Security Without Limits, AXGATE NF Series

AXGATE NGFW

AXGATE NEXT GENERATION FIREWALL

AXGATE
Security and Beyond

AXGATE NGFW

AI Driven, Next-Generation Firewall AXGATE NF Series

The AXGATE NF Series achieves maximum performance during operation through an engine design optimized for multi-core architecture and a proprietary load balancing algorithm.
In addition, it integrates multi-layered security features—including SSL encryption/decryption, application control, device control, VPN, and IPS—into a single platform, enabling the identification of threats within encrypted traffic and proactive response to advanced threats.

By leveraging AI technology that can be applied even in low-spec environments, we overcome the limitations of traditional firewalls with safer and smarter security, and proactively respond to advanced threats using robust quantum cryptography.

Features

- AI-based Threat Analysis
- APP Control
- Device Control
- SSL Inspection
- Virtualization
- QRNG
- PQC
- User-Friendly UI

Key Benefits

1 Application Control

- a Wide Range of Application Signatures
- Application Firewall Objects
- Object Definition using Predefined Filters

2 Visibility into Encrypted Traffic

- Proactively Blocking Web Security Threats by Securing Visibility into Encrypted Traffic
- Preventing Malware and Ransomware Infections in Advance
- Creating Decryption Zones for Encrypted Traffic and Supplying Decrypted Traffic to Existing Security Devices

3 Device Security

- Collect Device Information via Security Agent
- Control Devices based on Unique IDs (HDD Serial, MAC, IP, etc.)
- Restricts Access if Essential Programs are not installed or running
- Redirects to the installation page for required programs
- Uninstallation of Prohibited Program

4 AI-based Threat Analysis

- Delivers Optimal Performance even in low-spec environments
- License-based Model allowing Selection of only the Required Features
- Detects Threats in Encrypted Traffic by Combining Signature and AI Models
- Intelligent Analysis of Sophisticated Attacks through Decryption

Necessity

Security Threat	Necessity of AXGATE NF Series
Increasing IP Traffic Volume	Effective Handling Required Due to Surge in Session Volume
Transition to Encrypted Services	Need for Visibility into Encrypted Traffic
Evolution of Applications	Need to Distinguish and Control Applications and Users
Increasingly Sophisticated Security Threats	Need for Advanced Security Technologies
Existing Cryptographic Systems Threatened by Advancements in Quantum Technology	Need for Adoption of Post-Quantum Cryptography
Changes in the Work Environment	Need to Shift from Perimeter Security to Zero Trust Security

Specifications

Classification		AXGATE NF 200	AXGATE NF 400
Appearance			
CPU		4 Core	4 Core
Memory		8 GB	16 GB
Storage	System	eMMC 64 GB	SSD 250 GB
	Log	SSD 500 GB	SSD 500 GB
NIC	Slot	-	-
	1GC	8	12
	1GF	-	4
	QRNG	Option	Option
Power		Single	Single
FW Throughput		8 G	16 G
IPS Throughput		4 G	4.1 G
VPN Throughput		3.9 G	4.6 G
VPN Tunnels		40,000	50,000
Concurrent Session		3,000,000	8,000,000

Classification		AXGATE NF 6000	AXGATE NF 8000	AXGATE NF 10000
Appearance				
CPU		20 Core	16 Core * 2	24 Core * 2
Memory		64 GB	128 GB	256 GB
Storage	System	SSD 250 GB	SSD 250 GB	SSD 250 GB
	Log	SSD 2 TB	SSD 4 TB	SSD 4 TB
NIC	Slot	4	8	8
	1GC	8 (max 24)	0 (max 64)	0 (max 64)
	1GF	8 (max 24)	8 (max 64)	8 (max 64)
	10GF	0 (max 12)	4 (max 32)	4 (max 32)
	40GF	0 (max 4)	0 (max 16)	0 (max 16)
	100GF	0 (max 4)	0 (max 16)	0 (max 16)
	QRNG	Option	Option	Option
Power		Redundant	Redundant	Redundant
FW Throughput		116 G	250 G	320 G
IPS Throughput		60 G	100 G	130 G
VPN Throughput		29 G	42 G	61 G
VPN Tunnels		100,000	120,000	120,000
Concurrent Session		40,000,000	80,000,000	100,000,000

Detailed Features

NGFW

Application-Based Policy Control	QoS Policy Features by Application/User ID
7-Tuple Security Policies	Various Redundancy Protocols such as VRRP, IP Backup, and HARP
Various Network Address Translation Functions (SNAT, DNAT, LSNAT, Net-NAT, NAT64, IPv6-to-IPv6, etc.)	Vulnerability Checks for Policy Application to Any Object and Address/Service Objects Beyond a Specified Range
Harmful Site Block by Integrating with the Safenet DB from the Korea Communications Standards Commission	Detect and Block Abnormal Activities Based on Signatures, Protocols, and Traffic
Object Panels within Policies	Implement Filtering Techniques at the Kernel Level for Packet Processing
FQDN Objects	Map View-Based Country IP Lookup and Control
Implementing a Firewall System with Role-Based User Authentication Policies	

SSL Inspection

Automatic Detection of SSL Sessions and Automatic Exclusion of Non-Standard SSL Sessions from Decryption	Selective Decryption and Decryption Exceptions by Source, Destination, and Service
Port Conversion and Various Traffic Options When Linked with Mirroring Ports	Integration with Various Security Devices such as IDS, IPS, and APT without Network Changes
Simultaneous Encryption/Decryption of Forward and Reverse Traffic	Block Malicious and Non-Business Sites
SSL Decryption Bypass Based on System Resource Load Conditions	Certificate Distribution Guidance and Distribution Status

IPsec VPN

Equipped with Post-Quantum Cryptography (PQC) Algorithms	Supporting Integrity Algorithms (SHA1 / SHA256, 384, 512 / HAS160 / etc.)
Standard IPSec Protocol and Both IKE v1 and v2	Line Bonding for Multiple Lines
Enhanced Random Number Security with Quantum Random Number Generator (QRNG)	Active-Active Configuration Without L4 Switch via Multi-Tunnel Support
Connection Blocking in Case of VPN Unmanned Branch Device Theft	

Monitoring / Management Features

Vulnerability Checks for Policy Application to Any Object and Address/Service Objects Beyond a Specified Range	Policy Activation/Deactivation Based on Designated Interface and Communication Status with External Hosts
Administrator Privilege Profiles	REST API for All Features
Registration of Dedicated UI Web Server Certificates and Externally Issued Certificates	Simultaneous Configuration Change Notifications for Multiple Administrators
Traffic/Session Monitoring by Application and User	Calendar-Based Scheduled Reports and Comparison with Previous Reports

Virtualization

Providing Up to 250 Virtual Domains	Selective Assignment of Various Physical/Logical Interfaces to Virtual Domains
Independent Static and Dynamic (OSPF) Routing per Domain	Domain-Specific Administrators and Statistical Reports

Device Control Features

Alias Feature for Easy Monitoring of Device-Collected Identifiers (UUID) by Administrators	Automatic Object Classification Based on Various Device Status Information
Collection of Various Device Status Information	Input/Configuration and Statistics for Device Connection Reasons
Firewall Blocking When Essential Programs or Processes Are Not Running on the Device	Clipboard Usage Restriction and Local Resource Restriction for Remote Desktop

Product Inquiry : Global_BD@axgate.com / 070-4034-6413