



CASE STUDY

GOVERNMENT AGENCY SECURES ACCESS ACROSS DEPARTMENTS

BACKGROUND

A North American government agency was tasked to consolidate, streamline and improve IT access across government departments.

THE CHALLENGE

The Government system has between 1,500–2,000 remote users at any given time, and 20,000 users overall. Prior to Appgate SDP, the solution in use couldn't provide the level of security and agility that was needed. The central services team found that once users accessed a server, that user was able to authenticate themselves and go anywhere within the existing systems and servers, opening it up to potential data breaches. The agency needed an alternative solution.

REQUIREMENTS

With more than 20,000 users, this government agency needed to ensure secure access to its shared services. It required a solution to control and simplify remote, third-party and privileged user access. The agency wanted increased security, multi-factor authentication, granular controls for advanced roles and rights management.

SOLUTION

The agency was concerned that its solutions in place, including traditional solutions like VPNs, firewalls, and jump hosts. The agency needed to centrally control all user access privileges. During the agency's evaluation of technologies, it investigated Appgate SDP, a Software-Defined Perimeter solution that dynamically creates one-to-one network connections between the user and the resources they access. Everything else is invisible including the system itself. Appgate SDP provides consistent, adaptive and context-aware access in hybrid environments.

Appgate SDP enables this government agency agility and flexibility to adapt to the dynamic demands of the workforce, constituents and third-party vendors. Appgate SDP provides real-time access on a need-to-know basis and enables a unified way to control access while maintaining a tight security profile.



ORGANIZATION

A North American government agency focused on delivering IT services throughout departments.

INDUSTRY

Government

CHALLENGES

Secure access of 20,000 users to applications, email, web servers and datacenters across departments

Centralize management of all network devices across the 20,000 users and third-parties

Integrate seamlessly with existing two-factor authentication system Solution

SOLUTION

Appgate SDP

BENEFITS

Control privileged user access using secure, encrypted, point-to-point tunnels to protect network resources and dynamically provision access

Centrally managed solution to remotely secure privileged, remote employee, and third-party network access

Extensible monitoring and alert management so that access to network resources can be tracked and monitored

Appgate SDP was easy to set up and apply security rules—all without needing to expose apps to the internet or rewrite legacy apps that are agency critical. The agency was able to leave apps where they were, define authorization policies, record access logs, and pinpoint who accessed what and when. Appgate SDP integrated with the agency's existing two factor authentication system which had already been deployed at a significant cost. When tested, Appgate SDP proved to be one of the only out of the box solutions able to integrate with this system easily.

Furthermore, Appgate SDP provides extensible monitoring and alert management so that access to network resources can be tracked and monitored. It reduces overhead in reporting for regulatory compliance and quicker identification of potential risk scenarios.

BENEFITS OF APPGATE SDP

With Appgate SDP, the agency gained access control for its entire population of remote users. Initially this was for a few thousand users, but because the benefits were so vast, use was increased to all 20,000 users. Users are now able to securely access government resources from external locations. Policies control whether multi-factor authentication is required based on a user's role, location, and other attributes. The agency is able to grant role-based access enabling users to work interdepartmentally, increasing the productivity through the user community.

Failure to gain access to systems without the correct authorization and authentication safeguards the agency from internal and external threats.

Furthermore, Appgate SDP expands the traditional network security model beyond IP addresses and VLANs, allowing the agency to manage access at the most relevant and critical level—from user to app and service, on a one-to-one basis. This provides a secure, encrypted, point-to-point tunnel to protect network resources and dynamically provision access from any device in any location.

The administrator at the agency said that without Appgate SDP, they'd need to implement a VPN tunnel system, create and modify thousands of firewall rules, and modify their DNS. This would take months to accomplish across all of the agency's groups. It would have turned a short-term goal into a long-term project.

FUTURE PLANS

Over the next few years, the agency plans to move resources to the cloud to increase scalability, reliability, and high availability. Appgate SDP will secure access to the agency's hybrid environment.

Contact Information:

Web: <https://www.xbandenterprises.com/appgate>

Email: Ahmed.Sharaf@xband.net

Cloud, Cybersecurity & Internetworking Specialist

Phone: (877) 922-6346

Direct: (813) 466-9540