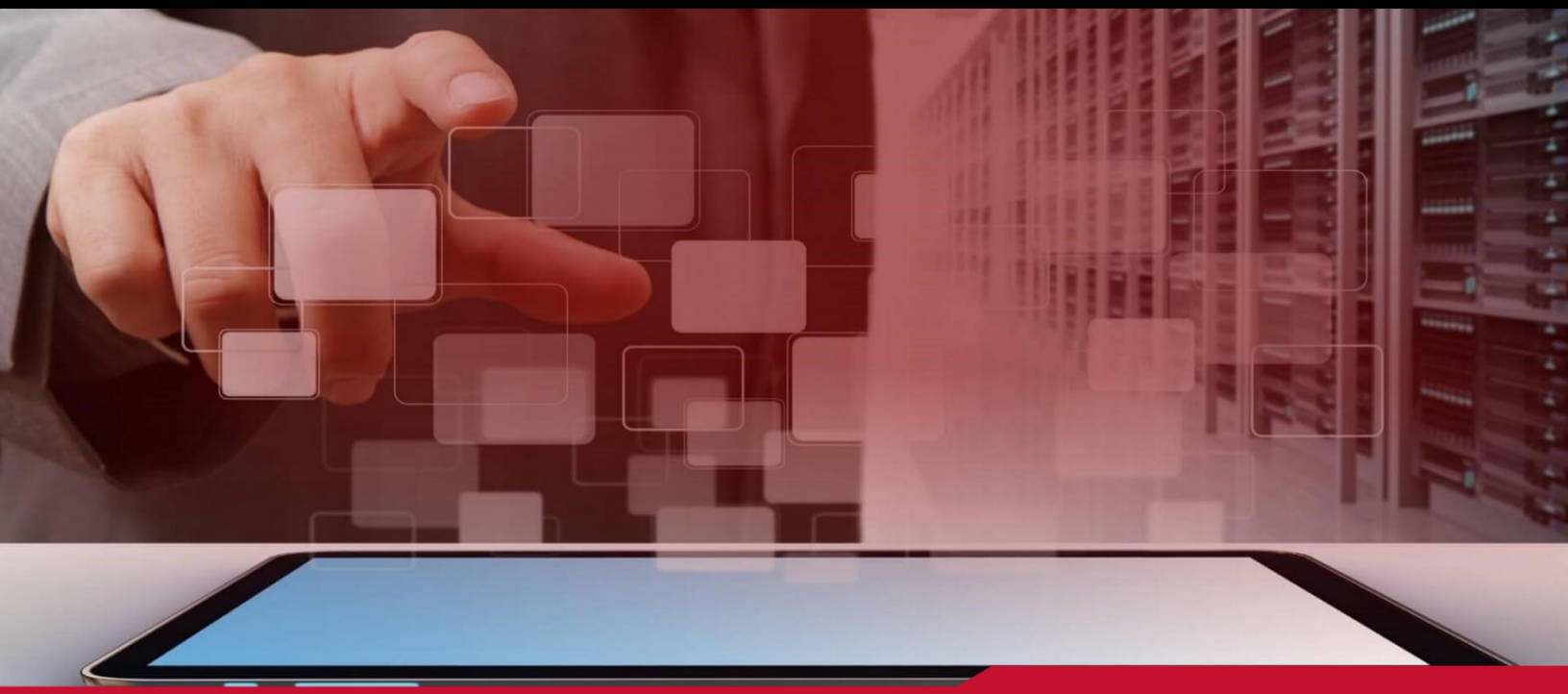
Atlas Cloud Security Proxy

High Assurance TLS and Reverse Proxy Solution

bivio NETWORKS



Key Benefits

- NIAP, FIPS & Commercial Solutions for Classified (CSfC) validated platform capability
- High performance and high assurance TLS or reverse proxy solution
- Web Application Firewall
- Application Delivery Controller (ADC) Load balancer
- High availability capability with active, passive modes
- Certificate-based access control with OCSP and CRL checking
- SSL and TLS session analysis for network security monitoring of the front-end data path
- Integrated analytics of proxy and TLS environment

Secure, Control and Protect

Bivio Networks *Powers Advanced Cyber Operations*™ with Atlas Cloud solutions. Atlas Cloud Security Proxy is a high assurance and high availability proxy solution. This proxy is ideally suited to secure, control and protect data in-transit as well as the information technology assets that provides that data. The Cloud Security Proxy is designed for enterprise, cloud and mobile security environments as either a TLS or reverse proxy.

www.bivio.net

Cloud Security Proxy Solution

The Cloud Security Proxy is integrated on Bivio's family of compact cyber applications platforms. These platforms implement a secure and robust architecture that enables the Cloud Security Proxy to operate in a high assurance mode. This is achieved through a unique architecture that segments the management control of the proxy from applications processing of the user's data. The platform incorporates a NIAP validated RedHat Enterprise 7 operating system for application processing and has been has been assessed to meet the stringent *Commercial Solutions for Classified (CSfC)* standard.

Whether the user is a mobile phone, tablet, laptop or remote desktop system, the Cloud Security proxy provides the external transport layer security (TLS) tunnel into the IT asset. Once the user reaches the Cloud Security Proxy, it delivers validation of the access, verifies the requested resource and creates the internal secure tunnel to that resource. The proxy solution enables logging of every session for full auditing, permits the access control through multiple security controls and affords full protection of the internal IT assets.

The proxy solution delivers secure communications with transport layer security for users accessing public or private information technology assets. It features 5 Gbps of AES-GCM encryption per processing core, supports a minimum of 500,000 sustained end-to-end TLS sessions and 800,000 client-side TLS sessions. The integrated platform is NIAP-Common Criteria and FIPS 140-2, Level-1 validation for high assurance operations. This is accomplished with the FIPS 140-2 validated crypto libraries where the proxy supports Advanced Encryption Standard (AES), Elliptical Curve Cryptography (ECC) encryption standards and Secure Hash Algorithm (SHA) message digest. The crypto module meets the NSA SuiteB standards for protecting classified data in-transit across the grey and red networks. Whether the cloud is implemented as a public, private or hybrid cloud infrastructure utilizing, wired, wireless or LTE networks access, the Cloud Security Proxy delivers assurance so that the communications path re-mains secure end-to-end.

In addition to the TLS proxy mode, the Cloud Security Proxy can be utilized as reverse proxy to protect the enterprise from reconnaissance and exposure of internal IT assets. The solution supports HTTPS validation and enforcement for connections originating from or destined to the cloud. To prevent unauthorized HTTP/HTTPS connections, the proxy implements dynamic ACL's for management of Whitelists, Blacklists and URL restrictions. The proxy with its Web Application Filtering can filter any element of the HTTP/HTTPS request or response as well as deliver to the user specific error codes for that request/response process. The proxy has embedded anti-bot and DDoS protection as well as optional security monitoring of the SSL/TLS process. The Cloud Security Proxy can also operate in an integrated load balancing mode.

High Availability

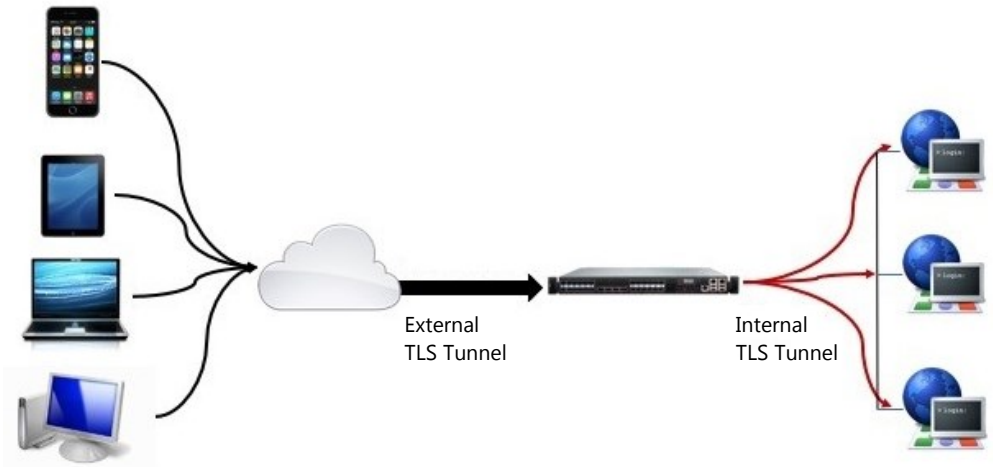
Ensuring availability is essential in mission critical networks. The Cloud Security Proxy meets this requirement with implementation of high availability mode for fail-over operations. In the compact cyber application platform, the Cloud Security Platform leverages Virtual Router Redundancy Protocol (VRRP) to support active, passive clustering of the proxy. To prevent situations where traffic overload can disrupt back-end web server operations, the proxy enables queueing of requests and ensures delivery. Finally, the proxy solution can perform routing protocol announcements based on the health of the network when used in the active-active clustering mode.

User Access and Control

Controlling user access to protected resources can be with simple username and password control systems or through security identification tokens. The proxy provides scripting for integration with those mechanisms or directly into active directory, LDAP and other security control mechanisms. For higher level of assurance where the user validation is certificate-based, it delivers the ability to control access through the use of digital certificates. The Cloud Security Proxy ensures the user is validated against the LDAP environment through OCSP and performs CRL checking prior to completing the connection request.

Integrated Security Monitoring and Analytics

Identifying and analyzing attempted fraudulent activity into the proxy is increasingly important. Bivio Networks' expertise in cyber security and information assurance ensures that the solution we deliver is secure and meets rigid standards. Over and above this embedded security, an organization should desire to monitor cloud access to the protected assets for any attempts of fraud, misuse and deception. The proxy supports integrated security monitoring which provides the ability to log every connection to – and – from the Cloud Security Proxy frontend as well as



connections from the proxy to backend resources. Each TLS session is evaluated, and the certificate are logged with the results of the CRL validation. Events such as DoS/DDoS are logged, analyzed and the cyber analyst is alerted to the event. The information can be "geo-tagged" with the GeoIP data for further analysis. All information for the security monitoring is available in the Systems Management Center analytics.

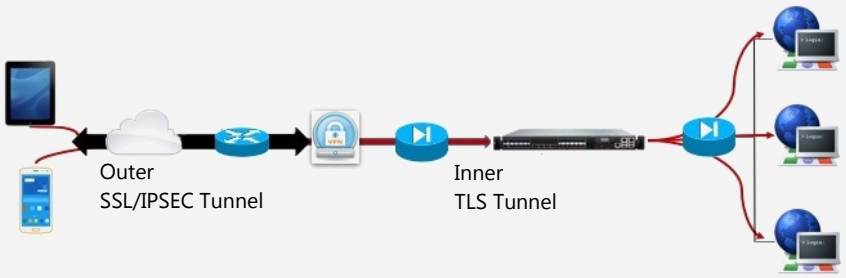
Systems Management Center monitors the Cloud Security Proxy and platform for operational effectiveness. Through monitoring process, the proxy can be "tuned" for optimal operations.

Key metrics for the session process is scrutinized to determine if configuration changes are required for the proxy. The platform core components such as interfaces, processors and memory can analyzed for determining the most effective settings as well as identify any potential problems prior to a failure.

Case Study - Commercial Solution for Classified (CSfC), Mobility

Enabling access to classified or sensitive data in protected networks with mobile devices such as smartphones or tablets presents a unique challenge. A higher-level of confidentiality, integrity and assurance (CIA) is needed. This is to ensure the data or systems that the user is accessing is not exposed to bad actors. Additionally, a dual tunnel configuration prevents traffic analysis from being applied to the user's connection request. The way this access is being facilitated is with commercial solutions and technology.

The combination of technology and components that are implemented utilizing the Commercial Solution for Classified framework is designed to specifically to address the special confidentiality, integrity and assurance aspect in classified mobile access. This framework enables the protection for accessing that data on those classified or sensitive networks. This solution involves the Bivio Compact Cyber Applications platform as a TLS-protected server and the Cloud Security Proxy application which is a TLS proxy application. The combination of these two components creates a unique capability that is a Commercial Solutions for Classified (CSfC) - approved TLS service for mobile users.



In the mobility diagram (shown above), a mobile device such as smartphone, tablet or even a laptop can access protected services through a wired, wireless or LTE network. The CSfC Mobility architecture enables this access with dual data protection technologies. This first data protection technology is supported by the implementation of a CSfC technology that provides an outer tunnel via a VPN gateway from the mobile device to the gateway that terminates in the outward facing (black) network. The second data protection technology is provided by Bivio's Cloud Security Proxy which enables the "inner-tunnel" with transport layer security for terminating client session access from those mobile users in the transitional (grey) network and validate their access.

Those mobile user devices (smartphone or tablet) may contain a client that is based on either Hypori™ by Intelligent Waves or SecureIO™ by Perspecta which will allow them to access the inner (red) network with the back-end virtual mobile or desktop infrastructure. From the laptop user, the access may be enabled by a client or through a TLS-enabled web browser. In this environment with these devices, the Cloud Security Proxy secures the connection from the client application on the mobile device via TLS, validates the user access with a digital certificate and routes the connection to the proper back-end server. Once this process is complete, the Cloud Security Proxy enables and manages the session for carrying data between protected IT assets and client on the smartphone, tablet or laptop.

Atlas Cloud Security Proxy

System Administration and Proxy Management

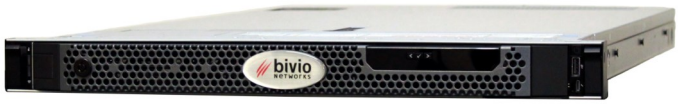
The Cloud Security Proxy provides for full systems administration and proxy management. The management can be conducted through console control, remote SSH access, Restful API or the Systems Management Center. The integrated management with Systems Management Center utilize playbooks for Ansible to perform command, control and configuration for each associated Cloud Security Proxy. This automates proxy functions and tasks such as enabling, disabling and draining back-ends.

Bivio 6310 Series TLS Protected Server

The B6310-NC Compact Cyber Application platform is a core component of the Cloud Security Proxy Technology. The platform provides from 16 to 56 cores of compute power for scalable encryption and proxy workloads. This enables proxy services for hundreds to thousands of simultaneous users. It facilitates an application-agnostic proxy environment for supporting multiple TCP-based traffic types including Web, Instant Messaging, Voice and Video applications from various vendors. The platform also supports multiple 1 and 10 Gb interfaces. The B6310R-NC ruggedized platform can be implemented in austere environments enabling mobile, deployable and tactical services.

Summary

The Atlas Cloud Security Proxy provides an exceptional level of confidentiality, integrity, and assurance for enabling TLS-based network communications in enterprise, cloud and mobile environments. Coupled with security monitoring and integrated analytics, Cloud Security Proxy is a unique and un-paralleled capability. This solution is the only application-agnostic transport layer security proxy that is enabled with National Information Assurance Partnership – Common Criteria, FIPS 140-2 and Commercial Solutions for Classified (CSfC) validation.



Cloud Security Proxy Features	*Comments*
NIAP, FIPS and CSfC-Enabled TLS Proxy Mode	*Applicable to TLS and Reverse Proxy Modes*
Integrated Application Delivery Controller (Load balancer)	
Advanced Proxy Security Features	*DDos Protection, Bot Detection, Web Application Firewall with Blacklist & Whitelist and HTTP Protocol validation*
Integrated Analytics and Security Monitoring	
Integrated Platform and Application Configuration and Control	
Plug-in and scripting extensibility	
User access control tools and scripts	
Configuration API	*Console, SSH, RestAPI, Web Interface in System Management Center*
High availability mode with active, passive clustering	
High performance modules, configuration and tuning scripts	
Platform operations at 1 & 10Gbps	
Licensing – Platform plus Per User license	*Per user license is based on annual subscription. Fee is based on user bands. Contact Bivio Networks for specific information.*

About Bivio Networks

Bivio Networks is dedicated to providing leading networking products that enable government agencies and service providers to control, monitor and secure critical network infrastructure. A leader in cyber intelligence, cyber security and network control solutions, Bivio products are deployed in a wide range of environments by a global customer base including leading intelligence agencies, service providers and enterprises. Bivio is privately-held and is headquartered in the San Francisco Bay Area.

bivio networks

Bivio Networks, Inc.
4457 Willow Road, Suite 240
Pleasanton, CA 94588
Tel: +1 925 924 8600
Fax: +1 925 924 8650
www.bivio.net