

# Advanced Security Services with Trend Micro Deep Security and VMware NSX Platforms

» This document is targeted at virtualization, security, and network architects interested in deploying cloud and software-defined data center (SDDC) architectures based on VMware® network virtualization solutions (VMware NSX) with the Trend Micro Deep Security Platform.



# Contents

Background and Executive Summary.....	3
Solution Benefits.....	3
VMware NSX Solution Components.....	4
Trend Micro Deep Security Solution Components.....	5
How the Integrated Solution Works.....	5
Overview.....	5
Integrate.....	6
Deploy.....	7
Automate.....	7
Putting it all together.....	8
Deep Dive.....	9
Network Introspection.....	9
Traffic Redirection.....	9
Guest Introspection.....	10
Scan Request and Integrity Changes.....	10
Reference Architecture.....	12
Conclusion.....	14
References.....	15

## Background and Executive Summary

It is an undisputed fact that virtualization has a remarkable impact on our data center computing environment. The cost savings from consolidation that were the initial focus of the virtualization journey have now been long realized by many organizations. These organizations have moved on to achieve benefits such as incredible flexibility and speed in application delivery that virtualization enables. We have seen the overall category of server virtualization mature while the other critical data center components such as networking technologies and security services have not advanced at a similar pace. Networking technologies in particular had remained relatively static until the start of the software-defined data center era.

The software-defined data center is an evolution and extension to server virtualization. While server virtualization provides dramatic efficiencies in the deployment of computing power, the software-defined data center does the same for all of the resources needed to host an application: storage, networking, and security. The VMware NSX networking and security platform is a key element of VMware's vision for the software-defined data center.

Trend Micro and VMware work closely together to develop joint solutions that extend NSX's core networking and security services with best-of-breed security deployed with enterprise-class scaling and manageability. [Deep Security](#) is Trend Micro's flagship server security solution for virtualized and cloud environments. Since 2009, Deep Security has been protecting thousands of customers worldwide with best-in-class agentless security for VMware vSphere. The integration of Trend Micro Deep Security with NSX extends Trend Micro's security services platform including anti-malware, firewall, intrusion detection/prevention (IDS/IPS), web application protection, and integrity monitoring to the software-defined data center, enabling customers to leverage combined strengths for superior security and automation.

## Solution Benefits

The key benefits of this integrated solution from Trend Micro and VMware include:

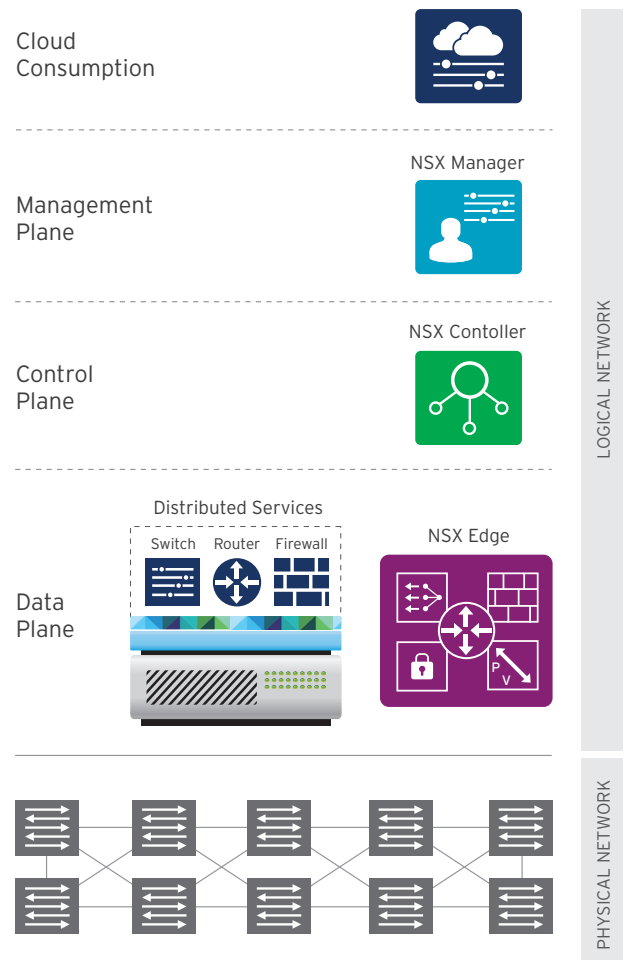
- **Integrated Security Services.** Organizations can provide enhanced security services such as Distributed Firewall from VMware NSX and traffic redirection to Trend Micro Deep Security for intrusion prevention and further traffic analysis to help protect critical business applications from known and unknown threats. Further leveraging Guest Introspection Services such as File Integrity Monitoring and Anti-Malware can provide a defense in depth security model all from a single security virtual appliance.
- **Operational Efficiency with Orchestration Framework.** Security services can now be deployed automatically without manual operational activity through the use of a new common NSX tagging and orchestration framework. Administrators can trigger vendor-defined or ad-hoc workflows based on security or administrative events. This could be used to automate real-time remediation and incident response during attacks, as well as, enable direct coordination between Trend Micro and VMware security layers.
- **Dynamic Security Policy Assignment.** The Deep Security Solution's ability to sync with VMware NSX Services groups allows organizations to define dynamic security policy assignment tasks within Deep Security Manager. As virtual machines are instantiated and placed in the NSX security groups, they can be mapped to specific Event-Based Tasks in Deep Security Manager to help enforce security policy created specifically for that security group. This seamless integration and real-time synchronization make it easy to apply correct security policy to the virtualized workloads regardless of when they are created and whether they move across the network.

## VMware NSX Solution Components

In conventional networking, the three planes of networking are implemented in the firmware of networking device. Software-defined networking (SDN) decouples the data and control planes, removes the control plane from network hardware, and implements it in software instead. VMware NSX contains various components that operate at data plane, control plane, and management plane as shown.

The following are the key components from VMware NSX for this integrated solution:

- NSX Manager.** The NSX manager is the centralized network management component of NSX, and is installed as a virtual appliance on any ESX host in a vCenter Server environment. It runs in a management plane and provides an aggregated system view. One NSX manager maps to a single vCenter Server environment and allows security administrators to interact with other NSX solution components such as a distributed firewall. It also allows VMware partner solutions to integrate with VMware NSX platforms using REST API's.
- Service Composer.** VMware Service Composer is an orchestration framework that provides a network and security services consumption model. It allows you to provision and assign firewall policies and security services to applications in real time in a virtual infrastructure. Security policies are assigned to groups of virtual machines, and the policy is automatically applied to new virtual machines as they are added to the group.
- NSX Controller.** The NSX controller is the central control point for all logical switches within a network and maintains information of all virtual machines, hosts, logical switches, and VXLANs. It is deployed as a virtual appliance through the NSX manager and it operates in control plane. It's the component of NSX that manages logical networks and provides directory services such as MAC, ARP, and VTEP tables.
- Distributed Services.** These are add-on NSX kernel-level modules (VIB's) that run within the hypervisor kernel and provide services such as distributed firewall, routing, and enabling VXLAN bridging capabilities.



## Trend Micro Deep Security Solution Components

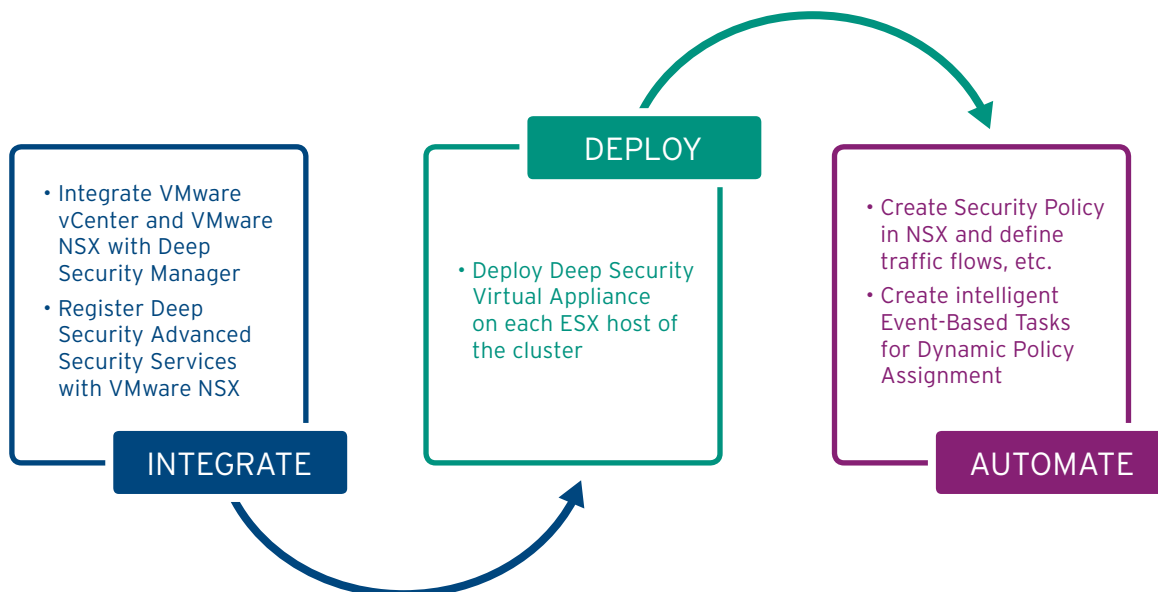
The following are the key components from Trend Micro for this integrated solution:

- **Deep Security Manager.** This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Virtual Appliance (DSVA). The Deep Security Manager is controlled using the web-based management console. From this interface, the administrator can define security policies, integrate VMware solution components (such as NSX manager), and query status of various managed instances.
- **Deep Security Virtual Appliance.** This is a security virtual machine built for VMware vSphere environments that agentlessly provides anti-malware, web reputation, host firewall, intrusion prevention, and integrity monitoring to virtual machines. It's a single virtual appliance that provides both Guest Introspection Services and Network Introspection Services by integrating with the VMware NSX platform.

## How the Integrated Solution Works

### OVERVIEW

The Trend Micro Deep Security solution integrates directly with VMware NSX Service insertion (NSX Service Composer) to enable automatic deployment of security services in the form of a security virtual appliance. Through this service insertion platform and dynamic linking of security groups, Deep Security allows organizations a safe enablement of applications and complete threat protection, that is, guest introspection services and network introspection services. The diagram provides the overview of the complete integration process.



## INTEGRATE

The integration of Trend Micro Deep Security with VMware vCenter and VMware NSX manager is done via a wizard that collects VMware vCenter and VMware NSX manager connection information and binding credentials. After successful integration with VMware solution components, Deep Security is aware of all ESXs and VMs within the virtualized environment.

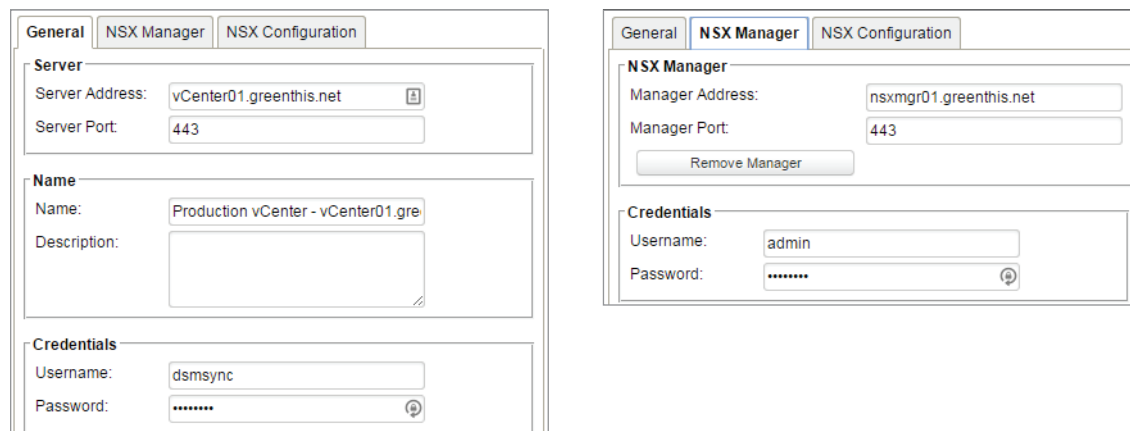
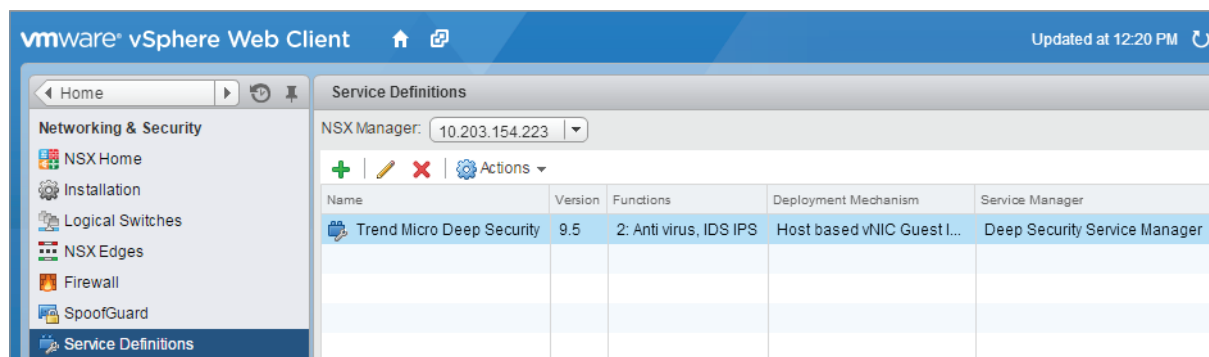


Figure 1: Trend Micro Deep Security Integration with VMware NSX

The integration also triggers the registration process with NSX so that Deep Security can be registered as an advanced security service to provide both Guest Introspection and Network Introspection Services from a single security virtual appliance.



Name	Version	Functions	Deployment Mechanism	Service Manager
Trend Micro Deep Security	9.5	2: Anti virus, IDS IPS	Host based vNIC Guest I...	Deep Security Service Manager

Figure 2: Trend Micro Deep Security Registration with VMware NSX

Additionally, this integration process provides necessary information to the NSX manager (Service Composer) to retrieve the Deep Security Virtual Appliance package (OVF) for automatic deployment.

## DEPLOY

This phase of the integrated solution involves deployment of Deep Security on each ESXi host of the cluster. NSX will automatically load the defined Deep Security Virtual Appliance on each host. If a new host is added to this cluster, these steps will automatically take place and the new host will be ready to provide protection to the virtual system and enforce defined security policy.

## AUTOMATE

Deep Security leverages VMware's NSX (Service Composer) logical groups to provide automatic workflow capabilities using its Event-Based Tasks feature. Deep Security Manager and NSX do a dynamic exchange of the protected policy objects. For example, when a Web-Tier Security Group is created in NSX and a virtual machine is added to it, this information is then transmitted to the Deep Security Manager by NSX. The Deep Security Manager can then apply the specific security policy created for the web servers.

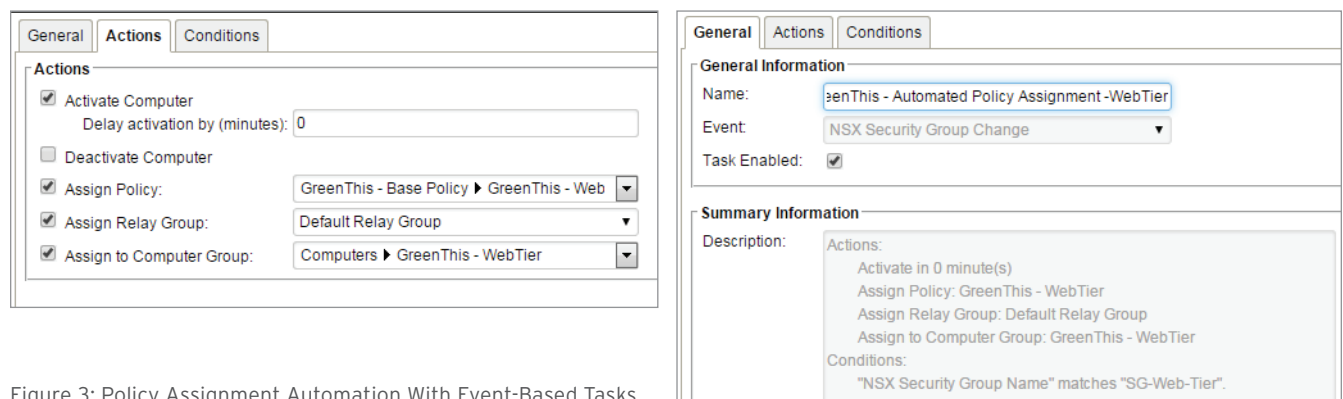


Figure 3: Policy Assignment Automation With Event-Based Tasks

If this virtual machine is moved to a different security group, this change is immediately reflected within the Deep Security Manager. Similarly, Deep Security can take actions as configured by the Deep Security Administrator, for example, assigning a different security policy with different firewall rules.

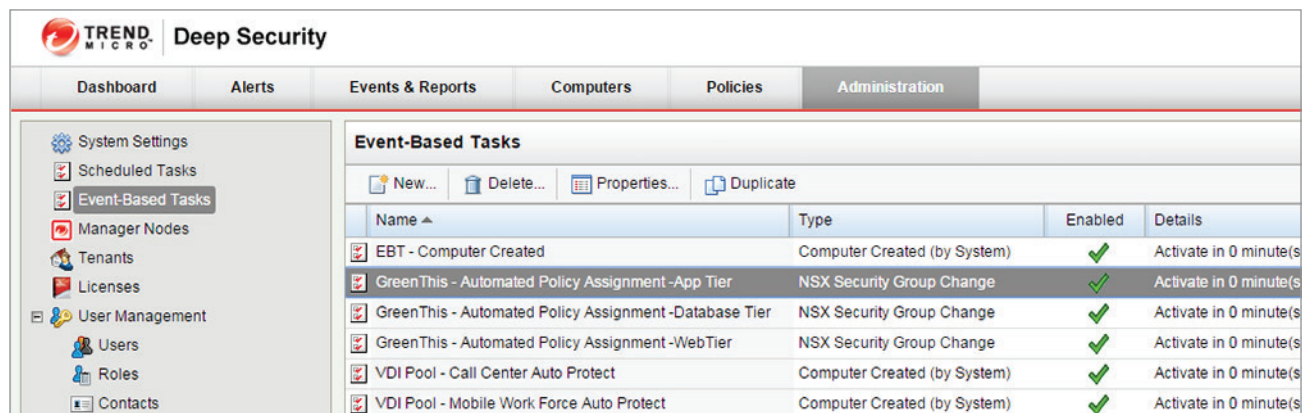


Figure 4: Policy Assignment Automation With Event-Based Tasks

## PUTTING IT ALL TOGETHER

With an integrated solution, organizations can now create automatic security policy assignment workflows and perform dynamic linking of service composer security groups with Trend Micro Security policy to protect their virtual workloads.

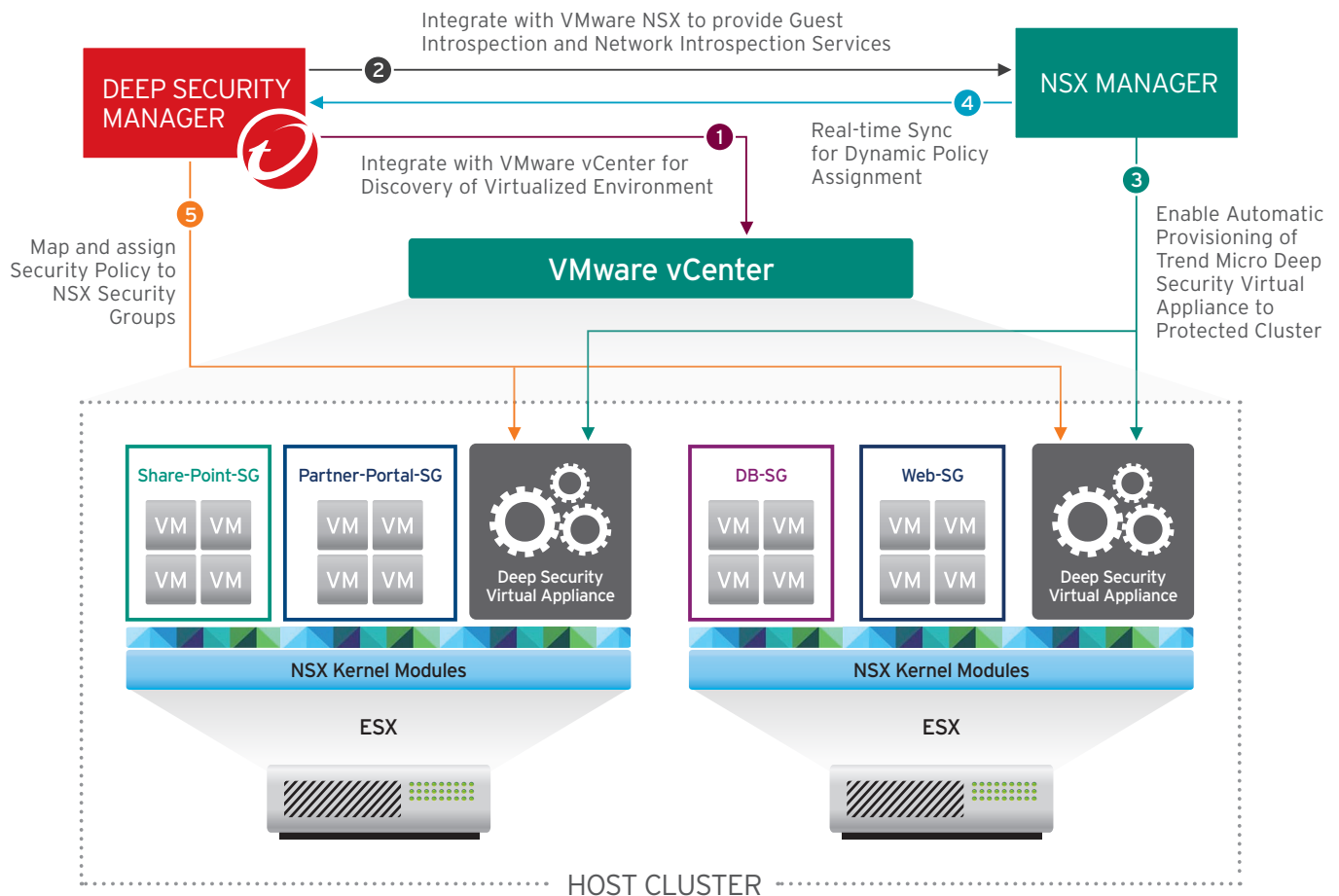


Figure 5: Trend Micro Deep Security and NSX Solution Components Integrated View



## Deep Dive

### NETWORK INTROSPECTION

The NSX distributed firewall (DFW) is the main component in the Trend Micro Deep Security and VMware NSX integrated solution that provides network introspection services. The DFW provides Layer 2 - Layer 4 stateful firewall services to workloads running in an NSX environment. The DFW is activated as soon as the host is prepared by NSX. During this process, a kernel-level vSphere Installation Bundle (VIB), the VMware Internetworking Service Insertion Platform (VSIP) (`esx-dvfilter-generic-fastpath`) is loaded into the hypervisor. This platform is responsible for all data plane traffic protection and redirection to Deep Security for advanced security services such as intrusion prevention and web reputation.

One DFW instance is created per VM per vNIC and it's located between the VM and the Virtual Distributed Switch (VDS). All ingress and egress traffic must go through the DFW instance which is loaded at the vNIC slot 2. Down the traffic flow at slot 4 there is a Filtering Module that either blocks traffic or routes traffic to VDS if it is bypassed. Or it performs traffic redirection to Deep Security via the Traffic Redirection Module for further inspection, policy enforcement, and advanced security services. Once traffic is inspected by Deep Security's network introspection module, it is then returned to the NSX VDS switch for delivery to the final destination. This final destination could be another guest VM or external system.

### Traffic Redirection

As discussed, the network introspection services are provided by redirecting the traffic to the security virtual appliance. This traffic redirection is defined under Security Policy in NSX Service Composer where a security administrator can define required traffic flows, e.g., redirection to Deep Security for advanced security services for all outbound and inbound traffic from web servers.

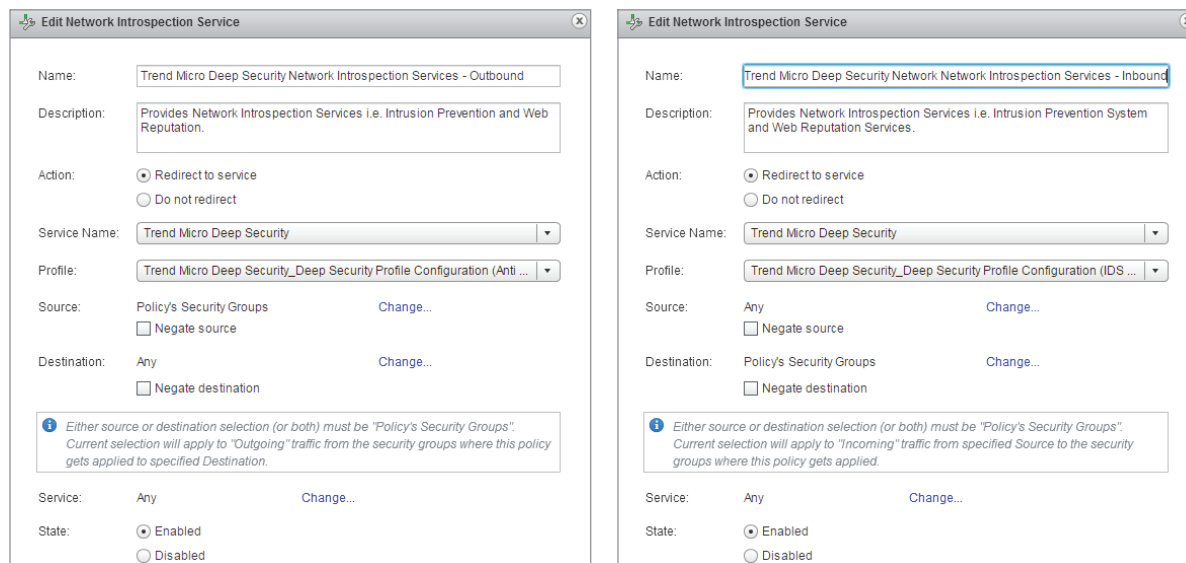


Figure 6: Outbound and Inbound Traffic Redirection to Trend Micro Deep Security

The defined traffic redirection rules can also be viewed from the Partner Security Services tab in NSX 6.1.

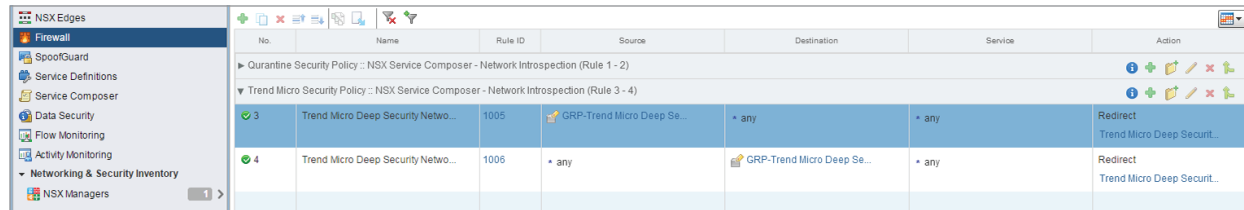
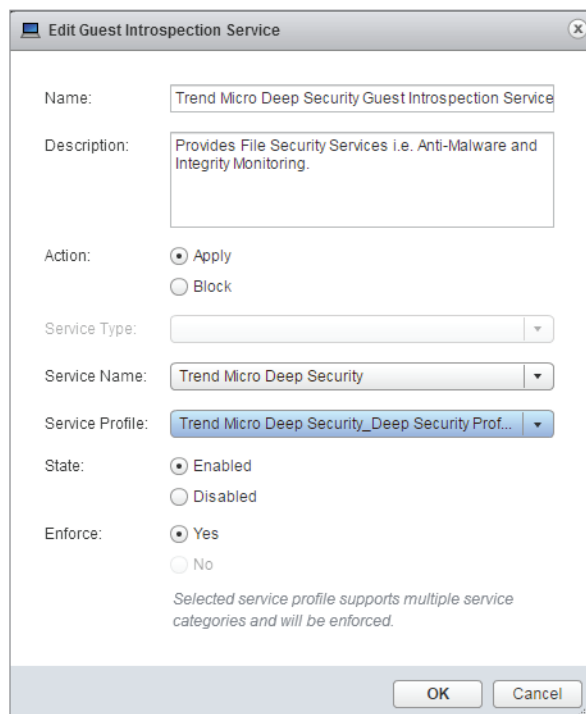


Figure 7: Traffic Rules Shown in the Partner Security Services Tab in NSX

## GUEST INTROSPECTION

Deep Security provides two security functions in the Guest Introspection Module; anti-malware and integrity monitoring. The VMware Guest Introspection Driver (part of VMware tools) is the key component in the Trend Micro Deep Security and VMware NSX integrated solution to provide guest introspection services. This component allows the capture of events from file read/write operations as they occur in the guest and initiate a scanning request of the file to Deep Security for anti-malware functionality. Depending on the result, the access to the file on the guest can be blocked or allowed. In addition, the VMware Guest Introspection Driver allows monitoring specific areas (such as files, directories, registry keys, and registry values) on the guest for changes. If a change occurs (e.g., file permissions are changed, a new file was created, etc.) in the monitored areas, it will be detected by Deep Security.



### Scan Request and Integrity Changes

As discussed previously, the guest introspection services are provided by redirecting the file read/write operations to the security virtual appliance for a scan request to determine if a file is safe to open, etc. This redirection is defined under Security Policy in NSX Service Composer for redirection to the Deep Security Virtual Appliance.

Figure 8: Scan Request Redirection to Deep Security for Anti-Malware and Integrity Monitoring

By leveraging the orchestration framework of VMware NSX and Trend Micro Deep Security, administrators can trigger various workflows. For example: upon malware detection on the VM, Deep Security can apply a security tag to the infected virtual machine and this security tag can then be consumed by VMware NSX (Service Composer) which in turn will move the VM into a quarantined security group. This quarantined security group can have a restricted firewall communication policy to block any external communication over the network except from security tools. Once the incident is dealt with the test system can be moved back to its operational security group.

The diagram below provides a close look of this integration:

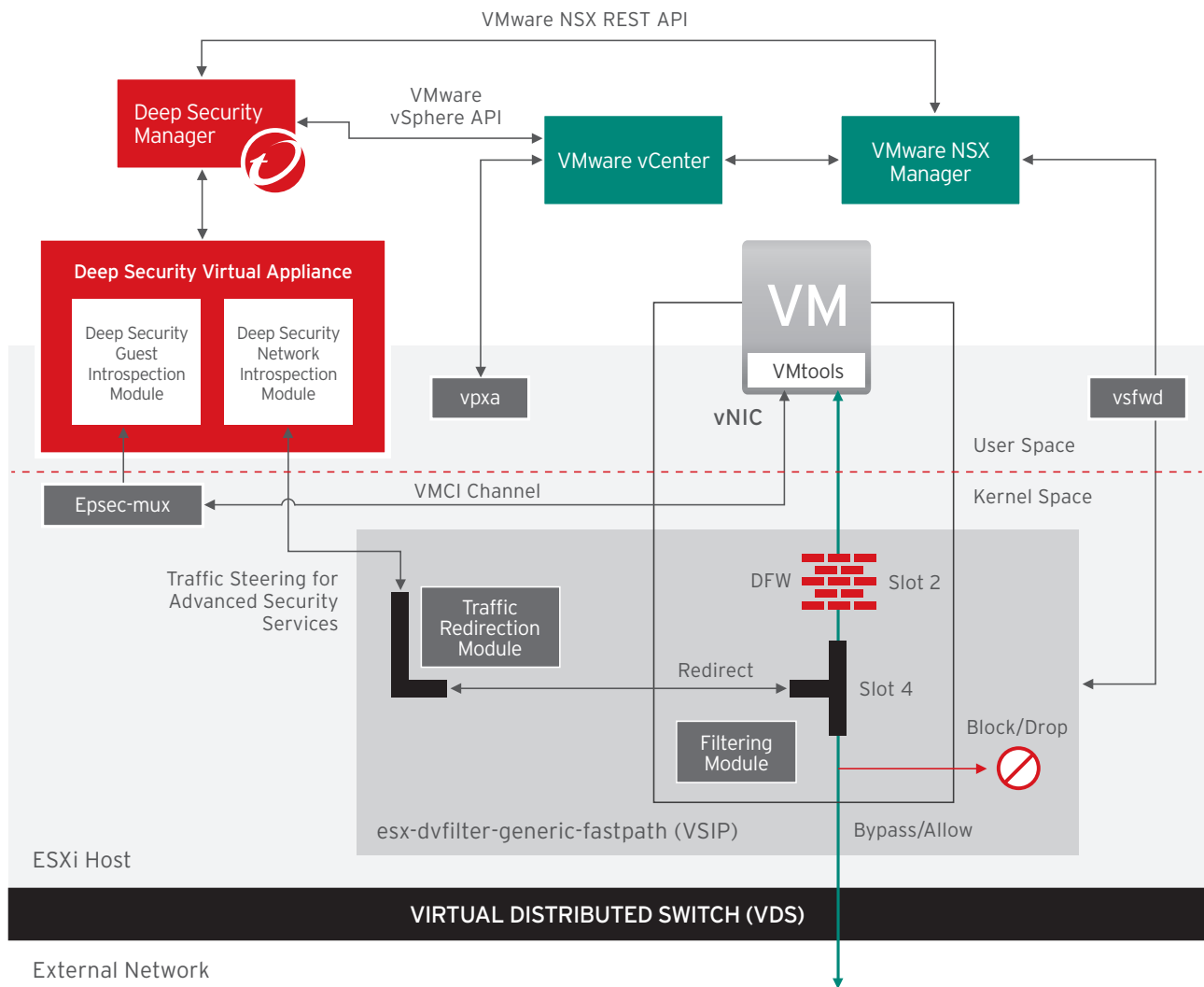


Figure 9: Closer look at VMware NSX and Deep Security Integration

## Reference Architecture

In an NSX-enabled data center, it is desirable to achieve logical separation and grouping of the ESXi hosts providing specific functions such as compute, management, and edge services. This proposed NSX reference architecture with Deep Security recommends grouping ESXi hosts used for computing in separate clusters striped across dedicated racks. The edge and management clusters can instead be combined in a single rack or dedicated racks depending on the scale of the design. Although not required, having separate clusters for compute, management, and edge allows for cluster-level configuration for each cluster without affecting hosts in other clusters. Also, it allows for some predictability of distributed resource scheduling at the cluster-level. This can help ensure, for example that an NSX controller (installed as a VM on a host in the management cluster) does not end up being vMotioned by the Distributed Resource Scheduler (DRS) to a host where NSX Edge Services (contained within the edge cluster) is running. In this reference architecture we have proposed:

- **Management Rack:** to host the management components, including vCenter Server, NSX Manager, NSX Controllers, Cloud Management Systems (CMS), Trend Micro Deep Security Solution Components, and other shared IP storage-related components.
- **Compute Rack:** to run your virtualized workloads.
- **Edge Rack:** to host NSX Edge appliance(s) and DLR Controller VMs to provide the north-south L3 routing feature, NSX L2 bridging, and host centralized logical or physical services (firewall, load balancing, etc.).

The Virtual Distributed Switch (VDS) is a building block for the overall NSX architecture. Although a design with a single VDS spanning all clusters (management, compute, and edge) is possible, we have proposed to have each cluster with its own Virtual Distributed Switch. This is not a requirement but is a design choice so NSX bits and infrastructure VLANs are only installed/configured on the hosts/clusters they need to be installed/configured on during the deployment process. There are several advantages in keeping a separate VDS for each cluster which go beyond the scope of this paper. However, there are different designs possible, such as having one VDS span across all clusters, or having one VDS for edge and compute clusters and another for the management cluster.

The design options for connecting ESXi hosts (i.e., the VDS uplinks connectivity) to the top of rack (ToR) switches in each rack/cluster is based on the dedicated uplinks for each type of traffic: VXLAN, vMotion, management, and storage.

The NSX bits have been installed into the compute and edge clusters and VXLAN has been enabled. However, the management cluster does not have the NSX bits installed or VXLAN enabled as it is not required. No logical network components (e.g., servers running in Web-Tier, App-Tier, and DB-Tier) need to connect to anything within the management cluster. If the management and edge clusters were on the same VDS, the transport VLAN would be automatically created on all management and edge hosts even though it is only needed on the compute and edge hosts. This is why we decided to have three separate VDS switches, one for each cluster.

Trend Micro Deep Security Manager and Deep Security Relay are deployed on the management cluster and Deep Security is deployed on each ESXi host of the compute cluster to provide Guest and Network Introspection Services to the VM. The Deep Security Virtual Appliance communicates with the Deep Security Manager and Deep Security Relay using the management network. The Deep Security Manager doesn't require any network connectivity to your virtual machines.

This reference architecture is depicted in the figure below:

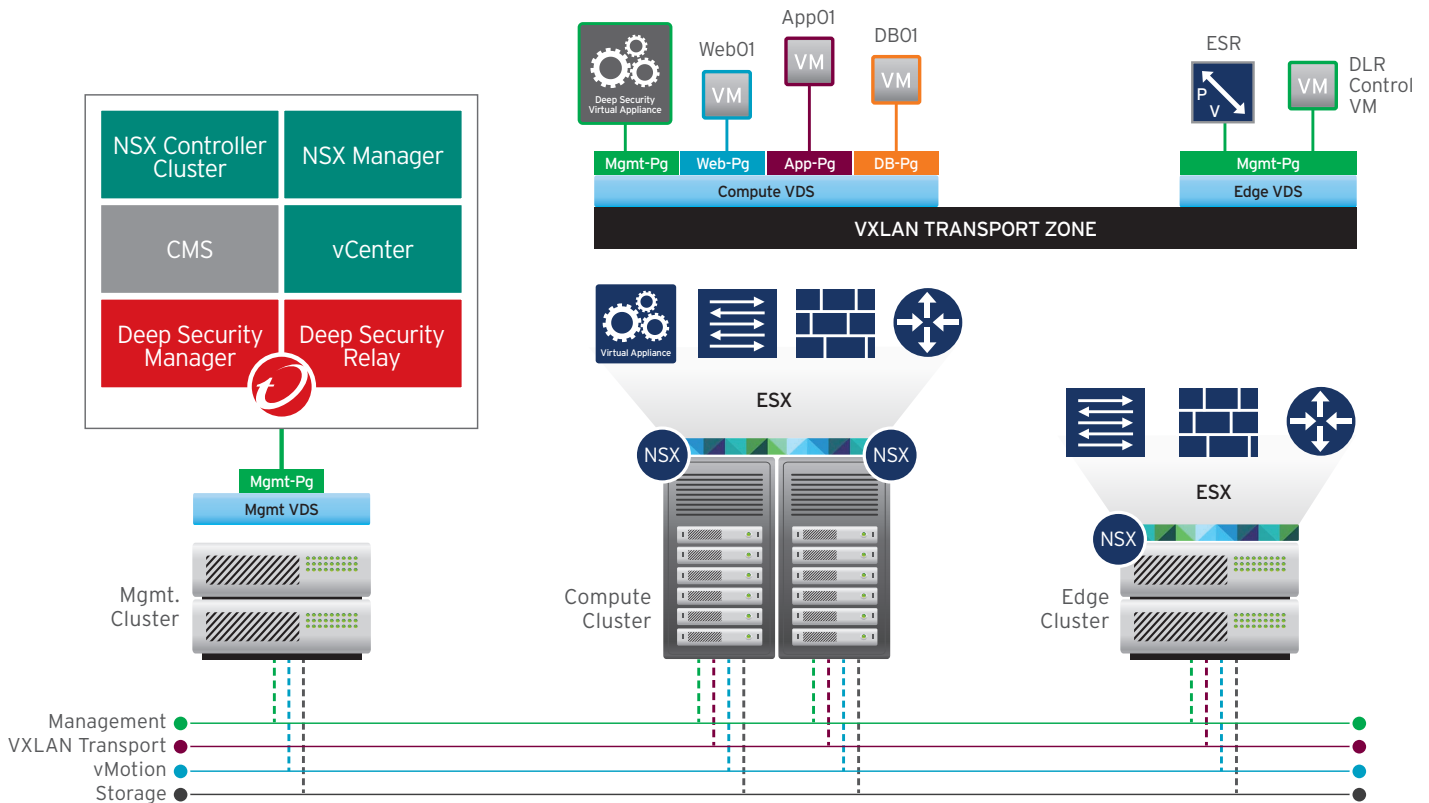


Figure 10: Reference Architecture for NSX with Trend Micro Deep Security

In Figure 11 below, we have also shown three logical switches to provide an example use case for micro-segmentation between the Web-Tier, App-Tier, and DB-Tier. These logical networks are interconnected through a Distributed Logical Router (DLR). IP addresses defined on a DLR are the default gateway for a VM connected to any of the Logical Switches. The DLR is connected to an Edge Services Gateway (ESG) that provides connectivity to the physical world. We have a total of three security groups (SGs) created in NSX Service Composer (one security group per tier). Grouping VMs into security groups based on server roles or functions is the foundation of implementing micro-segmentation. Once done, it is easy to implement traffic policy.

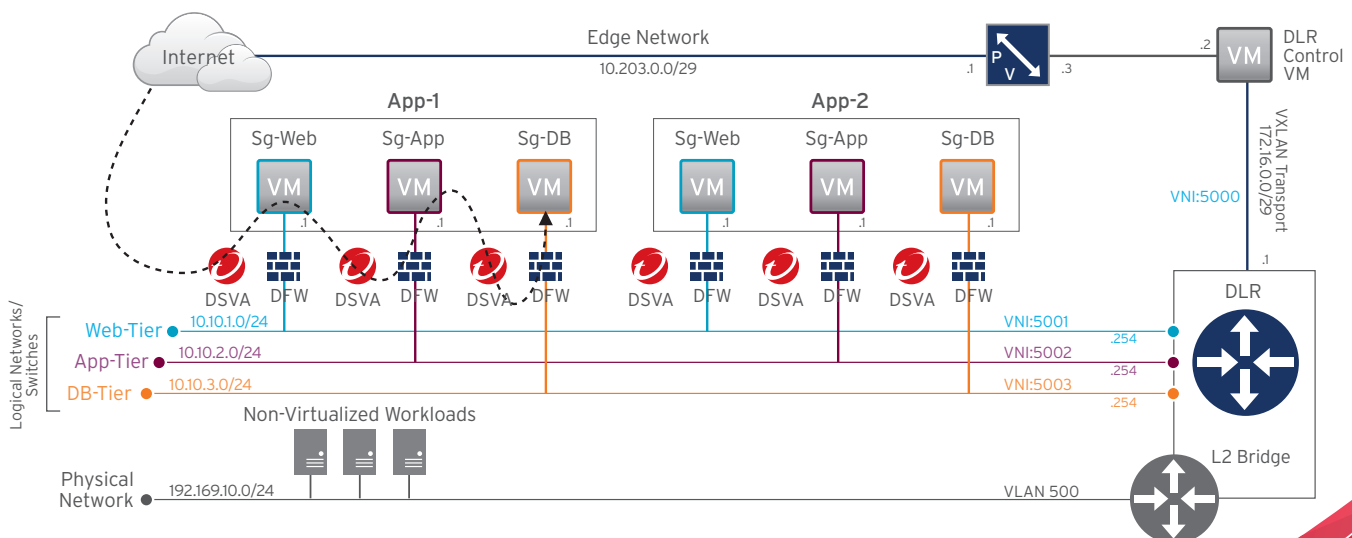


Figure 11: Micro-Segmentation and Traffic Steering To Trend Micro Deep Security

The logical view of our reference architecture shows network policy decisions we have taken. We have shown how firewall-rule policy is enforced using DFW and how to redirect traffic to Deep Security for advanced security services such as intrusion prevention and web reputation. Some of the key points of our sample network policy are:

- Traffic to web servers is allowed from anywhere on TCP ports 80 and 443 by the DFW. This allowed traffic is then redirected to Deep Security for further inspection before it can be sent to web servers.
- Traffic to servers in App-Tier is only allowed from the servers in Web-Tier on TCP ports 4120 by the DFW. This allowed traffic is then redirected to Deep Security for further inspection before it can be sent to application servers for further processing.
- Traffic to back-end database servers is only allowed from the servers in App-Tier on TCP ports 1443 by the DFW. This allowed traffic is then redirected to Deep Security for further inspection before it can be sent to database servers for further processing.

This network policy is not exhaustive but an example to show the flows that can be achieved to protect east-west traffic—which is not possible using perimeter security devices.

When inspecting traffic between these tiers, Deep Security will perform deep traffic analysis to ensure that only legitimate traffic that contains no threats (such as SQL injection, cross-site scripting, etc.) is allowed to hit your servers.

## Conclusion

VMware's software-defined data center (SDDC) architecture is extending virtualization technologies across the entire physical data center infrastructure. The VMware NSX network virtualization platform allows organizations to build next-generation infrastructures with reduced overall investment in implementation and operational activities. It overcomes current challenges of traditional networking by extending the virtualization capabilities of abstraction, pooling, and automation. Through policy-driven automation, NSX delivers a new operational model for networking that breaks through current physical network barriers and enables data center operators to achieve better speed and agility with reduced costs.

The VMware NSX and Trend Micro integrated solution complements and extends basic security services delivered by the NSX virtualization platform. The joint solution provides an integrated data center solution that allows organizations to automate the delivery of advanced security services from Trend Micro such as intrusion prevention, web reputation, anti-malware, and integrity monitoring to help achieve safe delivery of business-critical applications with complete threat protection.

## References

[VMware NSX Design Guide](#)

[VMware NSX Administrator's Guide](#)

[Trend Micro Deep Security and VMware NSX Solution Brief](#)

[Trend Micro Deep Security Installation Guide for NSX](#)

[Trend Micro Deep Security Administrators Guide](#)



· Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend  
· Micro provides individuals and organizations of all sizes with award-winning security software, hardware and  
· services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are  
· sold through corporate and value-added resellers and service providers worldwide. For additional information  
· and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

©2015 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.  
[WP01\_DS\_NSX\_Technical\_150610US]