

AppGate®

A Distributed, Dynamic *Segment of One* Designed for the Cloud

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, 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

Why AppGate is Needed

In the new world of pervasive internal and external threats, distributed organizations, and global ecosystems, the perimeter is more porous and less relevant than ever. And increasingly, applications and services are deployed on-premises in a private cloud, or leverage a public cloud infrastructure.

The old models simply aren't working. We need to move from perimeter-centric, VLAN and IP-focused security to a model that focuses on securing the entire path from user to application, device to service - on a one-to-one basis. Traditional security tools like VPNs, firewalls, and NAC provide all-or-nothing access, giving authenticated users overly broad network access.

AppGate

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 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.

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. Superior integration, including improved enterprise integration with SIEM and IDS systems builds bridges among security tools. The result is improved security and more efficient compliance reporting.

What makes AppGate different is its distributed, scalable architecture designed for dynamic, multi-tenant cloud environments. Its distributed architecture features three services:

- Controller - the central authentication and token-issuing service. This applies policies and determines access rights for clients
- Gateway - a distributed, dynamic firewall through which network traffic flows. Consumes tokens and enforces access policies
- LogServer - provides secure logging services

How it Works

Client devices, such as laptops, desktops, or mobile devices, use the AppGate network driver to authenticate to the Controller, which evaluates credentials, and applies access policies. The Controller returns a cryptographically signed token back to the client, which contains the set of network resources - at a server and service level - that the user is authorized to access, subject to further conditions.

When the user attempts to access a resource - for example by opening up a web page on a protected server, the network driver forwards the token to the appropriate Gateway, which applies policies in real-time - for example, to control access based on network location, device attributes, or time of day. The Gateway sets routes from a fully rendered firewall ruleset based on the user's entitlement list for each Gateway and may permit access, deny access, or require an additional action from the user, such as prompting for a one-time password.

Once granted, all access to the resource travels from the client, across a secure, encrypted network tunnel, and through the Gateway to the server. Access is logged through the LogServer, ensuring that there's a permanent, auditable record of user access. AppGate can also immediately block malicious traffic and feed alerts into a SIEM or IDS for analysis and response.

Scenarios

AppGate is used today in these key scenarios to secure access:

- Privileged user
- Third-party user
- Secure access to sensitive, high-value assets
- Infrastructure as a service
- Ensure overall security and isolation of data, processes and network traffic in Managed Cloud Services environments.

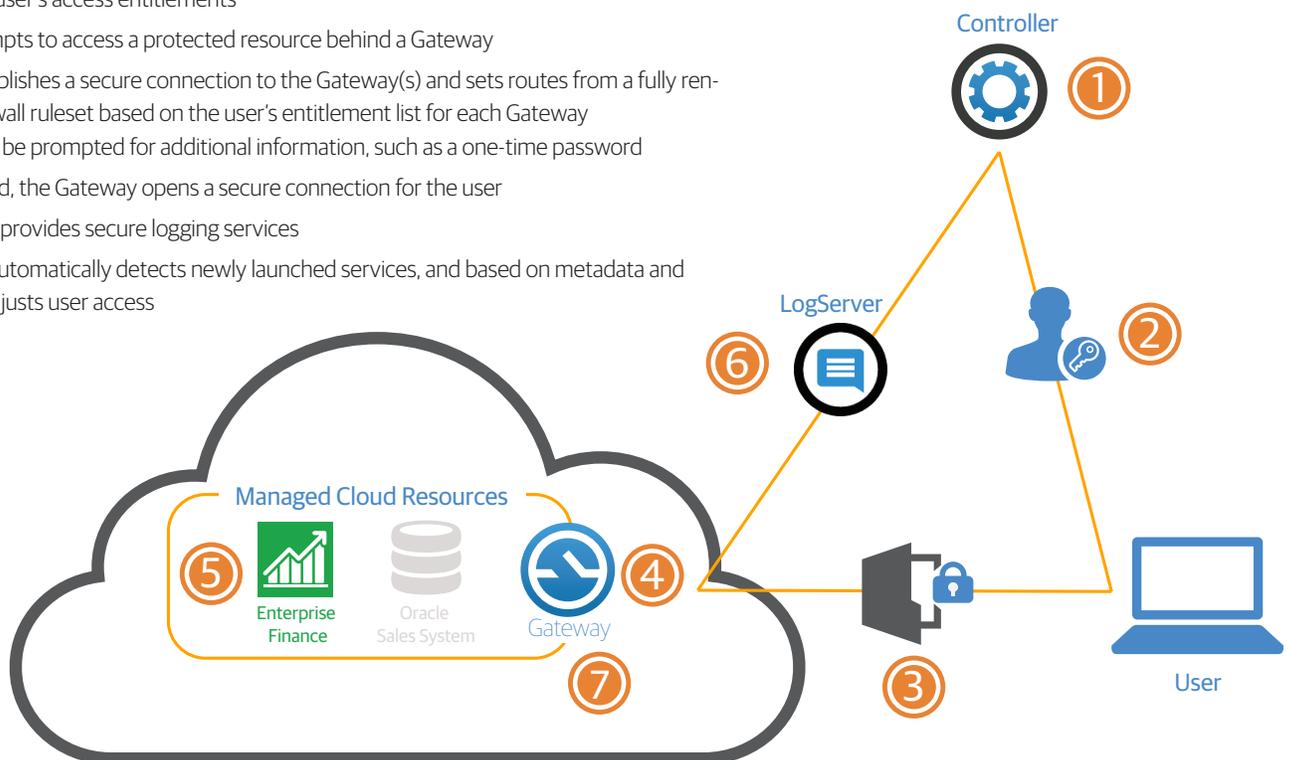
IaaS

In the past few years, enterprises have rapidly embraced the IaaS model for developing, building, and deploying enterprise applications. Whether deployed on-premises in a private cloud, or leveraging a public cloud infrastructure, the benefits are undeniable. And as more businesses embrace the DevOps methodology, maintaining secure access control and compliance can become more complicated.

The reality is that a move to the 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, these aren't designed to provide fine-grained access controls, or to adjust user access based on cloud server instance changes.

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



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.

AppGate designed to detect and adapt to changes in IaaS environments, dramatically simplifies the user access problem. By automatically detecting and responding to changes to IaaS server resources – such as creation of new server instances based on workload – AppGate will automatically adjust user access, based on policy. This helps ensure that users have immediate access to the resources they need – without requiring labor-intensive manual access configuration. The result is that enterprises avoid the security and compliance risks associated with overly-broad network access to IaaS resources.

Managed Cloud Service 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. AppGate's multi-tenant model easily separates different user populations, with support for multiple identity sources and authenticators. And, its 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.