Tenable and Sourcefire

Leverage Tenable vulnerability intelligence to improve operational efficiency of your Sourcefire investment

Key Challenges

The cyberthreat detection capability of a high-quality next-generation intrusion prevention system (NGIPS) is mission critical for any organization. Sourcefire's NGIPS solution generates an 'Impact Flag' for intrusion events based on target host attributes derived through passive analysis. While analysts can use this flag to focus on those events that have the highest likelihood of impacting the business, there are many situations where network visibility is limited, which can result in blind spots. In addition, patch status cannot be determined passively, which can increase the number of false positives even further and hinder auto-tuning capabilities.

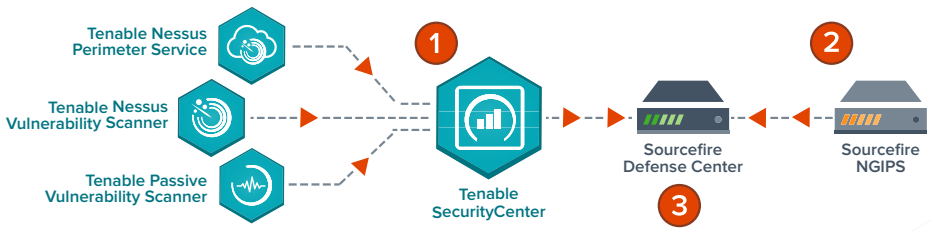
Without integrated vulnerability intelligence from a reputable vulnerability management solution, Sourcefire customers face the following challenges:

- Lack of visibility for network segments not yet monitored by Sourcefire FireSIGHT
- A fully patched targeted host may still generate a high-impact (Impact Flag 1) intrusion event, unnecessarily consuming security analyst resources
- Incomplete host intelligence to support automated detection policy tuning from only those network segments monitored by FireSIGHT

Solution Overview

Sourcefire's innovative FireSIGHT technology constantly profiles the network and logs host attributes—including potential (not actual) host vulnerabilities—into a host database contained within the Sourcefire Defense Center management console. Defense Center relies on this host intelligence to assess the impact of intrusion events and to determine which threat-detection rules are relevant to the protected network. Tenable SecurityCenter aggregates vulnerability scan data from Nessus scanners and Passive Vulnerability Scanner (PVS) devices and imports it into the Defense Center host database to extend Sourcefire's network visibility, strengthen impact assessment, and improve the quality of automated detection policy updates. Customers get the best of both worlds and the most accurate intrusion event prioritization possible.

How it Works



Step 1: SecurityCenter vulnerability data is periodically imported into the Defense Center host database via the Sourcefire Host Input API.

Step 2: Sourcefire NGIPS appliances detect threats and report them to Defense Center as intrusion events.

Step 3: Defense Center correlates threats against actual (not potential) host vulnerabilities to assign impact flag ratings. It also generates recommended detection policy updates based on host intelligence derived from both FireSIGHT and SecurityCenter.

Solution Components

- Tenable Nessus vulnerability scanners and/or Nessus Perimeter Service
- Tenable Passive Vulnerability Scanners (PVS)
- Tenable SecurityCenter management console
- Tenable SecurityCenter API
- Sourcefire NGIPS appliances with FireSIGHT
- Sourcefire Defense Center management console with FireSIGHT
- Sourcefire Host Input API

Key Benefits

- Extended visibility of network segments not yet monitored by FireSIGHT
- Improved accuracy of threat impact assessment
- Optimized detection policy updates
- Increased security and reduced operating risk
- Reduced total cost of ownership (TCO)

The Defense Center dashboard enables security analysts to view the impact of intrusion events as threats are correlated against actual (not potential) host vulnerabilities.

Integration Benefits

Tenable SecurityCenter makes Sourcefire's already-powerful NGIPS solution even better by incorporating highly accurate active and passive vulnerability intelligence into Sourcefire's impact assessment and automated policy tuning capabilities. Now threats are correlated against actual—not potential—host vulnerabilities, and detection policy updates now account for hosts on network segments not yet monitored by FireSIGHT.

The benefits of integrating Sourcefire with Tenable SecurityCenter are compelling:

- Extended visibility of network segments not yet monitored by FireSIGHT
- Improved accuracy of Defense Center's threat Impact Flag assessment capability, reducing the number of 'Impact Flag 1' intrusion events
- Optimized detection policy updates as recommended policy changes now account for hosts not currently monitored by FireSIGHT
- Increased security effectiveness and reduced operating risk
- Reduced total cost of ownership (TCO) as security analysts can now focus on those intrusion events that matter most

About Sourcefire

Sourcefire, a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize security risks to their dynamic networks, endpoints, mobile devices and virtual environments. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire's threat-centric approach provides customers with Agile Security that delivers protection before, during and after an attack. Trusted for more than 10 years, Sourcefire has earned a reputation for innovation, consistent security effectiveness and world-class research all focused on detecting, understanding and stopping threats. For more information about Sourcefire, please visit www.sourcefire.com.

About Tenable

Tenable Network Security is relied upon by more than 17,000 organizations in over 100 countries, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats, and compliance-related risks. Its award-winning Nessus and SecurityCenter solutions have received the highest-possible rating in Gartner's MarketScope for Vulnerability Assessment and continue to set the standard for identifying vulnerabilities, preventing attacks, and complying with a multitude of regulatory requirements. For more information about Tenable, please visit www.tenable.com.

For More Information

Questions, purchasing, or evaluation:
subscriptions@tenable.com or 410.872.0555, x506
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security