DEEP SECURE

Cross Domain Solution for Chat

Assured instant messaging between domains

Organisations running segregated networks have a need to collaborate with partners. Instant messaging (chat) is a common form of collaboration used particularly in defence 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 organisation, but enable chat between domains, a cross domain solution that supports chat protocols is required.

Deep Secure'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 defences 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, Deep Secure's cross domain solution verifies that the chat messages are appropriate to leave the network, including validation of any security labels and that there are no prohibited words or phrases in the text.

Key Advantages

- High assurance cross domain solution for XMPP chat
- Connect multiple networks and chat domains
- Hardware enforced verification and flow control
- Removes the threat of malware using transformation
- Removes hidden data from chat messages preventing the export 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

Three Deep Secure technologies combine to provide a cross domain chat solution:

- Threat Removal
- HardSec
- Chat Proxy

These three technologies provide a high assurance cross domain solution to ensure safe exchange of XMPP instant messaging.

Threat Removal

Threat Removal is an innovative solution to the malware problem. Data can contain hidden malware that is capable of avoiding traditional detection-based cyber security techniques such as Anti-Virus scanning and Sandboxing. Threat Removal is a zero-trust process which completely 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.

Threat Removal is provided by the Deep Secure iX Appliance.

HardSec

The verification phase of transformation in Threat Removal 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 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 Deep Secure High Speed Verifier.

Chat Proxy

The Chat Proxy is a Deep Secure XMPP gateway which enables XMPP data to be sent across the iX Appliance and its HSV. The Chat Gateway supports XMPP 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.

The Chat Proxy is provided by the Deep Secure Chat Proxy software installed on a Windows or Linux server.

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 Server to Server (S2S) protocol and to an iX Appliance using HTTPS. This architecture enables person to person and Multi-User chat across domains.

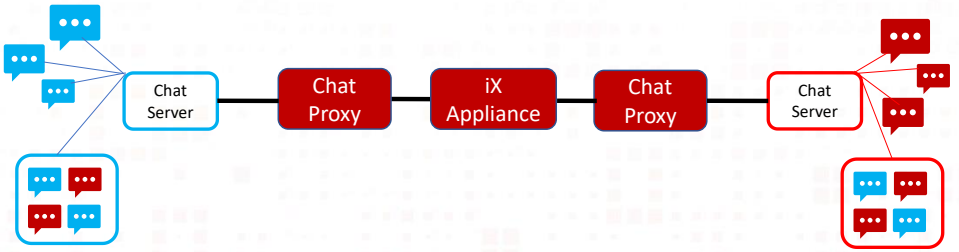

Figure 1: A high assurance cross domain solution for multi-user and person to person chat

The solution can be used to connect to multiple Chat Servers on the protected network and to multiple external networks. An iX Appliance / Chat Proxy is required for each external network that requires assured separation from the other connected networks.

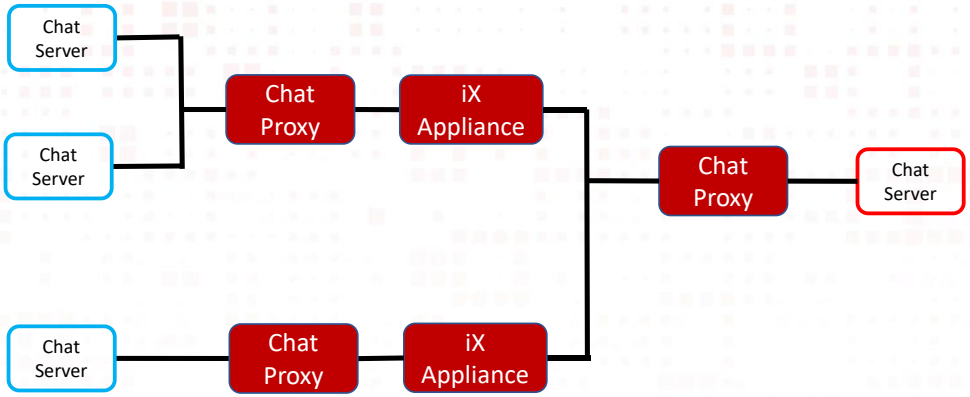

Figure 2: A cross domain chat solution for connecting to multiple separate external networks

Features

- Cross domain person to person chat
- Cross domain user discovery
- Controlled presence sharing
- Cross Domain Multi-User Chat (MUC rooms)
- 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 Deep Secure 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.

Summary: Enjoy Unparalleled Protection

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

Defences 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.

Threat Removal provides unparalleled protection when transferring data. It ensures all business information is 100% content threat free.

Learn More

For more information on how the Cross Domain Solution for Chat uses Deep Secure's products, visit **www.deep-secure.com/products.**