SOLUTION OVERVIEW

Privileged User Access with BIG-IP Access Policy Manager

Safeguard federal agency data and mitigate risks

KEY BENEFITS

Reduces the attack surface
F5 Privileged User Access creates a shell around vulnerable devices and administrative interfaces. Any access requires the use of a CAC/PIV which authorizes access to the individual resource.

Provides an audit trail
This solution provides an audit trail for security teams and agility for security policies; the enterprise determines the life of a session/password.

Requires no installation or modifications
The F5 solution doesn't require any installation of software or modification on backend critical systems.

The Vital Importance of Strong Authentication

Traditional username and password access to administrative resources is a major security vulnerability in our networks today. Supporting this priority, the Department of Defense (DoD) Cybersecurity Discipline Implementation Plan's number one line of effort is strong authentication for privileged users.[1]

> **Line of Effort: Strong Authentication**
> Reducing anonymity, as well as enforcing authenticity and accountability for actions on DoD information networks, improves the security posture of the DoD. The connection between weak authentication and account takeover is well-established. Strong authentication helps prevent unauthorized access, including wide-scale network compromise by impersonating privileged administrators. Commanders and Supervisors will focus attention on protecting high-value assets, such as servers and routers, and privileged system administrator access. This line of effort supports objective 3-4 in the DoD Cyber Strategy, requiring the DoD CIO to mitigate known vulnerabilities.

Additionally, the most recent DISA Network Device Management Security Requirements Guide—which details security practices and procedures applicable to the management of DoD network devices—provides for a CAT 2 (medium) finding for failure to use multi-factor authentication for privileged user accounts accessing network devices.[2]

> **Finding ID:** V-55105
> **Severity:** High
> **Details:** ...the DoD has mandated the use of the Common Access Card (CAC) token/credential to support identity management and personal authentication for systems covered under HSPD 12. DoD recommended architecture for network devices is for system administrators to authenticate using an authentication server using the DoD CAC credential with DoD-approved PKI...

However, CAC authentication to administrative resources can be difficult to achieve. There are a vast number of devices and systems which were not built to accommodate strong authentication or smart card access. The options have traditionally been limited to:

1. Accept the risk to the organization.
2. Remove or replace the device.

F5 Privileged User Access

The F5® Privileged User Access™ solution now provides an additional option that can add CAC authentication or another strong authentication method to a network infrastructure that does not natively support this functionality. It does this without requiring client software or

agents anywhere in the environment and allows you to fully leverage your legacy or non-compliant systems in a safe and secure manner. It integrates directly into DoD PKI systems and may be configured to work cooperatively with an existing RADIUS, TACACS, Active Directory, or a variety of third-party authentication databases.

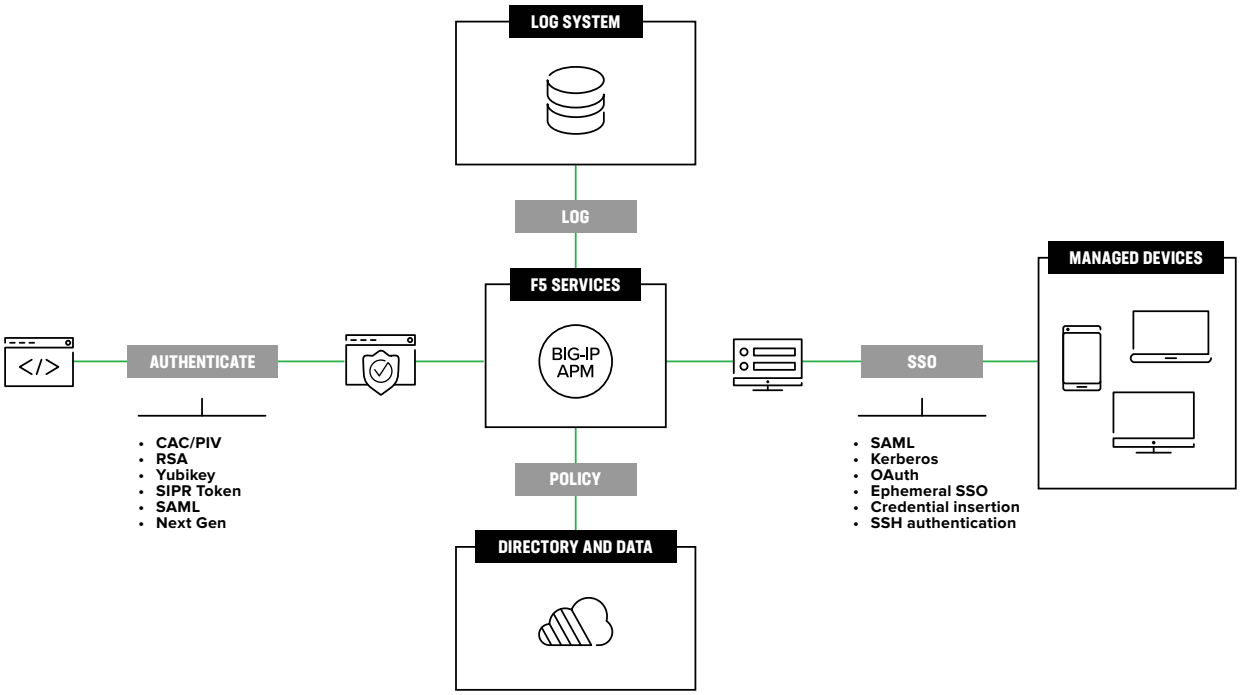

Figure 1: The F5 Privileged User Access solution ensures the right users have access to sensitive data through the strong authentication process highlighted in this diagram.

This solution has four major components including the F5 BIG-IP® platform, BIG-IP Access Policy Manager® (APM), Ephemeral Authentication, and Web SSH Client.

BIG-IP PLATFORM

The BIG-IP platform is a FIPS-compliant, Common Criteria-certified, and UC APL-approved product[3] which is available in both physical and virtual form factors. All the functions of the F5 Privileged User Access solution run within the BIG-IP platform. BIG-IP is a security product widely deployed throughout DoD networks that already performs strong authentication for thousands of critical applications. This additional solution simply applies that existing functionality to privileged user requirements.

THE ENTIRE SYSTEM EXISTS INSIDE F5 BIG-IP AND WORKS IN CONCERT WITH BIG-IP APM TO ENSURE A SECURE, END-TO-END ENCRYPTED CONNECTION WHILE ELIMINATING THE POSSIBILITY OF CREDENTIAL REPLAY.

BIG-IP Access Policy Manager

A privileged user accessing an application is first authenticated by BIG-IP Access Policy Manager (APM). BIG-IP APM first displays a U.S. Government (USG) warning banner to the user which requires acceptance before moving forward with authentication.

Next, BIG-IP APM requests CAC or strong credentials from the user which are then checked against a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) server to ensure their credentials have not been revoked. Optionally BIG-IP APM can query a directory server such as a Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) server, a Security Assertion Markup Language (SAML) provider, or a variety of third-party directories to further establish the user's identity of the user.

Once BIG-IP APM verifies that the privileged user is permitted to access the system, BIG-IP APM will query additional attributes to determine which resources the privileged user can access. Finally, the privileged user will be presented a portal page of the resources they are permitted to access. BIG-IP APM also provides advanced features to ensure the integrity of the client, such as verifying the client is Government Furnished Equipment (GFE), that it complies with The Host Based Security System (HBSS), and/or is running a supported operating system.

Ephemeral Authentication

Ephemeral authentication is essentially a closed-circuit, one-time password for systems which may only authenticate with a username and password. The entire system exists inside F5 BIG-IP and works in concert with BIG-IP APM to ensure a secure, end-to-end encrypted connection while eliminating the possibility of credential replay. At no point during the process does the user or client know this ephemeral password, and in the highly unlikely event this password is compromised, it is completely worthless to an attacker or bad actor. This even allows F5 to provide CAC or multi-factor authentication to any system that is restricted to using a username and password for authentication.

Web SSH Client

The Web SSH client is an HTML5 client which will run on any government-provided web browser and requires no installation of client-side components. This allows for instant access from any current and future U.S. Federal Government system with a web browser. This client provides full terminal emulation, mouse events, cut and paste, and the ability to log connections on the client. This client also supports the ability to overlay classification banners which may be specified per host or globally, as well as to provide cipher options per-host to ensure compatibility with legacy devices.

THE F5 SOLUTION SUPPORTS AUTHENTICATION FEDERATION MODELS AND CAN FACILITATE THE DOD ADOPTION OF SAML AND CLOUD TECHNOLOGY.

Consolidating Privileged User Access

While the F5 Privileged User Access solution covers a serious security gap for legacy and non-compliant systems, it's also an effective way to aggregate access to modern systems. F5 can protect many systems that require privileged user access. Some examples include:

- Telephony administration interfaces (e.g., Cisco Communications Manager Administration)
- Firewall, IDS/IPS, and DLP administration interfaces (e.g., Palo Alto web interface)
- Proxy administration interfaces (e.g., BlueCoat ProxySG)
- Storage array interfaces (e.g., NetApp OnCommand, Pure Storage)
- VDI administration interfaces and VDI client authentication requirements (e.g., VMWare Horizon, Citrix XenDesktop, Windows Remote Desktop)

By consolidating access control for administrators, you can take advantage of the extensive authentication and control capabilities of BIG-IP APM. It enables you to enforce the use of TLS encryption standards across untrusted networks. You can also use the logging functions of BIG-IP APM to provide a single point to log and audit the administrative access to these systems as well as integrate with reporting and logging systems for compliance purposes.

The Future of Authentication

F5 provides a framework to add capabilities that may become requirements in the future. Some of the authentication capabilities under consideration by government and DoD leadership are derived credentials, biometrics and additional factors of authentication. If the government chooses to move away from using CAC or authentication methods that are commonly used today, the F5 solution provides the flexibility to be extended to support those additional capabilities as they are defined.

The F5 solution supports authentication federation models and can facilitate the DoD adoption of SAML and cloud technology. F5 can provide strong authentication to applications, devices, management interfaces, and systems within DoD environments–in the cloud, or wherever they may reside in the future.

To learn more, visit www.f5.com/solutions/us-federal-government.

[1] DoD Cybersecurity Discipline Implementation Plan, found at http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf
[2] UCF STIG Viewer, found at https://www.stigviewer.com/stig/network_device_management_security_requirements_guide/2017-04-07/finding/V-55105
[3] BIG-IP Platform certifications, found at https://f5.com/about-us/certifications