

FlexNGFW

Deep packet inspection with centralized threat management for branch and edge security

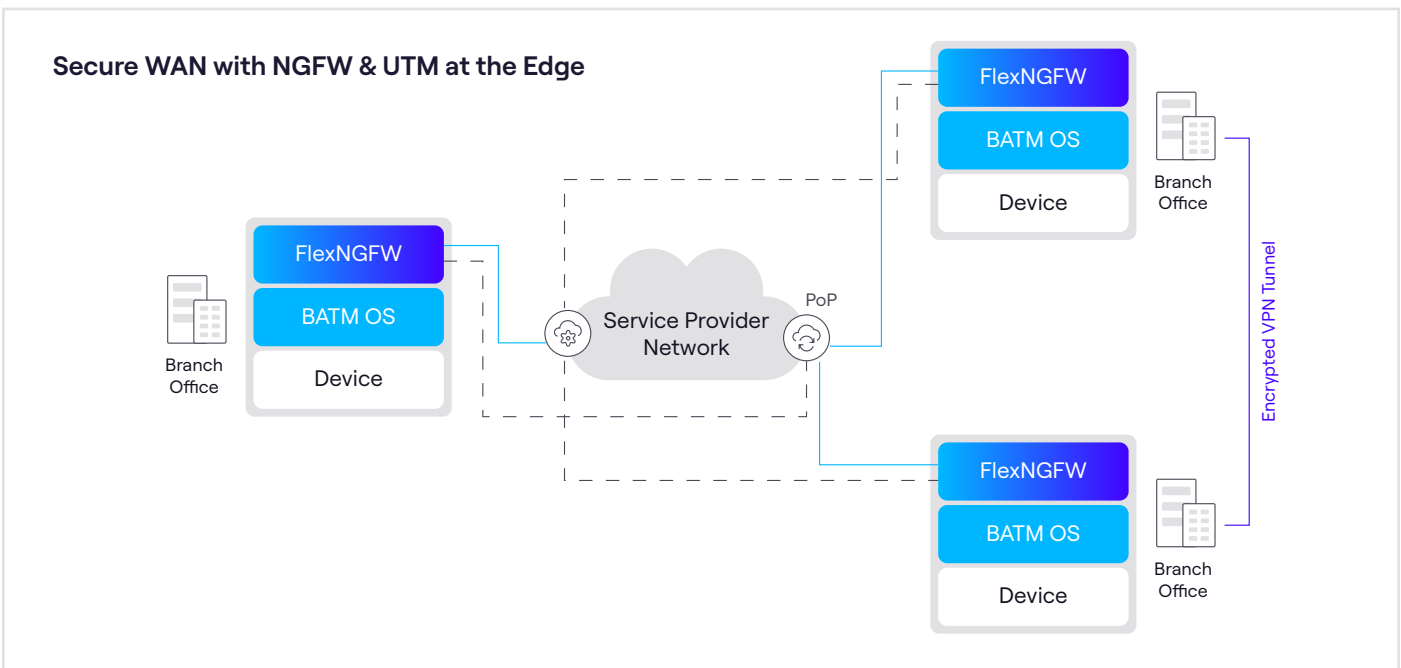
Layer-7 Security with Unified Threat Management for Distributed Networks

FlexProtect NGFW provides Layer-7 security inspection and unified threat management for branch and edge environments, combining deep packet inspection, intrusion prevention, malware protection, and application-aware policy enforcement in a single, high-performance NGFW device.

Designed for distributed deployments, FlexProtect NGFW delivers consistent security controls, full traffic visibility, and centralized management across multiple sites, without introducing WAN optimization or SD-WAN dependencies.

Key Benefits

- ✓ **Full Visibility & Control:** Inspect user, device, and application traffic at Layer 7 to enforce consistent security policies across all sites.
- ✓ **Application-aware Traffic Control:** Detect and classify over 3,000 applications to apply granular traffic shaping, prioritization, and access policies.
- ✓ **Integrated Threat Prevention:** Protect against known and emerging threats using IDS/IPS, stateful firewalling, IP reputation filtering, and geo-blocking.
- ✓ **Reliable Performance:** Support up to 1 Gbps throughput with high availability, redundancy, and state synchronization for uninterrupted operation.



FlexNGFW Hardware

Validated hardware profiles for branch and edge routing deployments, supporting wired, fiber, and wireless WAN access.



Armortec NC-GM4M



Silicom Ibiza



Armortec NC-C632D

Category	Small Device	Medium Device	Large Device
	Armortec NC-GM4M	Silicom Ibiza	Armortec NC-C632D
Form Factor	Fanless appliance	Fanless appliance with integrated antennas	Fanless appliance
CPU	Intel® Celeron® J4125 (4 cores)	Intel® Atom® x7405C (4 cores)	Intel® Atom® C3558 (4 cores)
Memory	8 GB	8 GB	8 GB
Storage	64 GB	64 GB	64 GB
Ethernet Interfaces	4 × 1 Gbps RJ45	4 × 2.5 Gbps RJ45	6 × 1 Gbps RJ45
Fiber Interfaces	-	1 × 1 Gbps SFP cage	2 × 10 Gbps SFP+ cages
Console Port	1 × RJ45	-	1 × RJ45
USB / Video	2 × USB, 1 × VGA	-	2 × USB, 1 × VGA
Expansion Slots	1 × Mini-PCIe	1 × PCIe	1 × Mini-PCIe
LTE Support	-	Up to 2 × 4G LTE dual-SIM radio cards (optional)	Via Mini-PCIe (optional)
5G Support	-	Up to 2 × 5G sub-6 dual-SIM radio cards (optional)	Via Mini-PCIe (optional)
Wi-Fi Support	-	Wi-Fi AP / client card (optional)	-
SIM Support	-	Integrated (per radio module)	External SIM expansion slot
Primary Use Case	Basic wired branch	Multi-access branch with wireless WAN	High-throughput edge / aggregation

Reliable Network Connectivity



Reliable Secure VPN

Secure connectivity for branch offices and remote locations



Network Address Translation

High-performance NAT for seamless traffic flow



High Availability

Minimize downtime and ensure business continuity

Advanced Security for Optimal Network Control



Application Visibility & Control

Deep Packet Inspection to identify and classify over 3,000 unique applications

Informed policy enforcement with custom application risk levels

Full visibility into application traffic, preventing lateral movement of threats across the network

Granular application usage policies for optimized resource allocation



Geo-blocking

Network traffic filtering with integrated GeoIP database

Restricts access from high-risk or suspicious locations

Customized geo-blocking policies for granular access control



Stateful Firewall

Dynamic monitoring of active network connections

Inspecting and filtering of IP packets based on trusted source & destination parameters



Device Intelligence

Detects and classifies connected devices, providing full visibility into device behavior

Identification of anomalies in device behavior patterns



Traffic Optimization

Secures bandwidth for critical applications and services

Minimizes latency and ensures resource efficiency

Unified Threat Management



Intrusion Detection and Prevention System

Extensive database of intrusion detection signatures

Protects against sophisticated code injection attacks

Detects and mitigates DoS/DDoS attack signatures and patterns



IP Reputation

Continuously updates local IP reputation database with latest threat intelligence

Blocks high-risk IPs based on real-time global threat analysis



DoS/DDoS Protection

Advanced traffic shaping and rate-limiting capabilities

Geo-fencing policies to block traffic from locations associated with attack sources



Antivirus Scanning

Stream-based scanning for real-time inspection of files, regardless of size

Configurable policies to allow, block, or log detected malware



Web Content Filtering

Categorizes web traffic in real time for granular access control

URL blacklists/whitelists with wildcard matching for flexible customization

Web usage logs for monitoring, analytics, and compliance purposes



Reverse Proxy

Intercepts incoming requests and forwards to backend servers while masking server identities

Prevents direct exposure of internal servers

Enhances performance with load balancing, caching, SSL/TLS offloading, and intelligent routing of HTTP requests



Botnet Blocking

Identifies and blocks communication with known botnet command-and-control servers

Intercepts inbound and outbound traffic to and from botnet-associated IP addresses

Performance Spec

Feature	Spec
Firewall throughput	Up to 1000Mbps
VPN throughput	Up to 1000Mbps
IPS throughput	Up to 1000Mbps
Concurrent connections	128,000
Concurrent VPN Tunnels (IPsec)	500
Ethernet interfaces	Up to 10
Virtual Interfaces (IEEE 802.1q/802.1ad)	1024
Virtual Routers	50
High Availability	Yes

BATM enables enterprises, communications service providers, and system integrators to build and operate resilient, secure, and flexible networks across distributed environments.

For more information contact us at salesnetworks@batm.com.