PAESSLER
THE NETWORK MONITORING COMPANY

HOW TO

How to Securely Monitor a FortiGate Firewall with PRTG

PRTG NETWORK MONITOR

Contents

DISCLAIMER

This is a document created by a PRTG user. I have carefully compiled this information and it is provided to the best of my knowledge. As the solution is not part of PRTG itself, it is **not officially supported by Paessler or PRTG Technical Support.** Yet, we wanted to share it with you as it might be of interest for many PRTG users.

You must also be aware that if you configure any of the parts incorrectly, you may leave yourself open to an intruder gaining access to anything configured within PRTG. This includes User ID's, passwords, IP names, etc. In other words: no warranties are expressed or implied. Paessler, its employees or partners cannot be held liable for any damages that you may incur as a result of following this guide.

Author: Florian Thiele

Website: https://how2itsec.blogspot.com/

My name is Florian Thiele and I'm an IT Security Architect. I have been working with FortiGate firewalls and PRTG for 10 years, and in this guide I provide some steps and references for monitoring your FortiGate Firewalls with PRTG.

Published: 09.11.2018

Introduction

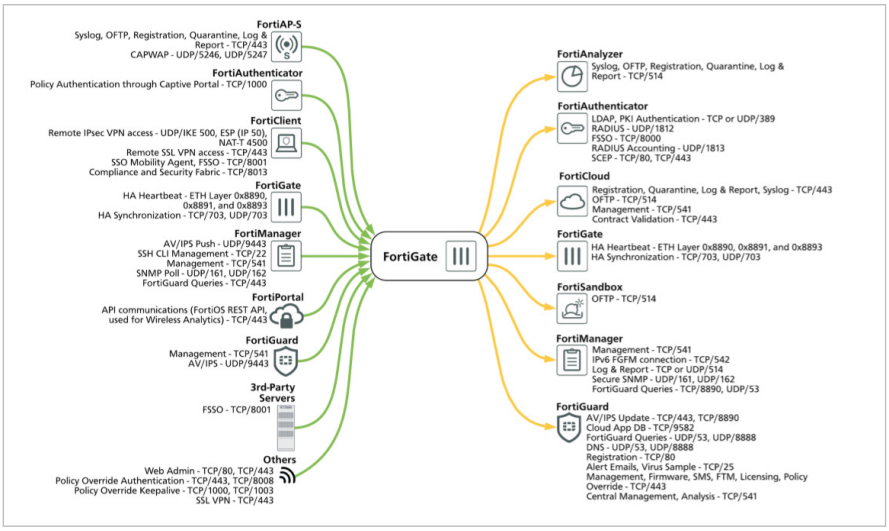
The FortiGate firewall offers a lot of different management interfaces. This article is about the secure and recommended interfaces from 10 years of experience with hundreds of FortiGates and PRTG installations all over the world. There are many more ways to monitor the FortiGate with PRTG but this article focuses only on the ones which really work and are secure.

Overview of Recommended Secure Monitoring Interfaces

The FortiGate firewalls offers the following management-interfaces which are secure:.

Protocol	Secure	Comment	Direction (Default FGT-Port)
SNMPv3 AuthPriv AES+SHA	Encrypted	SNMPv3 AuthPriv is recommended for authenticated and encrypted monitoring of the FGT	PRTG pulls from FGT (UDP:161)
SNMP Trap	Not encrypted	Enables the FortiGate to send information to PRTG	FGT sends to PRTG (UDP:162)
SSH	Encrypted		PRTG pulls from FGT (TCP:22)
HTTPS	Encrypted		PRTG pulls from FGT (TCP:443)
NetFlow	Not encrypted	Only recommended with setups where FortiGate has Network Processes ASIC NP6, NP7 or above. On FGTs without NPs NetFlow is done in CPU, which might cause high CPU utilization	FGT sends to PRTG (UDP?)
Syslog	Not encrypted		FGT sends to PRTG (UDP:514, Syslog Reliable TCP:514)

Overview of all FortiGate Interfaces



A full list of all FortiGate interfaces with a description of them can be found here: https://docs.fortinet.com/d/fortigate-communication-ports-and-protocols-60

Harden Interfaces

IMPORTANT:

- All access to the firewall should be limited to internal interfaces only
- All access to the firewall should be strictly limited to trusted host IPs/IP-networks only
- All unused management access protocols/interfaces should be deactivated
- Only secure protocols should be used (e.g. SSH instead of Telnet, SNMPv3 AuthPriv instead of SNMPv1/v2c,..). Secure encrypted protocols will cause a higher load on PRTG and the firewall, however due to the sensible nature of a firewall, which is often heart of the network backbone, it is highly recommended.
- Consider using two-factor-authentication for administrative login. This is highly recommended for strong authentication. Every FortiGate unit includes two trial tokens for free
- Rename the default admin administrator account, create backup-administrator accounts, use for both complex passwords (length 20+) and keep them in a safe. For regular administrative work use LDAPS authentication with personalized dedicated administrator accounts.

Hardening Guide for FortiOS 5.6:
https://docs.fortinet.com/uploaded/files/3624/fortigate-hardening-your-fortigate-56.pdf

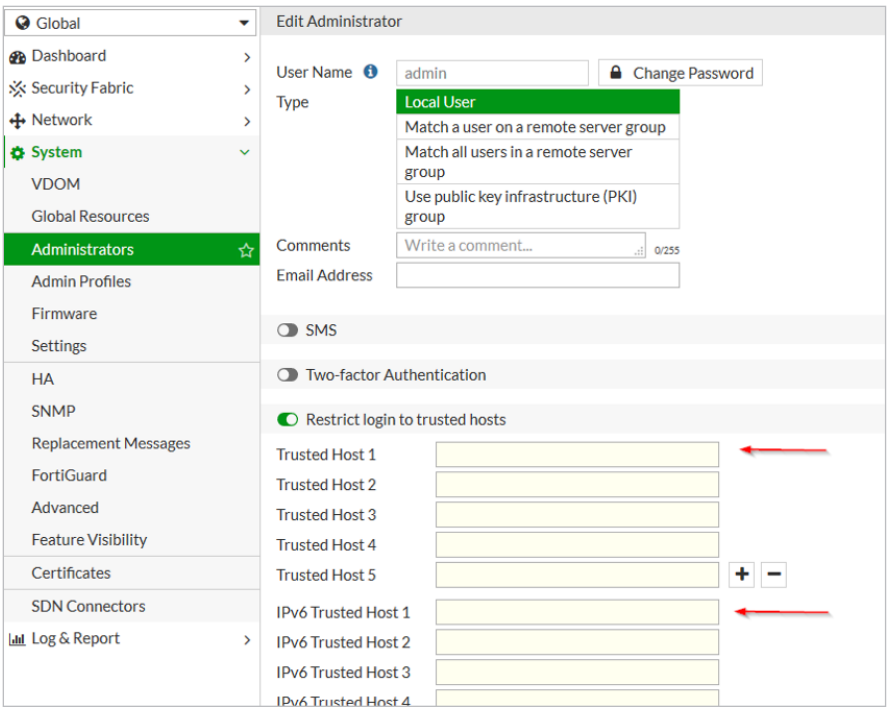
Hardening Guide for FortiOS 5.4:
https://docs.fortinet.com/d/fortigate-hardening-your-fortigate-1

Hardening Guide for FortiOS 5.2:
https://docs.fortinet.com/d/fortigate-hardening-your-fortigate

Fortinet Product Security Incident Response Team:
https://www.fortiguard.com/psirt

Configuring Trusted Hosts

Setting trusted hosts for administrators limits what computers an administrator can login to the FortiGate unit from. When you identify a trusted host, the FortiGate unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to login with the same credentials from any other IP address or any other subnet will be dropped. To ensure the administrator has access from different locations, you can enter up to ten IP addresses or subnets. Ideally, this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields. Trusted hosts are configured when adding a new administrator by going to System > Administrators in the web-based manager and selecting "Restrict login to trusted hosts":



Or config system admin in the CLI:

```
config system admin
    edit "admin-username"
        set trusthost1 "Any IPv4 address or subnet address"
        ip6-trusthost1 "Any IPv6 address"
```

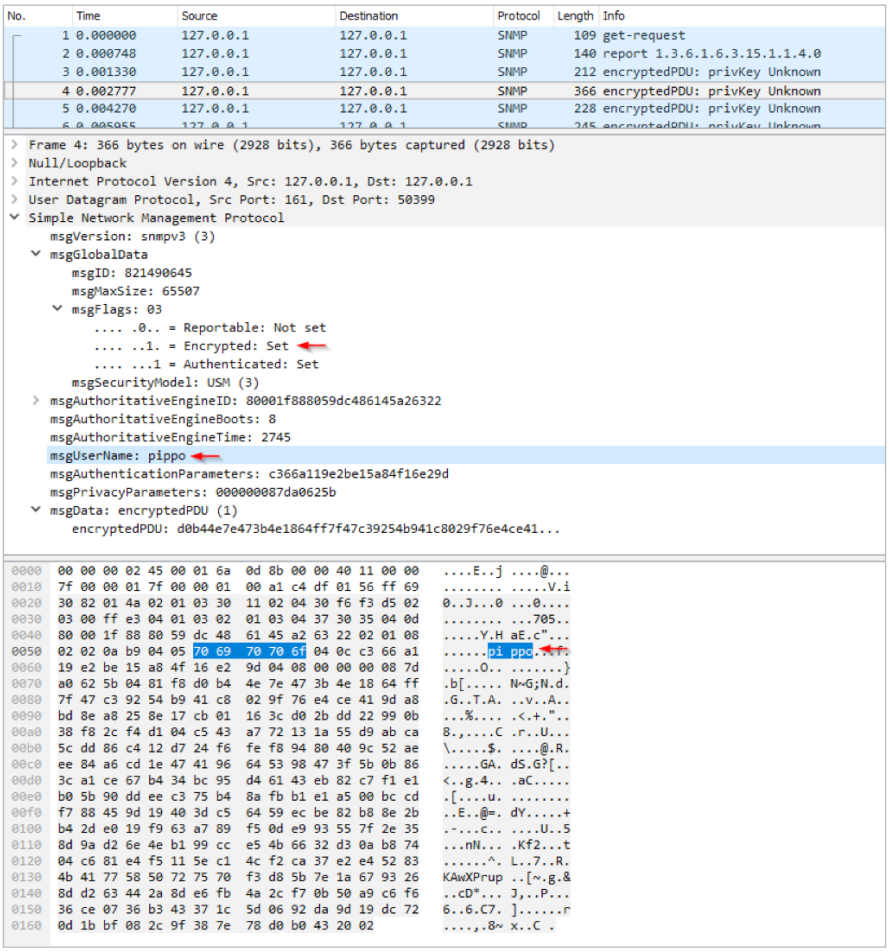
The trusted hosts apply to the web-based manager, ping (keep in mind that your FGT only responds to trusted hosts), SNMP and the CLI when accessed through SSH. CLI access through the console port is not affected. Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

SNMPv3 AuthPriv Monitoring

Depending on the FortiGate size/resources, the amount of sensors and interval of how often you query the FortiGate depends. You should closely monitor the CPU and memory utilization of your device in order to not cause too much of utilization to your device. Some sensors are more important than others, therefore they should be queried more often than others. For example it might not be a good idea to ask for the uptime every 30seconds, but it might be a good idea to check for the interface utilization of your most crucial (vlan-)interfaces like WAN/LAN/DMZ or VPN.

SNMPv3 AuthPriv is recommended for its authentication and encryption. However SNMPv3 AuthPriv will cause a higher load on PRTG and your FortiGate firewall compared to SNMPv1/v2c, which are not encrypted. Due to a firewalls sensivity, it is recommended to only use SNMPv3 AuthPriv.

Do NOT use the same SNMPv3 username, password and key. Instead use 3 different values with more then 20 numbers length, for example TbYrHh7zWiqF88cBcn63. This very important due to the username is sent in plaintext over the network eventhough you chose with AuthPriv authentication and encryption. The following screenshot shows the example of SNMPv3 AuthPriv from wireshark-examples https://wiki.wireshark.org/SampleCaptures#SNMP were you can see although encryption is chosen, the username is sent in plaintext. The whole security would be compromised if you chose the same username, password and/or key for SNMPv3 AuthPriv.



Fortinet SNMP OID-Tree:

1 ISO

1.3 identified-organization

1.3.6 dod

1.3.6.1 internet

1.3.6.1.4 private

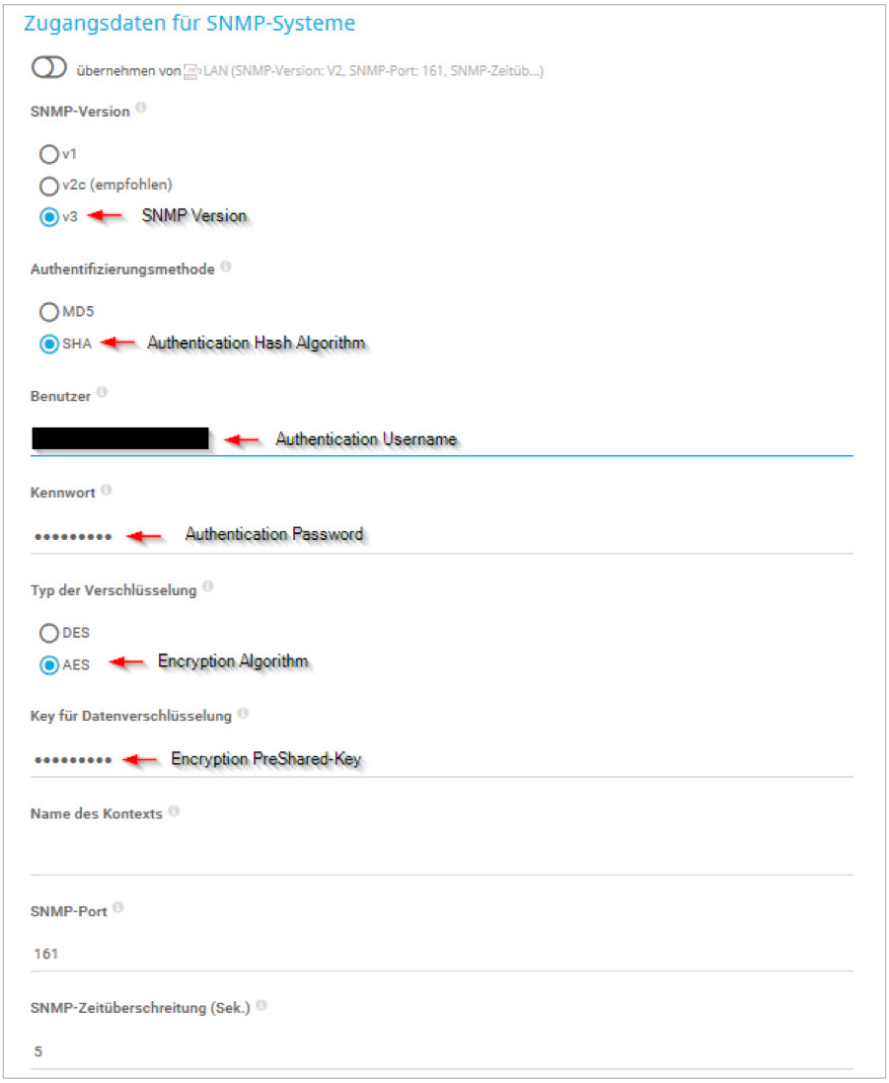
1.3.6.1.4.1 IANA enterprise numbers

1.3.6.1.4.1.12356 fortinet

OID	Name	Description
1.3.6.1.4.1.12356.0	fnTraps	None
1.3.6.1.4.1.12356.1	fnSystem	None
1.3.6.1.4.1.12356.2	fnFirewall, fnDomains	None
[…]		
1.3.6.1.4.1.12356.10	fortinetTrap	None
[…]		
1.3.6.1.4.1.12356.100	fnCoreMib	None
1.3.6.1.4.1.12356.101	fnFortiGateMib	MIB module for Fortinet FortiGate devices
[…]		

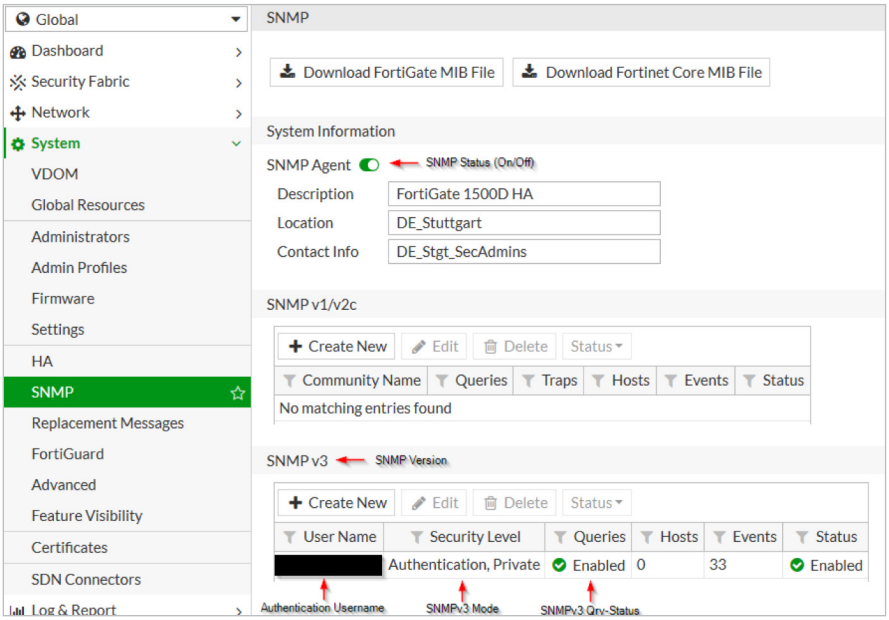
PRTG SNMPv3 Configuration

Add the FortiGate using a IPv4/IPv6/FQDN to PRTG and edit the device settings as shown in the following screenshot:

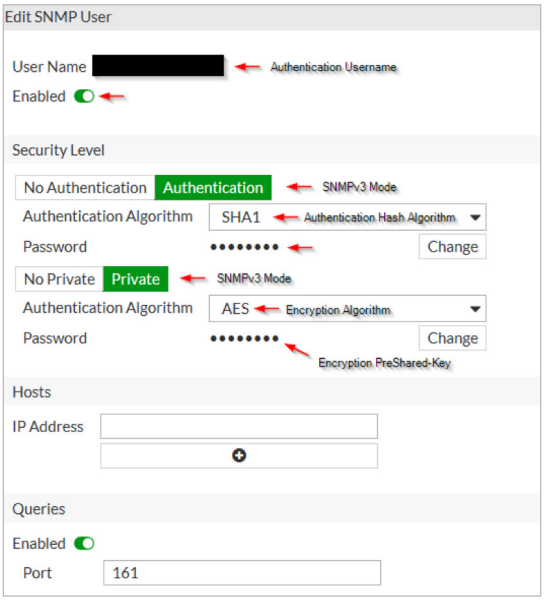


FortiGate SNMPv3 Configuration

In the FortiGate with activated VDOMs, select Global and go to System\SNMP. In a FortiGate with deactivated VDOMs, go to System\SNMP. Activate SNMP and create a SNMPv3 user as follows:



Using the Create New Button (or Edit button) you can enter a new SNMPv3 user:



SNMP OIDs

SNMP OID	Description	Importance	Recommended Interval	Recommended Threshold	Recommended Notification
1.3.6.1.4.1.12356.101.4.1.7.0	Total hard disk capacity (MB). Normally hard disks of FGTs have log rotation activated	Low	10 Minutes	-	-
1.3.6.1.4.1.12356.101.4.1.8.0	Number of active sessions on the device	Medium	60 Seconds	Warning – 50% of the max. of the supported sessions of your device Alert – 85% of the max. of the supported sessions of your device	When reaching alert for the second time
1.3.6.1.4.1.12356.101.4.1.4.0	Current memory utilization (percentage). FGT might be close to converse mode (overload protection)	High	60 Seconds	Warning – Utilization over 70% Alert – Utilization over 80%	When for over 2 hours at Warning, Once while Alert
1.3.6.1.4.1.12356.101.4.1.3.0	Current CPU usage (percentage). Your device might be too small for the traffic load and/or your UTM-settings to high or you have some kind of incident	High	60 Seconds	Warning – Utilization over 90% over 5 minutes Alert – Utilization at 100% over 10 minutes	When reaching alert for a second time
1.3.6.1.4.1.12356.101.13.2.1.1.5	Network bandwidth usage of the cluster member (kbps)	Medium	120 seconds	Warning – 50% of the max. of the supported bandwidth of your device Alert – 85% of the max. of the supported bandwidth of your device	When reaching alert for the second time
1.3.6.1.4.1.12356.101.3.1.2.0	The max. number of virtual domains allowed on the device as allowed by hardware and/or licensing	Low	4 hours	-	-
1.3.6.1.4.1.12356.101.3.1.1.0	The number of virtual domains in vdTable	Low	4 hours	Warning – when number is 90% of max. number of VDOMs Alert – when number is equal to max. number of VDOMs	When reaching alert
1.3.6.1.4.1.12356.101.8.2.1.1.1	Number of virus transmissions detected in the virtual domain since start-up	Low	4 hours	-	-
1.3.6.1.4.1.12356.101.9.2.1.1.1	Number of intrusions detected since start-up in the VDOM	Low	4 hours	-	-
1.3.6.1.4.1.12356.101.4.1.11.0	The average session setup rate over the past minute	Low	10 minutes	-	-
1.3.6.1.4.1.12356.101.4.1.12.0	The average session setup rate over the past 30 minutes	Low	10 minutes	-	-
1.3.6.1.4.1.12356.101.4.1.16.0	The average ipv6 session setup rate over the past minute	Medium	60 Seconds	Warning – 50% of the max. of the supported new sessions per second of your device Alert – 85% of the max. of the supported new sessions per second of your device	When reaching alert for the second time
1.3.6.1.4.1.12356.101.4.1.17.0	The average ipv6 session setup rate over the past 10 minutes	Low	10 minutes	-	-
1.3.6.1.4.1.12356.101.4.1.18.0	The average ipv6 session setup rate over the past 30 minutes	Low	10 minutes	-	-
1.3.6.1.4.1.12356.101.13.2.1.1.2.1	The serial number of the cluster unit	High	60 Seconds	Alert when value changes, the active node of your A-P HA-cluster has changed	-
1.3.6.1.4.1.12356.101.13.2.1.1.12.1	Current HA Sync status	High	60 Seconds	0 = not synchronized 1 = synchronized Alert - when return value is 0	When reaching alert for the third time

SNMP Traps

STANDARD TRAPS RFC 1215

OID 1.3.6.1.4.1.12356.1.3.0

1.3.6.1.4.1.12356.1.3.0.1
ColdStart

1.3.6.1.4.1.12356.1.3.0.2
WarmStart

1.3.6.1.4.1.12356.1.3.0.3
LinkUp

1.3.6.1.4.1.12356.1.3.0.4
LinkDown

Common FortiGate Traps

OID 1.3.6.1.4.1.12356.101.2

1.3.6.1.4.1.12356.101.2.101
CPU usage high – fnTrapCpuThreshold, see CLI:

```
config system snmp sysinfo
       set trap-high-cpu-threshold
```

1.3.6.1.4.1.12356.101.2.102
Memory low – fnTrapMemThreshold, see CLI:

```
config system snmp sysinfo
       set trap-low-memory- threshold
```

1.3.6.1.4.1.12356.101.2.103
Log disk too full – fnTrapLogDiskThreshold

Only when FGT has log disk, check Fortinet Product Matrix, see CLI:

```
config system snmp sysinfo
       set trap- log-full-threshold
```

1.3.6.1.4.1.12356.101.2.104
Temperature too high - fnTrapTempHigh

1.3.6.1.4.1.12356.101.2.105
Voltage outside acceptable range - fnTrapVoltageOutOfRange

1.3.6.1.4.1.12356.101.2.106
Power supply failure – fnTrapPowerSupplyFailure

Only when FGT has redundant power supplies, check Fortinet Hardware Manual

1.3.6.1.4.1.12356.100.1.3.0.108
A fan failure has been detected - fnTrapFanFailure

1.3.6.1.4.1.12356.101.2.201
Interface IP change – fnTrapIpChange
Useful for Interface with dynamic IP-addresses (e.g. DHCP or PPPoE)

High Availability FortiGate Traps

OID 1.3.6.1.4.1.12356.101.13.3

1.3.6.1.4.1.12356.101.13.3.401
HA switch – fgTrapHaSwitch

1.3.6.1.4.1.12356.101.13.3.402
HA State Change – fgTrapHaStateChange

1.3.6.1.4.1.12356.101.13.3.403
HA Heartbeat Failure – fgTrapHaHBFail, check Fortinet HA Guide, see CLI:

```
config system ha
       set hb-interval
       set hb-lost-threshold
       set hello-holddown
```

1.3.6.1.4.1.12356.101.13.3.404
HA Member Unavailable – fgTrapHaMemberDown

1.3.6.1.4.1.12356.101.13.3.405
HA Member Available – fgTrapHaMemberUp

VPN FortiGate Traps

OID 1.3.6.1.4.1.12356.1.3.0

1.3.6.1.4.1.12356.1.3.301
VPN tunnel is up – fgTrapVpnTunUp

1.3.6.1.4.1.12356.1.3.302
VPN tunnel down - fgTrapVpnTunDown

AntiVirus & Intrusion Prevention System FortiGate Traps

OID 1.3.6.1.4.1.12356.101.2
OID 1.3.6.1.4.1.12356.101.9

1.3.6.1.4.1.12356.101.2.0.503
An IPS signature has been triggered - fgTrapIpsSignature

1.3.6.1.4.1.12356.101.9.506
The IPS network buffer is full - fgTrapIpsFailOpen

1.3.6.1.4.1.12356.101.2.0.601
A virus has been detected by the anti-virus engine - fgTrapAvVirus

1.3.6.1.4.1.12356.101.9.605
The anti-virus engine has entered conservation mode due to low memory conditions - fgTrapAvEnterConserve

1.3.6.1.4.1.12356.101.9.606
The anti-virus engine has been bypassed due to conservation mode – fgTrapAvBypas

SSH

SSHv1 is disabled by default. To enforce large values for Diffie-Hellman exchanges in SSHv2 and to use strong ciphers use the following command:

```
config sys global
       set strong-crypto enable
       set dh-params 4096
end
```

You can also change the default TCP-SSH-port of the FGT to a random one, for example TCP:23345. This does not add additional security but default port-scanners have to execute a full scan, normal quick scans might not find your used port:

```
config system global
       set admin-ssh-port 23345
end
```

For authentication SSH with certificates can be used:

```
config system admin
    edit "name-of-admin-account"
        set accprofile "super_admin"
        set vdom "root"
        set ssh-certificate "your-imported-certificate"
    next
end
```

ABOUT PAESSLER AG

In 1997 Paessler revolutionized IT monitoring with the introduction of PRTG Network Monitor. Today over 200,000 IT administrators, in more than 170 countries, rely on PRTG to monitor their business-critical systems, devices and network infrastructures. PRTG monitors the entire IT infrastructure 24/7 and helps IT professionals to seamlessly solve problems before they impact users.

Our mission is to empower technical teams to manage their infrastructure, ensuring maximum productivity. We build lasting partnerships and integrative, holistic solutions to achieve this. Thinking beyond IT networks, Paessler is actively developing solutions to support digital transformation strategies and the Internet of Things.

Learn more about Paessler and PRTG at www.paessler.com

Paessler AG
www.paessler.com
info@paessler.com

HTTPS

Use the following command to require TLS 1.2 for HTTPS administrator access to the GUI:

```
config system global
      set admin-https-ssl-versions tlsv1-2
end
```

TLS 1.2 is currently the most secure SSL/TLS supported version for SSL- encrypted administrator access to your FortiGate. Restrict access to dedicated trusted hosts (see above) and deactivate HTTPS web access on all interfaces except your management-network. Also only use HTTPS, not HTTP.

For HTTPS use official or certificates from your certificate authority (Certificates with RSA 4096 or 2048Bit and SHA2-256 or SHA2-384 signature). Instead of browsing to the FGT ip address, use the FQDN so make sure no certificate warning is shown.

You can also change the default TCP-port of the FGT webinterface to a random one, for example TCP:33026. This does not add additional security but default port-scanners have to execute a full scan, normal quick scans might not find your used port:

```
config system global
      set admin-sport 33026
end
```

Enable strong ciphers using “strong-crypto enable”, disable statics keys for TLS sessions and enforce large values for Diffie-Hellman exchanges using the following commands:

```
config sys global
      set strong-crypto enable
      set ssl-static-key-ciphers disable
      set dh-params 4096
end
```

NetFlow

Only recommended with setups where FortiGate has Network Processes ASIC NP6, NP7 or above. On FGTs without NPs NetFlow is done in CPU, which might cause high CPU utilization:

“NP6 and NP6Lite offloading is supported when you configure NetFlow for interfaces connected to NP6 or NP6Lite processors. Offloading of other sessions is not affected by configuring NetFlow. Configuring sFlow on any interface disables all NP6 and NP6Lite offloading for all traffic on that interface.”

https://docs.fortinet.com/d/fortigate-hardware-acceleration-2