access Network – Best Practices

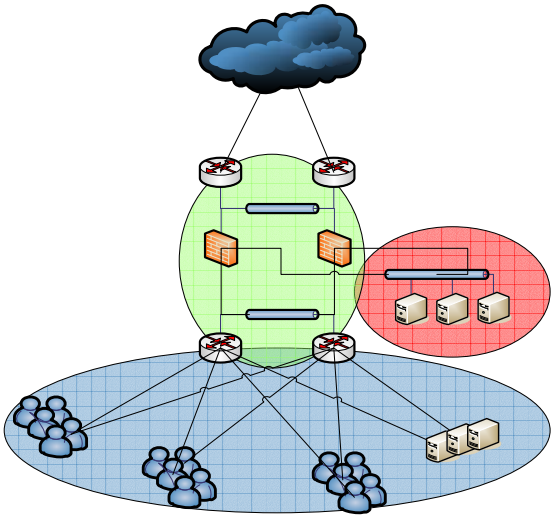
Mark Williams
Liaison, Academic Networking - Asia Pacific
miw@juniper.net

- **What is STOAN All About?**
- **STOAN Architecture**
- **Best Practices 1: Traffic Baseline**
- **Best Practices 2: DoS Mitigation**
- **Case Study**

What's STOAN About?

- **STOAN is about perimeter security for Networks where policy at the perimeter is "default allow"**
  - There may be tighter policies enforced inside the perimeter for sub-parts of the network.
- **STOAN is about "Clean Pipes"**
  - Drop "undeniably unwanted" traffic
  - Police "control plane" traffic (DoS Mitigation)
- **"Border of Liability"**
  - Stop known attacks from getting out.
  - Log activity in accordance with policy/laws.
- **STOAN is about availability.**
  - Build a network perimeter that can't be "taken out".
  - Build a network perimeter that is robust in the face of equipment failure.
- **STOAN is about visibility and manageability**
  - Know what is happening across the network perimeter.
  - Give NOC personnel robust and convenient tools for monitoring and controlling the network perimeter.

STOAN Reference Architecture



Best Practice 1:
Traffic Baseline

What the Baseline Should Tell you

- **What is my overall network utilisation?**
- **What is the makeup of my network utilisation?**
  - Protocols?
  - Time of day?
  - Which Subnets?
  - Where is the traffic coming from and where is it going?
- **How much of this traffic is business critical?**
- **What is the threat level of my network?**

Knowing what's Normal in your Network

Knowing normal behavior for your network is crucial to understanding how to detect and block abnormal behavior such as floods. Data should be recorded at both the router and the firewall using tools such as:

ACL Counters
X-Flow Data
MRTG / SNMP

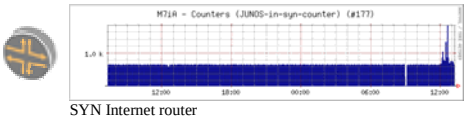
Firewall Logs / Counters
Session Table Size / Rate
FW Reports

What you should know:

% ICMP Normal	Sessions / Sec Peak
% UDP Normal	Total Sessions Peak
% TCP Control Normal	Session Distribution by Proto
Protocol Distribution	Session Usage per IP
Interface Bandwidth	Firewalls “Ramp-Rate” *

* A Firewalls Ramp-Rate is the measurement of how quickly it can setup new sessions, this will differ depending on the Model of the Firewall and its specific configuration. This number is usually provided on the Marketing Datasheet

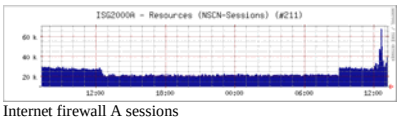
Knowing what’s Normal in your Network



SYN Internet router

Monitor bandwidth utilization
• Use SNMP tools like MRTG
• Collect both BPS and PPS
Implement counting ACLs
• TCP flags: SYN, FIN, RST
• DNS queries
• ICMP errors
• IP options
• IP fragments
Optional J-Flow data

Monitor bandwidth utilization
• Use SNMP tools like MRTG
• Collect both BPS and PPS
Monitor session table and rate
• “get perf ses det” “get ses info”
Enable SCREEN protections
• “get count screen zone X”
• “get zone X screen session”
Optional firewall traffic logs



Internet firewall A sessions

Baseline Assumptions

Although Every Network is different, some general assumptions can be made for detecting abnormal behavior with routers alone, such as:

- •TCP control packets such as SYNs and RSTs should not comprise more then 5% each of my bandwidth in normal circumstances
- •ICMP should not exceed 1% of my bandwidth in normal circumstances
- •Certain ICMP types (such as unreachable) should not exceed 1% of my bandwidth
- •IP Fragments should not exceed 1% of my bandwidth in normal circumstances
- •Packets with IP options should not exceed 1% of my bandwidth

Best Practice 2: Denial of Service Mitigation

Goal: Optimize each device for its purpose

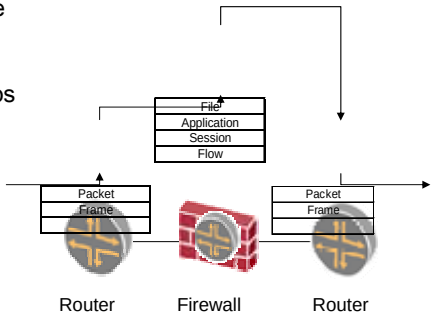
Device	Layer	Optimized For	DoS Protections
	4-7	Flow Inspection Deep Inspection	SCREENs, Session Limits Syn-Cookie
	2-4	Packet Inspection Frame Inspection	Line-Rate ACLs Rate-Limits

Routers are Optimized to process packets at Layer 2-4 at very high speeds; however they have no visibility into "flows" or "sessions" As a result, all packets can be processed at equally high speed.

Firewalls are Optimized to process packets at Layer 4-7 using technologies such as State full Inspection to examine flows and relate them to Sessions. As a result, new sessions through the Firewall require extra processing, some of which is done in Software. As a result different types of packets are processed at different speeds some requiring more Firewall CPU, such as during a Session Setup and Teardown.

Optimizing the Router

- **Discard Illegal Packets / Options** – Before they reach the Firewall
- **Apply Illegal Sources/Destinations –** Drops traffic not destined to/from your network before reaching the Firewall
- **Implement selective Rate-Limits –** Ensures Available Bandwidth *Protects the Network under heavy Flood*
- **Verify Unicast Reverse-Path** – Helps block SMURF Attacks with Spoofed IP Addresses before reaching the Firewall or enter/leave the local segment.



Border Router Requirements

- Line-Rate ACLs
- Agile ACLs
- Line-Rate Policers
- Layer 4 Visibility
- Dedicated Routing Engine

How the Router can help – Rate Limits

Rate Limits used to protect ISG2000 Firewall

Limit ICMP to 0.2% BW – Helps reduce the burden of large ICMP Floods on the Firewall
Limit TCP SYNs 5% BW – Helps reduce the burden of SYN Floods on the Firewall
Limit TCP RST/FIN 5% BW – Helps reduce the burden of RST/FIN Floods on the Firewall
Limit IP Fragments to 1% BW – Helps reduce the burden of IP Fragments on the Firewall
Limit Other IP Protocols to 1% BW – Eliminated other Protocols from consuming all bandwidth

JunOS Policers Configlet (Assumes 1GB Uplink)

```
set firewall policer one-percent if-exceeding bandwidth-limit 10m
set firewall policer one-percent if-exceeding burst-size-limit 100k
set firewall policer one-percent then forwarding-class network-control
set firewall policer point-2-percent if-exceeding bandwidth-limit 2m
set firewall policer point-2-percent if-exceeding burst-size-limit 50k
set firewall policer point-2-percent then discard
set firewall policer five-percent if-exceeding bandwidth-limit 50m
set firewall policer five-percent if-exceeding burst-size-limit 150k
set firewall policer five-percent then discard
```

Optimizing the Firewall SCREENs

•Configure based on Traffic Baseline

Firewall FLOW Settings:
•Enable TCP-SYN Checking
- •Prevents Session creation for illegal Packets

•Enable TCP-Sequence # Checking
- •Drops Illegal/Duplicate Packets

•Enable TCP-RST-Sequence checking
- Drops Illegal/Dupicate RST Packets

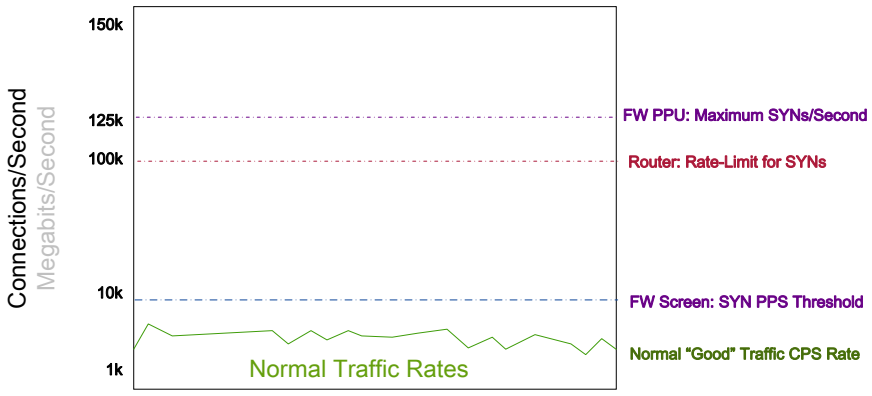
• Enable Syn-Proxy Syn-Cookie
- Prevents Session Creation on SYN Performed in PPU on NetScreen ISG and 5000 Systems

ISG-2000 5.4r1
SCREEN Thresholds used in STOAN Solution

SYNFlood – Threshold 10000 PPS
Src & Dst Threshold 250 PPS
UDP Flood – Threshold 10,000 PPS
ICMP Flood – Threshold 1,000 PPS
Session Limits – Per Source: 1,000 Per Dest: 10,000
Enable All specific DoS Defenses
Enable IP & TCP Protocol Anomalies SCREENs

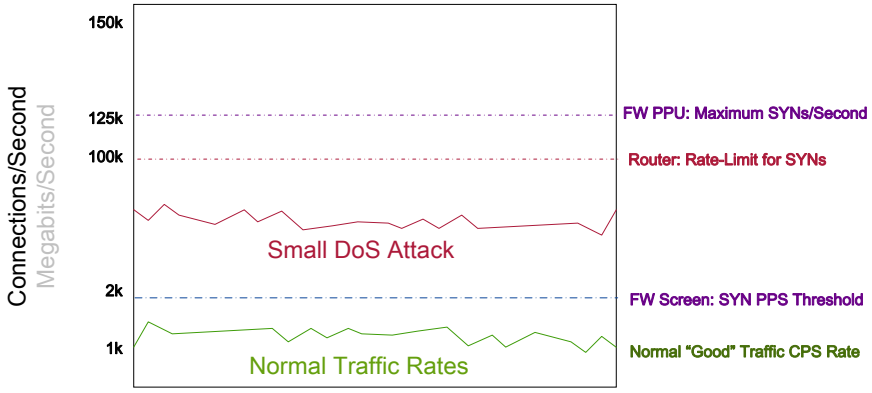
Scenario: SYN – Baseline

When configuring the SYN SCREEN Settings, set the SYN PPS Threshold to at least 5-10x your normal "Baseline" CPS rate to avoid false positives.



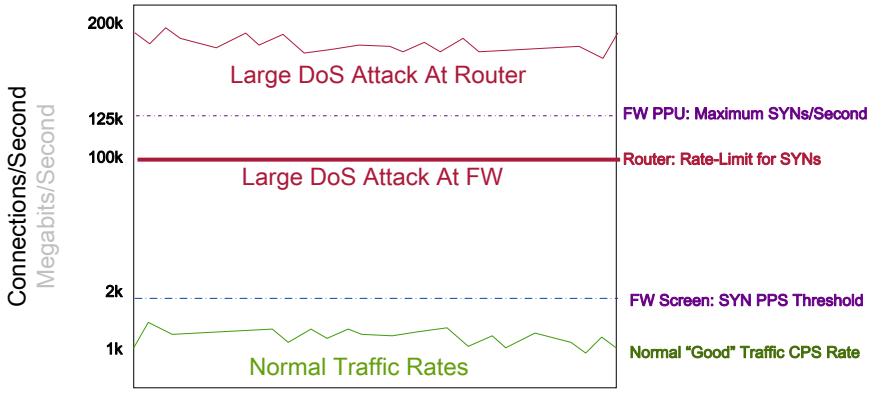
Scenario: SYN Flood – Small Flood

When under light SYN Flood, the Firewall SYN Protection and SYN-Cookie can handle and prevent the attack, without any assistance from the Router.



Scenario: SYN Flood – Large Flood

When under heavy SYN Flood, the Router's SYN Rate-Limits kick in, limiting SYN Packets to a rate that the Firewall's PPU can handle, protecting the Firewall from being overwhelmed by too many SYN packets.



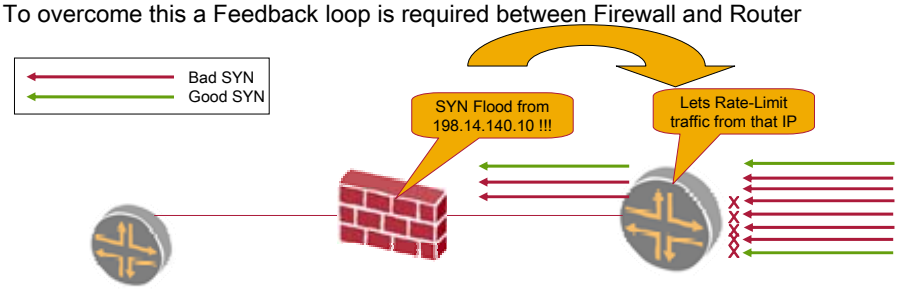
Examining Rate-Limiting and its Impact

If the Router is Rate-Limiting SYN or RST Packets under heavy attack, all SYNs or RSTs will be rate-limited equally, including Legitimate Connections

The Result is some legitimate connections may be dropped (experiencing retries/timeouts) while under Attack; However most of the dropped connections will be the Flood itself.

- e.g. If 99% of SYNs dropped are Floods, only 1% are legitimate

To overcome this a Feedback loop is required between Firewall and Router

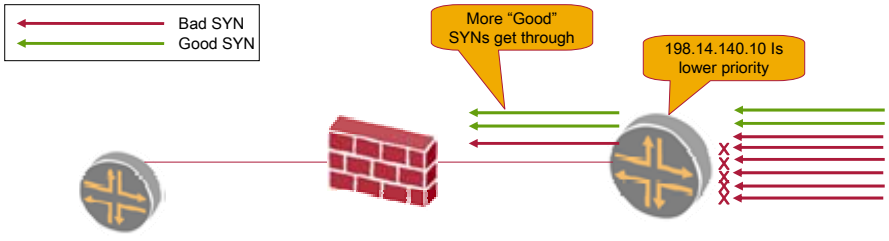


Examining Rate-Limiting and its Impact

With the Feedback Loop in Place, the Router will treat certain traffic from 198.14.140.10 as Lower Priority in the Rate-Limit buckets then other IPs

This will result in less “Good” SYNs being dropped by Rate-Limits and is a necessary step in sustaining a long-lived Flood attack

Feedback Loop can be manual (by Admins) or automated (via Script)

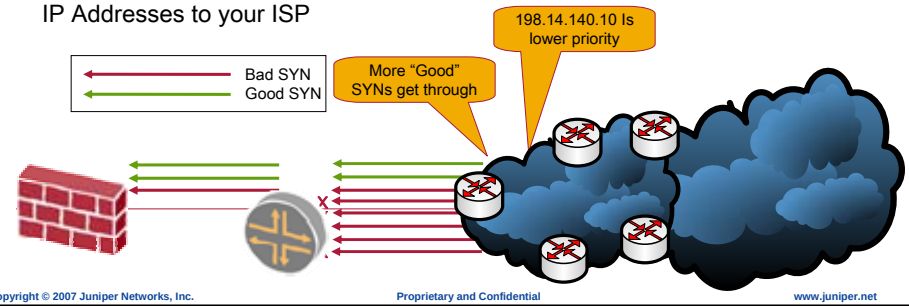


Dealing with things Upstream

If under sustained, heavy attack it may be necessary to take action upstream, closer to the source of the Attack, to free up bandwidth for Good Traffic

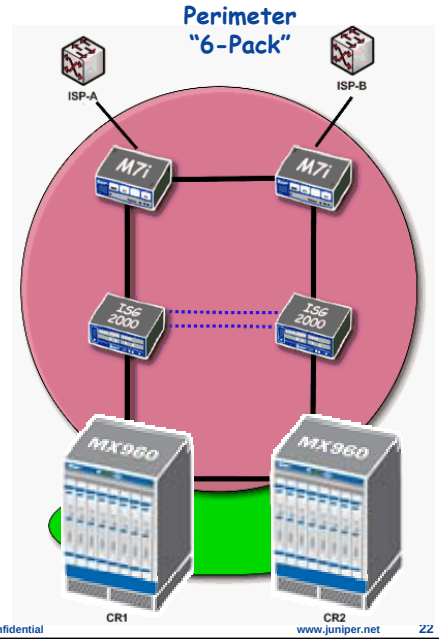
A Feedback Loop between the Enterprise's Internet Router(s) and Service Provider Router(s) is necessary in this case, Routers Upstream in the ISP Core can block or Rate-Limit Blacklisted IP Addresses

Juniper Routers implement BGP Flowspec that can be used to dynamically change Rate-Limits or Blacklist IPs, Alternatively you may report Blacklisted IP Addresses to your ISP



Summary

- **Screen Settings should be optimized for each network based on Traffic Profile to be effective**
- **Firewalls should be protected by Stateless Screening Router's to sustain heavy TCP Floods (100,000+ cps for ISG)**
- **Installing a new Firewall without implementing Router ACLs may cause problems *when* heavy floods occur**

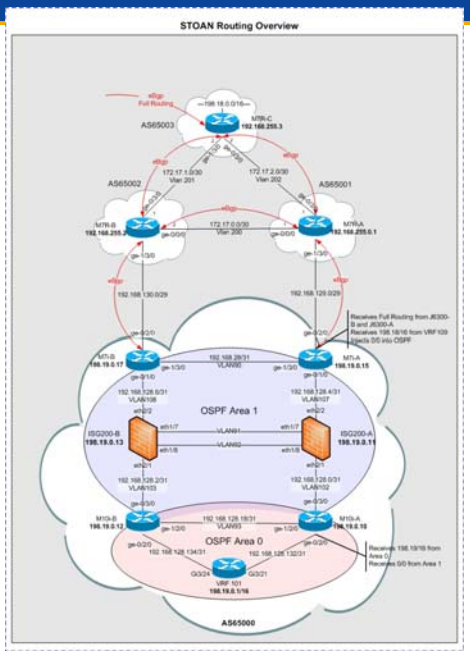


Case Study

Juniper NETWORKS

Perimeter Six Pack

- M7i Internet connecting border routers, redundant
- ISG-2000-IDP border firewalls, redundant
- M10i Core connecting routers, redundant
- 1Gbps



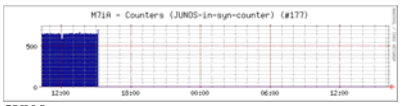
JUNOS Counting Filter Config

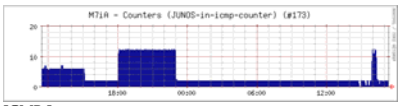
1. set firewall filter in term 1frag from first-fragment
2. set firewall filter in term 1frag then count 1frag
3. set firewall filter in term 1frag then next term
4. set firewall filter in term 2frag from is-fragment
5. set firewall filter in term 2frag then count 2frag
6. set firewall filter in term 2frag then next term
7. set firewall filter in term option from ip-options any
8. set firewall filter in term option then count option
9. set firewall filter in term option then next term
10. set firewall filter in term ping from protocol icmp
11. set firewall filter in term ping from icmp-type echo-request
12. set firewall filter in term ping from icmp-type echo-reply
13. set firewall filter in term ping then count ping
14. set firewall filter in term ping then next term
15. set firewall filter in term icmp from protocol icmp
16. set firewall filter in term icmp then count icmp
17. set firewall filter in term syn from protocol tcp
18. set firewall filter in term syn from tcp-flags syn
19. set firewall filter in term syn then count syn
20. set firewall filter in term synack from protocol tcp
21. set firewall filter in term synack from tcp-flags "(syn & ack)"
22. set firewall filter in term synack then count synack
23. set firewall filter in term fin from protocol tcp
24. set firewall filter in term fin from tcp-flags fin
25. set firewall filter in term fin then count fin
26. set firewall filter in term rst from protocol tcp
27. set firewall filter in term rst from tcp-flags rst
28. set firewall filter in term rst then count rst
29. set firewall filter in term dns from protocol udp
30. set firewall filter in term dns from destination-port 53
31. set firewall filter in term dns then count dns
32. set firewall filter in term other from protocol-except tcp
33. set firewall filter in term other from protocol-except udp
34. set firewall filter in term other from protocol-except ah
35. set firewall filter in term other from protocol-except esp
36. set firewall filter in term other from protocol-except gre
37. set firewall filter in term other then count other
38. set firewall filter in term default-permit then accept

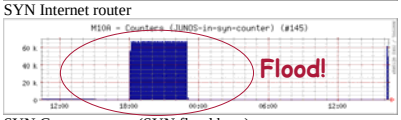
SCREENOS Config

1. set zone "Internet" screen icmp-flood
2. set zone Internet screen icmp-flood threshold 1000
3. set zone "Internet" screen udp-flood
4. set zone "Internet" screen udp-flood threshold 10000
5. set zone "Internet" screen syn-flood
6. set zone "Internet" screen syn-flood alarm-threshold 10000
7. set zone "Internet" screen syn-flood queue-size 20000
8. set zone "Internet" screen syn-flood attack-threshold 10000
9. set zone "Internet" screen syn-flood source-threshold 500
10. set zone "Internet" screen syn-flood destination-threshold 500
11. set zone "Internet" screen limit-session source-ip-based 10000
12. set zone "Internet" screen limit-session destination-ip-based 10000
13. set zone "Internet" screen port-scan
14. set zone "Internet" screen port-scan threshold 100000
15. set zone "Internet" screen ip-sweep
16. set zone "Internet" screen ip-sweep threshold 100000

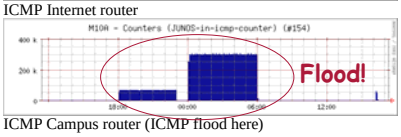
Using NetMRG or MRTG


SYN Internet router

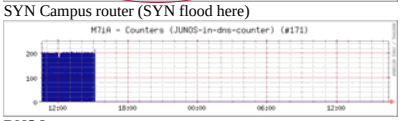

ICMP Internet router

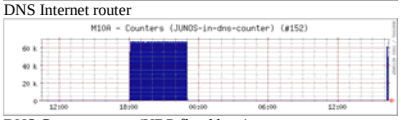


SYN Campus router (SYN flood here)



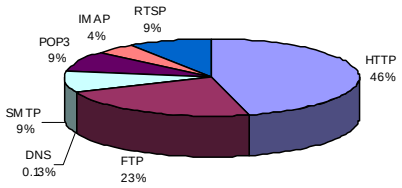
ICMP Campus router (ICMP flood here)


DNS Internet router

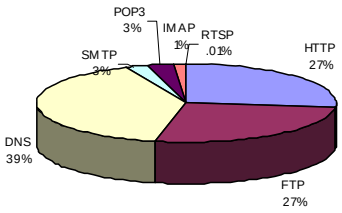

DNS Campus router (UDP flood here)

Deep-Dive: Background Traffic

Byte Distribution



Connection Distribution



JMIX

DNS, HTTP, FTP, SMTP, IMAP, POP3, RTSP

- **Background Traffic (using IxLoad)**
  - 1700 Sessions/Second Bidirectional
  - 420Mb/Second Bidirectional
  - Mix of 7 Common Protocols
  - Validate 99.9% of Attempted Connections Established

Deep-Dive: Background Traffic

Campus->Internet Traffic

Protocol	# Clients	# Servers	Fan-Out	CPS Rate	Avg Duration	Filesize	Avg bps	Avg Throughput
HTTP	4000	20000	5	200	18 Seconds	64k	101000064	**96.32 Mb/Sec**
FTP	4000	20000	5	200	7 Seconds	128 byte	50372142.5	**48.04 Mb/Sec**
DNS	4000	20000	5	300	7 Seconds	64k	282440.5	**0.27 Mb/Sec**
SMTP	4000	4000	1	20	14 Seconds	130k	19695189	**18.78 Mb/Sec**
POP3	4000	4000	1	20	14 Seconds	130k	19615362.2	**18.71 Mb/Sec**
IMAP	4000	4000	1	10	14 seconds	130k	9797663.3	**9.34 Mb/Sec**
RTSP	4000	4000	1	0.5	600 Seconds	64k / bps	20162204	**19.23 Mb/Sec**
Subtotal				**750.5**				**210.69 Mb/Sec**

Internet->Campus Traffic

Protocol	# Clients	# Servers	Fan-Out	CPS Rate	Avg Duration	Filesize	Avg bps	Avg Throughput
HTTP	4000	800	0.2	200	18 Seconds	64k	101000064	**96.32 Mb/Sec**
FTP	4000	800	0.2	200	7 Seconds	65k	50372142.5	**48.04 Mb/Sec**
DNS	4000	800	0.2	300	7 Seconds	128 byte	282440.5	**0.27 Mb/Sec**
SMTP	4000	800	0.2	20	14 Seconds	130k	19695189	**18.78 Mb/Sec**
POP3	4000	800	0.2	20	14 Seconds	130k	19615362.2	**18.71 Mb/Sec**
IMAP	4000	800	0.2	10	14 seconds	130k	9797663.3	**9.34 Mb/Sec**
RTSP	4000	800	0.2	0.5	600 Seconds	64k / bps	20162204	**19.23 Mb/Sec**
Subtotal				**750.5**				**210.69 Mb/Sec**
Total (Bi-Directional)				**1501**				**421.38 Mb/Sec**

SNMP Polling & Reporting

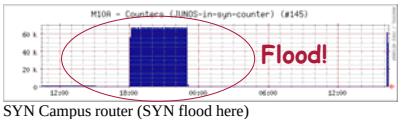
- **ScreenOS OIDs:**

Var	SNMP Name	SNMP OID	Instance	Command
S	nsResSessAllocate	1.3.6.1.4.1.3224.16.3.2	0	Get session info
SR	Session rate	None	None	Get performance session
U	User count	None	None	Get zone <name> screen session
B	ifOutOctets	1.3.6.1.2.1.2.2.1.16	All	Get counter statistic interface <name>
P	ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	All	Get counter statistic interface <name>
CPU	nsResCpuLast1Min	1.3.6.1.4.1.3224.16.1.2	0	Get performance cpu

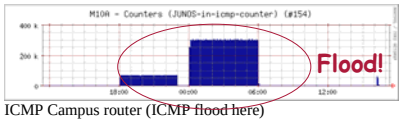
- **JunOS OIDs:**

	SNMP Name	SNMP OID	Instance	CLI Command
IP.TCP-SYN	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.TCP-SYN+ACK	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.TCP-FIN	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.TCP-RST	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.UDP-DNS	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.ICMP-PING	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.ICMP-Error	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.Fragments	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
IP.Proto-Other	jnxFWCounterPacketCount	1.3.6.1.4.1.2636.3.5.2.1.4	Index	Show firewall
Throughput, bps	ifOutOctets	1.3.6.1.2.1.2.2.1.16	All	Monitor interface traffic
Packets, pps	ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	All	Monitor interface traffic

Using NetMRG or MRTG



SYN Campus router (SYN flood here)



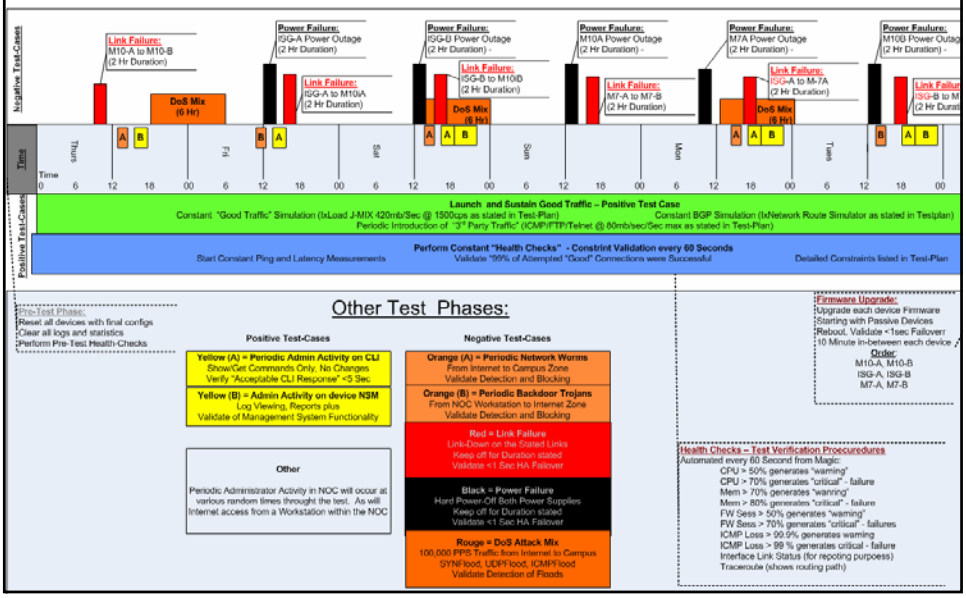
ICMP Campus router (ICMP flood here)

Calculations

- **Average**
- **Summary**
- **Confidence**

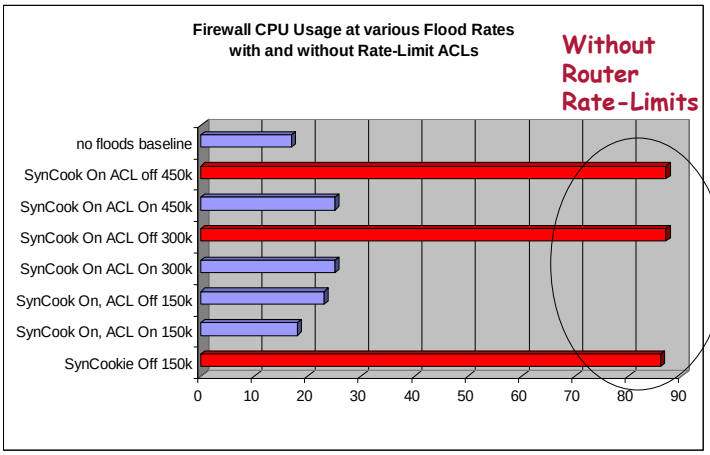
Measurement	Internet	Campus	Total	Calc	Formula
Device	*isg200a*	*isg2000a*	*Firewalls*		
Port	*e2/2*	*e2/1*			
Sessions	30,000	30,000	30,000		max(a, b)
Session Rate, cps	1,500	1,500	1,500		max(a, b)
Users	4,403	4,505	8,908		sum(a, b)
In Bandwidth, bps	na	na	na		
Out Bandwidth, bps	250,000,000	250,000,000	500,000,000		sum(a, b)
In Packets, pps	55000	55000	110,000		sum(a, b)
Out Packets, pps	55000	55000	110,000		sum(a, b)
CPU, %	30	5	30		max(a, b)
Session Duration, sec				20	sessions/session rate
Bandwidth per Session, bps				16,667	bandwidth/sessions
Data per Session, bytes				41,667	session bandwidth*duration
Sessions per User				3	sessions/users
Session Rate per User, cps				0.2	session rate/users
Bandwidth per User, bps				56,129	bandwidth/users
Router	*m7ia*	*m10ia*	*Routers*		
Port	*ge-0/2/0*	*ge-0/2/0*			
In Bandwidth, bps	250000000	250000000	500,000,000		sum(a, b)
Out Bandwidth, bps	250000000	250000000	500,000,000		sum(a, b)
In Packets, pps	55000	55000	110,000		sum(a, b)
Out Packets, pps	55000	55000	110,000		sum(a, b)
SYN, pps	650	650	1,300		sum(a, b)
SYN-ACK, pps	650	650	1,300		sum(a, b)
FIN, pps	1300	1300	2,600		sum(a, b)
DNS, pps	200	4	204		sum(a, b)
RST, pps	0	1	1		sum(a, b)
ICMP, pps	7	7	14		sum(a, b)
PING, pps	7	7	14		sum(a, b)
Frag, pps	0	0	0		sum(a, b)
Other, pps	0	0	0		sum(a, b)
Average Packet Size, b				568	bandwidth/packet rate
Session Rate, pps				1,518	sum(SYN+DNS+PING)
% SYN pps				1.18%	SYN/packet rate
% DNS pps				0.19%	DNS/packet rate
% PING pps				0.01%	PING/packet rate
% SYN bps				0.13%	SYN*64B/bandwidth
% DNS bps				0.03%	DNS*100B/bandwidth
% PING bps				0.00%	PING*64B/bandwidth

Combined 7 Day Test Cycle



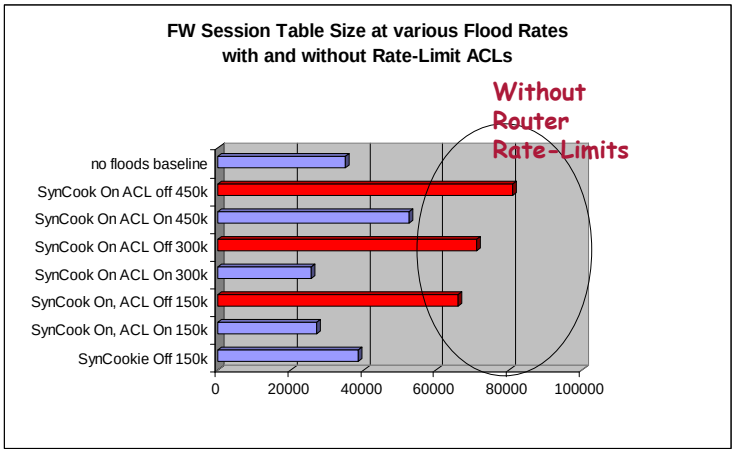
STOAN Solution DoS Test Results

Background Traffic of 420mb/Sec @ 1500 Sessions/Sec
SYN Flood (10 Source IPs, 1 Destination Target) at various Rates
CPU Recorded after 60 seconds of Flood Activity



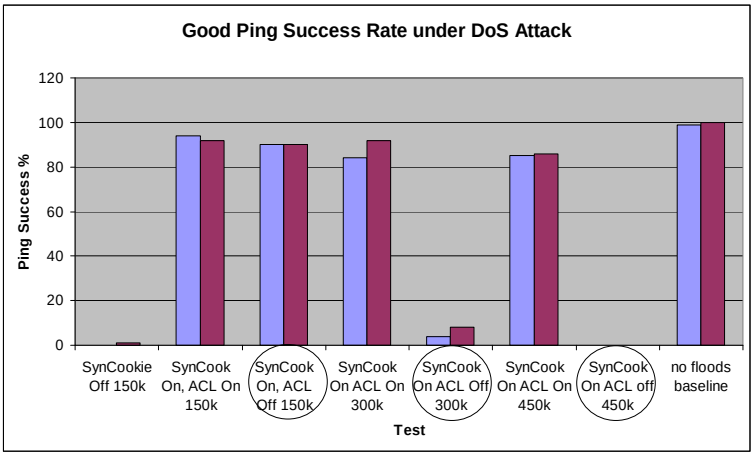
STOAN Solution DoS Test Results

Background Traffic of 420mb/Sec @ 1700 Sessions/Sec
SYN Flood (10 Source IPs, 1 Destination Target) at various Rates
Session Table Recorded after 5 Minutes of Flood Activity



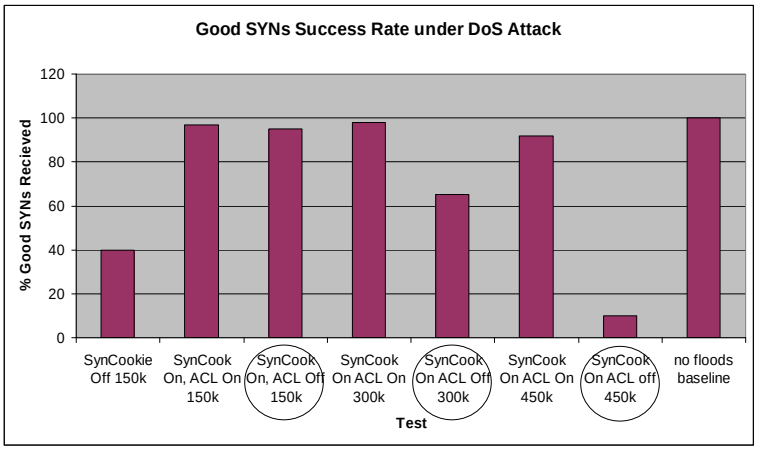
STOAN Solution DoS Test Results

Background Traffic of 420mb/Sec @ 1700 Sessions/Sec
SYN Flood (10 Source IPs, 1 Destination Target) at various Rates
Measurements taken with Ping every second – Average of 5 Minutes taken



STOAN Solution DoS Test Results

Background Traffic of 420mb/Sec @ 1700 Sessions/Sec
SYN Flood (10 Source IPs, 1 Destination Target) at various Rates
Measurements taken with hping2 – Average of 100 Attempted SYNs taken




Juniper your Net™
miw@juniper.net
Copyright © 2007 Juniper Networks, Inc.
Proprietary and Confidential
www.juniper.net
39