White Paper

Learn how to protect your data and build a secure, well-managed voice and data network.

verizon✓

VoIP and potential security risks.

Like many new technologies, Voice over IP (VoIP) has been thought to suffer from treating security as an afterthought. Although there have been well-documented security threats in the past (including eavesdropping, theft of service, and even denial-of-service attacks that can take down entire networks), the converged network composed of the old PSTN/TDM network and somewhat new IP telephony has been increasingly designed with security precautions in mind. This streamlined voice and data network is fast becoming the standard for enterprise communications, and security is one of its first considerations.

Verizon and VoIP Security.

Owning one of the largest networks in the world and a proven security expert, Verizon is leading the charge when it comes to VoIP network security. We build security into everything, with the understanding that your livelihood depends on how your employees, partners, and customers are able to communicate with one another.

We've gone to great lengths in designing a secure, layered infrastructure for our customers' converged networks. With each layer, we address the confidentiality, integrity, and availability of the call-setup information, as well as the voice flow itself. These layers are constructed with redundancy measures that provide reliable service. Many of our controls are not published, to maintain the security of our business VoIP network.

Our experience in both Voice over IP and security shows that we can meet the challenges faced from both within and outside your network. We've identified major issues, including:

- Phishing, phreaking (illegal use of another person's VoIP service), and eavesdropping.
- Network security and break-ins.
- Identity protection, including spoofing.
- End-to-end encryption and snooping by any party (internal or external) on signaling and media of communications.
- Denial of service (DoS, DDoS) and disruptive forces (TDoS, QoS).
- Core code vulnerabilities.
- Session Initiation Protocol (SIP) testing and hardening.
- Access to devices by approved personnel – identification of who is looking at my data and why.
- Storage of customer information (when, where, how long, how can it be used).
- Addressable IP ranges (attackable) versus private/hidden (both customer and infrastructure).

We recommend you follow the same security guidelines we use when deploying converged networks. This bottom-up approach helps to focus security goals with business objectives:

1. Define VoIP security policy – Add IP telephony to the existing security policy document. This will provide the framework in which VoIP can operate.
2. Business controls and processes – Build business controls and processes around the policy to meet company objectives.
3. Technical infrastructure – Implement the best products and technologies.
4. Compliance and incident response – Continually monitor for compliance and be prepared with an incident response system.

Verizon IP Trunking over Private IP (MPLS) is a collection of our best products and technologies layered into a secure VoIP network that meets the business needs of our customers. The service was designed with components you would expect to see in a hardened data network, including:

- MPLS VPN transport.
- Firewalls.
- Session border controllers (SBC).
- IPSec tunnels.
- Private VLANs.
- Out-of-band management.

The customer network.

The security of our network begins on your premises – because they're virtually an extension of our network. A more secure customer network increases the overall security of your VoIP services. Many of the threats against VoIP systems originate within our customers' network. So we've layered in security measures, including:

- Utilizing separate VLANs for voice and data – This lays a good foundation for applying access controls and QoS policies. VLANs can't be thought of as a magic bullet to VoIP security – history has shown VLAN hopping to be possible.

- Utilizing common features in layer 2 devices – Preventing "man-in-the-middle attacks" is paramount to all data applications in the local area network (LAN).

There are also precautions our customers can take, including:

- Using complex passwords – The largest known VoIP theft of service to date would have been deterred by setting more complex passwords.

- Restricting logical network access to critical servers and VoIP call processors – Protect your critical VoIP components by filtering access. Creating an approved device list during the design process can be very beneficial. Filtering can be completed at the network level by routers and switches or by adding a specialized appliance such as a firewall. Servers themselves can be protected by adding the approved device list to the underlying operating system level firewall. Access rules or black-hole routes can be used to layer protection on gateways.

- Turning off unnecessary services on all IP telephony components.

- Applying vendor-supplied patches in a timely manner – All major IP PBX vendors allow you to subscribe to a vulnerability notification system, or they provide this information on their website. Each time a vulnerability is announced, it should be ranked and prioritized. A plan for corrective action should follow.

- Utilizing session border controllers (SBC), VoIP-aware firewalls, and intrusion prevention systems (IPS) when possible – Adding these smart devices can help separate trusted networks from untrusted networks.

- Consulting vendor VoIP security documentation to harden applications – All major VoIP vendors have published best practices documents that outline how to best utilize the security features built in to their devices.

- Protecting the VoIP signaling and media by utilizing QoS throughout your network – The network must be provisioned to help prevent packet loss and reduce delay and jitter. Properly provisioned QoS helps limit the impact of unexpected high volumes of data such as the latest network worm. Predesigned VoIP readiness assessments can give you insight as to how your network will perform once VoIP traffic is added.

- Enabling logging of IP telephony components and establishing a practice of monitoring logs for security breaches and fraud – Multiple login failures, sudden spikes in call volumes, or an increase in toll calls can be easily identified through proper logging and monitoring procedures.

- Continuing to protect and educate against traditional system attacks (toll fraud, modem security, social networking attacks, etc.) – Even the most hardened network can be breached when credentials are stolen from legitimate users through social networking attacks.

- Performing a VoIP vulnerability assessment – A post-install assessment helps validate that security controls were implemented properly as well as identify any residual risk(s).

This is merely a sampling of possible, applicable security controls. Ultimately, it is up to you to decide which security controls are appropriate. Additional information may be found in numerous VoIP security books, vendor white papers, and websites.

The demarcation point.

Your network's first interface point is the Verizon Private IP customer premises equipment (CPE). This access router is provisioned by Verizon to communicate on your private MPLS VPN. The provisioning that takes place creates a unique configuration fingerprint for that location. No two CPE routers are configured exactly the same on the Verizon network, and only a unique, properly configured router will work on a particular circuit. Routers that are configured for BGP can optionally choose to turn on BGP router authentication. This step provides an additional level of trust authentication that validates the peers on each end of the circuit. Anyone attempting a "man-in-the-middle attack" would not be able to bring the circuit up without the provisioned authentication credentials. All Verizon service elements, service nodes, and IP networks are secured by Verizon.

The private IP network.

Private IP is based on MPLS technology, which complements Verizon's extensive public IP network capabilities. MPLS enables networks to take advantage of the best of IP, asynchronous transfer mode (ATM), and frame relay by allowing the integration of Layer 2 switching (ATM and frame relay, for example) and Layer 3 routing (IP). The MPLS signaling protocols support and create labels required to move traffic across the network. The labels identify the end address destinations of the network traffic.

Verizon has developed and deployed a highly scalable and resilient MPLS VPN architecture to meet the stringent requirements of your mission-critical IP data-networking applications. This architecture serves as the underlying infrastructure for Private IP. Verizon's design goal for Private IP is to provide a network service platform which is scalable, survivable, and efficient, without sacrificing performance. Verizon uses the best carrier class routers trunked over a dedicated high-capacity MPLS backbone to support MPLS VPNs with end-to-end QoS.

Verizon's Private IP backbone topology has been engineered for high resiliency and fast, efficient failover times. The P-core is a closed, private MPLS backbone (i.e., there is no Internet connectivity) that is dedicated solely to MPLS and does not support any direct customer access connections. Using a dedicated P-core enhances network scalability by reducing open shortest path first (OSPF) adjacencies and providing OC48 trunking and high-density aggregation of PE trunks.

Every PE router is diversely trunked into two diverse P-core routers so a node will never be isolated. The routers used are a combination of PE Routers (Cisco ESR/Cisco GSR/Juniper Networks M320 [2010]/Cisco CRS-1[2010]) and P-Core (Cisco GSR/ Juniper Networks T-series). Every P-core router has at least two physically diverse SONET/SDH paths to other P-core sites so a node will never be isolated. The P-core trunks are built on a combination of C-192, 10 Gbps Ethernet, and OC-768 (40 Gps) and are QoS-enabled with a Layer 3 QoS scheme that utilizes low-latency queuing (LLQ) and class-based weighted fair queuing (CBWFQ) to enable QoS on a per-hop basis instead of relying on overprovisioned trunks like other service providers. Customer access connections and the uplink trunks between the PE routers and the P-Core routers utilize a similar but enhanced Layer 3 QoS scheme (e.g., LLQ and CBWFQ), which, together with the core, provides end-to-end QoS support for Private IP customers.

The Verizon Private IP network can automatically detect and dynamically reroute around transmission path failures. The OSPF routing protocol is used within the Private IP network to establish and maintain IP reach ability. OSPF reroute times vary depending on where the path fails (fast for local physical failure and dead timer interval for remote failures). Label distribution protocol (LDP) is used to dynamically establish label-switched paths (LSPs) between all PE and P routers and will quickly reestablish the LSP following an OSPF rerouting event.

The Verizon Private IP network is secure due to:

- Full address space and routing separation. Within each MPLS VPN, customers have full control of the IP address assignments, which allows for private address (RFC1918) as well. The only traffic on the VPN is to or from provisioned locations as ordered by the customer. In the simplest IP trunking configuration to a single customer location, the only traffic on the circuit is between the customer's edge (CE) router and the Verizon SBC. It can logically be thought of as a point-to-point connection.
- Verizon MPLS core being a closed and hidden system. The internal structure of the Private IP service core network (PE and P elements) is not visible to outside networks (Internet or any connected VPN).
- Protection against label spoofing. An entity attempting to attack you might try to gain access to your VPN by inserting packets with a label that he doesn't "own." The provider edge (PE) router will reject any packets that do not match the provisioned label. This attack will not be successful, as all of the potential attack traffic will get discarded.

Separation of networks.

The Verizon IP Trunking over Private IP (MPLS) service utilizes the network separation abilities of an SBC to perform a number of security functions. For most people, the term SBC is new, but SBCs have been in use for securing VoIP networks for over five years. As its name implies, the SBC provides three services:

1. Session – It looks for real-time, interactive communications like SIP.

2. Border – It allows peer bordering services for IP-to-IP networks.

3. Controller – It provides security, service-level assurance, and service reach services.

The Verizon network–based session border controller sits on both your Private IP network and the Verizon high-speed backbone. An SBC is a VoIP session–aware device that controls call admission to a network at the border of that network.

The SBC functions as part of the intelligent layer of the VoIP network and has two primary responsibilities. First, it acts as a translator. The SBC actually terminates the SIP conversations from the two separate networks. All SIP packets are inspected for the proper content and formatting. Once the SIP message is verified to be valid, a new SIP message is then created on the other network, wrapped in a new IP packet. All layers (1–7) of the original packet are changed to offer complete topology hiding between the two networks.

Secondly, the SBC acts as a kind of translator traffic police. The SBC is configured to pass only the necessary protocols to deliver the service. Any extra traffic attempting to traverse the SBC is dropped. SBC is also involved in two distinct parts of calls – the first is the signaling function that controls access of VoIP signaling messages (SIP) to the network and manipulates the contents of these messages. The second is the media function which controls access of media packets to the network. When deployed in back-to-back user agent mode (B2BUA), SBCs can provide a number of security functions:

- Topology hiding and IP anonymity – Virtually any IP address can be configured to allow anonymity of your internal network if desired.
- Network protection – Protects you from malicious or nonmalicious attacks against the network. Due to its specific VoIP-only programming, it blocks other protocols from communicating to devices behind it.
- SIP-based denial of service protection – Throttling of SIP packets, SIP deep packet inspection (DPI) and call admission control help to control the SIP application. The SBC also has dynamic trust management to help protect the SBC itself from attacks.
- Session-based RTP pinholing – Provides rogue protection. Only RTP streams that are setup through the SIP messages are opened.
- SIP deep packet inspection is performed, looking for anomalies in the packet that may be caused by a rogue device.
- Call admission control (CAC) is enforced to detect congestion that may be caused by a DoS attack. This can be based off the number of sessions or amount of bandwidth.
- Denial of service protection through the use of dynamic trust management (DTM). DTM classifies devices as trusted, untrusted, or malicious based on their signaling behavior. Verizon SBCs utilize these queues with wire-speed packet classification and dynamic trust management to help prevent service disruption by an attacker. The SBC automatically promotes or demotes a device trust level based on behavior. When a device is introduced and begins communication, it is put in the untrusted queue by default. As it communicates properly, it is promoted to a trusted level. Devices determined to be malicious are blocked from utilizing any processor resources. This helps the network to operate at efficiency even while under attack.

IPSEC-encrypted sip messages in the Verizon high-speed ip backbone.

Beyond the SBC, the SIP packets and the RTP streams are separated. The SIP messages only traverse encrypted IPSec tunnels as they travel to our IP call-processing node via the Verizon high-speed IP backbone. Unlike call-setup messages in the TDM world, the modern era has dictated a greater value of the signaling information. Verizon creates tunnels between our VoIP nodes to maintain confidentiality and integrity of the call-setup information. Encrypting the SIP messages allows the RTP flows to be anonymous as they traverse the IP backbone to the media gateways, their ultimate destination.

Always on the lookout for attacks.

The Verizon VoIP nodes are constantly on the lookout for anomalous traffic. Intrusion-prevention devices drop attack traffic at the node edge usually before it can harm VoIP traffic. The intrusion prevention and detection systems are monitored 24x7x365 as they look for sudden changes in the traffic flow between nodes. A sudden spike of network traffic from the baseline is logged to our monitoring station for further investigation. Any device attempting to disrupt our service can be dealt with at the network entry point by our IP network engineering team.

Partner with experience.

Our IP communications consultant services are designed to help organizations become better able to support advanced communications services across their entire network infrastructure. Security specific services include:

- VoIP Security Assessment – We've developed a special program to address the unique security concerns related to the deployment and the operation of a VoIP infrastructure. This program covers all aspects of VoIP security, such as perimeter security of the VoIP infrastructure, segregation between voice and data, full testing of gateways and gatekeepers, etc., and pays special attention to problem areas such as phone tapping, Spam over Internet Telephony (SPIT), etc.
- Security Policy Update Assistance – Adding a new application like voice to your data network should be addressed by your security policy. Verizon consultants can help you create a custom policy for your environment.

- Enterprise Security Integration for Converged Networks – When moving to a converged network, how will VoIP integrate into the overall security structure of your network? How do you secure the endpoints? How do you authenticate users of the system? How will the VoIP components assimilate into your network access control (NAC) system? These are just some of the questions our consultants can assist you with.

- Installed VoIP Penetration Assessment – This post-installation scan verifies that our secure design has been implemented properly.

Why Verizon?

With our history in building networks and providing network security, we are well-suited to provide your enterprise with a multilayered VoIP solution. Find out how Verizon's Professional Services can help you build a secure and well-managed voice and data network. Visit verizonenterprise.com/products/advanced-communications/voice-over-ip/ for more information.

Useful Links.

Verizon Security Console –
verizonenterprise.com/us/products/security/

Verizon Securing VoIP White Paper –
verizonenterprise.com/resources/whitepapers/wp_securing-voip_en_xg.pdf

Verizon Global IP Backbone Map –
verizonenterprise.com/us/about/network/maps/maps.fxml

Verizon VoIP Products –
verizonenterprise.com/us/products/advanced-communications/

Verizon IP Trunking –
verizonenterprise.com/us/products/advanced-communications/

verizon✓

verizonenterprise.com