ORACLE COMMUNICATIONS

An Oracle White Paper
August 2015

Communications Security: A Blueprint for Enterprise Session Border Controller Deployments

ORACLE

Introduction

Enterprises are deploying IP-based unified communications (UC) solutions to increase productivity, improve collaboration, and reduce capital equipment and operating expenses. However, conventional IP security products (such as firewalls and intrusion detection and prevention systems) were not designed with these kinds of real-time communications in mind—leaving organizations vulnerable to security threats.

When introducing UC platforms, IT teams must craft new strategies and identify new security solutions to protect and control real-time communications flows. Enterprise session border controllers (E-SBCs) are designed to overcome the unique security challenges enterprises typically encounter when introducing unified communications solutions.

This white paper reviews common UC security issues and describes how Oracle Enterprise Session Border Controller—in concert with conventional data security solutions—can help businesses safeguard IT assets, mitigate financial loss or legal exposure, and maintain high service levels when deploying real-time communications over IP networks.

Unified Communications Security Challenges

Unified communications introduces a myriad of security and service-quality challenges for IT teams. Based on circuit-switched technology, traditional corporate voice networks were closed in nature. As such, they could be reasonably well protected against eavesdropping, service theft, and other threats by using physical security measures. These networks were purpose-built to have the stringent reliability and latency characteristics needed for high-quality voice communications.

IP-based unified communications, in contrast, convey a wide range of information (voice, video, instant messaging, presence, fax), using IP networks that are inherently open. These traffic types are typically combined with traditional data applications on the same private IP networks and the internet. This exposes the IP communications infrastructure, services, and applications to a wide range of threats and service quality problems.

Attackers can leverage public domain scanners and reconnaissance tools to identify and exploit security weaknesses from inside or outside the enterprise. They may try to manipulate signaling or media flows, disrupt networking infrastructure to disturb business operations, listen in on confidential exchanges, or commit service theft.[1]

In addition, the network elements used to switch, route, and protect data traffic may not handle UC with the proper quality of service (QoS). Voice and video sessions are often called real-time communications, because they are sensitive to delay. All network elements, including security systems, must handle real-time communications traffic with minimal latency to ensure an acceptable user experience.

IT organizations must implement new mechanisms to protect and control real-time communications traffic flows, to ensure predictable and reliable services, and to enable satisfactory user experiences.[2] A range of specialized elements such as proxy servers, registrars, redirect servers, gateways, gatekeepers, and E-SBCs is required.

[1] Real-time IP communications sessions are controlled and transported via distinct protocols. Session Initiation Protocol (SIP) or H.323 signaling protocols are typically used to establish, control, and terminate real-time communications sessions. Real-time Transport Protocol (RTP) is typically used to transmit voice, video, or other media streams.

[2] If packets are not delivered at a regular pace or if they arrive out of order, users might experience distorted audio or video. Best-of-breed low-latency security solutions can encrypt media or signaling streams and perform other security functions without impairing the user experience.

Key Recommendations

E-SBCs should be deployed at network border points to create a demarcation that protects and controls unified communications. Key recommendations for incorporating E-SBCs into a UC security blueprint include the following:

- Configure E-SBC denial of service (DoS) protection thresholds and call admission control policies based on observed traffic profiles.
- Implement diverse network access links and active/ standby redundant E-SBC configurations as necessary to achieve availability objectives.
- Use transport layer security (TLS) and Secure RTP (SRTP) encryption to protect communications that traverse public untrusted networks such as the internet, and consider establishing the same policy for all other communications.
- Deploy data security devices (firewalls, intrusion detection systems [IDSs], intrusion prevention systems [IPSs], and so on) in parallel with the E-SBC (or at least as passive agents) to minimize their impact on voice and video quality. If firewalls must be used in front of an E-SBC, all SIP application layer gateway (ALG) functions must be disabled.
- Do not deploy anti-malware solutions to scan real-time communications, and consider configuring an E-SBC security policy to block UC file transfers. (File transfers outside of UC should be protected by anti-malware solutions.)
- Do not allow administrative access over public networks, and do not assume that internal networks are immune from compromise.
- Examine real-time communications signaling messages that egress from the enterprise to ensure that internal network topology is hidden from outsiders and that protocol differences are normalized.
- Collect accounting and management information from sources such as syslog, Simple Network Management Protocol (SNMP), call detail records (CDRs), and the Historical Data Recording feature of Oracle Enterprise Session Border Controller, and send it to ancillary systems for fraud and performance analysis.
- Integrate the E-SBC into your existing Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System (TACACS)+ for authentication, authorization, and accounting (AAA). Regularly test the network for voice vulnerabilities to ensure that protections are correctly configured.

Oracle Enterprise Session Border Controller takes advantage of the following features to protect unified communications:

- Unique high-performance architecture with dedicated processing resources that enable the E-SBC to withstand DoS/ distributed DoS (DDoS) attacks while continuing to forward traffic for valid sessions
- High-performance encryption capabilities to ensure confidentiality, integrity, and authentication

- Stateful high availability (HA) that protects complete session functionality during failover events
- Field-proven configurable multivendor protocol normalization capabilities that ensure interoperability across SIP trunking services and premises-based communications systems
- Available in software (Virtual Machine Edition) and appliance configurations to meet a range of scalability requirements

Real-Time Communications Security Guidelines

IT organizations must re-evaluate security systems and practices when implementing real-time communications solutions. Security teams should take the following steps when deploying a UC platform:

- Create a demarcation and enforcement point for the UC network. The enforcement point may provide demarcation between zones of varying trust such as the internet (public) and the internal (private) network or other trust zones such as a guest network, a demilitarized zone (DMZ), or a bring your own device (BYOD) network.
- Hide your network topology. Hackers can plan attacks by ascertaining information about network equipment (determining equipment types and software versions) or by detecting the IP addressing scheme a company employs. A UC demarcation device should remove any protocol fields that may assist in "fingerprinting" and should provide network address translation (NAT) at all protocol levels to conceal internal addressing schemes.
- Encrypt endpoint communications. Businesses should encrypt communications flows when transiting public networks, to prevent eavesdropping and impersonation. Encryption should also be considered on private networks to verify identity and prevent eavesdropping on privileged communications. Unfortunately, encryption can hinder lawful intercept or other regulatory and corporate compliance requirements. By establishing a UC demarcation point and anchoring, unencrypting, and re-encrypting sessions at the network perimeter, security teams can tap or replicate sessions in the clear for compliance purposes.
- Normalize protocol differences on demand. Interoperability problems, which can occur in attempts to establish sessions between systems from different UC vendors, can appear to be service failures. The problems are caused when UC vendors implement SIP differently. In extreme cases, the "normal" messaging from one manufacturer might cause failures or outages for another. Rather than depending on vendors to fix these interoperability issues, it is preferable to do so in real time with an E-SBC.
- Prevent DoS attacks and overload. DoS or DDoS attacks and non-malicious events such as registration floods can impair IP communications infrastructure (border elements, application servers, endpoints) and disturb critical applications and services. Attackers may try to flood a network from one or more endpoints or send malformed messages (protocol fuzzing) to overwhelm network devices. A UC demarcation device can ensure continued service availability by identifying DoS and DDoS attacks and appropriately throttling or blocking traffic.

- Ensure high availability. In the event of an equipment failure, physical attack, or persistent DoS/DDoS attack, a strong redundancy strategy can help restore service. A local highly available backup for the demarcation device and a redundant but diverse access link can provide fast recovery. A disaster recovery plan with redundant sites should also be considered to maintain continuous service availability.
- Enable secure management. The demarcation point should support secure management with encrypted protocols, integrate with existing SNMP and Security Information and Event Management (SIEM) solutions, and provide extensive alarms and logging for security-related events such as DoS or fuzzing attacks.

E-SBCs Complement Traditional Security Solutions

Conventional IP security devices—firewalls, intrusion detection and prevention systems, and anti-malware solutions—were not designed to control real-time communications sessions and do not address the unique security or service quality concerns associated with unified communications.

Firewalls

Firewalls protect IP data networks, servers, and applications against a variety of threats by performing stateful inspection and filtering at Layers 2 through 4 of the Open System Interconnection (OSI) model. You can configure most firewalls to provide rudimentary support for Voice over IP (VoIP) and UC by opening one or more User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) ports for SIP or H.323 signaling and a wide range of UDP ports (thousands in some cases) for RTP media. For all intents and purposes, the firewall acts as a pass-through device for the media. It can block real-time IP communications sessions, but it cannot actively manipulate signaling or media streams to detect or protect against sophisticated threats.

Many firewalls perform NAT, which changes Layer 3 IP addresses and Layer 4 port numbers without altering the corresponding information contained in SIP signaling messages. This causes user agents to send media to the wrong IP address, which is manifested in one-way audio or video.

Some firewall manufacturers have added SIP ALG functionality to translate IP addresses within the SIP or Session Description Protocol (SDP) messaging, which enables the firewall to maintain the integrity of SIP addresses while performing NAT. However, SIP ALGs do not generally perform dynamic port management to open or close media ports based on SIP session state. What's more, current research shows that many ALGs can easily be bypassed. An attacker can simply set up a valid session, for which the firewall inserts a rule allowing any traffic to pass between the hosts using these ports, regardless of whether the traffic contains the protocol that was initially negotiated.

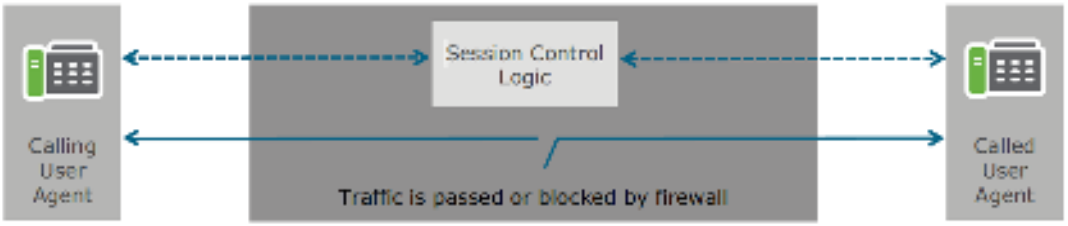

Figure 1. A SIP firewall implemented as a SIP proxy

Firewall vendors that have incorporated ALGs into their products must adapt to a broad range of data and real-time communications security threats. As a result, their products do not generally support the latest Internet Engineering Task Force (IETF) specifications for SIP or particular vendor-specific SIP implementations. When interoperability or one-way audio issues occur, a broken ALG implementation is often the culprit. In SIP terminology, an IP firewall with a SIP ALG function acts as a SIP proxy server, which is responsible for relaying and controlling SIP signaling information but is not actively involved in the RTP media path (the audio and video streams). An E-SBC, in contrast, is implemented as a back-to-back user agent (B2BUA), which actively processes both the signaling and media paths.

As its name implies, the B2BUA acts as an intermediary that terminates a session from one SIP entity, such as a calling party, and statefully establishes a distinct session with another SIP entity, such as a called party. Unlike a firewall, an E-SBC can control SIP sessions as well as control and manipulate the RTP media streams. By terminating, inspecting, manipulating, and re-establishing SIP sessions, an E-SBC can provide more-advanced security and control functions such as call admission control, protocol normalization, and transcoding.

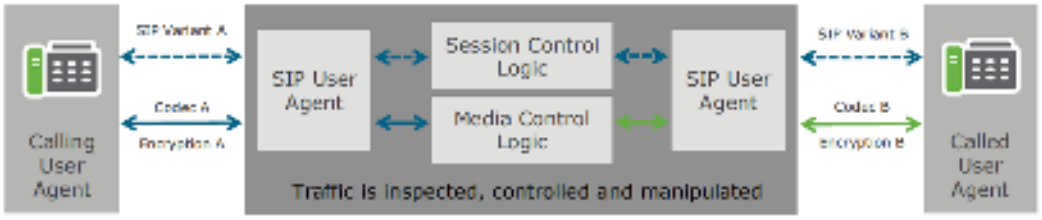

Figure 2. An E-SBC implemented as a SIP back-to-back user agent

A B2BUA acts as a user agent server (UAS) and user agent client (UAC), terminating and reoriginating signaling. Each session is divided into two distinct segments for the incoming (UAS) and outgoing (UAC) interface, and SIP signaling is performed separately for each leg. The E-SBC can inspect, add, delete, or modify SIP messages and log changes or rejections. This capability extends to the SDP information that defines the media.

After a session is successfully signaled, the requested media ports are opened. E-SBC settings can enforce a “latch” on the media source address, synchronization source identifier (SSRC), and contributing source identifier (CSRC) in the RTP stream, so that only media received from the authorized endpoint is passed. When the session is complete and a terminating message has been received (or a call timer has expired), the media ports are closed. For the duration of the session, the

signaling and media format and content are inspected and controlled according to administratively defined policies.

For all intents and purposes, the E-SBC acts as a highly specialized UC firewall. It defaults to a closed state (implicit deny) and allows only specified services to pass through it. Unlike traditional data firewalls, E-SBCs are designed to analyze and secure real-time communications protocols such as SIP, H.323, and RTP. E-SBCs can identify malformed frames, packets, and messages (which may have been generated for malicious purposes) and perform actions (throttle, log, alarm, block) according to policies to thwart attacks and alert IT security teams.

As a specialized UC security device, the E-SBC offers fundamental advantages over a conventional data firewall for VoIP or UC DoS/ DDoS protection. Traditional data firewalls limit traffic by using static or dynamic thresholds and applying access control lists. Adaptive rate limiters are vulnerable to false positives and negatives when handling real-time communications traffic. When presented with a new peak traffic load, the firewall may assume that a DoS attack is in progress. Conversely, an attacker can send traffic below the threshold to thwart detection.

When an attack is detected, a data firewall responds by throttling or dropping all traffic, including legitimate traffic, because it cannot inspect and intelligently classify real-time communications sessions. In contrast, Oracle Enterprise Session Border Controller is able to distinguish between legitimate and suspect traffic. It can drop or throttle malicious traffic while permitting legitimate traffic to flow normally.

Firewall performance is typically optimized for the large packet sizes used by data traffic, such as e-mail and Web pages. When they encounter the high messaging rate and small frame sizes used in high-capacity real-time traffic (or attacks against those services), firewalls often experience performance issues such as CPU and memory overloads and queue management and congestion problems. Small frame sizes can exhaust the commercial operating systems and x86 processors used by many firewalls, resulting in “choppy” or “robotic” audio and pixelated, jittery, or frozen video. Dedicated appliance firewalls based on ASIC (Application Specific Integrated Circuit) technology can deliver the performance needed for real-time communications, but the lack of intelligent traffic classification still limits their ability to respond to DoS/ DDoS attacks.

DoS attacks that consume all available bandwidth are the hardest to stop, because nothing can be done to recover services once the attacker’s traffic has reached the enterprise. Even if a network device is able to identify and drop 100 percent of the DoS traffic, there might not be sufficient bandwidth remaining for legitimate traffic. Some service providers offer a DoS mitigation service to handle this type of attack. The enterprise injects alternative Border Gateway Protocol (BGP) routes into its traffic to reroute the traffic through a high-bandwidth service provider network. The service provider performs DoS mitigation and filtering before forwarding the traffic to the enterprise.

Firewalls and E-SBCs

E-SBCs do not obviate the need for conventional data firewalls. The E-SBC secures VoIP, video, and UC traffic while the conventional firewall protects other data services. An E-SBC provides the demarcation and enforcement point for UC traffic between multiple “realms”—or IP ranges—of

varying trust levels, enabling a virtual topology similar to the firewall DMZ architectural model. Specific architectural configurations will vary, but generally speaking, an IT organization will configure an enterprise edge router to direct traffic to distinct public IP networks—one for UC and one for data. Separating UC and data traffic simplifies control, reporting, and troubleshooting.

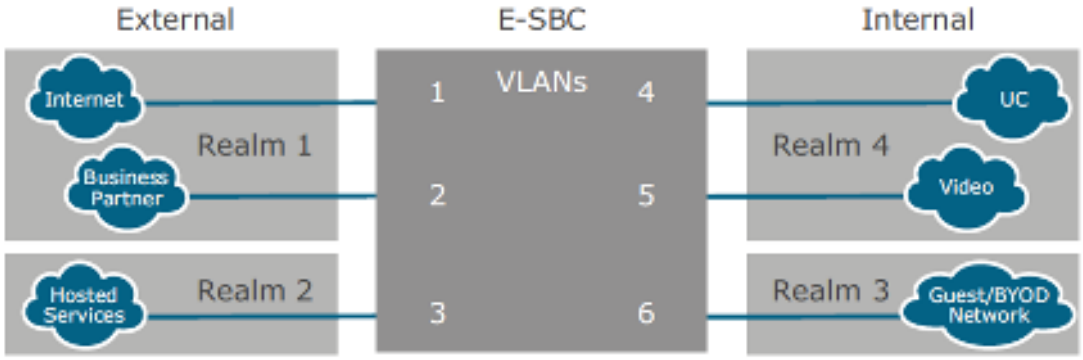

Figure 3. Using realms to establish zones with varying trust levels and corresponding thresholds for alerts and blacklisting

Realms are typically created for services such as SIP trunking, remote worker/ internet access, BYOD, or guest access. A typical SIP trunking or remote worker scenario will support two realms—one for public and the other for private connectivity. More-complex deployment scenarios might support multiple realms with varying trust levels on a single E-SBC.

Intrusion Detection and Intrusion Prevention Systems

Enterprises often deploy an IDS or an IPS to thwart certain types of malicious activities. Often connected to a mirrored switch port, the passive IDS simply generates alarms and events when it detects suspicious activities. In contrast, an IPS is an active device placed in the traffic path. As such, it can take corrective action, such as dropping a request or executing a program, when it detects suspicious behavior. Both types of devices detect attacks by comparing flows against known signatures, which are updated by IDS and IPS vendors on a reactive basis.

IDS as well as IPS systems introduce some complications for real-time communications traffic:

- Because they are deployed inline, underperforming signature-based IPS solutions can impair communications performance by introducing excessive latency.
- They can inadvertently block legitimate traffic by creating false-positive matches. (Some IDS systems classify normal SIP health check messages as attacks.)
- Encrypted traffic bypasses the signature analysis capabilities of IDS and IPS systems, opening a potential attack vector. As federated communications, cloud services, and other real-time communications applications adopt encryption, they circumvent the IDS/ IPS and create the possibility of attack.
- Hackers use message fragmentation and polymorphic code (software programmed to change frequently) to bypass the IPS—tactics that can be applied to communications traffic.

Intrusion Detection and Prevention Systems and E-SBCs

E-SBCs are deployed in conjunction with IDS or IPS solutions to address the challenges described above. Similar to firewalls, IDS or IPS solutions are used to contain malicious threats against data services, whereas E-SBCs are used to combat VoIP- and UC-specific threats. Best-of-breed E-SBCs such as Oracle Enterprise Session Border Controller employ anomaly-based threat detection mechanisms instead of signature-based schemes, obviating the need for signature updates or signature tuning.

With an anomaly-based approach, the E-SBC deconstructs SIP signaling messages and validates conformance with applicable IETF RFCs (it confirms syntax, examines for missing or duplicate parts, and so on) before forwarding the signaling information to the destination. Oracle Enterprise Session Border Controller executes these functions at near wire speed, without the use of signatures. It can be configured to discard invalid signaling messages and to generate SNMP traps or syslog messages in response to related security events.

Anti-malware Solutions

Enterprises deploy anti-malware solutions to detect and remove malicious software such as viruses, worms, and Trojan horses. Anti-malware solutions are deployed as gateways to prevent malware from entering the network and/ or as software on individual endpoints. Similar to IDS and IPS systems, anti-malware solutions use signatures to detect attacks.

Anti-malware detection should not be used for real-time communications, because viruses cannot infect an endpoint via RTP media streams and anti-malware solutions reduce quality of experience. There is no path for a virus to extend into a device's operating environment. A communications endpoint relays the RTP data payload to a codec that decompresses and plays media. If the payload were modified by a virus, it would simply produce unintelligible audio or video. In addition, anti-malware solutions must cache all or part of the data stream for analysis, which introduces latency, delay, and jitter into real-time communications streams.

Attackers may also attempt to disrupt an endpoint by "fuzzing" RTP protocol information, but these are not malware attacks and would not be detected by anti-malware solutions. Protocol fuzzing can be detected by an E-SBC, which drops non-conformant messages.

File transfers carried by certain types of instant messages can potentially contain malware. The Message Session Relay Protocol (MSRP) provides file transfer capabilities within the SDP, which is used by most UC clients. Two strategies are recommended for combating this type of malware:

- Block SDP that contains Message Session Relay Protocol (MSRP) or undesirable Multipurpose Internet Mail Extensions (MIME) types, so files cannot be transferred.

- Deploy malware detection and prevention software that processes the attachments that communications endpoints receive via UC.

Data Security Devices Are Not Sufficient for UC

Do not rely on data networking or security components to secure real-time communications sessions. The following subsections describe the range of security vulnerabilities and operational problems they can introduce.

Firewalls

Security and operational problems associated with firewalls include the following:

- NAT functions may change signaling enough to make it unusable.
- ALGs designed to protect signaling can be fooled into allowing unauthorized traffic; they may even break call flows.
- Firewalls may require large ranges of ports to be opened.
- Service availability can be impaired when firewalls become overwhelmed.
- Firewalls cannot handle DoS attacks efficiently.

Intrusion Detection Systems/Intrusion Prevention Systems

The security issues posed by such systems include the following:

- Threat identification relies on rules (signatures), which can be easily circumvented by attackers.
- Signatures need to be updated and tuned regularly—but often are not.
- When encryption is used, such systems may be bypassed.

Anti-malware Solutions

Anti-malware solutions are not effective for securing real-time communications for the following reasons:

- No viruses are carried in RTP streams, so anti-malware solutions just introduce latency—possibly even breaking real-time communications altogether.
- Anti-malware solutions are unable to match malware signatures in the small sample sizes required to keep real-time communications flowing.
- Although anti-malware solutions can detect malware in file transfers, the file transfers can be blocked by disabling them via MSRP or are better left to endpoint protection.

Oracle Delivers High Security, Performance, and Reliability

Oracle Enterprise Session Border Controller is purpose-built to enable highly secure, reliable, and scalable real-time communications. It leverages a unique multiprocessor design that delivers industry-leading performance, supports hardware-based encryption for ultimate scalability, and can be deployed in a redundant fashion to enable high availability. The platform also provides extensive management security features and capabilities to restrict administrative access and prevent management attacks.

Unique Dedicated Processing Resources

When deployed as an appliance/ engineered system, Oracle Enterprise Session Border Controller uses a unique, highly scalable architecture to deliver optimum performance and security. This architecture features dedicated network and signaling processing resources that enables Oracle Enterprise Session Border Controller to protect against a DoS attack while continuing to forward traffic for valid sessions.

Messages enter the network processor, where traffic is inspected at Layers 2–4 of the OSI model, matched against access control lists (ACLs); defragmented, unencrypted, and classified based on media type and trust level; and checked for rate limitations before being forwarded. Signaling is assigned to one of several traffic queues, depending on whether the source is trusted or untrusted, and forwarded to a host processing system or user space application that performs parsing and protocol validation, routing, load balancing, and other functions. Bandwidth for each queue between the network processing and host subsystem functions can be allocated separately to take into account variations in the ratio of trusted and untrusted traffic in a particular network environment.

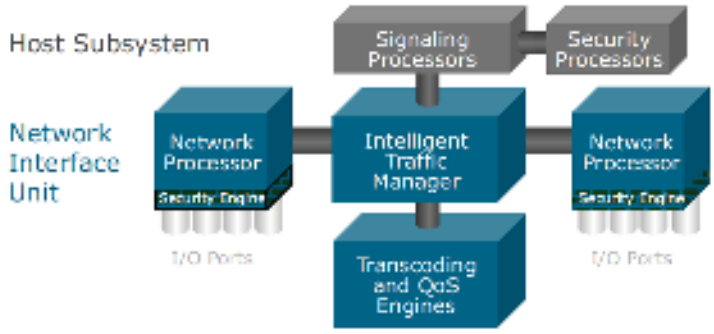

Figure 4. Dedicated processors for signaling and media tasks, enabling Oracle Enterprise Session Border Controller to deliver strong security and high performance

The host subsystem is composed of several functions, including signaling and security. Trusted traffic can be assigned priority over untrusted signaling traffic, enabling trusted services to be maintained even during a DoS attack. Once trusted signaling establishes a point-to-point connection through the E-SBC, the appropriate ports are opened and a “flow” for RTP media is established between the endpoints. A rule for the flow is inserted in the network processing function so that RTP packets can be inspected and forwarded to the next hop with minimum delay. This takes processing load off the host, gives priority to media, and yields the highest performance.

The E-SBC automatically regulates trust levels for incoming connections. Depending on the starting trust level and actions taken by the endpoint, connection requests are either promoted to the trusted queue and granted more bandwidth, demoted to an untrusted queue with less bandwidth, or denied altogether. The administrator for each network or logical group of networks (realm) that connects to the E-SBC can configure the thresholds and timers governing demotion and promotion. Managing trust based on realm allows "zones of trust" to be created and managed in the network. Trust can also be statically assigned for known endpoints so that there is no risk of accidentally blocking them.

Dedicated processing resources are used in all Oracle Enterprise Session Border Controller appliances. These appliances contain a network interface unit (NIU) with dedicated network processors that forward trusted media flows directly between input and output ports. Trusted media never crosses the backplane or engages host processing functions, enabling Oracle Enterprise Session Border Controller to deliver high performance and low latency. In addition, the backplanes are designed to provide more bandwidth than the total NIU port capacity, ensuring that the host system has sufficient capacity to process trusted and untrusted queues. The host system includes dedicated signaling processing hardware and a separate security processor to offload processor-intensive security functions.

The same logical architecture is implemented in the software used by the version of Oracle Enterprise Session Border Controller delivered on commercial x86 servers and the one that runs on VMware ESXi. The network processing function is implemented in the operating system kernel, and the host subsystem is implemented in a separate user space. Packet processing by the network function is dynamically balanced across all available processor cores and is symmetric multiprocessor (SMP) safe. With separate kernel resources, media can be forwarded quickly without the additional overhead of the host processing function in the user space. Signaling is processed by the host processing subsystem. This modular design provides a high degree of scalability in a format that addresses the unique functional and economic requirements of small to medium-size enterprises.

The unique architecture employed by Oracle Enterprise Session Border Controller has proven its superiority in numerous competitive comparison tests executed by customers using publicly available tools. The product is consistently resilient in the face of Layer 2 and Layer 3 floods as well as SIP floods.

Strong DoS and DDoS Protection

The Oracle Enterprise Session Border Controller DoS protection functionality protects enterprise network elements against DoS and DDoS attacks through overload protection, dynamic and static access control, and trusted device classification and separation at Layers 3-5.

The Oracle Enterprise Session Border Controller itself is protected from signaling and media overload, but more importantly the feature allows legitimate, trusted devices to continue receiving service even during an attack. DoS protection prevents the Oracle Enterprise Session Border Controller host processor from being overwhelmed by a targeted DoS attack from the following:

- IP packets from an untrusted source as defined by provisioned or dynamic ACLs
- IP packets for unsupported or disabled protocols

- Nonconforming/ malformed packets to signaling ports
- Volume-based attack (flood) of valid or invalid call requests, signaling messages
- Overload of valid or invalid call requests from legitimate, trusted sources

DoS attacks are handled in the Oracle Enterprise Session Border Controller's host path. The Oracle Enterprise Session Border Controller uses NAT table entries to filter out undesirable IP addresses; creating a deny list. After a packet from an endpoint is accepted through NAT filtering, policing is implemented in the Intelligent Traffic Manager subsystem based on the sender's IP address. NAT table entries distinguish signaling packets coming in from different sources for policing purposes.

The Traffic Manager includes two "pipes" (trusted and untrusted) for the signaling path. Each signaling packet destined for the host CPU traverses one of these two pipes. Packets from trusted devices travel through the trusted pipe in their own individual queues. In the Trusted path, each trusted device flow has its own individual queue (or pipe). The Oracle Enterprise Session Border Controller can dynamically add device flows to the trusted list by promoting them from the untrusted path based on behavior; or they can be statically provisioned.

Packets (fragmented and unfragmented) that are not part of the trusted or denied list travel through the untrusted pipe. In the untrusted path, traffic from each user/ device goes into one of 2048 queues with other untrusted traffic. Packets from a single device flow always use the same queue of the 2048 untrusted queues, and 1/ 2048th of the untrusted population also uses that same queue. To prevent one untrusted endpoint from using all the pipe's bandwidth, the 2048 flows defined within the path are scheduled in a fair-access method. As soon as the Oracle Enterprise Session Border Controller decides the device flow is legitimate, it will promote device to its own trusted queue.

Encryption and Authentication

Real-time communications media sessions are vulnerable to eavesdropping, tampering, and man-in-the middle attacks. RTP can be modified in real time to insert media in one or both directions. Signaling sessions can be intercepted to gather organizational intelligence, manipulate or tear down sessions, modify caller identities, insert spam, or collect registration credentials for offline cracking.

TLS encryption for SIP and SRTP can provide confidentiality for signaling and media sessions. If used in conjunction with client certificates and SIP credentials, TLS and SRTP provide assurance that the device is legitimate and offer a level of user identification. By encrypting signaling and media, organizations can prevent the previously mentioned type of attacks. And by verifying credentials, they can thwart man-in-the-middle attacks. In addition, the use of certificates and credentials enables administrators to refuse network access to devices that are lost or users who have left the organization.

An E-SBC performs client certificate authentication by using the Online Certificate Status Protocol (OCSP). It provides communications with an enterprise certificate authority, which issues unique client certificates for each client. Not all clients support installation of third-party certificates or encryption.

Most E-SBCs based on commodity off-the-shelf servers do not have sufficient capacity to perform encryption for large numbers of sessions. In fact, in tests with encryption enabled, some vendor capacity claims were slashed in half (or more). Oracle Enterprise Session Border Controllers support

optional NIUs that offload processor-intensive tasks. Hardware-accelerated NIU functions include high-capacity SRTP encryption, high-capacity termination for SIP-TLS, and high-capacity Internet Protocol Security (IPsec) encryption and TCP termination.

High Availability

Oracle Enterprise Session Border Controller can be deployed as a redundant pair referred to as an HA node. The HA configuration is designed to deliver continued operation if one unit experiences a power outage, a hardware or interface failure, or a service attack.

Each unit is deployed with redundant power supplies, along with redundant Ethernet links that provide the synchronization path for signaling and media state, configuration data, and health information. If one unit experiences a hardware failure or a process crash or cannot reach a monitored next-hop gateway, the other unit will take over automatically. High availability configurations are supported on the entire Oracle E-SBC product line.

In an HA node, one E-SBC operates in an active mode and the other E-SBC operates in a standby mode.

- Active. The active member of the HA node is the system actively processing signal and media traffic. The active member continuously monitors itself for internal process and IP connectivity health. If the active member detects a condition that can interrupt or degrade service, it hands over its role as the active member of the HA node to the standby member.
- Standby. The standby member of the HA node is the backup system. The standby member is fully synchronized with active member's session status, but it does not actively process signal and media traffic. The standby member monitors the status of the active member and it can assume the active role without the active system having to instruct it to do so. When the standby system assumes the active role, it notifies network management systems using an SNMP trap.

To produce a seamless switchover from one E-SBC to the other, the HA node members share a virtual MAC and virtual IP addresses for their media interfaces. Sharing these addresses eliminates the possibility that the MAC address and the IPv4 address set on one E-SBC in an HA node will constitute a single point of failure. Within the HA node, the E-SBCs advertise their current state and health to one another using checkpoint messages to apprise each one of the other one's status. Using the Oracle HA protocol, the E-SBCs communicate with UDP messages sent out and received on the rear interfaces. During a switchover, the standby E-SBC sends out an ARP request using the virtual MAC address to establish that MAC address on another physical port within the Ethernet switch. To the upstream router, the MAC address and IP address are still alive. Existing sessions continue uninterrupted.

The standby E-SBC assumes the active role when:

- It has not received a checkpoint message from the active E-SBC for a certain period of time.
- It determines that the active E-SBC's health score has decreased to an unacceptable level.
- The active E-SBC relinquishes the active role.

Each E-SBC establishes active and standby roles in the following ways:

- If an E-SBC boots up and is alone in the network, it is automatically the active system. The second E-SBC in the HA pair automatically establishes itself as the standby when it comes on-line.
- If both E-SBCs in the HA node boot up at the same time, they negotiate with each other for the active role using an internal algorithm.

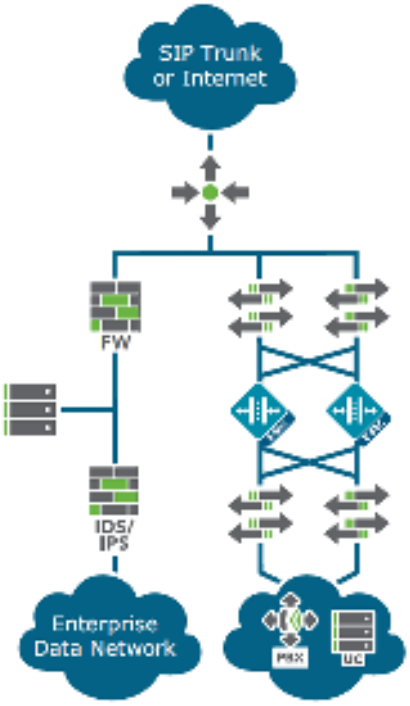

Figure 5. Oracle Enterprise Session Border Controller installed in parallel with data security devices and in active/standby configuration

Oracle Enterprise Session Border Controller stands up to equipment and interface failures as well as malicious attacks. Some E-SBC vendors leverage Virtual Router Redundancy Protocol (VRRP) to enable HA and may not provide continuous service in the face of DoS attacks. VRRP relies on underlying network services to communicate health information between units. If an E-SBC is under a DoS attack and the network becomes flooded, health advertisements may be lost and both E-SBCs will try to become the “master” of a single IP address, creating instability in the network. Some E-SBCs will try to recover from this condition by rebooting, which serves only to prolong the service outage.

In contrast, Oracle Enterprise Session Border Controller features intelligent load balancing capabilities that ensure that server destinations are not overwhelmed by surges in traffic. It monitors availability, session load, and call setup rate for each configured server (session agent). Oracle Enterprise Session Border Controller can temporarily remove a session agent from service to prevent it from being overwhelmed, based on thresholds set for maximum inbound or outbound sessions, maximum burst

rate, maximum sustained rate, and session agent availability. A sophisticated load-balancing scheme distributes incoming sessions across session agents, according to cost, preference, capacity, and other capabilities that are configured per server, enabling optimal utilization.

Stateful Media and Signaling Recovery

Some E-SBC vendors offer failover for the media path only. In contrast, Oracle Enterprise Session Border Controller provides stateful failover for media as well as signaling flows. All configuration parameters and the session state for all sessions are replicated to a standby unit over redundant dedicated links. If a failure occurs, Oracle Enterprise Session Border Controller will take over all sessions and associated media in as little as 40 milliseconds—with no session loss.

The resulting interruption may not even be perceptible to users. CDRs are preserved during failover, because the redundant unit is aware of the start and stop parameters for all sessions. Most competing solutions recover only the media, which causes the sessions to be dropped as soon as they need to be controlled.

Secure Administration and Management

Oracle Enterprise Session Border Controller provides robust management security. The platform features physically separate management interfaces, so administrative functions can be performed "out of band" over trusted connections. Various management flows can be encrypted with Secure Shell (SSH), Secure File Transfer Protocol (SFTP), and IPsec. Access control lists can be configured on the management interface to ensure that only authorized users can perform E-SBC administrative functions. All Oracle Enterprise Session Border Controller administrative processes have been hardened to resist DoS and fuzzing attacks. The platform does not allow outbound Telnet or SSH, so the E-SBC command-line interface (CLI) cannot be "hijacked" and used as a pivot for accessing other systems.

Standard CLI security features include an inactivity timer and two-stage user/ admin log-in levels. CLI audit trails can be logged locally, and when combined with RADIUS or TACACS+ for AAA, administrators can track individual user actions on the E-SBC. Optional security features include complex password support, role-based access control, and unmodifiable CLI audit logs that can be enabled with the Admin Security license.

SIP Topology Hiding

SIP transports signaling information as plain text. Some SIP headers—including Via, Path, Record-Route, and Service-Route—contain sensitive information such as the addresses of entities from the enterprise network or the number of such entities, which can be used to perpetrate attacks. Attackers can use this information to reconstruct the network topology. Oracle Enterprise Session Border Controller protects against these types of attacks by performing NAT. It automatically replaces addresses and removes extra headers from SIP messages when re-originating a session, making the next-hop device aware only of the E-SBC.

Virtual Machine Edition E-SBC

Oracle's Enterprise Session Border Controller Virtual Machine Edition (VME) deliver's Oracle's field-proven E-SBC functionality in the form of a software-based application for the popular VMware ESXi hypervisor. The Oracle E-SBC VME is a software-based solution that runs on industry-standard commodity x86 servers for ultimate choice, flexibility and economics. The solution scales to up to 1000 concurrent sessions per virtual machine and supports a wide range of security, interoperability, reliability, regulatory compliance and cost management features.[3] Oracle Enterprise Session Border Controller VME supports optional 1:1 high availability configurations as well as an optional on-board Enterprise Operations Monitor probe for advanced network monitoring, troubleshooting and analytics.

Interoperability Problems Can Impair Service Deployment

Common multivendor protocol interoperability problems can appear to be attacks. Such problems occur when service providers and communications system vendors implement SIP specifications in different ways or choose to include or exclude optional functions.

Private branch exchanges (PBXs) and UC systems may send unrecognized SIP headers or parameters or use a format that does not meet the expectations of a vendor's equipment, which can cause a PBX to deny access to a service or even cause a system crash. It is not unusual to perform a software upgrade on one SIP device only to introduce a new interoperability problem.

Oracle Enterprise Session Border Controller provides extensive protocol normalization and mediation functions that mitigate multivendor interoperability issues and improve service availability. It supports a wide variety of protocol configuration options that can be enabled or disabled and also supports two powerful tools for solving complex interoperability challenges.

SIP Header and Parameter Manipulation Rules

Many interoperability problems are the result of unrecognized SIP headers or parameters, or a format that does not meet the expectations of one vendor. The Oracle Enterprise Session Border Controller supports a unique SIP Header and Parameter Manipulation rules (HMR) feature that can be employed to add, modify, and delete SIP headers and parts of SIP headers such as the header value and header parameters to normalize SIP messages and alleviate SIP interoperability issues. Using this feature, the Oracle Enterprise Session Border Controller can edit response headers or the Request-URI in a request, and change the status code or reason phrase in SIP responses, based on administratively-defined policies. HMRs overcome vendor incompatibilities quickly and easily; they do not require a code update or a vendor patch.

[3] Some Oracle Enterprise Session Border Controller features are not supported with the Virtual Machine Edition. See Oracle Enterprise Session Border Controller VME data sheet for details.

The headers in the SIP messages can be manipulated both statically and dynamically. With static SIP HMRs, administrators configure rules to remove and/ or replace designated portions of specified SIP headers. With dynamic HMRs the Oracle Enterprise Session Border Controller has complete control over alterations to the header value. More specifically:

- The Oracle Enterprise Session Border Controller can search the header for dynamic content or patterns with the header value. It can search, for example, for all User parts of a URI that begin with 617 and end with 5555 (e.g., 617...5555).
- The Oracle Enterprise Session Border Controller can manipulate any part of a patterns match with any part of a SIP header. For example, 617 123 5555 can become 617 231 5555 or 508 123 0000, or any combination of those.

The Oracle Enterprise Session Border Controller uses regular expressions (special text strings for describing advanced search patterns) to provide a high degree of flexibility and simplify configuration for dynamic HMRs. As a result, an administrator can search a specific URI without knowing the value of the parameter.

HMRs can be applied to inbound or outbound traffic and can be applied to session agents, SIP interfaces and realms. Each HMR includes a set of parameters identifying the header parts to be manipulated, and in what way the Oracle Enterprise Session Border Controller is to manipulate them. Individual HMRs are chained together administratively to establish policies.

HMRs operate on single transactions; Session Plug-in Language (SPL) are used for manipulations based on the session state.

Session Plug-in Language

SPL can be used to perform sophisticated protocol manipulations. Similar to HMRs, SPL enables administrators to write a custom script or a set of rules for inspecting and modifying signaling traffic. Unlike HMRs, however, SPL provides callbacks or hooks directly into the E-SBC software and can maintain session state.

Because the SPL has direct access to the E-SBC software, it can perform a range of sophisticated actions, including removing a parameter from a request and replacing it in the response.

Beware of Third-Party Security Certifications

Many security departments look for independent third-party security “certifications” as evidence of rigorous testing and verification of a product’s security functions. Although some E-SBC vendors have sponsored tests of their equipment by third-party laboratories, it is important to note that there are no objective third-party certifications for E-SBC security functions. Labs for hire typically execute a test plan defined by the E-SBC vendor, and the scope is limited to functions the product performs well.

Common Criteria for Information Technology Security Evaluation (Common Criteria, or CC) is sometimes mistakenly applied to E-SBCs. CC defines “protection profiles,” or detailed requirements, for boundary protection devices and network-related devices such as data firewalls and routers.

Because no protection profile is defined for fundamental E-SBC functions (or SIP proxies, SIP servers, or SIP user agents), any CC certification for an E-SBC is based on protection profiles for ancillary functions, such as embedded firewall or routing software.

A recent review of a third-party SBC certification revealed that the SBC functionality and related VoIP/ video protocols such as SIP, TLS, and SRTP were not covered. Instead, the cryptography used in IPsec and RADIUS administration was tested. Translation: the certification proves only that the vendor's SBC can be securely administered.

Oracle Enterprise Session Border Controller has been tested and certified by numerous industry organizations, including the GSM Association, the MultiService Forum (MSF), and the SIP Forum. All of these certifications required testing of security capabilities. In addition, Oracle Enterprise Session Border Controller has passed the US government's Defense Information Systems Agency (DISA) UC requirements testing. Oracle Enterprise Session Border Controller 3820 and Oracle Enterprise Session Border Controller 4500 are FIPS 140-2–compliant and listed on DISA's Unified Capabilities Approved Product List.

Conclusion

Now that you've deployed IP-based unified communications solutions to increase productivity, improve collaboration, and reduce capital equipment and operating expenses, you need a strategy for protecting and controlling your real-time communications flows.

Oracle Enterprise Session Border Controller can serve as the linchpin of that strategy—working in concert with conventional data security solutions to help safeguard IT assets, mitigate financial loss and legal exposure, and maintain high service levels for deploying real-time communications over IP networks.

Appendix A: Common VoIP and UC Security Threats

VoIP and UC networks are susceptible to a variety of security threats. Hackers and fraudsters may try to manipulate real-time communications signaling or media flows, or they may attempt to disrupt networking infrastructure to impair operations, eavesdrop on conversations, or commit service theft. This table summarizes some of the more common VoIP and UC security threats. Enterprise session border controllers are designed to combat these threats.

TABLE 1. VOIP AND UC SECURITY THREATS

THREAT	EXAMPLE	POTENTIAL IMPLICATION
Reconnaissance scan	Address or port scan is used to footprint network topology	Targeted denial of service, fraud, theft
Man in the middle	Attacker intercepts session to impersonate (spoof) caller	Targeted denial of service, breach of privacy, fraud, theft
Eavesdropping	Attacker "sniffs" session for the purpose of social engineering	Breach of privacy, fraud, theft
Session hijacking	Attacker compromises valuable information by rerouting call	Breach of privacy, fraud, theft
Session overload	Excessive signaling or media traffic (malicious, non-malicious) is experienced	Denial of service
Protocol fuzzing	Malformed packets, semantically or syntactically incorrect flows are encountered	Denial of service
Media injection	Attacker inserts unwanted or corrupted content into messages	Denial of service, fraud

Making Unified Communications Secure
August 2015

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together