Securing VMware® NSX-T

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

NSX-T Traffic [Control, Management, and Data]

The main components of NSX-T includes the NSX Manager, NSX Controllers, NSX Edge, and N-VDS (NSX Virtual Distributed Switch). 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.

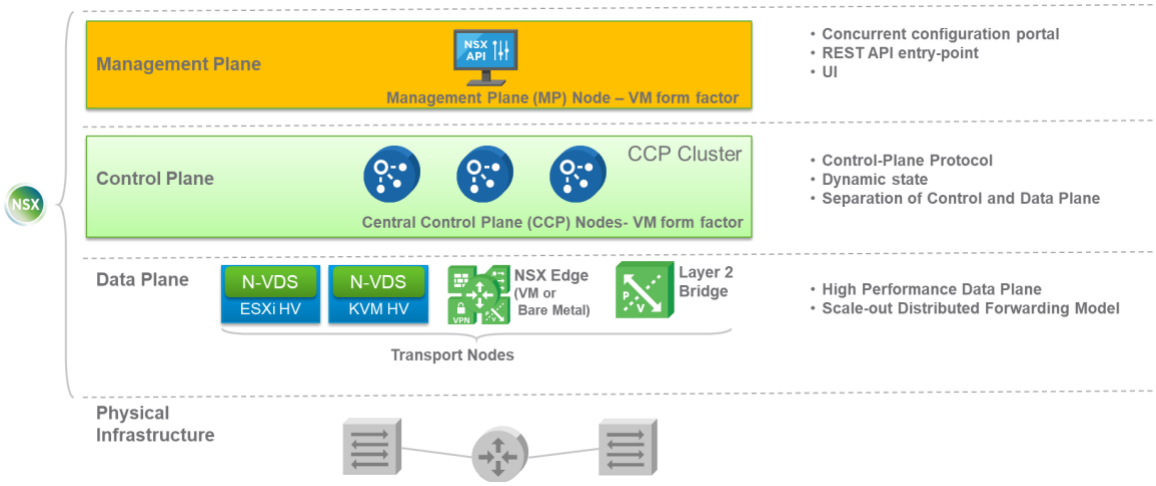


Figure 1 - NSX-T Architecture and Components

.

Consumption Platform

The consumption of NSX-T can be driven directly via the NSX manager UI. 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.

Management Plane

The NSX-T management plane is built by the NSX Manager. The NSX Manager provides the single point of configuration and the REST API entry-points. NSX Manager is delivered in a virtual machine form factor.

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 NSX-T components such as controllers, Edge, Transport Nodes (ESXi and KVM) & vCenter 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 control plane computes the runtime state of the system based on configuration from the management plane. It is also responsible for disseminating topology information reported by the data plane elements and pushing stateless configuration to forwarding engines.

NSX-T splits the control plane into two parts:

- **Central Control Plane (CCP)** – The CCP is implemented as a cluster of virtual machines called CCP nodes. The cluster form factor provides both redundancy and scalability of resources. The CCP is logically separated from all data plane traffic, meaning any failure in the control plane does not affect existing data plane operations. User traffic does not pass through the CCP Cluster.
- **Local Control Plane (LCP)** – The LCP runs on transport nodes. It is adjacent to the data plane it controls and is connected to the CCP. The LCP is responsible for programing the forwarding entries of the data plane.

The NSX Controller is the heart of the control plane. 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 3 members in order to enable high-availability and scale. Any failure of the controller nodes does not impact any existing data plane traffic.

NSX Controller to controller communication is encrypted, along with hypervisor to controller & controller to NSX Manager communication. 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-T Data plane is implemenated on transport nodes. The transport nodes are the hosts running the local control plane (LCP) daemons and NSX Virtual Distributed Switch (N-VDS) with additional components to enable rich services. The add-on components include kernel modules (VIBs) which run within the hypervisor kernel providing services such as distributed routing, distributed firewall and enable GENEVE tunneling capabilities. NSX-T currently supports hosts with VMware ESXi™ and KVM hypervisors to be transport nodes.

N-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. Some of the benefits of the N-VDS are:

- Support for overlay networking leveraging GENEVE 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

Additionally, the data plane also consists of Edge nodes which are service appliances dedicated to running network services that cannot be distributed to the hypervisors such as Edge FW, NAT, VPN, DHCP,LB etc.. They are grouped in one or several clusters, representing a pool of capacity. Edge can also be used to provide L2 bridging from the logical networking space (GENEVE) to the physical network (VLAN).

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

NSX-T Protocol & Port Requirements

Different NSX-T components communicate with each other to provide scalable distributed network & security services platform. Here are set of TCP/UDP ports used which might need to be opened if NSX-T compnets are secured behind the Firewall to meet company security policy requirements. Additional details available on NSX-T installation guide.

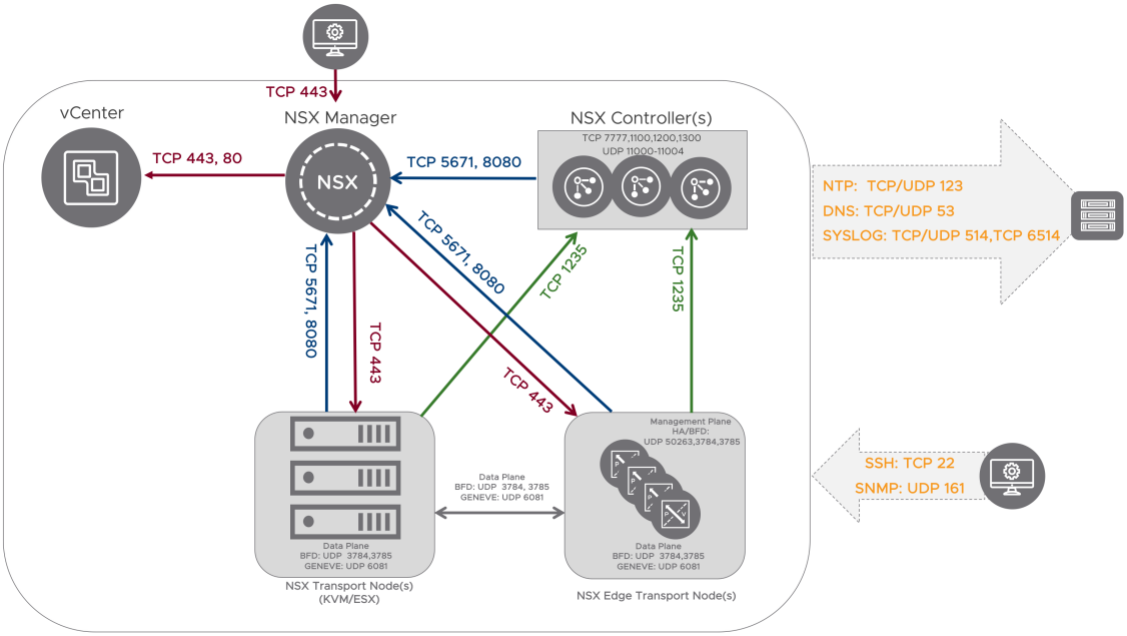
Table 1. NSX-T Port & Protocol Requirements

Source	Target	Port(s)	Protocol	TLS
Client	NSX Manager Admin Interface	443	TCP	TLS 1.2
REST Client	NSX Manager REST API	443	TCP	TLS 1.2
Client	NSX Manager SSH	22	TCP	SSH v2

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

Source	Target	Port(s)	Protocol	TLS
NSX Manager	ESXi hosts/KVM Hosts	443	TCP	TLS 1.2
NSX Manager	vCenter Server	443, 80	TCP	TLS 1.2
Controller/ESXi hosts/KVM Hosts/Edge	NSX Manager	5671	TCP	TLS 1.2
Controller/ESXi hosts/KVM Hosts/Edge	NSX Manager	8080	TCP	TLS 1.2
ESXi hosts/KVM Hosts/Edge	NSX Controller	1235	TCP	TLS 1.2
NSX Controller	NSX Controller	1100,1200,1300,7777	TCP	TLS 1.2
NSX Controller	NSX Controller	11000-11004	UDP	No
NSX Manager, NSX Controller, Transport Node, Edge	DNS Server	53	TCP & UDP	No
NSX Manager, NSX Controller, Transport Node, Edge	NTP Server	123	UDP	No
NSX Manager, NSX Controller, Transport Node, Edge	Syslog	514	UDP & TCP	Yes
NSX Manager, NSX Controller, Transport Node, Edge	SNMP	161, 162	UDP & TCP	No
Edge	Edge	50263,3784,3785	UDP	No
GENEVE Termination End Point(TEP)	GENEVE Termination End Point(TEP)	6081	UDP	No
Transport-Nodes	Transport-Nodes	3784,3785	UDP	No

Following diagram pictorially represents the communication ports used by NSX-T components as in the table above.



NSX Manager:

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, Physical and network security:** : Best practices dictate that the NSX Manager should be placed in a segmented and secured network. Typically, the NSX Manager, Controllers, Transport Nodes 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. The NSX manager need to communicate with NSX-T Nodes and Controllers. You can also provide additional isolation by having NSX manager, Controllers, Edge & Transport Nodes in separate management VLANS and have FW/Access-list policy on management gateway device. If you are securing the NSX-T components 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-T components.

2. **Access and login**: Login to the NSX Manager can be either through SSH or HTTPS web access or REST API. NSX-T uses only TLS1.2 for all communication both user interaction and also for internal communication between other NSX components. User can perform day-to-day operation for configurating, monitoring & troubleshooting using WEB UI or REST API. SSH access to NSX Manger should only be enabled when required for troubleshooting. SSH is disabled by default, during the NSX Manager installation, user may choose to enable SSH. After installation, SSH access can be enabled or disabled through the NSX Manager console. Admin can configure inactive timeout for both CLI &

UI sessions using command line interface. More info in the NSX-T administrative guide. SSH access is allowed only to local user.

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-T management logs.
   NSX-T allows to filter which log messages are sent to the logging server, based on the severity, facility or Message ID. Depending on your change management and operational model, you may want to change these settings. Please refer to the NSX-T 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-T VM console. Disabling SSH is recommended. If 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. NSX allow only SSHv2.
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. **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. Manging role assignments to users or user groups needs VMware Identity Manager integration with NSX-T. Please refer to the NSX-T Admin Guide for more details.

Role	Permissions
Enterprise Administrator	Full access, NSX-T operations, Networking, Load Balancer and security
Auditor	Read only.
Network Engineer	Full Access, NSX-T Networking. Read-only/Execute, for other related NSX-T Operations

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

Role	Permissions
Network Operations	Full Access, NSX-T Networking. Selective Read-only/Execute, for other related NSX-T Operations
Security Engineer	Full Access, NSX-T Security. Read-only/Execute, for other related NSX-T Operations
Security Operations	Read-only, NSX-T Security. Selective Read-only, for other related NSX-T Operations
Load Balancer Administrator	Full Access, NSX-T Load Balancer. Selective Read-only/Execute, for other related NSX-T Operations
Load Balancer Auditor	Read-Only, NSX-T Load Balancer. Selective Read-only, for other related NSX-T Operations

7. **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 SFTP. 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.

NSX Controllers:

Since the NSX Controller 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, Physical and network security:** 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 NSX-T Nodes and Manager. You can also provide additional isolation by having NSX manager, Controllers, Edge & Transport Nodes in separate management VLANS and have FW/Access-list policy on management gateway device. 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-T components.

2. **Access and login**: Login to the NSX Controllers can be achieved through console or SSH access, if enabled. NSX allow only SSHv2. The password for the controllers is set during the installation process.

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

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.

3. **Controller Clustering VPN:** The NSX-T uses OpenVPN (TLS based) for securing controller cluster communications. OpenVPN uses OpenSSL libraries for secure communication.

NSX Edge:

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

1. **Placement:** The Edge is typically placed at the network border to handle North/South traffic. Since the Edge 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 Edge, if enabled, firewall and other network controls should be used to limit access.

3. **Access and login:** Login to the Edge can be achieved through console or SSH access, if enabled. The password for the SSH access can be set during install or after leveraging the console/SSH access. A firewall rule must be created to allow SSH to a Edge management interface.. NSX allow only SSHv2.

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

Edge Certificates & Cipher Suites

Depending on what features are enabled on the Edge, 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 Edge will leverage a self-signed certificate if a commercial or organization certificate is not provided.

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

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

Load Balancer
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
IPSec VPN
Pre Shared Key for authentication
Key exchange: DH with group 14 (2048bits), group 15 (3072 bits), group 16 (4096bits).
Encryption & Digest Algorithm • AES (128,256) • AES GCM (128,256) • SHA1 • SHA2-256

NSX-T Certificates and their usage:

NSX-T and the NSX Manager leverages certificates in multiple places within the solution. NSX-T 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). For user management communication, NSX-T uses self signed certificate by default. However, users may use their own CA to manage NSX Manager certificate for for user management communication, i.e. browser access to the NSX Manager.

The NSX Manager uses a Java Keystore to store the certificates it has provisioned. The Java Key Store uses PBEWithMD5AndTripleDES to encrypt the keys. The key are also stored in internal Corfu database. The database access is protected. The keys are not directly accessible to users or clients. Keys stored in Corfu DB are only accessible through a hidden private API, only available to processes that run on the appliance.

Other NSX-T components, such as the NSX controllers leverage encrypted and password protected PEM files to store their certificates.

NSX-T Logs and Alerting:

NSX-T logs can be found in a variety of locations depending on the component that is generating the logs. NSX-T uses standard RFC5424 format for logging. Logs are stored in different partition on the appliance than the base OS. Logs are accessible to only previlaged local user from the CLI. NSX-T appliance also logs system/OS level service initialization log update like SSH, Syslog service. NSX-T storage has log rotation policy based on the size of the log files. So VMware recommends sending all NSX-T logs to centralized log collector by configuring the syslog settings on NSX Manager, Transport Nodes and Edge. More information about log and log formats can be found in the NSX-T Administration guide.