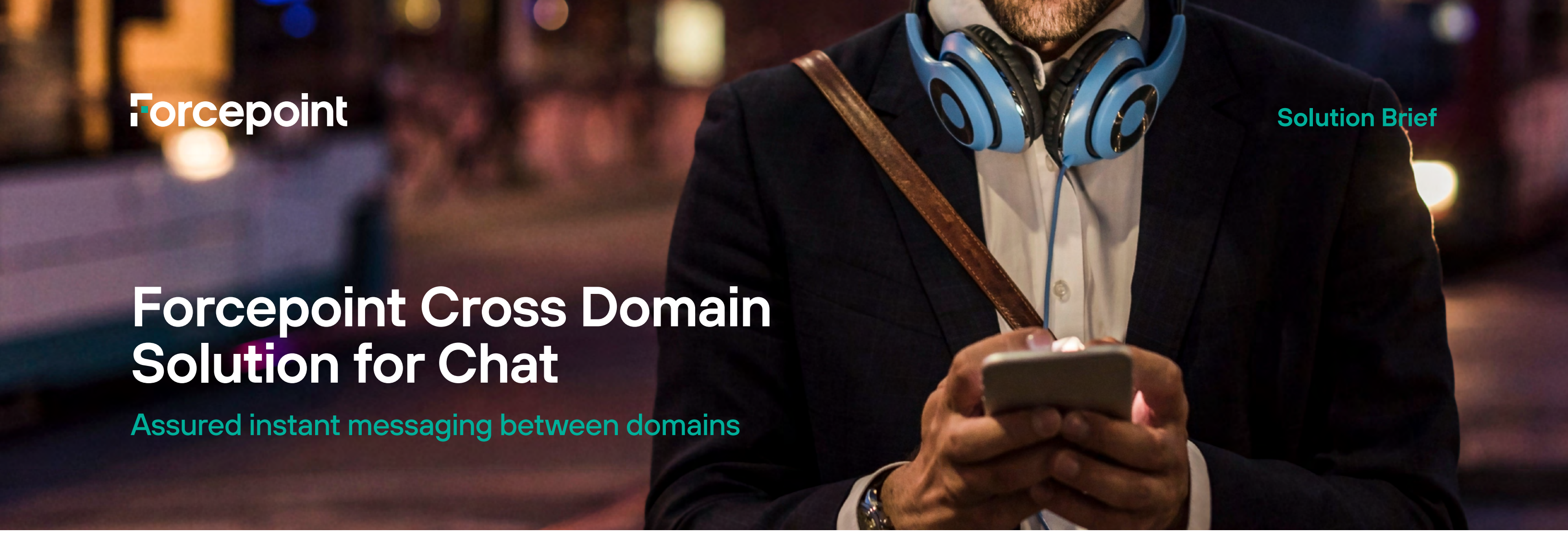

Solution Brief

Forcepoint Cross Domain Solution for Chat

Assured instant messaging between domains

Key Advantages

- High assurance cross domain solution for XMPP chat
- Connect multiple networks and chat domains
- Hardware-enforced verification and flow control
- Transformation that removes malware threats
- Removal of hidden data from chat messages to prevent exportation of sensitive information
- Protection against network protocol and content attacks
- Modular approach using COTS products for a low-risk, low-cost cross domain solution
- Proven technology, deployed and accredited for use between classified networks

Organizations running segregated networks have a need to collaborate with partners. Instant messaging (chat) is a common form of collaboration used particularly in defense with both person-to-person and multi-user chat. Enabling rapid information sharing and decision making without the bandwidth overheads of voice and video.

When instant messaging is enabled between different security domains there are risks of importing malware and leaking sensitive information. In order to protect an organization, but enable chat between domains, a cross domain solution that supports chat protocols is required.

Forcepoint's cross domain solution for chat provides protection against network- and content-borne attacks, including those against the solution itself. To protect particularly targeted networks, software defenses are not enough and hardware-based controls can be employed to enforce restrictions on the flow of data and provide assured independent verification that the information passing between networks is safe.

To ensure sensitive information does not leak out of a network, Forcepoint's cross domain solution verifies that the chat messages are permitted to leave the network, including validation of any security labels and that there are no prohibited words or phrases in the text.

Three Forcepoint technologies combine to provide a cross domain chat solution:

- Zero Trust Content Disarm and Reconstruction (CDR)
- HardSec—iX Appliance
- Chat Proxy

These three technologies provide a high assurance cross domain solution to ensure safe exchange of Extensible Messaging and Presence Protocol (XMPP) instant messaging.

Zero Trust CDR

Zero Trust CDR is an innovative solution to the malware problem. Data can contain hidden malware that is capable of avoiding traditional detection-based security techniques such as anti-virus scanning and sandboxing. Zero Trust CDR is a zero-trust process which removes the threat of malware in content by using a technique called transformation. This involves passing only the business information to the destination, not the data carrying it. Transformation works by first extracting the information into simple data structures, verifying the structures are as expected before building the information back into brand new data to deliver.

For assured instant messaging between domains, Zero Trust CDR is provided by the Forcepoint Information eXchange (iX) appliance.

HardSec—iX Appliance

The verification phase of transformation in Zero Trust CDR can be delivered using a hardware logic device. This sits in the middle of the iX appliance to verify the data as it passes through. Since the data is in simple data structures, the verification can be done in the hardware using programmable gate array (FPGA) chips. The hardware device provides both an independent verification of the transformation process and a hardware assured separation between a trusted and untrusted network.

Hardware enforced verification is provided by the Forcepoint High Speed Guard verifier.

Chat Proxy

The Chat Proxy is a Forcepoint XMPP gateway which enables XMPP data to be sent across the iX appliance and its HSV. The Chat Gateway supports XMPP Server to Server (S2S) protocol and so enables any XMPP-compliant Chat Server to communicate with one or more Chat Servers in an assured way.

The Chat Proxy also enforces policy to ensure sensitive data is not leaked from the protected network. Policy enforcement includes security label and dirty word checking.

Solution Architecture

A high-assurance cross domain chat solution is built using a Chat Proxy on each connected network, with an iX appliance providing connectivity between the Chat Proxy servers. The Chat Proxy connects to any XMPP-compliant Chat Server using XMPP S2S protocol and to an iX appliance using HTTPS. This architecture enables person-to-person and multi-user chat across domains.

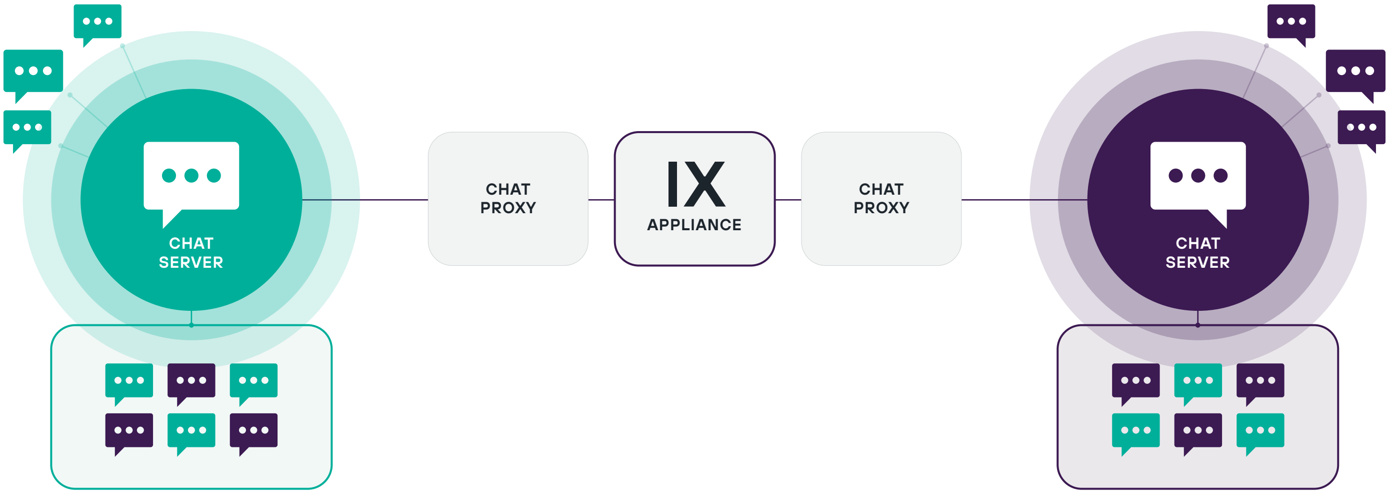

Figure 1: A high-assurance cross domain solution for multi-user and person-to-person chat

The solution can be used to connect multiple external chat servers to chat servers on a protected network. An iX appliance / Chat Proxy is needed for each external network that requires assured separation from the other connected networks.

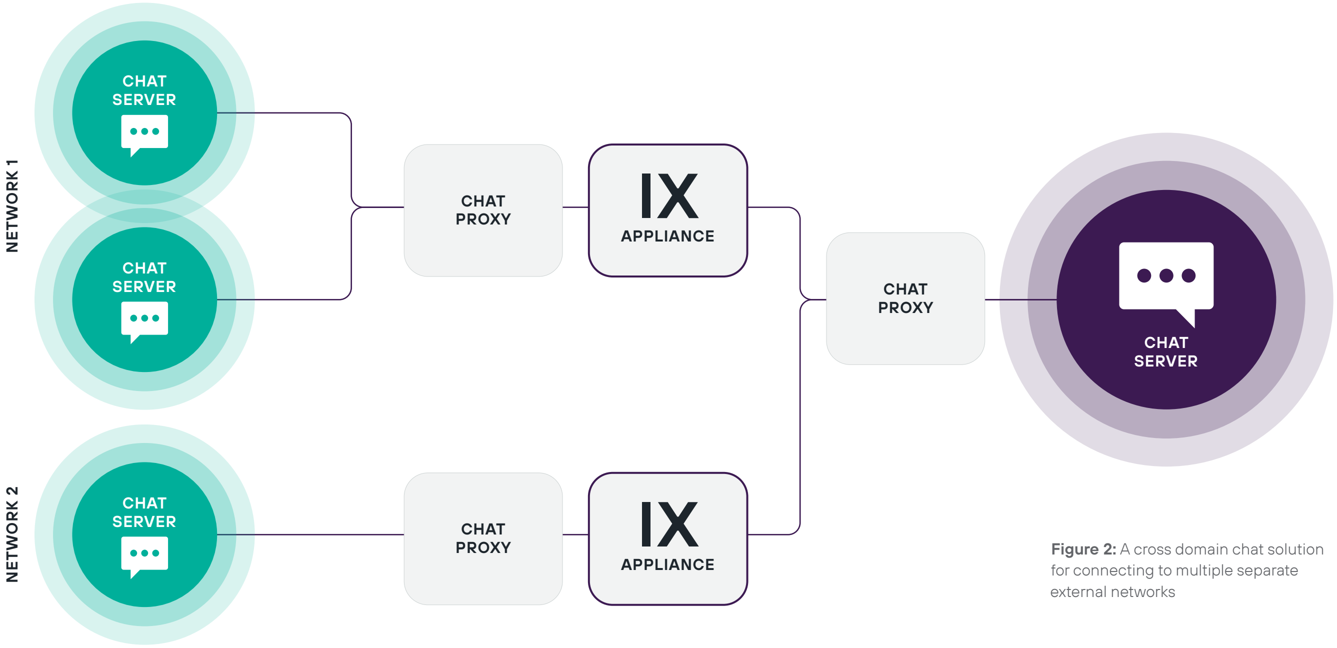

Figure 2: A cross domain chat solution for connecting to multiple separate external networks

Features

- Cross domain person-to-person chat
- Cross domain user discovery
- Controlled presence sharing
- Cross Domain Multi-User Chat (MUC)
- Cross Domain MUC room discovery
- Application-specific message length and content constraints
- Security label validation
- Dirty word searching
- Hardware-assured network separation
- Threat removal using transformation
- Hardware-enforced verification using FPGAs

Build a Winning Solution

Make sure that everything runs smoothly during and after deployment with Forcepoint Technical Support. Our highly skilled Solutions team have a wealth of expertise and information at their disposal and can be relied upon to act as a natural extension to your in-house team.

Enjoy Unparalleled Protection

We're on the brink of a technological revolution. In the face of relentless and concerted cyberattacks, organizations are being forced to re-evaluate every aspect of how they acquire, share, and transact digitally.

Defenses based on the detection of known threats are insufficient. Those based solely on software cannot offer adequate protection from targeted attack. What's needed is hardware-enforced threat removal using content transformation.

Zero Trust CDR provides unparalleled protection when transferring data. It ensures all business information is free of content threats.

Learn More

For more information visit **Forcepoint Zero Trust CDR**.

forcepoint.com/contact

[Forcepoint Cross Domain Solution for Chat] 12Apr2022