Joint Solution Brief

Bivio Networks & Hypori CSfC Mobility Solution

Bring Your Own Device - Bivio Networks and Hypori deliver a Commercial Solution for Classified capability that permits remote, mobile and tactical users to access controlled unclassified and classified information with BYOD technology.

Operational requirements and current events dictate the need to have constant access to controlled unclassified and classified information, especially for the remote, mobile and tactical user.

The combination of Bivio Networks' CSfC TLS Protected Server and FlowIntelligence™ Application Delivery Controller (ADC) with Hypori Virtual Mobile Infrastructure creates a unique capability that enables users to remotely access the most sensitive information within a controlled unclassified or classified network. The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end-user devices into government enterprise resources. Under the MACP v2.0, communications must be established using an inner and outer tunnel to provide a secure communications path. The Hypori Client v4.2 for iOS®, Android™, and Windows® 10 is eligible to be used as a TLS Software Application Product component in a CSfC solution. The Hypori technology in combination with Bivio Networks CSfC TLS Protected Server - B6310-NC and FlowIntelligence ADC application provides TLS Proxy services and enables remote users with the secure inner TLS tunnel.

Capabilities and Benefits

The joint solution from Bivio Networks and Hypori permits mobile, remote, or tactical end-user devices (laptop, smartphone or tablet) to securely access controlled unclassified or classified information services with a fully encrypted path from the client to the information servers. This enables those clients to access the inner (blue or red) secure network services through a back-end virtual mobile infrastructure. It provides a superior multimedia experience with performance optimized voice, video and data. The solution enforces enterprise identity and access management via Active Directory and Lightweight Directory Access Protocol integration. The enhanced identify authentication is supported by SIPR PKI Tokens with Soft-Certs as well as the DISA Purebred integration.

A requirement for a higher-level of confidentiality, integrity, and assurance (CIA) is needed to ensure the data or systems that users are accessing will not be exposed to undesirable or unauthorize actors. The Bivio -Hypori solution delivers this capability and enables the second of a dual tunnel *(IPSec-Outer and TLS-Inner)* configuration with a transport layer security *(TLS)* inner tunnel that is applied to the user's connection request and secures data traversing the blue or grey-red boundary. The solution supports the highest level of confidentiality through the use of *NSA-approved SuiteB* encryption algorithms. Full end-to-end encryption is applied with the solution to ensure confidentiality is maintained throughout the user's session.

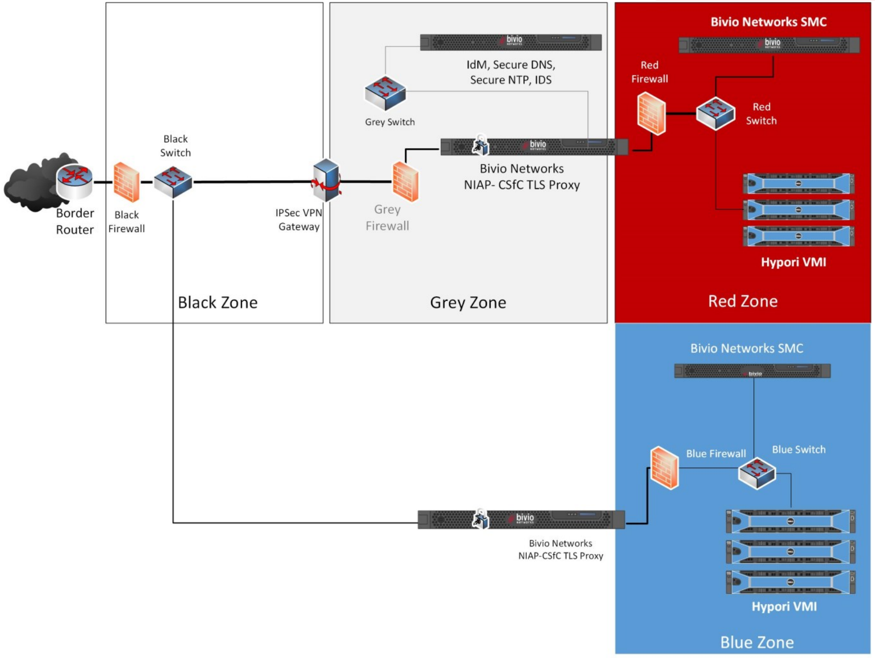

Figure 1 - Bivio and Hypori in a CSfC MACP Architecture

Technical capabilities overview -

- End-users install the Hypori application on their existing Android™, iOS® or Windows® 10 device. This provides a secure and convenient method for accessing application and corporate data. The Hypori application leverages a FIPS 140-2 cryptographic module, implements TLS 1.2 encryption and utilizes PKI credential-based, multi-factor authentication which is NIAP-Common Criteria and Commercial Solutions for Classified certified.

- Launching the Hypori application enables end-users to safely access their applications and corporate data. The Hypori Virtual Device acts as a virtual Android smartphone that can work on any Android, iOS or Windows 10 device. *Zero Trust* - Hypori implements a zero trust approach so no data ever touches the end point device. Hypori sends encrypted pixels to the device and the application transmit touch inputs back via a FIPS 140-2 compliant encrypted VPN to the Hypori VMI server (*shown* in *figure-1)* .

- The Bivio Networks NIAP-CSfC TLS-Protected Server platform (*shown* in *figure-1)* validates user identity based on the PKI credential with the secure services and IdM technology from Bivio Networks in the Grey Management zone.

- The Bivio Networks TLS-Protected server with the FlowIntelligence ADC provides the TLS Proxy services (*shown* in *figure-1)* which implements a NIAP-CSfC validate cryptographic module, enforces TLS 1.2 encryption, creates a secure inner TLS tunnel between the end user device and the TLS Proxy, implements a second secure TLS tunnel between the TLS Proxy and Hypori VMI server for end-to-end confidentiality of the data flow with CSfC-approved SuiteB encryption algorithms.

- The TLS Proxy securely delivers encrypted pixel data to and touch input data from the end user device and the VMI servers in Blue or Red zones.

- Systems Management Center from Bivio Networks collects all log and platform performance data from the TLS Proxy (ies) and Virtual Mobile Infrastructure servers in its zone to provide a unified logging and analysis of the environment.