A Reference Design

VPN user access and VPC networking

Version 08-16-2016

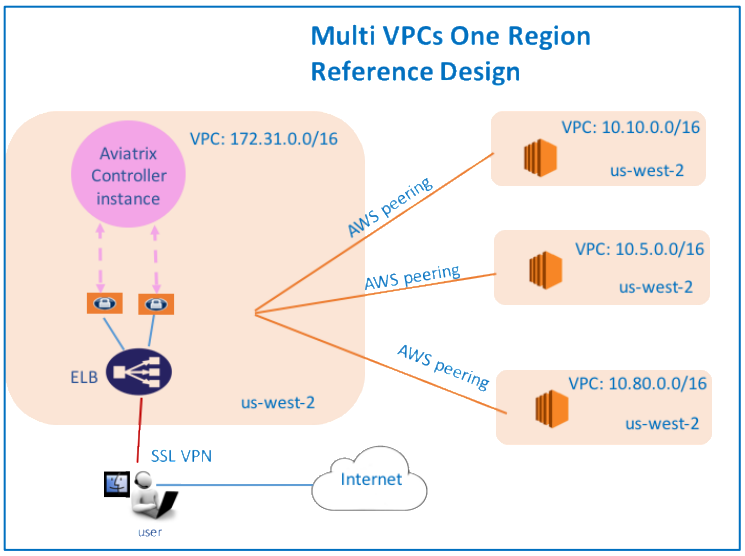
Copyright © 2014-2016 Aviatrix Systems, Inc. All rights reserved.

This reference design helps you build an end to end secure cloud network, from accessing the network (AWS VPC) by users to routing packets among the VPCs, such that once a user is connected via VPN, she can access any private resources in the cloud no matter where that resource is.

There are 3 use cases covered, from simple to more complex ones. You can read and decide which one suits you or combine parts from different ones to create a network that meet your requirements. You can easily build a full mesh network.

Multiple VPCs in one region

The network you have in mind is shown below where all VPCs are in the same region. The Aviatrix controller instance can be in the same or a different VPC.



Assume you have created 4 VPCs in the same region (us-west-2 in this case). You like to use the VPC with CIDR 172.31.0.0/16 to host gateways where users connect to. After a user connects to this VPC via SSL VPN, she should be able to access any instances in the other VPCs as long as her profile allows, without having to connect to each VPC with SSL VPN.

Another requirement is split tunnel mode, that is, only traffic destined to the cloud go through the SSL tunnel. If a user does general browsing to Internet or watch movies from Hulu, traffic should be routed via WI-FI to ISP to Internet. You do not wish to pay AWS for this type of compute and network costs.

Configuration Workflow

Tips: Mouse over the fields to see its definition. Do a software upgrade if an upgrade alert message appears on your dashboard page.

The description in the steps below provides critical fields you need to select; it may not include all fields. Make sure you have the correct VPC ID and its region for the VPC ID field and region in each step.

1. Launch a gateway with VPN capability in VPC 172.31.0.0/16.
    a. Go to Gateway menu and create. Make sure:
    b. At Gateway Name field, give it a distinct and convenient name. For example, mgmt-vpn-1
    c. Enable NAT is selected.
    d. VPN Access is selected.
    e. The VPN CIDR Block must be a subnet that is outside of all your current VPC CIDR range and outside your laptop or device subnet range. In the example above, you may enter 192.168.2.0/24.
    f. Split Tunnel Mode is selected.
        i. In the Additional CIDRs field under Split Tunnel, enter other VPCs/VNet or any network CIDRs you wish to reach beyond the VPC you are connecting to (in this case 172.31.0.0/16 is the connecting VPC). In the example shown, you should enter 10.10.0.0/16,10.5.0.0/16,10.80.0.0/16. It is a good idea to do some planning to include future VPCs or network address ranges. (In a case where you never have to worry about connecting to your corporate VPN, you may consider enter the entire private network address range in the Additional CIDRs range field, separating by comma: 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16. Doing so afford you not to have to reconfigure the gateway if you need to add more VPCs for networking with different CIDR range in the future.)
        ii. (Optional) For the Nameservers and Search Domain field under Split Tunnel, enter your DNS server IP addresses and search domain if you have setup to use DNS names to access instances inside VPCs. Leave it blank if you do not know what they are. If you use AWS Route 53 private zone records for your host names, make sure the Nameserver is the DNS server of the VPC. In this case, you should enter 172.31.0.2
    g. Enable AWS ELB is selected.
    h. Save Template is selected. This Template saves you from entering repeated fields if you wish to create more gateways with the same configuration.

2. Repeat Step 1 to create more gateways with VPN enabled. Note each gateway must have a different VPN CIDR Block and name. You may select different AZs for the Public Subnet field.

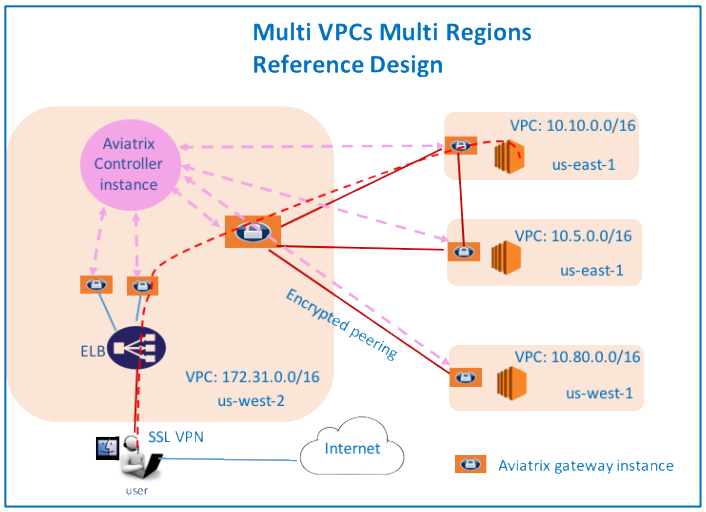
3. Configure AWS peering.
    a. Enter AWS console and select the region in which the VPCs were created. Select "Services"->"VPC"->"Peering Connections". Click "Create VPC Peering Connection" button to make AWS peering. In this case, we need to make the following three AWS peering connections. All these peering connections should have one peer at the VPC terminating your SSL VPN connections (VPC1 in this case).
        i. pcx-xxxxxxx1: VPC1 (CIDR 172.31.0.0/16) <-> VPC2 (CIDR 10.10.0.0/16)
        ii. pcx-xxxxxxx2: VPC1 (CIDR 172.31.0.0/16) <-> VPC3 (CIDR 10.5.0.0/16)
        iii. pcx-xxxxxxx3: VPC1 (CIDR 172.31.0.0/16) <-> VPC4 (CIDR 10.80.0.0.16)
    b. Modify the route tables of each VPC to add routes to its peer's subnets. In this case, the following route(s) should be added to each VPC's route table:
        i. VPC1 (172.31.0.0/16) route table:
            1. Destination 10.10.0.0/16 -> Target pcx-xxxxxxx1
            2. Destination 10.5.0.0/16 -> Target pcx-xxxxxxx2
            3. Destination 10.80.0.0/16 -> Target pcx-xxxxxxx3
        ii. VPC2 (10.10.0.0/16) route table:
            1. Destination 172.31.0.0/16 -> Target pcx-xxxxxxx1
        iii. VPC3 (10.5.0.0/16) route table:
            1. Destination 172.31.0.0/16 -> Target pcx-xxxxxxx2
        iv. VPC4 (10.80.0.0/16) route table:
            1. Destination 172.31.0.0/16 -> Target pcx-xxxxxxx3

4. Add Users and Profiles
    a. Go to Open VPN -> Profiles to create as many profiles as you please. The target field can be FQDN (DNS names or fully qualified domain name).
    b. Go to Open VPN -> Users to add as many user as you please. Associate each user with a profile. Note if no profile is associated, user has full access to all resources. When a user is added to the database, an email with .ovpn file or .onc (for Chromebooks) will be sent to the user with detailed instructions.

5. Launch VPN connections from remote users to VPC1 (172.31.0.0/16). Once the SSL VPN connection is established, this VPN user should be able to reach all instances (in all VPCs) to which he/she has access permission.
6. For support, send email to support@aviatrix.com.
7. For feature request, click Make a wish at the bottom of each page.
8. Enjoy!

Multiple VPCs in multi regions, split tunnel

The network you have in mind is shown below where VPCs are in different regions. The Aviatrix Controller instance can be in the same or a different VPC.



Assume you have created 4 VPCs. You like to use the VPC with CIDR 172.31.0.0/16 in us-west-2 to host gateways where users connect to. After a user connects to this VPC via SSL VPN, she should be able to access any instances in the other VPCs as long as her profile allows, without having to connect to each VPC with SSL VPN.

Another requirement is split tunnel mode, that is, only traffic originated from the user and destined to resources in VPCs is routed through SSL VPN tunnel. The traffic to Internet will be routed through ISP instead of SSL VPN tunnel.

Configuration Workflow

Tips: Mouse over the fields to see its definition. The description in each step does not include all fields. Make sure you have the correct VPC ID and its region for the VPC ID field and region in each step.

1. Launch a gateway with VPN capability in VPC 172.31.0.0/16.
    a. Go to Gateway menu and click create.
    b. At Gateway Name field, give it a distinct and convenient name. For example, mgmt-vpn-1
    c. Enable NAT is selected
    d. VPN Access is selected.
    e. The VPN CIDR Block must be a subnet that is outside your current VPC CIDR range and your laptop or device subnet range. In the example above, you may enter 192.168.2.0/24.
    f. Split Tunnel Mode is selected.
        i. For the Additional CIDRs field under Split Tunnel, enter other VPC/VNet or any network CIDRs you wish to reach beyond the VPC you are connecting to. In the example shown, you should enter 10.10.0.0/16,10.5.0.0/16,10.80.0.0/16. It is a good idea to do some planning to include future VPCs or network address ranges. (In a case where you never have to worry about connecting to your corporate VPN, you may consider enter the entire private network address range in the Additional CIDRs range field, separating by comma: 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16. Doing so afford you not to have to reconfigure the gateway if you need to add more VPCs for networking with different CIDR range in the future.)
        ii. (Optional) If you like to use private DNS name to access instance, you can fill Nameservers and Search Domain field under Split Tunnel. Enter your private DNS

name and search domain. If you use AWS Route 53 private hosted zone and records for your host names, make sure the Nameserver is the DNS server of the VPC. In this case, you should enter 172.31.0.2

   g. Enable AWS ELB is selected.
   h. Save Template is selected. This Template saves you from entering repeated fields if you wish to create more gateways with the same configuration.

2. Repeat Step 1 to create more gateways with VPN enabled. You may select different AZs for the Public Subnet field.

3. Build encrypted routing networks to reach other VPCs.
   a. Launch a gateway without VPN capability in VPC 172.31.0.0/16. This is the routing gateway, make sure:
      i. At Gateway Field, give it a distinct and convenient name. For example, dev-east-1, or teamKardashian-east-1 for the Kardashian game project.
      ii. VPN Access is not selected.
      iii. Enable NAT is NOT selected (since step 1 has enabled NAT function for this VPC)
      iv. Save Template is not selected. (so that you don't overwrite the hard work of entering the fields of gateways with VPN enabled)
   b. Repeat step 3 for VPC 10.10.0.0/16, 10.5.0.0/16 and 10.80.0.0/16. Select Enable NAT if you want instances in these 3 VPCs to be able to reach Internet directly.
   c. Configure encrypted peering. Go to Peering -> New Peering. Note each VPC is represented by one or more gateways. Make sure you want to peer between two gateways without VPN capability.

4. (Optional) Setup Stateful Firewall Rules at VPC level
   Go to Gateway, select the gateway you just created to edit Security Policies to add any policies for each VPC.

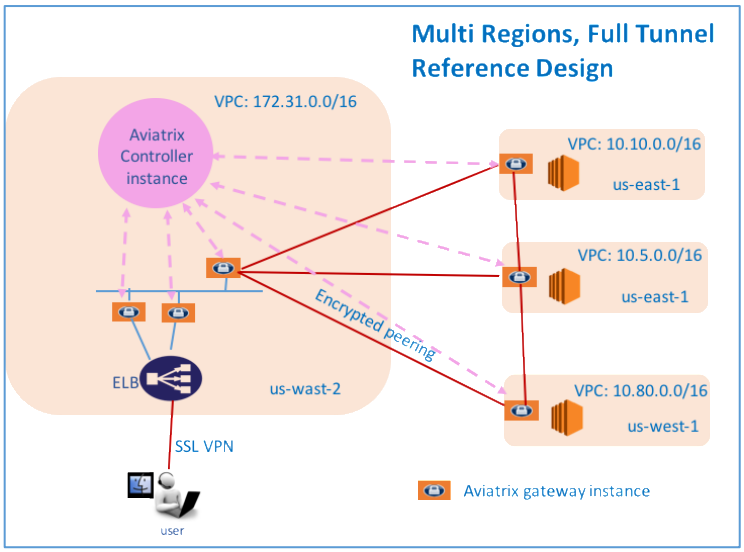
5. The above steps complete the network infrastructure setup.

6. Add Users and Profiles
   a. Go to Open VPN -> Profiles to create as many profiles as you please. The target field can be FQDN (DNS names or fully qualified domain name).
   b. Go to Open VPN -> Users to add as many user as you please. Associate each user with a profile. Note if no profile is associated, user has full access to all resources. When a user is added to the database, an email with .ovpn file or .onc (for Chromebooks) will be sent to the user with detailed instructions.

7. For support, send email to support@aviatrix.com.
8. For feature request, click Make a wish at the bottom of each page.
9. Enjoy!

Multiple VPCs in multi regions, full tunnel, your own firewall

The network you have in mind is shown below where VPCs are in different regions. The Aviatrix Controller instance can be in the same or a different VPC.



Assume you have created 4 VPCs. You like to use the VPC with CIDR 172.31.0.0/16 in us-west-2 to host gateways where users connect to. After a user connects to this VPC via SSL VPN, she should be able to access any instances in the other VPCs as long as her profile allows, without having to connect to each VPC with SSL VPN.

Another requirement is full tunnel mode, that is, all traffic originated from the user is routed through SSL VPN. Your organization requires to run its own firewall function for any Internet bound traffic.

Configuration Workflow

Tips: Mouse over the fields to see its definition. The description in each step does not include all fields. Make sure you have the correct VPC ID and its region for the VPC ID field and region in each step.

1. Launch a gateway with VPN capability in VPC 172.31.0.0/16.
    a. Go to Gateway menu and click create.
    a. At Gateway Name field, give it a distinct and convenient name. For example, mgmt-vpn-1
    b. Enable NAT is not selected.
    c. VPN Access is selected.
    d. The VPN CIDR Block must be a subnet that is outside your current VPC CIDR range and your laptop or device subnet range. In the example above, you may enter 192.168.2.0/24.
    e. Full Tunnel Mode is selected.
    f. Enable AWS ELB is selected.
    g. Enable Policy Based Routing (PBR) is selected.
        i. Note PBR Subnet must be a subnet that is in the same AZ as the primary subnet (Public Subnet where the gateway is launched). Enter the AWS subnet default

gateway for PBR Default Gateway field. For example, if PBR Subnet is 172.31.48.0/20, the default Gateway field is 172.31.48.1.

ii. (optionally) you can enable NAT Translation Logging to log every user's each activity to every server and site. This is useful to auditing and compliance.

h. Save Template is selected. This Template saves you from entering repeated fields if you wish to create more gateways with the same configuration.

2. Repeat Step 1 to create more gateways with VPN enabled. You may select different AZs for the Public Subnet field.

3. (Optional) If you have own your routing network to route between the VPCs and one of your own backbone routers can route traffic to your own firewall for Internet bound traffic, you can skip this step and the next two steps (step 4 and 5).
    a. Launch a gateway without VPN capability in VPC 172.31.0.0/16. This is the routing gateway, make sure:
        i. At Gateway Field, give it a distinct and convenient name. For example, dev-east-1, or teamKardashian-east-1 for the Kardashian game project.
        ii. Enable NAT is not selected.
        iii. VPN Access is not selected.
        iv. Save Template is not selected. (so that you don't overwrite the hard work of entering the fields of gateways with VPN enabled)

4. (Optional) Repeat step 3 for VPC 10.10.0.0/16, 10.5.0.0/16 and 10.80.0.0/16. Select Enable NAT if you wish the instances in these VPCs to be able to reach Internet directly.

5. (Optional) Configure encrypted peering. Go to VPC/VNet Encrypted Peering -> Add. Note each VPC is represented by one or more gateways. Make sure you want to peer between two gateways without VPN capability.

6. The above steps complete the network infrastructure setup.

7. Add Users and Profiles
    a. Go to Open VPN -> Profiles to create as many profiles as you please. The target field can be FQDN (DNS names or fully qualified domain name).
    b. Go to Open VPN -> Users to add as many user as you please. Associate each user with a profile. Note if no profile is associated, user has full access to all resources. When a user is added to the database, a email with .ovpn file or .onc (for Chromebooks) will be sent to the user with detailed instructions.

8. For support, send email to support@aviatrix.com.
9. For feature request, click Make a wish at the bottom of each page.
10. Enjoy!