Cryptzone™

DATASHEET

AppGate

Context-Aware, Secure Access for Third-Party Users

KEY BENEFITS

- All access blocked until third-party users are authenticated and rights are confirmed
- Secure connections are established for each authorized user
- Single, centralized logging of all application traffic, per user and per device, enabling a comprehensive digital paper trail for audit, compliance and forensics
- By detecting any unauthorized packets from an authorized client device, AppGate can immediately block malicious traffic and feed alerts into a SIEM or IDS. This enables faster response to malicious activity with fewer false positives
- Non-authorized services and resources are invisible, reducing attack surfaces by as much 95%
- Third-party users can access only resources they're entitled to
- Support external users without changing internal directories
- Secures internal and external access to on-premises and cloud-based resources
- Reduces cost, complexity and effort for configuring privileged user access

Easy Entry Points

You can count on cyber criminals to look for the easiest entry points into your network. They've discovered and continue to find that third-party vendors, service providers and partners often have extensive access to enterprise networks. By stealing credentials from them, they can acquire personal information, intellectual property and other data worth billions.

Several high profile data breaches have been linked to the supply chain and third-party accounts, which have proven easy targets for hackers. While you can keep tight controls on your own internal security practices and technologies, it's impossible to manage the security practices of your suppliers and partners.

Third parties will have their credentials stolen and their networks breached. In turn, this malicious access will be used to compromise your network. While working with each of your third-party vendors to help them boost their security profiles may be a noble goal, it won't be easy to implement. You could for instance require third parties to use stronger credentialing including two-factor authentication such as one-time password solutions (OTP). Current best practices also call for, among other measures, deploying next-gen firewalls, intrusion protection/prevention, SSL VPNs, IPsec and monitoring behavior patterns of all users. These technologies can help but too often result in third parties having far greater network access than is required.

What's missing from traditional security methods?

Third parties responsible for system support, development and/or maintenance can introduce security deficiencies exploited by attackers, so doesn't it make sense to put iron-clad controls over what they can access, when and from where?

Organizations have tried and largely failed. What's missing up until now are access controls that take user, role, and context (device, location, time) into effect and limit network access and visibility to only those services that are required by that specific user before access to precious resources and sensitive data occurs.

Dynamic, Context-Aware Third-Party Access Management

AppGate operates under the premise that users should never be entrusted with access to, or visibility of, resources that lie outside of the scope of their responsibilities. It dramatically simplifies the third-party user access problem and eliminates over-entitled network access, drawing on user context to dynamically create a secure, encrypted network *segment of one* that's tailored for each user session.

AppGate, a Software-Defined Perimeter (SDP) solution is a distributed, dynamic and scalable platform for fine-grained access control. It draws on user context to dynamically create a network *segment of one* that's tailored for each user session and hides all network resources - servers, services and applications - except those that the third-party user is authorized to see. By making

the rest of the network invisible, enterprises can simplify their security infrastructure, while granting access with confidence. AppGate provides real-time, user-centric access, enforces the principle of least privilege, and easily controls access while maintaining a strong security stance. AppGate is an enterprise-ready solution with platform maturity enabling production-ready deployment.

Centralized logging and alerts of all access attempts provide a comprehensive digital paper trail for audit, compliance and forensics. AppGate can, for instance, send an SMS message whenever a third party logs in. Seamless integrations, including those with SIEM and IDS systems, build bridges among security tools and further enable consistent compliance reporting across on-premises, hybrid and cloud infrastructures.

AppGate helps secure third-party user access with greater control than ever before, simplifying deployment and management, and provides comprehensive reporting and audit functionality to protect against insider and advanced threats.

Summary

Attackers will defeat perimeter defenses. The key is controlling access to network resources based on user, role and attributes (device, location, time) and then limiting access by abstracting applications and resources from the underlying physical infrastructure, ensuring that all resources (whether on-premises, private or public cloud) remain invisible until authorized.

AppGate's user-centric, role-based solution enforces strict access controls without preventing third-party users from using a variety of devices and working practices, perfect for today's distributed environments. AppGate increases scalability, reliability, and high availability, enabling enterprises to achieve the best of both worlds - fine-grained access control per user, and superior performance and reliability.

How It's Done

1. User presents Single-Packet Authorization key in order to establish connection to the Controller, and then authenticates

2. Controller applies policies based on the user's role and context, and issues a signed token listing the user's access entitlements

3. User attempts to access a protected resource behind a Gateway

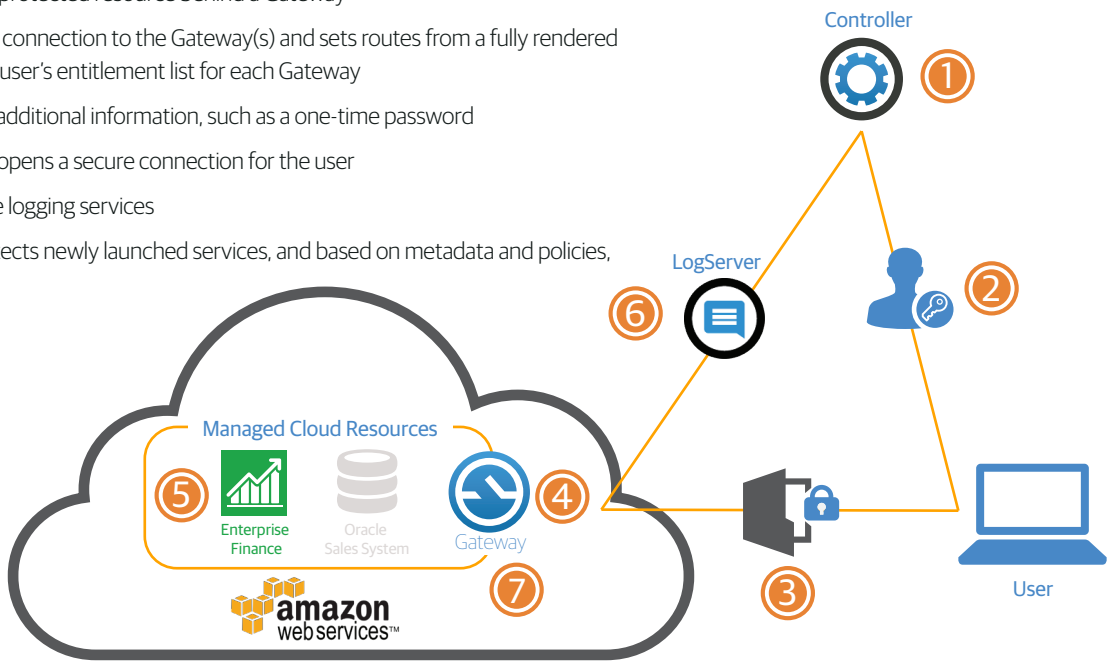
4. Client establishes a secure connection to the Gateway(s) and sets routes from a fully rendered firewall ruleset based on the user's entitlement list for each Gateway

Users may be prompted for additional information, such as a one-time password

5. If permitted, the Gateway opens a secure connection for the user

6. LogServer provides secure logging services

7. Gateway automatically detects newly launched services, and based on metadata and policies, adjusts user access



About Cryptzone

Cryptzone reduces the enterprise attack surface by 99% with its secure network access solutions. Using a distributed, scalable and highly available Software-Defined Perimeter model, Cryptzone protects applications and content from internal and external threats while significantly lowering costs. In cloud environments including AWS and Azure, Cryptzone provides user access control, increases operational agility and improves the ability to meet regulatory and compliance standards. More than 450 companies rely on Cryptzone to secure their network and data.
For more information visit www.cryptzone.com.

Cryptzone™

Americas +1 888 272 2484 | EMEA & APAC +44 118 900 1236 | www.cryptzone.com | sales@cryptzone.com