Application Note

Perimeter Gateway with Firewall, IDP and NSM

A Triage (Layered) Approach to Security in the Network Perimeter

Mike Swarm, Consulting Engineer

Alan Sardella, Marketing Consultant

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: **350070-001 June 2005**

Contents

Copyright © 2005, Juniper Networks, Inc.

Executive Summary

The network detailed in this application note was built to undergo a real world test for a large enterprise central site perimeter. It was requested for a public event that would have numerous sophisticated users, both wired and wireless; these users required both internal and Internet access. In addition to the topology of the network and the design decisions taken in putting it together, this document provides annotated configurations of the routers and firewalls used in the perimeter gateway.

Juniper tested this network with hundreds of users, and to verify the integrity of our attack prevention capabilities, we advertised a /8 network (or 1% of all allocated IPv4 space) to the public Internet, which naturally resulted in significant attack traffic. This exposure is far greater than a typical enterprise network would face. Essentially, Juniper Networks put its perimeter gateway design[1] to a virtual "torture test," and this test passed with 100% uptime over a two week period.

In this highly-effective "triage" approach (a layered process wherein the attacks are ranked in terms of priority) to network security, measurements are taken of the volume, type, sources and destinations of attacks. The method attempts to eradicate a large chunk of the problem and then repeat the process. In this example, we were able to take out approximately 75% of the attack traffic in the first pass, and then were able to identify more specific configuration changes to handle the remainder in increments.

The overriding security goal with this network was high availability. Juniper achieved this by mitigating security breaches such as floods and scans. In this application note, we provide concrete examples of the design and configuration of this network, as well as topology drawings and configuration snippets. Some of the basic services we illustrated were performance monitoring, High Availability (using OSPF and NSRP), Flood Settings, Layer 3/Layer 4 firewall, and Layer 7 IDP.

It is interesting to note that none of the engineers who maintained this network knew how to operate all of the products. In that sense, the division of specialties was not unlike that often found in an enterprise. Relevant content areas were JUNOS, ScreenOS, the Instant Virtual Extranet (IVE), IDP and the NetScreen-Security Manager (NSM). The management of this network was the essential key to the high security we achieved; we were able to collect and analyze attack information on a continual basis.

Background and Purpose

This network served as an enterprise demonstration on how to handle being a target for network attacks and other Internet mischief. A network security provider needs to focus on maintaining security through the use of firewalls and skilled security experts. The basic parameters of the project are outlined in the following sections.

[1] See *Central Site Edge Solution Brief* and *High Availability at the Central Site Edge* at www.juniper.net.

Copyright © 2005, Juniper Networks, Inc.

Edge Routers and Firewalls

The edge routers and firewalls provide a load-balanced path to the Internet, while protecting the network from attack with stateless filters (ACLs).

For this network, the specifications and requirements for edge routers and firewalls were as follows:

- Minimum of four (4) 100BaseTx Full Duplex interfaces, one for each of the secure interior routers and one for the each of the exposed exterior routers
- Ability to handle a minimum of 45 Megabits of sustained traffic inbound and outbound, while maintaining state with the other firewall and applying a useful set of security rules
- High Availability (HA) routed mesh with routed edge resiliency
- OSPF routing capability
- Ability to transmit ping and traceroute
- Ability to handle IP Multicast (PIM-SM) and multicast policy

The goal was to have the configuration of these firewalls allow full use of dual Internet connections, and to have intelligent, stateful failover should one path fail. Failover needed to be seamless for this test, and this was attained—every link in the perimeter was explicitly broken and failover was on the order of a second with no TCP sessions lost. Voice calls were also maintained during the high availability tests.

IDP Throughout the Network

The security solution included software that could analyze and act on intrusion attempts and modify the firewall/firewall rule set as necessary. Although the Juniper Networks IDP solution could have been placed inline for increased ability to prevent attacks, the sponsors of this network requested that the IDP devices be placed into tap mode, which meant that effectively the IDP devices were only performing intrusion detection.

Personnel

Engineers were needed to design, implement, and operate a security system that addressed the needs of the network users. HA was the major requirement of the system, along with the prevention of Denial of Service (DoS) attacks.

Responsibilities were as follows:

- Design security for specific events
- Install the network
- Establish and implement the network security policy
- Monitor the operation of the firewalls and alert staff to any security incidents

Juniper Equipment and Features

Juniper provided the following equipment to meet these requirements.

Copyright © 2005, Juniper Networks, Inc.

- 2 WAN routers (M7i, DS-3, GE, FE, AS PICs)
- 4 NS-5200 (one racked spare)
- 2 IDP-1000
- 1 SSL RA-500
- 2 rack-mount Linux servers for NSM and IDP management

The design included the following:

- High Availability with OSPF and NSRP
- Flood Settings
- SNMP performance monitoring
- NSM Custom Reports

We demonstrated excellent performance handling both Layer 3/Layer 4 and Layer 7 attacks.

Logical and Physical Topology

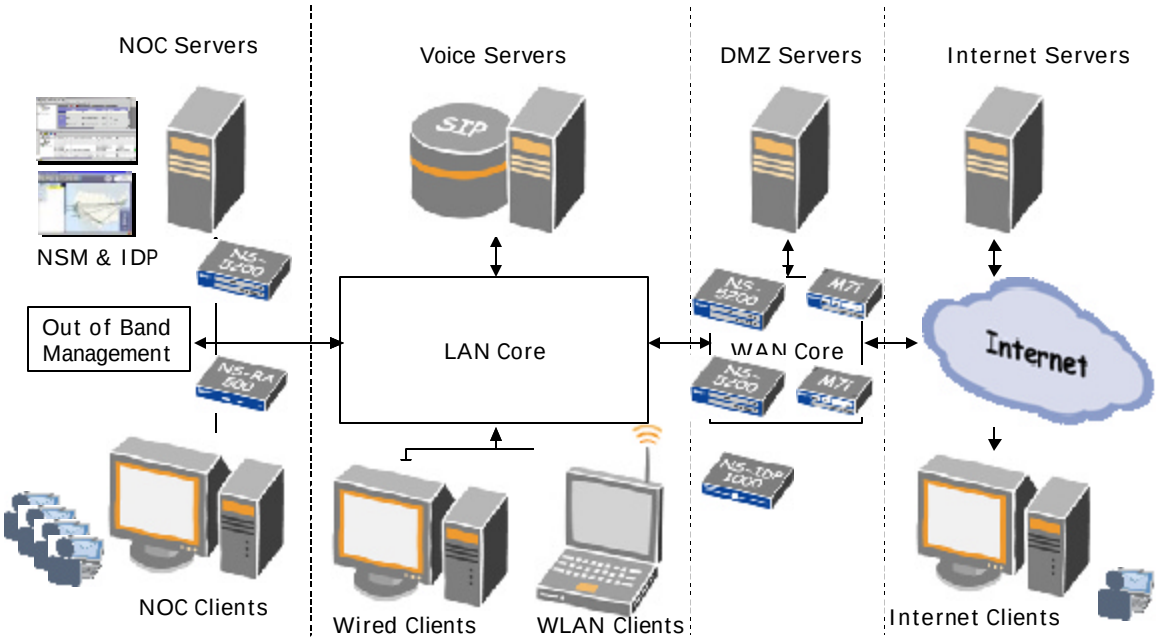
The security problem was to provide high availability and to control traffic between the following zones with policies:

- Management module
- Campus LAN
- WAN Gateway (Perimeter)
- An Internet component

We applied Juniper solutions to the NOC and the DMZ, and also provided engineering support.

Copyright © 2005, Juniper Networks, Inc.

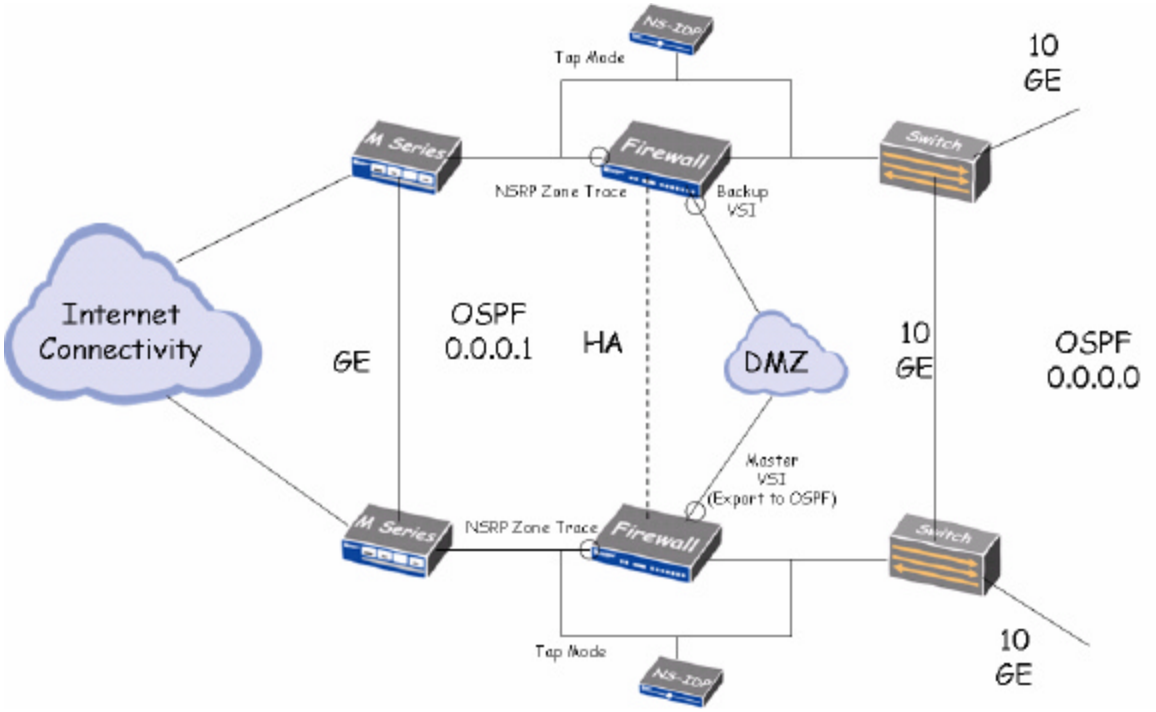
Figure 1: Logical View of the Network



The physical network diagram follows.

Copyright © 2005, Juniper Networks, Inc.

Figure 2: Physical View of Perimeter



Note: Annotated configurations for this network are provided in *Appendix A*.

System Capabilities

In this network, security services were centrally managed from the Network Operations Center (NOC) where security operations worked side-by-side with network operations. NetScreen Security Manager (NSM) and IDP Manager provided security engineers with security alerting, monitoring and reporting.

Availability and robust operation were critical to the network operation. Engineers monitored the following for attacks:

- Network Scans and Floods (zero-day)
- Known Exploits (known)
- Protocol Anomalies (zero-day)
- Spyware (known)
- Volumes and Rates (zero-day)

Endpoint Security was provided with endpoint profiles and host checks.

The core Gigabit Ethernet gateway (WAN to LAN) included firewall filtering for known network scans. The WAN gateway filtered large volumes of network scans and floods.

Copyright © 2005, Juniper Networks, Inc.

Many users provided their own gateway security, often doing address translation and using virtual private networks (VPNs) to remote applications. The network also provided wired access for media and conferences. Free wireless access was provided, and this guest access was provided in unsecured and secured options. Anonymous guest access was a particular challenge for endpoint security.

DMZ firewalls provided service-level access to network services like DNS, DHCP, RADIUS and SMTP relay.

Some of the security features included:

- Role-based SSL NOC access (SSL)
- Intrusion prevention (IDP)
- DoS flood protection (firewall, router and NSM)

Role-based SSL NOC Access

SSL integration with identity management provided external access to the NOC. So NOC personnel, corporate headquarters personnel, or network troubleshooters had access to all or specific NOC services based on their identities and roles.

Inline Intrusion Prevention

IDP gave NOC engineers the ability to identify and drop attacks. This helped contain worm infections and outbreaks. Most other kinds of attacks were also identified and monitored. The IDP was configured in tap mode per the request of the sponsors of the network.

DOS Flood Protection

Because availability was key, firewall stateful inspection synchronized and correlated traffic associated with normal traffic and DOS floods. Rate limits protected network availability, without restricting accepted use. Filters on both firewall and upstream routers (immediately upstream and across the narrow WAN link) enforced policy.

Methodologies and Observations

There are methodologies and observations from this project that are applicable to designing a perimeter gateway for high availability and for maintaining a secure network connected to the Internet. These are discussed in the following sections.

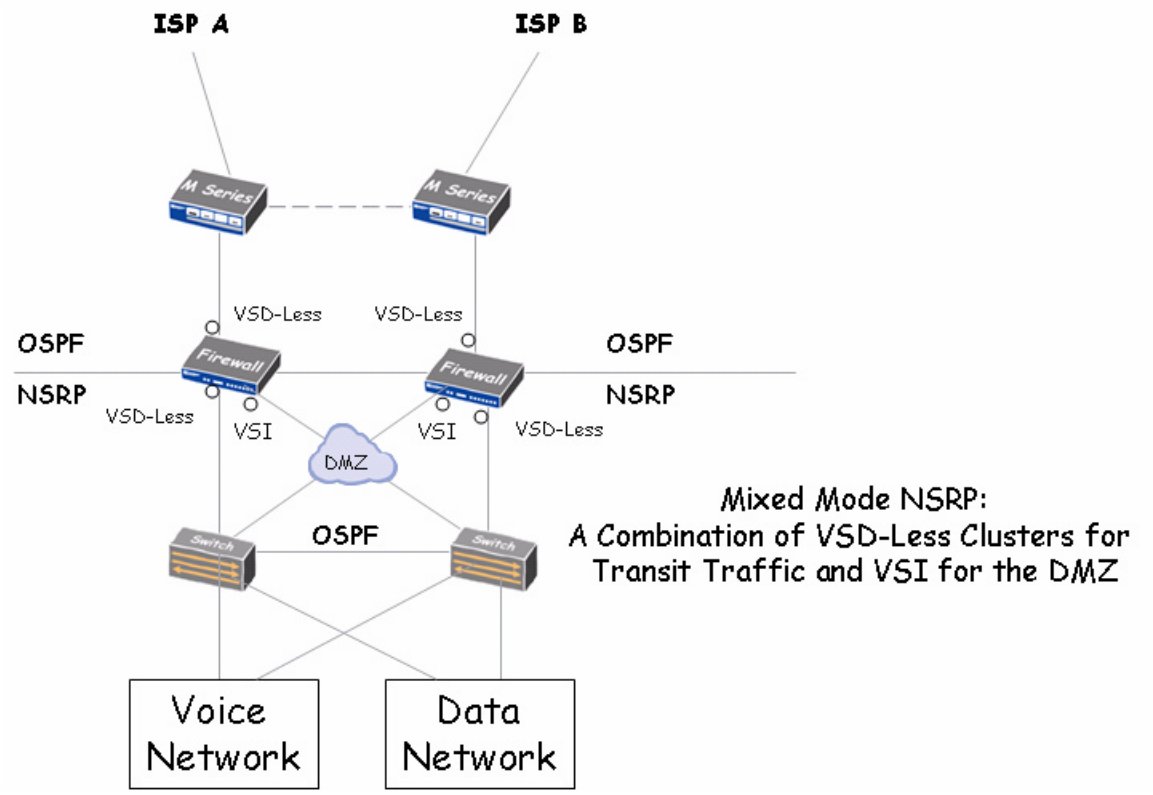
The main security problem that Juniper was charged with solving was to maintain a high availability Internet perimeter gateway, and to mitigate security breaches such as floods and scans. We had approximately 700-1000 scan events/second.

High Availability at the Edge

Copyright © 2005, Juniper Networks, Inc.

The following high availability design was used at the edge and it can be applied for redundancy in many other sectors of the network.

Figure 3: High Availability Solution with DMZ



The high availability solution was very similar to that presented in the application note, *High Availability at the Central Site Edge* at www.juniper.net. The difference here was that some interfaces were using Virtual Security Domains (VSD) so that a DMZ could be set up from the firewalls. See the annotated configuration files for the firewalls in *Appendix A* for details.

Attacks, Scans and Floods

The network advertised a Class A network with a /8 mask, which represented 1% of all Internet address space. This large address space acted much like a large honeynet, collecting a large sample of random attacks.

Because the network was an open network used for research and development as well as demonstration of multivendor security solutions, the perimeter security policy was to permit any traffic, except traffic which was an availability threat to the network.

Copyright © 2005, Juniper Networks, Inc.

Rule Sets and Access Control Lists

The resulting perimeter rule set implementation is to permit any traffic, but to have optional traffic blacklists, and to globally enforce flood and scan mitigation.

Figure 4: Perimeter Firewall Incoming Rule Set (DMZ Rule Set Not Shown)

Match					Action	Install On	Rule Options
From Zone	Source	To Zone	Destination	Service			
untrust	any	trust	any	services-black-list	deny	any	
untrust	internet-badboys-blacklist	trust	any	any	deny	any	
untrust	any	trust	any	any	permit	any	

The outgoing rule set, from trust to untrust, is shown next.

Figure 5: Perimeter Firewall Outgoing Rule Set (DMZ Rule Set Not Shown)

Match					Action	Install On	Rule Options
From Zone	Source	To Zone	Destination	Service			
trust	Client-Watch-List	untrust	any	any	permit	any	Log
trust	any	untrust	any	any	permit	any	
trust	any	untrust	any	imaps	permit	any	

The perimeter IDP rules follow.

Figure 6: Perimeter IDP Rule Set

Match		Look For	Action			
Source IP	Destination IP	Attacks	Action	Notification	Install On	Comments
Ike's	any	IKE: Malformed Packet	ignore	none	any-sensor	
any	any	none	none	logging	any-sensor	
any	any	Anomalies - Critical Signatures - Critical	none	logging alarm syslog log packets(10/100)	any-sensor	This rule drops all critical severity attacks and logs them as alarms. Enable this rule if you are running your IDP in in-line mode, and wish to protect your network against critical attacks and IDS evasion attempts.
any	any	Anomalies - High Signatures - High	none	logging alarm log packets(10/100)	any-sensor	This rule drops all high severity attacks and logs them as alarms. Enable this rule if you are running your IDP in in-line mode, and wish to protect your network against critical attacks and IDS evasion attempts.
any	any	Signatures - Medium	none	logging	any-sensor	This rule logs all mediumseverity attacks and protocol anomalies.

On the perimeter firewall, the following attacks are screened for; this is only a subset—not all attack settings are shown.

Figure 7: Perimeter Firewall Flood and Scan Attack Settings

Copyright © 2005, Juniper Networks, Inc.

```
set zone "Untrust" screen syn-flood
set zone "Untrust" screen syn-flood timeout 1
set zone "Untrust" screen syn-flood queue-size 20000
set zone "Untrust" screen syn-flood attack-threshold 1000
set zone "Untrust" screen syn-flood source-threshold 100
set zone "Untrust" screen syn-flood destination-threshold 500
set zone "Untrust" screen port-scan
set zone "Untrust" screen port-scan threshold 100000
set zone "Untrust" screen ip-sweep
set zone "Untrust" screen ip-sweep threshold 100000
set zone "Untrust" screen limit-session source-ip-based
set zone "Untrust" screen limit-session source-ip-based 2000
set zone "Untrust" screen limit-session destination-ip-based
set zone "Untrust" screen limit-session destination-ip-based 2000
set zone "Untrust" screen icmp-flood
set zone "Untrust" screen icmp-flood threshold 100
set zone "Untrust" screen udp-flood
set zone "Untrust" screen udp-flood threshold 5000
```

To see the screening rules on the WAN routers, see *Set Display of JUNOS Firewall Filters* in *Appendix A*. The first thing the security engineers observed was widespread attacks that correlated closely to the top attacks the Juniper Security Portal (www.juniper.net/security) honeynet was reporting. The top attacks were buffer overflows for SQL Server 2000, LSASS and RPC DCOM.) The top attacked ports were 445, 135-139 and 1433-1434.

Figure 8: WAN Router Firewall ACL (Snipped: See *Appendix A* for Complete Screens)

```
firewall {
    filter screen {
        term tcp135 {
            from {
                protocol tcp;
                destination-port 135;
            }
            then {
                count tcp135;
                discard;
            }
        }
        term tcp137 {
            from {
                protocol tcp;
                destination-port 137;
            }
            then {
                count tcp137;
                discard;
            }
        }
/* SNIPPED */
        term tcp1023 {
            from {
```

Copyright © 2005, Juniper Networks, Inc.

```
                protocol tcp;
                destination-port 1023;
            }
            then {
                count tcp1023;
                discard;
            }
        }
        term scanboy {
            from {
                source-address {
                    200.27.133.44/32;
                }
            }
            then {
                count scanboy;
                discard;
            }
        }
    }
```

The first round of triage identified and blocked the largest volume of attacks to Local Security Authority Subsystem Service (LSASS) and RPC DCOM. The top attacked ports were 445 and 135-139. These were first added to the firewall blacklist, and later moved to bulk blacklist on the WAN routers. (It is unlikely that legitimate clients would use these low-numbered UDP/TCP source ports.)

Figure 9: Top Attacked Ports after First Round of Triage (1433: SQL Slammer)

The second round of triage identified and blocked SQL Server 2000 attacks (SQL Slammer). Attacked ports 1433-1434 were first added to the firewall blacklist, and later moved to the bulk blacklist on the WAN routers. We wanted to ensure clients were not using these UDP source ports.

Copyright © 2005, Juniper Networks, Inc.

Figure 10: Top Attacked Ports after Second Round of Triage

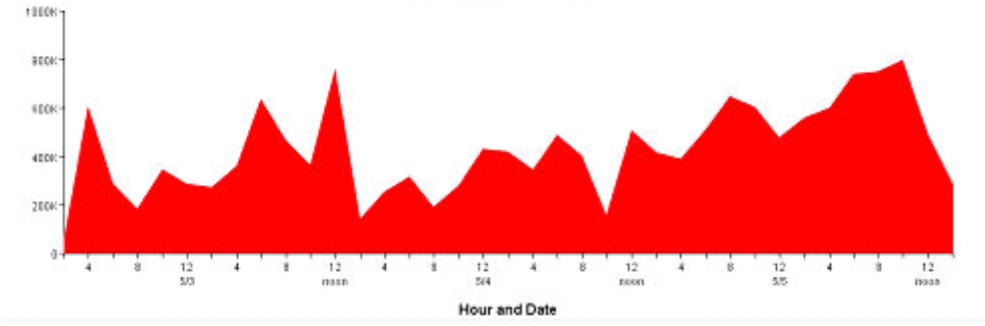
The WAN routers reported 20-30 Kpps of blacklisted scan attack traffic, which amounted to approximately 10-15 Mbps of the DS3 bandwidth. Eventually, to free 10-15 Mbps of DS3 bandwidth, the bulk blacklist on WAN routers was duplicated on the upstream service provider routers. After we did this, 20-30K pps of scan attacks were blocked, resulting in a savings of 10-15 Mbps of the DS3 bandwidth.

Blacklisting the widespread attacks reduced the noise, and reduced the largest threats to availability. This did not necessarily protect against the latest or highest severity attacks to the endpoints.

Bursts of scan attack traffic were usually from one well-connected source, continuously scanning for one destination vulnerability at hundreds to thousands of packets per second. Firewall flood and scan mitigation automatically rate-limited this. Flood and scan mitigation rate limiting dropped 1/3 of traffic between the untrust and trust ports. Engineers continued to monitor and triage the network, adding a handful of sources to the blacklist.

Rather than extending the use of port blocking, we opted for the use of blacklists of particular source IP addresses, because we did not want to block legitimate traffic. Several well-known attacks (mainly BOTS) were observed that scanned on high numbered ports. For example, TCP port 3127 is used by the myDoom/Novarg virus as a backdoor port. DoomJuice, Welchia, and Deadhat have appeared as the first widely spread worms to take advantage of this back door, but port 3127 has become one of the favorite infection vectors of an endless parade of Agobot and other malware. We averaged 3000 scans destined for this port per minute.

Figure 11: Port 3127 Scans per Hour



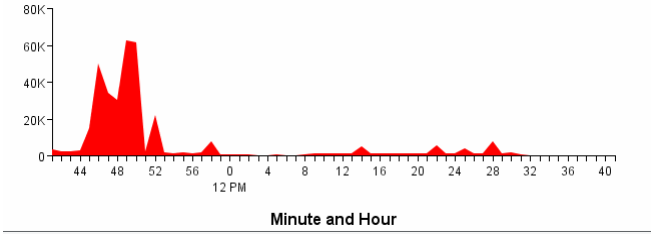
Copyright © 2005, Juniper Networks, Inc.

Triage Example

What follows is a single example, demonstrating the process of attack analysis by volume, type, source and destination, which occurred continuously at multiple layers, and for multiple types of attacks.

The following report shows the volume of flood attacks at 3,000-60,000 attacks/minute, or 50-1000 flood attacks per second.

Figure 12: Volume of Flood Attacks (L3/L4)

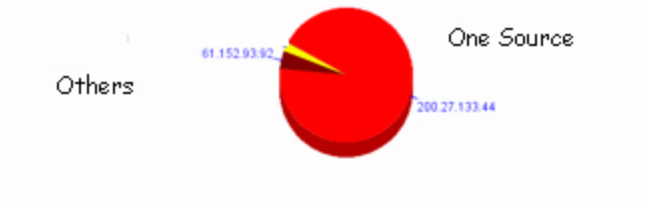


The following chart shows t he types of flood attacks. It indicates that the TCP SYN attack (Screen; IDS SYN Attack) is the most prevalent.

Figure 13: Types of Flood Attacks (Recent L3/L4 Flood Classes)

The following pie chart shows TCP SYN scan sources. A single well-connected s ource (200.27.133.44) represents most of the events.

Figure 14: TCP SYN Scan Sources



The following pie chart shows TCP SYN scan destinations. A single well-connected source is scanning for a single WINS vulnerability.

Copyright © 2005, Juniper Networks, Inc.

Figure 15: Destination of TCP SYN Scan Attacks

It should be noted that handling floods (Layer 3 and Layer 4) attacks, and Layer 7 attacks, is very similar.

Conclusion

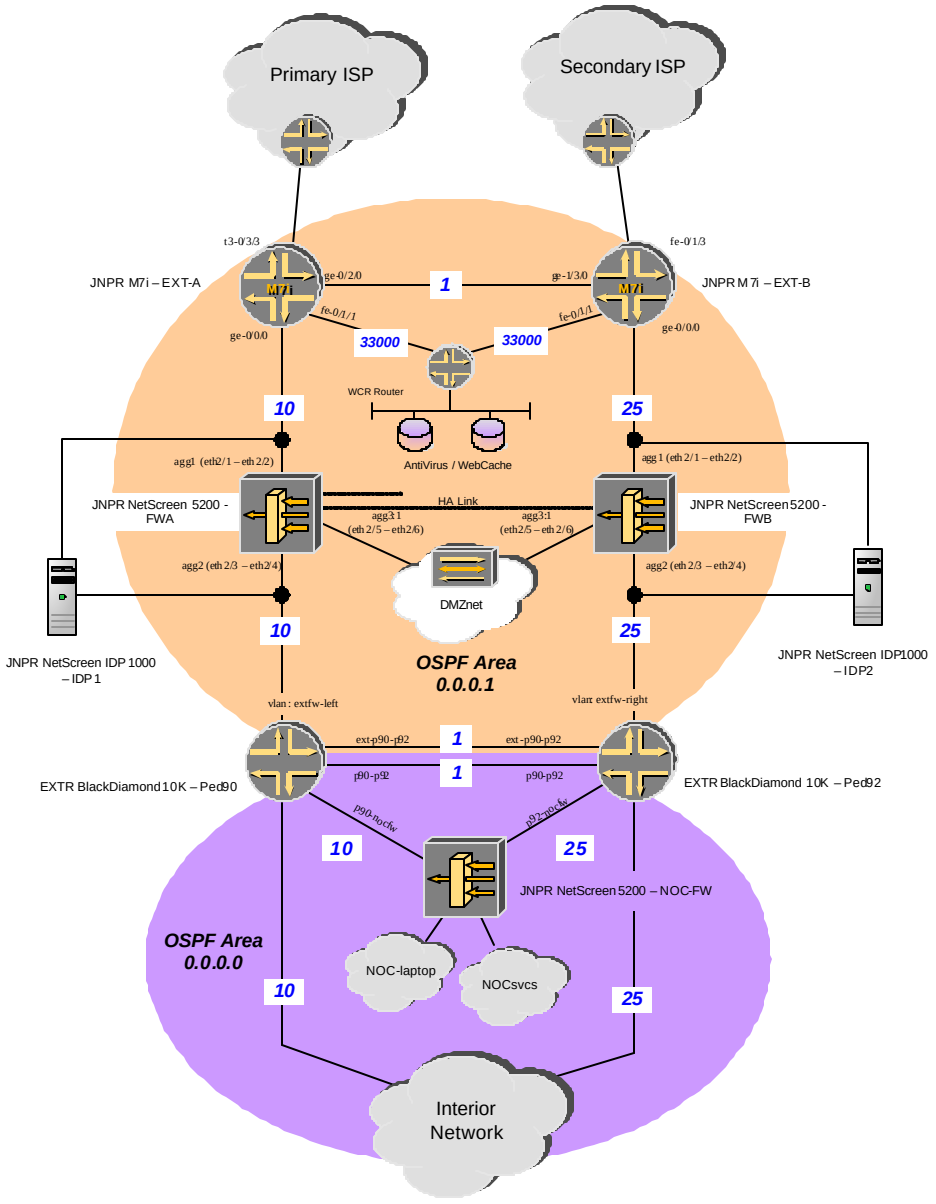
This network endured more attack traffic than a typical central site edge would ever endure, because it advertised such a large address range. Despite the resulting barrage of attacks over a two-week period, we obtained 100% uptime. This was due to the perimeter design, the performance and integrity of the Juniper Networks routers and firewalls, and the triage method of attack detection and prevention, which is especially effective with the product set used in the n etwork.

Appendix A: Annotated Configurations

Here's the network diagram with annotated interfaces and addresses.

Copyright © 2005, Juniper Networks, Inc.

Figure 16: Network Diagram with Annotated Interfaces/Addresses



Annotated configuration snippets follow.

EXT-A-M7i

```
version 7.1R1.3;
system {
```

Copyright © 2005, Juniper Networks, Inc.

```
    host-name EXTA-M7i;
    domain-name networkops.net;
    time-zone America/Los_Angeles;
    name-server {
        45.0.12.20;
    }
    radius-server {
        45.0.12.30 {
            secret "$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$"; ## SECRET-DATA
            source-address 192.16.170.101;
        }
    }
    services {
        ssh;
    }
    ntp {
        server 45.128.12.20 prefer;
        server 199.45.1.20;
        server 45.128.12.10 prefer;
    }
}
interfaces {
    ge-0/0/0 {
        description "Link to FWA";
        unit 0 {
            family inet {
                filter {
                    /* Filter-based forwarding for BlueCoat Web Proxy */
                    input webcache-dest80;
                }
                address 192.16.170.5/30;
            }
        }
    }
    fe-0/1/1 {
        description "Link to BlueCoat WCR";
        unit 0 {
            family inet {
                address 192.16.170.33/30;
            }
        }
    }
    ge-0/2/0 {
        description "Cross-link to EXT-B";
        unit 0 {
            family inet {
                address 192.16.170.1/30;
            }
        }
    }
    t3-0/3/3 {
        description "DS3 to ISP-A";
        clocking external;
```

Copyright © 2005, Juniper Networks, Inc.

```
        encapsulation ppp;
        t3-options {
            /* scambling added for optical DS3 extension */
            compatibility-mode digital-link;
            payload-scrambler;
            bert-period 90;
        }
        unit 0 {
            family inet {
                filter {
                    /* firewall filter to control ingress traffic
                       - known worm ports and address verification */
                    input screen;
                    /* verify outbound traffic source address */
                    output addrcheck;
                }
                address 192.16.170.81/30;
            }
        }
    }
    fxp0 {
        unit 0 {
            family inet {
                address 45.2.98.101/16;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    /* firewall filter to protect routing engine */
                    input re-protect;
                }
                address 192.16.170.101/32;
                address 45.127.0.1/32;
            }
        }
    }
}
snmp {
    location "NOC External-B";
    contact "Dan Backman: 702-xxx-xxxx";
    community secret1 {
        authorization read-write;
    }
    community secret2 {
        authorization read-only;
    }
}
routing-options {
    interface-routes {
        /* populate all interface routes into this RIB-group */
```

Copyright © 2005, Juniper Networks, Inc.

```
        rib-group inet allunicast;
    }
    /* static route for failover to external B router */
    static {
        route 0.0.0.0/0 next-hop 192.16.170.2;
    }
    aggregate {
        /* aggregate route for external array addresses */
        route 192.16.170.0/24 {
            community [ 290:100 290:200 290:500 ];
            as-path {
                origin incomplete;
            }
            passive;
        }
    rib-groups {
        /* populate unicast routes into inet.2 for multicast RPF */
        unicast-multicast {
            import-rib [ inet.0 inet.2 ];
        }
        /* populate interface routes into wcr routing instance */
        allunicast {
            import-rib [ inet.0 wcr.inet.0 ];
        }
    }
    router-id 192.16.170.101;
    autonomous-system 290;
}
protocols {
    bgp {
        group internal {
            type internal;
            local-address 192.16.170.101;
            family inet {
                unicast;
                multicast;
            }
            peer-as 290;
            neighbor 192.16.170.102;
        }
        group isp-a-net {
            type external;
            import isp-a-net-in;
            family inet {
                unicast;
                multicast;
            }
            export isp-a-net-out;
            remove-private;
            peer-as 35937;
            neighbor 192.16.170.82;
        }
        /* eBGP feed for Network Physics */
```

Copyright © 2005, Juniper Networks, Inc.

```
        group netphy1 {
            local-address 192.16.170.101;
            import denyAll;
            peer-as 65501;
            neighbor 192.16.170.161 {
                multihop {
                    ttl 3;
                }
            }
        }
        /* eBGP feed for Network Physics */
        group netphy2 {
            local-address 192.16.170.101;
            import denyall;
            peer-as 65502;
            neighbor 192.16.170.162 {
                multihop {
                    ttl 3;
                }
            }
        }
    }
    msdp {
        local-address 192.16.170.81;
        peer 192.16.170.82;
    }
    ospf {
        /* populate both inet.0 and inet.2 */
        rib-group unicast-multicast;
        export default-originate;
        area 0.0.0.1 {
            interface lo0.0 {
                passive;
                metric 10;
            }
            interface gr-1/2/0.0 {
                passive;
                metric 10;
            }
            interface ge-0/0/0.0 {
                interface-type p2p;
                metric 10;
            }
            interface fe-1/3/0.0 {
                passive;
                metric 10;
            }
            interface fxp0.0 {
                disable;
            }
            interface t3-0/3/3.0 {
                passive;
                metric 10;
```

Copyright © 2005, Juniper Networks, Inc.

```
            }
            interface fe-0/1/1.0 {
                interface-type p2p;
                metric 33000;
            }
            interface fe-0/1/3.0 {
                passive;
                metric 10;
            }
            interface fe-0/1/2.0;
            interface ge-0/2/0.0 {
                interface-type p2p;
                metric 1;
            }
        }
    }
    pim {
        rp {
            bootstrap-priority 100;
            bootstrap-import bsr-import-filter;
            bootstrap-export bsr-export-filter;
            local {
                address 192.16.170.101;
                priority 200;
                group-ranges {
                    224.0.0.0/4;
                }
            }
        }
        interface lo0.0;
        interface ge-0/0/0.0;
        interface ge-0/1/0.0;
    }
}
policy-options {
    policy-statement default-originate {
        from {
            route-filter 0.0.0.0/0 exact;
        }
        then {
            next-hop self;
            external {
                type 1;
            }
            accept;
        }
    }
    policy-statement isp-a-net-out {
        term term1 {
            from {
                route-filter 45.0.0.0/8 exact;
                route-filter 192.16.170.0/24 exact;
            }
```

Copyright © 2005, Juniper Networks, Inc.

```
            then {
                metric 50;
                origin incomplete;
                accept;
            }
        }
        term term2 {
            then reject;
        }
    }
    policy-statement bsr-import-filter {
        from interface [ gr-1/2/0.0 fe-1/3/0.0 ];
        then reject;
    }
    policy-statement bsr-export-filter {
        from interface [ gr-1/2/0.0 ge-0/0/0.2000 ge-0/0/0.2001 ];
        then reject;
    }
    policy-statement denyAll {
        then reject;
    }
    policy-statement isp-a-net-in {
        term term1 {
            from {
                protocol bgp;
                route-filter 0.0.0.0/0 exact;
            }
            then reject;
        }
        term term-def {
            then accept;
        }
    }
    community internal1 members 290:200;
    community internal2 members 290:300;
    community transit1000 members 290:500;
}
firewall {
    /* Filter-based forwarding for BlueCoat Web Proxy */
    filter webcache-dest80 {
        term exception {
            from {
                source-address {
                    45.128.0.0/9;
                }
            }
            then accept;
        }
        term redirect {
            from {
                protocol tcp;
                destination-port 80;
            }
```

Copyright © 2005, Juniper Networks, Inc.

```
            then routing-instance wcr;
        }
        term default {
            then accept;
        }
    }
    /* Filters for address verification and screening deleted for brevity */
}

routing-instances {
    /* web-cache redirect instance – forward to BlueCoat proxy */
    wcr {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 {
                    next-hop 192.16.170.34;
                    qualified-next-hop 192.16.170.2 {
                        metric 25;
                    }
                    metric 10;
                }
            }
        }
    }
}
```

EXT-B-M7i

```
version 7.1R1.3;
system {
    host-name EXTB-M7i;
    time-zone America/Los_Angeles;
    name-server {
        45.0.12.20;
    }
    radius-server {
        45.0.12.30 {
            secret "$$$$$$$$$$$$$$$$$$$$$$$$$$"; ## SECRET-DATA
            source-address 192.16.170.102;
        }
    }
    services {
        ssh;
    }
    ntp {
        server 45.128.12.20 prefer;
        server 199.45.1.20;
        server 45.128.12.10 prefer;
    }
```

Copyright © 2005, Juniper Networks, Inc.

```
}
interfaces {
    ge-0/0/0 {
        description "Link to FWB";
        unit 0 {
            family inet {
                filter {
                    input webcache-dest80;
                }
                address 192.16.170.21/30;
            }
        }
    }
    fe-0/1/1 {
        description "Link to BlueCoat WCR";
        unit 0 {
            family inet {
                address 192.16.170.37/30;
            }
        }
    }
    fe-0/1/3 {
        description "FastE to ISP-B";
        link-mode full-duplex;
        unit 0 {
            family inet {
                filter {
                    input screen;
                    output addrcheck;
                }
                address 68.110.32.14/29;
            }
        }
    }
    ge-1/3/0 {
        description "Cross-link to EXT-A";
        unit 0 {
            family inet {
                address 192.16.170.2/30;
            }
        }
    }
    fxp0 {
        unit 0 {
            family inet {
                address 45.2.98.102/16;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
```

Copyright © 2005, Juniper Networks, Inc.

```
                    input re-protect;
                }
                address 127.0.0.1/32;
                address 192.16.170.102/32;
            }
        }
    }
}
snmp {
    location "NOC External-B";
    contact "NOC staff: 702-xxx-xxxx";
    community secret1 {
        authorization read-write;
    }
    community secret2 {
        authorization read-only;
    }
}
routing-options {
    interface-routes {
        rib-group inet allunicast;
    }
    static {
        route 0.0.0.0/0 next-hop 68.110.32.9;
    }
    aggregate {
        route 192.16.170.0/24 {
            community [ 290:100 290:200 290:500 ];
            as-path {
                origin incomplete;
            }
            passive;
        }
        route 45.0.0.0/8 {
            community [ 290:100 290:200 290:500 ];
            passive;
        }
    }
    rib-groups {
        unicast-multicast {
            export-rib inet.2;
            import-rib [ inet.0 inet.2 ];
        }
        allunicast {
            import-rib [ inet.0 wcr.inet.0 ];
        }
    }
    router-id 192.16.170.102;
    autonomous-system 290;
}
protocols {
    bgp {
        /* no eBGP peering with ISP-B due to site restrictions */
```

Copyright © 2005, Juniper Networks, Inc.

```
        group internal {
            type internal;
            local-address 192.16.170.102;
            family inet {
                unicast;
                multicast;
            }
            peer-as 290;
            neighbor 192.16.170.101;
        }
        group netphy1 {
            local-address 192.16.170.102;
            import defaultdeny;
            peer-as 65501;
            neighbor 192.16.170.161 {
                multihop {
                    ttl 3;
                }
            }
        }
        group netphy2 {
            local-address 192.16.170.102;
            import defaultdeny;
            peer-as 65502;
            neighbor 192.16.170.162 {
                multihop {
                    ttl 3;
                }
            }
        }
    }
    msdp {
        local-address 192.16.170.102;
        peer 192.16.170.100;
    }
    ospf {
        rib-group unicast-multicast;
        export default-originate;
        area 0.0.0.1 {
            interface lo0.0 {
                passive;
                metric 10;
            }
            interface ge-0/0/0.0 {
                interface-type p2p;
                metric 25;
            }
            interface ge-1/3/0.0 {
                interface-type p2p;
                metric 1;
            }
            interface fxp0.0 {
                disable;
```

Copyright © 2005, Juniper Networks, Inc.

```
            }
            interface gr-1/2/0.0 {
                passive;
            }
            interface t3-0/3/1.0 {
                interface-type p2p;
                metric 2;
            }
            interface fe-0/1/1.0 {
                interface-type p2p;
                metric 33005;
            }
            interface fe-0/1/3.0 {
                passive;
                metric 10;
            }
        }
    }
    pim {
        rp {
            bootstrap-priority 50;
            bootstrap-import bsr-import-filter;
            bootstrap-export bsr-export-filter;
            local {
                address 192.16.170.102;
                priority 100;
                group-ranges {
                    224.0.0.0/4;
                }
            }
        }
        interface lo0.0;
        interface gr-1/2/0.0;
        interface ge-0/0/0.0;
        interface ge-1/3/0.0 {
            disable;
        }
    }
}
policy-options {
    policy-statement default-originate {
        from {
            route-filter 0.0.0.0/0 exact;
        }
        then {
            next-hop self;
            external {
                type 1;
            }
            accept;
        }
    }
    policy-statement bsr-import-filter {
```

Copyright © 2005, Juniper Networks, Inc.

```
        from interface [ gr-1/2/0.0 fe-0/1/0.0 ];
        then reject;
    }
    policy-statement bsr-export-filter {
        from interface [ gr-1/2/0.0 fe-0/1/0.0 ];
        then reject;
    }
    policy-statement defaultdeny {
        then reject;
    }
    community eNet members 290:200;
    community iLabs members 290:300;
    community transit1000 members 290:500;
}
firewall {
    filter webcache-dest80 {
        term redirect {
            from {
                protocol tcp;
                destination-port 80;
            }
            then routing-instance wcr;
        }
        term default {
            then accept;
        }
    }
/* filters for re-protect, screening, and address checking removed for brevity */
}
routing-instances {
    wcr {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 {
                    next-hop 192.16.170.38;
                    qualified-next-hop 192.16.170.1 {
                        metric 25;
                    }
                    metric 10;
                }
            }
        }
    }
}
```

Set Display of JUNOS Firewall Filters

```
set firewall filter screen term tcp137 from protocol 6
set firewall filter screen term tcp137 from destination-port 137
set firewall filter screen term tcp137 then count tcp137
```

Copyright © 2005, Juniper Networks, Inc.

```
set firewall filter screen term tcp137 then discard
set firewall filter screen term tcp139 from protocol 6
set firewall filter screen term tcp139 from destination-port 139
set firewall filter screen term tcp139 then count tcp139
set firewall filter screen term tcp139 then discard
set firewall filter screen term tcp445 from protocol 6
set firewall filter screen term tcp445 from destination-port 445
set firewall filter screen term tcp445 then count tcp445
set firewall filter screen term tcp445 then discard
set firewall filter screen term tcp135 from protocol 6
set firewall filter screen term tcp135 from destination-port 135
set firewall filter screen term tcp135 then count tcp135
set firewall filter screen term tcp135 then discard
set firewall filter screen term udp137 from protocol 17
set firewall filter screen term udp137 from destination-port 137
set firewall filter screen term udp137 then count udp137
set firewall filter screen term udp137 then discard
set firewall filter screen term udp139 from protocol 17
set firewall filter screen term udp139 from destination-port 139
set firewall filter screen term udp139 then count udp139
set firewall filter screen term udp139 then discard
set firewall filter screen term tcp1433 from protocol 6
set firewall filter screen term tcp1433 from destination-port 1433
set firewall filter screen term tcp1433 then count tcp1433
set firewall filter screen term tcp1433 then discard
set firewall filter screen term tcp5554 from protocol 6
set firewall filter screen term tcp5554 from destination-port 5554
set firewall filter screen term tcp5554 then count tcp5554
set firewall filter screen term tcp5554 then discard
set firewall filter screen term tcp9898 from protocol 6
set firewall filter screen term tcp9898 from destination-port 9898
set firewall filter screen term tcp9898 then count tcp9898
set firewall filter screen term tcp9898 then discard
set firewall filter screen term udp135 from protocol 17
set firewall filter screen term udp135 from destination-port 135
set firewall filter screen term udp135 then count udp135
set firewall filter screen term udp135 then discard
set firewall filter screen term udp1433 from protocol 17
set firewall filter screen term udp1433 from destination-port 1433
set firewall filter screen term udp1433 then count udp1433
set firewall filter screen term udp1433 then discard
set firewall filter screen term udp1434 from protocol 17
set firewall filter screen term udp1434 from destination-port 1434
set firewall filter screen term udp1434 then count udp1434
set firewall filter screen term udp1434 then discard
set firewall filter screen term tcp1023 from protocol 6
set firewall filter screen term tcp1023 from destination-port 1023
set firewall filter screen term tcp1023 then count tcp1023
set firewall filter screen term tcp1023 then discard
set firewall filter screen term addrchk from source-address 192.16.170.0/24
set firewall filter screen term addrchk from source-address 192.16.170.82/32
except
set firewall filter screen term addrchk from source-address 45.0.0.0/9
```

Copyright © 2005, Juniper Networks, Inc.

```
set firewall filter screen term addrchk then count IPspoof
set firewall filter screen term addrchk then accept
set firewall filter screen term scanboy from source-address 200.27.144.33/32
set firewall filter screen term scanboy then count scanIP
set firewall filter screen term scanboy then discard
set firewall filter screen term def then count default-accept
set firewall filter screen term def then accept
set firewall filter addrcheck term term1 from source-address 45.0.0.0/9
set firewall filter addrcheck term term1 then count eNet
set firewall filter addrcheck term term1 then accept
set firewall filter addrcheck term term1a from source-address 45.128.0.0/9
set firewall filter addrcheck term term1a then count iLabs
set firewall filter addrcheck term term1a then accept
set firewall filter addrcheck term term1b from source-address 192.16.170.40/29
set firewall filter addrcheck term term1b then count BlueCoat
set firewall filter addrcheck term term1b then accept
set firewall filter addrcheck term term1c from source-address 192.16.170.0/24
set firewall filter addrcheck term term1c from source-address 192.16.170.40/29
except
set firewall filter addrcheck term term1c then count ext-array
set firewall filter addrcheck term term1c then accept
set firewall filter addrcheck term term2 from source-address 10.0.0.0/8
set firewall filter addrcheck term term2 then count net10
set firewall filter addrcheck term term2 then accept
set firewall filter addrcheck term term3 from source-address 172.16.0.0/12
set firewall filter addrcheck term term3 then count net172-16
set firewall filter addrcheck term term3 then accept
set firewall filter addrcheck term term4 from source-address 192.168.0.0/16
set firewall filter addrcheck term term4 then count net192-168
set firewall filter addrcheck term term4 then accept
set firewall filter addrcheck term term5 from source-address 68.110.32.14/32
set firewall filter addrcheck term term5 then count ExtB-peering-IP
set firewall filter addrcheck term term5 then accept
set firewall filter addrcheck term other then count other
set firewall filter addrcheck term other then accept
set firewall filter re-protect term term1 from source-address 0.0.0.0/0
set firewall filter re-protect term term1 from source-address 45.0.0.0/24 except
set firewall filter re-protect term term1 from source-address 45.2.0.0/16 except
set firewall filter re-protect term term1 from source-address 45.0.12.0/24 except
set firewall filter re-protect term term1 from protocol 6
set firewall filter re-protect term term1 from destination-port 22
set firewall filter re-protect term term1 then count control-ssh
set firewall filter re-protect term term1 then discard
set firewall filter re-protect term term2 from source-address 0.0.0.0/0
set firewall filter re-protect term term2 from source-address 192.16.170.0/24
except
set firewall filter re-protect term term2 from protocol 6
set firewall filter re-protect term term2 from destination-port bgp
set firewall filter re-protect term term2 then count control-bgp
set firewall filter re-protect term term2 then discard
set firewall filter re-protect term term3 from source-address 0.0.0.0/0
set firewall filter re-protect term term3 from source-address 45.0.0.0/16 except
set firewall filter re-protect term term3 from source-address 45.2.0.0/16 except
```

Copyright © 2005, Juniper Networks, Inc.

```
set firewall filter re-protect term term3 from source-address 45.128.12.32/32
except
set firewall filter re-protect term term3 from protocol udp
set firewall filter re-protect term term3 from destination-port snmp
set firewall filter re-protect term term3 from destination-port snmptrap
set firewall filter re-protect term term3 then count manage-snmp
set firewall filter re-protect term term3 then discard
set firewall filter re-protect term term4 from source-address 0.0.0.0/0
set firewall filter re-protect term term4 from source-address 45.0.12.0/24 except
set firewall filter re-protect term term4 from protocol udp
set firewall filter re-protect term term4 from destination-port radius
set firewall filter re-protect term term4 from destination-port radacct
set firewall filter re-protect term term4 then count manage-radius
set firewall filter re-protect term term4 then discard
set firewall filter re-protect term default then accept
```

FW-A-NS5200

```
set hostname FW-A

# assign all zones to trust-vr (default behavior in ScreenOS)
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"

# assign interfaces to the appropriate zone
set interface "ethernet2/5" zone "DMZ"
set interface "aggregate1" zone "Untrust"
set interface "aggregate2" zone "Trust"
set interface "loopback.1" zone "Trust"

# configure aggregate interfaces
set interface ethernet2/1 aggregate aggregate1
set interface ethernet2/2 aggregate aggregate1
set interface ethernet2/3 aggregate aggregate2
set interface ethernet2/4 aggregate aggregate2

# configure IP addressing
set interface mgt ip 45.2.94.103/16
set interface ethernet2/5:1 ip 192.16.170.129/25
set interface ethernet2/5:1 route
set interface aggregate1 ip 192.16.170.6/30
set interface aggregate1 route
set interface aggregate2 ip 192.16.170.9/30
set interface aggregate2 route
set interface loopback.1 ip 192.16.170.103/32
set interface loopback.1 route

# enable management access (includes ping)
set interface ethernet2/5:1 ip manageable
set interface aggregate1 ip manageable
```

Copyright © 2005, Juniper Networks, Inc.

```
set interface aggregate2 ip manageable
set interface loopback.1 ip manageable
set interface aggregate1 manage ping


# define Screening values and thresholds for trust and untrust zones
# note: screening important for both inbound and outbound traffic
set zone "Trust" screen icmp-flood
set zone "Trust" screen udp-flood
set zone "Trust" screen winnuke
set zone "Trust" screen port-scan
set zone "Trust" screen ip-sweep
set zone "Trust" screen tear-drop
set zone "Trust" screen syn-flood
set zone "Trust" screen ip-spoofing
set zone "Trust" screen ping-death
set zone "Trust" screen ip-filter-src
set zone "Trust" screen land
set zone "Trust" screen syn-frag
set zone "Trust" screen tcp-no-flag
set zone "Trust" screen unknown-protocol
set zone "Trust" screen ip-bad-option
set zone "Trust" screen ip-record-route
set zone "Trust" screen ip-timestamp-opt
set zone "Trust" screen ip-security-opt
set zone "Trust" screen ip-loose-src-route
set zone "Trust" screen ip-strict-src-route
set zone "Trust" screen ip-stream-opt
set zone "Trust" screen syn-fin
set zone "Trust" screen fin-no-ack
set zone "Trust" screen limit-session source-ip-based
set zone "Trust" screen limit-session destination-ip-based
set zone "Trust" screen ip-spoofing drop-no-rpf-route
set zone "Untrust" screen icmp-flood
set zone "Untrust" screen udp-flood
set zone "Untrust" screen winnuke
set zone "Untrust" screen port-scan
set zone "Untrust" screen ip-sweep
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "Untrust" screen syn-frag
set zone "Untrust" screen tcp-no-flag
set zone "Untrust" screen unknown-protocol
set zone "Untrust" screen ip-bad-option
set zone "Untrust" screen ip-record-route
set zone "Untrust" screen ip-timestamp-opt
set zone "Untrust" screen ip-security-opt
set zone "Untrust" screen ip-loose-src-route
set zone "Untrust" screen ip-strict-src-route
set zone "Untrust" screen ip-stream-opt
```

Copyright © 2005, Juniper Networks, Inc.

```
set zone "Untrust" screen syn-fin
set zone "Untrust" screen fin-no-ack
set zone "Untrust" screen limit-session source-ip-based
set zone "Untrust" screen limit-session destination-ip-based

set zone "Trust" screen icmp-flood threshold 200
set zone "Untrust" screen icmp-flood threshold 100
set zone "Trust" screen ip-sweep threshold 100000
set zone "Untrust" screen ip-sweep threshold 100000
set zone "Trust" screen port-scan threshold 100000
set zone "Untrust" screen port-scan threshold 100000
set zone "Trust" screen udp-flood threshold 5000
set zone "Untrust" screen udp-flood threshold 5000
set zone "Trust" screen limit-session source-ip-based 2000
set zone "Untrust" screen limit-session source-ip-based 2000
set zone "Trust" screen limit-session destination-ip-based 2000
set zone "Untrust" screen limit-session destination-ip-based 2000
set zone "Trust" screen syn-flood timeout 1
set zone "Trust" screen syn-flood queue-size 20000
set zone "Trust" screen syn-flood attack-threshold 1000
set zone "Trust" screen syn-flood source-threshold 100
set zone "Trust" screen syn-flood destination-threshold 500
set zone "Untrust" screen syn-flood timeout 1
set zone "Untrust" screen syn-flood queue-size 20000
set zone "Untrust" screen syn-flood attack-threshold 1000
set zone "Untrust" screen syn-flood source-threshold 100
set zone "Untrust" screen syn-flood destination-threshold 500

# enable TCP 3-way handshake (SYN) checking for all traffic
# default behavior in ScreenOS 5.1
unset flow no-tcp-seq-check
set flow tcp-syn-check

# enable NetScreen Redundancy Protocol (NSRP) for “Mixed-mode” operation
# - VSD 0 is unset allowing active/active operation for OSPF routed topology
unset nsrp vsd-group id 0
 # non-VSI mirror allows traffic SYNC for non-VSI (OSPF) transit traffic
set nsrp rto-mirror session non-vsi

# - VSD 1 used to protect directly-attached DMZ network
set nsrp cluster id 1
set nsrp rto-mirror sync
set nsrp vsd-group id 1 priority 100
set nsrp vsd-group id 1 preempt
set nsrp vsd-group id 1 preempt hold-down 5
set nsrp vsd-group id 1 monitor threshold 100
# NSRP zone monitoring links VSD 1 failover with OSPF path
set nsrp vsd-group id 1 monitor zone Trust weight 150
set nsrp vsd-group id 1 monitor zone Untrust weight 150
set nsrp vsd-group id 1 monitor zone DMZ weight 150


# define custom timeout values for frequently used services (720 minutes)
```

Copyright © 2005, Juniper Networks, Inc.

```
set service "IMAP" timeout 720
set service "imaps" protocol tcp src-port 0-65535 dst-port 993-993 timeout 720
set service "ms-sql" protocol tcp src-port 0-65535 dst-port 1433-1434
set service "SSH" timeout 720
set service "TELNET" timeout 720
set service "mst-services" protocol udp src-port 0-65535 dst-port 135-139
set service "mst-services" + tcp src-port 0-65535 dst-port 445-445
set service "mst-services" + tcp src-port 0-65535 dst-port 5554-5554
set service "mst-services" + tcp src-port 0-65535 dst-port 135-139

# disable application level gateways for VoIP protocols
# - avoid conflicts with Sip/H.323 interoperability testing
unset alg q931
unset alg h245
unset alg ras
unset alg sip

# define locally assigned address-objects and groups
# - configuration includes objects added via Netscreen Security Manager (NSM)
#   and operations staff to block known threats during network operation
set address "Trust" "ilabs-worm-user" 45.210.5.215 255.255.255.255 "TCP-455
Network Scan"
set address "Untrust" "fri-portscan-user" 220.164.140.204 255.255.255.255
"220.164.140.204"
set address "Untrust" "fri-portscan-user2" 202.103.213.83 255.255.255.255
"202.103.213.83"
set address "Untrust" "fri-synflood-user2" 61.32.216.162 255.255.255.255
"61.32.216.162"
set address "Untrust" "fri-synflood-user3" 218.98.221.35 255.255.255.255
"218.98.221.35"
set address "Untrust" "friday-synflood-user" 202.105.233.31 255.255.255.255
"202.105.233.31"
set address "Untrust" "public-scan-user" 61.167.86.98 255.255.255.255 "tcp 1433
scan"
set address "Untrust" "sat-oracle-flooduser" 24.232.211.16 255.255.255.255
set address "Untrust" "sat-portscan-user" 61.187.238.55 255.255.255.255
"61.187.238.55"
set address "Untrust" "sat-portscan-user2" 202.104.11.68 255.255.255.255 "202.104.
11. 68"
set address "Untrust" "sat-portscanuser3" 218.200.128.236 255.255.255.255
"218.200.128.236"
set address "Untrust" "sat-portscanuser4" 221.203.153.26 255.255.255.255
set address "Untrust" "sat-portscanuser5" 218.246.182.217 255.255.255.255
set address "Untrust" "sat-portscanuser6" 61.152.102.10 255.255.255.255
set address "Untrust" "sat-portscanuser7" 60.191.128.133 255.255.255.255
set address "Untrust" "sun-noc-spoofuser" 169.254.178.199 255.255.255.255
set address "Untrust" "sun-portscanuser" 218.23.50.12 255.255.255.255
set address "Untrust" "sun-portscanuser2" 220.189.243.233 255.255.255.255
set address "Untrust" "sun-sshsynflooduser" 64.221.234.218 255.255.255.255
set address "Untrust" "sun-synflooduser" 207.44.194.72 255.255.255.255
set address "Untrust" "sun-synflooduser1" 61.152.93.92 255.255.255.255
set address "Untrust" "tue-portscanuser1" 61.152.108.21 255.255.255.255
set address "Untrust" "tue-tcp-3306-scan" 64.239.152.253 255.255.255.255
set address "Untrust" "tue-tcp-scan" 61.152.93.60 255.255.255.255
```

Copyright © 2005, Juniper Networks, Inc.

```
set address "Untrust" "wed-net-scan-tcp3306" 65.96.175.230 255.255.255.255 "c-65-
96-175-230.hsd1.ma.comcast"
set address "Untrust" "wed-net-scanuser" 219.148.108.156 255.255.255.255
set address "Untrust" "wed-portscanuser2" 218.59.140.28 255.255.255.255
set address "Untrust" "wed-synflooduser" 61.129.45.113 255.255.255.255
set address "Untrust" "wed-synsweepuser2" 70.84.213.43 255.255.255.255
set address "Untrust" "wed-synsweepuser3" 211.115.111.146 255.255.255.255
set address "DMZ" "dmz-ftp" 192.16.170.181 255.255.255.255
set address "DMZ" "dmz-mail-smtp" 192.16.170.180 255.255.255.255




set group address "Trust" "Client-Watch-List"
set group address "Trust" "Client-Watch-List" add "ilabs-worm-user"
set group address "Untrust" "internet-badusers-blacklist"
set group address "Untrust" "internet-badusers-blacklist" add "fri-portscan-user"
set group address "Untrust" "internet-badusers-blacklist" add "fri-portscan-user2"
set group address "Untrust" "internet-badusers-blacklist" add "fri-synflood-user2"
set group address "Untrust" "internet-badusers-blacklist" add "fri-synflood-user3"
set group address "Untrust" "internet-badusers-blacklist" add "friday-synflood-
user"
set group address "Untrust" "internet-badusers-blacklist" add "public-scan-user"
set group address "Untrust" "internet-badusers-blacklist" add "sat-oracle-
flooduser"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscan-user"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscan-user2"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscanuser3"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscanuser4"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscanuser5"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscanuser6"
set group address "Untrust" "internet-badusers-blacklist" add "sat-portscanuser7"
set group address "Untrust" "internet-badusers-blacklist" add "sun-noc-spoofuser"
set group address "Untrust" "internet-badusers-blacklist" add "sun-portscanuser"
set group address "Untrust" "internet-badusers-blacklist" add "sun-portscanuser2"
set group address "Untrust" "internet-badusers-blacklist" add "sun-
sshsynflooduser"
set group address "Untrust" "internet-badusers-blacklist" add "sun-synflooduser"
set group address "Untrust" "internet-badusers-blacklist" add "sun-synflooduser1"
set group address "Untrust" "internet-badusers-blacklist" add "tue-portscanuser1"
set group address "Untrust" "internet-badusers-blacklist" add "tue-tcp-3306-scan"
set group address "Untrust" "internet-badusers-blacklist" add "tue-tcp-scan"
set group address "Untrust" "internet-badusers-blacklist" add "wed-net-scan-
tcp3306"
set group address "Untrust" "internet-badusers-blacklist" add "wed-net-scanuser"
set group address "Untrust" "internet-badusers-blacklist" add "wed-portscanuser2"
set group address "Untrust" "internet-badusers-blacklist" add "wed-synflooduser"
set group address "Untrust" "internet-badusers-blacklist" add "wed-synsweepuser2"
set group address "Untrust" "internet-badusers-blacklist" add "wed-synsweepuser3"
set group service "services-black-list"
set group service "services-black-list" add "ms-sql"
set group service "services-black-list" add "mst-services"

# set default inter-zone policy behavior to permit all traffic
# - firewalls primarily configured for screen protections, not policy enforcement
```

Copyright © 2005, Juniper Networks, Inc.

```
set policy default-permit-all

# site-specific policies.
# - all policies configured and maintained using Netscreen Security Manager (NSM)
set policy id 700029 from "Trust" to "Untrust"  "Client-Watch-List" "Any" "ANY"
permit log
set policy id 9 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "imaps" permit
set policy id 163560 from "Untrust" to "Trust"  "Any" "Any" "services-black-list"
deny
set policy id 3 from "Untrust" to "Untrust"  "Any" "Any" "ANY" deny
set policy id 2 from "Trust" to "DMZ"  "Any" "dmz-ftp" "FTP" permit log
set policy id 213013 from "Trust" to "DMZ"  "Any" "dmz-mail-smtp" "MAIL" permit
log
set policy id 5 from "Untrust" to "DMZ"  "internet-badusers-blacklist" "Any" "ANY"
deny
set policy id 482912 from "Untrust" to "DMZ"  "Any" "dmz-ftp" "FTP" permit log
set policy id 607913 from "Untrust" to "DMZ"  "Any" "dmz-mail-smtp" "MAIL" permit
log
set policy id 668421 from "Trust" to "DMZ"  "Any" "Any" "ANY" permit log
set policy id 970661 from "Untrust" to "DMZ"  "Any" "Any" "ANY" permit log
set policy id 399443 from "DMZ" to "Untrust"  "Any" "Any" "ANY" permit log
set policy id 4 from "Untrust" to "Trust"  "internet-badusers-blacklist" "Any"
"ANY" deny
set policy id 8 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set policy id 100091 from "DMZ" to "Trust"  "Any" "Any" "ANY" permit log

# define permissive multicast policy for PIM-SM
set multicast-group-policy from "Untrust" mgroup any to "Trust" pim-message bsr-
static-rp join-prune bi-directional

# control management access to NOC subnets
set admin manager-ip 45.0.0.0 255.255.255.0
set admin manager-ip 45.0.12.60 255.255.255.255
set admin manager-ip 192.16.170.0 255.255.255.0
set admin manager-ip 45.2.0.0 255.255.0.0

# configure management variables including self-management alarms
set alarm threshold CPU 50
set alarm threshold session percent 50

# configure NSM management access
# - note: largely autoconfigured via NSM
set nsmgmt report alarm traffic enable
set nsmgmt report alarm attack enable
set nsmgmt report alarm other enable
set nsmgmt report alarm di enable
set nsmgmt report log config enable
set nsmgmt report log info enable
set nsmgmt report log self enable
set nsmgmt report log traffic enable
set nsmgmt init id E1A4DB6A3B272F8759E510F096EFB3D8B72CD48D00
set nsmgmt server primary 45.0.12.60 port 7800
set nsmgmt bulkcli reboot-timeout 60
```

Copyright © 2005, Juniper Networks, Inc.

```
set nsmgmt hb-interval 20
set nsmgmt hb-threshold 5
set nsmgmt enable

# enable appropriate SNMP access
set snmp community "secret1" Read-Write Trap-off  version v2c
set snmp community "secret2" Read-Only Trap-off  version any
set snmp host "secret2" 45.0.12.10 255.255.255.255 trap v2
set snmp host "secret2" 45.0.12.11 255.255.255.255 trap v2
set snmp host "secret2" 45.0.0.0 255.255.255.0
unset snmp auth-trap enable
set snmp port listen 161
set snmp port trap 162

# enable SSHv2 and SCP for secure CLI and file access
set ssh version v2
set ssh enable
set scp enable

# configure NTP and DNS servers (anycast addresses)
set ntp server "45.0.12.20"
set ntp server backup1 "45.128.12.10"
set ntp max-adjustment 0
set dns host dns1 45.128.12.20

# define router ID, OSPF and PIM-SM within trust-vr
set vrouter trust-vr
  set router-id 192.16.170.103
  set protocol ospf
    set enable
    set area 0.0.0.1
  exit
    set protocol pim
    set enable
  exit
exit

# add appropriate interface config for OSPF and PIM-SM
set interface aggregate1 protocol ospf area 0.0.0.1
set interface aggregate1 protocol ospf link-type p2p
set interface aggregate1 protocol ospf enable
set interface aggregate1 protocol ospf cost 10
set interface aggregate2 protocol ospf area 0.0.0.1
set interface aggregate2 protocol ospf link-type p2p
set interface aggregate2 protocol ospf enable
set interface aggregate2 protocol ospf cost 10
set interface loopback.1 protocol ospf area 0.0.0.1
set interface loopback.1 protocol ospf enable
set interface ethernet2/5:1 protocol ospf area 0.0.0.1
set interface ethernet2/5:1 protocol ospf passive
set interface ethernet2/5:1 protocol ospf enable
set interface ethernet2/5:1 protocol ospf cost 10
set interface aggregate1 protocol pim
```

Copyright © 2005, Juniper Networks, Inc.

```
set interface aggregate1 protocol pim enable
set interface aggregate2 protocol pim
set interface aggregate2 protocol pim enable

# END
```

FW-B-NS5200

```
# truncated config shows only interface, routing protocol and NSRP config
# - all screen, policy and other management config is identical to FW-A-NS5200

set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"

set interface "ethernet2/5" zone "DMZ"
set interface "aggregate1" zone "Untrust"
set interface "aggregate2" zone "Trust"
set interface "loopback.1" zone "Trust"
set interface ethernet2/1 aggregate aggregate1
set interface ethernet2/2 aggregate aggregate1
set interface ethernet2/3 aggregate aggregate2
set interface ethernet2/4 aggregate aggregate2

set interface mgt ip 45.2.94.104/16
set interface ethernet2/5:1 ip 192.16.170.129/25
set interface ethernet2/5:1 route
set interface aggregate1 ip 192.16.170.22/30
set interface aggregate1 route
set interface aggregate2 ip 192.16.170.25/30
set interface aggregate2 route
set interface loopback.1 ip 192.16.170.104/32
set interface loopback.1 route

set nsrp cluster id 1
unset nsrp vsd-group id 0
set nsrp rto-mirror sync
set nsrp rto-mirror session non-vsi
set nsrp vsd-group id 1 priority 200
set nsrp vsd-group id 1 preempt
set nsrp vsd-group id 1 preempt hold-down 5
set nsrp vsd-group id 1 monitor threshold 100
set nsrp vsd-group id 1 monitor zone Trust weight 150
set nsrp vsd-group id 1 monitor zone Untrust weight 150
set nsrp vsd-group id 1 monitor zone DMZ weight 150

set vrouter trust-vr
  set router-id 192.16.170.103
  set protocol ospf
    set enable
    set area 0.0.0.1
```

Copyright © 2005, Juniper Networks, Inc.

```
  exit
    set protocol pim
    set enable
  exit
exit

set interface aggregate1 protocol ospf area 0.0.0.1
set interface aggregate1 protocol ospf link-type p2p
set interface aggregate1 protocol ospf enable
set interface aggregate1 protocol ospf cost 10
set interface aggregate2 protocol ospf area 0.0.0.1
set interface aggregate2 protocol ospf link-type p2p
set interface aggregate2 protocol ospf enable
set interface aggregate2 protocol ospf cost 10
set interface loopback.1 protocol ospf area 0.0.0.1
set interface loopback.1 protocol ospf enable
set interface ethernet2/5:1 protocol ospf area 0.0.0.1
set interface ethernet2/5:1 protocol ospf passive
set interface ethernet2/5:1 protocol ospf enable
set interface ethernet2/5:1 protocol ospf cost 10
set interface aggregate1 protocol pim
set interface aggregate1 protocol pim enable
set interface aggregate2 protocol pim
set interface aggregate2 protocol pim enable
# END
```

Copyright © 2005, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.