



## Designated Operating Environment - 2022

Document Version: **2022-02-14**



The material in this guide defines the *Designated Operating Environment (DOE)* for a NETLAB+ Virtual Edition (NETLAB+ VE) System as of 02-14-2022.

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc.

## Contents

Introduction .....	2
1 Configuration Overview .....	3
1.1 DMZ .....	3
1.2 Campus LAN .....	4
1.3 Configuration Maximums .....	5
2 Virtual Infrastructure .....	6
2.1 Virtualization Components .....	6
2.2 Virtualization Product Support .....	7
2.3 Server Specifications for Hosting NETLAB+ Pod Virtual Machines .....	8
2.4 Storage Area Networks .....	9
2.5 Specifications for the Physical Management Server .....	10
2.6 Configuration for the Virtual vCenter Server .....	10
2.7 Guest Operating Systems (Virtual Machines) .....	11
3 Real Lab Equipment .....	12
4 Networking .....	13
4.1 LAN Connection .....	13
4.2 Internet Connection .....	13
4.3 Firewall Requirements .....	14
4.3.1 Network Address Translation (NAT) .....	14
4.3.2 NETLAB+ Server Inbound Port Requirements .....	15
4.3.3 NETLAB+ Server Outbound Port Requirements .....	15
4.3.4 Client Browser Outbound HTTPS Requirement .....	16
4.4 DNS Configuration .....	16
4.5 Encryption .....	16
4.5.1 Encryption Requirements .....	17
4.5.2 Encryption Performance .....	18
5 Uninterruptible Power Supply (UPS) .....	19
6 Supported Clients .....	20
7 Third Party Products (Disclaimer) .....	21

## Introduction


This is the *NETLAB+ Designated Operating Environment*, for the virtual edition of NETLAB+.

NETLAB+ is a remote access solution that allows academic institutions to deliver a hands-on IT training experience with a wide variety of curriculum content options. The training environment that NETLAB+ provides enables learners to schedule and complete lab exercises for information technology courses. NETLAB+ is a versatile solution for facilitating IT training in a variety of disciplines, including networking, virtualization, storage, and cybersecurity.

The *Designated Operating Environment* (referred to in the NETLAB+ Customer Agreement) is defined as the NDG-supplied NETLAB+ software and other hardware and third-party software required for the use of NETLAB+ software, configured in accordance with the specifications and connectivity requirements provided by NDG to the customer.

# 1 Configuration Overview


A NETLAB+ VE system may be configured behind a firewall DMZ (as recommended by NDG) or through a campus LAN. These two configuration options are illustrated in the subsections below.



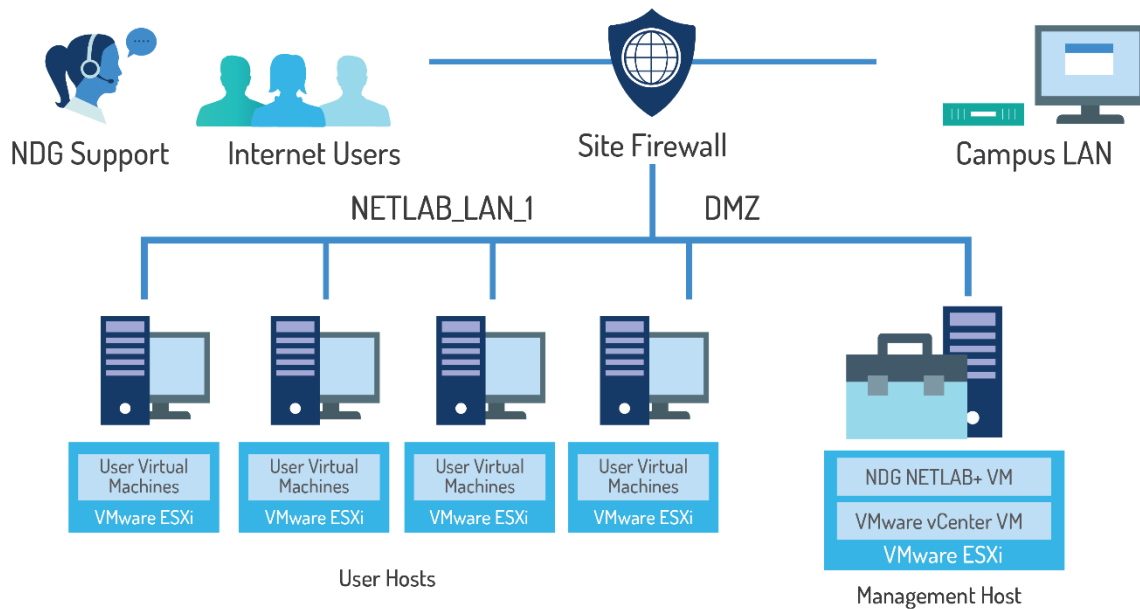
In each of the configuration options shown below, NETLAB+ and the VMware virtual infrastructure reside on a separate, dedicated segment. TCP 443 must be open to allow client traffic from the internet to the NETLAB+ VE server (see section 4.3 for details on port requirements). Note that NETLAB+ proxies traffic between the client and the lab environment, so it is not necessary to allow inbound traffic between the client and VMware virtual machines, and between client and real lab equipment.

## 1.1 DMZ

The following network topology is an overview of the Designated Operating Environment for NETLAB+ VE when configured behind a firewall DMZ (demilitarized zone).



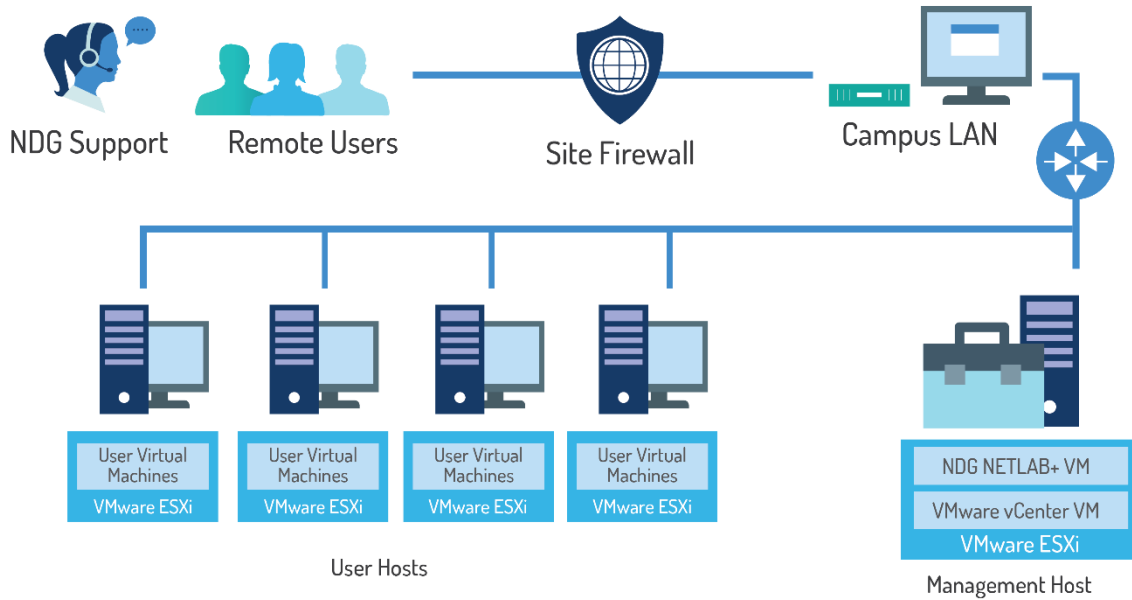
Configuring NETLAB+ VE behind a firewall DMZ as shown in this section is recommended by NDG.



**NETLAB+ VE Behind Firewall DMZ (demilitarized zone)**

## 1.2 Campus LAN

The following network topology is an overview of the Designated Operating Environment for NETLAB+ VE when configured through a campus LAN.



**NETLAB+ VE Through Campus LAN**

### 1.3 Configuration Maximums

Configuration maximums are dependent on the underlying physical host server. The default setting recommendations for NETLAB+ VE are based on the following virtual machine configuration:

<b>CPU</b>	4 cores
<b>RAM</b>	24GB
<b>HDD3</b>	100GB

With these settings, NETLAB+ VE will be able to support the following configuration maximums. Remember, the underlying host servers must also support these maximums.

#### Configuration Maximums



**Maximum active pods**  
("active" refers to pods scheduled during the same time block, i.e., 30 min block)

Up to 64 (currently tested), available for purchase in blocks of 16 active pods.

**Maximum number of active virtual machines**

Scales to Hardware

**Maximum custom pods**

Unrestricted

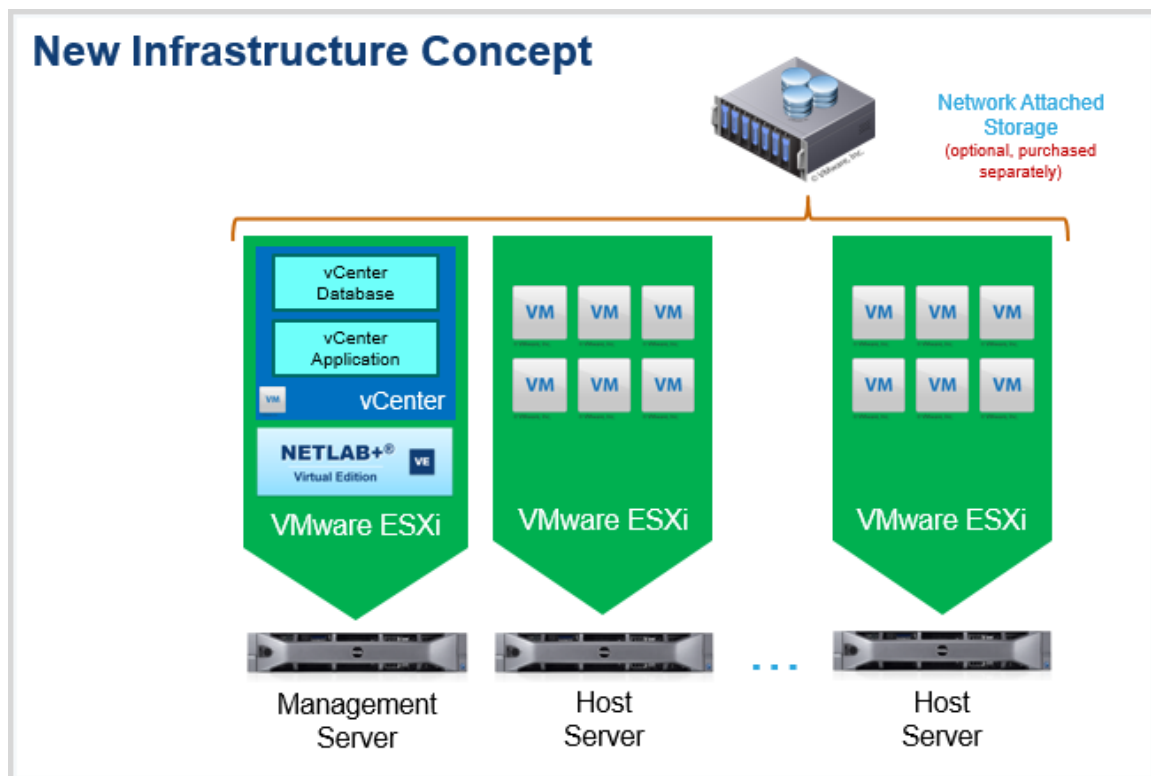
## 2 Virtual Infrastructure

NETLAB+ integrates with VMware vSphere to provide powerful and cost-effective remote PC support.

VMware Inc. provides cutting-edge virtualization technology and resources to academic institutions for little or no charge. Academic licenses for VMware ESXi and vCenter Server may be used for your NETLAB+ infrastructure. The procedure for obtaining licenses for this purpose will vary, depending on your participation in the [VMware Academic Program](#) and/or the [VMware IT Academy Program](#). For guidance on navigating the different licensing options that may be available to your organization, please refer to the [VMware Product Licensing Through VMware Academic Subscription \(VMAS\) Chart](#).

### 2.1 Virtualization Components

The virtualization components for the NETLAB+ VE system, including the Management Server and Host Server(s), are shown in the picture below.



## 2.2 Virtualization Product Support

Product	VMware Version	vCenter Required	NETLAB+ VE Support	Minimum NETLAB+ VE Version
VMware ESXi / vCenter	7.0	Yes	<b>Supported</b>	21.2.0
VMware ESXi / vCenter	6.7	Yes	<b>Supported, not documented*</b>	n/a
VMware ESXi / vCenter	6.0	Yes	<b>Deprecated</b>	16.1.21

\*Specifications and configuration guidance are not currently available for VMware vSphere 6.7.

The implementation of a virtual environment is discussed in the **NETLAB+ Remote PC Guide Series** - [Learn More](#)

- [Volume 1 - Introduction and Planning](#)
- [Volume 2 - Installing and Configuring VMware vSphere 7.0](#)
- [Volume 2b - Dell R720 BIOS and RAID Configuration](#)
- [Volume 2c - Dell R630 BIOS and RAID Configuration](#)
- [Volume 3 - Configuring the NETLAB+ Virtual Machine Infrastructure](#)
- [Volume 4 - Creating and Configuring Virtual Machines](#)



NETLAB+ is designed to work in a vSphere standard license environment. Enterprise-level components are not necessary and may interfere with the functionality of your NETLAB+ system.

**Advanced features/products that SHOULD NOT be used when deploying your virtual environment for NETLAB+ include:**

- Clusters
- Distributed Switches
- DRS
- vMotion
- vSAN



## 2.3 Server Specifications for Hosting NETLAB+ Pod Virtual Machines

The following table shows the current recommended specifications for ESXi host servers used to host virtual machines in NETLAB+ pods.

Please check the [VMware Compatibility Guide](#) to verify that all server hardware components are compatible with the version of VMware ESXi that you wish to use.

Components	Specifications
Server Model	ThinkSystem 1U
Chassis Hard Drive Configuration	2.5" Chassis with 8 or 10 Bays
Hypervisor (installed by you)	VMware vSphere ESXi 8.0
Physical CPUs (Minimum Host Server)	Intel Xeon Gold 6330 28C 205W 2.0GHZ
Physical CPUs (High-Performance Host Server)	2x Intel Xeon Gold 6338 32C 205W 2.0GHZ
Memory (Minimum Host Server)	8 x 64GB TruDDR4 3200 MHz (2Rx4 1.2V) RDIMM
Memory (High-Performance Host Server)	12x 64GB TruDDR4 3200 MHz (2Rx4 1.2V) RDIMM
SSD for OS Install	2x M.2 5400 PRO 240GB Read Intensive SATA 6Gb NHS SSD
SSD (Minimum Host Server)	2x U.2 PM1733 7.68TB Entry NVMe PCIe 4.0 x4 Hot Swap SSD
SSD (High-Performance Server)	2x U.2 PM1733 7.68TB Entry NVMe PCIe 4.0 x4 Hot Swap SSD
Network	Broadcom 57454 10GBASE-T 4-port OCP Ethernet Adapter Broadcom 5719 1GbE RJ45 4-Port PCIe Ethernet Adapter
Power Supply	2x 1100W (230Vac/115Vac) Platinum Hot Swap
Power Cords	2x 2.8m, 13A/120V, C13 to NEMA 5-15P (US) Line Cord
Rails	ThinkSystem Toolless Slide Rail Kit v2
Support	3 Year Support

## 2.4 Storage Area Networks

A *Storage Area Network (SAN)* is a dedicated network that provides access to consolidated, block-level data storage, which can be used for disk storage in a VMware vSphere environment.

**Currently, NDG does not provide benchmarks, guidance, or troubleshooting for SAN configurations.** Our documentation may show an optional SAN in the environment; however, this is not a recommendation or requirement to deploy a SAN.

**NDG benchmarks and capacity planning guidance do not account for the additional latencies introduced by SAN.**

- When compared to Direct Attached Storage, a SAN may introduce additional I/O latency between the ESXi server and disk. Therefore, a SAN may reduce the number of active VMs you can run on an ESXi host.
- If you deploy a SAN, you should perform your own benchmarks and determine the number of active VMs you can host on your ESXi server. Your mileage may vary.
- Always configure NETLAB+ Proactive Resource Awareness to ensure that the number of VMs that can be activated will remain within your predetermined performance limits.

## 2.5 Specifications for the Physical Management Server

VMware vCenter enables you to manage the resources of multiple ESXi hosts and allows you to monitor and manage your physical and virtual infrastructure. NETLAB+ VE integrates with VMware vCenter to assist the administrator with installing, replicating, and configuring virtual machine pods.

For performance reasons, a separate physical management server is required for the vCenter and NETLAB+ VE virtual machines.

Components	Specifications
<b>Server Model</b>	Lenovo ThinkSystem SR630
<b>Chassis Hard Drive Configuration</b>	2.5" Chassis with 10 Bays
<b>Hypervisor (installed by you)</b>	VMware vSphere ESXi 7.0
<b>Physical CPUs</b>	Two (2) x Intel Xeon Gold 5115 10C
<b>Memory</b>	8x 16GB TruDDR4 2666 MHz RDIMMs (128GB Total)
<b>SSD for OS Install</b>	2x M.2 CV3 128GB SATA 6Gbps SSD
<b>Raid</b>	ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter 8x 2.5" 600GB 10K SAS 12Gb HDD in RAID 5
<b>Network</b>	ThinkSystem 1Gb 4-port RJ45 LOM Intel X550-T2 Dual Port 10GBase-T Adapter
<b>Power Supply</b>	2x 750W (230/115V) Platinum Hot-Swap
<b>Power Cords</b>	2x 2.8m, 10A/120V, C13 to NEMA 5-15P (US)
<b>Rails</b>	ThinkSystem Toolless Slide Rail Kit with 1U CMA
<b>Support</b>	3 Year Support

Please adhere to VMware's requirements and best practices. vCenter requires at least eight CPU cores and 24GB RAM for the medium size inventory.

NDG does not support configurations where a virtualized vCenter server instance is running on a heavily loaded ESXi host and/or an ESXi host that is also used to host virtual machines for NETLAB+ pods. These configurations have exhibited poor performance and API timeouts that can adversely affect NETLAB+ operation.

## 2.6 Configuration for the Virtual vCenter Server

As of vSphere 5.1, NDG only supports the VMware vCenter Appliance. The physical server on which the vCenter Appliance resides should be a dedicated "management server" to provide ample compute power. It is strongly recommended you follow our server recommendations to provide ample compute power now and in the future. This appliance is a virtual machine that runs on ESXi 7.0.

The following table lists the vCenter server requirements for the vCenter 7.0 Appliance, based on the number of virtual machines in the inventory.

---

<b>vCenter 6.0 Appliance Size</b>	<b>Virtual Machines</b>	<b>CPUs</b>	<b>RAM</b>	<b>Disk</b>
Tiny	Up to 100	2	8GB	120GB
Small	Up to 1000	4	16GB	150GB
<b>Medium (Recommended)</b>	<b>Up to 4000</b>	<b>8</b>	<b>24GB</b>	<b>300GB</b>
Large	4000+	16	32GB	450GB

---

## 2.7 Guest Operating Systems (Virtual Machines)

NDG has tested Windows and Linux as guest operating systems. Novell Netware is not currently supported. Other operating systems that are supported by VMware may work but have not been tested by NDG. The guest operating system must support VMware tools for the mouse to work within NETLAB+.

### 3 Real Lab Equipment

*Real Lab Equipment* refers to physical hardware components, such as routers, switches, and firewalls, which are part of a topology and accessed by users.

For guidance on planning, installing, and supporting Cisco Networking Academy courses that contain real lab equipment (i.e., routers, switches, and firewall devices), please refer to the [Real Equipment Pod Installation Guide For Cisco Networking Academy](#).

## 4 Networking

The NETLAB+ infrastructure should be placed on a DMZ or dedicated LAN. Since a NETLAB+ system might be installed behind a firewall, many steps have been taken to make NETLAB+ secure and firewall-friendly. However, some TCP/IP ports will need to be opened through the firewall. Some firewall features or security devices may not be compatible with NETLAB+.

### 4.1 LAN Connection

Connection to a local area network is provided by a Gigabit Ethernet port on the management server.

- A unique static IP address is required.
- DHCP is not supported.

### 4.2 Internet Connection

NETLAB+ must have access to a broadband Internet connection. Actual bandwidth usage varies based on the number of simultaneous connections and connection types.



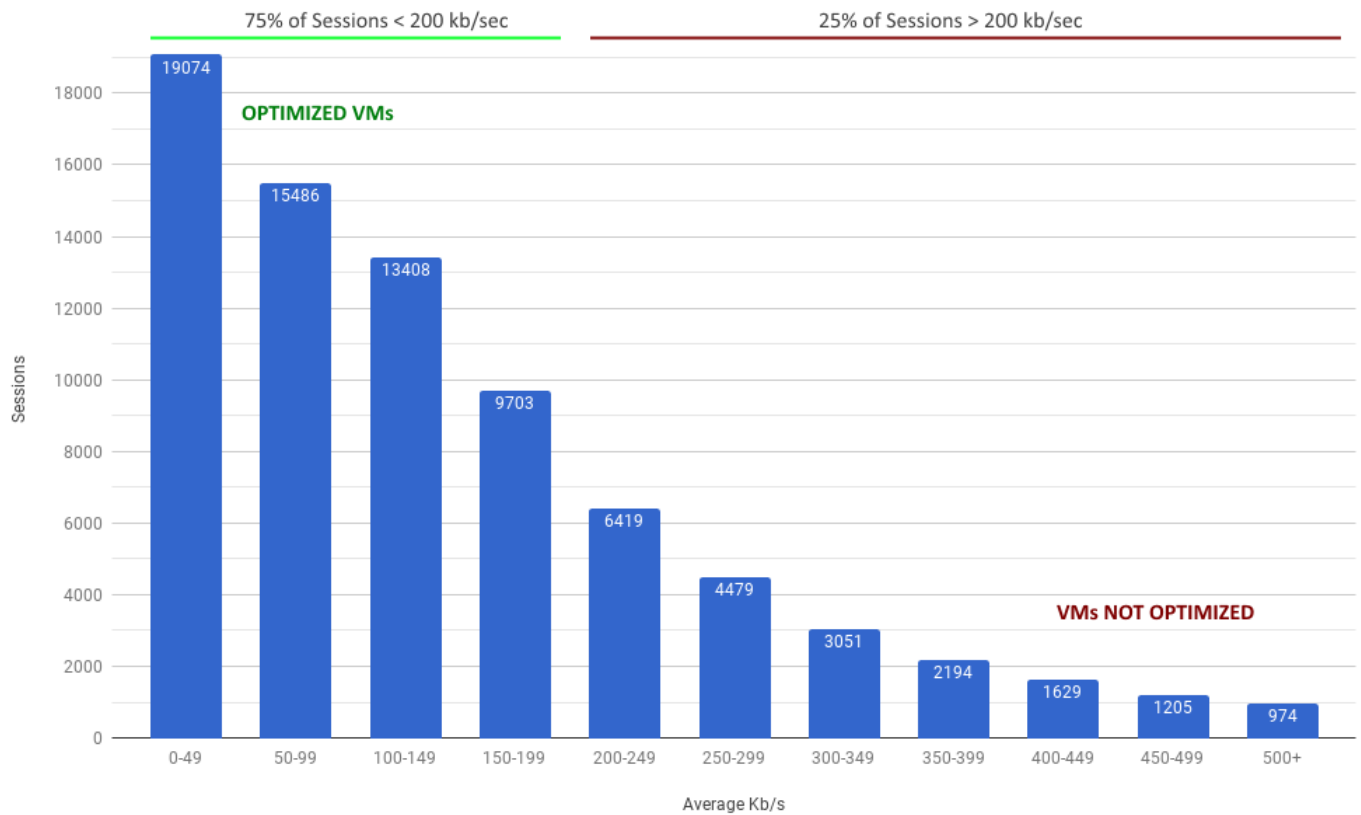
Some service offerings do not provide the same bandwidth in both directions; they are usually optimized for downloads from the Internet (inbound). For NETLAB+, it is desirable to have more bandwidth from the server towards the Internet (outbound).



NDG recommends planning 100-200 kilo-bits/sec server to client, per simultaneous user for average non-ILT workloads.

- VNC viewer server to client: see graph below
- VNC viewer client to server: < 10 kilo-bits/sec
- CLI viewer: character based, insignificant

## NETLAB+ VE PC Viewer Bandwidth - Server to Client - Distribution Over 84,480 Sessions



### 4.3 Firewall Requirements

This section includes details on firewall requirements.

#### 4.3.1 Network Address Translation (NAT)

NETLAB+ will work with **static NAT**.

- *Static NAT* is a type of NAT in which a single private IP address (A) is mapped to a single public IP address (B), where the public address is always the same IP address (i.e., it has a static address). This allows an internal host to have an unregistered (private) IP address and still be reachable over the Internet. This mapping should occur in both directions: traffic sent to public address B should be forwarded to private address A, and traffic sent from private address B should appear on the Internet as public address B.
- Port Address Translation and Dynamic NAT are not supported.

### 4.3.2 NETLAB+ Server Inbound Port Requirements

The following ports should be open to allow client traffic from the Internet to the NETLAB+ VE server. Note that NETLAB+ proxies traffic between the client and the lab environment, so it is not necessary to allow inbound traffic between the client and VMware virtual machines, and between client and real lab equipment.

Ports	Usage
<b>TCP 443</b>	Web interface and remote display proxy traffic.
<b>TCP 80</b>	This port must be allowed inbound through the firewall if you use Let's Encrypt™ as a certificate authority (see the NETLAB+ VE Installation Guide). If you are not using the Let's Encrypt service, port 80 (HTTP) inbound is still highly recommended as it will redirect HTTP pages to HTTPS on port 443.
<b>TCP 22</b>	SSH access for NDG staff. Contact NDG technical support to obtain our source IP address if you want to lock down this port further.

### 4.3.3 NETLAB+ Server Outbound Port Requirements

The NETLAB+ VE server may originate connections on the following ports. This list only includes ports for traffic that may egress the NETLAB+ LAN/DMZ. Additional ports are used within the NETLAB+ LAN/DMZ for interacting with virtual infrastructure and real lab equipment.

Ports	Usage
<b>UDP 53</b>	This is the standard DNS port used by NETLAB+ to resolve DNS queries. This port must be allowed outbound through the firewall unless NETLAB+ is configured to use local DNS servers.
<b>TCP 443</b>	Used by NETLAB+ to communicate with NDG central servers for license management, software upgrades, content downloads, and technical support. This port must be allowed outbound through the firewall.
<b>PING (ICMP)</b>	Used by NETLAB+ to verify the reachability of servers.



#### 4.3.4 Client Browser Outbound HTTPS Requirement

NETLAB+ uses Content Delivery Networks (CDN) to deliver fonts and other resources to the client. Some URLs in NETLAB+ web pages reference external URLs. Therefore, web clients inside the site firewall should be allowed to make HTTPS requests on port TCP port 443 to the Internet.

#### 4.4 DNS Configuration

A valid DNS entry for the NETLAB+ VE server must be configured for proper operation. When using NAT, the DNS should respond with the public address for external clients, and the private address for internal clients (this is standard NAT behavior).



Your system must have an Internet accessible public DNS entry if you choose to use Let's Encrypt™ as a certificate authority. Through an automated process (see the [NETLAB+ VE Installation Guide](#)), your NETLAB+ system will request and obtain a signed certificate from Let's Encrypt, a free certificate authority.



In previous versions of NETLAB+, it was possible to access the server by IP address. This is not supported in NETLAB+ VE because SSL/TLS over HTTPS does not support this. The NETLAB+ VE server **MUST** be accessed by hostname.

#### 4.5 Encryption

NETLAB+ uses SSL/TLS encryption between web clients and the NETLAB+ VE server. Within TLS, NETLAB+ uses HTML5 WebSocket technology to deliver two-way TCP communication between web clients and the virtual lab environment. End-to-end encryption between client and NETLAB+ server is necessary for the proper operation of WebSockets. Therefore, NETLAB+ VE uses only HTTPS for client communication. Unencrypted HTTP is not supported in NETLAB+ VE.

### 4.5.1 Encryption Requirements

The following items are required to meet NETLAB+ VE encryption requirements:

1. Use of strong encryption must be legal in your country.
2. The VMware host running the NETLAB+ VE virtual machine must support the AES-NI instruction set for hardware-accelerated encryption.
3. Unimpeded, routed connectivity (layer 3) between the client and the NETLAB+ server over SSL (TCP port 443).
4. A valid certificate for the NETLAB+ issued by a trusted certificate authority. Future versions of NETLAB+ may allow certificates to be obtained from the “Let’s Encrypt” service.
5. A valid DNS entry for the NETLAB+ server that matches the certificate.
6. Client browser must support HTTPS and WebSockets.

## 4.5.2 Encryption Performance

NETLAB+ VE must proxy a large volume of real-time remote display traffic between web clients and the VMware infrastructure. This traffic is VNC over WebSockets over SSL. In order to provide high performance, the NETLAB+ virtual machine is optimized to perform hardware-accelerated SSL using the AES-NI instruction set on the VMware host. As such, NDG does not support network proxy devices (transport layer or higher) that perform intermediate encryption and decryption of SSL traffic.



NDG recognizes that institutions may employ security devices that perform "SSL Inspection". This is typically implemented as an intentional, white-hat, man-in-the-middle device that masquerades as an SSL endpoint; the SSL data traveling through this feature incurs additional decryption, inspection, and re-encryption at the transport layer or higher. Bypass of SSL Inspection for NETLAB+ connections (TCP/443) is strongly recommended due to the high volume of SSL traffic NETLAB+ must handle and the complexity introduced by spoofing SSL endpoints. Most of the NETLAB+ SSL traffic is NETLAB+ is VNC over WebSockets. Inspecting this traffic will require lots of extra SSL processing, but with little increased security value.

Any connection or performance issues that arise with SSL inspection enabled shall be the responsibility of the customer and vendor providing the feature. Although NDG understands the motivation to enable SSL Inspection, please note that our ability to support and troubleshoot this configuration is limited. When handling network support cases, NDG may request that SSL Inspection be disabled to verify that the issue can be reproduced when SSL Inspection is not enabled in the network path.

## **5 Uninterruptible Power Supply (UPS)**






The management server which hosts the NETLAB+ VE virtual machine and VMware vCenter VM should be powered through a UPS to prevent abrupt power loss. Possible data loss may occur if these virtual machines are not powered down gracefully.

## 6 Supported Clients

NETLAB+ VE is accessed from a web browser. Using the most recent available version of the browser you select is recommended. Supported browsers are listed in the table below.



**Cookies and JavaScript** must be enabled in your browser. The latest information on supported web browsers is available from [Help > Supported Web Browsers](#) when signed in to a NETLAB+ account.

	Browser	Minimum Version	Support/Experience
	Google Chrome	54.0	* * * * *
	Mozilla Firefox	46.0	* * * *
	Apple Safari (MAC only)	11.0.3	* * * *
	Microsoft Edge	40.15063.674.0	* *
	Microsoft Internet Explorer		No longer supported

## 7 Third Party Products (Disclaimer)

NDG offers no warranties (expressed or implied) or performance guarantees (current or future) for 3rd party products, including those products NDG recommends. Due to the dynamic nature of the IT industry, our recommended specifications are subject to change at any time.

NDG recommended equipment specifications are based on actual testing performed by NDG. To achieve comparable compatibility and performance, we strongly encourage you to utilize the same equipment, exactly as specified, and configure the equipment as directed in our setup documentation. Choosing other hardware with similar specifications may or may not result in the same compatibility and performance. The customer is responsible for compatibility testing and performance validation of any hardware that deviates from NDG recommendations. NDG has no obligation to provide support for any hardware that deviates from our recommendations, or for configurations that deviate from our standard setup documentation.