SNMP Monitoring and SWG MIB

Secure Web Gateway

Release 10.0 • Manual Version 1.01

M86 SECURITY SNMP MONITORING AND SWG MIB

828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published November 2010 for SWG software release 10.0

Trademarks

CONTENTS

Introduction

The Simple Network Management Protocol (SNMP) is an application-layer Internet protocol designed to facilitate the exchange of management and monitoring information between network devices. It enables network administrators to manage network performance, find and solve network problems, and plan network capacity and growth. Although SNMP can also be used to configure network devices, we do not support that for security reasons.

Secure Web Gateway enables sending SNMP traps, and replying to SNMP queries based on a dedicated M86 Security MIB (or based on basic Linux system MIBs) and using SNMPv2c or SNMPv3.

Alert Settings

Navigate in the Management Console to **Administration → Alerts → Alert Settings** tab where you can monitor the main modules and components of the system. Secure Web Gateway will notify you of system events, application events update events, or security events. There are two different channels of communication:

- SNMP notification
- Email messages

NOTES: *The Email option is enabled only if the Enable Sending Email checkbox in* **Administration → System Settings → Mail Server** *is enabled. The SNMP option is enabled only if the Enable Trap Sending checkbox in* **Administration → Alerts → SNMP → SNMP General** *tab is enabled*

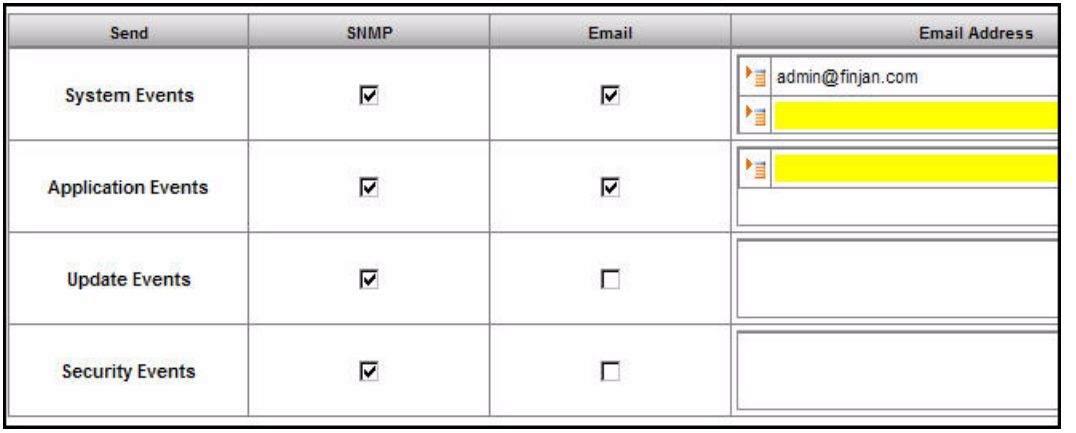

Figure 1-1: Alert Settings

For each of the event types (System, Application, Update, and Security Events), select the corresponding SNMP checkbox, or email alert checkbox and specify the email addresses to which the alert will be sent. Enter additional email addresses within the same field by clicking . To remove an address, right click and select **Delete Row** from the drop down menu.

The following table details the alerts available for each system event:

SNMP and Email Alerts
System Events
Hard Drive Threshold
System Load
Memory Usage Threshold
Application Events
Emergency Policy Selected
Archive Upload Failed
Backup Failed
Log Handler Down
Scanning Process is Unexpectedly Down
License Expiry
License Modification or Update
Active / Standby Policy Server
No Connection to Policy Server for Past Hour
Update Events
OS Update Available
Security Update Available
Security Update Failed
OS Update Failed
Security Update Successfully Installed
OS Update Successfully Installed

SNMP and Email Alerts
Could not download the update file
Error in validating checksum
Update failed due to internal error
Received update with unsupported version
Update exceeded maximum installation time
Could not find the update file
The update file was not created properly
Update installed successfully
Security Events
Incoming threat
Outgoing threat

SNMP Configuration

Navigate in the Management Console to **Administration → Alerts → SNMP**. The **General** tab allows you to configure monitoring of the main modules and components of the system. You can also react to these events in a timely manner and potentially resolve the issues.

SNMPv2 revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. SNMPv2 adds and enhances some of the SNMPv1 protocol operations.

SNMPv3 provides much more secure access to devices by a combination of authentication and encryption over the network (i.e. it includes authentication, privacy, and access control).

General

This section allows you to configure the SNMP protocol for MIB monitoring and Trap sending, as well as the ports that are used for these functions.

- Check **Enable MIB Monitoring** such that Secure Web Gateway Management System can be queried to get the MIB information and define the corresponding **Listening Port** (i.e. perform SNMP queries against specified port number, port 161 is default).
- Check **Enable Trap Sending** to enable Secure Web Gateway to send traps and define the corresponding **Trap Port** (port 162 is default).

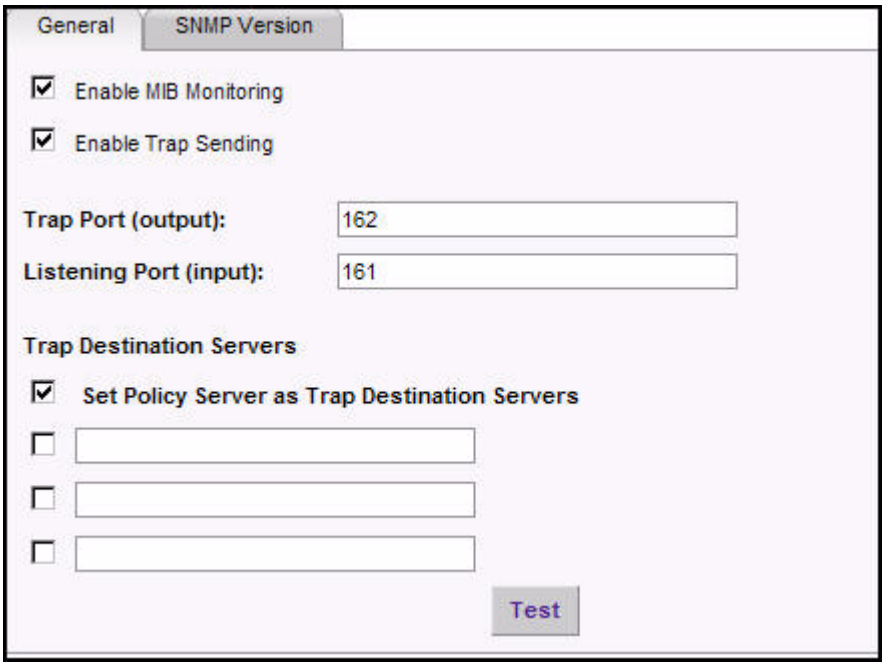

Figure 1-2: SNMP General Tab

- The Trap Destination Servers enable configuration of the Hostname/IP destination servers for receiving the SNMP traps. The trap destination is usually defined by an IP address, but a host name can also be used, if the device is set up to query a Domain Name System (DNS) server.

Make sure that the Secure Web Gateway devices can communicate with the trap server on the required port (default is UDP 162) – by configuring a firewall if necessary.

There is a possibility of defining three possible destination servers. You can configure the traps to be sent to any or all of these servers. If the checkbox next to the IP is unchecked, the remote server will not receive the SNMP trap.

The **Test** button allows you to test that the traps are successfully sent to the SNMP destination server/s. A test message will be sent to the pre-defined server/s with the SNMP name, IP and the Secure Web Gateway Software Version. Secure Web Gateway does not display proof of a successful test, but you can verify in the SNMP destination server if the test message was received.

After making changes to the SNMP screen, click **Save** and  .

SNMP Version

This section defines which version of SNMP the system works with: SNMPv2 (SNMPv2c) or SNMPv3.

The **SNMP Community** (for SNMPv2) is the group that the devices and management stations running SNMP belong to. You can use the community string in order to differentiate M86 Security SNMP traps from other appliances. The default string is “finjan”.

M86 Security uses the default context name for SNMPv3.

SNMP MIB Monitoring

The Management Information Base (MIB) is a configuration set of objects that can be monitored by the network management system (SNMP). The following options are available for configuration for SNMPv3 only.

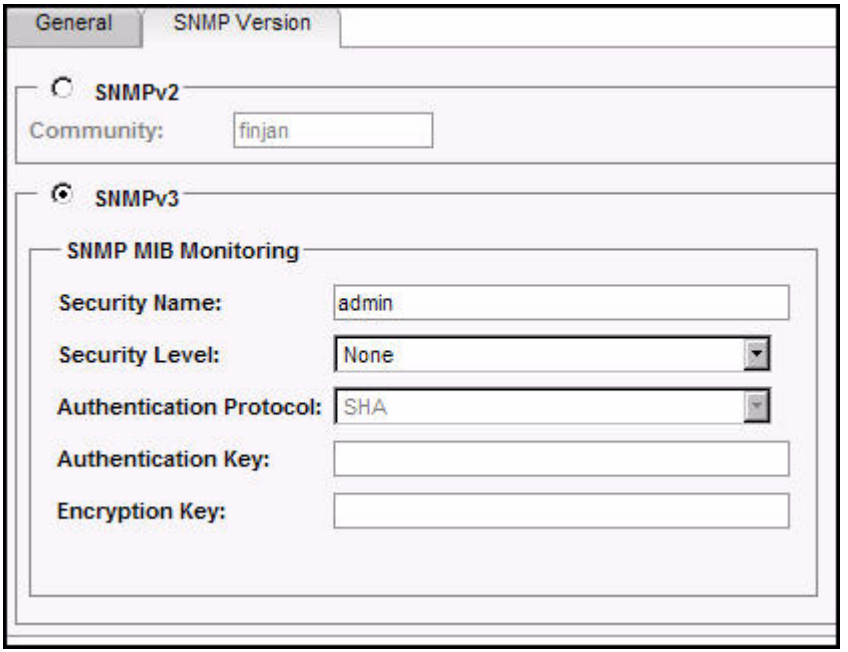

Figure 1-3: SNMP Version Tab

The table below provides an explanation of the fields:

Field Name	Description
Security Name	SNMP user name. If the Security Name in the SNMP MIB Monitoring section is the same as the Security Name in the SNMP Traps, the rest of the parameters must be the same as well.
Security Level	Messages can be sent unauthenticated, authenticated, or authenticated and encrypted. The corresponding possible configuration in the pull down list of this field include: None, Authentication, Authentication and Encryption.
Authentication Protocol	Either **MD5** or **SHA** (verification checksums).
Authentication Key	Authentication is performed by using the user's authentication key to sign the message being sent.
Encryption Key	Authentication is performed by using the user's encryption key which encrypts the data portion of the message that is being sent. (Encryption method used is DES)

NOTES:** The authentication / encryption options are enabled only when the corresponding Security Level is selected.**

SNMP Traps

SNMP traps are deployed as a mean of notifying the management console of specific events. SNMPv3 mandates that trap messages are rejected unless the SNMPv3 user sending the trap is defined in the user database of the management console. User is identified

by a combination of the user's name (Security Name) and an identifier for the given SNMP application (engineID). Secure Web Gateway uses a unique engineID for all the appliances.

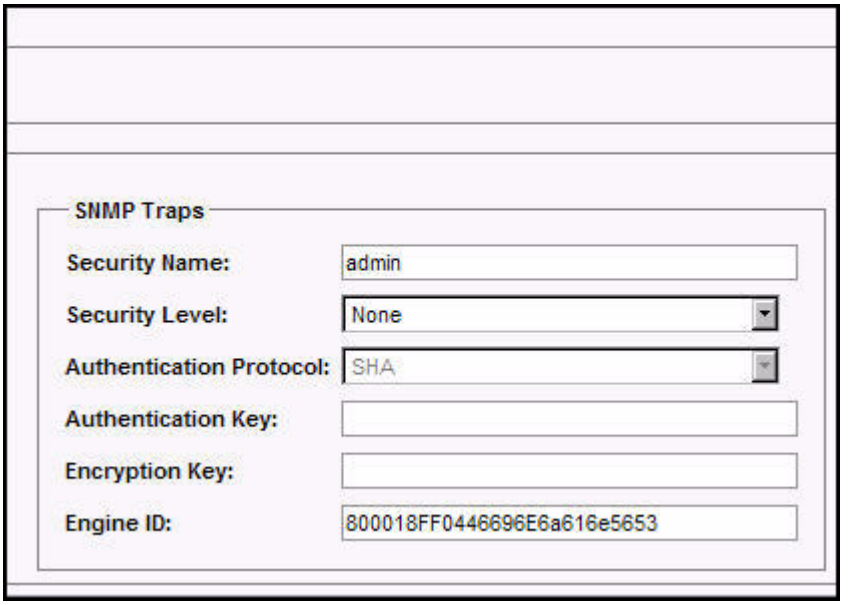

Figure 1-4: SNMP Traps

The table below provides an explanation of the fields:

Field Name	Description
Security Name	SNMP user name.
Security Level	Messages can be sent unauthenticated, authenticated, or authenticated and encrypted.
Authentication Protocol	Either **MD5** or **SHA** (verification checksums).
Authentication Key	Authentication is performed by using the user's authentication key to sign the message being sent.

Field Name	Description
Encryption Key	Authentication is performed by using the user's encryption key which encrypts the data portion of the message being sent.
EngineID	This is an identifier for the given SNMP application.

After making changes to the SNMP screen, click **Save** and  .

Management Information Base (MIB)

A Management Information Base (MIB) is a monitoring information list of objects that can be monitored by an SNMP Manager. A MIB is an information format that describes general information which is common to most devices.

The **Secure Web Gateway Web Appliances** support the following SNMP MIB types:

- System MIB||
- Interfaces MIBII
- IP MIBII
- TCP MIBII
- Host Resources MIB
- Application proprietary MIB

Using a Standard MIB

Any SNMP Management software that works with SNMP can be used, such as one of the followings:

- HPOV
- TEMIP
- MRTG/PRTG

Object Identifier (OID)

SNMP Management System needs to be familiar with the MIBs of the managed elements in the network in order to maximize its monitoring capabilities. The MIBs includes a technical description of the Object Identifiers (OID) that can be managed or monitored by the Manager which pre-loads the MIBs into memory during its initiation. An object Identifier, also known as a MIB variable, is described by a set of concatenated numbers separated by dots which build up a unique string identifier. Each OID defines a different value from various aspects, system, application or other. While system values are mostly supported through the standard MIB-II, the application and other values in Secure Web Gateway are exposed through M86 Security's specific (non-standard) object IDs (OIDs).

The SCANNER status OIDs contain the following vaues

Application	Values
Scanner Status	1.3.6.1.4.1.2021.8.1.100.1 Possible Values: 0: Scanner Up 1: Scanner Down
Scanner Status String	1.3.6.1.4.1.2021.8.1.101.1 Possible Values: Scanner is Up Scanner is Down

Example Using a Non-Standard OID

The following example enables the administrator to calculate the overall average of the CPU usage. Note that there are several different ways of calculating the CPU usage.

➲ **To calculate the CPU usage:**

1. Calculate delta values for all CPU counters (deltaIdle, deltaUser, deltaNice, deltaSystem, deltaKernel) by taking a sample for each CPU counter every n amount of time.
2. Then, minus the value taken at an earlier stage of time from the value calculated at a later stage of time in order to calculate the delta value. For example, if at 10.00am, the value for CpuUser was 15, and at 10.02, the value for CpuUser was 20, then 20-15=5.
3. Add up each of these delta values for each CPU counter (delta CpuIdle + delta CpuUser + delta CpuNice + delta CpuSystem + delta CpuKernel) to obtain the deltaTotal.
4. The CPU Usage in percentage is **100 - 100 * deltaIdle / deltaTotal**. This represents the CPU Usage between the sampled time intervals.

M86 Security MIB

M86 Security has designed its own MIB for the Secure Web Gateway product.

MIB Entries

Each of the following M86 Security OIDs begins with the same prefix: `1.3.6.1.4.1.6790`:

OID	Field	Values
1.3.6.1.4.1.6790.1.1.2.0	Secure Web Gateway product version	Alphanumeric string
1.3.6.1.4.1.6790.1.1.3.0	Secure Web Gateway Build Information	Alphanumeric string
1.3.6.1.4.1.6790.1.1.6.0	Current configuration version (obsolete)	Alphanumeric string
1.3.6.1.4.1.6790.1.1.10.0	Device Type	Integer where: 1 = All in One 2 = Scanning Server 3 = Policy Server 4 = Authentication Device 5 = Load Balancer 6 = Cache Device

OID	Field	Values
1.3.6.1.4.1.6790.1.1.11.0	Machine type	Alphanumeric string
1.3.6.1.4.1.6790.1.1.6.0	Current configuration version	Alphanumeric string
1.3.6.1.4.1.6790.1.1.20.2.0	Current emergency status	Integer
1.3.6.1.4.1.6790.1.1.30.7.1.0	Log Handler Process ID	Integer
1.3.6.1.4.1.6790.1.1.30.7.5.0	Last date and time the log handler data was reset	Date and Time
1.3.6.1.4.1.6790.1.1.30.7.12.1.0	Total number of logs since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.7.12.2.0	Total number of logs sent to the logging database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.7.12.3.0	Total number of logs sent to the archives database since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.7.12.4.0	Total number of logs sent to the reports database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.7.12.5.0	Total number of logs sent to syslog since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.8.1.0	Gateway Device total number of requests-per-second	Integer
1.3.6.1.4.1.6790.1.1.30.20.5.0	Last date and time the scanning server data was reset	Date and Time
1.3.6.1.4.1.6790.1.1.30.20.10.1.0	Total number of requests scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.10.2.0	Average rate of requests scanned per second	Integer
1.3.6.1.4.1.6790.1.1.30.20.10.5.0	Total input scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.10.6.0	Total output scanned since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.20.11.1.0	Total number of requests which were blocked since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.2.0	Total number of requests which were blocked due to Virus detection since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.3.0	Total number of requests which were blocked due to Behavior analysis since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.4.0	Total number of requests which were blocked due to being Blacklisted since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.5.0	Total number of requests which were blocked due to URL category since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.6.0	Secure Web Gateway scanner blocked requests per second	Integer
1.3.6.1.4.1.6790.1.1.30.20.11.7.0	Total number of HTTP requests blocked due to Data Leakage Prevention (DLP) since last reset.	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.20.12.1.0	Total number of requests which were logged since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.12.2.0	Total number of requests which were sent to the logging database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.12.3.0	Total number of requests which were sent to the archive database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.12.4.0	Total number of requests which were sent to the reports database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.20.12.5.0	Total number of requests which were sent to the syslog database since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.5.0	Last date and time the HTTP data was reset	Date and time
1.3.6.1.4.1.6790.1.1.30.21.10.1.0	Total number of HTTP requests scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.10.2.0	Average rate of HTTP requests scanned per second	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.21.10.5.0	Total HTTP input scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.10.6.0	Total HTTP output scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.11.1.0	Total number of HTTP requests which were blocked since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.11.2.0	Total number of HTTP requests which were blocked due to Virus detection since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.11.3.0	Total number of HTTP requests which were blocked due to Behavior analysis since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.11.4.0	Total number of HTTP requests which were blocked due to being blacklisted since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.21.11.5.0	Total number of HTTP requests which were blocked due to URL category since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.21.11.7.0	Total number of HTTP requests blocked due to Data Leakage Prevention (DLP) since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.5.0	Last date and time the HTTPS data was reset	Date and time
1.3.6.1.4.1.6790.1.1.30.22.10.1.0	Total number of HTTPS requests scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.10.2.0	Average rate of HTTPS requests scanned per second	Integer
1.3.6.1.4.1.6790.1.1.30.22.10.5.0	Total HTTPS input scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.10.6.0	Total HTTPS output scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.11.1.0	Total number of HTTPS requests which were blocked since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.22.11.2.0	Total number of HTTPS requests which were blocked due to Virus detection since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.11.3.0	Total number of HTTPS requests which were blocked due to Behavior analysis since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.11.4.0	Total number of HTTPS requests which were blocked due to being blacklisted since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.11.5.0	Total number of HTTPS requests which were blocked due to URL category since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.22.11.7.0	Total number of HTTPS requests blocked due to Data Leakage Prevention (DLP) since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.5.0	Last date and time the FTP data was reset	Date and time
1.3.6.1.4.1.6790.1.1.30.23.10.1.0	Total number of FTP requests scanned since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.23.10.2.0	Average rate of FTP requests scanned per second	Integer
1.3.6.1.4.1.6790.1.1.30.23.10.5.0	Total FTP input scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.10.6.0	Total FTP output scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.11.1.0	Total number of FTP requests which were blocked since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.11.2.0	Total number of FTP requests which were blocked due to Virus detection since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.11.3.0	Total number of FTP requests which were blocked due to Behavior analysis since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.11.4.0	Total number of FTP requests which were blocked due to being blacklisted since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.23.11.5.0	Total number of FTP requests which were blocked due to URL category since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.23.11.7.0	Total number of FTP requests which were blocked due to Data Leakage Prevention (DLP) since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.5.0	Last date and time the ICAP data was reset	Date and time
1.3.6.1.4.1.6790.1.1.30.24.10.1.0	Total number of ICAP requests scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.10.2.0	Average rate of ICAP requests scanned per second	Integer
1.3.6.1.4.1.6790.1.1.30.24.10.5.0	Total ICAP input scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.10.6.0	Total ICAP output scanned since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.11.1.0	Total number of ICAP requests which were blocked since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.11.2.0	Total number of ICAP requests which were blocked due to Virus detection since last reset	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.30.24.11.3.0	Total number of ICAP requests which were blocked due to Behavior analysis since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.11.4.0	Total number of ICAP requests which were blocked due to being blacklisted since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.11.5.0	Total number of ICAP requests which were blocked due to URL category since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.24.11.7.0	Total number of ICAP requests blocked due to Data Leakage Prevention (DLP) since last reset	Integer
1.3.6.1.4.1.6790.1.1.30.40.1.0	Total open HTTP and HTTPS connections	Integer

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.2.0	An alarm has been set or cleared in the Secure Web Gateway system	vsAlarmEventType vsAlarmProbableCause vsAlarmSpecificProblems vsAlarmSeverity vsAlarmAdditionalText vsAlarmProposedRepairActions vsAlarmServerIP vsAlarmServerName vsAlarmServerType vsAlarmServerVersion vsAlarmEventTimeI think we should distinguish those OIDs from the above ones. Those here are Trap related – one cannot GET them

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.1.1.1.0	Represents the event type values for the alarms	Integer where: 1 = Other 2 = Communications Alarm 3 = Quality of Service Alarm 4 = Processing Error Alarm 5 = Equipment Alarm 6 = Environmental Alarm 7 = Integrity Violation 8 = Operational Violation 9 = Physical Violation 10 = Security Service or Mechanism Violation 11 = Time Domain Violation

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.1.1.2.0	Represents the probable cause values for the alarms	Integer where: 1 = Other 2 = Adapter Error 3 = Application Subsystem Failure 4 = Bandwidth Reduced 5 = Call Establishment Error 6 = Communication Protocol Error 7 = Communication Subsystem Failure 8 = Configuration or Customization Error 9 = Congestion 10 = Corrupt Data 11 = CPU Cycles Limit Exceeded 12 = Data Set or Modem Error 13 = Degrade Signal 14 = dte Dce Interface Error 15 = Enclosure Door Open 16 = Equipment Malfunction 17 = Excessive Vibration 18 = File Error 19 = Fire Detected 20 = Flood Detected 21 = Framing Error 22 = Heating Vent Cooling System Problem 23 = Humidity Unacceptable 24 = Input Output Device Error 25 = Input Device Error 26 = LAN error 27 = Leak Detected 28 = Local Node Transmission Error 29 = Loss of Frame 30 = Loss of Signal 31 = Material Supply Exhausted 32 = Multiplexer Problem 33 = Out of Memory 34 = Output Device Error 35 = Performance Degraded 36 = Power Problem 37 = Pressure Unacceptable 38 = Processor Problem 39 = Pump Failure 40 = Queue Size Exceeded

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.1.1.2.0 (cont.)	Represents the probable cause values for the alarms (cont.)	41 = Receive Failure 42 = Receiver Failure 43 = Remote Node Transmission Error 44 = Resource at or nearing Capacity 45 = Response Time Excessive 46 = Retransmission Rate Excessive 47 = Software Error 48 = Software Program Abnormally Terminated 49 = Software Program Error 50 = Storage Capacity Problem 51 = Temperature Unacceptable 52 = Threshold Crossed 53 = Timing Problem 54 = Toxic Leak Detected 55 = Transmit Failure 56 = Transmitter Failure 57 = Underlying Resource Unavailable 58 = Version Mismatch 59 = Authentication Failure 60 = Breach of Confidentiality 61 = Cable Tamper 62 = Delayed Information 63 = Denial of Service 64 = Duplicate Information 65 = Information Missing 66 = Information Modification Detected 67 = Information out of Sequence 68 = Intrusion Detection 69 = Key Expired 70 = Non Repudiation Failure 71 = Out of Hours Activity 72 = Out of Service 73 = Procedural Error 74 = Unauthorized Access Attempt 75 = Unexpected Information

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.1.1.3.0	Represents the specific problems field for the alarm	Integer
1.3.6.1.4.1.6790.1.1.100.1.1.4.0	Represents the perceived severity values for the alarms	Integer where: 1 = Cleared 2 = Indeterminate 3 = Critical 4= Major 5= Minor 6 = Warning
1.3.6.1.4.1.6790.1.1.100.1.1.5.0	Represents the additional text field for the alarm	Alphanumeric string
1.3.6.1.4.1.6790.1.1.100.1.1.6.0	Represents the proposed repair actions field for the alarm	Alphanumeric string
1.3.6.1.4.1.6790.1.1.100.1.1.7.0	Secure Web Gateway Server Name	Alphanumeric string
1.3.6.1.4.1.6790.1.1.100.1.1.8.0	Secure Web Gateway Server IP	IP address
1.3.6.1.4.1.6790.1.1.100.1.1.9.0	Secure Web Gateway Server Version	Size

OID	Field	Values
1.3.6.1.4.1.6790.1.1.100.1.1.10.0	Secure Web Gateway Server Type (Scanning, Policy, etc)	Alphanumeric string
1.3.6.1.4.1.6790.1.1.100.1.1.11.0	Secure Web Gateway Event Date and Time (GMT)	Date and Time

The following items are provided by M86 Security Secure Web Gateway MIB. Generally, each Security OID begins with the same prefix. However, the following three OIDs are supplied by a third party (Squid), and as such, prefixes will be different..

OID	Field	Values
1.3.6.1.4.1.3495.1.1.2.0	Cache Disk	Integer
1.3.6.1.4.1.3495.1.3.1.3.0	Cache Memory Usage	Integer
1.3.6.1.4.1.3495.1.3.2.2.1.9.5	Cache Hit Ratio	Integer
1.3.6.1.4.1.3495.1.3.2.1.5	Total volume of KBs sent back to the users per requests	Integer
1.3.6.1.4.1.3495.1.3.2.1.12	Total volume of KBs received by the cache proxy from servers	Integer