

Fortinet XPA2023 - ZTNA

Track

Hands-On Lab

Fortinet Canada CSE Team

Last Update November 2023

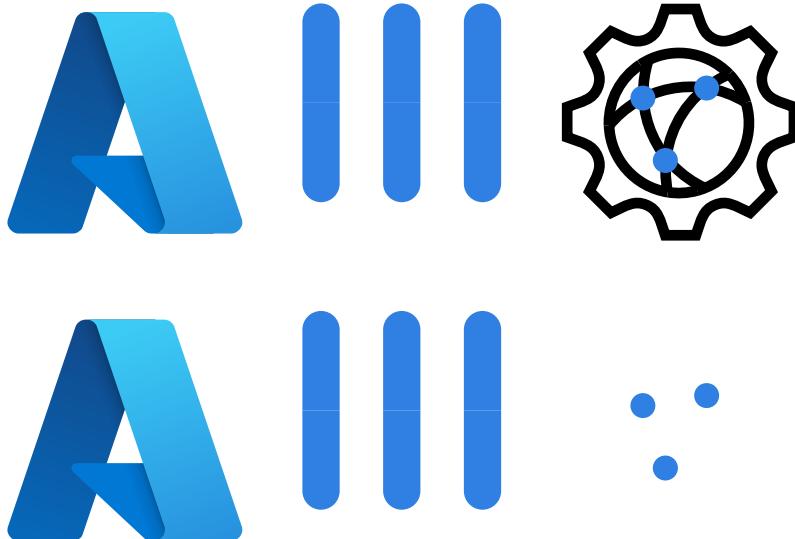
Table of contents

1. Hands-On Lab: Fortinet Azure Blueprint	4
1.1 Comparative Analysis of Azure NSG, FortiGate, and FortiWeb for Web Application Security	4
1.2 Introduction	4
1.3 Lab 1: Exploring Network Security with Azure NSG and FortiGate	4
Components	4
1.4 Lab 2: Enhancing Web Application Security with FortiWeb	4
Components	5
1.5 Network topology	5
2. Getting Started	8
2.1 Accessing your Azure Account	8
Accessing the Azure Portal	9
Changing Your Password	13
Switching Language Settings	17
Verifying Resource Groups	19
Launching CLI & Setting Up Storage Account	20
2.2 Your Lab Environment	22
Deploying your Lab Environment in Azure	22
Initializing DVWA	35
3. Hands on Labs	38
3.1 Protecting Web Application Using Azure Network Security Groups and FortiGate	38
Accessing DVWA via NSG's	38
Accessing DVWA via FortiGate	45
Demonstrating non-signature based attacks via FortiGate	53
3.2 Protecting Web Application Using FortiWeb	63
Connecting to DVWA	63
Sequence of Scans	65
FortiWeb Policy	0
Security Monitoring with FortiView	0
Signatures	0
Machine Learning	0
Client Management	0
X-Forwarded-For	0
Cookie Security	0
CSRF Protection	0
Hidden Fields Protection	0

File Security	0
Web Shell Detection	0
Let's Encrypt Certificates	0
Allow Method	0
Bot Mitigation Policy	0
DoS Protection Policy	0
URL Rewriting	0
User Tracking	0
Custom Policy	0
HTTP Protocol Constraints	0
HTTP Header Security	0
Parameter Validation	0
Man in the Browser (MiTB) Protection	0
URL Access	0
HTTP Authentication	0
IP List	0
FortiGate Quarantined IPs	0
GEO IP	0
Vulnerability Scanner	0
4. Resources	0
4.1 Fortinet Reference Architecture for Azure	0
Considerations and Justifications	0
FortiWeb Reference Architecture	0
FortiGate Reference Architecture	0
Frequently Asked Questions	0
4.2 FortiWeb Bootstrap	0
Part1 : Student-Specific Configuration Settings	0
4.3 Cloud Role Play	0
4.4 Download this HoL in PDF format	0

1. Hands-On Lab: Fortinet Azure Blueprint

1.1 Comparative Analysis of Azure NSG, FortiGate, and FortiWeb for Web Application Security



1.2 Introduction

Welcome to this hands-on lab experience, designed to give you practical insights into protecting your Damn Vulnerable Web Application (DVWA). This exercise is divided into two distinct labs, each exploring different security solutions.

1.3 Lab 1: Exploring Network Security with Azure NSG and FortiGate

In the first lab, we will explore Azure Network Security Groups (NSG) and FortiGate functionalities to establish a secure environment for your DVWA application. The aim of this section is not only to demonstrate how these tools operate and can be fine-tuned for application security, but also to highlight their limitations. By examining the differences between NSG and FortiGate, we set the stage for the second lab focused on FortiWeb, which provides a more comprehensive security solution.

Components

- Azure Network Security Groups (NSG)
- FortiGate Firewall
- DVWA Web Application

1.4 Lab 2: Enhancing Web Application Security with FortiWeb

The primary objective of this second lab is to introduce the various security measures available for protecting web applications. You will gain firsthand experience in implementing these tools and will have the opportunity to compare their effectiveness, with a focus on demonstrating FortiWeb's superior protection capabilities compared to previous solutions.

Components

- FortiWeb Web Application Firewall
- DVWA Web Application

1.5 Network topology

There are multiple ways to install **FortiGate**, **FortiWeb** and **DVWA**. In this document, we will utilize a predefined template available for Azure:

The Fortinet Reference Architecture for Azure

This template automatically deploys a **FortiGate** cluster, a **FortiWeb** cluster, and a **DVWA** instance, along with a predefined policy, enabling you to begin the demo immediately.



What is Fortinet Reference Architecture for Azure?

This architecture provides users with templates that deploy and preconfigure a perimeter solution to address dynamic security needs.

It features a **FortiGate** Next Generation Firewall, **FortiWeb WAF**, and **DVWA Endpoint**.



The WAF secures web servers against inbound attacks over HTTP/HTTPS, while the Next Generation Firewall supports various protocols, enabling connectivity, multi-protocol security, and serving as the primary egress mechanism. The FortiGate and FortiWeb solutions complement each other, with FortiWeb offering advanced features for HTTP/HTTPS traffic and FortiGate providing extensive capabilities for other protocols, routing, VPN termination, and SD-WAN.

Network Topology

This Azure BICEP template deploys a secure environment featuring **FortiGate** and **FortiWeb** for traffic inspection. The **FortiGate** setup receives non-HTTP(S) traffic, while **FortiWeb** handles HTTP(S) traffic, both using user-defined routing (UDR) and public IPs. Additionally, a **Damn Vulnerable Web Application** (DVWA) is included for security testing and learning purposes.

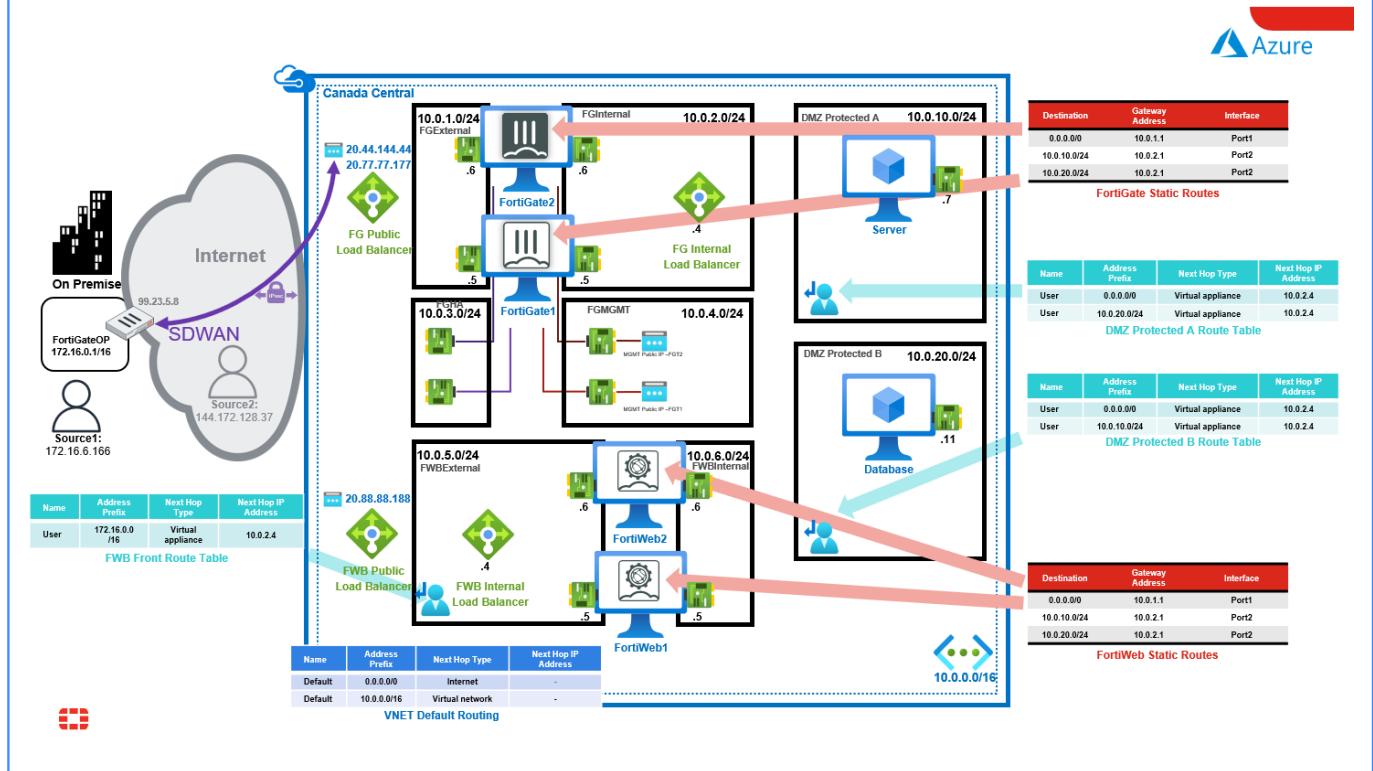
The environment includes:

- 2 x **FortiGate** Firewalls in an active/passive deployment
- 2 x **FortiWeb** WAFs in an active/active deployment
- 2 x Public Azure Standard **Load Balancers** for internet communication (1 x per cluster)
- 2 x Internal Azure Standard **Load Balancers** for forwarding traffic to Azure Gateways connected to ExpressRoute or Azure VPNs
- 1 x **VNET** with 1 protected subnet
- 4 x **Public IPs** for services and FortiGate/FortiWeb management
- **User Defined Routes** (UDR) for end-to-end communication via the FortiGate/FortiWeb deployment

VMs can be installed in different **Availability Zones** or **Availability Sets** for enhanced availability.

These templates can also be **extended** or **customized** based on your requirements, such as adding additional subnets and routing tables.

Click on the image if you want to enlarge it.

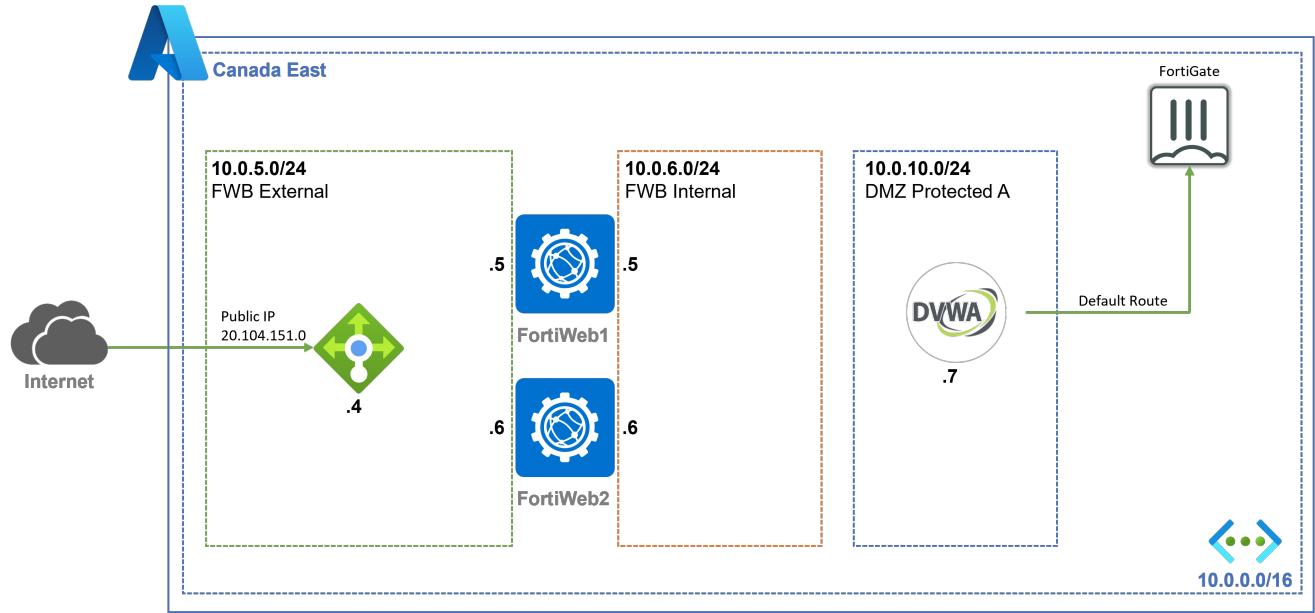


FortiWeb Deployment

FortiWeb is deployed with **2 interfaces** as an **active-active** cluster in **reverse proxy mode**.

- Web browsers connect to the public IP on Azure's Standard Load Balancers.
- FortiWeb decrypts and inspect the HTTP traffic, then forwards it to the DVWA via its internal IP
- Return packets are directed back to FortiWeb's internal IP.
- For DVWA OS updates or SSH connections, traffic is routed through FortiGate.

[Click on the image if you want to enlarge it.](#)



2. Getting Started

2.1 Accessing your Azure Account

This Hands-on-Lab is configured to allow each student to have their own training lab environment using pre-created Azure resource groups, all in one shared Azure Subscription.

Accessing the Azure Portal: Login Instructions

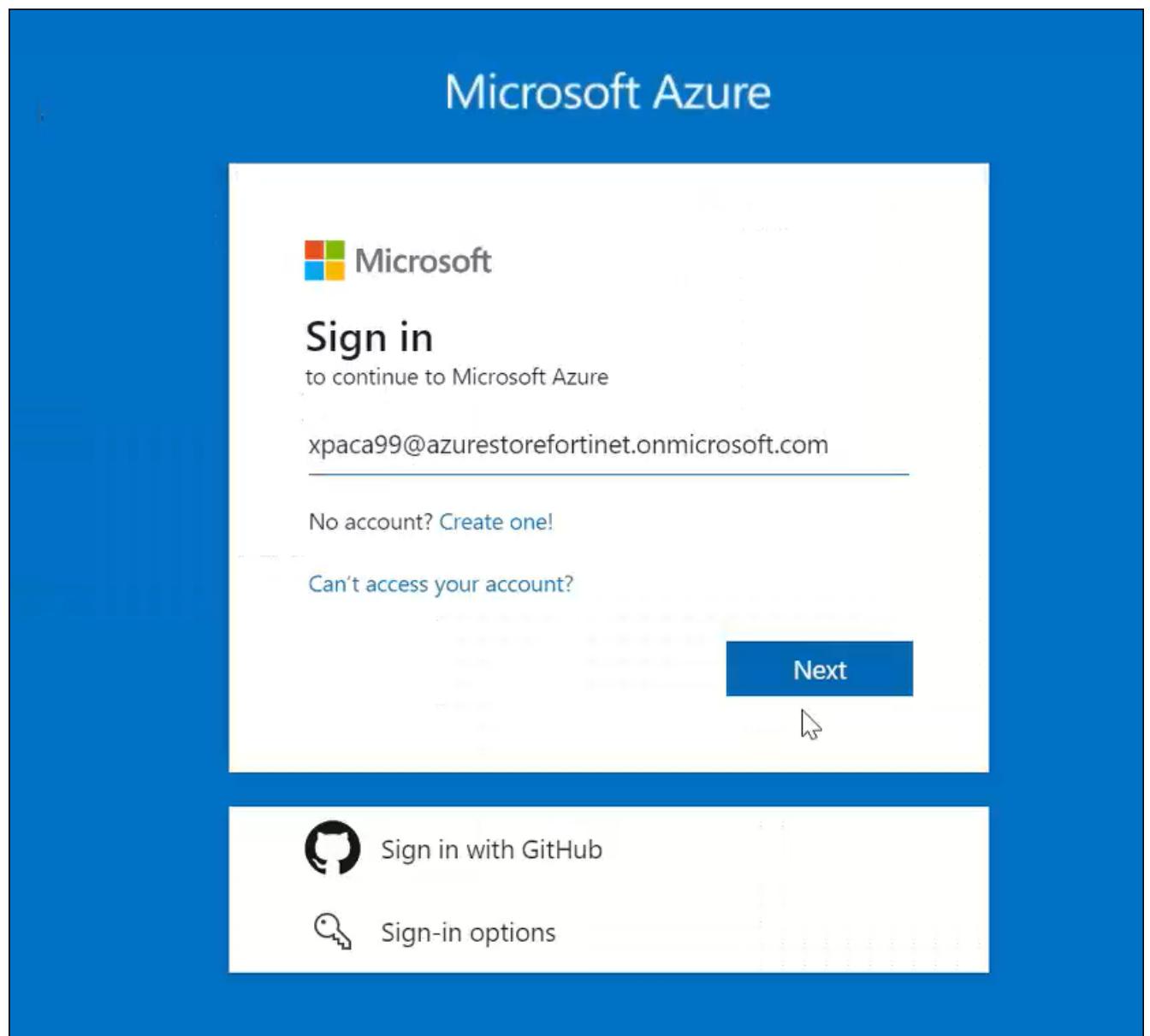
Accessing the Azure Portal

Browse to <https://portal.azure.com>

Use the credentials provided to you by your instructors.

If you can't find them, check your junk mail folder. Look for an email with the subject line: **MIS - Xperts Summit - Public Cloud Track - AZURE LAB Credentials.**

Username: xpacaXX@azurerestorefortinet.onmicrosoft.com



Password: <password provided by email>



Click to log in, and optionally select "Yes" to stay signed in.



When the **Welcome to Microsoft Azure** window appears, skip the tour.

A screenshot of the Microsoft Azure Portal dashboard. The top navigation bar includes the Microsoft logo, search bar, and user info (xpaca99@azurerestorefor...). The main area shows "Azure services" with icons for Create a resource, Quickstart Center, Virtual machines, App Services, Storage accounts, SQL databases, Azure Cosmos DB, Kubernetes services, Function App, and More services. Below is a "Resources" section with "Recent" and "Favorite" tabs, and a "Name" search input. A red box highlights a "Welcome to Microsoft Azure" modal window. The modal contains the text "Welcome to Microsoft Azure", "Let's show you around before you get started.", a "Start tour" button, a "Maybe later" button (which is highlighted with a red box), and a "View all resources" link at the bottom.

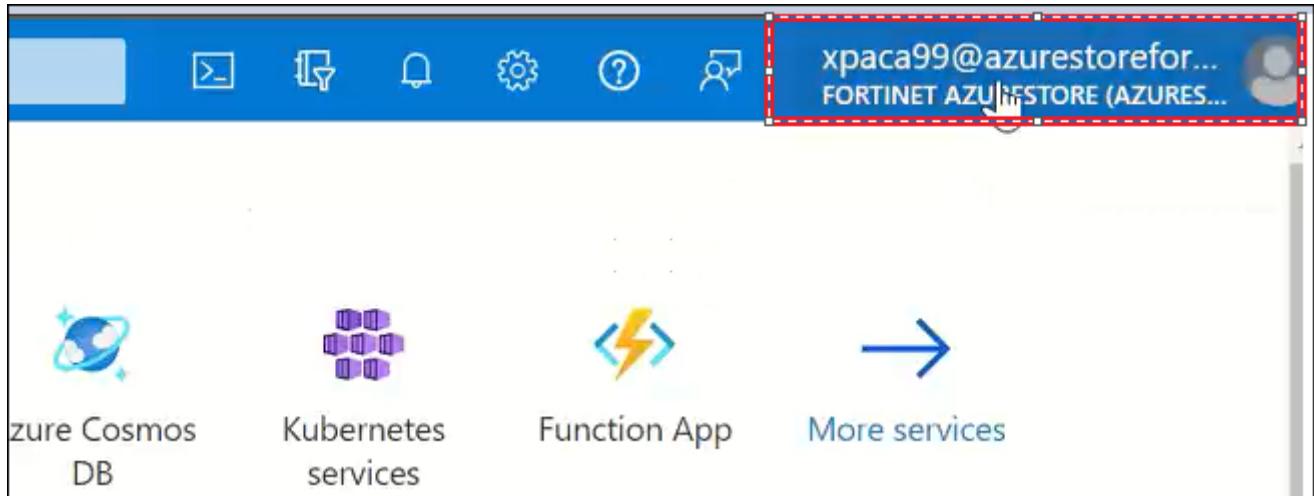
Now that you've signed in, you are on the Azure Portal Dashboard.

Notice your **username** in the top right corner.

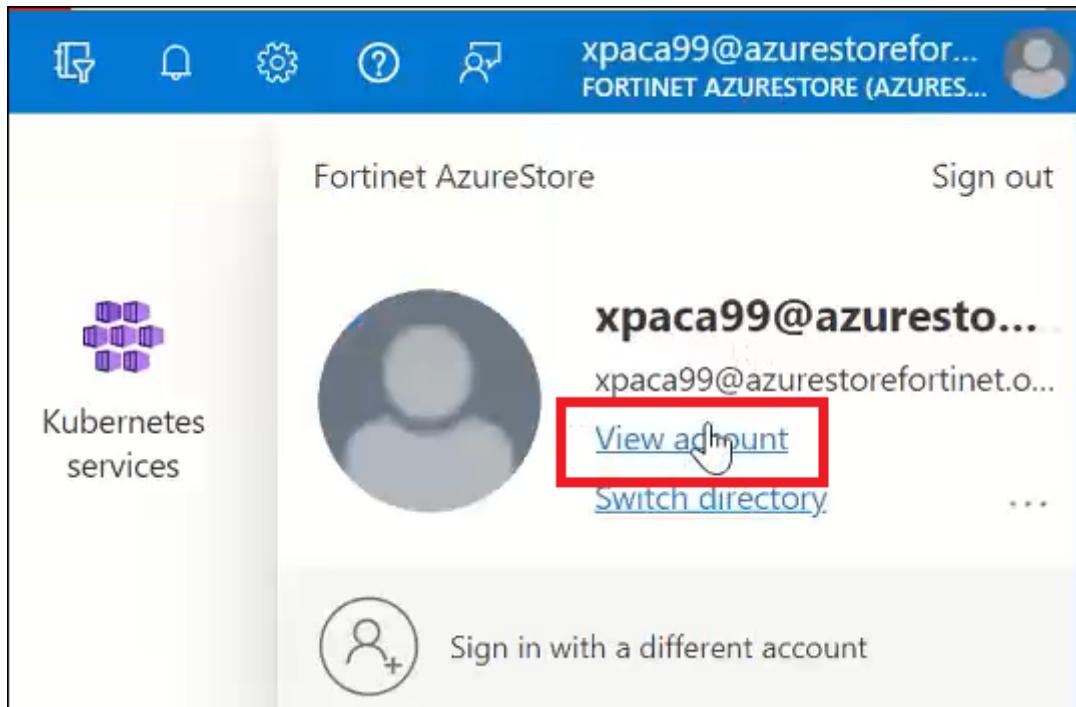
Changing Your Password

Changing Your Password

Click on your **username** located in the top-right corner of the screen.



Select **View Account**. This action will automatically open a new tab.



You can skip the Microsoft feedback in this new tab.

The screenshot shows a Microsoft Edge browser window with the URL myaccount.microsoft.com/?ref=MeControl. A red box highlights the address bar. A modal window titled "Give feedback to Microsoft" is open. At the top right of the modal is a hand cursor icon with a red box around it. The modal contains a satisfaction rating scale from 1 to 5, with 1 being "Not satisfied" and 5 being "Extremely satisfied". Below the scale is a text area for feedback, with a note: "Remember not to include personal or sensitive information like phone numbers, passwords or cryptographic keys." There is also a checkbox for "You can contact me about this feedback". At the bottom are "Submit" and "Cancel" buttons.

Scroll down, if needed, and click on **Change Password**.

The screenshot shows the Microsoft My Account overview page. On the left is a sidebar with links: Overview, Security info, Devices, Password, Organizations, Settings & Privacy, My sign-ins, and Give feedback. The "Overview" link is highlighted. The main content area has a "Sign out everywhere" button. Below it are three cards: "Password" (with a key icon), "Organizations" (with a briefcase icon), and "Devices" (with a laptop icon). The "Password" card has a red box around the "CHANGE PASSWORD" button. The "Organizations" card has a red box around the "MANAGE ORGANIZATIONS" button.

Fill in the required fields to change your password and click **Submit**.

Change password

Strong password required. Enter 8-256 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.

User ID

xpaca99@azurerestorefortinet.onmicrosoft.com

Old password

.....

Create new password

.....

strong

Confirm new password

.....

Submit

Cancel

©2023 Microsoft Legal | Privacy

Once you see the confirmation screen, you can close this tab. Your password has been successfully changed.

This Profile page is being replaced by 'My Account'.

[Learn more](#) [Try it now!](#) [Dismiss](#)

Profile



xpaca99

Email: [Manage account](#)
Alternate email: [Change password](#)

[Edit security info](#) [Review terms of use](#)

[Sign out everywhere](#)

Switching Language Settings

Switching Language Settings

If you wish to change the language of your Azure dashboard, follow these steps.

After logging into your Azure account, click on the **gear icon** in the upper-right corner.



Next, select **Language + Regional Format**.

Portal settings | Language + region

Choose your language and the regional format that will influence how your date/time and currency will appear.

Directories + subscriptions	Language	Français
Appearance + startup views	Regional format	Français (Canada)
Language + region		
My information		
Signing out + notifications		

Choose your preferred language and regional format.

For example, if you select "English (Canada)," it will change the Dashboard language to Canadian English.

Paramètres du portail | Langue + région

Menu Rechercher

Répertoires + abonnements

Apparence + affichages au démarrage

Langue + région

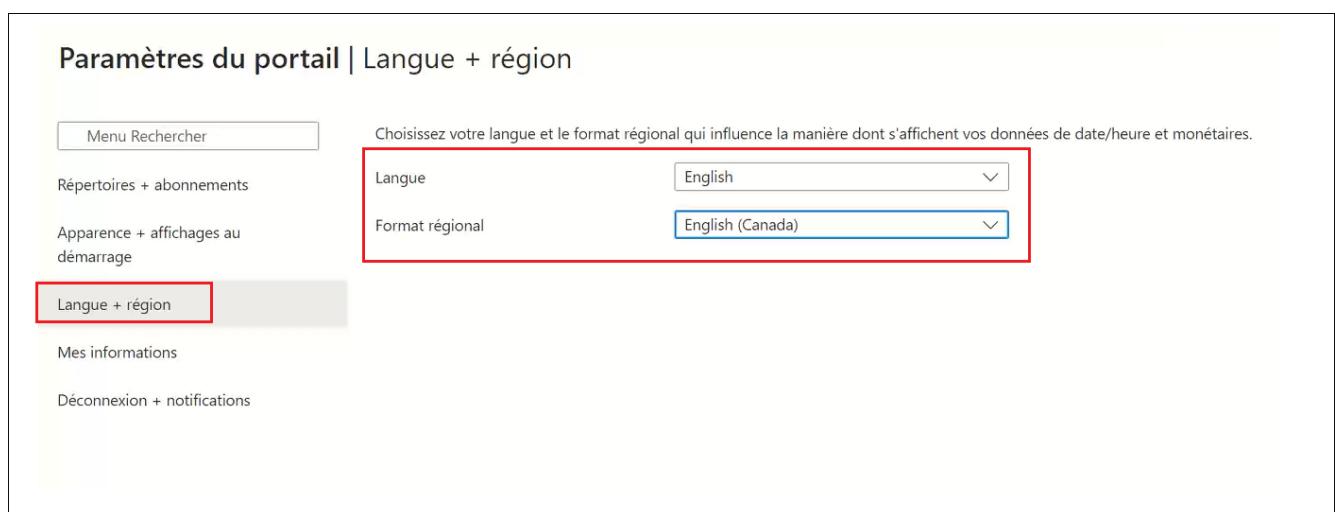
Mes informations

Déconnexion + notifications

Choisissez votre langue et le format régional qui influence la manière dont s'affichent vos données de date/heure et monétaires.

Langue English

Format régional English (Canada)



Click **Apply**. A message will appear asking for confirmation. Click **OK** to confirm the language change.

Microsoft Azure

Search resources, services, and docs (G+/)

Portal settings | Language + region

Search menu

Directories + subscriptions

Appearance + startup views

Language + region

My information

Signing out + notifications

Change language

Are you sure you want to apply these changes to your language and region settings? The portal will reload and apply these settings.

OK **Cancel**



Verifying Resource Groups

Verifying Resource Groups

In a new Azure subscription account, only two resource groups will be pre-existing. These will be used in this lab for security customization.

Navigate to **Resource Groups** on the main page.

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and several service icons: Create a resource, Quickstart Center, Virtual machines, App Services, Storage accounts, SQL databases, Azure Cosmos DB, Kubernetes services, Function App, and More services. Below this is the 'Resources' section with tabs for Recent (selected) and Favorite. It displays a table with columns for Name, Type, and Last Viewed. A message says 'No resources have been viewed recently' with a 'View all resources' button. At the bottom is the 'Navigate' bar with links for Subscriptions, Resource groups (which is highlighted with a red box), All resources, and Dashboard.

Make sure **two** resource groups are displayed, prefixed with your student number.

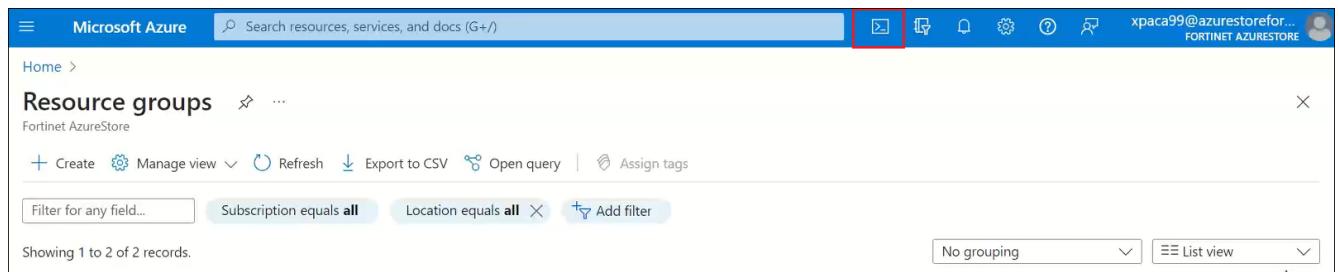
The screenshot shows the 'Resource groups' blade. At the top, there are buttons for Create, Manage view, Refresh, Export to CSV, Open query, and Assign tags. Below is a filter bar with 'Subscription equals all' and 'Location equals all'. It shows 1 to 2 of 2 records. Two resource groups are listed: 'xpaca99-blueprint' and 'xpaca99-training', both under 'FTNT-Training' subscription and 'East US' location. The entire list area is highlighted with a red box.

Launching CLI & Setting Up Storage Account (mandatory)

Launching CLI & Setting Up Storage Account

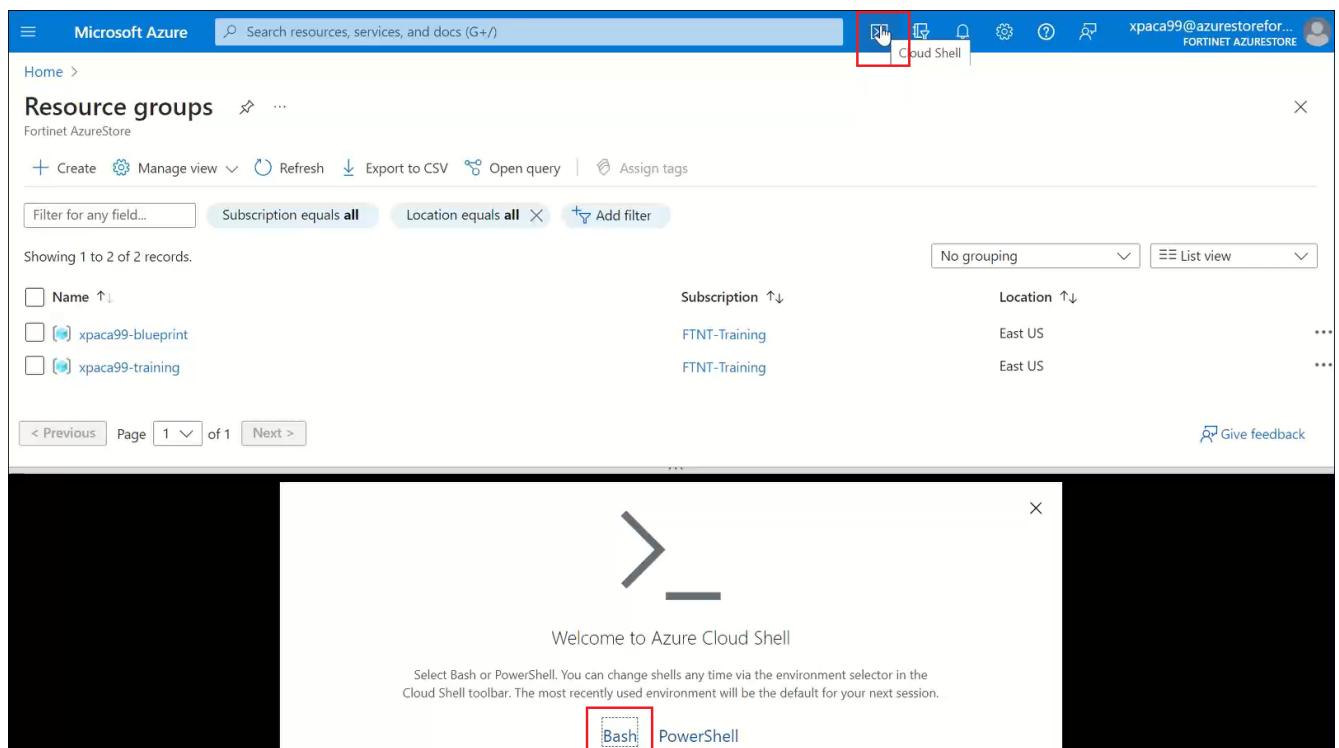
We'll next connect to the **Azure CLI**, which plays a key role in facilitating automated deployments. To do this, you'll need to have a storage account configured.

Click on the **CLI Icon**, found in the top-right corner.



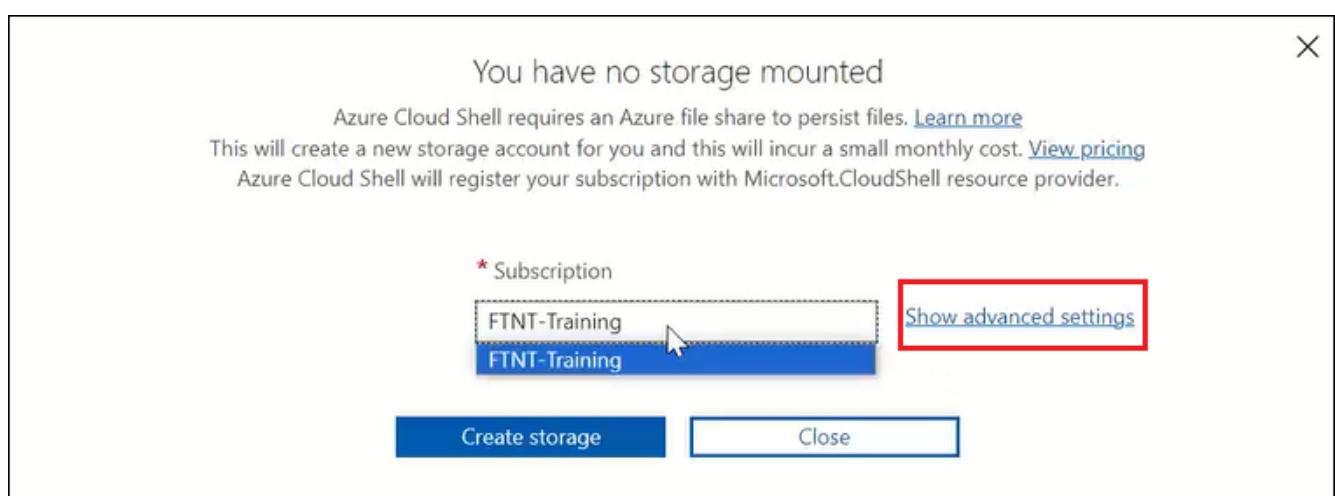
The screenshot shows the Microsoft Azure portal interface. The user is on the 'Resource groups' page for the 'Fortinet AzureStore' subscription. At the top right, there is a toolbar with various icons. One icon, specifically the one for launching the Azure CLI, is highlighted with a red box. The page displays a list of resource groups, with 'Showing 1 to 2 of 2 records.' The CLI icon is located at the far right of the toolbar.

This will open the CLI Shell at the bottom of the screen. Select **Bash Shell**.



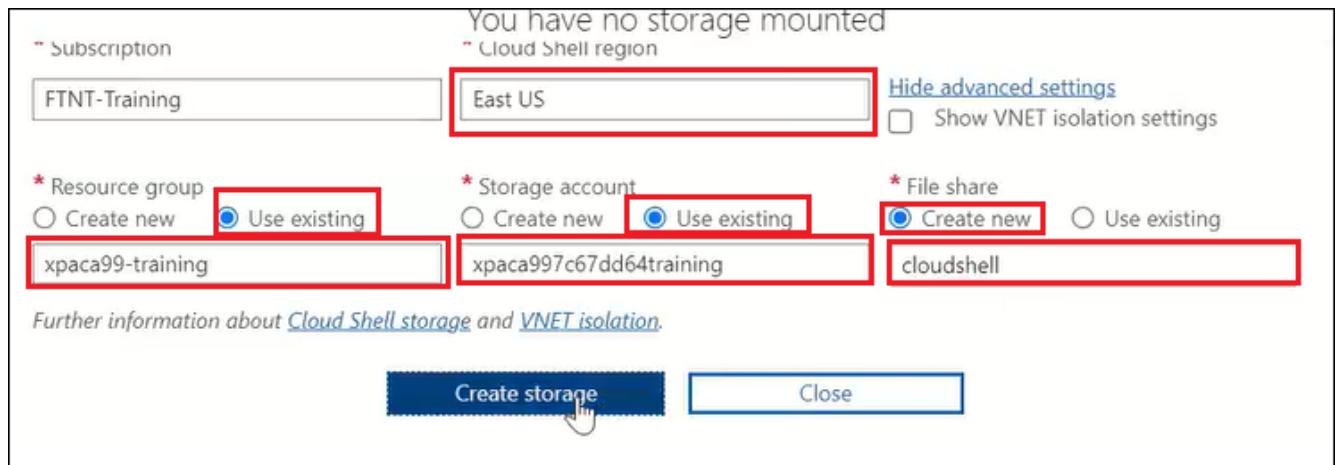
The screenshot shows the same 'Resource groups' page as before, but now the 'Cloud Shell' icon in the top right toolbar is highlighted with a red box. Below the toolbar, the main content area shows a list of resource groups. At the bottom of the screen, a large black rectangular area represents the Azure Cloud Shell interface. Inside this area, there is a smaller white window with a large right-pointing arrow icon. Below the arrow, the text 'Welcome to Azure Cloud Shell' is displayed. At the bottom of this window, there is a button labeled 'Bash' which is also highlighted with a red box. The rest of the shell interface is dark, matching the background of the main portal.

Select your **FTNT-Training** subscription and click on **Show Advanced Settings**.



These advanced settings allow you to select existing resources. Note that the default settings may not align with where our Resource Groups are located.

Adjust your settings to match the example below. **Note:** Your student number may differ.



You are now welcomed to the *Azure Cloud Shell*.

Bash | ⌂ ? ⚙ 📁 ⌂ ⌂ {} ⌂

Requesting a Cloud Shell.**Succeeded.**
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

xpaca99 [~]\$

Congratulation! You are all set to proceed with the lab activities.

2.2 Your Lab Environment

The accounts provided as a part of **Fortinet XPERTS Academy** have adjusted resource quotas to reflect the demands of this Hands on Lab. The subscription has also accepted the terms of the required marketplace offers.

Deploying your Lab Environment in Azure

This section will guide you through the essential steps to deploy your Lab Environment in Azure with the [Fortinet Reference Architecture for Azure](#).



Click on the images to view them in a larger format.

Define your Prefix, Region and Ressource Groupe Name

Before you proceed, complete the form below to personalize your Hands-on Lab experience by setting your **Prefix**, **Region**, and **Resource Group Name**.

Prefix:

xpacaXX

This prefix will be applied to all resources created during this lab for easier management and identification. Your prefix will be **xpacaXX** where **XX** is your student number.

Region:

eastus

You need to choose the **eastus** region (**Richmond, Virginia**) because this is where our Lab Quota is available. Outside of this HOL session, you could select any region in Canada such as **canadacentral** (Toronto, Ontario) or **canadaeast** (Quebec City, Quebec).

Resource Group Name:

xpacaXX-blueprint

This will be the name of the Azure Resource Group where all your lab resources will be contained. Your Azure Resource Group will be **xpacaXX-blueprint** where **XX** is your student number.

Deploy the Lab Environment with Bicep

- Access the Azure Cloud Shell either through the Azure Portal or directly via <https://shell.azure.com>.
- Log into the Azure Cloud Shell.
- Run the following commands in the Azure Cloud:

```
az bicep upgrade
git clone -b xPerts-HoL https://github.com/AJLab-GH/fortinetCloudBlueprint.git
cd fortinetCloudBlueprint
```

```
benoit [ ~ ]$ az bicep upgrade
git clone -b xPerts-HoL https://github.com/AJLab-GH/fortinetCloudBlueprint.git
cd fortinetCloudBlueprint
Cloning into 'fortinetCloudBlueprint'...
remote: Enumerating objects: 302, done.
remote: Counting objects: 100% (52/52), done.
remote: Compressing objects: 100% (38/38), done.
remote: Total 302 (delta 24), reused 32 (delta 14), pack-reused 250
Receiving objects: 100% (302/302), 633.80 KiB | 20.44 MiB/s, done.
Resolving deltas: 100% (171/171), done.
```

- Deploy the template

```
az deployment group create --name fortinetCloudBlueprint --resource-group @RESOURCE_GROUP_NAME --template-file 000-main.bicep
```

- When you execute the script, it will prompt you with a few questions to configure the necessary settings for deployment. You'll need to provide answers for these specific settings.

Parameter	Description	Requirements
USERNAME	The username you provide will grant you access to the FortiGate / FortiWeb GUI and SSH management interface. This username can differ from your Azure account username.	Username admin is not allowed.
PASSWORD	The password that will be used to log in to the FortiGate / FortiWeb GUI and SSH management interface. It's crucial to use a unique password that hasn't been used elsewhere, as it will appear in plaintext in the bootstrap process.	At least 12 characters long and must include characters from at least three of the following categories: uppercase, lowercase, numbers, special characters (excluding '\'' and '-').
PREFIX	Enter @PREFIX . It will be applied to all the resources created to make them easier to manage, use, and identify.	Needs to be unique .

- To proceed, please enter the necessary variables when prompted.

```
xpaca94 [ ~/fortinetCloudBlueprint ]$ az deployment group create --name fortinetCloudBlueprint
--resource-group xpaca94-blueprint --template-file 000-main.bicep
Please provide string value for 'adminUsername' (? for help): benoitb
Please provide securestring value for 'adminPassword' (? for help):
Please provide string value for 'deploymentPrefix' (? for help): xpaca94
■| Running ..
```

- Deployment can take up to 15 minutes. Time for a coffee break, maybe even two.**
- While the template is deploying, you can monitor its progress by navigating to the resource group **@PREFIX-blueprint** and selecting the **Deployments** menu.

The screenshot shows the Azure portal interface for the 'xpaca94-blueprint' resource group. The 'Deployments' section is selected and highlighted with a red box. The table lists the following deployment details:

Deployment name	Status	Last modified	Duration	Related events
fortigateDeployment	Deploying	10/27/2023, 11:10:40 AM	8 minutes, 6 seconds, 949 milliseconds	Related events
networkDeployment	Succeeded	10/27/2023, 11:03:52 AM	5 seconds, 76 milliseconds	Related events
fortinetCloudBlueprint	Deploying	10/27/2023, 11:11:40 AM	8 minutes, 34 seconds, 59 milliseconds	Related events
Microsoft.NetworkSecurityGroup-20231026160518	Succeeded	10/26/2023, 4:11:00 PM	3 seconds, 368 milliseconds	Related events
dwsDeployment	Succeeded	10/26/2023, 2:08:40 PM	37 seconds, 930 milliseconds	Related events
fortiwebDeployment	Succeeded	10/26/2023, 2:07:23 PM	3 minutes, 25 seconds, 971 milliseconds	Related events

- After deployment, you can output essential information such as public IP addresses that you will need to connect to your deployment:

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

Connect to FortiWeb

Once the deployment is complete, use the following **URLs** and **ports** to connect to your instances:

Instance	HTTPS Ports	SSH Ports
FWB-A	https://@PREFIX.@REGION.cloudapp.azure.com:40030	50030
FWB-B	https://@PREFIX.@REGION.cloudapp.azure.com:40031	50031
DVWA	https://@PREFIX.@REGION.cloudapp.azure.com:443	N/A

FAQ

Why is it hard to predict which FortiWeb unit will handle my traffic?

Traffic is distributed across both FortiWeb units, FWB-A and FWB-B. Due to this load-balancing mechanism, it's unpredictable to determine in advance which unit will manage a particular flow of traffic. That is said, we have enabled **connection persistence** on the external Azure Load Balancer. This ensures that once you've identified the correct FortiWeb unit, your traffic should consistently be managed by that unit.

What should I do if I find the traffic log empty?

If the traffic log is empty on one of the FortiWeb units, you'll need to log in to the other unit to see if the traffic is being managed there.

Why do I get logged out of one GUI when logging into the other?

Both FortiWeb units share the same domain and, consequently, the same cookies. Logging in to one GUI will overwrite the cookie for the other, automatically logging you out.

How can I stay logged into both GUIs simultaneously?

If you wish to keep both GUIs open at the same time, you will need to use two different web browsers. This will allow you to maintain separate sessions for each FortiWeb unit.

You can use the **az deployment group show** command to display all resources along with their URLs and ports.

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

When connecting to FortiWeb GUI, use the username and password that you provided when deploying the template. You should then be logged in to the main Dashboard.

The screenshot shows the FortiWeb-A dashboard with the following details:

- System Information:**
 - HA Status: Active-Active-High Volume
 - Cluster Name: xpacax94
 - Cluster Members: xpacaX94-FWB-A/FVBAZR00ddd9e846 (Primary), xpacaX94-FWB-B/FVBAZR00caf66c11 (Secondary)
 - Serial Number: FVBAZR00ddd9e846
 - Operation Mode: Reverse Proxy
 - System Time: Mon Oct 30 18:40:54 2023
 - Firmware Version: FortiWeb-Azure_OnDemand 7.40,build0577(GA),230721
 - System Uptime: [0 day(s) 0 hour(s) 58 min(s)]
- Licenses:**
 - VM License
 - Support Contract
 - Security Service
 - Antivirus
 - IP Reputation
 - GEO DB

You can double check your **DNS configuration** in the Azure Public IP settings.

In the Azure portal, search for **FWBAPClusterPublicIP**.

The screenshot shows the Microsoft Azure portal search results for "FWBAPClusterPublicIP". The search bar at the top has the query "FWBAPClusterPublicIP". Below it, the search results show one item: "FWBAPClusterPublicIP" under the "Resources" category. The item is highlighted with a red box.

You will find the DNS configuration under the configuration menu.

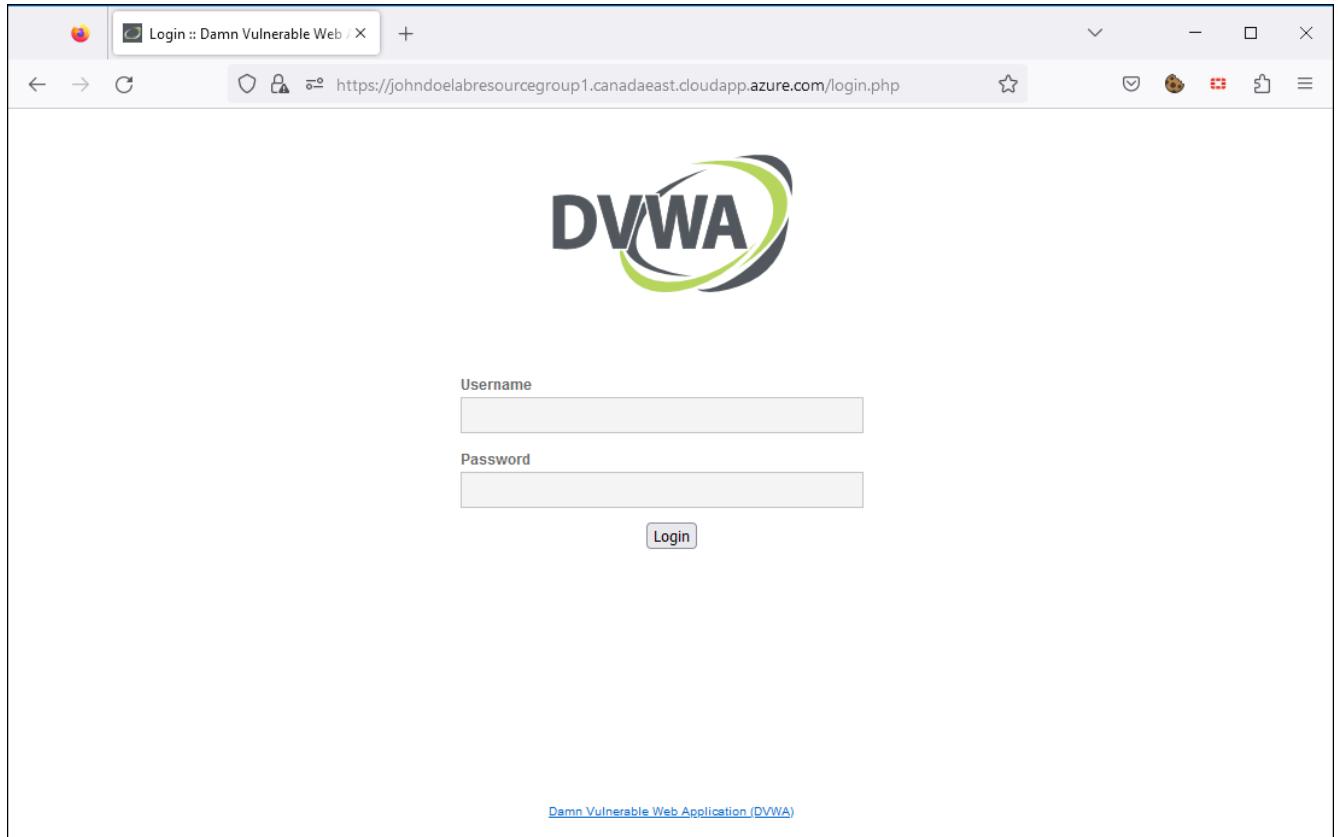
The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the URL 'Home > FWBAPClusterPublicIP | Configuration' is visible. On the left, a sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Settings' (which is expanded), 'Configuration' (which is selected and highlighted with a red box), 'Properties', and 'Locks'. The main content area shows 'IP address assignment' set to 'Static' with 'IP address' as '20.25.60.133'. Below that is an 'Idle timeout (minutes)' slider set to '4'. At the bottom, there's a 'DNS name label (optional)' input field containing 'xpaca94', which is also highlighted with a red box. To the right of the input field, the text '.eastus.cloudapp.azure.com' is displayed. At the very bottom of the configuration page, there are 'Save', 'Discard', and 'Refresh' buttons.

Ensure that your environment is operational

Ensure your environment is set up correctly by following this three-step checklist.

- 1 - You should be able to navigate to the DVWA application: <https://@PREFIX.@REGION.cloudapp.azure.com>

If you encounter a FortiWeb block page, clear your browser cache and try again.



DVWA

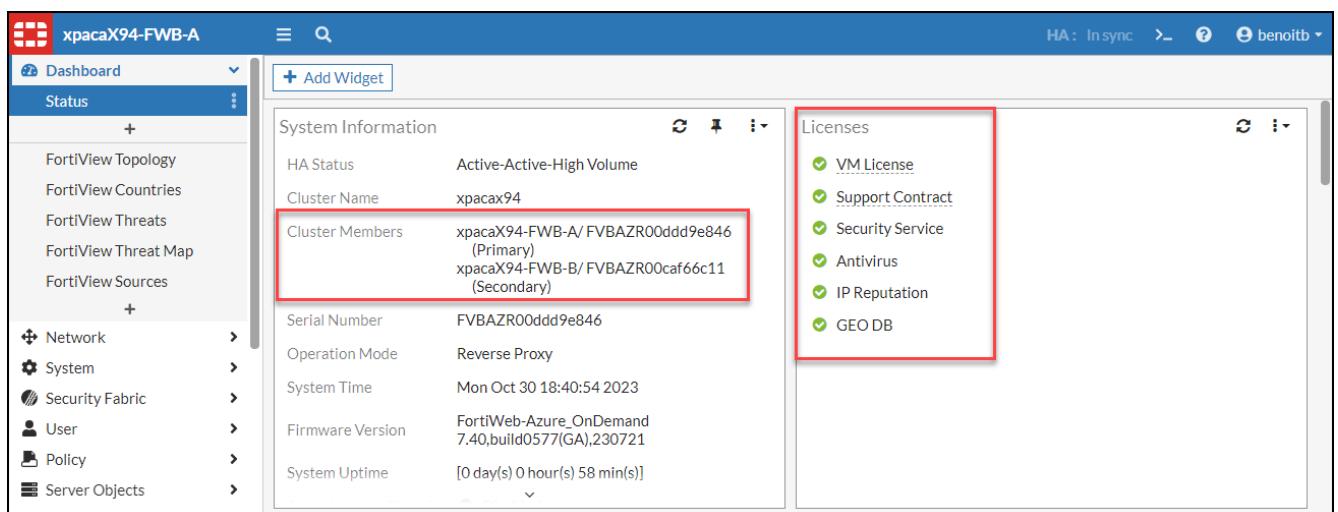
Username

Password

Login

Damn Vulnerable Web Application (DVWA)

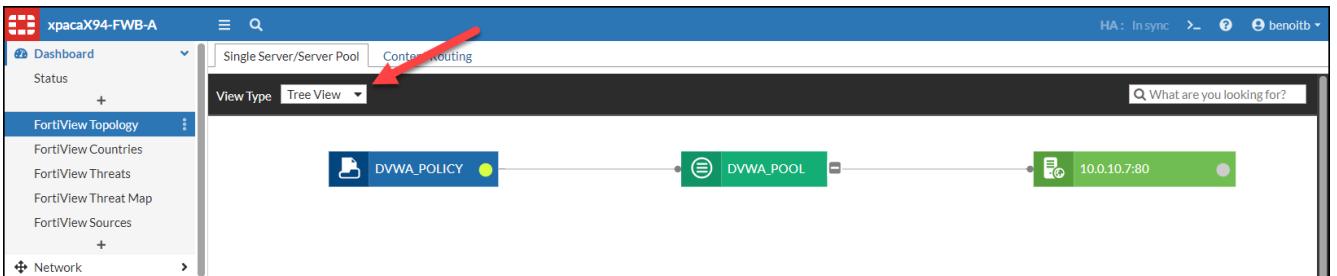
- 2 - Verify the presence of the two FortiWeb instances on the main dashboard by navigating to [Dashboard > Status](#). Additionally, check the status of your license. **Note:** we are using PAYG License model for this Lab.



System Information	
HA Status	Active-Active-High Volume
Cluster Name	xpacax94
Cluster Members	xpacaX94-FWB-A/FVBAZR00ddd9e846 (Primary) xpacaX94-FWB-B/FVBAZR00caf66c11 (Secondary)
Serial Number	FVBAZR00ddd9e846
Operation Mode	Reverse Proxy
System Time	Mon Oct 30 18:40:54 2023
Firmware Version	FortiWeb-Azure_OnDemand 7.40,build0577(GA),230721
System Uptime	[0 day(s) 0 hour(s) 58 min(s)]

Licenses	
VM License	✓
Support Contract	✓
Security Service	✓
Antivirus	✓
IP Reputation	✓
GEO DB	✓

- 3 - Verify the topology by going to the menu [Dashboard > FortiView Topology](#)



If you encounter any issues, refer to the following troubleshooting sections or consult your instructor.

Troubleshooting - What to do if the cluster is not operational?

During the initial startup, there's a possibility that **ARP on port2** may malfunction, which could render the cluster inoperative, as port2 is deemed faulty. In such cases, you'll need to restart both FortiWeb VMs via the Azure console.

Note that restarting the FortiWebs from the GUI will not resolve the ARP issue; only a restart from the Azure portal will fix it.

Navigate to the **Virtual Machines** menu in the Azure portal. Select the two FortiWeb VMs and click on **Restart**.

The screenshot shows the Microsoft Azure Virtual Machines list page. Two specific VMs, xpaca94-FWB-A and xpaca94-FWB-B, are selected and highlighted with a red box. A large red arrow points from these selected VMs to the 'Restart' button in the top toolbar. The table lists the following information for each VM:

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
xpaca94-DVWA	Virtual machine	FTNT-Training	xpaca94-blueprint	East US	Running	Linux	Standard_F2s_v2	-	1
xpaca94-FGT-A	Virtual machine	FTNT-Training	xpaca94-blueprint	East US	Running	Linux	Standard_F4s	4.157.173.242	2
xpaca94-FGT-B	Virtual machine	FTNT-Training	xpaca94-blueprint	East US	Running	Linux	Standard_F4s	4.157.173.242	2
xpaca94-FWB-A	Virtual machine	FTNT-Training	xpaca94-blueprint	East US	Running	Linux	Standard_F4s	20.25.60.133	2
xpaca94-FWB-B	Virtual machine	FTNT-Training	xpaca94-blueprint	East US	Running	Linux	Standard_F4s	20.25.60.133	2

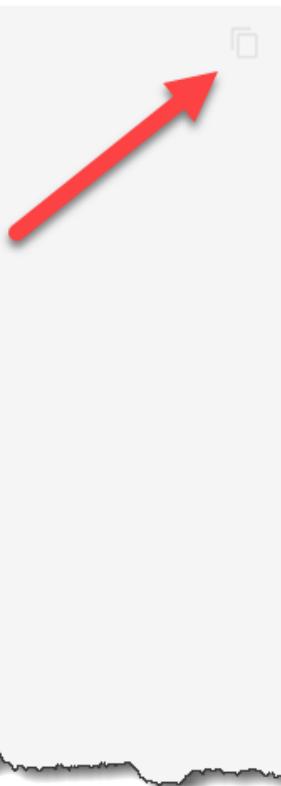
Troubleshooting - What to do if there is no policy in place, or if DVWA is not accessible?

The FortiWeb configuration, including the WAF policy, is automatically loaded when the VM is created. We achieve this by using the Azure **cloud-init** feature. Cloud-init is a widely used method for customizing a VM as it boots for the first time. However, there may be circumstances where the configuration doesn't load correctly. If this happens to you, you can simply manually import our configuration file.

- 1 - Navigate to the [bootstrap page](#)
- 2 - Copy **Part 2** of the configuration to your clipboard

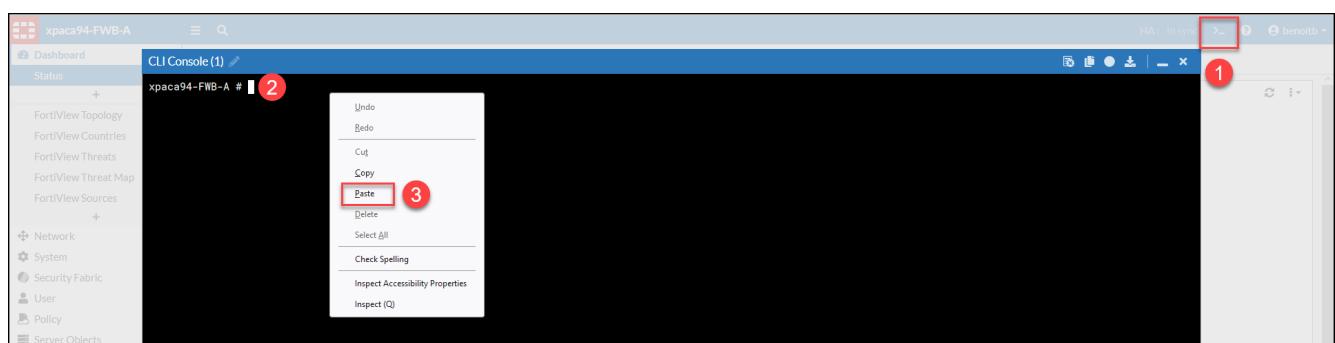
Part2 : General Configuration Settings for All Users

```
config system global
set admintimeout 480
set timezone 12
end
config log traffic-log
set status enable
set packet-log enable
end
config system fortigate-integration
set server 10.0.4.5
set port 443
set protocol HTTPS
set username admin
set password password
set flag enable
end
config system feature-visibility
set wvs enable
set fortigate-integration enable
end
config waf url-access url-access-rule
```

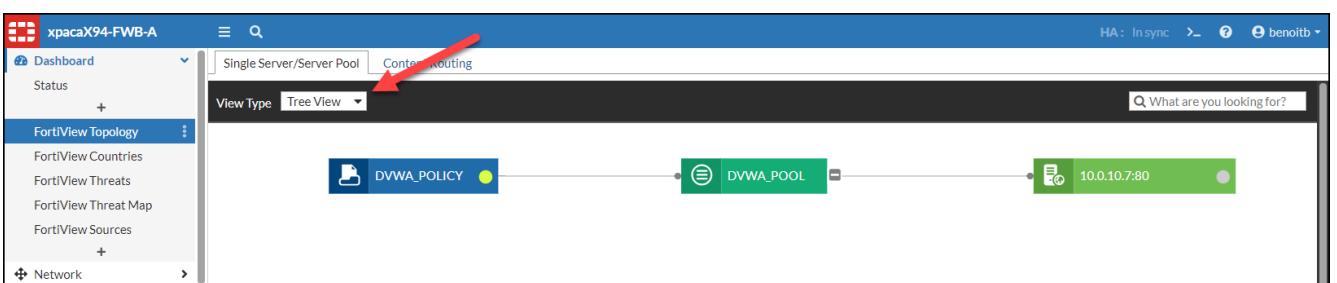


- 3 - Connect to [your FortiWeb instance](#), and open the CLI console located in the upper left corner

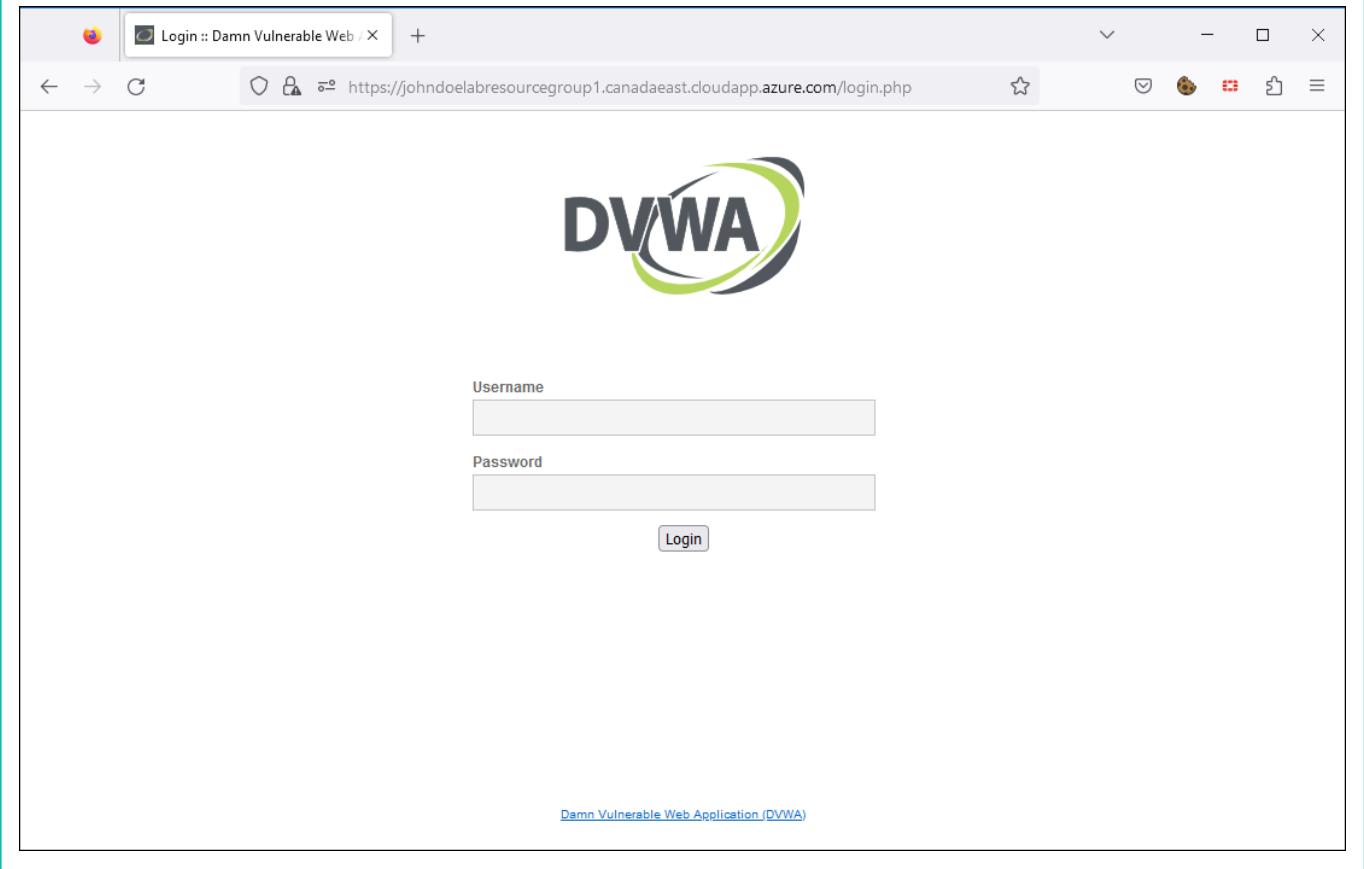
- 4 - Paste the copied configuration into the console



- 5 - Navigate to [Dashboard > FortiView Topology](#) and verify that the policy is now displayed



6 - You should be able to navigate to the DVWA application: <https://@PREFIX.@REGION.cloudapp.azure.com>



Troubleshooting - Delete and rebuild your Lab Environment

Here's the process to follow if you need to delete and rebuild your Lab environment:

Do not delete the resource group itself, as you won't be able to recreate it.

- Navigate to the Azure portal
- Choose your resource group, identified as **@RESOURCE_GROUP_NAME**
- Select all the resources within the group
- Click on **Delete**

Name	Type	Location
dvwa5f674bmxbikm	Storage account	East US
fgtsc5f674bmxbikm	Storage account	East US
FWBAPClusterPublicIP	Public IP address	East US
fwbsc5f674bmxbikm	Storage account	East US
xpacaX94-5f674bmxbikm-NSG	Network security group	East US
xpacaX94-DVWA	Virtual machine	East US
xpacaX94-DVWA-NIC	Network Interface	East US
xpacaX94-DVWA_OsDisk_1_f4a6af67b56046a98f4d2b3dec98f7a6	Disk	East US

- Opt for **Apply force delete for selected Virtual machines and Virtual machine scale sets**
- Type **delete** to confirm deletion
- Click on **Delete**

The selected resources along with their related resources and contents will be permanently deleted. If you are unsure of the selected resource dependencies, navigate to the individual resource page to perform the delete operation. More details of the resource dependencies are available in the manage experience.

Resources to be deleted (45)

Name	Resource type	Remove
dvwa5f674bmxblxm	Storage account	Remove
fgtsc5f674bmxblxm	Storage account	Remove
FWBAPClusterPublicIP	Public IP address	Remove
fwbsc5f674bmxblxm	Storage account	Remove
xpacaX94-5f674bmxblxm-NSG	Network security gr...	Remove
xpacaX94-DVWA	Virtual machine	Remove
xpacaX94-DVWA-NIC	Network Interface	Remove
xpacaX94-DVWA_OsDisk_1_f4a6af67b56046a98f4d2b3dec98f7a6	Disk	Remove
xpacaX94-FGT-A	Virtual machine	Remove

Apply force delete for selected Virtual machines and Virtual machine scale sets [\(i\)](#)

Enter "delete" to confirm deletion *

Delete **Cancel**

- Wait for the deletion process to complete

More events in the activity log →

Executed delete command on 45 selected items

Succeeded: 45, Failed: 0, Canceled: 0.

a few seconds ago

Dismiss all

- Navigate to [Azure Cloud Shell](#) and make sure you are in the **fortinetCloudBlueprint** folder

```
cd fortinetCloudBlueprint
```

- Redeploy the template using the following command

```
az deployment group create --name fortinetCloudBlueprint --resource-group @RESOURCE_GROUP_NAME --template-file 000-main.bicep
```

Check your System Configuration (optional)

Once you have access to the FortiWeb GUI, those are the main menu to check your system configuration.

Configuration	Menu
FortiWeb Network Access	Network > Interface
Routing	Network > Static Route
DNS Configuration	Network > DNS
VM License	Dashboard > Status > Licenses > Update VM License
FortiGuard Status and Updates	System > Config > FortiGuard
Time Zone Setting	System > Maintenance > System Time
Timeout Setting	System > Admin > Settings > Idle Timeout
Firmware Version	System > Maintenance > Firmware

Check your Application Policy (optional)

During the Bicep deployment, we imported this [bootstrap](#). Those are the main menus to check your Application Policy:

Configuration	Menu
Virtual IP	Network > Virtual IP
Virtual Server	Server Objects > Virtual Server
Server Pool	Server Objects > Server Pool
Signature	Web Protection > Known Attacks > Signatures
Web Protection Profile	Policy > Web Protection Profile
Policy	Policy > Server Policy

Initializing DVWA

Initialize DVWA database and authenticate

Connect to <https://@PREFIX.@REGION.cloudapp.azure.com/setup.php>

Click **Create / Reset Database**

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful

Please [login](#).



Username

Password

Click **Login** and authenticate with any of these accounts:

Username	Password
admin	password
gordonb	abc123
1337	charley
pablo	letmein
smithy	password

You should be directed to the welcome page.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!



How to install DVWA in another Lab Environment?

If you are not using the  Azure Fortinet Cloud Blueprint, you can install your own DVWA instance.

The most straightforward way to install DVWA is by utilizing Docker. Install any Linux distribution with Docker and run those 2 commands:

```
sudo docker pull vulnerables/web-dvwa
sudo docker run -d --restart unless-stopped -p 80:80 vulnerables/web-dvwa
```

You can explore additional deployment options on the official  [DVWA GitHub](#).

3. Hands on Labs

3.1 Protecting Web Application Using Azure Network Security Groups and FortiGate

Accessing DVWA via NSG's

The first step in this exercise will be to create a Network Security Group and associate it to the subnet where the DVWA instance is deployed.



Click on the images to view them in a larger format.

Creating a Network Security Group

In the search bar type **Network Security Groups**, and select the non-classic option.

The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, there is a search bar with the text 'Network Security Groups'. Below the search bar, there are several tabs: 'All', 'Services (43)', 'Marketplace (2)', 'Documentation (99+)', 'Resources (0)', and 'Resource Groups (0)'. Under the 'Services' section, there are two options: 'Network security groups (classic)' and 'Network security groups'. The 'Network security groups' option is highlighted with a red box. To the right of these options, there are links for 'Application security groups', 'Groups', 'Virtual networks', 'Security', and 'Application groups'. At the bottom of the service list, there are buttons for 'See all services' and 'More services'.

Create a new Security Group.

The screenshot shows the 'Network security groups' page in the Microsoft Azure portal. At the top, there is a search bar with the placeholder 'Search resources, services, and docs (G+)'. Below the search bar, there are buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. There are also filter options: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. On the right side, there are grouping and view mode buttons: 'No grouping' and 'List view'. The main table lists two existing Network Security Groups: 'xpaca94-5f674bmxblxm-NSG' and 'xpaca94-NSG-Allow-All'. Each entry includes columns for 'Name', 'Resource group', 'Location', 'Subscription', and 'Flow log'. The 'xpaca94-NSG-Allow-All' entry has a red box around its 'Name' column.

Select the Resource Group @**RESOURCE_GROUP_NAME** and give the Network Security Group a **unique name**.

Review +Create the Resource.

The screenshot shows the 'Create network security group' wizard in the Microsoft Azure portal. At the top, there are tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is selected. Under 'Project details', there is a 'Subscription' dropdown set to 'FTNT-Training' and a 'Resource group' dropdown set to 'xpaca94-blueprint'. Under 'Instance details', there is a 'Name' field set to 'BluePrintDemo94-NSG' and a 'Region' dropdown set to 'East US'. Both the 'Name' and 'Region' fields have red boxes around them. At the bottom of the page, there are buttons for 'Review + create' (highlighted with a red box), '< Previous' and 'Next : Tags >', and 'Download a template for automation'.

Once created, Click on **Go to Resource** to be redirected to your newly created NSG.

Microsoft.NetworkSecurityGroup-20231026160518 | Overview

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20231026160518
Subscription : FTNT-Training
Resource group : xpaca94-blueprint

Start time : 10/26/2023, 4:10:57 PM
Correlation ID : 9d80a5bd-d4ea-4bf7-915f-1e7c41f6966e

Deployment details

Next steps

Go to resource

Give feedback

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
[Set up cost alerts >](#)

Microsoft Defender for Cloud
Secure your apps and infrastructure
[Go to Microsoft Defender for Cloud >](#)

Navigate to the **Inbound Security Rules** menu Item.

BluePrintDemo94-NSG | Inbound security rules

Network security group

+ Add

Priority ↑	Name ↑	Port ↑↓	Protocol == all	Source == all	Destination == all	Action == all
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Create new entries to allow **HTTP**, **HTTPS**, **SSH** services from any sources.

AllowAnyHTTPInbound	AllowAnyHTTPSInbound	AllowAnySSHInbound
Source = Any	Source = Any	Source = Any
Source Port = Any	Source Port = Any	Source Port = Any
Destination = Any	Destination = Any	Destination = Any
Service = HTTP	Service = HTTPS	Service = SSH
Action = Allow	Action = Allow	Action = Allow

Add inbound security rule

BluePrintDemo94-NSG

Source ⓘ

Source port ranges * ⓘ

Destination ⓘ

Service ⓘ

Destination port ranges ⓘ

Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

Priority * ⓘ

Name *

Description

Add Cancel Give feedback

Once you've created the corresponding rules, you'll see your rules, in addition to the rules Azure had implicitly configured:

Microsoft Azure Network Security Group (NSG) settings showing Inbound security rules. The table lists the following rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
110	AllowAnyHTTPSInbound	443	TCP	Any	Any	Allow
120	AllowAnySSHInbound	22	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Navigate to the **Subnets** menu and **Associate** the Network security group to the **DMZProtectedA** Subnet.

Microsoft Azure Network Security Group (NSG) settings showing Subnets. The Subnets menu is selected (1). The Associate button is highlighted (2). The Associate subnet dialog shows the Virtual network (xpaca94-VNET) and Subnet (DMZProtectedA) selected (3). The OK button is highlighted (4).

Microsoft Azure Network Security Group (NSG) settings showing Subnets. The Subnets table now includes a row for the DMZProtectedA subnet, which is highlighted (1).

Name	Address range	Virtual network
DMZProtectedA	10.0.10.0/24	xpaca94-VNET

Testing your Network Security Group

In Azure CLI, print your deployment **Outputs** and click on <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com>

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

Log in to DVWA using the credentials **admin** and **password**.



The DVWA logo consists of the letters 'DVWA' in a bold, dark grey sans-serif font. The letter 'D' is partially overlaid by a thick, swooping green line that starts from the bottom left and curves upwards and to the right, ending under the 'V'.

Username
<input type="text" value="admin"/>
Password
<input type="password" value="*****"/>
<input type="button" value="Login"/>

Navigate to the **SQL Injection** menu item and type:

The screenshot shows the DVWA application interface. On the left is a sidebar with various menu items, some in grey boxes and one in a green box: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, **SQL Injection** (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout.

The main content area has a title "Vulnerability: SQL Injection". Below it is a form with a red border containing a "User ID" input field with the value "' OR 1=1#", a "Submit" button, and a "More Information" section with a list of links.

At the bottom, there is a status bar with "Username: admin|", "Security Level: low", "PHPIDS: disabled", and two buttons: "View Source" and "View Help".

The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.10 *Development*".

Notice the attack was not prevented.

Vulnerability: SQL Injection

User ID: Submit

ID: ' OR 1=1#
First name: admin
Surname: admin

ID: ' OR 1=1#
First name: Gordon
Surname: Brown

ID: ' OR 1=1#
First name: Hack
Surname: Me

ID: ' OR 1=1#
First name: Pablo
Surname: Picasso

ID: ' OR 1=1#
First name: Bob
Surname: Smith

Why? After the NSG permitted access to the DVWA Workload on Port 80 (HTTP) no subsequent inspection occurred.

Accessing DVWA via FortiGate

Now, we will execute the same attack, but this time, we will secure the DVWA Workload behind the FortiGate Firewall.

Testing SQL Injection Attack

Log in to the Primary FortiGate using the credentials you established during deployment.

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

Once logged in to the FortiGate, edit the firewall policy named **DVWA-HTTP-Inbound_Access**. Enable all the security profiles with their default settings.

Edit Policy

Name: DVWA-HTTP-Inbound_Access

Type: Standard

Incoming Interface: port1

Outgoing Interface: port2

Source: all

IP/MAC Based Access Control: Disabled

Logical And With Secondary Tags: Specify

Destination: DVWA-HTTP-VIP

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

Firewall/Network Options:

NAT:

Protocol Options: PROT default

Security Profiles:

AntiVirus	AV default	<input type="button" value="edit"/>
Web Filter	WEB default	<input type="button" value="edit"/>
DNS Filter	DNS default	<input type="button" value="edit"/>
Application Control	APP default	<input type="button" value="edit"/>
IPS	IPS default	<input type="button" value="edit"/>
File Filter	FF default	<input type="button" value="edit"/>

Click OK to apply the changes.

Browse again to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/sql/> and enter this **SQL injection** attack into the form.

' OR 1=1#



Vulnerability: SQL Injection

User ID: ' OR 1=1#

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_Injection
- <http://bobby-tables.com/>

Username: admin | Security Level: low | PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Notice that the page is hung.

Let's dive deeper and look at the FortiGate's Log. Open the **Security Events**, select the **Logs** tab and use the **Intrusion Prevention** filter.

The screenshot shows the FortiGate Management Interface. The left sidebar is titled "blueprintdemo-FGT-A" and includes sections for Dashboard, Network, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, Log & Report (with "Security Events" highlighted), Reports, and Log Settings. The main area has tabs for "Summary" and "Logs". The "Logs" tab is active, showing a table of log entries. A specific entry from 2023/10/03 at 13:02:14 is selected, showing details about a dropped attack. The "Intrusion Prevention" section of the right panel highlights the attack name "HTTPURLSQLInjection". The "Message" field in the detailed view is also highlighted with a red box and contains the text "web_msc: HTTP.URL.SQL.Injection". Other fields in the message detail include "Profile: default", "Attack Name: HTTPURLSQLInjection", "Attack ID: 15621", "Reference: http://www.fortinet.com/ids/VID15621", "Incident Serial: 132,120,580", "Direction: outgoing", and "Severity: High". The "Log Details" section indicates a "Policy Type: Firewall".

Why was this attack dropped? The attack triggered a signature set to block within the FortiGate's IPS Security Profile.

Testing Command Injection Attack

Now lets try a **Command Injection** attack.

Browse to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/exec/> and enter this **Command injection** attack into the form.

;/ps aux

DVWA

Vulnerability: Command Injection

Ping a device

Enter an IP address:

More Information

- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://www.owasp.org/index.php/Command_Injection

Username: admin
Security Level: low
PHPIDS: disabled

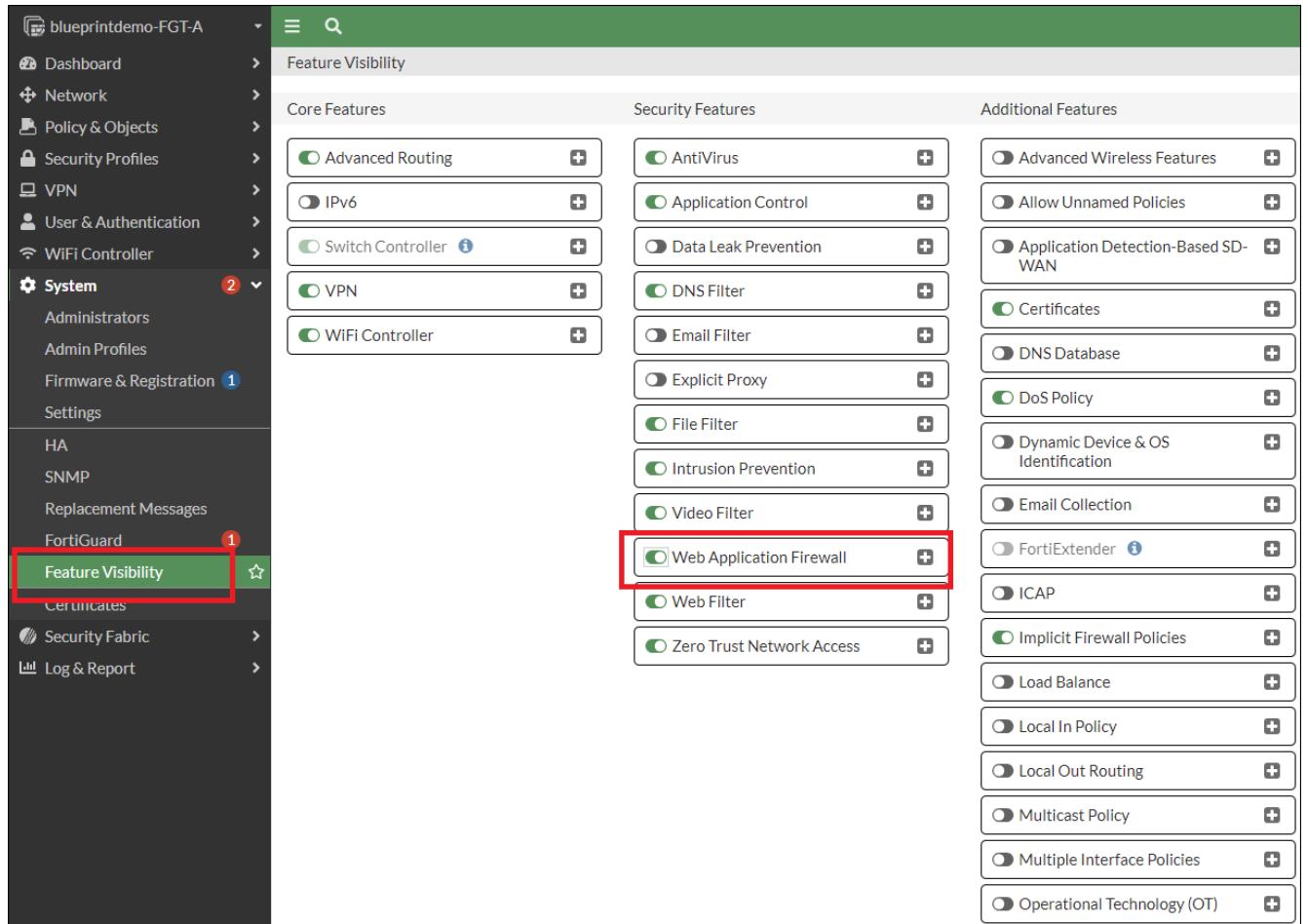
[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Why was the attack let through? The attack did not match a known IPS signature. Let's enhance the capabilities of the FortiGate by activating the **Web Application Firewall** security profile.

Enable WAF on FortiGate

Enable the **Web Application Firewall** Security Profile from System -> Feature Visibility



The screenshot shows the Feature Visibility page in the FortiGate management interface. The left sidebar shows the navigation path: blueprintdemo-FGT-A > System > Feature Visibility. The main content area is titled "Feature Visibility" and contains three columns: Core Features, Security Features, and Additional Features. In the Core Features column, "Advanced Routing", "IPv6", "Switch Controller", "VPN", and "WiFi Controller" are listed. In the Security Features column, "AntiVirus", "Application Control", "Data Leak Prevention", "DNS Filter", "Email Filter", "Explicit Proxy", "File Filter", "Intrusion Prevention", "Video Filter", and "Web Application Firewall" are listed. The "Web Application Firewall" checkbox is checked and highlighted with a red border. In the Additional Features column, "Advanced Wireless Features", "Allow Unnamed Policies", "Application Detection-Based SD-WAN", "Certificates", "DNS Database", "DoS Policy", "Dynamic Device & OS Identification", "Email Collection", "FortiExtender", "ICAP", "Implicit Firewall Policies", "Load Balance", "Local In Policy", "Local Out Routing", "Multicast Policy", "Multiple Interface Policies", and "Operational Technology (OT)" are listed.

Once enabled, go back to the **Firewall Policy** and edit the **DVWA-HTTP-Inbound_Access** Firewall Policy.

Toggle the **Inspection Mode** to **Proxy-Based** and enable the default **Web Application Firewall** Security Profile.

Name i DVWA-HTTP-Inbound_Access

Type Standard ZTNA

Incoming Interface port1

Outgoing Interface port2

Source all

IP/MAC Based Access Control i

Logical And With Secondary Tags Disabled Specify

Destination DVWA-HTTP-VIP

Schedule always

Service ALL

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Firewall/Network Options

NAT

Protocol Options PROT default

Security Profiles

AntiVirus	<input checked="" type="checkbox"/> AV default
Web Filter	<input checked="" type="checkbox"/> WEB default
Video Filter	<input type="checkbox"/>
DNS Filter	<input checked="" type="checkbox"/> DNS default
Application Control	<input checked="" type="checkbox"/> APP default
IPS	<input checked="" type="checkbox"/> IPS default
File Filter	<input checked="" type="checkbox"/> FF default
Web Application Firewall	<input checked="" type="checkbox"/> WAF default

Browse to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/exec/> and enter the **Command injection** attack again.

```
;ps aux
```

The **Command Injection** should now be prevented.



Web Application Firewall

This transfer is blocked by a Web Application Firewall.

This transfer is blocked.

URL http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com/vulnerabilities/exec/

Event ID 50050034

Event Type signature

The attack is blocked because WAF signatures have been activated.

Conclusion

Did you notice that all of the attacks stopped by the FortiGate were all stopped based on existing signatures?

Demonstrating non-signature based attacks via FortiGate

In this section, we will demonstrate various web application attacks to showcase and highlight the significance of the protections the Fortiweb will bring when compared to its Next Generation Firewall counterpart.

CSRF Attack via FortiGate

 **What is Cross site request forgery (CSRF) attack?**

Cross-Site Request Forgery (CSRF) is a type of security vulnerability that dupes a web browser into executing an undesired action within an authenticated application.

The attack usually involves deceptive social engineering tactics, such as sending a misleading email or link to the victim. Because the user is already authenticated within the application when the attack occurs, it becomes challenging to differentiate between legitimate and fraudulent requests.

How Cross Site Request Forgeries (CSRFs) Work



① A hacker creates a request (in the form of a URL) for their own benefit from a website

② Hacker embeds that request into a hyperlink and sends it to a visitor who they hope is logged in to the site

③ The website visitor clicks the link, unwittingly sending the request to the site

④ Assuming the request is legitimate, the website fulfills the request, sending data, funds, or access to the hacker

Authenticating to the Web Application

To successfully run the CSRF Attack, you must first authenticate yourself within the application.

Browse to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com> and log in using the username **admin** and password **password**.

Troubleshooting - If you encounter any authentication issues

- Browse to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/setup.php>
- Click on **Create / Reset Database**

The screenshot shows the DVWA setup page. On the left, a sidebar lists several messages indicating successful database setup: "Database has been created.", "'users' table was created.", "Data inserted into 'users' table.", "'guestbook' table was created.", "Data inserted into 'guestbook' table.", "Backup file /config/config.inc.php.bak automatically created", "Setup successful!", and "Please [login](#)". The "Create / Reset Database" button at the top of the sidebar is highlighted with a red box. A large red arrow points from the "Please login" link in the sidebar to the "Login" button on the main form. The main form includes fields for "Username" and "Password", and a "Login" button. The DVWA logo is visible in the background.

Executing CSRF Attack

Once authenticated to DVWA, click on the **LINK** below to generate the attack.



Dear user,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active

follow the **LINK** Sign in Re-activate your account to Outlook.

Thanks,

The Microsoft account team

The link employs **Cross-Site Request Forgery** to exploit your authenticated session in order to initiate a password change.

DVWA

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed.

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
- <http://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery

Username: admin
Security Level: low
PHPIDS: disabled

Logout

View Source **View Help**

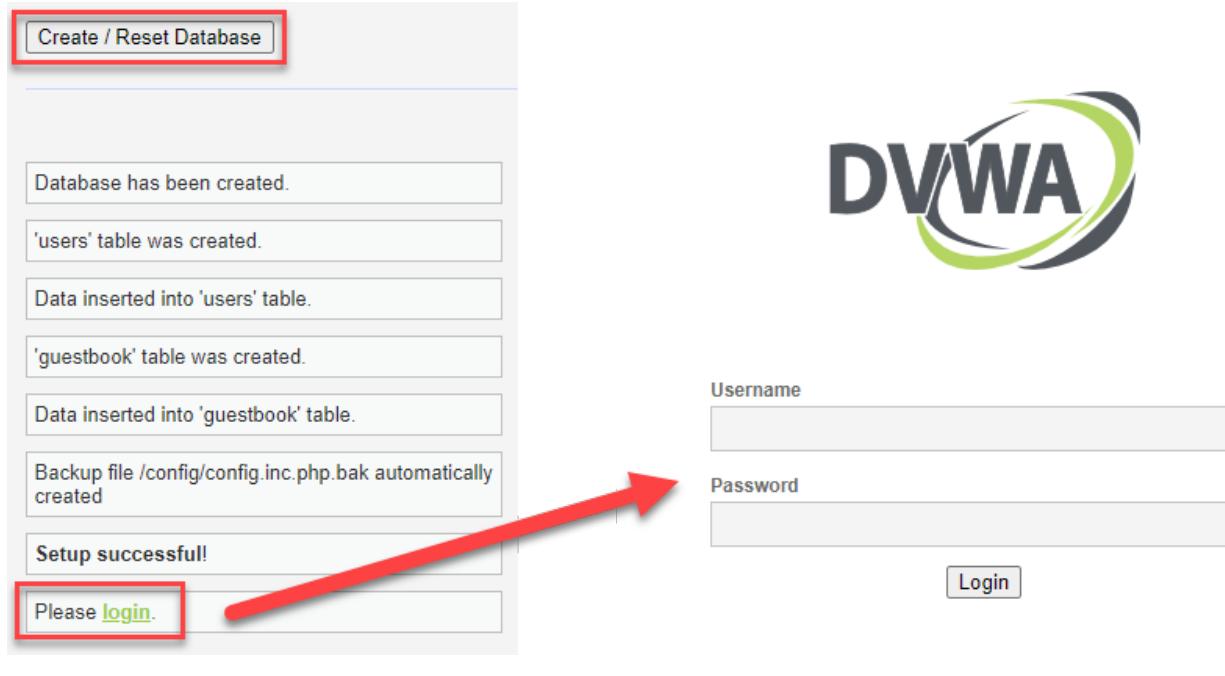
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Your password has been changed without your knowledge.

Logout of DVWA and Log back in using admin:pwned

Resetting the database for the next Lab

- Browse to <http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/setup.php>
- Click on **Create / Reset Database**
- You can now login with the original password



The screenshot shows the DVWA setup page. A red box highlights the "Create / Reset Database" button. Below it, a red arrow points from the "Please login" button on the left to the login form on the right. The DVWA logo is visible at the top right.

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

Please [login](#).

DVWA

Username

Password

Conclusion

We have observed that FortiGate provides an additional layer of protection compared to NSGs, thanks to its WAF signatures. However, we can see that more advanced attacks like CSRF are not addressed by FortiGate.

Cookie Poisoning via FortiGate

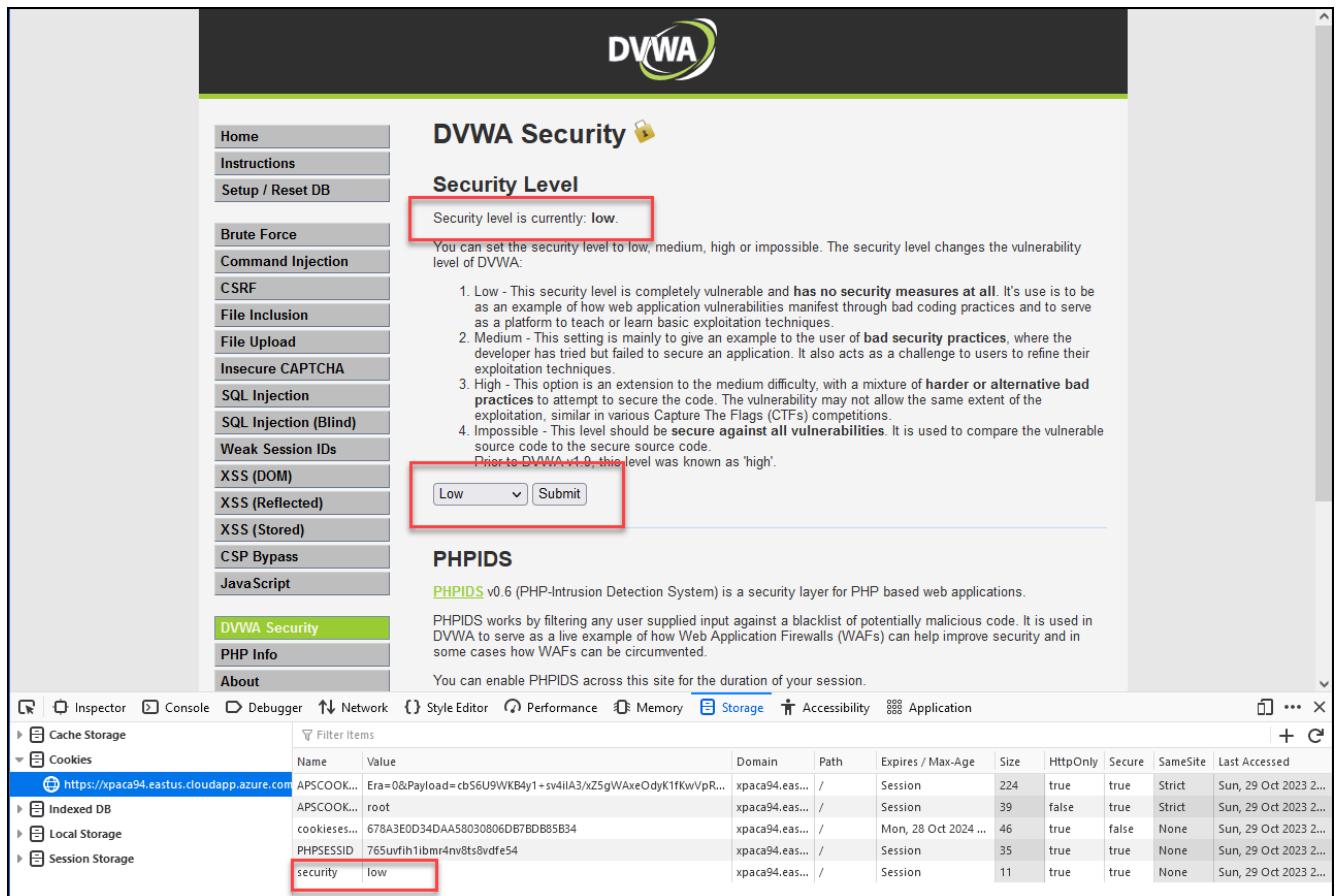
What is Cookie Poisoning?

In this lab, we will delve into the world of cookies - data stored in a user's browser that is specific to a website and session. These cookies serve a variety of purposes, from tracking user behavior to personalizing the online experience. However, they are also susceptible to cookie poisoning, a form of unauthorized manipulation by attackers aiming to gain access to sensitive information or services. This is particularly concerning because cookies often contain authentication data and other sensitive details, making them a prime target for hackers.

Changing Security Level Through Legitimate Web App Interactions

Browse to @PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/security.php

Right click the page and select **Inspect**, go to **Storage** (Firefox) or **Application** (Chrome, Edge) and select **Cookies**.



The screenshot shows the DVWA Security Level page. On the left is a sidebar with various exploit categories like Brute Force, Command Injection, and SQL Injection. The main area has a heading 'DVWA Security' with a lock icon. Below it is a section titled 'Security Level' containing the message 'Security level is currently: low.' A red box highlights this message. Further down, there's a detailed description of the four security levels (Low, Medium, High, Impossible) and a note about the history of the 'high' level. A red box highlights the 'Low' dropdown menu and the 'Submit' button. At the bottom, there's a section for PHPIDS.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented. You can enable PHPIDS across this site for the duration of your session.

At the bottom of the page, a browser developer tools window is open under the 'Storage' tab, showing the cookies for the current session. A red box highlights the 'security' cookie entry, which has the value 'low'.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
APSCOOK...	Era=0&Payload=cb56U9WKb4y1+sv4ilA3/xZ5gWAxeOdyK1fKwVpR...	xpac94.eas...	/	Session	224	true	true	Strict	Sun, 29 Oct 2023 2...
APSCOOK...	root	xpac94.eas...	/	Session	39	false	true	Strict	Sun, 29 Oct 2023 2...
cookieses...	678A3E0D34DAA58030806DB7BDB85B34	xpac94.eas...	/	Mon, 28 Oct 2024 ...	46	true	false	None	Sun, 29 Oct 2023 2...
PHPSESSID	765uwh11bmrr4nv8ts0vfe54	xpac94.eas...	/	Session	35	true	true	None	Sun, 29 Oct 2023 2...
security	low	xpac94.eas...	/	Session	11	true	true	None	Sun, 29 Oct 2023 2...

The security level granted to the user is stored in the cookie.

From the **Web page**, select **Medium** and click **submit**. This is a legitimate action, and your security level has changed.

DVWA Security

Security Level

Security level is currently: **medium**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA.

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
 Prior to DVWA v1.0.1 this level was known as 'high'.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

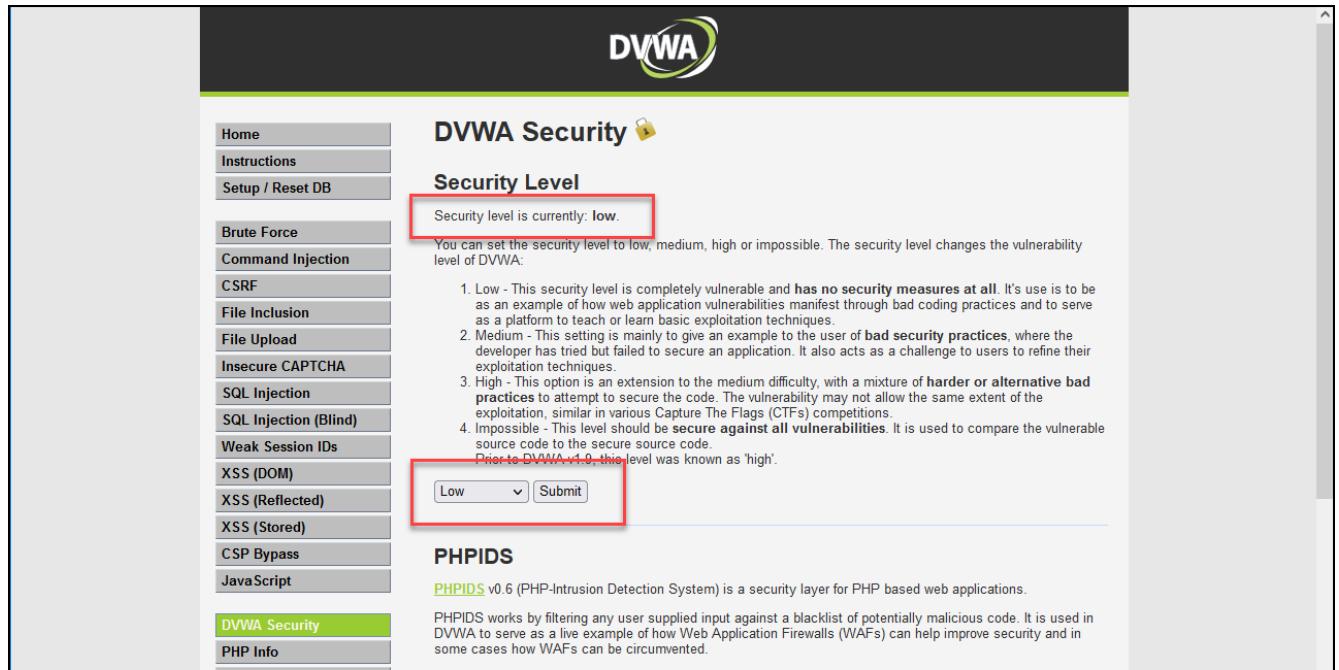
Storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
APSCOOK...	Era=0&Payload=cbS6U9WKB4y1+sv4IIA3/xZ5gWAxeOdyKtKwVpR...	xpac94.eas...	/	Session	224	true	true	Strict	Sun, 29 Oct 2023 2...
APSCOOK...	root	xpac94.eas...	/	Session	39	false	true	Strict	Sun, 29 Oct 2023 2...
cookieses...	678A3E0D34DAA58030806DB7BDB85B34	xpac94.eas...	/	Mon, 28 Oct 2024 ...	46	true	false	None	Sun, 29 Oct 2023 2...
PHPSESSID	765uvfih1ibmr4nv0ts0vdf54	xpac94.eas...	/	Session	35	true	true	None	Sun, 29 Oct 2023 2...
security	medium	xpac94.eas...	/	Session	14	true	true	None	Sun, 29 Oct 2023 2...

Change from low to medium

Overriding Security Level with Malicious Cookie Manipulation

Instead, now change the **security cookie** value manually to **low** and **reload** the page.



The screenshot shows the DVWA Security Level page. A red box highlights the message "Security level is currently: low." Below it, a red box highlights the dropdown menu where "Low" is selected. The dropdown menu has "Low" and "Submit" buttons.

Storage Type	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Cookies	https://xpaca94.eastus.cloudapp.azure.com/.ASPSESSIONID	Era=0&Payload=cbS6U9WKb4y1+sv4IIA3/xZ5gWAxeOdyK1fKwVpR...	xpaca94.eas...	/	Session	224	true	true	Strict	Sun, 29 Oct 2023 2...
Cookies	APSCOOK...	root	xpaca94.eas...	/	Session	39	false	true	Strict	Sun, 29 Oct 2023 2...
Local Storage	cookieses...	678A3E0D34DAA58030806DB7BDB85B34	xpaca94.eas...	/	Mon, 28 Oct 2024 ...	46	true	false	None	Sun, 29 Oct 2023 2...
Session Storage	PHPSESSID	765uvfh1ibmr4nv8ts0vdfe54	xpaca94.eas...	/	Session	35	true	true	None	Sun, 29 Oct 2023 2...
Session Storage	security	low	xpaca94.eas...	/	Session	11	true	true	None	Sun, 29 Oct 2023 2...

Notice we were able change the DVWA's security setting by tampering with the value of the **security cookie**.

Hidden Fields Manipulation via FortiGate

What is Hidden Fields

Hidden form inputs are often written into an HTML page by the web server when it serves that page to the client and are not visible on the rendered web page. Because HTTP is essentially stateless, like cookies, hidden form inputs are one way that web applications can use to remember session data from one page request to the next (called “persistence”).

Since they are not rendered visible, hidden inputs are sometimes erroneously perceived as safe. But like session cookies, hidden form inputs store the software’s state information client-side, instead of server-side. This makes it vulnerable.

Enforcing File Size Limitations - Successfully Blocking a Large File Upload

Download those 2 images to your computer:

- [Small Image](#) (14Ko)
- [Large Image](#) (433Ko)

Go to <https://fbw.canadaeast.cloudapp.azure.com/vulnerabilities/upload> and upload the two images one at a time.

The screenshot shows the DVWA File Upload interface. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, **File Upload**, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), and Weak Session IDs. The 'File Upload' option is highlighted. The main content area has a heading 'Vulnerability: File Upload' and a sub-section 'Choose an image to upload:' with a 'Browse...' button and an 'Upload' button. A message box contains the text '.../.../hackable/uploads/small.png successfully uploaded!' which is highlighted with a red border.

The screenshot shows the DVWA File Upload interface again. The sidebar menu is identical to the first screenshot. The main content area has a heading 'Vulnerability: File Upload' and a sub-section 'Choose an image to upload:' with a 'Browse...' button and an 'Upload' button. A message box contains the text 'Your image was not uploaded.' which is highlighted with a red border.

The website enforces a policy that prohibits the uploading of images larger than 100 KB. Let's see how we can bypass the policy restrictions.

Bypassing Policy Restrictions to Upload a Large File

Right click the page, select **Inspect**, go to **Inspector** tab (Firefox) or **Element** tab (Chrome, Edge) and find the **MAX_FILE_SIZE** hidden form.

Change the value to **500,000** and try to upload the large image again. Notice you were now able to successfully upload the larger file.

Conclusion

In summary, though the FortiGate is not inherently bound to the use of signatures, many functionalities revolving around Web Applications, IPS and AV are. This means, for attacks that do not have a corresponding signature, the FortiGate will be vulnerable to many unknown attacks.

In the next lab, we will evaluate FortiWeb and explore how to comprehensively protect a web application.

Info

To view the WAF Feature Comparison between FortiWeb and FortiGate, navigate to the [Reference Architecture](#) section.

3.2 Protecting Web Application Using FortiWeb

To begin, we will connect to the DVWA Web Application through FortiWeb.

Connecting to DVWA

Connecting to DVWA

Connect to <https://@PREFIX.@REGION.cloudapp.azure.com> and authenticate with one of these accounts:

Username	Password
admin	password
gordonb	abc123
1337	charley
pablo	letmein
smithy	password

Troubleshooting - If you encounter any authentication issues

- Browse to <https://@PREFIX.@REGION.cloudapp.azure.com/setup.php>
- Click on **Create / Reset Database**

The screenshot shows the DVWA setup page. A red box highlights the 'Create / Reset Database' button. Below it, several messages are displayed in boxes: 'Database has been created.', "'users' table was created.", 'Data inserted into 'users' table.', "'guestbook' table was created.", 'Data inserted into 'guestbook' table.', 'Backup file /config/config.inc.php.bak automatically created', 'Setup successful!', and 'Please [login](#)'. A red arrow points from the 'Please login.' message to the login form on the right.

DVWA

Username

Password

This Hands-on Lab allows us to demonstrate 25+ FortiWeb protections. Let's take a closer look at FortiWeb's sequence of scans.

Sequence of Scans

Sequence of Scans

FortiWeb applies protection rules and performs protection profile scans in the order of execution according to the following list. The second tab **highlights** the security features that will be demonstrated in this Hands-On Lab.

Protections	Highlights
1. TCP Connection Number Limit (TCP Flood Prevention)	
2. Add X-Forwarded-For	
3. Client Management	
4. IP List	
5. IP Reputation	
6. Quarantined source IP addresses	
7. Known Bots	
8. Geo IP	
9. WebSocket protocol	
10. Add HSTS Header	
11. Protected Server Check	
12. Allow Method	
13. Mobile Application Identification	
14. HTTP Request Limit/sec (HTTP Flood Prevention)	
15. TCP Connection Number Limit (Malicious IP)	
16. HTTP Request Limit/sec (Shared IP) (HTTP Access Limit)	
17. HTTP Authentication	
18. Global Object Allow List	
19. ADFS Proxy	
20. URL Access	
21. Mobile API Protection	
22. Padding Oracle Protection	
23. HTTP Protocol Constraints	
24. File Parse	
25. File Security	
26. Web Shell Protection	
27. Parameter Validation	
28. Bot Deception	
29. ML based Bot Detection	
30. Cross-site request forgery (CSRF) attacks	
31. Protection for Man-in-the-Browser (MiTB) attacks	
32. Biometrics Based Detection	
33. XML Protection	
34. JSON Protection	
35. Signatures	
36. SQL/XSS Syntax Based Detection	
37. Site Publish	
38. Hidden Fields Protection	
39. Custom Policy	
40. Threshold Based Detection	
41. User Tracking	
42. API Gateway	
43. OpenAPI Validation	
44. CORS Protection	
45. URL Rewriting (rewriting & redirection)	
46. ML based API Protection	
47. File Compress	
48. Cookie Security Policy	
49. ML based Anomaly Detection	