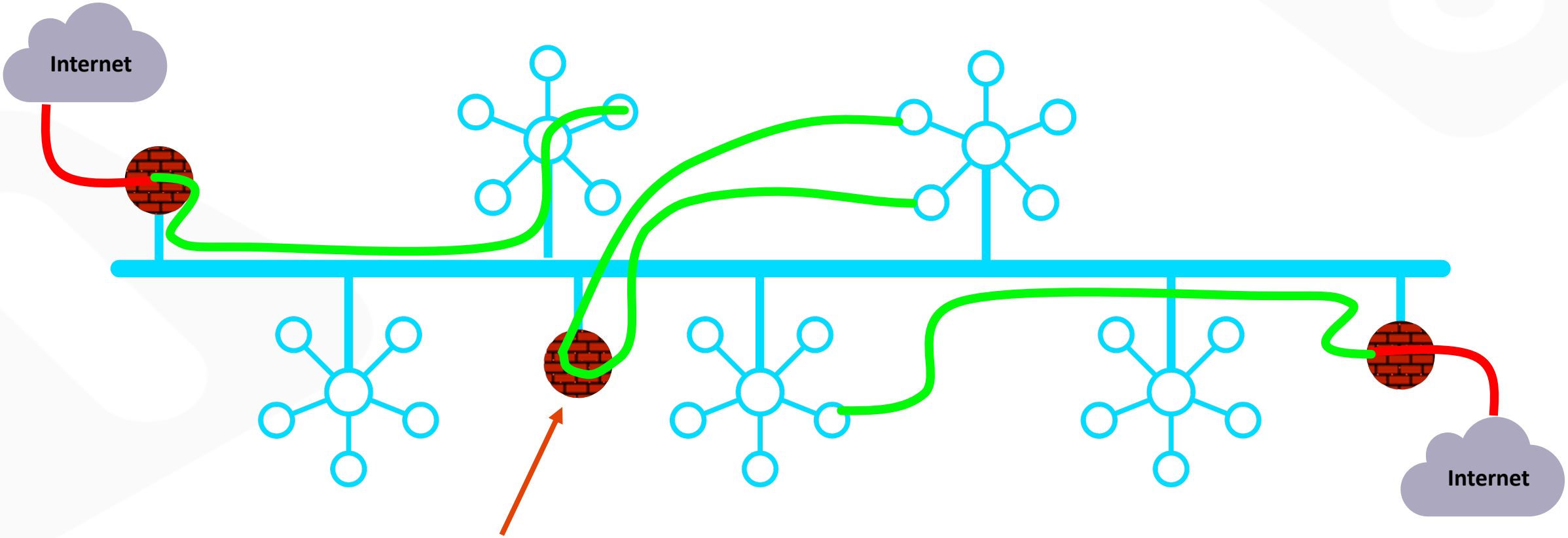
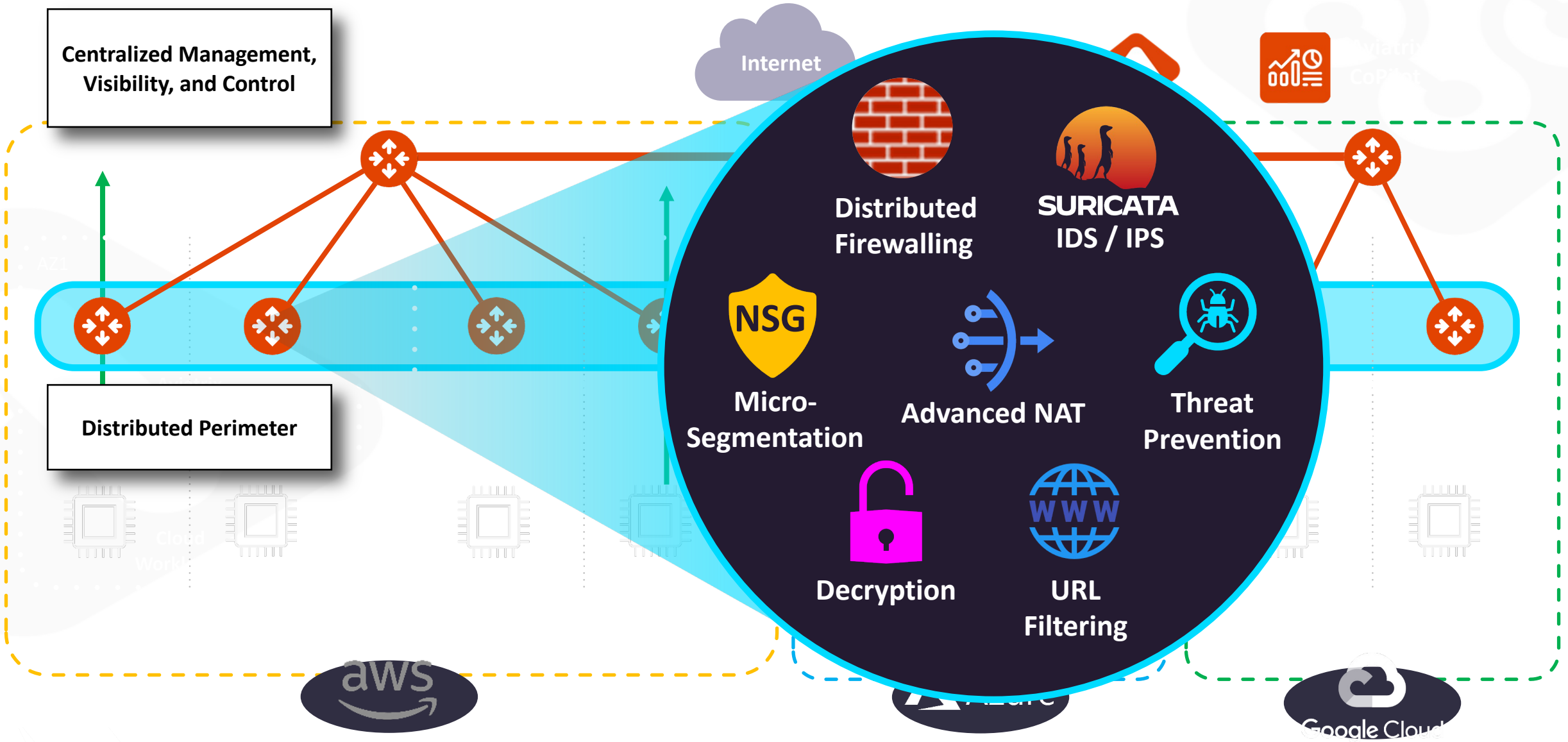
aviatrix

Distributed Cloud Firewall

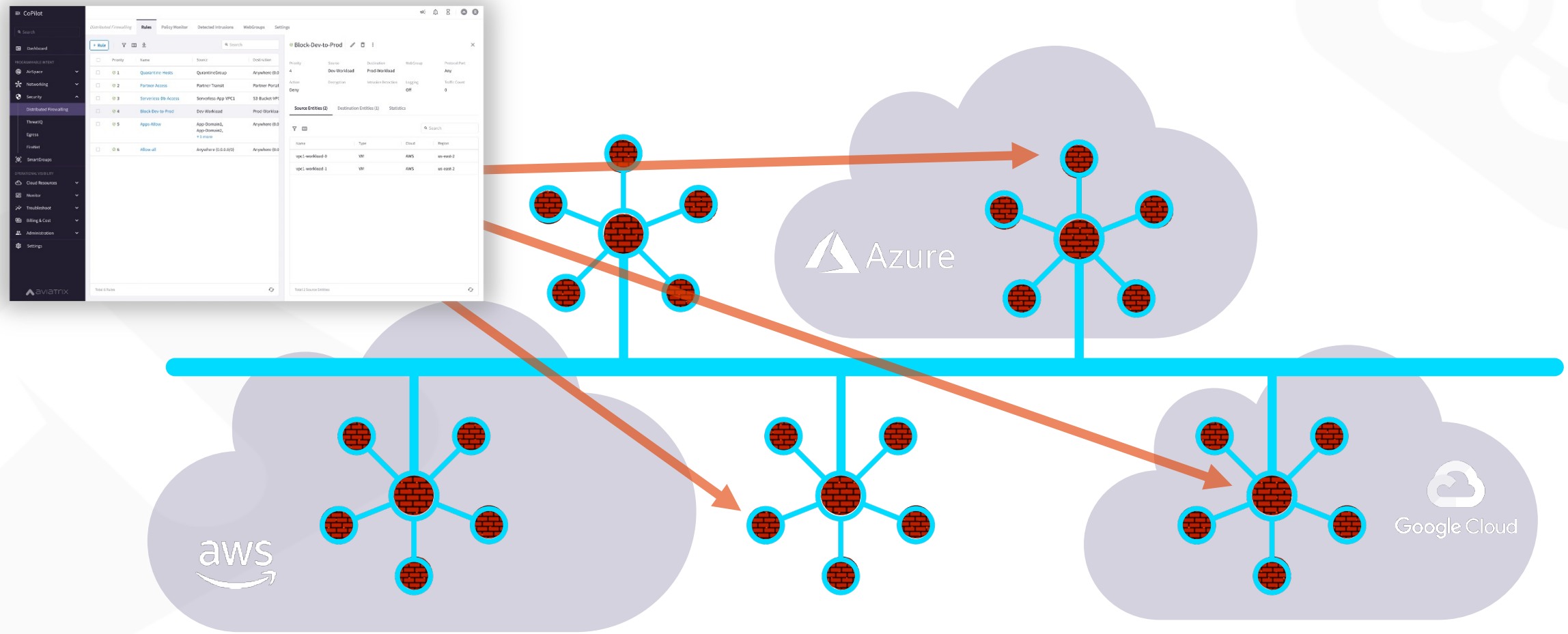
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…



Aviatrix Distributed Cloud Firewall



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



Where and How Policies Are Enforced Is Abstracted…

SmartGroup: Definition

- A firewall rule consists of two important initial elements:
  - **Source**
  - **Destination**

- **What is a SmartGroup?**

A SmartGroup identifies a group of resources that have similar policy requirements and are associated to the same *logical container*.

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

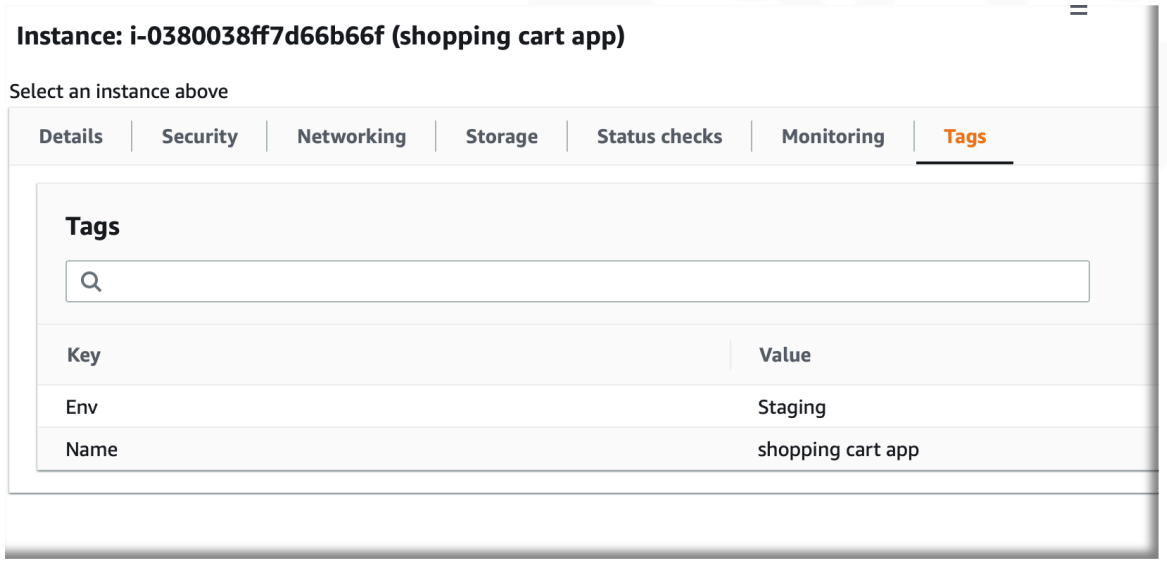
SmartGroups: Classification Methods

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}



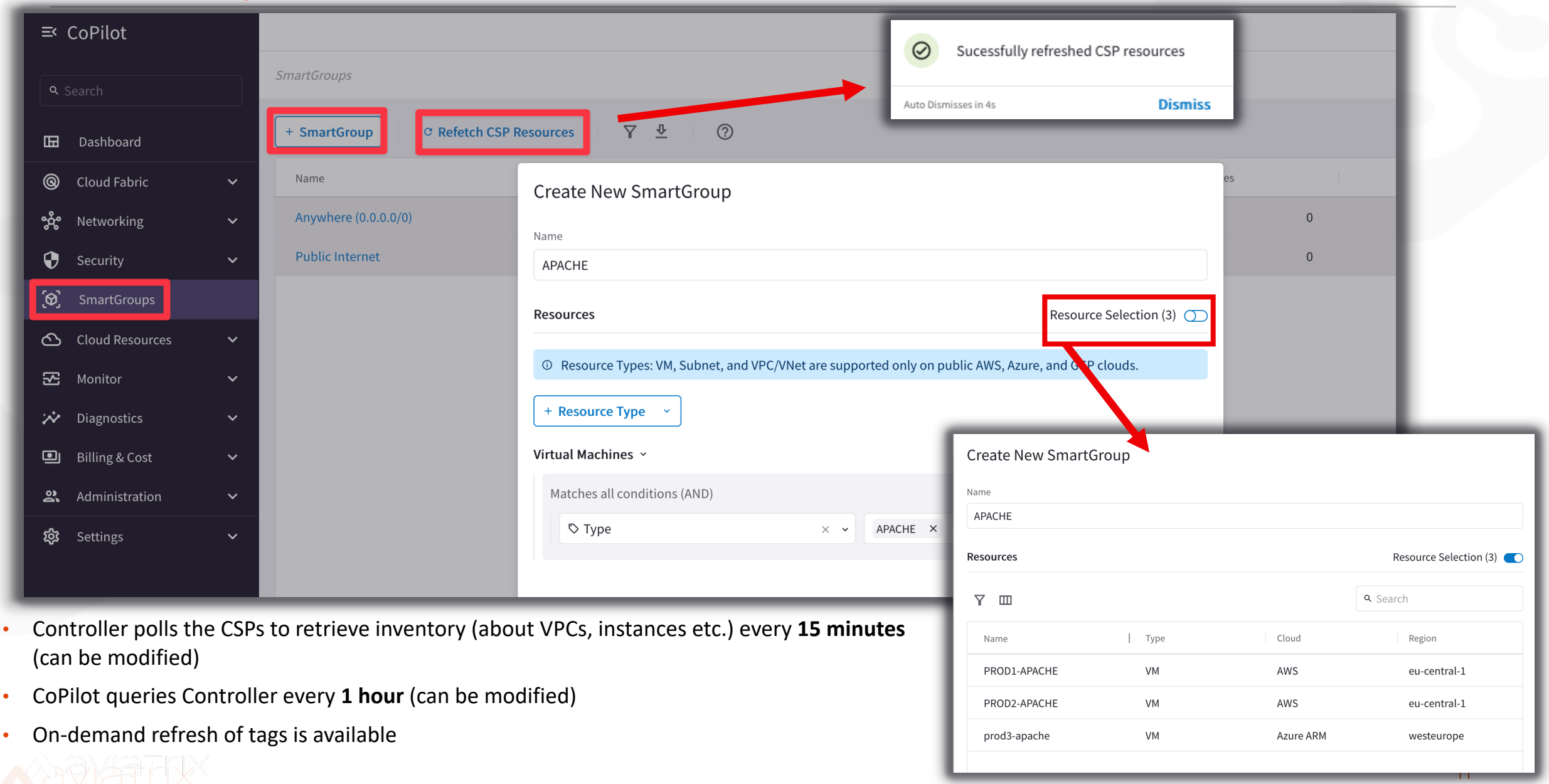
Resource attribute

- Region Name, Account Name

IP Prefixes

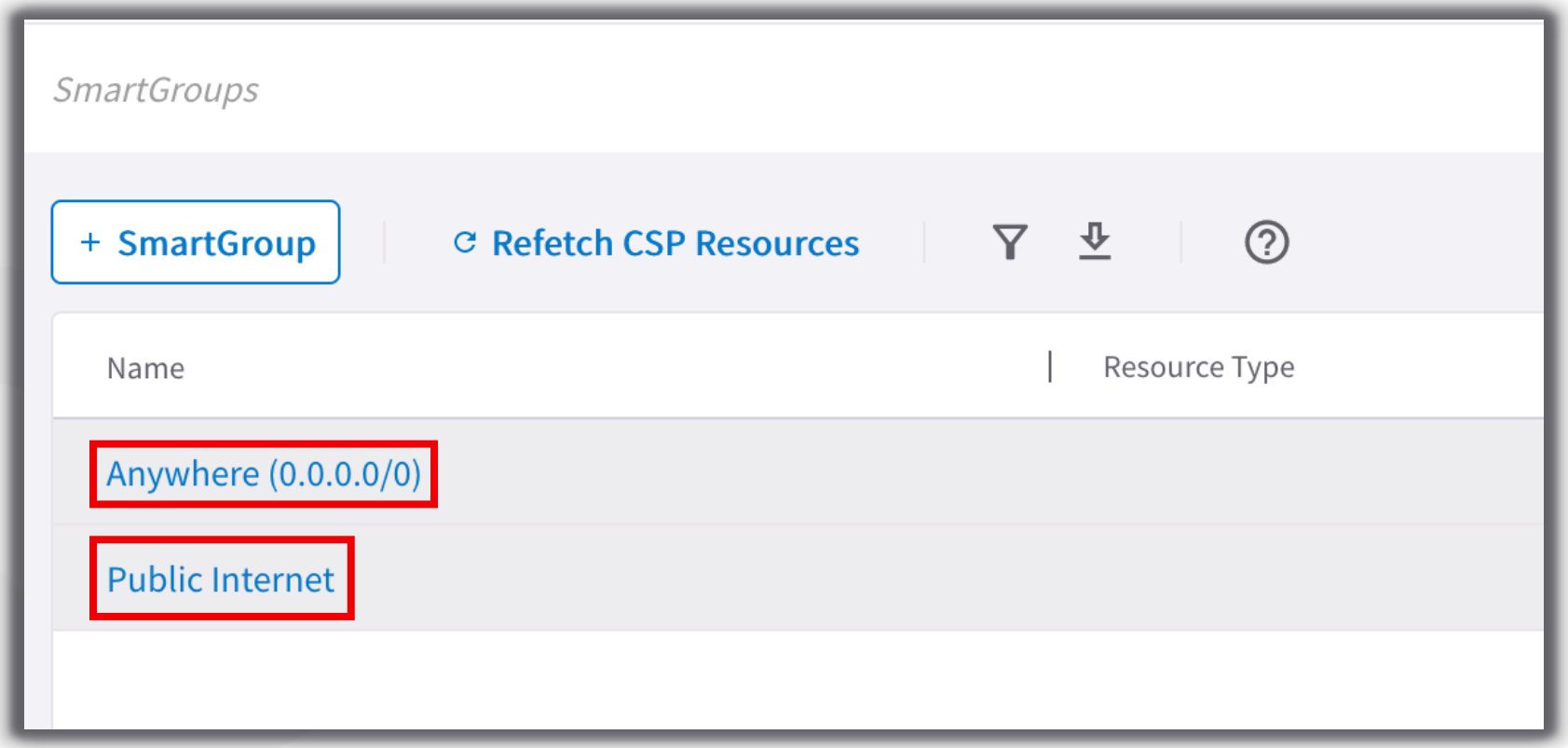
- CIDR

SmartGroups Creation



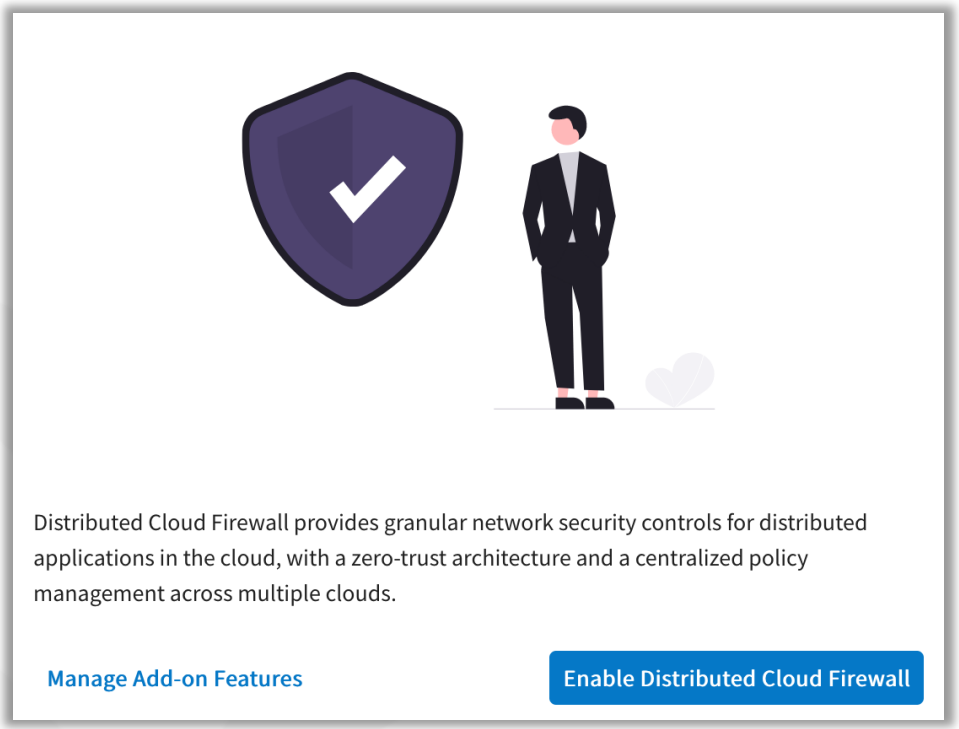
- Controller polls the CSPs to retrieve inventory (about VPCs, instances etc.) every **15 minutes** (can be modified)
- CoPilot queries Controller every **1 hour** (can be modified)
- On-demand refresh of tags is available

Pre-defined SmartGroups



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

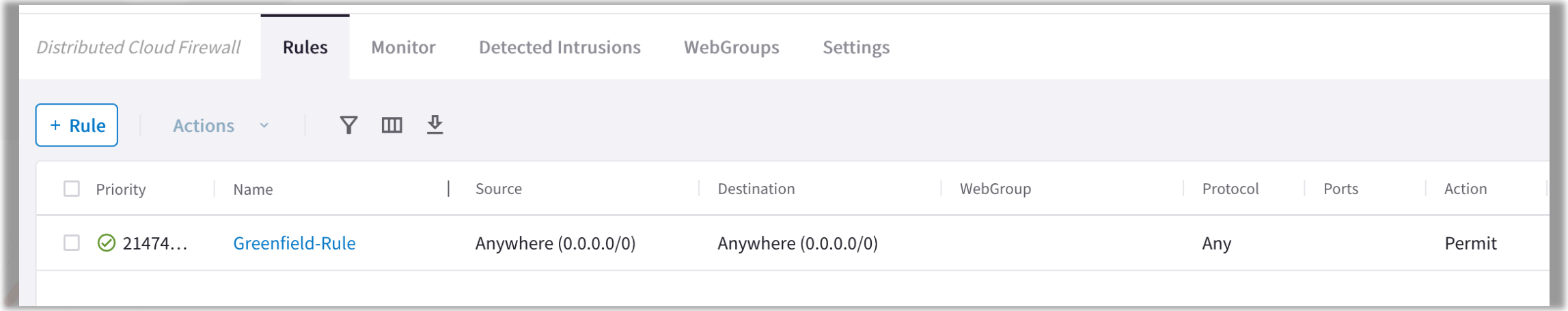
Enabling Distributed Cloud Firewall



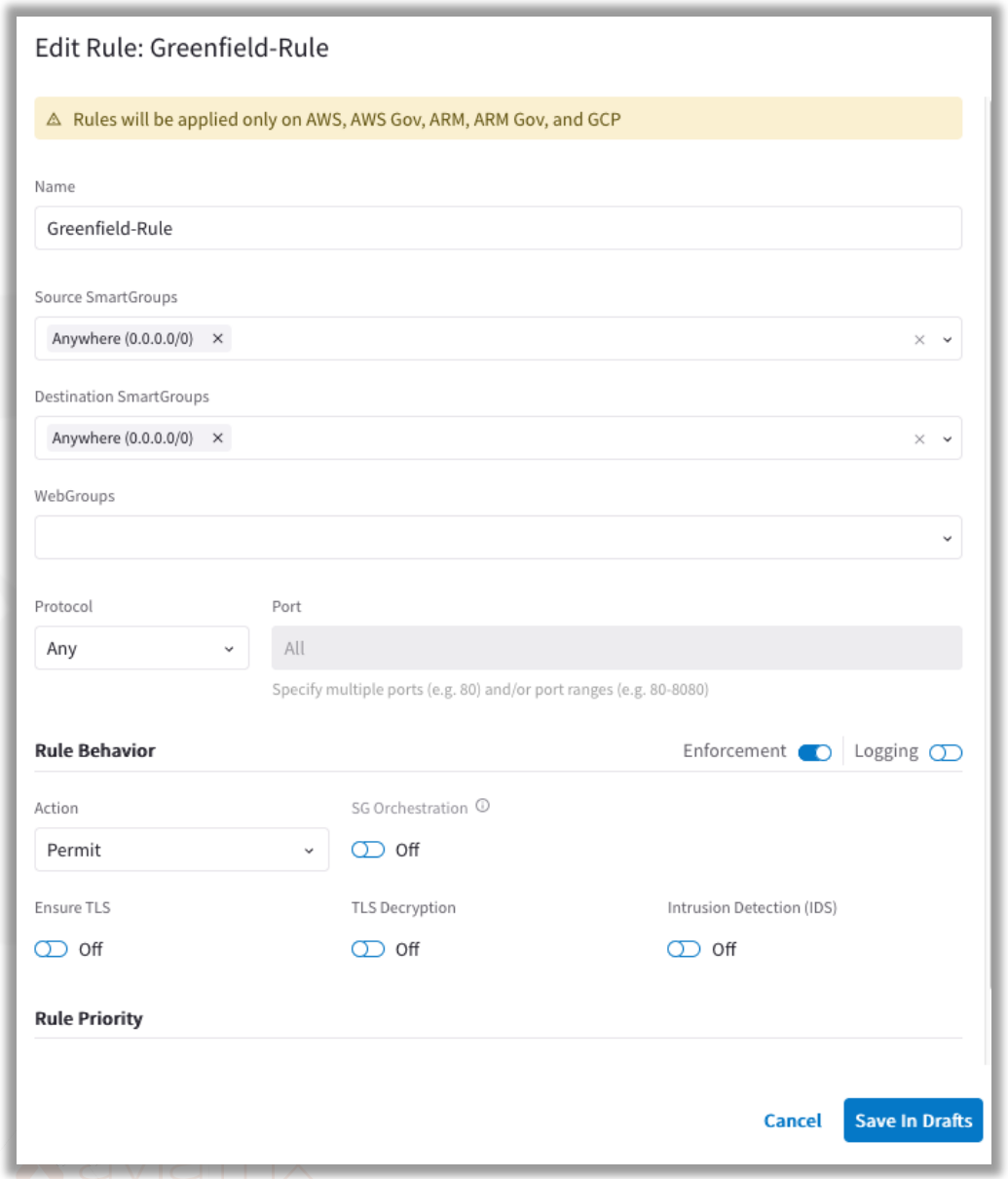
- Enabling the Distributed Cloud Firewall without configured rules will deny all previously permitted traffic due to its implicit Deny All rule.
- To maintain consistency, a **Greenfield Rule** will be created to allow traffic that maintains the current state, facilitating the creation of custom rules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

DENY LIST MODEL (THREAT-CENTRIC MODEL):

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

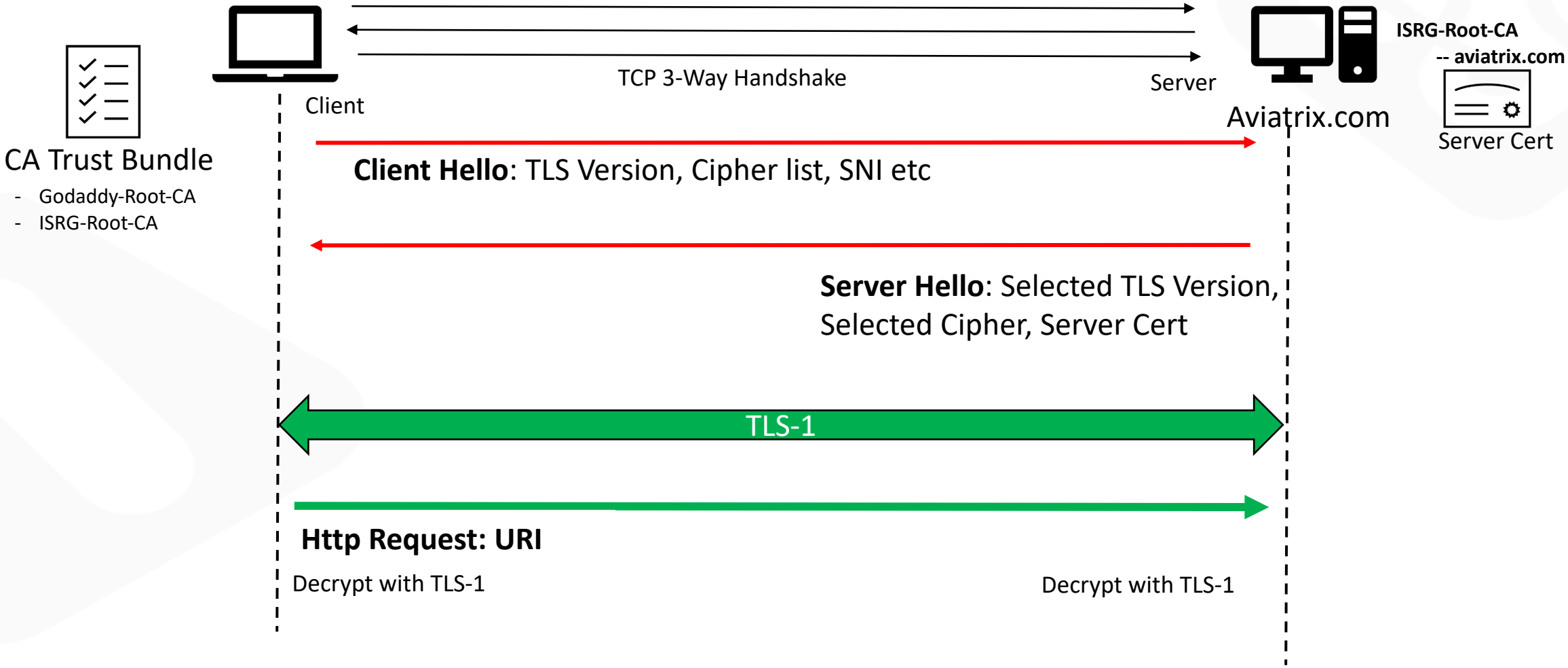


The Greenfield-Rule

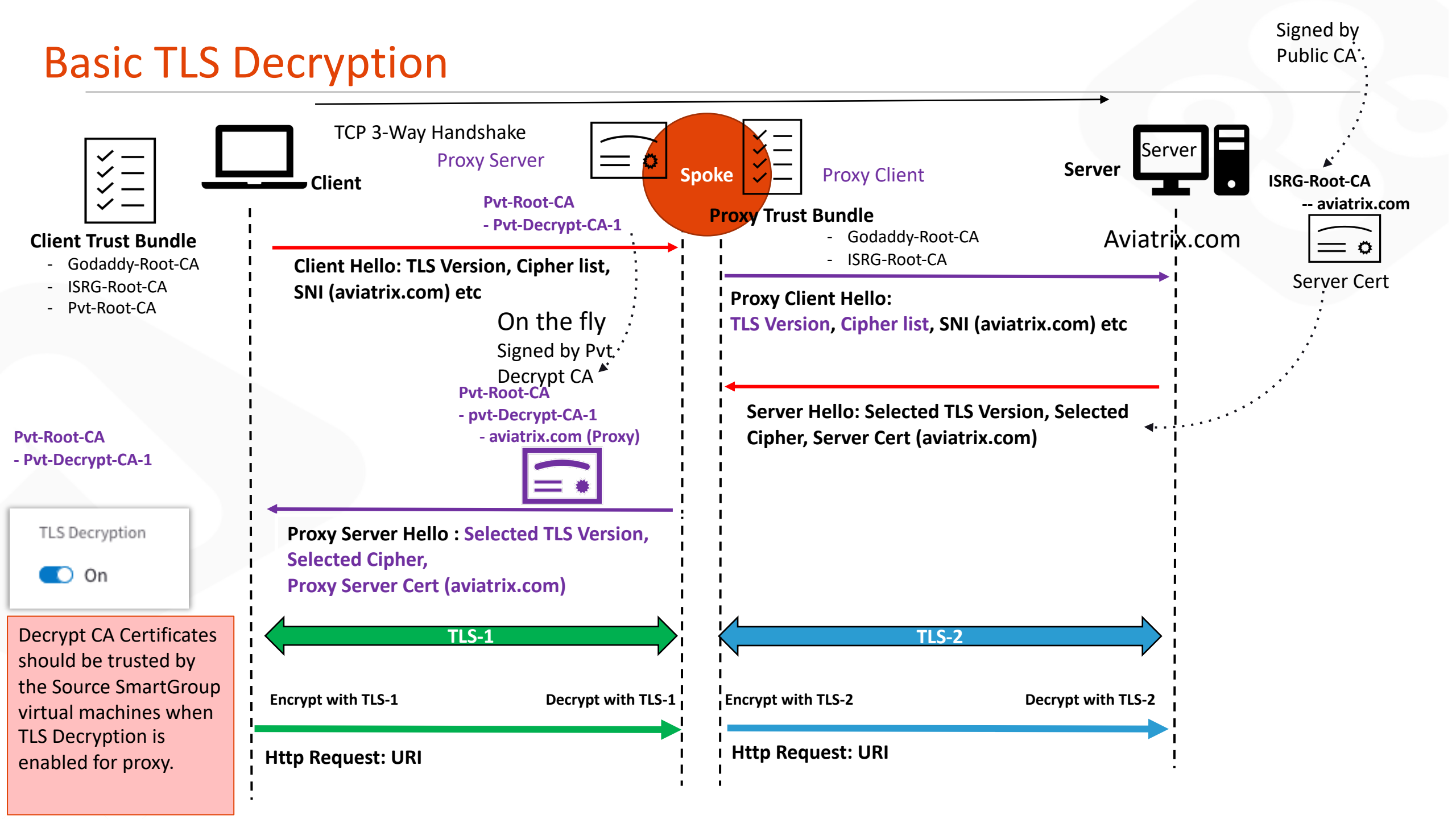


- **Source SmartGroups:** Anywhere(0.0.0.0/0)
- **Destination SmartGroups:** Anywhere(0.0.0.0/0)
- **Protocol:** Any
- **Action:** Permit
- Can be **edited** and **deleted**
- It can be **moved** when new rules are created like any other rules
- If it is the only rule present in the rules base, it is allocated above the implicit deny-all rule
- Customer would get an easy click button to create a greenfield rule, because by product design Zero trust is enforced with Deny-all at the end

Basic TLS Connection



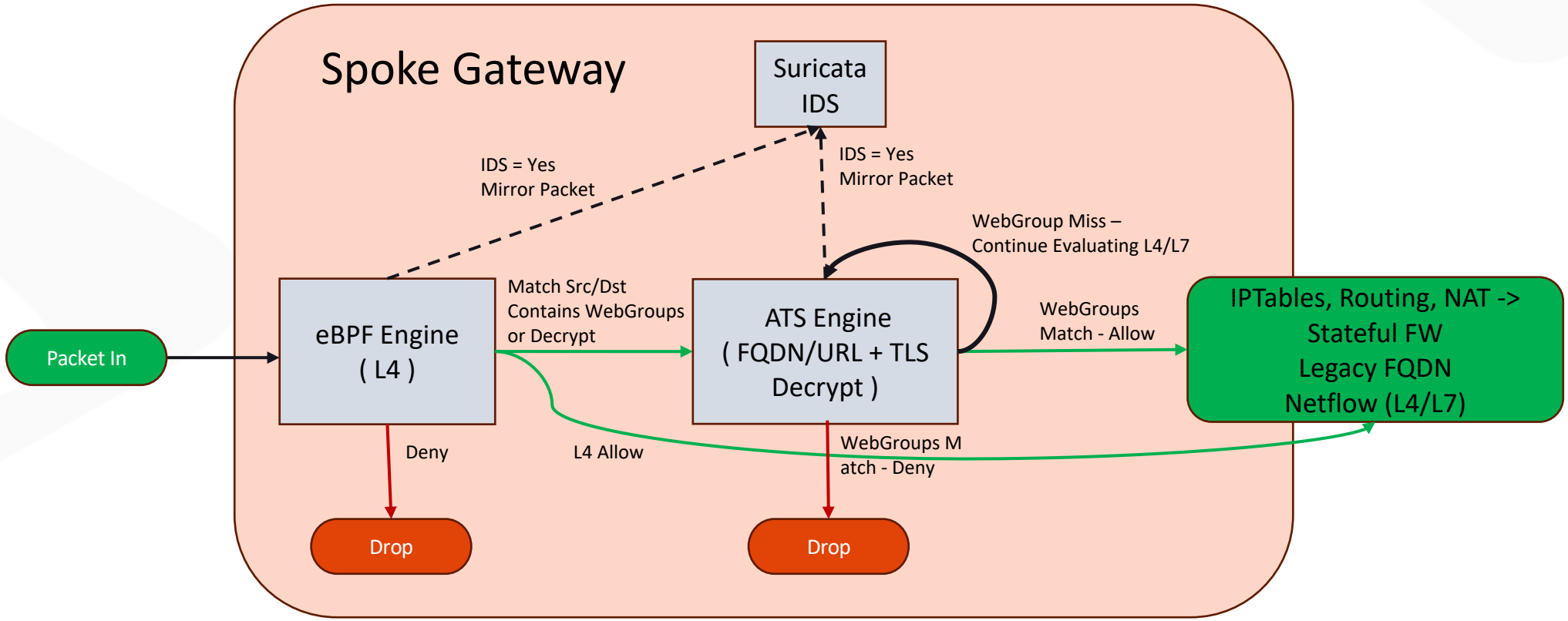
Basic TLS Decryption



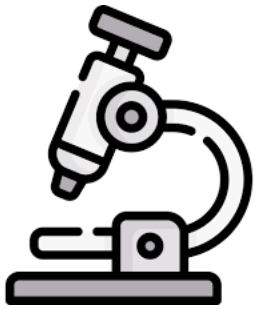
Decrypt CA Certificates should be trusted by the Source SmartGroup virtual machines when TLS Decryption is enabled for proxy.

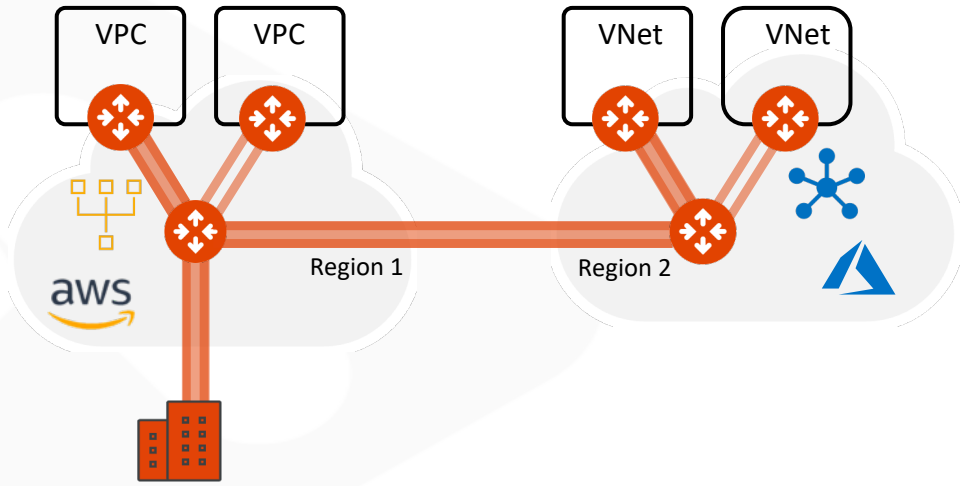
DFW Engines At-a-Glance

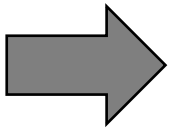
- **eBPF** (extended Berkeley Packet Filter) Engine (L4)
- WebProxy **ATS** (Apache Traffic Server) Engine (L7)
- **Suricata** Engine (DPI)

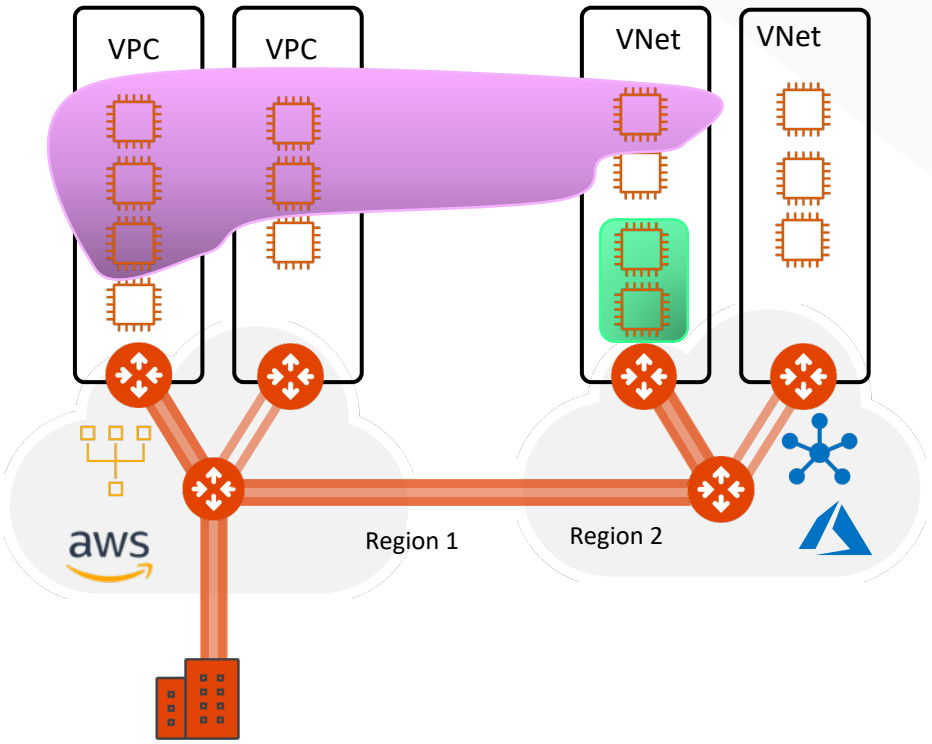


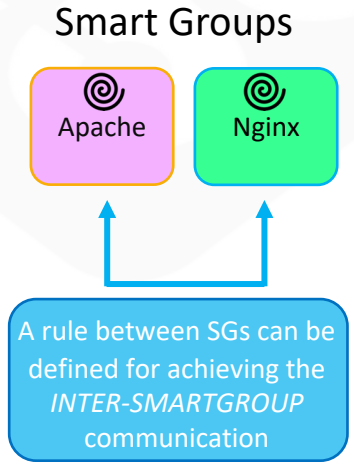
Distributed Cloud Firewall Rule Types: Intra-rule vs. Inter-rule









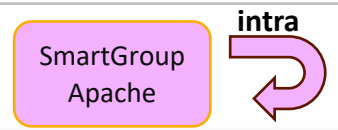


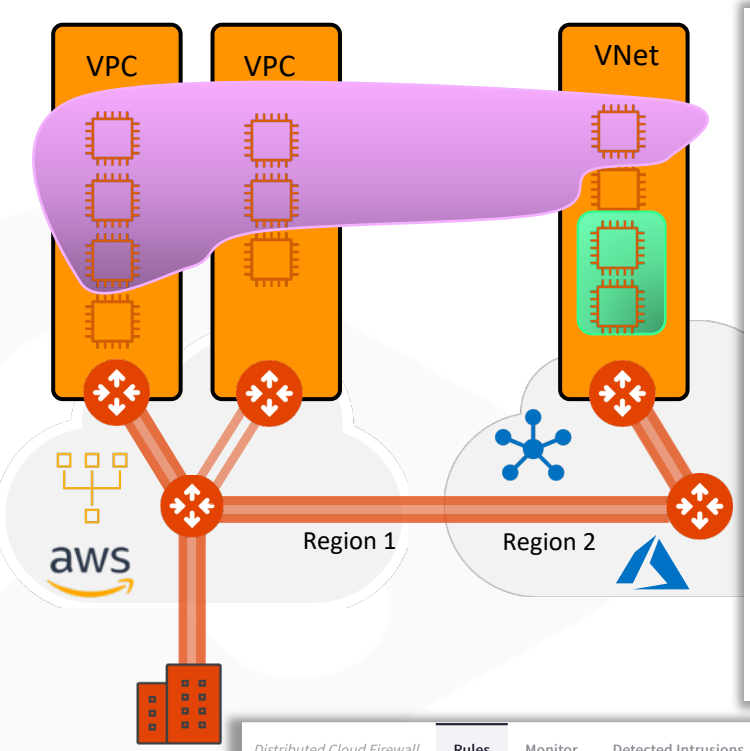
- **INTRA-RULE**: is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

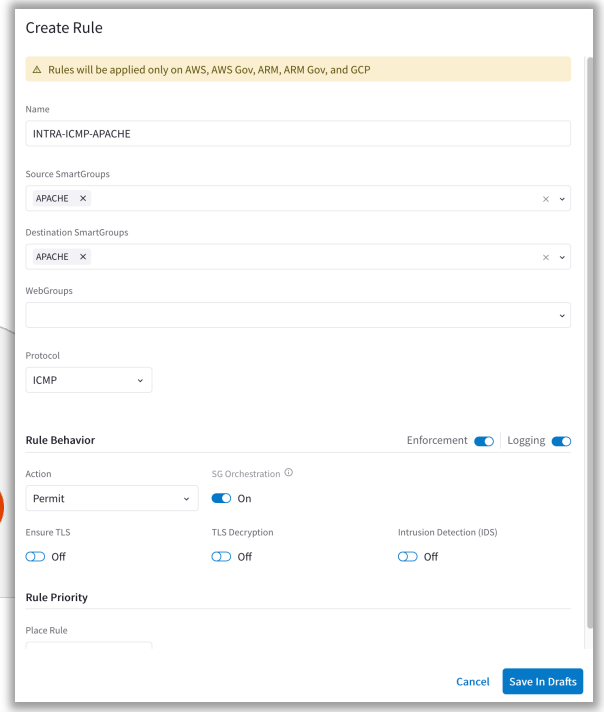
- **INTER-RULE:** is defined among Smart Groups, for dictating what kind of traffic is allowed/prohibited among two or more Smart Groups.

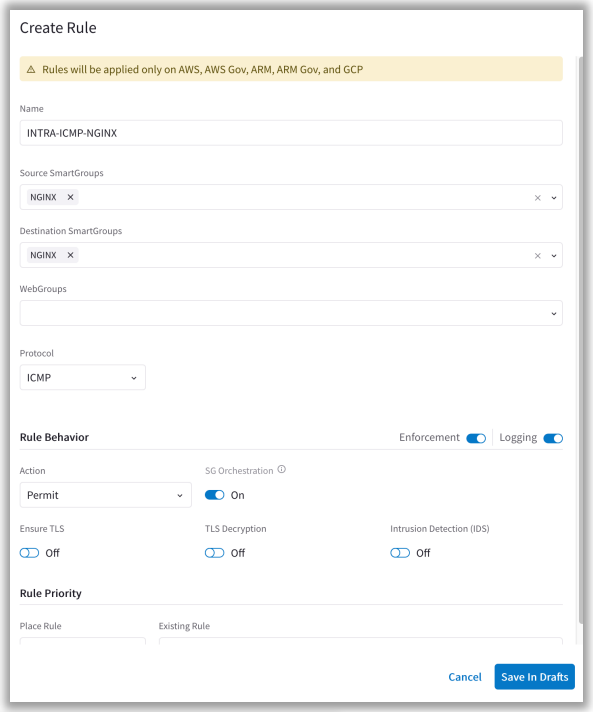
Aviatrix DCF: Intra and Inter Rules - Examples

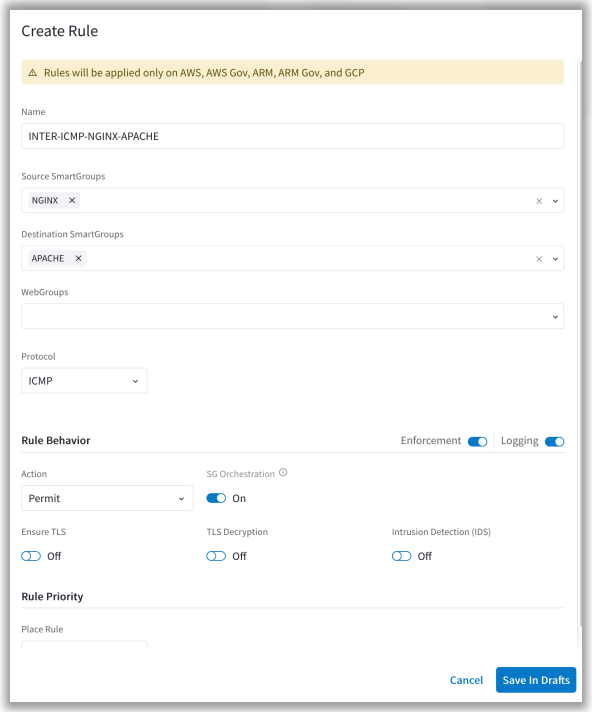
ALLOW LIST MODEL (TRUST-CENTRIC MODEL) → ZTN approach:
- ❑deny everything and only permit what you explicitly allow.

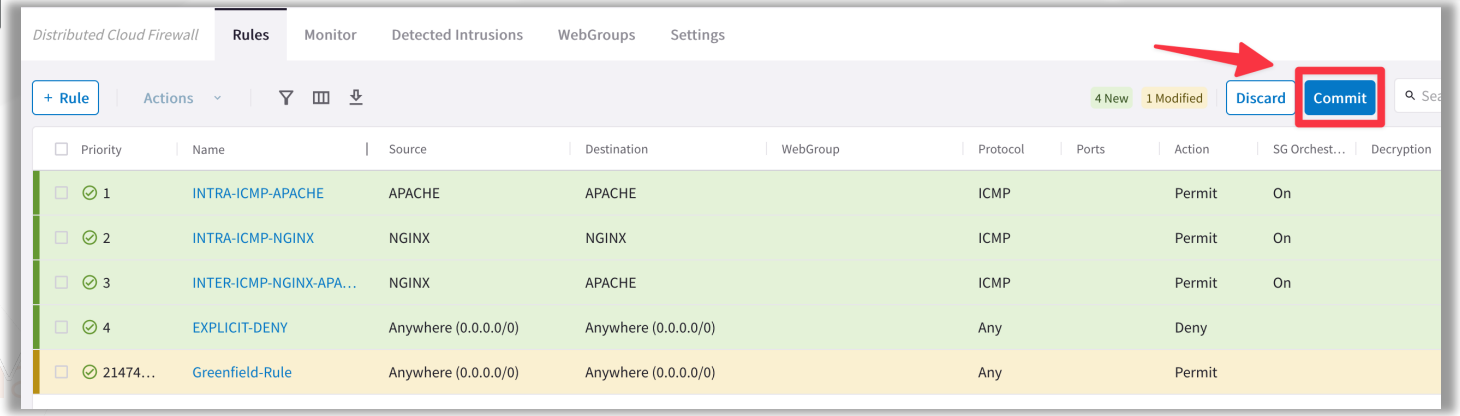






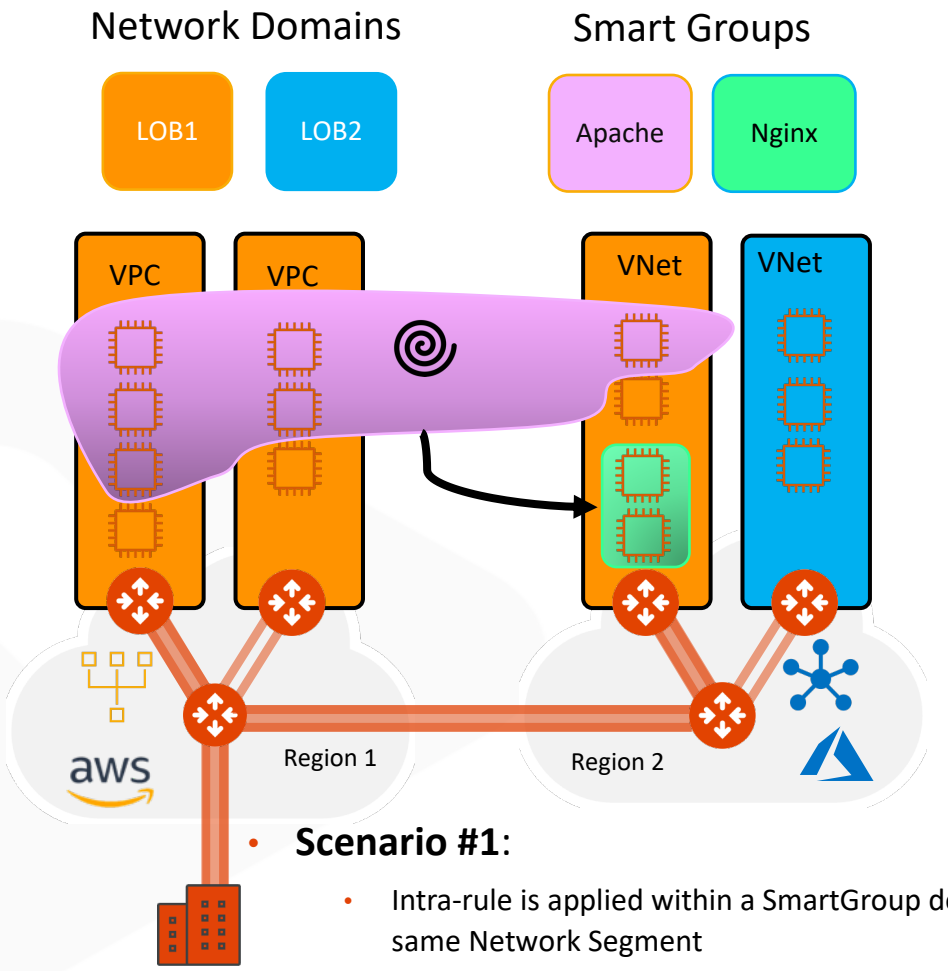




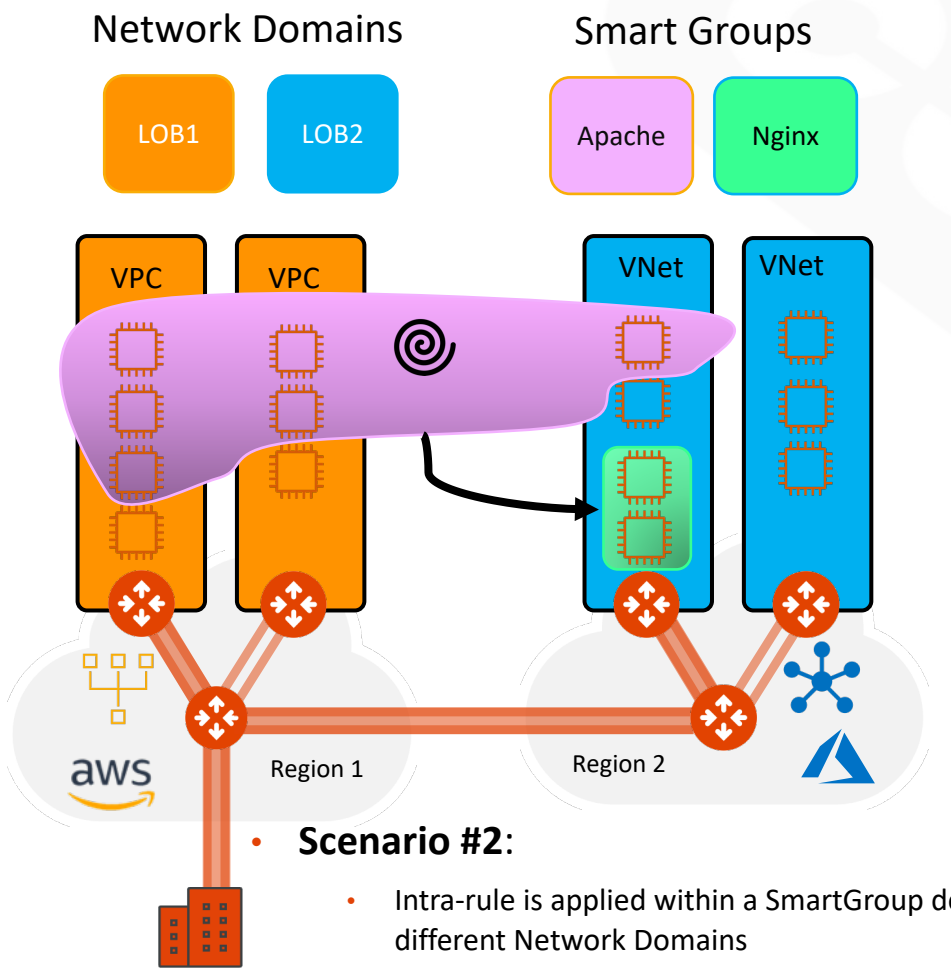


- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return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

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



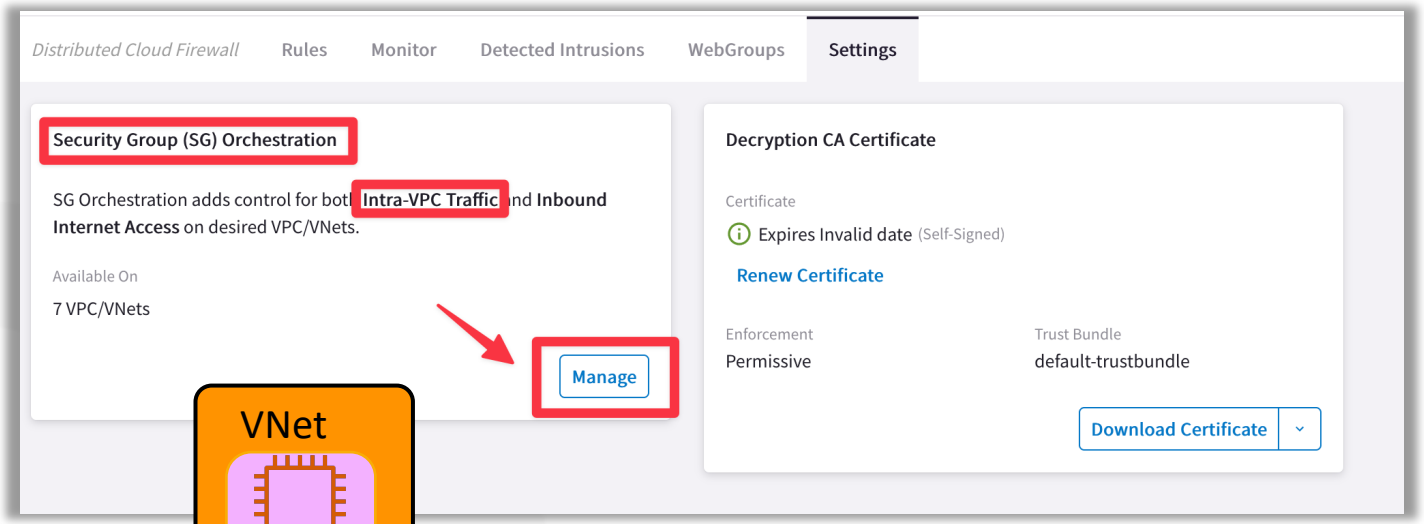
- **Scenario #2**:
  - Intra-rule is applied within a SmartGroup defined across two different Network Domains
  - Inter-rule is applied between SmartGroups defined across two different network Domains

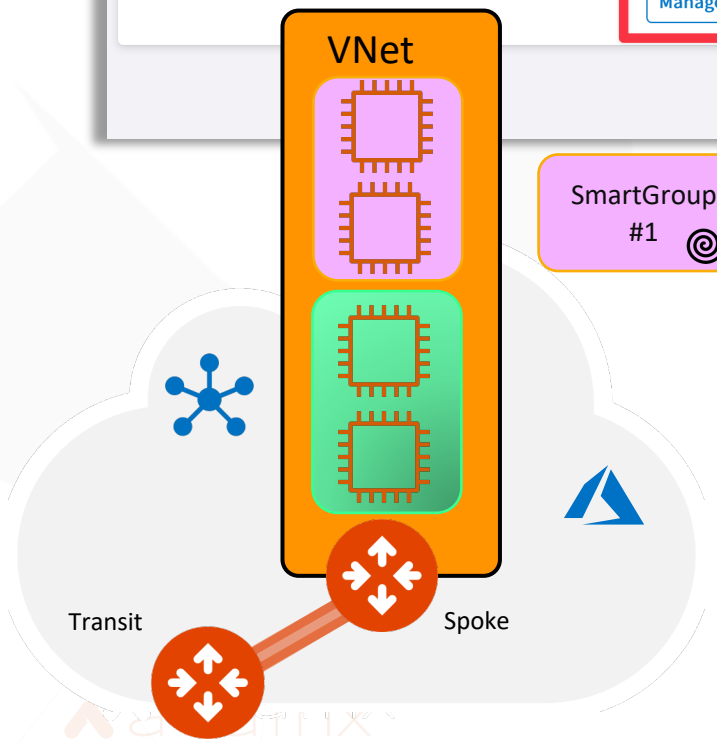
Caveat:

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

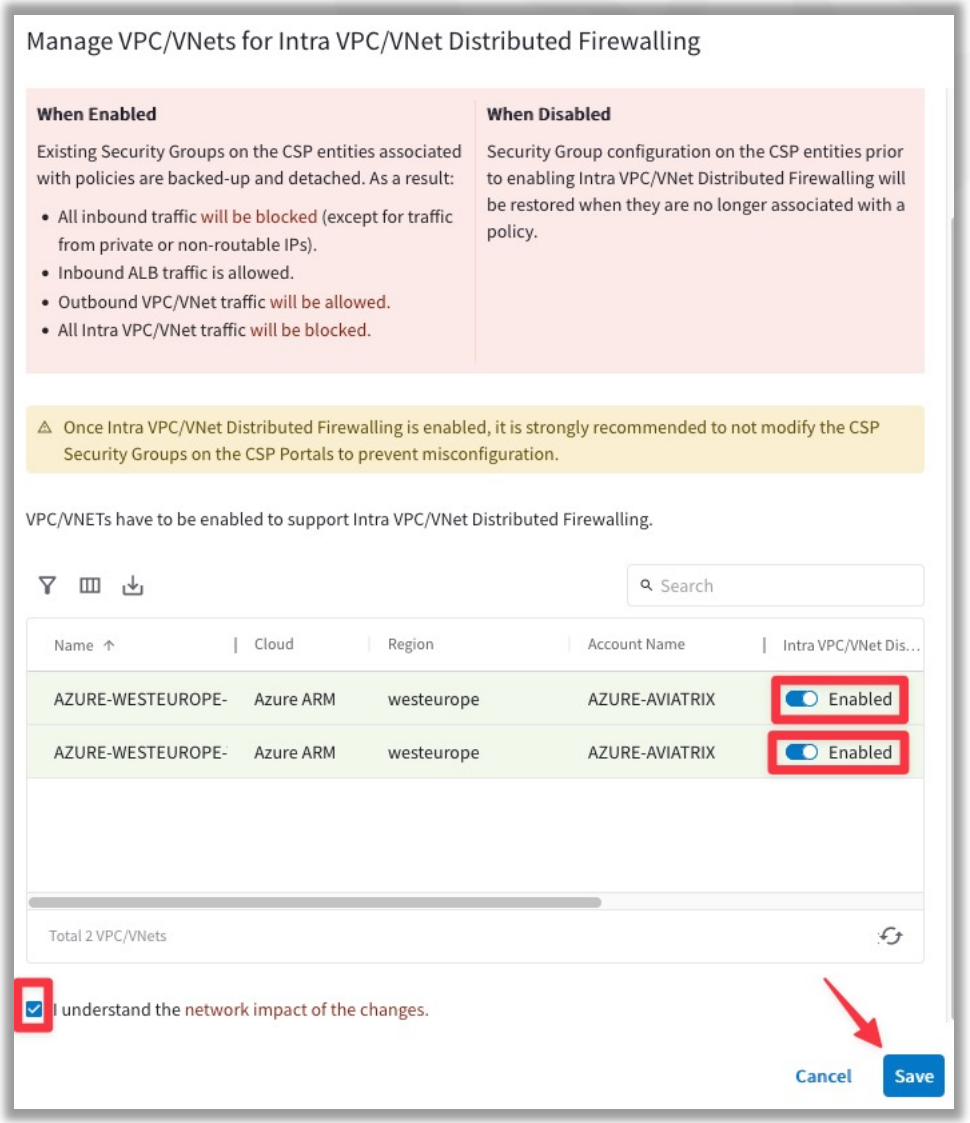
Intra VPC/VNET Distributed Firewalling (available on AWS/Azure)

❑ Enable the feature on the relevant VPC/VNet

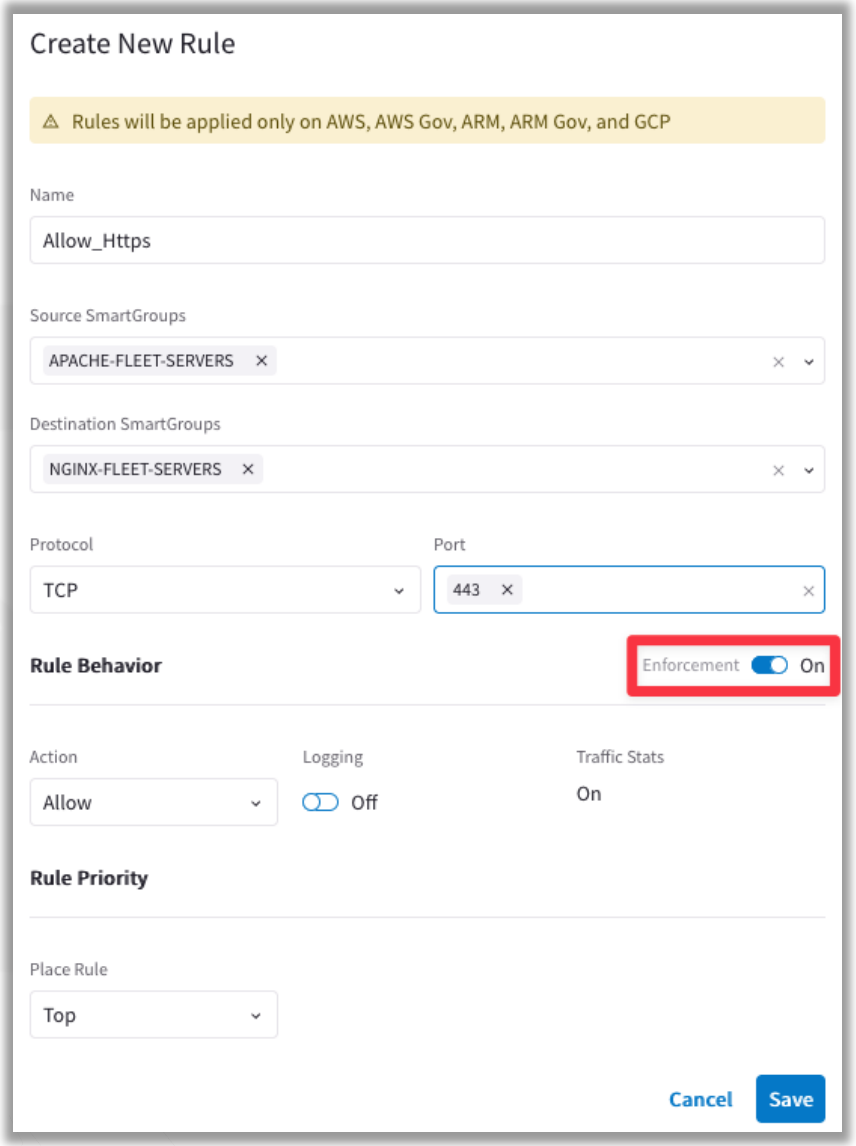




- If you enable the Security Group orchestration (*aka Intra-VPC Traffic Control*), the SmartGroups will not be able to communicate with each other unless an inter rule is applied between them.
- This is pure L4 separation using the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.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



Rule Enforcement



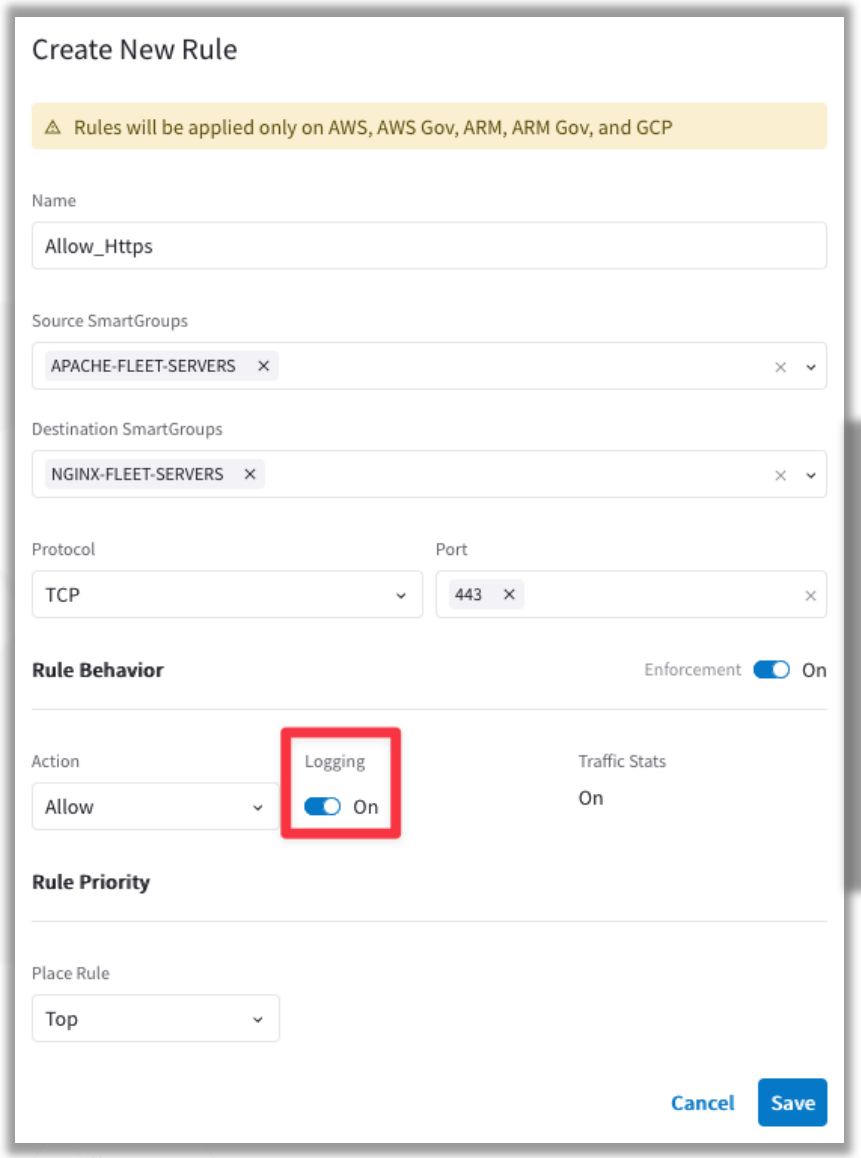
Enforcement ON

- Policy is enforced in the Data Plane

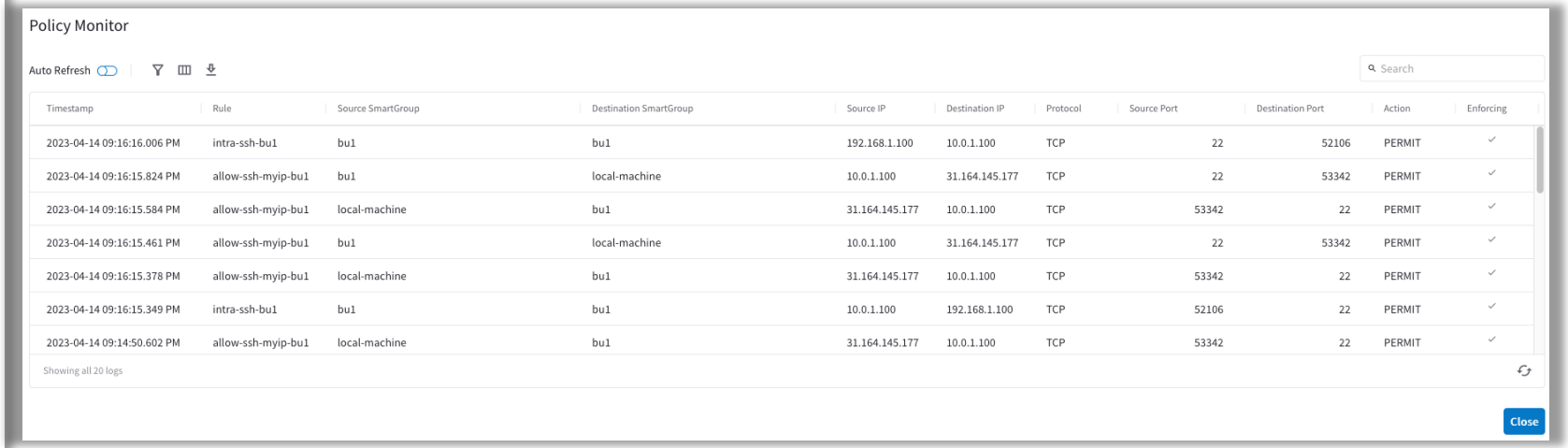
Enforcement OFF

- 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**



Next: Lab 10 – Distributed Cloud Firewall