# Securing VMware® NSX-T Data Center

MAR 2021
VERSION 1.1

vmware®

## Table of Contents



## *Executive Summary*

The VMware NSX Data Center network virtualization platform is a critical pillar of VMware's Software Defined Data Center (SDDC) architecture. NSX Data Center 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 Data Center 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 Data Center 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 Datacenter Architecture*

The main components of NSX-T Data Center includes the NSX Manager, NSX Edge, and N-VDS (NSX Virtual Distributed Switch) or VDS 7.0 (vSphere Distributed Switch), which makes data plane. 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. NSX-T Manager cluster provides both the management and control plane functionality.

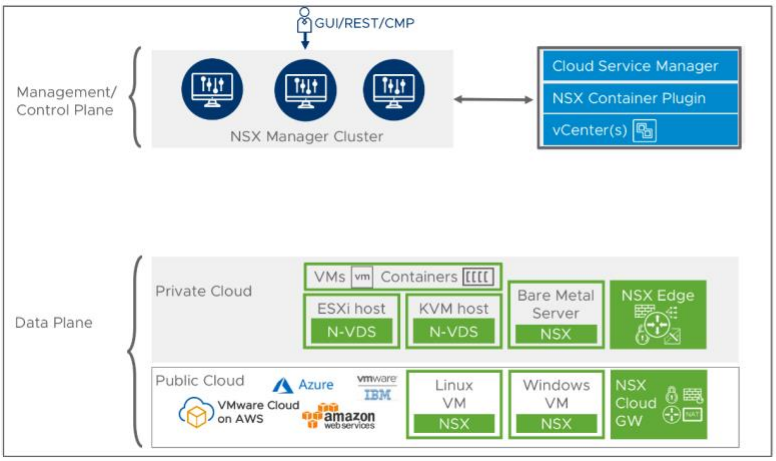


**Figure 1 - NSX-T Architecture and Components**

## Management Plane

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

The NSX-T management plane is built by the three node NSX Manager Cluster for redundancy and high avaiablilty. User can access the NSX management plane directly using individual IP's of the NSX manager or can configure Cluster Virtual IP to provides the single point of configuration and the REST API entry-points, while providing high avaiality at NSX management plane. NSX Manager is delivered in a virtual machine form factor with different flavor (Small, Medium, Large) for different scale requirements.

Access to the NSX Manager utilizes a web redirect to only allow access via HTTPS with TLS 1.1/1.2, with an option to set TLS version only to TLS 1.2.

NSX Manager provides management plane protection for deniel of service attack by having API rate limiting to limit the number of transactions per second and concurrent transactions to the NSX REST API. This protects the system from being impacted when one or more API clients make API requests at a rate the API cannot process. The API rate/concurrency limit configuration can be changed by user from the command line.

## 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 also implemented on NSX manager cluster as a separate service. 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.

NSX-T Manager cluster provides both the management and control plane functionality. The NSX Manager is the heart of the control plane. In all cases, the NSX manager is purely a part of the control plane and does not have any data plane traffic passing through it. Any failure of the manager nodes does not impact any existing data plane traffic.

Architecturally NSX Manager appliance has multiple independent services: like Manager, Controller, Database and other; to provide robust management and control plane fuctionality within same appliance. These services are protected from each other by having service level resource (CPU & Memory) isolation. Each of the services has its own dedicated memory & CPU, so having one service overwhelmed does't impact other services in the appliance.

NSX Manager to Manager communication is encrypted, along with communication between NSX manager and other NSX-T components Edge, Transport Nodes (ESXi and KVM) & vCenter are also encrypted. These safe guards reduce some of the risk to the NSX management and control plane traffic, but it is recommended that it be

separated from other traffic via physical or VLAN separation, at a minimum. Preferably behind existing management Firewall or router with access-control policies. No user machines should be on this network.
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.

## 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) or vSphere Distributed Switch 7.0 (VDS 7.0) 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.

Starting NSX-T 3.0 release NSX supports vSphere Distributed Switch 7.0 (VDS 7.0) as a virtual switch to enable all the NSX capabilities, no need to deploy N-VDS like prior releases, if ESX hosts are running VDS 7.0.

N-VDS and VDS 7.0 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 Deployment - Protocol & Port Requirements*

Different NSX-T components communicate with each other to provide scalable distributed network & security services platform. The set of TCP/UDP ports used between different NSX components are listed in the release specific document. These TCP/UDP ports might need to be opened if NSX-T components are secured behind the Firewall to meet company security policy requirements. Please refer to the NSX-T ports & protocols page linked here for reference.

## *NSX-T Manager Appliance Deployment*

The NSX Manager virtual machine (VM) is part of the management & control 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 with other managers in the cluster. You can also provide additional isolation by having NSX managers, 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 Protocols & Port section 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 TLS 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. SSH access is allowed only to local user.



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

On NSX Manager SSH console commands that can be executed 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 Manager from unauthorized package installation and compromise.

Please refer to NSX-T administrative guide for additional info.

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

**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 algorithm to choose is RSA or EC. RSA key sizes can be either 2048 or 3072 or 4096 and EC key size can be either 256 or 384 or 521.
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. By default, password expires in 90 days, expiration time is configurable. User can also define minimum password lenghth, by default 12.
6. **Users and Roles**
   The following roles are defined within the NSX Manager. Assigning the appropriate



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

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 Admin | Full Access, NSX-T Networking. Read-only/Execute, for other related NSX-T Operations |
| Network Operator | Read-only, NSX-T Networking. Selective Read-only/Execute, for other related NSX-T Operations |
| Security Admin | Full Access, NSX-T Security. Read-only/Execute, for other related NSX-T Operations |
| Security Operator | Read-only, NSX-T Security. Selective Read-only, for other related NSX-T Operations |
| Load Balancer Admin | 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 |
| GI Partner Admin | Endpoint Protection Admin. Full access on Endpoint Services, including partner registration, service definition and service deployment |
| Network Introspection Admin | Full access on Service Insertion, including partner registration, service definition and service deployment |
| VPN Admin | Full access to VPN Services |

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-T Edge Appliance Deployment:*

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.

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 |



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

| |
|---|
| 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 2, Group 5, Group 14 (default), Group 15, Group 16, Group 19-21 |
| Encryption: AES (128,256), AES GCM (128,192,256) |
| Digest Algorithm: SHA1, SHA2 (384, 512) |

## *NSX-T Certificates and their usage:*

NSX-T components identification & authentication is done through self-signed certificates (with option to use organizational certificates). This enables initial trust between NSX-T components for preventing a rogue device from asserting the identity of an NSX-T component.
NSX-T Manager appliance generates self-signed certificates (SHA-256 With RSA Encryption) as part of initial deployment. This is leveraged for trusted communication between itself and the other NSX Managers in the cluster and also NSX-T transport & Edge nodes.. 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 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 keys are also stored in internal distributed database and accessible only to processes that run on the appliance, through a hidden private API .

NSX controller service within NSX manager appliance has it's own self signed certificate for identification and authentication for secure connectivity to NSX-T transport & Edge nodes.. These leverage encrypted and password protected PEM

files to store their certificates.

With NSX-T Federation deployment, NSX-T Managers use self-signed certificates (SHA-256 With RSA Encryption) to communicate with NSX-T Global Managers and other remote Local NSX-T managers. Just like NSX Local Managers, users may use their own CA to manage NSX Global Manager certificate for user management communication, i.e. browser access to the NSX Global Manager.

## *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 (read only) 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.

## *Built in NSX-T Capabilities for Security compliance*

This section summarises some of the key built-in NSX-T platform security related capabilities to make NSX-T more secure as a overall system and to meet the security compliance requirements:

- NSX Management UI/API access uses HTTPS with TLS 1.1/1.2, with an option to set TLS version only to TLS 1.2.
- NSX Management remote SSH uses SSHv2. SSH is disabled by default, and have option to enable it.
- NSX-T components internal communications are encrypted and uses TLS 1.2.
- NSX Manager provides management plane protection for deniel of service attack by having API rate limiting to limit the number of transactions per second and concurrent transactions to the NSX REST API.
- NSX Manager appliance internally provides service (manager, controller & DB) level resource (CPU & memory) isolation in order to protect individual services, by containing overwhelmed services within its allocated resources.
- NSX-T components identification & authentication is done through self-signed certificates (with option to use organizational certificates). This enables initial trust between NSX-T components for preventing a rogue device from asserting the identity of an NSX-T component.

- Each of the NSX appliances (NSX Manager, Edge) is closed hardened appliance and have built in controls to help secure from unauthorized package installation and compromise.
- NSX-T allows to uniquely identify and authenticate organizational users and define predefined RBAC roles to manage the NSX through integration with Active Directory, Open LDAP and VMware Identity Manger (VIDM).
- Configure and Enforce a limit of consecutive invalid logon attempts by a user during a configurable time-period.
- Lock the user account for an defined time-period when the maximum number of invalid login attempts is reached.
- NSX-T components support configuration of an organizational specific system use notification banner via the CLI command 'set banner'. The banner is displayed after authentication has occurred.
- Automatically terminate a user session after user configurable session timeout.
- The system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Use internal system clocks (synced to NTP server) to generate time stamps for audit records.
- All audit events are only accessible via the restricted shell (SSH) of the NSX-T components which is only authorized for the built-in Admin account. Access to audit events for the Admin account was limited to read only and there was no opportunity to modify or delete audit event records.
- Enable/Disable Cookie-based Authentication - NSX admins can now turn off cookie (session-based) based API authentication to improve the security posture of NSX-T platform operations. Cookie-based authentication is available by default and can be turned off/on using CLI.
- Enable/Disable Basic Authentication - NSX admins concerned about secure use of basic authentication can now disable (or re-enable) basic authentication for API and CLI use. Basic authentication support is available by default and can be turned off/on using CLI.

## *VMware Security Development Cycle, Policies and Advisories*

As part of NSX-T release cycle, NSX Appliances goes through the penetration and vulnerability-scan test to harden the appliance. More information on VMware Security development cycle is covered in the following white paper – VMware Security Hardening Activity.

Here are the other links on VMware Trust & Assurance and Security Response

Policies. In addition, VMware regularly publishes Security Advisories with information on what VMware products are affected by known threats.

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