Next Generation Firewall (NGFW)

Single, Unified Network Security Solution

Next Generation Firewall (NGFW) helps you stay ahead of emerging threats, going beyond traditional IP address and port-blocking. Combined with Unified Threat Management (UTM) capabilities, NGFW safeguards your business against breaches, malware, ransomware, botnets, phishing attempts, viruses, and more.

Advanced Security with Unified Threat Management (UTM)

Protecting your network requires leading-edge security solutions designed to eliminate threats before they reach your mission-critical data. S-NET is your all-inclusive cloud services provider offering end-to-end protection of your mission-critical networks with fully managed Next Generation Firewall solutions, services, and support.

Solutions

S-NET offers a fully-managed Next Generation Firewall solution that protects your business from new and emerging threats. S-NET's NGFW solutions are tailored to core business needs and managed by our team of experts for enhanced network security.

Services

S-NET provides concierge services throughout the customer's journey. Our dedicated team conducts a business needs assessment and facilitates the NGFW implementation from beginning to end for a smooth transition to enhanced networking and security solutions.

Support

S-NET's ongoing white-glove support ensures your business receives dedicated attention for your NGFW solution and overall performance. We provide a dedicated Client Technology Advisor, 24/7/365 customer and technical support, and regular solution maintenance to ensure your ongoing success.

+1 877.777.7776 | SALES@SNETCONNECT.COM

Next Generation Firewall (NGFW) Benefits

S-NET's Next Generation Firewall includes an enterprise-grade security stack fit for organizations of any size. Block complex threats and easily meet regulatory compliance requirements.

Gain deep visibility into your network security, users, and applications through a single interface to make informed, timely, and effective decisions and mitigate threats.

Gain granular control over your infrastructure by putting protocols in place for individual or grouped users, applications, URLs, or IP addresses.

S-NET's URL filtering module keeps your business safe by proactively blocking attacks from high-risk website categories including 460 million domains and 13 billion URLs associated with malware and phishing.

Recognize and prevent unauthorized access to your critical systems and data with Unified Threat Management that leverages an anomaly- and signature-based detection engine and real-time threat intelligence.

Prevent sensitive information from leaving your organization with inbound and outbound SSL decryption settings based on URL category, source, destination, user, user group, and port.

Allow, deny, or restrict access to individual or entire groups of applications and restrict access to malicious, risky, and unwanted applications using custom application monitors.

Customize your firewall settings and policies through a single pane of glass and mass-deploy policies to any number of locations in your network with just a few clicks.

Keep your web security up-to-date with new threats and safeguard your business against attacks from over 12 million malicious IP Addresses.

Block Trojans, viruses, spam, intrusion attempts, and other violations of normal protocol communication to prevent attacks before they happen with Deep Packet Inspection.

Inspect internet traffic in real-time and identify malware hiding in incoming files downloaded from HTTP, FTP, SMTP, POP3, IMAP, and MAPI sources. Reduce the need for anti-virus software on user devices with protection built into your core network.

s·net COMMUNICATIONS

S-NET Communications, Inc.
1100 Woodfield Rd., Ste. 101
Schaumburg, IL 60173 USA