Hillstone A-Series

Next-Generation Firewall

The Hillstone A-Series next-generation firewall features high security performance, expansion as needed, complete advanced threat detection and prevention, and smart and automated policy operation. This future-ready NGFW series is based on a brand new hardware architecture that offers industry-leading application layer performance to meet real-world network security needs. High-density ports ensure excellent access capability, and large storage options offer better visibility and analytics. The Hillstone A-Series NGFW offers complete, advanced defenses against known and unknown threats, coupled with smart, automated and efficient policy operation that makes security operations easy.

Product Highlights

Advanced Threat Detection and Protection

The Hillstone A-Series NGFW includes a full arsenal of mechanisms to provide real-time detection and protection across the full lifecycle of network attacks and malwares. Before a breach can even occur, proactive protections like IPS block the vulnerabilities exploitation. IP reputation services block requests from risky sites potentially involved in malware and spamming. URL filtering prevents users from inadvertently accessing sites associated with phishing, malware downloads and other exploits. Anti-virus detects and blocks known malwares at the network level with an advanced signature database that is continuously updated. Anti-spam provides real-time spam classification and prevention for both inbound and outbound traffic.

During a breach, anti-virus plays an important role as well by continuing to detect and block known malwares. A cloud sandbox provides sophisticated detection and prevention of malicious files through static analysis and pre-processing, followed by behavioral analysis that includes detection of evasive maneuvers. Cloud intelligence then identifies and blocks malicious files, generates logs and reports, and shares threat intelligence back to the cloud.

Completing protections across the full threat lifecycle, the A-Series continues to defend even after a breach has occurred. Hillstone's advanced Botnet C&C prevention feature prevents communication to the control channel, and detect and block bots within the intranet as well.

Further, the system's unified threat detection and analytics engine coordinates across all built-in security mechanisms to dramatically enhance efficiency while reducing network latency.

© 2021 Hillstone Networks All Rights Reserved.

Product Highlights (Continued)

High-Performance Hardware Architecture

The future-ready A-Series features compact form factor and a powerful computing foundation that ensures high performance with uncompromising security. A-Series NGFWs offer robust performance for firewall throughput, concurrent and new sessions, and blazing fast performance for application layer, which is critical in meeting the needs of current security environments. It also offers a friendly software ecology for third-party integration to support additional security features if desired. All rackmount models feature front and rear ventilation to assist in heat dissipation, which is a concern in networks of almost any size.

Excellent Access Capability and Storage Expansion

The Hillstone A-Series offers high I/O port density, allowing the NGFW to act as a switch or router as needed, lowering deployment and management costs. In addition, expansion slots are available for a number of A-Series models to further increase performance. Bypass pairs on most A-Series models help ensure business continuity.

All models, including the desktop versions, include a large 8 GB onboard storage and have expansion options for very-large hard disk storage up to 2 TB. With more storage the system can save more logs and data for longer time, enabling deeper analysis. In addition, the expanded storage allows the system to provide richer reports with far more information, including visualized results and actionable recommendations. Further, with deeper threat analysis the WebUI can display much richer threat detection information, which in turn gives admins better visibility. The increased visibility lets admins quickly zero in on anomalies and other suspicious network events or traffic, analyze them and respond.

Smart Policy Operation

The A-Series includes intelligent management and operation across the full policy lifecycle, from deployment to management, optimization and operation. The system features automated user policy deployment using RADIUS dynamic authorization. Policy management is made far more efficient through policy groupings based on business requirements. In addition, policies can be aggregated to allow a set of policies to act as a single policy. An innovative policy assistant analyzes traffic patterns and recommends refined policies for faster, easier and more accurate policy management. Policy operation is made more efficient and precise through policy redundancy checks, which identify redundant policies for deactivation or deletion, and policy hit count analysis, that helps further refine and adjust policies.

© 2021 Hillstone Networks All Rights Reserved.

Features

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 – connects to SPAN port
- Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking)
- L2/L3 switching & routing
- Multicast(PIM-SSM)
- Virtual wire (Layer 1) transparent inline deployment

Firewall

- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Policy objects: predefined, custom, aggregate policy, object grouping
- Security policy based on application, role and geo-location
- 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 and ALG 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
- Security policy redundancy inspection, policy group, policy configuration rollback, aggregate policy
- Policy Assistant for easy detailed policy deployment
- Policy analyzing and invalid policy cleanup
- Comprehensive DNS policy
- Schedules: one-time and recurring
- Support policy import and export

Intrusion Prevention

- 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
- IPS threat packet capture (with expansion storage only)

Antivirus

- Manual, automatic push or pull signature updates
- Manually add or delete MD5 signature to the AV database
- MD5 signature support uploading to cloud sandbox, and manually add or delete on local database
- Flow-based antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Compressed file virus scanning

Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment, etc.
- ARP attack defense
- Allow list for destination IP address

URL Filtering

- 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
- Support URL allow list and block list

Anti-Spam

- Real-time Spam Classification and Prevention
- Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- Protection Regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Inbound and outbound detection
- White lists to allow emails from trusted domains

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP, FTP and SMB
- Support file types including PE, ZIP, RAR, Office, PDF, APK, JAR, SWF and Script
- File transfer direction and file size control
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Support detection only mode without uploading files
- URL allow / block list configuration

Botnet C&C Prevention

- Discover intranet botnet host by monitoring C&C connections and block further advanced threats such as botnet and ransomware
- Regularly update the botnet server addresses
- Prevention for C&C IP and domain
- Support TCP, HTTP, and DNS traffic detection
- Allow and block list based on IP address or domain name
- Support DNS sinkhole and DNS tunneling detection
- Support DGA detection

IP Reputation

- Identify and filter traffic from risky IPs such as botnet hosts, spammers, Tor nodes, breached hosts, and brute force attacks
- Logging, dropping packets, or blocking for different types of risky IP traffic
- Periodical IP reputation signature database upgrade

SSL Decryption

- Application identification for SSL encrypted traffic
- IPS enablement for SSL encrypted traffic
- AV enablement for SSL encrypted traffic
- URL filter for SSL encrypted traffic
- SSL encrypted traffic whitelist
- SSL proxy offload mode
- Support application identification, DLP, IPS sandbox, AV for SSL proxy decrypted traffic of SMTPS/POP3S/IMAPS

Endpoint Identification and Control

- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operating systems including Windows, iOS, Android, etc.
- Support query based on IP, endpoint quantity, control policy and status etc.
- Support the identification of accessed endpoints quantity across layer 3, logging and interference on overrun IP
- Redirect page display after custom interference operation
- Supports blocking operations on overrun IP
- User identification and traffic control for remote desktop services of Windows Server

Data Security

- File transfer control based on file type, size and name
- File protocol identification, including HTTP, FTP, SMTP, POP3 and SMB
- File signature and suffix identification for over 100 file types
- Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols
- IM identification and network behavior audit
- Filter files transmitted by HTTPS using SSL Proxy and SMB

Application Control

- Over 4,000 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 cloud applications in the cloud
- Provide multi-dimensional monitoring and statistics for cloud applications, including risk category and characteristics

Quality of Service (QoS)

- 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

© 2021 Hillstone Networks All Rights Reserved.

Features (Continued)

- 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
- Bandwidth allocation based on URL category
- Bandwidth limit by delaying access for user or IP
- Automatic expiration cleanup and manual cleanup of user used traffic

Server Load Balancing

- Weighted hashing, weighted least-connection, and weighted round-robin
- Session protection, session persistence and session status monitoring
- Server health check, session monitoring and session protection

Link Load Balancing

- Bi-directional link load balancing
- Outbound link load balancing: policy based routing including ECMP, time, weighted, and embedded ISP routing; Active and passive real-time link quality detection and best path selection
- Inbound link load balancing supports SmartDNS and dynamic detection
- Automatic link switching based on bandwidth, latency, jitter, connectivity, application etc.
- Link health inspection with ARP, PING, and DNS

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
  - IKEv1 support DH group 1,2,5,19,20,21,24
  - IKEv2 support DH group 1,2,5,14,15,16,19,20,21,24
  - 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
- PnPVPN
- VTEP for VxLAN static unicast tunnel

IPv6

- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE
- IPv6 routing including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, Antivirus, Access control, ND attack defense, iQoS
- IPv6 jumbo frame support
- IPv6 Radius support
- IPv6 support on the following ALGs: TFTP, FTP, RSH, HTTP, SIP
- IPv6 support on distributed iQoS
- Track address detection

VSYS (only available on rackmount models)

- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support firewall, IPsec VPN, SSL VPN, IPS, URL filtering, app monitoring, IP reputation, QoS
- VSYS monitoring and statistic, app monitoring, IP reputation, AV, QoS

High Availability

- Redundant heartbeat interfaces
- Active/Passive and peer mode
- 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
- Dual HA data link ports

Twin-mode HA (only available on A3000 and above models)

- High availability mode among multiple devices
- Multiple HA deployment modes
- Configuration and session synchronization among multiple devices

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
- User group synchronization based on AD and LDAP
- Support for 802.1X, SSO Proxy
- WebAuth: page customization, force crack prevention, IPv6 support
- Interface based authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor
- Support IP-based and MAC-based user authentication
- Radius server issues user security policy via CoA message

Administration

- Management access: HTTP/HTTPS, SSH, telnet, console
- Central Management: Hillstone Security Manager (HSM), 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 storage; up to 6 months log storage with expansion storage (SSD hard drive), syslog server, Hillstone HSM or HSA
- Encrypted logging and log integrity with HSA scheduled batch log uploading
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets, URL etc.
- 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
- Three predefined reports: Security, Flow and Network reports
- User defined reporting
- Reports can be exported in PDF, Word and HTML via Email and FTP

Statistics and Monitoring

- Application, URL, threat events statistic and monitoring
- Real-time traffic statistic and analytics
- System information such as concurrent session, CPU, memory and temperature
- iQOS traffic statistic and monitoring, link status monitoring
- Support traffic information collection and forwarding via Netflow (v9.0)

CloudView

- Cloud-based security monitoring
- 24/7 access from web or mobile application
- Device status, traffic and threat monitoring
- Cloud-based log retention and reporting

© 2021 Hillstone Networks All Rights Reserved.

Specifications

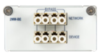
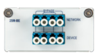
	SG-6000-A1000	SG-6000-A1100	SG-6000-A2000	SG-6000-A2600
Firewall Throughput [1]	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput [2]	1.2 Gbps	1.2 Gbps	1.2 Gbps	1.8 Gbps
Threat Protection Throughput [3]	800 Mbps	800 Mbps	800 Mbps	1.6 Gbps
Maximum Concurrent Sessions [4]	300,000	300,000	1 Million	1.2 Million
New Sessions/s [5]	48,000	48,000	48,000	120,000
IPS Throughput [6]	3.2 Gbps	3.2 Gbps	3.2 Gbps	4.5 Gbps
AV Throughput [7]	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
Virtual Systems (Default/Max)	N/A	N/A	1/5	1/5
Management Ports	1 × Console Port, 2 × USB3.0 Port	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)
Fixed I/O Ports	4 × GE	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A
Expansion Module Option	N/A	N/A	N/A	N/A
Twin-mode HA	N/A	N/A	N/A	N/A
Local Storage	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	256 GB SSD	256 GB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD
Power Specification	30W, Single AC	50W, Single AC	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
Dimensions (W × D × H, inches)	10.6 × 6.3 × 1.7	10.6 × 6.3 × 1.7	17.2 × 12.6 × 1.7	17.2 × 12.6 × 1.7
Weight	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

© 2021 Hillstone Networks All Rights Reserved.

Specifications (Continued)

	SG-6000-A3000	SG-6000-A3600	SG-6000-A3700	SG-6000-A3800
Firewall Throughput (1)	20 Gbps	20 Gbps	20 / 40 Gbps	20 / 40 Gbps
NGFW Throughput (2)	1.8 Gbps	1.8 Gbps	1.8 Gbps	3.7 Gbps
Threat Protection Throughput (3)	1.6 Gbps	1.6 Gbps	1.6 Gbps	2.8 Gbps
Maximum Concurrent Sessions (4)	2 Million	3 Million	6 Million	8 Million
New Sessions/s (5)	140,000	140,000	140,000	310,000
IPS Throughput (6)	8.3 Gbps	8.5 Gbps	8.6 Gbps	17.5 Gbps
AV Throughput (7)	4.8 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
Virtual Systems (Default/Max)	1/5	1/50	1/100	1/100
Management Ports	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
Fixed I/O Ports	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)
Available Slots for Expansion Modules	N/A	N/A	1	1
Expansion Module Option	N/A	N/A	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD
Power Specification	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44
Dimensions (W × D × H, inches)	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7
Weight	13.2 lb (6 kg)	13.2 lb (6 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Module Options

	IOC-A-4SFP+	IOC-A-2MM-BE	IOC-A-2SM-BE
			
Names	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module
I/O Ports	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)
Dimension	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

NOTES:

(1) Firewall throughput data is obtained under UDP traffic with 1518-byte packet size. The firewall throughput for A3700 and A3800 can be increased from 20 Gbps to 40 Gbps via additional IOC-A-4SFP+ expansion module;

(2) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;

(3) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;

(4) Maximum concurrent sessions is obtained under HTTP traffic;

(5) New sessions/s is obtained under HTTP traffic;

(6) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;

(7) AV throughput data is obtained under HTTP traffic with file attachment.

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R8. Results may vary based on StoneOS® version and deployment.

www.HillstoneNet.com

© 2021 Hillstone Networks All Rights Reserved.

Version: EX-08.01-NGFW-A-Series-5.5R8-0221-EN-03