Fortigate Firewalls

All about Fortinet, Firewall and other stuff of the daily work with the products.

Design

Operation

Operation

Using the save option "set cfg-save revert" to automatically reboot and revert to a previous configuration of a FortiGate

Description

> This article describes the system global option "**set cfg-save revert**" that can be used during remote changes on a Fortigate and where the operator would like an automatic revert to the previous configuration in case of problems arise (if for example the connection to the FortiGate is lost).

Solution

The global setting parameter "set cfg-save" dictates the way that configuration changes applied on the FortiGate are saved:

```
FGT# config system global
FGT# (global) # set cfg-save ?

automatic    automatically save config
manual       manually save config
revert       manually save config and revert the config when timeout
```

- The default setting is "**automatic**" : in this mode, any changes applied after an "end" or "Apply" will be saved.

- If set to "**revert**", an additional global parameter is required, which is the timeout in seconds : "**set cfg-revert-timeout**"

> **Once this is applied, any new changes must be saved manually with the command "execute cfg save"within the period of the timeout, otherwise the FortiGate will reboot.**
>
> A warning CLI message will be displayed 10s before the reboot :

```
FGT # System will reboot if no input is received in the next 10 seconds...
System will reboot if no input is received in the next 9 seconds...
System will reboot if no input is received in the next 8 seconds...
System will reboot if no input is received in the next 7 seconds...
```

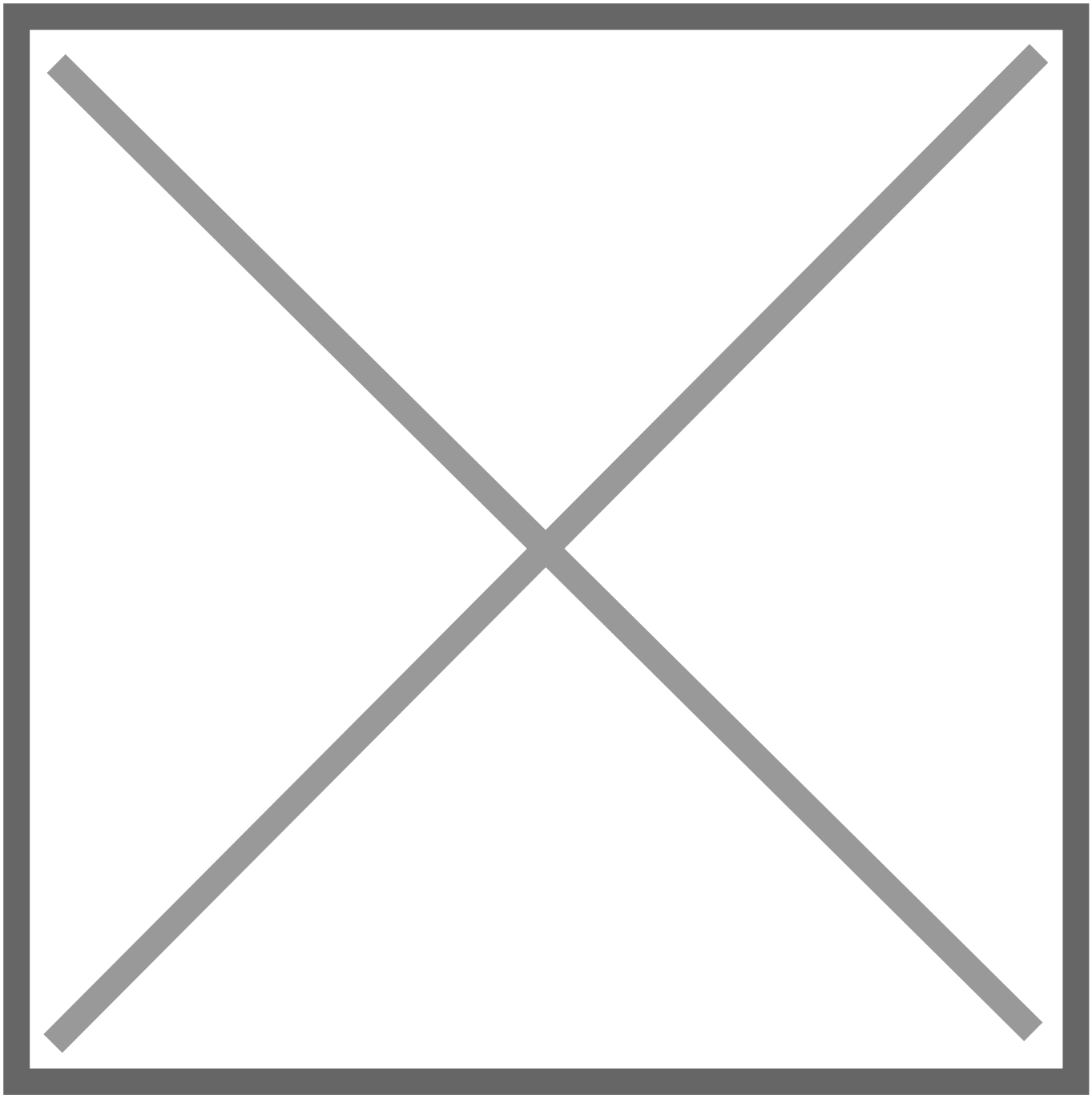
Example :

This example explains the use of the **cfg-save revert** command and its associated event log Fortigate Restarted when newly added configuration is not confirmed.

```
FG100D_Primary (global) # set cfg-save
automatic   Automatically save config.
manual      Manually save config.
revert      Manually save config and revert the config when timeout.

FG100D_Primary (global) # show full-configuration | grep cfg
set cfg-save automatic

FG100D_Primary (global) # show full-configuration | grep cfg
set cfg-save revert     <<--- Changed from automatic to revert
set cfg-revert-timeout 600   <<--- (10 Minutes)

FG100D_Primary (lan) # set role
lan         Connected to local network of endpoints.
wan         Connected to Internet.
dmz         Connected to server zone.
undefined   Interface has no specific role.

FG100D_Primary (lan) # set role lan   <<-- Added a new role to the LAN interface configuration in order to
generate a new change in the current configuration.
FG100D_Primary (lan) # end
```

FG100D_Primary (lan) # show full-configuration | grep role
set role lan <<-- New configuration added to interface

FG100D_Primary (lan) # show full-configuration | grep role
set role undefined <<-- The newly added configuration of role on the interfaces was never added to the current configuration due to the “timeout” of 600 seconds, (10 Minutes) expired and the newly added configuration was never confirmed generating the event log “Fortigate Restarted” under system events.



Backup Configuration

Backing up the configuration

Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Backup*.
2. Direct the backup to your *Local PC*or to a *USB Disk*.
   The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
3. If VDOMs are enabled, indicate whether the scope of the backup is the entire FortiGate configuration (*Global*) or only a specific VDOM configuration (*VDOM*).
   If backing up a VDOM configuration, select the VDOM name from the list.
4. Enable *Encryption*. Encryption must be enabled on the backup file to back up VPN certificates.
5. Enter a password, and enter it again to confirm it. This password will be required to restore the configuration.
6. Click *OK*.
7. When prompted, select a location on the PC or USB disk to save the configuration file. The configuration file will have a .conf extension.

Using the CLI

Use one of the following commands:

```
execute backup config management-station <comment>
```

or:

```
execute backup config usb <backup_filename> [<backup_password>]
```

FTP

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

TFTP

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

VDOM

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom

edit <vdom_name>
```

Using REST-API

> REST-API user must have write access to FortiGate and VDOM

Create access profile

```
FGT # config system accprofile
FGT (accprofile) # edit readOnly
new entry 'readOnly' added
FGT (readOnly) # set sysgrp read
FGT (readOnly) # end
```

Create API user in FortiGate

```
FGT # config system api-user
FGT (api-user) # edit api-admin
new entry 'api-admin' added
FGT (api-admin) # set accprofile "readOnly"
FGT (api-admin) # set vdom root
FGT (api-admin) # config trusthost
FGT (trusthost) # edit 1
new entry '1' added
FGT (1) # set ipv4-trusthost 'ip_address_of_your_machine' 255.255.255.255
FGT (1) # end
FGT (api-admin) # end
```

Generate API Token

```
FGT # execute api-user generate-key api-admin
New API key: 'your_api_token'
NOTE: The bearer of this API key will be granted all access privileges assigned to the api-user api-admin.
```

Get the backup

```
HOSTNAME=<hostname>
API_TOKEN=<api-token>
DATE=`date +%F_%T%S`
curl -k -o $HOSTNAME_$DATE.conf -H "Authorization: Bearer $API_TOKEN"\
"https://$HOSTNAME/api/v2/monitor/system/config/backup/?scope=global&amp;access_token=$API_TOKEN"
```

Restoring a configuration

Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Restore*.
2. Identify the source of the configuration file to be restored: your *Local PC*or a *USB Disk*. The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Click Upload, locate the configuration file, and click *Open*.
4. Enter the password if required.
5. Click *OK*.

Using the CLI

`execute restore config management-station normal 0`

or:

`execute restore config usb <filename> [<password>]`

FTP

`execute restore config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]`

TFTP

`execute restore config tftp <backup_filename> <tftp_server> <password>`

The FortiGate will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Operation

Useful CLI commands FortiOS

Cheatsheets

- FortiOS 6.2 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-version-6-2/)
- FortiOS 7.0 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-7-0/)
- FortiOS 7.2 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-v7-2/)

CLI Commands

> To start a transaction in CLI use ***execute config-transaction start***.

> A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded

> Commit config changes with ***execute config-transaction commit.***
> Abort with ***execute config-transaction abort.***

Generic Commands

Default Device Information

admin / no password	Default login
192.168.1.99	Default IP on port1, internal or management port
9600/8-N-1, hw flow control disabled	Default serial console settings

General system commands

get system status	General system information

exec tac support	Generates report for support
tree	List all commands
<command> ? / tab	Use ? or tab in CLI for help
<command> | grep [filter]	Grep commands to filter output

Fortigate most used ports

UDP/53, UDP/8888	Fortiguard Queries
TCP/389, UDP/389	LDAP, PKI Authentication
TCP/443	Contract Validation, FortiToken, Firmware Updates
TCP/443, TCP/8890	AV and IPS Update
UDP/500, ESP	IPSEC VPN
UDP/500, UDP/4500	IPSEC VPN with NAT-Traversal
TCP/514	FortiManager, FortiAnalyzer
TCP/1812, TCP/1813	RADIUS Auth & Accounting
UDP/5246, UDP/5247	CAPWAP
TCP/8001	FSSO
TCP/8013	Compliance and Security Fabric
ETH Layer 0x8890, 0x8891 and 0x8893	HA Heartbeat For HA The virtual MAC address is determined based on following formula: 00-09-0f-09-<group-id_hex>-(<vcluster_integer> + <idx>)

Network commands

Interface information

diag ip address list	List of IP addresses on FortiGate interfaces
diag firewall iplist list	List of IP addresses on VIP and IP-Pools

Security Fabric

diag sys csf upstream / downstream	List of up/downstream devices
diag sys csf neighbor list	MAC/IP list of connected FG devices
diag automation test <stich_name>	Test stitches in the CLI
diag test appl csfd 1 ...	Display security fabric statistics
diag debug appl csfd -1	Real-time debugger

Switch Controller

diag switch-controller switch-info mac-table	Managed FortiSwitch MAC address list
diag switch-controller switch-info port-stats	Managed FortiSwitch port statistics
diag switch-controller switch-info trunk	Trunk information
diag switch-controller switch-info mclag	Dumps MCLAG releated information from FortiSwitch
execute switch-controller get-conn-status	Get FortiSwitch connection status
execute switch-controller diagnose-connection	Get FortiSwitch connection diagnostics

SD-WAN

diag sys virtual-wan-link member	Provide interface details
diag sys virtual-wan-link health-check <name>	State of SLAs
diag sys virtual-wan-link service <rule-id>	SD-WAN rule state
diag sys virtual-wan-link intf-sla-log <intf-name>	Link Traffic History
diag sys virtual-wan-link sla-log <sla> <link_id>	SLA-Log on specific interface
diag test application lnkmtd 1/2/3	Statistics of link-monitor
diag debug application link- monitor -1	Real-time debugger of link-monitor

Network Troubleshooting

get hardware nic [port]	Interface information
get system arp **get system arp | grep x.x.x.x** **diag ip arp list**	ARP table
exec clear system arp table	Clears ARP table
exec ping x.x.x.x **exec ping-options [option]**	Ping utility
exec traceroute x.x.x.x **exec traceroute-options [option]**	Traceroute utility
exec telnet x.x.x.x [port]	Telnet utility
exec dhcp lease-list	Show DHCP Leases
diag traffictest server-intf **diag traffictest client-intf** **diag traffictest port [port]** **diag traffictest run -c [public_iperf_server_ip]**	Iperf test directly run from FortiGate

Transparent Mode

diag netlink brctl	Bridge MAC table

Routing

Routing troubleshooting

get router info routing-table all	Show routing table
get router info routing-table details x.x.x.x	Show routing decision for specified destination-IP
get router info routing-table database	Routing table with inactive routes
get router info kernel	Forwarding information base
diag firewall proute list	List of policy-based routes
diag ip rtcache list	List of route cache
exec router restart	Restart of routing process
diag sys link-monitor status/interface/launch	Show link monitor status / per interface / for WAN LB

BGP

get router info bgp summary	BGP summary of BGP status
get router info bgp neighbors	Information of BGP neighbors
diag ip router bgp all enable **diag ip router bgp level info**	Real-time debugging for BGP protocol
exec router clear bgp all	Restart of BGP session

OSPF

get router info ospf status	OSPF status
get router info ospf interface	Information on OSPF interfaces
get router info ospf neighbor	Information on OSPF neighbors
get router info ospf database brief / router lsa	Summary / Details of all LSDB entries
get router info ospf database self-originate	Information on LSAs originating from FortiGate
diag ip router ospf all enable **diag ip router ospf level info**	Real-time debugging of OSPF protocol
exec router clear ospf process	Restart of OSPF session

VPN

diag debug appl ike 63	Debugging of IKE negotiation

diag vpn ike log filter	Filter for IKE negotiation output
diag vpn ike gateway list	Phase 1 state
diag vpn ike gateway flush	Delete Phase 1
diag vpn tunnel list	Phase 2 state
diag vpn tunnel flush	Delete Phase 2
get vpn ike gateway	Detailed gateway information
get vpn ipsec tunnel details	Detailed tunnel statistics
get vpn ipsec tunnel summary	Detailed tunnel information
diag vpn ipsec status	Shows IPSEC crypto status
show full vpn certificate local	Export all keys and certs

Troubleshooting

Troubleshooting

Wrong DNS Server used by random clients

Problem

Fortigate VPN users reporting that they cannot connect to internal resources anymore.
When you check the client the internal host is reachable by IP but it appears that windows isn't using the internal DNS server to resolve the host name. A check with nslookup was working when testing this on the VPN client.

Solution

the clients having issues were using IPV6 and learned about this feature in Windows call "Smart Multi-Homed Name Resolution". It sounds like Windows will forward a DNS query to both the IPV6 and IPV4 DNS servers and use the first response.

Adding a regkey to disable the parallel queries and the issue cleared.

Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

- If the Dword value DisableParallelAandAAAA exists already, make sure its value is set to 1.
- If the value does not exist, right-click on Parameters, and select New > Dword (32-bit) Value.
- Name it DisableParallelAandAAAA.
- Set the value of the Dword to 1. You can turn the feature back on by setting the value to 0, or by deleting the value.

Link

https://forum.fortinet.com/tm.aspx?m=190334

Links & Tools

Access to Demo Fortinet Appliances

Fortinet offers for most appliances a demo access.

You can use the following as an example:

Product	URL	Login
Authenticator	https://fortiauthenticator.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
WEB Security	https://fortiweb.fortidemo.com	demo / demo
MAIL Security	https://fortimail.fortidemo.com/admin	demo / demo
Firewall	https://fortigate.fortidemo.com	demo / demo
FortiGate SD-WAN Demo	https://fortigate-sdwan.fortidemo.com	demo / demo
Switching LAN	https://fortiswitch.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
FortiSwitch as Standalone	https://lanedge.fortidemo.com	demo / demo
FortiSwitch managed by FortiGate	https://lanedge.fortidemo.com	demo / *40Network!*
VoIP Switching	https://fortivoice.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
DDOS Protection	https://fortiddos.fortidemo.com	demo / demo
Device Management	https://fortimanager.fortidemo.com	demo / demo

Log Analyzer	https://fortianalyzer.fortidemo.com	demo / demo
FortiPortal (MSSP Solution for FortiManager / FortiAnalyzer)	https://fortiportal.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
FortiEMS (FortiClient Endpoint Management Server)	https://fctems.fortidemo.com	corp\demo / Fortinet1
Recorder and Surveillance	https://fortirecorder.fortidemo.com	demo / demo
Sandbox	https://fortisandbox.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
Security Information and Event Management (SIEM)	https://fortisiem.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
Wireless Access Point	https://fortiap.fortidemo.com	demo / demo
Proxy	https://fortiproxy.fortidemo.com	demo / demo
Application Delivery Controller (ADC)	https://fortiadc.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
Virtual Security Analyst	https://fortiai.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center
Deception-based Solution	https://fortideceptor.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center

Security, Orchestration, Automation and Response Solution	https://fortisoar.fortidemo.com	demo / demo But it shows error: "FSR-Auth-043: Login denied as all concurrent user seats are currently in use. Please wait or contact the administrator for access."
Network Tester	https://fortitester.fortidemo.com	demo / demo
Wireless Manager	https://fortiwlm.fortidemo.com	demo / demo
Carrier Grade NAT (CGN)	https://forticarrier.fortidemo.com	Unknown Request credentials here: https://www.fortinet.com/demo-center

Links & Tools

Fortinet Blog Links

Fortigate Blog

https://yurisk.info/category/fortigate.html

Fortinet Blog

- https://yurisk.info/category/fortinet.html
- https://troublenet.de/category/fortinet/