Enterprise Strategy Group | Getting to the bigger truth.™

Lab Validation Report

McAfee Next Generation Firewall

Examining Next Generation Network Security

By Tony Palmer, Senior Lab Analyst

April 2014

Contents

Introduction 3
- Background 3
- Next Generation Firewalls 3
- McAfee Next Generation Firewall 4

ESG Lab Validation 6
- NGFW Security Services 6
- Centralized Management 12
- Scalability and Availability 15
- Advanced Evasion Detection 18

ESG Lab Validation Highlights 22

Issues to Consider 22

The Bigger Truth 23

Appendix 24

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about Enterprise technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by McAfee.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

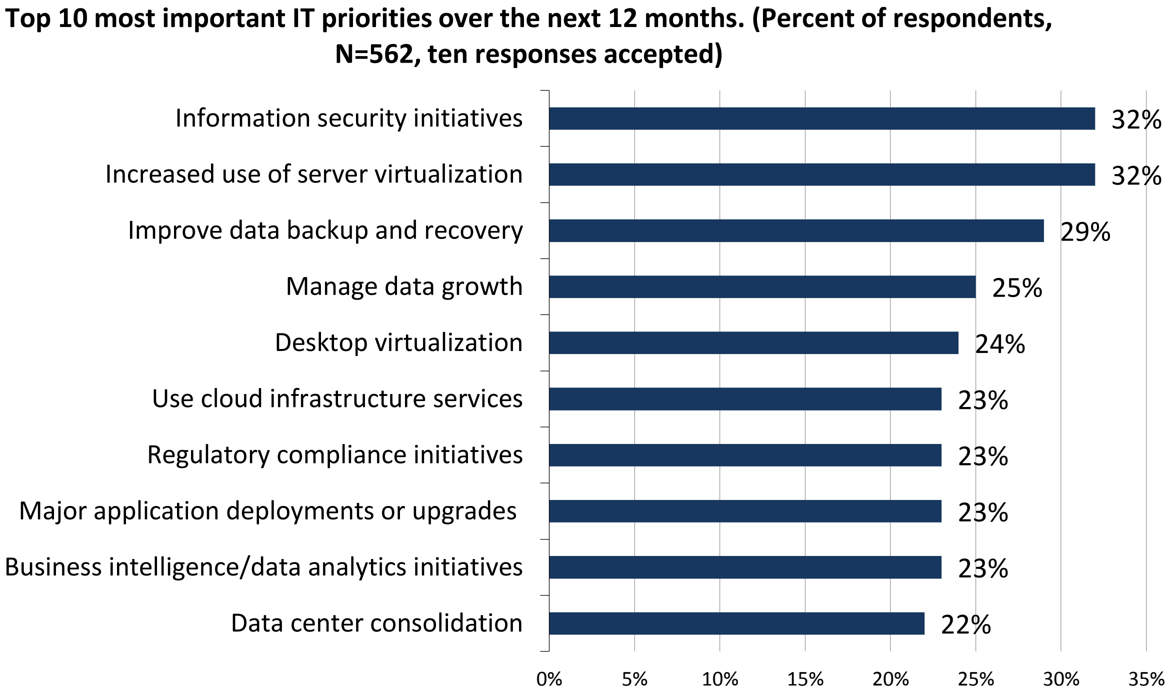
Introduction

This report presents the results of ESG Lab's validation testing of the McAfee Next Generation Firewall. Integrating application control, intrusion detection, and evasion prevention, the product is designed to provide next generation firewall services, leveraging a unified software core to enable the deployment of multiple security services when and where they are needed.

Background

ESG asked 562 IT professionals and managers to name their most important IT priorities and information security was once again the most-often cited response with 32% of respondents, as shown in Figure 1.[1] In the same survey, organizations were asked to identify spending plans for network infrastructure in 2014. Network security was the most cited by a wide margin, by 52% of respondents.

Figure 1. Top 10 IT Priorities for 2014



Source: Enterprise Strategy Group, 2014.

Organizations have relied on the traditional firewall as the first line of security for their private networks and intranets for many years. Traditional firewalls can filter traffic based on: protocols and the ports they use, stateful packet inspection, which holds packets until enough information is received about their state, and application layer filtering to detect whether an unwanted protocol is attempting to bypass the firewall using an allowed port.

Traditional firewalls come with a number of challenges, from complex configuration and management of different types of filters, to increasingly sophisticated attack vectors that can bypass traditional firewall technology, like fragmentation of packets and obfuscation of traffic flows. Next Generation firewalls have come to market in an attempt to address the challenges of traditional firewalls.

Next Generation Firewalls

The term Next Generation Firewall (NGFW) is applied to many modern firewalls, and can be defined as follows: A device that filters traffic between networks based on traffic types or applications using specific flows. Applications

[1] Source: ESG Research Report, _2014 IT Spending Intentions Survey_, February 2014.

can be port-agile and communicate across different ports depending upon configuration. Granular, application-specific security policies can help Next Generation Firewalls to potentially detect more malicious activity than traditional firewalls.

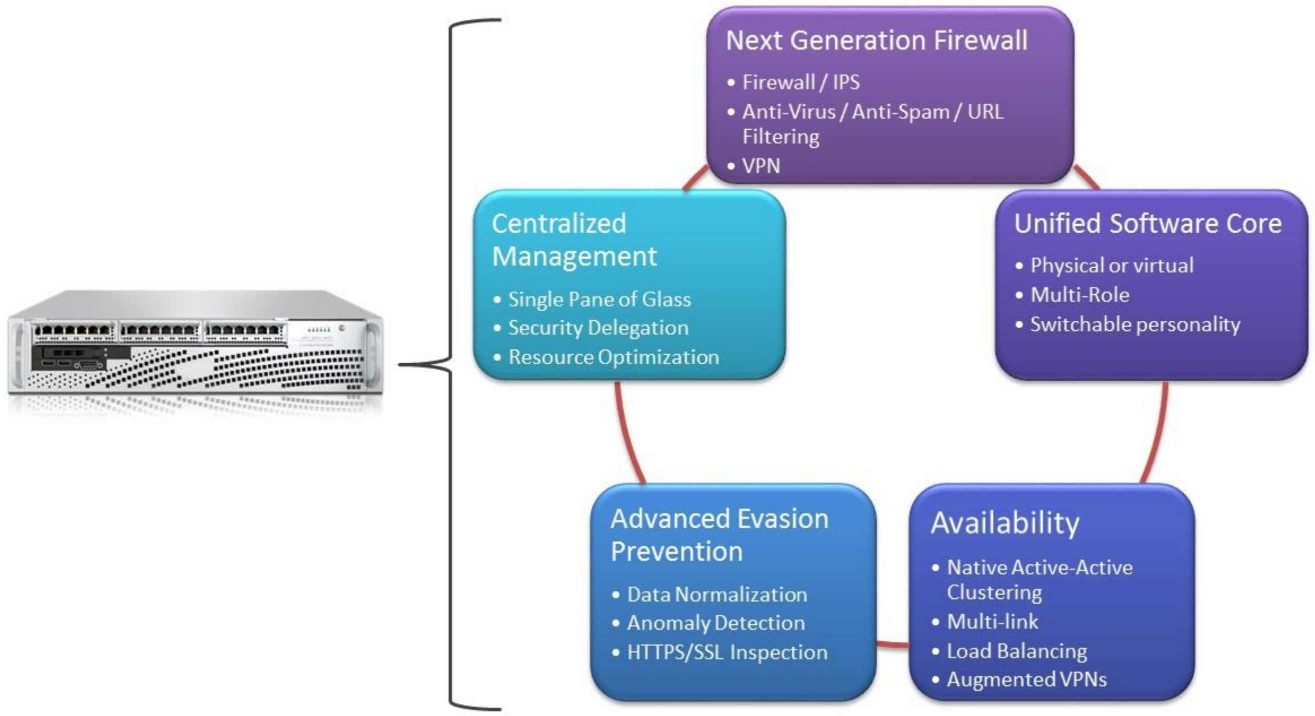
In ESG's opinion, a next generation firewall should blend the capabilities of first-generation network firewalls and network intrusion prevention systems (IPS), while providing deeper network traffic inspection to enable granular policy enforcement. For example:

- **Identification and Filtering of Application Traffic–**To prevent malware from using non-standard ports to evade detection, an NGFW needs to be able to identify and filter traffic based upon specific application characteristics, rather than just opening or closing ports.
- **Intrusion Detection and Prevention–**NGFWs should be able to leverage flow-based deep packet inspection to assist with detection and prevention of intrusions into a private network.
- **SSL and SSH Inspection–**NGFWs should be able to decrypt and inspect SSL and SSH encrypted traffic, to validate that the conversation is from an allowed application and in accord with security policies.
- **Identity-based intelligence–**To manage authorized applications and traffic based upon users and user groups, NGFWs should integrate with common directory services, like Active Directory and LDAP.
- **Malware Detection and Filtering–**NGFWs should be able to detect and filter malware traffic based on reputation or activity to block malicious applications and sites.
- **Provide comparable throughput and performance–**As compared to traditional firewalls with all security capabilities enabled and active.

McAfee Next Generation Firewall

In 2013, McAfee acquired Stonesoft, a Finnish company that developed and sold a "next-generation firewall" (NGFW) platform sold primarily in the European market. Now sold as the McAfee Next Generation Firewall, the platform is designed to integrate multiple advanced capabilities in a single platform. The Next Generation Firewall can behave as a firewall, an intrusion detection and prevention system, or a VPN concentrator McAfee refers to these functions as personalities, all of which can be configured in a native high-availability environment and managed through a unified single-pane-of-glass management system, as seen in Figure 2.

Figure 2. McAfee Next Generation Firewall



The McAfee Next Generation Firewall combines common NGFW functionality with specific security, deployment, management, and availability features:

- **Next Generation Firewall–**McAfee's Next Generation Firewall is designed for tight integration of multiple security features—firewall, intrusion prevention, VPN, antivirus/anti-spam/URL Filtering, and advanced evasion prevention. This integration creates a solution where data packets are inspected once as they traverse the security infrastructure, and are either blocked or allowed to pass directly to the client inside the network without having to take multiple hops through point security control devices. This can improve a client's security posture while simplifying their administrative burden, from the simplest SMB implementation to the most complex multi-network, multisite enterprise or managed service provider environment.
- **Unified Software Core–**A single unified software image runs all packet inspections, delivering high-performance processing of the entire network stream. Each personality is selected and enabled through license keys, enabling administrators to change the personality of the appliance without the need to install additional software. McAfee delivers the solution both as an appliance and as a software stack that can run on either a virtual or physical machine, providing administrators the ability to implement next generation firewall services in the combination and manner that best suits their particular situation.
- **Performance and High Availability–**Up to 16 firewall nodes can be clustered for availability and load balancing, all without using external hardware or implementing load balancing through complex DNS configurations. The Next Generation Firewall implements native active-active clustering, allowing administrators to scale up quickly and simply to adjust performance and bandwidth for changing business conditions. The Next Generation firewall also implements multi-link support, enabling the administrator to direct specific types of traffic to use specific links, and to fail over to backup links when primary network connections fail.
- **Advanced Evasion Prevention–**Advanced Evasion Techniques (AETs) are used to execute Advanced Persistent Threat (APT) attacks. AETs utilize a combination of evasion techniques to disguise attacks and allow them to bypass network security devices to exploit target systems. AETs evade traditional firewalls by breaking malicious packets into small chunks and sending over multiple, often encrypted, combinations of protocols. The McAfee next generation firewall uses HTTPS and SSL deep packet inspection along with other sophisticated analyses to normalize the data and block the threats from delivering their payload.
- **Centralized Management–**All tools necessary to configure and manage the security ecosystem are contained within a single management console. The console enables administrators to configure and maintain NGFWs, IPSs, VPNs, while performing real-time monitoring of the network, including third party devices via syslogs. The console provides tools to automate routine tasks and the ability to reuse elements. With these features, McAfee's centralized management console aims to increase administrator efficiency.

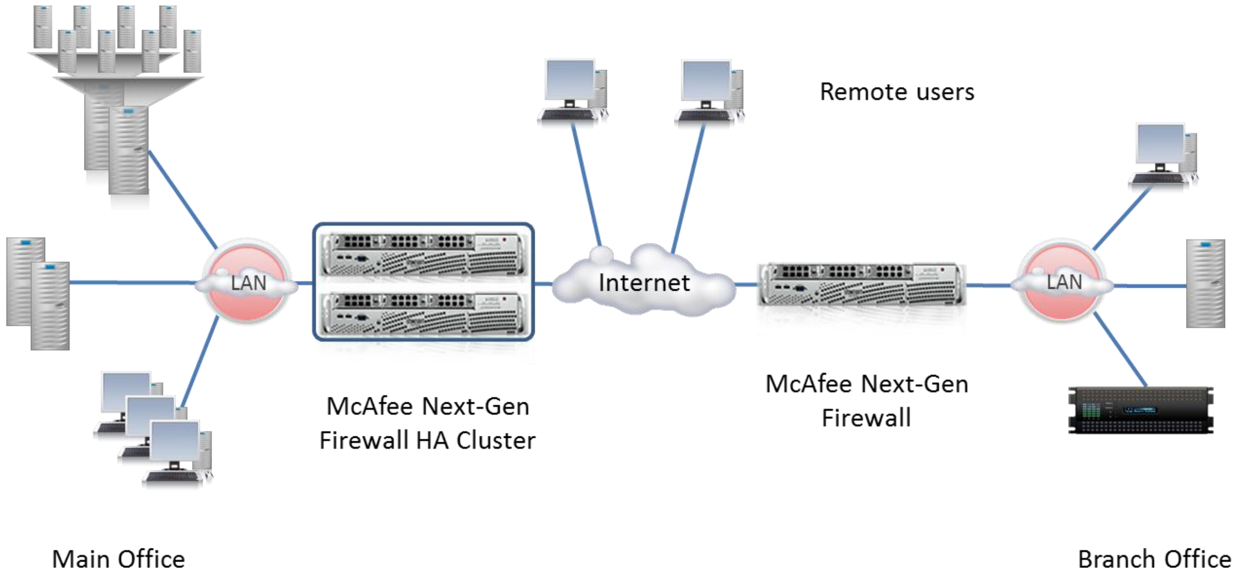
ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of the McAfee Next Generation Firewall at McAfee facilities in Santa Clara, California with a goal of validating the capabilities of the McAfee Next Generation Firewall platform, focusing on the ability of the platform to deliver a scalable, highly available next generation firewall with functionality beyond the basic requirements of an NGFW. The validation started with an audit of the test bed environment and the use case scenarios.

NGFW Security Services

ESG Lab started with a pre-staged test bed as shown in Figure 3. The environment was designed to emulate key elements of a distributed enterprise network. A number of physical and virtual endpoint machines were deployed behind two McAfee Next Generation Firewalls configured in an HA cluster. A branch office environment was simulated behind a single McAfee firewall, and remote users connected to corporate resources over the internet using the McAfee VPN client. The main and branch offices were connected via a VPN tunnel between the cluster of firewalls at the main office and the single firewall at the remote site.

Figure 3. The ESG Lab Test Bed



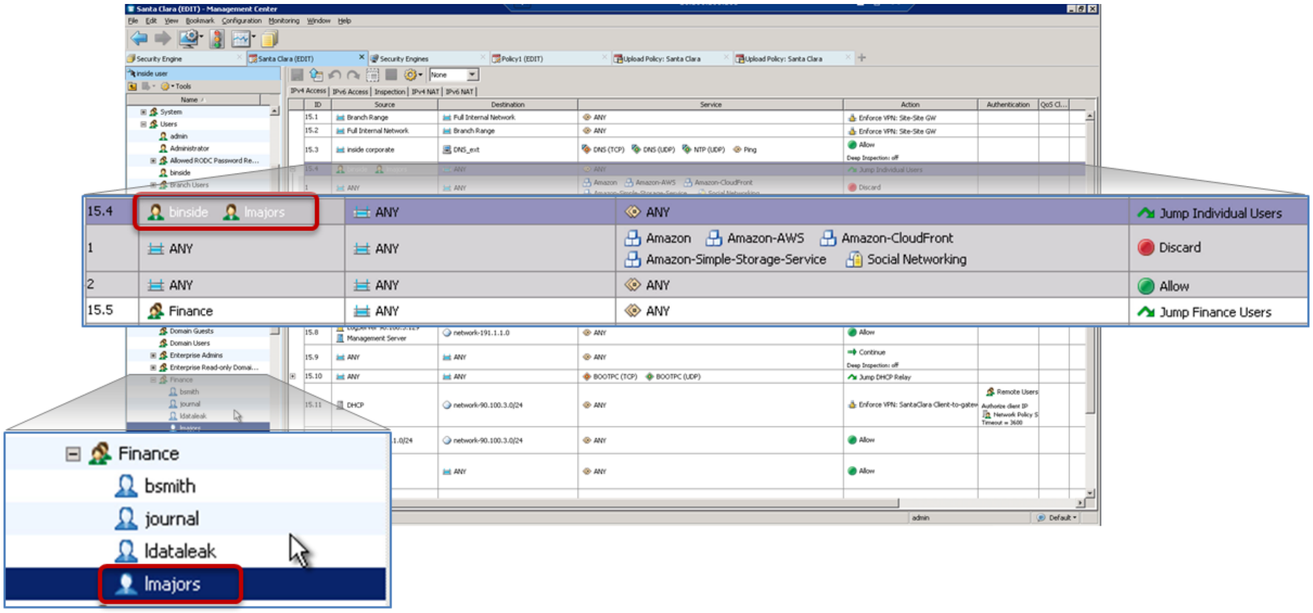
In the first stage of testing, ESG Lab was looking at global security policy configuration and enforcement, testing access by a variety of users from different locations inside and outside of the corporate network. Integration with Active Directory to provide identity based security was also of interest, as was the ability to deploy multiple functions on the same platform, testing VPN services working in concert with McAfee Next Generation Firewall in these tests.

ESG Lab Testing

ESG Lab tested access using endpoints in three different scenarios: Office users attempting to access prohibited sites and services; the same users accessing the internet over the corporate VPN; and finally branch office access to corporate resources over a VPN Tunnel.

McAfee Next Generation Firewall integrates with Microsoft Active Directory to leverage defined users and groups when creating and enforcing policies to restrict access to certain sites or services. A single policy set used by all firewalls in the cluster, so that no matter where a user connects from, the same rules apply. Figure 4 shows policies defined for two users, including user lmajors, a member of the finance group, and the subject of our first test.

Figure 4. Integrating Active Directory Users and Groups into Firewall Rules

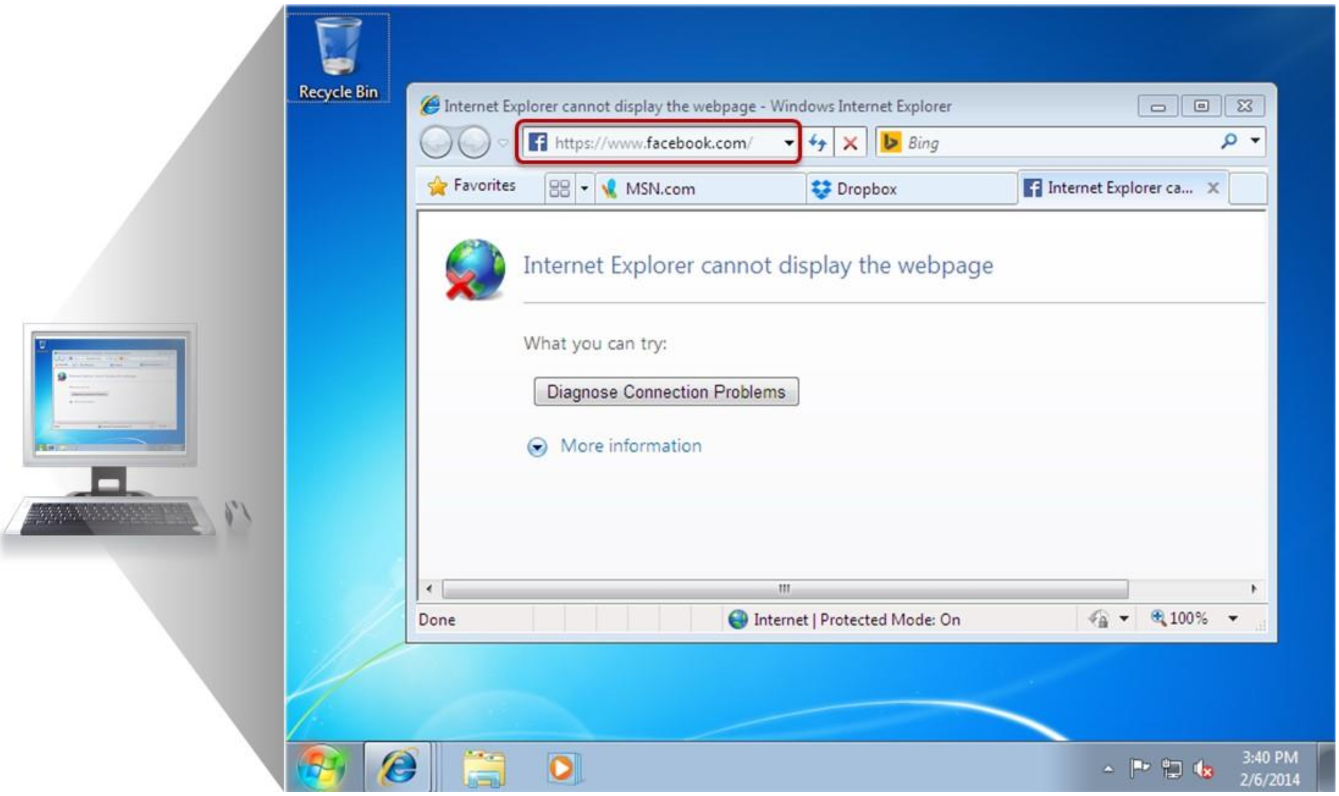


15.4	binside lmajors	ANY	ANY	Jump Individual Users
1	ANY	ANY	Amazon Amazon-AWS Amazon-CloudFront Amazon-Simple-Storage-Service Social Networking	Discard
2	ANY	ANY	ANY	Allow
15.5	Finance	ANY	ANY	Jump Finance Users

- Finance
  - bsmith
  - journal
  - ldataleak
  - lmajors

The ESG Lab Engineer logged into a virtual desktop as user lmajors and attempted to access a social networking site. As seen in Figure 5, the user was unable to access the website.

Figure 5. Social Network Access Blocked by User Identity



Internet Explorer cannot display the webpage - Windows Internet Explorer

https://www.facebook.com/

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems

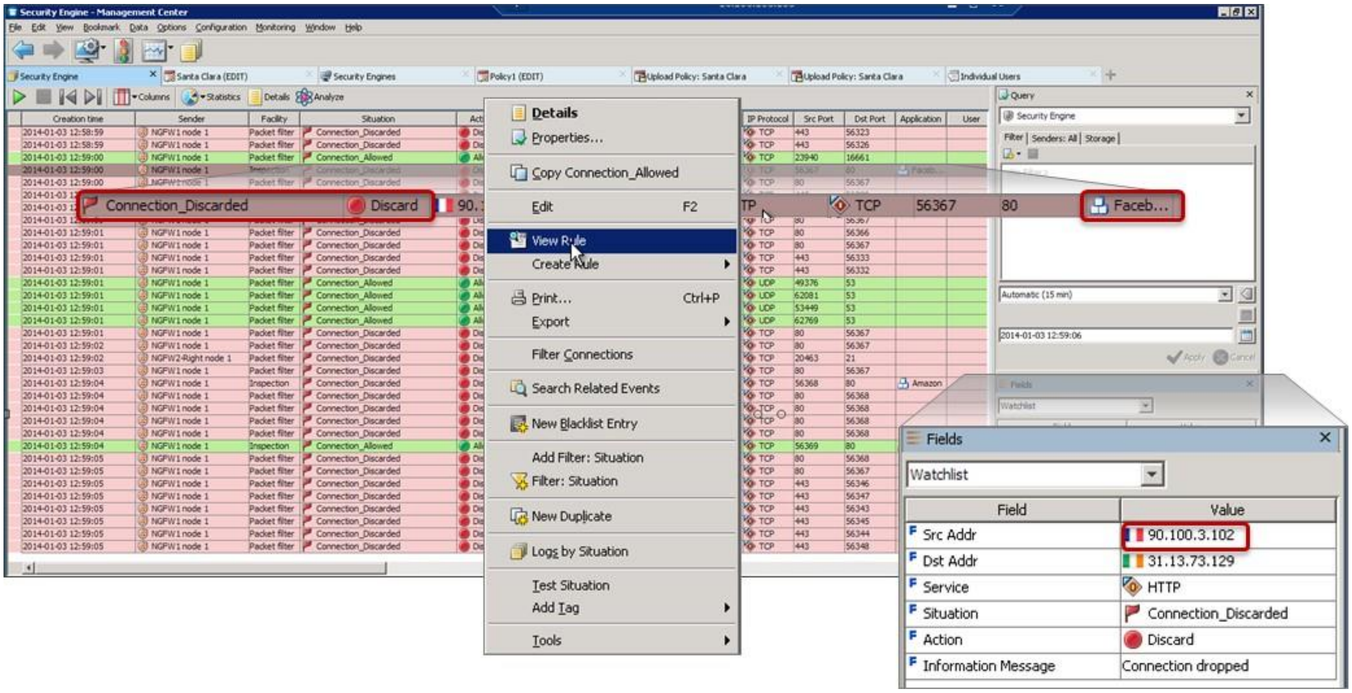
More information

Done

Internet | Protected Mode: On

Using the Security Engine Management Center, ESG was able to locate the event, cross referencing the virtual desktop's IP address: 90.100.3.102.

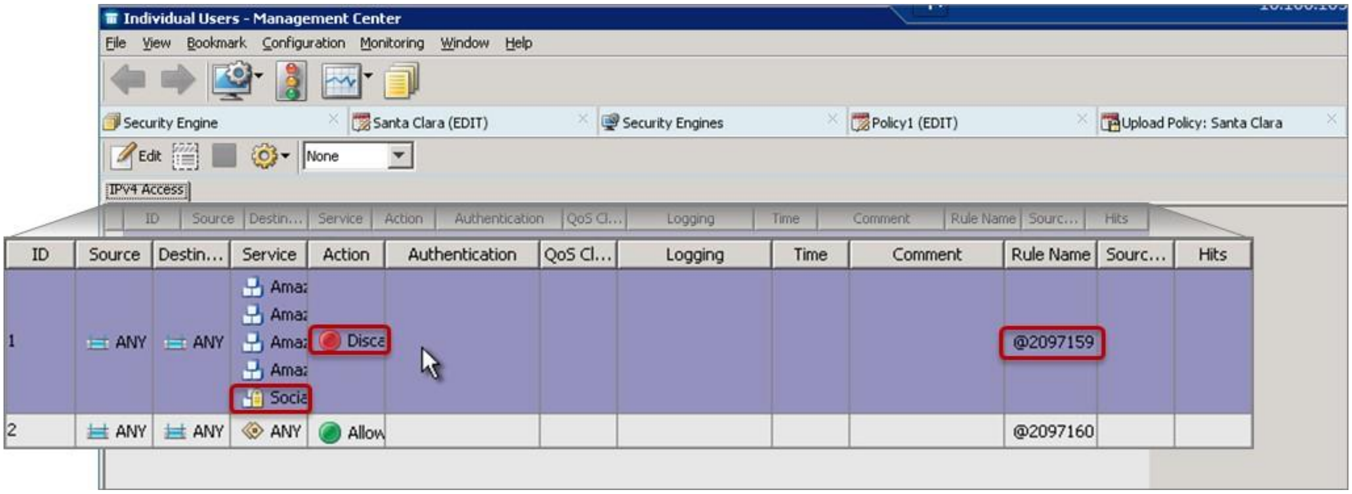
Figure 6. Examining the Event in the Log–Restricted Site Access



Field	Value
Src Addr	90.100.3.102
Dst Addr	31.13.73.129
Service	HTTP
Situation	Connection_Discarded
Action	Discard
Information Message	Connection dropped

By right-clicking on the event and selecting "View Rule," ESG Lab was able to view the precise firewall rule that blocked the connection, shown in Figure 7. Rule 2097159 was confirmed as the policy previously defined for user lmajors.

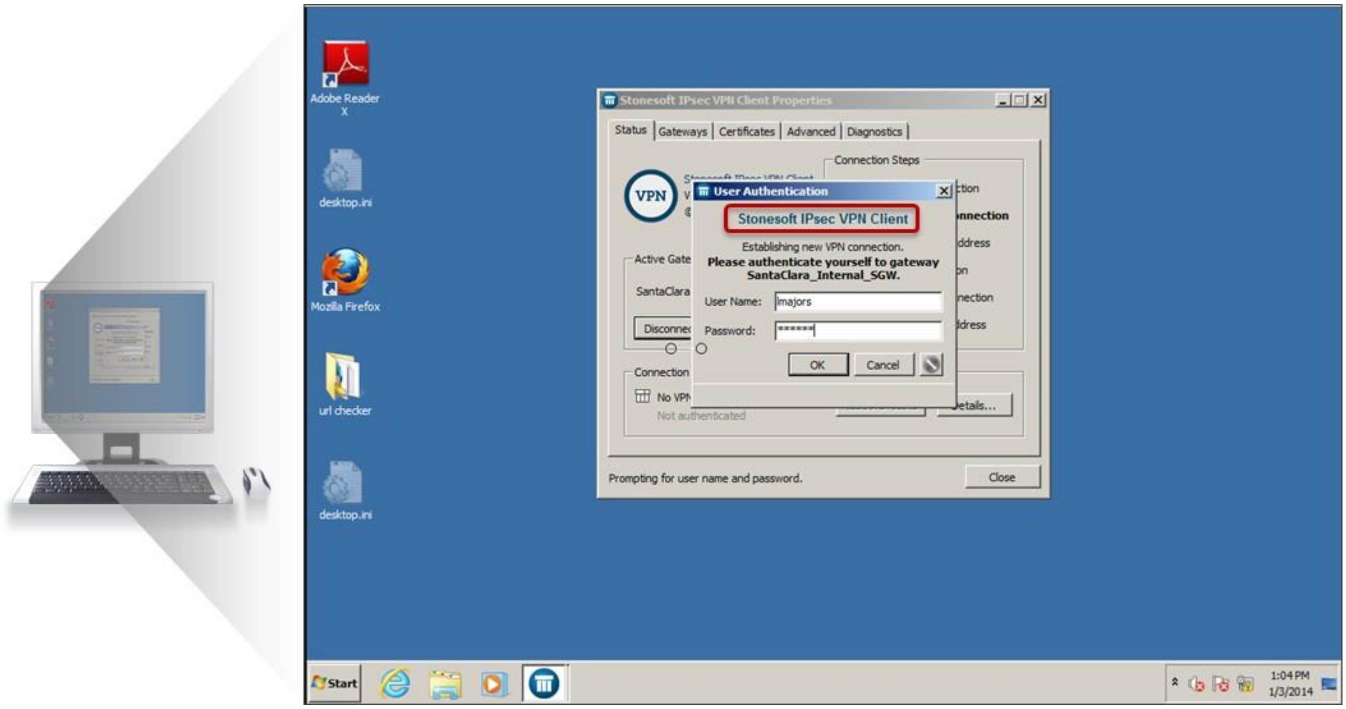
Figure 7. Examining the Firewall Rule that was Invoked


Individual Users - Management Center
File View Bookmark Configuration Monitoring Window Help
Security Engine
Santa Clara (EDIT)
Security Engines
Policy1 (EDIT)
Upload Policy: Santa Clara
Edit
None
IPv4 Access

ID	Source	Destin...	Service	Action	Authentication	QoS Cl...	Logging	Time	Comment	Rule Name	Sourc...	Hits
1	ANY	ANY	Ama: Ama: Ama: Ama: Socia	Disca						@2097159		
2	ANY	ANY	ANY	Allow						@2097160		

Next, ESG Lab logged out of the desktop and logged the user in through a secured VPN connection from a different machine outside the firewall, as seen in Figure 8.

Figure 8. Remote User Login Over VPN



Stonesoft IPsec VPN Client Properties

Status | Gateways | Certificates | Advanced | Diagnostics

User Authentication

Stonesoft IPsec VPN Client

Establishing new VPN connection.
Please authenticate yourself to gateway SantaClara_Internal_SGW.

User Name: lmajors

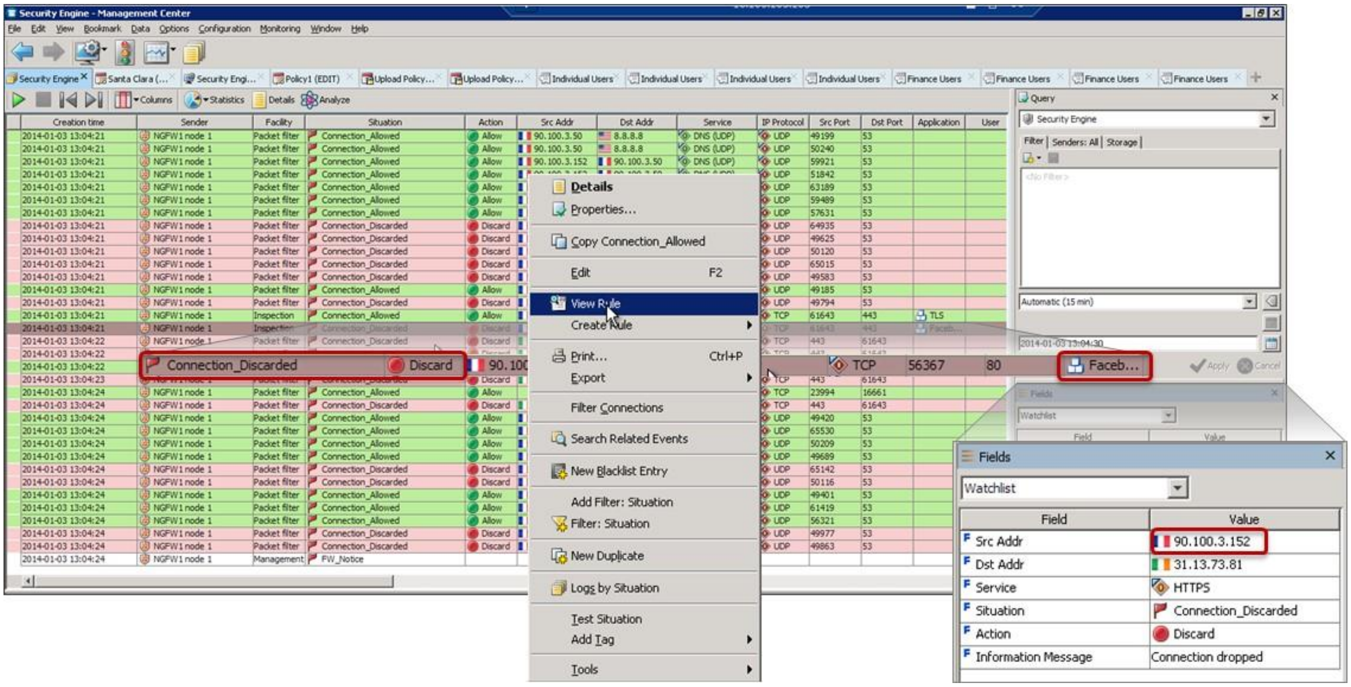
Password: ******

OK | Cancel

Prompting for user name and password.

When the login was complete, Internet Explorer was used to attempt to access a social networking site. Once again, the user was unable to access the website. Examining the event in the log once again showed that the connection was discarded, and came from a completely different IP address. Clicking on “View Rule” confirmed that the exact same rule had been invoked–rule 2097159–the policy defined for user lmajors.

Figure 9. Examining the Event in the Log–Remote VPN Restricted Site Access



Security Engine - Management Center

Connection_Discarded | Discard | 90.100 | TCP | 56367 | 80 | Faceb...

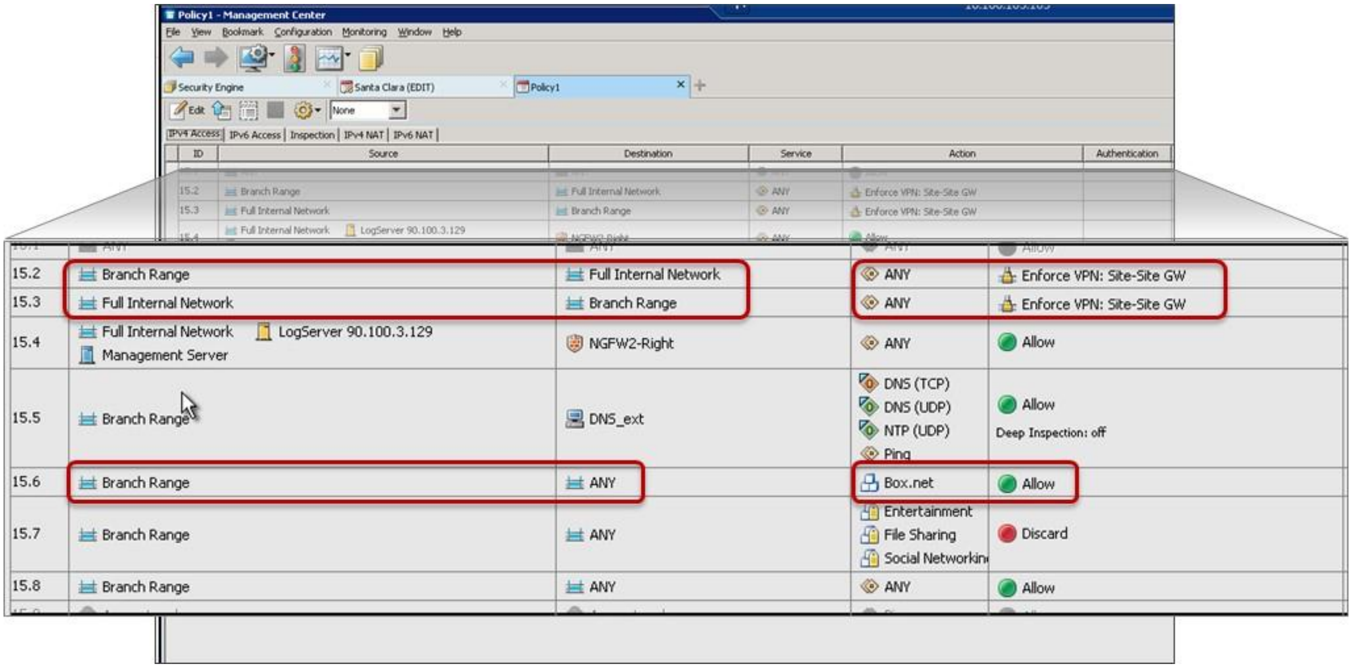
Fields

Watchlist

Field	Value
Src Addr	90.100.3.152
Dst Addr	31.13.73.81
Service	HTTPS
Situation	Connection_Discarded
Action	Discard
Information Message	Connection dropped

Next, ESG Lab examined the policies defined for inter-office communications over the company’s secure VPN. As seen in Figure 10, the main office and branch office are mutually allowed to access each other’s full network.

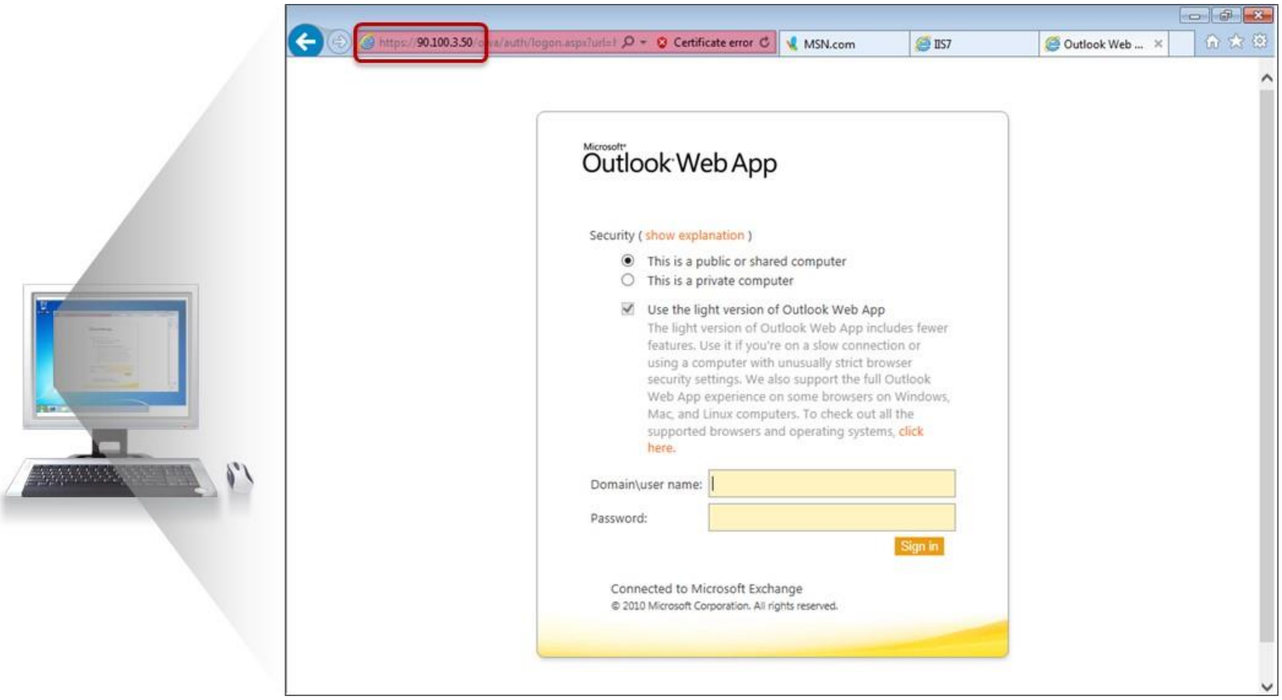
Figure 10. Branch Office Over VPN Tunnel–Rules


Policy1 - Management Center
File View Bookmark Configuration Monitoring Window Help
Security Engine
Santa Clara (EDIT)
Policy1
Edit
None
IPv4 Access | IPv6 Access | Inspection | IPv4 NAT | IPv6 NAT

ID	Source	Destination	Service	Action
15.2	Branch Range	Full Internal Network	ANY	Enforce VPN: Site-Site GW
15.3	Full Internal Network	Branch Range	ANY	Enforce VPN: Site-Site GW
15.4	Full Internal Network LogServer 90.100.3.129 Management Server	NGFW2-Right	ANY	Allow
15.5	Branch Range	DNS_ext	DNS (TCP) DNS (UDP) NTP (UDP) Ping	Allow Deep Inspection: off
15.6	Branch Range	ANY	Box.net	Allow
15.7	Branch Range	ANY	Entertainment File Sharing Social Networkin	Discard
15.8	Branch Range	ANY	ANY	Allow

Next, the engineer logged in from a system in the branch office as user bsmith. First, ESG Lab confirmed that user bsmith was able to browse the Internet, and could not access restricted sites, such as social networking. ESG Lab also confirmed that the user could access the one permitted online file sharing site and no others. Finally, Internet Explorer was used to access corporate e-mail using the Microsoft Outlook Web Client. The user was able to connect as seen in Figure 11.

Figure 11. Branch Office Over VPN Tunnel–Corporate Exchange Webmail Access



Microsoft Outlook Web App

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

☑ Use the light version of Outlook Web App

The light version of Outlook Web App includes fewer features. Use it if you're on a slow connection or using a computer with unusually strict browser security settings. We also support the full Outlook Web App experience on some browsers on Windows, Mac, and Linux computers. To check out all the supported browsers and operating systems, click here.

Domain\user name:

Password:

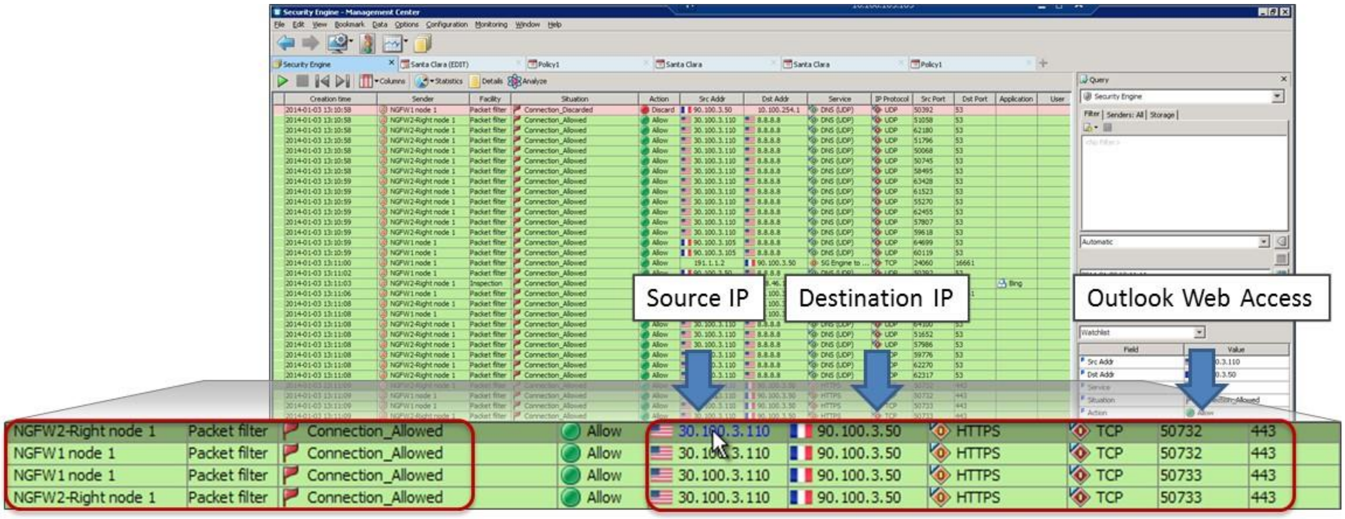
Sign in

Connected to Microsoft Exchange

© 2010 Microsoft Corporation. All rights reserved.

Once again, ESG Lab was able to quickly find and examine the event in the log, and link directly to the rule invoked.

Figure 12. Examining the Event in the Log–VPN Tunnel Intranet Access



NGFW2-Right node 1	Packet filter	Connection_Allowed	Allow	30.100.3.110	90.100.3.50	HTTPS	TCP	50732	443
NGFW1 node 1	Packet filter	Connection_Allowed	Allow	30.100.3.110	90.100.3.50	HTTPS	TCP	50732	443
NGFW1 node 1	Packet filter	Connection_Allowed	Allow	30.100.3.110	90.100.3.50	HTTPS	TCP	50733	443
NGFW2-Right node 1	Packet filter	Connection_Allowed	Allow	30.100.3.110	90.100.3.50	HTTPS	TCP	50733	443

Why This Matters

As previously stated, ESG research indicates that information security is once again a top concern of organizations large and small—32% of the IT managers surveyed cited information security initiatives as their most important IT priority for 2014.[2] Faced with a dangerous threat landscape and a multitude of new IT initiatives, security professionals and executives are forced to address new security requirements with legacy tools, point products, short-staffed security groups, and manual processes. What's needed to address these challenges are intelligent, automated, and tightly integrated security management systems leveraging multiple technologies and tools.

ESG Lab validated McAfee Next Generation Firewall was able to use a single, global policy set to control access by users no matter where in the organization they connected to the network. McAfee Next Generation Firewall also demonstrated that organizations can deploy multiple functions on the same platform, with VPN servers and VPN tunnel servers working in concert with McAfee Next Generation Firewall in these tests, but much wider functionality available by simply enabling what McAfee refers to as "personalities" via license keys–as a function of the McAfee unified software core. Consolidation of security functions means fewer devices to manage and less operational overhead.

[2] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

Centralized Management

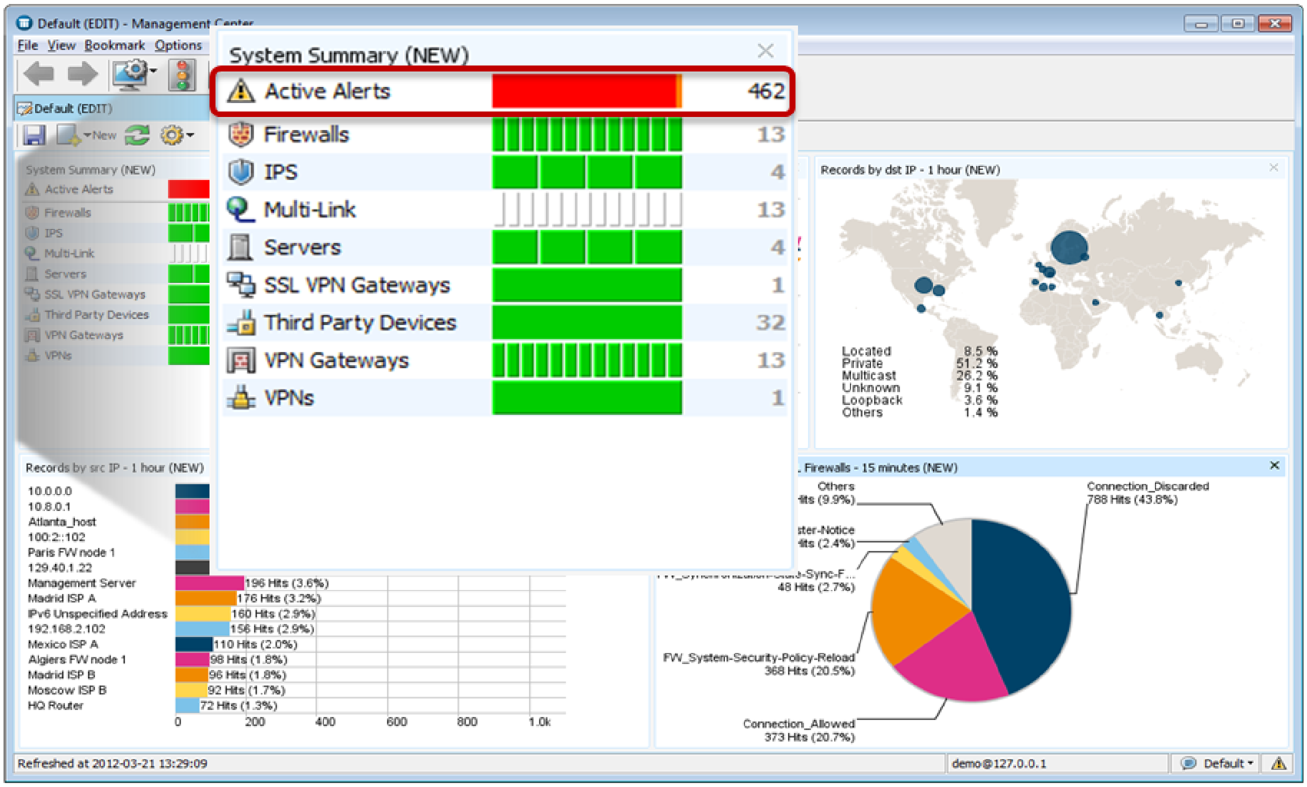
The McAfee Security Management Center gives administrators the ability to configure and manage all next generation security systems throughout the network. The Security Management Center provides complete single-pane-of-glass visibility and control of both physical and virtual networks, and can integrate with third-party devices and event management tools. The console enables one-step management of firewall and IPS rules, and accelerates the investigation and management of security events by providing a correlated view of all network activity.

The Security Management Center is the central repository for all configuration information, and contains shared rules for Firewall and IPS as well as backups for disaster recovery. Supporting customizable, role-based access, the console can manage multiple domains, relieving the management burden in the service provider environment. On top of traditional management console features such as real-time reporting and monitoring and customizable dashboards, the Security Management Center includes rule-based optimization and the ability to create rules directly from logs, designed to increase performance and simplifying the administrator workload.

ESG Lab Testing

For the evaluation of the McAfee Security Management Center, ESG Lab used a preconfigured test bench representing a typical enterprise implementation of multisite high-availability next generation firewalls. As shown in Figure 13, the Security Management Center Dashboard provides a comprehensive overview of the environment, which in this case includes 13 firewalls, four intrusion protection systems, one SSL VPN, 13 VPN gateways, and integration with an additional 32 third-party devices.

Figure 13. McAfee Security Management Center Dashboard



System Summary (NEW)

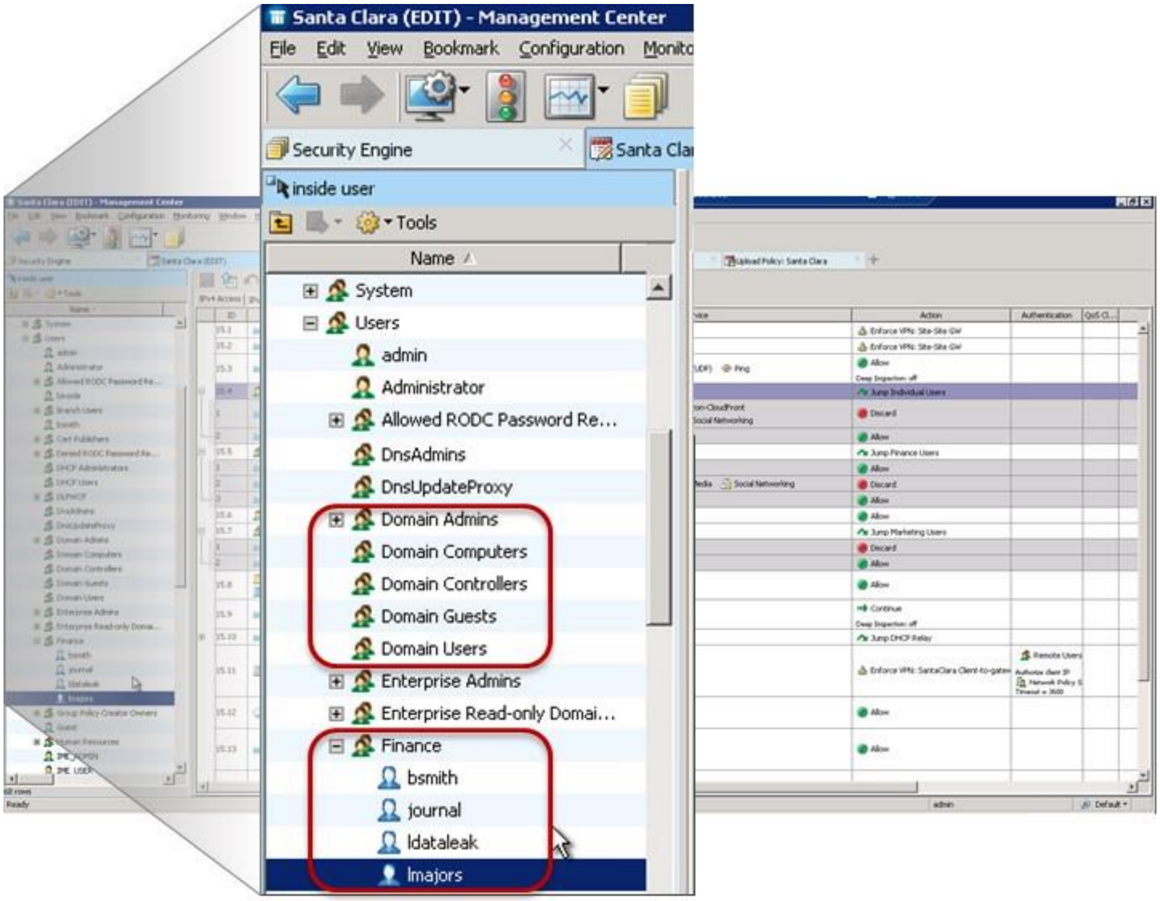
Active Alerts	462
Firewalls	13
IPS	4
Multi-Link	13
Servers	4
SSL VPN Gateways	1
Third Party Devices	32
VPN Gateways	13
VPNs	1

Default (EDIT) - Management Center
File View Bookmark Options
Default (EDIT)
New
Records by dst IP - 1 hour (NEW)
Located 8.5 %
Private 51.2 %
Multicast 26.2 %
Unknown 9.1 %
Loopback 3.6 %
Others 1.4 %
Records by src IP - 1 hour (NEW)
10.0.0.0
10.8.0.1
Atlanta_host
100:2::102
Paris FW node 1
129.40.1.22
Management Server 196 Hits (3.6%)
Madrid ISP A 176 Hits (3.2%)
IPv6 Unspecified Address 160 Hits (2.9%)
192.168.2.102 156 Hits (2.9%)
Mexico ISP A 110 Hits (2.0%)
Algiers FW node 1 98 Hits (1.8%)
Madrid ISP B 96 Hits (1.8%)
Moscow ISP B 92 Hits (1.7%)
HQ Router 72 Hits (1.3%)
0 200 400 600 800 1.0k
Firewalls - 15 minutes (NEW)
Others
Hits (9.9%)
ster-Notice
Hits (2.4%)
-Sync-F...
48 Hits (2.7%)
FW_System-Security-Policy-Reload
368 Hits (20.5%)
Connection_Allowed
373 Hits (20.7%)
Connection_Discarded
788 Hits (43.8%)
Refreshed at 2012-03-21 13:29:09
demo@127.0.0.1
Default

The top left pane of Figure 13 provides an at-a-glance green/yellow/red stoplight overview of system status. During the evaluation, there were 462 active alerts, ranging from active threats and intrusion attempts to link failures. The top right pane provides a geographic overview of recent network traffic, while the bottom left pane provides traffic summaries for the highest bandwidth IP addresses or domains. The bottom right pane provides a pie-chart classification of the traffic, showing accepted and discarded connections. This comprehensive overview of system status enables the administrator to rapidly determine the health of both the security system and the network as a whole, and guides the administrator to any trouble areas, providing a quick means to address potential threats, resource imbalances, or act on other issues.

As a next generation security solution, the McAfee system integrates directly with Microsoft Active Directory. From the Security Management Center, administrators can create firewall rules and security policies specifying AD domains and users. Rules and policies are enforced regardless of the computer or IP address originating traffic, greatly easing the administrative burden as more users transition to using multiple mobile devices with rapidly changing IP addresses.

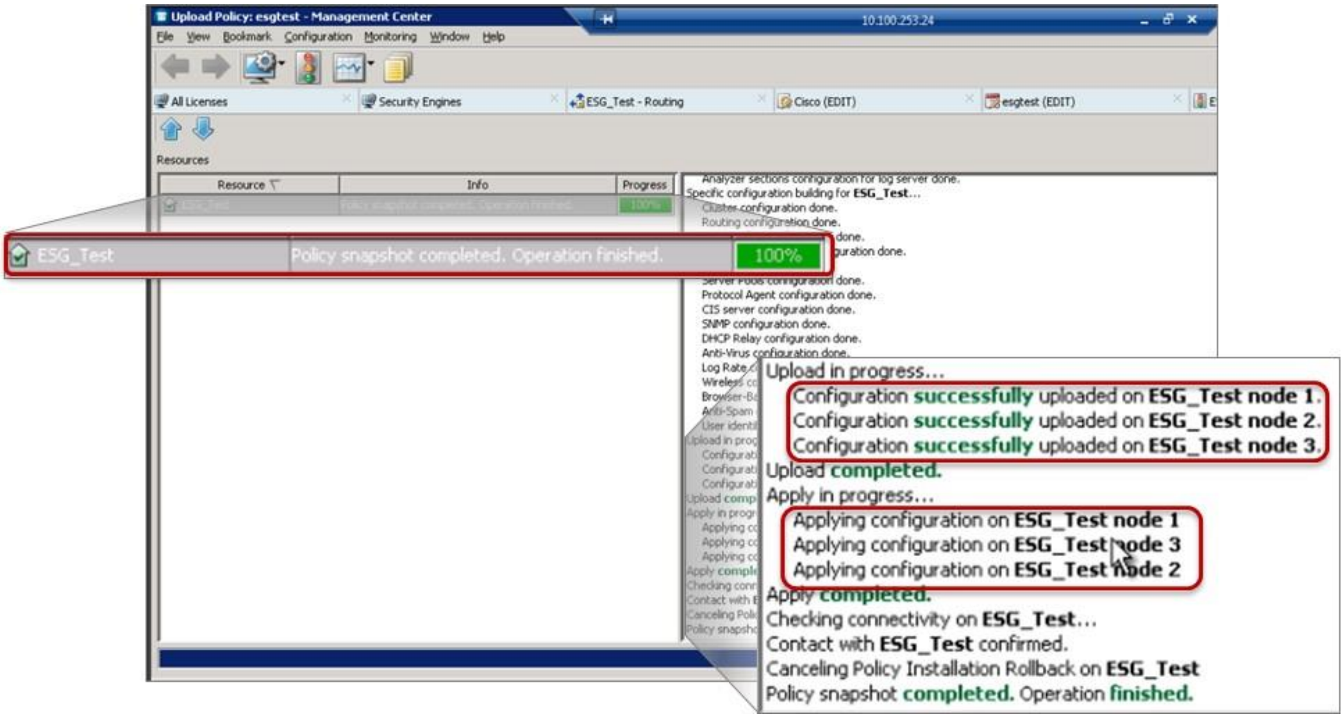
Figure 14. Management Integration with Active Directory



The McAfee Security Management Center is designed from the ground up to configure and manage multiple high-availability clusters of next generation security systems. The current configuration of each cluster is maintained in the Security Management Center for rapid deployment after configuration changes or during the addition of new systems for scaling.

As shown in Figure 15, when the administrator deploys a new configuration, the Security Management Center first creates a snapshot of the policy set. It then validates the new configuration and uploads the configuration to each system in the cluster. The new configurations are applied, and each system is tested to ensure proper operation. Should a configuration upload fail, the system can easily roll back to the snapshot of the previous policy set, ensuring continuity of operations.

Figure 15. Deploying Policy Sets to the Cluster


Upload Policy: esgtest - Management Center
10.100.253.24
File View Bookmark Configuration Monitoring Window Help
All Licenses
Security Engines
ESG_Test - Routing
Cisco (EDIT)
esgtest (EDIT)
Resources

Resource	Info	Progress
ESG_Test	Policy snapshot completed. Operation finished.	100%

```
    Analyzer sections configuration for log server done.
Specific configuration building for ESG_Test...
    Cluster configuration done.
    Routing configuration done.
    done.
    guration done.
    Server Pools configuration done.
    Protocol Agent configuration done.
    CIS server configuration done.
    SNMP configuration done.
    DHCP Relay configuration done.
    Anti-Virus configuration done.
Upload in progress...
    Configuration successfully uploaded on ESG_Test node 1.
    Configuration successfully uploaded on ESG_Test node 2.
    Configuration successfully uploaded on ESG_Test node 3.
Upload completed.
Apply in progress...
    Applying configuration on ESG_Test node 1
    Applying configuration on ESG_Test node 3
    Applying configuration on ESG_Test node 2
Apply completed.
Checking connectivity on ESG_Test...
Contact with ESG_Test confirmed.
Canceling Policy Installation Rollback on ESG_Test
Policy snapshot completed. Operation finished.
```

Why This Matters

ESG research has found that five of the challenges of protecting IT assets most-cited by administrators are related to managing the security infrastructure.[3] These challenges span monitoring network and server activities to event detection and keeping track of configuration changes. All of these challenges, while necessary to maintain the ongoing security of the network, represent activities that are both time consuming and demand attention to detail, distracting IT from other pressing issues.

The McAfee Security Management Center provided an excellent interface, making it easy for ESG Lab to understand the current health of the security infrastructure at a glance as well as the security of the network as a whole. The console enabled rapid and painless drill-down from overall status and alerts to the underlying configuration and logs. Policies and configuration changes were easy to create and edit with a single action and applied to all nodes in the environment with a single click. This can represent a significant reduction in time and effort for organizations with dozens of globally distributed networks and hundreds of firewalls to manage.

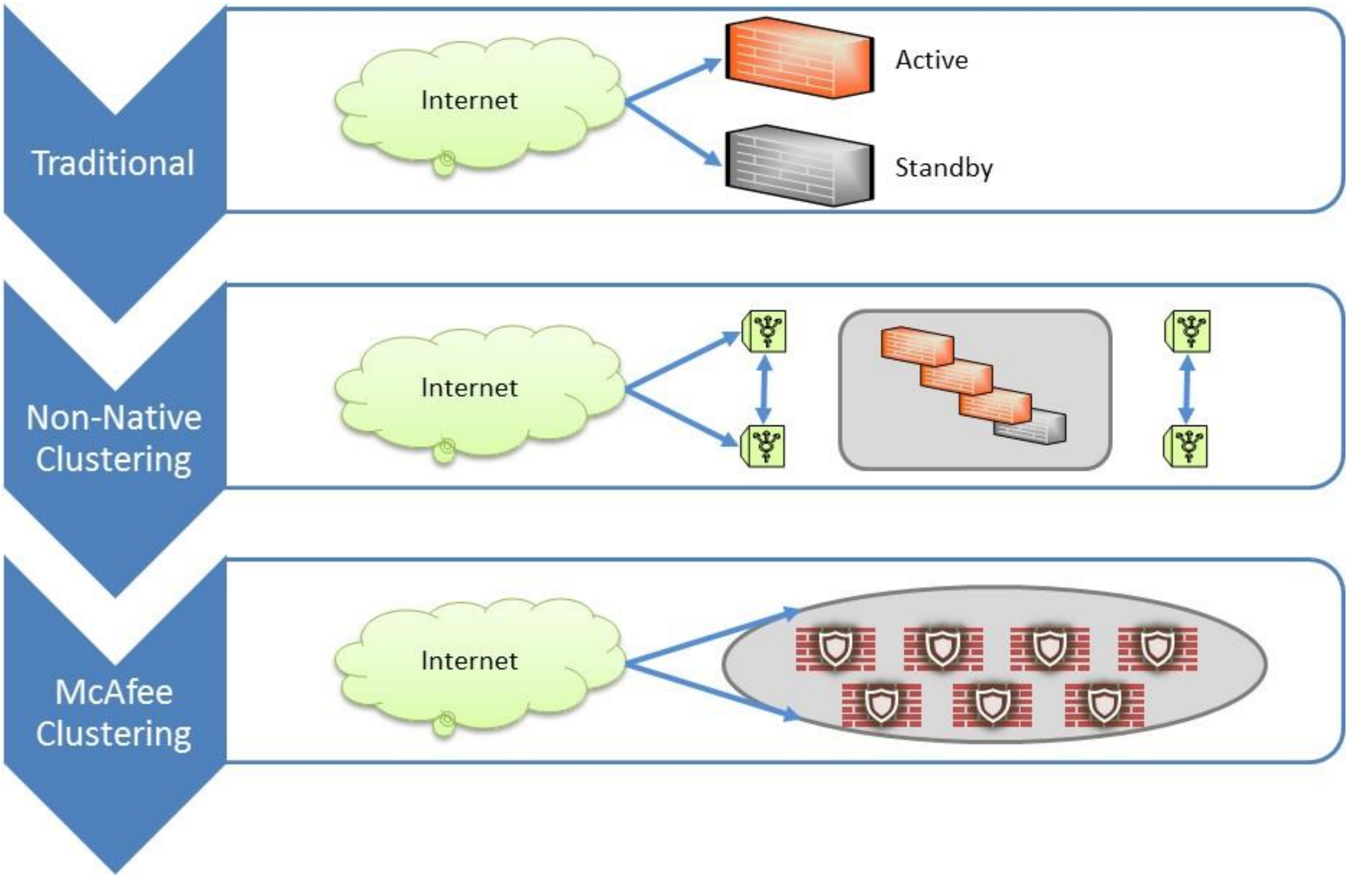
[3] Source: ESG Research Brief, Top Security Challenges for IT Assets Residing in Data Centers, May 2013.

Scalability and Availability

The McAfee Next Generation Firewall is designed to enable high availability through native clustering, ensuring that administrators are able to maintain network connectivity in the face of failures. Native clustering also provides scaling of both bandwidth and processing power, allowing IT to provide the necessary performance for demanding workloads.

As shown in Figure 16, the traditional method of achieving high availability is to manually implement a cluster composed of two nodes—an active node and a passive backup node. If the active node fails, the network connections and operations move to the passive node. This implementation often requires the administrator to keep the configuration of the active and passive nodes in sync. While traditional active-passive configurations provide a measure of high availability, this method does not provide scaling for bandwidth or performance.

Figure 16. Native Clustering



The next level of availability is best described as non-native clustering because the clustering technology is not built into the security solution. Non-native clustering is built on the traditional active-passive clustering methodology, and implements additional active nodes. Because the nodes are not cluster-aware and do not communicate or cooperate, non-native clustering must implement external third-party load balancers on either side of the security infrastructure to provide both availability and scaling of bandwidth and performance. As with traditional clustering, configuration synchronization must be implemented–often manually–by the IT administrator and the additional cost and management of load balancers must be taken into account.

McAfee's Next Generation Firewall implements native clustering, where all nodes in the cluster are aware of and communicate with all other nodes in the cluster. Load balancing is automatically handled by the nodes, eliminating the need for external devices and greatly simplifying implementation and management. McAfee Security Management Center maintains the central repository of the security infrastructure configuration. Upon changes in the configuration, the Security Management Center updates the configuration in each node, maintaining configuration synchronization automatically.

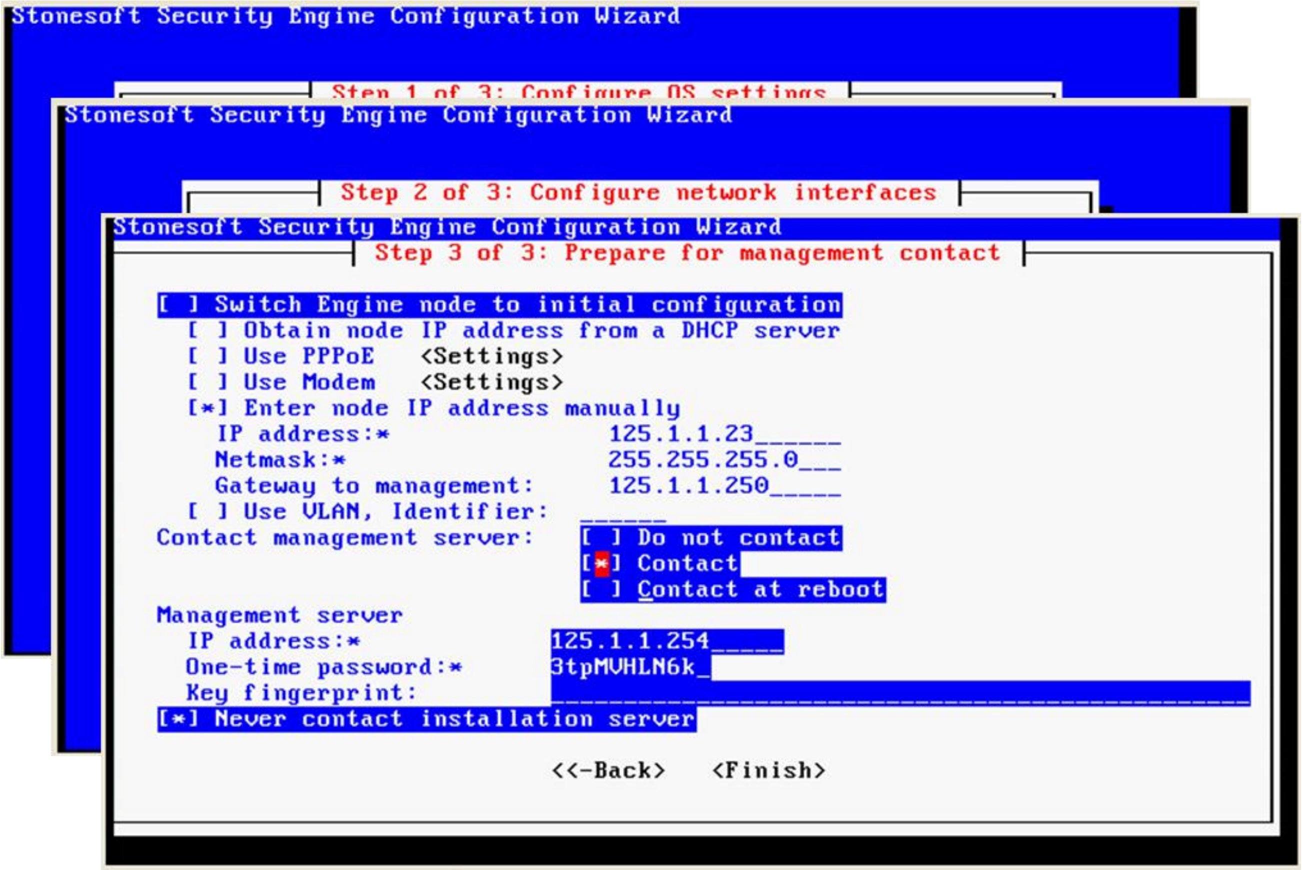
If a node in the cluster is taken offline for any reason, the other nodes in the cluster automatically pick up the workload, providing resilience and high availability with minimal performance impact and without administrator intervention. As the cluster is expanded, the processing power and network bandwidth of the new nodes provide additional packet processing and network capacity, scaling the security infrastructure for both performance and bandwidth.

ESG Lab Testing

To evaluate scalability and availability, ESG Lab added a node to the two-node cluster in the test bed shown in Figure 3.

The setup of the firewall software is a three-step process that required very little administrator interaction. In the first step, basic operating system parameters such as keyboard/mouse and time zone were configured. The second step configured the network interfaces, and the third step configured the management network. This step also required entering a one-time password generated by the Security Management Center, ensuring secure communication between the node and the management station. Once all steps were completed, the software was installed, and the node was rebooted and ready to be configured.

Figure 17. Installation

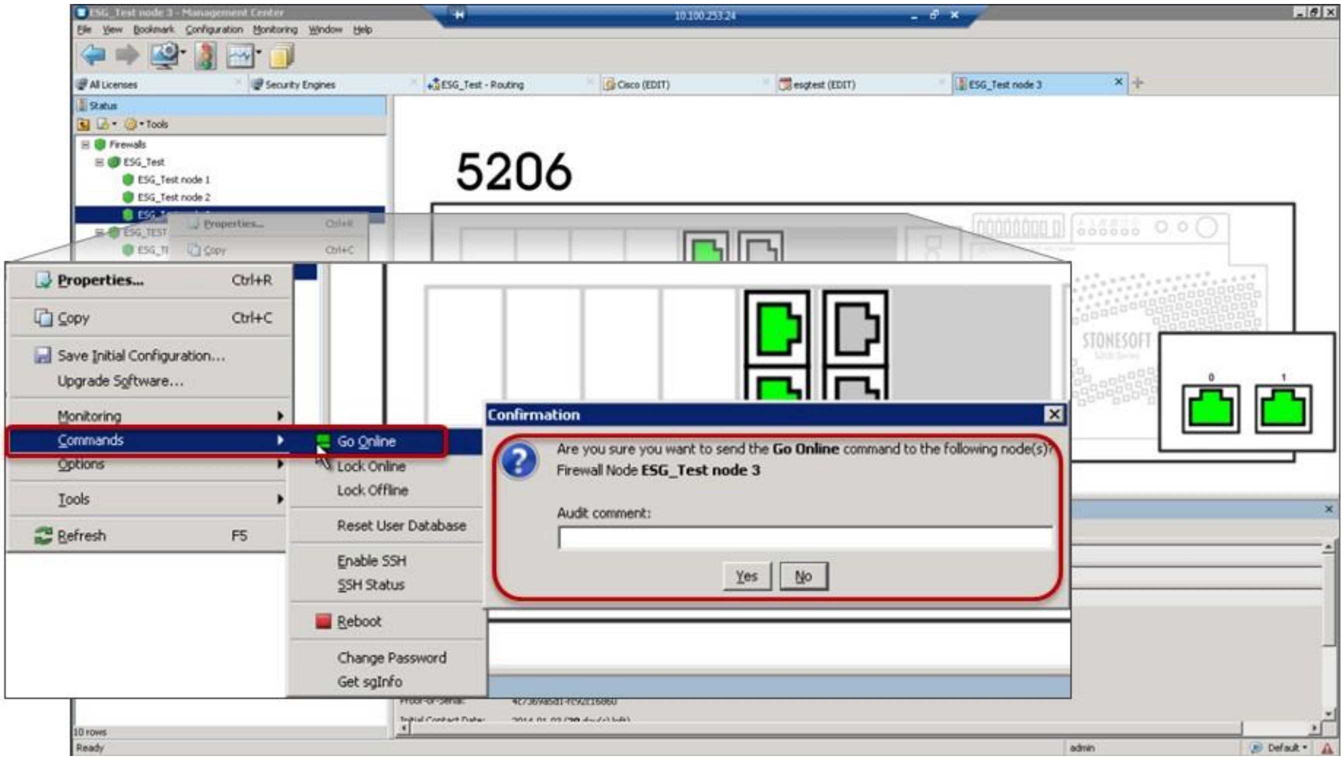


```
Stonesoft Security Engine Configuration Wizard
        Step 1 of 3: Configure OS settings

Stonesoft Security Engine Configuration Wizard
        Step 2 of 3: Configure network interfaces

Stonesoft Security Engine Configuration Wizard
        Step 3 of 3: Prepare for management contact

[ ] Switch Engine node to initial configuration
  [ ] Obtain node IP address from a DHCP server
  [ ] Use PPPoE    <Settings>
  [ ] Use Modem    <Settings>
  [*] Enter node IP address manually
    IP address:*                125.1.1.23______
    Netmask:*                   255.255.255.0___
    Gateway to management:      125.1.1.250_____
  [ ] Use VLAN, Identifier:     ______
Contact management server:      [ ] Do not contact
                                [*] Contact
                                [ ] Contact at reboot

Management server
  IP address:*                125.1.1.254_____
  One-time password:*         3tpMVHLN6k_
  Key fingerprint:            ________________________________________________
[*] Never contact installation server

                        <<-Back>    <Finish>
```

The second step in the process of expanding the cluster was to join the node to the cluster. ESG Lab used the Security Management Center to inspect the new node, which highlighted the active network ports in green (see Figure 18).

Using a few mouse clicks, the node was joined to the cluster, and the cluster configuration was installed on the new node. At that point, a single command was used to bring the new node online.

Figure 18. Post-installation Configuration



Are you sure you want to send the **Go Online** command to the following node(s)?
Firewall Node **ESG_Test node 3**

Audit comment:

Why This Matters

Security infrastructure scalability, resilience, and performance are significant challenges as organizations embrace the critical role of information security in the face of ever expanding threats against the network. This is exacerbated by the increasing trend of embracing public and private cloud technologies, which puts a premium demand on network bandwidth. Traditional solutions have relied on monolithic architectures requiring custom hardware and over-provisioning to meet these challenges or have utilized third party load balancers to insert more independent appliances into the network path.

ESG Lab confirmed that McAfee Next Generation Firewall native clustering can offer scalability and resilience while securing the network. Adding a node to meet increasing demands for packet processing and network bandwidth was simple and fast. ESG Lab added an additional McAfee NGFW physical appliance to the native cluster with no interruption in services. ESG Lab validated that McAfee native clustering supports nodes with mixed software versions in the same cluster. ESG Lab confirmed uninterrupted protection as nodes were added to and removed from the cluster, enabling continuous availability through planned and unplanned events.

Advanced Evasion Detection

Because highly targeted, sophisticated cyber-attacks are so resource-intensive, they now include advanced evasion techniques (AETs) in increasing numbers to circumvent security defenses. An evasion is simply an attempt to disguise an attack to avoid detection and blocking by network security systems. Some of the general types of evasion techniques that have been identified include:

- *Evasions that are based on techniques defined in a specification and used according to the specification*. IP fragmentation is an example of this type of technique where IP datagrams are broken down into smaller datagrams to disguise the contents.
- *Techniques defined in a specification, but not used according to the specification*. An example of this technique is Microsoft Remote Procedure Call (MSRPC) endian manipulation, in which MSRPC is used in "big-endian" format rather than "little-endian" as defined in the specification.
- *Techniques defined in a specification for some other component, but used in a different way*. MSRPC network data representation (NDR) value manipulation is an example of this technique.
- *Evasion techniques that are forbidden by a specification, but accepted by the target system*, such as TCP overlap where overlapping segments of a TCP stream are sent with conflicting data to hide malicious code.

An advanced evasion combines a number of known techniques simultaneously across multiple protocols and is capable of changing on the fly during an attack. More than 800 million combinations have been identified to date by McAfee.

McAfee Next Generation Firewall uses data normalization to enable full inspection of data traffic by reconstructing data streams that have been hidden or obscured by AETs. Data normalization is the process of deconstructing or decoding packets for all protocols, at all layers of the stack. Protocol or packet deconstruction and reconstruction is a computationally intensive effort, and McAfee has built this capability into the core of the McAfee NGFW.

McAfee NGFW examines data traffic at layer 7 and continuously deconstructs, fully inspects, and reconstructs the streams. Then the same is done for TCP-level segments, pseudo packets, and IP-level packets to provide continuous visibility. Once identified, advanced evasions that can carry or forge the path for exploits are removed.

McAfee Evader

While testing evasions on single network layers and at the protocol level, McAfee began to learn about more complex and dynamic evasions appearing in the wild. McAfee created an automated testing tool and started to run more advanced, combined, and dynamic evasions across all network layers and protocols. In 2010, McAfee published on the discovery of AETs, and highlighted the vulnerabilities of most security devices at the time. McAfee asserts that most security devices are still vulnerable to AETs today. McAfee runs millions of evasion combinations in their labs daily, and shares their findings with the Computer Emergency Readiness Team (CERT) and numerous security vendors.

The Evader tool was developed to provide in-house testing capability for companies that deploy network security devices that use deep packet inspection, such as IPS and next generation firewalls. Companies can use Evader for real-world tests of their protection against AETs and thus improve security levels and evaluate the results against vendor claims and published lab results. Evader is provided free of charge by McAfee on their website.[4] It's important to note that Evader is not a hacking tool or a penetration test harness. Evader simply tests if a known exploit can be delivered using AETs through currently installed security devices to a target host.

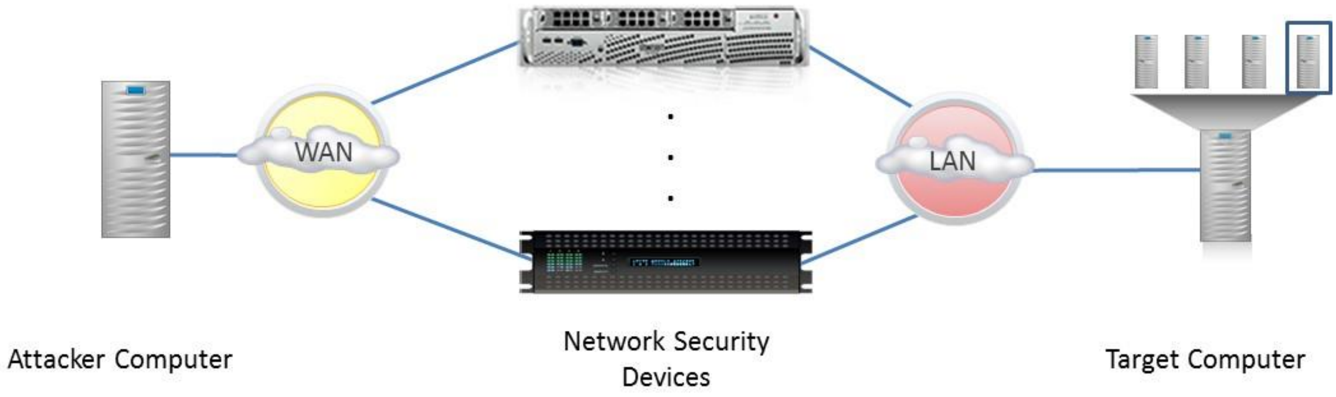
ESG Lab Tested

ESG Lab tested Evader in a McAfee lab that included the McAfee NGFW and a next generation firewall device from another vendor configured according to the vendor's best practices. The test bed, shown in Figure 19, consisted of a computer designated as the attacker, which was running the Evader tool under Xubuntu Linux and another

[4] http://evader.mcafee.com/

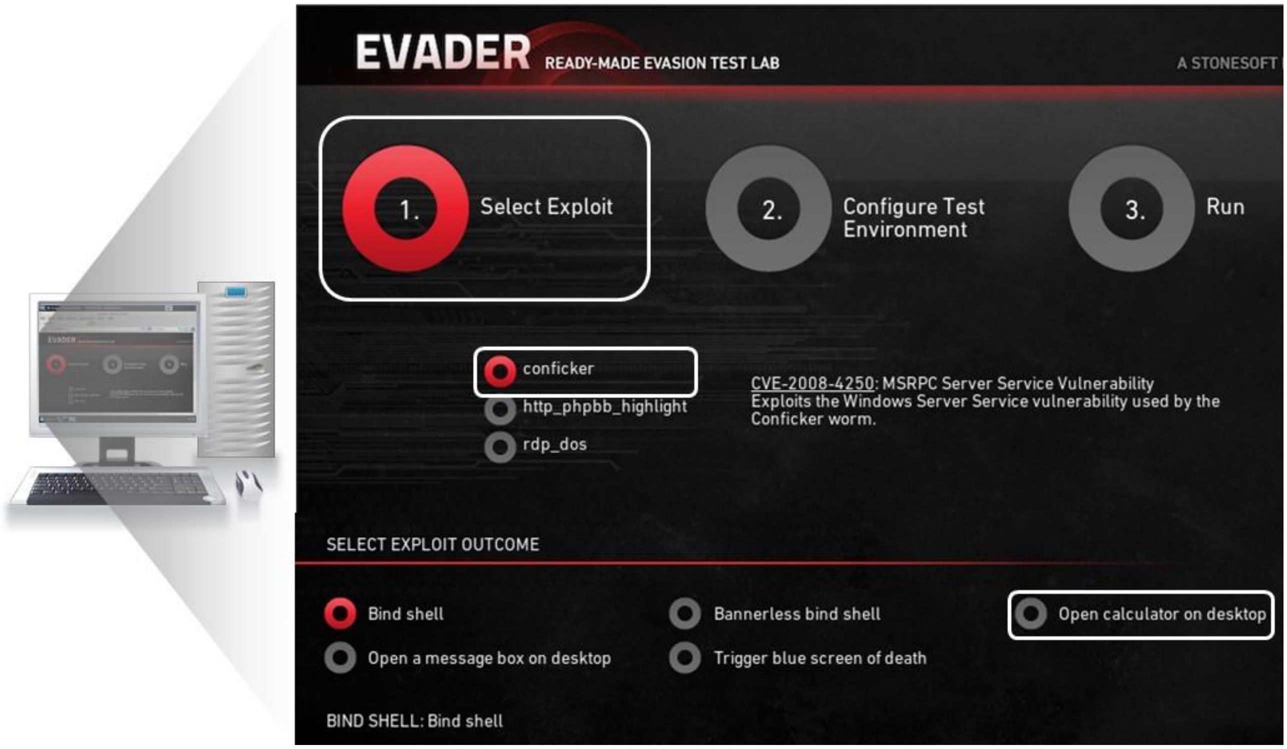
computer running Windows XP designated as the target with multiple network security devices available for testing.

Figure 19. The McAfee Evader Test Bed



First, ESG Lab opened the Evader tool on the attacker machine, as seen in Figure 20. The tool walks the user through the process in just three steps. The first step was to select the exploit and the outcome, or action to be taken should the evasion succeed. McAfee presents several outcome options. ESG Lab selected conficker, a well-known Windows XP exploit, and open calculator on desktop for the outcome. If the evasion is successful, the Evader tool will be able to open a calculator on the target system’s desktop.

Figure 20. The McAfee Evader Tool–Selecting the Exploit



EVADER READY-MADE EVASION TEST LAB

A STONESOFT

1. Select Exploit
2. Configure Test Environment
3. Run

● conficker
○ http_phpbb_highlight
○ rdp_dos

CVE-2008-4250: MSRPC Server Service Vulnerability
Exploits the Windows Server Service vulnerability used by the Conficker worm.

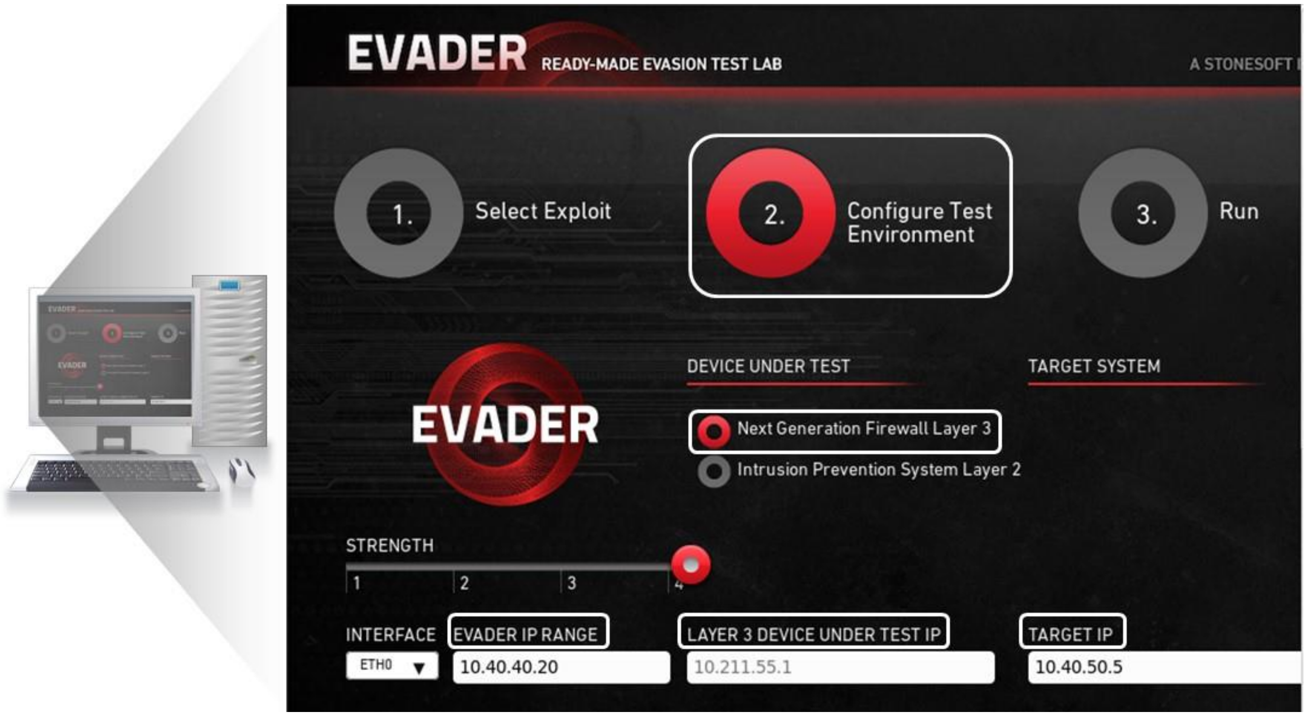
SELECT EXPLOIT OUTCOME

● Bind shell
○ Open a message box on desktop
○ Bannerless bind shell
○ Trigger blue screen of death
○ Open calculator on desktop

BIND SHELL: Bind shell

The test environment was configured next, where ESG Lab specified the device to be tested, the strength of the test, i.e.: how many evasions will be simultaneously used by the Evader tool, and confirmed the IP addresses of the device under test and the target computer. For the first round of tests, ESG Lab selected a next generation firewall from another vendor.

Figure 21. The McAfee Evader Tool–Configuring the Environment


EVADER READY-MADE EVASION TEST LAB
A STONESOFT
1. Select Exploit
2. Configure Test Environment
3. Run
EVADER

DEVICE UNDER TEST

● Next Generation Firewall Layer 3
○ Intrusion Prevention System Layer 2

TARGET SYSTEM

STRENGTH: 1 2 3 ●4

INTERFACE: ETH0 ▼

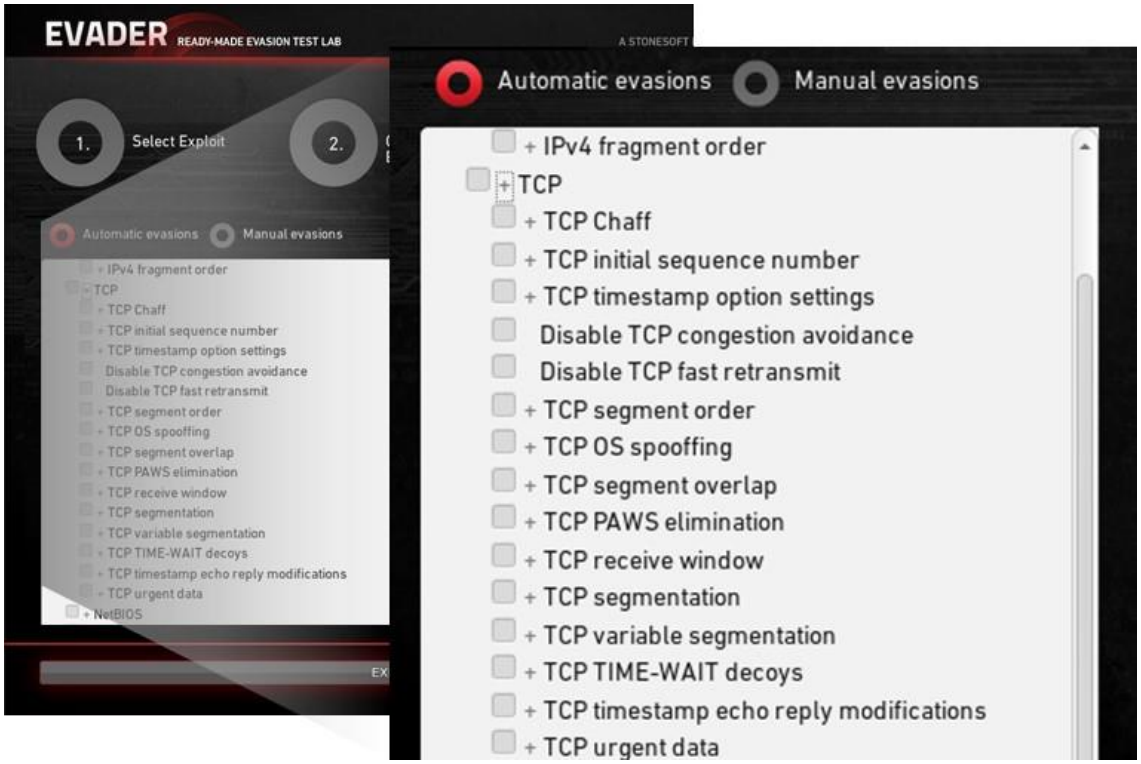
EVADER IP RANGE: 10.40.40.20

LAYER 3 DEVICE UNDER TEST IP: 10.211.55.1

TARGET IP: 10.40.50.5

ESG Lab next clicked "Run" to set runtime options including selecting the evasions to be executed in the test. As of this writing, Evader supports more than three dozen evasions. When the user selects "Automatic evasions" all evasions appropriate to the selected attack are included in the test.

Figure 22. The McAfee Evader Tool–Selecting Evasions



● Automatic evasions ○ Manual evasions

- □ + IPv4 fragment order
- □ + TCP
  - □ + TCP Chaff
  - □ + TCP initial sequence number
  - □ + TCP timestamp option settings
  - □ Disable TCP congestion avoidance
  - □ Disable TCP fast retransmit
  - □ + TCP segment order
  - □ + TCP OS spoofing
  - □ + TCP segment overlap
  - □ + TCP PAWS elimination
  - □ + TCP receive window
  - □ + TCP segmentation
  - □ + TCP variable segmentation
  - □ + TCP TIME-WAIT decoys
  - □ + TCP timestamp echo reply modifications
  - □ + TCP urgent data

Evader also supports selecting specific evasions for inclusion. The first test, ESG Lab selected manual evasions and left all evasions unchecked so that Evader would try to deploy the conficker file without evasions. As expected, the conficker file was detected by both the McAfee NGFW and by the third party next gen firewall. In both cases, the file was blocked.

Next, the test was repeated with Automatic evasions enabled. In this test, Evader used multiple evasion techniques simultaneously. In this case the third party next gen firewall was not able to detect or block the conficker file and the target system was compromised in a matter of seconds. The McAfee NGFW was able to detect and block the intrusion completely. It's important to note here that conficker file is a well understood worm that has been in the field since November 2008, and all next gen firewalls, IDS, and IPS systems should be able to easily detect and block it. By applying advanced evasion techniques, Evader was able to bypass a modern next gen firewall completely, and gain unfettered access to the target machine.

Why This Matters

In an ESG research survey, the majority (57%) of enterprise security professionals told ESG that they believe the malware landscape was worse in 2013 than it was in 2011. A comparable percentage (55%) believe that malware has grown more sophisticated, 47% say that malware attacks are more frequent, and 43% feel that malware uses more obfuscation techniques. Fifty eight percent of security professionals told ESG that they believe that network-based anti-malware technology should be integrated into next-generation firewalls, making this the most popular response by a wide margin.[5]

This is noteworthy since malware is used to give attackers access to internal systems and the key information stored on them, while further distributing itself across private networks. Detection of malware's entrance point into the network remains difficult since sophisticated malware attacks tend to use multiple, advanced obfuscation techniques to appear to be normal network activity and evade detection. If security analysts had a way to identify and remove these advanced evasions, they could improve their organizations' security postures and reduce endpoint incidents on their networks.

ESG Lab has confirmed that advanced evasion techniques can be used to circumvent modern, sophisticated network security devices and deliver malware that would otherwise be easily detected and blocked. The McAfee NGFW demonstrated the ability to normalize the data stream to detect and block the attacks, regardless of the evasion techniques being used or in what combination.

Considering that many organizations are so intent on identifying new malware that they are failing to focus on advanced evasion techniques that can enable malware to circumvent their security defenses, AETs pose a great threat because most security solutions can't detect or stop them. Security professionals and executive managers need to acknowledge and address this very real threat.

[5] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.

ESG Lab Validation Highlights

☑ ESG Lab testing has validated that the management console enabled an administrator to efficiently monitor and examine events in detail, and made identification of policies and violations simple and fast.

☑ Policies followed users and groups—and were enforced—across the entire network.

☑ McAfee Next Generation Firewall also demonstrated that organizations can deploy multiple functions on the same platform, with VPN servers and VPN tunnel servers working in concert with McAfee Next Generation Firewall in these tests.

☑ The McAfee Security Management Center provided at-a-glance visibility into the health of the security infrastructure as well as the security of the network as a whole.

☑ The console enabled rapid and streamlined drill-down from overall status and alerts to the underlying configuration and logs, as well as real-time visibility into actionable data.

☑ Rapid configuration changes were easy to make and uploading the configuration to all nodes in a cluster was accomplished with almost zero effort.

☑ Adding a node to the cluster to provide additional packet processing and network bandwidth was simple and took less than five minutes. ESG Lab validated that McAfee native clustering supports physical and virtual node types in the same cluster.

Issues to Consider

☑ A network-based security strategy can be used to complement an existing endpoint security software/antivirus strategy. While the cost and complexity of deploying and managing endpoint security software continues to rise and the effectiveness against zero day attack/polymorphic malware continues to fall, a strategy that includes a network-based solution that can detect and neutralize advanced evasion techniques can greatly improve coverage and reduce risk.

☑ ESG Lab does not report on named head to head tests without the permission of all vendors involved, but is confident that any reader can easily replicate the advanced evasion tests and results presented here in their own network with their own security devices.

The Bigger Truth

In a recent ESG survey, 32% of IT professionals and executives cited information security as an IT priority for 2014.[6] In another survey, security professionals were asked about the overall malware landscape, and 67% responded that it was either somewhat worse or much worse in 2013 than it was in 2011.[7] When asked to identify the reasons most responsible for their opinions, frequency, sophistication, and stealthy evasion techniques were the three most cited reasons. Due to ever-increasing sophistication and capabilities of malicious actors, organizations must constantly work to maintain and enhance their security systems and strategies.

Advanced threats are circumventing existing security controls, compromising hosts, and inflicting tremendous damage using sophisticated evasion techniques. In the real world, 100% prevention is impossible and a daunting task for organizations. Traditional network-based security systems can't protect against threats they can't see. Security analysts need a way to identify and block these advanced evasions.

McAfee Next Generation Firewall is engineered to provide protection against advanced evasion techniques, which are sophisticated attacks designed to confound traditional network security devices and deliver advanced persistent threats. Using the Evader tool, ESG Lab has confirmed that McAfee Next Generation Firewall normalizes the content in the data stream to protect against both known and unknown evasion techniques, across multiple protocols.

McAfee Next Generation Firewall demonstrated flexible, unified, and modular network security, delivering security features with high availability and simple manageability to businesses of all sizes. ESG Lab used the unified management console to monitor and examine events in detail, which made identification of users and policies simple and fast. Organizations can deploy multiple functions on the same platform, with VPN servers and VPN tunnel servers working in concert with McAfee Next Generation Firewall in our tests.

ESG Lab found the management console easy to use to gain insight into the overall health of the security infrastructure as well as the security of the entire network. Rapid and efficient drill-down from status and alerts to configuration and logs guided ESG Lab directly to the issue under investigation. Swift configuration changes were easy to make and uploading the configuration to all nodes in a cluster was accomplished quickly. The Security Management Center interface was complete and robust, enabling comprehensive management of the security infrastructure from a single console.

Scalability and resilience were integral to the solution using native clustering. Adding a node to meet increasing demands was simple and fast. ESG Lab deployed McAfee native clustering with physical and virtual nodes in the same cluster.

Products in the firewall space have different strengths, weaknesses, and capabilities for various types of security needs. ESG Lab believes that the McAfee Next Generation Firewall offers the features, capabilities, and integration with the McAfee suite of security products that may satisfy organizations' requirements for intelligent, actionable network security with the additional capabilities to address new and advanced evasion techniques. Any IT organization looking at next generation firewalls to improve their network security posture should give McAfee Next Generation Firewall a closer look.

[6] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.
[7] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.

Appendix

Table 1. ESG Lab Test Bed

Network Security Infrastructure	Platform
McAfee Next Generation Firewall Appliance	NGF-3202
McAfee Next Generation Firewall Appliance	NGF-5206
McAfee Next Generation Firewall Virtual Appliance	VMware vSphere Virtualization Platform
Virtualization Infrastructure	**Guests**
VMWare vSphere 5.1	Windows 7 Professional

ESG Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com