Micro-Segmentation

AVIATRIX DCF FOR INTRA VPC/VNET MICRO-SEGMENTATION

Micro-Segmentation Basics

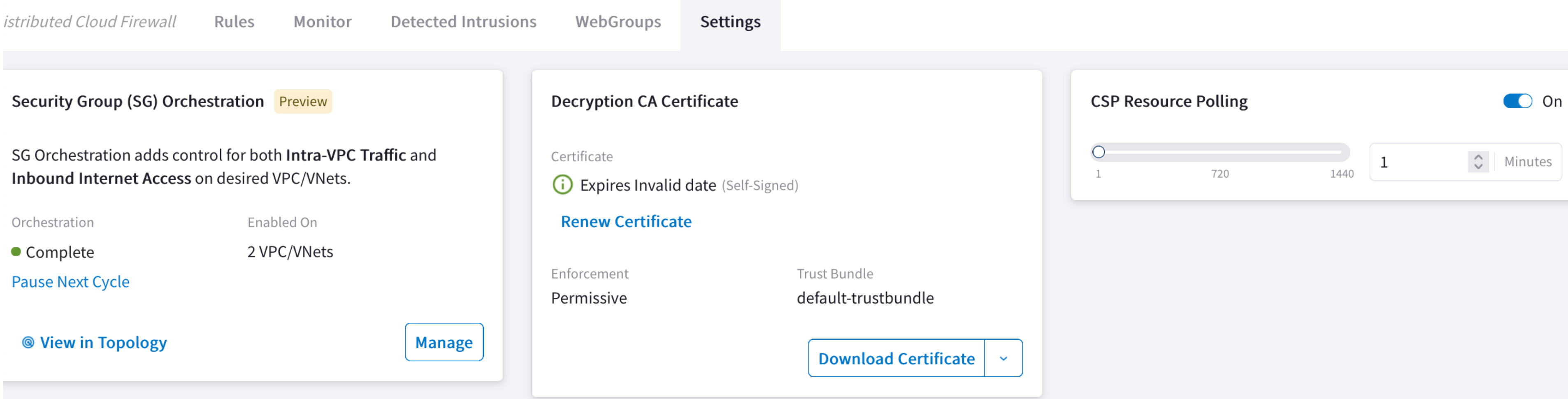
Aviatrix Distributed Cloud Firewall enforces policy exactly where needed across the entire network.

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

Intra VPC/VNET Distributed Firewalling (Micro-Segmentation)



istributed Cloud Firewall | Rules | Monitor | Detected Intrusions | WebGroups | **Settings**

Security Group (SG) Orchestration Preview

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

Orchestration: ● Complete

Enabled On: 2 VPC/VNets

Pause Next Cycle

View in Topology | Manage

Decryption CA Certificate

Certificate: Expires Invalid date (Self-Signed)

Renew Certificate

Enforcement: Permissive

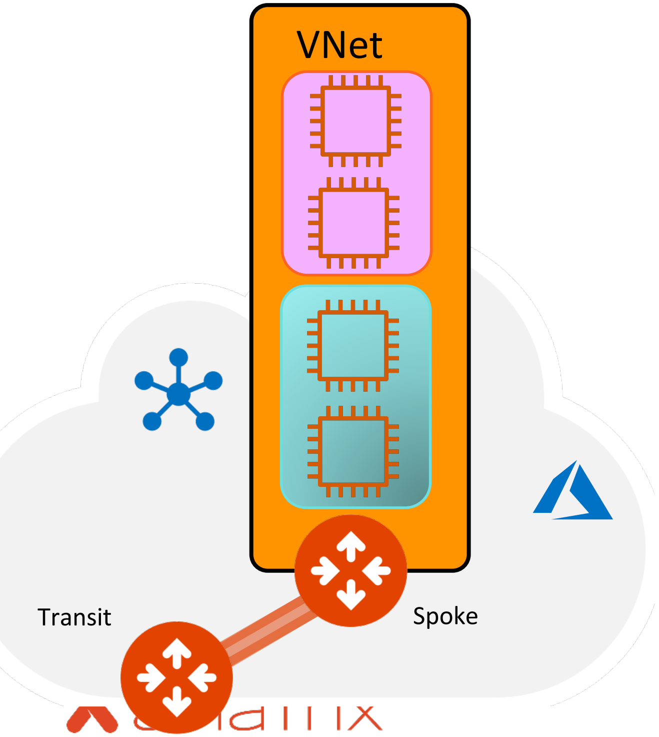
Trust Bundle: default-trustbundle

Download Certificate

CSP Resource Polling On

1 | 720 | 1440

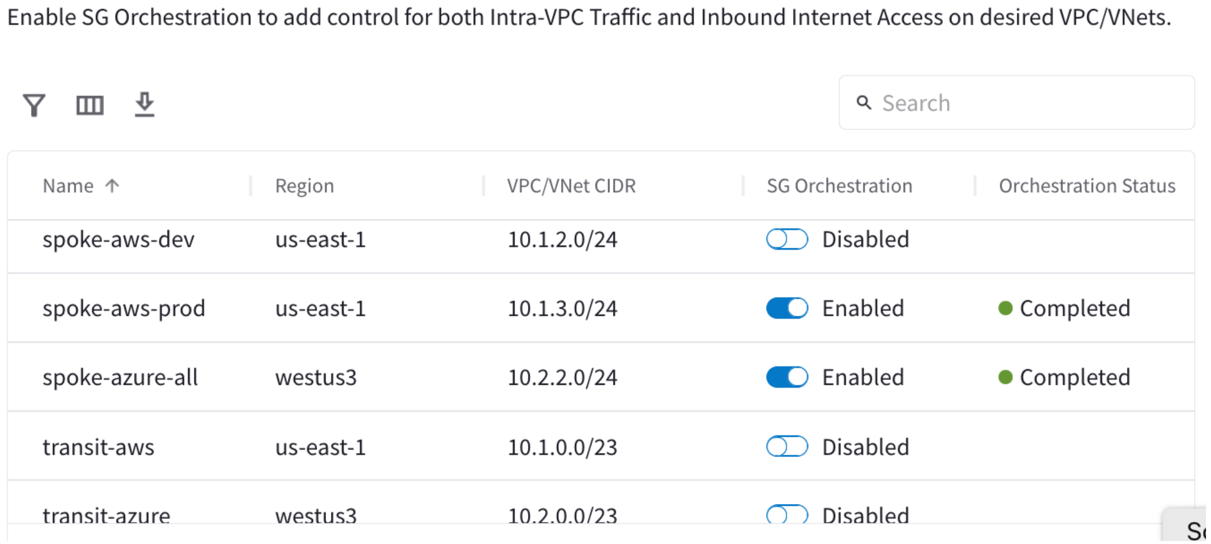
1 Minutes



SmartGroup #1

SmartGroup #2

Enable the feature on the concerned VPC/VNETS

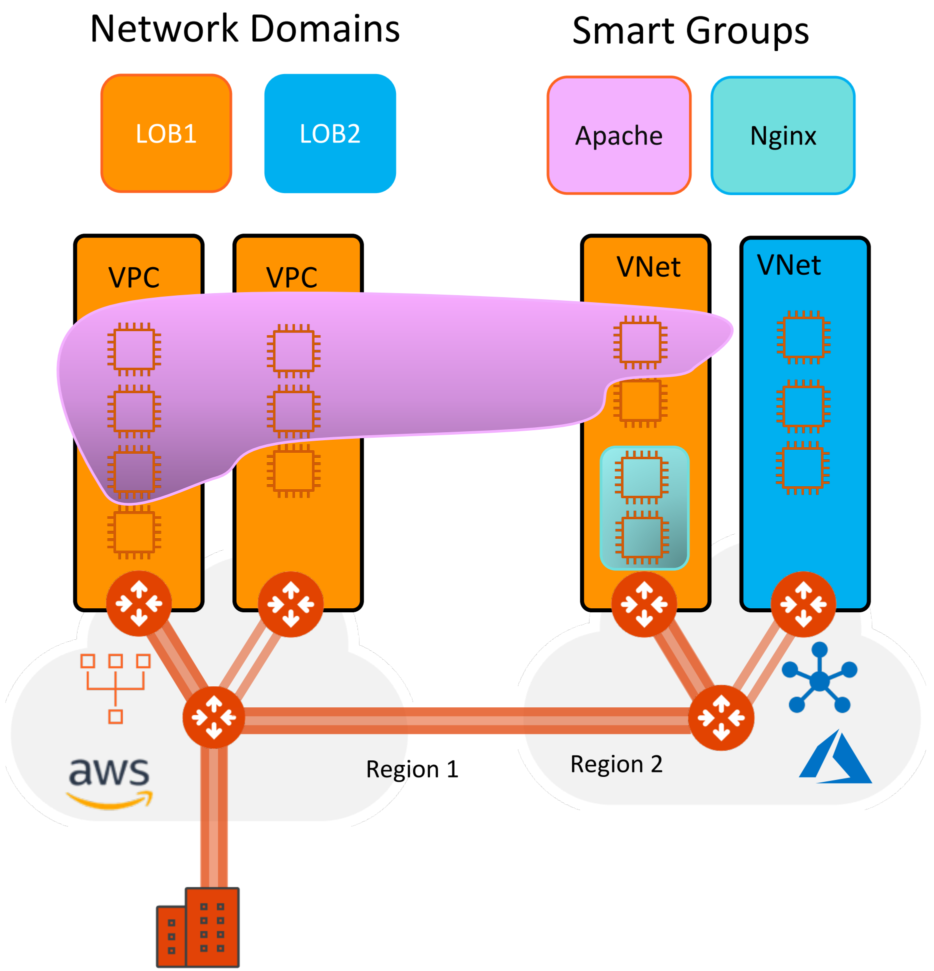


Enable SG Orchestration to add control for both Intra-VPC Traffic and Inbound Internet Access on desired VPC/VNets.

Search

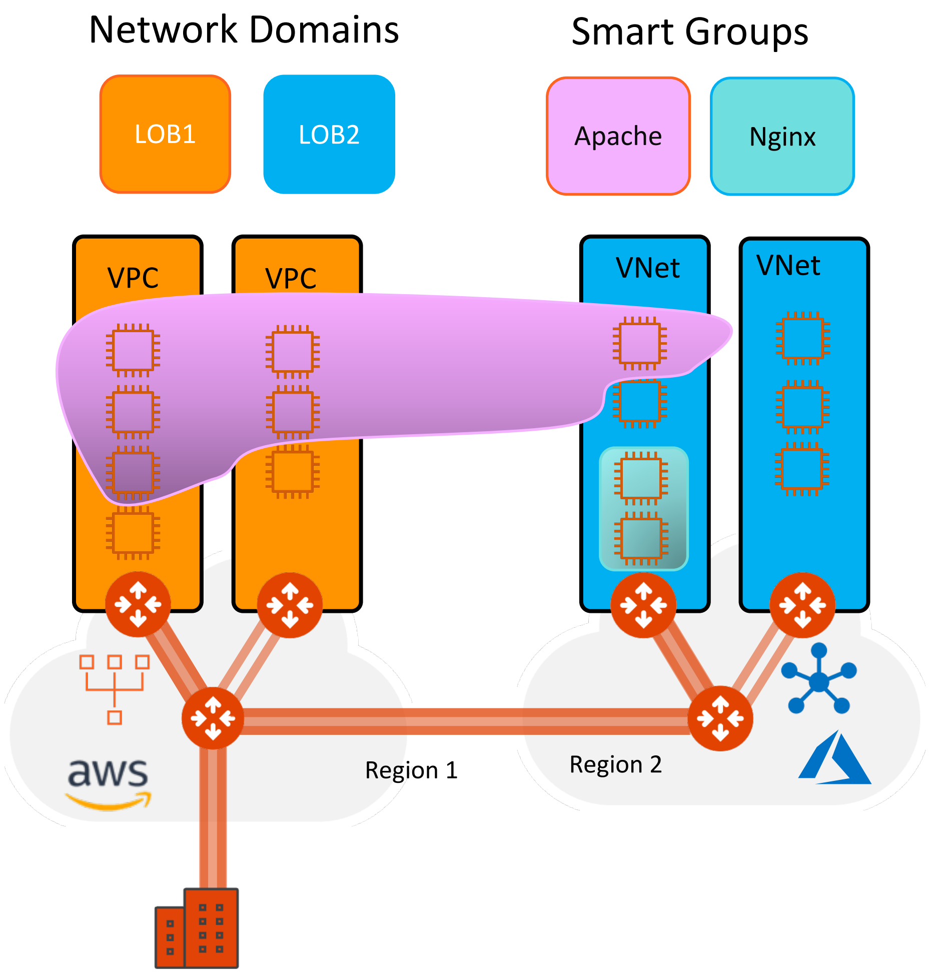
Name ↑	Region	VPC/VNet CIDR	SG Orchestration	Orchestration Status
spoke-aws-dev	us-east-1	10.1.2.0/24	Disabled	
spoke-aws-prod	us-east-1	10.1.3.0/24	Enabled	● Completed
spoke-azure-all	westus3	10.2.2.0/24	Enabled	● Completed
transit-aws	us-east-1	10.1.0.0/23	Disabled	
transit-azure	westus3	10.2.0.0/23	Disabled	

Network Segmentation & Micro-Segmentation Together



- **Scenario #1**: Smart Group defined within a Network Segment
- No connection policy between LOB1 and LOB2
- Apache and Ngnix are part of two different Smart Groups and can communicate.
- INTRA rule between Apache to Apache and only allow ICMP
- Only Apache VMs can ping each other
- Now, only Apache to Ngnix, only 443, is permitted.
- Since implicit deny is there, only 443 is allowed.
- Network Segmentation and Distributed Firewalling are NOT mutually exclusive.

Network Segmentation & Micro-Segmentation Together



- **Scenario #2**: Smart Group stretched between two Network Domains
- Network Segmentation takes precedence over the extent of a Smart Group

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

COMMUNITY
https://community.aviatrix.com