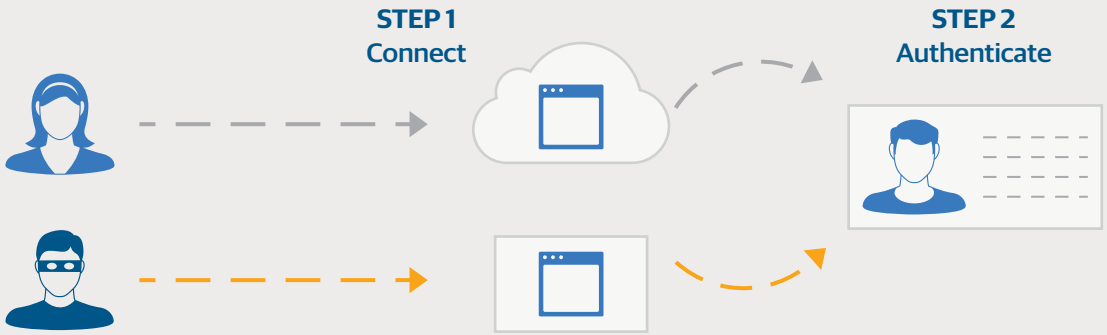
Cryptzone™

The Software-Defined Perimeter: Identity-Based Security for Hybrid Environments

TCP/IP was designed for a safer and more open world

Its "connect first, authenticate second" approach puts organizations at risk, and exhibits many security vulnerabilities:



- Servers are subject to reconnaissance scans
- Unauthenticated users can exploit servers
- Systems are vulnerable to DDoS attacks
- Unauthorized users consume server resources

The Software-Defined Perimeter stops attackers but lets authorized users connect

It takes an "authenticate first, connect second" approach, ensuring that only authorized users can connect to network resources.

This reduces the attack surface and significantly improves security:

- All resources are invisible to reconnaissance
- Only authenticated users can connect
- DDoS attacks are ineffective
- Unauthorized users cannot impact servers

Cryptzone's AppGate Solution Implements the Software-Defined Perimeter Specification

Distributed, scalable, highly available architecture

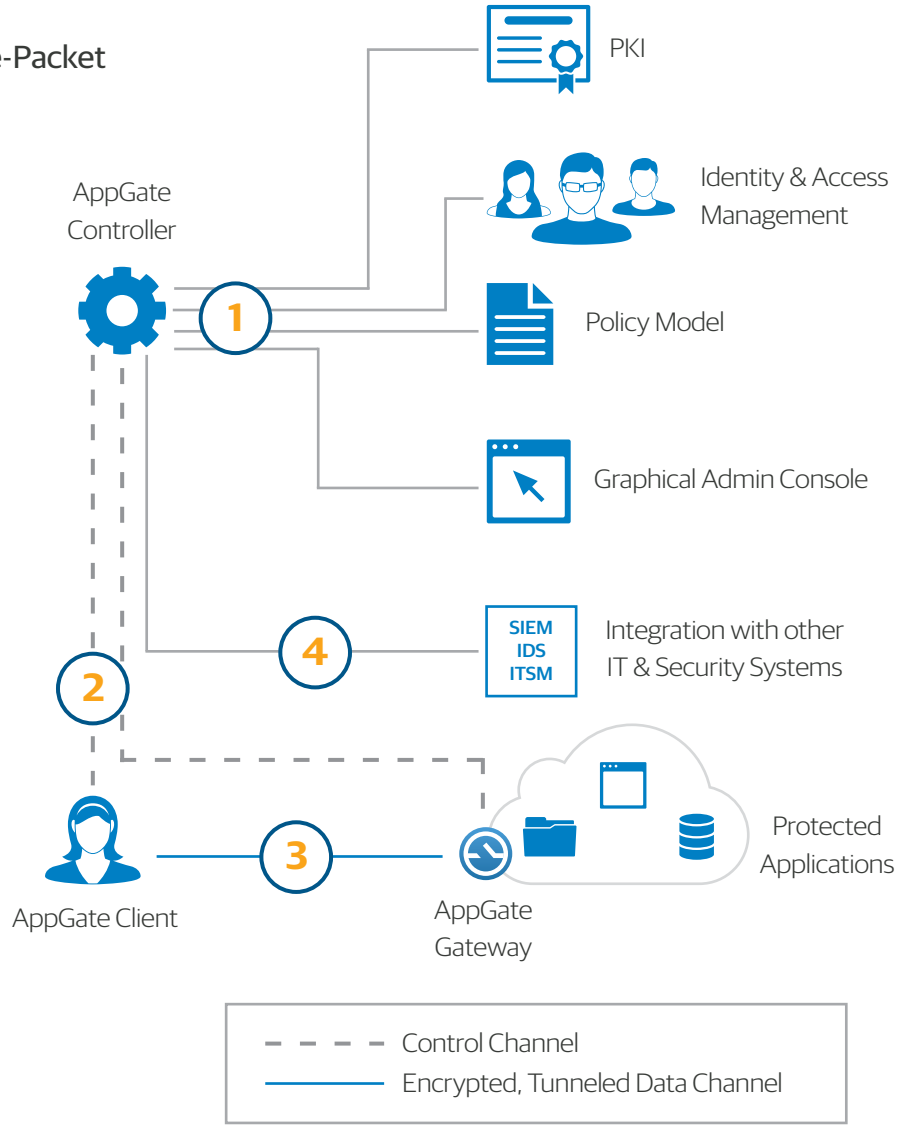
Protected by Single-Packet Authorization

1
- Controller integrates with PKI and IAM systems
- Controller is an authentication point and policy store
- System is administered via graphical admin console

2
- Secure client onboarding process
- Client authenticates to Controller
- Communication secured with mutual TLS

3
- Distributed Gateways protect cloud and network resources
- Clients securely access resources via Gateways with mutual TLS tunnels
- Real-time policy enforcement by Gateway
- Gateways dynamically adjust user access as systems change

4
- Controller enhances SIEM and IDS with detailed user activity logs
- Controller queries ITSM and other systems for context and attributes used in Policies



Learn more about SDP, and about how AppGate provides an individualized network "segment of one" for each user
www.cryptzone.com/SDP

Cryptzone™