Bursa Trade Securities 2 ('BTS2')

Fix Certification Environment

Site to Site Virtual Private Network Connection Guide

Prepared By:

Technology & Systems

TABLE OF CONTENTS

1 DOCUMENT CONTROL

1.1 REVISION HISTORY

Date	Author	Version	Change Reference
08-Feb-2012	Danny Ng	V1.0	Document Created
06-Mar-2012	Danny Ng	V1.1	Update the A1 form
21-Mar-2012	Danny Ng	V1.2	Update the content
16-Jan-2013	Reza Farouq	V1.3	Update content for Fix Cert Enviroment
23-Jan-2013	Raymond Tan	V1.4	Update the A1 form
30-Jan-2013	Danny Ng	V1.5	Update the A1 form
05-Feb-2013	Danny Ng	V1.6	Update the A1 form
23-Sep-2019	Murugiah Namasivayagam	V1.7	Removed the A1 form
18-Jan-2021	Reza Farouq	V1.8	Updated to support IKEv2

1.2 REVIEWERS

Date	Name	Position
10-Feb-2012	Raymond Tan	Head
10-Feb-2012	Baizura Ahmad	Head
25-Jan-2013	Danny Ng	Head

1.3 DOCUMENT PROPERTIES

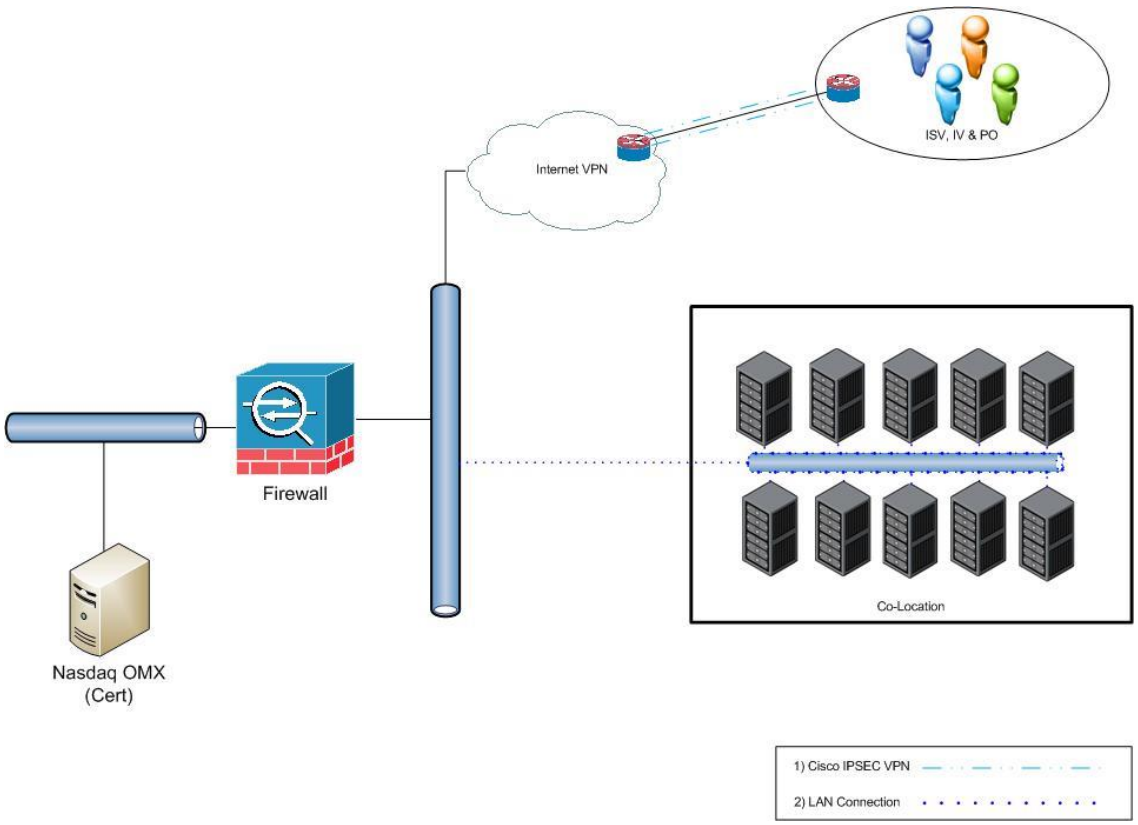
Item	Details
Document Title	Bursa Trade Securities 2 FIX Certification Environment VPN Connection Guide
Author	Danny Ng
Creation Date	08th Feb 2012
Last Updated	26th Apr 2021

2 VPN CONNECTIVITY GUIDE

2.1 OBJECTIVES

This documentation is meant to guide the users on how to configure and to manage their own network connection and connect to the new Bursa Malaysia Trade Securities 2 FIX Certification environment herewith known as 'BTS2 FIX CERT'.

The test participant users must have a high-speed connection to Internet for this Site to Site Virtual Private Network ('VPN') connection setup and connect to BTS2 FIX CERT environment.



High Level diagram for Internet VPN setup for accessing BTS2 Fix Cert Environment

2.2 REQUIREMENTS

1. New and existing Bursa test participants who require access to BTS2 FIX CERT environments must complete and submit the BTS2-A1 form to Bursa Malaysia. Kindly fax and e-mail completed form to IT Infrastructure, Fax: +603-20722567 email: bts2@bursamalaysia.com. All of the information requested on the form must be provided and please note the missing or ambiguous information may cause delays to the above request. Please contact Bursa Customer Service at +603-20265099 with additional questions regarding an existing VPN or a new VPN setup.

2. The VPN connection setup must meet the following requirements:

    - 1024 Kbps is the recommended connection speed.
    - The registered Public IP address must be static and routable on the Internet.

    The test participant Internet service provider (ISP) must support VPN protocols routing and switching.

3. IP Addresses Scheme – The test participant must configure their router or firewall for their server (i.e. 10.1.0.0/16) appears to have a private IP address from the RFC1918 IP address range provide by Bursa. This can be achieved by configuring the router or firewall to use network address translation ('NAT').

4. Hardware - The VPN router is recommended to have the following configuration:

NO.	PRODUCT CODE	DESCRIPTION
	Router & Module	
1.	CISCO1941/K9	CISCO Cisco141/K9 with 2GE, SEC License PAK,
2.	CAB-ACU	Power Cord UK
3.	UTP CABLE	UTP Cable, 10 feet (**x 2)
	Optional item	
5.	Switch	Switch to connect the router & application server. **Note: The UTP crossover cable can be used to connect the VPN router & application server when only 1 server used for the testing.

The test participant may opt for other model of Cisco router or to use Cisco ASA firewall. Please note the Cisco router to be installed must come with the security features set for enabling the IPSEC VPN connection to BTS2 FIX CERT environment. Please note we can only provide limited support if the test participant setup is a the Cisco router or Cisco firewall.

5. Software - The 'CISCO1921-**SEC/K9**' router software shall come with the minimum ***IOS version 15.7(3)M6*** which can support site to site vpn configuration using IKEv2 with following encryption requirements:

    - PSK for Internet Security Association and Key Management Protocol (ISAKMP)/IKE/IKE2
    - AES GCM 256 Encryption for ISAKMP/IKE/IKEv2
    - AES GCM 256 Encryption for IPSec

2.3 PROCEDURE TO SETUP THE VPN CONNECTION

1. Upon receipt of the BTS2-A1 form, Bursa Network Services engineer will review and evaluate the provided information. The engineer will send the following information to be used in configuring the test participant network:

    - A range of private addresses (i.e. RFC 1918) for test participant to assign addresses to testing hosts
    - A sample remote VPN router configuration
    - A unique pre-shared key (PSK) for authenticating devices and encrypting/decrypting packets

2. After Configuring the VPN Connection, the test participant can verify the connection by ping the BTS2 FIX CERT server network gateway IP address 10.1.117.1, and using a source IP address from the Bursa assigned private address range. Kindly ensure there should not have packet loss across the VPN connection by running the extended pings. This will verify basic network connectivity to BTS2 FIX CERT environments.
   ***Note**: You will not be able to ping the Bursa public IP VPN peer address 103.161.166.10 from anywhere on the Internet because we do not permit this traffic.*

3. The following Cisco IOS commands are helpful in troubleshooting issues that may arise when turning up new VPN connections:

    - sh crypto ikev2 isakmp sa | i 103.161.166.10 (a good output should show "READY" state)
    - sh crypto ipsec sa | b 10.1.117.0 (a good output will show packets being encapsulated and decapsulated with no errors)

3 GENERAL GUIDELINES

1. All requests must be submitted at least five (5) working days before the proposed test period. Bursa will revert on the acceptance of the request to the Test Participants on the following working day.

2. The BTS2 FIX CERT environment will be available on weekdays. Each session will occupy from 8:30am to 5:00pm from Monday to Friday. However, Bursa reserves the right to change the testing dates and times without giving prior notice.

3. Each Test Participant will be allowed to use the BTS2 FIX CERT environment a period of maximum ***three month*** at one time. Any further request to use the facility must be made again, as in (a) above and subject to availability and it is based on a first-come-first-serve basis.

4. Bursa Malaysia reserves the right to reject, reschedule or limit the requests.

5. Bursa Malaysia reserves the right to reject any request if Test Participant breaches any of Bursa Malaysia Policies.

6. Bursa Malaysia provides this facility to assist Test participants to test the interface between the systems and the functionality of the FIX application. This service provided should not be misused as a stress test facility.

7. Bursa Malaysia will provide the necessary network configuration and the Test Participants are expected to configure the test servers accordingly. The Test Participants are required to use the assigned network configuration and are responsible for the network configuration of the FIX systems and networking equipment.

8. Bursa Malaysia will not be responsible for any failure or delay of the testing activity of the Test Participants.

9. Bursa Malaysia reserved the right to claim against any damages caused by Test Participants.

4 APPENDIX – SAMPLE VPN ROUTER CONFIG

Test Participant Cisco Router Configuration

```
!
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service dhcp
!
hostname Customer-VPNrouter
!
boot-start-marker
boot-end-marker
!
logging buffered 163840
!
enable secret qwertyasdfgh
!
clock timezone MAL 8
!
no ipv6 cef
no ip source-route
ip cef
!
no ip bootp server
no ip domain lookup
!
! #(IKEv2 Phase 1 security policy will be provided upon new setup of VPN connection)
crypto ikev2 proposal AES-GCM-256
 encryption aes-gcm-256
 prf sha384
 group 19
!
 ! #(  IKEv2 profile and pre-shared key  will be provided upon new setup of VPN connection)
crypto ikev2 profile Profilename
 match identity remote address 103.161.166.10 255.255.255.255
 authentication remote pre-share key xxxxxxxxxxxxxxxxx
 authentication local pre-share key xxxxxxxxxxxxxxxxx
!
 ! #( IKEv2  Phase 2 security policy key  will be provided upon new setup of VPN connection)
crypto ipsec transform-set AES-GCM-256 esp-gcm 256
 mode tunnel
!
!
crypto map bursavpn xx ipsec-isakmp
 set peer 103.161.166.10
set transform-set AES-GCM-256
 set ikev2-profile Profilename
match address xxx
!
! #(Please use the IP address provided by Bursa)
interface f0/0
 ip address 10.1.x.x 255.255.255.224
 duplex auto
 speed auto
 no cdp enable
```

```
!
interface f0/1
 ip address 118.189.25.212 255.255.255.X   #(Please use the correct netmasks)
 crypto map bursavpn
 ip access-group 199 in
!
ip route 10.1.x.x 255.255.255.0 x.x.x.x#(Please use the correct gateway IP to Internet)
!
!
ip classless
no ip http server
no ip http secure-server
!
!
 #(the following ACL statement will permit the encryption/decryption traffic in IPSEC tunnel)
access-list xxx permit ip 10.1.x.x 0.0.0.31 10.1.x.x 0.0.0.255
!
access-list 199 permit ip 10.1.x.x 0.0.0.255 10.1.x.x 0.0.0.31
access-list 199 permit udp any any eq isakmp
access-list 199 permit ahp any any
access-list 199 permit esp any any
!
!
line con 0
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
```