# Table of Contents

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

**Integration Overview** ................................................................................................. 4  

**Integrate with Fortinet** .............................................................................................. 5  
  Fortinet NGFW Configuration Audit ............................................................................. 6  
  Import Fortinet NGFW Logs ......................................................................................... 16  
  Dashboards and Reports ............................................................................................... 18
Introduction

This document describes how to deploy Tenable.sc and Nessus® for integration with the FortiGate next-generation firewall (NGFW) platform by Fortinet. Please email any comments and suggestions to Tenable Support.

Monitoring the security settings of your Fortinet firewalls is critical for maintaining your network’s security posture. Unless your vulnerability management (VM) platform is equipped with configuration assessment checks specifically designed for Fortinet firewalls, your network may be exposed to unnecessary risk.

Additionally, better VM platforms offer continuous listening through passive vulnerability monitoring to help bridge the vulnerability intelligence gap in between periodic active scans and audits. However, placing passive monitors on every network segment throughout a global enterprise can be impractical. Although more organizations are turning to SIEMs (security information and event management) to uncover hidden threats, most SIEMs take months to deploy and are costly to acquire and maintain.

Benefits of integrating Tenable Tenable.sc with Fortinet include:

- Maintain compliance with industry best practices for firewall hardening
- Achieve real-time, 100% asset discovery by detecting new hosts connected to network segments not monitored by Nessus Network Monitor
- Discover system vulnerabilities and security misconfigurations of mobile devices and virtual machines not present during the last periodic full-network scan
- Maintain compliance with government and industry regulations that mandate log aggregation, such as PCI, HIPAA, FISMA and more
- Uncover advanced cyberthreats
Integration Overview

Tenable.sc and Nessus offer a series of plugins specifically designed to audit Fortinet physical and virtual firewalls to identify security misconfigurations and ensure best-practice hardening guidelines are followed. To perform the audit, Tenable.sc (via Nessus) initiates a credentialed scan of the Fortinet firewall, authenticating credentials through the Fortinet XML API. Once completed, detailed findings of the Fortinet audit can be reviewed within Tenable.sc scan results, dashboards and reports.

In addition to configuration audits, Tenable can also import real-time log data from Fortinet firewalls into its Log Correlation Engine® (LCE®) to help identify assets on networks not monitored by Nessus Network Monitor. Once hosts are identified they can be automatically assigned to dynamic asset lists and audited with Nessus to detect any possible vulnerabilities or misconfigurations.

Nessus Manager version 6.x, Tenable.io, and Tenable.sc version 4.8 and higher support Fortinet integration. Nessus, Tenable.io and Tenable.sc solutions work with Fortinet FortiOS versions 4.3 and above.
Integrate with Fortinet

Fortinet NGFW Configuration Audit

Import Fortinet NGFW Logs

Dashboards and Reports
Fortinet NGFW Configuration Audit

To begin the integration configuration, log in to Tenable.sc, click **Scans** and select **Audit Files**.

Click **+Add** and select **FortiGate FortiOS** from the list of available audit file templates.
In the “General” section, enter a name for the audit file and a description (optional).
Click **Credentials** and click **+Add**.

In the “General” section, enter a name for the SNMP credentials and a description (optional). Under the “Credential” section, click the drop-down and select **SNMP**. In the “Community” box, enter the SNMP community string. Click **Submit**.
Next, create the scan policy by navigating to “Policies” and clicking +Add.

Select the **Policy Compliance Auditing** template.
In the “Setup” section, enter a name for the audit policy and a description (optional). The options under “Configuration” can be left as “Default” or set to “Custom.” If the configuration options are set to “Custom,” the “Advanced” and “Host Discovery” categories will be enabled in the left-hand menu. Leaving the options as “Default” will keep those items hidden.
Navigate to the “Compliance” section and click **Add Audit File**. In the “Compliance” section, click the **Select a Type** drop-down and select **FortiGate FortiOS**. Next, click the **Select an Audit File** drop-down and select the previously configured FortiGate audit file. Click the checkmark to finalize the settings. Click **Submit**.

In the “Policies” section, navigate to **Credentials**.
In the “General” section, enter a name and description (optional).

Within the “Credential” section, click the drop-down next to “Type” and select SSH. Click the Authentication Method drop-down and select the correct option for your environment. Enter the SSH username used to authenticate to the Foritnet firewall and then click Choose File to select the Private Key file. Next, enter the Passphrase and then click the Privilege Escalation drop-down and select None. Click Submit.
To create an audit scan of Fortinet NGFWs, click on **Scans** and select **Active Scans**. Click on **+Add**.

In the “General” section, enter a scan name and description (optional). Click the **Select a Policy** dropdown and select the previously configured FortiGate FortiOS audit policy. In the “Schedule” section, the scan can be configured to run “On Demand” (default), or it can be configured to run on a custom schedule as required.
Navigate to the “Targets” section and click the Target Type drop-down. Select IP/DNS Name and enter the Fortinet NGFW IP address or DNS name.
Navigate to “Credentials” and click + Add Credential. Click the drop-down and select SSH. Once SSH is selected, a second drop-down box will appear. Click the box and select the previously configured SSH credentials for FortiOS. Click the checkmark to finalize the settings. Click Submit.

![Add Active Scan](image)

**Note:** Integrating Tenable.sc and Fortinet to perform audit checks requires configuration in both Tenable.sc and FortiOS. For detailed instruction on configuring FortiOS for integration, please refer to the [Fortinet FortiGate/FortiOS Admin Guide](#).
Import Fortinet NGFW Logs

Real-time log data from Fortinet NGFWs can be imported into Tenable.sc (via LCE). Integration requires configuration changes within FortiOS and within Tenable.sc, as well as the installation and configuration of Tenable NetFlow Monitor.

To begin the integration, download the Tenable NetFlow Monitor LCE client from the Tenable Downloads page.


**Note:** The Tenable NetFlow Monitor LCE client can be run directly on the LCE server. It must be configured to connect to either the localhost (127.0.0.1) or the IP address of the LCE server. Multiple LCE Client types (such as the LCE Log Agent and the Tenable NetFlow Monitor) can be run at the same time as well.

Log in to Tenable.sc using an admin account and navigate to “Resources.” Select LCE Clients.

Click the drop-down arrow to the right of the “netflowclient” and select Authorize. If successful, a pop-up message stating it has been successfully authorized will appear.
To complete the Tenable.sc configuration, click on the netflowclient to edit the LCE client and assign a policy. Click the Policy drop-down to select the desired policy. Click Submit. If successful, a pop-up message stating “LCE Client Edited Successfully” will appear.

Note: To complete the integration, please refer to the Fortinet FortiGate/FortiOS Admin Guide for detailed instructions on how to configure a syslog server and enable log forwarding.

Once configured, log data from the Fortinet NGFW will be imported into Tenable.sc to help achieve 100% asset discovery. The log data can also be correlated against other data sources to uncover any potential advanced threats and to help organizations meet compliance obligations.
Dashboards and Reports

Information obtained through Fortinet NGFW configuration audits and the collection of log data can be easily viewed and analyzed through Tenable.sc’s pre-defined, customizable dashboards and reports.
Fortigate FortiOS Audit Report
February 20, 2016 at 12:07pm EST

[SC_Manager]
ORG_1

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

FortiGate FortiOS Audit Report Title Page
# Table of Contents

**About This Report** .................................................................................................................................................................................. 1

**Executive Summary** .............................................................................................................................................................................. 2

**Audit Summary** ................................................................................................................................................................................... 4

- 3.2 - Failed Audits .................................................................................................................................................................................. 5
- 3.3 - Manual Audits .................................................................................................................................................................................. 6
- 3.4 - Passed Audits .................................................................................................................................................................................. 7