

|  |
| --- |
|  |

Next Generation Firewall ZXSEC US Series

**ZXSEC US2680B NGFW Datasheet**

**High Performance Next Generation/Edge Firewall for the Enterprise**

* Overview

Next Generation Firewall ZXSEC US Series consolidated security platforms deliver unmatched performance and protection while simplifying the network. ZXSEC US offers models to satisfy any deployment requirement from the ZXSEC US300B for small offices to the ZXSEC US6820B for large enterprises, service providers and carriers. ZXSEC US series A Products integrate the operating system with ASIC processor platform. ZXSEC US series B Products provide MIPS processor platform and the latest-generation CPUs to provide comprehensive, high-performance security. Each ZXSEC US includes the widest range of security and networking functions on the market, including:

Firewall, VPN, and Traffic Shaping

Intrusion Prevention System (IPS)

Antivirus/Antispyware/Antimalware

Application Control

Data Loss Prevention (DLP)

IPv6 Support

Web Filtering

Anti spam

VoIP Support

Layer 2/3 Routing

ZXSEC US appliances provide enterprise-class protection against network, content, and application-level threats. Dynamic updates ensure the customer’s systems are protected against the latest threats. ZXSEC US platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain (VDOM) capabilities to separate various networks requiring different security policies.

* Features

ZXSEC US Series next generation firewalls provide visibility and control of web applications regardless of port, protocol, or evasive action. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking inappropriate or malicious applications. ZXSEC US Series firewalls incorporate comprehensive network security and advanced firewall features. They provide superior price performance, excellent energy efficiency, and a smaller size when compared to competing products.

* Granular Application Control

ZXSEC US Series firewalls provide granular application control. Administrators can build policies that allow specific users or user-groups to access selected applications. (Allow Marketing to access Facebook). It is even possible to limit access to certain features within an application. (Allow Marketing to access MSN IM but Not file sharing). Policies can also be defined that block or limit access to applications. For example, certain games may be blocked during work hours but allowed after work hours. Alternatively, some applications may be allowed during work hours but with limited bandwidth.

* Proactive Threat Protection

ZXSEC US Series firewalls provide real-time protection for application and network attacks including viruses, spyware, worms, botnet , ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections. It incorporates a unified malware detection engine that shares packet details with multiple security defenses (IPS, URL filtering, and Anti-Virus), which significantly reduces latency.

* Visibility and Control

ZXSEC US Series provides visibility and control of network traffic. An intuitive user interface displays all applications traversing the network along with application categories and bandwidth. An administrator can quickly choose an application and see all the users who are accessing that application along with bandwidth consumption. If a particular user is of interest the administrator can see all the applications that user is using - now and in the past. Inappropriate applications can be blocked or limited by bandwidth or time of day. Multiple reports show top applications, top users, top URLs, top URL categories, top threats, etc.

* Deeper Visibility

With powerful intrusion prevention, application control and antimalware intelligence, the ZXSEC US allows you to look deeper into your content, applications, user and device behavior. Rich console views and reports together with a flexible policy engine provide the visibility and control you need to empower employees yet secure your enterprise.

* Industry Validation

The US family of physical and virtual appliances has earned more certifications than any other vendor by consistently meeting rigorous third-party standards. Our industry-leading technology provides you with air-tight security which you can safely count on.

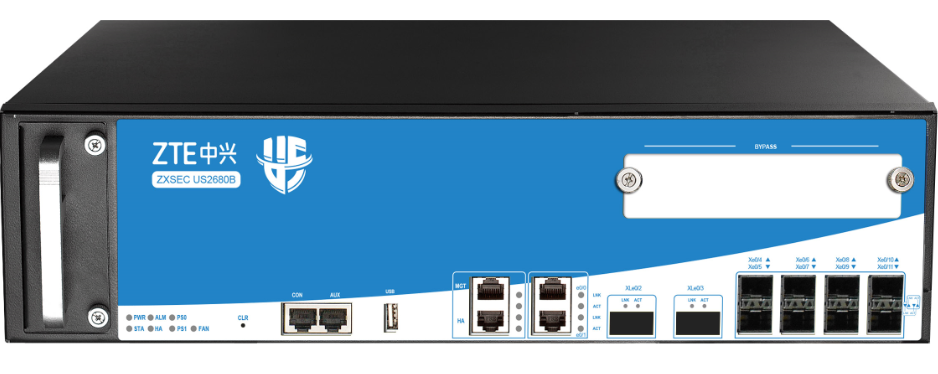
* Complete and Real-time Security

ZXSEC US Subscription Services provide automated, real-time, up-to-date protection against the latest security threats. Our threat research labs are located worldwide, providing 24x7 updates when you most need it.

* World-Class Technical Support and Documentation

ZTE support offerings provide comprehensive global support for all ZTE products and services. You can rest assured your ZTE security products are performing optimally and protecting your users, applications, and data around the clock.

* Specifications



|  |  |
| --- | --- |
| FW Throughput (Maximum) | 80Gbps |
| IPSec Throughput | 50Gbps |
| AV Throughput | 27Gbps |
| IPS Throughput | 35Gbps |
| Combined Throughput | 20Gbps |
| IPSec Tunnel Number | 20,000 |
| Maximum SSL VPN Users | 10,000 |
| Maximum Concurrent Sessions | 30M |
| New Sessions/s | 1.1M |
| Virtual Domains (Default / Maximum) | 10/250 |
| Management Ports | 1 x Console Port, 1 x AUX Port, 1 MGT, 1 x USB 2.0 Port, 1 x HA Port |
| Fixed I/O Ports | 2x GE, 8 x SFP+, 2 x QSFP+ |
| Available Slots for Extension Modules | 2 x Generic Slot，1 x Bypass Slot |
| Expansion Module Option | ZX-IOC-8GE, ZX-IOC-8SFP |
| Maximum Power Consumption | 1 x 450W Redundancy 1 + 1 |
| Power Supply | AC 100-240V 50/60Hz DC -40 ~ -60V |
| Dimension (W×D×H, mm) | 2.5U (440×460×110 mm) |
| Weight | 13.8kg |
| Package Size (W×D×H, mm) | 740×640×300 mm |
| Gross Weight | 19.9kg |
| Temperature | 32-104 F (0-40℃ ) |
| Relative Humidity | 10-95%(no dew) |

* Module Options

|  |  |  |
| --- | --- | --- |
| **Specification** | **ZX-IOC-8GE** | **ZX-IOC-8SFP** |
| Picture | **C:\Users\huangsang\Desktop\IOC-8GE-M_front.tif** | **C:\Users\huangsang\Desktop\IOC-8SFP-M_front.tif** |
| Name | 8GE Extension Module | 8SFP Extension Module |
| I/O Ports | 8 x GE | 8 x SFP, SFP module not included |
| Dimension | 0.5U (Occupies 1generic slots) | 0.5U (Occupies 1generic slots) |
| Weight | 0.8kg | 0.9kg |

* Highlights
* Secure Networking

Small Today’s network security threats have evolved into highly sophisticated assaults using multiple attack vectors to penetrate networks and steal valuable information. Small and medium enterprises and remote branch offices of larger enterprises face these attacks while storing and transferring increasing amounts of sensitive data across their networks. To ensure the security of this sensitive data, legislation such as PCI, HIPAA, Sarbanes-Oxley, and others have warranted the implementation of security measures

* The Needs of Small and Medium Enterprise and Branch Offices

In order to comply with legislation and secure the valuable data traversing networks, small and medium enterprises and remote branch offices need a security solution that integrates multiple attack recognition technologies into a single device. With limited budgets and modest remote resources, these smaller networks desire a cost effective solution that is simple to install, connect and maintain. Just as importantly, networks are ever-expanding and need a solution that leaves them with room to grow over time.

* Simple, Powerful, Secure

ZXSEC US are ideal security solution for small and medium enterprise or remote branch office networks, because they combine firewall, IPSec and SSL VPN, intrusion prevention, antivirus, antimalware, anti spam, P2P security, and web filtering to identify numerous types of threats from a single device. ZXSEC US installs in minutes, automatically downloading regular updates to protect against the latest viruses, network vulnerabilities, worms, spam and phishing attacks, and nefarious websites with no administrator intervention. Leveraging patented ASIC acceleration, ZXSEC US offers market leading performance, with ten ports that facilitate network growth and expansion.

* Functions Feature Specifications

**FIREWALL**

Network Services

Dynamic routing (OSPF, BGP, RIPv2)

Static and Policy routing

Route controlled by application

Built-in DHCP, NTP, DNS Server and DNS proxy

Tap mode – connect to SPAN port

IPv6 Support: Mgt. over IPv6, IPv6 routing protocols, IPv6 tunneling, IPv6 logging and HA

Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking)

L2/L3 switching & routing

Virtual wire (Layer 1) transparent inline deployment

**Firewall**

Operating modes: NAT/route, transparent (bridge), and mixed mode

Policy objects: predefined, custom, and object grouping

Application Level Gateways and session support: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323

NAT support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN

NAT configuration: per policy and central NAT table

VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing

Global policy management view

Schedules: one-time and recurring

QoS Traffic Shaping:

Max/guaranteed bandwidth tunnels or IP/user basis

Tunnel allocation based on security domain, interface, address, user/user group, server/server group, application/app group, TOS, VLAN

Bandwidth allocated by time, priority, or equal bandwidth sharing

Type of Service (TOS) and Differentiated Services (DiffServ) support

Prioritized allocation of remaining bandwidth

Maximum concurrent connections per IP

Virtual Firewall: Up to 250 vSYS load balanced firewalls

Load balancing:

Weighted hashing, weighted least-connection, and weighted round-robin

Session protection, session persistence and session status monitoring

Bidirectional link load balancing

Outbound link load balancing includes policy based routing, ECMP and weighted, embedded ISP routing and dynamic detection

Inbound link load balancing supports SmartDNS and dynamic detection

Automatic link switching based on bandwidth and latency

Link health inspection with ARP, PING, and DNS

Access control based on IP address geolocation

Repetitive and redundant firewall rule inspection

Security for file transmission based on name, size or type

**VPN**

IPSec VPN:

IPSEC Phase 1 mode: aggressive and main ID protection mode

Peer acceptance options: any ID, specific ID, ID in dialup user group

Supports IKEv1 and IKEv2 (RFC 4306)

Authentication method: certificate and pre-shared key

IKE mode configuration support (as server or client)

DHCP over IPSEC

Configurable IKE encryption key expiry, NAT traversal keep alive frequency

Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256

Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512

Phase 1/Phase 2 Diffie-Hellman support: 1,2,5

XAuth as server mode and for dialup users

Dead peer detection

Replay detection

Autokey keep-alive for Phase 2 SA

IPSEC VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)

IPSEC VPN configuration options: route-based or policy based

IPSEC VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode

One time login prevents concurrent logins with the same username

SSL portal concurrent users limiting

SSL VPN port forwarding module encrypts client data and sends the data to the application server

Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS

Host integrity checking and OS checking prior to SSL tunnel connections

MAC host check per portal

Cache cleaning option prior to ending SSL VPN session

L2TP client and server mode, L2TP over IPSEC, and GRE over IPSEC

View and manage IPSEC and SSL VPN connections

**User and Device Identity**

Local user database

Remote user authentication: TACACS+, LDAP, Radius, Active Directory

Single-sign-on: Windows AD

2-factor authentication: 3rd party support, integrated token server with physical and SMS User and device-based policies

**IPS**

7,000+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia

IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time

Packet logging option

Filter Based Selection: severity, target, OS, application or protocol

IP exemption from specific IPS signatures

IDS sniffer mode

IPv4 and IPv6 rate based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)

Active bypass with bypass interfaces

Predefined prevention configuration

**Threat Protection**

Over 1.3 million AV signatures

Botnet server IP blocking with global IP reputation database

Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, and FTP/SFTP

Flow-based web filtering inspection

Manually defined web filtering based on URL, web content and MIME header

Dynamic web filtering with cloud-based real-time categorization database: over 140 million URLs with 64 categories (8 of which are security related)

Additional web filtering features:

Filter Java Applet, ActiveX or cookie

Block HTTP Post

Log search keywords

Exempt scanning encrypted connections on certain categories for privacy

Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP

Web filter local categories and category rating override

Proxy avoidance prevention: proxy site category blocking, rate URLs by domain and IP address, block redirects from cache & translation sites, proxy avoidance application blocking, proxy behavior blocking (IPS)

**Application Control**

Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk

Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference

Actions: block, reset session, monitor, traffic shaping

Identify and control applications in the cloud

Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics

**High Availability**

Redundant heartbeat interfaces

Active/Active and Active/Passive

Standalone session synchronization

HA reserved management interface

Failover:

Port, local & remote link monitoring

Stateful failover

Sub-second failover

Failure notification

Deployment Options:

HA with link aggregation

Full mesh HA

Geographically dispersed HA

**Administration**

Management access: HTTP/HTTPS, SSH, telnet, console

web service APIs

System Integration: SNMP, syslog, alliance partnerships

Rapid deployment: USB auto-install, local and remote script execution

Dynamic real-time dashboard status and drill-in monitoring widgets

Language support: English

**Logs & Reporting**

Logging facilities: local memory and storage (if available), multiple syslog servers and

Encrypted logging and log batch log uploading

Reliable logging using TCP option (RFC 3195)

Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets

Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events

IP and service port name resolution option

Brief traffic log format option

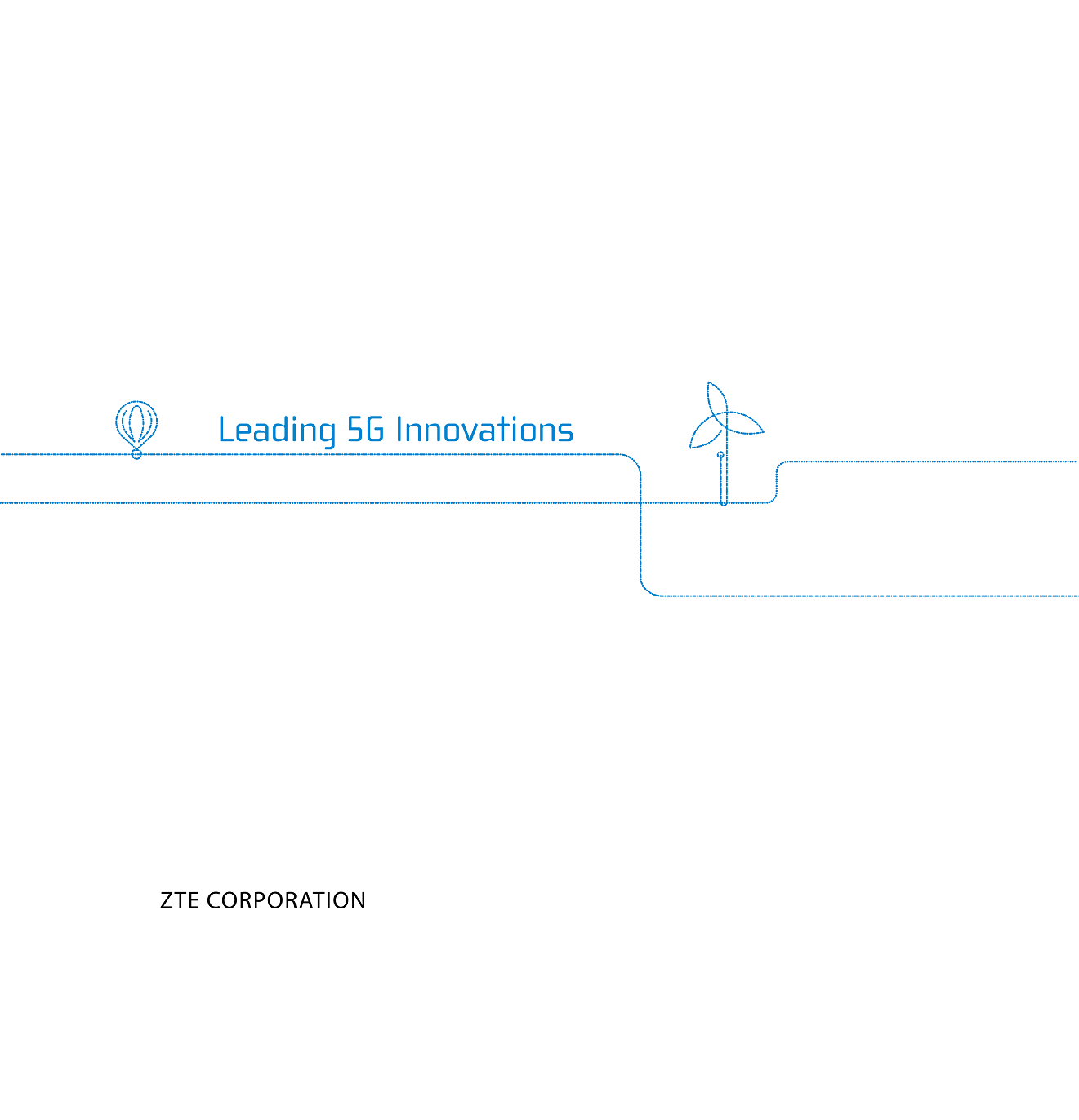
**SSL Decryption**

Inspect SSL encryption traffic

Supports IPS enablement for SSL encrypted traffic

Supports AV enablement for SSL encrypted traffic

Support URL filter for https encrypted traffic



NO. 55, Hi-tech Road South,ShenZhen,P. R. China

Postcode: 518057

Web: www.zte.com

Tel: +86-755-26770000

Fax: +86-755-26771999