Oracle’s Tunneled Session Management Solution for Over-the-Top Services

Tap Into the Growing Demand for Secure, First-Class Services
Offering “over-the-top” (OTT) services to the growing base of mobile data subscribers requires a network that can meet their ubiquitous internet access demands.

Driven by the growing base of mobile data subscribers, ubiquitous internet access, and high bandwidth that is now available in both fixed and mobile networks, services accessed via the internet, also known as OTT services, have become hugely popular. But while Microsoft Skype and other OTT services threaten traditional telephony offerings, innovative service providers looking to differentiate and expand are introducing their own OTT services. Despite this tremendous opportunity, service providers must overcome a number of unique challenges as they deploy and market these new services.

Oracle’s solution for addressing OTT challenges for native applications is known as the Tunneled Session Management solution. This solution includes support for Evolved Packet Data Gateway (ePDG) Firewall Traversal Function (EFTF), an emerging standard under development within the Third Generation Partnership Project (3GPP). The solution employs a client/server architecture powered by the Oracle Communications Session Border Controller and client applications provided by partners or developed via a freely available software developer’s kit (SDK). The solution enables any service provider to offer secure, first-class services on or off its network.

Oracle’s Tunneled Session Management solution leverages real-time communications (RTC)–enabled client applications supported on popular smartphone, tablets, and desktop operating systems (OSs). Using standard communications and security protocols, client applications initiate secure communications sessions with the service provider over the internet. Session border controllers (SBCs) at the edge of the network use Tunneled Service Controller (TSC) software to terminate and control these tunnels before passing the secure traffic into the service core. This solution improves upon traditional OTT services in several ways.

- **Robust firewall traversal.** Ensures successful Voice over IP (VoIP) connectivity through strict firewalls that reject traditional VoIP traffic.
- **Simplification of Session Initiation Protocol (SIP)–based OTT services.** Tunneled sessions are secure yet easier to troubleshoot and manage than sessions based on
native SIP or Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP).

- **Strong privacy, confidentiality, and integrity.** The solution leverages 256-bit encrypted TLS or Datagram Transport Layer Security (DTLS) tunnels.

- **High-quality audio, even over “lossy” networks (such as the internet).** Where other state-of-the-art OTT services fail outright, TSC delivers consistently high quality even under the most dire network conditions, without requiring the use of proprietary codecs.

### Challenges in Over-the-Top Services

Existing OTT services have proven that the public internet can be a viable transport for secure, high-quality communications. However, the uncontrolled nature of internet traversal and the multimodal nature of OTT communications create unique challenges for service providers wishing to launch new services or broaden the reach of their existing offerings. These challenges include the following:

- **Strict firewalls deployed by many enterprises are configured to block or suppress internet access to hosted unified communications (UC) or other interactive communications services.**

- **Privacy and confidentiality, basic requirements for internet-based communications, require encryption, which adds cost and complexity to endpoints as well as service elements.**

- **Lossy network conditions impede high voice quality, especially when using standard voice codecs.**

- **Lack of standards for OTT communications has prevented easy integration with existing VoIP services, UC systems, and IP Multimedia Subsystem (IMS) networks.**
REAL-TIME COMMUNICATIONS AND STRICT FIREWALL TRAVERSAL

For data and web applications, firewalls are a necessity for blocking unwanted or malicious traffic from untrusted networks. However, firewalls present a number of issues for real-time communications. For instance, in enterprise networks, firewalls are often used to suppress SRTP port ranges. Firewalls can also present unwanted barriers to OTT communications when deployed in public Wi-Fi hotspots and satellite/home offices. Finally, some service providers block traffic originating from competitor networks or forcibly disable TCP connections that exceed certain time limits. These very common scenarios make sustaining OTT communications extremely difficult. By creating secure tunnels for audio, video, and data that look like permissible web traffic, Oracle’s TSM solution delivers secure connectivity even through strict firewalls.

The table illustrates how Oracle’s Tunneled Session Management solution addresses these challenges.

<table>
<thead>
<tr>
<th>OTT Challenges</th>
<th>Oracle Solution Functions/Features</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Strict firewall policies suppress SRTP port ranges</td>
<td>• TLS (TCP) tunneling traverses strict firewalls and HTTP proxies</td>
<td>• Maximizes service availability</td>
</tr>
<tr>
<td>• Service providers disconnect TCP-based SIP sessions past specified time limits</td>
<td>• DTLS (UDP) tunneling optimized for RTC</td>
<td></td>
</tr>
<tr>
<td>• Secure signaling and media (SIP/TLS and SRTP) is difficult to diagnose when problems arise</td>
<td>• Traffic to endpoints is normalized locally within the service core, making them easier to monitor, track, and manage than traditional OTT</td>
<td>• Eases troubleshooting of secure communications SIP sessions past specified time limits</td>
</tr>
<tr>
<td>• Complex application development environment—new codecs and firewall traversal protocols (for example, ICE, STUN, and TURN) often not included with third-party software libraries</td>
<td>• Easy-to-implement client source code with third-party or open source signaling and media libraries</td>
<td>• Simplifies application development</td>
</tr>
<tr>
<td>• Patent-pending tunnel redundancy ensures timely, reliable media delivery</td>
<td>• Complete SDK for Windows, Linux, Android, and iOS with reference applications and tools</td>
<td>• Improves fidelity of audio and video communications</td>
</tr>
</tbody>
</table>

Solution Components

Oracle’s Tunneled Session Management solution comprises:

• Oracle’s TSC server software
• Acme Packet 4500 hardware platform configured with a specialized network interface unit (NIU)
• TSC client application—available from Oracle partners or developed with a TSC client SDK provided by Oracle
OPTIMIZING AUDIO QUALITY

Tunnel redundancy is a patent-pending technology from Oracle to improve audio quality under adverse packet loss ranging from 5 percent to 25 percent or more. This unique innovation creates redundant tunnels with replicated signaling and media that is transparent to the client application. Like a tunnel or transport layer, the application does not need to be aware of the underlying mechanisms that help surmount packet loss in challenging OTT network environments.

As packets traverse networks and encounter packet loss, the TSC server and TSC-enabled clients choose the most available and timely packet from the duplicated tunnel set. Within redundant tunnels, packets are slightly offset, so as intermediate routers or the Wi-Fi access point drops packets, the same packet that was dropped in one tunnel will remain in another. When the packets reach their destination in the core or on the client, the media stream is reformed as if packet loss never happened.

Tunneled Service Controller Software

TSC software is integrated into Acme Packet OS and is responsible for tunnel creation and control that complement and leverage Oracle’s proven SBC features. For 3GPP-based IMS architectures, TSC software can also operate as a relay between client applications and IMS Proxy Call Session Control Function (P-CSCF). Oracle’s TSC software is fully compliant with the in-progress 3GPP EFTF draft.

Acme Packet 4500

Server-side functionality is provided by a specially configured Acme Packet 4500 that delivers the industry’s highest levels of performance and capacity in a rack unit (1U) form factor, in addition to the carrier-class, high availability (HA), and Network Equipment Building System (NEBS) certification required by service providers. Acme Packet 4500 integrates Acme Packet OS and Oracle’s purpose-built hardware to deliver the highly scalable signaling and media control functions necessary for first-class OTT services.

A specialized NIU delivers hardware-accelerated encryption, in addition to other packet processing intensive controls, for maximum performance and scalability.

Tunneled Service Controller Client Applications

Commercial-ready client applications are available from major client vendors. In addition, Oracle provides native client SDKs for major desktop and mobile OSs for developers who want to create or add TSC client functionality to their applications. The SDK supports a wide variety of OSs, including Linux, Microsoft Windows, Google Android, and Apple iOS. Upon registering to the network, the TSC client application initiates tunnels, which persist as long as the application is active.
These tunnels are capable of transporting all the signaling and media flows that comprise RTC sessions. Unencrypted SIP (User Datagram Protocol) and Real-Time Transport Protocol (RTP) flow securely within the tunnel, minimizing the overhead caused by separately encrypting (SIP/TLS and SRTP) the individual flows. Another benefit of this approach is simple troubleshooting and analytics, because each client’s signaling and media flows are aggregated in their own tunnel and terminated within the network, where they can be analyzed.

Key Functions and Features

The uncontrolled nature of the internet requires specialized techniques to maintain high media quality. Unlike most OTT applications, Oracle’s tunneled session management solution does not require proprietary codecs and protocol extensions to provide high-quality media in adverse conditions. It leverages standard codecs such as G.711 and G.729 and standard protocols, including SIP, that make it completely interoperable with existing standards-based business and consumer VoIP services. Because it is designed
for service providers and based on the market-leading Acme Packet 4500, it features carrier-grade performance, capacity, and HA. Additionally, because it is based on Oracle’s market-leading SBC technology, it can be implemented on existing SBC elements to augment and extend existing services, while leveraging the industry’s broadest range of security and other SBC functions needed to protect internet borders.

Key features include:

- **Strict firewall traversal.** The solution features intelligence that autosenses the presence and nature of strict firewalls or firewall/HTTP proxies to determine the most effective tunneling method between the client and TSC.

- **Improved audio quality over lossy networks.** When packet loss becomes an issue, tunnel redundancy, a function unique to this solution, can be dynamically invoked to surmount packet loss in the access network, while maintaining impeccable media quality in the core.

- **Secure, yet simple services.** All communications are fully secured through 256-bit encryption using TLS or DTLS tunnels. Local addressing as well as traceable signaling and media ensure quick diagnosis when troubleshooting is required.

- **Standards-based technologies.** EFTF standardization is in mature phases within the 3GPP.

- **Unprecedented scale and performance.** Oracle’s hardware-based encryption ensures unprecedented performance and value compared with competing solutions.

- **Highly available.** Oracle Communications Session Border Controller HA across tunnels in addition to industry-leading reliability for SIP with client tunnel re-establishment and keep-alive mechanisms.
- **Tunnel redundancy.** Tunnel redundancy is a patent-pending technology from Oracle to improve media quality under adverse packet loss ranging from 5 to 25 percent or more. This unique innovation creates redundant tunnels with replicated signaling and media transparent to the client application. As packets traverse networks and encounter packet loss, the TSC server and TSC client choose the most available and timely packet from the duplicative tunnels. Within redundant tunnels, packets are slightly offset, so as intermediate routers or the Wi-Fi access point drops packets, the same packet that was dropped in one tunnel remains in another. When the packets reach their destination in the core or on the client, the media stream is reformed as if packet loss never happened.

![Figure 2](image)

Figure 2. Within redundant tunnels, packets are slightly offset, so the same packet that was dropped in one tunnel remains in another. When the packets reach their destination, the media stream is reformed as if packet loss never happened.

**Conclusion**

Based on the Oracle Communications Session Border Controller, Acme Packet 4500, and Acme Packet OS, Oracle’s Tunneled Session Management solution enables service providers to offer secure, first-class OTT services.