HUAWEI NGFW Module

NGFW module

Overview

Enterprise networks are evolving into next-generation networks that feature mobile broadband, big data, social networking, and cloud services. Yet, mobile applications, Web2.0, and social networks expose enterprise networks to the risks on the open Internet. Cybercriminals can easily penetrate a traditional firewall by spoofing or using Trojan horses, malware, or botnets.
HUAWEI NGFW Module is designed to address these challenges. Based on ACTUAL (application , content, time, user, attack, and location) awareness, it uses the cloud technology to identify unknown threats and provide high-performance application-layer protection for enterprise networks. In addition, the NGFW module can be inserted on basic network devices, such as the S12700, S9700, and S7700 switches, providing plug and play and scalability features. This greatly simplifies user management and reduces maintenance costs.

Product Features

Easy Deployment And Expansion

- Uses software to adjust the networking, which simplifies the installation and deployment and frees the administrators from adjusting the complex cables.
- In case of performance bottlenecks, more NGFW modules can be inserted into the slots on the switches, without requiring extra space.
- Integrates networks with security using products from the same vendor, which facilitates unified management and simplifies the management.

Comprehensive Threat Prevention

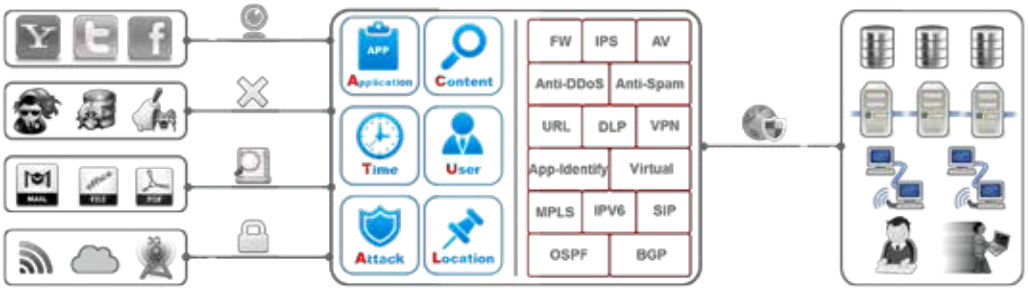
- Provides professional security functions, including IPS, AV, anti-spam, web security, and application control, besides basic defense functions, such as SVN, authentication, and anti-DDoS.
- Provide samples of worldwide suspicious threats. The NGFW module executes suspicious samples within the sandbox in the cloud to monitor the activities of the samples and identifies unknown threats, automatically extracts threat signatures, and rapidly synchronizes the signatures to the devices to defend against zero-day attacks.

Granular Application Access Control

- Innovative next-generation context awareness and access control: Identifies application-layer threats from six dimensions: application, content, time, user, attack, and location to implement application-layer security protection.
- Diversified reports: Provides all-round visibility into service status, network environment, security postures, and user behaviors.
- Integrated next-generation content security: Provides an analysis engine that integrates application identification and security functions to prevent application-based malicious code injections, network intrusions, data interceptions, and Advanced Persistent Threat (APT) attacks.

Excellent Performance

- Employs dedicated software and hardware platform architecture and provides an Intelligent Awareness Engine (IAE) capable of parallel processing with all security functions enabled after intelligent application identification.
- Implements hardware acceleration for content checks to improve application-layer protection efficiency and ensure the 10G+ performance with all security functions enabled.



HUAWEI NGFW Module

Specifications

Model	NGFW module
Hardware interface	
Application scope	S12700, S9700, S7700
Fixed ports	4 x GE
USB port	1
Console port	1
Functions	
Context awareness	ACTUAL (Application, Content, Time, User, Attack, Location)-based awareness capabilities
	Eight authentication methods (local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security)
Application security	Fine-grained identification of over 6000 application protocols, application-specific action, and online update of protocol databases
	Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications
	Combination of application identification and content detection to identify file types and sensitive information to prevent information leaks
Intrusion prevention	Provides over 3000 signatures for attack identification.
	Provides protocol identification to defend against abnormal protocol behaviors.
	Supports user-defined IPS signatures.
Web security	Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 130 categories
	Defense against web application attacks, such as cross-site scripting and SQL injection attacks
	HTTP/HTTPS/FTP-based content awareness to defend against web viruses
	URL blacklist and whitelist and keyword filtering
Email security	Real-time anti-spam to detect and filter out phishing emails
	Local whitelist and blacklist, remote real-time blacklist, content filtering, keyword filtering, and mail filtering by attachment type, size, and quantity
	Virus scanning and notification for POP3/SMTP/IMAP email attachments
Data security	Data leak prevention based on content awareness
	File reassembly and data filtering for more than 20 file types (including Word, Excel, PPT, and PDF), and file blocking for more than 60 file types
Security virtualization	Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)
Network security	Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks
	VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE
Routing	IPv4: static routing, RIP, OSPF, BGP, and IS-IS IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6
Working mode and availability	Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/Standby mode
Intelligent management	Provides a global configuration view and integrated policy management. The configurations can be completed in one page.
	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.