Microsoft

IPSec over ExpressRoute for GSTN Connectivity

Note on configuring IPSec on ExpressRoute / MPLS connection to GSTN DCs

Prepared for

GSP Technical Decision Makers and Networking team
Thursday, 31 August 2017
Version 1.0

Prepared by

Microsoft GSP / ASP team

Contributors:
Lakshmi Krishnamurthy, Mandar Samant

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
16 Aug 2017	Lakshmi Krishnamurthy	1	

Reviewers

Name	Version approved	Position	Date

Table of Contents

Table of Figures.

1 Introduction

GSTN requires all the GSPs (GST Suvidha Providers) to connect to GSTN's APIs over a private network connected via MPLS. As MPLS is inherently un-encrypted there is an additional requirement of configuring an IPSec VPN (Virtual Private Network) to encrypt the traffic between GSP datacenter and GSTN's datacenter.

This short note provides high level guidance, list of resources and vendor contact information to get the above task achieved and is meant for consumption of *GSP's Technical Team* only.

2 IPSec over ExpressRoute:

To get started, the following diagram represents a setup with a DMZ between Azure and on-premises networks. In our context, GSTN's DC represents the on-premises DC and Azure DC represents the GSP solution hosted on Azure.

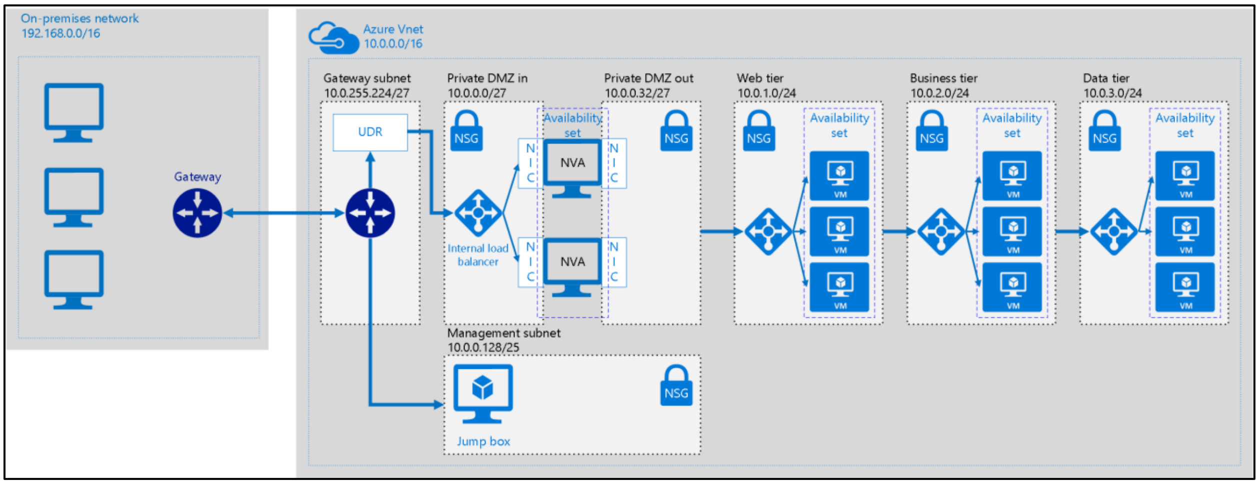


Figure 1 DMZ between On-Premises DC and Azure

More details on the setup are available at the link below.
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-hybrid

On the Azure DC side a NVAs (Network Virtual Appliances), provided by vendors such Cisco/ Barracuda/ CheckPoint etc, combined with UDR (User Defined Routing, explained here https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview) achieve our goal of routing traffic between On Premise DC and Azure DC.

In case of GSP – GSTN connectivity the connection happens over MPLS/ ExpressRoute (ER). Though this establishes a private connection it doesn't offer encryption of traffic by default.

There are two ways to achieve traffic encryption over ExpressRoute:

a> An Azure customer or an ER provider can encrypt traffic over the connection by defining IPSec tunnel-mode policies for all traffic flowing between the on premises, in this case GSTN's, resources and Azure resources.

b> The second option would be to use a firewall / appliance at each end point of the ExpressRoute circuit and configure routing to route the traffic using a IPSec VPN. This will require the GSP to setup an 3rd party firewall VMs/Appliances on the GSP Azure subnet to be installed on both ends to encrypt the traffic over the ExpressRoute circuit.

The figure below illustrates the general network setup for option (a) .

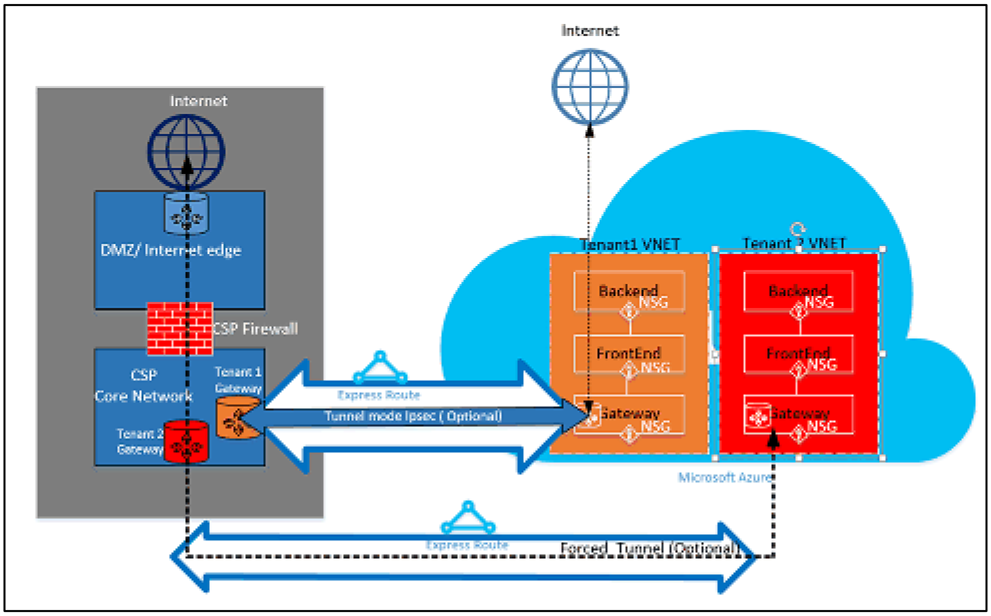


Figure 2 IPSec over ExpressRoute

More information on this setup is available at this link:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-for-cloud-solution-providers

The second option, option (b) above, is to employ (network virtual appliances) NVAs on the Azure DC side and route the traffic to GSTNs DC via an IPSec tunnel formed by the NVA with the network device on the GSTN side.

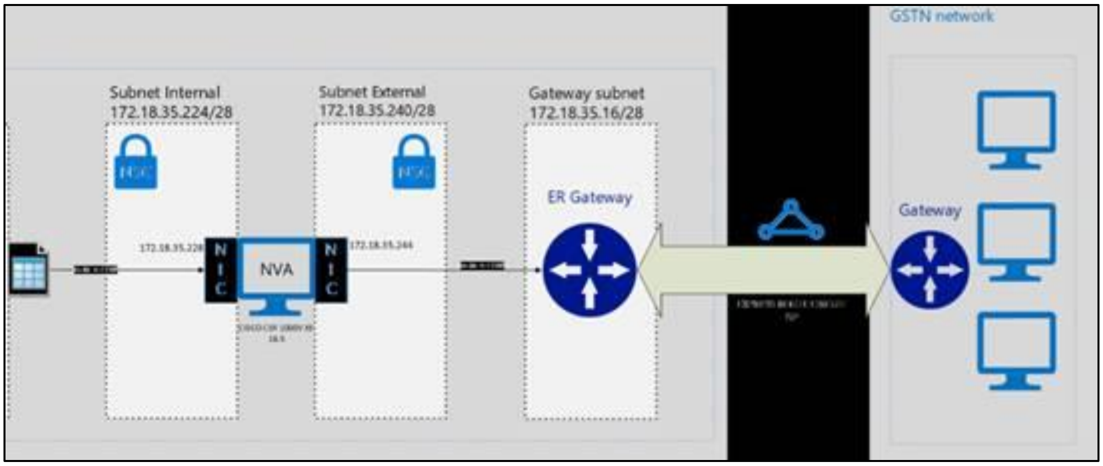


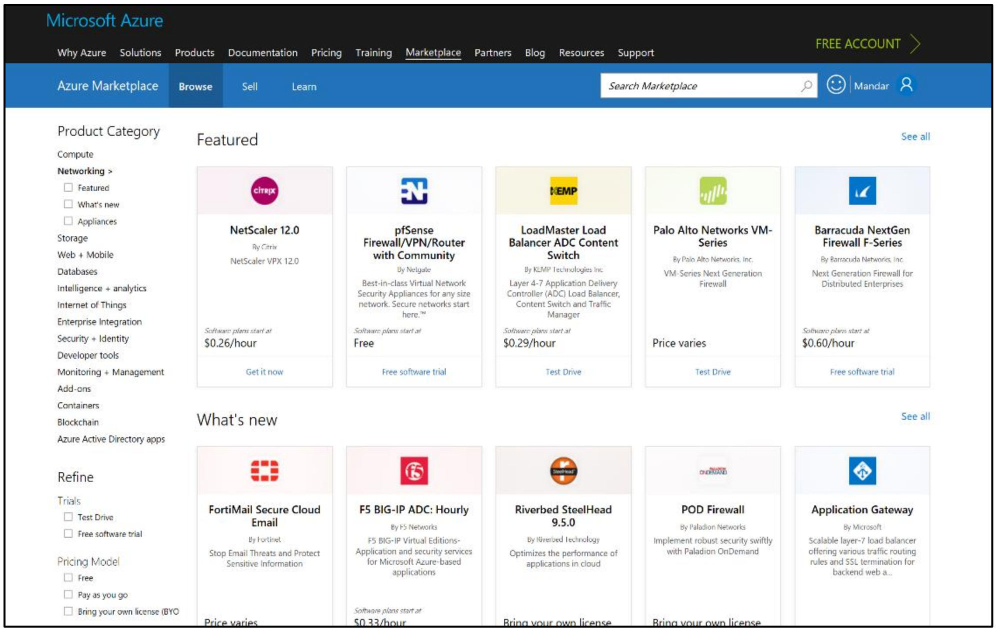
Figure 3 Using NVA and UDR to encrypt ER traffic [the IP addresses shown are for illustration only]

3 Working with NVA

Once the ER route is setup between the GSP DC and Azure DC network, one can start setting up the IPSec tunnel.

The NVAs and their pricing are available on the Azure Marketplace and one can provision and configure them as any other resource.

You can find the pricing and plan for these virtual appliances on Azure at:
https://azuremarketplace.microsoft.com/en-us/marketplace/apps/category/networking?page=1



Featured

NetScaler 12.0
By Citrix
NetScaler VPX 12.0
Software plans start at
$0.26/hour
Get it now

pfSense Firewall/VPN/Router with Community
By Netgate
Best-in-class Virtual Network Security Appliances for any size network. Secure networks start here.™
Software plans start at
Free
Free software trial

LoadMaster Load Balancer ADC Content Switch
By KEMP Technologies Inc
Layer 4-7 Application Delivery Controller (ADC) Load Balancer, Content Switch and Traffic Manager
Software plans start at
$0.29/hour
Test Drive

Palo Alto Networks VM-Series
By Palo Alto Networks, Inc.
VM-Series Next Generation Firewall
Price varies
Test Drive

Barracuda NextGen Firewall F-Series
By Barracuda Networks, Inc.
Next Generation Firewall for Distributed Enterprises
Software plans start at
$0.60/hour
Free software trial

What's new

FortiMail Secure Cloud Email
By Fortinet
Stop Email Threats and Protect Sensitive Information
Price varies

F5 BIG-IP ADC: Hourly
By F5 Networks
F5 BIG-IP Virtual Editions-Application and security services for Microsoft Azure-based applications
Software plans start at
$0.33/hour

Riverbed SteelHead 9.5.0
By Riverbed Technology
Optimizes the performance of applications in cloud
Bring your own license

POD Firewall
By Paladion Networks
Implement robust security swiftly with Paladion OnDemand
Bring your own license

Application Gateway
By Microsoft
Scalable layer-7 load balancer offering various traffic routing rules and SSL termination for backend web a...

Figure 4 NVAs on Azure Marketplace

It is always advisable to seek assistance from the ExpresRoute Provider and NVA vendor to plan, deploy, configure, secure and test the solution.

The planning process will need to include:

a> Current GSP solution network topology and addressing scheme

b> Inputs from GSTN to setup the IPSec VPN including DNS settings, alternate DC connections etc.

c> NVA specific configurations

For those who chose to go with the NVA based options the sections below mention some of the popular NVA vendors and links to their product literature and contact information as of date. Note that the list is not exhaustive, and details may change with time.

We have few GSPs up and running on Azure with ER and IPSec configured using some of the appliances mentioned below however we do expect all GSPs to do due diligence before selecting a NVA.

Contact information provided below is for convenience only and as per our best information and may change.

3.1.1 Barracuda

Appliance

Link to documentation:

https://assets.barracuda.com/assets/docs/dms/Barracuda_NextGen_Firewall_F_SB_Deploying_Multi-Tier_Architectures_Azure_US.pdf

Barracuda Contacts:
Gerald Tang gtang@barracuda.com
Director, Public Cloud (APJ)
Barracuda Networks Inc.
M: +65 9816 3887

Shashwat Uniyal suniyal@barracuda.com

3.1.2 Cisco

Appliance:

Cisco CSR 1000v.
Link to documentation:
https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/azu/b_csr1000config-azure.html

Licensing of the NVA Works on Bring Your Own License (BYOL) concept. The customer would need to buy the license from Cisco (typically via a Cisco Partner). The customer can spin up the CSR1000v from Azure Market Place and apply the license.

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-csr-basic-template

The BYOL allows the customer to get support from Cisco TAC for any troubleshooting or ongoing support.

Cisco Contacts:
SREEJESH T P (sretp) sretp@cisco.com
+91 96632 46767
Annamalai Ramanathan anramana@cisco.com
Sudhanshu Manglic smanglic@cisco.com

Cisco Partner – Velocis contact:
Mohd Shadab mohd.shadab@velocis.in
+91- 99111 20419

3.1.3 Check Point

Appliance Setup:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110993

3.1.4 F5:

Appliance Setup:
https://devcentral.f5.com/articles/securing-express-route-with-the-big-ip-26671

<End of Document>