

In the Cloud, No One Can Hear you Scream

Dangerous Cloud Defaults in Azure.

Garth Boyd
OWASP Ottawa
February 2023

Who is this Guy?

- Erstwhile Engineer (B.Eng. Electrical/Computer Systems 1987)
- Blue Team: MMHS, Key Management, PKI, Threat Modeling
- Red Team: Pentest
- Web/Cloud Application Security Architecture
- DevSec*.*
- OWASP Ottawa Chapter Leader/Volunteer
- Creator of Devious Plan



Agenda

- Disclaimer
- Azure Functions
- Azure Functions and the 1990s
- Azure Storage Accounts
- Azure Key Vaults
- Azure Event Hub
- Azure Managed SQL
- Azure VMs
- Azure Data Factory
- Azure Cosmos DB

Disclaimer

- The cloud is *always* changing
- Every attempt has been made at the accuracy of the information presented in this slide deck at the time the slide deck was created
- For those seeing this deck, or presentation at a later date – check the sources as they may have changed.
- The author has submitted issues to Microsoft documentation on some items, so they may be changed, they may not.

The Fine Print and the MVP

<RANT>

Cloud documentation is such that a rare hidden factoid that you find (later) on an unrelated documentation page and that may or may not be uncovered in time will change the outlook of an entire project

</RANT>

Creating an Account By Default...

- When creating an Azure account you are required to prove that you are human
- This requires to click on several image that represent a given subject.
- Once you select all the appropriate image, over several iterations it moves on to the next phase of account creation
- But only if you have a browser with a chrome engine
 - Chrome, Edge, etc
- If you happen to use firefox, then you are in an endless loop

Irony Alert:

A robot testing to see if you are human

Azure Functions - HTTPS

By Default...

"HTTPS is not required of incoming requests by default..."¹

"...optional for traffic on private networks..."²

"...clients can connect to function endpoints by using both HTTP or HTTPS..."³

- Azure functions do not enforce HTTP Only.
- You must configure HTTP to redirect to HTTPS.

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/functions-security-baseline#ns-1-implement-security-for-internal-traffic>

2. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/functions-security-baseline#dp-4-encrypt-sensitive-information-in-transit>

3. <https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4#require-https>

Why does this fail?

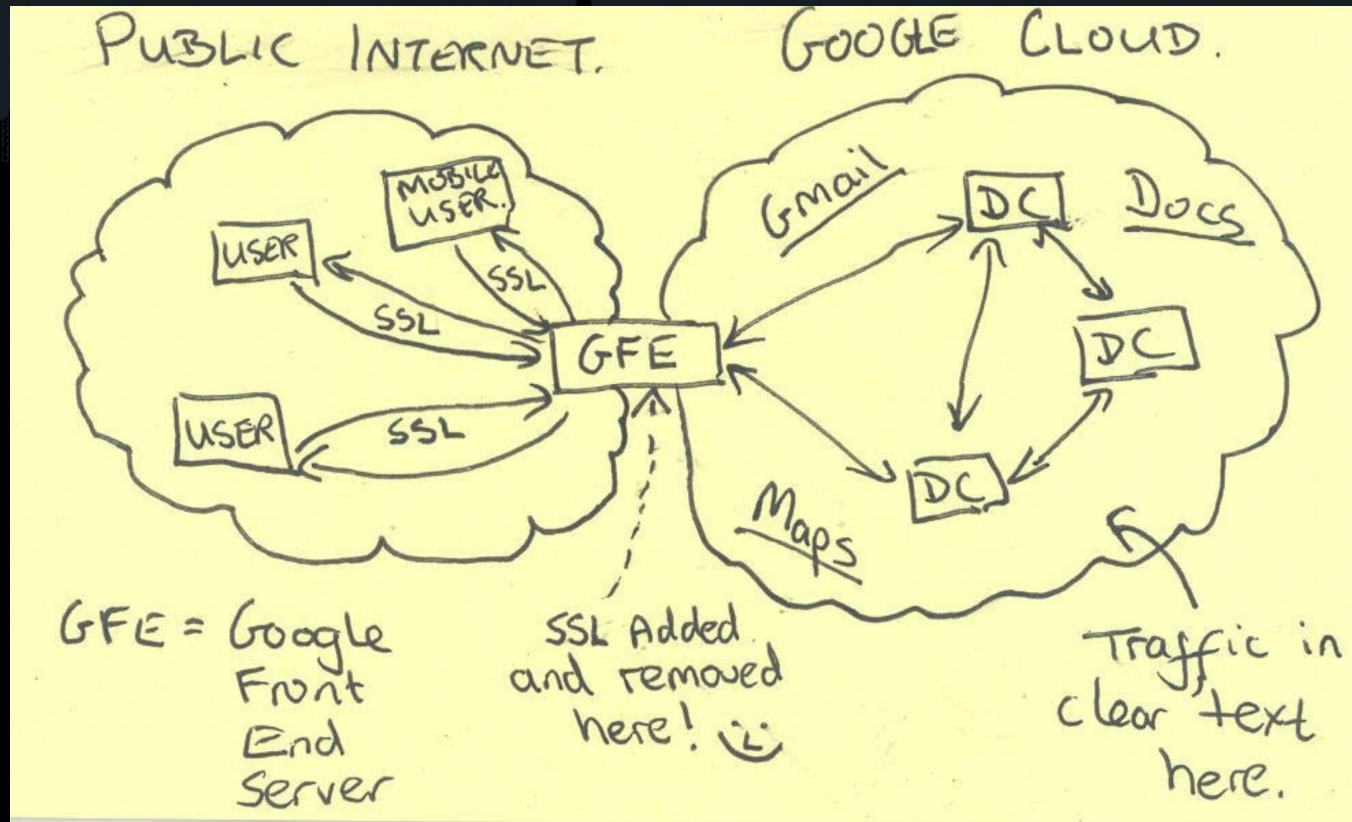
- Fails the “Defence in depth” test.
 - If any outside defences fail then all internal traffic is exposed.
- Can you trust everything on your internal network?
- Beachhead to lateral movement in network. Sniffing internal.
- TLS provides AuthN plus integrity in addition to confidentiality.

One Click Mitigation

The screenshot displays the Azure App Service management interface for TLS/SSL settings. The left-hand navigation pane shows various settings categories, with 'TLS/SSL settings' highlighted. The main content area is divided into two tabs: 'Bindings' (selected and highlighted) and 'Private Key Certificates (.pfx)'. Under the 'Bindings' tab, the 'Protocol Settings' section includes a toggle for 'HTTPS Only' which is currently set to 'On', and a dropdown for 'Minimum TLS Version' set to '1.0'. Below this, the 'TLS/SSL bindings' section indicates that no bindings are currently configured for the application.

<https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#enforce-https>

Why does this fail?



- Leaked NSA Slide deck 2013 from https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

But wait! There's more!

- Every Azure Function instance requires an Azure Storage Account.
- By default, this storage account will hold:
 - connection strings
 - secrets
 - bindings as application settings in the storage account.
 - Managing Triggers, Logging function executions
- *Blob storage* maintains state and function keys
- *Table storage* stores matrices related to function execution along with other information.
- By default, Azure Storage Accounts, including the one associated with the Azure Function enables a public endpoint.

Azure Function Storage Account Mitigation

- Enable Private endpoint/private link
- You can use a key vault instead

Azure Function App - FTP

The 90s called. They want their internet service back.

By Default...

- each function app has an FTP endpoint enabled¹.
- Transfer files to Azure Functions².
- This FTP Endpoint is public internet facing.
- Protected with deployment credentials.
- Microsoft even recommends to NOT use FTP for deployment.

1. <https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4#disable-ftp>

2. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-deployment-technologies#ftp>

Sidebar:

A function app, is like a container for azure functions. Like a murder of crows, a function app is the plural for your “application”.

Azure Storage Accounts

“By default, storage accounts accept connections from clients on any network.”¹

“...requests can be authorized ... by using the account access key for Shared Key authorization.”²

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#change-the-default-network-access-rule>

2. <https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal>

Azure Storage Accounts

- Beware when using the Networking “blade”.
- Do not leave a storage account with public access unless
 - Read only static content.
 - Or rather use a real CDN.
- RBAC and Access Keys as a storage mechanism.
 - If leaked this could be devastating, especially with public internet access

Azure Storage Account

- “Trusted” Services

Exceptions

- ☒ Allow Azure services on the trusted services list to access this storage account. ⓘ
- ☐ Allow read access to storage logging from any network
- ☐ Allow read access to storage metrics from any network

- SA Firewall sets an exception for “trusted” Azure services
- In this case:
 - Only for those who are trusted services
 - Are registered in your subscription

*Resources of some services, **when registered in your subscription**, can access your storage account **in the same subscription** for select operations, such as writing logs or backup*

- Beware if checkboxes allowing public access to logging and metrics.

Azure Storage Account - Mitigations

- If there is no need for public internet traffic then:
 - Disable public anonymous access
 - limit access to requests originating from specified
 - IP addresses, IP ranges,
 - subnets in an Azure Virtual Network (VNet),
 - or resource instances of some Azure services.
 - Tagging helps here
 - Private Link/Endpoint

Azure Storage Account - Mitigations

- Disable Shared access key access
 - portal

Allow storage account key access ⓘ

☒ Disabled ☐ Enabled

⚠ When Allow storage account key access is disabled, any requests to the account that are authorized with Shared Key, including shared access signatures (SAS), will be denied. Client applications that currently access the storage account using Shared Key will no longer work. [Learn more about Allow storage account key access](#) ↗

PowerShell

```
Set-AzStorageAccount -ResourceGroupName <resource-group> `
  -AccountName <storage-account> `
  -AllowSharedKeyAccess $false
```

Azure CLI

```
az storage account update \
  --name <storage-account> \
  --resource-group <resource-group> \
  --allow-shared-key-access false
```

Azure Key Vault

- By default:
 - Azure Key Vault is accessible from the public internet¹.
 - Azure Key Vault has logging disabled².
 - Azure Key Vault's firewall is disabled³.


1. <https://learn.microsoft.com/en-us/azure/key-vault/general/authentication#configure-the-key-vault-firewall>

2. https://www.tenable.com/audits/items/CIS_Microsoft_Azure_Foundations_L1_v1.3.1.audit:07f9892a24aee7bb0b24729db6d817c3

3. <https://learn.microsoft.com/en-us/azure/key-vault/general/network-security#key-vault-firewall-disabled-default>

Azure Key Vault - Mitigations

- Disable public Access
 - Vnet Access, Vnet integration(?), Private Link/endpoint

Firewalls and virtual networks	Private endpoint connections
Allow access from:	<p><input type="radio"/> Allow public access from all networks</p> <p><input checked="" type="radio"/> Allow public access from specific virtual networks and IP addresses</p> <p><input type="radio"/> Disable public access</p> <p> Only networks you choose can access this key vault. Learn more</p>

Azure Key Vault - Mitigations

- Enable firewall
- Enable logging/event grid

Azure Event Hub

- By default,
Event Hub namespaces are accessible from the public internet.¹
(namespace:
a management container for event hubs (or topics, in Kafka parlance). It provides DNS-integrated network endpoints)
- Event Hubs do not support VNet integration.
 - So network access restrictions are not available
- But does support an IP firewall to restrict network access.
 - IP firewall is not available on the Basic Subscription Tier
 - Each instance of a PaaS service has a public IP address exposes that service to the Internet. By default, the firewall service allows all traffic from the Internet.
- Service Endpoints are not supported on the Basic Subscription Tier

1. <https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-ip-filtering>

Azure Managed SQL

“Allow Azure Services and resources to access this server”

- The implication here is that “Azure” services administered by Microsoft are permitted access. This is stated for other services.
- You may also think that these are services that are only part of your subscription.

The Reality? (by hovering over in info icon)

*This option configures the firewall to allow connections from IP addresses allocated to any Azure service or asset, **including connections from the subscriptions of other customers.***

Moar Managed SQL

- This enables public network access to your SQL Instance.
- Eliminates network security layer
- Overrides any other network restriction - because it is considered an exception.
- Attacker needs address, and a connection string.

Managed SQL Mitigations

- Don't select the “exception”.
- Configure only specific VNets or IPs for network access.
 - VNet “injection” not available
 - Use integrated firewall service
- Private Link/endpoint.
 - Removed from public network
 - Enable logging on private endpoints.
 - VNet peering

<https://learn.microsoft.com/en-us/azure/azure-sql/database/firewall-create-server-level-portal-quickstart?view=azuresql>

Azure Virtual Machines

- A new VM is not configured with the NSG for the VNET/Subnet its assigned.
- It is assigned a default NSG on its network interface
- This default NSG has port 22 (SSH) open
 - From anywhere
- Subnets are created without an NSG link
 - Access to subnet not restricted

Azure Data Factory

- On the NSG that is automatically created by Azure Data Factory, Port 3389 is open to all traffic by default.¹

[1] <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/data-factory-security-baseline#ns-2-secure-cloud-services-with-network-controls>

Azure Data Factory Mitigations

- Lock port 3389 down so only authorized personnel from authorized locations can access the control plane.
 - Use Azure SQL Server Integration Services (SSIS) Integration Runtime disallows port 3389 outbound by default at the Windows Firewall Rule on each IR node for protection.

Cosmos DB

- By default, your Azure Cosmos DB account is accessible from internet¹

1. <https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-firewall#ip-access-control-overview>



Thank You



Q&A

