AppGate®

Context-Aware, Secure Access to AWS

AppGate is purpose-built for the AWS environment and draws on user context to dynamically create a secure, encrypted network *segment of one* that's tailored for each user session.

AWS: Speed and Cost Advantages

Enterprises are rapidly embracing Amazon Web Services (AWS), but securing access to these cloud-based workloads isn't easy. The root cause is that AWS' native security groups are simple IP-based firewalls which do not provide the user-centric access control needed by security teams to efficiently and effectively control user access to EC2 resources. And trying to control "who can access what" with static IP addresses and port mapping just doesn't scale.

This results in over-privileged users, unmanaged vulnerabilities, and a never-ending manual configuration change treadmill. The bottom line is that with AWS security groups, your team can't meet security or compliance needs, and can't keep up with the business. As a security professional you're tasked with protecting the enterprise's most valuable assets, yet AWS native and traditional solutions don't give you the functionality you need.

Native and Traditional Tools

For two reasons traditional security tools like VPNs, firewalls, and NAC are not well-suited to controlling user access to the AWS environment.

First, AWS is located outside the company perimeter, and may be accessible without users being present on the corporate network.

Second, cloud environments by their nature are highly dynamic, with server instances being created and terminated on an ongoing basis. These changes can happen due to human interaction, or automatically, for example based on workload. Traditional security tools cannot keep up with these ever-changing environments, and typically result in users being granted access to all services running on all servers within the cloud environment, which creates security and compliance risks.

The Solution

AppGate dramatically simplifies the user access problem, drawing on user context to dynamically create a network *segment of one* into IaaS 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. AppGate ensures that users can only access authorized resources in the cloud environment, and dynamically responds to creation or termination of IaaS server resources.

How it's Done

AppGate stops attackers from accessing valuable network resources at multiple levels, with a unique Zero Trust security model that includes:

- Encrypted communications – for secure, trusted connections from all clients, over public or private networks

- Strong User Authentication – ensuring that users are who they claim to be, with multi-factor assurance

- Single-Packet Authorization provides enterprises with the ability to hide all AppGate services on the network from unauthorized users

- Per-Session Authorization – dynamically determines which resources should be available based on device, user, and session context (attributes)

- Policy Enforcement – ensure users only access authorized resources through strict network access control

- Global Audit Logging – Tracks user access in detail for log and audit purposes

- By detecting any unauthorized packets from an authorized client device, AppGate can immediately block malicious traffic and feed alerts into a SIEM or IDS

Benefits

- Automated creation and enforcement of network and application access rules based on user and device context
- Every new instance will now be automatically traced and added or removed from the access filter, without the need of changing the policies
- Secure, service-specific tunnels between a user and an authorized resource – a *segment of one*
- Non-authorized services and resources are invisible, reducing attack surfaces by as much as 95%
- 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
- Reduces cost, complexity and effort for configuring privileged/user access

The Benefit of using AppGate in Combination with AWS

AppGate creates a *segment of one* for each user and device combination. AppGate makes sure that the context of the user and device is evaluated in real-time before providing network access to the user-authenticated instances and services in the AWS environment. AppGate is a linear and scalable distributed access system that creates a unique access filter for each user/device combination.

This patent pending access system dynamically matches the context information from the user and device with the context information it polls in real-time from the cloud provider. Users, devices and their context can now be matched by the policy engine to allow access to and only to the desired instances.

The context information pulled from the cloud is based on the metadata we get from the cloud APIs such as all/some instances in a certain VPC, security group, with a certain key or value, etc.

With these simple policies in place, network access automatically adapts in real-time to changing conditions on the client as well as on the cloud infrastructure side. Every new instance is automatically traced and added or removed from the access filter. It becomes an automated network access process that can be audited by simple policies.

AppGate is based on the zero trust principle. This means that all user traffic is encrypted, we authenticate and authorize the user first before giving access, and that all traffic is logged through our system, and by detecting any unauthorized packets, 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.

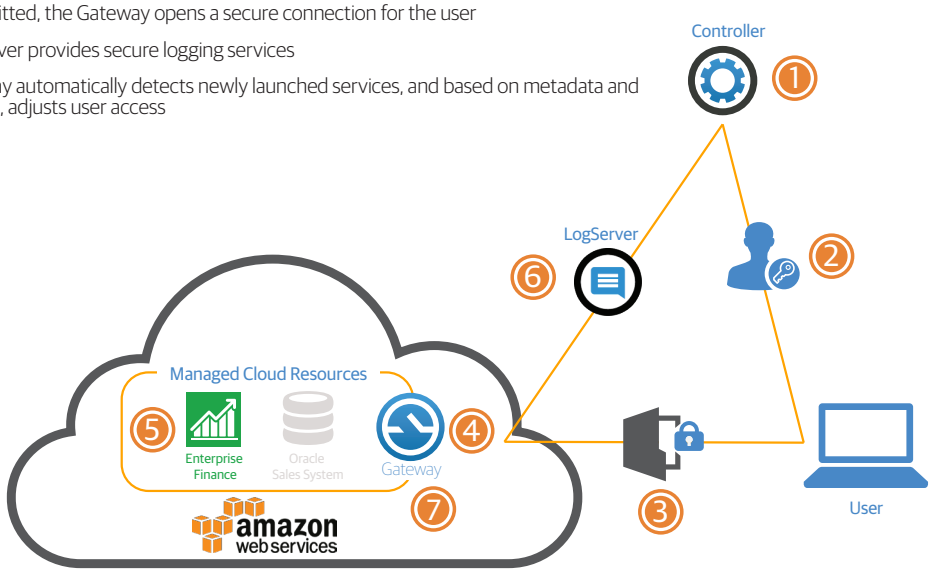
Is your business right for AppGate?

AWS customers that obtain the most value from AppGate have robust DevOps needs, dynamic environments, and a heightened need for security and compliance-driven access controls. AppGate is also a key technology in the Cloud Security Alliance's initiative regarding Software-Defined Perimeter for IaaS.

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



Cryptzone™

sales@cryptzone.com

www.cryptzone.com

@cryptzone

Americas: +1 888 272 2484 (US & Canada)
+1 603 578 1870

Europe, Middle East and Africa: +44 208 899 6189
00 800 9111 3358 *(UK, SE, DACH only)*