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.

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Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) server to ensure their credentials have not been revoked.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.
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.

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.