AIR ZEN

Software-defined Networking

AIRZEN OS DATASHEET

The AirZen Operating System for Routers & Servers.

Executive Summary

This document aims at a technically versed audience.
It describes the structure and the technical details of the AirZen platform. All AirZen solutions connecting businesses and people are based on the proprietary technologies described herein.

CONTENT

PROBLEM OUTLINE

Contemporary network technology is sourced mainly from US-based companies. Recurring problems with security and conflicting legal requirements are regular topics for operators of centrally managed network installations. Presently, no provider from Europe offers network technology that can compete internationally. The entry barrier for new enterprises is comparatively high. Building and maintaining a product over many years is cost-intensive and requires a passionate team.

SOLUTION

Our mission at AirZen is to provide simple and secure network technology "Made in Europe". AirZen technologies are used in leading finance institutes - evidence of our success. Everyday problems are the central drivers for our innovation. We aim to make life easier for IT departments without eroding security requirements.

SERVICES & PRODUCTS

AirZen Managed Network Services (AMS)
The managed service offered by AirZen is based on our hard- and software through certified partners or AirZen directly. Customers have their networks - including WiFi - taken care of by AirZen and can make requests, provide feedback, or report issues via live chat using the AirZen Smartphone App. Results are gathered in a ticket system that other team members can access. We firmly believe that customers and service providers should be able to communicate easily.

AirZen Node Hardware (AZN)
To users, WiFi is the most important interface on a network. End users require secure access from a plethora of devices, and admins need a way to manage those users and facilities.
AirZen Nodes ("Nodes") provide the foundation for the AirZen platform at every location. They combine the latest WiFi 6 connectivity with the most modern CPUs available. Switches and 5G hardware are also available.

AirZen Software (AOS, ACF, APF)
Together, the software driving the WiFi routers (AirZen OS) and that running on the various server components (AirZen ServerOS) form the operating system of the AirZen platform itself. It provides the AirZen Core Features (ACF) and the AirZen Security Framework (APF).

The solution is designed to be a modular and software-based networking system (SDN /Software-defined Networking) that can be accessed via API, command line interface (ACF-CLI), and the management app (ACF-APP).

AIRZEN OPERATING SYSTEM

AOS-FW: AirZen OS, the Network Operating System

A WiFi router provides the connection of end devices and the network/internet. To ensure the secure operation of the entire network, these routers must use up-to-date software. New updates are installed automatically on all routers overnight as soon as they become available.

AirZen Nodes are not configured individually, apart from a few particular settings. Instead, AirZen ServerOS generates a configuration for the assigned location through one of its components. In the Node, this configuration is handed to the various components. The AirZen OS components are predominately written in the C language and are tied to a particular domain. Core features (ACF) and security features (APF) can usually be pinpointed to a single service implementing them. The entire platform is based around the Linux operating system, enhancing it with the AirZen Core Features.

Connecting to Nodes is possible via SSH using the AirZen Cloud-Command-Line (ACF-CLI). This mode of access is reserved for administrators to investigate bugs - not to change the behaviour of the device.

Security

During the factory process, every Node is equipped with a device-specific X509 certificate. This certificate is required to communicate with the AirZen server infrastructure. When a certificate nears its expiration, the Node will renew it automatically. Unlike other manufacturers, AirZen won't renew expired or invalid certificates automatically.

Certificates grant read-only access to the corresponding Nodes' configuration. An attacker gains little from extracting a certificate from the flash memory (requires access to the inside of the case and specialized hardware). Note that other connection secrets, such as WiFi passwords or VPN credentials, are stored on the device and are accessible to such attackers. Should a Node be stolen or opened by unauthorized personnel, it should be detached virtually to reduce further risk. Furthermore, it is recommended to change any secrets that might have been compromised - both of which require only a few actions.

AOS-SR - AirZen ServerOS

The AirZen ServerOS was designed to be open about how its components are implemented. To do this, a replacement server must implement only a few JSON-based interfaces, allowing operation using an independently hosted backend.
At the time of writing, AirZen OS runs on servers inside Europe. In the future, we will help set up self-hosted AirZen server installations with options to integrate parts of the AirZen-hosted infrastructure. To make that possible, most components of the AirZen ServerOS today are already limited in scope, have narrow interfaces to other services, and operate on independent databases. Their small size allows these components to be easily maintained, updated, or replaced. Moreover, special requirements can often be addressed by adding a custom service.

AIRZEN MODULES

AOS-BU: AirZen Business for Teams
Managing a business network is a sensitive matter with a high impact on security. It looks much the same as it did ten years ago, despite tools and threats having evolved heavily. User management, in particular, pushes IT departments to their limits. "Easy" and "secure" are typically seen as conflicting goals. Companies implementing a RADIUS-based authentication (WPA-EAP) mechanism for their WiFi struggle to integrate privately owned devices into their systems. Many IT departments want to grant these devices WiFi access but find it challenging to organize it without being able to rely on, for instance, a mobile device management (MDM) solution.

On the other hand, companies with less than 500 employees often use just one password for everyone, including the caretaker. Over time, changing the password becomes cumbersome, while at the same time, more and more people outside the company retain access to the network—be it former employees or visitors who just accessed the network once to load. We consider this to be a negligent practice, no matter whether it is caused by a lack of awareness or lack of time.

The AirZen Office Module addresses this issue by providing each user with an individual password. A self-service interface, accessible via the web or app, allows employees to manage their devices themselves. Limiting the number of devices or expiring provisions is possible. The transition from a single-password setup can be eased by temporarily setting the old password for anonymous logins.

That way, the AirZen Office Module enables "network hygiene". Network access can now be revoked for employees leaving the company, and inactive users can be deleted automatically after a set period.

For employees, the intended way of interacting with the system is the self-service interface. There are different ways to activate new provisions. Often, the company email address contains a fixed domain that can be used. If granting WiFi access to all company email address holders is undesirable, additional steps for clearance can be enabled, like by push notification to the local admin.

Overall, the AirZen managed service drastically reduces administrative efforts, eliminating some mundane tasks altogether by empowering authorized users to manage their resources.

Company processes can be realized in different ways, with the self-service interface being only one of them. The API is very versatile. Professionals can use the CLI to reach almost all functions quickly, and the AirZen App simplifies the most important interactions.

Use case
An SSID' teamwork' provides network access for employees at multiple locations. Employees can obtain access once their devices have been fitted with an individual passphrase. There is no common passphrase. Disabling a user blocks the user from the network by deactivating their passphrases.

The network operators control the network using the AirZen App and the CLI on their computers. Users access the self-service portal from their work computers or AirZen App on their smartphones. Registering an account with AirZen and multi-factor authentication is not necessary for users.

The AirZen App aids users by 'remembering 'the networks they gained access to and enabling access to the corresponding self-service portals. When help is needed, the App can be used for direct contact with the user.

AOS-HF: AirZen HomeOffice - Remote Work
Remote work is becoming more and more common. Employees and freelancers operate in networks containing other devices, like home appliances or personal devices of other family members.
In other words: Devices with unknown security parameters. 'Smart Home' appliances are known to be lacking in terms of maintenance and security. Older phone models might no longer receive updates. Businesses recognise the added risk and the increased attack surface when operating in such an environment.

AirZen clearly distinguishes between 'Home' and 'HomeOffice' and offers sets of three AirZen Nodes for employees to cover their homes. Employees who like the company network coverage can also use AirZen to provide their home WiFi. A pass-through 'home' SSID provides access to the home network, and a walled-off company SSID is used for work. It's also possible to assign Ethernet ports to either network.

Using the same device for both domains might seem counter-intuitive, but the device that separates the company network from the private network is also the device that connects them.
If a private computer is also used for work, there's little need for a physical separation of networks. Making the company network more visible in home environments also communicates the separation to employees.

Devices on the work network might be visible to the employer, and company devices shouldn't be used on the private network. If the same device supplies both networks, there should be less reason to switch to the other network because of coverage issues.

Regardless of the chosen paradigm: A logical separation of work networks is fundamental for IT security - especially with work appliances like telephones or printers involved. Most companies acknowledge this issue and address it by installing software VPNs on end devices or requiring end-to-end authentication inside applications. Still, there is a lack of solutions for separating company devices on a network layer.

It's possible to terminate a VPN on the AirZen Nodes. That enables the use of VPNs with devices that would not otherwise be able to encrypt their traffic, as some SIP phones do. This is also useful when end-to-end authenticated applications (cloud) are used alongside resources that require a VPN connection. Traffic can be redirected either through routing or by adding another company WiFi. Another way this might be useful is by allowing users to securely connect to their work infrastructure when they are not working from home.

Other means of increasing network security can be found in the "AirZen Protection Framework" section. For instance, the AirZen WatchDog Malware- & Bot-Net-Blocker.

If the domestic Internet service proves unreliable, the Node G5 can be used to gap outages with the built-in 4G & 5G modem. In addition, the ability to use 4x4 MIMO or to connect external antennas sets it apart from other solutions. Our home office white paper contains more details.

CORE-FEATURES OF AIRZEN OS

ACF-APP: AirZen Tools, Management App & Command Line Interface

The AirZen App and the command line interface are the main ways of interacting with the system for self managed installations and managed services. The App is dedicated to performing everyday tasks on the go efficiently. However, the CLI covers a broader range of functions in more detail—in fact, AirZen also uses the CLI. The App provides an easy way to check on an installation and manage employees, and, for most users, it is the primary way of staying in contact with AirZen via live chat and the ticket system.

ACF-GNC: Generic Network Controller for Software-defined Networking

The AirZen Generic Network Controller comprises multiple services and databases and is the centre piece for remote administration of network devices. Users can make incremental adjustments to logical and physical network entities in the configuration and assign them to locations and nodes through the API. Conversely, any consuming device can be sent its entire configuration at any time. That happens automatically every time a device boots or performs an update. Always configuring all services allows swapping devices at any time. Moreover, because most configurations are mapped from the location, new devices can be added easily.

The list of configurable entities includes:

- WiFi radios
- WiFi networks (SSIDs, mesh)
- Bridges (for Ethernet, WiFi, and VPN)
- VPNs
- WWAN (4G, 5G, LoRa)
- Captive Portal (for guest WiFi)

These entities can be connected dynamically. For instance, it is possible to have a guest WiFi using a Software-VPN for Internet access in one location and a VLAN in another without creating another WiFi.

Generic Network Controller Templates

As an alternative to the Generic Network Controller, AirZen also offers templates that allow configuring Nodes without dealing with the underlying entities. Templates are the easiest way to quickly set up networks while supporting more complex setups.

ACF-EVE: Event Engine

The Event Engine allows automating responses to different kinds of events like changes in Node connection state or firmware updates. Emails, text messages, push-notification, and webhooks are among the options.

ACF-LOG: Log-Service

The Log Service eases access to logs from multiple devices. The devices to process logs from can be selected either directly or by location.

ACF-AMP: AirZen Message Protocol

In order to communicate efficiently with many devices, AirZen employs a custom message protocol.

ACF-API: AirZen API

Use the API to automate interactions with the AirZen system. The App and the CLI also use the API under the hood.

ACF-IDM: Identity Management with AirZenID

Access requests to AirZen system resources are authorized using AirZenIDs, which can be created using the app or the website. In most cases, an AirZenID will belong to a person - the ‘user’. Two-factor authentication is mandatory. Most resources belong to an ‘account’. AirZenIDs are authorized to access these accounts. Thus, more fine-grained control is possible per AirZenID for many types of resources. The special ‘owner’ relation is used to grant unrestricted access. ‘Groups’ can be used to organize management permissions further, while ‘teams’ allow managing access for network users (e.g., other household members or employees) and their client devices. Team members aren’t required to have AirZenIDs. Accounts can also be authorized to access other accounts; such accounts are called ‘partners’.

ACF-LOC: Location Management
Locations are not only the logical representation of a place of operation. They are used to connecting network resources and devices as well.
Simply creating a WiFi network has no effect until it is attached to a location. Similarly, Nodes must be assigned to a location as well. Otherwise, they will only connect to the Internet and run updates.

Most resources have some parameters that must be configured per location and some that apply to all locations they are assigned. For software bridges, it is possible to configure Ethernet ports down to the device level. For WiFi networks, only their bridge association is configurable per location.

ACF-NOD: Node Management
Because most configurations are associated with locations, the primary method to configure Nodes is by assigning them to a location.
When replacing a Node with another, the replacement of the physical object can be mirrored digitally as well, allowing the new Node to continue operation without the need for manual configuration. In order to be able to assign Nodes, they must be claimed by an account first. This is typically done by scanning a license key in the app that comes with a batch of Nodes. This allows the associated Nodes to be used inside the account.

ACF-WQC: WiFi Quality Control
WiFi quality control is based on connection scores. Scores are calculated on the Nodes using signal-related metrics.
The distribution of scores can be generated to judge the overall WiFi quality experience for a givenNode. Similarly, the scores within a location can be used to understand how the WiFi ‘feels' to end users.

ACF-SSP: Self-Service-Portal
Most IT departments are responsible not only for installing and operating equipment but for user management.
The self-service portal offered by AirZen enables end users to perform some of the more mundane tasks related to network access.

This is particularly useful if users aren't managed using a RADIUS-capable service or storing WiFi-related information with LDAP or AD is undesireable. The AirZen PSK technology is designed to make per-user provisioning feasible even in such cases, and the self-service portal can further reduce the workload for admins. There are different options to authenticate and authorize users: They can still have their access provision created manually by an admin. But, it is also possible to allow them to make a request granted by an admin receiving a push notification. Domain-based authorization of email addresses is also possible, as is LDAP authentication. Contact us if you want to use AirZen with a system that uses another mechanism.
Once they have logged into the portal, users can generate individual passwords for their allowed WiFis, manage their devices, or access other related resources – like a request form for home office equipment.

ACF-LMT: Licence-Management-Tool
Automated license management is likely not considered exciting by most admins, but it is useful to have under certain conditions.
When the installation is spread across different companies or there are tight bureaucratic requirements, managing contract parameters alongside billing information is a clear advantage.

ACF-SUP: Support-System & Tools
The integrated ticket system brings first-class connections with Nodes and client devices and includes a live chat that connects end users and network operators. Support cases can also be used to increase logging verbosity temporarily, for example, by including kinds of events that are ignored otherwise or by collecting data related to a specific end device. Logs are saved with the ticket and be viewed later. The AirZen App also provides a support function that can be used to diagnose

the user's device itself. For example, if users report that their connection is slow, a link can be sent to them identifying their device on the network while providing signal data from the device — or even generating or capturing data streams for diagnosis. To some degree, it is possible to guide the user through the first steps of creating a ticket with information that would otherwise have to be asked for later.
There will always be some problems that must be diagnosed live, and finding the time for both parties can be difficult. AirZen tries to rule out common issues early to free up resources both for users and operators.

ACF-WAN: SD-WAN
Software-defined networking stands for modular and flexible systems. SD-WAN is concerned mainly with connecting resources over the Internet.
In this context, AirZen offers multi-WAN routing with failover support for fibre lines, DSL, and WWAN.

ACF-SMW: Smart WiFi
Network cables might have significant advantages over WiFi but they are also a lot less practical when dealing with moving devices. Ultimately, WiFi is how most people interact with networks and AirZen has made it a core part of the platform, even though it is still possible to go without.

Starting in 2022, all AirZen Nodes will support WiFi 6 or WiFi 6E, bringing significant changes that improve the overall experience. For example, most devices have two radios to operate on multiple bands at once.

Roaming is another essential feature that heavily influences the WiFi experience. Traditionally, the access point infrastructure tries to 'steer' client devices from one access point to another, but the more modern approach enables end devices to make better roaming decisions by enhancing their information. All Nodes communicate on the local network using IPv6 multicasts to have the necessary data when informing devices about neighbouring WiFis (802.11v). The "Fast Transition" (FT) is a sped-up version of the WiFi handshake, and it is enabled automatically depending on the SSID (802.11r).

Frame protection (802.11w) is an option to encrypt management frames. The primary use is to prevent disassociation attacks. Unfortunately, some clients don't support it, and it slows down the connection process. It can be configured per SSID and is enabled by default.

When installing Nodes, the signal coverage areas often overlap with those of foreign access points. Therefore, access points should be spread out across the available channels to reduce interference. It is possible to either assign channels manually or enable the automatic channel selection by setting an interval in the radio configuration. The automatic channel selection setting is ignored for radios within a mesh network. Here, the first available channel is used. You can configure multiple channels to limit the selection of channels to choose from, or else, all channels supported by the individual hardware will be used. In very dense installations, however, the automatic channel selection can cause instability.

Client isolation is enabled automatically depending on the setting of the bridge.
WiFi authentication is possible using either PSK (WPA2/WPA3) or EAP (WPA2/WPA3) using RADIUS (802.1x).

ACF-MES: MeshNode Technology
For small stores or homes, installing cables and drilling holes can be a liability. In some industrial applications, it is outright impossible. The AirZen MeshNode Technology can gap small distances and increase coverage - only requiring a power source. It can be used on mediums like VPNs, Ethernet cables, fibre lines, and WiFi, making it a powerful and versatile tool in environments where running a cable would otherwise be necessary.
The Airzen Mesh creates a virtual Ethernet network (OSI layer 2) using underlying Ethernet links. On the outside, the collective of mesh nodes behaves

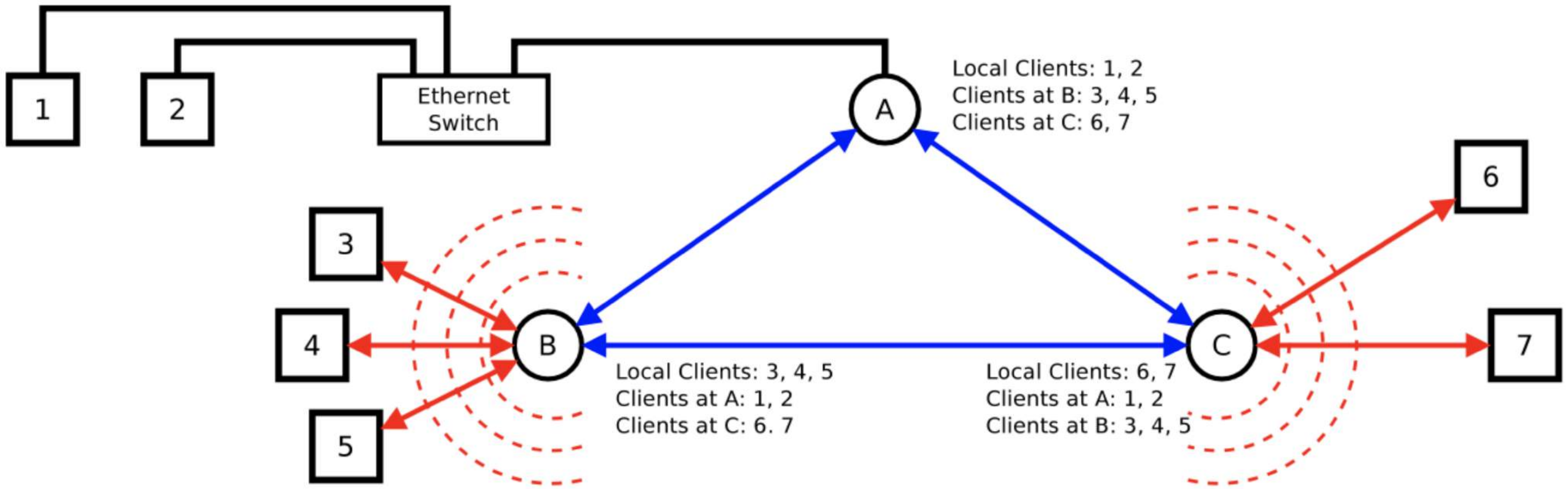
like a giant distributed switch. However, inside the virtual network, each Node is effectively a small virtual switch that keeps track of its neighbours, multicast traffic, and VLANs while permanently negotiating with its peers the optimal routes to any specific MAC address.

Mesh Setup Example
A typical application for the AirZenMesh is a wireless extension for small networks with little infrastructure. Within the configuration, a 'mesh' port is added to the network to be extended – most likely the one used to access the local gateway. All mesh nodes must operate the mesh SSID on the same channel. Reducing channel overlap isn't possible on mesh nodes without using a dedicated radio module. By default, the mesh SSID is active on the first 2.4GHz radio.

At least one of the mesh nodes is connected via Ethernet cable to the Internet uplink router or a switch. The network can then be extended by placing additional mesh nodes within the wireless range of the already established SSID. It is important to consider that in order to be able to connect to the encrypted mesh network, the nodes need to learn the key before they can join.

Typically, nodes are first assigned to the location and then connected to the Internet via Ethernet cable for a few minutes to receive their configuration before it is installed.

The Ethernet ports of remote nodes can be used to attach cable devices like printers or sound systems. It is also possible to disable the Ethernet ports on those nodes.



ACF-LOR: LoRa
In the future, the AirZen ecosystem will be extended using LoRa-capable devices and modules (2023/2024). Through LoRa, the AirZen Generic Network Controller System will also support applications requiring long range,low power, and low bandwidth.

ACF-VPN: VPN Engines
The AirZen platform supports a variety of VPN technologies suited for three broad categories of applications:

- redirection of Internet-bound traffic
- cross-site networking
- connecting to a network from a remote location

Redirecting Internet-bound traffic is often done for legal reasons - to an observer on the Internet, traffic originates from an AirZen VPN gateway instead of a client's network. Another reason might be the need to adhere to security requirements on the local network that are undesireable for guest networks. For these applications, encryption is likely optional, as the traffic inside the tunnel will be sent verbatim by the gateway anyway.
It is often helpful to terminate the VPN on each node instead of a central gateway so that the computer power required for the tunnelling scales within the covered area. Occasionally, a carrier imposes restrictions that prevent the use of established protocols like IPsec or Wireguard.
Like most settings, VPNs are configured per location on a network level. The AirZen Dynamic Network Controller generates the configuration for individual nodes. Then, a node is simply attached to the corresponding location to add a new VPN gateway. This is more time-efficient than configuring individual appliances - especially for huge installations.

ACF-PWG: Public WiFi Portal
The Public WiFi Portal is covered in-depth in a dedicated white paper. What follows is an overview of technical details.
The 'portal' option is available for gateway networks. When it is active, Nodes will hijack TCP connections on port 80 and redirect it to a local portal daemon listening on port 81. Additionally, CAPPORT-related options for IPv4 and IPv6 addressing are used to direct clients to an encrypted socket listening on port 441. The local daemon collects the network ID and the MAC address, combines both into a 'v-hash' using SHA256, and redirects the client to a centrally hosted portal server. The Node uses a hostname comprised of 'node-' followed by the hostname of the portal server. This hostname must be a CNAME of the portal server hostname.

The certificate for the encrypted socket is supplied by the portal server above alongside an OCSP package to allow verification before Internet access has been granted.

The server renders the UI of the portal. A portal's main components are the elements/pages and routes. Elements are waypoints for portal traversal. Pages are elements that are shown to the user. Each can contain a basic user input element, text, and an image. In addition, elements can have routes that determine the next element using a priority and a condition. Conditions are LUA expressions that are checked in order of priority and, depending on their Boolean value, determine whether the route is taken. These LUA expressions have access to user input and internal data related to the session but not to any external resources. To access those, it is possible to assign webhooks to elements. A webhook must return a JSON object, and the contained values will be attached as session data.

One possible application is sending a code to an email address; the code can be checked in a routing condition or displayed on a page.
Another application might be a portal that helps users to generate a password for another network.

AIRZEN PROTECTION FRAMEWORK

APF-SBD: Security by Design

There should be no need to mention it, but AirZen solutions are designed with an attacker in mind. For instance, adding a new ZenPSK device is only possible for a short time after viewing the password. Access authorization for API resources is enforced in the request router. Applications typically only cover a few functions related to their primary domain.

APF-SUO: Security Updates OverNight

Regular updates are considered a good security practice because of one perfect reason:
A patch for a security vulnerability is also a release of knowledge about a potential exploit. In fact, most successful attacks rely on well-known exploits against out-of-date software.

AirZen Nodes will look for an update once a day at a specified time - usually very early in the morning. Only the core configuration is carried over during the update, and all other potential modifications are discarded.

APF-ZSK: ZenPSK Technology

Typically, there is no way to use a personalised passphrase with WPA2- or WPA3-PSK or revoke access for a particular user. The standard way to enable these features is by using enterprise authentication (WPAEAP), which involves connecting the WiFi system to a company's LDAP infrastructure using RADIUS (see AOS-OF).

This is not always desirable - there might not even be such infrastructure. Even with an enterprise setup, users might still want to access the network using different devices or to be able to manage their devices.

For a proper setup, the RADIUS server's CA certificate must be installed on end devices. Other PSK-only solutions exist, but they might also require using RADIUS to find the passphrase belonging to a particular MAC address. Those that do not still require knowledge of the end device's MAC address to create a provision. It is not only challenging to obtain the MAC address in advance for private devices, but modern WiFi clients also randomise the MAC address per SSID.

AirZen ZenPSK addresses the difficulties by dropping the RADIUS requirement and allowing the creation of provisions without immediately attaching a MAC address. Instead, users and devices are stored within the WiFi configuration. That not only means an AD outage won't take down the WiFi, but it enables their provisions to be managed by AirZen software.

For that to work, AirZen implements a new way of onboarding new devices (learning the MAC address of a client device): A provision must be enabled for first-time use. After it has been enabled, the associated passphrase becomes available for use with any device for a limited time. Then, when a device joins a network using that passphrase, its MAC address is associated with the provision.

There are different ways to allow users to obtain their passphrase and start the onboarding process. Instead of the passphrase, admins can send personalised URLs to their users. These URLs can be used to connect devices up to the number configured. Alternatively, users can also create their provisions themselves using a configurable process.

A constraint of ZenPSK is that only a limited number of devices can be in the "enabled for first-time-use" state before clients start to see timeouts during their initial connection. That is simply because the Node must test the cryptographic handshake against the list of eligible passphrases. The Node's processing power influences the limit, but ultimately, the handshake was designed to be time-consuming to make it more secure. The Node will continue to find the match in the background so that the next attempt by the same client should succeed.

Under normal conditions, around 100 devices can be in the onboarding state simultaneously before the constraint is noticeable. If that becomes a problem, it is possible to shorten the time window during which the initial login is possible (30 minutes by default).

APF-MWB: WatchDog BotNet & Malware Blocker
On gateway networks, there is an option to block connections to hosts known to be operated or taken over by viruses or malware. This measure is no replacement for protection on the end device. It should be considered an 'extra', but it can be useful in some scenarios.
When the option is active, latency will increase a little on all gateway networks.

APF-SSE: Guest Session Engine
The Guest Session Engine is a distributed system that runs on the AirZen Nodes and the backend. When a client joins a guest network, and the Node does not know of an active session for that MAC address, it will be redirected to the captive portal using a "v-hash" computed using the network ID and the MAC address of the device. The MAC address does not leave the Node for data protection reasons. It is still possible to fulfill law enforcement requests for a given MAC address and network by computing the v-hash.

The captive portal looks up the v-hash in a temporary session store and, if there is an active session, tells the node about it so that the client can be activated for the remainder of the session duration.

If the client is unknown, a new session is created, and they will have to complete the customizable captive portal process to activate their session. When a Node is notified about an activated session, it broadcasts the session information to other Nodes on the local network to improve the roaming experience (this requires local IPv6 broadcasts to work).

APF-CFR: Public WiFi Content Filter
When forwarding Internet-bound traffic, it is only a matter of time before a device sends unwanted traffic. That could be an infected phone of an employee or a guest abusing the free WiFi.
While AirZen believes that the Internet should be as open as possible, some things can easily be blocked without disturbing legitimate use cases, like unencrypted SMTP traffic. Because of that, guest network firewall rules are enforced on AirZen gateways. In addition, gateway networks for Nodes have a corresponding option to use the guest firewall rules with other gateways or drop traffic early when managing bandwidth use.

This baseline defense is necessary to guard against traffic that could otherwise trigger a response from the ISP or a government institution. However, it does not generally protect against criminal activities as they are impossible to protect against reliably, and the countermeasures almost always affect legitimate traffic, e.g., VPNs.

CLOUD-SERVICES

ADC-CON: Configuration DataBase
This relational database is used for storing any configuration required to configure a Node. Relations between entities are constrained so that most semantic errors don’t need to be handled on end devices but are immediately visible when changing a setting.

ADC-SUD: Status DataBase
To speed up queries about network state, the status database caches information about Nodes in RAM. Without it, a simple client overview would require contacting all relevant Nodes, which is much slower and less reliable.

ADC-VNE: VPN-Controller & Endpoints
Writing software just to maintain a few VPN endpoints might seem excessive, but it has proven to be of great help. A VPN endpoint should have good connectivity to its clients and be easy to replace.

The VPN controller helps to achieve that by operating a DNS server fuelled by a transactional database. In addition, the DNS server and client-facing API are also used to improve connectivity from restricted networks.

AIRZEN IDENTITY

AirZen is a manufacturer of European, innovative, high-quality and easy-to-use network solutions. Our pioneering Network-as-a-Service approach strengthens IT security and sustainably optimizes IT management to ensure maximum customer benefit.

Responsibility is the guiding principle for the development and deployment of AirZen products and solutions, with a focus on security, reliability, and performance.

As a manufacturer, we value direct collaboration with customers as well as partnerships with experienced IT partners. AirZen offers comprehensive solutions comprising proprietary hardware and software components.

For more information and contact details, please visit www.airzen.io.

AirZen Networks Lda.

Avenida Arriaga 30 / 1A
9000-064 Funchal
Madeira / Portugal

business@airzen.io

www. AirZen.io

AirZen reserves the right to make technical changes to the product specifications and features contained in this document, such as in the course of further product developments. Some information provided here may be outdated, inaccurate, incomplete, or misleading and is provided without warranty; errors are excepted.