F5 SSL VPN and SendQuick ConeXa One-time-Password Configuration Guide

Prepared by

TalariaX Pte Ltd
76 Playfair Road
#08-01 LHK2
Singapore 367996
Tel: 65-62802881
Fax: 65-62806882

F5 SSL VPN & SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure F5 SSL VPN to run with SendQuick Conexa for One-time-password via SMS.

TESTING ENVIRONMENT	
Product Name	
SendQuick Conexa	F5 Big IP Access Policy Manager

The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

2.0 CONFIGURE F5 SSLVPN

Open a web browser and access the Internet address (URL) for F5 access.
To create an AAA server

- On the Main tab, expand Access Policy, and then click AAA servers.
- Click the Create button.
- In the Name box, provide a name for the sendQuick Conexa (eg, Conexa).
- From the Type list, select the RADIUS protocol.
- Mode : Auth
- Auth Host : IP address of sendQuick Conexa
- Auth Service Port : 1812 (this must be 1812 as this is the port used in Conexa)
- Shared secret (the same secret need to be included in Conexa)
- NAS IP Address : IP address of F5
- Timeout – configure a value of between 40-60 seconds (value need to be higher than 25 seconds for the system to perform well)

- Click Finished.

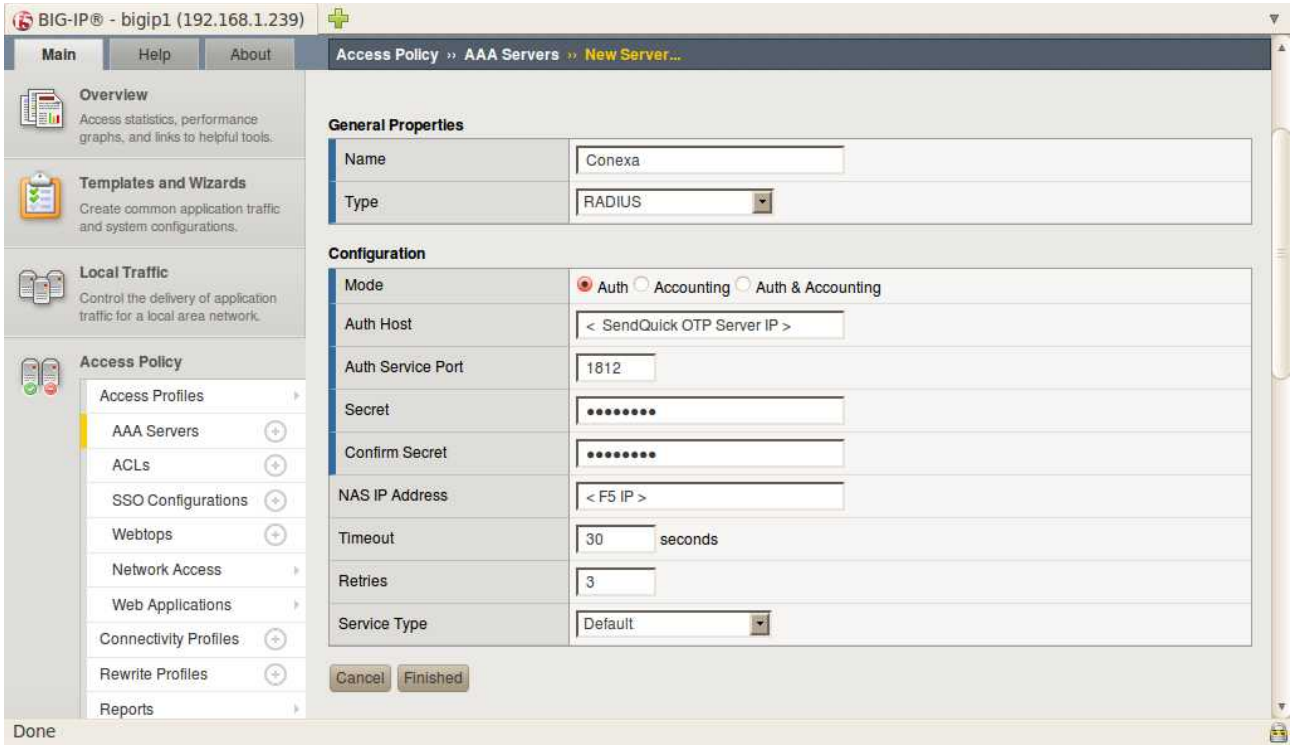

Figure 1: New AAA server configuration

To Edit the Access Profile

1. On the Main tab, expand Access Policy, and then click Access Profiles.

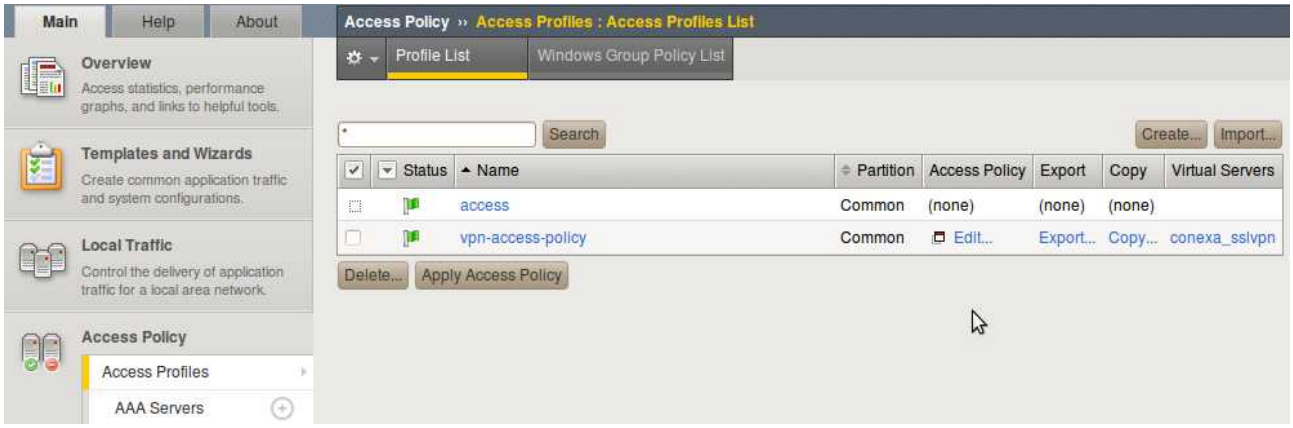

Figure 2 : Access Profiles List

2. Locate the Access Profile you created, and in the Access Policy column, click Edit. The Visual Policy Editor opens. (See Figure 3)

3. Click the + symbol between Logon Page and Deny.

4. In the Authentication section, click the RADIUS Auth option button, and then click the Add Item button.

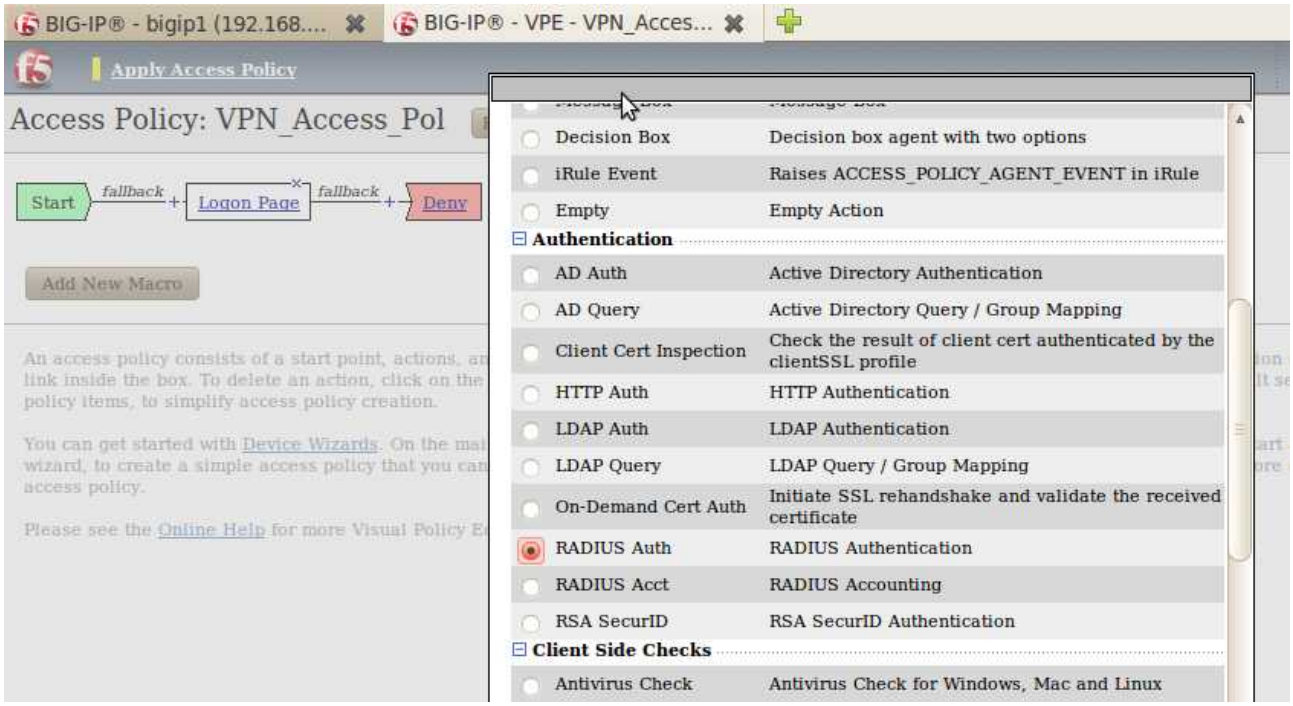

Figure 3 : RADIUS Authentication box on the Visual Policy Editor

5. From the Server list, select the AAA Source you created in Creating an AAA resource, (see Figure 4).

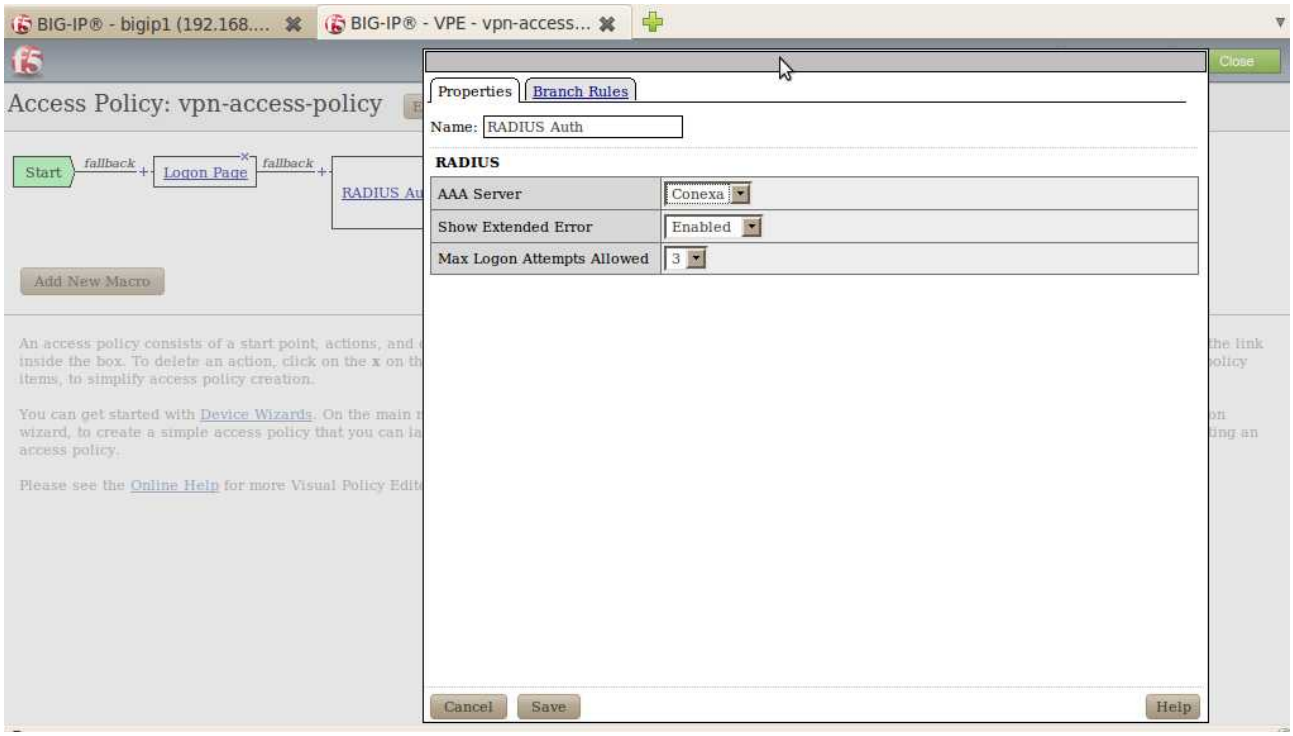

Figure 4 : RADIUS Authentication box on the Visual Policy Editor

6. Click the Save button. You now see two paths, Successful and Fall Back. (See Figure 5)

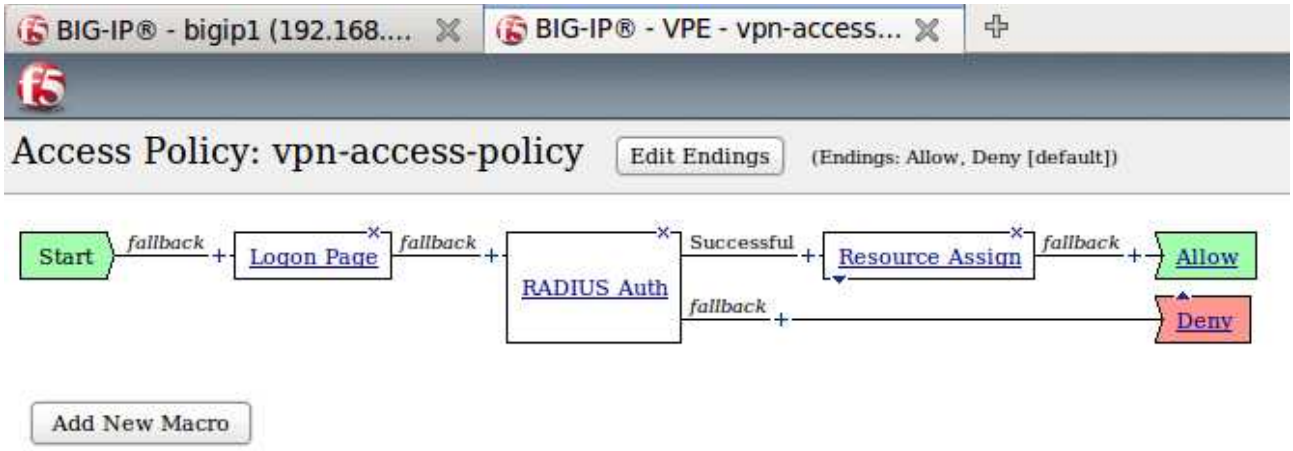

Figure 5 : Final result of our Access Policy example

Once the configuration is completed, select Apply Access Policy as shown in Figure 6 below.

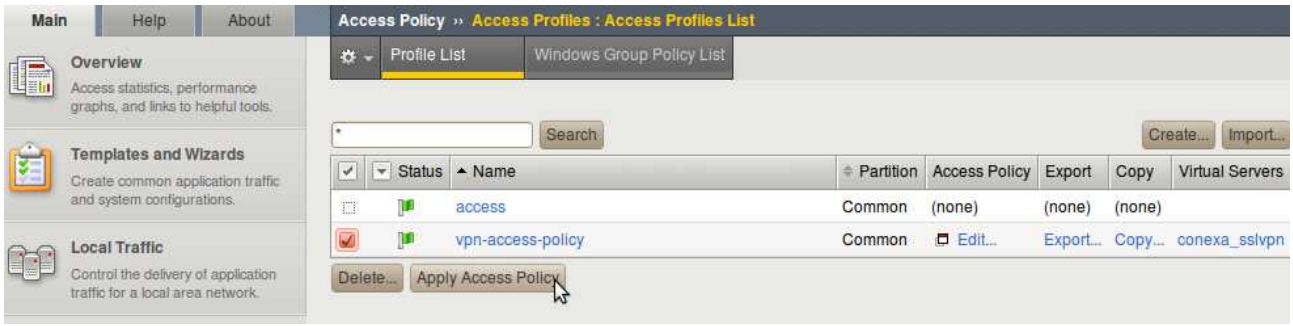

Figure 6 : Apply Access Policy

To select the name of the policy, On the Main tab, expand Local Traffic, click Virtual Servers and then select virtual server you created.
In the Access Policy section, from the Access Profile list, select the name of the policy you created in an Access Profile List.

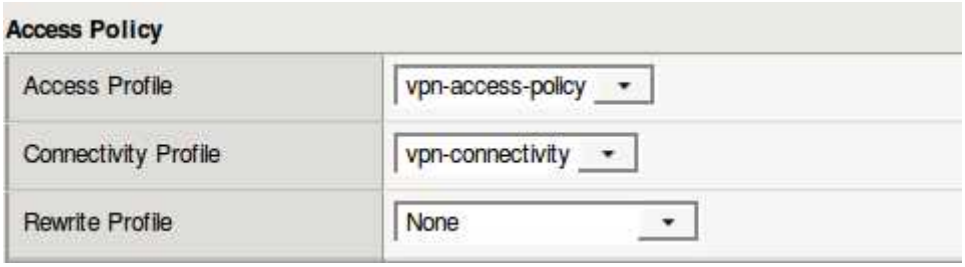

Figure 7 : Access Policy section of the virtual server configuration

3.0 CONFIGURE SENDQUICK CONEXA

Log in to sendQuick ConeXa **Admin** Page (Fig 8). Select **New Radius Configuration**.

Configure the following items as below

- IP address and description – IP address and description for F5
- Radius status - Enable
- Radius Secret – Use the same shared secret text string that was earlier configured on F5

Click **Submit** when completed

Figure 8: Radius configuration on sendQuick

Next, go to **Configuration** tab and select **New OTP Configuration.** See Figure 9 below.

Configure the following items as below:

- NAS IP and VPN description – F5 NAS IP and desc
- Authentication Type – Select desired authentication type

If LDAP is used, configure the following:

- LDAP Login Mode and IP address – LDAP server login details and IP address
- LDAP Query Attribute - LDAP Query Attribute for sendQuick to access. For example, “mobile” for the mobile number used by sendQuick to deliver OTP by SMS
- LDAP Base DN
- LDAP Domain

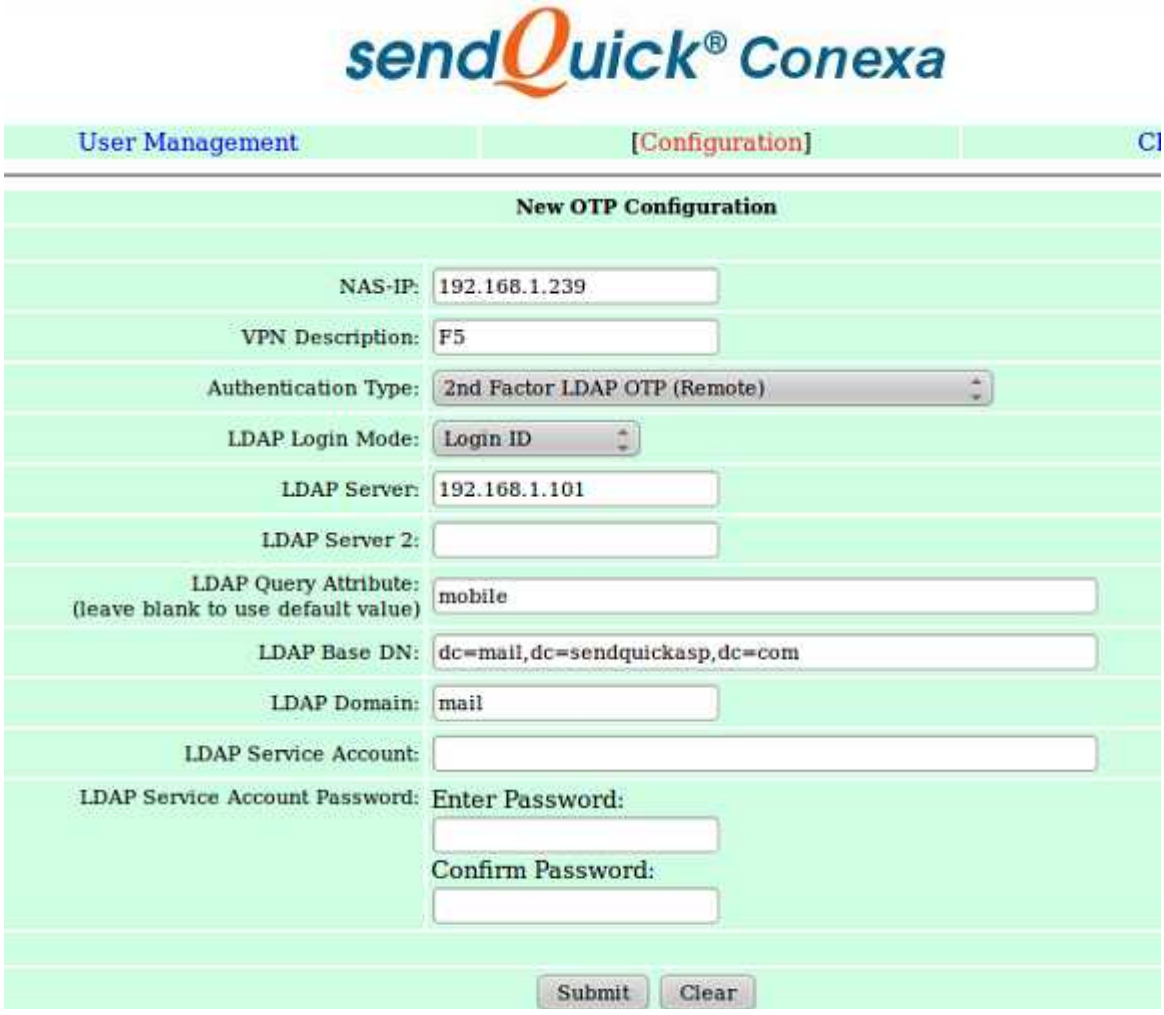

Figure 9: 2 Factor Authentication configuration on sendQuick

4.0 REMOTE ACCESS WITH TWO FACTOR AUTHENTICATION

I. Using F5 Edge Client

Establish a SSL VPN connection using the F5 Edge Client. After click connection, the page for Username and Password will appear as shown in Figure 10 below.

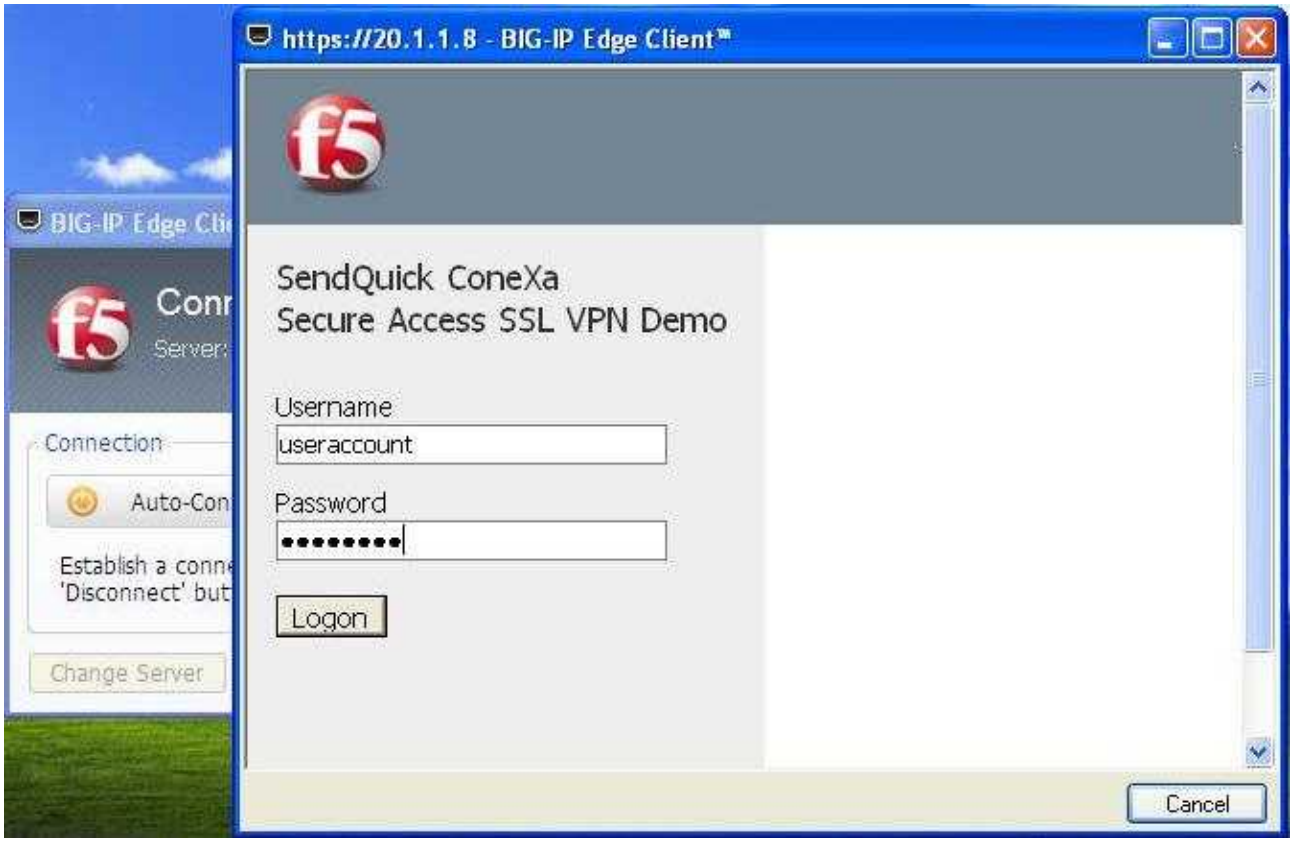

Figure 10 : F5 Login with Username and Password

Enter the Username and Password and click Logon. Once the first authentication is successful, the Enter OTP page will appear as shown in Figure 9 below. The OTP will be sent to the mobile phone. Enter the OTP in the space provided and click Logon.

Figure 11 : OTP Prompt

Once successfully connected, the client will display a Connected message and the Inbound and Outbound Traffic byte per second (b/s) will start increasing.

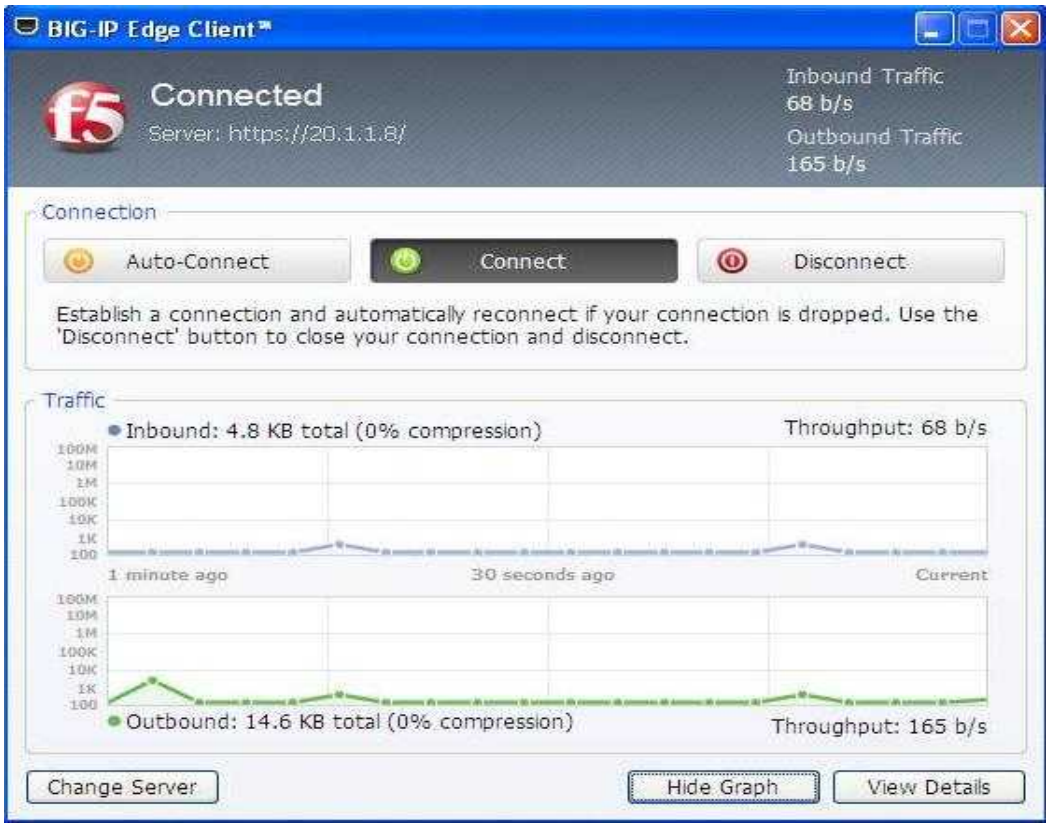

Figure 12 :

Figure 13 : Successful Connection for F5 Edge Client

II. Using SSL VPN

When accessing using SSL VPN, open a web browser and access the Internet address (URL) for SSL VPN access. The Username and Password will appear as shown in Figure 14 below.

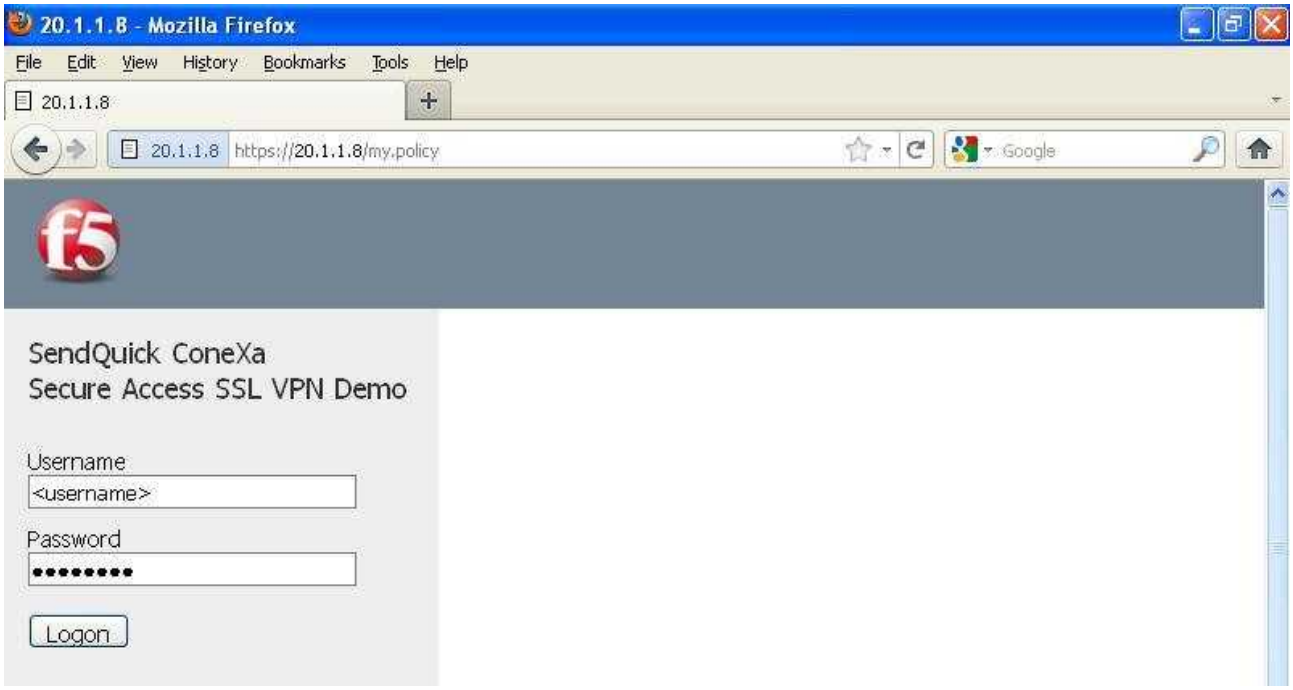

Figure 14 : SSLVPN Login with Username and Password

Enter the Username and Password and select Logon. Once the first authentication is completed, an Enter OTP page will appear. The SMS will be sent to the mobile phone. Enter the OTP in the Response space provided and select Continue, as shown in Figure 15 below. Once the second factor authentication is approved, the success page will be shown as in Figure 16 below.

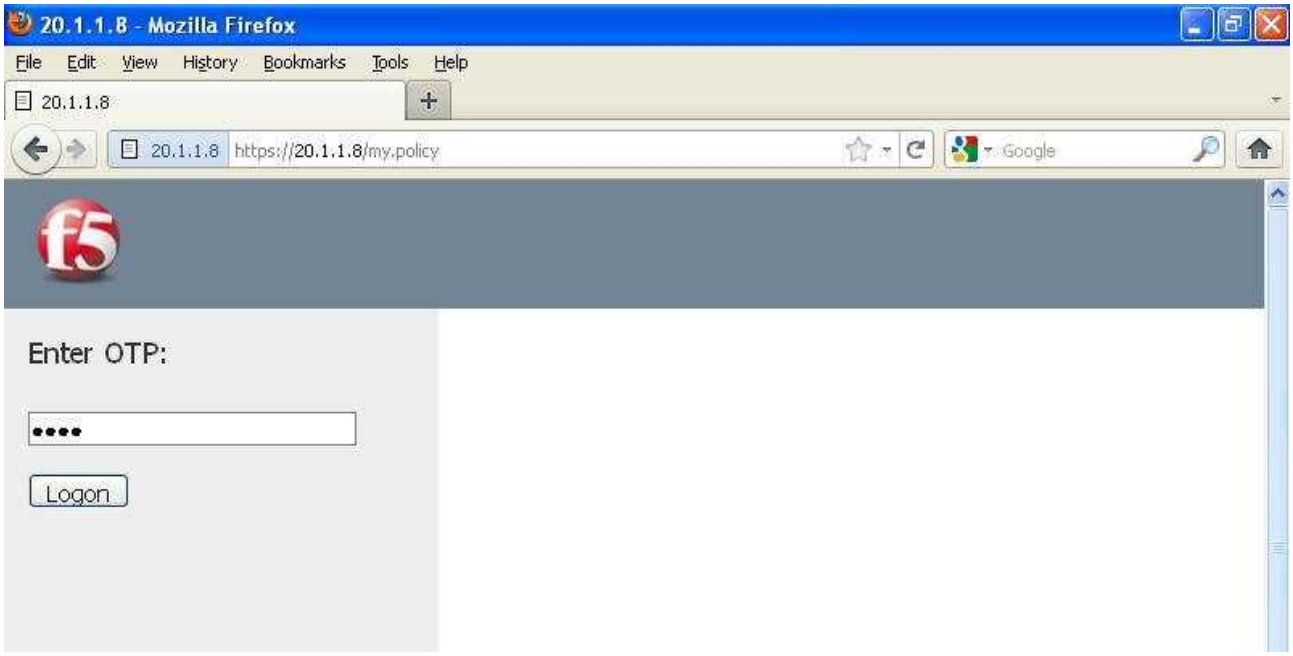

Figure 15 : Enter OTP for SSL VPN Authentication

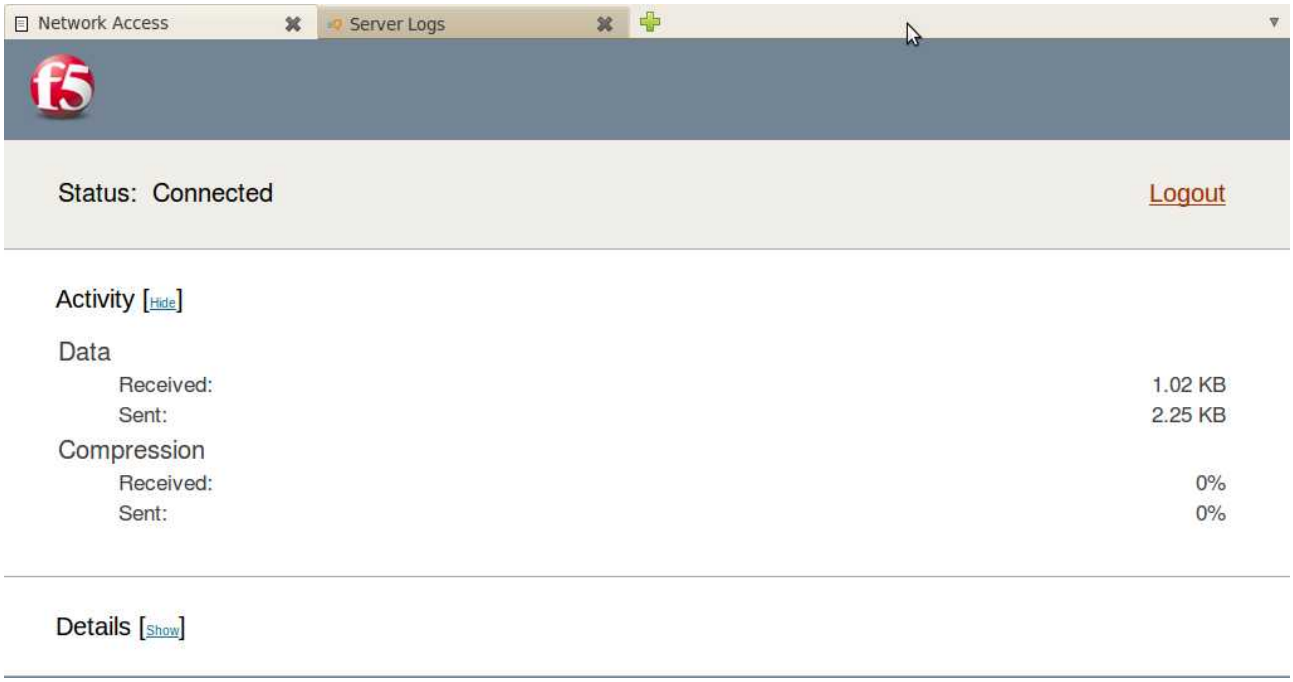

Figure 16 : Successful Access with SSL VPN