



NetWyl Informatik
IT-Security Experts

Checkpoint ClusterXL Configuration

Version 1.0

Dokument Name: Checkpoint_ClusterXL Configuration

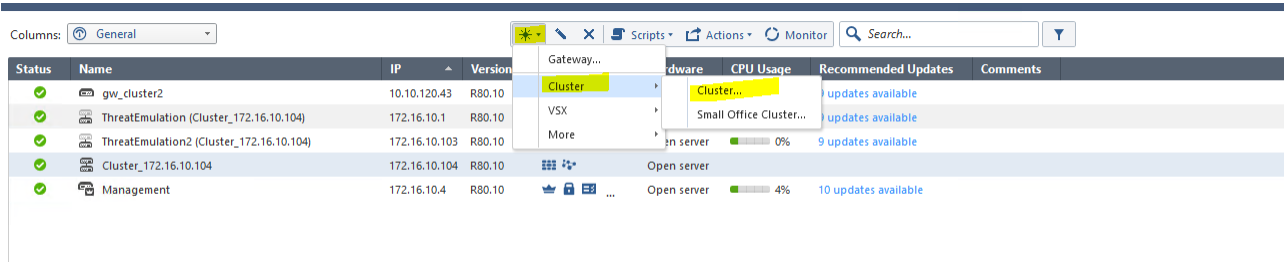
Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

Copyright 2024 NetWyl Informatik

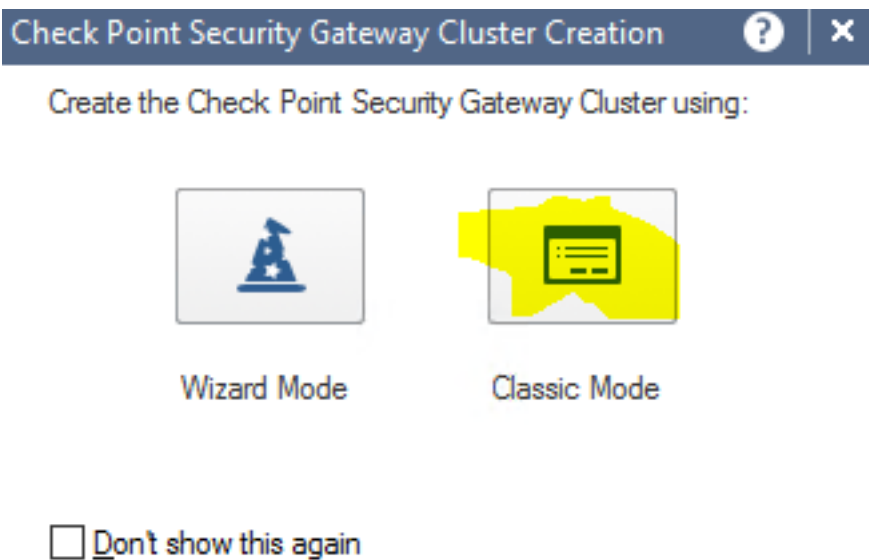
NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

1. for New Object -> Cluster -> Cluster



Status	Name	IP	Version	Gateway...	Hardware	CPU Usage	Recommended Updates	Comments
✓	gw_cluster2	10.10.120.43	R80.10	Cluster			updates available	
✓	ThreatEmulation (Cluster_172.16.10.104)	172.16.10.1	R80.10	VSX			updates available	
✓	ThreatEmulation2 (Cluster_172.16.10.104)	172.16.10.103	R80.10	More			updates available	
✓	Cluster_172.16.10.104	172.16.10.104	R80.10	Open server		0%	9 updates available	
✓	Management	172.16.10.4	R80.10	Open server		4%	10 updates available	

2. Choose Either Wizard mode or Classic mode. In that example we choose a classic mode



3. Give your Cluster a name, IP address of the cluster.

Gateway Cluster Properties - Cluster_172.16.10.104

General Properties

- Cluster Members
- ClusterXL and VRRP
- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- IPSec VPN
- VPN Clients
- Logs
- Fetch Policy
- Optimizations
- Hit Count
- Other

Machine

Name: Color:

IPv4 Address:

IPv6 Address:

Comment:

Platform

Hardware: Version: OS:

Network Security (3)

<input checked="" type="checkbox"/> Firewall	<input type="checkbox"/> IPS	Advanced Networking & Clustering:	
<input checked="" type="checkbox"/> IPSec VPN	<input type="checkbox"/> Anti-Bot		
<input type="checkbox"/> Policy Server	<input type="checkbox"/> Anti-Virus		
<input type="checkbox"/> Mobile Access	<input type="checkbox"/> Threat Emulation		
<input type="checkbox"/> Application Control	<input type="checkbox"/> Threat Extraction		
<input type="checkbox"/> URL Filtering	<input type="checkbox"/> Anti-Spam & Email Security		
<input type="checkbox"/> Data Loss Prevention	<input type="checkbox"/> Identity Awareness		
	<input type="checkbox"/> Contact Assessment		
			<input type="checkbox"/> Dynamic Routing
			<input type="checkbox"/> SecureXL
		<input type="checkbox"/> QoS	
		<input checked="" type="checkbox"/> ClusterXL	
		<input type="checkbox"/> Monitoring	

4. In cluster Members add your 2 existing gateways you want to add you your cluster and establish SIC, if it has not been established before.

5. It will fetch the topology after, you have successfully established SIC.

Gateway Cluster Properties - Cluster_172.16.10.104

Get Interfaces... Edit Actions Search... 3 items

Name	Topology	Virtual IP	ThreatEmu...	ThreatEmu...	Comments
eth0	External	10.10.120.104/24	10.10.120.103/24	10.10.120.102/24	
eth1	This network	172.16.10.105/24	172.16.10.103/24	172.16.10.1/24	
eth2	This network	192.168.1.105/24	192.168.1.103/24	192.168.1.1/24	

6. We are going to add the Gateways that we have created and make them a part of the cluster.

7. Now we need to define

- External interfaces of your Gateways + 1 shared Virtual IP address
- Internal Interfaces of your Gateways + 1 shared Virtual IP address
- Internal Interfaces of your Gateways + 1 shared Virtual IP address
- Sync interfaces (to synchronize traffic between your Gateways) (You can combine Cluster + sync interface)

Gateway 1

- Eth0 External
- Eth1 Private leading to my management Subnet
- Eth2 Private secured Net
- Eth3 Sync

VMware ThreatEmulation

Network Management > Network Interfaces

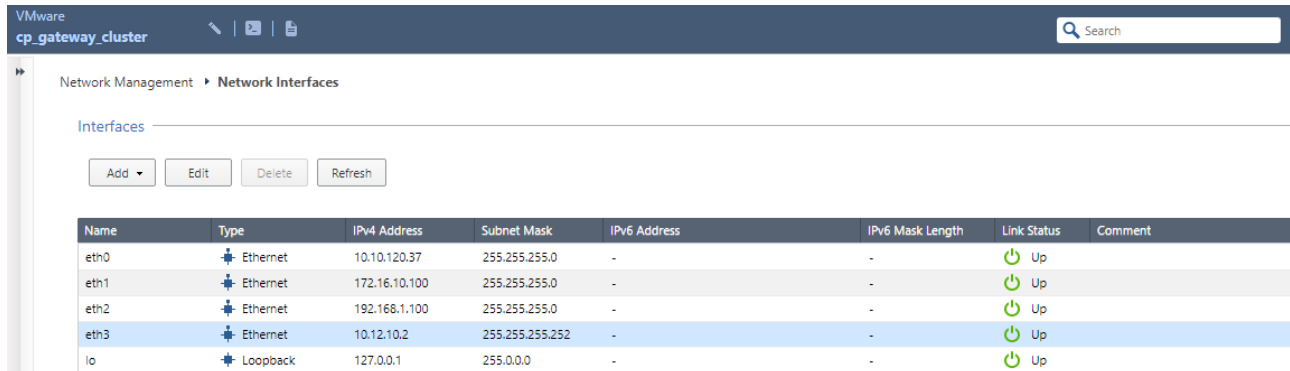
Interfaces

Add Edit Delete Refresh

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.10.120.102	255.255.255.0	-	-	Up	
eth1	Ethernet	172.16.10.1	255.255.255.0	-	-	Up	
eth2	Ethernet	192.168.1.1	255.255.255.0	-	-	Up	
eth3	Ethernet	10.12.10.1	255.255.255.252	-	-	Up	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

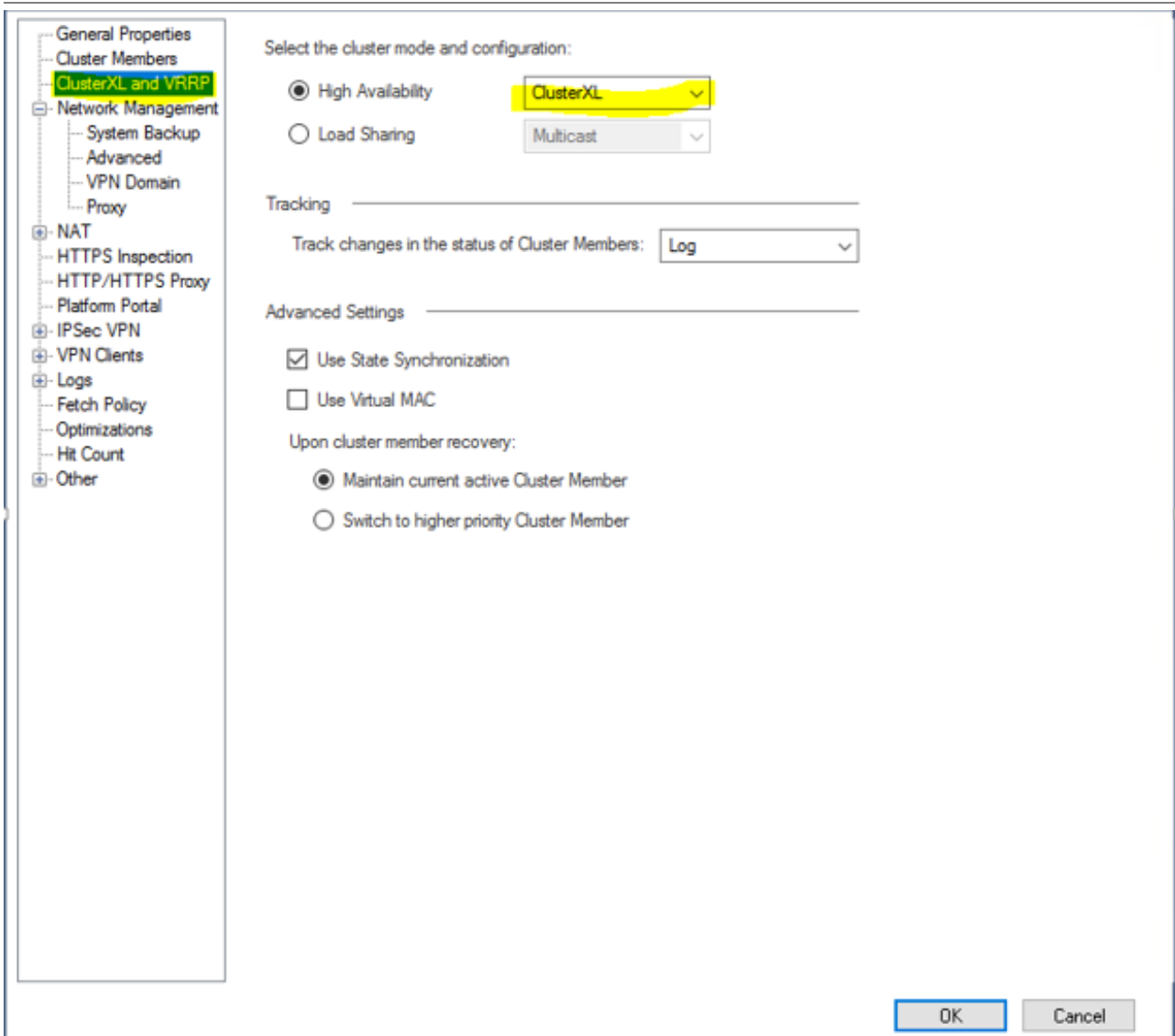
Gateway 2

- ◇ Eth0 External
- ◇ Eth1 Private leading to my management Subnet
- ◇ Eth2 Private secured Net
- ◇ Eth3 Sync



Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.10.120.37	255.255.255.0	-	-	Up	
eth1	Ethernet	172.16.10.100	255.255.255.0	-	-	Up	
eth2	Ethernet	192.168.1.100	255.255.255.0	-	-	Up	
eth3	Ethernet	10.12.10.2	255.255.255.252	-	-	Up	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

8. Fetch the topology from the SmartConsole and Define Interfaces. Network Management ◇ Get Interfaces with Topology. The configuration has to match.
9. To enable High Availability (ClusterXL) or LoadSharing setup ◇ Navigate to ClusterXL and VRRP tab



The screenshot shows the configuration interface for ClusterXL and VRRP. On the left is a navigation tree with the following items: General Properties, Cluster Members, ClusterXL and VRRP (highlighted), Network Management (with sub-items: System Backup, Advanced, VPN Domain, Proxy), NAT, HTTPS Inspection, HTTP/HTTPS Proxy, Platform Portal, IPsec VPN, VPN Clients, Logs, Fetch Policy, Optimizations, Hit Count, and Other. The main configuration area is titled 'Select the cluster mode and configuration:' and contains the following options:

- High Availability: ClusterXL (selected in a dropdown menu)
- Load Sharing: Multicast (selected in a dropdown menu)

Tracking section:

Track changes in the status of Cluster Members: Log (selected in a dropdown menu)

Advanced Settings section:

- Use State Synchronization
- Use Virtual MAC

Upon cluster member recovery:

- Maintain current active Cluster Member
- Switch to higher priority Cluster Member

At the bottom right, there are 'OK' and 'Cancel' buttons.

10. On each gateway you have to SSH \diamond cpconfig \diamond Enable Cluster Membership (6)

```
admin@ThreatEmulation:~  
[Expert@ThreatEmulation:0]# cphaprob stat  
HA module not started.  
  
[Expert@ThreatEmulation:0]# cpconfig  
This program will let you re-configure  
your Check Point products configuration.  
  
Configuration Options:  
-----  
(1) Licenses and contracts  
(2) SNMP Extension  
(3) PKCS#11 Token  
(4) Random Pool  
(5) Secure Internal Communication  
(6) Enable cluster membership for this gateway  
(7) Disable Check Point SecureXL  
(8) Check Point CoreXL  
(9) Automatic start of Check Point Products  
  
(10) Exit  
Enter your choice (1-10) :6
```

11. Make sure you have the same OS, Hotfixes. (ab R81.20 ist Multiversion Cluster möglich)
12. If you are doing your Check Point Cluster in the esxi Environment. Make sure you check these in the virtual switch

General		
Advanced		
VLAN	Promiscuous mode	Accept
Security	MAC address changes	Accept
Teaming and failover	Forged transmits	Accept
Traffic shaping		
Monitoring		
Miscellaneous		

13. Publish the database and Install the policy

14. To view the status of your cluster ssh to any of your devices and type in the command "cphaprob stat". It will show the statuses of your members.

15. To manually bring of your devices down to verify your transparent cluster is working, type in the command "clusterXL_admin down".