NIAGARA NETWORKS

Application Note

Decryption Solution for Unified Communications

Visibility in Unified Communication

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 Communication (UC) and is defined as 'an evolving set of technologies that automates and unifies human and device communications in a common context and experience. It 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 communications, the requirement for privacy and security were imperative as dependency on the internet communication channels became widely used.

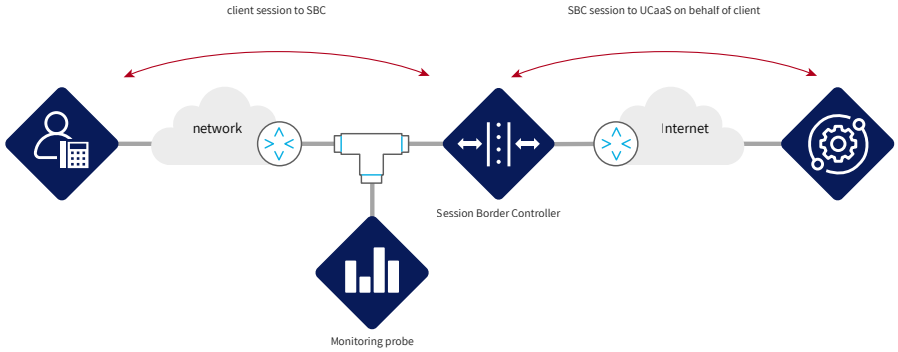
Nowadays most internet traffic is routinely encrypted, but not only the internet traffic is encrypted by default. Communications in enterprise networks are often encrypted by default to secure data against potential compromises and to comply with regulations.

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/RSTP/).
The new generation of Unified Communication as a Service (UCaaS) systems like Skype, MS Teams, 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 is an important factor in IT strategy in design, 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 monitor and report on. Targeted decryption is the method to regain visibility into this traffic.

The diagram below shows a typical UCaaS deployment:



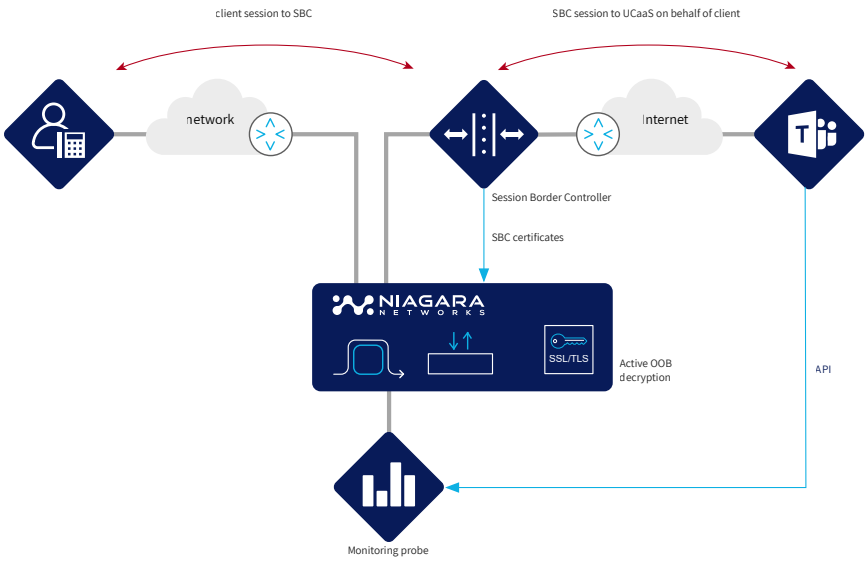
UC clients, either remote or connecting through an enterprise network connect to a Session Border Controller (SBC) which hides the network topology and protects the service provider or enterprise packet network.

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 is as important as it is in voice and UC networks all components must meet these standards, regardless whether they are in or outside the session's communication path. With the introduction of the ephemeral keys in TLS1.2 and TLS1.3 it became impossible to decrypt a copy of the traffic for analytic and quality assurance purposes, the decryption engine must be an integral part of the service's communication path.

Solution

Niagara Networks N2 series, a modular hybrid packet broker combines Niagara's unprecedented dual bypass protection with a robust inline decryption engine. The hybrid packet broker can receive traffic from multiple network segments, each segment having its own bypass functionality, and filter the secure SIP signaling traffic, forwarding it to the decryption engine, while other traffic passes the hybrid packet broker untouched.



A copy of the decrypted traffic can be forwarded to one or multiple probes or other tools for inspection and analysis purposes.
A typical example of a UC decryption deployment is shown above. The setup shows an MS Teams deployment with an inline decryption solution. Network traffic is forwarded to an N2 hybrid packet broker. An embedded bypass module protects against service outages. The decryption engine, impersonating the SBC and using the SBC's certificate(s) establishes a secure connection with the client, decrypt the session and send a copy of the traffic to a monitoring probe where it is analyzed using MS Teams API functionality.

The session is 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 above example,a hybrid packet broker is used to provide the bypass, packet broker, and decryption functionality. In certain deployment scenarios, it is more convenient to separate these functionalities. With the introduction of the Niagara 4248-6C and 4540 fixed packet brokers with advanced processing functionality in combination with a separate network bypass, a similar setup with the same protection can be achieved.

Summary

Unified Communication with its voice, video, and unified messaging has become a standard means of enterprise communication. In our day-to-day life, UC also gained an important role in replacing the traditional telephone infrastructure.

With the internet serving as the underlying transport, encryption of the UC services is imperative.
Encryption seriously hampers the visibility of these services and makes it difficult to maintain the required quality of service.

Niagara Network's Award-winning Open Visibility platform with its advanced and robust decryption capabilities enables the decryption of the communication channels required for maintaining high-quality services.

- Full visibility in unified connection flows
- Scalable solution for small and large deployments
- Supports voice, video and messaging
- Uninterrupted traffic flows using integrated or separate bypass switching
- Supports all major voice and video quality monitoring tools

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

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