aviatrix

White Paper

Microsoft Active Directory in the Cloud.

Technical Whitepaper

Introduction

Enterprise networking has traditionally centered around data center connectivity. The connectivity model was based on the delivery of applications and data located in the data centre to the campus sites and remote sites. Legacy networking architecture confined the connectivity, security infrastructure and application delivery locally in the remote sites linking back to the data center with a direct inbound private link. This architecture was optimal when majority of the application workloads and the data is served from the data center. However, with the accelerated adoption of public cloud infrastructures like Amazon AWS, Microsoft Azure and Google Cloud platform, traditional networking architecture results in sub-optimal traffic flow resulting in degraded application performance, security concerns and in-ordinate network provisioning and management time.

The traditional model served its purpose for some time, but new application and connectivity requirements trigger a new approach to service consumption.

Hybrid Cloud & Challenges

The **digital transformation** of application workloads puts pressure on Enterprise IT to adopt and deploy better cloud connectivity. Public cloud network architecture is based on newer connectivity constructs but the Internet that connects the clouds was formed with old protocols; never built with performance and security in mind. Cloud connectivity left to the **defaults of the Internet leads** to degradation of application performance and user experience.

The new model requires a change to the business critical app and data deployment and management. It moves from an internal data centre approach to a hybrid cloud-centric approach. Application performance is improved as services are strategically placed in remote cloud locations nearer to the originator.

However, moving business-critical applications and data to a public cloud opens doors of interesting network and security problems. The parameters have changed; news security and connectivity challenges must be addressed. Services such as Microsoft Active Directory (AD) have strict performance metrics to adhere too. As soon as these services are pushed to the cloud, one should consider migration paths, latency, security and synchronization modes. For Active Directory authentication and replication services to pass efficiently over the Internet new mechanisms must be in place to optimize network path selection and session consolidation.

Active Directory to the Cloud

Active Directory is a critical network infrastructure component for window-server based application workloads.

As 80% of workloads are Windows-server based, it's a critical cloud component for efficient and authenticated workload delivery.

Migrating on-premise applications or deploying new cloud-based applications require local Active Directory service for fast and reliable system response. Applications require consistent connectivity to Active Directory for authentication and identity management.

Active Directory Options

When pursuing Active Directory in the cloud, there are some options to consider:

1. Identity management for new applications supported by Windows Azure Active Directory.
2. Identity management for existing on-premise applications supported by Windows Server Active Directory on Azure Virtual Machine (VM).

Microsoft Azure Active Directory

The Microsoft Azure Active Directory offers cloud-based authentication, for example, Office 365, Single Sign On (SSO) and other 3rd party entities such as Salesforce. It is primarily used for "Cloud-first" applications.

Azure Active Directory is a REST based service managed by Azure teams. The deployment model based on specific regions lacks the flexibility to connect clients to their nearest Azure region. Independent to client location the design does not allow customers to choose regions for their AD service to live.

The Azure AD can be integrated with existing on-premise Windows Server Active Directory infrastructure via:

1. Directory Synchronization.
2. Active Directory Federation Services (ADFS).

Active Directory Synchronization

Active Directory Sync is an easy, low-cost first step to cloud AD. The on-premise Domain Controller synchronizes with the Azure AD solution. An agent called Microsoft Identity Manager (MIM) is installed on premise that replicates directory objects to Azure.
It has a filter feature enabling the filtering of objects such as Distribution Groups (DG) so replication items are always optimized. Password write back allows password resets from Azure AD; vital for the travelling worker.

Active Directory Federation Service

If you don't want to sync to Azure AD you could opt for Active Directory Federation Service (AD FS). It operates a Redirect mode that redirects requests from the cloud Active Directory service back

to the on-premise location. As a result, requires an on-premise demilitarized zone (DMZ) presence.

Active Directory on an Azure VM

This option provides a full instance of Windows Server Active Directory Windows Server 2008 R2 SP1 or Windows Server 2012 on a VM. A fully-fledged Domain Controller is placed in Azure along with full replication service extension between on-premise and chosen Azure region.

The new VM is configured as a Replica Domain Controller within the existing Windows Server Active Directory hosted on-premise. The two DCs -- VM in the cloud and on-premise, become peer DC's replicating changes back and forth. A new site is created in the cloud acting as the replication boundary of the directory to control things such as bandwidth and security functions.

The solution offers full flexibility for Active Directory placement as you are no longer tied down to specific Azure regions. This type of extension has strict performance requirements, typically implemented with Express Route. Efficient network connectivity is essential for smooth operations.

Cloud Connectivity Challenges for Microsoft AD

Global changes to the Internet's underlying fabric is not happening anytime soon. As a result, we need to look at the edge of the network to optimize cloud connectivity to improve critical application performance.

First, let's address key network challenges that compel network administrators to re-design the enterprise network:

Distance / latency

It takes 100 milliseconds (msec) for light to travel the world so why does it take two endpoints close to each other over 100ms or even minutes? These boils down to latency. Latency is added due to the processing times occurred on hops in the packet path.

Physical proximity is the primary factor contributing to latency. The further the requested service the more hops and higher latency. Our hands are tied unless we find ways to change the speed of light or move services closer together.

TCP and BGP behavior

Transmission Control Protocol (TCP) starts a connection as if there is no packet loss, jitter or delay and works back from there.

However, the internet is bundled with asymmetric links and various performance challenges. As a result, TCP should start assuming a world of poor performance metrics as this would more accurately reflect today's application environment. Also, TCP needs to pass some stages before data is sent and its inbuilt congestion mechanisms are not performance optimized.

Border Gateway Protocol (BGP), the protocol that connects islands on the Internet does not by default take performance metrics into account. BGP paths are chosen based on AS (Autonomous Systems) hop count which may lead to suboptimal path selection with high latency and packet loss. Also, BGP route convergence delays will affect application performance.

These are just some of the problems that lag application performance. However, there is also problems with security. Internet Protocol (IP) has no built-in security and does not validate sources

forcing administrators to look at different ways to protect data transmission.

The Internet's complications require the introduction of new techniques to fully optimize cloud connectivity.

Challenges to AD in the Cloud

There are a number of challenges to Cloud Active Directory:

1. Authentication Timeouts.
2. Scalability concerns.
3. Security.

Authentication timeouts

Latency is the main pain point and there is not much we can do about it except shortening the distance.

The time incurred from high latency affects Active Directory authentications times and degrades the user experience. Latency not only degrades the user experience but on occasion may cause complete application outage. If you don't authenticate within a specified period, there will be application timeouts.

Content Delivery Networks (CDN) distributed PoPs are perfect for caching static content but critical services like Active Directory require a purpose-built end to end network and security solution.

Scalability

Morning rush events instantiate periods of high utilization requiring Active Directory and its connectivity to scale. A morning rush involves hundreds of thousands of authentications requests; all at the same time. There are no guaranteed route requests will take,

some on low latency paths while others on high. The connections to Active Directory must be optimized, so these responses are answered quickly to mitigate login issues.

Security

When you pass AD credentials to Azure, there could be a segment in the network where it goes as a clear text when the handshake happens at the beginning. Aviatrix overcomes all these challenges with intelligent tunnel optimizations based on well-known security standards.

Aviatrix to the Rescue

This is where Aviatrix comes in with its magic formulas!

Introducing Aviatrix

Aviatrix offers a software only hybrid network solution designed to overcome the challenges of cloud connectivity. We can't change the underlying fabric or the speed of light but we can do smarter things at the data center and large sites to overcome the limitations of hybrid cloud connectivity.

Aviatrix offers a transport agnostic overlay for cloud connectivity with techniques guaranteed to secure transmissions and pin traffic to the most optimized path. It beats the latency problem and secures all data transmission between two endpoints. Making sure services, such as Microsoft Active Directory operate reliably and serve requests on time.

When placing critical services on the cloud that has strict performance metrics, you cannot rely on Internet defaults.

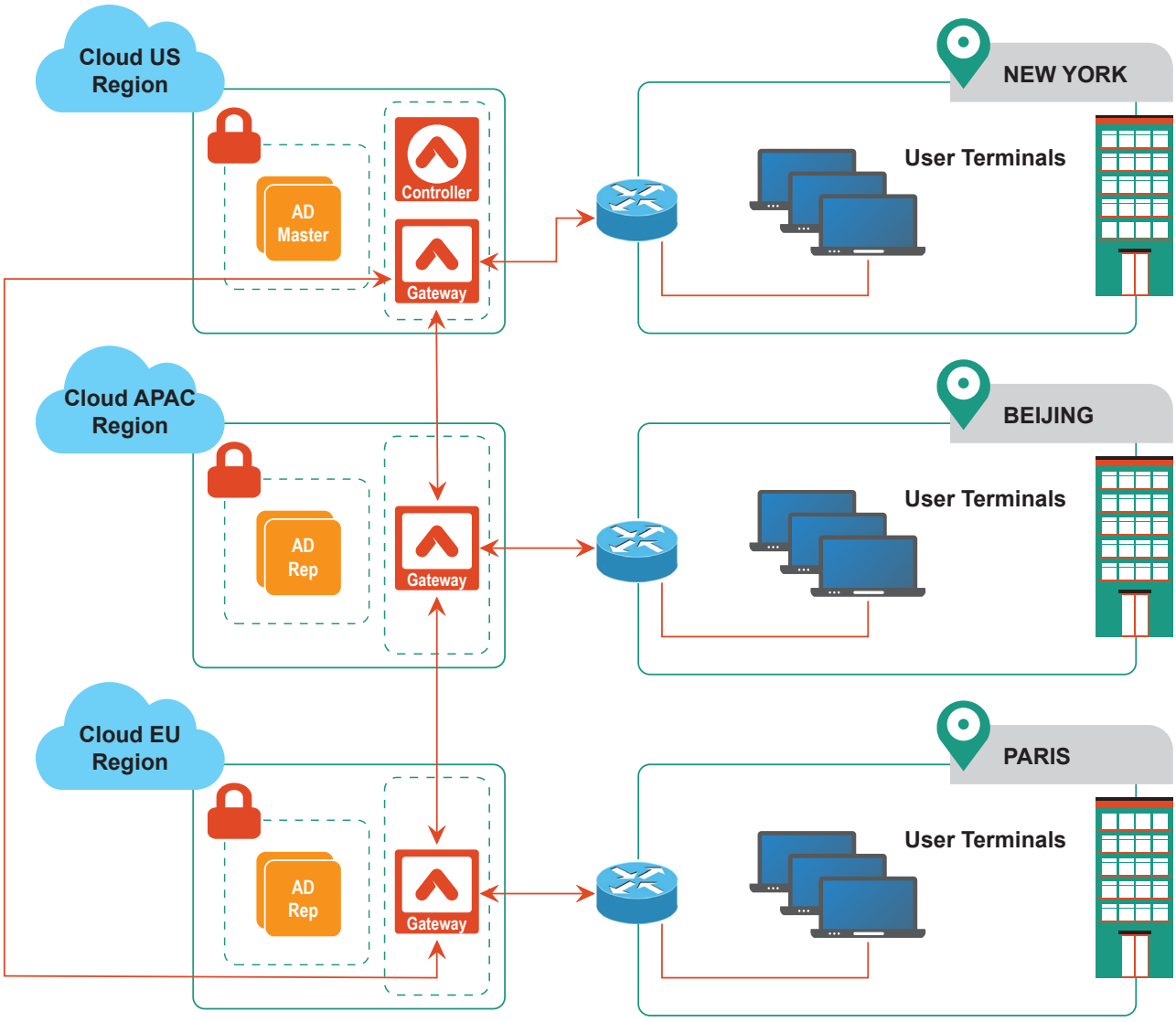

Figure: Active Directory Deployment in the Cloud with Aviatrix

First and foremost, Aviatrix offers a secure solution with encryption services on top of any transport. All system services are encrypted both for the handshake and the payload. Each packet is entirely encrypted. Not a single packet goes in clear text.

The Aviatrix overlay is a static based tunnel. Nothing is on demand, so there is no time loss with unnecessary teardown and rebuilding of the overlay. Operationally it's easy to manage and support. It's a well-known IPSEC tunnel with no managerial complexity or complex Dynamic VPN configurations.

Magic Formulas

The Aviatrix solution consists of a number of **magic formulas**.

Instead of sending hundreds of thousands of sessions over WAN links, all sessions are consolidated into a single IPSEC overlay pinned to a low latency path. The best paths are selected based on Azure latency tools; packets are always placed on optimal links.

You cannot replicate AD into every region, so the Aviatrix controllers designate the nearest Azure region for AD services. Instead of relaying all connections back and forth, Aviatrix chooses the closest Azure region; connections are never forwarded to a suboptimal Azure location. The reduction of distance reduces the latency. As a result, authentication requests that used to take minutes now takes millisecond (ms).

It's a software-only solution, so there is no need to provision physical edge devices and have spares in stock just in case. Seamless

implementation is rare these days but Aviatrix can be running in less than 10 minutes. This type of agility is second to none and not many can compete.

A call to security folks!

The cloud spreads the security paradigm to a multi-tenant 3rd party platform. No one can doubt the cloud draws sensitive questions on network entry and security. Active Directory (AD) is part of the **forest's infrastructure**, as a result, contains sensitive employee information. Understandably, many are still unconceived to move this critical service to the cloud.

However, are the obstacles to migration formulated via old cultures? If it's not locked on-premise, then it must be insecure, right? Microsoft and Amazon spend billions every year on security. Many companies with on-premise services may not even have dedicated security professional managing their security infrastructure.

Old physical on-premise security appliances may have old IOS, obsolete rules/policies, only stuck in the middle of the network feared to be touched and upgraded. These devices are known as **holy cows**. Are they more secure than a well-managed cloud infrastructure? There is no quick answer, but the recommended approach is to first look at what is already out there on the cloud? Governments and other big company names.

Microsoft has security blueprints for each Azure location. We propose to examine the security blueprint for the chosen location to consider if it's meet your security requirements. Think of it as your personal data centre and run it through existing security checks.

About Aviatrix

Aviatrix is a Cloud Native Networking startup that simplifies scaling in the cloud, enables connectivity across a wide range of cloud architectures, and delivers end to end network security. Our solution is built from the ground up for AWS, Azure, and Google based on software defined architecture that enables enterprises to realize the benefits of agility, scale and mobility from deploying applications in the cloud. To learn more about Aviatrix solutions, please visit the website, call +1.844.262.3100, follow us on Twitter, or connect with us on LinkedIn.