State Synchronization Using Clustering in NGAI

Assumptions

- IPSO 3.7 buildXX
- Checkpoint NG with Application Intelligence (NGAI r55)
- You have defined your Monitored Circuits in IPSO. This document does not cover VRRP.
- 2 Firewalls (Primary and Backup) each running IPSO 3.7 with NGAI, and with Clustering Enabled.

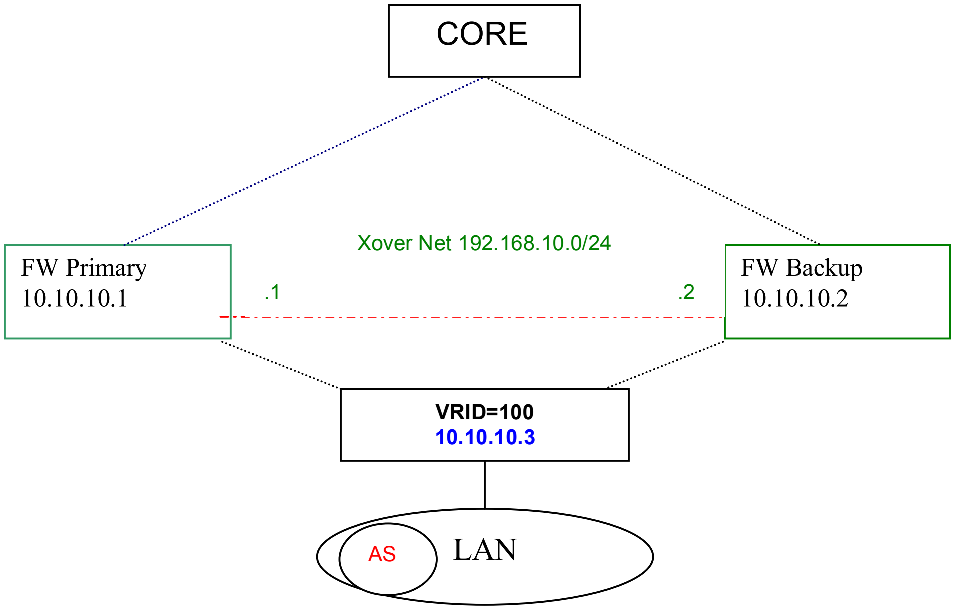
Note: If you haven't already enabled clustering, run "cpconfig" and choose:

```
(6)  Enable cluster membership for this gateway
```

- Define a Virtual IP (VIP) for your cluster. You can also use a VIP from any of your existing Monitored Circuits.

Example:

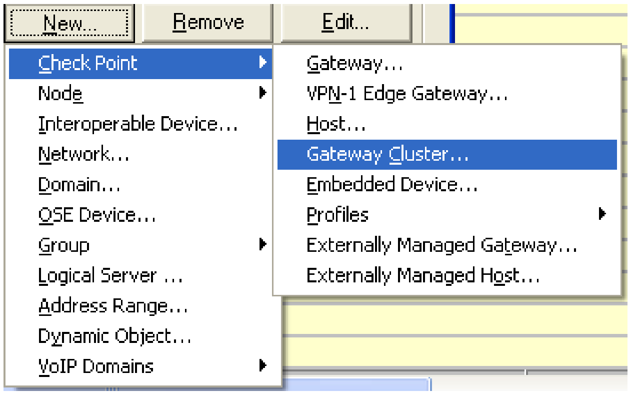
```
LAN6002-1A/3/9
  10.10.10.1/24 Mode: ( ) off ( ) VRRPv2 (*) Monitored Circuit
Virtual Router: 100 (*) on ( ) off Priority: 90__________ Hello Interval: 10__________
VMAC Mode: [VRRP_____] Static VMAC: _________________
10.10.10.3 (*) on ( ) off
  Backup Address: _______________
  eth-s1p3c0 (*) on ( ) off Priority Delta: 20
  Monitor Interface [None______] Priority Delta: ____________
```



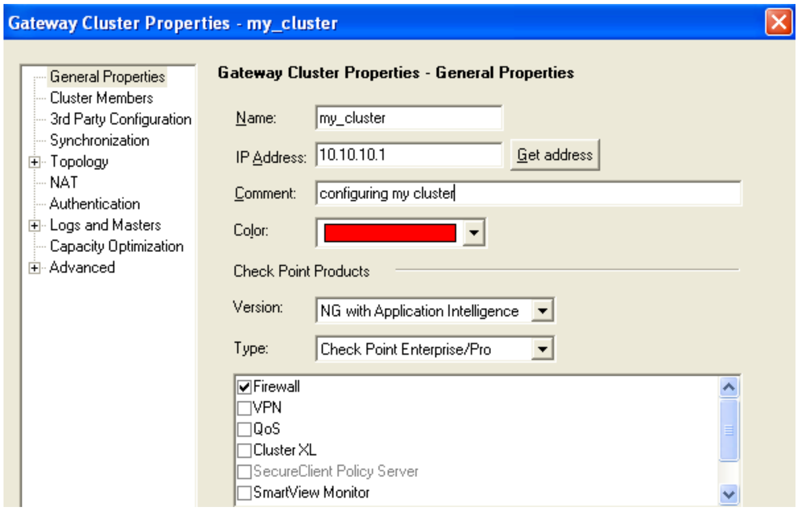
- Define your Crossover Network and preferably configure for 100 MB/s F/D
- Ensure your Antispoofing Nets (AS) are defined in SmartCenter.

SmartCenter Configuration

Open SmartCenter, Click Manage, Network Objects, New….



- Under General Properties – **IP Address**: Enter the VIP you picked for the cluster ex: (10.10.10.3)



Gateway Cluster Properties - my_cluster

Gateway Cluster Properties - General Properties

Name: my_cluster

IP Address: 10.10.10.1

Comment: configuring my cluster

Color: 🟥

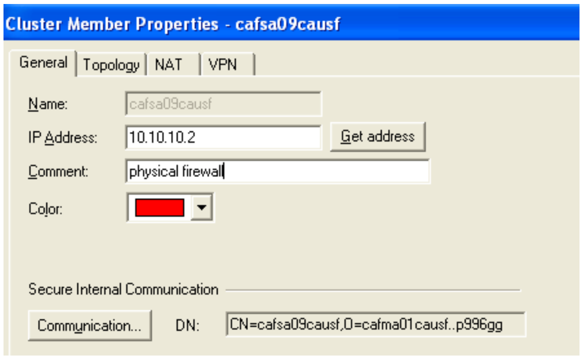
Check Point Products

Version: NG with Application Intelligence

Type: Check Point Enterprise/Pro

☑ Firewall
□ VPN
□ QoS
□ ClusterXL
□ SecureClient Policy Server
□ SmartView Monitor

- Ensure the Version = NG with Application Intelligence.
- Click Cluster Members, and click "**Add**" followed by "**Add Gateway to Cluster".** Add Firewall 1, then Firewall 2. Select one of the firewalls, and click Edit:



Cluster Member Properties - cafsa09causf

Name: cafsa09causf

IP Address: 10.10.10.2

Comment: physical firewall

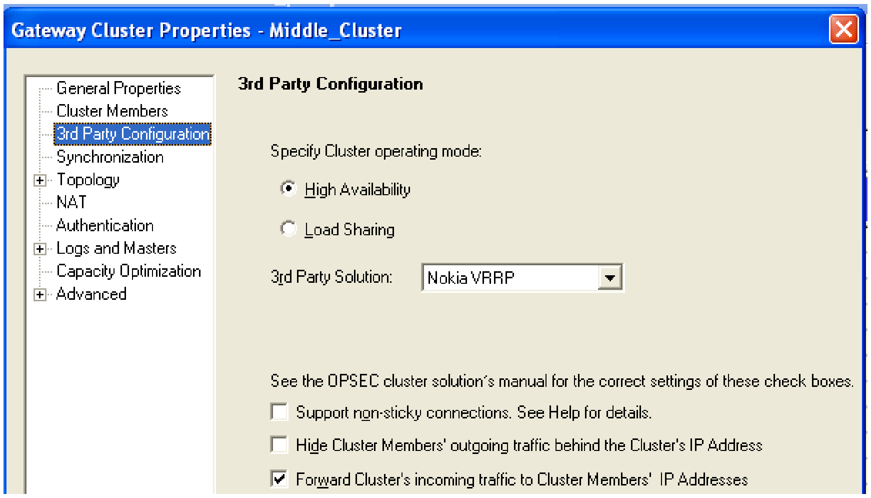
Color: 🟥

Secure Internal Communication

DN: CN=cafsa09causf,O=cafma01causf..p996gg

- Click the **Communication** tab, and establish SIC.
- Click **Topology**, and do a "Get interfaces", and Accept.
- Repeat for the other firewall

- Click the 3rd **Party Configuration** tab: Ensure mode=High Availability and solution=Nokia VRRP are selected



3rd Party Configuration

Specify Cluster operating mode:

● High Availability

○ Load Sharing

3rd Party Solution: Nokia VRRP

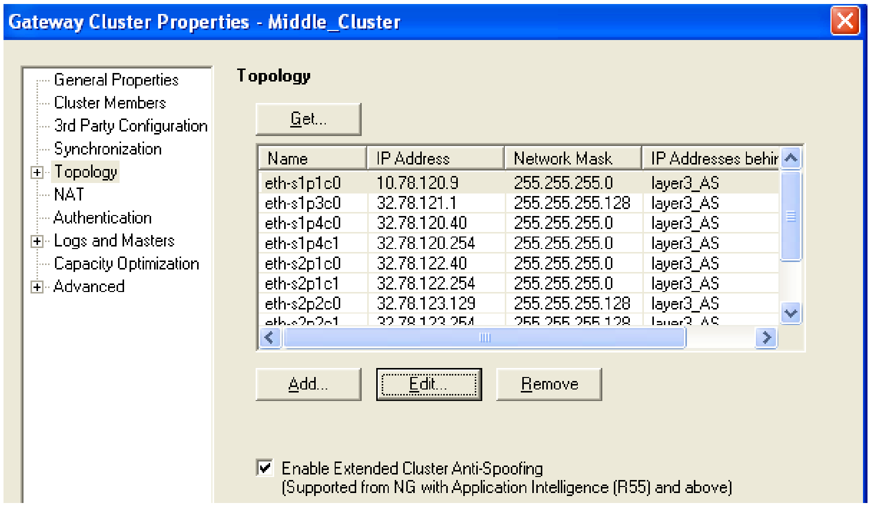
See the OPSEC cluster solution's manual for the correct settings of these check boxes.

□ Support non-sticky connections. See Help for details.

□ Hide Cluster Members' outgoing traffic behind the Cluster's IP Address

☑ Forward Cluster's incoming traffic to Cluster Members' IP Addresses

- Click the **Synchronization** tab. Add the Crossover Network subnet in here.
- Click the **Topology** tab. Enter each **VIP and Subnet Mask** defined in your Monitored Circuits. For multiple VIPs **on the same interface**, use increments of the NIC identifier c0, c1, c2, etc. Example: eth-s1p1c0 would be the primary IP, c1 the next VIP, c2 the next VIP.
- Click **Edit, Topology,** and set the required Topology Antispoofing Network Group. If you don't want Antispoofing (Bad!) leave Toplogy undefined and you will receive warning errors later.

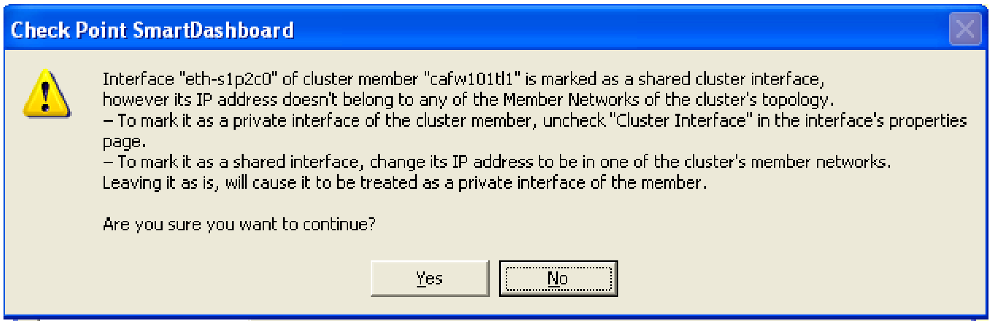


Topology

Name	IP Address	Network Mask	IP Addresses behir
eth-s1p1c0	10.78.120.9	255.255.255.0	layer3_AS
eth-s1p3c0	32.78.121.1	255.255.255.128	layer3_AS
eth-s1p4c0	32.78.120.40	255.255.255.0	layer3_AS
eth-s1p4c1	32.78.120.254	255.255.255.0	layer3_AS
eth-s2p1c0	32.78.122.40	255.255.255.0	layer3_AS
eth-s2p1c1	32.78.122.254	255.255.255.0	layer3_AS
eth-s2p2c0	32.78.123.129	255.255.255.128	layer3_AS
eth-s2p2c1	32.78.123.254	255.255.255.128	layer3_AS

☑ Enable Extended Cluster Anti-Spoofing
(Supported from NG with Application Intelligence (R55) and above)

Click **OK** when you're done. You might see the following message or similar:



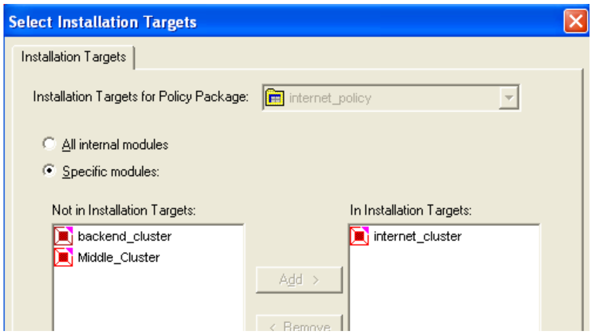
Interface "eth-s1p2c0" of cluster member "cafw101tl1" is marked as a shared cluster interface, however its IP address doesn't belong to any of the Member Networks of the cluster's topology.
– To mark it as a private interface of the cluster member, uncheck "Cluster Interface" in the interface's properties page.
– To mark it as a shared interface, change its IP address to be in one of the cluster's member networks.
Leaving it as is, will cause it to be treated as a private interface of the member.

Are you sure you want to continue?

This usually occurs because the **CrossOver** network is marked as a cluster when it is really not. This message can be safely ignored, but if you really want to avoid it, go into the Cluster Object, click “Cluster Members”, pick each firewalls **CrossOver** interface, click “Edit” and uncheck “Cluster Interface”. **This message can also occur if you have accidently missed adding a VIP to the Cluster Topology tab.**

Note: If you had previously defined Antispoofing settings, when you select High Availability and Nokia VRRP under the 3rd Party Configuration tab, all your AS settings will be deleted from the physical cluster members. This is normal, as in NG FP3, they remain in the individual cluster member’s Topology, but in NGAI, AS is defined only in the Topology tab of the cluster object.

Note: If you have any NAT rules which have an Install On field set to a firewall object, change the Install On to *Policy Targets only, otherwise you will receive an error. Similarly, if your **Policy** Installation targets are firewalls, you will have to go into Select Targets, remove the firewalls and select the new Cluster Object as the target. (See next image).



Select Installation Targets

Installation Targets

Installation Targets for Policy Package: internet_policy

○ All internal modules

● Specific modules:

Not in Installation Targets:

backend_cluster
Middle_Cluster

In Installation Targets:

internet_cluster

- Make sure your **Installation Target** is the cluster object for your Policy Installs.

- Click **Install Policy,** and **OK.** The policy should be installed to the cluster object. Rectify any Antispoofing errors by verifying you have all VIPs in the Cluster Topology tab and each has an antispoofing network defined.

- Open **SmartView Tracker**, and set the Origin= to filter on the Cluster Object. Ex: my_cluster. The primary (active) cluster firewall should be showing traffic.

- Verify your traffic is in state synchronization by running the following commands on each firewall in the cluster on the IPSO console:

cpstat ha

Should return:

```
Product name: High Availability
Version:      N/A
Status:       OK
HA installed: 1
Working mode: Sync only (IPSO cluster) HA started:   yes
```

cphaprob state

Should return: (your xover subnet will be shown)

```
Number     Unique Address  Firewall State (*)
1 (local)  10.10.100.8     active
2          10.10.100.7     active
```

fw tab –t connections –s (run on each firewall): The **PEAK** column should show no >10% difference:

```
firewall_A[admin]# fw tab -t connections -s
HOST          NAME                    ID #VALS #PEAK #SLINKS
localhost     connections            8158   874  1070   2502

firewall_B[admin]# fw tab -t connections -s
HOST          NAME                    ID #VALS #PEAK #SLINKS
localhost     connections            8158   886  1075   2549
```