Maestro Orchestrator (MHO) basic setup guide.

In this guide I will try to assist you in setting up a Maestro Orchestrator configuration in a step by step way, most of the references regarding ports are based on the MHO140.

First of all you need to decide which clustering method to use

1. Local site clustering,
    a. 2 MHO's and multiple gateways
    b. all gateways have a connection to each MHO
    c. local sync with a DAC on Sync interface
    d. maximum 31 appliances in 1 SG
2. Dual site clustering single MHO
    a. 2 MHO's and multiple gateways
    b. all gateways have a connection to each local MHO
    c. sync between sites on other port than 48 (in this sample 47)
    d. maximum of 28 appliances in total (14 per Site) in 1 SG
3. Dual site clustering dual MHO
    a. 4 MHO's and multiple gateways
    b. all gateways have a connection to each local MHO
    c. local sync with DAC on Sync interface, sync between sites on other port than 48 (in this sample 47) per pair of MHO's
    d. maximum of 28 appliances in total (14 per site) in 1 SG

Sync between sites requires 1 glass connection per MHO pair. The switchports in between need to be set to QinQ and preferably set to support jumbo frames.

Console connection are preferred to ALL devices, on the GW's to make sure you have R80.20SP on it (install from USB).
You also need a 10Gb switch for connecting all Mgmt ports of the security groups you will be creating, unless you have 1GB SFP's as those are also supported. Connections from each MHO port 1 is the minimum you need. Also the Mgmt1 1Gb port on the back of the MHO140 or on the front of the MHO170 needs to be connected to a switch. Both need to be connected to the network you use for staging your setup. Cable all devices according the above list and the supplied drawing to the designated ports on the MHO. Also make sure to check time zone, date and time.

Start the setup with updates.

Power up the first MHO for the first site and the first gateway connected to that MHO .
On MHO site 1 setup: via the console, set the interface Mgmt1 to your staging network, all using standard GAIA clish commands.

!! Watch out NEVER manually update the deployment agent !!
Now ssh into the MHO and move the latest Jumbo file to it (set user admin shell /bin/bash) with winscp and use installer import local or the WebUI to add the file to the repository and install the jumbo.
!! Jumbo files for MHO and GW's are different !!

Now let's start the configuration.

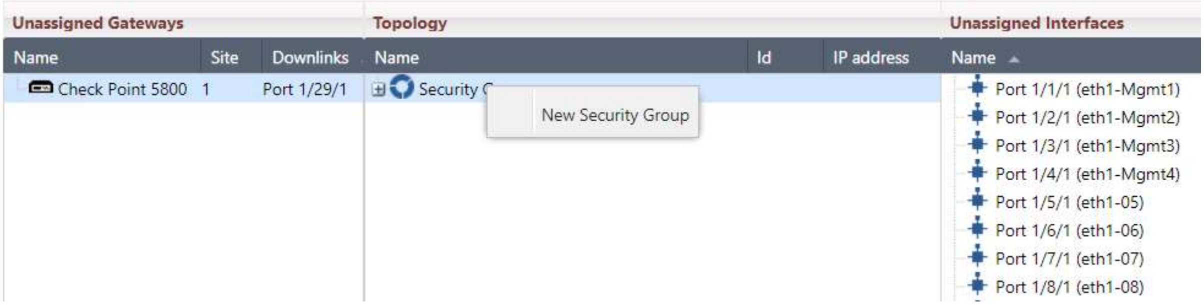
Always begin with 1 MHO and 1 gateway, with a local cluster use assigned port 48 for local Sync between the 2 MHO's.
Before you continue execute this command from the MHO clish:

```
set maestro configuration orchestrator-amount 1
```

Otherwise it just will not work as the default value is 2, remember this value is per site.

Login to the WebUI of the MHO, for all clustering methods, remember the following: all security group configurations are done from the first member.
Now in the WebUI go to the tab Orchestrator and see if it shows the powered-on gateway under Unassigned Gateways and all interfaces under Unassigned Interfaces.

If all looks ok you can create a Security group, right mouse click on security groups and choose New Security Group



Unassigned Gateways

Name	Site	Downlinks
Check Point 5800	1	Port 1/29/1

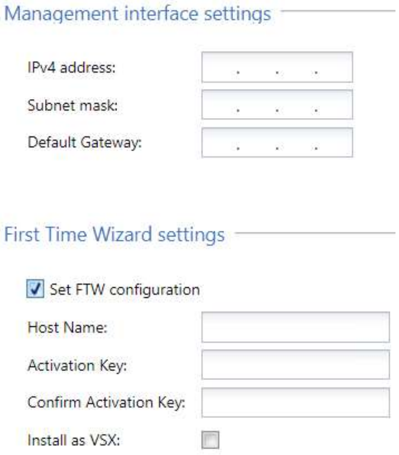
Topology

Name	Id	IP address
Security G		

Unassigned Interfaces

Name
Port 1/1/1 (eth1-Mgmt1)
Port 1/2/1 (eth1-Mgmt2)
Port 1/3/1 (eth1-Mgmt3)
Port 1/4/1 (eth1-Mgmt4)
Port 1/5/1 (eth1-05)
Port 1/6/1 (eth1-06)
Port 1/7/1 (eth1-07)
Port 1/8/1 (eth1-08)

Set the IP and check set FTW on, give it a name and add a PSK.



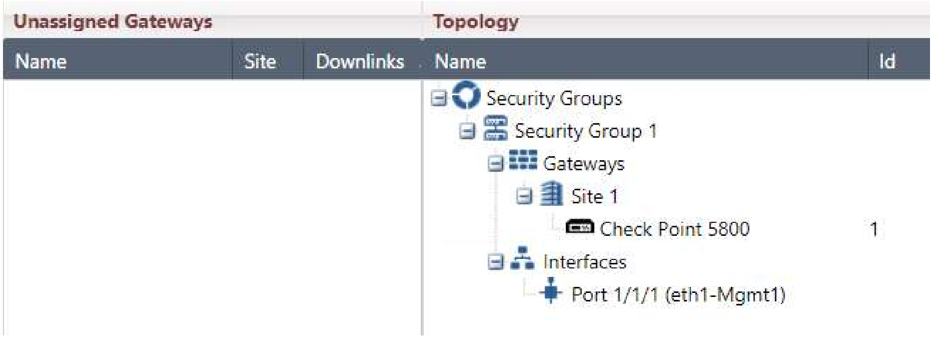
Management interface settings

IPv4 address: . . .
Subnet mask: . . .
Default Gateway: . . .

First Time Wizard settings

☑ Set FTW configuration
Host Name:
Activation Key:
Confirm Activation Key:
Install as VSX: □

Drag the gateway to the gateways item under the Security Group you just created, from the right you drag eth1-Mgmt1 to the interfaces and add 1 or 2 extra interfaces.
Make sure port 1 of the MHO is patched on the switch.



Unassigned Gateways

Name	Site	Downlinks

Topology

Name	Id
Security Groups	
Security Group 1	
Gateways	
Site 1	
Check Point 5800	1
Interfaces	
Port 1/1/1 (eth1-Mgmt1)	

From this point you need to wait for at least 6 minutes before you can connect to the Security Group (the gateway).

Now let's prepare the gateways

SSH into the IP of the security Group and get ready to update the gateway to the latest JHF, set the admin password and change the admin shell to /bin/bash to be able to upload files with WinSCP, as you only want to do this once do not add more than 1 gateway to the security group!!

!! Watch out NEVER manually update the deployment agent !!

Next use WinSCP to copy the latest jumbo file to the gateway, import and install the jumbo before you continue.

```
   installer import local /home/admin/Check_Point_R80_20SP_JHF_MAIN_Bundle_T<##>_FULL.tgz
   installer install 1
```

Run from gclish to update all assigned gateways in the group on the same site, until you set the site-amount in the security group (see below) you can only add gateways from the same site.
Before adding more gateways you can issue the following command on the security group:

```
      set smo image auto-clone state on
```

Now you can start the adding of gateways and additional security groups.
The advice I got was to use cloning only during the setup phase.

Ready to complete your setup.

Now you are ready to add the 2nd MHO, depending on the clustering method, you need to change the settings for number of Orchestrators and sites.

Best way forward is to setup sites with dual MHO independent from each other before connecting them together. When both sites are running and seeing all members and the first gateway you can hook them all together by a glass patch between the ports 47. (MHO1-S1 to MHO1-S2 and MHO2-S1 to MHO2-S2). Now SSH to each MHO and set the correct values as shown below:

Single site dual MHO:
on the MHO's (after adding the 2nd):

```
      set maestro configuration orchestrator-amount 2
```

Dual site single MHO:
On the MHO:

```
      set maestro configuration orchestrator-amount 1
      set maestro configuration orchestrator-site-amount 2
      set maestro port 1/47/1 type site_sync
```

On MHO1 Site1:

```
      set maestro configuration orchestrator-site-id 1
```

On MHO1 Site2:

```
      set maestro configuration orchestrator-site-id 2
```

In each security group in gclish, to be able to add gateways from multiple sites:

```
      set smo security-group site-amount 2 (number of sites, currently 2 is the max)
```

Dual site dual MHO:
On all MHO's:

```
      set maestro configuration orchestrator-amount 2
      set maestro configuration orchestrator-site-amount 2
```

On the MHO1 both sites:

```
      set maestro port 1/47/1 type site_sync
      set maestro port 2/47/1 type site_sync
```

On MHO1 and MHO2 Site1:

```
      set maestro configuration orchestrator-site-id 1
```

On MHO1 and MHO2 Site2:

```
      set maestro configuration orchestrator-site-id 2
```

In each security group in gclish, to be able to add gateways from multiple sites:

```
      set smo security-group site-amount 2 (number of sites)

      set maestro configuration orchestrator-site-vlan xxxx
```

See CP-R80.20SP Getting Started Guide to change single to dual site, when you already have security groups defined and need to change the site amount.
Important notice: UTP-SFP 1Gb only supported from Jumbo 191 and higher with auto config or change the speed manually:

```
    set maestro port 1/1/1 qsfp-mode 1G
```

Licenses

On the MHO no license is required, the gw is licensed on it's 192.0.2.x address.
HA Licenses are NOT supported, you will need to upgrade those licenses to full blown licenses.

What's next?

When you want to configure anything on the Global Clish of the Security Group, 1 member will always be down when it has the initial policy loaded, so push a policy to the Security Group.

On single or dual site with dual MHO you will need to setup bond interfaces, for management and for the uplink interfaces in gclish, connect through the MHO and hop to the SG with: m 1 1 etc:

```
    add bonding group 1 mgmt
    set interface eth2-Mgmt1 state on
    add bonding group 1 mgmt interface eth2-Mgmt1
    set bonding group 1 mode active-backup
    set interface magg1 ipv4-address 1.2.3.11 mask-length 26
    set management interface magg1
    delete interface eth1-Mgmt1 ipv4-address
    add bonding group 1 mgmt interface eth1-Mgmt1
    set bonding group 1 primary eth1-Mgmt1
```

For a normal Uplink interface ethx-10:

```
    add bonding group 1
    add bonding group 1 interface eth1-10
    add bonding group 1 interface eth2-10
    set bonding group 1 mode 8023AD
    set bonding group 1 lacp-rate slow
```

To enable Jumbo frames just change the MTU size of the interfaces, including interface on a virtual Switch, to the value set in the network i.e. 9216, this value should be the same as the setting on the switchport.

Downlink bonding, when you do not need NGTP, the throughput can be increased above the 10Gb, so downlink bonding would be useful, in a Dual MHO setup always use port 1 and 3 for MHO1 and port 2 and 4 for MHO 2!! Downlink bond groups are created automatically. Also minimize the number of ports where possible, MultiQueue is limited to 5 interfaces.

The 40Gb/100Gb ports will not be numbered like the numbers on the box itself, but will be numbered with the uneven numbers only so 49, 51, when you use a splitter cable the bottom ports will be disabled! And numbering will just be 49, 50, 51, 52, this way the next port will always be 53.

Handy commands and things to know:

Check on the hardware neighbors, from any device in expert:

lldpctl

You can ssh into a Security group IP to get to the SGMs.
On the SGM:
Move from expert to clish:

clish is for the gateway specific
gclish is to apply changes to the entire security group.
set global-mode off/on from clish

To see the state of the groups on the MHO:

asg monitor

To see what is not really going the way you think, on the MHO:

asg diag verify

For a full diag on a SG run:

show smo verifiers report

Jump ssh from the MHO to a gateway (expert mode only):

m <sec grp> <gw> example: *m 2 1*

Jump ssh from gateway to a gateway in same security group (expert mode only):

m <site>_<gw> example: *m 2_1*

To see the gclish config:

asg_config show

To see the status and versions of the gateways/ports:

asg stat -v
asg monitor -all

Find drops over all SGM's, from expert:

g_fw ctl zdebug drop

sx_ …. Lot of scripts in expert press the <Tab> key
tcpdump is not supported but cppcap is

SNMP traps settings: start wizard with asg alert

To see the performance load:

asg perf -v

Performance checking

asg perf hogs

To see the VSX status of current VS

asg stat vs

To see the VSX status of all VS's

asg stat vs all
vsx stat -v (expert only)
asg perf -vs all -v -vv
asg_vsx_verify

To view the VSLS configuration:

show configuration vsls

VSLS:
Per vs

set chassis high-availability mode 3 ➔ *vsls*
set chassis vsls system primary_chassis 0 / 1 / 2 ➔ *prio op site 1 of 2 of auto*
set chassis high-availability vs chassis_priority ➔ *weight per vs*