aviatrix_docs Documentation

Release

Mark Ennamorato

Oct 10, 2017

Getting Started

All Aviatrix documentation can be found here. If you can't find it here, please leave us a note via our GitHub page. Please also visit our main website for more information regarding use cases and upcoming events.

While all content is searchable, the site is organized into the following sections:

CHAPTER 1

Site2Cloud between Azure VPN Gateway and Aviatrix Gateway

This guide helps you to configure Site2Cloud IPSEC tunnels between an Aviatrix gateway and an Azure "Virtual network gateway"

Configuration Workflow

Before you start make sure you have the latest software by checking the Dashboard. If an alert message displays, click Upgrade to download the latest software.

The Site2Cloud on CloudN configuration workflow is very simple.

1. At Aviatrix Controller, go to "Gateway" page to create one non-vpn gateway.
2. At Azure portal, go to "Virtual network gateways" page. Fill in the following information to create a new virtual network gateway:
    - Name: Enter an Azure VPN gateway name (e.g. Azure-VPN-GW)
    - Gateway type: VPN
    - VPN type: Policy-based
    - SKU: Basic
    - Location: Select a desired location
    - Virtual network: Select a desired VNet
3. Once the virtual network gateway is provisioned, record its public IP address
4. At Aviatrix Controller, go to "Site2Cloud" page. Fill in the following information to create a site2cloud connection:
    - VPC ID/VNet Name: Select the VPC/VNet where your Aviatrix gateway is created at Step 1
    - Connection Type: Unmapped
    - Connection Name: Enter a site2cloud connection name

- Remote Gateway Type: Select "Azure VPN"
- Algorithms: Uncheck this box
- Encryption over ExpressRoute/DirectConnect: Uncheck this box
- Enabled HA: Uncheck this box
- Primary Cloud Gateway: Select the gateway created at Step 1
- Remote Gateway IP Address: Enter the public IP of your virutal network gateway (collected at Step 3)
- Pre-shared Key: Enter your own pre-share key or leave it blank so that Controller will generate one
- Remote Subnet: Enter the CIDR of the VNet, in which your virtual network gateway is created at Step 2
- Local Subnet: Enter the CIDR of the VPC/VNet, in which your Aviatrix gateway is created at Step 1

5. Once the site2cloud connection is created, select the same connection at "Site2Cloud" page. Select the following values for each specific field and click "Download Configuration" button.
   - Vendor: Generic
   - Platform: Generic
   - Software: Vendor Independent
6. Collect the following information from the downloaded configuration template:
   - Pre-Shared Key from "#1: Internet Key Exchange Configuration"
   - Aviatrix Gateway Public IP from "#3: Tunnel Interface Configuration"
   - Cloud Network(s) from "Subnets" section of "#3: Tunnel Interface Configuration"
7. At Azure portal, go to "Local network gateways" page. Enter the following information to create a local network gateway:
   - Name: Enter a local gateway name (e.g. AVX-GW)
   - IP address: Enter the Aviatrix gateway's public IP collected at Step 6
   - Address space: Enter "Cloud Network" CIDR collected at Step 6
   - Configure BGP settings: uncheck
8. At Azure portal, go to "Virtual network gateways" page and select the gateway created at Step 2
9. Select "Connections" from "Settings". Enter the following information to create a connection:
   - Name: Enter a VPN connection name (e.g. Azure-AVX-S2C)
   - Connection type: Select "Site-to-site (IPsec)"
   - Virtual network gateway: Select the VPN gateway created at Step 2
   - Local network gateway: Select the local gateway created at Step 7
   - Shared key (PSK): Enter the pre-shared key collected at Step 6
10. Send some interesting traffic between Aviatrix gateway's VPC/VNet and Azure VPN gateway's VNet to bring up the site2cloud connection

Troubleshooting

To check a tunnel state, go to Site2Cloud, the tunnel status will be displayed in a pop up window.

To troubleshoot a tunnel state, go to Site2Cloud -> Diagnostics.

CHAPTER 2

Aviatrix VPN Client Changelog

1.4 - August 8 2017

- Signed Mac application
- Parallel windows execution fix

1.3 - June 15 2017

- Disconnection fixes
- Timeout fixes
- Connection profile is diplayed
- IE support for SAML
- Signed Windows application

1.2 - Mar 15 2017

- HTTPS Version for SAML
- Multiple Profiles
- Linux version
- Connection status detection
- Unblock disconnection while connecting
- Retry prompt for LDAP
- Multi process feature for Mac/Linux.
- Removed VPN Lockdown
- Permissions fixes
- Fixes in logging

1.1 - Jan 30 2017

- Settings window for troubleshooting

- Mac default application behavior
- Bug fixes for hangs
- In built resources
- Connection timeout issues fixed
- Kill other OpenVPN on start
- Connection status fix
- VPN lockdown feature

1.0 - Dec 15 2016

- Initial release
- HTTP Version

CHAPTER 3

DATADOG Datadog Integration

Summary

The Datadog integration sends system metrics from Aviatrix Gateways and the Controller to your Datadog instance.

Once enabled, all existing and new Gateways will send system metrics via an installed Datadog agent to the configured Datadog instance.

Prerequisites

In order to complete the steps in this guide, you'll need:

- An Aviatrix license key

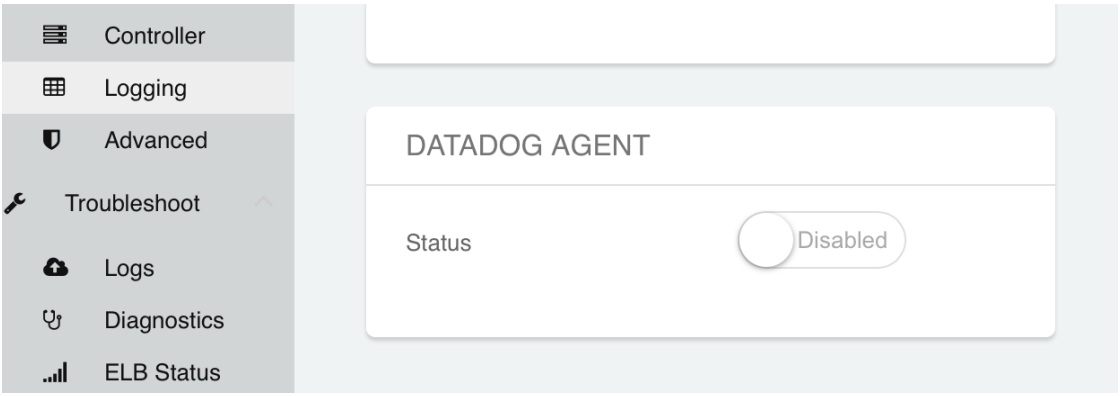
Tip: email info@aviatrix.com if you don't have a license key

- A Datadog account and API Key

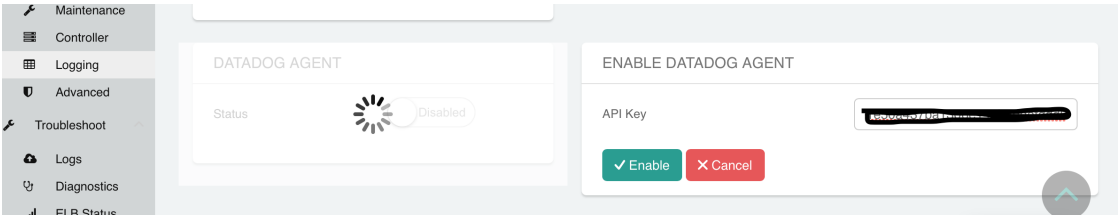
Tip: Sign up for a Datadog account here. Once you have an account, you can create a new *API Key* from the Integrations~APIs menu.

Enable/Disable Integration

Login to the Aviatrix Controller. Go to the *Settings* in the navigation bar and click on *Logging*. At the bottom of the page, find *Datadog Agent*:



Change the status to *Enabled* and enter your Datadog *API Key* and finally click *Enable*.



What Data Is Collected

Once enabled, the Controller will install and configure the Datadog agent on each of your Gateways and on the Controller automatically.

Host Name

Metrics from Aviatrix Gateways will have a host name in this format

```
aviatrix-gw-<Gateway Name>
```

The Aviatrix Controller will appear as:

```
aviatrix-ucc-<Controller Public IP Address>
```

CHAPTER 4

Enterprise Cloud Adoption Journey: Technical Challenges

Technical Whitepaper

Last updated: May 11, 2017

Introduction

The enterprise journey to cloud adoption can be driven by two different types of incentives. The business drives one type, building new, transformative capabilities. Here the cloud is an enabler that did not exist in the past. The other type is focused on optimizing the legacy data center environments within IT to contain evolving pressures. These two types are usually happening in parallel. In all cases, cloud adoption is accelerating, and along with it an increasing number of challenges.

Competitive pressures on businesses to move more quickly and be more agile, are forcing decisions on where to deploy new applications. The public cloud is a resource for creating new disruptive applications that would be difficult if not impossible to implement in other means. It provides competitive leverage to not only new businesses but existing enterprises.

Additionally, massive application workloads like Enterprise Resource Planning applications (ERP), large custom applications, high performance computing applications and backup and disaster recovery applications are migrating to the public cloud out of necessity to mitigate the constant strain to keep costs under control over time.

Most enterprises are stepping into the cloud with a hybrid approach. Aviatrix for Hybrid Cloud enables enterprises to design, configure and operate secure and scalable hybrid cloud networks to migrate, access and run applications in the public cloud.

Business Drivers to Migrate to the Hybrid Cloud

This is a typical list of CIO and enterprise motives that drive the move of enterprise applications to the cloud.

New transformative business models

- pay-as-you-go flexibility to expand / reduce IT footprint as needed
- untested workloads, “fail-fast, fail-cheap” POC’s
- apps with cloud native architecture, rapid flex-up and scale-out

Disaster recovery and high availability

- geo-dispersed sites
- system redundancy
- significantly easier and automated periodic testing

Cost savings

- especially storage costs and high-performance computing
- limited IT staff and resource growth
- temporary scale up **and** scale down in capacity demands

International expansion and collaboration

- M&A activities resulting in geographically dispersed disparate systems
- expansion into new global markets

Compelling events

- expiring data center equipment support
- expiring data center leases

Compliance

- requirements for local data hosting in the region being served vs centralized

Use Cases

The following use cases represent examples of the above scenarios.

Use Case #1: Home grown (legacy) applications

HR departments may have large workloads: recruitment management, relocation, benefits administration, human capital management, finance and accounting, SCM/procurement, expense reporting, time management, etc. These applications may be used sporadically and have low performance requirements, making them an ideal choice to offload from on-premises and into the cloud.

Other legacy applications used by finance/legal departments may be used infrequently and have low performance needs, as well as legacy custom stubs for SSO or employee VPN access all would benefit by moving to the cloud.

Offloading these applications means that IT can reallocate this hardware to applications that require more steady computing power, or decommission the hardware altogether. Either scenario means time and efficiency gains for the IT department, without any noticeable change in performance from end users.

Use Case #2: Disaster recovery and high availability

Instances in the cloud are not much different than instances in the data center in terms of failure possibilities. This includes server/service/VM failures and reboots, zone failures, and multi-zone cloud failures. To achieve multiple 9s of availability, processes need to be in place for these types of failure mechanisms, including the need to automate everything and do on-going assurance testing on a regular basis.

Cloud customers can use hybrid clouds to promote both DR and HA, oftentimes extending DR protection to important, yet previously unprotected systems.

Use Case #3: Big data, storage and backup/archiving

Enterprises have accumulated huge volumes of data, stored in databases, which power the applications that their end users and customers rely on every day. These applications often involve many VMs as part of their architecture, and their databases often hold terabytes worth of data, even though much of that data lays "at rest" for large portions of the time.

There are two major benefits to getting these applications and their datasets into the cloud. First, a greatly reduced on-premises hardware footprint by reducing both servers and storage. Second, these applications can now benefit from the elasticity of the cloud, by easily adding more compute (for the application) or storage (for the databases) whenever needed.

Use Case #4: DevOps/QA/Test

Developers need an agile, flexible, dynamic environment for developing and testing software applications. Moving CI/CD applications for development and testing to the cloud has clear benefits, including cost savings and increased time-to-market. These applications are lower-risk, lower performance, mostly self-contained with no dependencies, and good "phase 1" candidates for migration.

Use Case #5: International expansion

Businesses that expand internationally may need applications and data to be closer to the new locations. This could be due to localization requirements, minimizing latencies to apps/data, or compliance reasons. A new acquisition or merger could result in almost instantly geographically dispersed public clouds that now need to be peered or connected back to other data centers.

Technical Challenges

The technical requirements and challenges enterprises face during this journey to the cloud are multi-faceted. Enterprise applications represent a significant on premise investment with critical value, and years of development. Even with a "lift and shift" methodology, organizations may struggle with inherent interdependencies to move them, along with the data, to the public cloud. One of the CIO's highest priorities must be to minimize risk when the move is made as these applications usually are mission critical.

Latency

The demands on performance and user experiences with cloud based applications can sometimes be subpar, resulting in not only user frustrations but real business financial impacts.

The roles of both the Internet and cloud computing complicate latency, with networks broken down into hundreds of components, and layers of virtualization and virtualized network infrastructure. Bringing the applications closer to the end-user is oftentimes the most viable and flexible solution to reduce latencies, since there are few restrictions on physical location that exist with custom engineered direct connections.

Security

Enterprises must minimize risk migrating applications to the cloud. Cloud computing and security go hand in hand. Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target.

Network security groups allow organizations to shield parts of their public cloud from direct outside access – like a firewall. Hybrid and multicloud environments present new cloud security challenges and risks as data moves between on premises and the cloud. If custom Internet-bypassing connections are used, no native end-to-end encryption is provided.

Agile role-based secure access

As enterprises move applications to the public cloud, the users and organizations owning the applications now have interconnects to the public cloud that did not exist previously. These interconnects must be secure. Companies have a need to authenticate and enable their mobile employees to securely access the companies evolving network via the Internet with a secure VPN solution. This solution must be easily deployed, managed, highly scalable, and agile to meet the constantly evolving network topologies caused by migrating applications.

Multi-vendor cloud providers

To enable geographically dispersed data redundancy, and other types of redundancy, or to support unique workloads, it is common to buy cloud services from more than one vendor. While each has its own uniqueness and strengths, the IT organization wants to minimize operational complexities and create inter-cloud connections that are visible, manageable, robust, scalable, and easy to deploy.

Enterprises need to plan ahead by assuming hybrid IT will be the future and take steps accordingly. Hybrid management systems, integration, workload portability, automation and skills using various public cloud platforms are all important investments to make early in the cloud deployment process.

Custom network configurations

Creating and securely connecting the on-premise datacenter to the cloud resources is often slow and manual. Seamless extension of the private IP address space into the public cloud such that resources in the public cloud are easily accessible, reducing the attack surface, reducing issues with overlapping IP address space is a key challenge facing network engineers.

Large data center and cloud environments have complex network configurations and settings to satisfy regulatory and internal policies. Matching the workload compute and storage requirements to the cloud services is not the total solution – mapping of the existing network environment to the cloud network can be very daunting and error prone. Enterprise workloads may need to be configured for specific sub-networks, VLANs and use of specific IP address ranges as well as physical IP address.

It can take weeks to provision secure connectivity, involving complex router configurations managed by network experts and expensive installations. Aviatrix hybrid cloud networking provides a one-click software-only model to set up encrypted connections to public clouds in minutes, with the ability to extend the private IP network to public clouds.

Throughput/Performance

Cloud performance depends on network performance. While cloud providers like to talk about the latest software offerings, the speed and capacity of the cloud provider's network will usually be a determining factor for the viability of any cloud-based software application. The key measure of network performance is throughput – sometimes called bandwidth.

What is critical for networks in cloud computing is not only achievable performance, but consistency of performance, which is important when sending large amounts of data between servers. One of the latest trends is buying network capacity on an incremental basis, just like any other cloud resource. Other cloud provider direct connect solutions also add bandwidth improvements for transferring large amounts of data when more capacity is needed. However, these solutions do not provide native end-to-end security.

Summary

The enterprise cloud adoption journey is just that – a journey. New technical solutions are appearing at an ever-increasing rate, as well as new challenges they bring. A well thought out migration plan that includes all the aspects of vendor features, performance, security and networking is required.

Aviatrix provides an innovative Cloud Networking software solution that simplifies connectivity to the cloud in a secure and scalable way. At Aviatrix, we believe that networking is a foundational element of cloud computing and, should be as dynamic, scalable, and elastic as compute and storage.

Aviatrix for Hybrid Cloud eliminates the complexity of connecting to and across public clouds with a simple mesh architecture, and is fully integrated with Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform.