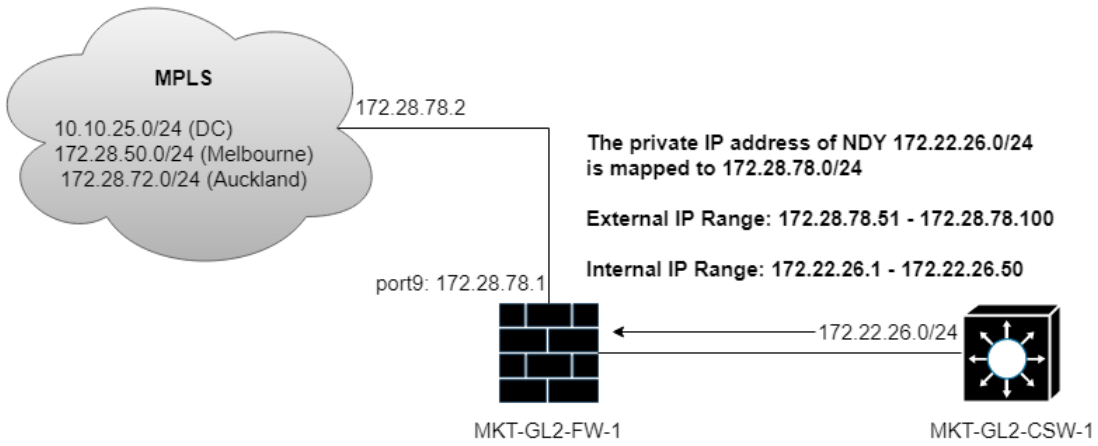
Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201916132			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	June 8, 2019			
Proposed Change Start/End Time	6:00 PM – 8:00 PM			
Proposed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



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

Test Environment implementation and Verification Summary

1. Connect a Laptop going to NDY Router gi0/0/1
2. Statically assign an IP that is inside the *172.28.78.0/24 range*

IP Address: *172.28.78.x*
Subnet Mask: *255.255.255.0*
Default Gateway: *172.28.78.2*

3. Run CMD and Ping the default gateway *172.28.78.2*
4. Ping the following IPs below

10.10.25.1
172.28.50.1
172.28.72.1

5. After pinging the following IPs do a traceroute. See command below

Tracert -d 10.10.25.1
Tracert -d 172.28.50.1
Tracert -d 172.28.72.1

Verification of the Testing should be as follows

PING

```
C:\Users\Ian Lastimoso>ping 172.28.78.2

Pinging 172.28.78.2 with 32 bytes of data:
Reply from 172.28.78.2: bytes=32 time<1ms TTL=255
Reply from 172.28.78.2: bytes=32 time=1ms TTL=255
Reply from 172.28.78.2: bytes=32 time=1ms TTL=255
Reply from 172.28.78.2: bytes=32 time=1ms TTL=255

Ping statistics for 172.28.78.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\Users\Ian Lastimoso>ping 10.10.25.1

Pinging 10.10.25.1 with 32 bytes of data:
Reply from 10.10.25.1: bytes=32 time=129ms TTL=249
Reply from 10.10.25.1: bytes=32 time=130ms TTL=249
Reply from 10.10.25.1: bytes=32 time=129ms TTL=249
Reply from 10.10.25.1: bytes=32 time=129ms TTL=249

Ping statistics for 10.10.25.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 129ms, Maximum = 130ms, Average = 129ms
```

```
C:\Users\Ian Lastimoso>ping 172.28.50.1

Pinging 172.28.50.1 with 32 bytes of data:
Reply from 172.28.50.1: bytes=32 time=130ms TTL=246
Reply from 172.28.50.1: bytes=32 time=130ms TTL=246
Reply from 172.28.50.1: bytes=32 time=132ms TTL=246
Reply from 172.28.50.1: bytes=32 time=130ms TTL=246

Ping statistics for 172.28.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 130ms, Maximum = 132ms, Average = 130ms
```

```
C:\Users\Ian Lastimoso>ping 172.28.72.1

Pinging 172.28.72.1 with 32 bytes of data:
Reply from 172.28.72.1: bytes=32 time=172ms TTL=246
Reply from 172.28.72.1: bytes=32 time=176ms TTL=246
Reply from 172.28.72.1: bytes=32 time=172ms TTL=246
Reply from 172.28.72.1: bytes=32 time=173ms TTL=246

Ping statistics for 172.28.72.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 172ms, Maximum = 176ms, Average = 173ms
```

TRACE ROUTE

```
C:\Users\Ian Lastimoso>tracert -d 10.10.25.1

Tracing route to 10.10.25.1 over a maximum of 30 hops

  1     1 ms    <1 ms     1 ms  172.28.78.2
  2     1 ms     1 ms     1 ms  10.219.124.161
  3     *        *        *     Request timed out.
  4   127 ms   127 ms   127 ms  10.219.124.169
  5   128 ms   128 ms   128 ms  10.219.124.170
  6   136 ms   127 ms   130 ms  10.10.18.254
  7   139 ms   134 ms   132 ms  10.10.25.1

Trace complete.
```

```
C:\Users\Ian Lastimoso>tracert -d 172.28.72.1

Tracing route to 172.28.72.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  172.28.78.2
  2     1 ms     1 ms     1 ms  10.219.124.161
  3     *        *        *     Request timed out.
  4   133 ms   127 ms   127 ms  10.219.124.169
  5   129 ms   129 ms   128 ms  10.219.124.170
  6   128 ms   128 ms   128 ms  10.10.18.254
  7   170 ms   170 ms   169 ms  203.97.184.220
  8   171 ms   171 ms   171 ms  172.31.0.17
  9   175 ms   184 ms   172 ms  172.31.0.2
 10   173 ms   173 ms   172 ms  172.28.72.1

Trace complete.
```

```
C:\Users\Ian Lastimoso>tracert -d 172.28.50.1

Tracing route to 172.28.50.1 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  172.28.78.2
  2     1 ms    <1 ms     1 ms  10.219.124.161
  3     *        *        *     Request timed out.
  4   127 ms   127 ms   127 ms  10.219.124.169
  5   129 ms   129 ms   129 ms  10.219.124.170
  6   128 ms   128 ms   128 ms  10.10.18.254
  7   130 ms   130 ms   131 ms  10.10.2.1
  8   128 ms   128 ms   128 ms  10.9.1.254
  9   130 ms   130 ms   130 ms  192.168.26.91
 10   130 ms   130 ms   130 ms  172.28.50.1

Trace complete.
```

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.

Configuration Change Template

Baseline File	3.1.10.2
Baseline Version	April 18, 2019

Baseline File Changes:

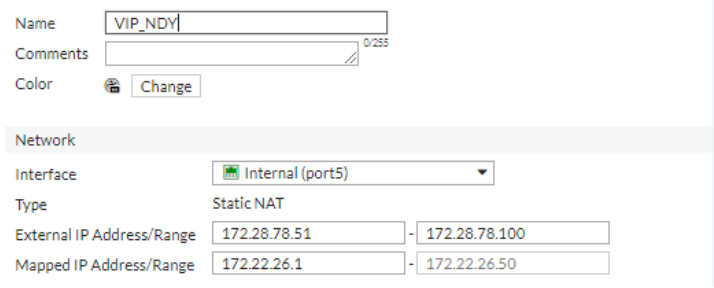
Existing Configuration	Proposed Change	Impact	Section
There are no existing configurations.	To add IPv4 Policies, Static Routing, and NAT for NDY.	IPv4 Policies, Static Routing, Virtual IPs, IP Pools, Address Objects/Groups	3.1.10.2

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

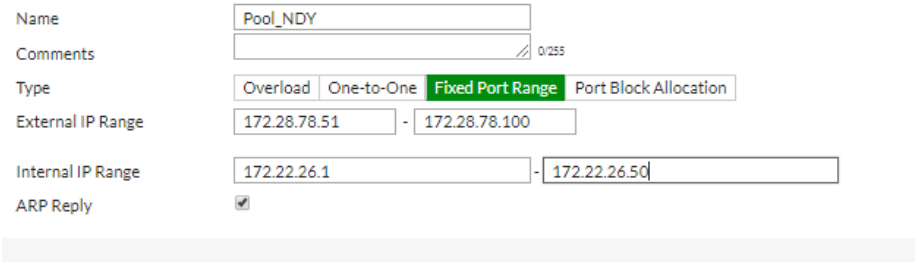
Backup Procedures
Access FortiGate G2 via Web. Backup the configurations files using the naming conventions: BACKUP_DEVICENAME_DATE.cfg Example: BACKUP_MKT-GL2-FW-1_642019.cfg

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:



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



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

   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

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

   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
   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**.