



## DIRECT-ROUTED ZTNA: Transforming Federal Network Security While Meeting Compliance Needs

### Enhance Federal Cybersecurity Without FedRAMP Constraints

Federal civilian agencies face the dual challenge of securing sensitive systems and adhering to rigorous compliance requirements, including those outlined by the Federal Risk and Authorization Management Program (FedRAMP). Appgate's direct-routed Zero Trust Network Access (ZTNA) enhances security and offers a transformative solution. Under certain criteria, it's exempt from FedRAMP certification requirements, empowering agencies to implement robust cybersecurity without being tied to vendor-dependent cloud platforms.

### Challenges of Traditional Approaches

Federal civilian agencies that rely on VPNs and perimeter-based defenses face:

- **Static Access Controls:** Broad permissions create vulnerabilities for advanced persistent threats (APTs).
- **Cloud Traffic Bottlenecks:** Cloud-routed architectures increase latency and degrade operational performance.
- **Complex Compliance:** Cloud-based security solutions often require FedRAMP certification, adding time and complexity to deployment.

### The Advantage of Direct-Routed ZTNA for Federal Agencies

Direct-routed ZTNA eliminates the need for cloud-based intermediaries, creating secure, direct connections between users and resources. This approach:

- **Meets FedRAMP Exemption Criteria:**  
Agencies can deploy direct-routed ZTNA solutions under the FedRAMP exemption for systems hosted within an agency's security boundary, used exclusively for its operations, and not offered as a shared service.
- **Supports Federal Security Frameworks:**  
Direct-routed ZTNA adheres to standards like FISMA, NIST SP 800-53, and OMB Circular A-130, ensuring robust protection for federal information systems.
- **Simplifies Compliance:**  
Direct-routed ZTNA eliminates the need for vendor-managed, shared responsibility models, reducing administrative overhead while meeting federal security requirements.

### KEY BENEFITS OF DIRECT-ROUTED ZTNA FOR FEDERAL AGENCIES

#### ENHANCED SECURITY

Enforces Zero Trust security with end-to-end encryption, continuous verification, and least privilege access to protect data from user devices to federal systems without relying on intermediary decryption points.

#### IMPROVED PERFORMANCE

Direct routing eliminates cloud traffic bottlenecks, ensuring low latency and high availability for critical applications.

#### REDUCED ATTACK SURFACE

Cloaks resources, making them invisible to unauthorized users and significantly reducing the attack surface.

#### FLEXIBLE DEPLOYMENT

Works seamlessly across hybrid infrastructures, including on-premises, cloud, and supports air-gapped deployments.

#### SIMPLIFIED MANAGEMENT

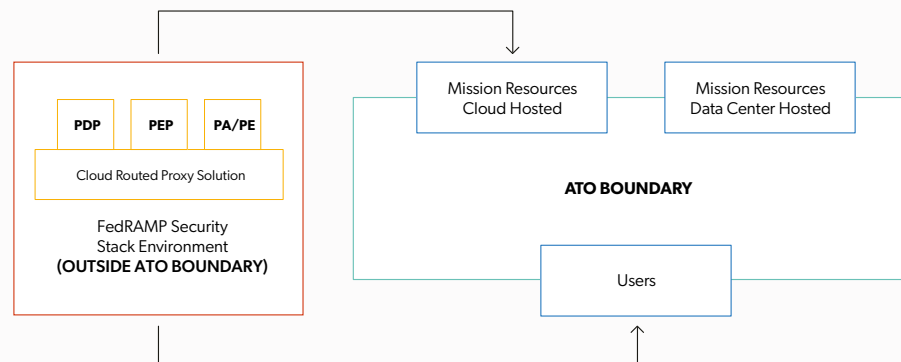
Granular access controls and streamlined policy enforcement reduce the burden on federal IT teams.

#### COST PREDICTABILITY

Avoids variable cloud costs, offering predictable pricing that aligns with federal budgeting processes.

### CLOUD-ROUTED ARCHITECTURE

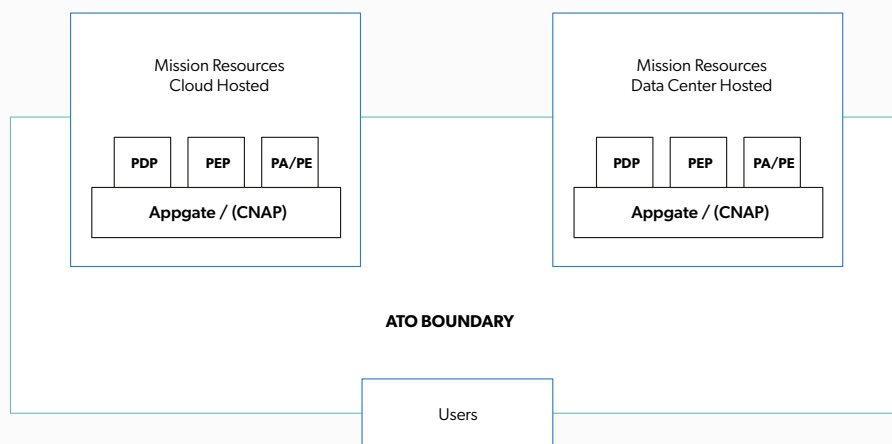
1. FedRAMP is required in a cloud-routed architecture as the "security stack is outside of your ATO boundary".
2. DISA's CNAP reference architecture requires the use of Single Packet Authorization (SPA) to cloak the enterprise edge and mission applications. Cloud-routed architectures are exposed and discoverable to the entire internet.
3. Cloud-routed architectures require the consumer to place full trust of the entire security stack to the cloud-routed provider (certificates, configurations, key material, etc.). This approach is Trust + 1 (not true Zero Trust).





## DIRECT-ROUTED ARCHITECTURE

1. FedRAMP does not apply to a direct-routed architecture. The Appgate security stack is within your ATO security boundary. Appgate does not route to a vendor-hosted cloud, or proxy user traffic to third party.
2. The government remains in full control of certificates, configuration, user data, etc.
3. SPA and Mutual TLS are used to cloak the edge and protect against man in the middle (MITM) attacks.



### How Direct-Routed ZTNA Works

1. **Authentication:** Verifies user identity with multi-factor authentication (MFA).
2. **Context Evaluation:** Assesses user device posture, location and risk context.
3. **Policy Enforcement:** Enforces least privilege access using real-time contextual data.
4. **Secure Tunnel Creation:** Establishes an encrypted connection directly to authorized resources.
5. **Dynamic Access Management:** Adapts permissions based on ongoing threat analysis.

### Why Appgate ZTNA?

Appgate ZTNA delivers a direct-routed Zero Trust solution designed for federal civilian agencies. Unlike traditional or cloud-routed ZTNA models, Appgate's direct-routed ZTNA solution offers:

- **Unmatched Security:** Combines Zero Trust principles with a direct-routed architecture.
- **Regulatory Alignment:** Simplifies adherence to federal standards like NIST CSF and FISMA.
- **Mission-Ready Performance:** Ensures uninterrupted operations across globally distributed and hybrid networks.

### EMPOWER FEDERAL AGENCIES WITH APPGATE'S DIRECT-ROUTED ZTNA

Appgate ZTNA enables federal civilian agencies to modernize their cybersecurity approach, maintain compliance with federal mandates, and enhance their operational resilience. By leveraging direct-routed ZTNA, agencies can bypass FedRAMP requirements while building a robust Zero Trust security framework tailored to their unique missions.

**Contact us today to learn how Appgate ZTNA can secure your agency's critical infrastructure while simplifying compliance.**

#### Dillon Cox

Director, Federal Civilian  
[dillon.cox@appgate.com](mailto:dillon.cox@appgate.com)

#### Jonathan Early

Customer Success Manager  
[jonathan.early@appgate.com](mailto:jonathan.early@appgate.com)

#### Jonathan Roy

Senior Security Architect  
[jonathan.roy@appgate.com](mailto:jonathan.roy@appgate.com)

#### Timothy Winters

Director Federal Channel & Alliances  
[timothy.winters@appgate.com](mailto:timothy.winters@appgate.com)

### About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate ZTNA for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at [appgate.com/federal](https://appgate.com/federal)