Acme Packet session border controllers in the contact center

Acme Packet session border controllers enable the delivery of trusted, first-class contact center IP telephony today and Unified Communications tomorrow

Whitepaper

Introduction

Contact centers are in the middle of a long-term transition from traditional TDM-based telephony to Voice over IP (VoIP). VoIP delivers significantly lower recurring costs and is a key enabler of contact center virtualization, allowing agents to work anywhere they have IP network access, including at home and while mobile. VoIP is also the critical first step toward truly comprehensive IP-based interactive communications - presence-enabled audio and videoconferencing, chat/instant messaging (IM), multimedia collaboration and communications-enabled business applications. Many contact centers are adding these services as integrated suites of applications referred to as Unified Communications (UC).

VoIP and UC are widely expected to help agents collaborate more effectively with other agents and non-contact center coworkers, thereby increasing first call resolution rates and decreasing average call resolution times. Voice and other real-time communication services over IP will help contact centers improve customer satisfaction and reduce overall operating and capital costs. But significant challenges in security, interoperability, service assurance and regulatory compliance emerge as contact centers begin migrating voice, conferencing and other real-time interactive services from TDM to IP networks.

Session border controllers (SBCs), product solutions extensively used by service providers to address these shortcomings, are being deployed by contact centers to enable the delivery of secure, high-quality, real-time interactive communications, including VoIP and UC. Similarly, service providers are using SBCs in their new offerings for their hosted and outsourced contact center solutions.

Business challenges

Contact centers bear the burden of rising expectations from two groups. Management is increasingly leaning on the contact center to attain higher performance targets on service quality and revenue generation, improve operating efficiency under constrained budgets and build customer loyalty and the brand. Meanwhile, user expectations of contact center service levels are rising as customers expect to be able to use whichever contact channel is most convenient to them and to get fast resolution to their issues on the first call. These dual pressures translate into the following challenges:

- Improve the customer experience to meet growing service expectations and to yield higher customer satisfaction and loyalty
- Improve first call resolution and average call resolution times by giving agents real-time access to other employees (subject matter experts and other second- and third-level resources) throughout the contact center, in effect making every employee a potential member of the virtual contact center
- Augment voice services with additional real-time communications services— presence, IM, conferencing, and communications-enabled applications—as the means by which agents can reach other colleagues and by which customers can reach agents
- Effectively manage agents in highly distributed, virtual contact center environments
- Mine customer knowledge to uncover cross-selling opportunities for additional revenues
- Improve agent motivation, morale, loyalty and job satisfaction to increase their productivity and reduce turnover; this means enabling agents to work from smaller remote locations or from home
- Reduce contact center capital and operating expenses
- Maintain and improve regulatory compliance in the virtual contact center environment

Technology trends and challenges

IT strategists working to arm the contact center with the tools it needs to survive in an increasingly competitive world must address several overarching technology trends and challenges.

Voice services are migrating inexorably from TDM to IP. The deployment of IP-PBX technology (in pure or hybrid IP/TDM form) is already well underway in most contact centers. On the IP-PBX trunk side, ISDN-PRI trunks are being upgraded to SIP or H.323 trunks. On the line side, TDM phones are being replaced with IP endpoints that use SIP or other open VoIP signaling standards; these include IP phones as well as PCs and handhelds running VoIP soft clients or UC clients. But this migration to newer technology must be managed incrementally while extending the life of existing equipment, both to maximize investments in legacy gear and to minimize the risks associated with the transition to newer technologies.

Contact center virtualization has emerged as a critical requirement. The flexibility to let agents work from anywhere in the world—including in centralized contact centers, in distributed locations, in home offices, at outsourcing service providers and while mobile—has become essential to both contact center labor cost optimization and agent retention. Agents must be able to work from practically anywhere in the world and access contact center infrastructure over a wide range of network types, while contact center management retains the ability to route, monitor, record and report on calls, managing these far-flung resources as a single pool of agents. Multi-vendor equipment interoperability issues are surfacing as formerly isolated signaling elements become integrated into the virtual contact center.

Contact center business continuity is growing in importance. As the contact center becomes more central to customer service and new revenue generation initiatives, IT strategists are working to improve the robustness of the contact center infrastructure. This effort focuses on the contact center's ability to continue functioning under peak load conditions as well as failures of service provider connections or contact center infrastructure elements. Tactics to improve contact center business continuity include load-balancing calls among virtual contact center resources and the use of routing intelligence combined with redundant service provider connections and internal infrastructure elements. These fault-tolerant systems enable faster, more seamless recovery from outages and overload conditions on service provider connections and the contact center IP communications infrastructure.

Call recording systems must evolve to keep up with changes to the contact center. As the contact center moves from TDM to IP voice services and toward virtualization, the architecture of call recording solutions must likewise evolve to become more open, robust, and flexible. Contact centers want to take advantage of new features that IP enables in call recording solutions, e.g., the ability to centralize distributed resources or to add geo-redundancy.

The addition of new IP-based application services including Unified Communications is imminent. Most contact center strategists have recognized the potential for presence-enabled IM, videoconferencing and online collaborative applications to enhance agent effectiveness and to engage employees external to the contact center in problem resolution to reach higher service quality targets. In many cases, the goal is also to make these new channels available for use by customers as well.

The transformation of the contact center to exploit VoIP and UC is widely expected to yield lower recurring costs, improved agent efficiency, and better resiliency in the face of heavy call volumes and infrastructure outages. But real-time interactive communications in general and voice over IP in particular require a level of control that existing contact center data network and security infrastructure—including routers, firewalls, and network intrusion prevention systems—cannot deliver. Thus, among the most critical new technology challenges is to assert this control over IP interactive communications across all the borders of the contact center.

Contact center operators should look to the example of service providers, including operators of hosted and outsourced contact center services, that were forced to confront this same set of problems several years ago. The technology widely deployed by service providers, including those that specialize in contact center services, is session border controllers (SBCs).

New control requirements

Successful delivery of IP-based interactive communications throughout the contact center requires additional controls in five key areas:

Security

Contact center infrastructure must be protected from deliberate attacks and non-malicious adverse events that can cripple voice and other IP interactive communication services. The direct threats include denial of service (DoS) and distributed denial of service (DDoS) attacks on signaling elements like IP-PBXs and automatic call distributors (ACDs), as well as non-malicious events like the re-registration floods that follow power outages.

Privacy is a significant issue due to regulatory constraints and/or the sensitive nature of some contact center communications (e.g., medical records, credit card numbers, etc.) The openness of IP networks also facilitates certain attacks on privacy. As a result, contact centers will need to encrypt certain sessions (signaling, media or both) end-to-end, or at least the portions of a session that must traverse untrusted IP networks.

Other significant security threats include intrusions by new viruses designed explicitly for real-time communications, unsolicited messages used as advertising or vectors for malware, referred to as spam for Internet telephony (SPIT), and directed attacks that exploit knowledge of network topology and addressing conventions. Other security threats associated with unauthorized access, including DoS/DDoS attacks, identity theft and information theft, must be minimized.

Application reach maximization

Voice and other IP interactive communications must extend beyond traditional centralized pools of agents to distributed agent pools, home-based agents, mobile agents, agents at outsourcing providers and ultimately to all callers. But IP communications hardware and software from one vendor doesn't always interoperate easily with those of other vendors, or with corresponding service provider infrastructure. For example, it is common for slight variations in implementations of the SIP signaling protocol to prevent one vendor's IP-PBX from successfully communicating with another vendor's softswitch.

These incompatibilities must somehow be mediated in order to achieve pervasive IP interactive communications throughout the virtual contact center, its various external service providers and its users. Many other potential incompatibilities exist that also must be mediated: different signaling protocols (e.g., SIP vs. H.323), transport protocols (TCP, UDP and SCTP), encryption protocols (TLS, MTLS, SRTP and IPsec), and codecs (G.711, G.729 A/B, G.729 E, G.723.1, G.726, G.728, iLBC). Incompatible dial plans, overlapping IP addressing schemes and incompatible IP protocol versions (IPv4 vs. IPv6) can also impede the reach of IP communications services throughout the virtual contact center.

Many agents working from home or small offices now connect to the contact center via the public Internet. However, most Internet access services use customer premise equipment (CPE) like a DSL modem or cable modem that includes a firewall and network address translation (NAT) gateway, both significant roadblocks to IP interactive communications. The firewall only allows inbound traffic that has been requested by the user, which prevents anyone outside the firewall from initiating real-time communications with that user. The NAT gateway presents a single IP address to the outside world, another problem for IP interactive communications if there is more than one IP phone or UC client behind the gateway.

Several NAT traversal techniques obviate both of these issues, but not every technique (e.g., STUN, ICE, TURN) will work for every access device. Supporting a patchwork of NAT traversal techniques is also a challenge for contact center IT staff, and non-technical remote users cannot be expected to make the requisite configuration changes to their CPE. Contact centers must therefore deploy a NAT traversal solution that can scale to support many Internet-connected remote agents without requiring an onerous level of IT support or any configuration changes by remote users.

SLA assurance

Given the business criticality of the contact center, its real-time communications infrastructure must exhibit very high levels of service quality and availability. Defending signaling elements from malicious DoS and DDoS attacks is one key component of service level agreement (SLA) assurance. Another is providing protection against non-malicious overloads, e.g., the flood of IP phone registrations that follows a contact center power outage, or a sudden surge in call volumes due to promotional events. The resulting dramatic spikes in call signaling rates can overwhelm call control elements in much the same way as DoS attacks.

Delivering SLA assurance also requires compliance with the traffic classification schemes many contact centers employ to give real-time traffic the bandwidth and low latency limits it requires at the expense of non-real-time traffic. QoS marking and VLAN mapping must be performed to assign IP interactive communications traffic to appropriate paths through the network. Mediation between different policy schemes and VPN types may be necessary to ensure appropriate traffic prioritization end-to-end. Reports on voice quality (based on R-factor or MOS scoring) and answer seizure ratio (ASR) should be available for network performance monitoring, capacity planning and service provider SLA compliance validation.

The contact center must also be able to survive overload conditions and outages on service provider links and critical internal signaling elements such as automatic call distributors (ACDs), IP-PBXs, softswitches, media gateways, and SIP proxies. Asserting policy-based admission control on external trunks helps avert overload conditions on signaling elements. Load-balancing across service provider connections and internal signaling elements also adds survivability. Ideally, the load-balancing mechanism should monitor the health and capacity thresholds of service provider links and signaling elements, and intelligently rebalance sessions to minimize the impact of infrastructure failures and overload conditions.

Cost optimization

Contact centers are under pressure to reduce capex and OPEX. One way to achieve this is to use interworking and protocol normalization to allow the ongoing use of legacy equipment at the same time that new IP communications services are being deployed. This extends the usable life of older systems and enables a gradual, incremental cutover to the newer technologies. Such interworking capabilities also become critical to integrating formerly autonomous IP-PBXs into the virtual contact center, and integrating heterogeneous contact center infrastructure in the wake of mergers and acquisitions.

Given the enormous amount of billable voice minutes used by the typical contact center, efficiencies in the use of service providers can reap huge cost savings. Hence, the ability to load-balance calls across multiple service providers, and to route calls based on factors like time-of-day, caller location, or trunk congestion, is extremely valuable. With toll-free numbers, the extensive use of take-back-and-transfer services, also known as transfer-connect or agent-redirect services, can incur service provider feature charges that run to millions of dollars annually in large contact centers. Mechanisms to execute these toll-free call transfers on the contact center’s own voice infrastructure instead of in the service provider network can yield significant cost savings.

Regulatory compliance

Failure to comply with various government and commercial regulatory mandates can expose the contact center to fines, increased merchant fees, legal liabilities and customer defections, often damaging reputation and brand image. Thus any mechanism deployed for regulatory compliance purposes in the legacy TDM environment must be preserved as the contact center migrates to the world of IP communications services.

For example, emergency service (E9-1-1) regulations require that emergency calls from agents located throughout the virtual contact center must be handled with the appropriate priority. In some contact centers, domain separation between business groups is important for regulatory compliance, e.g., to prevent leakage of insider information from an investment bank’s corporate finance division to its research arm. In others, call recording to archive voice conversations like stock trading orders is necessary. In still others, the privacy of real-time communications must be protected through the use of signaling and/or media encryption.

Acme Packet session border control solutions for IP contact centers

Acme Packet® session border controllers (SBCs) enable contact centers to assert these controls over their four critical IP network borders, as shown in Figure 1:

- **IP trunking border**—connections over SIP or H.323 trunks to service provider IP networks, affording connectivity to PSTN endpoints via media gateways in the service provider's IP network.
- **Private managed IP network border**—peering connections to IP network service providers whose business and consumer customers originate calls from native IP phones and VoIP or UC soft clients on PCs and handhelds; no media conversions between TDM and IP occur anywhere in the session.
- **Internet border**—connections to the public Internet over which home-based agents, mobile employees, and small remote agent pools establish VPN connections into the contact center, and over which customers establish unsecured VoIP calls and other IP interactive communications to the contact center using public-Internet VoIP services like Skype or Vonage.
- **Virtual contact center border**—connections over private IP network services (such as MPLS) to distributed pools of contact center agents, contact center outsourcing service providers and contact center hosting providers.

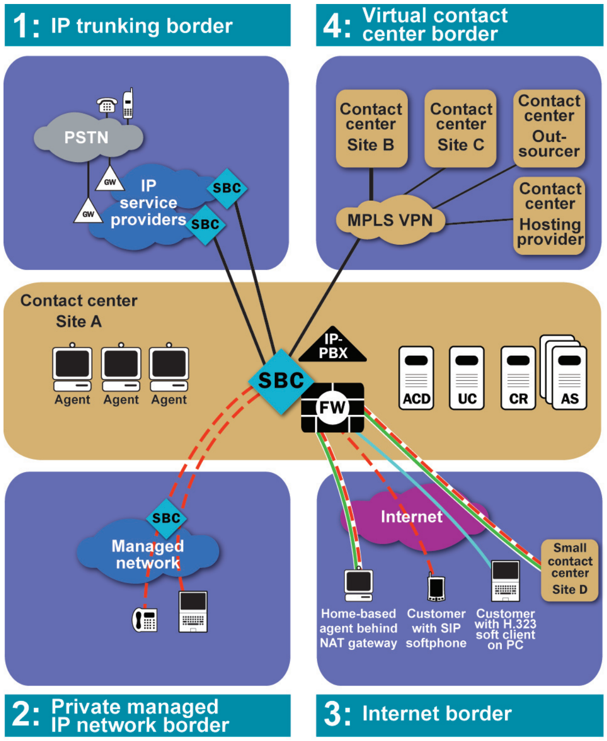
1: IP trunking border
4: Virtual contact center border
PSTN
GW
GW
IP service providers
SBC
SBC
Contact center Site B
Contact center Site C
Contact center Out-sourcer
Contact center Hosting provider
MPLS VPN
Contact center Site A
Agent
Agent
Agent
IP-PBX
SBC
FW
ACD
UC
CR
AS
SBC
Managed network
Internet
Small contact center Site D
Home-based agent behind NAT gateway
Customer with SIP softphone
Customer with H.323 soft client on PC
2: Private managed IP network border
3: Internet border

Figure 1: The four critical IP network borders of the contact center

1: IP trunking border

The first critical IP network border over which the contact center must assert control is the IP trunking border that connects it over IP trunking services (SIP or H.323 trunks) to service provider IP networks, which in turn connect to the PSTN via service provider media gateways. Using IP trunks instead of ISDN-PRIs offers contact centers a number of cost-saving and operational advantages (see sidebar).

Despite these benefits, IP trunks present some challenges. First, the service provider's IP network, like any IP network, cannot be trusted. It provides an attack vector for signaling and media overloads, DoS and DDoS attacks, and viruses and worms. These security threats can cripple contact center ACDs and IP PBXs, sap network performance and call quality and compromise the confidentiality of voice traffic.

Next, the IP trunking service may use signaling, networking protocols, encryption methods and codecs that are incompatible with contact center VoIP infrastructure. These incompatibilities must be mediated.

On the plus side, the IP trunking border provides a logical place to add session routing intelligence, improving the contact center's ability to recover from network failures, to choose the most optimal service providers and routes for outbound sessions (based on characteristics like cost, time of day, codec type, caller location and network congestion) and to generate reports necessary for traffic management and planning.

Benefits of IP trunking

Replacing ISDN-PRI, T1/E1 or larger TDM trunks with one or more IP trunks allows the contact center to:

- Reduce PSTN call termination costs by letting IP trunks route each outbound call over the service provider IP backbone to the service provider media gateway in closest proximity to the call's destination
- Reduce capital and operating costs by eliminating media gateways and TDM trunks in the contact center and supporting voice applications on the existing data network
- Add network fault tolerance (also referred to as geo-redundancy) by provisioning multiple IP trunks to diverse PoPs and/or diverse service providers
- Simplify operations by relegating media gateway and PSTN interconnection management to the service provider
- Cut the time to provision and deploy IP interconnects to a matter of days, as opposed to the months typically needed to provision and deploy TDM services.

Most contact centers must record some or all of their calls for regulatory, quality management and/or training purposes. The IP trunking border provides an optimal point at which to replicate ireal-time communications sessions for delivery to a call recording system.

To effectively take advantage of IP trunking services, contact centers must deploy SBCs to perform the following functions:

Security

The contact center is vulnerable at the IP trunking border to attacks by service provider employees motivated by malice or profit, and to non-malicious signaling overloads caused by events like power outages. These attacks and overloads can cause outages in contact center voice and other interactive IP communication services. The SBC must defend contact center signaling elements (as well as itself) against these DoS/DDoS attacks and overloads.

To prevent attacks from external IP networks, the SBC must enforce access control policies by limiting incoming sessions to the IP addresses of service provider peer SBCs. Knowledge of contact center IP addressing schemes and topologies can be used to compromise user privacy and mount directed attacks on contact center resources. Network Address Translation (NAT) must be employed to hide the topology of IP interactive communications servers and internal endpoints defending against directed attacks and protecting user privacy.

Intrusion monitoring and reporting should be provided by the SBC to help the contact center validate that its service providers are complying with security SLAs. Fraudulent use of contact center resources, e.g., unauthorized use of international calling or telepresence services by employees, can be costly and can adversely affect legitimate usage; the SBC should be able to detect and report on such unauthorized usage.

Application reach maximization

Incompatibilities between contact center signaling elements and service provider infrastructure for IP trunks must be mediated. The SBC must provide signaling protocol interworking for SIP trunks to H.323 IP PBXs, H.323 trunks to H.323 or SIP IP PBXs and between differing vendor implementations of SIP. Other required types of interworking that the SBC may need to provide include: transport protocol interworking for TCP, UDP and SCTP; encryption protocol interworking for TLS, MTLS, SRTP, and IPsec; and response code translations. The SBC may also need to provide IP address translation between overlapping private IP address spaces or between IPv4 and IPv6 addresses

SLA assurance

Given the business-critical nature of real-time communications in the contact center, the SBC must offer mechanisms to reinforce their uptime and performance. To enable contact center geo-redundancy, the SBC must be able to load-balance traffic across multiple IP trunks, monitor the health of trunks for overload and outage conditions and adjust load-balancing if a trunk reaches capacity or suffers an outage. Routing decisions should also be able to factor in quality metrics collected over time, giving preference to service providers with the best historical call quality or ASR.

When SIP trunks approach session capacity, allowing additional sessions on the same trunk degrades the quality of all sessions on the trunk. Likewise, too high a call acceptance rate can overload signaling elements. To ensure high session quality and prevent signaling element failures, the SBC must assert call admission control, refusing calls where necessary to prevent trunk saturation and signaling overload conditions.

Most contact centers utilize some combination of packet tagging and VLANs to ensure appropriate bandwidth and acceptable latency for real-time traffic at the expense of non-real-time data traffic. The SBC should support QoS marking and VLAN mapping for incoming traffic to comply with these policy mechanisms. It should also monitor and report on QoS and ASR to help the contact center validate service provider SLA compliance.

Cost optimization

The SBC must help contact center reduce service provider charges for VoIP and UC traffic via flexible session routing policies based on a variety of metrics, including least-cost routing, observed call quality and codec types. For example, the SBC might route outbound calls from the contact center to different service provider trunks depending on which offered the lowest charges based on time-of-day or caller location. Where possible, it should handle toll-free call transfers within the contact center network to reduce feature charges associated with service provider takeback-and-transfer services. The SBC should also provide flexible usage reporting for cost accounting and traffic planning purposes.

Traditional IP call recording topologies perform session replication with port mirroring in a Layer 2 switch. This approach does not offer optimum reliability and consumes an additional ACD port for every session to be recorded. Performing session replication for call recording in the SBC offers two distinct advantages. One, it offers more reliable transport of replicated sessions to the call recording system than a Layer 2-based solution. Two, moving session replication to the trunk side of the ACD eliminates consumption of an extra ACD port for every recorded session; these costly ACD ports can thus be recovered for use as agent seats.

Regulatory compliance

In addition to its use for training and quality management purposes, call recording is used extensively in contact centers for compliance with regulatory mandates like the Payment Card Industry (PCI) Data Security Standard and the Health Insurance Portability and Accountability Act (HIPAA). The SBC must provide a cost-effective and reliable session replication mechanism for recording IP communications services signaling and media.

In North America, contact centers must comply with regulations for E9-1-1 services, which require that emergency calls be handled with appropriate priority. The SBC must be able to identify emergency calls from anywhere within the virtual contact center, exempt them from admission control policies and route them with priority to the appropriate Public Safety Answering Point (PSAP).

2: Private managed IP network border

This border presents a number of additional challenges. For example, besides non-malicious signaling overloads and threats from service provider insiders, the contact center is vulnerable on this border to DoS attacks and malware originating from IP endpoints in the private managed network. Signaling protocol variations and other incompatibilities between the private managed IP network and the contact center must be overcome through interworking and normalization. To protect call quality and maximize contact center availability, admission control must be asserted and health monitoring of critical signaling elements performed.

The contact center must deploy SBCs on the private managed IP network border to perform the following functions:

Security

The contact center is vulnerable at this border to a range of attacks originating from native-IP end-users and from service provider insiders. While less threat-prone than the public Internet border, the private managed IP network border carries significantly higher security risks than the IP trunking border (Border 1). For example, malicious DoS/DDoS attacks and non-malicious signaling overloads (e.g., mass calling events) can traverse this border to bring down contact center signaling resources.

The SBC must therefore police inbound sessions at this border to avert both non-malicious overload events and malicious attacks; it must defend itself from attacks and overloads, otherwise a successful DoS attack on the SBC would leave contact center infrastructure open to subsequent attacks.

The SBC must employ NAT to hide the topology and IP addresses of signaling and media elements, thereby thwarting directed attacks. It should also provide monitoring and reporting for use in anomaly detection and post-attack forensics. On the malware front, the SBC should perform deep packet inspection (DPI) on incoming sessions to detect and eliminate viruses and worms, and use behavioral analysis to identify and block generators of SPIT.

Application reach maximization

Native managed IP voice services providers may use equipment that is incompatible with contact center infrastructure for IP communications services. The SBC must be able to obviate these differences through interworking capabilities, including the ability to mediate technology differences in signaling protocols (e.g., SIP vs. H.323), vendor implementations of signaling protocols (e.g., incompatibilities between the SIP used by contact center signaling elements and the service provider's infrastructure, such as a cable MSO's cable modem termination system), transport protocols (TCP, UDP and SCTP), encryption protocols (TLS, MTLS, SRTP and IPsec), and different versions of IP (IPv4 vs. IPv6).

SLA assurance

The SBC must maintain the uptime and performance of contact center IP voice and UC infrastructure via session admission control policies that intelligently assesses available bandwidth and session agent capacity. The SBC must manage incoming sessions so as not to exceed the maximum number of allowed sessions or maximum rate of session establishment that the contact center's signaling elements can handle. It should also monitor the health of logically-adjacent elements (such as IP-PBXs, ACDs, softswitches, and SIP registrars) and reroute and redistribute traffic around those elements when they suffer overload conditions or failures.

3: Internet border

The third critical IP network border over which the contact center must assert control is the Internet border, defined by connections to the public Internet. This border provides access to the contact center by two critical communities: employees who use VPN links over the public Internet to participate as members of the virtual contact center, including agents in distributed offices, home-based agents, and mobile employees; and end-users who call the contact center via public-Internet VoIP services like Skype and Vonage.

Public Internet VPN connections are an important enabler for contact center virtualization, allowing small pools of agents based in remote offices as well as home-based agents and mobile employees to cost-effectively connect to the contact center. But compared to other contact center IP network borders, the Internet border presents the broadest array of security threats, including malicious DoS/DDoS attacks on session control elements, non-malicious signaling overload events, viruses and worms specifically created to exploit real-time communications and SPIT.

Extending the reach of IP interactive communications from the contact center to remote agents through this border is also problematic due to the firewall/NAT traversal problem. Reaching home-based agents and small contact center pools over public Internet connections demands a scalable, manageable NAT traversal solution that does not require remote users to reconfigure their Internet access devices.

Depending upon industry and employee role, the privacy of sessions established across this border may be necessary for business reasons or compulsory for regulatory compliance, especially given the perceived higher risk of eavesdropping on the public Internet. However, homogeneous end-to-end encryption is not always feasible, as not all IP phones, media gateways or voice mail servers have the requisite encryption capabilities.

Finally, session quality across public Internet links can vary significantly, and must be monitored regularly to determine whether upgrading a pool of agents from an Internet connection to a higher-quality private network connection such as MPLS would be appropriate.

To address these challenges, the contact center requires SBCs on the Internet border to perform the following functions:

Security

The SBC must protect contact center signaling and media elements and itself from the broad range of attacks that originate on Internet-connected endpoints, including malicious DoS/DDoS attacks and non-malicious signaling overload events. It should perform deep packet inspection on incoming sessions to detect and eliminate viruses and worms, and use behavioral analysis to identify and block generators of SPIT.

The SBC should hide the topology and IP addresses of signaling and media elements to thwart directed attacks from across the Internet border. It should also monitor the Internet border for anomalous traffic and generate reports for use in post-attack forensics. Where appropriate due to the high value or sensitive nature of the content, the SBC should support encryption of signaling and media to protect the confidentiality of remote agent sessions and customer calls.

Application reach maximization

The SBC must provide hosted NAT traversal so that IP interactive communications sessions can be established to home-based agents without the remote employee having to install new CPE or reconfigure their existing firewall/NAT gateways. In sessions where each endpoint uses a different codec or frame rate, the SBC should provide transcoding or transrating.

SLA assurance

The SBC must perform a variety of functions to provide high-performance, highly available access to Internet-connected agents and consumer callers without exposing contact center signaling elements to DoS attacks and signaling overloads. Session admission control should be asserted to defend against DoS/DDoS attacks and avert call quality problems due to trunk saturation. To improve session quality for real-time communications between remote endpoints, the SBC should selectively release the media portion of a session so that endpoints can communicate directly, peer-to-peer, without hairpinning the media stream through the SBC.

The SBC must also provide quality of experience (QoE) reporting to help planners understand when an Internet connection to a remote agent pool needs to be upgraded to a higher-quality private WAN connection such as MPLS.

Regulatory compliance

For distributed agent pools and home-based agents, the SBC must enable compliance with government and industry regulations, including E9-1-1 handling to ensure that any emergency call placed by a remote agent is given the necessary priority.

Where needed for compliance with government or commercial privacy regulations, the SBC must support encryption of signaling and media to protect the confidentiality of remote agent sessions and customer calls. It should also offer encryption interworking to enable encryption end-to-end (using different encryption protocols on either side of the SBC) or partial encryption (so that the session can at least be encrypted between the SBC and the endpoint that supports encryption).

4: Virtual contact center border

The fourth IP network border over which the contact center must assert control is the virtual contact center border, encompassing private IP network connections to remote pools of contact center agents. These sites may consist of large contact centers established for business continuity purposes, regional offices, international offices, and agents working for contact center outsourcing service providers. These locations are large enough to require the bandwidth and reliability offered by private IP network services like MPLS. These services are also generally mandated for connecting the contact center to outsourcing or hosting service providers.

Because security is so critical to the business of enterprise-oriented private IP network service providers, outsourcers and hosters, the security risk associated with this border is low compared to Borders 2 and 3. Nonetheless, protecting the performance and availability of virtual contact center resources connected across this border is critical.

To overcome these challenges, contact centers need to deploy SBCs on the virtual contact center border to perform the following functions:

Security

The SBC must perform a number of functions to defend contact center IP interactive communications signaling elements (as well as itself) against DoS and DDoS attacks and signaling overloads originating inside the service provider, outsourcing provider or hosting provider network. The primary threat here is a service provider employee, an insider motivated by malice or financial gain.

The SBC should enforce access control policies by limiting incoming sessions to the IP addresses of service provider peer SBCs. Network Address Translation (NAT) must be employed to hide the topology of contact center signaling elements and internal endpoints, thereby foiling directed attacks and protecting user privacy. The SBC must provide intrusion monitoring and reporting capabilities to validate service provider compliance on security and network performance SLAs.

Application reach maximization

The SBC should provide interworking capabilities to mediate technology differences between signaling and media infrastructure elements across this border, including signaling protocols (e.g., SIP vs. H.323), variations in vendor implementations of signaling protocols, transport protocols (TCP, UDP and SCTP), and encryption protocols (TLS, MTLS, SRTP and IPsec). The SBC may also need to provide IP address translation between overlapping private IP address spaces or between IPv4 and IPv6 addresses.

SLA assurance

The SBC has a crucial role to play in maintaining service levels in the virtual contact center. The SBC must intelligently load-balance traffic among redundant contact center infrastructure elements, e.g., IP-PBX clusters. It should be able to monitor the health and traffic load on critical IP communications infrastructure elements, including ACDs, IP-PBXs, media gateways, softswitches, and SIP proxies. When it detects a problem—a hardware failure or the exceeding a capacity threshold—it should adjust accordingly, shifting traffic to one or more redundant standby or load-sharing systems. This same intelligent load balancing can help the contact center handle peak-period calling volumes by routing sessions to a contact center outsourcer for overflow call handling. Where appropriate, the SBC should also assert session admission control to prevent trunk saturation and signaling element overload.

The SBC must also work with traffic prioritization and QoS mechanisms to ensure that real-time communications traffic receives the bandwidth and low latency it requires at the expense of non-real-time data. Thus, it must provide transport control for incoming sessions with QoS marking and VLAN mapping, and monitoring capabilities like QoS and ASR reporting to validate service provider SLA compliance. This function may require the SBC to provide interworking between different types of VLANs.

Summary

The migration of voice services in the contact center from TDM to IP is now well underway, and the addition of new IP-based application services like UC is not far behind. IT strategists see this migration as essential to the contact center's strategic goals: meeting customers' growing service expectations, achieving ever-higher performance and quality metrics, improving agent retention rates, growing revenues and reducing capital and operating costs.

However, existing network and security infrastructure that was originally deployed for TDM voice services and non-real-time data exhibits crucial deficiencies for IP interactive communications. To address these shortcomings, contact center strategists should follow the example of service providers (including contact center outsourcers and hosting providers) by deploying SBCs. Session border controllers enable the contact center to assert control over its four critical IP network borders: its connections to IP trunking service providers, to managed private IP networks, to the public Internet, and to virtual contact center locations. With SBCs to reinforce these borders in five key functional areas—security, application reach, SLA assurance, cost optimization, and regulatory compliance—contact centers can successfully and safely navigate the transition to an all-IP world.

71 Third Avenue
Burlington, MA 01803 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com

10/01/08

The content in this document is for informational purposes only and is subject to change by Acme Packet without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Acme Packet assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Acme Packet, Acme Packet has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.