1. **Secure Web App  ?**

                The web apps created in Azure PaaS are by default public and has general application environment and security , however for added measures we can chose many of the options like mentioned below :

1. **Don’t Want the Web app to be available publicly or want more control over environment ?**

                I would recommend you to create an **App Service environment (ASE)**. Depending upon whether you want your web app to be available internally or externally, choose one of the following:

* [Create External ASE](https://docs.microsoft.com/en-in/azure/app-service/environment/create-external-ase)
* [Create Internal ASE](https://docs.microsoft.com/en-in/azure/app-service/environment/create-ilb-ase)

                   (If you need assistance on **ASE creation**, then please create a ticket our team will assist you with this. )

1. **WAF implementation & IDS :**

Once the ASE is created, I would request you to create a new ticket, so that our peers in the Azure networking can help you with configuring **WAF** and **NSG( also DMZ)** for the VNET in which the ASE was created. Regarding the network watcher, this feature is dependent on which region the **VNET** is hosted in and not on **ASE**. This should address points **1** & **2**.

|  |
| --- |
| **NOTE**: Please provide more details on what all needs to be configured, so that the concerned team can help you with your expectations concerning **Intrusion Detection System**. |

                Here are some additional documents (WAF with a standard App Service) : <https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-app-powershell>

The Barracuda Azure appliance would be good detection/mitigation for this type of issue.

<http://www.prweb.com/releases/2013/2/prweb10465095.htm>

                Web Application Firewall on Azure

<https://www.barracuda.com/WAFonAzure>

                Deploying the Barracuda Web Application Firewall Vx - Windows Azure

<http://techlib.barracuda.com/display/BWAFv76/Deploying+the+Barracuda+Web+Application+Firewall+Vx+-+Windows+Azure>

1. **IDS  &** Vulnerability Assessment **:**

For general restrictions you can also refer IP based /domain based restrictions here : <https://azure.microsoft.com/en-us/blog/ip-and-domain-restrictions-for-windows-azure-web-sites/>

<https://azure.microsoft.com/en-us/blog/confirming-dynamic-ip-address-restrictions-in-windows-azure-web-sites/>

**Vulnerability assessment of Azure App Service**, I would recommend you to use **Tinfoil security**. You may either purchase it via marketplace or contact them directly here: <https://www.tinfoilsecurity.com/support>

1. **TLS 1.0 :**

By Default , the Azure Web app are using TLS 1.0 and accessing them with URL *<webappname>.azurewebsites.net* will always be supporting TLS 1.0 , however using **ASE** as mentioned in point **2,** you can disable TLS 1.0**.**

<this is changed in April 2018 , we can choose TLS now >

1. **DMZ/NSG :**

**Refer :** <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-dmz-nsg-asm>

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz>

However using NSG you can implement DNZ , this is already taken care in point