GWN.Cloud Security White Paper

Updated Time: 03/02/2023

Overview

GWN.Cloud is a cloud management platform used to manage and monitor GWN devices (access points, routers, and switches). Protects against known and unknown threats in real time in a networking environment, providing advanced security defense capabilities for the network. This document introduces the GWN.Cloud data security, privacy and compliance, and operational security, in order to help you understand how we provide reliable and secure services to our customers.

Infrastructure Security

Network Security

We use cybersecurity and surveillance technology to provide multiple layers of protection and defense. The firewall of all servers is strictly audited, and only the corresponding ports are open to the corresponding address range, preventing unauthorized access and bad traffic to our network. To protect sensitive data, our system is split into separate networks. The network environment for testing and development is on a different network from the GWN.Cloud online system.

We have professionals who regularly review all changes made to the firewall and monitor access to the firewall on a strict schedule. We also monitor infrastructure and applications for any discrepancies or suspicious activity. We use our proprietary tools to continuously monitor key parameters of the network and trigger notifications whenever abnormal information is detected.

Both Web services and Gateway services (which communicate with devices) use the TLS security protocol, and the server certificate is a trusted certificate issued by DigiCert to ensure the security of the end-to-end communication link.

Deployment Security

Each of our service systems and programs has an independent account with corresponding permissions to manage the deployment, that is, only the permission account of the corresponding program is used to run the deployment, and the system directory and other software directories cannot be accessed, so that the deployment risk is controlled in the lowest range.

When the maintenance persons connect to the server, they need to use the authorized springboard machine to connect to the server. After each connection, the server updates the certificate for connection and sends it to the maintenance person before the next connection.

DDoS Protection

Our server will automatically detect abnormal massive data outflow and shield abnormal data to prevent it from being used by DDoS attacks.

In addition, when DDoS attacks are detected, our cluster supports rapid expansion to cope with a large number of attacks. This can block a large number of attacks to ensure service continuity.

Data Security

Transmission Encryption

All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We require Transport Layer Security (TLS 1.2) encryption and strong passwords for all connections to our servers, including network access, API access, and mobile apps.

Each GWN device has a different built-in Grandstream independent certificate. GWN.Cloud will authenticate the connected GWN device based on this independent certificate to prevent attackers from using anonymous identities to attack GWN.Cloud.

Data Storage and Encryption

Consumer data stored the data base is encrypted to ensure confidentiality and integrity.

GWN.Cloud does not store user passwords in plaintext format. Passwords are hashed before storage and cannot be decrypted to protect user privacy.

We store your file data in AWS S3 and protect it from unauthorized access using encryption features and access management tools. S3 encrypts uploaded files for storage and provides a redundant backup mechanism to prevent data loss.

AWS ELBs are used to achieve dynamic load balancing of services to avoid the impact of single machine failures and maintenance.

About the storage of client traffic information reported by the device: We store this part of data in the big data storage service, and the traffic information is only used for network graph analysis.

In addition, we store your device configuration data and user data in AWS storage servers, and use a powerful VPC network management mechanism to isolate data and prevent hackers from using various attack methods.

Data Access Permissions and Restrictions

The data stored in our system is owned by the user, and the user configures role permissions to control access restrictions.

On GWN.Cloud, data owned by different enterprises are isolated from each other. The data managed by different users are restricted to the assigned user's role and permission. Users can only view and manage data that their assigned permissions allow them to.

On GWN.Cloud, an enterprise's data is not shared with any other enterprise unless the user authorizes it. Users can only view and manage data that their assigned permissions allow them to. Grandstream GWN.Cloud technical support does not have permission to manage user devices unless specifically authorized by the user to Grandstream.

Invalid Data Disposal

When a user deletes data such as a device or template, the associated data is deleted immediately.

When a GWN.Cloud account is deleted, we immediately delete all data associated with that GWN.Cloud account from the database.

Legal Basis for Data Processing

GWN.Cloud is GDPR compliant, and data stored in its US and EU servers are managed separately.

With the exception of user login credentials, channel's devices and relationship information for the channels, data stored in the US server's database is not shared with the EU server's, and vice versa. Account login information, channel's devices and channels' relationship information are stored in a centralized database. Sensitive user data is not included in the information mentioned above.

Authentication Security

User Authentication

Users must use their own accounts and passwords to log in to the GWN.Cloud. Users are required to provide additional information based on risk factors. For example, if a user enters a wrong password for three times, the user must enter a verification code to log in to the GWN.Cloud; the user will receive security alert if the user logs in the GWN.Cloud through different IP addresses. After the user is authenticated, the identity service issues credentials

such as cookies and OAuth tokens for use in subsequent invocations.

Multi-factor Authentication

In addition to the password, we also provide multi-factor authentication, additional security hardening account. This can greatly reduce the risk of unauthorized access if a user's password is accidentally disclosed.

Users can purchase supported physical devices or virtual MFA devices to enable MFA for GWN.Cloud accounts.

Operation Security

Record and Monitor

We provide 7*24 hours operation and maintenance support. We monitor the real-time CPU/ memory/hard disk/network status of all servers, and have separate monitoring and abnormal alarm for each service. Once abnormal information is detected, we will inform the operation and maintenance staff through SMS/phone call/etc. to deal with it in time. At the same time, we check the health status and trends of all services every day to prevent security incidents in advance.

Vulnerability Management

We conduct regular internal penetration test and security inspection, including common Web attack test, business logic and permission test, software reinforcement for public vulnerabilities, and etc. Once we find a vulnerability that needs to be fixed, we will immediately track it until it is resolved through a patch.

Backup

We carry out incremental backup every day and full database backup every week, and back up data to Amazon S3 for encrypted storage, to ensure that user data will not be lost. All backup data is retained for three months. If a customer requests to restore data during the retention period of the backup data, we will restore their data and provide secure access to it.

Business Continuity Assurance

All servers have the hot backup and automatic migration functions. If some servers are abnormal, they can be automatically switched over to normal nodes to ensure uninterrupted service running. When the overall server pressure is large, the horizontal expansion will be

automatically carried out to equalize the huge service pressure by adding servers to ensure the stability of the service.

Feedback

We have a dedicated support team. You can report a security or privacy incident to us via the Grandstream Forum or the GWN.Cloud feedback platform, and our team will respond to your report in the first place, track and resolve the incident with appropriate corrective action.

For common events, we will notify users in time through email.