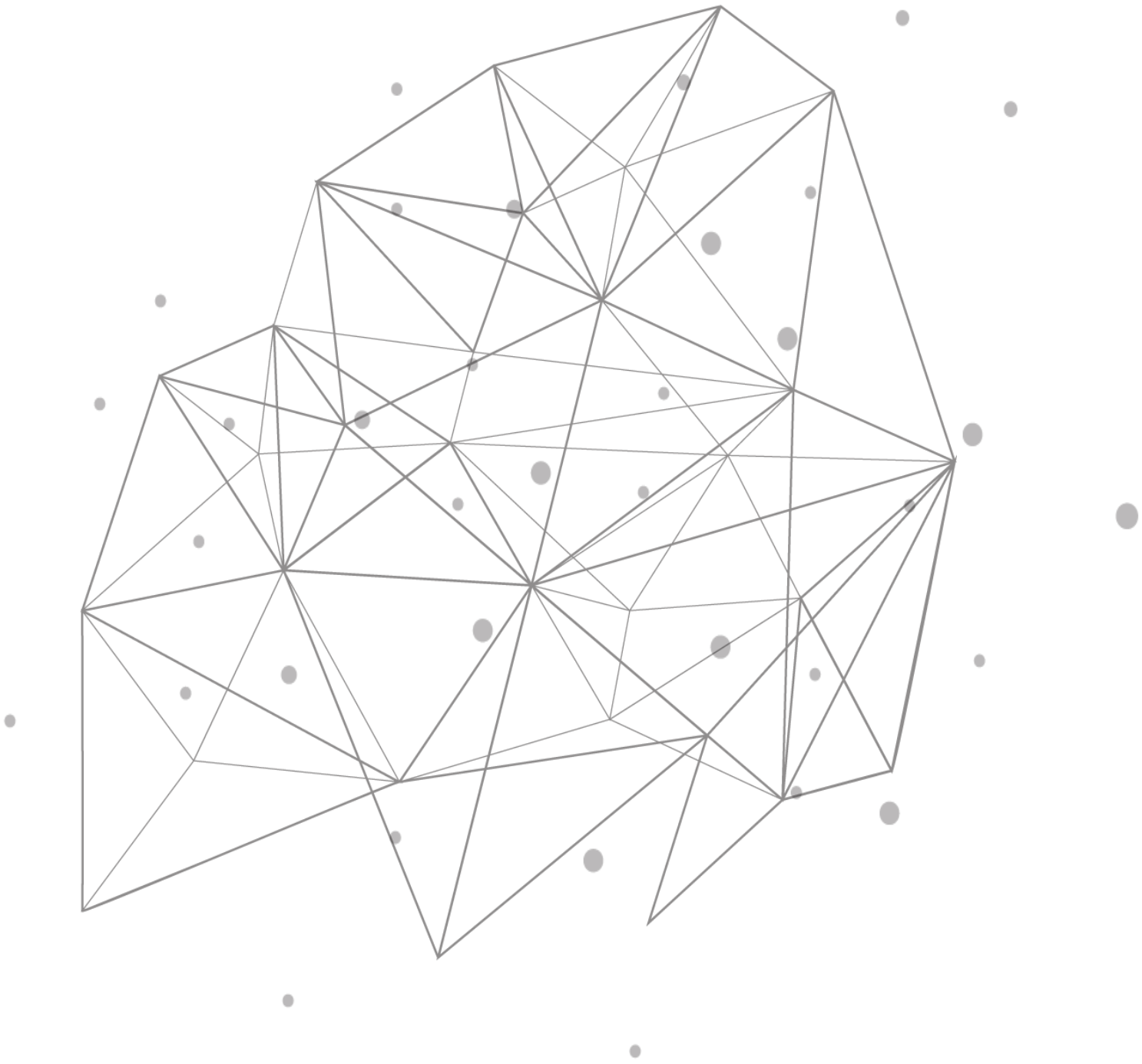
TCPWave

Security Features



Introduction

With the rapidly evolving technological landscape, cyberthreats are intensifying. The graph of the cyberthreats is elevating to a point where there is no sign of it slowing down. TCPWave security solutions help enterprises understand the network security vulnerabilities that threaten the enterprise‘s ecosystem. Furthermore, it prepares organizations for combating cyber-attacks proactively. TCPWave security features address the enterprise’s needs and help in streamlining the security operations.

DNS Access Control List

The DNS ACLs defined in the TCPWave IPAM allow the network administrators to restrict the source IP addresses that can query DNS. The dynamic modifications to the ACLs are audited and propagated to all the DNS remotes in real-time.

Dual DNS Engines

TCPWave’s Dual DNS feature provides resistance to certain types of attacks and increased reliability. With Dual DNS, if the BIND DNS service stops running—due to an attack that exploits a BIND vulnerability, a malfunction, or another reason—then failover to another DNS service will occur. The failover is automatic to Unbound caching. This failover ensures that users continue to have access to DNS service even if BIND crashes.

DNS Firewall

TCPWave’s Advanced DNS Firewall, integrated into TCPWave’s DNS appliances, allows the configuration of multiple firewall templates in IPAM. The rules that are set in the template drop malicious traffic, thus improving DNS stability and performance. Rules can be specified for various protocols, including UDP and TCP, and are dynamically updated via REST API calls.

DNS Response Policy Zones (RPZ)

TCPWave IPAM’s integration with the DNS Response Policy Zones (RPZ), a layer-7 firewall that blocks malware, phishing, ransomware sites, and botnets, contains rules that recursive DNS appliances use to redirect or block queries for malicious sites. TCPWave supports customization of RPZ rules and files then fetches RPZ data feeds from popular reputation data providers, such as ThreatSTOP and Deteque. Using data feeds, possibly supplemented with custom rules, DNS RPZs provide an effective firewall that prevents users from accessing harmful sites.

DNS Security Extensions (DNSSEC)

DNSSEC provides functionality for DNS resolvers (clients) to authenticate that the source of query responses is trustworthy and confirms the responses' integrity. TCPWave fully supports DNSSEC deployment and provides automatic DNSSEC key generation, zone and key signing, and key rollover.

Response Rate Limiting

Response Rate Limiting (RRL) is an enhancement to the DNS protocol, which serves as a mitigation tool for the DNS amplification attacks. RRL implementation is recommended only for the authoritative servers but can also be implemented for cache servers. RRL uses a credit or token bucket scheme.

Machine Learning-Based DNS Tunnel, DGA, and Anomalous Traffic Detection

TCPWave's DNS TITAN, a machine learning module, inspects DNS traffic in real-time to detect DNS tunnels, traffic associated with domain generation algorithms, and other anomalous traffic. In addition, this module identifies malicious traffic by detecting distinctive characteristics. This module is included in TCPWave's base product at no additional charge.

Rule-Based DNS Threat Detection and Prevention

Using a robust and high-performance rule-based network threat detection engine (Suricata), TCPWave's DNS TITAN Threat Protector can monitor DNS traffic in real-time to detect and prevent malicious activity. In addition, administrators can create or import engine rules, including from third parties, to drop specific packets and produce alerts on specific packets or traffic patterns.

Also, a default ruleset is provided that consists of over 2,500 DNS-related rules that produce alerts. It is based on Emerging Threats' Open ruleset and can be modified. These default rules primarily detect protocol anomalies, higher than expected frequencies of specific packets or queries, and queries for domains related to malware, command and control, phishing, ransomware, and tunnels.

TCPWave's effective threat detection and prevention capabilities protect DNS appliances and users by using DNS-specific rules that go far beyond the capabilities of general-purpose firewalls.

DNS End-User Security

TCPWave's DNS TITAN End-User Security prevents users from accessing malicious sites. It blocks DNS queries for domain names of malicious hosts, queries to malicious DNS servers, and IP addresses of malicious sites in DNS query responses.

The items to block are based on domain and IP reputation data provided by TCPWave's partner, Spamhaus, a leader in providing threat intelligence information. This reputation data consists of a feed of continually updated rules in DNS

Response Policy Zones (RPZs). Using this continually updated information, TITAN End-User Security protects users from accessing malicious sites, including malware, phishing, ransomware, adware, and botnet sites.

SIEM Integration

To support the processing of logs by Security Information and Event Management (SIEM) and other systems, TCPWave produces audit log files that comply with the Common Event Format (CEF) standard. Using this standard, TCPWave integrates with Micro Focus ArcSight. Also, TCPWave provides log forwarding to IBM QRadar, Splunk, Apache Flume, and others. These capabilities help security personnel quickly detect and respond to threats.

Identity Administration

TCPWave Identity Administration provides user management functionality. Segregation of Duties (SoD) is a preventive and most critical control. It reduces the risk of error and malicious DNS/DHCP activities through a proper division of tasks among an organization's employees. When manipulating the core functionality of mission-critical network services, the appropriate segregation of duties prevents the potential for employee circumvention of controls.