WHITE PAPER
January 2025

Securing VMware® NSX 4.x

vmware® by Broadcom

Table of contents

Executive Summary

The VMware NSX network virtualization platform is a critical pillar of VMware by Broadcom's Software Defined Data Center (SDDC) architecture. The NSX network virtualization delivers for networking what VMware has already delivered for compute and storage. In a similar 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, 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 that 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 NSX Architecture

The main components of VMware NSX version 4.x are NSX Manager, NSX Edge, and vSphere Distributed Switch (VDS) version 7. 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. The NSX Manager cluster provides both the management and control plane functionality.

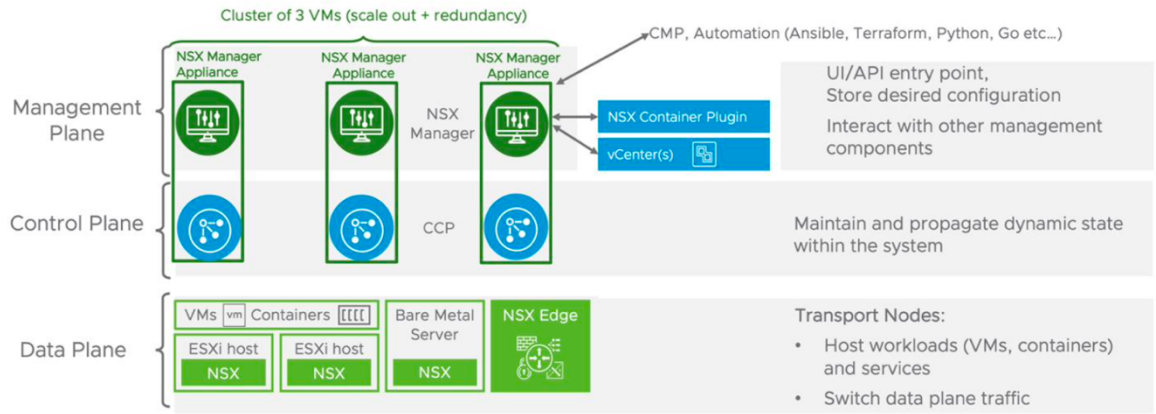
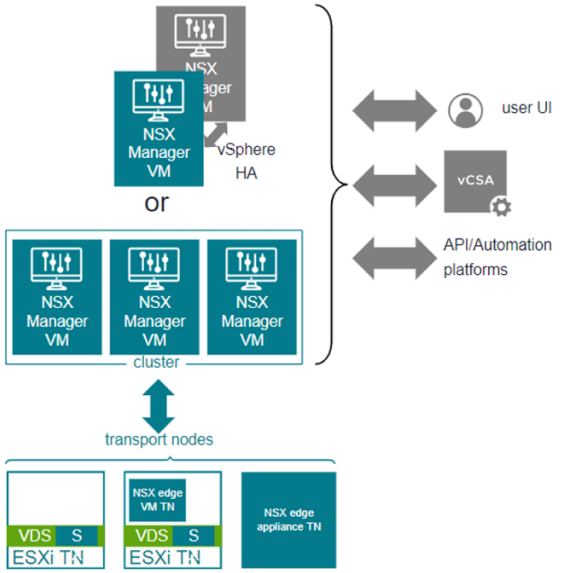


Figure 1: NSX Architecture and Components.



NSX Manager connects to and manages the NSX Transport Nodes (TN).

Transport Nodes implement the NSX Data Plane: this is where NSX switches traffic.

There are two kinds of transport nodes:

- ESXi hosts – The VDS of the ESXi host is enhanced with NSX components to enable NSX features.
- NSX Edge nodes – These are appliances running services that cannot be distributed on ESXi hosts.

Figure 2: NSX Components and Connectivity.

MANAGEMENT PLANE

The consumption of NSX 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 integrations into virtually any CMP via the REST API.

The NSX management plane is built by a three-node NSX Manager cluster for redundancy and high availability. Users can access the NSX management plane directly using individual IP's of the NSX Manager nodes or can configure a cluster Virtual IP (VIP) to provide a single point of configuration and REST API entry-points, while providing high availability at the NSX management plane. NSX Manager is delivered in a virtual machine form factor with different flavors (Small, Medium, Large, and Extra Large) for different scale requirements.

NSX Manager supports WEB access via HTTPS with TLS 1.1/1.2/1.3, with an option to set the TLS version to 1.3 only.

NSX Manager provides management plane protection for denial-of-service attacks by controlling the rate of API invocations, which limits the number of transactions per second and concurrent transactions to the REST API. This protects the system from being impacted when one or more clients make API requests at a rate the REST server cannot process. The API rate/concurrency limit configuration can be changed by users 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 splits the control plane into two parts:

- **Central Control Plane (CCP)** – The CCP is also implemented on the 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 (ESXi hosts prepared for NSX). It is adjacent to the data plane it controls and is connected to the CCP. The LCP on each Transport Node is responsible for programming the forwarding entries of the data plane.

The NSX 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, the NSX Manager appliance has multiple independent services: like Manager, Controller, and Database, to provide robust management and control plane functionality within the 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 allocation, so having one service overwhelmed does not impact other services in the appliance.

NSX Manager to Manager communication is encrypted by Mutual Transport Layer Security (mTLS), and so is the communication between NSX Manager and other NSX components: NSX Edge Nodes, Transport Nodes and vCenter. These safeguards 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 tagging, at a minimum. Preferably behind existing a management firewall or router with access-control policies. No user workloads should be on this network. The VMware vSphere Security Configuration Guides can be used to further explore protection of the management network.
http://www.vmware.com/security/hardening-guides.html

DATA PLANE

The NSX data plane is implemented on Transport Nodes. Transport Nodes are the hosts running the local control plane (LCP) daemons and vSphere Distributed Switch 6.5 and above 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 and distributed firewall, and enable GENEVE tunneling capabilities. NSX currently supports hosts with VMware ESXi™ to be Transport Nodes.

Beginning with the NSX-3.2 release NSX supports vSphere Distributed Switch (VDS) 7.0 & 6.7 for security-only use case, whereby users can define distributed security policies for workloads connected to Distributed Virtual Port Groups (DVPG).

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 are independent of physical constructs.

Network virtualization networking leveraging GENEVE and centralized network configuration provides 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 virtual network and operate as if they were connected to a physical L2 network

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

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

NSX Deployment – Protocol & Port Requirements

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

NSX 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 NSX VMs.

1. **Placement and network security**: Best practices dictate that the NSX Manager (a cluster of three NSX Manager instances) 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. Each NSX Manager node needs to communicate with the other NSX Manager instances in the NSX cluster. You can also provide additional isolation by having NSX Managers, NSX Edges & Transport Nodes in separate management VLANs and have firewall/access-list policies on the management gateway device. If you are securing the NSX components from other network services, make sure the appropriate ports are open. Refer to the Protocols & Port section to identify the ports that are used for communication to and from NSX components.

2. **Access and login**: Users can log in and operate NSX Managers through the vCenter console, SSH, HTTPS WEB access, and REST API. NSX uses TLS for HTTPS WEB access and REST, and Mutual TLS (mTLS) for internal communications between other NSX components. Users can perform day-to-day operations for configuration, monitoring and troubleshooting using the NSX WEB UI or programmatically with the REST API. SSH and the vCenter console provides users with access to the NSX Command Line Interface (CLI). SSH access to NSX Manager should only be enabled when required for troubleshooting. SSH is disabled by default during the NSX Manager installation for additional protection. For troubleshooting, SSH can be enabled temporarily for local users.
   The **admin** user can configure inactive timeouts for UI sessions.

3. NSX supports a few options for local and external authentication of users. You can log in to NSX Manager using a local user account, a user account managed by VMware Identity Manager (vIDM), or a user account managed by a directory service such as Active Directory over LDAP or OpenLDAP. For VMware Cloud Foundation environments only, WorkspaceOne Access Broker for SSO between vCenter, the SDDC Manager and NSX Manager is available.

Please refer to the NSX Administration Guide for additional info.

CONFIGURATION THROUGH NSX MANAGER

1. NTP

NTP is needed for many functions within NSX and VMware. If vIDM or SSO are leveraged in NSX, time synchronization in all components is crucial for the products to work correctly. It is critical that all systems within the VMware infrastructure have their time synced.

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. NSX 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 Administration Guide for more details.

3. SSH

During the NSX Manager installation, users may choose to enable SSH, otherwise SSH is disabled by default. SSH can be enabled or disabled via the NSX VM console. Disabling SSH is recommended. If SSH access is required for troubleshooting with tech support, it can be enabled during the troubleshooting process, and then disable the SSH service once it has been completed. NSX allows 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 certificates signed by their Certificate Authority (CA) for the NSX Manager WEB & REST certificate. The NSX WEB UI allows for an easy workflow to apply, import, and replace certificates to several NSX services, such as the WEB & REST service, the cluster manager service, etc.

When generating a Certificate Signing Request (CSR), the algorithms supported are RSA and Elliptic Curves (EC). RSA key sizes can be either 2048, 3072 or 4096, and EC key size can be either 256, 384 or 521.

5. Login Password

In order to login to NSX Manager WEB Interface, local users and users stored in LDAP or Active Directory will need to provide their credentials (username or username@domain and password) in the NSX login page. vIDM and WS1B users will be directed to the vIDM/WS1B consoles for authentication.

It is recommended to frequently change the login password based on the company's IT policies. By default, passwords for local users expire in 90 days. Expiration time is configurable. NSX administrators can define the applicable password policy for local users, such as minimum password length (by default 12 characters), complexity, history, lockout time, etc.

6. Users and Roles (RBAC)

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 assignment to users or user groups is needed for all local and external users, except for the pre-provisioned local users admin and audit, which roles cannot be edited. Please refer to the NSX Administration Guide for more details.

Role	Permissions
Enterprise Administrator	Full access, NSX Operations, Networking, Load Balancer and Security
Auditor	Read only
Network Admin	Full Access, NSX Networking. Read-only/Execute, for other related NSX Operations
Network Operator	Read-only, NSX Networking. Selective Read-only/Execute, for other related NSX Operations
Security Admin	Full Access, NSX Security. Read-only/Execute, for other related NSX Operations
Security Operator	Read-only, NSX Security. Selective Read-only, for other related NSX Operations
Load Balancer Admin	Full Access, NSX Load Balancer. Selective Read-only/Execute, for other related NSX Operations
Load Balancer Operator	Read-only, NSX Load Balancer. Selective Read-only, for other related NSX 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
VPC Admin	Full access to all networking and security objects inside an NSX VPC
Project Admin	Limited access within multi-tenancy, users may only manager a specific project and its objects
VPN Admin	Full access to VPN Services
Support Bundle Collector	Support bundle collection only

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 Edge Appliance Deployment

The NSX Edge Transport Nodes (NSX Edges) reside within the data plane of the NSX solution. A NSX Edge can be best described as a virtual or bare-metal appliance that provides North-South traffic management and services. NSX Edges are grouped in a NSX Edge Cluster to provide high availability of services. NSX Edges can provide the following functions: gateway firewalling, load balancing, IPSec VPN, SNAT/DNAT, routing, VRF and bridging.

1. **Placement:** Edges (at least two) are typically placed at the network border to handle North/South traffic. Since Edges 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 Edges can be achieved through console or SSH access, if enabled. The password for the SSH access can be set during installation of NSX Edges or from the NSX WEB UI. NSX Edges allow only SSHv2. if NSX components are secured behind a firewall to meet company security policy requirements, ensure that SSH traffic between the client and the NSX Edges is allowed.

   The SSH console provides a limited set of commands that can be run on Edge appliances. These commands include a list of show and debug commands. Please see the NSX Administration Guide for more information.

NSX EDGE CERTIFICATES & CIPHER SUITES

Depending on what features are enabled on NSX Edges, 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, NSX Edges 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
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 Certificates and their usage

NSX components identification & authentication is done through self-signed certificates at deployment time. This enables initial trust between NSX components for preventing a rogue device from asserting the identity of an NSX component.

NSX 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 for Transport Nodes and NSX Edge Nodes. For user management communication, NSX uses self-signed certificates by default. However, users may import their own CA-signed certificates for WEB & REST communications, e.g., browser access to the NSX Manager.

Keys are stored securely in the distributed database Corfu or in JDK files. These keys cannot be read from NSX APIs. The corresponding certificates can be read by public APIs.

With NSX Federation deployment, NSX Local Managers use by default self-signed certificates (SHA-256 with RSA encryption) to communicate with NSX Global Managers and other remote NSX Local Managers. Just like NSX Local Managers, users may use their own CA-signed certificates for the NSX Global Manager WEB & REST communication, e.g., for browser access to the NSX Global Manager.

NSX Logs and Alerting

NSX logs can be found in a variety of locations depending on the component that is generating the logs. NSX uses standard RFC5424 format for logging. Logs are stored in a different partition on the appliance to the base OS. Logs are accessible to only privileged local user (read only) from the CLI. NSX also logs initialization of services. NSX storage has log rotation policy based on the size of the log files. So VMware by Broadcom recommends sending all NSX logs to centralized log collector by configuring the syslog settings on NSX Manager, Transport Nodes and Edge Nodes. More information about log and log formats can be found in the NSX Administration Guide.

Built-in NSX Capabilities for Security compliance

This section summarizes some of the key built-in NSX platform security related capabilities to make NSX more secure and to meet security compliance requirements:

- NSX Manager supports WEB access via HTTPS with TLS 1.1/1.2/1.3, with an option to set the TLS version to 1.3 only.
- NSX Management remote SSH uses SSHv2. SSH is disabled by default and has an option to enable it.
- NSX components internal communications are encrypted and use TLS 1.3.
- NSX Manager provides management plane protection for denial of service attacks 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 components identification & authentication is done through self-signed certificates (with the option to use organizational certificates). This enables initial trust between NSX components for preventing a rogue device from asserting the identity of an NSX component.
- Each of the NSX appliances (NSX Manager, NSX Edge Nodes) is closed hardened appliance and have built in controls to help secure from unauthorized package installation and compromise.

- NSX allows to uniquely identify and authenticate organizational users and map predefined and custom RBAC roles to manage NSX through integration with Active Directory, Open LDAP, VMware Identity Manager (vIDM), and Workspace One Access Broker (WS1B).
- Configure and enforce a limit of consecutive invalid logon attempts by a user during a configurable time-period.
- Lock the user account for a defined time-period when the maximum number of invalid login attempts is reached.
- NSX 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 a 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 components which is only authorized for the built-in **admin** account. Access to audit events for the **audit** account is limited to read only and there is no opportunity to modify or delete audit event records.
- Enable/disable cookie-based authentication: NSX admins can now turn on & off cookie (session-based) based API authentication to improve the security posture of NSX platform operations. Cookie-based authentication is available by default and can be turned on & off using CLI.
- Enable/disable basic authentication: NSX administrators 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 on & off using CLI.
- The audience for the VMware NSX 4.x STIG is VMware NSX 4.x customers in the DoD needing to harden or accredit their vSphere environment. Other entities can use this guidance, however there are items that are specific to the DoD that will not be applicable to a non-DoD environment. The guidance is available to download here.
- NSX is configured to use FIPS 140-2 validated cryptographic modules to comply with FIPS requirements. The modules are validated to FIPS 140-2 standards by the NIST Cryptographic Module Validation Program (CMVP). More information about the validated modules can be found here.

VMware Security Development Cycle, Policies and Advisories

As part of NSX release cycle, NSX Appliances go through penetration and scan tests to evaluate the vulnerabilities of the appliances. More information on VMware Security development cycle is covered in the following white paper – VMware Security Hardening Activity.

Here are 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.

Item No: vmw-bc-wp-temp-a4-word-2024 1/24