Because of its extensive functionality, IP Clustering technology will be phased into IPSO in a series of releases. The first implementation, in IPSO 3.6, clusters both firewall and VPN services. This is the first time Nokia's IP Clustering technology has been integrated with a firewall application, services that behave quite differently than a VPN application. This document has been prepared for NIC Sales and describes the implementation of IP Clustering with IPSO 3.6 and Check Point's VPN-1, as compared to the Nokia CC VPN solution. It should be used as guide for existing Nokia CC VPN customers who need to understand how their products are being migrated to a new solution. Refer to the Appendix for a chart comparing AOS and IPSO clustering features.

Nokia IP Clustering in IPSO:

Reliable, Scalable VPN-1/FireWall-1 Solutions

Beyond security itself, reliability is the most important attribute of any network security device. To be truly useful to the enterprise, that reliability must include:

– **High availability** – the instantaneous failover to a redundant device of even the most delicate connections, like IPSec security associations in a VPN, in case of fault

– **Scalability** – increase in throughput and tunnel capacity that leverages prior investments in VPN and firewall devices by smoothly adding capacity to the original configuration…while it's running

– **Maintainability** – upgrade, reconfiguration, and replacement of devices in a cluster of security devices without a moment of application downtime… Nokia calls this "zero downtime maintenance".

There's generic "clustering" and then there's "IP Clustering"

Clustering technology can be used to enhance reliability, but not all clustering technologies are created equal. The industry term "clustering" is generally used to describe multiple systems forming what appears to be a single, larger, highly reliable system. Nokia's clustering functionality, specifically tailored with the needs of VPN and firewall products in mind, goes beyond this basic level. While generic clustering can provide load balancing, it doesn't necessarily provide dynamic load balancing and rebalancing, and while generic clustering can provide failover, with application information preserved, this failover is typically applied to preserving server content, not to the more challenging requirements of TCP and VPN application state. Nokia uses its patented IP Clustering technology to accomplish this additional functionality.

IP Clustering is distinguished by two unique attributes, "Active Session Failover" and "Dynamic Load Balancing", described more fully below. IP Clustering is integrated into the hardened Nokia IPSO operating system. IP Clustering in IPSO (starting with version 3.6) gives customers high availability, scalability and maintainability. But, unlike third party firewall and VPN clustering technologies, it involves tight integration of the OS kernel and IP Clustering code, it includes tight integration with Check Point's VPN-1 and FireWall-1 applications, it works with Nokia Horizon Manage r, and it carries the Nokia brand commitment to quality.

IP Clustering "Dynamic Load Balancing" vs traditional external load balancing devices – In a traditional load balancing scenario, a separate load balancing device controls the flow of network traffic to and from servers behind the load balancing device itself. The servers are typically a heterogeneous mix of content servers, e.g. e-mail, web, and database servers. On the other hand, with IP Clustering, a group of homogenous network devices, in other words a "cluster", provides high availability, scalability and maintainability for the cluster itself and for the specific application, such as VPN-1 and/or FireWall-1 functionality running on the clustered devices. Both approaches to load balancing have clear value in a network, but they perform it differently.

The remainder of this document describes the clustering functionality users can expect from the implementation of IP Clustering technology in IPSO 3.6.

Firewall/VPN Market Requirements

Enterprise and service provider networks depend on the constant availability of network devices such as firewall and VPN gateways to maintain continuous, uninterrupted services for employees, partners, and customers. Minutes of network downtime can cost companies millions of lost dollars. No room exists for gateway failure. Downtime, even during a planned upgrade is also a constraint to business operations. Since no single network component can be guaranteed to be faultless, and since reconfiguration and upgrades are inevitable, availability needs to be assured through redundancy. As processing load on network devices increases, automatic distribution of load between redundant devices becomes more challenging. While load distribution can be achieved for classic packet forwarding or routing, it becomes computationally difficult to guarantee optimal load distribution with redundancy when maintaining active IPSec tunnels in VPNs.

Networks using firewalls and VPNs are greatly enhanced when they can: 1) provide scalability for VPN/firewall services; and 2) ensure connectivity to those using these VPN/firewall services. These two requirements define key shortcomings currently present in firewall and VPN gateway offerings on the market today. Nokia initiated an extensive, highly focused effort to determine how to distribute IP packet processing load among network devices to guarantee effective scalability and redundancy. These two shortcomings were eliminated through Nokia's development of IP clustering technology.

About Nokia IP Clustering Technology

Nokia patented IP clustering technology allows several devices to act as a single network entity, sharing one internal IP address, one external IP address, one DMZ IP address, etc. Acting as a single entity, these devices are called a **gateway cluster**. A gateway cluster is made up of multiple gateway nodes. Each gateway node in a cluster has unique real IP addresses for each interface, and all gateway nodes share a common virtual IP address for each interface. The interfaces are used for intracluster communication and network traffic.

IP packet processing is distributed among all member gateway nodes to achieve equal member processing loads. Using IP clustering technology, several gateways can be clustered together to create a distributed and fully redundant architecture for supporting networking functions. Each gateway node continually maintains state information on all of the activities occurring on each of the other gateway nodes in the cluster, so that failure of any one gateway node and automatic failover of its workload to other nodes has no perceived effect on the active firewall or VPN services across the gateway cluster. In addition, the performance of a gateway cluster can be increased dramatically as network requirements grow by simply adding more gateway nodes to an existing cluster.

How Dynamic Load Balancing Works

A network device equipped with Nokia's IP clustering technology handles load balancing of its own activities differently than other VPN or firewall solutions. The gateway cluster members elect a master member gateway. The master member keeps track of the workload, processing power, and state of all gateways and then allocates workloads so that the load is distributed evenly. The master member also serves as an active member of the cluster, handling its share of the load.

As additional gateways are added to the cluster, the load is automatically balanced among the new gateways. This behavior allows administrators to easily upgrade a cluster to include more gateways with no downtime because VPN and firewall services are not interrupted during the upgrade. Gateways can also be removed from a cluster at any time without interrupting VPN or firewall services. Some UDP packets may be lost, but TCP connections and VPN tunnels will be maintained.

How Active Session Failover Works

In a gateway cluster, one gateway node is elected to be a master member. All members (including the master member) do work and actively keep track of other members. A gateway cluster uses a keepalive mechanism to monitor the health of all its members. The master member sends multicast keepalive messages to the other cluster members. The members send keepalive messages to the master member. If a gateway should become unavailable for any reason, pl anned or unplanned, or if the load needs to be rebalanced throughout the gateway cluster, IPSec SA sets and TCP/UDP connections are assigned to other gateways within approximately a second. The keepalive mechanism is a proactive method for allowing members to confirm presence of other gateways and have work allocated to the other gateways when needed.

Active Session Failover as applied specifically to VPNs

Nokia IP clustering technology provides availability of VPN services by providing redundancy for all active IPSec tunnels. More specifically, each gateway continually tracks IPSec SAs (security associations) occurring on all cluster members. IPSec SAs can be thought of as “tunnel building blocks” because they contain information like encryption algorithms and key lifetimes that are used for setting up and maintaining tunnels. In the cluster, IPSec SAs are grouped together in sets and separate gateway nodes work on these sets. Each gateway node has knowledge of current IPSec SA sets being worked on across the cluster and is assigned its own IPSec SA set to work on. As IPSec SA work sets change, that information is communicated to all the other gateway nodes in the cluster. During failover, IPSec SA sets do not have to be communicated to other gateway nodes since they are already aware of them. The sets are simply reassigned to another active gateway node by the current master member. This reassignment is completely transparent to endpoints of the session—mobile users and other gateways. Since IPSec tunnels do not need to be rebuilt during or after failover, mobile users and other gateways do not experience disruption of VPN services (or connectivity).

THE STATEMENTS HEREIN ARE BASED ON AVAILABLE TO NOKIA INTERNET COMMUNICATIONS AT THE TIME OF PUBLICATION AND ARE OF A DESCRIPTIVE NATURE ONLY. THE STATEMENTS HEREIN ARE NOT INTENDED TO CONVEY ANY EXPRESS OR IMPLIED WARRANTY, ALL OF WHICH ARE DISCLAIMED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. WARRANTIES, IF ANY, FOR THE PRODUCTS DESCRIBED HEREIN SHALL BE GOVERNED BY NOKIA INTERNET COMMUNICATIONS' TERMS OF PURCHASE AT THE TIME OF SALE OR LICENSE.