A10 Thunder CFW IPsec VPN Interoperability with Azure VPN Gateways

Table of Contents

Disclaimer

Overview

Organizations typically transfer sensitive data between remote sites, data centers, and public and private clouds. To protect the transfer of sensitive data, a site-to-site VPN solution should be implemented.

IPsec is a mature, cost-effective site-to-site VPN solution to secure communication from snooping and data theft, and to address compliance issues. With the advent of mobility, cloud and IoT, enterprises and service providers are rethinking their VPN strategies to support unprecedented IPsec throughput levels and leverage Border Gateway Protocol (BGP) routing for high availability and rapid scaling.

A10 Networks Thunder® CFW supports BGP routing protocol, which not only allows routers to communicate across IPsec VPN tunnels, but also enables organizations to demonstrate business agility by allowing rapid IPsec network deployments.

This guide provides step-by-step instructions and configuration procedures for A10 Thunder CFW's IPsec VPN connection with BGP on Microsoft Azure VPN Gateways using Azure Resource Manager and PowerShell.

Deployment Prerequisites

In this guide, the following components are used to deploy the IPsec VPN solution between an A10 Thunder CFW and Microsoft Azure VNet gateway:

- A10 Thunder Convergent Firewall (CFW) hardware appliance
- A10 Networks Advanced Core Operating System (ACOS®) 4.1.0-P5 or higher
- A10 IPsec AppCentric Templates
- Client/server machines at each site
- Internet access through a (gateway) router
- An Azure subscription and Azure Resource Manager PowerShell cmdlets

Network Topology

For this deployment guide, the Thunder CFW device is deployed in route-based L3 mode. Interfaces on Thunder CFW are connected as follows:

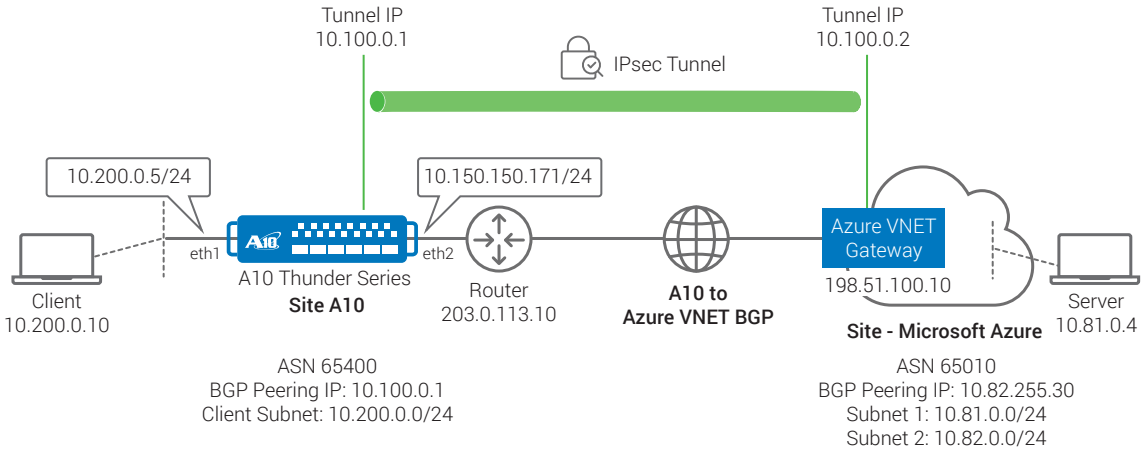

Figure 1: IPsec VPN Tunnel – A10 Thunder CFW to Microsoft Azure

***Note**: The router at the A10 site is configured with Source NAT (to translate IP addresses between 203.0.113.10 and 10.150.150.171). If your Thunder CFW has an interface with a public IP address, the deployment can be further simplified.*

***Note**: The tunnel endpoint IP, 10.100.0.2 is referred as tunnel remote IP address on Thunder CFW. You do not need to configure it on the Azure gateway.*

Accessing A10 Thunder CFW

Thunder CFW can be accessed either from a Command Line Interface (CLI) or through AppCentric Templates (ACT):

- Command Line Interface (CLI)

  Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or the network using either of the following protocols:

  a. Secure protocol – Secure Shell (SSH) version 2

  b. Unsecure protocol – Telnet (if enabled; not recommended)

- AppCentric Templates (ACT)

  A10 ACOS GUI plug-in module that enhances the user experience to deploy, monitor and troubleshoot applications in a frictionless manner. Obtain the latest ACT file and import it into ACOS. Refer to Appendix B for details on how to acquire and import the file.

***Note**: HTTP requests are redirected to HTTPS by default on the Thunder CFW device.*

Default username: admin

Default password: a10

Default IP address of the device: 172.31.31.31 (Management IP address of the A10 device)

***Note**: Thunder CFW can also be configured using the standard GUI that can be accessed by entering the management IP address in a Web browser's address bar (e.g., https://172.31.31.31) and using the default access credentials mentioned above.*

***Note**: The AppCentric Templates can be accessed by opening the GUI (by entering the Management IP in the browser's address bar e.g. https://172.31.31.31/) and navigating to **System > App Template**.*

Thunder CFW IPsec VPN Configuration using AppCentric Templates

AppCentric Templates Overview

A10 Networks AppCentric Templates are easy-to-use configuration tools for features like SSL Insight and IPsec VPN, and ADC deployment for popular applications such as Microsoft Exchange. The AppCentric Templates offer guided topology configuration, easy and quick IPsec-related configurations, as well as a widget-based dashboard. This tool is available in ACOS 4.1.0-P5 release, and is accessible via the GUI through **System > App Template**.

Once you logged in to the ACT, select IPsec from AppCentric Templates menu. There are three main sections in the IPsec AppCentric Templates:

1. Wizard

   The wizard provides users with a flow-based configuration of the CFW device.

2. Dashboard

   The dashboard gives users a view of different statistics related to the current state of the system, including IPsec traffic statistics.

3. Configuration

   This section provides users with the current configuration of the device as well as access to some advanced options.

***Note**: If IPsec ACT is not available from the navigation bar, you must install the latest ACT file. Refer to Appendix B for details.*

Wizard – Topology

Basic configuration of the A10 Thunder CFW device will be done in the Wizard section of the AppCentric Templates for IPsec. The first step in the Wizard section is Topology. In this step, you will choose the deployment topology to use for creating IPsec a connection between the A10 device and third-party device (in this case, Azure VNet Gateway).

1. Navigate to **Wizard > Topology** and choose the topology you will be working with. In this example, select "A10-3RD PARTY IPsec VPN Topology". Click **NEXT**.

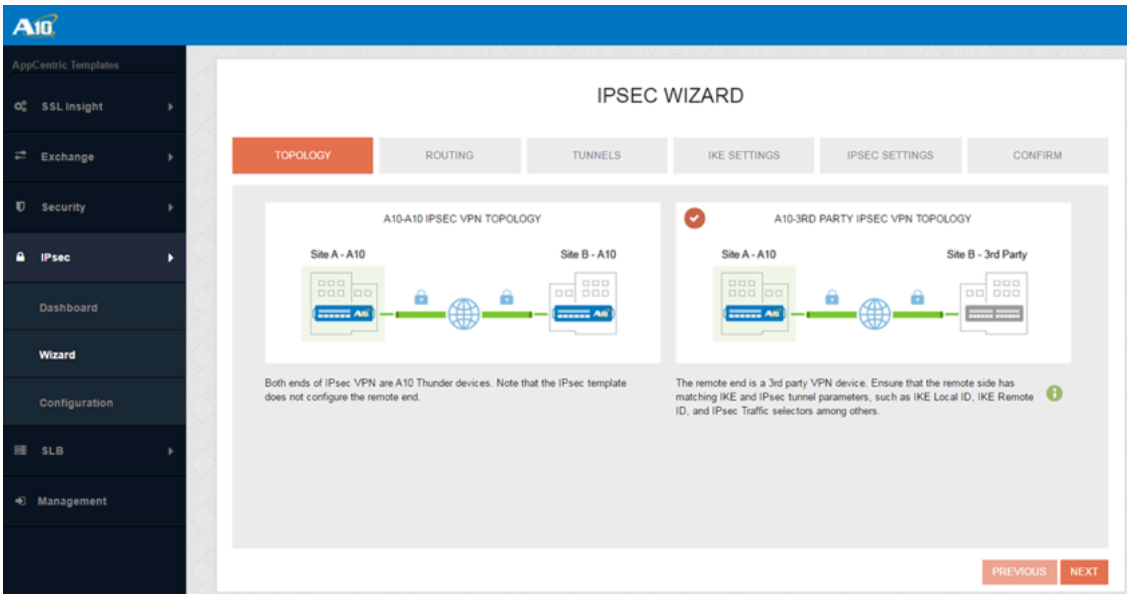

Figure 2: Wizard – Topology Selection

Wizard – Routing: Interface Settings

The Routing step is further divided into two parts: Configuration of interfaces with corresponding IP addresses and Layer 3 routing configuration of the CFW device.

2. **Internal Interface Settings:** This interface is internal, facing the client subnet (SiteA-A10, as shown in Figure 3. Choose an interface (e.g., Ethernet 1) from the drop-down menu and assign an IP (10.200.0.5/24).
3. **External Interface Settings:** This interface is external, facing the gateway router/Internet. Choose an interface (e.g., Ethernet 2) and assign an IP (10.150.150.171/24). Click **NEXT**.

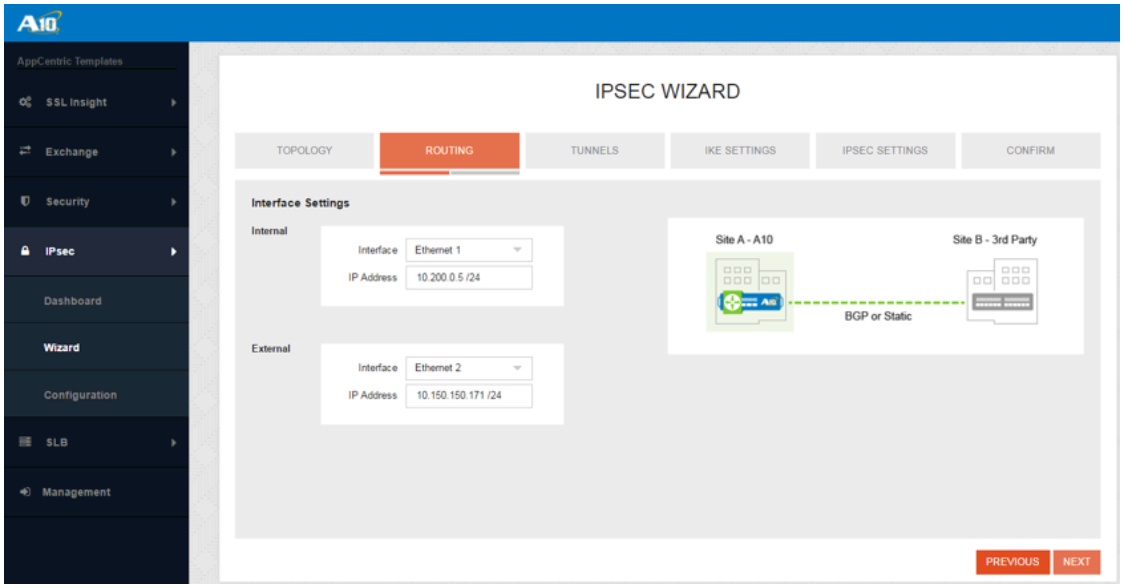

Figure 3: Wizard – Routing: Interface Settings

Wizard – Routing: BGP Settings

4. Configure the default gateway and dynamic BGP parameters:
   a. Default Gateway interface facing A10 Thunder CFW (e.g., 10.150.150.1)
   b. AS number 65400
   c. Local Subnets (in our example, all clients on the A10 site are connected on the subnet 10.200.0.0/24)
   d. Click **NEXT**

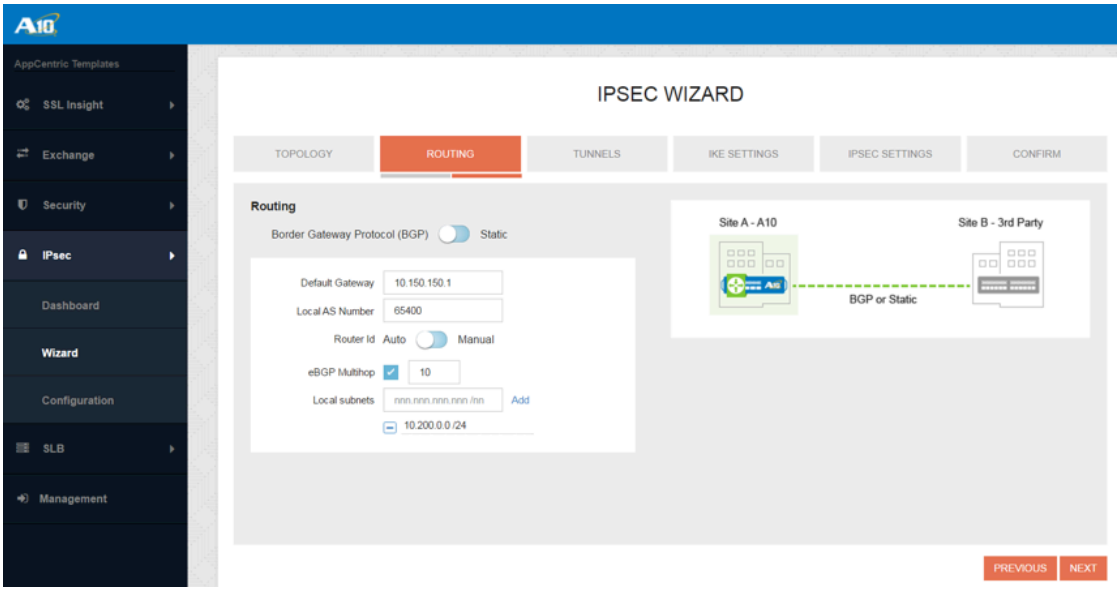

Figure 4: Wizard – Routing: BGP Settings

Wizard – Tunnels

IPsec involves many component technologies and encryption methods. This step involves configuring IKE (Internet Key Exchange) and IPsec tunnel parameters, such as IKE Local ID, IKE Remote ID and IPsec traffic selectors. IKE works in two steps, generally called IKE phases 1 and 2:

IKE phase 1: IKE authenticates IPsec peers and negotiates IKE Security Association (IPsec SAs) during this phase, setting up a secure channel for negotiating IPsec SAs in phase 2.

IKE phase 2: IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers.

5. In this section, IP addresses used in IKE phase 1 and IKE phase 2 are configured as shown in Figure 5:
   - IKE IPs
     a. Local IP – 10.150.150.171/24
     b. Remote IP – 198.51.100.10
   - Tunnel IPs
     a. Local IP – 10.100.0.1/24
     b. Remote IP – 10.100.0.2
   - Routing Information
     a. BGP Peer IP – 10.82.255.30
     b. BGP Remote AS – 65010

***Note**: The remote tunnel IP only needs to be specified on the A10 device. It doesn't need to be configured on the Azure gateway. Also, you can confirm the BGP peer IP and remote AS number by using PowerShell command on Azure. For more details, refer to [Obtain the Azure BGP Peer IP address](#).*

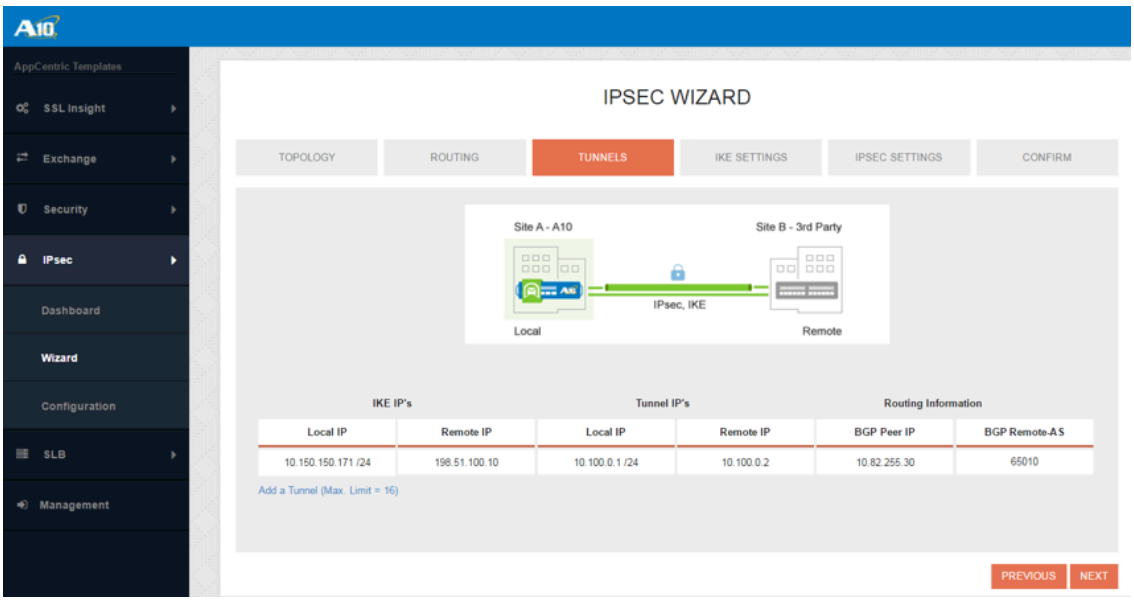

Figure 5: Wizard – Tunnels

Wizard – IKE Settings

6. The next step is to configure the IKE channel properties. This is done in two sub-sections, as shown in Figure 6:
   - **Authentication** Settings
     a. Pre-Share Key (e.g., a10)

- Encryption Settings
  a. Encryption – aes-256
  b. Hash – sha256
  c. DH Group – 2

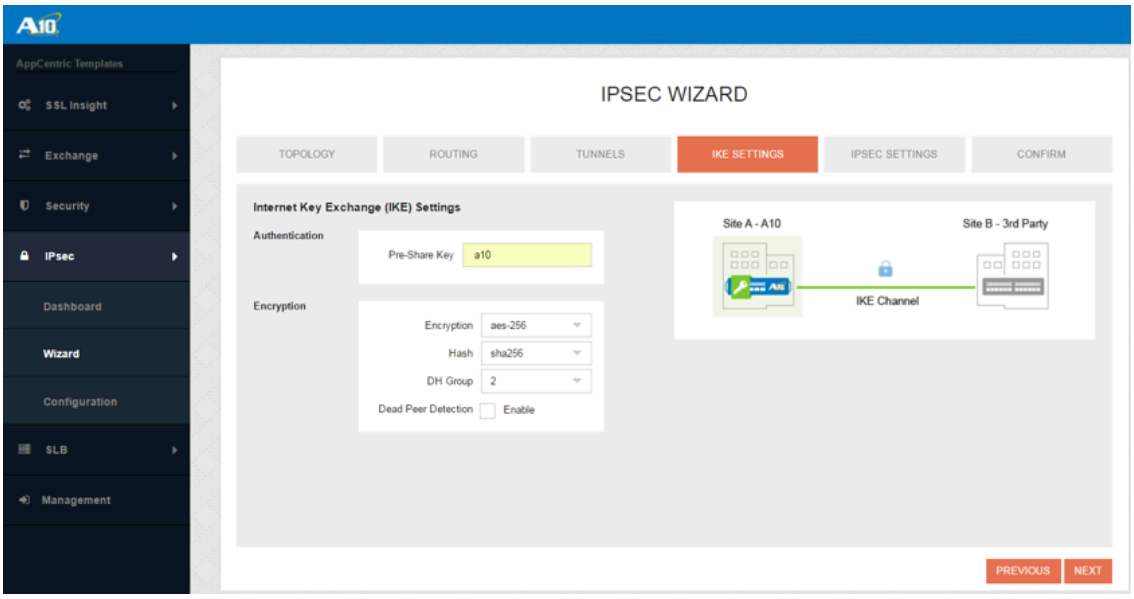

Figure 6: Wizard – IKE Settings

Wizard – IPsec Settings

7. In this step, IPsec-specific settings for the IPsec Tunnel are configured, as shown in the Figure 7. Configure the encryption, hash and DH group settings to match the parameters chosen in IKE settings in Figure 6.

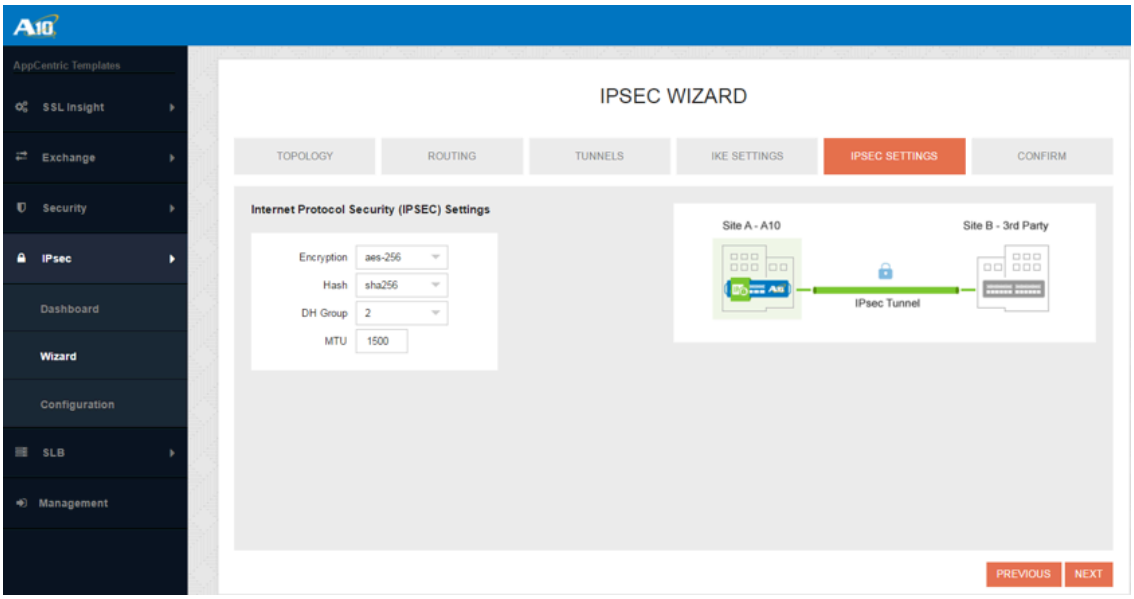

Figure 7: Wizard – IPsec Settings

Wizard – Confirm

The final step in the IPsec Wizard-based configuration is the Confirm tab. Here, you can review a summary of the IPsec configuration prepared so far. You can edit the configuration by clicking **PREVIOUS** or selecting the appropriate tab.

Once the configurations are confirmed, click **FINISH** to finalize the IPsec Tunnel topology configuration. This action opens a pop-up window showing the actual CLI-based configuration.

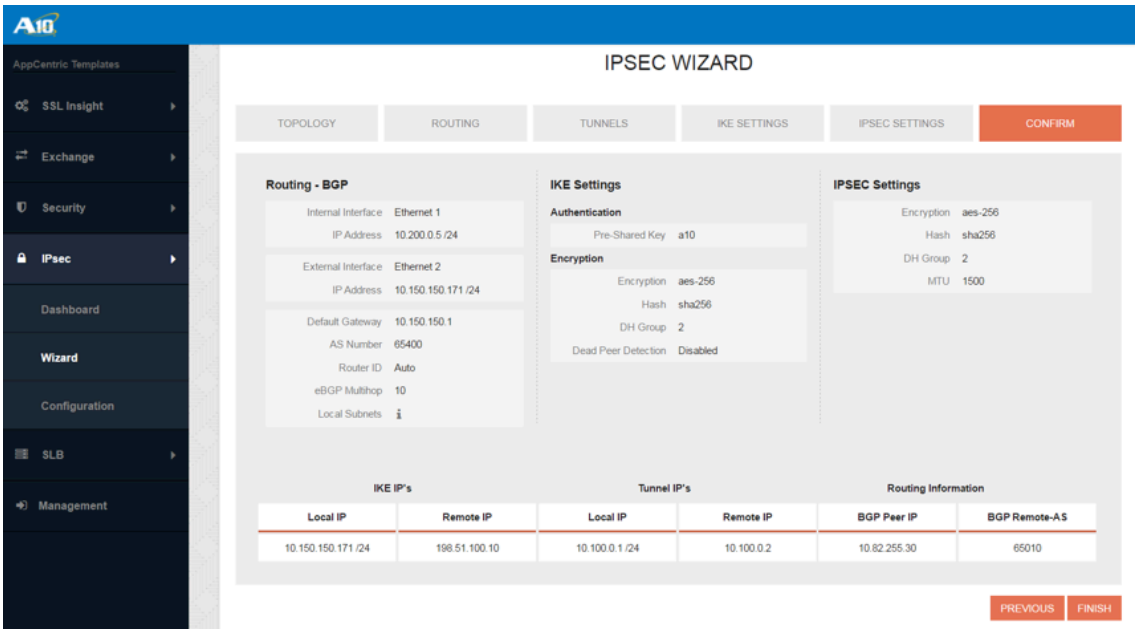

Figure 8: Wizard – Confirmation

You can either click **APPLY** to activate the setting on the Thunder CFW device, or you can click **COPY** to configure the CFW manually through the CLI.

To view the complete configuration in text format, refer to Appendix A.

Thunder CFW IPsec Configuration Using CLI

The IPsec VPN can also be configured directly on the Thunder CFW through the device CLI.

Interface and VLAN Configuration

Configure the internal and external interfaces on the Thunder CFW.

The internal interface is facing the client subnet on the Thunder CFW (Site-A10), and external interface is facing the Internet on the Thunder CFW (Site-A10).

A VLAN (e.g., 851) is created for the physical port on eth 1 and all untagged traffic on eth 1 is included in this VLAN. A virtual interface will also be created and assigned an IP address. (10.200.0.5/24).

Similarly, a VLAN (e.g., 852) is created for the physical port on eth 2 and all untagged traffic on eth 2 is included in this VLAN. A virtual interface will also be created and assigned an IP address. (10.150.150.171/24)

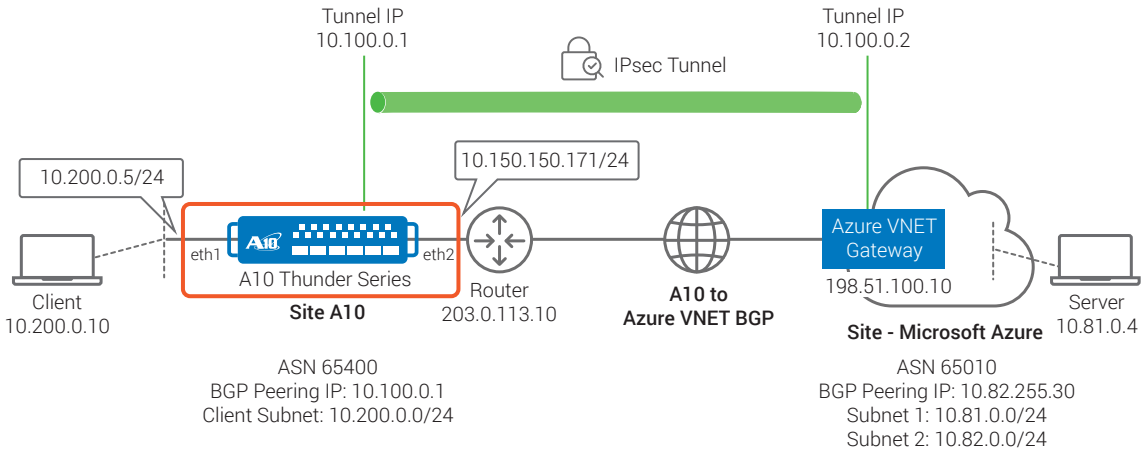

Figure 9: Thunder CFW Configuration

```
vlan 851
 untagged ethernet 1
 router-interface ve 851
!
vlan 852
 untagged ethernet 2
 router-interface ve 852
!
interface ve 851
 ip address 10.200.0.5 /24
!
interface ve 852
 ip address 10.150.150.171 /24
!
```

Default Route Configuration

The next step is to configure a default route facing the Internet with the IP address 10.150.150.1

```
ip route 0.0.0.0 /0 10.150.150.1
```

IKE Configuration

IPsec involves many component technologies and encryption methods. This step involves configuring matching IKE and IPsec tunnel parameters, such as IKE Local ID, IKE Remote ID and IPsec traffic selectors. IKE works in two steps, generally called IKE phases 1 and 2:

IKE Phase 1: IKE authenticates IPsec peers and negotiates IKE Security Association (IPsec SAs) during this phase, setting up a secure channel for negotiating IPsec SAs in phase 2.

IKE Phase 2: IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers.

The following are the commands to configure IKE Phase 1:

```
vpn ike-gateway AzureTestVPN4
  auth-method preshare-key <<Password>>
  encryption aes-256 hash sha256
  dh-group 2
  local-address ip 10.150.150.171
  remote-address ip 198.51.100.10
!
vpn ipsec AzureTestVPN
  ike-gateway AzureTestVPN4
  dh-group 2
  encryption aes-256 hash sha256
  bind tunnel 1 10.100.0.2
```

IPsec Tunnel Configuration

Once the secure IKE channel is established in the IKE Phase 1, the next step is to configure the IPsec Tunnel. The following steps configure both the tunnel end points.

```
interface tunnel 1
  enable
  ip address 10.100.0.1 255.255.255.0
  mtu 1500
```

Also, note that all the traffic intended for the BGP peer on the Azure VNet Gateway is routed to the IPsec tunnel.

```
ip route 10.82.255.30 /32 tunnel 1 10.100.0.2
```

BGP Configuration

The final step is to configure the BGP peer parameters, as follows:

```
router bgp 65400
 maximum-paths 16
 network 10.200.0.0 mask 255.255.255.0
 neighbor 10.82.255.30 remote-as 65010
 neighbor 10.82.255.30 ebgp-multihop 10
!
```

Azure VPN Gateway IPsec VPN Configuration

This section explains the steps to enable BGP on a cross-premises site-to-site (S2S) VPN connection using the Resource Manager deployment model and PowerShell.

The following configuration details can be found in detail at https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-bgp-resource-manager-ps/. Refer to the link for further details.

Configure IPsec VPN and BGP on the Azure VPN Gateway

The following configuration steps set up BGP parameters on the Azure VPN Gateway on the remote enterprise site.

Create and Configure Virtual Network (VNet1)

Declare your variables

The first step in this process is declaring the variables. Modify the variables if necessary, and then copy and paste into your PowerShell console.

```
$Sub1          = "Replace_With_Your_Subcription_Name"
$RG1           = "TestBGPRG1"
$Location1     = "West US"
$VNetName1     = "TestVNet1"
$FESubName1    = "Frontend"
$BESubName1    = "Backend"
$GWSubName1    = "GatewaySubnet"
$VNetPrefix11  = "10.81.0.0/16"
$VNetPrefix12  = "10.82.0.0/16"
$FESubPrefix1  = "10.81.0.0/24"
$BESubPrefix1  = "10.82.0.0/24"
$GWSubPrefix1  = "10.82.255.0/27"
$VNet1ASN      = 65010
$DNS1          = "8.8.8.8"
$GWName1       = "VNet1GW"
$GWIPName1     = "VNet1GWIP"
$GWIPconfName1 = "gwipconf1"
$Connection15  = "VNet1toA10"
```

Connect to your subscription and create a new resource group

Open the PowerShell console and connect to your account using the following commands.

```
Login-AzureRmAccount
Select-AzureRmSubscription -SubscriptionName $Sub1
New-AzureRmResourceGroup -Name $RG1 -Location $Location1
```

Create TestVNet1

The following commands create a virtual network named TestVNet1 and three subnets, namely *GatewaySubnet*, Frontend and Backend. When substituting values, it's important that you always name your gateway subnet specifically *GatewaySubnet*.

```
$fesub1 = New-AzureRmVirtualNetworkSubnetConfig -Name $FESubName1 -AddressPrefix
$FESubPrefix1
$besub1 = New-AzureRmVirtualNetworkSubnetConfig -Name $BESubName1 -AddressPrefix
$BESubPrefix1
$gwsub1 = New-AzureRmVirtualNetworkSubnetConfig -Name $GWSubName1 -AddressPrefix
$GWSubPrefix1

New-AzureRmVirtualNetwork -Name $VNetName1 -ResourceGroupName $RG1
-Location $Location1 -AddressPrefix $VNetPrefix11,$VNetPrefix12 -Subnet
$fesub1,$besub1,$gwsub1
```

Create the VPN Gateway for TestVNet1 with BGP Parameters

Create the IP and subnet configurations

Request a public IP address to be allocated to the gateway you will create for your VNet. You'll also define the subnet and IP configurations required.

```
$gwpip1    = New-AzureRmPublicIpAddress -Name $GWIPName1 -ResourceGroupName
$RG1 -Location $Location1 -AllocationMethod Dynamic

$vnet1     = Get-AzureRmVirtualNetwork -Name $VNetName1 -ResourceGroupName
$RG1

$subnet1   = Get-AzureRmVirtualNetworkSubnetConfig -Name "GatewaySubnet"
-VirtualNetwork $vnet1

$gwipconf1 = New-AzureRmVirtualNetworkGatewayIpConfig -Name $GWIPconfName1
-Subnet $subnet1 -PublicIpAddress $gwpip1
```

Create the VPN gateway with the AS number

Create the virtual network gateway for TestVNet1. Note that BGP requires a route-based VPN gateway, and also the addition parameter, -Asn, to set the ASN (AS Number) for TestVNet1. Creating a gateway may take up to 30 minutes or more to complete.

```
New-AzureRmVirtualNetworkGateway -Name $GWName1 -ResourceGroupName $RG1
-Location $Location1 -IpConfigurations $gwipconf1 -GatewayType Vpn -VpnType
RouteBased -GatewaySku HighPerformance -Asn $VNet1ASN
```

Obtain the Azure BGP Peer IP address

Once the gateway is created, you will need to obtain the BGP Peer IP address on the Azure VPN Gateway. This address is needed to configure the Azure VPN Gateway as a BGP Peer for A10 Thunder CFW device.

```
$vnet1gw = Get-AzureRmVirtualNetworkGateway -Name $GWName1 -ResourceGroupName
$RG1

$vnet1gw.BgpSettingsText
```

The Azure VPN gateway will allocate a single IP address from the GatewaySubnet range defined for the virtual network. By default, it is the second-to-last address of the range. For example, if your GatewaySubnet is 10.82.255.0/27, ranging from 10.82.255.0 to 10.82.255.31, then the BGP Peer IP address on the Azure VPN gateway will be 10.82.255.30.

Establish a Cross-Premises Connection with BGP

To establish a cross-premises connection, you need to create a Local Network Gateway to represent your on-premises A10 Thunder CFW device, and a Connection to connect the Azure VPN gateway with the local network gateway.

Create and Configure the Local Network Gateway

Declare your variables

```
$RG5           = "TestBGPA10"
$Location5     = "West US"
$LNGName5      = "A10"
$LNGPrefix50   = "10.100.0.1/32"
$LNGIP5        = "203.0.113.10"
$LNGASN5       = 65400
$BGPPeerIP5    = "10.100.0.1"
```

In the above variables, the A10's BGP ASN is 65400 and Peering IP Address is 10.100.0.1. The minimum prefix you need to declare for the local network gateway is the host address of your BGP Peer IP address on your VPN device. In this case, it's a /32 prefix of "10.100.0.1/32". The Local Network gateway IP is configured to the external IP (203.0.113.10) configured by the router facing the Internet, as specified in our deployment. If your Thunder CFW has an interface with a public IP address, then use this IP to configure this variable instead. The local network gateway can be in the same or different location and resource group as the VPN gateway. This example shows them in different resource group and same location.

Create the local network gateway for A10

```
New-AzureRmResourceGroup -Name $RG5 -Location $Location5
```

```
New-AzureRmLocalNetworkGateway -Name $LNGName5 -ResourceGroupName $RG5
-Location $Location5 -GatewayIpAddress $LNGIP5 -AddressPrefix $LNGPrefix50 -Asn
$LNGASN5 -BgpPeeringAddress $BGPPeerIP5
```

Connect the VNet Gateway and Local Network Gateway

Get the two gateways

```
$vnet1gw = Get-AzureRmVirtualNetworkGateway -Name $GWName1 -ResourceGroupName
$RG1
```

```
$lng5gw = Get-AzureRmLocalNetworkGateway -Name $LNGName5 -ResourceGroupName
$RG5
```

```
Create the TestVNet1 to A10 connection
```

```
New-AzureRmVirtualNetworkGatewayConnection -Name $Connection15
-ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw -LocalNetworkGateway2
$lng5gw -Location $Location1 -ConnectionType IPsec -SharedKey '<<password>>'
-EnableBGP $True
```

Viewing VPN/BGP Status on A10:

Once the configurations are done, use the following commands to check the VPN and BGP status on Thunder CFW:

```
TH3230S#show vpn ike-sa
Name            Local/Peer IP    Enc/Hash  Lifetime  Status       Auth-method
-------------------------------------------------------------------------------
AzureTestVPN  10.150.150.171  aes-256     84287s  Established  preshare-key
              xx.xx.xx.xx     sha1
-------------------------------------------------------------------------------
Total: 1

TH3230S#show vpn ipsec-sa
Gateway:AzureTestVPN4    Local IP:10.150.150.171    Remote IP:198.51.100.10
Name           Selectors  In/Out SPI  Mode/xform    Time/Bytes
-----------------------------------------------------------
AzureTestVPN  0.0.0.0/0  0x4e90c7cc  esp-tunnel     26618s
              0.0.0.0/0  0xb718f746  aes-256-sha1   unlimited

TH3230S#show ip bgp sum
BGP router identifier 10.100.0.1, local AS number 65400
```

```
BGP table version is 41
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down    State/PfxRcd
10.82.255.30 4    65010      95       94       41   0    0 00:39:21 7

Total number of neighbors 1
```

Troubleshooting

Once the configuration of the IPsec VPN tunnel is complete and the status of BGP and IPsec are verified, some problems (listed below) may arise. If issues are discovered, follow the steps mentioned to troubleshoot the configuration.

1. VPN tunnel is not coming up on A10:
   - Confirm PSK on both A10 and Azure VPN Connection
   - VPN tunnel on the A10 will only come UP if traffic is passed or manually forced up.
     To manually force tunnel UP, use the following commands

     ```
     TH3230S#configure
     TH3230S(config)#vpn ipsec AzureTestVPN
     TH3230S(config-ipsec:AzureTestVPN)#up
     ```

2. VPN Connection on Azure is in 'Not Connected' State:
   - If the configuration is new or changed, this may take up to 5 minutes to reach a connected state
   - lear ike-gateway on A10 to re-establish
     - TH3230S#clear vpn ike-sa AzureTestVPN
   - Clear BGP neighbor to re-establish
     - TH3230S#clear bgp 10.82.255.30
3. BGP not connecting on A10:
   - Confirm variable BGPPeerIP5 is configured in Establish a Cross-Premises Connection with BGP section
   - Confirm ebgp-multihop is configured under router bgp
4. Traffic is not passing with internal clients behind A10:
   - On clients, add route back to A10 for Azure's client subnets

Summary

Organizations require a trusted solution to deliver reliable site-to-site IPsec VPN connectivity, but also can interoperate with their existing routers and IPsec VPN gateways. The A10 Thunder CFW IPsec VPN capability enables organizations to encrypt traffic at high speed and support BGP routing and on-demand VPN provisioning.

Appendix A - Thunder CFW CLI Configuration

```
active-partition shared
!
vlan 851
 untagged ethernet 1
 router-inter ve 851
!
vlan 852
 untagged ethernet 2
 router-inter ve 852
!
interface ve 851
 ip address 10.200.0.5 /24
!
interface ve 852
 ip address 10.150.150.171 /24
!
ip route 0.0.0.0 /0 10.150.150.1
!
vpn ike-gateway AzureTestVPN4
  auth-method preshare-key <<Password>>
  encryption aes-256 hash sha256
  dh-group 2
  local-address ip 10.150.150.171
  remote-address ip 198.51.100.10
!
interface tunnel 1
  enable
  ip address 10.100.0.1 255.255.255.0
  mtu 1500
!
vpn ipsec AzureTestVPN
  ike-gateway AzureTestVPN4
  dh-group 2
  encryption aes-256 hash sha256
  bind tunnel 1 10.100.0.2
!
ip route 10.82.255.30 /32 tunnel 1 10.100.0.2
!
router bgp 65400
maximum-paths 16
network 10.200.0.0 mask 255.255.255.0
neighbor 10.82.255.30 remote-as 65010
neighbor 10.82.255.30 ebgp-multihop 10
!
```

Appendix B – AppCentric Templates Upgrade

ACOS release 4.1.0-p5 and later is required for AppCentric Templates (ACT).

1. Obtain the latest version of ACT.
   - Send an e-mail to app-template@a10networks.com to get the latest copy.
   - The file size is about 2-3 MB.
2. Log in to A10 Thunder GUI.
3. Ensure that the clock and time zone of your Thunder device are set correctly.
4. Click System > App Template Import and follow instructions.

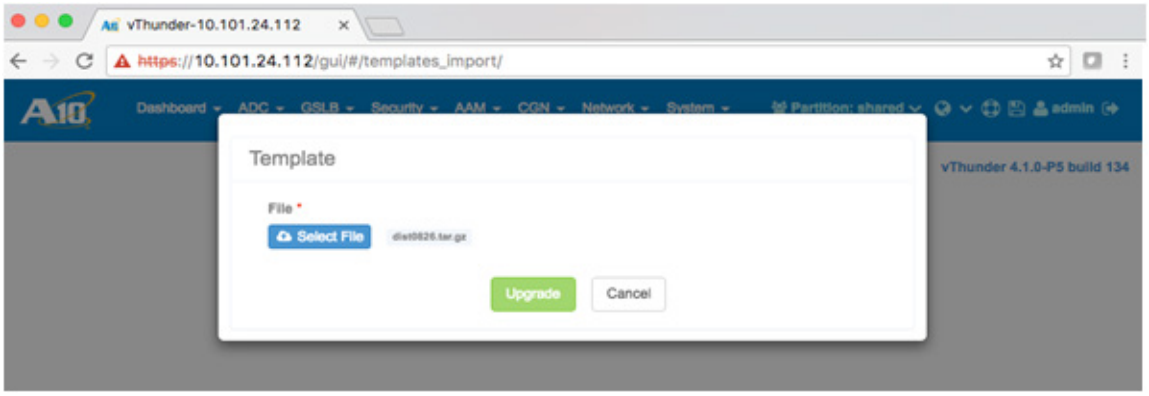

Figure 10: AppCentric Templates Upgrade

5. The upgrade is achieved seamlessly without disrupting any Thunder operations.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at a10networks.com/contact or call to speak with an A10 sales representative.

Part Number: A10-DG-16161-EN-01
Nov 2016