NIAGARA NETWORKS

Application Note

Unified Communications Visibility and Threat Protection

Visibility in Unified Communications

Since the early days of the internet where it was primarily used by scientists to exchange information and share data, the internet has grown immensely and has become a commerce tool and a universal communication channel for billions of people.
This universal communication channel is often referred to as Unified Communications (UC) and is defined as an evolving set of technologies that automates and unifies human voice and device data communications in a common context and experience. UC optimizes business processes and enhances human communications by reducing latency, managing flows, and eliminating device and media dependencies'

With the transition from a scientific network to a global public communication infrastructure that serves the entire universe of data and voice communications, the requirement for privacy and security became imperative as the dependency on internet communication channels continues to expand.

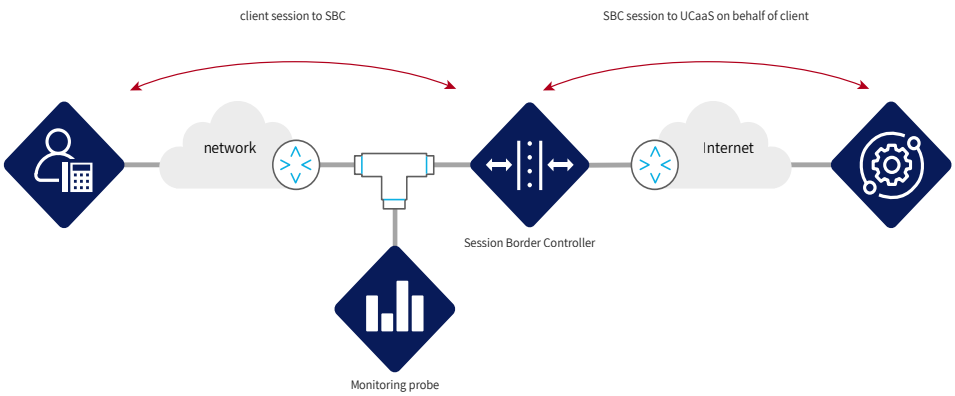
Today most IP data and voice traffic is routinely encrypted by default. However, encryption can mask hidden threats. Therefore, all traffic including IP voice must be decrypted and inspected in order to protect the network, reduce risk, and generate needed business and compliance metrics.

Challenges

As a result of the increasing need for security and privacy, Unified Communication networks are increasingly utilizing encryption to secure signaling (SIP/SIPS) and data channels (RTP/SRTP).
The new generation of Unified Communications as a Service (UCaaS) web conferencing systems like MS Teams, Google Meet and Zoom provide by default the TLS encrypted services to sustain privacy, integrity, and security of the associated voice and video communication channels. This new avalanche of digital transformation increases the dependency on high quality and high availability for communication services.

Service Assurance and Quality of Experience are important factors in the design strategy, implementation and maintenance of UC and voice networks. Traditionally, tools like Oracle's Communications Operations Monitor (OCOM) or Enterprise Operations Monitor (EOM) are deployed to monitor the network and provide analysis and service assurance. Encryption blinds these tools to the traffic they should be monitoring and reporting on. Targeted decryption is the method to regain visibility into this traffic.

The diagram below shows a typical UCaaS deployment:



End user clients, either remote or connecting through an enterprise network connect to a Session Border Controller (SBC) which hides the network topology and protects the service provider or enterprise packet network.

A TAP provides a copy of the session's traffic which is fed to the monitoring probe for analysis and reporting. To analyze a TLS encrypted session, the traffic must be decrypted first. When the quality of service (QoS) is as important as it is in voice communications, all components must meet minimum QoS standards, regardless of whether they are in or outside the session's communication path.
With the adoption of forward secrecy (ephemeral key exchange) in TLS 1.2 and TLS 1.3, decrypting only a mirrored copy of traffic for analytics is no longer feasible; the decryption engine must sit inline in the service communication path.

Solution

Niagara Networks' Advanced Packet Brokers, enhanced by the award-winning Open Visibility Platform (OVP) and the pluggable Packetron acceleration module, provide a programmable, high-performance visibility layer that ensures the right data reaches the right tool at the right time. They can be configured for active TAP as well as fully integrated packet broker functions. With Packetron, the system enables comprehensive packet parsing and manipulation for IPv4 and IPv6 across OSI Layers 2–7, along with TLS decryption and advanced network intelligence. The packet broker can filter and steer encrypted SIP signaling to the onboard Packetron decryption engine, while other traffic passes untouched; decrypted signaling can then be inspected for fraud and security threats.

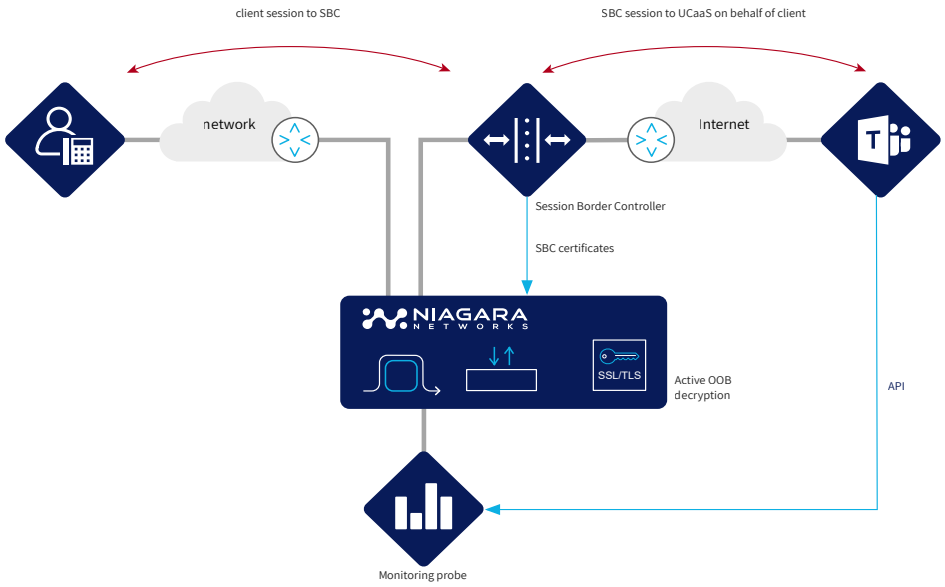
To protect your network, Niagara has integrated world-class IP voice protection from RedShift Networks. This partnership leverages Niagara's Open Visibility Platform (OVP) and Packetron technology to deploy either RedShift's IP voice Threat Protection Service (TPS) or RedShift's full Communication Threat Management (CTM) service directly on Niagara solutions.

TPS leverages RedShift's global Voice Network Threat Intelligence (VNTI) database to root out high-risk calls passing in and out of the network. Implementation and management of TPS on Niagara solutions requires minimal effort, yet delivers superior protection against a host of threats including robocalls, scams and network attacks.

For customers that wish to have enhanced fraud and security protection with underlying analytics and reporting, RedShift's CTM service can be just as easily deployed on Niagara's Packetron technology. The CTM service adds stateful Layer 7 inspection and AI & ML driven behavioral analysis of signaling traffic to deliver the world's most comprehensive IP voice protection available today. The CTM is a single pane of glass fraud and security solution with enterprise functionality including policy control, SAML, RBAC and SIEM support that is easily deployed on Niagara's Packetron, packet acceleration solution.

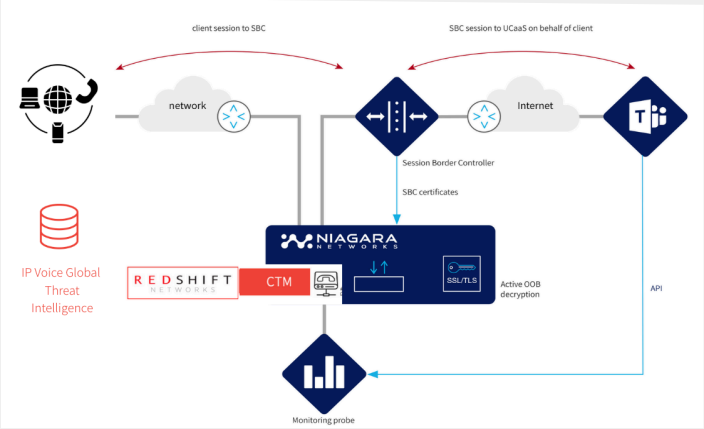
A typical example of an IP voice web conferencing deployment is shown below. The setup illustrates an MS Teams deployment with network traffic forwarded to a Niagara Packet Broker. An embedded or external bypass (depending on the selected option) protects against service outages. The Packet Broker's decryption engine, impersonating the SBC and using its certificate(s), establishes a secure connection with the end-user client and decrypts the session.

A copy of the decrypted traffic can then be sent to a monitoring probe where it is analyzed using MS Teams API functionality.
The session traffic is then re-encrypted, and a connection is established with the Session Border Controller which in turn will handle the call with the MS Teams service.
In the below example, a hybrid packet broker is used to provide the bypass, packet broker, and decryption functionality in a single solution. In certain deployment scenarios, it may be advantageous to separate these functionalities. With the introduction of the Niagara 4248-6C and 4540 fixed packet brokers with advanced processing functionality, a similar setup with the same protection can be achieved in combination with a separate network bypass.



Summary

Unified Communications (UC), encompassing voice, video, and unified messaging, has become a standard method of enterprise communication and a cornerstone of modern business. In daily life as well, UC is increasingly replacing traditional telephone infrastructure. With the internet serving as the underlying transport, encrypting UC services is imperative to ensure privacy and protection. However, encryption also creates challenges: it hampers the ability to safeguard these services against fraud and security threats, while making it more difficult to maintain the required quality of service.



Niagara's Advanced Packet Brokers - enhanced with the award-winning Open Visibility Platform (OVP) and the pluggable Packetron acceleration module—solve this challenge by extending packet broker functionality with third-party virtual hosting and advanced packet processing. This enables robust TLS decryption, deep packet inspection, and full network intelligence (L2–L7), allowing organizations to maintain high-quality UC services while protecting against threats and ensuring compliance.

Through this highly integrated, world-class partnership, Niagara's OVP and Packetron technology support deployment of RedShift's IP Voice Threat Protection Service (TPS) or the comprehensive Communication Threat Management (CTM) service directly on Niagara solutions..

- Full visibility into Unified Communications IP voice flows
- Comprehensive IP voice fraud and security protection, powered by integrated RedShift CTM & TPS
- Flexible options using OVP and Packetron technology
- Scalable solutions for small and large deployments
- Supports all major voice, video and messaging solutions

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership. A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including network TAPs, bypass elements, packet brokers and a unified management layer.
For more information please visit us at www.niagaranetworks.com

About RedShift Networks

RedShift Networks delivers worldclass, real-time security and fraud protection with underlying analytics for IP voice networks. RedShift's partner friendly Threat Protection Service (TPS) and single pane of glass Communication Threat Management (CTM) platform technology provide end-to-end visibility and automated mitigation against known and emerging IP voice threats, including Robocalls, Toll Fraud, TDoS and AI driven threats. Fueled by a continuously updated global IP voice threat intelligence database and patented behavioral analysis, the highly scalable TPS, CTM and mobile device Call Assurance technology provides superior protection for Enterprise, Service Provider and Carrier managed voice networks worldwide. For more information, please visit us at www.redshiftnetworks.com.

NIAGARA NETWORKS
48430 Lakeview Blvd,
Fremont, CA 94538, USA
www.niagaranetworks.com
info@niagaranetworks.com
Tel: +1 408 622 0354
Fax: +1 408 213 7529