Table of Contents

**Introduction** ........................................................................................................... 3

**Network Assessment** .......................................................................................... 4

Network Topology .................................................................................................... 5

Scan Target Identification ....................................................................................... 7

Customer Requirement Dependencies and Limitations ........................................... 9

Tenable Resource Allocation ..................................................................................... 11

**Scanning Methodology** ......................................................................................... 12

Active Scan Schedule Options .................................................................................. 13

Scan Policy Configuration ......................................................................................... 14

Host Discovery ........................................................................................................... 15

Vulnerability Scan .................................................................................................... 16

External Vulnerability Scan ..................................................................................... 17

Compliance Checks .................................................................................................. 18

Advanced Scanning Tips ........................................................................................... 19

**Related Documents** ............................................................................................ 20
Introduction

The purpose of this document is to describe scan strategies that Tenable Professional Services Consultants recommend for their various customer environments. This document focuses on Tenable.io and Tenable.sc active scans that utilize Nessus.
Network Assessment

The recommended Tenable scan strategy depends on the following factors:

- Network Topology
- Scan Target Identification
- Customer Requirements
- Tenable Resource Allocation
Network Topology

The organization’s network topology determines Nessus scanner placement and Scan Zone configuration.

- **Flat Network**
  - The Nessus scanner(s) can directly access all targets without firewall or other network device configuration.
  - One or more scanners can be configured to scan network targets in a single Scanner Group/Scan Zone.

- **Segmented Network**
  - If a network is behind a firewall or is VLAN separated, such as a DMZ, the Nessus Scanner may not be able to successfully scan its target.
  - A Nessus Scanner should be placed in each network segment.
  - Nessus requires port TCP/443 to communicate with Tenable.io and TCP/8834 for Tenable.sc.
  - If a Nessus Scanner cannot be placed in the network segments, then firewall rules must be configured so the scanner can reach all intended target ports and protocols.

- **Geographically Separated**
  - To minimize network bandwidth utilization and potentially decrease scan duration, consider placing a Nessus Scanner at geographically separated sites.

- **Operational Technology (OT)** (e.g., ICS/SCADA, or other sensitive networks)
  - Nessus Network Monitor is highly recommended.
  - If Nessus Scanners are used, first test in a non-production environment.
  - Any combination of the previous network topology examples

### Scanner Groups (Tenable.io) / Scan Zones (Tenable.sc)

Example Scanner Groups/ Scan Zones:
• **Default/Primary**
  • Flat network
  • Nessus can reach all targets

• **<Site> or <DMZ> Zone(s)**
  • Scanner at geographically separated site
  • Scanner in DMZ

• **Public**
  • The Tenable.io cloud-based scanner is in the External Nets scan zone that contains public-facing IP ranges.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io Scanner Groups</td>
<td>About Scanner Groups</td>
</tr>
<tr>
<td>Tenable.sc Scan Zones</td>
<td>Scan Zones</td>
</tr>
</tbody>
</table>
Scan Target Identification

Scan strategy depends on scan targets. A list of targets, such as IP addresses, ranges, subnets, and DNS names, can be used to create Tenable.io Target Groups or Tenable.sc Scan Targets.

- **Operating Systems (Windows, Linux, macOS)**
  - The OS type, quantity of each, and use of credentials impact the scan duration.

  **Note:** To scan by OS, ensure all your scans are credentialed and properly targeted by tags in Tenable.io or assets in Tenable.sc.

- **Application (DB, vCenter, etc)**
  - Scan duration varies based on application server type. Conduct a scan of a sample of systems to estimate scan duration and target system behavior.

  **Tip:** Scan on a non-production instance to prevent interrupting your production systems.

- **Network Devices (switch, router, firewall, etc)**
  - Credentialed scans are typically the fastest and provide the most thorough vulnerability scan results.

- **Public External**

  Use a Nessus Scanner that is able to communicate to the target public IP address. The scanner can be cloud-based or internal, such as:

  - **Tenable.io Sensor**
  - **AWS BYOL scanner**
  - **Azure**
  - **Nessus Scanner installed on Linux/UNIX/Windows virtual instance.**

  **Note:** For proper vulnerability detection, Tenable recommends scanning external servers by FQDN.

- **Quantity of targets.**

  To reduce the scan duration of a large number of targets:
• Add additional scanners
• Pool scanners in a Scanner Group/Scan Zone
• Scan by network segment/VLAN

• **Sensitive hosts**
  • Exclude any sensitive hosts from normal scanning:
    • [Create an Exclusion in Tenable.io](#)
    • [Create a Freeze Window in Tenable.sc](#)
  • If a sensitive host must be scanned, create a lab instance of your environment to troubleshoot scan sensitivity.

• **Transient Devices, e.g., laptops**
  • [Nessus Agents scans](#)

  **Tip:** If you cannot use Nessus Agents, view the [Nessus Agent Deployment Considerations](#) for other options.

• **AWS/Azure Machine Instances**
  • Utilize the AWS/Azure Connector feature in Tenable.io to collect an inventory of your deployed hosts. If the inventory of hosts are not a natural extension of your current network, then deploy the Nessus Pre-Authenticated Scanner found in the AWS/Azure marketplace.
  • If the inventory of hosts are a virtual extension of your internal network, you can use internal Nessus scanners to assess the hosts.
Customer Requirement Dependencies and Limitations

Customer restrictions and policies may limit the ability to scan at an industry best cadence. Tenable recommends scanning twice per week with all plugins to achieve the highest scan tempo and scan depth. For more information, see Lumin Metrics.

- **Software patch and scan cadence**
  - Many organizations have configuration management processes in place that define patch schedules. For example, if patches are only applied monthly, it may not make sense to scan weekly.

- **Regulation and compliance**
  - Configuration and compliance with regulatory standards often center around audit times such as quarterly or annually.
  - Compliance scanning requires credentialed scans.

- **Change management process**
  - If prior approval is required to conduct scans, create a baseline scan policy and propose a scan schedule that can be automated and predictable.

- **Maintenance windows**
  - If active scanning can only occur within a specific time window, e.g., after business hours, adapt the scan strategy to adapt to the restrictions.
    - Add additional Nessus Scanners and pool them in a Scanner Group / Scan Zone.
    - Increase the scan policy performance settings, such as Max hosts per scan.
    - Set Active Scans to Rollover and launch at the same time on the following day.

- **Control Systems**
  - Control Systems are any hardware or software that shapes, inspects, blocks, or inhibits network communications.
    - Ensure Nessus scanners can target all intended hosts on all ports. This involves whitelisting on firewalls, proxies, content filters, local firewalls, local IPS, etc.
Nessus scanners must be able to report results to Tenable.sc or Tenable.io. SSL inspectors, SSL MITM proxies, content filters, some transparent proxies, etc. can sometimes break this communication or inhibit performance.
Tenable Resource Allocation

Depending on scan policy settings, the Nessus scanner minimum hardware requirements may not be sufficient to meet scan frequency or duration goals.

**Nessus Scanner**

Tenable recommends using a Linux-based operating system. If your organization has an established Linux team, use their recommended RHEL image or CentOS build. You can also use Tenable Core. For a full list of supported operating systems, see [Nessus Scanner Software Requirements](#).

A Windows-based Nessus scanner must have its scan policy performance (max number of concurrent TCP sessions per scan) throttled to ensure accuracy. Contact Tenable Support for further assistance.

For recommended Nessus hardware settings, see [Nessus Scanner Hardware Requirements](#). Scan policy performance settings will impact CPU and RAM utilization, so monitor Nessus scanner resource and adjust as necessary.

**Tenable.sc**

For hardware and software requirements, see [Tenable.sc Hardware Requirements](#) and [Tenable.sc Software Requirements](#). Ensure Tenable.sc hardware resources meet minimum requirements for in-scope IPs.

**Caution:** It is important that you meet the recommended Tenable.sc hardware requirements otherwise performance issues could result.

**Tenable.io**

Tenable maintains Tenable.io hardware resources.
Scanning Methodology

- Active Scan Schedule Options
- Scan Policy Configuration
- Scan Policy Settings
Active Scan Schedule Options

You can choose from the following active scan scheduling options to match your scan cadence.

- **On-demand**: Manually launched by the user.
- **Scheduled**: Scheduled scans can be set to automatically launch daily, weekly, or monthly.
- **Dependent**: The active scan will launch when a scheduled parent scan completes. Dependent scans can be daisy-chained to other dependent scans.
Scan Policy Configuration

Use the following scan policies to fit your desired scan strategy:

- [Host Discovery](#)
- [Vulnerability Scanning](#)
- [External Vulnerability Scan](#)
- [Compliance Checks](#)
Host Discovery

Before you run a discovery scan, you should create a discovery process:

- If you know all of your active ranges, scan these ranges using the Host Discovery template.
- If you do not know all of your active ranges, develop a strategy to scan a portion of your network daily/nightly using the Host Discovery template.
  - Discovery scans can be dangerous if too many scanners participate and cross firewalls. If this happens, move the scanners closer to their targets. Alternatively, use NMAP for discovery.
  - Tenable recommends using NNM in discovery mode for the most successful discovery. If you have central IDS, netwitness, or other traffic sniffing solutions, put NNM in the same tap location in discovery mode until networks are mapped, scans are scheduled, etc.
  - Monitor Discovery dashboards in Tenable.sc and Tenable.io to find unassessed, newly discovered hosts and schedule scans to assess them.
Vulnerability Scan

A Basic Network Scan template is suitable for any host. If a Basic Network Scan impacts resources, something is blocking the scanning and needs to be fixed.

Because basic network scans do not scan for CGI and most http:// family settings, you must run a separate Web Application Test scan that targets ONLY known web servers.

**Note:** A Web Application Test scan can take 5-8 times longer than normal scans and does not require credentials.

Scan Progression

1. Scan known ranges with Basic Network Scan without credentials. This should identify most operating system types and fill in dynamic assets and tags.

2. Target scans with Basic Network Scan with credentials to known target groups of similar OS types. This prevents the practice of stacking credentials.

3. If an asset requires further inspection, target specific assets with an Advanced Network Scan with all plugins turned on

4. Target all known web servers with the Legacy Web Applications scan template without credentials to understand web exposures. Basic or Advanced scan templates do not include Web Applications because web assessments take longer than normal scans.

5. If a deeper inspection is needed, target specific web server assets with a licensed WAS scan.
External Vulnerability Scan

When scanning external (internet-facing) hosts, Tenable recommends scanning by FQDN instead of by IP. Since 5000 separate hosts can run on a single web server, if FQDN is not invoked for the scan, traffic is not routed to the internal hosts of an IP.

**Tip:** To determine your external DNS names, view:

- Assets for Domain Inventory in Tenable.sc
- Explore, Assets, and Domains in Tenable.io

Then, select the assets you want to assess and run a Basic Network Scan or Legacy Web App Scan to collect vulnerabilities.
Compliance Checks

For information on compliance checks, see the following documents:

- [Nessus User Guide](#)
- [Nessus Compliance Checks Reference](#)
- [Nessus Compliance Checks PDF](#)
Advanced Scanning Tips

Advanced Scan Templates are available for use by Nessus experts to scan more deeply using custom plugins, or faster or slower as required. Misuse could cause asset outages or network saturation. Use at own your own risk. For more information, see Advanced Settings in the Nessus User Guide.
## Related Documents

<table>
<thead>
<tr>
<th>Document Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.sc User Guide</td>
</tr>
<tr>
<td>Nessus User Guide</td>
</tr>
<tr>
<td>Tenable.io User Guide</td>
</tr>
<tr>
<td>Nessus Network Monitor User Guide</td>
</tr>
<tr>
<td>Nessus Compliance Checks Reference Guide</td>
</tr>
<tr>
<td>Tenable Core User Guide</td>
</tr>
</tbody>
</table>