McAfee Multi-Link

Always-on connectivity with significant savings
Table of Contents

Executive Summary ................................................................. 3
How McAfee Multi-Link Works ................................................... 4
  Outbound traffic ................................................................. 4
  Load balancing ................................................................. 4
  Standby links for high availability ....................................... 6
  Quality-of-Service (QoS) classes ......................................... 7
  Activating outbound McAfee Multi-Link for selected traffic only ........................................... 7
Inbound Traffic .......................................................................... 8
VPN Traffic ............................................................................... 10
Executive Summary
In today’s 24/7/365 world, organizations of all sizes and types depend on always-on network connectivity. Service interruptions can mean lost revenue when an online trading company cannot execute orders, lost clients for a law firm if their attorneys cannot file briefs in time, or even lost lives if critical patient data is not immediately available when needed. According to the study performed by Ponemon Institute, sponsored by Emerson Network Power,1 the cost of a data center outage has increased since 2010. The cost per square foot of data center outages now ranges from $45 to $95. Or, according to the study, a minimum cost of $74,223 to a maximum of $1,734,433 per organization. The overall average cost is $627,418 per incident. Whether communicating with customers, partners, or employees, organizations rely on continuous connectivity anytime, anywhere.

Traditionally, connections provided by Internet links have been a single point of failure. To eliminate this risk, organizations have resorted to complicated and costly solutions such as redundant systems, separate “failover” or “standby” products, complex protocols like border gateway protocol (BGP), and different connection types like multiprotocol label switching (MPLS) and frame relay.

Now there’s a better approach—McAfee® Multi-Link technology built into the McAfee Next Generation Firewall. McAfee Multi-Link is ideal for providing organizations with highly available Internet connectivity in a simple, straightforward, and cost-effective manner. If one line fails, traffic is automatically switched over to the remaining links. McAfee Multi-Link eliminates the need for complicated solutions like BGP or separate wide area network (WAN) load balancer solutions, which not only means cost savings, but also a simplified infrastructure.

McAfee Multi-Link technology can integrate with any type of connection to ensure that inbound, outbound, and VPN traffic is delivered securely through the fastest connections without incident or disruptive downtime. McAfee Multi-Link can accommodate digital subscriber lines (DSL), leased lines, cable modems, satellite, mobile broadband, and even WAN links such as point-to-point MPLS. Organizations gain the flexibility to deploy the type and number of connections that are best suited for their environments and their budgets.

Combined with active load balancing and Quality-of-Service (QoS) capabilities, McAfee Multi-Link also optimizes networks and supports technologies, such as Voice-over-IP (VoIP) and video conferencing. Organizations gain granular control of their networks and ensure the availability of applications that are mission-critical to their operations.
How McAfee Multi-Link Works

Outbound traffic
A single connection to the Internet is a single point of failure. If the connection becomes unavailable, all outbound traffic is blocked. To prevent this, patented McAfee Multi-Link technology distributes outbound traffic between multiple network connections. McAfee Multi-Link ensures that Internet connectivity remains available even if one or more network connections fail. McAfee Next Generation Firewall can also load balance outbound traffic between network connections to use the available Internet connection capacity more efficiently.

Organizations can use McAfee Multi-Link on both single and clustered firewalls. The network connections for McAfee Multi-Link are represented by netlink elements in McAfee Security Management Center (McAfee SMC). In most cases, a netlink element is used to represent an Internet service provider (ISP) connection. However, netlinks can also represent a leased line, xDSL, or any other type of network connection mediated by the firewall.

Load balancing
There are two load balancing methods: round-trip time and ratio. When the round-trip time method is used, netlink performance is measured for each new transmission control protocol (TCP) connection by sending the initial request (SYN) to the destination through all the available netlinks. When the destination host sends the reply (SYN-ACK), the netlink that receives the reply first is used to complete the TCP connection establishment. The firewall cancels the slower connection attempts by sending a TCP reset (RST) to the destination through the other netlinks. This way, the fastest route is selected automatically for each connection based on the round-trip time measurement.

Information about the performance of each netlink is cached, so no new measurement is made if a new connection is opened to the same destination within a short time period.

Figure 1. Select the fastest netlink for outbound connections.
There are, however, times when a ratio method may be preferred. For example, if one ISP’s bandwidth far exceeds other connections being used and is supplemented by smaller ISPs, the smaller ISP may return a faster SYN-ACK. While this may seem like the “fastest” connection, it may not take into account the proportionate bandwidth available. McAfee Multi-Link technology can resolve this by using a ratio method. When the ratio method is used, traffic is distributed among all of the available netlinks according to the relative capacity of the links. The bandwidths of the other netlinks are automatically compared to the bandwidth of the netlink with the most bandwidth to produce a ratio for distributing the traffic. When the volume of traffic is low, the ratio of actual traffic distribution is approximate. When the volume of traffic is high, the ratio of traffic handled by each netlink is closer to the ratio calculated from the link capacity.

In the example below, using standard outbound load balancing could result in using the 2 Mbps link even though the 5 Mbps link may be more efficient. Using ratio-based load balancing allows McAfee Multi-Link to take the larger link(s) into consideration to allow for a more granular and efficient use of available links.

**Figure 2.** Traffic is distributed according to the relative capacity of the links.
Standby links for high availability

Standby netlinks allow organizations to define a netlink as a backup that is only activated when all primary netlinks are unavailable. This minimizes the use of netlinks that are more expensive (where the cost is based on the amount of used traffic) or otherwise less preferable, while still ensuring high availability of Internet connectivity. To test which netlinks are available, the status of the netlinks is monitored by sending Internet control message protocol (ICMP) echo requests (pings) through each netlink. If no response is received before the end of the defined timeout interval, the netlink is considered unavailable.

Figure 3. The standby netlink is activated only if all the primary netlinks fail.

As soon as one or more primary netlinks become active again, the standby netlinks are deactivated. Previously established connections continue to be handled by the deactivated netlink, but new connections are no longer sent to the standby netlink. Organizations can define multiple active netlinks and multiple standby netlinks.

When load balancing is used with standby netlinks, traffic is only distributed between the netlinks that are currently active. Standby netlinks are not activated to balance the load. Organizations can use expensive traffic-based links as backup links, since in emergency situation even they become cost effective compared to having to risk attack.
Quality-of-Service (QoS) classes
Organizations can optionally assign a QoS class to each netlink. Assigning a QoS class to a netlink specifies that traffic with the selected QoS class is routed through the selected netlink. The same QoS class can be assigned to more than one netlink. When no QoS class is assigned to a particular netlink, traffic is routed through that netlink according to the load-balancing method selected. The actual QoS classes can be assigned to specific traffic in the firewall policy or in the QoS policy based on the differentiated services code point (DSCP) codes of the incoming traffic. Figure 4 shows one example where you would use QoS with netlinks.

Figure 4. Email traffic can be sent over the high latency satellite connection while the VoIP traffic is sent over the low-latency links.

Activating outbound McAfee Multi-Link for selected traffic only
McAfee Multi-Link for outbound connections is implemented with network address translation (NAT) rules in the firewall policy, which makes the configuration very granular. It is not necessary for all traffic to be balanced, but the decision can be made on a rule-by-rule basis using any combination of the match fields in the firewall policy.

When a NAT rule that balances outbound connections matches the traffic, only the traffic that matches the rule is balanced, and according to the settings that have been made for this specific rule only. Obviously, organizations can share the settings in multiple NAT rules, or they can define all the outbound traffic to be balanced same way.

Some protocols cannot use dynamic NAT based on IP/port translation. To achieve high availability and load balancing for connections that use these protocols, organizations can use static NAT as well. When static NAT is used, the size of the source network must be the same as the size of the network used for address translation.
Inbound Traffic

McAfee Next Generation Firewall has a built-in load balancer that can be used for distributing incoming traffic between a group of servers to balance the load efficiently and to ensure that services remain available even when a server in the pool fails. The server pool has a single external IP address that users (customers, partners, and employees) can connect to, and McAfee Next Generation Firewall then uses NAT to distribute the incoming traffic to the different servers.

This does not require the use of McAfee Multi-Link, but it can be used to improve availability by providing the connection access to the server pool through multiple Internet connections. Organizations can also use McAfee Multi-Link with just one server in the server pool to take advantage of dynamic domain name system (DNS) updates as shown in Figure 5.

When dynamic DNS updates are not used, McAfee Multi-Link is based on assigning a different IP address for the server pool in each netlink. The server pool's DNS entry on the external DNS server must be configured with an individual IP address for each netlink so that users can access the servers through the different netlinks. When the connecting user requests the IP address for the server pool's DNS name, the DNS server sends the server pool's DNS entry with the corresponding IP addresses on the different netlinks. The user connects to one of these addresses, and McAfee Next Generation Firewall then allocates the connection to one of the server pool members. If the first server pool IP address is unreachable, the user can connect to the server pool's next IP address on a different netlink, depending on the user's application.

When dynamic DNS updates are used, the firewall automatically updates the DNS entries based on the availability of the netlinks. When a netlink becomes unavailable, the server pool's IP address for that link is automatically removed from the DNS entry on the external DNS server. When the netlink becomes available, the IP address is again automatically added to the DNS entry.
Figure 5. A user connects to one of the external IP addresses given by the DNS server. If that netlink fails, the user can connect to the next external IP address. Optionally, dynamic DNS can be used to update the DNS entries accordingly.
**VPN Traffic**

Using McAfee Multi-Link enhances the reliability of the VPN communications by offering any-to-any connectivity with several ISP connections. McAfee Multi-Link can balance the VPN traffic between multiple network links and fail-over when a link goes down. This reduces the possibility of link congestion or ISP network connectivity breaks and enables always-on connectivity.

This feature is specific to McAfee, a part of Intel Security. To obtain the full benefits from this technology, McAfee Next Generation Firewall must be placed on each side of the connection. If a third-party gateway supports configuring multiple VPN tunnels between two devices, organizations can still take advantage of McAfee Multi-Link’s benefits, but this may limit the capabilities to the events that can be controlled by McAfee Next Generation Firewall. “Compared to other solutions, our new solutions allow for the dynamic adoption of VPN tunnels,” says Susanne Wesner, technical manager at meetyou conferencing GmbH. “Additionally, the configuration process can be carried out according to the second-set-of-eyes principle—this increases security with an additional inspection level.”

In a McAfee Multi-Link configuration, VPN traffic can use one of multiple alternative tunnels to reach the same destination. This ensures that even if one or more tunnels fail, VPN service continues as long as there is at least one tunnel available.

McAfee Multi-Link VPN can be used between two McAfee Next Generation Firewalls when one or both gateways use(s) multiple network connections. Some of the connections can be defined as backup links for VPN traffic, so that they are only used if the active tunnels fail. The standby selection in a VPN is independent from other VPN configurations, so other VPNs can still use those connections continuously. The standby setting is not tied to a particular ISP (netlink) either. For example, in Figure 6, the tunnel between ISP1 and ISP4 could be standby while the tunnel between ISP1 and ISP5 is active.

It is also possible to define certain traffic to use a certain tunnel (or set of tunnels) by default. For example, VoIP and video conferencing could be defined to use the MPLS connection primarily, but the Internet connections would still be used as a backup if the MPLS is down for any reason. Even when the fail-over occurs from the MPLS to the Internet links, it is completely transparent to users, as the existing VoIP and video conferencing sessions are maintained.

VPN traffic is balanced between the tunnels based on the link availability checks on each VPN tunnel. If one of the links fails or becomes congested, the VPN traffic is routed through the other tunnels.

---

“McAfee Multi-Link has significantly improved the reliability and capacity utilization of our VPN lines. This creates considerable time savings for the employees in our IT department and optimizes the costs for the company.”

—David Ong
Head of IT
Cura Group

---

**Figure 6.** McAfee Multi-Link VPN configurations use Internet, MPLS, and leased-line connections transparently. Some tunnels can be defined as standby, like the leased line in this example.
Standby tunnels are used if all active tunnels become unavailable. Individual tunnels can also be completely disabled so that they are not used for that specific VPN under any conditions.

Remote users accessing the corporate network via McAfee VPN client software can also benefit from McAfee Multi-Link technology. If one of the gateway links fails, the VPN client connects to the next available netlink.

For more information, visit www.mcafee.com/ngfw.

About McAfee

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security’s mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.