Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point
vSEC 4 AZURE
„HANDS-ON“

Nils Schäfer
Security Engineer

©2016 Check Point Software Technologies Ltd.

[Protected] Non-confidential content

Check Point®
SOFTWARE TECHNOLOGIES LTD.

HYBRID CLOUD ALLOWS IT TO DELIVER APPLICATIONS IN A FRACTION OF COST AND TIME!

Check Point®
SOFTWARE TECHNOLOGIES LTD.

LEGACY SECURITY IS A SHOWSTOPPER, AND DOESN'T PROTECT APPLICATIONS FROM MODERN THREATS

Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURITY IN THE HYBRID CLOUD….

Must **prevent lateral move of threats** between applications and not only at the perimeter

Should protect new IT services and applications **in seconds** not in weeks

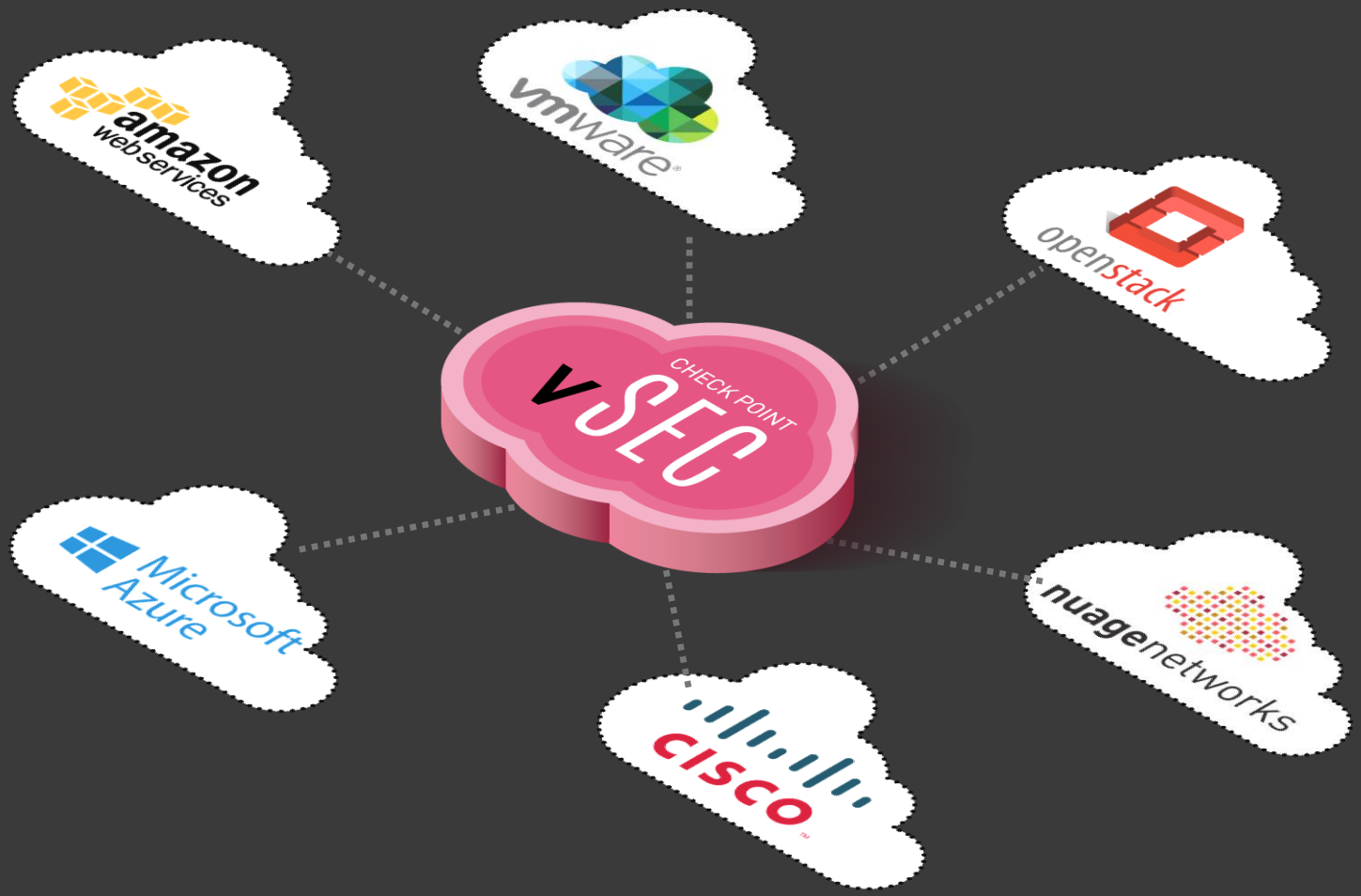
Should **automatically be provisioned and scale** within the environment without operational overhead

Check Point
SOFTWARE TECHNOLOGIES LTD.

INSTANTLY SECURE RAPIDLY-EVOLVING SERVICES IN ALL HYBRID CLOUD ENVIRONMENTS WITH PAY-AS-YOU-GO VIRTUAL SECURITY

SECURE YOUR MODERN DATACENTER
WITH AUTOMATION AND TIGHT SECURITY BETWEEN APPLICATIONS

Check Point
SOFTWARE TECHNOLOGIES LTD.



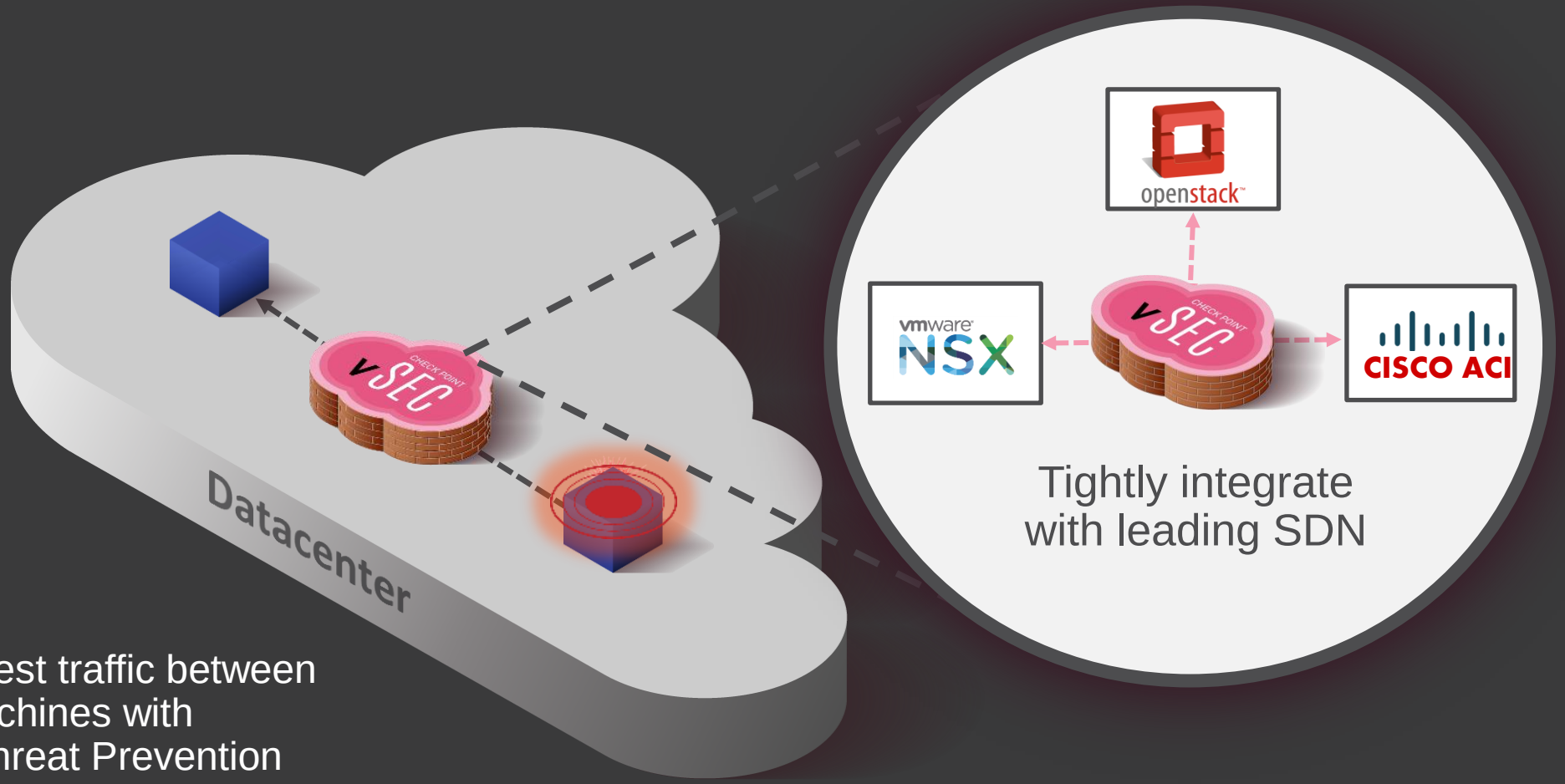
Check Point®
SOFTWARE TECHNOLOGIES LTD.

vSEC SECURES YOUR APPLICATIONS

EVERYWHERE

PREVENT LATERAL THREATS
BETWEEN APPLICATIONS

Check Point
SOFTWARE TECHNOLOGIES LTD.



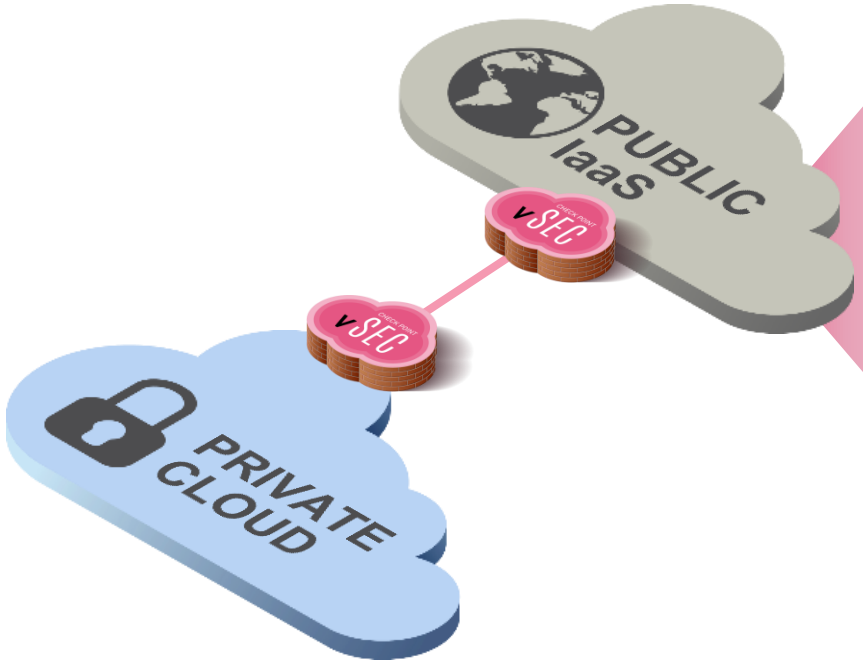
vSEC Inspects East-West traffic between physical and virtual machines with Sandblast Advanced Threat Prevention

SECURE YOUR APPLICATIONS

IN THE HYBRID CLOUD

Check Point
SOFTWARE TECHNOLOGIES LTD.

Extend your vSEC Security
to your Public IaaS



CHECK POINT vSEC — **vSEC for AWS**

CHECK POINT vSEC — **vSEC for Azure**

CHECK POINT vSEC — **vSEC for vCloud Air**

Check Point®
SOFTWARE TECHNOLOGIES LTD.

FROM WEEKS TO SECONDS WITH

vSEC AUTOMATION

vSEC SECURITY AUTOMATION USE CASES

Check Point
SOFTWARE TECHNOLOGIES LTD.

PERFORM THESE OPERATIONS…

- Change application's networking
- Scale up your application
- Virtual Patching
- Provision a new application
- Connect a new IOT device

KNOWING THAT….

- Security is automatically provisioned
- Application is instantly secured
- Application admin never waits
- No tickets overhead
- Everything is auditable

CHECK POINT vSEC

CHANGE APPLICATION NETWORKING

Check Point
SOFTWARE TECHNOLOGIES LTD.

Changing
Web VM IP

App owner opens ticket to FW Admin to change policy → FW admin changes the policy → New policy is published on the weekend

Many Days / Manual process

Legacy Way

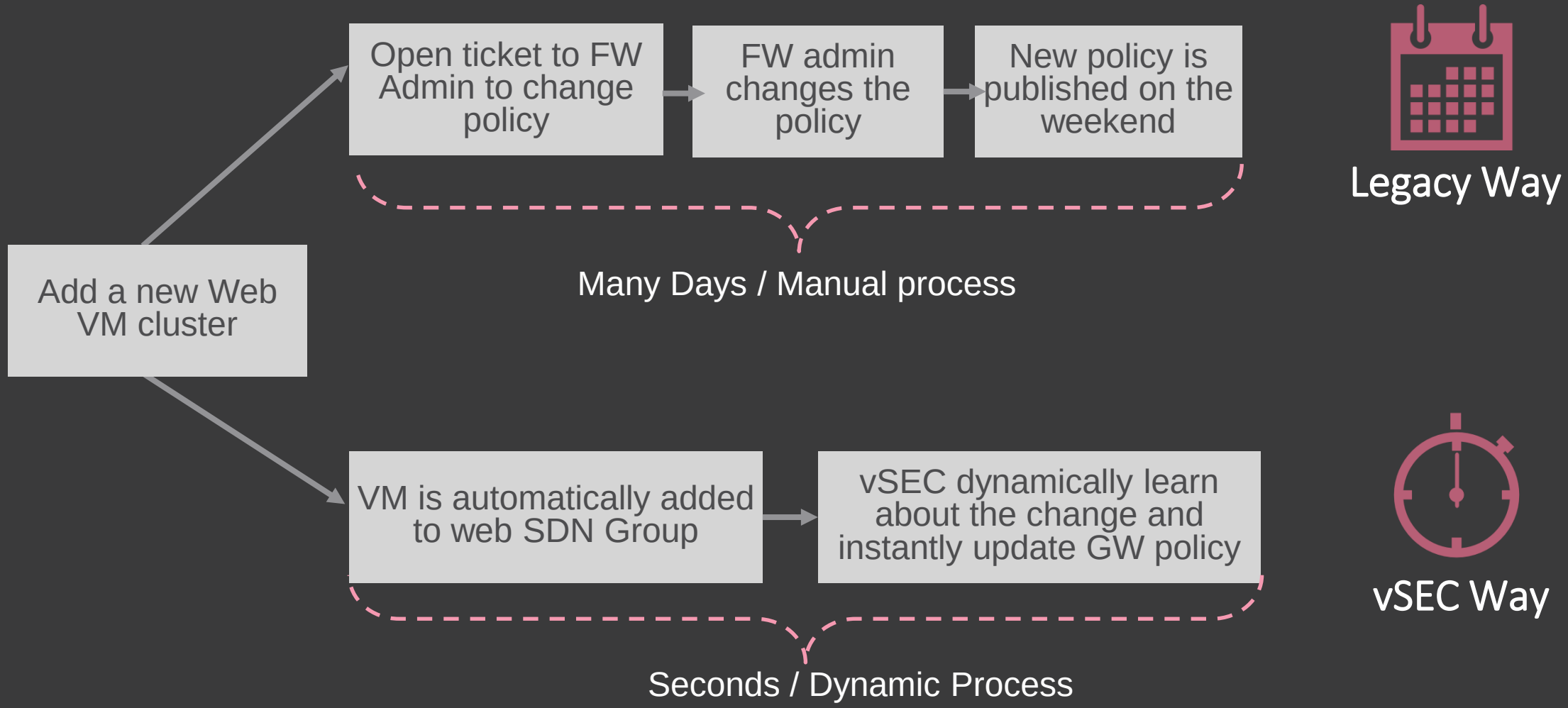
vSEC dynamically learns about this change from vCenter and all virtual and physical GWs are instantly updated

Seconds / Dynamic Process

vSEC Way

SCALE UP YOUR APPLICATION

Check Point
SOFTWARE TECHNOLOGIES LTD.



VIRTUAL PATCHING

Check Point
SOFTWARE TECHNOLOGIES LTD.

Legacy Way

It takes days to test, approve and deploy a new security patch

Meanwhile, vulnerability is known and applications are exposed

vSEC Way

Virtually patch your applications with vSEC IPS and advanced threat prevention before security patch is announced

PROVISION A NEW APPLICATION

Check Point
SOFTWARE TECHNOLOGIES LTD.

Develop a manual procedure for new Database → Manually configure the FW to secure the new Database

Many hours / Manual process

Legacy Way

Develop an orchestration recipe for new Database with security → Recipe is executed and provision the FW policy

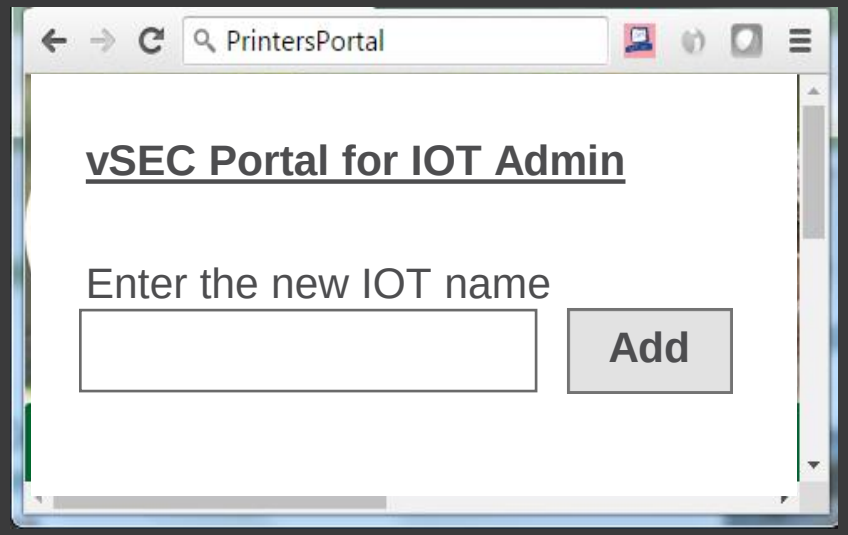
Seconds / Automation Process

vSEC Way

CONNECT A NEW IOT DEVICE

Check Point
SOFTWARE TECHNOLOGIES LTD.

Connect IOT
to the network



New rule is created
to IOT and all GWs are
instantly updated

vSEC Way

30 Secs Manual
(avoid open a ticket)

Seconds / Automation
Process

Check Point
SOFTWARE TECHNOLOGIES LTD.

5 REASONS WHY vSEC R80 IS

THE BEST

SECURITY AUTOMATION SOLUTION

1st REASON

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point vSEC & R80

Trusted Policy Delegation

Scope automation privileges only to relevant application's rules

Other Vendors

Giving the keys for the kingdom

If you allow automation to change one rule, you allow it change any rule

2nd REASON

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point vSEC & R80

Simultaneous updates

Many automations can run simultaneously

Other Vendors

Entire Policy Lockdown

Only one automation can run at a time

3rd REASON

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point vSEC & R80

Dynamic Changes

Gateways policy dynamically learns about network changes of VMs & Applications

Other Vendors

Static Changes

Admin must manually update policy anytime VM networking is changed

4th REASON (roadmap)

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point vSEC & R80

Auto security service chaining

vSEC automatically configures SDN controller to chain security based on policy

Other Vendors

Manual security service chaining

SDN Admin must manually configure the controller policy to chain security

5th REASON (roadmap)

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point vSEC & R80

Application role Auto-Discovery

Admin is educated on what policy to apply between VMs

Other Vendors

Security role manual discovery

Admin is oblivious on what security policy to apply between VMs

Check Point
SOFTWARE TECHNOLOGIES LTD.

THE JOURNEY TO HYBRID CLOUD STARTED

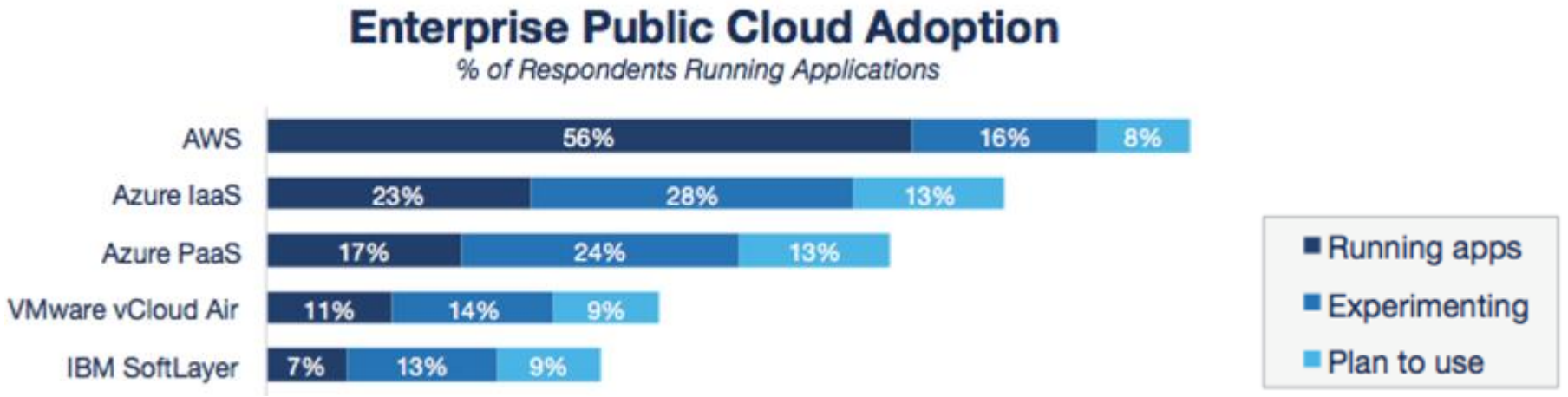
BE RELEVANT

STAY COMPETITIVE

HYBRID CLOUD & SDN TIPPING POINT (July 2016)

Check Point
SOFTWARE TECHNOLOGIES LTD.

AZURE	VMware NSX	Cisco ACI
120K New customers/month	100+ Customers spent over $1M on NSX	7200+ ACI-ready customers



THE EFFORT OF HYBRID CLOUD

Check Point
SOFTWARE TECHNOLOGIES LTD.

MOVING TO CLOUD IS A STRATEGIC MOVE

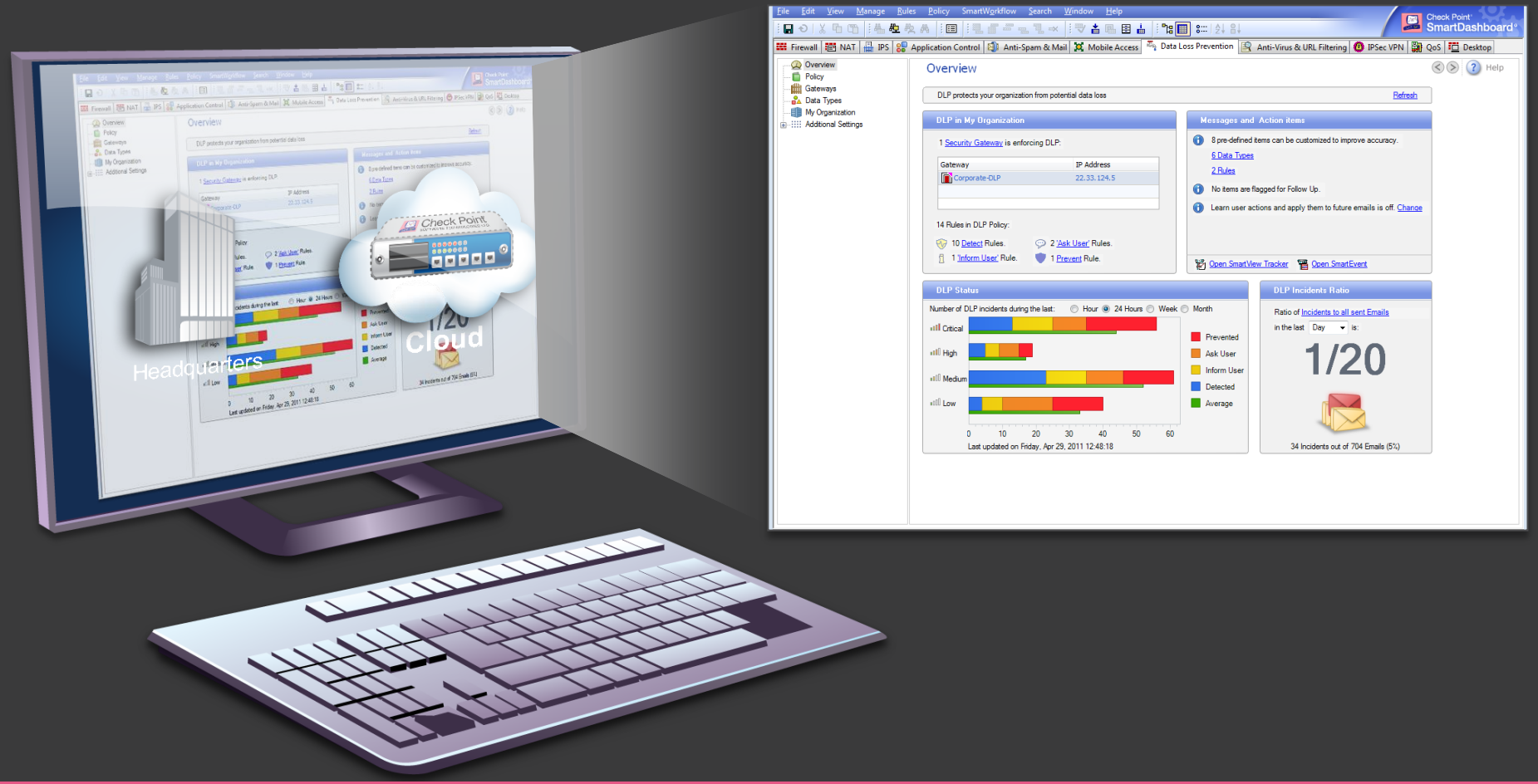
IT TAKES TIME AND EFFORT TO REALIZE THE FULL POTENTIAL

Phase #1: New Infrastructure	Phase #2: New Applications	Phase #3: New Operation
Compute (Hypervisor) SDN (Network)	Software Defined Applications	DevOps & Orchestration

SECURITY MUST PAVE THE WAY OF THIS JOURNEY

Unified Management with Single Console

Check Point
SOFTWARE TECHNOLOGIES LTD.



Manage Cloud and On-Premise Security from a Single Console

Check Point vSEC

Integrates with

Azure Security Center

MICROSOFT

Azure Security Center integrates with Check Point

Check Point
SOFTWARE TECHNOLOGIES LTD.

Security Center discovers deployments which benefit from vSEC deployments

Check Point's vSE gh Azure Security Center:

- **Simplified Deployment - just few clicks**
- **Integrates Check Point's logs in Security Center alerts dashboard**

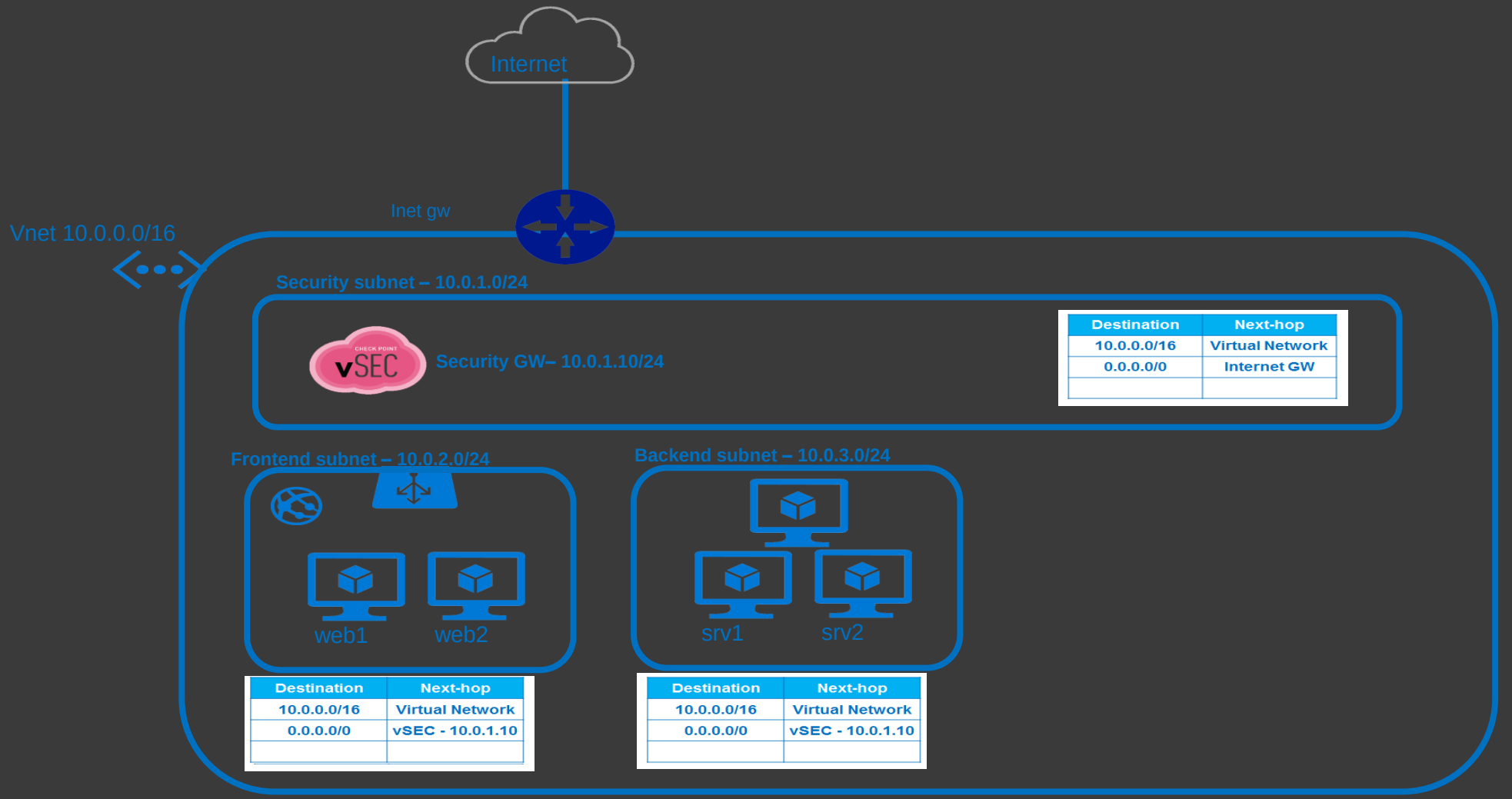
MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Check Point
SOFTWARE TECHNOLOGIES LTD.

USE CASE – Change your Mind !

... From limitation to advantage

North -South Service Insertion



Implementation CPX-Mgmt #1

- Setup of R80 Mgmt
- adding Log-Server Object with public IP
- activate SmartEvent Server
- create new gw Object, change Log-Srv
- create sample ruleset – 4 Rules (Stealth, Frontend/Backend and Cleanup)

[Restricted] ONLY for designated groups and individuals

Implementation CPX-Mgmt #2

- config of NAT (hide NAT + static for HTTP)
- verify logging and NAT

[Restricted] ONLY for designated groups and individuals

Implementation CPX-NET #1

- Setup R77.30 vSec gw in Azure
  - disable NSG
  - configure basic vnet and secure subnet
- run initial wizard in order to setup SIC
- config of new subnets
  - Frontend
  - Backend
- config of new UDR‘s
  - Frontend
  - Backend
  - Secure (linked to the vSec NIC)

[Restricted] ONLY for designated groups and individuals

Implementation CPX-NET #2

- verify access to gw
- activate IP forwarding for gw‘s nic in Azure
- install 2x centos vm‘s (for frontend + backend services)
  - without public IP
  - without NSG

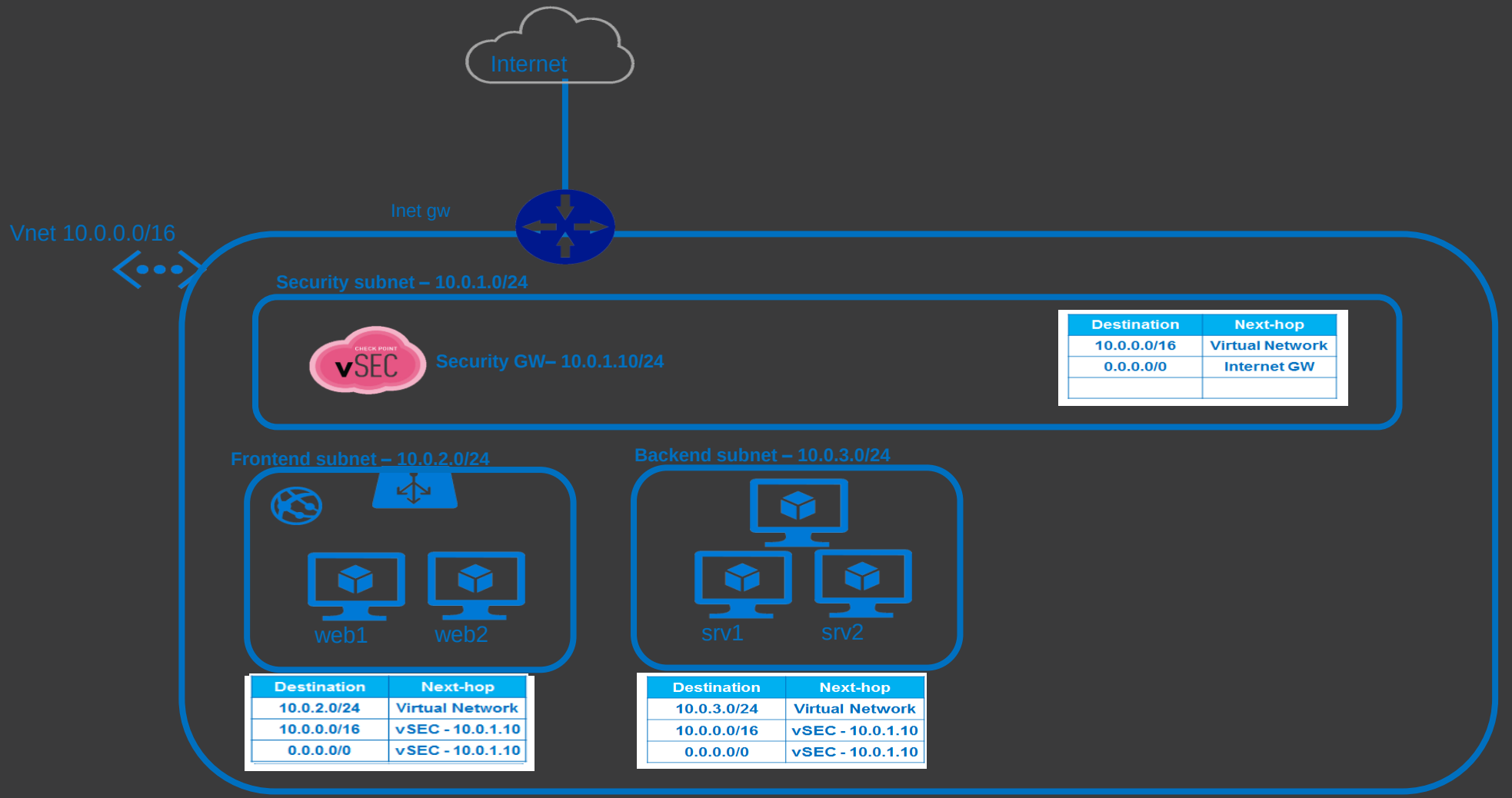
[Restricted] ONLY for designated groups and individuals

Implementation CPX-NET #3

- ssh login to gw – verify connectivity of centos vm‘s in frontend and backend subnet
- ping gateway (verify result)
- ping frontend to backend (verify result)
- ping internet (verify result)
- install httpd on frontend machine
- check access from outside to web server

[Restricted] ONLY for designated groups and individuals

East – West Service Insertion

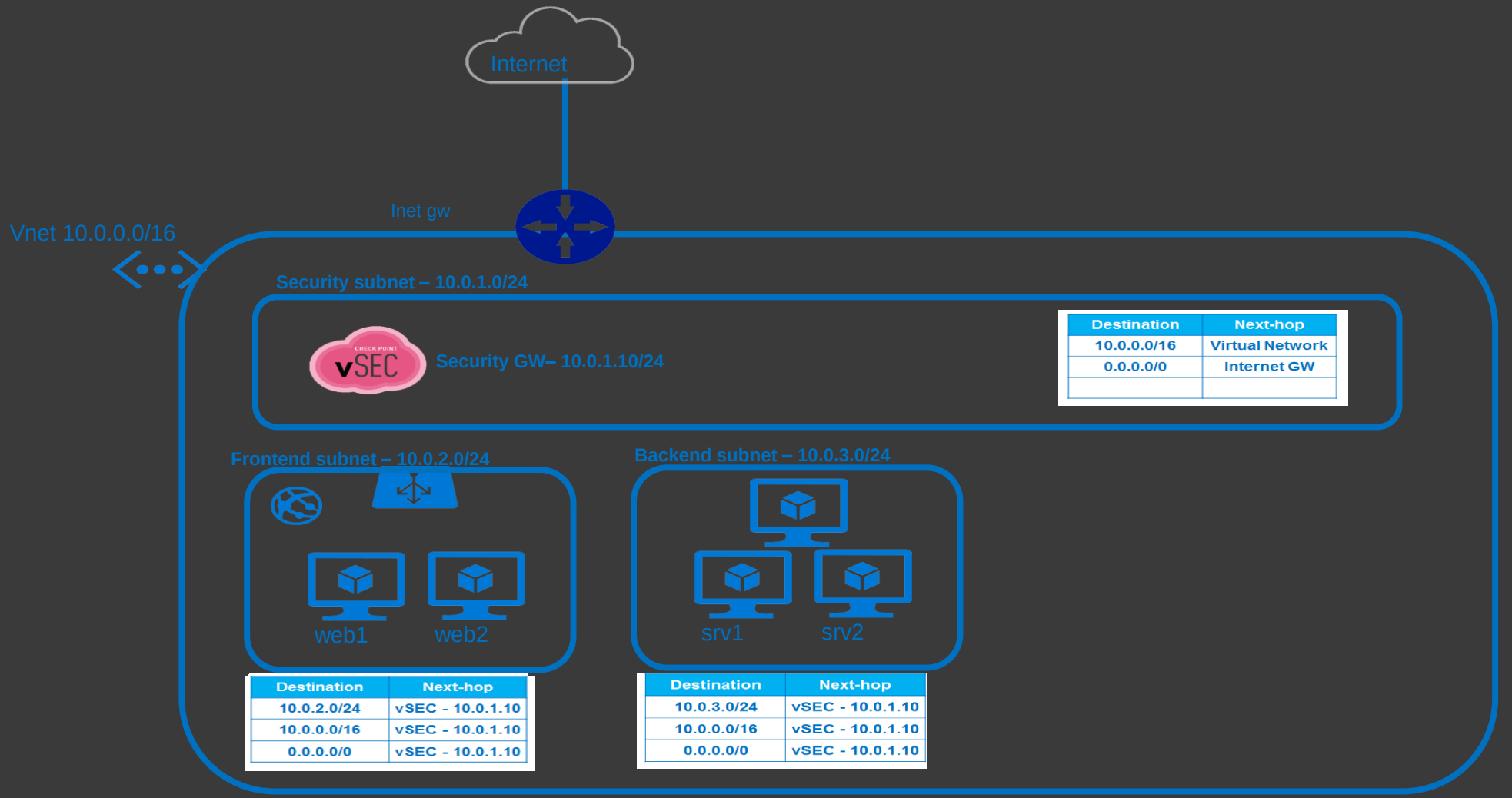


from NFV to East-West Security & 1SA

- change UDR‘s in order to route traffic via vSec Azure gw
- verify logging – check rules

[Restricted] ONLY for designated groups and individuals

VM-to-VM Service Insertion



Destination	Next-hop
10.0.0.0/16	Virtual Network
0.0.0.0/0	Internet GW

Destination	Next-hop
10.0.2.0/24	vSEC - 10.0.1.10
10.0.0.0/16	vSEC - 10.0.1.10
0.0.0.0/0	vSEC - 10.0.1.10

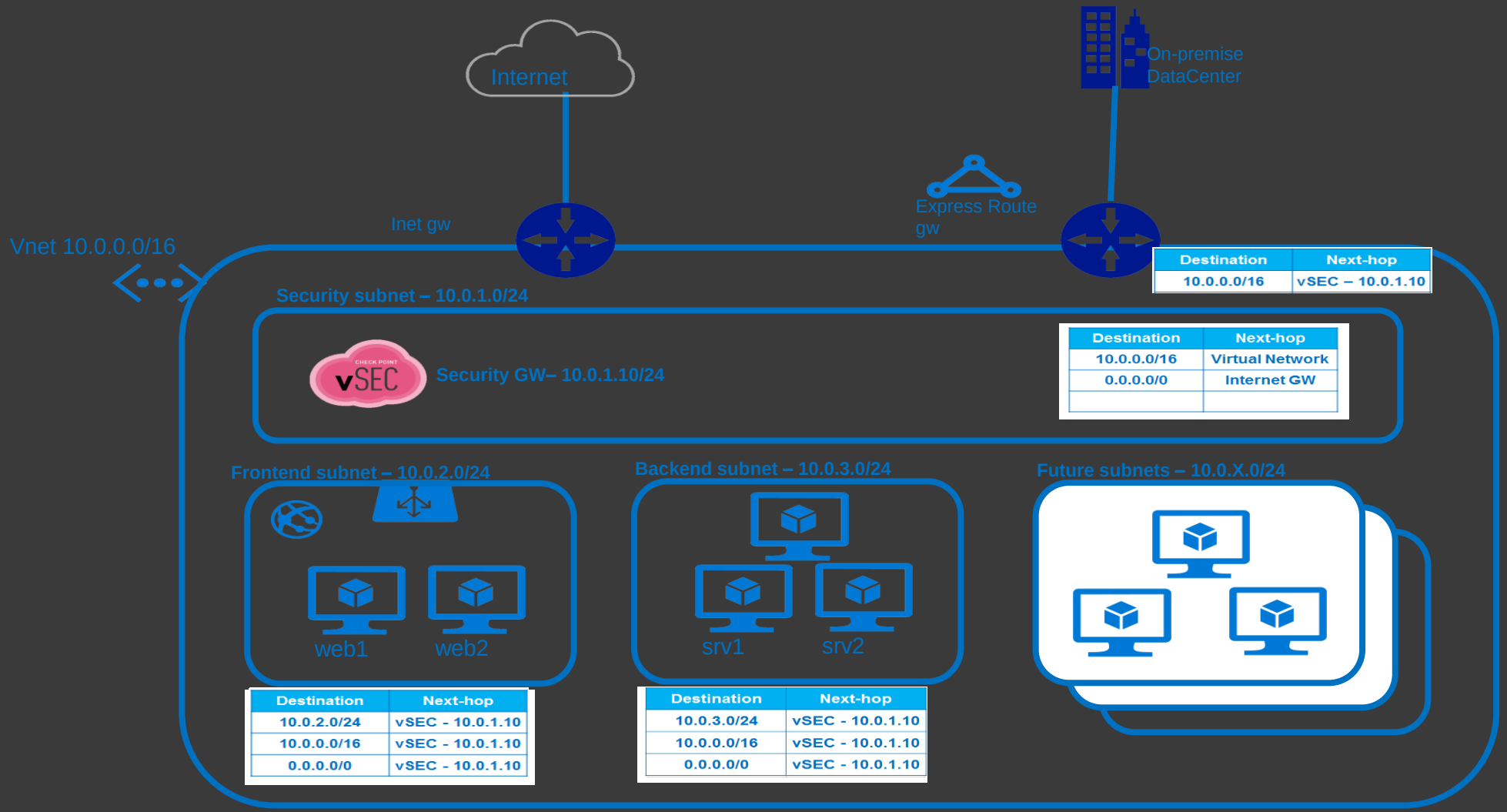
Destination	Next-hop
10.0.3.0/24	vSEC - 10.0.1.10
10.0.0.0/16	vSEC - 10.0.1.10
0.0.0.0/0	vSEC - 10.0.1.10

Activation of more security features

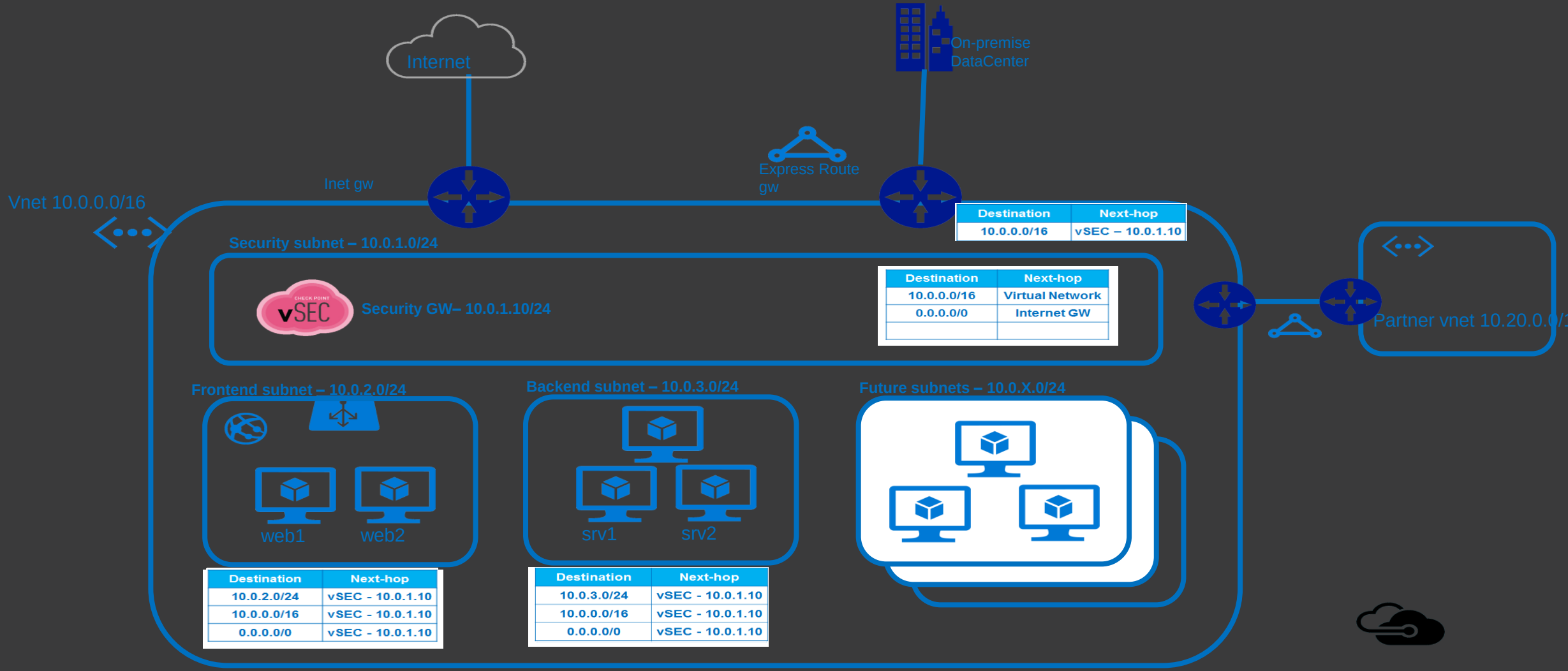
- activate more blades
- config of application control policy in order to log only and accept
- run demos (external access via http) – verify log entries and smart event

[Restricted] ONLY for designated groups and individuals

On-premise Connection



VNet-to-VNet Connection



Check Point
SOFTWARE TECHNOLOGIES LTD.

Deployment Methods

Deployment Methods

Check Point
SOFTWARE TECHNOLOGIES LTD.

Azure Portal – Build, manage, and monitor everything from simple web Apps to complex cloud applications in a single, unified console

Azure Resource Manager (ARM) - enables you to deploy, update or delete all of the resources for your solution in a single, coordinated operation. You use a template for deployment

Azure Powershell - powerful scripting environment that you can use to control and automate the deployment and management of your workloads in Azure.

Check Point
SOFTWARE TECHNOLOGIES LTD.

SUMMARY

MICROSOFT AZURE

- Highest level of Security Partner
- The only NGFW solution in Azure Security Center
- Automated solution to simplify deployments

[Restricted] ONLY for designated groups and individuals

Check Point®
SOFTWARE TECHNOLOGIES LTD.

vSEC SECURES THE FUTURE DATACENTER TODAY

vSEC SOLUTIONS & PRODUCTS

Check Point
SOFTWARE TECHNOLOGIES LTD.

vSEC for Private Cloud with SDN

vSEC for NSX

vSEC for ACI

vSEC for Virtual-Datacenter

vSEC Virtual Edition
(also known as VE)

vSEC for OpenStack

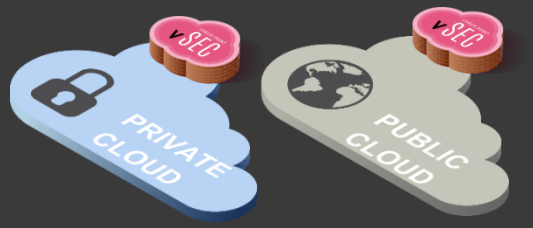
vSEC for Public IaaS

vSEC for AWS

vSEC for AZURE

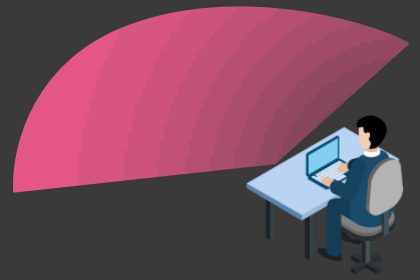
vSEC for vCloud Air

SUMMARY:



Advanced Security for Hybrid Cloud

Security Automation



Unified Security Control &Visibility

SECURITY THAT TAKES YOUR MODERN DATACENTER

ONE STEP AHEAD

[Restricted] ONLY for designated groups and individuals

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU

ONE STEP AHEAD

©2016 Check Point Software Technologies Ltd.

[Protected] Non-confidential content