Secure IP Telephony For The Enterprise
Pingtel and Check Point Software Technologies

Summary
Voice over IP (VoIP), or IP telephony, is a growing market that affords cost saving opportunities for companies that use traditional telephony or are looking to expand their connectivity capabilities. In five years, IP telephony will be a $15 billion market and 2.2 million businesses will be using VoIP in some form. Companies are looking to VoIP to reduce their telecommunications and network operating costs. Voice-enabled applications also provide opportunities to improve efficiency, productivity, and competitiveness. However, companies considering VoIP have two important concerns: the cost and ease of migration to VoIP and the security of their networks and business.

Security is an important consideration when implementing VoIP because each element in the VoIP infrastructure, accessible on the network like any computer, can be attacked or used as a launching point for deeper attacks. In addition, VoIP presents certain specific security challenges. Both parts of a VoIP call, the call setup messages and the actual call media stream, need to be inspected by a firewall capable of both network and application level protection. Without this protection VoIP calls are susceptible to Denial of Service attacks, hacked gateways leading to unauthorized free calls, call eavesdropping, and malicious call redirection. Lastly, Session Initiation Protocol (SIP) is a new application protocol for VoIP and the firewall must understand this protocol to properly enforce the company’s security policies.

Pingtel and Check Point offer a VoIP solution that addresses these concerns. Pingtel is a market leader with an affordable, low-risk software IP telephony solution entirely based on SIP. Check Point, the market leader in Internet security, leverages its Application Intelligence technology to protect voice communications from all the same threats that endanger data communications, such as denial of service attacks, hacking, and loss or corruption of business-sensitive information. The Pingtel–Check Point solution enables organizations to deploy VoIP cost-effectively and securely.

In This Document
1 Voice over IP (VoIP) is a healthy, growing market
2 Customers are ready for VoIP
3 SIP emerges as the de facto VoIP standard
4 VoIP and security vulnerabilities
5 The secure VoIP-enabled enterprise: The Pingtel–Check Point solution
6 Check Point advantages in the VoIP-enabled enterprise
7 Security buyer’s checklist
8 Implementation scenarios for transition to secure VoIP
Voice over IP is a healthy, growing market

**VoIP** is voice delivered over IP (Internet Protocol). Voice in digital form goes from computer to computer or computer to phone in packets over the same network as data, avoiding the tolls charged by telephone service over the public switched telephone network.

An estimated 70 percent of U.S. companies are experimenting with voice over IP (VoIP), and many pilot programs are ready for widespread roll out. Companies in the news for their enterprise VoIP implementations include IBM, Dow Chemical, DuPont, and Merrill Lynch.

IP telephony will be a $15 billion market by 2007, predicts IDC. Nineteen percent of all U.S firms, approximately 2.2 million businesses, will be using VoIP in some form by 2007, says market research firm In-Stat/MDR. That is up from 2 percent in 2003. IDC estimates that revenue for the total IP telephony market will grow from $281 million in 2003 to $6.7 billion in 2007. LAN IP-PBXs will account for 70 percent of this total market by 2006, up from 60 percent in 2002.

Buying a new circuit-switched PBX is investing in a dead-end technology, says Raymond D. Keneipp, vice president of Networks & Telecom Strategies for the Burton Group. “I think everybody has accepted the fact that we will end up with a converged [voice and data] infrastructure. It’s only a question of are you going to do it sooner or later.” (“Pack up PBX—VoIP is Here,” ZDNet Tech Update, August 12, 2002)

**PBX** is a phone system owned and operated by an enterprise that switches calls between users who share external phone lines. Companies save money because they don’t need a separate telephone line for every user. Companies implementing VoIP have three PBX options: upgrade their traditional PBXs, replace their traditional PBX with new IP-BPX hardware, or use commodity hardware running IP-PBX software.

Customers are ready for VoIP

Most customers are interested in VoIP because it promises significant cost savings—as much as 40 percent over traditional telephony, according to some estimates. The savings come in several areas.

- Reduced charges for voice calls. Local calls within the company bypass the telephone company and avoid toll charges or take advantage of lower rates that some carriers offer for IP voice packets.

- Reduction in network operation costs. Voice and data over the same network eliminates redundancy in hardware and wiring. It also streamlines network management.

- Relocations are easier and less expensive. Employees simply unplug their phones from one network jack and plug into another.

- Higher functionality. Moving voice into the data environment generally lowers the cost of integrating voice and data systems to achieve business efficiencies.
Prime candidates for VoIP solutions are those companies seeking the tactical advantage of cost reduction in telecommunications and network management. They include:

- Companies with many branch offices and a significant volume of telecommunications among them and headquarters.
- Fast-growing companies that are frequently changing their voice systems by adding many users or making many moves and changes.
- Companies with a very mobile workforce or who are migrating towards having employees work substantially from home.
- Companies with centralized IT management and limited staff or skills at remote locations.
- Companies with a high dependence on telephone communications. These include companies with customer contact centers for sales and support.

The advantages of VoIP, however, aren’t limited to cost savings. VoIP enables many new applications that promote productivity as well. Presence applications let users log in anywhere and receive calls routed to them along with related data. Unified messaging lets users manage email and voicemail from one desktop GUI. Voicemails can be sent to e-mail addresses and then forwarded to other phones and locations from the Web browser. A call can ring multiple numbers simultaneously for conferencing. Dialed, missed, and received calls can be logged. Speech-to-text services can be implemented.

Customers who are attracted to the strategic advantages of VoIP include:

- Companies that aggressively seek out new technology applications that operate over IP data networks for strategic competitive advantage
- Early adopters and extensive users of video conferencing
- Early adopters of unified voice and email messaging
- Companies with many users of personal productivity applications, such as PDAs.

Sales opportunities for VoIP solutions typically open up when:

- A PBX has reached its maximum configured capacity, yet additional users or phones need to be added.
- A company's investment in legacy voice infrastructure (PBX) is fully depreciated.
- Maintaining and upgrading the legacy PBX equipment has become too difficult and expensive. Parts can be hard to find and expertise can be in short supply.
- Companies undergo significant changes, such as opening new offices, relocations, acquisitions, and divestitures.
SIP emerges as the de facto VoIP standard

SIP is a signaling protocol. It locates and connects endpoints or applications on an IP network. It uses SDP (Session Description Protocol) to determine the capabilities of the endpoint devices or applications and negotiate a connection. Once SIP establishes the connection, RTP (Real-time Transport Protocol) handles transmission. ("It’s Time to Take a Look at SIP," Network Computing, April 17, 2003)

H.323 is a protocol suite approved by the International Telecommunication Union (ITU) for multimedia communication over LANs and the Internet.

Voice sessions in an IP network are set up, controlled, and concluded by a signaling protocol. Early VoIP solutions used H.323 or proprietary protocols. However, SIP—Session Initiation Protocol—has quickly emerged as the industry standard for new development in VoIP.

SIP messages contain call control methods for requests or response codes for replies that are exchanged to initiate a session. This involves locating the target, determining if the target is available, determining the media capabilities of the target, establishing the connection, and ending the session by terminating or transferring the connection. Figure 1 shows how SIP session is set up and terminated. In addition to telephony sessions, SIP can set up instant messaging, gaming, or streaming video sessions.

![Figure 1: SIP gateway-to-SIP gateway call](image)

Vendors, large and small, of VoIP products are adopting SIP. Microsoft has built it into the Windows XP operating system and bases its instant messenger program on it. IBM has committed to SIP for all future voice and video communications products. Carriers and ISPs are also adopting SIP.
SIP offers several strong points.

**Scalability.** SIP is a lightweight protocol, using few packets to establish a call.

**Versatility.** Intelligence is more widely distributed among network elements, such as VoIP endpoints, gateways, and application servers, resulting in less system impact when new features and functions are added.

**Support for any media type.** SIP supports instant messaging, video, and voice.

**Support for mobility.** Users can register all their devices—cell phone, office phone, PDA, home phone with a centralized location registrar. A SIP proxy server can look up and contact all the registered devices sequentially or simultaneously.

**Easy to manage and troubleshoot.** All SIP messages are formatted as text using http-like syntax. Because SIP is an IETF standard, it provides a dependable, open foundation for application developers and stimulates competition and innovation in VoIP solutions.

VolP and security vulnerabilities

Corporate VoIP is gaining momentum, and SIP is becoming a dominant protocol for VoIP products. However, a top concern holding companies back from broad VoIP deployment is security.

A VoIP infrastructure adds IP-PBXs, gateways, servers (proxy, registrar, and locator servers), and IP phones to the IP backbone network. Each VoIP element, whether it is an embedded system or an off-the-shelf server running a commercialized operating system, is addressable and accessible over the data network like any computer. Each contains a processor running software that can be attacked or used as a launching point for deeper attacks.

Attacks on data communications can come through the IP voice infrastructure and vice versa. Denial of service attacks targeting weak VoIP elements could flood the network with voice traffic, degrading network performance or shutting down both voice and data communications. Hacked-into gateways might be used to make unauthorized free telephone calls. Unprotected voice communications might be intercepted and stolen or corrupted. Unswitched voice packets can be sniffed out and listened to in real time. PC-based soft phones are vulnerable to eavesdropping if the PC is infected with a Trojan horse that snoops into LAN traffic. Voicemail can be redirected to “ghost” mailboxes: inserting the IP address of the ghost mailbox in the SDP can cause the RTP connection to be opened toward it.

In short, VoIP opens voice communications to the same kinds of security threats that imperil data communications.

VoIP presents certain specific security challenges. A VoIP phone call has two parts—the exchanged signaling messages that set up the call and the media stream, which carries the voice communication. Signaling and media pathways are separate, requiring two logical connections. SIP signaling passes through proxy servers. Once connections are established through the proxy server, media transmission takes place directly between the initiator and target. Both streams—signaling and media—need to be inspected by a firewall as they cross security boundaries in order to enforce security policies. And since SIP is a new application protocol, a firewall must understand the protocol sufficiently to enforce these policies.
The signaling path. The signaling path is vulnerable to impersonators trying to steal or disrupt phone service and to eavesdroppers looking for account codes to override toll call restrictions. The signaling path uses UDP/TCP port 5060. The firewall must be able to disassemble and inspect the packets on the signaling stream and dynamically open the port to let them into the network. A firewall that is not VoIP-protocol aware must be manually configured to leave port 5060 open, creating a hole for attacks against elements actively listening for activity on this port.

The media stream. The media stream bypasses security enforcement points located at proxy servers and flows directly between the endpoints. Common threats to the voice stream include eavesdropping and transport disruption. This stream can be encoded and transmitted via a virtual private network. However, the stream still needs to traverse a firewall that can dynamically allocate ports to the media streams. A complicating issue is that the ports used by the endpoints are dynamically selected by the endpoints themselves during call setup signaling. Thus, the firewall needs to read inside the signaling packets to discover the ports selected in order to enable the two endpoints to send media packets to each other.

NAT and VoIP. Network Address Translation (NAT) poses a special problem for VoIP. NAT maps internal unroutable IP addresses to external routable IP addresses. Businesses use NAT to connect many devices to the Internet through one IP address or to hide internal IP addresses from the outside world. Typically, NAT looks for IP addresses in packets at the network layer (layer 3) and then allocates a port and patches the packet with a substitute address. However, VoIP protocols embeds IP addresses at the session layer, (layer 5), so NAT won’t work. Callers from outside the network won’t be able to find users with dynamic and non-routable IP addresses. Callers going out of the network can connect and transmit media but can’t receive.

Any VoIP implementation running an environment that uses firewalls for security must address these issues.

The secure VoIP-enabled enterprise

Pingtel and Check Point bring secure VoIP to enterprises that want to reduce network and communications costs and improve efficiency and productivity.

Pingtel: VoIP-enabling the enterprise

Pingtel, a Check Point OPSEC™ (Open Platform for Security) certified partner, is a leading provider of open source SIP based software IP telephony. The Pingtel solution includes the following elements:

- **SIPxchange.** This software suite turns industry-standard, general-purpose servers into full-featured IP-PBXs. This open source solution provides call control and intelligent routing, including SIP proxy, redirect, registrar and AAA (authentication, authorization, and accounting) server functions. It provides media services such as voice mail, auto-attendant, and interactive voice response. And it provides centralized system configuration and management for all the diverse network elements.

- **SIP phones.** The programmable xpressa desk phone is an easily extensible platform for voice solutions using Java. The Instant xpressa open source soft phone for Windows enables a laptop to act as a full-function office phone while retaining all the Java extensibility of xpressa desk phones.

A typical SIPxchange implementation also includes:

- **IP-to-PSTN gateways for connecting the VoIP LAN traffic to a public telephone network.**
- **Analog station adapters for connecting SIPxchange to traditional PSTN phones, fax machines, modems, and other analog devices.**
A SIPxchange VoIP system provides value in several ways.

**Secured by open source.** SIPxchange brings the big benefits of open source to one of the most important parts of an enterprise — its phone system. With open source, nothing is hidden — no hidden security swamps, no hidden interfaces that might expose enterprise networks to unanticipated security threats. Customers can gain a detailed understanding of how a system works and how they can secure their solution. Open source permits rapid adaptation to changing security conditions in businesses, networks, and systems to which it is connected. Open source communities have proven time and again to be able to respond more quickly to new security threats or attacks than vendors of proprietary solutions are able to respond. The freedom of open source brings fast improvements in software security and quality, as well as accelerating the pace of innovation.

**Low entry cost.** SIPxchange software runs on low-cost commodity hardware.

**Scalability.** SIPxchange scales economically from one small site to multiple large sites by adding more IP phones, gateways, and servers. No forklift swaps of large frames filled with switching cards. A SIPxchange server or gateway can serve multiple offices or act as a backup or load-balancer in an environment with multiple SIPxchanges.

**Flexibility and choice.** SIPxchange integrates easily with TDM networks enabling customers to migrate to IP telephony at their own pace. Since all signaling uses SIP exclusively, customers can choose the best component products at the right price, and preserve their investment in these components for years to come without fear of obsolescence or vendor lock-in.

**Manageability.** SIPxchange components and functions distributed across the network are centrally managed from an intuitive browser interface. And monitoring of all functional components can be performed using industry-standard SNMP consoles.

**Productivity.** SIPxchange supports a wide range of productivity enhancing applications, such as LDAP corporate phone books with click-to-dial and contact pop, personalized computer-telephone integration, and dynamic phone-Web conferencing. Users can retrieve voice messages from any convenient interface to the system—IP phones, PSTN phones, email accounts, PDAs, and Web browsers.

**Check Point: Securing the VoIP-enabled enterprise**

Check Point provides the security that allows enterprises to deploy the Pingtel SIPxchange IP telephony solution with confidence. Check Point’s VPN-1® Pro™ is a tightly integrated software solution that combines sophisticated VPN technology with market-leading FireWall-1® products that leverage Stateful Inspection and Application Intelligence technologies. The cornerstone of Check Point’s Intelligent Security Solutions, VPN-1 Pro with Application Intelligence protects against all common threats to VoIP traffic, which can lead to the compromise of sensitive, business critical information or costly disruption of business. Theses threats include:

- **Call hijacking.** Calls intended for one receiver are redirected to someone else. For example, when an SIP agent sends an INVITE message to set up a call, the attacker sends a 3xy redirection message indicating that the called party has moved and will provide its own forwarding address. At best hijacked calls are a disruptive nuisance; at worst they can steal valuable sensitive information.

- **Fooled billing.** For example, fake BYE and OK messages exchanged over the SIP signaling path appear to terminate a call and billing is stopped, while the media path actually remains open. Undetected, these attacks can rob an organization of considerable revenue.
Denial of Service (DoS) attacks. The attacker mimics caller identities and cancels pending SIP INVITE requests. The result: an organization’s phone system is effectively shut down.

VPN-1 Pro provides security in complex environments of mixed VoIP protocols. SIP and H.323 protocols may be used together with appropriate gateways, and VPN-1 Pro supports both equally. VPN-1 Pro inspects VoIP control signals passing through the enforcement point to prevent call hijacking, fooled billing, and DoS attacks. Using information derived from the control signals, VPN-1 Pro provides this protection through:

- Dynamic management of RTP (media) sessions
- Analysis and enforcement of message states
- Verification of the existence and correctness of call parameters
- Maintenance of the call state for each call
- Enforcement of handover domains

VPN-1 Pro overcomes a significant limitation of other firewalls in a VoIP environment. It is the only firewall solution that accepts and allows inbound calls to the local network for both dynamic and non-routable IP addresses, handling both signaling and media traffic in real time.

The next section highlights Check Point advantages for SIP VoIP implementations.

Check Point advantages in the VoIP-enabled enterprise

OPSEC certification is the customers’ assurance of the compatibility and integration of the Pingtel–Check Point solution. This section explains how VPN-1 Pro secures enterprises implementing SIP.

Support for all SIP elements

VPN-1 Pro supports all SIP architectural elements in the security rule base. These elements include the following.

- **SIP Terminal (IP Phone).** VPN-1 Pro supports real-time, two-way communication between SIP entities. It supports both signaling and media. In SIP, only IP-enabled phones can be used. IP phones are defined in SmartDashboard™, usually as a network of IP phones. There is normally no need to define network objects for individual IP phones within the firewall boundaries.

- **Proxy Server.** This server manages a number of IP phones. It contacts one or more clients or next-hop servers and passes the call request further.

- **Redirect Server.** This server converts SIP URL address into zero or more new addresses, and returns those addresses to the client. It does this before the VoIP connection begins. It does not initiate requests or accept calls.

- **Registrar.** This server accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and may offer location services.

- **Authentication proxy server.** This server performs authentication, authorization, and accounting functions. During the SIP INVITE message exchange, the Authentication Proxy inserts a “Record-Route,” which forces all future messages relating to the session to be sent back through the Authentication Proxy.
The Proxy Server, Redirect Server and Registrar are signal routing devices. Signal routing devices are defined in SmartDashboard as host nodes that manage a VoIP Domain. Signal routing locations can be limited by defining a VoIP Domain. A VoIP Domain will typically be a network or group of networks. If the signal routing devices have the same IP address, only one VoIP Domain need be defined, otherwise, a VoIP Domain must be defined for each one.

SIP conversations are allowed by creating rules to let SIP control signals through the VPN-1 Pro gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. VPN-1 Pro derives this information from the signaling. Given a particular VoIP signaling rule, VPN-1 Pro automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.

Security for all SIP topologies
VPN-1 Pro secures all SIP topologies. The signal routing devices can be on the protected or the unprotected side of the VPN-1 Pro gateway, or in a DMZ. Typical SIP topologies include

- Peer-to-peer, where both signaling and media pass endpoint to endpoint.
- One or more signal routing devices, where signaling passes through one or more proxy servers, redirect servers, or registrar servers. Once the call has been set up, the media passes peer to peer.

Restriction of signal routing locations using VoIP Domains
VPN-1 Pro makes it possible to specify the IP addresses of the endpoints that are allowed to take part in VoIP calls. This is done by defining a VoIP Domain, which is the group of endpoints that the signal routing device is allowed to manage. The VoIP Domain also controls the allowed direction of the call.

The signal routing device (SIPxchange) is allowed to route calls only to the endpoints in its VoIP Domain. For example, in figure 2, if A and B are in the VoIP domain of the signal routing device C, VPN-1 Pro ensures that A sends its media streams only to B, by ensuring that the address of B that the signal routing device C provides to A (step 3 in figure 1), is in the VoIP Domain. This prevents unwanted callers getting through the firewall.

![Figure 2: VoIP Security by VPN-1 Pro](image)
Control of signaling and media connections

SIP control signals always pass through the VPN-1/FireWall-1 enforcement point. VPN-1/FireWall-1 is therefore able to secure the call by opening ports only for those endpoints negotiated during the signaling. It also keeps those ports open only for as long as required and closes them as soon as the call ends, without waiting for a timeout. VPN-1/FireWall-1 also enforces the order and direction of the packets.

If both endpoints are on the same side of the VPN-1/FireWall-1 enforcement point but the signal routing device is on the other side, VPN-1/FireWall-1 will be aware of this fact, and will not open any ports for the media stream.

Application Intelligence for SIP

The critical need for providing a network and application level protection is accomplished through Check Point Application Intelligence. Using INSPECT, the most adaptive and intelligent inspection technology, VPN-1 Pro integrates both network-level and application-level protection and provides the highest level of security, with access control, attack protection, content security, authentication, and integrated Network Address Translation (NAT). VPN-1 Pro leverages SMART Management, enabling you to intelligently manage security infrastructure with maximum efficiency.

Leveraging its intelligent security capabilities VPN-1 Pro restricts signal routing locations and controls signaling and data connections. For SIP, VPN-1 Pro Application Intelligence™ ensures packets conform to RFC 3261 for SIP over UDP/IP and inspects SIP-based Instant Messaging protocols. It protects against Denial of Service (DoS) attacks and against penetration attempts such as connection hijacking and connection manipulation.

VPN-1 Pro validates the expected usage of the SIP protocol. For example, if an end-of-call message comes immediately after the start of the call, the call will be denied because this behavior is characteristic of a DoS attack.

Application level checks include:

- Checks for binaries and illegal characters in the packets
- Strict RFC enforcement for header fields
- Header fields lengthen restrictions
- Removal of unknown media types
- Removal of characters that should not be used for addresses

Application Intelligence checks can be granularly turned on or off.

Synchronizing of user information

The user IP phone sends SIP messages to the Redirect Server in order to register itself on the network. Once a phone is registered, it can make calls. These SIP messages cross VPN-1/FireWall-1, which reads them. The VoIP user databases on VPN-1/FireWall-1 and the Redirect Server are, therefore, always synchronized with each other.

Registration makes it possible to initiate calls from outside the VPN-1/FireWall-1 enforcement point to phones whose addresses are translated using Hide NAT. This case solves the problem of allowing incoming calls to a dynamically allocated IP phones that are using non routable IP addresses in the local network. If the VPN-1/FireWall-1 machine is rebooted, the VoIP user database is deleted.
NAT Support for SIP

All VPN-1/FireWall-1 features can be used with SIP, with the following restrictions regarding Network Address Translation (NAT):

- Static NAT can be used in both automatic and manual NAT rules.
- Hide NAT can be used on endpoints that make outgoing calls.
- Hide NAT can be used on endpoints that allow incoming calls. (This is possible because the phone number in the incoming call is associated with the real telephone number by means of the database on the Redirect Server). However, Manual Hide NAT rules cannot be used with Hide NAT for incoming calls. For security reasons, when using Hide NAT for incoming calls, the Destination of the VoIP call in the appropriate rule in the Security Rule Base cannot be Any.

- Where both endpoints are on the trusted side of the VPN-1/FireWall-1 enforcement point, calls cannot be made from the same source to two endpoints, where one endpoint is NATed (either Static or Hide) and the other is not. The same firewall can not NAT both the source of the connection and the destination of the connection. There are no restrictions when a NATed IP phone is calling a phone that is behind another NAT device or vice versa

- NAT on a Proxy, Redirect Server or Registrar is not supported.
- Bidirectional NAT of VoIP calls is not supported.
Security Buyer’s Checklist

A VoIP gateway security solution should have the following features. Check Point has them all.

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>CHECK POINT VPN-1</th>
<th>BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GENERAL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support RFC2543bis05</td>
<td>YES</td>
<td>Standard compliance with different VoIP vendors and systems</td>
</tr>
<tr>
<td>Support RFC-3261</td>
<td>YES</td>
<td>Standard compliance with different VoIP vendors and systems</td>
</tr>
<tr>
<td>Rule-based SIP support with full GUI</td>
<td>YES</td>
<td>Ease of use</td>
</tr>
<tr>
<td>Integrated High Availability and load sharing</td>
<td>YES</td>
<td>High uptime and performance. Note: All Check Point products can be clustered with HA or load sharing</td>
</tr>
<tr>
<td>IP de-fragmentation support</td>
<td>YES</td>
<td>Support fragmented traffic on any IP port, including non standard ports in order to meet any networking scenario and mitigate DoS attacks</td>
</tr>
<tr>
<td><strong>SECURITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parse SIP header to determine media type and associated media port</td>
<td>YES</td>
<td>Define security rules and actions based on media type</td>
</tr>
<tr>
<td>Ability to open RTP/RTCP ports, as indicated in SDP header, and monitor connection states</td>
<td>YES</td>
<td>Track the state of each call in order to mitigate DoS and kidnapping attacks, including day-zero attacks</td>
</tr>
<tr>
<td>The SIP service always enforces the control-data connection relationship</td>
<td>YES</td>
<td>Ensures the security and integrity of billing processes. The SIP service will not allow one type of connection to exist independently of the other</td>
</tr>
<tr>
<td>Validate SIP protocol call flow according to the RFC, and drop out of state SIP messages</td>
<td>YES</td>
<td>Track the state of each call in order to mitigate DoS and kidnapping attacks, including day-zero attacks</td>
</tr>
<tr>
<td>Ability to define SIP Handover Domain object, protocols to allow non-VoIP communication</td>
<td>YES</td>
<td>Disable the possibility to abuse the redirect capabilities of the signaling</td>
</tr>
<tr>
<td>Handle extensive SIP protocol feature set: re-invite messages (with the ability to limit the re-invite messages), hold, and Call conference</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td><strong>NAT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hide and static NAT for outgoing calls</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Hide and static NAT for incoming calls</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td><strong>LOGGING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call logs: Each log contain the “from” and “to” SIP URLs and phone numbers</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Registration logs, contain the SIP URLs</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Reject logs with detailed description</td>
<td>YES</td>
<td>Detailed forensics</td>
</tr>
<tr>
<td>Special SIP logs all the registration and calls are logged, including the SIP URI's</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td><strong>ADDITIONAL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated QoS</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>
Implementation scenarios

Organizations can deploy the secure Pingtel–Check Point VoIP solution in several ways without changing their network infrastructure or abandoning their investments in traditional PBX equipment.

Toll Bypass

Many VoIP implementations start as toll bypass solutions because the risk and cost is low and return on investment is rapid through substantially lower telecommunications costs. In this scenario, a distributed organization with a high volume of toll traffic between multiple offices routes voice communications over its existing IP WAN or LAN instead of tie lines. The company continues to use its traditional PBXs and phones, and users don’t change their behavior.

SIP gateways on the network front the TDM PBXs at the various locations and convert voice signaling and transport to IP format. A SIPxchange IP-PBX manages dial plans and routes the calls for the entire organization. Overflow calls can be directed to the PSTN. Organizations starting with a toll bypass solution lay the foundation for VoIP migration without having to replace a significant investment in traditional telecommunications.

- Immediate benefit— eliminates tie line/voice VPN costs
- Simple — no change in user behavior
- Low cost, low risk — no forklift upgrades
- Baseline for network migration
Typical security configuration: Sites may vary in size from very large to small branch offices.

<table>
<thead>
<tr>
<th>WAN characteristics</th>
<th>Redundancy</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet based</td>
<td>Sites require firewall redundancy. There is no IP LAN/WAN redundancy.</td>
<td>Use VPN to tunnel and secure traffic between different offices. Mission critical sites will install clustered firewalls in high-availability (HA) configuration. Sites with more than 40,000 concurrent VoIP calls should install the firewalls in load sharing mode. Recommended: add firewalls with FloodGate-1® to define QoS.</td>
</tr>
<tr>
<td>Leased lines</td>
<td>Sites require firewall redundancy. There is no IP LAN/WAN redundancy.</td>
<td>If no VPN is needed, a centralized firewall can be installed in front of the SIP exchange gateway. Mission critical sites will install clustered firewalls in HA configuration. Sites with more than 40,000 concurrent VoIP calls should install the firewalls in load sharing mode. Recommended: add firewalls with FloodGate-1 to define QoS.</td>
</tr>
<tr>
<td>Internet and leased</td>
<td>All sites require firewall redundancy. Internet and leased lines provide mutual backup.</td>
<td>Use VPN to tunnel and secure traffic between different offices. VPN-1 will route traffic via the VPN tunnel or leased line in case of fail over. Mission critical sites will install clustered firewalls in HA configuration. Sites with more than 40,000 concurrent VoIP calls should install the firewalls in load sharing mode. Recommended: add firewalls with FloodGate-1 to define QoS.</td>
</tr>
</tbody>
</table>
Branch Office Extension

Many organizations transition to IP telephony by implementing it in branch offices first. The Pingtel-Check Point solution gives organizations with geographically dispersed offices tremendous flexibility while eliminating long-distance charges for intracompany phone calls.

The architecture of the Pingtel solution enables intelligence and functionality to be distributed where it is needed and managed centrally, saving hardware, software, and operations costs. A SIPxchange in one location can do the call routing for small offices, where the number of users doesn’t justify the cost of a dedicated IP-PBX. In this way, new offices can be deployed quickly and economically by simply plugging SIP phones into the WAN. And the entire organization functions more efficiently because users everywhere have access to the same VoIP enabled services for voicemail, unified messaging, conferencing, and more.

Typical security configuration: Small branch offices can be connected to the Internet using different methods: cable modems, leased lines, or ADSL. Small sites can use a single firewall and VPN device to connect to the headquarters via VPN and tunnel VoIP traffic. Other characteristics are the same as in the table for the preceding scenario.
Mobile and remote workers
In this scenario, SIPxchange provides PBX functionality and connections to the TDM network for mobile and remotely located workers. Employees at home or on the road can be reached by their office number wherever they are; they can use the corporate LAN/WAN to make free calls; and they have the full functionality of their office voice and data system. The only requirements are a broadband Internet connection, a SIP phone, and a cost-effective SIPxchange system secured by Check Point.

Typical security configuration: Home users (using a soft phone installed on one desktop PC) can use VPN-1 SecureClient™, a centrally managed, integrated VPN and personal firewall client that can also check for proper configurations such as latest virus definition files and OS patches. Small branch offices can be connected to the Internet using different methods, such as cable modems, leased lines or ADSL. These small sites can use an easy to deploy Check Point VPN-1 Edge Appliance to connect to the headquarters via VPN and tunnel VoIP traffic while providing the highest level of security in the industry with Check Point’s patented Stateful Inspection technology.

Immediate benefit — saves $80 per worker/month, <3 month payback
Enhances service to remote workers, corporate telephony is mobile
Low cost — $220 per user
Low risk — integrates with TDM
VoIP returns without sacrificing flexibility
Conclusion

Pingtel and Check Point offer an affordable, secure solution for VoIP-enabling the enterprise.

Pingtel’s market advantage is an affordable, open source software IP telephony solution entirely based on SIP. The Check Point advantage is firewall technology that is completely aware of Internet telephony protocols, including SIP. The Pingtel–Check Point solution integrates into an organization’s existing network and telephony infrastructure, enabling a secure move to VoIP so that companies can realize lower telecommunications and network operating costs while improving efficiency and productivity with voice-enabled applications.

About Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company’s Zone Labs (www.zonelabs.com) division is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry’s framework and alliance for integration and interoperability with “best-of-breed” solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,300 Check Point partners in 92 countries.