Zero-Trust with VMware vDefend

Current Threat Landscape

44%

of breaches reported lateral movement[1]

204

Days to detect a breach[2]

$4.35M

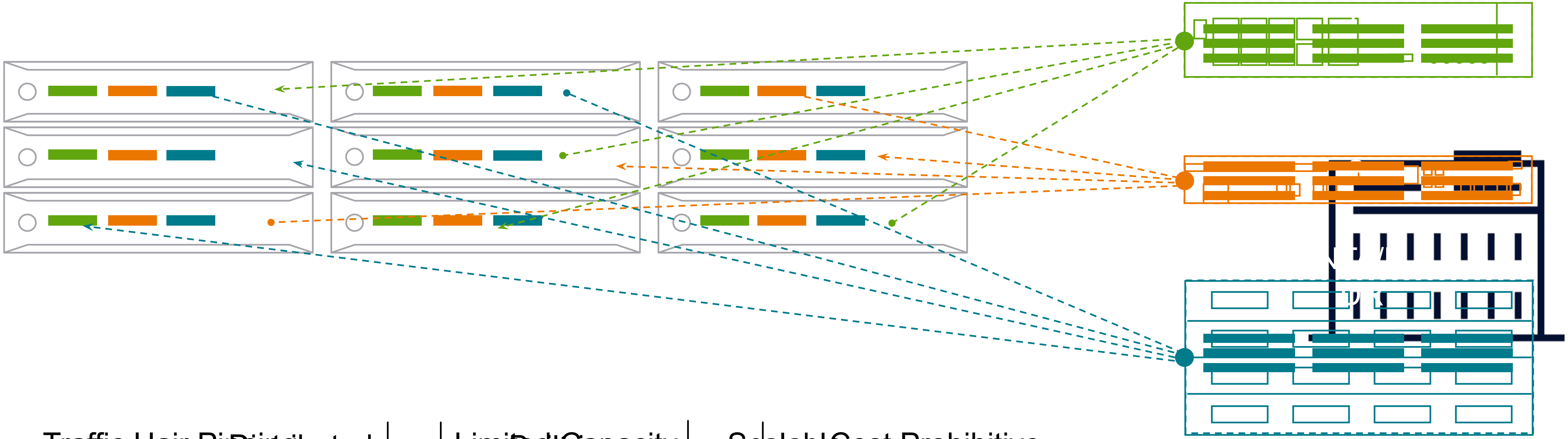
Average cost of a data breach[3]

Source 1 – 2022 VMware Global Threat Report, Source 2 - 2023 Verizon Data Breach Investigation report, 3 – 2023 IBM Cost of Data Breach Report

vmware by Broadcom

Challenges with Traditional Approaches for Lateral Security

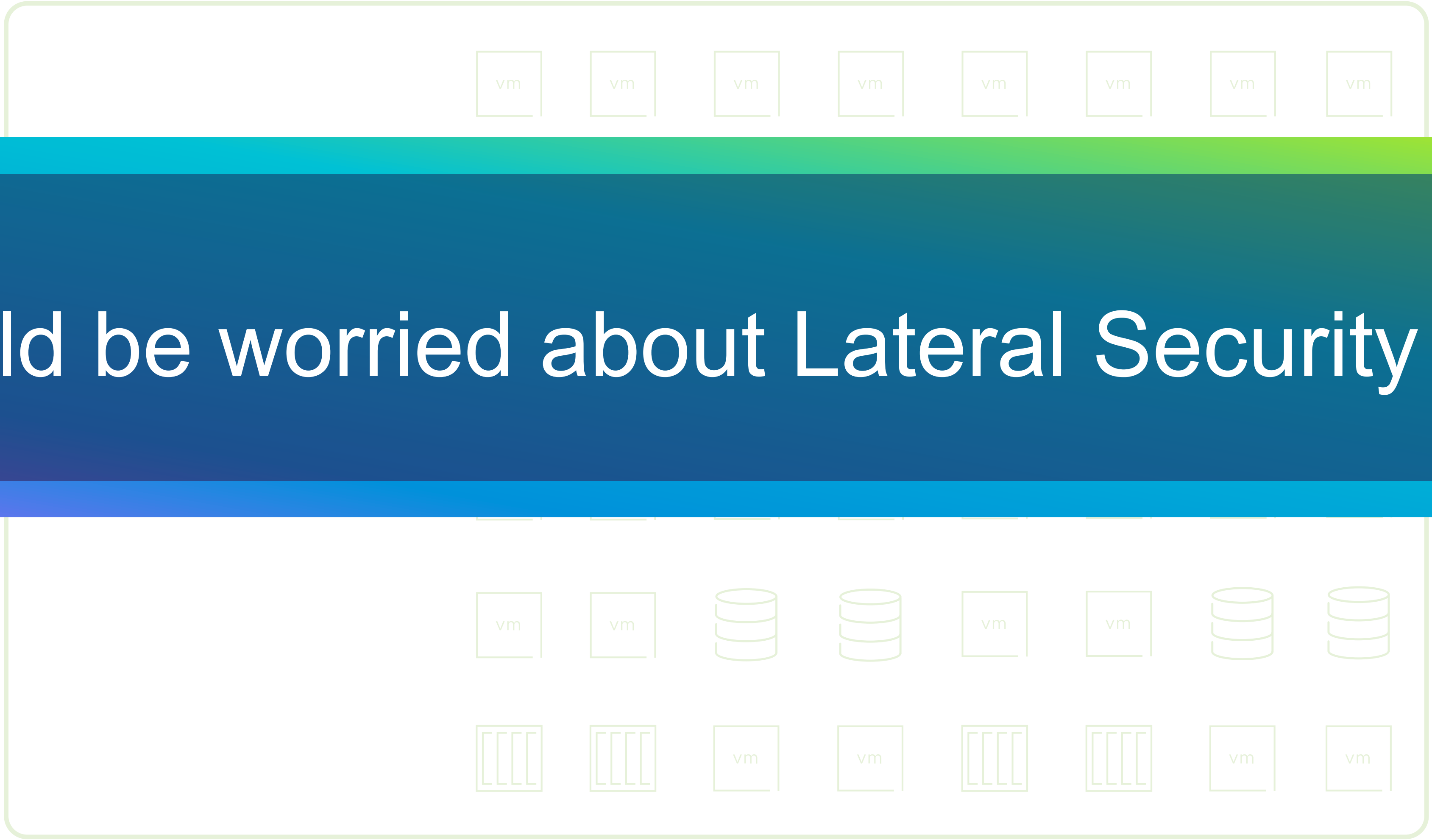
vDefend Security Architecture



Traffic Hair Pinning | Limited Capacity | Cost Prohibitive

Distributed | Built-in | Scalable

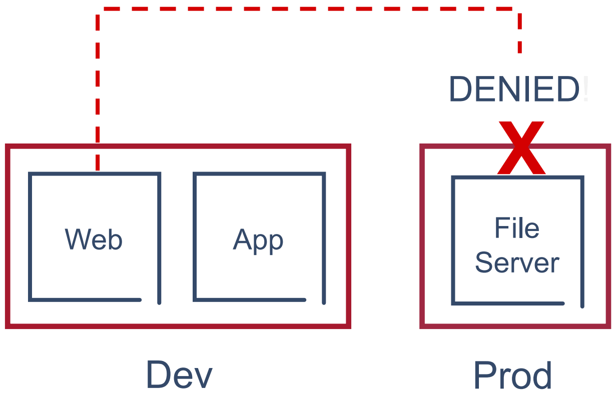
Securing Just at the Perimeter Isn’t Enough



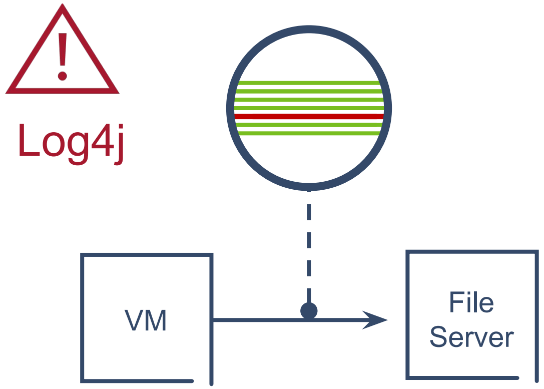
You should be worried about Lateral Security

Common Type of Attack Vectors

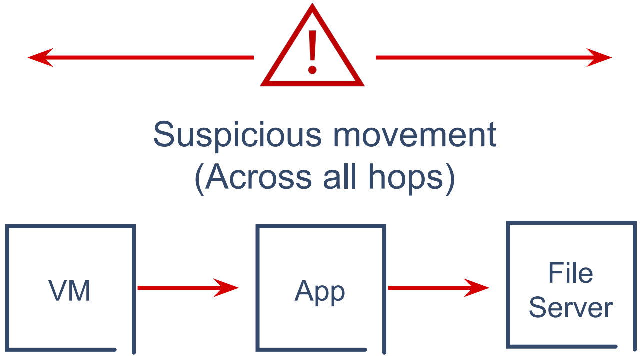
Lateral Movement



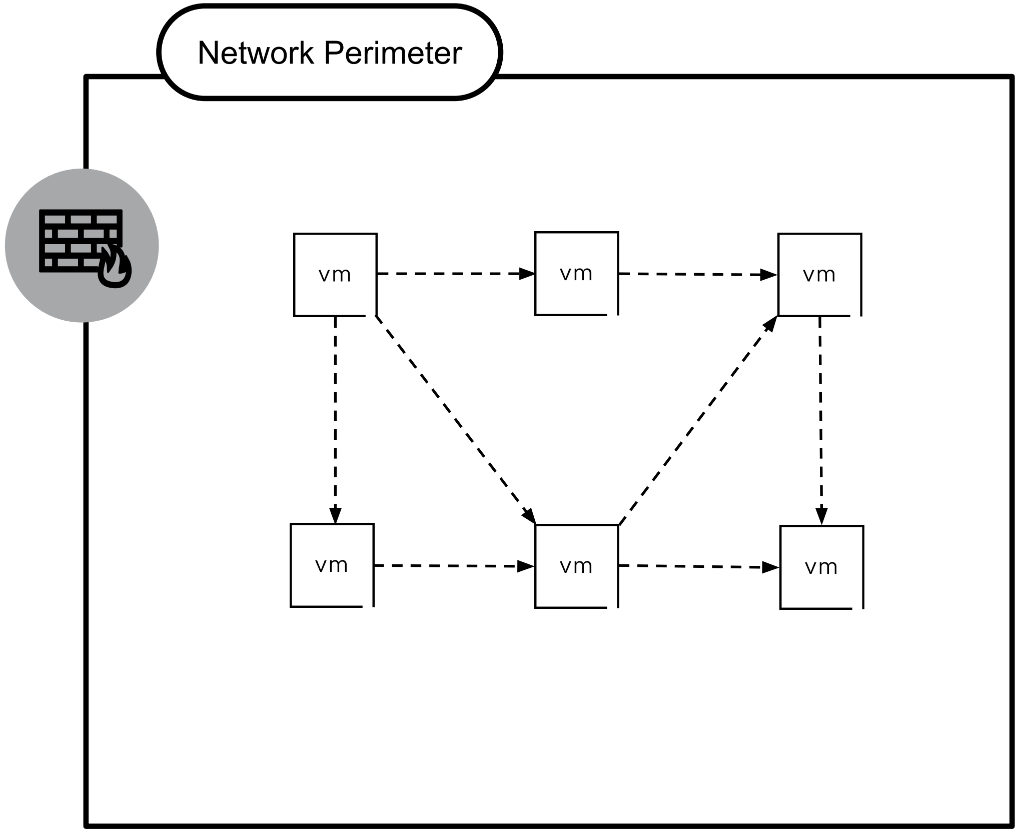
Vulnerability Exploits



Zero-Day Attacks

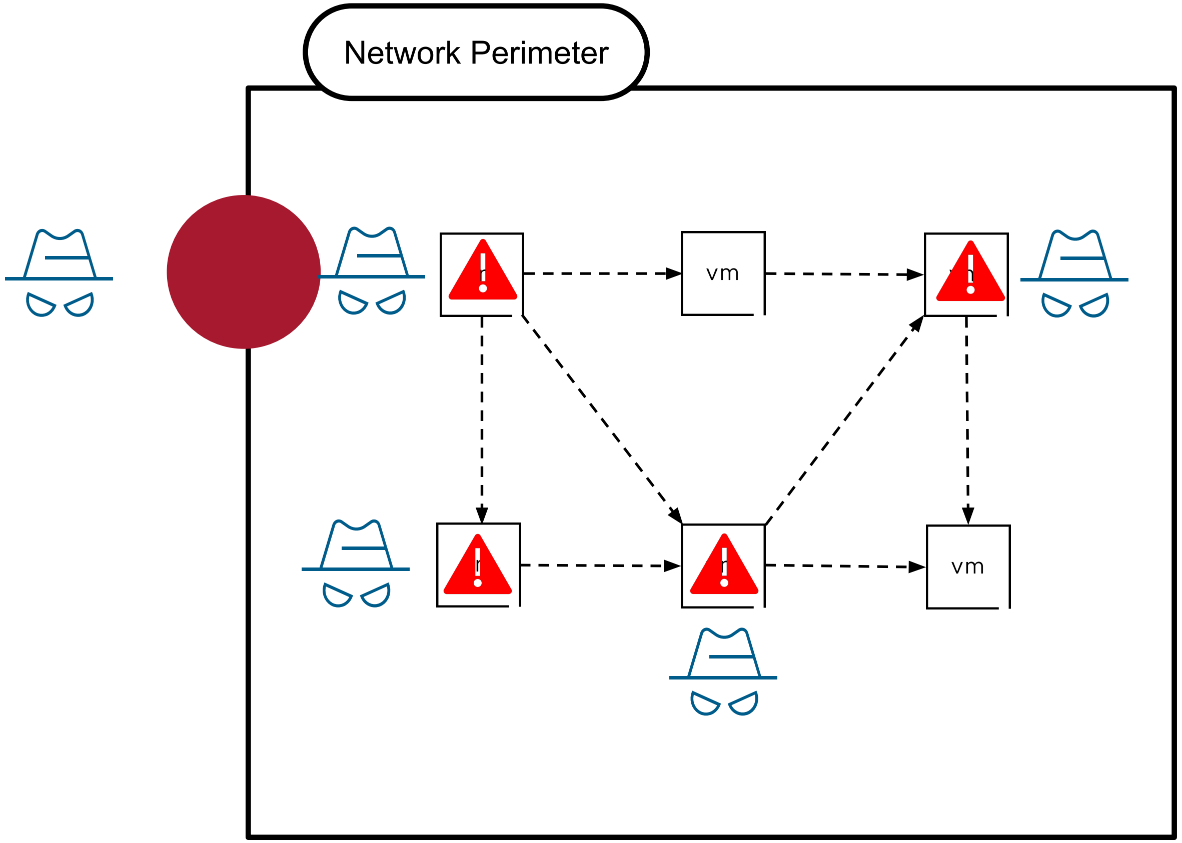


Perimeter Security is Inadequate



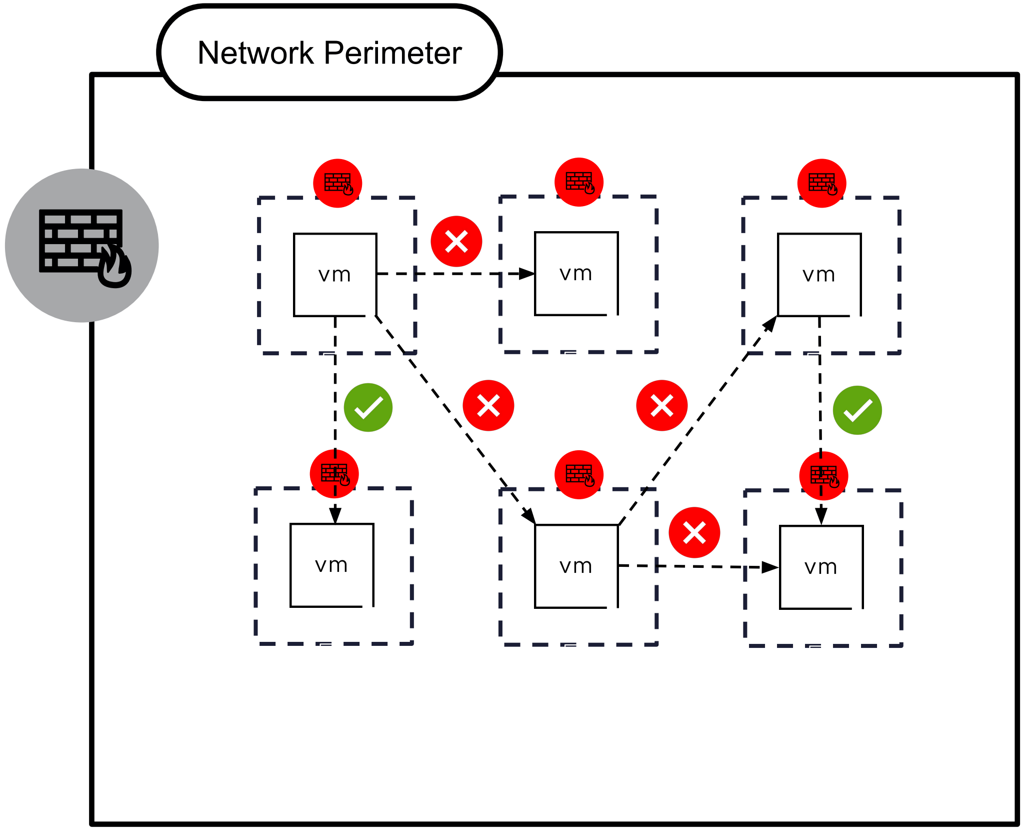
Perimeter Security is Inadequate

If the perimeter is breached, the attacker has free movement within the datacenter



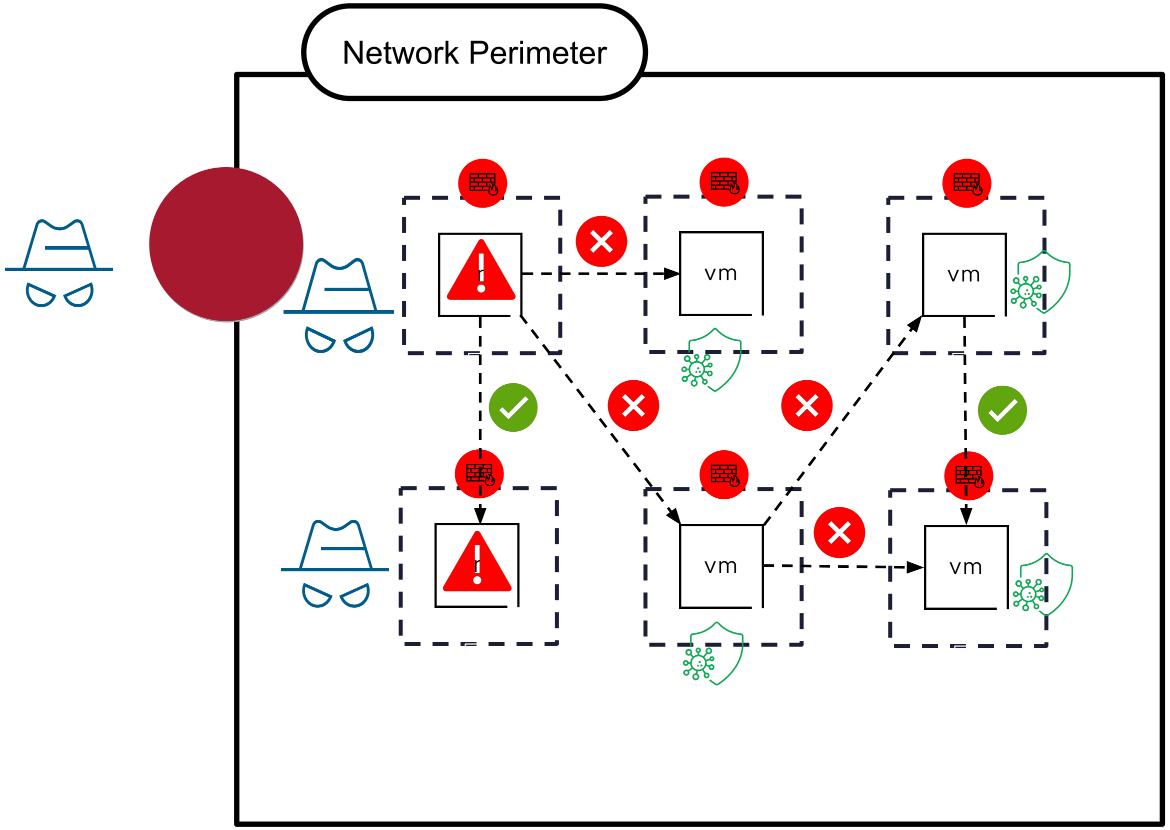
Perimeter Security is Inadequate

DFW can be configured to allow traffic only between VMs that need to communicate for org needs

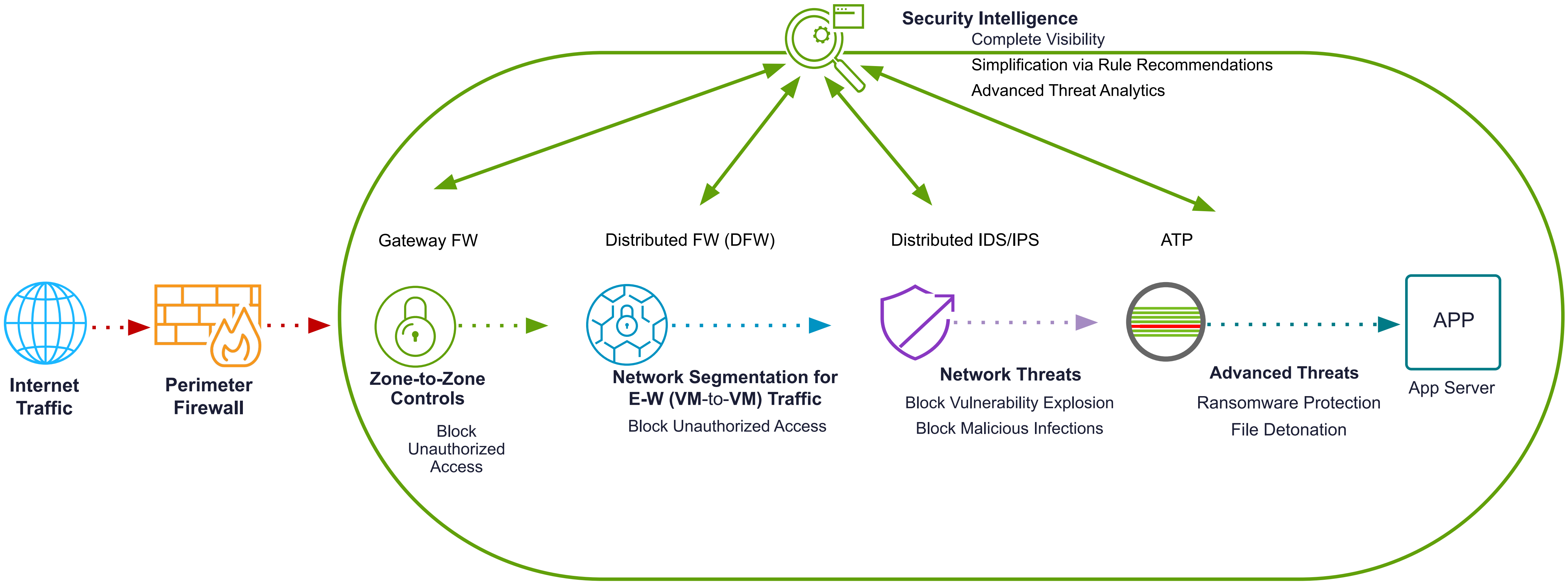


Perimeter Security is Inadequate

Should the perimeter be breached, this limits the scope and contains the lateral movement of the attacker



Multi-layer Defense-in-Depth Protection Enables Zero Trust



Security Intelligence

Complete Visibility

Simplification via Rule Recommendations

Advanced Threat Analytics

Internet Traffic

Perimeter Firewall

Zone-to-Zone Controls

Block Unauthorized Access

Network Segmentation for E-W (VM-to-VM) Traffic

Block Unauthorized Access

Network Threats

Block Vulnerability Explosion

Block Malicious Infections

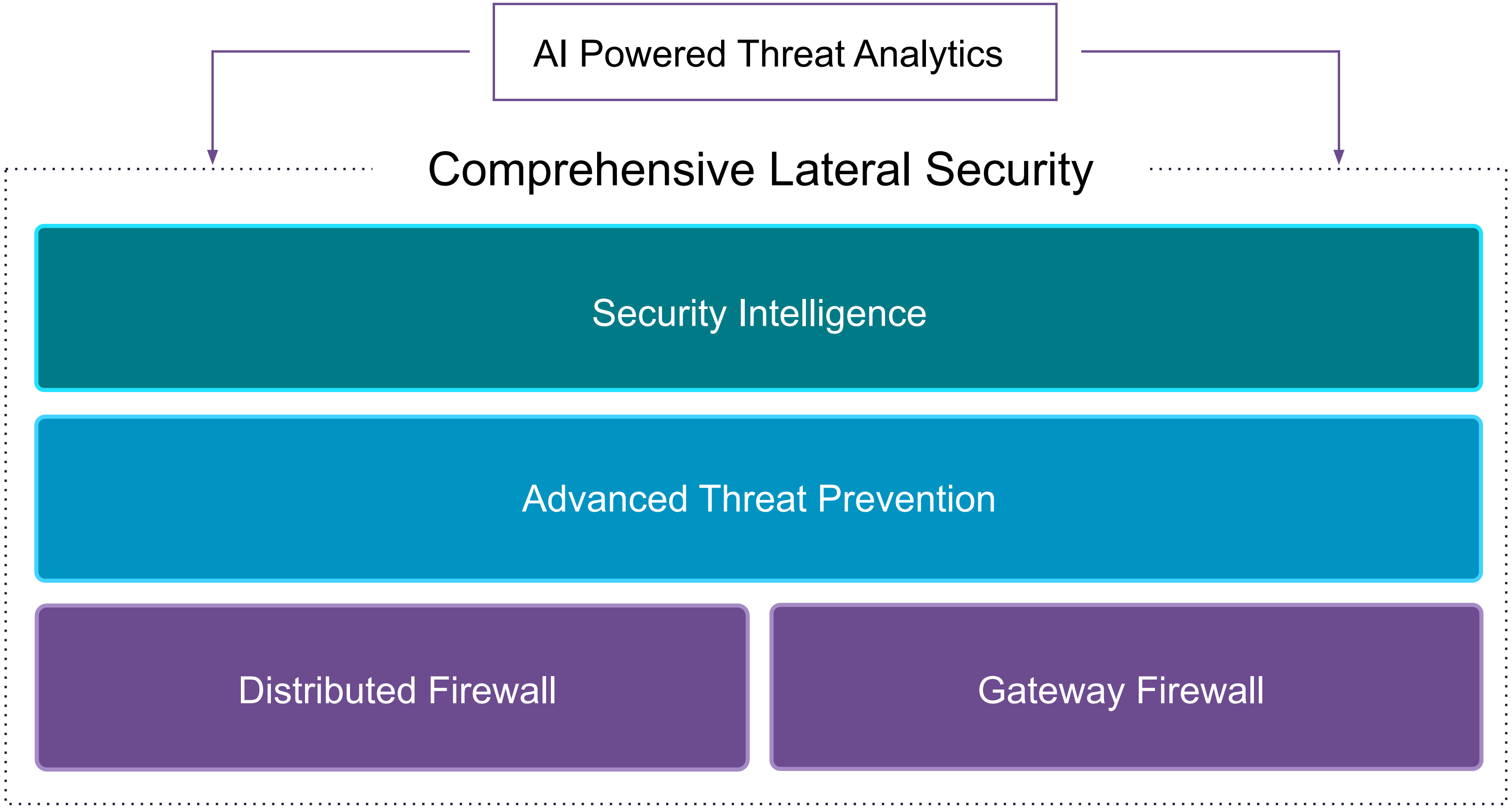
Advanced Threats

Ransomware Protection

File Detonation

App Server

Fully Integrated Security Stack

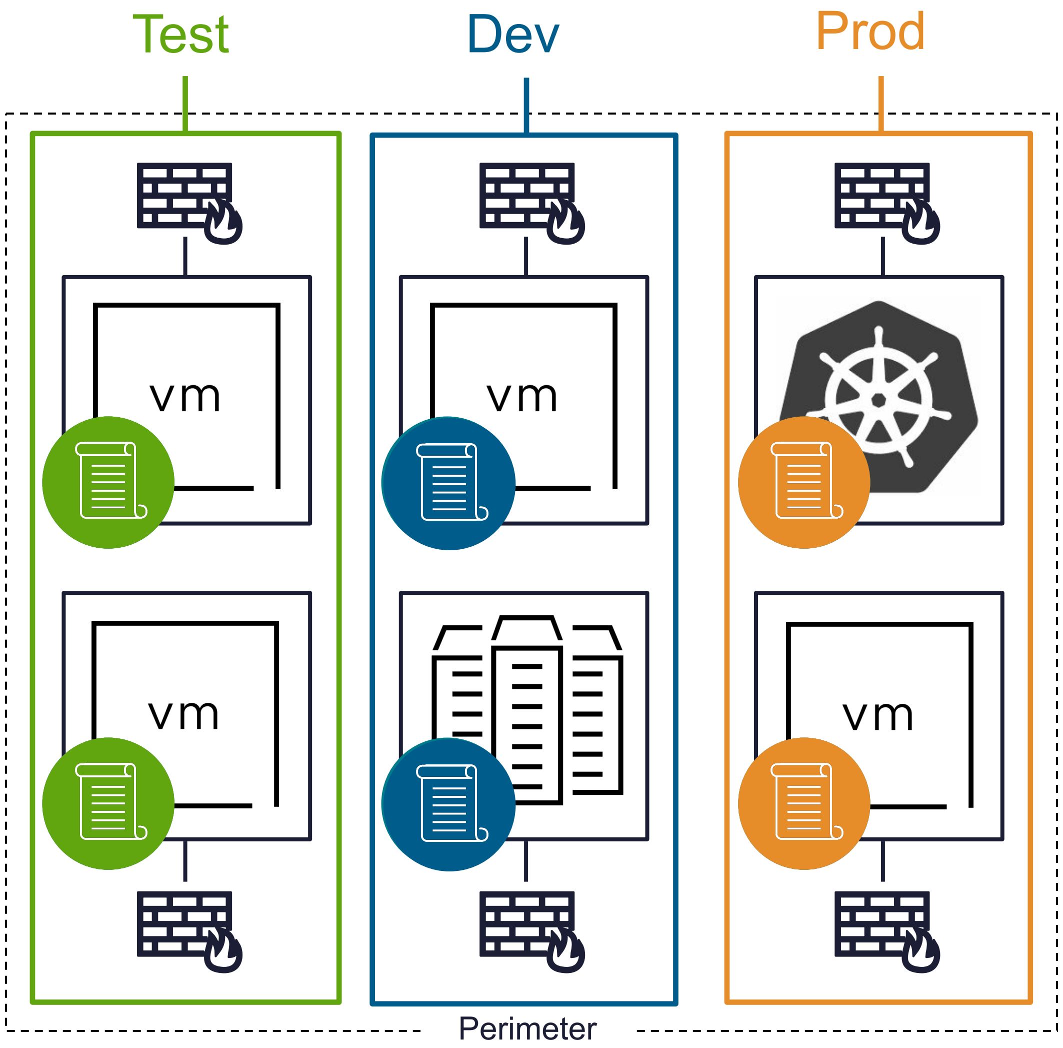

AI Powered Threat Analytics
Comprehensive Lateral Security
Security Intelligence
Advanced Threat Prevention
Distributed Firewall
Gateway Firewall

App Discovery
Security Analytics
Rule Recommendations

Ransomware Prevention
Malware Prevention
Vulnerabilities

Secure Infrastructure
Secure Virtual Zones
Secure Apps
Compliance

VMware vDefend Distributed Firewall



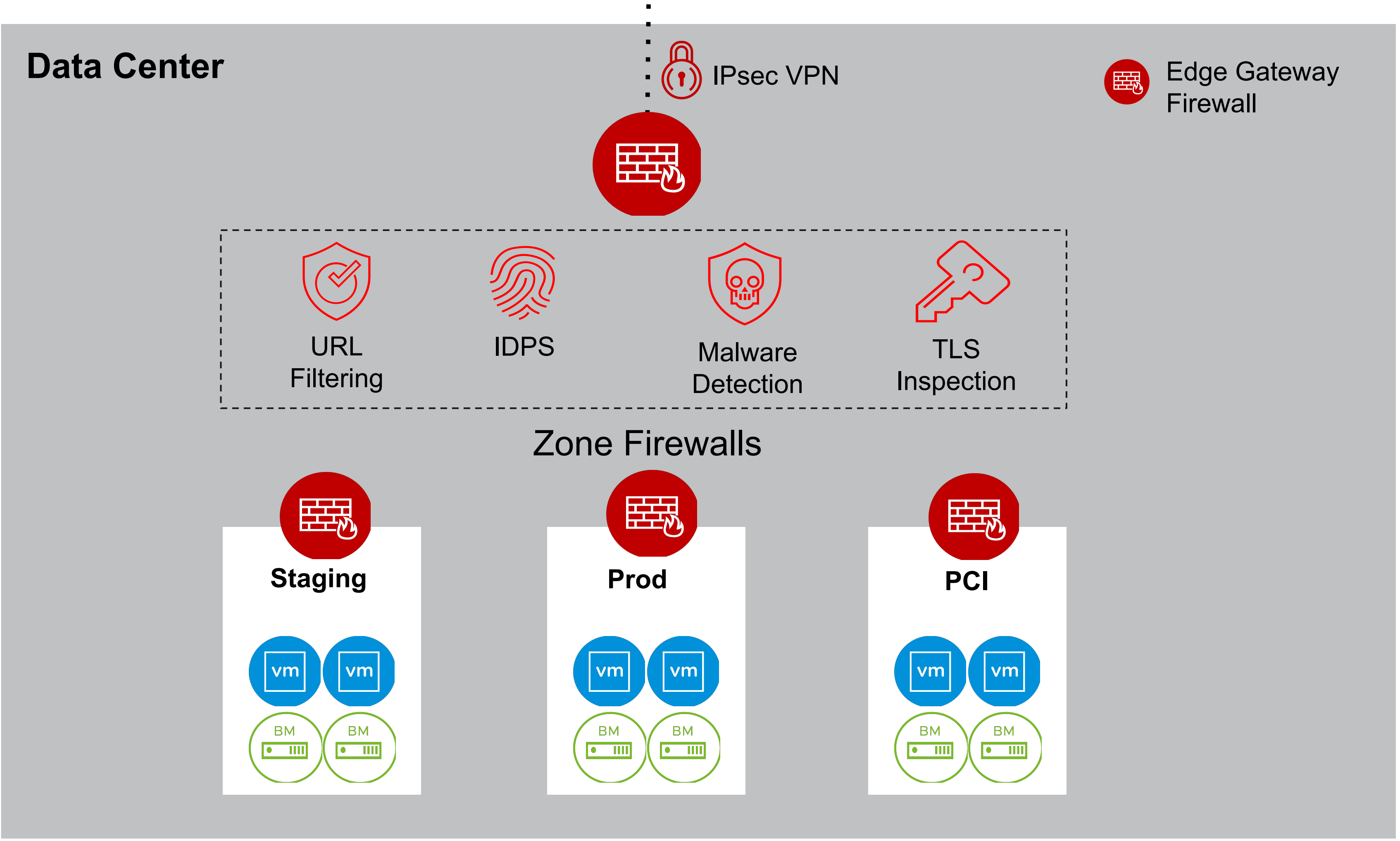
Elastic Throughput
Distributed Architecture
Rich API

L2-L4 Firewall
L7 Application Inspection
Identity-Based
Malicious IP Filtering

Dynamic/Static Grouping
Flexible Matching Criteria
Optimized Configuration

Vmware vDefend Gateway Security

Next Generation Edge Gateway Firewall



1. Gateway Firewall is a centralized service and needs the Service Router (SR) component of the Gateway

2. The Gateway Firewall can be implemented on the NSX-T Edge Node in both:
   - VM form factor
   - Bare Metal form factor

VMware vDefend Gateway Security

Next Generation Edge Gateway Firewall - Key Capabilities

Stateful L3-L4 Firewall

L7 Application Identity
Addition of > 750 APP-IDs

Intrusion Prevention & Detection (IPS/IDS)
Behavioral & Lua script-based signatures

Malware Detection including Sandboxing
Known and day0 malware

TLS Inspection (TLS Decryption)
Identify attacks in encrypted traffic

User-ID Firewalling for Physical Servers
Identity Firewall with Event Log Scraping

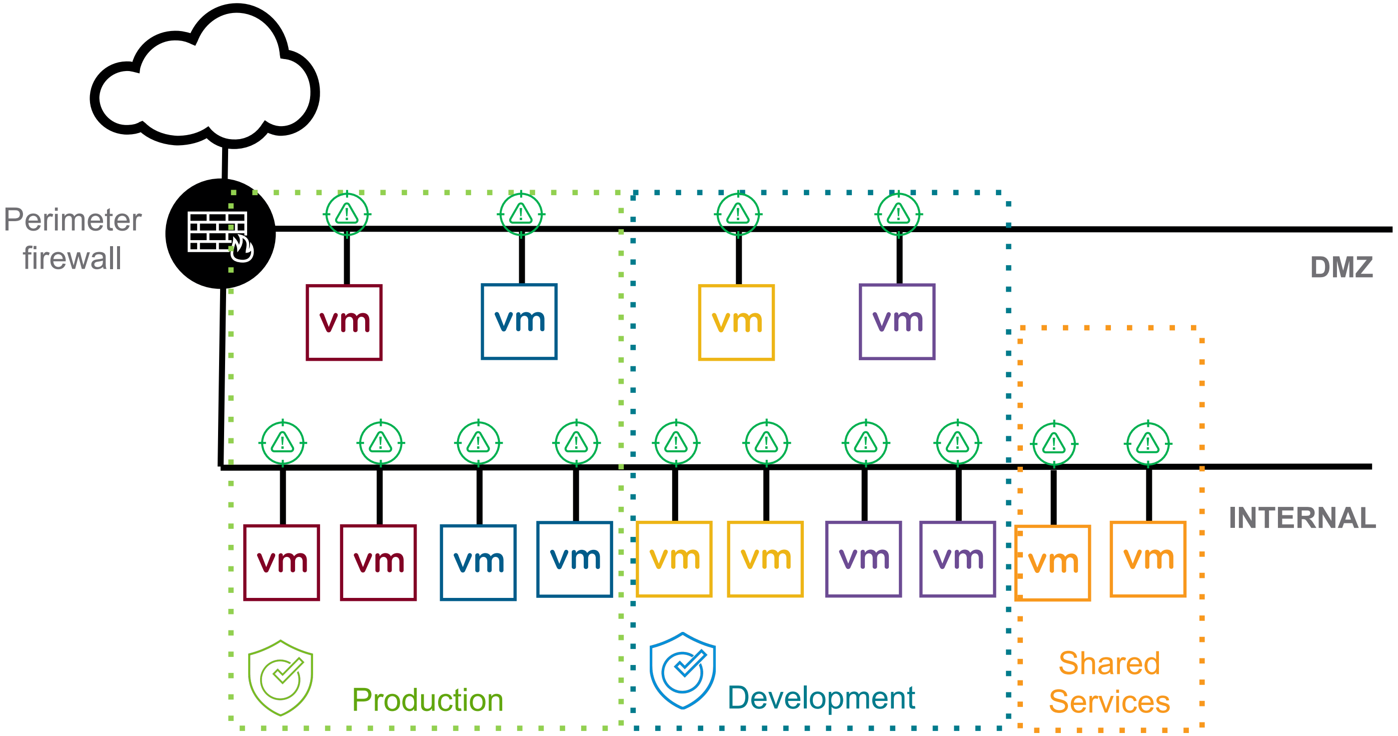
URL Filtering
URL category and reputation-based

FQDN Analysis
Visibility into user and Application Internet Usage

Stateful Active/Active
Horizontal scale out for higher throughput

NAT, IPSec VPN, L2 VPN, dynamic Routing

Advanced Threat Prevention



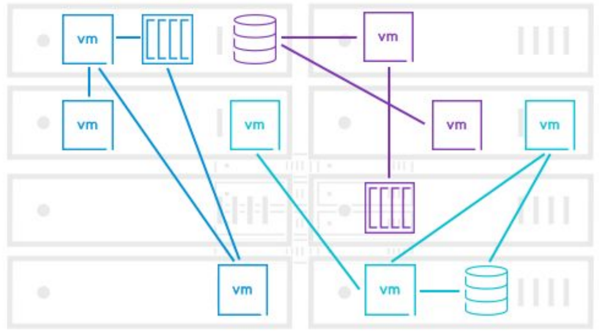
Elastic Throughput
Distributed Architecture
Rich API

IDS/IPS
NTA
Malware Prevention
Virtual Patching

Context-Based Threat Detection
Curated Signature Distribution

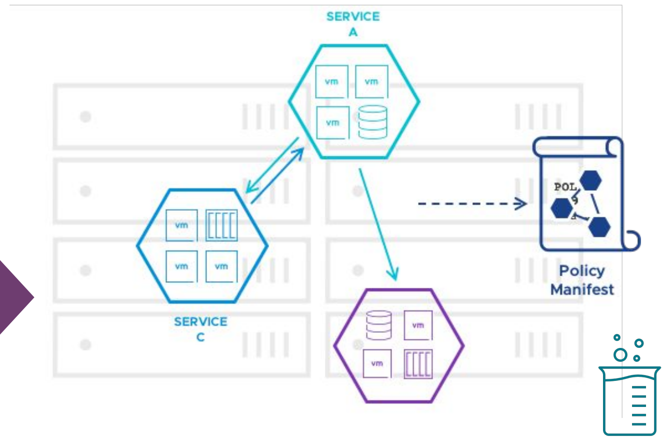
VMware vDefend Security Platform (Security Intelligence)

From Visibility to Insights



App Flow Visibility

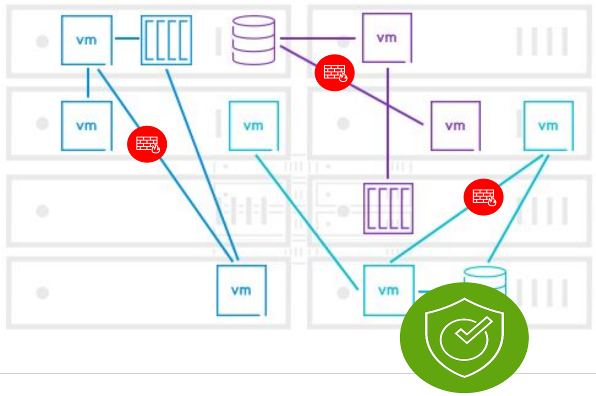
- **Contextual visibility** color codes flows with Segmentation rules
- **Eliminates blind spots** with comprehensive Visibility Into Flows and Posture with Full Visibility to E-W Traffic
- **Enhanced Context** - Provides visibility to process and application visibility with L7 context



Analytics and Automation

Uses NSX Inventory and Config to detect unprotected flows, workloads and applications to provide high fidelity rule recommendation

- **Reuses** existing groups or services
- **L7 Recommendation**



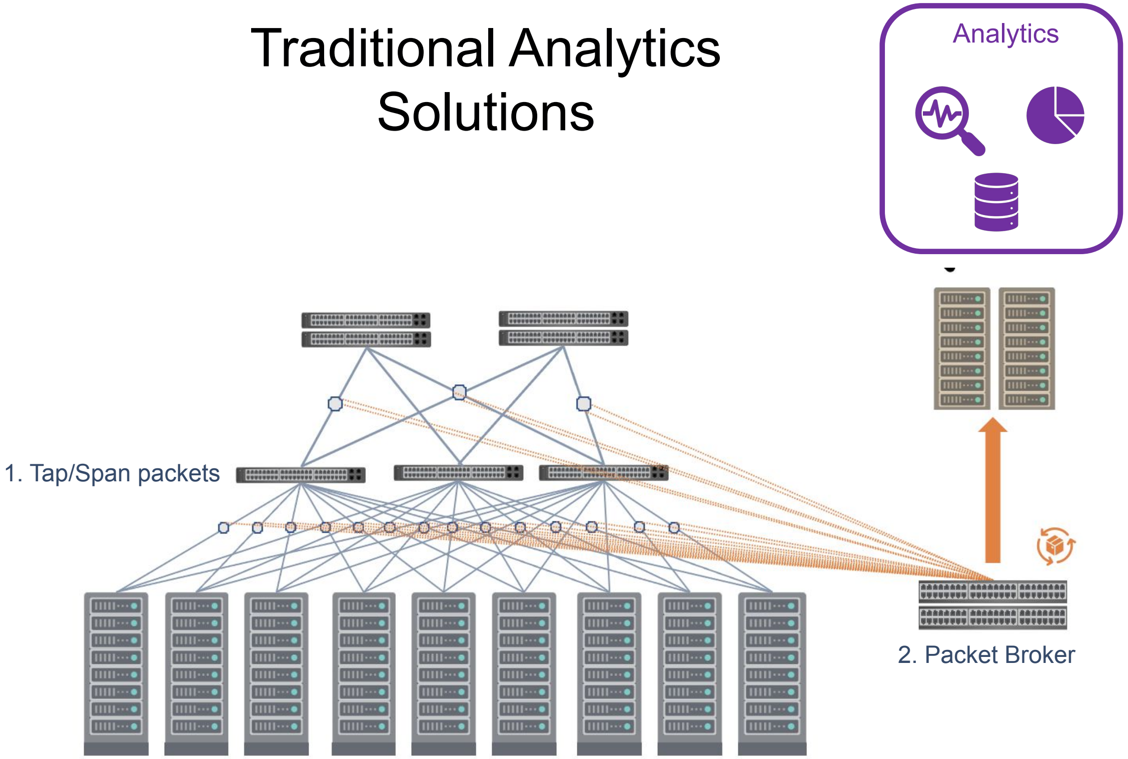
AI/ML Driven Anomaly Detection

Behavioral detection of suspicious activity threat based on traffic patterns

Transformational Network and Security Analytics

Bolted-on versus Built-in Model for Analytics

Traditional Analytics Solutions

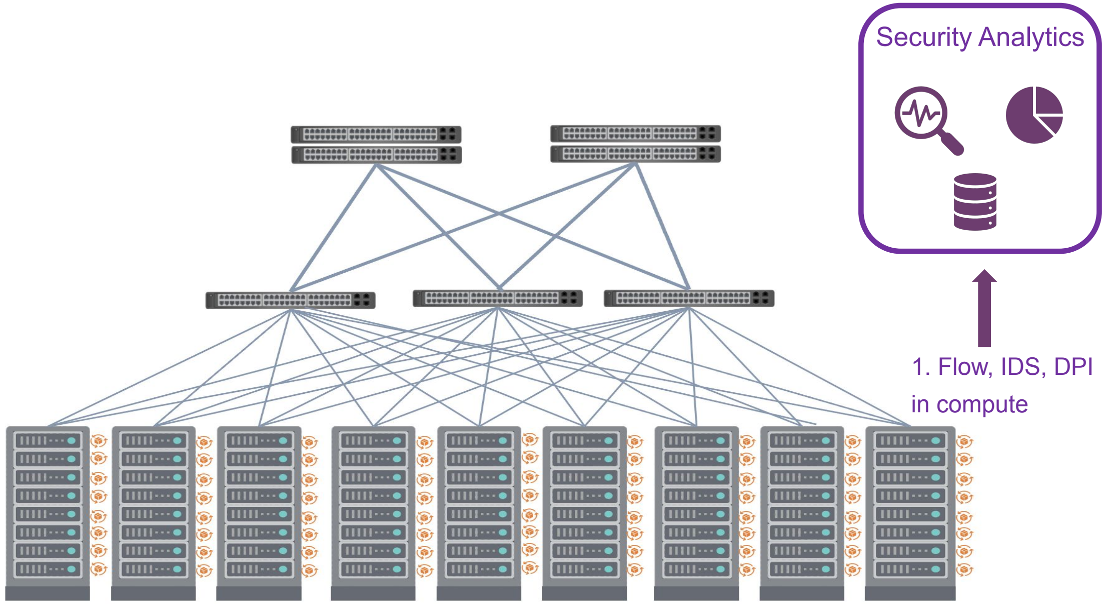


Duplicate/Mirror traffic to Analytics solutions

High Capex and Opex implications

Limited coverage due to performance and cost implications

vDefend Security Platform

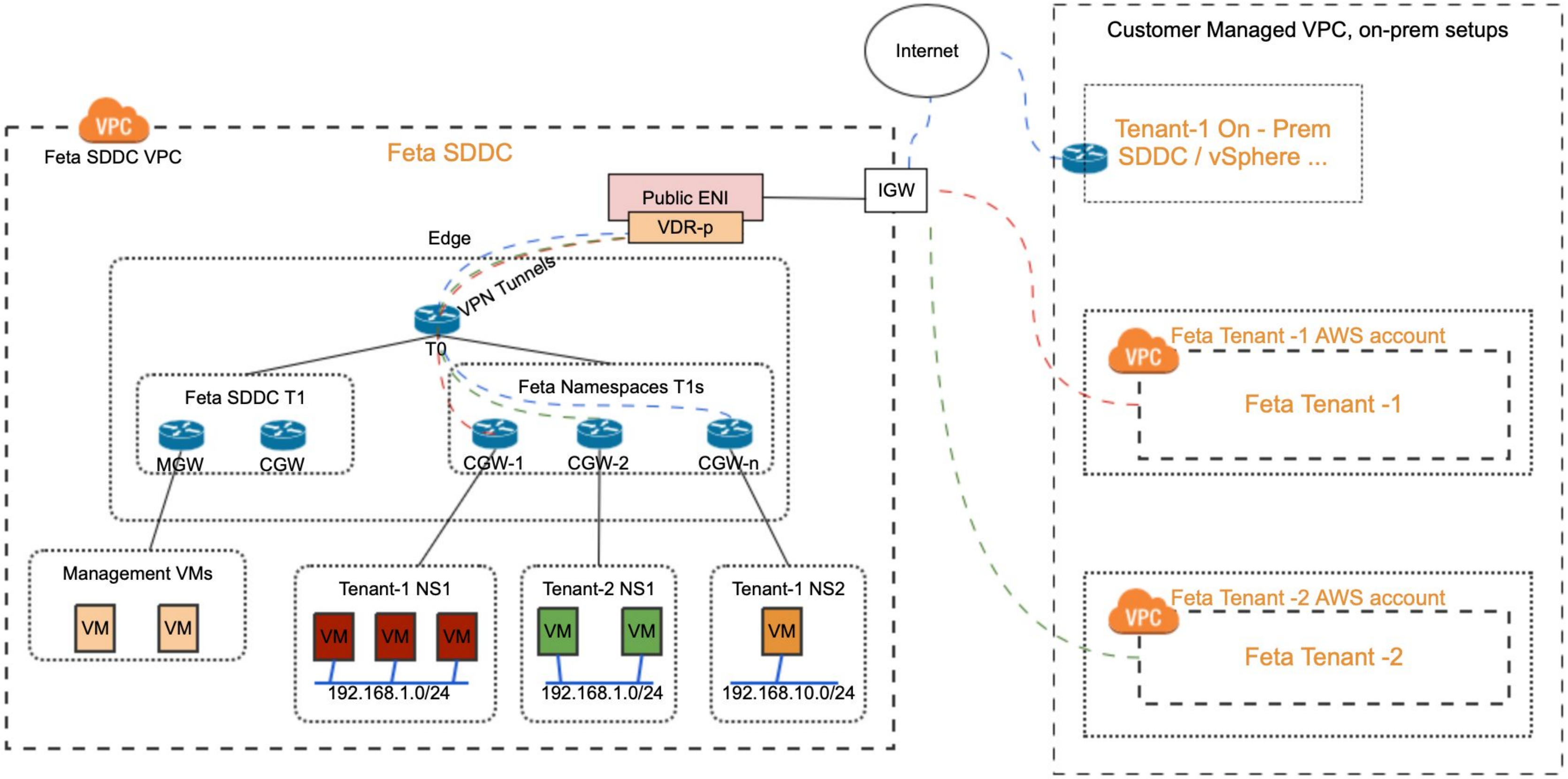


Analytics (Flows, IDS, DPI) done on each compute

No Network Changes, Taps and Packet Brokers

Complete network coverage

VMC

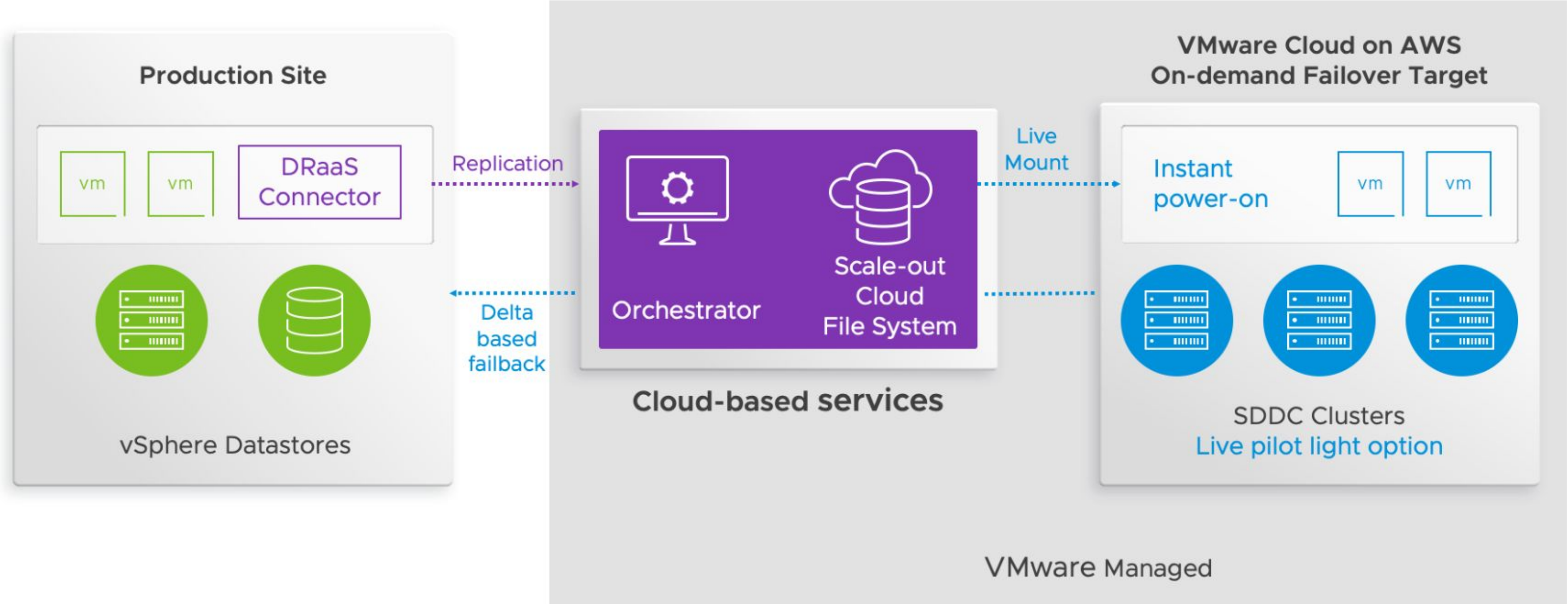


Secure workloads with DFW and GFW

NSX Tier 1 router per tenant, enforcing security and resource limits

Unified cloud and on-prem security portfolio

VMware Cloud Disaster Recovery

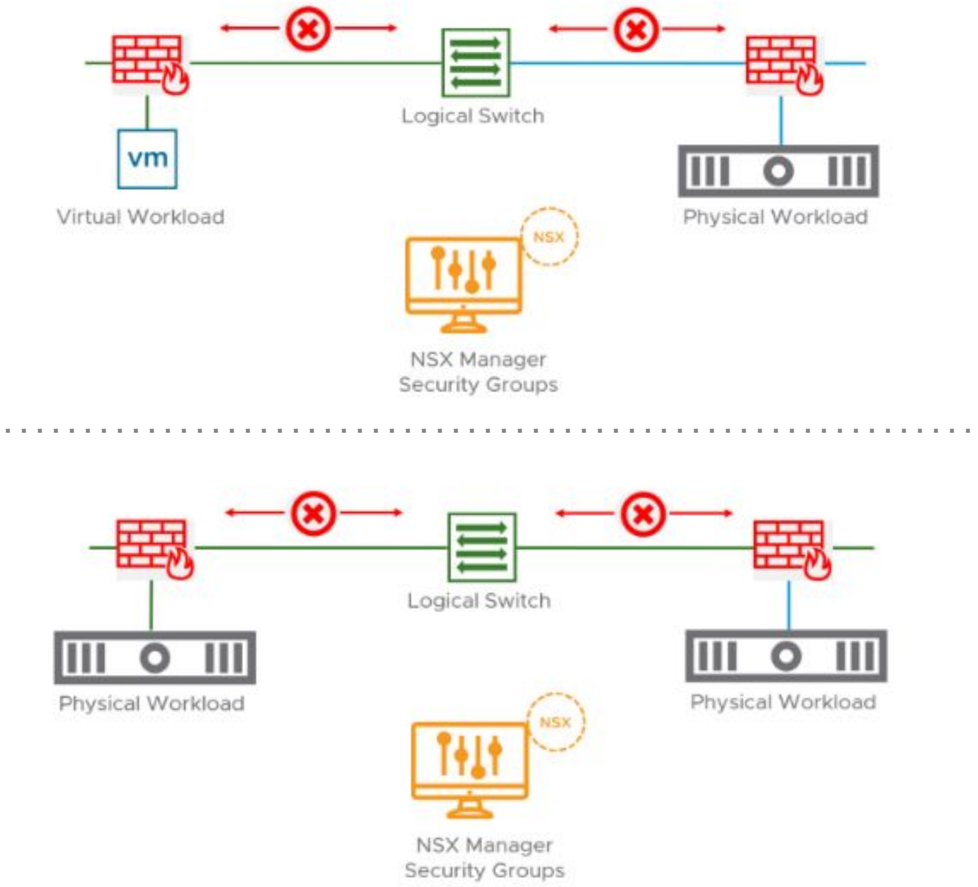


Protected Sites - and the policies that provide the coverage of your production workloads whether they are in on-premises data center locations or running in other VMC SDDCs

Scale-out Cloud File System (SCFS) - that provides the immutable, off-site recovery points for effecting the desired site failover, managed by a separate Orchestrator UI running as a service in VMware Cloud

VMC Recovery SDDC - the DR site in the cloud - for running workloads when the Protected Site has experienced a disaster

VMware vDefend Benefits Extend to Bare-metal



Filter ingress and egress traffic to and from the physical workload

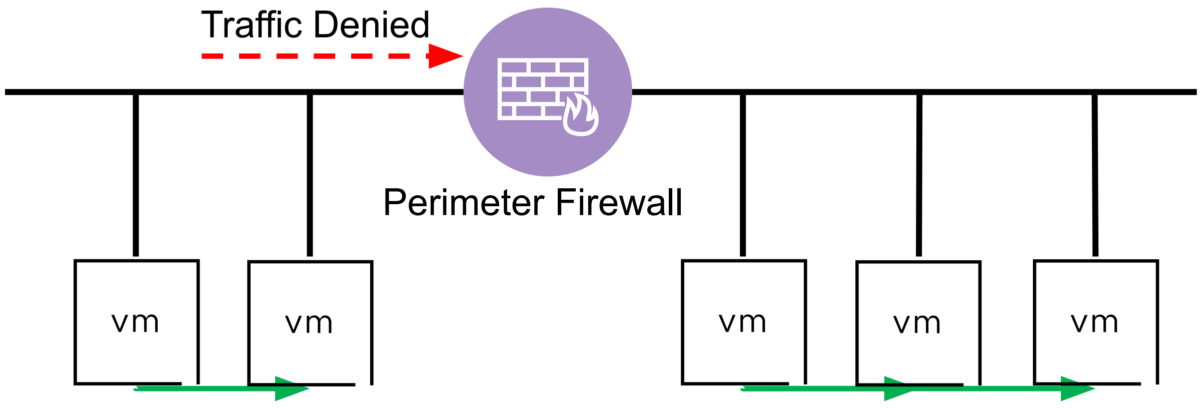
Stateful Layer 4 Firewall with OVS-Based NSX Agent inside Bare-metal OS

Unified policy management for Virtual and Physical Workloads

Traditional Perimeter Security vs VMware vDefend

Traditional Firewall	VMware Firewall
Protect Perimeter Traffic	Virtual DMZ and Internal Traffic
HW Appliance-based Architecture	Distributed Architecture
Hard to scale	Elastic
IP-based rules – complex to manage	Tag-based rules – easy to manage
Higher TCO	Lower TCO

Traditional Firewall



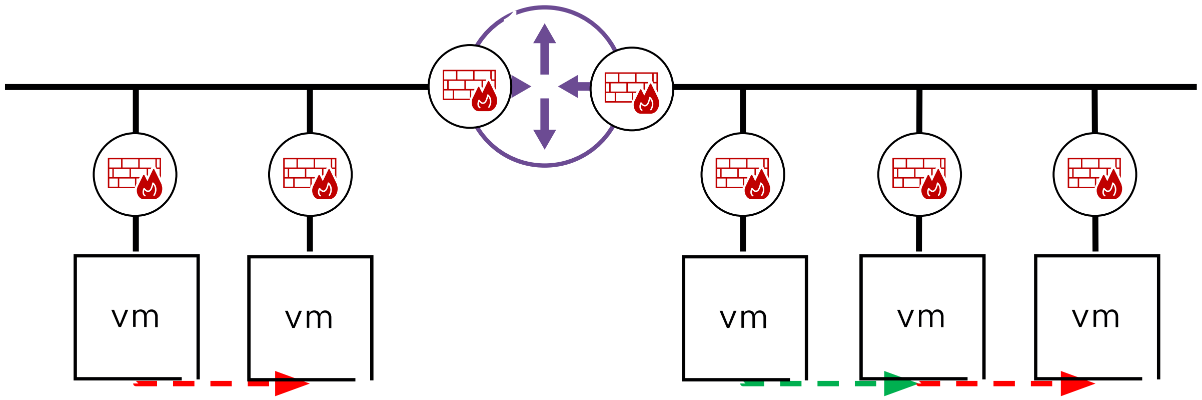
Network Design dictated and performance by security requirements

Sub-optimal traffic patterns

East/West traffic cannot be subjected to security policy

Limited visibility into East/West traffic patterns

Distributed Firewall and Gateway Firewall



East/West traffic secured at vNIC with DFW

GFW extends security to physical infrastructure and provides defense in-depth approach

Visibility into East/West traffic with Security Intelligence

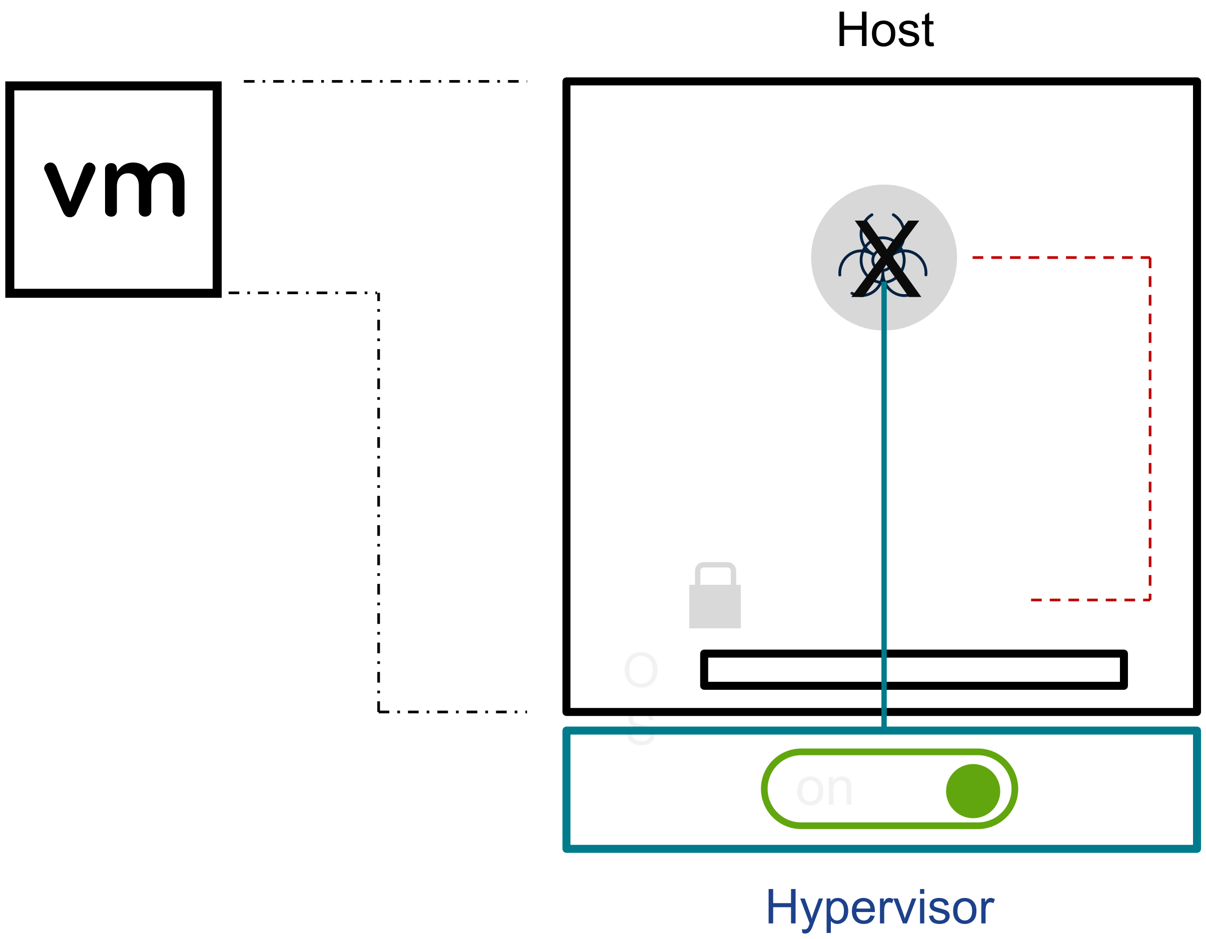
IDS/IPS, L2-L7 features provided across fabric

Agent-Based Solutions vs VMware vDefend

Agent-Based	VMware Firewall
Host OS Security Dependent	Built into the Hypervisor
Susceptible to workload compromises	Unaffected by workload compromises
Competes with application resources	Application resources unaffected
L3 to L4 functionality	L2 to L7 functionality
Limited to segmentation	Full ransomware protection

vmware® by Broadcom

Agent Based Distributed Approaches Are not Secure



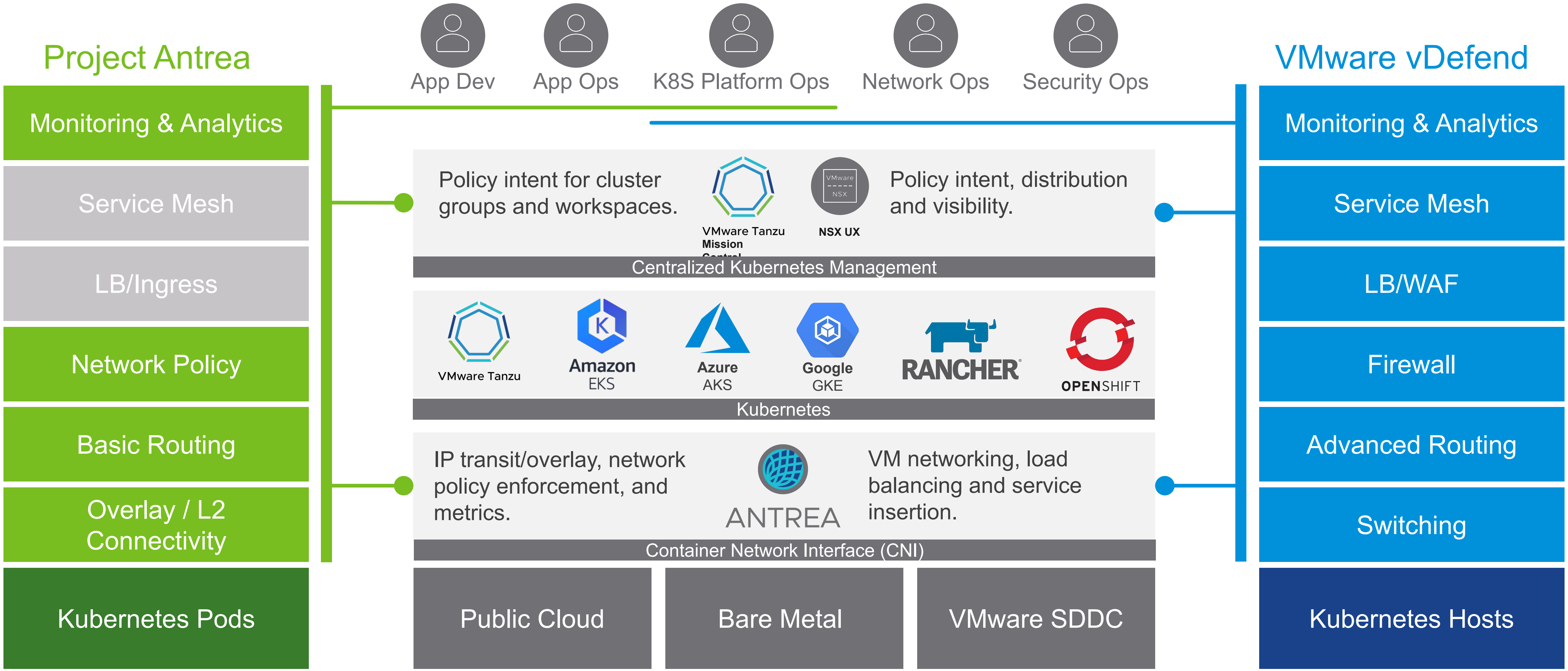
Once a threat takes hold of root, it can turn off the protection agent

Host can’t protect itself effectively

Controls intrinsic to the hypervisor are hard to subvert

Hypervisor can block the threats effectively

Antrea + vDefend = Better Together



App Dev

App Ops

K8S Platform Ops

Network Ops

Security Ops

Project Antrea

- Monitoring & Analytics
- Service Mesh
- LB/Ingress
- Network Policy
- Basic Routing
- Overlay / L2 Connectivity
- Kubernetes Pods

VMware vDefend

- Monitoring & Analytics
- Service Mesh
- LB/WAF
- Firewall
- Advanced Routing
- Switching
- Kubernetes Hosts

Policy intent for cluster groups and workspaces.

VMware Tanzu Mission Control

NSX UX

Policy intent, distribution and visibility.

Centralized Kubernetes Management

VMware Tanzu

Amazon EKS

Azure AKS

Google GKE

RANCHER

OPENSHIFT

Kubernetes

IP transit/overlay, network policy enforcement, and metrics.

ANTREA

VM networking, load balancing and service insertion.

Container Network Interface (CNI)

Public Cloud

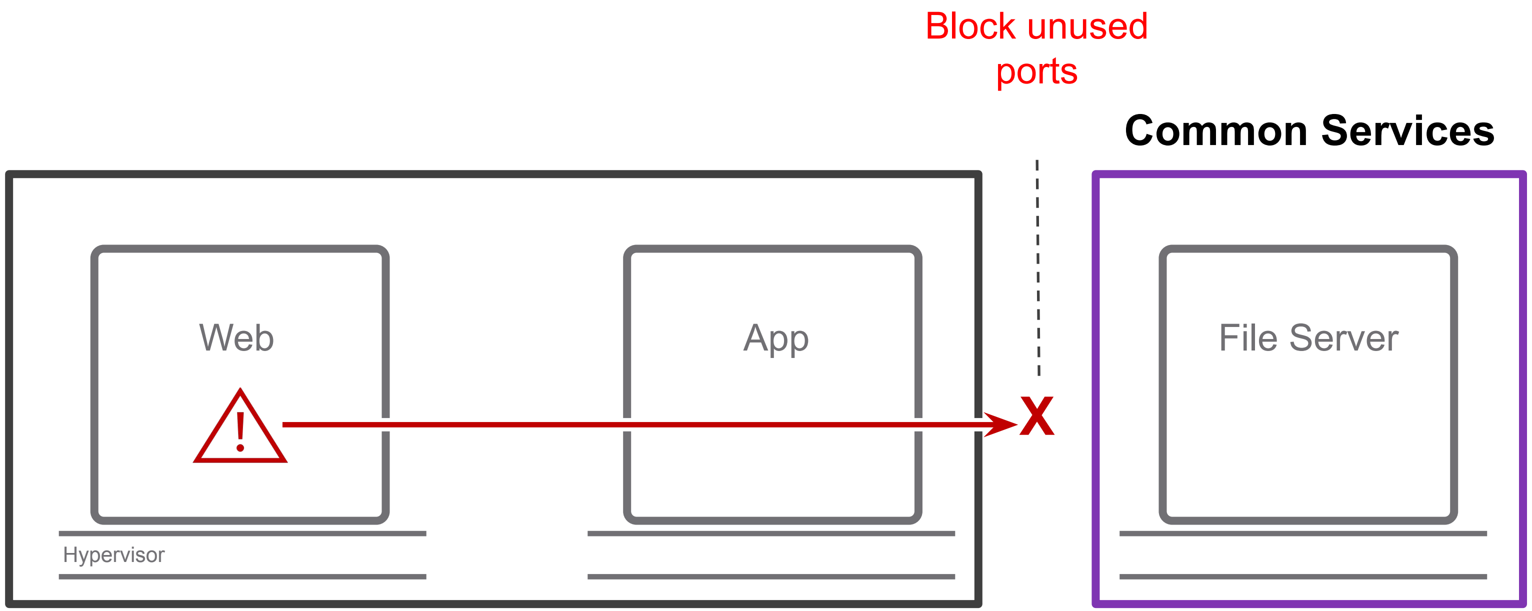
Bare Metal

VMware SDDC

Segmentation Use-Cases

Secure Infrastructure	Secure Virtual Zones	Secure Apps	Compliance
• SIEM		• Automotive	

vDefend Distributed Firewall and Gateway Firewall

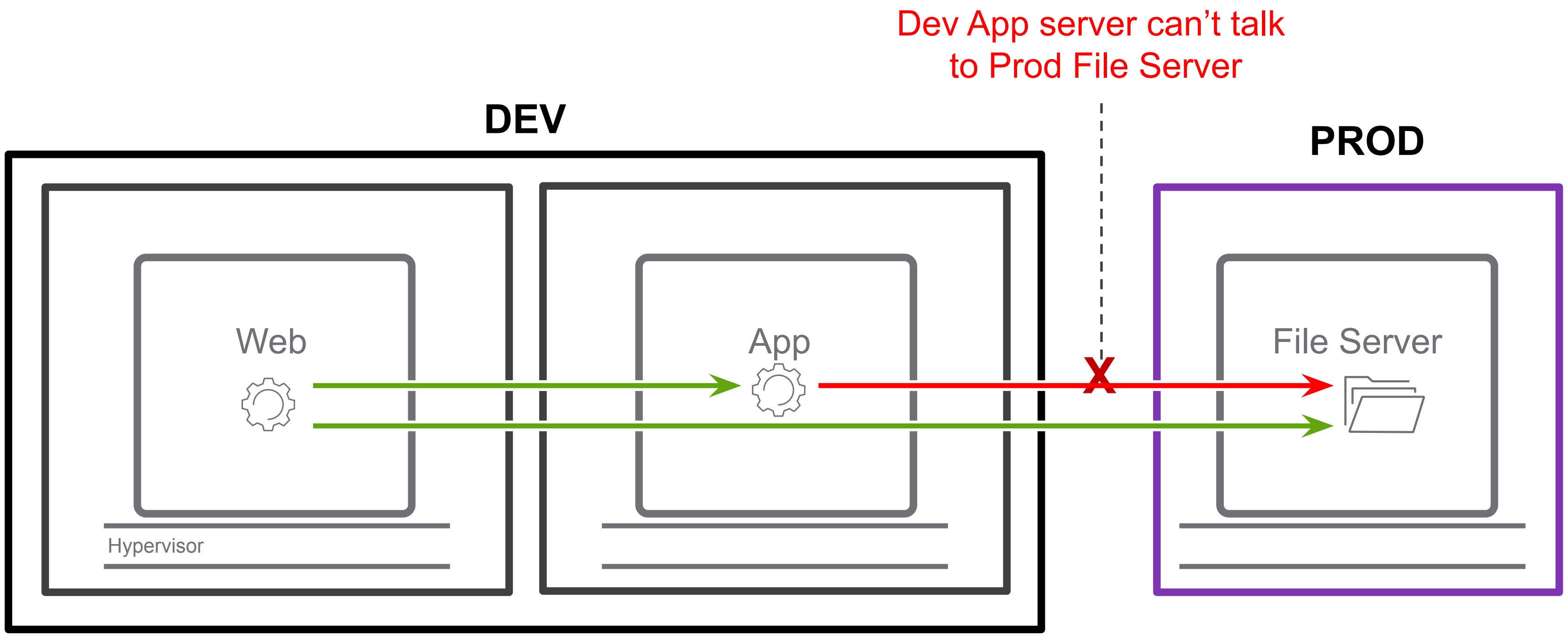


Secure Infrastructure

Secure Virtual Zones

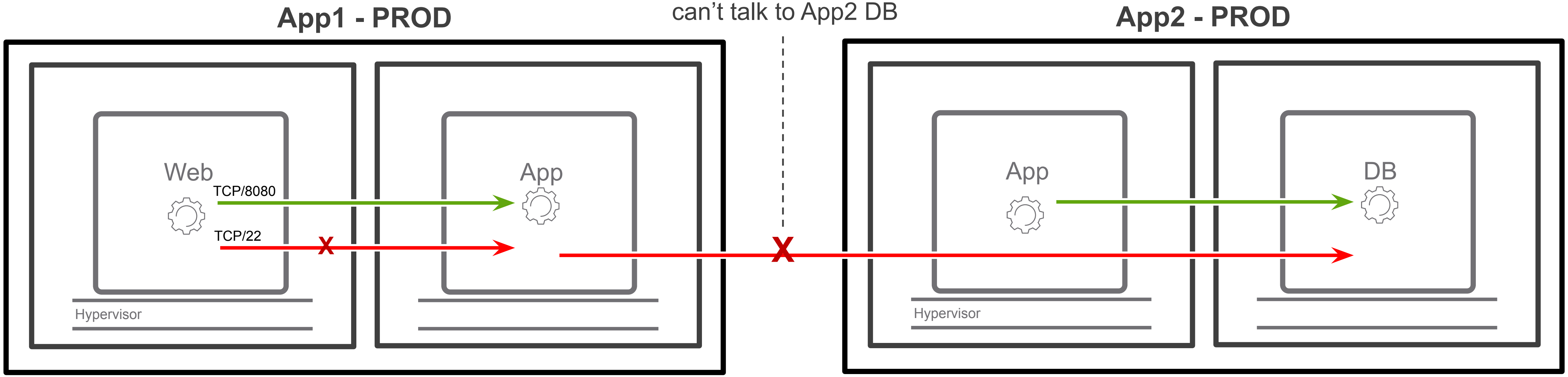
Secure Apps

Compliance



Secure Infrastructure | Secure Virtual Zones | Secure Apps | Compliance

App1 middleware
can't talk to App2 DB



App1 - PROD

App2 - PROD

Web

TCP/8080

TCP/22

App

Hypervisor

App

DB

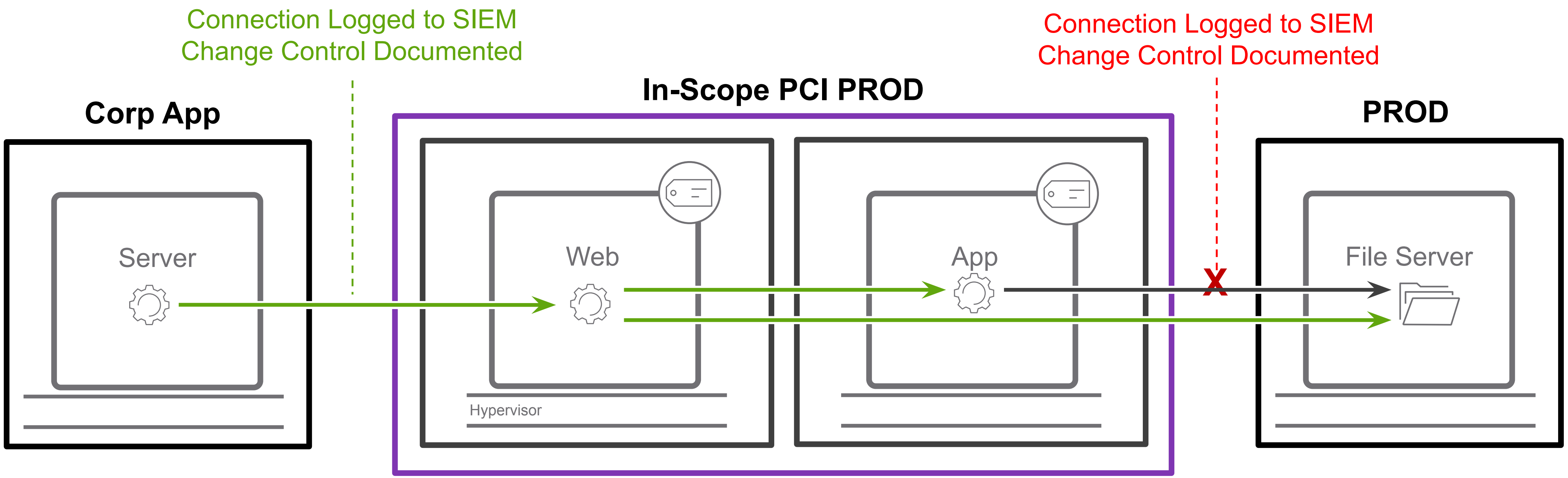
Hypervisor

Secure Infrastructure

Secure Virtual Zones

Secure Apps

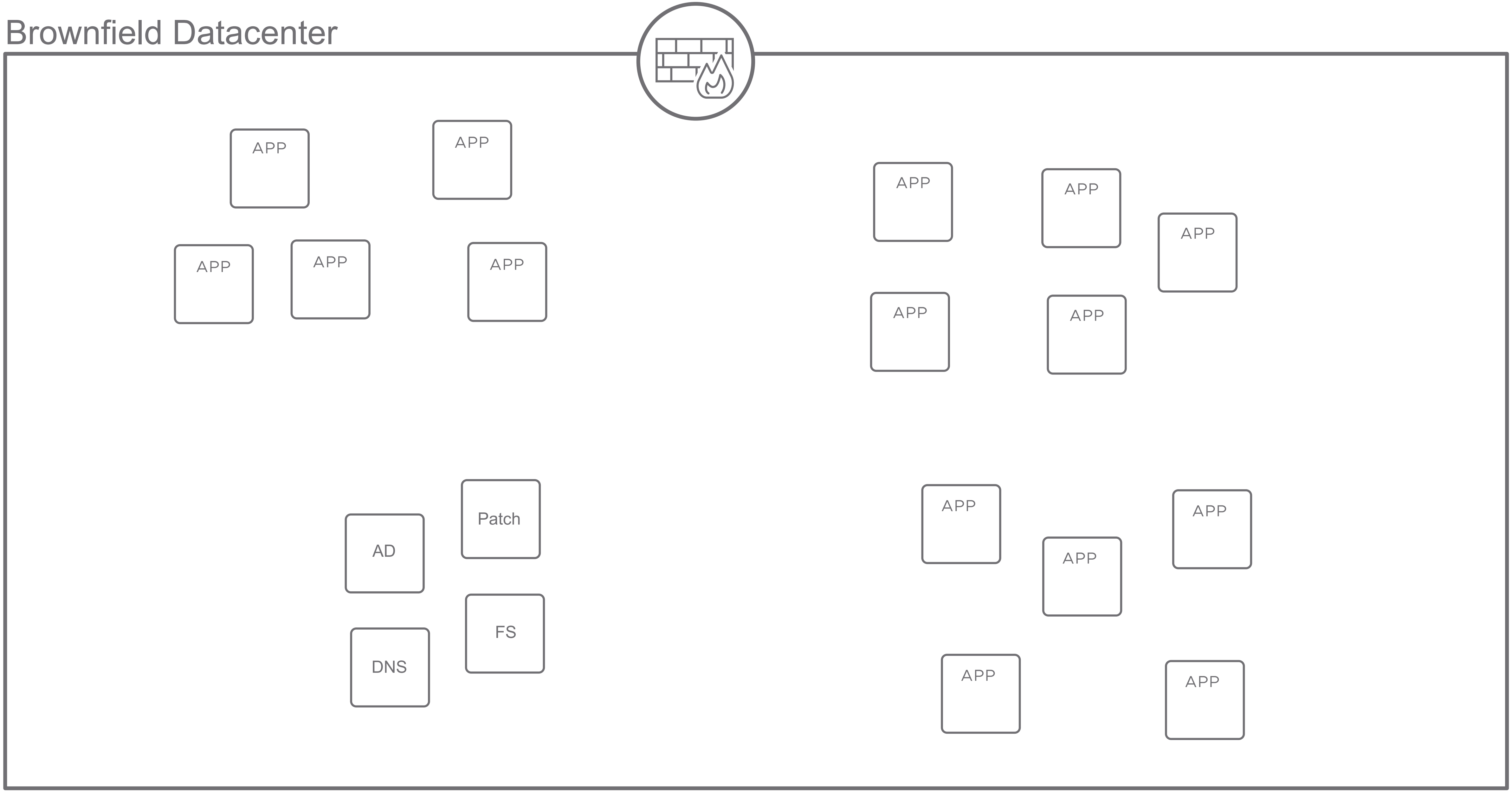
Compliance


Connection Logged to SIEM
Change Control Documented
Connection Logged to SIEM
Change Control Documented
Corp App
In-Scope PCI PROD
PROD
Server
Web
App
File Server
X
Hypervisor

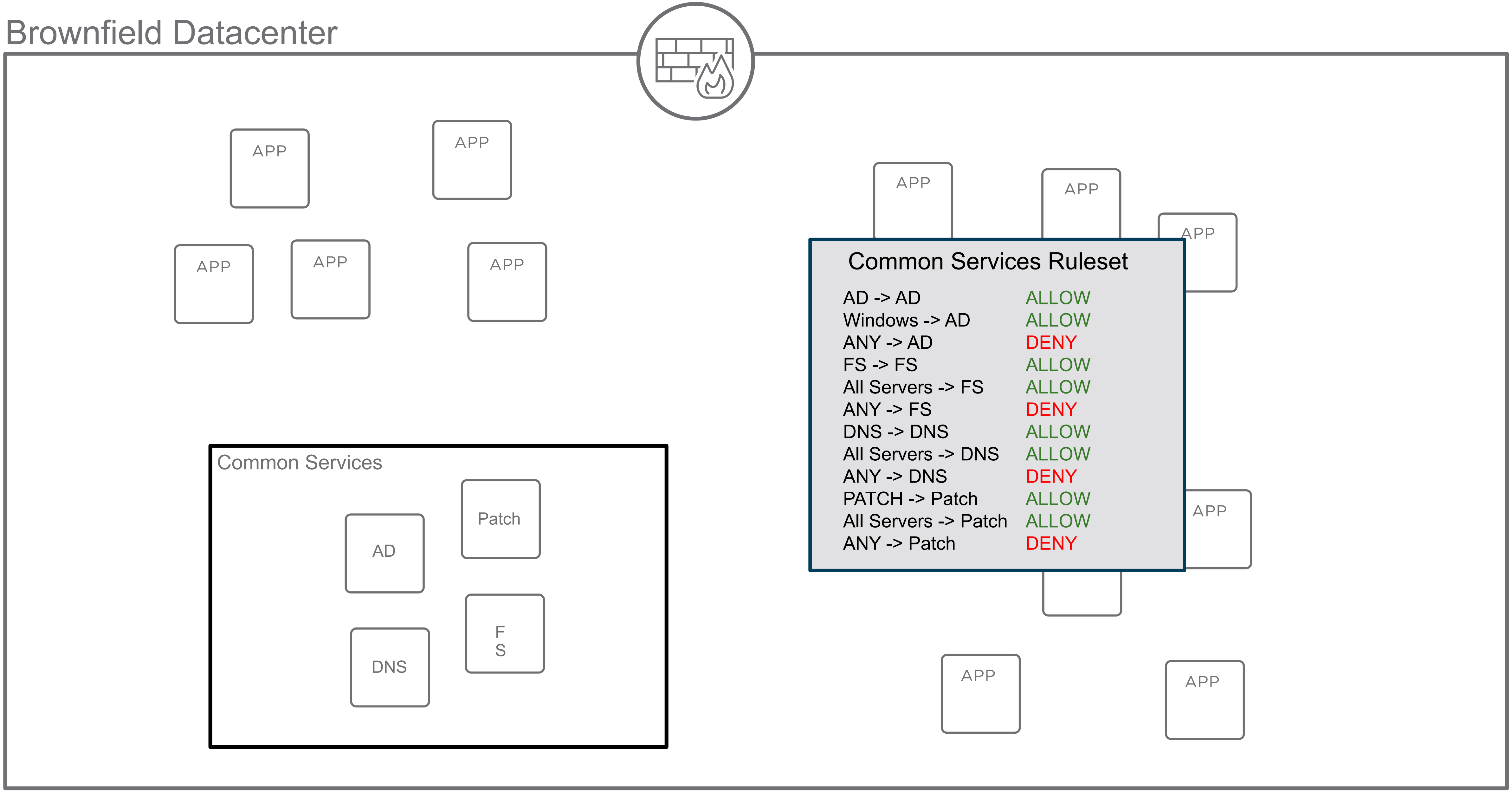
Secure Infrastructure | Secure Virtual Zones | Secure Apps | Compliance

Lateral Security in a Brownfield Environment

Brownfield Datacenter



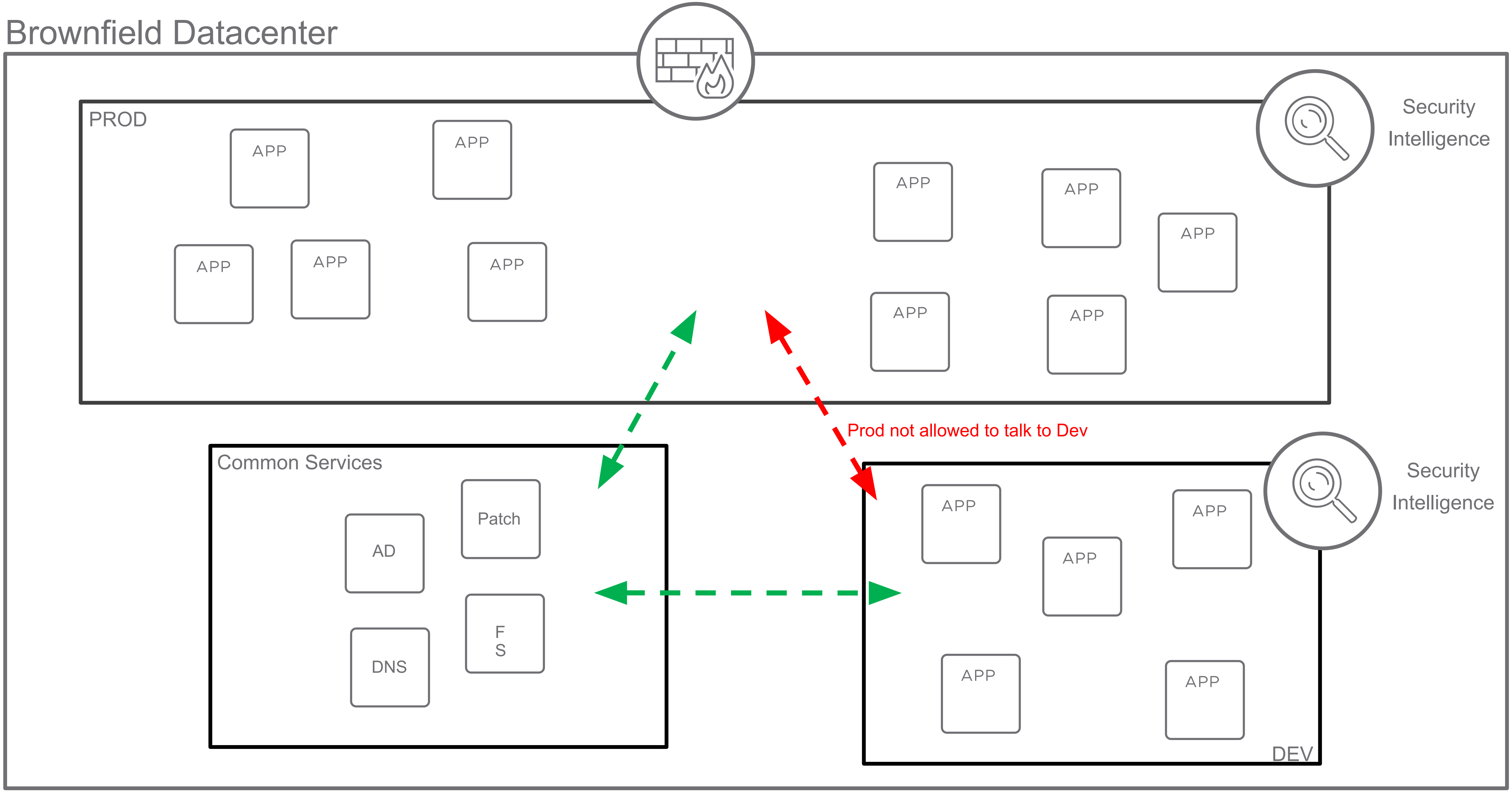
Brownfield Datacenter



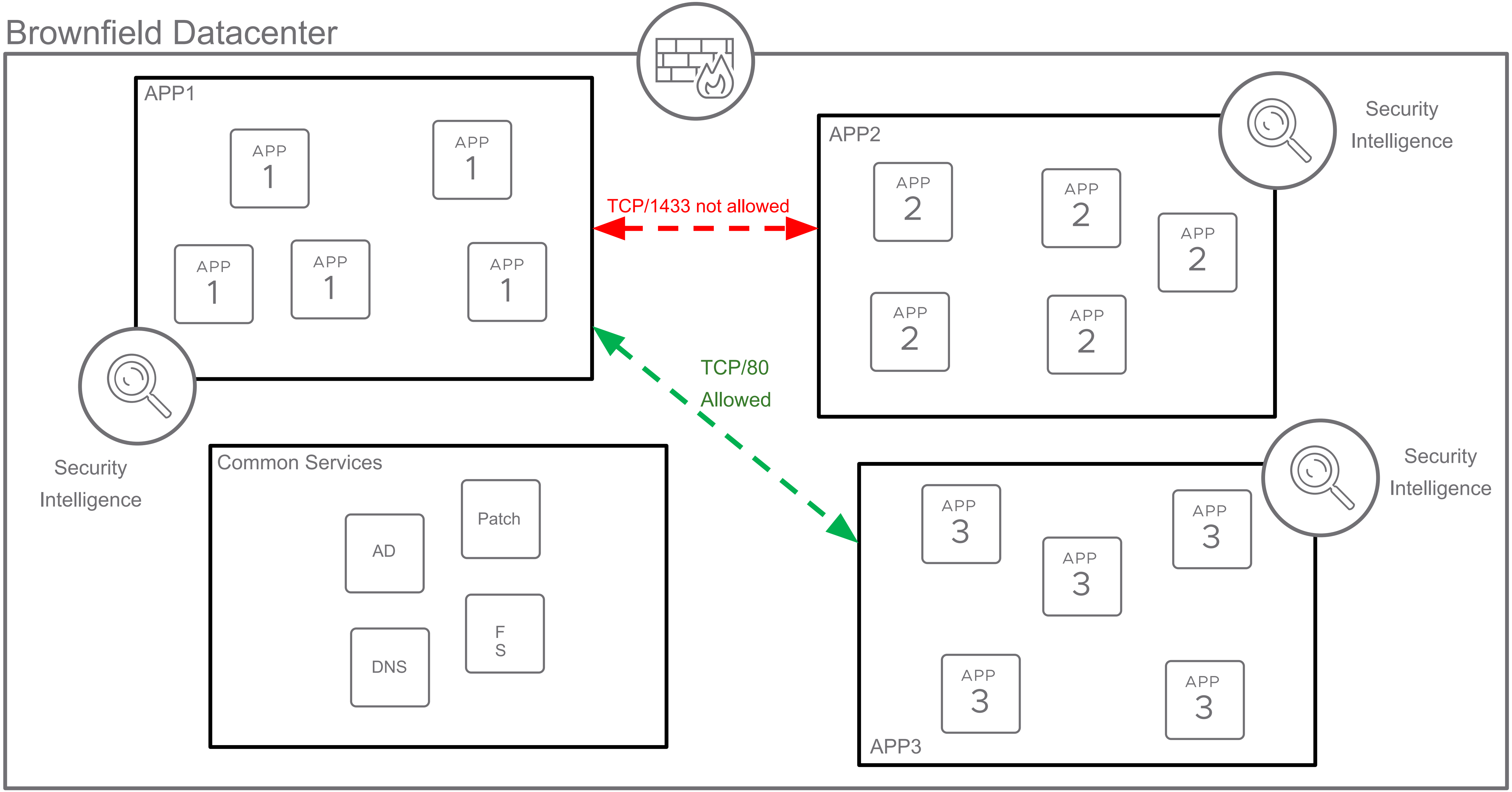
Common Services Ruleset

AD -> AD	ALLOW
Windows -> AD	ALLOW
ANY -> AD	DENY
FS -> FS	ALLOW
All Servers -> FS	ALLOW
ANY -> FS	DENY
DNS -> DNS	ALLOW
All Servers -> DNS	ALLOW
ANY -> DNS	DENY
PATCH -> Patch	ALLOW
All Servers -> Patch	ALLOW
ANY -> Patch	DENY

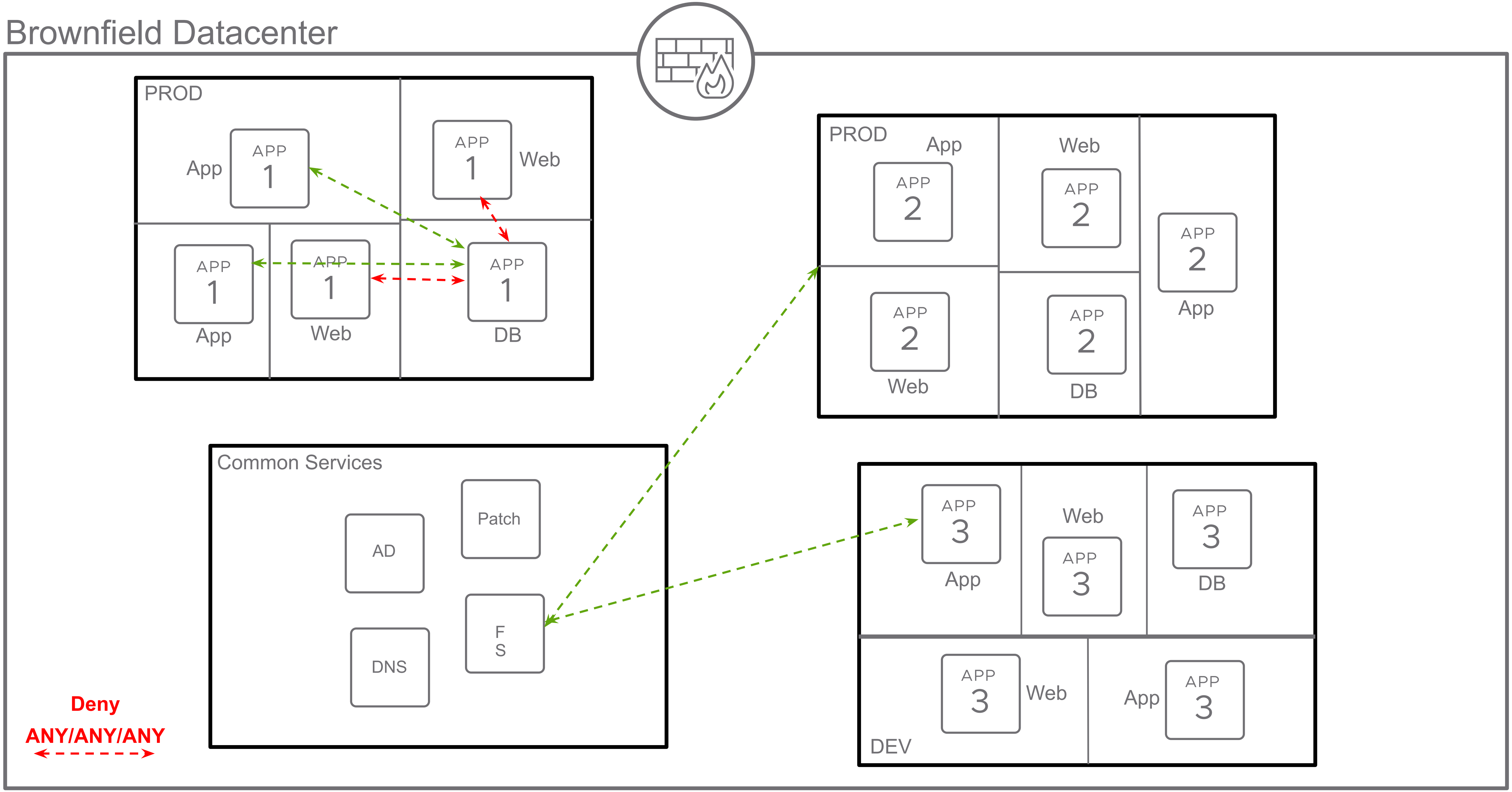
Brownfield Datacenter



Brownfield Datacenter

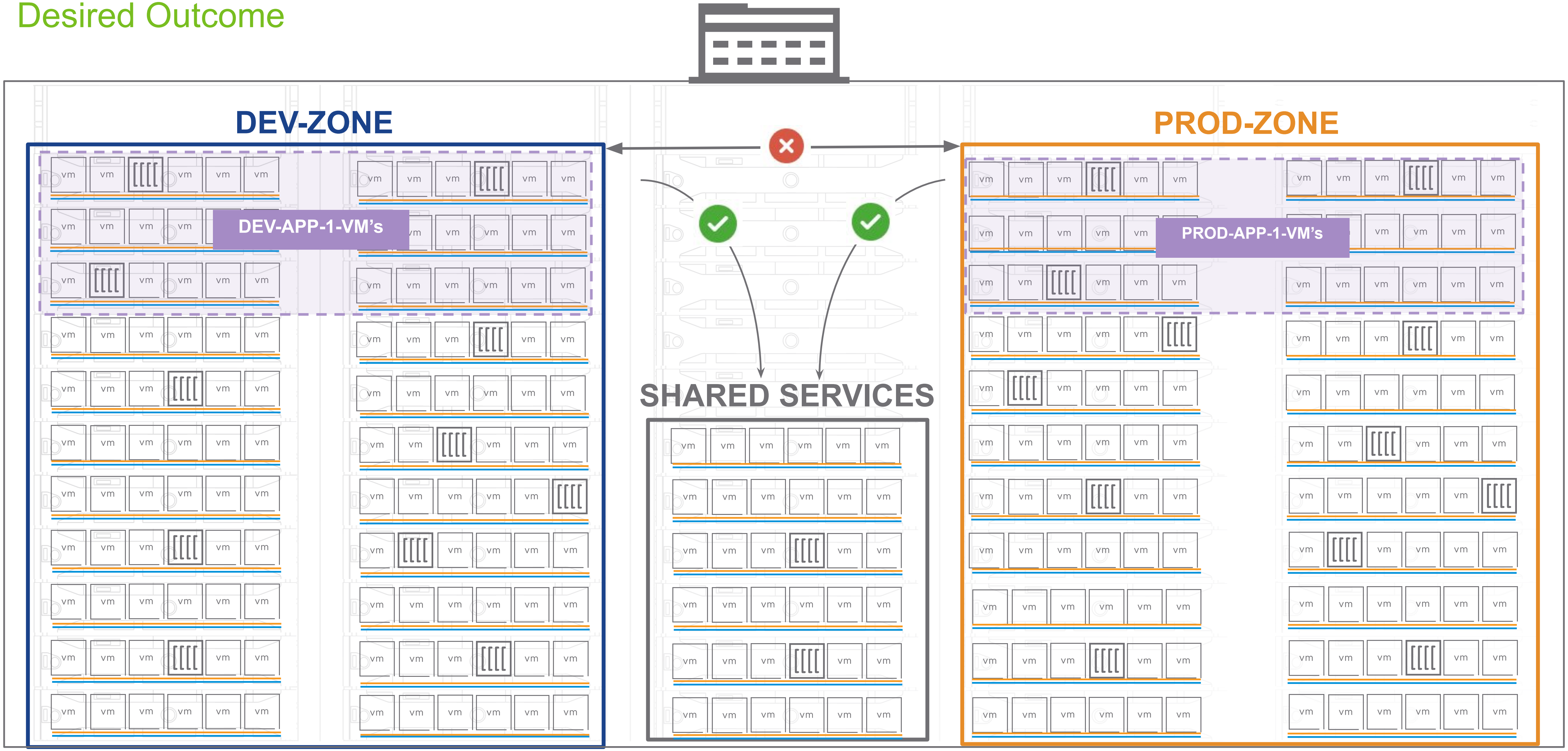


Brownfield Datacenter



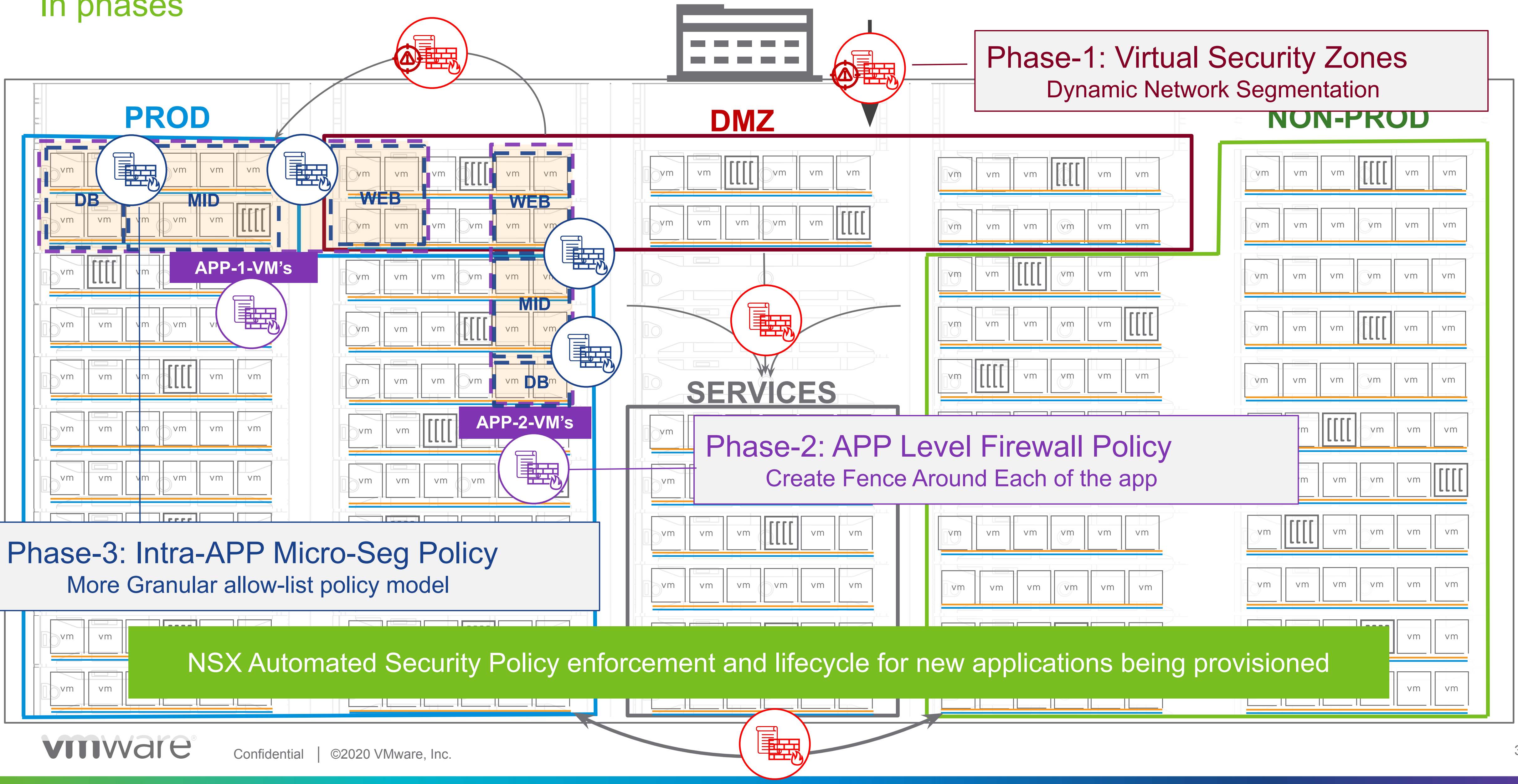
Vmware Distributed Firewall Use Cases

Desired Outcome



Vmware Distributed Firewall Use Cases

In phases



Phase-1: Virtual Security Zones
Dynamic Network Segmentation

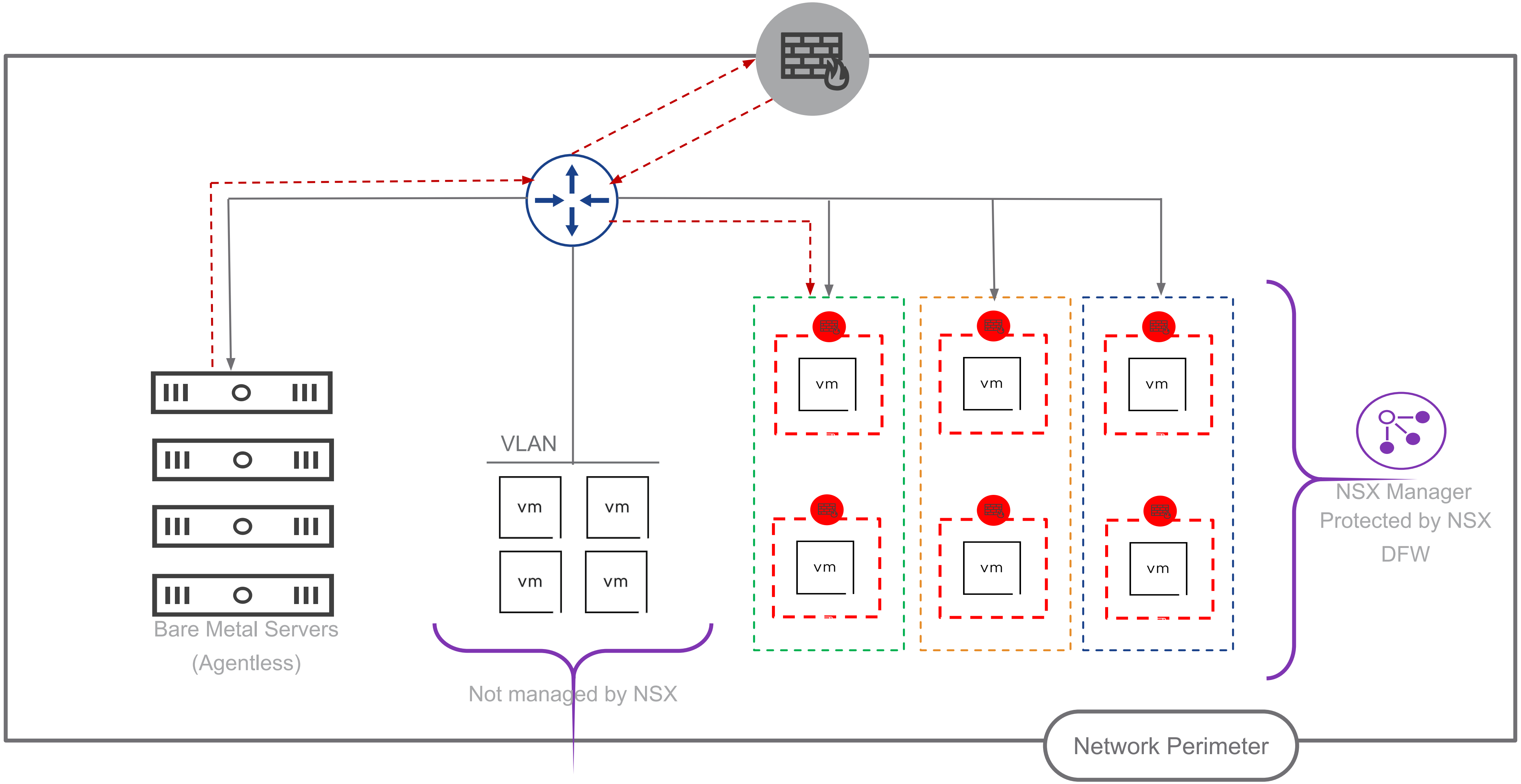
Phase-2: APP Level Firewall Policy
Create Fence Around Each of the app

Phase-3: Intra-APP Micro-Seg Policy
More Granular allow-list policy model

NSX Automated Security Policy enforcement and lifecycle for new applications being provisioned

Physical and Virtual Infrastructure coexist in the datacenter

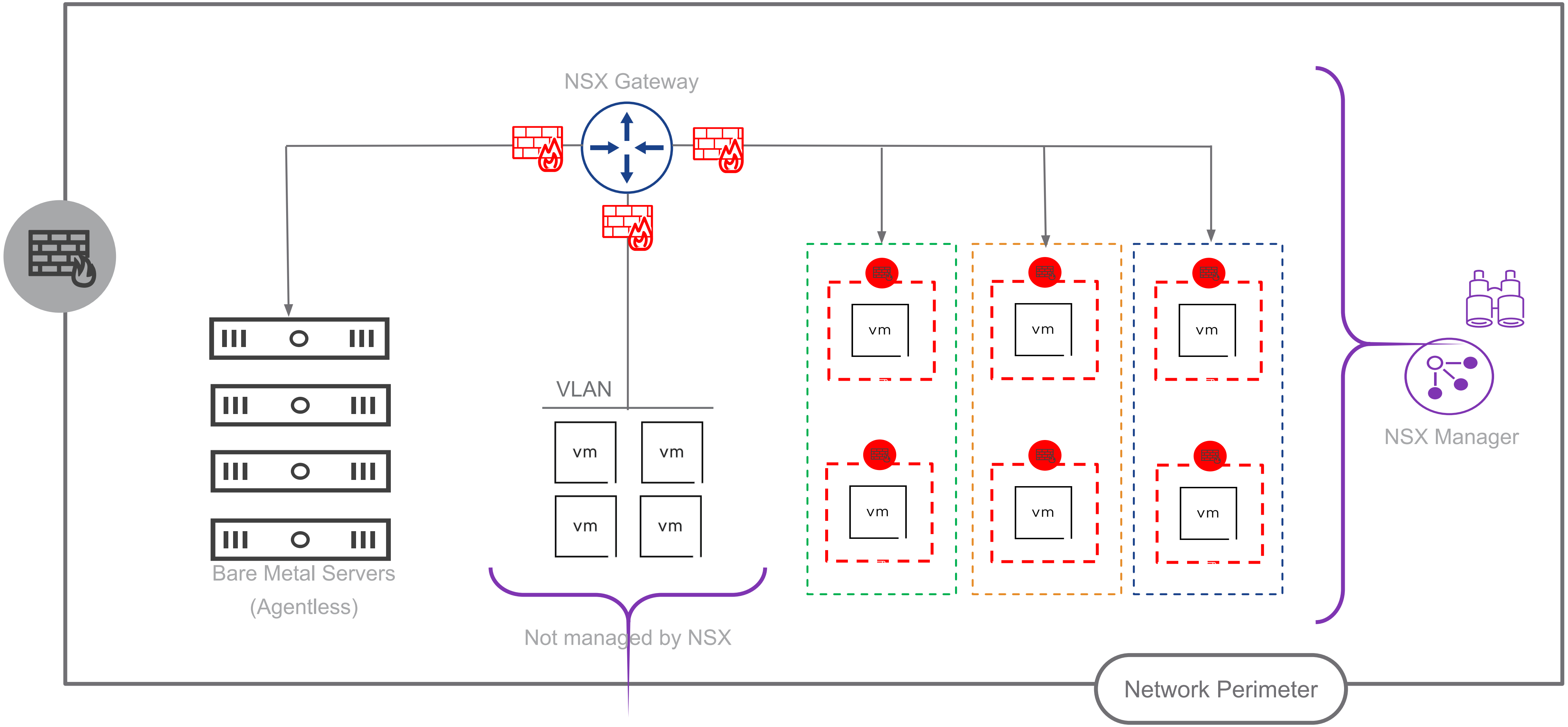
All traffic between Physical and Virtual Infrastructure will need to be hairpinned to perimeter FW



Gateway Firewall is a service available on the NSX Gateway

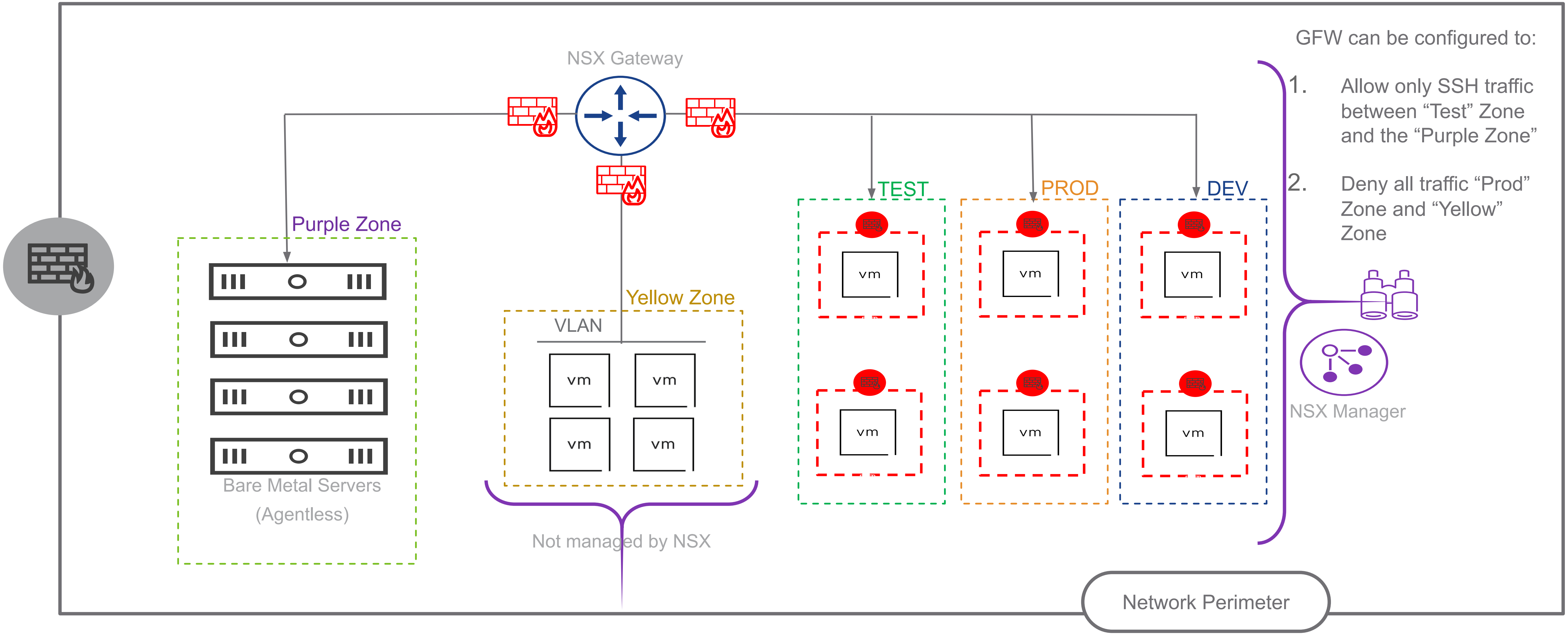
NSX Gateway provides connectivity between Physical and Virtual Infrastructure

GFW rules leverage tags to enforce firewall policies between virtual machines and physical servers



Gateway Firewall is a service available on the NSX Gateway

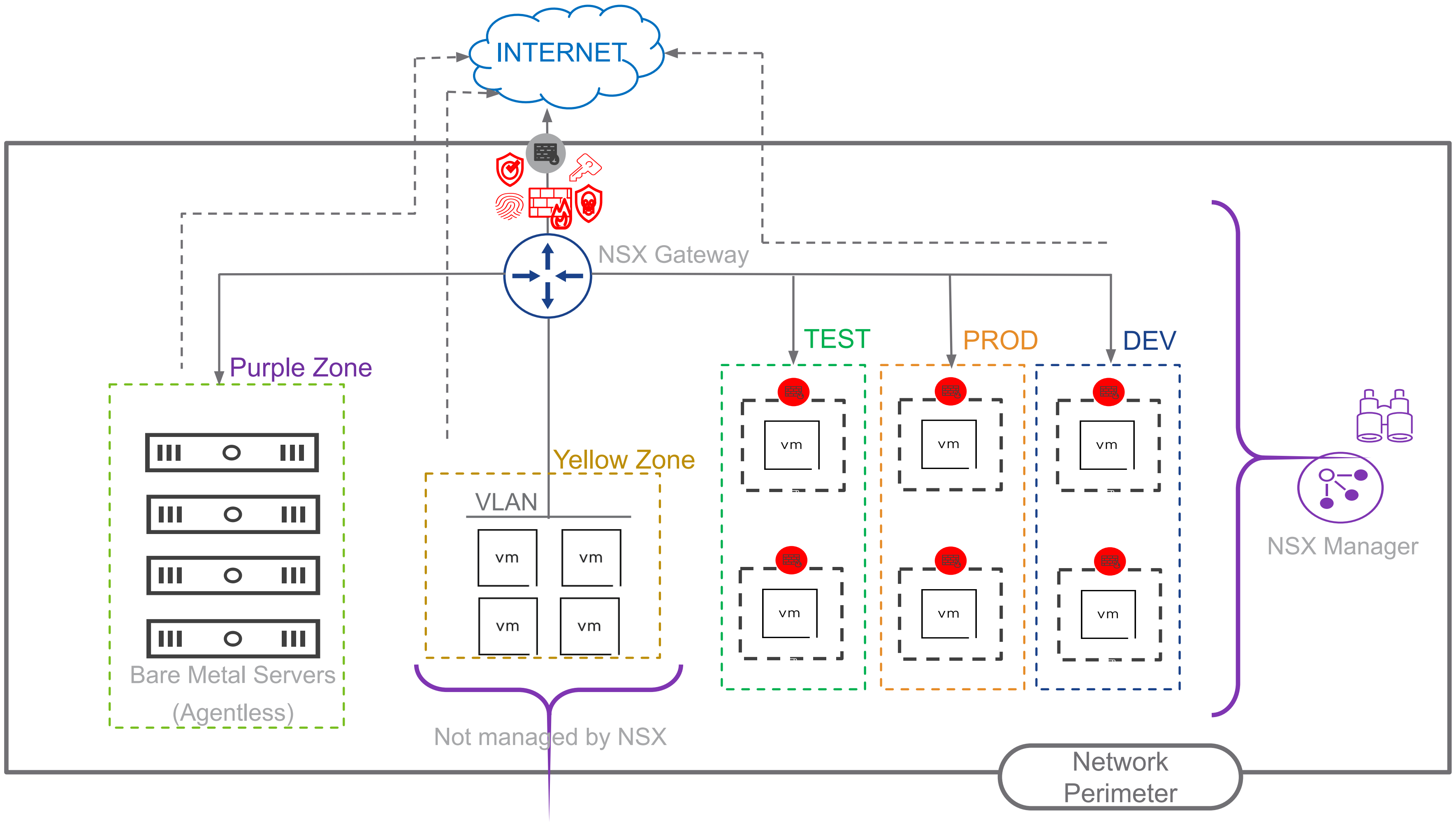
GFW rules leverage tags to enforce firewall policies between virtual machines and physical servers



GFW can be configured to:

1. Allow only SSH traffic between "Test" Zone and the "Purple Zone"
2. Deny all traffic "Prod" Zone and "Yellow" Zone

Gateway Firewall is critical to protect N<->S Traffic

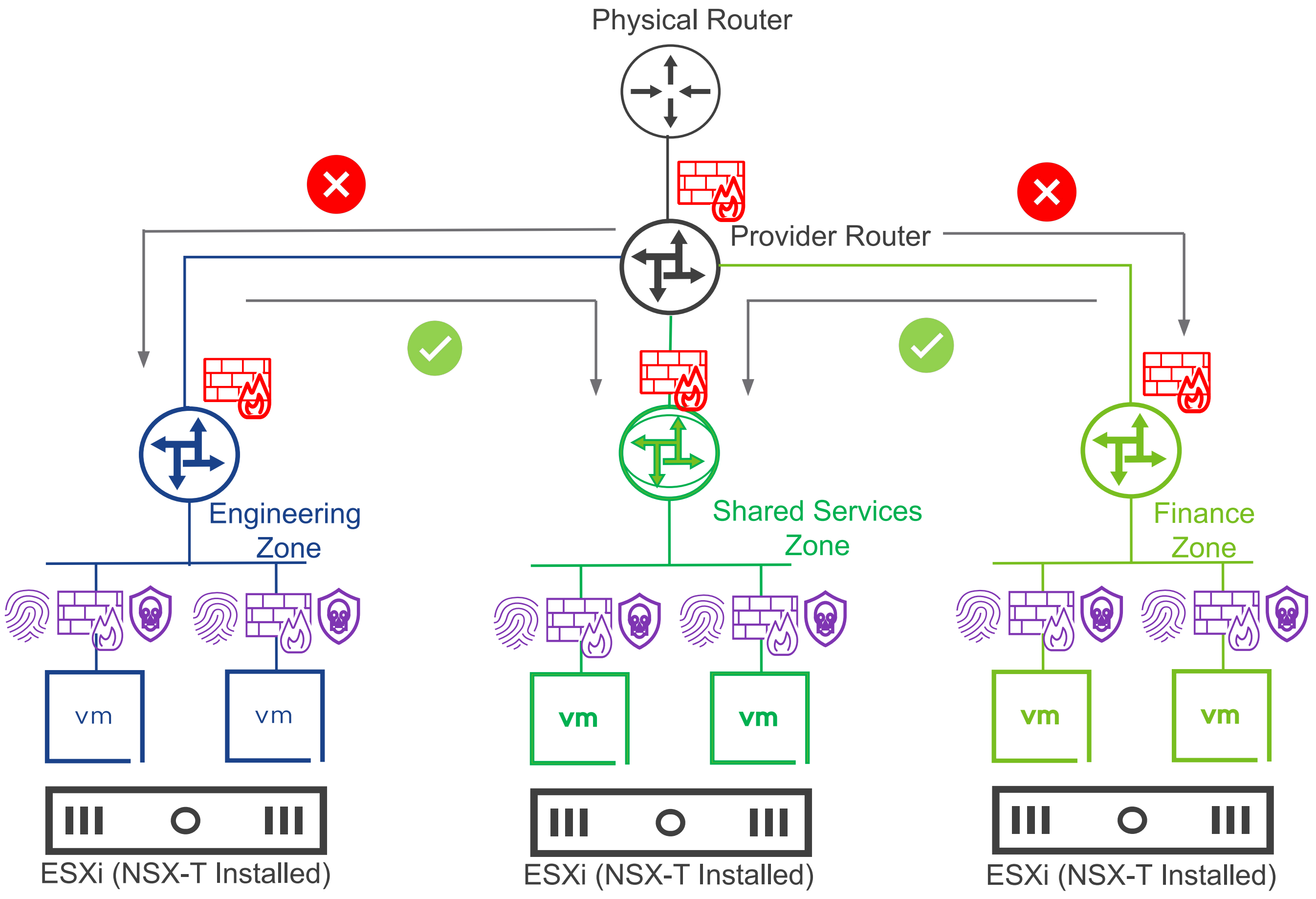


All outbound traffic from both Physical Servers and Virtual Infrastructure are now protected by Gateway Security [which includes the following features]:

- Firewall
- Intrusion Detection & Prevention
- Malware Detection
- TLS Inspection
- URL Filtering

Inter Tenant Filtering using GFW

Gateway security for zoning with network virtualization



GFW can be leveraged to implement multiple zones/tenants within an Enterprise or for a Service Provider

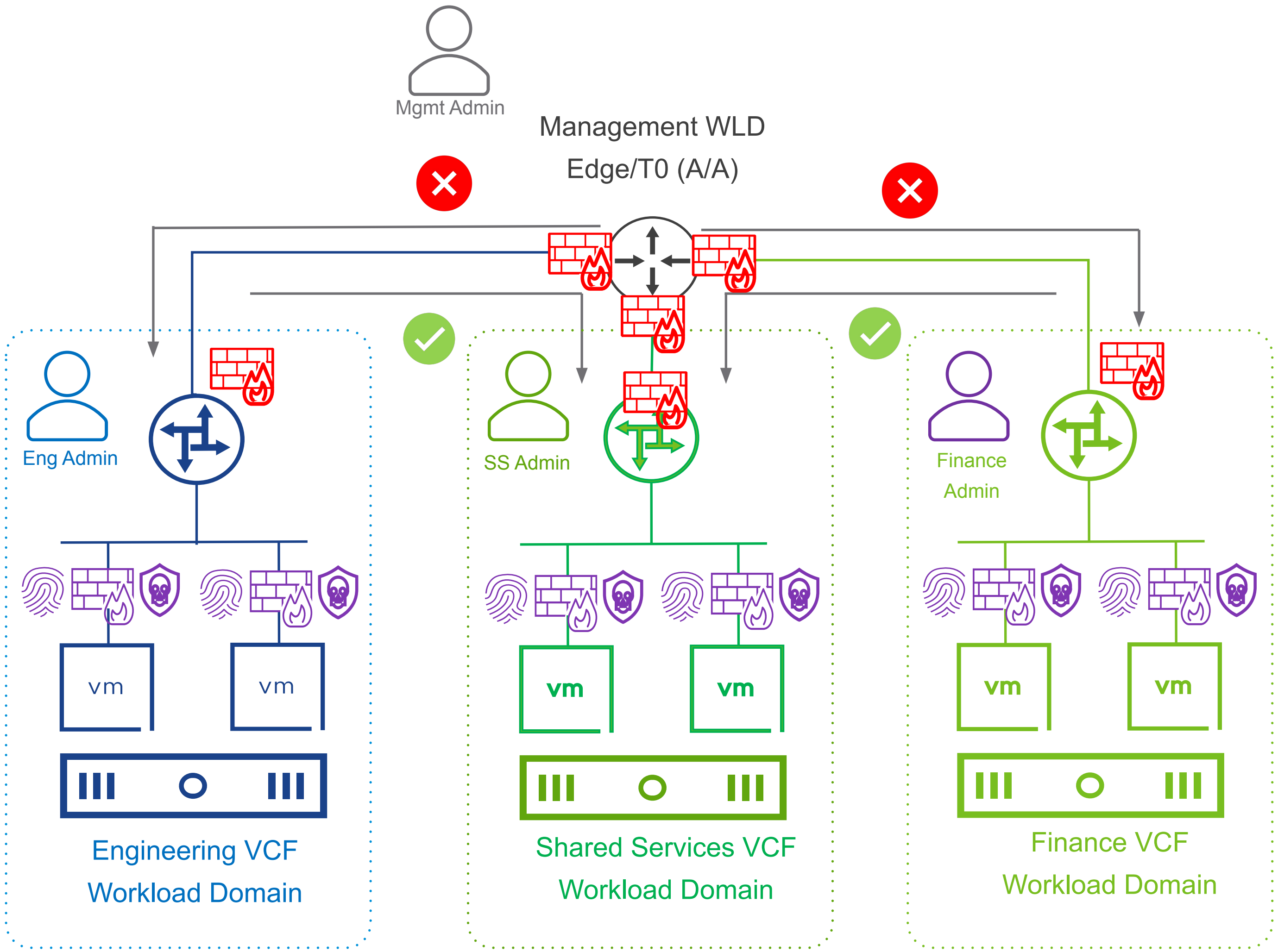
GFW rules can be configured to allow traffic between zones that are required to communicate and block all other traffic.

GFW continues to protect all Outbound Traffic from all the tenants.

Additional Layer of Security that can be used in conjunction with DFW for Defense in Depth

Inter-WLD Filtering using GFW

Gateway security for WLD zoning



GFW can be leveraged to implement multiple zones/tenants within an VCF domain

Mgmt WLD Persona sets GFW rules to allow traffic between WLD that are required to communicate and block all other traffic.(IP based)

VI WLD Personas can configure additional GFW rules on their own WLD

VI WLD Personas can provide an additional Layer of Security (intra) with DFW, Distributed IDPS, Malware Prevention for Defense in Depth

Lateral Security in a Greenfield Environment

Development of a new application

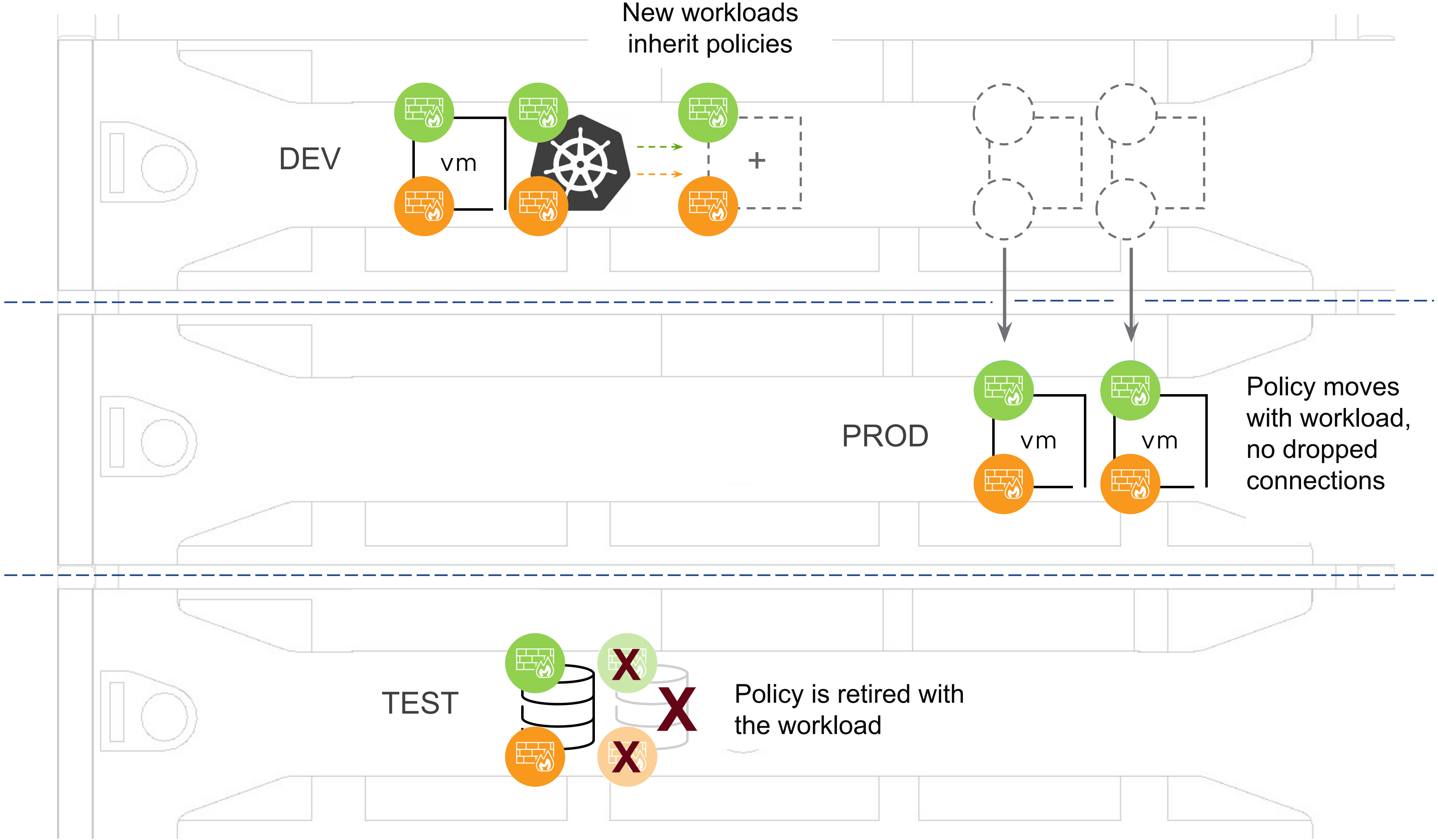
Developers focus on WRITING CODE!

Self-Service to allow Developers to configure infra

Policy applied to secure newly deployed app

Segmentation

Tying the lifecycle of a security policy to the lifecycle of an application



New workloads inherit policies
DEV
vm
+
PROD
vm
vm
Policy moves with workload, no dropped connections
TEST
X
Policy is retired with the workload

Securing Virtual Infrastructure Workload Domains

Highlighted Use Cases

Secure Zones

Gateway or Distributed Firewall

Between WLDs or within a WLD

Create network-based or network-agnostic zones/environments (i.e. dev/test/prod/compliance)

Isolated zones or provide controlled zone access

Secure Apps

DFW and Security Intelligence

Minimize the blast radius/attack surface

Zero-Trust model for Network Security

Align security policy lifecycle with application lifecycle

Ransomware Protection & Threat Investigation

Advanced Threat Prevention

Prevent exploits and extend patching cycles with Virtual Patching

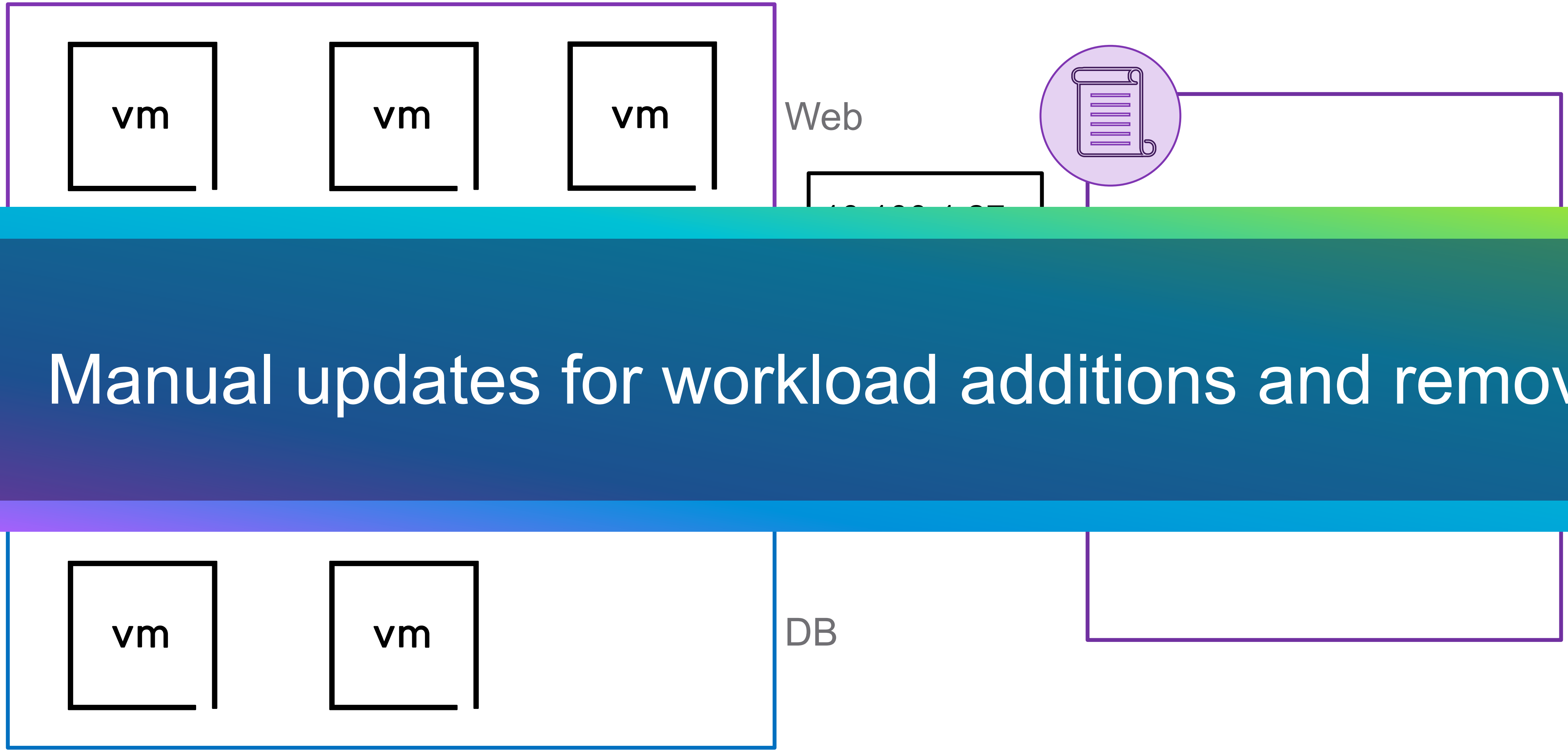
Detect & Prevent evasive malware

Prioritize and correlate threats into actionable campaigns

Security across Sites with NSX Federation

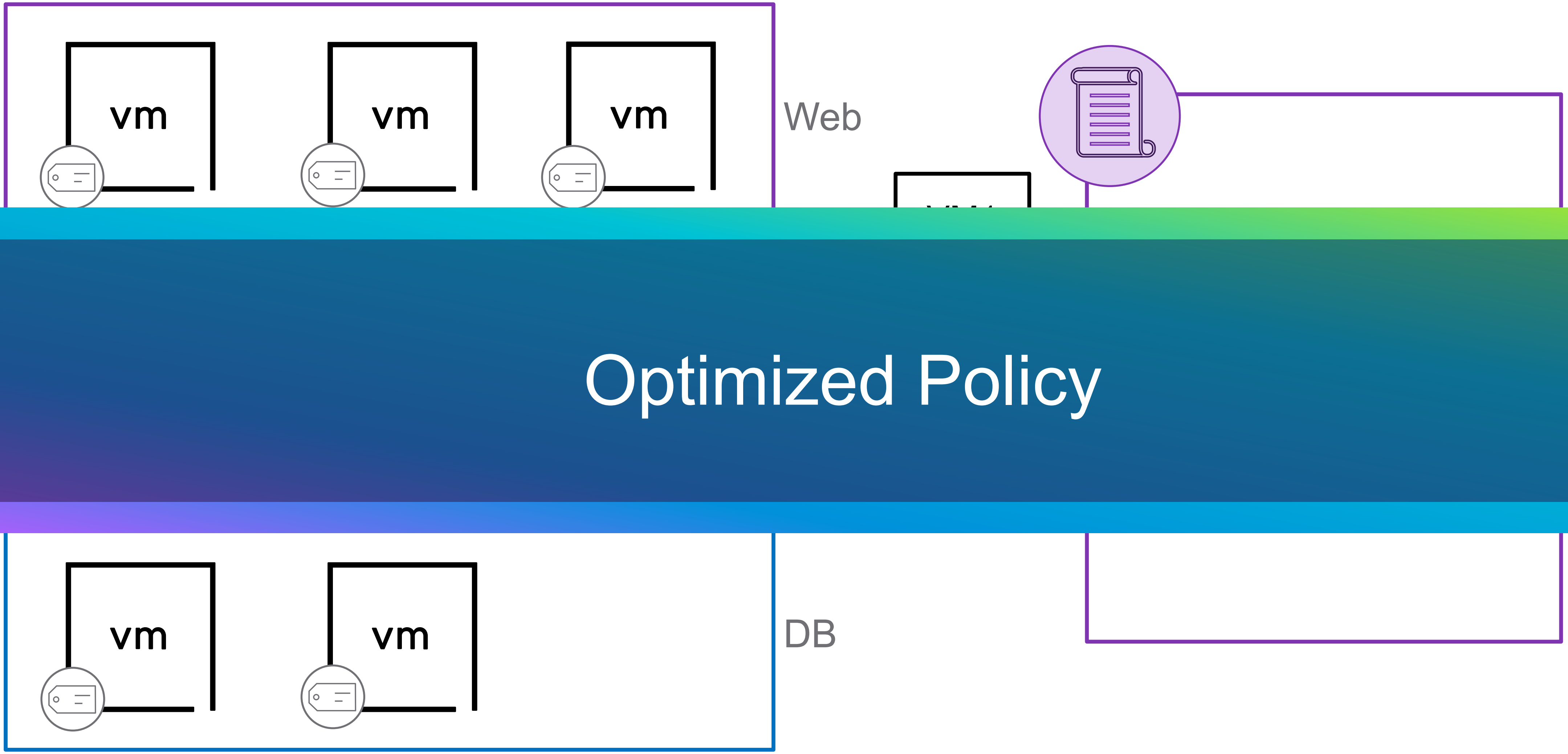
Lateral Security Tools

Legacy Firewall Policy



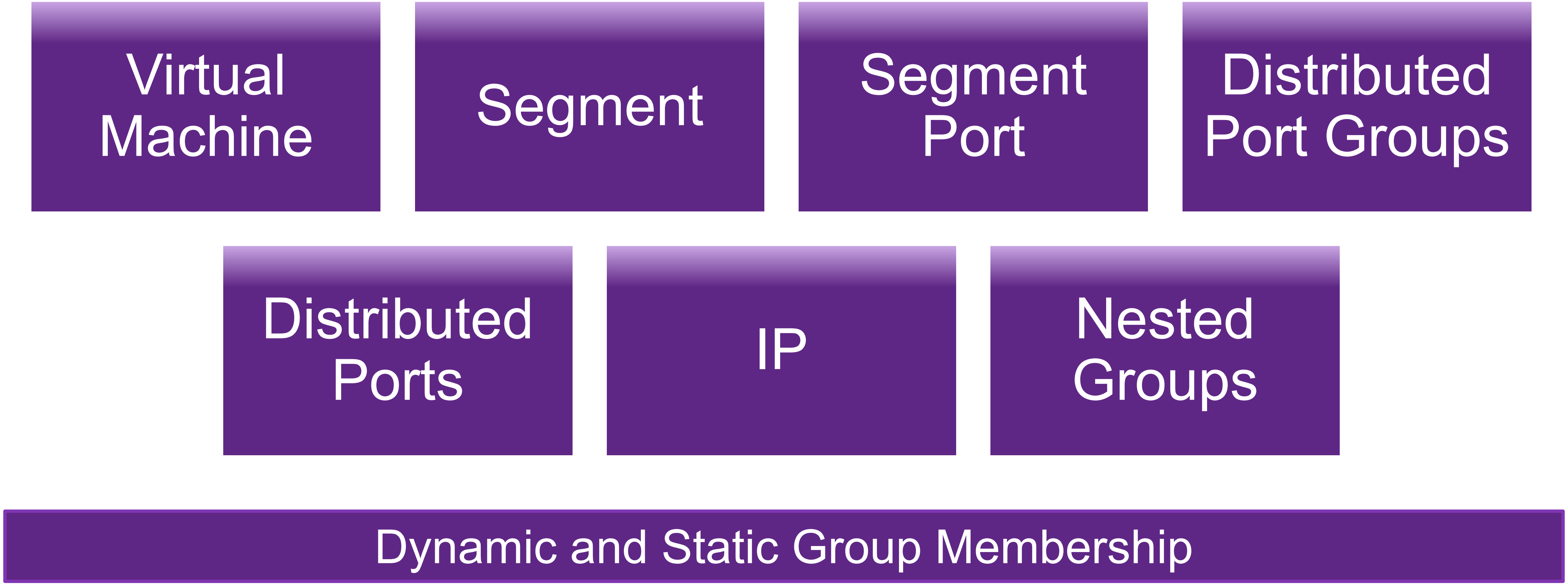
Manual updates for workload additions and removal

Tag-Based Firewall Policy



Optimized Policy

Group Membership Options



Virtual Machine

Segment

Segment Port

Distributed Port Groups

Distributed Ports

IP

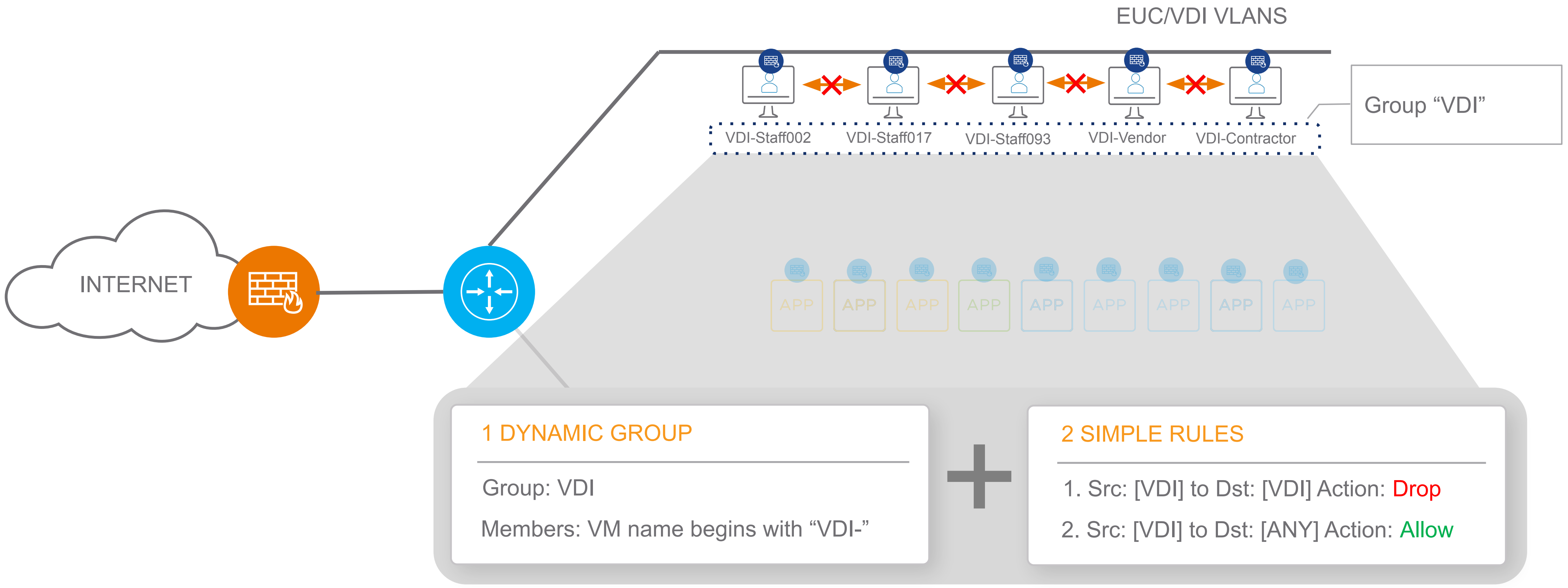
Nested Groups

Dynamic and Static Group Membership

Lateral Security Quick Wins

Segmentation

VDI security automation



1 DYNAMIC GROUP

Group: VDI

Members: VM name begins with “VDI-”

+

2 SIMPLE RULES

1. Src: [VDI] to Dst: [VDI] Action: Drop
2. Src: [VDI] to Dst: [ANY] Action: Allow

Segmentation

Security for Legacy Operating Systems

1 DYNAMIC GROUP

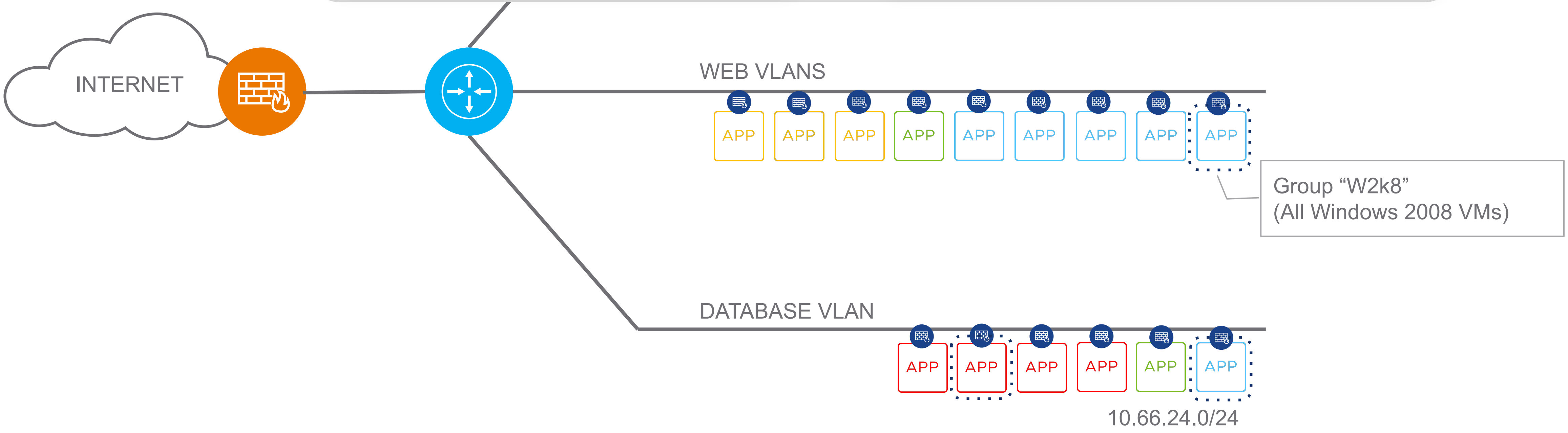
NS Group: W2k8

Members: OS name = Windows 2008

+

2 SIMPLE RULES

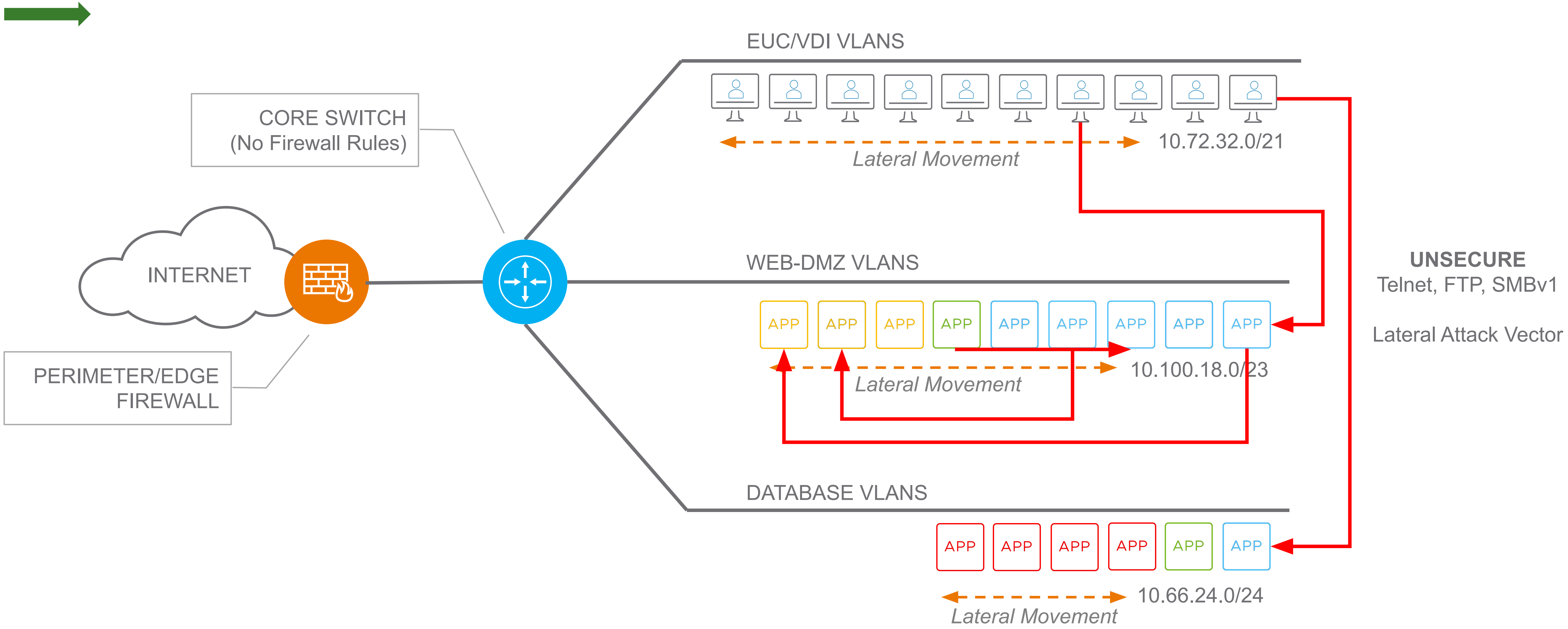
1. Src: [W2k8] to Dst: [10.0.0.0/8] Action: Allow
2. Src: [W2k8] to Dst: [Any] Action: Drop



Segmentation

Known Unsecure Protocols - The problem

BEFORE *AFTER*



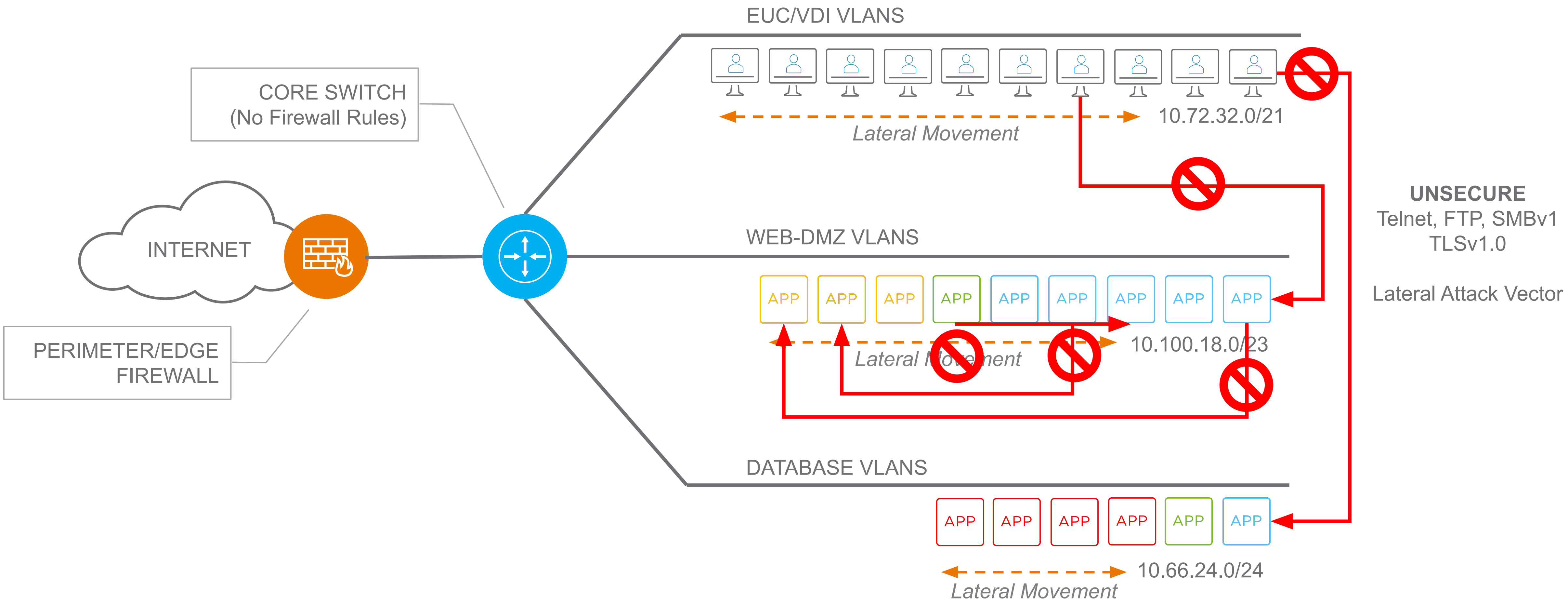
Segmentation

Known Unsecure Protocols - The solution

BEFORE *AFTER*

2 SIMPLE RULES

1. Src: [Any] to Dst: [Any] [TELNET] Action: Drop
2. Src: [Any] to Dst: [Any] [FTP] Action: Drop

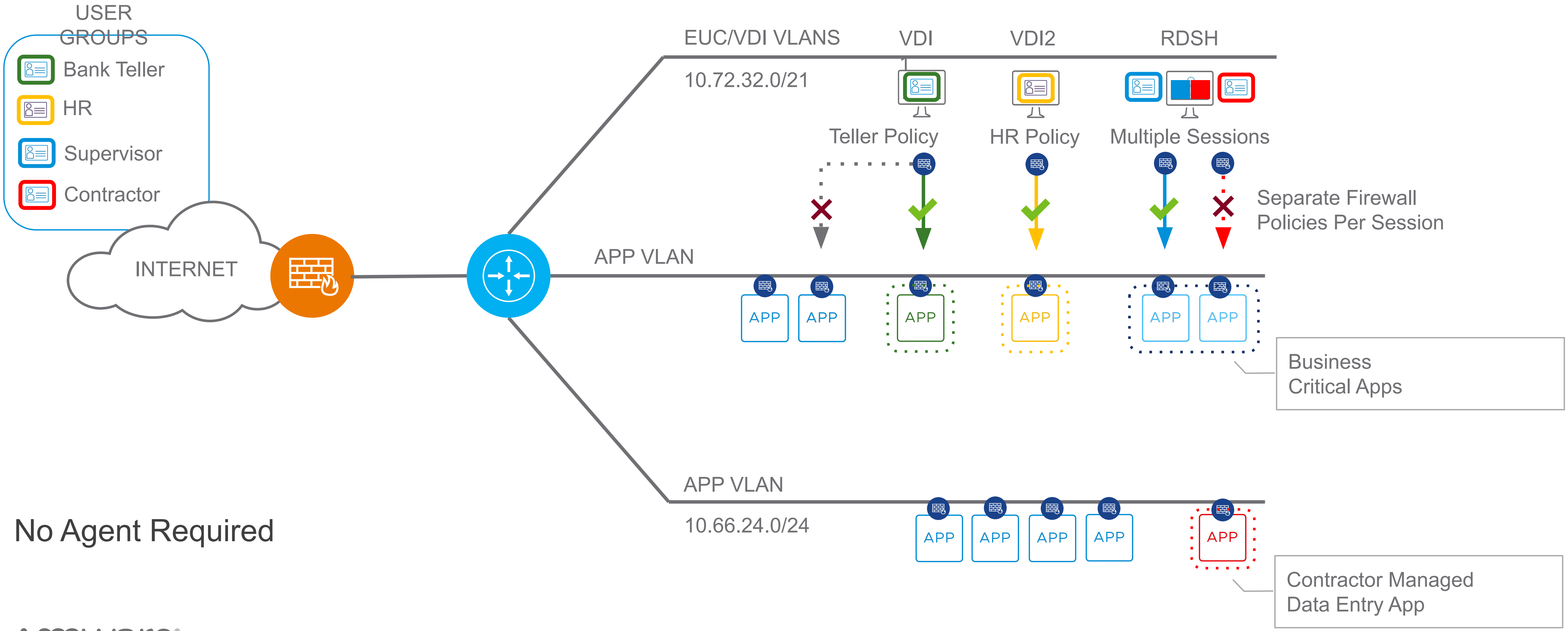


UNSECURE
Telnet, FTP, SMBv1
TLSv1.0

Lateral Attack Vector

Segmentation

Identity Firewall - VDI and RDSH to App Control



No Agent Required

Up to 50%

CapEx Reduction

with Firewall + IDS/IPS

Up to 73%

OpEx Reduction

with Firewall + IDS/IPS

Internal VMware Customer Study: DICE ROI and Value Modeling

Better Security, Compelling Savings

No network changes

Easily segment your network in software

No blind spots

Advanced threat prevention for every hop

Operationally simple

Rule recommendations & policy automation

Resources