BlueSky® GNSS Firewall Network Security

Ensuring Hardened Network-Based Security While Protecting Against GNSS Jamming and Spoofing

Summary

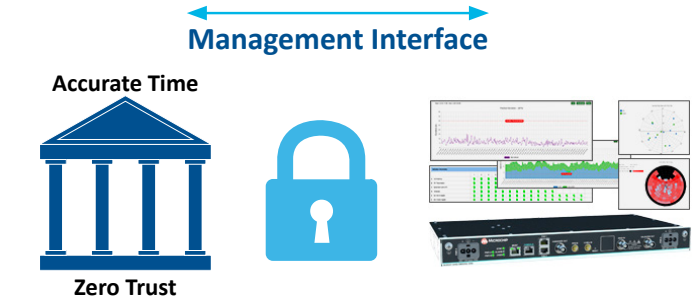
It's essential to protect the timing reference used by networks that support critical infrastructure. For most critical infrastructure, the primary timing reference is derived from GNSS systems, which rely on externally exposed GNSS antennas. However, these antennas are vulnerable to various jamming and spoofing threats. GNSS systems face risks not only from external live sky threats but also from threats originating within the network itself.

To enhance the security provided by the BlueSky® GNSS Firewall, the network management interface must meet the increasingly stringent security requirements of critical infrastructure. It is crucial to defend against both live sky GNSS adversities while adhering to network zero-trust principles and integrating into a zero-trust architecture.

The BlueSky GNSS Firewall now offers robust protection against live sky jamming and spoofing threats, along with a highly secure Trusted Time™ technology network management interface to defend against cyber threats. This ensures the security of time in compliance with the fundamental pillars of zero trust, including users, devices, network and analytics.

GNSS Features

- Identifies and protects GNSS systems from spoofing and jamming
- Integrates seamlessly between existing GNSS antenna and GNSS systems(s)
- Independent RF power monitoring of L1, L2, and L5 bands
- Optional Internal Rubidium Miniature Atomic Clock (MAC) for holdover
- 1 PPS and 10 MHz timing reference inputs for extended holdover (for example, connection of external cesium reference)



BlueSky GNSS Firewall Network Security

BlueSky GNSS Firewall Anomaly Detection

Figure 1: The BlueSky® GNSS Firewall provides live sky GNSS security and a secure network interface to meet the fundamental pillars for zero-trust networks.

Network Security Features

- Barrier between untrusted GNSS sky signals and downstream systems
- Supports RADIUS, TACACS+ and LDAP authentication
- Hardened web GUI with Transport Layer Security (TLS) 1.2
- Controlled access to software updates
- X.509 CA-signed certificates
- Enable/disable system control through web GUI
- Secure Syslog
- Trusted Time™ Anomaly Detector for comparing Network Time and GNSS Time
- GPS Subframe Reference detection enabling the BlueSky GNSS Firewall to compare live-sky subframe data with subframe data received from a remote BlueSky GNSS Firewall

Security Hardening of Network Interface

Configurable User Security Privileges and Authentication Protocols

Our BlueSky® GNSS Firewall supports two-factor authentication with RADIUS, which requires an additional login credential beyond just the username and password to gain account access. TACACS+ can be utilized to manage and control device access effectively.

The BlueSky GNSS Firewall is compatible with LDAP v2 and LDAP v3, which are protocols used for authenticating users to access directory services. LDAP facilitates the centralized storage and management of user information, including usernames, passwords and groups, to streamline directory management.

In the administrator role, only the administrator has the authority to create user roles with designated passwords and access levels. Administrators can also configure session timeouts and set password expiration periods for users. If these values are not specified by the administrator, default thresholds will be applied.

Leveraging the Latest PKI Infrastructure and TLS Hardening

The BlueSky GNSS Firewall's web GUI, designed for monitoring and upgrading the unit, is user-friendly yet highly secure. The interface is fortified with X.509 CA-signed certificates and employs robust TLS 1.2-based encryption to provide a very secure connection.

Secure, Web-Based Communications and Enhanced Management

Network Security utilizes HTTPS to provide encrypted and secure web-based communications between the user and the device. This secure communication protocol is crucial for preserving the confidentiality and integrity of the data exchanged during the configuration and monitoring process.

The BlueSky GNSS Firewall also employs SNMP and Secure Shell (SSH) to enhanced management and security. SNMP facilitates efficient network management by allowing administrators to monitor the device's performance and identify potential issues promptly.

SSH provides a secure remote access to the BlueSky GNSS Firewall's command line interface. By encrypting the session, SSH ensures that administrative tasks, such as firmware updates and advanced configurations, can be performed securely to protect the system from potential cyber threats.

Remote Log Server Support

Analytics rely on network telemetry data, which includes activities such as user logoffs/logons, configuration changes and software upgrades. The BlueSky GNSS Firewall also integrates with the TimePictra® management platform to monitor and verify the latest configuration changes. The TimePictra management platform provides an interface for viewing multiple BlueSky GNSS Firewalls, enabling network administrators to swiftly identify and respond to potential threats or anomalies in GNSS signals.

Secure Software Installation With Encrypted Authorization Files

The BlueSky GNSS Firewall features in-field service update capability. As attacks on GNSS systems are expected to become increasingly sophisticated, these in-field service updates enable users to stay ahead of the evolving threat landscape.

Access to the BlueSky GNSS Firewall software downloads is restricted to authenticated and authorized users only. These downloads include encrypted authorization files that govern the software installation process. Prior to installation, the BlueSky GNSS Firewall verifies the integrity of the software to ensure its authenticity.

Security Timing Protection Using Interconnected Network BlueSky GNSS Firewalls

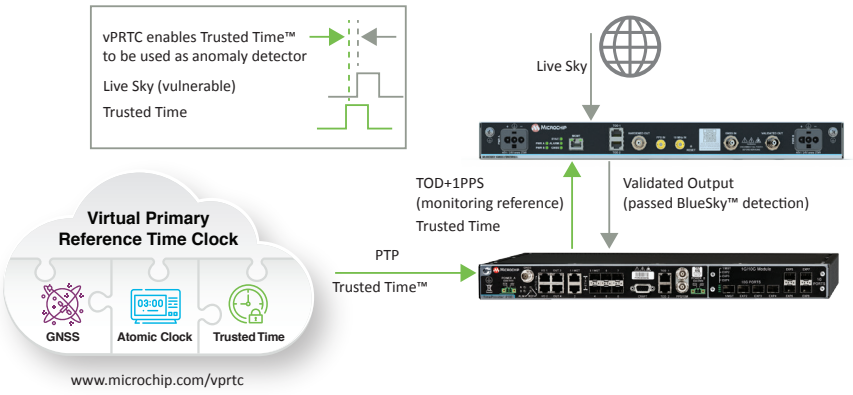
The BlueSky GNSS Firewall is equipped with both a local console port and a dedicated network management port. The local console port is ideal for direct user access to the BlueSky GNSS Firewall, facilitating straightforward configuration and management. The network management port, on the other hand, enables connectivity to a centralized network management system such as TimePictra. This port can also be utilized for interconnecting multiple BlueSky GNSS Firewalls to perform advanced anomaly detection.

Additionally, the BlueSky GNSS Firewall features two Time-of-Day (TOD) ports, which can also be employed for anomaly detection purposes, enhancing the overall security and reliability of the system.

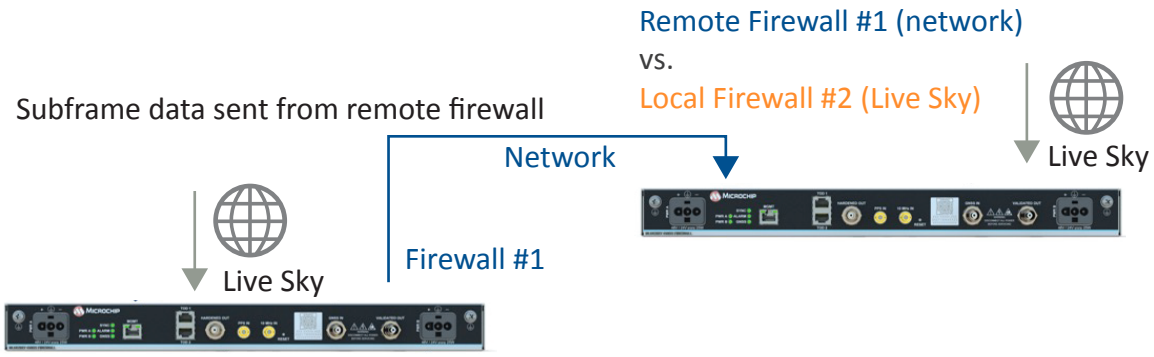
GNSS Anomaly Detection Leveraging Network Interfaces

Trusted Time™ Anomaly Detector: Release 3.0 of the BlueSky GNSS Firewall can make use of Trusted Time as an anomaly detector for GNSS Vulnerabilities. Using the TimeProvider 4100 as a high-performance boundary clock (HPBC), Trusted Time can be connected to the BlueSky GNSS Firewall using the standard Time-of-Day (TOD) interface or the 1PPS signal input. This enables the BlueSky GNSS Firewall to measure and compare the incoming live-sky signal to the Trusted Time as delivered over the network. The result is that the Trusted Time Anomaly detector within the BlueSky GNSS Firewall can alarm if the "network time" and the "GNSS time" drift too far apart.

Using the Validated Output of the BlueSky GNSS Firewall, the GNSS signal is passed through to the downstream TimeProvider 4100 after being verified by the BlueSky detection algorithms, including the Trusted Time detector. If the live sky signal is determined to be compromised, the Validated Output is turned off and the TimeProvider 4100 enters holdover. The Trusted Time Anomaly Detector can use either the TOD or the 1PPS input for monitoring. The threshold (phase difference between Live Sky and Trusted Time) for triggering an alarm is configurable by the user.



GPS Subframe Reference Detector: The BlueSky GNSS Firewall enables a revolutionary new approach to verify GNSS reception using a technique called GPS Subframe Reference Detection. Redundant BlueSky GNSS Firewall systems can be deployed throughout a building, across an airport, rail station, maritime port, datacenter or across large geographical areas and can be interconnected together to compare subframe data. The remote BlueSky GNSS Firewall can be identified as the "truth source" such that the local BlueSky GNSS Firewall compares it's locally received live sky subframe data to the remote (trusted) subframe data coming from the remotely deployed Firewall. If a difference is detected, then an alarm can be generated to indicate a miss-match (i.e., an anomaly).



BlueSky GNSS Firewall Trusted Time Security Check List for Zero Trust Network

Users	RADIUS authentication and two-factor authentication
	TACACS+ support
	Administrative security
	a. Web session timeouts (5-1440 minutes long)
	a. Custom login banners
	LDAP authentication (LDAP v2 and LDAP v3)
	User settings
	a. Password expiration
	b. User management (creation/deletion, username, password, email)
	c. Multiple user privilege levels
	I. Administrator: Can create new roles and users
	II. User: Default basic role
	SSH (allowed and denied users)
Devices	**Software upgrade**
	a. Available exclusively through the Microchip customer portal
	b. Requires authenticated user access to the Microchip customer portal
	c. Requires authorization to download the system software file and serialized authorization file
	Alarms (extensive user-configurable alarms, notification via trap, logs)
	Hardened output provides a synthesized GPS signal isolated from the live-sky environment
	Validated output delivers a verified pass-through of the actual GNSS signal being analyzed
	HTTPS secure management
	a. Protocols: TLS 1.2 or higher
	b. Session timeout: 5 to 1440 minutes
	c. Self-signed certificate: 2048 or 4096 RSA key bit; expiration days 1-1825; customizable locality codes
	X.509 Cert/CSR: Create and download Certificate Signing Requests (CSRs) with 2048 or 4096 RSA key bits
	X.509 installation: Install multiple CA-signed X.509 certificates
	Timing security
	a. Anti-jam antenna
	b. Atomic clock upgrades for timing holdover
Architectures	Dedicated and distinct network management port, along with a local console port
	Service/system control (enable/disable HTTPS, SNMP, SSH, ToD)
	GPS Subframe Anomaly Detector compares subframes from a remote firewall to those received from the live-sky signal within the local firewall (For more information, see the BlueSky® GNSS Firewall Software-Release 3.0 data sheet)
	Trusted Time Anomaly Detector allows terrestrial network-based time to cross check GNSS time (For more information, see the BlueSky GNSS Firewall Software-Release 3.0 data sheet)
Analytics	**SNMP V3**
	a. Secure authentication
	b. Secure encryption
	TimePictra® platform monitoring
	a. Tracks last configuration changes
	b. Supports autonomous messaging
	c. Monitors firmware versions
	Secure Syslog
	a. X.509 authentication
	b. TLS encryption

DS00005768A

MICROCHIP