

# Security and Interoperability Issues to Consider When Enabling SIP Services for the Enterprise

Technology Brief

Voice over IP (VoIP) adoption has flourished over the past decade, allowing companies to streamline their voice and data networks, drive efficiency, and enable new applications with great success.

In the past, VoIP deployments in the enterprise have primarily focused on IP PBX, unified communications, and VoIP networking across private IP networks. Now many enterprise IT departments are looking to SIP trunking and hosted VoIP services to yield additional cost savings and efficiency benefits.

## What Is SIP Trunking?

SIP trunking is a PSTN replacement that connects external voice networks to internal ones in a flexible, cost-effective way that uses broadband IP and VoIP technology. Having proven its worth, SIP trunking now enjoys broad availability from service providers in many regions, including many incumbent PSTN providers.

If you are thinking about deploying a SIP trunking service, there are several issues that you may want to consider: secure firewall traversal, SIP interoperability and security, VoIP service demarcation, legacy PBX integration, and Fax over IP (FoIP) support. This technology brief discusses these topics and introduces the Dialogic® BorderNet™ 500 Enterprise Session Border Controller (ESBC) as a network edge product that can help you deliver SIP trunking services smoothly and efficiently in your enterprise environment.

Figure 1 illustrates an example of a placement of a BorderNet 500 ESBC in an enterprise network.

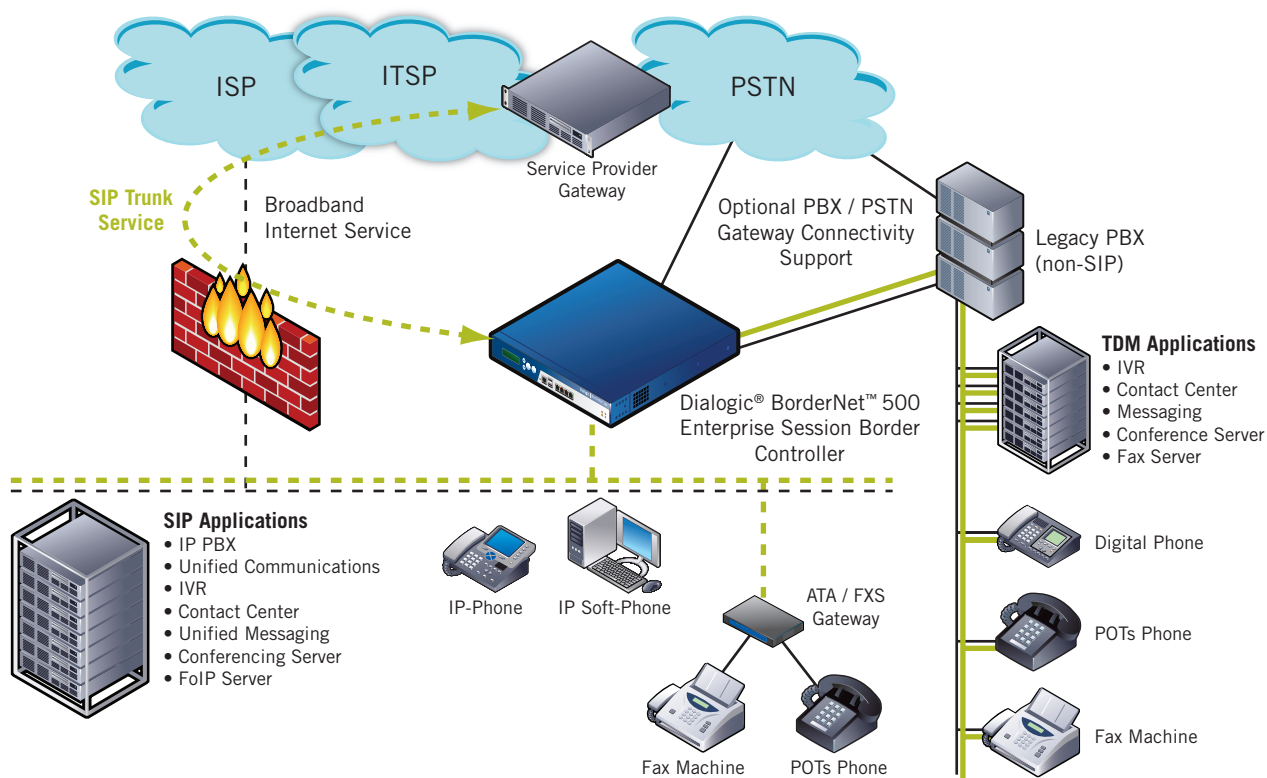


Figure 1. Dialogic® BorderNet™ 500 Enterprise Session Border Controller in the Enterprise Network

# Security and Interoperability Issues to Consider When Enabling SIP Services for the Enterprise

## Secure Firewall Traversal

Typical data network firewall implementations aim to allow public internet data traffic to securely traverse the enterprise network edge. They normally do not support the SIP protocol and consider inbound telephone calls using the SIP protocol that seek a particular IP endpoint or address within the enterprise network domain as unexpected external requests. In fact, data firewalls are specifically designed to protect against such external requests, which are seen as an attack and a danger to the internal network.

The BorderNet 500 ESBC works seamlessly with existing firewalls on the customer premise to allow authenticated SIP traffic through the enterprise firewall at the network edge. While traditional firewalls normally block SIP traffic — including mission-critical applications such as VoIP — the 500 ESBC resolves this issue by working with existing security solutions to permit authenticated traffic from SIP trunks to flow freely into an enterprise.

## SIP Interoperability

SIP protocol implementations from various service providers and customer premise equipment vendors usually have subtle differences, and SIP components and extensions supported by one vendor may not be supported by another.

The BorderNet 500 ESBC can resolve SIP interoperability issues in a number of ways. First, the 500 ESBC has been tested for interoperability with IP-PBXs from leading vendors such as Alcatel, Avaya, Cisco, Mitel, NEC, Nortel, and Siemens. In addition, its ESBC function has been tested with service providers such as AT&T, Level 3, Broadvox, and many others.

The BorderNet 500 ESBC is also equipped with a SIP interoperability toolkit that allows the customization of SIP protocol messages through header manipulation, advanced routing capabilities, and a Back-to-Back User Agent (B2BUA), which can be used to rapidly enable connectivity between new services and premise endpoints.

## SIP Security

Data network firewall implementations typically protect the enterprise from IP data threats originating on the public internet. They are not designed to secure the corporate network from threats that use the SIP communications protocol.

To supplement firewall security and protect the enterprise from SIP communications threats, the BorderNet 500 ESBC includes a wide variety of SIP security features, such as B2BUA network elements, deep packet inspection, NAT traversal, SRTP, TLS, and HTTPS. These features can provide a secure border for the premise network edge, nullifying threats from denial of service, theft of service, SPAM, and SPIT attacks, and addressing additional SIP security concerns.

## VoIP Service Demarcation

When the PSTN is in use, a demarcation point (an actual physical location) exists on the enterprise premise at which the service provider terminates its trunking service. On one side, the enterprise owns and maintains services and equipment while on the other, the service provider takes that responsibility.

Since no clear physical demarcation point normally exists when SIP trunking is used, The BorderNet 500 ESBC can supply a logical service termination point along with detailed call quality statistics for managing service quality.

## Legacy PBX Integration

While many enterprise PBX systems are now based on the SIP protocol, a substantial number of non-SIP-based hybrid PBXs, IP-PBXs, and TDM PBXs are still in use. Many of these legacy PBX systems either cannot handle the SIP protocol, or a very expensive upgrade may be required to enable SIP trunking service.

The BorderNet 500 ESBC is available with SIP-to-TDM gateway subsystems capable of converting SIP trunks into T1/E1, PRI, CAS, or ISDN BRI trunk groups to create an interface with legacy PBX systems. The TDM interfaces can also be used for connectivity to the PSTN, either for failover or for general call routing.

# Security and Interoperability Issues to Consider When Enabling SIP Services for the Enterprise

Technology Brief

## Fax over IP Support

Fax is often overlooked when a SIP trunk deployment is planned, and the traditional fax transmission protocol (T.30) has proven unreliable when sent over packet networks. Although T.30 fax pass-through techniques improve reliability, better results can be achieved by using the FoIP T.38 protocol across an IP network, including an Internet Telephony Service Provider (ITSP) network.

The BorderNet 500 ESBC supports both standard T.30 fax and T.38 FoIP gateway capabilities, and can handle up to 120 channels of simultaneous fax traffic. The gateways also support high V.34 transmission rates (33.6 kbps) for both T.30 and T.38 protocols, which significantly reduces the time needed to send a fax with the older and considerably slower V.17 (14.4 kbps) fax transmission technique.

## For More Information

If you are planning a SIP trunking service deployment and would like to learn more about the capabilities of the BorderNet 500 ESBC, visit the [product information page](#) on the Dialogic website or [contact](#) your local Dialogic sales representative.



[www.dialogic.com](http://www.dialogic.com)

**Dialogic Inc.**  
1504 McCarthy Boulevard  
Milpitas, CA 95035-7405  
USA

Dialogic and BorderNet are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at the address provided above. The names of actual companies and products mentioned herein are the trademarks of their respective owners.

Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement their concepts or applications, which licenses may vary from country to country. None of the information provided herein forms part of the specifications of the product(s) and any benefits specified are not guaranteed. No licenses or warranties of any kind are provided hereunder.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.

Dialogic may make changes to specification, product descriptions, and plans at any time, without notice.