inGate

Enterprise Session Border Controllers (E-SBCs)

- Ingate SIParator® / Firewall®
- Ingate Software SIParator® / Firewall®

Product Family

SIParator/Firewall S95/S97/S98
4000/8000/20000 Calls maximum*

SIParator/Firewall S42/82
2000/4000 Calls maximum*

SIParator/Firewall S22
800 Calls maximum*

Software SIParator/Firewall
Calls maximum: As much as the hardware supports
For x86 virtual machines and for the clouds.

* Calls = Concurrent RTP Sessions, SIP Trunks, 20 ms G.711 packets

aws   Microsoft Azure   Google Cloud   openstack CLOUD SOFTWARE

Why Ingate?

- Cost-effective
- Ease of installation
- Scalable 1-20,000 sessions
- Firewall and NAT traversal
- SIP and SIP media routing

- WebRTC media (ICE lite)
- Q-TURN server (patented)
- Quality of Service (QoS)
- SIP normalization and repair
- Support for remote workers

- Security, firewall
- Interoperability
- Diagnostics
- Proven, reliable

In More Than 10,000 Installations Worldwide
Ingate makes it easy to connect SIP trunks to PBXs,
Unified Communications (UC) solutions and call centers.

20A

Ingate Systems AB · Phone: + 46 8 600 77 50 · Ingate Systems Inc. · Phone: + 1 603 883 6569
info@ingate.com · www.ingate.com

1

The Enterprise Session Border Controller For Your Network

The Ingate SIParator® is a powerful, flexible and cost-effective E-SBC for SIP connectivity, security and interoperability, such as connecting PBXs and Unified Communications (UC) solutions to SIP trunking service providers.

The Ingate Firewall®, which is always included in the product, makes the Ingate SIParator an all-in-one appliance for data security as well as the E-SBC.

Ingate Software SIParator/Firewall is a software deliverable for virtual machines and for the cloud (Amazon Web Services, Microsoft Azure, OpenStack and Google Cloud Platform).

Ingate's SIP Trunking Startup Tool configures the SIParator in three easy steps.

Feature Summary of the Ingate SIParator/Firewall®

SIP Security Features
- Topology hiding
- Authentication against a RADIUS server or local database
- Access control
- Intrusion Detection System / Intrusion Protection System
  o Denial of Service and Distributed Denial of Service attacks
  o Malformed message attacks
  o RTP session hijacking
  o SIP spam (SPIT)
- Signaling Encryption interworking:
  UDP/TCP/TLS/SIP over WSS/SIP over VPN
  (in any combination)

SIP Functions
- SIP proxy
- B2BUA on a per call basis
- SIP Registrar
- PBX and ITSP interoperability
- Load balancing of SIP traffic
- DNS override for SIP requests
- Strict SIP parser
- Dynamic port opening/closing, controlled by SIP proxy
- Maintains the state of all sessions and rejects all unrelated SIP packets
- Header manipulation and regular expressions
- HTTP requests from Dial Plan
- IPv4, IPv6 support
- WebRTC SIP over WSS, Media DTLS-SRTP/ICE
- TURN and Q-TURN server

Quality of Service (QoS)
- Classification and Prioritization
- Bandwidth limitation
- DSCP (diffserv)

VPN Functionality
- IPSec
- PPTP (server)
- Certificate/PSK(shared secret)/XAUTH(user, password)
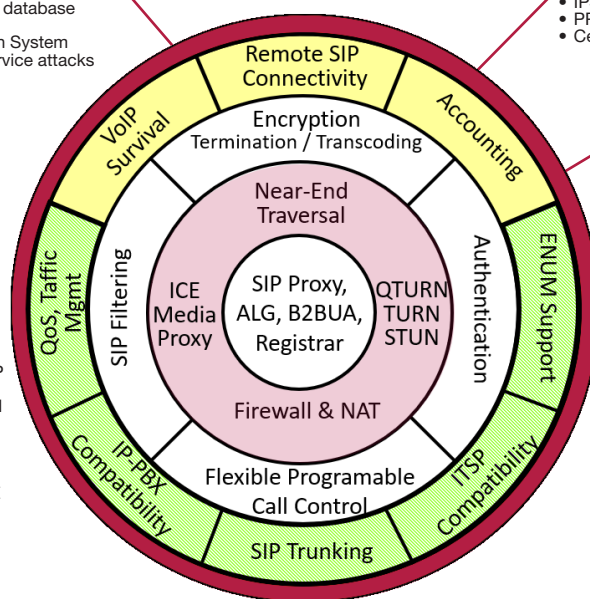
Firewall/Routing
- Stateful inspection
- Packet filtering
- Provides flexible NAT and PAT
- Dynamic port forwarding
- IPv4, IPv6 relays

Monitoring and Diagnostics
- SNMP
- Internal logging to HD
- Logging to PCAP file
- Syslog
- Automatic check for new releases
- Monitoring using SIP OPTIONS

Media
- Dynamic port opening/closing, controlled by SIP proxy
- Media Encryption interworking RTP/SRTP/DTLS-SRTP
- Transcoding between any of: PCMU, PCMA, G722 and G729A, OPUS and SILK

Diagram labels: Remote SIP Connectivity, VoIP Survival, Accounting, Encryption Termination / Transcoding, Near-End Traversal, SIP Proxy, ALG, B2BUA, Registrar, QTURN TURN STUN, ICE Media Proxy, SIP Filtering, QoS, Traffic Mgmt, Authentication, ENUM Support, Firewall & NAT, IP-PBX Compatibility, Flexible Programable Call Control, SIP Trunking, ITSP Compatibility

Bringing Global SIP Communications to the Private Network

Ingate SIParators are enterprise session border controllers (E-SBCs) made for small to large enterprises and service providers to provide a secure solution for bringing SIP into the private network. Traditional firewalls block SIP communications or if opened, compromise security and/ or don't provide full quality for IP telephony and UC communications. The SIParator works with existing SIP-unaware firewalls to allow and secure SIP traffic, maintaining the existing security infrastructure.

Available in a range of sizes, Ingate's security products offer unprecedented value to enterprises adopting SIP.

Ingate's award-winning SIParators also include a fully featured stateful inspection and packet filtering enterprise firewall. The SIParator, in addition to its SIP functionality, can also be used as the enterprise's main firewall. The built-in firewall also provides a complete and secure environment for the SIParator functions and customer services, all in one and the same product.

Firewall and NAT (Network Address Translation) traversal and SIP security are fundamental functions of an E-SBC. SIP, like all real-time communication protocols, is blocked by firewalls, not being aware of SIP signaling and media. The SIParator's SIP proxy routes the SIP traffic and opens media ports in the built-in NAT/firewall to securely deliver calls to the protected enterprise LAN.

The SIParator connects any type of ITSP's SIP trunk, managed like MPLS or over the public Internet, and also connects home workers and road warriors. Ingate's FENT (Far End NAT Traversal) function connects SIP phones and soft clients behind remote NAT/firewalls.

Trusted Network Security for VoIP and Unified Communications

Ingate's SIP proxy architecture grants fully secure NAT/firewall traversal of the SIP traffic, so does its ICE support, using STUN and TURN for client based NAT/firewall traversal.

The SIParator's enhanced security can handle and add TLS (Transport Layer Security) as well as WSS (Web Socket Secure) for secure SIP signaling. It also supports and transcodes SRTP (Secure Real-Time Transport Protocol, both SDES-SRTP and DTLS-SRTP) for encrypted voice and video. The high level of security and confidentiality further includes authentication and replay protection and other firewall means to shield users from eavesdroppers, hackers and spoofers and protect against theft of service.

SIP IDS/IPS (Intrusion Detection System/Intrusion Prevention System) works in tandem with Ingate's existing security technologies, further strengthening security for VoIP, SIP trunking, UC and other SIP applications.

Diagnostics, Troubleshooting and Monitoring

The SIParator has extensive logging and diagnostic features, to ease troubleshooting and resolve problems quickly. It can also directly generate PCAP traces, allowing more extensive analyses with WireShark and similar tools. There is a built-in test agent that can schedule calls and assess MOS scores.

The voice quality of calls can be monitored and reported via RADIUS, including packet loss, jitter, delay and MOS score.

## Reliability, Load Balancing and High Availability Failover

The SIParator fully supports load balancing and failover using

DNS SRV and speeds up failover by monitoring SIP servers.

In addition, the SIParators can be used in failover pairs. By synchronizing long time states and allowing the idle device to take over at the Ethernet level, this failover method also protects against software faults, since it directly allows dropped calls to be setup freshly again. The largest Ingate E-SBC servers (S95/S97/S98) are highly protected against hardware failure with redundant dual power supplies and RAID 1 hard disks. The powerful Ingate desktop models (S22/S42/S82) manages 800/2000/5000 concurrent calls and can also be used in failover pairs. All models except the S22 allow permanent continuous logging to internal hard disk for monitoring.

Flexible Network Deployment Scenarios

The Ingate SIParator/Firewall can be implemented in various ways to fit the customer network:
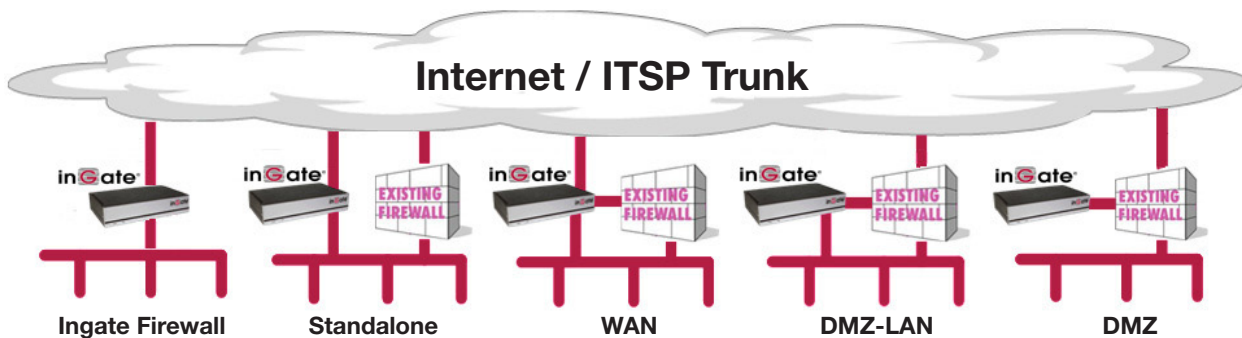
QoS (voice quality over data-crowded accesses) is provided by the SIParator. DMZ-LAN & DMZ modes also require QoS setup in existing firewall.

Software Modules and Licenses

SIP Trunking allows over 100 trunk groups and configures the SIP trunk between IP-PBXs and SIP trunking services in three easy steps. Licenses for the number of concurrent calls needed over a particular trunk group are easily added. The Back-to-Back User Agent (B2BUA) brings extensive SIP normalization for interoperability and a dial plan including support for regular expressions, header manipulation, prefix addition / removal and much more.

Remote SIP Connectivity lets remote workers leverage the benefits of Unified Communications by performing Far-End NAT Traversal (FENT) to allow home workers and road warriors to use their SIP clients behind well-behaved remote NATs and firewalls. One simply adds the number of Remote User SIP Session licenses needed.

Quality of Service (QoS) prioritizes voice and video traffic and allocates bandwidth to assure the highest voice quality, undisturbed by data traffic. This is a standard feature and also

enables computation and reporting of Mean Opinion Scores (MOS) and other voice quality metrics on a per call basis.

Ingate VoIP Survival is another standard feature, allowing an enterprise using a hosted PBX solution to fail over to the Ingate, to enable internal calls and redirect outside calls to a local PSTN gateway.

SIP Registrar user licenses make the Ingate SIParator or Firewall the primary registrar server and permits SIP clients to register.

TURN and Q-TURN are now standard features with a capacity shared among all calls through the SIParator (the total number of licenses for concurrent sessions). Q-TURN is Ingate's patented technology for a TURN server between the LAN and the WAN, allowing prioritized real-time traffic separated from data traffic often congesting the Internet access. The TURN server can also be used stand alone for a service provider's users and works with WebRTC and other real-time protocols using ICE/STUN/TURN.

The Ingate Advantage

For enterprises, Ingate provides for a seamless transition to SIP and Unified Communications globally. Ingate enables fast, simplified deployments with controlled firewall border traversal, for quality and security.

For service providers, Ingate products offer a high-quality, reliable SIP trunk demarcation point between the customer's IP-PBX and the service provider network. Placed at the customer network edge (locally as a CPE, at the service provider or in the cloud), Ingate provides secure firewall traversal, interoperability, diagnostics and security to simplify SIP trunk deployments whether over a managed connection or the public Internet.

Flexible and advanced Call Control REST API, for adding and extending various service provider, contact center and PBX features and functions. The configurable API allows integration with external web services during call processing, by HTTP commands modifying the SIP requests being processed.

Ingate Software SIParator® / Firewall®

Ingate's SBC, the SIParator®/ Firewall® is available as one of six hardware products or as various software variants for virtualized x86 hardware (for your own or for clouds). The customer selects which is best for the application, depending on the service, VoIP, UC and security equipment involved.

The Software SIParator®/Firewall® has complete feature parity with Ingate's SBC hardware products. The Software SIParator®/ Firewall® is delivered as an ISO file that runs on all major commercial hypervisors.

Like all Ingate SBCs, the Software SIParator®/Firewall® makes secure SIP-based communications – including VoIP, SIP Trunking and Unified Communication (UC) – possible. With Ingate's Software SIParator SBC you can harness the benefits of secure real-time communication without introducing new hardware products.

The Ingate Software SIParator® / Firewall® is the ideal solution for carriers, IP-PBX vendors, system integrators, and all customers that want to deploy the SIParator on virtual x86 machines, typically on COTS (Commercially Off The Shelf) servers.

Ingate Cloud SIParator® / Firewall®

If the VoIP, WebRTC, UC or real-time applications have components in a commercial cloud, it may be beneficial (or necessary) to deploy the Ingate SIParator SBC in the same cloud. The Ingate Cloud SIParator® / Firewall® is now available for Amazon Web Services (AWS Marketplace) for Microsoft Azure, OpenStack and Google Cloud Platform.

Ingate's SIParator for the commercial cloud platforms is a software version of Ingate's SIParator, specially customized for each of the cloud platforms.

Like all Ingate's SBCs the Ingate Cloud SIParator/Firewall, is a key component to build secure SIP-based communications - including VoIP, RTC, SIP Trunking and UC.

Ingate's SIParator is – contrary to many other SBCs - a real-time session (RTS) firewall and router for both signaling and media, handling both front end and back end SBC needs in the same device and only pulling media into the cloud when required.

Ingate SIParator® / Firewall® S22

The S22 model is a small fan less (silent) desktop device, but still capable of handling 800 simultaneous calls. It was recently introduced and has a new rack mounting kit option, now being a tray where two S22 (if needed) can be mounted side by side, occupying only 1U space.

Ingate SIParator® / Firewall® S42/S82

These midrange desktop models with hard disks for permanent logging and monitoring, replace Ingate's classic S5x server type models and comes standard with "ears" that can be used for both 19" rack mounting and for wall mounting.

The S42/S82 have two SFP+ 1/10 Gbps network ports, for fiber and direct access cables as standard and the S82 has very high capacity.

Ingate SIParator® / Firewall® S95/S97/S98

The Ingate SIParator®/Firewall® S95/S97/S98 are high capacity, high performance SBCs designed for large enterprises, call centers and service providers, and can handle up to 20,000 concurrent calls (RTP sessions). This server line comes with dual redundant power supplies and hard disks for very high reliability.

Optional Power Over Ethernet for the S42 and S82
On special request, the S42 and the S82 models can be equipped with Power Over Ethernet to feed local VoIP phones.

Wireless WiFi and LTE Additions for Volume Projects
Upon request, for volume projects, Ingate can add WiFi modules for the LAN side of the S22, S42 and S82 models. For the WAN side connection, the S42 and S82 models can be equipped with a 4G/LTE wireless module.

Since 2001, Ingate® Systems has been developing firewall technology to enable SIP-based communication to provide the best access for telephony, global real-time and unified person-to-person communication. Ingate offers enterprises, service providers and carriers elegant solutions for SIP trunking and trusted real-time communications beyond the LAN. Ingate products are used by retail companies, financial institutions, industrial firms, government agencies, call centers and small-to-large enterprises throughout Europe, Asia and North America.

Technical Specifications Ingate SIParator® / Firewall®

Feature	Ingate SIParator S22	Ingate SIParator S42	Ingate SIParator S82
Interfaces 10/100/1000 Mbps Ethernet	4	6	6
Interfaces 1/10 Gbps DA/SFP+ optical	No	2	2
DISK:	SATA DOM SDD	500 GB	500 GB
Dimension WxDxH	180x132x34 mm	250x252x44 mm	250x252x44 mm
Rack Mounting Kit	Optional tray for 2 units	Rack ears included	Rack ears included
Certifications	CE, FCC, UL, CB	CE, FCC, UL, CB, AS/NZS	CE, FCC, UL, CB, AS/NZS
Power consumption (typical)	10W	20W	30W
External power supply 100 – 240 V AC	12 V DC, 2 A	12 V DC, 5.4 A	12 V DC, 5.4 A
Management/Configuration options: Web GUI (HTTP, HTTPS), CLI (SSH, serial cable) and HTTP Rest API	Yes	Yes	Yes, also IPMI port
SNMP, V1, V2, V3	Yes	Yes	Yes
VLAN Support	Yes	Yes	Yes
Internal log to HD	No	Yes	Yes
Logging to PCAP file	Yes	Yes	Yes
Syslog	Yes	Yes	Yes
Support for failover multiple ISPs	Yes	Yes	Yes
Failover to secondary incactive device	Yes	Yes	Yes
External RADIUS server authentication for IPsec, GUI and SIP	Yes	Yes	Yes
Free software upgrades, incl. with Support	Yes	Yes	Yes
Firewall functionality*			
Stateful inspection	Yes	Yes	Yes
Packet filtering	Yes	Yes	Yes
Throughput (Mbit/s) (1500 byte packets)	400	1000	1000
Packets per second (46 byte packets)	50 000	250 000	250 000
DHCP client and PPPoE	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes
DHCP proxy	Yes	Yes	Yes
Proxies for TCP, UDP and FTP	Yes	Yes	Yes
Flexible NAT and PAT	Yes	Yes	Yes
VPN functionality			
VPN tunnels	100	600	600
3DES (168) (Mbit/s) (1438 byte packets)	20	50	50
AES (128-bit) (Mbit) (1438 byte packets)	30	100	100
X.509 certificate, shared secret or XAUTH	Yes	Yes	Yes
Generating of X.509 certificates for clients	Yes	Yes	Yes
PPTP server	Yes	Yes	Yes
IPsec (IKEv1 and IKEv2)	Yes	Yes	Yes
SIP functionality			
SIP proxy	Yes	Yes	Yes
SIP registrar	Yes	Yes	Yes
SIP traffic to private IP addresses (NAT/PAT)	Yes	Yes	Yes
SIP Connection set up, max calls/s	40	60	60
RTP media packet delay (+ at transcoding packets)	0.02-0.07 ms (+ voice packet ms)	0.02-0.07 ms (+ voice packet ms)	0.02-0.07 ms (+ voice packet ms)
Number of concurrent calls (20 ms G.711 voice packets)	800	2000	4000
Secure VoIP (TLS+SRTP) transcoding sessions	550	1100	2200
Media Transcoding (G.722, G.729, G.711; OPUS, SILK; PCMA and PCMU): Max transcoding sessions	125; 50; 300	250; 100; 600	500; 200; 1200
Billing and authentication of SIP users from an external RADIUS server	Yes	Yes	Yes
Add-on licenses			
Concurrent Calls SIP Session Licenses (CCS), multiple trunk groups	Yes	Yes	Yes
Remote User SIP Session Licenses (RUS), can be added for the number of users needed.	Yes	Yes	Yes
SIP Registrar User Licenses (SRU), can be added for the number of clients needed.	Yes	Yes	Yes

[1] Transcoding sessions are doubled if unit is equiped with two CPUs.

* The Firewall functions in the SIParator/Firewall product are hidden by default — can be reconfigured to be available.

Ingate Firewall® and Ingate SIParator® are registered trademarks of Ingate Systems.

Technical Specifications Ingate SIParator® / Firewall®

Feature	Ingate SIParator S95	Ingate SIParator S97	Ingate SIParator S98	Ingate Software SIParator
Interfaces 10/100/1000 Mbps Ethernet, (10 Gbps DA/SFP+ optical optional)	6 (2 optional 10 Gbps)	6 (2 optional 10 Gbps)	6 (2 optional 10 Gbps)	**For x86 VM & Cloud Platforms:**
Redundant power supply	Yes	Yes	Yes	
DISK:	1 TB Raid 1	300 GB Raid 1	300 GB Raid 1	Amazon Web Service (AWS) Marketplace
Dimension WxDxH	426x607x43 mm	426x705x43 mm	426x705x43 mm	
Rack Mounting Kit	Sliding included	Sliding included	Sliding included	Microsoft Azure
Certifications	CE, FCC, UL, CB	CE, FCC, UL, CB	CE, FCC, UL, CB	OpenStack
NEBS (Network Equipment-Building System)	No	Compliant	Compliant	Google Cloud Platform
Power consumption (typical)	180 W	200 W	250 W	
Power supply 100 – 240 V AC, (48 V DC optional)	Internal	Internal (DC optional)	Internal (DC optional)	
Management/Configuration options: Web GUI (HTTP, HTTPS), CLI (SSH, serial cable) and HTTP Rest API	Yes	Yes, also iDRAC port	Yes, also iDRAC port	Yes
SNMP, V1, V2, V3	Yes	Yes	Yes	Yes
VLAN Support	Yes	Yes	Yes	Platform Dependent
Internal log to HD	Yes	Yes	Yes	Yes
Logging to PCAP file	Yes	Yes	Yes	Yes
Syslog	Yes	Yes	Yes	Yes
Support for failover multiple ISPs	Yes	Yes	Yes	Yes
Failover to secondary incactive device	Yes	Yes	Yes	Yes
External RADIUS server authentication for IPsec, GUI and SIP	Yes	Yes	Yes	Yes
Free software upgrades, incl. with Support	Yes	Yes	Yes	Yes
Firewall functionality*				
Stateful inspection	Yes	Yes	Yes	Yes
Packet filtering	Yes	Yes	Yes	Yes
Throughput (Mbit/s) (1500 byte packets)	4 500	4 500	4 500	Hardware Dependent
Packets per second (46 byte packets)	500 000	900 000	2 200 000	
DHCP client and PPPoE	Yes	Yes	Yes	Yes
DHCP server	Yes	Yes	Yes	Yes
DHCP proxy	Yes	Yes	Yes	Yes
Proxies for TCP, UDP and FTP	Yes	Yes	Yes	Yes
Flexible NAT and PAT	Yes	Yes	Yes	Yes
VPN functionality				
VPN tunnels	1200	1 600	1 600	Hardware Dependent
3DES (168) (Mbit/s) (1438 byte packets)	100	130	130	
AES (128-bit) (Mbit) (1438 byte packets)	200	270	270	
X.509 certificate, shared secret or XAUTH	Yes	Yes	Yes	Yes
Generating of X.509 certificates for clients	Yes	Yes	Yes	Yes
PPTP server	Yes	Yes	Yes	Yes
IPsec (IKEv1 and IKEv2)	Yes	Yes	Yes	Yes
SIP functionality				
SIP proxy	Yes	Yes	Yes	Yes
SIP registrar	Yes	Yes	Yes	Yes
SIP traffic to private IP addresses (NAT/PAT)	Yes	Yes	Yes	Yes
SIP Connection set up, max calls/s	80	100	100	Hardware Dependent **Compare with:** (S95: 4 Core, 2GHz) (S97: 6 Core, 1.9GHz or 4 Core 3GHz) (S98: 12 Core, 2.3GHz)
RTP media packet delay (+ at transcoding packets)	0.01-0.05 ms (+ voice pkt ms)	0.01-0.05 ms (+ voice pkt ms)	0.01-0.05 ms (+ voice pkt ms)	
Number of concurrent calls (20 ms G.711 voice packets)	4000	8 000	20 000	
Secure VoIP (TLS+SRTP) transcoding sessions	2500	3 000	8 000	
Media Transcoding (G.722, G.729, G.711; OPUS, SILK; PCMA and PCMU): Max transcoding sessions	500; 200; 1200	550[1]; 215[1]; 1500[1]	1500[1]; 600[1]; 7000[1]	
Billing and authentication of SIP users from an external RADIUS server	Yes	Yes	Yes	Yes
Add-on licenses				Yes
Concurrent Calls SIP Session Licenses (CCS), multiple trunk groups	Yes	Yes	Yes	Yes
Remote User SIP Session Licenses (RUS), can be added for the number of users needed.	Yes	Yes	Yes	Yes
SIP Registrar User Licenses (SRU), can be added for the number of clients needed.	Yes	Yes	Yes	Yes

[1] Transcoding sessions are doubled if unit is equiped with two CPUs.

* The Firewall functions in the SIParator/Firewall product are hidden by default — can be reconfigured to be available.

Ingate Firewall® and Ingate SIParator® are registered trademarks of Ingate Systems.

inGate®

Ingate's mission is to enable the best access for telephony, global real-time and unified person-to-person communication for everyone.

Ingate Systems AB · Phone: + 46 8 600 77 50 · Ingate Systems Inc. · Phone: + 1 603 883 6569
info@ingate.com · www.ingate.com

6