Micro-Segmentation

AVIATRIX DCF FOR INTRA VPC/VNET MICRO-SEGMENTATION

Micro-Segmentation Basics

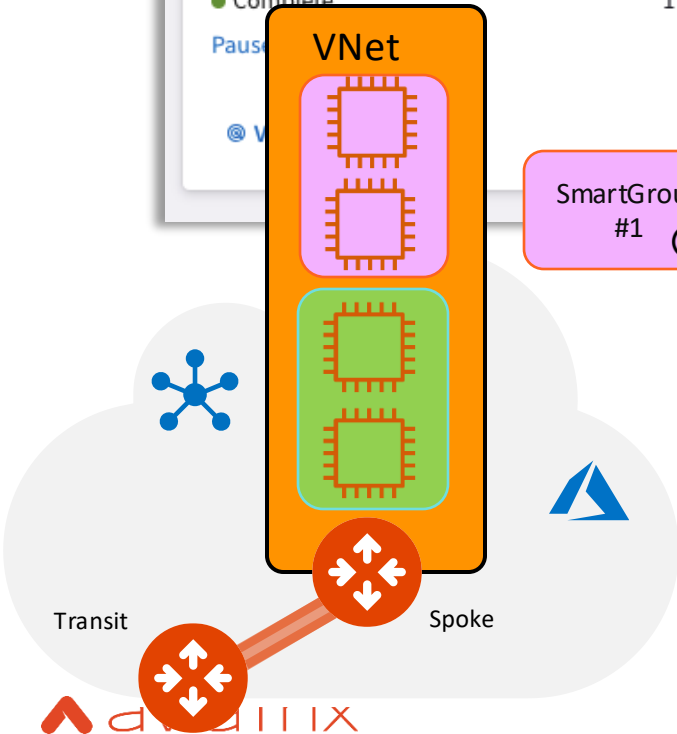**Aviatrix Distributed Cloud Firewall enforces policy exactly where needed across the entire network.**
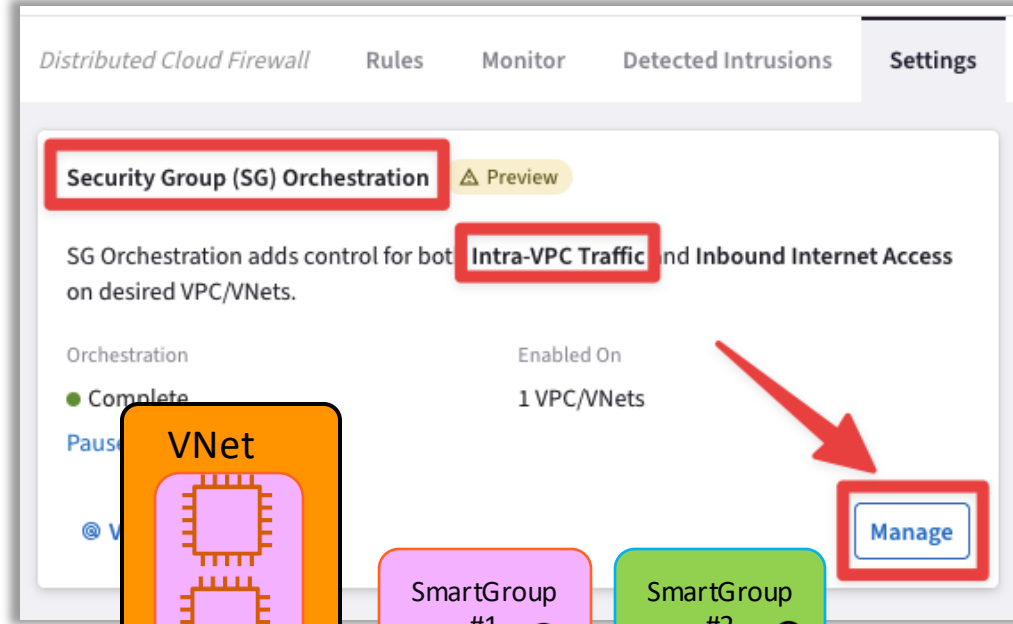
Aviatrix DCF for Micro-Segmentation is for Intra and Inter VPC/VNET Segmentation

Characteristics:

- Two components: Smart Groups & Policy (Rule)

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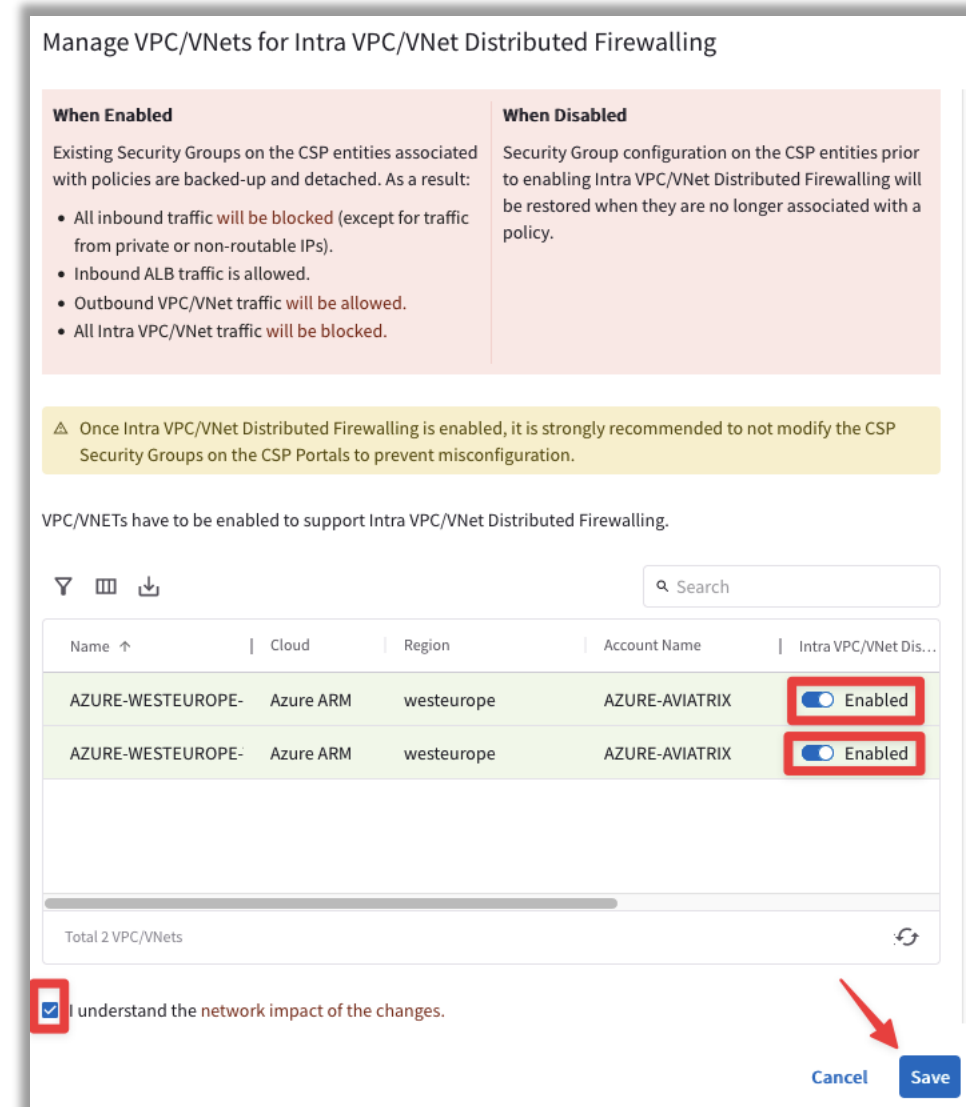
Security Group (SG) Orchestration: Intra VPC/VNET Traffic Control

❑ **Enable the feature on the relevant VPC/VNet**

Distributed Cloud Firewall | Rules | Monitor | Detected Intrusions | **Settings**

Security Group (SG) Orchestration ⚠ Preview

SG Orchestration adds control for both **Intra-VPC Traffic** and Inbound Internet Access on desired VPC/VNets.

Orchestration | Enabled On
● Complete | 1 VPC/VNets

VNet

SmartGroup #1

SmartGroup #2

Manage

Transit — Spoke

- 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

Manage VPC/VNets for Intra VPC/VNet Distributed Firewalling

When Enabled	**When Disabled**
Existing Security Groups on the CSP entities associated with policies are backed-up and detached. As a result: • All inbound traffic will be blocked (except for traffic from private or non-routable IPs). • Inbound ALB traffic is allowed. • Outbound VPC/VNet traffic will be allowed. • All Intra VPC/VNet traffic will be blocked.	Security Group configuration on the CSP entities prior to enabling Intra VPC/VNet Distributed Firewalling will be restored when they are no longer associated with a policy.

⚠ Once Intra VPC/VNet Distributed Firewalling is enabled, it is strongly recommended to not modify the CSP Security Groups on the CSP Portals to prevent misconfiguration.

VPC/VNETs have to be enabled to support Intra VPC/VNet Distributed Firewalling.

🔍 Search

Name ↑	Cloud	Region	Account Name	Intra VPC/VNet Dis...
AZURE-WESTEUROPE-	Azure ARM	westeurope	AZURE-AVIATRIX	🔵 Enabled
AZURE-WESTEUROPE-	Azure ARM	westeurope	AZURE-AVIATRIX	🔵 Enabled

Total 2 VPC/VNets

☑ I understand the network impact of the changes.

Cancel | **Save**

Next: ThreatIQ and Anomaly Detection