White Paper

Augmented VPN

Table of Contents

Executive Overview

Comparing an augmented virtual private network (VPN) to a traditional VPN is similar to comparing a GPS navigator to a simple road map. A GPS navigator has many embedded functionalities, like location awareness, current traffic information, search, service locator, route tracking, and other features that have provided an evolutionary step forward. A similar development is taking place with VPN. During the early phase of globalization, it was enough for a company to be able to connect its offices and production sites with a simple VPN or point-to-point dedicated circuit. However, the situation has changed dramatically since those days.

There are three problems that companies are facing today:

- The production systems are online, and they need to be available at all times and from any location. In fact, many companies cannot operate anymore without online systems like enterprise resource planning (ERP), mail, or cloud-based services such as Salesforce.com. Is there a cost-effective way to provide backup connections if the multiprotocol label switching (MPLS) connection fails? The Internet connection is always too limited, and its usage is growing every day. How do you differentiate between critical production traffic and other traffic? How do you provide enough capacity for critical business traffic, yet allow other traffic when there is excess capacity? Is there a way to direct only production traffic via the multiprotocol label switching (MPLS) connection and use a more cost-effective connection for the rest?
- Network connection costs are too high. Many companies are global, and they need to have a reliable, fast connection between their production sites and business offices. For example, an MPLS provides reliable connection between sites, but it will become expensive if used between several countries around the globe.
- The business environment is often very dynamic, requiring agility from network connectivity. Long service delivery times and long binding contracts with service providers do not meet the needs of many fast-moving businesses.

This white paper will examine solutions to these three problems and an additional security bonus.

Case Study 1: Augmented Connections

An organization had their production sites in the United States, and one of their sales offices was in Bermuda. The Bermuda office was totally dependent on the connection to the company's production sites. There was one MPLS connection between the production site and the Bermuda office. The CIO was still worried because Bermuda is a known hurricane area. One big hurricane could disrupt the communication lines and put the company out of business for a long time.

The company compared several different options, including satellite backup connections and an additional MPLS connection from another Internet service provider using border gateway protocol (BGP). All alternatives turned out to be quite complex and costly. The company solved the problem cost effectively by using the McAfee® Multi-Link and McAfee Firewall/VPN solution with two MPLS connections from two different Internet service providers. This solution enabled them to avoid a cumbersome border gateway protocol (BGP) setup and gain highly available connections.

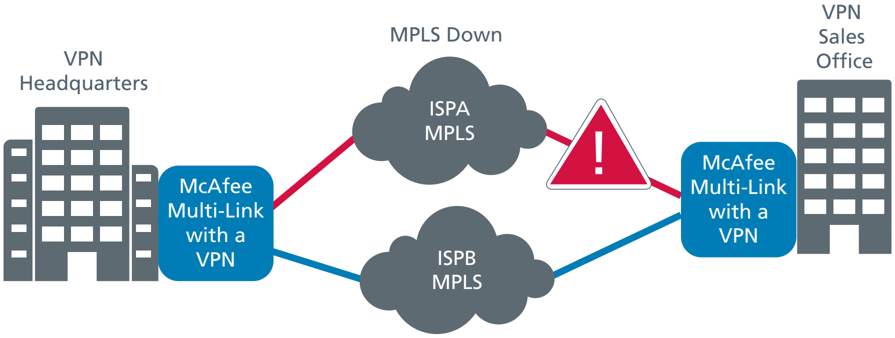

Figure 1. McAfee Multi-Link high availability.

About one year after that, a category four hurricane swept through Bermuda and took out one of the main Internet service providers. Once that was in the news, McAfee support personnel called the organization's IT manager and asked if he had noticed that one of the company's Internet service providers had been wiped out. The IT manager said that he had not noticed anything—connections were functioning flawlessly. This is just an example of the power of McAfee Multi-Link. The traffic from the failing Internet service provider connection was automatically transferred to the still functioning one. Business continued without any interruptions.

As the role of Internet-driven business grows, the reliability of connections and constant availability of services is an absolute necessity for corporations. Because of the risk of downtime, organizations have become very adept in making their networks highly available by implementing solutions such as redundant gateways, firewalls, switches, routers, and other highly available network components. However, even when using such methods, the corporate network can suffer from outages if a network link to the Internet or to the other production sites fails.

Internet service providers can provide a variety of different network links, but they all are subject to a failure. Even MPLS connections are vulnerable. An ISP failure may come in many shapes, sizes, and colors. For example, your Internet service provider could be taken down by a denial-of-service (DoS) attack or by a malicious virus or worm. Outages may also result from a routing misconfiguration by the Internet service provider, which may take some time to locate and rectify. Internet service providers can also be brought down for non-technical reasons, such as a network line that is broken because of road construction, the Internet service provider filing for bankruptcy, or a natural disaster. Whatever the reason, the result is the same: despite all efforts to make your network highly available, your connectivity comes to an abrupt halt just the same.

To eliminate the Internet service provider as a single point of failure, many corporations have deployed a battery of redundant external routers and switches which require the use of complex routing protocols, such as BGP, hot standby routing protocol (HSRP), and peering arrangements through Internet service providers. Others regard this approach as too complicated and expensive, as it requires redundant hardware, more expensive routers, additional software, and Internet service provider arrangement costs just to get started. Once implemented, administrators face the daunting task of configuring and maintaining the complex network in order to achieve high availability.

To illustrate this, we simply need to examine BGP a bit further. BGP is a routing protocol designed to allow the creation of redundant routes to a set of networks. BGP, however, creates additional complexity and expenses.

- You are required to get a provider-independent IP address space and an autonomous system number (ASN), which may not be possible for IPv4 addresses today. An ASN is a unique ID that identifies corporate networks to routers on the Internet and allows other routers to understand there is more than one way to get to the network.
- To make use of a provider-independent address space, an organization must negotiate an agreement with at least two different ISPs on routing for their ASN. For mid-sized companies, or even some larger enterprises and service providers, this may be challenging to arrange.
- Businesses with tight budgets also face the costs of upgrading routers with additional memory and software to perform the complex dynamic routing required by BGP.

Companies need a way to make Internet service provider connections redundant with a single simple solution—without expensive hardware or software, complex configurations, or cooperation between service providers. Ideally, this solution should also address additional challenges, such as the security of the system, fault tolerant VPNs, load-balancing, scalability, upgradeability, and manageability.

McAfee Multi-Link technology provides a simple way to create Internet service provider redundancy and ensure uninterrupted Internet connectivity. McAfee Multi-Link eliminates the need for complicated and expensive third-party hardware and software solutions and makes network administration significantly easier. With McAfee Multi-Link, Internet and VPN access is no longer a single point of failure in the network. Organizations can easily add multiple Internet connections to their network by utilizing multiple Internet service providers, leased lines, or a combination of the two. This enables companies to:

- Ensure that their network connection will be always available, even if one of their Internet service providers fails or is taken offline.
- Improve their Internet performance with increased bandwidth.
- Provide for flexible migration from one Internet service provider to another without long-term contractual agreements.

- Implement a gradual and transparent migration from costly leased lines with the option to keep them as backups when needed.
- Increase customer satisfaction.

McAfee Multi-Link eliminates an individual Internet service provider as a single point of failure by allowing the organization to establish multiple Internet links simply and cost effectively. All of the links are active and in use. If one link fails, traffic is automatically transferred over to the remaining links. McAfee Multi-Link supports a combination of all kinds of Internet links. Companies know they will always have Internet connectivity when they need it.

With McAfee Multi-Link, organizations no longer need to worry about their Internet service provider being taken down by a DoS attack or malicious virus. If a backhoe digs up the cable between them and their Internet service provider, they will remain connected. If their Internet service provider misconfigures its routing table, goes bankrupt, or suffers a major catastrophe, business continues as usual, with McAfee seamlessly routing connections through the remaining network links. McAfee Multi-Link technology comes pre-packaged as part of the McAfee Next Generation Firewall and McAfee Multi-Link VPN solution. It comes with McAfee clustering and load-balancing technology built in. When McAfee Multi-Link is used with clustered McAfee Next Generation Firewalls, load balancing between nodes provides further reliability to the network architecture. Connections lost due to node failure can be recovered transparently, with no apparent loss of service.

Even though the problems that McAfee Multi-Link solves are complex, the implementation is remarkably simple and cost effective. Unlike traditional solutions, McAfee Multi-Link technology requires no additional or specialized hardware or software. This significantly reduces comparable implementation and maintenance costs. Furthermore, McAfee Multi-Link provides ISP redundancy without the need for peering agreements between competing ISPs. In fact, the ISPs do not need to communicate with each other at all. This significantly helps to simplify implementation, system maintenance, and troubleshooting.

Case Study 2: Augmented Bandwidth

An organization had problems with their Internet connection capacity. Its main business traffic consisted of customer relationship management (CRM) traffic, which was offered as a cloud service for them. At first they had an MPLS connection, but bandwidth soon became a bottleneck when other Internet traffic increased and employees started to use social networking services like Facebook and LinkedIn. Social networking was part of the company's customer service and marketing strategy, so it could not prohibit the use of those services. The company increased the MPLS connection bandwidth to 8 Mbps and that provided relief for a while. However, quite soon even that pipe was almost 100% utilized.

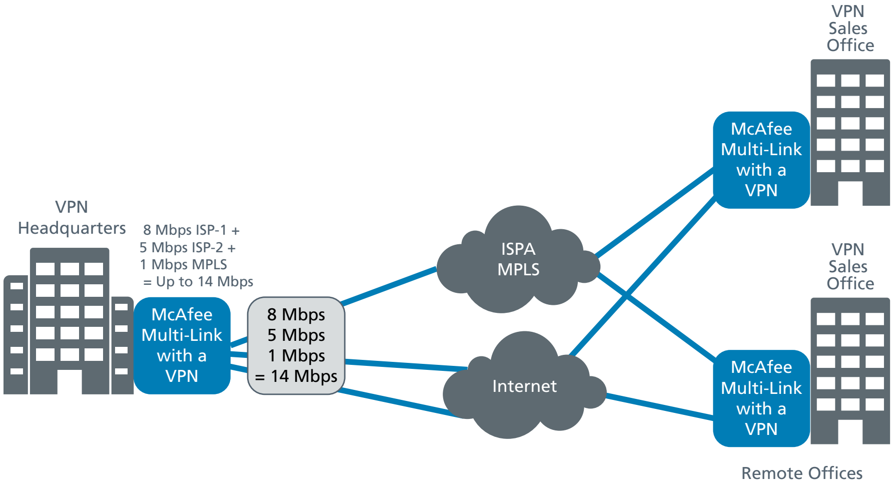

Figure 2. Highly granular aggregation.

Now the company faced a bigger investment decision because their Internet service provider only offered up to 8 Mbps connection using copper lines. For speeds higher than 8 Mbps, it either had to have a fiber connection from its ISP or a wireless radio link. Fiber connection speeds can go up to tens of gigabits per second, and wireless radio links can go up to 100 Mbps. Both options would include additional hardware and setup fees because both options required the ISP to install new equipment on premises. Neither option was available immediately, and setup time varied from three weeks to two months. That was too long for the organization—it needed the new bandwidth immediately.

Fortunately, the company was using the McAfee Augmented VPN solution. McAfee Multi-Link technology allows aggregating several low-cost lines into one larger line. For example, two 5 Mbps ADSL lines can be used to create one 10 Mbps line. The company purchased two 5 Mbps lines from the ISP to provide immediate relief to its bandwidth needs. In the future, even more new low-cost lines can be added if bandwidth needs increase. An additional benefit is also improved high availability because the additional lines provide redundancy in the event of a line failure.

Example:

- CRM traffic = Priority 1 = Forced on the MPLS link with backup line on ADSL 1.
- HTTP traffic = Priority 4 = Forced on the aggregated line ADSL 1 + ADSL 2.

McAfee Multi-Link improves VPN performance significantly, as it allows connections to transparently select different VPN links based on traffic volumes and network conditions. With QoS-based preferred link selection configuration, different traffic can by default be directed to different links. Critical CRM traffic can have the best link as the active link and other links act as backup links. Less critical traffic can then have only some of the links in use so that bandwidth is always saved for more critical traffic. Here are some key advantages:

- Higher bandwidth and lower latency help support new technologies such as Voice-over-IP (VoIP) and video conferencing.
- The company benefits from increased customer satisfaction based on a better user experience.

Case Study 3: Augmented Priority for Business Traffic

A global retail company had been using one MPLS connection from each of its locations to its central data center where the main SAP system was located. The problem was that the SAP traffic did not always have enough bandwidth available. The reason for this bandwidth problem was that the other traffic (email, Internet browsing, and other traffic) was driven through the same MPLS connection. The retail company wanted to remove the other traffic from the MPLS connection to make sure the SAP traffic would always have enough bandwidth. The company had several offices, so adding a second MPLS connection everywhere was too costly. Raising the capacity of the MPLS connection was also considered, but it was expensive, and, additionally, there was the problem of a single point of failure of the MPLS connection.

Even though the company had good service level agreements with its Internet service provider, the maximum compensation for the connection outage was as high as the subscription payments it had already paid. In case of a connection outage, it would not cover the production losses, so the company wanted to have a cost-effective backup connection for the SAP traffic.

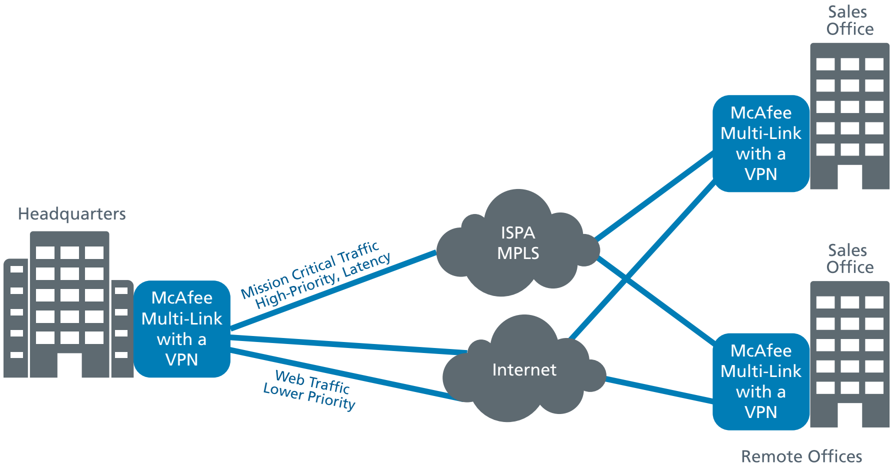
Sales Office
McAfee Multi-Link with a VPN
Headquarters
McAfee Multi-Link with a VPN
Mission Critical Traffic High-Priority, Latency
ISPA MPLS
Sales Office
Internet
Web Traffic Lower Priority
McAfee Multi-Link with a VPN
Remote Offices

Figure 3. QoS link selection.

The retail company solved their problems with the use of McAfee Augmented VPNs. The company purchased an additional ADSL connection for all their offices. This was a cost-effective way to get more bandwidth to each location. McAfee Multi-Link technology was used for load balancing the traffic between the ADSL and MPLS connections. The quality of service (QoS) feature was implemented for SAP traffic prioritization. That means that SAP traffic always has priority in the MPLS connection and that other traffic is automatically directed to use the ADSL connection. If there is unused capacity on the high-quality MPLS connection, the other traffic is able to use it. This way, the expensive and high-quality MPLS connection was close to 100% utilization at all times. On the other hand, the cost-effective ADSL connection provided capacity expansion whenever needed.

Example:

- SAP traffic = Priority 1 = Forced on the MPLS link.
- HTTP traffic = Priority 4 = Normally using ADSL + free capacity on MPLS link.

With quality of service-based (QoS-based) preferred link selection provided by McAfee Multi-Link, the QoS functionality provides control over how each application can utilize the available bandwidth resources. Mission-critical applications can be placed on links that provide high priority with low latency, while all other applications are placed on the links that have available bandwidth or provide best effort.

McAfee Multi-Link QoS makes more efficient use of network resources by servicing the most important traffic for your business while not requiring the need to purchase more bandwidth. The company benefits from guaranteed bandwidth for mission critical/time sensitive applications and a better user experience.

Augmented Cost Efficiency

A global manufacturing company wanted to use lower-cost Internet connections to provide connectivity between its production sites and sales offices. The company had several conflicting requirements:

- The production facilities were in developing countries where production costs were low, but the local infrastructure did not provide reliable Internet connections, or if it did, the connections were very expensive.
- The ERP system required low latency connections—an MPLS connection with strict SLA, if possible.
- The use of VoIP service was desirable wherever possible to save costs.
- The network infrastructure (800 sites) had to be centrally managed by two to three people.

In many developing countries land lines are either non-existent or of very poor quality and unreliable. However, there is a relatively good chance that the wireless infrastructure is in place. With McAfee Augmented VPN, it is possible to first use 3G wireless connections and add fast land line connections later on when they are ready. If the land line connections break up or are out of order, then McAfee Augmented VPN can automatically use the 3G connection as a backup.

MPLS connections are moderately priced when used within one country. If there is a need for MPLS connections globally, then the pricing starts to rise sharply as the distance between the sites grows. In this case, the ERP system needed low latency connection and the MPLS could provide it. Fortunately, the ERP system did not require much bandwidth, but Internet usage and VoIP calls did. The manufacturing company decided to use a very low bandwidth MPLS line for ERP traffic and directed all the other traffic to lower-cost ADSL lines in order to keep global connections costs low. They were able to manage that using McAfee Multi-Link VPN technology, which seamlessly combined different ISP connections.

Managing 800 sites is not an easy task if you do not have centralized management. McAfee Security Management Center provides a clear overview of the VPN infrastructure and allows centralized remote management for all VPN devices. Currently, the company is managing its 800 sites with two administrators.

VPNs offer enterprises a cost-effective way to secure their communications compared to other alternatives, such as leased lines. However, VPN connections have proven to be unreliable and, therefore, risky for business critical communication. McAfee Multi-Link technology solves this problem by adding fault tolerance and transparent fail-over to VPN tunnels.

McAfee Augmented VPN provides further cost savings by allowing companies to migrate from expensive leased line solutions to more cost-effective ones. This migration is made simple by the fact that companies can keep their current connections during the migration, and make the final transfer after they have tested the new lines and completed their setup process.

Security Bonus

McAfee Augmented VPN provides strong security that is built into the solution. A high percentage of the traffic that flows through the McAfee Augmented VPN is security critical, so encryption is a must. Although MPLS connections are said to be secure, they are not encrypted. The traffic flows in clear text format inside the Internet service provider's network. Often, McAfee Augmented VPN is used to encrypt the MPLS traffic to make sure that the traffic is not read by anybody else on the network.

Augmented VPN offers possibilities for traffic deep inspection, antivirus, anti-spam, antispyware, and, finally, anti-evasion checks. As the global forerunner in anti-evasion research, McAfee provides unparalleled protection against advanced evasion techniques (AET).

Artificial Intelligence in McAfee Augmented VPN

Load balancing traffic between several different Internet service providers is not as easy as it sounds. Handling different problem situations gracefully can be especially challenging.

McAfee Augmented VPN uses several cutting edge technologies, including fuzzy logic, to solve VPN load balancing and high availability issues.

Here are some examples of problems that might occur if the load balancing or VPN resilience is not done correctly:

- Traffic goes to only one ISP link, even though there are multiple active links available.
- Traffic goes to a link of a poor quality, even though a better link is available.
- Traffic goes to a standby link, even though an active link works.
- Switching to a standby link takes too long.

Fuzzy logic fits nicely to these problems because it is multivalue logic. Instead of "0" or "1," there are multiple values. This means imprecise data and therefore fuzzy logic is required; it can use imprecise data and calculate "degrees of truth," providing answers to these question:

- How high is the load?
- How close are we to failover?

Fuzzy logic uses input variables, fuzzy sets, output variables, rules, and "de-fuzzification" in to provide an answer. Fuzzy logic helps McAfee Augmented VPN to work optimally even in a very fast-changing and unpredictable environment. In addition to fuzzy logic, McAfee Augmented VPN uses McAfee Multi-Link technology, which allows it to always choose the fastest Internet service provider line.

Assessing the Alternatives

As previously explained, technologies other than McAfee Multi-Link can be used to support multiple ISP connections, although they fall short of the performance that can be expected from McAfee Multi-Link technology. For instance, BGP routes connections using an algorithm that determines the shortest path, calculated by the number of hops (routers) between source and destination. Virtual router redundancy protocol (VRRP) and hot standby router protocol (HSRP) are used to make routers highly available. All these specialized protocols, whether used for router redundancy or for choosing the fastest route, are not required but can coexist in the network with a McAfee Multi-Link implementation.

Border gateway protocol (BGP)

Organizations that maintain multiple Internet links to ensure high Internet availability often implement BGP, which can be described as follows:

- BGP is a routing technology that selects packet routes from all available ISPs.
- BGP can be configured to use static load sharing. It does not perform true load balancing. For example, some statically configured networks always use link A and some other networks always use link B.
- BGP chooses carriers without measuring their performance. When BGP chooses slow or congested carriers, network performance suffers.

Limitations

BGP is an ISP-level solution. It has not been designed for implementation by end users, so it requires specialized ISP resources and equipment. For instance, implementing BGP requires a provider-independent IP address range. (It is difficult to get provider-independent IPv4 addresses anymore.) This poses a significant risk of service failures, which may lead to incorrect routing unless the user successfully negotiates dedicated cooperation between competing ISPs. The implementation itself is a multistep process with several activities that fall well beyond the normal bounds of software configuration. The implementation team must negotiate agreements between two ISPs, acquire and configure sophisticated hardware and routing schemes, and have advanced BGP programming expertise.

In comparison, McAfee Multi-Link is a single solution that requires no additional or specialized hardware or software. This significantly reduces comparable implementation and maintenance costs. McAfee Multi-Link selects the connection with the fastest throughput, while BGP cannot tell whether a path with more hops is faster than a congested path with fewer hops. Finally, McAfee Multi-Link resides on the McAfee Next Generation Firewall and does not require additional processing capacity or hardware, while BGP resides on the router and requires extra processing capacity to calculate the shortest path, which is an additional expense.

External load balancers

External load balancers are appliances that are located in front of a network gateway. They are not dependent on BGP or any other routing protocol, and, in fact, they use methods similar to McAfee Multi-Link to address multiple ISPs.

Limitations

External load balancers require special equipment and constant maintenance. However, even under the best circumstances, they cannot participate in a VPN network without slowing network performance.

As with BGP, if users want to implement load balancers, they must purchase specialized hardware. External load balancers require specialized network components to use multiple ISPs, such as a pair of gateways and a pair of load balancers (for achieving high availability on the load balancers), which adds to the cost of implementation.

External load balancing equipment requires constant supervision, administration, and system updates, adding to maintenance costs. Administrators must also ensure the separate configuration of the gateway and the load-balancing box is consistent, which adds to the technical complexity of the management process.

Conclusion

McAfee Augmented VPN provides a simple and cost-effective way to create fast, secure, high-capacity connections between sites and ensure uninterrupted Internet connectivity. Designed for ease of use, the implementation requires no special equipment, software, or Internet service provider peering agreements.

McAfee Multi-Link enables organizations to flexibly and simultaneously connect to multiple network providers, creating fault-tolerant and highly available connections without having to change their existing network infrastructures.

For a constantly available network, organizations usually rely on several Internet service providers or wide area network (WAN) access points to ensure always-on connectivity and increase bandwidth while maintaining a low TCO. With McAfee Augmented VPN, the aggregation of all Internet service provider links is now possible. Link aggregation is a unique feature that enables organizations to combine different Internet service provider lines to obtain a single high-capacity tunnel.

Studies show that employees are increasingly using applications that have been designed to be installed in a professional environment (Skype, MSN, and Facebook). This phenomenon also has a significant impact on bandwidth, which is often used for non-critical activities and puts the quality of business applications and productivity of the organization at stake. McAfee Augmented VPN enables the prioritization of network flows and the definition of bandwidth portions dedicated to different types of flows. Business applications can have priority on high-quality Internet connections and the rest of the traffic can use more cost-effective Internet connections.

A VPN delivers the best return on investment in securing communications. However, the lack of reliability of VPN links is risky for critical communication within organizations. McAfee Multi-Link technology solves this problem by adding load balancing of VPN tunnels and fault tolerance due to automatic transparent failover to active or backup VPN.

When compared to other ISP multihoming solutions, McAfee increases performance by providing true ISP load balancing, provides greater flexibility for implementation, and significantly reduces administration costs, all while adding security to the network with McAfee Next Generation Firewall. In addition, McAfee Multi-Link provides a significant increase in VPN reliability and performance. The ability to fail over VPNs among multiple providers is unique to McAfee Multi-Link technology.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

McAfee®
An Intel Company

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