Business Process Forwarder Set to Work

These instructions assume that they are being executed on a recent Windows Operating System. Some adaptation will be necessary, particularly steps 11-16, if executing on a Linux or Mac operating system.

Preparation for AWS EC2 instance build

1. Create AWS account.
    a. Navigate to https://aws.amazon.com/ and select ‘Create an AWS Account’ to create a root user account.
    b. Once logged in, select IAM, and create a subordinate IAM user:
        i. Create a new User Group, e.g. “AWS_Instance_Creators” and assign the following permissions to the group: “AmazonEC2FullAccess” and “AmazonVPCFullAccess”
        ii. Create a new User, e.g. “EC2_Builder”. Assign the new user to the User Group created above in i). Note: When prompted, this user only requires programmatic access (i.e. not Management Console access).
        iii. Store the provided User “Access Key ID” and “Secret Access Key” securely.
    c. Create a key pair to support remote SSH access of the cloud EC2 instance that will be established in future steps:
        i. Navigate to your desired AWS region, e.g. London (eu-west-2)
        ii. Navigate to EC2>Key pairs and click on ‘Create key pair’.
        iii. Provide a name for the key pair, e.g. “AWS_BPFwd_Putty”
        iv. When prompted, select RSA, and .ppk options
        v. Create key pair and save locally on your PC.

2. Install Terraform, which will support the automated building of the cloud platform.
    a. Install the Terraform CLI, following instructions here: https://learn.hashicorp.com/tutorials/terraform/install-cli?in=terraform/aws-get-started
    b. Install AWS CLI, following instructions here: https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

Build the AWS cloud infrastructure (Virtual Private Cloud and EC2 instance)

3. Download the BPForwarder installation files from Github and store in a working directory: https://api.github.com/repos/WD-Dissertation/BPForwarderPlatform/releases/latest
4. Open a CMD window in the working directory.
5. Type the following commands:
    a. `terraform init`
    b. `terraform validate`
    c. `terraform apply`, type '`yes`' and enter when prompted.
6. The AWS cloud infrastructure build is now completed.
7. Run the following command and note the EC2 instance's public_ip address:
    a. `terraform state show aws_eip.BPWebserverEIP`
    b. public_ip:

Configure the SIEM

8. If a SIEM isn't already installed locally, install your preferred SIEM now following the vendor instructions. If you don't have a preference, download and install Kiwi Syslog Server Free Edition from: https://www.solarwinds.com/kiwi-syslog-server/pricing
9. Configure the SIEM to listen for Syslogs from localhost (127.0.0.1) and TCP Port 1468. Note: Must use TCP Port, UDP packets are unable to be sent over a reverse SSH tunnel.
10. If using Kiwi Syslog Server Free edition:
    a. Open Kiwi Syslog Server Console from the Windows Start menu.
    b. Select 'File' and 'Setup'
    c. Select the 'Inputs' menu item in the left pane. Add localhost IP Address (127.0.0.1), and click 'Apply'.
    d. Select the 'TCP' menu item in the left pane. Check the 'Listen for TCP Syslog messages' box, and type in TCP Port 1468. Click 'Apply' and Ok.

Preparation for remote SSH login to AWS EC2 instance

11. Download, install and open Putty: https://www.putty.org/
12. On the 'Session' tab, input the following:
    a. Host Name: ubuntu@[public Ip Address noted in 7.b. above]

b. Port: 22

c. Connection Type: SSH

13. In the Saved Sessions pane, type a Session name, e.g. “AWS_BPForwarder” and click ‘Save’.

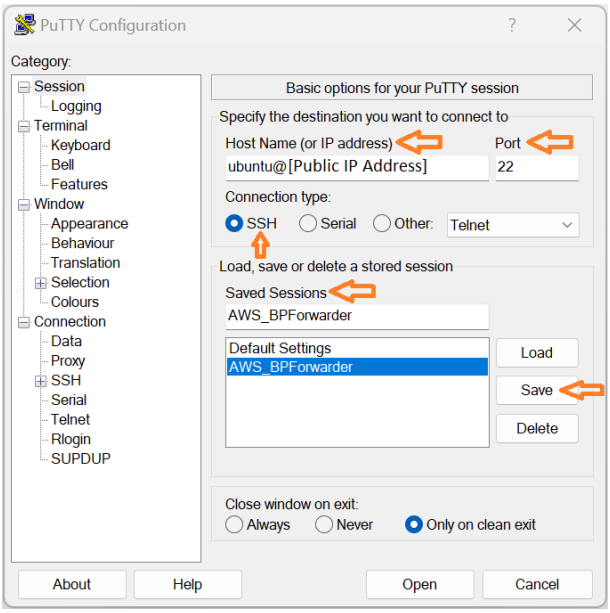

Figure 1 PuTTY Basic options configuration

14. On the ‘Connection>SSH>Auth’ tab, click on ‘Browse’ and navigate to the key pair file saved in step 1.c.v.

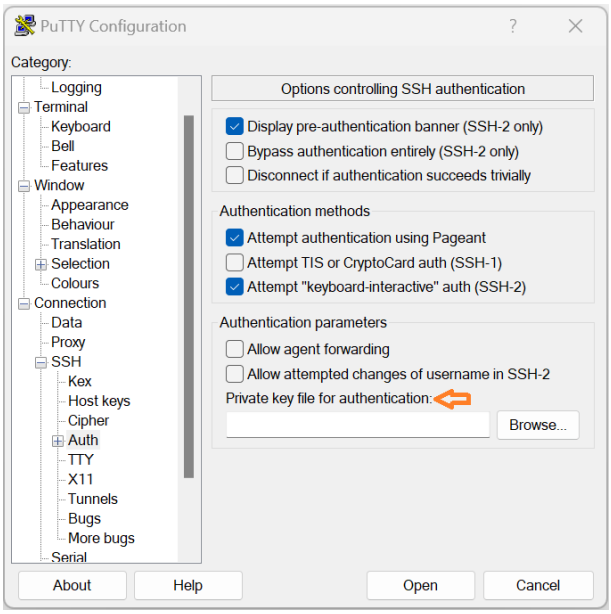

Figure 2 PuTTY key pair authentication configuration

15. On the ‘Connection>SSH>Tunnels’ tab, input the following:

a. Select “Local ports accept connections from other hosts”

b. Select “Remote ports do the same (SSH-2 only)

c. Source Port: 2210

d. Destination: localhost: 1468

e. Click ‘Remote’ and ‘IPv4’

f. click ‘Add’

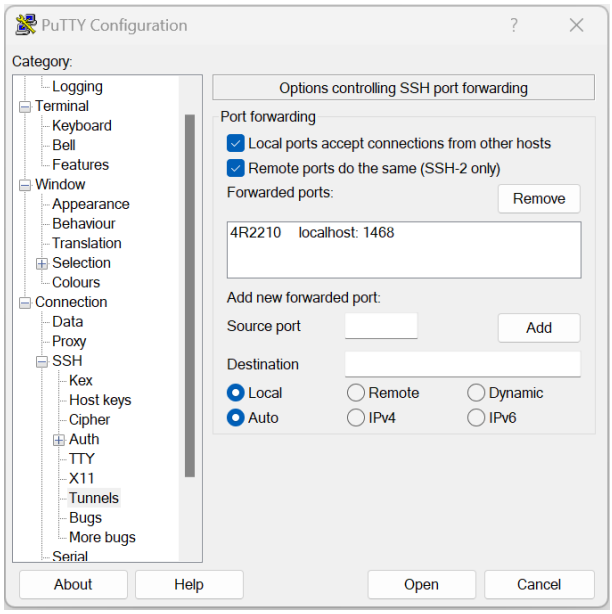

Figure 3 PuTTY reverse SSH tunnel configuration

16. Return to ‘Session’ tab, click ‘Save’
17. Open puTTYgen, which was installed alongside PuTTY by default.
18. Click the ‘Load’ button and navigate to the key pair file saved in step 1.c.v. Click “Open”.
19. Enter a strong passphrase, as defined in NIST 800-63b *Password Guidelines and Best Practices*. Ensure you can remember the passphrase, or record within a password manager.
20. Click “Save private key”, and overwrite the existing private key. The private key now requires the passphrase to use.

Build BPForwarder webserver

21. ‘Open’ the SSH connection saved in step 16. Note: If the Putty Security Alert is prompted, click ‘Accept’ to store the SSH keys within registry cache.
22. Once logged into Ubuntu, type the following commands into the terminal:
    a. `cd /home/ubuntu/`
    b. `mkdir BPForwarder`
    c. `cd BPForwarder`

d. `wget https://github.com/WD-Dissertation/BPForwarderPlatform/archive/refs/tags/v1.0.tar.gz`

e. `tar -xvf v1.0.tar.gz`

f. `sudo cp /home/ubuntu/BPForwarder/BPForwarderPlatform-1.0/BuildBPForwarderWebserver.sh .`

g. `sudo chmod 755 BuildBPForwarderWebserver.sh`

h. `sudo ./BuildBPForwarderWebserver.sh`

23. The BPForwarder Platform is now operational.

24. Apply a strong passphrase for the root user by typing the following commands:

    a. `sudo -i`

    b. `passwd`

    c. `[Enter and re-type new password]`

    d. `Exit`

25. Root password has been changed. Ensure you can remember the passphrase, or record within a password manager.

Edit BPForwarder Configuration file for target cloud BPM platform

26. Navigate to BPFconf.JSON file within the /home/ubuntu/BPForwarder directory on the webserver. Open with a native editor, such as 'vim', and configure the subject BPM platform's identifier and desired parameters.

27. Note: If the subject BPM platform's documentation does not adequately describe its webhook structure, it may assist to send a test webhook to webhook.site (Fredsted, 2022), to provide the opportunity to inspect it and determine the paths to identifiers and desired parameters.

28. Type the following commands to restart the WSGI service and check its status is "online":

    a. `sudo systemctl restart BPForwarder`

    b. `sudo systemctl status BPForwarder`

Test with subject BPM platform

29. Navigate to the cloud-based BPM platform and configure a sample business process.

30. Configure the BPM platform to output a webhook to the domain name of your webserver, appending '/webhook' to the end of the address.

31. Create a new instance of your business process (e.g. an Issue), and move it forward one step in the business process lifecycle.
32. You should observe your configured parameters arrive as a syslog in the SIEM.

Destroy AWS EC2 instance

33. If you wish to completely destroy the AWS EC2 instance and associated VPC, open a CMD window in the working directory created in Step 3, and type the following:
    a. `terraform destroy`