Editorial Brief

Eight Ways to Improve Your Network High Availability

Put your next-generation firewall to work

High availability is a must in our current cyberculture, and several advanced features that should be part of your next-generation firewall can help ensure that your network and your enterprise are continually up and running.

1. Centralized Management Reduces Response Time

High network availability requires that your team knows what is going on in your network at any given time. It also requires organizations to empower that team to make business-critical changes without risk of downtime. Running back and forth to different devices doesn't work even if you can log in remotely. It takes too much time and is not coordinated. You have to rely on a centralized management system.

Today's next-generation firewalls (NGFWs) can act as the core of your network security, centralizing monitoring, managing, and reporting across diverse virtual, physical, and third-party devices. NGFWs can also give your team real-time visualization of network operations, improving response time for recognition and remediation of incidents and threats.

Centralized management is a key capability for deployment of appliance initial configurations, policy updates, and software patches. This reduces overall risk to availability, as well as time needed to perform these business-critical and compliance-related changes on the fly. In the long run, this will incur significant savings in everything, including off-hour change windows. It also reduces the time needed to test and deploy changes across multiple devices and locations and give your network IT staff the ability to focus on other important tasks and not be consumed by regular network security operations.

2. Multilayer Inspection Technology

Multilayer inspection technology digs deep into traffic streams, inspecting at all layers of the Open System Interconnection (OSI) model. Superior NGFWs still inspect packet headers, but they don't stop there. They dive deep to examine the entire packet and its encapsulated data. This is done through a data-stream-based, full-stack normalization and inspection process. This way, all protocol layers are normalized continuously, providing full stack visibility identifying hidden attacks, and removing malware. Rather than relying on traditional firewall methods of merely screening the packet header and then the payload in a layer-segmented approach, multilayer inspection carefully examines the packets in a streamed approach across all layers, ensuring that traffic streams as a whole, rather than just individual packets, are safe.

The most advanced NGFWs use multilayer inspection technology that can detect and block attacks from any type of malicious invaders, including those engaging in advanced evasion techniques (AETs). These stealthy cyberattack methods rely on a multilayered approach to easily bypass many traditional security devices, so by making sure that your NGFW can perform deep-packet inspection and full data normalization as part of its inspection process, you ensure your network is protected from these sophisticated attacks.

3. Clustering

Clustering devices is a must for uninterrupted operations, especially during system maintenance and updates. Each component that is part of that cluster handles its optimal share of connections, depending on environmental variables at any given time.

Clusters must pay attention to nodes that are coming online and going offline, moving connections from one node to another as the situation warrants. Packets that belong to one connection or a set of related connections may sometimes be handled by different nodes within the cluster, requiring targeted synchronization across the nodes.

While old-school devices may have only synchronized all nodes periodically, high-end NGFWs can increase the synchronization that takes place in predetermined situations or they can even replace periodic synchronization with synchronization initiated by new connections or specific node requests rather than periodically across the board.

The end result is a savings of bandwidth and memory on the cluster nodes, leading to cost-effective use of network hardware and resources. The most capable NGFWs will feature active-active/active-standby firewall clustering for up to 16 nodes, instead of the usual two to four, along with intrusion prevention system (IPS) clustering and SSL VPN clustering.

4. Active-Active Load Balancing

Clustering is a strategy that can help with load balancing, which is another key feature of effective NGFWs. Load balancing involves the automatic distribution of traffic or operations to the components most able to handle it at any given time. The most advanced NGFWs will come with an integrated server that has load-balancing capabilities along with firewall load balancing for at least a dozen or more nodes.

While active-passive load balancing relies on one component doing all the work while the other stands by in case of failure, active-active load balancing allows two components to work as a team to efficiently distribute the workload. Active-active configuration also keeps track of information requests from specific users, retrieving information from the cache and fulfilling the request without needing to send it to the network server. This reduces your traffic load, enhances performance, and once again enables high availability for your network.

5. Multiple ISP Linking Technology

Using new technology like McAfee Multi-Link, you can now combine separate ISP connections into a high-throughput and highly available Internet access solution so that you can significantly reduce connectivity costs. McAfee Multi-Link technology lets you use multiple ISP connections with smart load sharing, resulting in maximum reliability, speed, traffic shaping, and cost effectiveness. The most advanced NGFWs will apply this technology to your virtual private networks as well, serving up a McAfee Multi-Link VPN, which lets you easily build resilient and secure office-to-office connections.

McAfee Multi-Link VPN fortifies your network by combining independent connections into a high-bandwidth and highly available Internet access solution. If your NGFW utilizes this technology, you won't need to go through any special setup or coordination. All you need to do is select the configuration that should be already integrated into your NGFW's central management center.

McAfee Multi-Link technology is a prime solution for any company that requires always-on Internet connectivity, providing a cost-effective and robust alternative to point-to-point strategies, such as multiprotocol label switching (MPLS).

6. Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is another key feature that ensures high availability with your NGFW. This Internet protocol lets you have one or more backup routers at your service when you are using a router on your local area network, or LAN.

The traditional arrangement involves designating a single router to handle the task of forwarding packets from a collection of hosts on a LAN. The big problem with this setup is having no backup router available should your designated router fail. VRRP eliminates that risk by letting you specify a virtual IP address as your default router.

All routers share the virtual IP address, with a single router selected as the master and others selected as backups. Should your master router ever fail, a backup router automatically comes into action, as designated by the virtual IP address, and the backup then serves as your master router. NGFWs can use VRRP to not only protect against having a single potential point of failure, but to also help with load balancing.

7. Interface Link Aggregation (802.3ad)

NGFWs that feature interface link aggregation provide secure and redundant connectivity over multiple connections, a notable step up from conventional connections that rely on individual interfaces. Link aggregation allows you to aggregate multiple physical interfaces as one, giving you a robust, flexible, and completely fault-tolerant firewall cluster.

Current NGFWs include support for link aggregation that allow load balancing across these multiple interfaces, as well as the ability to provide high availability. This way, even if an individual physical link goes down, your link aggregation will continue to function and provide automatic recovery as long as at least one of the physical links is working. Interface link aggregation can result in an increase in bandwidth that leads to faster connectivity and a higher transmission speed, along with higher availability overall.

8. Stateful Failover

Stateful failover is one more essential NGFW feature to ensure continuous security and availability throughout your network. Stateful failover keeps a record of activity, so if you experience any downtime, your environment continues to process and forward your NGFW traffic uninterrupted. Link failure detection is another feature that can protect your network from downtime, letting standby components automatically take over if needed. With active-active clustering, high availability is guaranteed by automatically distributing the load across multiple members of the cluster while maintaining a constantly updated state table. This is done through an incremental state synchronization, which will continuously update state synchronization across all members of the cluster as state changes occur dynamically. This way, any member of the cluster may actively take up any connections by a failed member of the cluster, should hardware failure occur due to environmental incidents or otherwise.

About the Author

Joe Metzler is currently a regional security engineer at McAfee, now part of Intel Security. He works with customers to help design and implement solutions for enterprise network security, including advanced application of next generation firewall technologies. Joe holds a Bachelor of Science in Cyber Security Systems and Network Security from St. John’s University.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com