NETWORK FIREWALL PRODUCT ANALYSIS

Fortinet 800c FortiOS v4.3.8 build632

2012

1 Introduction

Firewall technology is one of the largest and most mature security markets. Firewalls have undergone several stages of development, from early packet filtering and circuit relay firewalls to application layer (proxy based) and dynamic packet filtering firewalls. Throughout their history, however, the goal has been to enforce an access control policy between two networks, and thus should be viewed as an implementation of policy. A firewall is a mechanism used to protect a trusted network from an untrusted network, while allowing authorized communications to pass from one side to the other, thus facilitating secure business use of the Internet.

In order to establish a secure perimeter, a basic network firewall must provide granular control based upon the source and destination IP Addresses and ports at a minimum. Next Generation Firewalls (NGFW) will extend this to provide additional control based on application and user/group ID, but are not within the scope of this report. As firewalls will be deployed at critical points in the network, the stability and reliability of a firewall is imperative. In addition, it must not degrade network performance or it will never be installed.

The firewall market is mature, populated with established vendors and providing limited scope for true innovation. Cost and capabilities, together with ability to integrate with the established security and network infrastructure, become the drivers for final product selection by customers. NSS Labs' test reports are designed to address the challenges faced by IT professionals in selecting and managing security products. The scope of this report is focused on:

- Security effectiveness
- Performance
- Management
- Total cost of ownership (TCO)

Table of Contents

Table of Figures

2 Summary Results

NSS Labs performed an independent test of the Fortinet 800c FortiOS v4.3.8 build632 firewall. The product was subjected to thorough testing at the NSS Labs facility in Austin, Texas, based on the network firewall methodology v4.0 available on www.nsslabs.com. This test was conducted free of charge and NSS Labs did not receive any compensation in return for Fortinet's participation.

While the companion Network Firewall Comparative Analysis Reports (CAR) on security, performance, management, and total cost of ownership (TCO) will provide comparative information about all tested products, this individual Product Analysis Report (PAR) provides detailed information not available elsewhere.

As part of this test, **Fortinet** submitted the **800c FortiOS v4.3.8 build632.**

Product	Overall Protection	Throughput
Fortinet 800c FortiOS v4.3.8 build632	100%	9,667 Mbps
Stability & Reliability	Firewall Enforcement	Security Effectiveness
100%	100%	100%

Fortinet 800c FortiOS v4.3.8 build632 was able to withstand our stability test and remain functional throughout the test. The Fortinet 800c is a robust and stable firewall.

The product successfully was rated by NSS Labs at 9.6 Gbps. NSS Labs rates throughput based upon an average of the results from tests: "Real World" Protocol Mix (Perimeter), "Real World" Protocol Mix (Core), and 21 KB HTTP Response.

Fortinet's web management interface for the 800c is intuitive and easy to navigate, making it ideal for small to medium environments. Users are presented with a configurable dashboard, and the CPU and memory meters are easy to read. Administrators can add a library of widgets, and it is possible to create custom widgets. Logging is granular, and filters can be constructed with ease. Logs can be stored locally (up to 1GB), and they may be offloaded to a Syslog server, Fortinet's hosted storage system, or Fortinet's proprietary and encrypted logging solution, FortiAnalyzer, though the last two options are separate purchases from the 800c. The alternative method for management of the 800c is the command line interface (CLI). The CLI is accessible via the web browser interface or via SSH from a workstation, and this interface provides more configurable options and capabilities to the administrator than the web interface alone. To manage multiple nodes centrally, FortiManager, Fortinet's centralized management server solution, is required.

The Fortinet 800c FortiOS v4.3.8 build632 as tested is suited to smaller SMB deployments where there may be no dedicated support available.

Enterprises and larger distributed deployments will require FortiManager and FortiAnalyzer for centralized management and logging of multiple nodes simultaneously.

3 Security Effectiveness

This section verifies that the device under test (DUT) is capable of enforcing a specified security policy effectively. NSS Labs' firewall testing is conducted by incrementally building upon a baseline configuration (simple routing with no policy restrictions and no content inspection) to a complex real world multiple zone configuration supporting many addressing modes, policies, applications, and inspection engines.

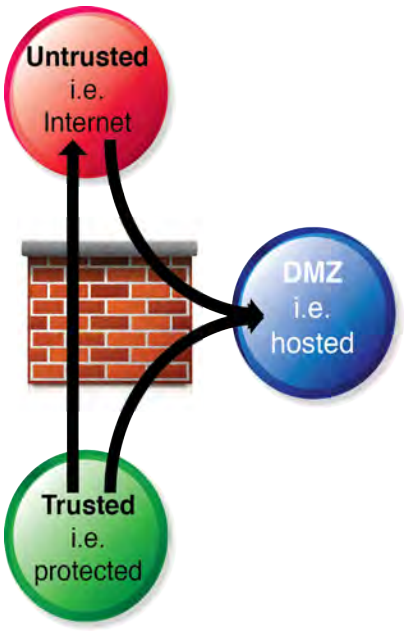
With each new security policy, test traffic is passed across the DUT to ensure that only specified traffic is allowed and the rest is denied, and that appropriate log entries are recorded.

The DUT must support stateful firewalling either by managing state tables to prevent "traffic leakage" or as a stateful proxy. The ability to manage firewall policy across multiple interfaces/zones is a required function. At a minimum, the DUT must provide a "trusted" internal interface, an "untrusted" external/Internet interface, and one or more DMZ interfaces. In addition, a dedicated management interface is preferred.

3.1 Firewall Policy Enforcement

Policies are rules that are configured on a firewall to permit or deny access from one network resource to another based on identifying criteria such as: source, destination, and service. A term typically used to define the demarcation point of a network where policy is applied is a *demilitarized zone* (DMZ). Policies are typically written to permit or deny network traffic from one or more of the following zones:

- **Untrusted –** This is typically an external network and is considered to be an unknown and non-secure. An example of an untrusted network would be the Internet.
- **DMZ –** This is a network that is being *isolated* by the firewall restricting network traffic to and from hosts contained within the isolated network.
- **Trusted –** This is typically an internal network; a network that is considered secure and protected.



The NSS Labs firewall tests verify performance and the ability to enforce policy between the following:

- Trusted to Untrusted
- Untrusted to DMZ
- Trusted to DMZ

Note: Firewalls must provide at a minimum one DMZ interface in order to provide a DMZ or "transition point" between untrusted and trusted networks.

Test ID	Test Procedure	Result
3.1.1	Baseline Policy	PASS
3.1.2	Simple Policy	PASS
3.1.3	Complex Policy	PASS
3.1.4	Static NAT	PASS
3.1.5	Dynamic / Hide NAT	PASS
3.1.6	SYN Flood Protection	PASS
3.1.7	Address Spoofing Protection	PASS
3.1.8	TCP Split Handshake Spoof	PASS

Testing determined that Fortinet 800c FortiOS v4.3.8 build632 correctly enforced complex outbound and inbound policies consisting of many rules, objects and applications. NSS engineers verified that the device successfully inspected traffic and took the appropriate action based upon the policy, raising the appropriate alerts and creating associated log entries.

4 Performance

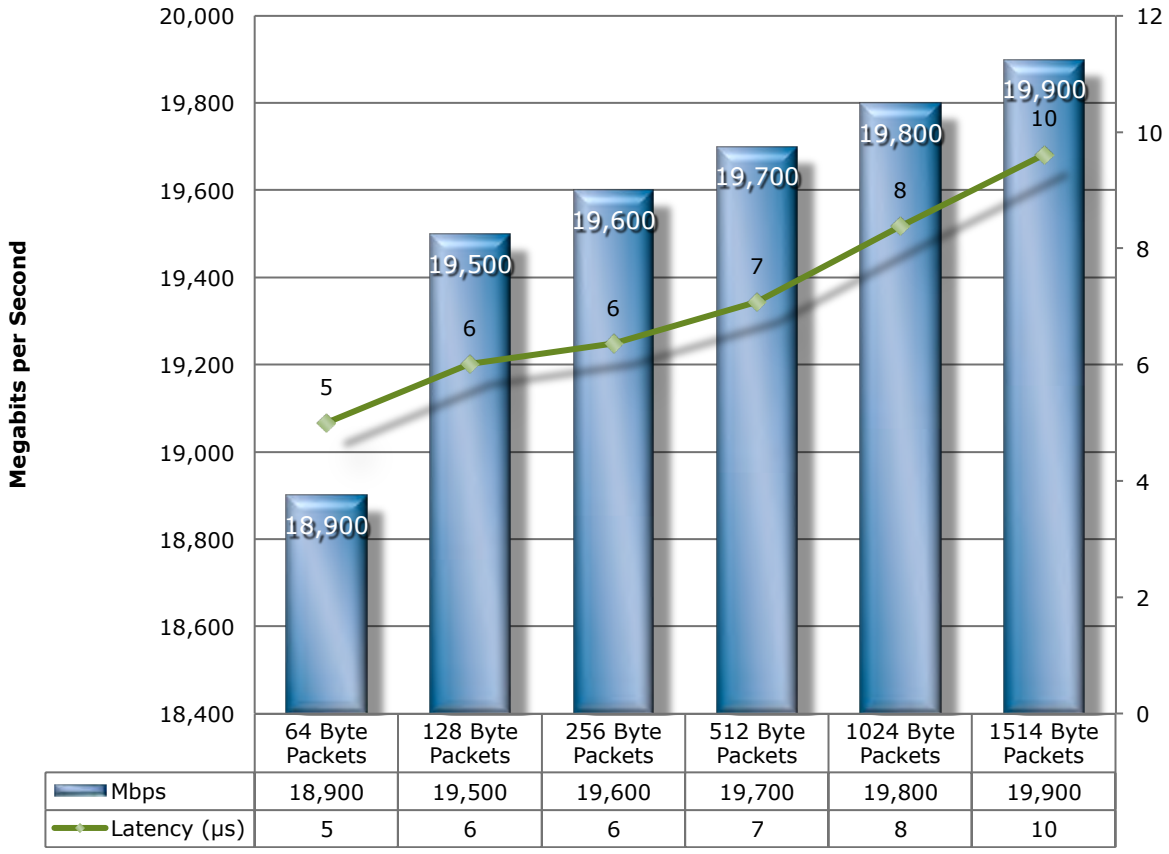
There is frequently a trade-off between security effectiveness and performance. Because of this trade-off, it is important to judge a product's security effectiveness within the context of its performance (and *vice versa*). This ensures that new security protections do not adversely impact performance and security shortcuts are not taken to maintain or improve performance.

4.1 UDP Throughput

This test uses UDP packets of varying sizes generated by BreakingPoint Systems traffic generation tool. A constant stream of the appropriate packet size — with variable source and destination IP addresses transmitting from a fixed source port to a fixed destination port — is transmitted bi-directionally through each port pair of the DUT.

Each packet contains dummy data, and is targeted at a valid port on a valid IP address on the target subnet. The percentage load and frames per second (fps) figures across each in-line port pair are verified by network monitoring tools before each test begins. Multiple tests are run and averages taken where necessary.

This traffic does not attempt to simulate any form of "real-world" network condition. No TCP sessions are created during this test, and there is very little for the state engine to do. The aim of this test is purely to determine the raw packet processing capability of each in-line port pair of the DUT, and its effectiveness at forwarding packets quickly in order to provide the highest level of network performance and lowest latency.



	64 Byte Packets	128 Byte Packets	256 Byte Packets	512 Byte Packets	1024 Byte Packets	1514 Byte Packets
Mbps	18,900	19,500	19,600	19,700	19,800	19,900
Latency (µs)	5	6	6	7	8	10

Figure 1: Raw Packet Processing Performance (UDP Traffic)

4.2 Latency – UDP

Firewalls that introduce high levels of latency lead to unacceptable response times for users, especially where multiple security devices are placed in the data path. These results show the latency (in microseconds) as recorded during the UDP throughput tests at 90% of maximum load.

Note that in the table below, the latency for this device is extremely low, and evironments that require minimal latency should consider this.

4.2	Latency - UDP	Microseconds
4.2.1	64 Byte Packets	5
4.2.2	128 Byte Packets	6
4.2.3	256 Byte Packets	6
4.2.4	512 Byte Packets	7
4.2.5	1024 Byte Packets	8
4.2.6	1514 Byte Packets	10

4.3 Maximum Capacity

The use of BreakingPoint appliances allows NSS Labs' engineers to create true "real world" traffic at multi-Gigabit speeds as a background load for the tests.

The aim of these tests is to stress the inspection engine and determine how it handles high volumes of TCP connections per second, application layer transactions per second, and concurrent open connections. All packets contain valid payload and address data, and these tests provide an excellent representation of a live network at various connection/transaction rates.

Note that in all tests, the following critical "breaking points" - where the final measurements are taken - are used:

- **Excessive concurrent TCP connections -** unacceptable increase in open connections on the server-side
- **Excessive response time for HTTP transactions -** excessive delays and increased response time to client
- **Unsuccessful HTTP transactions -** normally there should be zero unsuccessful transactions. Once these appear, it is an indication that excessive latency causing connections to time out

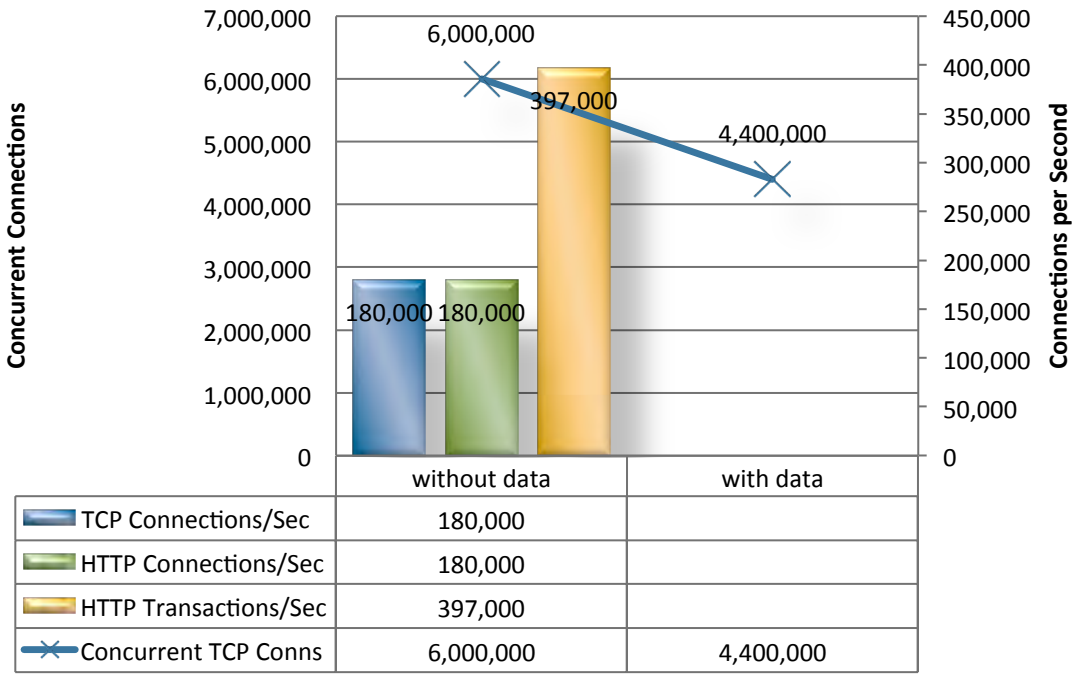


Figure 2: Concurrency and Connection Rates

4.4 HTTP Connections per Second and Capacity

The aim of these tests is to stress the HTTP detection engine and determine how the DUT copes with network loads of varying average packet size and varying connections per second. By creating genuine session-based traffic with varying session lengths, the DUT is forced to track valid TCP sessions, thus ensuring a higher workload than for simple packet-based background traffic. This provides a test environment that is as close to "real world" as it is possible to achieve in a lab environment, while ensuring absolute accuracy and repeatability.

Each transaction consists of a single HTTP GET request and there are no transaction delays (i.e. the web server responds immediately to all requests). All packets contain valid payload (a mix of binary and ASCII objects) and address data. This test provides an excellent representation of a live network (albeit one biased towards HTTP traffic) at various network loads.

Note that the throughput for the 800c decreases substantially when response object sizes are less than 4.5KB.

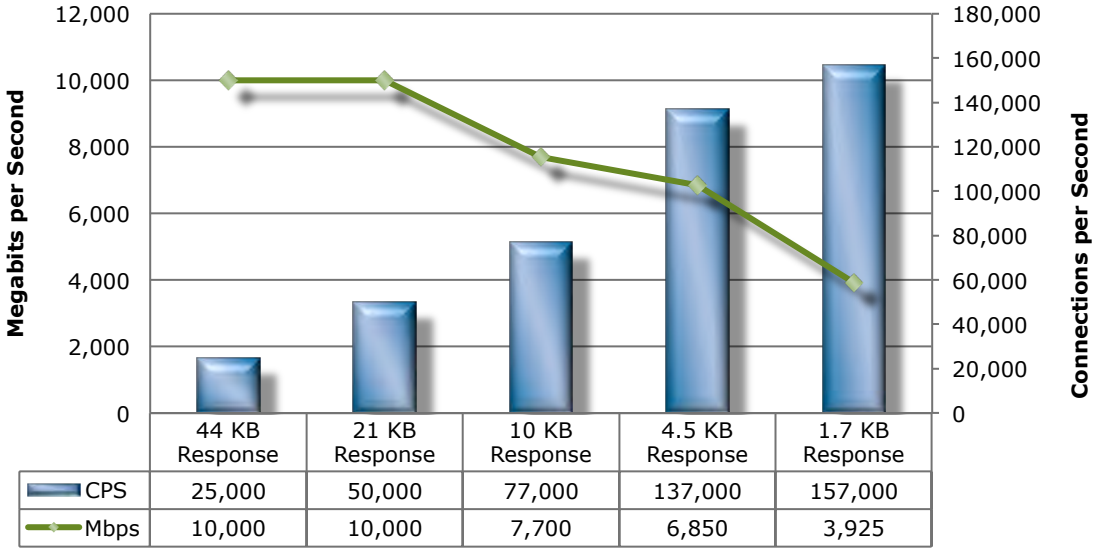


Figure 3: HTTP Connections per Second and Capacity

4.5 Application Average Response Time – HTTP

4.5	Application Average Response Time - HTTP (at 90% Max Load)	Milliseconds
4.5.1	2.500 Connections Per Second – 44Kbyte Response	0.94
4.5.2	5,000 Connections Per Second – 21Kbyte Response	0.78
4.5.3	10,000 Connections Per Second – 10Kbyte Response	0.53
4.5.4	20,000 Connections Per Second – 4.5Kbyte Response	0.40
4.5.5	40,000 Connections Per Second – 1.7Kbyte Response	0.34

4.6 HTTP Connections per Second and Capacity (With Delays)

Typical user behavior introduces delays between requests and reponses, e.g. “think time”, as users read web pages and decide which links to click next. This group of tests is identical to the previous group except that these include a 5 second delay in the server response for each transaction. This has the effect of maintaining a high number of open connections throughout the test, thus forcing the firewall to utilize additional resources to track those connections.

The Fortinet 800c performed significantly better on 10KB reponse testing with delay than without. This is uncommon, and suggests the 800c performs better with smaller response object sizes when the delay is added to give the device more time to process the protocol.

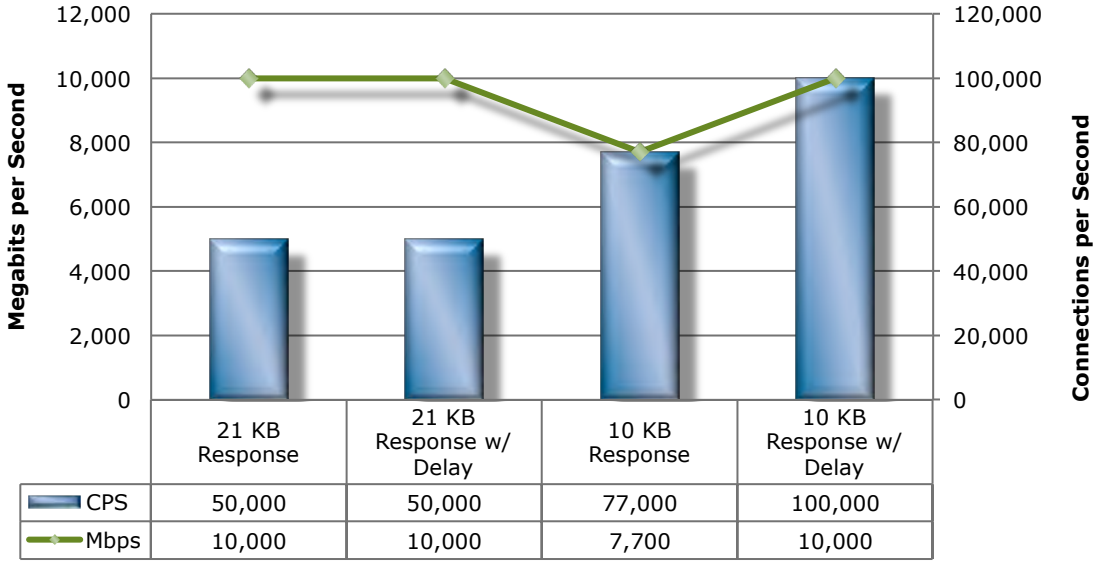


Figure 4: HTTP Connections per Second and Capacity (With Delays)

4.7 Real-World Traffic Mixes

The aim of this test is to measure the performance of the device under test in a "real world" environment by introducing additional protocols and real content, while still maintaining a precisely repeatable and consistent background traffic load. Different protocol mixes are utilized based on the intended location of the device under test (network core or perimeter) to reflect real use cases. For details about real world traffic protocol types and percentages, see the NSS Labs Network Firewall Test Methodology, available at www.nsslabs.com.

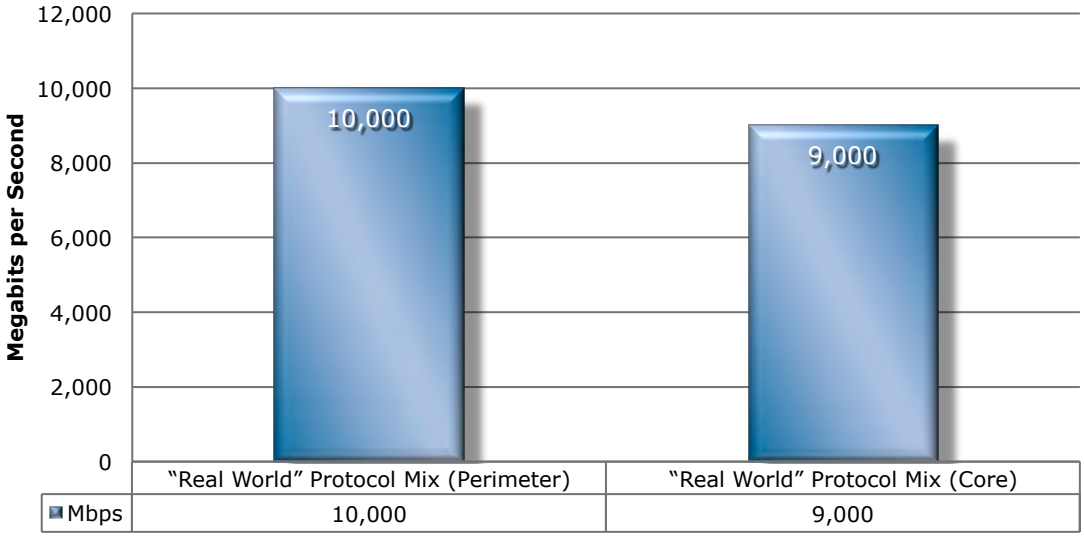


Figure 5: Real-World Traffic Mixes

5 Stability & Reliability

Long-term stability is particularly important for an in-line device, where failure can produce network outages. These tests verify the stability of the DUT along with its ability to maintain security effectiveness while under normal load and while passing malicious traffic. Products that are not able to sustain legitimate traffic (or crash) while under hostile attack will not pass.

The DUT is required to remain operational and stable throughout these tests, and to block 100 per cent of previously blocked traffic, raising an alert for each. If any non-allowed traffic passes successfully - caused by either the volume of traffic or the DUT failing open for any reason - this will result in a FAIL.

Test ID	Test Procedure	Result
5.1	Blocking Under Extended Attack	PASS
5.2	Passing Legitimate Traffic Under Extended Attack	PASS
5.3	Protocol Fuzzing & Mutation	PASS
5.4	Power Fail	PASS
5.5	Redundancy	Optional
5.6	Persistence of Data	PASS
5.7.1	Failover – Legitimate Traffic	PASS
5.7.2	Failover – Time To Failover	1.81 seconds
5.7.3	Stateful Operation	PASS
5.7.4	Active-Active Configuration	PASS

6 Management & Configuration

6.1 General

In addition to the specific tests noted below, NSS has executed an in-depth technical evaluation of all the main features and capabilities of the enterprise management system offered by the vendor. This will typically be offered as an extra-cost option.

Question	Answer
Routed Mode - Is DUT capable of running in full routed mode, with IP address assigned to detection ports.	Yes
Management Port - Does DUT feature a dedicated management port, separate from detection ports. Although this is the preferred configuration, lack of a management port (requiring DUT to be managed via one of the detection ports) will not be an issue providing management connection and communication is securely encrypted.	The device features two dedicated Ethernet management ports.
Management Protocol – Is connection from management console to DUT protected by a minimum of a user name/password combination or multi-factor authentication system, and are all communications securely encrypted. Where a three-tier management architecture is employed, all communication between console and management server(s), and between management server(s) and sensor(s) should be securely encrypted.	Yes, for direct management, SSH, Telnet, and Serial Console provide access to all configuration options. Major options, though not all options, are accessible via HTTP, HTTPS, and SNMP.
Authentication – Is access to management console protected by a granular user authentication system which allows for separation of read only and read-write access, preventing users who require reporting access only from modifying device parameters, etc. No access to administrative functions should be permitted (using either direct or centralized administration capabilities) without proper authentication.	Yes, admin profiles can be customized. Two are built in. There are many configuration settings that can be switched from “none”, to “read only” and “read-write” access such as network, system, VPN, firewall, etc.
Enterprise Authentication – Is access to management console protected by a granular user authentication system that allows for restriction of individual users to specific devices, ports, reports, and security policies. Authenticated users should be unable to access devices/ports/policies/alerts/reports/etc. restricted to other users of the system.	Yes, Fortinet’s management system, FortiManager, supports Radius, TACAS, and LDAP integration for granular access control. This is not available via the Local Management Interface (LMI)
Direct Device Management – Is direct access to the DUT provided (either via command line or Web interface) for single-device management.	Yes, a web interface is provided, and there is a CLI with configuration and monitoring ability via SSH.

Centralized Device Management – Is a centralized management system provided to manage one or more firewalls from a single point, including centralized device configuration, policy definition, alert handling and reporting for all sensors under the control of the management system. This should be scalable to large numbers of devices.	FortiManager is available for centralized device management (CDM).
Secure Device Registration – Is initial registration of DUT to central management console performed in a fully secure manner (it is permitted to offer a less secure/rapid option, but this should not be the default).	Inputting the IP of the management server into the firewall completes the registration, then accepting the devices registration's via FortiManager.

1.1 Policy

Question	Answer
Device Configuration - Does management system provide the means to configure one or more devices from a central location, assigning security policies, device settings, etc.	FortiManager provides this functionality.
Policy Definition - Does management system provide the means to define and save multiple security policies, consisting of: general device configuration, system-wide parameters, firewall policy, actions to take when malicious traffic discovered	FortiManager provides the ability to push policies to multiple devices, and traffic will go through previous policy until new one is fully installed. Not available via LMI.
Granularity – Is the DUT capable of blocking or creating exceptions based on IP address, application, user/group ID, protocol, VLAN tag, etc. (i.e. never block HTTP traffic between two specific IP addresses, always block FTP traffic to one specific IP address, etc.)	Yes, multiple rules may be created based on IP, interfaces, ports, etc.
Policy Association - Once policies have been defined, is it possible to associate them with specific devices or groups of devices	Available with CDM only.
Inheritance – Is it possible to create groups and sub-groups of devices such that sub-groups can inherit certain aspects of configuration and policy definition from parent groups	No
Virtualization - Once policies have been defined, is it possible to associate them with specific "virtual" devices or groups of devices, comprising an entire DUT, individual ports, port groups, IP address range, subnet or VLAN.	Policies can be created based and applied to interfaces and/or zones on the LMI. CDM provides for multiple devices.
Policy Deployment - Once policies have been defined, is it possible to distribute them to the appropriate device(s), virtual device(s), or groups of devices in a single operation.	Available with CDM only

Policy Auditing - Are changes to policies logged centrally. Log data should include at a minimum the date/time the changes were made, and the identity of the user who made them. If possible the system should record the actual changes.	Available with CDM only
Policy Version Control - Are changes to policies recorded by saving a version of the policy before each change. Is it possible to roll back to a previous version of any policy via a single operation	Available with CDM only

6.2 Alert Handling

Question	Answer
Generic Log Events - Does DUT record log entries for the following events: Detection of malicious traffic, termination of a session, successful authentication by administrator, unsuccessful authentication by administrator, policy changed, policy deployed, hardware failure, power cycle	The 800c records all appropriate logs for protection from events that a stateful firewall can provide such as SYN flood and DDOS attacks.
Log Location - Are log events logged on the DUT initially, in a secure manner, and subsequently transmitted to a central console/management server for permanent storage.	The 800c only provides logging to disk or syslog server. However, Fortinet offers hosted logging as well as a reporting server, FortiAnalyzer. Both are extra purchases. Logs can be shared via FTP and SQL.
Communication Interruption - Where communications between device and console/management server are interrupted, how much storage capacity is available on the DUT to store log data (in days/weeks). If it is not possible to restore communication in a timely manner, once the local logs are full, the DUT should either (1) continue passing traffic and overwrite oldest log entries, or (2) stop passing traffic. Which option is employed, and is it configurable by the administrator.	64 Gigabytes of local storage, (1) in normal mode, (2) in CC mode
Log Flooding – Are mechanisms in place (aggregation) to prevent the DUT from flooding the management server/console with too many events of the same type in a short interval. Is it possible to disable aggregation/flood protection completely for testing purposes to ensure NSS can see every individual alert.	Yes, the device provides the ability to disable event logging, as well as provides check boxes for which types of events to record. Also, it provides configurable level and time intervals for email alerts only.
Alerts - Does DUT record log entries each time it detects malicious traffic. What information is recorded?	Yes: time, source ip/port, destination ip/port, type of attack, etc.

Alert Accuracy - Does DUT record log entries that are accurate and human readable without having to use additional reference material. The DUT should attempt to minimize the number of alerts raised for a single event wherever possible.	Yes
Centralized Alerts – Are all alerts delivered to, and handled by, a single, central, management console. Is it possible to view all alerts globally, or select alerts from individual devices (logical or physical).	FortiAnalyzer provides this functionality.
Alert Delivery Mechanism - Does the DUT deliver alerts in a timely manner to a central database for permanent storage, central console for a real-time display, and SMTP server for e-mail alerts.	Available with CDM only
Alert Actions - On detecting malicious traffic, what actions can the DUT perform e.g. ignore, log only, allow, block, drop packet (no reset), drop session (no reset), e-mail administrator, send TCP reset (or ICMP redirect) to source only, send TCP reset (or ICMP redirect) to destination only, send TCP reset (or ICMP redirect) to both source and destination, reconfigure switch to isolate/quarantine offending port, page administrator	Ignore, log, drop packet, drop session, TCP reset client/server, email or page the administrator
Forensic Analysis - Can DUT capture individual packets, a range of packets, or an entire session where required (globally, or on a rule-by-rule basis)	The device can capture packets via the command line interface and output to the console. FortiAnalyzer can be used to store packet captures, but only from a Fortinet Intrustion Prevention Sensor (IPS).
Summarize Alerts – Can the central console provide the ability to select a particular piece of data from an alert and summarize on that data field (i.e. select a source IP address and view all alerts for that source IP). Alternatively, it should be possible to construct data filters manually in a search form and summarize on the specified search criteria. The preferred scenario is to offer both of these options.	The web interface provides filters for the logs to search for user provided values.
View Policy - Having selected an alert, does the system provide the ability to access directly the policy and rule that triggered the event in order to view and/or modify the policy for further fine-tuning	Available with CDM only
View Packet Contents – Does the central console provide the ability to select an individual alert and view the contents of the trigger packet	Available with CDM only

Alert Suppression - The central console should provide the ability to create exception filters based on alert data to eliminate further alerts which match the specified criteria (i.e. same alert ID from same source IP). This does not disable detection, logging or blocking, but merely excludes alerts from the console display.	Available with CDM only
Correlation (Automatic) – Does the system provide the means to infer connections between multiple alerts and group them together as incidents automatically	Available with CDM only
Correlation (Manual) – Does the system provide the means for the administrator to infer connections between multiple alerts and group them together as incidents manually.	No
Incident Workflow – Does the system provide the ability to annotate and track incidents to resolution	Available with CDM only

6.3 Reporting

Question	Answer
Centralized Reports – Is the system capable of reporting on all alerts from a single, central, management console. From that console, is it possible to report all alerts globally, or to report on alerts from individual devices (logical or physical).	Available with CDM only
Built In Reports - Does system provide built in reports covering typical requirements such as list of top attacks, top source/destination IP addresses, top targets, etc.	The LMI provides built in reports for bandwidth and application useage, web use, emails, threats, and VPN usage
Custom Reports – Does the system offer a report generator providing the ability to construct complex data filters in a search form and summarize alerts on the specified search criteria	Only the layout of built-in reports can be customized via the web interface. Other reporting functionality requires FortiAnalyzer.
Saved Reports - Having defined a custom report filter, is it possible to save it for subsequent recall	Available with CDM only
Scheduled Reports – Is it possible to schedule saved reports for regular unattended runs. If so, how is the output saved (as HTML or PDF, for example). Is it possible to publish reports to a central FTP/Web server, and/or e-mail reports to specified recipients.	Available with CDM only
Log File Maintenance - Does system provide for automatic rotation of log files, archiving, restoring from archive, and reporting from archived logs.	Yes

7 Total Cost of Ownership (TCO)

Implementation of firewall solutions can be complex, with several factors affecting the overall cost of deployment, maintenance and upkeep. All of these should be considered over the course of the useful life of the solution.

- **Product Purchase** – the cost of acquisition.
- **Product Maintenance** – the fees paid to the vendor (including software and hardware support, maintenance and other updates.)
- **Installation** – the time required to take the device out of the box, configure it, put it into the network, apply updates and patches, and set up desired logging and reporting.
- **Upkeep** – the time required to apply periodic updates and patches from vendors, including hardware, software, and other updates.

7.1 Labor Per Product (in Hours)

This table estimates the annual labor required to maintain each device. NSS Labs' assumptions are based upon the time required by an experienced security engineer ($75 per hour fully loaded,) allowing is to hold constant the talent cost, and measure only the difference in time required to maintain. Readers should substitute their own costs to obtain accurate TCO figures.

Product	Installation (Hrs)	Upkeep / Year (Hrs)
Fortinet 800c FortiOS v4.3.8 build632	8	12

7.2 Purchase Price and Total Cost of Ownership

Calculations are based on vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is utilized since this is the option typically selected by enterprise customers. Prices are for single device management and maintenance only; costs for central device management (CDM) solutions may be extra. For reference, the CDM cost is included in the scorecard, though is not factored into the single device TCO. For additional TCO analyses, including CDM, see the Management Comparative Analysis Report (CAR.)

Product	Purchase	Maintenance / year	Year 1 Cost	Year 2 Cost	Year 3 Cost	3 Year TCO
Fortinet 800c FortiOS v4.3.8 build632	$9,998	$2,188	$13,686	$3,088	$3,088	$19,861

- Year One Cost is calculated by multiplying the Labor Rate ($75 per hour fully loaded x (Installation + Upkeep)) + Purchase Price + Maintenance
- Year Two Cost is calculated by multiplying the Labor Rate ($75 per hour x Upkeep) + Maintenance
- Year Three Cost is calculated by multiplying the Labor Rate ($75 per hour x Upkeep) + Maintenance

7.3 Value: Total Cost of Ownership Per Protected Mbps

There is a clear difference between price and value. The least expensive product does not necessarily offer the greatest value if it offers significantly lower performance than only slightly more expensive competitors. The best value is a product with a low TCO and high level of secure throughput (security effectiveness x performance).

The following table illustrates the relative cost per unit of work performed: Mbps-Protected

Product	Protection	Throughput	3 Year TCO	Price / Mbps-Protected
Fortinet 800c FortiOS v4.3.8 build632	100%	9,667	$19,861	$2

Price per Protected Mbps was calculated by taking the Three-Year TCO and dividing it by the product of Protection x Throughput. Three-Year TCO/(Protection x Throughput) = Price/Mbps-Protected.

8 Detailed Product Scorecard

The following chart depicts the status of each test with quantitative results where applicable.

Test ID	Description	Result
3	Security Effectiveness	
3.1	Firewall Policy Enforcement	
3.1.1	Baseline Policy	PASS
3.1.2	Simple Policy	PASS
3.1.3	Complex Policy	PASS
3.1.4	Static NAT	PASS
3.1.5	Dynamic / Hide NAT	PASS
3.1.6	Syn Flood Protection	PASS
3.1.7	Address Spoofing Protection	PASS
3.1.8	TCP Split Handshake	PASS
4	Performance	
4.1	UDP Throughput	Mbps
4.1.1	64 Byte Packets	18,900
4.1.2	128 Byte Packets	19,500
4.1.3	256 Byte Packets	19,600
4.1.4	512 Byte Packets	19,700
4.1.5	1024 Byte Packets	19,800
4.1.6	1514 Byte Packets	19,900
4.2	Latency - UDP	Microseconds
4.2.1	64 Byte Packets	5
4.2.2	128 Byte Packets	6
4.2.3	256 Byte Packets	6
4.2.4	512 Byte Packets	7
4.2.5	1024 Byte Packets	8
4.2.6	1514 Byte Packets	9
4.3	Connection Dynamics - Concurrency & Connection Rates	
4.3.1	Theoretical Max. Concurrent TCP Connections	6,000,000
4.3.2	Theoretical Max. Concurrent TCP Connections w/Data	4,400,000

4.3.3	Maximum TCP Connections Per Second	180,000
4.3.4	Maximum HTTP Connections Per Second	180,000
4.3.5	Maximum HTTP Transactions Per Second	397,000
4.4	HTTP Connections per Second & Capacity	CPS
4.4.1	2.500 Connections Per Second – 44Kbyte Response	25,000
4.4.2	5,000 Connections Per Second – 21Kbyte Response	50,000
4.4.3	10,000 Connections Per Second – 10Kbyte Response	77,000
4.4.4	20,000 Connections Per Second – 4.5Kbyte Response	137,000
4.4.5	40,000 Connections Per Second – 1.7Kbyte Response	157,000
4.5	HTTP Average Application Response Time	
4.5.1	2.500 Connections Per Second – 44Kbyte Response	0.94
4.5.2	5,000 Connections Per Second – 21Kbyte Response	0.78
4.5.3	10,000 Connections Per Second – 10Kbyte Response	0.53
4.5.4	20,000 Connections Per Second – 4.5Kbyte Response	0.40
4.5.5	40,000 Connections Per Second – 1.7Kbyte Response	0.34
4.6	HTTP Connections per Second & Capacity with Delays	CPS
4.6.1	5,000 Connections Per Second – 21Kbyte Response with Delays	50,000
4.6.2	10,000 Connections Per Second – 10Kbyte Response with Delays	100,000
4.7	“Real World” Traffic	Mbps
4.7.1	“Real World” Protocol Mix (Perimeter)	10,000
4.7.2	“Real World” Protocol Mix (Core)	9,000
5	Stability & Reliability	
5.1	Blocking Under Extended Attack	PASS
5.2	Passing Legitimate Traffic Under Extended Attack	PASS
5.3	Protocol Fuzzing & Mutation	PASS
5.4	Power Fail	PASS

5.5	Redundancy	Optional
5.6	Persistence of Data	PASS
5.7.1	Failover – Legitimate Traffic	PASS
5.7.2	Failover – Malicious Traffic	PASS
5.7.3	Time to Failover	1.81 Seconds
5.7.4	Stateful Operation	PASS
5.7.5	Active-Active Configuration	PASS
6	Management & Configuration	
6.1	General	
6.1.1	Management Port	Yes
6.1.2	Management Protocol	Yes
6.1.3	Authentication	Yes
6.1.4	Enterprise Authentication	Yes
6.1.5	Direct Device Management	Yes
6.1.6	Centralized Device Management	Yes
6.1.7	Secure Device Registration	Yes
6.2	Policy	
6.2.1	Firewall Configuration	Yes
6.2.2	Policy Definition	Yes
6.2.3	Granularity	Yes
6.2.4	Policy Association	Yes
6.2.5	Inheritance	No
6.2.6	Virtualization	Yes
6.2.7	Policy Deployment	Yes
6.2.8	Policy Auditing	Yes
6.2.9	Policy Version Control	Yes
6.3	Alert Handling	
6.3.1	Generic Log Events	Yes
6.3.2	Log Location	Yes
6.3.3	Communication Interruption	See Section 6.3
6.3.4	Log Flooding	Yes
6.3.5	Alerts	Yes
6.3.6	Alert Accuracy	Yes

6.3.7	Centralized Alerts	Yes
6.3.8	Alert Delivery Mechanism	Yes
6.3.9	Alert Actions	See Section 6.3
6.3.10	Summarize Alerts	Yes
6.3.11	View Alert Detail	Yes
6.3.12	View Policy	Yes
6.3.13	Alert Suppression	Yes
6.4	Reporting	
6.4.1	Centralized Reports	Yes
6.4.2	Built In Reports	Yes
6.4.3	Custom Reports	Yes
6.4.4	Saved Reports	Yes
6.4.5	Scheduled Reports	Yes
6.4.6	Log File Maintenance	Yes
7	Total Cost of Ownership	
7.1	Ease of Use	
7.1.1	Initial Setup (Hours)	8
7.1.2	Time Required for Upkeep (Hours per Year)	12
7.2	Expected Costs	
7.2.1	Initial Purchase (hardware as tested)	$9,998
7.2.2	Initial Purchase (enterprise management system)	$5,993
7.2.3	Annual Cost of Maintenance & Support (hardware/software)	$2,188
7.2.4	Annual Cost of Maintenance & Support (enterprise management system)	$1,405
7.2.6	Installation Labor Cost (@$75/hr)	$600
7.2.7	Management/Upkeep Labor Cost (per Year @$75/hr)	$900
7.3	Total Cost of Ownership	
7.3.1	Year 1	$13,686
7.3.2	Year 2	$3,088
7.3.3	Year 3	$3,088
7.3.4	3 Year Total Cost of Ownership	$19,861

Contact Information

NSS Labs, Inc.
6207 Bee Caves Road, Suite 350
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com