WHITE PAPER

G1 Platform Security

Executive Summary

The Tarana next-generation fixed wireless platform is designed to deliver services securely based on industry standards. This includes everything from hardware-based, tamper-proof crypto chips to end-to-end encryption of control and management communications, over-the-air encryption of subscriber data, and a strong, RBAC-based multi-tenant cloud services design. Periodic third-party penetration tests are conducted to ensure continued security.

Solution Components

There are three components that comprise the Tarana G1 platform:

- Base node (BN) — installed on a vertical asset such as a tower
- Remote node (RN) — installed at the subscriber location
- Tarana Cloud Suite (TCS) — SaaS offering that includes centralized monitoring and management of Tarana devices
- Tarana mobile installation app — a mobile device application for simplified, faster installation of Tarana remote nodes

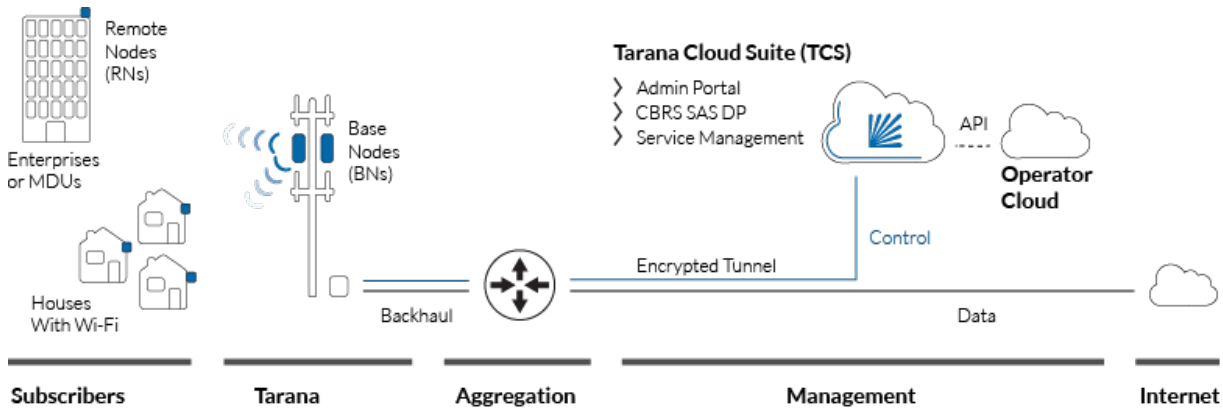

Figure 1: Tarana G1 platform

Hardware Security

All G1 hardware (base nodes and remote nodes) have a tamper-proof crypto chip installed at manufacture time. This is used to securely store cryptographic information, which is used to encrypt traffic to TCS. Hardware devices are also shipped from the factory with a signed digital certificate. TCS and G1 hardware authenticate each other through mutual TLS 1.3 (mTLS).

Each base node and remote node also host a local web UI, accessible over HTTPS from a local device, such as a laptop or remotely via TCS. The local web UI requires administrator credentials for login. The device hosts an onboard firewall that restricts

access to the device SSH port. SSH access can be administratively disabled for base nodes and remote nodes.

All operators are issued a unique operator ID that ensures their remote nodes only connect to their base nodes. Device security further enhances this, allowing only authorized RNs to connect to an operator's BNs.

Traffic Flows

There are three main types of traffic in the G1 platform: management plane, control plane, and data plane. All management and control plane traffic (monitoring/telemetry, configuration, and management) are transmitted securely between the remote node or base node via an encrypted VPN tunnel to TCS. All over-the-air (OTA) traffic between the base node and the remote node is encrypted using AES-128 security.

Data plane traffic, however, is not transmitted to TCS. All user data stays within the operator's network and is routed onward from there, according to the operator's traffic engineering rules.

Management and Control Plane Traffic

Management and control plane traffic include configuration, monitoring (including streaming telemetry), software upgrades, event logs, alarms, and operations, such as muting/unmuting the base node radio and rebooting devices.

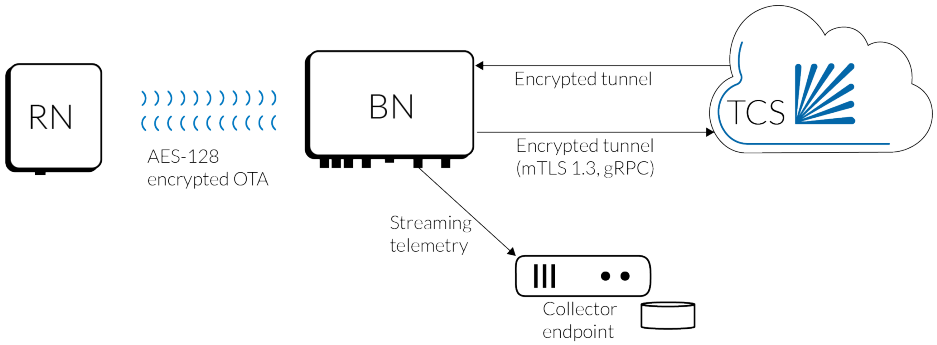

Figure 2: Management and control plane traffic is encrypted end-to-end

Data Plane Traffic

Data traffic is encrypted OTA between the remote node and the base node using AES-128 encryption. In addition, Tarana recommends VLAN separation between management and data traffic. Under no circumstances is user data transmitted to TCS. OTA transmissions from one node to another node are blocked at the base node. Broadcast and multicast traffic is also blocked at the base node's downlink unless specifically enabled by an administrator. All devices feature broadcast storm controls. Figure 3, on the next page, illustrates the data traffic flow.

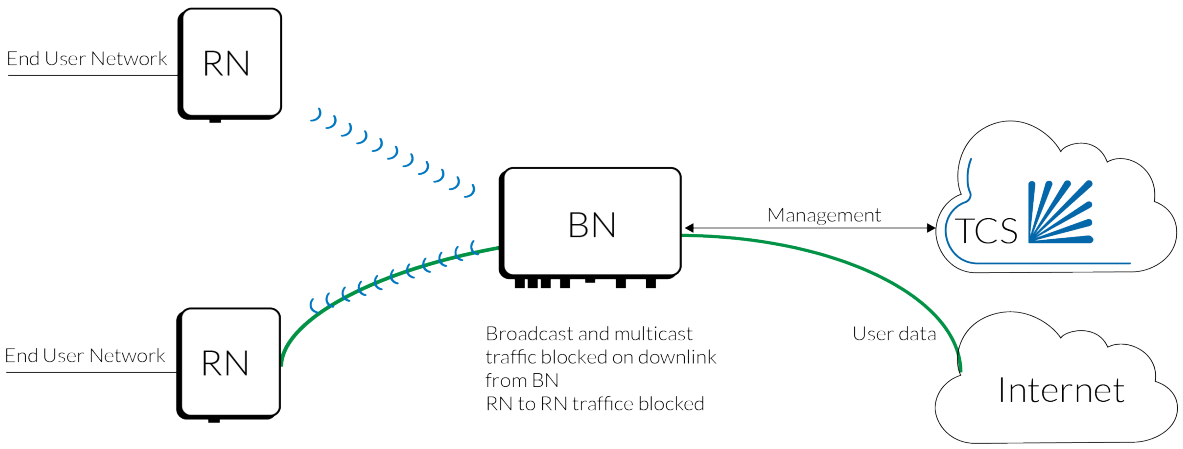

Figure 3: Data traffic is encrypted OTA and handed off to the operator's network

DHCP Option 82

Operators have further control over management traffic through the use of DHCP Option 82. With option 82, a relay agent can add option 82 information to a DHCP request and response. This ensures DHCP requests and responses are coming from trusted sources. Option 82 can also be used by the operator to control how dynamic IP addresses are assigned to subscriber equipment and to prevent IP pool exhaustion.

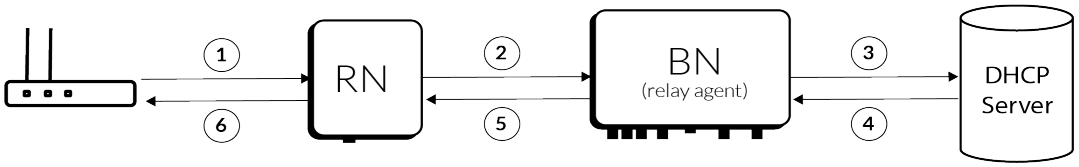

Figure 4: Six steps of DHCP Option 82 interaction

The figure above and table below describe the entire DHCP Option 82 process. It is important to ensure the DHCP server supports and is configured for option 82.

Table 1: DHCP Option 82 workflow

Step	Action
1	Subscriber equipment connected to the RN sends a DHCP request
2	DHCP request is forwarded by the RN
3	A BN configured as a relay agent adds either the serial number or MAC of the RN to the request
4	Server responds with a dynamic IP address assignment
5	The BN removes DHCP Option 82 field before forwarding the response to the RN
6	The DHCP response is forwarded by the RN to the subscriber equipment

TCS Security Architecture

TCS operates as an instance of AWS virtual private cloud and uses the 3-tier AWS architecture. TCS takes advantage of AWS' multi-zone resiliency, spanning 3 different availability zones. Both the TCS portal application and associated database and messaging services are part of protected, private subnets. All data, including user profiles, profiles, device configuration, etc. are stored in an encrypted database.

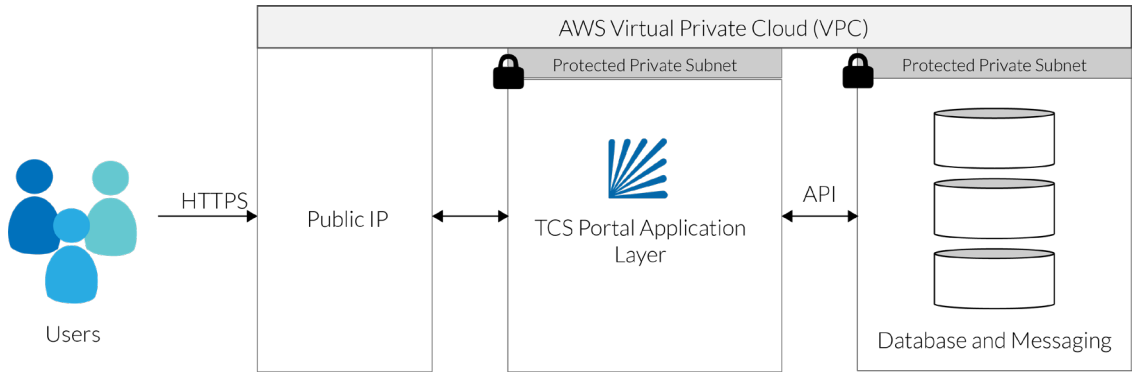

Figure 5: TCS is implemented as part of an AWS virtual private cloud, with encrypted data and messaging

HTTPS is the only supported protocol for user login to the TCS portal. Only the TCS application has access to microservices and databases. The TCS portal application accesses microservices through secure APIs using JSON web tokens (JWTs). Databases are accessed using their respective authentication mechanisms.

Multi-Tenant TCS Data Access

TCS is a multi-tenant platform that allows multiple operators to access their network from anywhere securely. As part of the multi-tenant architecture, each operator (tenant) is assigned a unique identifier. This identifier is used to restrict visibility and access between tenants. Thus, each tenant can only see their own information and assets.

Role-based access control (RBAC) has also been implemented for further security within the operator context. TCS supports six different roles to which a user can be assigned. This role determines the privileges that account has within the operator's network.

Role	Access Privileges
NOC L1 User	Read-only (view) access to devices, including: ❯ Access device notes, events, alarms, charts, maps, and device notes ❯ Run speed tests ❯ Cannot access the web UI of a device from TCS
NOC Operator	Read and write operations for devices, including: ❯ All the privileges of NOC L1 User ❯ Device configuration ❯ Device operations (software upgrade, reboot, snapshot, primary BN search and connect) ❯ Can access the web UI of a device from TCS
Operator Admin	The highest-level administrator within TCS, OP Admin includes all NOC L1 User and NOC Operator privileges, plus: ❯ Create, delete, or modify users ❯ Create, configure, delete, or modify the network hierarchy ❯ Define and modify network policies
Retailer Viewer	Read-only (view) access to a subset of RNs (owned and managed by a particular retailer or group within the operator) and their associated events and alarms. Limited read-only view of associated BNs.
Retailer Operator	All read and write operations for a subset of RNs and their events and alarms. Limited read-only view of associated BNs.
Retailer Admin	All Retailer Viewer and Retailer Operator privileges, plus the ability to create new users for their organization. Limited read-only view of associated BNs.

Login Security

TCS login includes features to protect against brute force attacks and compromised credentials.

- TCS users must change their password at least once every six months
- Passwords must follow a strict set of complexity and reuse rules
- A user account will be temporarily locked after multiple failed attempts
- The account user is notified when a login attempt is made from a new device or location
- User accounts inactive for more than 90 days are automatically disabled.

Multi-Factor Authentication

Multi-factor authentication (MFA) is available as a globally enforced security option. MFA onboarding is automatically initiated at user login. A wide variety of authenticator apps are supported, including Google Authenticator, Duo, Authy, etc.

OAuth 2.0 Support

TCS supports single sign-on via an external server that supports OAuth 2.0. With this feature, TCS users will authenticate using their corporate credentials rather than a local TCS user account.

Tarana Support Access

As part of troubleshooting support, a customer may temporarily grant Tarana Support engineers access to their network in TCS. There are three levels of access: read-only, basic, and advanced. Read-only access is equivalent to the NOC L1 User level of permissions. Basic is equivalent to NOC Operator, and advanced is equivalent to OP Admin and SSH access privileges. These basic and advanced permissions may be granted and revoked at any time.

3rd-Party Security Testing

Tarana periodically hires an independent cybersecurity advisor to conduct and report on penetration testing of TCS. The testing methodology includes PTES, OWASP, and NIST 800-115.

Summary

Each component of the G1 platform is secured according to the means and methods available for that component. This includes:

- All hardware devices include a tamper-proof crypto chip to store private keys for mutual authentication with other components
- All control and management plane traffic is encrypted from the device to TCS
- No subscriber data is transmitted to TCS
- All over-the-air (OTA/in-flight) traffic between the base node and the remote node is encrypted using AES-128 encryption
- JSON web tokens (JWT) are used to ensure the integrity of any session
- Each operator has a unique identifier that is used to prevent access between multiple tenants on TCS
- Role-based access (RBAC) further limits the privileges available to a TCS user
- Periodic 3rd-party penetration testing to ensure continued TCS security

Interested in learning more about our innovative solutions? Get in touch with us at taranawireless.com/how-to-buy

Tarana's mission is to accelerate the deployment of fast, affordable internet access around the world. Through a decade of R&D and more than $400M of investment, the Tarana team has created a unique next-generation fixed wireless access (ngFWA) technology instantiated in its first commercial platform, Gigabit 1 (G1). It delivers a game-changing advance in broadband economics in both mainstream and underserved markets, using either licensed or unlicensed spectrum. G1 started production in mid-2021 and has been embraced by more than 200 operators in 23 countries and 45 states. Tarana is headquartered in Milpitas, California, with additional research and development in Pune, India.

@taranawireless taranawireless.com

TARANA