ServiceNow® Firewall Audit and Reporting

The IT challenge

Firewalls are a critical component of your IT infrastructure—a crucial front-line defense against increasingly frequent and sophisticated cyberattacks.

Delivering reliable, secure, and responsive services requires a unified firewall management framework. This needs to combine robust policy management with agile firewall change processes, allowing you to respond quickly and safely to rapidly evolving business needs. However, implementing a comprehensive firewall management strategy is a major challenge, particularly if you rely on manual processes. Here's why:

- **Lack of firewall visibility.** If you don't have visibility of your firewalls, you can't manage them. IT organizations often have hundreds of physical and virtual firewalls, and even more policies. Tracking all these manually is next to impossible. Just creating a basic centralized inventory is a huge effort, let alone tracking policies, versions, patches, and vulnerabilities.
- **Disjointed manual processes.** Many IT organizations still use emails and spreadsheets to manage their firewalls. End users have no easy way to request firewall changes, while backend fulfillment processes are time-consuming and error-prone. This drives up costs, slows fulfillment times, and increases operational risk. And, since firewall change processes typically involve both security and IT operations teams, creating end-to-end process visibility is an even bigger challenge.
- **Compliance failures.** Because there is no centralized visibility of firewalls or associated processes, there is no easy way to detect and remediate policy compliance failures. IT organizations can spend millions trying to track firewall deployments, policies, and owners, but they still struggle with audits because of a lack of consistent, timely, and reliable audit data. This results in issues such as orphaned policies, which pose a significant security risk.

The ServiceNow solution

With ServiceNow® Firewall Audit and Reporting, you take charge of your firewalls, creating centralized visibility, automating end-to-end processes, and avoiding compliance failures (and associated security risks). It lets you manage your firewall policies in the same place you manage the rest of your IT infrastructure, leveraging established ServiceNow processes and capabilities to create a robust, efficient, and secure firewall management framework.

Firewall Audit and Reporting:

- Discovers your firewalls along with their policies, versions, and other attributes.
- Creates a centralized inventory in your CMDB alongside your other infrastructure data.
- Allows end users to easily submit firewall requests through the ServiceNow Portal.
- Automatically routes requests to your security team for risk analysis and approval.
- Routes approved changes to your network firewall team for fulfillment.
- Tracks all changes for audit purposes and also lets admins initiate audits on demand.
- Provides dashboards and insights that deliver comprehensive process visibility.

Gain visibility of your firewalls

Manage your firewall policies in the same place you manage the rest of your IT infrastructure, using ServiceNow Discovery to create a complete, accurate, and up-to-date record of your firewall infrastructure and policies in your CMDB.

Empower end users with self-service

Let IT infrastructure and application owners submit and track firewall requests through the ServiceNow Service Portal, improving the user experience while offloading your network firewall team.

Accelerate and de-risk policy changes

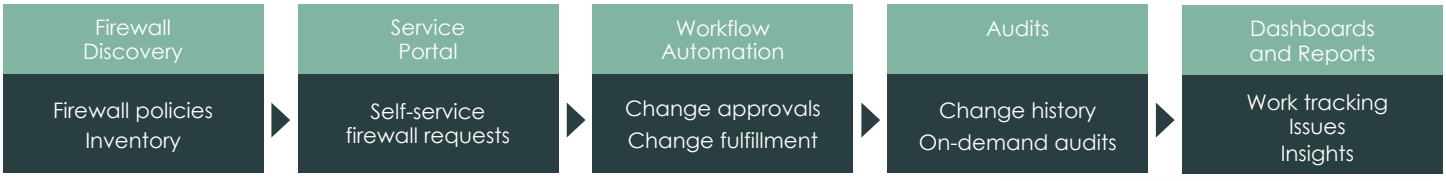
Route firewall requests to your security team for risk analysis, automatically forwarding approved changes to your network firewall team for fulfillment. Associate policies with owners and track the end-to-end policy change process, creating the visibility needed to reduce risk.

Strengthen audits while reducing costs

Leverage comprehensive, accurate firewall policy information and process data to simplify and strengthen your firewall audit processes.

Easily track status and pinpoint issues

Get complete process visibility with a unified dashboard that tracks firewall changes and audit requests, and provides insights into issues such as orphaned policies.

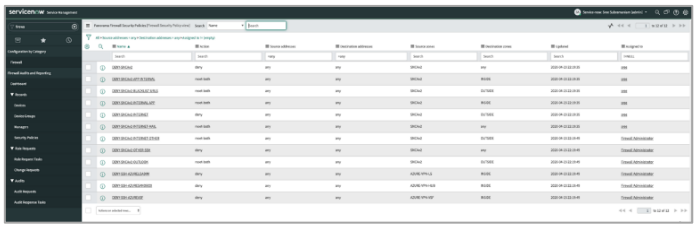


Manage the complete firewall policy lifecycle

Quickly gain visibility of your firewall infrastructure

Firewall Inventory and Audit leverages ServiceNow® Discovery to automatically discover your firewall infrastructure. It currently supports Palo Alto Networks firewalls out of the box and can easily be extended to discover other firewall vendors using Discovery's built-in pattern framework. This lets you configure new patterns for any IP-enabled device with little or no coding.

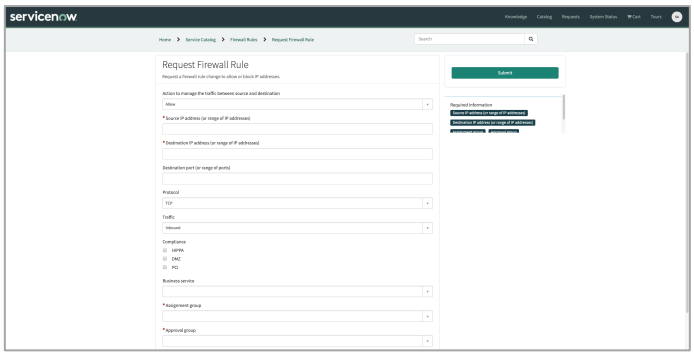
Discovered firewall data, including policies, software and firmware versions, patches, and other attributes are automatically stored in the ServiceNow CMDB, creating a complete, up-to-date, and accurate record. And because the CMDB is built on a consistent common data model, you get a unified, centralized view across firewall vendors. Now your security and network firewall teams can instantly see all your firewall policies and associated owners in one place, as well as the asset data they need to maintain your firewalls and address vulnerabilities.



Instantly see all your firewall policies in one place

Empower end users with intuitive self-service firewall requests

With Firewall Audit and Reporting, you can add firewall requests to your ServiceNow Service Catalog, allowing end users to submit and track requests using the ServiceNow Service Portal. This makes it easy for IT infrastructure and application owners to request firewall rule changes, and it also offloads your network firewall team, which can now focus on managing your firewalls instead of responding manually to user requests and follow-ups.



Easily request firewall changes using the Service Catalog

Automate, accelerate, and de-risk policy workflows

Firewall Audit and Reporting routes firewall requests to your security team for risk analysis and approval. Once approved, it creates a corresponding change request and sends this to your network firewall team to implement the policy change. Simply record the change number in the policy description on the firewall, and Firewall Audit and Reporting automatically associates the policy with the corresponding owner, application service, and other related entities in the ServiceNow CMDB. The entire process is automated and tracked, accelerating policy changes while creating the visibility needed to lower risk.

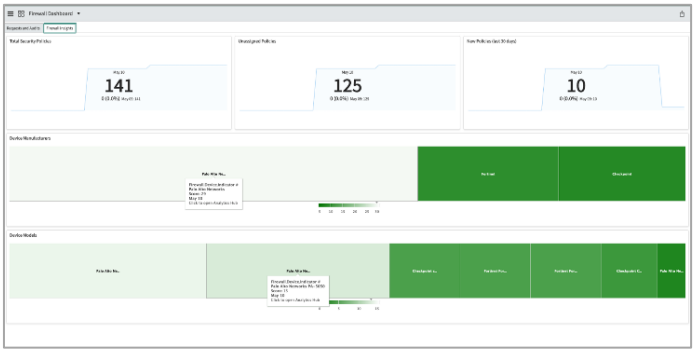
Automated policy workflows

Increase audit coverage and accuracy while reducing costs

Firewall Audit and Reporting provides comprehensive, accurate firewall policy information and associated process data. This allows you to easily audit your firewalls, avoiding costly and error-prone data-gathering exercises. You can also initiate both random and targeted audits, proactively checking firewall hygiene by issuing and tracking audit requests for specific firewall devices or managers..

Easily track status and pinpoint issues with a unified dashboard

Firewall Audit and Reporting comes with a unified dashboard that provides complete process visibility. This includes current firewall changes and audit requests, as well as historical data. The dashboard also provides insights that help you pinpoint issues such as orphaned policies.



Firewall and Inventory Audit Dashboard