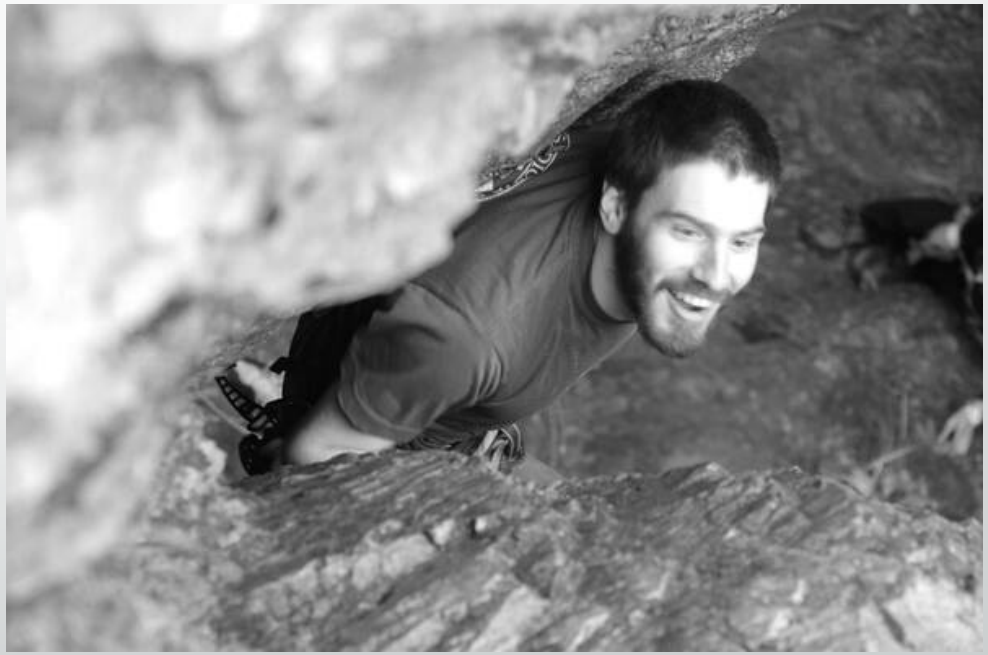
Automatically find and fix security misconfigurations in Azure deployments

Danny Rosseau
Kenneth Wilke
March 14, 2019

About Danny

- Senior consultant at Carve Systems
- Almost local - Eagle CO



About Kenneth

- Roughly a decade of cloud-fu
- Primarily OpenStack and AWS experience
- Texas native, not driving in Colorado
- Blog: https://suchprogramming.com

Outline

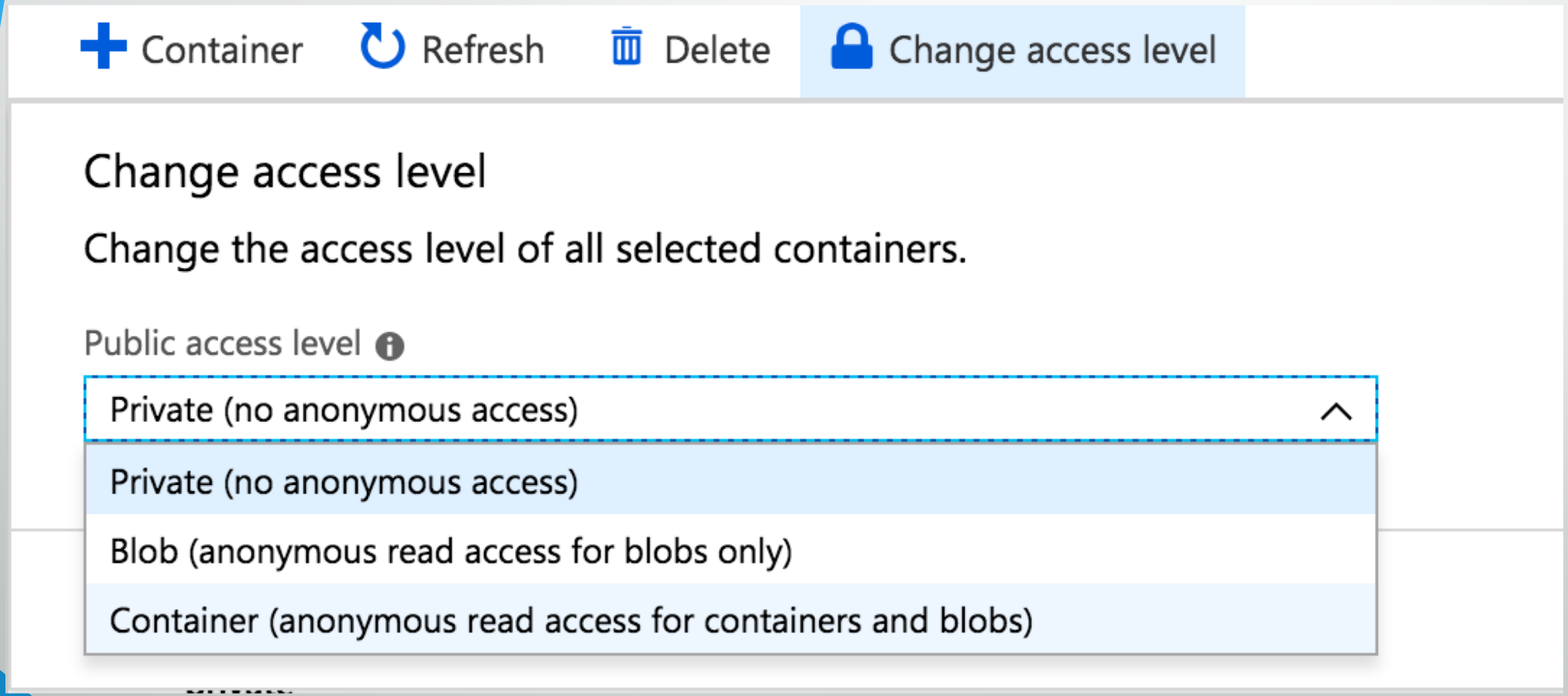
- Cloud security overview
- Common configuration “gotchas”
- What is a cloud security audit?
- Automated discovery, reporting, and remediation

Outline

- Cloud security overview
- Common configuration “gotchas”
- What is a cloud security audit?
- Automated discovery, reporting, and remediation

Cloud Security

- Cloud services are primarily usable by default, not secure by default
- Configured through portals or APIs


Container
Refresh
Delete
Change access level
Change access level
Change the access level of all selected containers.
Public access level
Private (no anonymous access)
Private (no anonymous access)
Blob (anonymous read access for blobs only)
Container (anonymous read access for containers and blobs)


```
[inzure-demo> buckets -p azure -a ls inzurestorageaccount1/pcont
0 B               backups/
0 B               js/
[inzure-demo> buckets -p azure -a ls inzurestorageaccount1/pcont/backups/
8.0 KiB           backups/968463ee4bbaa157eba204af40ed6fd378e84b0b1fe2f49ff0daa9b3564
7f139.db
[inzure-demo> buckets -p azure -a get inzurestorageaccount1/pcont/backups/968463ee4b
baa157eba204af40ed6fd378e84b0b1fe2f49ff0daa9b35647f139.db
[inzure-demo> sqlite3 backups_968463ee4bbaa157eba204af40ed6fd378e84b0b1fe2f49ff0daa9
b35647f139.db 'select * from users'
bob|suchpassword
joe|muchpassword
suchuser|p@ssw0rd
```

Cloud Security

- Cloud services are primarily usable by default, not secure by default
- Configured through portals or APIs
- Security needs didn’t go away!

Outline

- Cloud security overview
- Common configuration “gotchas”
- What is a cloud security audit?
- Automated discovery, reporting, and remediation

COMPUTE (23)

- Virtual machines
- Virtual machines (classic)
- Virtual machine scale sets
- Container services (deprecated)
- Function Apps
- App Services
- Container instances
- Batch accounts
- Service Fabric clusters
- Mesh applications PREVIEW
- Cloud services (classic)
- Kubernetes services
- Availability sets
- Disks
- Disks (classic)
- Snapshots
- Images
- OS images (classic)
- VM images (classic)
- Citrix Virtual Desktops Essentials
- Citrix Virtual Apps Essentials
- CloudSimple Virtual Machines
- SAP HANA on Azure PREVIEW

NETWORKING (27)

- Virtual networks
- Virtual networks (classic)
- Load balancers
- Application gateways
- Virtual network gateways
- Local network gateways
- DNS zones
- CDN profiles
- Traffic Manager profiles
- ExpressRoute circuits
- Network Watcher
- Network security groups
- Network security groups (classic)
- Network interfaces
- Public IP addresses
- Public IP Prefixes
- Reserved IP addresses (classic)
- Connections
- On-premises Data Gateways
- Route tables
- Route filters
- Application security groups
- DDoS protection plans
- Firewalls
- Front Doors PREVIEW
- Service endpoint policies PREVIEW
- Virtual WANs

STORAGE (11)

- Storage accounts
- Storage accounts (classic)
- Recovery Services vaults
- StorSimple Device Managers
- Data Lake Storage Gen1
- Storage explorer PREVIEW
- StorSimple Data Managers
- Storage Sync Services
- Import/export jobs
- Data Box Edge / Data Box Gateway PREVIEW
- Azure NetApp Files PREVIEW

WEB (13)

- App Services
- API Management services
- CDN profiles
- Search services
- Notification Hubs
- Notification Hub Namespaces
- App Service plans
- App Service Environments
- API Connections
- App Service Certificates
- App Service Domains
- Media services
- SignalR

Azure Firewall Consistency

- Redis – open by default
  - No VNet support on lower tiers
- PostgreSQL – closed by default
- Cosmos – open by default
- NSG – VNets open by default
- SQL – closed by default*

Redis Firewalls

inzure-redis-1 - Firewall

Redis Cache

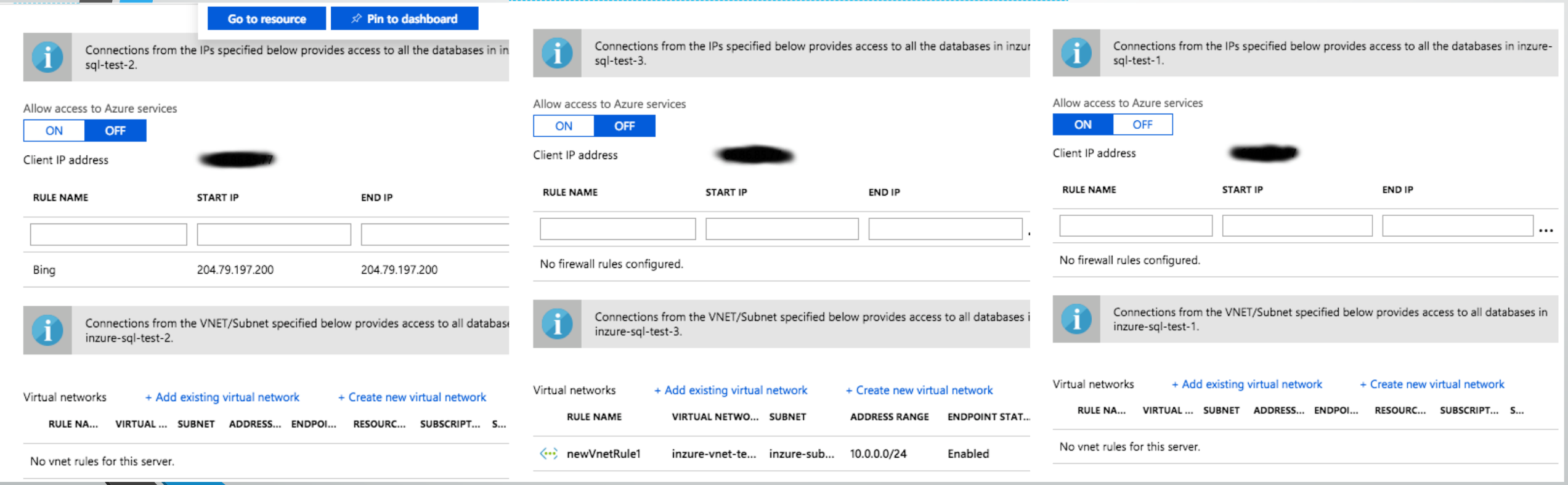
Save Discard

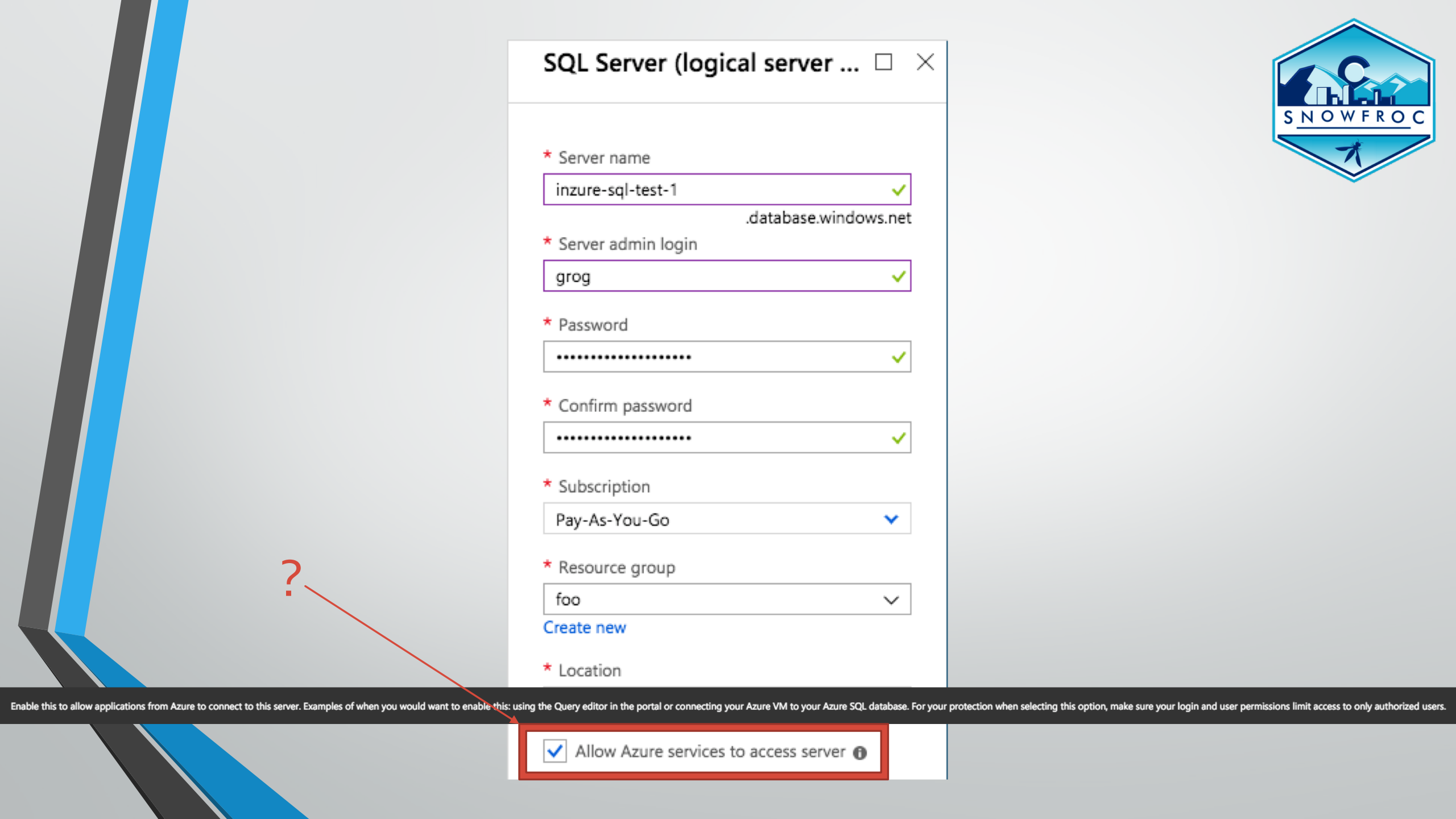
No rules are defined. Connections are allowed from any IP address (default configuration).

RULE NAME	START IP ADDRESS	END IP ADDRESS

No results

SQL Server Firewall Game




SQL Server (logical server ...
* Server name
inzure-sql-test-1
.database.windows.net
* Server admin login
grog
* Password
* Confirm password
* Subscription
Pay-As-You-Go
* Resource group
foo
Create new
* Location
?
Enable this to allow applications from Azure to connect to this server. Examples of when you would want to enable this: using the Query editor in the portal or connecting your Azure VM to your Azure SQL database. For your protection when selecting this option, make sure your login and user permissions limit access to only authorized users.
Allow Azure services to access server

Network Security Group

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	...

Network Security Group

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	⚠ WorldSSH	22	Any	Any	Any	✔ Allow ...
110	⚠ WorldRDP	3389	Any	Any	Any	✔ Allow ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow ...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny ...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow ...
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow ...
65500	DenyAllOutBound	Any	Any	Any	Any	✖ Deny ...

Network Security Group

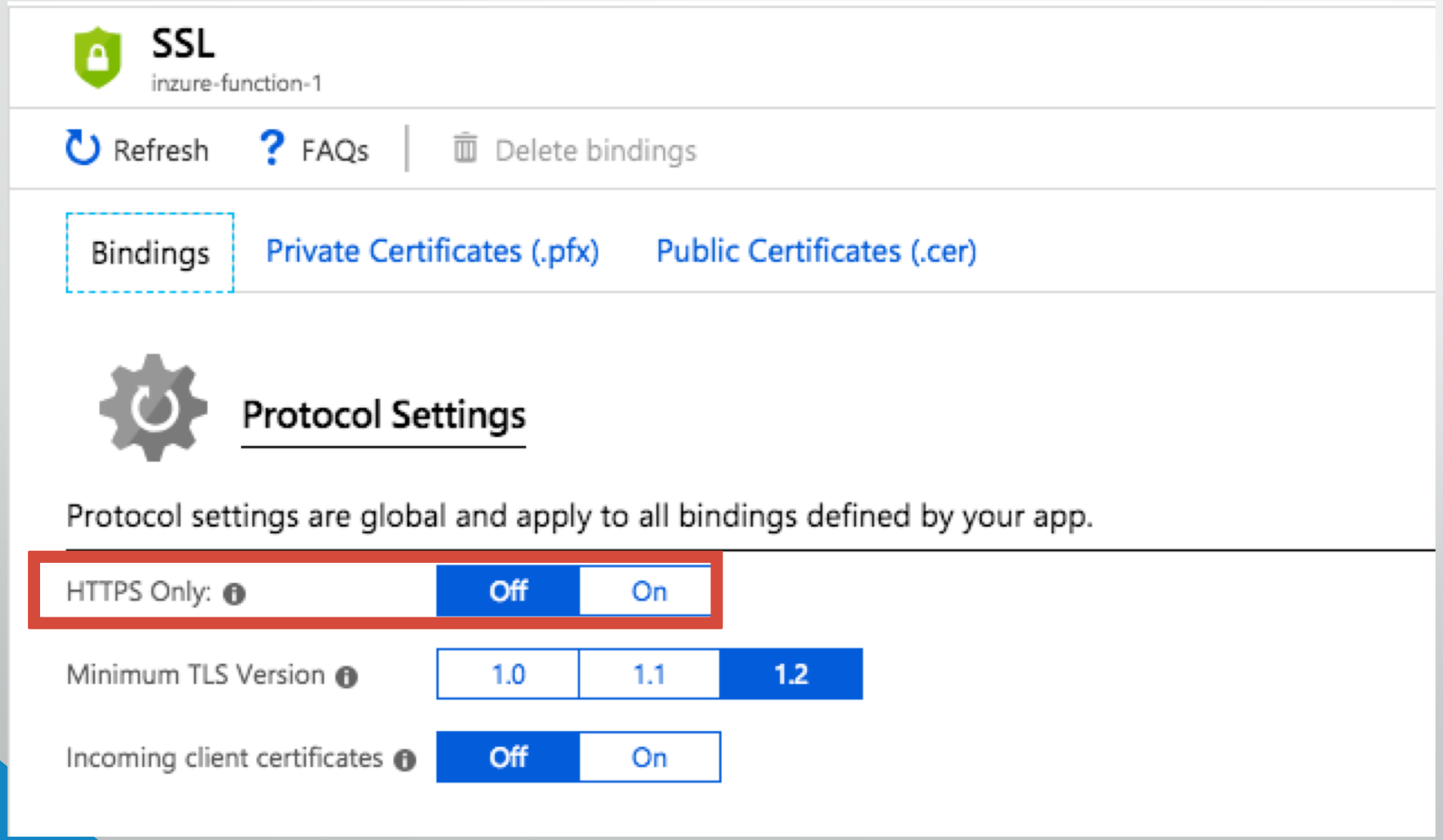
Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	WorldSSH	22	Any	204.79.197.200	Any	Allow
110	WorldRDP	3389	Any	0.0.0.0/1	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

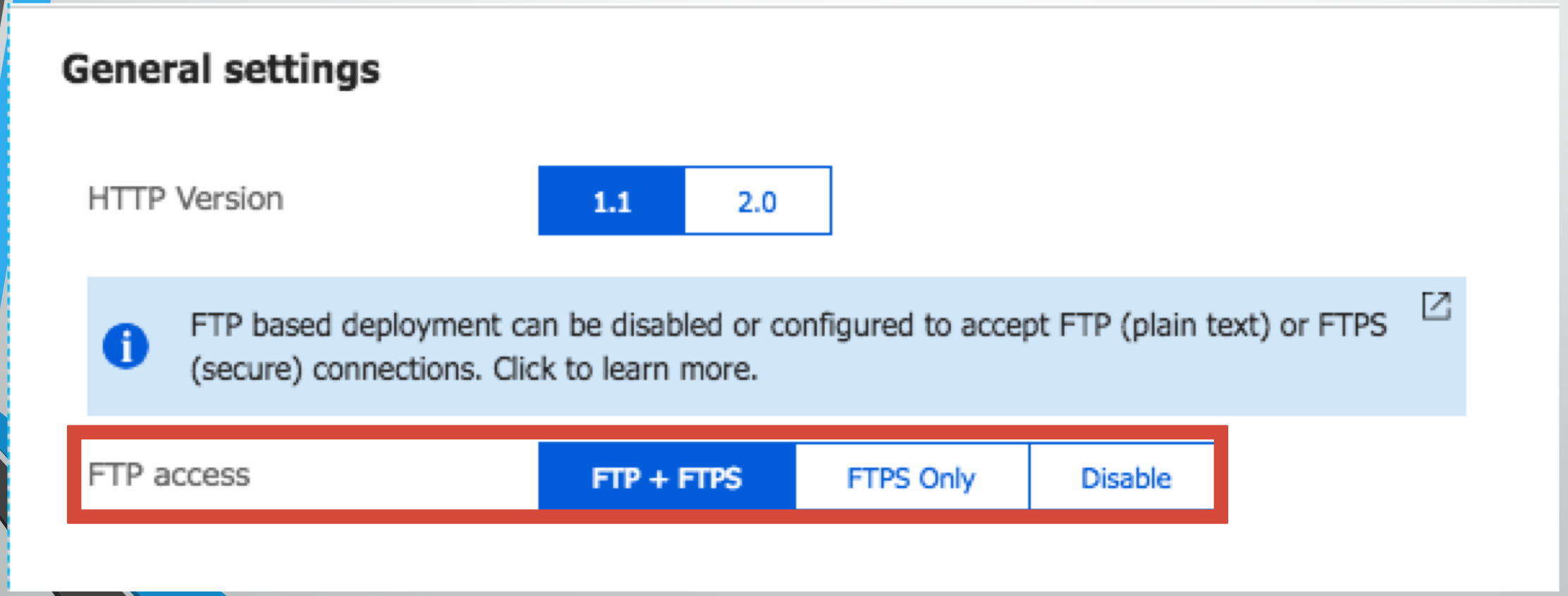
Outbound security rules

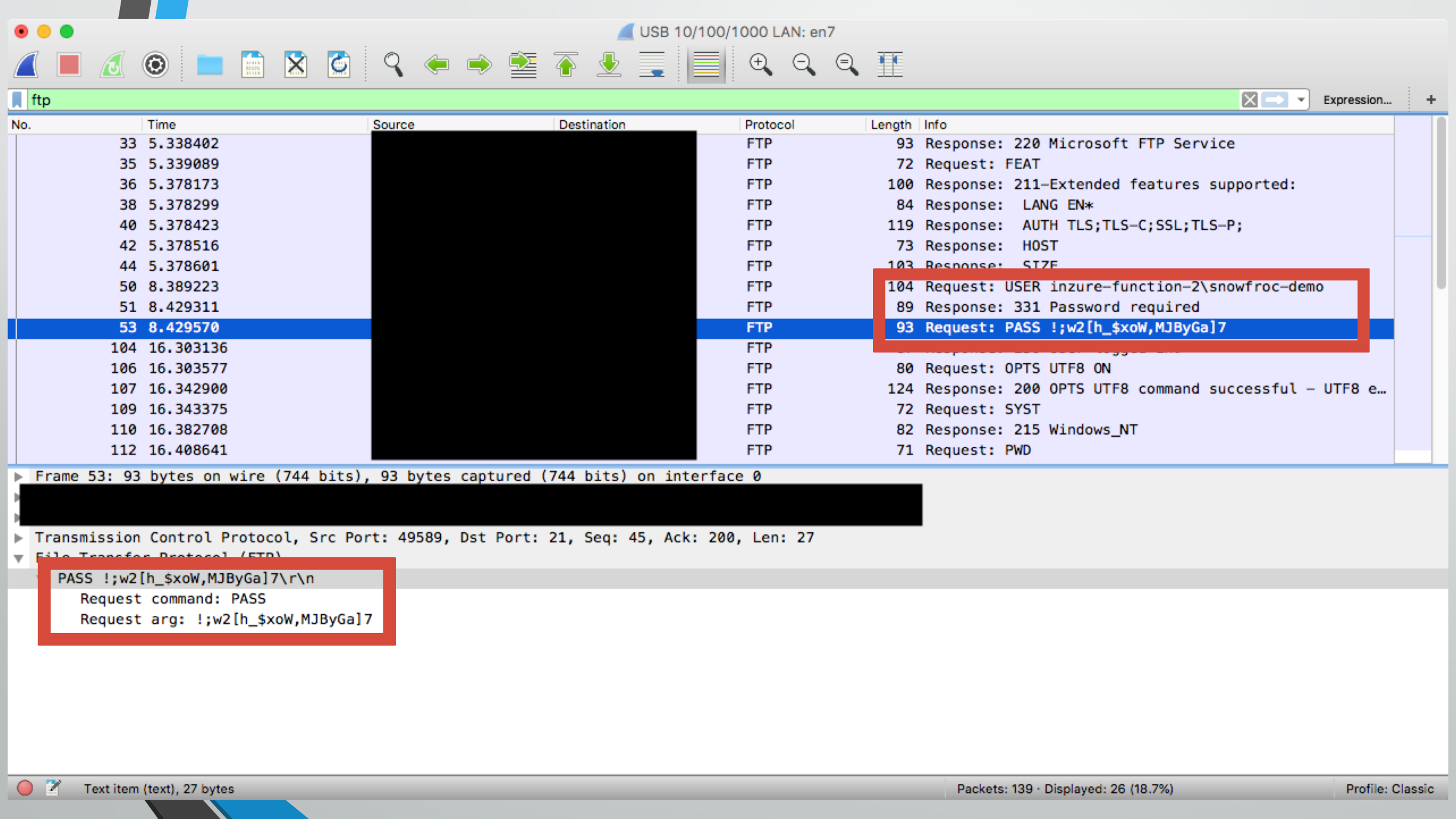
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

App Default TLS Config



App Default General Config




USB 10/100/1000 LAN: en7
ftp
Expression...
No. Time Source Destination Protocol Length Info
33 5.338402 FTP 93 Response: 220 Microsoft FTP Service
35 5.339089 FTP 72 Request: FEAT
36 5.378173 FTP 100 Response: 211-Extended features supported:
38 5.378299 FTP 84 Response: LANG EN*
40 5.378423 FTP 119 Response: AUTH TLS;TLS-C;SSL;TLS-P;
42 5.378516 FTP 73 Response: HOST
44 5.378601 FTP 103 Response: SIZE
50 8.389223 FTP 104 Request: USER inzure-function-2\snowfroc-demo
51 8.429311 FTP 89 Response: 331 Password required
53 8.429570 FTP 93 Request: PASS !;w2[h_$xoW,MJByGa]7
104 16.303136 FTP
106 16.303577 FTP 80 Request: OPTS UTF8 ON
107 16.342900 FTP 124 Response: 200 OPTS UTF8 command successful - UTF8 e…
109 16.343375 FTP 72 Request: SYST
110 16.382708 FTP 82 Response: 215 Windows_NT
112 16.408641 FTP 71 Request: PWD
Frame 53: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Transmission Control Protocol, Src Port: 49589, Dst Port: 21, Seq: 45, Ack: 200, Len: 27
PASS !;w2[h_$xoW,MJByGa]7\r\n
Request command: PASS
Request arg: !;w2[h_$xoW,MJByGa]7
Text item (text), 27 bytes
Packets: 139 · Displayed: 26 (18.7%)
Profile: Classic

Azure Containers

- 3 levels of access
  - Private
  - Public Blob
  - Public Container
- Easy to misuse

Enough?

Outline

- Cloud security overview
- Common configuration “gotchas”
- What is a cloud security audit?
- Automated discovery, reporting, and remediation

Azure Configuration

- Did you click all of the right buttons?
- Matching use case to service

External Pentest

- Broad evaluation of exposed attack surface with deeper dives on targeted components
- Virtual machine exposed services
- Exposed APIs
- Exposed application services and functions
- Brute forcing credentials

Outline

- Cloud security overview
- Common configuration “gotchas”
- What is a cloud security audit?
- Automated discovery, reporting, and remediation

Current Azure tooling

- Azure CLI
  - Usable with bash and jq
  - Not extensible
  - Just recon
- Azurite (https://github.com/mwrlabs/Azurite)
  - Powershell based
  - No library for extensibility
  - Mostly just recon
- Azucar (https://github.com/nccgroup/azucar/)
  - Recon
  - Powershell

A few quick demos

- inzure for pentesters
- inzure in a reporting pipeline
- Inzure for automated remediation

Recon

https://golang.org/doc/gopher/pencil/gopherhelmet.jpg - Renee French

Demo

Inzure Query Strings

- Share inzure resource identifiers across applications
- Quickly query inzure data
  - Compare fields
  - Call methods

Inzure Query Strings

- /Resource
  - /SQLServers
- /Resource/ResourceGroup
  - /StorageAccounts/foo
- /Resource/ResourceGroup/ResourceName
  - /VirtualMachines/foo/bar

Inzure Query String Conditionals

- /Resource[.Field.Selector == "Value" && .Field.Method() < 2]
- /Resource[.Field.Slice[ANY] == "Value" || .Field.Slice[LEN] == 0]

Demo

Inzure as a library

- Accuracy is paramount
  - Accepts uncertainty as a reality
- Aims for quick development
  - Godoc
  - Query strings
  - Generic helper functions included for you


func main() {
qs := "/NetworkSecurityGroups[.AllowsIPToPortString(\"Internet\", \"22\") != BoolFalse]"
nsgs := make([]*inzure.NetworkSecurityGroup, 0)
if err := sub.FromQueryString(qs, &nsgs); err != nil {
fmt.Fprintln(os.Stderr, err)
os.Exit(1)
}
if len(nsgs) > 0 {
fixNSGPorts(nsgs)
}
}

Reporting

- Ingest inzure data
- Run tests (or use query strings)
- Report it!

Automated Fixing

- Ingest inzure data
- Run tests (or use query strings)
- Fix it!

Testing Framework

- Modular
  - Plugin based
- Leverage inzure as a library for quick test development

Demo

Future Work

- Active Directory
- Add more services
- Network mapping (this is close!)
- Testing plugins
- Community involvement

Thanks!

- https://github.com/CarveSystems/inzure
- GPLv3 license
- Testing framework will be released once the API is solidified