Datasheet

NG2000

HIGH PERFORMANCE UTM & NEXT-GENERATION FIREWALL

PRODUCT HIGHLIGHT

UNIQUE GATEWAY ARCHITECTURE

Combine digital security with productivity and improve your network's protection level. Its Policy based ISP Failover & Load Balancing to distribute important applications over more robust Internet links and less imp. App. over backup connections and also to provide redundancy.

SIMPLICITY, SECURITY & SCALABILITY

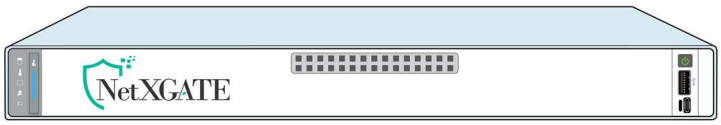
The Next-Generation Firewall allows for the creation of policies for applications, users, groups, programming, and other features that are not available in conventional firewalls.

COMPLETE VISIBILITY (BYOD)

UTM enabled HotSPOT Gateway Management engine feature enhance the in NG-Series to inspect, detect and monitor the traffic and control the devices being used by employees or guest.

MODERNITY & FLEXIBILITY

Secure Access Gateway is the core engine of NG-Smart VPN technology. It is ideal for establishing a secure tunnel over any WAN link. Result- reductions in cost, optimization of time and easy management, alternative to costly MPLS.



The NetXGATE NG2000, specifically designed for Most Demanding Networks and especially big educational Institute / Universities. It scales to support up to concurrent 3000+ users depending on your network load, and your specific deployment scenario. It provides Gigabit performance with all the features and tools available in enterprise end appliances. NG2000 and all other NetXGATE appliances offer comprehensive network security with easy configuration and unified management. This ensures an optimized solution for any geographically dispersed enterprise deployment.

It comes with built in **AAA | User Management Hotspot** functionalities for individual user control on both wired and wireless network. It also helps to provide secure Internet access to guest along lawful Tracking & Filtering with detailed in-built logs and reports on every configured features.
Performance and security: NG2000 is versatile, scalable, robust & rack mountable. With throughput that can reach 75.0 Gbps, look no further for better value and performance to secure next generation traffic

FEATURES	HARDWARE SPECIFICATIONS
Interfaces	8 /12 GbE + 4 SFP+
Modularity	Copper and Fibre Interfaces Both
Firewall Throughput	75.0 Gbps
Firewall IMIX	30.0 Gbps
Concurrent Sessions	3,00,00,000
New Sessions / Sec.	3,10,000
SSL VPN Throughput	9.10 Gbps
NG UTM Throughput	9.10 Gbps
AV Throughput	11.0 Gbps
IPS Throughput	12.5 Gbps
Storage-SSD	256 x 2 GB
Memory /Max	16 / 32 GB
Firewall Policies	Unrestricted
Maximum Connections	Unrestricted
Inbound NAT Connection	Unrestricted
Local User Database	Unlimited
Suggested concurrent Users /Devices	3000 +

SPECIFICATIONS

NETWORK Services
- Multi-Link Auto Failover.
- 4G LTE Support : SIM* |USB Dongle |Tethering
- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Configurable LAN/WAN/DMZ Ports
- NAT & ALG Support - DNAT ,SNAT , PAT
- Routing - Static, Source , Destination & Policy based
- Policy Rule : predefined, custom & Grouping
- Authentication, Authorization & Accounting.
- Support Multicast Forwarding , VLAN Tagging
- Static, DHCP, PAP/CHAP Support

NETWORK SECURITY
- Stateful & Deep Packet Inspection Firewall
- Application Visibility & Control.
- Demilitarized Zone (DMZ)
- Zone - based access control list.
- Access scheduling
- Flooding detection and protection
- Stops all types of DoS; Prevents DNS Spoofing & Flooding, Bypass Websites, Packet Capturing
- IP-Mac bind, MAC Whitelist / Blacklist.
- Comprehensive DNS policy

LINK LOAD BALANCING
- Bi-directional link load balancing
- Outbound link load balancing includes policy based routing and weighted, and dynamic detection
- Inbound link load balancing supports Smart DNS & dynamic detection
- Automatic link switching based on Traffic, latency, jitter, connectivity etc.
- Link health inspection with ARP, PING, and DNS

URL FILTERING
- Web or URL / IP / Geography / Keyword / Port / Application Filter
- Block predefined categories on specific time
- Create | Edit | Delete Manual Categories & Add exception
- Manually defined web filtering based on URL, web content. Key word and MIME header
- Web filtering profile override: allows admin to temporarily assign different profiles to User/IP
- Web filter local categories and category rating override
- Additional web filtering features:
  - Force Google Safe search
  - Force educational YouTube
  - Exempt scanning encrypted connections on certain categories for privacy

USER| GUEST MANAGEMENT |AAA
- ID & Password login – fixed users
- Approval-based Login.
- Social Media & OTP based login
- BYOD Self & Voucher Registration with OTP
- Create users with auto-expiry, Renew & Block
- Seamless connectivity from Wired to W-LAN
- Auto Login /No Authentication after First Login
- Auto login based on IP & MAC or combination
- Concurrent logins, auto MAC binding
- Easy migration - import/export data
- Restrictions based on Device & OS
- Create user groups & apply policies
- Allow login only when user comes from specific segments

BANDWIDTH MANAGEMENT | QoS
- Define enhanced quality of service (QoS)
- Max/Guaranteed bandwidth tunnels or IP/User basis
- Bandwidth allocated by time, priority, or equal bandwidth sharing
- Restrict users based on data, b/w &time
- Individual and shared bandwidth quota
- Contention ratio based bandwidth allocation.
- Schedule based committed & burstable b/w.
- Configure multiple b/w policy on a user at different hours of day

VIRTUAL PRIVATE NETWORK
- Virtual private network
- SSL VPN - TCP/UDP tunnelling with failover
- Encryption – 3DES,DES,AES, Blowfish
- Hash algorithms - MD5, SHA-1, SHA-2
- Authentication – pre-shared key, certificates
- Supports IKEv1 and IKEv2.
- DH groups - 1, 2, 5, 14, 15, 16, 17…
- NAT traversal & PFS support
- SSL authentication – AD, LDAP, radius, local
- Multi-layer client authentication - certificate, username/password ,mac address , OTP*
- Network access - Split and Full tunnelling
- Granular access control to all network resources
- Administrative controls - session timeout, DPD
- User and group policy enforcement
- Multicast support over SSL VPN
- SSL VPN deployment modes: Client to site , Site to Site
- View and manage IPSEC and SSL VPN connections
- Supports SSL VPN clients that run Windows, Linux, iOS & Android

CAPTIVE PORTAL CAPABILITIES
- Intuitive self-service portals for users.
- Customise captive form input fields
- Mobile/desktop responsive login page
- Social media based login, mac based auto login
- Create hourly and day based plans with FUP
- Accounting based on hours, days, data transfer

INTRUSION PREVENTION
- Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopaedia
- IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- IDS sniffer mode
- Predefined prevention configuration

ANTI-VIRUS & ADVANCE THREAT PROTECTION
- Virus, Worms, Trojan detection & removal
- Spyware, Malware, Phishing, Bot & Pharming protection
- Manual, automatic push or pull signature updates
- Scans HTTP/S, FTP, SMTP/S, POP3, IMAP
- Block files based on their type.
- Threat logs with action.
- Compressed file virus scanning
- Spam filtering

ATTACK DEFENCE
- Abnormal protocol attack defence
- Anti DoS / DDoS, including SYN Flood, UDP Flood, DNS Query Flood defence, TCP fragment, ICMP fragment etc.
- ARP attack defence

DATA LEAKAGE PREVENTION
- Restricts file upload over HTTP, FTP, P2P and other file sharing applications.
- Blocks file transfer (upload & Download) over IM like Facebook, Whats-app & other Social Sites .
- Controls file upload /download over HTTPS/SSL websites.
- Logging & Reporting in accordance to HIPAA, CIPA compliance.

SYSTEM MANAGEMENT
- System Configuration Backup / Restore
- Auto/ Manual backup of User & Threat Logs
- Enable appliance & PMS remote access
- Set auto/manual firmware updates
- Create Child Admins and check logs
- Set NTP , SMTP Email
- Integrate Syslog, SNMP, Net-flow
- Three levels of users: Admin | Operator | Monitor
- Dynamic real-time dashboard status and drill-in monitoring widgets

LOGS | REPORTING |MONITERING
- Real-time traffic statistic and analytics
- User Management & Account Expiry Report
- Bandwidth ,Data usages & Session Report
- Web Browsing & Records surfing logs of each user
- Search logs based on User, IP, Site ,Time & File Type
- Change Log Report / Activity Timeline
- Comprehensive event logs: system & admin activity audits, routing & networking, VPN, user authentications,
- User & System based overall and user wise analytics
- Real Time monitoring Tools to get visibility into network Traffic & Bandwidth consumption
- On-Appliance (Local) Logging and reporting facilities
- Reports can be exported in PDF, Word and via Email
- System information such as concurrent session, CPU, Memory and temperature
- Support traffic information collection and forwarding via Net-flow

ALERT MANAGEMENT
- Real-time alerts to user on data consumption limit, voucher expiry etc.
- Real-time alerts to admin on link failure & Speed, Remote Access etc.
- Schedule Alerts for specific reports

SMS GATEWAY
- Pre-configured SMS gateway*
- Click –n-configure custom gateway
- Facilitates different message templates

VULNERABILITY ASSESSMENT
- Scans LAN Devices for vulnerability
- Generates summary and detailed reports of found possible threats

CUSTOM DEVELOPMENT
- Personalized development on request*
- Third party application Integration*

HIGH AVAILABILITY
- Active-Passive with state synchronizations
- Stateful Failover to Keep-Alive Sessions
- Redundant heartbeat interfaces

HARDWARE
- From factor- 1U /2U
- Memory - 16 / 32 GB
- SSD – 256 / 512 GB
- Modularity – Copper and Fibre Interfaces.
- 2 USB Ports, 1 VGA, 1HDMI
- Dimension-(mm)-(HxWxD)- 44x438x470
- Weight- 8.5 Kg

POWER AND RELIABILITY
- Power Supply – 2 x 200 W ATX
- Operating Temperature - (0°C ~ 40°C)
- Storage Temperature - (-20°C ~+70°C)
- Relative humidity - 10% - 90%, no condensing

SecurITy made in India

All specification and photos are subject to change without prior notice
1. Maximum throughput performance is measured under ideal test conditions using industry standard performance test tools. 2. Firewall UDP throughput performance is based on RFC 2544 guidelines. 3. All Performance values are upto or rough guideline only and vary depending on system configuration. 3. IPS throughput (http) measured using default IPS rule set and 512KB object size. 4. VPN throughput measured using multiple tunnels with 512KB response size. 5. Testing done with multiple flows through multiple port pairs. +if all slot populated

www.netxgate.com | 9891@netxgate.com | +91-9891-412158

#628 ,Signature Global Mall , Sec-3 , Vaishali , GZB , Delhi /NCR – 201012 (INDIA)

6/1 , 1st Main , Vasanth Nagar Bangalore – 560 052 (INDIA)