What are the benefits of Nokia IP Clustering in IPSO?

By providing redundancy, IP Clustering in IPSO prevents a single point of failure in network gateway function (firewall/VPN), dramatically improving gateway and network availability. If one gateway node in the cluster of nodes should fail for any reason, or a gateway is removed from the node for maintenance, its workload is automatically and transparently shifted to the other nodes in the cluster. No TCP connections are dropped, nor are any IPSec VPN security associations lost, so the failover transition is invisible to network users.

Further, gateway performance (throughput, connection rate) will scale with the addition of each gateway node into the cluster. Cluster performance scaling enables incremental growth to match growing network requirements, and is a way to meet even the most challenging performance requirements that can't be met with a single gateway device. Effective performance scaling requires dynamic load balancing – a function inherent in IPSO's clustering protocol.

Why would I want to use a clustering approach to obtain high availability?

High availability is achieved through redundancy with the intent of avoiding any potential single point of failure. That redundancy can be implemented at one or more of several levels – component level, subsystem level, or network device level. Redundant devices can be configured for active-standby, where one or more devices stand by to take over the workload normally handled by the active device, or all devices or can share the workload on an ongoing basis (active-active) and the workload of an active device that fails is redistributed to the other active device(s). A cluster builds network device-level redundancy, with workload statically shared or dynamically balanced across the redundant devices. A dynamically load balanced cluster adds the benefit of effective performance scalability to the inherent high availability.

If Check Point has ClusterXL why did Nokia develop its own clustering?

Nokia has perfected its patented IP Clustering technology independently in its CC-series VPN product line. This high performance, field-proven, dynamic load balancing cluster technology has been migrated to IPSO in version 3.6 to support firewall and VPN clusters in conjunction with Check Point™ VPN-1®/FireWall-1®. Nokia and Check Point worked together on the integration of this technology and it is their premium HA solution on Nokia IPSO-based platforms. By contrast, ClusterXL is an HA solution for VPN-1/FireWall-1 running on Linux, NT or Solaris that sits on top of the general purpose OS without the high degree of integration found in IPSO's IP Clustering. ClusterXL only has static load sharing – comparable to IPSO's VRRP solution. IP Clustering in IPSO, with dynamic load balancing, is offered at no additional cost in Nokia's security appliances.

How does IP Clustering in IPSO compare to ClusterXL for Linux, NT and Solaris?

The name "ClusterXL" implies both high availability and scalability, but in fact, ClusterXL does not provide dynamic load balancing, which is required for effective performance scaling. Static load sharing involves a predetermined, fixed function for determining assignment of traffic to cluster nodes, independent of traffic patterns. The decision function might be based on IP addresses, ports, and/or IPSec SPI parameter. The fixed decision function doesn't enable adaptive reassignment of traffic to other nodes as traffic patterns vary. Quite likely, traffic sent to one node will exceed that node's capacity and traffic will be lost, while other nodes still have slack unused capacity. The effect is that cluster capacity is capped at a fraction of the traffic that could be handled by a dynamically load balanced cluster.

Thus, ClusterXL is comparable to IPSO's VRRP high availability and load sharing solution, while IP Clustering in IPSO provides dynamic load balancing to enable effective performance scaling.

What are the patented elements of IP Clustering in IPSO that make it superior?

Nokia's patents covering IP Clustering disclose a novel clustering protocol that minimizes overhead (which optimizes performance scalability), and includes an adaptive heartbeat that minimizes failover time in the case that a gateway node fails or is removed from the cluster. At the same time, unnecessary failovers are minimized in the event of normal packet loss on the intracluster network segment. The result is a robust gateway that scales effectively with additional nodes, and fails over rapidly should a node fail, redistributing workload to remaining active nodes.

Can IP Clustering in IPSO and ClusterXL for Linux, NT and Solaris work smoothly together (are they compatible)?

Since IPSO's IP Clustering protocol is not implemented in Check Point's ClusterXL, a cluster can't consist of a mix of IPSO-based security appliances and Linux, NT or Solaris workstations running ClusterXL.

Will Nokia IP series appliances support ClusterXL?

Since Nokia's security appliances already offer the benefits of ClusterXL at no additional cost (through their VRRP high availability and static load sharing solution) and since Nokia now offers, in addition, IP Clustering in IPSO, with dynamic load balancing, there is no need to support ClusterXL.

Will ClusterXL take advantage, technically, of IP Clustering in IPSO?

No. ClusterXL for Linux, NT and Solaris is not related to IP Clustering in IPSO.

Will IP Clustering in IPSO take advantage, technically, of ClusterXL?

IPSO's IP Clustering leverages Check Point's firewall/VPN synchronization feature, present in VPN-1/ FireWall-1 since version 4.1. Firewall/VPN sync ensures that all active TCP connection states, UDP "pseudo-connection states," and VPN security associations in every cluster node are replicated in every other node in the cluster to enable Active Session Failover – failover without loss of TCP connection states, UDP "pseudo-connection states," or IPSec security associations.

How much does ClusterXL for Linux, NT and Solaris cost?

Check Point has set the suggested list price of ClusterXL for Linux, NT and Solaris at $10,000 per cluster. (Refer to the current Check Point price list for any pricing changes and/or promotions.)

How much does IP Clustering in IPSO cost?

IP Clustering in IPSO is provided as part of IPSO 3.6 at no additional charge.

Do I need both or will one be enough (so that I can save money)?

Use VRRP, or IP Clustering in IPSO where effective performance scaling is also required. Both are provided in IPSO at no additional cost. ClusterXL is not available for Nokia's security appliances, as it provides no additional value to the Nokia-Check Point IPSO-based offering.

Even if I don't absolutely need both to achieve greater availability, is there a reason to buy both anyway, i.e. even greater availability ("belt and suspenders")?

No, not at all. Nokia's VRRP solution provides a complete high availability solution, and IP Clustering in IPSO provides a complete high availability and scalability solution.

If I'm just going to use just one, which one should I use?

IP Clustering in IPSO provides the most complete and the most highly integrated high availability and scalability clustering solution for Check Point VPN-1/FireWall-1.

What's the difference between IP Clustering in IPSO and VRRP? When do I use each HA solution?

While both are effective high availability solutions, IP Clustering in IPSO adds dynamic load balancing, which allows the maximum performance to be obtained from the cluster since the workload is evenly balanced across each node. Each gateway node in the cluster can approach its maximum workload capacity, and the performance of the cluster will scale with the number of nodes. On the other hand, with VRRP (and ClusterXL for Linux, NT and Solaris), static load sharing is unable to dynamically level the workload across the nodes, meaning that quite likely, traffic sent to one node will exceed that node's capacity and traffic will be lost, while other nodes still have slack unused capacity. The effect is that cluster capacity is capped at a fraction of the traffic that can be handled by a dynamically load balanced cluster.

What's the difference between IP Clustering in IPSO and Nokia BIG-IP load balancing and failover? When do I use each HA solution?

An external load balancer hardware solution like the Nokia BIG-IP product can be used to balance firewall and VPN traffic for high availability and scalability, but is more commonly used to balance content servers, e.g. web servers. Only the most extreme gateway scalability requirements that cannot be met by a software-only solution (like IP Clustering in IPSO) call for an external load balancer. The external load balancing device will offload the gateway nodes of cluster protocol traffic required in a software-only solution, enabling each gateway to maintain its traffic handling capacity even as the cluster size grows.

Does IP Clustering in IPSO consist of Check Point code or is it something separate that Nokia has created?

IP Clustering in IPSO is a collaborative effort between Nokia and Check Point. While it is Nokia intellectual property, it is a clustering-based solution for Check Point VPN-1/FireWall-1 gateway applications running on the IP series platforms, and it does cooperate with the Check Point firewall/VPN synchronization feature.