tenable network security

Network Infrastructure Is Not Immune

Using the Tenable Solution to Audit and Protect Firewalls, Routers, and Other Network Devices

May 14, 2013

(Revision 1)

Table of Contents

Executive Summary

Operational failures of network devices can significantly impact revenues and employee productivity and are a primary concern of most IT organizations. As a result, organizations consume considerable resources to ensure the availability of these devices. Often organizations overlook the security exposures that may be present and could be exploited at any time under the assumption that these are hardware devices that are not exploitable. In fact, they may have already been exploited and, as long as the devices remained operational, no one would know.

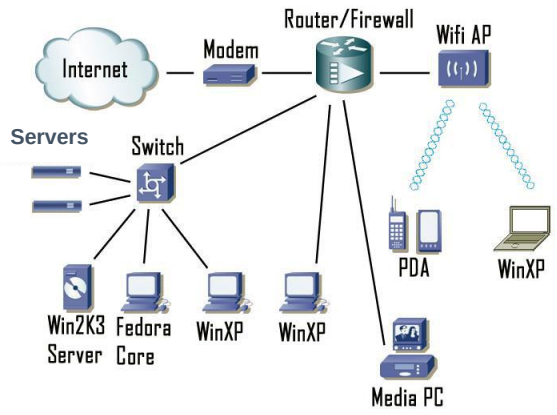
Network devices, such as firewalls, routers and switches, play a critical role in providing access to sensitive data. As such, network administrators are not enthusiastic about any activity, such as security auditing that may adversely impact the performance of these devices. It's difficult to convey security risks when the consequences of these risks are not readily apparent.

While a full-on security breach is a great demonstration of security risks on network devices is it not prudent to wait for such an event to implement a security monitoring program for such devices. Security monitoring of network devices must be integrated into an overall Threat Management program that provides the ability to correlate and summarize security events into critical actionable items.

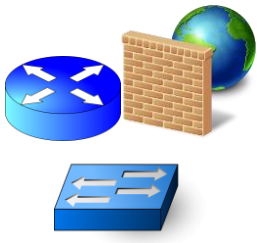
This paper describes how Tenable's Unified Security Monitoring solution resolves this issue and lowers IT risk by providing organizations with the tools and technologies they need to thoroughly audit and assess the security posture of their network infrastructure on a continuous basis with low impact to operations.

Network Infrastructure is Not Immune

Despite being classified as "hardware," network devices incorporate a substantial software component, including remotely accessible management interfaces that leverage browser accessible web technologies (e.g., HTTP, XML). They are also complex systems in their own right, enabling tens to hundreds of configurable options as a way to support the needs of the broadest possible set of customers.



These devices are often directly exposed to the Internet and have the same risks for misconfiguration and vulnerabilities as any other software/web-based solution. The Nessus vulnerability scanner includes hundreds of vulnerability checks for networking and security devices from Cisco, Juniper, Check Point, and many others. You can simply search on "exploiting web management interfaces" to see how common Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks are against these devices.



Network infrastructure devices are also governed by numerous compliance requirements. The Payment Card Industry Data Security Standard (PCI DSS) validates this point as it extends numerous requirements to all "network components" in any way involved with processing cardholder data. Here are just a handful of the relevant requirements:

- **2.2.2.b** Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.
- **2.2.3.c** For a sample of system components, verify that common security parameters are set appropriately.

- **2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.

- **4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.

- **6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.[1]

Another example is the widespread use of Center for Internet Security (CIS) configuration benchmarks to ensure that networking and security devices remain compliant with FISMA, SOX, HIPAA, and a wide variety of other compliance regimens. Routinely validating adherence to these benchmarks is an essential part of an enterprise's overall compliance process.

Obstacles

Network infrastructure is clearly not immune to vulnerabilities and compliance requirements. As a result, enterprises need to actively audit and secure related devices – just like they do for their servers. Why then are more organizations not doing so, or, more accurately, not doing it more thoroughly?

There are several obstacles that enterprises have had to overcome to audit network devices. These primarily involve inadequacies of the tools and technologies that have been available in the past, and include:

- The inability to remotely perform scans with sufficient accuracy
- Relatively meager configuration auditing coverage for network devices – for example, many solutions support little more than Cisco routers and firewalls
- The inability to adequately account for changes in networks and related devices
- The need for multiple, separately managed products to accomplish both objectives – that is, in-depth vulnerability assessments *and* configuration audits – across all devices that require such attention, endpoint and network ones alike; and,
- The substantial manual effort and financial investments required to overcome each of the preceding deficiencies.
- The ability to passively monitor sensitive network devices without risking operational failures

A key obstacle is that the networking and security teams are often at odds. Whereas networking personnel typically focus on operational issues - delivering reliable, high-performance connectivity to all networked resources - the solutions implemented by security professionals are perceived as diminishing performance and limiting access to resources. This conflict invariably impacts daily interactions between the two teams and limits the ability to achieve certain objectives – such as performing detailed scans of networking devices, or remediating identified vulnerabilities in network devices.

How Tenable Can Help

Tenable's Unified Security Monitoring platform combines in-depth vulnerability and configuration auditing with real-time detection and network monitoring to deliver unparalleled insight into an organization's network infrastructure and its exposure to related vulnerabilities, threats, and risks.

With the Tenable solution, enterprises obtain a single, role-based interface for administrators, auditors, and risk managers to evaluate, communicate, and report information necessary for effective decision making and systems management.

Organizations also benefit from a wealth of integral capabilities that overcome the many limitations of traditional tools and technologies to provide a superior solution for proactively auditing, assessing, and continuously monitoring the security, configuration, and compliance status of essential network infrastructure.

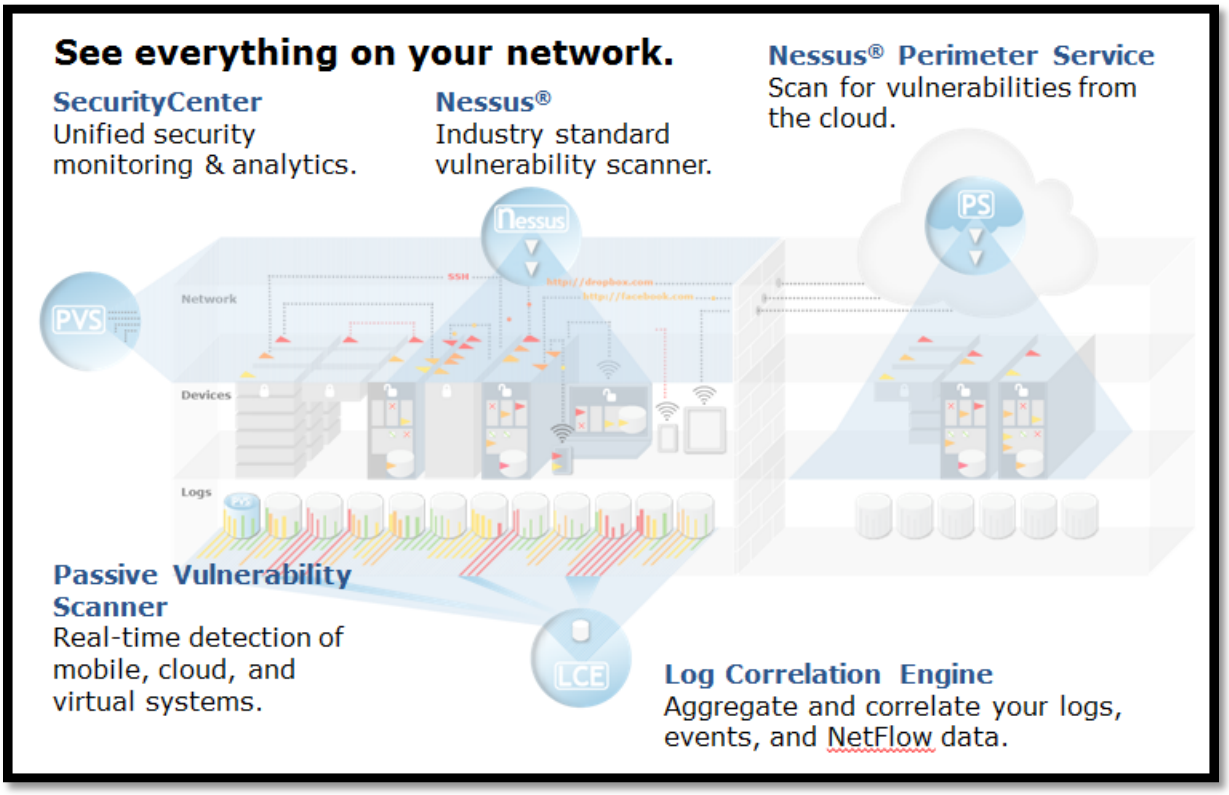


Figure 1: Tenable's Enterprise Architecture

A tight integration of Nessus®, the Tenable Passive Vulnerability Scanner (PVS), and the Tenable Log Correlation Engine (LCE) with the SecurityCenter (SC) centralized management system, Tenable Unified Security Monitoring delivers a comprehensive set of functionality for network infrastructure that enables enterprises to:

- Automatically and thoroughly discover all types of network devices – including transient/migratory ones, such as mobile and VM-based systems
- Accurately enumerate, qualify, and proactively manage the risk from vulnerabilities present in all types, brands, and models of network devices
- Ensure mission-critical routers, switches, and firewalls are properly updated and that important security settings are always configured in accordance with corporate policies
- Achieve situational awareness by complementing in-depth, point-in-time assessments with always-on, real-time detection and monitoring
- Overcome many of the obstacles that keep security, compliance, and networking teams from working together more effectively
- Limit impact of security breaches on production operations

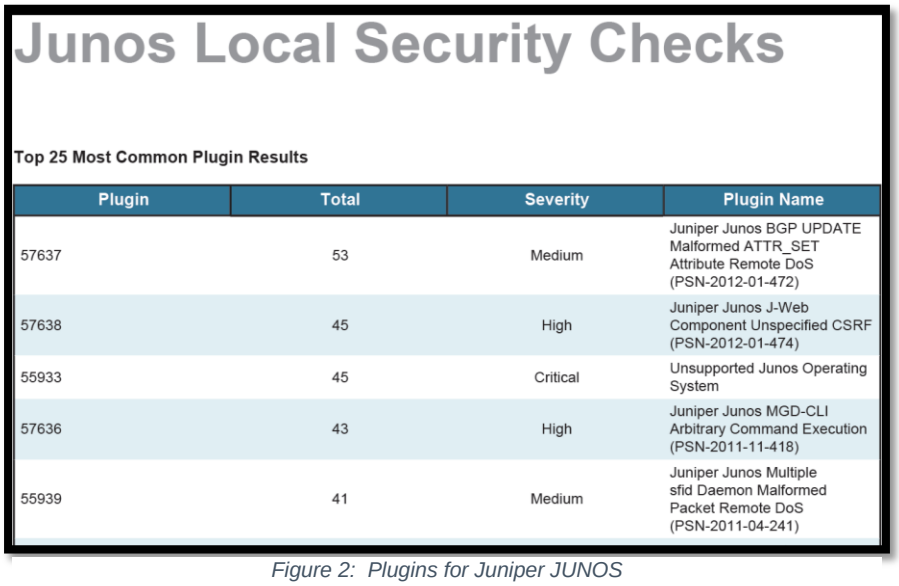
Network Infrastructure Discovery and In-Depth Vulnerability Assessments

Organizations may have rogue wireless access points, employee-installed workgroup switches, hundreds of distributed sites, “open” environments as well as IPv6 networks with immense address spaces. It’s easy to miss something in such

an environment. Virtual system/multi-tenancy technologies change the game entirely by allowing a single physical device to act as many, individually configurable instances of the same solution.

The Tenable solution addresses all of these scenarios. The high-speed asset discovery capabilities of Nessus and always-on network monitoring and decoding capabilities of PVS ensure that nothing slips through the cracks, including all types of network devices. The completely passive approach of PVS is also particularly attractive as it eliminates the risk of "knocking devices over" and minimizes the introduction of new traffic on the network. Complete coverage is even provided for IPv6 networks and devices, which can be extremely problematic for solutions limited to traditional "ping sweep" discovery techniques.[2]

Discovery of a new network device can also be used to automatically trigger an immediate scan for known vulnerabilities, and/or to assign the device to an asset group that is scheduled to receive similar scans on a periodic basis. Nessus not only has entire families of checks for Cisco devices, Juniper equipment, and network firewalls, but also provides extensive checks for a wide variety of devices from other vendors, including everything from load balancers and wireless access points to IP telephony components, VPN concentrators, web application firewalls, and other types of security gateways.



Plugin	Total	Severity	Plugin Name
57637	53	Medium	Juniper Junos BGP UPDATE Malformed ATTR_SET Attribute Remote DoS (PSN-2012-01-472)
57638	45	High	Juniper Junos J-Web Component Unspecified CSRF (PSN-2012-01-474)
55933	45	Critical	Unsupported Junos Operating System
57636	43	High	Juniper Junos MGD-CLI Arbitrary Command Execution (PSN-2011-11-418)
55939	41	Medium	Juniper Junos Multiple sfid Daemon Malformed Packet Remote DoS (PSN-2011-04-241)

Figure 2: Plugins for Juniper JUNOS

Coverage is provided between periodic in-depth Nessus vulnerability scans via the always-on assessment capability of Tenable PVS, which also includes checks for Cisco, Juniper, and Check Point devices, among others. PVS analyzes the traffic generated from its defined focus network and reports any anomalies or vulnerabilities observed. Unlike an active scanner, it does not target network devices with port scans or queries - it simply observes the traffic that these devices are generating as a normal part of their operation.

Automated Configuration Audits for Security and Compliance

The Tenable solution also enables in-depth auditing of software updates and configuration for network infrastructure.

A credentialed inspection is used to efficiently and precisely determine the patch level or operating system level of a given device. This information is then compared to a master list to ensure the device is compliant with corporate standards.

Configuration audits work in a similar way, but are much broader in scope. In this case, the Tenable solution:

- Collects detailed configuration information from each network device
- Compares the results with corporate policies and applicable best-practices guidelines – such as DISA STIGs and benchmarks from the Center for Internet Security (CIS) – all of which are codified in an extensive library of

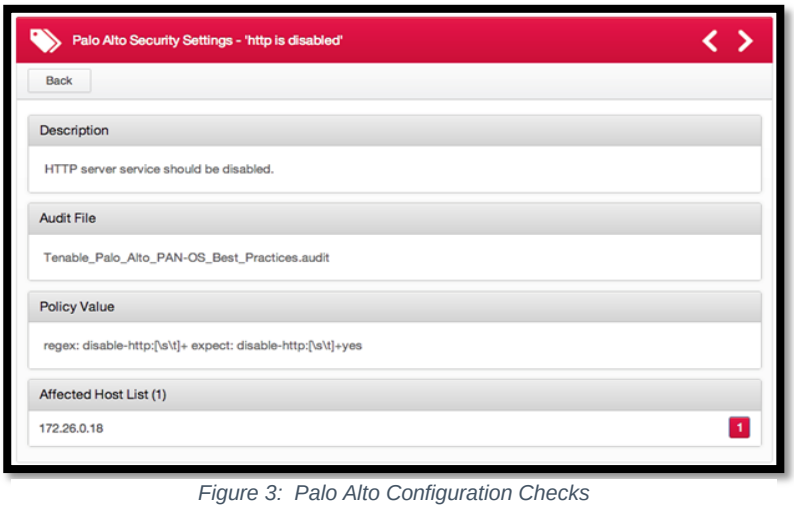


Figure 3: Palo Alto Configuration Checks

pre-defined and customizable audit files
- Leverages PVS for ongoing, real-time monitoring of configuration status
- Reports on findings, both as means to drive security improvements and to support internal and external compliance audits

The goal with these audits is to ensure that important security settings are properly configured – such as setting the remote management interface to utilize HTTPS (vs. HTTP), to require a certain level/type of authentication. The solution is also flexible enough for administrators to automatically inspect just about any configuration parameter that might be of interest to the organization. Tenable's support for Palo Alto Networks next-generation firewalls demonstrates this point.

By automatically logging into a Palo Alto Networks firewall and taking advantage of its XML API, the Tenable solution can be used to:

- Audit/verify a wide range of firewall settings
- Ensure the presence and currency of associated content subscriptions (e.g., for application, anti-virus, URL filtering, and threat signatures)
- Query more than 40 pre-defined, device-level reports – such as Top Applications, Top Attackers, and Spyware Infected hosts – and include the results in a Nessus report
- Establish additional compliance checks based on the content of these reports, for example, to alert on the presence of unsafe/undesirable application traffic on the network

Overall, the Tenable solution conveys several important advantages in this area:

- It enables in-depth audits of network devices
- It combines active auditing techniques with passive technology that is completely non-disruptive and that efficiently accounts for dynamic environments by eliminating the time gaps between active scans and periodic audits.
- It doesn't require any further tools or management systems beyond those already used for device discovery, vulnerability assessment, and the other capabilities covered below.
- In contrast to many competing solutions – which don't support software update audit and configuration audit for network devices at all, or support only one vendor (e.g., Cisco) – it provides coverage for a wide variety of network equipment using any of these popular operating systems:
    - Check Point GAiA
    - Cisco Nexus (NX-OS)
    - Cisco IOS
    - Cisco IOS-XE
    - Juniper Junos
    - Palo Network PAN-OS

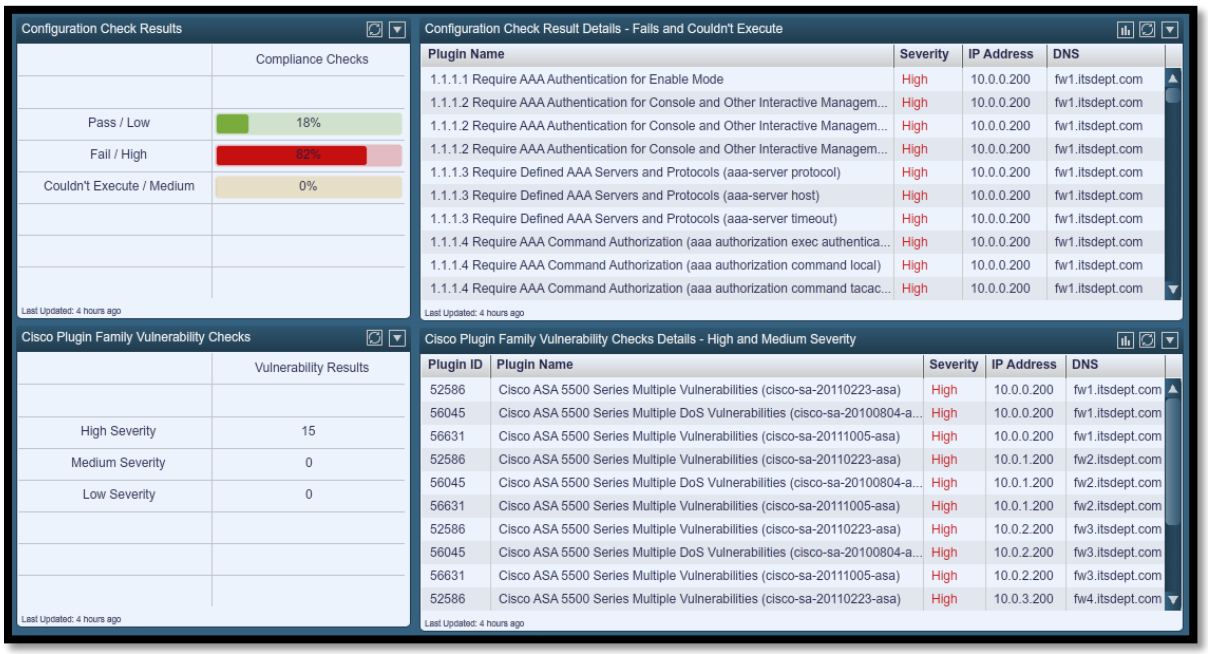


Figure 4: Dashboard showing both configuration and vulnerability audits for a Cisco firewall

Advanced Boundary Audits and Attack Path Detection

Effective network security (and compliance) ultimately demands more than confirming that a device's individual security settings are properly configured. It is also important to validate that configured access policies are working as intended and that there are no unintended holes that allow traffic to cross boundaries it shouldn't be crossing. Typically, this entails detailed analysis and modeling of complex firewall rule sets, an endeavor that requires considerable manual effort and/or specialized tools.

IT security departments can leverage the Tenable Unified Security Monitoring platform for this purpose as well. By strategically locating and configuring a combination of Nessus and PVS instances to inspect boundary devices (e.g., for open ports) and monitor both ingress and egress traffic, administrators can gain extensive insight into the policies being enforced by the devices – and, more importantly, those that aren't. All of this data can be used for alerting, trending, and reporting.[3]

This same data can be combined with other information obtained via the Tenable platform to enable yet another invaluable capability: attack path detection. By stitching data about devices that have vulnerabilities for which there are known exploits together with details about the trust relationships between different devices and the aforementioned boundary audit results, security analysts can readily identify open paths through which attackers can gain access to a network. The results can then be used to effectively reduce risk by more accurately prioritizing remediation and mitigation activities based on the potential for a vulnerable device or host to act as stepping stone to high-value resources. The following dashboard demonstrates what has changed in the network in the past month by tracking new vulnerabilities of high or medium severity that are exploitable with CVSS score of 10 and that are Internet facing.[4]

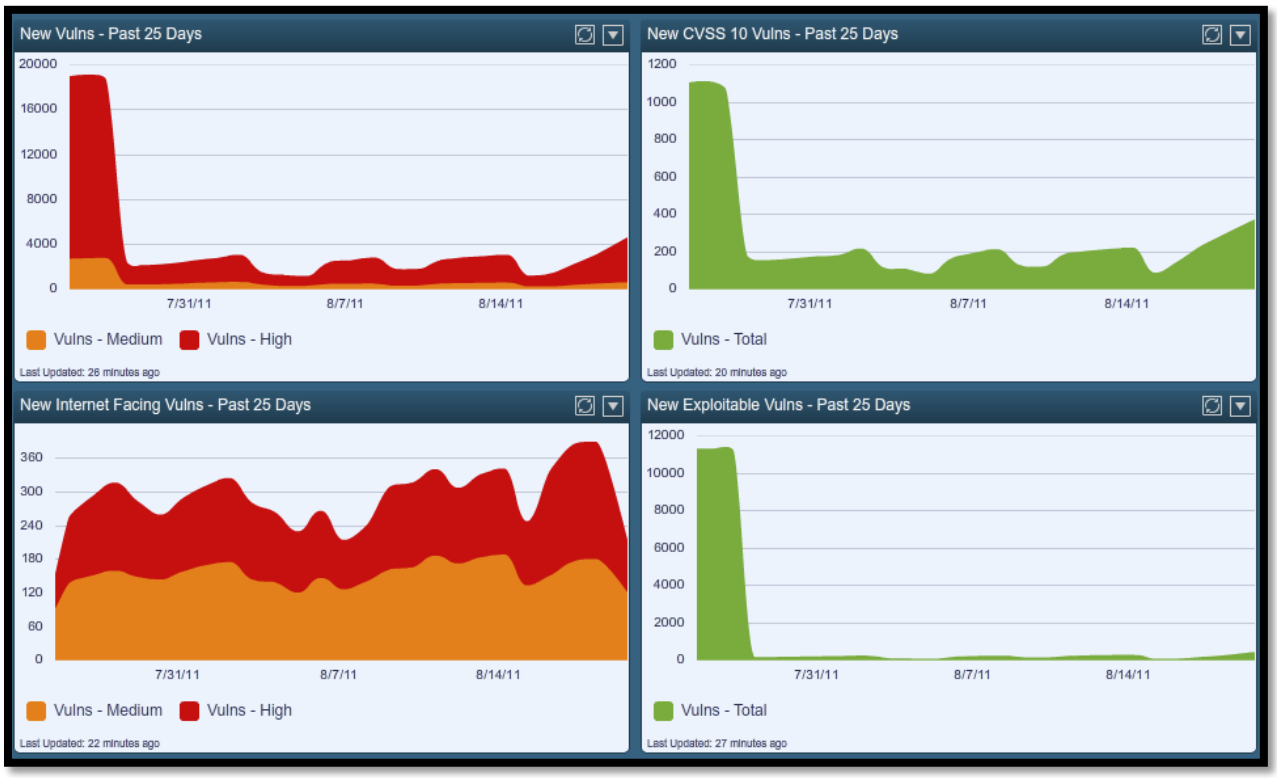


Figure 5: Dashboards illustrating attack paths

Continuous Monitoring and Enhanced Situational Awareness

Tenable LCE also facilitates and extends the continuous monitoring capability. In particular, network infrastructure logs aggregated and normalized by LCE can serve as another invaluable mechanism for real-time change and vulnerability detection. The system can easily be configured, for example, to alert on logs indicating that new administrative accounts have been provisioned for a given set of network devices, or that new ports have been opened on a firewall.

Figure 6: Monitoring Firewall Deny Events

Administrators can use SecurityCenter to view numerous dashboards and reports, subsequently drilling down to obtain further detailed information about specific network devices, their vulnerabilities, and any relevant configuration audit findings. IT can also track important trends, including the total number of devices detected over a period of time, or the total number of devices with high severity vulnerabilities and/or compliance discrepancies.

Overall, the ability to thoroughly and efficiently discover, assess, audit, and monitor the network infrastructure provides IT operations with substantially greater situational awareness than they would otherwise have. The resulting information can be leveraged for any number of purposes, such as:

- Normalize, correlate, and analyze event log data from a single console
- Store, compress, and perform full-text search for rapid attack analysis
- Demonstrate compliance with internal and external mandates efficiently
- Continually assess security and compliance posture through flexible reporting and consistent metrics
- Reduce Incident Response times when investigating and mitigating security incidents.

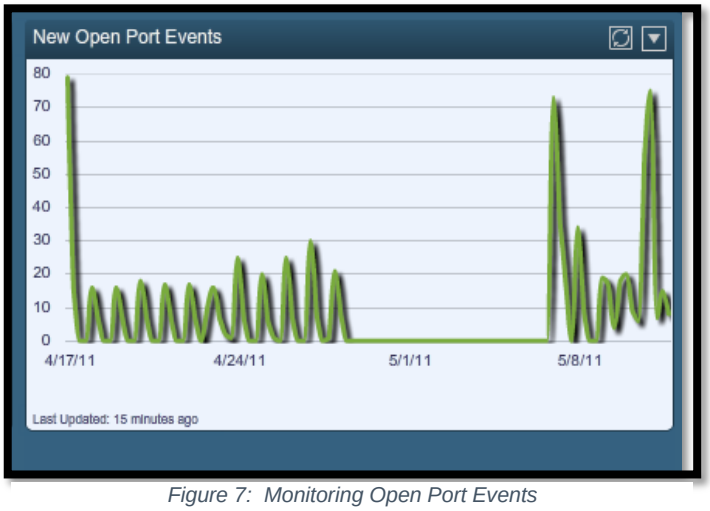


Figure 7: Monitoring Open Port Events

Another major benefit of the Tenable solution is its ability to improve the relationship and ongoing interactions between an organization's security, compliance and networking teams. This is accomplished by utilizing an approach that inherently reduces the impact on the network while also enabling the security team to more thoroughly and effectively convey the impact of discovered vulnerabilities, threats, and configuration errors on both network availability and the organization's ability to comply with applicable regulations, legislation and standards.

Conclusion

Network infrastructure is by no means immune to vulnerabilities and threats. Tenable's Unified Security Monitoring platform overcomes the limitations of traditional tools and technologies by providing enterprises with the solution they need to thoroughly and efficiently assess, audit, and continuously monitor these absolutely crucial resources. Benefits that enterprises stand to gain include the ability to reduce IT security risk, reduce IT security infrastructure TCO, and vastly improve their situational awareness with regard to the security, compliance, and operational status of their networks. Don't wait for a security breach to demonstrate the need for network infrastructure updates.

Footnotes:

1. Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0, October 2010

2. Tenable White Paper, *"IPv6 Requires Fundamental Changes to Vulnerability Management Programs"*

3. Tenable White Paper, *"Firewall and Boundary Auditing"*

4. Tenable White Paper, *"Boosting Your Network Defenses with Tenable's Integral Attack Path Analytics"*

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com

tenable network security