USE CASE 4: HIGH AVAILABILITY—CLUSTERING

A single firewall can be a single point of failure. This can affect the availability of business-critical applications and complicate the maintenance of firewall equipment. Clustering firewall nodes together can significantly reduce the risk of these problems while also supporting higher performance. Firewall clustering allows uninterrupted operations during system maintenance and updates and is transparent to users.

McAfee Next Generation Firewall offers high availability by natively "clustering" as many as 16 firewall cluster nodes without using extra load-balancing products. If any individual nodes fail, others will keep going. And you can perform maintenance or add nodes to scale performance and availability without compromising service. For the administrator, the cluster is managed as a single firewall entity.

Design

A McAfee Next Generation Firewall cluster is a single virtual entity that can include from two to as many as 16 physical devices (Figure 28). Each physical device that makes up the firewall cluster is called a firewall node (FW node).

McAfee offers two types of clustering: active-standby and active-active. In active-standby clustering, only one node at a time processes traffic, and the other nodes wait on standby, ready to take over when the currently active node goes offline. Nodes that should not take over automatically can be set offline as usual.

In active-active mode, the firewall engines dynamically load balance individual connections between the nodes, transparently transferring connections to available nodes in the event a node becomes overloaded or experiences a failure. Clustering in active-active mode improves performance when heavy packet processing functions are needed, such as deep inspection, VPNs, application identification, URL logging, or complex policies.

When you design a firewall cluster, ensure that, if one or more nodes goes offline, the remaining nodes have enough capacity to handle the increased load. For example, in a three-node cluster with a 50%-50%-50% load on each node, if one node goes down, then the remaining two nodes will be able to handle 75%-75% load. But if the three nodes are at 80%-80%-80% load each and one node goes offline, the remaining two nodes will become overloaded.

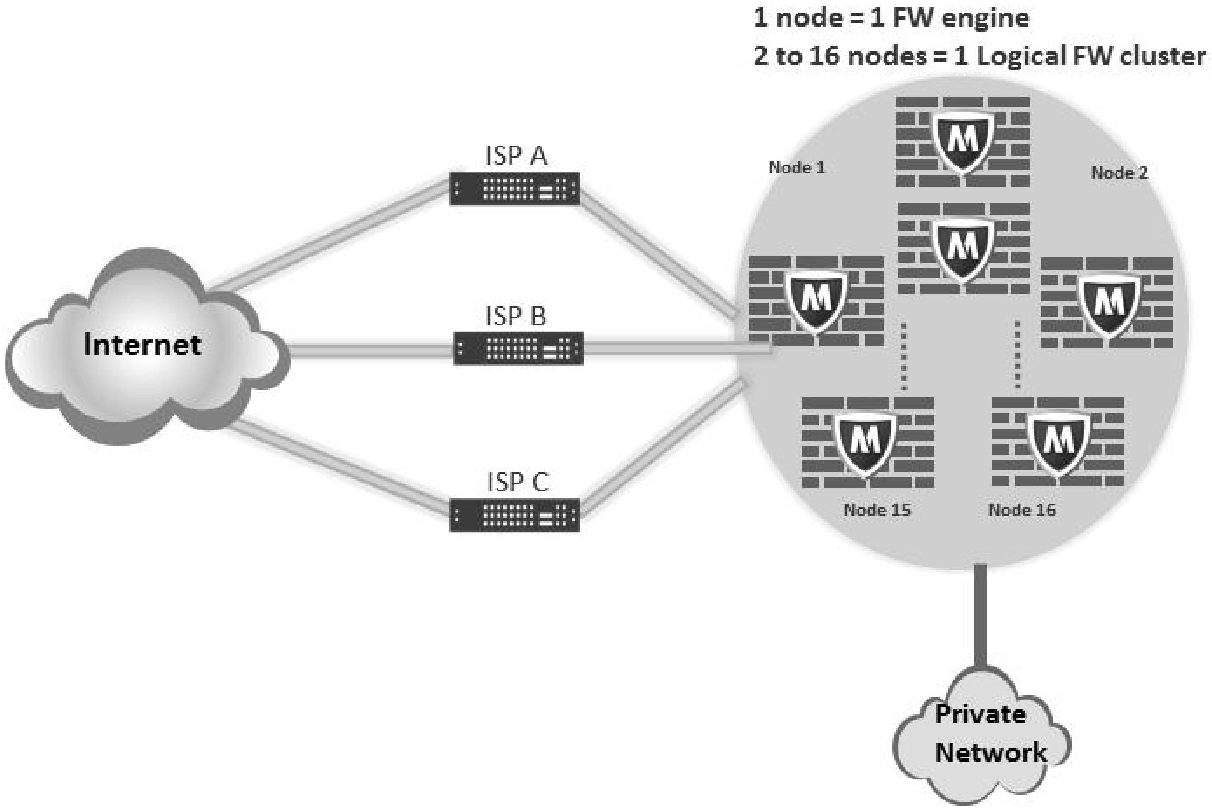

Figure 28. McAfee Next Generation Firewall native clustering of up to 16 firewall nodes.

McAfee Next Generation Firewall Node Interfaces

There are two types of interfaces on a node:

- **Cluster virtual interface (CVI)** is a logical interface shared by all nodes in a cluster and is used for traffic routed through the firewall for inspection.
- **Node-dedicated interface (NDI)** handles communication between nodes, as well as between the nodes and the McAfee Security Management Center server.

The cluster's firewall nodes exchange information constantly. The state tables that list open connections (state sync) and the operating state of the other nodes (heartbeat) are exchanged. This exchange of information ensures that all nodes have the same information about the connections and that if a node becomes unavailable, the other nodes of the cluster immediately detect this. The exchange of information between clustered firewall nodes is synchronized through selected interfaces via a heartbeat network using multicast transmissions.

One NDI on a node must be selected as the primary heartbeat interface. Another NDI should be configured as the backup heartbeat interface. A dedicated network is recommended for the primary heartbeat.

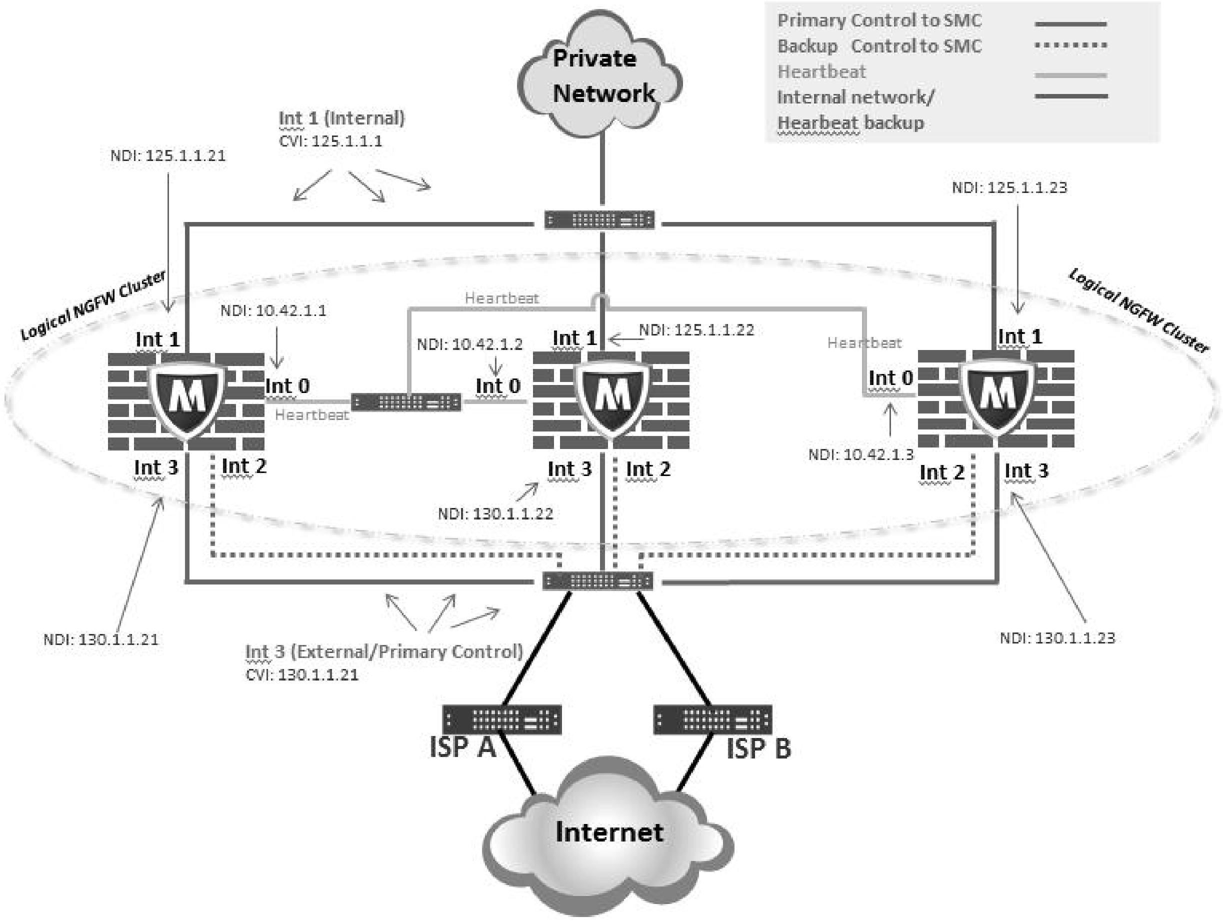

Figure 29. McAfee Next Generation Firewall node interfaces in a three-node cluster.

Because of their dual role as members of a common virtual entity and as separate physical devices, firewall engines in a cluster have two types of IP addresses:

- ***Cluster virtual IP address* (CVI)—**An IP address that is used to handle traffic routed through the cluster for inspection. This is an IP address that is shared by all nodes in a cluster, in effect making the node appear as if it were a single entity for the outside network behind the IP address.

- ***Node-dedicated IP address* (NDI)—**An IP address that is used to handle traffic from or to a single node in a cluster. These IP addresses are used for the heartbeat connections between the engines in a cluster, for control connections from the McAfee Security Management Center server.

You can configure several CVIs and/or NDIs on the same physical interface.

In the example in Figure 29, interface 1 is used as the CVI for protected network traffic and for the heartbeat backup. Interface 3 is used as the CVI for Internet traffic (for example, Internet traffic from clients in the protected network). It is also the primary control NDI for management server. Interface 2 is the backup control NDI for management server. Interface 0 on each node is the NDI used for heartbeat traffic between the nodes in a dedicated network. There is no CVI on Interface 0, since it handles only node-to-node traffic.