Fortinet technical support requirements for support issues

If you have a valid support contract on your Fortinet device, you may submit a support request via the FortiCare web site http://support.fortinet.com/Login/UserLogin.aspx (Partners: http://www.fortinet.com/partners/login.html)

In order for Fortinet Technical Support to provide you with the quickest and best quality of support, we require that the problem be clearly described and that the details of your network layout and FortiGate device configuration are supplied. In describing the problem, you can explain what you are trying to achieve and how it may be failing. You should also describe situations where it may, or has worked.

The device's configuration file is only part of what is usually required. In most cases, a detailed network diagram showing how the unit is implemented and interacting with other devices must be known to us. This is crucial so we can understand and analyze the problem most efficiently, and propose a solution for it. A small amount of time spent by you in creating a detailed network diagram, can reduce the time to resolve a problem dramatically. An example of what is required at a minimum, is explained below.

If more than one unit is involved, for example, High Availability or site-to-site VPN, then the unit and network layout details of each device, and site are required.

The following are the required details which make a technical support request complete, and allows us to effectively work on your problem immediately:

- a clear problem description.
- the FortiGate unit's latest configuration file.
    - v2.80 (**System** > **Maintenance** > **Backup & Restore** > **System Configuration**).
    - v3.00 (**System** > **Maintenance** > **Backup & Restore** > **Backup**)
- the unit's latest "debug.log" file(s).
    - v2.80 (**System** > **Maintenance** > **Backup & Restore** > **Debug Log**).
    - v2.80-MR11 (or later) HA Cluster (**System** > **Config** > **HA** > **Cluster Members** > **Download Debug Log** (icons))
    - v3.00 (**System** > **Maintenance** > **Backup & Restore** > **Advanced** > **Debug Log**).

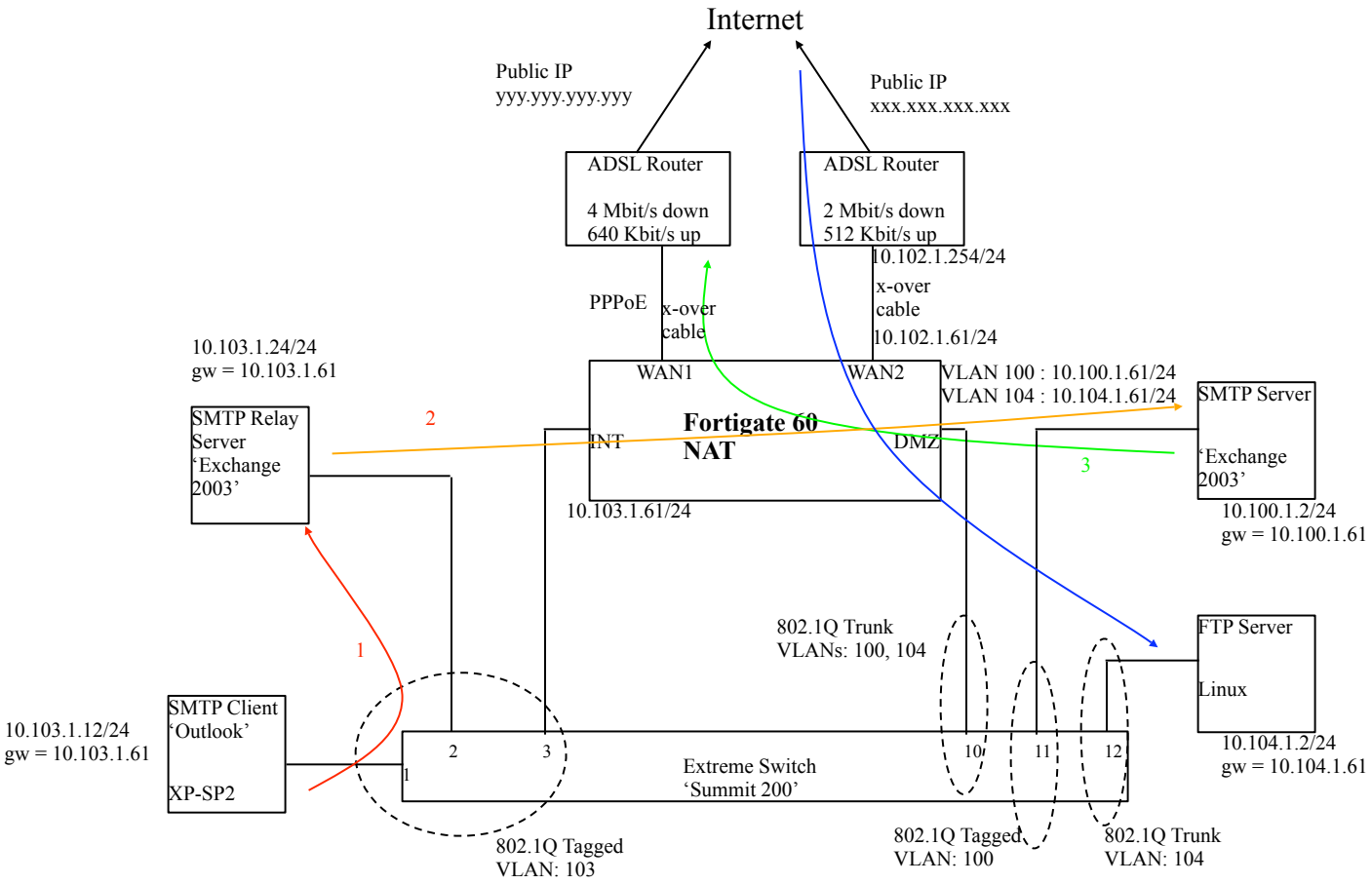
- the output from the following CLI commands to complement the configuration file:

v2.80	v3.00
	MR2 and above - diag debug report will gather all of the below
conf sys con	con sys con
set outp stan	set outp stan
end	end
General/System	**General/System**
exe time	exe time
exe date	exe date
get sys stat	get sys stat
get sys perf	get sys perf status
diag sys matr	???
diag hard sys mem	diag hard sys mem
get sys global	get sys global
AntiVirus	**AntiVirus**
diag sys auto stat	diag sys auto stat / MR5 and above – diag auto stat
diag sys auto ver	dag sys auto ver / MR5 and above – diag auto ver
diag test update info	diag test update info
get sys auto over	get sys autoupdate over
get sys auto push	get sys autoupdate push
get sys auto sche	get sys autoupdate schedule
get sys auto tun	get sys autoupdate schedule

Interface/Ethernet stats	**Interface/Ethernet stats**
diag netl dev list	diag netl dev list
diag netl int list	diag netl int list
diag hard dev nic <interface_name>	diag hard dev nice <interface_name>
...for each interface...	...for each interface...
get sys int	get sys int
get sys int <interface_name>	get sys int <interface_name>
...for each interface...	...for each interface...
Routing/Sessions	**Routing/Sessions**
diag netl ip list	diag ip address list
diag netl neighbor list	get sys arp / diag ip arp list
get rout info routing	get rout info routing all
diag netl route list	diag ip route list
diag sys sess stat	diag sys session stat / get sys sess list
HA (High Availability/Cluster)	
get sys ha	get sys ha
diag sys ha status	diag sys ha status
diag sys ha mac	diag sys ha mac
diag sys ha ldb	diag sys ha fib
diag sys ha diffcs [On Slave unit(s) only]	diag sys ha dump
Configuration	
show	show

- a detailed network diagram which clearly indicates all of the following:
    - each configured Fortinet device interface (including the interface used for management).
    - all IPs and netmasks of each interface and attached host(s).
    - connection of these interfaces to their layer-2 devices (switches).
    - implementation of layer-3 devices (routers).
    - VLAN definitions if used.
    - the traffic flow and type, which is causing the problem. Indicate the source and destination devices. If the responsible traffic flow is not known, identify all traffic flows of the concerned protocol. For example, detail the outgoing and incoming SMTP traffic flow, to and from the email client.
    - any/all hosts and servers which are affected by the traffic flow problem, for example SMTP, FTP or HTTP, along with their default gateway IP (and routing table if more than just a default gateway is configured).
    - identify any relays/proxies/secondary servers which might be used in your network layout and their usage. For example, whether a web/ftp client is configured to first access a proxy, or if two SMTP email servers are relaying emails to each other.
    - identify whether any load balancers are being used, and for which protocols/ports.
    - the up/down network bandwidth on each WAN link.

Network Diagram Example



-providing us with remote HTTPS and SSH access to the unit(s), is also of great help, as we may need to interactively (and passively) troubleshoot and debug a problem. By "passively", we mean that we will not perform any configuration changes or perform traffic/service disruptions without your prior approval. We can supply you with our source IP address, so you can add it to your device's 'trusted host' table.