

Securing Nokia Network Voyager Guidelines

Prepared for:

FishNet Security Support Clients

Prepared by:

FishNet Security

FishNet Support and Piranha Team
Security Services

FishNet Security
1710 Walnut
Kansas City, MO 64108

Phone: 816-421-6611
Toll Free: 888-732-9406
Fax: 816-421-6677

Date Prepared:
October 28th, 2003

The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination or other use of or taking of any action upon this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability.

FishNet Security has conducted work associated with this report as an independent, third party vendor, and maintains no ownership or interest in the Client.

Copyright © 2003 FishNet Security. All rights reserved. The FishNet Security logo is a registered trademark of FishNet Security. All other products and company names mentioned herein are trademarks or registered trademarks of their respective owners.



General Information 1
 Company Background1

Executive Summary..... 2
 Purpose.....2
 Perspective.....2
 Securing Nokia Voyager3

General Information

Company Background

Founded in 1996, FishNet Security has become one of the country's leading and most respected innovators in the network security industry. FishNet Security is focused exclusively on network security. Our roots are grounded in the engineering and technical aspects of network security as opposed to consulting firms that have ventured resources into the network security arena. Our business foundations offer strength and stability that set us apart from the "dot-com" model.

Commitment to our Customers

Headquartered in Kansas City, Missouri, FishNet Security is committed to being the largest network security company in the Midwest. In order to provide superior customer service, FishNet has regional offices in St. Louis, Dallas, Minneapolis, and New York. Our management team works to ensure high level of service through frequent and direct contact with our customers.

Engineering Expertise

FishNet Security offers a technical staff with experience, training and industry certifications such as Check Point Certified Security Expert, Cisco Certified Internetwork Engineer (CCIE), Certified Information System Security Professional, Microsoft Certified System Engineer and more. Our engineers are certified in industry leading security product lines, and in the networking, operating system and routing foundations that underscore successful implementations.

Executive Summary

Purpose

FishNet Security would like to recommend that all Nokia customers review their Nokia IP Security platform configurations, specifically regarding Nokia Network Voyager, and ensure that they have followed vendor recommended guidelines and best practices in securing this platform.

FishNet Security Support Services and Assessment Services have observed Nokia Network Voyager configurations in production at client sites that include use of HTTP and lack granular client access restrictions. This puts the Nokia Network Voyager interface at unnecessary risk, and we highly recommend clients take the steps included in this document to mitigate any potential risks against this platform.

Perspective

Any security product or platform managed by insecure protocols, including HTTP, TELNET, and/or FTP should be considered at risk. Secure protocols, including HTTPS and SSH should be used at all times.

The information in this document is specific to Nokia's Network Voyager web interface to managing the IPSO platform, and does not cover all IPSO platform security recommendations. Conceptually, the same recommendations apply to IPSO as a whole: disable clear protocols like FTP and TELNET and replace them with cryptographically secure protocols like SSH. Restrict access to the interfaces to limited list of authorized clients.

This document was created in response to:

<http://www.fishnetsecurity.com/CSIRT/disclosure/Nokia/advisory.public.FN2003111001.txt>

Securing Nokia Voyager

This section describes techniques for locking down access to the Nokia Voyager interface. It is not intended to be a step-by-step implementation document; rather, it outlines high-level changes that can be implemented.

There are two groups of changes, Standard and Advanced. The Standard set requires less effort, and the changes should be implemented by most administrators. The Advanced set is more complex in terms of implementation and ongoing management, and the changes should be evaluated and implemented if they are deemed necessary.

Please note that this document applies only to the security of the Voyager interface, not the Nokia IP device in general.

Standard Security Practices

Configure SSL: The Voyager interface should always use at least 128-bit SSL. By default, the interface uses HTTP on port 80, which is undesirable for a number of reasons. Apart from the danger of sending the traffic in the clear, this also makes it easier for an attacker to use a spoofed source IP address (since there is no SSL negotiation).

The administrator is required to create a certificate and configure a required level of encryption (recommend 128 bit or greater). This process is straightforward and requires little maintenance. The certificate may either be an externally signed CSR, or a self-signed certificate.

Change the Voyager TCP Port: By default, Voyager over SSL will use the normal HTTPS port, 443. While using the default port can make administration easier, it can also lead to misconfiguration that allows an attacker access.

The best example of this would be when the firewall software is configured to allow the entire internal network access to any destination via HTTPS/TCP443. If there is not a superceding rule in place that prevents access to the Nokia device (or the rules are ordered improperly), this rule would allow any internal user access to the default Voyager port.

This port can be changed via the Voyager interface.

Configure Access Control: TCP/IP access to the Voyager port should be limited using some type of access control device. Ideally, this would be limited to a specified number of IP addresses that are controlled by the administrator.

In many cases, the Nokia IP appliance is used to run Check Point Firewall-1 software. In these instances, it is a simple procedure to allow and disallow access to the Voyager port. If the device is not running firewall software, an internal Access Control List (ACL) can be configured via the Voyager interface.

In an advanced configuration, the Nokia ACL can be used as added protection against firewall misconfiguration.

Caveat: If you enable Nokia ACLs, you will not be able to utilize flow acceleration in IPSO/Firewall-1. Flow acceleration has to bypass the ACL function.

Advanced Security Practices

Monitor and Audit: The Nokia device should be audited on a regular basis and/or monitored continuously for unwanted changes. SNMP can be configured to send traps to an SNMP trap receiver when configuration changes are made.

The Nokia device should be configured through the “System Logging” interface to log all management activity and record both transient and permanent changes. These changes should be logged to a dedicated log file, which can be monitored via the Voyager Monitoring interface (Management Activity Log).

Third party software is also available to monitor for, give a historical view of, and alert on changes. This includes products like Tripwire that can install on IPSO and monitor for unexpected changes, and products like Firemon (<http://www.firemon.com>) for auditing platform changes. Refer to the Nokia OK program for more information.

Independent Audit Trail: Nokia IPSO syslog features may also be utilized to remotely duplicate log entries. This would require a hacker to compromise at least two separate devices to cover their tracks.

Use Strong Authentication: The Voyager interface can be authenticated via AAA, allowing for the use of strong authentication. RADIUS or TACAS+ authentication mechanism can be applied to Voyager (HTTPD) access, which would allow for several strong authentication schemes.

Caution: When changing authentication schemes, care should be taken configuring the new authentication mechanism, as it is possible to entirely lock yourself out of the Voyager interface. This is not a flaw in Voyager or IPSO, but merely a reminder to follow vendor-supplied steps closely when enabling strong authentication.

Another strategy for strong authentication would be to configure SSH Client Authentication certificates and disable Voyager access via the network using the IPSO ACL feature.