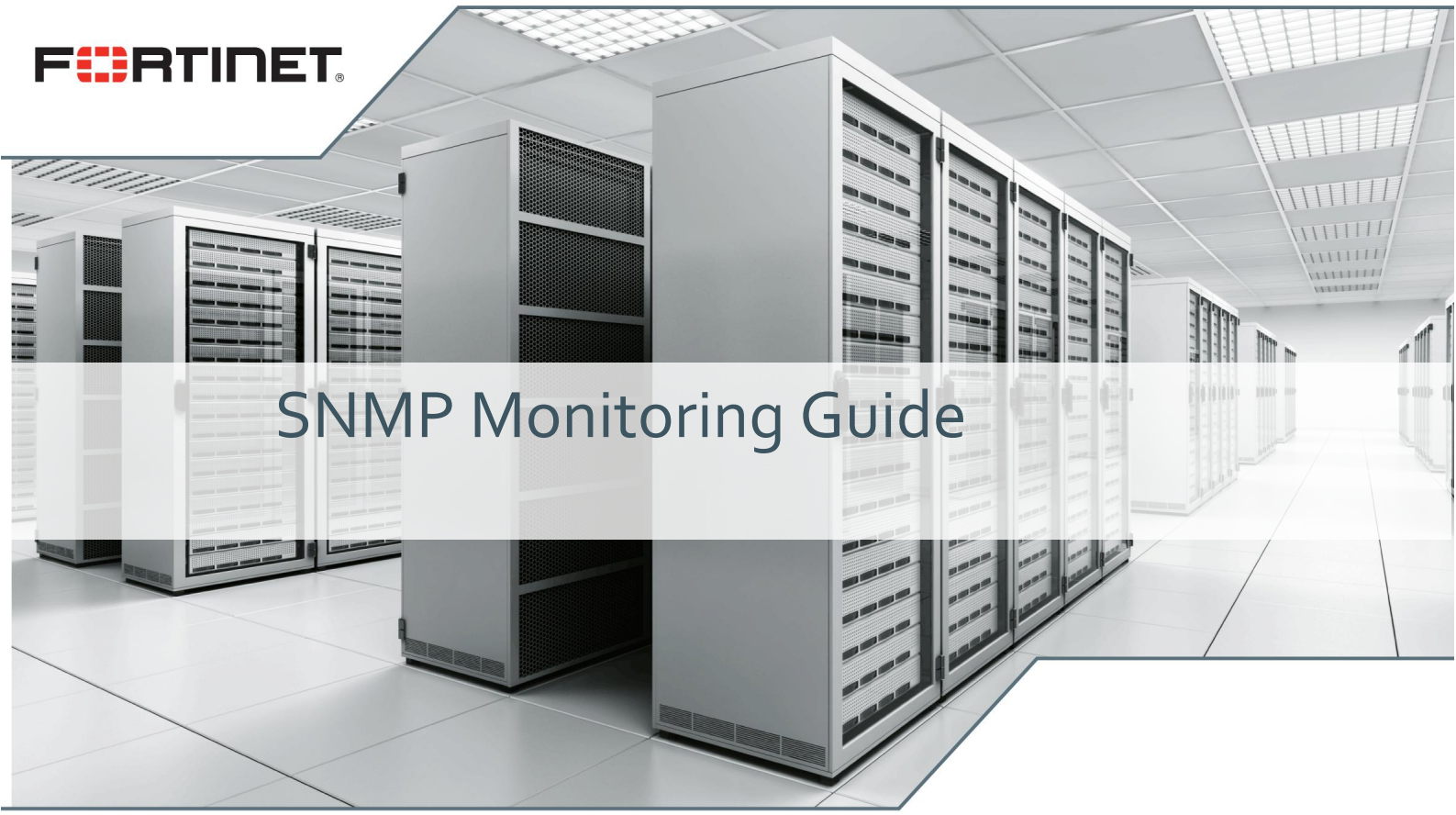


SNMP Monitoring Guide

SNMP Monitoring Fortinet Appliances

FortiGate
FortiAnalyzer
FortiManager

Document Revision History

Version	Date	Author	Status	Comment
1.00	18.10.2012	Alida de Beer	First Draft	
1.06	19.02.2013	Martin Adamini	New chapter	Configuring a FortiAnalyzer for Custom SNMP Traps with log-based alerts
1.07	09.07.2014	Sabine Kerjean		Minor changes

1. Background

Introduction

The purpose of this document is to provide recommendations for SNMP monitoring of Fortinet appliances.

Something to keep in mind is that each network is different. And the use of each device in a network can be different. The Best Practice will be to create a Baseline for each network device. With a defined base-line one should start to investigate as soon as there is a deviation of 10% or more from the baseline.

To create this Baseline SNMP monitoring should be done for a long enough period to be able to define "normal" behaviour. The period that comes to mind is at least one month but this depends on the network and the daily variation. The interval between SNMP queries should be in the order of 5 minutes in order to have updated information without too much strain on the device.

Base-lining is not a static process it should be done with regular intervals and the current Baseline should be updated.

SNMPv3 has Authorization and Encryption and is more secure than SNMPv1 or v2. The suggestion would be to use SNMPv3 in the network for SNMP queries as well as traps.

Technical documentation for all Fortinet appliances and software can be located at http://doc.fortinet.com.

Scope of Document

All of the recommendations provided are specifically based upon the latest 4.3.x firmware release

2. Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as RFCs 1213 and 2665. The support for these RFCs includes parts of RFC 2665 (Ethernet-like MIB) and those elements of RFC 1213 (MIB II) that apply to the FortiGate unit configuration.

There are two MIB files for all FortiGate appliances;

- The Fortinet CORE MIB contains traps, fields and information that are common to all Fortinet products.
- The FortiGate MIB contains traps, fields and information that are specific to FortiGate units. Each Fortinet appliance has its own MIB file.

You can download these two MIB files via the Support Portal. Log-in the Support portal with username and password is needed.

https://support.fortinet.com/

On the Customer Service Support page - Click on Download - On the firmware Images Page click on the device you need the MIB's for. In this case Fortigate click on the version V4.00 then CORE MIB

For more information on how to download the MIB files look at Knowledge Base (KB)

http://kb.fortinet.com

These articles are a good start.

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=11607&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=39332098&stateId=0%200%2039330427

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD30891&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=39332098&stateId=0%200%2039330427

Your SNMP manager may already include standard and private MIBs in a compiled database. If this is not the case you need to download and compile the standard MIB2 files. Afterwards you will need to add the Fortinet Core and proprietary MIBs to this database to view Fortinet specific information

SNMPv3 with authentication and security level defined will assure encryption of the SNMP queries and replies

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The propriety Fortinet MIB includes all system configuration and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiGate unit configuration settings and receive traps from the FortiGate SNMP agent.
FORTINET-FORTIGATE-MIB.mib	The FortiGate SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity.
RFC-2665 (Ethernet-like MIB)	The FortiGate SNMP agent supports Ethernet-like MIB information with the following exception. • No support for the dot3Tests and dot3Errors groups.

3. FortiGate Traps

An SNMP manager can request information from the FortiGate's SNMP agent, or the SNMP agent can send traps when certain pre-defined events occur.

To receive FortiGate device SNMP traps, you must load and compile the *FORTINETCORE- MIB* and *FORTINET-FORTIGATE-MIB* into your SNMP manager. All traps sent include the trap message as well as the FortiGate unit serial number (*fnSysSerial*) and hostname (*sysName*).

The tables in this section include information about SNMP traps and variables. These tables have been included to help you locate the object identifier number (OID), trap message, and trap description of the Fortigate trap or variable you require.

The name of the table indicates if the trap is located in the Fortinet MIB or the FortiGate MIB. The Trap Message column includes the message included with the trap as well as the SNMP MIB field name to help locate information concerning the trap.

Traps starting with fn such as *fnTrapCpuThreshold* are defined in the Fortinet MIB. Traps starting with fg such as *fgTrapAvVirus* are defined in the FortiGate MIB.

The object identifier (OID) is made up of the number at the top of the table with the index then added at the end. For example if

- the OID is 1.3.6.1.4.1.12356.1.3.0 and the index is 4
- the full OID is 1.3.6.1.4.1.12356.1.3.0.4

The OID and the name of the object allow SNMP managers to refer to the specific fields and traps from the Fortinet and FortiGate MIBs.

Indented rows are fields that are part of the message or table associated with the preceding row.

The following tables are defined:

- Generic Fortinet traps (OID 1.3.6.1.4.1.12356.1.3.0)
- System traps (OID 1.3.6.1.4.1.12356.1.3.0)
- FortiGate VPN traps (OID 1.3.6.1.4.1.12356.1.3.0)
- FortiGate HA traps (OID 1.3.6.1.4.1.12356.1.3.0)

Generic Fortinet traps (OID 1.3.6.1.4.1.12356.1.3.0)

Index	Trap message	Description
.1	ColdStart	Standard traps as described in RFC 1215
.2	WarmStart	
.3	LinkUp	
.4	LinkDown	

System traps (OID1.3.6.1.4.1.12356.1.3.0)

Index	Trap message	Description
.101	CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds 80%. This threshold can be set in the CLI using config system snmp sysinfo, set trap-high-cpu-threshold.

.102	Memory low	(fnTrapMemThreshold) Memory usage exceeds 90%. This threshold can be set in the CLI using config system snmp sysinfo, set trap-low-memory-threshold.
.103	Log disk too full	(fnTrapLogDiskThreshold) Log disk usage has exceeded the configured threshold. Only available on devices with log disks. This threshold can be set in the CLI using config system snmp sysinfo, set trap-log-full-threshold.
.104	Temperature too high	(fnTrapTempHigh) A temperature sensor on the device has exceeded its threshold. It should be noted that not all devices have thermal sensors, you need to verify the manual for specifications
105	Voltage outside acceptable range	(fnTrapVoltageOutOfRange) Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
.106	Power supply failure	(fnTrapPowerSupplyFailure) Power supply failure detected. Available on some devices which support redundant power supplies.
.201	Interface IP change	(fnTrapIpChange) The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE

FortiGate VPN traps (OID1.3.6.1.4.1.12356.1.3.0)

Index	Trap message	Description
.301	VPN tunnel is up (fgTrapVpnTunUp)	An IPSec VPN tunnel has started
.302	VPN tunnel down (fgTrapVpnTunDown)	An IPSec VPN tunnel has shut down.
	Local gateway address (fgVpnTrapLocalGateway)	Address of the local side of the VPN tunnel. This information is associated with both of the VPN tunnel traps. (OID1.3.6.1.4.1.12356.101.12.3.2)
	Remote gateway address (fgVpnTrapRemoteGateway)	Address of remote side of the VPN tunnel. This information is associated with both of the VPN tunnel traps. (OID1.3.6.1.4.1.12356.101.12.3.2)

FortiGate HA traps (OID1.3.6.1.4.1.12356.1.3.0)

Index	Trap message	Description
.401	HA switch (fgTrapHaSwitch)	The specified cluster member has transitioned from a slave role to a master role.
.402	HA State Change (fgTrapHaStateChange)	The trap sent when the HA cluster member changes its state.
.403	HA Heartbeat Failure (fgTrapHaHBFail)	The heartbeat failure count has exceeded the configured threshold.
.404	HA Member Unavailable (fgTrapHaMemberDown)	An HA member becomes unavailable to the cluster.
.405	HA Member Available (fgTrapHaMemberUp)	An HA member becomes available to the cluster.
	(fgHaTrapMemberSerial)	Serial number of an HA cluster member. Used to identify the origin of a trap when a cluster is configured. (OID1.3.6.1.4.1.12356.101.13.3.1)

4. FortiGate MIB Fields

The FortiGate MIB contains fields which give access to FortiGate status information. The tables below list the names of the MIB fields and describe the status information available for each one.

You can view more details about the information available for all FortiGate MIB fields by compiling the *FORTINET-CORE-MIB.mib* and *FORTINETFORTIGATE- MIB.mib* files into your SNMP manager and browsing the MIB fields on your computer.

To help locate a field, the object identifier (OID) number for each table of fields has been included. The OID number for a field is that field's position within the table, starting at 0.

For example *fnSysVersion* has an OID of 1.3.6.1.4.1.12356.2.

The following tables include

- FortiGate HA MIB Information fields (OID 1.3.6.1.4.1.12356.101.13.1)
- FortiGate HA unit stats fields (OID 1.3.6.1.4.1.12356.101.13.2)
- FortiGate Administrator accounts (OID 1.3.6.1.4.1.12356.101)
- FortiGate Virtual domains (OID 1.3.6.1.4.1.12356.101.3.1)
- FortiGate Virtual domain table entries (OID 1.3.6.1.4.1.12356.101.3.2.1.1)
- FortiGate Active IP sessions table (OID 1.3.6.1.4.1.12356.101.11.2.1.1)
- FortiGate Firewall policy statistics table (OID 1.3.6.1.4.1.12356.101.5.1.2.1.1)
- FortiGate Dialup VPN peers (OID 1.3.6.1.4.1.12356.101.12.2.1.1)
- FortiGate VPN Tunnel table (OID 1.3.6.1.4.1.12356.101.12.2.2.1)

Index	MIB field	Description
.1	fgHaSystemMode	High-availability mode (Standalone, A-A or A-P).
.2	fgHaGroupId	HA cluster group ID.
.3	fgHaPriority	HA clustering priority (default - 127).
.4	fgHaOverride	Status of the master override flag.
.5	fgHaAutoSync	Status of an automatic configuration synchronization.
.6	fgHaSchedule	Load balancing schedule for cluster in Active-Active mode.
.7	fgHaGroupName	HA cluster group name.
.8	fgHaTrapMemberSerial	Serial number of an HA cluster member.

FortiGate HA unit stats fields (OID 1.3.6.1.4.1.12356.101.13.2)

Index	MIB field	Description
	fgHaStatsTable	Statistics for the individual FortiGate unit in the HA cluster.
.1	fgHaStatsIndex	The index number of the unit in the cluster

.2	fgHaStatsSerial	The FortiGate unit serial number.
.3	fgHaStatsCpuUsage	The current FortiGate unit CPU usage (%).
.4	fgHaStatsMemUsage	The current unit memory usage (%).
.5	fgHaStatsNetUsage	The current unit network utilization (Kbps).
.6	fgHaStatsSesCount	The number of active sessions.
.7	fgHaStatsPktCount	The number of packets processed.
.8	fgHaStatsByteCount	The number of bytes processed by the FortiGate unit
.9	fgHaStatsIdsCount	The number of attacks that the IPS detected in the last 20 hours.
.10	fgHaStatsAvCount	The number of viruses that the antivirus system has detected in the last 20 hours.
.11	fgHaStatsHostname	Hostname of HA Cluster's unit.

FortiGate Administrator accounts (OID 1.3.6.1.4.1.12356.101)

Index	MIB field	Description
.1	fgAdminIdleTimeout	Idle period after which an administrator is automatically logged out of the system.
.2	fgAdminLcdProtection	Status of the LCD protection, either enabled or disabled.
	fgAdminTable	fgAdminVdom The virtual domain the administrator belongs to. (OID 1.3.6.1.4.1.12356.101.6.1.2.1.1.1)

FortiGate Virtual domains (OID 1.3.6.1.4.1.12356.101.3.1)

Index	MIB field	Description
	fgVdInfo	FortiGate unit Virtual Domain related information.
.1	fgVdNumbe	The number of virtual domains configured on this FortiGate unit.
.2	fgVdMaxVdoms	The maximum number of virtual domains allowed on the FortiGate unit as allowed by hardware or licensing.
.3	fgVdEnabled	Whether virtual domains are enabled on this FortiGate unit.

FortiGate Virtual domain table entries (OID 1.3.6.1.4.1.12356.101.3.2.1.1)

Index	MIB field	Description
	fgVdTable.fgVdEntry	Table of information about each virtual domain—each virtual domain has an

		fgVdEntry. Each entry has the following fields.
.1	fgVdEntIndex	Internal virtual domain index used to uniquely identify entries in this table. This index is also used by other tables referencing a virtual domain.
.2	fgVdEntName	The name of the virtual domain.
.3	fgVdEntOpMode	Operation mode of this virtual domain - either NAT or Transparent.

FortiGate Active IP Sessions Table (OID 1.3.6.1.4.1.12356.101.11.2.1.1)

Index	MIB field	Description
.1	fgIpSessIndex	The index number of the IP session within the fgIpSessTable table
.2	fgIpSessProto	The IP protocol the session is using (IP, TCP, UDP, etc.).
.3	fgIpSessFromAdd	The source IPv4 address of the active IP session.
.4	fgIpSessFromPort	The source port of the active IP session (UDP and TCP only).
.5	fgIpSessToAddr	The destination IPv4 address of the active IP session.
.6	fgIpSessToPort	The destination port of the active IP session (UDP and TCP only).
.7	fgIpSessExp	The number of seconds remaining until the sessions expires (if idle).
.8	fgIpSessVdom	Virtual domain the session is part of. Corresponds to the index in *fgVdTable*.
	fgIpSessStatsTable	IP Session statistics table for the virtual domain.
	fgIpSessStatsEntry. fgIpSessNumber	Total sessions on this virtual domain. (OID 1.3.6.1.4.1.12356.101.11.2.1.2.1.1)

FortiGate Firewall policy statistics table (OID 1.3.6.1.4.1.12356.101.5.1.2.1.1)

Index	MIB field	Description
	fgFwPolicyStatsTable.fg FwPolicyStatsEntry	Entries in the table for firewall policy statistics on a virtual domain
.1	fgFwPolicyID	Firewall policy ID. Only enabled policies are available for querying. Policy IDs are only unique within a virtual domain.
.2	fgFwPolicyPktCount	Number of packets matched to policy (passed or blocked, depending on policy action). Count is from the time the policy became active.
.3	fgFwPolicyByteCount	Number of bytes matched to policy (passed or blocked, depending on the policy action). The count is from the time the policy became active.

FortiGate Dialup VPN peers (OID 1.3.6.1.4.1.12356.101.12.2.1.1)

Index	MIB field	Description
.1	fgVpnDialupIndex	An index value that uniquely identifies an VPN dial-up peer in the table
.2	fgVpnDialupGateway	The remote gateway IP address on the tunnel.
.3	fgVpnDialupLifetime	VPN tunnel lifetime in seconds.
.4	fgVpnDialupTimeout	Time remaining until the next key exchange (seconds) for this tunnel.
.5	fgVpnDialupSrcBegin	Remote subnet address of the tunnel.
.6	fgVpnDialupSrcEnd	Remote subnet mask of the tunnel.
.7	fgVpnDialupDstAddr	Local subnet address of the tunnel.
.8	fgVpnDialupVdom	The virtual domain this tunnel is part of. This index corresponds to the index in *fgVdTable*.
.9	fgVpnDialUpInOctets	The number of bytes received over the tunnel.
.10	fgVpnDialUpOutOctets	The number of byes send over the tunnel.

VPN Tunnel table (OID 1.3.6.1.4.1.12356.101.12.2.2.1)

Index	MIB field	Description
.1	fgVpnTunEntIndex	An index value that uniquely identifies a VPN tunnel within the VPN tunnel table.
.2	fgVpnTunEntPhase1Name	The descriptive name of the Phase1 configuration for the tunnel.
.3	fgVpnTunEntPhase2Name	The descriptive name of the Phase2 configuration for the tunnel.
.4	fgVpnTunEntRemGwyIp	The IP of the remote gateway used by the tunnel.
.5	fgVpnTunEntRemGwyPort	The port of the remote gateway used by the tunnel, if it is UDP
.6	fgVpnTunEntLocGwyIp	The IP of the local gateway used by the tunnel
.7	fgVpnTunEntLocGwyPort	The port of the local gateway used by the tunnel, if it is UDP.
.8	fgVpnTunEntSelectorSrcBeginIp	Beginning of the address range of the source selector.
.9	fgVpnTunEntSelectorSrcEndIp	Ending of the address range of the source selector.
.10	fgVpnTunEntSelectorSrcPort	Source selector port.
.11	fgVpnTunEntSelectorDstBeginIp	Beginning of the address range of the destination Selector
.12	fgVpnTunEntSelectorDstEndIp	Ending of the address range of the destination selector.
.13	fgVpnTunEntSelectorDstPort	Destination selector port.
.14	fgVpnTunEntSelectorProt	Protocol number for the selector.
.15	fgVpnTunEntLifeSecs	Lifetime of the tunnel in seconds, if time based lifetime is used.
.16	fgVpnTunEntLifeBytes	Lifetime of the tunnel in bytes, if byte transfer based lifetime is used.
.17	fgVpnTunEntTimeout	Timeout of the tunnel in seconds.
.18	fgVpnTunEntInOctets	Number of bytes received on the tunnel.
.19	fgVpnTunEntOutOctets	Number of bytes sent out on the tunnel.
.20	fgVpnTunEntStatus	Current status of the tunnel - either up or

		down.
.21	fgVpnTunEntVdom	Virtual domain the tunnel belongs to. This index corresponds to the index used in *fgVdTable*.

5. Specific SNMP Monitoring of a FortiGate

Physical Errors per Interface

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

ifInErrors	.1.3.6.1.2.1.2.2.1.14
ifInDiscards	.1.3.6.1.2.1.2.2.1.13
ifOutDiscards	.1.3.6.1.2.1.2.2.1.19
ifOutErrors	.1.3.6.1.2.1.2.2.1.20

Suggested KPI: Not more than 1% of total port utilization.

Traffic per Interface

For accelerated ports (NP2, NP4 etc) SNMP monitoring can be performed ONLY for the physical port, not for the VLAN interfaces. On non-accelerated ports the traffic can be monitored for VLAN interfaces.

Something else to keep in mind when adding or deleting a VLAN the ifIndex is modified. The SNMP ifIndex indicator needs to be modified after a VLAN modification. For example poll the ifIndex of the interface table and delete the interface vlan1. In this example the ifIndex for vlan2 is modified from 30 to 29.

Name/OID: ifDescr.28; Value (OctetString): ssl.root
Name/OID: ifDescr.29; Value (OctetString): vlan1
Name/OID: ifDescr.30; Value (OctetString): vlan2 <====

Deleted
Name/OID: ifDescr.28; Value (OctetString): ssl.root
Name/OID: ifDescr.29; Value (OctetString): vlan2 <====

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

ifInOctets	.1.3.6.1.2.1.2.2.1.10
ifOutoctets	.1.3.6.1.2.1.2.2.1.1

CPU Usage

Many of the FortiGate appliances have more than one CPU it is therefore important to monitor each Processor.

The SNMP query to issue to identify the number of CPU's in the device

Number of processors : FORTINET-FORTIGATE-MIB.iso.org.dod.internet

fgProcessorCount .1.3.6.1.4.1.12356.101.4.4.1.0

Usage per processor

FORTINET-FORTIGATE-MIB.iso.org.dod.internet

fgProcessorUsage .1.3.6.1.4.1.12356.101.4.4.2.1.2.<processor_id> with <processor_id> =1,2,3 …
fgprocessorModuleCount

Example
1.3.6.1.4.1.12356.101.4.4.2.1.2.1 => CPU0 usage average over the last minute
1.3.6.1.4.1.12356.101.4.4.2.1.2.2 => CPU1 usage average over the last minute
1.3.6.1.4.1.12356.101.4.4.2.1.2.3 => CPU2 usage average over the last minute
1.3.6.1.4.1.12356.101.4.4.2.1.2.4 => CPU3 usage average over the last minute

Or if more accuracy is required the average over the last 5 seconds can be polled

1.3.6.1.4.1.12356.101.4.4.2.1.3.1 => CPU0 usage average over the last 5 seconds
1.3.6.1.4.1.12356.101.4.4.2.1.3.2 => CPU1 usage average over the last 5 seconds
1.3.6.1.4.1.12356.101.4.4.2.1.3.3 => CPU2 usage average over the last 5 seconds
1.3.6.1.4.1.12356.101.4.4.2.1.3.4 => CPU3 usage average over the last 5 seconds

Suggested KPI: Max 70 % for each CPU during peak traffic duration with possible spikes of more than 90% not longer than 4 seconds

Number of packets that goes thru a processor

FORTINET-FORTIGATE-MIB.iso.org.dod.internet
fgProcessorPktRxCount .1.3.6.1.4.1.12356.101.4.4.2.1.6
fgProcessorPkTxCount .1.3.6.1.4.1.12356.101.4.4.2.1.7

Number of packets dropped in the CPU

FORTINET-FORTIGATE-MIB.iso.org.dod.internet
fgProcessorPktDroppedCount .1.3.6.1.4.1.12356.101.4.4.2.1.8

Suggested KPI: No constant amount of dropped packets more than 1% of fgProcessorPktRxCount

Memory Usage

The memory of the FortiGate is divided into zones there is a high memory and low memory zone. All kernel data structures are located in the low memory zone. Usage information is available for Overall memory and Low memory. **Regular conserve mode** is triggered when the overall memory is getting low. It could be a process that consumes too much memory (rate case) or high usage of the shared memory buffers**. Kernel conserve mode** is triggered when the amount of Low memory is getting to low.

Please refer to this document for more information

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD33103&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=39636481&stateId=0%200%2039638350

FORTINET-FORTIGATE-MIB.iso.org.dod.internet

Overall Memory

fgSysMemUsage .1.3.6.1.4.1.12356.101.4.1.4.0
fgSysMemCapacity .1.3.6.1.4.1.12356.101.4.1.5.0

Suggested KPI : 65% of constant Overall memory usage.

Low Free Memory (LowFree)

fgSysLowmemUsage .1.3.6.1.4.1.12356.101.4.1.9.0
fgSysLowmemCapacity .1.3.6.1.4.1.12356.101.4.1.10.0

The device will enter the Kernel conserve mode when there is 20% of Low Total left

Suggested KPI : 65% of constant Low memory usage

Concurrent sessions

FORTINET-FORTIGATE-MIB.iso.org.dod.internet
fgSysSessCount .1.3.6.1.4.1.12356.101.4.1.8.0

Suggested KPI : 70% of the Product data sheet for the specific model

HA Information

FORTINET-FORTIGATE-MIB.iso.org.dod.internet
fgHaStatsSerial .1.3.6.1.4.123456.101.13.2.1.1.1.2.1
fgHaStatsHostname .1.3.6.1.4.1.12356.101.13.2.1.1.11
fgHaStatsMemusage .1.3.6.1.4.1.12356.101.13.2.1.1.4
fgHaStatsSessCount .1.3.6.1.4.1.12356.101.13.2.1.1.6
fgHAStatsPktCount .1.3.6.1.4.1.12356.101.13.2.1.1.7
fgHaStatsNetUsage .1.3.6.1.4.1.12356.101.13.2.1.1.5

6. Configuring a FortiGate for SNMP Traps and Monitoring

Methods to query a SLAVE in a HA cluster

On the FORTIGATE there are two possible ways to do SNMP queries to the slave in a HA cluster. One method is explained in the following KB article

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=13077&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=39632294&stateId=0%200%2039634080

The syntax for this SNMP get command is:

snmpget -v2c -c <community_name>-<fgt_serial> <address_ipv4> <OID>

<community_name> is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. All units in the cluster have the same community name. The most commonly used community name is public.

<fgt_serial> is the serial number of any cluster unit. For example FGT4002803033172. You can specify the serial number of any unit in the cluster, including the primary unit, to get information from the specified unit.

<address_ipv4> is the IP address of the FortiGate interface that the SNMP manager connects to.

<oid> is the object identifier for the MIB field.

If the specified serial number matches the serial number of a subordinate unit, the SNMP get request is sent over the HA heartbeat link to the subordinate unit. After processing the request, the subordinate unit sends the reply back over the HA heartbeat link back to the primary unit. The primary unit then forwards the response back to the SNMP manager.

If the serial number matches the serial number of the primary unit, the SNMP get request is processed by the primary unit. You can actually add a serial number to the community name of any SNMP get request

The second method to monitor both the Master and the Slave in a HA configuration is to configure a HA-mgmt interface. In order to enable the slave to reply to SNMP queries a different IP address and administrative access should be configured on an interface for each unit in the cluster.

To monitor each cluster unit using SNMP, just add the IP address of each cluster unit's reserved management interface to the SNMP server configuration. If your SNMP configuration includes SNMP users with user names and passwords you must also enable HA direct management for all SNMP users. Enable direct management of cluster members in the cluster SNMP configuration

```
Config  system ha
  set ha-mgmt-status enable
  set ha-mgmt-interface <interface-name>
  set ha-mgmt-interface-gateway x.x.x.x
end
```

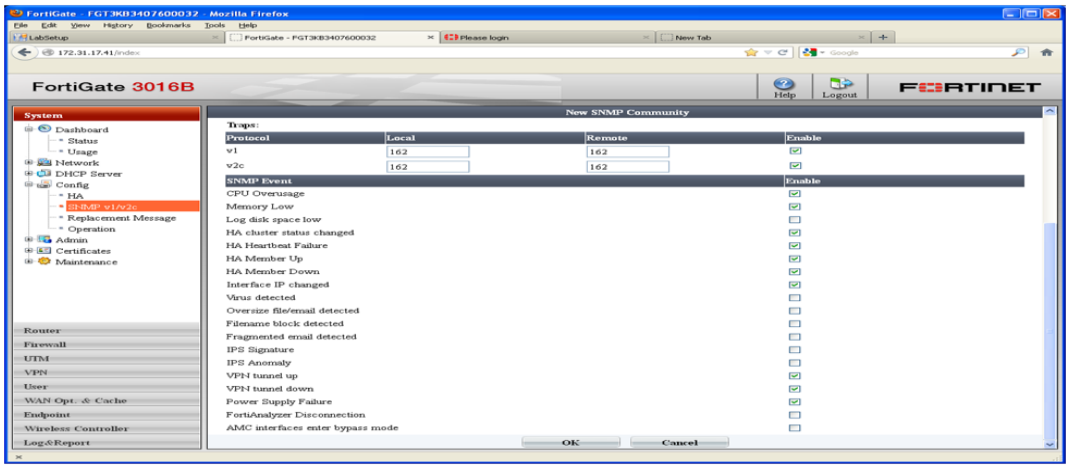
The reserved management interface default route is not synchronized to other cluster units.

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD32214&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=39336444&stateId=0%200%2039334829

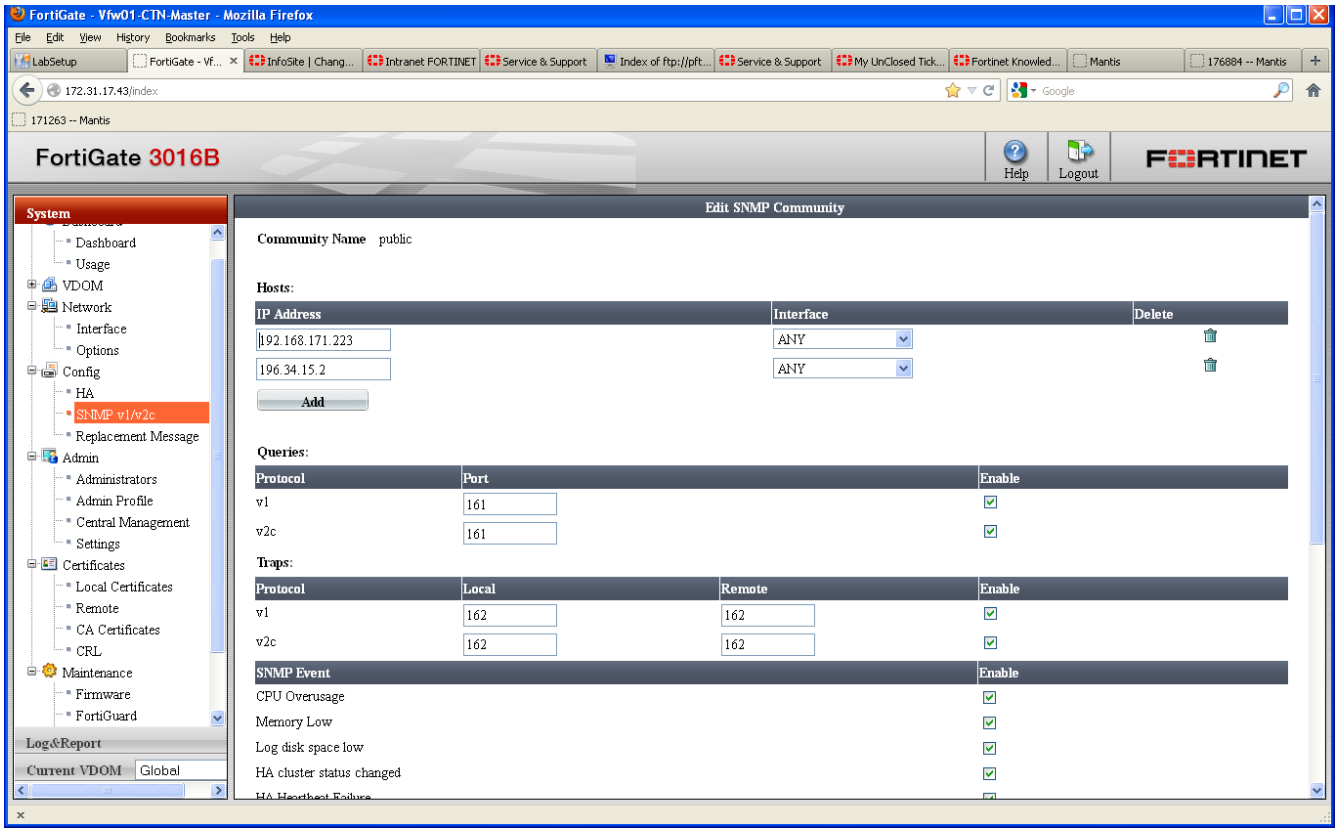
For both methods one needs to enable SNMP on an Interface.

```
config system interface
   edit "portx"
      set vdom "Management Vdom  normally root"
      set ip x.x.x.x/y.y.y.y
      set allowaccess  snmp
```

GUI Configuration of Traps on the FortiGate



GUI Configuration for SNMP monitoring on the FortiGate



CLI configuration for all SNMP queries and Traps on a FortiGate

Need to enable SNMP agent

```
config system snmp sysinfo
   set status enable
   next
end
```

Configure the SNMPv2 Community if version 2 is used

```
config system snmp community
   edit 1
      set events cpu-high mem-low intf-ip vpn-tun-up vpn-tun-down ha-
switch ha-hb-failure ha-member-up ha-member-down power-supply-failure
         config hosts
            edit 1
               set ha-direct enable
               set interface “InterFaceOfSNMPQuery”
               set ip x.x.x.x
               set source-ip 0.0.0.0
            next
         end
      set name "ReadCommunityString"
      set query-v1-port 161
      set query-v1-status enable
```

```
        set query-v2c-port 161
        set query-v2c-status enable
        set status enable
        set trap-v1-lport 162
        set trap-v1-rport 162
        set trap-v1-status enable
        set trap-v2c-lport 162
        set trap-v2c-rport 162
        set trap-v2c-status enable
    next
end
```

Suggestion is to use SNMPv3. Configure SNMPv3 queries and Traps via CLI .

```
config system snmp user
    edit "test"
        set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ha-member-up
ha-member-down ent-conf-change
        set ha-direct enable
        set notify-hosts 192.168.171.233
        unset notify-hosts6
        set queries enable
        set query-port 161
        set security-level auth-priv
        set auth-proto md5
        set auth-pwd ENC AAB2AphhIsKSFeoOXvxLrIeJrsVEzv1c51V8uWdMqa/0DREWJXn8lpo
mdLlz5kaGA4g6IQEa0uH7PTvk9fUe1T+LLX08v3mLs5DQQ0I7u/aonp+m
        set priv-proto des
        set priv-pwd ENC AAB2AphhIsKSFeoOXvxLrIeJrsVEzv1c51V8uWdMqa/0DREWcofB0K1
C8Iz10uH+gWsa10jyW9zde+vdW/dkRBhZKycIIayJ8K/ru+byx91q+dzA
    next
end
```

7. FortiAnalyzer MIB Fields

The FortiAnalyzer support the following MIBs

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices. *Except:* There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, etc.) do not accurately capture all FortiAnalyzer traffic activity. More accurate information can be obtained from the information reported by the FortiAnalyzer MIB.
RFC-2665 (Ethernet-like MIB)	The FortiAnalyzer SNMP agent supports Ethernet-like MIB information except the dot3Tests and dot3Errors groups

The MIB files are located at:

https://support.fortinet.com/

For login to the Technical support page the username and password needed.

On the Customer Service Support page - Click on Download - On the firmware Images Page click on the device you need the MIB's for. FortiAnalyzer in this case click on the version V4.00 then CORE MIB

ftp://support.fortinet.com/FortAnalyzer/v4.00/Core%20MIB/

The FortAnanlyzer MIBS for version 4.2 are available in the 4.0MR2 folder

ftp://support.fortinet.com/FortiAnalyzer/v4.00/4.0MR2/MR2/MIB/

For more information on how to download the MIB files look at Knowledge Base (KB)

http://kb.fortinet.com

8. Specific SNMP monitoring of a FortiAnalyzer

FortiAnalyzer SNMP is read-only: SNMP v1/2 and v3 compliant SNMP managers have read-only access to FortiAnalyzer system information and can receive FortiAnalyzer traps. RFC support includes most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). FortiAnalyzer units also use object identifiers from the Fortinet proprietary MIB.

Physical Errors per Interface

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

ifInErrors	.1.3.6.1.2.1.2.2.1.14
ifInDiscards	.1.3.6.1.2.1.2.2.1.13
ifOutDiscards	.1.3.6.1.2.1.2.2.1.19
ifOutErrors	.1.3.6.1.2.1.2.2.1.20

Suggested KPI: Not more than 1% of total port utilization

Traffic

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

IfInOctets	.1.3.6.1.2.1.2.2.1.10
IfOutOctets	.1.3.6.1.2.1.2.2.1.16

CPU Usage

FORTINET-FORTIANALYZER-MIB.iso.org.dod.internet.private.enterprises.fortinet

Fa300SysCpuUsage	.1.3.6.1.4.1.12356.102.99.2.3.0

Suggested KPI : Max 70 % for CPU during peak traffic duration with possible spikes of more than 90% not longer than 4 seconds

Memory Usage

FORTINET-FORTIANALYZER-MIB.iso.org.dod.internet.private.enterprises.fortinet

Fa300SysmemCapacity	.1.3.6.1.4.1.12356.102.99.2.8.0
Fa300SysmemUsage	.1.3.6.1.4.1.12356.102.99.2.4.0

Suggested KPI : Max 70 % during peak usage

Session Count

FORTINET-FORTIANALYZER-MIB.iso.org.dod.internet.private.enterprises.fortinet

Fa300SysSesCount	.1.3.6.1.4.1.12356.102.99.2.5.0
Fa300IpSessProto	.1.3.6.1.4.1.12356.102.2.2.1.1.2.1

Suggested KPI : Max 70 % during peak usage

Disk Usage

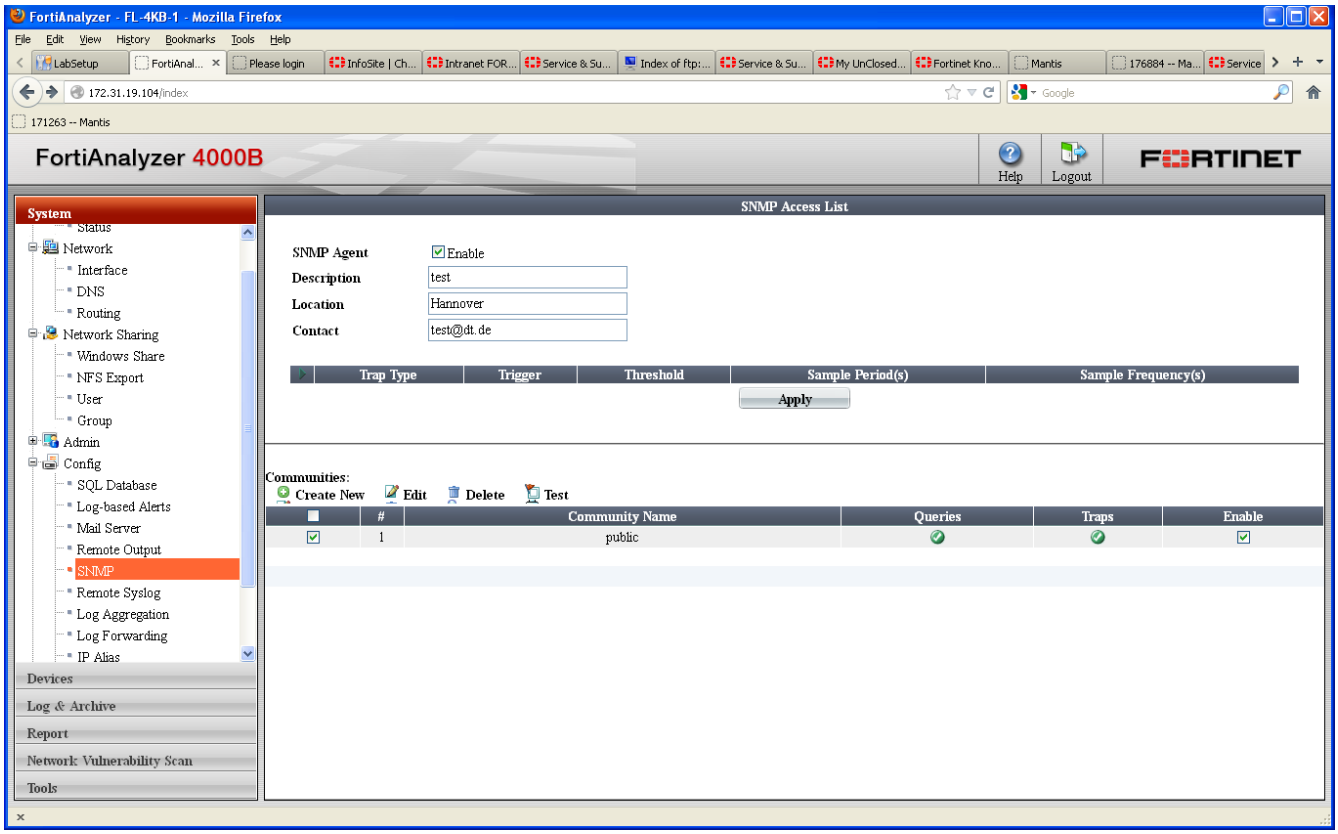
FORTINET-FORTIANALYZER-MIB.iso.org.dod.internet.private.enterprises.fortinet

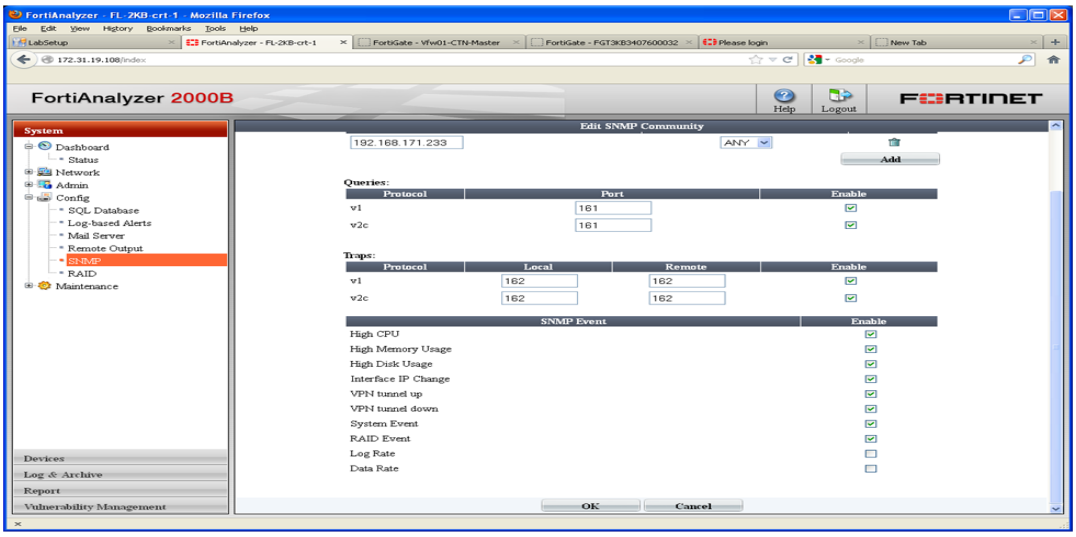
Fa300SysDiskCapacity	.1.3.6.1.4.1.12356.102.99.2.6.0
Fa300SysDiskUsage	.1.3.6.1.4.1.12356.102.99.2.7.0

Suggested KPI: Max 70% of usable disk space

9. Configuring a FortiAnalyzer for SNMP Traps and Monitoring

GUI configuration for SNMP traps and monitoring





CLI configuration for SNMPv2 Queries and Traps

```
config system snmp community
   edit "ReadCommunityString"
```

```
        config hosts
          edit 1
            set ip 192.168.171.233
          next
        end
      set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down system_event raid
  next
end

config system snmp sysinfo
  set agent enable
end
```

Suggestion is to use SNMPv3 Queries and Traps. The CLI configuration as follows

```
config system snmp user
  edit "test"
    set notify-hosts 172.168.171.233
    set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down sys
tem_event raid power-supply-failure power-supply-restored log-rate data-rate
    set security-level auth-priv
    set auth-proto md5
    set auth-pwd ENC ablUWJq0vyNlybw2fUQokvwMFNekxjcGZfWAiQwHuqHuEOGUTyn7Wup
APVeDTdCL
    set priv-proto des
    set priv-pwd ENC eddcb0vcdKAABeOzhte0J1780Q9mhoa2H40SRalqEYWRIh+gOMd82lg
CdbDV2LGe
  next
end
```

10. Configuring a FortiAnalyzer for Custom SNMP Traps with log-based alerts

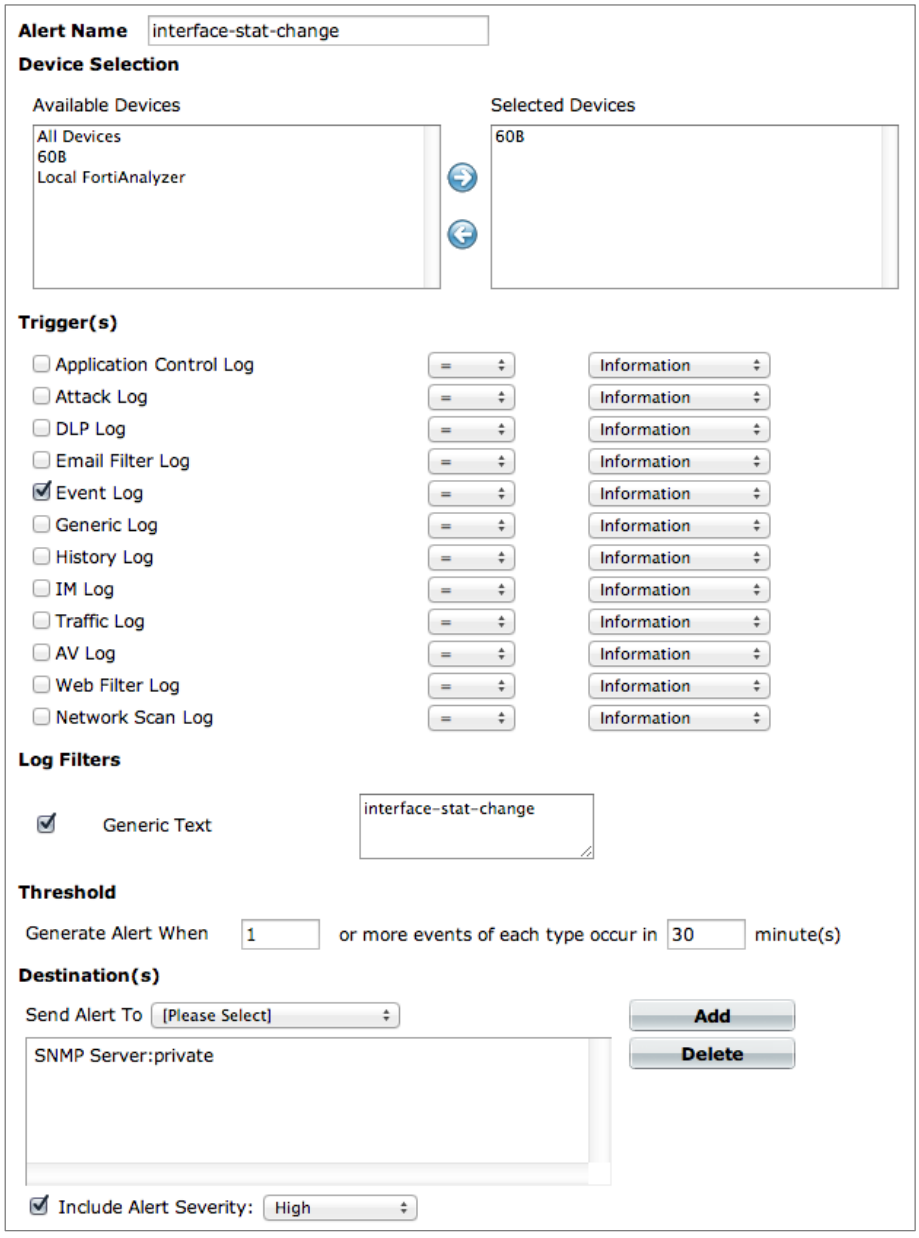
Detailed information can be found in the FortiAnalyzer Setup and Administration Guide starting from page 110.

http://docs.fortinet.com/fa/fortianalyzer-admin-40-mr3.pdf

SNMP must be configured for this to work. (Chapter 9)

The following example shows how one can send traps with a FortiAnalyzer for interface status changes on a Fortigate:

Under System -> Config -> Log-based Alerts:



11. FortiManager MIB Fields

The FortiManager support the following MIBs

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FORTINETFORTIMANAGERMIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. No support for the EGP group from MIB II (RFC1213, section 3.11 and 6.10). Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (EthernetlikeMIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

The MIB files are located at:

https://support.fortinet.com/

In order to download the MIB login to the Technical support page with username and password.

On the Customer Service Support page - Click on Download - On the firmware Images Page click on the device you need the MIB's for. Fortimanager in this case click on the version V4.00 then CORE MIB

ftp://support.fortinet.com/FortiManager/v4.00/Core%20MIB/

The FortManager MIBS for version 4.2 are available in the 4.0MR2 folder

ftp://support.fortinet.com/FortiManagerr/v4.00/4.0MR2/MR2/MIB/

One can find more information on how to download the MIB files in Knowledge Base (KB)

http://kb.fortinet.com

12. Specific SNMP Monitoring of a FortiManager

Fortinet device SNMP agents support Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to Fortinet unit configuration.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

Physical Errors per Interface

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

ifInErrors	.1.3.6.1.2.1.2.2.1.14
ifInDiscards	.1.3.6.1.2.1.2.2.1.13
ifOutDiscards	.1.3.6.1.2.1.2.2.1.19
ifOutErrors	.1.3.6.1.2.1.2.2.1.20

Suggested KPI: Not more than 1% of port total utilization

Traffic

RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2

IfInOctets	.1.3.6.1.2.1.2.2.1.10
IfOutOctets	.1.3.6.1.2.1.2.2.1.16

CPU Usage

fnFortiManagerMib.fmSystem.fmSystemInfo

fmSysCpuUsage	.1.3.6.1.4.1.12356.103.2.1.1

Suggested KPI : Max 70 % for each CPU during peak traffic duration with possible spikes of more than 90% not longer than 4 seconds

Memory Usage (Physical)

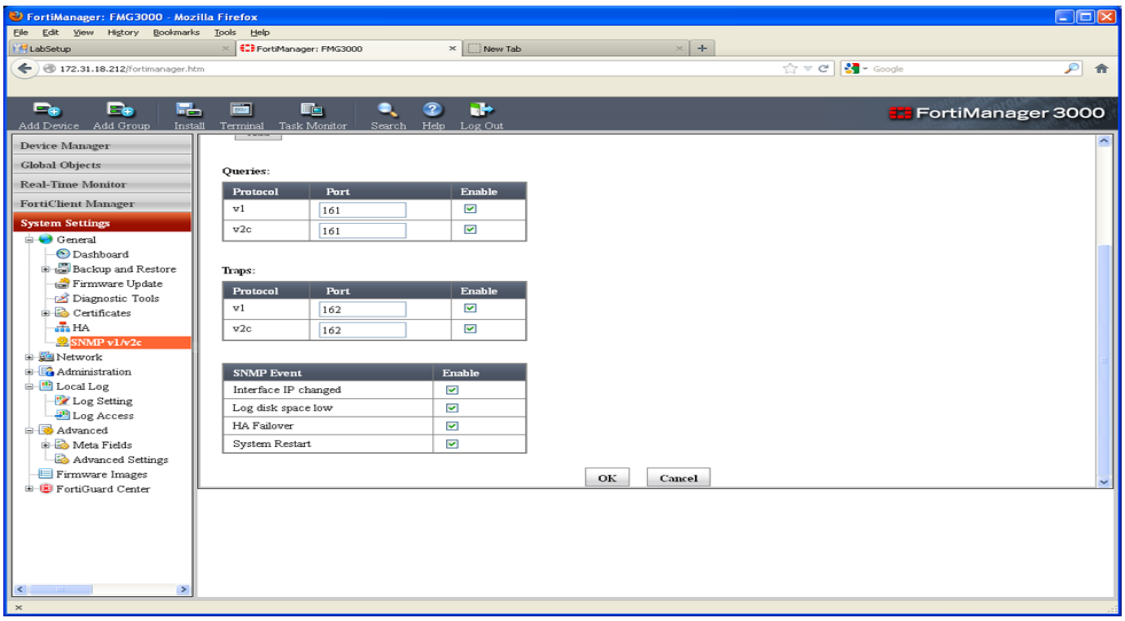
fnFortiManagerMib.fmSystem.fmSystemInfo

fmSysMemUsed	.1.3.6.1.4.1.12356.103.2.1.2

Suggested KPI : Max 70 % during peak usage of fmMemorySize

13. Configuring a FortiManager for SNMP traps and Monitoring

GUI Configuration of a FortiManager for SNMPv2 Queries and Traps



CLI Configuration a FortiManager for SNMP v2 Queries and Traps

Enable the SNMP agent

```
config fmsystem snmp sysinfo
   set status enable
end
```

Configure the SNMP community

```
config fmsystem snmp community
   edit 1
      set events disk_low ha_switch intf_ip_chg sys_reboot
         config hosts
            edit 1
               set ip 192.168.171.233
            next
         end
      set name "ReadCommunityString"
   next
end
```

Suggested SNMPv3 Configuration of a FortiManager for SNMP Queries and Traps

```
config fmsystem snmp user
   edit "test"
      set events disk_low ha_switch intf_ip_chg sys_reboot cpu_high mem_low
      set notify-hosts 192.168.171.233
      set security-level auth-priv
```

```
        set auth-proto md5
        set auth-pwd ENC Tw1DC+lpXEIfKIwo6BLCBUzt1QIo5MNR1zcxSjD0eqQojzbR0Mm2HDK
rMmTdXbnfhu/VSm8a9hD9+QXt1aV27W5MP/o8ysHRMMdy058+mjPtyLXm
        set priv-proto des
        set priv-pwd ENC p4xEK+eqObw0rtzVa5+J9IL5yBCd/UyR/qKeyS6C7+BFBk+Q4spNT13
nIsu4+7xJmClvjX0kDDKt2KWMepCPRbPeQFm3ROYk1ylZ615DuZnd6at5
    next
end
```

Appendix A:
Recommended KPI

Description	Recommended KPI
Physical Errors per Interface	Less than 1% of total traffic
CPU usage	Not more than 70% of CPU capacity
Number of sessions	Less than 70% of the datasheet
Memory usage	Less than 70% of memory capacity
Disk usage	Less than 70% of disk capacity