VCF TechCon
Powered by VMUG

Start *vandaag* nog met microsegmentatie!

Robert Cranendonk

VMUGNL
VMware User Group

Start with micro segmentation *today*!

Robert Cranendonk

VCF TechCon 2025

Robert Cranendonk MSc.

- 🐣 Since 1990
- 🏢 From 2015 working with NSX
- 🎓 2024 MSc. Cyber Security Engineering
- 😎 IT Consultant @ itq
- 🎯 Broadcom Knight, vExpert
- 🌐 significant-bit.com

Terminology

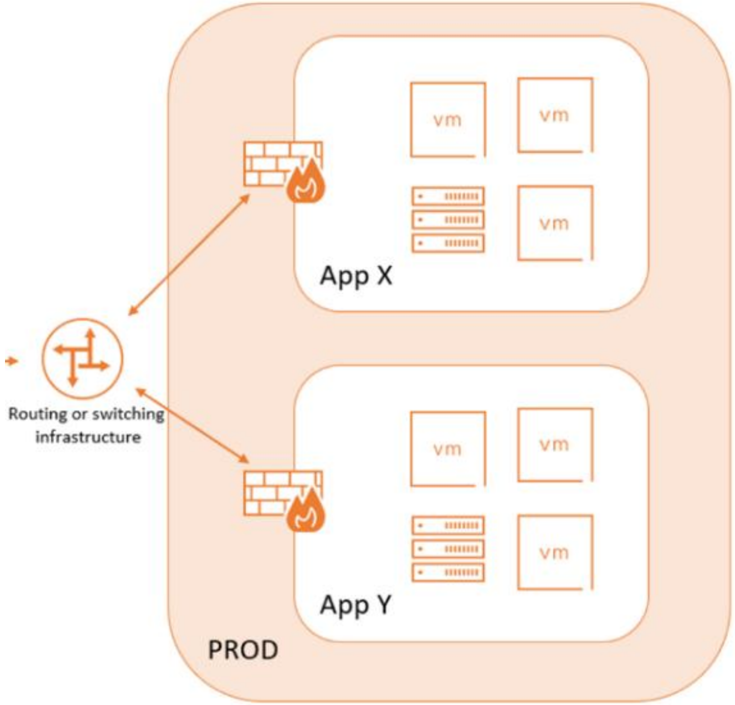
- Zero Trust
  - *"All devices and network flows are not trusted by default"*
- Micro Segmentation
  - *"Logically divide the data center into distinct security segments down to the individual workload level"*
- North-South traffic
  - *"Traffic going in and out of the NSX fabric"*
  - *"Physical to virtual"*
- East-West traffic
  - *"Traffic within the NSX fabric"*

Misconceptions

- Microseg = Microseg?
    - Application Centric Security
- Need to know all flows
- All or nothing
- Big bang, big problems!
- Physical workloads are a problem

WRONG

Application Ring Fencing

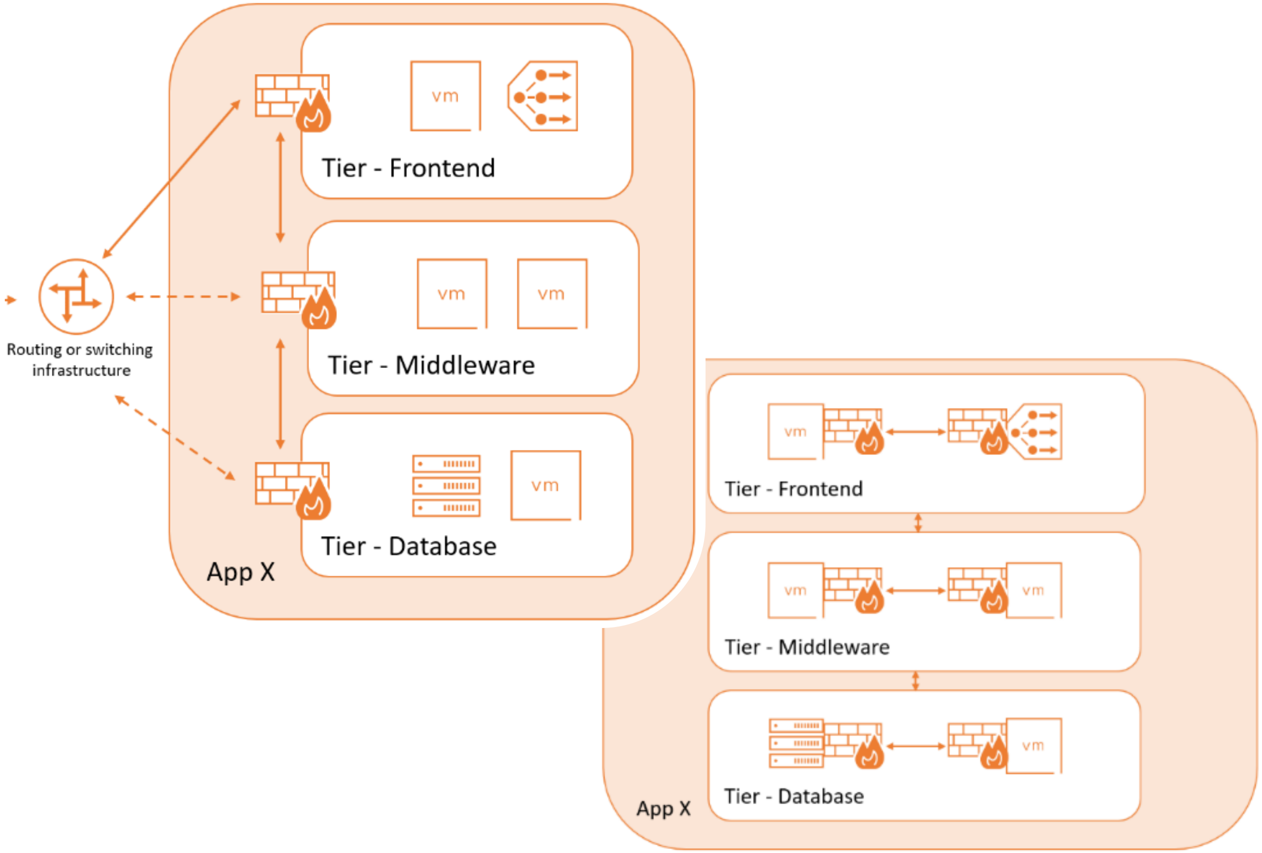


Filtering only on Application group as a whole

Rules apply to ALL VMs in app

Intra-app traffic default allowed

Micro Segmentation



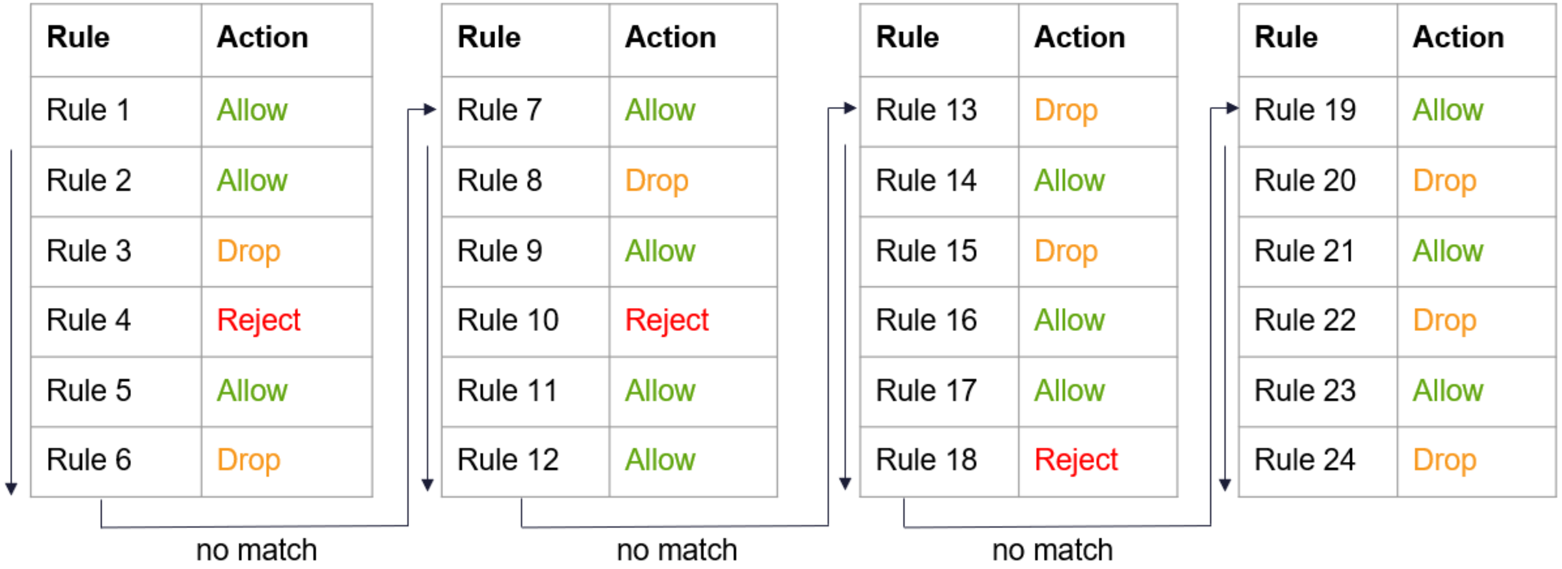
Filtering on Tier or individual VM

Rules only apply to Tier or VM

Intra-app traffic not default allowed

Rule Evaluation

ETHERNET (1) | EMERGENCY (0) | INFRASTRUCTURE (6) | ENVIRONMENT (9) | APPLICATION (3)



Rule	Action
Rule 1	Allow
Rule 2	Allow
Rule 3	Drop
Rule 4	Reject
Rule 5	Allow
Rule 6	Drop

no match

Rule	Action
Rule 7	Allow
Rule 8	Drop
Rule 9	Allow
Rule 10	Reject
Rule 11	Allow
Rule 12	Allow

no match

Rule	Action
Rule 13	Drop
Rule 14	Allow
Rule 15	Drop
Rule 16	Allow
Rule 17	Allow
Rule 18	Reject

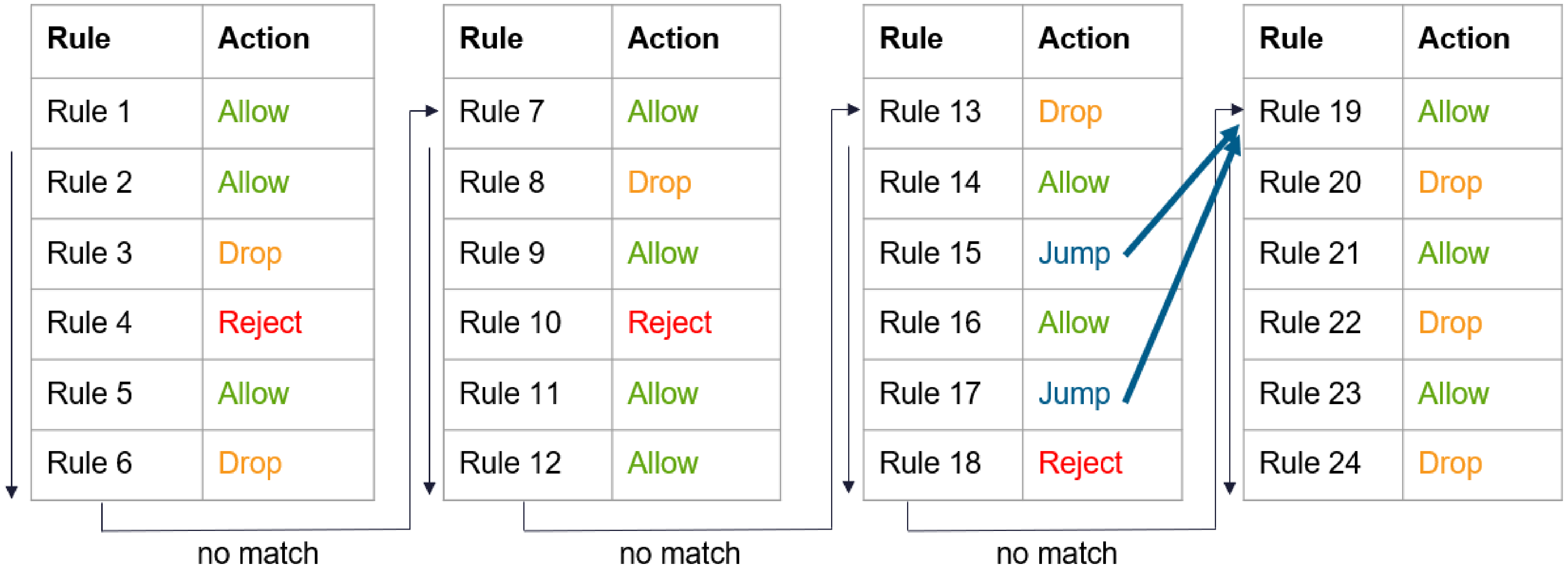
no match

Rule	Action
Rule 19	Allow
Rule 20	Drop
Rule 21	Allow
Rule 22	Drop
Rule 23	Allow
Rule 24	Drop

Rule evaluation stops at the first hit

Image source: Broadcom

Rule Evaluation



Rule	Action
Rule 1	Allow
Rule 2	Allow
Rule 3	Drop
Rule 4	Reject
Rule 5	Allow
Rule 6	Drop

Rule	Action
Rule 7	Allow
Rule 8	Drop
Rule 9	Allow
Rule 10	Reject
Rule 11	Allow
Rule 12	Allow

Rule	Action
Rule 13	Drop
Rule 14	Allow
Rule 15	Jump
Rule 16	Allow
Rule 17	Jump
Rule 18	Reject

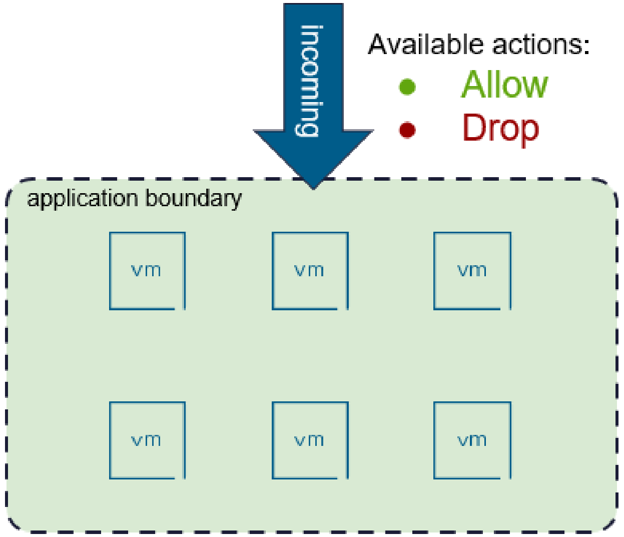
Rule	Action
Rule 19	Allow
Rule 20	Drop
Rule 21	Allow
Rule 22	Drop
Rule 23	Allow
Rule 24	Drop

Jump-to-application skips the remainder and goes to the top of the 'Application' section and continues from there

Image source: Broadcom

Filter Direction

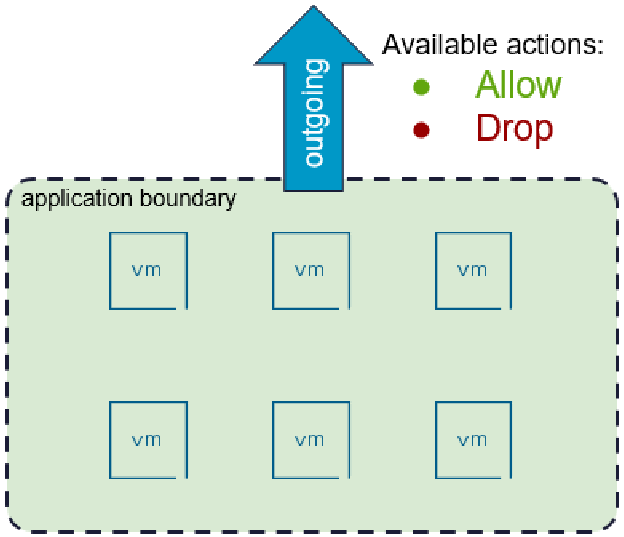
Incoming Traffic



Available actions:

- Allow
- Drop

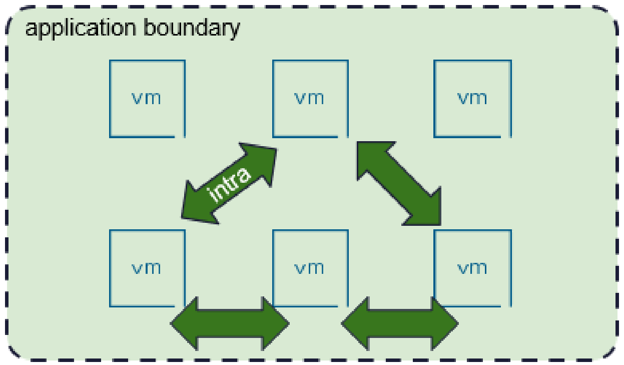
Outgoing Traffic



Available actions:

- Allow
- Drop

Intra-application Traffic



Available action:

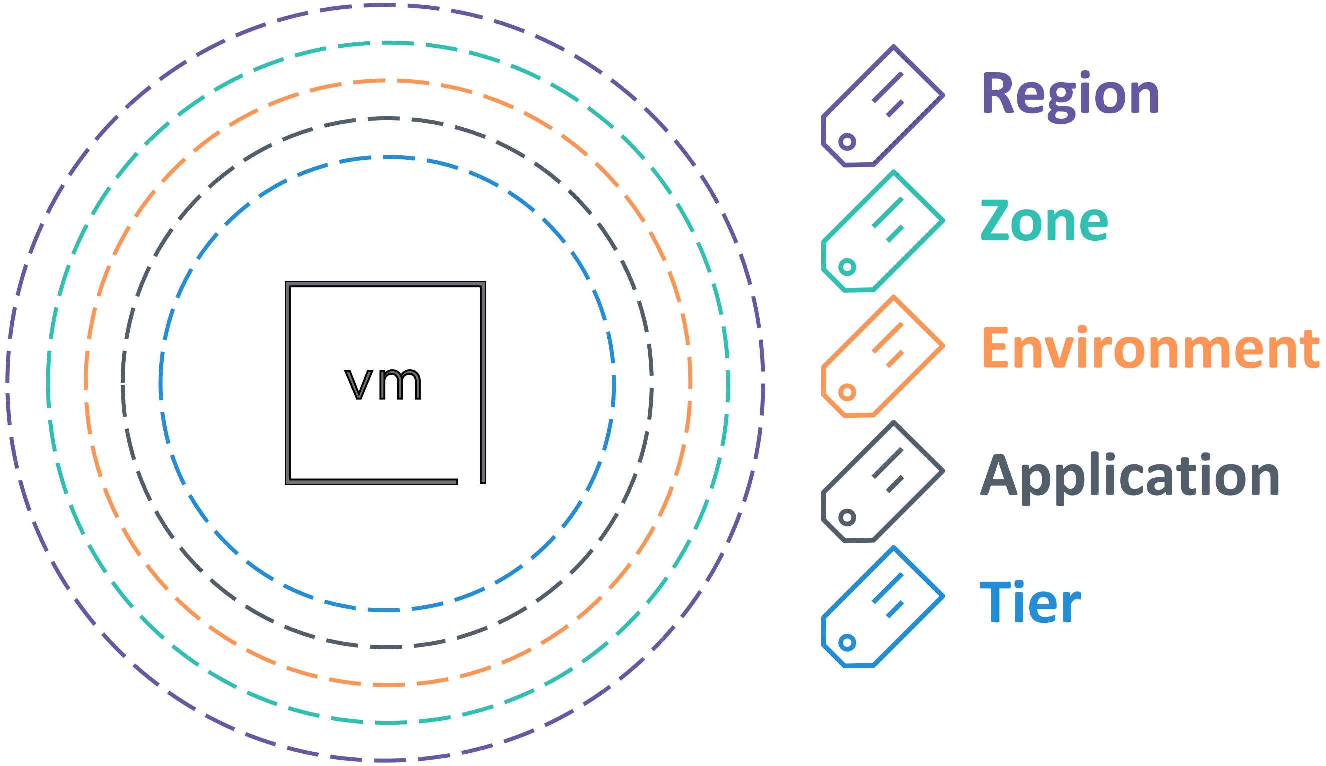
- Allow

Image source: Broadcom

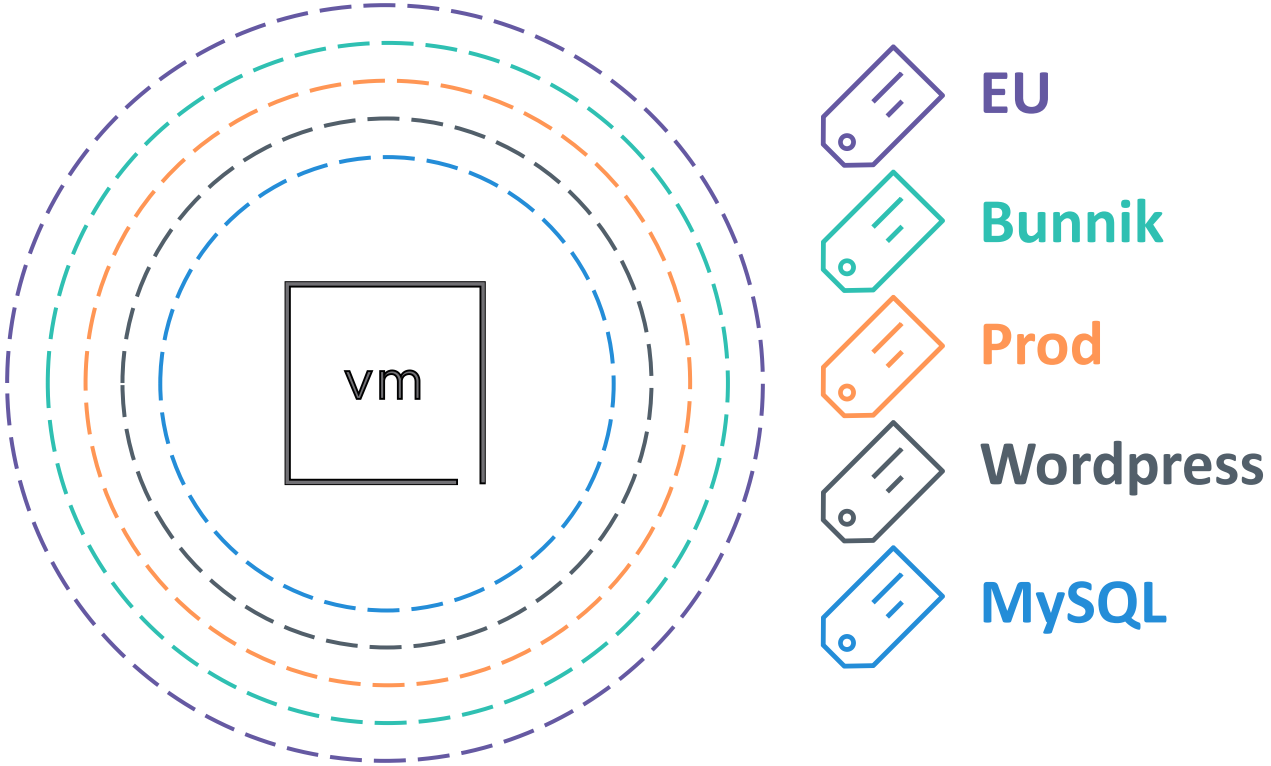
Overall concept

- VM identification agnostic to underlying network
  - Tags & Security Groups
- Security “onion” (next slide)
  - Layers
  - Datacenter hierarchy
- Allow some stuff – deny the rest
  - Easier troubleshooting
  - No need for be-all, end-all any-any-deny (but recommended!)
- Build outside-in
  - Shared services -> environments -> applications -> (tiers?)

Security Onion

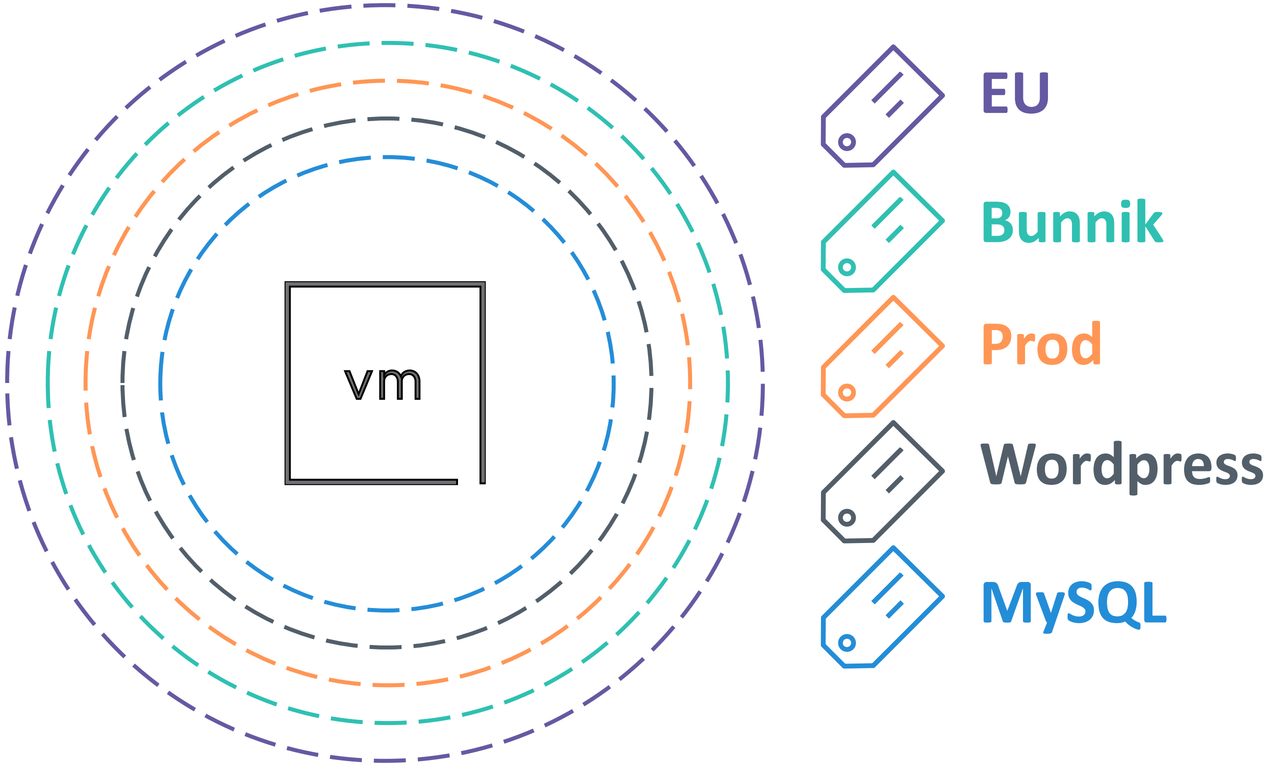


Security Onion



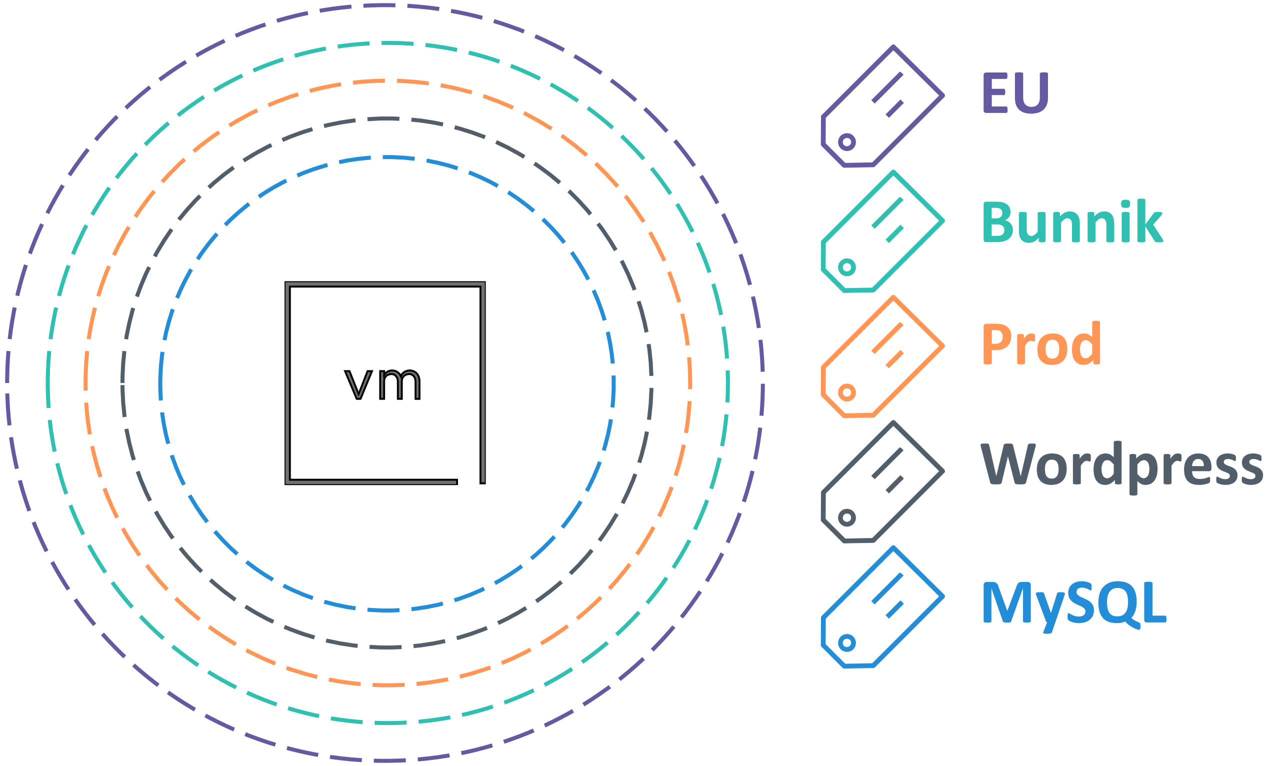
All VMs located in Bunnik, in the EU

Security Onion



All Wordpress VMs in production

Security Onion



EU

Bunnik

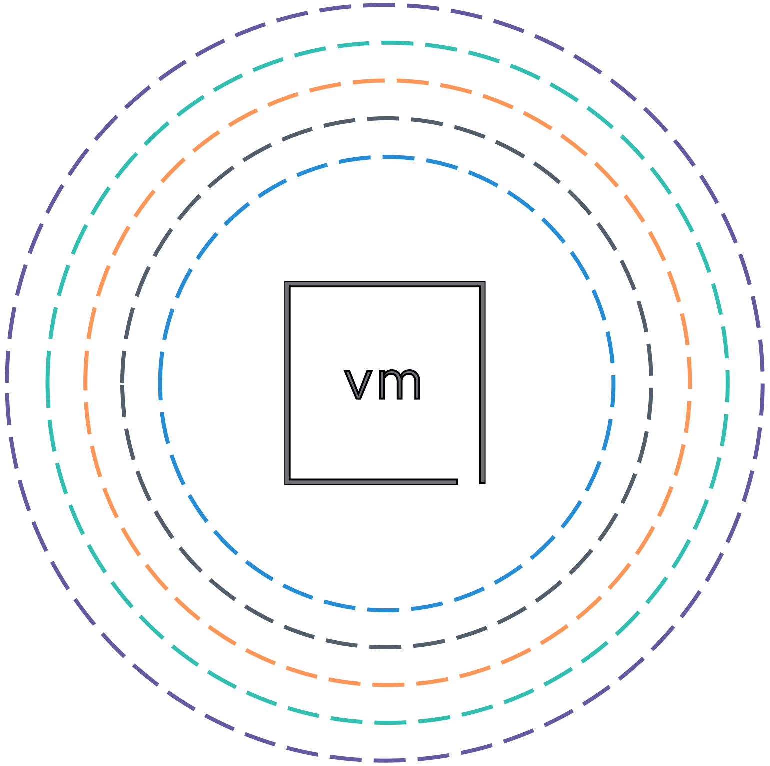
Prod

Wordpress

MySQL

VMs running MySQL in the Wordpress app in production, located in Bunnik in the EU region

Security Onion



EU

Bunnik

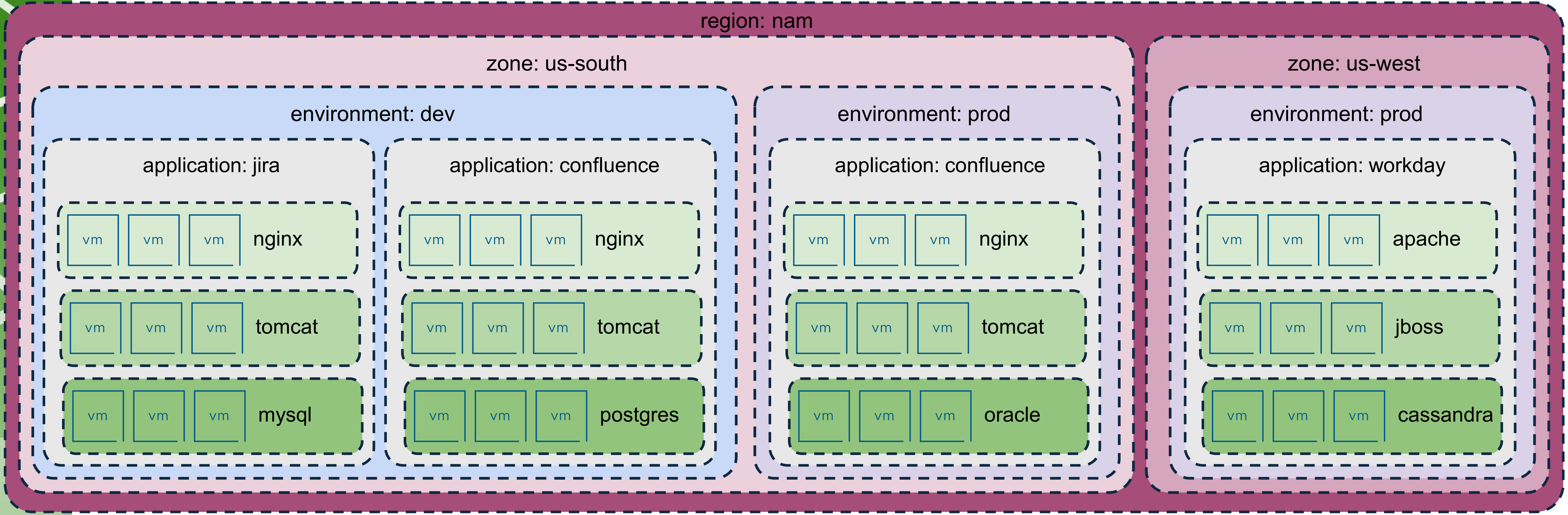
Prod

Wordpress

MySQL

All VMs running MySQL for Wordpress

Datacenter Hierarchy



- region: nam
  - zone: us-south
    - environment: dev
      - application: jira
        - vm vm vm nginx
        - vm vm vm tomcat
        - vm vm vm mysql
      - application: confluence
        - vm vm vm nginx
        - vm vm vm tomcat
        - vm vm vm postgres
    - environment: prod
      - application: confluence
        - vm vm vm nginx
        - vm vm vm tomcat
        - vm vm vm oracle
  - zone: us-west
    - environment: prod
      - application: workday
        - vm vm vm apache
        - vm vm vm jboss
        - vm vm vm cassandra

Image source: Broadcom

Step 1: Tag, Tag, Tag

This is the most annoying part of the project

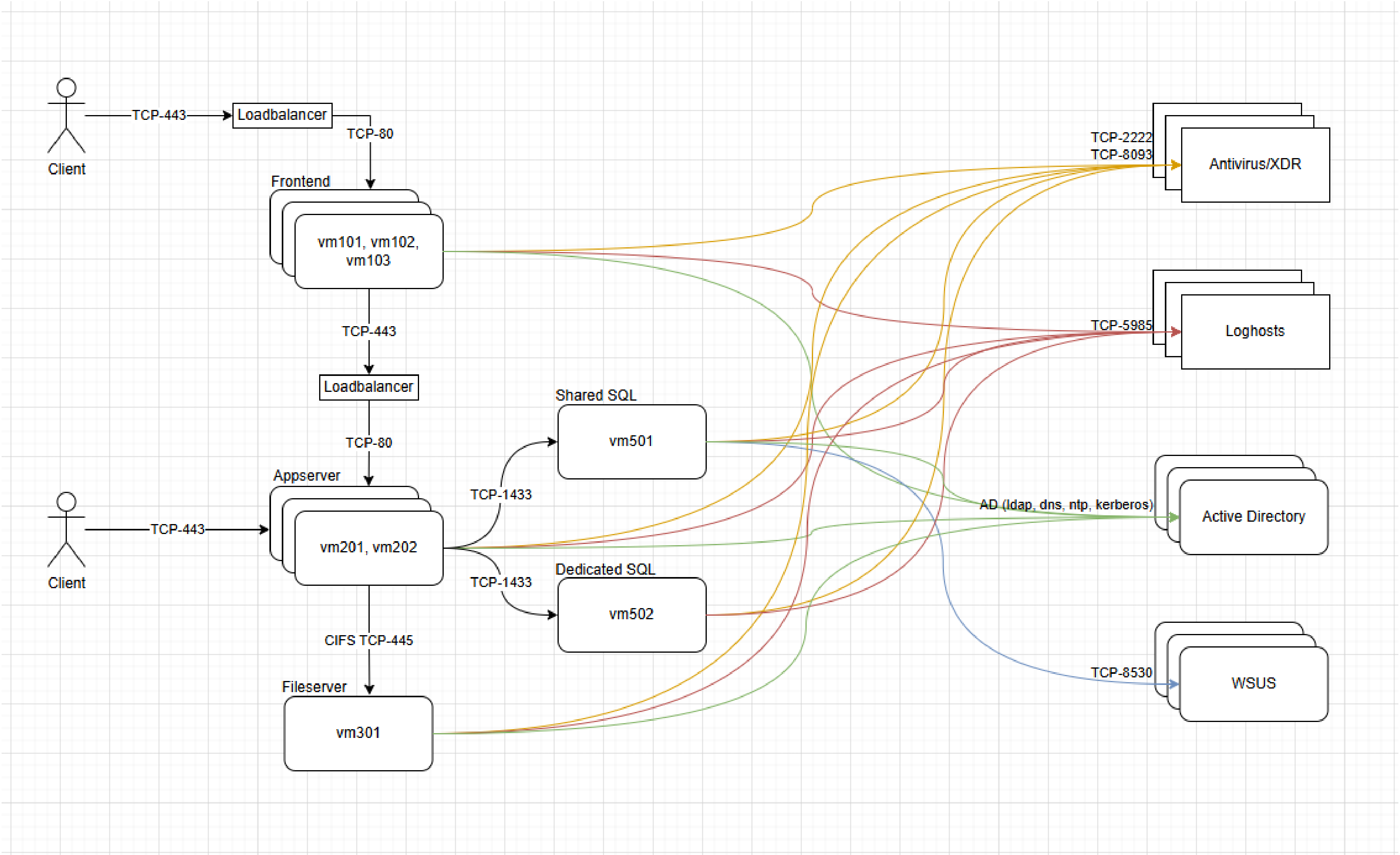
- Know thyself! Or... your environment. (know thyronment? Thyvironment?)
- All VMs need to be tagged
  - One tag per category
- It depends:
  - Manual
    - Existing tags, CMDB
  - Algorithmically
    - Naming convention, folders
  - Magically
    - K-nearest Neighbours, flow analysis

VCF TechCon Powered by VMUG

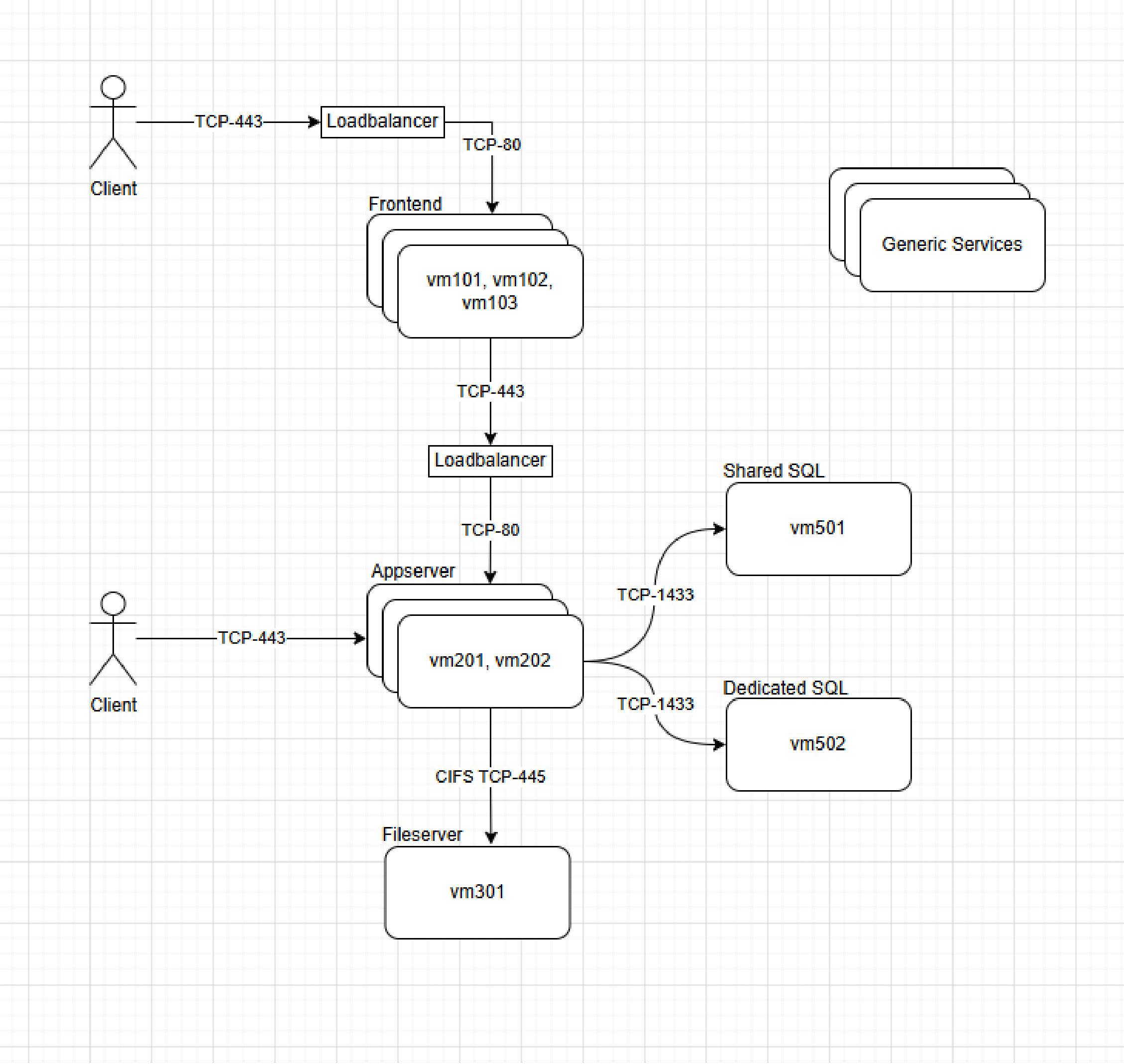
Step 2: shared services

- Examples?
- DNS, NTP, AD, Monitoring, XDR, Repo, etc.
- Broad rules, generic access
- Initial set of rules for each new VM
  - Even without tags!

From this:


Client
TCP-443
Loadbalancer
TCP-80
Frontend
vm101, vm102, vm103
TCP-443
Loadbalancer
TCP-80
Appserver
Client
TCP-443
vm201, vm202
TCP-1433
Shared SQL
vm501
TCP-1433
Dedicated SQL
vm502
CIFS TCP-445
Fileserver
vm301
TCP-2222
TCP-8093
Antivirus/XDR
TCP-5985
Loghosts
AD (ldap, dns, ntp, kerberos)
Active Directory
TCP-8530
WSUS

To this:



Client
TCP-443
Loadbalancer
TCP-80
Frontend
vm101, vm102, vm103
Generic Services
TCP-443
Loadbalancer
Shared SQL
vm501
TCP-80
Appserver
TCP-1433
Client
TCP-443
vm201, vm202
Dedicated SQL
TCP-1433
vm502
CIFS TCP-445
Fileserver
vm301

Rules

INFRASTRUCTURE ENVIRONMENT APPLICATION

From	To	Service	Action
Any	SG_Infra_NTP	NTP	Allow
Any	~~SG_Infra_NTP~~	NTP	Drop
Any	SG_Infra_DNS	DNS	Allow
Any	~~SG_Infra_DNS~~	DNS	Drop
SG_Windows	SG_Infra_AD	SS_LDAPS	Allow
SG_Windows	~~SG_Infra_AD~~	SS_LDAPS	Drop

Security Group containing all Windows VMs

Security Set containing services related to AD

Step 3: Environments

- Create a security matrix like so

From\To	**Dev**	**Prod**	**HighSec**
Dev	Allow	Allow	Allow
Prod	Allow	Allow	Allow
HighSec	Allow	Allow	Allow

INFRASTRUCTURE → ENVIRONMENT → APPLICATION

Environment Pair	From	To	Service	Action
Dev ↔ Dev				
	Dev	Dev	Any	Allow
Prod ↔ Prod				
	Prod	Prod	Any	Allow
HighSec ↔ HighSec				
	HighSec	HighSec	Any	Allow

- Lock down environment transitions

From\To	**Dev**	**Prod**	**HighSec**
Dev	Allow	Drop	Drop
Prod	Drop	Allow	Drop
HighSec	Drop	Drop	Allow

INFRASTRUCTURE → ENVIRONMENT → APPLICATION

Environment Pair	From	To	Service	Action
Dev ↔ Dev				
	Dev	Dev	Any	Allow
Dev ↔ Prod				
	Dev	Prod	Any	Drop
Dev ↔ HighSec				
	Dev	HighSec	Any	Drop

- Allow for reality

From\To	**Dev**	**Prod**	**HighSec**
Dev	Allow	Drop with Exceptions	Drop
Prod	Drop with Exceptions	Allow	Drop with Exceptions
HighSec	Drop	Drop with Exceptions	Allow

INFRASTRUCTURE

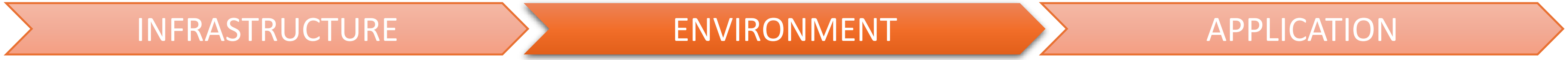
ENVIRONMENT

APPLICATION

Environment Pair	From	To	Service	Action
Dev ↔ Dev				
	Dev	Dev	Any	Allow
Dev ↔ Prod				
	Dev-AppA	Prod-DatabaseX	Any	Allow
	Dev	Prod	Any	Drop
Dev ↔ HighSec				
	Dev	HighSec	Any	Drop

- Prepare for step 3: Application security

From\To	**Dev**	**Prod**	**HighSec**
Dev	Jump to Application	Drop with Exceptions	Drop
Prod	Drop with Exceptions	Jump to Application	Drop with Exceptions
HighSec	Drop	Drop with Exceptions	Jump to Application



Environment Pair	From	To	Service	Action
Dev ↔ Dev				
	Dev	Dev	Any	Jump to Application
Dev ↔ Prod				
	Dev-AppA	Prod-DatabaseX	Any	Jump to Application
	Dev	Prod	Any	Drop
Dev ↔ HighSec				
	Dev	HighSec	Any	Drop

Step 4: Applications

- Reminder:
  Jump to Application = skip current category, start atop Application
- Reminder:
  Strategy – Application ring fencing or micro segmentation?
- Key point: monitor before lockdown

Application ring fencing

INFRASTRUCTURE → ENVIRONMENT → **APPLICATION**

Application	From	To	Service	Action
EU_Bunnik_Dev_Wordpress	Applied to: EU_Bunnik_Dev_Wordpress			
	EU_Bunnik_Dev_AppX	Any	HTTPS	Allow
	EU_Bunnik_Dev_AppY	Any	MySQL	Allow
	EU_Bunnik_Dev_Wordpress	Any	Any	Allow
	Any	Any	Any	Drop

Note the ‘Applied to’!

Micro segmentation

INFRASTRUCTURE → ENVIRONMENT → APPLICATION

Application	From	To	Service	Action
EU_Bunnik_Dev_Wordpress	Applied to: EU_Bunnik_Dev_Wordpress			
	Any	Nginx	HTTPS	Allow
	Nginx	Apache	HTTPS	Allow
	Apache	MySQL	MySQL	Allow
	Any	Any	Any	Drop

Full group name: EU_Bunnik_Dev_Wordpress_Nginx

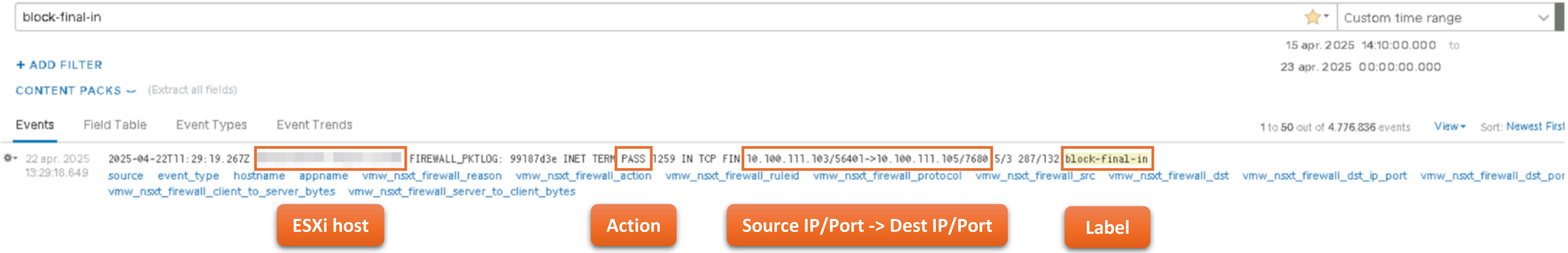
Logging & Learning

INFRASTRUCTURE → ENVIRONMENT → APPLICATION

Application	From	To	Service	Action
EU_Bunnik_Dev_Wordpress	Applied to: EU_Bunnik_Dev_Wordpress			
	Any	Nginx	HTTPS	Allow
	Nginx	Apache	HTTPS	Allow
	Apache	MySQL	MySQL	Allow
	Any	Any	Any	Allow & Log

After learning: Drop & Log!

More about logging & learning



block-final-in

Custom time range

15 apr. 2025 14:10:00.000 to

23 apr. 2025 00:00:00.000

+ ADD FILTER
CONTENT PACKS
(Extract all fields)
Events
Field Table
Event Types
Event Trends

1 to 50 out of 4.776.836 events

22 apr. 2025 13:29:18.649

```
2025-04-22T11:29:19.267Z [redacted] FIREWALL_PKTLOG: 99187d3e INET TERM PASS 1259 IN TCP FIN 10.100.111.103/56401->10.100.111.105/7680 5/3 287/132 block-final-in
```

source event_type hostname appname vmw_nsxt_firewall_reason vmw_nsxt_firewall_action vmw_nsxt_firewall_ruleid vmw_nsxt_firewall_protocol vmw_nsxt_firewall_src vmw_nsxt_firewall_dst vmw_nsxt_firewall_dst_ip_port vmw_nsxt_firewall_dst_por
vmw_nsxt_firewall_client_to_server_bytes vmw_nsxt_firewall_server_to_client_bytes
ESXi host
Action
Source IP/Port -> Dest IP/Port
Label

- Exposes **all** flows
- Trigger alerts on hit:
  - It means bona fide traffic that must be allowed
  - It means malicious traffic that must be investigated

Either way: action is needed!

Security Journey with Security Services Platform

Customer Challenges

Where should I start?

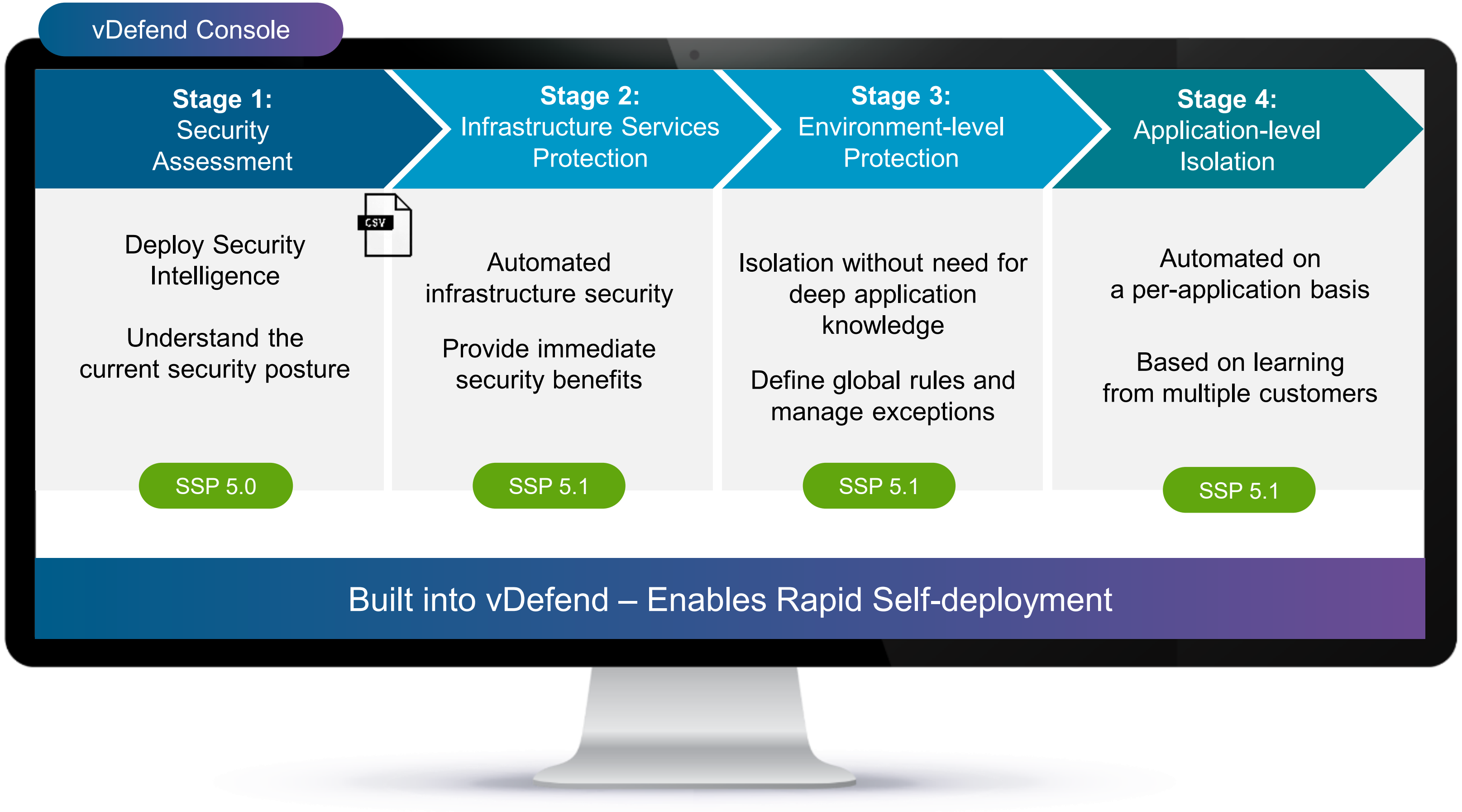
What is my current security posture?

How can I secure so many applications?

How can I do it safely and quickly?

Security Journey

New



vDefend Console

Stage 1: Security Assessment

Deploy Security Intelligence

Understand the current security posture

SSP 5.0

Stage 2: Infrastructure Services Protection

Automated infrastructure security

Provide immediate security benefits

SSP 5.1

Stage 3: Environment-level Protection

Isolation without need for deep application knowledge

Define global rules and manage exceptions

SSP 5.1

Stage 4: Application-level Isolation

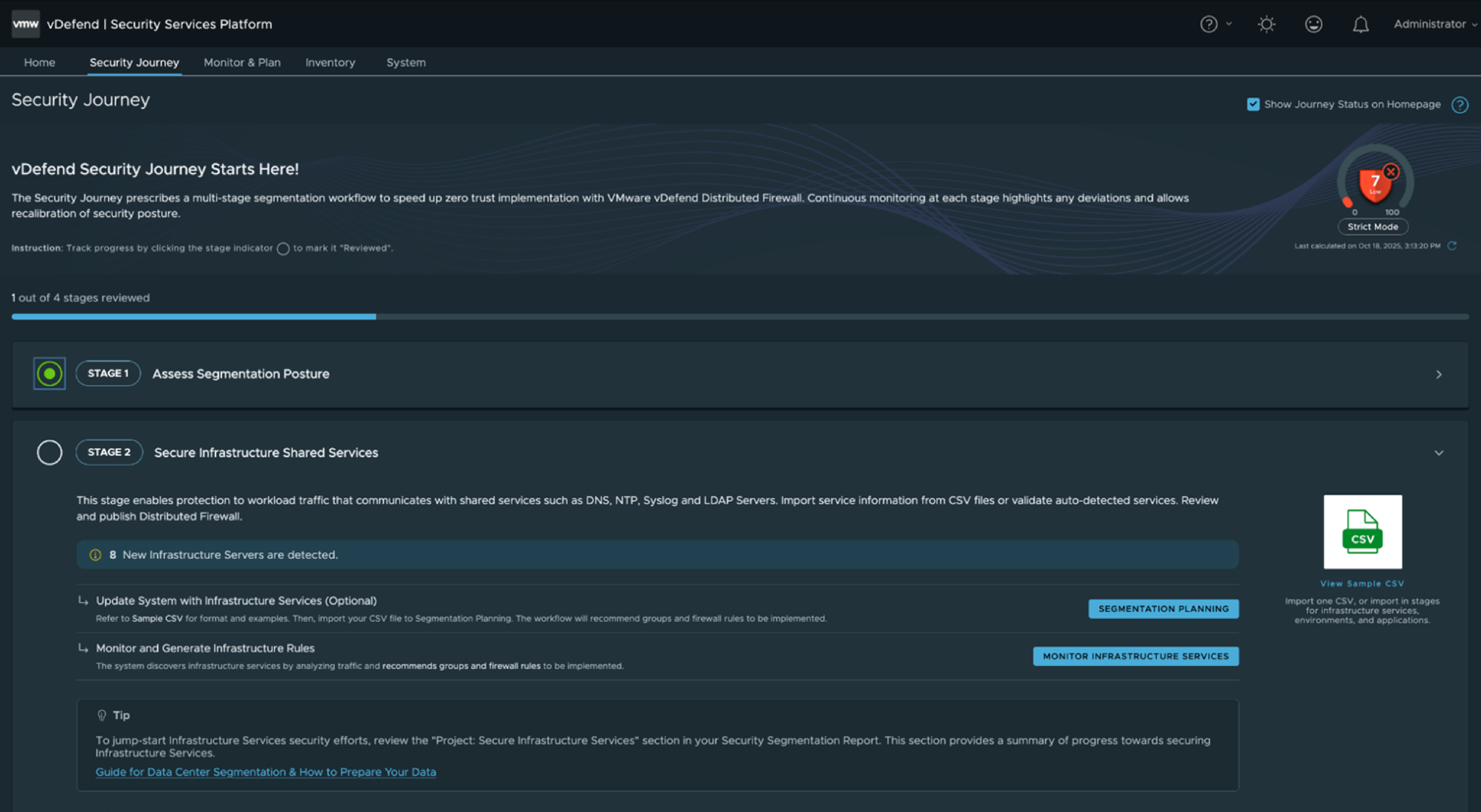
Automated on a per-application basis

Based on learning from multiple customers

SSP 5.1

Built into vDefend – Enables Rapid Self-deployment

Slide courtesy of Broadcom



Security Journey

☑ Show Journey Status on Homepage

vDefend Security Journey Starts Here!

The Security Journey prescribes a multi-stage segmentation workflow to speed up zero trust implementation with VMware vDefend Distributed Firewall. Continuous monitoring at each stage highlights any deviations and allows recalibration of security posture.

Instruction: Track progress by clicking the stage indicator ○ to mark it "Reviewed".

Last calculated on Oct 18, 2025, 3:13:20 PM

1 out of 4 stages reviewed

● STAGE 1 Assess Segmentation Posture

○ STAGE 2 Secure Infrastructure Shared Services

This stage enables protection to workload traffic that communicates with shared services such as DNS, NTP, Syslog and LDAP Servers. Import service information from CSV files or validate auto-detected services. Review and publish Distributed Firewall.

ⓘ 8 New Infrastructure Servers are detected.

↳ Update System with Infrastructure Services (Optional)
Refer to **Sample CSV** for format and examples. Then, import your CSV file to Segmentation Planning. The workflow will recommend groups and firewall rules to be implemented.

SEGMENTATION PLANNING

↳ Monitor and Generate Infrastructure Rules
The system discovers infrastructure services by analyzing traffic and **recommends groups and firewall rules** to be implemented.

MONITOR INFRASTRUCTURE SERVICES

View Sample CSV

Import one CSV, or import in stages for infrastructure services, environments, and applications.

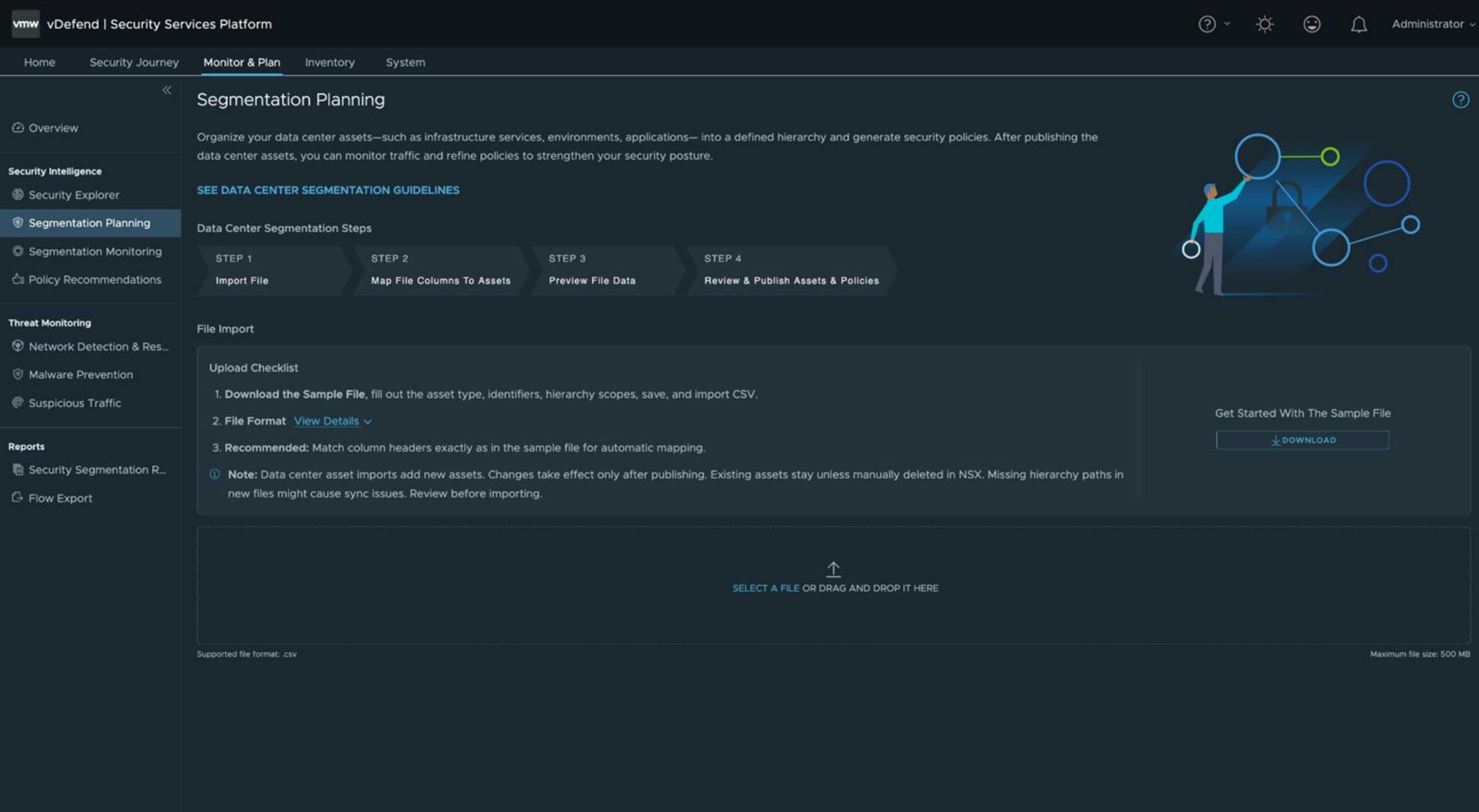
Tip

To jump-start Infrastructure Services security efforts, review the "Project: Secure Infrastructure Services" section in your Security Segmentation Report. This section provides a summary of progress towards securing Infrastructure Services.

Guide for Data Center Segmentation & How to Prepare Your Data

Additional Resources

Slide courtesy of Broadcom



Segmentation Planning

Organize your data center assets—such as infrastructure services, environments, applications— into a defined hierarchy and generate security policies. After publishing the data center assets, you can monitor traffic and refine policies to strengthen your security posture.

SEE DATA CENTER SEGMENTATION GUIDELINES

Data Center Segmentation Steps

STEP 1 Import File

STEP 2 Map File Columns To Assets

STEP 3 Preview File Data

STEP 4 Review & Publish Assets & Policies

File Import

Upload Checklist

1. **Download the Sample File**, fill out the asset type, identifiers, hierarchy scopes, save, and import CSV.
2. **File Format** View Details ⌄
3. **Recommended:** Match column headers exactly as in the sample file for automatic mapping.

ⓘ **Note:** Data center asset imports add new assets. Changes take effect only after publishing. Existing assets stay unless manually deleted in NSX. Missing hierarchy paths in new files might cause sync issues. Review before importing.

Get Started With The Sample File

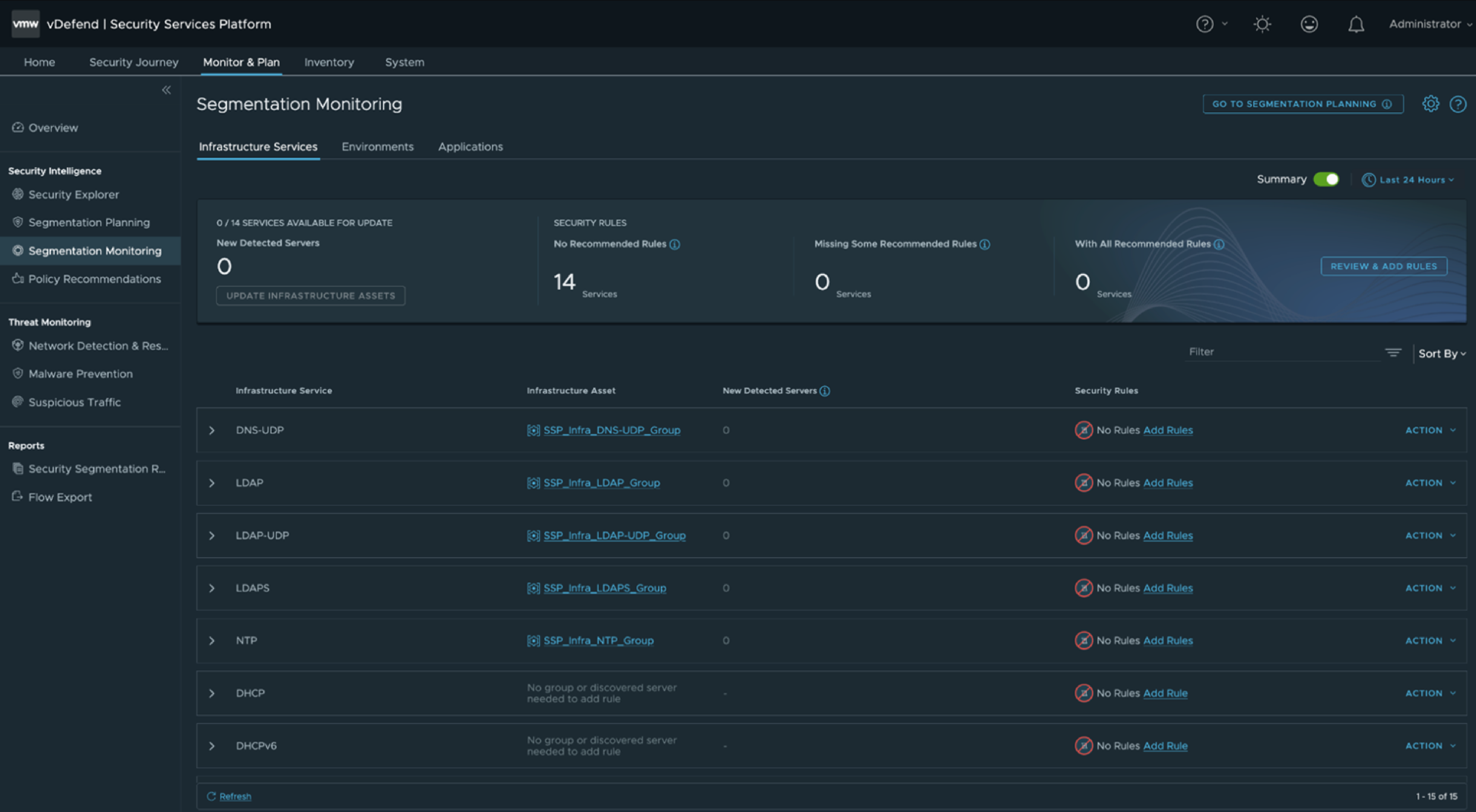
DOWNLOAD

SELECT A FILE OR DRAG AND DROP IT HERE

Supported file format: .csv

Maximum file size: 500 MB

Slide courtesy of Broadcom



Segmentation Monitoring

0 / 14 SERVICES AVAILABLE FOR UPDATE

New Detected Servers 0

UPDATE INFRASTRUCTURE ASSETS

SECURITY RULES

No Recommended Rules: 14 Services

Missing Some Recommended Rules: 0 Services

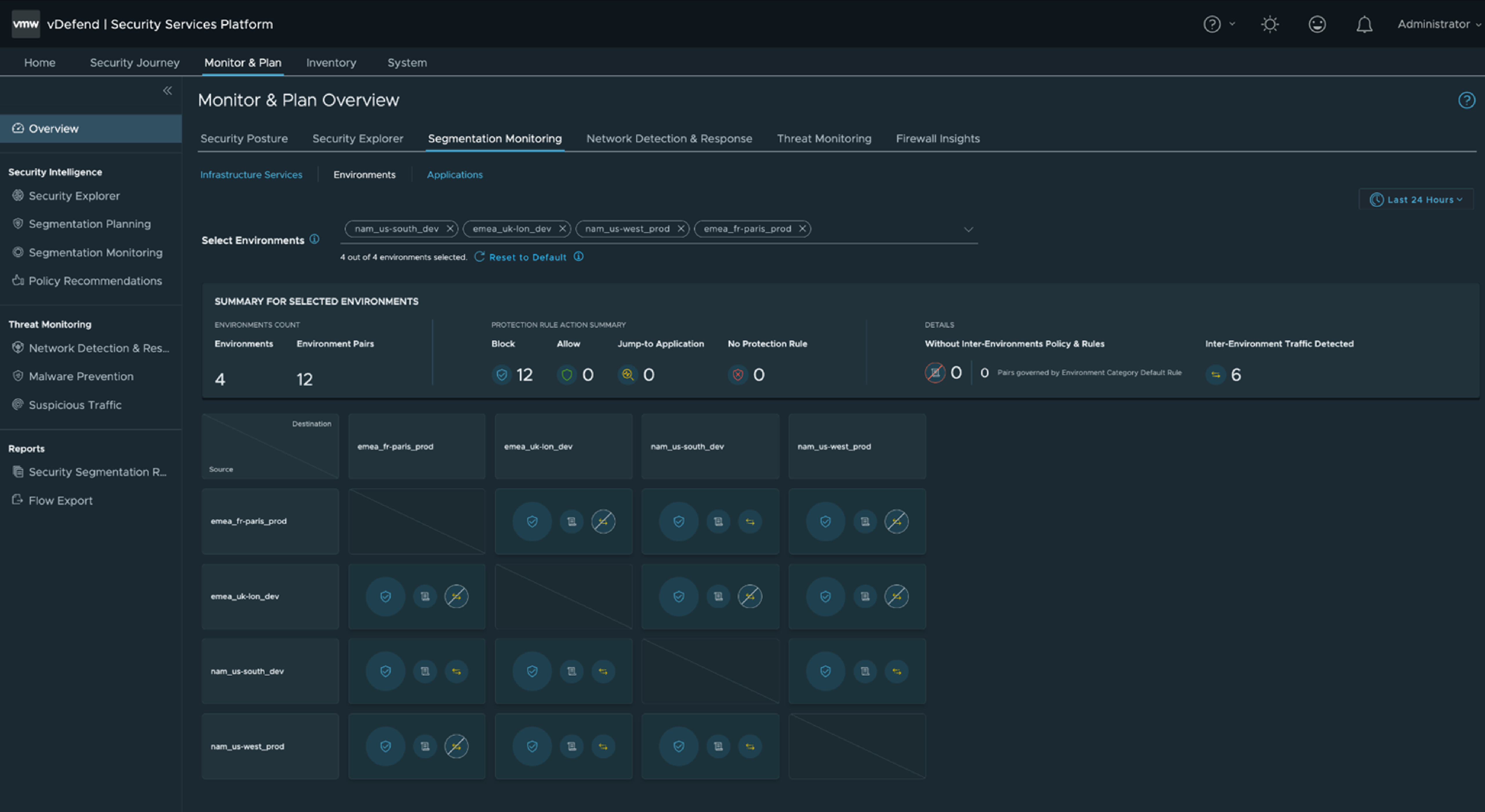
With All Recommended Rules: 0 Services

REVIEW & ADD RULES

Infrastructure Service	Infrastructure Asset	New Detected Servers	Security Rules	
DNS-UDP	SSP_Infra_DNS-UDP_Group	0	No Rules Add Rules	ACTION
LDAP	SSP_Infra_LDAP_Group	0	No Rules Add Rules	ACTION
LDAP-UDP	SSP_Infra_LDAP-UDP_Group	0	No Rules Add Rules	ACTION
LDAPS	SSP_Infra_LDAPS_Group	0	No Rules Add Rules	ACTION
NTP	SSP_Infra_NTP_Group	0	No Rules Add Rules	ACTION
DHCP	No group or discovered server needed to add rule	-	No Rules Add Rule	ACTION
DHCPv6	No group or discovered server needed to add rule	-	No Rules Add Rule	ACTION

1 - 15 of 15

Slide courtesy of Broadcom



Monitor & Plan Overview

Select Environments ⓘ nam_us-south_dev ✕ emea_uk-lon_dev ✕ nam_us-west_prod ✕ emea_fr-paris_prod ✕

4 out of 4 environments selected. Reset to Default ⓘ

SUMMARY FOR SELECTED ENVIRONMENTS

ENVIRONMENTS COUNT		PROTECTION RULE ACTION SUMMARY				DETAILS	
Environments	Environment Pairs	Block	Allow	Jump-to Application	No Protection Rule	Without Inter-Environments Policy & Rules	Inter-Environment Traffic Detected
4	12	12	0	0	0	0 | 0 Pairs governed by Environment Category Default Rule	6

Source \ Destination	emea_fr-paris_prod	emea_uk-lon_dev	nam_us-south_dev	nam_us-west_prod
emea_fr-paris_prod		🛡 ▤ ⊘	🛡 ▤ ⇆	🛡 ▤ ⊘
emea_uk-lon_dev	🛡 ▤ ⊘		🛡 ▤ ⊘	🛡 ▤ ⊘
nam_us-south_dev	🛡 ▤ ⇆	🛡 ▤ ⇆		🛡 ▤ ⇆
nam_us-west_prod	🛡 ▤ ⊘	🛡 ▤ ⇆	🛡 ▤ ⇆	

Slide courtesy of Broadcom

Robert’s tips for success

- Define your end goal:
  - Microseg, App Centric, something else?
  - Any-any deny at the end or no?
- Go step-by-step
  - You *cannot* do this quickly, it takes time
- Focus! Get a project owner
- Shared services first, high risk next
- All VMs need tags - one tag per category max!
  - VM that serves multiple? Give it the most-secure tag
  - Example: VM serves dev & prod? Then tag as prod

VCF TechCon Powered by VMUG

So, get started today... How?

- Tag your environment!
  - Create an export
  - Give each VM a home
  - Work together with application owners
- Define your shared services
  - What applies to for all VMs?
  - Which services are needed regardless of application?
- Minimum of tools needed:
  - vDefend
  - Syslog
  - Excel (probably)

VCF Tech on
VMUG

daag t
osegm tatie!

Robert Cranendonk

VMUGNL
VMware User Group

VCF TechCon

Powered by VMUG

Start *vandaag* nog met microsegmentatie!

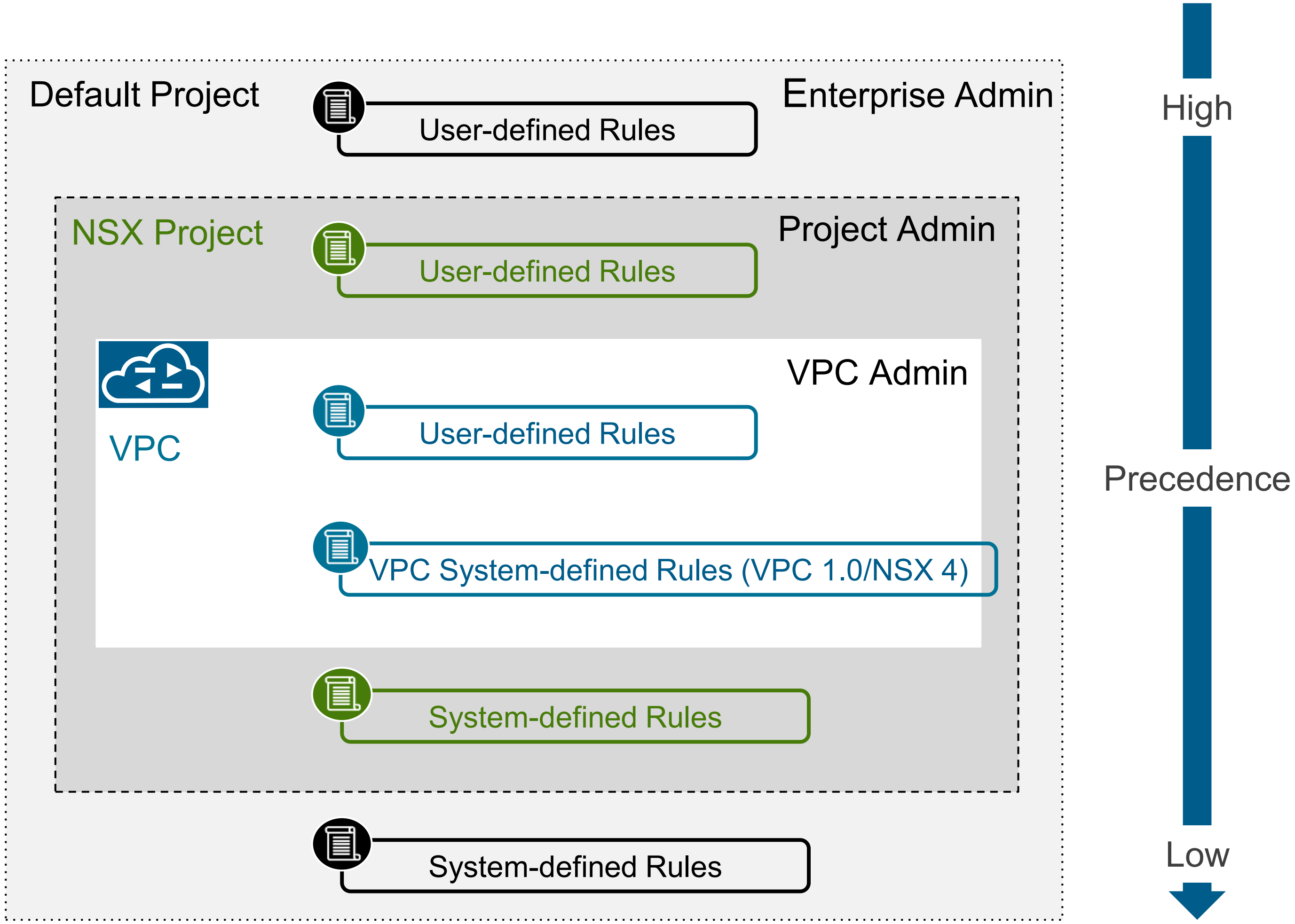
Robert Cranendonk

VMUGNL
VMware User Group

Extra

vDefend Security Policies Across Multi-Tenancy Scope

Distributed Firewall Rules Precedence



DFW Security policies are defined at the multi-tenancy space (Default Project, NSX Project, and VPC) by respective user personas

Default Project and NSX Project user-defined security policies get enforced before the VPC security policies

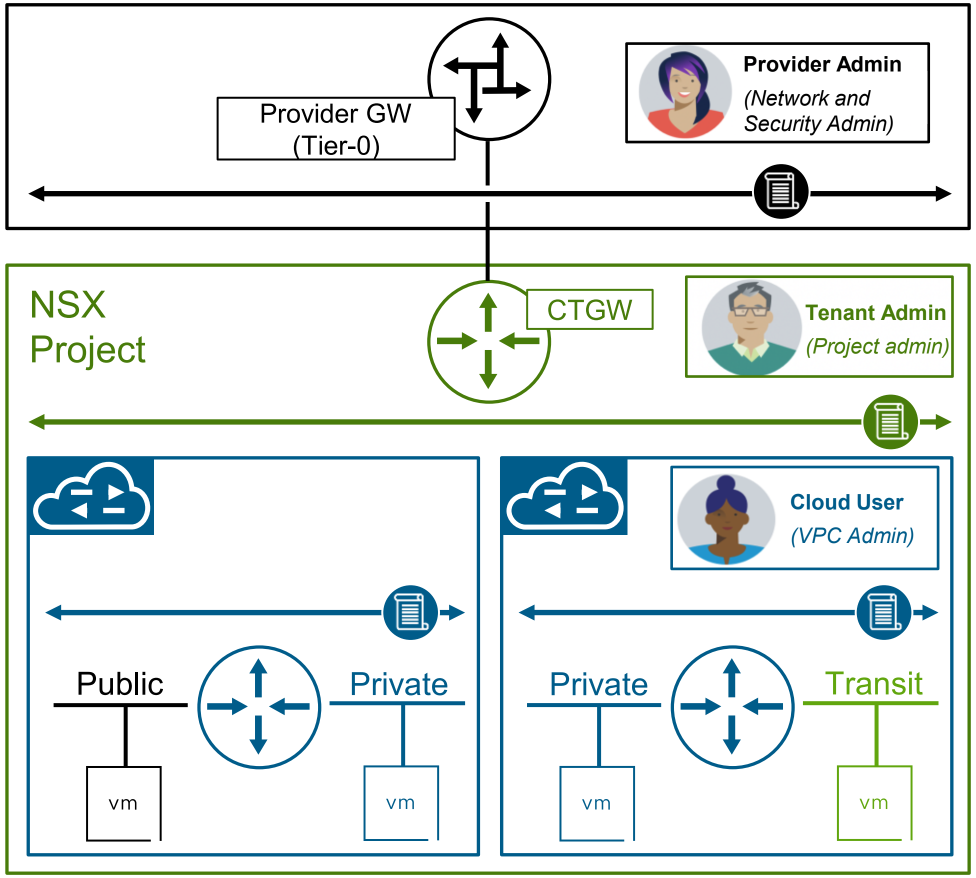
Default Project and NSX Project system-defined (default) security policies get enforced after the VPC security policies

VPC policies by default are hidden in the Project view, but can be shown if desired

Slide courtesy of Broadcom

vDefend Self-Service Security

Persona-specific capabilities with CTGW connectivity



Provider Admin:

- Gateway Firewall on A/S Tier-0
- NSX Project system-defined DFW Policy (on/off)
- Default Project' DFW Policy
- Resource share with Projects

Tenant Admin

- Project DFW Policy
- Project Distributed IDS/IPS
- Project-level Groups, Tags, Services, and Profiles definition
- Resources share with VPCs

Cloud User

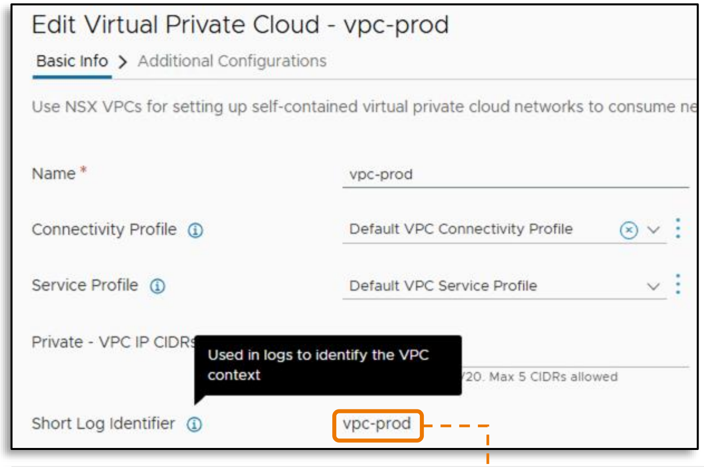
- VPC Groups definition
- VPC E-W Firewall
- VPC N-S Firewall

vmware by Broadcom

Slide courtesy of Broadcom

vDefend Firewall Multi Tenant Logging

Logs segregation for Projects and VPCs

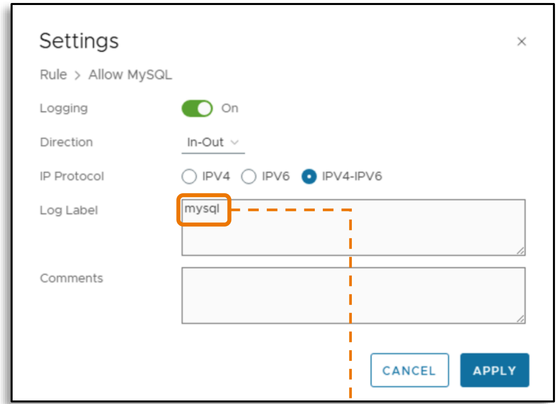


Edit Virtual Private Cloud - vpc-prod

Use NSX VPCs for setting up self-contained virtual private cloud networks to consume ne

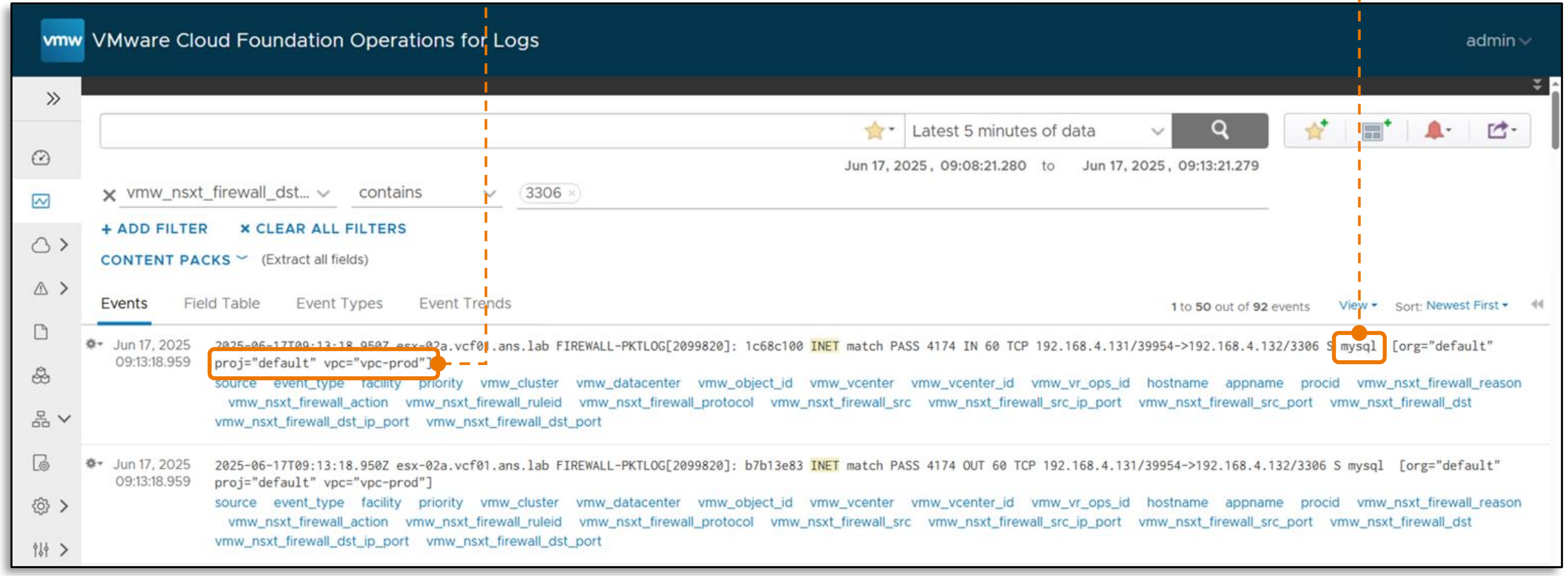
Name *	vpc-prod
Connectivity Profile ⓘ	Default VPC Connectivity Profile
Service Profile ⓘ	Default VPC Service Profile
Private - VPC IP CIDRs	20. Max 5 CIDRs allowed
Short Log Identifier ⓘ	vpc-prod

Used in logs to identify the VPC context



Settings

Logging	On
Direction	In-Out
IP Protocol	○ IPV4 ○ IPV6 ● IPV4-IPV6
Log Label	mysql
Comments	



Jun 17, 2025, 09:08:21.280 to Jun 17, 2025, 09:13:21.279

vmw_nsxt_firewall_dst... contains 3306

1 to 50 out of 92 events

Jun 17, 2025 09:13:18.959

```
2025-06-17T09:13:18.950Z esx-02a.vcf01.ans.lab FIREWALL-PKTLOG[2099820]: 1c68c100 INET match PASS 4174 IN 60 TCP 192.168.4.131/39954->192.168.4.132/3306 S mysql [org="default"
proj="default" vpc="vpc-prod"]
```

source event_type facility priority vmw_cluster vmw_datacenter vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id hostname appname procid vmw_nsxt_firewall_reason vmw_nsxt_firewall_action vmw_nsxt_firewall_ruleid vmw_nsxt_firewall_protocol vmw_nsxt_firewall_src vmw_nsxt_firewall_src_ip_port vmw_nsxt_firewall_src_port vmw_nsxt_firewall_dst vmw_nsxt_firewall_dst_ip_port vmw_nsxt_firewall_dst_port

Jun 17, 2025 09:13:18.959

```
2025-06-17T09:13:18.950Z esx-02a.vcf01.ans.lab FIREWALL-PKTLOG[2099820]: b7b13e83 INET match PASS 4174 OUT 60 TCP 192.168.4.131/39954->192.168.4.132/3306 S mysql  [org="default"
proj="default" vpc="vpc-prod"]
```

source event_type facility priority vmw_cluster vmw_datacenter vmw_object_id vmw_vcenter vmw_vcenter_id vmw_vr_ops_id hostname appname procid vmw_nsxt_firewall_reason vmw_nsxt_firewall_action vmw_nsxt_firewall_ruleid vmw_nsxt_firewall_protocol vmw_nsxt_firewall_src vmw_nsxt_firewall_src_ip_port vmw_nsxt_firewall_src_port vmw_nsxt_firewall_dst vmw_nsxt_firewall_dst_ip_port vmw_nsxt_firewall_dst_port

NSX Project and VPC unique Short Log Identifiers

Appended to the DFW and GFW rules with logging enabled

Easy logs filtering for a specific Project and VPC workload

Set at the creation time and can’t be changed later

If not specified, a system one is generated

Rule-level log labels are also appended to the firewall logs

vmware by Broadcom

Slide courtesy of Broadcom