Checkpoint :

Commande	Signification
The default Shell CLI mode is “clish” (Simple, does not give access to low level system functions). For advanced configurations, use the more permissive Expert mode shell. Excecute “expert”. To exit from the Expert shell and return to Gaia Clish, run: “exit”.	
`show configuration`	Affichage de la Conf
`save config`	Sauvegarde de la Conf
`show route all (clish)` `netstat -nr / route -n / ip route show (expert)`	Affichage de la Table de routage
`set static-route 10.10.10.0/24 nexthop gateway address 10.10.10.1 on`	Ajout d’une route statique
`set static-route default nexthop gateway address 10.10.10.1 on`	Ajout d’une Default Route
`show route destination 10.10.10.0/24`	Affiche d’une route spécifique dans la table de Routage
`show arp (clish)` `arp -n (expert)`	Affichage de la table ARP du FW

`show interfaces (clish)`
`fw getifs (expert)`
`ifconfig -a (expert)`
`ip addr (expert)`
	Vérification de statut de toutes les interfaces

`fw tab -t connections -s`
`fw tab -t connections -u`
`fw ctl conntab`
	Affichage des sessions actives

`cphaprob stats`
`cphaprob state`
`cpstat -f all ha`
	Affichage de l’état d’un Cluster de 2 Firewalls

`cphaprob -a if`	Vérification de statut de toutes les interfaces d’un Cluster
`clusterXL_admin down; clusterXL_admin up`	Effectuer un Failover entre les deux FWs du Cluster
`show version all` `fw ver`	Version du Firewall
`uptime`	System Uptime
`top` `cpview`	Utilisation CPU / RAM

`fw monitor -e "accept host(10.10.10.180);"`
`tcpdump -i eth0 host 10.10.10.180`
`fw log | grep 10.10.10.180`
	Debug du traffic

Fortinet :

Commande	Signification

config global
config system global
  set hostname FW200RISK
  set vdom-mode multi-vdom
end
	Attribution d'un Hostname au FW et activation du multiple vdom mode.

config global
config system interface
  edit "mgmt1"
  set ip 10.10.10.1 255.255.255.0
  set allowaccess ping https ssh snmp
  set type physical
  next
end
	Configuration de l'IP du management du FW

config vdom
  edit VDOM200
  next
end
	Creation d'un VDOM

execute factoryreset	Effacer toute la conf du FW
config system interface show Ou: show system interfaces	Affichage de l'état des Interfaces du FW
show system interface port2 Ou : get system interface port2	Affichage de l'état d'une Interface spécifique du FW
show full-configuration	Affichage de toute la Conf du FW
show firewall policy	Affichage de la liste des Policies implémentées sur le FW
get system performance status	Etat des CPU, Mémoire, …
get system arp	Affichage de la table ARP du FW
get router info routing-table all	Affichage de la Table de Routage du FW
get router info routing-table details 10.200.2.33	Check d'une route spécifique dans la table de routage
get router info bgp summary	Affichage d'un résumé des sessions BGP implémentées
get router info ospf neighbor	Etat de voisinage OSPF
get sys ha status diagnose sys ha status	Affichage et Debug de l'Etat d'un Cluster de 2 FWs (HA)
diag sys ha reset-uptime	Effectuer un Failover entre les deux FWs d'un Cluster

`get system status`	Version du Firewall
`diagnose hardware sysinfo`	Information du Hardware, SN, …
`diagnose sys top-summary`	Liste des process qui consomment plus de CPU (sorted).

`diagnose debug enable`
`diagnose debug console timestamp enable`
`diagnose debug flow show console enable`
`diagnose debug flow filter addr 10.10.10.10`
`diagnose debug flow trace start 100`
 	
`(Pour arrêter le Debug) : diagnose debug disable`
	Debug du traffic

`diagnose sniffer packet any "host 10.10.10.10" 4` `diagnose sniffer packet any "port 443" 4`	Sniffer un Traffic spécifique (Capture)

`execute nslookup www.chakerbchir.fr`
`execute ping 8.8.8.8`
`execute traceroute 2.2.2.2`
	Tests Networks