Cryptzone™

DATASHEET

AppGate®

Context-Aware, Secure Access to IaaS Resources

IAAS: SPEED AND COST ADVANTAGES

In the past few years, enterprises have rapidly embraced the Infrastructure as a Service (IaaS) model for developing, building, and deploying enterprise applications. Whether deployed on-premises as a private cloud, or leveraging a public cloud infrastructure, the benefits are undeniable: highly-scalable, on-demand compute and storage resources, nearly unlimited flexibility of the virtualized network environment, and a cost model that shifts from heavy up-front capital expenditures (CapEx) to "pay as you go" operational expenditures (OpEx) which better aligns cost and value. And, in the case of public cloud, the ability to eliminate on-premises datacenter costs for real estate, electricity, and cooling are an added benefit.

While the ride may not always have been smooth or easy, many organizations are now successfully using IaaS, and in fact some have made the strategic decision that all new applications must follow a "cloud-first" model. And as more businesses embrace the DevOps methodology, maintaining secure access control and compliance can become more complicated.

The Cloud Brings Risks and Requires Hard Work

The reality is that a move to cloud (either private or public) brings risks with it, and requires security and compliance teams to work harder to keep up. While cloud infrastructures such as Amazon Web Services™, Microsoft Azure®, and VMware® each have their own network configuration and security models, the reality is that these aren't designed to provide fine-grained access controls, or to adjust user access based on cloud server instance changes. Like traditional on-premises network security tools, these cloud systems only manage access to entire server groups based on source IP address or subnet, not based on individual user context. The result is over-privileged network access for users.

Dynamic, Policy-Based Cloud Access Control

In contrast, AppGate, a *Software-Defined Perimeter* (SDP) solution, 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 cloud resource 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. Individual network routes are created for each user, based on authorized entitlements.

AppGate provides layered defenses for managing IaaS user access that are easy to deploy and begin with strong identification using two factor authentication, such as one-time passwords (OTP). It then creates secure, encrypted, service-specific tunnels to authorized applications and resources based on dynamic context-aware understanding of factors including user, role location and device – and most important – it ensures that all cloud resources remain invisible until authorized. Firewall rules aren't written once and saved forever, but are created and enforced in real-time when access is requested. AppGate creates completely isolated management or service networks to micro-segment network access. This provides a secure, encrypted, service-specific connection to each individual application or service. And single-packet authorization provides enterprises with the ability to hide all AppGate services on the network from unauthorized users. This approach enables secure deployment of SDP on public-facing networks, which in turn protects and isolates all types of services from what Gartner terms "the internet cesspool". And it automatically detects changes to the cloud environment (such as new servers being instantiated), and adjusts user access according to policy. 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.

Managed Cloud Services Providers

AppGate is also designed to meet the needs of managed cloud service providers – whether offering such a service within an enterprise, or as a commercial offering. Its multi-tenant model easily separates different user populations, with support for multiple identity sources and authenticators. And, AppGate's delegated administration model makes it simple to grant just the right level of a control to customers, while ensuring overall security and isolation of data, processes, and network traffic.

BENEFITS

- Enforce "Zero Trust" model consistently at both the network and application level
- Automated creation and enforcement of network and application access rules based on user and device context
- Management of access to on-premises private cloud, and remote public cloud environments
- Entitlement-based Routing creates individual network routes for each user, based on authorized entitlements. This enhances control of client network traffic at a fine-grained level, enabling simpler and incremental AppGate deployments even in complex network environments
- Dynamic access driven by user and service attributes, which changes to keep up with cloud environment changes
- Non-authorized services and resources are invisible, reducing attack surfaces by as much as 95%
- Single-Packet Authorization provides enterprises with the ability to hide all AppGate components on the network from unauthorized users. This approach enables secure deployment of SDP on public-facing networks, protecting and isolating all types of services
- Single, centralized logging of all authorized application traffic, per user and per device
- 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.
- Reduces cost, complexity and effort for configuring privileged / 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.

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

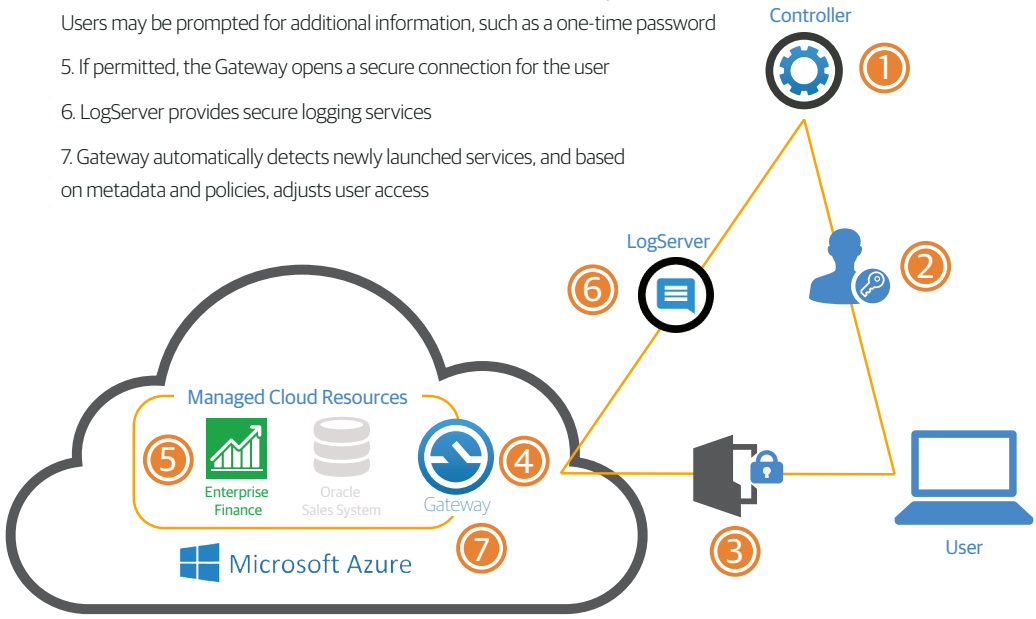
3. User attempts to access a protected resource behind a Gateway

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

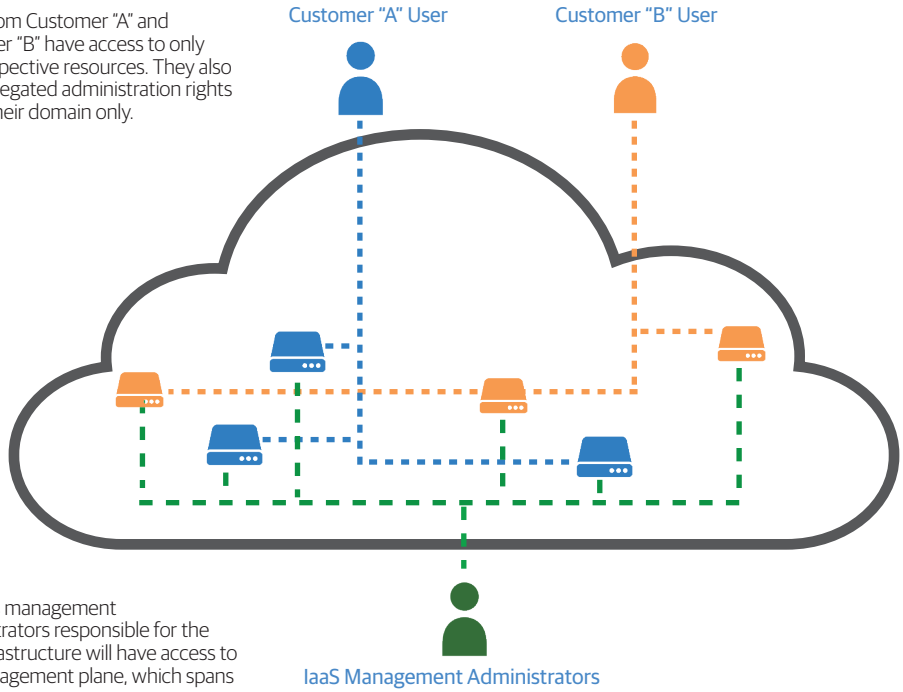
6. LogServer provides secure logging services

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



Cloud Service Providers

Users from Customer "A" and Customer "B" have access to only their respective resources. They also have delegated administration rights within their domain only.



Systems management administrators responsible for the IaaS infrastructure will have access to the management plane, which spans customer resources.

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