Configuring the BIG-IP as an SSH Jump Server using Smart Card Authentication and WebSSH Client

Steve Lyons, 2018-12-07

Based on the feedback I got when talking about this capability on social media, I figured I would write an article and expose everyone to what this solution actually looks like and how to deploy it. First off, I want to dig into the use case itself. While the use case for each organization could and is likely different, for a small group of us at F5 Networks had a requirement to smart card enable network devices. Well of course that statement alone comes with a lot of hesitation and questions from your network shop. One likely being "how the heck do you smart card enable something that doesn't support smart card authentication? Then if you can, how the heck to you configure putty to support smart cards without spending a billion dollars?" This is when you tell them, I'm glad you asked because you can't. However, with F5 being the magical software company it is we can enforce smart card authentication, OCSP validation, generate a one-time password (OTP) and present that to the device to authentication all while using your favorite browser. Sound impossible? I think not, so let's get to it!

Before getting to far ahead, I wanted to clarify, this is NOT a solution I developed but rather hoped to educate some folks on. The heavy lifting and development came from F5 all stars like Bill Church and Michael Coleman. So when you get done reading this article and want to thank someone, make sure to send them a note.

Prerequisites

- LTM Licensed and Provisioned
- APM Licensed and Provisioned
- iRulesLX Provisioned
- 8Gb of Memory

Alright, now that I have provided you with what my use case is lets go ahead and begin the deployment. From a browser, go ahead and navigate to https://github.com/billchurch/f5-pua to download the offline privileged user access zip file that contains all necessary components and for the most part deploys this solution for you. Yes....once again, thank you Bill Church! Once downloaded, extract the build_pua_offline.sh file from the zip.

Copy Shell Executable to BIG-IP

If you are using a Windows box like myself, go ahead and either download or launch something like WinSCP so that you can transfer the shell executable to your BIG-IP. I simply transferred the .sh file to my /tmp directory as shown below. Once transferred, go ahead and close WinSCP.

Run the build_pua_offline.sh Script

Because we haven't deployed our WebSSH solution yet we are going to use putty to SSH to our BIG-IP and run the script. Once authenticated, navigate to the directory you stored the .sh file and run the command *bash build_pua_offline.sh.*

You will first be presented with a set of instructions regarding questions you will be asked during the running of this script. Press any key continue.

As the instructions imply, you will be providing several IP addresses for the required virtual servers. Please note, the only IP that can NOT be shared is the IP for the WebSSH proxy.

- **WebSSH IP:** 10.1.20.100
- **Radius Service IP:** 10.1.20.101
- **LDAP Service IP:** 10.1.20.101
- **LDAPS Service IP:** 10.1.20.101
- **Webtop IP:** 10.1.20.102

Once you have provided all of the necessary IP addresses you will be presented with an option to create a CA for testing purposes. In this guide, we will select N for this option.

After all profiles, virtual servers and policies have been created you will be presented with a question of whether or not to configure the BIG-IP to test Radius by configuring remote user authentication for Radius. We will select N for this option.

If the script completes successfully, this will be the last item you are prompted for. In our case we had a successful deployment of the build_pua_offline.sh script so let's take a look at the objects that were created.

Virtual Servers

LX Workspaces

LX Plugins

Access Policy

Portal Access List

Webtop List

HTTP Basic Auth Profile

- While we could review each and every one of these, that is not the intent of this article. Now that the script has been deployed, let's begin by focusing on our defined use case which is smart card auth with a WebSSH client.

Configure SSL Client Profile

- To support client certificate-based authentication, we must also create a Client SSL Profile on the BIG-IP using the steps below.
- Navigate to **Local Traffic > Profiles > SSL > Client > Create**
- Name: **WebtopSSLProfile**
- Certificate Key Chain: Place a check mark under the custom field. Click **Add** to select the appropriate cert/key pair.

- Client Certificate: Leave it set to **ignore** as the APM ODCA will perform this function.
- Trusted Certificate Authorities: Select the CA or CA bundle certificate
- Advertised Certificate Authorities: Select the CA or CA bundle certificate

- All other settings can be left at their defaults.
- Click **Finished**

Create a LDAP Pool

- Navigate to **Local Traffic > Pools > Click Create**

- Navigate to **Local Traffic >> Pools >> Click Create**
- Name: **LDAP_Pool**
- Health Monitor: **TCP**

- Address: **IP of your Directory Server**
- Service Port: **389**
- Click **Add**
- Click **Finished**

Configure BIG-IP LDAP Bypass User

When configuring the BIG-IP to use LDAP Authentication as you will see at the end of this article, you will need to include that user account in the ephemeral_LDAP_Bypass Data Group List.

- Navigate to **Local Traffic >> iRules : Data Group List** >> Click the **ephemeral_LDAP_Bypass** list that was created when deploying the PUA Offline Script.
- String: **CN=admin,CN=Users,DC=demo,DC=lab**
- Click **Update**

Configuring a LDAP AAA Resource

- Navigate to **Access >> Authentication >> LDAP** and select **Create**
- Name: **LyonWebtopLDAP**
- Server Connection: **Direct**
- Base Port: **389**
- Admin DN: **CN=admin,CN=Users,DC=demo,DC=lab**
- Leave all other settings at their defaults and select **Finished**

Configure APM HTTP Basic SSO Profile

Navigate to **Access >> Single-Sign-On >> HTTP Basic > Click Create**

Name: **ephemeral_auth_clientcert-ephemeral-basic**

Username Source: **session.ldap.last.attr.sAMAccountName**

Password Source: **session.custom.ephemeral.last.password**

Click **Finished**

Configure APM Portal Access List for BIG-IP Shell

While the script run at the beginning of this article does indeed create a portal access list with resources, we will go ahead and create one in order to show a bit more of the solution and its inner workings.

- Navigate to **Access >> Connectivity / VPN >> Portal Access >>** Click **Portal Access List**
- Click **Create**
- Name: **LyonsPortalAccess**

- Link Type: **Application URI**
- Application URI: **https://IPofWebSSHVS:2222/ssh/host/mgmtIP**
- Caption: **BIG-IP Shell**
- Click **Create**

- Click **Add** to create a resource item.

- Link Type: **Paths**
- Destination: **IP Address of your WebSSH virtual server**
- Paths: **/***
- Scheme: **https**
- Port: **2222**
- SSO Configuration: **ephemeral_auth_clientcert-ephemeral-basic**
- Click **Finished**

Configuring APM Access Policy to Support Smart Card Authentication

- Navigate to **Access >> Profiles / Policies: Access Profiles (Per-Session Policies)**
- From here we are going to use the prebuilt policy as our template by selecting **Copy**.

- Provided a Copied Profile Name and select **Copy**.

- You will be returned to the previous screen automatically.
- Select **Edit** in the same row as the profile you created above.

This policy was created for demo purposes only though it also provides a very good starting point for configuring our own policy to support smart card authentication.

- From the page shown in the screenshot above, select the X above the Logon Page to remove it from our visual policy editor.

- Leave the defaults and select **Delete**.

- Once removed, select the **+** between **USG Warning Banner** and **Admin Access**.

- Select the **Authentication** tab and add **On-Demand Cert Auth**
- Click **Add Item**

When prompted to select the Auth Mode, select **Require** from the drop down menu and click **Save.**

- Once you have been returned to the visual policy editor, select the **+** between On-Demand Cert Auth and Admin Access following the Successful branch.

- From the Assignment tab, select **Variable Assign** and click **Add Item**

- When redirected to the page to configure variables as shown below, select **Add new entry.**

- When redirected, select **change** on line item 1.

We will configure the following variables based on F5 solution article K17063 found at *https://support.f5.com/csp/article/K17063*.

- In the **Custom Variable** section, type **session.logon.last.username.**
- In the **Custom Expression** section, type the following.

```
set upn [mcget {session.logon.last.upn}];
# if $upn contains @ symbol, extract the username, otherwise return $upn as-is.
if { $upn contains "@" } {
# Use string first to find index of the @ symbol, then return everything in-front of the @.
return [string range $upn 0 [expr { [string first "@" $upn] - 1 } ] ]; } else {
# Assume UPN only contains a username
return $upn;
}
```

- Click **Finished**
- Once again click **Add new entry** and select **change.**
- In the **Custom Variable** section, type **session.logon.last.upn.**
- In the **Custom Expression** section, type the following.
- Click **Finished**

```
set x509e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"];  # For each element in the li
if { $field contains "othername:UPN" } {  ## set start of UPN variable  set start [expr {[string firs
```

- Click **Save**
- Navigating back to the visual policy editor, select the **+** between Variable Assign and Admin Access

- From the Authentication tab, select **LDAP Query** and click **Add Item**.

When redirected to the LDAP Query Properties page, configure the following.

- From the drop down menu select the LDAP AAA Server created in previous steps.
- SearchDN: CN=Users,DC=demo,DC=lab
- SearchFilter: userPrincipalName=%{session.logon.last.upn}
- Click **Add new entry** and add **memberOf**
- Click **Add new entry** and add **sAMAccountName**

- Select the **Branch Rules** tab
- Remove the text **User Group Membership**
- Type **LDAP Query Passed**
- Click **change** following the branch rule expression

- Click the X as shown below to remove the existing expression.

- Click **Add Expression**
- From the **Agent Sel** drop down menu select **LDAP Query**
- From the **Condition** drop down menu select **LDAP Query Passed**
- Click **Add Expression**

- Click **Finished**
- Click **Save**
- From the Admin Access Macro click **Advanced Resource Assign**

- Click **Add/Delete**

- Select the **Portal Access** tab, remove the check box from the sample_pua_policy-webssh_portal and place a check box in the portal access resource created in the previous steps.
- Click **Update**

- Click **Save**

- In the top left hand corner of the VPE, click **Apply Access Policy**

You have now completed the VPE portion of the access policy.

Configure the PUA Webtop Virtual Server

- Navigate to **Local Traffic >> Virtual Servers >>** click **pua_webtop**

- Scroll until you locate **SSL profile (Client)** and assign the SSL profile created in the previous steps.

- Scroll until you reach the **Access Policy** portion of the VS.
- From the Access Profile drop down select the profile created in the previous step.

- Click **Update**
- Click the **Resources** tab

- From the **Default Pool** drop down menu, select the Pool created earlier in this document.
- Click **Update**

Configure BIG-IP Authentication

- Navigate to **System >> Users >> Authentication**
- From the Users Authentication page click **Change**
- From the User Directory drop down menu select **Remote - LDAP**
- Host: **IP of LDAP Virtual Server**
- Remote Directory Tree: **DC=demo, DC=lab**
- Scope: **Sub**
- Bind DN**: CN=admin,CN=Users,DC=demo,DC=lab**
- Check the box next to **Check Member Attribute in Group**
- Login LDAP Attribute: **sAMAccountName**
- Click **Finished**

Configuring Remote Role Groups

Navigate to **System > Users > Select Remote Role Groups**

- Click **Create**
- Group Name: **BIGIPAdmins**
- Line Order: **1**
- Attribute String:**memberOF=CN=BIGIPadmins,OU=Groups,DC=demo,DC=lab** Note: Use the full DN of the active directory security group you are defining with a preceeding 'memberOF='.
- Assigned Role: **Administrator**
- Partition Access: **All**
- Terminal Access: **tmsh**

Validation Testing

For my validation testing, I created a DNS record for webtop.demo.lab pointing to my webtop virtual server.

- From a web browser navigate to webtop.demo.lab.

- Click **OK, Proceed to Application**
- Select your user certificate when prompted and click OK

- From the Webtop, select the portal access resource you created in previous steps.

If authentication is successful, you will be presented with a webSSH session as shown below.

While this wraps up an overview of deploying and accessing F5's WebSSH capability with integrated smart card authentication, I would like to continue this into a series which includes other network devices or applications, end point checks, restricting access to the management interface and more. If this benefits at least one of you out there this was well worth it for me. Until next time.