Securing the hybrid cloud network with Azure ExpressRoute

At Microsoft Core Services Engineering and Operations (CSEO, formerly Microsoft IT), we use Azure ExpressRoute to enable effective private hybrid connectivity between our cloud and on-premises networks. Azure ExpressRoute offers the reliability and low latency that our environment requires. We’re taking advantage of software-defined networking (SDN) in Azure to achieve a level of security, agility, and scalability that was difficult in our previous environment. We’ve moved from a flat, open network model to a segmented and controlled model that securely bridges the network gap between our on-premises and cloud network environments, adds end-to-end visibility for our network traffic, and gives us unprecedented control over our network and the data that flows within it. We’re now able to make changes to our network infrastructure in minutes instead of months—while meeting all our requirements for security, compliance, and reliability.

Harnessing the power of Azure and SDN

Microsoft Azure is our default platform for new applications and infrastructure. We now host over 80 percent of our infrastructure in the cloud, and that number grows every day. Although our migration to Azure has decreased our need for on-premises resources, we still require hybrid connectivity. We use Azure ExpressRoute to connect our on-premises and cloud datacenters to facilitate communication between environments, enable migration scenarios from the datacenter to the cloud, and provide connectivity across our entire infrastructure.

Connecting the datacenter to Azure with ExpressRoute

Historically, the ExpressRoute connectivity between Azure and our on-premises datacenters has been a simple conduit. As our Azure infrastructure grew larger over time, the compensating controls for network security needed to account for that growth. As attacks evolved over time and increased in their level and frequency, the controls of a traditional network struggled to keep up.

Most intranet environments operate as a relatively flat structure. Devices and infrastructure on the network are primarily protected by the security controls that provide access to the network itself. After access is granted to the network, there are fewer controls that isolate or protect devices and data within the network. Our flat network environments were more vulnerable to lateral movement between resources and network segments than we were willing to accept. Vast network capacity and limited monitoring capabilities meant that we couldn’t capture and analyze all the potential traffic in such a broad environment. Put simply, there were too many data paths and too much network noise to monitor at the level we desire.

Using ExpressRoute as a hybrid network bridge

In our first forays into Microsoft Azure, much of that legacy flat network design made its way into our cloud network infrastructure. Most of our initial Azure workloads were ported from the datacenter to Azure, so it made sense to align with the topologies of our on-premises and Azure networks to ease the transition to the cloud and enable interoperability across both networks.

ExpressRoute was used largely as a bridge between cloud and on-premises networks. Our primary focus was on how our firewalls handled traffic flowing in and out of our network; we were less focused on how traffic was treated after it went past the outer firewalls of either the cloud network or the on-premises network. This resulted in a complex and interconnected set of networks in both Azure and the on-premises network.
Identifying network shortcomings

As we migrated our infrastructure and apps to Azure, the cloud datacenter became more complex. We responded by implementing controls within Azure to manage our network environment. Because Azure networking is almost all software defined, we found new ways to manage and control our networking in Azure that couldn’t be easily done in the on-premises environment. We recognized that many problems inherent in the flat network could be solved—or at least mitigated—in Azure. The primary problem areas with on-premises networking and our initial Azure networking included:

- **The network was too flat.** Connectivity between different internal endpoints inside the on-premises network was largely uncontrolled. The general assumption for years had been: “Use firewalls and control mechanisms to keep the bad guys out while making sure the good guys on the inside aren’t too restricted.” This approach created highly secure and monitored extranet and perimeter networks intended to keep malicious users out, but it wasn’t as effective at preventing malicious actors from causing harm if they were already on the network. From a traffic control perspective, almost every device could talk to every other device on the network.

- **Identity and access controls were too broad.** We used Active Directory Domain Services (AD DS) for authentication and authorization, so our model wasn’t designed to be cloud-native. Although we used Azure Active Directory and synchronized it with AD DS, coordinating permissions throughout the hybrid network was difficult and required several transition technologies to bridge identity across both the cloud and on-premises datacenters.

- **Monitoring was difficult.** The sheer volume of traffic within the flat network model made it very difficult to accurately identify issues in a timely manner from a monitoring perspective. Typically, each portion of the network had multiple ingress and egress points, making it difficult to pinpoint traffic flow and timing.

Using ExpressRoute to secure and enable the hybrid cloud

We wanted a more comprehensive, cloud-native model for our hybrid network. We recognized the improved functionality and new features in Azure ExpressRoute as the key bridge between our cloud and on-premises datacenters, but we also recognized that we could gain greater business and technical benefit by building the solution even deeper into Azure. We wanted our solution to do several things:

- Improve our security posture and align compliance with industry standards.
- Modernize our infrastructure and migrate to the cloud.
- Enable the hybrid cloud platform for modern and secure applications.
- Implement a network segmentation strategy and remediate flat network–based firewall controls.
- Improve identity and firewall lifecycle management processes.

The CSEO ExpressRoute Secure Azure Datacenter

The CSEO ExpressRoute Secure Azure Datacenter is an internal service offering that provides a secure, software-defined, network-hosting environment for Microsoft internal datacenter workloads. CSEO leverages the security and reliability of Azure ExpressRoute and networking technology to create private connections between select Azure datacenter regions and infrastructure that’s on-premises or in a colocation environment. The CSEO ExpressRoute service securely hosts datacenter workloads and applications that can be accessed publicly in a perimeter network scenario or privately, based on the connectivity and security requirements.

This design dramatically increases the security posture in hosting these datacenter workloads, and it adds significant value to our cloud migrations scenarios. The design segments the network traffic from other non-datacenter network traffic in addition to isolating workloads within the CSEO ExpressRoute service, which allows us to easily and
confidently migrate our on-premises workloads into a secure and agile network environment. This cloud-based environment offers a significant improvement over what we can achieve with our on-premises model.

Creating complete control over the hybrid network

The CSEO ExpressRoute Secure Azure Datacenter design uses ExpressRoute as the bridge between on-premises and cloud datacenters. It also uses several other Azure components to extend security and management into the cloud datacenter, offering complete control. Network segmentation is achieved with virtual networks, network security groups, and Azure Policy. We use Desired State Configuration (DSC) and Azure Resource Manager templates to control configuration drift and enable automation. Azure Active Directory, along with on-premises Active Directory Domain Services, provides a reliable identity source for authentication and authorization. Together, these technologies help to create a secure, agile, and controlled network environment on which we run our business.

Controlling traffic flow with network segmentation

Network segmentation provides the most impactful functionality within the broader network design. We segment our network to control traffic. Segmentation creates isolated environments within which our apps and data can reside. Segmentation provides controls that enable direct control of the incoming and outgoing traffic for a segment. On our network, the goal of segmentation is to reduce the overall amount of noise and chatter on the network by limiting scope and direction of traffic to make it as intentional and direct as possible. Think of it as least-required privilege for network traffic. We have two primary categories for traffic flow: north/south (N/S), which defines traffic flowing between distinctly separate network zones; and east/west (E/W), which defines traffic flowing between applications, network nodes, or other workloads within the same network zone. We use two primary methods to segment traffic according to category: macrosegmentation for N/S traffic and microsegmentation for E/W traffic.

Controlling network flow with macrosegmentation

We use macrosegmentation to control flow between connected network environments. We implement hardware firewall devices in colocation environments, where our network service providers interface with the Azure network. Macrosegmentation helps us reduce our attack surface as it relates to a shared environment. The cloud is multitenant by nature, and our macrosegmentation strategies help to keep our data in our hands, and only our hands.

Isolating workloads and apps with microsegmentation

Microsegmentation treats each app or workload as a separate, isolatable section of the network. We use microsegmentation to govern the types of traffic that can flow in or out of a portion of the network, and to create isolation between portions of the cloud datacenter that don’t require traffic flow. The primary functional component for microsegmentation is the Network Security Group (NSG) in Azure. Using NSGs, we gain specific control over traffic in Azure. NSGs can be applied to an entire virtual network, subnets within a virtual network, a range of IP addresses, or even a single host or workload.
Managing configuration and automation with DSC and Azure Resource Manager templates

The Azure Resource Manager platform gives us greater control over, and visibility into, how infrastructure is configured in Azure. We use a virtual network provisioning package that consists of custom policies that lock and monitor network configurations state. We’re using DSC and Azure Resource Manager templates to create a tightly configured and consistent network environment in Azure.

**Desired State Configuration**

We use DSC to prevent configuration drift in our network infrastructure as well as any platform or operating system-related components that make up an app or solution. With DSC, we can set a desired state, apply it to the Azure components, and know that the critical configuration settings will always be enforced and maintained. We also use secure host control, which is implemented through Azure Resource Manager templates. DSC reach includes Azure networking components, ExpressRoute configuration, and operating system and platform settings.

**Azure Resource Manager templates**

Azure Resource Manager templates give us control over the deployment configuration and process for all our networking in Azure. When combined with DSC, our network deployment and management is achieved using standardized, repeatable infrastructure as code. By using these templates, we can specify explicit parameters for network configuration that simplify the network deployment and management process. With infrastructure as code, we know we can quickly and faithfully recreate a network environment or make subtle changes to an existing environment and redeploy it anywhere in our Azure network. It’s more agile and dependable than the on-premises
network infrastructure ever could have been, and procurement and deployment are essentially non-factors in the cloud in terms of time and cost.

**Extending identity with Azure Active Directory**

Historically, the on-premises domain structure has required a lot of maintenance and consideration in the on-premises model. Even as we transitioned to Azure early on, our Windows-based AD DS domains provided the core of our authorization and authentication functionality. Large-scale federation and several functional workarounds were necessary to bridge the AD DS environment to the cloud; it was designed for the on-premises datacenter, not Azure.

With Azure Active Directory (Azure AD), we’re establishing a versatile authentication and authorization solution that bridges our entire infrastructure. We can use our on-premises directory data and format but still enable our identity solution to be cloud-native. Because it’s cloud-based, it’s available from anywhere with built-in security controls we expect in a cloud-based solution. With Azure AD, we have identity-based authorization controls that can be exposed per network zone. We don’t have to spend the time creating workarounds and custom solutions in Azure to fully enable our users in the cloud.

**Benefits**

We’ve identified several significant benefits from implementing the Azure ExpressRoute secure datacenter design, including:

- **A more agile and effective network infrastructure.** Our network can adapt to change as quickly as the change occurs. With SDN, we can quickly and effectively deploy, redeploy, and configure any portion of our network. Because of the self-service nature of our ExpressRoute design, users can quickly get their environments up and running.

- **Better monitoring and network control.** With segmentation in place, traffic flow is greatly decreased throughout the environment and only traffic that’s required flows between separate points on the network.

- **Reduced threat vector.** Due to the decreased data flow and general access, our surface area for attack is greatly reduced. Segmentation limits inbound and outbound traffic, and identity controls ensure that only authorized access is permitted anywhere on the network.

- **Simplified cloud migration scenarios.** We found that our business groups were much more interested in migrating their workloads to the cloud when we told them we could place them in a secure and segmented network environment while still maintaining the connectivity they needed across the hybrid network. Having a hybrid robust network in place means we can immediately start taking advantage of the scalability, agility, and reliability of public cloud computing.

**Lessons Learned**

- **Get your whole organization onboard.** We found that a move to this level of network change—while not very disruptive—involves the entire organization and has broad-reaching impact. The benefits of implementing our solution have reached every part of our organization, and we realized those benefits more quickly and to a greater extent because our management understood the need and the value.

- **Gather all requirements and processes for the design.** Because a solution like ours is so far-reaching, we needed to get our teams together to understand design and process requirements from an organizational perspective. Planning up front saved us a lot of time later on. We made sure that we carried out due diligence and got our teams talking to each other and looking at how the new solution could affect our overall network design, functionality, security, and compliance.

- **Put a cloud migration plan in place.** We put our solution in place to better enable migration to the cloud, so we made sure that our migration plan was ready to take advantage of the benefits provided by ExpressRoute and SDN. We were ready from a migration perspective, so we immediately gained benefit from the solution and migration to the cloud in general.
Looking forward

We’re already looking at how we can improve and further take advantage of our hybrid datacenter environment. The segmented model we’ve created using ExpressRoute and SDN provides a whole new perspective on networking for our IT organization. We can quickly create and change large sections of network infrastructure, and we’re using that to build test and development environments and to refine our network. We’re using our new network model to build more internet-native accessibility for our applications and extend our network to be closer to our users and customers. We’ll be building more automation and self-service options into our environment in the near future—and we’re always looking for ways to take advantage of the security, agility, and reliability that ExpressRoute and SDN in Azure provide.

Next steps

For more information about ExpressRoute pricing and features, or to sign up for a free trial of Azure today, go to Azure Express Route at Azure.com.

For more information

Microsoft IT Showcase

microsoft.com/itsshowcase

Designing a software-defined strategy for securing the Microsoft network

Microsoft Azure Virtual Datacenter: A Network Perspective

How Microsoft manages a hybrid infrastructure with Azure

Automating cloud infrastructure management with Azure Resource Manager

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.