CHECK POINT™

SECURITY AT HYPERSCALE

Yaron Weiler

Head of Product Management Security Platforms

Anatoly Masover

Scalable Platforms Expert

YOU DESERVE THE BEST SECURITY

Agenda

- **Maestro roadmap**
  - **Short term R81.20**
  - **Long term R81.30**

R81.20 / R81.30

Code Unification for Scalable Platforms into Maintrain

R81.20 main Maestro features

Fast Policy
reduce the policy installation from >10 min to seconds

MDPS
Data plane separation

Dynamic balancing for Maestro
Balancing cores utilization in SP

Fast Policy
reduce the policy installation from >10 min to seconds

Fast Forwarding
accelerate trusted traffic upon match of policy rule at the mho level

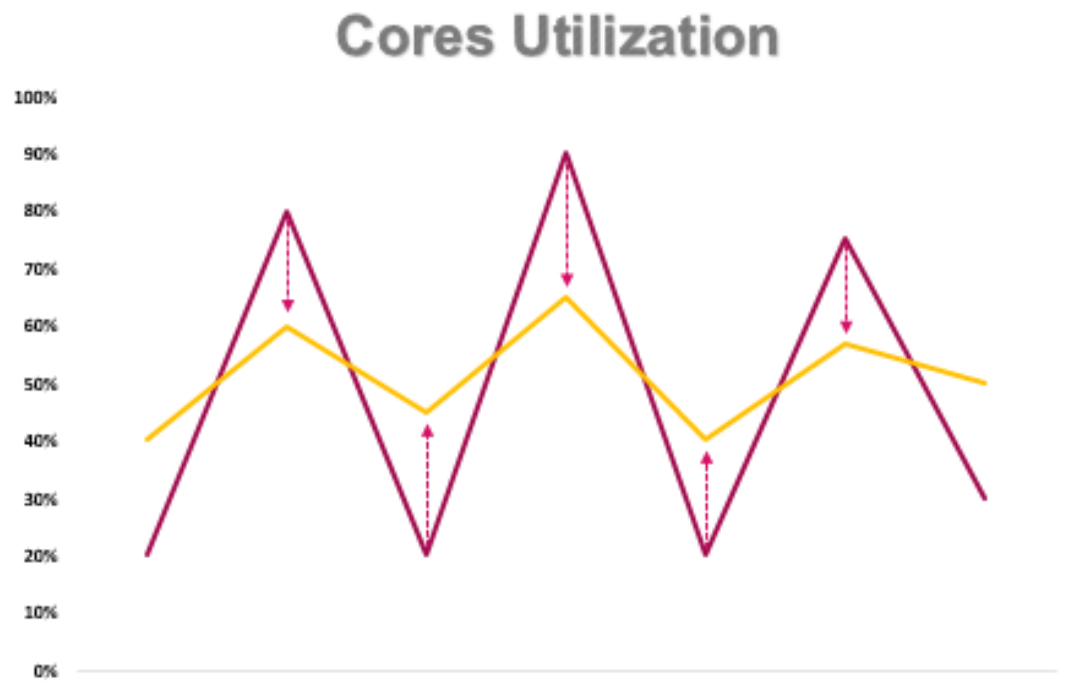
Connection upgrade / MVC
Zero downtime of the upgrade

Auto scale
Shifting GWs between SGs based on utilization

Dynamic balancing for Maestro

Dynamic Balancing overview - purpose

- Improve performance
  - Cores utilization
  - Avoid traffic bottle-necks



SP Adaptation design

- Every SGM calculate his own Dynamic Balancing, based on it’s traffic
- Enable/disable is per SG, can’t disable/enable Dynamic Balancing on specific members
- All other commands- can be executed on specific members if specified and on all member by default.

SP Adaptation design- dual site

- Active site:
  - All members will start Dynamic Balancing from default
  - Only SMO is syncing his fw/snd split to the sync table
  - On SMO failover– the new SMO will override the previous state

- Standby site:
  - Pull the SMO (of active site) fw/SND split and start the Dynamic Balancing from that state (to make failover softer)

SP Adaptation design- gclish commands

- Show dynamic-balancing state
- Set dynamic-balancing state { disable | enable | stop | start }
- Show / Set <CMD> member_ids <IDS_LIST>
  - Will perform the command on the specified members
  - Disable/enable is not allowed with member_ids option

MVC

Multi-Version Cluster (Connectivity Upgrade)

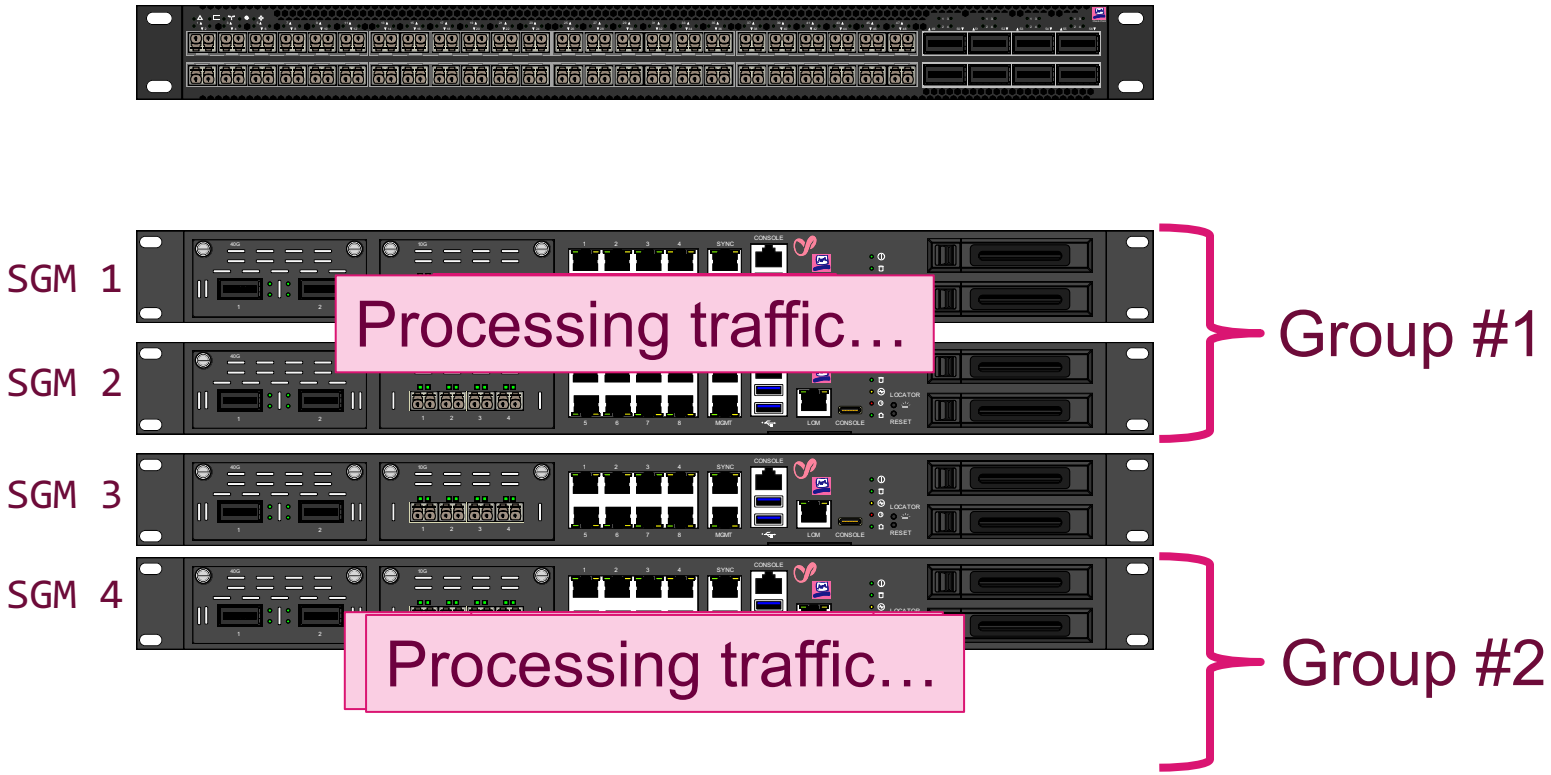
Motivation for MVC

- MVC allows to synchronize connections between Cluster Members with different versions installed
- MVC helps to upgrade to a newer version without connectivity loss
- MVC allows to test the new version on some of the Cluster Members before upgrading the rest of the Cluster Members

SP Upgrade without MVC (R81.10)

- Cluster members split into 2 groups.
- While 1st group is upgraded 2nd group processes the traffic
- Sync is disabled between 2 groups
- Iterator is not running during upgrade.
- After 1st group is upgraded failover occurs which leads to outage as connections were not synced.

SP Upgrade without MVC



SP Upgrade with MVC (R81.20)

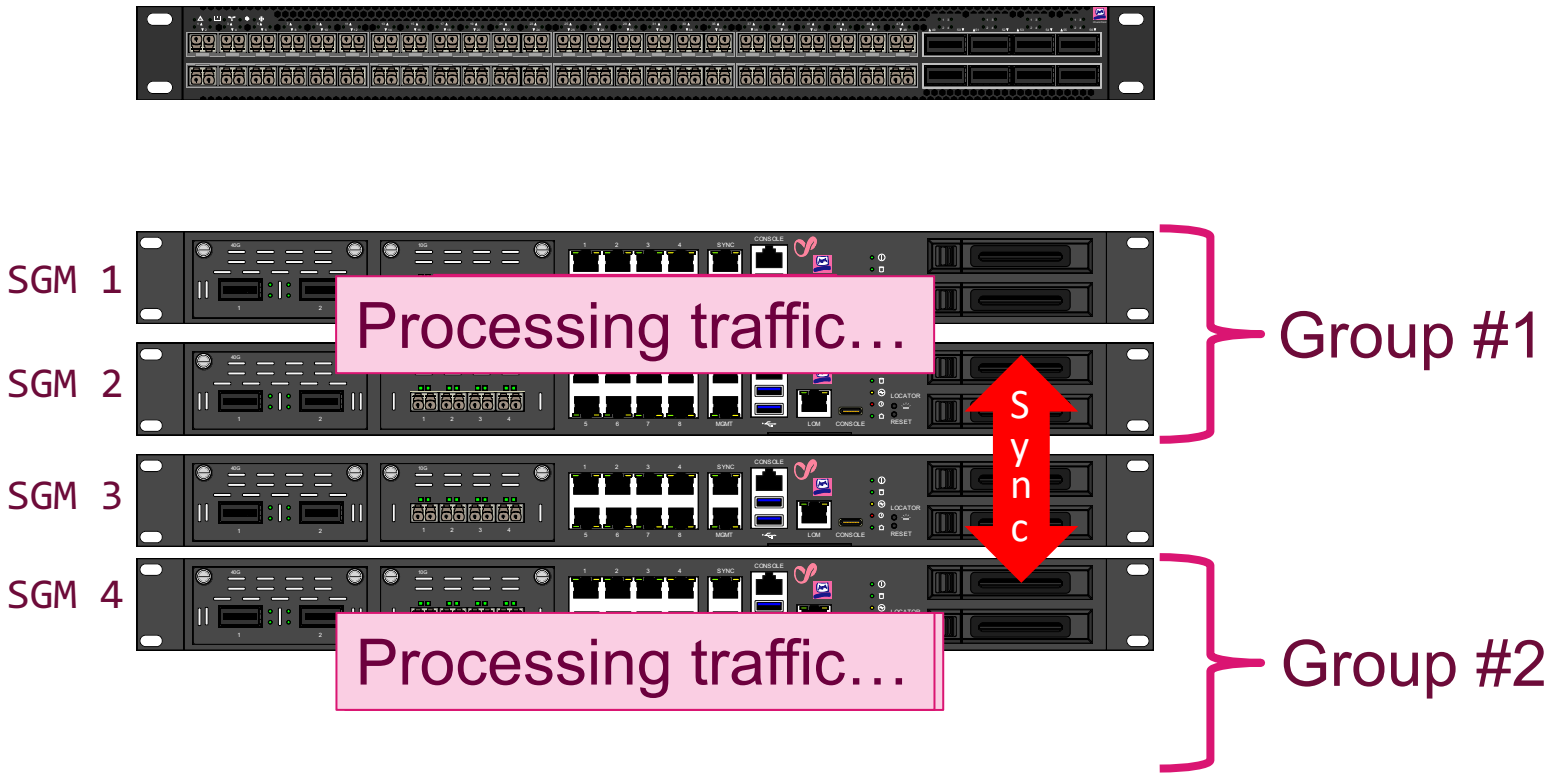
R81.20 will provide MVC (connectivity upgrade) which will allow keeping existing connections and gradually upgrade the Maestro system:

- Can be upgraded member by member
- 2 groups or more – upgrade of group by group

*All while keeping opened connections synched between the different members (versions)

SP Upgrade with MVC

- Cluster members split into 2 groups
- While 1st group is upgraded 2nd group processes the traffic
- Sync IS ENABLED between 2 groups
- Iterator IS RUNNING during upgrade
- After 1st group is upgraded we make all members ACTIVE
- All connections are synced and only then we upgrade 2nd group
- No outage



SP Upgrade with MVC (roadmap)

- Next phase of upgrade would be to automate this process thru CDT
- The current plan is to automatically upgrade:
    1. The whole group (will require downtime)
    2. Using 2 groups – upgrade at 2 phases group by group

MVC design in few words

- MVC is based on CU feature.
- MVC is enabled only on newly upgraded members.
- When enabled MVC allows newly upgraded members:
  - To translate CCPs (opcodes, protocol versions)
  - To translate sync data (connection records)

Troubleshooting

- MVC cluster will act similarly to a regular cluster, therefore, the troubleshooting should be similar to regular cluster.

- If the failover will cause unpredicted outage then we will need to debug MVC feature itself:
  - Relevant log files: var/log/messages, fwk.elg.
  - Debug: g_fw ctl zdebug –m cluster + cu ccp conf stat
  - Check that connections are synchronized: g_fw tab -t connections –s
  - In case of VPN check that tunnels are synchronized: vpn tu

FAST FORWARDING

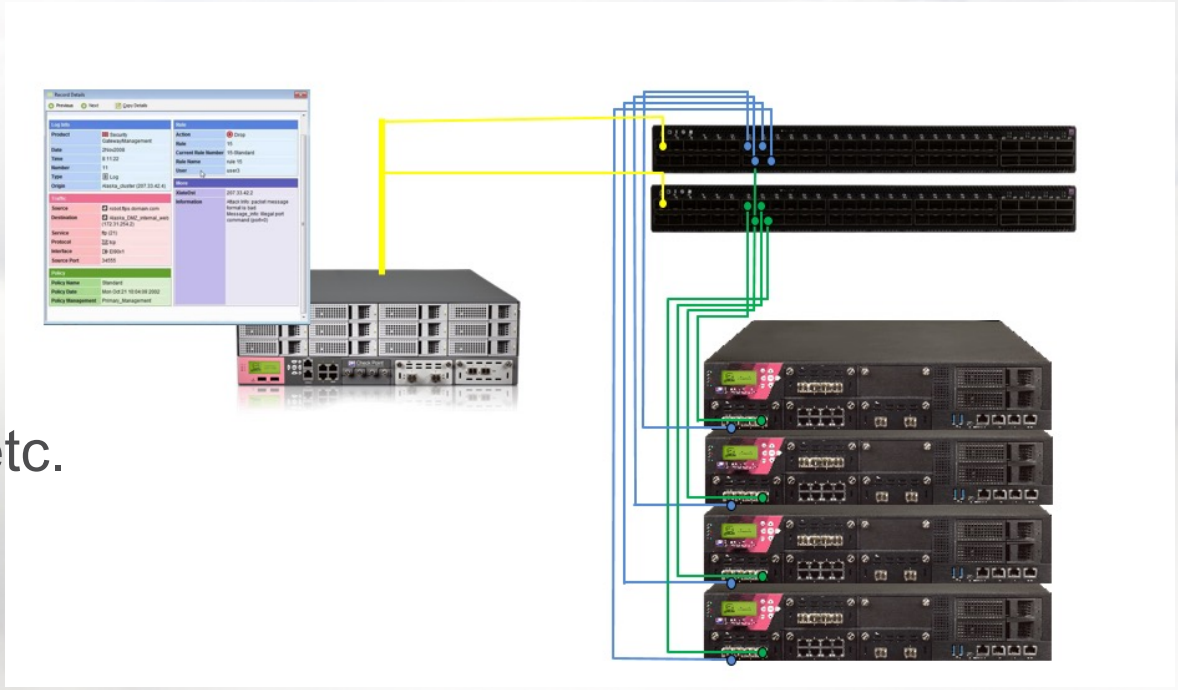
Overview

- Significantly improving throughput and latency of chosen trusted connections

- Achieved by allowing the enforcement of policy rules on the orchestrator hardware

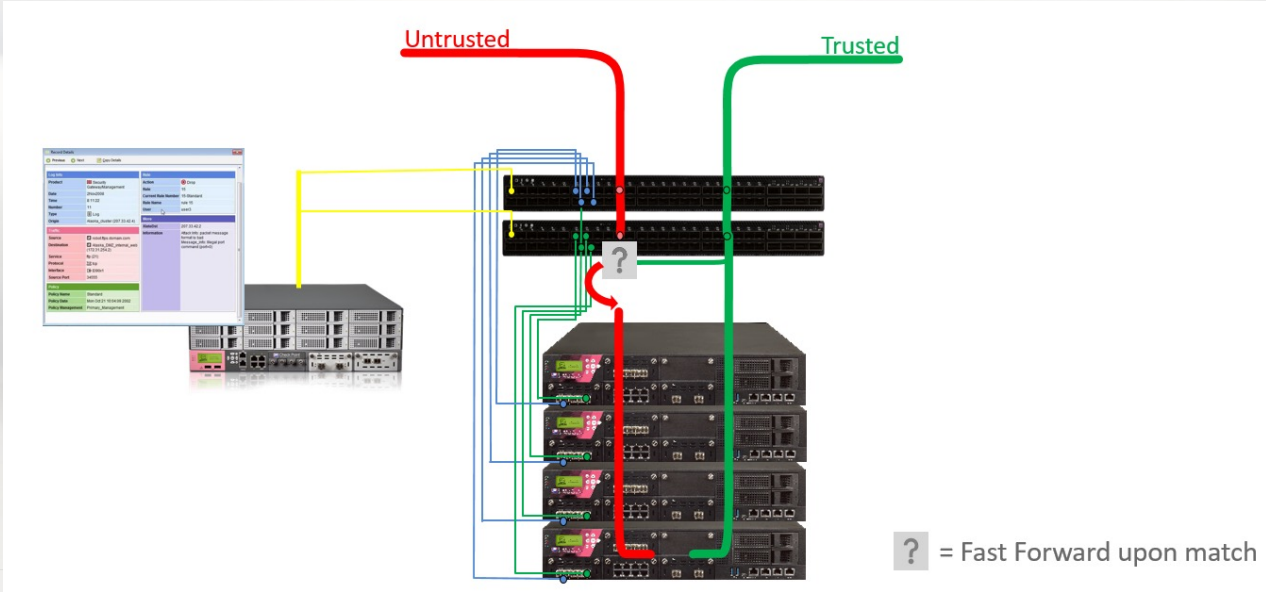
Solution Flow - Policy

- Admin defines security policy via SmartConsole or API
- Selected rules which were marked for acceleration (currently by rule name):
  - Will get translated into stateless Access Lists and communicated to MHO via REST API
  - Access Lists will be applied on the MHOs
- Routing Information
  - Routing info is offloaded to the MHOs
  - This in order to fully handle L3 forwarding
  - We offload Interfaces, neighbors, routes etc.



Solution Flow - Enforcement

- Packet arriving at uplink port will first get checked against fast-forward policy rules' attributes.
  - Accept action: will be routed via hardware outside
  - Drop action: will get dropped at hardware level
- In case of no match, it will continue to the Security Group for regular enforcement

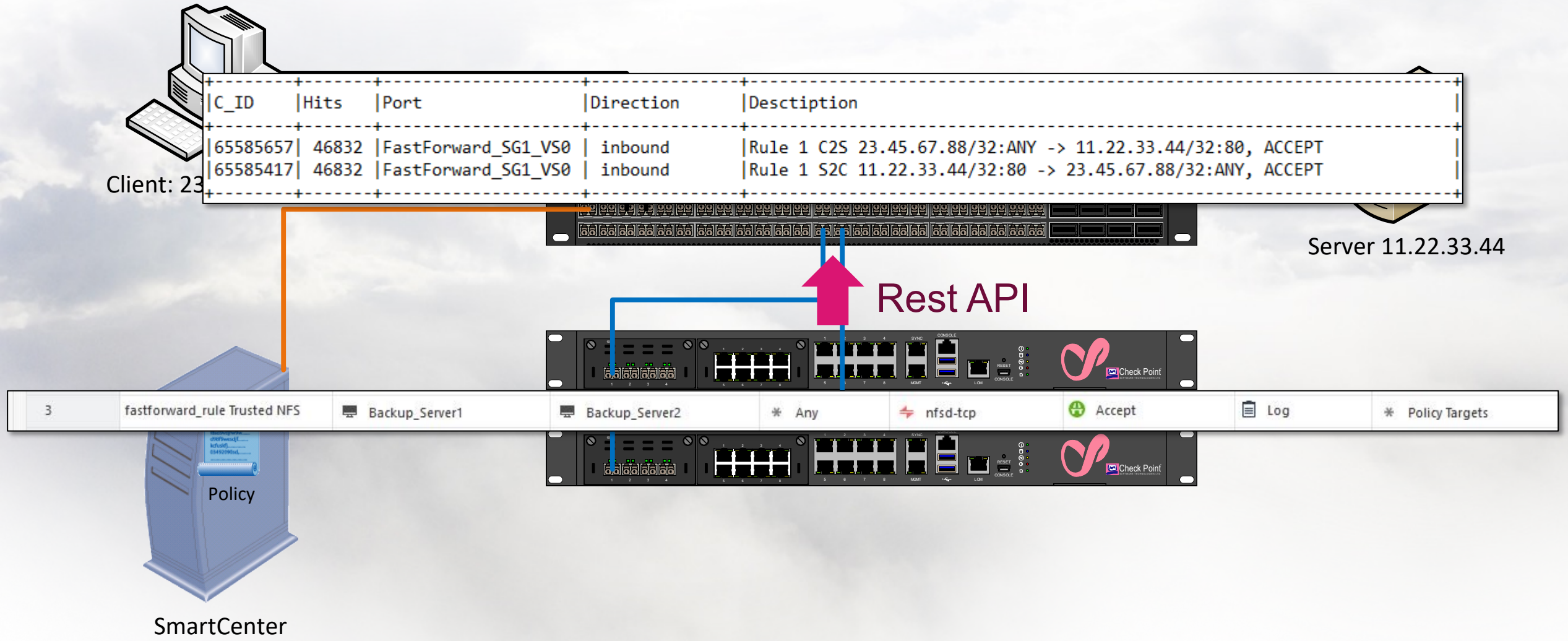


Routing

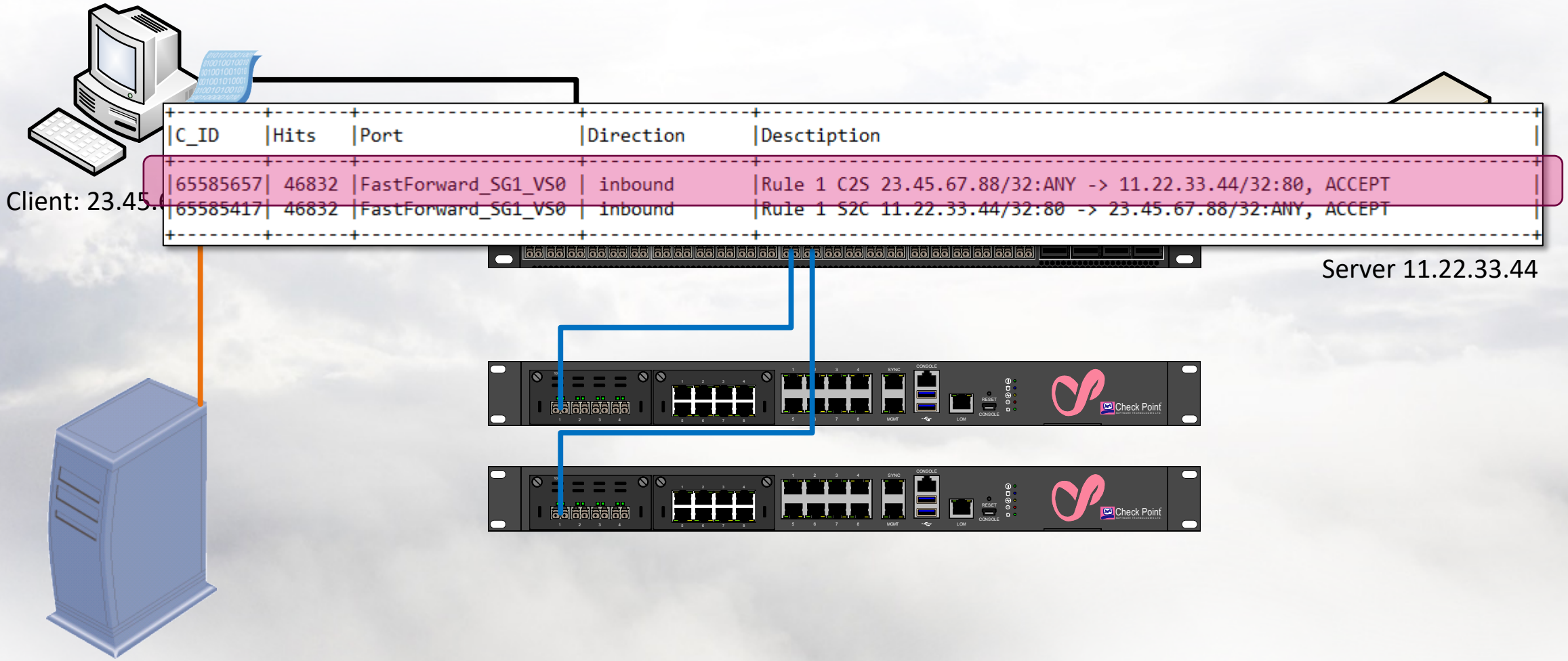
In order to accelerate trusted connection on the MHO at layer 3 level (routing), the MHO has to know the networking information of the gateway in order to send the packet through the right outgoing interface to the right next hop.
(it must have the exact view of the topology as the gateway has).

Therefore, the feature replicates the gateway / virtual system routing topology, so it will be able to accelerate traffic at the MHO level. This logic is also done in hardware level hence very performant.

Example: Security Policy → Access List



Example: Packet matching



Monitoring

TCP connections are logged as usual in the firewall in the log server.

Additional utilities can be executed from the MHO:

View ACL rules hits:

```
Expert# tor_util fastforward show rules <sgid> <vsid>
```

```
Fastforward Rule Hits:
======================

+--------+----------+--------------------+----------+-----------------------------------------------------------------------------------------+
|C_ID    |Hits      |Port                |Direction |Description                                                                              |
+--------+----------+--------------------+----------+-----------------------------------------------------------------------------------------+
|65585152|472065    |FastForward_SG3_VS0 |inbound   |Rule 1 C2S TCP, 17.0.0.4/32:ANY -> 47.0.0.4/32:80, ACCEPT                                |
|65601536|23740853  |FastForward_SG3_VS0 |inbound   |Rule 1 S2C TCP, 47.0.0.4/32:80 -> 17.0.0.4/32:ANY, ACCEPT                                |
|65617920|0         |FastForward_SG3_VS0 |inbound   |Rule 1 C2S TCP, 47.0.0.4/32:ANY -> 47.0.0.4/32:80, ACCEPT                                |
|65634304|0         |FastForward_SG3_VS0 |inbound   |Rule 1 S2C TCP, 47.0.0.4/32:80 -> 47.0.0.4/32:ANY, ACCEPT                                |
|65650688|0         |FastForward_SG3_VS0 |inbound   |Rule 1 C2S TCP, 17.0.0.4/32:ANY -> 17.0.0.4/32:80, ACCEPT                                |
|65667072|0         |FastForward_SG3_VS0 |inbound   |Rule 1 S2C TCP, 17.0.0.4/32:80 -> 17.0.0.4/32:ANY, ACCEPT                                |
|66289664|0         |FastForward_SG3_VS0 |inbound   |Rule 1 C2S TCP, 47.0.0.4/32:ANY -> 17.0.0.4/32:80, ACCEPT                                |
|66273280|0         |FastForward_SG3_VS0 |inbound   |Rule 1 S2C TCP, 17.0.0.4/32:80 -> 47.0.0.4/32:ANY, ACCEPT                                |
|65323008|0         |FastForward_SG3_VS0 |inbound   |Rule 2 C2S ip proto ANY, 19.0.0.4/32:ANY -> 49.0.0.4/32:ANY, ACCEPT                      |
|65339392|0         |FastForward_SG3_VS0 |inbound   |Rule 2 S2C ip proto ANY, 49.0.0.4/32:ANY -> 19.0.0.4/32:ANY, ACCEPT                      |
|65404928|11307793  |FastForward_SG3_VS0 |inbound   |Rule 3 C2S TCP, 17.0.0.0/24:ANY -> 47.0.0.0/24:25, ACCEPT                                |
|65306624|589884    |FastForward_SG3_VS0 |inbound   |Rule 3 S2C TCP, 47.0.0.0/24:25 -> 17.0.0.0/24:ANY, ACCEPT                                |
|65290240|968405    |FastForward_SG3_VS0 |inbound   |Rule 3 C2S TCP, 17.0.0.0/24:ANY -> 47.0.0.0/24:80, ACCEPT                                |
|65273856|46638060  |FastForward_SG3_VS0 |inbound   |Rule 3 S2C TCP, 47.0.0.0/24:80 -> 17.0.0.0/24:ANY, ACCEPT                                |
+--------+----------+--------------------+----------+-----------------------------------------------------------------------------------------+
```

Note: Rule ids are based on fastforward rules order, and not the actual policy rule ids

Monitoring

View current MHO configuration status:

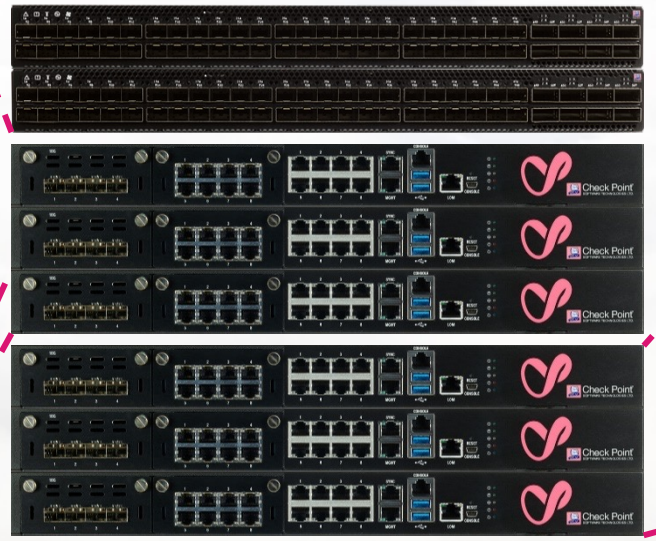
```
Expert# tor_util fastforward show status <sgid> <vsid> [verbose]
```

*for Security Gateway deployment vsid should be 0

Auto Scale

Auto-Scale - Scalability and Flexibility

Physical Shops Security



Internet Shop Security

Maestro HyperScale Security

Part of R81.20 release

Agenda

- **Maestro roadmap**
  - **Short term R81.20**
  - **Long term R81.30**

R81.20 / R81.30

Code Unification for Scalable Platforms into Maintrain

R81.20 main Maestro features

Dynamic balancing for Maestro
Balancing cores utilization in SP

Fast Policy
reduce the policy installation form >10 min to seconds

Fast Forwarding
accelerate trusted traffic upon match of policy rule at the mho level

Connection upgrade / MVC
Zero downtime of the upgrade

MDPS
Data plane separation

Auto scale
Shifting GWs between SGs based on utilization

R81.30 (R82) main Maestro features

Single ISO
ISO unification

RestAPIs support
Full Provisioning for GWs & MHOs

Dual Site Active / Active
For redundant/DR sites

Enhanced SNMP Monitoring
Improved monitoring capabilities; enable SNMP per member

RestAPIs

Maestro full provisioning

Maestro APIs

1. Creation/deletion/viewing of Maestro SG
2. Adding/removing of SGMs to/from a security group
3. Adding/removing/modifying of datalink ports

GWs APIs

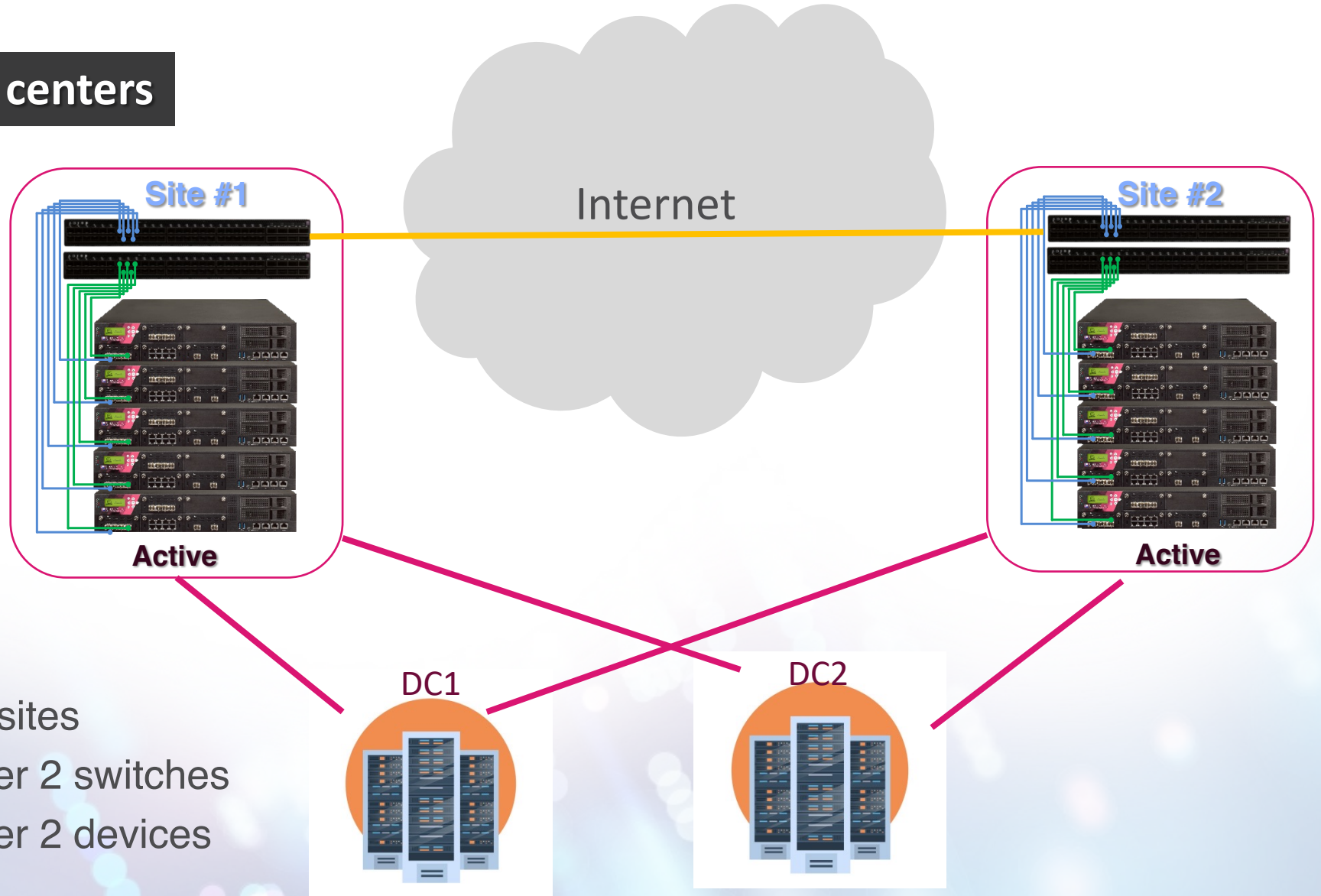
- Align with none SP env capabilities and add the SP specific APIs (e.g. change distribution)

Documentation will be available towards end-2022

EA version for testing – interested?

Maestro Geo Active-Active cluster

Protecting 2 active data centers



Traffic is duplicated between sites

- Simplicity of sync over layer 2 switches
- Simplicity of sync over layer 2 devices

THANK YOU