Securing VMware® NSX

OCTOBER 2018

vmware®

Table of Contents

Executive Summary

The VMware NSX network virtualization platform is a critical pillar of VMware's Software Defined Data Center (SDDC) architecture. NSX network virtualization delivers for networking what VMware has already delivered for compute and storage. In much the same way that server virtualization allows operators to programmatically create, snapshot, delete and restore software-based virtual machines (VMs) on demand, NSX enables virtual networks to be created, saved and deleted and restored on demand without requiring any reconfiguration of the physical network. The result fundamentally transforms the data center network operational model, reduces network provisioning time from days or weeks to minutes and dramatically simplifies network operations.

Due to the critical role NSX plays within an organization, configuration of the product along with secure topology will reduce the risk an organization may face. This document is intended to provide configuration information and topology recommendations to ensure a more secure deployment.

vmware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

NSX Traffic [Control, Management, and Data]

The main components of NSX include the NSX Manager, NSX Edge/Gateway, NSX Controllers, and NSX vSwitch. Great care must be given toward the placement and connectivity of these components within an organization's network. NSX functions can be grouped into three categories: management plane, control plane, and data plane.

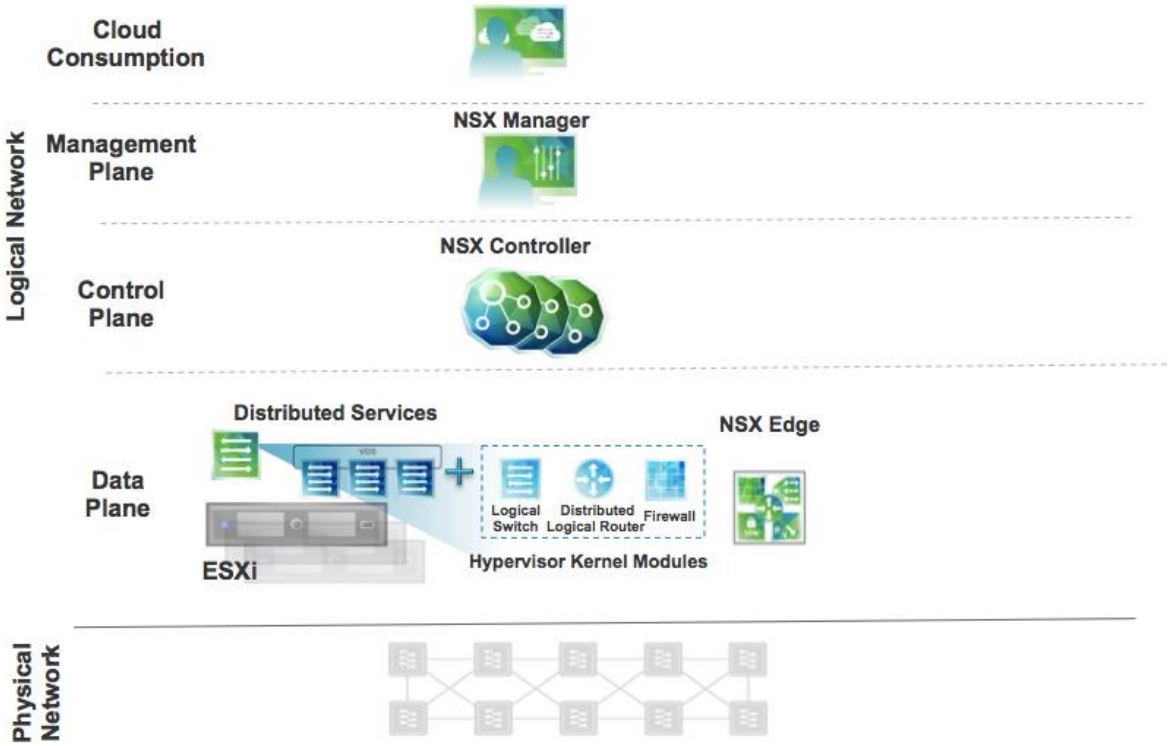

Figure 1 - VMware Network Virtualization Solution Components

.

Consumption Platform

The consumption of NSX can be driven directly via the NSX manager UI. In a vSphere environment, this is available via the vSphere web interface. Typically end-users tie in network virtualization to their cloud management platform for deploying applications. NSX provides a rich set of integration into virtually any CMP via the REST API. Out of the box integration is also available through VMware's vRealize Automation product.

Management Plane

The NSX management plane is built by the NSX Manager. The NSX manager provides the single point of configuration and the REST API entry-points in a vSphere environment for NSX. The NSX Manager is also the integration point with vCenter.

Network traffic to and from the NSX Manager should be restricted and it's recommended that it be placed on a management network where access is limited. Access to the NSX manager utilizes a web redirect to only allow access via HTTPS. Traffic from the NSX manager to other components such as vCenter and the ESXi is encrypted. These safe guards reduce some of the risk to the NSX manager, but it is recommended that it be separated from other traffic via physical or VLAN separation, at a minimum. The VMware vSphere Security Configuration Guides (http://www.vmware.com/security/hardening-guides.html) can be used to further explore protection of the management network.

Control Plane

The NSX Controller is the heart of the control plane. In a vSphere-optimized environment where VMware's virtual distributed switches (VDS) are deployed on ESXi nodes, the controllers enable network virtualization such as logical distributed routing and logical distributed switching of networking traffic within and across hypervisors.

In all cases, the controller is purely a part of the control plane and does not have any data plane traffic passing through it. The controller nodes are also deployed in a cluster of odd members in order to enable high-availability and scale. Any failure of the controller nodes does not impact any existing data plane traffic.

These communications does not carry any sensitive application data, but it is required for NSX to work properly. As of version 6.3.0 of NSX, controller to controller communication is encrypted, along with hypervisor to controller communication. Additionally, as of vSphere 6.5 version, vMotion traffic can also be encrypted, if enabled, thus providing an additional layer of security. It's recommended that management network be separated from other traffic via physical or VLAN separation, at a minimum. No user machines should be on this network.

Data Plane

The NSX Data plane consists of the NSX vSwitch. The vSwitch in NSX for vSphere is based on the vSphere Distributed Switch (VDS) with additional components to enable rich services. The add-on NSX components include kernel modules (VIBs)

which run within the hypervisor kernel providing services such as distributed routing, distributed firewall and enable VXLAN tunneling capabilities.

The NSX vSwitch (VDS) abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that is independent of physical constructs such as VLAN. Some of the benefits of the VDS are:

- Support for overlay networking leveraging VXLAN and centralized network configuration. Overlay networking enables the following capabilities:
  - Creation of a flexible logical layer 2 (L2) overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks
  - Provisioning of communications (east–west and north–south) while maintaining isolation between tenants
  - Application workloads and virtual machines that are agnostic of the overlay network and operate as if they were connected to a physical L2 network
- NSX vSwitch facilitates massive scale of hypervisors.
- Multiple features—such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP—provide a comprehensive toolkit for traffic management, monitoring and troubleshooting within a virtual network.

Additionally, the data plane also consists of gateway devices that can either provide L2 bridging from the logical networking space (VXLAN) to the physical network (VLAN), or be utilized as an edge network gateway device providing perimeter firewall, load balancing and other services such as SSL VPN, DHCP, etc.

The dataplane (VXLAN) traffic is not encrypted by NSX. For tenant application level data security, it is recommended to secure traffic at the application layer.

NSX Manager:

Topology and the NSX Manager Virtual Machine

The NSX Manager virtual machine (VM) is part of the management plane, certain considerations must be taken into account when deciding where to install and connect the VM.

1. **Placement**: Best practices dictate that the NSX Manager should be placed in a segmented and secured network. Since the NSX manager and vCenter are in continuous communication, it is recommended they be placed on the same network. Typically, the

NSX manager and vCenter are placed on a management network where access is limited to specific users and/or systems. The management network should not contain any user or general network traffic.

2. **Physical and network security:** The following table provide ports used in communications with and between the NSX Manager, as well as vCenter and the ESXi hosts. If you are securing the NSX manager from other network services, make sure the appropriate ports are open.

Table 1. NSX for vSphere Port & Protocol Requirements

Source	Target	Port(s)	Protocol	TLS
Client	NSX Manager Admin Interface	443	TCP	Yes
Client	NSX Manager REST API	443	TCP	Yes
Client	NSX Manager SSH	22	TCP	Yes
NSX Manager	ESXi hosts	80	TCP	No
vCenter	ESXi hosts	80	TCP	No
vCenter	NSX Manage	80	TCP	No
ESXi hosts	vCenter	80	TCP	No
NSX Manager	vCenter Server	443, 902	TCP	Yes
NSX Manager	ESXi hosts	443, 902	TCP	Yes
ESXi hosts	ESXi hosts	6999	UDP	Yes
ESXi hosts	NSX Manager	8301, 8302	UDP	Yes
NSX Manager	ESXi hosts	8301, 8302	UDP	Yes
ESXi hosts	NSX Controller	1234	TCP	Yes
NSX Controller	NSX Controller	2878, 2888, 3888, 7777, 30865	TCP	Yes
NSX Manager	NSX Controller	443	TCP	Yes
ESXi	NSX Manager	5671	TCP	Yes
NSX Manager	DNS Server	53	TCP & UDP	No
NSX Manager, NSX Controller	NTP Server	123	TCP & UDP	Yes

Source	Target	Port(s)	Protocol	TLS
NSX Manager	Syslog	514	UDP or TCP	Yes
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	4789	UDP	Yes

3. **Access and login**: Login to the NSX Manager can be either through SSH or HTTPS web access. During the NSX Manager installation, user may choose to enable SSH., otherwise SSH is disabled by default. SSH access can be enabled or disabled through the NSX Manager. Access through the web management provides the general confirmation and management needs. The configuration and setup can be found in the NSX install guide.

   The SSH console access provides more detailed information through its menu driven interface. These include running the setup process to set the NSX Manager IP settings. Terminal configuration such as banner to display, resetting the enable password and adding users can also be performed within the SSH console.

   The NSX Manager virtual application appliance is a purpose built Linux based VM. Access to the VM is limited to SSH (if enabled) or console access. Access via console or ssh should only be enabled when required for troubleshooting.

Configuration through NSX Manager

1. **NTP**
   NTP is needed for many functions within NSX and VMware. If SSO is leveraged with NSX, time synch is crucial for the product to work correctly. It is critical that all systems within the VMware infrastructure have their time synched.
2. **Syslog**
   Within the NSX Manager, the syslog server for the management of the NSX manager can be specified. This address will be used to forward on all NSX management logs. Logging for other components will be enabled either through the vCenter client or RESTApi calls. Please refer to the NSX Admin Guide for more details.
3. **SSH**
   During the NSX Manager installation, user may choose to enable SSH., otherwise SSH is disabled by default. SSH can be enabled or disabled via the NSX Web UI. Disabling SSH is recommended. If console/SSH access is required for troubleshooting with tech support, one can then enable the ssh access and disable the service once troubleshooting has been completed.
4. **SSL Certificates**
   The certificate used to manage the NSX Manager Web UI can be either by self-signed (default) or signed. If an organization has an existing PKI infrastructure, it is recommended that they use their CA for the NSX Manager UI manager certificate.

   When generating a Certificate Signing Request (CSR), the only algorithm to choose is

RSA. Key sizes can be either 2048 or 3072.

5. **Login Password**
   In order to login to NSX Manager Web Interface, the user needs to use the 'password' created at the time of installation. It is recommended to frequently change the login password based on the company's IT policies.

6. **Backup**
   In order to recover from a system disaster and unauthorized changed to the NSX Manager, scheduled backups of the NSX manager are recommended. Target system IP address and port are configured for the backups, which are sent via FTP and SFTP. Select SFTP to encrypt the backup traffic, selecting FTP doesn't encrypt the traffic. Automatic backups scheduling is available with frequency options of weekly, daily and hourly. Please note that the backup information is not encrypted, and hence should be placed on a secure and encrypted location. Information that is encrypted on the NSX manager already will remain encrypted during backup. The FTP/SFTP user credentials used for backups are stored on NSX manager appliance database and it is encrypted.

Configuration through vSphere Web Client and vCenter

The below settings are used to make management settings to the NSX Manager but are configured through the vSphere web client.

1. **System event severity settings**
   - Within the NSX Manager settings, you can change the default severity levels of events that may be generated by NSX. Depending on your change management and operational model, you may want to change some of the settings up or down.
2. **Users and Roles**
   - The following roles are defined within the NSX Manager. Assigning the appropriate roles to your users will reduce your risk of inappropriate access and possible unauthorized change.

Role	Permissions
Enterprise Administrator	NSX operations and security
NSX Administrator	NSX operations only: for example, install virtual appliances, configure port groups.
Security Administrator	NSX security only: for example, define data security policies, create port groups, create reports for NSX modules.
Auditor	Read only.

   - Users may be added to the above roles as specific vCenter users or vCenter groups. These users and groups maybe AD user/groups or local users/groups.

- Users and groups may also be limited to a specific Scope. This allows for the segmentation and RBAC that may be needed in a highly secure or segmented organization. Scope access can be defined as a port group, datacenter, or NSX Edge device. Scope can only be used for the Security Administrator and Auditor role

NSX Controllers:

Since the NSX controllers VMs are part of the control plane, certain considerations must be taken into account when deciding where to install and connect the VMs. Users should not have access to the NSX controllers and the network they reside on unless it's required for troubleshooting purposes.

1. **Placement:** Typically, the NSX Controllers are placed on a management network where access is limited to specific users and/or systems. The management network should not contain any user or general network traffic. The controllers need to communicate with each other as well as the VM hosts.

2. **Physical and network security:** If you are securing the NSX Controllers from other network services, make sure the appropriate ports are open. Refer to Table 1 above to identify the ports that are used for communication to and from NSX Controllers.

3. **Access and login**: Login to the NSX Controllers can be achieved through console or SSH access, if enabled. The password for the controllers is set during the installation process through the vSphere web client.

   The SSH console access provides controller specific commands that may be needed for troubleshooting. In the console, type 'help' and all commands available are displayed. Access through SSH should be limited or disabled due to the commands that may be executed on the controller. These commands include the shutting down or restarting of a controller.

   Commands that can be executed on the NSX Controllers are pre-parsed before passing to binary in a string. Along those lines, all installation packages are signed and verified before they can be installed. These built in controls help secure the NSX Controllers from unauthorized package installation and compromise.

4. Controller OS: Starting 6.3.3, Controller base operating system is moved from Ubuntu 12.04 to Photon OS 1.0.

5. Controller Clustering VPN: The NSX Controller uses IPsec VPN to connect Controller clusters starting NSX 6.3.0 release. NSX controllers use following Crypto module for IPsec VPN based on NSX release.

   a. Prior to NSX 6.3.3, StrongSwan for IKE functionality (the key management part of IPSec), which in turn uses OpenSSL for the actual cryptography.

b. Starting 6.3.3, uses the VMware Linux Kernel Crypto Module (LKCM) (Photon OS 1.0 environment). FIPS certification Pending.

NSX Edge Gateway:

The NSX Edge Gateway (EG) resides within the data plane of the NSX solution. An EG can be best described as a virtual appliance which provides North-South traffic management and features. The EG can provide the following functions; firewall, load balancer, SSL VPN, IPSec VPN, SNAT/DNAT, and routing.

1. **Placement:** The EG is typically placed at the network border to handle North/South traffic. Since the EG may be connected to external networks that are not protected, care should be taken to create a "defense in depth" architecture.

2. **Physical and network security:** As discussed earlier in this paper, care should be taken to segment management and data traffic. SSH may be used to connect to an EG, if enabled, firewall and other network controls should be used to limit access.

3. **Access and login:** Login to the NSX Edge Gateway can be achieved through GUI or SSH access, if enabled. The password for the SSH access can be set during install or after leveraging the "Change CLI Credential" options from within the EG GUI. A firewall rule must be created to allow SSH to a specific interface.

   The SSH console provides a limited set of commands that can be run on an EG device. These commands include a list of show and debug commands. Please see the NSX Administrator guide for more information.

Edge Certificates

Depending on what features are enabled on the Edge Gateway(EG), there are a variety of certificates and cipher suites that can be leveraged. Below is a table to provide a listing of supported ciphers. By default, the EG will leverage a self-signed certificate if a commercial or organization certificate is not provided.

- The Edge IPSec VPN uses following software stack and crypto module based on NSX release:

  - Prior to NSX 6.3.3, OpenSwan for IKE functionality (the key management part of IPSec), which in turn uses Mozilla NSS for the actual cryptography. The IPSec bulk packet encryption and decryption is handled by the Linux OS (NSX Edge 3.14 OS) crypto routines, and includes AES and 3DES for static IPSec tunneling with 128 or 256 bit key lengths

  - In NSX 6.3.3, NSX 6.3.3 moved to a newer version of Mozilla NSS that has not been FIPS certified. VMware affirms that the module works correctly, but it is no longer formally validated.

- In NSX 6.4, StrongSwan for IKE functionality (the key management part of IPSec), and uses OpenSSL Crypto Module for the actual cryptography. The IPSec bulk packet encryption and decryption is handled by the Linux OS (NSX OS 4.4) crypto routines, and includes AES and 3DES for static IPSec tunneling with 128 or 256 bit key lengths. These modules are FIPS certified.

- Edge SSLVPN (TLS based) service which has two components – gateway and clients.
  - Gateway service runs on edge and uses openssl for encryption (openssl is ported in kernel by VMware). Encryption algorithms supported are: AES, RSA.
  - Client component uses openssl library – same protocol support, except on the Macintosh -- where Apple CryptoCore is used

- Edge L2VPN (TLS based) uses OpenSSL for encryption (openssl is ported in kernel by VMware). Encryption algorithms supported are: AES, RSA.

Supported cipher suites for Load Balancer, SSL VPN, and IPSec VPN services:

Load Balancer	**SSLVPN:**
ECDH-ECDSA-AES256-SHA	AES128-SHA
ECDH-RSA-AES256-SHA	AES256-SHA
AES256-SHA	AES128-GCM-SHA256
DES-CBC3-SHA	ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA	ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-SHA	**IPSec VPN**
AES128-SHA	**IKE (uses OpenSwan or StrongSwan, starting NSX 6.4)**
ECDHE-RSA-AES256-GCM-SHA384	RSA 1024bits, 2048bits, 4096bits
ECDHE-RSA-AES128-GCM-SHA256	Key exchange: DH with group 2 (1024bits) and group 5(1536)
	Encryption and Hash: AES128-CBC-SHA, AES256-CBC-SHA

NSX Certificates and their usage:

NSX and the NSX Manager leverages certificates in multiple places within the solution. As pointed out earlier, users may use their own CA to cert certificates for the NSX manager to leverage for user management communication, i.e. browser access to the NSX Manager. NSX uses self-signed certificates, managed by the NSX Manager, to create trusted communication between itself and the NSX controllers and kernel level modules such as the distributed firewall (DFW).

The NSX Manager uses a Java Keystore to store the certificates it has provisioned. Other NSX components, such as the NSX controllers leverage encrypted and password protected PEM files to store their certificates.

NSX Logs and Alerting:

NSX logs can be found in a variety of locations depending on the component that is generating the logs. To ensure a more secure environment, VMware recommends sending all NSX logs to log collector by configuring the syslog settings on NSX, ESXi hosts, and vCenter. More information about log and log formats can be found in the NSX Administration guide.

3rd Party Hardware / Software products for NSX Cryptographic Functionality:

NSX uses the following cryptographic modules when in FIPS mode:

In NSX 6.4.0 Release:

- OpenSSL 1.0.2n (VMware OpenSSL FIPS Object Module 2.9), BouncyCastle FIPS 1.0.0, Linux Kernel v4.4 (NSX OS 4.4), Apple OS X CoreCrypto Module v5.0

Prior to NSX 6.4.0 Release:

- OpenSSL 1.0.2(p to l), BouncyCastle FIPS 1.0.0, Mozilla NSS 3.23 (VMware NSS Cryptographic Module 3.23), Linux Kernel (v3.13 and 3.14), Apple OS X CoreCrypto Module v5.0

Different version of OpenSSL version were used prior to 6.4.0 release. Latest version in NSX 6.2 SW release train is 6.2.9, which uses 1.0.2j. Similarly, latest version in NSX 6.3 SW release train is 6.3.5 which uses OpenSSL version 1.0.2l.

VIX communication uses older version of OpenSSL so it is not allowed when FIPS mode is enabled.

OpenSSL, Mozilla NSS, and Linux crypto routines are configured to use Intel AES-NI when it is available. AES-NI is an extended set of functionality available on certain Intel and AMD processors, which allows offloading some cryptographic operations from software to the processor.

All crypto, except Apple CoreCrypto are open-source components, primarily maintained by non- profit foundations. Although VMware has support agreements, commercial licenses are not required in order to use these components.