SOLUTION OVERVIEW

Privileged User Access with F5 Access Policy Manager

September 2017

Bill Church

Principal Security Solutions Engineer

Are Your Network Administrators Using Strong Authentication?

As the Office of Personal Management breach[1] has shown us, traditional user name and password access to administrative resources is a major security vulnerability in our networks today. Supporting this priority, the **DoD Cybersecurity Discipline Implementation Plan's** number one line of effort is strong authentication for privileged users. This implementation plan also includes references to USCYBERCOM tasking orders that further document this requirement.

> ***Line of Effort 1 - Strong Authentication***[2]
> 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 by the end of 2016.

Additionally, the most recently updated **DISA Network Device Management Security Requirements Guide**[3] which details security practices and procedures applicable to the management of DoD network devices provides for a CAT I (High) finding[4] for failure to use multifactor authentication for privileged user accounts accessing network devices.

> ***Finding ID:*** *V-55105*
> ***Severity: High***
> ***Details:*** *…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…*

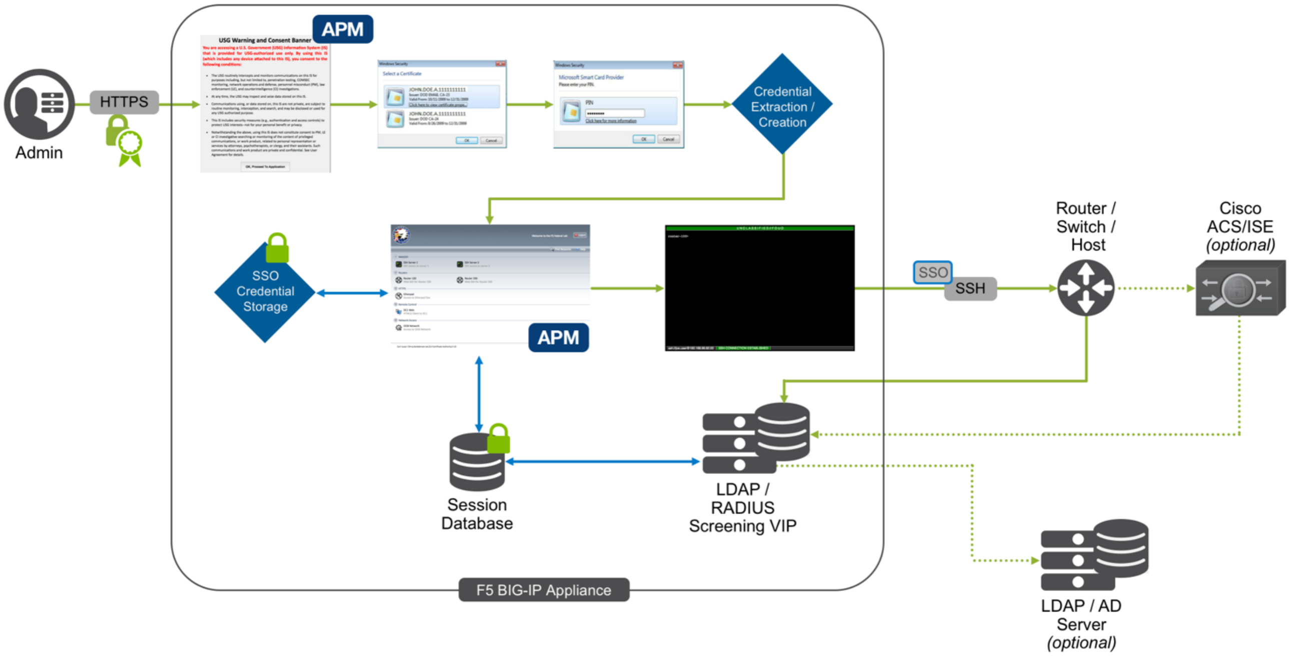
However, CAC authentication to administrative resources can be difficult to achieve. There are a vast number of devices and systems which were not built to accommodate strong authentication or smart card access. The options have historically seemed limited to:

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

[1] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[2] http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf pg.5
[3] https://www.stigviewer.com/stig/network_device_management_security_requirements_guide/
[4] https://www.stigviewer.com/stig/network_device_management_security_requirements_guide/2017-04-07/finding/V-55105

F5 Privileged User Access Solution Overview

The F5 Privileged User Access Solution now provides an additional option that can add CAC authentication or another strong authentication method to network infrastructure that does not support this functionality natively. It does this without requiring the addition of 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.



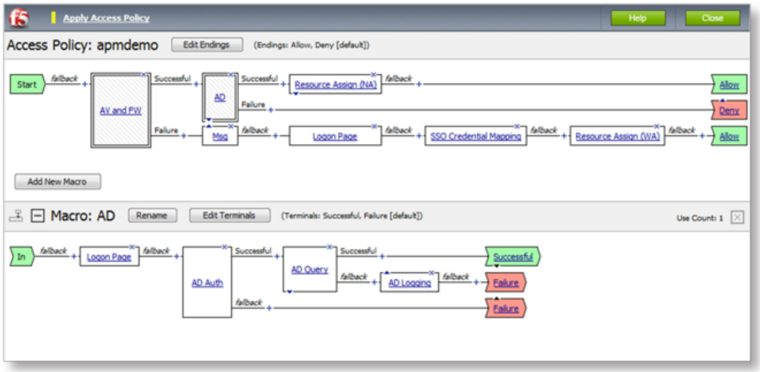
This solution has 4 major components including the BIG-IP platform, Access Policy Manager, Ephemeral Authentication, and Web SSH Client.

BIG-IP Platform

The F5 BIG-IP platform is a FIPS compliant, Common Criteria certified, and UC APL approved product[5] which is available in both physical and virtual form factors. All the functions of the F5 Privileged User Access Solution are run within the BIG-IP. The F5 BIG-IP is a security product widely deployed throughout DoD networks and is already performing strong authentication for thousands of critical applications. This solution simply applies that existing functionality to privileged user requirements.

[5] https://f5.com/about-us/certifications

Access Policy Manager



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

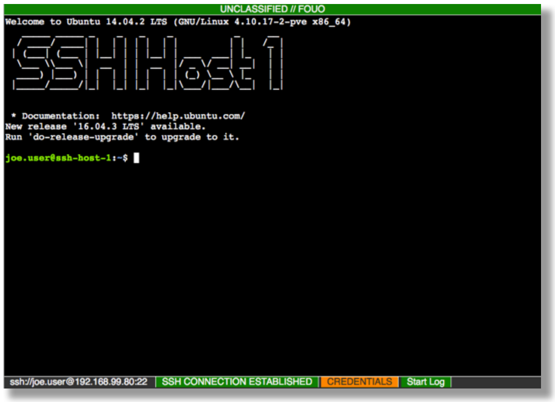
Once APM verifies the privileged user is permitted to access the system, APM will query additional attributes to determine which resources the privileged user is permitted to access. Finally, the privileged user will be presented a portal page of the resources they are permitted to access. APM also provides advanced features to ensure the integrity of the client such as verifying the client is Government Furnished Equipment (GFE), 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 the F5 BIG-IP and works in concert with 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 what this ephemeral password is, and in the highly unlikely event this password is compromised it is completely worthless to an attacker or bad actor. This allows F5 to even provide CAC or multi-factor authentication to any system that is restricted to using a user name 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 US Federal Government system with a web browser. This client provides full terminal emulation, mouse events, cut and paste, and the ability 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 provide cipher options per-host to ensure compatibility with legacy devices.



```
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 4.10.17-2-pve x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

joe.user@ssh-host-1:~$
```

Consolidate Privileged User Access

While this solution covers a serious security gap for legacy and non-compliant systems, it also works great to aggregate access to modern systems. F5 can protect many systems that require privileged user access. Some of these examples include:

- Telephony administration interfaces (ex: Cisco Communications Manager Administration)
- Firewall, IDS/IPS, and DLP administration interfaces (ex: Palo Alto web interface)
- Proxy administration interfaces (ex: BlueCoat ProxySG)
- Storage array interfaces (ex: NetApp Oncommand)
- VDI administration interfaces and VDI client authentication requirements (ex: VMWare Horizon or Citrix XenDesktop)

And by consolidating the access control for administrators you can now take advantage of the extensive authentication and control capabilities of APM. You can enforce the use of TLS encryption standards across untrusted networks. You can use the logging functions of 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 for the addition of 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 become 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 intefaces, and systems within DoD environments, in the cloud, or wherever they may reside in the future.

It’s impossible to predict the future, however having the BIG-IP with it’s flexible authentication methods is the closest you can come to having a crystal ball in your environment.

F5 Government Solutions
12012 Sunset Hills Road, Suite 900, Reston, VA 20190
888-882-4447 https://f5.com/solutions/enterprise/industries/government