DATASHEET

Next Generation Firewall

Data-Driven Security for coordinated safeguarding of perimeters

Overview

QAX Next Generation Firewall is an innovative firewall product that can comprehensively respond to traditional network attacks and advanced threats. It can be widely used in the business network boundaries of various enterprises and organizations to achieve network security domain isolation, refined access control, and high efficiency. Based on the next-generation firewall, this product transcends the integration of innovative security technologies such as threat intelligence, big data analysis, and security visualization, and through intelligent collaboration with the cyber threat perception center, security management analysis center, endpoint security management system, etc., Users build a new generation of data-driven threat defense platform at the network perimeter.

Main Functions

Function	Description
Basic Firewall Function	Support various forms of flexible deployment, with load balancing,nat,ipv6 support, vpn,vsys,ha and other functions, and can protect scanning, flooding, abnormal packets and other traditional network attacks
Delicacy application control	Can accurately identify more than 3000 kinds of network applications and users, terminals, geographical location, transmission of content and other information, and can achieve the application, users, content multi-dimensional integrated fine control
High-performance threat protection	Deep integrated threat protection engine,provide high performance protection against more than 5 million epidemic viruses, more than 5000 vulnerability attacks and more than 1000 spyware behaviors
Intelligent Cooperative Defense	Support intelligent cooperation with cloud and terminal security system to realize advanced security functions such as virus cloud detection, threat intelligence real-time disposal, emergency response strategy push, high risk terminal control,etc.
Compromise detection and disposal	Threat intelligence detection and depth analysis can be carried out on the behavior data generated by network traffic, local compromised host can be warned in real time , one-click disposal of threat sources
Visual association analysis	Multi-dimensional information including application, user, content, threat , location,etc. can be presented graphically, and the security analysis can be realized by progressive data drilling

Features

Data-driven security innovation

Make full use of QAX's rich security big data and Internet threat information, develop intelligent cooperation with cloud and terminal security system, break the limitation of traditional static, passive and isolated protection mode with data driven and cooperative linkage, improving security effectiveness and real-time defense dramatically.

Efficient and reliable system architecture

Based on asynchronous parallel processing, management and data plane separation of single engine and optimization of many data processing mechanisms, using the fourth generation secos operating system, the device can always maintain high performance in the case of large traffic, complex scenarios, security functions, and ensure stability and reliability under extreme conditions.

Panoramic Platform-based Management

Provide a wealth of platform-based security management tools. For large-scale deployment scenarios, through supporting platforms such as the "Security Management Analysis Center (SMAC)" and "Network Threat Perception Center", it is possible to achieve centralized status monitoring, unified management, operation and maintenance, analysis and early warning of the entire network for thousands of devices. Global disposal response.

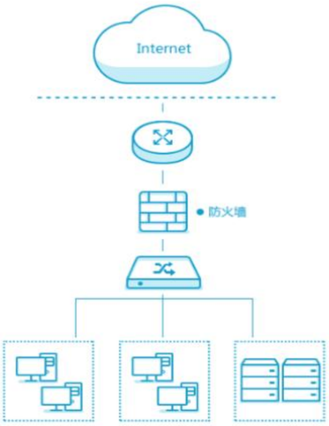
Values

Realize all-round attack protection, effectively defend against various attack behaviors, and ensure the security of enterprise and branch Internet access and enterprise private network.

Enhance threat perception capabilities, build a security system that emphasizes both defense and detection, and make up for the shortcomings of traditional protection.

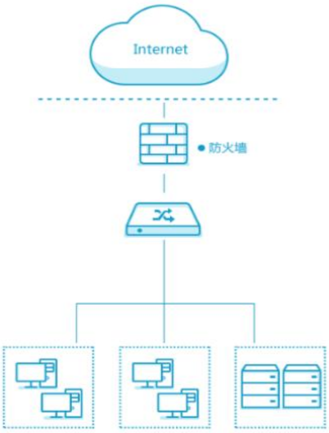
Significantly reduce the management cost of the entire network equipment and improve management efficiency.

Deployment Solution



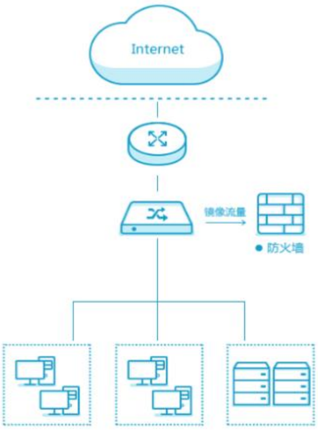
Transparent Mode

Firewalls are used as two-tier devices without changing the original network structure



Routing Mode

Firewalls are used as three-tier devices deployed at network boundaries



Bypass Mirroring Mode

Firewall bypass mirror port, only do traffic monitoring, do not change the original network structure

Hardware Specifications

Products model		NSG2000-TE05P-QW	NSG3000-TE35M-QW	NSG5000-TG35M-QW
Basic FW Performance indicators	throughput (layer 3)	800Mbps	6Gbps	10Gbps
	Maximum number of concurrent connections	180000	2000000	2600000
	New connection	12000/s	80000/s	180000/s
NGF Performance indicators	throughput(Layer 7)	500Mbps	3Gbps	6Gbps
	NEW HTTP	8000/s	65000/s	120000/s
	IPS throughput	100Mps	1.8Gbps	3.4Gbps
	AV throughput	150Mbps	2Gbps	3.8Gbps
	throughput under security module full open	80Mbps	1.4Gbps	3Gbps
VPN Performance indicators	IPSec throughput	300Mbps	400Mbps	850Mbps
	number of IPSec tunnels (Standard/maximum)	16/100	15/200	25/3000
	Number of SSL VPN concurrent users (Standard/maximum)	16/100	15/200	25/500
Others	default interface modules	6*10/100/1000 M Base-T+2*1000M SFP	6*10/100/1000 M Base-T+2*1000M SFP	6*10/100/1000 M Base-T+4*1000M SFP
	Extension slots	none	1	2
	BYPASS support	no	support	support

QAX Group

Addr: No. 1, 26 of Xizhimenwai South Road, Xicheng District, Beijing, China

Website: https://www.qianxin.com/

Email: Global-support@qianxin.com

QAX
Leader in next-generation cybersecurity