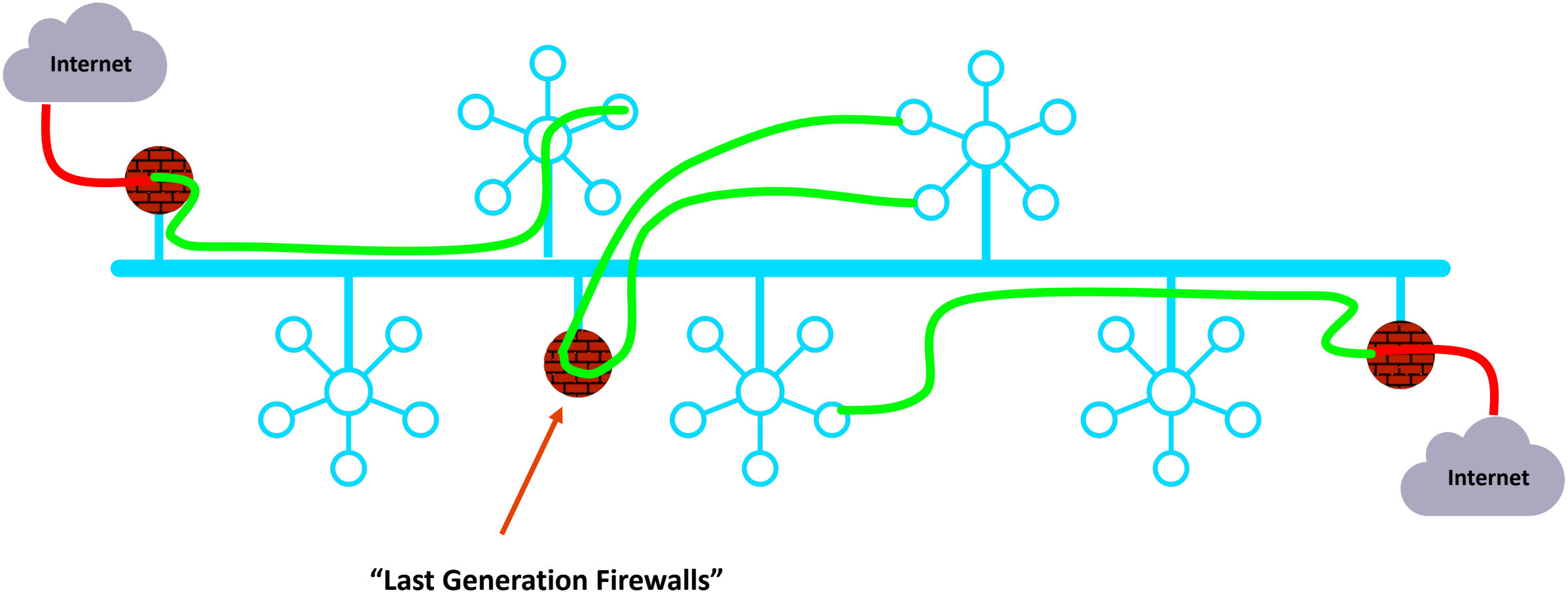
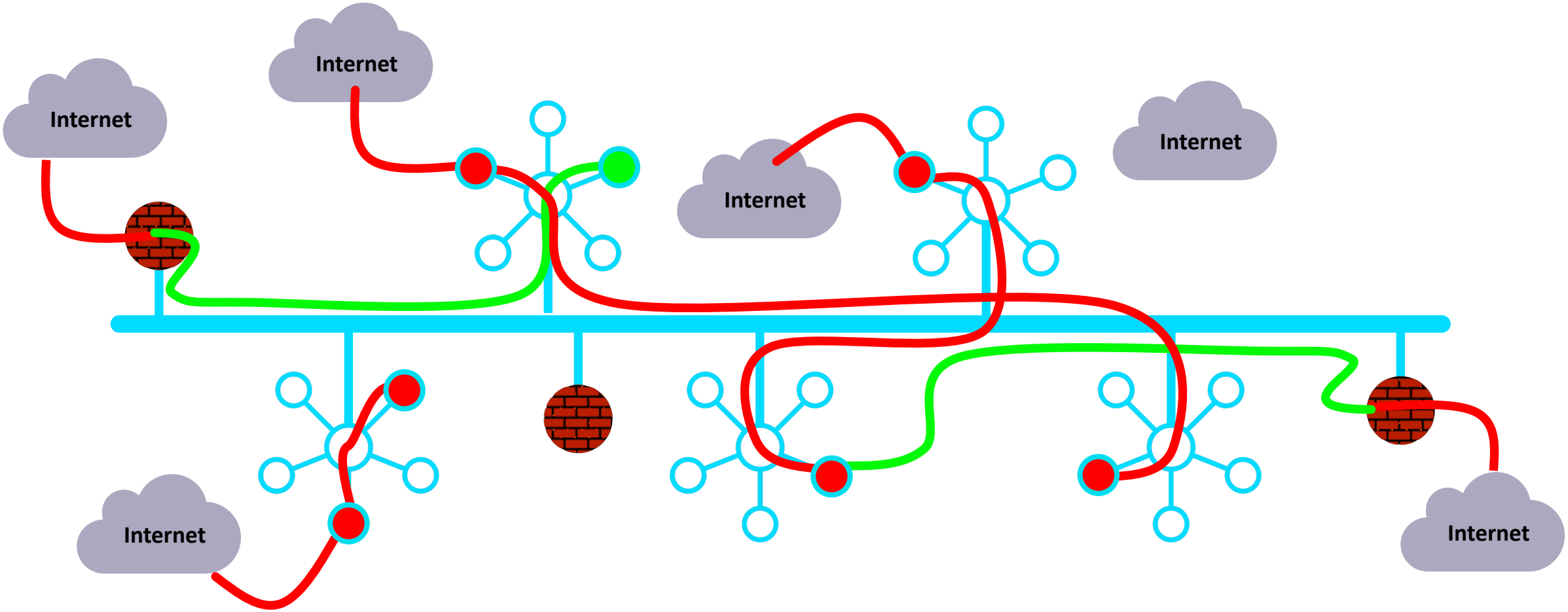
Distributed Cloud Firewall

ACE Solutions Architecture Team

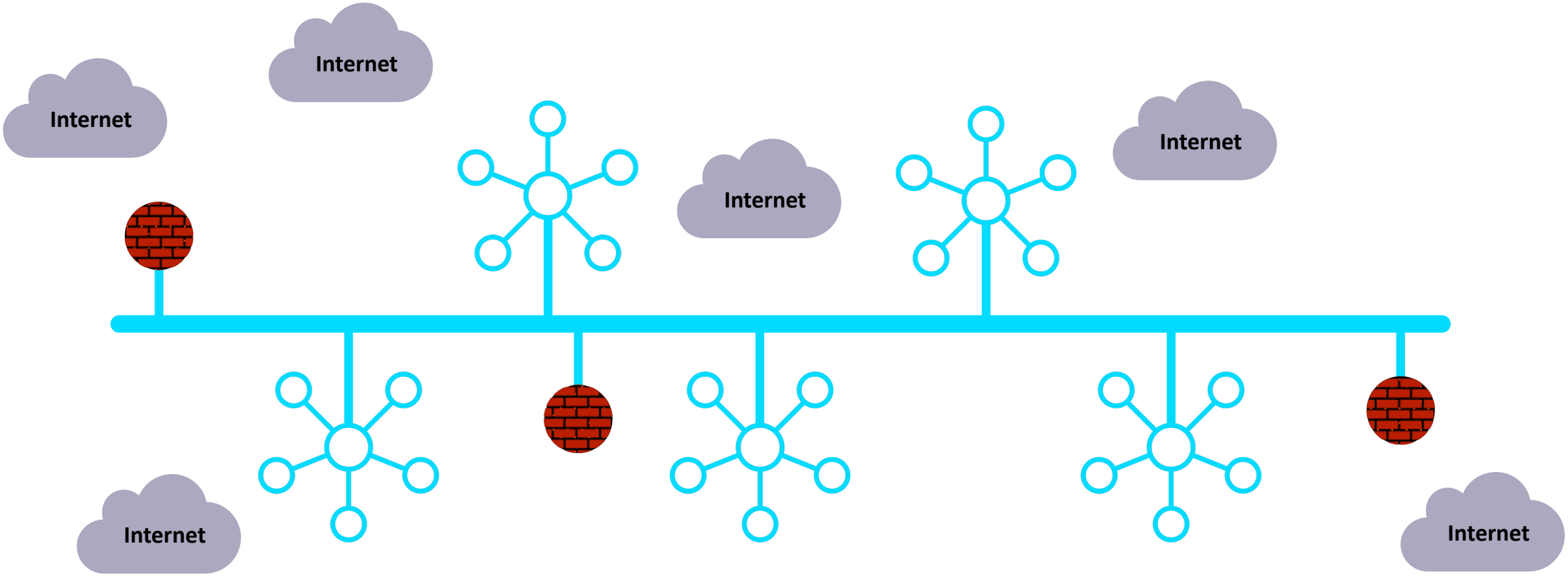
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…



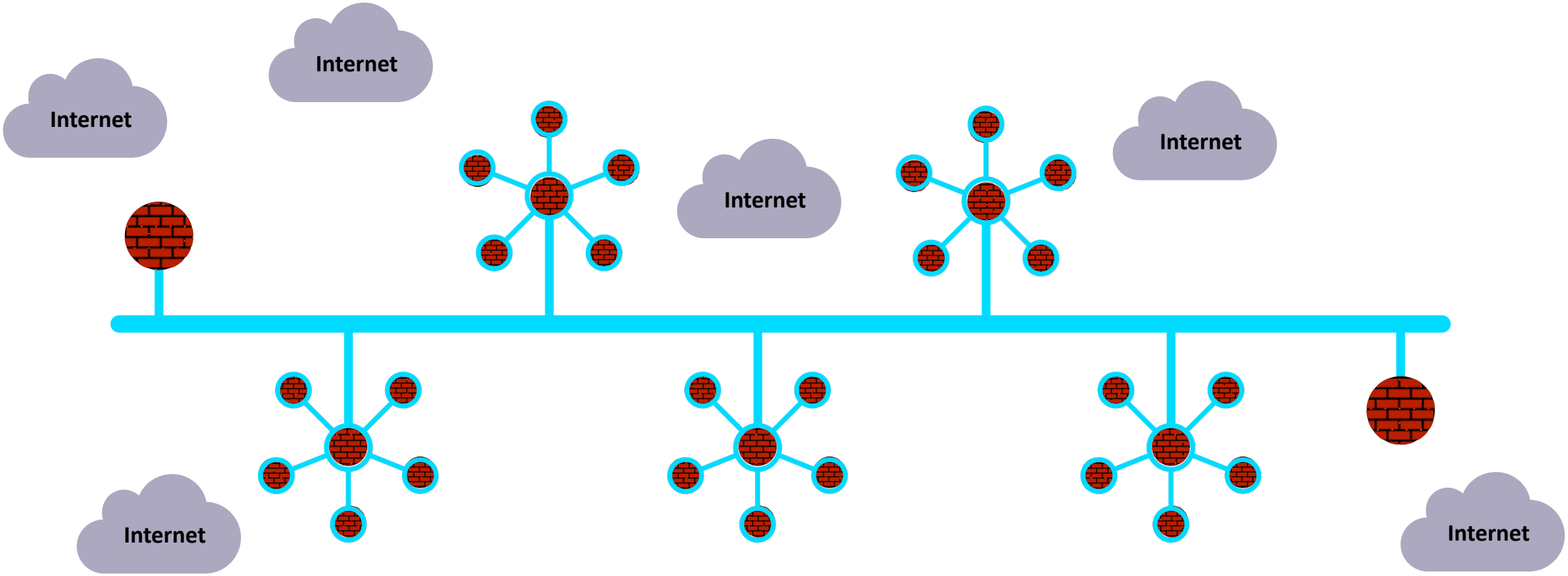
In Reality…


Internet
Internet
Internet
Internet
Internet
Internet
Internet

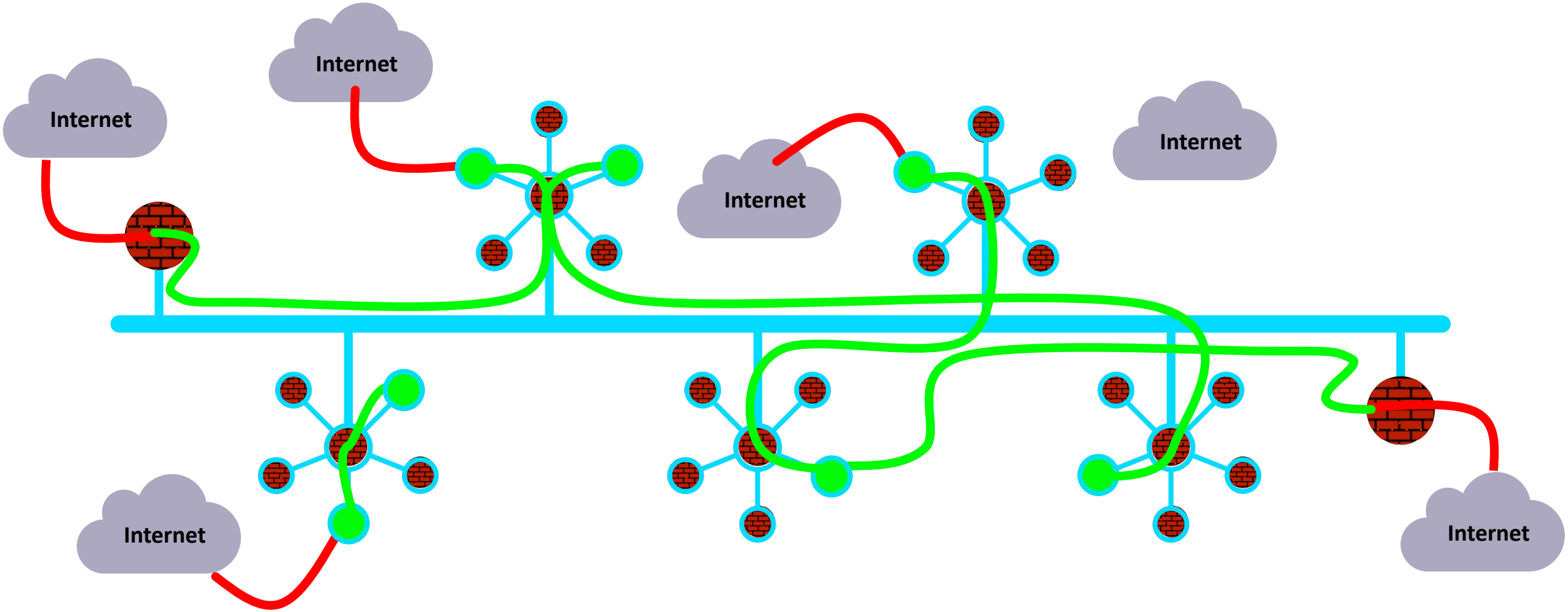
What If… the architecture was built for cloud



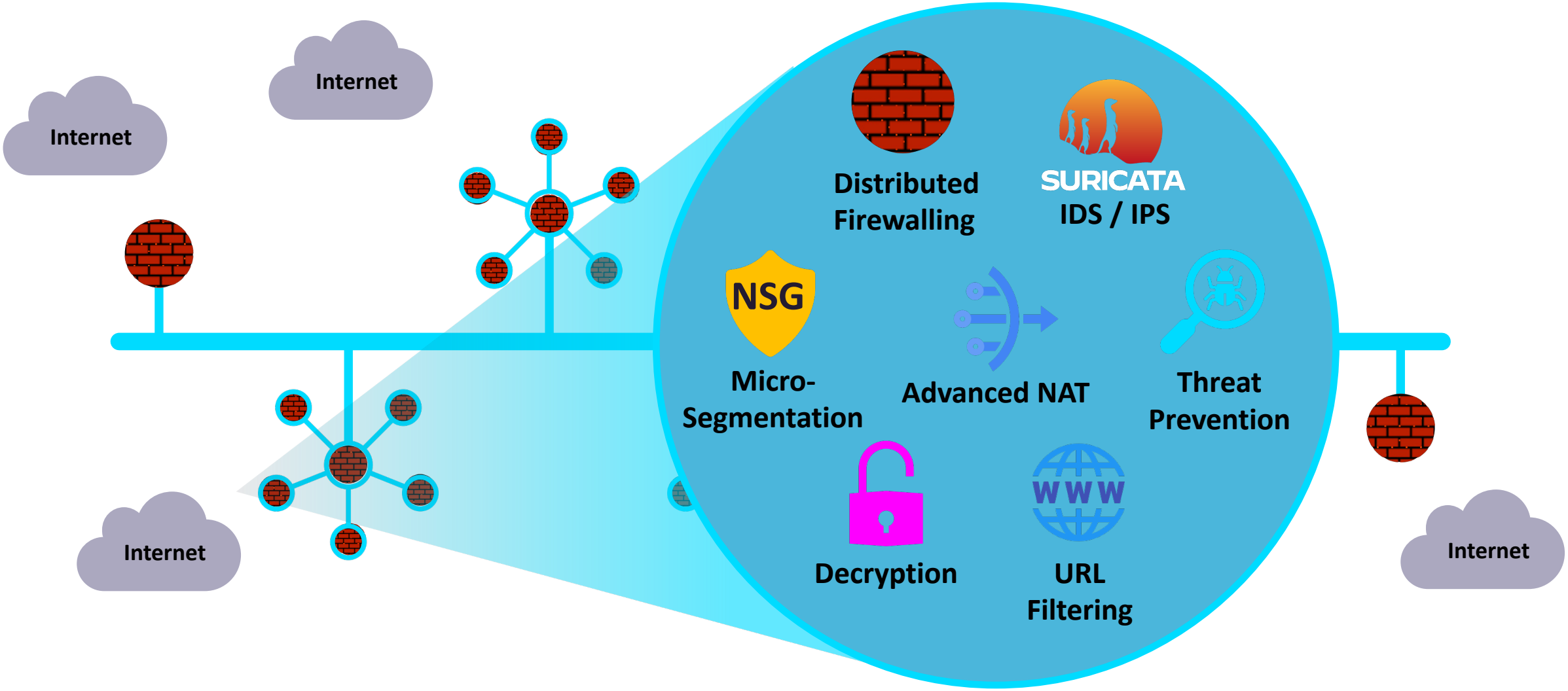
Firewalling Functions were Embedded in the Cloud Network Everywhere…



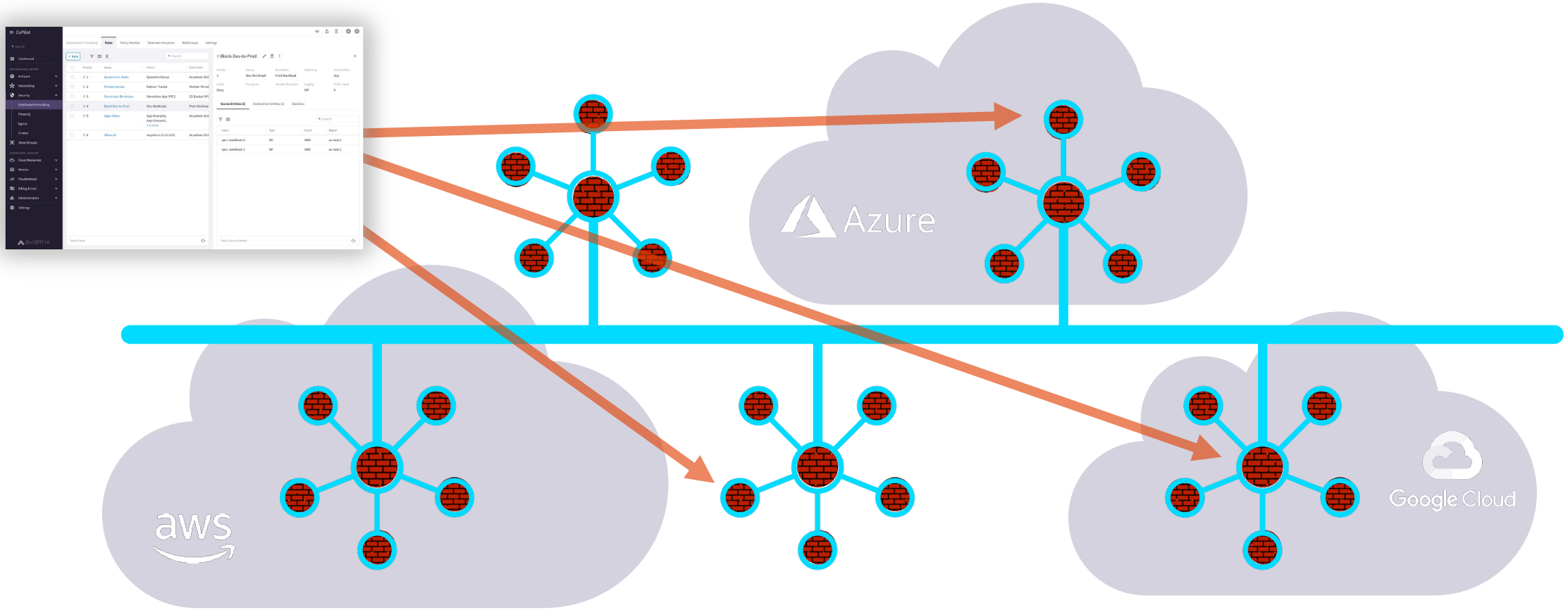
Centrally Managed, with Distributed Inspection & Enforcement…



And, What If it was more than just firewalling…



Policy Creation Looked Like One Big Firewall … A Distributed Cloud Firewall…



Where and How Policies Are Enforced Is Abstracted…

Smart Group

- **What is a Smart Group?**

A Smart Group identifies a group of resources that have similar policy requirements, that are confined in the same logical container.

- The members of a Smart Group can be classified using *three* methods:
  - CSP Tags
  - Resource Attributes
  - CIDR

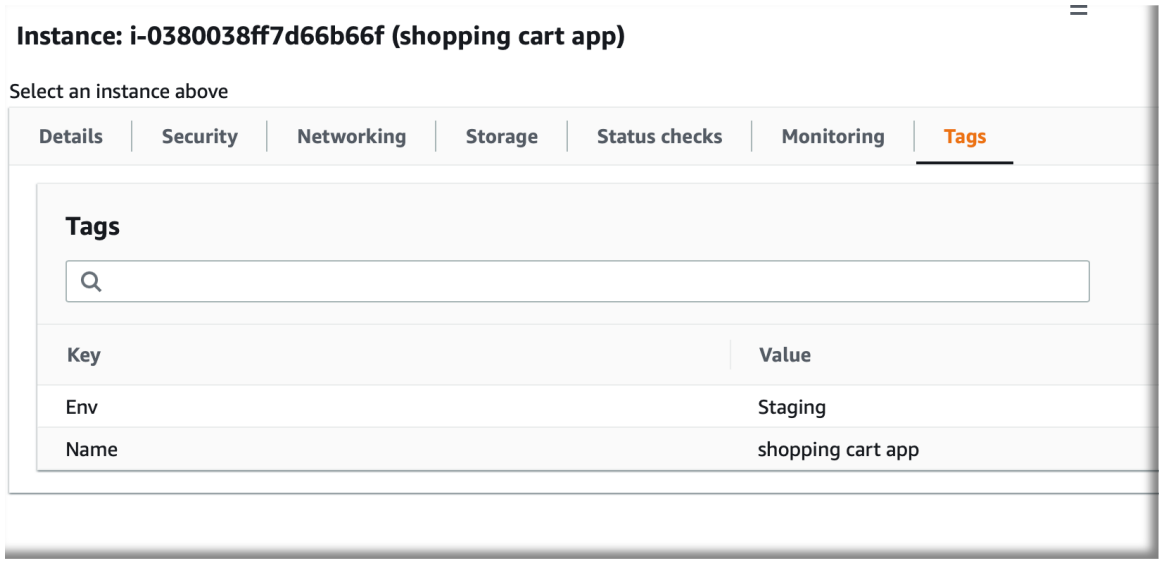
Classification Methods

CSP Tags (recommended)

- Tags are assigned to:
  - Instance
  - VPC/VNET
  - Subnet
- Tags are {Key, Value} pairs
- Eg: A VM hosting shopping cart application can be tagged with:

  {Key: Type, Value: Shopping cart app}

  {Key: Env, Value: Staging}



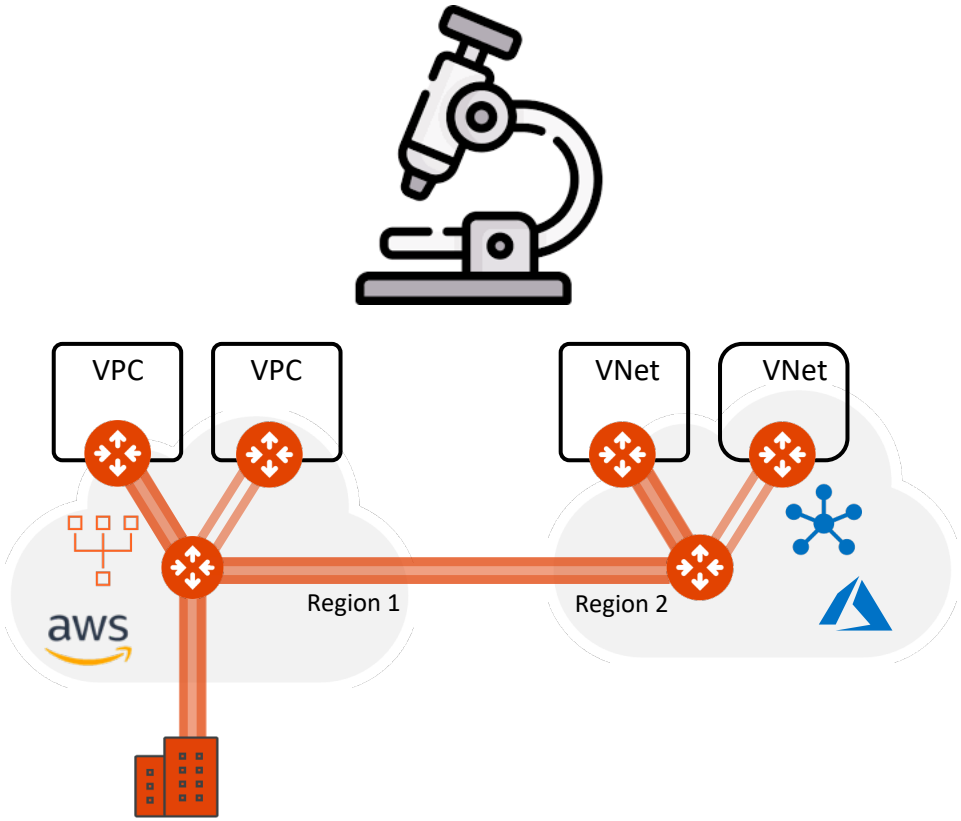
Resource attribute

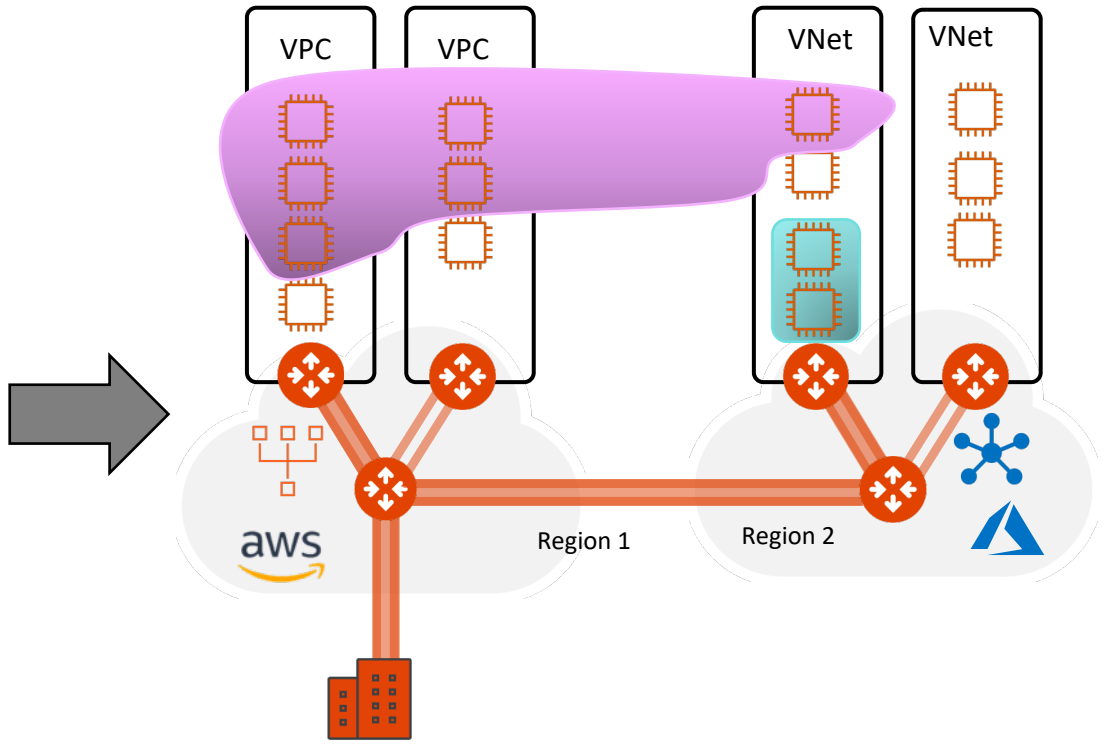
- Region Name, Account Name

IP Prefixes

- CIDR

Distributed Firewalling: Intra-rule vs. Inter-rule





Smart Groups

Apache

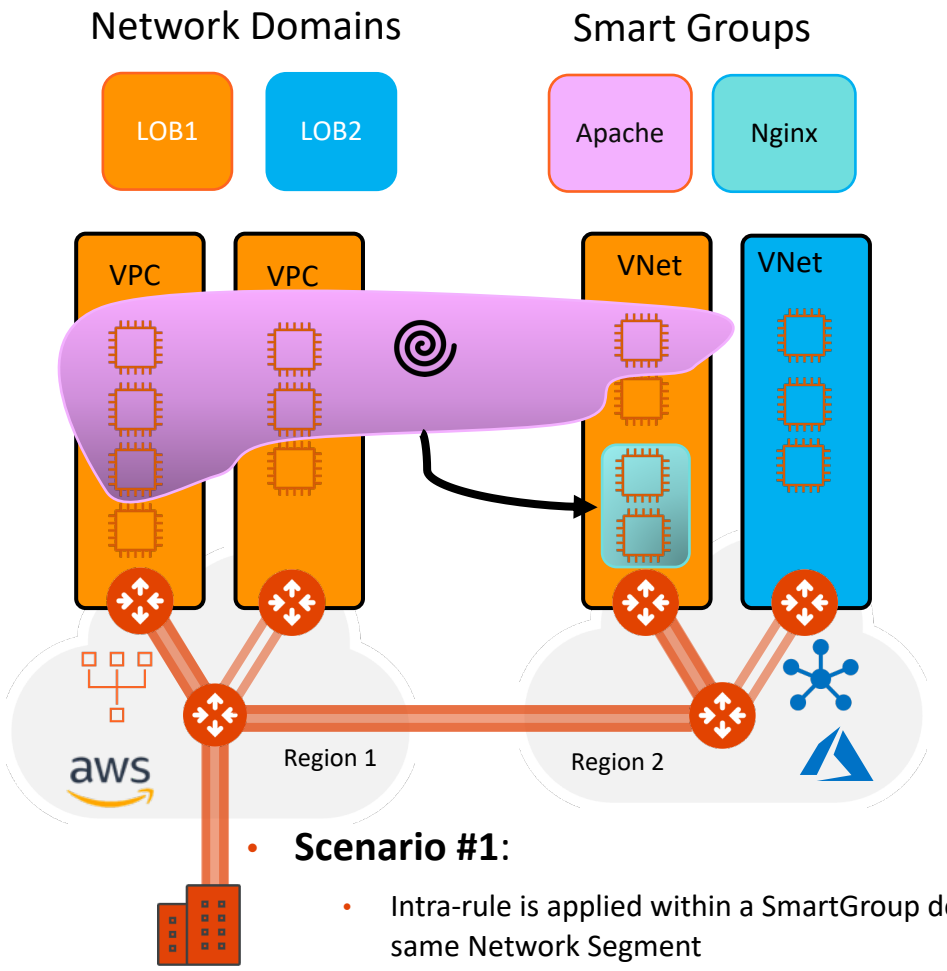
Nginx

A rule between SGs can be defined for achieving the *INTER-SMARTGROUP* communication

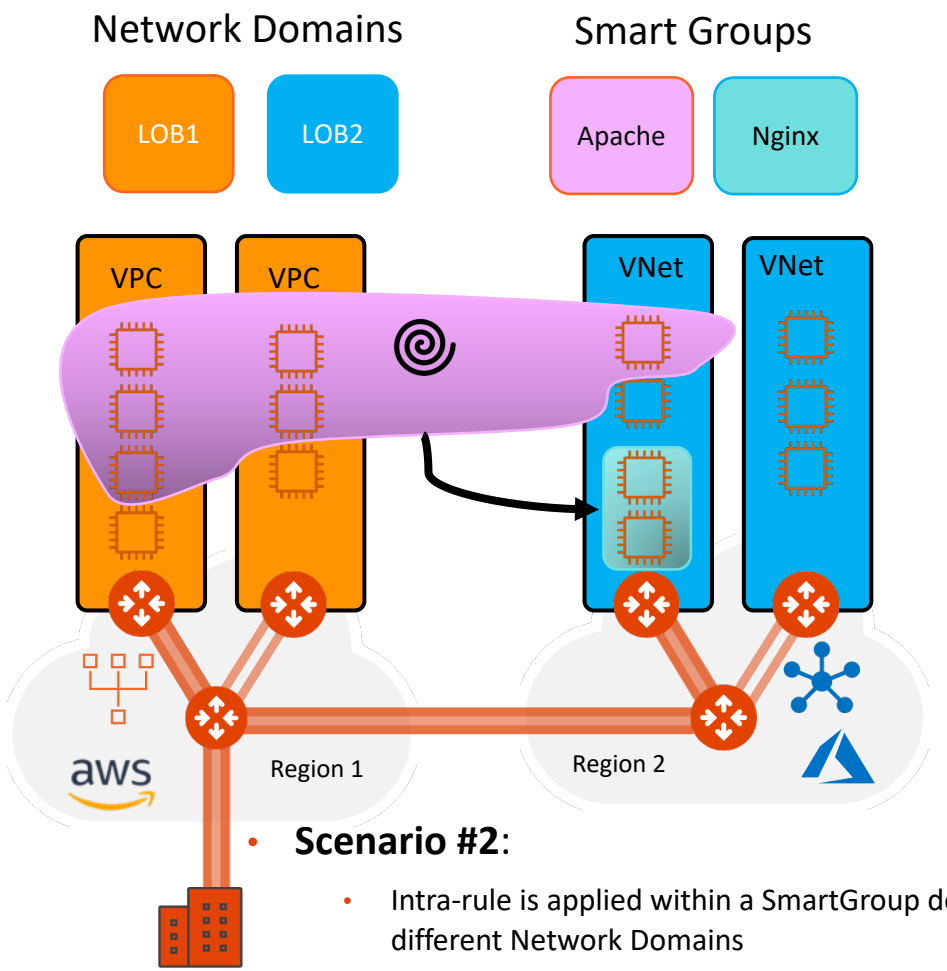
- **INTRA-RULE**: is defined <u>within</u> a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

- **INTER-RULE:** is defined among Smart Groups, for dictating what kind of traffic is allowed/prohibited among two or more Smart Groups.

Network Segmentation & Distributed Cloud Firewall Rule



- **Scenario #1**:
  - Intra-rule is applied within a SmartGroup defined in the same Network Segment
  - Inter-rule is applied between SmartGroups within the same network Domain

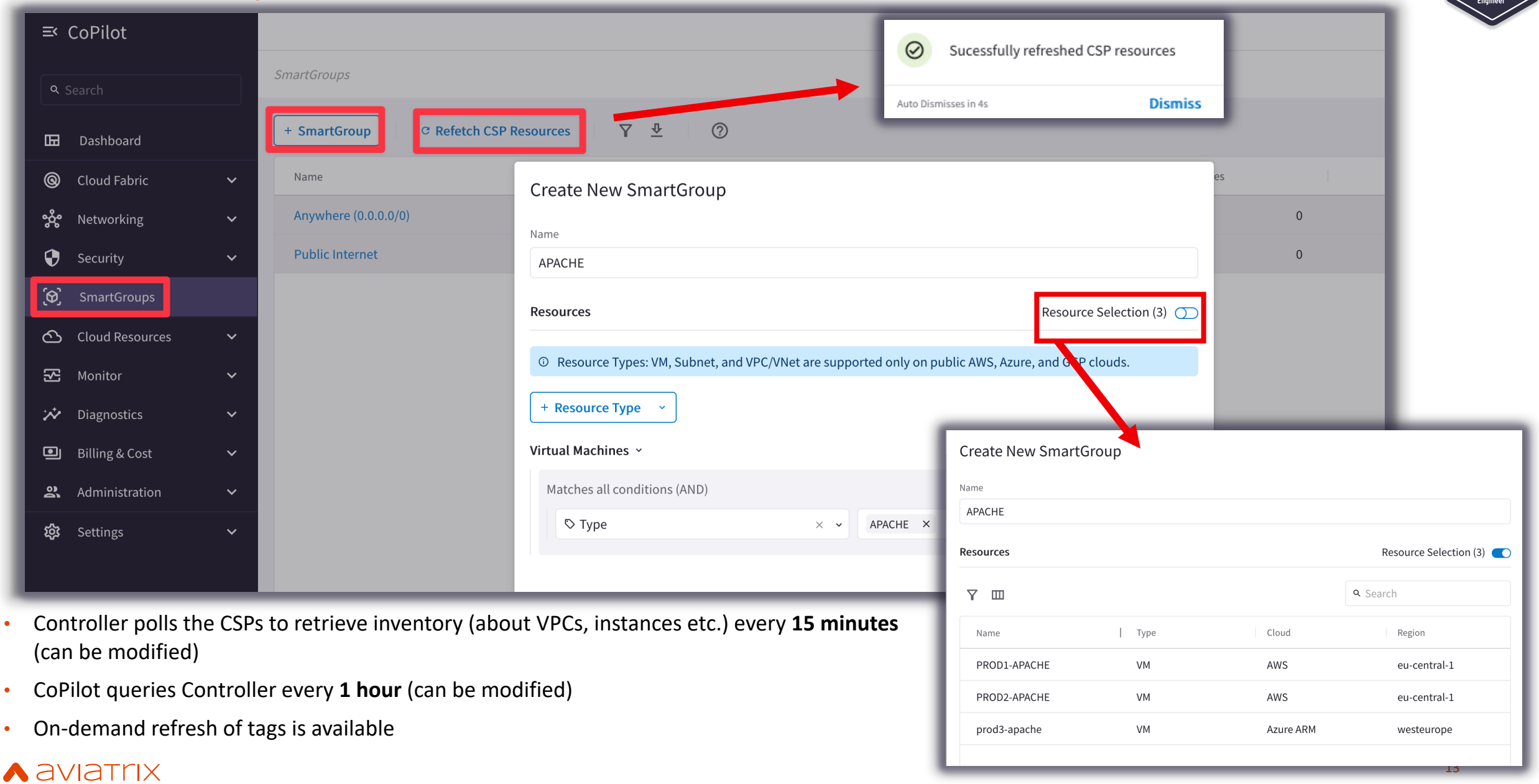


- **Scenario #2**:
  - Intra-rule is applied within a SmartGroup defined across two different Network Domains
  - Inter-rule is applied between SmartGroups defined across two different network Domains

Caveat:

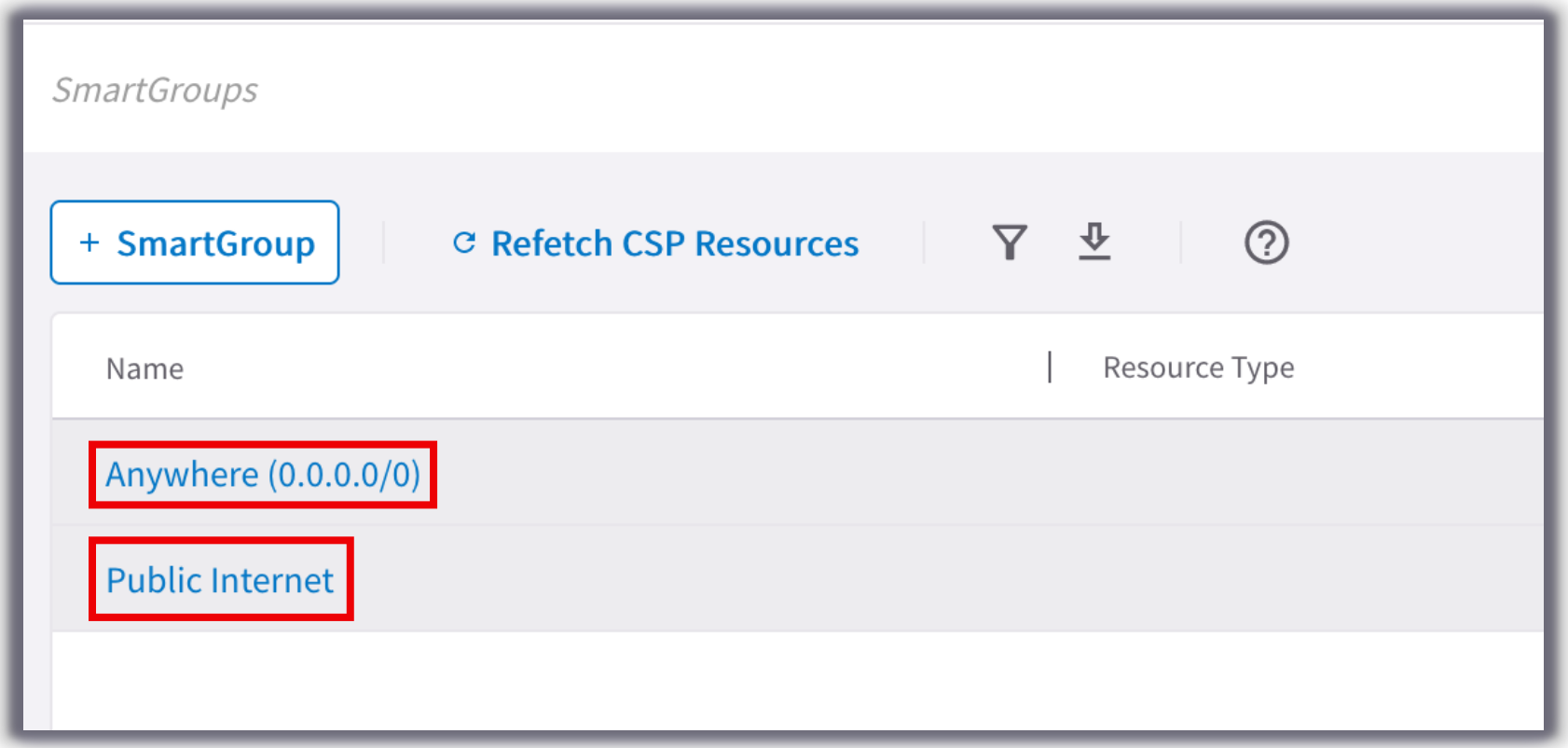
- Network Segmentation and Distributed Firewalling are **NOT** mutually exclusive!
- Network Segmentation takes **precedence** over the extent of a SmartGroup

Smart Groups Creation



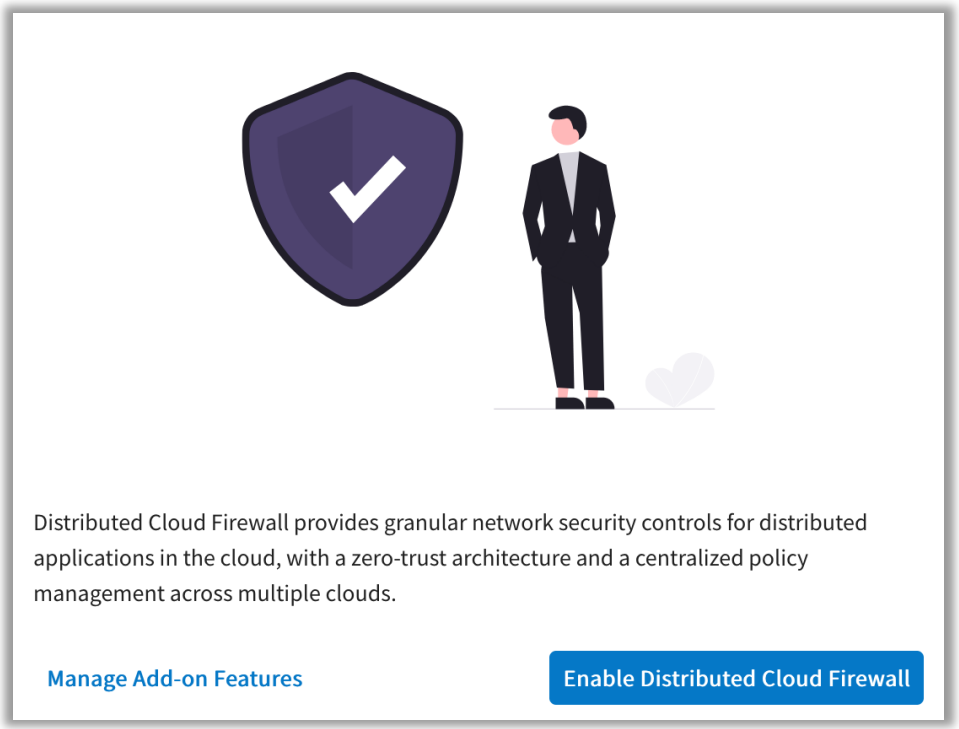
- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

Pre-defined Smart Groups



- **Anywhere (0.0.0.0/0)** → RFC1918 routes + Default Route (IGW)
- **Public Internet** → Default Route (IGW)

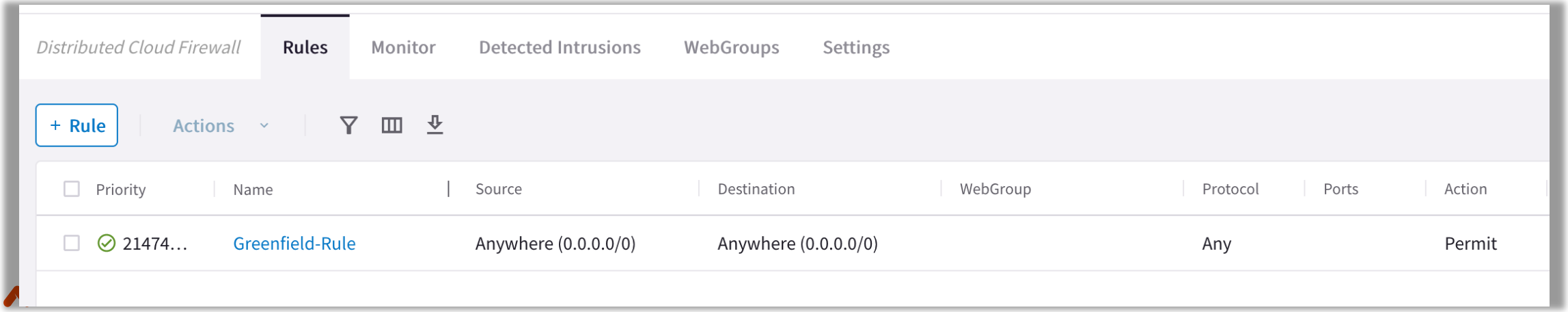
Enabling Distributed Cloud Firewall



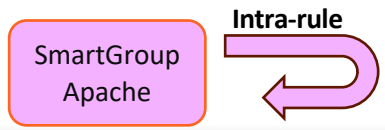
- Enabling the Distributed Cloud Firewall without configured rules will deny all previously permitted traffic due to its implicit Deny All rule.
- To maintain consistency, a **Greenfield Rule** will be created to allow traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.

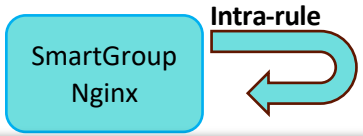
DENY LIST MODEL (THREAT-CENTRIC MODEL):

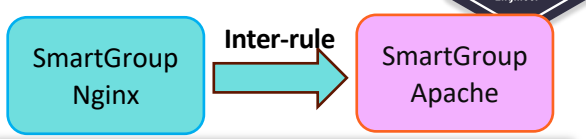
❑allow all data to flow, except for exactly what you say should be stopped.

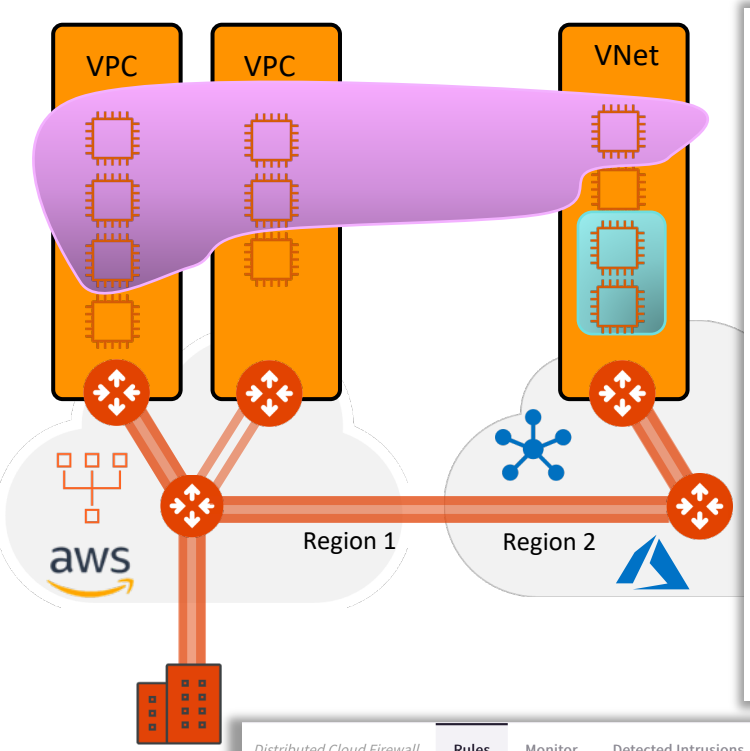


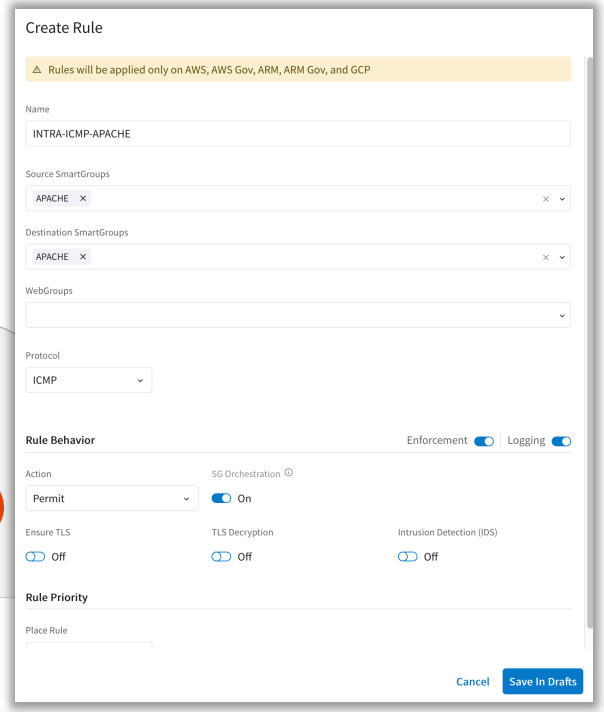
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules

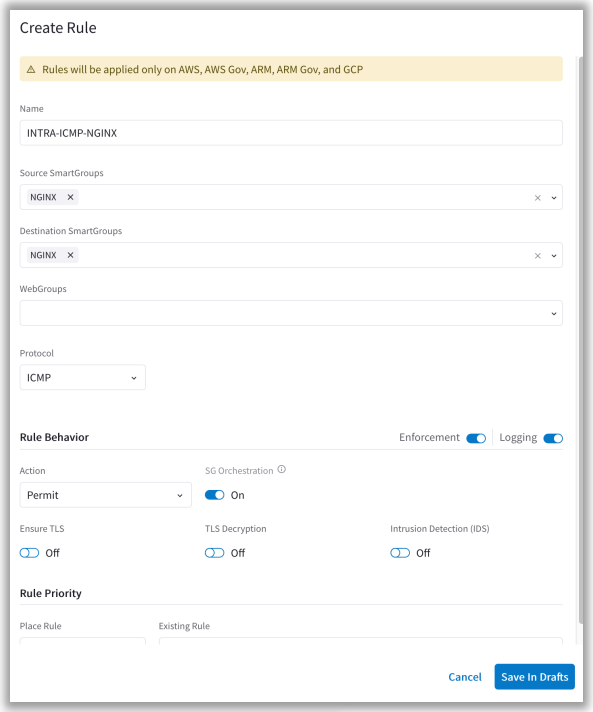


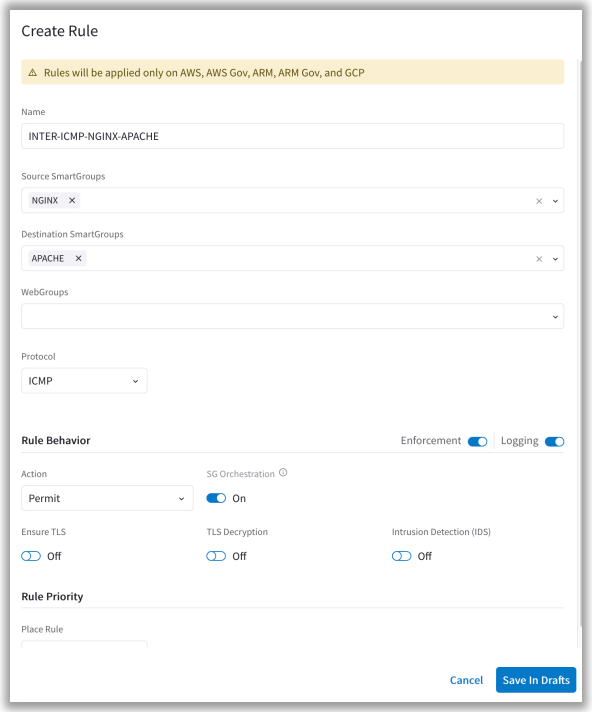


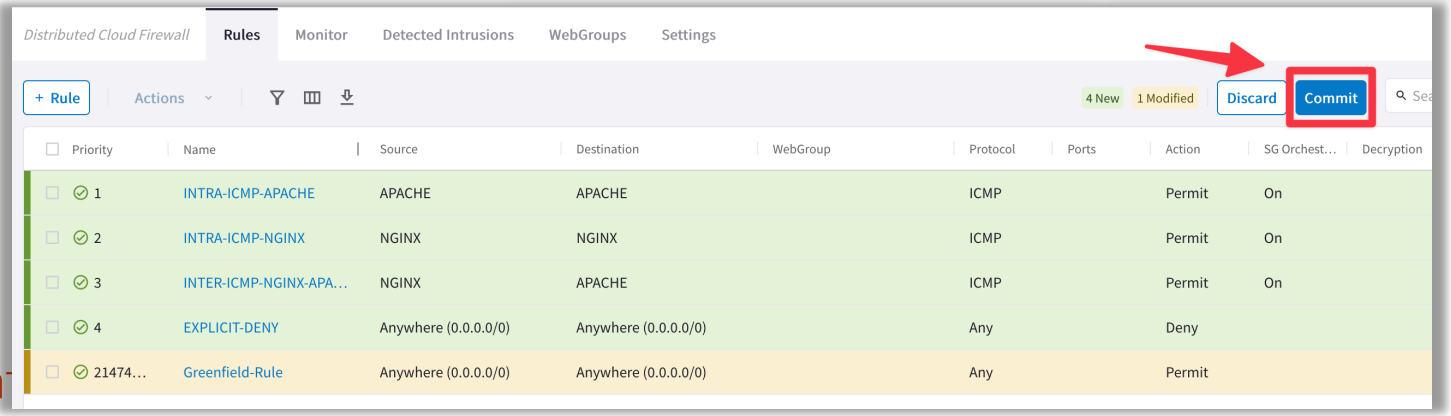








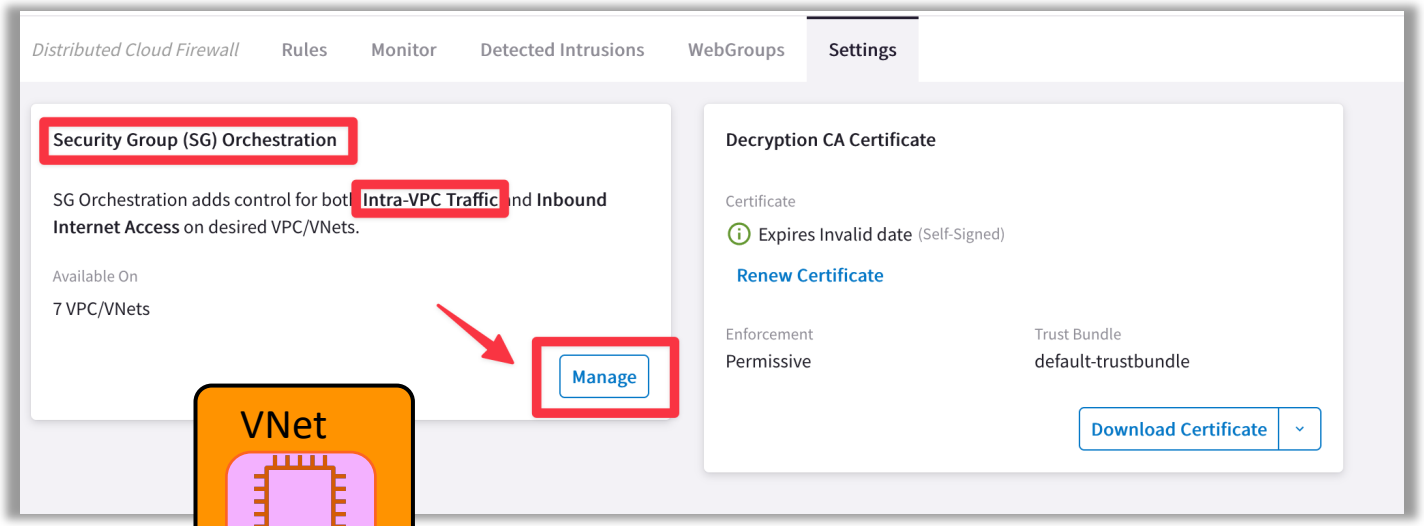


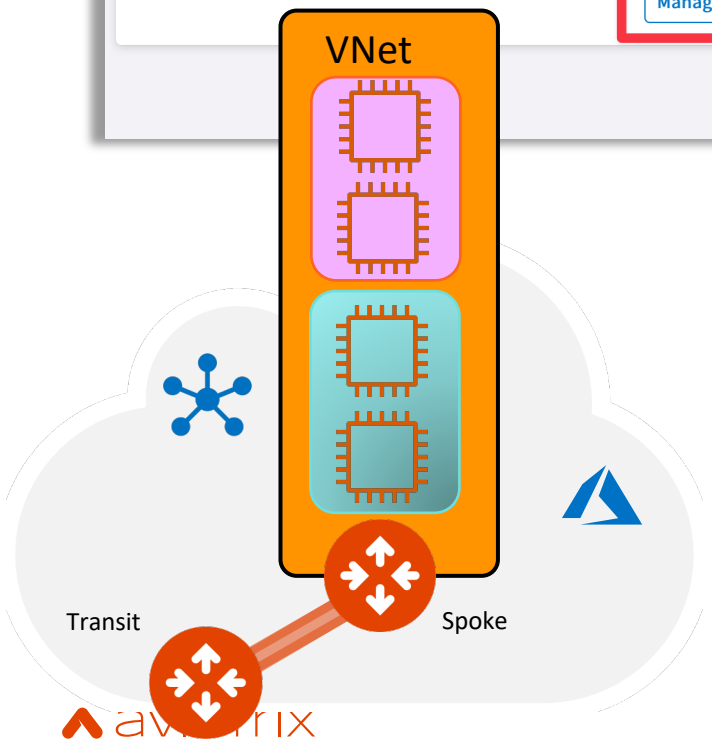


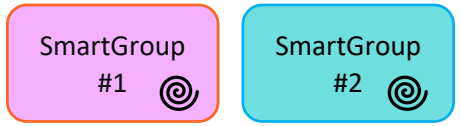
- **Micro-Segmentation**: Combination of SmartGroups and DCF Rules
- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return traffic is allowed automatically

Intra VPC/VNET Distributed Firewalling (available on AWS/Azure)

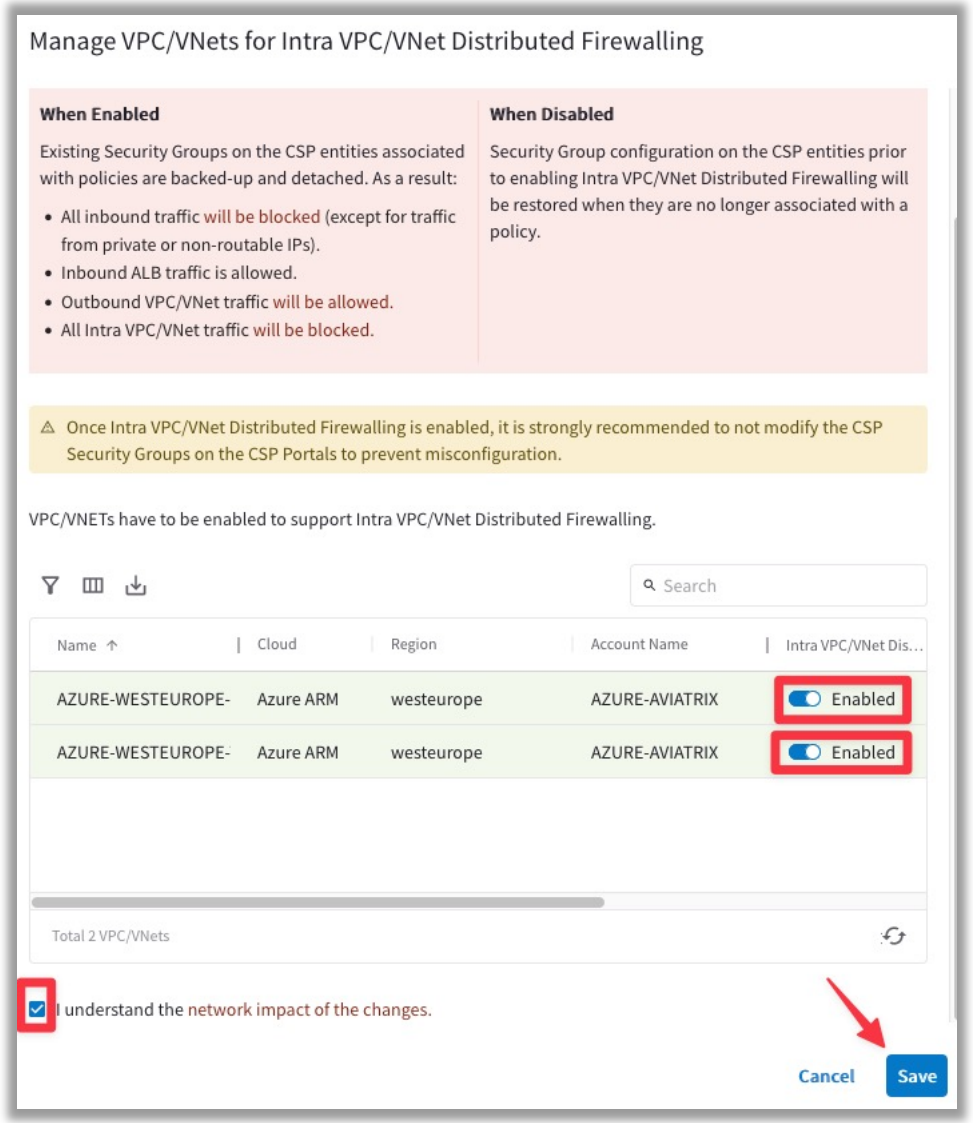
❑ Enable the feature on the relevant VNets



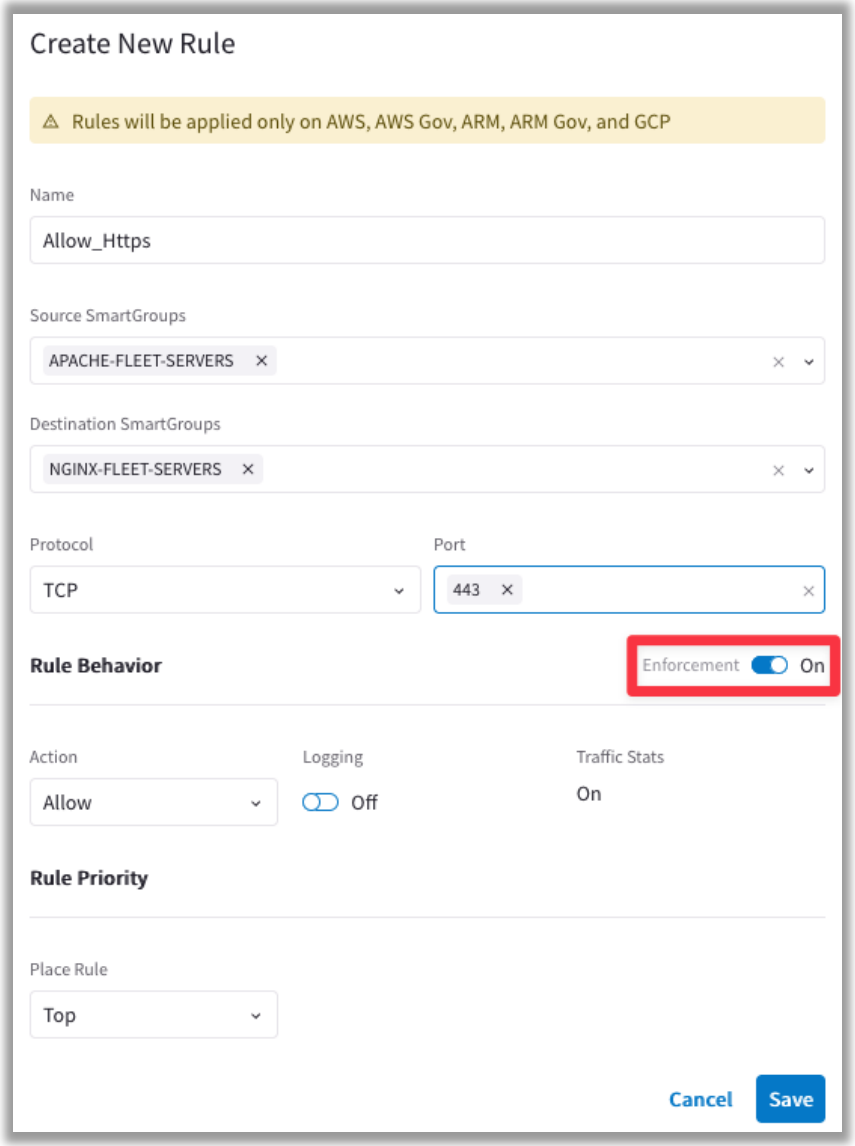




- If you enable the Security Group orchestration (*aka Intra-VPC Traffic Control*), the SmartGroups will not be able to communicate with each other unless an inter rule is applied between them.
- This is pure L4 separation using the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.
- **Future Implementation**: traffic will be diverted to the nearby Spoke GW for the L7 inspection



Rule Enforcement



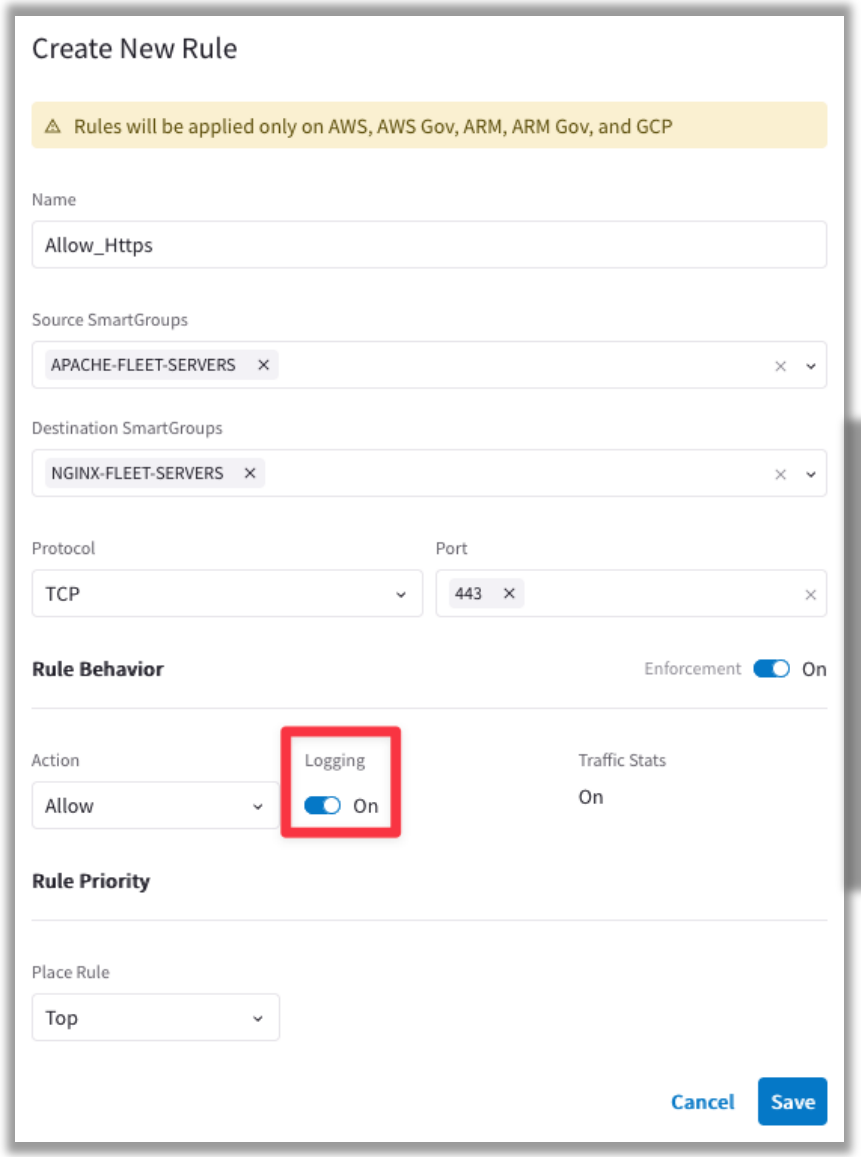
Enforcement ON

- Policy is enforced in the Data Plane

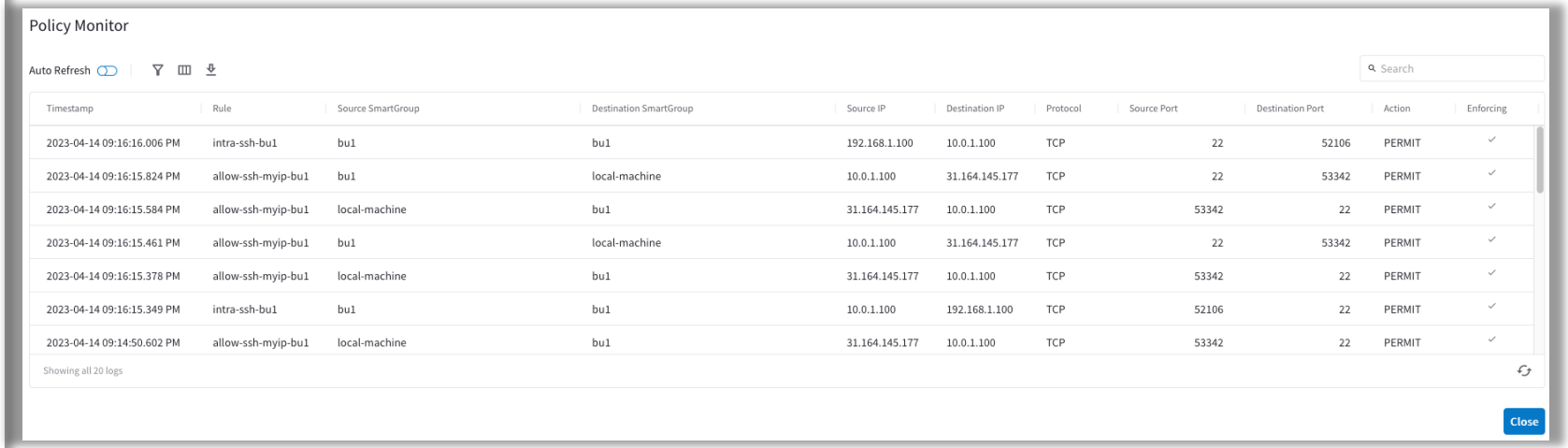
Enforcement OFF

- Policy is NOT enforced in the Data Plane
- The option provides a *Watch/Test* mode
- Common use case is with deny rule
- Watch what traffic hits the deny rule before enforcing the rule in the Data Plane.

Rule Logging



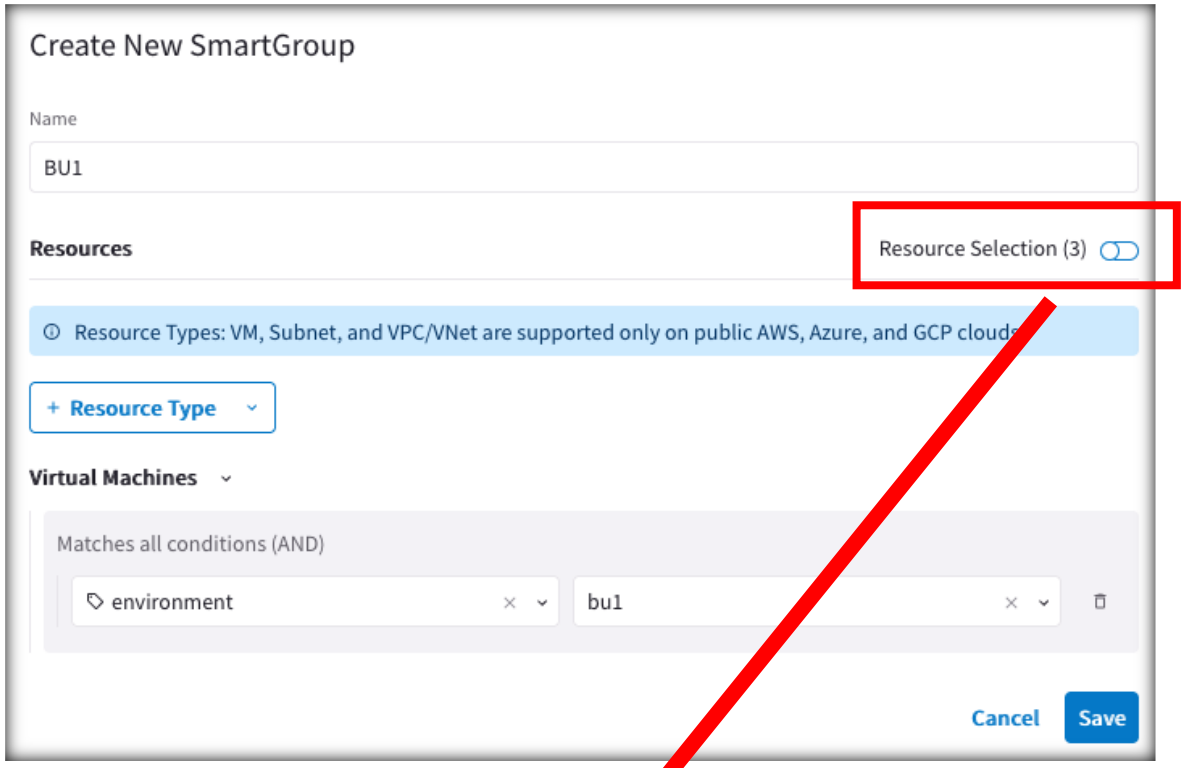
- **Logging can be turned ON/OFF per rule**
- **Configure Syslog to view the logs**

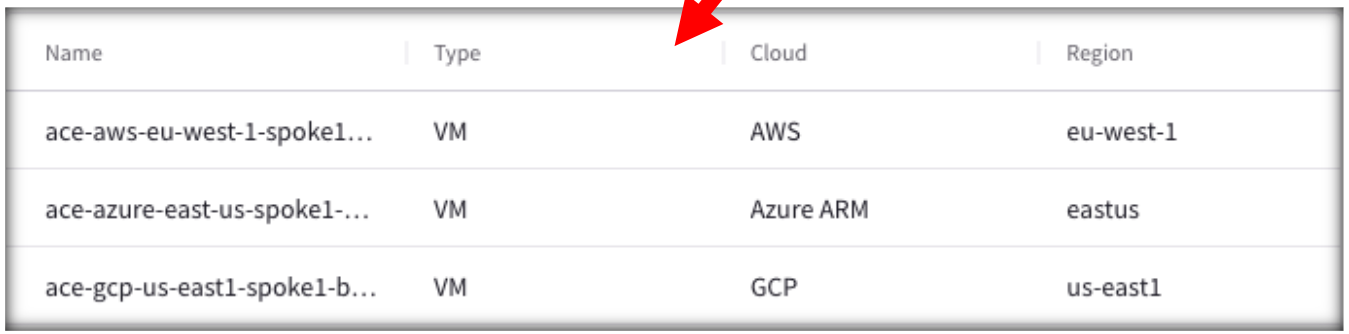


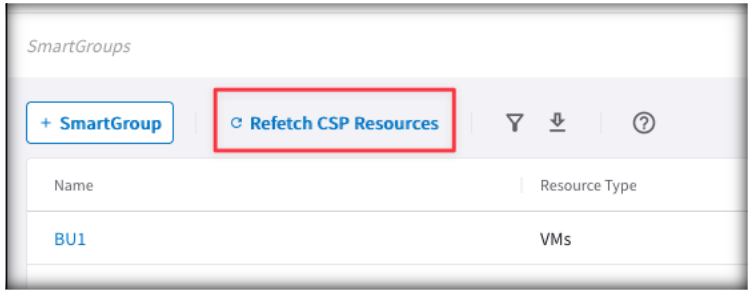
Tools for troubleshooting Distributed Cloud Firewall

Creation of the SmartGroup: the right matching criteria dilemma

1) Choose the right matching criteria for resources that you want to see assigned to a specific SmartGroup:
   - Classification based on the **CSP Tags**
   - Classification based on the **Resource Properties** (i.e. Name, Region or Account Name)
   - Classification based on the **IPs/CIDRs**
2) Use the **Preview Resources** toggle switch to verify the selected resources that have been mapped to the Smart Group
3) Use the On-Demand **Refetch CSP Resources** button to retrieve the most recent inventory



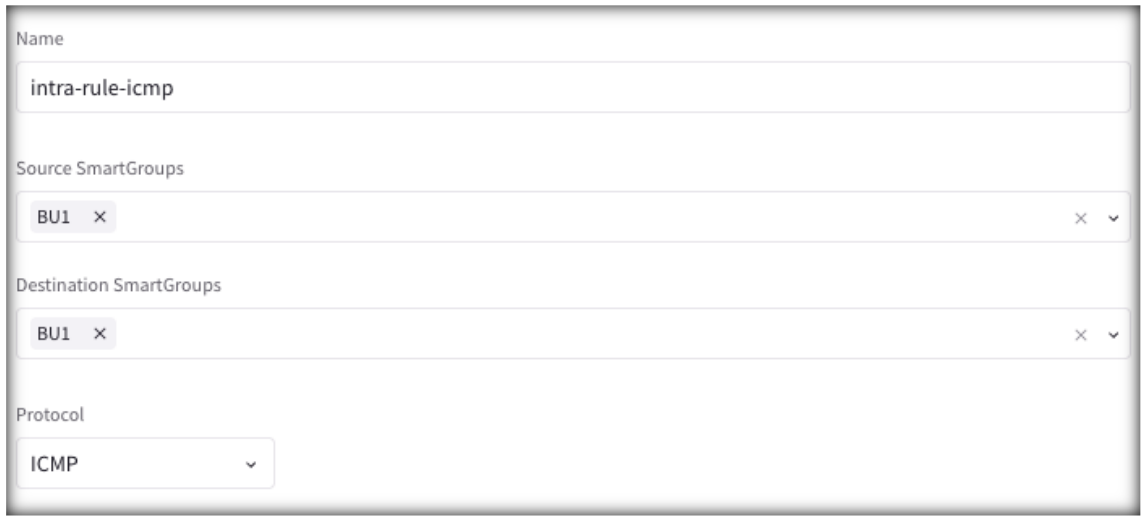


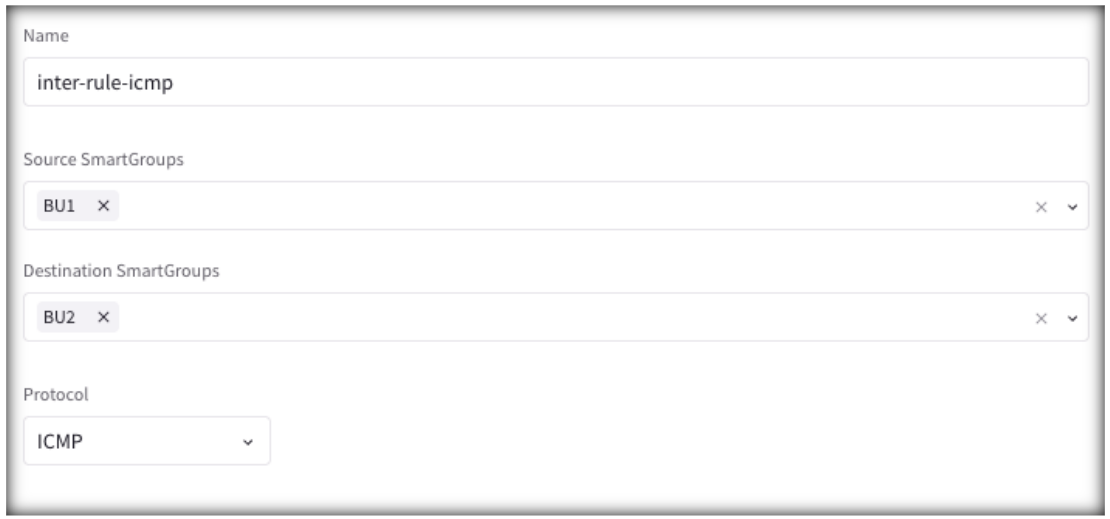


Creation of the Rules: intra-rule vs. inter-rule

1) **Intra-rule** will affect the traffic WITHIN a Smart Group
   - Source Smart Group and Destination Smart Group must be the same

2) **Inter-rule** will affect the traffic BETWEEN SmartGroups
   - Source Smart Group and Destination Smart Group must differ





CAVEAT – The Invisible Implicit Deny: as soon as a Rule is committed (either intra-rule or inter-rule) a hidden deny is applied at the bottom of your Rules list. The implicit deny is really an "invisible deny"; you won't see a "deny any" line automagically added! Since you don't see it, it's easy to forget about. Forgetting about the implicit deny is the #1 reason for Distributed Firewalling Rule not giving you the desired results.

Next:

Lab 8 Distributed Cloud Firewall