Cryptzone™

DATASHEET

AppGate

Context-Aware, Secure Access for Privileged Users

KEY BENEFITS

- All access is blocked until 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
- Client communications are encrypted
- Non-authorized services and resources are invisible, reducing attack surfaces by as much as 95%
- Privileged users can access only authorized resources
- Secures internal and external access to on-premises and cloud-based resources
- Reduces cost, complexity and effort for configuring privileged user access

Traditional network security fails to secure privileged user access

Traditional methods of securing networks are simply inadequate for privileged users. Due to their powerful entitlements, privileged users require strict access control and management. Traditional security methods such as Next Generation Firewalls (NGFW), Privileged Access Management (PAM), VLANs and NAC fall short. They don't provide fine-grained access control and do not consider the user's role and attribute-based context. For example, a privileged user's device type and their location must be considered in real-time. Not all information should be accessed anytime or anywhere. In addition, traditional tools lack the ability to centrally log all access attempts across on-premises, hybrid and cloud infrastructures, making it difficult to create a comprehensive digital paper trail necessary for audit, compliance and forensics.

Are attackers lurking in your network?

Once attackers slip through network defenses they become trusted users who gain a foothold in otherwise secure environments, including unsecured ports or management tools, such as jump hosts. Ultimately attackers will obtain privileged user access.

Dynamic, Context-Aware Privileged Access Management

AppGate operates under the premise that privileged users should never be entrusted with access to, or visibility of, resources that lie outside of the scope of their responsibilities. AppGate dramatically simplifies the privileged 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 privileged 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.

Seamless integrations, including integrations with SIEM and IDS systems, build bridges among security tools and enables efficient and consistent compliance reporting across on-premises, hybrid and cloud infrastructures. It also immediately blocks malicious traffic, perfect for intercepting would-be privileged user lookalikes.

Summary

From enterprises on-premises or hybrid environments to complex, multi-tenancy cloud infrastructure-as-a-service environments, AppGate controls privileged user access while reducing cost and simplifying deployment and management, and provides comprehensive reporting and audit functionality.

AppGate creates secure, service-specific tunnels to authorized resources and it provides complete visibility of all users' actions. Most important, non-authorized resources are invisible and inaccessible. AppGate increases scalability, reliability, and high availability, allowing enterprises to achieve the best of both worlds - fine-grained access control per user, and superior performance and reliability. Isn't it time your organization adopt a modern approach to securing privileged user access?

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

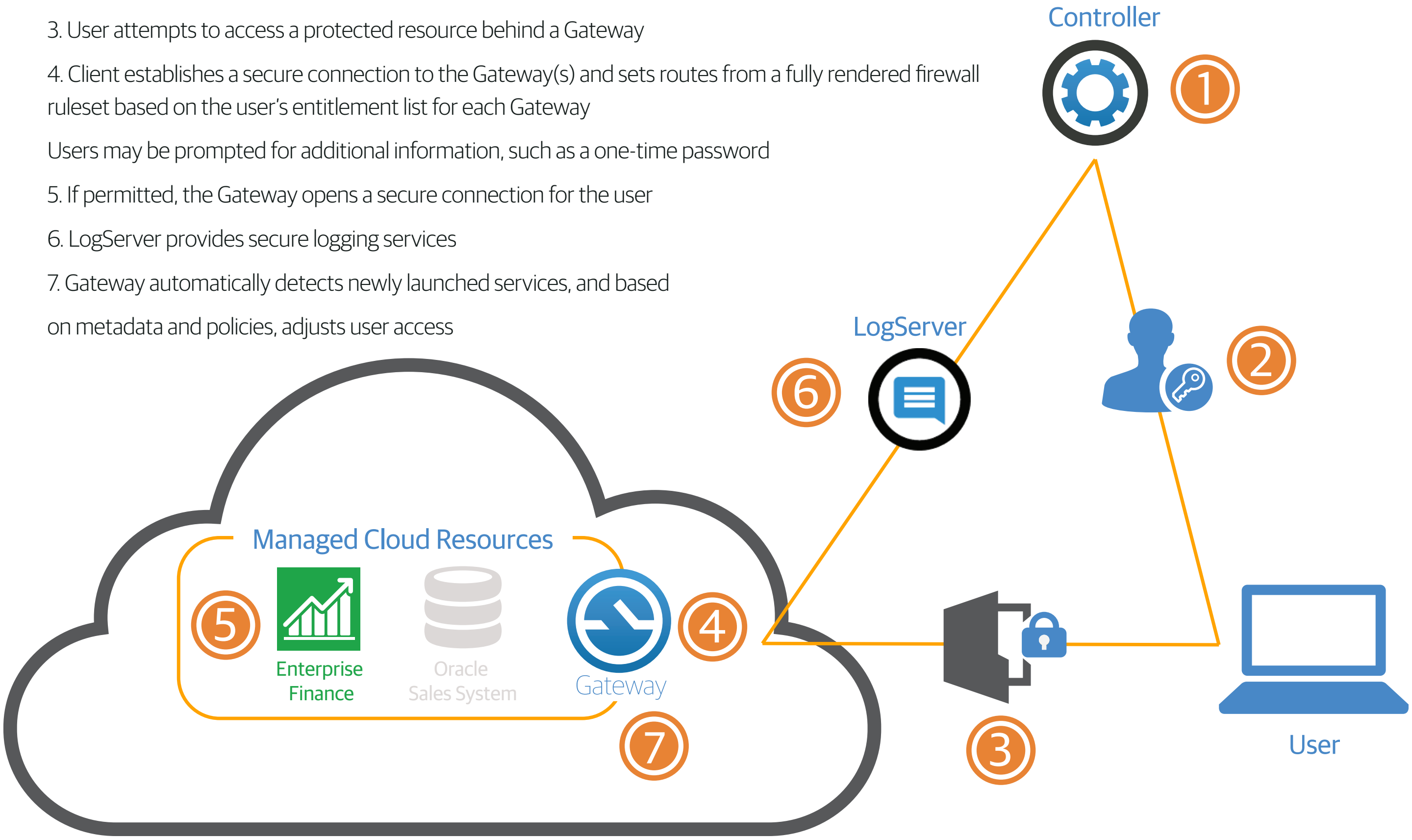
4. Client establishes a secure connection to the Gateway(s) and sets routes from a fully rendered firewall ruleset based on the user's entitlement list for each Gateway

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.