WEB APPLICATION FIREWALL (WAF+)

WHY CHOSE NETWORK BOX USA
WEB APPLICATION FIREWALL (WAF+)

NWB WAF+ is a fully managed Web Application Firewall.

Our SOC continuously monitors and manages it on your behalf, so you can sit back and focus on your business while enjoying predictable recurring revenue.

Network Box's Web Application Firewall is fully managed and continuously tuned by a 24/7 Security Operations Center. It provides real-time protection with custom rules tailored to your applications, backed by global, award winning threat intelligence feeds. Integrated into a full-stack managed security platform, it ensures deep HTTP/HTTPS inspection and compliance-ready reporting, making it ideal for organizations that need robust, expert-driven protection without the overhead.

MCES IS POWERED BY NETWORK BOX USA:

BEST-IN-CLASS THREAT INTELLIGENCE

ZERO-DAY THREAT PROTECTION

SELF-OPERATED SECURITY RESPONSE CENTER

3 ISO Certifications
PCI DSS 3.2 attestation
70+ threat intelligence partners

FULLY STAFFED SECURITY OPERATIONS CENTER

UNIFIED MANAGEMENT GUI

WEB APPLICATION FIREWALL (WAF+)

WAF+ BENEFITS

Fully Managed
WAF+ is fully managed and configured by a 24/7 SOC, so no need to handle rules or tuning yourself.

Enterprise-Grade Compliance
Ideal for regulated industries:
Certified for ISO 27001, ISO 9000, ISO 20001, ISO 31000, and SOC.
PCI DSS 3.2 attestation.

DDoS Support with Human Backup
Cloud-based protection with real-time SOC support during DDoS attacks, not just automated mitigation.

Unlimited Domains
While some WAFs restrict domains or charge for more, Network Box supports unlimited domains/subdomains and page rules.

NETWORK BOX USA WAF+ DATASHEET

WEB APPLICATION FIREWALL (WAF+) SERVICE INCLUDES:

- ✓ Protection against OWASP Top 10
- ✓ Firewall: stateful inspection, packet filtering, NAT, advanced routing
- ✓ Intrusion Prevention Systems (IPS)
  - Frontline IPS
  - Inline IPS
  - Infected LAN (Layer 3 and Layer 7)
- ✓ SSL Protection
  - Identifies, decrypts, and scans SSL traffic, subjecting it to security functions (e.g., anti-malware protection, content filtering, and organizational policy enforcement)
  - Allows certificate validation policy to be performed and enforced at the gateway
- ✓ Full integration with DDoS Protection (Layer 3 to Layer 7)
- ✓ IPv4-IPv6 bi-directional translation (Layer 3 to Layer 7)
- ✓ Customizable Log Portal and Reporting Modules
- ✓ 24x7x365 Monitoring and PUSH Updates
- ✓ Granular policy management (e.g., ability to place restrictions on user, path, URL, etc.)
- ✓ High performance rules engine capable of millions of customizable rule-checks per second
- ✓ Internal and external load balancing
- ✓ Response filtering and data exfiltration protection
- ✓ Client authentication
- ✓ WireGuard VPN
- ✓ Perimeter MDR + IRR

ADDITIONAL SERVICES INCLUDED:

- ✓ Threat Intelligence - named top 10 threat intelligence providers to Microsoft
- ✓ 24/7 SOC
- ✓ SIEM – 90 days free for NWB appliances with 90 day rolling access
- ✓ Security Response Center (SRC)
  - 3 ISO certifications
  - PCI DSS 3.2 attestation
  - 70+ threat intelligence partners
- ✓ Standard SLA