secunet SBC –
Wir hören uns in der Zukunft

secunet

Sicher Telefonieren in VoIP-Netzen geschützt durch den secunet Session Border Controller

Analoge und ISDN Telefonie gehören der Vergangenheit an – das Telefonieren erfolgt heutzutage hauptsächlich internetbasiert. Die Voice-over-IP-Telefonie (VoIP-Telefonie) bietet viele Vorteile, birgt aber ebenso neue Gefahren. Wirksame Abhilfe schafft der secunet SBC: Die Netzwerkkomponente ermöglicht sichere VoIP-Telefonie zwischen internen und externen Netzen in Unternehmen und Behörden.

secunet SBC kombiniert einen Session Border Controller mit einer hochsicheren Firewall, die diesen umhüllt und unerwünschte Datenübertragungen verhindert. Der Session Border Controller setzt eine optimale Verknüpfung von verschiedenen VoIP-Netzen um und ist zentraler Zugangspunkt für diese Netze. Die Firewall-Funktionalität übernimmt wesentliche Aufgaben zum Schutz des internen Netzes und bietet zudem Fraud Detection und Prevention, um zusätzlich vor Angriffen von außen zu schützen.

Die Lösung ergänzt die klassische Firewall mit Session Initiation Protocol (SIP) Know-how: Datenströme werden somit analysiert und können feingranular abgewiesen werden. secunet SBC schafft vollständige Netztransparenz, sichert die Servicequalität und verhindert, dass sensitive Netzinformationen abfließen. Zudem wird durch den Session Border Controller Routing, Load-Balancing und Fail-Over implementiert. Darüber hinaus bietet secunet SBC die Möglichkeit bei Bedarf zu verschlüsseln.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt die Vertrauenswürdigkeit und hohe Qualität der Lösung: Der secunet SBC befindet sich im CC EAL 4+ Zertifizierungsprozess durch das BSI mit der Zertifizierungskennung BSI-DSZ-CC-1089.

Rundumschutz
mit dem secunet SBC

Physische Netztrennung – Der SBC realisiert mittels separater physischer Netzwerkschnittstellen die physische Netztrennung und den kontrollierten Übergang zwischen den Netzen.

Nur ausgehandelte RTP-Verbindungen zulassen – Gewöhnliche Paketfilter haben stets eine hohe Anzahl von Ports geöffnet um RTP-Ströme passieren zu lassen. Der SBC lässt nur ausgehandelte RTP-Verbindungen zu den Endgeräten zu und verringert somit die Angriffsfläche.

Verschleierung der internen Netzstruktur – Der SBC verschleiert nach außen hin die interne Netzstruktur. Informationen wie IP-Adressen und verwendete Komponententypen werden durch den Session Border Controller ersetzt.

Einschränkung des Protokollumfangs – SIP ist ein Protokoll mit vielen, teilweise beliebigen Erweiterungen. Der SBC schränkt diesen Umfang ein und verringert damit die Angriffsoberfläche in den internen Elementen.

Einschränkung der Codecs und Mediatypen – Die in einem SIP-Call beteiligten Geräten können beliebige Mediatypen und Codecs aushandeln. Der SBC kann diese bspw. auf „Nur Audio", „Nur Audio und Video" oder bestimmte Codecs einschränken.

Limitierungen – Der SBC kann eine Limitierung der Datenleitung vornehmen, um eine Denial of Service (DoS)-Attacke zu verhindern. Die Einschränkungen gelten für die Anzahl paralleler Anrufe, die gesamte Bandbreite oder die Bandbreite per Anruf. Dies ist jeweils per Datenleitung und Richtung, Quell-IP-Adresse, Benutzer oder für andere Parameter möglich.

Systemanalyse – Eine Systemanalyse der Ereignisse (Netzverhalten, Kommunikationsbeziehungen, Angriffe, etc.) kann an einem optional erhältlichen Monitoring-System erfolgen.

Abgrenzung des Session Border Controllers zu anderen Netzelementen

SBC vs. Firewall

Eine Firewall schützt das Datennetz vor Angriffen auf Netzwerkebene auf den ISO/OSI Schichten 2–4. Sie filtert die Daten primär nach Absender und Empfänger (Header). Der SBC überprüft nicht nur den Header, sondern auch den Inhalt der Datenströme: Er filtert zusätzlich im Datennetz auf Sprachebene die Audio- und Video-Protokolle, die auf den ISO/OSI Schichten 5–7 übermittelt werden.

SBC vs. ALG

Bei Sprachprotokollen wie SIP oder RTP findet die Übertragung auf zufällig gewählten Ports statt, weshalb immer eine große Anzahl an Ports geöffnet sein muss. Dies bietet eine große Angriffsfläche. Ein Application Layer Gateway (ALG) löst dieses Problem, indem es nur die benötigten Ports dynamisch öffnet. Jedoch kann ein ALG nur Anrufe annehmen oder abweisen. Der SBC bietet die Technologie eines ALG und arbeitet darüber hinaus mit Anomalie-Erkennung. Dadurch erkennt der Session Border Controller auch wesentlich komplexere Angriffsmuster.

SBC vs. PBX

Ein Private Branch Exchange (PBX) leistet die gesamte Koordinationsarbeit der Anrufe im Netz. Die benötigten Schutzfunktionalitäten kann ein PBX jedoch nicht abbilden: Dies wird zum einen durch den hohen Durchsatz verhindert. Zum anderen vergrößert sich die Gefahr im Angriffsfall, wenn Datenpakete erst innerhalb des internen Netzes nach Schadcodes gefiltert werden. Diese Schutzfunktion übernimmt deshalb der Session Border Controller am Netzübergang.

Die Bausteine für eine sichere und komfortable Lösung

secunet SBC Appliance

Zuverlässige Absicherung durch komplette Netztrennung und kontrollierte, regelbasierte Anbindung

- Hohe Sicherheit durch Kombination von Firewall und Session Border Controller
- Netztrennung von physikalischer bis Applikationsebene
- Große Flexibilität im Einsatz mit durchgehend regelbasierter Konfiguration
- Vertikale Skalierbarkeit durch große Leistungsfähigkeit
- Einfache SBC Administration mit Web-Schnittstelle
- Enterprise Management Tool für Rollout Update und Backup
- Bridging für privaten IPv4 und öffentlichen IPv6 Raum

---

secunet wall

Bestandteil der Appliance

Firewall als Trägerplattform für den SBC

- Zusätzlicher Schutz durch eine Firewall die den SBC umgibt
- Integrierte DMZ Struktur
- Dient als Containerplattform für beliebig viele Applikationen
- Verfügt über ein eigenes Software Management- und Konfigurationssystem
- Komplexe und feingranulare Konfigurationsmöglichkeit
- Befindet sich im CC EAL 4+ Zertifizierungsprozess

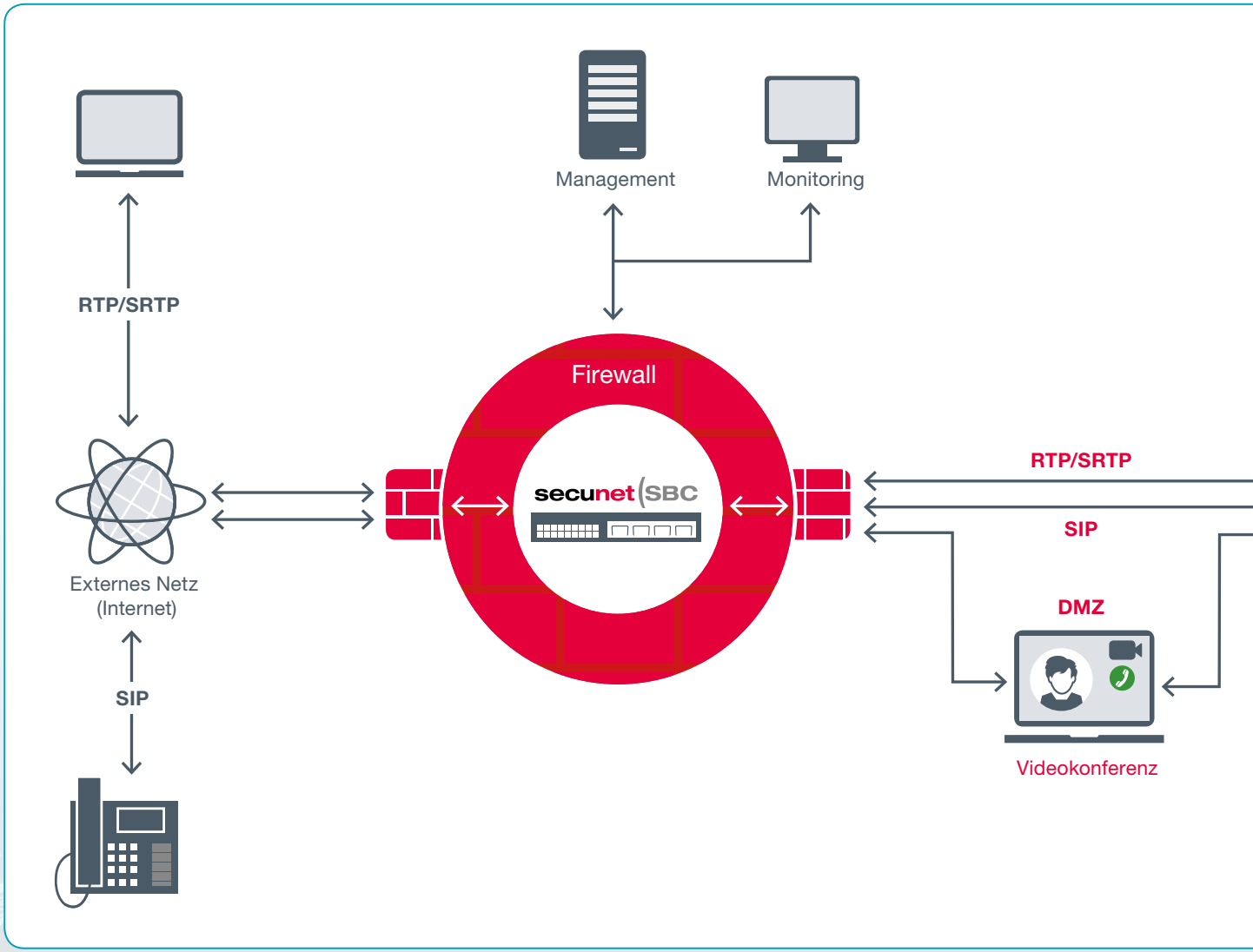
SBC Management

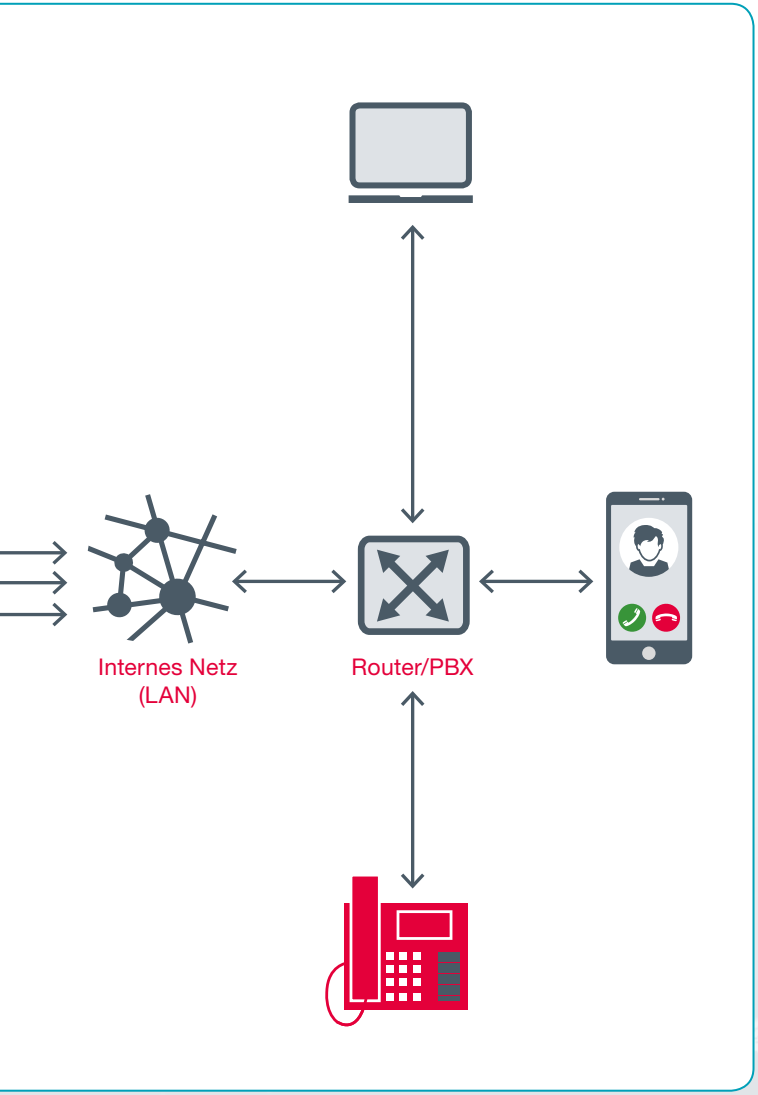
Bestandteil der Appliance

Zentrales Managementsystem für den SBC

- Remote Administration und Konfiguration des SBC
- Gleichzeitiges Management von mehreren SBCs über eine zentrale Schnittstelle
- Intuitive Benutzeroberfläche die eine einfache Benutzerführung ermöglicht
- Zentrale Vorhaltung und Einspielung von Backups

State-of-the-Art-Telefonie
mit dem Einsatz von secunet SBC





SBC Monitor

optionale Lizenz

Servicequalitätssicherung durch proaktive Diagnostik, einfache Fehlersuche und Angriffsanalyse

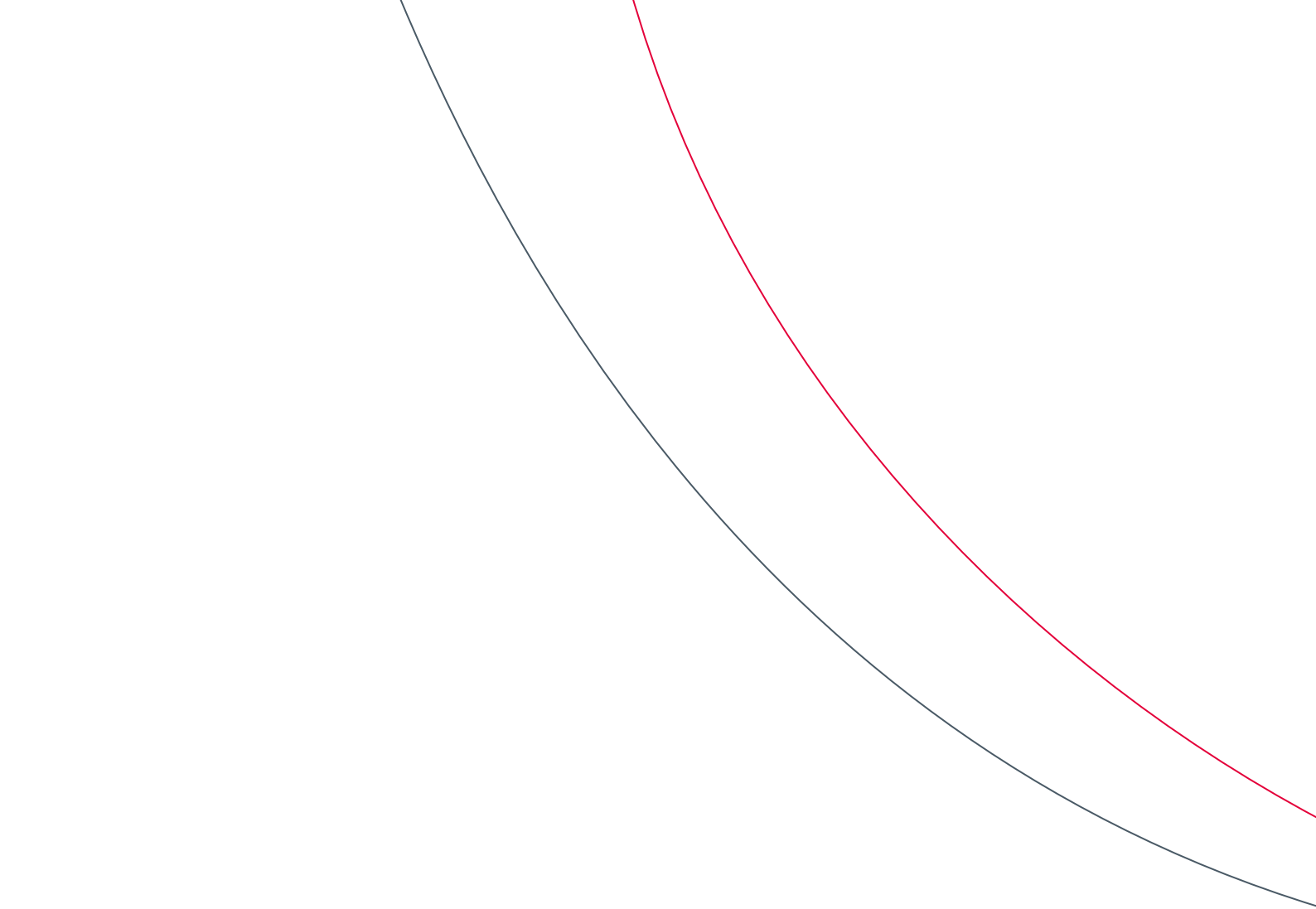
- Suche über die komplette Historie der Vorhaltezeit
- Statistiken zu Nutzung und Fehlercodes
- Trendanalyse Anrufe und Registrierungen
- Analyse zu sicherheitsrelevanten Ereignissen und Überschreitung von Limitierungen
- Überwachung der Systemressourcen
- Umfassende Reporting Möglichkeiten

Web Real-Time-Communication Gateway

optionale Lizenz

Sichere Einbindung von Teilnehmern aus dem Internet in bestehende SIP-Infrastruktur

- Audio und Audio/Video-Anrufe
- Einfache Benutzung im Browser
- Für Desktop und mobile Clients



secunet

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

www.secunet.com