

Acme Packet Net-Net 3800

Acme Packet's Net-Net 3800 is a session border controller (SBC) for service providers, security and defense-focused government agencies, enterprise sites and contact centers requiring control for up to 4000 VoIP/Unified Communications (UC) sessions. The platform operates Acme Packet's industry-leading Net-Net OS to provide the critical control for delivering trusted, first class interactive communications—voice, video and multimedia sessions—across IP network borders. These controls span five areas - security, service/application reach maximization, SLA assurance, regulatory compliance and cost/revenue management. The Net-Net 3800 complements Acme Packet's Net-Net OS-E, 2000, 4000 and high-end Net-Net 9000 series platforms and supports all of the same SBC functions and features.



Acme Packet Net-Net 3800

Solutions

For service providers, the Net-Net 3800 SBC secures the subscriber access and interconnect/peering borders. It enables interoperability of heterogeneous endpoints, service infrastructure elements and networks to maximize service reach. It controls session admission, call/session control/server loads and overloads, IP network transport and SIP/H.323 session routing to assure SLAs, maximize revenues and minimize costs. Lastly, the Net-Net 3800 enables regulatory compliance with emergency service (E911), national government priority service (GETS) and lawful intercept (CALEA) requirements.

For enterprise and contact center sites, the Net-Net 3800 secures the high quality delivery of a broad range of interactive communications services and applications ranging from basic VoIP to Service Oriented Architecture (SOA)-enabled unified communications. It secures the SIP/H.323 trunking border to service provider IP networks and the Internet border to remote offices, teleworkers and mobile employees. In extremely security-conscious organizations, the Net-Net 3800 even secures the border to the private VPN connecting other sites. The SIP and H.323 interworking capabilities of the Net-Net 3800 ensures interoperability with and between legacy IP PBX equipment and next-generation unified communications platforms. The Net-Net 3800 controls session admission, IP PBX or UC server loads and overloads, IP network transport and SIP/H.323 session routing to assure SLAs and minimize costs. Regulatory compliance requirements are also satisfied with encryption ensuring session privacy and call/session replication for recording.

For government defense and security-focused agencies, the Net-Net 3800 meets the stringent requirements needed to comply with standards such as the U.S. Federal Information Processing Standard (FIPS) and Common Criteria. Acme Packet's implementations of SIP-TLS, SRTP, IPsec, SSH and SFTP all comply with FIPS 140-2 without requiring special hardware. The Net-Net 3800 assures proper implementation of security functionality, counter common/known threats and are documented as sufficiently free from flaws, vulnerabilities and side effects to meet U.S. Common Criteria Evaluation Assurance Level (EAL) 4. It also features configuration options to mitigate security vulnerabilities required for product approval by the U.S. Defense Information Services Agency (DISA).

Net-Net OS for SBCs

Acme Packet Net-Net® OS, our operating software, offers industry-leading, proven session border control functionality in many dimensions:

- **Session control protocols** - SIP, H.323, SIP-H.323 interworking, MGCP/NCS, H.248 and RTSP
- **Control functions & features** - comprehensive session control in the areas of security, application/service reach maximization, SLA assurance, regulatory compliance and cost/revenue management
- **Carrier-class high availability (HA)** - check-pointing of media, signaling & configuration state ensures no loss of active calls, or call state required for NAT traversal, session handling (transfer/hold, etc.) or accounting
- **Integrated, hardware-software-based DoS/DDoS protection** - dynamic SBC self-protection against layer 3/4, IPsec and signaling protocol-related attacks and overloads
- **Management** - Net-Net EMS and SAS, CLI, telnet, FTP, XML, RADIUS, SNMP, syslog
- **Proven interoperability** - production deployments with all major IP PBXs, Unified Communications platforms, SIP servers, application servers, media servers, media gateways, softswitches, IMS CSCF elements, H.323 gatekeepers, call agents, and numerous IP-based voice and video endpoints

Net-SAFE™, Acme Packet's security framework, is supported via the tight integration of the Net-Net 3800 hardware and Net-Net OS software. Net-SAFE features powerful denial-of-service/distributed denial-of service protection at the layer 3, layer 4, IPsec and SIP signaling level, and intrusion detection/prevention capabilities. Other security features support dynamic access control, topology hiding, privacy and confidentiality, service infrastructure DoS/DDoS protection, virus and SPIT protection, and fraud prevention.

Net-Net EMS, a GUI/browser-based client/server application supporting configuration, fault, performance and security management for multiple border elements in multiple networks, is one of many management tools available. Net-Net EMS can efficiently integrate into existing and next-generation enterprise management or service provider operational support systems through industry-standard SOAP/XML, SNMP v2c and syslog interfaces. Other management tools include command line interface (CLI), telnet, file transfer protocol (FTP) and RADIUS.

Net-Net 3800 capacity, performance and availability

The Net-Net 3800 supports up to 4000 sessions, offers high availability operation for non-stop service and includes hardware acceleration options for encryption and QoS measurements. It complements Acme Packet's Net-Net 2000, 4000 and 9000 series platforms.

- Session capacity* - up to 4000 simultaneous signaled sessions
- High-availability (HA) configuration - active/standby systems (1:1 redundancy) with check-pointing of signaling, media and configuration state for no loss of service
- In-line, wire-speed QoS measurement processor option
- Two-level encryption acceleration hardware options
 - Session set-up - IPsec tunnels and TLS sessions
 - Traffic encryption/decryption - IPsec and SRTP
- IPsec tunnel capacity
 - Up to 1000 tunnels with manual keys
 - Up to 5000 tunnels with IMS-AKA
- Local route table entries - up to 1,000,000 routes
- Network interfaces - four active 10/100/1000 Mbps Ethernet interfaces
- System throughput - 5 Gbps

* Performance and capacity vary by signaling protocol, call flow, codec, configuration and feature usage.

Net-Net 3800 specifications

Chassis	1U, rack-mount Front - power and HA status LEDs, physical system reset pinhole, console and local storage interfaces Rear - one network interface unit slot (signaling, media and management interfaces), single fixed power supply, outgoing air exhaust Optional mounting brackets for front/rear or center-mount in 19" or 23" rack
Memory	1 GB for active configuration and operation 256 MB internal flash memory for file storage (operating software, configuration, accounting, log)
Content addressable memory (CAM)	128K entries for static & dynamic ACLs, media control rules and ARP entries
Encryption options	TLS - Software-based encryption for low capacity TLS sessions - Secure Services Module (SSM) hardware accelerator for high capacity TLS sessions SRTP - Network Interface Unit-based encryption processors IPsec - Tunnel set-up - software-based for use of manual keys; Secure Services Module (SSM) hardware accelerator for use of dynamic keys - Traffic encryption - Network Interface Unit-based encryption processors
Network interfaces unit (NIU)	Service network interface options for signaling, media and data - Four 10/100/1000 Mbps Ethernet copper ports (RJ-45 connector) NIU management interfaces - included on all NIU options - Two 10/100/1000 Mbps interfaces with RJ-45 for HA node configurations - One 10/100/1000 Mbps interface with IPsec encryption processor and RJ-45 for management networks (Optional IPsec encryption of management interface via encryption capable NIU) - One RS-232 serial console interface with RJ-45 connector (only rear or front interface may be used at any time) - One alarm interface with RJ-45 connector

Front panel management interfaces	One RS-232 serial console interface with RJ-45 connector (only rear or front interface may be used at any time) One USB 2.0 interface LEDs for displaying power and HA status Physical system reset pinhole
Power	Single AC power supply, 230 VA max Voltage: Autoranging 100-240 VAC wide input with power factor correction Frequency: 50/60 Hz Current: 1.5A at 115 VAC and .75A maximum at 230 VAC Cable: 2.0 meter 18 AWG 3-wire cable, with 3-lead IEC-320 receptacle on the power supply end, and country-dependent plug on the power source end
Physical	
Dimensions	1.72 in H x 17.10 in W x 19.00 in D (not including mounting hardware) 4.37 cm H x 43.43 cm W x 48.26 cm D (not including mounting hardware)
Weight	18 lbs (8.16 kg) fully configured
Colors	Front panel - Midnight black with Glacier blue trim
Temperature	Operating: 32°F to 104°F, 0°C to +40 °C Storage: -4°F to 149°F, -20°C to +65 °C
Relative humidity	10 to 85%, non-condensing
Air flow	30 cfm front to back
Heat dissipation	100W (341 BTU/hour) typical, 160W (546 BTU/hour) maximum
Power dissipation	100W typical, 180W maximum
Regulatory	Product bears CE ¹ marking indicating compliance with the 99/5/EC directive, which includes EN and IEC standards for safety and EMI
Safety	US: USA/CSA UL ² 60950-1, 1st Ed. Canada: CAN/CSA ³ -C22.2 No. 60950-1-03, 1st Ed. EU: EN ⁴ 60950-1:2001
EMI	US: FCC ⁵ Part 15 (CFR 47) Class A limits Canada: ICES ⁶ -003 Issue 4, Class A limits EU: EN 55 022:1998 +A1:2000 + A2:2003 Class A limits Germany: FTZ 1TR9 Australia: CISPR 22 and C-Tick Japan: VCCI ⁷ Class A
Immunity	EU: EN 55 024:1998 + A1:2001 +A2:2003 EU: EN 300 386 v1.3.3

¹CE = European Compliance

²UL = Underwriters Laboratory

³CSA = Canadian Standards Association

⁴EN = European Norm

⁵FCC = Federal Communications Commission

⁶ICES = Interference-Causing Equipment Standard

⁷VCCI = Voluntary Control Council for Information Technology Equipment (Japan)