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 10-22, if executing on a Linux or Mac operating system.

These instructions also assume that a public domain name has been acquired/purchased. This is to support the issuing of an SSL certificate to enable HTTPS connections to BPForwarder. The example domain name used in this instruction is: wes-dissertation.me.

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 1.b.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

c. Follow instructions in the link above to configure the AWS CLI installation with the "Access Key ID" and "Secret Access Key" stored in para 1.b.iii. using the `aws configure` command in Windows CMD.

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://github.com/WD-Dissertation/BPForwarderPlatform/releases/tag/v2.0

4. Open the terraform.tfvars file and change:

   a. 'keyname' parameter to the key pair name created in 1.c.iii.

   b. 'region' to the desired region

   c. 'publicip' to the public IP address of your server/workstation

5. Open a CMD window in the working directory.

6. Type the following commands:

   a. `terraform init`

   b. `terraform validate`

   c. `terraform apply`, type '`yes`' and enter when prompted.

7. The AWS cloud infrastructure build is now completed.

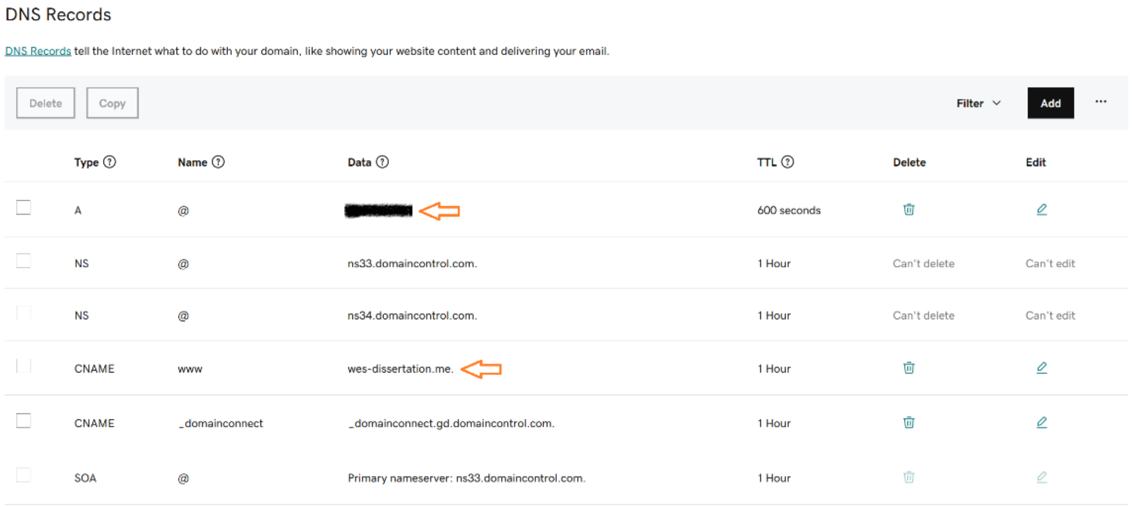
8. Run the following command and note the EC2 instance's public_ip address:

   a. `terraform state show aws_eip.BPWebserverEIP`

   b. public_ip:

Update Domain DNS settings

9. Configure the Type A DNS record for your domain with the public ip address recorded in step 8.b. An example of the GoDaddy.com DNS configuration pages is shown in Figure 1.



DNS Records

DNS Records tell the Internet what to do with your domain, like showing your website content and delivering your email.

	Type	Name	Data	TTL	Delete	Edit
□	A	@	[redacted]	600 seconds	🗑	✎
□	NS	@	ns33.domaincontrol.com.	1 Hour	Can't delete	Can't edit
□	NS	@	ns34.domaincontrol.com.	1 Hour	Can't delete	Can't edit
□	CNAME	www	wes-dissertation.me.	1 Hour	🗑	✎
□	CNAME	_domainconnect	_domainconnect.gd.domaincontrol.com.	1 Hour	🗑	✎
□	SOA	@	Primary nameserver: ns33.domaincontrol.com.	1 Hour	🗑	✎

Figure 1 GoDaddy Domain DNS configuration

Configure the SIEM

10. 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

11. 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.

12. 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

13. Download, install and open Putty: https://www.putty.org/

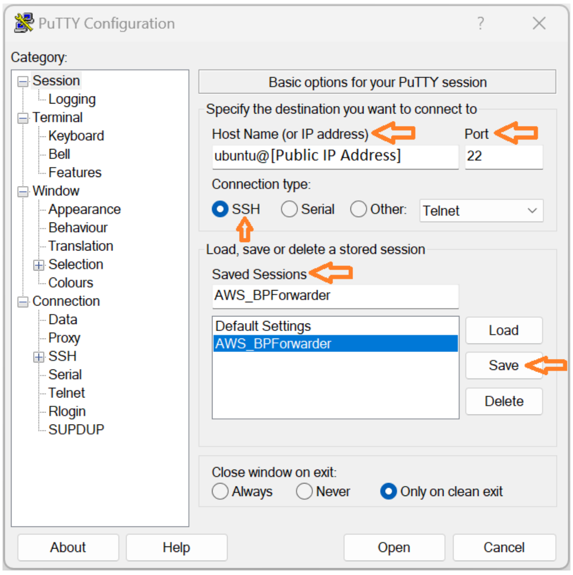
14. On the 'Session' tab, input the following:

    a. Host Name: ubuntu@[public Ip Address noted in 8.b. above]

    b. Port: 22

    c. Connection Type: SSH

15. In the Saved Sessions pane, type a Session name, e.g. "AWS_BPForwarder" and click 'Save'.



Specify the destination you want to connect to

Host Name (or IP address): ubuntu@[Public IP Address]

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

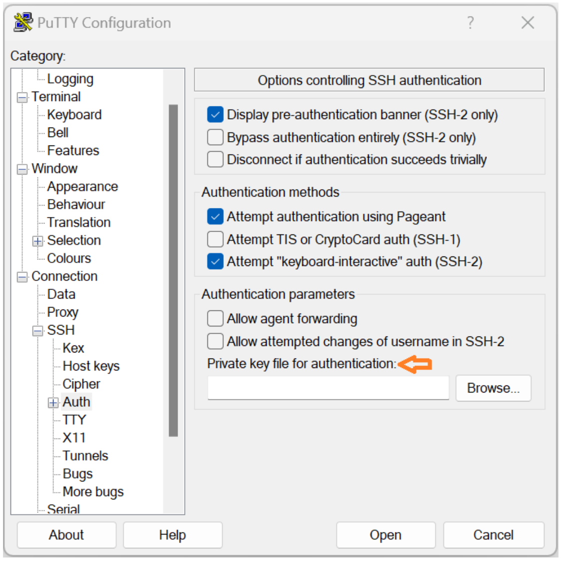
Saved Sessions: AWS_BPForwarder

Default Settings
AWS_BPForwarder

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 2 PuTTY Basic options configuration

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



☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)
☐ Disconnect if authentication succeeds trivially

Authentication methods
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters
☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

Figure 3 PuTTY key pair authentication configuration

17. On the 'Connection>SSH>Tunnels' tab, input the following:

    a. Select "Local ports accept connections from other hosts"

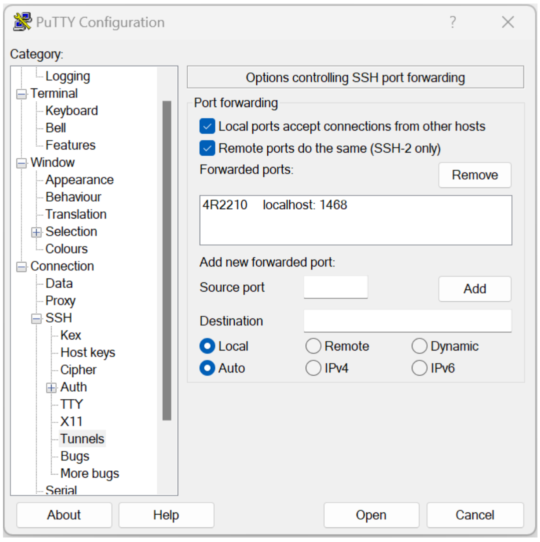
    b. Select "Remote ports do the same (SSH-2 only)

    c. Source Port: 2210

    d. Destination: localhost: 1468

    e. Click 'Remote' and 'IPv4'

f. click ‘Add’



Options controlling SSH port forwarding

Port forwarding

☑ Local ports accept connections from other hosts

☑ Remote ports do the same (SSH-2 only)

Forwarded ports:

4R2210 localhost: 1468

Add new forwarded port:

Source port

Destination

● Local ○ Remote ○ Dynamic

● Auto ○ IPv4 ○ IPv6

Figure 4 PuTTY reverse SSH tunnel configuration

18. Return to ‘Session’ tab, click ‘Save’
19. Open puTTYgen, which was installed alongside PuTTY by default.
20. Click the ‘Load’ button and navigate to the key pair file saved in step 1.c.v. Click “Open”.
21. 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.
22. Click “Save private key”, and overwrite the existing private key. The private key now requires the passphrase to use.

Build BPForwarder webserver

23. ‘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.
24. 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/v2.0.tar.gz`
    e. `tar -xvf v2.0.tar.gz`
    f. `sudo cp /home/ubuntu/BPForwarder/BPForwarderPlatform-2.0/BuildBPForwarderWebserver.sh .`

g. `cd BPForwarderPlatform-2.0`

h. Change the Domain configured in the ‘BPForwarderNGINXserverblockconfigHTTP’ file:

   i. `sudo vim BPForwarderNGINXserverblockconfigHTTP`

   ii. Click “INSERT” button on the keyboard

   iii. Replace “wes-dissertation.me” with acquired/purchased Domain.

   iv. Type `:wq!` to exit vim.

   v. `cd ..`

i. `sudo chmod 755 BuildBPForwarderWebserver.sh`

j. `sudo ./BuildBPForwarderWebserver.sh`

25. The BPForwarder Platform is now operational.

26. 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`

27. 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

28. 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.

29. 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.

30. 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

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

32. Configure the BPM platform to output a webhook to the domain name of your webserver, appending ‘/webhook’ to the end of the address.
33. Create a new instance of your business process (e.g. an Issue), and move it forward one step in the business process lifecycle.
34. You should observe your configured parameters arrive as a syslog in the SIEM.

Destroy AWS EC2 instance

35. 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`