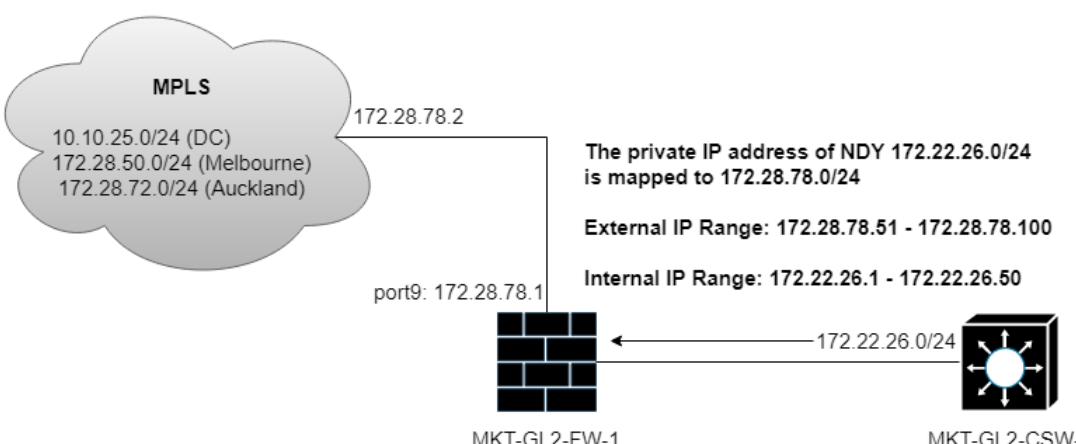


Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201916132			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	June 6, 2019			
Proposed Change Start/End Time	6:00 PM – 8:00 PM			
Proposed Change Verification Time	7:00 PM			

Objective of the change	
To configure and map the private address of NDY to the address given by TetraTech/Telstra.	
 <p>The private IP address of NDY 172.22.26.0/24 is mapped to 172.28.78.0/24</p> <p>External IP Range: 172.28.78.51 - 172.28.78.100</p> <p>Internal IP Range: 172.22.26.1 - 172.22.26.50</p>	

Technical/Operational Impact of the change		
Negative: Additional CPU and Memory consumption due to NAT and port6.	Beneficial: All tools of NDY will pass thru their own MPLS network.	Neutral: Additional cable for MKT-GL2-FW-2 for redundancy.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-FW-1	172.17.3.102	Site Firewall
G2	MKT-GL2-FW-2	172.17.3.102	Site Firewall

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
IT	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176328103

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

Test Environment implementation and Verification Summary

Testing will be after the implementation since there's no available test environment.

Test Environment Results Summary

Per testing, all networks given 10.10.25.0/24, 172.25.50.0/24, 172.28.72.0/24 should be reachable via NDY's private segment 172.22.26.0/24.

Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

Configuration Change Template

Baseline File	3.1.10.2
Baseline Version	April 18, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
There are no existing configurations.	To add IPv4 Policies, Static Routing, and NAT for NDY.	IPv4 Policies, Static Routing, Virtual IPs, IP Pools, Address Objects/Groups	3.1.10.2

Physical Implementation Procedures / Advisory

From NDY's router, connect a cable on port gi0/1 to port9 of MKT-GL2-FW-1.



Backup Procedures

Access FortiGate G2 via Web.

Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg

Example: BACKUP_MKT-GL2-FW-1_642019.cfg

Technical Configuration Procedures

1. Access FortiGate G2 via Web.
2. Navigate to Policy & Objects then Virtual IPs. Create new Virtual IP with the following details:

Name	VIP_NDY	
Comments		
Color	Change	
Network		
Interface	Internal (port5)	
Type	Static NAT	
External IP Address/Range	172.28.78.51	172.28.78.100
Mapped IP Address/Range	172.22.26.1	172.22.26.50

3. Navigate to Policy & Objects then IP Pools. Create new IP Pools with the following details:

Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

Name	<input type="text" value="Pool_NDY"/>
Comments	<input type="text" value=""/> 0/255
Type	<input type="button" value="Overload"/> <input type="button" value="One-to-One"/> <input type="button" value="Fixed Port Range"/> <input type="button" value="Port Block Allocation"/>
External IP Range	<input type="text" value="172.28.78.51"/> - <input type="text" value="172.28.78.100"/>
Internal IP Range	<input type="text" value="172.22.26.1"/> - <input type="text" value="172.22.26.50"/>
ARP Reply	<input checked="" type="checkbox"/>

4. Navigate to Network then Interfaces. Edit port9 with the following details:

Alias: NDY
 Role: LAN
 Addressing mode: Manual
 IP/Network Mask: 172.28.78.1/24
 Administrative Access: PING
 Interface State: Enabled

5. Navigate to Network then Static Routes. Create new route entries with the following details:

Destination: Subnet - 10.10.25.0/24
 Interface: port9(NDY)
 Gateway Address: 172.28.78.2
 Administrative Distance: 10
 Comments: NDY DC
 Status: Enabled

Destination: Subnet - 172.28.50.0/24
 Interface: port9(NDY)
 Gateway Address: 172.28.78.2
 Administrative Distance: 10
 Comments: NDY Melbourne
 Status: Enabled

Destination: Subnet - 172.28.72.0/24
 Interface: port9(NDY)
 Gateway Address: 172.28.78.2
 Administrative Distance: 10
 Comments: NDY Auckland
 Status: Enabled

6. Navigate to Policy & Objects then Addresses. Create new Address objects and group with the following details:

Name: EXT_NDY_DC
 Type: Subnet
 Subnet / IP Range: 10.10.25.0/24

Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

Name: EXT_NDY_Melbourne
Type: Subnet
Subnet / IP Range: 172.28.50.0/24

Name: EXT_NDY_Auckland
Type: Subnet
Subnet / IP Range: 172.28.72.0/24

Address Group
Name: EXT_GR_NDY
Members: EXT_NDY_DC, EXT_NDY_Melbourne, EXT_NDY_Auckland

7. Navigate to Policy & Objects then Services. Create new Category, Service, and Service Group.

Category

Name: NDY Services

Services

Name	Comment	Category	Type	Destination Port	
NDY_53	DNS	NDY Services	TCP/UDP/SCTP	TCP - 53	UDP - 53
NDY_80	HTTP	NDY Services	TCP/UDP/SCTP	TCP - 80	UDP - 80
NDY_443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 443	
NDY_123	NTP	NDY Services	TCP/UDP/SCTP	TCP - 123	UDP - 123
NDY_389	LDAP	NDY Services	TCP/UDP/SCTP		UDP - 389
NDY_636	LDAP	NDY Services	TCP/UDP/SCTP	TCP - 636	
NDY_1494	ICA	NDY Services	TCP/UDP/SCTP	TCP - 1494	UDP - 1494
NDY_1812	Radius	NDY Services	TCP/UDP/SCTP	TCP - 1812	UDP - 1812
NDY_2589	Session	NDY Services	TCP/UDP/SCTP	TCP - 2589	UDP - 2589
NDY_3268	LDAP	NDY Services	TCP/UDP/SCTP		UDP - 3268
NDY_3269	LDAP	NDY Services	TCP/UDP/SCTP	TCP - 3269	
NDY_9080	Active Sync	NDY Services	TCP/UDP/SCTP	TCP - 9080	UDP - 9080
NDY_9443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 9443	UDP - 9443
NDY_8443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 9443	UDP - 9443

Service Group

Name: NDY Ports

Members: NDY_53, NDY_80, NDY_443, NDY_123, NDY_389, NDY_636, NDY_1494, NDY_1812, NDY_2589, NDY_3268, NDY_3269, NDY_9080, NDY_9443, NDY_8443

Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

8. Navigate to Policy & Objects then IPv4 Policy. Create new IPv4 Policies for the outbound traffic with the following details:

Name: PublishRule NDY to Citrix Outbound
 Incoming Interface: internal(port5)
 Outgoing Interface: NDY(port9)
 Source: INT_SUB_NDY
 Destination: EXT_GR_NDY
 Schedule: always
 Service: NDY Ports
 Action: ACCEPT

NAT: Enabled
 IP Pool: Use Dynamic IP Pool - Pool_NDY

Log Allowed Traffic: Enabled - Security Events

Verification Procedures

1. Coordinate with NDY agents and have them test their Citrix connectivity.
2. Go to the Forward Logs of FortiGate and filter it by Policy: PublishRule NDY to Citrix Outbound. There should be a traffic passing thru.

Back-out Procedures

1. Navigate to Policy & Objects then IPv4 Policy. Delete the IPv4 Policy named **PublishRule NDY to Citrix Outbound**.
2. Navigate to Policy & Objects then Addresses. Delete the following Address group and objects:

Address Group
EXT_GR_NDY

Address Object
EXT_NDY_DC
EXT_NDY_Melbourne
EXT_NDY_Auckland

3. Navigate to Policy & Objects then Services. Delete all the services listed below:
4. Navigate to Policy & Objects then Services. Create new Category, Service, and Service Group.

Category

Name: NDY Services



Proprietary and Confidential

Effectivity:
 April 1, 2019

Page 6

Template Version : **02**

Process Owner: IT Operations	FORM	F-CMG-3.1
	Configuration Change Request	

Services

Name	Comment	Category	Type	Destination Port	
NDY_53	DNS	NDY Services	TCP/UDP/SCTP	TCP - 53	UDP - 53
NDY_80	HTTP	NDY Services	TCP/UDP/SCTP	TCP - 80	UDP - 80
NDY_443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 443	
NDY_123	NTP	NDY Services	TCP/UDP/SCTP	TCP - 123	UDP - 123
NDY_389	LDAP	NDY Services	TCP/UDP/SCTP		UDP - 389
NDY_636	LDAP	NDY Services	TCP/UDP/SCTP	TCP - 636	
NDY_1494	ICA	NDY Services	TCP/UDP/SCTP	TCP - 1494	UDP - 1494
NDY_1812	Radius	NDY Services	TCP/UDP/SCTP	TCP - 1812	UDP - 1812
NDY_2589	Session	NDY Services	TCP/UDP/SCTP	TCP - 2589	UDP - 2589
NDY_3268	LDAP	NDY Services	TCP/UDP/SCTP		UDP - 3268
NDY_3269	LDAP	NDY Services	TCP/UDP/SCTP	TCP - 3269	
NDY_9080	Active Sync	NDY Services	TCP/UDP/SCTP	TCP - 9080	UDP - 9080
NDY_9443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 9443	UDP - 9443
NDY_8443	HTTPS	NDY Services	TCP/UDP/SCTP	TCP - 9443	UDP - 9443

Service Group

Name: NDY Ports

Members: NDY_53, NDY_80, NDY_443, NDY_123, NDY_389, NDY_636, NDY_1494, NDY_1812, NDY_2589, NDY_3268, NDY_3269, NDY_9080, NDY_9443, NDY_8443

5. Navigate to Network then Static Routes. Delete all the route entries going to NDY.

Destination: Subnet - 10.10.25.0/24

Interface: port9(NDY)

Gateway Address: 172.28.78.2

Administrative Distance: 10

Comments: NDY DC

Destination: Subnet - 172.28.50.0/24

Interface: port9(NDY)

Gateway Address: 172.28.78.2

Administrative Distance: 10

Comments: NDY Melbourne

Destination: Subnet - 172.28.72.0/24

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

Interface: port9(NDY)
Gateway Address: 172.28.78.2
Administrative Distance: 10
Comments: NDY Auckland

6. Navigate to Network then Interfaces. Edit port9 to its default properties.

Alias: none
Role: undefined
Addressing mode: dhcp
Administrative Access: none
Interface State: Disabled

7. Navigate to Policy & Objects then IP Pools. Delete the IP Pool named **Pool_NDY**.
8. Navigate to Policy & Objects then Virtual IPs. Delete the Virtual IP named **VIP_NDY**.