Remote Access Setup to Bursa Malaysia Systems - MCO (ADAs/ADMs)

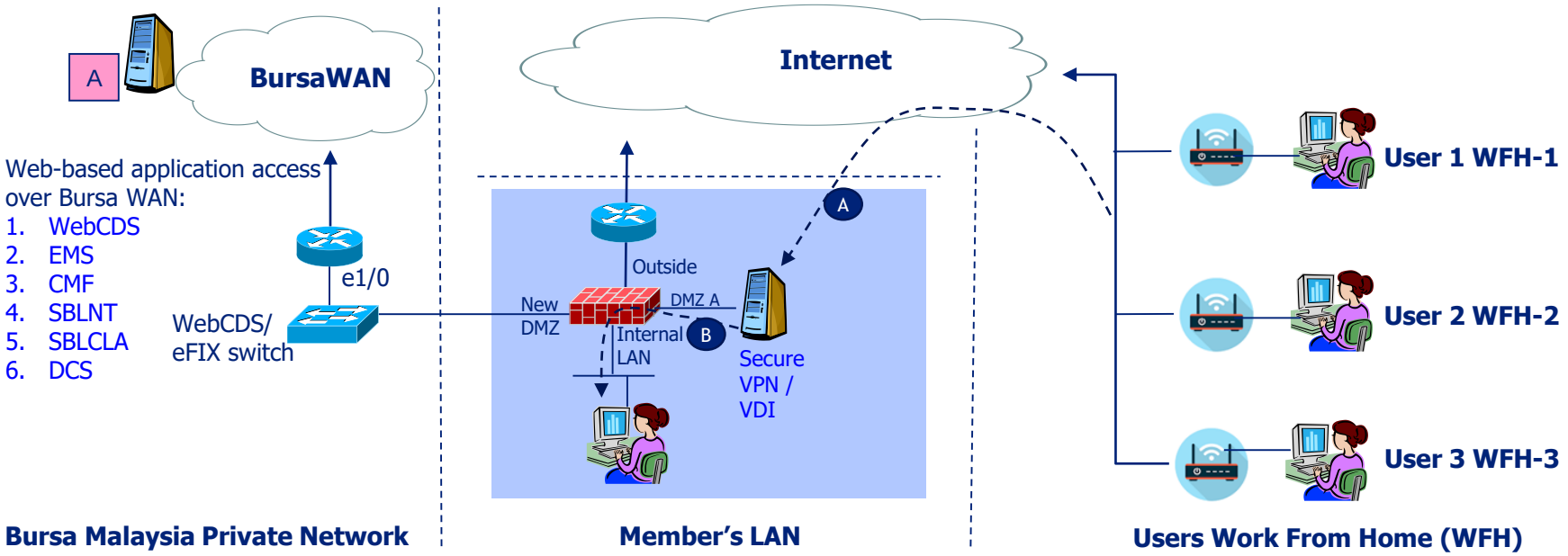
Web-based PCs IP address to be NATed to the IP range provided by Bursa (integrate with firewall)

Group Technology
Bursa Malaysia
2 April 2020

Remote Access Setup to Bursa Malaysia Systems - MCO

(ADAs/ADMs)

Web-based PCs IP address to be NATed to the IP range provided by Bursa (integrate with firewall)



Services/Port that needs to be enabled at member firewall or Security components

Traffic Flow	Source	Destination	Service	TCP/UDP	Remarks
A	10.X.X.129-254 *	10.X.X.XX 10.X.X.XX	443	TCP	** The IP details to be provided based on the need to know basis. Bursa technology team will liaise the IT coordinator.*

Notes:

1. ADA/ADM to inform the Exchange via email to cdssysadm@bursamalaysia.com for notation, if this is implemented.
2. In order to support the remote access, ADA/ADM IT team will need to perform the necessary network configuration and security controls within their IT infrastructure with secure VPN/VDI solution. ADA/ADM will need to map/allow (e.g. NAT, ACLs, Routing, physical, etc.) the IP addresses provided by Bursa Malaysia to enable the remote users for accessing the respective Web applications.
3. In the event if additional IP addresses are needed, ADA/ADM can apply it following the current process.

Remote Access Setup to Bursa Malaysia Systems - MCO (Cont.)

(ADAs/ADMs)

Web-based PCs IP address to be NATed to the IP range provided by Bursa (integrate with firewall)

Notes:

4. The following are the recommendations for risk mitigation when enabling the remote access setup:
   a) Must have authentication credential with complex password for secure VPN/VDI. In addition, 2FA is recommended as the passcode are dynamically generated and constantly changing which are safer to use than fixed (static) log-in information;
   b) Restrict access to limited IP ranges and TCP ports as well as time control for the remote access;
   c) The PC/Laptop for the user for this purpose is hardened and updated with latest end user device protection (i.e. AV, AM, APT, etc.) and must not come with administrator privileges;
   d) Do not use PUBLIC and unsecure network (i.e. cafe, restaurant, etc.) when accessing Bursa Malaysia Web-based application;
   e) The user must be made aware of their responsibilities and strictly adhere to procedures, guidelines & policies that align with SC/BURSA/BNM guidelines;
   f) To perform an assessment after the post implementation to validate if there is any impact on security. You can do this internally by someone who is independent of change execution. e.g. Internal Audit/CISO unit or to engage external party by conducting a Penetration Testing; and
   g) To ensure that you have ability to monitor, detect and respond in a timely manner to any event related to this change.

Thank you