Nokia IP VPN Technology Overview Version 1.0

Part No. N451099001 Rev A
Published November, 2003
Nokia Contact Information

<table>
<thead>
<tr>
<th>Nokia Internet Communications</th>
<th>Nokia House, Summit Avenue</th>
<th>438B Alexandra Road</th>
</tr>
</thead>
<tbody>
<tr>
<td>313 Fairchild Drive</td>
<td>Southwood, Farnborough</td>
<td>#07-00 Alexandra Technopark</td>
</tr>
<tr>
<td>Mountain View, CA 94043-2215</td>
<td>Hampshire GU14 ONG UK</td>
<td>Singapore 119968</td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Web Site: http://www.nokia.com

Telephone
- Americas: 1-888-477-4566 or 1-650-625-2000
- Europe: +44 161 601 8908
- Middle East, and Africa: +33 170 708 166
- Asia-Pacific: +65 6588 3364

Fax
- Americas: 1-650-691-2170
- Europe: +44 (0) 125-286-8900
- Middle East, and Africa: +44 (0) 125-286-5666
- Asia-Pacific: +65 67232999

Mail Address
- Americas: Nokia Inc.
- Europe: Nokia House, Summit Avenue
- Middle East, and Africa: Nokia House, Summit Avenue
- Asia-Pacific: 438B Alexandra Road

Address
- Americas: 313 Fairchild Drive
- Europe: Southwood, Farnborough
- Middle East, and Africa: Hampshire GU14 ONG UK
- Asia-Pacific: Singapore 119968

Nokia Customer Support

Web Site: https://support.nokia.com/

Email: tac.support@nokia.com

<table>
<thead>
<tr>
<th>Americas</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice:</td>
<td>Voice:</td>
</tr>
<tr>
<td>1-888-361-5030 or 1-613-271-6721</td>
<td>+44 (0) 125-286-8900</td>
</tr>
<tr>
<td>Fax:</td>
<td>Fax:</td>
</tr>
<tr>
<td>1-613-271-8782</td>
<td>+44 (0) 125-286-5666</td>
</tr>
</tbody>
</table>

Asia-Pacific

Voice: +65-67232999
Fax: +65-67232897
Contents

About This Guide ................................................. 9
In This Guide ..................................................... 9
Conventions This Guide Uses ................................. 10
  Notices ......................................................... 10
  Text Conventions ............................................. 11
Related Documentation ....................................... 11

1 Introducing the Nokia IP VPN ......................... 13
  Nokia IP VPN Gateways .................................. 14
  Nokia IP VPN Management ............................... 18

2 Using VPNs and Nokia IP VPN Gateways ........ 21
  Benefits of a Virtual Private Network ............. 21
  Creating a Nokia IP VPN .............................. 24
    Using IPSec .............................................. 26
  How IPSec Works ........................................... 28
    Security Associations .................................. 29
    Selectors .................................................. 29
    Security Association Database .................. 29
    Security Policy Database ......................... 30
  IKE Authentication Considerations ............. 30
    IKE Configuration Options ......................... 30
    IKE (Phase 2) Options ................................. 32
  Public-Key Infrastructure ......................... 33
  Preshared Keys .......................................... 34
  Raw Public Keys ......................................... 34
Public-Key Certificates ........................................... 35
Certificates ..................................................... 35
Certificate Revocation Lists ...................................... 36
Using an Internal CA .............................................. 36
Using an External CA ............................................. 37
Building a Virtual Private Network .............................. 37
Using IPSO Clustering ............................................ 38
Active Session Failover .......................................... 39
Dynamic Load Balancing ......................................... 40
Example Cluster .................................................. 41
Clustering Options ................................................ 42
Unicast Mode ....................................................... 43
Multicast Mode ..................................................... 43
Forwarding Mode ................................................ 43
Node Addition and Intracluster Communication .............. 44
Keepalive Referee ................................................ 44
Using NAT ......................................................... 45
Stateful Inspection Technology .................................. 46
Other Nokia IP VPN Gateway Features ........................ 46
Command-Line Interface ......................................... 47
Bootstrap Security Tokens ....................................... 47
Secure Communications ......................................... 47
Secure Shell ....................................................... 47
Secure Sockets Layer ............................................. 48
Secure Internal Communications ............................... 49

3 Designing a Nokia IP VPN ..................................... 51

Choosing a Network Topology .................................. 51
Single-Hub Topology ............................................. 51
Star Topology ..................................................... 52
Mesh Topology ................................................... 53
Partial Mesh Topology .......................................... 54
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Mesh Topology</td>
<td>55</td>
</tr>
<tr>
<td>Determining Gateway Placement</td>
<td>56</td>
</tr>
<tr>
<td>Using the Gateway Outside the Firewall</td>
<td>56</td>
</tr>
<tr>
<td>Forwarding IPSec Traffic Only</td>
<td>57</td>
</tr>
<tr>
<td>Forwarding Unencrypted and IPSec Traffic</td>
<td>58</td>
</tr>
<tr>
<td>Using the Gateway Inside the Firewall</td>
<td>58</td>
</tr>
<tr>
<td>Using the Gateway Parallel with the Firewall</td>
<td>61</td>
</tr>
<tr>
<td>Single Interface Configuration</td>
<td>63</td>
</tr>
<tr>
<td>Combining with the Firewall</td>
<td>64</td>
</tr>
<tr>
<td>Routing Considerations</td>
<td>64</td>
</tr>
<tr>
<td>Basic Routing Defined</td>
<td>64</td>
</tr>
<tr>
<td>Types of Routing</td>
<td>65</td>
</tr>
<tr>
<td>Supported Routing Protocols</td>
<td>66</td>
</tr>
<tr>
<td>High Availability</td>
<td>67</td>
</tr>
<tr>
<td>IPSO Clustering</td>
<td>67</td>
</tr>
<tr>
<td>Virtual Redundancy Routing Protocol</td>
<td>68</td>
</tr>
<tr>
<td>Comparing Clustering and VRRP</td>
<td>68</td>
</tr>
<tr>
<td>Using IPSO Clustering Versus VRRP</td>
<td>69</td>
</tr>
<tr>
<td>Address Translation Considerations</td>
<td>69</td>
</tr>
</tbody>
</table>

4 Implementing a Nokia IP VPN

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Nokia IPSO CLI</td>
<td>71</td>
</tr>
<tr>
<td>Using Nokia Network Voyager</td>
<td>72</td>
</tr>
<tr>
<td>Managing Policies with Check Point SMART</td>
<td>72</td>
</tr>
<tr>
<td>SmartCenter Server</td>
<td>74</td>
</tr>
<tr>
<td>SMART Client</td>
<td>74</td>
</tr>
<tr>
<td>Check Point Smart Large Scale Manager (SmartLSM)</td>
<td>75</td>
</tr>
<tr>
<td>Using VPN Communities</td>
<td>75</td>
</tr>
</tbody>
</table>
5 Managing a Nokia IP VPN ................................. 79
   Using NTP ........................................... 79
   Using Syslog ....................................... 80
   Using SNMP ........................................ 80
   Upgrading IPSO ..................................... 81
   Backing Up and Restoring Files ..................... 82
   Using Nokia Horizon Manager ....................... 82

6 Glossary ................................................. 85

A Overview of Standards and Protocols .................... 95
   IPSec ................................................. 95
      Authentication Header ............................ 96
      Encapsulating Security Payload ................. 96
      Message Digests .................................. 97
   Authentication Algorithms .......................... 97
      Message Digest 5 (MD5) .......................... 98
      Secure Hash Algorithm 1 (SHA-1) ............... 98
      RIPEMD ........................................... 98
   Algorithms .......................................... 98
   Lifetimes .......................................... 99
   Perfect Forward Secrecy ............................ 99
   Encryption Algorithms .............................. 100
      Advanced Encryption Standard .................. 100
      Data Encryption Standard ....................... 101
      Triple Data Encryption Standard ............... 101
      CAST ............................................ 101
      Blowfish ......................................... 102
      RC5 ............................................... 102
      Diffie-Hellman ................................... 102

Index ..................................................... 105
About This Guide

This manual is written for system administrators and other knowledgeable professionals who are deploying Nokia Internet Protocol (IP) virtual private network (VPN) gateways to create site-to-site virtual private networks. It provides information on how to design, implement, and manage VPNs and introduces new features for large-scale VPN infrastructure deployments. To use this guide, administrators should have a basic knowledge of IP networking, routing, and network architecture.

This preface provides the following information:

- In This Guide
- Conventions This Guide Uses
- Related Documentation

In This Guide

This guide is organized into the following chapters and appendixes:

- **Chapter 1, “Introducing the Nokia IP VPN”** provides an overview of the Nokia IP VPN including concepts and basic architecture.
- **Chapter 2, “Using VPNs and Nokia IP VPN Gateways”** describes the way a VPN works, the benefits a VPN provides, and the gateways that Nokia offers to implement a reliable, high-performance VPN.
- **Chapter 3, “Designing a Nokia IP VPN”** describes how to determine the placement of Nokia IP VPN gateways in an existing network. This
Chapter also summarizes the changes you might need to make to the connections or configurations of your routers or firewalls to implement a VPN.

- Chapter 4, “Implementing a Nokia IP VPN” describes how to implement and configure a VPN by using the Nokia IPSO CLI, Nokia Network Voyager, Check Point SmartClient, and Nokia Horizon Manager.
- Chapter 5, “Managing a Nokia IP VPN” describes how to manage a Nokia IP VPN by using Nokia Horizon Manager, SNMP, and IPSO services.
- Appendix A, “Overview of Standards and Protocols” provides a brief introduction to the standard protocols and technologies used to implement a VPN with Nokia IP VPN products.

Conventions This Guide Uses

The following sections describe the conventions this guide uses, including notices and text conventions.

Notices

---

**Note**

Notes provide information of special interest or recommendation
Text Conventions

Table 1 describes the text conventions this guide uses.

Table 1  Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monospace font</td>
<td>Indicates command syntax, or represents computer or screen output, for example:</td>
</tr>
<tr>
<td></td>
<td>Log error 12453</td>
</tr>
<tr>
<td><strong>bold monospace font</strong></td>
<td>Indicates text you enter or type, for example:</td>
</tr>
<tr>
<td></td>
<td># configure nat</td>
</tr>
<tr>
<td>Key names</td>
<td>Keys that you press simultaneously are linked by a plus sign (+):</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl + Alt + Del.</td>
</tr>
<tr>
<td>Menu commands</td>
<td>Menu commands are separated by a greater than sign (&gt;):</td>
</tr>
<tr>
<td></td>
<td>Choose File &gt; Open.</td>
</tr>
<tr>
<td>The words enter and type</td>
<td>Enter indicates you type something and then press the Return or</td>
</tr>
<tr>
<td></td>
<td>Enter key.</td>
</tr>
<tr>
<td></td>
<td>Do not press the Return or Enter key when an instruction says type.</td>
</tr>
<tr>
<td><em>italics</em></td>
<td>• Emphasizes a point or denotes new terms at the place where they are defined in the text.</td>
</tr>
<tr>
<td></td>
<td>• Indicates an external book title reference.</td>
</tr>
<tr>
<td></td>
<td>• Indicates a variable in a command:</td>
</tr>
<tr>
<td></td>
<td>delete interface if_name</td>
</tr>
</tbody>
</table>

Related Documentation

In addition to this guide, documentation for this product includes the following:

- *Nokia IP VPN Gateway Getting Started*—provides a brief overview about how to configure and build a Nokia IP VPN.
- **Nokia IP VPN Gateway Release Notes**—provides important information you should know before you install and configure your Nokia IP VPN.

- **Nokia IPSO 3.7 Clustering Configuration Guide**—provides an overview of IPSO clustering, configuring and managing a cluster, configuring VPN-1/FireWall-1 clustering, and clustering examples.

- **Nokia CLI Reference Guide for IPSO 3.7**—provides information about how to create and implement command-line interface commands that are applicable to IPSO 3.7.

- **Nokia Network Voyager Reference Guide**—provides information about the Nokia Voyager software used to configure interfaces and routing protocols, manage firewall routing policies, and how to monitor network traffic and protocol performance.

- **Nokia IP40 Quick Start Guide**—provides a quick reference about configuring features for the Nokia IP40.

- **Nokia IP40 User’s Guide**—provides information and procedures about installing and configuring the Nokia IP40.

- **Nokia IP40 CLI Reference Guide**—provides information about how to create and implement command-line interface commands that are applicable to the Nokia IP40.

- **Nokia Horizon Manager User’s Guide**—provides information about the Nokia Horizon Manager (NHM) software that allows administrators to perform remote, centralized upgrades and maintenance of multiple IP security appliances simultaneously.
Introducing the Nokia IP VPN

The Nokia Internet Protocol (IP) virtual private network (VPN), is a joint initiative between Nokia and Check Point that delivers features for large-scale IP VPN infrastructure deployments. This VPN solution is targeted for enterprises with hub-and-spoke or star topologies that scale thousands of sites. Nokia delivers a single cohesive set of capabilities for scalable IP VPN end-to-end and provides a new class of availability and performance in Nokia IP VPN gateways.

Nokia IP VPN delivers the following features:

- Full suite of IPSec VPN protocols
- Integrated routing and security
- Robust high-availability features
- Optimized branch office solutions
- End-to-end management

Three major components comprise the Nokia IP VPN architecture:

- Central office gateways
- Branch office gateways
- Management systems

From these basic building blocks, a full range of IP VPN solutions are possible. The Nokia IP VPN architecture includes both Nokia and Check Point components. A summary of these hardware and software components follows.
Nokia IP VPN Gateways

The Nokia IP VPN solution is deployed by using Nokia IP VPN gateways. The gateway consists of a combination of Nokia hardware, the IPSO operating system, and Check Point software. The following table lists the Nokia IP VPN central office and branch office gateways and the features they support.

<table>
<thead>
<tr>
<th>Nokia IP VPN Features</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nokia IP1260</td>
<td>Nokia IP40</td>
</tr>
<tr>
<td></td>
<td>Nokia IP380</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nokia IP350</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nokia IP130</td>
<td></td>
</tr>
</tbody>
</table>

**VPN Protocols**

- **IPSec VPN transport**: x x
- **IKE key management**: x x
- **Diffie-Hellman Groups 1, 2, and 5**: x x
- **Perfect Forward Secrecy**: x x
- **SHA1 data integrity**: x x
- **MD5 data integrity**: x x
- **AES-256, 192, and 128 data encryption**: x x
- **3DES data encryption**: x x

**Access Control**

- **Stateful Inspection firewall**: x x
- **Network address translation**: x x
## Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.509v3 digital certificates</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Preshared secrets</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

## PKI Support

<table>
<thead>
<tr>
<th>PKI Support</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal certificate authority</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>External certificate authority</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Certificate enrollment requests (with PKCS#7 and PKCS#10)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Certificate revocation lists (CRLv2)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Secure private-key handling</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Distributed-key management</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

## Dynamic Addressing

<table>
<thead>
<tr>
<th>Dynamic Addressing</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>DHCP client</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PPPoE</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>DDNS client</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

## Routing Services

<table>
<thead>
<tr>
<th>Routing Services</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border Gateway Protocol (BGP-4)</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Nokia IP VPN Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nokia IP 1260</td>
<td>Nokia IP380</td>
<td>Nokia IP40</td>
</tr>
<tr>
<td>Nokia IP 350</td>
<td>Nokia IP130</td>
<td></td>
</tr>
<tr>
<td>Open Shortest Path First (OSPFv2 and v3)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Routing Information Protocol (RIPv1 and v2)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Distance Vector Routing Protocol (DVMRP)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Protocol Independent Multicast (PIM-SM and PIM-DM)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Static routes</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Fault Tolerance

<table>
<thead>
<tr>
<th>Feature</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nokia IP Clustering with SA load balancing</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Full-state synchronization</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRPv2)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Multihomed Internet access</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Multihomed IPSec tunnels</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>WAN backup with encryption</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Dial backup over PPP with encryption</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Known good state recovery</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>No moving parts design</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Dual hot-swap HDD with RAID disk mirroring</td>
<td>IP1260 only</td>
<td></td>
</tr>
<tr>
<td>Dual hot-swap power supplies</td>
<td>IP1260 only</td>
<td></td>
</tr>
</tbody>
</table>
### Nokia IP VPN Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nokia IP1260</td>
<td></td>
<td>Nokia IP40</td>
</tr>
<tr>
<td>Nokia IP380</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia IP350</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia IP130</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nokia IP40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual hot-swap fan assembly</td>
<td>IP1260 only</td>
<td></td>
</tr>
<tr>
<td>Hot-swap interface cards</td>
<td>IP1260 only</td>
<td></td>
</tr>
<tr>
<td>Built-in encryption accelerator</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Element Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Web-based graphical user interface with SSL</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Secure command-line interface with SSHv2</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Network Time Protocol (NTP) over IPSec</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>SNMPv3 monitoring</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SNMPv2 monitoring over IPSec</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Syslogd logging over IPSec</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Out-of-band management through PPP</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Advanced staging configuration</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>Nokia Horizon Manager Support</strong></td>
<td>v1.3.1 or later</td>
<td>v1.3.1 or later</td>
</tr>
<tr>
<td>Do-no-harm upgrades (requires Nokia Horizon Manager)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Software and hardware inventory</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
The management system for the Nokia IP VPN solution consists of two primary components: system management tools that Nokia provides and policy management tools that Check Point provides. These management systems include:

- **System management**—management of the information technology systems in an enterprise. Management services report, monitor, and analyze the entire infrastructure. Network management services include NTP, syslog, SNMP, the IPSO CLI, Nokia Network Voyager and Nokia Horizon Manager. You can upgrade, back up, or restore the IPSO operating system software by using the CLI, Voyager, or Nokia Horizon Manager. In addition, you can manage your system by configuring features such as high availability and routing.

- **Policy management**—enables administrators to centrally manage and deploy a single policy to a large number of VPN-1/FireWall-1 enforcement points. Once a policy is defined, you can automatically distribute it to all locations. This distribution dramatically increases management efficiency and strengthens security because the security policy is always up-to-date at all security enforcement points.

You can manage policies with Check Point SmartCenter, IPSec policies, and access control lists (ACLs). Examples of policy management include

### Nokia IP VPN Features

<table>
<thead>
<tr>
<th>Nokia IP VPN Features</th>
<th>Central Office</th>
<th>Branch Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure remote script execution</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Template-based configuration</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Nokia IP1260</td>
<td>Nokia IP380</td>
<td>Nokia IP350</td>
</tr>
<tr>
<td>Nokia IP350</td>
<td>Nokia IP130</td>
<td>Nokia IP40</td>
</tr>
</tbody>
</table>

### Nokia IP VPN Management
internal or external CAs, key generation, and certificate enrollment and revocation.

The following chapters discuss how a VPN works, the benefits that a VPN provides, placement of Nokia IP VPN gateways in the network, managing and implementing a VPN, and a brief overview of IPSec standards and protocols.
Using VPNs and Nokia IP VPN Gateways

This chapter describes the way a virtual private network (VPN) works, the benefits a VPN provides, and the gateways that Nokia provides to implement a reliable, high-performance VPN. This chapter contains the following sections:

- Benefits of a Virtual Private Network
- Creating a Nokia IP VPN
- How IPSec Works
- Building a Virtual Private Network
- Using IPSO Clustering
- Stateful Inspection Technology
- Other Nokia IP VPN Gateway Features

Benefits of a Virtual Private Network

A VPN connects networks in different geographic regions over the Internet, while ensuring the privacy and integrity of the transmitted information. A VPN provides a cost-effective, reliable, and secure alternative to a traditional private network.

In a traditional private network, an organization uses leased or switched lines that the long-distance telecommunications network provides. Figure 1
illustrates a private network with WAN links interconnecting a number of branch office LANs and the headquarters (HQ) LAN. In this kind of network, each pair of networks requires a separate link with a router at the end of each link.

Figure 1  A Traditional Private Network

A traditional private network is expensive to establish and maintain. Network costs and administrative overhead increase exponentially as more sites are added to the network. Typically, network designers use a hub-and-spoke configuration to reduce the many-to-many scalability problem. However, using hubs to concentrate network traffic introduces performance and reliability problems, which can only be solved by increasing the cost and complexity of the network.

The Internet was specifically designed to quickly route traffic between any two connected points and to solve the scalability problems encountered in establishing networks with point-to-point links. However, the Internet is composed of countless network devices administered by many organizations. No organization can control or be responsible for the privacy or integrity of information transmitted over the Internet. A variety of well-publicized
attacks, worms, and viruses have made it obvious that the Internet is inherently insecure.

A VPN, as illustrated in Figure 2, lets you take advantage of the strengths of the Internet, while providing encryption and authentication features to address the lack of security on the Internet. A VPN is virtually private because it provides encryption and security mechanisms for using the Internet to interconnect the regional networks of an organization without putting private data at risk.

**Figure 2 A Virtual Private Network (VPN)**

Although a VPN can provide various benefits, the main purpose for implementing a VPN is to provide greater security for transmitting and receiving traffic over the Internet. Providing Internet security requires that you address a number of specific issues, including:

- **Message integrity**—ensures that data is not altered in transit over the network. This ability prevents an attacker from changing the contents of a
message that a legitimate user sends and assures the recipient that the message received is exactly what the sender transmitted.

- **Privacy**—prevents eavesdropping by unauthorized network users and assures confidentiality of information.

- **Authentication**—identifies the parties exchanging messages so that each party can be sure they know with whom they are communicating.

- **Replay protection**—ensures that data packets are not captured in transit and retransmitted another time. Replay protection prevents certain man-in-the-middle attacks that might be otherwise difficult to defend against.

In addition to security benefits, a VPN can help with addressing problems that can occur when you connect a private network to the Internet. Many companies have implemented TCP/IP networks without any intention of connecting to the Internet, and therefore use IP addressing schemes based on private IP addresses, which cannot be routed over the Internet. These address ranges include the following:

- Class A networks: 10.xxxx.xxx.xxx
- Class B networks: 192.168.xxx.xxx

You can use VPNs to connect subnetworks that use these private IP addressing ranges over the Internet. The original packet address is encapsulated within another frame or packet, which hides these internal addresses from routers on the Internet.

**Creating a Nokia IP VPN**

The Nokia IP VPN solution is based on IPSec, the IETF standard for securing communications over the Internet. This solution is composed of the Nokia IP VPN gateways and the Nokia IP VPN management system.

Together, these hardware and software products provide a secure, reliable, high-performance VPN that is easy to implement and maintain, and that scales easily as network requirements grow. This section describes how these products work together to provide the infrastructure required to implement a VPN.
In the Nokia VPN gateway product line, a gateway is one or more devices that work together. A gateway usually has two IP interfaces and appears to the network very much like an IP router.

While a normal IP router passes the packets from one interface to the next, a security gateway has an additional function. For each packet, the gateway consults an internal database, called the security policy database (SPD). Based on the entries in the SPD, the gateway takes one of the following three actions:

- Pass, without modification
- Drop, without further inspection
- Protect, by performing authentication and (usually) encryption operations, based on the security policy for the VPN

As Figure 3 shows, to build a VPN, you place Nokia IP VPN gateways between your private networks and the Internet. Data transmitted to a remote network from each private network is received by each gateway and is encrypted before the data is transmitted over the Internet. When encrypted data is received from the Internet, the gateways decrypt the data and forward it to the private network.

**Figure 3 Using a Nokia IP VPN Gateway**

---

**Note**

*Figure 3* shows a Nokia IP VPN gateway outside a firewall and between the firewall and the VPN gateway. However, the actual placement can
vary according to the design of your network. For information about placement options, see Chapter 3, “Designing a Nokia IP VPN.”

Nokia IP VPN gateways are designed to support IPSO clustering, a Nokia patented technology. With IPSO clustering, a number of individual gateways can function as a single gateway. Clustering uses dynamic load balancing to allow greater throughput than a single device provides and uses active session failover to provide redundancy required to eliminate a single point of failure. For more details about clustering, see “Using IPSO Clustering” on page 38.

Using IPSec

A VPN works by creating secure tunnels between networks connected over the Internet. A VPN tunnel is built by adding authentication and encryption mechanisms to existing protocols. A VPN is built on protocols implemented at different layers of the OSI 7-layer model, as summarized in Table 3.

Table 2 OSI Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Name</th>
<th>Example</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>Data link layer</td>
<td>Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) built over Point-to-Point Protocol (PPP)</td>
<td>Uses password authentication to prevent unauthorized dial-up connections.</td>
</tr>
<tr>
<td>Layer 3</td>
<td>Network layer</td>
<td>IPSec built over IP</td>
<td>Authenticates and encrypts data transmission by adding network layer information to each packet.</td>
</tr>
<tr>
<td>Layer 4</td>
<td>Transport layer</td>
<td>Secure Shell (SSH) built over TCP</td>
<td>Provides secure shell communication over TCP.</td>
</tr>
</tbody>
</table>

The IPSec protocol was specifically developed to address the limitations of layer 2 security protocols such as PPTP and L2TP. The Nokia IP VPN solution is built with IPSec, the only VPN protocol that provides a full range
of security features in an interoperable, scalable, and virtually transparent way.

The IPSec protocol provides a transparent, secure communication mechanism to use over shared or public networks. IPSec was defined within the IETF to provide a set of open standards security services for the Internet Protocol (IP). The IPSec protocol provides integrity and authenticity checking, which detects changes that might have occurred to packets during transmission. It also provides privacy to ensure that secure communication can occur even on unsecured networks. In addition, IPSec provides replay protection, which ensures that a valid data packet is not captured and resent to a device.

Two of the key advantages of IPSec over other security mechanisms are interoperability and adaptability. Devices running different operating systems and residing on different types of networks can communicate securely by using IPSec. Any IPSec-compliant network device can communicate securely with any other IPSec device. Also, as new techniques for encryption and authentication emerge, the IPSec standard can be expanded to include new developments with no effect on existing implementations.

IPSec provides two main protocols:

- AH (Authentication Header)
- ESP (Encapsulated Security Protocol)

The AH protocol is an older protocol that provides a strong form of authentication but lacks any features to prevent eavesdropping or altering a message in transit. For this reason, AH is supplanted by ESP, which provides similar authentication mechanisms, but includes strong encryption features to ensure message integrity and confidentiality.

Although you can implement IPSec ESP in a number of ways, it is commonly used for establishing an encrypted tunnel between IPSec gateways or between an IPSec client and a gateway. For information about the other ways IPSec is implemented, see Appendix A, “Overview of Standards and Protocols.”

Figure 4 shows how IPSec tunnels are used to create a site-to-site VPN by establishing secure communications between security gateways. The IPSec protocol is also used to allow secure remote access by establishing a tunnel
between an IPSec client and a security gateway. Other remote access scenarios can be implemented by combining IPSec with other remote access protocols.

**Figure 4 IPSec Tunnel Mode**

How IPSec Works

The IPSec protocol combines a number of pre-existing protocols into a coherent framework for establishing secure communication over TCP/IP networks. This section briefly describes how you implement a VPN with Nokia IP VPN gateways including:

- Security Associations
- Selectors
- Security Association Database
- Security Policy Database
- IKE Authentication Considerations
Security Associations

The IPSec protocol authentication and access control is based on security associations (SAs), which are negotiated between the two end points on an IPSec tunnel. An SA describes the encryption and authentication parameters that both end points agree to use. The SAs are stored in an SA database that each gateway maintains and are referenced by a unique security parameter index. You can assign a lifetime to an SA so that it expires after a given period of time. This lifetime limits the time a potential attacker has to eavesdrop or otherwise compromise the security of the connection.

Selectors

To create an SA, the proper selector must be defined on both end points. Selectors are essentially access list entries, which map IP packets to IPSec policy. Selectors identify source and destination IP addresses as well as IP protocols. They can also include port numbers when this degree of detail is necessary. When a selector matches a packet, it can apply one of three processing mechanisms to a packet flow:

- Drop
- Bypass (pass without protection)
- Apply security (protect with IPSec)

Ideally, these selectors are identical on both gateways at each end of the VPN tunnel. This redundancy ensures that the common security policies of both sides are enforced.

Security Association Database

The SA database contains all of the SAs that a device negotiates. The SA database is examined by an IPSec device every time an inbound or outbound IP packet passes. This database contains authentication and encryption parameters for each SA, including the SA, SA lifetime, sequence numbers for
antireplay protection, the IPSec protocol mode (tunnel or transport), and the path maximum transmission unit (MTU).

Security Policy Database

The security policy database stores the selectors and the action to be taken (drop, bypass, or apply security) if the packet matches. If the action taken is to apply security, the details are retrieved from the SA database.

IKE Authentication Considerations

The Internet Key Exchange (IKE) is a standardized protocol used to negotiate secure communications between IPSec peers and to automatically create security associations (SA). The IKE SA works in both directions, therefore only one IKE SA is required for each pair of gateways or other IPSec end points. This section discusses the IKE configuration options and authentication methods that enables IKE to be used in large, dynamic networks. This section includes the following subsections:

- IKE Configuration Options
- Public-Key Infrastructure

IKE Configuration Options

A VPN is a network that uses encrypted tunnels to exchange securely protected data. The encrypted tunnels are created by using the Internet Key Exchange (IKE) and IPSec protocols. IKE creates the VPN tunnel and the tunnel is used to transfer IPSec encoded data. Information can be securely exchanged only if the key belongs exclusively to the communicating parties.

The goal of IKE is for both sides to independently produce the same symmetrical key. This key then encrypts and decrypts the IP packets used in the transfer of data between VPNs.
How IPSec Works

This agreement about keys and methods of encryption must be performed securely. For this reason, IKE is composed of two phases. The first phase lays the foundation for the second. The two phases are as follows:

- IKE (Phase 1) Options
- IKE (Phase 2) Options

**IKE (Phase 1) Options**

Phase 1 or Main Mode establishes an IKE SA. Phase 1 requires three steps to establish the IKE SA:

- **Negotiation of the attributes of the IKE SA**—establishes common parameters that both peers (gateways or IPSec clients) can use.
- **Diffie-Hellman key exchange**—establishes a shared secret that uses a large prime number, called a Diffie-Hellman group.
- **Peer authentication**—establishes the identity of both peers.

You can decide on most of the attributes of the IKE SA negotiated in the first step of a Main Mode exchange when you configure your gateway.

The IKE policy determines how security gateways build their IKE security associations (SAs) during Phase 1 (Main Mode) of IPSec negotiation.

**Diffie-Hellman Group Number**

Currently five Diffie-Hellman (DH) groups are defined for IKE. The group ID gives you parameters to use in the DH exchange to generate the shared-secret keying material. Larger groups provide stronger shared secrets by using larger prime number exponentiation, but require computation. Nokia supports Group 1, Group 2, and Group 5. Groups 3 and 4 are elliptic curve groups, which are not supported in IPSO. Stronger, more secure keying material is derived from Group 5, Group 2 is less secure, and Group 1 is the least secure.

**Lifetime**

Lifetime is used to determine how long an IKE SA uses an existing set of DH keys before it needs to rekey. Considerably less traffic is generated on the IKE SA than on the IPSec SAs, since the IKE SA is used only to negotiate SAs for
IPSec. This indicates that the IKE SA lifetime is much longer than the lifetime of the IPSec SA.

IKE (Phase 2) Options

Phase 2 or Quick Mode uses an existing IKE SA to establish an IPSec SA for the actual exchange of encrypted data. A Quick Mode exchange is a negotiation of the parameters of IPSec SAs. This negotiation step is similar to the one performed in the Phase 1 exchange (in that one side offers choices and the other side either picks one or rejects the establishment of a tunnel), but the actual attributes for negotiation are different because these are specific to IPSec. These attributes include the protocol (AH or ESP) and any other necessary attributes, such as key length for variable keyed ciphers and a lifetime.

After completion of a Quick Mode exchange, IKE delivers the IPSec SAs to the SA database (SADB), and IPSec can immediately begin using them. The IKE SA can remain idle and negotiate more IPSec SAs at a later time.

This section describes the parameters you can set to use during Phase 2 (Quick Mode) of IPSec negotiation including:

- Perfect Forward Secrecy
- Diffie-Hellman Group Number
- Commit Bit
- Lifetime

Perfect Forward Secrecy

You can use perfect forward secrecy (PFS) in Phase 2 of IKE to ensure that a new Diffie-Hellman key exchange is made each time a new IPSec SA is established. If PFS is not specified, the keying material can be obtained from the keying material negotiated in Phase 1 by using a pseudo-random function over the original keying material.

Diffie-Hellman Group Number

The Diffie-Hellman group is configured in Phase 2 if and only if PFS is enabled.
Commit Bit

A Quick Mode exchange is composed of three messages. Upon receipt of the second message, the initiator of the protocol has all of the information necessary to create the IPSec SAs, while the responder must wait for the final message. Therefore a small window is available where the initiator can send IPSec-protected packets to the responder before the responder is ready—that is, before the responder has a chance to process the final Quick Mode message and create copies of the SAs.

The commit bit is used to extend Quick Mode to four messages. The final message is from the responder back to the initiator. When the commit bit option is used, the initiator does not complete its SAs until this final message is received. This procedure allows the responder to complete its SAs before it receives IPSec traffic.

The commit bit option is the default for Nokia IKE negotiation, but for traffic that is not sensitive to packet loss this option can be disabled, which results in IPSec SAs being established more quickly.

Lifetime

Lifetime is used to determine how long the IPSec SA can be used before a new SA must be established. This interval can be specified in either time or traffic volume or both.

Public-Key Infrastructure

Public-Key Infrastructure (PKI) provides scalable authentication methods that enables IKE to be used in large, dynamic networks. PKI manages the public keys required for public- and private-key authentication.

Public-key encryption, also called asymmetric encryption, uses a pair of keys, called the public key and private key. Symmetric encryption uses the same key to encrypt and decrypt messages.

Public-key encryption uses one key to encrypt a message and another to decrypt the message. The public key is distributed freely, while the private key is kept secret. Only the owner of the private key can read a message.
encrypted with the public key or generate a message that can be decrypted with the public key.

Whichever method of authentication you choose has important implications for your VPN design. The IKE protocol supports three authentication methods for establishing a secure authentication channel:

- Preshared Keys
- Raw Public Keys
- Public-Key Certificates

Note
The IPSec end point at each end of an IPSec tunnel must use the same method for authentication.

Preshared Keys

Preshared keys are essentially the same as passwords, and must be kept secret. Preshared keys are more likely to interoperate with security products from different vendors. However, because each pair of IPSec end points should have a unique preshared key, preshared keys can pose manageability and scalability problems. Also, the preshared key method lacks an automatic mechanism to deal with a compromised key. In such an event, all hosts on the network must be reconfigured.

If you choose to use preshared keys, Nokia recommends that they be a minimum of 20 characters long, difficult to guess, randomly generated, and changed on a regular basis.

Raw Public Keys

Using a raw public key is better than using preshared keys because the portion of the public-private key pair that is distributed does not need to be kept secret. Only the public key is distributed.
However, because each IPSec end point has a unique public-private key pair, this mechanism also suffers from manageability and scalability problems. Although management software might make administration easier, this authentication method can be cumbersome in dynamically changing networks. Any change to a raw public key must be distributed to any nodes that need to establish an IKE and IPSec tunnel with the node that has the changed key.

**Public-Key Certificates**

If scalability is required, it is a good idea to use public-key (digital) certificates. Digital certificates, based on the X.509v3 protocol, scale better than raw public keys because a public-key certificate require that you apply changes to a single node only.

The use of certificates solves scalability problems because devices are configured to trust a small number of CAs rather than a large number of potential users. Certificates solve manageability problems because PKI provides methods for issuing, distributing, and revoking certificates. When you use digital certificates, you do not have to configure each IPSec gateway with a preshared key or a public key for each IPSec end point. Instead, you configure the gateway to trust a CA and the certificates it issues.

---

**Note**

SmartCenter generates Nokia IP40 gateway certificates. Nokia central branch gateways certificates are generated locally during the installation and configuration of the Check Point software.

---

**Certificates**

A certificate binds an entity to a public key, which is signed to give it authenticity. A public-key certificate is a collection of attributes (such as a name and a public key) that is digitally signed by a trusted third party, called the certificate authority (CA). Certificate authorities (CAs), are entities that validate identities and issue certificates. They can be either independent third
parties such as VeriSign or organizations running their own certificate-issuing server. The integrity of the CA ensures that the attributes contained in a certificate belong to the individual or entity named in the certificate—the Subject of the certificate. PKI includes all of the services that are used to issue, distribute, validate, and revoke public-key certificates.

**Certificate Revocation Lists**

The Nokia IP VPN provides support for certificate revocation lists (CRLs). CRLs are certificates that are suspended or revoked by the CA before their expiration dates. The list generally indicates the name of the CRL issuer, the date of issue, the date of the next scheduled CRL issue, the serial numbers of the suspended or revoked certificates, and the specific times and reasons for suspension and revocation.

The Nokia IP VPN gateway provides a blocked certificate list, which is a more convenient mechanism that allows the VPN administrator to revoke any certificates from any CA. By placing a certificate on the blocked certificate list, the certificate is treated as if it was revoked by the issuer of the certificate and is not accepted by any gateway within the VPN.

**Using an Internal CA**

The Nokia IP VPN gateway provides an internal CA that you can use to issue the certificates required to implement your PKI. However, if you want other vendors to accept your certificates, you might need at least some certificates from an external CA. If you obtain certificates from an external authority, you can import a root certificate to your internal CA, or import device certificates to your Nokia IP VPN gateways. You can then use the internal CA on the Nokia IP VPN gateway to issue client certificates.

Any cluster can serve as a CA for the entire VPN. This CA can issue and sign certificates for clusters and remote clients. The internal CA generates standard ISO X.509v3 certificates through the Check Point SMART software. You can export these certificates from this software, which is encoded in standard privacy enhanced mail (PEM) format.
Check Point uses an internal certificate authority (ICA). The ICA is created during the SmartCenter server installation process and is responsible for issuing certificates for authentication. For example, ICA issues certificates, such as SIC certificates, for authentication purposes to administrators, and VPN certificates to users and gateways.

**Using an External CA**

For the Nokia IP VPN gateway to use certificates that an external CA generates, the CA must be able to issue certificates in response to certificate signing requests (CSRs) in PKCS#10 format. The issued certificates need to contain the `SubjectAltName` extension. The `SubjectAltName` certificate extension contains the Internet *names* of the certificate owner, such as an IP address.

The Nokia IP VPN gateway can use any X.509v3-compliant certificate that contains the following:

- An RSA signature key between 512 and 2048 bits long
- The `SubjectAltName` extension
- The gateway IP addresses in the `IPAddress` field of the `SubjectAltName` extension.

For `SubjectAltName` in the Nokia IP VPN gateway, the two supported options are IP address and DNS name. Only the address of the interface that sends or receives IPSec traffic, usually the external address, is specified in the certificate.

**Building a Virtual Private Network**

To create a VPN, use security gateways to interconnect separate networks over the Internet. You can establish site-to-site VPNs in a number of different scenarios, including:

- Both gateways on a private local area network
- Both gateways on a wide area network (WAN) connected over private leased lines
Using VPNs and Nokia IP VPN Gateways

- Branch office connection to headquarters over the Internet
- A partner-to-partner tunnel over the Internet or any shared network

In site-to-site VPNs, each gateway encrypts data before sending it over the Internet and decrypts data received from the Internet. This arrangement protects against external threats and prevents Internet connectivity from compromising the level of security already established on internal networks.

Using IPSO Clustering

IPSO clustering is a feature patented by Nokia, which improves availability, reliability, and performance by allowing multiple Nokia IP VPN gateways to work as a single gateway. The IPSO 3.6 and later operating system lets you create firewall and VPN clusters that provide fault tolerance and dynamic load balancing. A cluster is made up of multiple appliances (nodes) that share common IP addresses; the cluster appears as a single system to the networks connected to it.

A cluster continues to function if a node fails or is taken out of service for maintenance purposes. The connections being handled by the failed node are transferred to one of the remaining nodes.

IPSO clusters are scalable with regard to VPN performance—as you add nodes to a cluster, the VPN throughput improves. IPSO clusters also support a variety of Check Point VPN-1/FireWall-1 NG features, including:

- Synchronizing state information between firewalls
- Firewall flows
- Network address translation
- VPN encryption

Note
To use clustering, you must use Check Point VPN-1/FireWall-1 NG FP2 and later, and all cluster nodes must run the same version of VPN-1/FireWall-1.
Active Session Failover

Active session failover ensures high availability of the Nokia IP VPN gateway cluster. If any node should fail, active session failover protection ensures that the other nodes in the cluster keep working and take over processing from the failed node. Active session failover is referred to as SA load balancing in IPSO.

Because VPNs are based on tunneling technology, typically a single point of failure occurs at either end of the tunnel. Further, an end point must keep a great deal of state information about each tunnel, because the tunnels are not just transparently forwarding traffic. Unlike traditional next-hop forwarding, where rerouting is dynamic and need not interrupt the flow of data, tunneled solutions rely on a single intermediate IP address (and therefore a single device). A failure of any component in this device can destroy VPN tunnels for many users. With IP clustering, the failure of a node does not result in a failed tunnel, because tunnel state information is distributed among all the nodes in the cluster.

Clustered nodes act as a single entity with a single external IP address and a single internal IP address. The nodes use internally recognized IP addresses to communicate among themselves. Figure 5 depicts Nokia IP VPN gateway packet processing.

Figure 5 Nokia IP VPN Gateway Packet Processing
The IPSO clustering is implemented in IPSO, which is an operating system with a custom kernel specifically designed to support the Nokia clustering technology and to support IPSec protocols.

An adaptive keepalive mechanism monitors the health of all nodes. The master node in a cluster exchanges keepalive messages with other nodes. If a node within the cluster becomes unavailable for any reason, the cluster master automatically reassigns the active sessions of the node among the remaining nodes. The time required to detect an unavailable node and rebalance the cluster load is between 250 to 500 milliseconds, so little or no disruption in service occurs after the device fails.

**Dynamic Load Balancing**

The Nokia clustering technology is designed to dynamically support large clusters of Nokia IP VPN gateways, handling tens of thousands of users without performance degradation. When additional capacity is required, you can add one or more gateways on an incremental basis, while the cluster is running, without any disruption of service.

The master node tracks the load, state, and processing power of all nodes in the cluster and allocates workloads so that the load is evenly distributed. Each node uses a filter to examine portions of an IP packet. For each protocol, the filter uses those fields most likely to provide the greatest variation in output values to evenly distribute the workload.

As additional nodes are added to the cluster, the session load is automatically balanced to include the new nodes, with no negative effect on current operations. In forwarding mode, if a new node with a higher performance rating than the current master is added into an existing cluster, the new node takes over as master after approximately one minute. During normal operation, you do not need to distinguish a master from other cluster members.
Example Cluster

The following diagram shows a cluster with two nodes: firewall A and firewall B. The cluster balances inbound and outbound network traffic between the nodes. If an internal or external interface on one of the nodes fails, or if a node itself fails, the existing connections that the failed node handles are not dropped—the other node processes them. The other node continues to function and handle all of the traffic for the cluster. Figure 6 on page 41 shows an example of a cluster.

Figure 6  Example of a Cluster

Routers connected to an IPSO cluster must have appropriate static routes to pass traffic to the cluster. In this example:
• The external router needs a static route to the internal network (192.168.1.0) with 192.168.2.10 as the gateway address.
• The internal router needs a static route to the external network (192.168.2.0) with 192.168.1.10 as the gateway address.

The IP addresses shown in bold are cluster IP addresses, addresses shared by multiple interfaces in the cluster.

The IPSO operating system uses the cluster protocol networks shown in the diagram for cluster synchronization and cluster management traffic. If a primary cluster protocol interface fails on a node, the node uses its secondary cluster protocol interface, and service is not interrupted. Nokia recommends that these networks be separate networks that are dedicated to this purpose, as in Figure 6.

The IPSO cluster management features allow you to configure firewall A and firewall B as the same virtual device, and also lets you set up automatic configuration of cluster nodes. You can manage the entire cluster as though it were a single device by using Nokia Network Voyager or the CLI.

For more information about clustering, see the Nokia IPSO 3.7 Clustering Configuration Guide.

### Clustering Options

You can configure IPSO clusters to work in one of three modes:

- **Unicast Mode**
- **Multicast Mode**
- **Forwarding Mode**

Each mode has certain advantages and is best used in particular situations. Limitations of some Ethernet switches might require a certain mode.

Multicast and unicast modes allow all cluster nodes to receive all traffic addressed to the cluster IP address. Unicast mode allows a virtual unicast MAC address to be shared by all cluster members. Multicast mode is often used if the connected Ethernet switch does not allow the same unicast MAC address on multiple ports. In forwarding mode, the master node receives
packets at its MAC address and forwards assigned traffic to the other nodes from their individual unicast MAC addresses.

If unicast or multicast mode (direct distribution) is used to deliver cluster traffic to all nodes, each node performs an evaluation on incoming packets: it processes packets for which it is responsible and drops those for which it is not responsible.

**Unicast Mode**

In unicast mode, a virtual MAC address is bound to the cluster IP address. Each node identifies with this MAC address, and each expects to receive all packets sent to the cluster address at this MAC address. Each node communicates with the master to determine its current workload, and each performs the classification operation to determine which traffic to process. The remainder of the cluster packets, for which the node is not responsible, are dropped, since another node handles them. The MAC address (layer 2) does not set the multicast bit.

**Multicast Mode**

Multicast mode behaves in almost the same way as unicast mode. The difference is that the MAC address in multicast mode sets the multicast bit. This works well on those switches that refuse to map a unicast MAC address to multiple ports for forwarding.

The spanning tree algorithm can sometimes cause issues with this mode as well as with unicast mode. Whenever possible, disable the spanning tree algorithm on the switch or switch ports connected to the Nokia IP VPN gateway.

**Forwarding Mode**

You can use forwarding mode in most network scenarios. The other modes sometimes have problems with switches running a spanning tree algorithm, or with switches that disallow a unicast MAC address on several ports or a multicast address without using a multicast IP address. Forwarding mode
allows the cluster master node to receive all packets sent to the cluster from its MAC address.

In forwarding mode, the master sends gratuitous ARPs for the cluster IP address. This binding allows the master to represent the entire cluster when it interacts with devices outside the cluster. The master then forwards the traffic assigned to the other nodes from their individual unicast MAC addresses. The other node IP and MAC addresses are used only for network management and cluster activities.

**Node Addition and Intracluster Communication**

To boot into a cluster, the node must be bootstrapped with a few lines of information that ensures its identity. This information includes a security token that is used as a preshared key in initial SSL communication with the management software. The first portion of the security token is a hash of the rest of the bootstrap information. This hash ensures that the device cannot be misconfigured. Once the management software completes the installation of the new node, the node contacts the cluster master, authenticates itself with the token, and downloads the rest of the cluster configuration and all session state information. After initialization, a node can begin processing traffics flows. When the node has been up and running for a while, the master balances the traffic load so that the new node processes its portion of the current load.

Communication between nodes in a cluster is authenticated by using an HMAC-MD5 hash. Any keying material is protected by using 3DES-CBC. This traffic is only sent on the internal interface (Ethernet0).

**Keepalive Referee**

The keepalive referee is an IP address used when a node loses connectivity. When this occurs, the node attempts to communicate outside the cluster by using the next hop towards this address. Nokia recommends that keepalive referees be configured for both the internal and external interfaces of the Nokia IP VPN gateway. The keepalive referee speeds recovery in the event of
Using IPSO Clustering

Nokia IP VPN Technology Overview v1.0

Using NAT

Network address translation (NAT) translates IP addresses on an internal network to different addresses on an external network. The Nokia IP VPN gateway provides NAT, which you can use with IPSec tunnel mode to connect to networks that use nonroutable IP addresses to the Internet.

The Check Point VPN-1/FireWall-1 uses SecureNAT network address translation. Robust and easy-to-manage, SecureNAT conceals internal network addressees from the Internet, thereby avoiding their disclosure as public information.

Integrated with the Check Point Stateful Inspection technology, SecureNAT provides one of the most secure implementations of address translation and supports a broad range of Internet services. SecureNAT also helps overcome IP addressing limitations such as restricted IP address allocation and unregistered internal addressing schemes.

VPN-1/FireWall-1 also provides advanced NAT capabilities that support H.323 applications and services such as the Microsoft NetMeeting, Intel Internet, VideoPhone, and VXtreme. Support for VPNs are seamless. For example, you can establish a tunnel between two gateways that allow internal hosts on each network to communicate securely, even if each hosts uses an illegal IP address.

VPN/FireWall-1 uses two types of NAT operating modes:

- **Dynamic mode**—uses a single IP address to hide all internal network resources. This mode conserves registered IP addresses and hides the
actual IP addresses of network resources. With dynamic mode, an unlimited number of internal IP addresses can be mapped to a single public IP address. Because the IP address is used only for outbound communication and is not used by any internal user, using dynamic mode can prevent hacking and spoofing of your Nokia IP VPN.

- **Static mode**—provides a one-to-one assignment between the published IP address and the internal IP address. Static mode is typically implemented when an organization needs to publish IP addresses for public servers, such as file transfer protocol (FTP) and Web servers without revealing the actual IP addresses of those servers.

### Stateful Inspection Technology

Stateful inspection, a technology developed and patented by Check Point, has become the de facto standard for firewalls. Stateful inspection extracts the state-related information required for security decisions and maintains this information in dynamic state tables for evaluating subsequent connection attempts. This technique provides a solution that is highly secure and offers maximum performance, scalability, and extensibility.

For detailed information about Check Point’s VPN-1/FireWall-1 and stateful inspection technology, see the *Check Point Management Guide*.

### Other Nokia IP VPN Gateway Features

This section describes other important features that Nokia IP VPN gateways provide, including:

- Command-Line Interface
- Bootstrap Security Tokens
- Secure Communications
Command-Line Interface

The Nokia IPSO command-line interface (CLI) provides an alternative to the Voyager GUI-based management for administrators who prefer a command-line interface or who want to include gateway commands in scripts. For more information, see the Nokia CLI Reference Guide for IPSO 3.7.

Check Point SmartLSM Command Line Utility (LSMcli) is a simple command-line utility and an alternative to SmartLSM GUI. The LSMcli utility lets you perform SmartLSM GUI operations from a command line or through a script. For more information, see the Check Point SmartLSM Guide.

Bootstrap Security Tokens

To ensure that an unauthorized node cannot be booted into the Nokia IP VPN gateway, the SMART software automatically generates a security token whenever you add nodes to your configuration. The security token is entered into the Nokia IP VPN gateway during bootstrap configuration, and it contains a secure hash of the configuration. The security token is used as a preshared session key to authenticate an anonymous secure sockets layer (SSL) communication between the SMART software and the Nokia IP VPN gateway.

Secure Communications

This section describes what methods you can use to manage the security and access features for your Nokia IP VPN. You can protect all communication between the Nokia IP VPN and branch offices by using either secure shell (SSH), Secure Sockets Layer (SSL), or the Check Point secure internal communication (SIC).

Secure Shell

Secure Shell (SSH) is a protocol that allows you to securely log into another computer over a network, execute commands in a remote platform, and move
files from one platform to another platform. You can use SSH instead of utilities such as Telnet or rlogin to securely manage your platform, tunnel HTTP over SSH with Voyager, or set up SSH public-key authentication with Nokia Horizon Manager. You can also secure communications by enabling and configuring the SSH service on your security platform using the Command-Line Interface (CLI).

The Nokia IP VPN supports both SSHv1 and SSHv2. Some of the differences between SSHv1 and SSHv2 include what part of the packet the protocol encrypts and how each protocol authenticates; SSHv1 authenticates with server and host keys, while SSHv2 authenticates using only host keys. Even though SSHv1 uses server and host-key authentication, SSHv2 is a more secure, faster, and more portable protocol. In some cases, SSHv1 might be more suitable because of your client software or your need to use the protocol authentication modes. SSH provides you with session protection from the following security threats:

- DNS spoofing
- Interception of passwords
- IP spoofing
- IP source routing
- Person-in-the-middle attacks (SSHv2 only)

For more information about SSH, see the Nokia Network Voyager Reference Guide or Nokia Horizon Manager User’s Guide. To enable and configure SSH by using the CLI, see, the Nokia CLI Reference Guide for IPSO 3.7.

Secure Sockets Layer

Secure Sockets Layer (SSL), gives you a secure way to connect to network appliances by using IPSO. SSL is the industry standard for secure Web connections because the protocol uses a pair of asymmetric keys to establish Web sessions. Each pair of keys consists of a public key and a private key. Keeping the private key secret is critical to your security.

The Nokia IP VPN supports SSLv3 which provides the following features:
- **Cryptographic security**— establishes a secure connection between two parties.
- **Interoperability**— allows programmers to successfully exchange cryptographic parameters without knowledge of each other’s code.
- **Extensibility**— provides a framework into which new public key and encryption methods can be incorporated as necessary. Also prevents the need to create a new protocol, thereby risking the introduction of possible new weaknesses.

You can configure SSL for Voyager Web access by using the CLI, or by enabling it in Voyager. When you use SSL, you reduce the risk of unauthorized parties tampering with your Voyager Internet sessions.

For more information about SSL, see the *Nokia Network Voyager Reference Guide*. For information about how to configure SSL with the CLI, see the *CLI Reference Guide for IPSO 3.7*.

### Secure Internal Communications

Check Point uses a proprietary protocol called secure internal communications (SIC). Based on SSL with digital certificates, SIC determines how Check Point components communicate with each other in Check Point Next Generation (NG). The SIC protocol allows the exchange of secure policies between gateways.

Using SMART, the Check Point Secure Management Architecture, the administrator and the SmartCenter server authenticate each other and create a secure channel of communication between them by using SIC. Once both the administrator and the SmartCenter Server are successfully authenticated, SmartCenter launches the selected SmartConsole.

For more information about SIC, see the *Check Point SmartLSM Guide*.
After you determine the goals for implementing your VPN and choose the Nokia IP VPN gateway products that meet your needs, your next step is to create a network design or plan.

This chapter describes how to design a Nokia IP VPN, including:

- Choosing a Network Topology
- Determining Gateway Placement
- Routing Considerations
- Address Translation Considerations

**Choosing a Network Topology**

Nokia IP VPN supports several types of network topologies, the most common being single hub-and-spoke and multiple hub-and-spoke. It also supports several complex topologies, such as star and mesh topologies. This section describes these topologies and shows example scenarios to help you choose a topology that reflects the business needs of your organization.

**Single-Hub Topology**

The hub and spoke topology represents a many-to-one relationship between branch office gateways and central office gateways. All communication between the gateways passes through the hub, which manages and controls all
functions of the network. Traffic is first sent to the hub and then the hub directs the traffic to the appropriate gateway associated with the destination address.

An advantage of implementing a single-hub topology is that a branch office gateway failure does not disable the entire network. In addition, the centralized hub makes it easier to add new gateways or reconfigure the network. Figure 7 shows an example of a single-hub topology.

**Figure 7 Single-Hub Topology**

![Single-Hub Topology Diagram]

---

**Star Topology**

In a star topology, the multiple central office gateways are interconnected to provide a single virtual hub for spoke connectivity. This topology is one of the most common network topologies found in offices.

The advantage of the star topology is that if one gateway on the star topology fails, only the failed gateway is unable to send or receive data. The other hubs
are not affected and can continue communicating on the network. The remainder of the network functions normally. Multiple hubs exist for regional distribution of spokes, ensuring business continuity.

**Figure 8** shows an example of a star topology.

**Figure 8  Star Topology**

---

**Mesh Topology**

In a mesh topology, devices are connected with many redundant interconnections between network nodes. In a true mesh topology, every node has a connection to every other node in the network.
Mesh topologies have the following configurations:

- Partial Mesh Topology
- Full Mesh Topology

**Partial Mesh Topology**

A partial mesh topology is less expensive to implement and yields less redundancy than full mesh topology. With partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two nodes in the network. Partial mesh topology is commonly found in peripheral networks connected to a full mesh backbone. Figure 9 shows an example of a partial mesh topology.

**Figure 9  Partial Mesh Topology**

---

**Note**

You can use both the Nokia IP1260 and the Nokia IP40 in a partial mesh topology.
**Full Mesh Topology**

A full mesh topology is a complex topology in which all gateways are interconnected with all other gateways and provides any-to-any communication among trusted peers. Full mesh topology occurs when every node has a circuit that connects it to every other node in a network. Full mesh is expensive to implement but yields the greatest amount of redundancy, so in the event that a node fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks. Figure 10 shows an example of a full mesh topology.

**Figure 10  Full Mesh Topology**

![Full Mesh Topology Diagram]

**Note**

You cannot do a full mesh topology with the Nokia IP40.
Determining Gateway Placement

How you place a gateway in relation to a firewall can affect network connectivity and the software configuration of your firewall or WAN routers. This section describes the placement options and considerations that apply when you determine gateway placement:

- Using the Gateway Outside the Firewall
- Using the Gateway Inside the Firewall
- Using the Gateway Parallel with the Firewall
- Single Interface Configuration
- Combining with the Firewall

**Note**
The term *firewall* also applies to any external router that filters traffic to protect internal network resources from the Internet.

Using the Gateway Outside the Firewall

When you place the Nokia IP VPN gateway outside the firewall, the external IP address is accessible from the Internet. The internal address of the gateway is only accessible from the internal firewall.

Firewall policy is not affected by this placement because the firewall receives unencrypted (clear text) packets from the Nokia IP VPN gateway. Because this placement does not interfere with existing firewall policy, organizations with a substantial investment in their existing security infrastructure might favor this implementation.
Placing the gateway outside the firewall is the best solution if the firewall is providing network address translation (NAT). For further information about NAT, see “Address Translation Considerations” on page 69.

The disadvantage of this placement is that the Nokia IP VPN gateway is exposed directly to the Internet and the firewall cannot tell if the traffic arrives properly encrypted at the Nokia IP VPN gateway. Also, with the Nokia IP VPN gateway outside the firewall, you have to determine how to forward or discard the unencrypted traffic that it receives.

**Forwarding IPSec Traffic Only**

If you are implementing a VPN because you are not satisfied with the current level of protection that your existing firewall and other security infrastructure provide, you might want to drop or discard all unencrypted traffic. This ensures that only encrypted traffic decoded by the security gateway is forwarded to the firewall for further processing. In this case, you must be careful that all of your existing users, applications, and partners that currently access your intranet can use IPSec.

This option is preferable when all traffic on a connection receives IPSec protection and when firewall policy is applied to the traffic after it is forwarded through the firewall.
Forwarding Unencrypted and IPSec Traffic

You might be satisfied with the level of security you established and want to use a VPN to make your network resources available to additional users. Your main concern in implementing a VPN might be to avoid disturbing existing users or applications. In this case, configure the security gateway to forward both detunneled IPSec traffic and unencrypted traffic to the firewall.

If both types of traffic are forwarded to the same firewall interface, the firewall cannot distinguish between traffic that was detunneled from IPSec and traffic that was not. To treat encrypted traffic differently, consider adding a second firewall in parallel with the first, or use a firewall with a separate interface for detunneled IPSec traffic.

You can apply filters on the Nokia IP VPN gateway to ensure that traffic from certain subnets is only forwarded if it arrives properly encrypted. In this case, you can adjust your firewall policy to apply different rules to traffic from these IPSec-enabled subnets.

Using the Gateway Inside the Firewall

When you place a Nokia IP VPN gateway inside the firewall, it is protected from the Internet by the firewall. The firewall forwards IPSec traffic to the Nokia IP VPN gateway. Figure 12 illustrates the placement of the Nokia IP VPN gateway inside a firewall.
Determining Gateway Placement

Figure 12  Nokia IP VPN Gateway Inside a Firewall

The downside of this implementation is that the firewall must be configured to pass IPSec and possibly other tunnelled traffic to the Nokia IP VPN gateway. In addition, security policies and access control lists that the firewall maintains cannot be applied to IPSec traffic because this traffic is still encrypted when the firewall receives it.

In this implementation, access control is implemented by using filtering on the Nokia IP VPN gateway. The Nokia IP VPN gateway performs full stateful inspection, which allows a firewall to base forwarding decisions on the state of specific connections.

Also, you cannot place a Nokia IP VPN gateway inside a firewall if the firewall is providing NAT. The only exception is to use IPSec Encapsulated Security Protocol (ESP) in tunnel mode.

For organizations that choose this implementation, Table 4 lists the protocols and port numbers that the Nokia IP VPN gateway uses. The protocols that your VPN uses must pass through the firewall when a Nokia IP VPN gateway is placed inside.
Make sure that the destination IP address on the firewall filter specifies the cluster external address. To provide the strictest possible firewall filtering, add filter entries for each remote VPN gateway IP address.

**Note**
If you are supporting remote IPSec or L2TP client access, you can only filter on the local Nokia IP VPN gateway external IP address.

The Nokia IP VPN gateway should be the only acceptable destination for these specified protocols, since it is detunneling all of the traffic before forwarding, or dropping it based on the configured security policy. Be careful to ensure that the policy you implement on the gateway is properly coordinated with the firewall policy.

In a site-to-site implementation, you can limit the filter in the firewall to IKE and IPSec peer addresses. All traffic to and from the network is transparently evaluated to determine whether it needs to be protected.

If your SMART software is on the opposite side of a firewall or filtering device from the cluster, allow configuration access, error monitoring, and logging access. The ports used for remote network management access are summarized in Table 5.

### Table 3 Port Numbers Used for Firewall Configuration

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IP Protocol</th>
<th>Transport</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE</td>
<td>IP 17</td>
<td>UDP</td>
<td>500</td>
</tr>
<tr>
<td>ESP</td>
<td>IP 50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AH</td>
<td>IP 51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td>IP 17</td>
<td>UDP</td>
<td>1701</td>
</tr>
</tbody>
</table>
Table 4  Server Port Numbers Used with SMART

<table>
<thead>
<tr>
<th>Server</th>
<th>Port number</th>
<th>Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration server</td>
<td>9876</td>
<td>TCP</td>
</tr>
<tr>
<td>Log server</td>
<td>9875</td>
<td>TCP</td>
</tr>
<tr>
<td>Monitor server</td>
<td>9874</td>
<td>TCP</td>
</tr>
<tr>
<td>SofaWare Management Server (SMS)</td>
<td>9282</td>
<td>UDP</td>
</tr>
<tr>
<td>Check Point Remote Installation</td>
<td>18208</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Note
SofaWare SMS and Check Point Remote Installation are required when you use SmartLSM.

Using the Gateway Parallel with the Firewall

Figure 13 illustrates a Nokia IP VPN gateway placed in parallel with a firewall. In this implementation, the firewall does not detect IPSec traffic and the Nokia IP VPN gateway handles only the IPSec traffic. However, this configuration can create greater routing complexity and should only be attempted where routing is simple and sufficiently stable. This implementation might be straightforward in a small or home office environment, where the IP addresses on both sides of the tunnel are known in advance.
When you use this placement, configure the routing to make sure that the traffic from your internal network that requires IPSec protection is properly routed to the Nokia IP VPN gateway.

In a site-to-site configuration, if the IP addresses are fixed and known, you can configure the firewall to redirect packets to the Nokia IP VPN gateway. In a remote access scenario, you can make this work if you know the addresses of the remote clients. This scenario might also work if application servers are dedicated to encrypted users and the routing is not ambiguous.

If you place the Nokia IP VPN gateway in parallel with a firewall, configure the external router to protect the gateway. Configure the Nokia IP VPN gateway to forward IPSec traffic and to drop all other traffic. This configuration might not work if you depend on the firewall to perform network address translation (NAT).
Single Interface Configuration

You can also implement the Nokia IP VPN gateway with a single interface, as shown in Figure 14.

Figure 14 Single Interface Configuration

This placement option does not provide a central point to control all incoming and outgoing traffic, but is useful in small or testing environments. You configure the firewall or router to forward encrypted traffic to the gateway, which decrypts the packets and passes them on to the destination host. A single interface configuration is especially useful in situations where the Nokia IP VPN gateways sit on a demilitarized zone (DMZ) or home LAN, and protects traffic for destinations over the Internet.

This configuration is easy to implement and does not require any change to the existing network infrastructure. However, in this scenario you cannot enforce encryption rules and you must configure static routes on the firewall to direct traffic to the Nokia IP VPN gateway.
Single interface support uses a single Ethernet interface on the Nokia IP VPN gateway. All traffic enters and leaves the Nokia IP VPN gateway by using the same interface. Like all Nokia IP VPN gateway configurations, the IPSec protocol is applied to the data when it passes through the gateway. However, you only need to configure a single IP address and interface for the connection.

**Combining with the Firewall**

The Nokia IP VPN gateway combined with a firewall provides robust network security. The gateway provides encryption and the firewall provides thorough access control protection at the central office or branch office point of entry. The Nokia IP VPN gateways provide authentication of other secure gateways on the network. Data communications from locations outside the secure network are passed directly to the firewall for its access control process. Traffic from sites that use Nokia IP VPN gateways is decrypted when it reaches the secure gateway at the receiving location.

**Routing Considerations**

This section discusses considerations you need to take into account when you determine routing for your Nokia IP VPN. The following topics are covered:

- Basic Routing Defined
- Types of Routing
- Supported Routing Protocols
- High Availability

**Basic Routing Defined**

IP routing is a set of mechanisms through which the gateway determines where to forward an IP packet so that it can arrive at the destination IP address. If the gateway that sends the packet and the destination gateway are
physically connected through a serial line or local area network, the sending gateway can send the packet to the destination directly. If the gateways are not physically connected, the gateway that sends the packet must identify the next hop that can forward the packet until it reaches the destination.

A router can create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet might travel through a number of network points with routers before it arrives at its destination.

For detailed information about routing, see the *Nokia Network Voyager Reference Guide*.

**Types of Routing**

This section describes the two IP addressing types. Each type has its own application and practicality.

**Static routing**—explicitly specifies the next hop for packets destined for a certain subnet. Packets with a destination that does not match any defined static route are routed to the default gateway. The Nokia IP VPN supports static routing.

**Dynamic routing**—uses special routing information protocols to automatically update the routing table with routes known by peer routers. These protocols are grouped according to whether they are Interior Gateway Protocols (IGP), or Exterior Gateway Protocols.

When you deploy Nokia IP VPNs, dynamic routing simplifies deployment and maintenance by:

- Treating an IP VPN connection like any other interface
- Eliminating the burden of setting and maintaining static routes
- Automatically reroutes VPN traffic if a system neighboring the VPN gateway fails providing high-availability.
Supported Routing Protocols

You can protect your routing protocols by using VPN over IPSec. Routing over IP VPNs also protects against outsiders learning information about an enterprise network, reduces the complexity of routing in an enterprise network, and enables use of routing despite intervening third-party networks (that is, ISP network that might not allow direct exchange of dynamic routing information). Using VPNs between your branch offices can prevent false routing messages, false routing table updates, or spoofing.

Nokia IP VPN provides support for the following routing protocols:

- **Border Gateway Protocol (BGP-4)**—widely deployed exterior routing protocol for IP networks. BGP-4 allows branch office gateways to communicate with central office gateways dynamically.

- **Open Shortest Path First (OSPFv2 and v3)**—routing protocol used within larger autonomous system networks in preference to RIP. The Nokia IP VPN supports both major OSPF versions:
  - OSPFv2—most commonly used OSPF version.
  - OSPFv3—provides support for IPv6 networks.

- **Routing Information Protocol (RIPv1 and v2)**—one of the oldest and simplest routing protocols.

- **Distance Vector Routing Protocol (DVMRP)**—the original Internet multicast routing protocol.

- **Protocol Independent Multicast (PIM-SM and PIM-DM)**—currently the most popular Internet multicast routing protocol.

**Note**

Central office gateways support BGP-4, OSPF, RIP, DVMRP, PIM, and static routes. Branch office gateways (for instance, the Nokia IP140), only supports BGP-4 and static routes.
High Availability

Nokia provides two options for configuring your IP VPN gateway for high availability. Both methods let you set up redundant gateways without the need to configure dynamic routing or router discovery protocols on every host. The options are:

- **IPSO Clustering**
- **Virtual Redundancy Routing Protocol**

Nokia recommends that you enable VPN-1/FireWall-1 and activate your security policy before you bring the high-availability configuration on line to use Check Point VPN-1/FireWall-1 with clustering or Virtual Redundancy Routing Protocol (VRRP).

**IPSO Clustering**

IP clustering in IPSO enables the construction of scalable, highly available firewall and VPN gateways by using multiple Nokia security appliances. Clustering offers an alternative to the IPSO Virtual Router Redundancy Protocol (VRRP) high-availability solution, providing performance scaling in addition to rapid, automatic failover for high-availability.

Clustering provides for high availability by eliminating potential single points of failure through redundancy of cluster nodes. Remaining nodes take over the work load of any node that fails or is removed from the cluster. Seamless failover requires application state synchronization (firewall, VPN) among all the cluster nodes. State sync is provided by VPN-1/FireWall-1.

With clustering, you can easily create load-balanced, fault-tolerant firewalls or VPN gateways. A cluster comprises multiple devices that share a common IP address, and it appears as a single system to the networks on either side of it.

A cluster continues to function if a node fails or is taken out of service for maintenance purposes, with no single point of failure if you configure a backup synchronization connection.

To use clustering, you must use Check Point VPN-1/FireWall-1 NG FP2 and later, and all cluster nodes must run the same version of VPN-1/FireWall-1.
The integration of IP routing functionality with support for VRRP and Check Point Firewall-1 make this high availability configuration an integral part of enterprise networks.

For more information on IP clustering, see the *Nokia IPSO Clustering Configuration Guide* and the *Nokia Network Voyager Reference Guide*.

**Virtual Redundancy Routing Protocol**

Virtual Redundancy Routing Protocol (VRRP), provides dynamic failover of IP addresses from one Nokia IP security platform to another in the event of a failure. You configure VRRP in one of two ways:

- An active-passive configuration, in which one or more passive Nokia IP security platforms back up one active system and do not forward any traffic unless they become the active system.
- An active-active configuration in which each Nokia IP security platform is active and also is a backup for the other devices in the set. This configuration allows a certain degree of load balancing because you can use static routes to direct traffic at each of the systems.

For more information about how to configure VRRP, see “Configuring Router Services” in the *Nokia Network Voyager Reference Guide*.

**Comparing Clustering and VRRP**

Clusters balance the traffic load among the nodes. VRRP configurations do not do this, although you can use an active-active configuration to achieve some load balancing.

Cluster nodes monitor Check Point VPN-1/FireWall-1 and stop forwarding traffic if the Check Point application stops working. When you run VRRP, an appliance does not stop forwarding traffic if VPN-1/FireWall-1 fails.

Appliances that run VRRP can run dynamic routing protocols and can forward multicast traffic. IPSO clusters do not support dynamic routing, and they cannot forward multicast traffic.

When you use clustering, you can use Cluster Voyager to configure and manage all the cluster nodes simultaneously through one browser or CLI.
session. VRRP does not offer this capability; you must configure and manage each system individually.

Whether you use clustering or VRRP, Nokia recommends that you use a separate network for VPN-1/FireWall-1 synchronization traffic. If you use clustering, you can also configure a backup synchronization network, which eliminates the primary synchronization network as a single point of failure. You cannot create a backup synchronization network with VRRP.

Finally, you can use VRRP in combination with transparent (bridging) mode, but clustering cannot.

**Using IPSO Clustering Versus VRRP**

Although VRRP enables some performance scaling through static load sharing, IPSO clustering dynamic load balancing is more practical and effective for scaling gateway performance—particularly VPN performance, which is highly scalable.

Use IPSO clustering when:
- You create a new high-availability installation, or
- You need VPN performance scaling.

Use VRRP when:
- You already have an existing VRRP pair for high-availability and do not need performance scaling.
- You need to assign multiple IP addresses for each logical interface.
- You need to emulate single-system-image dynamic routing.

**Address Translation Considerations**

Many organizations have IP addressing schemes that cannot be directly connected to the Internet. You can solve this problem by using one of the following translation schemes:
- Network address translation (NAT)
- Port address translation (PAT or NAPT)
- Encapsulating nonroutable addresses within IPSec packets

A NAT gateway changes the source address of each packet based on internal mapping tables. With NAT each inside address requires a unique Internet address. This solution requires that the organization have a valid Internet address for each workstation or server that connects directly to the Internet.

You can use NAT with Nokia IP VPN gateways, but you must be careful how the gateway is placed in relation to any router or firewall that performs NAT. The Nokia IP VPN gateway can perform NAT itself, in which case this placement issue is avoided.

When you design a VPN that includes a NAT gateway, the Nokia IP VPN gateway should generally be connected directly to the Internet. Avoid placing a separate NAT gateway between a Nokia IP VPN gateway and the Internet.

A PAT gateway changes the source address of each packet to its own Internet address and assigns a new TCP port number. The TCP port number uniquely identifies the source IP host to the PAT gateway. PAT allows an organization to use a single Internet address for a large number of users and servers on its internal network. A PAT gateway does not work if you place it between a Nokia IP VPN gateway and the Internet.

You can solve the addressing issue without using NAT or PAT by using IPSec in tunnel mode to encapsulate nonroutable addresses within IPSec packets.

For more information about how to use NAT, see “Using NAT” on page 45.
Implementing a Nokia IP VPN

After you design your Nokia IP VPN gateway, including choosing a topology, placing the gateway in your network, and determining routing considerations, you are ready to implement and configure your VPN. To implement your Nokia IP VPN, you need to perform the basic gateway configuration by using the software applications described in this chapter, which include the following:

- Using the Nokia IPSO CLI
- Using Nokia Network Voyager
- Managing Policies with Check Point SMART

Note
For detailed information about the protocols and standards used to implement a VPN with the Nokia IP VPN gateway, see Appendix A, "Overview of Standards and Protocols."

Using the Nokia IPSO CLI

The Nokia IPSO command-line interface (CLI) provides an alternative to the Network Voyager GUI-based management for administrators who prefer a command-line interface or who want to include gateway commands in scripts. The first time you turn power on to a Nokia appliance, the initial configuration process begins. Using a console connection to perform the
initial configuration, you can configure the network settings and gain access to the admin account using the CLI commands. The IPSO CLI also provides commands for configuring interface, routing, network and security, traffic management, system configuration, SNMP, monitoring, and IPv6.

For more information about how to install and configure your appliance by using the CLI, see the installation guide for your appliance. For example, the Nokia IPXXX Series Installation Guide.

**Using Nokia Network Voyager**

You configure the Nokia IP security platforms based on the Nokia IPSO operating system with Voyager, the Web-based element management application. Voyager provides a convenient network-extensible configuration user interface to manage network elements. Using Voyager, the administrator access can configure the following:

- System resources (dynamic and static monitoring)
- Interfaces
- Routing
- Traffic management
- System functions
- Security and access
- SNMP

For more information about using Network Voyager, see the Nokia Network Voyager Reference Guide.

**Managing Policies with Check Point SMART**

An enterprise network and an ordinary network are not clearly distinguishable. However, if making a change to the network configuration is a major event, then you probably have an enterprise network. When a network of any kind is small, you normally manage one piece at a time. This is called
element management, because a change has to be applied to each piece individually. As the number of elements increase, element management becomes impractical. Managing large mesh networks one element at a time is impractical because of the scaling problem.

The step beyond element management is policy management. With policy management, the network manager perceives the network as a single large system. Managing VPN policy is much more efficient than managing individual elements.

The Check Point Secure Management Architecture (SMART) is used to define and distribute policies.

SMART is divided into two components:

- **SmartCenter Server** (management server)—maintains the databases of network object definitions, user definitions, security policies, and log files for any number of enforcement modules. Policies are defined by using SmartDashboard on the SMART Client and saved on the management server.

- **SMART Client** (management client)—runs the SmartDashboard (policy editor), which provides a GUI interface for the administrator to define network objects, users, and policies. SMART Client includes the SmartDashboard, SmartMap, SmartViewStatus, SmartViewTracker, and SmartView Reporter. SmartDashboard, SmartView Status, and SmartView Tracker are included in SmartCenter; other SMART Client applications require separate licenses.

**Note**

You can deploy the SmartCenter Server and SMART Client on the same gateway or on separate gateways.

For detailed information about SMART and SMART components, see the *Check Point SmartCenter User Guide*. 
SmartCenter Server

You define policies by using SmartDashboard on the SMART Client and save them on the SmartCenter management server. The management server maintains the VPN-1 databases, which include network object definitions, user definitions, security policy, and the log files for firewalled gateways. VPN-1 implementations are integrated into an overall enterprise security policy. Once policies are created or modified, they are distributed to enforcement modules. Centralized policy management increases efficiency when compared to solutions that require either multiple management interfaces or policy installation for each device. Security is strengthened because the policy is always up-to-date at all network enforcement modules.

SMART Client

The applications available in the SMART Client include SmartDashboard, SmartMap, SmartUpdate, SmartView Status, SmartView Tracker, and SmartView Reporter. SmartDashboard, SmartView Status, and SmartView Tracker are included in SmartCenter and SmartCenter Pro. Other SMART applications require separate licenses.

**SmartDashboard**—provides a single graphical user interface for defining and managing multiple elements of a secure virtual network: firewall security, VPNs, network address translation, QoS, and VPN client security.

**SmartMap**—security policy visualization tool that provides a detailed graphical map of the security deployment of an organization.

**SmartView Status**—provides a snapshot of the status of the module in a VPN-1 security architecture.

**SmartView Tracker**—provides real-time visual tracking, monitoring, and accounting information for all logged connections.

**SmartView Reporter**—provides log data consolidation and reporting, creating custom reports for security audits, activity trending, and accounting.
Check Point Smart Large Scale Manager (SmartLSM)

Check Point SmartLSM works in conjunction with the SmartDashboard to define, manage, and monitor branch office gateways. Administrators can view the status of each branch office gateway, including what profile it is associated with and what version of the VPN security policy it is enforcing. In addition, critical notifications about branch office gateways are also displayed that alert administrators to take appropriate action.

SmartLSM manages and monitors the standard Check Point VPN-1 gateway at the corporate headquarter site and VPN-1 gateways at branch office sites. SmartLSM allows system administrators to manage thousands of branch office gateways from a single SmartCenter server. The SmartLSM management concept is based on gateway profiles that are defined in the standard Check Point SmartDashboard. Instead of representing a single physical gateway, each gateway profile object represents multiple branch office gateways.

SmartLSM reduces the administrative overhead for each gateway by defining most of the gateway properties, as well as the policy, by profile object instead of by the physical branch office gateway.

For more information, see the Check Point SmartLSM User Guide.

Note
SofaWare SmartCenter Connector 4.x is required to support SmartLSM with the Nokia IP40. SofaWare SmartCenter Connector (SSC) is an add-on for Check Point SmartCenter that enables centralized management of the Nokia IP40 branch office gateways.

Using VPN Communities

Check Point SmartDashboard enables administrators to create large-scale VPNs in a single operation. Administrators can define VPN communities and set security parameters for the entire VPN, such as intranet and extranet, in one step. VPN communities can use SmartLSM profiles.
By grouping all VPN-1 gateways in a community, they share the same VPN security parameters, such as encryption algorithms. As new sites are added to the community, they automatically inherit the appropriate properties and can immediately establish secure IPSec sessions with the rest of the VPN community.

Creating VPN tunnels between gateways is made easier through the configuration of VPN communities. A VPN community is a collection of VPN-enabled gateways that can communicate by using VPN tunnels.

To understand VPN communities, a number of terms are defined as follows:

- **VPN community member**—refers to the gateway that resides at one end of a VPN tunnel.
- **VPN domain**—refers to the hosts behind the gateway. The VPN domain can be the entire network that lies behind the gateway or only a section of that network. For example, a gateway might protect the corporate LAN and DMZ. Only the corporate LAN needs to be defined as the VPN domain.
- **VPN Site**—community member in addition to VPN domain. A typical VPN site is a branch office.
- **VPN Community**—collection of VPN tunnels, links, and their attributes.

The methods used for encryption and ensuring data integrity determine the type of tunnel created between the gateways, which in turn is considered a characteristic of that particular VPN community.

The SmartCenter server can manage multiple VPN communities, so that you can create communities and then organized according to specific needs. The SmartCenter server is a component of the VPN-1/FireWall-1 application and manages the security policies.

For more information about the SmartCenter server, see the *Check Point VPN-1 User Guide*. 
Implementing a Nokia IP VPN
Managing a Nokia IP VPN

The Nokia IP VPN solution has a variety of management services that assist you to monitor, debug, and maintain your VPN. Running these services over IPSec VPN establishes secure, end-to-end private network connections over a public networking infrastructure and protects data from unauthorized access, or where vulnerabilities exist.

This chapter describes the Nokia IP VPN management services and includes:

- Using NTP
- Using Syslog
- Using SNMP
- Upgrading IPSO
- Backing Up and Restoring Files
- Using Nokia Horizon Manager

Using NTP

Network Time Protocol (NTP) is a protocol that allows you to synchronize to UTC time by querying a server with an accurate clock. This protocol can synchronize distributed clocks within milliseconds over long time periods. NTP is ideal for distributed applications that require time synchronization, such as Check Point FireWall-1 Sync, or analyzing event logs from a different machine.
NTP runs as a continuous background client program on the gateway and sends periodic time requests to NTP servers to obtain server time stamps and uses them to adjust the client clock. A time stamp provides evidence that an item existed at a specific time, such as a time-stamped digital certificate that a certificate authority issues for client authentication purposes.

Although NTP is a reliable method to maintain and synchronize times on gateway servers, vulnerabilities exist. If the server times vary with each other or with the correct time, processes can fail, data can be lost, and security is compromised. To prevent hacking or IP spoofing, these time mechanisms need to be secure.

Using Syslog

The Nokia IP VPN gateway logging system allows you to configure a variety of options for viewing logging information for particular users, resources, authentication methods, and gateway components. Logging messages are stored to the syslog daemon which runs on the gateway. The output stored in the log files include information about events such as administrative events, configuration changes, and tunnel events.

Because messages are passed in cleartext, an attacker might be able read the contents of a syslog message or, for example, obtain records of administrative access. You can secure syslog messages by running syslog over IPSec. VPNs provide an encrypted data channel that tunnels the syslog information over the network, protecting all the logging information.

Using SNMP

The Simple Network Management Protocol (SNMP), provides a common framework for managing and monitoring network devices. This protocol provides a message format for communication between SNMP managers and agents.

The Nokia IP VPN gateway includes support for SNMP traps that alert you when particular events occur during the gateway operation. You must
configure the IPSO SNMP agent from Voyager or the CLI to use the SNMP traps. The IPSO SNMP agent is responsible for performing the SNMP communication to the network management station, based on the Voyager SNMP settings.

For the definitions of the SNMP traps, you can download MIB files. These files define the object identifiers that the gateway uses. Once you place these files on the network management station, the station can interpret the traps that the gateway sends through the IPSO SNMP agent.

Using IPSec, you can define IPSec policies in your monitored systems and management stations so that all SNMP traffic is authenticated and encrypted. You can also configure the SNMP agent to only accept SNMP requests from a certain set of VPNs. With this configuration, providers can provide network management services to their customers, so that customers can manage all user VPN devices.

**Note**

Central office gateways support SNMPv2c and SNMPv3. Branch office gateways (for instance, the Nokia IP40) only support SNMPv2c.

For information about how to configure SNMP and detailed descriptions of the MIBs, see the *Nokia Network Voyager Reference Guide*.

**Upgrading IPSO**

This section describes how to upgrade IPSO operating system software on your Nokia devices. You can upgrade IPSO by using the CLI, Voyager, or Nokia Horizon Manager.

Depending on the versions of the software you currently have installed, you can use Nokia HM either to upgrade from an older version of the software to a newer version or to install the new software.

If you use Nokia HM to manage your appliances, you can upgrade and revert to earlier versions of IPSO on all your appliances simultaneously or in groups.
of multiple appliances. Nokia HM employs *Do No Harm* intelligence to prevent incompatible package installations on Nokia appliances.

For more information about how to upgrade IPSO, see the appropriate installation guide for your appliance.

### Backing Up and Restoring Files

You can configure your Nokia IP VPN to perform manual or regularly scheduled backups and to restore files from locally stored backup files by using the IPSO CLI, Nokia Network Voyager, or Nokia Horizon Manager.

You can back up and restore files quickly by using the CLI. If your configuration consists of a single gateway or cluster of gateways, use Voyager. For multiple devices or large network deployments, you can back up and restore files by using Nokia Horizon Manager.

For detailed information about how to back up and restore files, see the *Network Voyager Reference Guide*, the *CLI Reference Guide for IPSO 3.7*, *Nokia IP40 CLI Reference Guide*, and the *Nokia Horizon Manager User’s Guide*.

### Using Nokia Horizon Manager

Nokia Horizon Manager provides users the ability to securely manage software packages, maintain a hardware and software inventory, and provide overall platform management of Nokia IP security platforms.

Using Horizon Manager, an administrator can obtain configuration information, upgrade the operating system, revert back to previous configurations, perform application installations, and distribute necessary licensing to multiple platforms simultaneously, thereby reducing potential human error and improving productivity.

Nokia Horizon Manager is designed to manage and configure a large number of Nokia security platforms (devices) that reside on a corporate enterprise, managed service provider, or hosted applications. Using Horizon Manager, a
network security professional can manage multiple devices simultaneously, perform parallel software upgrades, device verifications, device configuration, file backups, and more.

The Nokia Horizon Manager configuration management tool takes into account not only software deployment (both IPSO and applications such as Check Point), but also extracts and maintains configurations, deploys modified configurations, allows a staging model where one or more appliances can be configured at a time, performs DNS, Telnet, SSH, and other operating system-specific configuration functions for one or more appliances. This tool also offers configuration functionality to enable new configurations to occur at more convenient times, coupled with scheduled operations.

For more information about how to manage your network using Horizon Manager, see the *Nokia Horizon Manager User’s Guide*. 
6 Glossary

**AH**
Authentication Header

**Authentication Header**
A protocol used in IPSec that provides packet source authentication, data integrity, and antireplay protection.

**BGP-4**

**blocked certificate list**
A list of invalid certificates that a Nokia VPN gateway does not accept.
Border Gateway Protocol, version 4
The standard Internet routing protocol for routing between autonomous domains.

CA
certificate authority

certificate
Information that binds an entity to a public key.

certificate authority
A trusted third party that digitally signs certificates to give them authenticity.

certificate revocation list
A list of invalid certificates associated with a CA.

Challenge Response Authentication with Cryptographic Keys
An authentication method which provides mutual authentication when one side is using secret-key authentication, such as RADIUS, SecurID, or OTP, and the other is using public-key authentication, with optional digital certificates.

CLI
Command-line interface used for entering commands and configuration options.

CRL
Certificate Revocation List
custom
A topology between gateways in a partition where all the tunnels must be manually defined and generated.

DDNS
Dynamic Domain Name System. Notifies DNS server of hostname and IP address mappings and is used when the local DHCP server lacks this capability. The relevant IETF RFC is 2136.

DH
Diffie-Hellmann

DHCP
Dynamic Host Configuration Protocol. A protocol that is used to lessen the administrative task of manually configuring TCP/IP hosts on a network.

Diffie-Hellman group number
A number which specifies the parameters to use in a Diffie-Hellman exchange.

Encapsulated Security Protocol
A protocol used in IPSec.

DMZ
Demilitarized Zone

Demilitarized Zone network
A DMZ network provides a safe, relatively neutral location for communication between systems in a inside protected network and those on the outside.
ESP
Encapsulated Security Protocol

Encapsulated Security Protocol
A protocol used in IPSec that provides packet source authentication, data integrity, antireplay protection, and data confidentiality.

hub and spoke
A topology between gateways in a partition where a single node called the hub has tunnels to each of the remaining gateways in the partition.

IETF
Internet Engineering Task Force

IKE
Internet Key Exchange

Internet Key Exchange
A proposal/acceptance mechanism used to negotiate and provide authenticated keying material for security associations in a protected manner. Used by VPNs to establish SAs between IPSec peers.

IP
Internet Protocol

LAC
L2TP Access Client
Layer 2 tunneling protocol
A link layer protocol used to move data from point to point. Extends PPP functionality by allowing the layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. Often used to tunnel PPP frames.

LNS
L2TP Network Server

L2TP
Layer 2 tunneling protocol

mesh
A topology between gateways in a partition where each gateway has a tunnel to every gateway in the partition.

message digest
A hash of a message that is used to check the integrity of a message.

MIB
Management Information Base. A database that a SNMP router maintains to hold information about all resources managed by a network management system.

NAS
Network Access Server

NAT
network address translation
**OSPF**
Open Shortest Path First

**Open Shortest Path First**
A popular link state protocol for routing within an autonomous domain.

**partition**
Represents a group of security gateways that share a common security policy.

**PAT**
Port address translation

**PKI**
Public Key Infrastructure

**PPP**
A protocol for transporting multiprotocol packets across layer 2 point-to-point links.

**PPPoE**
Point-to-point protocol over Ethernet.

**Public Key Infrastructure**
A infrastructure designed to manage and support scalable authentication methods using public keys.

**RADIUS**
Remote Access Dial-In User Service
realm
A collection of gateways and partitions for which management actions can be applied to each of its members automatically.

Remote Access Dial-In User Service
A protocol that provides user authentication, authorization, configuration, and accounting between a client (called a Network Access Server) and a server (called an Authentication Server). Uses shared secret for authentication using PPP PAP or CHAP, UNIX login, and others. Often used with dial-in PPP clients.

RIP
Routing Information Protocol

Routing Information Protocol
A simple distance vector (hop count based) protocol for routing within an autonomous domain.

RIPv2
An enhanced version of RIP that supports variable length subnet masks.

SA
security association

security association
Represents the contract between two communicating entities that determines various parameters such as the encryption protocol, authentication protocol, and the lifetime of the keys.
Security Policy Database
Database used to define and store the policy which defines the characteristics of the communication between two entities. Used in addition to the Security Association Database.

Secure Sockets Layer
A protocol that provides secure socket communication over TCP.

Security association database
Database of security associations used by an IPSec device to maintain SAs.

Security Parameter Index
A quantity that uniquely identifies an SA to each of the communicating entities.

Selector
An entry in an access list which maps IP traffic to IPSec policy. If a packet matches a selector, the selector is used to specify whether the packet should be dropped, passed, or protected using IPSec. The selector defines which packets match by specifying the source and destination IP addresses of the packet, as well as any additional information that is needed to identify the packets of interest.

SNMP
Simple Network Management Protocol. As a standard method of managing and monitoring network devices on a TCP/IP-based internet, it allows network administrators to connect, setup, and maintain a network.

SPD
Security Policy Database
SPI
Security Parameter Index

SSH
Secure Shell. A program to log into another computer over a network that allows execution of commands and movement of files. Intended as a replacement for rlogin, rsh, and rcp, it provides strong authentication and secure communications over channels that are not secure.

SSL
Secure Sockets Layer

TACACS+
Terminal Access Controller Access Control System. TACACS+ provides access control for routers, network access servers and other networked computing devices that use one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. TACACS+ is a Cisco protocol that is used only when interoperating with Cisco equipment.

TCP
Transmission Control Protocol

template
A group of common settings that can be installed as a unit on one or more gateways.

TLS
Transport Layer Security
**transform**
In the context of IKE, a cryptographic entity, such as the secrecy algorithm or the integrity algorithm, that is requested during initial negotiation between communicating parties. For example, the proposer can request that IPSec communication use ESP with the triple data encryption standard. This is done by specifying the ESP_3DES transform id in the request.

**virtual private network**
Connects networks over the Internet in a secure, private manner.

**VPN**
virtual private network

**VPN gateway**
A single node or cluster of nodes that function as a single device and share the same VPN policy and security configurations.
This appendix provides additional details regarding the protocols and other standards used to implement a VPN with Nokia IP VPN gateways. This appendix contains the following sections:

- IPSec
- Authentication Algorithms
- Encryption Algorithms

**IPSec**

IPSec operates in one of two modes:

- Transport mode places the IPSec header after the original outer IP header and before the upper layer protocol.
- Tunnel mode encapsulates the entire IP header and datagram, prepends an IPSec header, and then creates an outer IP header to tunnel the packet.

Transport mode can be performed only by the sender of the original datagram, and the destination address must handle de-tunneling itself. This means that IPSec protection needs to occur on the device building the IP packets. Tunnel mode can be done either by the sender of the original datagram or by another device within the network. Thus, tunnel mode is required when a gateway
protects traffic between a node (positioned behind the gateway) and hosts over the Internet or other shared network.

Nokia IP VPN gateways use tunnel mode to perform almost all of the IPSec tunneling, whether to other gateways or to individual hosts. The one exception is when the Nokia IP VPN gateway terminates layer 2 tunnels. Transport mode can be used when using L2TP with IPSec.

Authentication Header

Authentication Header is an IP protocol (type 51) that can provide data integrity and origin authentication as well as replay detection for IP packets. It functions by appending the datagram Integrity Check Value (ICV) to the datagram. AH can provide these authentication services using keyed one-way hash functions.

AH functions in transport mode by inserting an AH header into the datagram after the IP header and before the upper layer protocol, including any other IPSec headers. AH functions in tunnel mode by placing an AH header in front of the entire original datagram and adding another IP header on the outside. AH computes an ICV that actually includes some fields in the outer IP header, as well as the upper layer protocol and some fields in the AH header itself.

Some fields in this outer header may be modified en route to the destination. These fields are set to zero for calculation of the ICV. The values of some fields are predictable; in this case the expected value is inserted into that field for ICV calculation. The Type of Service (TOS), Flags, Fragment Offset, Time to Live (TTL), Header Checksum, and the Authentication Data field are set to zero prior to computation of the ICV over the entire transmitted packet.

Encapsulating Security Payload

Encapsulating Security Payload (ESP) is an IP protocol (type 50) that can provide confidentiality and authentication of both message integrity and data origin, and replay detection for IP packets. It is not mandatory that all of these services be used; however, it is possible to enable them all simultaneously.
ESP can provide authentication services using keyed one-way hash functions. ESP can also provide privacy services using symmetric data encryption algorithms. It is possible to combine these two services, in which case encryption is performed before authentication.

ESP functions in transport mode by inserting an ESP header right after the IP header (including any options) and in front of the upper layer protocol. It protects everything beyond this header. In tunnel mode it takes the entire IP datagram and inserts an ESP header before the original IP header and encapsulates that inside a new IP datagram to be forwarded.

**Message Digests**

Message integrity is achieved by producing a hash or message digest and appending this value to the message. The nature of message digest algorithms is that the same algorithm always achieves the same result on the same data, but never achieves the same result on even slightly different versions of the same data.

**Authentication Algorithms**

In general, authentication algorithms used in AH and ESP are used as a mechanism to ensure two pieces of information: the source of the datagram and the integrity of the data. The former ensures that it was sent by the claimed source, while the latter ensures that the data was not altered along the way. These operations are performed using one-way hash functions. Special one-way hash functions have the property that it is statistically infeasible for any two messages to have the same hash output. This ensures that the sender is the claimed source and that the message has not been changed along the way. Longer outputs are cryptographically stronger. These are done using a hashed message authentication code (HMAC) version of these hashes.
A  Overview of Standards and Protocols

Message Digest 5 (MD5)
MD5 was created by Ron Rivest in response to a potential weakness discovered against his MD4 algorithm, when two of the three rounds were cryptanalyzed. The result is MD5, which was strengthened to include a fourth round by using a different operation 16 times, as well as adding other cryptographic strengths. MD5 produces a 128-bit hash value. It is sometimes theorized that MD5 might have a potential weakness that can leave it vulnerable to some attacks in the future also.

Secure Hash Algorithm 1 (SHA-1)
SHA-1 was created by the National Institute of Standards and Technology (NIST) along with the National Security Agency (NSA). It is generally similar to MD4, with some strengthening similar to that of MD5. It produces a 160-bit hash value. Since this value is longer and no known attacks or even partial attacks are known, cryptographers generally consider it more secure than MD5.

RIPEMD
RIPE is a European program that is attempting to define the standards that should be used in telecommunications in the European community. The algorithm defined by RIPEMD is very similar to MD4. It is used throughout the European community to produce hash values of 128 bits and 160 bits. It is thought to be resistant to cryptanalysis. Nokia only offers this hash in the 160-bit form.

Algorithms
Choose AH and/or ESP. These decisions can be made separately for each traffic flow. For encryption, if you have no export or other restrictions you can freely make the most secure choice you prefer. In some instances, you might be restricted to a certain algorithm. Company security policies might
already be in place for these purposes. If not, you might want to create one. You might want to evaluate the appropriate cryptographic literature to examine the research and testing that has been done on the various algorithms. Those that have undergone the most cryptanalysis are considered more secure.

**Lifetimes**

Lifetimes can have a relationship to the algorithm chosen in that if you choose, or have to choose, a less durable algorithm, you might want to decrease the rekeying lifetime in order to provide fewer opportunities to break an individual key. If you can choose a stronger algorithm, you do need to rekey as frequently. You never want to make this number unrealistically low, however, since the node needs to perform expensive exponentiation calculations for each rekeying. The default of one hour for Phase 2 SAs provides adequate security for most deployments.

**Perfect Forward Secrecy**

Perfect Forward Secrecy (PFS) is an option (which is the default) that forces a Diffie-Hellman exchange to generate new keying material for each IPSec SA. This means that each new SA has keying material that is not related in any way to the keying material used in creation of the IKE SA or any previous IPSec SA. This makes attacks more difficult. This forces attackers to perform the attacks separately for the packets generated in each SA lifetime.

When using PFS, you need to specify the group number for Diffie-Hellman. The default is Group 2. Group 1 provides for less cryptographically secure keying material and Group 5 provides for more secure keying material. This choice also affects the strength of your IPSec security.
Encryption Algorithms

At the time of this writing the algorithms discussed in this section were generally accepted by the cryptographic community. Please consult an applied cryptography source for further information, since these sources are much more authoritative. The following information is offered as a general description of these algorithms.

Encryption algorithms are used as mechanisms to ensure that data remains private. The operations performed by encryption algorithms are meant to scramble packet data to make it appear to be random and unreadable to anyone who might be “eavesdropping” on the conversation, while allowing the other side to be able to read the contents of the datagrams. The essence of encryption is the use of an algorithm to combine a key with cleartext, which is the original data, in order to change it into a series of seemingly random bits. This encrypted data, or ciphertext, can then be transmitted through whatever means available and subsequently decrypted on the receiving side, where it becomes meaningful data again.

ESP, one of the main IPSec protocols, uses symmetric key algorithms. A symmetric key algorithm uses the same key to encrypt and decrypt data. The algorithms used are all published and some have been evaluated more carefully than others. Some were created to be implemented in hardware and some in software. They vary in key length and all rely on the secrecy of the session keys used in deriving the encrypted data.

Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a symmetric 128-bit block data encryption algorithm developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. This algorithm was developed to secure sensitive but unclassified material by U.S. Government agencies. The U.S government adopted AES as its encryption technique in October 2000, replacing the Data Encryption Standard (DES). AES works at multiple network layers simultaneously.
Data Encryption Standard

The Data Encryption Standard (DES) was created in the 1970s when NIST was looking for a suitable encryption standard. IBM created it with some input from the NSA. DES uses substitution followed by permutation based on a key, where key bits are shuffled around in a prescribed way. It uses fixed s-boxes to do substitution operations, and expansion is performed using the shared secret key after it undergoes some shifting. This was all designed to be performed in hardware, although it can also be done in software. An identical operation is used to decrypt the ciphertext. The cryptographic strength of DES has been controversial for some time. Recent demonstrations have shown that DES is not adequate for most transactions. Brute force computing power is used to try all possible keys in this attack. Special chips and software programs can crack DES easily today. It is unlikely that anyone would want to use it in practice, unless export or import restrictions limit you to this choice.

Triple Data Encryption Standard

Triple data encryption standard (3DES) is based on the original DES discussed above. 3DES performs DES three times. However, the fact that DES is no longer adequate has little to do with the cryptographic strength of 3DES. The same operations are performed as are done in DES; however, with additional key shifting the operations are performed three times. This does not mean that 3DES is only three times harder to crack than DES. The difference in difficulty between DES and 3DES is in fact $2^{56}$ versus $2^{112}$. Not only is 3DES very strong, it might be one of the strongest algorithms today. It is currently believed that 3DES will not be broken any time soon with any techniques known today. 3DES has been cryptoanalyzed more thoroughly than any other algorithm today.

CAST

CAST was created in Canada by Carlisle Adams and Stafford Tavares. In this method, 64-bit keying material is combined with part of the data, and then this is XORed with other data in a series of eight rounds. CAST also uses s-boxes.
for substitution. However, these are not fixed, but rather implementation-specific and fixed once an implementation has been created. These substitution boxes are the key to the security of the algorithm. There is no known attack on the algorithm. CAST is a variable key-length cipher. Nokia uses a 128-bit key in its CAST implementation The key length can be 40 to 128.

**Blowfish**

Blowfish is an algorithm created by Bruce Schneier to be performed quickly in software and use relatively little memory space. The algorithm consists of key expansion and data encryption. The key expansion must be done before data can be encrypted, and there are four 32-bit “s-boxes” with 256 entries each. Since these boxes are based on the session key rather than a fixed key, there is more work to be done up front. The decryption algorithm is the same, using sub-keys in the reverse order. It is a variable key-length cipher that has been defined with capabilities to reach 448-bit keys. The Nokia default is 128-bit keys. The key length can be 40 to 448.

**RC5**

RC5 was created by Ron Rivest. It is a relatively new algorithm that was analyzed by RSA laboratories for a considerable period of time, and it is believed to be secure. RC5 is of variable length; the Nokia default is 128 bits. The key length can be 40 to 2048.

**Diffie-Hellman**

The secret keys used in authentication and encryption are never sent between two peers. Diffie-Hellman is the mechanism by which keying material is derived. The public keys or pre-shared keys are not related to the Diffie-Hellman keys.
Because it is important that these keys are kept secret, any kind of key exchange must ensure that an eavesdropping third party cannot determine the session key. This key exchange takes place over what is assumed to be an unsecure link. Diffie-Hellman is the most widely used and trusted key exchange mechanism. It is very secure, because at no time is the session key actually transmitted over the wire. Further, a third party cannot determine the value of the key, even if they see all the exchange information that goes over the wire. Diffie-Hellman prevents key interception by using an agreed-upon prime number defined through the IKE Diffie-Hellman group number. Diffie-Hellman prevents key computation by exponenting with large numbers. This exchange is subject to an active man-in-the-middle substitution attack, and so it must be authenticated.
Index

**Numerics**

3DES 101

**A**

- access control 14
- active session failover 26, 39
- adaptive keepalive 40
- addressing problems 24
- advanced encryption standard. See AES.
  AES 100
  AH
  - authentication algorithms 97
  - description 27, 96
  - IPSec protocol 27
  - overview 96
  - transport mode 96
- algorithms
  - 3DES 101
  - authentication 97
  - blowfish 102
  - CAST 101
  - DES 101
  - encryption 100
  - lifetimes 99
  - overview 98
  - RC5 102
  - RIPEMD 98
  - SHA-1 98
  - asymmetric encryption, PKI 33
  - authentication algorithms 97
  - defined 24
  - IKE 30
  - pre-shared keys 34
  - preshared keys 34
  - public key certificates 35
  - raw public key 34
  - authentication algorithms 97
  - authentication header. See AH.
  - authentication methods 15

**B**

- backing up files 82
- BGP-4 66
- blocked certificate list. See CRLs.
  - blowfish 102
  - bootstrapping 44
  - branch office gateways 66
  - SNMP 81

**C**

- CA
  - defined 35
  - external 36, 37
  - integrity 36
  - internal 36
  - trust relationships 35
  - CAST 101
central office gateways 66
SNMP 81
certificate
defined 35
digital 35
DNS name in 37
IP address in 37
public key 35
X.509 35, 36, 37
certificate authorities. See CA
certificate revocation lists. See CRLs.
Check Point
internal CA 37
SIC 49
SMART 60
SmartCenter 35, 49
software 14
stateful inspection 46
CLI 47, 71
configuring SSL 49
cluster, defined 38
clustering 26
active session failover 39
compared to VRRP 68
forwarding mode 43
IPSO 38, 40, 67
master node 40
multicast mode 43
options 42
unicast mode 43
combining gateway and firewall 64
command-line interface. see CLI
command-line interface. See CLI.
commit bit 33
configuration
IKE phase 1 31
IKE phase 2 32
CRL 36

D
data encryption standard. See DES and 3DES.
data link layer VPN 26
DES 101
DH. See Diffie-Hellman.
Diffie-Hellman 31, 32
defined 102
group number 31
group, and PFS 32
groups supports 31
lifetime 31
digital certificate 35
DNS name in certificates 37
documentation
conventions 10
related 11
DVMRP 66
Dynamic 40
dynamic addressing 15
dynamic load balancing 26, 38
defined 40
dynamic mode 45
dynamic routing, defined 65

E
element management 17
capsulated security protocol. See ESP.
capsulating security payload. See ESP.
cryptography
encryption algorithms 100
asymmetric 33
private key 33
public key 33
symmetric 33
cryptography algorithms 100
ESP
authentication algorithms 97
defined 27
encryption algorithms 100
IPSec protocols 27
overview 96
transport mode 97
tunnel mode 59
external CA 36, 37

F
fault tolerance 16, 38
features
access control 14
authentication methods 15
CLI 47
dynamic addressing 15
element management 17
fault tolerance 16
Nokia Horizon Manager 17
PKI 15
routing services 15
security token 47
SSL 48
VPN protocols 14
files, backing up and restoring 82
filtering
firewall 60
unencrypted packets 57, 58
firewall
combining with gateway 64
filters 60
forwarding IPSec traffic 56
gateway inside 58
gateway outside 56
gateway parallel to 61
policy 60
forwarding
IPSec 57
IPSec and unencrypted traffic 58
mode 43
full mesh topology 55

G
gateway
combining with firewall 64
forwarding IPSec traffic 56
inside firewall 58
parallel with firewall 61
placement 25, 56
placing outside firewall 56
single interface configuration 63
group number, Diffie-Hellman 31

H
hardware
Nokia gateways 14
hub and spoke 51

I
IKE
authentication 30
main mode 31
phase 1 options 31
phase 2 options 32
preshared keys 34
quick mode 32
quick mode commit bit 33
inside firewall gateway placement 58
internal CA 36
internet engineering task force (IETF) 27
internet key exchange. See IKE.
Internet security. See security.
IP address, in certificates 37
IP clustering 26, 38
IPSec
advantages 27
AH 27
authentication algorithms 97
benefits 27
defined 27
ESP 27
forwarding 57, 58
how it works 28
overview 95
security association database 29
security associations (SAs) 29
transport mode 95
tunnel mode 28, 95
IPSO 26
clustering 38, 40
defined 40
operating system 14
upgrading 81
IPSO clustering
compared to VRRP 69
management 42
options 42
K
keepalive
adaptive 40
referee 44
L
L2TP, limitations 26
layer 2 tunneling protocol. See L2TP.
layer 2, VPN 26
layer 3 VPN 26
layer 4 VPN 26
lifetime
algorithms 99
Diffie-Hellman 31
SA 29, 33
logging. See syslog.
M
management
IPSO clustering 42
policy 18
system 18
management connections, ports used for 60
man-in-the-middle attack, preventing 24
master node 40
MD5, overview 98
mesh topology 53
full 55
partial 54
message digest 5. See MD5.
message digest, overview 97
message integrity 23
multicast mode 43
N
NAT 45, 70
dynamic mode 45
SecureNAT 45
static mode 46
network
layer VPN 26
network address translation. See NAT.
network time protocol. See NTP.
network topology
full mesh 55
hub and spoke 51
mesh 53
partial mesh 54
single-hub 52
star 52
Nokia Horizon Manager
support for 17
using 82
NTP 79
operating system, IPSO 14
OSI 7-layer model
  layer 2 26
  layer 3 26
  layer 4 26
OSPFv2 66
parallel with firewall gateway placement 61
partial mesh topology 54
PAT 70
perfect forward secrecy. See PFS.
phase 1, configuration 31
phase 2
  configuration 32
  IKE, commit bit 33
PIM-DM 66
PIM-SM 66
PKI 15
  asymmetric encryption 33
  internal CA 36
  symmetric encryption 33
PKI certificate 35
point-to-point tunneling protocol. See PPTP.
policy management 18
port address translation. See PAT.
port numbers, SMART 61
ports for management connections 60
PPTP, limitations 26
preshared keys
  description 34
  recommended length 34
privacy 24
private
  IP addressing 24
  key, encryption 33
private network, traditional 22
public key
  certificate 35
  encryption 33
  raw 34
  See also PKI.
public-key infrastructure. See PKI.
quick mode 32
raw public key 34
RC5 102
related documentation 11
replay protection 24
restoring files 82
RIP
  RIPv1 66
  RIPv2 66
RIPEMD, overview 98
routing
  basic, defined 64
  dynamic, defined 65
  issues with VPN configuration 69
  protocols supported 66
  static, defined 65
  types 65
routing protocols supported 66
branch office gateways 66
central office gateways 66
routing services 15
RSA signature key 37
IPSec 29
  lifetime 29, 33
secure hash algorithm 1. See SHA-1.
secure internal communications. See SEC.
secure shell. See SSH.
secure sockets layer. See SSL.
SecureNAT 45
security
  association database 29
  authentication 24
  message integrity 23
  privacy 24
  replay protection 24
  VPN benefits 24
security association. See SA.
security parameter index. See SPI.
security policy database. See SPD.
security token 47
SHA 98
SHA-1 98
SIC 49
signature key, RSA 37
simple network management protocol. See SNMP.
single interface configuration 63
single-hub topology 52
site-to-site VPN 37
SMART 60
  port numbers used 61
SmartCenter 49
  Check Point 35
SNMP 80
  branch office gateways 81
  central office gateways 81
  traps 80
software, Check Point 14
SPD 25, 30
SPI 29
SSH 47
SSL 48, 49
  configuring with CLI 49
  configuring with Voyager 49
star topology 52
stateful inspection 46
static mode 46
static routing, defined 65
subjectaltname 37
supported routing protocols 66
symmetric encryption 33
  PKI 33
syslog 80
system management 18
TCP/IP
  addressing problems 24
  private addressing 24
topology. See network topology.
transport layer VPN 26
transport mode
  AH 96
  ESP 97
  IPSec 95
trust relationships 35
tunnel mode 28, 59, 95
unencrypted packets, filtering 57, 58
unicast mode, clustering 43
virtual private network. See VPN.
VPN
  benefits 21
  creating Nokia IP VPN 24
  creating site-to-site 37
defined 21
gateway placement 25
how it works 26
layer 2 26
layer 3 26
layer 4 26
routing issues 69
security benefits 24
VPN protocols 14
VRRP 68
  compared to clustering 68
  compared to IPSO clustering 69

X
X.509 certificate 35, 36, 37