Lab Testing Detailed Report
DR130215

Competitive Testing of the Cisco ISA500 Security Appliance

24 May 2013

Miercom

www.miercom.com

Table of Contents

Copyright © 2013 Miercom

1.0 Executive Summary

Miercom conducted an independent third-party validation of the ISA550 Security Appliance with competitive assessment to the Fortinet FortiGate-20C and SonicWALL TZ105 products.

Testing conducted focused on five areas of testing:

- Deployability Assessment
- Performance with Services Enabled
- Antivirus Protection
- Application Control
- Web Reputation

We looked at the ease of use of each of these products by performing a time and motion analysis for typical management tasks, and noted whether any additional elements were required to perform these tasks. Without any additional configuration, we tested each vendor's appliance "out of the box" for their security level of protection. Test results are detailed on the following pages and demonstrate a clear advantage for the Cisco ISA 550W solution in the five areas of focus for this study.

Testing included performance with all services enabled. Using test and measurement equipment, we objectively measured the throughput performance for each of the products in this study.

Cisco had an all-in-one functionality for security. One license supported all features and functionalities compared to the FortiGate-20C and SonicWALL TZ105.

We were pleased with the overall performance of the Cisco ISA550 Security Appliance in all tests. It is to be noted that the Cisco 550W Security Appliance proved particularly more effective at blocking malicious websites, including re-direct sites and those with drive-by installers compared to the competitive offerings.

Rob Smithers
CEO
Miercom

Copyright © 2013 Miercom

2.0 Key Findings

Cisco Small Business ISA500 Series Integrated Security Appliance is an all-in-one Internet access and security solution that combines highly secure Internet, wireless, site-to-site VPN, and remote access VPN with a range of Unified Threat Management (UTM) capabilities. These capabilities include firewall, email, web security, application control, IPS and Antivirus.

We found that the Cisco ISA550 proved better in testing in the following areas:

- Cisco ISA550 blocked 99.75% of malicious URLs, while Fortinet and SonicWALL blocked less than 25% of these URLs
- Cisco achieved a 93% block rate for antivirus attacks, while Fortinet blocked 62% and SonicWALL blocked 50%
- The Cisco Security Appliance solution attained 44 Mbps throughput with multiple security features enabled; Fortinet and SonicWALL achieved less than half that amount
- ISA550 had the quickest installation setup, requiring only 36 clicks for the initial setup, while Fortinet required 49 and SonicWALL required 66
- ISA550 offered easy and comprehensive out-of-box features to guide users to prep the device for deployment.

The ISA500 is an easy-to-use solution that can be setup and deployed quickly for a branch to mid size office. It leverages Cisco Security Intelligence Operations (SIO), which provides global threat intelligence to deliver advance threat protection. The ISA500 has comprehensive UTM security capabilities, easy-to-use design, and sophisticated threat intelligence that make it a superior security appliance.

Management of the appliance was clear and concise, requiring less time and fewer clicks to create/apply policies and to create reports than the competition. The ability to create customized reports is built into the unit and does not require the purchase of additional products.

The Cisco ISA500 Series utilizes a cloud-based approach to email and web security that minimizes management tasks and can enable responsive protection against new threats. This thorough inspection controls web access, reduces spam emails, and minimizes phishing attacks, unauthorized intrusions and other emerging threats.

ISA500 offers WAN redundancy that supports failover, load balancing and policy-based routing (PBR) to keep businesses running when failures occur due to either a failed Internet connection or a failure within an ISP itself.

Copyright © 2013 Miercom

3.0 Methodology

3.1 Systems Under Test

Testing was performed on the following systems:

- Cisco ISA550
  Integrated Security Appliance
  Version: 1.1.14
- SonicWALL TZ105
  SonicOS Enhanced 5.8.1.8-37o
- Fortinet FortiGate-20C
  Version: 4.0, build0639,120906 (MR3 Patch 10)

3.2 Test Bed Environment

See specific sections for the test bed configuration diagrams.

Copyright © 2013 Miercom

4.0 Deployability Assessment

The objective of this test was to evaluate how easy businesses can get the vendors' solutions up and running with effective security protections in place to protect their businesses. This is important as confusing or poorly organized product configuration interfaces can lead to incorrect or improper security settings and, bottom line, leave open security vulnerabilities. The device user interface and configuration flow play an important role to guide users to deploy the solution quickly, without error.

Specifically, we conducted the test by evaluating two areas:

1. Out-of-box features/tasks: how the vendors' solutions handle several key "out-of-box" tasks that can guide users to situate their security devices in an optimal state for deployment
2. Initial deployment: How easy one can use the vendor's GUI to configure the security appliance for Day 0 deployment

4.1 Out-of-box Features/Tasks

In this test, the features/tasks evaluated included the following:

- Prompt for software upgrade
- Forced default password change
- Installation of license
- Default ACLs and default attack protection

"Prompt for software upgrade" is selected as vendors are constantly improving their software to keep up with new and evolving threats. Having the ability to inform businesses about their new software for their security appliance helps businesses stay on the latest software with up-to-date patches and improvements to secure their businesses.

"Forced default password change" is selected as it is important for businesses to move away from a vendor's factory default password that can be literally known by everyone. This is also important as this feature can be required by some government regulations.

"Security services license installation" is evaluated because before a business can take full advantage of the security appliance to protect their company, they typically need to install and activate the license.

"Default ACL and attacks protections" is also evaluated, because as in a small office environment, a business may simply just plug-in-and-play the device on Day 1 and make security policy adjustments over time.

We measured how well vendors handled those features/tasks in terms of their availability and "coverage" concerning their meaningfulness in real-world deployment.

Copyright © 2013 Miercom

4.1.1 Findings

Figure 1: Out-of-Box Features Summary Table

	Cisco ISA550W	Fortinet FortiGate-20C	SonicWALL TZ105
Prompt for Software Upgrade	●	■	■
Forced Password Change	●	▲	▲
Installation of License	●	▲	▲
Default ACLs & Attack Protection	●	▲	●

Scoring Key:

● = Full coverage

▲ = Some utility or capabilities but not complete for real world deployment.

■ = No coverage

Prompt for Software Upgrade

Cisco ISA500 firmware upgrade is easy. The ISA500 Security Appliance provides an automatic new firmware notification feature. This feature prompts users with a notification when a newer firmware (newer than the local version) is detected. However, the notification can be improved with clearer messages to indicate the reason for failure.

SonicWALL and Fortinet products, on the other hand, do not provide the automatic new firmware notification feature, or indication of where to obtain a firmware upgrade, other than accessing their website and searching for the specific appliance.

Forced Password Change

The Cisco ISA500 Security Appliance prompts users to change the default factory password once they log into the device for the first time. This is required before the device can be further configured. This password handling prevents users from using publicly-known user names and passwords, which can lead to a security compromise.

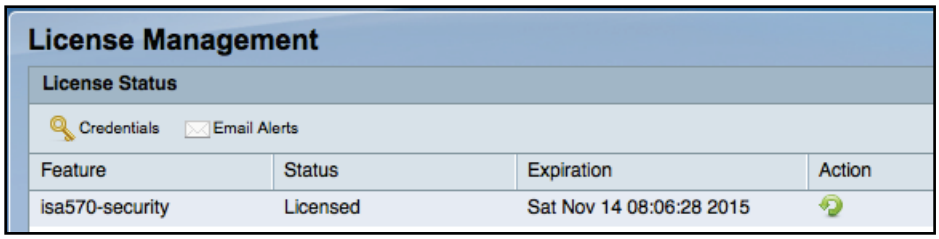
In our testing, we did not observe any prompts in the SonicWALL and Fortinet devices to users for changing usernames and/or passwords.

Copyright © 2013 Miercom

License Installation

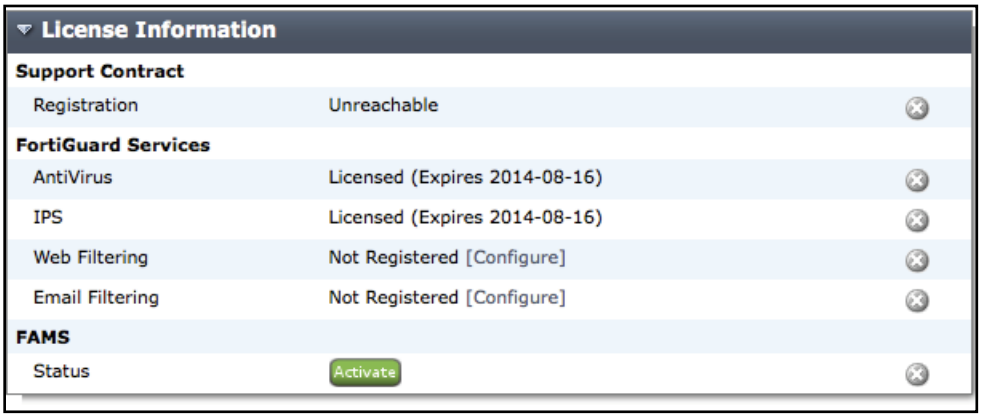
Cisco ISA500 Security Appliance - License installation is included in its Setup Wizard. Only one license needed to be installed for our testing.

Figure 2: Cisco License Management Screen



Fortinet FortiGate-20C - Limitless user licensing and a feature screen helped with deployment and maintenance.

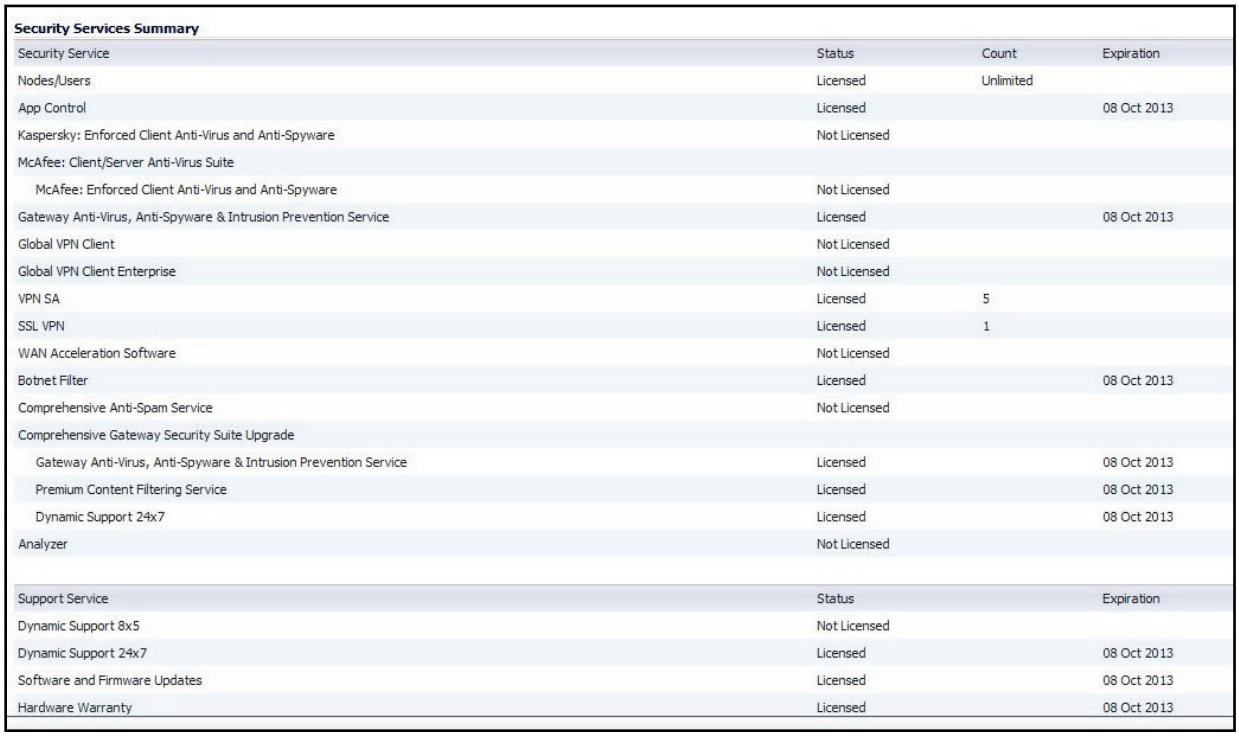
Figure 3: Fortinet License Information Screen



Copyright © 2013 Miercom

SonicWALL - Additional licenses were required for added features for testing. See *Figure 4* for a summary of the license options.

Figure 4: SonicWALL Licenses Service Summary



Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		08 Oct 2013
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
McAfee: Client/Server Anti-Virus Suite			
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		08 Oct 2013
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	5	
SSL VPN	Licensed	1	
WAN Acceleration Software	Not Licensed		
Botnet Filter	Licensed		08 Oct 2013
Comprehensive Anti-Spam Service	Not Licensed		
Comprehensive Gateway Security Suite Upgrade			
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		08 Oct 2013
Premium Content Filtering Service	Licensed		08 Oct 2013
Dynamic Support 24x7	Licensed		08 Oct 2013
Analyzer	Not Licensed		

Support Service	Status	Expiration
Dynamic Support 8x5	Not Licensed	
Dynamic Support 24x7	Licensed	08 Oct 2013
Software and Firmware Updates	Licensed	08 Oct 2013
Hardware Warranty	Licensed	08 Oct 2013

SonicWALL Security Services Summary interface shows the licensing status during initial set up of the appliance. Some added features require the purchase of additional licenses.

Copyright © 2013 Miercom

Default ACLs and Attacks

Figure 5: Default ACLs Detail

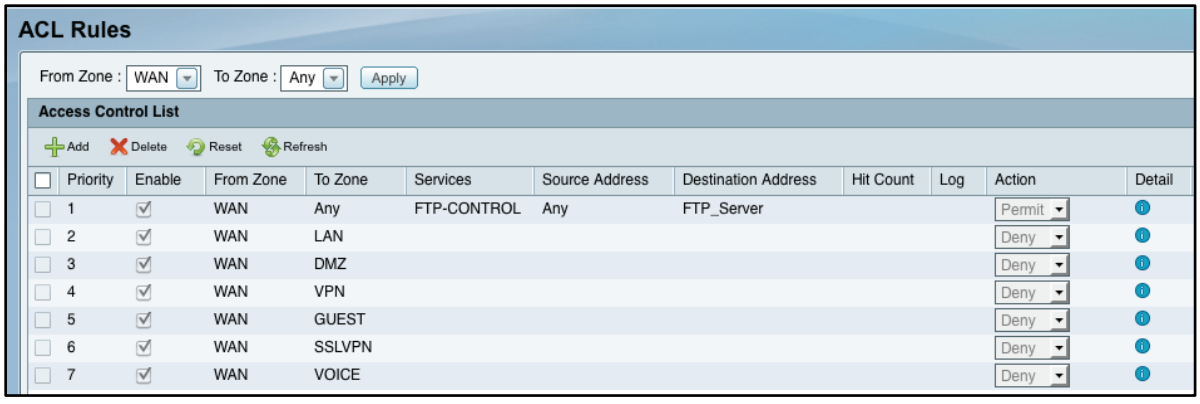
	Cisco ISA550	Fortinet FortiGate 20C	SonicWALL TZ105
Deny access from WAN to all internal zones	YES	YES	YES
Deny access from low security level factory default to higher or equal zones	YES	NO	NO
Enable security services for LAN, WAN, DMZ	YES	NO	YES

The firewall configuration for each product for the basic “Deny access from WAN to all internal zones” was activated. However, Cisco went beyond that to secure each LAN, WAN and DMZ. The configuration for the Cisco ISA550 was conducted using an easy-to-use setup wizard. We could efficiently configure DMZ address, services, LAN/WAN IP addresses, DHCP poll etc. Cisco allows for multiple ports to be configured in the ISA550W appliance:

- 1 WAN, 6 LAN
- 1 WAN, 1 DMZ, 5 LAN
- 1 WAN, 1 WAN backup, 5 LAN
- 1 WAN, 1 WAN backup, 1 DMZ, 4 LAN

Extra steps to configure these ports are required.

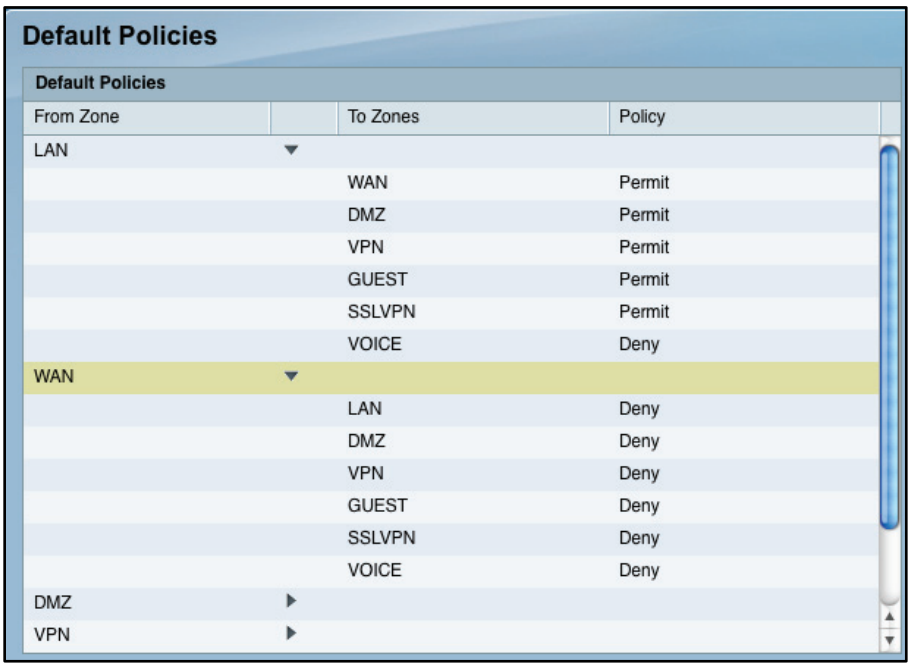
Figure 6: Cisco ISA550 ACL Rules



Cisco ISA550 provides a useful Configuration Wizard interface for configuring access control lists.

Copyright © 2013 Miercom

Figure 7: Cisco ISA550 Default Policies



The Cisco ISA550 WAN to LAN zone policy screen as configured in testing.

Copyright © 2013 Miercom

Figure 8: Default Attack Settings

Blocked	Cisco ISA550	Fortinet FortiGate-20C	SonicWALL TZ105
Ping WAN Interface	YES	YES	YES
Port Scan (Stealth Mode)	YES	NO	NO
TCP flood, TCP SYN	YES	YES	YES
UDP Flood	YES	NO	NO
Echo Storm/ICMP Flood	YES	NO	NO
ICMP Notifications	YES	NO	NO
Multicast Packets	YES	NO	YES
Max Segment Life Check	NO	NO	YES
Enable TCP Handshake Timeout	NO	NO	YES
Block Echo Storm	YES	NO	NO
ICMP Flood	YES	NO	NO

Cisco ISA550's default attack setup offered the most protection compared to all the products tested. If it was required to unblock any protocol, this could be accomplished with several clicks and the intuitive dashboard. From the same screen, we could also specify the zones and/or range that should be blocked. This feature makes this utility granular and easy even for a beginner administrator to use.

Copyright © 2013 Miercom

4.2 Initial Deployment

This test will determine the number of clicks it required to manually configure all security features by a new user on Day 0 for a small business network. These configurations include:

1) Change default admin account
2) System time
3) Set up remote management
4) Configure primary WAN, LAN
5) Configure security services: IPS, AV, web security
6) Configure load balancing/failover
7) Upgrade to the latest software

Measurements were logged for the amount of time and number of steps required to perform common management tasks. Evaluation was based on factoring in the amount of time to complete a specific task; the number of steps (clicks) and the number of different screens or pages accessed, the number of sub-menus or individual elements within a screen that are used to complete the task, and the security that the device provided.

Copyright © 2013 Miercom

4.2.2 Findings

Figure 9: Clicks for Initial Security Setup

Number of Clicks			
	Cisco ISA500	**SonicWALL TZ105**	**Fortinet FortiGate-20C**
Wizard	36	21	27
License		7	8
Security:		33	
Web			6
IPS enable		7	
AV		3	
WEB			
Black list		6	
Anti spyware		3	
Web threat		8	6
Failover		6	
Software Upgrade		5	4
Remote Management			4
Total Clicks	36	66	49

Copyright © 2013 Miercom

All of the initial setup for Cisco is performed in the Wizard Configuration. This feature sets up all the initial requirements using default parameters. Once the initial setup is completed, no other configuration is required unless a customizable security setup is needed.

Although SonicWALL's and Fortinet's products had Wizard configurations for initial setup, they did not include as many items as Cisco. Therefore, additional set ups were required to implement and complete initial security setup. This requires us to move around configuration GUI, go to different configuration sections, and figure out their relationship and configuration logics. This took more time to set up the devices and appears error-prone.

Summary & Other Findings

We found the initial setup easy to accomplish for the Cisco ISA500 Security Appliance. It provides a nice out-of-box feature to guide users to prepare for initial deployment. A deployment can be done quickly and without spending too much time in learning the device configuration logics and flows. Among all three vendors, Cisco had fewer clicks than Fortinet and SonicWALL in total for initial configuration. We found the SonicWALL initial configuration to be the most complex compared to Cisco and Fortinet.

In addition to supporting management and monitoring, the Cisco ISA500 Configuration Utility provides security and network usage reports for administrators to quickly review security activities and network operation status.

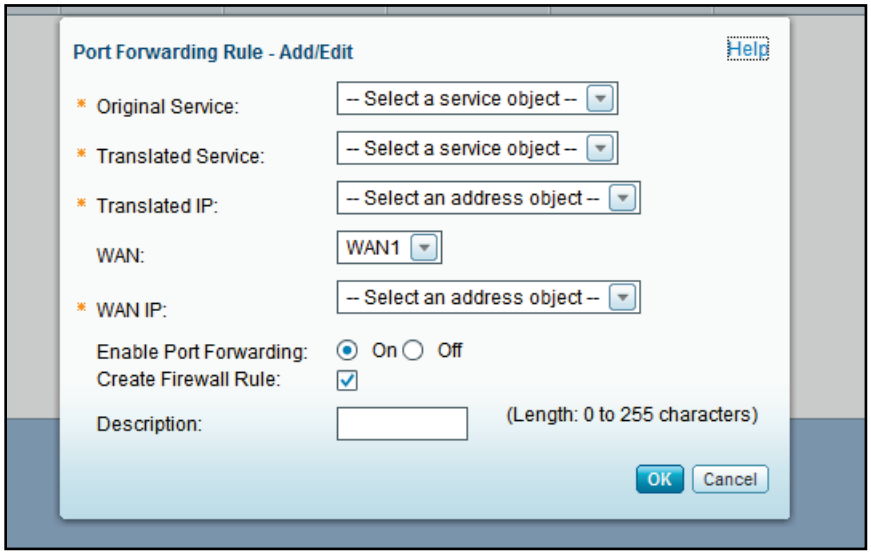
Cisco's dashboard and configuration utility was straight forward and easy to use with drop-down menus and well organized, intuitive options to select. The utility provided a list of options which included Networking, Wireless, Firewall, Security Services, VPN, Users and Device Management. These options were shown on the left side, each one providing a drop-down menu. To the right side of the screen is the configuration/data screen which is self explanatory when configuring.

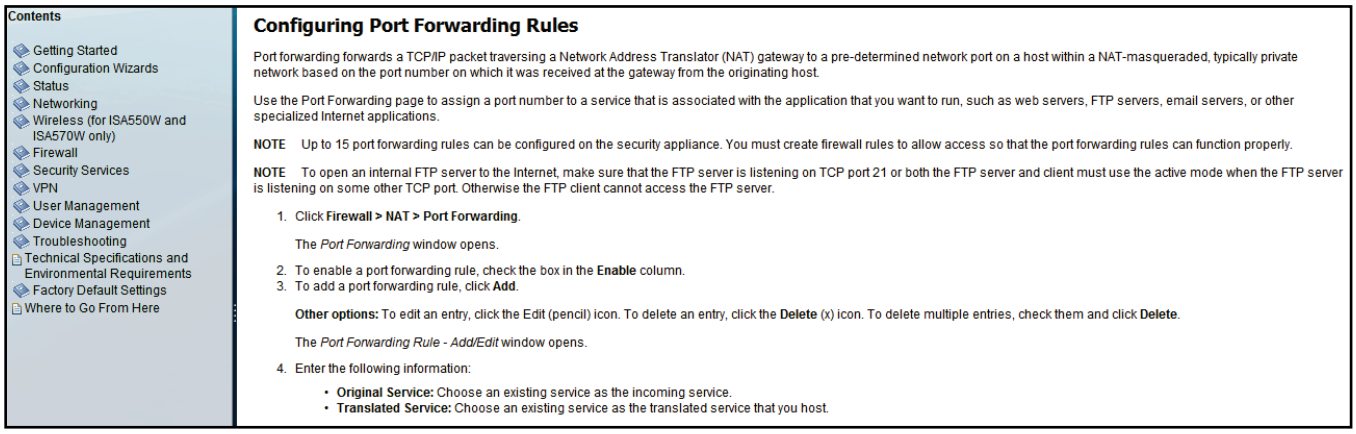
When configuring certain security functions and/or protocols, such as port mirroring, a help button was available on the configuration screen. When clicked, this help function brought the user directly to the location in question (see *Figure 10* on the next page).

Another ease of use and convenience advantage of the Cisco ISA500 is that the security license need not be reinstalled after a factory reset. Both Fortinet's and SonicWALL's licenses needed to be reinstalled when we performed a factory default reset.

Copyright © 2013 Miercom

Figure 10: Cisco Help





Contents

- Getting Started
- Configuration Wizards
- Status
- Networking
- Wireless (for ISA550W and ISA570W only)
- Firewall
- Security Services
- VPN
- User Management
- Device Management
- Troubleshooting
- Technical Specifications and Environmental Requirements
- Factory Default Settings
- Where to Go From Here

Configuring Port Forwarding Rules

Port forwarding forwards a TCP/IP packet traversing a Network Address Translator (NAT) gateway to a pre-determined network port on a host within a NAT-masqueraded, typically private network based on the port number on which it was received at the gateway from the originating host.

Use the Port Forwarding page to assign a port number to a service that is associated with the application that you want to run, such as web servers, FTP servers, email servers, or other specialized Internet applications.

NOTE Up to 15 port forwarding rules can be configured on the security appliance. You must create firewall rules to allow access so that the port forwarding rules can function properly.

NOTE To open an internal FTP server to the Internet, make sure that the FTP server is listening on TCP port 21 or both the FTP server and client must use the active mode when the FTP server is listening on some other TCP port. Otherwise the FTP client cannot access the FTP server.

1. Click **Firewall > NAT > Port Forwarding**.

   The *Port Forwarding* window opens.

2. To enable a port forwarding rule, check the box in the **Enable** column.
3. To add a port forwarding rule, click **Add**.

   Other options: To edit an entry, click the Edit (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

   The *Port Forwarding Rule - Add/Edit* window opens.

4. Enter the following information:
   - **Original Service:** Choose an existing service as the incoming service.
   - **Translated Service:** Choose an existing service as the translated service that you host.

Easily understandable help for Port Forwarding Rules is available for use when setting up the appliance.

Copyright © 2013 Miercom

5.0 Performance with Services Enabled

Testing focused on both the effectiveness of the UTM appliance, as well as performance throughput. The tests were designed to stress the filtering capabilities of the appliances and determine how these countermeasures impacted network throughput. Security effectiveness and different capabilities assessments were conducted and the throughput for each assessment logged.

The Avalanche and Spirent/Mu Dynamics were used as attack test servers against Cisco, Fortinet and SonicWALL UTM appliances to test their ability to protect a network from threats with published signatures. For each security feature that was enabled, a test was conducted to verify that the throughput maintained high percentages.

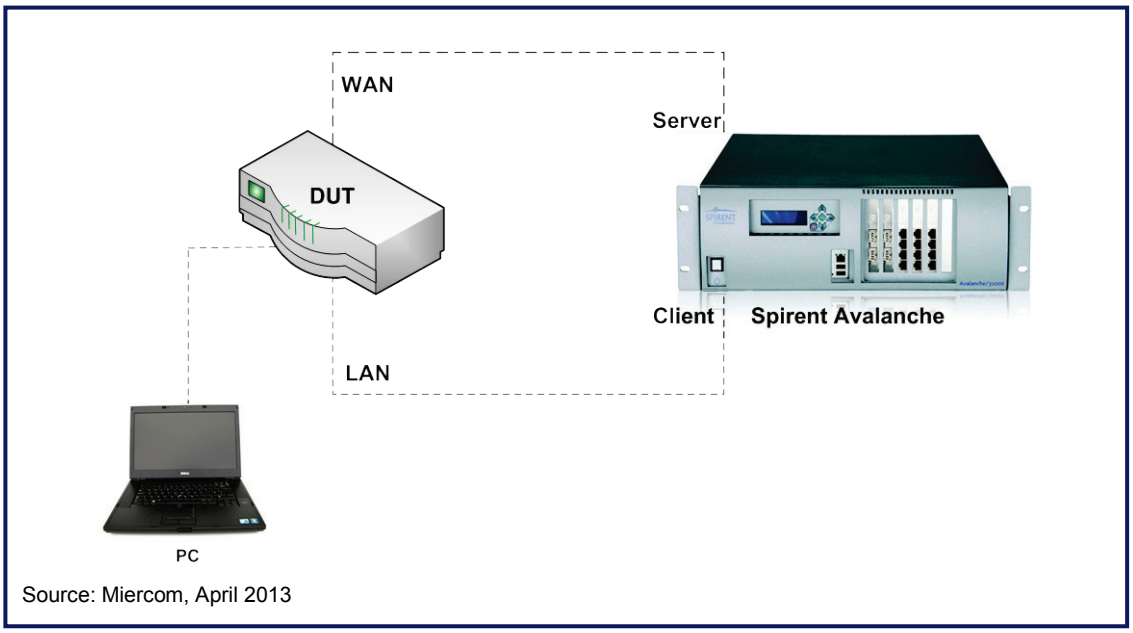
Tests were conducted for:

1. Firewall with IPS and application control services enabled
2. Firewall with Antivirus services enabled
3. Firewall with IPS, Application Control, and Antivirus services enabled
4. Firewall with IPS, Application Control, Antivirus services and Web URL filtering enabled

Copyright © 2013 Miercom

5.1 Performance Throughput Testing

Figure 11: Topology for Performance Throughput



Source: Miercom, April 2013

Spirent Avalanche was used to test the performance and throughput of each product. The configuration used data that could be passed through, such as EMIX. See *Figure 12* on the following page.

To determine the accuracy of performance throughput, logging and monitoring all Devices Under Test (DUTs) were disabled. In the firewall, the advanced settings were set with either "syn flood" detection being disabled or “allowed concurrent” connections increased. The default settings were used for IPS filtering for each of the products tested.

Copyright © 2013 Miercom

Figure 12: Traffic Profile

Protocol	Bandwidth Percentage
HTTP	44
FTP	9
Bittorrent (Sapee)	22
SMTP	8
IMAP	17

EMIX traffic with bandwidth distribution

The table shows the EMIX mode settings that were used. EMIX traffic profile is used in the industry to simulate real-world traffic patterns and packet distributions.

5.2 Results

Figure 13: Security Features and Throughput per Mbps

Enabled Protocol	Cisco ISA550W	SonicWALL TZ105	Fortinet FortiGate-20C	
			Proxy Mode	Flow Mode
FW, IPS, APP	73.7 Mbps	32.0 Mbps	25.7 Mbps	25.7 Mbps
FW, AV	85.7 Mbps	69.0 Mbps	42.4 Mbps	95 Mbps
FW, IPS, APP, AV	52.0 Mbps	32.0 Mbps	12 Mbps	25 Mbps
FW, IPS, APP, AV, Web URL	44.0 Mbps	12.5 Mbps	10 Mbps	22 Mbps

- FW = Firewall
- AV = Antivirus
- IPS = Intrusion Protection System
- URL = Uniform Resource Locator
- APP = Application Control

For the performance test, similar configurations were used for all three products. We disabled logging and onboard reporting, and used the default settings for IPS, application control and Web URL filtering. The same set of protocols was enabled for antivirus protection.

Copyright © 2013 Miercom

6.0 Gateway Antivirus Protection

Gateway antivirus technology uses up-to-date data feeds to protect your internal network resources from the most wide spread and active virus attacks to the Internet gateway. It also integrates a high performance Real-time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious viruses.

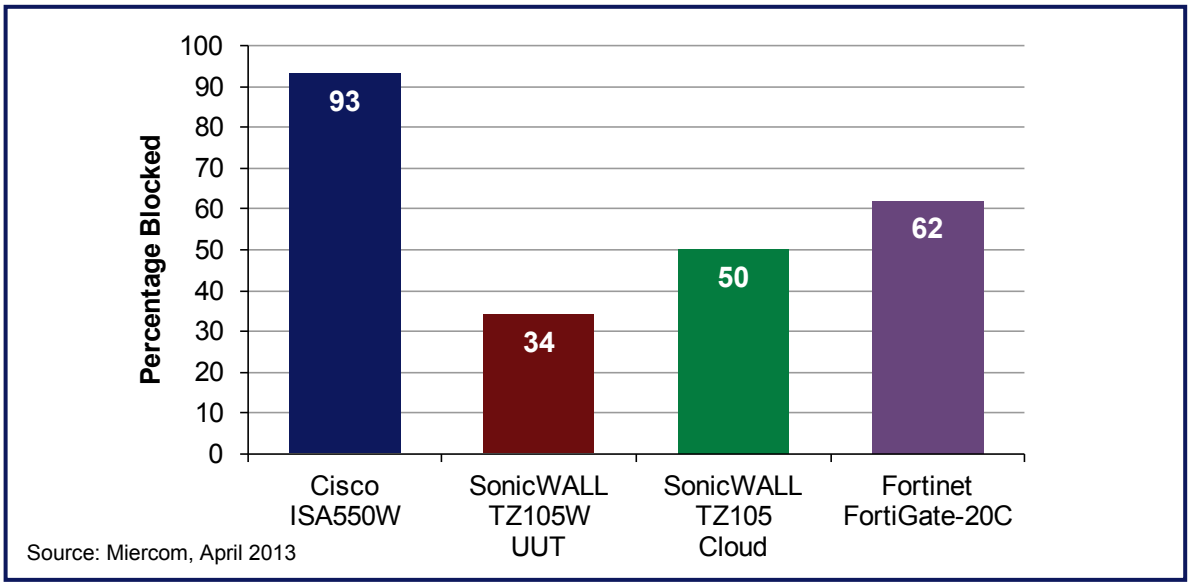
The tests in this section are designed to determine the effectiveness of the appliances by gauging the detection rate of the most recent virus threats in the wild. We determined which products used the best technology by detecting "zero day" virus samples. The script consisted of the most lethal viruses, using samples such as botnets, payloads, and exploits. Each DUT was configured so that antivirus protection was enabled.

In this test, we used 100 virus signatures to test the vendor's antivirus security services. Those signatures consisted of top wild active viruses. With this virus sample, it allowed us to evaluate how well the vendors' solutions were in preventing a Zero Day virus.

6.1 Results

Out of the 100 samples, Cisco led with a 93% block rate while Fortinet blocked 62% with the proxy server. SonicWALL blocked an average of 50%. For SonicWALL, testing was done using the cloud and the appliance together. This allowed for higher than average blocking to occur.

Figure 14: Percentage Blocked for Antivirus



UTM competitive gateway antivirus block rates for the top 100 in the wild, active virus samples as of April 2013.

Copyright © 2013 Miercom

7.0 Application Control

Application Control objectives relate to the confidentiality, integrity, availability of data and the overall management of any size business. The main emphasis for Application Control is geared toward managing access to Web 2.0 applications/sites that even small businesses need to consider to maintain employee productivity.

An application control policy allows you to permit or block traffic for the applications by schedule. These applications include Instant Messaging, Games, Streaming Media and Social Networks.

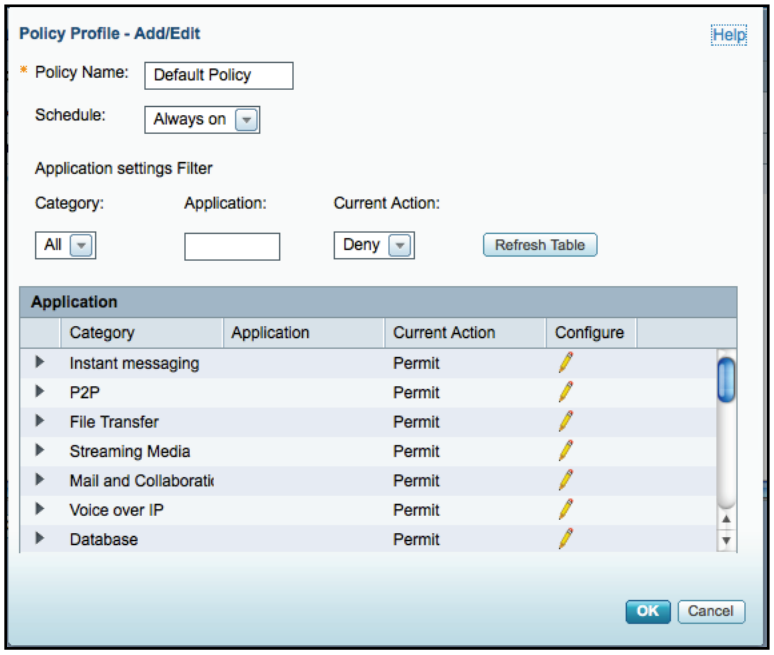
The purpose of this test was to discover the percentage of sites that are blocked. A mix of sites used included Facebook, LinkedIn, Skype and many others. All three appliances were configured to block social networking sites and subordinate daughter pages of social networking sites. A URL script with social networking sites ran and the percentage of blocked sites was recorded.

7.1 Findings

Cisco ISA500 Application Control surpassed the other vendors. Its interface has very granular configuration capabilities. It allows users to either permit or deny a list of sites in that category. The exact social networking site components can be set to either permit or deny. In addition, Cisco ISA500 allows a system administrator to determine what internal zone or IP address should allow or deny access. This is useful since some users, such as executives and/or Human Resource departments, may need the ability to access certain sites, such as LinkedIn.

These databases can be updated either manually or automatically, which can be scheduled.

Figure 15: Application Control for Social Networking Cisco ISA500



Copyright © 2013 Miercom

In terms of efficacy, the Cisco ISA500 could block the most social networking sites and daughter pages of social networking sites – Cisco blocks at 65%. SonicWALL followed at 40% and Fortinet blocked 31%. The result is captured in *Figure 16*. This indicates that Cisco ISA500 has the most accurate application category among the tested vendors.

Figure 16: Social Networking Sites and Daughter Pages Blocked

	Cisco ISA550W	SonicWALL TZ105	Fortinet FortiGate-20C
Percentage Blocked	65%	40%	31%

Copyright © 2013 Miercom

8.0 Web Reputation

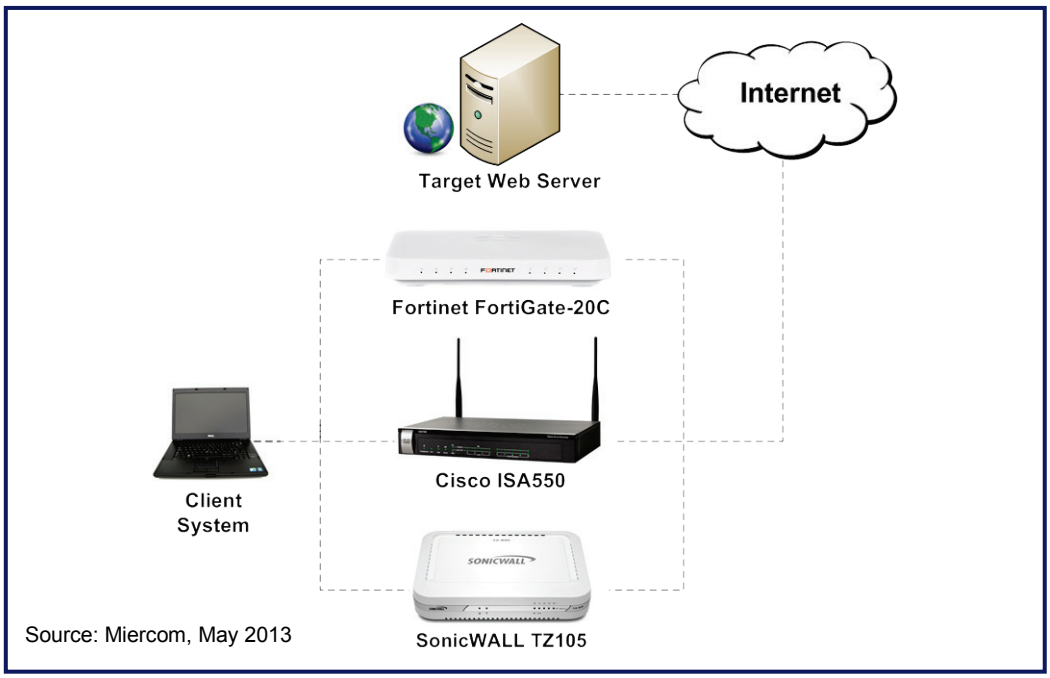
Reputation-based web filtering protects employees from accidently accessing dangerous web sites that may contain virus, phishing links, or other types of malware. This control ability helps businesses minimize web-based security threats, reduce employee downtime, and improve business productivity. This test evaluates how well the tested vendors' solutions can effectively achieve those business benefits.

8.1 Test Setup

The test contained a sample URL list that included approximately 4,200 URLs. For each vendor's appliance, only the Web Reputation was enabled. The script ran via a python program and the percentage of blocked URLs was recorded. The main emphasis for this Web Reputation testing was on the number of blocked URLs, and to a lesser degree, the number of re-directs.

A proxy server was used in the testing to allow "unreachable" URL destinations to also be checked for reputation. Some malicious websites sporadically hide themselves to avoid detection, therefore it is important to check the reputation of these URL destinations, even if the site is unreachable at that time.

Figure 17: Topology for Testing Web Reputation

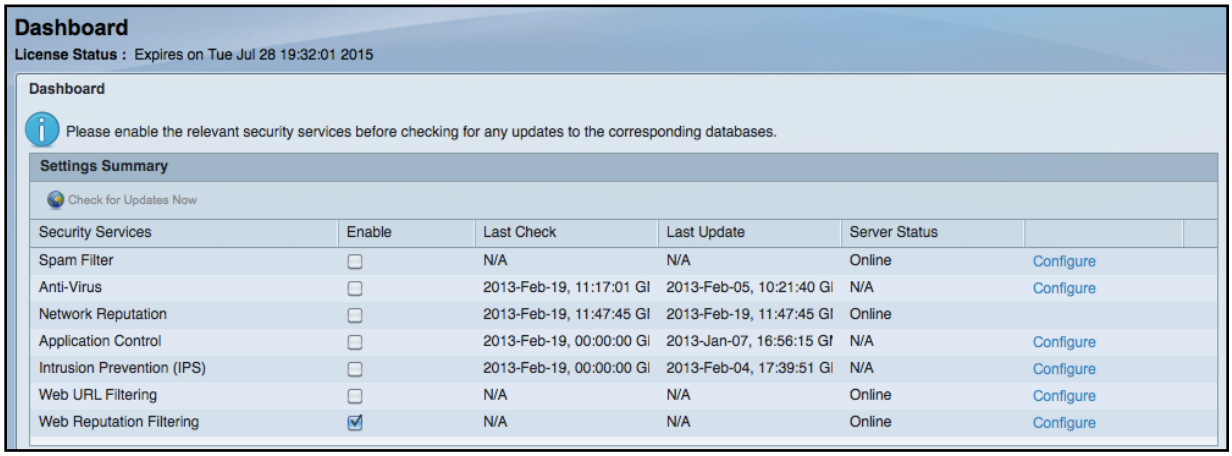


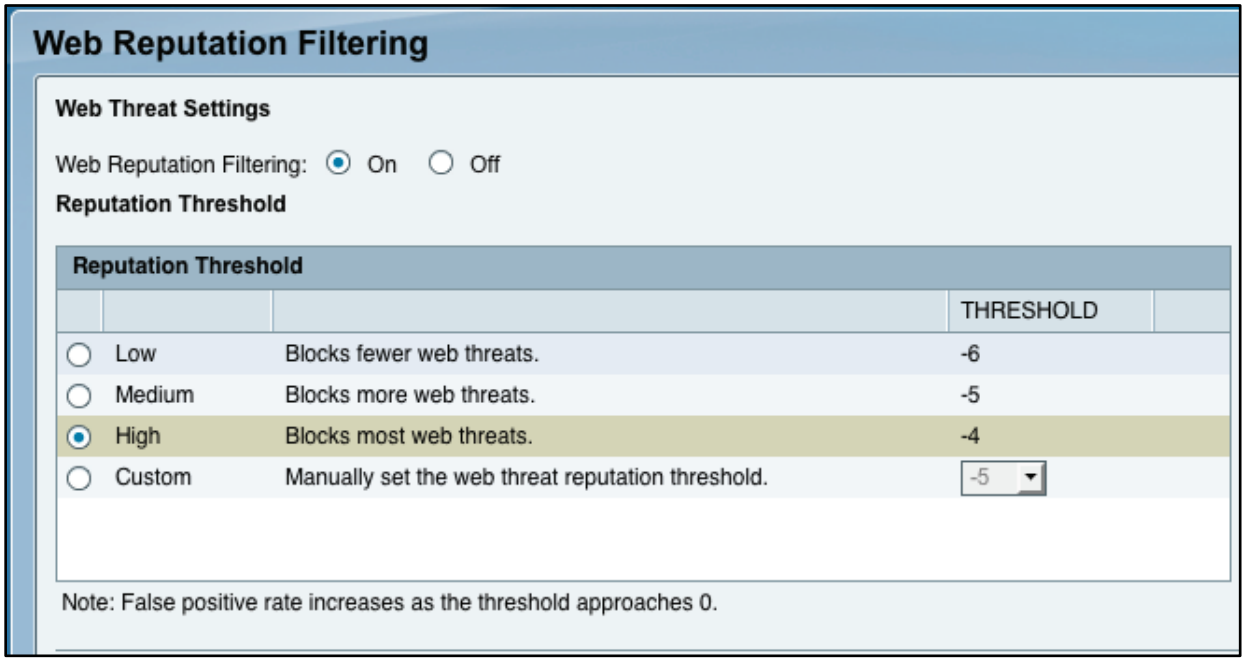
Test scripts were run, sending HTTP "GET" requests to the target Web server through the Web gateway. The client system then waited for a response code to be returned. Instead of using a public proxy, a simple web server was used. This web server is used to help set up the TCP handshake so that the client PC can send out a HTTP GET Uniform Resource Locator (URL). At this point, the Units Under Test (UUT) can query the URL rating, then decide to allow or block the HTTP connection. The response code determined whether the URL was blocked or not and the appropriate category was then determined and logged. Management of the appliance was also done through the client system.

Copyright © 2013 Miercom

Cisco's ISA550W Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware or phishing links. Web Reputation Filtering detects the web threats based on the reputation score of a web page. Its reputation scores range from -10 (bad) to +10 (good). Web pages with reputation scores below a specific threshold are considered threats and are blocked. In our test, we enabled the Web reputation filtering with its highest protection option. See *Figure 18*.

Figure 18: ISA550W Web Reputation Filtering Enabled



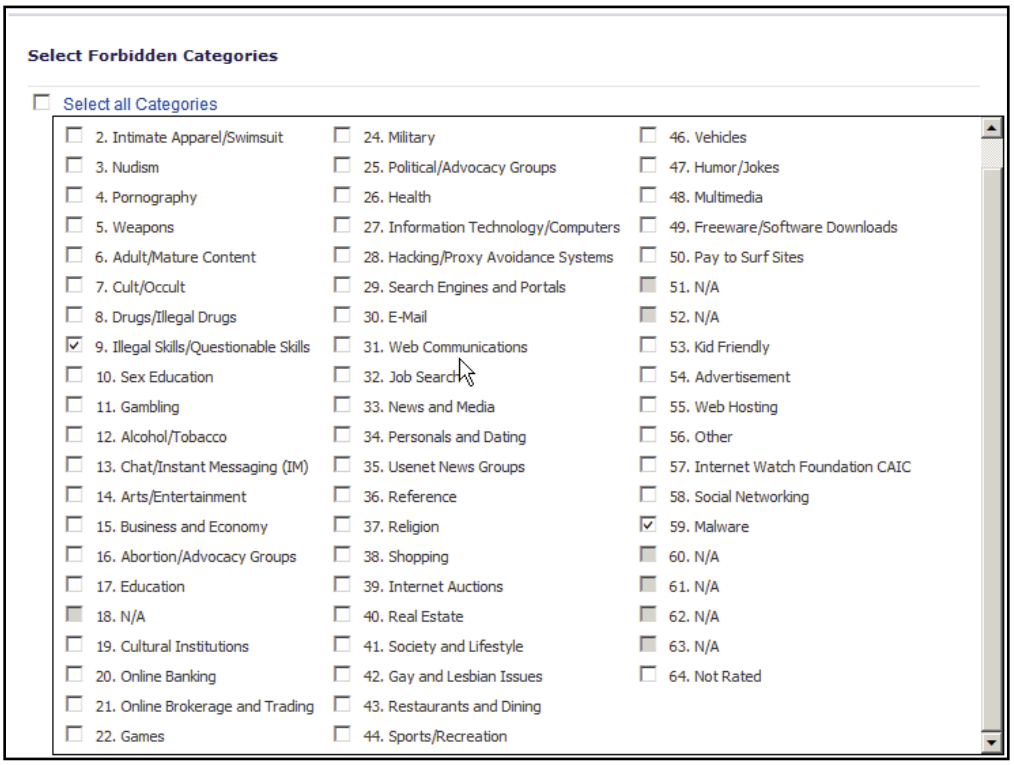


The configuration for the Cisco ISA500 provides a +10 to -10 range for a more granular level for the Web Reputation filtering threshold.

Copyright © 2013 Miercom

For the SonicWALL TZ105 interface, the content filtering setting was configured with malware blocking enabled. A total of 64 categories can be selected for the Web Reputation Filtering.

Figure 19: SonicWALL – Malware Blocking Enabled



SonicWALL TZ105 has 64 categories for URL filtering (shown above) in the interface for configuring "forbidden categories."

Copyright © 2013 Miercom

For the Fortinet device, we used its web filtering for the test. The inspection mode was set to Proxy enabled and all categories were also enabled. HTTPS scanning was turned on with the exemption of Banking, Healthcare and Personal Privacy.

Figure 20: Fortinet – Web Filtering for Security

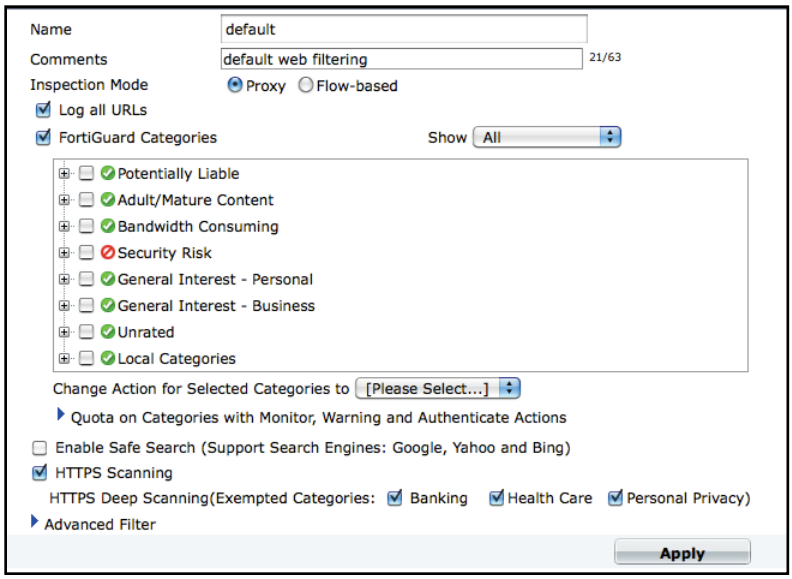
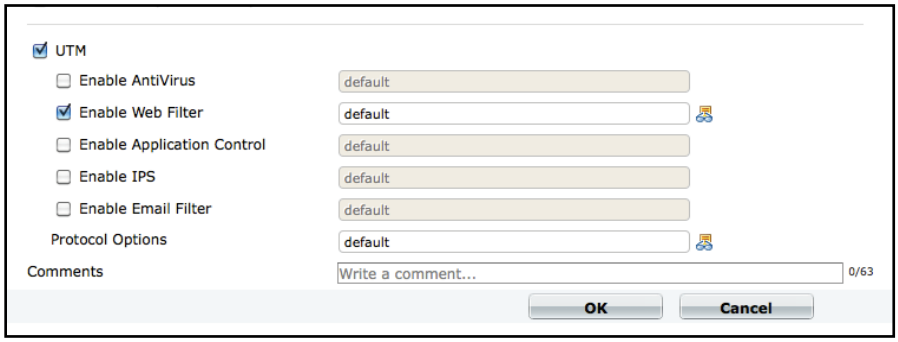


Figure 21: Fortinet – Bind Policy



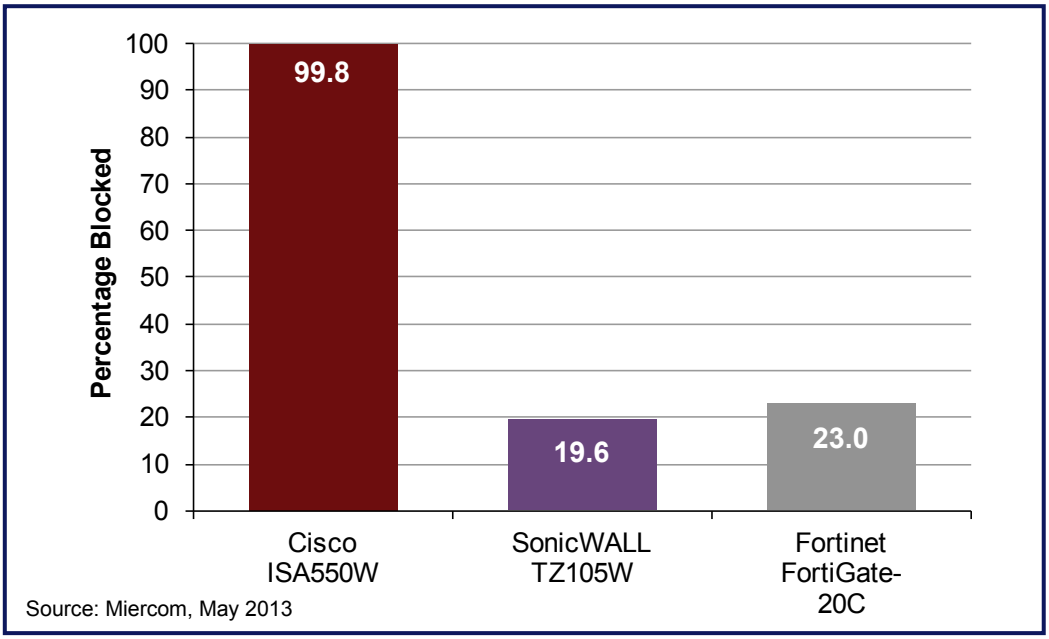
Copyright © 2013 Miercom

8.2 Results

The blocked percentage of dangerous URLs by the Cisco ISA500 far exceeded the competitors, SonicWALL and Fortinet.

We found that the Cisco ISA550W blocked 99.75% of the bad URLs, the SonicWALL TZ105 blocked 19.56% and the Fortinet FortiGate-20C blocked 23.04%.

Figure 22: Percentage of Malicious URLs Blocked

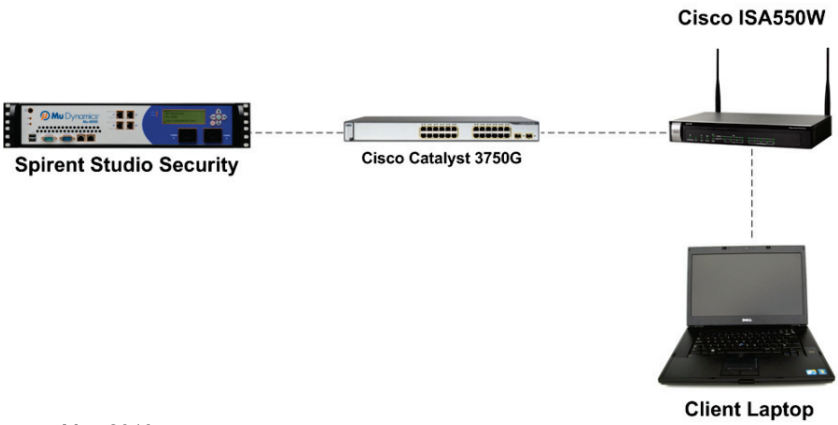


Copyright © 2013 Miercom

Appendix

DoS Attacks

Figure A-1: Topology used for the DoS Attacks



Source: Miercom, May 2013

The Spirent MU Dynamics 4000 with DoS attack and protocol mutation test contained cases for IPv4 datagrams that carry data for higher-layer protocols across a physical network link. An IPv4 datagram contains a header and data payload information.

The header contains the source and destination IPv4 address of the datagram, fragmentation information, a checksum used for data integrity, and other information. Payload carries the message data received from the higher-layer protocol.

One of DoS attacks that was used is the ping-of-death. The ping-of-death datagram, which has a total length of 65,535 bytes and exceeds the maximum IP packet size supported by most devices (normal pings are 64 bytes). Fragments in a ping-of-death datagram sequence have increasing Fragment Offset values that approach 65,535.

Attackers can fragment this malicious, oversized datagram to bypass security checks along the source-destination path or at the destination itself. When verified by a firewall or IDS, each fragment is seemingly benign and innocuous. However, when the destination IP layer reassembles the fragments into the original datagram, the total length of the datagram exceeds the maximum packet size of 65,536, causing a buffer overflow followed by a system crash.

We ran a test on Cisco's appliances, only allowing ping to be enabled. Mutated traffic tests ran at the interfaces and through the interfaces of the DUTs to an end point laptop. Network / CPU utilizations should maintain normal operating values and the laptop remain accessible throughout the course of the testing.

Copyright © 2013 Miercom

When running the DoS attack through the Cisco ISA550W appliance to the laptop, no deterioration in performance was experienced, nor were any spikes detected in the performance or network manager. The settings that were in place on the ISA550W were:

- Antivirus – on for http, ftp, smtp, pop3, imap, netbios
- IPS – on for WAN zone
- Web Reputation – on low -8 threshold
- Routing Mode – on
- Firewall – WAN to WAN - any - any - any - deny

  WAN to LAN - Mu Test - any - any - permit

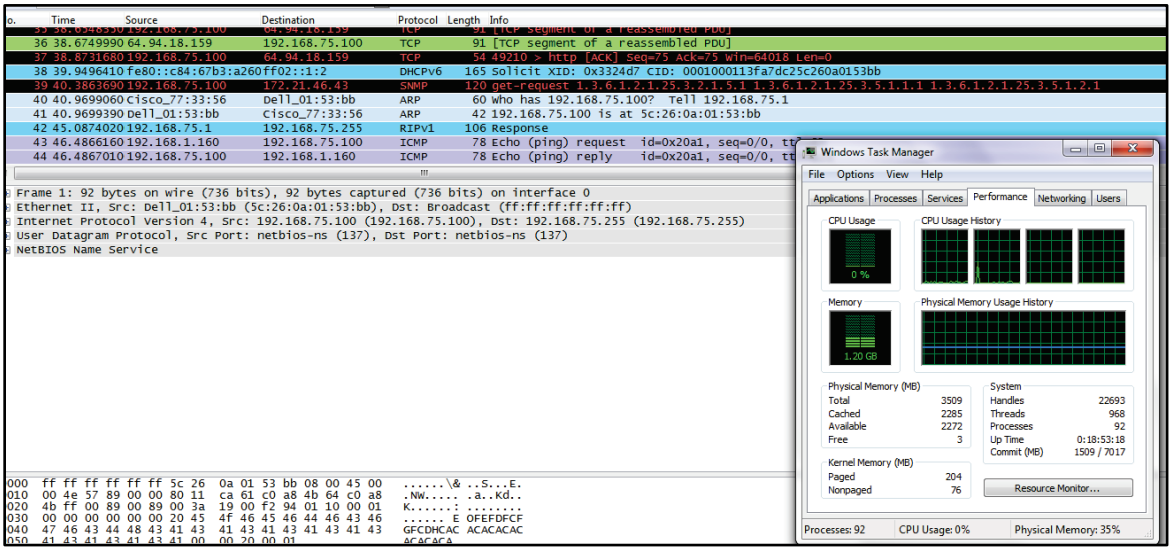
  - Mu Test – ICMP destination unreachable

    ICMP ping reply

    ICMP ping request
  - Attack Protection: Block Ping WAN Interface -- off

Figure A-2: DoS Attack Results

Cisco Screenshot of the End-Point Laptop



Both Wireshark and Task Manager were running while the DoS attack was taking place. No spikes were reported in the Task Manager. The executive summary of the Spirent/Mu Dynamics gives the ISA550W 5-9's as shown on the following page.

Copyright © 2013 Miercom

Figure A-3: ISA550 DoS Attack Summary

Executive Summary Report: ISA DoS Attack

Mu System User	admin
Start Date/Time	2/15/13 10:08:27 AM
Duration	1 minute 6 seconds 663 milliseconds

Product	Mu Test Suite (6.5.1.r48259)
Mu System IP	172.21.46.78
Mu System Serial #	0104-0100-0000-00D9

Denial-of-Service (DoS) Results

(default) IP DoS Protocol

A+
100%
> Five 9's

In this Denial-of-Service (DoS), the target was tested with a maximum packet rate of **100,000** for a duration of 1 minute 757 milliseconds . The target was **unavailable** for a total of **0 milliseconds (0%)** and was **available for 1 minute 757 milliseconds (100%)** of the time.

Duration	PPS at Failure	Recovery	Availability
1 minute 757 milliseconds	0	Recovered within 1 minute	100.000%

Results

Cisco ISA550W stopped all DoS attacks by using their default setting “out of the box” configuration. No other protection or configuration was required. When we ran attacks from Spirent/Mu Dynamics through the ISA550W to the laptop (target), no signs of the attack appeared. A recording of a baseline on the metrics of the laptop was taken prior to the attack, and then the metrics were recorded after the attack was performed. The recordings showed that all logs and activities maintained normal operation on the laptop during the attack.

However, the ISA550W managing interface became unavailable during the attack. The CPU utilization did spike to 100%. This occurred both when the attack was either directed through the ISA or at it. Although as mentioned previously, ping needed to be allowed in order for the test to take place. In addition, the units that the ISA was protecting were not affected by the attack.

This test was not run on Fortinet or SonicWALL.

Copyright © 2013 Miercom