Overview

Network virtualization helps you achieve better efficiencies, more rapid workload provisioning and increased workload security as you deploy cloud and software-defined data center strategies. VMware's portfolio of Network Virtualization and Security Services enables you to rapidly deploy, test, validate and learn VMware's network virtualization and security technologies purpose-built for your key use cases.

SERVICE BENEFITS:

- Plan, design, build and test network virtualization capabilities in any deployment environment
- Learn how to evolve and transform from your current operational capabilities to operating a virtualization networking environment that enables the NaaS vision
- Learn how to enable granular, dynamic control over security policies
- Deploy network virtualization utilizing best practices while ensuring IT and staffing readiness
- Provide centrally managed distributed security policies
- Rapidly deploy the full suite of Network Virtualization services including Logical Switching, Distributed Routing, Distributed Firewalling, Micro-Segmentation Security, VPN, NAT, plus more.

DIFFERENTIATORS:

- Expertise that encompasses the VMware solutions portfolio — NSX, vRealize Suite, Virtual SAN, vCloud Air, vSphere, End-user computing and more
- Structured engagement delivery approach, based on proven, repeatable, reliable methodologies
- Solutions validated against VMware best practices

EXPERTISE

- VMware Professional Services consultants are experts in implementing VMware's network virtualization and security technologies to build next generation Software-Defined Data Centers.
- Technology specialists have the deployment experience to identify and resolve common implementation and integration challenges.
- Unmatchable expertise in complex design and deployment integration with other VMware Software-Defined Data Center products, including vRealize Automation and vCenter Operations.
- Complex design and deployment integration with other market leading network services vendors that form part of the Network Virtualization eco-system including F5, Palo Alto Networks, Trend Micro, Symantec, EMC Smarts and more.
- Documentation and Consulting advice on:
  - Design components for key NSX features
  - Guidance on standard and complex NSX APIs
  - Firewall and Security design recommendations

OFFERINGS

- Micro-Segmentation and Security Accelerator
- Network Virtualization Accelerator
- Micro-Segmentation and Security Design and Deploy
- Network Virtualization Design and Deploy

METHODOLOGY

Phase 1: Planning
Phase 2: Kickoff
Phase 3: Solution Overview
Phase 4: Assess
Phase 5: Design
Phase 6: Deploy
Phase 7: Validate
Phase 8: Knowledge Transfer
Phase 9: Conclusion
OPERATIONS, PEOPLE, PROCESS

Understand the journey to the Network-as-a-Service operating model from both an operational and organizational standpoint. With Operations Transformation services you gain an understanding of the concepts of a new IT operating model and why network and security should be part of it. The Envisioning Workshop focuses on the role of NaaS in the IT-as-a-Service operating model, and how a NaaS model can help the customer achieve specific IT outcomes. The Discovery Workshop focuses on identifying key operational capabilities within three main areas: Proactive Operations Management, Network and Security Service Provisioning, and Security Operations. (Workshops applicable to Network Virtualization Design and Deploy Service only)

OUTCOMES

VMware Network Virtualization and Security Services deliver a functioning solution using VMware NSX™ for vSphere®, that expands the power of virtualization and automation to data center networking services. This service provides rapid deployment of virtual networking capabilities in a customer environment.

At the conclusion of the engagement, VMware consultants will provide the agreed deliverables. The resulting deployment from this engagement is an operational software-defined network environment at the customer site.

Key Outcomes

• Rapid Deployment Delivery - Achieve the business benefits of network virtualization faster.
• Better Security - Implement micro-segmentation / tenant segmentation and security with distributed firewall architecture
  - Automated security and network services that follow the workloads
  - Deliver centrally managed distributed security containers which significantly expand the security within the virtual data center
• Reduced OpEx
• Reduced CapEx
• Higher Availability

<table>
<thead>
<tr>
<th>SERVICE NAME</th>
<th>OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro-segmentation and Security Accelerator</td>
<td>Non-production implementation of micro-segmentation and security capability within a customer test environment.</td>
</tr>
<tr>
<td>Network Virtualization Accelerator</td>
<td>Rapid deployment of virtual networking capabilities in a limited, non-production environment suitable for deploying development / test and non-production workloads on a limited scale.</td>
</tr>
<tr>
<td>Micro-segmentation and Security Design and Deploy</td>
<td>Production architecture and implementation of micro-segmentation and security capability within a production environment.</td>
</tr>
<tr>
<td>Network Virtualization Design and Deploy</td>
<td>Delivers a functioning solution using VMware NSX™ for vSphere®, that expands the power of virtualization and automation to data center networking services within a customer’s production environment by leveraging a phased methodology.</td>
</tr>
</tbody>
</table>
SERVICES PORTFOLIO

The VMware Network Virtualization and Security services portfolio includes the choice of four (4) offerings:

1. Micro-Segmentation and Security Accelerator (Non-Production)
   Key Activities:
   • Planning and solution design workshop that identifies technical requirements
   • Deploy components in a prescriptive design
   • Demonstration of traffic blocking/passing for a sample three-tier application
   • Knowledge transfer on the implemented solution

2. Network Virtualization Accelerator (Non-Production)
   Key Activities:
   • Planning and solution design workshop that identifies use cases and technical requirements
   • Deploy components in a non-production environment
   • Validate solution against use cases
   • Conduct a knowledge transfer session

3. Micro-Segmentation Design and Deploy (pre-production/production)
   Key Activities:
   • Adapt existing security and firewall policies to provide dynamic control over guest network communication profiles.
   • Firewall rule optimization and strategy
   • Configuration of logging and monitoring
   • Knowledge transfer around enablement of security automation via NSX service composer

4. Network Virtualization Design and Deploy (pre-production/production)
   Key Activities:
   • Review capabilities of NSX for vSphere, gap analysis, use case selection
   • Conduct Architecture Design and Network-as-a-Service Transformation Workshops
   • Create test and deployment plans
   • Install, configure, and validate solution according to the design
   • Deliver knowledge transfer session

For more information about VMware Professional Services visit: [www.vmware.com/services](http://www.vmware.com/services)