Solution Brief

Tenable and Fortinet

Maximize Your Security Investment

The Challenge

Organizations today are tasked with the difficult job of defending their borders, interiors and obtaining full visibility into everything that traverses their networks. Firewalls are indispensable tools, meeting this challenge by intercepting and examining traffic, and passing information along. However, this indispensable piece of hardware can become your greatest enemy when compromised by an attacker. Active security assessment of firewall configurations, and their integration into your overall security program, ensures that firewalls are updated and hardened against possible attacks.

Keeping your firewalls current is just the first step to maintaining your network's security health. To have a complete and continuous view of your network security posture, you need to continuously monitor and assess your environment to discover changes, capture transient hosts not present during scans and identify new hosts on remote network segments. The security of your network must respond to change as it occurs, not as an afterthought.

To combat the ever-increasing threat landscape, many organizations have several solutions deployed as a part of their security strategy. This layered approach frequently leads to silos of data with little visibility or context available to inform appropriate action. As enterprise firewalls pass traffic, they generate enormous amounts of data for the networking and security teams. With the right analysis, this data becomes a powerful tool to quickly adapt and ensure coverage and visibility into even the most remote corners of the network.

The Solution

Tenable™ and Fortinet offer best-in-class security combining active network protection with powerful weakness detection, maximizing the number of unique security controls that you get for your investment. The integrated solution provides continuous visibility and critical context, enabling decisive actions to protect your organization from risk, exposure and loss.

Tenable Nessus® not only audits Fortinet FortiGate devices for vulnerabilities, but assesses configuration settings against best practices for securing them against attackers. Nessus performs security configuration audits specifically designed for both physical and virtual Fortinet devices giving you peace of mind that your firewalls will always be in check with best-practice hardening guidelines and ensuring you have the visibility to quickly identify misconfigurations that can lead to vulnerabilities.

Tenable solutions are uniquely capable of gathering and assessing FortiGate firewall log data. Tenable SecurityCenter ContinuousView® (SecurityCenter CV™) leverages the real-time information captured by Fortinet devices throughout your environment to enhance visibility into your security posture and uncover advanced cyberthreats. This enables you to identify assets not active during vulnerability scans, find unknown assets not previously catalogued and provide the context needed to pinpoint potential weaknesses. By correlating FortiGate logs with other security data across your environment, you can identify security threats with behavior monitoring and indicators of compromise through continuous analysis using current threat intelligence. Actions, such as sending an alert or starting an active scan can be triggered by real-time security detections, speeding time to detection and resolution.

With the Tenable Fortinet Firewall dashboard, you can easily monitor the configuration and traffic status of your Fortinet firewall(s) and correlate firewall log data with other security data to discover unknown assets, indicators of weakness and suspicious user behavior, eliminating blind spots – all without requiring firewall management privileges. In addition, Tenable helps you improve your situational awareness by providing reports of all new hosts – along with complete scan results – that can be automatically sent to administrators.

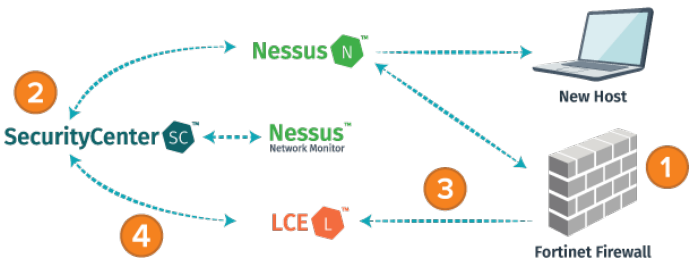
Components:

- Tenable SecurityCenter Continuous View or
- Tenable Nessus
- Fortinet FortiGate Firewalls running FortiOS

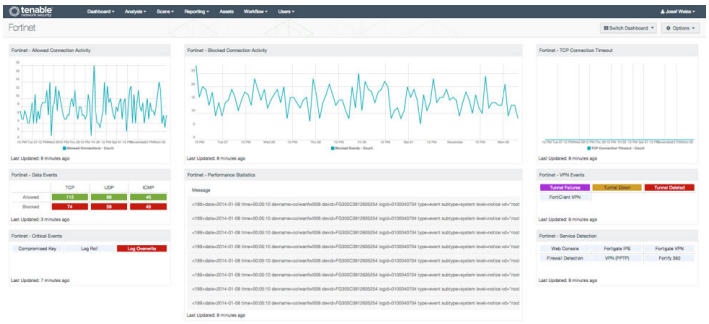
Benefits:

- **Reduce your attack surface** by ensuring your firewalls are configured to Fortinet and industry best practices
- **Monitor configuration and traffic status** from a single pane of glass, without requiring firewall management privileges
- **Uncover advanced cyberthreats** by correlating FortiGate firewall log data with log data from other network and security devices
- **Discover vulnerabilities and misconfigurations** of mobile devices and virtual machines not present during your last full-network scan

How It Works



1. Tenable initiates a credentialed scan of the Fortinet firewall.
2. Any detected Fortinet firewall security misconfigurations can be reviewed within Tenable dashboards and reports.
3. The Fortinet firewall exports log data in real-time to Tenable, which adds never-before-seen hosts to dynamic asset lists, thus triggering Nessus active scans.
4. Tenable correlates log data from the Fortinet firewall with other security and network log sources to uncover hidden cyberthreats.



The Tenable Dashboard for Fortinet FortiGate devices allows security administrators to view a summary status of firewall information including indicators for events, connection activity and performance alerts in a single location.

Combining Fortinet and Tenable maximizes your investment in both solutions, yielding a formidable defense against today's ever-changing threat environment. Tenable brings continuous visibility across your entire security program, including the state and activity of physical, virtual, mobile, network and security devices, along with the critical context you need to take decisive actions that improve your security. To learn more about Tenable's solutions visit tenable.com.

About Fortinet

Fortinet protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments - be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at fortinet.com, the Fortinet Blog or FortiGuard Labs.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact