Firewall Product Functional Summary

1. Product Version

Vendor Name: Nokia

Product Version: Nokia IPSO v3.2 Firewall Feature Set
(for Nokia IP330, IP440, and IP650 series)

Date of Publication: November 1999

2. Executive Overview

Nokia IP Security Solutions

Nokia IP Security Solutions offer a comprehensive line of products for Internet security applications. We combine world class routing capabilities with the best-of-breed firewall software from Check Point Technologies, Ltd. This unique combination of Nokia IPSO; routing operating system and Check Point FireWall-1; gives one an unprecedented security solution for Internet access and Virtual Private Networking (VPN).

The IPSO platform software is an operating system designed for high-speed IP routing and forwarding. It is scalable, robust and secure. The original foundation of IPSO was a variant of FreeBSD UNIX known for its networking capabilities. Several years of design and development work now provide the secure operating system foundation for Nokia platform offerings. IPSO is customized to support Nokia's enhanced routing capabilities and Check Point's FireWall-1 firewall functionality. Unnecessary features have been stripped out to minimize the need for UNIX system administration.

Nokia IPSO/Check Point Firewall-1 integration combines Virtual Routing Redundancy Protocol (VRRP) with FireWall Synch to provide highly available routing along with stateful inspection, pioneered by Check Point. This ensures tracking of network connections for security.

Nokia platforms running IPSO and Check Point FireWall-1 can function as an Internet, intranet, or extranet firewall providing security and packet filtering between

- your corporation and Internet Traffic

- internal departments within your network

- your corporation and remote branch offices

- your corporation and partner sites

Nokia IPSO is standards-based routing and is architected to inter operate with all standards-based routers including Cisco, Bay, and 3COM. The IPSO routing kernel, Ipsilon Routing Daemon (IPSRD) supports a comprehensive suite of IP routing protocols including RIPv1/RIPv2, IGRP, OSPF, and BGP4 for unicast traffic and DVMRP for multicast traffic. The IPSO operating system also supports other router functions such as router discovery, full set IDR route aggregation, and route redistribution. The advanced integrated router functionality eliminates the need for separate intranet and access routers in firewall applications.

3. Overview of firewall product functional summary program

3.1. Scope and purpose of firewall product functional summaries

The purpose of the firewall product functional summary program is twofold:

* To provide a structured format in which vendors can describe the distinguishing features and advantages of their products

* To provide a structured format from which potential firewall customers can compare and contrast the features and design principles of firewall products

The summary format used in the program has been derived through an open process including firewall vendors, agencies of the computer security community, and the firewall customer community. This cooperative effort is a voluntary program.

3.2. Security and design principles

When designing computer security systems, as with other mission critical systems, it is important that the basic design principles of the system be sound, and that the implementation be of high quality. When choosing a computer security system, it is important for the customer to be able to judge the capabilities and design principles of the system in terms of the protections required by that customer's intended deployment of the system. The functional summary program permits computer security product manufacturers to present their products and designs in the best

possible light, while adhering to a format that encourages accurate product comparison. The summary format requests information from the vendor about design decisions made in a number of important areas, yet tries to permit the response to be as free-form as necessary so as not to constrain the vendor within the bounds of a narrow definition of what constitutes a "firewall."

3.3. Terms and definitions

Since the network security field is dynamic and rapidly growing, new techniques and terms are constantly being brought into use. To provide a basis for clear communication, a simple glossary of terms and definitions is provided as a part of the summary format. Vendors are welcome to define their own terminology, distinct from the terms in the glossary, but are requested to provide definitions in the glossary section for new terminology that is coined, and to annotate them as such. Readers of this document are encouraged to peruse the glossary section for annotations and definitions of such new terms as may appear.

4. Product Overview

Operating System - Nokia firewalls run IPSO, a UNIX-like operating system based on FreeBSD. IPSO is customized to support Nokia's enhanced routing capabilities and Check Point's FireWall-1 firewall functionality, and to "harden" network security. Unnecessary features have been stripped out to minimize the need for UNIX system administration. The Nokia IPSO firewall feature set is available on the IP330, IP440 and IP650 Security Series.

The Nokia routing subsystem, Ipsilon Routing Daemon (IPSRD), is an essential part of the firewall. IPSRD's role is to dynamically compute paths or routes to remote networks. Routes are calculated by a routing protocol. Besides providing routing protocols, IPSRD also allows routes to be converted or redistributed between routing protocols. Finally, when there are multiple protocols with a route to a given destination, IPSRD allows you to specify a ranking of protocols. Based on this ranking, a single route is installed in the forwarding table for each destination.

One can configure each of the supported routing protocols, route redistribution, and other routing options via the Configuration Routing section in Voyager.

Routing monitoring is available by following links from the individual protocol pages or by clicking the Monitor button in Voyager. Another monitoring tool is ICLID. This tool provides interactive, text-based monitoring of the routing subsystem.

As a fully-featured networking and security appliance, the IPSO supports a comprehensive suite of IP routing protocols including RIPv1/RIPv2, IGRP, OSPF, and BGP4 for unicast traffic and DVMRP for multicast traffic. The IPSO also supports other router functions such as router discovery, full set IDR route aggregation, and route redistribution. The advanced integrated

router functionality eliminates the need for separate intranet and access routers in firewall applications.

Nokia IPSO supports Virtual Router Redundancy Protocol (VRRP) and firewall synchronization, enabling full load sharing active redundancy. This protocol is used by multiple routers on the same LAN to implement a "virtual" router. The virtual router is then used by hosts on the LAN as their default router. Only one of the routers in the VRRP cluster - the "master" - acts as the virtual router at any one time; the protocol describes the method by which other routers in the cluster take over from the master if it goes down or resigns as the virtual router.

The main benefit of this protocol is that hosts on the LAN can switch from one router to another (in the case of failure) without changing their
routing configuration or running additional protocols. Load balancing can also be implemented by configuring multiple VRRP clusters across multiple
routers, each router being the master of a different cluster.

Services

- SSH (secure shell), with strong encryption and authentication, for secure administrative access to system
- S/Key authentication for 'telnet' and 'ftp' available (and can be made mandatory)
- Standard Unix shadow passwords with MD5
- IP Access lists and rate shaping can be used to prevent various attacks, including denial of service from ICMP floods, SYN attacks, and ICMP error responses
- Routing protocols (RIPv2, OSPF, and BGP) all have strong authentication via keyed MD5
- SecuRemote and other FireWall-1 access services
- Web server is Apache, a widely-used and secure web server

Access Methods

Serial Console
Connecting via serial console requires physical access to the system administrator has the option to allow logins only from the serial console

telnet
Telnet can be turned on or off (on by default) this is the only service on by default ftpd can be turned on or off (off by default).

User Accounts

Limited, Multiple User Support - Provisions have been added to the Password Settings of the Network Voyager that allow the addition of multiple administrative or monitoring users. These

users names are used when configurations changes are logged by the system.

"admin" (privileged) -- the "root" user configured during Boot Manager initial configuration. The *admin* account has read/write permissions on the unit.

"monitor" (read-only) -- by default the "monitor" account is disabled. The result is a single user system, which avoids many security holes involving unprivileged users becoming "root" (in this case "admin"). There is limited ability to add new users, which protects against "hidden" accounts and related attacks.

Nokia is positioned to leverage the vast competition in the Intel marketplace, delivering new hardware interfaces, components, and peripherals. IP Security solutions are designed to fit in a standard rack with front access connectors to facilitate maintenance. No local keyboard or monitor is necessary; remote management capabilities leverages centralized IT expertise.

Design

From a design standpoint, we started with no binaries and libraries and then added what we needed with an eye toward a compact and secure system. The 'inetd.conf' starts empty, and services must explicitly be added via Voyager, the web interface used to configure the Nokia IP Security Solutions appliance.

Applications such as sendmail (a major source of security risk) have been removed instead, we provide a send-only mail system that does not accept connections on port 25, and does not accept incoming email.

In addition, the kernel has been hardened by removing, Berkeley "r" commands, such as 'rsh', 'rlogin', 'rexec', etc. -- these are known to be insecure, exportable file systems (such as NFS), which can be a security risk, remote user information daemons/services such as 'finger', 'who', and 'talk' which can leak information, and compiler or development environment on the system, which stops any intruders from building binaries which could be used to replace existing valid binaries. No small services ('chargen', 'echo', etc.) are enabled by default, however they can be enabled by administrator if desired. The BIND (DNS server), or dependence on external DNS service for anything has been removed from the IPSO kernel. There is no news server, printing server, NIS, POP, IMAP, or X Window System, which have historically been potential security risks or extraneous CGI program on the system.

Security hole coverage

We have fixed problems or verified lack of the problem described in any applicable CERT advisories, including:

'Smurf' attack (which relates to IP directed broadcast)
'Teardrop' (which relates to overlapping IP fragments)
'Land' (which relates to spoofed IP packets)
Ping of Death
SYN Flooding

ICMP Redirect, Destination Unreachable, and Ping Sweep
Source Routing
Bogus RIP/OSPF Message
DNS Siege
NTP Siege and Replay
Portmapper Scan and Redirection
TCP/IP Spoofing with Sequence Number Prediction
TCP/UDP Port Sweeping
Bootp Spoofing with TFTP reconfiguration of routers and many more . . .

5. Vendor information

Nokia

Nokia is one of the top ten largest providers of telecommunications products in the world. Headquartered in Helsinki, Finland, Nokia has a long and rich history in advanced technologies. Since 1988, Nokia has increased its focus on Telecommunications and has become the global leader in advanced digital wireless communications, including wireless infrastructure as well as the most advanced handsets in the world. In addition, Nokia has a strong presence in wireline technology, central-office switching, broadband access, high-performance multimedia terminals, and next-generation set-top boxes for digital broadcasting.

With revenues of approximately $16 Billion annually, Nokia is one of the largest suppliers of telecommunications equipment in the world. Nokia's worldwide team of 52,000 people is growing, and looking for qualified professionals in every major discipline. Nokia targets a growth rate of 25% per year. More information on Nokia's worldwide operations can be obtained at www.nokia.com.

Nokia IP Security Solutions

Nokia IP Security Solutions are designed to provide secure Internet access while maintaining the integrity of your private network. Nokia puts engineering emphasis on ease of installation and highest standard for security in the marketplace. IP Security solutions are managed, monitored, and configured from any authorized location within the network using Network Voyager, the Nokia web-based management tool. Network Voyager is designed for ease of use - no training necessary. And all IP Security Solutions products come standard with Check Point FireWall-1, Data Fellows F-Secure SSH (SecureShell) software for secure management, and all interfaces pre-installed to save the user effort.

The Future of Communications

The world is changing - the way we communicate with others and access information is undergoing a dramatic transformation. Every conceivable piece of information is now available on the Internet. The challenge is how to provide access to this wealth of information in a fast, reliable and secure way.

By partnering with Nokia, telecommunications operators and ISPs across the globe are upgrading their existing networks to support the next generation of data services, including:

Wireless data solutions - totally mobile IP access, anyplace, anytime
Broadband IP access - the ultimate in high speed Internet
Advanced corporate data solutions - from secure Intranets to VPNs
Voice Over IP - data networks with guaranteed quality of service (QoS)

As the world leader in wireless data, Nokia is ideally positioned to meet the needs of mobile operators. As the amount of IP traffic carried by GSM continues to increase at a dramatic rate - operators depend on carrier grade solutions from Nokia to meet their business needs.

Our vast experience in mobile data has also given Nokia a unique advantage in the converging worlds of data and telecommunications. Fixed-line telecommunications operators are now deploying broadband access solutions to offer a range of high speed data services. Utilizing our experience in mobile data and IP services, Nokia is now among the world leaders in providing broadband IP solutions based on ADSL. In fact, Nokia has the only commercially available system in the world that allows operators to provide high-speed Internet with dynamic ISP selection to the end-user.

Nokia is also providing ISPs with the next generation of IP network solutions. For example, Nokia's advanced customer care and billing solution allows ISPs to provide flexible billing of IP services with end-user self service activation. As ISPs expand to provide business services, they depend on products and solutions from Nokia to provide reliable and secure LAN interconnection and VPN services.

Nokia - we have the solution to meet your communications needs:

Total Connectivity Mobile
Total Connectivity ISDN
Total Connectivity IP Access
Total Connectivity Broadband

Nokia is one of the top ten largest providers of telecommunications products in the world. Headquartered in Helsinki, Finland, Nokia has a long and rich history in advanced technologies. Since 1988, Nokia has increased its focus on Telecommunications and has become the global leader in advanced digital wireless communications, including wireless infrastructure as well as the most advanced handsets in the world. In addition, Nokia has a strong presence in wireline technology, central-office switching, broadband access, high-performance multimedia terminals, and next-generation set-top boxes for digital broadcasting.

5.1. Contact Information:

Contact name: Nokia

Contact Business Hours: 8:00am - 5:00pm PST

Contact telephone number: 1-650-625-2000

Contact FAX number: 1-650;.692.2170

Contact Email address: www.nokia.com

Contact Web URL: www.nokia.com

Contact postal address: 313 Fairchild Drive
Mountain View, CA 94043

Nokia Europe (Finland)

Corporate Communications
Keilalahdentie 4, FIN-02150 Espoo
P.O. Box 226, FIN-00045 NOKIA GROUP
Tel. +358 9 180 71
Fax +358 9 652 409

Investor Relations
Keilalahdentie 4, FIN-02150 Espoo
P.O. Box 226, FIN-00045 NOKIA GROUP
Tel. +358 9 180 7289
Fax +358 9 176 406

Nokia Networks
Keilalahdentie 4, FIN-02150 Espoo
P.O. Box 300, FIN-00045 NOKIA GROUP
Tel. +358 9 511 21
Fax +358 9 5112 5560

Nokia Mobile Phones
Keilalahdentie 4, FIN-02150 Espoo
P.O. Box 100, FIN-00045 NOKIA GROUP
Tel. +358 10 5051
Fax +358 10 505 5768

Nokia Communications Products
Keilalahdentie 4, FIN-02150 Espoo
P.O. Box 226, FIN-00045 NOKIA GROUP
Tel. +358 9 180 71
Fax +358 9 656 388

Nokia Americas

Nokia Mobile Phones
Customer Service (USA)
Tel. +1 888 665 4228

Nokia Americas

6000 Connection Drive
Irving, Texas 75039
Tel. +1 972 894 5000
Fax +1 972 894 5050

Corporate Communications
6000 Connection Drive
Irving, Texas 75039
Tel. +1 972 894 5000
Fax +1 972 894 4706

Investor Relations
6000 Connection Drive
Irving, Texas 75039
Tel. +1 972 894 4880
Fax +1 972 894 4831

6. Product security architecture

6.1. Rationale

When describing a networked computer security system, there are several aspects of its design that must be taken into consideration. A security system such as a firewall must be able to protect not only the systems *connected* to it, it must be able to protect *itself*. Generally, the mechanisms whereby this is accomplished are different. The firewall system's security is dependent on whatever security mechanisms the firewall has built into itself. The systems connected to the firewall's security are dependent on whatever security mechanisms the firewall provides to them. In some cases these mechanisms may be based on a common design feature. In others they may be a result of a combination of features. In this section we explain how the firewall protects itself and the systems connected to it. In cases where additional protections are provided, or additional protective relationships are provided, we will explain the design principles and operation of these protective relationships.

6.2. Security Architecture

The Nokia IPSO is designed to be intrinsically secure. Starting with a clean OS with a single point of entry for the Voyager Console web-based application, each security appliance will run the System Startup procedure upon power up. Using the System Startup procedure, you assign a hostname to the unit and assign a password to the admin account. Then you configure the initial interface you use to establish a network connection to the unit. When you have network

connectivity, complete the configuration using the web-based Voyager configuration program.

Serial Console
Connecting via serial console requires physical access to the system administrator has the option to allow logins only from the serial console.

telnet
Telnet can be turned on or off (on by default). This is the only service on by default ftpd can be turned on or off (off by default).

User Accounts

Limited, Multiple User Support - Provisions have been added to the Password Settings of the Network Voyager that allow the addition of multiple administrative or monitoring users. These users names are used when configurations changes are logged by the system.

> "admin" (privileged) -- the "root" user configured during Boot Manager initial configuration. The *admin* account has read/write permissions on the unit.
>
> "monitor" (read-only) -- by default the "monitor" account is disabled. The result is a single user system, which avoids many security holes involving unprivileged users becoming "root" (in this case "admin"). There is limited ability to add new users, which protects against "hidden" accounts and related attacks.

Secure Shell

Secure Shell (SSH) is a program that allows you to securely log into another computer over a network, execute commands in a remote machine, and move files from one machine to another machine. You can use SSH instead of TELNET to securely manage a Nokia IPSO based machine. YOu can also tunnel HTTP over SSH to use Voyager to securely manage your machine.

Secure Shell (SSH) features:

- Strong Authentication - protects your network from DNS spoofing, which is when an attacker forges name server records, and from people listening for passwords being sent over the network (SSH never sends passwords in the clear).
- Automatic and Transparent Encryption - protects against spoofed packets and hijacked connections.

6.3. Product default operations

Default Features

IP Security Solutions are managed, monitored, and configured from any authorized location within the network using Network Voyager, the Nokia web-based management tool. These services are enabled within the Nokia IP Security Solution family.

Standard services within the IP Security Solutions

Nokia IP Security Solutions are powered by an integrated framework that is made up of three components: hardware that leverages the flexible Intel platform, a hardened routing operations system, and Check Point FireWall-1 software.

Routing and Security Combined

The Nokia integrated approach to firewall applications eliminates the need for separate intranet and access routers, management stations, and firewall servers.

High Availability

Nokia delivers continuous availability from both routing systems and firewall with VRRP (Virtual Router Redundancy Protocol) and Firewall Sync (firewall synchronization technology from Check Point) - enabling load-sharing active redundancy between two or more Nokia systems - standard with all IP Security Solutions.

Virtual Private Networks

Provide secure connections to your key supplier and remote users while maintaining the integrity of your private network. Nokia IP Security Solutions, with encryption by Check Point Software Technologies, Ltd., make global VPNs and Extranets a reality.

High Availablility VPN Tunnels

The High Availability Virtual Personal Network (HA VPN) feature is an IPSO-only feature that provides site-to-site IPSEC encryption tunnels. The configuration is arranged such that a fail over is possible in the event of a firewall loss. This feature provides IP tunnels through which IPSO routes and dynamically re-directs traffic when a particular tunnel goes down.

The VPN mechanism depends of an IGP protocol to re-route traffic to the new tunnel.

Network Management

IP Security Solutions are managed, monitored, and configured from any authorized location within the network using Network Voyager, the Nokia web-based management tool. Network Voyager is designed for ease of use, running on any standard web browser.

Routing Features

A comprehensive set of IP routing protocols and functions, including RIPv1/RIPv2, IGRP (optional), OSPF, BGP4 (optional), DVMRP, and VRRP, are supported. Other router functions supported include Router Discovery, BOOTP Relay, Mail Relay, NTP, DNS, IP Broadcast Helper, Router Discovery, full set IDR Route Aggregation, and Route Redistribution.

Traffic Management

Nokia's bandwidth management functionality allows you to seperate traffic based on address, protocol, or interface into distinct streams and then shape, limit, or prioritize the stream.

Network Address Translation

Check Point FireWall-1's Network Address Translation (NAT) features can aid in establishing connectivity with private networks whose addresses are either "illegal" (not valid on the Internet) or must remain unexported for security reasons. IPSO does not inherently support NAT.

Transaction Logging

IPSO contains transaction logging to syslog for system errors, kernel debug messages, and authorization information. Transaction logging, as directed by the user, can be written to the local syslog file or to a remote system.

User Accounts

Limited, Multiple User Support - Provisions have been added to the Password Settings of the Network Voyager that allow the addition of multiple administrative or monitoring users. These users names are used when configurations changes are logged by the system.

- "admin" (privileged) -- the "root" user configured during Boot Manager initial configuration. The *admin* account has read/write permissions on the unit.
- "monitor" (read-only) -- by default the "monitor" account is disabled result is a single user system, which avoids many security holes involving unpriviledged users becoming "root" (in this case "admin") no ability to add new users, which protects against "hidden" accounts and related attacks.

Interface Configuration

The user will need to configure the IPSO kernel for each interface on the system as well as the Nokia routing subsystem and routing protocols. The user will configure the physical ID which identifies the interface type and provides information about the slot and port number. Physical IDs are used internally by the IPSO software. These interfaces can include, depending on the IP appliance purchased:

- Four-port Ethernet/Fast Ethernet
- Dual-port Ethernet/Fast Ethernet
- Single-port V.35 Serial
- Dual-port V.35 Serial
- Single-port X.21 Serial
- Dual-port X.21 Serial
- Single-port T1 with built-in CSU/DSU
- Single-port HSSI
- ATM 155 UTP or MM Fiber
- FDDI

- Single-port Ethernet/Fast Ethernet (IP330)

Token Ring Support for the IP650

A Token Ring NIC is supported on the IP650 platform only. The Token Ring implementation is half-duplex capable and fully compatible with IBM and IEEE 802.5. It provides source routing as well as 4Mbps and 16Mbps ring speeds without speed-auto negotiation, and supports multicast, including broadcast mode.

Configuration parameters include ring speed, maximum frame size, source routed option, multicast mode, logical interface, and interface statistics. Additionally, the implementation:

- Supports the Racore A8168 PMC carrier interface with DB9 and RJ45 connectiosrs and the Racore A8154-010 PCI interface
- Provides MIB support as specified in RFCs 1213 and 1748

Once installed, Token Ring configuration is accomplished through the Interfaces option of the Network Voyager configuration software.

NOTE: Hotswapping Token Ring interfaces in IP650s is not supported

Nokia routing Subsystem

The Nokia routing subsystem, Ipsilon Routing Daemon (IPSRD), is an essential part of the firewall. IPSRD's role is to dynamically compute paths or routes to remote networks. Routes are calculated by a routing protocol. Besides providing routing protocols, IPSRD also allows routes to be converted or redistributed between routing protocols. Finally, when there are multiple protocols with a route to a given destination, IPSRD allows you to specify a ranking of protcols. Based on this ranking, a single route is installed in the forwarding table for each destination.

The user can configure each of the supported routing protocols, route redistribution, and other options via the Configuration Routing section of Voyager.

The user can configure the routing protocols for two major categories: exterior gateway protocols (EGPs) and interior gateway protocols (IGPs).

Interior Routing Protocols supported by IPSRD: RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First). Static routes and aggregate routes are also supported.

Exterior Routing Protocls supported by IPSRD: BGP (Boarder Gateway Protocol) which supports two basic types of sessions between neighbors: internal (IBGP) and external (EBGP).

Check Point FireWall-1

FireWall-1 initializes in a completely secure state and initially blocks all gateway traffic. Specific rules must be defined by the administrator to permit traffic through the firewall. FireWall-1 adheres strictly to the policy of, "that which is not expressly permitted, is prohibited."

alled.

The user will be required to configure any and all policies within the Check Point FireWall-1.

6.4. Protection of the firewall system

Nokia IPSO is a hardened FreeBSD Unix based kernel.

Services

- SSH (secure shell), with strong encryption and authentication, for secure administrative access to system
- S/Key authentication for 'telnet' and 'ftp' available (and can be made mandatory)
- Standard Unix shadow passwords with MD5
- IP Access lists and rate shaping can be used to prevent various attacks, including denial of service from ICMP floods, SYN attacks, and ICMP error responses
- Routing protocols (RIPv2, OSPF, and BGP) all have strong authentication via keyed MD5
- SecuRemote and other FireWall-1 access services
- Web server is Apache, a widely-used and secure web server

Security hole coverage

We have fixed problems or verified lack of the problem described in any applicable CERT advisories, including:

'Smurf' attack (which relates to IP directed broadcast)
'Teardrop' (which relates to overlaping IP fragments)
'Land' (which relates to spoofed IP packets)

Check Point FireWall-1

FireWall-1's Stateful Inspection technology intercepts all network communications before reaching the operating system. The FireWall-1 Inspection module resides in the IPSO kernel, below the network layer, at the lowest software level. The Inspection module handles the incoming data packet communications and can intercept and analyze all packets before they reach the IPSO kernel. Therefore, FireWall-1 does not leave the underlying operating system vulnerable to attack, either by network users or Internet hackers.

6.5. Protection of attached networks and hosts

The Nokia IPSO routing protocols compute the best route to each destination and may block or permit traffic based on the configuration of these protocols.

Static Routes are routes manually configured in the routing table. There are three types of static routes:

- Normal
- Black Hole
- Reject

A normal static route is used to forward packets for a given destination in the direction indicated by the configured firewall

A black hole route uses the loopback address as the next hop. This route discards packets that match the route for a give destination.

A reject static route uses the loopback as the next hop, discards packets that match the route for a given destination and sends an ICMP unreachable message back to the sender of the packet.

6.6. Protection of individual hosts [optional]

The Nokia IPSO kernel and the Voyager Management Console can use Secure Shell that allows the user to log into another computer over a network, execute commands in a remote machine, and move files from one machine to another machine. You can use SSH to securely manage your machines. You can also tunnel HTTP over SSH to use Voyager to securely manage your machine.

The following list porvides SSH features:

- Strong Authentication - protects your network from DNS spoofing, which is when an attacker forges name server records, and from people listening for passwords being sent over the network (SSH never sends passwords in the clear).
- Automatic and Transparent Encryption - protects against spoofed packets and hijacked connections.

The IPSO kernel has limited and highly secure access points - Serial Console and Voyager.

Serial Console
Connecting via serial console requires physical access to the system administrator has the option to allow logins only from the serial console.

telnet

Telnet can be turned on or off (on by default) this is the only service on by default ftpd can be turned on or off (off by default)

User Accounts

Limited, Multiple User Support - Provisions have been added to the Password Settings of the Network Voyager that allow the addition of multiple administrative or monitoring users. These users names are used when configurations changes are logged by the system.

- "admin" (privileged) -- the "root" user configured during Boot Manager initial configuration. The *admin* account has read/write permissions on the unit.
- "monitor" (read-only) -- by default the "monitor" account is disabled result is a single user system, which avoids many security holes involving unpriviledged users becoming "root" (in this case "admin") no ability to add new users, which protects against "hidden" accounts and related attacks.

Secure Shell

Secure Shell (SSH) is a program that allows you to securely log into another computer over a network, execute commands in a remote machine, and move files from one machine to another machine. You can use SSH instead of TELNET to securely manage a Nokia IPSO based machine. YOu can also tunnel HTTP over SSH to use Voyager to securely manage your machine.

6.7. Other protective relationships [optional]

The IPSO kernel is a closed system with mail, ftp, telnet and other protocols disabled which protects the kernel against viruses on the internal network.

From a design standpoint, we started with no binaries and libraries and then added what we needed with an eye toward a compact and secure system.

System Security

- The 'inetd.conf' file starts empty, and services must explictly be added via Voyager, the web interface.
- No sendmail (a major source of security risk) instead, we provide a send-only mail system that does not accept connections on port 25, and does not accept incoming email.
- No Berkeley "r" commands, such as 'rsh', 'rlogin', 'rexec', etc. -- these are known to be insecure.
- No exportable filesystems (such as NFS), which can be a security risk.
- No remote user information daemons/services such as 'finger', 'who', and 'talk' which can leak information.

- No compiler or development environment on the system, which stops any intruders from building binaries which could be used to replace existing valid binaries.
- No small services ('chargen', 'echo', etc.) by default can be enabled by administrator if desired.
- No BIND (DNS server), or dependence on external DNS service for anything.
- No news server, printing server, NIS, POP, IMAP, or X Window System, which have historically been potential security risks.
- No extraneous CGI program on the system.

Filesystem

- Binaries are all on a filesystem which is mounted read-only.
- Only "admin" can change any filesystem characteristics, and all mount, unmount and file timestamp changes are syslog'd for accounting purposes.
- Easy to install a full new image (takes less than 15 minutes for a full install), or verify an existing install from a known-good release image.
- All configuration settings are stored in a single file, which can easily be backed up and checked for changes.
- All changes to security settings (passwords, security options) and configured daemons are syslog'd.
- Syslog can be directed to a server over the network and/or to a local file.

Nokia IPSO has the Virual Routing Redundant Protocol (VRRP) to protect against network outages.

VRRP Description

Virtual Redundant Routing Protocol (VRRP) provides dynamic fail-over of IP addresses from one router to another in the event of failure. It is used on shared media where end hosts are configured with a static default route. In this environment, normally the loss of the default router results in a catastrophic event, isolating all end hosts that are unable to detect any alternate path that may be available. Using VRRP, a router can automatically assume responsibilty for forwarding IP traffic sent to the default router's address, should the default router fail. This allows a higher availability default path without requiring configuration of dynamic reouting or router discovery protocols on every end host.

Virtual Routers

To back up a default router using VRRP, a Virtual Router must be created for it. A Virtual Router consists of a unique Virtual Router ID (VRID), and the default router's IP address(es) on the shared LAN.

The Virtual Router is created on the default router by specifying the router's interface to the shared LAN and by specifying the VRID by which this router's addresses will be identified in the LAN. The default router's IP addresses are added to the Virtual Router automatically.

Once a Virtual router has been created ont he default router, other routers can be configured as backup routers. This is done by configuring the default router's Virtual Router information (its VRID and IP addresses) on each of the backup routers. They will then use VRRP to take over the default router's addresses, should it fail.

Priority

Priority provides a way to prefer one router in favor of another during contention for a failed router's addresses. If more than one backup router is configured for a Virtual Router, only one of them will assume forwarding responsibility for the failed default router. The routers' relative priorities are used by VRRP to determine which router that will be.

- Priority is a numberic value; the higher the value, the higher the priority. If the configured priorites of two backup routers is equal, their IP addresses are used as the tiebreaker.

- The router that owns the IP addresses configured in the Virtual Router always has the highest priority. Once a failed router recovers, it will always reclaim responsibilty for forwarding traffic sent to its own addresses.

The user specifies priority when configuring a router to back up another.

Hello Interval

The Hello Interval is the time interval (in seconds) between VRRP Advertisements. It also determines the fail-over interval; that is, how long it takes a backup router to take over from a failed default router.

VRRP Advertisements are broadcast on the LAN by the current master of each Virtual Router. Backup routers listen for these Advertisements and assume failure if they have not received an Advertisement within three Hello Intervals. They can elect a new master of the Virtual router, based on their relative priorities.

Authentication Methods

VRRP is designed for a range of internetworking environments that may emply different security policies. The protocol includes several authentication methods to protect against attacks from remote and local networks.

Independent of any authentication type, VRRP includes a mechanism (setting TTL=255, checking on receipt) that protects against remote networks rejecting VRRP packets. This limits vulnerablility to local attacks.

The support authentication methods include the following:

- No Authentication - This authentication type means that VRRP protocol exhanges are not

authenticated. This method shuld be used only in environments where there is minimal security risk and little chance for configuration errors.

- Simple Text Password - This authentication type means that VRRP protocol exchanges are authenticated bya simple clear-text password. This method is useful to protect against accidental misconfiguration of routers of the LAN. It also protects against routers inadvertently backing up another router. This type is recommended when there is minimal risk of nodes on the LAN actively disrupting VRRP operations.

The authentication Method selected must be the same for all routers running VRRP on the shared media network.

Monitored Circuit

Running VRRP in a static routed environment can lead to a "black hole" failure senario. If a link on the VRRP master fails, it may accept packets from an end host but be unable to forward them to destinations reached via the failed link. this creates an unnecessary black hole for those destinations if there is an alternate path available via the VRRP backup.

The VRRP monitored circuit feature allows the virtual router master election priority to be made dependent on the current state of the access link. With proper selection of base priority and dynamic priority update based on interface status, the virtual router forwarding responsibility can be made to gracefully failover due to interface failure on the master router.

In order to utilize the monitored circuit feature, the use must select a virtual router addrews that does not match an interface address or any IP address alloacted to a host. The ICMP redirect messages must be disabled as well.

The user can select either monitored circuit mode or VRRP v.2.

7. Product features and mechanisms

7.1. Services Provided

Nokia's IPSO operating system supports a broad range of protocols, applications and services including:

Protocol Descriptions

RIP - Routing Information Protocol

IGRP - Interior Gateway Routing Protocol

OSPF - Open Shortes Path First

DVMRP - Distance Vector Multicast Routing Protocol

BGP - Boarder Gateway Protocol

IBGP - Internal BGP

EBGP - External BGP

Aggregate Routes - allows user to take small routes and aggregate them into one larger route.

Static Routes - routes that are manually configured in the routing table to cause packets moving between a source and destination to take a specific next hop.

Route Redistribution - controls which routes are advertised by IPSRD to other systems, as well as which routes are redistributed between the protocols run on the router.

Router Services

Bootp (Bootstrap Protocol) - allows all interfaces on a LAN to be loaded from a single configuration server on the LAN

DHCP (Dynamic Host Configuration Protocol) - is a protocol for automating the configuration of the unit by assiging an IP addresses to delilver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information sucha as the addresses for printer, time and news servers.

IP Broadcast Helper - is a form of static addressing that uses directed broadcasts to forward local and all-nets broadcasts to desired destinations within the internetwork.

Router Discovery (ICMP Router Discovery Protocol) - IETF standard protocol used to inform hosts of the existance of routers.

VRRP (Virtual Router Redundancy Protocol) - provides dynamic fail-over of IP addresses from one router to another in the event of failure.

NTP - is a protocol that allows you to synchronize th UTC time by quering a server with an accurate clock.

Inbound Route Filters - allows a network administrator to restrict the set of routes that a specific routing protocol will accept. The filters allow an operator to include or exclude ranges of prefixes from the routes that will be accepted into RIP, IGRP, OSPF, and BGP.

Traffic Management

The user can configure the unit to seperate network traffic into distinct streams of packets and perform actions on those streams. The actions consist of the following: drop, reject, accept, or shape. The first three ations - drop, reject, or accept - can be used to implement a simple packet-filtering security policy.

SNMP

SNMP as implemented on the device supports the following characteristics. The proprietary MIBs are supplied with the system. Definitions of the public MIBs are available on the Web and

are also supplied with the system.

- *Gets* and *traps* (Link up and link down traps)
- *Coldstart* and *authentication failure* traps.
- MIB-II
- Other public and proprietary MIB

Latest Features:

- Trap receivers can be labeled with a hostname.
- All traps can be enabled or disabled individually.
- SNMP coldstart traps can be enabled from the Voyager SNMP configurations page. Traps are controlled by radio buttions to allow or prevent specific trap types from being generated by the SNMP agent.
- The SNMP daemon logs its messages using the syslog.

System Configuration

Database - the user can back up the database to an FTP server. The user can also back up to a host machine or workstation. The database can also be restored from an FTP server, a host machine, or a workstation. The active database can be switched to apply a new set of rules for the device.

Time - the user can set the time and date of the device.

DNS - the user can define a Domain Name Server (Primary and Secondary).

Static Host - the user can specify static host entries.

Managing IPSO Images - IPSO images can be loaded, enabled, and deleted onto the device.

Managing Packages - the user can install, enable, disable and delete packages. FTP can be used to load packages.

Mail Relay - mail relay allows the user to send email from the IP Security device. Email can be sent interactively or from a script. The mail is relayed to a mail hub which will then send the mail to a final recipient.

Security and Access

Password - the user can set and change the user account passwords for user names "admin" and "monitor".

S/Key - the user can enable S/Key for both "admin" and "monitor" accounts. S/Key is a one-

time password system that protects TELNET and FTP.

Network Access - the user can enble the following network access on the unit: FTP, Telnet, Admin Network Login, COM2 Login, and COM3 Login.

Services - the following services can be enable by the user on the unit: Echo Service, Discard Service, Chargen Service, Daytime Service, and Time Service.

Check Point FireWall-1 - The user can enable the Check Point FireWall-1 on the Nokia IP Security Solution device. The FireWall-1 consists of two primary modules:

- The Management Module
- The Firewall or Inspection Module

The Firewall Module is an Inspection Module that provides the additional FireWall-1 features of User/Client/Session Authentication, Connection Control, and Content Security. Either module may support encryption.

The Management Module consists of two modules as well:

- The Control Module
- The Graphical User Interface (GUI) Module

Monitoring

The user can monitor statistical information on the following routing protocols:

OSPF
BGP
RIP
VRRP
DVMRP
IGMP

The user can also monitor the routing daemon's information regarding the routing table.

iclid - IPSRD Command-Line Interface Daemon
The user can obtain diagnostic information by creating a telnet session on the router. **Show** command provides many kinds of information displayed in table formats for: bgp, bootpgw, dvmrp, igmp, interface, krt, memory, ospf, rip, route, version, and vrrp.

7.2. Additional Services

IPSO Logging Enhancements

Support for logging to a remote system, and for receiving logging records from other IPSO boxes

is standard on all Nokia IP Security Solutions Appliance devices. This will enable users to better monitor, track system changes and ensure security on mission critical networking devices. The IPSO kernel allows local as well as remote logging of system configuration changes.

The options which will be provided are:

- accept network syslog (no filtering is possible)
- network syslog messages above a given severity to a list of ip addresses
- syslog locally

The customer can activate both local and remote logging at the same time.

IPSO daemons syslog such as cron and snmpd. This allows these deamons to use syslog instead of writing to a log file which must be separately rotated and monitored. This allows a common location for deamon activity logging.

Changes via the Voyager management console will be logged. This feature involves xpand writing an entry to syslog when config changes are made. The feature is a syslog only logging enhancement to enable the logging of configuration changes after each "Apply" within the Voyager HTML-base configuration tool.

Nokia IPSO logging of Check Point FireWall-1 events

There are times when it may be desirable to log some or all events to syslog instead of or in addition to FireWall-1 proprietary log files. This can be accomplished using the User-Defined Tracking function of Check Point FireWall-1 and the "logger" utility that comes with IPSO. Redirecting the Log and Alert output destination of the Rulebase Properties of FireWall-1 the events will be written through the logger daemon to syslog. Optionally the user can set up the Anti-Spoof and User Authentication Alert commands to be logged to syslog in the same manner.

Mail Relay

Mail relay allows the user to send mail from the firewall. You can send email interactively or from a script. The mail is relayed to a mail hub which will then send the mail to the final recipient.

Mail relay can be used as an alerting mechanism when a Check Point FireWall-1 rule has been triggered. It can also be used to email the system administrator the results of cron jobs.

Features:

- Presence of a mail client or mail user agent (MUA) that can be used interactively or from a script.
- Presence of a sendmail-like replacement that will relay mail to a mail hub using SMTP
- Ability to specify the default recipient on the mailhub.

Nokia IPSO also has specific mail features diabled to ensure security within the operating

system.

- No support for incoming mail.
- No support for mail transfer protocols other than outbound SMTP.
- No ability to telnet to port 25.
- No support for mail accounts other than admin or monitor.

8. Product audit/event reporting and summaries

Nokia IPSO logs activities to the syslog file via the syslogd daemon. This file can be rotated utilizing "cron", a basic UNIX daemon to execute scheduled commands, such as Monthly, Weekly, and Daily to move the logs to a compressed format in another directiory. A user can create a script that will automatically switch the log when run out of cron, and then mail the log entries for dropped packets to the system administrator as an e-mail attachment. This allows the user to maintain the logs and have information updated at a central administration device. The log format is standard syslog as defined within the kernel.

Standard output format to the syslog -

May 11 15:57:41 g12 [LOG_ERR] ipsrd[96]: OSPF IO: 172.22.10.3-224.0.0.5: no such configured address for packet received on interface eth-s2p1c0

There are times when it may be desirable to log some or all events to syslog instead of or in addition to FireWall-1 proprietary log files. This can be accomplished using the User-Defined Tracking function of FireWall-1 and the "logger" utility that comes with IPSO.

9. Product testing methodology

Nokia's internal Quality Assurance team performs feature by feature tests, system level tests, application level tests and stress/performance analysis tests. The Nokia Quality Assurance team consists of highly qualified and experienced engineers working closely with the product development engineers from functional specification, design and develpment of the product. The Quality Assurance team handles the following:

- Manage Risk
- Prevent Defects
- Detect Defects

- Demonstrate Functionality
- Measure Performance
- Predict Reliability
- Ensure Interoperability

Each of these goals are met through the Quality Assurance groups close attention to detail as well as working closely will all aspects of the product design, update, new feature release, and testing.

- Work with product teams

  Ensure testability is built-in
  Allocate test resources
  Track schedules

- Assign QA/Test individuals at product inception

  Team up with development - one to one
  Transfer developers knowledge to testers
  Implementation changes are tracked

- Establish shipment criteria

  The litany: Conformance, Performance, Reliability, Interoperability

- Focus on what the customer sees

  Ease of installation
  Ease of use
  Ease of maintenance
  Performance, performance, performance

What functions of this feature are tested.

- What performance benchmarks - are important for this feature
- What gets tested under cross-function System Testing
- What gets tested under Stress oriented System Testing

The first item namely "performance benchmarks" refer to the various measurements that are interesting to record as an indication of the goodness of the design and implementation. This should again cover all possible categories like:

Performance measurements regarding the installation of the Feature

Performance menasurements regarding rendering the feature active

Performance measurements regarding the configurational aspect of the feature

Performance menasurements regarding the core functions of the Feature

The second item namely "cross-function System Testing" refers to a style of testing which is considerate to other feature sets present in the product. These feature sets are either called out explicitly or are otherwise very fundamental to the product. When testing Firewall the important cross features that this feature is probably* fundamentally effected by are:

Interfaces (ATM, FDDI, Ethernet, HSSI, Frame Relay)

Routing Protocols (RIP, DVMRP, IGRP, OSPF)

Protocol oriented Traffic types (HTTP, FTP, TELNET)

Redundancy (VRRP)

Testing with investigate the effects of the following important Cross-feature items ALWAYS independent of what is being tested.

Routing Protocols (OSPF,RIP,IGRP,BGP,IGMP,DVMRP)

Interfaces (ATM 1483, Ethernet, FDDI, Frame Relay, X.21,V.35,HSSI)

Traffic Types (HTTP,FTP,TELNET, NFS, TCP, UDP,ICMP,ARP)

Third Party Software (Firewall)

Layer Two Devices (Hub, Ethernet Switches)

Layer three Devices (Routers)

The next item namely "stress oriented System Testing" refers to the style of testing where the implementation is tested for stability and reliability in a working network environment. This style of testing to stress the System.

Load Oriented Testing: Peak load condition

Volume Oriented Testing: Conditions of continous heavy load

Configuration Oriented Testing: Those legal hardware and or software configuration

Security Oriented Testing: Find ways to stress the security provisons of the System

Reliability Oriented Testing: Measure reliability and stability while the system is operating with a "typical" load

Recovery/Failover Oriented Testing: Behaviour of the system after the occurence of an error or an abnormal condition

Human Factors Oriented Testing; To identify some aspects of the feature that will be an inconvenience to the Human users

Nokia utilizes outside experts for both performance and interoperability for all Nokia IP Security Solution platforms.

UNH Interoperability lab is used to confirm the overall interoperablilty with various other vendors hardware/software solutions. The Nokia standards-based routing is architected to interoperate with all standards-based routers including Cisco, Bay, and 3Com.

KeyLabs is utilized by Nokia for performance evalutions on the Nokia platforms.

Nokia Testing Tools

Nokia currently run two distinct classes of applications on these boxes. The most common application performs normal data movement over sockets to generate a traffic load for test. This includes applications like tcpblast, ftp, traceroute, and some home-grown applications like ex, mr, and traffic. These applications have the desirable quality of performing operations over the network the way a user would.

The second application class involves controlling the network interface directly. This ``raw'' access to the port has been provided by either the ``gatm'' device driver in the IPSO kernel or through bpf in a standard FreeBSD system. This class includes programs like the GSMP and IFMP-C conformance test suites, various snooping/state verification tools, and the ANVL Test Suite.

Toolchest Kernel

The idea is to provide a standard platform that provides support for the existing applications as well as the primitives to build additional tools in the future. Toolchest is proprietary code built and used by Nokia Engineering and QA to test the IPSO kernel and associated hardware platforms.

The main architectural component of the Toolchest is the Network Interface Filter (NIF). A NIF is essentially a logical abstraction of the physical network interface that supports arbitrary filters up to 64 bytes long. A filter is essentially a pattern and mask that is compared against the incoming packets. There are two fundamental types of filters supported by the NIFs - Capture filters and counting filters.

- Capture filters are used to ``snoop'' packets on the NIF and pass then up the the user process space through the socket library.
- Counting filters simply keep track of the number of packets and bytes that are received by the kernel that match the filter.

The NIF also provides a handle to transmit packets. Each packet is treated as a raw byte stream which must include the link level information. To provide a consistent interface, this includes the ATM interface as well. This means that the first four bytes of a packet sent to or received from the ATM interface will be the VCI in network byte order.

In addition to the packet transmission and filtering capabilities, the kernel also includes a packet transmit scheduling mechanism. This allows the user to specify a packet train with relative time offsets between each packet down to sub-micro second resolution. Once all the packet definitions

are pushed down to the kernel, it can be sent into a loop transmitting the packets for a specified number of iterations. This of course means that the machine will not respond to user input until the packet transmission is complete.

Nokia QA uses many tools in its' comprehensive testing efforts:

- SmartBits/PowerBits
- ANVL
- QOSNetics
- ToolChest (variant of BSD)
- Sniffer Protocol Analyzer
- WebPerf
- NetPerf

10. Product performance attributes

Nokia has utilitzed the IPSO, a Unix-like operations system, which is customized to suport Nokia's enhanced routing capabilities and Check Point's FireWall-1 firewall functionality. The Ipsilon Routing Daemon (IPSRD) minimizes performance impact wherever possible.

11. Product operational assumptions

Nokia IP Security Solutions are designed to provide secure Internet access while maintaining the integrity of your private network. The Nokia integrated approach to the routing (IPSO) and firewall applications eliminates the need for separate intranet and access routers, management stations, and firewall servers.

Nokia IP Security flagship - the IP650 - offers carrier-class serviceability options such as hot-swappable interface cards, fan trays, and power supplies to the mission-critical network.

When price-per-port and interface diversity is the priority, the IP440 delivers. Up to sixteen interfaces with a wide range of choices offers flexibility and price-per-port performance required by ISPs and network managers alike.

Nokia's entry-level IP Security Solutions product, the IP330, is popular choice for both small offices and service providers offering managed firewall service.

Each IP Security Solutions product is secured by Check Point FireWall-1 software and supported

by Nokia advanced routing and system software. You choose the number of ports, interface diversity, serviceability, and size that are right for your network.

Nokia IP Security Solutions supports numerous standard network topologies dependant on the hardware platform selected by user. Only the IP330 is hardwired with 3 Ethernet/Fast Ethernet Ports.

IP650	IP440	IP330
Single-port T1 with CSU/DSU	4 Port Ethernet/Fast Ethernet	3 Ethernet/Fast Ethernet Ports
Single-port V.35/X.21 Serial	Single-port Ethernet/Fast Ethernet	Single-port T1 with CSU/DSU
Single-port HSSI	Single-port FDDI (DAS)	Single-port V.35 Serial
4 Port Ethernet/Fast Ethernet	Single-port ATM 155 UTP or MM Fiber	
Single-port X.21 Serial		
Single and Dual V.35/X.21 Serial	Single and Dual V.35/X.21 Serial	
Analog Modem (Optional)		
Single-port ATM MMF	Single-port T1 with integrated CSU/DSU	
Dual-port Ethernet/Fast Ethernet		
Single-port Token Ring UTP/STP	Single-port HSSI	
	Analog Modem (Optional)	

12. Product operational/management requirements and interface

Nokia IPSO requires initial configuration of interface, routing protocols enabled per interface, router services, traffic management, SNMP and various system configurations (i.e. database procedures, time and date procedures, hostname procedures, static host procedures, managing IPSO images, managing packages, and mail relay). Updates and patches wil need to be applied to devices as they are released by Nokia. In addition no other maintenance is required for the Nokia IPSO operating system.

All Nokia IP Security Solutions hardware devices are managed through Voyager. Voyager communicates with the routing sofware to configure interfaces and routing protocols, to manage routing policy for the firewall, and to monitor network traffic and protocoll performance. Voyager also provides online documentation. Voyager itself runs on a remote machine as a client application of the Nokia routing software and is HTML-based.

Nokia IP Security Solutions appliances Network Voyager management software is web-based HTML management application developed by Nokia to provide fully centralized remote management. With Voyager, one can manage, monitor, and configure any combination of the Nokia IP Security Solution family of products from any authorized location within the network.

Routing monitoring is available by following links from the individual protocol pages or by clicking the Monitor button on Voyager. Another monitoring tool is ICLID. This tool provides interactive, text-based monitoring of the routing subsystem.

Monitoring

Voyager supports online monitoring through the HTM-based interface for the following: routing protocols, resources, forwarding table, interface statistics, and hardware monitoring.

Routing Protocols
- OSPF - if enabled
- RIP - if enabled
- IGRP - if enabled
- DVMRP - if enabled
- IGMP - if enabled
- Route - Using this page, you can view the various route settings.
- Interface - Using this page, you can view the interface settings

Resource - Using this page, the user can view the Routing Resource settings.

Forwarding Table - This page displays the IP forwarding table that the kernel is using to make its forwarding decisions.

Interface Statistics - These pages display the statistics for each physical and logical interface. This includes input, output, errors, and miscellaneous.

Hardware Monitoring

System Status - Using this page, the user can monitor various elements of your system such as temperature, fan, power, and watchdog timer, as well as retrieve specific information on the installed power supplies. Status will only be displayed for elements that are relevant to your particular system.

CPI Slot Monitoring - Using this page, the user can monitor the status of the PCI slots in their machine. Status will only be displayed for the elements that are relevant to your particular system.

13. Product customer support

Software Updates

Nokia IPRG will provide free software updates to the End User who has purchased a Nokia Support Package whenever such updates are formally released by Nokia IPRG provided such upgrades do not include elements that are designated by Nokia IPRG as new products for which it charges a separate software license fee. Software updates are made available via the Web downloads and CDROM Media can also be ordered.

Technical Information

Nokia IPRG shall provide End User with password access to the Confidential and Proprietary Support pages on the Nokia IPRG corporate Web site. These pages contain technical information (including technical bulletins, FAQs and release documentation) that Nokia IPRG creates in support of its Product as well as information regarding open and solved known problems. Proactive Notification. Nokia IPRG shall provide e-mail notification of new releases and important
information. This e-mail is sent to registered users of the Support Web Site.

All Nokia IP Security Solution Appliances carry a 90 warranty. Customers should purchase a service contract as listed below.

SP-5001-000 Nokia End User Platinum Support Plus
Nokia IPRG's End User support programs are designed to provide End Users with a comprehensive package of support services that includes telephone assistance and support, hardware repair, software maintenance and access to technical information and expertise. These support services shall be provided by Nokia to the End User only for the products owned by the End User for which End User has paid to Nokia the applicable support services fees. The following are the highlights of the Nokia End User Platinum Support Plus program.

Technical Support (2hr Response).
Nokia IPRG shall provide telephone support to End User support staff. This service is performed by Nokia IPRG support personnel providing telephone support to End User's technical staff or by remotely accessing the end-user customer's equipment as required. Diagnostic Support is provided in English during the Principal Period of Support (PPS) which is defined as 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, exclusive of Nokia IPRG-observed holidays. Response guarantee from Nokia is 2 hours. Nokia Support can be contacted as follows:

· Call Us at 1-888-477-9824 or 1-408-990-2525
· Mail Us at support@iprg.nokia.com
· Submit Problem Report via Web

Network Emergency Assistance.
Nokia IPRG will provide technical support for "Network Emergencies" twenty-four (24) hours a day, seven (7) days a week. A Network Emergency is defined as a problem with the Product for which there is no workaround available and which renders the Product inoperative or causes it to fail catastrophically, with critical impact to the end-user's business if service is not restored quickly. Nokia IPRG reserves the right to charge the End User, at the time and material rates then in effect, for support services requested by End User outside the PPS if Nokia IPRG determines that the problems is not a Network Emergency.

SP-5002-000 Nokia End User Gold Support Plus
Nokia IPRG's End User support programs are designed to provide End Users with a comprehensive package of support services that includes telephone assistance and support, hardware repair, software maintenance and access to technical information and expertise. These support services shall be provided by Nokia to the End User only for the products owned by the End User for which End User has paid to Nokia the applicable support services fees. The

following are the highlights of the Nokia End User Gold Support Plus program.

Technical Support (4hr Response).
Nokia IPRG shall provide telephone support to End User support staff. This service is performed by Nokia IPRG support personnel providing telephone support to End User's technical staff or by remotely accessing the end-user customer's equipment as required. Diagnostic Support is provided in English during the Principal Period of Support (PPS) which is defined as 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, exclusive of Nokia IPRG-observed holidays. Response guarantee from Nokia is 4 hours. Nokia Support can be contacted as follows:

· Call Us at 1-888-477-9824 or 1-408-990-2525
· Mail Us at support@iprg.nokia.com
· Submit Problem Report via Web

SP-1004-000 Nokia VAR Platinum Support Plus
Nokia IPRG's Reseller support programs are designed to provide Resellers with a comprehensive package of support services that include telephone assistance and support, hardware repair, software maintenance and access to technical information and expertise. These support services shall be provided by Nokia to Reseller, and Reseller to its end users, only for the products owned by the reseller or its end users for which Reseller has paid to Nokia the applicable support services fees. The following are the highlights of the Nokia VAR Platinum Support Plus program.

Third Level Diagnostic Support (2hr Response).
Nokia IPRG shall provide telephone diagnostic support to Reseller's technical support staff. Reseller's support organization shall provide direct support to Reseller's customers and end-users. This service is performed by Nokia IPRG support personnel providing telephone support to Reseller's technical staff or by remotely accessing the end-user customer's equipment as required. Diagnostic Support is provided in English to Reseller during the Principal Period of Support (PPS) which is defined as 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, exclusive of Nokia IPRG-observed holidays. Response guarantee from Nokia is 2 hours. Nokia Support can be contacted as follows:

· Call Us at 1-888-477-9824 or 1-408-990-2525
· Mail Us at support@iprg.nokia.com
· Submit Problem Report via Web

SP-1003-000 Nokia VAR Gold Support Plus
Nokia IPRG's Reseller support programs are designed to provide Resellers with a comprehensive package of support services that include telephone assistance and support, hardware repair, software maintenance and access to technical information and expertise. These support services shall be provided by Nokia to Reseller, and Reseller to its end users, only for the products owned by the reseller or its end users for which Reseller has paid to Nokia the applicable support services fees. The following are the highlights of the Nokia VAR Gold Support Plus program.

Third Level Diagnostic Support (4hr Response). Nokia IPRG shall provide telephone diagnostic support to Reseller's technical support staff. Reseller's support organization shall provide direct support to Reseller's customers and end-users. This service is performed by Nokia IPRG support

personnel providing telephone support to Reseller's technical staff or by remotely accessing the end-user customer's equipment as required. Diagnostic Support is provided in English to Reseller during the Principal Period of Support (PPS) which is defined as 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, exclusive of Nokia IPRG-observed holidays. Response guarantee from Nokia is 4 hours. Nokia Support can be contacted as follows:

· Call Us at 1-888-477-9824 or 1-408-990-2525
· Mail Us at support@iprg.nokia.com
· Submit Problem Report via Web

14. Product interoperability considerations

The Nokia IPSO operating system supports a comprehensive suite of IP routing protocols including RIPv1/RIPv2, IGRP, OSPF, and BGP4 for unicast traffic and DVMRP for multicast traffic. IPSO also supports other router functions such as router discovery, full set IDR route aggregation, and route redistribution. Nokia IPSO supports Virtual Router Redundancy Protocol (VRRP) and firewall synchroniztion, enabling full load sharing active redunancy.

Voyager - Voyager communicates with the routing software to configure interfaces and routing protocols, to manage routing policy for the firewall, and to monitor network traffic and protocol performance. Voyager also provides online documentation. Voyager itself runs on a remote machine as a client application of the Nokia routing software and is HTML-based.

15. Glossary

15.1. Format

Newly added terms or annotated/re-interpreted glossary terms specific to this document are prefaced with a mark to denote the change or addition. Readers of this document are requested to pay special attention to such terms.

15.2. Glossary of Terms

Abuse of Privilege: When a user performs an action that they should not have, according to organizational policy or law.

Application-Level Firewall: A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Authentication: The process of determining the identity of a user that is attempting to access a system.

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

Authorization: The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.

Bastion Host: A system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., UNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

Challenge/Response: An authentication technique whereby a server sends an unpredictable challenge to the user, who computes a response using some form of authentication token.

Chroot: A technique under UNIX whereby a process is permanently restricted to an isolated subset of the filesystem.

Cryptographic Checksum: A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting filesystem tampering on UNIX.

Data Driven Attack: A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Defense in Depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

DNS spoofing: Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

Dual Homed Gateway: A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

Encrypting Router: see Tunneling Router and Virtual Network Perimeter.

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

Host-based Security: The technique of securing an individual system from attack. Host based security is operating system and version dependent.

Insider Attack: An attack originating from inside a protected network.

Intrusion Detection: Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

IP Splicing / Hijacking: An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

Least Privilege: Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

Logging: The process of storing information about events that occurred on the firewall or network.

Log Retention: How long audit logs are retained and maintained.

Log Processing: How audit logs are processed, searched for key events, or summarized.

Network-Level Firewall: A firewall in which traffic is examined at the network protocol packet level.

Perimeter-based Security: The technique of securing a network by controlling access to all entry and exit points of the network.

Policy: Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Proxy: A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Screened Host: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

Screened Subnet: A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.

Screening Router: A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.

Session Stealing: See IP Splicing.

Trojan Horse: A software entity that appears to do something normal but which, in fact,

contains a trapdoor or attack program.

Tunneling Router: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption.

Social Engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to systems.

Virtual Network Perimeter: A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks.

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

16. References to additional documents

Nokia Release Notes IPSO 3.2
© 1999 by Nokia Corporation, All Rights reserved.
Rights are reserved under the copyright laws of the United States.

Part Number: 45-0342-001
Version 3.2, September 1999

Nokia Voyager Reference Guide
© 1999 by Nokia Inc, All Rights reserved.
Rights are reserved under the copyright laws of the United States.

Part Number: 45-0231-001
March, 1999

Nokia IP600 Series Installation Guide
© 1999 by Nokia Inc, All Rights reserved.
Rights are reserved under the copyright laws of the United States.

Part Number: 45-0221-001
February, 1999

17. Appendices

Functional Summary Program: Contacts

How to contact the functional summary program group, for more information or to participate:

Email: **fwall-summaries@iwi.com**

Web: **http://www.iwi.com/sponsors.html**

Format version: 1.0 RELEASE

LEGAL NOTICE

NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR FOR BUSINESS INTERRUPTION ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SERVICE, EVEN IF NOKIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW EXCLUSION OF CERTAIN WARRANTIES OR LIMITATIONS OF LIABILITY, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THE LIABILITY OF NOKIA WOULD IN SUCH CASE BE LIMITED TO THE GREATEST EXTENT PERMITTED BY LAW.

For your easy accessibility Nokia may include links to sites on the Internet that are owned or operated by third parties. By linking to such third-party site, you shall review and agree to that site's rules of use before using such site. You also agree that Nokia has no control over the content of that site and cannot assume any responsibility for material created or published by such third-party sites. In addition, a link to a non-Nokia site does not imply that Nokia endorses the site or the products or services referenced in such third party site.

By submitting material to any of our servers, for example, by e-mail or via the Nokia World Wide Web pages, you agree that: (a) the material will not contain any item that is unlawful or otherwise unfit for publication; (b) you will use reasonable efforts to scan and remove any viruses or other contaminating or destructive features before submitting any material; and (c) you own the material or have the unlimited right to provide it to us and Nokia may publish the material free of charge and/or incorporate it or any concepts described in it in our products without accountability or liability (d) you agree not to take action against us in relation to material that you submit and you agree to indemnify us if any third party takes action against us in relation to the material you submit.

Nokia does not and cannot review the content posted by users on its site and is not responsible for such content. Nokia may at any time at its discretion remove any content posted by users.

Nokia is a registered trademark of Nokia Corporation. Nokia's product names are either trademarks or registered trademarks of Nokia. Other product and company names mentioned herein may be trademarks or trade names of their respective owners. Your access to this site should not be construed as granting, by implication, estoppel or otherwise, any license or right to use any marks appearing on the site without the prior written consent of Nokia or the third party owner thereof.