FRAFOS
Member of the Frequentis Group

Zero Trust VoIP-Monitoring

Zero-Trust VoIP-Sicherheit und Anomalie-Erkennung

Wesentliche Merkmale

- Zero-Trust-Sicherheit
- Aufdeckung von Betrug
- DoS-Erkennung
- Statistik der Anrufe
- Tägliche Berichte
- Überwachung der Verfügbarkeit
- Schwarze Liste
- Analyse des Call Flows
- Anruf-Log Verlauf

Eine detaillierte Überwachung eines VoIP-Systems ist eine wesentliche Voraussetzung für einen sicheren und geschützten VoIP-Dienst. Eine VoIP-Überwachungslösung bietet Einblicke in das Nutzungsverhalten und ermöglicht es dem Systemadministrator nicht nur, den Zustand des Dienstes zu überprüfen, Hotspots und Überlastung zu identifizieren, sondern auch verdächtiges Verhalten und bösartigen Datenverkehr zu erkennen.

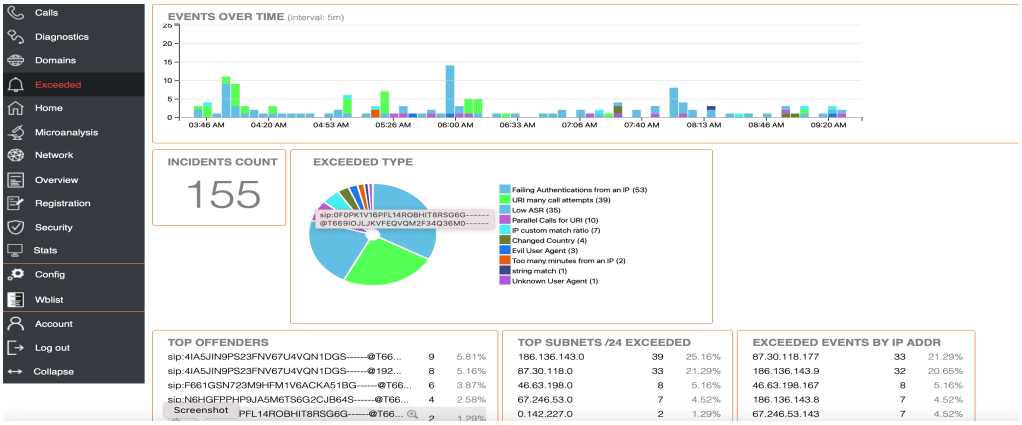
Der ABC Monitor hat sich als vielseitiges Überwachungstool bewährt, das VoIP-Systemadministratoren bei der Überwachung ihres VoIP-Dienstes, der Analyse von Anrufabbrüchen und der Erkennung von Denial-of-Service-Angriffen und Betrugsversuchen unterstützt. Der ABC Monitor hat sich zwar als unverzichtbar für Systemadministratoren erwiesen, aber die Menge der von diesem Tool gesammelten und angezeigten Informationen kann Fragen zum Datenschutz aufwerfen. Um den VoIP-Verkehr analysieren zu können, sammelt der ABC Monitor den gesamten Verkehr, der von dem verwalteten VoIP-Dienst verarbeitet wird, und nicht nur verdächtigen Verkehr. Der Administrator des ABC Monitors kann also nicht nur verdächtiges Verhalten analysieren, sondern auch das Verhalten eines jeden Nutzers des VoIP-Dienstes! Während dies oft ein akzeptabler Nebeneffekt ist, da man davon ausgehen kann, dass der Administrator des Dienstes vertrauenswürdig ist, betrachten gesetzliche und arbeitsrechtliche Bestimmungen eine solche Möglichkeit oft als Eingriff in die Privatsphäre der Mitarbeiter und verbieten diese Art der Datensammlung und -analyse.

Der FRAFOS ZT-Monitor ist eine Erweiterung des ABC-Monitors, die es dem VoIP-Administrator ermöglicht, sich einen Überblick über den Zustand des VoIP-Dienstes zu verschaffen, bösartiges Verhalten zu erkennen und Probleme bei Anrufausfällen zu analysieren. Die Zero-Trust-Erweiterung bietet jedoch einen entscheidenden Unterschied: Die Privatsphäre der Nutzer des VoIP-Dienstes bleibt gewahrt!

Die vom ZT FRAFOS Monitor erfassten Daten werden während des Erfassungsprozesses verschlüsselt. Alle Analyse- und Verarbeitungsschritte, die der Monitor durchführt, erfolgen auf der Grundlage verschlüsselter Daten. Die Ergebnisse der Analyse und Verarbeitung werden in anonymisierter Form angezeigt, so dass der Administrator zwar System- und Sicherheitsprobleme erkennen kann, aber keine benutzerbezogenen Daten angezeigt werden.

Wenn dies aufgrund von Gesetzen, Arbeitsvorschriften oder technischen Notwendigkeiten erforderlich ist, kann der Administrator von FRAFOS ZT Monitor dennoch auf die verschlüsselten Daten zugreifen, indem er ein Entschlüsselungsgeheimnis anwendet. Die Anwendung des Entschlüsselungsgeheimnisses ermöglicht es dem Systemadministrator, die gesammelten Daten im Klartext anzuzeigen und Zugriff auf den tatsächlichen Datenverkehr anstelle des verschlüsselten Datenverkehrs zu erhalten.

Zusammenfassend lässt sich sagen, dass der FRAFOS ZT Monitor die Anforderungen an die Überwachung und Analyse von VoIP-Daten mit dem Schutz der Privatsphäre der Nutzer verbindet. Diese Lösung wird



als Upgrade für den ABC Monitor angeboten.

Die angebotene Lösung wird unsere Kunden mit:

- Zero-Trust-Analyse: Die vom FRAFOS ZT Monitor gesammelten Daten werden anonymisiert, bevor sie in den Datenbanken des Monitors gespeichert werden. Alle Analyse- und Überwachungsfunktionen werden mit anonymisierten Daten durchgeführt, so dass die Privatsphäre der Kundendaten gewahrt bleibt.
- Tägliche Übersicht: Ein täglicher Überblick über durchgeführte Anrufe, Serviceunterbrechungen und Servicequalität.
- Überwachung der Verfügbarkeit: Erkennen und berichten Sie über die Verfügbarkeit der VoIP-Lösungen des Kunden sowie der SIP-Trunks.
- Detaillierte Sicherheitsüberprüfungen: Die Lösung bietet umfassende Überwachungs- und Sicherheitstools, die auf intelligenten Erkennungsalgorithmen und Big Data-Analysen basieren.
- Erweiterte Richtlinien zur Betrugserkennung: Einerseits bietet die Lösung intelligente Richtlinien, die auf Ereignisse wie Dienstunterbrechungen oder bekannte Betrugsmuster hinweisen, z. B. nächtliche Anrufe an verdächtige Nummern. Darüber hinaus können Kunden zusätzliche Alarme einstellen, die auf bösartiges Verhalten wie nicht autorisierte Anrufe oder überhöhte Ausgaben hinweisen.
- Auto-Service-Schutz: Schließen Sie den Kreislauf, indem Sie verdächtige Quellen auf eine schwarze Liste setzen und betrügerische Anrufe unterbinden.
- Einfache Integration: Der ZT-Monitor wird als Erweiterung für den ABC-Monitor bereitgestellt. Nach der Aufrüstung werden alle neu erfassten Daten verschlüsselt.

Zero-Trust-Analyse

Der FRAFOS ZT Monitor integriert die folgenden Technologien:

- Big Data-Verarbeitung: Die von unseren Kunden gesammelten Überwachungs- und Protokollierungsdaten müssen über Tage, wenn nicht sogar Monate hinweg aufbewahrt werden. Dies ist erforderlich, um einen historischen Überblick über die Aktivitäten der Kunden sowie über die gesetzlichen Vorschriften zu erhalten. Dies wird mit Big-Data-Lösungen wie Elastic Search und Logstash erreicht.
- VoIP-Analyse: Das Session Initiation Protocol (SIP) ist mit seinen vielen Optionen und unterschiedlichen Anrufabläufen immer komplexer geworden. Mit jahrelanger Erfahrung hat das FRAFOS-Team SIP-Analyse- und Verarbeitungsmechanismen entwickelt, die eine detaillierte Untersuchung von SIP-Problemen sowie die Erkennung von Interoperabilitäts- und Signalisierungsproblemen ermöglichen.

- Anonymisierung: Um den Datenschutz der Kundendaten zu gewährleisten, wird eine Anonymisierungsschicht zwischen dem Kunden und dem Überwachungsdienst eingesetzt. Diese Schicht verschlüsselt private und kundenbezogene Daten, die in Protokollen, Ereignissen oder Kundenverkehr enthalten sind, mit Unternehmensschlüsseln. Welche Teile der Unternehmensdaten anonymisiert werden sollen und wer auf die Daten im Klartext zugreifen darf, kann ebenfalls vom Kunden selbst bestimmt werden.
- Datenerfassung: Protokollierungs- und Überwachungsdaten werden entweder von den VoIP-Komponenten des Kunden oder von einer speziellen VoIP-Sonde von FRAFOS (SIPBeat) erfasst. Beide Optionen ermöglichen die Erfassung von SIP-Signalisierungsdaten und das Senden dieser Daten an den ZT Monitor. Die SIPBeat-Sonde ermöglicht es jedem Kunden, den FRAFOS ZT Monitor zu nutzen, unabhängig davon, ob der Kunde auch den FRAFOS SBC verwendet.