Micro-Segmentation

Aviatrix DCF for Intra VPC/VNET Micro-Segmentation

Micro-Segmentation Basics

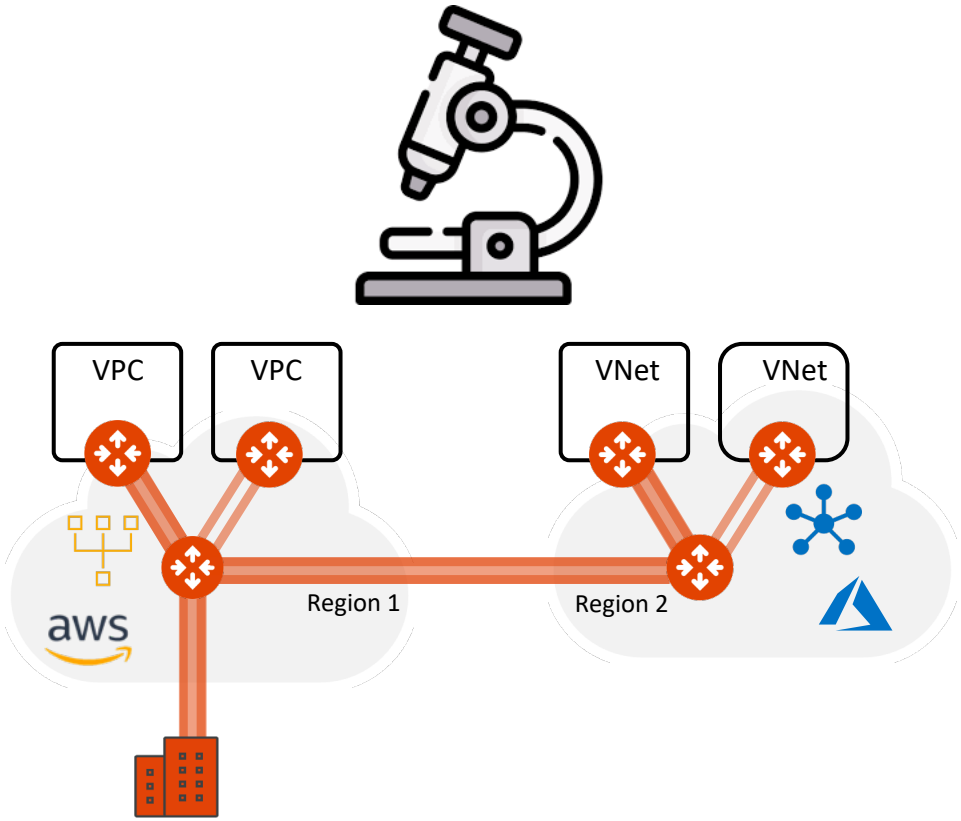
Aviatrix Distributed Cloud Firewall enforces policy exactly where needed across the entire network.

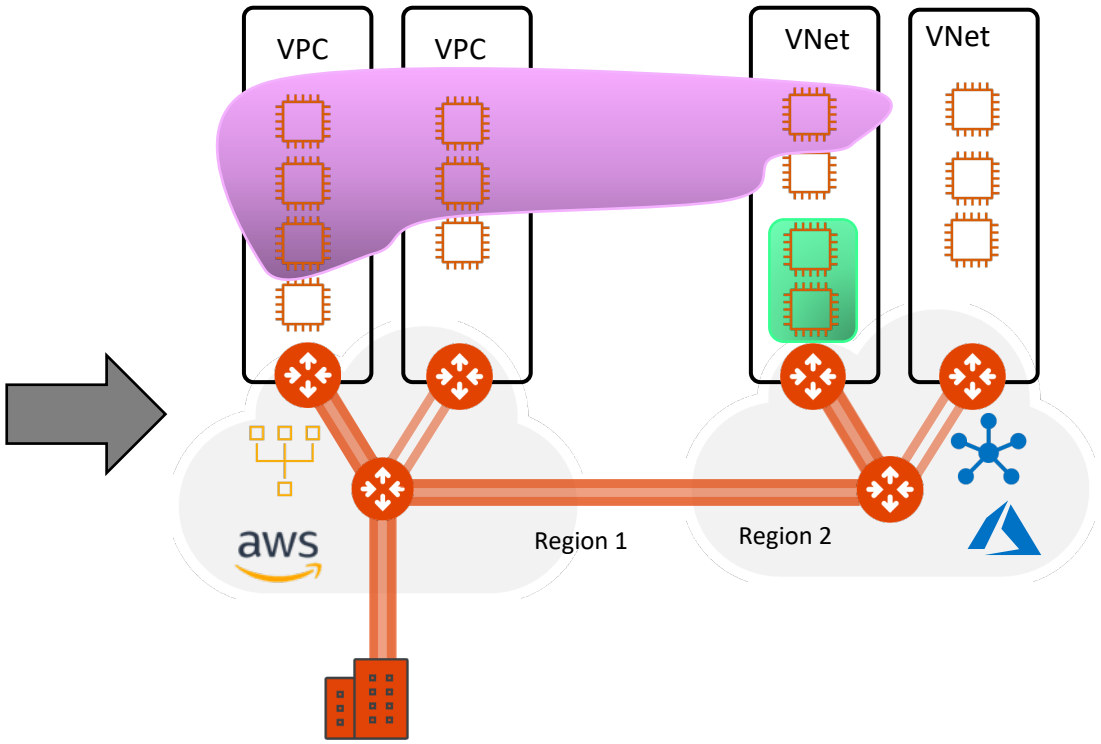
Aviatrix DCF for Micro-Segmentation is for Intra and Inter VPC/VNET Segmentation

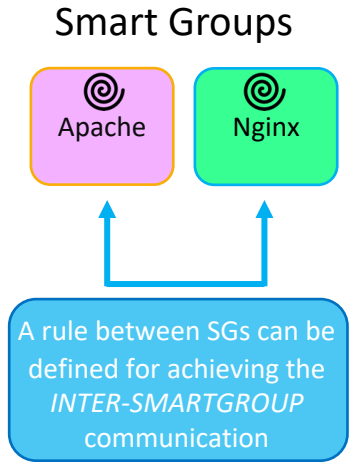
Characteristics:

- Two components: Smart Groups & Policy (Rule)
- Available for AWS and Azure
- Fine-grained control, even for workloads in the same VPC/VNET
  - Orchestrating AWS Security Groups and Azure Network Security Group (NSG) for Intra-VPC or Intra-VNET segmentation

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



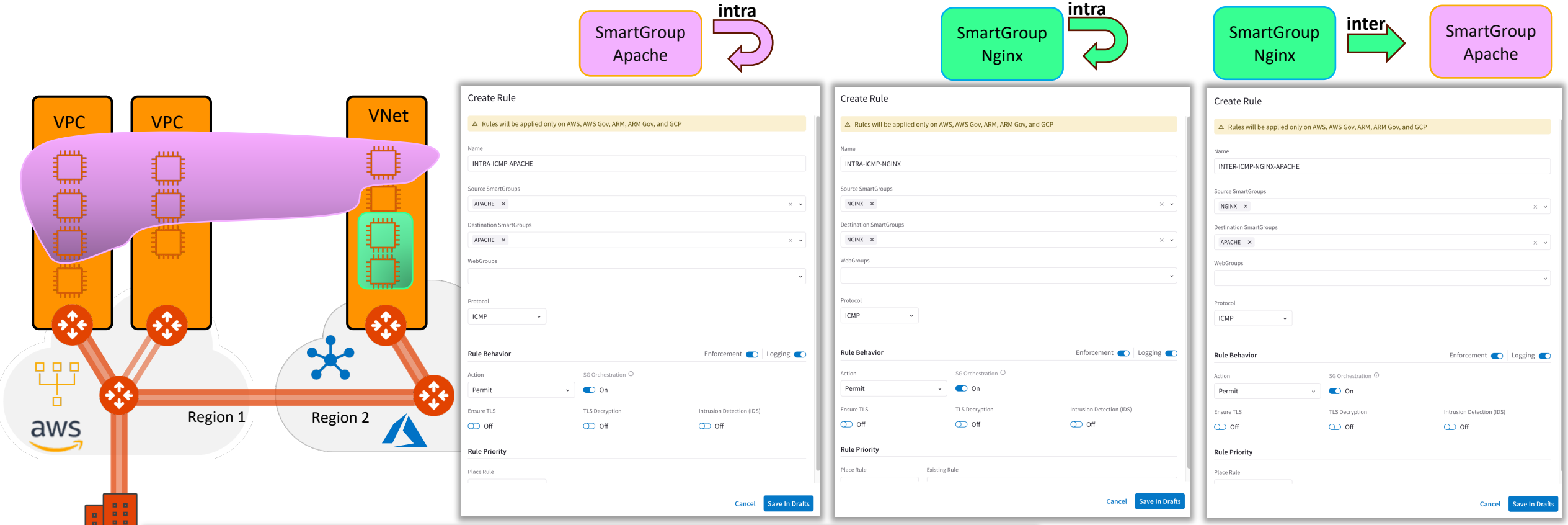


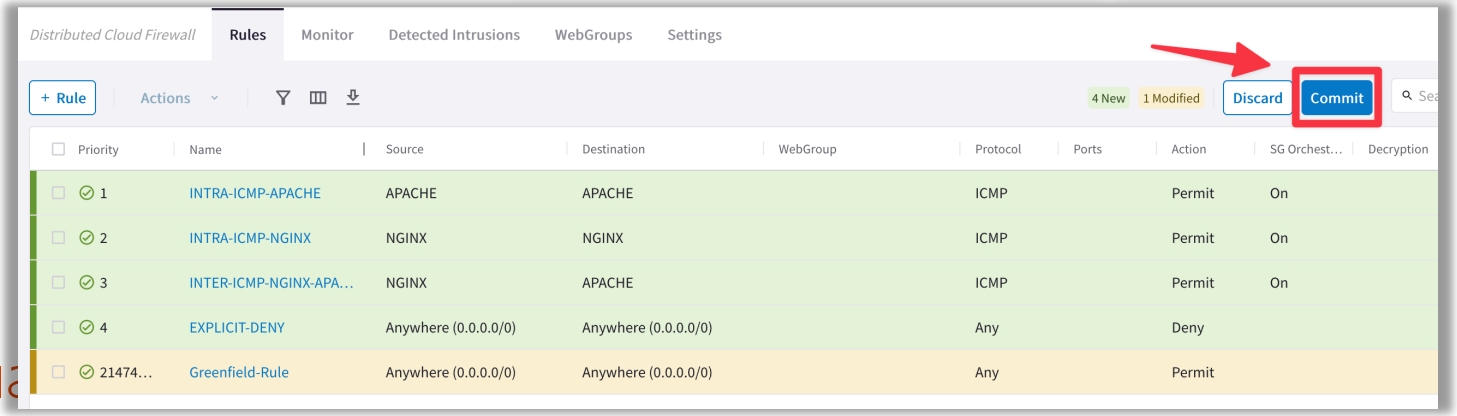


- **INTRA-RULE**: is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

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

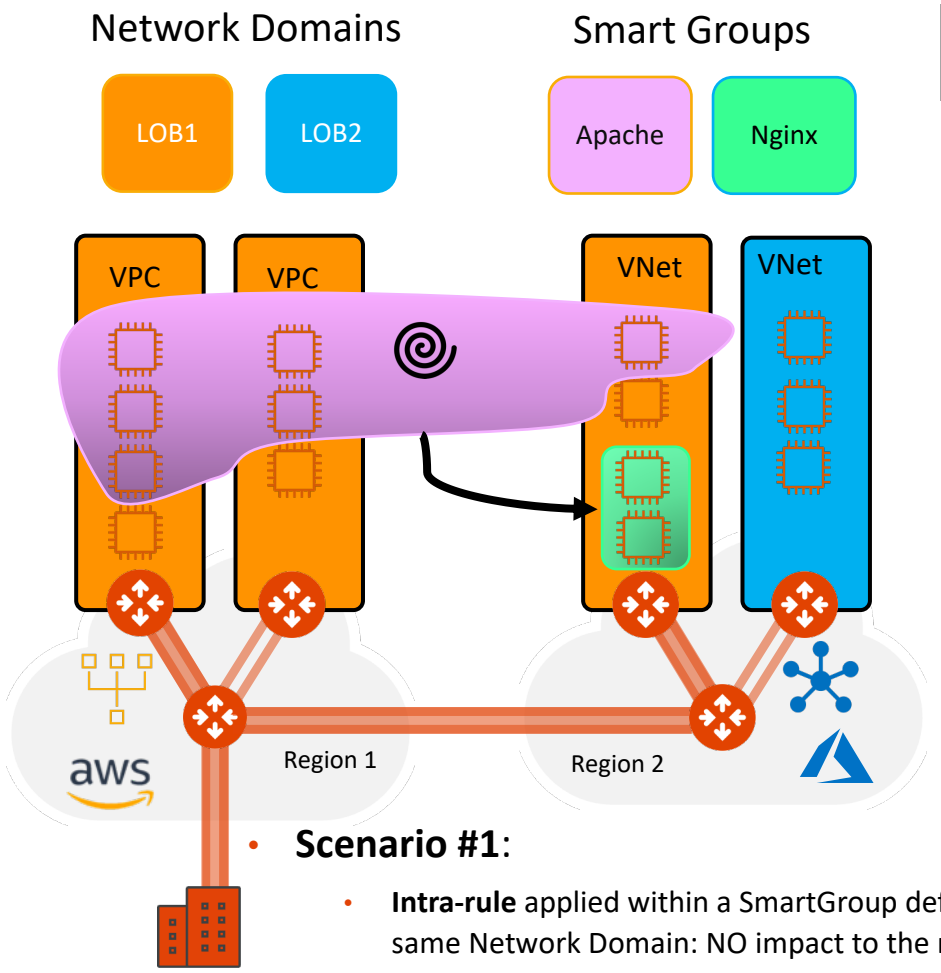
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules



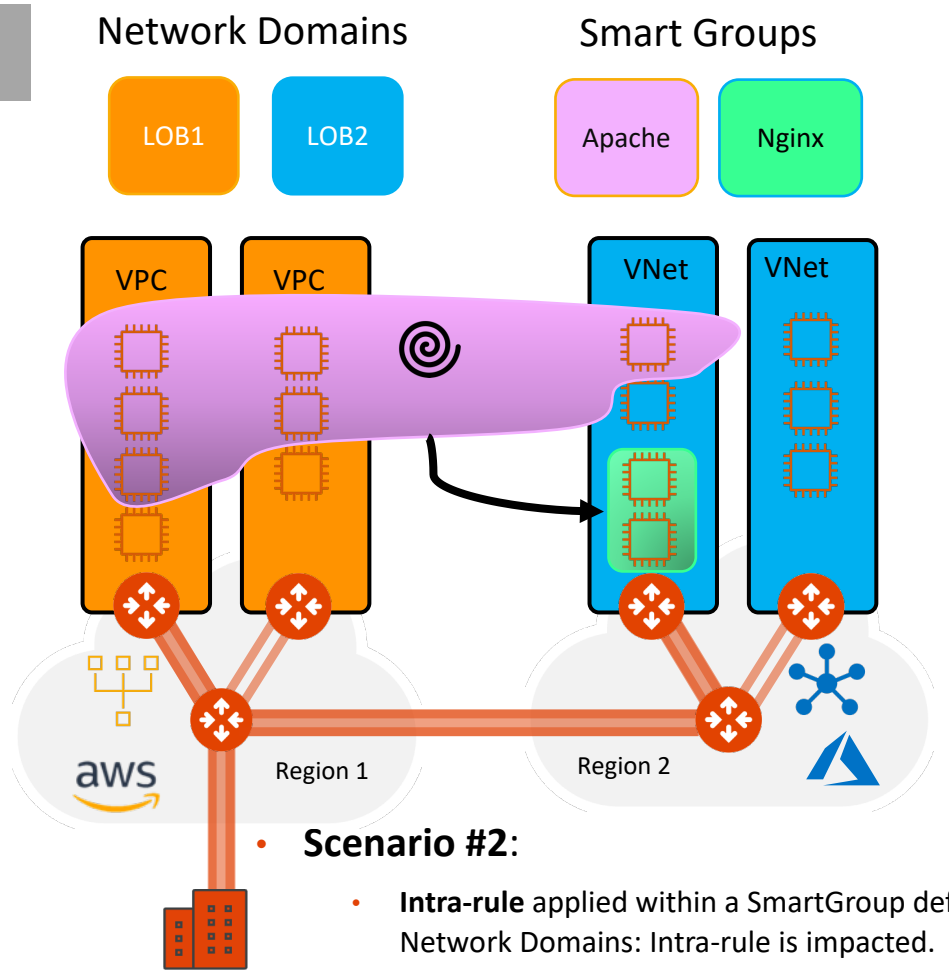


- **Micro-Segmentation**: Combination of SmartGroups and DCF Rules
- Rule changes are saved in **Draft** state.
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash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

Network Segmentation & Distributed Cloud Firewall Rule together



NO connection policy is applied



- **Scenario #1**:
  - **Intra-rule** applied within a SmartGroup defined within the same Network Domain: NO impact to the rule
  - **Inter-rule** applied between SmartGroups defined within the same Network Domains: NO impact to the rule

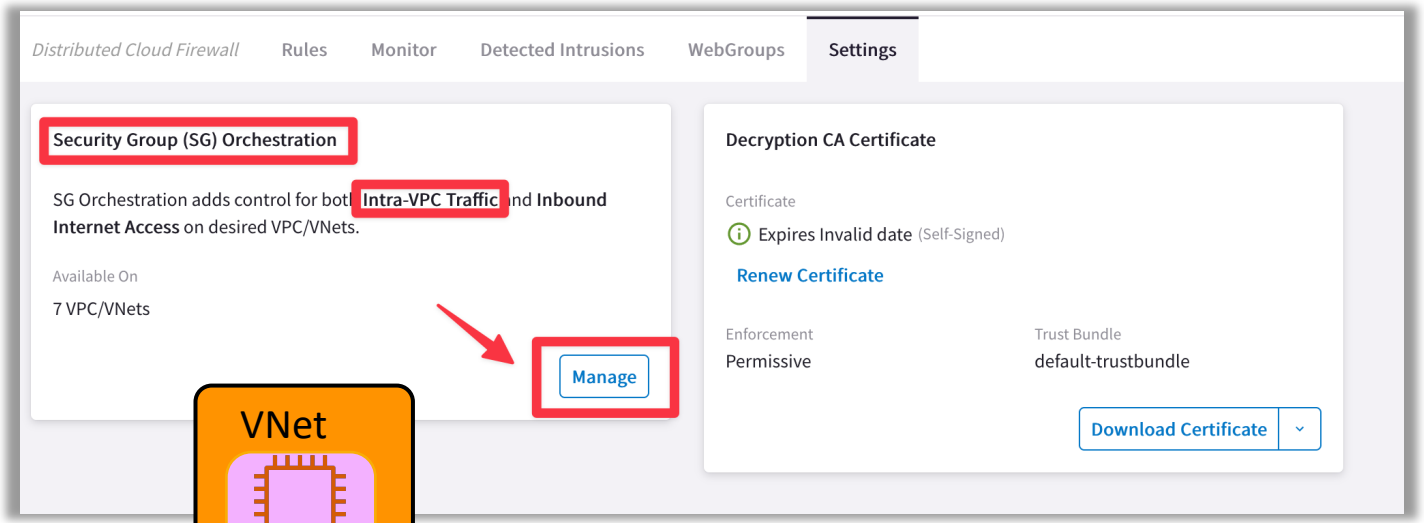
- **Scenario #2**:
  - **Intra-rule** applied within a SmartGroup defined across two Network Domains: Intra-rule is impacted.
  - **Inter-rule** is applied between SmartGroups defined across two different Network Domains: Inter-rule is impacted

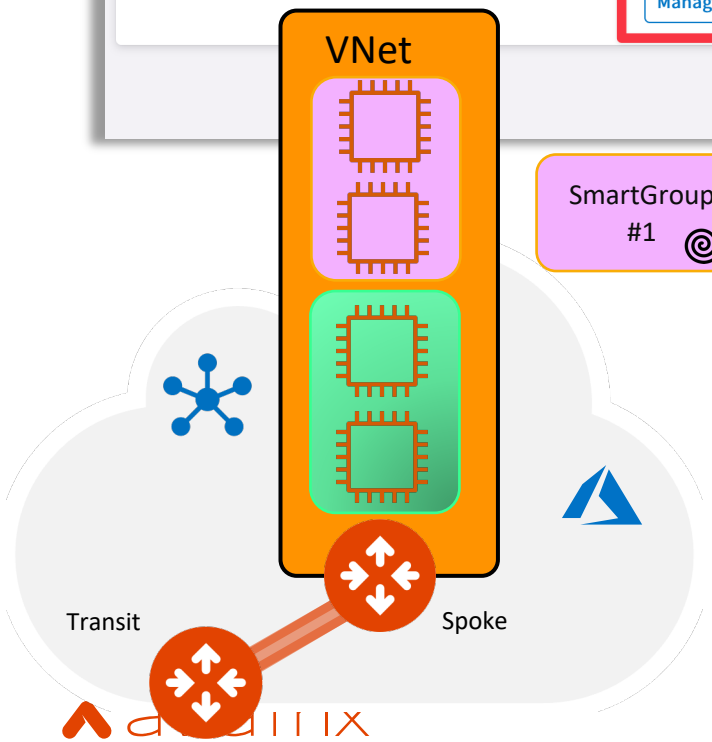
Caveat:

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

Security Group (SG) Orchestration: Intra VPC/VNET Traffic Control

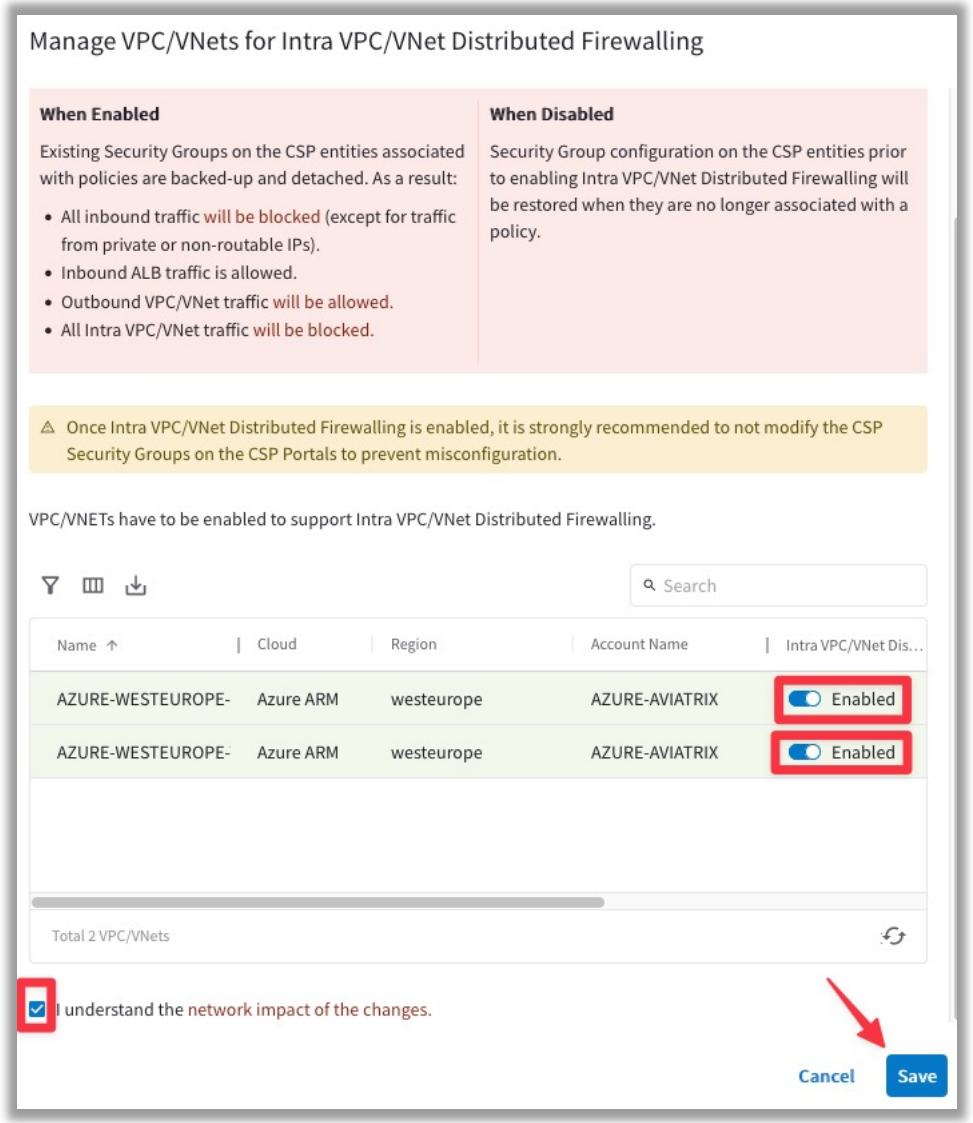
❑ Enable the feature on the relevant VPC/VNet





- If you enable the **Security Group (SG) Orchestration** (*aka Intra-VPC Traffic Control*), the SmartGroups defined within the same VPC/VNet will not be able to communicate with each other, unless an inter rule is applied between them.
- This is pure L4 separation, leveraging the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.

CAVEAT: Available in AWS/Azure



aviatrix

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com