Managed Firewall

Last updated 12-01-22

The state's firewalls are the foundation of the security infrastructure at the edge of the internet and again at the edge of each agency within the state network. WaTech teams manage the enterprise Internet edge firewall access rules but agencies may request delegated management of their agency specific firewalls within the state network if they want their technical staff to have an active role in the administration of the agency specific internal firewall rules.

Managed Firewalls are there to protect networks from unauthorized access and malicious attacks. Firewalls are the critical gateway into a network and firewalls managed by WaTech come with the highest degree of attention and expertise to protect critical agency assets and provide peace of mind.

Intended customers

This service is intended for organizations connected into WaTech's digital ecosystem that includes, but is not limited to, organizations connected to the State Government Network (SGN), Intergovernmental network partners (state counties, cities, federal agencies, tribes, health districts) and organizations that are part of the Small Agency Services.

There are approximately 174 WaTech-managed firewalls, and approximately 43 delegated customer-managed firewalls. Agencies are required to maintain compliance with the Washington State IT Security Policy and Standards in a manner appropriate with the sensitivity of the data that resides within the agency network. Agencies are required to provide primary and secondary customer security contacts that will be authorized to request changes to agency rule sets. These security contacts will be verified annually to ensure accuracy of information.

Options available with this service

Managed Firewall services are available in two categories:

- WaTech-managed firewalls are a fully managed firewall solution, including policy and configuration. The service is tailored to meet the customer's changing business requirements.
- Co-managed firewalls offer a solution for agencies that want their technical staff to maintain an active role in the administration of their agency perimeter firewall. State network border firewall rulesets are managed and maintained by WaTech security staff. All firewall rulesets are audited with a third-party tool to identify and mitigate any unintentional access.
- The optional add-on features available for Co-managed Firewalls Intrusion Prevention System (IPS) technology protect your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

Customer engagement

- Semi-annual customer Town Hall with all Network Services teams providing updates and gathering customer feedback.

Helpful information

Service category
Network

Service availability
24/7/365

Planned maintenance
Planned maintenance is performed after hours and coordinated with agency representatives.

Related services
- Transport and Connectivity
- Cloud Highway
- Network Core
- Domain Naming Service (DNS)
- Strong Authentication
- Fortress Anonymous
- Cloud Virtual Private Network (VPN)
- Vulnerability Assessment
- Office Virtual Private Network (VPN)
- Client Virtual Private Network (VPN)

How to request service
Submit a request for service through our Customer Portal.

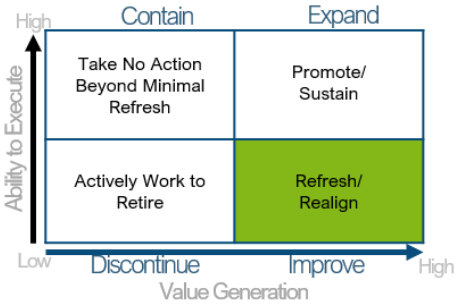
Service owner
Jason Miller

- Monthly Technology Management Council (TMC) and Business Management Council (BMC) meetings for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- Regularly scheduled meetings between customers and Business Relationship Managers (BRM) to connect, advise, address concerns and provide solutions.
- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives, and services.
- Requests for new consultations and modifications to existing applications.

Action plan

Current activity

- Continuous auditing and reviewing of all firewalls for suspicious traffic as well as firewall subscription services to allow the blocking of specific geographic regions while actively responding to security threats.
- Updating the software running the firewalls annually.
- Submitting a decision package for the life cycle of the core and edge firewalls. The decision package will include next-generation firewalls that will provide additional security features to the state.



One- to two-year goals

Procure new core and edge firewalls and start the replacement effort of the existing firewalls before they reach end-of-vendor support in September 2024. Identify what next-generation firewall features it may offer and deploy to provide additional layers of security to the state and our customers.

Three- to five-year goals

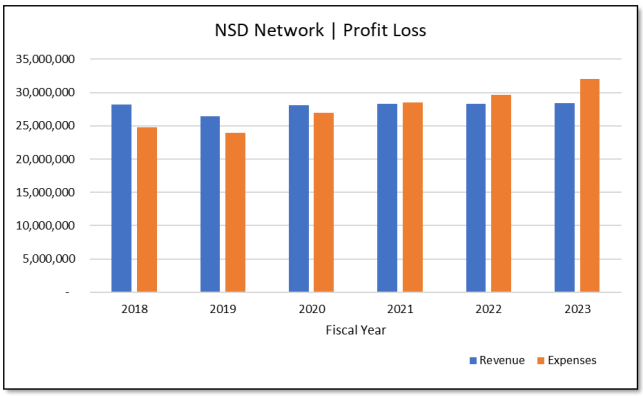
Provide next-generation firewall features such as SSL deep inspection, application firewall and additional intrusion prevention services. Offer these features to our customers and position the state for the future.

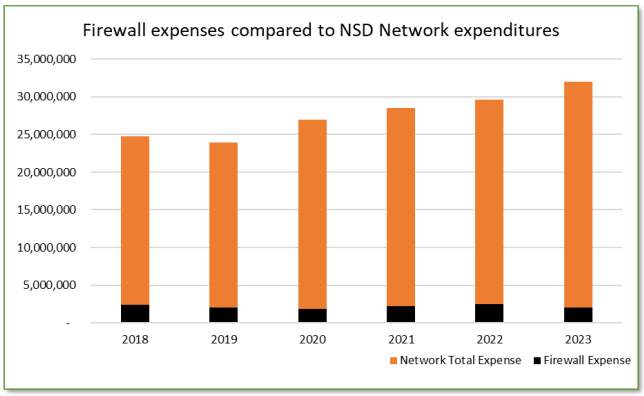
Service review and fully loaded service budget projection

Revenue source

The Managed Firewall budget is primarily funded via the network allocation. Customers that are not included in the network allocation can purchase the service on a pay-per-use basis. Revenue received from this rate structure goes directly against the cost incurred to provide the service.

Net Income over time:





Decision packages

In the 23-25 biennial budget, WaTech will be submitting a funding request to replace the equipment and shift the service to meet the current industry standards.