



# Quantum Maestro Hyperscale

## Introduction

Lari Luoma | Principal Security Consultant, Maestro SME | Check Point

May 28, 2024

YOU DESERVE THE BEST SECURITY

# Agenda

Check Point Scalable Platforms

Maestro Introduction

Maestro Installation and Deployment Options

Working with Maestro Security Groups

SMO Concept

Traffic Distribution

Global Command Line

01

# Introduction to Scalable Security and Quantum Maestro

# SECURE THE ENTERPRISE

AI-Powered. Cloud-Delivered.



## SECURE THE NETWORK



### Maestro

Hyperscale Data Center

### VPN

Virtual Private Remote Access

### Force

Enterprise Firewalls

### SD-WAN

Optimized Connectivity

### Spark

SMB Suite

### Rugged

ICS Security

### IoT Protect

IoT Security

### Smart-1 Cloud

Security Management

## SECURE THE CLOUD



### Network

Cloud Access Control and Prevention

### WAF

Web Application Firewall

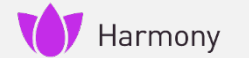
### Cloud Native Application Protection (CNAPP)

Unified Security from Code to Cloud

### Cloud Detection and Response

Contextual and Actionable Intelligence

## SECURE THE WORKSPACE



### Endpoint

Protection & Posture Management

### Email

Cloud Email and Collaboration Suite Security

### Mobile

Mobile Threat Defense

### SASE

Internet Access Private Access

### SaaS

Threat Prevention for SaaS Applications

## COLLABORATIVE SECURITY OPERATIONS & SERVICES



### Security Operations and AI

### Global Services

#### XDR/XPR

Extended Prevention and Response

#### Playblocks

Orchestration and Automation

#### Events

Unified Events

#### ThreatCloud AI

AI-Powered Threat Intelligence

#### AI Copilot

Automating Security with AI

#### MDR/MPR

Managed Prevention and Response

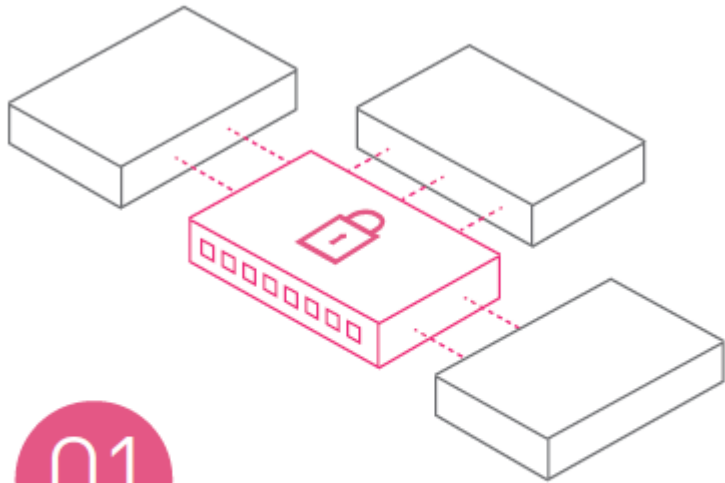
#### Incident Response

Keep Your Business Running

#### Consulting & Training

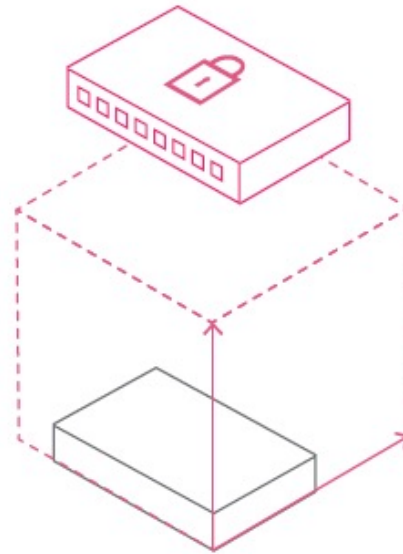
Leverage security architecture design experts

# What are the Benefits of Hyperscale Systems?



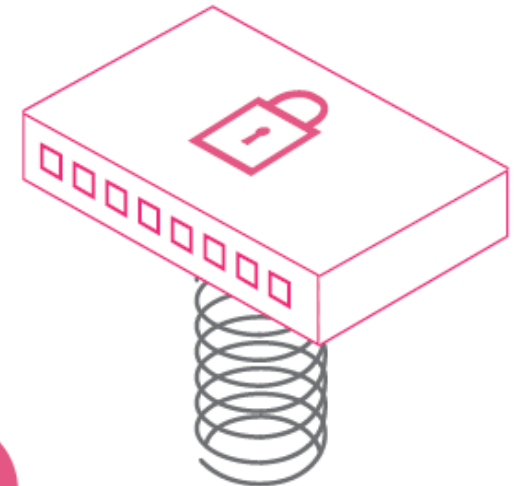
## 01 Operational Supremacy

Hyperscale deployments are managed intuitively by Hyperscale Orchestrators using the same R81.x code as maintrain / JHFAs



## 02 Hyperscale Security

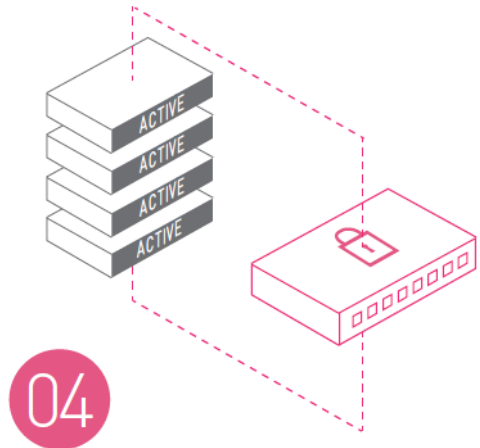
Provides seamless expansion to Hyperscale security, while protecting organizations' existing and future investments



## 03 Cloud-Level Resiliency

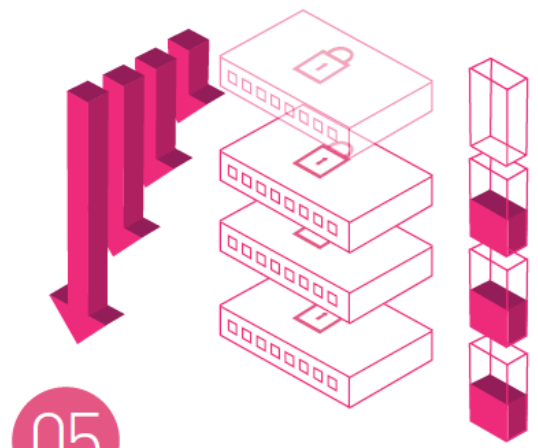
Offers cloud-level resilience and reliability to all deployments, with Check Point's patented HyperSync technology

# What are the Benefits of Hyperscale Systems?



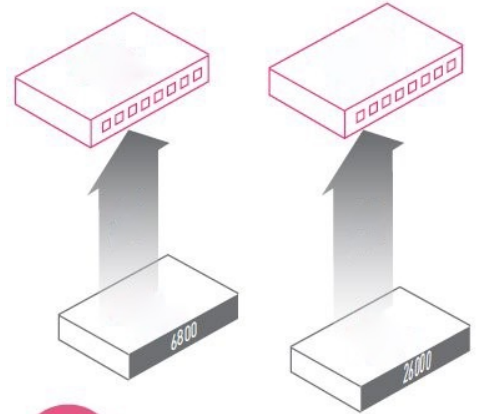
**04**  
Maximum  
Cost-Efficiency

Fully utilises all hardware  
deployed in the system



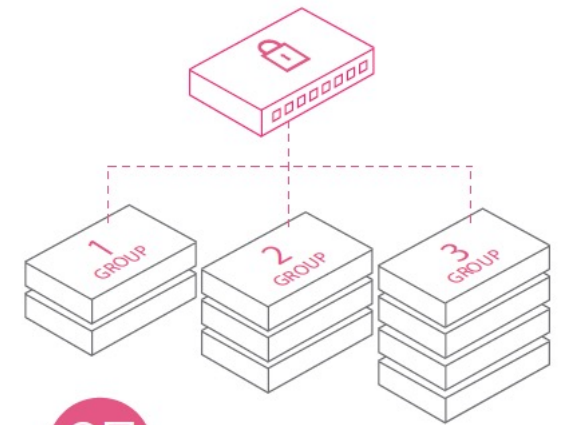
**05**  
Telco-Grade Technology

Minimise risk of  
downtime  
with N+N clustering



**06**  
Linear Scalability

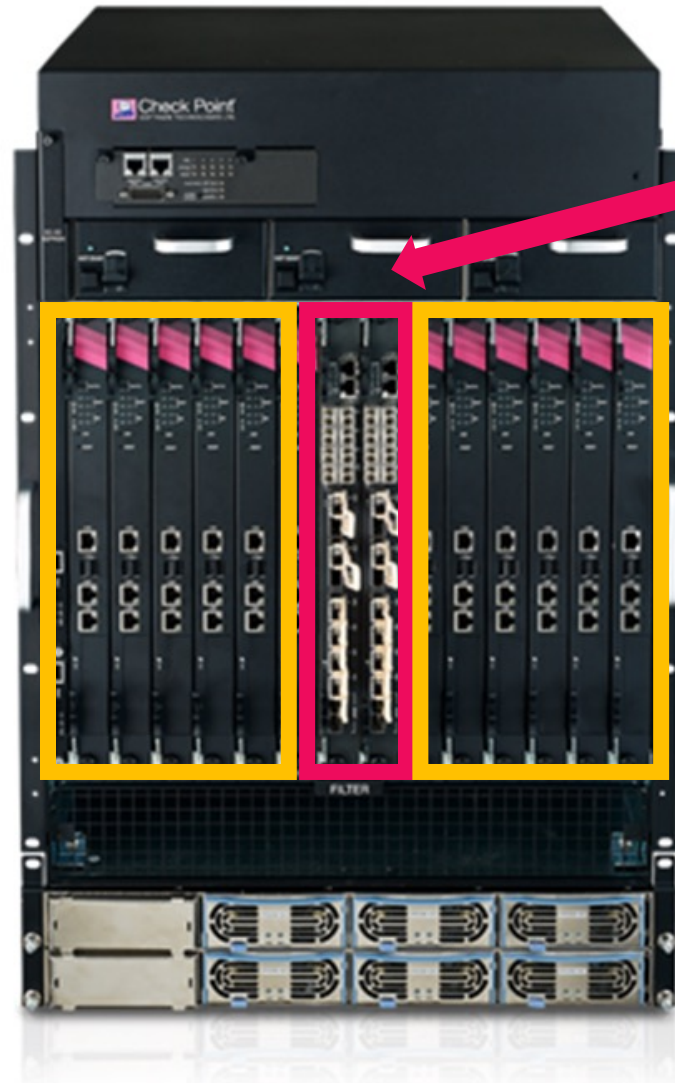
Hypersync offers unique  
Scalability when adding  
more resources



**07**  
Security Groups

Group appliances to  
perform the same  
function reducing admin  
overhead

# It all Started with a Scalable Chassis



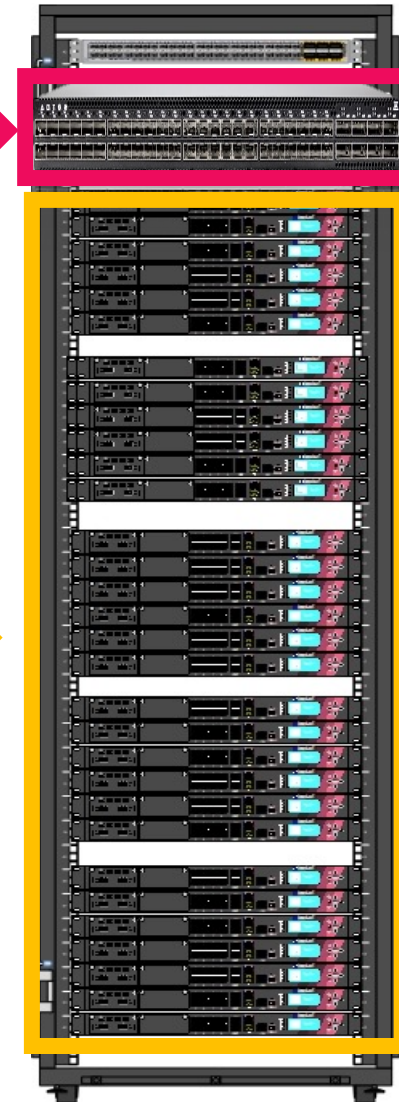
Orchestration Layer



Compute Resources

# Scalable Clustering Reinvented - Hyperscale

Orchestration Layer



Compute Resources





# The Orchestration Layer



**Maestro Hyperscale Orchestrator 140**

48 x 1/10/25GbE ports  
8 x 40/100GbE ports



**Maestro Hyperscale Orchestrator 175**

32 x 40/100GbE ports  
Options for 10/25GbE with  
adapters/splitters

# Compute Resource

All supported Appliance Models: [SK181433](#)



# Connect the Components



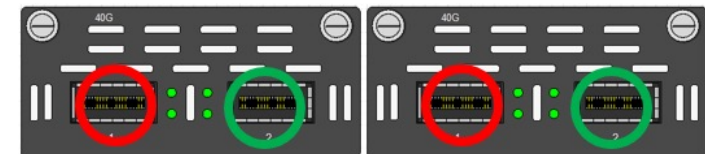
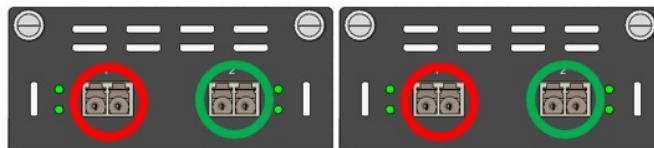
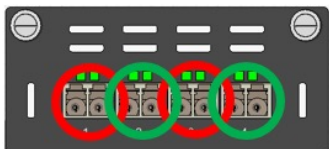
**Downlinks:** Between Appliances and Orchestrators – use **DAC or Fibre**

**Uplinks:** Between Orchestrators and your network – use **Fibre**

# Connectivity and Redundancy

- **Two orchestrators are recommended** for any location
- Always **bond your uplinks**
  - **Switches should present as a single device** towards the MHOs
- Ensure **the appliances are connected correctly** to the MHOs
  - Odd ports to Orchestrator 1, and even ports to Orchestrator 2
- Ensure you have **capacity to handle the load during upgrades**
  - On the available appliances and downlink ports

Connect 2, or 4 cables



# 02

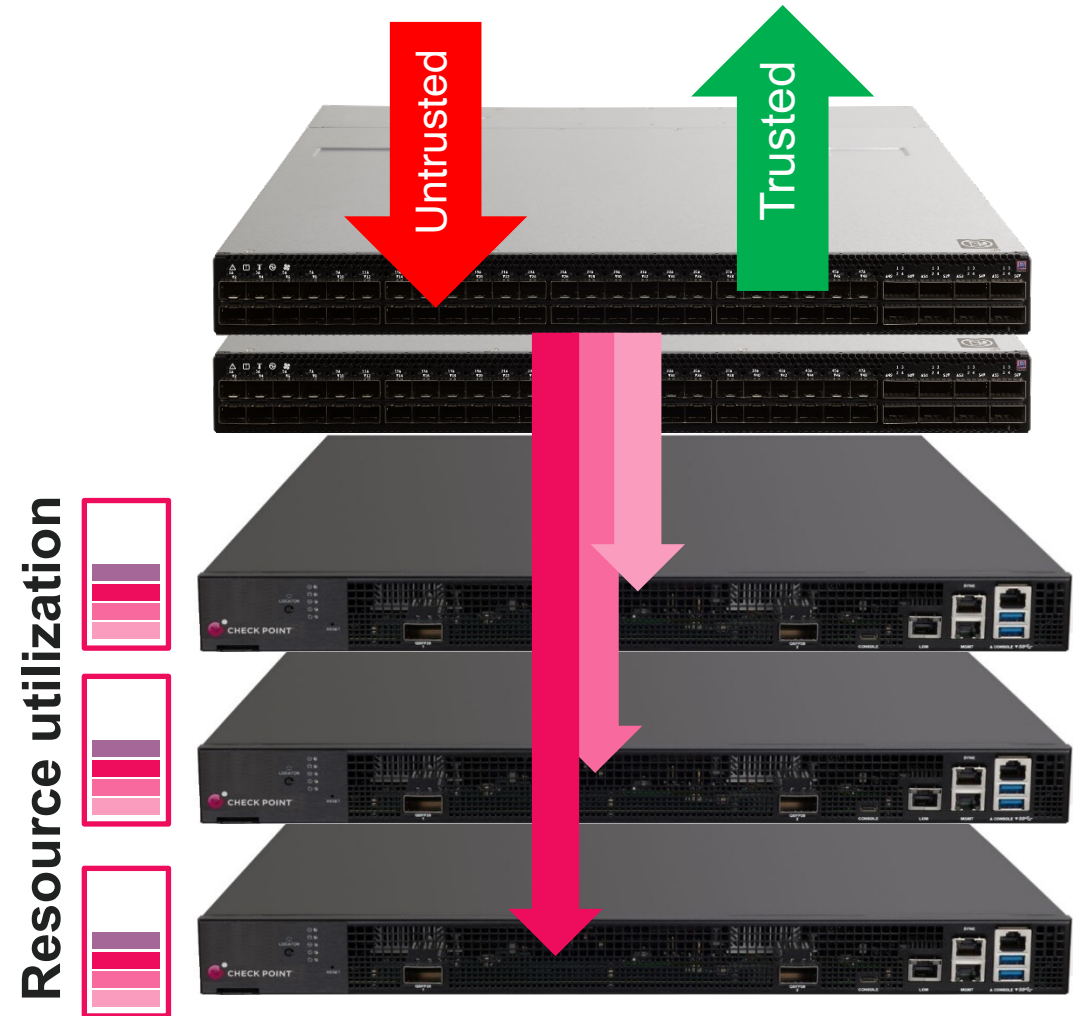
## Maestro Installation and Operation

# Traffic flow

Traffic is received from **Untrusted** networks and distributed to the appliances.

**Security** and **threat prevention** enforced on the traffic by each appliance

Traffic is then forwarded from the appliances to **trusted** networks



# Create Security Groups to mirror business needs

Physical Implementation

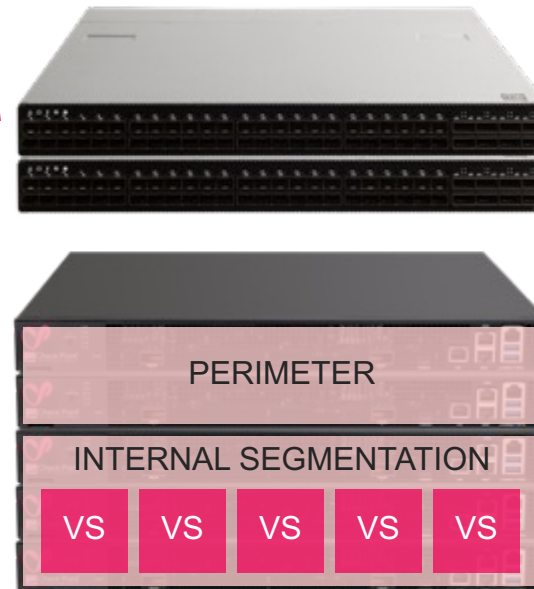
1 or 2 Maestro Hyperscale Orchestrators

Up to 14 Security Gateways per group per site

Logical Implementation

Up to 8 Security Groups

Virtual Systems



Each Security Group is an independent security gateway segregated from other security groups

# Drag and Drop Security Group Creation

Orchestrator

Security Group 1 configuration

Security Group settings   Auto Scaling settings

Topology

Name	ID	Hostname	IP address	Default Gateway
Security Groups				
Security Group 1		EMEA-SG1	172.31.100.182/22	172.31.100.1

Unassigned Interfaces

Name	Type
Port 1/5/1 (eth1-05)	ethernet

Group Settings

Group Sites and Members

Site	ID
Site 1	
Check Point 6500	1
Check Point 6500	2
Check Point 6500	3

Group Interfaces

Interface
Port 1/1/1 (eth1-Mgmt1)
Port 1/2/1 (eth1-Mgmt2)
Port 1/25/1 (eth1-25)
Port 2/25/1 (eth2-25)

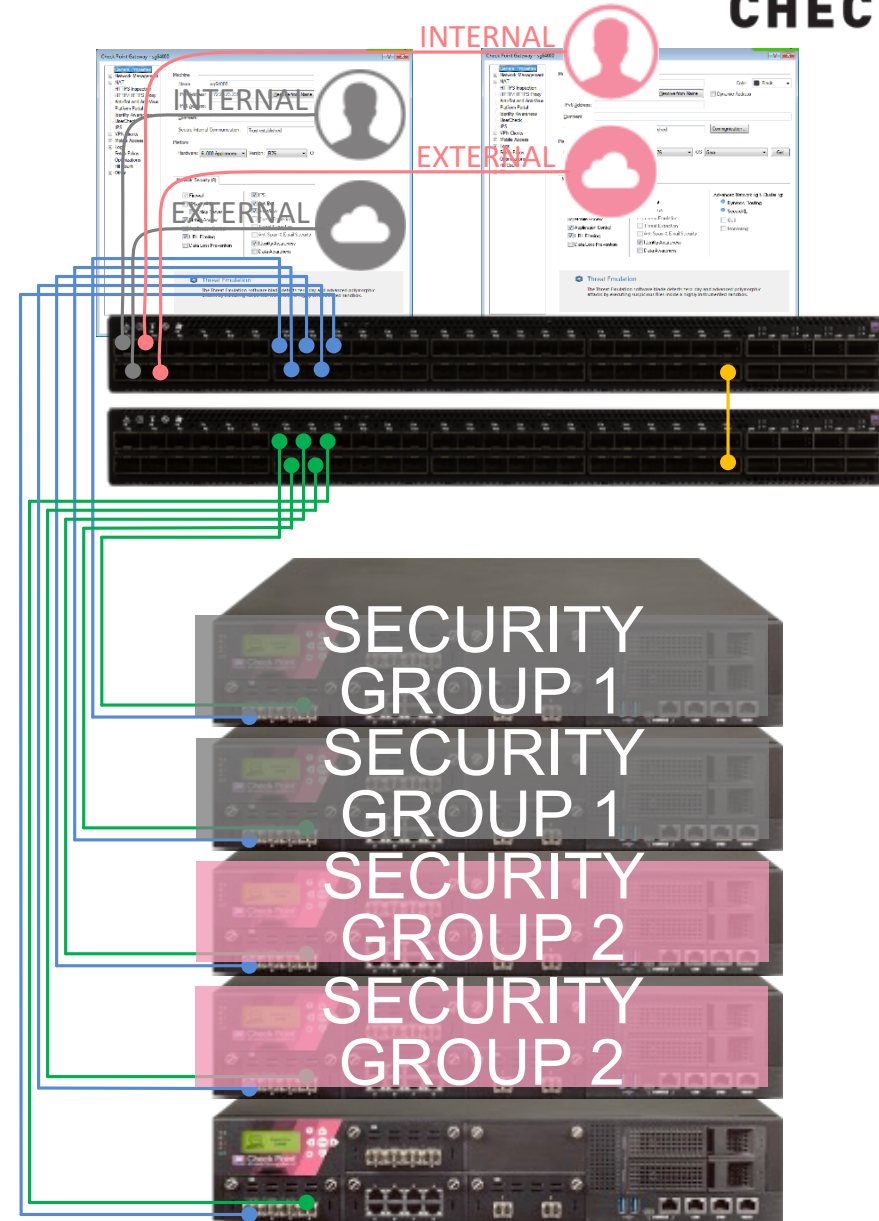
Install as VSX:

OK   Cancel



# Working with Security Groups

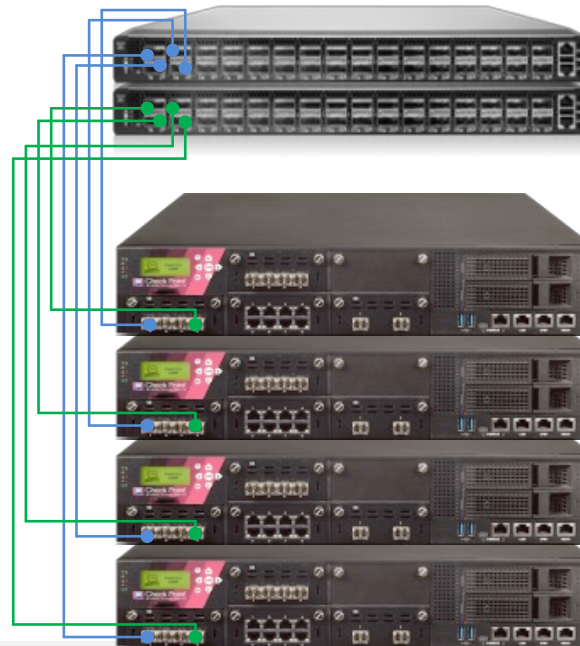
- Each SGM acts like a blade in a chassis boosting the performance of the Security Group.
- When adding a new SGM, it will clone configuration and JHFA from the SMO.
- No changes in SmartConsole necessary when adding gateways to an existing SG.
- Each SGM can only be assigned to one Security Group at a time.



# Single Management Object (SMO)

- **Single** Security GW object per Security Group in SmartC
- **Single** IP-address for management
- **Clone** all configurations between members
- **Faster** policy installation
- **Hierarchic** System Stats
- **Cluster** Abstraction

SMO Master is always the upmost active appliance in the stack.



Check Point Gateway - SecGroup1

General Properties

- Network Management
  - NAT
  - HTTPS Inspection
  - HTTP/HTTPS Proxy
  - ICAP Server
  - Platform Portal
  - Mail Transfer Agent
- Logs
  - Fetch Policy
  - Optimizations
  - Hit Count
- Other

Machine

Name: SecGroup1 Color: Black

IPv4 Address: 172.25.161.83 Resolve from Name  Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established Communication...

Platform

Hardware: Maestro Version: R81.10 OS: Gaia Get

Network Security (1) Custom Threat Prevention (0) Management (0)

Access Control

- Firewall
- IPSec VPN
- Policy Server
- Mobile Access
- Application Control
- URL Filtering
- Identity Awareness
- Content Awareness

Advanced Networking & Clustering

- Dynamic Routing
- SecureXL
- QoS
- Monitoring

Other:

- Data Loss Prevention
- Anti-Spam & Email Security

Firewall

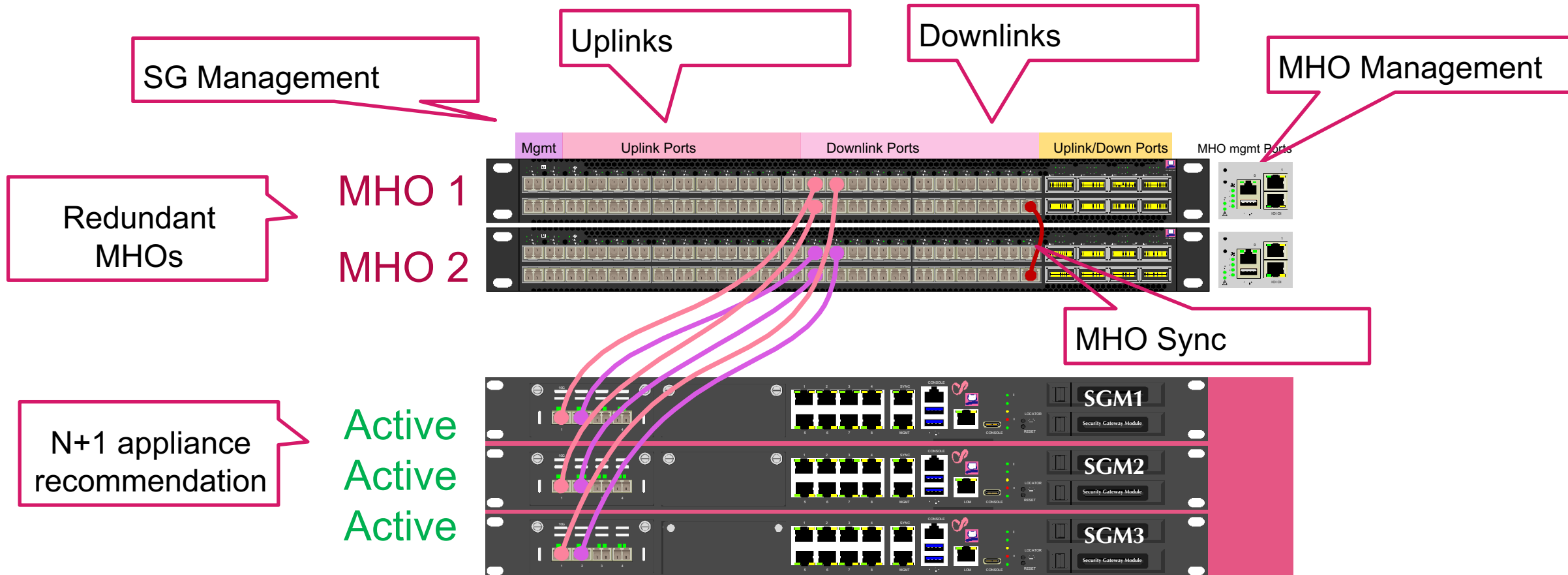
World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

OK Cancel

```
# asg_blade_config
get_smo_ip
SMO ip is: 192.0.2.1
# grep '192.0.2.1' /etc/hosts
192.0.2.1 1_01
```

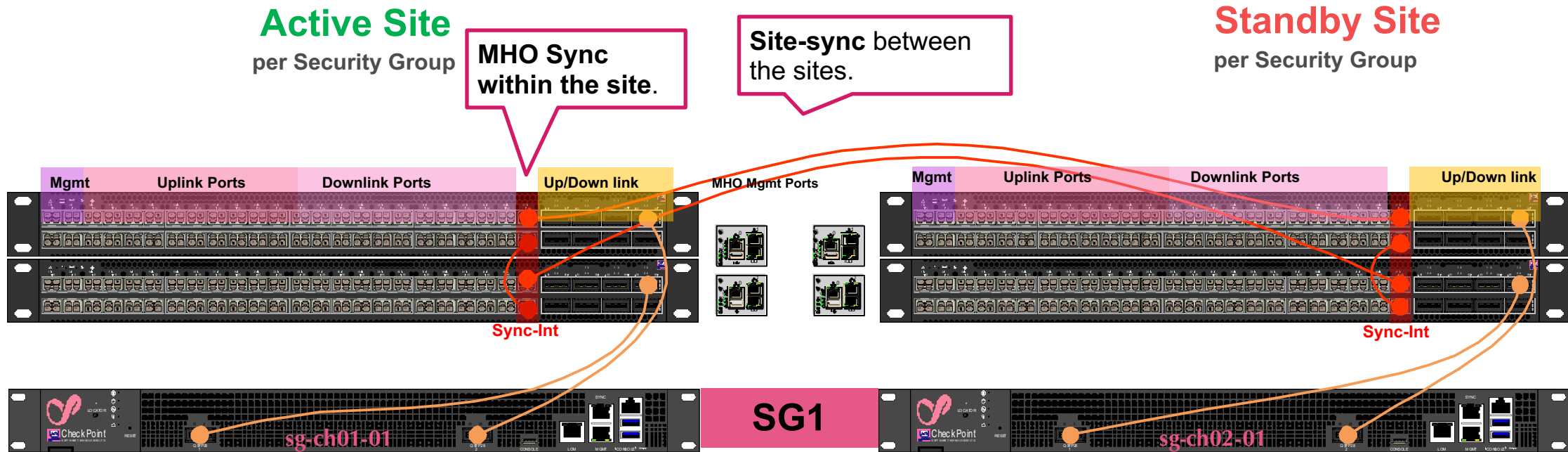
# Maestro Deployments: Single Site Maestro

MHOs and gateways on the same site. All gateways active. One entity in the network.



# Maestro Deployments: Dual Site Maestro

Operate in active/standby. One logical entity in the network.



MHO Sync within the site.

Site-sync between the sites.

Recommendation: Same number of appliances on both sites!

# Maestro Clustering



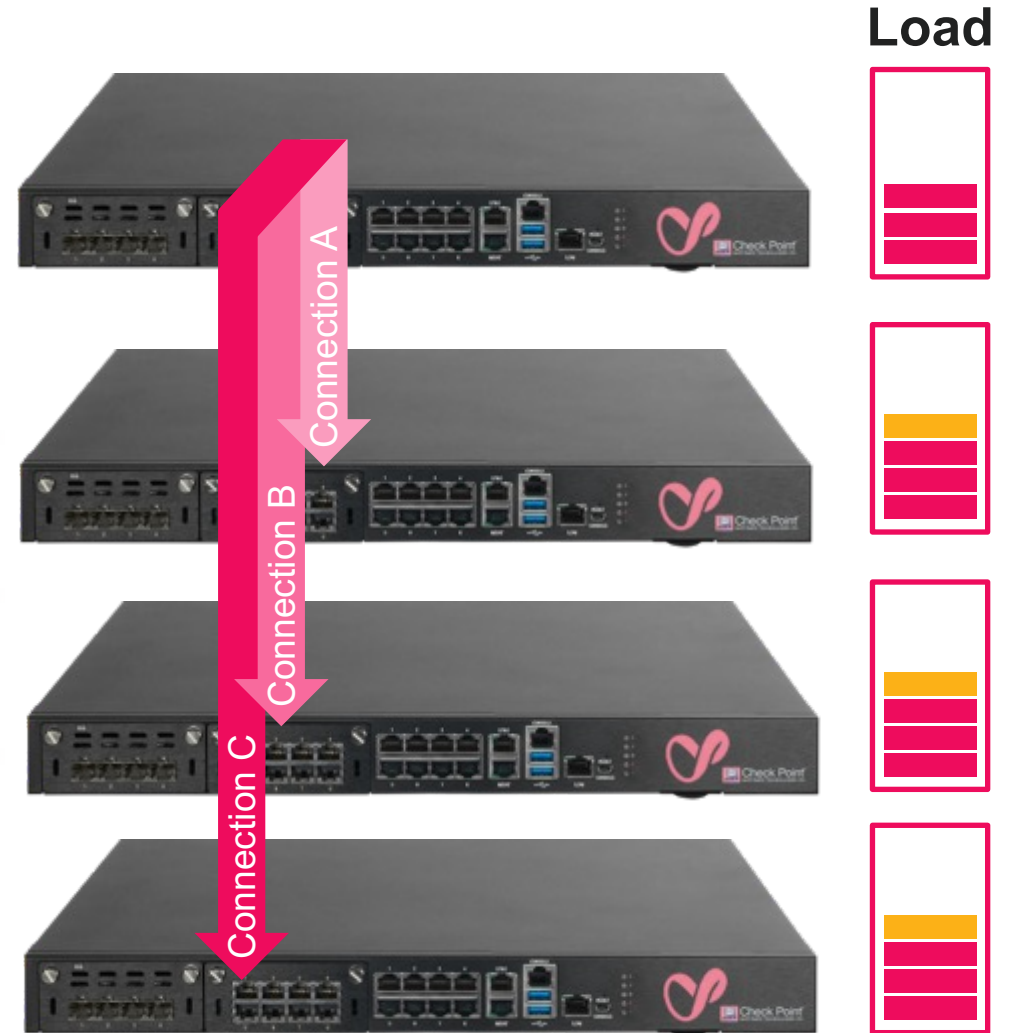
PATENT

## HyperSync

Full Redundancy within a system

Cost Efficient cluster Deployment

All Hardware resources utilized



# Traffic Distribution

- Traffic load-balancing mechanism across Security Group members
  - Calculated dynamically, members can be seamlessly added/removed
  - Uses combinations of Source/Destination IP-addresses and ports
- Sk168814 – Recommendation
  - Perimeter (NAT): Auto Topology (default)
  - Data Center (no NAT): Manual General
  - Disable L4-mode unless told to be enabled by Check Point support or PS (*set distribution l4-mode disabled*)

# Traffic Distribution

## Single Site - Perimeter

```
# gclish -c "show distribution configuration"; dxl stat
Distribution Mode: auto-topology (per-port)
Chassis:  Blade:  State:      Distribution:
1         1         Active      33.4%  171/512
1         2         Active      33.4%  171/512
1         3         Active      33.2%  170/512
1         4         Not In Group -
1         5         Not In Group -
1         6         Not In Group -
1         7         Not In Group -
1         8         Not In Group -
1         9         Not In Group -
1        10         Not In Group -
1        11         Not In Group -
1        12         Not In Group -
1        13         Not In Group -
1        14         Not In Group -

Chassis:  Activity:
1         Active

General Mode  : Disabled
Control Blade : Disabled
Static Mode   : Disabled
```

## Dual Site – Data Center

```
# gclish -c "show distribution configuration"; dxl stat
Distribution Mode: manual-general
Chassis:  Blade:  State:      Distribution:
1         1         Active      100.0%  512/512
1         2         Not In Group -
1         3         Not In Group -
1         4         Not In Group -
1         5         Not In Group -
1         6         Not In Group -
1         7         Not In Group -
1         8         Not In Group -
1         9         Not In Group -
1        10         Not In Group -
1        11         Not In Group -
1        12         Not In Group -
1        13         Not In Group -
1        14         Not In Group -
2         1         Active      100.0%  512/512
2         2         Not In Group -
2         3         Not In Group -
2         4         Not In Group -
2         5         Not In Group -
2         6         Not In Group -
2         7         Not In Group -
2         8         Not In Group -
2         9         Not In Group -
2        10         Not In Group -
2        11         Not In Group -
2        12         Not In Group -
2        13         Not In Group -
2        14         Not In Group -

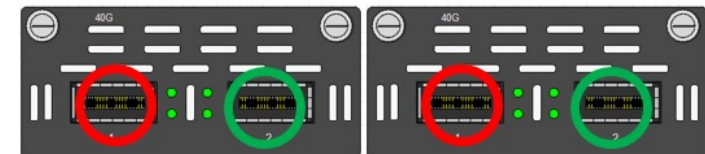
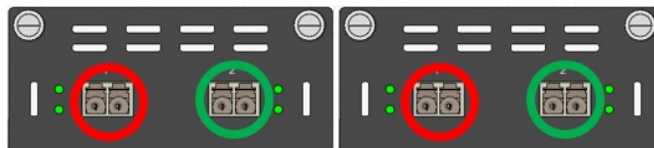
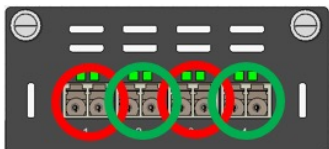
Chassis:  Activity:
1         Active
2         Standby

General Mode  : Enabled
Control Blade : Disabled
Static Mode   : Disabled
```

# Deployment Tips – Redundancy

- **Two orchestrators are recommended** for any location
- Always **bond your uplinks**
  - **Switches should present as a single device** towards the MHOs
- Ensure **the appliances are connected correctly** to the MHOs
  - Odd ports to Orchestrator 1, and even ports to Orchestrator 2
- Ensure you have **capacity to handle the load during upgrades**
  - On the available appliances and downlink ports

Connect 2, or 4 cables





# Deployment Tips – CLI goes Global

```
[Global] DR-SG01-VSX-ch01-01:0> set interface magg0 comments "Management"  
1_01:  
success  
  
1_02:  
success  
  
1_03:  
success  
  
1_04:  
success  
  
[Global] DR-SG01-VSX-ch01-01:0> █
```

## Best Practices:

- Commands **Synchronized** to all gateways
- **Automatic SAVE**
- **Expert-mode** commands can be run globally with **global prefixes**
- **Avoid** use of local CLISH

# Moving Between Components

# m

member  
command

## How does it work?

`m` is an SSH wrapper.  
You could also type:  
`ssh 1_02` or `ssh 1_02`

`m` re-uses your `username` and looks up the pre-configured entries in `/etc/hosts` to connect.

- You can connect between components using the `m`-command (short for member).  
Example: `m 1_02`
- You can also use just the SGM number, e.g. `m 2`. This will connect you to that SGM on the site you are currently connected to.
- To connect MHO from SGM use `m ssm1` or `m ssm2`

```
[Expert@SG1-md-ch01-01:0]# m 2
Moving to member 1_2
This system is for authorized use only.
Last login: Mon May  2 23:07:38 2022 from 192.0.2.1
You have logged into the system.
Warning: System diagnostics failed on the following tests: Licenses.
[Expert@SG1-md-ch01-02:0]# m 2_1
Moving to member 2_1
Warning: Permanently added '192.0.2.15' (ECDSA) to the list of known hosts.
This system is for authorized use only.
Last login: Mon May  2 23:07:54 2022 from 192.0.2.16
You have logged into the system.
Warning: System diagnostics failed on the following tests: Licenses.
[Expert@SG1-md-ch02-01:0]# m 2
Moving to member 2_2
Warning: Permanently added '192.0.2.16' (ECDSA) to the list of known hosts.
This system is for authorized use only.
Last login: Mon May  2 23:07:42 2022 from 192.0.2.1
You have logged into the system.
Warning: System diagnostics failed on the following tests: Licenses.
[Expert@SG1-md-ch02-02:0]#
```

```
[Expert@LAB-test-ch01-01:0]# m ssm1
Moving to ssm1
The authenticity of host 'ssm1 (198.51.101.126)' can't be established.
RSA key fingerprint is 35:ae:ce:6b:50:51:4f:bc:61:05:be:1f:8c:76:55:c3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ssm1,198.51.101.126' (RSA) to the list of known hosts.
This system is for authorized use only.
admin@ssm1's password:
Last login: Wed Oct 21 23:48:48 2020 from 172.25.215.195
[Expert@MH0140_01-AN32:0]#
```

# Running Commands Globally in Expert-mode

- Expert-mode is always local to the SGM where you are connected to.
- Maestro allows running commands globally also in expert-mode by using global prefixes of `g_`, `g_all`, `g_allc` and `gexec`.
- You can also run commands on specific blades by using `-b` switch.
- `g_` is not supported by all commands, `g_allc` shows the output in the same format in one line that can be useful in some cases.

- `gexec` allows execution of commands on specific blades.

```
[Expert@lab-ch01-01:0]# g_cat /home/admin/testfile
-*- 2 blades: 1_01 1_02 -*-
This is a testfile!!!

[Expert@lab-ch01-01:0]# g_all 'cat /home/admin/testfile'
1_01:
This is a testfile!!!
1_02:
This is a testfile!!!
[Expert@lab-ch01-01:0]# g_allc 'cat /home/admin/testfile'
[1_01]This is a testfile!!!
[1_02]This is a testfile!!!
[Expert@lab-ch01-01:0]# g_allc 'cat /home/admin/testfile'
-*- 2 blades: 1_01 1_02 -*-
This is a testfile!!!

[Expert@lab-ch01-01:0]# █
```

```
[Expert@lab-ch01-01:0]# gexec -b 1_01-1_02 -c 'tail /home/admin/testfile'
[1_01]This is a testfile!!!
[1_02]This is a testfile!!!
[Expert@lab-ch01-01:0]# █
```



# 03

## R82 Features

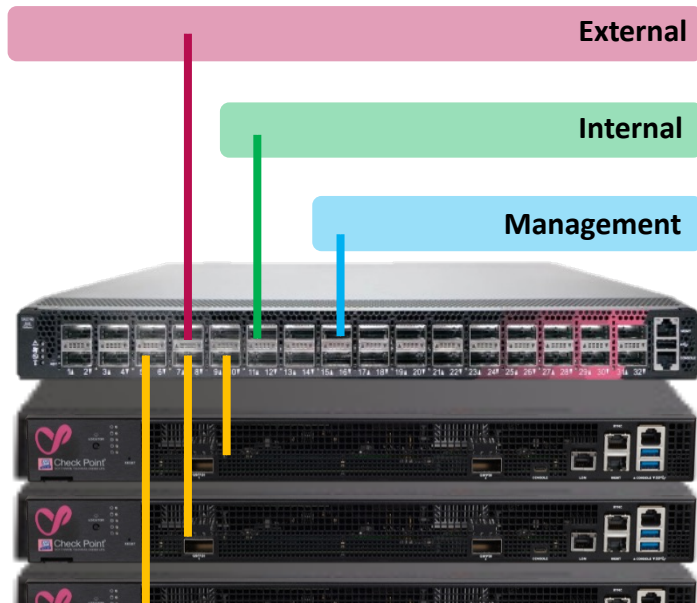
# R82 in Maestro

- R82 is Check Point's newest software release (coming up in 2024). Fully supported in Maestro.
- The focus in Maestro is Simplification and Unification
- We provide a “One gateway for All” mindset - One ISO
- Users of Maestro will see operations get simpler
- Users of the new ElasticXL solution will see many of the Maestro benefits carried over
- Activities will have common look and feel, and unified command set, tools and utilities

# Maestro vs. ElasticXL

## Maestro

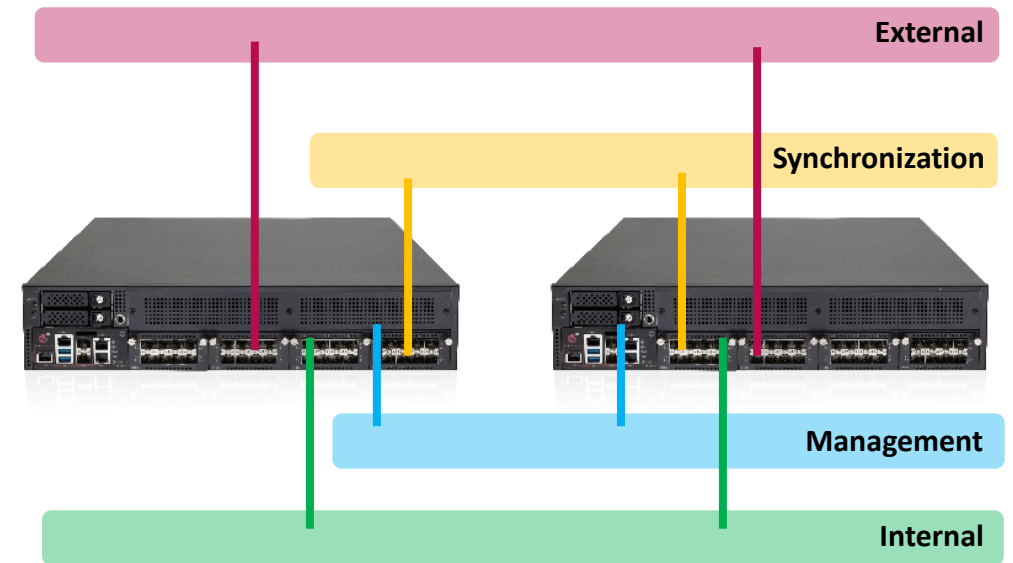
- Hardware-based load balancer with **linear scaling**
- Unique separate orchestration layer (up to 8 security groups)
- Simplified cabling & integration



Up to 14 appliances per security Group per site

## ElasticXL

- **Simplified** & automated clustering
- Up to three nodes per site (in 1 group)
- Pivot mode-based traffic forwarding



Up to 3 appliances per security Group per site

# One Gateway For All

## Unification

The image displays two screenshots of Check Point Cluster Management interfaces, illustrating the unification of Maestro and ElasticXL.

**Maestro Cluster Management (Top Screenshot):**

- View mode: Basic
- Cluster Gateways: 4 items
- Table columns: Status, Name, Model, Version, Serial-number, CPU, RAM, Throughput, Disk space
- Table data:

Status	Name	Model	Version	Serial-number	CPU	RAM	Throughput	Disk space
✓	Site 1							
✓	SG1-s01-01	Maestro	R82	2228BA4465	63%	21%	0.0004425048828125 Mbps	OK
✓	SG1-s01-02	Maestro	R82	2228BA4552	34%	21%	0 Mbps	OK
✓	SG1-s01-03	Maestro	R82	2228BA4559	33%	23%	0 Mbps	OK
✓	SG1-s01-04	Maestro	R82	2228BA4535	43%	22%	0 Mbps	OK

**ElasticXL Cluster Management (Bottom Screenshot):**

- View mode: Advanced
- Cluster Gateways: 2 items
- Table columns: Status, Name, Model, Version, Serial Number, CPU, RAM, Throughput, Disk space
- Table data:

Status	Name	Model	Version	Serial Number	CPU	RAM	Throughput	Disk space
✓	Site 1							
✓	Jaguar-16200-s01-01	Check Point 16200	R82	LR202103001094	0%	10%	0 Mbps	OK
✓	Jaguar-16200-s01-02	Check Point 16200	R82	LR202011018435	0%	10%	0 Mbps	OK

Maestro  
Cluster  
Management

ElasticXL  
Cluster  
Management

# One Gateway For All

## System Overview

Model	Check Point 16200
OS Role	Check Point VSNext
CPU Amount	0
Policy Name	Standard
Version	R82
Kernel	4.18.0-372.9.lcp86_64
Edition	64-bit
Build Number	293
System Uptime	36 minutes
Recommended Software Updates	No new recommended Jumbo Hotfix detected.

## Software Blades

Firewall	Evaluation
Virtual Systems	Evaluation

## HCP Score

0

## Throughput

Data	134.27K	Mgmt	298	Sync	0
	Kbps		Kbps		

## Connection Rat

0 cps

## Connections

63

## Packets Rate

298 pps

## Cpu Avg.

0 %

## Memory Usage A

10 %

## /

35 %

## /boot

45 %

## /var/log

1 %

Insights on MHO

## Cluster Members Overview

ID	Model	Version	Throughput	Packet Rate	Conn. Rate	Conn.	CPU Usage	FW/SND	Memory Usage	State	Notes	HCP Score	Last Update
1	Check Point 16200	R82	0	0	0	18	0	(0/0) 0/0	10	ACTIVE	None	0	7
2	Check Point 16200	R82	134.27K	298	0	45	0	(0/0) 0/0	10	ACTIVE	None	0	6

Insights on ElasticXL



# R82: Monitoring Maestro

All 1 2 15 16

Run it

Report Date: 2024-01-10 19:51:37

Idx	Member	Name	Description	Result
1	16	Blocker handlers check	Inspecting US processes log for block handlers	Success
2	16	Orchestrators ports link integrity	This test checks the Orchestrators ports link integrity.	Warning
3	16	Orchestrators SX API	This test checks if the Orchestrators SX API is responding to commands.	Success
4	16	ASIC sanity	The purpose of this test is to determine if the system recognizes the ASIC.	Success
5	16	Orchestrators kernel modules	This test checks if the Orchestrators kernel modules are loaded.	Success
6	16	Security Appliances physical connections	This test checks if the Security Appliances' physical connections are connected to Orchestrators as expected.	Success
7	16	maestro.json Configuration Sanity	This test checks that there are no missing values in maestro.json and that the relevant values are identical on all Orchestrators.	Success
8	16	smodb.json Configuration Sanity	This test checks that there are no missing values in smodb.json and that the relevant values are identical on all Orchestrators.	Success
9	16	Daemons state	This test checks if the Orchestrators daemons are up	Error
10	16	Collect Data from Orchestrators	This test collects the required data for next tests from local and remote Orchestrators	Success
11	16	Orchestrators REST server	This test checks if the local and remote Orchestrators respond to REST requests	Success
12	16	Orchestrators reachability	This test checks if the local Orchestrator can ping the local and remote Orchestrators	Success
13	16	Read Local Configuration	This test reads local Orchestrator configuration which is required for the tests execution	Success
14	16	SSD Health	Verifying SSD SMART health	Skipped
15	16	Zombie processes	This test checks if zombie (defunct) processes exists.	Success
16	16	Soft lockup	Checking if soft lockup occurred during the last lime	Success
17	16	ARP neighbour table overflow	Checking ARP neighbour table overflow occurred during the last time	Success
18	16	Transceivers Support	This test checks that all installed transceivers are supported	Error
19	16	Memory Usage	This test verifies if memory usage (RAM) crossed threshold of 85%, and verifies additional thresholds for the different sections.	Success
20	16	Core Dumps	This test checks if there are any user mode core dumps and if possible, prints their backtrace.	Success
21	16	File Descriptors	This test verifies the usage of File Descriptors of opened processes	Success
22	16	Hardware Co		Success
23	16	ARP Cache L		Success
24	16	Interface E		Success
25	16	Kernel cras		Success
26	16	Gaia DB		Success
27	16	Software Ve		Success
28	16	SYSLOG time		Success
29	16	MTU	This test checks the MTU values on interfaces	Success
30	16	Disk Space	This test verifies that disk space usage is in the normal threshold on all file systems.	Success

Watch it

X ERROR  
X WARNING  
X INFO  
SUCCESS

Monitor operations & members activities  
Understanding the cause / reason for system activities and alerts

# R82: MHO First Time Wizard

The image displays two screenshots of the Maestro First Time Wizard on MHO, showing configuration steps for Environment, Member, Synchronization Ports, and VLAN settings.

**Environment Configuration**

- Orchestrator Amount: [ ] [▲] [▼] [?]
- Site Amount: [ ] [▲] [▼] [?]

**Member Configuration**

- Orchestrator Member ID: [ ] [▲] [▼] [?]
- Site ID: [ ] [▲] [▼] [?]

**Synchronization Ports**

- Internal Sync: [ 1/48/1 ] [▼]
- External Sync: [ 1/47/1, 1/56/1 ] [▼]

**VLAN Configuration**

- Change VLAN configuration [?]
- Orchestrators Base VLAN: [ 3950 ] [▲] [▼]
- Security Appliances Inter Site Base VLAN: [ 3600 ] [▲] [▼]

Navigation buttons: < Back, Next >, Cancel

Maestro First Time Wizard on MHO allows Environment, Member, Sync-port and dual-site VLAN settings to be configured.

# R82: Simpler Security Group Creation

Topology

Apply Refresh Help  Show selection in map

Unassigned Gateways

Name	Site	Serial	Downlinks
Check Point 6200B	1	2108BA1129	Port 1/42/1
Check Point 6200P	2	2252BA0316	Port 1/51/2, Port

Security Group 2 configuration

Security Group settings Auto Scaling settings

Management interface settings

IPv4 address:

Subnet mask:

Default Gateway:

Create MGMT interface as bond:

Bond Mode:  active-backup  xor  8023AD

First Time Wizard settings

Set FTW configuration

Hostname:

Admin Password:

Confirm Admin Password:

SIC Password:

Confirm SIC Password:

Install as VSX:

OK Cancel

In R82 you can create the Management bond during the Security Group creation wizard

# R82: New MHO View

- New MHO view shows:
  - Port connectivity / diagnostics / status / usage

Topology

Apply Refresh Help  Show selection in map

Unassigned Gateways				Topology				
Name	Site	Serial	Downlinks	Name	ID	Hostname	IP address	Default Gateway
Check Point 6200B	1	2108BA1129	Port 1/42/1	Security Groups				
Check Point 6200P	2	2252BA0316	Port 1/51/2, Port 1/51/4	Security Group 1		idan-sg1	172.23.96.131/24	172.23.96.4
				Gateways				
				Site 1				
				Check Point 6200P	1			
				Site 2				
				Check Point 6200P	1			
				Interfaces				
				Port 1/1/1 (eth1-Mgmt1)				
				Port 1/13/1 (eth1-13)				
				Port 1/15/1 (eth1-15)				
				Port 2/13/1 (eth2-13)				
				Port 2/15/1 (eth2-15)				
				Port 2/17/1 (eth2-17)				

Orchestrator 2\_1 (Local)

Orchestrator 2\_1 (Local) port status grid showing various port states and a context menu. The grid displays port numbers 1 through 56. A context menu is open over port 15, showing options: Edit Port, Blink LED, and Diagnostics. A legend at the bottom indicates port types: Mgmt (orange), Uplink (pink), Downlink (cyan), Sync (blue), Unplugged Port (grey), Inactive (red), Link State Up (green), and Link State Down (red).

# R82: Build Maestro via API

- ▼ Maestro
  - ▼ Gateways
    - show-maestro-gateway
    - show-maestro-gateways
    - set-maestro-gateway
  - ▼ Ports
    - show-maestro-port
    - show-maestro-ports
    - set-maestro-port
  - ▼ Security Groups
    - show-maestro-security-group
    - show-maestro-security-groups
    - set-maestro-security-group
    - add-maestro-security-group
    - apply-maestro-security-groups-changes
    - delete-maestro-security-group
    - discard-maestro-security-groups-changes
  - ▼ Sites
    - show-maestro-site
    - show-maestro-sites
    - set-maestro-site

Command

```
mgmt_cli add maestro-security-group interfaces.id "1/1/1" gateways.1.id "2108BA1058" gateways.1.description "GW 2108BA1058 Description" sites.1.id 1 sites.1.description "site1 description in new S  
G context" ftw-configuration.hostname "My_Host_Name" ftw-configuration.is-vsx True ftw-configuration.one-time-password "otp_pass" ftw-configuration.admin-password "admin_pass" mgmt-connectivity.ip  
v4-address "1.1.1.1" mgmt-connectivity.ipv4-mask-length 24 mgmt-connectivity.default-gateway "1.1.1.4" description "New Security Group Description" --context gaia_api --version 1.8 --format json  
* "--format json" is optional. By default the output is presented in plain text.
```

R82 adds API with the ability to manipulate:

- Maestro **Gateways**
- Maestro **Ports**
- Maestro **Security Groups**
- Maestro **Sites**

# Maestro Training Resources

- Official CCME Certification and Training  
<https://training-certifications.checkpoint.com/#/courses/Check%20Point%20Certified%20Maestro%20Expert>
- Jump Start Series in CheckMates  
<https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Check-Point-Jump-Start-Course-Maestro/ba-p/153352?cat=10>
- Maestro Masters in CheckMates  
<https://community.checkpoint.com/t5/Maestro/bd-p/maestro>
- <https://www.youtube.com/c/checkpoint>
- <https://www.brighttalk.com/channel/16731/>



**Thank You!**

YOU DESERVE THE BEST SECURITY