AppGate SDP

SECURE EAST-WEST TRAFFIC. ELIMINATE LATERAL ATTACKS.

Last revised November 5, 2019

APPGATE®

Contents

Overview

Today's malicious actors are sophisticated and knowledgeable in their attacks on our enterprises. Once they obtain an entry point into the perimeter, these ill-intended actors quickly move within the environment in what is known as east-west or lateral movement. East-west traffic is the communication of data between two or more "peer" servers within a data center or other multi-server environment. The notion stems from typical network illustrations that show LAN traffic traversing horizontally in a network between servers whereas server to user traffic is shown in a north-south or vertical layout.

When a malicious actor breaches an instance, it is only a means to an end. Movement across a network from one system to another is usually necessary to achieve an adversary's goals, such as the execution of tools, pivoting to additional systems, accessing specific files, encrypted keys or user credentials. Similarly, if server egress policies are not well-defined within an environment, any malicious code planted can also easily spread laterally through services running on open ports.

Despite all the advances in security and related operational measures, there has been a notable absence of security solutions that are well-suited to provide microsegmentation for both north-south and east-west needs. Historically, if an enterprise has attempted to thwart east-west attacks, additional disparate security tools and services were required as an effort to offer this protection. AppGate SDP streamlines network security for server-to-server traffic and user-to-server traffic within a single system in a tightly coupled policy model.

This document highlights how to incorporate AppGate SDP to secure east-west traffic utilizing the capabilities of a Software Defined Perimeter (SDP).

East-West Security Challenges

Current architectures, while agile from a development perspective, greatly increase security risks due to a broad attack surface and management complexity.

As software architects and developers appreciate, the best-laid plans for designing a solid architecture are likely to be a far cry from the actual implementation. To offset these unplanned discrepancies and provide a level of agility, many organizations have adopted microservices. Microservices attempt to deliver focused functions in an effort to decouple capabilities from a traditionally monolithic application stack. Yet while loosely coupled, microservices typically increase server interrelationships and can significantly increase complexity and the attack surface.

> 57% of operations teams don't follow security best practices.
> The Threat Stack

Development teams will often open security groups and ACL to speed up progress that results in wide open network access. The combination of large teams of developers and human error means these security groups and ACLs are often left open when dev environments deploy to production. This open-access presents heightened security (and compliance) risks.

Traditional security methods do not address this problem either. Traditional approaches protect at the perimeter, and the edge's inbound and outbound rules are restricted per the needs of the service. However, once an edge instance is compromised, other instances are easily traversed via lateral attack, since servers within the environment are typically free to communicate. Edge-based access control made sense with single server environments, but those days are long gone.

Outside of the microservice development paradigm, there is countless other machine-to-machine use cases where ensuring controlled and limited access is a requirement. Enterprises are known to implement ad-hoc business to business relationships and "Data as a Service" offerings that have compliance or payment enforcement demands which need to be tightly managed on a firewall or other basis then quickly becomes unmanageable for even skilled technicians and ultimately, insecure.

Simplifying East-West Complexity with an SDP

A Software-Defined Perimeter enables businesses to architect and operationally manage a wide range of server to server solutions; whether an agile microservices architecture or an ad-hoc data sharing solution between businesses. An SDP provides policy-based definitions for each class of service while maintaining strict inbound and outbound rules. With an SDP, organizations can:

- Dynamically extend per server microsegmentation based on policies
- Greatly simplify management
- Eliminate the potential for human error

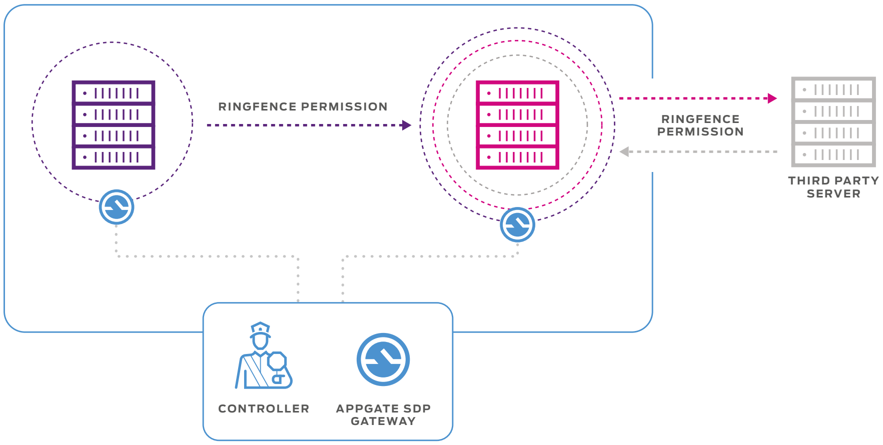
Implementing an SDP solution manages policies for each service. These policies can be moved and scaled with the workload to provide an agile and responsive solution that is resilient to east-west attacks.

USE CASES

- Encrypted tunnel from datacenter to on-premises or cloud without complex network redesign
- Dynamic access for batch processes such as back up
- Policy based server to server connectivity to elastic resources
- Restrict inbound or outbound traffic to one or more ports based on temporal or dynamically instantiated criteria
- Secure complex microservices environments
- Simplify migration of hybrid cloud infrastructure
- Privileged or ad-hoc customer access to proprietary applications or datasets

AppGate SDP for East-West Microsegmentation

AppGate SDP secures east-west microsegmentation with its dynamic policy model, which includes its Ringfencing capability. Ringfencing provides policy-enabled control of inbound and outbound rules for servers. The following diagram shows how AppGate SDP secures an east-west environment using Ringfencing.

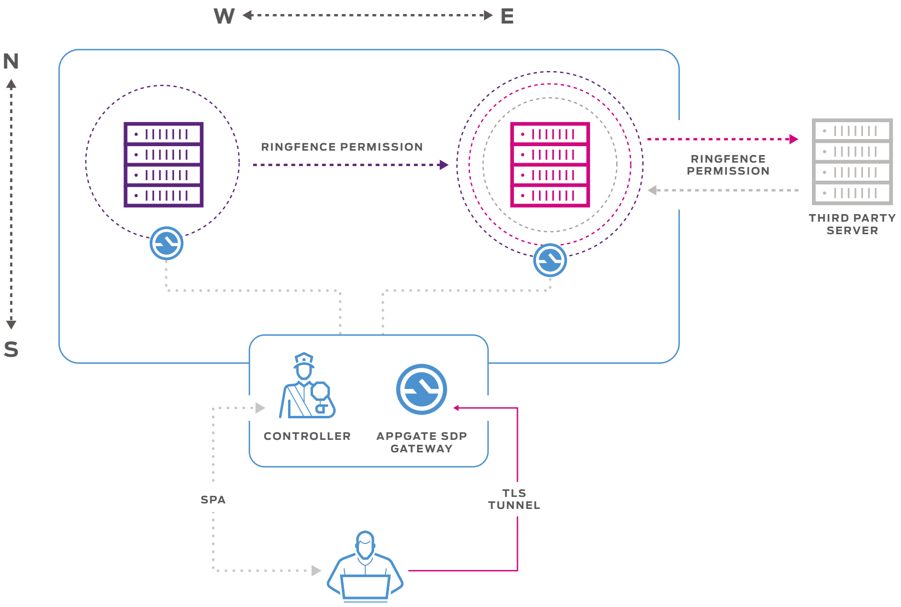


Server A (purple) is able to communicate with Server B (magenta). Server B can communicate bi-directionally to third parties (gray), but only receive inbound communication from Server A. Server A and Third Party Server are not able to communicate as permissions are ringfenced.

AppGate Ringfencing provides per-server firewall rules which explicitly limit the direction, port, and allowed source and destination of all traffic. When coupled with a centralized policy model and the AppGate Controller, fine-grained administration greatly limits east-west attacks from over-entitled servers while enabling information flow conditionally or as-authorized.

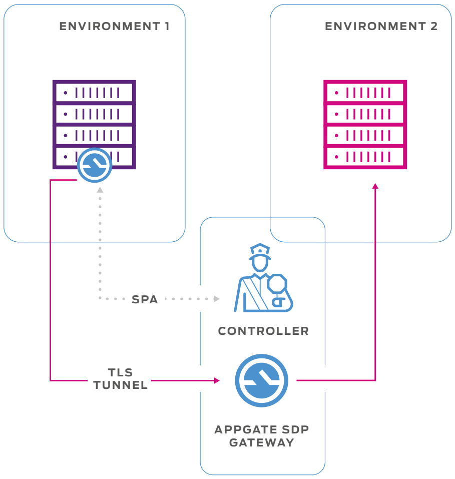
Applied in environments that have remote access needs for secure data access whether it's for day to day operations or development; businesses can utilize the common policies and administration to streamline operations and provide a single system for Zero Trust and compliance requirements.

Additionally, when utilizing unique capabilities within AppGate such as our metadata resolvers; logical values such as tags can automatically grant permissions to users and servers – greatly simplifying administration and reducing deployment time while providing the level of security needed for the particular user or server. In the case shown below, remote users accessing the cloud resource are utilizing SPA (Single Packet Authorization) to gain authorization to the protected resources via an encrypted TLS tunnel. Since the servers are inside a protected environment and likely utilizing encryption between one another, they are using Ringfencing to enable the appropriate port, IP, and flow (direction).



AppGate SDP supports both users in North-South traffic and East-West server to server communication in a common policy model, logging, and deployment framework.

In addition, while encrypted tunnels protect harsher, untrusted environments for users that are exposed in north-south scenarios, this same security can be applied for machine to machine networks with AppGate SDP by applying TLS tunnels between internally owned server connections and utilizing SPA. This can be useful for hybrid cloud scenarios or when you want to enforce an "authorize first, connect second" security as defined in the Zero Trust model.



In environments such as hybrid clouds or trusted business to business communications across the internet, AppGate can securely manage connectivity on a multi-factor basis including business rules. Connectivity can be limited to port, time, or posture of the remote server.

Summary

Today's dynamic, on-demand infrastructure makes security management far from easy. AppGate SDP provides the powerful ability to mitigate unauthorized access such that if there is an intrusion, malicious users cannot move laterally through the network and infect, steal, or corrupt data. With AppGate SDP deployed on servers, businesses can achieve:

- Reduced compliance reporting efforts with a policy enabled Zero Trust framework.
- Ability to proactively monitor network and server activity to dynamically restrict or limit access to critical services.
- Unified policy framework and language for establishing rules across any user, any server, and any location.

AppGate SDP provides enterprises agility and a unified policy model to maintain a microsegmented security posture accross users and servers. It combines definition and enforcement of north-south and east-west security controls in a single, dynamic platform.