

# NGX™

## **Embedded NGX 8.0 Release Notes** **General Availability Version**

October 2008

---

## Contents

<b>CONTENTS .....</b>	<b>2</b>
<b>INTRODUCTION .....</b>	<b>3</b>
Highlights of This Version .....	3
Supported Platforms .....	3
Availability .....	4
Copyright .....	4
<b>NEW FEATURES .....</b>	<b>5</b>
VStream Antispam .....	5
VStream Antispam Service Availability .....	8
New Security Features .....	9
New Network Access Control Features .....	12
New Networking Features .....	14
New Monitoring Features .....	18
New Maintenance Features .....	21

## Introduction

### Highlights of This Version

Embedded NGX 8.0 incorporates a host of new and improved features, including:

- VStream Antispam
- Firewall Monitor
- Enhanced Policy Editors
- Built-in 802.1x and WPA Authenticator
- Built-in RS-232 Terminal Server
- Built-in DNS Server
- BGP Dynamic Routing
- Enhanced SNMP MIB
- New Status Dashboard
- SmartDefense SCADA Protections

### Supported Platforms

Embedded NGX 8.0 EA supports the following hardware platforms:

- Check Point Safe@Office **100B** series
- Check Point Safe@Office **200** series
- Check Point Safe@Office **400W** series
- Check Point Safe@Office **500** series
- Check Point UTM-1 Edge (VPN-1 UTM Edge) **X** series
- Check Point UTM-1 Edge (VPN-1 UTM Edge) **W** series
- Check Point UTM-1 Edge Industrial
- Check Point ZoneAlarm **Z100G**

- NEC SecureBlade **300**
- Nokia **IP60**

### Availability

- Embedded NGX 8.0 is available to existing Embedded NGX customers with a valid software subscription contract.  
For additional information and documentation, [click here](#).

### Copyright

© Copyright 2008 SofaWare Technologies Ltd.

SofaWare is a registered trademark of SofaWare Technologies Ltd.

Check Point is a registered trademark of Check Point Software Technologies Ltd.

## New Features

### VStream Antispam

Email spam, also known as “bulk email” or “junk email”, is estimated to cost Internet users over \$50 billion annually in lost productivity, and to consume over 80 percent of all email traffic.

To help organizations combat spam, Embedded NGX 8.0 offers a new, integrated, inline antispam engine: VStream Antispam.

VStream Antispam relies on the latest in spam detection technology: a global spam detection network that allows extremely rapid response to spam and phishing email outbreaks, providing a higher than 98 percent detection rate and a less than 0.05 percent false positives rate.

Antispam Policy Safe Senders

#### VStream Antispam

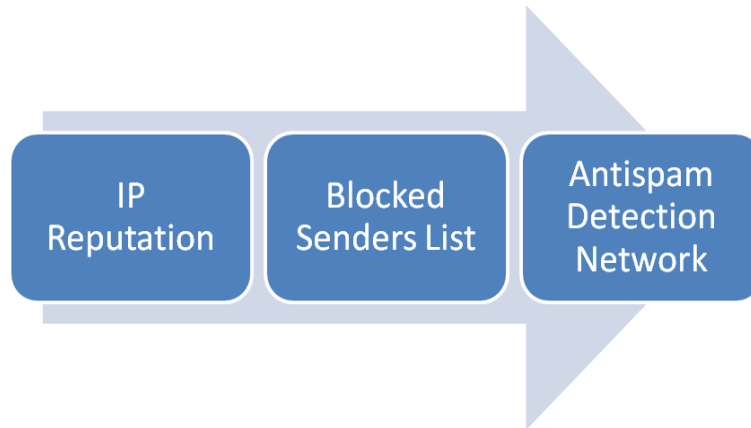
VStream Antispam

- On Monitor Only **Antispam Detection Network Monitor Only**  
 Email messages will be checked against an online spam detection database. Offending messages will be tracked. [Settings](#)
- On Monitor Only **Blocked List On**  
 Emails from specified senders will be tracked and blocked. [Edit List](#) [Settings](#)
- On Monitor Only **SMTP IP Reputation Checking On**  
 SMTP Email connections will be checked against an online IP reputation database. Emails from low reputation sources will be tracked and blocked. [Settings](#)

Status		
Email Messages	SMTP	POP3
Pending	0	0
Spam	0	0
Suspected Spam	0	0
Non Spam	0	0
Total	0	0
IP Reputation		
Pending	0	
Allowed	0	
Blocked	0	
Total	0	

VStream Antispam offers three layers of protection:

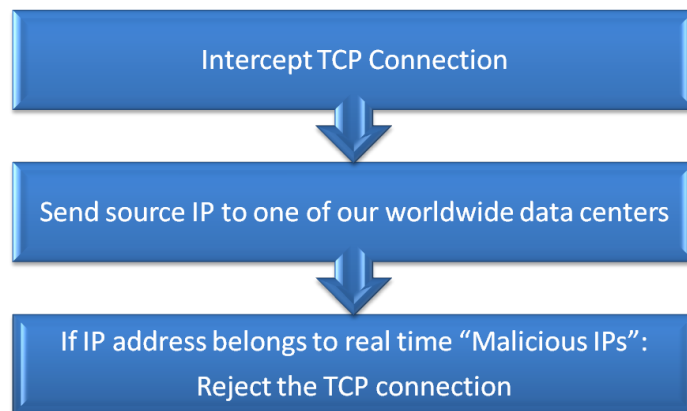
- IP Reputation Checking (Malicious IP Address Filtering)
- Content-based Antispam
- Block/Allow Lists (User-defined Black/White List)



### ***IP Reputation Checking***

IP Reputation Checking is the first component the VStream Antispam's multi-layered protection approach. The IP Reputation Checking engine checks the sender's "reputation" on the fly, before granting permission to send email over the SMTP protocol.

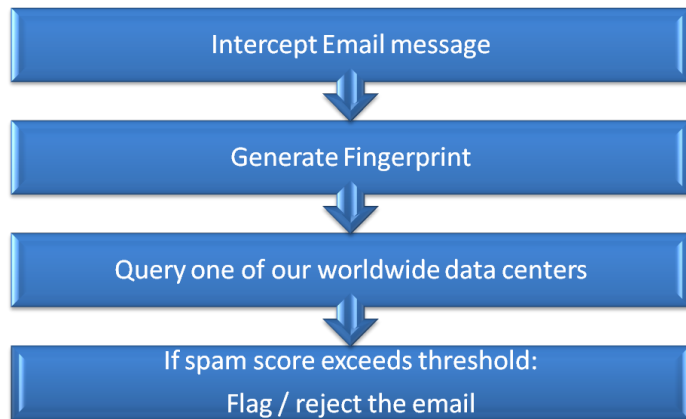
By working at the TCP connection level, the VStream Antivirus IP Reputation Checking engine stops most spammers before any of their traffic reaches your mail server. Before accepting the SMTP email connection, the sender's IP address is checked against an online and constantly updated IP Address reputation database. If the IP address belongs to a "known offender", the connection is immediately blocked at the TCP connection level, meaning that the untrusted sender cannot send even a single packet to your mail server. Using IP Reputation Checking provides increased protection against spammers overloading your mail server, and drastically reduces the amount of network and mail server resources consumed by spam email.



Efficient caching allows the IP Reputation Checking engine to protect against even the heaviest spam attacks.

## Content Based Antispam

Content Based Antispam is a fingerprint-based antispam engine that calculates a short “spam fingerprint” for each incoming email message. The fingerprint is then passed to one of our geographically distributed VStream Antispam data centers and compared to our constantly updated database of millions of known spam messages. The Content Based Antispam then returns a "spam score": a probability value in percentages indicating the likelihood that the message is spam.



If the spam score exceeds a user-configurable threshold (called the “confidence level”), the message header and/or subject can be flagged as spam, or the message can be deleted altogether.

Content Based Antispam supports both the POP3 and SMTP protocols.

Content Based Antispam and IP Reputation Checking complement one another and are typically used together to combine the benefits of both engines:

	<b>IP Reputation Checking</b>	<b>Content Based Antispam</b>
<b>Detection Method</b>	Sender IP Address	Email Contents
<b>Supported Protocols</b>	SMTP	SMTP, POP3
<b>Mail Rejection Method</b>	TCP Reset	Mark Subject, Mark Header, SMTP Reject, POP3 Delete
<b>Server Overloading Protection</b>	Yes	No

### Block/Allow List

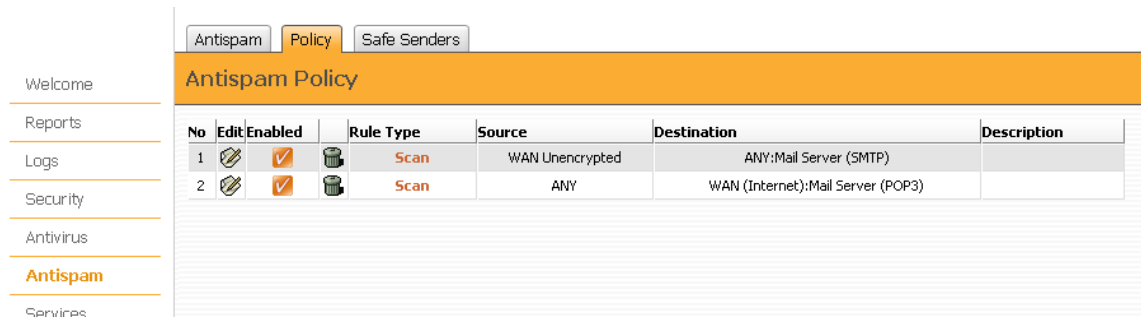
In addition to Content Based Antispam and IP Reputation Checking, VStream Antispam includes the ability to define lists of allowed and blocked senders. The addresses in these lists can contain wildcards, allowing for blocking entire domains or marking entire domains as safe.





Blocked Sender List	
@spammer.com	 <a href="#">Erase</a>
@annoying.com	 <a href="#">Erase</a>

### VStream Antispam Policy

The VStream Antispam policy allows the administrator to specify, with a very fine level of granularity, which email traffic should be scanned and which should be considered safe.

The VStream Antispam policy is comprised of rules that are processed sequentially. Each rule defines a type of email traffic according to protocol, source IP address/network, and/or destination IP address/network, and indicates whether matching connections should be scanned, automatically allowed, or automatically rejected.



No	Edit	Enabled	Rule Type	Source	Destination	Description
1		<input checked="" type="checkbox"/>	 Scan	WAN Unencrypted	ANY:Mail Server (SMTP)	
2		<input checked="" type="checkbox"/>	 Scan	ANY	WAN (Internet):Mail Server (POP3)	

### VStream Antispam Service Availability

VStream Antispam is supported in all Embedded NGX appliance types.

The appliance must be connected to a Service Center that supports VStream Antispam. The VStream Antispam service is supported with SMP 7.0 or later, and will be soon be available with Check Point SmartCenter.



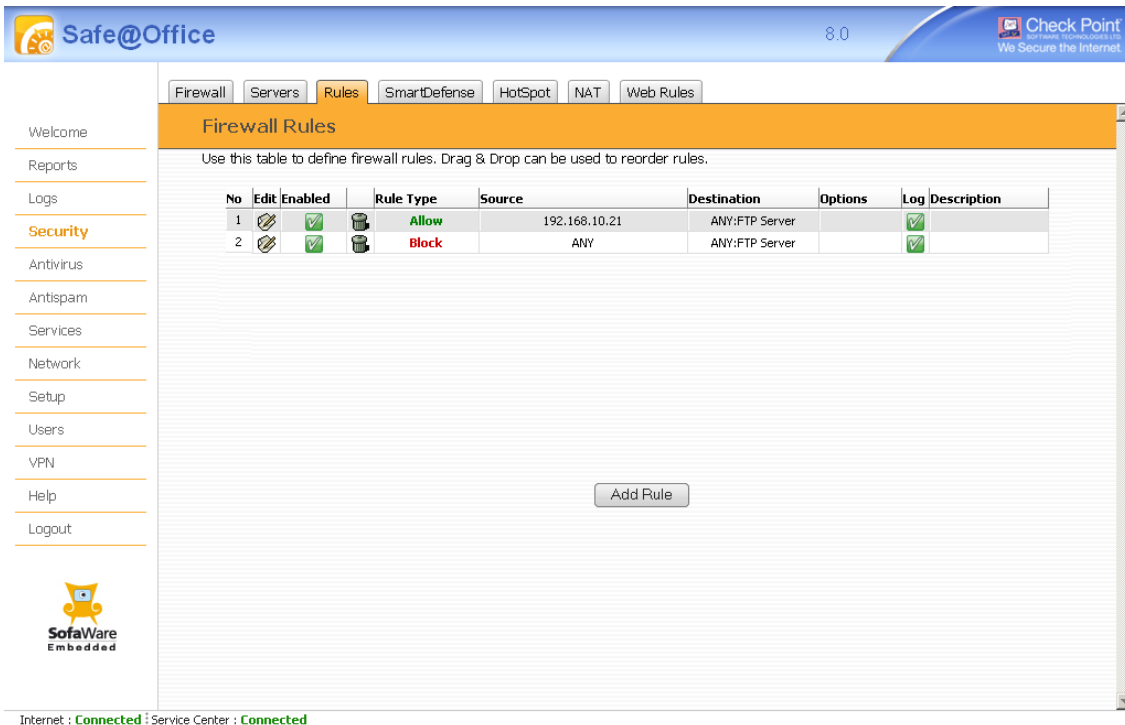
## New Security Features

### Enhanced Policy Editors

Embedded NGX 8.0 includes enhanced Web-based policy editors, allowing for easier editing of security policies in the appliance's Web interface. The enhancements to the policy editors include **drag & drop-based** reordering of rules and an improved display format.

The following editors use the enhanced interface:

- Firewall Rules
- NAT Rules
- Web Rules
- VStream Antivirus Rules
- VStream Antispam Rules (New)



Safe@Office 8.0

Firewall Servers **Rules** SmartDefense HotSpot NAT Web Rules

### Firewall Rules

Use this table to define firewall rules. Drag & Drop can be used to reorder rules.

No	Edit	Enabled	Rule Type	Source	Destination	Options	Log	Description
1		<input checked="" type="checkbox"/>	Allow	192.168.10.21	ANY:FTP Server		<input checked="" type="checkbox"/>	
2		<input checked="" type="checkbox"/>	Block	ANY	ANY:FTP Server		<input checked="" type="checkbox"/>	

Add Rule

Internet : Connected Service Center : Connected

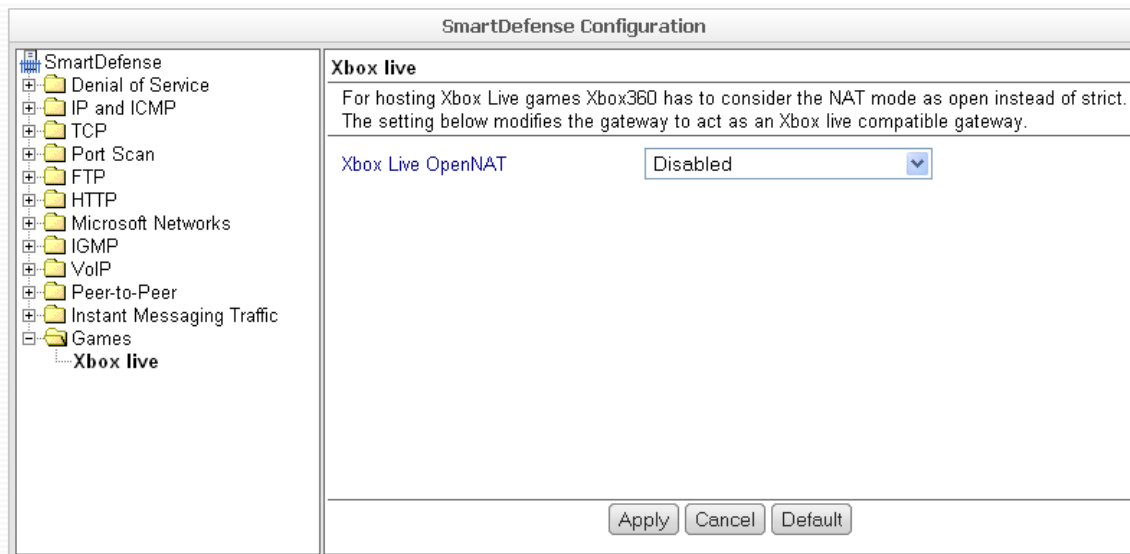
### **Xbox LIVE Open NAT Support**

Xbox LIVE is an online gaming and entertainment service. For our more young-at-heart customers, Embedded NGX 8.0 offers integrated ALG (Application Level Gateway) for Xbox LIVE game hosting.



To host Xbox LIVE games, Xbox 360 requires gateways to use the “Open NAT” method rather than the normal “Strict NAT” method. You can modify the Embedded NGX appliance to allow hosting Xbox LIVE games on your Xbox 360 console, by going to the **Security > SmartDefense** page and selecting **Enabled** in the **Xbox LIVE Open NAT** drop down list.

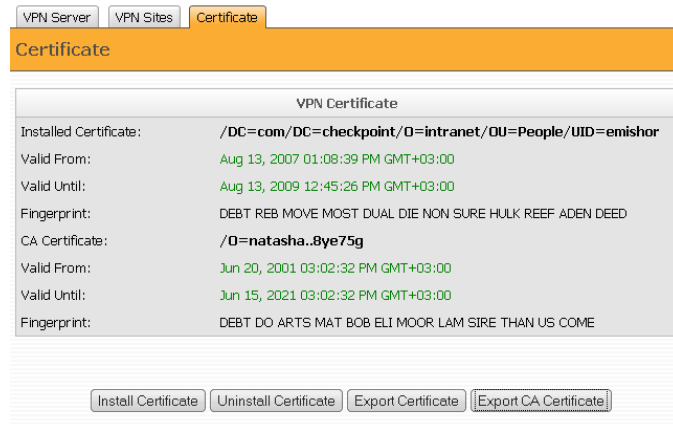
Note: This setting is required only if you want to host online games on your Xbox 360 console. If you just want to join existing games, there is no need to enable this setting.



## Export Certificate

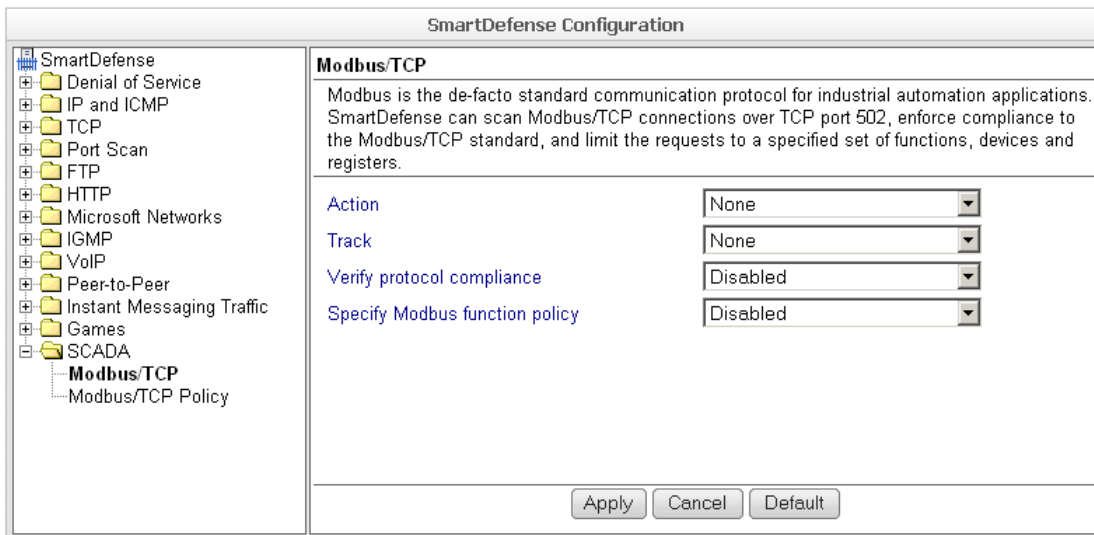
Embedded NGX 8.0 now supports exporting the device certificate and/or the device CA (Certificate Authority) certificate. The certificates are exported in PKCS#12 format.

To export a certificate, go to the **VPN > Certificate** page and click **Export Certificate** or **Export CA Certificate**.



## SmartDefense SCADA Protections

Embedded NGX 8.0 includes new SmartDefense protections related to supervisory control and data acquisition (SCADA) equipment.



SCADA equipment uses the Modbus/TCP protocol over TCP port 502 for communication. You can configure SmartDefense to scan Modbus/TCP connections, enforce compliance to the Modbus/TCP standard, and limit Modbus/TCP requests to a specified set of functions, devices, and registers.

*This feature is supported in the UTM-1 Edge platform only.*

## New Network Access Control Features

### Internal 802.1x and WPA Authenticator

Wi-Fi Protected Access (WPA and WPA2) Enterprise is a wireless network access control and encryption protocol that creates a secure wireless network based on a centralized user database. WPA Enterprise allows each wireless user to use a different password for authentication, and is therefore considered to provide a superior level of security compared to other wireless authentication methods that use a single password for all wireless stations, for example, WPA-PSK (Preshared Key).

802.1x is an IEEE standard for port-based network access control. It enables wired Ethernet users to securely authenticate to the switch, before gaining access to the network.

Traditionally, the downside of using 802.1x or WPA Enterprise has been the requirement to install a complex and costly RADIUS server, rendering these solutions unsuitable for smaller networks.

Not anymore. Embedded NGX 8.0 integrates a built-in EAP (Extended Authentication Protocol) authenticator, enabling you to use WPA Enterprise and 802.1x access control, without any need for an external RADIUS server.



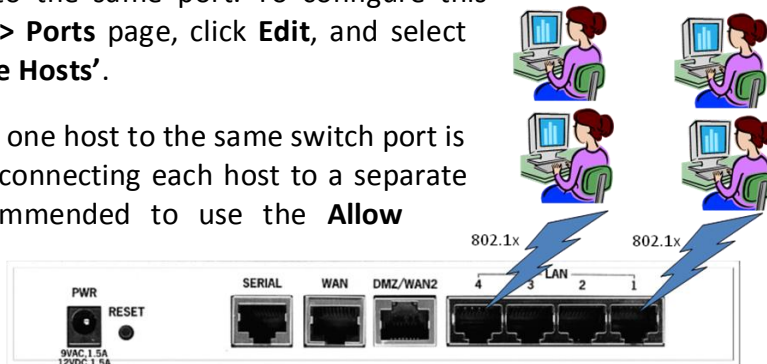
WPA Enterprise and 802.1x access control are now tied to the gateway's internal user database, making strong Network Access Control (NAC) so easy to use, that it is now suitable even for the smallest of networks.

Port Setup : DMZ / WAN2		
Assign to network	DMZ	?
Link Configuration	Automatic Detection	?
Port Security	802.1x	?
Authentication Server	RADIUS	?
Allow multiple hosts	<input checked="" type="checkbox"/>	?

### **Enhanced Wired 802.1x Support**

Normally, 802.1x network access control allows only a single host to connect to each switch port. To overcome this limitation, Embedded NGX 8.0 now optionally allows multiple hosts to connect to the same port. To configure this option, go to the **Network > Ports** page, click **Edit**, and select the checkbox **'Allow Multiple Hosts'**.

Note: Connecting more than one host to the same switch port is somewhat less secure than connecting each host to a separate port; therefore, it is recommended to use the **Allow Multiple Hosts** option only in locations where the number of switch ports are a limiting factor, and where an external 802.1x-capable switch cannot be installed.

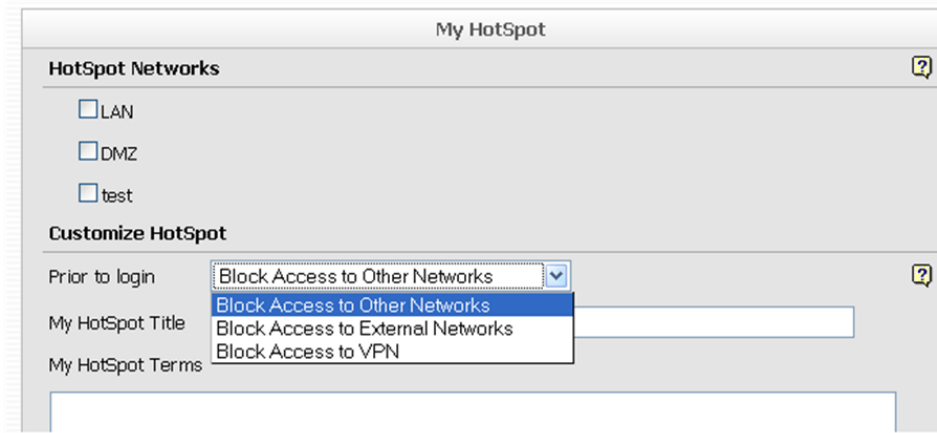


### **Enhanced Secure HotSpot NAC**

Secure HotSpot facilitates the creation of managed guest access networks (either wireless or wired) with Web-based authentication, guest user accounts, and RADIUS support.

To enhance Secure HotSpot functionality, Embedded NGX 8.0 now allows the administrator to choose between three ways of handling Secure HotSpot clients who failed to authenticate:

- Block Access to Other Networks (the default)
- Block Access to External Networks Only
- Block Access to VPN Only



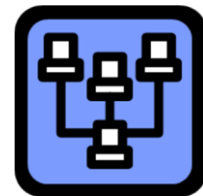
*This feature is supported in the following platforms: UTM-1 Edge, Safe@Office 500 with Power Pack, Safe@Office 225, and Safe@Office 410/425.*

## New Networking Features

### **BGP Support**

Previous Embedded NGX versions supported dynamic routing through the Open Shortest Path First (OSPF) protocol. Embedded NGX 8.0 extends this existing support, by adding support for Border Gateway Protocol (BGP). Both iBGP (Internal Border Gateway Protocol) and eBGP (External Border Gateway Protocol) variants are supported.

The advantages of using dynamic routing are automatic distribution of routing tables across the enterprise and automatic rerouting of traffic around failures, for high resiliency. Since the BGP implementation is fully integrated with VPN, you can enjoy all of the BGP protocol advantages in VPN links, allowing for a fully dynamic, resilient, multi-hop VPN network. It is even possible to use BGP in a mixed VPN and leased line environment, for automatic failover between VPN links and leased lines.



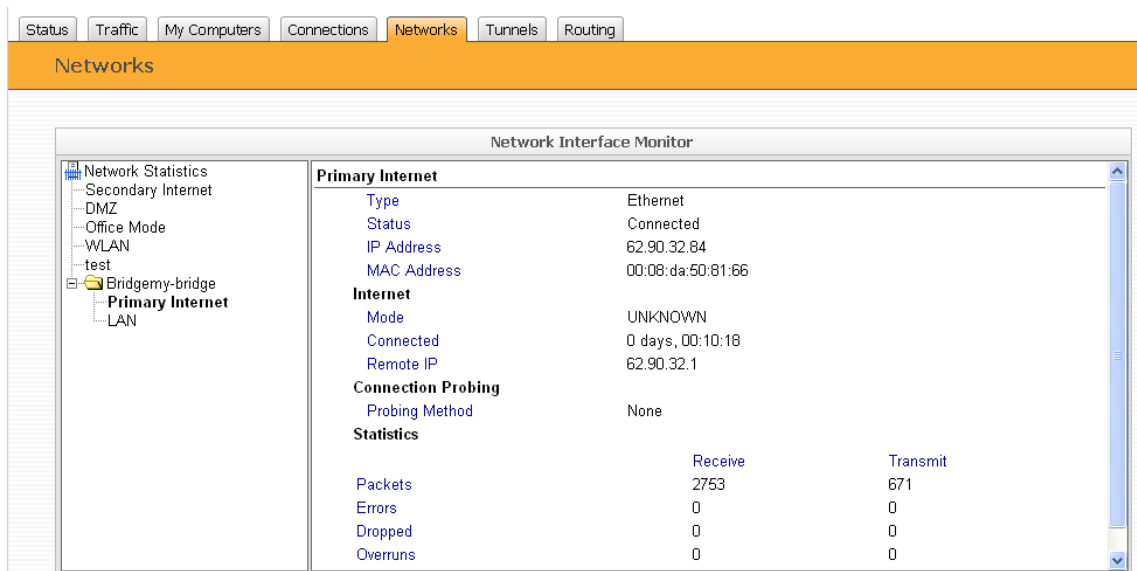
Note: BGP requires a unique firmware version. To obtain the required version, contact the SofaWare support team.

*This feature is supported in the following platforms: UTM-1 Edge, Safe@Office 500 with Power Pack, Safe@Office 225, and Safe@Office 410/425. BGP and OSPF cannot be used in parallel.*

## Network Interface Monitor

Embedded NGX 8.0 includes a Network Interface Monitor that allows easier network monitoring and provides detailed information on each of the gateway's internal and external interfaces.

The Network Interface Monitor can be accessed in the **Reports > Networks** page, as well as through the command line interface command **info net**.



The screenshot shows the 'Networks' page in the management console. The 'Network Interface Monitor' window displays the following information for the 'Primary Internet' interface:

Primary Internet		
Type	Ethernet	
Status	Connected	
IP Address	62.90.32.84	
MAC Address	00:08:da:50:81:66	
Internet		
Mode	UNKNOWN	
Connected	0 days, 00:10:18	
Remote IP	62.90.32.1	
Connection Probing		
Probing Method	None	
Statistics		
	Receive	Transmit
Packets	2753	671
Errors	0	0
Dropped	0	0
Overruns	0	0

## Internal RS-232 Terminal Server (Device Server)



Terminal servers (sometimes called device servers) offer an easy and cost-effective way of adding IP connectivity to legacy RS232 serial devices.

Ideal for Point of Sale (POS) and SCADA applications, Embedded NGX 8.0 now incorporates built-in terminal server functionality that can network-enable just about any device attached to the appliance's RS232 port in a matter of minutes. When used in



conjunction with VPN connectivity, the internal terminal server enables secure remote monitoring, diagnostics, and management of legacy serial devices, so that you can preserve investment in your present equipment. In addition, it reduces operating costs.

Existing devices are instantly “Internet-enabled”, without any need for hardware modification or additional equipment.

The terminal server supports two operation modes:

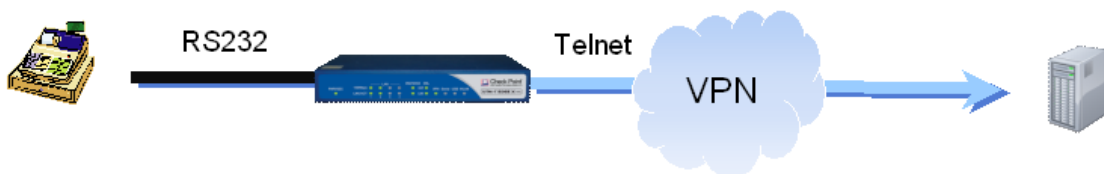
**Passive Mode** – The terminal server accepts connections from an external Telnet client and relays traffic to and from the appliance’s serial port.

### Passive Mode



**Active Mode** – The terminal server connects to an external Telnet server and relays traffic to and from the appliance’s serial port.

### Active Mode



A gateway in passive mode can even be used back-to-back with another gateway in active mode, to enable tunneling of serial RS232 data over the Internet or VPN.

*This feature is supported in the following platforms: UTM-1 Edge Industrial, UTM-1 Edge X Series, UTM-1 Edge W Series.*



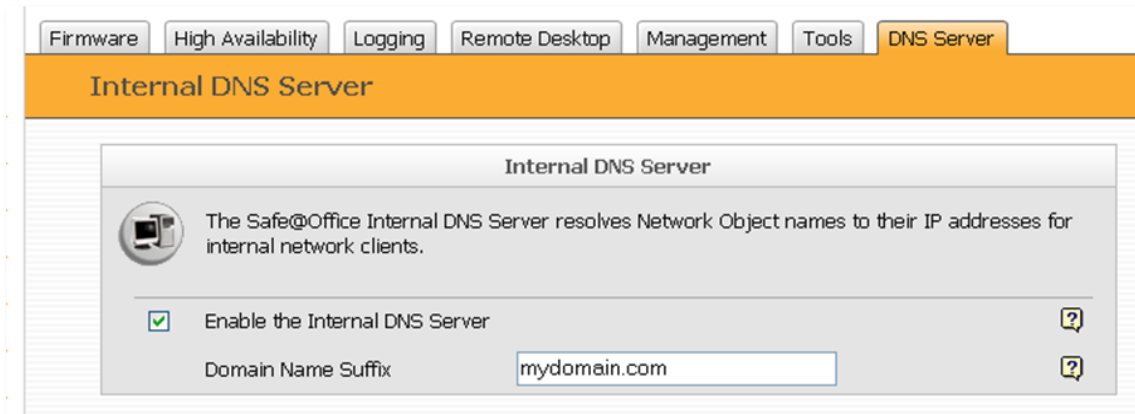
## Internal DNS Server

Embedded NGX 8.0 includes an internal DNS server, which can provide DNS resolution for internal hosts based on defined network objects. This can be used as a quick and easy internal DNS solution for smaller networks that lack resources for a dedicated DNS/WINS server.

To enable the internal DNS server, go to the **Setup > DNS Server** page, select the **Enable the Internal DNS Server** check box, and optionally specify a domain name suffix. The appliance will automatically reply to DNS requests from the internal networks, for all hosts defined as network objects.

For example, assume that the configured DNS suffix is “mydomain.com”, and a network object with the name “server1” is defined with the IP address 192.188.22.1. If queried by an internal host for the DNS name “server1.mydomain.com”, the gateway will reply to the request with the IP address 192.188.22.1.

If a gateway hostname is defined, the DNS server will also respond to requests in the format “<hostname>.mydomain.com” with the gateway’s internal IP address.

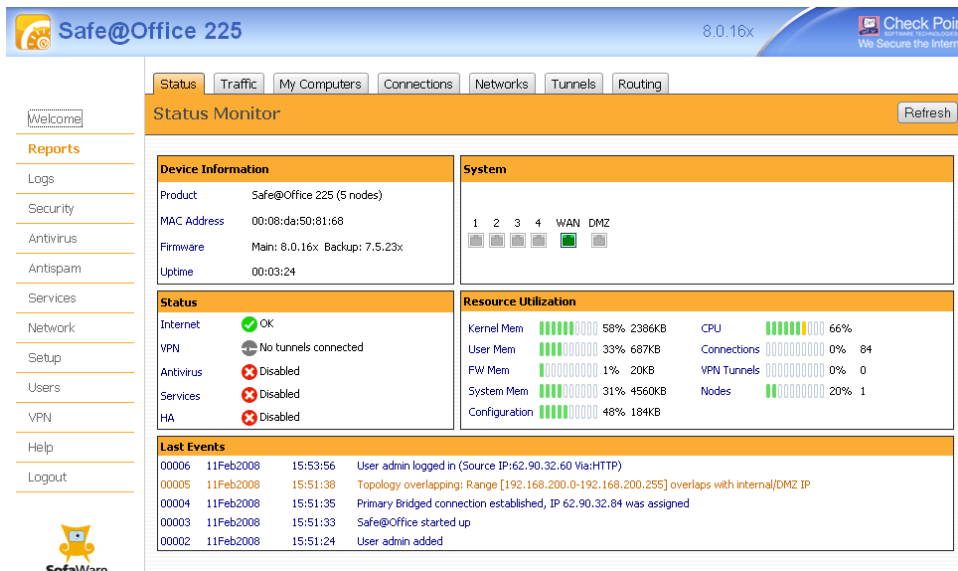


## New Monitoring Features

### Status Monitor

Embedded NGX 8.0 adds a new “Status Monitor” page to the Web interface, offering quick access to a wide variety of status information, including:

- Device Information: License, MAC Address, Installed Firmware, etc.
- Modules Status
- Resource Utilization: Memory, Storage, CPU, etc.
- Port Status



The screenshot displays the 'Status Monitor' page for a 'Safe@Office 225' device. The interface includes a navigation menu on the left with options like Reports, Logs, Security, Antivirus, Antispam, Services, Network, Setup, Users, VPN, Help, and Logout. The main content area is divided into several sections:

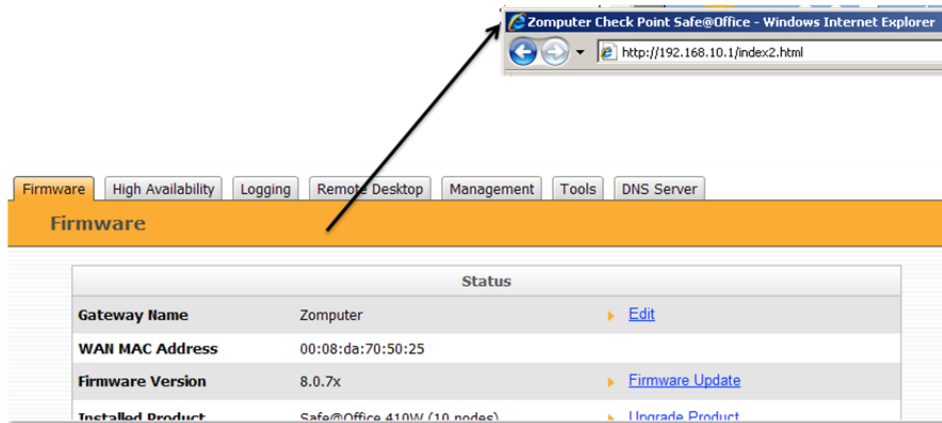
- Device Information:** Product: Safe@Office 225 (5 nodes), MAC Address: 00:08:da:50:81:68, Firmware: Main: 8.0.16x Backup: 7.5.23x, Uptime: 00:03:24.
- System:** A row of status indicators for ports 1, 2, 3, 4, WAN, and DMZ.
- Status:** Internet: OK (green checkmark), VPN: No tunnels connected (grey icon), Antivirus: Disabled (red X), Services: Disabled (red X), HA: Disabled (red X).
- Resource Utilization:** Kernel Mem: 58% 2386KB, CPU: 66%, User Mem: 33% 687KB, Connections: 0% 84, FW Mem: 1% 20KB, VPN Tunnels: 0% 0, System Mem: 31% 4560KB, Nodes: 20% 1, Configuration: 48% 184KB.
- Last Events:** A list of system events with timestamps and descriptions, such as 'User admin logged in' and 'Safe@Office started up'.

### Gateway Hostname

Embedded NGX 8.0 allows defining a “gateway hostname”. The hostname is used for as an identifier and is displayed in the following places:

- The Web interface’s title bar
- The SNMP hostname
- Syslog messages sent from this gateway

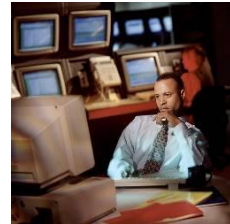
By default, the gateway hostname is set to the appliance MAC address.



### **Enhanced SNMP MIB**

The Embedded NGX 8.0 SNMP agent now exposes additional status parameters, including:

- Detailed RAM and Storage Utilization
- CPU Usage
- Hardware Details
- Installed License
- Firmware Details
- More...



### **Enhanced Log Viewer**

The Embedded NGX 8.0 log viewer has been significantly enhanced, for increased functionality and ease of use.

For clearer separation between security events and non-security related events, the log viewer has been split into two tabs: the Event Log and the Security Log.

In addition, to allow easier navigation between large numbers of log messages, log paging is supported. This also means that the log pages now load much more quickly, especially when viewing the logs remotely, over slow links.

Finally, the log display format is now clearer and more concise, including easy-to-understand icons, a new color scheme, a “single row per event” design, horizontal and vertical scrolling, and the ability to resize each column to the desired width.

Event Log Security Log

Security Log Save Refresh Clear

No	Date	Time	Dir/Act/Source	Port	Destination	Service	Reason	Rule/Net	Informatic
00618	01Jan2008	17:38:12	☞ 212.150.2.130	16836	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00617	01Jan2008	17:37:11	☞ 212.150.2.130	16819	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00616	01Jan2008	17:36:26	☞ 212.150.2.130	16812	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00615	01Jan2008	17:36:26	☞ 212.150.2.130	16811	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00614	01Jan2008	17:36:10	☞ 212.150.2.130	16798	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00613	01Jan2008	17:35:39	☞ 212.150.2.130	16793	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00612	01Jan2008	17:35:22	☞ 212.150.2.130	16787	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00611	01Jan2008	17:35:22	☞ 212.150.2.130	16786	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00610	01Jan2008	17:31:03	☞ 212.150.2.130	16684	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00609	01Jan2008	17:31:03	☞ 212.150.2.130	16683	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00608	01Jan2008	17:30:38	☞ 62.90.32.194 (SOFWARE)	1151	212.150.2.132	TCP 36867	TCP out of state	-11 LAN	
00607	01Jan2008	17:30:31	☞ 62.90.32.194 (SOFWARE)	1156	212.150.2.132	TCP 36867	TCP out of state	-11 LAN	
00606	31Dec2007	17:51:39	☞ 212.150.2.130	52853	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00605	31Dec2007	17:50:39	☞ 212.150.2.130	52834	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00604	31Dec2007	17:49:37	☞ 212.150.2.130	52817	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00603	31Dec2007	17:48:36	☞ 212.150.2.130	52799	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00602	31Dec2007	17:47:36	☞ 212.150.2.130	52786	62.90.32.194 (SOFWARE)	UDP 6004	Policy rule	15 WAN (Internet)	
00601	31Dec2007	17:47:20	☞ 62.90.32.194 (SOFWARE)	4386	212.150.2.132	TCP 36867	TCP out of state	-11 LAN	
00600	31Dec2007	17:46:59	☞ 62.90.32.194 (SOFWARE)	4391	212.150.2.132	TCP 36867	TCP out of state	-11 LAN	
00599	31Dec2007	17:46:56	☞ 62.90.32.194 (SOFWARE)	4477	212.150.2.132	TCP 1025	TCP out of state	-11 LAN	

100 Next >

## Firewall Monitor

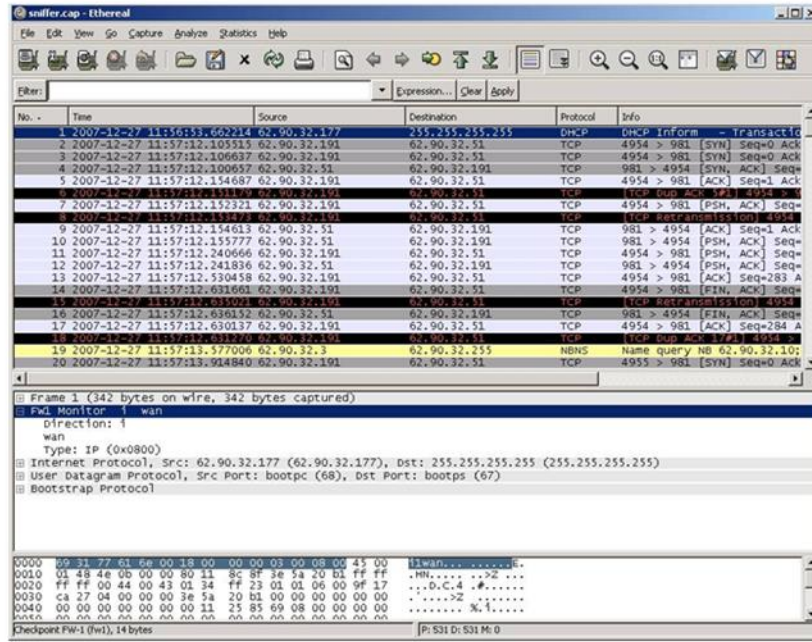
The integrated traffic sniffer in Embedded NGX 8.0 now includes a powerful troubleshooting tool: the Firewall Monitor.

When **Firewall Monitor** mode is enabled, special tags are added to the traffic sniffer's packet capture file, and each packet is recorded in multiple stages, as it passes through the gateway: before firewall processing (input) and after firewall processing (output). This allows you to observe exactly what the firewall does to your packets.

To view the results in Ethereal/Wireshark, select the menu option **Edit > Preferences > Ethernet** and enable the **Attempt to interpret as Firewall-1 monitor file** option.

For each packet, the following additional information is displayed:

- The interface name on which the packet was captured
- The packet's processing direction:
  - i - Input (before firewall processing)
  - o - Output (after firewall processing)

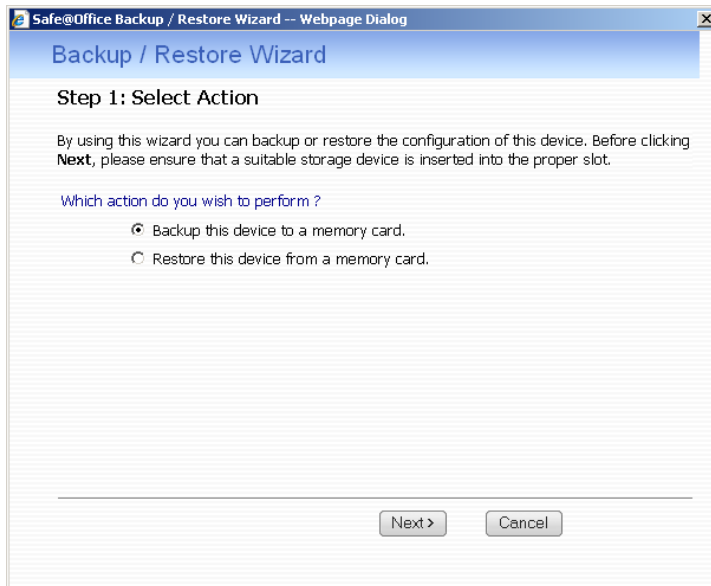


## New Maintenance Features

### *Backup and Restore Using a USB Flash Drive*

Embedded NGX 8.0 allows backing up the appliance configuration, security policy, and certificate to USB flash drives. You can then restore the appliance settings from the USB flash drive as needed.

Backup and restore operations are performed by inserting the USB flash drive into the Embedded NGX appliance's USB port, and then running the **Backup/Restore Wizard** in the **Setup > Tools** page.



### ***Rapid Deployment Using a USB Flash Drive***

Embedded NGX appliances are shipped with a specific firmware and group of settings that represent the appliance's default state. When installing a new appliance, you can configure different settings and install new firmware versions as needed; however, this can be time-consuming.

Embedded NGX 8.0 rapid deployment avoids this hassle, by allowing you to load the desired firmware, configuration, security policy, and certificate from a USB flash drive during product initialization. Rapid deployment can be used on individual appliances at the customer site, or on multiple appliances before they leave the warehouse.

Before performing a rapid deployment, it is necessary to prepare the USB flash drive. For each appliance you want to deploy, you must create a folder named after the appliance's MAC address, and then add the desired configuration files to the folder.

Rapid deployment is performed by pressing the RESET button at the back of the appliance, and then inserting the USB flash drive into the Embedded NGX appliance's USB port. The appliance will automatically load the settings from the relevant folder on the USB flash drive.