ZRJ Z-FW-1800E Series Next Generation Firewall

Product Overview

The ZRJ Next Generation Firewall (NGFW) adopts a high-performance architecture, provides rich hardware specifications, supports advanced virtualization technology, and adapts to various cloud environments. It integrates precise multi-dimensional control based on identity, application, content, assets, etc., can comprehensively protect against various network threats such as denial of service attacks, brute force cracking, scanning and sniffing, intrusion attacks, and malicious code, and can quickly build a cost-effective, efficient, and integrated security protection hub for users.

Main Features

High-performance processing architecture

High-speed software and hardware diversion technology enables ultra-high-speed packet forwarding and linear performance growth.

The software architecture with separated forwarding and control planes uses kernel-bypass zero-copy technology to maximize security processing capabilities.

Firewalls adapted to the cloud

It supports virtualized deployment and operation on mainstream virtualization platforms such as VMware, KVM, and Hyper-V, and is compatible with public cloud platforms such as Microsoft Azure, Alibaba Cloud, Tencent Cloud, and Huawei Cloud, providing professional boundary security protection for cloud networks and cloud services.

Powerful network capabilities

It offers a variety of static, dynamic, and policy-based routing, provides intelligent routing based on users, applications, regions, and ISPs, and supports multiple VPNs such as IPSec, SSL, GRE, VXLAN, and L2TP.

Through its secure SD-WAN capabilities, zero-configuration onboarding, and configuration template distribution, it enables quick, intelligent, and secure wide area network deployment.

It provides full IPv4 and IPv6 dual-stack network support, offers comprehensive in-depth protection based on IPv6, and ensures synchronized security and network upgrades.

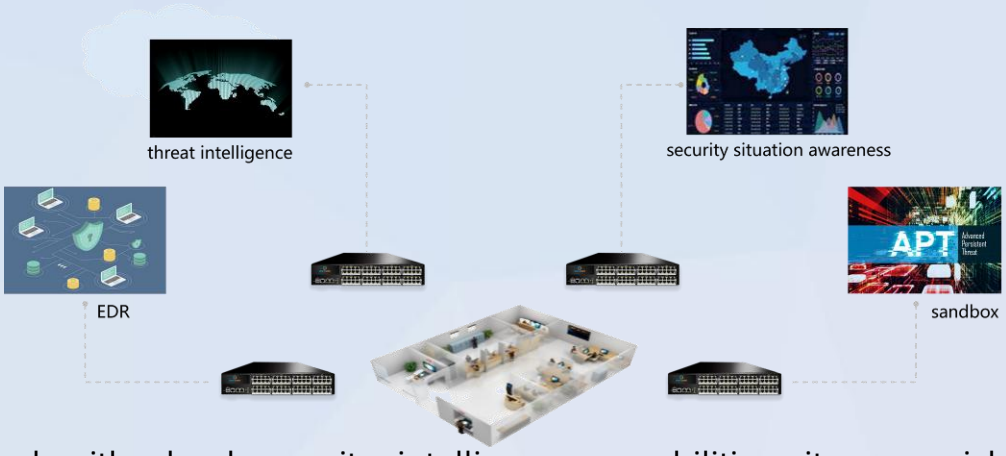
Digital asset security management

It supports one-click asset discovery and quickly discovers and manages digital assets through traffic learning, scanning detection, terminal linkage, manual entry, etc.

It performs unified security sorting of assets based on attributes such as department, business system, and importance.

Multi-dimensional defense

It features an integrated security engine, providing application identification, intrusion protection, virus protection, URL classification, and content filtering, etc.



Combined with cloud security intelligence capabilities, it can quickly mark malicious behaviors and establish defense capabilities for hot attack events at the first time.

It provides a fully open API to support the formation of a joint defense system with situational awareness, sandbox, NTA, and other products.

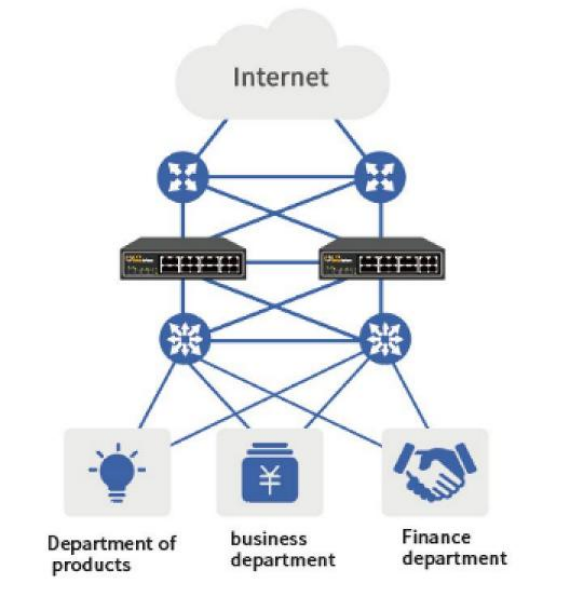
Intelligent and efficient operation and maintenance management

Based on security analysis of network tags, user identities, geographic locations, and assets, it supports displaying attack chain views and can collect evidence of attack threats to facilitate rapid positioning and response.

It supports intelligent policy analysis to quickly discover and optimize redundant policies, mergeable policies, empty policies, and expired policies, etc.

It cooperates with the SD-WAN platform to batch upgrade the device system version and feature library, provides real-time monitoring of the firewall status, security situation analysis, configuration distribution and backup, and centralized log management.

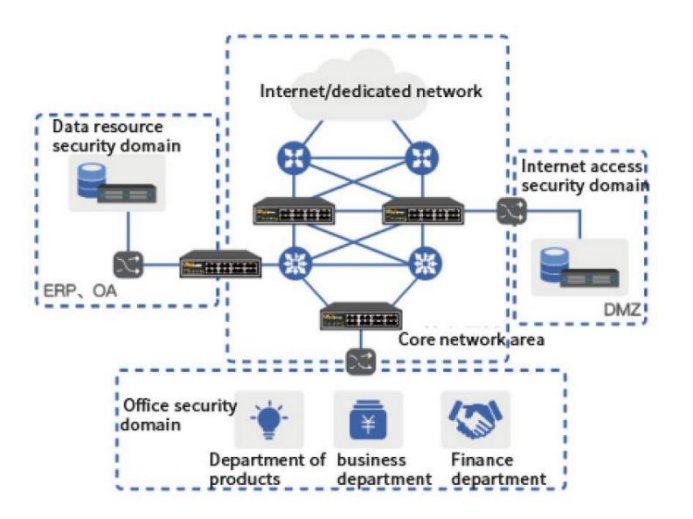
Typical Scenarios



Internet egress

✓ It provides comprehensive protection against Internet threats, refined application and Internet behavior control, and multi-link load scheduling and traffic management.

✓ It supports HA for configuration and traffic sessions to improve reliability.

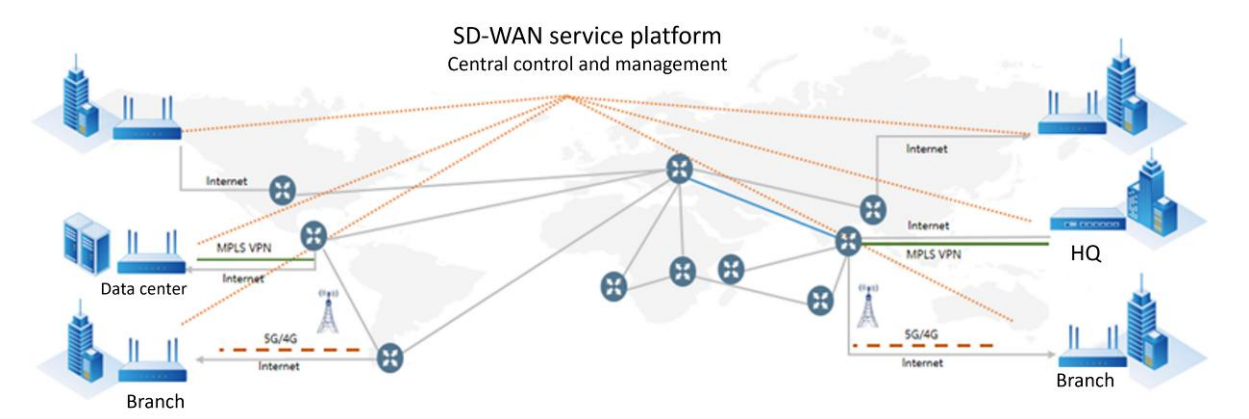


Domain isolation

✓ It sets up refined security policies based on multiple dimensions such as users, applications, and time.

✓ It prevents network threats from spreading internally and protects core business security.

✓ It provides access log audit to meet compliance requirements.



SD-WAN secure interconnection

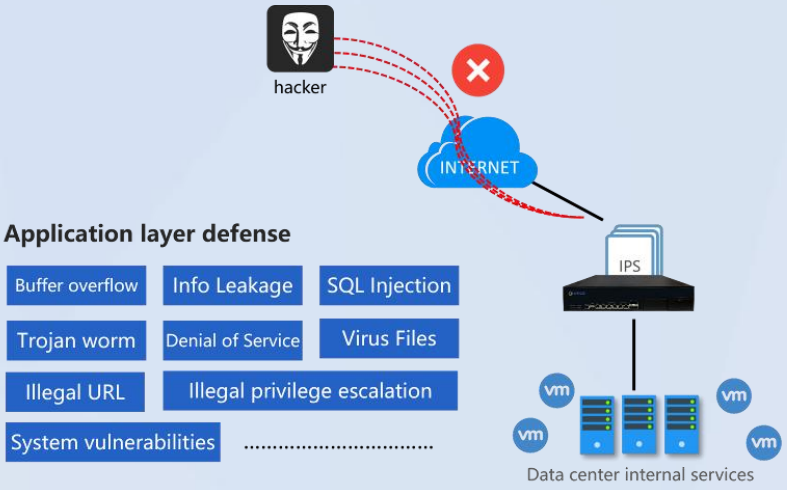
✓ It supports multiple VPN tunnels to quickly build overlay networks between branches and headquarters, and between branches and clouds.

✓ It provides encrypted networks using algorithms such as DES, 3DES, AES, SM1, SM2, SM3, and SM4 to ensure secure data transmission.

✓ Through its own security capabilities, it provides multi-dimensional security functions such as intrusion attack defense, malicious code detection, application and URL control, and auditing.

✓ Based on application SLAs, it performs intelligent routing, supports high-reliability networking with dual links and dual centers, and ensures service availability.

Key Features

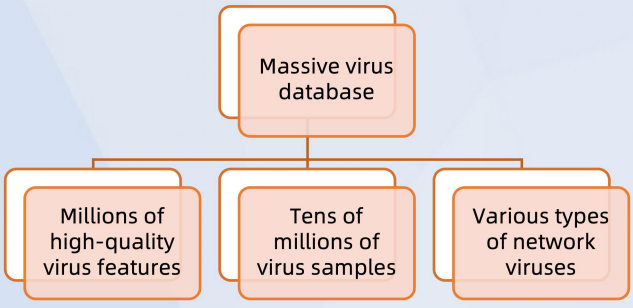


Intrusion Detection and Defense

✓ Z-FW-1800E has 12 categories and over 10,000 attack features, including vulnerability scanning, directory traversal, and security bypass, and supports manual and automatic upgrades.

✓ It supports IPS custom rules and provides rich custom fields such as protocol fields, operation types, and payload content.

✓ It allows setting alarm log merging, supports IPS high-level alarms, and can accurately record session information and attack information.



Virus protection

✓ It provides virus detection for web websites, file transfers, emails, etc., and supports millions of virus databases and regular update services.

✓ It detects 20 types of file formats and compressed files, and supports trusted file whitelists.

Application control and auditing

✓ It identifies more than 5,000 applications, supports Web, PC, and mobile application identification, regularly updates application signature databases, and allows customizing application signatures.

✓ It controls access to social networks, P2P downloads, file transfers, e-commerce, instant messaging, office software, and online games, etc.

✓ It supports application and website access auditing based on users, applications, behaviors, and content.

URL filtering

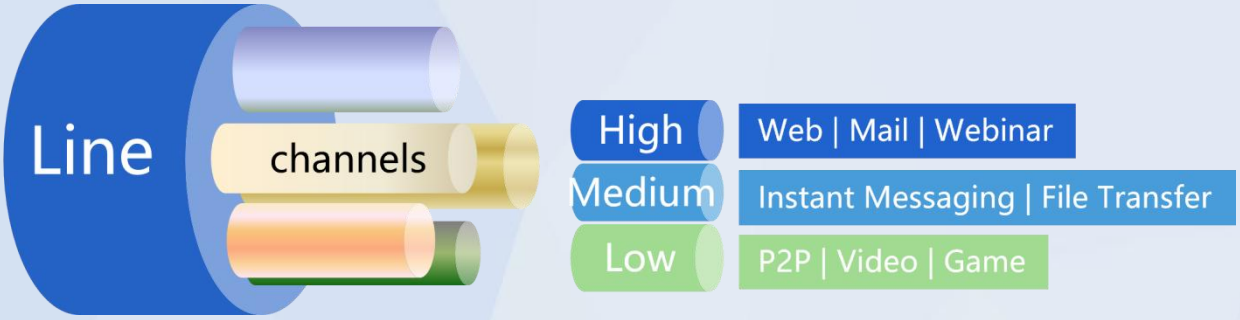
✓ It provides more than 100 categories and tens of millions of predefined URLs, and supports custom URLs as well as batch import and export.

✓ It implements URL classification control and performs operations such as discarding, redirecting, and logging for malicious or risky traffic according to policies.

Intelligent flow control

✓ It supports multi-level nested application flow control strategies and total bandwidth management.

✓ It supports priority channel setting, flow control strategies, elastic bandwidth, application speed limits, and flow control whitelists.



User management

✓ It supports automatic user identification and user resource policy management.

✓ It supports local authentication, Portal authentication, LDAP and RADIUS authentication, WeChat authentication, SMS authentication, and visitor QR code authentication, etc.

It supports user monitoring, user quotas, and user anti-brute force cracking.

Collaborative linkage

✓ It supports cloud threat intelligence linkage, checks and protects malicious IPs, domain names, and URLs, and provides hot security event pushes.

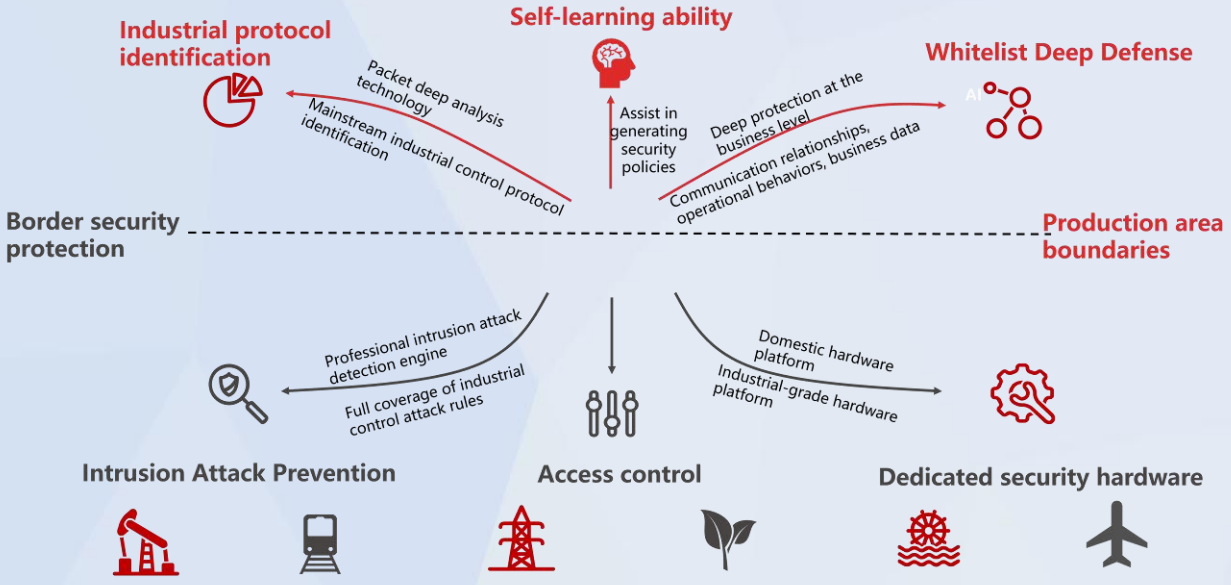
✓ It supports EDR terminal protection linkage, terminal user access control, and isolates hosts according to terminal health status.

✓ It supports sandbox linkage and analyzes suspicious files and suspicious host behavior.

Industrial protection

✓ It supports three working modes: learning, verification, and protection.

✓ It supports all-round integrated protection for IT/OT traffic, combining application identification, deep content analysis, intrusion prevention, virus detection, and other technologies for security protection.



Asset Management

✓ It supports manual addition, scanning discovery, and traffic self-learning of IPv4/IPv6 assets, and supports import and export of asset information.

✓ It supports obtaining asset IP, operating system, online status, and other information through EDR, and automatically synchronizes to the firewall.

Other security features

✓ It supports ARP attack protection, DoS/DDoS attack protection, and anti-brute force cracking.

✓ It provides illegal external connection protection and supports automatic learning of server external connections.

✓ It supports port risk scanning and weak password scanning.

Security Analysis

✓ It supports TOP 10 statistics of viruses and intrusion events according to attack source, attack purpose, and attack event, and displays the location of the attack source.

✓ It supports security status analysis based on threat intelligence, providing TOP 10 statistics of source IP, destination IP, intelligence indicators, and intelligence types.

✓ It supports receiving sudden hotspot intelligence events, presenting intelligence descriptions, Domain IOC, IP IOC, Hash IOC, and other intelligence information.

✓ It supports asset-based security analysis, showing assets with security risks in the network and their corresponding risk levels.

Network

✓ It supports multiple interfaces such as physical, bridge, VLAN, tunnel, loopback, and aggregation, etc.

✓ It supports multiple routes such as static, dynamic (RIP, OSPF, BGP), policy, ISP routing, and application routing, etc.

✓ It supports source NAT, destination NAT, static NAT, transparent NAT, and ALG.

✓ It supports multiple deployment modes such as transparent, routing, bypass, hybrid, and virtual line.

✓ It supports interface static IP, DHCP dynamic acquisition, and PPPoE client configuration.

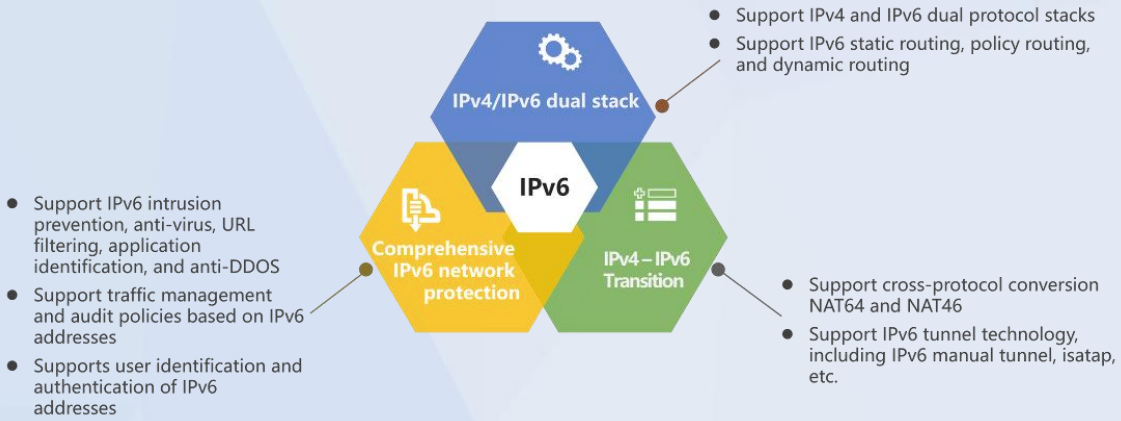
✓ It supports DHCP server, DHCP relay, DNS server, and DNS proxy.

IPv6

✓ It supports IPv4/IPv6 dual protocol stack, NAT66, and cross-protocol conversion (NAT64 and NAT46).

✓ It supports IPv6 routing and IPv6 tunnel technology.

✓ It supports IPv6 intrusion prevention, virus protection, URL filtering, application identification, and anti-DDoS attack.



VPN

✓ It supports GRE, IPsec VPN, and SSL VPN.

✓ It supports multiple international standard encryption algorithms such as DES, 3DES, and AES.

✓ It supports VPN technology based on cryptographic algorithms SM1, SM2, SM3, and SM4.

✓ It supports VPN clients for multiple terminal systems and supports VPN two-factor authentication.

VXLAN

✓ It supports VXLAN tunnel forwarding under Layer 2 network and supports specified destination port.

VRF

✓ It supports VRF routing isolation and integrated strategies, static routing, dynamic routing, policy routing, and other policy isolation.

Secure SD-WAN

✓ It cooperates with the SD-WAN centralized management and control platform to achieve zero configuration of equipment and minute-level deployment.

It supports automatic batch upgrade of equipment, real-time status monitoring, security situation awareness, automatic configuration backup, log collection, etc.

High availability

✓ It supports active-active and active-standby modes, standard VRRP, and interface linkage.

✓ It supports active-standby automatic monitoring, HA switching, HA configuration and traffic synchronization, and HA monitoring.

✓ It supports hardware-based interface bypass.

System management

✓ It supports graphical interface and command line management configuration.

✓ It supports separation of powers, administrator security settings, and provides dual system backup and configuration backup.

✓ It supports policy analysis, detecting redundant policies, conflicting policies, expired policies, empty policies, etc.

✓ It provides web graphical debugging and diagnostic tools, and supports Ping/trace tools and packet capture tools.

Log and monitoring

✓ It supports local storage and external transmission of logs, log query, export and clearing, and industry-specific log standards.

✓ It supports system logs, application control logs, audit logs, security logs, intrusion logs, virus logs, and threat intelligence logs.

✓ It supports automatic generation of analysis reports daily, weekly, and monthly, and reports can be saved locally, downloaded, exported, and sent via FTP or email.

Specifications

Item	Z-FW-1800E-X8430	Z-FW-1800E-X6024R	Z-FW-1800E-X6012R	Z-FW-1800E-X3012R
Hardware Specification				
Interface	6*GE+4*SFP	16*GE+4*SFP+4*SFP+	8*GE+2*SFP+2*SFP+	8*GE+2*SFP
USB	2	2	2	1
Console	1	1	1	1
CF card	4G CF	8GB EMMC	8GB EMMC	8GB EMMC
Management	1MGT, 1HA	N/A	N/A	N/A
Bypass (pairs)	16	2	2	N/A
Bypass feature	4GE: 0<->1;2<->3 8GE:0<->1; 2<->3; 4<->5; 6<->7 4GE4SFP:4<->5; 6<->7	GE0/2<->GE0/3 GE0/4<->GE/5	GE0/2<->GE0/3 GE0/4<->GE/5	N/A
Slot	3	2	2	N/A
Module(optional)	8GE 8SFP 4GE+4SFP 4SFP+	8GE 8SFP 4GE+4SFP 4SFP+	8GE 8SFP 4GE+4SFP 4SFP+	N/A
hard disk(optional)	1TB	1TB	1TB	N/A
Security Performance				
IPS throughput	8G	2.5G	2G	300M
AV throughput	8G	2.5G	2G	300M
NGFW throughput	55G	20G	10G	2.1G
System performance (throughput)				
1518 bytes	55G	20G	10G	2.1G
512 bytes	25G	7.6G	7.5G	720M
64 bytes	4.4G	1.2G	1.1G	110M

New sessions per second				
New sessions (TCP)	420000	140000	140000	18000
New sessions (HTTP)	320000	117000	117000	11000
New sessions (APP enabled)	200000	47000	47000	3800
New session (APP\IPS\AV enabled)	86000	19000	19000	1400
Concurrent sessions				
Concurrent sessions (APP disabled)	8000000	4000000	4000000	1000000
Concurrent sessions (APP enabled)	5700000	2300000	2300000	700000
Concurrent sessions (APP\IPS\AV enabled)	5700000	2300000	2300000	700000
IPSec VPN performance				
IPSec tunnels	10000	10000	10000	2300
1400 bytes (without accelerator card)	5.6G	3.5G	3.4G	450M
SSL VPN performance				
New VPN Tunnels (clients) per second	150	130	130	15
Maximum concurrent users	10000	3000	3000	1200
Throughput	1000M	770M	770M	125M

Physical and electrical specifications				
Dimension(W*D*H)	550*440*88mm	440*450*44mm	440*450*44mm	440*330*44mm
AC power supply	dual AC	dual AC	dual AC	dual AC
Power consumption	350W	120W	120W	30W
Power redundancy	1+1	1+1	1+1	1+1
Power input	110 ~ 240V	100 ~ 240V	100 ~ 240V	100 ~ 240V
Lightning and surge protection level	PSU: common mode: ±2kV, differential mode: ±1kV; Ethernet interface: ±1kV	PSU: ± 6KV@1.2/50us Ethernet interface: ± 4KV@10/700us	PSU: ± 6KV@1.2/50us Interface: ± 4KV@10/700us	PSU: ± 2.5KV@1.2/50us Interface: ± 4KV@10/700us
Weight	17KG	5.32KG	5.24KG	3.7KG
Environment				
Operating temperature	0 ~ 40℃	0 ~ 40℃	0 ~ 40℃	0 ~ 40℃
Storage temperature	-20 ~ 70℃	-25~70℃	-25~70℃	-40~70℃
Operating humidity	5% ~ 85%, non-condensing	5% ~ 90%, non-condensing	5% ~ 90%, non-condensing	5% ~ 85%, non-condensing
Storage humidity	5% ~ 95%, non-condensing	5% ~ 95%, non-condensing	5% ~ 90%, non-condensing	5% ~ 95%, non-condensing

Item	Z-FW-1800E-E12	Z-FW-1800E-E8	Z-FW-1800E-E4	Z-FW-1800E-E2
Hardware Specification				
Interface	8*GE+2*SFP+2*SFP+	4*GE+2*SFP	8*GE+2*SFP	5*GE+1*COMBO
USB	2	1	1	1
Console	1	1	1	1
CF card	8GB EMMC	32GB mSATA	8GB EMMC	8GB EMMC
Management	N/A	1MGT	N/A	N/A
Bypass (pairs)	2	1	N/A	N/A
Bypass feature	GE0/2<->GE0/3 GE0/4<->GE/5	fixed port:GE0/2<->GE0/3	N/A	N/A
Slot	2	N/A	N/A	N/A
Module(optional)	8GE 8SFP 4GE+4SFP 4SFP+	N/A	N/A	N/A
hard disk(optional)	1TB	1TB	N/A	N/A
Security Performance				
IPS throughput	2G	800M	300M	300M
AV throughput	2G	800M	300M	300M
NGFW throughput	10G	6G	2.1G	2.1G
System performance (throughput)				
1518 bytes	10G	6G	2.1G	2.1G
512 bytes	7.5G	4G	720M	720M
64 bytes	1.1G	0.65G	110M	110M
New sessions per second				
New sessions (TCP)	140000	40000	18000	18000
New sessions (HTTP)	117000	30000	11000	11000
New sessions (APP enabled)	47000	18000	3800	3800
New session (APP\IPS\AV enabled)	19000	9000	1400	1400

Concurrent sessions				
Concurrent sessions (APP disabled)	4000000	1000000	1000000	450000
Concurrent sessions (APP enabled)	2300000	600000	700000	240000
Concurrent sessions (APP\IPS\AV enabled)	2300000	600000	700000	240000
IPSec VPN performance				
IPSec tunnels	10000	5000	2300	1000
1400 bytes (without accelerator card)	3.4G	650M	450M	380M
SSL VPN performance				
New VPN Tunnels (clients) per second	130	30	15	15
Maximum concurrent users	3000	3000	1200	180
Throughput	770M	200M	125M	125M

Physical and electrical specifications				
Dimension(W*D*H)	440*330*44mm	360*440*44mm	440*330*44mm	240*182*28mm
AC power supply	AC	AC	AC	AC
Power consumption	100W	60W	30W	18W
Power redundancy	N/A	N/A	N/A	N/A
Power input	100 ~ 240V	110 ~ 240V	100 ~ 240V	100 ~ 240V
Lightning and surge protection level	PSU: ± 6KV@1.2/50us Interface: ± 4KV@10/700us	PSU: ± 2.5KV@1.2/50us Ethernet interface: ± 4KV@10/700us	PSU: ± 2.5KV@1.2/50us Interface: ± 4KV@10/700us	PSU: ± 2.5KV@1.2/50us Interface: ± 4KV@10/700us
Weight	4.44KG	4kg	3.5KG	1.24KG
Environment				
Operating temperature	0 ~ 40℃	0 ~ 45℃	0 ~ 40℃	0 ~ 40℃
Storage temperature	-25~70℃	-40 ~ 70℃	-40~70℃	-40 ~ 70℃
Operating humidity	5% ~ 90%, non-condensing	5% ~ 90%, non-condensing	5% ~ 85%, non-condensing	5% ~ 85%, non-condensing
Storage humidity	5% ~ 90%, non-condensing	5% ~ 90%, non-condensing	5% ~ 95%, non-condensing	5% ~ 95%, non-condensing

Order Information

NGFW Firewall	
Z-FW-1800E-X8430	Carrier-grade high-end 10G security firewall (2U) with a 1T hard disk, 1*HA interface, 1*management port, 2*USB ports, 4*extended module slots, and onboard 6*GE + 4*GE(SFP) (occupying one slot). It can be extended up to 30*GE, 28*GE(SFP), or 12*10G(SFP+) interfaces. It comes standard with dual AC power supplies and a 1-year USG license, including: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license
Z-FW-1800E-X6024R	Next-Generation Firewall (1U) with 16*GE + 4*GE(SFP) + 4*10GE(SFP+) ports, a 1T hard disk, and built-in dual AC power supplies, and a 1-year USG license including: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license
Z-FW-1800E-X6012R	Next-Generation Firewall (1U) with 8*GE + 2*GE(SFP) + 2*10GE(SFP+) ports, built-in dual AC power supplies, and a 1-year USG license including: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license
Z-FW-1800E-X3012R	Next-Generation Firewall (1U) with 8*GE + 2*GE(SFP) ports, built-in dual AC power supplies, and a 1-year USG license including: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license

Z-FW-1800E-E2	Desktop Next-Generation Firewall with 5*GE and 1*GE combo port, powered by an external adapter.
Z-FW-1800E-E4	Next-Generation Firewall (1U) with 8*GE + 2*GE(SFP) ports and a built-in single AC power supply.
Z-FW-1800E-E8	Next-Generation Firewall (1U) with 4*GE + 2*GE(SFP) ports and a built-in single AC power supply.
Z-FW-1800E-E12	Next-Generation Firewall (1U) with 8*GE + 2*GE(SFP) + 2*10GE(SFP+) ports and a built-in single AC power supply.
Z-FW-X3012R-USG-1Y	1-year package of all USG feature library upgrades for the Z-FW-X3012R next-generation firewall. It includes: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license
Z-FW-X3012R-USG-3Y	3-year package of all USG feature library upgrades for the Z-FW-X3012R next-generation firewall. It includes: 3-year virus library upgrade license 3-year URL classification library upgrade license 3-year IPS signature library upgrade license 3-year application signature library upgrade license
Z-FW-X6024R-USG-1Y	1-year package of all USG feature library upgrades for the Z-FW-X6024R next-generation firewall. It includes: 1-year virus library upgrade license 1-year URL classification library upgrade license 1-year IPS signature library upgrade license 1-year application signature library upgrade license
Z-FW-X6024R-USG-3Y	3-year package of all USG feature library upgrades for the Z-FW-X6024R next-generation firewall. It includes: 3-year virus library upgrade license 3-year URL classification library upgrade license 3-year IPS signature library upgrade license 3-year application signature library upgrade license