VMUG usercon

NSX DFW - Migliorare la sicurezza nel settore finanziario

Who am i?

Giovanni Dominoni

- SDN e Infrastructure Architect / Value Transformation Services
- vMUG Italia Board Member
- IT Academy Lead Instructor Corsi VCP-DCV / EforHum.it
- Blog personale: www.giovannidominoni.it

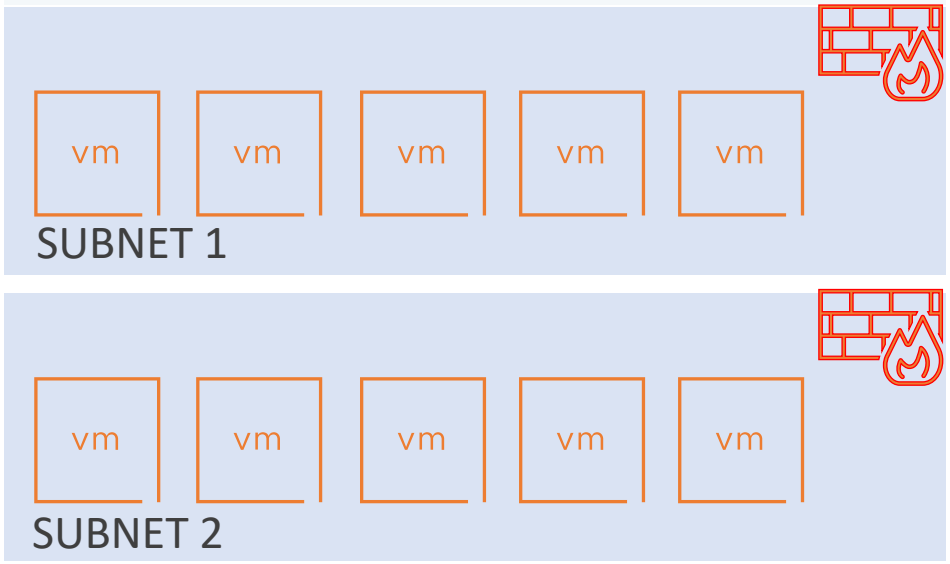
Agenda

- Customer Use Case
  - NSX Customer Environments Overview
    - Zero Trust Security Model
      - Security via TAGs
        - Communication outside NSX
          - Environment and Rule Automation
            - Important Security Design consideration
              - Future NSX enhacements

Customer Use case

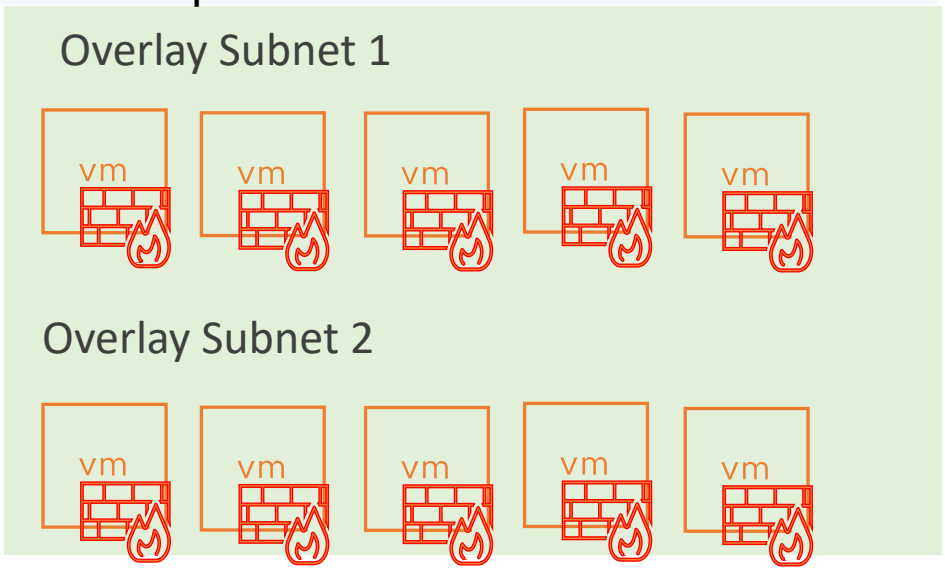
SECURITY WITH CENTRALIZED FIREWALL / LEGACY MODEL

- Security Zone based on Subnets
- No lateral movement protection
- Partial Automation, High Manual Operational load



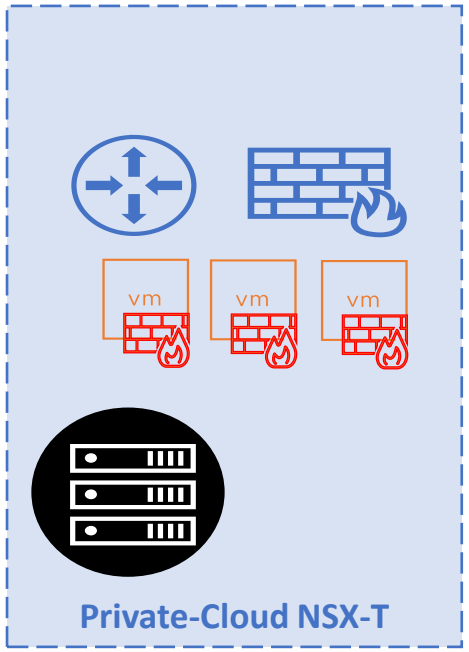
SECURITY WITH DFW / MICROSEGMENTATION

- Security Zone based on Security TAGs, Zero Trust
- Network agnostic
- Preventing Lateral Movements
- Full Automation, Low to Zero Operational load

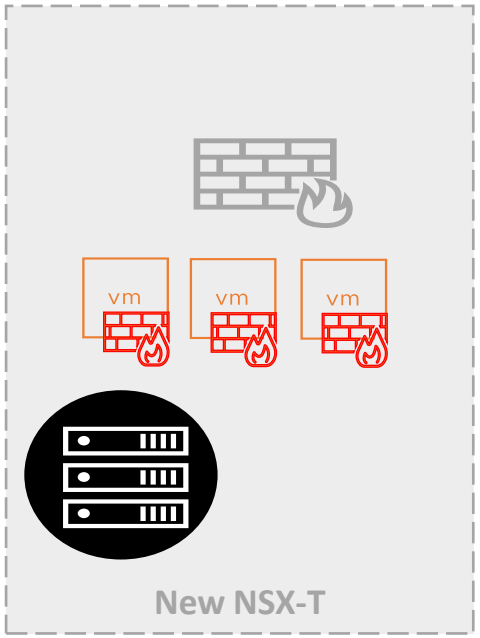


NSX Environment Overview

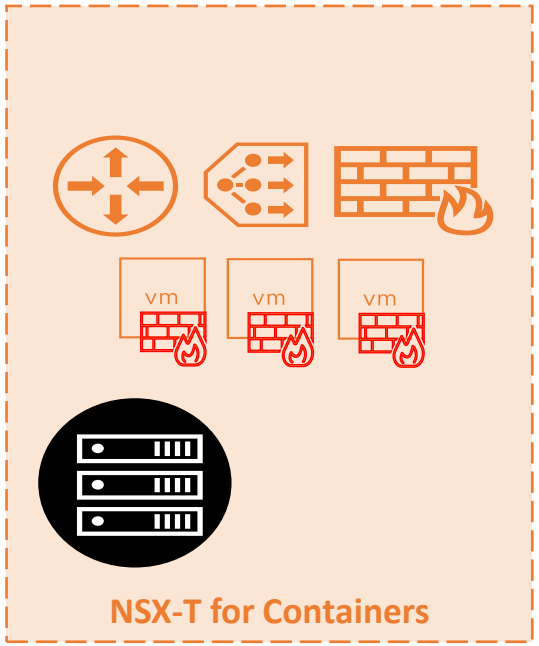
Private Cloud Environment using both **Overlay Networks and DFW** with automatic VM deployment (vRA), Rule creation via Custom Automation >3000 VMs
This environment was **Migrated from NSX-V to NSX-T**



New Greenfield Environment NSX-T 3.2 using **SECURITY ONLY**"DFW service" and Cisco Switches for Networking.
VLAN Backed vSphere Networking
Security Model equal to Private Cloud with Custom Script Automatism for Rule Creation
Migration Ongoing >1000 VMs

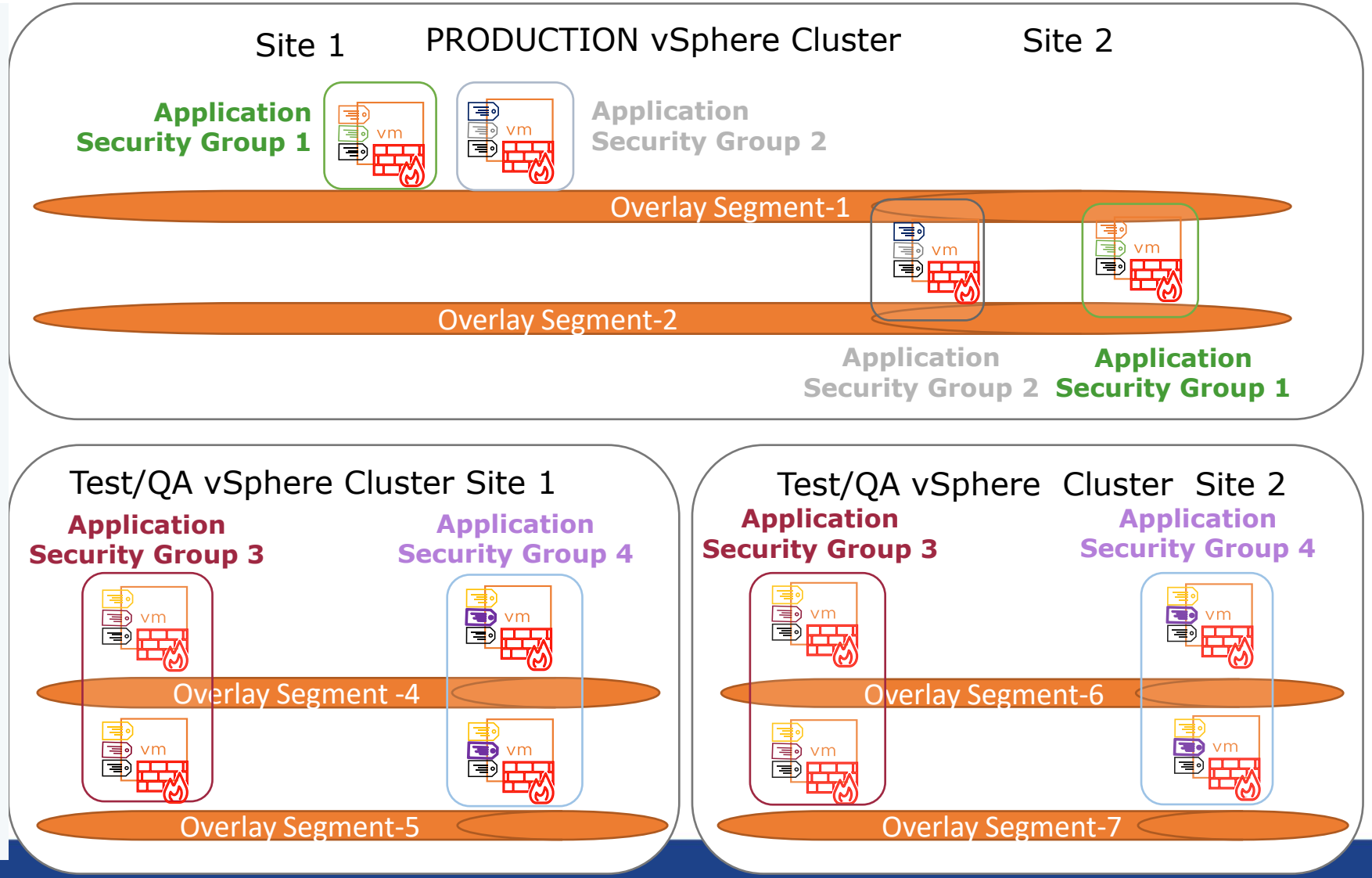


NSX-T with NCP Integration for Containers "Only" managed through Red Hat OpenShift Platform.
Micro segmentation **Security Model adapted for Cloud Native Workloads**
Rule Automation via Custom Script



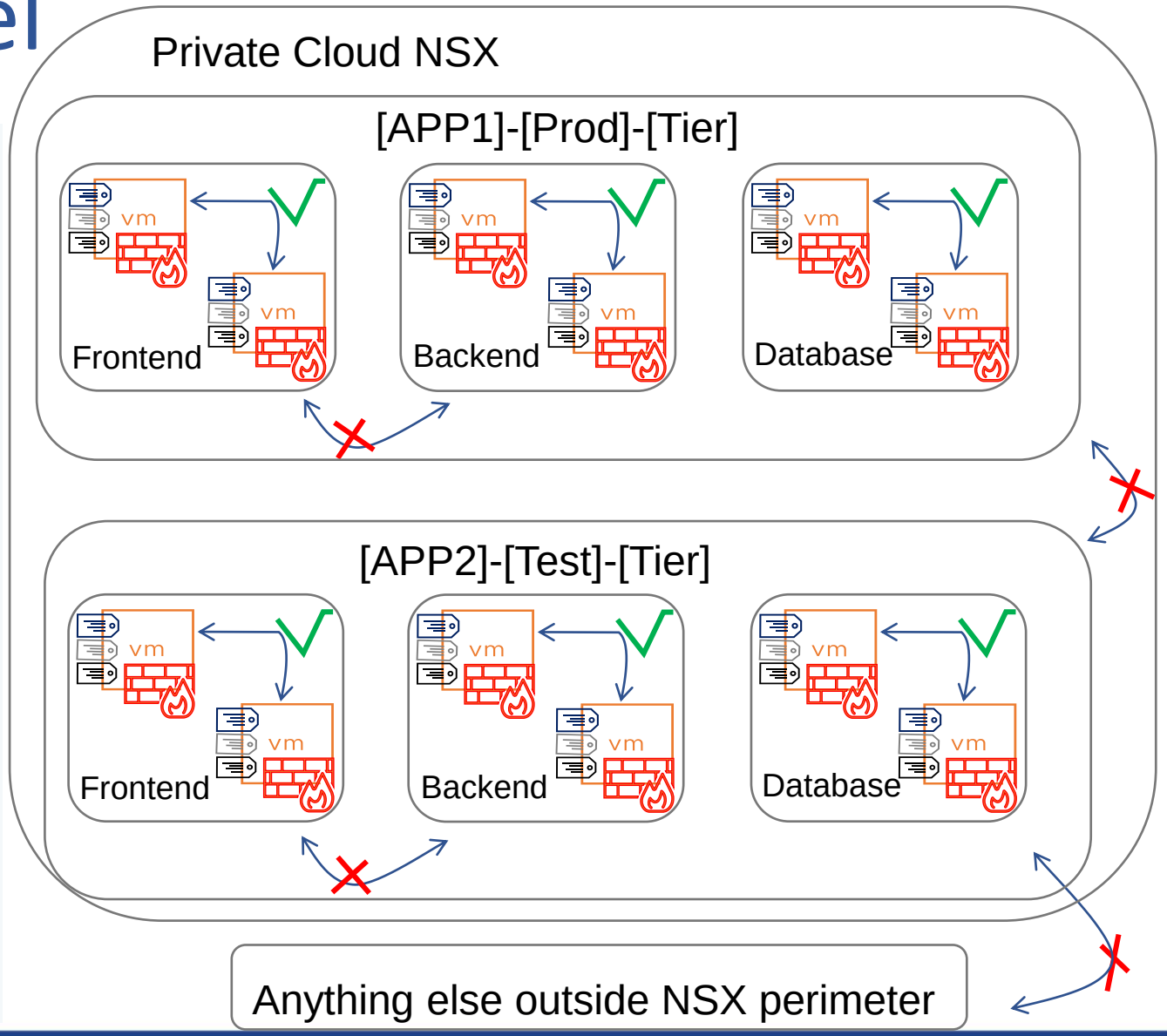
Security Consumption Model

- Group Membership criteria defined through TAGs
- L3/L4 Security Policies
- Agnostic to the IP/Subnet
- VM mobility across Sites without losing security



Zero Trust Security Model

- For VMs/Members part of the same Security Group, all traffic is permitted by default
- Between different environments communication is not permitted by default
- Between different APPs communication is not permitted by default
- Between different tiers communication is not permitted by default
- External communication is not permitted by default
- Explicit permit rule to allow traffic



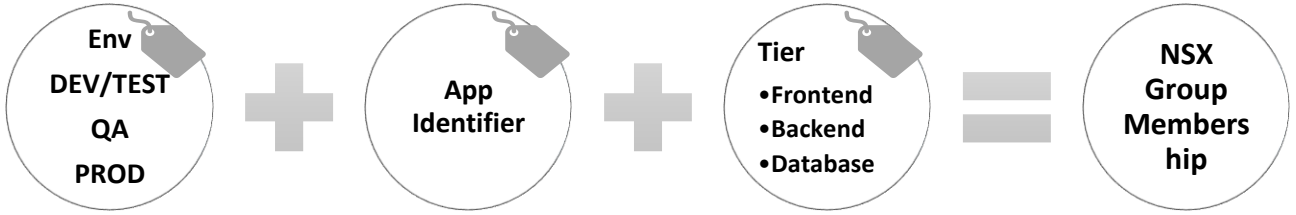
Security Model via TAGs

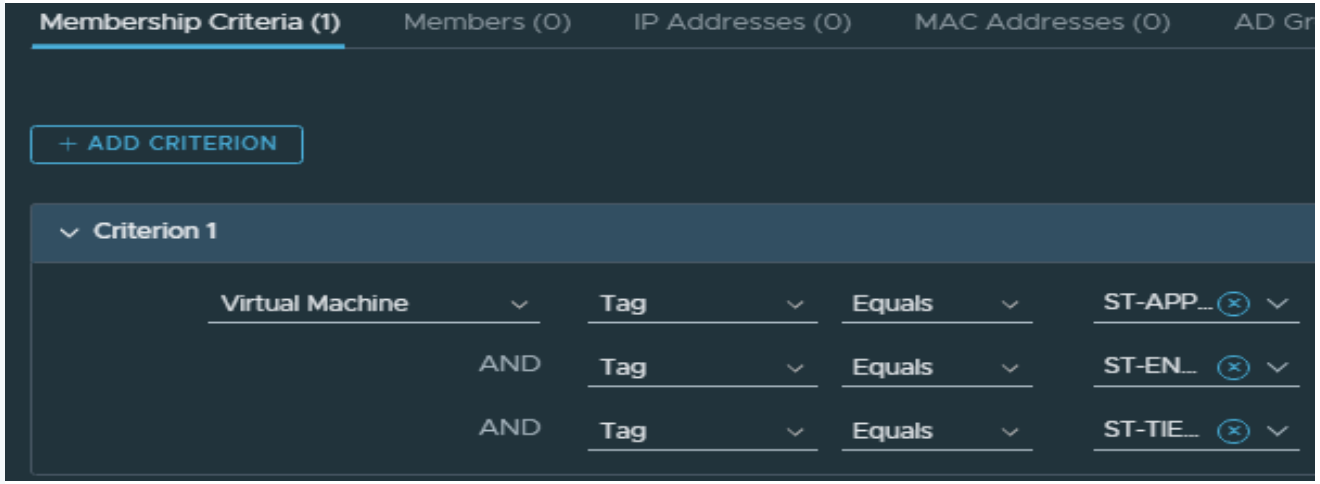
The Group membership is defined by multiple security TAGs:

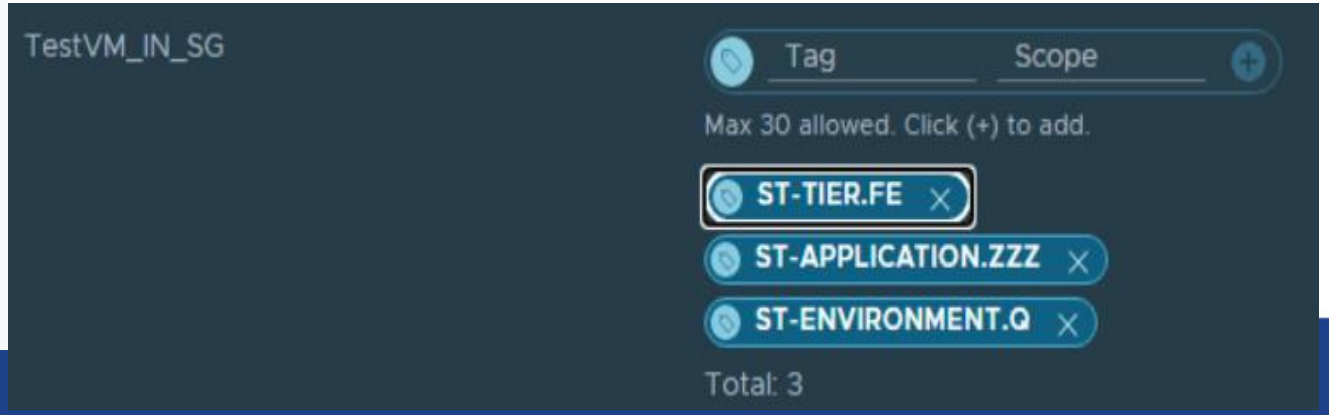
- **Environment**
- **App Identifier**
- **Tier**

Security enforcement lifecycle through dynamic membership criteria

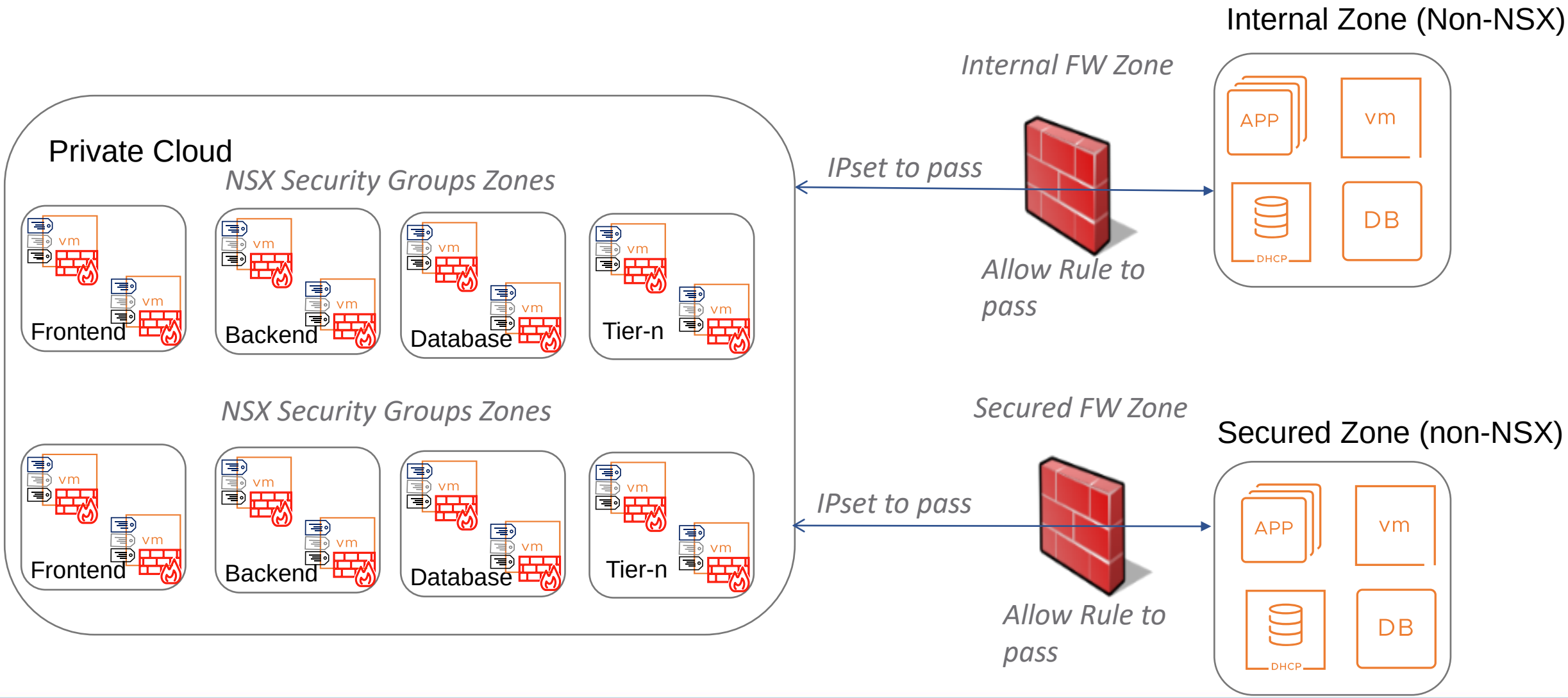
Zero Trust is applied to all workloads VMs in case missing TAGs



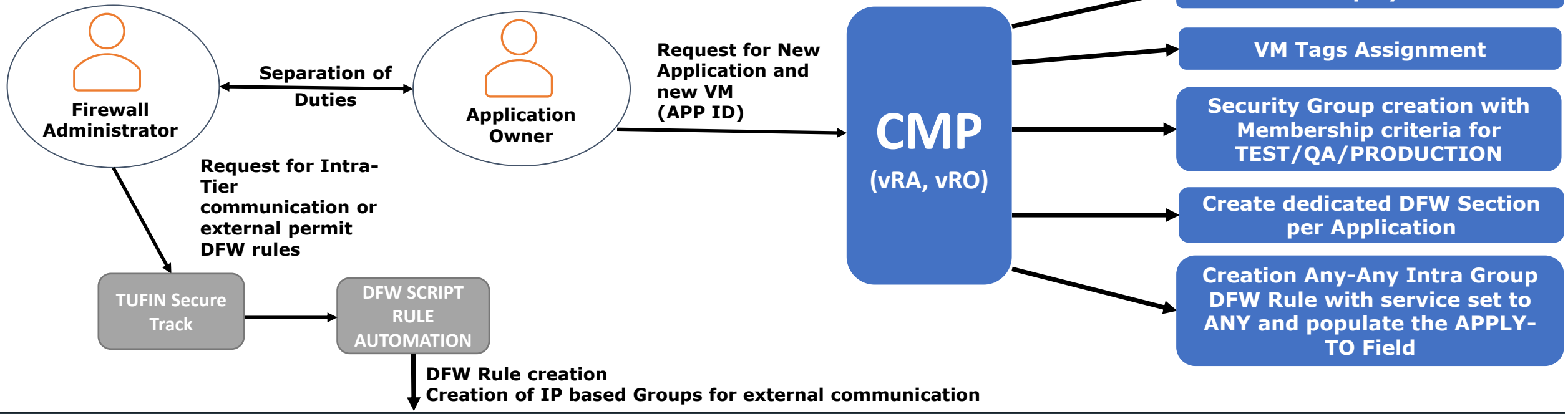




Communication outside NSX



Environment Automation



Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
ZZZ (4) Applied To DFW							Success
SG Intra Any	317443	SG-ZZZ-P-FE	SG-ZZZ-P-FE	Any	None	SG-ZZZ-P-FE	Allow
SG to SG	317444	SG-ZZZ-P-FE	SG-ZZZ-P-BE	HTTPS	None	SG-ZZZ-P-FE SG-ZZZ-P-BE	Allow
SG to Ext	317445	SG-ZZZ-P-FE	n-192.168.0.0/24	SSH	None	SG-ZZZ-P-FE	Allow
Ext to SG	317446	n-192.168.0.0/24	SG-ZZZ-P-FE	HTTPS	None	SG-ZZZ-P-FE	Allow

Important Security Design consideration

Leverage ALWAYS the Apply-TO field to minimize DFW resource consumption

- Limits rules per vnic
- Limits rules per Host

Monitoring NSX manager Dashboard for Distributed Firewall relevant object

- Distributed Firewall Rules
- Distributed Firewall Section
- Groups
- Groups Based on IP-Addresses

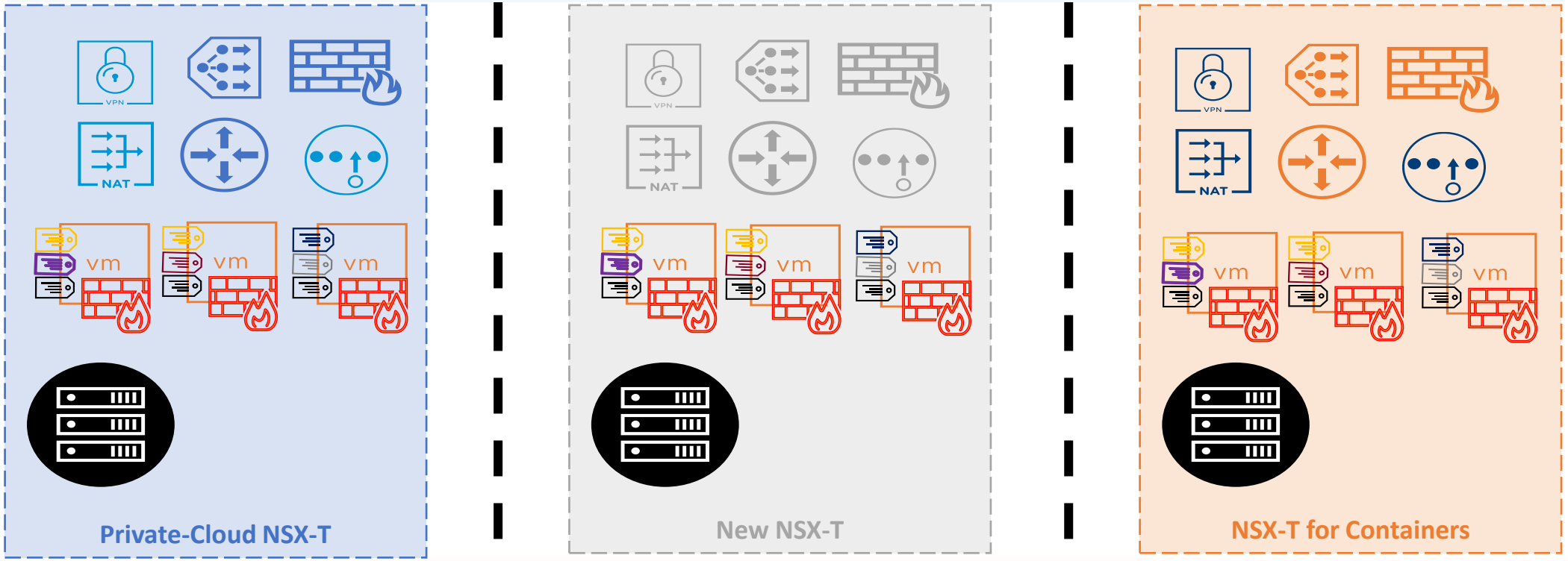
VRNI and Syslog for Monitoring, Troubleshooting and cleanup

- No hit rules
- Masked rules
- Flows monitoring

NSX Future Implementations

Enhance the Security Posture and NSX Services for all the NSX environments with:

- DFW with Context Profiles (L7 App)
- IaaS / DFW as a Code
- Advance Threat Prevention (Distributed IDS/IPS, Distributed Malware Prevention, NDR, NSX Intelligence)
- Advanced LB



Q/A

VMUG usercon