Palo Alto Networks and ServiceNow

Firewall management made easy—bridge IT, security, and risk

The Challenge

Enterprise IT and security experts are under increasing pressure to manage complex network environments and keep up with growing business demands. Lack of centralized visibility of critical network firewalls hinders the ability to deliver services and applications reliably. Regulatory and corporate compliance requirements, such as SOX, PCI DSS, and ISO 27001, mandate data visibility and automated policy governance for firewalls. With rapid migration to the cloud, IT and security teams often come across orphan firewall policies, increasing exposure to external threats.

ServiceNow IT Operation Management Visibility

The ServiceNow ITOM Visibility product gives an accurate, up-to-date view of IT infrastructure and services, spanning multi-cloud and on-premises environments. The ServiceNow solution automates the end-to-end infrastructure discovery and service mapping process, including tracking ongoing changes and creating a reliable record in the configuration management database (CMDB). This infrastructure and service information is seamlessly leveraged by products across customer, employee, IT, and security teams.

ITOM Visibility provides two key features for IT and security teams:

- **Discovery** provides visibility into the network's physical and logical entities, such as servers, switches, routers, virtual machines, storage elements, databases, and applications. It also discovers relationships between them, creating dependencies by identifying communication flows down to the TCP port and process level. Along with infrastructure, Discovery identifies TLS certificates to aid in risk management.
- **Service Mapping** builds on the Discovery data, creating end-to-end topology maps of services. It identifies all of the infrastructure entities that support each service, along with their service-specific relationships. This includes mapping complex service topologies that incorporate shared and redundant elements, such as an enterprise bus or server cluster.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls (NGFWs) inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The applications and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies.

Palo Alto Networks Panorama™ network security management offers easy-to-implement centralized management features to provide insight into network traffic, logs, and threats as well as simplify configuration, deployment, and management of Palo Alto Networks ML-Powered NGFWs.

For more information, visit paloaltonetworks.com/network-security/next-generation-firewall.

Palo Alto Networks and ServiceNow ITOM

ServiceNow integrates with Panorama to create a leading network security solution connecting IT, security, and compliance teams. ServiceNow extracts useful information, such as policies, tags, source and destination IP addresses, network zones, users, applications, and ports. The ServiceNow CMDB is the central system of record, allowing IT and security administrators to access the same data as needed.

Use Case No. 1: Gain Complete Visibility into the State of Every Firewall

Challenge

With physical and virtual form factors, organizations may have thousands of firewalls and even more policies. This complexity is difficult to manage if they're unable to centrally track these deployments, such as firewall inventory, versions, patches, and vulnerabilities associated with them.

Solution

ServiceNow collects unified asset inventory and policies from Palo Alto Networks NGFWs and maintains the data in

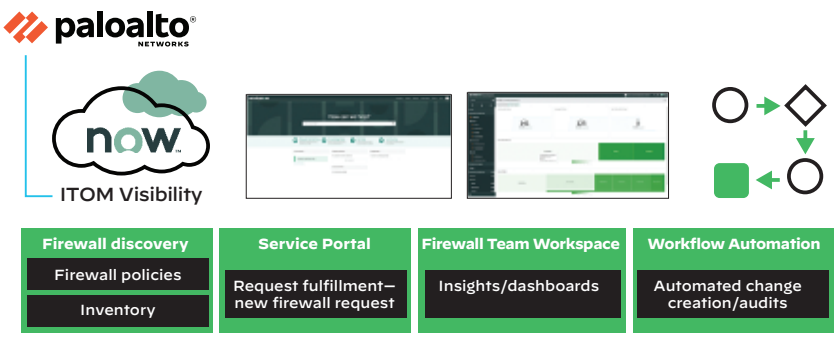

Figure 1: End-to-end ServiceNow and Palo Alto Networks firewall management flow

ServiceNow CMDB to enable tracking of firewall assets for IT service and operations management use cases. The joint solution enables complete visibility of your firewall deployments and firewall policy ownership.

Use Case No. 2: Automate Policy Change Requests Across IT, Security, and Risk Teams

Challenge

Requesting new firewalls, rules, and changes is a complex process. With manual change and infrastructure management processes, organizations often have outdated rules and inventory that can compromise compliance and increase risk.

Solution

Panorama contains firewall configurations and policies that can be shared with ServiceNow to digitize the workflow end-to-end. Using ServiceNow Service Portal, application and IT administrators can request new policies and rules for firewalls. An out-of-the-box firewall request management workflow automates change record creation, saving time and manual effort. This happens automatically without hindering productivity, and changes are routed back to Panorama for execution. The overall process improves security posture and reduces the risks of compliance failures.

Use Case No. 3: Automated Firewall Policy Audit

Challenge

With manual change and infrastructure management processes, organizations often have outdated rules and inventory that can compromise compliance and increase risk.

Solution

On-demand firewall audits detect compliance issues and lapses in firewall ownership. Identifying orphan policies in the system can improve overall security posture, reducing risk and increasing compliance. Additional capabilities in the ServiceNow Governance Risk and Compliance (GRC) application can take compliance further. ServiceNow GRC identifies potential risks associated with orphan policies that should be addressed before they cause widespread problems.

Palo Alto Networks and ServiceNow Product Integrations

Product integrations between Palo Alto Networks and ServiceNow include:

- Palo Alto Networks NGFWs and ServiceNow IT Service Management (ITSM)
- Palo Alto Networks NGFWs, Panorama, and ServiceNow ITOM

About ServiceNow

ServiceNow makes work, work better for people. Our cloud-based platform and products streamline and simplify how work gets done. We deliver digital experiences that help people do their best work fast, creating great employee and customer experiences. ServiceNow (NYSE: NOW) works for you. To learn more, visit servicenow.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

Contact your Palo Alto Networks or ServiceNow sales representative to learn more.

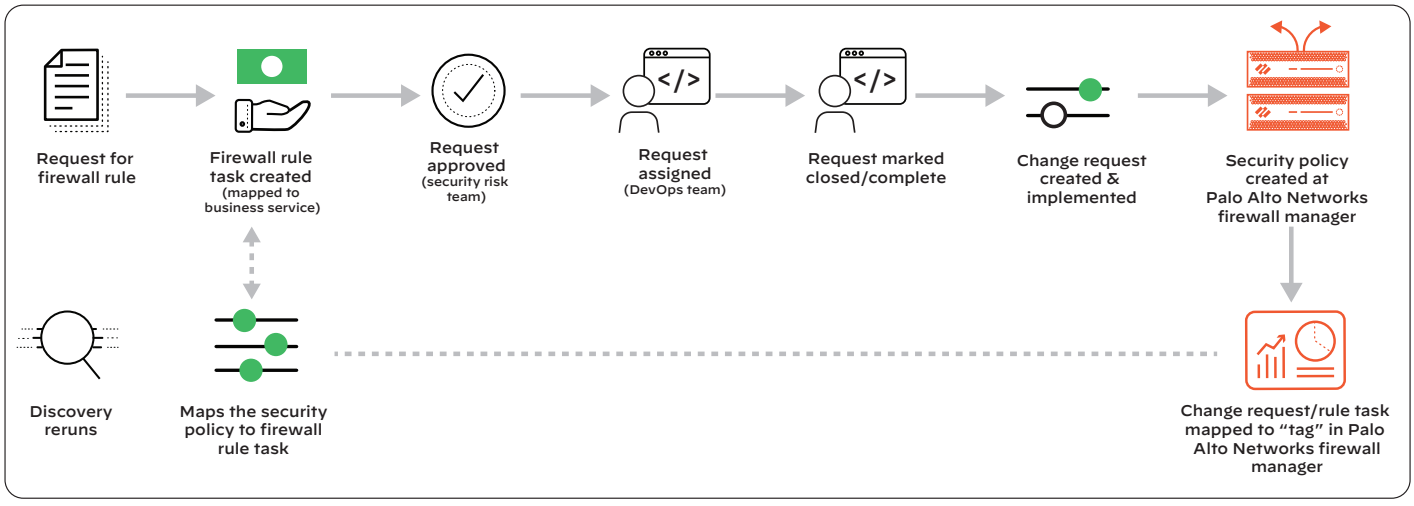

Figure 2: Automated firewall request management workflow

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
servicenow-tpsb-092220