secunet
SBC

Farewell ISDN. Hello All-IP.

Secure telephony in VoIP networks.

Protected by the secunet Session Border Controller.

Farewell ISDN. Hello All-IP.

Analogue and ISDN telephony is a thing of the past – telephony today is mostly internet-based. Voice-over-IP telephony (VoIP) offers many advantages, but also presents new risks. secunet SBC provides effective assistance here – the network component enables secure VoIP telephony between internal and external networks in companies and public authorities.

secunet SBC combines a Session Border Controller with a highly secure firewall that encapsulates the SBC and prevents unwanted data transmissions. The Session Border Controller creates an optimised link between different VoIP networks and serves as the central access point for these networks.

The firewall handles essential jobs related to the security of the internal network and also provides fraud detection and prevention functionality to provide additional protection from external attacks.

The solution is used as a supplement to a traditional firewall, contributing Session Initiation Protocol (SIP) expertise – ensuring that data flows are analysed and can be rejected with fine precision. secunet SBC creates complete network transparency, ensures service quality and prevents sensitive network information from leaving the network. The Session Border Controller also implements routing, load balancing and a fail-over solution. secunet SBC also offers encryption where necessary.

The German Federal Office for Information Security (BSI) has confirmed the trustworthiness and high quality of the solution:

- **secunet SBC is CC EAL 4+ certified by the BSI with the certification report BSI-DSZ-CC-1089 (SBC container) and BSI-DSZ-CC-1116-2020 (secunet wall platform).**
- **The secunet SBC also has a RESTRICTED (VS-NfD) release recommendation (for version 6.1.0).**

The fundamental elements of a secure and convenient solution

secunet SBC appliance

Service quality assurance by means of proactive diagnostics, easy error finding and attack analysis

- High security thanks to combination of firewall and Session Border Controller
- Network separation from physical to application layer
- Considerable flexibility in use with consistently rule-based configuration
- Vertical scalability thanks to high performance
- Simple SBC administration with web UI
- Enterprise Management Tool for roll-out, updates and backups
- Bridging for private IPv4 and public IPv6 space

secunet wall

Component of the appliance

Firewall as foundation platform for the SBC

- Additional protection by a firewall surrounding the SBC
- Integrated DMZ structure
- Used as a container platform for any number of applications
- Has its own software management and configuration system
- Complex and finely adjustable configuration options
- CC EAL 4+ certification
- Release recommendation for RESTRICTED (VS-NfD)

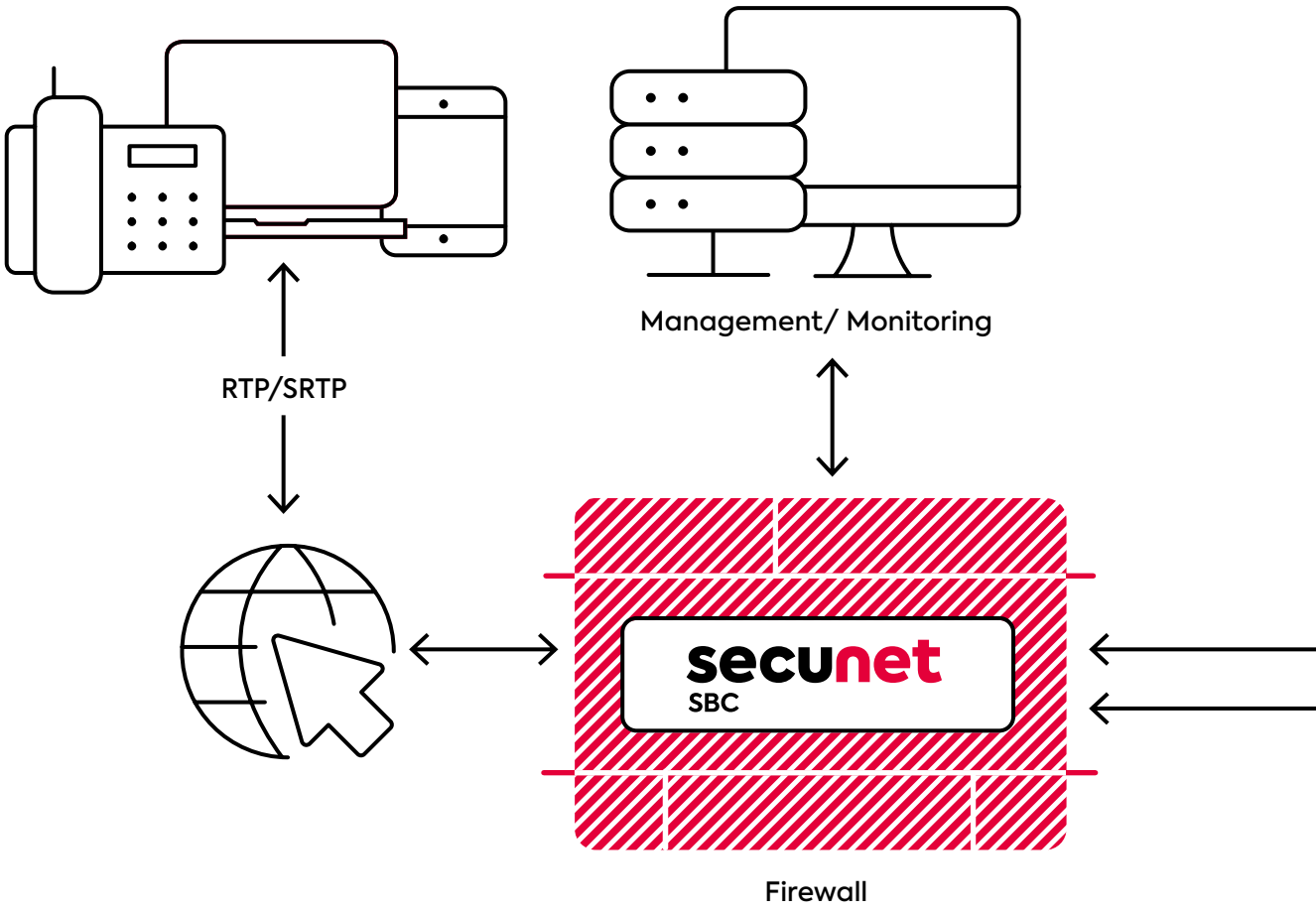
SBC Management

Component of the appliance

Central management system for the SBC

- Remote administration and configuration of the SBC
- Simultaneous management of multiple SBCs via a central interface
- Intuitive user interface
- Centralised storage and import of backups

State-of-the-art telephony using secunet SBC



SBC Monitor

Optional licence

Service quality assurance by means of proactive diagnostics, easy error finding and attack analysis

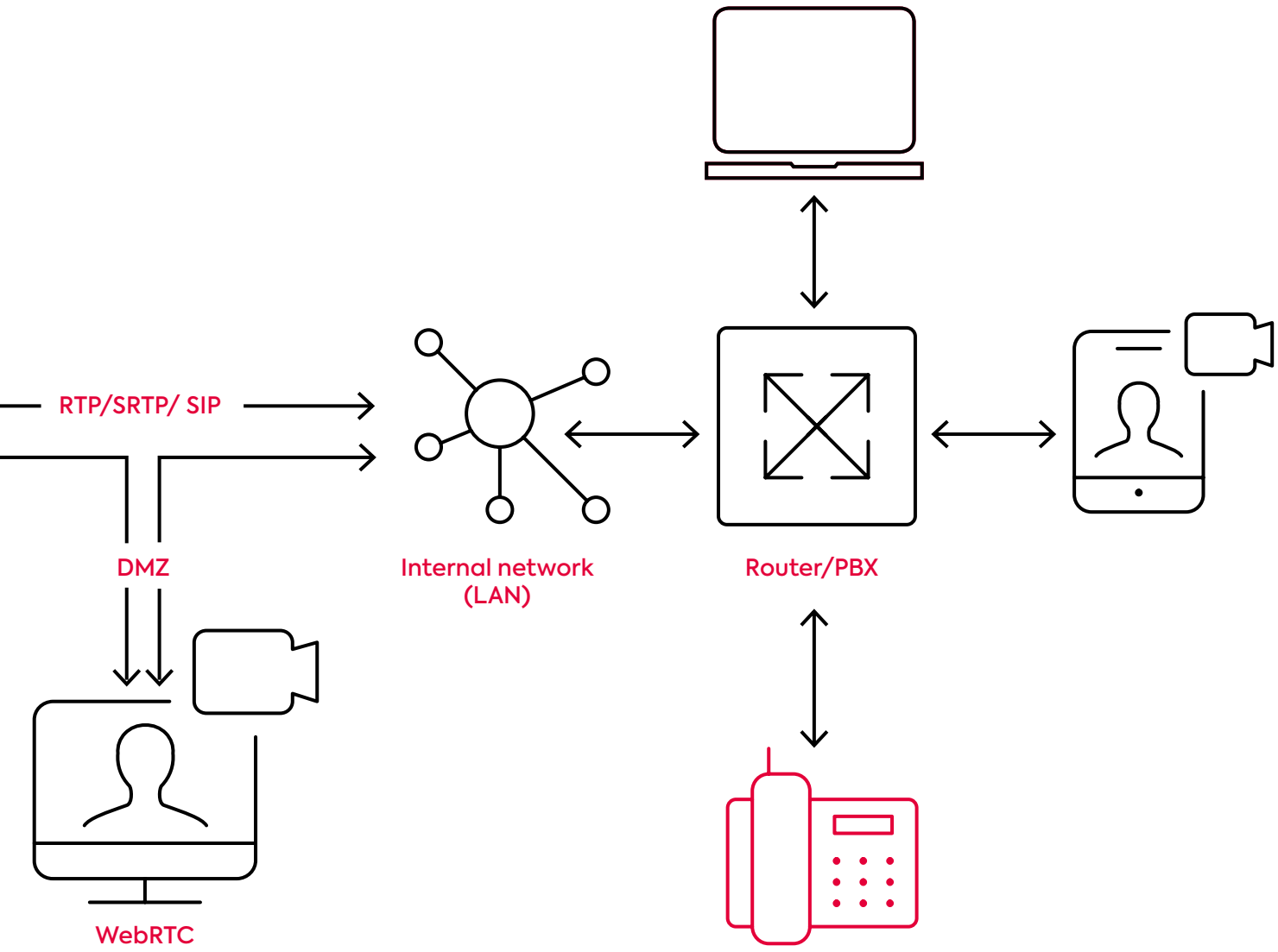
- Search through the entire log of the period in service
- Statistics on usage and error codes
- Trend analysis of calls and registrations
- Analysis of security-related events and overruns of limits
- Monitoring of system resources
- Comprehensive reporting options

Web Real-Time Communication Gateway

Optional licence

Secure integration of clients connecting from the internet into existing SIP infrastructure

- Audio and audio/video calls
- Easy to use in a browser
- For desktop and mobile clients



Separation of the Session Border Controller from other network elements

SBC vs. firewall

A firewall protects the data network from attacks at a network level at ISO/OSI layers 2–4. It primarily filters data based on the sender and receiver (header). The SBC checks not only the header but also the content of the data flows, additionally filtering audio and video protocols transmitted over ISO/OSI layers 5–7 for voice communication in the data network.

SBC vs. ALG

Voice protocols such as SIP or RTP transmit data over randomly selected ports, which is why there must always be a large number of ports opened. This presents many attack vectors. An Application Layer Gateway (ALG) solves this problem by only opening the required ports dynamically. However, ALGs are only able to accept or reject calls. The SBC offers the technology of an ALG as well as offering anomaly detection. The Session Border Controller also recognises much more complex attack patterns.

SBC vs. PBX

A Private Branch Exchange (PBX) handles everything related to call coordination in the network. However, a PBX is unable to provide the required security functionality – the high data throughput prevents this. There is also a greater risk from attacks if data packets are only filtered for malicious code once already in the internal network. This security function is therefore performed by the Session Border Controller at the network transition point.

Comprehensive protection through secunet SBC

Physical network isolation
The SBC physically isolates networks by means of separate physical network interfaces and allows controlled transitions between networks.

Allows only negotiated RTP connections
Normal packet filters always have a large number of ports left open to allow RTP data streams to pass. The SBC only allows negotiated RTP connections to access the end devices, thus reducing the number of potential attack vectors.

Conceals internal network structure
The SBC conceals the internal network structure from external eyes. Information such as IP addresses and the component types in use are substituted by the Session Border Controller.

Restrictions on protocol extensions
SIP is a protocol with many, sometimes unnecessary extensions. The SBC limits these extensions and in doing so limits the number of potential attack vectors in internal elements.

Restrictions on codecs and media types
Devices party to an SIP call may negotiate any media type or codec. The SBC can limit these to “only audio”, “only audio and video” or certain codecs, for example.

Limits
The SBC can limit data rates to prevent Denial of Service attacks (DoS). These restrictions apply for the number of concurrent calls, the total bandwidth or the bandwidth per call. These can be configured per data line and direction, per source IP address, per user or using other parameters.

System analysis
A system analysis of events (network behaviour, communication relationships, attacks, etc.) may be performed on an optionally available monitoring system.

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed in the SDAX and generated revenues of around 337 million euros in 2021.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

secunet SBC_EN_10/2022