Ashey, Bryce

Optum | Provider

Provider Transit Hub

with Azure Virtual WAN

Contents

[Applicable Datacenters & Regional Hubs 3](#_Toc52715862)

[Two Subscriptions 3](#_Toc52715863)

[Statement of Overall Business Goal 3](#_Toc52715864)

[Use Case Definitions Supporting Virtual WAN Connectivity 4](#_Toc52715865)

[Azure ExpressRoute [Hybrid] Connectivity 4](#_Toc52715866)

[Hospital HL7v2 Connectivity (Site-to-Site VPN) 4](#_Toc52715867)

[Future M&A Datacenter Connectivity 4](#_Toc52715868)

[Developer Access to Cloud Development Resources (Point-to-Site VPN) 4](#_Toc52715869)

[Production Support Access to Cloud Production Resources (Point-to-Site VPN) 4](#_Toc52715870)

[Ingress/Egress Management for Unmanaged Resources 5](#_Toc52715871)

[Legacy Domain Controller Support 5](#_Toc52715872)

[Virtual Machine Access Control (Non-Immutable Resources) 5](#_Toc52715873)

[Virtual Machine Configuration (Non-Immutable Resources) 5](#_Toc52715874)

[The Virtual WAN and Transit Hub is NOT… 6](#_Toc52715875)

[Provider Transit Hub 6](#_Toc52715876)

[Introduction to Azure Virtual WAN 6](#_Toc52715877)

[Provider’s Virtual WAN Implementation 7](#_Toc52715878)

[Common Design 8](#_Toc52715879)

[Transit Hub Firewall Design 9](#_Toc52715880)

[Routing Traffic within the Virtual WAN 10](#_Toc52715881)

[Securing Virtual Network Boundaries 11](#_Toc52715882)

[In-Region High Availability 11](#_Toc52715883)

[Transit Hub VPN Infrastructure Design 11](#_Toc52715884)

[VPN Authentication and Read-Only Domain Controllers 12](#_Toc52715885)

[Securing VPN TCP/IP Traffic 12](#_Toc52715886)

[Site-to-Site VPN Configuration [Discovery in Progress] 12](#_Toc52715887)

[Point-to-Site VPN Configuration [Discovery in Progress] 13](#_Toc52715888)

[Virtual WAN & Transit Hub ITSM 13](#_Toc52715889)

[Requiring Infrastructure as Code 13](#_Toc52715890)

[Change Management 13](#_Toc52715891)

[Infrastructure Changes 14](#_Toc52715892)

[Firewall Rules [Discovery in Progress] 14](#_Toc52715893)

[Site-to-Site VPN Setup [Discovery in Progress] 14](#_Toc52715894)

[Point-to-Site VPN Setup [Discovery in Progress] 15](#_Toc52715895)

[Peering Connections within the Virtual WAN 15](#_Toc52715896)

[Observability [Discovery in Progress] 15](#_Toc52715897)

[Integration Hub: General Infrastructure Health 15](#_Toc52715898)

[Palo Alto Health [Discovery in Progress] 15](#_Toc52715899)

[Hybrid Connectivity Health 15](#_Toc52715900)

[SIEM: Azure Sentinel and the Palo Altos [Discovery in Progress] 16](#_Toc52715901)

[Chargeback Model [Discovery in Progress] 16](#_Toc52715902)

[Appendix A: Cost Detail 17](#_Toc52715903)

[Appendix B: IP Allocations 18](#_Toc52715904)

[Appendix C: Per Use Case Implementation Detail 19](#_Toc52715905)

[Azure ExpressRoute [Hybrid] Connectivity 19](#_Toc52715906)

[Hospital HL7v2 Connectivity (Site-to-Site VPN) 20](#_Toc52715907)

[Future M&A Datacenter Connectivity 21](#_Toc52715908)

[Developer Access to Cloud Development Resources (Point-to-Site VPN) 22](#_Toc52715909)

[Production Support Access to Cloud Production Resources (Point-to-Site VPN) 23](#_Toc52715910)

[Ingress/Egress Management for Unmanaged Resources 24](#_Toc52715911)

[Legacy Domain Controller Support 25](#_Toc52715912)

[Virtual Machine Access Control (Non-Immutable Resources) 26](#_Toc52715913)

[Virtual Machine Configuration (Non-Immutable Resources) 27](#_Toc52715914)

[References 28](#_Toc52715915)

# Applicable Datacenters & Regional Hubs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Common Name | M&A or UHG |  | On UHG Network | CIDRs / # Devices |
| Ashburn | M&A | VA730 | Yes via MPLS | 1120 devices  10.210.128.0/18  10.211.128.0/18  10.250.160.0/21 |
| Austin | M&A | TX746 | Yes via MPLS | 290 devices  10.211.64.0/18 |
| Chaska | UHG | MN011 | N/A | ~848 devices |
| Elk River | UHG | MN053 | N/A | ~848 devices |
| Georgia RNH | UHG | GA777 | N/A | N/A |
| NTTA | M&A | VA732 | Via VPN | ~250 devices  216.167.124.64/26  216.167.127.0/26  209.207.253.0/24  209.207.254.0/24  209.207.255.0/24  198.107.199.0/24  198.64.143.64/29  198.65.114.64/29  198.65.147.152/29  198.104.156.x  161.58.180.x  161.58.191.x |
| Pennsylvania | M&A | PA007 |  |  |
| Sommersville | M&A | MA710 |  | 560 devices  172.30.64.0/18 |
| Tampa | M&A | FL750 | Yes via MPLS | 4890 devices  10.140.0.0/19 & 10.142.64.0/19 |

# Two Subscriptions

ASK ID: **UHGWM110-026739**

|  |  |  |
| --- | --- | --- |
| Name | Prod? | Description |
| Transit Hub | Non-Prod | Used for pre-testing any infrastructure changes to the Virtual WAN or Transit Hub before deploying to production. |
| Transit Hub | Prod | Host to the Virtual WAN itself. Also hosts both the Palo Alto Firewall and the Palo Alto VPN implementations. |

# Statement of Overall Business Goal

Provider, as a business, has elected to migrate out of all physical datacenters and move its entire platform onto one or more public cloud providers. This decision is based on the forecasted savings versus continuing to host Provider’s products in various M&A and “core” (Chaska/Elk River) datacenters. To this end, a large sum of L.E.G.O. funding is now available to the teams to facilitate rapid migration.

**During the course of executing this goal, Provider Engineering teams will continue to strive to move to highly isolated environments exposing HTTPS endpoints**. However, there will be instances where Provider chooses speed of migration over technology refactor. Likewise, there will be instances where refactor is not an option (e.g. vendor products). These exceptions are evaluated in each cost-benefit analysis and may be deemed acceptable given Provider’s overall goal of a purely cloud based infrastructure.

In addition to supporting hybrid, business partner, and employee access the Provider Virtual WAN will facilitate operation and maintenance of the systems that cannot be natively migrated. The following section outlines the various use cases, supported by the Virtual WAN, in greater detail.

# Use Case Definitions Supporting Virtual WAN Connectivity

## Azure ExpressRoute [Hybrid] Connectivity

Provider hosts a 10Gbps Azure ExpressRoute connection to the FL750 “Tampa” datacenter. The primary use case behind this connectivity is to facilitate the transfer of backup data from FL750 to Azure via Azure Site Recovery (for application servers) and the command line utility, “az copy”, for SQL Servers residing in FL750. A secondary use case, for this connectivity, has developed in the form of enabling temporary access to on-premise infrastructure in order to expedite migrating data or services to Azure. The architecture utilizes a Palo Alto to control traffic between on-premise and the various product virtual networks in the cloud. Change management is performed via the UnitedHealth Group firewall change management process.

This functionality is in place today.

## Hospital HL7v2 Connectivity (Site-to-Site VPN)

The Provider portfolio of products currently supports over 200 Site-to-Site VPN connections to various partners and customers. These VPN connections primarily consist of HL7v2 traffic utilizing the Minimal Lower Layer Protocol (MLLP). Today the endpoints primarily connect to several of Provider’s merger and acquisition (M&A) datacenters including NTTA (VA726), Ashburn (VA730), and Tampa (FL750). While Provider is working to migrate these older technologies to HL7v3 (i.e. over HTTPS) that work is projected to take the next 3 to 5 years.

## Future M&A Datacenter Connectivity

Provider must maintain the ability to integrate future merger & acquisition datacenters into Provider’s platform through both public and private network connectivity. To this end, Provider’s WAN infrastructure must support Site-to-Site VPN (including source/destination NAT) and dedicated line (e.g. ExpressRoute).

## Developer Access to Cloud Development Resources (Point-to-Site VPN)

As Provider’s entire platform shifts to the cloud Developers must be able to access resources that are hosted on both public and private endpoints in the cloud. These resources include databases, cache services, queue services, and other managed services. Access to these resources should be limited to the scope of the resources the team is working with (i.e. one product team should not be able to interact with another product team’s resources).

## Production Support Access to Cloud Production Resources (Point-to-Site VPN)

In similar fashion to developers, production support personnel need to access unmanaged databases and other resources in Production environments for both troubleshooting and maintenance. This access must be tightly controlled and must adhere to all compliance controls.

## Ingress/Egress Management for Unmanaged Resources

For non-managed infrastructure (i.e. traditional Virtual Machines) both ingress and egress must be actively controlled through Layer 7 capable inspection. While there are a number of cloud native tools available for inspection of inbound HTTPS the control of outbound HTTPS and other protocols (at layer 7) is lacking. In these scenarios the use of a Network Virtual Appliance, such as a Palo Alto, is required.

## Legacy Domain Controller Support

In some migration use cases the teams are unable to refactor their large (30+ terabytes) legacy database implementations within the time frame given for migration (in some cases that refactor is projected to take 3-5 years). This necessitates providing the ability to move those databases to the cloud over time while keeping the on-prem instance in-sync with the cloud instance. Unfortunately, technology limitations with Microsoft SQL Server require that both on-prem and cloud instances utilize the same domain for authentication. This, in-turn, requires that connectivity be maintained and protected for an extended, but still temporary, period.

## Virtual Machine Access Control (Non-Immutable Resources)

Most of Provider’s products adhere to one compliance paradigm or another; perhaps the most common paradigm being SOC2. As part of SOC2 and UHG’s own compliance policies there are a number of controls that are required for user access to virtual machines. These controls cover areas such as least privilege, disallowing shared logins, entitlement reviews, password strength policies, and many more. Any non-immutable unmanaged resources will need to adhere to these policies. Therefore, appropriate connectivity and resources must be created to meet this need.

## Virtual Machine Configuration (Non-Immutable Resources)

Unless under very dire exception all resources within a public cloud must be configured using Configuration as Code techniques. It is outside the scope of this document to describe the reasons why this is a minimum requirement however supporting the connectivity required to allow for Configuration as Code tools is very much within the scope of this document. It is most common for configuration tools (Chef, Puppet, Ansible, etc.) to operate over SSH for Linux and WinRM for Windows. Sufficient connectivity must be maintained to these resources to allow the configuration tools to operate.

# The Virtual WAN and Transit Hub is NOT…

To clarify before going to much farther, the Virtual WAN and Transit Hub is **not** a replacement for ingress and egress to Azure managed services. It is not replacing Azure Front Door, Application Gateway, nor is it facilitating ingress/egress for Azure Kubernetes Service. In point of fact, all resources using the Transit Hub for ingress/egress should have a plan to migrate to more native solutions as quickly as possible. This solution is meant to facilitate migration when there are other business factors driving a shift to the cloud which may not allow for adoption of more native technologies.

# Provider Transit Hub

## Introduction to Azure Virtual WAN

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface (Microsoft, 2020). These functionalities include branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE), Site-to-site VPN connectivity, remote user VPN (Point-to-site) connectivity, private (ExpressRoute) connectivity, intra-cloud connectivity (transitive connectivity for virtual networks), VPN ExpressRoute inter-connectivity, routing, Azure Firewall, and encryption for private connectivity.

The Virtual WAN architecture is a hub and spoke architecture with scale and performance built in for branches (VPN/SD-WAN devices), users (Azure VPN/OpenVPN/IKEv2 clients), ExpressRoute circuits, and virtual networks. It enables global transit network architecture, where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.

Azure regions serve as hubs that you can choose to connect to. All hubs are connected in full mesh in a Standard Virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity. For spoke connectivity with SD-WAN/VPN devices, users can either manually set it up in Azure Virtual WAN or use the Virtual WAN CPE (SD-WAN/VPN) partner solution to set up connectivity to Azure.

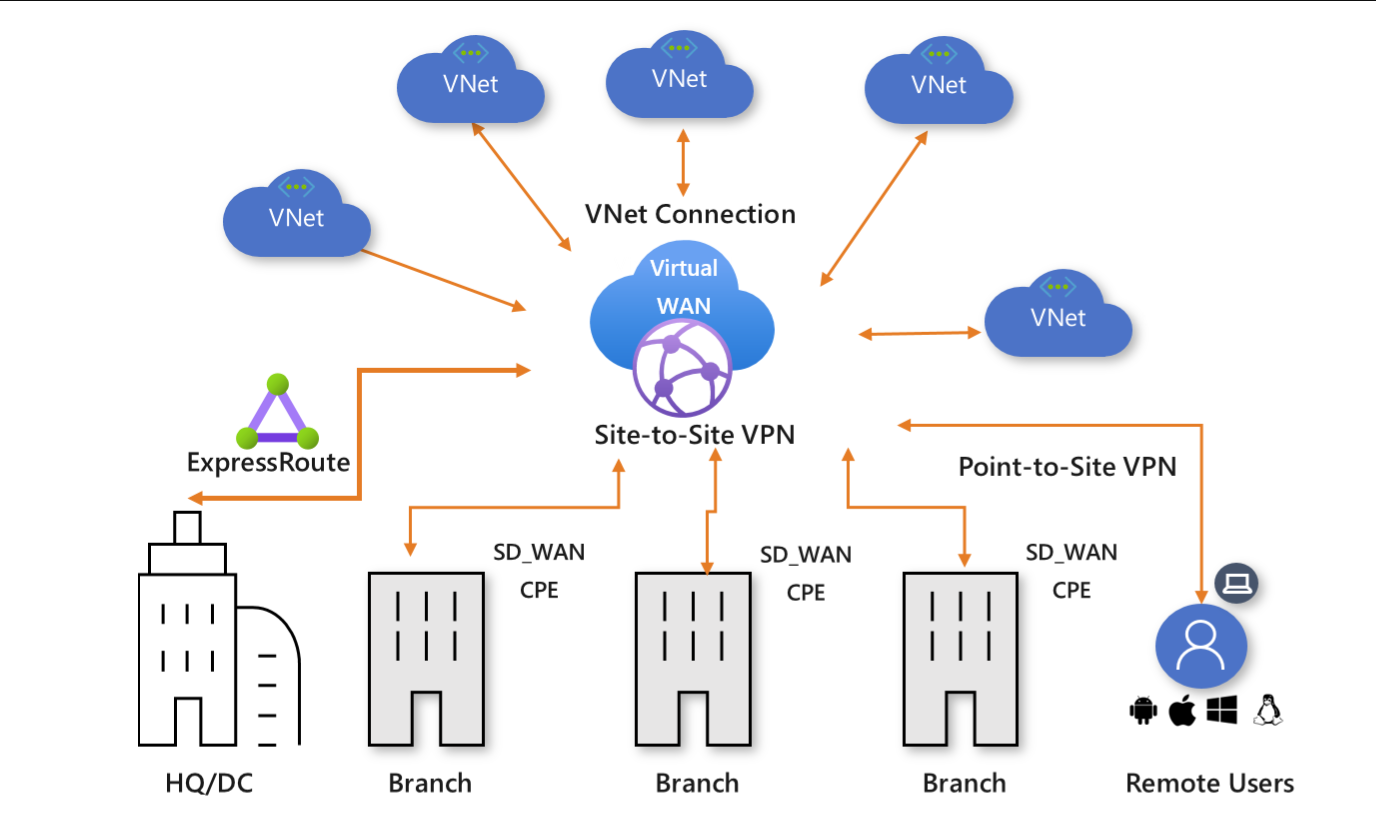


Figure : Azure's Reference Virtual WAN

## Provider’s Virtual WAN Implementation

The Provider team participated in several discovery discussions with Microsoft around implementing Azure Virtual WAN. This discovery outlined the broad SD-WAN capabilities of Azure Virtual WAN and the various use cases it could potentially solve for. Based on this information, and some POC work to validate the routing use cases, the decision has been made to move forward with integrating Azure Virtual WAN into Provider’s network layer.

However, during the aforementioned sessions the need for a customized approach was identified. This approach involves routing traffic through a Network Virtual Appliance (NVA) in order to meet UHG requirements around Layer 7 controls (Microsoft, 2020). Provider will use Palo Alto devices for its NVAs.

Likewise, Provider will utilize Palo Alto devices for its site-to-site VPN needs. This is due to the need to support source and destination NAT for prospective VPN (i.e. hospital) sites. Both are represented in *Figure 1: Azure's Reference Virtual WAN* by the “VM-Series” icons on the right.

Routing rules will be setup on the Virtual WAN such that all traffic routes through the Transit Hub firewall appliances before carrying on to its final destination. Examples of this routing is detailed in the *Per Use Case Implementation Detail* section at the end of this document. In the case of routing to product virtual networks there is still a requirement to allow various inbound and outbound flows via network security group. This is due to the default “deny all” rule inherent to the Dojo network security group profile.

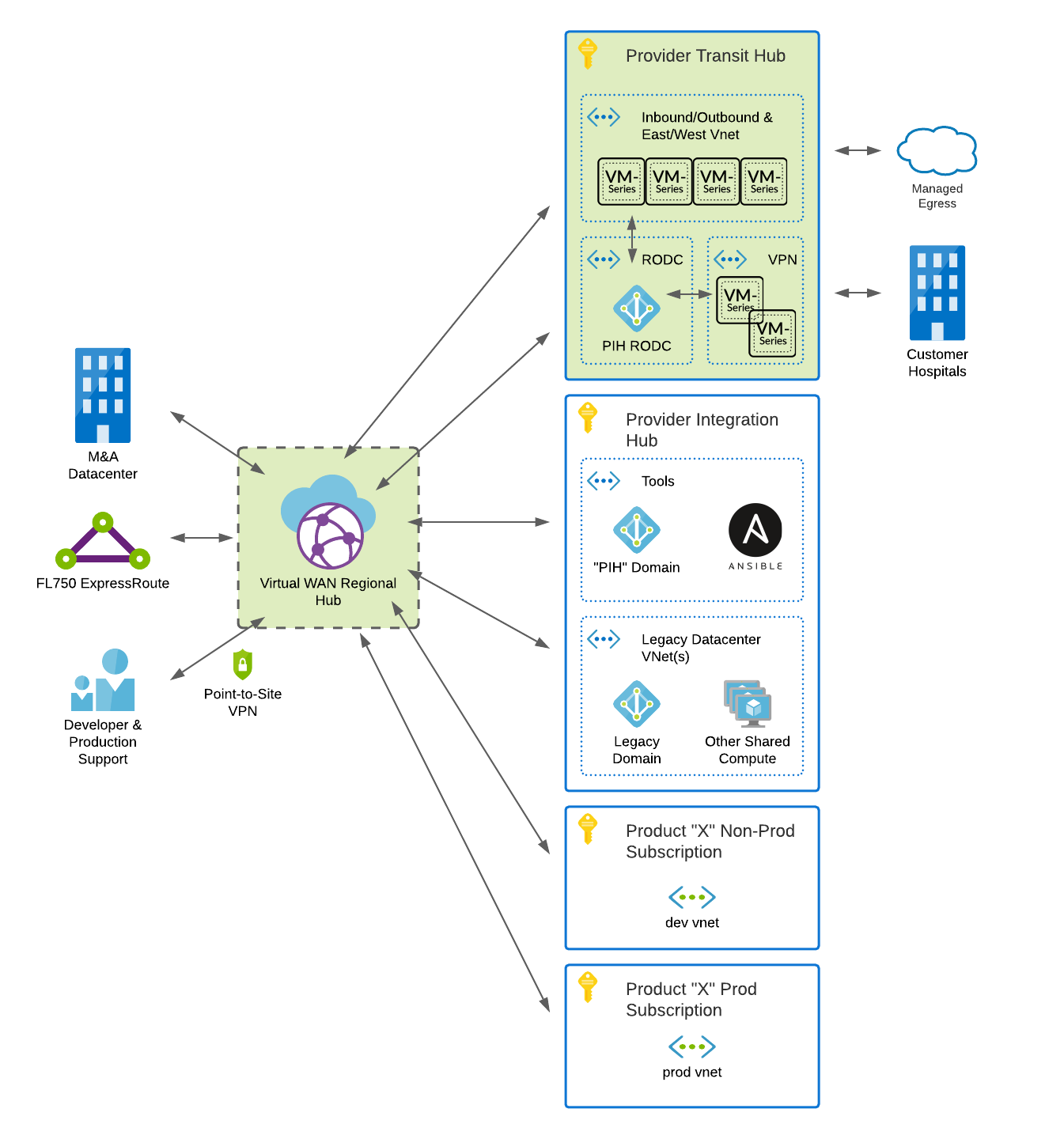


Figure : Provider Virtual WAN & Transit Hub (Highlighted)

## Common Design

The following table describes the resource groups utilized in the creation of the Provider Virtual WAN.

|  |  |
| --- | --- |
| **Resource Group** | **Description** |
| Optum-pth-tfstate | Contains terraform state files for the Transit Hub |
| Provider-transit-hub-iobew-eastus-rg | Contains the Palo Alto firewalls (x4) in Transit Hub configuration. |
| Provider-transit-hub-vpn | Contains the Palo Alto VPN Appliances |
| Provider-transit-hub-vwan-centralus | Contains the CentralUS Regional Hub |
| Provider-transit-hub-vwan-eastus | Contains the Virtual WAN and EastUS Regional Hub |
| Provider-transit-hub-vwan-eastus2 | Contains the EastUS2 Regional Hub |
| Provider-transit-hub-vwan-westus | Contains the WestUS Regional Hub |
| Pth-subscription-bootstrap-eastus | Contains the bootstrap resources for the subscription |

## Transit Hub Firewall Design

As previously mentioned, the primary method of controlling traffic within the Virtual WAN implementation is a set of four Palo Alto devices configured based on Palo Alto’s Transit Hub design (Palo Alto, 2020). In this model, the functions and resources are allocated across multiple Virtual Networks that are connected in a hub-and-spoke topology. The hub of the topology, or transit Virtual Network, is the central point of connectivity for all inbound, outbound, east-west, and backhaul traffic. The spokes isolate workloads in their own Virtual Networks. This design model is highly scalable and highly resilient and is suitable for large-production deployments.

The model separates inbound traffic flows onto a dedicated set of firewalls, allowing for greater

scaling of inbound traffic loads. Outbound, east-west, and backhaul traffic flows through a common firewall set that is a shared resource (OBEW in *Figure 3: Palo Alto Transit Hub Implementation (Sample CIDRs)*). All firewalls are deployed in the Transit Virtual Network.

This model consolidates resources that multiple workloads can share. This model also offers

increased scale and operational resiliency while reducing the chances of high bandwidth use from the inbound traffic profile affecting other traffic profiles. Palo Alto recommends this model for production deployments

For Provider’s setup the default configuration found in the Transit VNet Design Model (Palo Alto, 2020) will be sufficient.

The Transit Hub will *replace* the existing Palo Alto implementation connected to Provider’s FL750 ExpressRoute connection. Management of the new firewalls will transition from the UHG firewall team to the Provider DevOps Enablement Team.

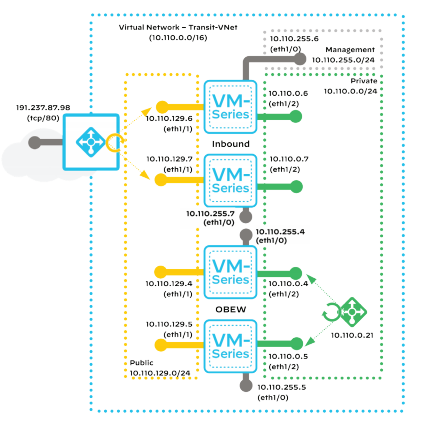


Figure : Palo Alto Transit Hub Implementation (Sample CIDRs and Ports)

### Graphical user interface, diagram, application Description automatically generated

Figure : Detailed diagram of the Transit Hub as implmented by Provider

### Routing Traffic within the Virtual WAN

By default, all traffic which crosses the Virtual WAN, will have a default route set to the OBEW firewalls. The rulesets within these firewalls will manage all traffic bound for other virtual networks.

While Provider strongly encourages inbound requests to be managed through Azure native capabilities (Front Door (FD), Web Application Firewall (WAF), Application Gateway (AG), etc.) there may be instances where, due to default outbound routing, the Palo Altos will also need to service inbound requests (to avoid asymmetric routing concerns). In these scenarios the traffic will flow through the Inbound firewalls and subsequently routed to their final destination. Both the firewall and the destination subnet network security groups will need to be updated to allow this traffic. It is expected that destination application adheres to the same policies as if the architecture was using a Web Application Firewall instead.

Examples of various routing scenarios can be found in [Appendix C: Per Use Case Implementation Detail](#_Appendix_C:_Per).

The following tables document the routing implemented within the Transit Hub to ensure that all traffic is routed to Palo Altos before continuing on to its final destination.

The RT\_Subscriber table is placed on each Virtual Network that connects to the Provider Transit Hub. This forces all private traffic through the OBEW firewalls.

|  |  |  |  |
| --- | --- | --- | --- |
| RT\_Subscriber | | | |
| Route Name | Destination Type | Destination Prefix | Next Hop |
| RT\_Core | CIDR | 10.0.0.0/8 | transit-hub-iobew-to-eastus-hub |

The RT\_Hub\_EastUS route table is placed on the EastUS Regional Hub and directs any traffic that leaves the firewalls back down the VWAN hubconnection and into the Provider Virtual WAN.

|  |  |  |  |
| --- | --- | --- | --- |
| RT\_Hub\_EastUS | | | |
| Route Name | Destination Type | Destination Prefix | Next Hop |
| RT\_Subscriber | CIDR | 10.225.160.0/20 | transit-hub-iobew-to-eastus-hub |
| RT\_Subscriber | CIDR | 10.225.208.0/22 | transit-hub-iobew-to-eastus-hub |
| RT\_Subscriber | CIDR | 10.225.212.0/23 | transit-hub-iobew-to-eastus-hub |
| RT\_Subscriber | CIDR | 10.225.214.0/24 | transit-hub-iobew-to-eastus-hub |
| RT\_Subscriber | CIDR | 10.225.216.0/22 | transit-hub-iobew-to-eastus-hub |
| RT\_Subscriber | CIDR | 10.225.224.0/20 | transit-hub-iobew-to-eastus-hub |

The RT\_Shared route table is associated to the transit-hub-iobew-to-eastus-hub connection and all subscribing virtual networks. As virtual networks are associated to the route table their routes become available on the IOBEW hubconnection.

|  |  |  |  |
| --- | --- | --- | --- |
| RT\_Shared | | | |
| Route Name | Destination Type | Destination Prefix | Next Hop |
| Empty |  |  |  |
| Associate to transit-hub-iobew-to-eastus-hub | | |  |
| Propogate to transit-hub-iobew-to-eastus-hub | | |  |
| Propogate to ExpressRoute | |  |  |
| Propogate to all Subscriber connections? | | |  |
| Propogate to integration hub connection? | | |  |

The final route table resides on the transit-hub-iobew-to-eastus-hub connection itself and routes traffic bound for other networks to the load balanced IP on the OBEW firewalls.

|  |  |  |
| --- | --- | --- |
| transit-hub-iobew-to-eastus-hub | | |
| Route Name | Destination Prefix | Next Hop |
| 1 | 10.140.0.0/19 | 10.225.215.90 |
| 2 | 10.225.160.0/20 | 10.225.215.90 |
| 3 | 10.225.208.0/21 | 10.225.215.90 |
| 4 | 10.225.212.0/23 | 10.225.215.90 |
| 5 | 10.225.214.0/24 | 10.225.215.90 |
| 6 | 10.225.216.0/22 | 10.225.215.90 |
| 7 | 10.225.224.0/20 | 10.225.215.90 |

### Securing Virtual Network Boundaries

Securing Virtual Networks within the Provider Virtual WAN will occur at Layers 3, 4, and 7 and in two locations: the Palo Altos and the network security groups on the individual subnets within a given Virtual Network.

* Palo Altos
  + Layer 3:
    - All IPs default to DENY
    - Any easing of default DENY requires firewall request
  + Layer 4:
    - All ports default to DENY
    - Any easing of default DENY requires firewall request
  + Layer 7:
    - Whenever possible the [App ID](https://applipedia.paloaltonetworks.com/) will be specified on rules within the Palo Altos
* Network Security Groups on Subnets
  + Layer 3:
    - All IPs default to DENY
    - Rules must be added for each group of IPs
    - Either source or destination must generally be specific (i.e. not a range).
  + Layer 4:
    - All ports default to DENY
    - Rules must be added for each set of ports

### In-Region High Availability

Each pair of Palo Alto’s will be setup using Azure Availability Zones allowing for upgrade and patching to occur as well as failover.

## Transit Hub VPN Infrastructure Design

The Transit Hub VPN appliances are designed to support the Site-to-Site VPN requirements of Provider. The Point-to-Site VPN needs will be handled by the Virtual WAN itself.

Site-to-site VPN functionality will be handled by a pair of HA Palo Altos in a Virtual Network connected to the Virtual WAN Hub (Palo Alto, 2020). This model is a standard Active/Passive implementation. Hospital (or other) traffic inbound for product virtual networks will route across the OBEW firewalls before continuing on to its final destination. Client traffic will be limited at both the Palo Alto OBEW device and at the Azure Network Security Group level within each destination subnet.

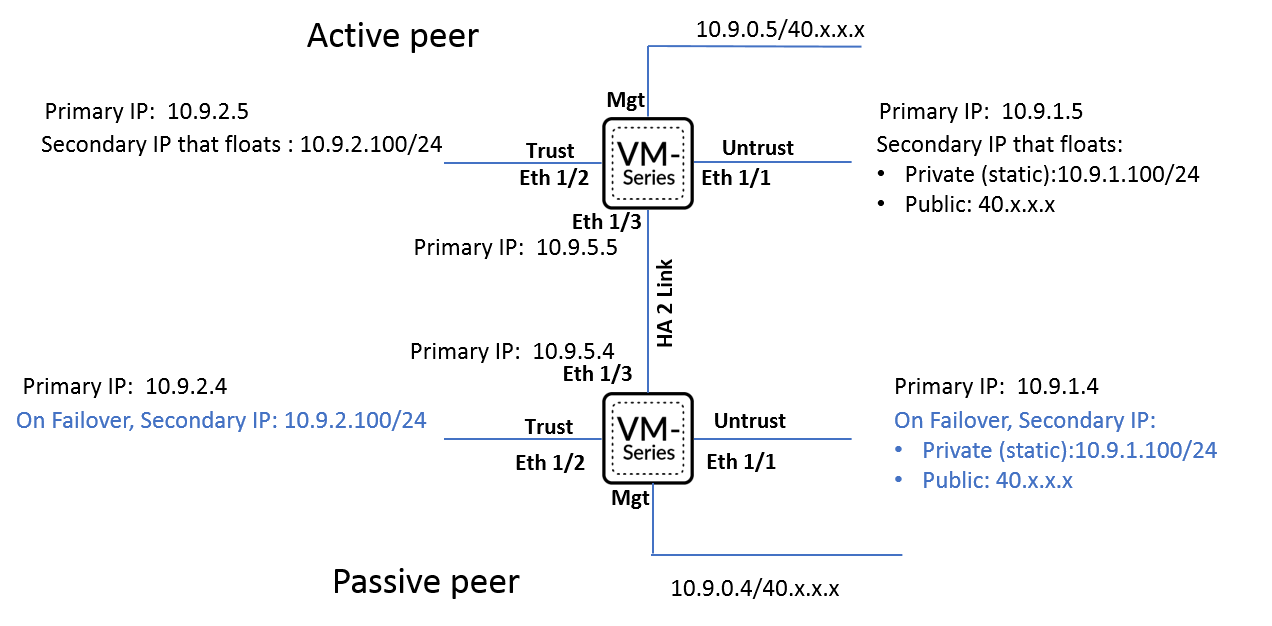


Figure : Palo Alto HA Implementation (Sample CIDRs)

### VPN Authentication and Read-Only Domain Controllers

Per policy 9D.1.02.02 internet facing devices should access read-only domain controllers for authentication. To meet this need, a pair of read-only domain controllers will be setup in a Transit Hub virtual network. This virtual network will be connected to the Virtual WAN and only accessible from the Palo Alto devices in the Transit Hub.

### Securing VPN TCP/IP Traffic

VPN traffic will be limited by policy to ensure that said traffic only has access to the infrastructure required by each given use case. For example, if ODXI needs to allow a customer hospital to access its Ensemble application servers on TCP 7501 then only that access shall be granted. Likewise, for point-to-site, network access shall be limited to only those resources and ports that are required for that use case.

### Site-to-Site VPN Configuration [Discovery in Progress]

Reference Control Mapping excel sheet for current status.

### Point-to-Site VPN Configuration [Discovery in Progress]

[ON HOLD PENDING DISCUSSIONS WITH INTERNAL VPN TEAM AND ALWAYS ON VPN]

# Virtual WAN & Transit Hub ITSM

Managing the operation and maintenance of Provider’s Virtual WAN falls to the Provider DevOps Enablement group, the production support team(s), production database administrators, and the Application Operations Center (AOC). The Provider Cloud Enablement team will provide support, guidance, and enhancements whenever and wherever there is a need. At the time of this writing those teams are managed by Bryan Moore, John Harrast, Girum Fida, and Chris Dutilly respectively. These teams will leverage the tools and processes outlined below to manage Provider’s Virtual WAN.

## Requiring Infrastructure as Code

Wherever and whenever possible it is expected that all changes will be implemented via code and deployed via a continuous delivery pipeline (such as Jenkins). In some cases, custom coding may be required to create the change via API. The Cloud Enablement team will strive to codify these more complex updates within the ProviderRM terraform provider.

In rare exceptions, for instance mapping fiber circuits to Azure ExpressRoute, changes can only be completed manually via the Azure Portal. When a change must be done manually that change must have detailed steps documented within the change ticket and must have a corresponding rollback plan. Manual changes must not subsequently break the terraform deployments (i.e. terraform state must be kept in sync or somehow exclude the manual changes).

## Change Management

Optum’s ServiceNow Change Management process will be leveraged to track all changes deployed to the Virtual WAN. This includes any changes to the Virtual WAN itself, firewall changes, Site-to-Site VPN changes, Point-to-Site VPN changes, and the creation or removal of any peering connections within the Virtual WAN. The following devices and device rollups will, initially, be registered with CMDB to allow for tracking of changes:

* Provider FL750 ExpressRoute (rollup for all circuits and devices)
* Provider Virtual WAN
* Provider Virtual WAN Point-to-Site VPN “NNN” (each unique VPN will have an entry)
* Provider Transit Hub Firewall (rollup for all four firewall devices)
* Provider Transit Hub VPN (rollup for both VPN devices)

As stated, this is an initial list and will change over time. CMDB should be considered the source of truth not this document. It is the responsibility of downstream services to manage their dependencies upon the above configuration items. This management can be accomplished through CMDB and Central CI located at <https://ask.optum.com>.

### Infrastructure Changes

All infrastructure changes will require a ServiceNow Change Management ticket with dependent configuration items added for all devices and/or rollups that are being affected by the change.

### Firewall Rules [Discovery in Progress]

*This section’s guidance is subject to change pending follow-on discussions with Ryan Hightshoe (Optum Info Sec Engineering), Scot Long (firewall team), David Mott (Cloud EIS), EGRC administrators, and other stakeholders.*

With the advent of the Virtual WAN firewall changes will be handled by Provider personnel (versus the internal Optum team; Scot Long’s group). Therefore, sufficient review must occur to track the changes within Optum’s systems.

Firewall rules follow a three-step process:

1. A submission via an interface similar to Optum’s Navigator tool will send a request to the Provider DevOps Enablement team with the detail behind the associated rules.
   1. This interface has yet to be codified and will be created in collaboration between the DevOps Enablement and Cloud Enablement teams.
2. Does a submission to EGRC (i.e. a Risk Review) for a firewall change using the firewall policy 9A.2.03.03 need to occur?
   1. A conversation with EGRC and Scot Long’s group must occur to ensure this conversation flows smoothly.
3. Once the above review is complete, the Provider DevOps Enablement team document the change to occur and will schedule a firewall change ticket within ServiceNow.
4. The Provider DevOps Enablement team will complete the change at the appropriate window and notify the requestor to validate.

### Site-to-Site VPN Setup [Discovery in Progress]

<need change management detail>

### Point-to-Site VPN Setup [Discovery in Progress]

[ON HOLD PENDING DISCUSSIONS WITH INTERNAL VPN TEAM AND ALWAYS ON VPN]

## Peering Connections within the Virtual WAN

Provider already has an established pattern for peering connections within Azure. There is an established ServiceNow Ticket under “Optum360 Infrastructure >> Cloud” which is subsequently then assigned to the Provider Cloud Enablement group for completion. The peering connection is currently routed through a pair of Palo Altos managed by the UHG firewall team. This is true for both virtual network to virtual network connectivity and virtual network to ExpressRoute connectivity.

Two changes will occur with the advent of the Provider Virtual WAN:

1. Peering connections will no longer be virtual network to virtual network. Both virtual networks will connect to the Virtual WAN Hub and be routed through the OBEW firewalls.
2. Over time, Provider expects this solution to move from ServiceNow to the Terraform provider being created by the Provider Cloud Enablement team. This Terraform Provider will allow teams to request a peering connection from an API and said connection will be automatically provisioned.

## Observability [Discovery in Progress]

### Integration Hub: General Infrastructure Health

In general, all systems within the Integration Hub will be monitored by Provider’s Splunk Suite of tools including SignalFx. The standard detectors for VM health (CPU, Memory, Disk, etc.) will be utilized. Any VM logs will be expected to be forwarded to Provider’s Event Hubs either directly or potentially via a Syslog forwarder. Custom detectors are of course encouraged on the platform.

### Palo Alto Health [Discovery in Progress]

Likely utilize the [Palo Alto Splunk App](https://splunkbase.splunk.com/app/491/) combined with VictorOps.

### Hybrid Connectivity Health

Azure network performance monitor will continue to be used to determine the health of the circuits and connections between the Azure Virtual WAN and other datacenters or clouds.

## SIEM: Azure Sentinel and the Palo Altos [Discovery in Progress]

*This guidance is pending full review with the Cloud team (Vanguard and EIS) to determine the best methodology. For instance, do we log to both our platform and launchpad? The assumption is yes but need to perform discovery.*

Azure Sentinel will be leveraged for logging, analytics, and threat detection on the Palo Alto devices (regardless of firewall or VPN configuration. The Palo Alto Networks data connector allows Palo Alto Networks logs to easily connect with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. Using Palo Alto Networks on Azure Sentinel will provide more insights into Provider’s internet usage, and will enhance its security operation capabilities (Microsoft, 2019).

Azure Sentinel provides out-of-the-box, built-in templates to help create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across the environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to an organization’s needs. The alerts generated by these rules will create incidents that can be assigned and investigated within the environment (Microsoft Docs, 2020).

The alerts originating from Azure Sentinel will be routed to Provider’s VictorOps Incident Management platform where the notification will be escalated according to the team escalation policies stored therein (VictorOps, 2020). The DevOps Enablement team (network and security personnel) will be responsible for responding to the alerts according to the severity of the alert.

# Chargeback Model [Discovery in Progress]

Much like the other shared services (Splunk, SignalFx, email relay, SQL Proxy, etc.) offered in Provider’s portfolio the Integration Hub, Transit Hub, and any Virtual WAN servcies are designed to be billed based on usage. At the time of this writing the discussions with finance, operations, and other stakeholders are ongoing as to the exact mechanism with which to perform this chargeback. This section will be updated as that conversation continues.

# Appendix A: Cost Detail

In addition to the device cost below there will be a transit charge of $.02/hour/GB across each Hub. There will also be charges for each unique service utilized (each VPN, ExpressRoute connection, etc.). More detail can be found on Azure’s [Virtual WAN pricing web page](https://azure.microsoft.com/en-us/pricing/details/virtual-wan/).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Description** | **Detail** | **VM Type** | **1 unit per hour** | **1 unit annual** | **total annual** |
| Transit Hub | I/OBEW Firewall | 4x PaloAlto | Standard DS3\_v2 | 1.38 | 12088.8 | 48355.2 |
| Transit Hub | HA VPN | 2x PaloAlto | Standard DS3\_v2 | 1.38 | 12088.8 | 24177.6 |
| Transit Hub | PIH Read-Only DC | 2x Windows2019 | Standard DS3\_v2 | 0.209 | 1830.84 | 3661.68 |
| Virtual WAN | East, West, & Central Hubs | 3 Virtual Wan Hubs |  | 0.25 | 2190 | 8760 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  | **Total** | 84954.48 |

# Appendix B: IP Allocations

10.225.160.0/20 – Original Allocation (since exhausted) – Reserved for Product Virtual Networks and FL750 DR

10.225.215.0/20 – Reserved for Virtual WAN, Integration Hub, and Transit Hub

10.225.224.0/20 – Additional Allocation for Product Virtual Networks

172.30.0.0/16 – Reserved for the VPN appliances to use when source and/or destination network address translation (NAT) of customer traffic needs to occur.

172.31.0.0/16 – Reserved for Transit Hub connected virtual networks to use for Bastion Hosts

# Appendix C: Per Use Case Implementation Detail

## Azure ExpressRoute [Hybrid] Connectivity

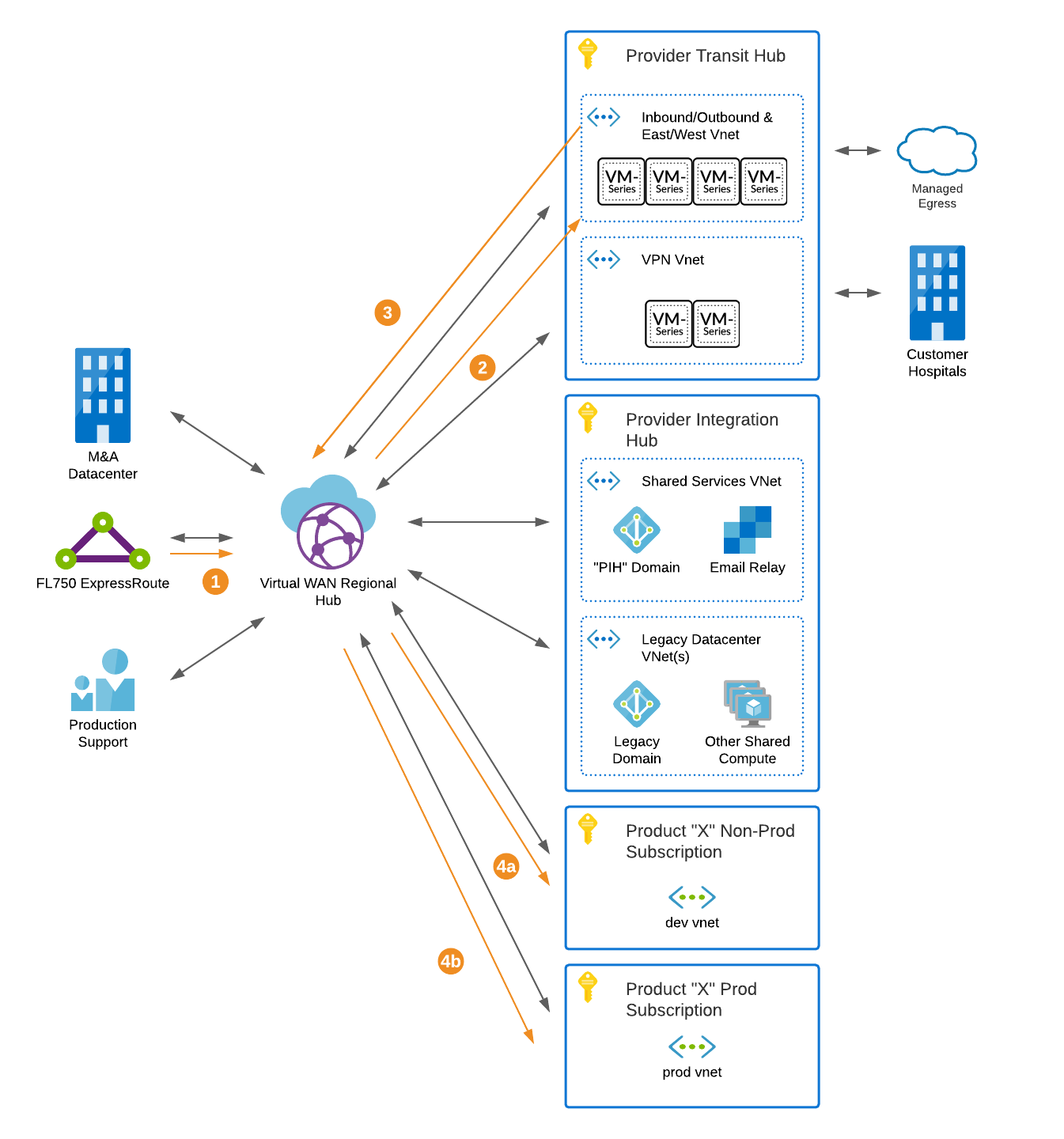


Figure : ExpressRoute Routing

## Hospital HL7v2 Connectivity (Site-to-Site VPN)

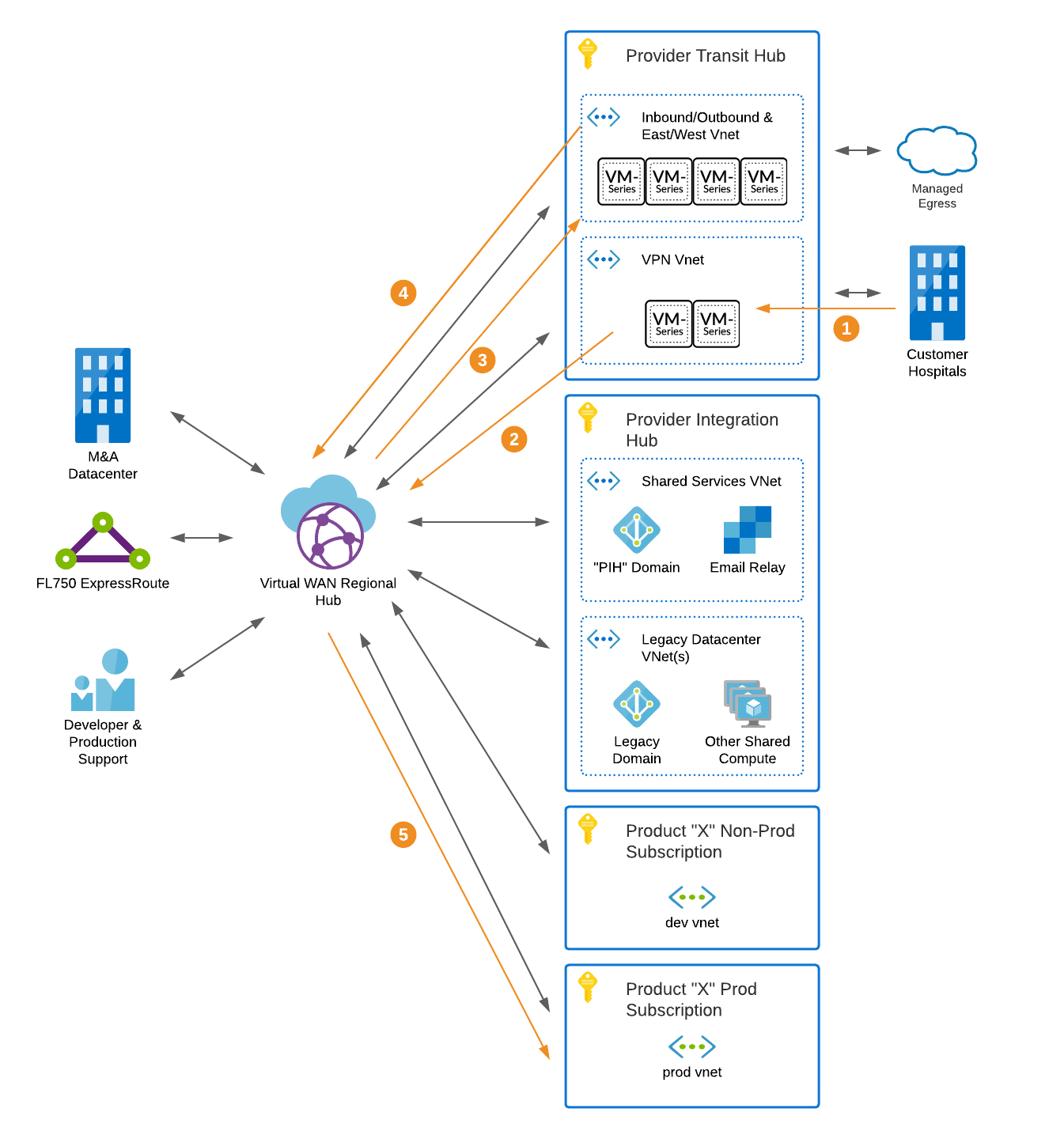


Figure : Hospital VPN Routing

## Future M&A Datacenter Connectivity

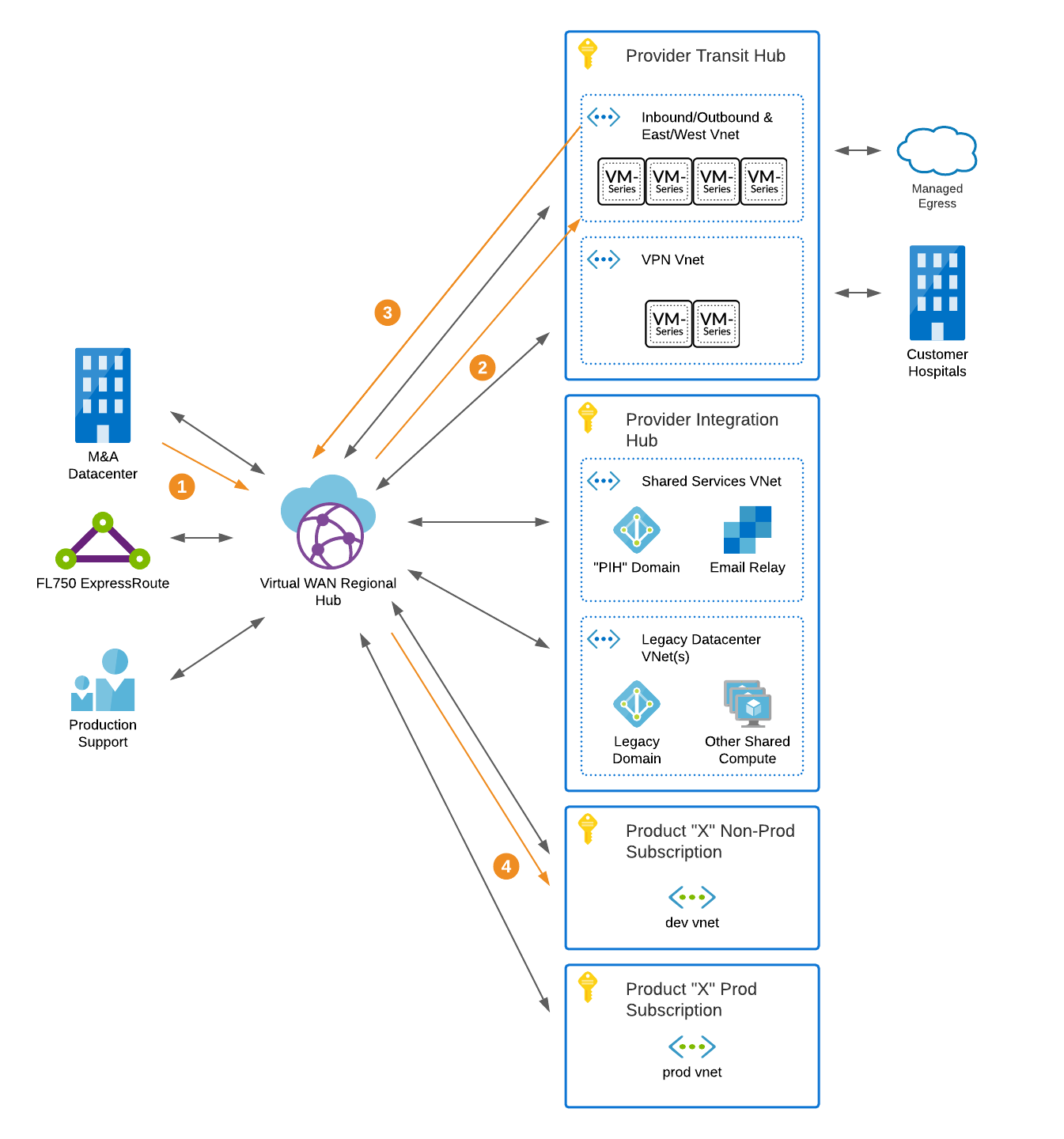


Figure : M&A Datacenter Routing

## Developer Access to Cloud Development Resources (Point-to-Site VPN)

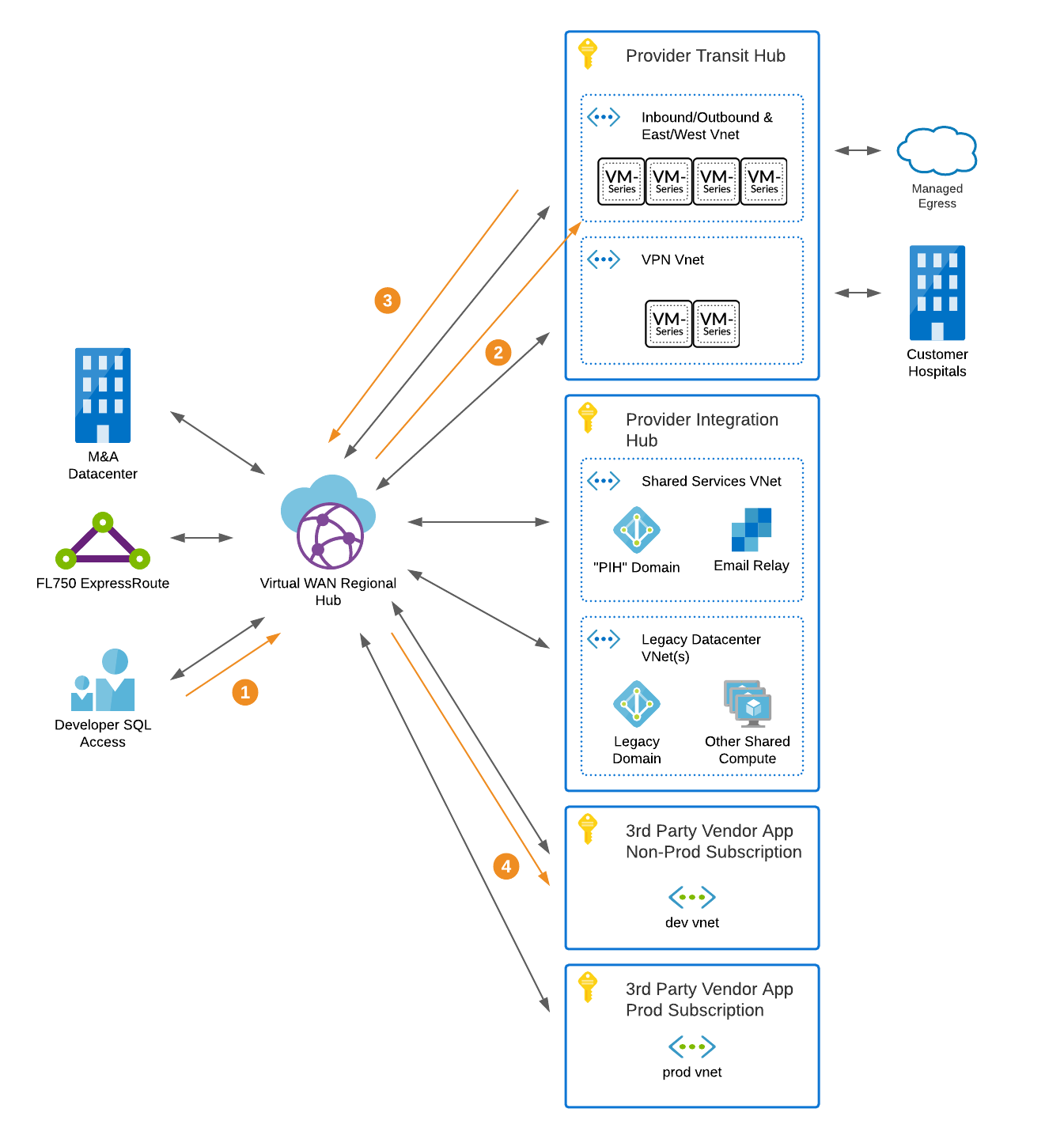


Figure : Developer SQL Access Routing

## Production Support Access to Cloud Production Resources (Point-to-Site VPN)

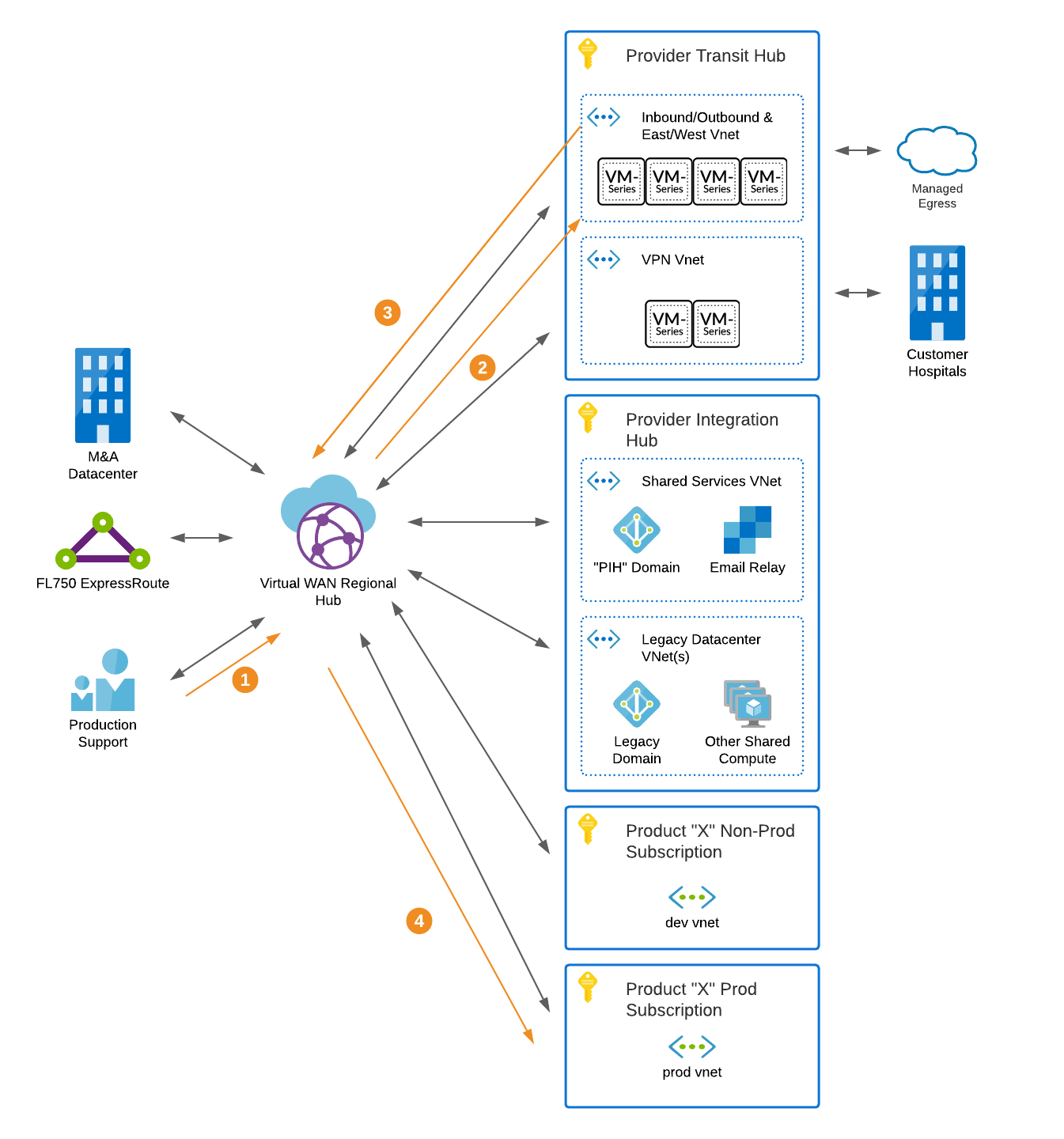


Figure : Production Control Access Routing

## Ingress/Egress Management for Unmanaged Resources

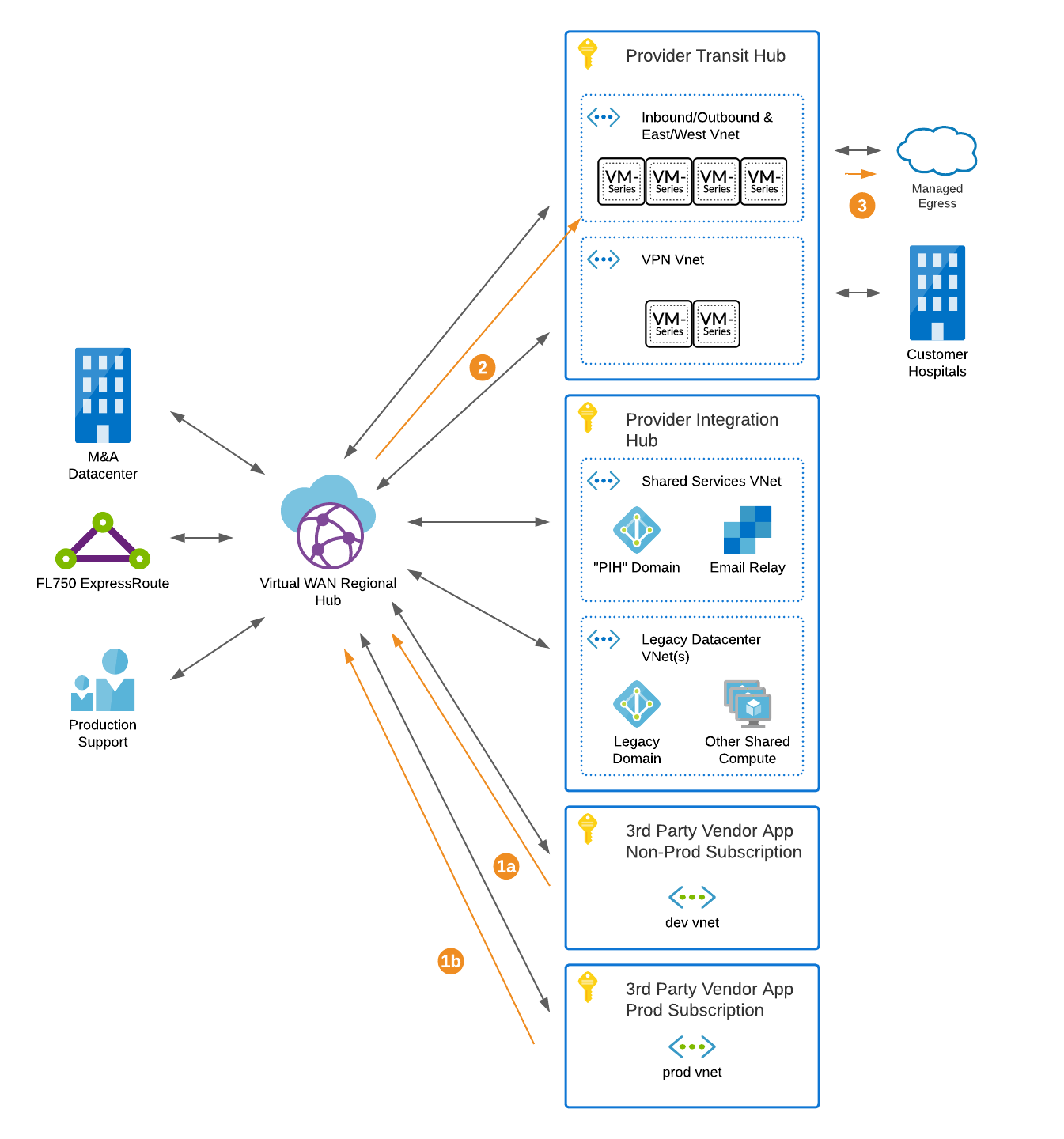


Figure : Managed Egress Routing

## Legacy Domain Controller Support

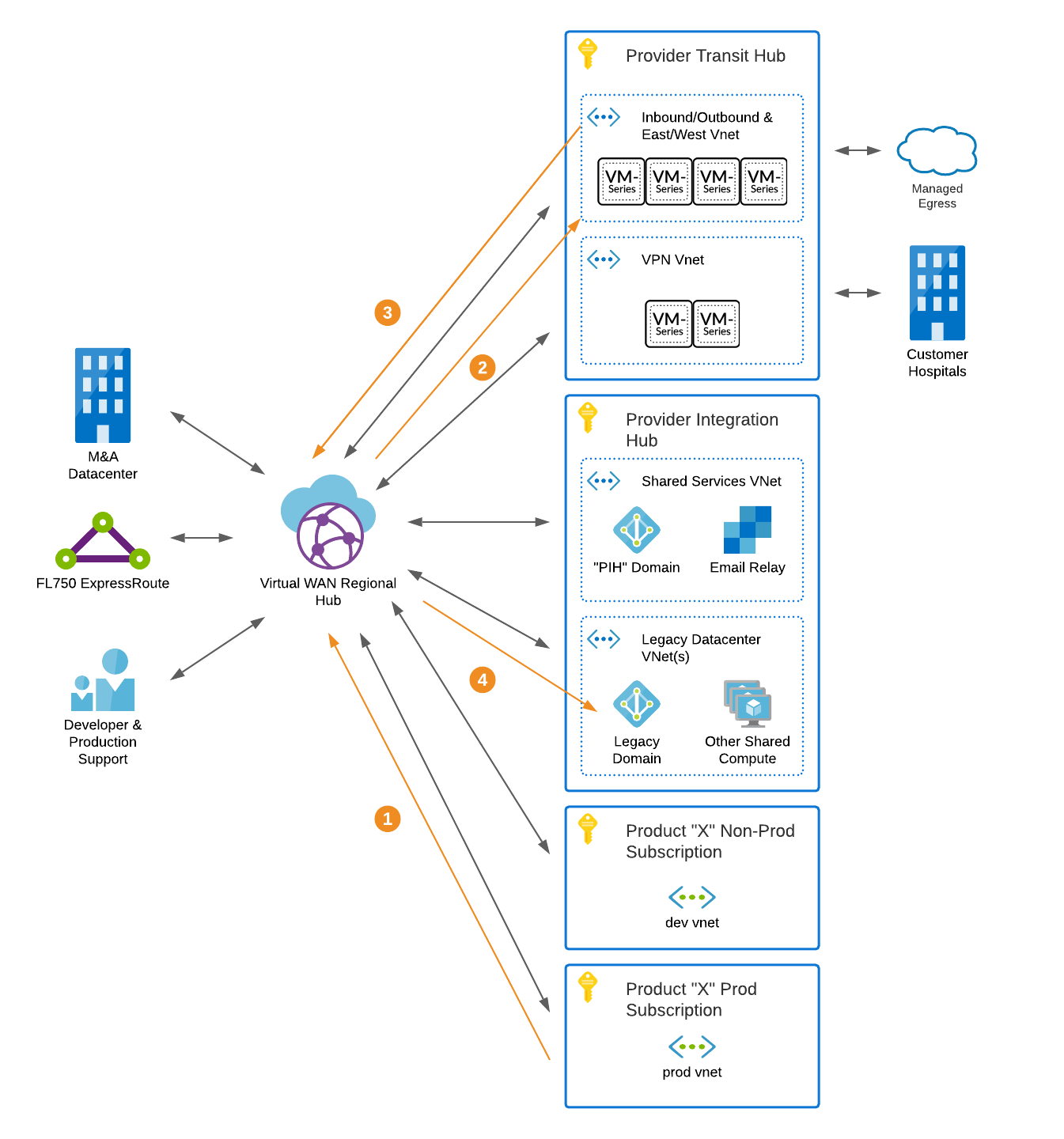


Figure : Legacy Domain Authentication Routing

## Virtual Machine Access Control (Non-Immutable Resources)

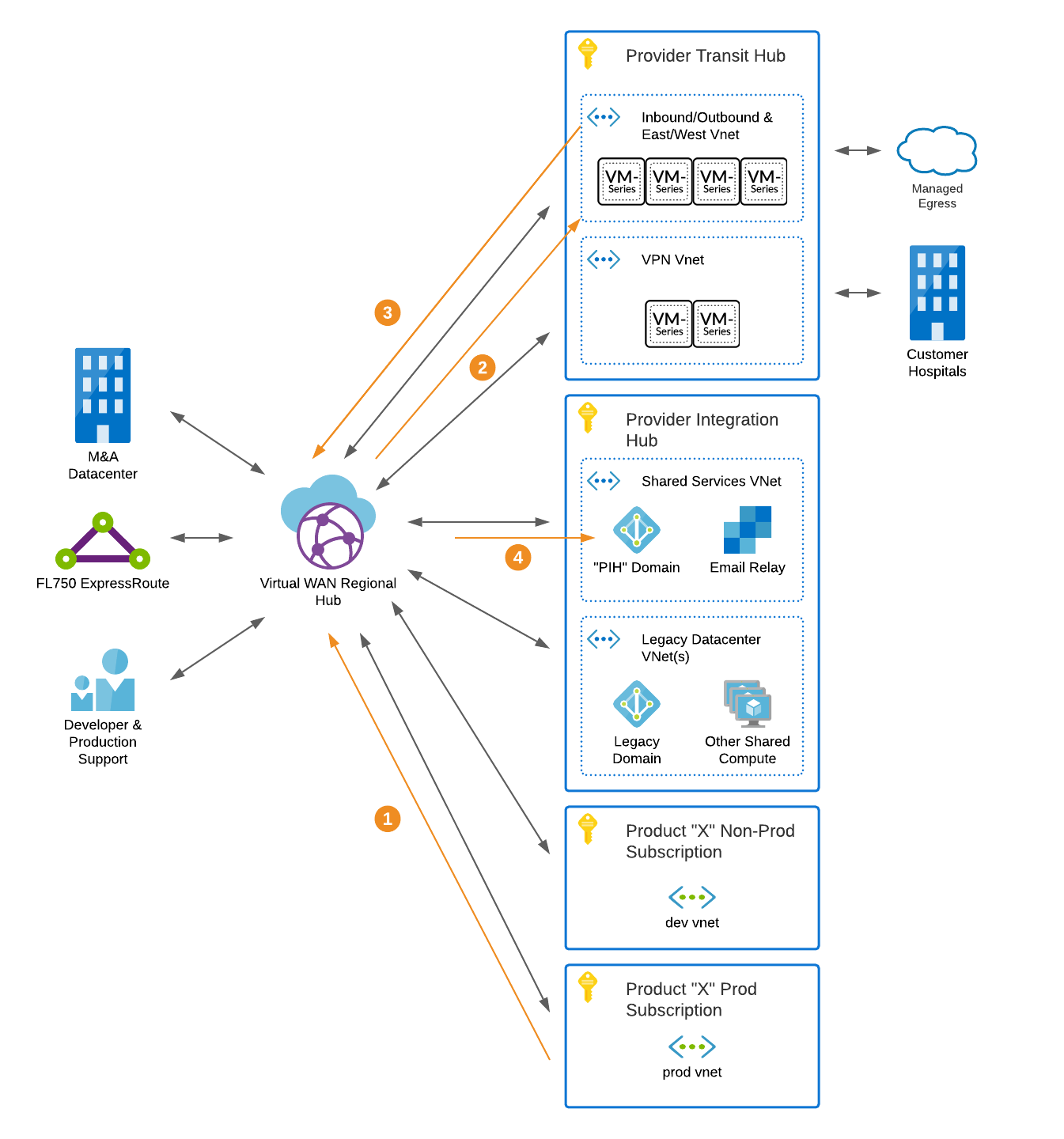


Figure : Virtual Machine Authentication Routing

## Virtual Machine Configuration (Non-Immutable Resources)

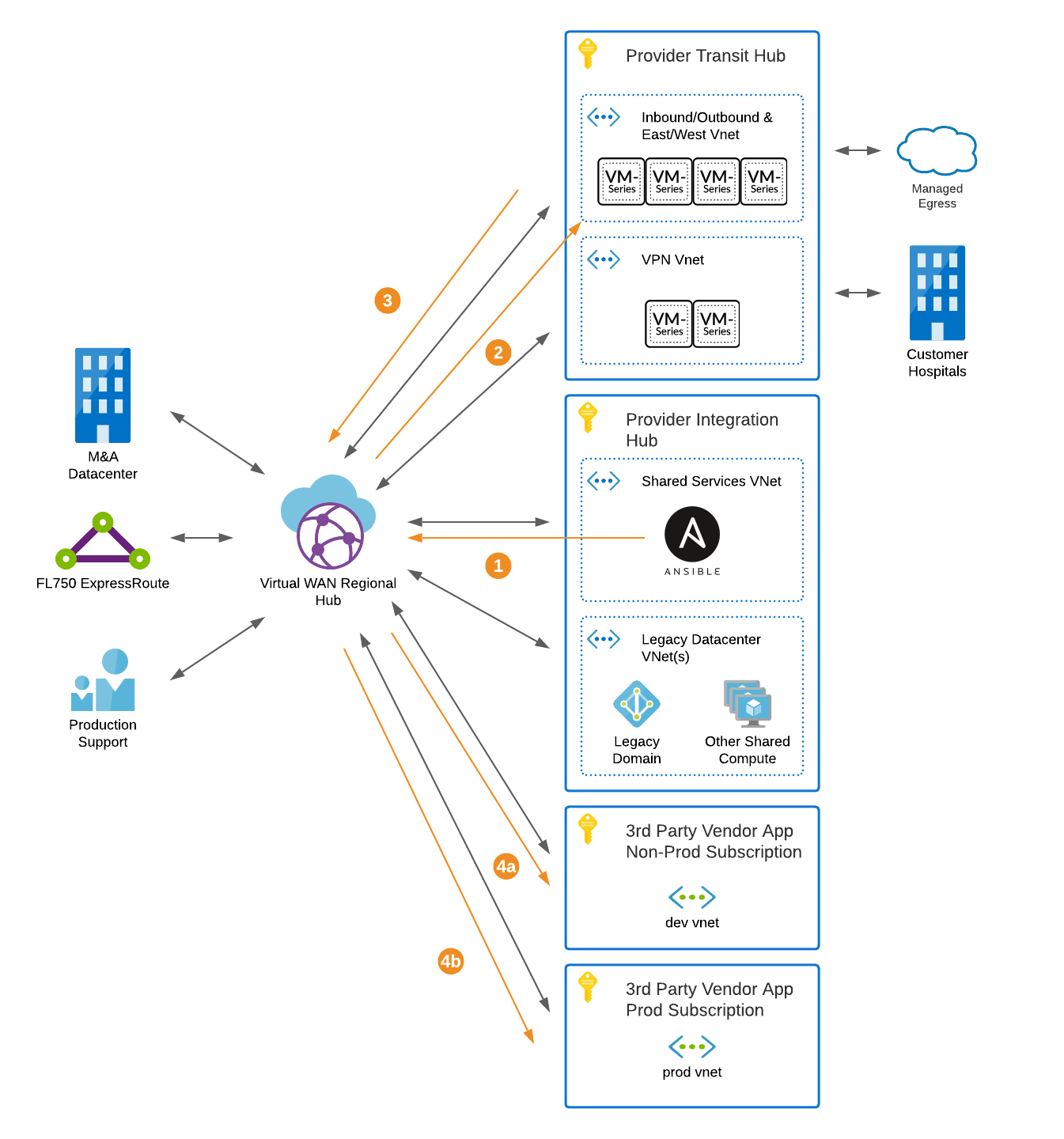


Figure : Virtual Machine Configuration Routing

# References

Microsoft. (2019, December 30). *Connect Palo Alto Networks to Azure Sentinel*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/sentinel/connect-paloalto

Microsoft. (2020, September 22). *Scenario: Route traffic through NVAs - custom (Preview)*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/virtual-wan/scenario-route-through-nvas-custom

Microsoft. (2020, September 22). *What is Azure Virtual WAN*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Microsoft Docs. (2020, July 06). *Tutorial: Detect threats out-of-the-box*. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in

Palo Alto. (2020, August 19). *Deployment Guide for Azure – Transit VNet Design Model.* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/resources/guides/azure-transit-vnet-deployment-guide

Palo Alto. (2020, August 6). *Setup Active/Passive HA on Azure*. Retrieved from Palo Alto Tech Docs: https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-azure/configure-activepassive-ha-for-vm-series-firewall-on-azure.html

VictorOps. (2020, September 27). *Azure Monitoring Integration Guide*. Retrieved from VictorOps Help: https://help.victorops.com/knowledge-base/azure-monitoring-integration-guide-victorops/