

Implementation Guide

Protecting the Network from Denial of Service Floods



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

Introduction	4
Scope	4
Design Considerations	4
Perimeter Locations and Roles	4
Denial of Service Attacks	4
Types of DoS Attacks.	5
SYN Floods	5
ICMP Floods	5
UDP Floods	5
Illegal TCP Flag Flood.	5
Distributed DoS Floods	5
Spoofed Address Floods	6
Adaptive Threat Management and DoS Attacks.	6
Implementation Guidelines	7
Mitigating Large Scale DoS Attacks on the Network.	7
Optimizing the Firewall	8
Implementing Stateful Inspection	8
Implementing Stateful SYN Proxy Mechanisms	9
Limiting the Number of SYNs per Second per Source IP	9
Limiting the Number of SYNs per Second per Destination IP.	10
Limiting the Number of Sessions per Source/Destination IP.	10
Preventing ICMP Floods.	10
Preventing UDP Floods	10
Optimizing the Router	11
Configuring J-Flow for Detecting Traffic	11
Enable the Flow Collector at the Interface:	12
Export the Information to STRM:	12
Rate-limiting TCP Control Traffic	12
Rate-Limiting ICMP	12
Rate-Limiting UDP	13
Rate-Limiting Other IP Protocols	13
Implementing Reverse Path Validation.	13
Drop Non-Local Subnets with Filters	13
Responding to Large Floods	13
Responding Upstream	13
Automating a Response	14
Configuring STRM.	14
Using STRM to Poll Statistics Automatically	14
Using STRM to Determine Attack Status	15

Summary	16
Appendix A Baseline Network Traffic using Router and Firewall Counters	17
Configuring the Router	17
Configuring the Firewall	18
Configuring NSM to Export Logs to STRM	19
Appendix B JUNOS Software Router Configuration for Counting Traffic	20
Appendix C Baseline SCREEN Settings	21
Appendix D Optimized Firewall Configuration	22
Appendix E Optimized Router Configuration	24
Appendix F Test Results	26
About Juniper Networks	28

List of Figures

Figure 1. Reference Test Network	7
Figure 2. Device, Layer, Optimization and Types of DoS Protections	7
Figure 3. Stateless Screening Routers Surrounding Stateful Firewalls	8
Figure 4. Handling SYN-Cookie on Juniper Networks Firewalls	11
Figure 5. Communicating to Upstream ISP Devices to Address Floods	14
Figure 6. STRM Dashboard Showing Attacks	15
Figure 7. STRM Offense Manager Showing DoS Attack Details	15
Figure 8. Drilling Down on the Attacker	16
Figure 9. Action Parameters Window of NSM	19
Figure 10. Selecting Device Log Action Criteria on NSM	19

Introduction

Denial of Service (DoS) and Distributed DoS (DDoS) floods are commonplace across today's Internet. This paper describes several types of DoS floods that are plaguing today's enterprise networks and describes in detail how to detect and counter them. Enhanced tools are now available to analyze and respond to these attacks, reducing complexity and streamlining operational responses. This document describes the steps necessary to optimize the network to survive the heaviest of floods and how to effectively respond when they occur.

Scope

This document helps the reader to implement Juniper Networks security products on their network to protect from external DoS and DDoS attacks on the network perimeter. For the purposes of this document, we will focus on two strategies: a single Juniper Networks Secure Services Gateway (SSG) class device running ScreenOS, and a hybrid higher throughput termination that combines a JUNOS™-software based router with an SSG/ISG (Integrated Security Gateway) class firewall running ScreenOS.

Design Considerations

This section describes the various types of DoS attacks and the critical design considerations to address them.

Perimeter Locations and Roles

The first question that should be asked in a security posture evaluation is: what am I defending? In this case, we are protecting the network perimeter from external attacks. The perimeter of an autonomous system (for example, your enterprise routed network) is not homogeneous in its composition; different devices will be used to terminate WAN traffic based on role. The most common deployment scenario for an Internet connected enterprise network is to use a private network of some kind to connect traffic securely between the branches, campus and data centers while allowing split tunneling for Internet bound traffic. While this simplifies the routing of traffic to the Internet, it increases risk by exposing all termination points to potential DoS attacks. Detecting and mitigating these attacks will require a combination of edge device configuration with centralized analysis and control elements.

Branch offices are generally smaller and don't have onsite staff to maintain network devices. In this role, an "all in one" termination device is usually used in smaller and possibly mid-sized deployments. The device that would be deployed in this location would be an SSG class device running ScreenOS. The detection and mitigation of DoS attacks will depend on screening, logging and firewall configuration.

The campus location requires the ability to handle higher traffic loads and more advanced and complex routing configurations. Here, a standalone M-series multiservice edge router or J-series router handles the connectivity, while higher end SSG Series or ISG Series firewalls perform the security function. This requires that both the JUNOS software and ScreenOS element of the system be configured to detect and mitigate attacks at each layer.

Denial of Service Attacks

The goal of a DoS attack is to deny access to a particular network resource. This is often accomplished through a flood of illegitimate connections targeted to a resource in an attempt to overwhelm that resource. Unfortunately, DoS floods sent at a high enough volume can also exhaust available network bandwidth and place additional burdens on stateful devices such as firewalls found along the path between the attacker and target system.

Types of DoS Attacks

While the goal of any DoS attack is to generate large amounts of illegitimate traffic, each type of DoS attack works by exploiting specific weakness in an IP protocol. This requires unique detection and protection mechanisms for each type of attack. Next, we will examine some common DoS attacks and identify steps one can take to detect and prevent these flows. For a more detailed description of specific types of DoS floods, refer to *Concepts & Examples ScreenOS Reference Guide Volume 4: Attack Detection and Defense Mechanisms Release 6.0.0, Rev. 03* (http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/CE_v4.pdf)

SYN Floods

A SYN flood works by establishing half-open connections to a node. When the target receives a SYN packet to an open port, the target will respond with a SYN-ACK and try to establish a connection. However, during a SYN flood, the three-way handshake never completes because the client never responds to the server's SYN-ACK. As a result, these "connections" remain in the half-open state until they time out.

Imagine this process occurring several thousand times per second. Soon, the target server will run out of memory/resources, or cause a system crash. Additionally, any stateful devices in the path between the attacker and target will also be overwhelmed with connection requests, possibly filling up the session table on those devices if the SYN flood is not dealt with effectively.

Because SYN packets are normal and necessary for TCP communication, a system cannot simply drop all SYN packets as in the case of a "Ping of Death" DoS attack, for example. SYN floods can be mitigated effectively up to a certain point using a SYN proxy feature in a stateful firewall. Above this rate, a stateless screening router can be used to further limit TCP-SYNs.

ICMP Floods

While several types of Internet Control Message Protocol (ICMP) floods exist, each exploits the openness of the ICMP protocol itself, and the fact that most systems with IP stacks will respond to most ICMP messages. Large ICMP floods can affect available network bandwidth and impose extra load on the firewall, which must examine and inspect each ICMP packet. These risks can be mitigated by implementing a Juniper Networks firewall with ICMP flood protection, in combination with adjacent routers to rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance.

UDP Floods

A User Datagram Protocol (UDP) flood can cause significant impact on network bandwidth. Additionally, if a UDP flood is directed to an unopened port, the target server will respond to each packet with an ICMP unreachable message, creating an ICMP flood in the opposite direction. To mitigate the impact of UDP floods, a stateful firewall with both UDP and ICMP flood protection should be implemented. To survive a larger UDP flood, rate limits on UDP traffic may need to be implemented on adjacent routers to protect available bandwidth.

Illegal TCP Flag Flood

Certain combinations of TCP flags, such as a SYN packet with the FIN bit set, are illegal and shouldn't be seen on any network. While a firewall will clearly detect and drop these anomalies, it will only handle these illegal packets up to a certain rate. Above this rate, these packets should be rate-limited by adjacent routers to a rate that the stateful firewall can handle.

Distributed DoS Floods

Further compounding the flood problem is the proliferation of zombies, which are actually hosts that are infected with malware. A crafty attacker can infect thousands of machines and direct them all to attack a specific system at once. In this scenario, the attacks originate from several hundred to many thousands of source IPs, making detection and prevention more difficult. To mitigate DDoS floods, customers should implement per-destination IP session limits and SYN proxy destination thresholds

on a stateful firewall. While this will mitigate any traffic passing the firewall, the incoming link can still be saturated. If the network under attack is part of a network that is routed with BGP, mitigation can be achieved upstream of the link via BGP Slow Specification commands. This is best accomplished at the service provider level, as it requires a modification to the peering agreement and the provider being willing to accept flow specification information from routers they don't directly control.

Spoofed Address Floods

Some DoS attacks use spoofed or illegal IP addresses, which will never be properly routed back to the source. To mitigate these spoofed attacks, one should implement reverse path validation on ingress routers in combination with dropping non-local subnets at egress routers. This combination of ingress and egress filtering will drop these illegal packets before they reach the firewall.

Adaptive Threat Management and DoS Attacks

Adaptive Threat Management is the ability to detect and respond to security threats in a quick and flexible manner, allowing timely mitigation of the security issue. To function properly, Adaptive Threat Management depends on three primary elements:

- *A sensor/enforcement point.* Any device that is aware of network security status and can send logs is a sensor. In this case, we use SSG and ISG firewalls, JUNOS software routers and dedicated Juniper Networks Intrusion Detection and Prevention (IDP) systems. Our sensors are also enforcement points that can be configured to defend against the attacks.
- *A central point of configuration and control.* The log output from the SSG, ISG and IDP is more efficiently collected by the Juniper Network and Security Manager (NSM) system. Using NSM to collect the logs reduces the CPU required on the individual security elements and scales to large deployments. It also allows a centralized point of control to push out system updates that can respond to the attack.
- *An analysis system.* Security Threat Response Manager (STRM) has the ability to accept network performance and security metrics from all elements of the network, including the servers. This allows the security professional to have a "birds-eye view" of the entire security posture. The STRM system also automatically baselines the system and presents preformatted reports based on tested sampling analysis to highlight and alert on threat conditions.

The first step in evaluating your flood state is to establish a traffic baseline under normal network operating conditions. Normal operating conditions are defined as average traffic and application flow crossing the network edge devices averaged over time while the network is not under attack. The period used could be as short as a day, but a week is a good starting time interval for traffic analysis. The basic idea is to monitor your network traffic and determine protocol distribution, connection rates and average session durations under normal (non-flood) circumstances.

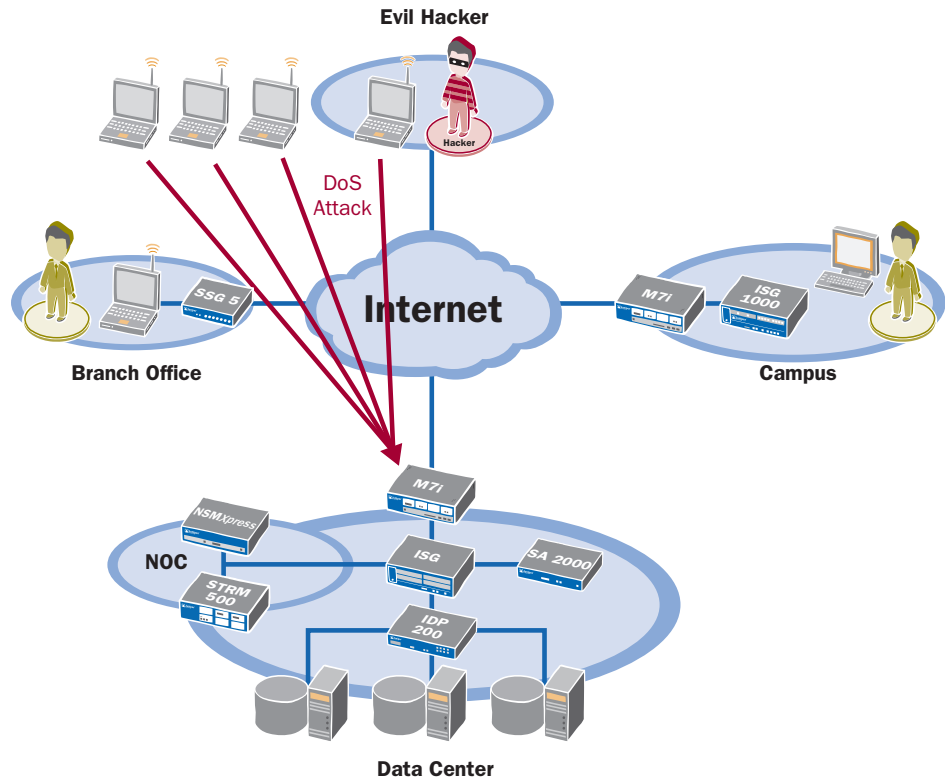
Given this baseline information, one can make some assumptions about abnormal traffic patterns that indicate a traffic flood. Even if there is no firewall in place, simple counters on a router can provide some insight into what's going on. However, a simpler approach is to use Juniper Networks Security Threat Response Manager (STRM). STRM allows aggregation of data and performs meta-analysis of trending to identify security threats. See the appendices for configuration of manual traffic baselining on the routers and firewalls.

The elements of the reference network are as follows:

- SSG 5 and ISG 2000 as firewall-based sensors and enforcers, IDP 100 as a detector, and Juniper M7i routers as detectors
- Centralized configuration settings are provided by NSM v2007.3r1.

Analysis provided by a STRM 500 v2008.1.0 Build 52 (6.1.1.28)

Figure 1 illustrates an example of DoS attacks on a data center network.



Example of DoS Attacks on Data Center Network

Implementation Guidelines

In this section, we discuss two important topics:

- How to mitigate large scale DoS attacks on the network
- How to respond to large scale flood attacks

Mitigating Large Scale DoS Attacks on the Network

The entire network must be optimized to control large floods. Stateless screening routers and stateful firewalls both play important roles in flood protection.





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

Figure 2. Device, Layer, Optimization and Types of DoS Protections

Juniper Networks firewalls perform stateful inspections and correlate flows into sessions giving much needed visibility into the source, destination and rates of attacks. SCREEN features allow advanced detection and blocking of many types of floods. Juniper Networks firewalls also implement session limits to control the total number of sessions that may be allocated to any single user. A SYN-cookie feature enables the firewall to do a stateless SYN proxy when under heavy SYN attack.

Routers perform Layer 2-4 stateless inspection at high speed. However, they lack visibility into flows or sessions and typically cannot provide detailed statistics about an attack.

By combining the DoS protection features available on both routers and firewalls, the network can be optimized to handle large floods at a much higher rate. Stateful firewalls should be protected on all interfaces by stateless screening routers that implement access lists, rate limits and counters specifically to deal with flood traffic. This best practice dates back to the early days when software firewalls or proxies were protected by adjacent routers.

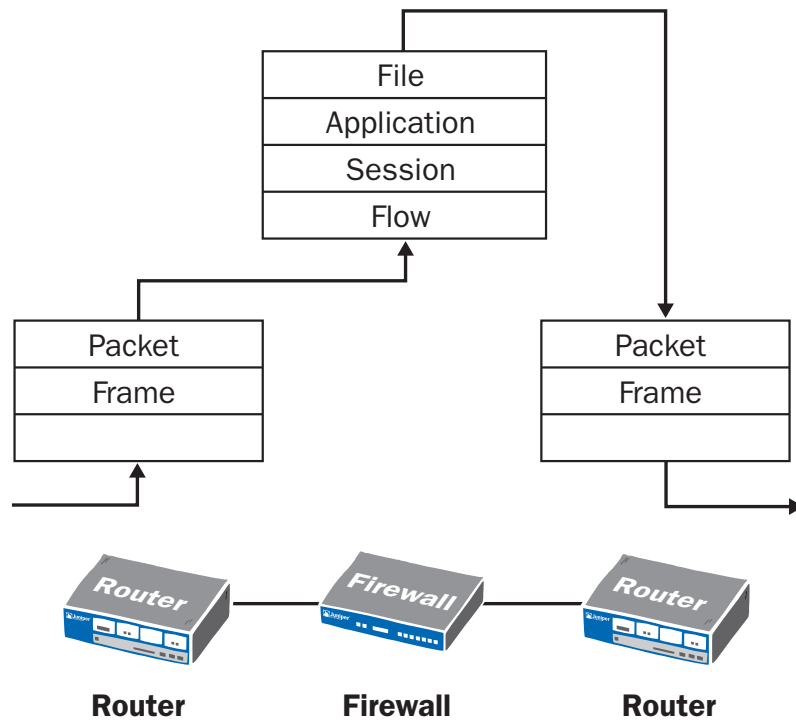


Figure 3. Stateless Screening Routers Surrounding Stateful Firewalls

Optimizing the Firewall

The firewall SCREEN settings must be optimized according to each specific network environment. These optimizations can be calculated from the traffic baseline data. SCREEN protections must be enabled on all appropriate zones. In the above illustration, the “Untrust” zone represents the Internet-facing side and the “Trust” zone represents the campus-facing side of the firewall.

In the next section, we will explore how to fine tune the SCREEN settings for your particular network’s profile and the individual impact of each setting. *Appendix E* of this document provides the full configuration of firewall SCREEN settings used in the solution.

Implementing Stateful Inspection

A stateful inspection firewall provides both visibility and protection against floods up to their rated capacity, in addition to security features outlined in *Juniper Networks Stateful Inspection Firewall* (Firewall/VPN Feature Brief) at http://www.juniper.net/products/integrated/stateful_inspection_firewall.pdf

Because a stateful firewall monitors the TCP control traffic and associates flows with sessions, it can easily identify illegal or abusive control traffic. The following settings enable TCP sequence number checking for all connections, including resets. It also prevents TCP sessions from being created if a SYN packet is not seen.

```
set flow check tcp-rst-sequence
unset flow no-tcp-seq-check
set flow tcp-syn-check
```

Implementing Stateful SYN Proxy Mechanisms

Most firewalls implement a SYN proxy type mechanism specifically for dealing with SYN floods. When a Juniper Networks ScreenOS firewall receives SYN packets at a rate higher than the defined threshold to a specific destination, the firewall will begin responding to each SYN with a SYN-ACK between the protected zones to thwart the attack. It is important to set this threshold at least **two** times higher than the baseline traffic rate of SYN per second because under ordinary circumstances, the firewall should *not* be used to proxy SYN requests.

When rates exceed an alarm threshold, alerts are generated via alarms pertaining to the flood. This rate is the amount that exceeds the attack threshold before the alarms occur. In the following example, alarms will *not* be generated until a 20,000 PPS of SYN are proxied through the firewall.

The queue size represents the total number of proxy connection requests held before the firewall begins rejecting new connections. The queue size should be set to the maximum possible value.

```
set flow syn-proxy syn-cookie
set zone Trust screen syn-flood attack-threshold 10000
set zone Trust screen syn-flood alarm-threshold 20000
set zone Untrust screen syn-flood attack-threshold 10000
set zone Unrust screen syn-flood alarm-threshold 20000
set zone Trust screen syn-flood timeout 5
set zone Untrust screen syn-flood timeout 5
set zone Trust screen syn-flood queue-size 20000 (use max value)
set zone Untrust screen syn-flood queue-size 20000
```

Beginning with ScreenOS 5.4r1, all NetScreen firewalls support the SYN-Cookie feature. This feature works in conjunction with the SYN proxy mechanisms. When enabled, sessions will *not* be set up unless a valid SYN/ACK is received from the client in response to the server's SYN. On the NetScreen ISG Series firewalls, this SYN-Cookie is done in the Packet Processing Unit (PPU) without affecting the CPU. The use of SYN-Cookie on any platform dramatically lowers CPU and session utilization. To enable SYN-Cookie, enter in the following command using the Command Line Interface (CLI).

```
set flow syn-proxy syn-cookie
```

Limiting the Number of SYNs per Second per Source IP

ScreenOS firewalls can also limit the number of SYNs per second from a particular source IP, if a client sends SYNs through the firewall above this rate. The firewall will simply ignore the additional SYN packets above this threshold and *not* perform the SYN-Proxy function. This limitation protects the CPU further when the majority of the flood originates from a small number of IP addresses.

Note: SCREEN settings and thresholds are specific to the ingress zone. For the “Untrust” zone, choose a higher value because Network Address Translation (NAT) can often make large organizations appear as a single IP when accessing the network.

```
set zone Trust screen syn-flood source-threshold 250
set zone Untrust screen syn-flood source-threshold 500
```

Limiting the Number of SYNs per Second per Destination IP

Limiting the number of SYNs per second targeting a specific destination prevents a distributed SYN flood from taking out a particular destination IP. Again, the firewall will simply ignore any additional SYN packets exceeding this threshold that target the same destination IP address and will *not* perform any SYN-Proxy.

Note: SCREEN settings and thresholds are specific to the ingress zone. For the “Trust” zone, choose a higher value, as many users may connect to the same popular sites on large networks.

```
set zone Trust screen syn-flood destination-threshold 10000
set zone Untrust screen syn-flood destination-threshold 1000
```

Limiting the Number of Sessions per Source/Destination IP

Limiting the total number of sessions that can be established to/from a specific IP address eliminates the chance of any particular user consuming too much of the firewall session capacity. These settings are especially helpful in preventing the effects of network worms or zombie-connections where a large number of legitimate connections are established in an attempt to overflow the network.

```
set zone Trust screen limit-session source-ip-based
set zone Trust screen limit-session source-ip-based 1000
set zone Trust screen limit-session destination-ip-based
set zone Trust screen limit-session destination-ip-based 10000

set zone Untrust screen limit-session source-ip-based
set zone Untrust screen limit-session source-ip-based 1000
set zone Untrust screen limit-session destination-ip-based
set zone Untrust screen limit-session destination-ip-based 10000
```

Preventing ICMP Floods

PING floods and other ICMP-based flood attacks can have a dramatic effect on the firewall, as each ICMP packet must be examined for checksum, sequence number and type. Large ICMP packets can also have an impact on available bandwidth. The following SCREEN settings will protect against large ICMP packets and limit the total number of ICMP packets per second to 1000. When that threshold is exceeded, the firewall ignores further ICMP packets for the remainder of that second plus the next second.

```
set zone Trust screen icmp-large
set zone Trust screen icmp-flood
set zone Trust screen icmp-flood threshold 1000

set zone Untrust screen icmp-large
set zone Untrust screen icmp-flood
set zone Untrust screen icmp-flood threshold 1000
```

Preventing UDP Floods

UDP floods generally have the least impact on the firewall itself because UDP is a connectionless protocol, and a stateful inspection firewall needs only to perform minimal inspection of UDP. The UDP flood can affect network availability by using excessive bandwidth. Because of this, using the firewall SCREEN protection to limit the number of UDP packets per second that targets a destination IP is recommended.

Note: Beginning with ScreenOS 5.4r2, UDP flood thresholds can be set per destination IP. This is especially useful for Domain Name System (DNS) servers, which may receive many requests per second in a large network.

```

set zone Trust screen udp-flood
set zone Trust screen udp-flood threshold 10000

set zone Untrust screen udp-flood
set zone Untrust screen udp-flood threshold 10000

```

Optimizing the Router

Many network environments typically place routers in front of the firewall. This allows the router to inspect, count and drop certain types of traffic before it reaches the firewall. Juniper Networks M-series routers, for example, feature the Internet2 application-specific integrated circuit (ASIC) support line rate Access Control Lists (ACLs), counting and policing. These features enable JUNOS software-based routers to provide additional protection against large floods. The following actions can be taken on any JUNOS software-based router to minimize the impact of large floods on both the firewall and available network bandwidth. *Appendix E* summarizes this configuration.

A large flood can present a challenge to any network as it can consume all available network bandwidth and may require extra processing by stateful firewalls. Large floods cause high CPU usage and slow response times.

While stateful firewalls provide both much needed visibility and fine-grade protection against a variety of floods, all stateful firewalls have an upper limit in their capacity to deal with certain types of floods such as SYN or ICMP floods. If faced with a flood beyond its capacity, the firewall experiences high-CPU load and as a result can drop legitimate traffic. The specific rate of attacks varies per firewall, depending upon its configuration and software version.

To protect the firewall and network against massive floods, rate limits should be implemented on routers protecting all interfaces of a firewall. The goal is to limit certain types of traffic, such as TCP control traffic and ICMP types, to rates that will *not* impact available bandwidth and overwhelm the firewall.

The following diagram shows how a small SYN attack can be handled by the firewall alone. However, a larger SYN attack that exceeds the firewall's packet processing rate can be rate-limited by adjacent routers to protect the firewall and network itself from the impact of a large flood

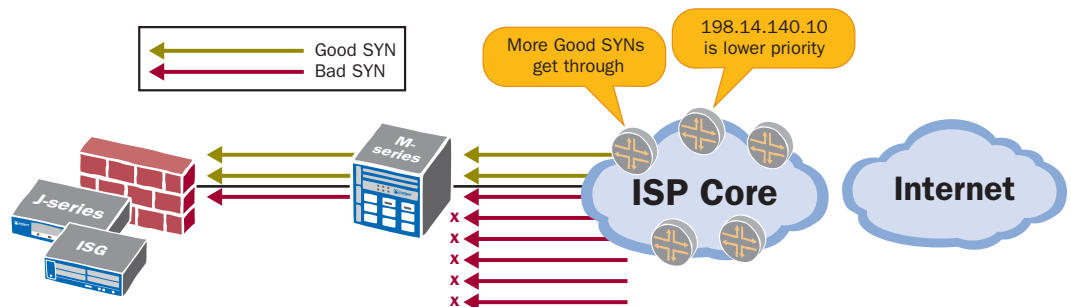


Figure 4. Handling SYN-Cookie on Juniper Networks Firewalls

Configuring J-Flow for Detecting Traffic

Flow statistics allow for greater granularity in the traffic data that is forwarded to the analysis engine. Enabling flow-based accounting in routers is an important step in gathering information for detecting DoS attacks. Follow these steps to enable accounting on the JUNOS software-based devices:

Enable the Flow Collector at the Interface:

```

interfaces {
  fe-0/0/1 {
    unit 0 {
      family inet {
        filter {
          input flow-filter<--- And/Or output, if desired.

```

Export the Information to STRM:

```

forwarding-options {
  sampling {
    input {
      family inet {
        rate 1;
        run-length 1;
      }
    }
  }
  output {
    cflowd <IP address of STRM> {
      port 9995;
      source-address <Loopback Address on Source Router>;
<--- It's best to use a loopback address for the source
      version 5;
    }
  }
}

```

Now that we can see the attack, how do we rate-limit it?

Rate-limiting TCP Control Traffic

In a normal baselined network, the percentage of TCP control traffic (SYN, FIN, register suppression times or RSTs) should typically not exceed 5 percent of bandwidth. Most stateless routers support the ability to rate-limit these TCP control packets. Once the counters have been implemented and a traffic baseline for the percentage of TCP control traffic in the network is established, one should consider rate-limiting this traffic to further protect the network.

If under normal conditions the network experiences less than 2 percent TCP control traffic—and suddenly the utilization increases to 10 or 20 percent—this can indicate a large flood attack. To ensure available bandwidth and protect the stateful devices within the network from being overwhelmed, rate-limiting TCP control traffic between 2 and 3 times above the baseline rates causes the router to start dropping TCP control traffic under heavy flood conditions.

However because the router can not distinguish between legitimate connections and floods, some legitimate connection requests are dropped as well. If 2 percent of the traffic is legitimate TCP control traffic, and the remaining 8 percent a flood, then rate-limiting the TCP control traffic to 5 percent will effectively block 4 percent of the flood and 1 percent of the legitimate control traffic. Any flood attacks allowed by the router are further detected and blocked by the firewall SYN-proxy mechanism, described on page 10, *Optimizing the Router*.

Rate-Limiting ICMP

Rate limits should also be used to protect the firewall against ICMP floods. Typically ICMP traffic should *not* exceed 1 percent of bandwidth. By rate-limiting all ICMP traffic on the routers surrounding the firewall, the firewall will never be overwhelmed with more ICMP floods than it can handle, and ICMP floods will never have a significant impact on a network's available bandwidth.

Rate-Limiting UDP

In most circumstances, UDP traffic does *not* need to be rate-limited to protect the firewall. However, rate limits could be implemented if desired to prevent UDP from consuming all available network bandwidth. The percentage of UDP traffic can vary from less than 5 percent to more than 50 percent of network traffic. After establishing a baseline, one can decide if it is necessary to rate-limit UDP to preserve bandwidth for other protocols.

Rate-Limiting Other IP Protocols

While a flood of non-IP traffic will *not* have a major effect on the firewall, it could have a large impact on bandwidth utilization. With the exception of routing, VPN and tunneling protocols, other IP protocols should typically be limited to 1 percent of network bandwidth. This helps prevent a flood of non-IP traffic from consuming all available network bandwidth.

Implementing Reverse Path Validation

Validating the return path prior to forwarding a packet can ensure that each packet allowed into the network has a valid return path. Validation helps eliminate the possibility of spoofed or illegally addressed packets entering the network.

Drop Non-Local Subnets with Filters

Internal traffic destined for the Internet should be subject to an access list which validates the source IP/subnet information. The ACL prevents spoofed packets from leaving the network before they reach the firewall.

For detailed information concerning enacting rate limiting policies with policing, refer to <http://www.juniper.net/techpubs/software/junos/junos91/swconfig-policy/frameset.html>.

Configure the system to limit traffic to the parameters suggested above and log the results. These logs can be used to determine the attack status at the router.

Responding to Large Floods

For sustained floods at rates 2 to 3 times higher than the router's rate-limit setting, the impact of the flood may cause excessive TCP retries in the network, as some legitimate SYNs may be dropped by the rate limits in addition to the flood traffic. The larger the floods, the more likely the rate limits will drop legitimate traffic and cause excessive retries or connection timeouts. In this instance, some "good" traffic is dropped sacrificially to preserve the network's availability.

One can minimize the effects of a large flood by blocking the source IPs of the flood in upstream routers. However, blocking the entire source IP or subnet is *not* possible in all cases because you could be blocking the firewall NAT address of a large organization, thereby blocking legitimate users from accessing the network. An alternative to blocking all traffic from the source IP is to rate-limit that traffic to a conservative amount. This will block the rate of flood and still allow legitimate traffic from the source, albeit at a reduced speed.

Note: By using counters on blacklist rules, you can constantly monitor if an attack is still in progress.

Responding Upstream

When floods are large enough to start reducing your available bandwidth and creating network congestion, upstream devices are the best method of addressing this problem. Typically, Internet Service Providers (ISPs) will rate-limit or drop traffic from a specific set of source IPs that are targeting the network. By selecting to rate-limit rather than block traffic, the size of the flood is reduced to a manageable level while still accepting legitimate connections from those source IPs. Again, counters can be used to indicate when the flood stops.

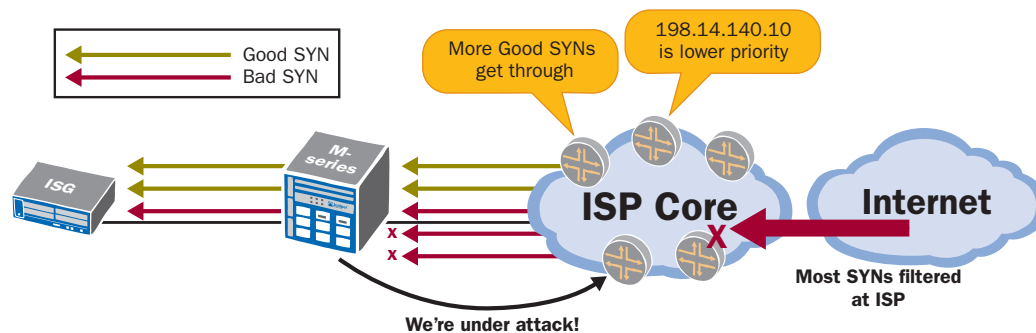


Figure 5. Communicating to Upstream ISP Devices to Address Floods

Automating a Response

If an automated response is preferred, scripts can be used to automatically blacklist offending IP addresses on the router. When the firewall detects an excessive flood above the alarm threshold, a SYSLOG message is sent indicating the source IP of the attacker. Periodic monitoring of the SYSLOG messages can trigger a script that will log into the router and blacklist or rate-limit that IP address. Continual monitoring of the counters associated with each blacklisted IP will indicate when the flood event stops, and the non-offending IP addresses can then be removed from the blacklist.

Juniper Networks is also working with Internet Engineering Task Force (IETF) members in the BGP community and has implemented a BGP notification message that can be configured to automatically blacklist or rate-limit offending IP addresses on upstream routers. This mechanism is used today by many service providers to block a flood closer to its source. The mechanism on which the response is based is called BGP Flow Specification.

It is possible to implement BGP Flow Specification in an enterprise network that is sufficiently large and has a BGP-based routing architecture. However, it would require that the enterprise renegotiate the peering agreements with their service providers and convince them to allow routing tables to be modified by the enterprise. This is *not* likely. The better way of achieving DDoS protection is to use a service provider-based mitigation service.

Configuring STRM

Using STRM to Poll Statistics Automatically

STRM is a security analysis and reporting system that can aggregate and apply rules to all data from network and server assets in your network. This system has the capability to baseline and report anomalous behavior in the network. The configuration of this system is covered in detail by the product documentation at <http://www.juniper.net>, but here are the basic steps to enable the system:

1. Configure all devices to send logging and SNMP data to the STRM. If devices such as SSG, ISG and IDP are controlled by Network Security Manager (NSM), use NSM to aggregate logging data and send it up to the STRM. This is configured by adding an action parameter under the Action Manager dialog that specifies the STRM IP address as the upstream syslog server. This reduces the CPU load on the individual firewall devices. See Figure 3.
2. Be sure to select what log parameters to be sent upstream with the “Device Log Action Criteria” configuration under the “Action Manager” tab on NSM. This command selects what log types and severity to send up to STRM. In the case of a SYN attack, we need to be sure that we’re sending TCP and DoS events. See Figure 4.
3. STRM will now automatically store and analyze the security events sent from NSM. The system presents a number of pre-generated reports that are quite useful for baselining network traffic. The reports also include delta traffic—from one day to the next—and automatic threat detection reports. See *Appendix D, Optimized Firewall Configuration*, for examples of automatically-generated reports.

Using STRM to Determine Attack Status

Enabling all of the recommendations discussed earlier provides a large amount of rich log activity for STRM to analyze. The system will now automatically detect and report attacks. The dashboard will show the attack status and the corresponding events can be used to “drill down” to determine the attack source and destination. See the following three figures for an example of a captured attack. This attack was accomplished by using HPING3 to send fragmented SYN packets against the data center firewall. The attack was at a constant rate (faster) and executed for more than 12 hours from two sources.

There are a large number of automatically generated reports available as soon as STRM receives data. Refer to the STRM documentation at <http://www.juniper.net> for a complete overview of available reports and instructions on how to build customized reports.

Figure 6 details the initial “Dashboard” display of a DoS attack. The event created is an “IDS SYN Attack” and is reported in the Most Severe Offenses by default. STRM is preconfigured to classify and categorize common security events.

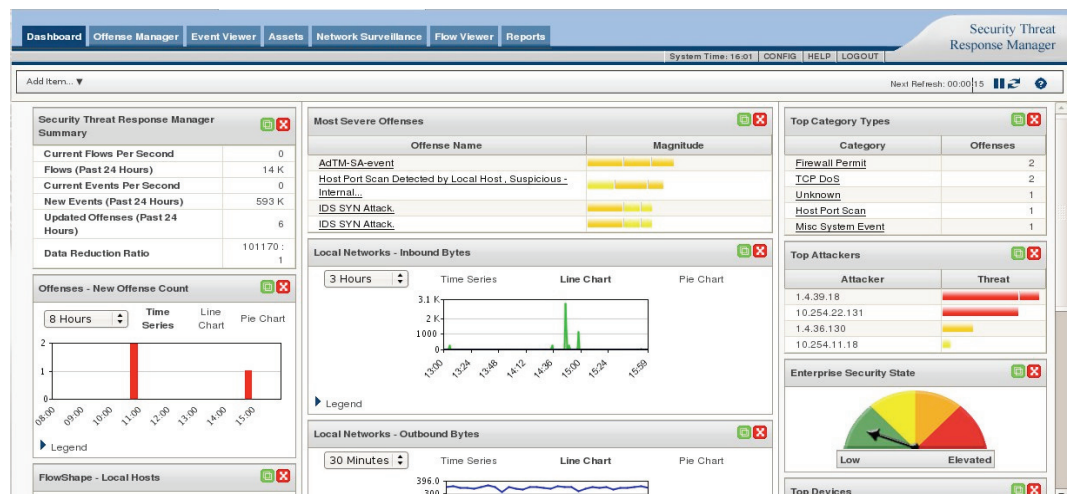


Figure 6. STRM Dashboard Showing Attacks

The attack can be analyzed in greater detail by clicking on its hyperlinked location on the Dashboard. Figure 7 shows greater detail on the incident, including the source, destination and event counts:

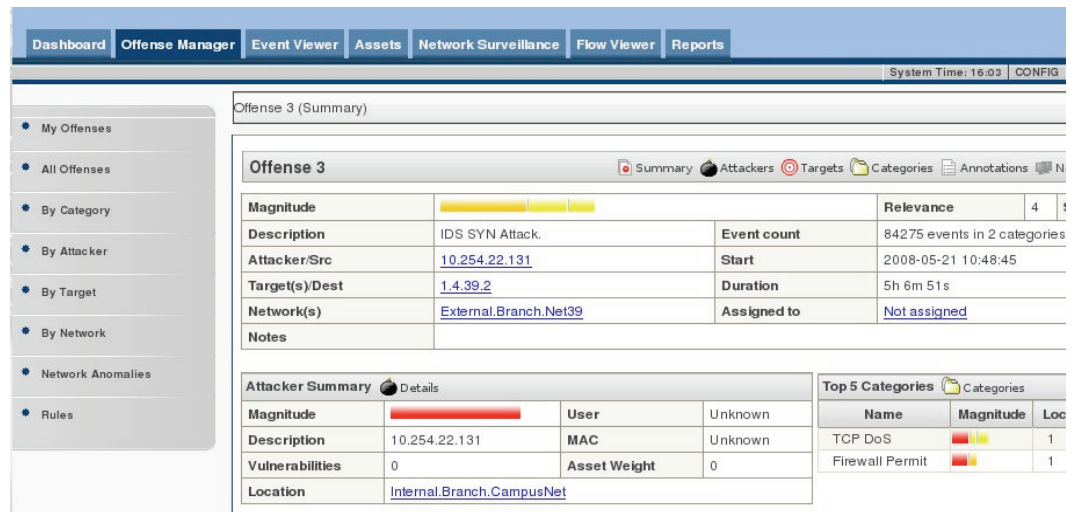


Figure 7. STRM Offense Manager Showing DoS Attack Details

Further detail on the attacker is provided by following the link on the Offense Manager page for the attack. Figure 8 shows detail on the attacker, including last known attack and all known attacks.

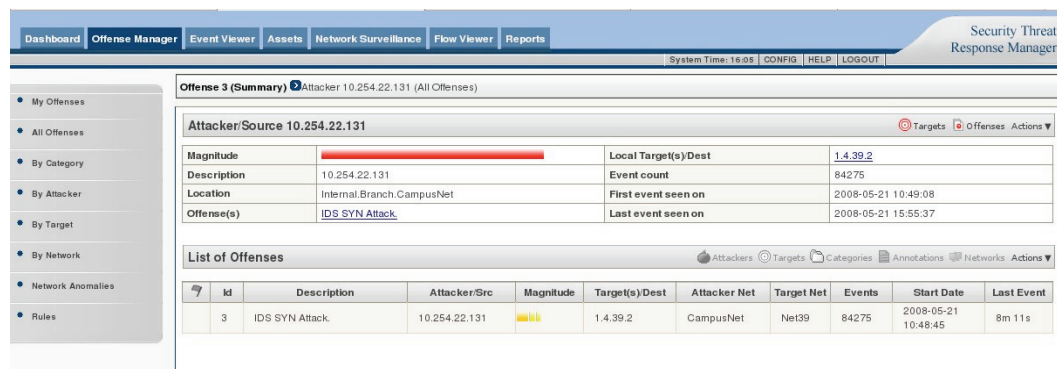


Figure 8. Drilling Down on the Attacker

Summary

In most cases, flood protection is typically implemented as a reflex reaction after an attack has taken place and exhausted network resources. The results of such attacks in the past have included impact to a company’s reputation, lost customers or lost data, ultimately leading to impact on a company’s financial health. The proactive approach discussed in this document requires minimal time and due diligence to configure and maintain. The benefit is a network that is capable of withstanding the impact of a large flood without sacrificing network availability—clearly an exercise worth expending resources on.

Understanding a network’s normal operating behavior, establishing baseline measurements and continuously monitoring events are critical in identifying DoS floods and optimizing the countermeasures discussed. When used together, stateful firewalls and stateless routers each provide complementary mechanisms to help mitigate the effects of DoS attacks on network availability by dropping the majority of undeniably unwanted flood traffic.

The combination of STRM, NSM and network elements can be used to rapidly analyze and respond to attacks. STRM allows operators to quickly locate attacks, attackers and targets. NSM allows a network administrator to quickly take preventive action. The net result is a more secure network, better visibility and a reduced burden on operations.

Appendix A Baseline Network Traffic using Router and Firewall Counters

Configuring the Router

Counters should be implemented on routers to count TCP control, ICMP and UDP packets traversing the network. By comparing these counters with the total number of packets seen, one can derive a percentage of total packets and bandwidth. *Appendix E* provides an example of such counter filters, which could be applied to any interface.

The following example shows counter values used to calculate the percentage of SYN packets and bytes compared with total packets and bytes.

```
admin@M7iA> show firewall
Filter: input-transit
Counters:
Name                               Bytes           Packets
count-ping                          33768           402
count-icmp                          55664           994
count-syn                            45599104        814280
count-rst                           47042208        817276

admin@M7iA> sho interface extensive ge-0/2/0
Traffic statistics:
Input bytes   :      29322316413           292786872 bps
Output bytes  :      27812702368           261606632 bps
Input packets:      43059013             54100 pps
Output packets: 49114141             60153 pps
```

Baseline Calculations:

$(814280 / 43059013) * 100 = 1.89$ percent of all packets are SYN packets

$(45599104 / 27812702368) * 100 = 0.164$ percent of all bytes are SYNs

Typically TCP control traffic should be less than 5 percent of packets and 1 percent of bytes, as shown in the above example. By monitoring interface counters from the router command line, one can easily calculate the percentage of SYN packets seen in the network. In the example below, 18 percent of all packets are SYNs—this network is experiencing heavy SYN flood.

Flood Condition Calculations:

```
admin@M7iA> show firewall
Filter: input-transit
Counters:
Name                               Bytes           Packets
count-ping                          40488           482
count-icmp                          62664           1119
count-syn                            585549488        14241013
count-rst                           58485346        1015695

admin@M7iA> sho interface extensive ge-0/2/0
Traffic statistics:
Input bytes   :      37724535633           375357040 bps
Output bytes  :      34492840916           230827360 bps
Input packets:      78210483             344162 pps
Output packets: 73980105             208047 pps
```

$(14241013 / 78210483) * 100 = 18.2$ percent of all packets are SYN packets
 $(585549488 / 37724535633) * 100 = 1.55$ percent of all bytes are SYNs

Similar logic can be applied to ICMP, UDP and RST floods using the ACLs documented in *Appendix E*.

Configuring the Firewall

If a Juniper Networks firewall is deployed within the network, it can give detailed visibility into the source and destination of the floods. See *Appendix F* for implementing the baseline SCREEN settings on the firewall that provide baseline settings for detecting these attacks.

Once enabled, SCREEN will create alarms when triggered. These are directed to the event log, SYSLOG or NSM Server. Detailed SCREEN statistics can be seen from the firewall's CLI and the number of attacks per second can be counted. This number can then be compared with the total number of connections counted to derive a percentage of flood traffic.

```
isg2000a(M)-> get count screen zone Internet

Screen counter on zone Internet
ICMP flood protection                0
UDP flood protection                0

UDP flood count for destination IP:
WinNuke attack protection           0
Port scan protection                0
IP sweep protection                 0
Teardrop attack protection          0
SYN flood protection                5341
SYN Flood(same source)              1598
SYN Flood(same destination)         2230
IP spoof attack protection           0

isg2000a(M)-> get count flow zone Internet
Flow counter on zone Internet
in bytes      740547675 | out bytes      345229152 | tcp proxy      12997
tear drop      0 | in vlan        0 | out vlan        0
in permit     828895568 | out permit    1005933079 | src route      0
no g-parent    0 | ping of death  0 | no gate sess   0
address spoof  0 | in icmp        115240 | no nat vector  0
land attack    0 | in self        0 | no map         0
icmp flood     0 | in un-auth     0 | no conn        0
udp flood      0 | in unk prot    0 | no dip         0
winnuke        0 | in vpn         0 | no gate        0
port scan      0 | in other       0 | no xmit vpf    0
ip sweep       0 | no mac         0 | no route       0
tcp out of seq 22 | mac relearn    0 | no frag sess   0
wrong intf     0 | slow mac       0 | no frag netpak 0
wrong slot     0 | trmng queue    0 | no sa          0
icmp broadcast 0 | trmng drop     0 | no sa policy   0
illegal pak    241348 | tiny frag      0 | sa inactive    0
url block      0 | syn frag       0 | sa policy deny 0
encrypt fail   0 | connections    1478769 | policy deny    0
```

Configuring NSM to Export Logs to STRM

1. Log into the NSM system and expand the **Action Manager** menu item on the left side of the page.

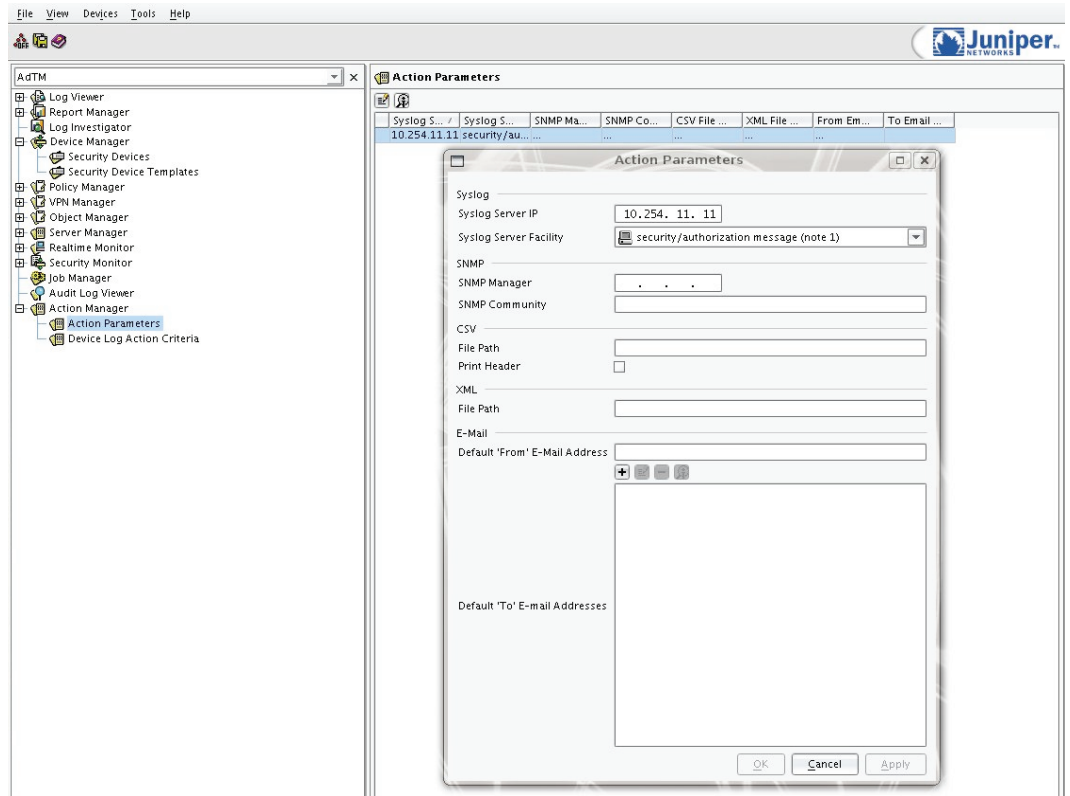


Figure 9. Action Parameters Window of NSM

1. Configure the **Action Parameters** to send Syslog messages to the STRM servers IP address, with the Syslog Server Facility set to local use 0 (local0).
2. Select the events that must be forwarded to this syslog target. Select **Action Manager/Device Log Action Criteria** submenu with the following main categories included: SCREEN, INFO, ALARM, SIGNATURE and TRAFFIC. All priorities were selected and most sub-categories as well. See Figure 10.

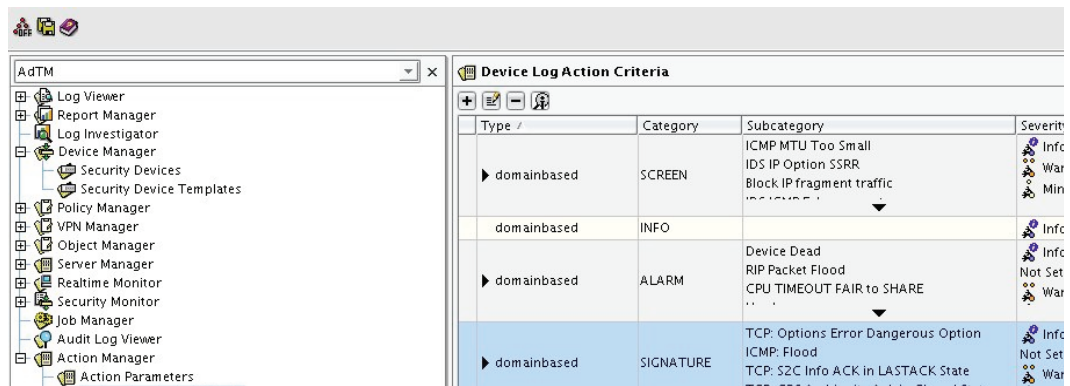


Figure 10. Selecting Device Log Action Criteria on NSM

Appendix B JUNOS Software Router Configuration for Counting Traffic

Note: These Firewall terms must be applied to interfaces before counting will occur. The term can be applied to multiple interfaces. However, if you wish to track counters per interface, you should create multiple identical terms and use one for each interface.

```
set firewall filter in term 1frag from first-fragment
set firewall filter in term 1frag then count 1frag
set firewall filter in term 1frag then next term
set firewall filter in term 2frag from is-fragment
set firewall filter in term 2frag then count 2frag
set firewall filter in term 2frag then next term
set firewall filter in term option from ip-options any
set firewall filter in term option then count option
set firewall filter in term option then next term
set firewall filter in term ping from protocol icmp
set firewall filter in term ping from icmp-type echo-request
set firewall filter in term ping from icmp-type echo-reply
set firewall filter in term ping then count ping
set firewall filter in term ping then next term
set firewall filter in term icmp from protocol icmp
set firewall filter in term icmp then count icmp
set firewall filter in term syn from protocol tcp
set firewall filter in term syn from tcp-flags "(syn & !ack)"
set firewall filter in term syn then count syn
set firewall filter in term synack from protocol tcp
set firewall filter in term synack from tcp-flags "(syn & ack)"
set firewall filter in term synack then count synack
set firewall filter in term fin from protocol tcp
set firewall filter in term fin from tcp-flags fin
set firewall filter in term fin then count fin
set firewall filter in term rst from protocol tcp
set firewall filter in term rst from tcp-flags rst
set firewall filter in term rst then count rst
set firewall filter in term dns from protocol udp
set firewall filter in term dns from destination-port 53
set firewall filter in term dns then count dns
set firewall filter in term other from protocol-except tcp
set firewall filter in term other from protocol-except udp
set firewall filter in term other from protocol-except ah
set firewall filter in term other from protocol-except esp
set firewall filter in term other from protocol-except gre
set firewall filter in term other then count other
set firewall filter in term default-permit then accept

#Apply the Filters to the appropriate Interface for your Network.
set interface ge0/2/0 unit 0 family inet filter input in
```

Appendix C Baseline SCREEN Settings

Note: The following Baseline SCREEN settings may be used as a starting point if no SCREEN settings were previously enabled on the device. Settings for Internet zone are shown; however, these baseline settings should be enabled on all zones subject to DoS attacks.

```
set zone "Internet" screen icmp-flood
set zone "Internet" screen udp-flood
set zone "Internet" screen udp-flood threshold 10000
set zone "Internet" screen syn-flood
set zone "Internet" screen ip-spoofing
set zone "Internet" screen syn-frag
set zone "Internet" screen tcp-no-flag
set zone "Internet" screen icmp-large
set zone "Internet" screen syn-fin
set zone "Internet" screen fin-no-ack
set zone "Internet" screen syn-flood alarm-threshold 10000
set zone "Internet" screen syn-flood queue-size 20000
set zone "Internet" screen syn-flood attack-threshold 10000
set zone "Internet" screen syn-flood source-threshold 500
set zone "Internet" screen syn-flood destination-threshold 500
set zone "Internet" screen limit-session source-ip-based 10000
set zone "Internet" screen limit-session destination-ip-based 10000
```

Appendix D Optimized Firewall Configuration

The following example configuration implements *all* of the SCREEN and flow settings described in the implementation section of this document. The example is based on the STOAN (Securing the Open Access Network) solution and implies 1 GB Internet uplinks, 1500 Sessions/Second of normal “background traffic” and an ISG Series firewall with the SYN-Cookie performed entirely in hardware.

```
set flow check tcp-rst-sequence
unset flow no-tcp-seq-check
set flow tcp-syn-check
set flow syn-proxy syn-cookie

set zone "Internet" screen icmp-flood
set zone "Internet" screen udp-flood
set zone "Internet" screen winnuke
set zone "Internet" screen port-scan
set zone "Internet" screen tear-drop
set zone "Internet" screen syn-flood
set zone "Internet" screen ip-spoofing
set zone "Internet" screen ping-death
set zone "Internet" screen ip-filter-src
set zone "Internet" screen land
set zone "Internet" screen syn-frag
set zone "Internet" screen tcp-no-flag
set zone "Internet" screen ip-bad-option
set zone "Internet" screen ip-record-route
set zone "Internet" screen ip-timestamp-opt
set zone "Internet" screen ip-security-opt
set zone "Internet" screen ip-loose-src-route
set zone "Internet" screen ip-strict-src-route
set zone "Internet" screen ip-stream-opt
set zone "Internet" screen icmp-fragment
set zone "Internet" screen icmp-large
set zone "Internet" screen syn-fin
set zone "Internet" screen fin-no-ack
set zone "Internet" screen limit-session source-ip-based
set zone "Internet" screen limit-session destination-ip-based
set zone "Internet" screen icmp-id
set zone "Internet" screen ip-sweep threshold 100000
set zone "Internet" screen port-scan threshold 100000
set zone "Internet" screen udp-flood threshold 10000
set zone "Internet" screen limit-session source-ip-based 1000
set zone "Internet" screen syn-flood alarm-threshold 1000
set zone "Internet" screen syn-flood attack-threshold 1000
set zone "Internet" screen syn-flood source-threshold 250
set zone "Internet" screen syn-flood destination-threshold 250
set zone "Internet" screen limit-session destination-ip-based 10000
```

```
set zone "Campus" screen icmp-flood
set zone "Campus" screen udp-flood
set zone "Campus" screen winnuke
set zone "Campus" screen port-scan
set zone "Campus" screen tear-drop
set zone "Campus" screen syn-flood
set zone "Campus" screen ip-spoofing
set zone "Campus" screen ping-death
set zone "Campus" screen ip-filter-src
set zone "Campus" screen land
set zone "Campus" screen syn-frag
set zone "Campus" screen tcp-no-flag
set zone "Campus" screen ip-bad-option
set zone "Campus" screen ip-record-route
set zone "Campus" screen ip-timestamp-opt
set zone "Campus" screen ip-security-opt
set zone "Campus" screen ip-loose-src-route
set zone "Campus" screen ip-strict-src-route
set zone "Campus" screen ip-stream-opt
set zone "Campus" screen icmp-fragment
set zone "Campus" screen icmp-large
set zone "Campus" screen syn-fin
set zone "Campus" screen fin-no-ack
set zone "Campus" screen limit-session source-ip-based
set zone "Campus" screen limit-session destination-ip-based
set zone "Campus" screen icmp-id
set zone "Campus" screen ip-sweep threshold 100000
set zone "Campus" screen port-scan threshold 100000
set zone "Campus" screen udp-flood threshold 10000
set zone "Campus" screen limit-session source-ip-based 1000
set zone "Campus" screen limit-session destination-ip-based 10000
set zone "Campus" screen syn-flood alarm-threshold 1000
set zone "Campus" screen syn-flood attack-threshold 1000
set zone "Campus" screen syn-flood source-threshold 250
set zone "Campus" screen syn-flood destination-threshold 250
```

Appendix E Optimized Router Configuration

The following configuration example implements *all* of the rate limits and filters discussed previously. The example is based on the STOAN solution and implied 1 GB uplinks. Rate limits are set according to the ISG 2000 capacity with SYN-Cookie enabled. This is *only* the flood configuration. Configurations necessary to harden the routers are *not* shown.

```
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 5m
set firewall policer point-2-percent if-exceeding burst-size-limit 150k
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
set firewall policer point-2-percent2 if-exceeding bandwidth-limit 5m
set firewall policer point-2-percent2 if-exceeding burst-size-limit 150k
set firewall policer point-2-percent2 then discard

set firewall filter out term source from source-address 0.0.0.0/32
set firewall filter out term source then log
set firewall filter out term source then discard
set firewall filter out term destination from destination-address 0.0.0.0/32
set firewall filter out term destination then log
set firewall filter out term destination then discard
set firewall filter out term 1frag from first-fragment
set firewall filter out term 1frag then policer one-percent
set firewall filter out term 1frag then next term
set firewall filter out term 2frag from is-fragment
set firewall filter out term 2frag then policer one-percent
set firewall filter out term 2frag then next term
set firewall filter out term options from ip-options any
set firewall filter out term options then policer one-percent
set firewall filter out term options then next term
set firewall filter out term ping from protocol icmp
set firewall filter out term ping from icmp-type echo-request
set firewall filter out term ping from icmp-type echo-reply
set firewall filter out term ping then policer point-2-percent
set firewall filter out term ping then next term
set firewall filter out term icmp from protocol icmp
set firewall filter out term icmp from icmp-type-except echo-request
set firewall filter out term icmp from icmp-type-except echo-reply
set firewall filter out term icmp then policer point-2-percent2
set firewall filter out term syn from protocol tcp
set firewall filter out term syn from tcp-flags "(syn & !ack)"
set firewall filter out term syn then policer five-percent
set firewall filter out term synack from protocol tcp
set firewall filter out term synack from tcp-flags "(syn & ack)"
set firewall filter out term synack then policer five-percent
```



```
set firewall filter out term fin from protocol tcp
set firewall filter out term fin from tcp-flags fin
set firewall filter out term fin then policer five-percent
set firewall filter out term rst from protocol tcp
set firewall filter out term rst from tcp-flags rst
set firewall filter out term rst then policer five-percent
set firewall filter out term other from protocol-except tcp
set firewall filter out term other from protocol-except udp
set firewall filter out term other from protocol-except ah
set firewall filter out term other from protocol-except esp
set firewall filter out term other from protocol-except gre
set firewall filter out term other then policer one-percent
set firewall filter out term default-permit then accept
#Apply the Filters to the appropriate Interface for your Network.
Set interface ge0/2/0 unit 0 family inet filter output out
```

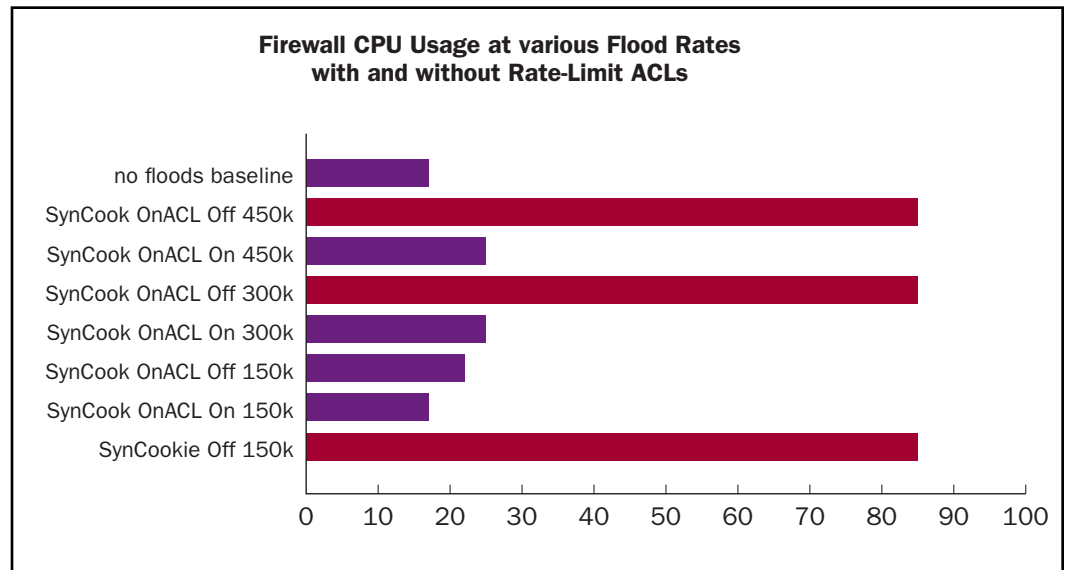
Appendix F Test Results

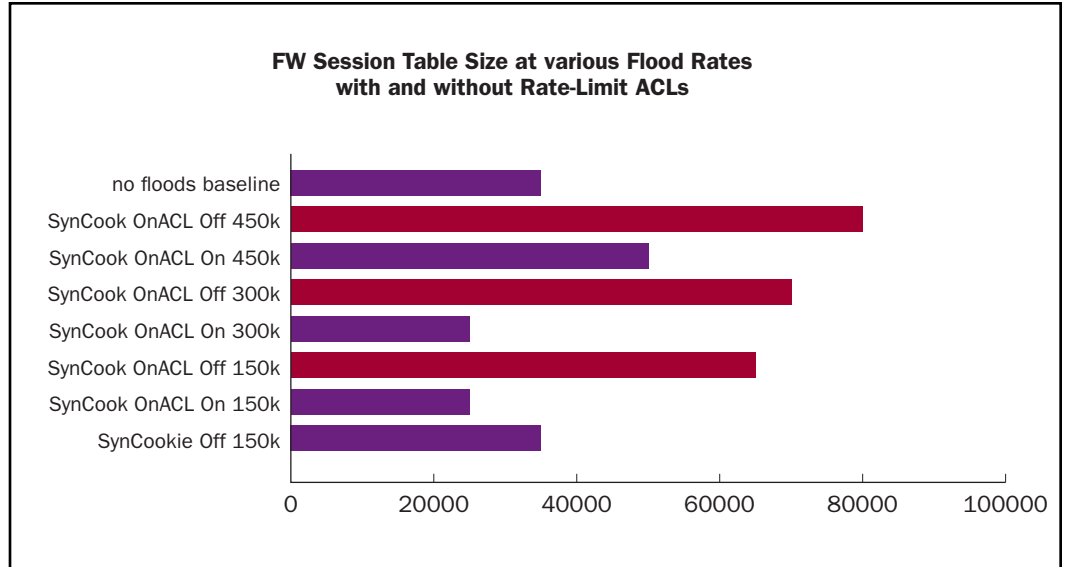
Extensive DoS testing was performed on the STOAN solution, which consists of an ISG 2000 firewall placed between a pair of Juniper Networks M-series routers on its “Untrust” and “Trust” zones. Testing was performed both with and without the above mentioned rate limits in place on the routers. The router and firewall configurations used for the tests were the same as referenced in the appendices of this document. Testing was performed with ScreenOS 5.4r1 using the configuration referenced above. Background traffic of 420 Mbps (1700 sessions/sec) was run constantly during testing to create a normal traffic baseline. Floods were introduced for a period of 5 minutes and results recorded.

The results clearly show the improvement that the rate limits provide in dealing with large floods. For SYN floods smaller than 150,000 packets per second (PPS) (or 73 Mbps), the ISG firewall with SYN-Cookie mechanism can proxy enough connections to suppress the flood and pass the background traffic with a comfortable CPU level of 22 percent utilization.

At rates slightly above this, the router ACLs will start dropping SYNs. The trade off is that now some legitimate SYNs will be sacrificed to protect the network. In a normal network, this will result in occasional retries and timeouts—a much better alternative than a complete network outage. As the flood rate increases above the settings of the rate limits, the firewall’s CPU and session table level out.

A final test was run with a mix of floods: SYN flood, PING flood and UDP flood, each being sent through the solution at 107,000 PPS, for a total of 321,000 PPS (or 150 Mbps) of flood traffic. At these rates, both the SYN and ICMP rate limits were exceeded and traffic was dropped sacrificially to protect the network. After five minutes, the firewall CPU remained a constant 30 percent and legitimate PING and SYN response times through the network were acceptable.





About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

**CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA**
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Aldlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

**To purchase Juniper Networks solutions, please
contact your Juniper Networks sales representative
at 1-866-298-6428 or authorized reseller.**