zGateway

Secure Application Access

KEY FEATURES

SECURE ENTERPRISE MOBILITY

Gain complete control over which devices can connect to the corporate network and hosted applications

SANDBOX SECURITY

Enable clipboard, printing functions, desktop session recording, file saving, USB devices and more

SEAMLESS INTEGRATION

Compatible with VMware and Microsoft hypervisors and supports Windows, Mac, and Linux environments

PRODUCT OVERVIEW

AmZetta zGateway is an application access gateway that enables enterprise mobility and secure access to corporate applications, desktops and network services from any device working from any network. zGateway enables users working from any network, be it trusted LAN, untrusted WAN, Internet or mobile network to securely access corporate resources. zGateway's SPAN technology makes secure access a simple, fast deployment without requiring complex network configurations. Users can access a browser, desktop client or mobile application and begin to utilize their corporate applications without any configuration required on the devices.

AmZetta zGateway combines the performance, simplified management and functionality required for enterprise remote access and reduces complexity and costs traditionally associated with traditional VPN solutions.

As an application access gateway, AmZetta's zGateway enables enterprise mobility, as well as secure access to your organization's network services, corporate applications and physical or virtual desktops from any user device and from any network. Through zGateway, users can securely access corporate resources from any trusted or untrusted LAN, WAN, Internet or mobile network. By removing the need for complex network configurations, zGateway can be easily deployed in virtually any IT infrastructure – giving users quick and secure access through zGateway's SPAN technology. Additionally, no user endpoint device configuration is required for users to begin accessing applications through a browser, desktop client or mobile application. AmZetta's zGateway provides the simplified management, user performance and functionality to meet and exceed corporate requirements for remote access while simplifying setup and reducing the costs that are typically associated with conventional VPN solutions.

Are You Really Protected?

VPN + +

Common Vulnerabilities

VPN Issues
Secure connections, such as through VPN, do not equate to secure devices

Security Risks
Standard VPNs often run browsers at low security, exposing networks to cyberattacks

Vulnerable Users
Vulnerable users expose entire corporate networks to external threats

FEATURES

SPAN Technology

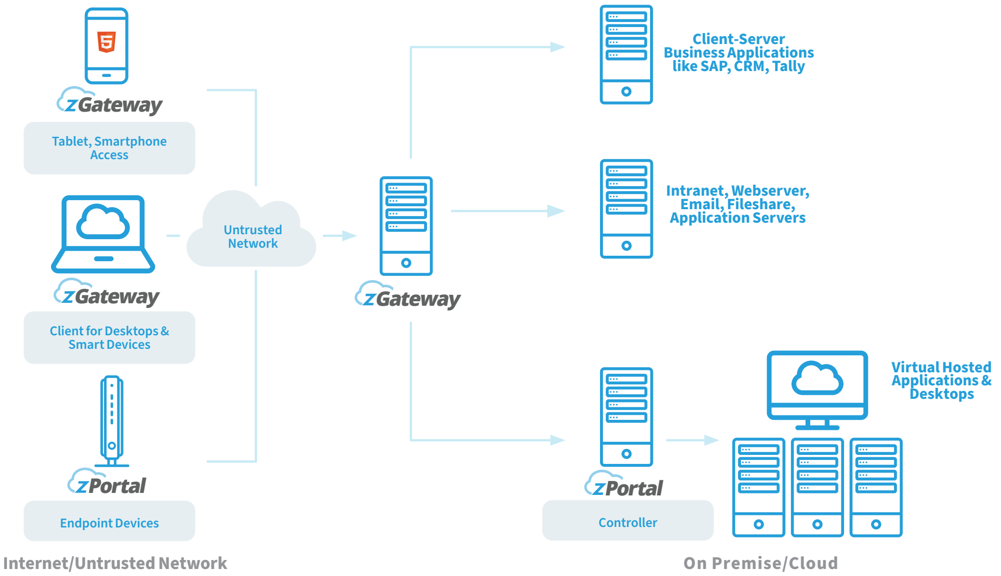
AmZetta zGateway's Secure Private Application Network (SPAN) technology delivers high performance and simplifies remote access deployment. SPAN technology makes access to business applications available to remote and mobile workers through any device without the need to install special network adapters or create complex network routing changes. Users achieve the highest performance, even when using high latency networks, and network security administrators maintain complete control over which applications are available to remote users with AmZetta SPAN technology.

Scalability

Anytime an end user is provided access to corporate resources and applications, organizations must evaluate the users' devices in order to scan and detect malicious viruses and determine a trust level for that device. zGateway governs the endpoint device and ensures the device is not compromised or becomes compromised during session with the corporate resources based on the trust level of the device. zGateway has the ability to restrict internet access as well as determine the location of a users' device and deploy different policies based on location.

Authentication, Authorization Auditing

It is paramount to secure corporate applications with a strong authentication layer prior to exposing them to untrusted networks. AmZetta's Multi-Factor Authentication (MFA) software, called zMFA, is an optional add-on software to zGateway which guarantees that only authorized users can access the applications. zGateway provides a flexible and multi-layers authorization framework. This allows enterprises to control access to corporate applications based on a multitude of parameters. zGateway provides the ability for IT administrative personnel to gain insight into what users access which applications and when – all through the intuitive management interface.


zGateway
Tablet, Smartphone Access
zGateway
Client for Desktops & Smart Devices
zPortal
Endpoint Devices
Untrusted Network
zGateway
Client-Server Business Applications like SAP, CRM, Tally
Intranet, Webserver, Email, Fileshare, Application Servers
zPortal
Controller
Virtual Hosted Applications & Desktops
Internet/Untrusted Network
On Premise/Cloud

FEATURES

Anywhere, Anytime Computing

zGateway provides end users with a single window where they can choose from a listing of applications available to them. This provides a seamless experience for the user as well as reduces the number of support calls to the IT team. zGateway provides a web portal to end users where business applications can be accessed. When paired with zBrows, zGateway can deliver any Microsoft Windows- and Linux-based virtual hosted applications and virtual desktops to end users in a secure sandbox environment. The zGateway client for desktop provides power users and locally-installed applications to access the applications. zGateway can operate on machines without administrative rights and also supports automatic updates when new versions are available. There are no pre-configuration requirements with the zGateway client

Secure Enterprise Mobility

zGateway utilizes strong and current TLS protocol based data security and integrity for application traffic. Organizations can secure all business applications and make them available to end users without requiring any pre-configuration on end users machine with the zGateway solution. zGateway makes it simple for organizations to enable extranet users, vendors and consultants to bring their own device and gain access to applications.

Strong Endpoint Control

AmZetta's zGateway can scale to thousands of users to ensure required uptime for critical business operations through the built-in load-balancing and high availability features. Load balancing for incoming users, as well as application traffic, is included with the zGateway software to ensure that deployed hardware is effectively utilized. zGateway can be configured in DR mode with a client-side failover feature so that end users can always connect.

Secure Sandbox Computing

Organizations can create a secure sandbox for user computing by combining zGateway with zPortal. Users can be restricted to run limited applications or restricted from copying data from applications to local applications, or from taking the data out of their machine in the secure sandbox. zGateway provides control over clipboard, printing functions, desktop session recording, file saving, and USB devices in the secure sandbox. The secure sandbox can also self-adjust to automatically release restrictions if the user is working from a trusted location.

Strong Two Factor Authentication

Protect corporate resources with strong authentication with the zMFA multi-factor authentication solution which is an optional feature in the zGateway solution. Two factor authentication based on One-Time-Password (OTP) can be enabled in zMFA for zGateway logins. A user must login with an OTP received via SMS, Email, or using the AmZetta's zMFA Mobile Application. SSO for applications like Microsoft RDP Connections, SSH to Linux Server and zPortal, along with presenting OTP for login into desktops, servers and network devices can all be configured in zGateway

Application Support

- All web based, TCP and UDP based client-server applications
- Windows file shares and drive mapping
- Dynamic port based applications
- Publish Subnet or IP Range for network access
- Special support for RDP virtual channels
- Application server load balancing
- Session caching for load balanced applications
- Per application based compression switch
- MyDesktop for direct personal desktop access
- Terminal server application publishing via Propalms TSE , RDP & VNC
- zPortal VDI

Access Security

- TLS 1.0 and above
- Encryption: Strongest available: DES, 3DES, AES
- Authentication: SHA-2, RSA 2048/4096
- 4096 bit RSA key
- CA certificate support
- Internet network masking and IP address/ hostname mangling
- Application level gateway and not layer 2 bridging
- Hardened gateway operating system
- Split & Full tunnel modes
- Secure sandbox computing
- DDOS Protection

Management

- Web based management console
- Dashboard with graphical reporting
- Menu driven console interface for system configuration
- Wizard driven installation procedure
- Self-signed certificate generation
- CLI
- Delegated administration
- Certificate based strong authentication for administrators
- Inline help

Authentication

Authentication based on:

- User identity, OU/group/realm
- Static passwords, OTP – dynamic passwords
- Certificates
- Device signature: CPUID, HDDID, IMEI, more
- User location, MAC ID, IP Address
- Endpoint security trust level

Two Factor authentication:

- Certificates, Device Signatures
- One Time Passwords (OTP) : SMS/Email/ Hardware/Software Token
- Local database with full customization per user, password policies, password reset support
- RSA Secure ID or any 3rd party OTP server
- Integrates with AD/LDAP/RADIUS
- Fully integrated client certificate based two factor authentication server with automatic CA and certificate provisioning through zMFA*
- Email based user provisioning
- Support for multiple authentication servers with cascading mode
- Realm based multi-organization support

Authorization - Application based access control

Application based access control Access control based on:

- Device identity and profile
- Endpoint Security trust level
- User Authentication method
- User Role
- User's organization
- User's location
- Dynamic policy evaluation based on run time information about device, authentication method and user role
- Display of allowed applications and availability of the application server to users
- Time based restriction policies
- Scheduled account expiry
- Block specific groups
- Multiple VPN Domain based control
- Control User's Internet access
- Support for external authorization servers
- Automatic fetching of group information from AD/LDAP/RADIUS

Endpoint Control

- Strong device identification based on 20 parameters includes CPUID, MBID, HDDID, MACID, IMEI No. and more
- Detect managed and unmanaged devices
- Login control from managed and unmanaged device
- Support for checking for antivirus, firewall and antispyware products

Real time status check for:

- Last update time
- Real time protection check
- Application control based on device profile
- Mandatory profile for nonavoidable policy checks on all endpoints
- Quarantine profile for devices that fails all other profile
- Secure endpoints from attacks over Internet or becoming a proxy for attacks
- Restrict Internet access of the user based on policy
- Restricts users from leaking data using clipboard, printing, USB devices

Auditing

Information logged includes:

- Time of access
- Username, domain
- MAC Address of endpoint
- IP address of endpoint
- Application accessed
- Device profile
- Complete reporting of user logons and activity
- Detailed logging of endpoint security scans results
- Extract logs in CSV format for feeding to third part report generation
- Search logs
- Auto-archiving of logs
- Monitor and disconnect live users
- Alerts on new device registrations, user account lockouts
- Reporting on domain wise access, applications accessed, failed login attempts, concurrence graph

Access Modes

Multiple access modes:

- zBrows portal for clientless access*
- Portal with java applications
- Agent based access from any browser
- Full access client for desktops
- iOS & Android app

Client platforms supported:

- z Windows 7/8/10
- Windows server 2003/2008R2/2012R2/2016 Linux OS , MAC OS X
- iPad / iPhone / Android Access
- No configuration required on end user machines
- Site to site access
- zBrows: Access on any device with a HTML5 browser: Blackberry, Windows Mobile, iOS etc.*

*Additional License Required

Deployment

- Scalable to thousands of users
- Active-Active N+1 cluster
- SSL connections load balancing, multiple algorithms
- Application connection load balancing
- Session persistence: Users do not need to re-authenticate
- ISP load balancing for incoming connections
- Client side failover using Alternate gateways
- Runs on hardened Linux based platform
- Menu driven console interface for easy configuration