WEB APPLICATION FIREWALL (WAF+)

WHY YOU NEED
WEB APPLICATION FIREWALL (WAF)

Since the 1990s, websites have become the primary way that companies exchange information with clients and stakeholders. While a network firewall can stop cybersecurity attacks at the network level, it is incapable of stopping attacks aimed at your web server. and stakeholders.

Given how pervasive corporate websites have become, they are popular attack vectors for bad actors. It is estimated that roughly 50% of all cybersecurity attacks are focused on web applications. A DDoS on a website may even hinder your ability to conduct business and hold your company hostage. The threat to business is real, leading to diminished customer trust, reputation, brand value, share value, as well as direct financial loss.

Because of the significance of the threat, many companies are legally required to have proper security measures in place. A WAF has become one of the most essential security measures to meet compliance requirements.

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

Network Box USA's WAF+ is a multi-level Web Application Firewall that provides comprehensive protection for web servers and web applications. It effectively mitigates attacks and vulnerabilities at the web application layer, while simultaneously providing a load-balanced, fault-tolerant production environment.

Its features include:

- Built-in protection against OWASP Top 10
- Internal and external load balancing
- Powerful rules to protect against common attacks and customizable for specific web applications
- SSL proxy and scanning technology
- SSL offload and upgrade
- Protocol validation and policy restriction
- Response filtering
- Client authentication
- Support for major Content Management Systems, including Joomla, Drupal, and WordPress

WAF+ 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

Network Box USA Web Application Firewall (WAF+) Secures a Business's Web Application

PROTECTING WEB SERVERS AND WEB APPLICATIONS IS JUST AS IMPORTANT AS PROTECTING A NETWORK

WAF+ FEATURES

Comprehensive Protection

Network Box's WAF+ is a multi-level Web Application Firewall that provides comprehensive protection for web servers and web applications. It effectively mitigates attacks and vulnerabilities at the web application layer, while simultaneously providing a load-balanced, fault-tolerant production environment.

Powerful Rules

As a standard, WAF+ is preconfigured with rules to protect against common web application attacks. It is highly customizable with the ability to add/create rules to protect against attacks that target specific web applications. In addition, WAF+ is tightly integrated with our Anti-DDoS module, enabling it to track usage patterns and identity attack sources.

SSL Proxy Technology

WAF+ includes a Secure Socket Layer (SSL) proxy that allows certificate validation policy to be performed and enforced at the gateway. SSL traffic is transparently identified, decrypted and then subjected to policy control and other such security functions. Without SSL Proxy technology, it is impossible to scan SSL encrypted data streams for malware, spyware, and other undesirable content.

SSL Offload and Upgrade

The system can be configured as a terminator for SSL traffic, offloading cryptographic computation workload onto the WAF+, relieving web content servers of significant CPU stress. In addition to the standard SSL Offload feature, Network Box middleware software uses an up-to-date and actively maintained SSL software infrastructure, effectively upgrading a client's secure website to the latest, most secure protocols.

IPv4/IPv6 Translation

Network Box's WAF+ has built in full IPv4/IPv6 translation capabilities. You can set up your servers with a public IPv6 IP address without having to change any settings on the servers themselves.

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 rule-checks per second

ADDITIONAL SERVICES INCLUDED:

✓ Standard SLA

✓ 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

✓ Threat Intelligence - named top 10 threat intelligence providers to Microsoft