APPLICATION NOTE

SECURING AND HARDENING NSM USING IPTABLES

Table of Contents

Introduction

Network managements systems need access to all of the network devices they manage or monitor. Since different network devices use different methodologies to be managed, network management systems typically have unrestricted access, making them a prime target for malicious hackers and their protection a vital security requirement.

Juniper Networks® Network and Security Manager provides a single point of control for managing Juniper's network infrastructure of routing, switching, and security devices. NSM provides centralized, end-to-end life cycle management and granular policy configuration. It also includes comprehensive monitoring, reporting, and investigative tools that allow users to improve IT management and cost efficiencies and maximize network security.

The UNIX kernel doesn't get hardened when NSM is installed. This means that the UNIX box can accept connections on any port (provided there is any application listening to it). This vulnerability can be exploited and further elevated to scan and map the complete network. Tools like netcat or a malicious script can be programmed to listen on unused port(s) and use these as a covert channel into the network. Modified and recompiled UNIX tools (i.e. rootkits) such as ps, netstat, and passwd are available that can hide any trace of an intruder's presence or existence. These can be exploited to monitor traffic, create back doors, alter log files, change the configuration of managed devices, bring the network down or attack individual machines on the network. An effective way of mitigating these risks involves the closing of all unused ports.

The iptables utility controls the network packet filtering. It is a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores. It has a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

For these reasons, it is always a good idea to have a decent iptables configuration in place on any given machine, regardless of the outside firewalls you may be using.

Scope

This application note will help security architects, consultants, managers, and administrators to harden Juniper Networks Network and Security Manager using iptables, without affecting NSM's functionality. It also explains some of the best practices that can be used to mitigate the vulnerabilities of open ports in UNIX on which NSM is built and deployed.

Design Considerations

Keeping the unused ports open in NSM introduces risk, as traffic on an unused port doesn't belong to NSM and, as such, is unmanaged. Table 1 shows some of the best known trojans and the ports that they use.

Table 1: Well-Known Trojans with Protocols and Ports

Trojan	Protocol	Port
Back Orifice	UDP	31337, 31338
Deep Throat	UDP	2140, 3150
NetBus	TCP	12345, 12346
Whack-a-mole	TCP	12361, 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423, 40426

Known or future trojans can use unused open ports to create a backdoor channel which can go undetected unless you have an external mechanism to monitor this traffic. As we have already noted, Network and Security Manager requires access to all network devices, but keeping all unused ports open decreases network security. Even on the NSM appliance, the generic iptables firewall rules apply only to the incoming traffic and are turned off by default. For these reasons, hardening the box is a good idea regardless of the outside firewalls that you deploy.

Table 2 shows the ports that are required for NSM functionality.

Table 2: Required Inbound NSM Ports and Functionality

Port	Protocol	Purpose
22	TCP	• To access the box using secure shell (SSH) from the administrator's network. • To resynchronize (rsync) for high availability (HA).
162	UDP	• To listen for SNMP traps and informs.
443	TCP	• Web interface in Juniper Networks NSMXpress.
5432	TCP	• For the STRM Series device to connect to the PostgreSQL to get profiler data.
7800	TCP	• ScreenOS Software firewalls connect on this port.
7801	TCP	• Device server connects on this port. • GUI clients prior to 2008.2 versions use this port.
7802	UDP	• In HA, the heartbeats are sent to the peer on this port.
7803	TCP	• IDP Series sensors connect on this port.
7804	TCP	• IC Series, SA Series, devices running Junos OS, and EX Series devices connect on this port.
7808	TCP	• GUI clients (from 2008.2 onwards) connect on this port.
8443	TCP	• Optional, used to download GUI client from the NSM server.

Table 3: Required Outbound NSM Ports and Functionality

Port	Protocol	Purpose
21	FTP	• To upload the tech-support output to Juniper FTP for technical support.
22	TCP	• When IP reachable option is used, the NSM server uses this for sending the commands to the device via SSH (a one time connection).
23	TCP	• When IP reachable option is used, the NSM server uses this for sending the commands to the device via Telnet (a one time connection).
25	TCP	• For SMTP client to connect to its server if configured to send alerts via email.
53	UDP	• For Domain Name System (DNS) client to resolve the address during an attack database download.
123	UDP	• To connect to Network Time Protocol (NTP) server.
161	UDP	• SNMP
443	TCP	• To download the attack database and Device Management Interface (DMI) schema.
514	UDP	• To send system logs (syslog) if configured.
1645	UDP	• RADIUS server authentication port.
1646	UDP	• RADIUS server accounting port.
7801	TCP	• To be used if it's a device server only (e.g., extended HA).
9020	UDP	• Integrated surf control for Web filtering.

Table 4: Required Inter-Process NSM Ports and Functionality

Port	Protocol	Purpose
5005	TCP	• Virtual Machine
5432	TCP	• PostgreSQL communication
6991	TCP	• Xvfb: To schedule reports using graphics library for font, etc.

Description and Deployment Scenario

Let's discuss how we can harden the kernel of Network and Security Manager for incoming and outgoing traffic, to provide only the required access without affecting NSM's functionality.

Prerequisite

Iptables gets installed along with the default installation of Linux. If you don't find iptables installed on your box, you can install it from the rpm available with the Linux CD. You can also download it from this link: **www.netfilter.org/projects/iptables/downloads.html**. Please refer to page 12 for instructions related to installation/upgrade to the current version.

The commands listed below were tested on iptables v1.3.5.

Methodology Used for Hardening the NSM Box

The most commonly used rules are listed first and should be placed on the top in the rule-base to avoid unwanted lookup against other rules and for faster processing. Not all rules are required; you only need to use those that are required in your setup. Rules 1-5, 12, 24, 27, 29-32 are less likely to change; the remaining rules can be customized based on your setup and IP addressing.

- eth0 is considered here as the ingress/egress interface (modify it if required).
- With the option "-s" (source) and "-d" (destination), either the "device ip" or the "network/mask" can be provided.

The files of interest on the NSM box are:

/etc/sysconfig/iptables-config Iptables controls

/etc/sysconfig/iptables The place where rules are stored

Let's discuss how to implement NSM hardening with different types of installations.

A) For a Standalone (Single Server) Installation

1) Drop xmas and null packets

```
/sbin/iptables -A INPUT -p tcp --tcp-flags ALL ALL -j LOG --log-prefix "XMAS_
PACKET: "
/sbin/iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
/sbin/iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG --log-prefix "NULL_
PACKET: "
/sbin/iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

2) Prevent SYN flood attacks

```
/sbin/iptables -N syn_flood
/sbin/iptables -A INPUT -p tcp --syn -j syn_flood
/sbin/iptables -A syn_flood -m limit --limit 10/s --limit-burst 30 -j RETURN
/sbin/iptables -A syn_flood -j LOG --log-prefix "SYN_FLOOD: "
/sbin/iptables -A syn_flood -j DROP
```

- All incoming connections are allowed until limit is reached:
- Limit 10/s: Maximum average matching rate in seconds
- Limit-burst 30: Maximum initial number of packets to match

3) Allow return sessions

```
/sbin/iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT
```

4) Allow inter-process communications (this rule can be avoided with individual ones, however, it is a preferred rule, as the underlying UNIX kernel, depending on the version, relies on this for rpc and other processes)

```
/sbin/iptables -A INPUT -d 127.0.0.1 -j ACCEPT
/sbin/iptables -A OUTPUT -d 127.0.0.1 -j ACCEPT
```

5) Restrict PostgreSQL access

```
/sbin/iptables -A OUTPUT -p tcp -m tcp --dport 5432 -m owner ! --uid-owner nsm -j
LOG --log-prefix "PGSQL_NOT_NSM_USER: "
/sbin/iptables -A OUTPUT -p tcp -m tcp --dport 5432 -m owner ! --uid-owner nsm -j
DROP
```

6) 7801/TCP: Device server use this port to connect to the GUI server

```
/sbin/iptables -A INPUT -s <nsm_ip> -d <nsm_ip> -p tcp -m tcp --dport 7801 -j
ACCEPT
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <nsm_ip> -p tcp -m tcp --dport 7801 -j
ACCEPT
```

7) 7801/TCP/IN: Prior to NSM version 2008.2, GUI clients use this port to connect to the server

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
7801 -j ACCEPT
```

8) 7800/TCP/IN: To manage firewalls running Juniper Networks ScreenOS® Software

```
/sbin/iptables -A INPUT -s <fw_ip> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport 7800
-j ACCEPT
```

9) 7803/TCP/IN: To manage Juniper Networks IDP Series Intrusion Detection and Prevention Appliances sensors

```
/sbin/iptables -A INPUT -s <idp_ip> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
7803 -j ACCEPT
```

10) 7804/TCP/IN: To manage Juniper Networks IC Series Unified Access Control Appliances, Juniper Networks SA Series SSL VPN Appliances, Juniper Networks Junos® operating system, and Juniper Networks EX Series Ethernet Switches

```
/sbin/iptables -A INPUT -s <device_ip> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
7804 -j ACCEPT
```

11) 7808/TCP/IN: From NSM version 2008.2 onwards, GUI clients use this port to connect to the server

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
7808 -j ACCEPT
```

12) Protect against brute force entry attacks

```
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW -m recent
--set --name SSH
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW -m recent
--update --seconds 60 --hitcount 8 --rttl --name SSH -j LOG --log-prefix "BRUTE_
FORCE: "
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW -m recent
--update --seconds 60 --hitcount 8 --rttl --name SSH -j DROP
```

- Together, these will rate-limit all incoming SSH connections to eight in a one minute window.
- Normal users will have no trouble logging in, but brute force attacks will be dropped by limiting the number of possible account combinations from unlimited to eight.

13) 22/TCP/IN: To connect to NSM via SSH (an important step to prevent losing access to the box)

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
22 -j ACCEPT
```

14) 22/TCP/OUT: To add devices to NSM via SSH. The NSM server uses this to send commands to a device via SSH (a onetime connection). We recommend disabling this rule after the device has been added, and saving the table with a name like "iptables-with-ssh" (refer to steps 33 and 34 below) so that it can be reinstated when required.

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <managed_device> -o eth0 -p tcp -m tcp
--dport 22 -j ACCEPT
```

15) 23/TCP/OUT: To add devices to NSM via Telnet, The NSM server uses this port to send commands to a device via SSH (a onetime connection). We recommend disabling this rule after the device has been added, and saving the table with a name like "iptables-with-telnet" (refer to steps 33 and 34 below) so that it can be reinstated when required.

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <managed_device> -o eth0 -p tcp -m tcp
--dport 23 -j ACCEPT
```

16) 514/UDP/OUT: To send syslog events, if configured

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <syslogd_ip> -o eth0 -p udp -m udp
--dport 514 -j ACCEPT
```

17) 25/TCP/OUT: For the SMTP client to connect to its server, if configured to send alerts via email

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <smtp_server_ip> -o eth0 -p tcp -m tcp
--dport 25 -j ACCEPT
```

18) 162/UDP/IN: For SNMP traps

```
/sbin/iptables -A INPUT -s <remote_ip> -d <nsm_ip> -i eth0 -p udp -m udp --dport
162 -j ACCEPT
```

19) 161/UDP/OUT: For SNMP to listen

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <snmp_server_ip> -o eth0 -p udp -m udp
--dport 161 -j ACCEPT
```

20) 53/UDP/OUT: For DNS

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <dns_ip> -o eth0 -p udp -m udp --dport 53
-j ACCEPT
```

21) 1645/UDP/OUT: RADIUS server authentication port

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <radius_server_ip> -o eth0 -p udp -m udp
--dport 1645 -j ACCEPT
```

22) 1646/UDP/OUT: RADIUS server accounting port

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <radius_server_ip> -o eth0 -p udp -m udp
--dport 1646 -j ACCEPT
```

23) 9020/UDP/OUT: Integrated surf control for Web filtering

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <server_ip> -o eth0 -p udp -m udp --dport
9020 -j ACCEPT
```

24) 443/TCP/OUT: To download the attack database and DMI schema

```
/sbin/iptables -A OUTPUT -d services.netscreen.com -o eth0 -p tcp -m tcp --dport
443 -j ACCEPT
/sbin/iptables -A OUTPUT -d xml.juniper.net -o eth0 -p tcp -m tcp --dport 443 -j
ACCEPT
```

25) ICMP/IN: To enable you to ping the NSM on eth0 to see if the system is up or down

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p icmp -m icmp --icmp-
type 8 -j ACCEPT
```

26) ICMP/OUT: To enable you to ping out from the NSM, which is useful to test the reachability of the managed devices

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <managed_devices> -o eth0 -p icmp -m icmp
--icmp-type 8 -j ACCEPT
```

27) FTP/OUT: To upload tech-support data from the server to the Juniper FTP site

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d ftp.juniper.net -o eth0 -p tcp -m tcp -j
ACCEPT
```

Note: Keep the FTP rule simple, as there will be multiple rules if ftp has to be restricted based on ports.

28) 8443/TCP/IN: Allows the NSM GUI clients to download from the server

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
8443 -j ACCEPT
```

29) 123/UDP/OUT: NTP client uses this to connect to its server

```
/sbin/iptables -A OUTPUT -s <nsm_ip> -d <ntpserver_ip> -o eth0 -p udp -m udp
--dport 123 -j ACCEPT
```

30) Log any suspicious connection coming in or getting initiated (also useful for troubleshooting connectivity issues)

```
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m state
--state NEW -j LOG --log-prefix “NEW_PACKET_IN: “
/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m state
--state NEW -j DROP
/sbin/iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j LOG
--log-prefix “NEW_PACKET_OUT: “
/sbin/iptables -A OUTPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j DROP
```

31) Log all other traffic

```
/sbin/iptables -A INPUT -j LOG --log-prefix “UNKNOW_TRAFFIC_IN: “
/sbin/iptables -A OUTPUT -j LOG --log-prefix “UNKNOW_TRAFFIC_OUT: “
```

32) Drop rule (*it is very important to drop everything else!!*)

```
/sbin/iptables -A INPUT -j DROP
/sbin/iptables -A OUTPUT -j DROP
```

33) Save the rules

```
/sbin/iptables-save > iptables.rules.1
```

Flush the rules (just in case of issues)

```
/sbin/iptables -F OUTPUT (flushes the egress rules)
/sbin/iptables -F INPUT (flushes the ingress rules)
/sbin/iptables -F (flushes everything)
```

34) Reinstate flushed rules

```
/sbin/iptables-restore iptables.rules.1 (iptables.rules.1 was the saved rule at
step 33, but any previously saved rule can be reinstated as well)
```

35) To check hits on rules

```
/sbin/iptables -L -v
```

36) To check hits against rules in real time

```
/usr/bin/watch -d “/sbin/iptables -L -n -v”
```

B) Device Server on a Different Machine

7801/TCP/IN: For device server to connect to GUI server

On the GUI server, add this (anywhere above the drop rule), then follow the steps in rules 1-4, 7, 11-13, 20, 24-33

```
/sbin/iptables -A INPUT -s <dev_ip> -d <gui_ip> -i eth0 -p tcp -m tcp --dport
7801 -j ACCEPT
```

On the device server, add this (anywhere above the drop rule), then follow rules 1-5, 8-10, 12-26, 29-33

```
/sbin/iptables -A OUTPUT -s <dev_ip> -d <gui_ip> -o eth0 -p tcp -m tcp --dport
7801 -j ACCEPT
```

C) Juniper Networks NSMXpress Installations

443/TCP/IN: To enable connection to the Web interface

```
/sbin/iptables -A INPUT -s <your_net> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport
443 -j ACCEPT
```

After this step, complete all of the above numbered steps for the standalone installation.

D) In High Availability Environments

22/TCP: To resynchronize

```
/sbin/iptables -A INPUT -s <peer_ip> -d <self_ip> -i eth0 -p tcp -m tcp --dport
22 -j ACCEPT
/sbin/iptables -A OUTPUT -s <self_ip> -d <peer_ip> -o eth0 -p tcp -m tcp --dport
22 -j ACCEPT
```

7801/TCP: For the device server to connect to the GUI server

```
/sbin/iptables -A INPUT -s <peer_ip> -d <self_ip> -i eth0 -p tcp -m tcp --dport
7801 -j ACCEPT
/sbin/iptables -A OUTPUT -s <self_ip> -d <peer_ip> -o eth0 -p tcp -m tcp --dport
7801 -j ACCEPT
```

7802/UDP: For HA heartbeats

```
/sbin/iptables -A INPUT -s <peer_ip> -d <self_ip> -i eth0 -p udp -m udp --dport
7802 -j ACCEPT
/sbin/iptables -A OUTPUT -s <self_ip> -d <peer_ip> -o eth0 -p udp -m udp --dport
7802 -j ACCEPT
```

After this step, complete all of the steps for a standalone install on both of the servers.

E) With STRM Series Support

5432/TCP/IN: To enable Juniper Networks STRM Series Security Threat Response Managers to connect to the profiler database (PostgreSQL)

```
/sbin/iptables -A INPUT -s <strm_ip> -d <nsm_ip> -i eth0 -p tcp -m tcp --dport 5432 -j ACCEPT
```

These steps go along with the steps of your respective NSM installation. If STRM Series support needs to be enabled, then this port needs to be allowed access.

Force Iptables to Log Message to a Different Log File

By default, iptables log messages are written to a /var/log/messages file. The command tail `-f /var/log/messages` will show iptables logs in real time. However, this file can contain other data as well, often making the analysis of iptables log traffic a difficult task.

The following steps show how to create a new log file called /var/log/iptables.log. Using a new file allows you to create better statistics, and also allows you to analyze traffic and attacks more easily.

1. Edit the file /etc/syslog.conf

- Add the following line (so that it will be processed first)
  kern.warning /var/log/iptables.log

2. Optional: Modify the line below to include "kern.!=warning" as shown below (this is to prevent the log from iptables to be written to the /var/log/messages again)
   info;kern.!=warning;mail.none;authpriv.none;cron.none /var/log/messages
   - Save and close the file.
   - **Note:** This will also put *any warning level kernel* messages into the iptables.log
3. Edit the file /etc/logrotate.conf
   - Add the code below to enable weekly log rotation
     /var/log/iptables.log {
     }
4. Restart syslogd
   - /etc/init.d/syslog restart

Logs can also be analyzed in a graphical format: **www.gege.org/iptables/.**

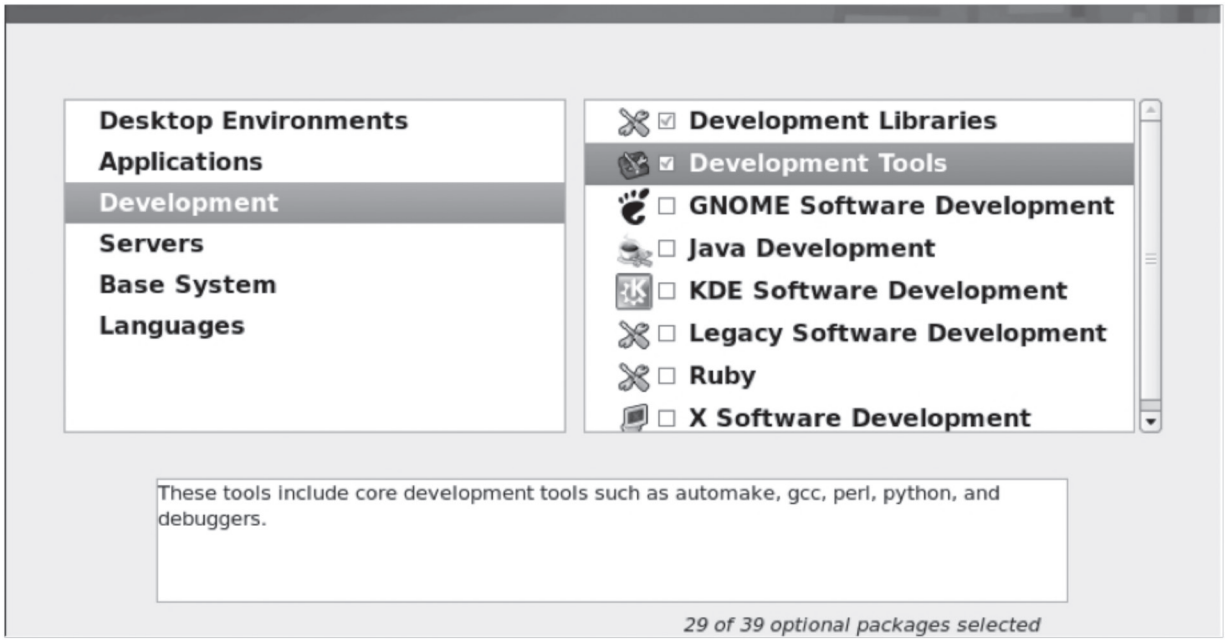
Logs can be made to write in pcap format, so that they can be analyzed by Wireshark. This requires extra packages (ulogd ulogd-pcap wireshark-gnome) to be installed.

Installing/Upgrading Iptables to the Latest Version (v1.4.5)

Prerequisites

1. A compiler, glibc-devel, and linux-kernel-headers

If you are not sure which packages are needed or which package dependencies you might be dealing with, select the option to customize the installation and then select the development tools and development libraries as shown in the screenshot below.



2. If it's an upgrade, then make a backup of current rules

```
cp -rf /etc/sysconfig/iptables /tmp/iptables.back
```

Caution: No rpm is available for the version 1.4.5 as of this writing. As such, it is not possible to do the rpm upgrade; the only option is to put the rules back into the new version.

3. Remove the previous version of iptables

```
/bin/rpm -qa | grep iptables (This will list the installed iptables rpm.)
/bin/rpm -ev --nodeps iptables* (To remove the iptables)
```

4. Install Iptables version 1.4.5, which can be downloaded from **www.netfilter.org/projects/iptables/downloads.html**.

5. `tar -xjvf iptables-1.4.5.tar.bz2`

6. `cd iptables-1.4.5`

- Refer to the file INSTALL for the installation options. Using the default installation, iptables will be available at /usr/local/sbin/iptables.
- The command "echo $PATH" should list the path "/usr/local/sbin" so that you can call and create the rules just by typing iptables. If you skip this step, you will need to type the complete path as /usr/local/sbin/iptables.

7. `./configure`

8. `make`

9. `make install`

Summary

In this application note, we have discussed how to harden the UNIX kernel on which Juniper Networks Network and Security Manager is built for incoming and outgoing traffic. We have also shown how to provide only the required access without affecting NSM's functionality. We have seen that iptables functionality provides an excellent set of features for restricting network traffic and network access, and for protecting against some of the most commonly launched attacks. Iptables also facilitates traffic analyses and provides insights into connectivity and security issues with the help of tagged logs. All of these features help in mitigating the risks that stem from open unused ports on Network and Security Manager, helping to secure the NSM system and thus the networks it manages.

However, securing NSM need not be limited to the use of iptables, the best practices involve additional steps that broaden NSM's benefits and protections:

- Installing only the minimal required software and applications on the UNIX kernel
- Patching the system
- Restricting access with Security-Enhanced Linux (SELinux)
- Securing the file system permissions and S*ID binaries
- Improving the login, user security, and password policies
- Employing proper physical and boot security controls
- Securing processes via network access controls
- Increasing the logging and audit information
- Configuring vendor supplied security software (intrusion prevention system, firewall)
- Making regular data backups to facilitate recovery in case of failures
- Maintaining reliable power and cooling
- Securing cabling
- Deploying redundant hardware
- Maintaining well trained and motivated employees to avoid intentional or unintentional sabotage to the device

References

For additional information on this topic, please refer to the following:

http://www.juniper.net/nsm

http://vinodbm.wordpress.com

http://www.netfilter.org

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
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

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

3500183-002-EN Mar 2012 Printed on recycled paper