zAccess

KEY FEATURES

ZTNA solution from AmZetta
Access to network resources is based on ZTNA principles.

Flexibility
Network resources can be in the Cloud, on-prem or hybrid.

IdP Integration
Supports integration with various popular IdPs like Microsoft AD, Google etc.

Product Overview

zAccess is a Zero Trust-based Network Access solution from Amzetta that enables secure enterprise mobility and seamless access to corporate resources like applications, servers, desktops, and network services from any device, from anywhere, across any network. Whether users connect via a trusted LAN, an untrusted WAN, the internet, or a mobile network, zAccess ensures safe access to corporate resources. It applies the principle of least privilege, providing users with only the access they need based on their roles and responsibilities.

zAccess continuously monitors and audits user activity in real-time to detect and respond to potential threats, while enforcing detailed access policies based on factors like user identity, device health, and location to enhance security and mitigate risks.

zAccess Components

• Director

This component is the centralized management interface which control and manages underlying networks, end user clients' connections and gateway routers

• zAccess Gateway

This component serves as a data path gateway into protected resources. All access Control for data traffic is enforced in this component.

• Client

This component will be installed directly into end users' device, and it is responsible for providing app access with zero-trust based access controls. Clients are available for Windows 10/11, IoS, Android, MacOS and Linux.

• Connectors

This component can act as a data path for any resources that are not part of the zAccess Gateway's network. This acts like a proxy for both cloud and on-premises resources.

Is your company equipped with zAccess ZTNA solution from Amzetta?

A short list of common cybersecurity issues zAccess will address:

Lack of Perimeter Security

Traditional security models are built on the concept of a "perimeter" where everything inside network is considered trusted. This perimeter becomes harder to define and secure with increasing adoption of work-from-anywhere policies and with the increasing popularity of SaaS.

Insider Threats

Traditional security models trust users and devices once they are inside the network. This can lead to data leaks, unauthorized access

Managing complex Access Control

Traditional network models have a hard time providing access controls for users, consultants, devices and apps. This often leads to granting excessive privileges and consequently causing higher security risks.

Monitoring Device Posture

Legacy system often lack the ability to continuously track user activity and device posture.

Features

• zAccess Deployments

zAccess supports both Cloud based deployments and on-premises deployment.

• IdP with MFA Support

zAccess has an inbuilt IdP called zID for local users and it also supports user federation with other popular IdP like Microsoft Active Directory and Google. It has an inbuilt MFA support through TOTP using Mobile authenticators.

• Auditing and Logging

zAccess provides logs on user logons and other user activities. It also provides logs on Time of access, username, MAC address, and IP address of endpoints. It also provides Application network activity.

• Device Posture

zAccess collects various endpoint device details for providing ZTNA based access control. Some of the data parameters include

- zAccess Client Version
- MAC address of endpoint Device
- Serial number of the Device
- OS process and registry check
- Antivirus and Firewall check
- Hard disk encryption check
- Secure boot

• Tunnel Support

zAccess supports UDP based Wireguard tunnels, This enables better speed combined with higher security.

• Policies

zAccess policies define which applications or application groups users are allowed to access. These applications could be cloud-based, on-premises or hybrid resources.

• RuleSets

zAccess rulesets are preconfigured conditions that help the system decide what level of access to grant. These rules are typically set based on various criteria like user attributes, Device attributes, and Network context.

• Endpoint Clients

zAccess supports the following Clients.

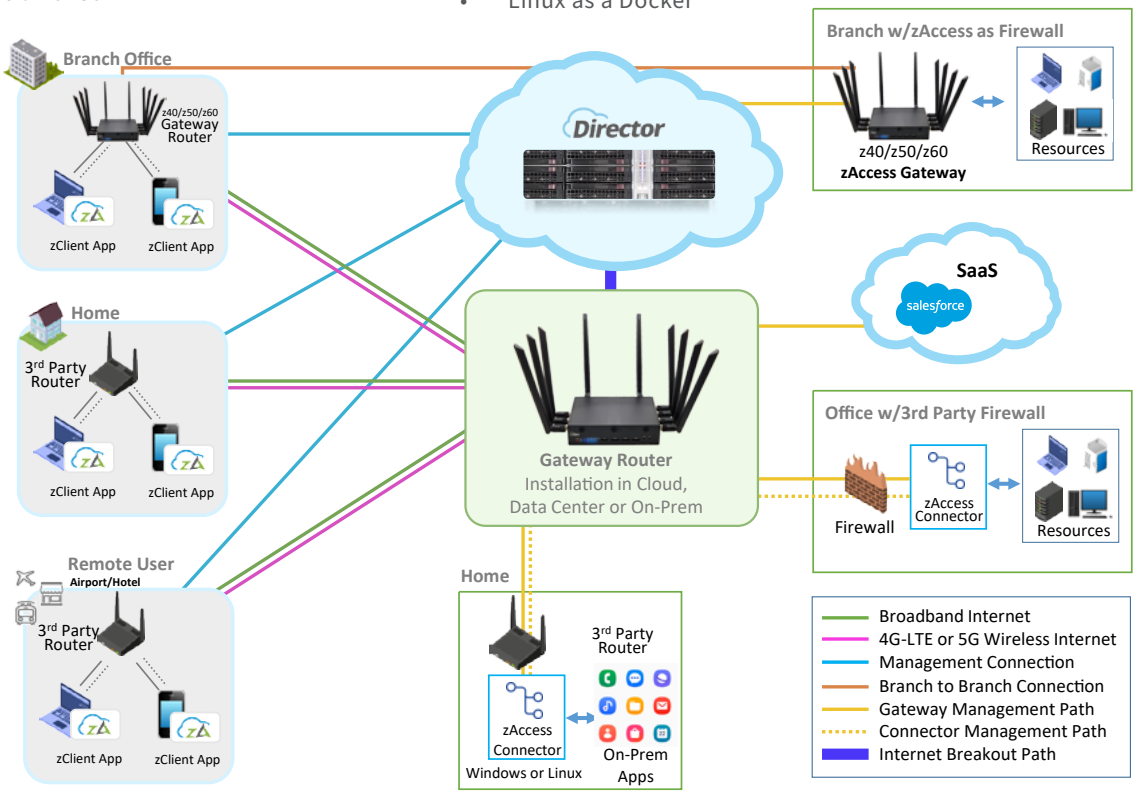
• Windows • MacOS • Android • iOS

• Connectors

zAccess Connectors can be installed in the following Operating systems.

- Windows as a standalone installer
- Linux as a Deb package
- Linux as a Docker

zAccess Architecture



AMZETTA.COM