

Citrix NetScaler 1000V with vPath



Gunnar Anderson, Cisco Product Manager
Sonali Kalje, Cisco Technical Marketing Engineer
Eric Keener, Cisco Product Marketing Manager [host]
Steven Barnes, Citrix NetScaler Technical Specialist

Cisco Nexus 1000V and NetScaler 1000V Resources

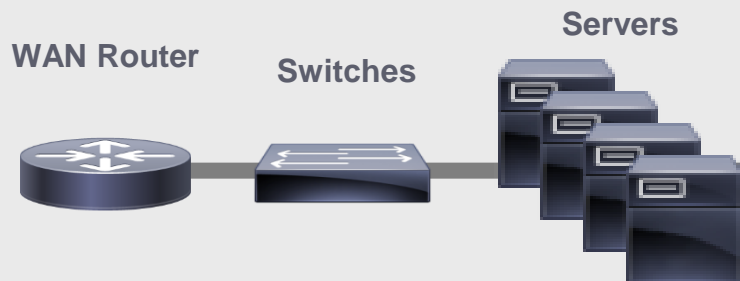
External Links

- Nexus 1000V & Virtual Services: <http://www.cisco.com/go/1000v>
- Citrix NetScaler 1000V: <http://www.cisco.com/go/ns1000v>
- Nexus 1000V & Virtual Services Community: <http://www.cisco.com/go/1000vcommunity>
(recording and presentation from today posted here within 24 hours)
- vPath Ecosystem, Release 2.5 (includes N1KV, VSG, ASA1KV, vWAAS, Prime NSC, and NS1000V)
http://www.cisco.com/cisco/web/docs/solutions/n1kv/vpath-ecosys/2_5/index.html

Cisco Virtual Networking and Cloud Network Services

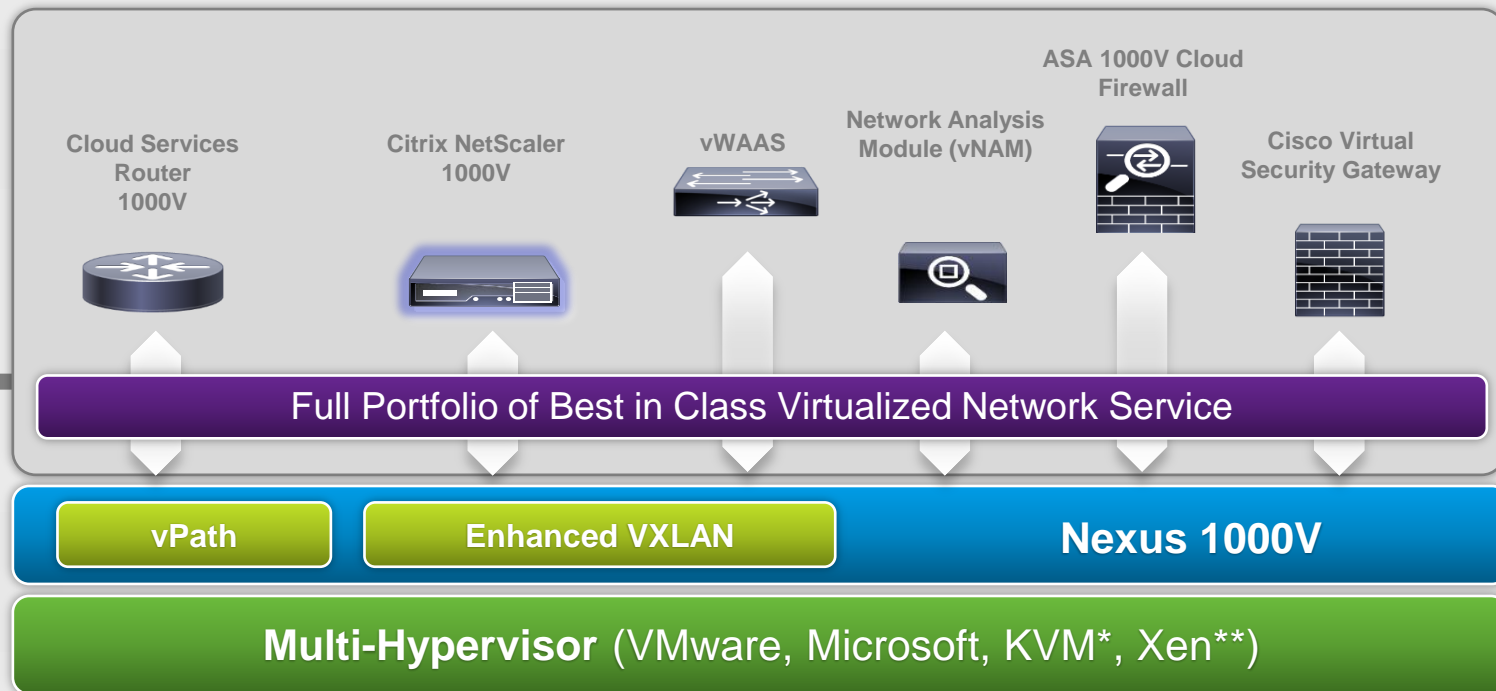
PHYSICAL INFRASTRUCTURE

Integration with Network Fabric



Single Network

CLOUD NETWORK SERVICES



*KVM in beta, ** Xen Targeted 2H-CY'14

Nexus 1000V	VSG	ASA 1000V	vWAAS	CSR 1000V (Cloud Router)	Ecosystem Services
<ul style="list-style-type: none"> Distributed switch NX-OS consistency 	<ul style="list-style-type: none"> VM-level controls Zone-based FW 	<ul style="list-style-type: none"> Edge firewall, VPN Protocol Inspection 	<ul style="list-style-type: none"> WAN optimization Application traffic 	<ul style="list-style-type: none"> WAN L3 gateway Routing and VPN 	<ul style="list-style-type: none"> Citrix NetScaler 1000V virtual ADC

Citrix NetScaler 1000V on Cloud Services Portfolio

- Citrix Best-in-Class virtual application delivery controller (vADC)
- Sold and supported exclusively Cisco
- Tightly integrated via vPath (policy based traffic steering)
- Integrated with Nexus 1100 Series Cloud Services Platform (CSP)
- Part of Cisco Validated Design – VMDC 4.0 VSA



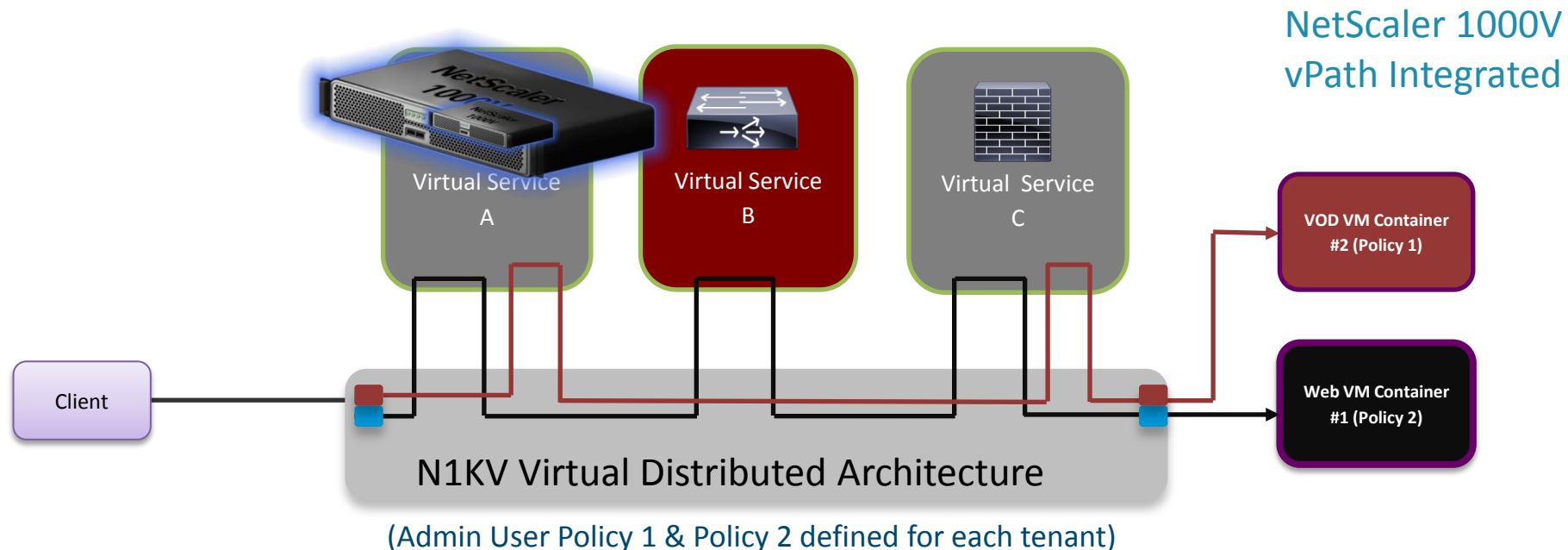
Citrix NetScaler 1000V SKUs

	Editions		
Throughput	Standard	Enterprise	Platinum
500 Mbps	L-NS-1KV-500S=	L-NS-1KV-500E=	L-NS-1KV-500P=
1 Gbps	L-NS-1KV-1KS=	L-NS-1KV-1KE=	L-NS-1KV-1KP=
2 Gbps	L-NS-1KV-2KS=	L-NS-1KV-2KE=	L-NS-1KV-2KP=

Licenses applicable for Nexus 1110/1010 or ESXi

vPath Service Chaining Benefits

- You define which L4-7 Virtual Services through policy, NOT network topology
- Transparent Services Insertion
- Dynamic Service chains enabled per VM/Application/Tenant

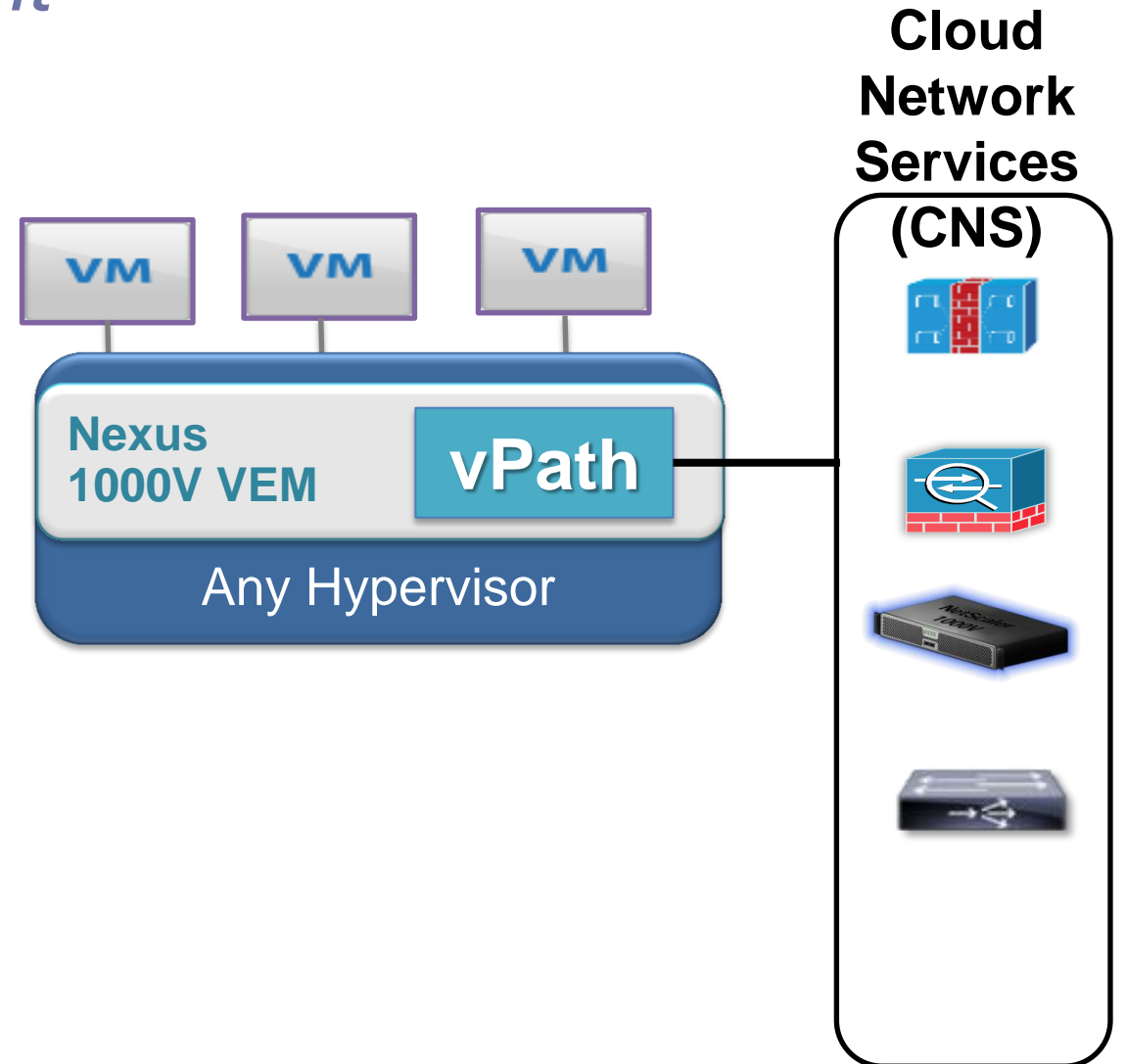


vPATH

Policy Based Service Enablement

vPath is Nexus 1000V dataplane component:

1. Distributed Service insertion architecture, with Intelligent traffic intercept and redirection mechanism
2. Intelligent Service insertion at hypervisor level
3. Topology agnostic service insertion model
4. Service Chaining across multiple virtual services
5. Performance acceleration with vPath e.g. VSG flow offload
6. Efficient and Scalable Architecture
7. VM Policy mobility with VM mobility



vPath Benefits

Without vPath

- Complex deployment- per host service nodes
- Service chaining is static
- No Fast path acceleration
- Services tightly coupled with network topology

With vPath

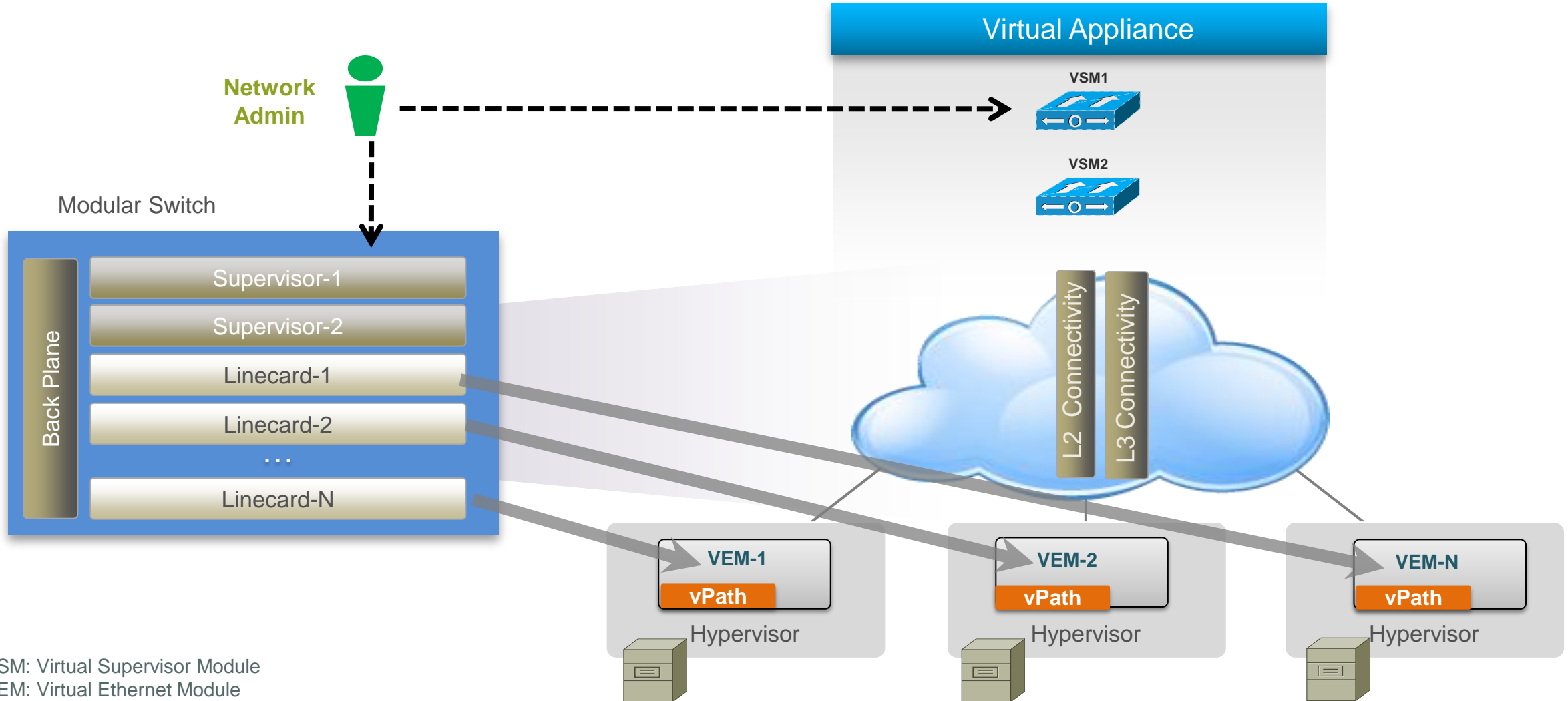
- Distributed policy-driven Service Insertion & chaining
- Non-disruptive operations
- Fast-Path acceleration
- Decouple services from network topology

Evolve the Network for the next wave of application requirements

NetScaler 1000V

- vPath Architecture Overview
- Why vPath with NetScaler
- Use cases

Nexus 1000V Architecture with vPath

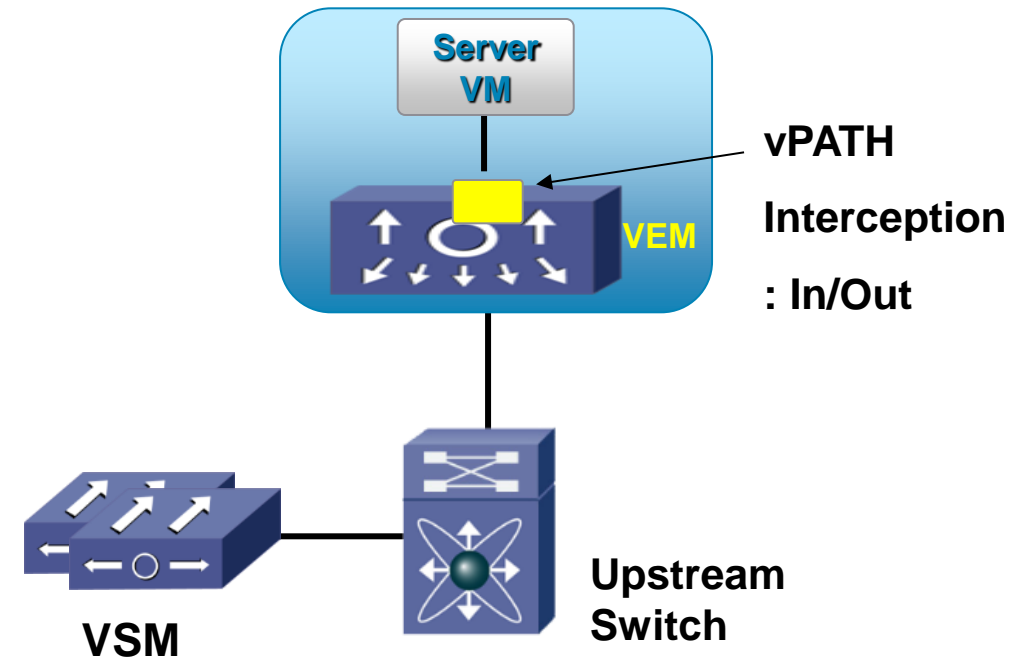


VSM: Virtual Supervisor Module
VEM: Virtual Ethernet Module

vPath

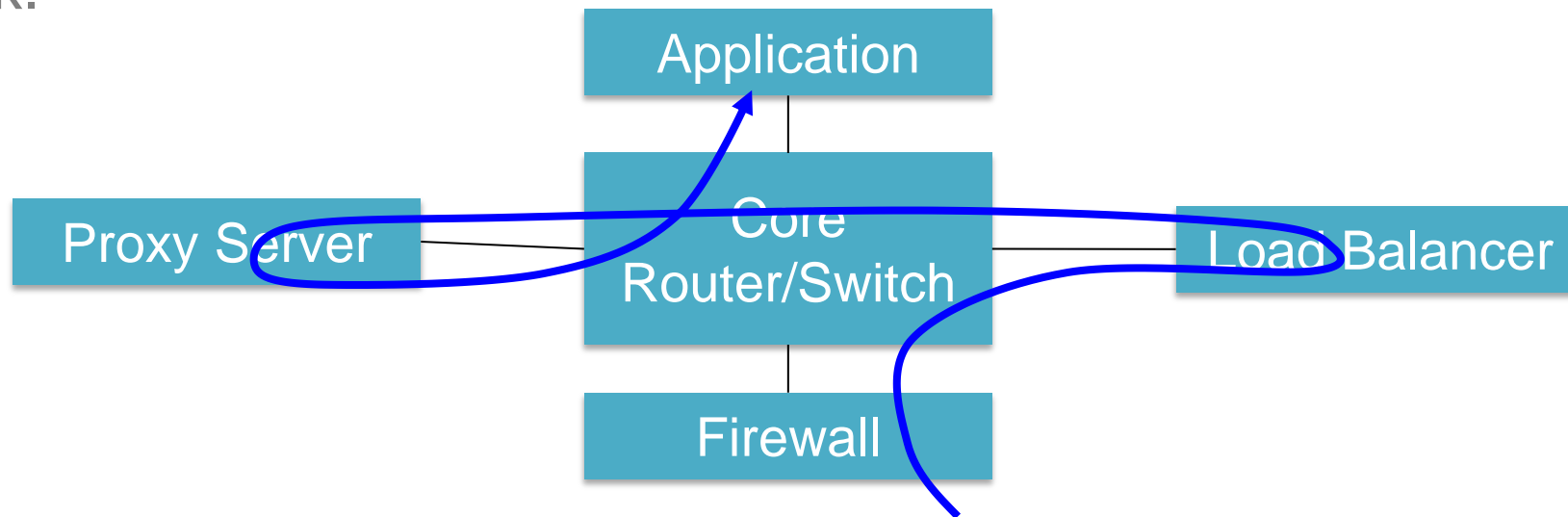
Services enabled per VNIC

- vPath enables service insertion based on policies created for Application VM's
- vPATH Interception is configured on Server VM's Port Profile in both directions to redirect packets to a Service Node
- Server traffic is intercepted by vPATH interception in VEM and redirected to a Virtual Service Node
- Both ingress and egress traffic for a VM is intercepted by vPath



Application Requirements for Network Services

- Current generation network capabilities are driven by physical network topology. Example, If the firewall is plugged into the Internet connection and then the load balancer into firewall, the path of traffic must always flow in that order.
- Application driven requirements that change the relationship (load balancing, then firewall) cannot be supported without physically changing the layout of the network.



SLB : Challenges today

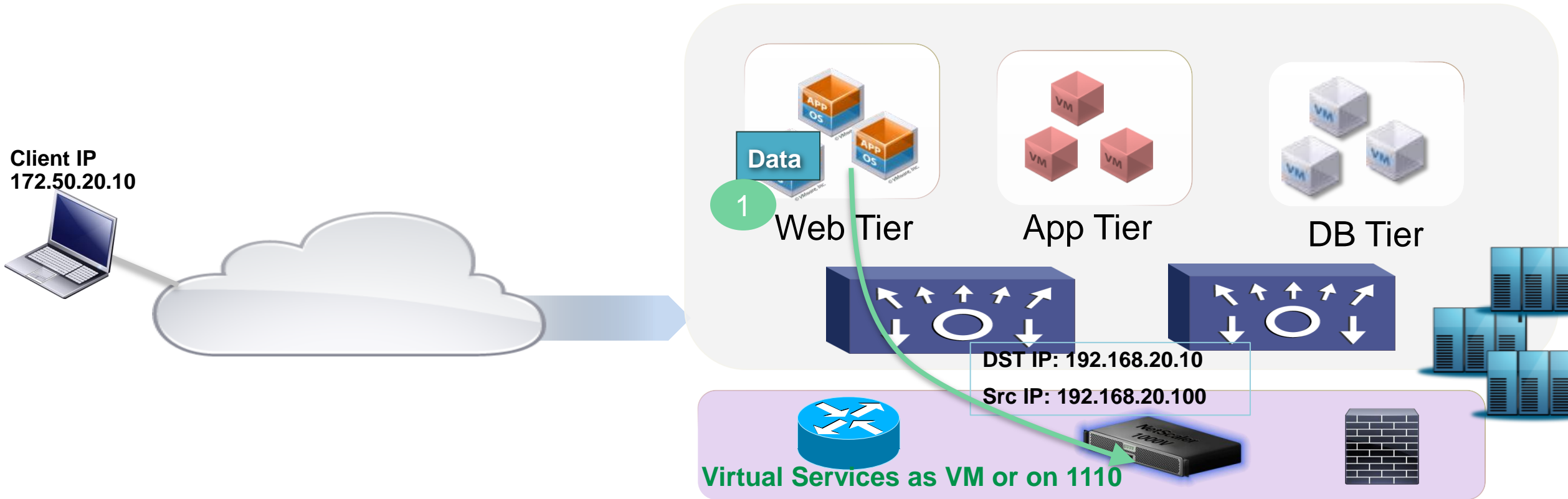
- Source NAT (SNAT) is primarily for its simplicity, however client source is obscured often preventing SNAT deployment
- Policy Based Routing (PBR) is a partial solution to preserve the client source, but increases deployment complexity and operation cost
- Inline ADC's become performance bottleneck high-performance and scalable datacenters
- Despite this performance limitation, the most deployments (> 70%) are inline due to their relative simplicity in configuration
- Only necessary traffic needs to be sent to ADC for optimal capacity usage

SLB : with vPath

vPath is the solution :

- No SNAT needs to be configured on NetScaler 1000V; vPath redirects return traffic to SLB
- Application workload and East-West services (eg. Firewall) have full visibility into source and destination VM
- ADC is not required to be deployed as a gateway or inline mode for application VM's. vPath redirection will handle traffic flows to SLB
- Enables policy-based service chaining for applications; decouple services from underlying network
- Enables new use-cases for SLB in east-west flows

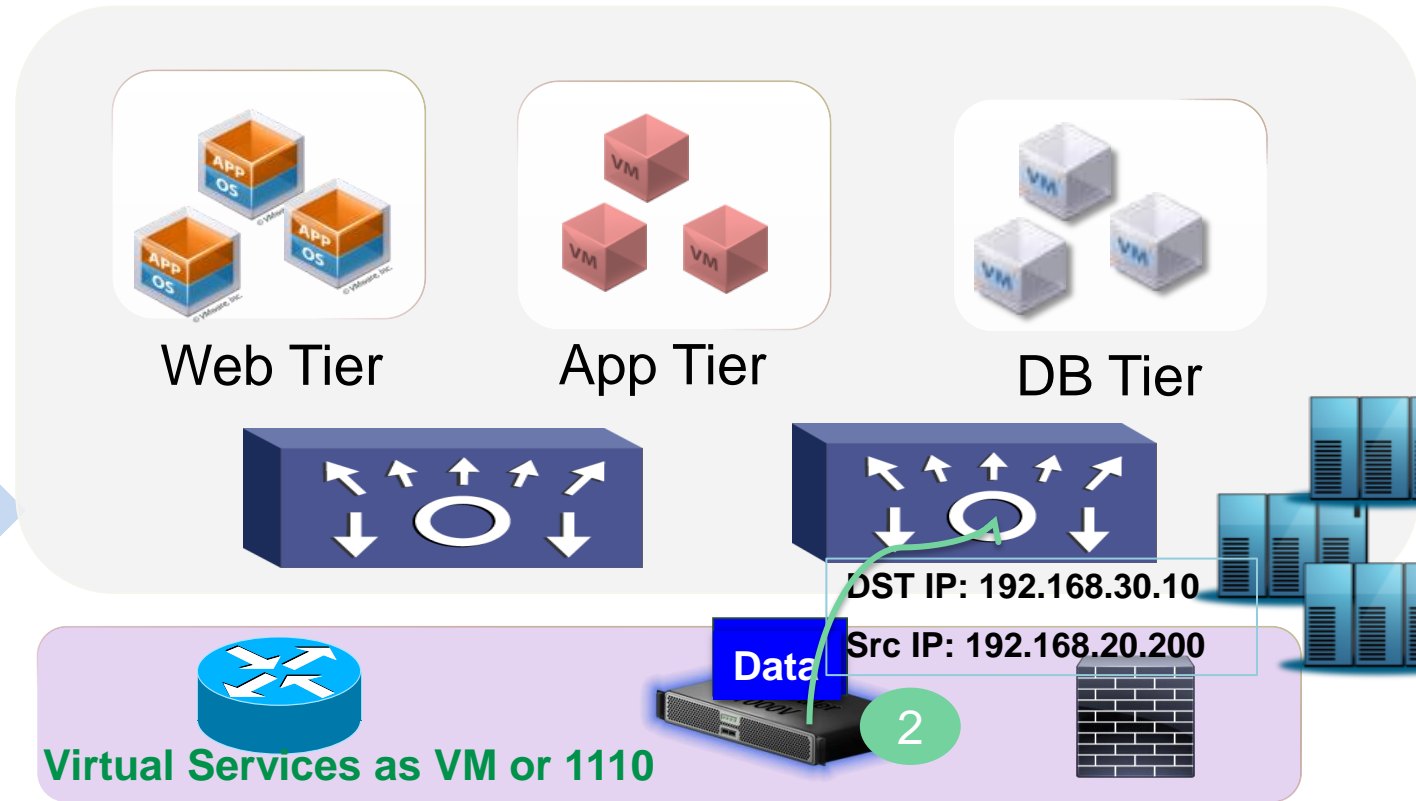

NetScaler 1000V without vPath East-West / Distributed Services



- 1 Web Server initiates connection to App Server with LB service enabled, so Destination is VIP

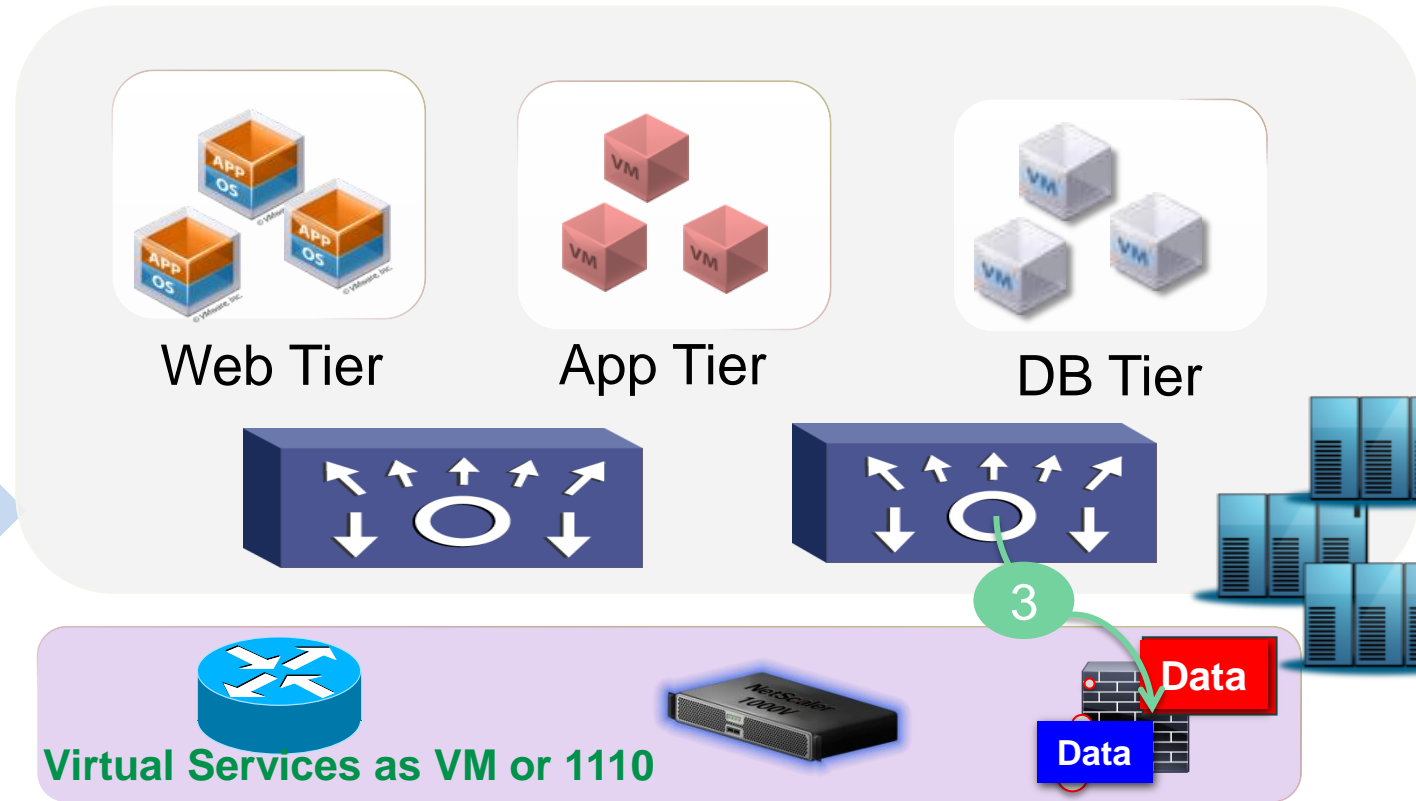
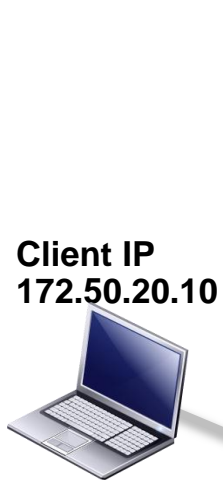
NetScaler 1000V without vPath East-West / Distributed Services

Client IP
172.50.20.10



- 2 VIP selects App Server for the destination; sends packet with destination IP of App Server , and Source IP of SNIP

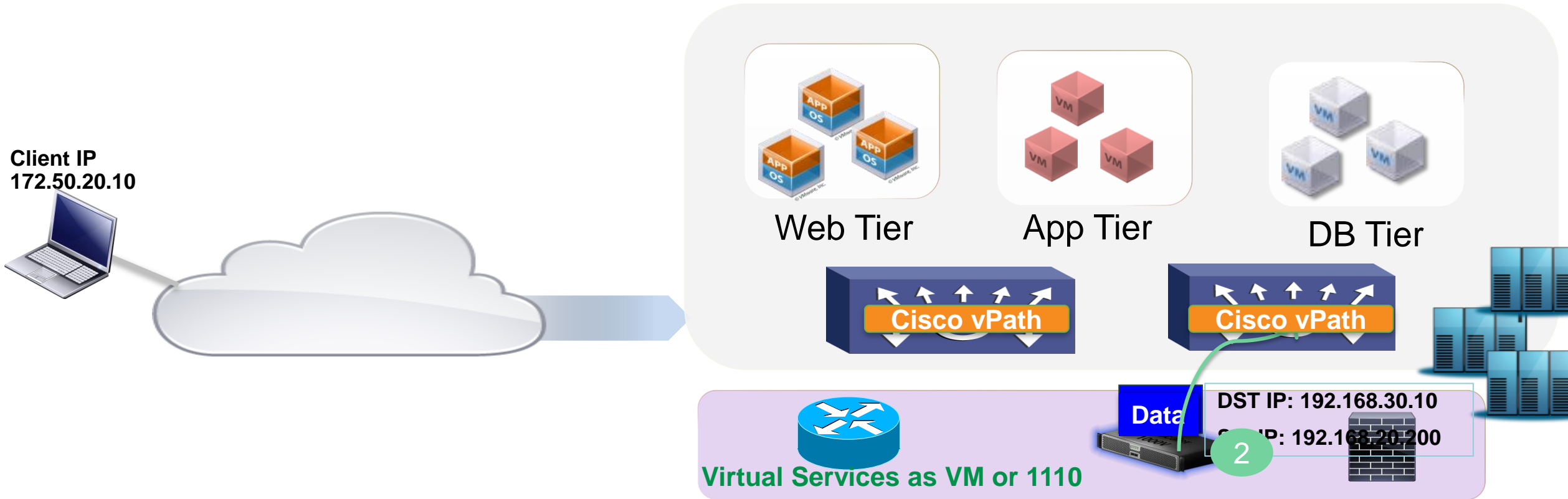
NetScaler 1000V without vPath East-West / Distributed Services



3 Distributed Firewall policy for App Server receives packet, but lacks visibility of Source information for policy evaluation. Policy fails !

Firewall needs to know Source/Client IP for policy evaluation

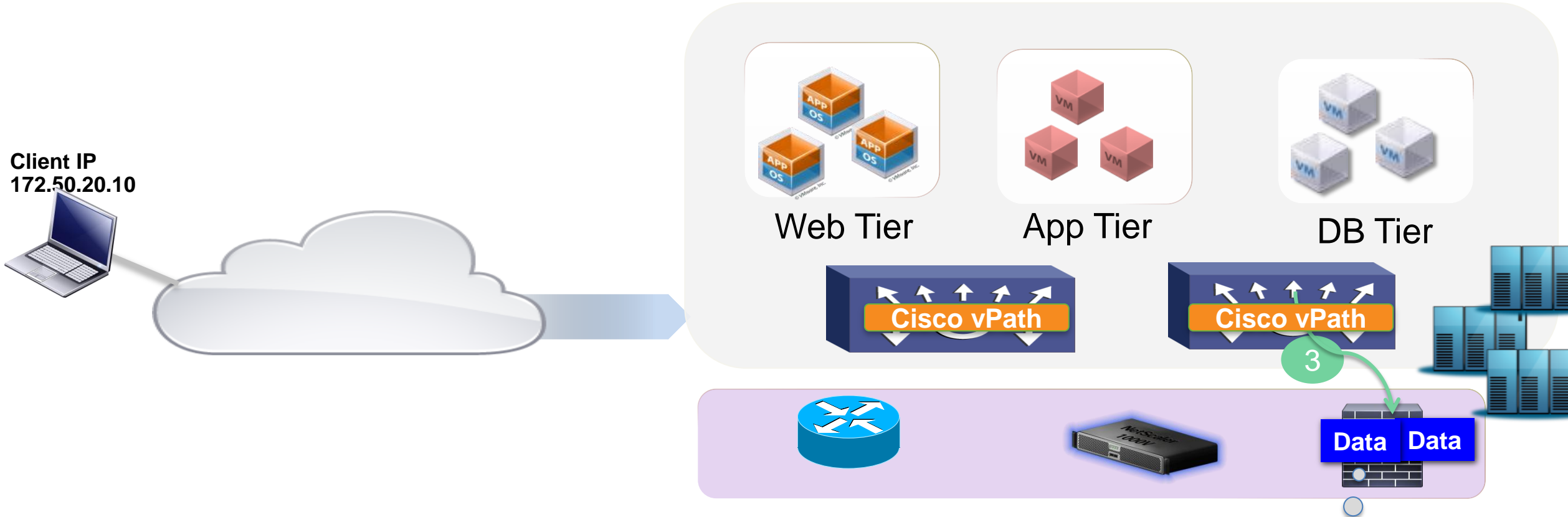
NetScaler 1000V with vPath East-West / Distributed Services



- 2 VIP selects App Server for the destination; sends packet with destination IP of App Server , and Source IP of Client

NetScaler 1000V with vPath

Enabling East-West flow usecase for SLB



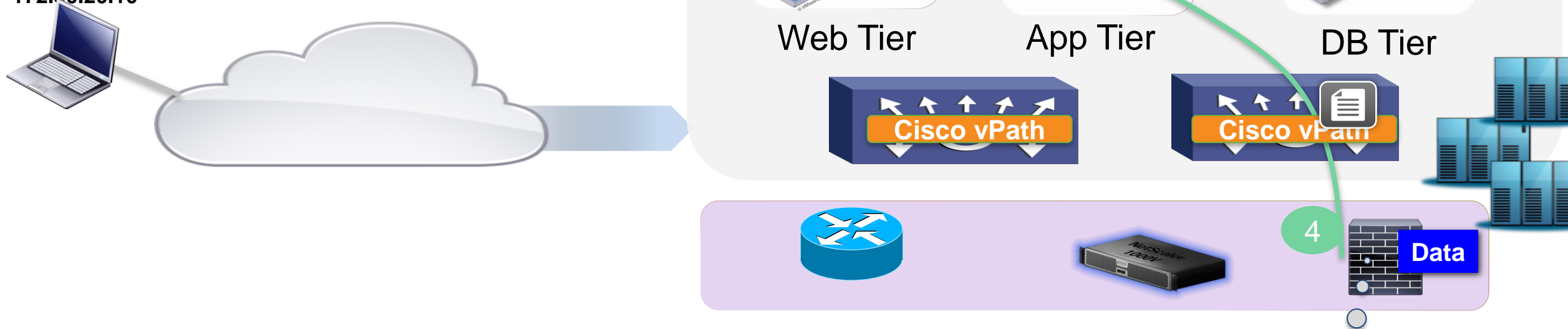
3 Distributed Firewall enabled for App Server receives packet, and has full visibility of Source information for policy evaluation

Firewall has visibility of Source and destination for Policy evaluation

NetScaler 1000V with vPath

- East-West Services and Application Servers ready to deliver best in class services 😊

Client IP
172.50.20.10

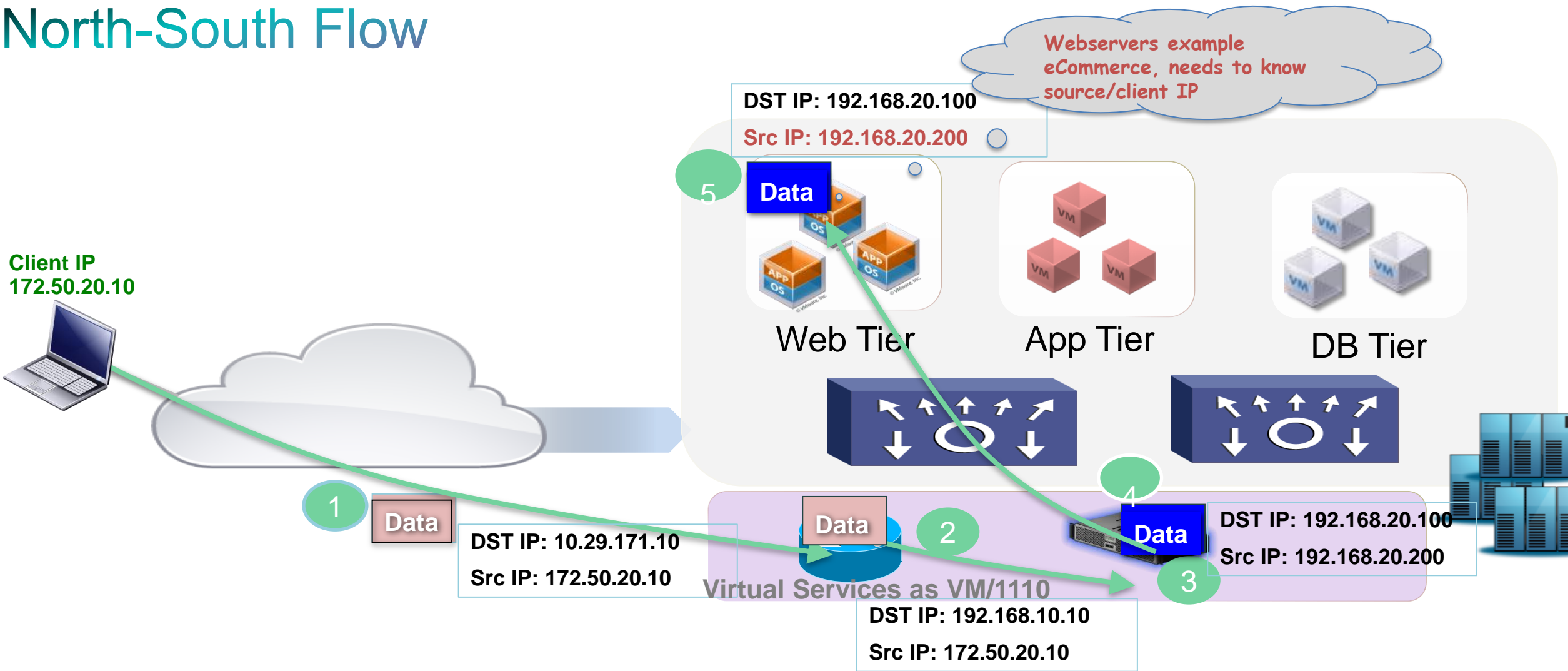


4 Packet is forward to App Server on Policy evaluation

Firewall has visibility of Source and destination for Policy evaluation

NetScaler 1000V without vPath

North-South Flow



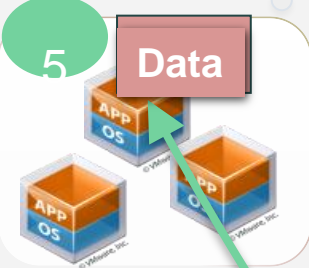
NetScaler 1000V with vPath North-South Flow

Client IP
172.50.20.10

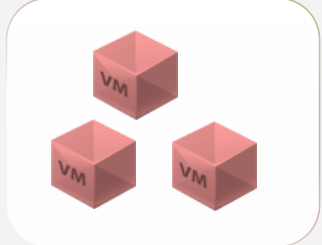


Application knows
the client

DST IP: 192.168.20.100
Src IP: 172.50.20.10



Web Tier



App Tier



DB Tier



DST IP: 10.29.171.10
Src IP: 172.50.20.10

Virtual Services as VM/1110



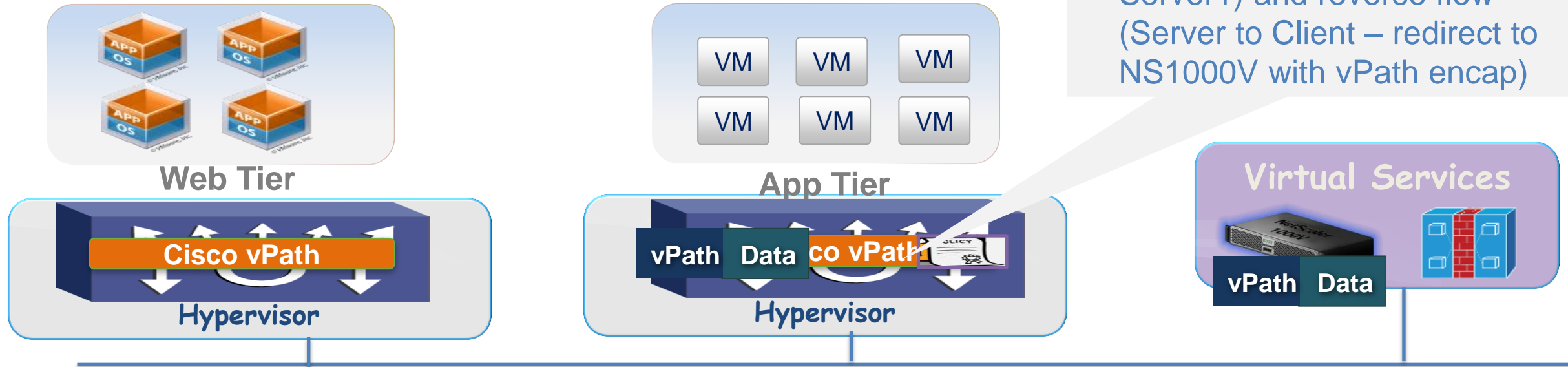
DST IP: 192.168.10.10
Src IP: 172.50.20.10



DST IP: 192.168.20.100
Src IP: 172.50.20.10



NetScaler 1000V with vPath - vPath Flow entry



- All communication between NetScaler1000V and Application Servers happens with vpath encapsulation

SLB - why vPath ?

Without vpath

- ~~Source NAT (SNAT) - Client/ Source Obscured~~
- ~~Policy Based Routing (PBR) - Complex~~
- ~~Inline ADC's - Performance bottleneck~~
- ~~Selective traffic - Optimal implementation~~

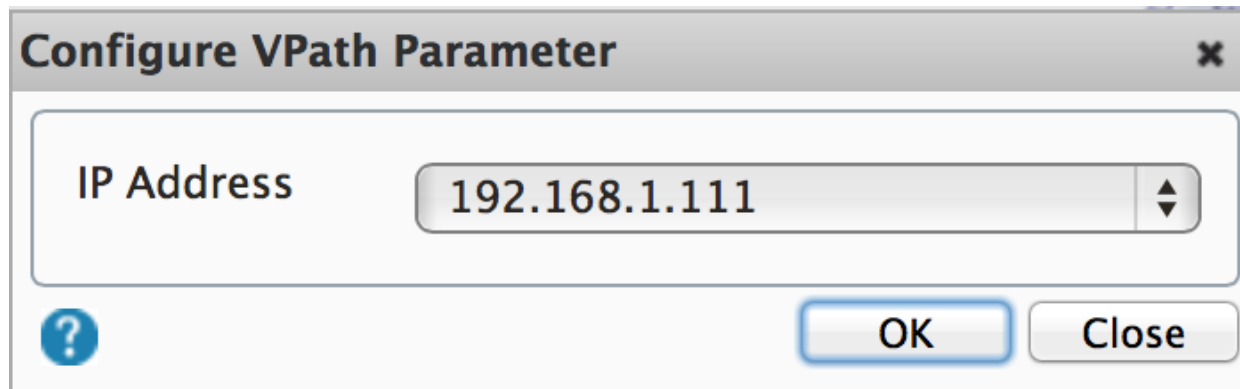
With vPath

- **Preserve Source IP with vPath; vPath redirects server-return traffic to SLB**
- **Easy deployment - Topology agnostic**
- **Service Chaining**
- **Optimal Performance utilization**
- **Enable New east-west flow use cases**

NetScaler 1000V Deployment

NetScaler 1000V Deployment

- **NetScaler 1000V only works with Nexus 1000V-vPath**
- vPath Mode is enabled by default
- One vPath Profile is configured per NS1000V
- Configuration via CLI or NetScaler GUI



Configure VPath Parameter

IP Address 192.168.1.111

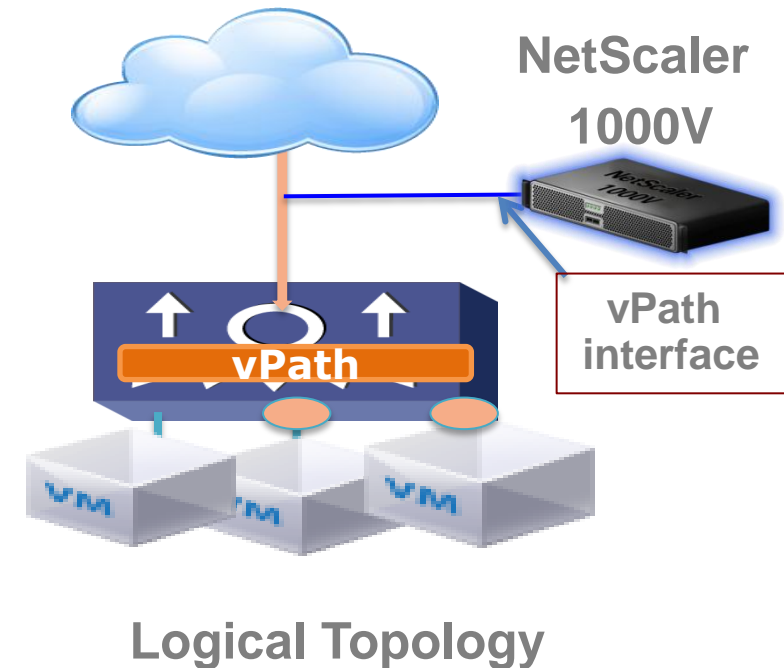
?

OK Close

NetScaler 1000V deployment

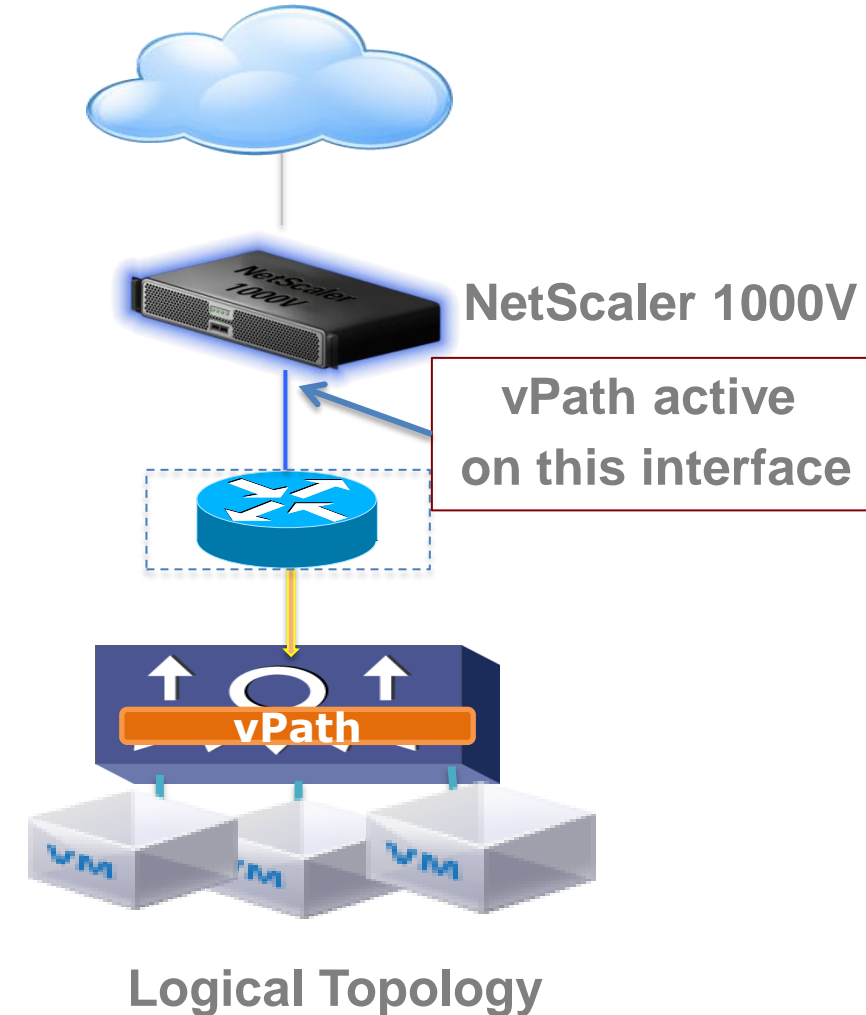
One Arm Mode

- One-armed topologies have several benefits
 - Simple, one network interface
 - Can make use of Link Aggregation to satisfy bandwidth requirements
 - SLB does not have to be default gateway for application VM's
 - Very few failure modes, easing HA failure analysis



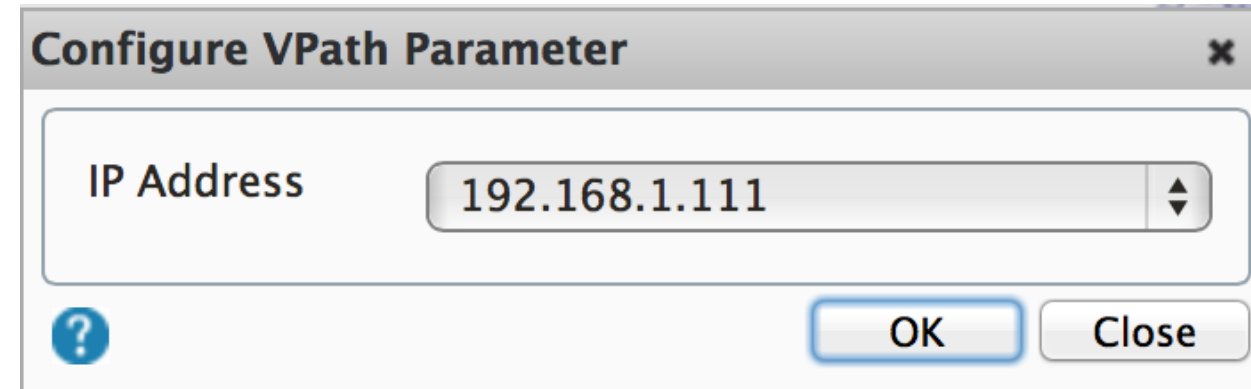
NetScaler 1000V deployment Two Arm Mode

- NetScaler 1000V is inline between client and server (vPath). Can be L3 hops away from Server
- vPath is active on the Inside (server) Interface of NetScaler 1000V
- Allows layer 3 style deployments with split subnets
- Recommend when virtual service enabled ahead of NetScaler 1000V (outbound) in a Service Chain



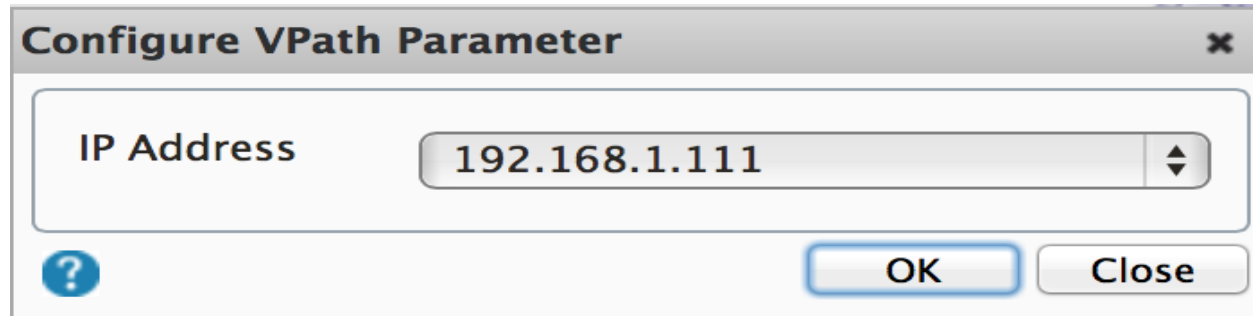
NetScaler1000V Interfaces

- NSIP = NetScaler IP for Management
- SNIP, used for vPath data transport
 - Binds vpath profile with this IP
 - *This IP should be network reachable from vservice VMK interfaces on VEM/ESXi hosts*
- VIPs = Virtual IPs
 - SLB Virtual IP
- NSIP – Used for vPath if no SNIP is configured
- SNIP = Subnet IPs (Proxy Address)
 - This address is used to manage backend service status



NetScaler 1000V

vPath Configurations



Configure VPath Parameter

IP Address 192.168.1.111

OK Close

Subnet IP used as vPath
Source IP for data
transport/redirection

- **Configure NS1000V service node on VSM**

```
vservice node ns1000v-A type adc  
ip address 192.168.1.250  
adjacency I3
```

- **Bind Service to a Port-Profile**

```
Port-profile TenantA  
Vmware port-group  
Switchport mode access  
Switchport access vlan 100  
vservice node ns1000v-A  
No shut  
State en
```

Register NetScaler 1000V
as a Service in Nexus
1000V

Define vPath profile and
attach to Service

vPath Service Chaining

vPath Service Chaining Benefits

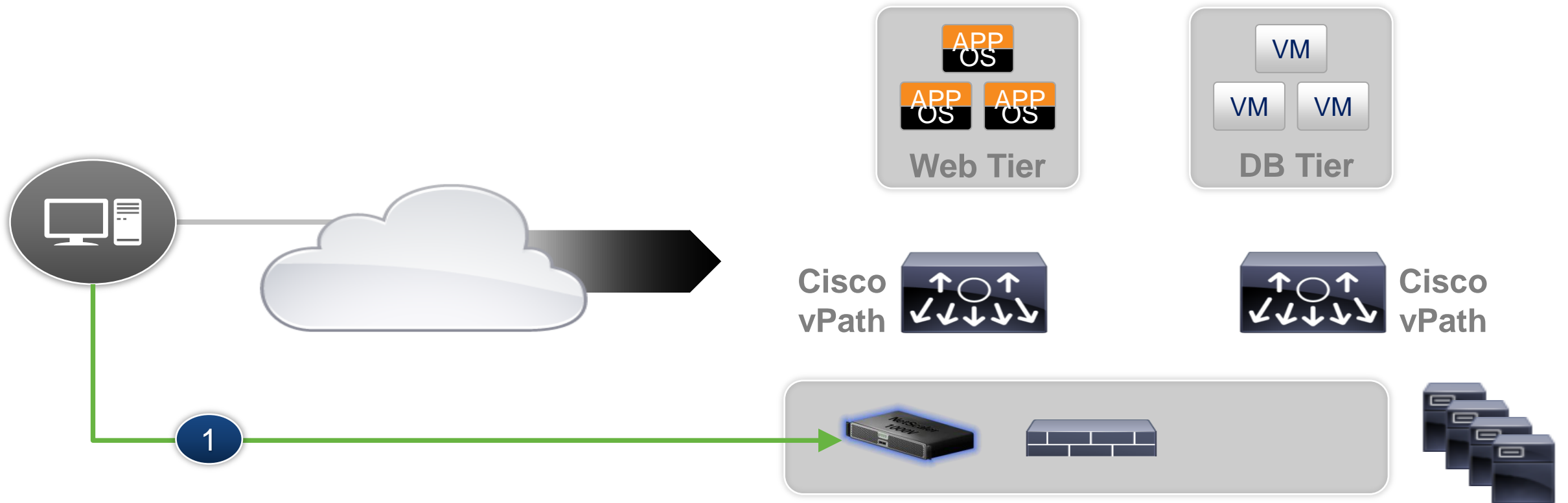
Intelligent policy-based traffic steering through multiple network services

- Decouples network services from underlying network topology with vPath Overlays
- Dynamic Service chains enabled per VM port
- Programmability
- Transparent Services Insertion
- Multi-Tenancy
- VxLAN

Expanded vPath Ecosystem: VSG, ASA 1000V, vWAAS, & NetScaler 1000V

Services Chaining with vPath

Intelligent Policy-based Traffic Steering Through Multiple Network Services



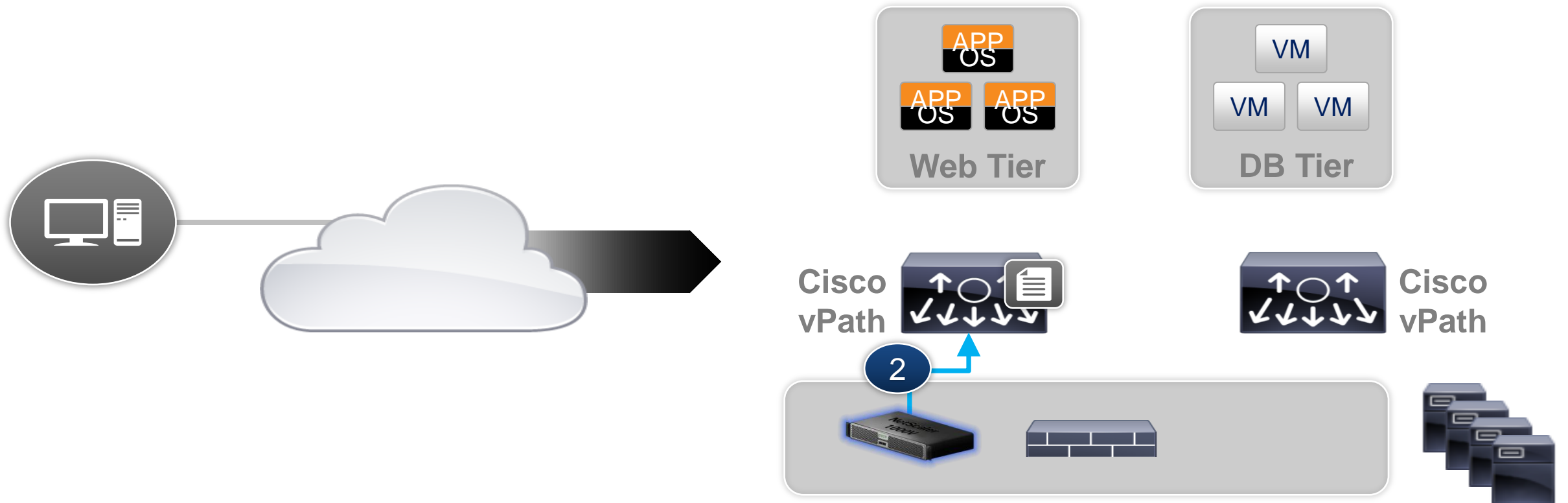
Client Initiates Flow to Web Server (VIP as Server IP)

1

Client > LB-VIP

Services Chaining with vPath

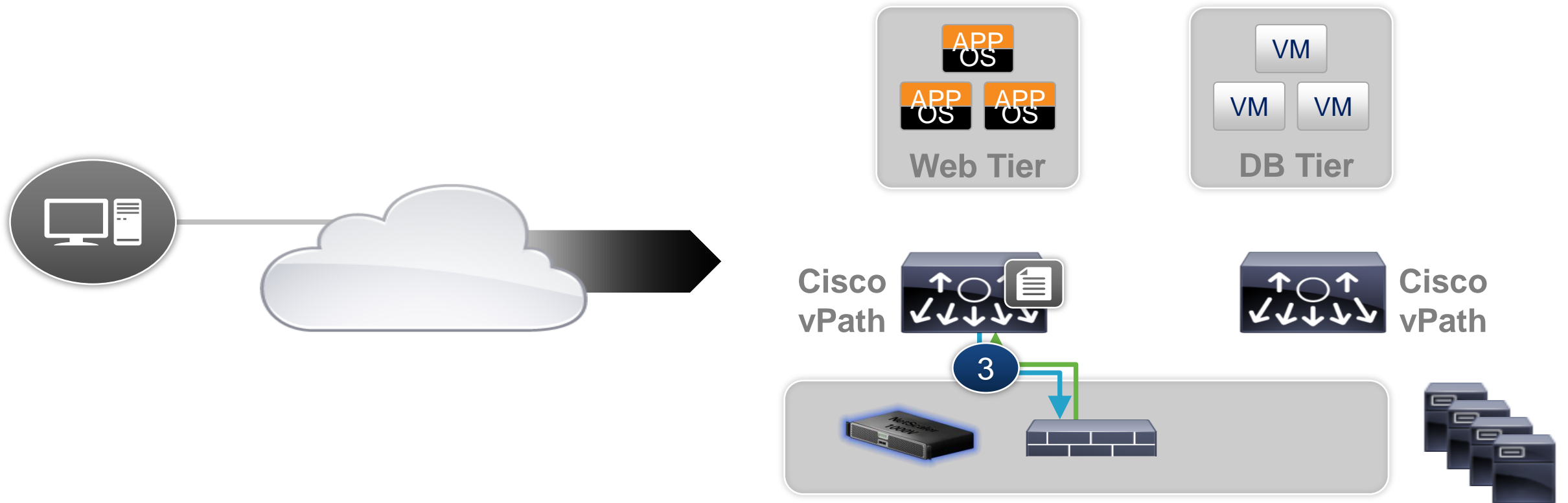
Intelligent Policy-based Traffic Steering Through Multiple Network Services



2 NS1000V load balance web request, selects Web Server 1 (Client > S1)

Services Chaining with vPath

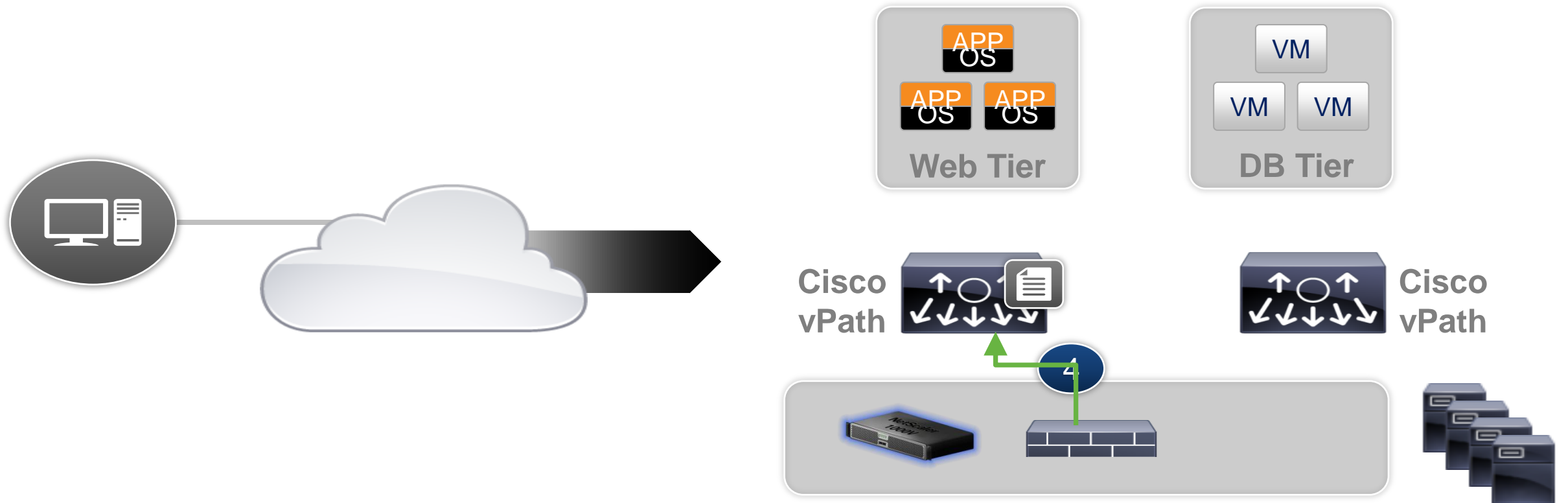
Intelligent Policy-based Traffic Steering Through Multiple Network Services



3 Based on policy, vPath redirect traffic to service chain, starting with zone-based firewall, VSG

Services Chaining with vPath

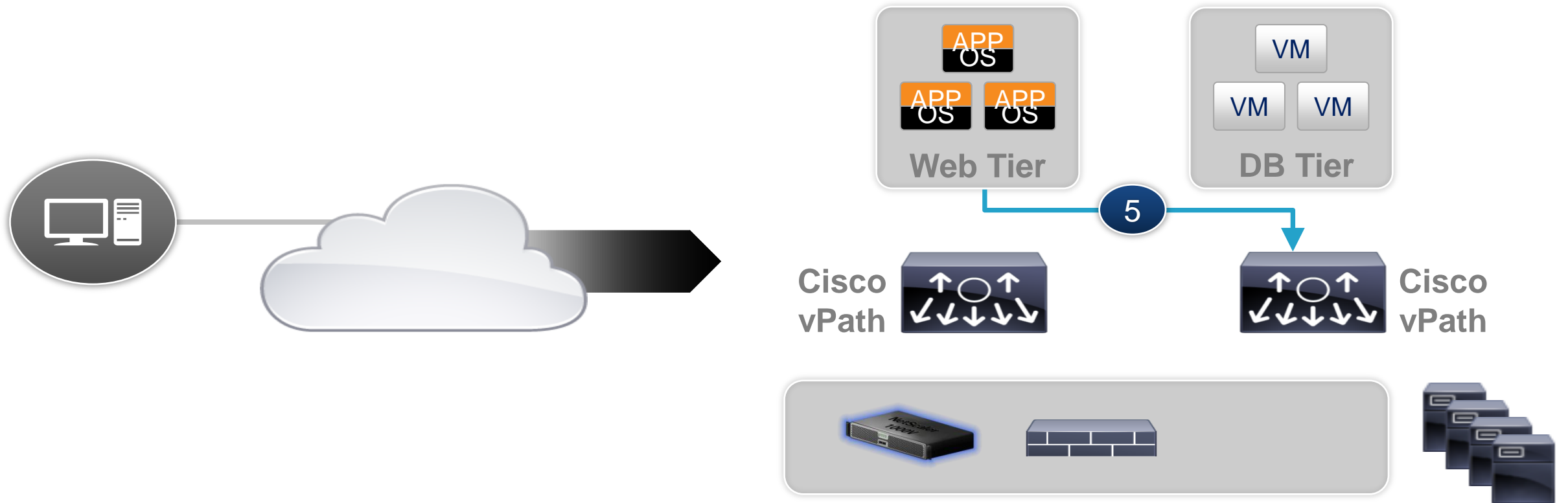
Intelligent Policy-based Traffic Steering Through Multiple Network Services



4 Traffic returns to Virtual Ethernet Module ready for next network service

Services Chaining with vPath

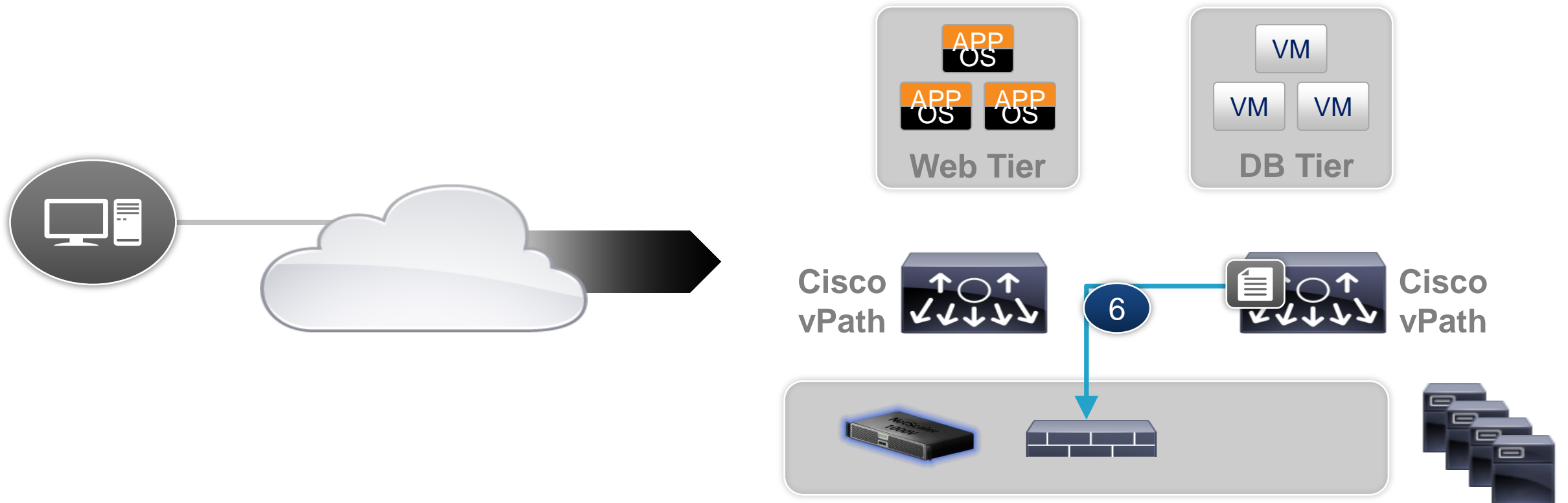
Intelligent Policy-based Traffic Steering Through Multiple Network Services



5 Web to DB Tier Connection

Services Chaining with vPath

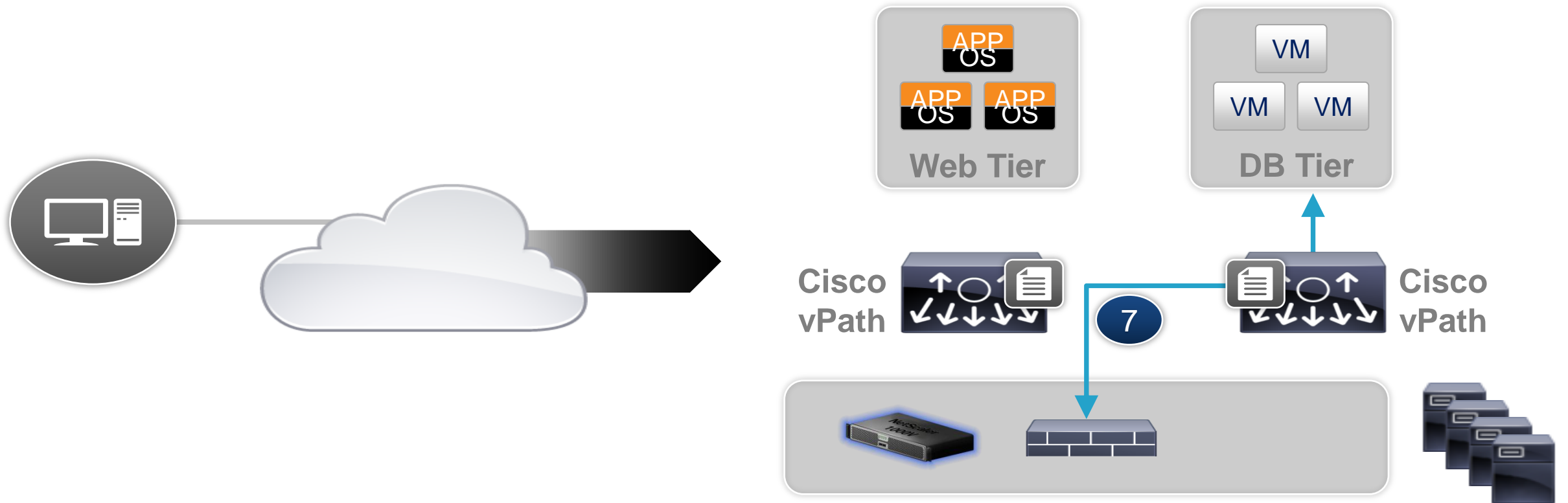
Intelligent Policy-based Traffic Steering Through Multiple Network Services



6 Web to DB Tier Connection : Database tier security policy

Services Chaining with vPath

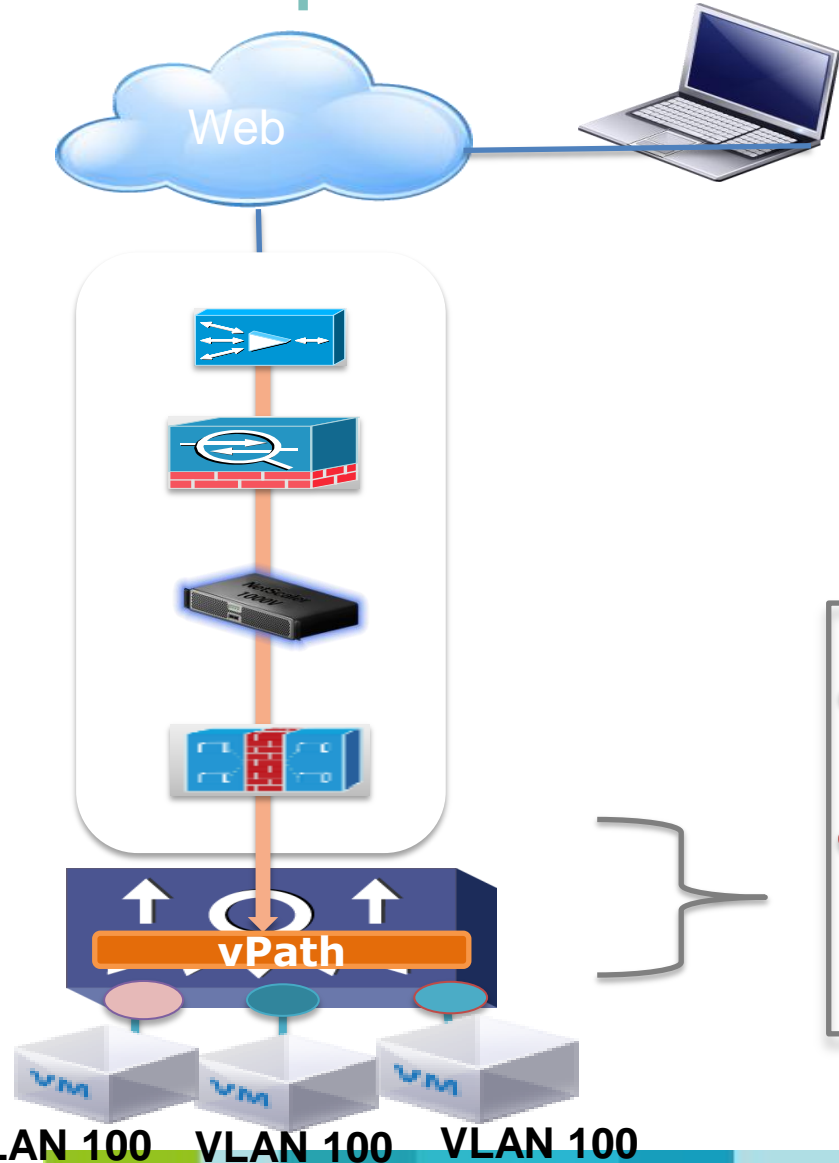
Intelligent Policy-based Traffic Steering Through Multiple Network Services



7 Apply VSG policy and forward packet to database

NetScaler 1000V Use Cases

Enterprise: Multi-Tier Applications



- Intelligent service chaining
- Flat network: As shown, all application workload is on VLAN 100 segment, still each have different set of services enabled
- Service chain stays attached to VM on VM mobility

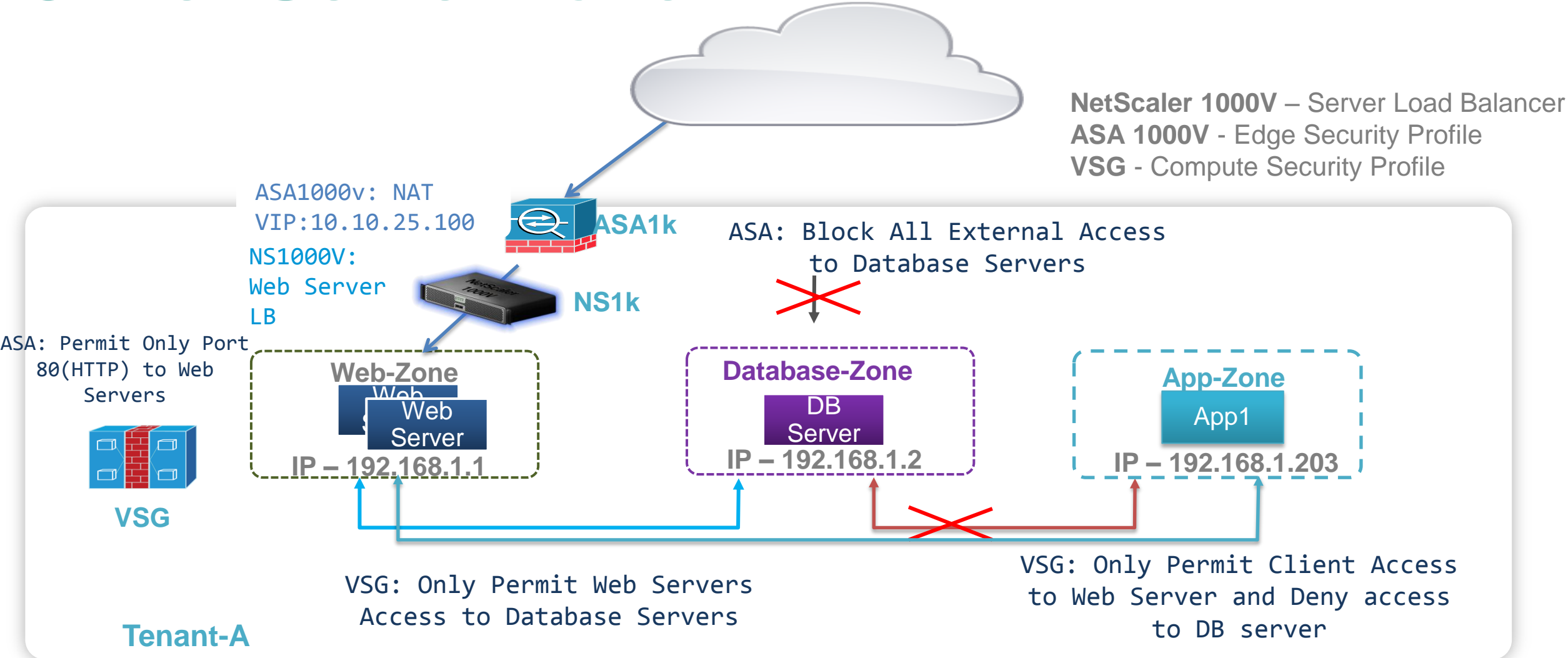
● WAN Optimization + Edge Firewall + NAT + Load Balancer + Web Application Firewall + Zone based Firewall

● Load Balancer + Zone based Firewall

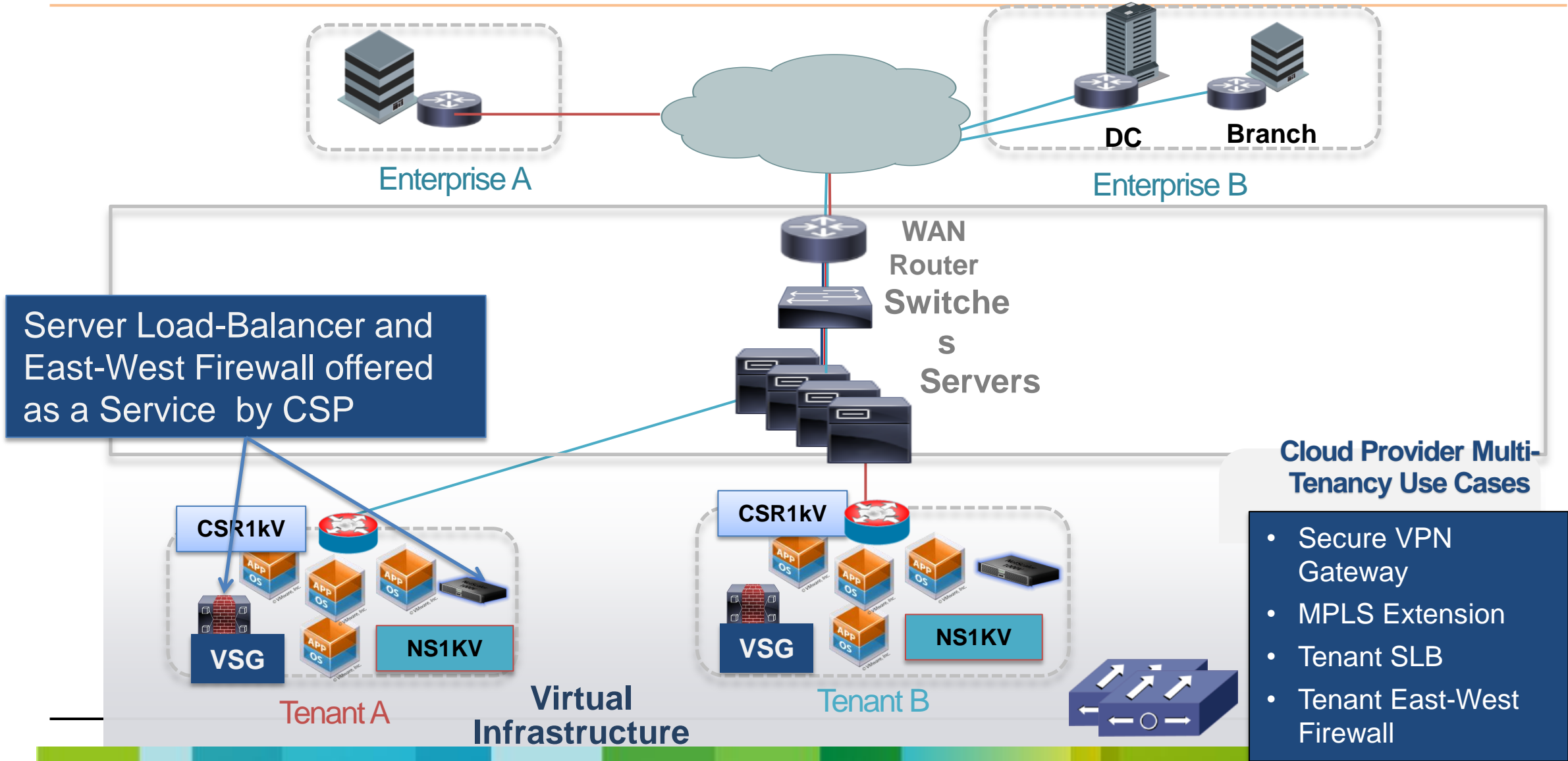
● VSG Zone based Firewall

VLAN 100 VLAN 100 VLAN 100

3-Tier Server zone



Cloud Provider's Data Center Multi-Tenancy



NetScaler 1000V in a Service Chain

```
vservice node VSG type vsg
```

```
ip address 192.168.1.97
```

```
adjacency I3
```

```
vservice node NS1000 type adc
```

```
ip address 192.168.1.99
```

```
adjacency I3
```

```
vservice path chain-TenantA
```

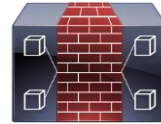
```
node VSG profile sp-web order 10
```

```
node NS1000 order 15
```

```
port-profile type vethernet Tenant-A
```

```
org root/Tenant-A
```

```
vservice path chain-TenantA
```



Defining the Service Nodes
on Nexus 1000V

Chain the Service Nodes

Enable the Service Chain Per
Port-Profile

Port Profile Configuration

```
switch# show port-profile name service-ABC
```

```
port-profile service-ABC
```

```
type: Vethernet
```

```
description:
```

```
status: enabled
```

```
config attributes:
```

```
switchport mode access
```

```
switchport access vlan 270
```

```
org root/ABC
```

```
vservice node ns1000v
```

```
no shutdown
```

```
assigned interfaces:
```

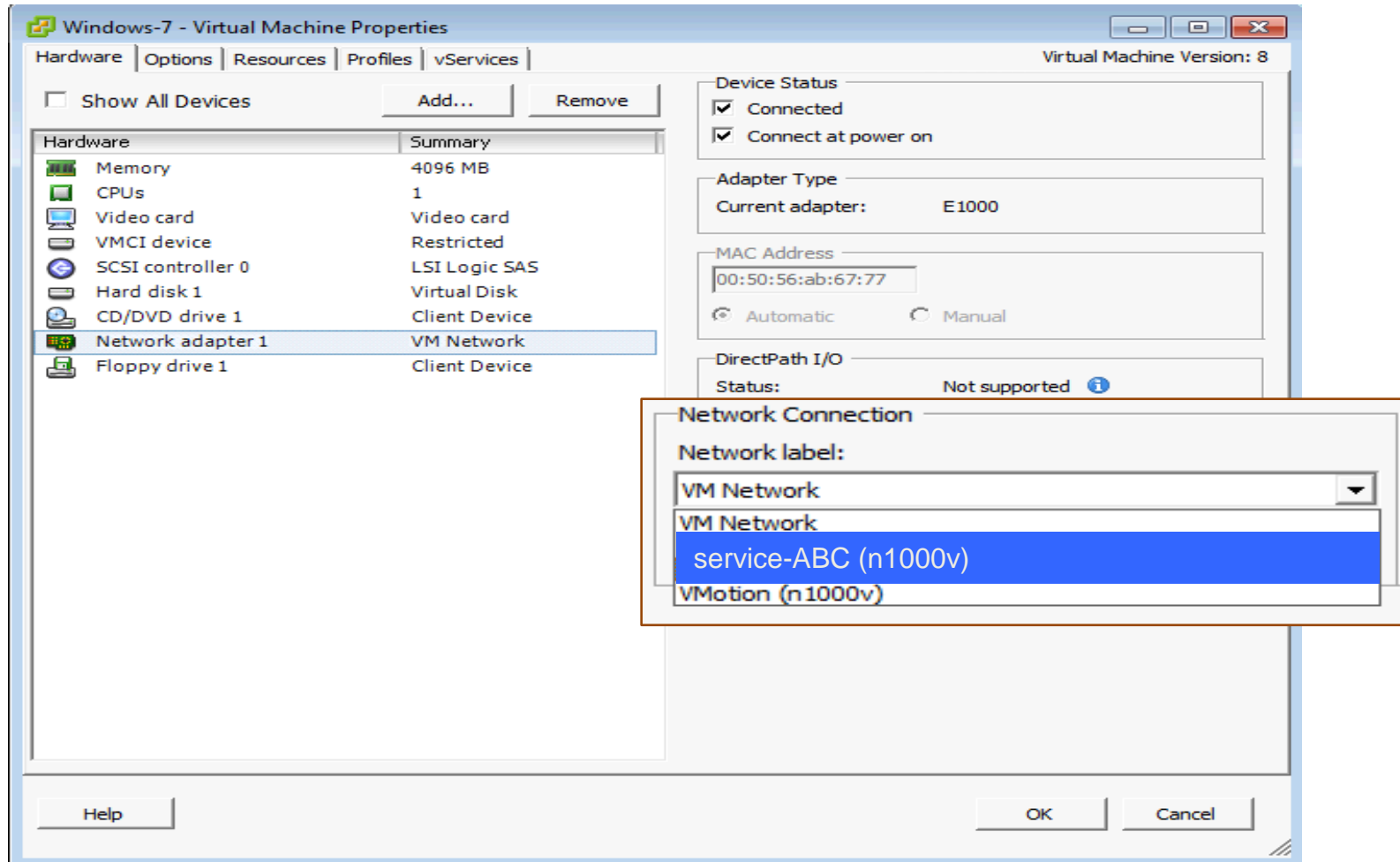
```
Vethernet10
```

```
Vethernet11
```

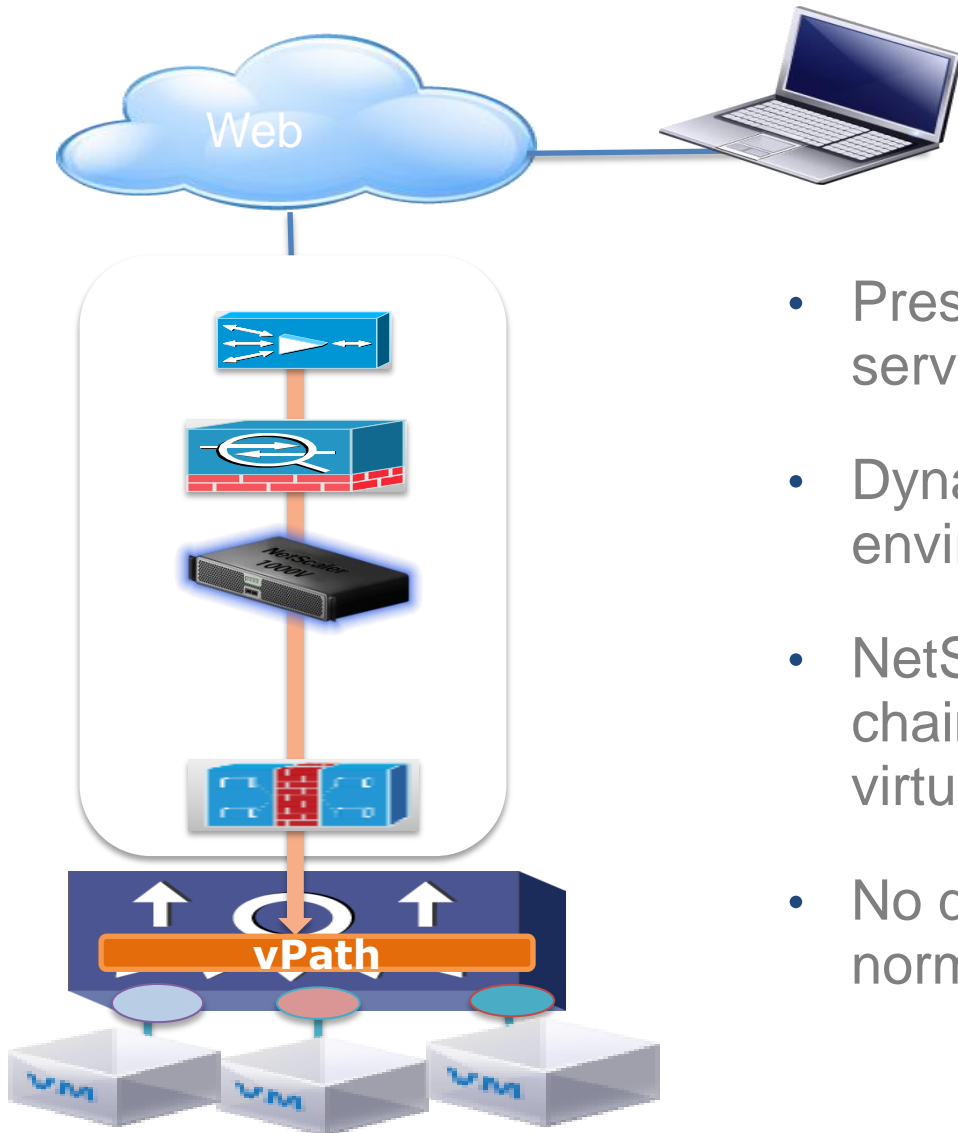
Support Commands Include:

- ✓ Port management
- ✓ VLAN
- ✓ PVLAN
- ✓ Port-Channel
- ✓ ACL
- ✓ Netflow
- ✓ Port security
- ✓ QoS
- ✓ **vService**

Attach VM to Port-Profile in vCenter Server



Key takeaway for NetScaler 1000V with vPath



- Preserve Client IP; No Source NAT or PBR required to send server return traffic to NetScaler1000V
- Dynamic SLB (NS1000V) deployments in Multi-Tenant environment
- NetScaler 1000v gets rich benefits of intelligent service chaining with no worrying about VLAN stitching in dynamic virtual environments
- No disruption to east-west / distributed services, that would normally happen with source NAT

Thank you.

