MANAGED SERVICES → MANAGED FIREWALL

Secure your business with a purpose-built, customized solution

Defend your operations with an arsenal of up-to-date security tools, best practices and experts monitoring your network 24/7/365. Your dedicated Frontier partner will customize a solution for your specific business environment. So you get the right protection while only paying for what you need.

Managed Firewall Packages

We offer 12 managed firewall packages—unique combinations of four models and three service options—along with additional vulnerability management add-ons. You can even add Security Information and Event Management (SIEM) to your non-firewall devices.

FortiGate 40F: 200 VPN Tunnels

Service Levels: Business, Advanced and Enterprise
Throughput:
- → Threat prevention: 600MB

FortiGate 400E: 2,000 VPN Tunnels

Service Levels: Business, Advanced and Enterprise
Throughput:
- → Threat prevention: 5GB

FortiGate 100F: 2,500 VPN Tunnels

Service Levels: Business, Advanced and Enterprise
Throughput:
- → Threat prevention: 1GB

FortiGate 1000D: 20,000 VPN Tunnels

Service Levels: Business, Advanced and Enterprise
Throughput:
- → Threat prevention: 4GB

Frontier BUSINESS

Questions? Contact a Frontier Managed Firewall expert today at 844.244.7118 or visit enterprise.frontier.com/managed-firewall

Managed Service-Level Options

Business

Security appliance, SIEM,
24/7/365 maintenance
4 Fortinet Unified Protection
Security features:

- IPsec VPN
- Stateful firewall
- Remote worker network access
- Application control

Advanced

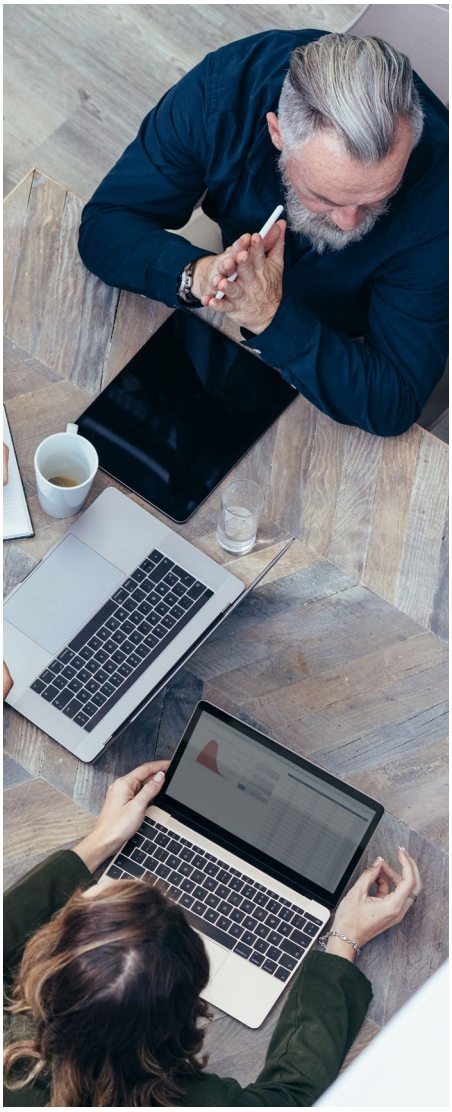
Security appliance, SIEM,
24/7/365 maintenance
All Business Fortinet Unified Protection
Security features, plus:

- Web content/URL filtering
- Antivirus/antimalware
- Intrusion prevention systems

Enterprise

Security appliance, SIEM,
24/7/365 maintenance
All Business + Advanced Fortinet Unified
Protection Security features, plus:

- DNS filtering
- Cloud sandbox
- Botnet protection
- Content disarm and reconstruction
- Antispam



Optional Vulnerability Management Add-Ons

Every time there is a change to any component of your network or infrastructure, like update patches, switches, routers, firewalls and servers, there is the risk of opening new, undetectable security vulnerabilities. Our Vulnerability Management add-ons help you stay ahead of these risks by monitoring every aspect of your information technology.

Continuous Vulnerability Management

Performs the following security activities on a regular basis:

- Identifies internal and external vulnerabilities with details, risk levels and potential impact
- Allows you to quickly find and remediate issues within equipment and applications
- Provides accurate network vulnerability information and streamlined, actionable remediation guidelines to quickly resolve issues

Ongoing Vulnerability Management

- Runs an initial scan to establish a baseline
- Shares results of initial scan to identify high and medium vulnerabilities
- Recommends a remediation plan to resolve any vulnerabilities found during baseline scan
- Investigates the security of your environment after implementation of new components

Reporting and Analytics

- Analyzes basic firewall reports and extends your company's protection through weekly and monthly emails from our team of security experts, summarizing common vulnerability exposures (CVEs), known vulnerabilities, high-risk targets, remediation recommendations and mitigation techniques
- Includes recommendations to improve network security posture
- Provides appropriate regulatory compliance reports, such as PCI, HIPAA and ISO

Frontier BUSINESS

Questions? Contact a Frontier Managed Firewall expert today at 844.244.7118 or visit enterprise.frontier.com/managed-firewall

Optional SIEM for Non-firewall Devices

SIEM is included with all Managed Firewall packages. You may also purchase SIEM as an add-on for your non-firewall devices.

Using state-of-the-art security tools and best-practice techniques for adaptive awareness, SIEM allows our Security Operations Center to detect anomalous behavior and traffic and notify you in the event of an incident. The 24/7/365 proactive monitoring and alerting includes SIEM platform tools, global threat feeds, indicators of compromise, collectors and scheduled reporting as follows.

SIEM Reporting and Analytics

- Research and analysis of event data using cross-correlation tools and methodologies
- Ownership of all proactive and reactive event tickets on your behalf:
  - Analyze events
  - Open incident tickets
  - Categorize threat levels
  - Notify you with appropriate threat response based on event correlation techniques, including threat feeds, common vulnerability exposure (CVE), indicators of compromise (IOC), knowledge base and available data
  - Escalate to appropriate incident level
  - Generate incident ticket

SIEM Incident Management

- Recommendations for best practices and remediation steps
- Documentation of event anomalies, timelines and suspected exposure
- Initial notification of the incident, details and other relevant information about the incident's potential impact

Related Offerings

Evolve, grow and make strides toward your strategic goals with an expert guide at your side. Together, we'll select and layer the Frontier Connectivity, Collaboration and Managed Services Solutions that will help your business thrive into the future.

Managed SD-WAN

MEF certified Software-Defined WAN connects all your local area networks from a central location, giving you total network control.

Cloud Managed Solutions

End-to-end configurations of public, private, multi-cloud and hybrid platforms streamline your infrastructure, reducing costs and ensuring continuity.

Connectivity

Three foundational technologies designed for total network control while building a foundation for your digital future.

Frontier BUSINESS

Questions? Contact a Frontier Managed Firewall expert today at 844.244.7118 or visit enterprise.frontier.com/managed-firewall