SOLUÇÃO MAESTRO

SEGURANÇA EM HIPERESCALABILIDADE

Ricardo Bacelar | Security Engineer

José Irapuan | Security Engineer

SEGURANÇA COMPLETA

CloudGuard — SECURE THE CLOUD

- **CloudGuard Posture Management** — Posture Management & Visibility
- **CloudGuard Intelligence** — Network Traffic Analysis
- **CloudGuard Workload** — Runtime Workload Protection
- **CloudGuard Network** — Cloud Access Control & Prevention
- **CloudGuard AppSec** — Web & API Protection

Multi & Hybrid Cloud

SD-WAN

Quantum — SECURE THE NETWORK

- **Quantum Security Gateway** — Enterprise Firewall
- **Quantum Maestro** — Hyperscale
- **Quantum Lightspeed** — Hyper-Fast Firewall
- **Quantum R81** — Secure-OS
- **Quantum SMB** — SMB-Suite
- **Quantum Rugged** — ICS Security
- **Quantum IoT Protect** — IoT Security
- **Quantum Smart-1 Cloud** — Security Management

• Access Control	• Wide Range of Firewalls	• Unified Policy
• Advanced Threat Prevention	• Up to 3 Tbps Throughput	• Autonomous Security
• Data Protection	• 1, 10, 25, 40, 100 GbE ports	• Event Management
	• Wi-Fi, DSL, 3G/4G/LTE	• Compliance

Horizon — UNIFIED MANAGEMENT & SECURITY OPERATIONS

- **Horizon MDR** — Managed Prevention & Response
- **Horizon XDR** — Extended Prevention & Response
- **Horizon Events** — Unified Events
- **INFINITY PORTAL** — Management & Unified Visibility
- **THREATCLOUD** — Threat Intelligence

Harmony — SECURE USERS & ACCESS

SECURE ACCESS SERVICE EDGE (SASE)

Harmony Connect (SASE)

- Zero Trust Network Access (ZTNA)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Branch FWaaS

EMAIL & COLLABORATION

Harmony Email & Collaboration

- Account Takeover Protection
- Data Loss Prevention
- Threat Prevention
- Zero Phishing

ENDPOINT & MOBILE

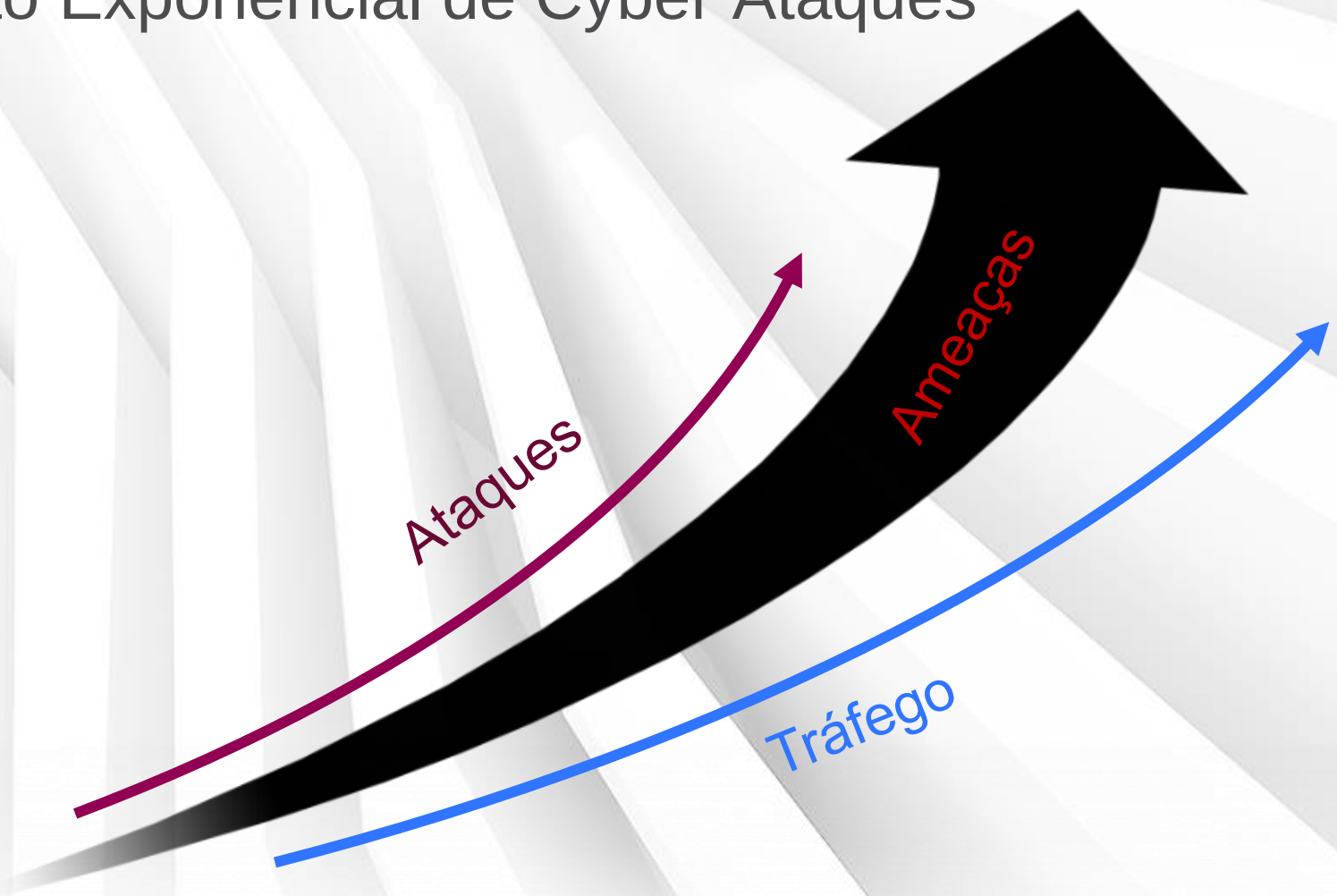
Harmony Endpoint	Harmony Browse	Harmony Mobile
• Threat Prevention	• Zero Day Browser Protection	• App Protection
• Anti-Ransomware	• Threat Prevention	• Network Protection
• Forensics	• Zero Phishing	• Device Protection
• Secure Media		
• Access Control		

©2021 Check Point Software Technologies Ltd.


Atualmente…
Tráfego Dobra
A cada 3 anos
Nossa rede cresce até
25%
Ano após ano

Onde nós Estamos?

Crescimento Exponencial de Cyber Ataques



E AS PLATAFORMAS DE SEGURANÇA???

©2020 Check Point Software Technologies Ltd.

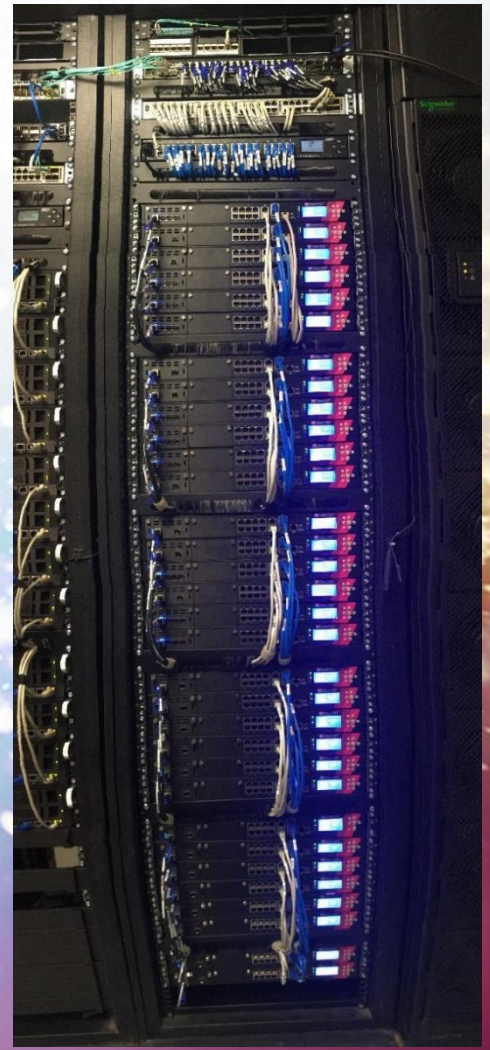
Plataformas Escaláveis Check Point

64000

44000

Novas Opções

Quantum Maestro



©2022 Check Point Software Technologies Ltd.

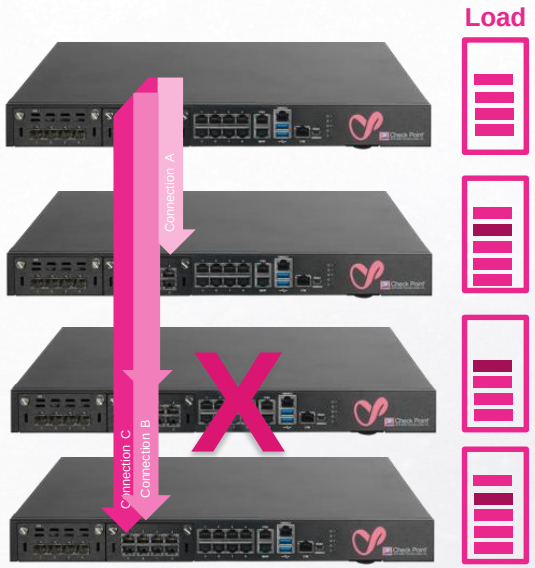
Cluster HiperEscalável - *"Chassisless"*

Conceito reinventado para Plataforma Escalável

Appliances **já conhecidos**

Agora é a hora de **Cloudificar** nossas **Redes e Datacenters**

Escalabilidade



Redundância

Load Balancing de tráfego

Resiliência

Sincronização de Software e Configuração

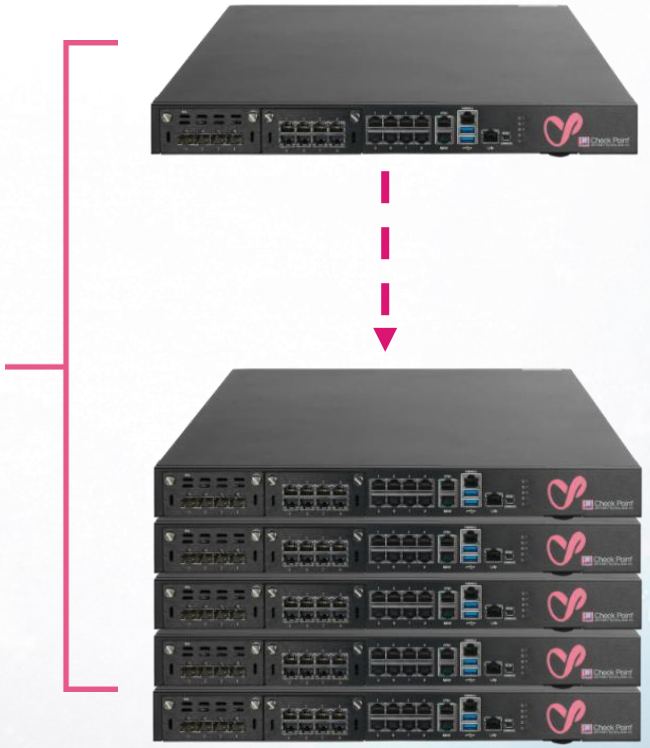
Eficiência de custo

©2022 Check Point Software Technologies Ltd.

Arquitetura Física - Entendendo em detalhes

Performance e Simplicidade

M A E S T R O
Orquestradores
HiperEscalabilidade



Q u a n t u m
Appliances

1.5 Tbps

Zero Touch Provisioning

Up to 52 appliances

Threat Prevention

©2022 Check Point Software Technologies Ltd.

Arquitetura Física **MAESTRO**

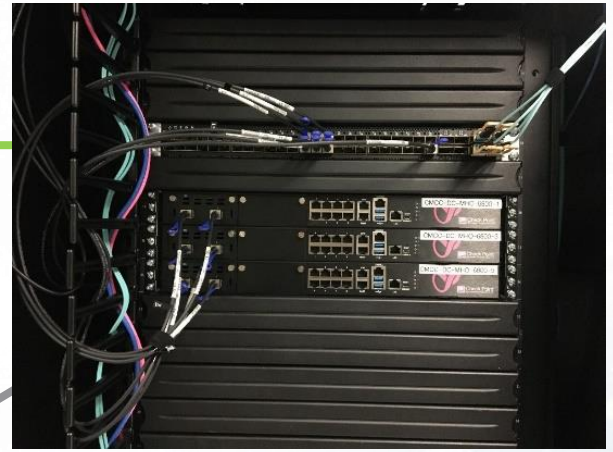
- **Camada de Orquestração**

- **Camada de Recursos Computacionais**

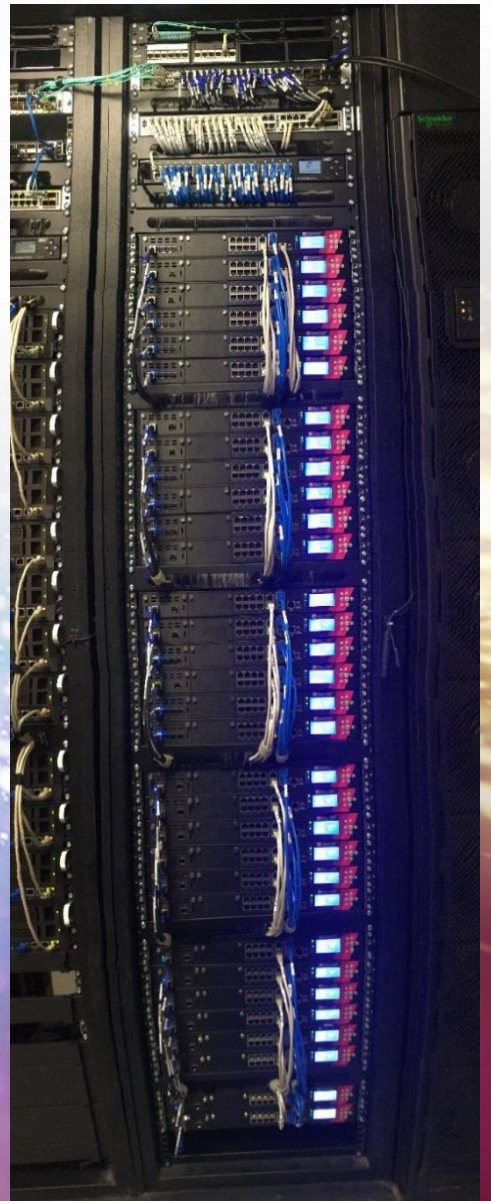
©2022 Check Point Software Technologies Ltd.

Arquitetura Física **MAESTRO**

- **Camada de Orquestração**



- **Camada de Recursos Computacionais**



©2022 Check Point Software Technologies Ltd.

Tecnologias **Smart** - Quantum Maestro

Mix and Match HW

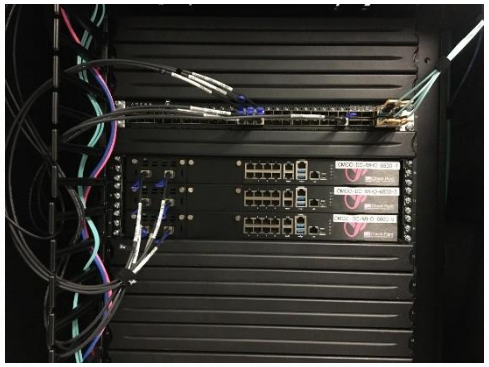


Image Auto-Cloning

```
admin@Gateway-Reference-ch02-01:~
[Global] Gateway-Reference-ch02-01 > set smo image auto-clone state on
1_01:
Image auto-clone state is on

1_02:
Image auto-clone state is on

1_03:
Image auto-clone state is on

2_01:
Image auto-clone state is on

2_02:
Image auto-clone state is on

2_03:
Image auto-clone state is on

[Global] Gateway-Reference-ch02-01 >
```

Global configuration

```
ggaudi_t13-ch01-01 > set interface eth1-12 ipv4-address 33.33.33.1 mask-length 24
1_01:
success

1_02:
success

1_03:
success

ggaudi_t13-ch01-01 >
```

Auto-discovery

```
[Expert@wal-orch1:0]# tldpctl
LLDP neighbors:
Interface:    dl30, via: LLDP, RID: 1, Time: 34 days, 17:30:26
  Chassis:
    ChassisID:    local SG2-ch01-02
    SysName:      SG2-ch01-02
    SysDescr:     #sid*1910BA1411#/sid*#name*Check Point 6500#/name*
    MgmtIP:       198.51.102.2
    Capability:   Bridge, off
    Capability:   Router, on
    Capability:   Wlan, off
  Port:
    PortID:       mac 00:1c:7f:02:00:fe
    PortDescr:    ethsBP1-01
     Port is aggregated. PortAggregID: 17
Interface:    dl33, via: LLDP, RID: 6, Time: 34 days, 17:30:24
  Chassis:
    ChassisID:    local SG2-ch01-01
    SysName:      SG2-ch01-01
    SysDescr:     #sid*1910BA1395#/sid*#name*Check Point 6500#/name*
    MgmtIP:       198.51.102.1
    Capability:   Bridge, off
    Capability:   Router, on
    Capability:   Wlan, off
  Port:
    PortID:       mac 00:1c:7f:01:00:fe
    PortDescr:    ethsBP1-01
     Port is aggregated. PortAggregID: 17
Interface:    dl43, via: LLDP, RID: 1, Time: 34 days, 17:30:24
  Chassis:
    ChassisID:    local SG2-ch01-02
    SysName:      SG2-ch01-02
    SysDescr:     #sid*1910BA1411#/sid*#name*Check Point 6500#/name*
    MgmtIP:       198.51.102.2
    Capability:   Bridge, off
    Capability:   Router, on
    Capability:   Wlan, off
  Port:
    PortID:       mac 00:1c:7f:02:00:fe
    PortDescr:    ethsBP1-03
     Port is aggregated. PortAggregID: 17
```

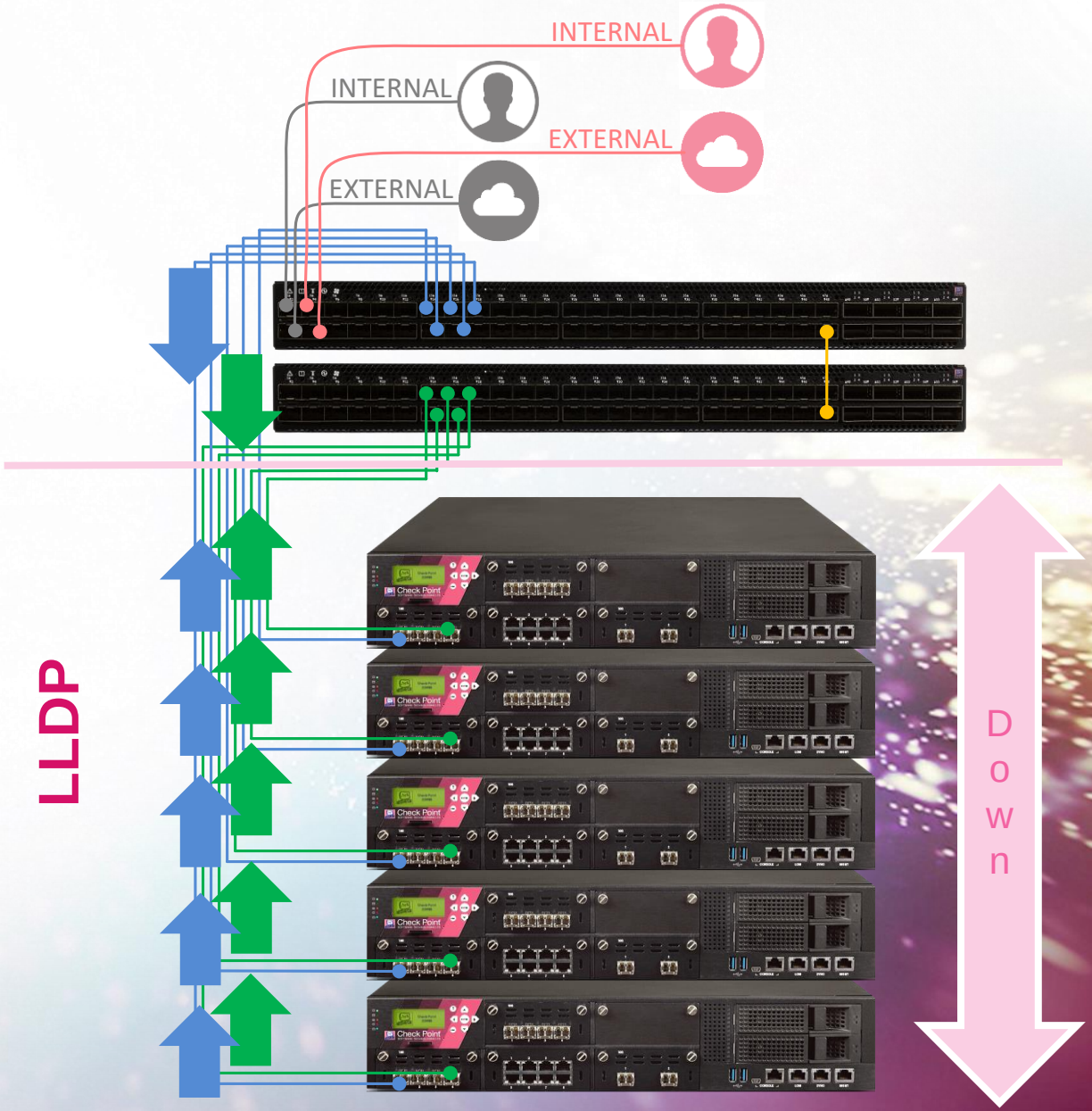
Auto-diagnostics

```
[Expert@SG1-ch01-01:0]# asg diag list
-------------------------------------------------------
| ID | Title                | Command
-------------------------------------------------------
| System Components
-------------------------------------------------------
|  1 | System Health        | asg stat -v
|  2 | Resources            | asg resource
|  3 | Software Provision   | asg_provision
|  4 | Media Details        | transceiver_verifier -v
|  5 | SSD Health           | asg resource --ssd
|  6 | Firmware Verifier    | firmware_verifier -v
-------------------------------------------------------
| Policy and Configuration
-------------------------------------------------------
|  7 | Distribution Mode    | distutil verify -v
|  8 | DXL Balance          | dxl stat
```


©2022 Check Point Software Technologies Ltd.

Auto-Discovery

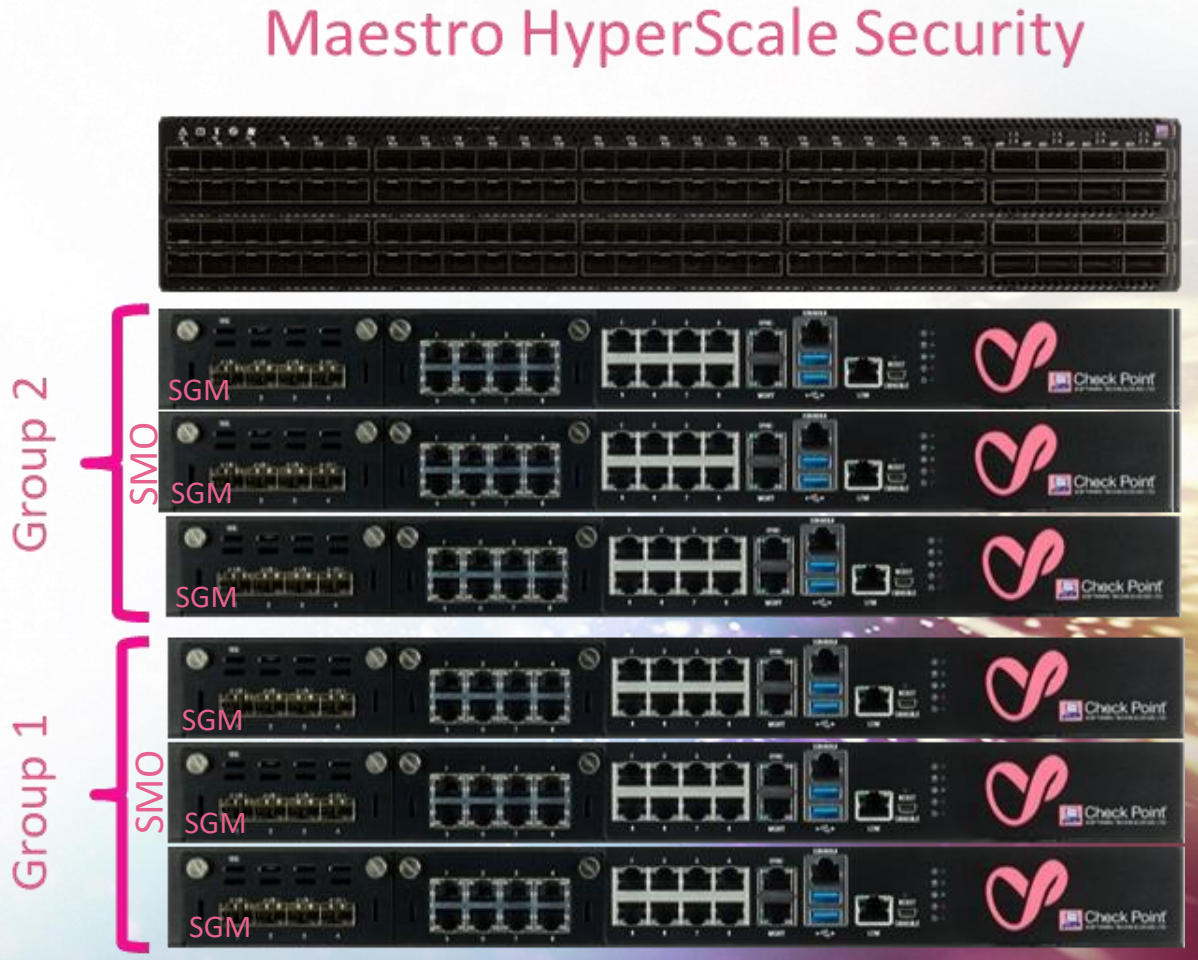
- *Appliances* se comunicam com o Orquestrador utilizando **Link Layer Discover Protocol (LLDP)**
- *Appliances* recebem a configuração do Orquestrador e SMO
- Tráfego passa pelo SGM logo após a configuração é aplicada



©2022 Check Point Software Technologies Ltd.

Grupos de Segurança - Security Groups (SG)

- Configurado através do Orquestrador
- Cada *Security Group* contém Appliances, portas de gerência e uplinks
- Até 8 Security Groups
- Até 28 appliances por SG
- Até 14 appliances por site
- Até 52 appliances por sistema



©2022 Check Point Software Technologies Ltd.

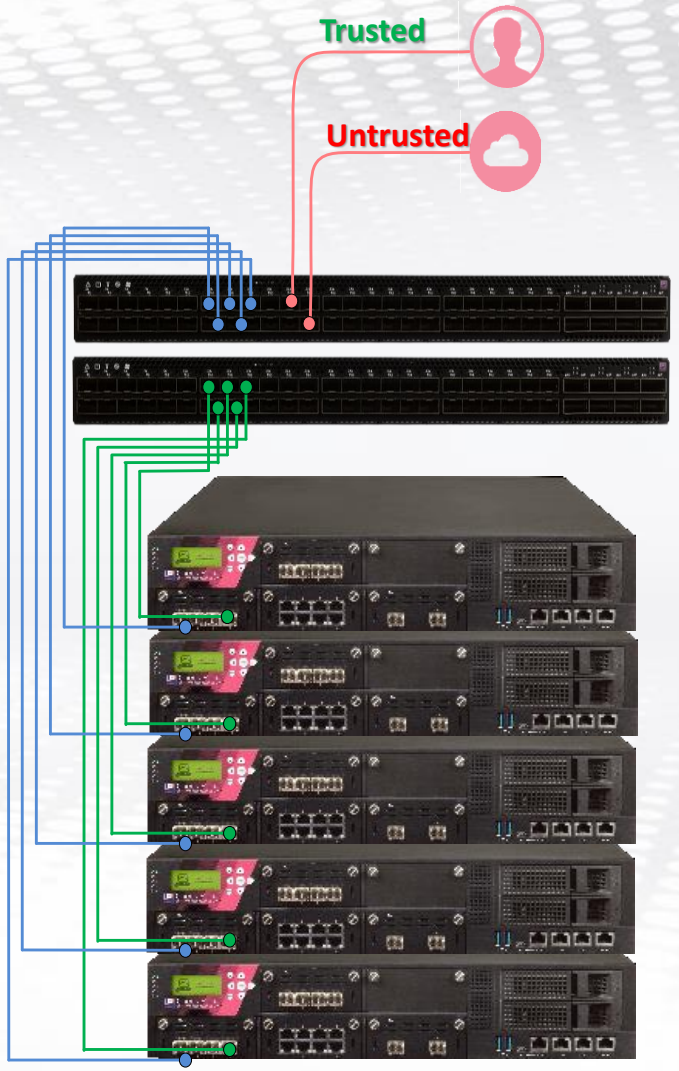
Redução de Complexidade

UPLINKS

Conexões para zonas Confiáveis e Não Confiáveis. Interfaces são **visíveis aos admins** no SmartDashboard, WebUI, CLISH, etc.

DOWNLINKS

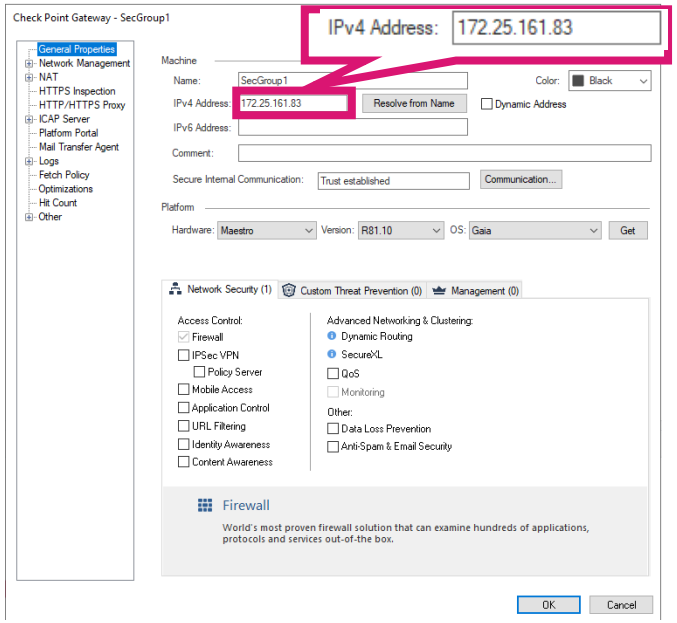
Camada de **Abstração** que forma o Sistema de Backplane **(Configuração não é requerida)**

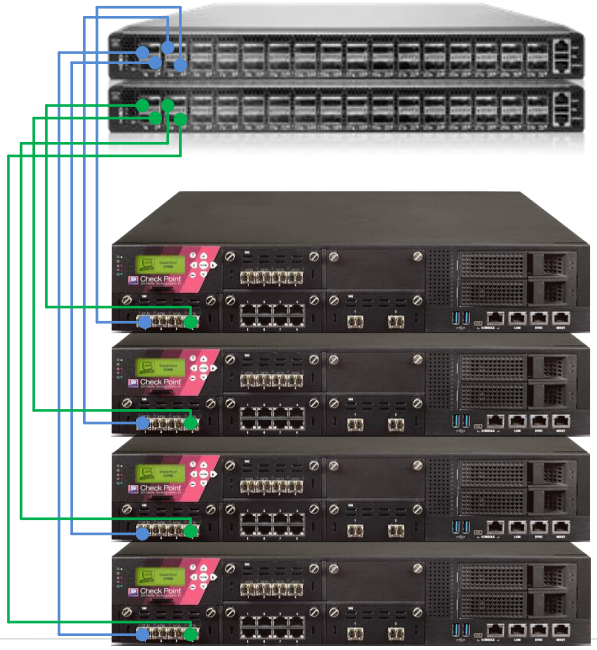


©2022 Check Point Software Technologies Ltd.

Single Management Object (SMO)

- **Único Objeto** para Security GW por Security Group na SmartConsole
- **Único** endereço IP para gerência
- **Clona** toda configuração entre os membros
- **Rápida** instalação de Política
- **Hierarquico** - Sistema
- **Cluster** - Abstração





©2022 Check Point Software Technologies Ltd.

Monitorando Maestro

SNMP

sk168878

Security Group

asg monitor

asg stat -v

g_all cphaprob stat

asg perf -v -p --delay 1

asg perf -v -k

cpview

```
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Chassis Mode                | Primary Up (1 2)                              |
| Up time                     | 80 days, 11:47:39 hours                       |
| SGMs                        | 2 / 2                                         |
| Version                     | R81 (Build Number 396)                        |
| FW Policy Date              | Standard                                      |
| AMW Policy Date             | N/A                                           |
-------------------------------------------------------------------------------
| SGM ID            Chassis 1                       Chassis 2                 |
|                   ACTIVE                          STANDBY                   |
-------------------------------------------------------------------------------
|  1                  ACTIVE                          ACTIVE                  |
-------------------------------------------------------------------------------
| Chassis HA mode:            Primary Up                                      |
-------------------------------------------------------------------------------
```

Orchestrator

orch_stat –a

Physical Port	Interface Name	Type	SG	QSFP Mode	Admin State	Link State	Transceiver
1/1/1	eth1-Mgmt1	Mgmt	1	10G	UP	DOWN	UNPLUGGED
1/2/1	eth1-Mgmt2	Mgmt	---	10G	DOWN	DOWN	UNPLUGGED
1/3/1	eth1-Mgmt3	Mgmt	---	10G	DOWN	DOWN	UNPLUGGED
1/4/1	eth1-Mgmt4	Mgmt	---	10G	DOWN	DOWN	UNPLUGGED
1/5/1	eth1-05	Uplink	1	10G	UP	UP	PLUGGED
1/6/1	eth1-06	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/7/1	eth1-07	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/8/1	eth1-08	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/9/1	eth1-09	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/10/1	eth1-10	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/11/1	eth1-11	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/12/1	eth1-12	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/13/1	eth1-13	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/14/1	eth1-14	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/15/1	eth1-15	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/16/1	eth1-16	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/17/1	eth1-17	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/18/1	eth1-18	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/19/1	eth1-19	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/20/1	eth1-20	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/21/1	eth1-21	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/22/1	eth1-22	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/23/1	eth1-23	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/24/1	eth1-24	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/25/1	eth1-25	Uplink	---	10G	DOWN	DOWN	UNPLUGGED
1/26/1	eth1-26	Uplink	1	10G	UP	UP	PLUGGED
1/27/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/28/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/29/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/30/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/31/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/32/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/33/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/34/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/35/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/36/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/37/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/38/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/39/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/40/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/41/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/42/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/43/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/44/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/45/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/46/1	---	Downlink	---	10G	UP	DOWN	UNPLUGGED
1/47/1	SYNC-EXT	Site Sync	---	10G	UP	UP	PLUGGED
1/48/1	SYNC-INT	SSM Sync	---	10G	UP	UP	PLUGGED
1/49/1	eth1-49	Uplink	1	100G	UP	UP	PLUGGED
1/50/1	eth1-51	Uplink	1	100G	UP	DOWN	UNPLUGGED
1/51/1	eth1-53	Uplink	---	100G	DOWN	DOWN	UNPLUGGED
1/52/1	eth1-55	Uplink	---	100G	DOWN	DOWN	UNPLUGGED
1/53/1	eth1-57	Uplink	---	100G	DOWN	DOWN	UNPLUGGED
1/54/1	eth1-59	Uplink	---	100G	DOWN	DOWN	UNPLUGGED
1/55/1	ethsBP1-01	Downlink	---	100G	UP	UP	PLUGGED
1/56/1	---	Downlink	---	100G	UP	DOWN	UNPLUGGED

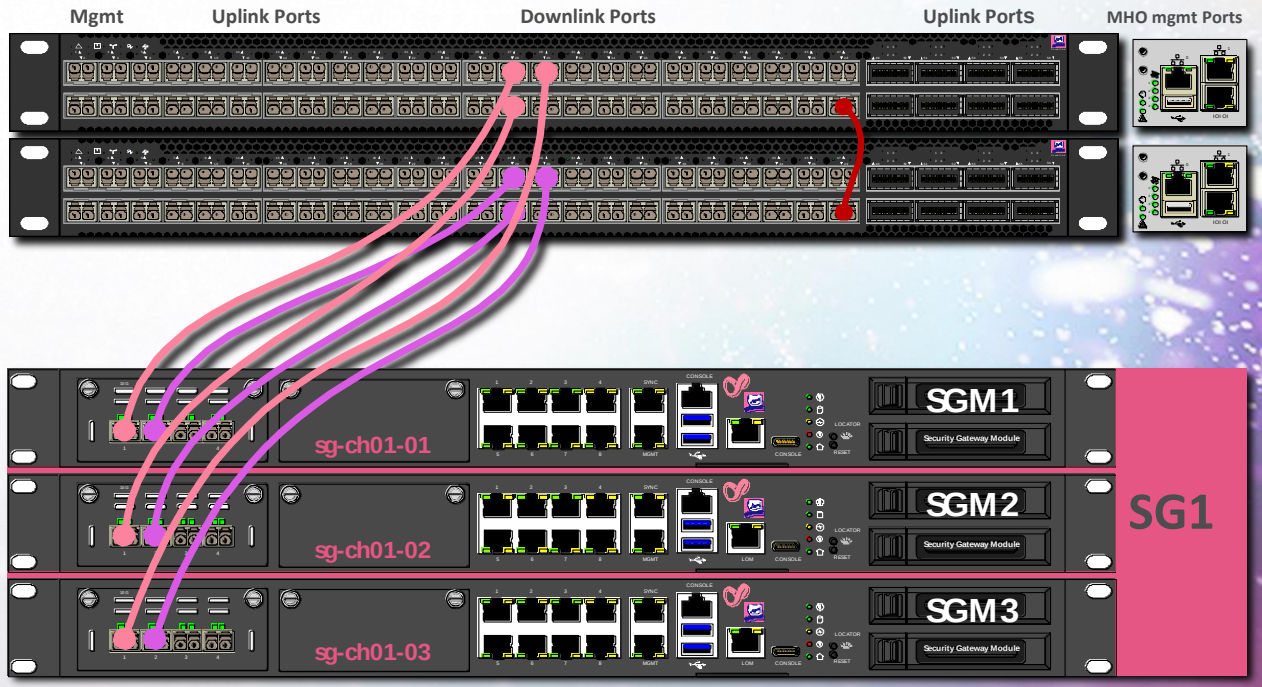
©2022 Check Point Software Technologies Ltd.

Arquitetura – Maestro Single Site

Uplinks conectados a switches de produção. **Sempre use bond!**

Downlinks são o backplane do Maestro: Cada SGM se conecta a ambos os MHOs.

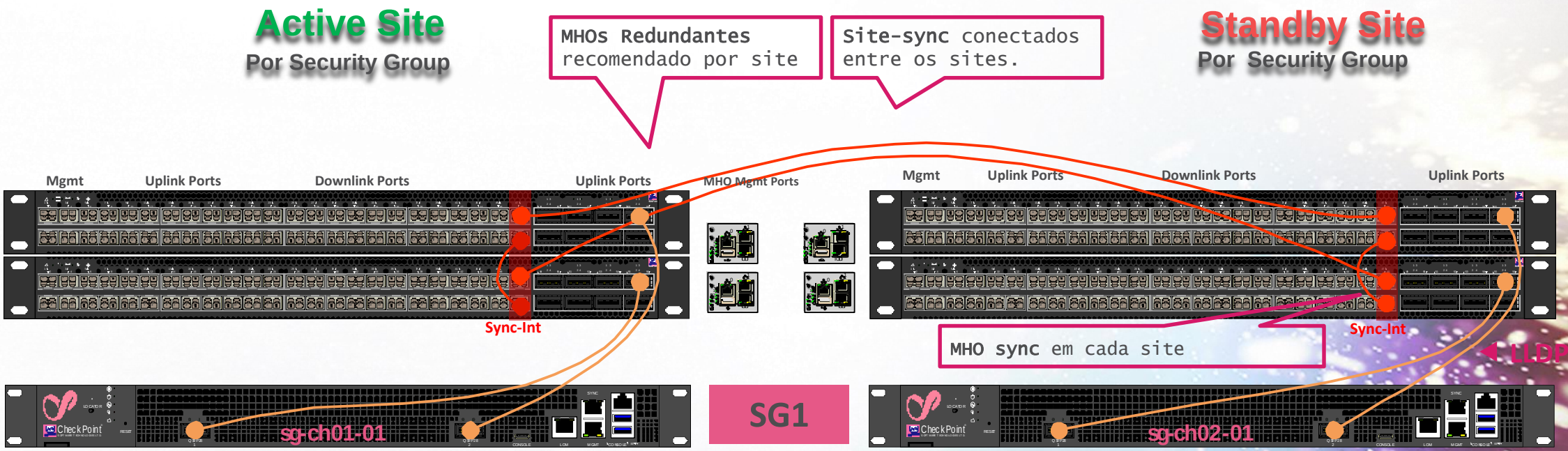
MHOs redundantes recomendado



©2022 Check Point Software Technologies Ltd.

Arquitetura – Maestro Dual Site

- **Dois sites** (max.) em modo active/standby. Uma única entidade na rede.



©2022 Check Point Software Technologies Ltd.

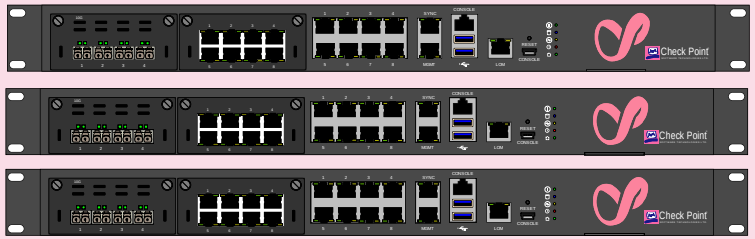
Data Centers Distribuídos – Security Groups

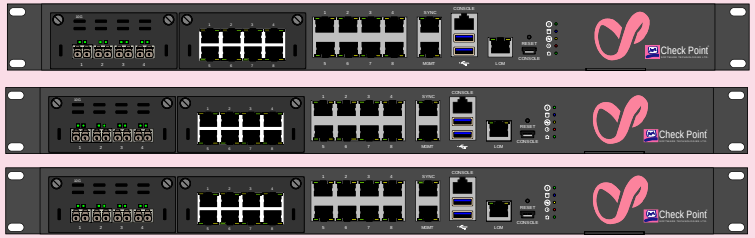
TOPOLOGIA DO MAESTRO

Site #1

Site #2

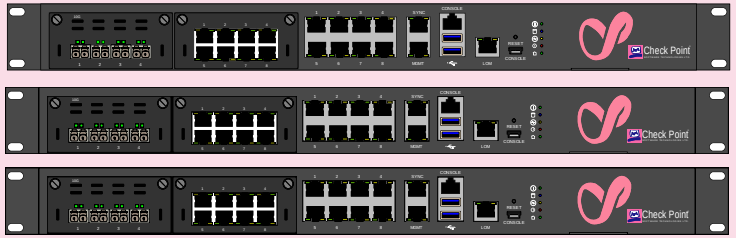
Security Group 1





Security Group 2

Security Group 3



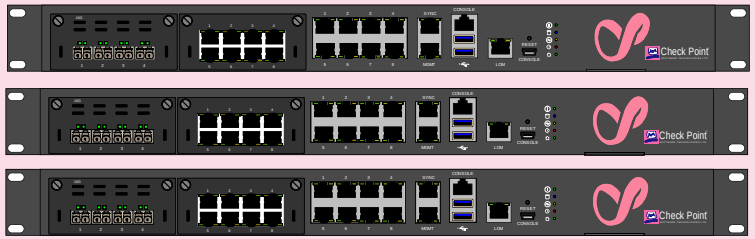
Data Centers Distribuídos – Security Groups

TOPOLOGIA DO MAESTRO

Site #1

Site #2

Security Group 1



HyperSync com Dual site – Security Group

Site **Ativo**

SGM-1

SGM-2

SGM-3

Site **Standby**

A **1.1.1.1:1234 -> 2.2.2.1:80**

B **1.1.1.1:1234 -> 2.2.2.1:80**

B 1.1.1.10:2211 -> 2.2.2.20:22

A 1.1.1.10:2211 -> 2.2.2.20:22

A **3.5.6.3:4578 -> 2.2.2.1:80**

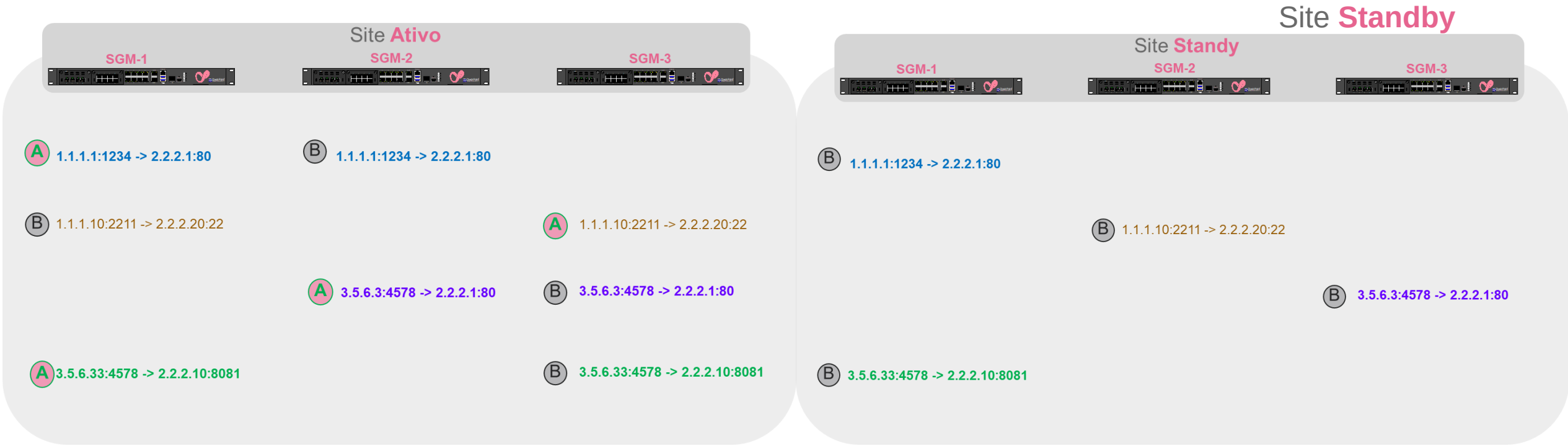
B **3.5.6.3:4578 -> 2.2.2.1:80**

A **3.5.6.33:4578 -> 2.2.2.10:8081**

B **3.5.6.33:4578 -> 2.2.2.10:8081**

©2022 Check Point Software Technologies Ltd.

HyperSync com Dual site – Security Group

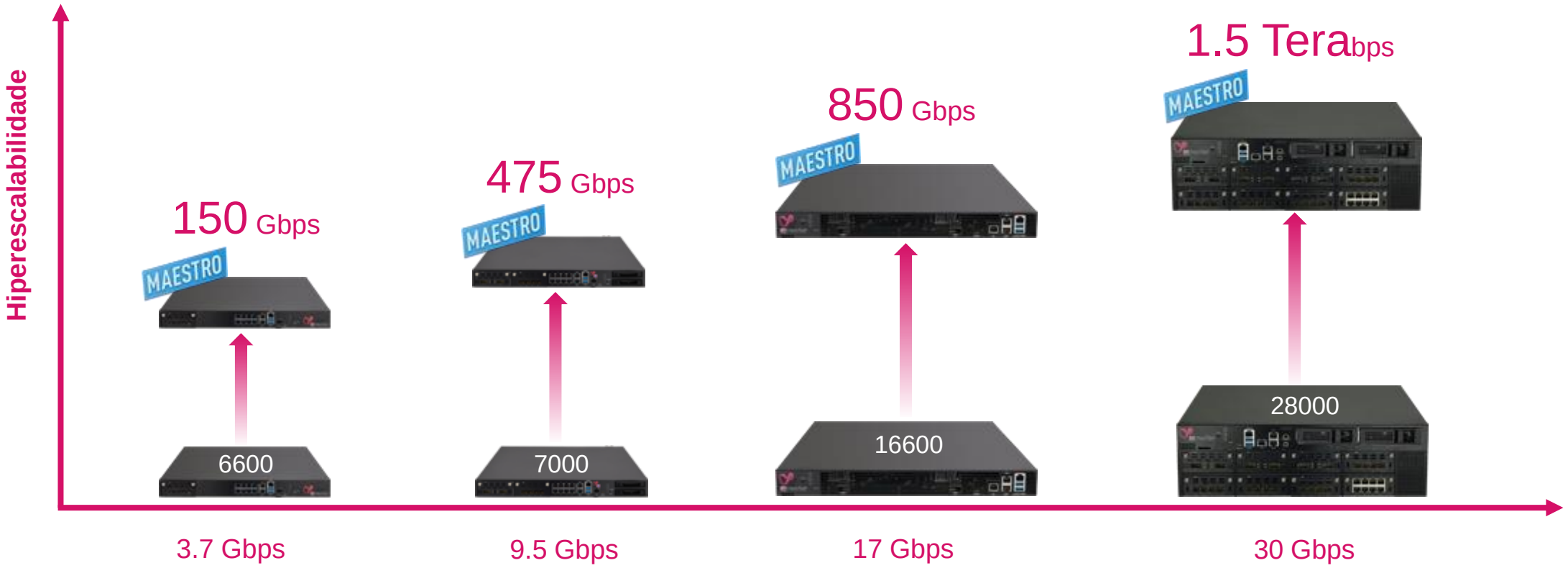


Security Group

©2022 Check Point Software Technologies Ltd.

Um salto para a Hiperescalabilidade

SGM (Security Gateway Module)



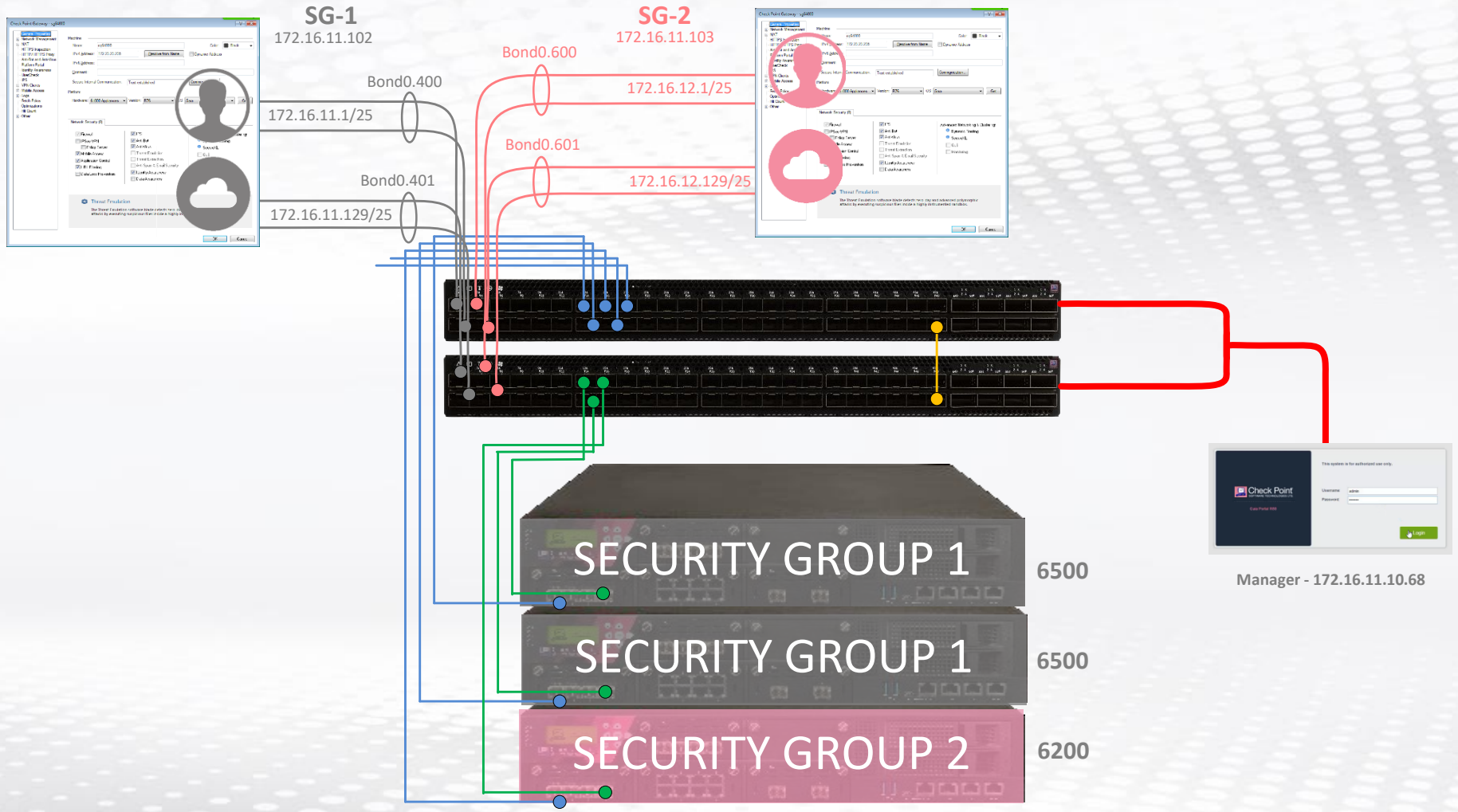
©2020 Check Point Software Technologies Ltd.

Quantum
Maestro

DEMO

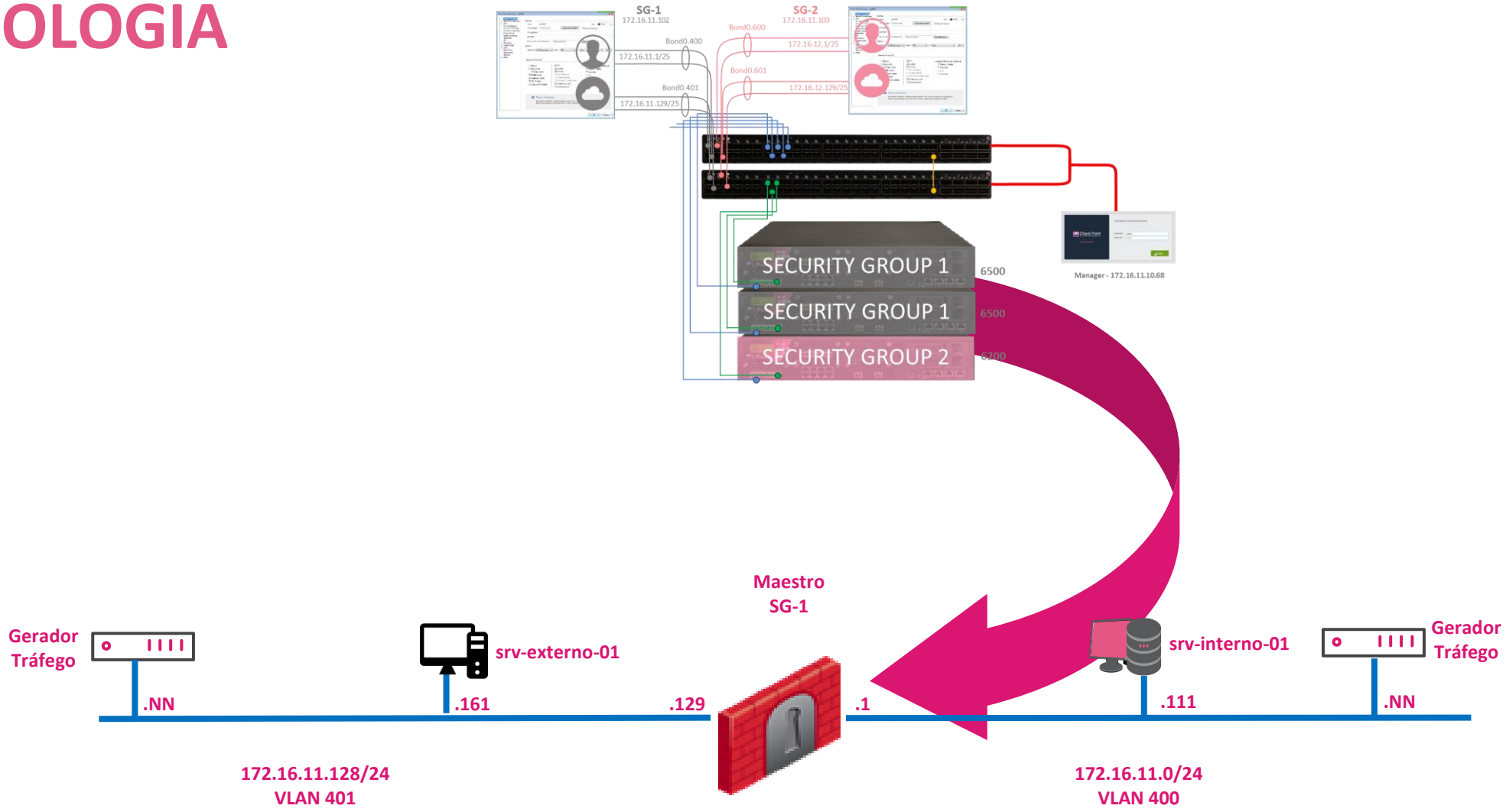
[Protected] Distribution or modification is subject to approval ©2022 Check Point Software Technologies Ltd.

TOPOLOGIA



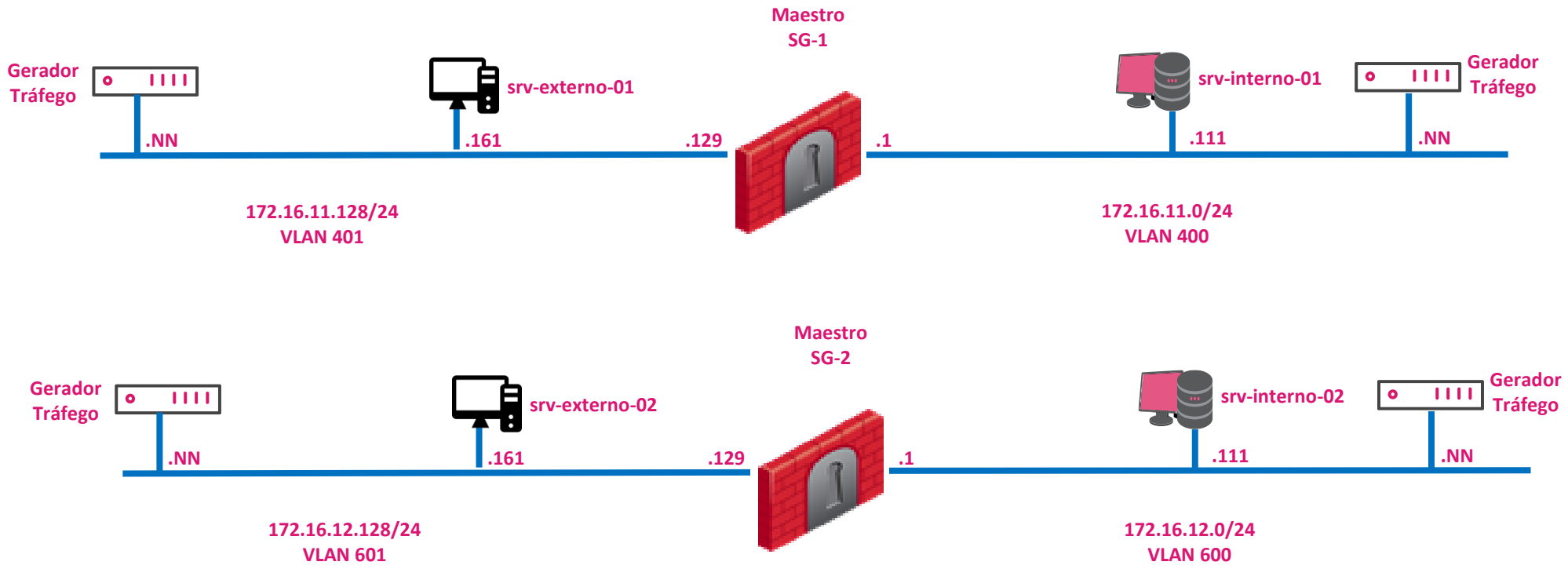
©2022 Check Point Software Technologies Ltd.

TOPOLOGIA



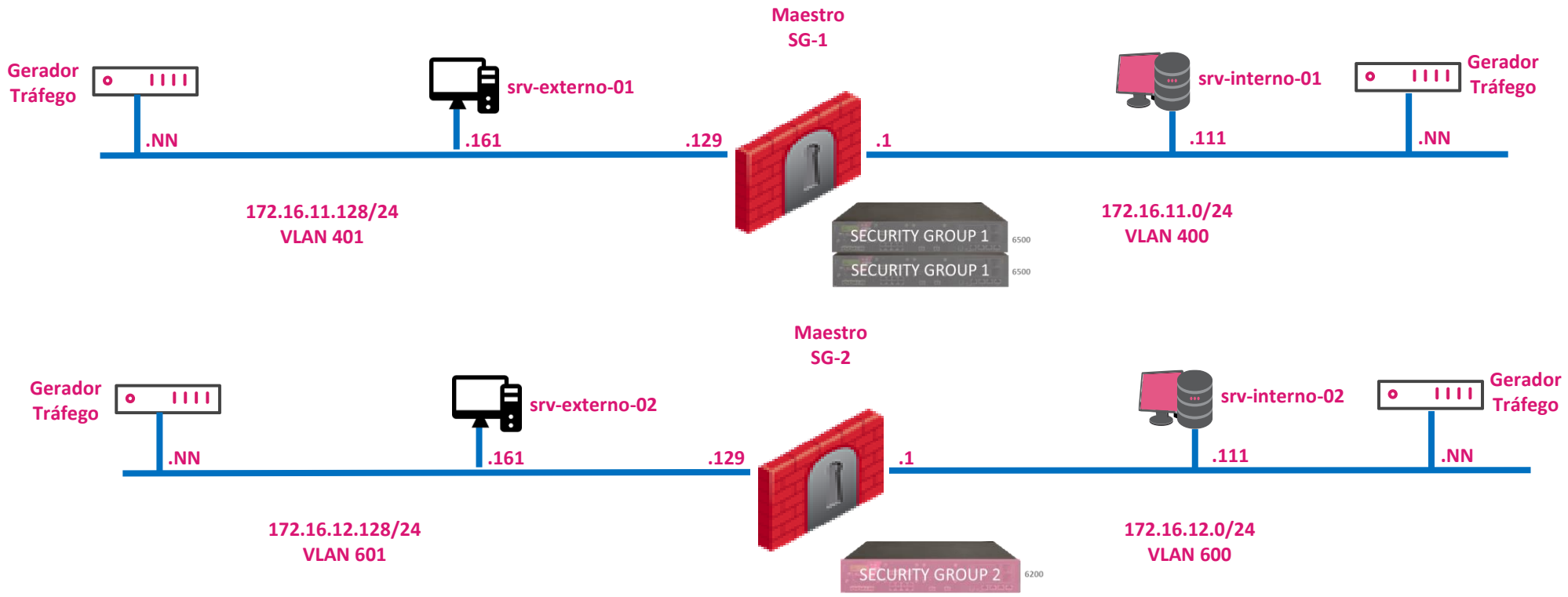
©2022 Check Point Software Technologies Ltd.

TOPOLOGIA



©2022 Check Point Software Technologies Ltd.

TOPOLOGIA



©2022 Check Point Software Technologies Ltd.

Políticas Distintas para Departamentos na Empresa

Escritórios

TRÁFEGO DE CLOUD

Consolidação de Gateways

Gerencia múltiplos gateways lógicos baseado em um SISTEMA ÚNICO para MÁXIMA EFICIÊNCIA

©2022 Check Point Software Technologies Ltd.

Políticas Distintas para Departamentos na Empresa

Alavanca o uso do
RESTful API do Orquestrador

ESCRITÓRIOS

AUTO-SCALING

TRÁFEGO DE CLOUD

Auto-Escalável

Aloca Dinamicamente recursos entre
Múltiplos grupos de Segurança em tempo real

©2022 Check Point Software Technologies Ltd.

CHECK POINT™

Quantum
Maestro

Free Online Training

https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Check-Point-Jump-Start-Course-Maestro/ba-p/153352?cat=10

YOU DESERVE THE BEST SECURITY

OBRIGADO

YOU DESERVE THE BEST SECURITY