Readiness Checklist: Enabling Advanced UTM Features

Checklist for preparing to implement Web Filtering, Spam Detection, or FortiAnalyzer Indicators of Compromise (IOC).

As part of the Next-Generation Firewall Implementation project, customer agencies will have access – at no additional cost to enhanced cybersecurity features. This readiness checklist will help ensure your agency is prepared to activate and integrate these tools effectively.

Research & Training

☐ Review onboarding materials provided by WaTech.

☐ Explore Fortinet's documentation and official training resources for Spam Detection, Web Filtering, and FortiAnalyzer IOC.

☐ Ensure relevant staff have a foundational understanding of each feature's purpose and functionality.

Goals & Requirements

☐ Define the intended goals and desired outcomes for implementing each UTM feature.

☐ Document specific requirements and success criteria for your agency's environment.

Authorization

☐ Confirm that an Authorized Firewall Admin from your agency has reviewed and approved the implementation.

Infrastructure Review

☐ Examine your agency's existing firewall rules.

☐ Understand your current traffic flows and patterns.

☐ Identify critical business applications, systems, and sites to ensure continuity.

Redundancy & Overlap

☐ Determine if your agency is already using other tools that perform similar functions.

☐ Assess whether enabling these UTM features will replace or complement existing solutions.

Schedule Consultation

☐ To obtain services from WaTech after July 1, 2025, view the How to Order section on our Secure Connectivity page.