

Next Generation Firewall FAQs

What is a next-generation firewall with Unified Threat Management (UTM) features?

A Next-Generation Firewall (NGFW) with Unified Threat Management (UTM) features combines multiple security functions into a single device to simplify network protection. Some key features include:

- Antivirus and Anti-malware: Scans for and blocks viruses and other malware.
- Anti-spam: Filters out unwanted email traffic.
- Content and Web Filtering: Blocks access to unwanted websites and content.
- Intrusion Prevention System (IPS): Detects and prevents network attacks.
- VPN: Provides secure remote access to the network.
- Deep Packet Inspection (DPI): Examines the data within network packets to detect threats.

By integrating these features, NGFWs offer comprehensive protection and simplify security management

What's the vision for the NGFW project, and why now?

WaTech's vendor-supported UTM firewalls safeguard the network against security threats while eliminating unnecessary complexity and disparities in security posture. By consolidating redundant security tools within WaTech's and customer networks, IT-related expenses for Washington State are reduced. This coordinated security approach benefits the entire state. With WaTech's existing core and edge firewalls reaching the end of their useful life, the new firewalls will enable WaTech to offer IPS services on core and edge firewalls at no additional cost. Additionally, the new hardware will provide customers with enhanced Next-Generation security features.

Is the NGFW project happening with existing infrastructure or is it something we need to migrate to?

Primarily existing infrastructure. For some features, some extra infrastructure is being added on the WaTech end. Customers will not need to migrate.

What is the cost to add these UTM features?

Web security/Filtering, FortiAnalyzer IOC, Intrusion Prevention System (IPS), and Spam Detection features will be added to the enterprise cost allocation at no additional cost.

FortiSandbox Advance Malware Protection, SSL Decryption, and Identity Based Firewall Policies are currently in the Proof-of-Concept stage. The information gained will help with future prioritization and budget requests.

What training will we need and what will be available to me?

This depends on your current knowledge, job role, and how you plan to use these features. If you'd like a more detailed discussion, you can request a consultation with the Firewall team regarding NGFW-related questions.

If making changes in one environment, will it affect or conflict with each other?

Changes in one should not affect the other.

Would we need to switch to a new firewall environment to implement these UTM features?

The NGFW features will be available on the current WaTech Core Firewall and can be turned on per your request.

How does this project relate to the Security Service Edge (SSE) project?

SSE is for securely connecting users to applications, no matter where they are. NGFW adds additional tooling to the security of traffic inside the state's data centers only.

How do I get started if I want to incorporate these new UTM features?

Use this [Readiness Checklist](#) as a first step to incorporating these features into your agency roadmap and aligning them with your implementation strategy.