The 2013 Next Generation Firewall Challenge

Next Generation Firewalls provide the needed protection against Advance Evasion Techniques
Analyst Introduction:
Urgent Need for Better Security

Cisco
Cisco Next-Generation Firewalls Deliver Security Without Compromise

STONESOFT
Visionary Cyber Security for Every Generation

Dell Software
Unleash the power of intelligent, uncompromising Next-Gen Firewall

SOPHOS
Sophos UTM keeps your network safe and productive

McAfee
NGFW Which to Choose?
Urgent Need for Better Security

Advanced evasion techniques mean enterprises need a new firewall and IPS solution

The bad guys just keep getting better. They have figured out advanced evasion techniques that get around our old defenses. Scanning for their signatures was enough for a while, but not now. We can no longer just lock a few ports and feel safe at night. An application can use one port one day, and then another one the next time. These security bandits hijack IP addresses, hiding behind legitimate people and locations to launch their attacks. Though our task of stopping them has gotten harder, our defenses have become more durable.

Older enterprise firewalls and IPS are not up to the task. We need to deploy a new generation of defenses that combines firewalls and IPSs with the ability to respond to new threats. This new generation goes by the name of Next Generation Firewalls.

A Next Generation Firewall (NGFW) combines the power of several security solutions, starting with a stateful and stateless inspection firewall. A stateful inspection firewall understand connections. It applies the enterprise’s policies regarding which ports can be used, and blocks known problem addresses, while monitoring for any problems with the connection. An Application Firewall is added to the mix to gain an understanding of what is happening at the application layer - layer 7. It can identify an application, no matter which port, protocol or address it uses. It can also identify the user independently of their address, location or device. If an attacker or application changes the port, location, or even the protocol used, the Application Firewall can still identify the attacker and take action against application-borne threats and enforce policies.

The Next Generation Firewall then adds an IPS. The IPS brings the ability to use signatures to identify known attacks. It also looks for anomalies and protocol deviations in the packet flow. Web filtering is also included in the Next Generation Firewall, completing the security package that provides Layer 3 through 7 protection.

Next Generation Firewalls don’t stop at this complete protection package. Since it is already taking apart the application layer, the Next Generation Firewall can also provide detail visibility into what is happening at the application layer. Since you can see such details, creating policies for applications is much easier. NGFWs also add in other very useful features, such as bandwidth management to control how much throughput a user or application receives and VPN.

A Next Generation Firewall is not just a collection of the last generation’s answers. It takes security to the next level with its ability to detect Advanced Evasion Techniques (AET). Combining all the abilities in one solution allows it to see a more complete picture, providing enterprises with better security.
The ability to understand the reputation of the sender is yet another feature. Has this location been a problem in the past? Have attacks come from a particular port or application? This information along with other information the NGFW collects allows it to develop a reputation score for the sender or application. If the score doesn't meet a certain threshold, it can block it, or take a more complex look at the packet flow. Some Next Generation Firewalls have the ability to share their reputation information with other firewalls and develop a more complete reputation score.

It’s great that a Next Generation Firewall has all these new abilities to create policies to stop the bad guy. But it doesn’t help if you’ve never heard of a new bad guy or an application that can affect productivity. A Next Generation Firewall can help, not only by showing you new problems, but also by helping you create policies that deal with the problem.

These are just three of the ways Next Generation Firewalls take security to the next level.

Issues

The need for a Next Generation Firewall is clear, but not all Next Generation Firewalls are all alike. Here are some of the key issues should you explore with Next Generation Firewall vendors:

- What pieces of the Next Generation Firewall puzzle does the solution provide?
- What Advanced Evasion Techniques does the solution provide? Ask how they define AET and what can they do.
- What type of reputation solution do they provide? How do they share information to develop a better reputation score?
- How finely can it differentiate applications within applications? For example, Facebook is one large application and includes both looking at and updating profiles, along with playing games such as Farmville. You may want to allow viewing and updating, but treat Farmville differently by blocking it, blocking it based on the time of day or limiting the bandwidth it can consume. Can the Next Generation Firewall understand the difference, not just for Facebook, but for all applications that are composed of sub-applications?
- How robust is their filtering? Can it filter based on users, groups, time and where it is coming from?
- How much visibility does it provide? Does it display sub-application? New applications are being created every day. Can it handle the flood of new applications and give you the ability to understand them?
- Does it help you easily create policies to handle the new applications and situations?
- High availability is critical since Next Generation Firewalls are key to your enterprise’s security. How does it provide high availability? Does the vendor provide robust clustering? How are updates handled? Does it require the firewall be taken offline?
- A Next Generation Firewall does a lot, but it must also bear a large demand. Does it have the performance you need? You want enough performance, but you don't want to pay for too much performance. Does the vendor provide a cost-effective range of solution to meet all your needs?
2013 Next Generation Firewall Challenge

- Today a significant amount of traffic is encrypted using SSL. Can the Next Generation Firewall de-encrypt the traffic, so it can examine it and then re-encrypt it?
- Take a careful look at their management solution. Does it fit in with your existing scheme and does it give you what you need?
- What other features does it provide such as bandwidth management, VPN and authentication?
- What form factor does the vendor provide? The range can include a hardware solution, along with a software version, or even a service offering.
- Is it a cost-effective solution? Do you buy their Next Generation Firewall and get every feature? Or is there a base set of functionality with options?
- How secure is the firewall itself? What protection do they provide to prevent the bad guy from gaining control over your Next Generation Firewall?

There is no one right answer to these questions, and not every enterprise cares about everyone one of them. You need to understand what you are protecting and what is best for your environment.

The Challenge to the Industry

It is clear enterprises need to upgrade to the next generation in security. But the question is “Which Next Generation Firewall solution?” All of them have the same goal of stopping the bad guy, but that doesn’t mean they are the same. Next Generation Firewall vendors come from different backgrounds, so they approach the solution differently. You need to understand these differences, and then find the one that best fits into your existing security architecture.

I have brought together five leading enterprise-class vendors to help you understand how they approach the Next Generation Firewall:

- Cisco
- Dell Software
- McAfee
- Sophos
- Stonesoft
- McAfee

I asked them to explain their primary competitive differentiators. If each of them tried to address all the issues mentioned above, they would need many more pages than I have given them. So, instead, I requested that they concentrate on where they excel compared with their competition. Your next step is to read and listen to what they have to say, so you can understand how they can help you build the right next generation security infrastructure for your enterprise. Later, you should contact the vendors directly to answer your longer list of questions.

This document is just one part of The 2013 Next Generation Firewall Challenge. There are also three webcasts. In these webcasts, I bring together two vendors to explore three topics in depth. Each one will help you gain a better understanding of what a NGFW can do for you. You will also see how to solve real-world problems and get additional information on solutions from specific vendors. The three webcast topics are:

- What should be done about Black Market IT?
- Tips on deploying a Next Generation Firewall cost effectively
- How to stop the Bad Guy

The webcast address many of the issues not covered in this document so check them out to get the complete story on Next Generation Firewalls.
Network administrators are encountering the highest levels of change in history as they attempt to balance security with productivity. Today’s workforce is becoming increasingly mobile, with users requiring anywhere, anytime access to the network from a variety of company-owned and personal mobile devices. This has prompted businesses of all sizes and types to embrace “bring your own device” (BYOD) policies to increase employee productivity and satisfaction. Further complicating the situation, applications have evolved to be highly dynamic and multifaceted, blurring the line between legitimate business applications and those that waste time and increase a company’s exposure to Internet-based threats.

Despite their business productivity benefits, these network trends also introduce serious new security risks. As a result, the primary business challenges facing organizations today are how to enforce acceptable use policies, control evasive applications, authorize personal devices, and protect against Internet threats.

A new approach to security is required – without abandoning time-tested methods – to enhance network visibility and control, accelerate business innovation, and proactively protect against new and emerging threats. While some vendors believe that organizations should rip and replace their existing stateful inspection firewall with a “next-generation appliance, Cisco understands that a comprehensive security solution requires administrators to supplement this proven security device with additional network-based security controls – for end-to-end network intelligence and streamlined security operations.

**Security Without Compromise**

Some firewall vendors make you choose between a proven stateful inspection firewall and one that provides additional visibility into applications and users. However, this approach has several critical drawbacks and can actually reduce security, compared with a traditional stateful inspection firewall. First, stateful inspection firewall policies are deterministic by nature, so a given policy will always deliver the same security result. This is an essential component for all types of organizations, since it leaves nothing to chance. This is particularly important for industries which require regulatory compliance, since many regulatory standards specifically require the deterministic capabilities of a stateful inspection firewall. In contrast, NGFW policies are non-deterministic, which reduces security and jeopardizes the organization’s compliance status.
In addition, the exclusive use of an NGFW builds many of the organization’s security policies around application identification, which requires packet inspection at the front end of each transaction, prior to making a security decision. To avoid unacceptable levels of network latency, the other packets associated with the transaction must still be allowed to pass through the firewall during the course of inspection, with ports defaulting to open until the application-specific policy determines otherwise. As a result, dangerous levels of packet leakage can occur with every transaction that uses an active port.

In contrast, using a proven layer 3 / layer 4 stateful inspection firewall as the first line of defense, coupled with a robust next generation firewall for enhanced layer 7 visibility and control, provides the best of both worlds – for a comprehensive security solution without compromise. With Cisco ASA 5500-X Series Next-Generation Firewalls, all traffic goes through layer 3/ layer 4 first, for proven, deterministic stateful inspection. Firewall policies then determine which traffic is sent to layer 7 for a deeper level of inspection.

That’s why Cisco ASA 5500-X Series Next-Generation Firewalls combine the proven protection of the industry’s most deployed stateful inspection firewall with the enhanced visibility and control of a robust set of next-generation firewall services, including:

- Threat intelligence from nearly 2 million Cisco security devices worldwide for proactive web reputation information and near-real-time protection from zero-day threats
- Visibility and control of more than 1,000 applications and over 150,000 micro-applications, as well as specific behaviors within micro-applications
- Advanced user ID awareness, with support for both active and passive authentication mechanisms
- Reputation-based web security and robust content-based URL filtering
- Proactive, context-aware intrusion prevention that uses device awareness, network reputation of the source, target value, and user identity to drive mitigation decisions
- Awareness of the specific type of device attempting to gain access to the network

Comprehensive Suite of Next-Generation Firewall Services

Cisco ASA 5500-X Series Next-Generation Firewalls go beyond the current industry definition of what comprises a next generation firewall to deliver a comprehensive, integrated suite of next-generation firewall services to enable administrators to enforce differentiated policies based on the specific user, group, role, device, application, and application type.

Cisco ASA 5500-X Series Next-Generation Firewalls integrate with a wide range of software- and cloud-based security services that our customers need today, and are built to scale to meet the functional and security requirements of future networks. Current next-generation firewall services include:

- **Application Visibility and Control (AVC).** In addition to recognizing over 1,000 applications, Cisco AVC further distinguishes these applications into more than 150,000 micro-applications, enabling administrators to enforce individual- and group-based access to specific components of an application while disabling others. Port- and protocol-hopping applications can also be blocked for more effective security, while writing fewer policies. Specific behaviors can be blocked within allowed micro-applications for an additional layer of control.
• **Web Security Essentials (WSE).** Cisco WSE enables robust content-based URL filtering with differentiated access policies based on user, group, device, and role. It includes 65 URL categories and a comprehensive URL database that encompasses sites in more than 200 countries and over 60 languages. Web reputation feeds from Cisco Security Intelligence Operations (SIO) enable more granular policies based on reputation of the host site, as well as the most effective, timely coverage.

• **Intrusion Prevention System (IPS).** Cisco IPS is the industry’s only context-aware and most proactive intrusion prevention that uses device awareness, network reputation of the source, target value, user identity, and key information about the attack to drive mitigation decisions. Based on the broadest visibility of any IPS in the industry, administrators can write proactive policies to act more aggressively on threats that present a more serious or immediate risk to network resources.

• **Robust User authentication.** In addition to passive authentication methods using Active Directory agent and Lightweight Directory Access Protocol (LDAP), Kerberos and NT LAN Manager are supported to provide active authentication.

• **Granular device-level information.** Cisco AnyConnect provides information on the specific types of user devices attempting to gain access to the network, as well as whether the device is located locally or remotely, enabling administrators to confidently allow devices while maintaining high levels of network protection and control.

• **Reputation-based threat defense.** Threat intelligence feeds from Cisco SIO use the global footprint of Cisco security deployments (nearly 2 million devices) to analyze approximately 70 percent of the world's Internet traffic from email, IPS, and web threat vectors. The feeds are updated every three to five minutes for near-real-time protection from zero-day threats. These feeds can also be used to enable reputation-based security policies for a wide range of next-generation firewall services, including WSE and IPS.

### Proactive Security

Cisco ASA 5500-X Series Next-Generation Firewalls protect networks against many types of malware, including web-based threats, vulnerabilities, and advanced persistent threats (APTs) using Cisco Security Intelligence Operations (SIO). Through our unique approach to network reputation, we can protect customers from bad actors at zero-day, prior to any new exploit hitting the wire.

Cisco SIO is a cloud-based service that performs real-time analysis of telemetry from nearly two million security devices and more than 150 million mobile endpoints throughout the world. Continuous updates on Internet threats, network vulnerabilities, and host site reputation are sent to Cisco security devices every three to five minutes, providing near real-time protection from zero-day threats. This information greatly enhances the capabilities of our Next-Generation Firewall Services by enabling Cisco customers to develop and enforce more granular, robust security policies to proactively protect their networks months ahead of a specific threat.

For more information about Cisco's solutions described here, please visit: [cisco.com/go/asac](http://cisco.com/go/asac).
There will always be a next generation. As business requirements for IT and the threat landscape evolve, we must embrace the changes required to ensure the security, performance, efficacy, and cost-effectiveness of our enterprises.

“Next generation” security architecture must enable the business, factoring in how strategic, operational and technical drivers are addressed. Constant change provides us the opportunity to design security as a primary goal and not an after-thought.

Traditional network architectures insert firewalls and IPS systems at strategic points as an afterthought. The architectures are focused on delivery. As the investment and complexity of the added-in security systems increases, inefficiencies creep into the enterprise. The associated management solutions are disjointed and have no common logging in, no common user experience, and no common rule base. Ultimately, these types of architectures create inefficiencies that cost time, money, and resources.

The addition of mobile computing, secure remote access, and cloud solutions further exacerbate the situation. The success of next-generation products largely depends on their ability to respond to current and future threats, ease of use and management-interface capabilities.

What is the future state of network security? Here is what our customers identify as requirements:

- Robust filtering, including users and groups, time and place
- Centralized management with one common view of the universe
- Security resources that are clusterable and updatable during production hours
- Advanced Evasion Technique protection with continued deep inspection across all layers
The Analysts Confirm Stonesoft as the Best Choice for TCO and Thinking Ahead.

In 2013, Gartner placed Stonesoft in the visionary position of the Magic Quadrant for Enterprise Network Firewalls and Intrusion Prevention Systems (IPS). No other vendor was listed as a visionary. Why? Here is what Stonesoft’s founder and CEO Ilkka Hiidenheimo said:

“The only way to stay ahead of the ever-changing threat landscape is to be a visionary and Gartner has recognized us for our efforts. We invest significantly in research and development of solutions that can evolve and protect lives and businesses in cyber space. Attackers also invest heavily in their strategies and they fully understand the technology behind IPS and Firewalls. Advanced evasion techniques (AET) now are becoming more prevalent because they avoid detection. Embedding AET protection in our products is one of the reasons Stonesoft is a visionary.”

For overall total cost of ownership (TCO), Stonesoft points to recent reports from NSS Labs, which confirmed that the Stonesoft IPS-1302 provides 100 percent protection against all tested evasion techniques, and a low total cost of ownership during real-world traffic and threat scenarios. Stonesoft is one of only two vendors in the world with NSS Labs recommended status across firewall, next generation firewall and IPS.

Next Generation Means Changeable – Hardware, Software or Virtual.

Stonesoft products are based on its Security Engine (NGN) -- a single solution that fits any type of environment. It can be reconfigured quickly and easily depending on future requirements. It can adapt to be a virtual, physical or software solution regardless of the scale of the deployment with unified code.

The Stonesoft Security Engine is the first-of-its-kind and can be configured to several different product modes – including a traditional or next generation firewall, traditional or next generation IPS, layer 2 firewall, Evasion Prevention System (EPS), VPN or UTM solution. The security role can be changed anytime according your business requirements thus gaining investment preservation. Automatic updates and robust core functionality helps improve the security footprint while trimming operational costs.

Stonesoft Next Generation Firewall/VPN Resets Expectations.

Four essential elements make up Stonesoft’s next generation firewall solution:

1. **Tight integration.** A unified solutions architecture creates a single view into all traffic passing decisions, improving the coordination of corporate policy and the engines tasked to enforce it. This includes integration with external naming and authentication services for highly granular, robust filtering based on user and group identities, application awareness, and N-factor authentication.

2. **Powerful management.** Stonesoft’s award-winning Management Center provides highly available administrative access and centralized management for any Stonesoft network security device – whether virtual, physical, hybrid, or from another vendor.
3. **High Availability.** High availability is at the core of the Stonesoft Firewall/VPN solution. Active clustering of up to 16 nodes provides great flexibility when addressing high traffic volumes, high availability requirements, session survivability, and both hardware and software refresh during production hours. And with Stonesoft Multi-Link, high availability is extended to cover network and secured (IPsec VPN) connections.

4. **Advanced Anti-Evasion capabilities.** All Stonesoft security engines include the industry’s most advanced anti-evasion capabilities to protect against today’s advanced threats and evasion techniques. It is the only security solution to protect against highly sophisticated and dynamic Advanced Evasion Techniques (AETs). In fact, Stonesoft offers a free evasion test lab for organizations to test existing network security for anti-evasion capability (available at evader.stonesoft.com).

**Centralized Management Critical to Next Generation Operations**

The Stonesoft Management Center (SMC) forms the core of the Stonesoft platform, providing unified network security management for the Stonesoft Security Engine, Firewall/VPN, IPS, and SSL VPN. In addition to managing Stonesoft devices, Stonesoft Management Center also provides event management, status monitoring, and reporting capabilities for third-party devices (syslog & soon Netflow v10). By collecting all this information in one centralized system, administrators can have a unified view into what is happening in their environment.

The SMC helps manage the geographically distributed installations typical of large enterprises. High-availability support ensures uninterrupted access to management and logging resources. All SMC functions including configuration, monitoring, logging, the generation of status alerts and reports, updates, and upgrades can be managed centrally for all devices with unified code.

**The Final Thought on First Thought Security**

Success for IT security professionals is measured in the ease with which the desired controls are implemented, maintained, and utilized to provide visibility and support when addressing vulnerabilities and threats to the enterprise. Enterprises need the ability to respond to any security challenge at any time by pushing policy during the day without a change window, and the ability to roll changes back. It’s a risk management effort with controls and countermeasures. Enterprises need the ability to have a highly robust and available VPN solution that can easily be centrally managed as you move to the cloud and as collaboration becomes more important in the enterprise.

When building new architectures or redesigning existing ones, Stonesoft can deliver the best approach to a more agile security-centric, centrally managed configuration. Building a strong cyber security solution reflecting corporate goals is an achievable goal. Doing the same with improved cost-effectiveness, visibility, functionality is the mission of Stonesoft.

For more information about Stonesoft solutions described here, please visit: [http://www.stonesoft.com](http://www.stonesoft.com) or call Stonesoft at 866-869-4075
Unleash the power of intelligent, uncompromising Next-Gen Firewalls

Every day your network is asked to do more. Carry more traffic. Ward off more sophisticated threats. You can meet these challenges with Dell™ SonicWALL™ Next-Generation Firewalls (NGFWs) that examine every packet without compromising network performance.

The Dell SonicWALL SuperMassive E10800 earned the coveted ‘Recommend’ rating in NSS Labs 2013 Next Generation Firewall Security Value Map for the second year in a row, and Dell SonicWALL rates as one of the top vendors for security effectiveness. (Get the details by downloading the NSS Labs 2013 Product Analysis Report on the SuperMassive E10800 report.)

The Dell SonicWALL architecture was engineered to address the security and high performance demands of carriers and service providers. While throughput varies by model, the very same architecture found in the SuperMassive E10800 is found in virtually every Dell SonicWALL NGFW.

Reassembly Free Deep Packet Inspection
The Dell SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) engine provides superior threat protection and application control without compromising performance. This patented1 engine relies on streaming traffic payload inspection in order to detect threats at Layers 3-7. The RFDPI engine takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including SSL decryption, it is analyzed against a single proprietary memory representation of three signature databases: intrusion attacks, malware and applications.

In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified. (see first diagram)

1 U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361
Extensible architecture for extreme scalability and performance

The RFDPI engine is designed from the ground up with an emphasis on providing security scanning at a high level of performance, to match both the inherently parallel and ever-growing nature of network traffic. When combined with multicore processor systems, this parallel software architecture scales up perfectly to address the demands of deep packet inspection at high traffic loads.

Dell SonicWALL platforms rely on processors that, unlike x86 processors, are optimized for packet, cryptographic and network processing, while retaining flexibility and programmability in the field—a weak point for ASICs systems. This flexibility is essential when new code and behavior updates are necessary to protect against new attacks that require updated and more sophisticated detection techniques.

Another aspect of the platform design is the unique ability to establish new connections on any core as opposed to just a few select processors in competing architectures, therefore providing additional scalability and the ability to deal with traffic spikes. This approach delivers extremely high rates on new session establishment (new conn/sec) while Deep Packet Inspection is enabled—a key metric that is often a bottleneck for data center deployments.

Security and protection

The dedicated, in-house Dell SonicWALL Threats Research Team researches and develops countermeasures, and deploys them to the firewalls in the field for up-to-date protection. The team leverages more than one million sensors across the globe for malware samples, and for telemetry feedback on the latest threat information, which, in turn, is fed into the intrusion prevention, anti-malware and application protection capabilities.

Dell SonicWALL NGFW customers with the latest security capabilities receive continuous updated threat protection around the clock, with new updates taking effect immediately without reboots or interruptions. The signatures in the firewalls are designed to protect against wide classes of attacks, not just individual threats, thus covering up to tens of thousands of individual threats with a single signature.

In addition to the countermeasures on the appliance, Dell SonicWALL NGFWs also have access to the Dell SonicWALL CloudAV Service, which extends the onboard signature intelligence with more than twelve million—and growing—signatures. This CloudAV database is accessed via a proprietary, light-weight protocol by the firewall to augment the inspection done on the appliance. Dell SonicWALL NGFWs are able to block traffic from dangerous domains or entire geographies using Geo-IP and botnet filtering, thus reducing the risk profile of the network.
Application intelligence and control
It can be a real challenge for IT administrators to efficiently deliver critical corporate solutions while also contending with employee use of wasteful and often dangerous applications. Critical applications need bandwidth prioritization while social media and gaming applications need to be bandwidth throttled or completely blocked.

Because the stateful packet inspection firewalls used in many organizations rely on port and protocol, they cannot solve the problem because they are not able to identify applications. Boiling it down, stateful packet inspection firewalls cannot sort out the good from the bad. Inbound and outbound network traffic often is not easy to classify as being just good or bad.

For example, peer-to-peer (P2P), social networking, VoIP, instant messenger (IM), and similar applications can range from very useful in certain organizations to completely unproductive in others.

Dell SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications. This puts the power back into the hands of IT administrators with new levels of management and ease of use, allowing them to implement granular control of applications and users. Administrators can easily create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups. As new applications are created, new signatures are pushed to the firewalls and the appropriate policies are automatically updated without IT spending costly time and effort to update rules and application objects. In addition, administrators can use granular application-based policy to restrict or block the transfer of specific files and documents, prioritize or throttle bandwidth and deny access to internal or external websites.

Value-Add Security Features
Dell SonicWALL NGFWs incorporate numerous Value-Added security features. In particular, three areas where these solution stands out are Clean Wireless, Mobile Connect and integrated SSL VPN.

The security enforcement of Dell SonicWALL NGFWs does not stop at the firewall itself, since good security includes layers of protection. For an additional layer, beyond that provided by the gateway based threat prevention, the Enforced Client Anti-Virus feature ensures that all MS Windows endpoints behind the firewall have the latest version of the Dell SonicWALL client anti-virus and are fully in policy defined by the administrator.

Extensive Customer Base
Dell SonicWALL has shipped over two million appliances to customers across the world. Large enterprises and distributed networks from multiple markets are protected by Dell SonicWALL NGFWs. Companies that have deployed Dell SonicWALL solutions include Arby's®, New York Life, Patagonia, Ace Hardware®, Aaron's, State University of New York (SUNY) Old Westbury and Glentel.

For more information about Dell SonicWALL Security solutions described here, please visit http://www.sonicwall.com or call Dell SonicWALL at 1.888.557.6642 or at sales@sonicwall.com.
Sophos UTM gives you more than just protection against modern threats like botnets and sophisticated malware. It gives you options. Our next-generation firewall, included as part of Sophos UTM, lets you add modules as needed, increasing your protection as your business needs grow. With the Sophos UTM, you get the essential firewall and you build out your protection by simply activating a variety of add-ons at any time.

Sophos next-generation firewall capabilities are delivered through the combination of the Network Protection and Web Protection modules in Sophos UTM. This provides fast, accurate scanning for viruses, spyware and active content using two parallel antivirus engines. We protect your network using advanced packet filtering, network address translation, stateful inspection and network intrusion prevention system (IPS) technologies.

**Complete Control of Your Network**

The Sophos UTM also gives you great visibility and control of the web applications being used on your network. And our URL filter lets you select from over 100 categories such as gambling, nudity, criminal activities, shopping, drugs and job search. This lets you stop access to nasty and non-productive websites using policies for certain users and particular times.

A graphical flow monitor shows everything as it happens, letting you maximize the bandwidth for what’s important and minimize it for what’s not. Deep Layer-7 inspection gives you complete control to block, allow, shape and prioritize web applications. It identifies over 900 applications, as well as giving you feedback on unclassified applications. And you’ll get detailed reports, helping you understand what’s going on and how to improve your network performance and protection.

In addition to an enterprise-class firewall, the Sophos UTM also allows you to easily connect people and offices with innovative and secure VPN options. We provide users with a simple portal, letting them connect from any device, even smartphones and tablets. And when it comes to hooking up remote offices, we’ve really broken the mold. Sophos RED is a box that plugs in at any remote office and requires no onsite configuration. Connect it to the internet, register it centrally and the remote site instantly gets full UTM protection.
A variety of devices accommodates the needs of small, midsized, and large businesses. And, our flexible delivery options let you choose how you deploy it; hardware, software, virtual or in the cloud.

Intelligent Intrusion Prevention
A big problem with many IPSs is that they rely on you knowing which types of attacks you need to stop. With our next-generation firewall you can easily see attacks targeting your resources. Then, choose to stop them by just ticking a box. And our IPS is multicore engineered to run at maximum speeds on the latest processors.

Traditional firewalls are no longer enough to control and protect your users on the internet. Many web applications can’t be managed by just blocking or allowing IP addresses and ports. Our UTM lets you secure your web traffic using intrusion protection and application control. Our next-generation firewall shows you everything that’s happening in your network in amazing detail. You’ll be able to make educated decisions on what to accelerate, limit or block.

Applications like Salesforce.com and Google Docs might be tools you need in your business. Social networking on Facebook and Twitter are popular, but you want to make sure they aren’t hogging productivity or bandwidth. YouTube and other streaming media sites can end up using lots of your web resources. And perhaps, in your company, Dropbox shouldn’t be used at all. You need a way to see what people are using and control their access when you have to. With a single click, you can accelerate, limit or block traffic to these sites.

Easily Block Malware
Today, around 85% of malware comes from legitimate websites being infected. Our next-generation firewall prevents malware infection using fast, accurate scanning. We search and stop viruses, spyware and active content using two parallel antivirus engines. The system also blocks the hidden sending of personal information from already-infected PCs to the outside world.

Our UTM also allows for our UTM Endpoint Protection for Windows networks. Preconfigured installation packages detect and remove your existing antivirus and deploys our self-updating agent. Endpoints automatically register in the UTM. You can also deploy protection via USB stick, email, Active Directory GPO and standard software deployment tools. Tamper protection prevents unauthorized users and malware from uninstalling or disabling endpoint protection.

What comes in a Sophos Next-Gen Firewall?

- Application Control can prioritize or limit traffic from hundreds of apps, like Facebook, Dropbox and Bittorrent. It can even control individual features, like Facebook Chat
- Network Visibility lets you see bandwidth-hungry applications, then shape or control the traffic with a single click
- Sophos UTM 9 Intrusion Protection is multicore engineered to run at maximum speeds on the latest processors
- Patterns for Application Control and IPS are automatically delivered every few minutes without interrupting connectivity
- Next-generation firewall features are available in all models, not just the largest enterprise-focused ones
- On-box reporting covers over 50 reports around bandwidth, application usages and client activity
- Username reporting is available even without Active Directory authentication using the Sophos Authentication Agent—a free client for Windows machines.
We’ve also recently added URL Filtering in our UTM Endpoint. With the web being the biggest source of infection, we’ve integrated advanced web protection into the UTM Endpoint agent. Even when users are on the road, the Endpoint agent enforces the web security policy as if they were in the office. You can sync endpoint and gateway policies or create different rules for people out of the office. You get full control to block, allow or track access to over 90 content categories.

Sophos UTM gets a Five-Star Recommended Rating from SC Magazine

The Sophos UTM 220 received a five-star SC Recommended rating from SC Magazine. The rating is a result of comprehensive product tests and an analysis of overall product value.

SC Magazine’s detailed product review describes the Sophos UTM as a strong product for the mid-market. It also lists the UTM’s greatest strengths as a comprehensive feature set and the integration between endpoint and perimeter security into a single product. Sophos received five-stars in all six review categories, and received an overall ‘Recommended’ rating.

Over the past several months, Sophos has released several new UTM offerings to help improve IT security. Included in these offerings are the Sophos UTM 100 with BasicGuard, and a Wireless Security Access Point 5 model, providing enterprise-level security to small businesses. Sophos also released updated versions of UTM 525 and 625 devices and introduced the RED 50 device, extending UTM to the enterprise.

Wireless Gets Safer, Stronger
To prevent unauthorized access to your wireless network, we use the most advanced encryption and authentication standards available, including WPA2-Enterprise in combination with IEEE 802.1X (RADIUS authentication). And, our Access Points (APs) forward wireless traffic to the UTM. This gives wireless clients the same level of security as if they were physically connected to the LAN.

Sophos UTM already acts as a wireless controller to centrally manage our powerful wireless APs. Now, we’re improving signals and reaching devices that don’t even have wireless connectivity. The Sophos AP 50 access point can act as a repeater or wireless network bridge, extending coverage to areas where an Ethernet jack is not available. All you need is a power outlet. It can also act as a network bridge and use the Ethernet port on a wired device to link back to a wireless signal. This not only improves your connectivity, but provides you with complete network security, wired or wireless.

For more information about Sophos’ solutions described here, please visit: http://www.sophos.com or call Sophos at 1-866-866-2802.
Without question, the firewall market has evolved from where it was just a few years ago, moving to what the market calls Next Generation Firewalls (NGFW). As defined by many analysts, NGFW includes all of the functionality of traditional firewalls, plus some IPS, application awareness and full-stack visibility, user identity and external reputation services. While it may have been easy yesterday to select the best firewalls simply by their adoption of NGFW features, today it seems like all of the vendors claim the same functionality. Fortunately, McAfee Firewall Enterprise brings two things you will not find together from any other NGFW:

- World’s most secure firewall
- Optimal economic packaging

**World’s Most Secure Firewall**

When you get down to the main role of your firewall, it is important to bear in mind that your firewall acts as a security guard, making sure that only approved traffic comes into your network. The best and most sophisticated firewall protection technology in the world is useless if the firewall itself is compromised. With many of today’s NGFW based on common LINUX platforms and kernels, there is a good chance that they are just as susceptible to attack as any of your LINUX servers. So one of the key questions you need to ask yourself, when determining the best NGFW for your organization, is how well protected is the firewall itself?

McAfee Firewall Enterprise is based on SecureOS, a truly hardened operating system that was originally designed for the US National Security Agency (NSA). McAfee Firewall Enterprise is still the only major firewall that has never been hacked and is certified with some of the toughest government qualifications, including Common Criteria and FIPS. It is designed for the world’s highest security networks, and is trusted by government agencies and financial institutions around the world.
Other vendors without such a robust firewall operating system that has been proven to be protect as well as McAfee's may counter this concern with logic that NGFW management is handled through dedicated management ports that cannot be accessed from the outside. However, relying on isolation as the foundation of firewall security is not safe.

The same kind of logic protects most cash points, automatic teller machines (ATM), and point of sale (POS) devices. These devices do not typically have interfaces to the Internet, or outside the internal network, and certainly do not typically see users surf the web or answer email on them, which are common vectors for attacks. Many architects have relied on their isolation as a primary means to protect them. This level of comfort ended when McAfee discovered the vSkimmer botnet.

Other than vSkimmer’s sophisticated targeting ATMs and POSs, the real danger that vSkimmer introduced was its ability to get around isolation as a defense. Delivered as a bot through the network to end users (not to the actual target), vSkimmer was able to find these cash points and POS devices from inside the network. Launching an attack from inside circumvented organization’s strong defenses at the perimeter and also sidestepped isolation. Remotely controlled from outside the network, vSkimmer bots are able to launch their attacks from inside the network, usually from an unknowing (and unwilling) end user. Once successfully compromising their true target (the ATM or POS), they remove all trace of their presence on the end user machine they used to access the inside.

These same kinds of techniques can easily be applied to NGFWs and vendors who do not take the kinds of precautions that McAfee has on McAfee Firewall Enterprise are vulnerable.

For the ultimate in security, McAfee partnered with CloudShield to bring the world’s only true high assurance NGFW. The combined solution with the CloudShield CS-4000 is FIPS-140-2 Level 4 capable, delivering anti-tamper technology that can safely be used in untrusted locations. Should anyone attempt to open the hardware, influence the configuration, or otherwise compromise the system, the system shuts down the network and erases all information, preventing cybercriminals for access to any information that may help them.

While still enjoying the rich NGFW features and capabilities, McAfee Firewall Enterprise customers also have the protection and comfort of the world’s highest assurance firewall.

**Optimal Economic Packaging**

There is a difference between most vendors’ list of NGFW features and the price organizations are initially quoted. There is a base model and many of the essential NGFW features are considered bolt-on additions. This is not the case with McAfee. NGFW capability is the base offering with McAfee. Most vendors charge an additional fee for NGFW features even though these are exactly the capabilities they feature as they sell the product to you, as if most organizations do not purchase them. On the other hand, McAfee Firewall Enterprise includes them all for no additional fee.
2013 Next Generation Firewall Challenge

- Application control (including Network Integrity Agent)
- User identification
- URL filtering
- SSH/SSL inspection
- Gateway AV inspection
- Reputation services (GTI)

McAfee expects (and encourages) McAfee Firewall Enterprise customers to use all of the NGFW features. These features are not an afterthought, but were integrated with the core of the firewall, and McAfee’s pricing structure reflects this philosophy. When considering the total cost of ownership for a NGFW, it is important to consider the entire acquisition cost – not just an estimate based on a stripped down version of the firewall.

Not only is the philosophy part of the packaging for sale from McAfee, but it is also part of the product workflow philosophy. McAfee assumes that all of these features will be available to every customer and can therefore design workflows that elegantly take advantage of them. Other vendors must design multiple workflows because some customers do not have access to all of the NGFW features. The result is that you end up with compromises and less optimal workflows.

Suboptimal workflows result in slower and less effective operation. Tasks take longer and are more likely to user error. This makes operation more expensive, preventing security engineers from focusing on other important tasks. Inevitably, this leads to needs in the future to purchase some of the needed NGFW features in the future, usually as an unplanned necessity, which further raises the total cost of ownership and complicates operations.

Fortunately, McAfee Firewall Enterprise customers avoid all of these un-pleasantries, saving cost and effort with the comfort of the most secure NGFW in the market. Amidst all of the confusion where most vendors claim to have the same capabilities, McAfee Firewall Enterprise stands apart packaging all of the NGFW capabilities in the standard offering, wrapping this all in an ultra secure platform.