



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

# Architecture References and Best Practices

## CloudGuard Private IaaS for VMware NSX-T 2.5

**WELCOME TO THE FUTURE OF CYBER SECURITY**

© 2020 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without the prior written authorization of Check Point. While every precaution has taken in the preparation of this Whitepaper, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

**RESTRICTED RIGHTS LEGEND:**

Use, duplication, or disclosure by the government is subject to restrictions as outlined in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

**TRADEMARKS:**

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks. Refer to the Third Party copyright notices [http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

## Abstract

This Whitepaper outlines the integration of VMware NSX-T with Check Point CloudGuard to provide Best practices, Use Cases, Architecture diagrams, and Zero-Trust approach to enable customers to build the best strategy to Secure Software-Defined Data Center according to with the business needs.

## Audience

The Architecture diagrams and different technical topics described in this document taken from VMware, Check Point Software Technologies, and different technical Blogs. All information presented in this paper in-order to educate, enable Security and Networking Engineers, Solution Architects and designers who would like to integrate VMware NSX-T and Check Point Software Technologies for advanced security. Readers should be versed in virtualization, network, and security design, as well as Zero-Trust. This document deals specifically.

# Table of Contents

<b>Table of Contents</b> .....	<b>4</b>
<b>Introduction to Software-Defined Data Center (SDDC)</b> .....	<b>5</b>
Legacy Approach .....	5
VMware NSX-T: A more holistic implementation for SDDC .....	6
Micro-Segmentation and Zero-Trust.....	7
<b>NSX overview</b> .....	<b>9</b>
NSX Components .....	9
VMware NSX Modes (NSX-V and NSX-T) .....	10
NSX-T Networking scenarios.....	12
Dynamic Context-Based Grouping .....	14
<b>Check Point integration with NSX using CloudGuard</b> .....	<b>15</b>
Key Business Benefits .....	15
Automation and Orchestration .....	15
Ubiquitous Security Enforcement .....	16
Policy Enforcement.....	17
Context-Aware Security Policies .....	17
Data Protection.....	17
Auto-Quarantine of Infected Hosts .....	17
Threat Prevention .....	17
Centralized Security Management.....	18
Check Point CloudGuard controller .....	18
Check Point CloudGuard Private IaaS gateway .....	20
When to use Service Insertion versus Service Chaining? .....	21
Integration Modes with NSX-T .....	22
CloudGuard Private IaaS with Service Insertion at the Edge (NSX-T 2.3) .....	22
CloudGuard Private IaaS with Service Chaining (NSX-T 2.4) .....	22
CloudGuard Private IaaS with Service Chaining and Edge Service Insertion (NSX-T 2.5).....	23
<b>Use cases and best practices scenarios</b> .....	<b>24</b>
Service chaining between Security Groups for East-West traffic .....	24
Edge Service insertion for East-West traffic between Security Groups .....	25
Edge Service insertion for East-West traffic between Virtual Machines.....	26
Service chaining between Security Groups and Virtual Desktops for East-West traffic.....	27
Edge Service insertion for North-Southth traffic between Virtual Desktops and External Networks.....	28
Service Chaining (E-W) + Edge Service Insertion (N-S) .....	30
<b>Conclusion</b> .....	<b>31</b>



# Introduction to Software-Defined Data Center (SDDC)

We often hear about Software-Defined Data Center; however, it is not easy to understand and deploy it. Software-Defined Data Centers allows the organizations to accomplish four Business Drivers: Agility, Speed, Automation, and Policy-Driven approach considering the premise of the Business Process modeling.

First, let us analyze the Traditional approach for Data Centers, where perimeter security solutions are not suitable to address the dynamic demands the modern needs. Some of the security challenges that must overcome include:

- The shift in traffic behavior within the data-center - Historically, the majority of traffic loads were between entities that were external to the data-center (“North-South” traffic), driven by the extensive use of siloed client-server applications and secured by the perimeter gateway.
- Data Center traffic today has now shifted. Workloads are more heavily “East-West” – intra-data-center traffic – because of virtualization, shared services, and updated distributed applications.
- Within virtual environments, these complex communications get little to none of the advanced controls or protections from traditional security solutions that safeguard “North-South” traffic since it never passes through the network perimeter or gateway. Perimeter firewalls typically have limited visibility into this “east-west” traffic, leaving it and the data-center vulnerable to malware and other malicious payloads.
- Traditional security approaches are manual, operationally complex, and slow to implement and not designed to keep pace with dynamic virtual network changes that come with rapid application provisioning. Moreover, sole reliance on perimeter security leads to resource-intensive choke points on the network. It has a tremendous impact on data-center performance and increases security complexity, thus placing additional burdens on security teams.
- The extensive use of VLANs in data-centers increases the threat to all applications. Due to the lack of inter-system (and VM) advanced security, a breach of a single (virtual) host network can allow malware to spread laterally and propagate across the network, compromising all applications, including those residing on different VLAN’s. Successful attacks on even low priority services can expose the most critical or sensitive systems because intra-VM / East-West security protections do not exist.

In the Digital Transformation process, the organizations need to migrate into agile data-center architectures to reduce IT costs to improve and increases the business response for market needs. Business applications should be benefited from the provisioning on-demand using self-service user interfaces, operational, and provisioning automation.

Two important definitions that are key for SDDC:



- **Automation:** Any Task can be executed without human intervention or interaction (e.g., Scripts or Asset scanners to collect or abstract the components deployed in the Datacenter)
- **Orchestration:** Different tasks that can be automated or manual in a synchronized way (workflow) to provide Service or deliver a product (e.g. playbooks that can integrate several elements in an integrated way to provisioning Network, Computing, Storage and Security).

Increasingly virtualized data-centers and dynamic cloud environments have led to a dramatic increase in network traffic going East-West (laterally within the data-center). When it comes to security, the focus has mainly been on protecting the perimeter (north-south traffic, going into and out of the data-center). There are few controls to secure east-west traffic inside the data-center. Traditional security approaches to those challenges are manual, operationally complex and slow, and are unable to keep pace with dynamic virtual network changes and rapid application provisioning.

## Legacy Approach

In the traditional Datacenter, the organizations focused on providing security for the North-South traffic, just only deploying Firewalls at the “Edge,” providing segmentation at network level separating the Users Network and the Datacenter. This approach derivate in a big problem, it was not scalable, and it is a problem when customers need to deploy new security solutions.

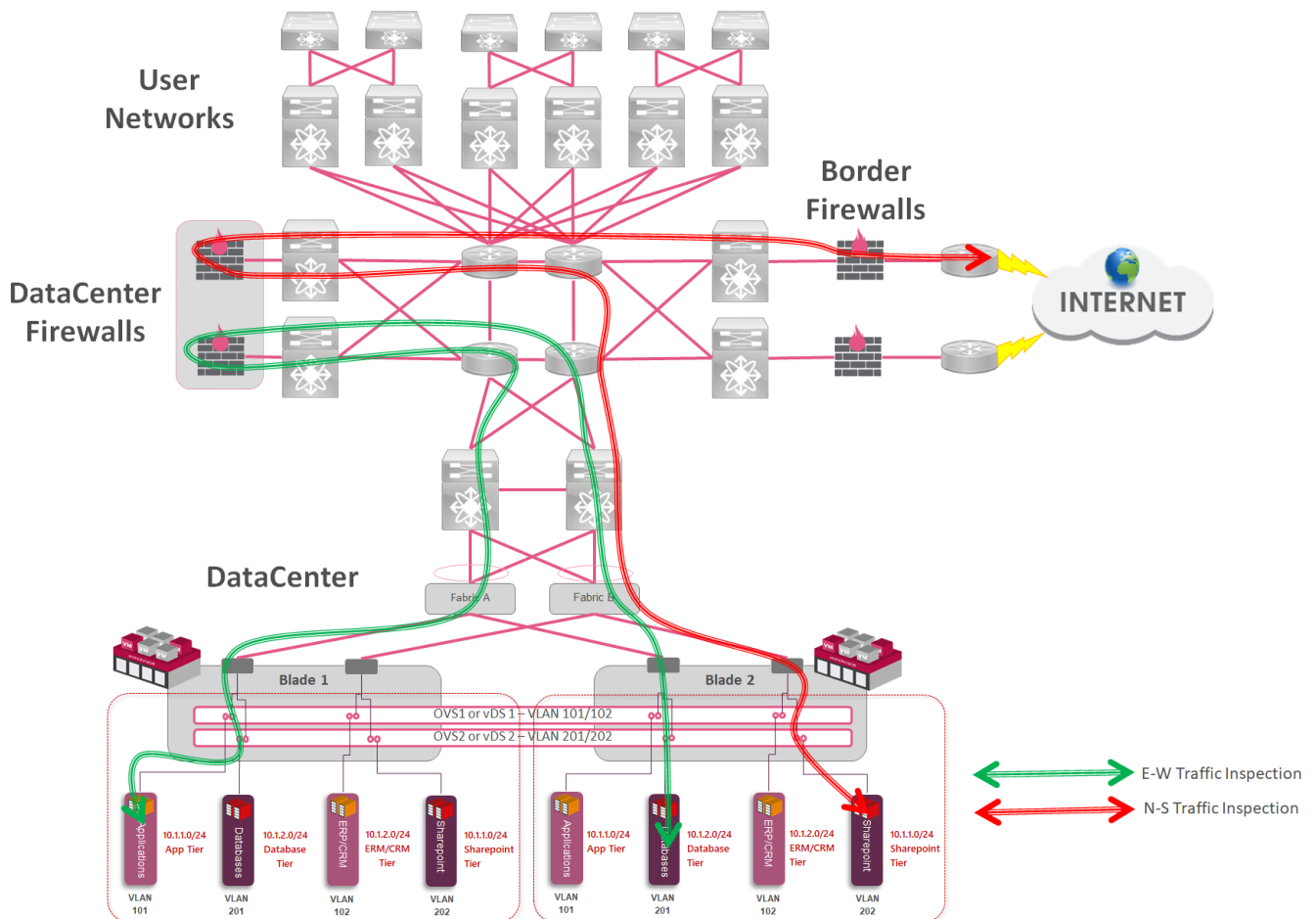
WELCOME TO THE FUTURE OF CYBER SECURITY

**What if an attacker does successfully infiltrates inside the Traditional DataCenter?**



In the traditional network security mindset, the Security segmentation is more focused on the VLAN configuration only, however, when an attacker successfully infiltrates, it will have the capability to access all assets in the Datacenter. This scenario allows the propagation of malicious code or advanced persistence in all “trusted” networks with all the elements connected in the LAN or Virtual LAN. This scenario is more complex to provide quarantine or remediation activities leading to several business concerns to stop the business. This is the definition of Lateral Attacks when an element in the network has been compromised.

Additionally, in the Virtual Environment, the traffic generated from the first VM needs to go out of the Host to receive the Routing or Firewall policy and then back into the Host and to the other Virtual Machine.



**Figure 1: Traditional Segmentation for Datacenter**

Additionally, these types of Data-centers cannot escalate appropriately and can not provide agility and application-centric security. The original objective w to deploy firewalls as close to the core of the network as possible (or as close to the WAN/Internet), allowing leave data-center internal traffic unprotected and unsegmented, as a consequence significant risk for the Business. However, today in the Digital Transformation, the organizations will focus more on the East-West traffic, especially from Application Servers to Databases, due to it will be more than 80% of the traffic expected.

**VMware NSX-T: A more holistic implementation for SDDC**

According to VMware<sup>1</sup>, the NSX-T™ Data Center is focused on providing agile software-defined infrastructure capabilities to build cloud-native application environments, providing networking, security, automation with operational simplicity. NSX-T Data Center supports cloud-native applications, bare-metal workloads, multi-hypervisor environments, public clouds, and multiple clouds. NSX-T Data Center designed for management, operation, and consumption by development organizations, allowing IT and development teams to select the technologies best suited for their applications.

<sup>1</sup> Source: <https://docs.vmware.com/en/VMware-NSX-T-Data-Center/index.html>

WELCOME TO THE FUTURE OF CYBER SECURITY

## Micro-Segmentation and Zero-Trust

Micro-segmentation<sup>2</sup> is the ability and capability to insert security services into the access layer between two virtualized workloads in the same broadcast domain or x86 host.

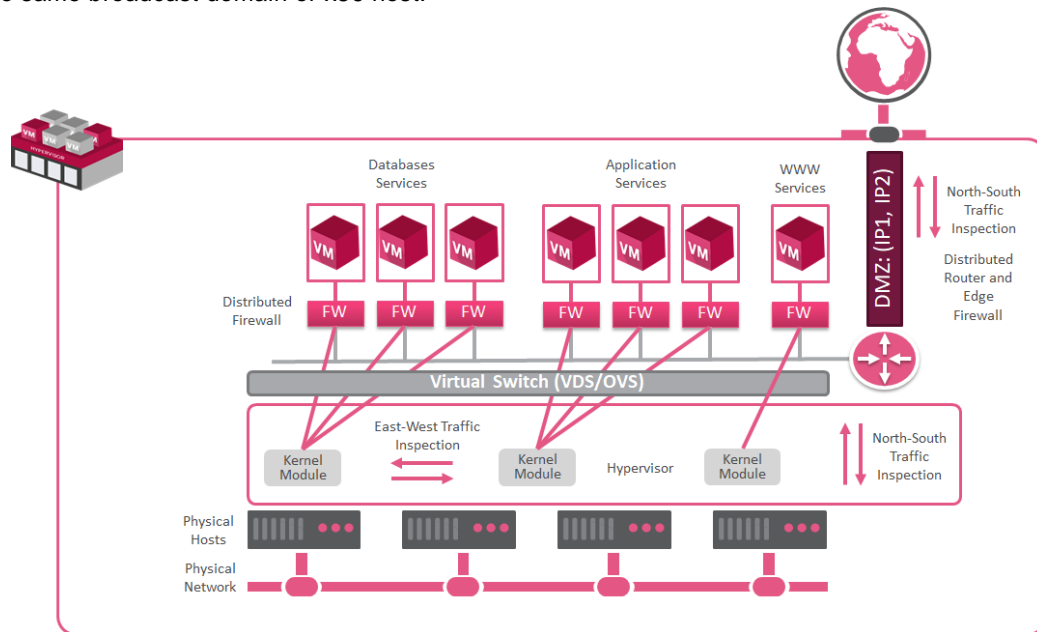


Figure 2: Hypervisor-Based Micro-segmentation, Source: Gartner Security & Risk Management Summit 2019

Micro-segmentation helps organizations to implement what often referred to as the “zero-trust” model of security where all network endpoints viewed as dangerous. Before to provide a more in-depth explanation, it is essential to have the following definitions:



- **Business Drivers:** Business drivers are the **key inputs and activities** that drive the operational and financial results of a business. Common examples of business drivers are salespeople, number of stores, website traffic, number and price of products sold, units of production, etc.
- **Business Process:** A business process is a collection **of linked tasks**, which find their end in the delivery of a service or product to a client. A business process has also defined as a set of activities and tasks that, once completed, will accomplish an organizational goal.

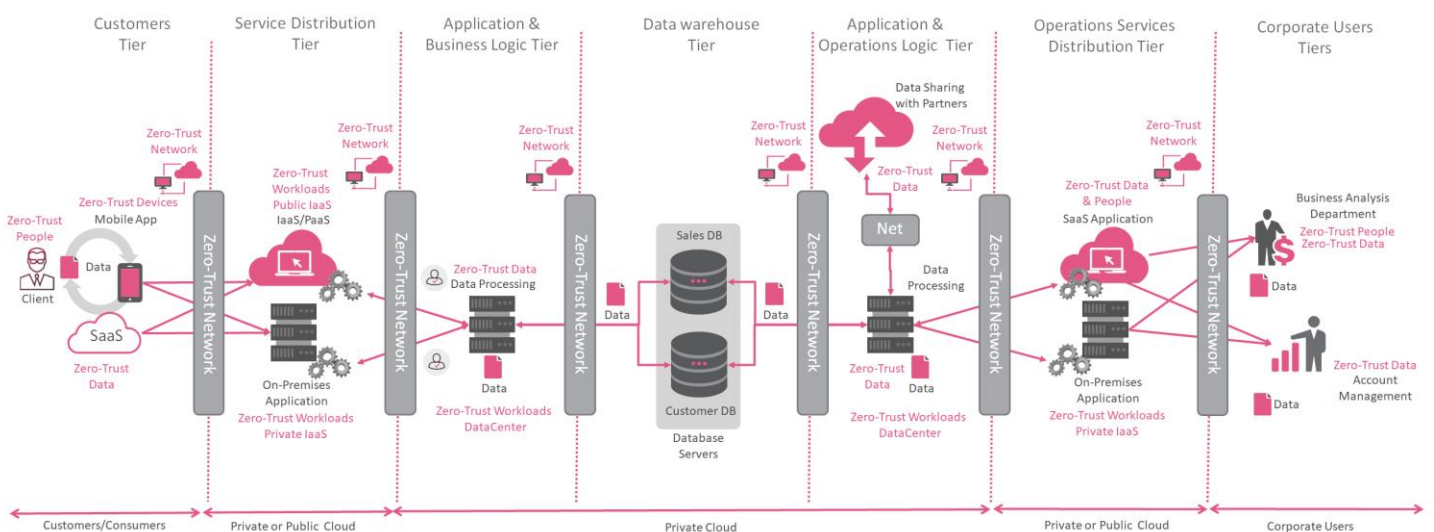


Figure 3: Security Segmentation for Business Process aligned with Zero-Trust framework

<sup>2</sup> Source: Micro-segmentation Today — Deployment and Use Cases (Gartner Security & Risk Management Summit)

WELCOME TO THE FUTURE OF CYBER SECURITY

- **ZERO TRUST DATA:** Keep Data Safe, Anywhere, with a Comprehensive Multi-layered Protection as one of the pillars of a Zero Trust strategy, securing and managing the data, categorizing and developing data classification schemas, and encrypting data both at rest and in transit.
- **ZERO TRUST WORKLOAD:** Workload refers to the entire application stack from the application layer through the hypervisor or self-contained components of processing such as containers and virtual machines. Typically, the workloads are located in the Frontend, Middleware, and Backend segments/layers wherein conjunction runs the business process to provide a service or product. The connections, applications, and components must be treated as a threat vector and must have Zero Trust controls and the right technologies applied to them.
- **ZERO TRUST NETWORKS:** Reduce the Risk of Lateral Movement with Micro-perimeters and Identity-based Policies providing the ability to segment, isolate, and control the network being a pivotal point of control for Zero Trust.
- **ZERO TRUST DEVICES:** Secure, Control, and Isolate Every Device on your Network. Network-enabled device technologies have introduced a massive area of potential compromise for networks and enterprises, and security teams must be able to isolate, secure, and control every device on the network at all times.
- **ZERO TRUST PEOPLE:** Use different layers of authentication to deny Identity to hackers from stealing digital assets as the last line of any Zero Trust strategy. The main focus is to limit and strictly enforce the access of users and securing those users as they interact with the internet. This encompasses all the technologies necessary for authenticating users and continuously monitoring and governing their access and privileges. It also encompasses the technologies for securing and protecting users' interactions like traditional web gateway solutions.
- **VISIBILITY & ANALYTICS:** Enable full threat visibility with a single view of security risks using advanced analytics platforms. As an example, the user and entities behavior analytics (UEBA) provides a comprehensive overview of how the users are interacting with the business process and potential impacts derivated of non-common behavior. This focus area of the extended Zero Trust ecosystem helps with the ability of a tool, platform, or system to empower the security analyst accurately to observe threats that are present and orient defenses more intelligently.
- **AUTOMATION & ORCHESTRATION:** Allows Tasks and processes to use Flexible APIs and Rich 3rd Party Integrations, providing the ability and speed to have positive command and control of the many components of the Business Process and used as part of the Zero Trust strategy as a vital tool for Operations.

Security Segmentation provides a hierarchical model that can be used to design the Zero-Trust network, where elements can be grouped hierarchically by function and data sensitivity. This approach allows providing appropriate protections at the segment boundaries and selects the appropriate protection types that differentiate between access controls, data protection, and threat prevention controls. Designing Software-Defined Data Center with Micro-Segmentation as the basis in the design approach, it will assist the organizations in solving several security problems when deploying L4-7 policies directly at the Hypervisor Level (Service Chaining) or Switch Fabric through Service-Insertion. It is essential to say, to have correctly mapped all the **Business Process with the application flows**, this approach will help and will provide a more easy approach to implement technologies like NSX-T.

The Security Policies (Access Control or Threat Prevention) now deployed in the Control Plane protecting all flows for the Data Plane. Considering the Micro-segmentation approach, now Virtual-to-Virtual, Virtual-to-Physical, or Physical-to-Physical should have the capability to communicate using more optimal paths. Micro-segmentation with VMware NSX allows building network security policy that is simply not possible with traditional network security and provide more flexibility. These constructs include building security blocks for Production, Distribution, and Operation Services.

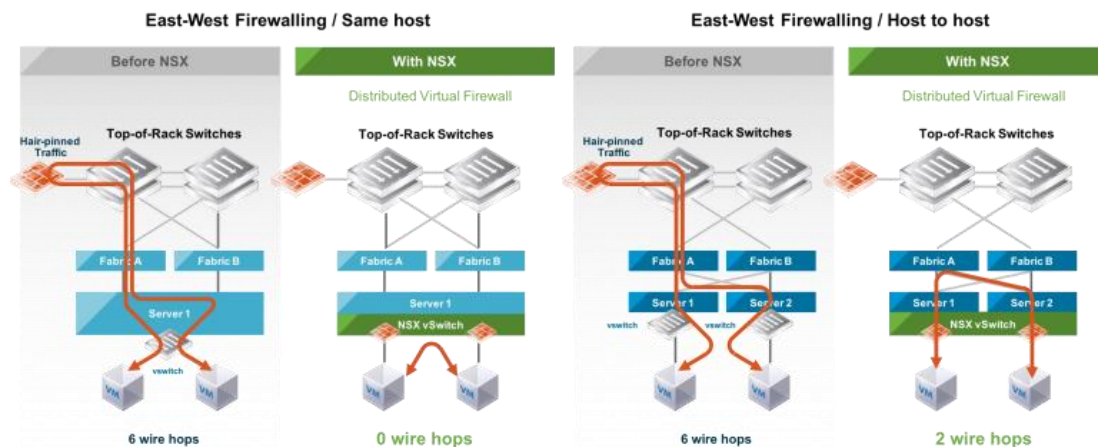


Figure 4: Micro-segmentation strategies for NSX (Source: VMware Inc.)



WELCOME TO THE FUTURE OF CYBER SECURITY

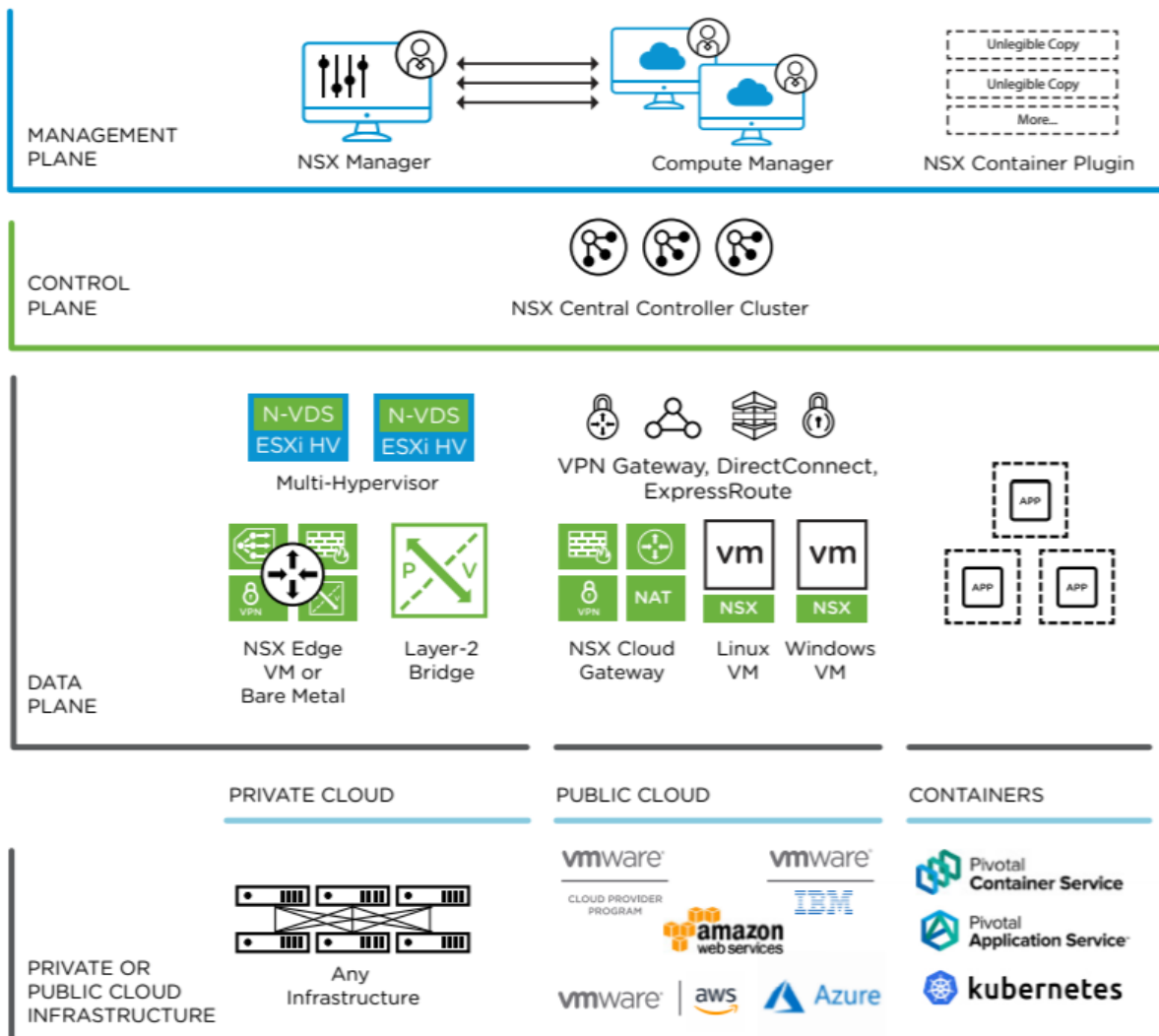
**What if an attacker does successfully infiltrates inside the Virtual DataCenter?**



In Software-Defined Data Center with properly deployed business-driven micro-segmentation, we can implement the Zero-Trust approach (Don't Trust verify). A compromised Virtual Machine now is not trusted and allowed to communicate with the specific network endpoints that you define for remediation or block everything when an attacker successfully infiltrates the attack surface is considerably reduced due to the segmentation approach.

## NSX overview

VMware NSX provides the foundation for securing east-west traffic by delivering micro-segmentation through a broad set of virtualized networking elements, including logical switches, routers, and firewalls. These services are provisioned programmatically within the SDDC when virtual machines are deployed and move with virtual machines as they move.



**Figure 5: Holistic approach for NSX-T (Source: VMware Inc.)**

NSX-T Data Center 2.4 introduces a broad array of native security functionalities such as Layer 7 Application Identity, FQDN Whitelisting, and Identity Firewall, all of which allow more granular micro-segmentation. In addition to the native security controls delivered by the Distributed and Gateway Firewall, the NSX Service Insertion Framework allows various types of Partner Services (e.g., IDS/IPS, NGFW, and Network Monitoring solutions) to be inserted transparently into the data path and consumed from within NSX without making changes to the topology.

## NSX Components

Different components integrate NSX infrastructure; these are:

- **NSX Manager** – The NSX Manager provides access to the management plane of the NSX solution and provides access to the APIs that can interact with from a programmatic standpoint. The NSX Manager can be deployed as a virtual appliance in both the NSX-V and NSX-T platforms.
  - NSX-T 2.4, Introduced the combined appliance that contains both the NSX Manager and NSX Controller

WELCOME TO THE FUTURE OF CYBER SECURITY

- **NSX Controller** – The NSX Controller is an NSX infrastructure component that creates the overlay networks using the network encapsulation protocol to carry virtual network traffic across the various segments of the physical network.
  - NSX-T 2.4, the controller is combined with the NSX Manager
- **NSX Edge** – The NSX Edge provides the routing and gateway services for the NSX infrastructure as well as DHCP, NAT, HA, and load balancers

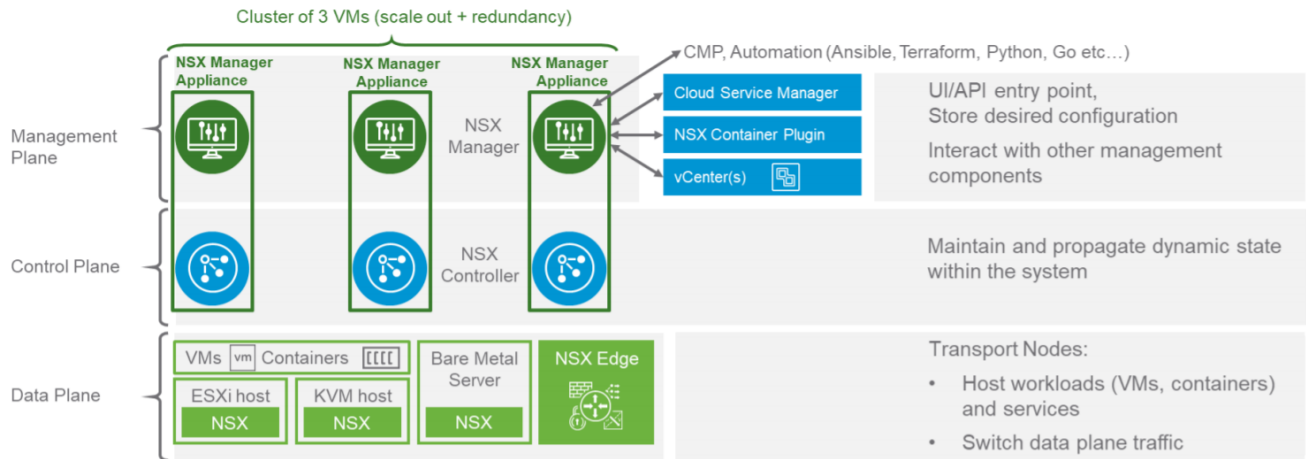


Figure 6: NSX Three-layer components (Source: VMware Inc.)

## VMware NSX Modes (NSX-V and NSX-T)

NSX-V is built around the VMware vSphere ecosystem, where you need a vCenter Server and ESXi hosts only. However, NSX-T is the next-generation software-defined networking solution providing an evolution to be more holistic and integrating other Hypervisors providing more flexibility. For the organizations, this substantial difference between NSX-V versus NSX-T allows to deploy Hybrid clouds working on their Digital transformation demands the deployment of Containers technologies where it is not mandatory to vCenter Server to deploy NSX-T. This new approach allows organizations to have true hybrid infrastructures providing support for different hypervisors and environments. The Cloud Transformation for organizations demands supports cloud-native applications, bare-metal workloads, multi-hypervisor environments, public clouds, and multi-cloud environments. Now, NSX-T supports ESXi, KVM, Kubernetes, OpenShift, Bare-metal servers, AWS, and Azure.

	NSX-V	NSX-T
Tight integration with vSphere	Yes	No
Working without vCenter	No	Yes
Support for multiple vCenter instances by NSX Manager	No	Yes
Provides virtual networking for the following virtualization platforms	VMware vSphere	VMware vSphere, KVM, Docker, Kubernetes, OpenStack, Azure, AWS
NSX Edge deployment	Virtual Machine	Virtual Machine or Appliance
Overlay encapsulation protocols	VXLAN	GENEVE <sup>3</sup>
Virtual switches (N-VDS) used	vSphere Distributed Switch (VDS)	Open vSwitch (OVS) or VDS
Logical switch replication modes	Unicast, Multicast, Hybrid	Unicast (Two-tier or Head)
ARP suppression	Yes	Yes
A two-tier distributed routing	No	Yes
Configuring the IP addressing scheme for network segments	Manual	Automatic (between Tier 0 and Tier 1)
Integration for traffic inspection	Yes	No
Kernel-level distributed firewall	Yes	Yes

Table 1: Differences between NSX-T versus NSX-V (Source: VMware Inc.)

<sup>3</sup> GENEVE: <https://docs.vmware.com/en/VMware-Validated-Design/4.3/com.vmware.vvd.sddc-nsxt-design.doc/GUID-CF3C47CA-9BEB-4213-8F08-1494261BF3EC.html>

WELCOME TO THE FUTURE OF CYBER SECURITY

Let us explain several and fundamental concepts related to NSX-T to understand how it works for successful deployment.



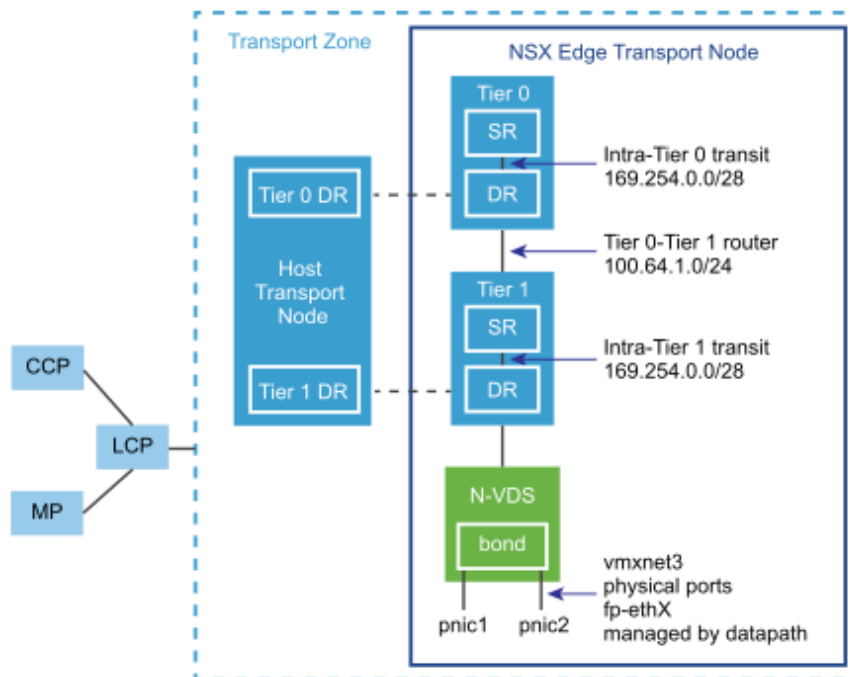
**North-South traffic is the traffic entering or leaving** the NSX-T environment or Domain. Virtual machines can be connected with external networks, like Corporate Network or Users Network.

- **East-West traffic is the traffic inside** the NSX-T environment or domain, the Virtual Machines connected in the same logical or different logical switches (vDS/N-vDS) can be connected to transfer traffic.

Transport zones and transport nodes are essential concepts in NSX-T due to they are crucial elements for successful deployment; let us start with the definitions:



- **The transport zone** provides the capability to reach transport nodes; for example, organizations with several ESXi hosts that are configured as transport nodes can allow the virtual machines on these different hosts to communicate with each other using an overlay network.
- **The transport node** provides the capability to participate in an overlay network, any node with Hosts Switch can serve as a transport node; additionally, it is Hypervisor holistic, for example, ESXi or KVM, or an NSX Edge node that participates in an overlay network.
- **The NSX-T Edge Nodes** can provide the bridge between the virtual network and the physical network, this node needs to be part of same transport zone and multiple VLAN transport zones where the Virtual Machines are connected providing access to access to the external networks,



**Figure 7: Transport Nodes, Transport Zones and Edge Transport Node**  
(Source: VMware Inc.)

Routing is another essential element in the NSX-T environments, to deploy the North-South and East-West traffic processing and inspection correctly; we have two crucial elements in the routing traffic: the DR (Distributed Router) & SR (Services Router).



- **The Distributed Routers** are responsible for providing one-hop distributed routing between logical switches and/or logical routers connected to this logical router (for example, the Tier-0 and Tier-1 for multitenant environments), it is essential to say that the Distributed routers are integrated into the Hypervisor at Kernel level.
- **The Service Routers** provides a centralized function and belongs only to the Edge nodes.

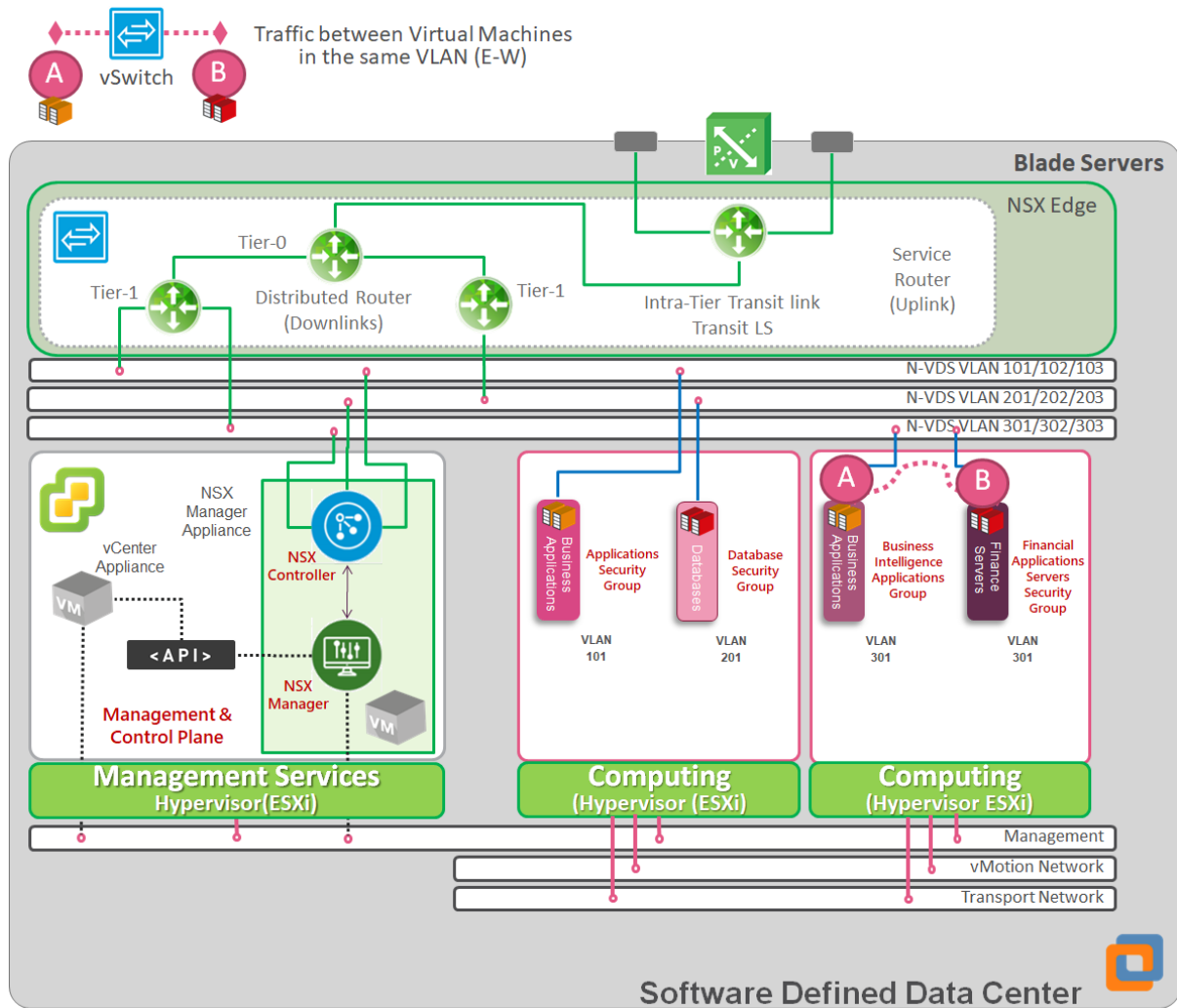
WELCOME TO THE FUTURE OF CYBER SECURITY

How are the Logical Routers connected? We have three different types of interfaces:



- **Downlink interface** that can connect with the Logical switch.
- **Uplink Interface** that can connect with the physical infrastructure or physical router, this is common for North-South traffic.
- **Intra-Tier Transit Link interface** is the internal link between the Distributed Router and Service Router to allow the communications of East-West with North-South.

## NSX-T Networking scenarios



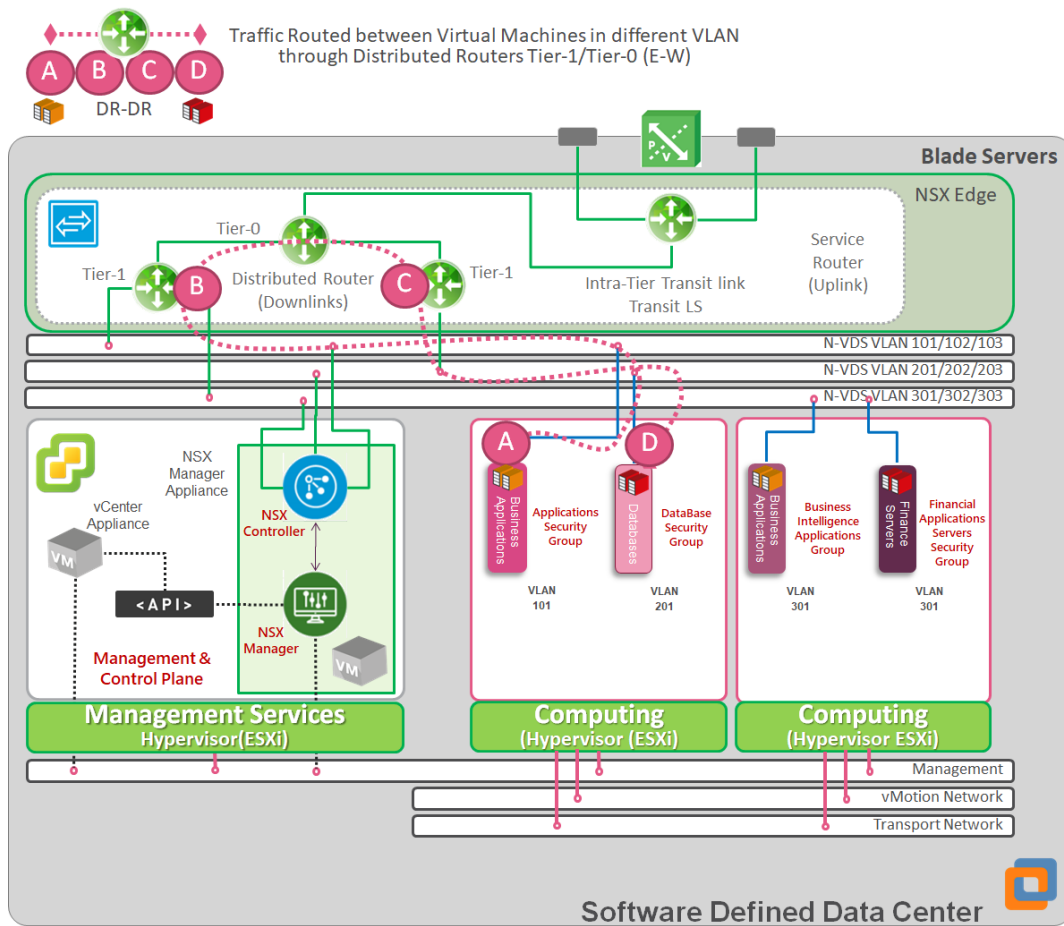
**Figure 8: Traffic communications between the same VLAN, no routing required.**

This scenario is the most simple and common in all organizations. Virtual Machines and Security Groups shares the same network segment (Virtual Switches or VDS) with all the communications without any segmentation or protection; however, this approach is tough to segment the traffic due to the resources are entirely mixed.

Let us talk about traffic Flow:

**From A to B:** The Application Server (AP-1) with IP address X.X.X.1 sends a packet to Database Server (DB-1) with IP Address X.X.X.2, no routing required here; this is the most simple scenario to transport traffic between the Virtual Machines; however, for the organizations with a huge Flat network, it could be very complex do security segmentation. For this scenario, this is the best option to enable Service Chaining.



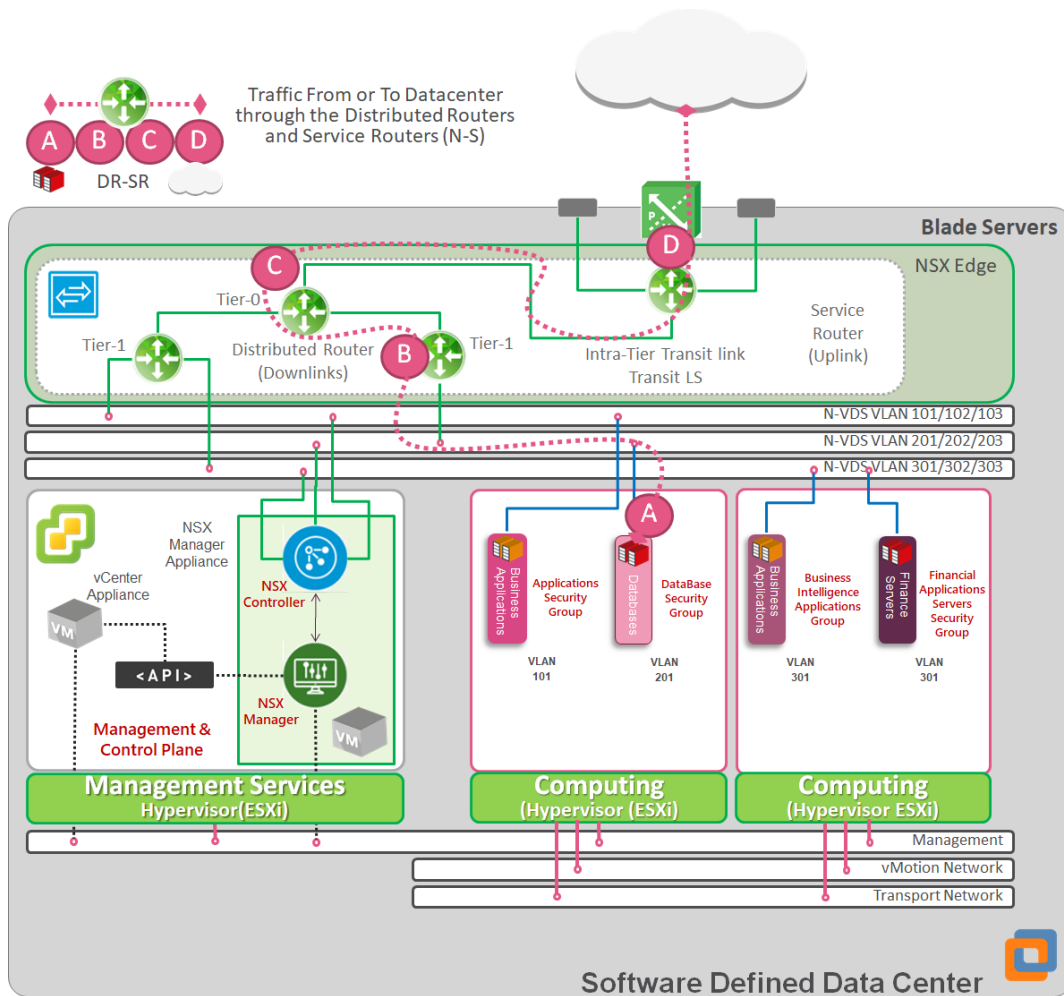


**Figure 9: Traffic communications between different VLANs using Distributed Routers (Tier-1 & Tier-0)**

This scenario is another typical routing implementation in the organizations and the business justification to deploy NSX, the idea here is to provide the segmentation approach at network basis, deploying VLANs to provide East-West routing that wholly distributed in the Hypervisor. However, it is essential to explain that each ESXi hypervisor in the transport zone must have running a Distributed Router in its Kernel.

Let us talk about traffic Flow:

- **From A to B:** The Application Server (AP-1) with IP address X.X.X.1 sends a packet to Database Server (DB-1) with IP Address Y.Y.Y.1. The packet is sent to the default gateway interface X.X.X.254 for "AP-1" located on the local DR.
- **From B to C:** The Distributed Router installed on the Hypervisor where the Virtual Machine in the Source Security Group requests a connection performing a routing lookup to determine the destination subnet Y.Y.Y.0/22 that is directly connected subnet on Virtual Switch 2 with VLAN 202. This lookup performed in the Virtual Switch 2 ARP table to determine the MAC address associated with the IP address for "DB-1". If the ARP entry does not exist, the NSX-T controller queries to get the ARP; otherwise, if there is no response from the NSX-T controller, an ARP request is flooded to learn the MAC address of DB-1.
- **From C to D:** Once the MAC address of DB-1 is learned, a layer 2 lookup is performed in the local MAC table to determine how to reach "DB-1", and the packet is sent.
- **From D to A:** The return traffic from DB-1 follows the same process, and routing would happen again on the local Distributed Router. All traffic flows processed at Kernel Level follow this approach providing lower latency for the applications.



**Figure 10: Traffic communications using Distributed Routers (Tier-1 & Tier-0) and Service Routers**

This scenario is focused on providing access to external network elements, for example, to provide Internet access to the Virtual Machines to Download Patches using the Services router (SR) – also referred to as a services component. The Service Router can have the following interfaces:

- **Linked Segments (From A to B):** It considered all the interfaces connecting to an overlay segment; in the diagrams, you see it as a downlink interface.
- **Distributed Routers in the Hypervisors (From B to C):** All Routing traffic between Tier Routers (T1/T0)
- **Intra-Tier Transit Link (From C to D):** Internal link between the DR and SR to provide routing capabilities between the Tier Routers (DR's) to the Service Router.
- **Service Interface (At D):** Interface connecting to VLAN segments to provide connectivity to VLAN backed physical or virtual workloads.
- **External Interface (From D to External network):** Interface connecting to the physical infrastructure/router, this element can integrate static routing and dynamic routing (like BGP); in the diagrams, you see it as the uplink interface.

## Dynamic Context-Based Grouping

Additionally, VMware NSX has rich contextual knowledge of the workloads it's protecting. Instead of using grouping and rules based on where an object or host is on the network, NSX customers can construct a policy-based on specific characteristics of the workload, for example, the workload's Operating System or name or type of service provided. By applying Security Tags, workloads can be grouped based on criteria such as the function of the application, the application tier the workload is part of, the security posture, regulatory requirements, or the environment the application deployed. Through the use of Security Tags, policies can be applied automatically to newly created workloads, allowing reduce manual administrative overhead. For example, when an add a new VM tag is added, it automatically assumes the relevant policies of the tag's groups.

WELCOME TO THE FUTURE OF CYBER SECURITY

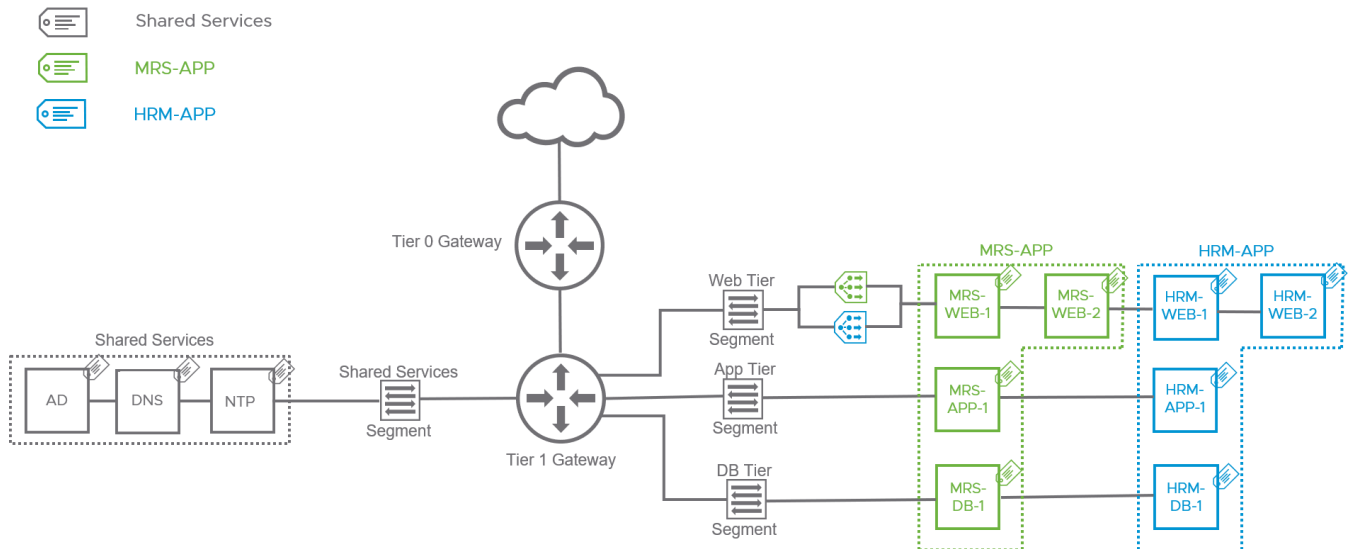


Figure 11: Dynamic Context-Based Grouping (Source: VMware Inc.)

## Check Point integration with NSX using CloudGuard

The integration of Check Point CloudGuard with NSX-T brings consistent policy management and enforcement of advanced security protections automatically deployed and dynamically orchestrated into software-defined data-center environments. CloudGuard provides industry-leading threat prevention security to keep data-centers protected from even the most sophisticated threats.

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, and QoS) in software. As a result, these services can programmatically be assembled in any arbitrary combination to produce unique, isolated virtual networks in a matter of seconds.



For more information related to Technical configuration and deployment modes, please refer to the SK [sk139213](#) (CloudGuard for NSX-T: Service Insertion at the Edge & Service Chaining), [sk157912](#) (CloudGuard for NSX-T Known Limitations) and CloudGuard IaaS for NSX-T Security Gateway R80.30 Deployment Guide.

### Key Business Benefits

- Dynamic insertion and orchestration of Check Point's advanced threat prevention security
- Operationally feasible secure micro-segmentation for east-west traffic protection
- Fine-grained access control policies tied to NSX defined objects, security groups, and virtual machines
- Unified security management and visibility across physical networks, SDDCs and hybrid cloud environments
- Security services provisioned in minutes for fast application deployments
- Shared security context to enable better alignment across security controls
- Isolation and auto-remediation of infected virtual machines
- Improved day-to-day operational efficiencies by automating routine tasks and integrating security into workflow and change management processes
- Advanced security services seamlessly provisioned and orchestrated at the speed of DevOps processes

### Automation and Orchestration

Check Point CloudGuard Controller leverages NSX security automation for dynamic distribution and orchestration of CloudGuard Gateway for protecting east-west traffic. In the data-center environment, there is often a need to integrate different systems that manage the security workflow. Besides, repetitive manual tasks must be automated to streamline security operations. Check Point's security management API allows for granular privilege controls, so that edit privileges can be scoped down to a specific rule or object within the policy, restricting what an automated task or integration can access and change. This ability to automatically provision trusted connectivity provides security teams with the confidence to automate and streamline the entire security workflow.

WELCOME TO THE FUTURE OF CYBER SECURITY

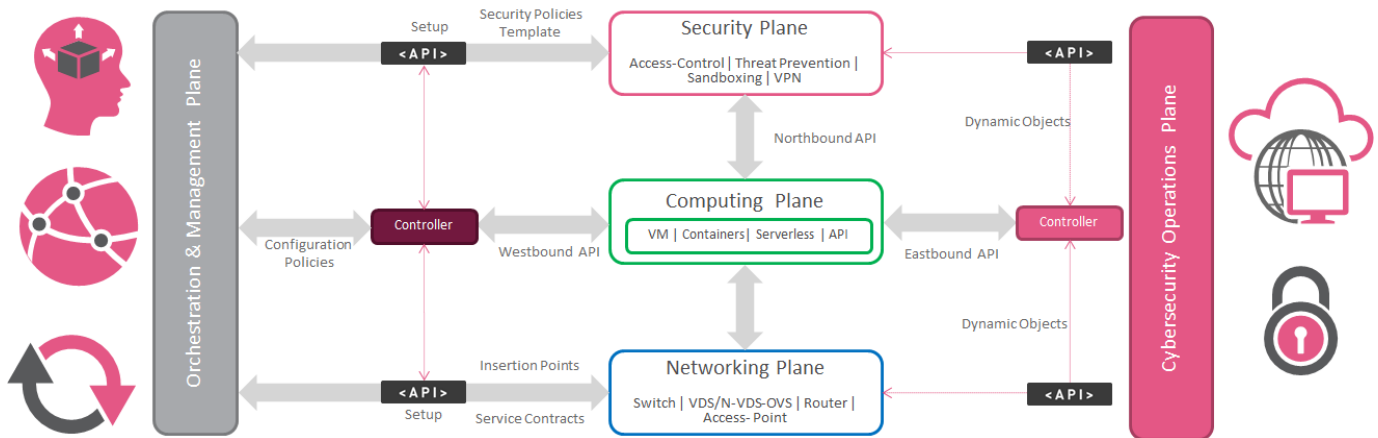


Figure 12: SDDC Automation and Orchestration Planes (Source: ...)

## Ubiquitous Security Enforcement

Check Point CloudGuard integration with VMware NSX allows dynamic insertion of advanced security protection between workloads enabling distributed enforcement at every virtual interface. The integration automates and simplifies the provisioning of CloudGuard gateways into the NSX virtual fabric to protect east-west traffic from lateral movement of threats enabling feasible micro-segmentation. NSX's essential firewalling capability can be extended with Check Point's CloudGuard, whose layered security policy approach makes it easy to segment policy and provide granular rule definitions specific to network segments.

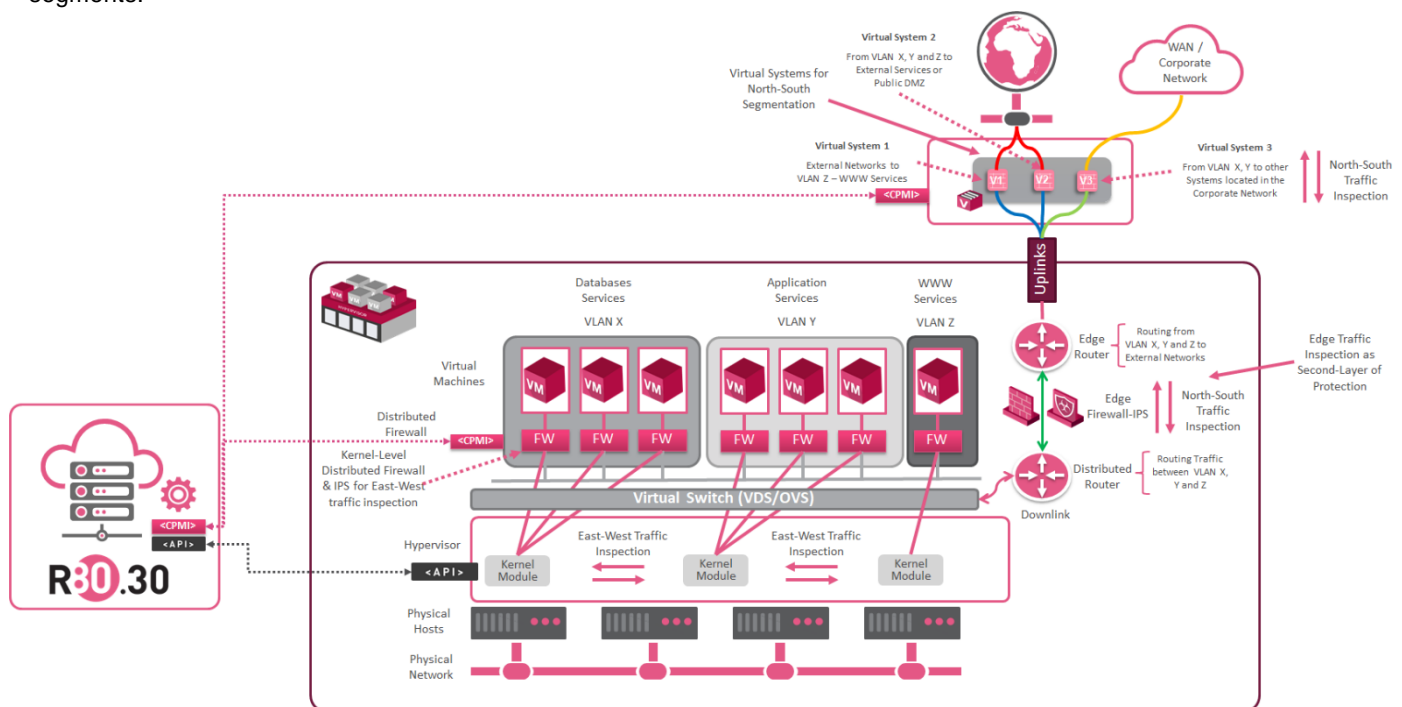






Figure 13: Check Point VSX and CloudGuard integrated with NSX-T (Based in the Gartner Security & Risk Management Summit 2019)



WELCOME TO THE FUTURE OF CYBER SECURITY



## Policy Enforcement

	Firewall	Limits network access to only permitted services and allowed network segments
	Identity Awareness	Limits access to users with the proper credentials, i.e., only to those who have authorized access
	Application Control	Limits access to approved applications and enable and educate users on the safe use of the Internet
	URL Filtering	Limits access to approved sites and enable the safe use of the Internet

## Context-Aware Security Policies

The integration with VMware NSX controller and vCenter shares context with the Check Point CloudGuard controller allowing security groups and VM identities to be imported and reuse within Check Point security policies. This reduces security policy creation from minutes to seconds. Real-time context sharing of security groups maintained so that any changes or additions to the infrastructure automatically tracked without the need for administrator intervention. Security protections dynamically applied to newly created applications regardless of where they hosted.






## Data Protection

	Content Awareness	Restricts the Data Types that users can upload or download
	Data Loss Prevention	Protects personal healthcare information (PHI), personally identifiable information (PII), financial data and others

## Auto-Quarantine of Infected Hosts

Hosts identified by CloudGuard as infected can be automatically isolated and quarantined. This accomplished by CloudGuard tagging the infected hosts and sharing this information with the NSX controller. Additionally, automated remediation services can be triggered by an orchestration platform. Threats are quickly contained, and the appropriate remediation service can be applied to the infected VM.

## Threat Prevention

	IPS	Enables virtual-patching of network services and applications that may be vulnerable to exploits
	Antivirus	Prevents known malware
	Anti-Bot	Detects and block bot behaviors and communications with known Command and Control servers
	Sandboxing	Inspects files for malicious content and behaviors
	Threat Extraction	Delivers safe content to users while files are analyzed in the background

WELCOME TO THE FUTURE OF CYBER SECURITY

## Centralized Security Management

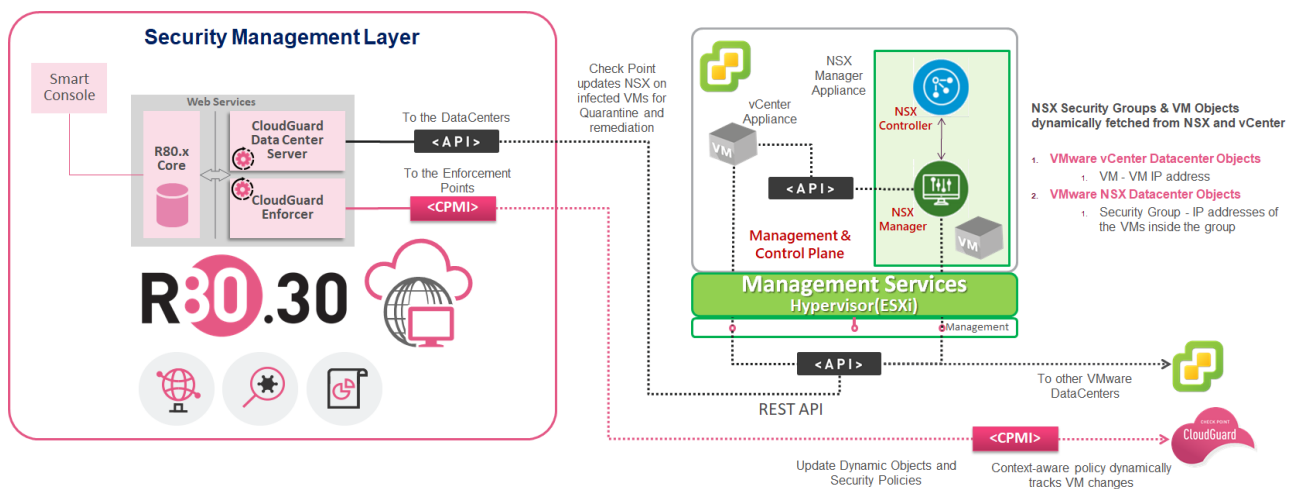
Security management becomes dramatically simplified with centralized configuration and monitoring using CloudGuard. Traffic logged can easily be viewed within a single dashboard; the security reports can be generated to track security compliance across both the data-center and hybrid network. A layered approach to policy management allows administrators to segment a single policy into sub-policies for customized protections and delegation of duties per application or segment. With all aspects of security management such as policy management, logging, monitoring, event analysis and reporting centralized via a single dashboard, security administrators get a holistic view of the security posture across their entire organization – from legacy premises to SDDC to hybrid cloud.

## Check Point CloudGuard controller

CloudGuard can read the Datacenter inventory from NSX and allows the security operator to use objects from the inventory as part of the security policy. CloudGuard Controller watches these objects and updates the gateway regarding any change that might occur on the NSX side. It is essential to mention that API communication to NSX-T v2.4/2.5 allows the dynamic export of network topology, providing immediate access to all network configuration changes. As Asset Scanner, it helps to build Virtual Machines and Security Group's inventory is an excellent tool for Asset management process providing a “Data-center abstraction” when importing from NSX manager and vCenter objects dynamically tracking object changes and allowing using security groups in the Check Point security policies, reports, and logs.



For more details, please refer to the following [SK128612](#) (R80.20 and R80.30 CloudGuard Controller Known Limitations). In a cross-vCenter NSX environment, you can have multiple vCenter Servers, each of which must be paired with its NSX Manager. One NSX Manager assigned the role of primary NSX Manager, and the others assigned the role of secondary NSX Manager.

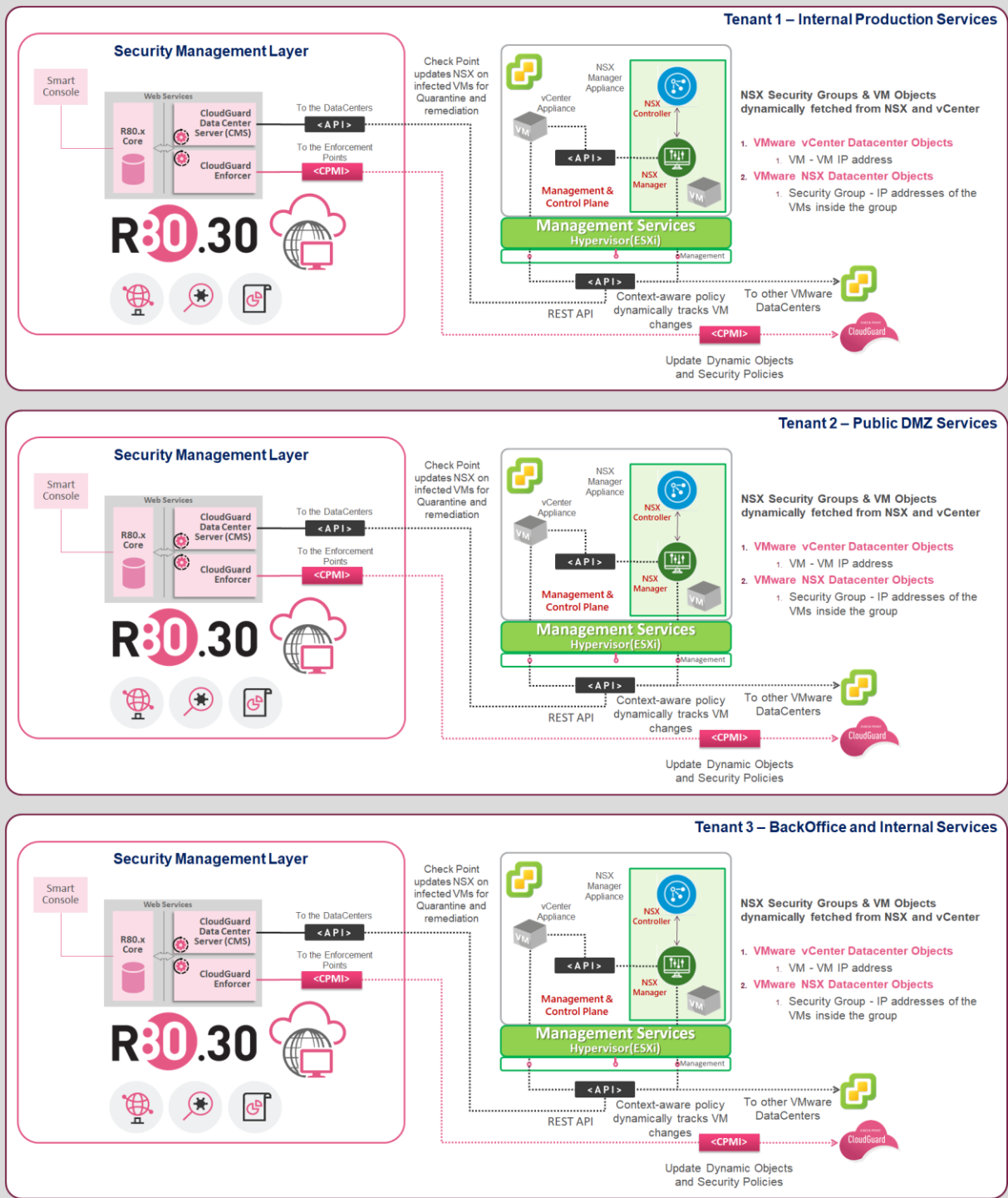


**Figure 14: Check Point CloudGuard Controller integration with VMware vCenter and NSX Manager for Single Tenant**

Additionally, we can provide support for Multitenant environments, and this capability provides to the organizations the capability to split Security Management. Multi-domain Security Management (aka. Provider-1) delivers more security and control by segmenting your security management into multiple virtual domains for different Tenants deployed in NSX-T. Now the organizations of all sizes can easily create virtual domains based on business units.

**Note:** Using VMware objects in the Global Policy is not supported; they are defined only at the Domain Management Server level; for more details, please refer CloudGuard Controller R80.30 Administration Guide.

**Multitenant Manager**

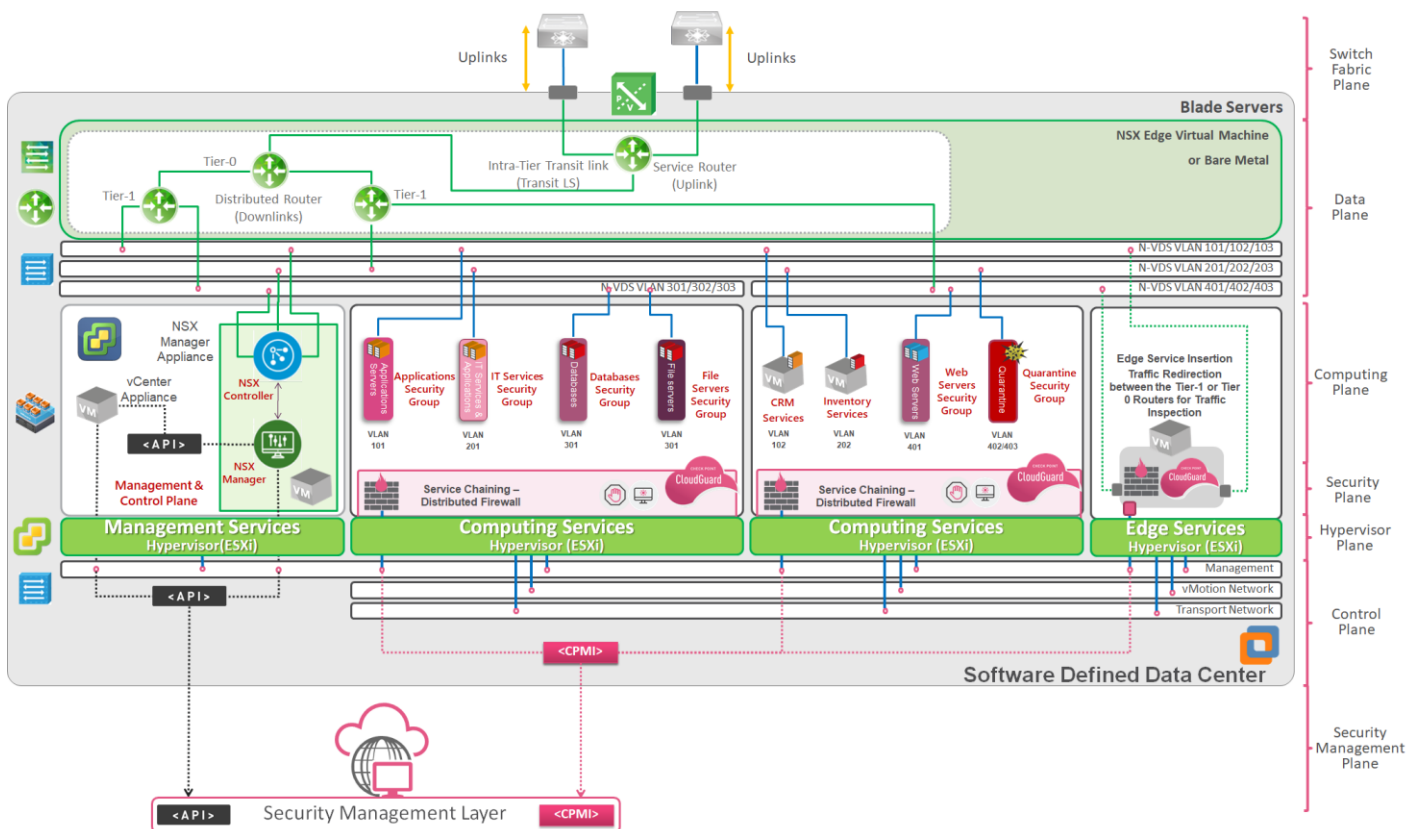


**Figure 15: Check Point CloudGuard Controller integration with VMware vCenter and NSX Manager for Multitenant environments**

## Check Point CloudGuard Private IaaS gateway

CloudGuard Private IaaS Gateway provides enforcement of advanced security protections automatically deployed and dynamically orchestrated into software-defined data-center environments with the integrated multi-layered security protections:

- Stateful Firewall, Intrusion Prevention System (IPS), Antivirus and Anti-Bot technology to protect data-centers against lateral movement
- SandBlast Zero-Day Protection sandbox technology provides the most advanced protection against malware and zero-day attacks
- Application Control to help prevent application layer Denial of Service (DoS) attacks and by that protect the software-defined data-center
- Context-aware Inspection: By focusing on the relevant content for any given connection, CloudGuard eliminates wasted processing, thus reducing latency.



**Figure 16: Reference Architecture integrating Service Chaining and Edge Service Insertion**

CloudGuard Private IaaS gateway can be deployed in two different options: Edge Service Insertion and Service Chaining, this capability allows to the organizations to do the segmentation in the DataCenter; however, it is essential to define four different activities before to implement NSX-T:

1. **Servers identification and Classification:** This is an essential activity because all the internal systems must be named and grouped according to the Service Functionality, for example, Web Servers, Application Servers, Databases, File Servers, Directories, etc. This step is critical for accurate design. In the Flat environment, most of those systems share the same network, and the surface attack is high due to the capability of Lateral Attacks. This identification and classification are tasks in the Asset Management process, providing the visibility of all assets in the datacenter.
2. **Server grouping or Functionality Grouping:** Create functional groups, applications, Web Servers, Application Servers, Databases, File Servers, Directories assigned in separate and different groups. This activity is the basis of the Security and Functionality Segmentation attributing the Distributed Firewall and Threat Prevention rules to the group instead of individual Virtual Machines. This is a great benefit due to the management is simplified and centralized, providing the "abstraction" allowing the automation to manage the discovery of assets building a repository of multiple types of Assets.
3. **Group security policies:** Commonly, organizations require to inspect all the traffic in the SDDC; however, the Server Grouping/Functionality Grouping approach requires to create completely separate Distributed Firewall and



WELCOME TO THE FUTURE OF CYBER SECURITY

Threat Prevention rules for each group, this is the approach of the Rule-Based IPS to provide accurate traffic inspection and being more proactive.

4. **Threat Prevention and Access Control rule:** Once the abstraction of data-center is done, Access Control rules for east-west traffic can easily be deployed, including the usual traffic between the load balancer, application servers, and databases, additionally the traffic inspection with the Threat Prevention rules.

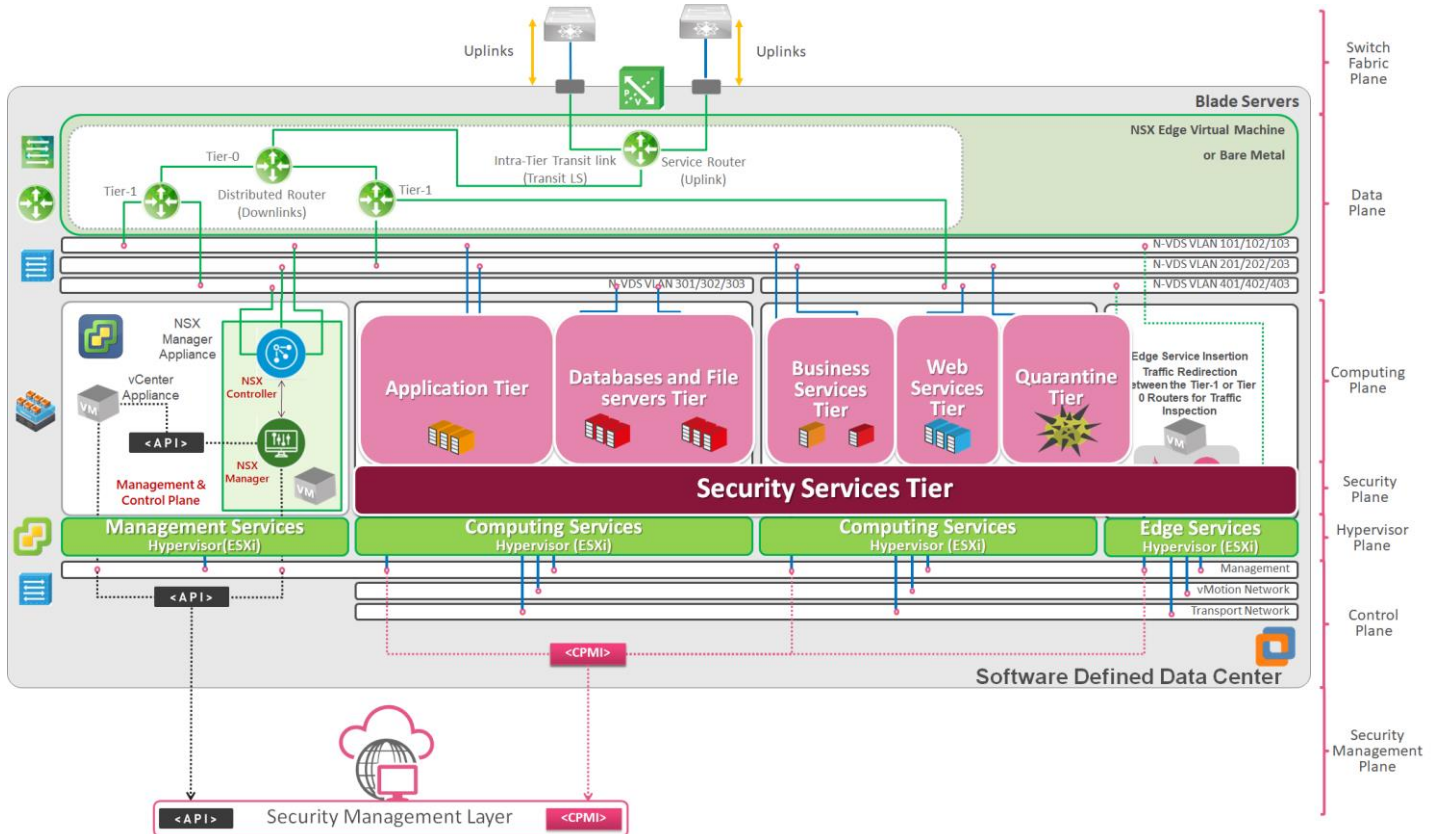


Figure 17: Reference Architecture integrating Security/Functionality Zones

### When to use Service Insertion versus Service Chaining?

Before discussing different use cases with CloudGuard and NSX-T, it is crucial to understand the differences between Service Insertion and Service Chaining. First, we will start to define Service insertion, and it refers to the capability to add different network services, such as Firewalls, Intrusion Prevention Systems, NAT, VPN, and load balancers into the forwarding path of traffic. For another hand, Service chaining builds on service insertion allowing to link (build chains) of multiple services in a predefined manner, for example, **Web Servers** → **IPS** → **Application Servers** → **IPS** → **Databases** and also integrating malware protection before forwarding to deliver the services to the End-User.



- **Service insertion (NSX-T 2.3):** Good for Security Segmentation, uniquely to identify and steer selected traffic to and from a Security Group or Virtual Machine.
- **Service chaining (NSX-T 2.4):** Excellent for links multiple services for specific purposes, deploying targeted measures for low latency and packet transactions.

WELCOME TO THE FUTURE OF CYBER SECURITY

## Integration Modes with NSX-T

- **Service Insertion at the Edge NSX-T** Data Center as a key networking platform provides a rich set of capabilities that allow you to create network topologies that connect and secure application endpoints (VMs, containers, bare-metal servers). With this release, NSX can now deploy your choice of partner security solutions at the edge of NSX-T network topologies, i.e., at the Tier 0 and Tier 1 routing boundaries. NSX-T Data Center onboards and catalogs the partner services, allowing the NSX Administrator to deploy and consume the cataloged services.
- **Service Chaining for the East-West** service plane provides its forwarding mechanism. The forwarding mechanism allows policy-based redirection of traffic along chains of services. Forwarding along the service plane entirely automated by the platform: failures detected, existing/new flows redirected as appropriate, flow pinning performed to support stateful services, and multiple path selection policies are available to optimize for throughput/latency or density.

### CloudGuard Private IaaS with Service Insertion at the Edge (NSX-T 2.3)

Using VMware NSX-T and Check Point CloudGuard together provides robust security for North-South traffic entering the data-center from the outside, done by connecting the CloudGuard IaaS security gateway to the T0-T1 router.

- NSX handles the deployment, **plumbing, and selective redirection of traffic** to the CloudGuard IaaS security gateway. CloudGuard for NSX-T acts as a Security Gateway in a bridge mode that is invisible to Layer-3 traffic. When authorized traffic arrives, the Security Gateway passes it to the next interface through the bridging.
- Then, it creates a Layer-2 relationship between two or more interfaces.
- Traffic that enters one interface exits the other interface.
- Bridging lets the Security Gateway inspect and forward traffic without the original IP routing.

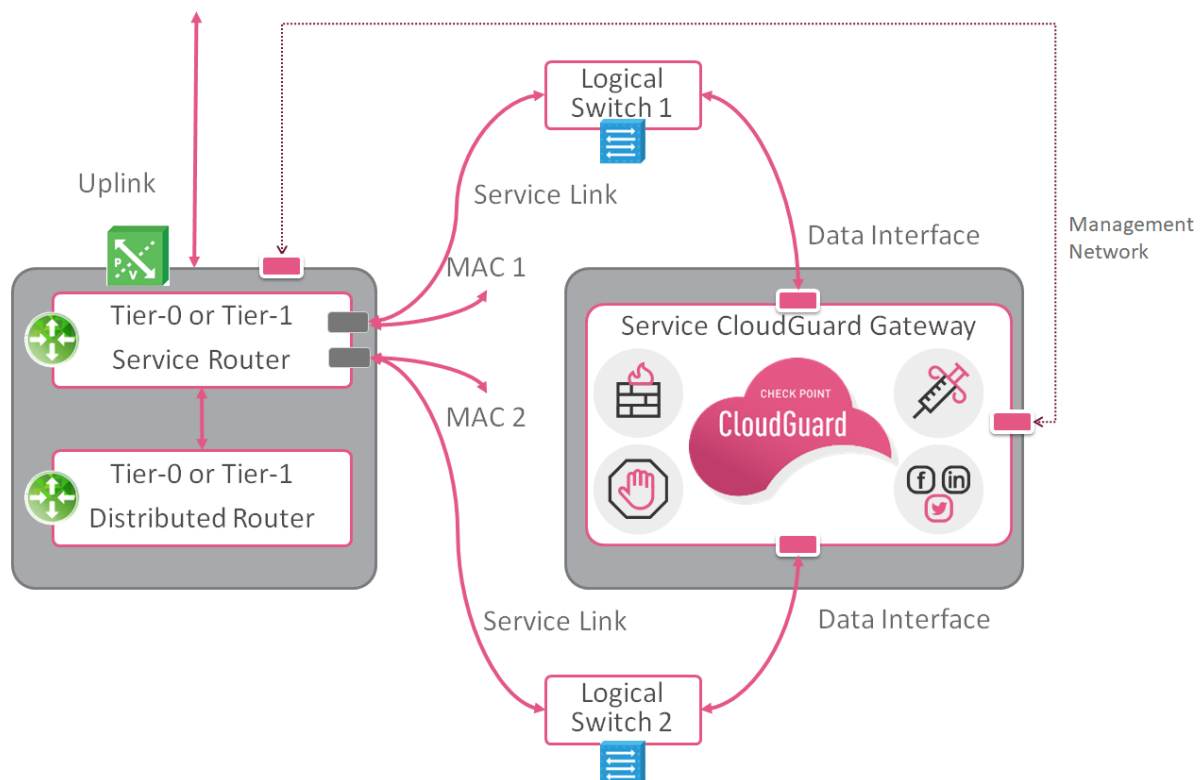
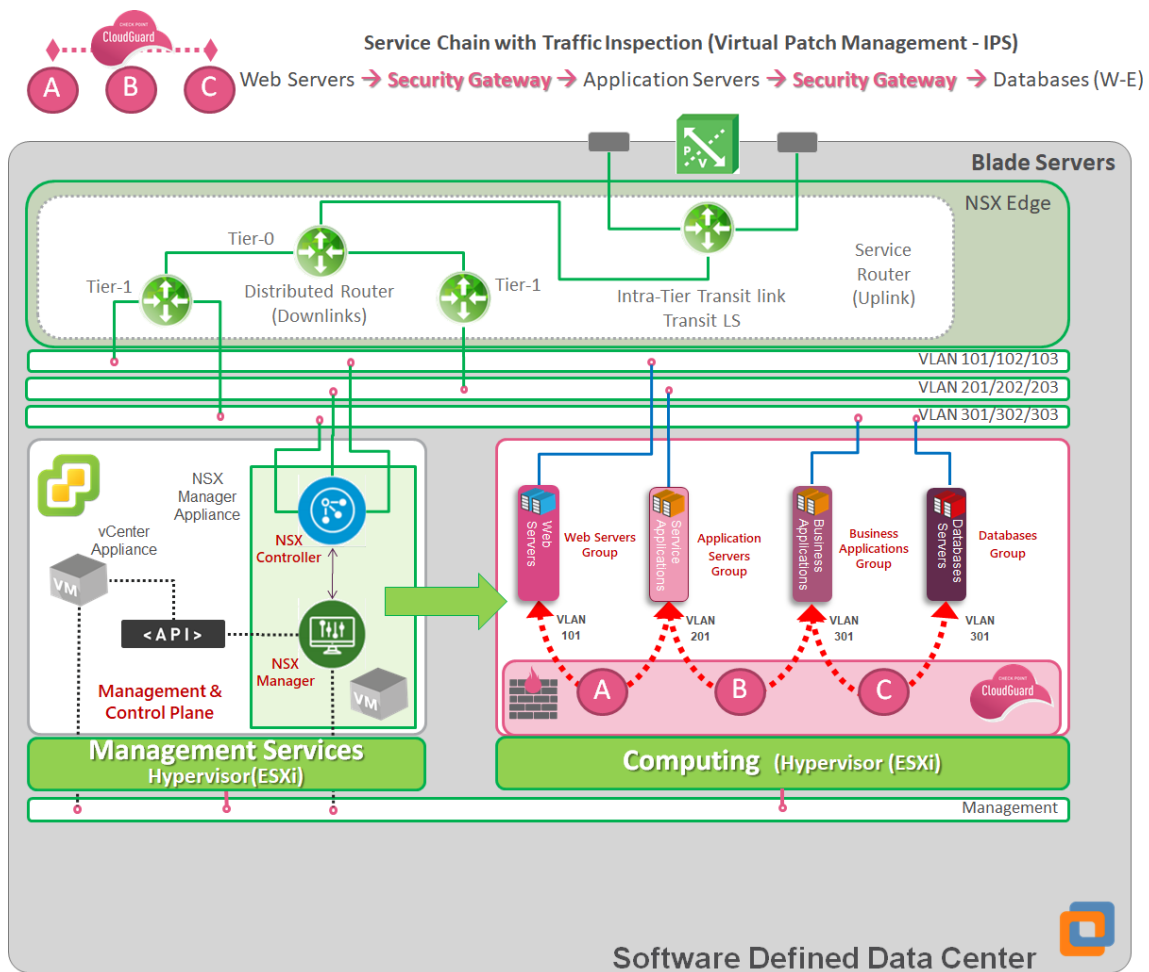


Figure 18: CloudGuard Service Machine for Service Insertion

### CloudGuard Private IaaS with Service Chaining (NSX-T 2.4)

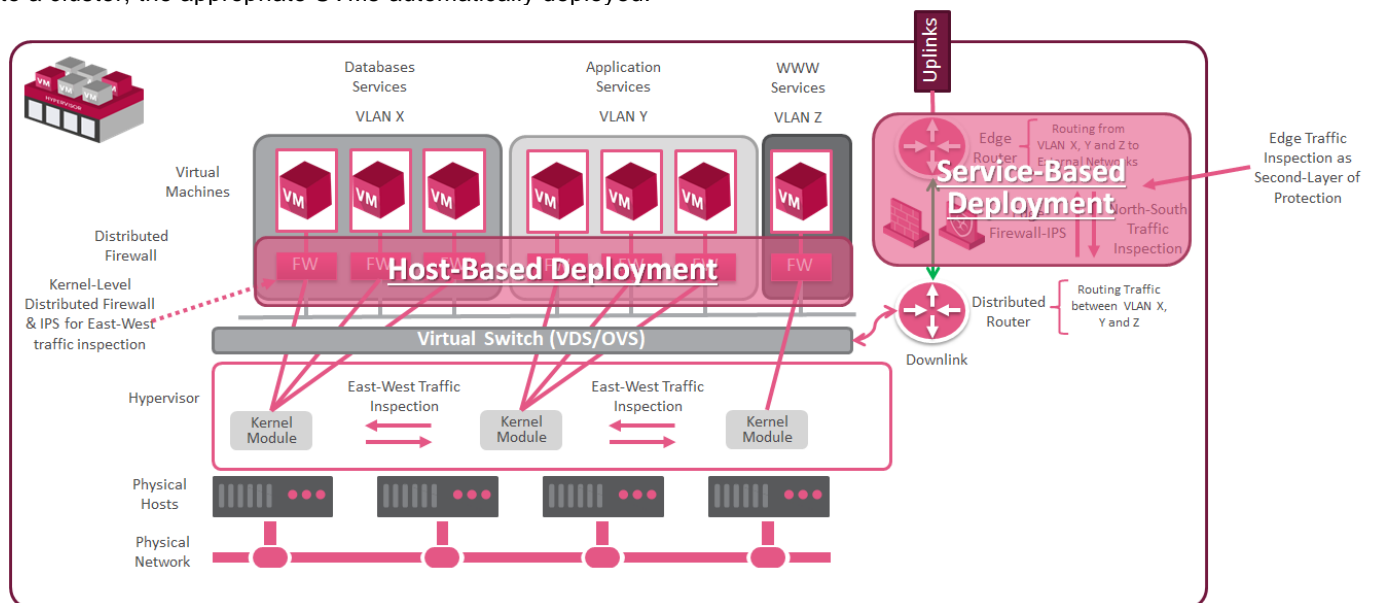
CloudGuard for NSX-T can leverage service insertion to act as a Security Gateway in hairpin bridge mode, in which the Gateway can inspect all the traffic redirected to it by the forwarding mechanism; authorized traffic will be passed back to the bridge interface, **allowing the forwarding mechanism** to return the traffic to its original path. Bridging lets the Security Gateway inspect and return traffic without the original IP routing.



**Figure 19: Rule-Based Traffic Inspection using Service Chaining**

### CloudGuard Private IaaS with Service Chaining and Edge Service Insertion (NSX-T 2.5)

In NSX-T 2.5, we have two modes of Partner SVM deployment supported: Clustered deployment, in which Service Virtual Machines are deployed on a dedicated vSphere (Service) Cluster and Host-Based deployment, in which one Service Virtual Machine per service is deployed on each Compute Host in a particular cluster. In this mode, when a new compute host is added to a cluster, the appropriate SVMs are automatically deployed.



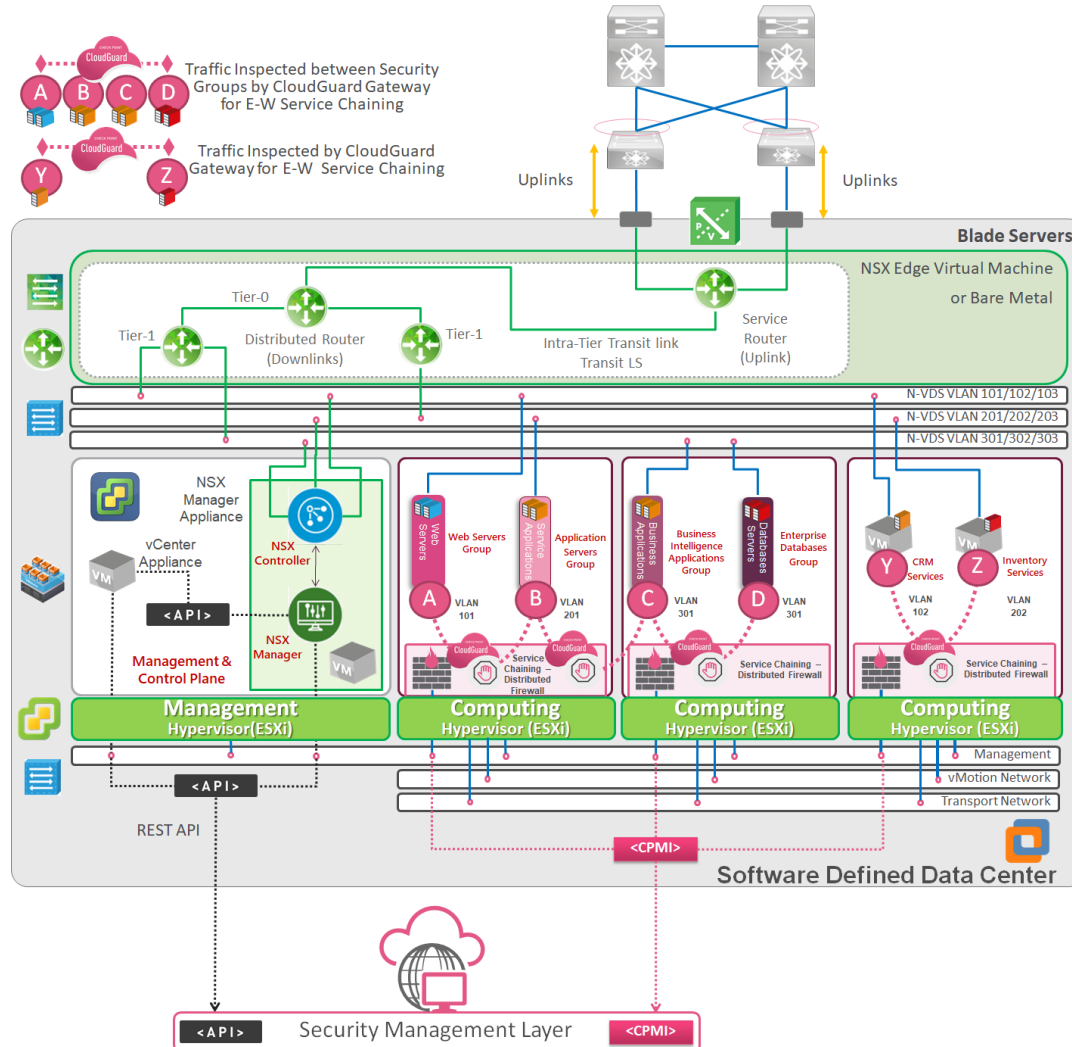
**Figure 20: Service chaining and Edge Service insertion with NSX-T 2.5 and Check Point CloudGuard**

WELCOME TO THE FUTURE OF CYBER SECURITY

# Use cases and best practices scenarios

This main section focus is to explain different use cases, where we can overview different scenarios where Edge Service Insertion and Service Chaining can deploy with suggested security policies.

## Service chaining between Security Groups for East-West traffic



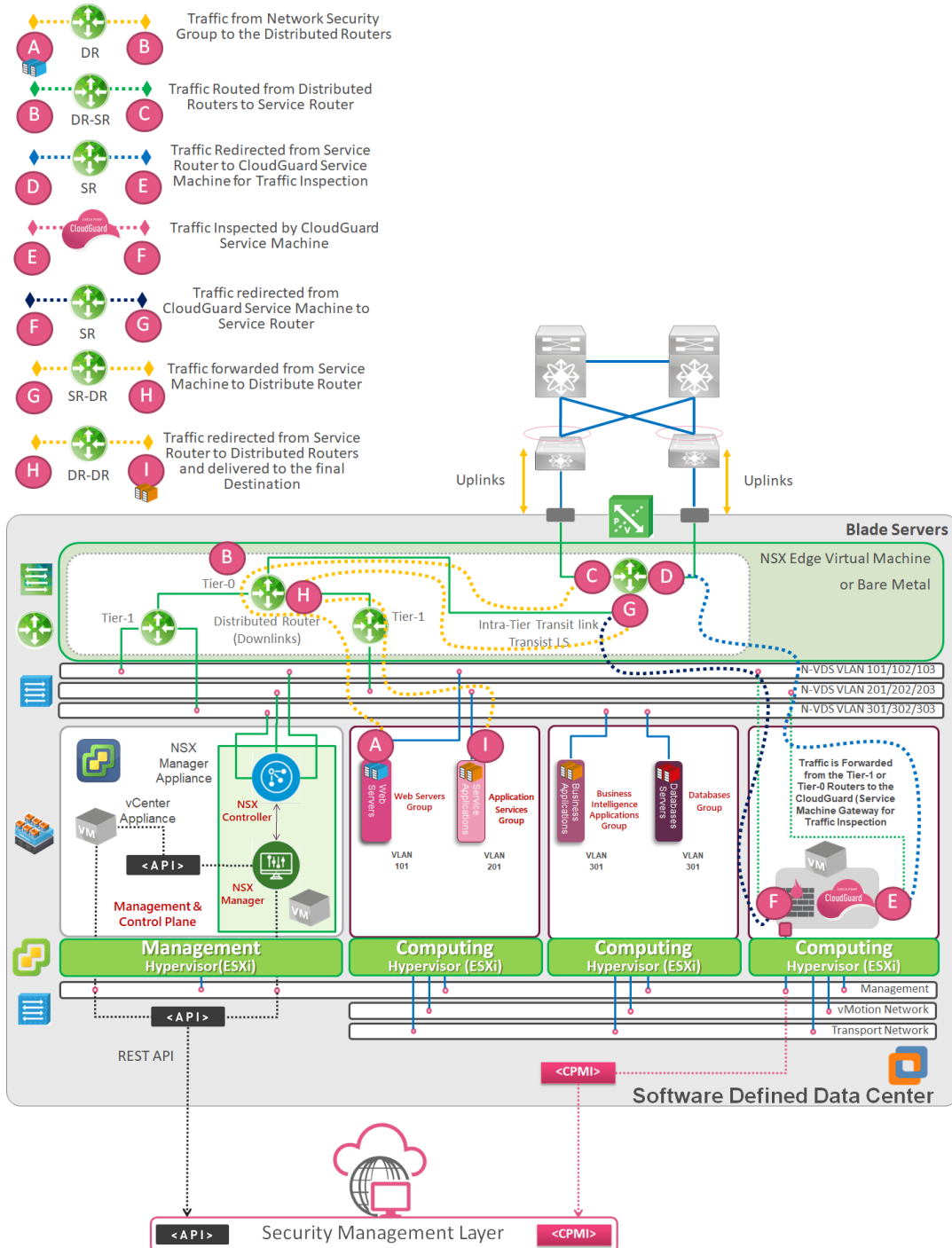
In this scenario, we process all the Internal traffic (E-W), and we can provide micro-segmentation capabilities, where the traffic is forwarded through the Service Chaining configuration. In general cases, organizations choose this option due to the Low-latency and fast throughput provided at the Kernel Level. The security enablers and controls suggested for this scenario are the Firewall, IPS (for virtual patching), Antivirus and Security Tags (for Dynamic context grouping) and some cases Application Control for specifically customized signatures if the customer wants to protect and to log third-party and legacy applications with custom development. About automation and orchestration, CloudGuard Controller can do the Data Center “abstraction,” it means that all Virtual Machines and Security Groups can dynamically be updated in the security policies using dynamic objects; additionally, the Dynamic Context Grouping can provide in an automated way the right policy for traffic inspection or quarantine in the case the Antivirus detects malicious code.

### Suggested Security Policy:

Security Segment (Security Tags)	Source	Destination	Access Control	Threat Prevention	IPS Signatures	NSX-T Mode?
Applications-Tiers (Production)	Web Servers Security Group	Application Servers Security Group	LOG	LOG	Tomcat	Service Chaining
Business Intelligence (Production)	Application Servers Group	Business Intelligence Application Group	LOG	LOG	Java/PHP/XML	Service Chaining
Database-Tier (Production)	Business Intelligence Application Group	Databases Security Group	LOG	LOG	Microsoft SQL Postgress/Oracle	Service Chaining

WELCOME TO THE FUTURE OF CYBER SECURITY

## Edge Service insertion for East-West traffic between Security Groups



This scenario-focused for the Security segmentation between the SDDC and external networks. It means that at the Edge, we can create specific perimeters for certain services provided by the DataCenter and protected by the Enforcement module (Security Gateway), where we can deploy the Firewall, IPS, Antibot, Antivirus and probably specific scenarios advanced sandboxing to prevent Malicious code. As we discussed before, with the automation and orchestration process, CloudGuard Controller can do Data Center “abstraction,” meaning that all Virtual Machines and Security Groups can dynamically be updated in the security policies. Additionally, the Dynamic Context Grouping can provide in an automated way the right policy for traffic inspection or quarantine in the case the Antivirus detects malicious code.

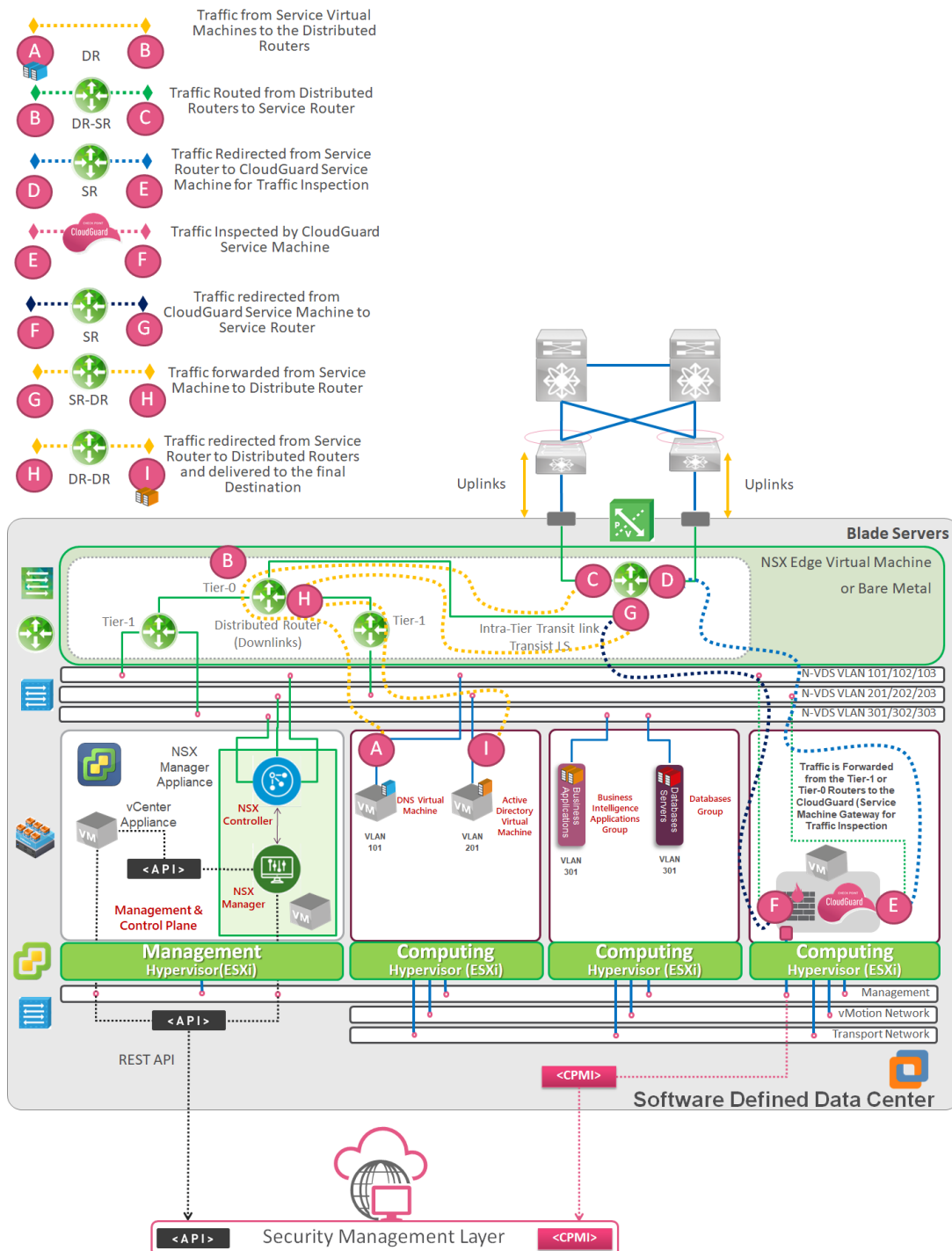
### Suggested Security Policy:

Security Segment (Security Tags)	Source	Destination	Access Control	Threat Prevention	IPS Signatures	NSX-T Mode?
Applications-Tiers (Production)	Web Servers Security Group	Application Servers Security Group	LOG	LOG	Tomcat/Java	Edge Service Insertion



WELCOME TO THE FUTURE OF CYBER SECURITY

# Edge Service insertion for East-West traffic between Virtual Machines



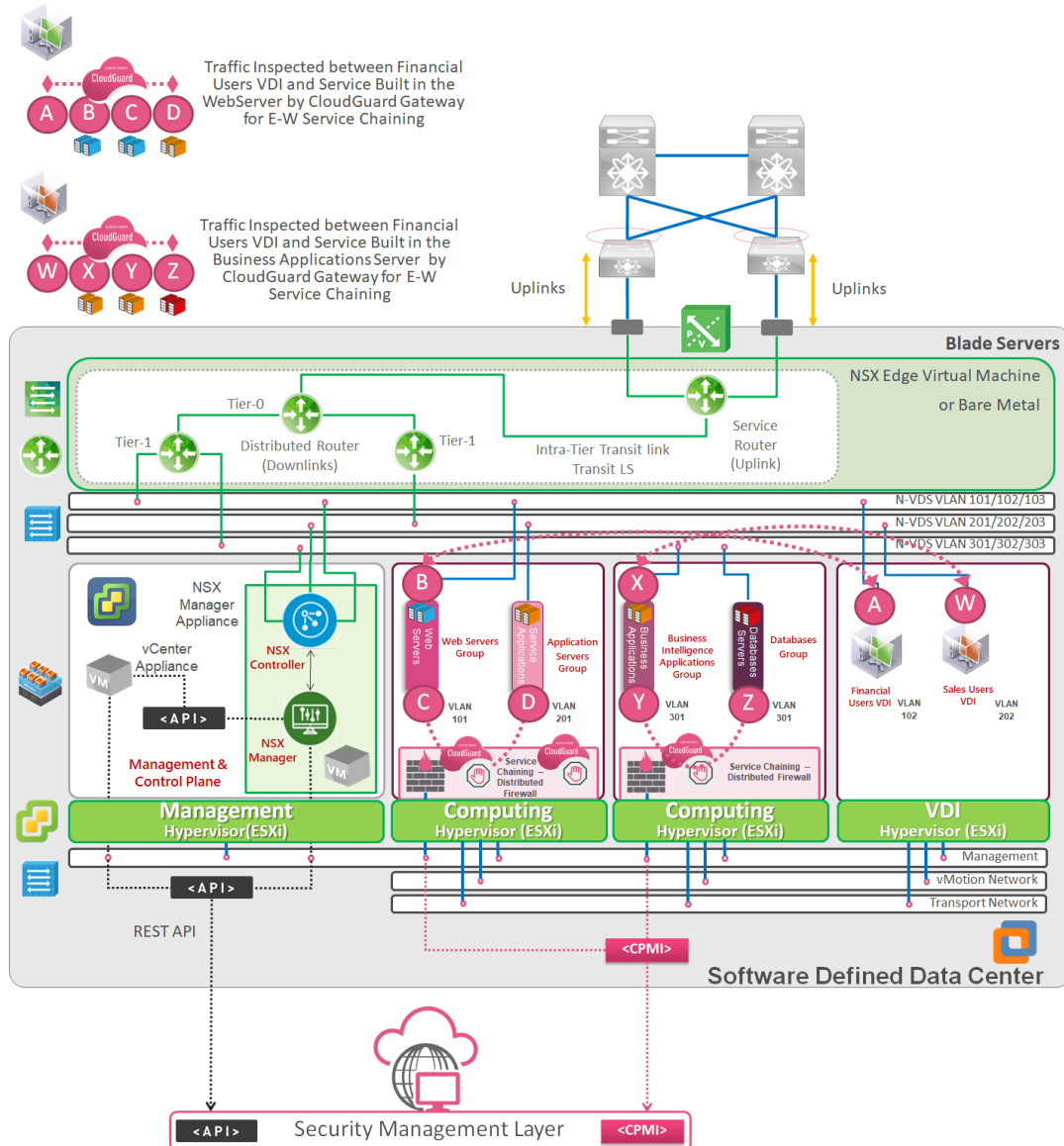
This scenario is similar to scenario number 2; the main difference here is the use of only Virtual Machines instead of Security Groups.

### Suggested Security Policy:

Security Segment (Security Tags)	Source	Destination	Access Control	Threat Prevention	NSX-T Mode?
IT Services Tier (Operations)	Active Directory - VM	DNS Server - VM NTP Server - VM			Service Chaining

WELCOME TO THE FUTURE OF CYBER SECURITY

# Service chaining between Security Groups and Virtual Desktops for East-West traffic



This scenario is growing in several organizations where the focus is to close “Users” with the “Applications” using thin clients and however, the lack of security segmentation and the appropriate traffic inspection can lead security issues. Providing security to the VDI Virtual Machines provides the capability to have a “Service chaining” just only for the approved or authorized applications. This approach helps organizations to reduce the surface attack. Ransomware attacks in the data-centers can lead to a considerable problem, especially for the availability and continuity of the Business.

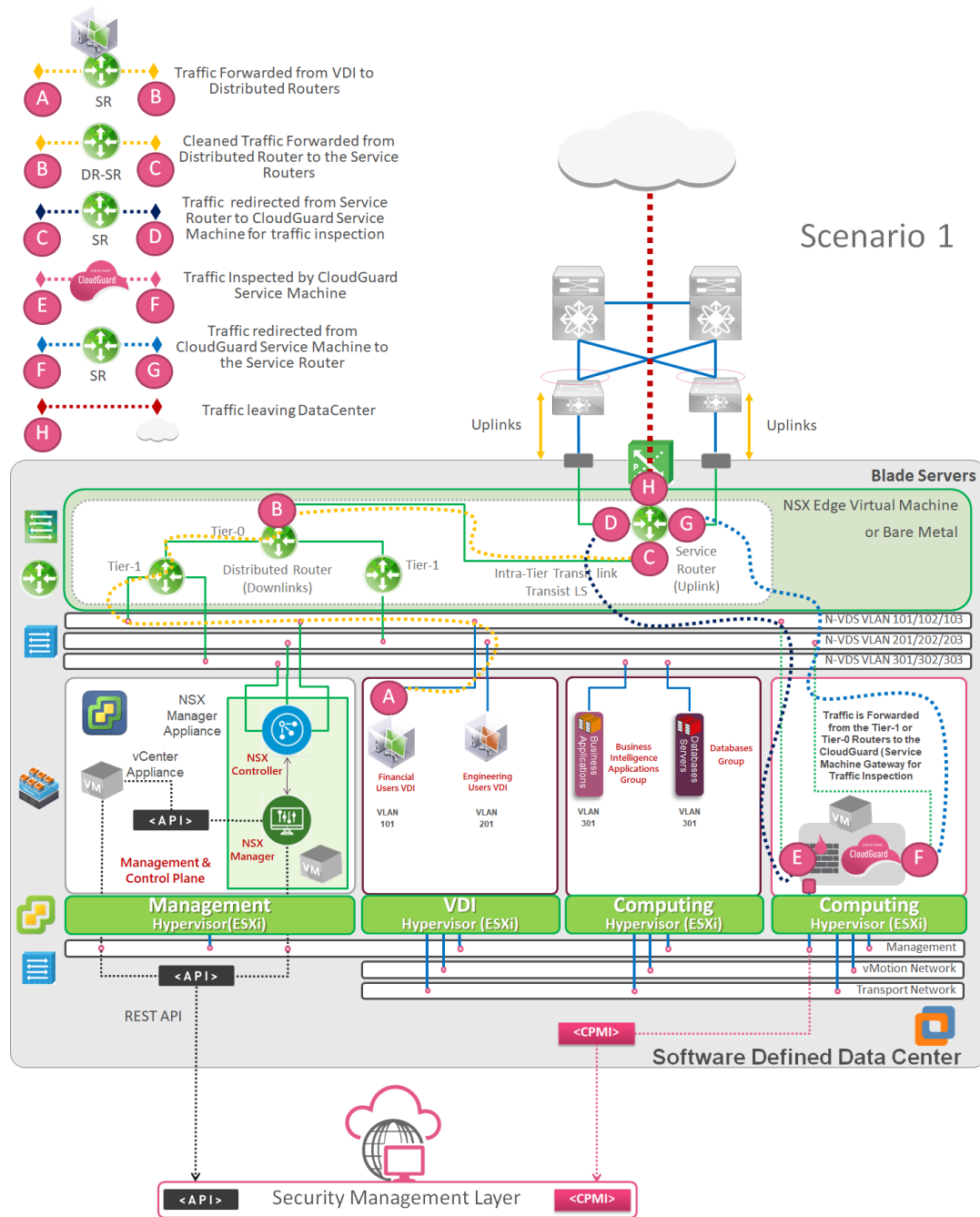
Under this scenario, we can help the organizations to reduce the lateral attacks providing the right micro-segmentation from authorized desktops to authorized applications providing the alignment for the Zero-Trust approach: **“Do not trust, Verify.”**

## Suggested Security Policy:

Security Segment (Security Tags)	Source	Destination	Access Control	Data Protection	Threat Prevention	NSX-T Mode?
Thin Clients (Operations)	Virtual Desktops	Web Servers Group	LOG	LOG	LOG	Service Chaining
Applications-Tiers (Production)	Web Servers Security Group	Application Servers Security Group	LOG	N/A	LOG	Service Chaining
Business Intelligence (Production)	Application Servers Group	Business Intelligence Application Group	LOG	N/A	LOG	Service Chaining
Database-Tier (Production)	Business Intelligence Application Group	Databases Security Group	LOG	N/A	LOG	Service Chaining

WELCOME TO THE FUTURE OF CYBER SECURITY

# Edge Service insertion for North-South traffic between Virtual Desktops and External Networks

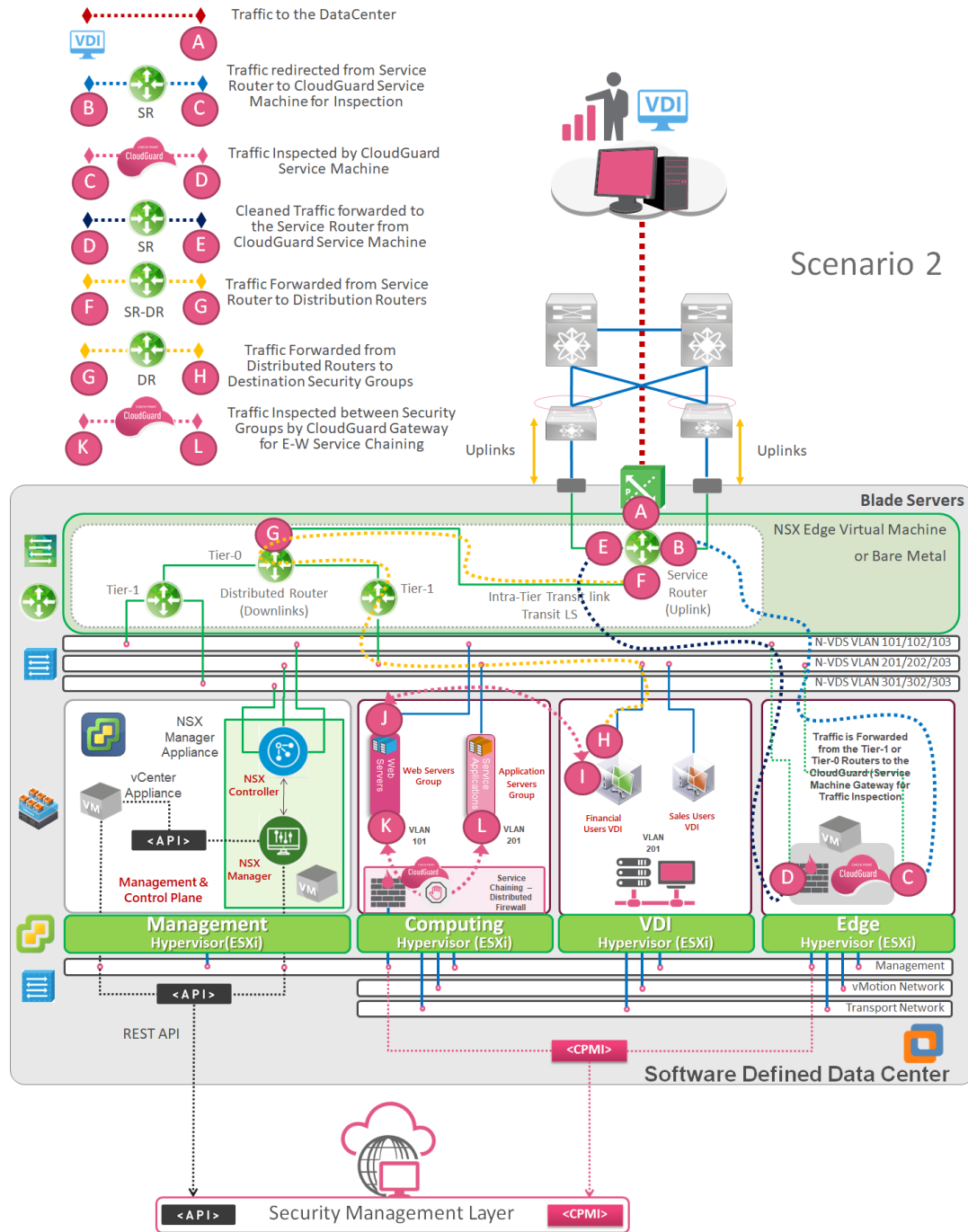


This scenario is focused **only and only** if the organization is looking to provide internet access for specific VDI's, not all. However, this approach could lead to different security breaches if the organizations do not implement appropriate security controls. In this use case, the Edge Service Insertion is relevant due to we can provide a "security" perimeter to isolate the VDI user to access the Internet or another external resource of Datacenter. The suggested security controls to be deployed are: Firewall, IPS (Virtual Patching – Client signature ONLY), Antivirus, Antibot, and Sandboxing capabilities to PREVENT entering potential malicious codes. This scenario could prevent the Lateral-Attacks in the Virtual Machines and Security Groups inside the Data Center.

### Suggested Security Policy:

Security Segment (Security Tags)	Source	Destination	Access Control	Data Protection	Threat Prevention	NSX-T Mode?
Thin Clients (Operations)	Virtual Desktops		URL, LOG	LOG	LOG	Edge Service Insertion

WELCOME TO THE FUTURE OF CYBER SECURITY

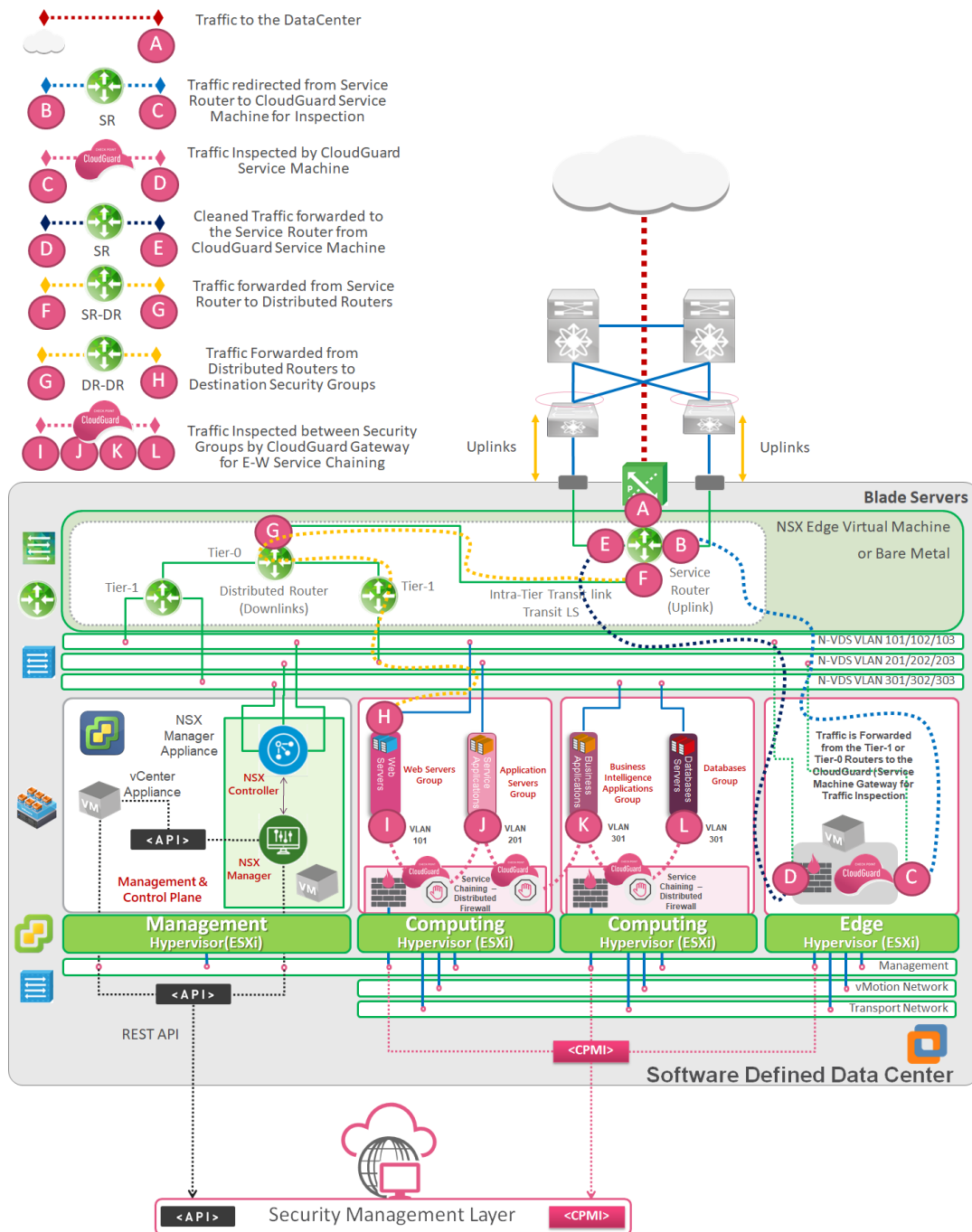


**Suggested Security Policy:**

Security Segment (Security Tags)	Source	Destination	Access Control	Data Protection	Threat Prevention	NSX-T Mode?
Thin Clients to VDI	Thin Clients Subnets	Virtual Desktops	LOG			Edge Service Insertion
VDI Clients (Operations)	Virtual Desktops	Web Servers Group	LOG	LOG		Service Chaining
Applications-Tiers (Production)	Web Servers Security Group	Application Servers Security Group	LOG	N/A		Service Chaining
Business Intelligence (Production)	Application Servers Group	Business Intelligence Application Group	LOG	N/A		Service Chaining
Database-Tier (Production)	Business Intelligence Application Group	Databases Security Group	LOG	N/A		Service Chaining

WELCOME TO THE FUTURE OF CYBER SECURITY

## Service Chaining (E-W) + Edge Service Insertion (N-S)



This scenario is the complete approach to reduce surface attacks. The Edge Service Insertion provides the appropriate segmentation between the SDDC and external networks or the Internet. The first layer is focused on reducing the surface attack and providing access for specific services only, and this is the Edge Service Insertion. In the second layer, Service Chaining can provide a better approach for traffic inspection; however, integrating Dynamic grouping, the organizations can use much better traffic inspection. We have the principle of Rule-Based IPS or Rule-Based Threat Prevention. This principle is focused only to inspect the relevant traffic for the relevant applications, optimizing and improving the performance in the Data Center. Implementing Full traffic inspection for all the SDDC Applications is not the right approach, due to the organizations could lead to performance issues and affect the continuity of the business. Service Chaining with Rule-Based Threat Prevention and Dynamic Context Grouping can provide a cost-effective, secure, and stable solution for the organizations.



WELCOME TO THE FUTURE OF CYBER SECURITY

**Suggested Security Policy:**

Security Segment (Security Tags)	Source	Destination	Access Control	Threat Prevention	IPS Signatures	NSX-T Mode?
Web-Tier (Distribution)		Web Servers Group			Windows Apache/IIS Linux Apache	Edge Service Insertion
Applications-Tiers (Production)	Web Servers Security Group	Application Servers Security Group			Tomcat/Java	Service Chaining
Database-Tier (Production)	Application Servers Security Group	Databases Security Group			Microsoft SQL Postgress/Oracle	Service Chaining

## Conclusion

Software-defined networking and security provided by VMware solution via NSX-V and NSX-T with Check Point CloudGuard provide a robust network virtualization platform. VMware NSX is a network “hypervisor” for virtual networks, which allows extending and designing a virtual network infrastructure in line with organization needs, providing the tools required to solve the challenges faced in terms of security, compliance, and micro-segmentation.

NSX-V and NSX-T are both great solutions for software-defined networking needs. However, while solving many of the same challenges, NSX-V and NSX-T share some essential differences. NSX-V is a software-defined solution that has brought vSphere customers to where they are today with their SDN solution; NSX-T is the next step. With NSX-T 2.4, VMware has made an evolution for Multi-cloud, and the Multi-hypervisor approach for Hybrid Cloud will provide a considerable benefit for the organizations that are working into their Cloud Transformation strategy.

### ABOUT CHECK POINT

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leading provider of cybersecurity solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry-leading catch rate of malware, ransomware, and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises’ cloud, network, and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

### ABOUT VMWARE INC.

VMware is a leader in cloud infrastructure and business mobility. Build on VMware’s industry-leading virtualization technology; our solutions deliver a brave new model of IT that is fluid, instant, and more secure. Customers can innovate faster by rapidly developing, automatically delivering, and more safely consuming any application. VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at [www.vmware.com](http://www.vmware.com)

### CONTACT US

**Worldwide Headquarters** | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)

**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-654-4233 | [www.checkpoint.com](http://www.checkpoint.com)