Entity	Name	Details
Main settings of the CloudBridge Connector tunnel setup		
IP address of the CloudBridge Connector tunnel end point (NS_Appliance-1) in Datacenter-1		• 198.51.100.100
IP address of the CloudBridge Connector tunnel end point (FortiGate-Appliance-1) in Datacenter-2		• 203.0.113.200
Datacenter–1's subnet whose traffic is to be protected over the CloudBridge Connector tunnel		• 10.102.147.0/24
Datacenter–2's subnet whose traffic is to be protected over the CloudBridge Connector tunnel		• 10.20.20.0/24
Settings on NetScaler appliance NS_Appliance-1 in Datacenter-1		
	SNIP1(for reference purposes only)	• 198.51.100.100
IPSec profile	NS_Fortinet_IPSec_Profile	• IKE version: v1 • Encryption algorithm: AES • Hash algorithm: HMAC_SHA1 • psk = examplepresharedkey (Note: This is an example of a pre-share key, for illustration. Citrix does not recommend to use this string in your CloudBridge Connector configuration)
CloudBridge Connector tunnel	NS_Fortinet_Tunnel	• Remote IP = 203.0.113.200 • Local IP= 198.51.100.100 • Tunnel protocol = IPSEC • IPSec profile= NS_Fortinet_IPSec_Profile
Policy based route	NS_Fortinet_Pbr	• Source IP range = Subnet in the Datacenter-1=10.102.147.0-10.102.147.255 • Destination IP range =Subnet in Datacenter-2=10.20.20.0-10.20.20.255 • IP Tunnel = NS_Fortinet_Tunnel
Settings on Fortinet FortiGate-Appliance-1 in Datacenter-2		
Phase 1 Configuration	P1-NETSCALER-TUNNEL	• Remote Gateway: Static IP Address • IP Address: 198.51.100.100 • Local Interface: port1 • Mode: Main (ID Protection) • Authentication Method: Preshared Key • Pre-Shared Key: examplepresharedkey • Enable IPSec Interface Mode: Disabled • IKE Version: 1 • P1 Proposal

		• 1- Encrytion: AES • Authentication: HMAC_SHA1 • DH Group: 2 • XAUTH: Disabled • Dead Peer Detection: Enabled
Phase 2 Configuration	P2-NETSCALER-TUNNEL	• Phase 1: P1-NETSCALER-FORTIGATE • P2 Proposal • 1- Encrytion: AES • Authentication: HMAC_SHA1 • Enable replay detection: Enabled • Enable perfect forward secrecy (PFS): Enabled • DH Group: 2 • Auto Key Keep Alive: Enabled • Auto-Negotiate: Enabled • Quick Selector Mode • Source address: FORTINET-SIDE-SUBNET • Source port: 0 • Destination address: NETSCALER-SIDE-SUBNET • Destination port: 0 • Protocol: 0
Policy Addresses		• FORTINET-SIDE-SUBNET • Subnet / IP Range: 10.20.20.0/255.255.255.0 • Interface: port2 • NETSCALER-SIDE-SUBNET • Subnet / IP Range: 10.102.147.0/255.255.255.0 • Interface: port1
IPSec Security Policy		• Policy Type: VPN • Policy Subtype: IPsec • Local Interface: port2 • Local Protected Subnet: FORTINET-SIDE-SUBNET • Outgoing VPN Interface: port1 • Remote Protected Subnet: NETSCALER-SIDE-SUBNET • VPN Tunnel • Use Existing: Enabled • VPN Tunnel: P1-NETSCALER-FORTIGATE • Allow traffic to be initiated from the remote side: Enabled