INTEGRATION BRIEF

Mitigate Zero-Day Threats

With Palo Alto Networks Next Generation Firewall (NGFW) and Rapid7 InsightVM or Nexpose

A major problem facing today's security teams is the ability to quickly respond to threats in an efficient manner. By combining Rapid7 InsightVM* or Nexpose and Palo Alto Networks Next Generation Firewall (NGFW), you can tackle that problem by seamlessly managing your assets based on the dynamic asset groups established in your Rapid7 vulnerability scanner; this allows your team to apply security policies to your dynamic asset groups, combining those policies with the vulnerabilities and risks flagged during scans.

The interoperability between these best-of-breed products creates a solution that helps identify and mitigate zero-day threats quickly. By being able to effortlessly tag and restrict access to these assets, security teams can rapidly remove threat vectors within their environments.

THE TECHNOLOGY: INTEGRATED NEXT GENERATION FIREWALLS

Incorporating the dynamic asset groups from InsightVM with Palo Alto Networks NGFW gives you the ability to quickly pivot between the two products with the same asset mapping in both GUIs. This mirrored view allows you to trust the data you are viewing and more quickly respond to vulnerabilities and zero-day threats to the network.

HOW IT WORKS

First, run a scan in InsightVM and establish dynamic asset groups for all assets. Once the Ruby Gem (available free to download) is installed and run, it will then pull the asset and group data. The Gem then creates the corresponding tag in the Palo Alto Networks NGFW and assigns the assets accordingly. Security policy within the firewall can then be assigned to the asset groups. By applying a simple cron job to the Gem, you can make this an automated solution, giving you greater visibility into the assets on your network.

INTEGRATION BENEFITS

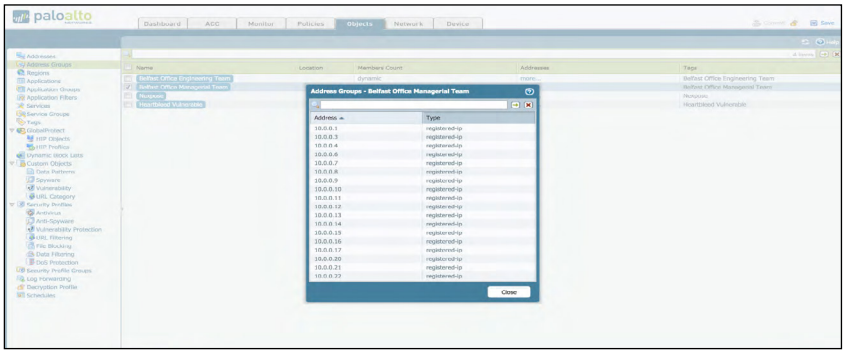
- Automate security policy for new Palo Alto Networks assets utilizing dynamic asset groups
- Quickly identify and mitigate zero-day threats
- Enhance network visibility
- Configure and deploy via Ruby Gem easier than before

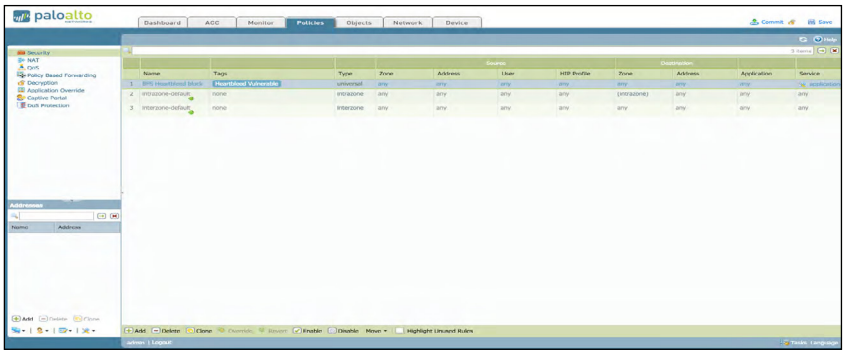
*All mentions of Rapid7 InsightVM associated with its integration with Palo Alto Networks Next Generation Firewall (NGFW) also apply to Rapid7 Nexpose.

Overview of the Integration Process

- Step 1: User creates asset group in InsightVM
- Step 2: User runs the Integration Gem with the asset group in the configuration
- Step 3: Gem polls InsightVM for the assets in the asset group
- Step 4: Gem creates the tag in PAN NGFW with the name of the asset group ("Linux Web servers") if it's not already created
- Step 5: Gem registers the IP addresses of the assets in PAN NGFW with the tag created in Step 4
- Step 6: User applies a policy for the group in PAN NGFW
- Step 7 (Optional): User runs Gem a second time (via cron job or manually) and InsightVM finds new assets in the asset group; user goes back to Step 5

Figure 1: PAN-tagged asset groups via InsightVM (or Nexpose)





What You Need

- Rapid7 InsightVM or Nexpose
- PANOS 6.0

About Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection basedon what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

About Rapid7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for organizations across the globe.

To learn more about Rapid7, visit www.rapid7.com.

SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113, or through our support portal.