

BYTESCREEN Tech Pvt Ltd presents an extensive suite of cutting-edge network infrastructure solutions tailored to meet the dynamic requirements of modern businesses. Our product datasheet outlines the array of features and capabilities that make our offerings stand out in ensuring seamless connectivity, optimal performance, and robust security.

1. Embedded OS (Hardened and Crash-proof):

Our network devices are equipped with a crash-proof embedded operating system, meticulously hardened for stability and reliability. This optimized operating system forms a robust foundation for ensuring optimal performance and unwavering security, even in the most demanding environments.

2. ISP Load Balancing:

Experience unparalleled efficiency in network traffic distribution with our ISP load balancing capabilities. This functionality empowers you to utilize multiple Internet Service Providers concurrently, preventing bottlenecks and maximizing resource efficiency.

3. Stateful Inspection Firewall:

Security is paramount, and our stateful inspection firewall takes it to the next level. By monitoring and controlling incoming and outgoing traffic based on predefined rules, it makes intelligent decisions to allow or block traffic, thereby fortifying network security.

4. Multi WAN Support:

Enhance redundancy and boost performance by simultaneously connecting to multiple Wide Area Network (WAN) providers. Our devices ensure uninterrupted connectivity, effectively managing diverse service providers.

5. SNI-Based HTTPS Domain Filter:

Exercise control over HTTPS traffic with Server Name Indication (SNI)-based domain filtering. This feature empowers you to restrict access to specific domains based on their SSL certificates, fortifying security against unauthorized or malicious websites.

6. Policy-based Auto Failover:

Continuous connectivity is non-negotiable. Our devices incorporate policy-based automatic failover, responding dynamically to link failures based on predefined criteria such as link quality or availability.

7. Location Anomaly Detection and Protection:

Stay ahead of potential threats or performance issues with our advanced anomaly detection and protection mechanisms. These mechanisms identify abnormal network behavior in various locations, allowing for timely and appropriate action.

8. Policy-based Load Balancing:

Optimize bandwidth utilization with policy-based load balancing. This functionality ensures that network traffic is distributed intelligently across multiple links, aligning with predefined policies.

9. MAC ID, IP, and User-based Policy:

Tailor your network access policies with precision using our devices. Define policies based on MAC addresses, IP addresses, and user identities, providing granular control and enhancing overall network security.

10. Static Routing:

Navigate complex network environments with ease. Our devices support static routing, allowing manual configuration of the routing table to dictate the path network packets should take.

Certainly! Here's the content with numbering starting from 11 and replacing the previous numbering:

11. RADIUS User ID and Passkey:

RADIUS authentication enhances network security by requiring users to authenticate using unique User IDs and Passkeys. This robust authentication mechanism ensures secure access to the wireless network, preventing unauthorized users from gaining entry. By verifying user identity before granting network access, RADIUS adds an extra layer of protection to your network infrastructure.

12. LDAP Integration:

The NGFW seamlessly integrates with Lightweight Directory Access Protocol (LDAP) directories for user authentication. This centralized approach streamlines user management, ensuring consistency with existing directory services. LDAP integration enhances security by authenticating users against LDAP servers, reducing the risk of unauthorized access.

13. Customizable Captive Portal:

The NGFW offers a customizable captive portal, allowing organizations to create branded login pages with personalized messages, images, and login options. This not only enhances the user experience but also adds an additional layer of security by requiring users to authenticate before accessing the network.

14. NTLM Authentication:

NT LAN Manager (NTLM) authentication support simplifies user authentication in Microsoft Windows environments. Users can seamlessly authenticate using their Windows credentials, streamlining the login process and ensuring compatibility with existing authentication systems.

15. Multifactor Authentication (UserID/Passkey, OTP, Voucher):

The NGFW supports multifactor authentication, allowing users to authenticate using multiple factors such as User ID/Passkey, One-Time Passwords (OTP), or vouchers. This robust feature enhances security by requiring users to provide additional authentication factors beyond a simple username and password.

16. Multi Authentication (PPPoE/IPoE/MAC/Captive Portal/Voucher-based):

The NGFW provides flexibility with multiple authentication methods, including Point-to-Point Protocol over Ethernet (PPPoE), IP over Ethernet (IPoE), MAC-based authentication, captive portal authentication, and voucher-based authentication. This versatility accommodates various user scenarios, ensuring seamless access to the wireless network.

17. Gateway Antivirus:

The gateway antivirus feature intercepts and scans network traffic at the entry point of the network, preventing malicious content from infiltrating the infrastructure. By inspecting traffic in real time, the NGFW's gateway antivirus effectively blocks known threats and identifies suspicious activities before compromising network security.

18. Extended Signatures Support:

The NGFW supports extended signatures to detect and mitigate advanced threats beyond traditional antivirus definitions. By employing advanced signature-based detection techniques, the antivirus engine identifies and neutralizes emerging threats that may evade conventional methods.

19. Zero-hour Virus Protection:

Zero-hour virus protection provides proactive defense against newly emerging and unknown threats. By leveraging heuristic and behavior-based analysis techniques, the antivirus engine detects and blocks zero-day attacks in real time, minimizing the risk of infection before antivirus signatures are available.

20. DoS / DDoS Protection / Brute Force Protection:

The NGFW includes mechanisms for DoS/DDoS protection and brute force protection to defend against denial-of-service attacks and brute force login attempts. These features mitigate the impact of malicious attacks on network availability, ensuring continuous and reliable operation of the wireless infrastructure.

21. Virus, Worm, Trojan, Spyware, Malware, Phishing Protection Detection & Removal:

The antivirus engine provides comprehensive protection against a wide range of threats, including viruses, worms, Trojans, spyware, malware, and phishing attacks. By detecting and removing malicious code and suspicious activities, the antivirus feature safeguards the network and data from cyber threats and unauthorized access.

22. Protocols Scanning:

The protocols scanning feature analyzes network protocols and traffic patterns to detect and block malicious activities and anomalous behavior. By inspecting network communications at the protocol level, the antivirus engine identifies and neutralizes threats that may exploit vulnerabilities in network protocols.

23. Signatures Support - Zero-Hour Solution:

The NGFW supports zero-hour solutions for antivirus signatures, enabling rapid detection and response to new and emerging threats. Continuous updates to antivirus signatures in real-time protect against the latest malware variants, ensuring effective threat prevention and mitigation.

24. Content Replace:

The content replace feature allows for the replacement of malicious or unwanted content with benign or customized content. This prevents users from accessing harmful or inappropriate material, helping enforce acceptable use policies and enhance web security.

25. Automatic Real-Time Virus Signature Database Update:

The NGFW automatically updates the virus signature database in real-time, ensuring it is always current with the latest threat intelligence. Continuous refreshing of antivirus signatures enables effective detection and blocking of new and evolving malware threats, minimizing the risk of infection.

26. Indicator:

The indicator feature provides visual alerts and notifications to administrators when antivirus events occur. These include malware detection, virus quarantine, or threat mitigation actions. This feature helps administrators monitor antivirus activity and respond promptly to security incidents, ensuring the integrity and security of the network.

27. Gateway AntiSpam:

The gateway anti-spam feature intercepts and scans incoming email traffic at the network gateway, identifying and blocking spam messages before reaching the email server or user inbox. Filtering out unwanted emails at the gateway level reduces the load on email servers and improves overall network security.

28. Policy-wise Scanning:

The anti-spam solution allows for policy-based scanning of email traffic. Administrators can define custom rules and criteria for spam detection and filtering, providing flexibility in configuring anti-spam policies to meet specific organizational requirements.

29. AntiSpam Engine:

The anti-spam engine employs advanced algorithms and heuristics to analyze email content and headers. It identifies patterns and characteristics associated with spam and malicious messages, accurately detecting and filtering out spam emails while minimizing false positives.

30. Configurable Spam Policy per Email Address or Group:

Administrators can configure spam policies on a per-email-address or per-group basis. This granular control over spam filtering settings enables customization of anti-spam policies to suit the needs and preferences of individual users or user groups.

31. Quarantine Spam Email:

The anti-spam solution includes quarantine functionality to isolate and quarantine suspected spam emails for further review. Quarantined emails are held in a secure environment, preventing them from reaching users' inboxes until verified and approved by administrators.

32. Filter Based on Message Header, Body, Sender, Recipient:

The anti-spam solution filters emails based on various criteria, including message headers, body content, sender information, and recipient addresses. This multi-dimensional filtering approach ensures comprehensive detection and blocking of spam messages from multiple sources and in various formats.

33. Ability to Filter SMTPS (465), SMTP, POP3 & IMAP Traffic:

The anti-spam solution supports filtering of email traffic over multiple protocols, including SMTPS (port 465), SMTP (port 25), POP3 (port 110), and IMAP (port 143). This broad protocol support ensures protection across different email platforms and services.

34. Bandwidth Management Features:

In addition to anti-spam capabilities, the NGFW provides robust bandwidth management features to optimize network performance and ensure equitable distribution of bandwidth resources.

35. Web Application-Based Bandwidth Allocation:

Administrators can allocate bandwidth based on web application usage patterns, prioritizing critical applications and services that require high-speed connectivity. This ensures optimal performance for mission-critical applications while preventing bandwidth congestion caused by non-essential web traffic.

36. Shared Bandwidth:

The bandwidth management solution supports shared bandwidth allocation, allowing multiple users to share available bandwidth resources.