

# About Sophos XG Firewall

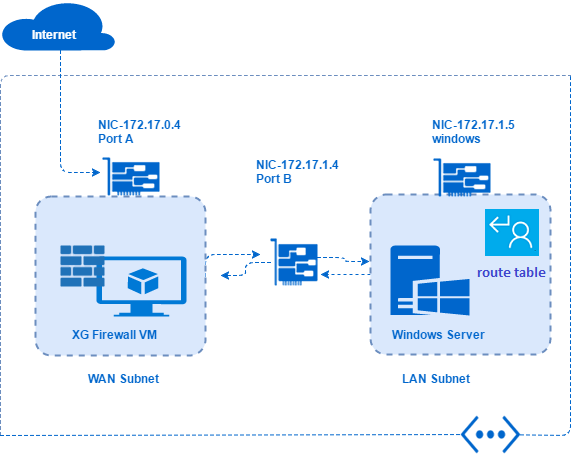
Sophos XG Firewall is a next-generation firewall that is packaged as an all-in-one solution. It combines advanced networking capabilities, as well as protections such as Intrusion Prevention Systems (IPS) and Web Application Firewall (WAF), plus user and application controls. It is designed to help you protect your Azure-based workloads against advanced threats.

# Objective

Sophos XG Firewall on Azure is a solution to run XG Firewall on Microsoft Azure.

The specific use case for this scenario highlights the Sophos XG WAF component. A customer will launch the Test Drive. Azure Resource Manager Templates will deploy an XG firewall, as well as a Windows Virtual Machine (VM). The customer can log in remotely to the XG Firewall as view the preconfigured security policy. The policy will also provide web filtering and blocked sites, so customers can test acceptable usage policy enforcement (e.g. no porn, gambling, known malicious web sites) of Remote Desktop users.

# Architecture of Sophos XG Firewall



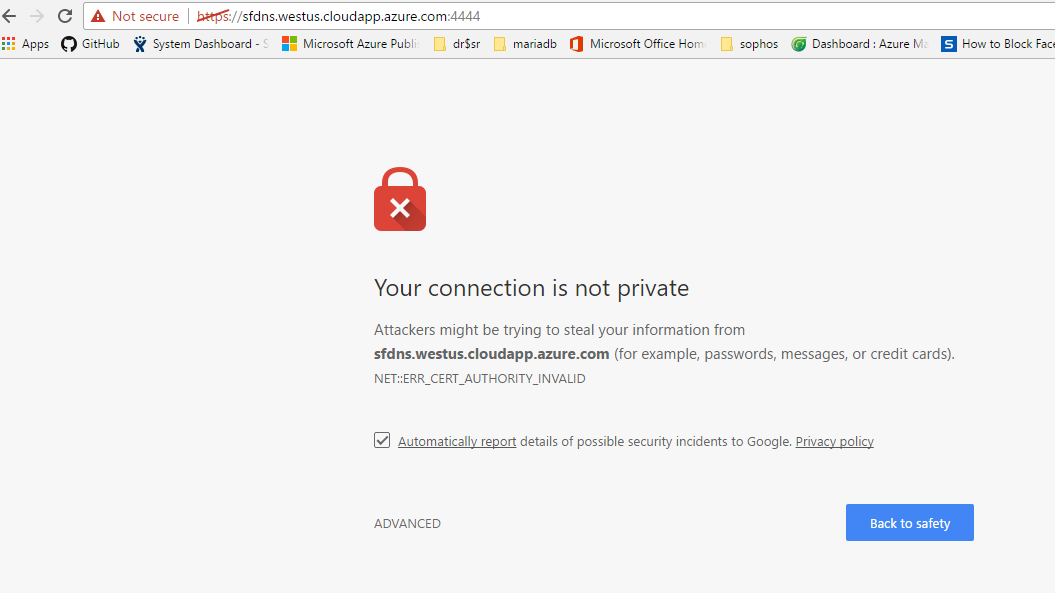
The architecture describes how you can deploy and run Sophos XG Firewall on Azure.

On deploying ARM template, a Vnet is created with 2 subnets (WAN and LAN).

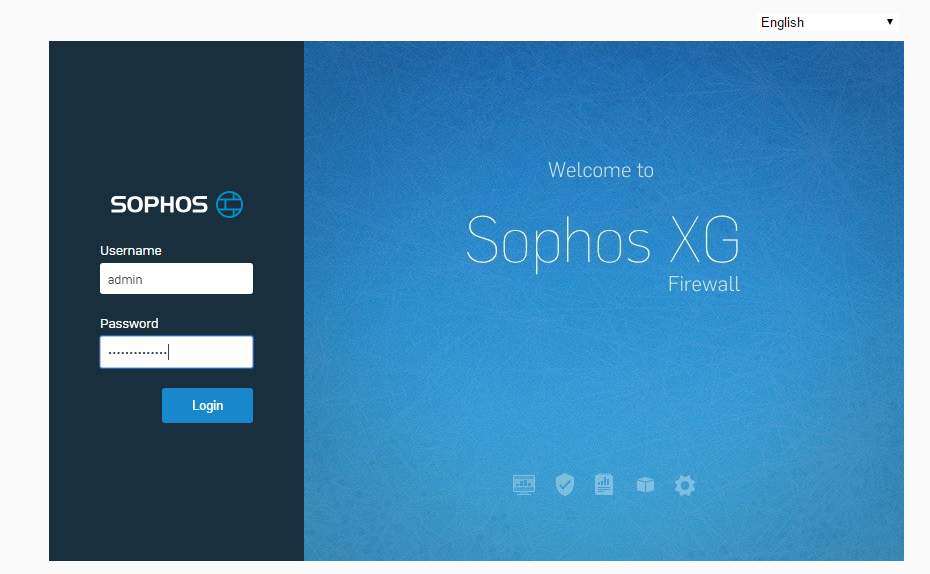
XG Firewall VM is associated with WAN subnet and windows VM with LAN subnet. Firewall rules are added to the Sophos XG Firewall NIC,that allow both inbound and outbound traffic and to allow backend access. The outbound traffic from windows VM goes to XG Firewall and is send through the LAN subnet using route table. Inbound traffic should go directly to Windows VM via XG Firewall.

# Configuring Network Wizard

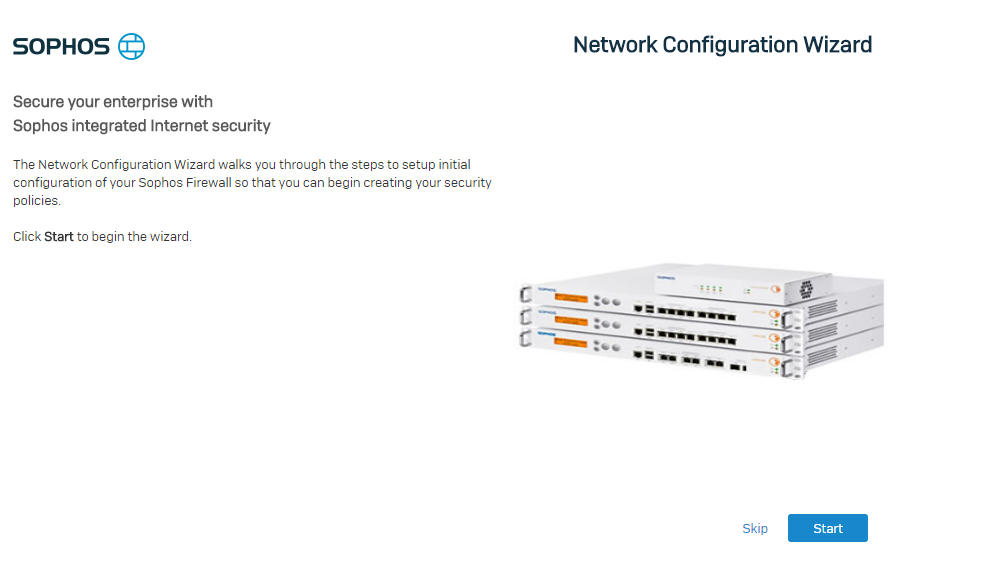
1. Copy the IP address of the Sophos XG Firewall and enter in new browser. Click on **ADVANCED**.



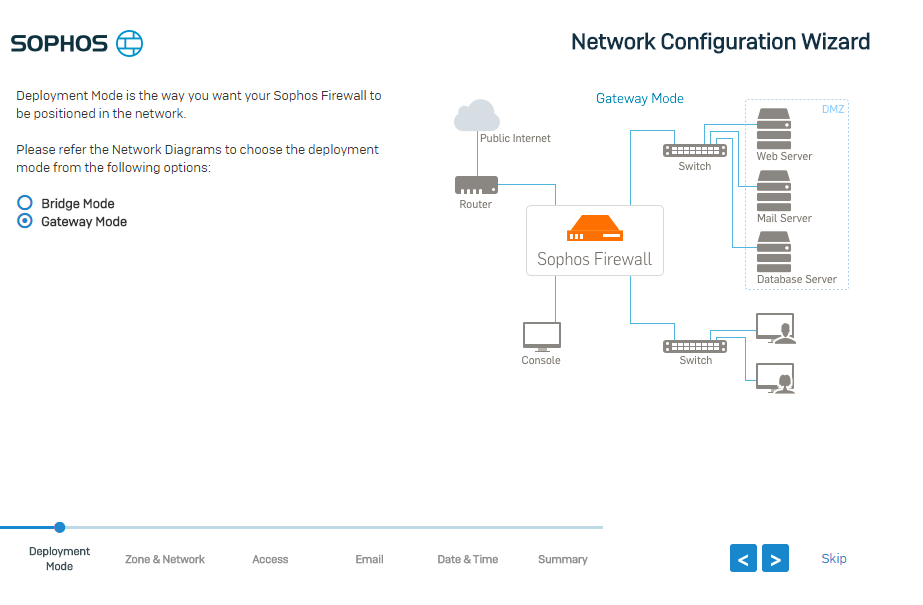
1. This navigates to Sophos admin console. Enter your Sophos credentials with **Username** as ***admin***.



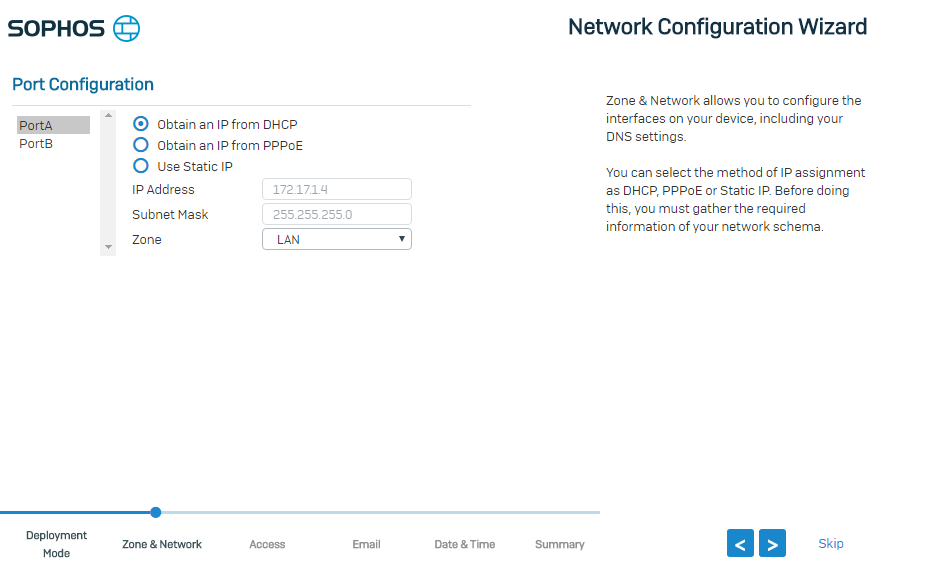
1. Click on **Start**, this opens the network configuration wizard to perform basic system setup.

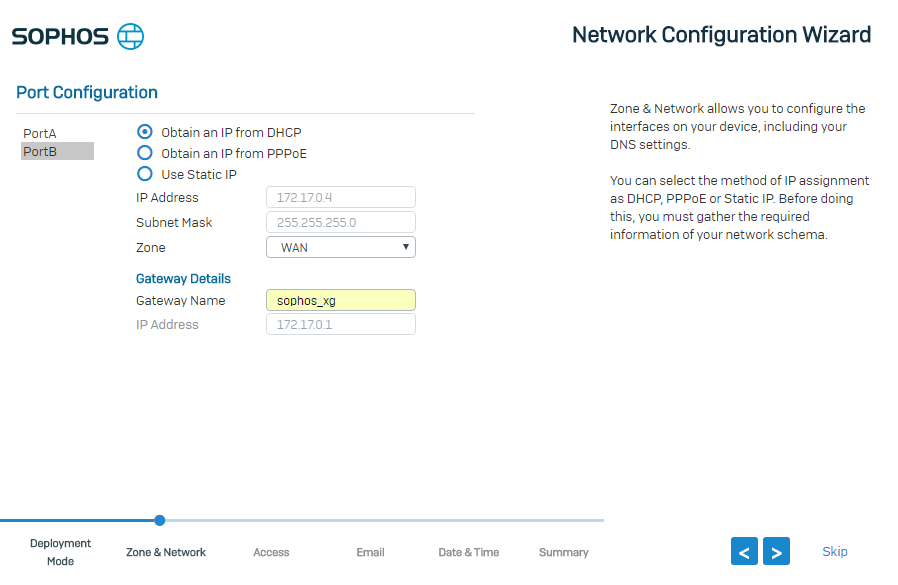


1. We get to select XG Firewall to run in Gateway or Bridge mode.

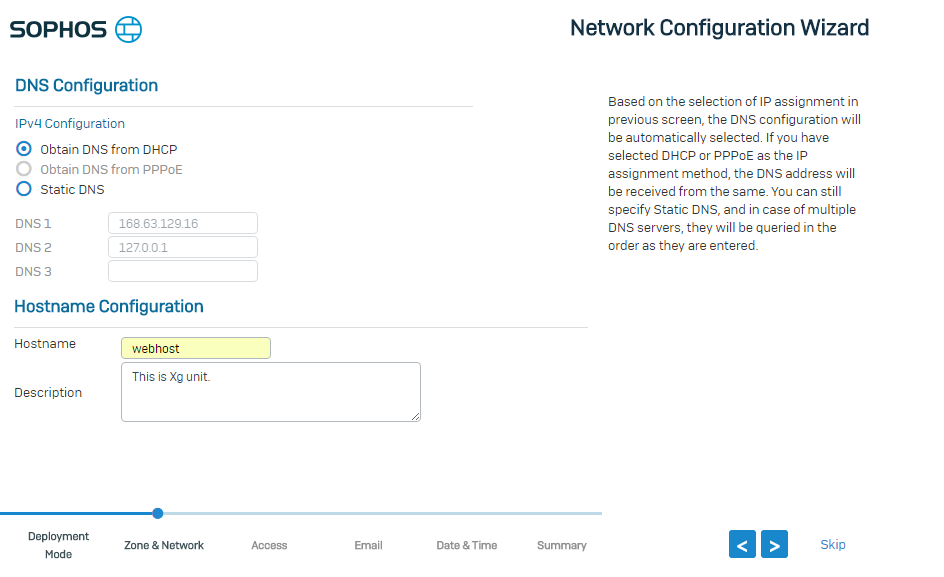


1. The azure currently doesn’t support bridge mode, So select **Gateway Mode**.
2. Make sure that both interfaces of XG Firewall are configured to **Obtain an IP from DHCP**. The Gateway name of interface can be changed.



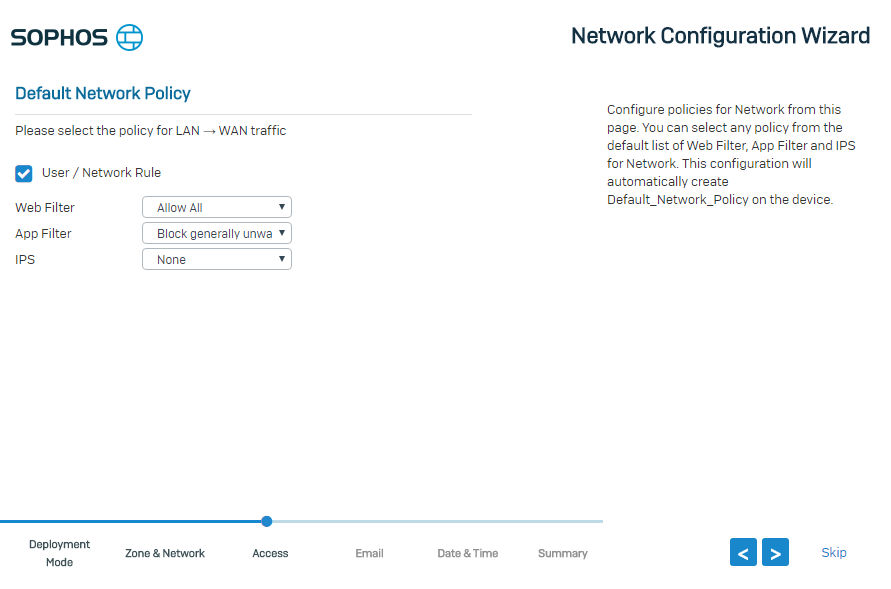


1. Configure DNS settings on the XG Firewall to **Obtain DNS from DHCP** which is a default setting and give the **Hostname** and enter the Description for easy reference.



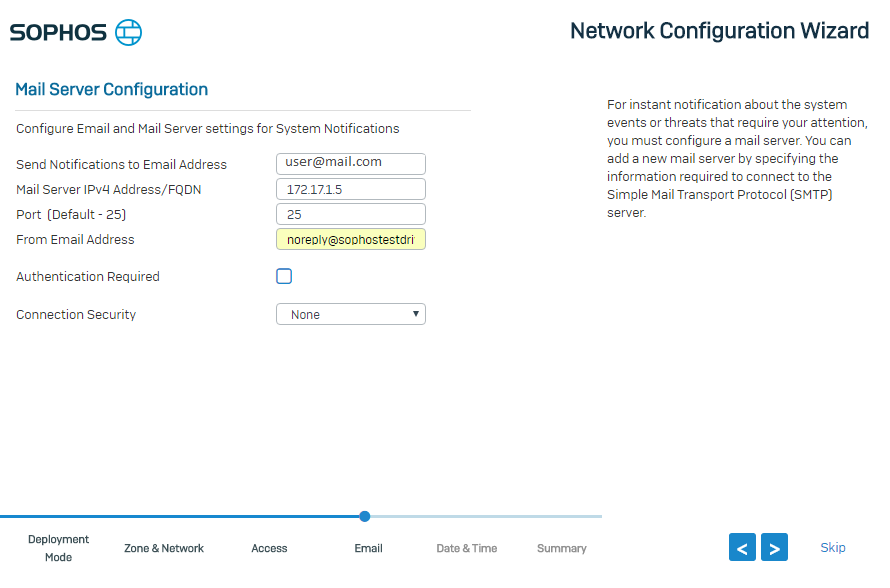
1. Select policy for LAN to WAN traffic.

* Select default **Web Filter** template from the list as **Allow All**.
* Select **App** Filter, which is necessary for your application such as **Blocking generally unwanted application** by allowing the rest.
* For **IPS**, which determines the level and strictness of IPS filtering applied to traffic. Select **None**.



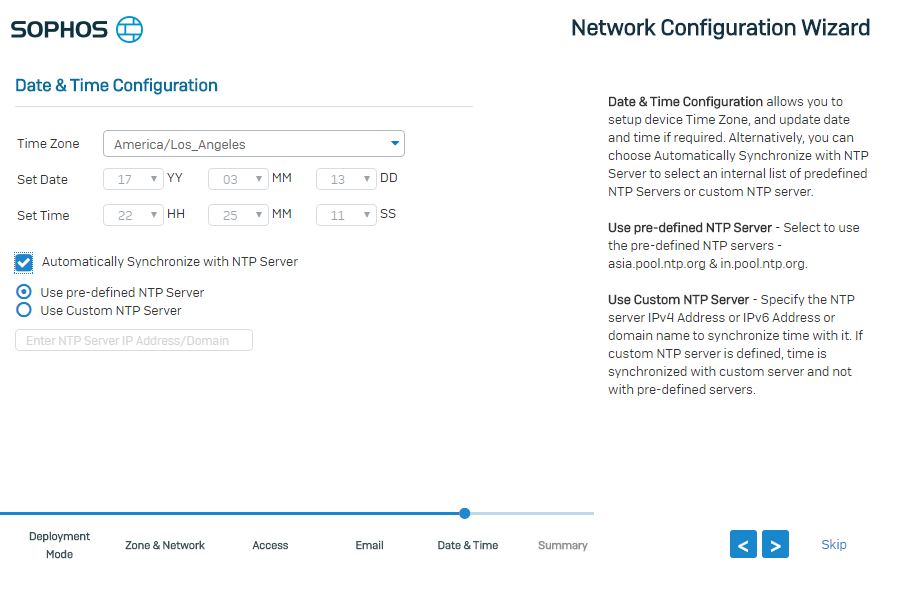
1. The **Mail Server Configuration** page appears where XG Firewall sends the important notification of significant events.

* In **Send Notification to Email Address**, give the recipient email address.
* Give windows server IP address in **Mail Server IPv4 Address/FQDN** and set to default port.
* Followed by email address from where the XG Firewall will send emails in From Email Address.
* Set the **Connection security** to **None**.

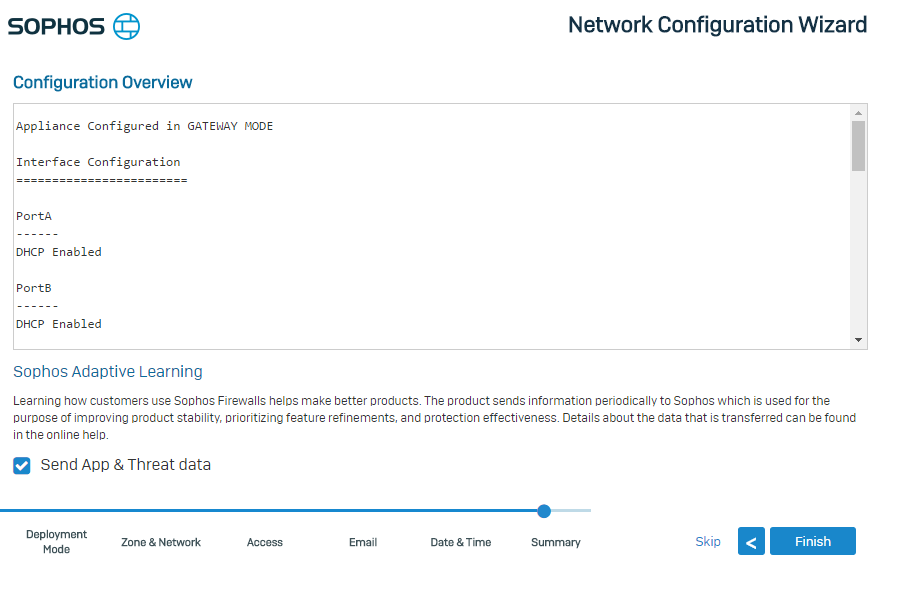


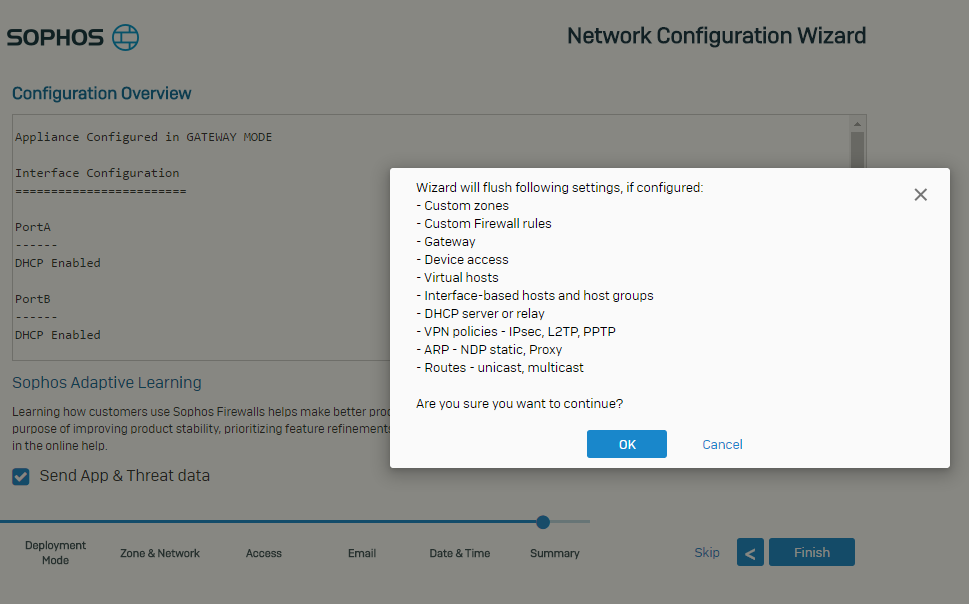
1. Select the **Time Zone** from drop down menu and manually select date and time.

* Check the **Automatically synchronous with NTP Server**.
* Sophos recommend the using NTP for time synchronization when using timing critical protocol such as Microsoft server Active Directory. Select **Use pre-configured NTP server**.

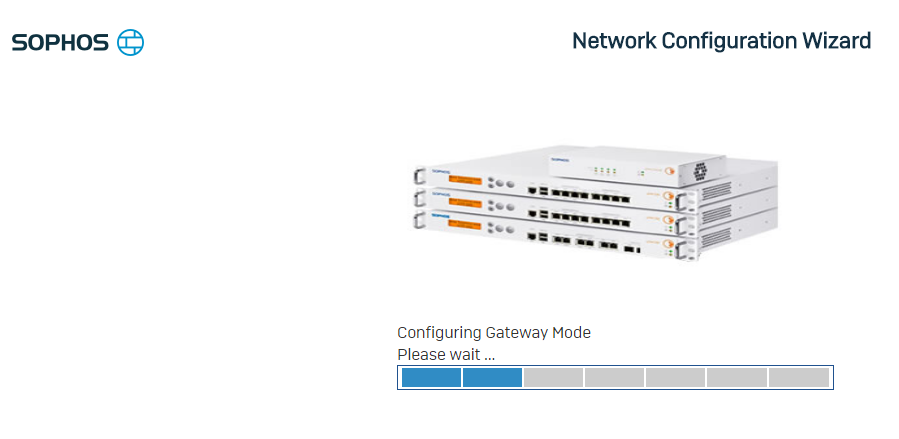


1. The very last setup of wizard gives overview of settings configured through the wizard before committing them to system. A quick summary is shown if any changes are needed. Click **OK** to proceed and commit.





1. Progress indicator is shown ,this process takes several minutes. A success page appears which shows that the settings are deployed to the XG Firewall.



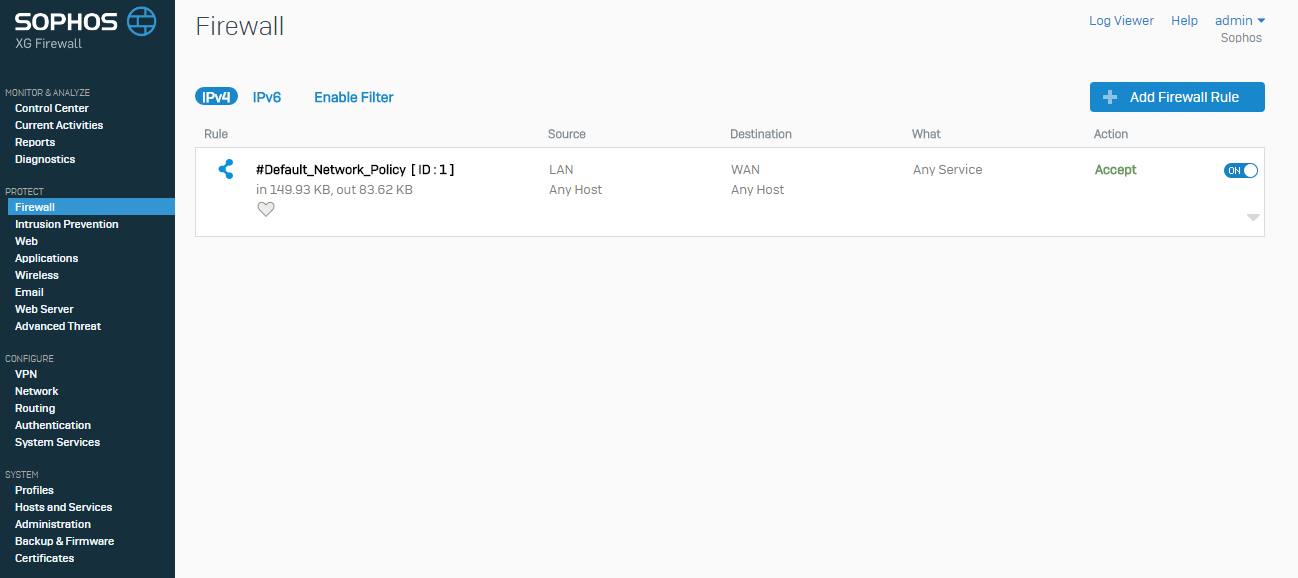
1. Reload the admin console with the login credentials used earlier which leads to XG Dash board. Your XG Firewall is ready to use.

# Configuration of XG Firewall for Specific Use Case

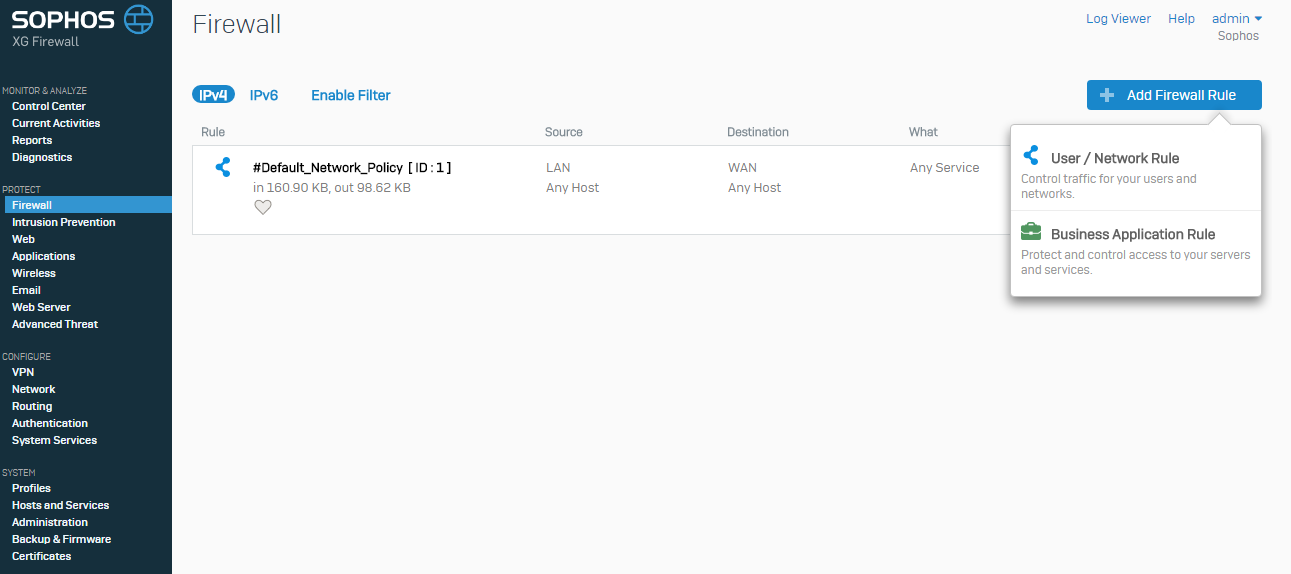
### The following section describes the configuration steps for RDP access and Blocking Facebook website.

## 4.1. Configuration for Creating RDP access to Windows server

1. Log in to your XG Firewall.
2. Navigate to **Protect** > **Firewall**, click **Add Firewall Rule**.

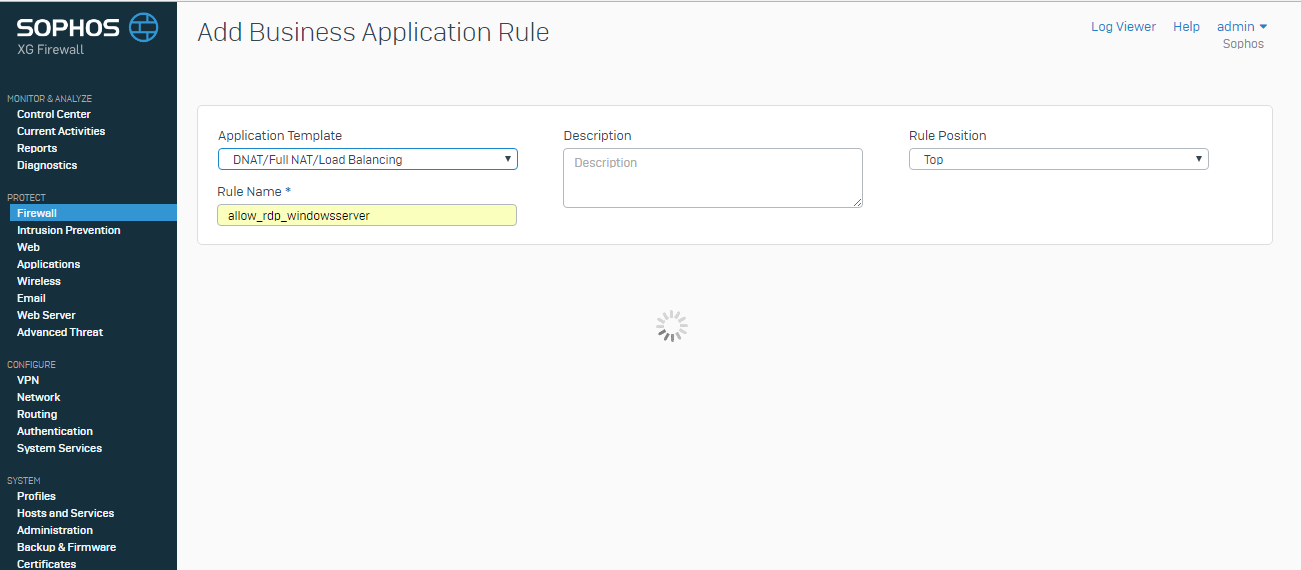


1. Select Business Application Rule for RDP access. The Add Business Application Rule page opens.

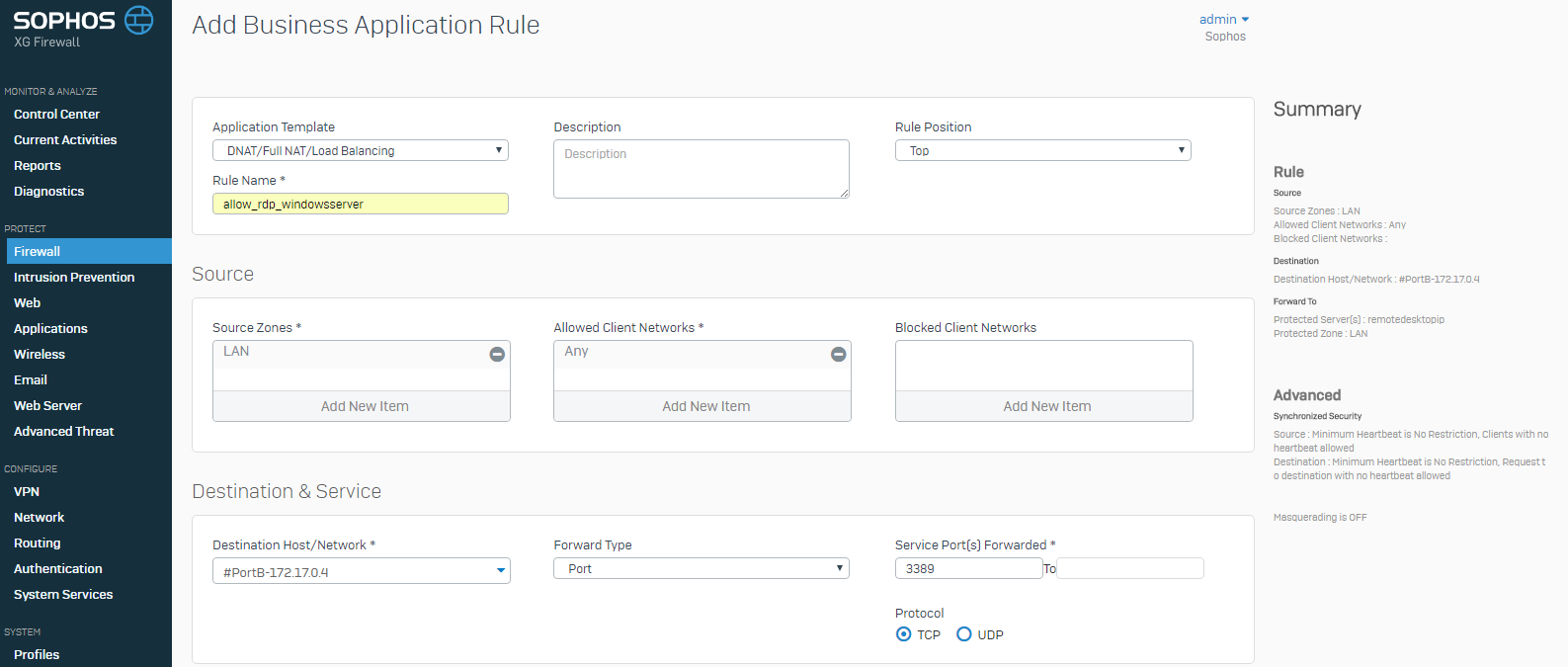


1. Make the following settings:

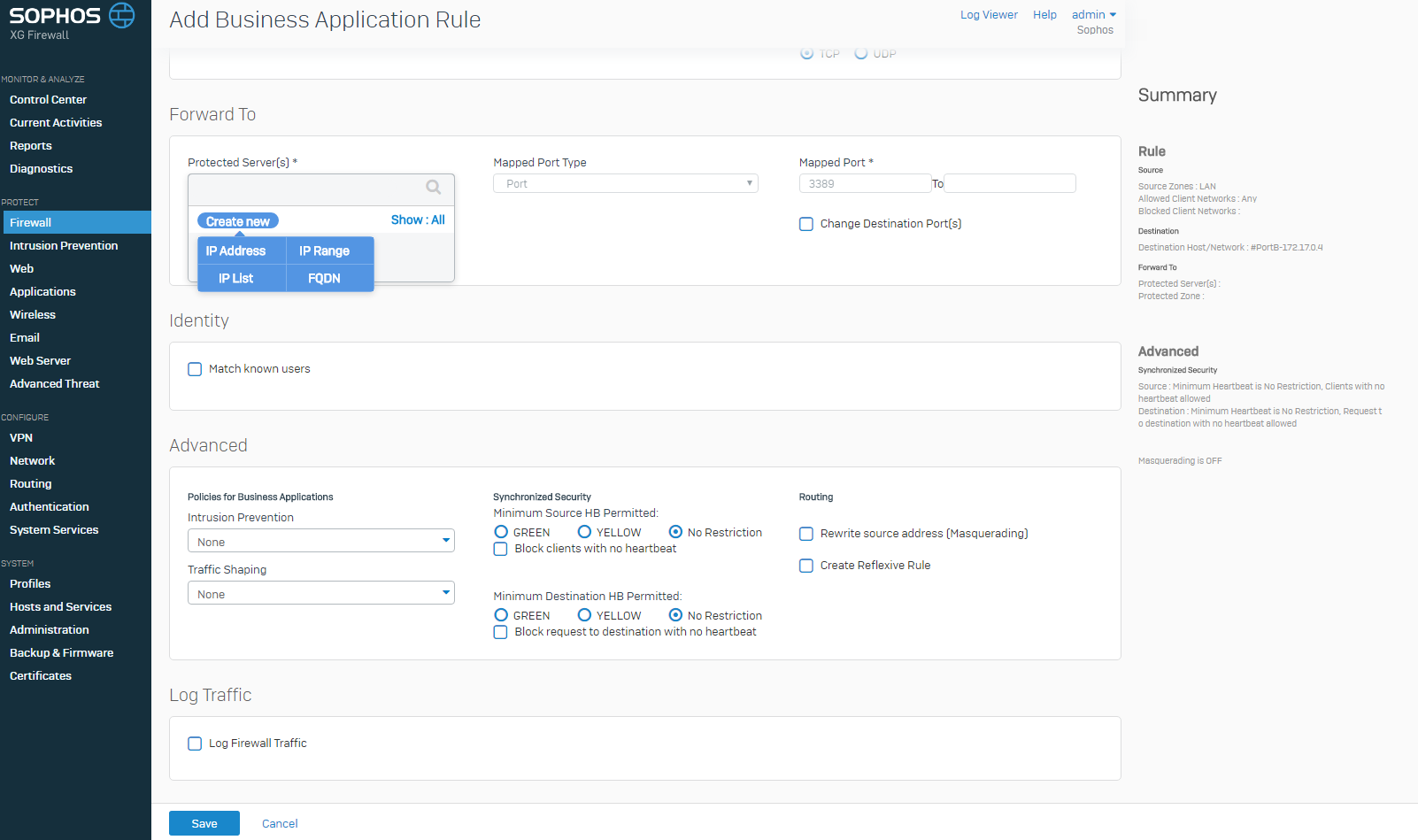
* **Application Template**: Select ***DNAT/Full NAT/Load Balancing***.
* Mention the name of the Business Rule.



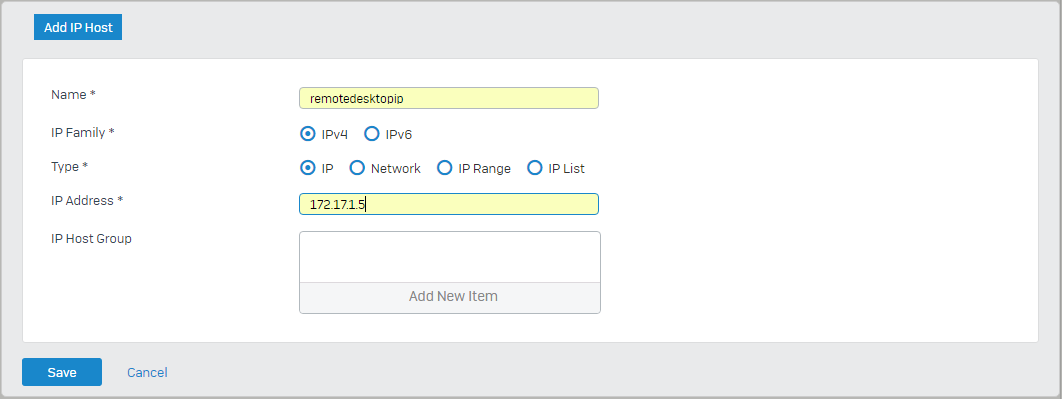
* **Source**: Select Source Zones as ***LAN*** and Allowed Client Networks as ***Any***.
* **Destination & Service**: Select Destination Host Network as the **WAN** port i.e Port B and Services Port(s) Forwarded to ***3389***.

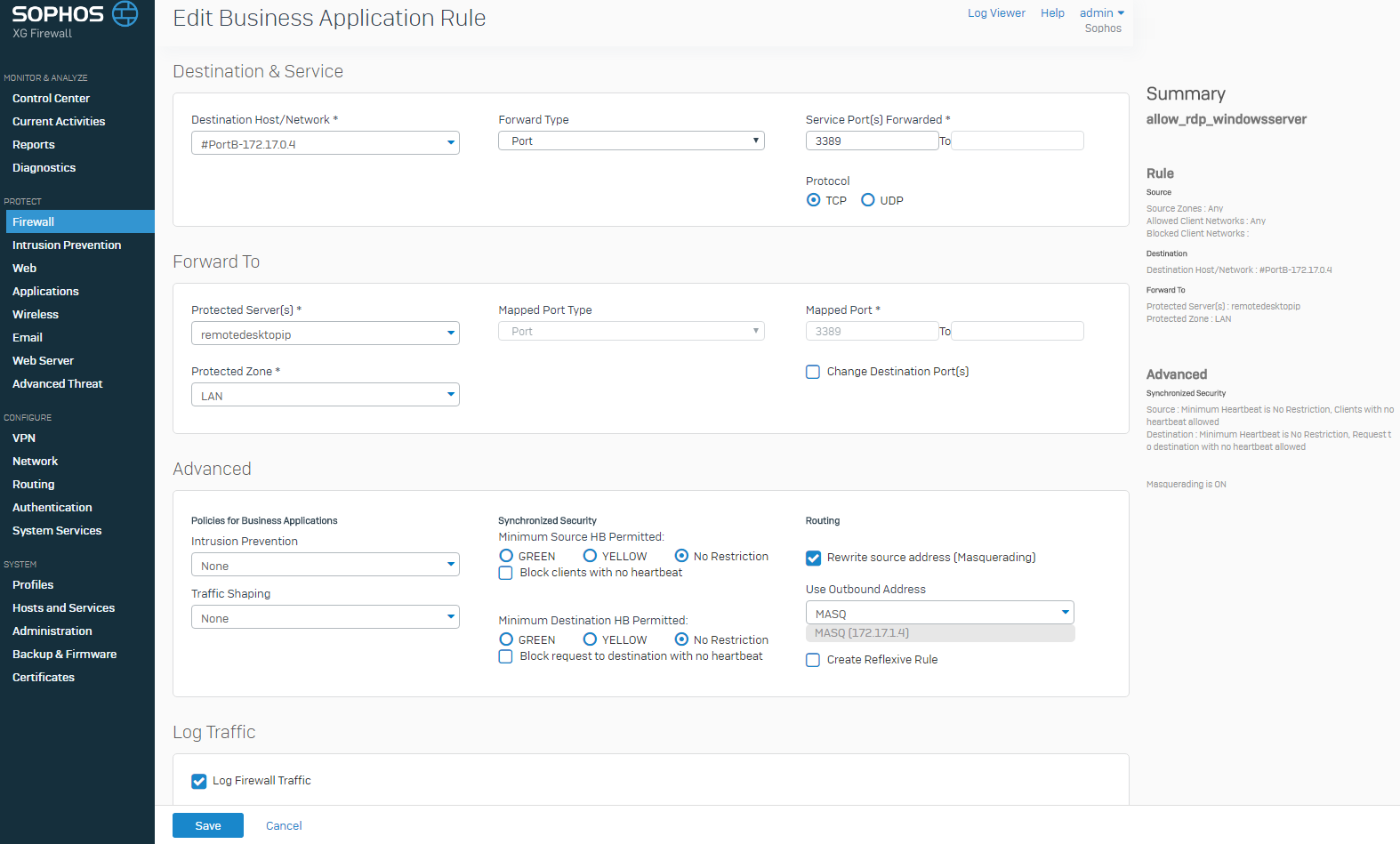


* **Forwarded To**: In **Protected servers**, click on **Create New** and click on **IP Address**, give windows server IP address. Select the **Protected Zone** as ***LAN***.



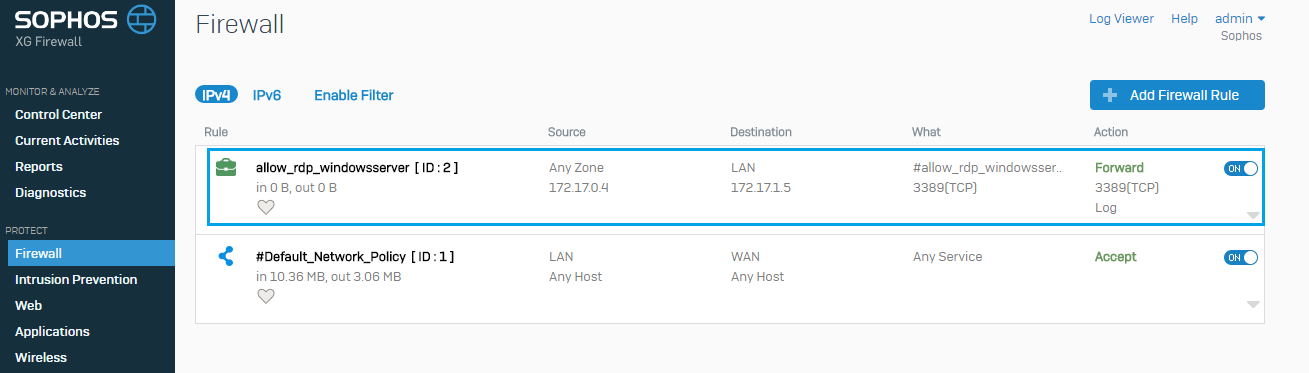
* Give a Name for the IP Host and mention the Private IP address of ***Window server*** in **IP Address.**





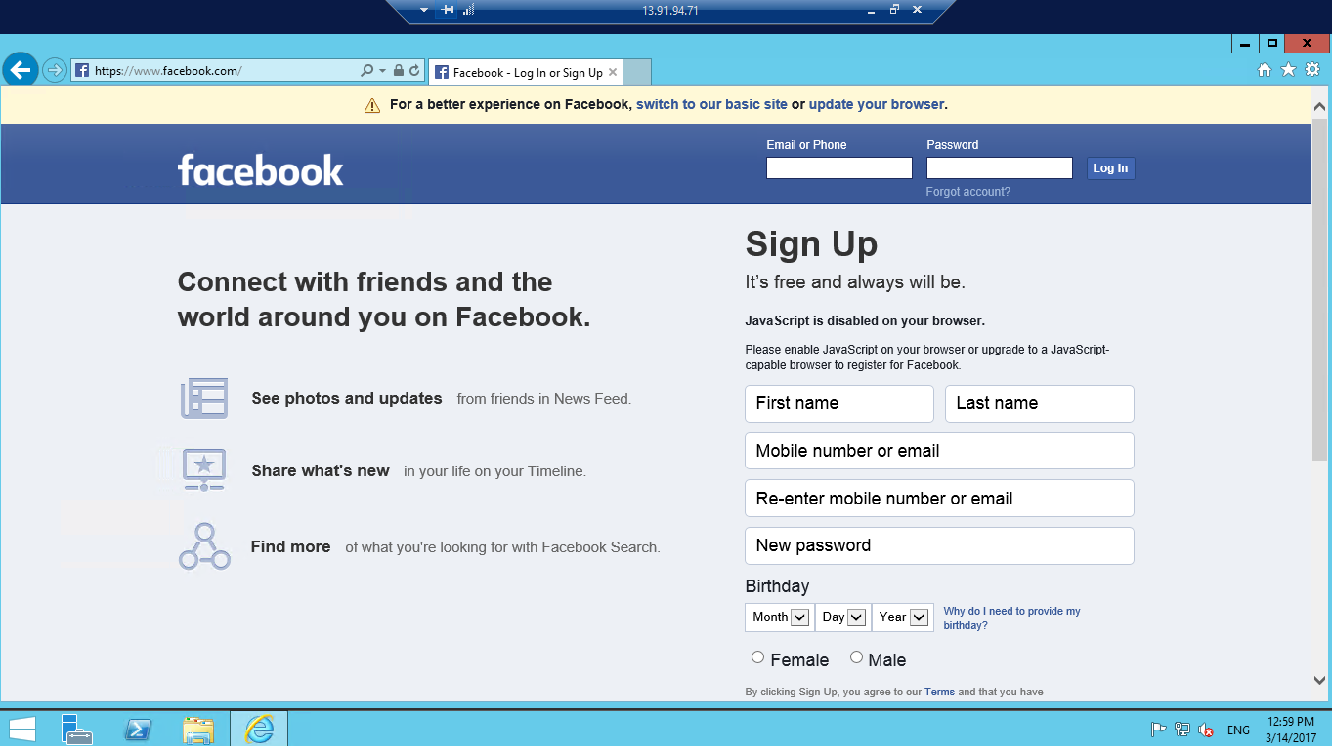
* Check the **Log Firewall Traffic**.

1. Check for the created Firewall Rule.



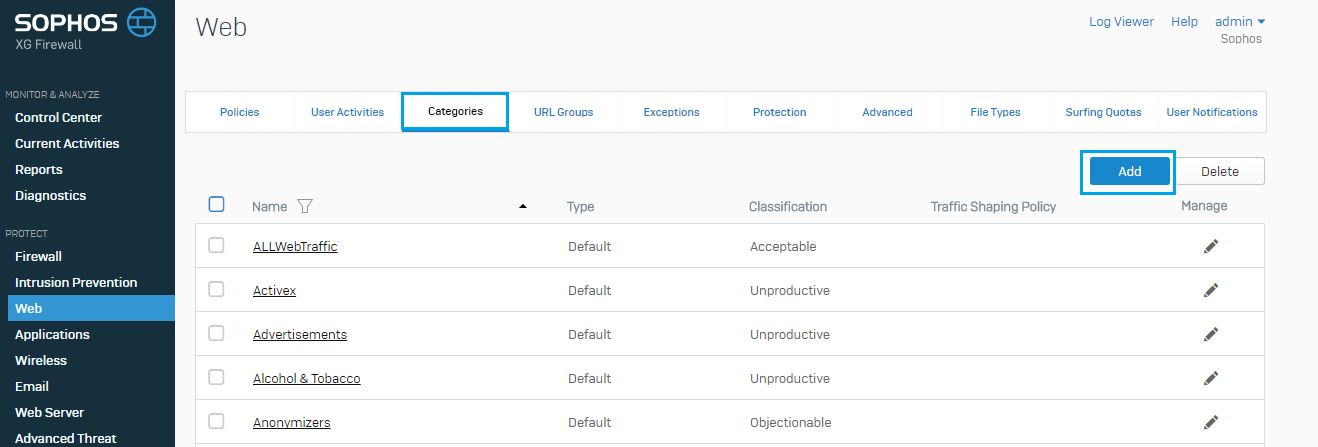
## Configuration To BLock the WEBSITE

1. Before configuring Web policy, we can RDP into Firewall VM using windows server credentials and check for Facebook access.

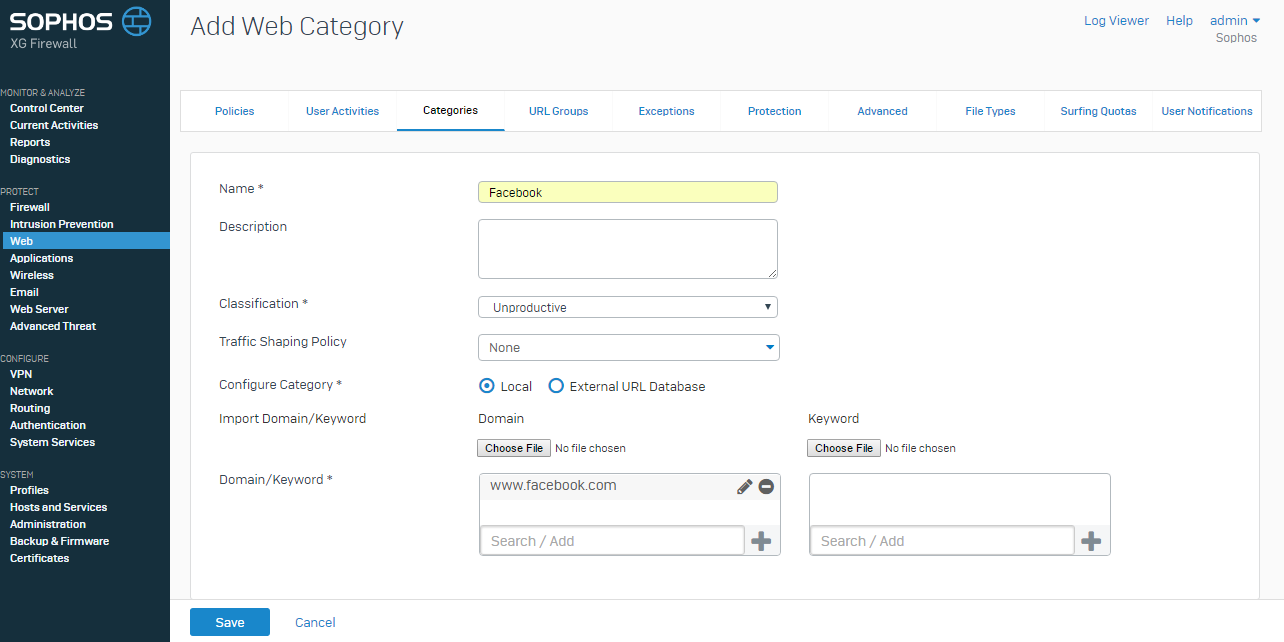


1. Log in to your XG Firewall.
2. Create a Custom Web Category.

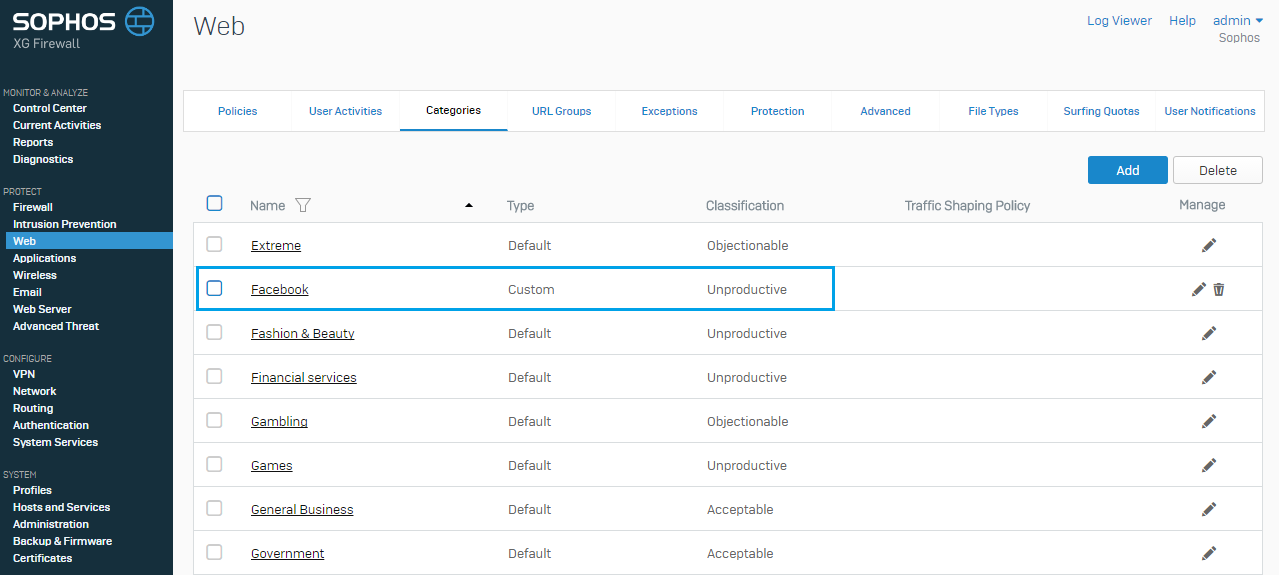
* Navigate to **Protect**>**Web**. Go to **Categories** and click **Add** to create a new category.



* Give the Name for Web category with ***Unproductive*** as Classification. Mention the website which is required to be blocked in **Domain**.

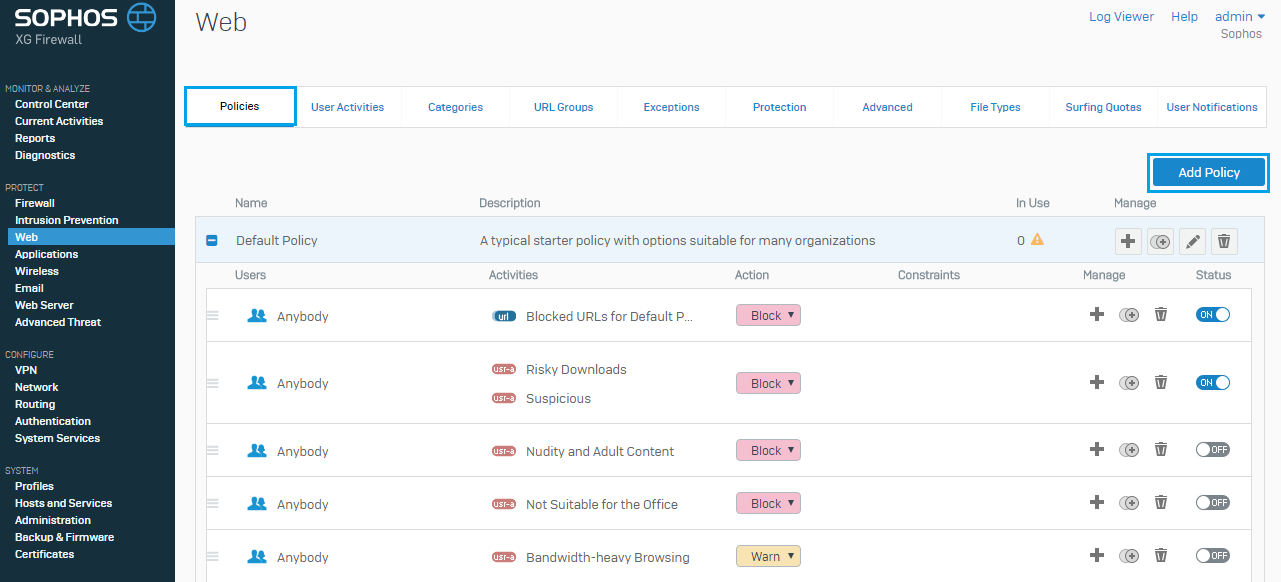


* A web Category is created on name of Facebook.



1. Create a Web Filter Policy to Block Facebook.

* Go to **Policies** and Click on **Add Policy**.

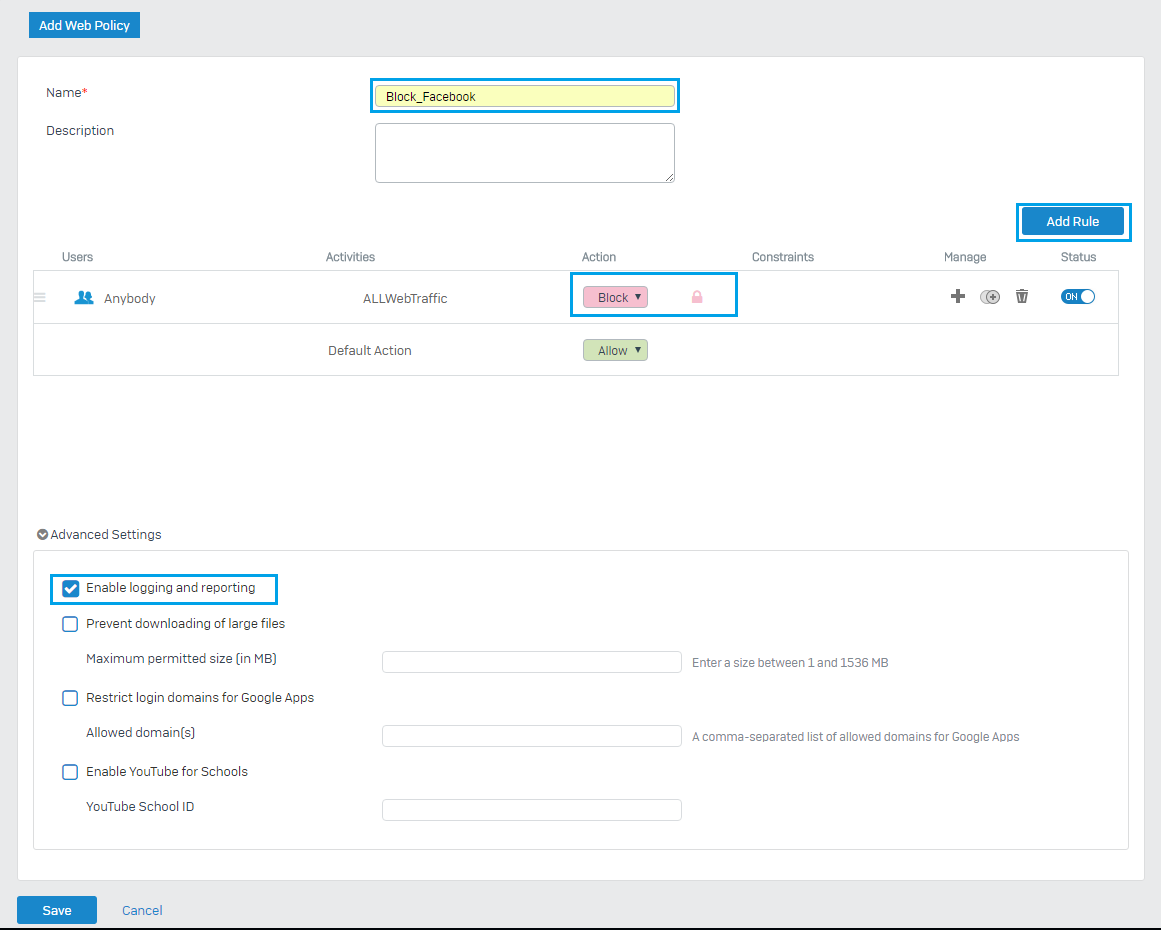


* Create a new Web Filter Policy named **Block\_Facebook**.
* Click on **Add Rule** to add a Web Filter Policy Rule with the following parameters.

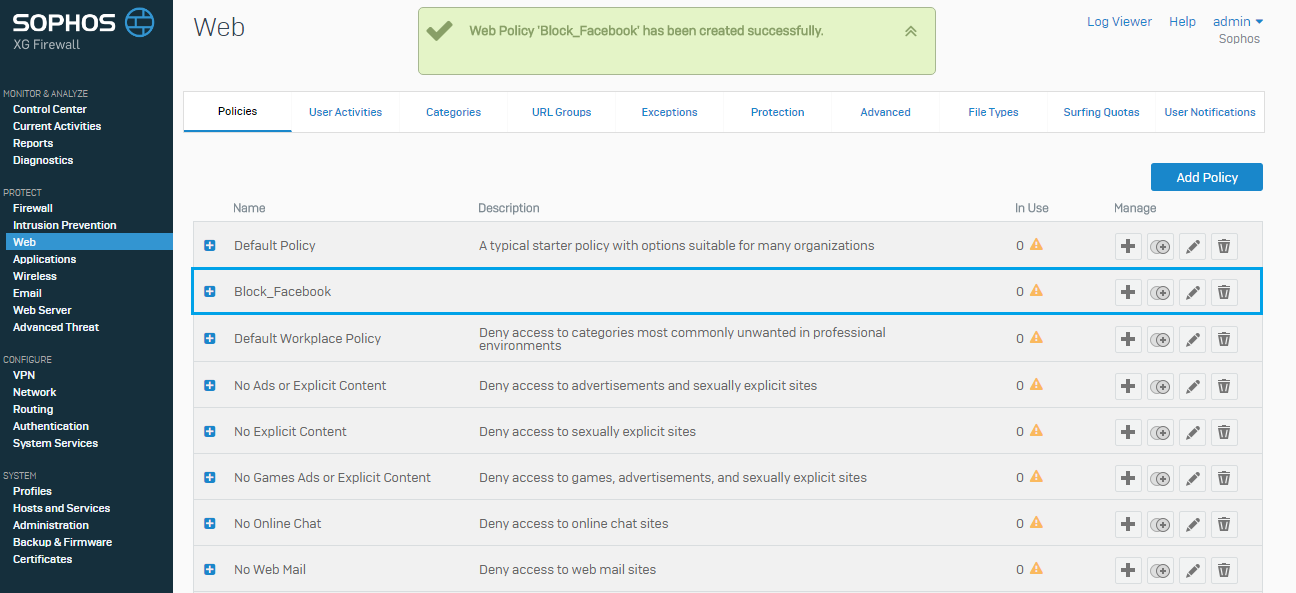
**Action**: Select ***Block*** from drop down list and choose ***Block HTTPS***.

**Constraints**: Select ***All the Time.***

* In Advanced Settings make sure that the **Enable logging and reporting** is ***checked*** and click on **Save**.

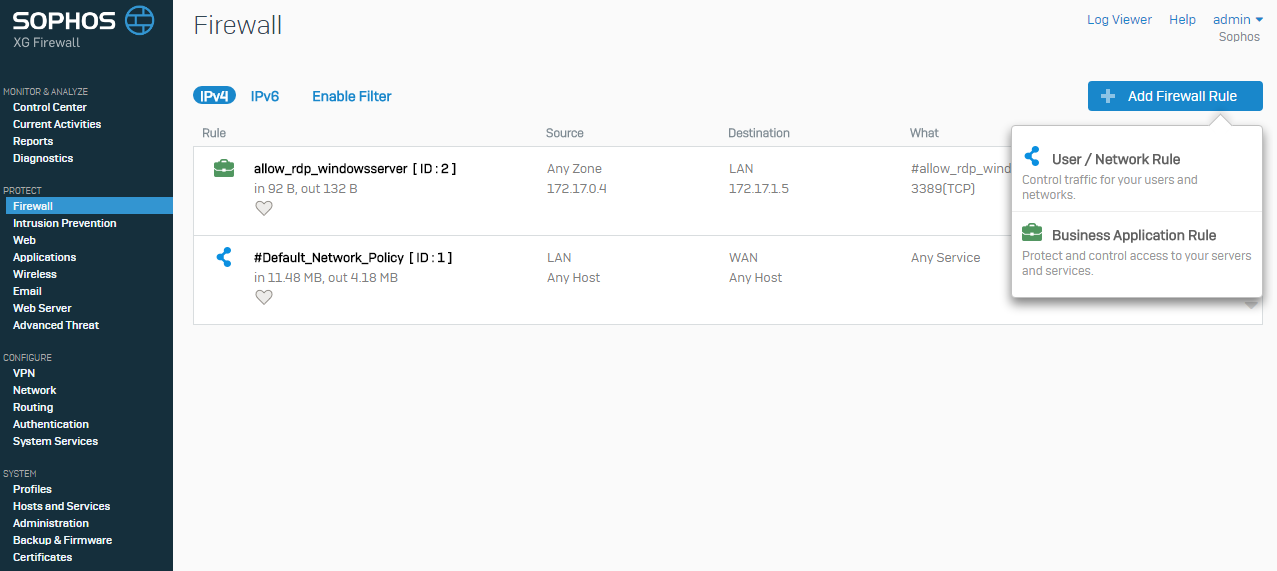


* A web Policy ***‘Block\_Facebook’*** has been created successfully.



1. Apply the Policy to a Firewall Rule or User/User Group.

* To create a Rule navigate to **Firewall**, click on **Add Firewall Rule** and select **User/network Rule**.

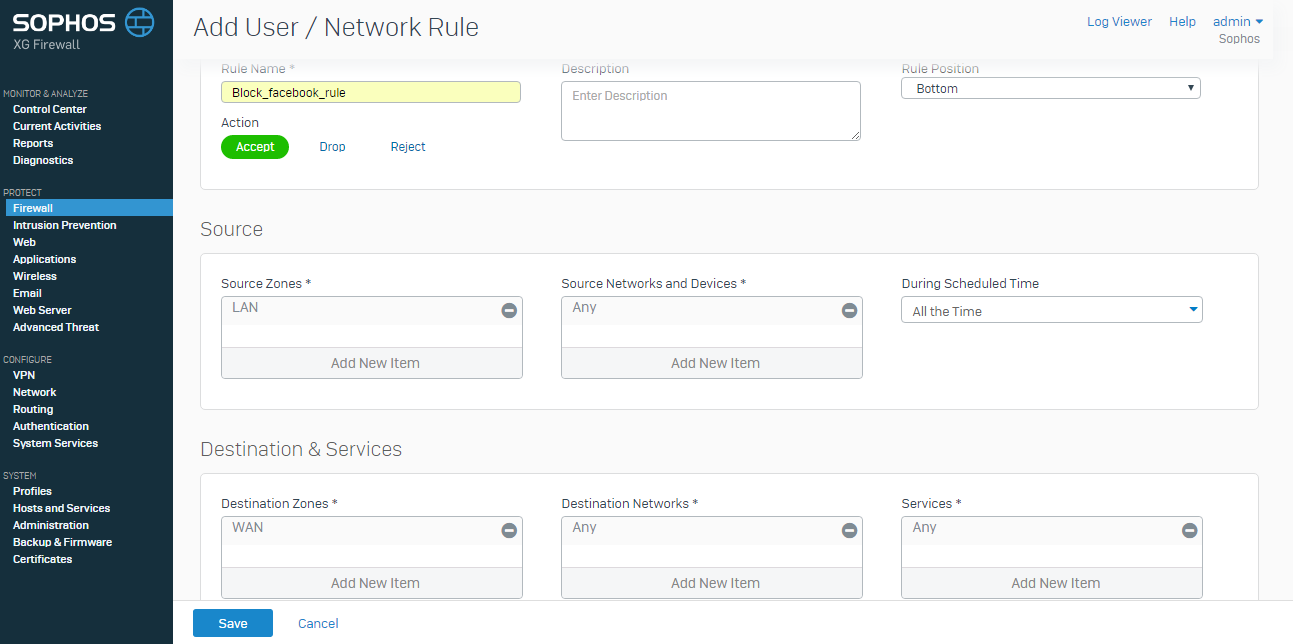


* Make the following settings

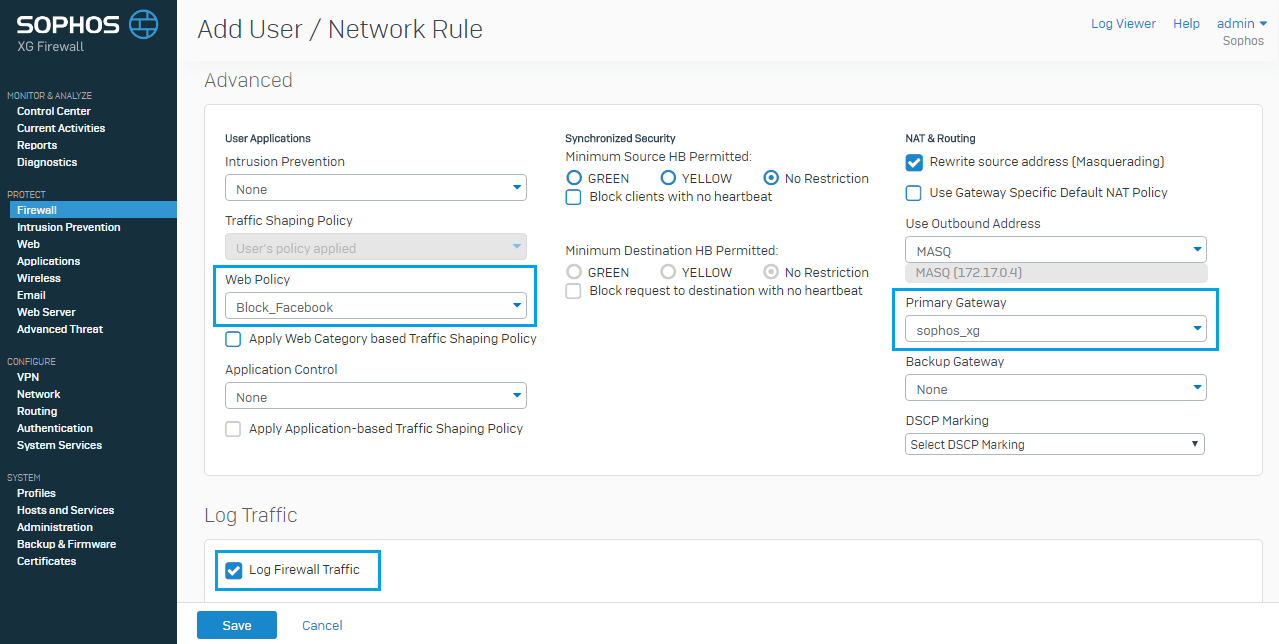
**Rule Name**: Give the rule name as ***Block\_facebook\_rule***.

**Source**: Select **Source Zones** as ***LAN*** from drop down list and **Source Networks** **and Devices** as ***Any***.

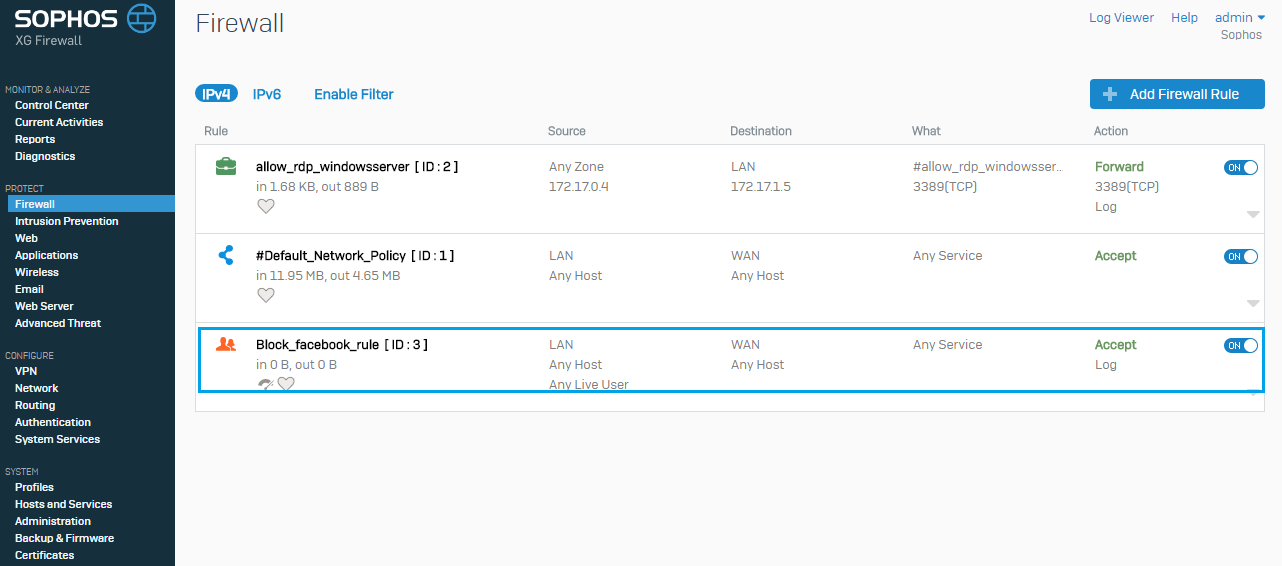
**Destination & Services**: Select **Destination Zones** as ***WAN*** and **Destination Networks** as ***Any***.



* In **Advanced**, Select the **Web Policy** name given earlier and select the **Primary Gateway**, which was given during network configuration wizard. Check the **Log Firewall Traffic** and click on **Save**.

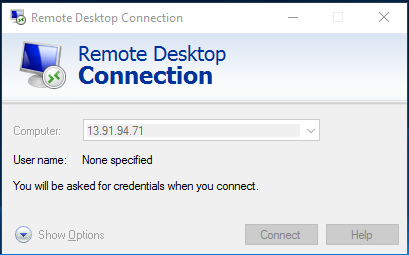


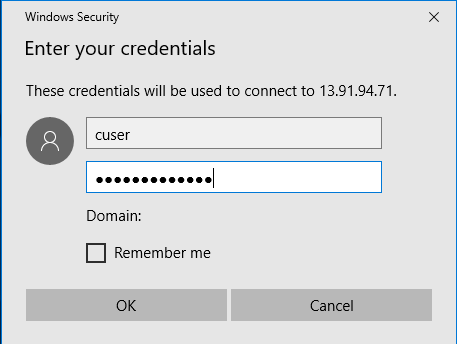
* A Firewall rule **‘Block\_facebook\_rule’** is created.

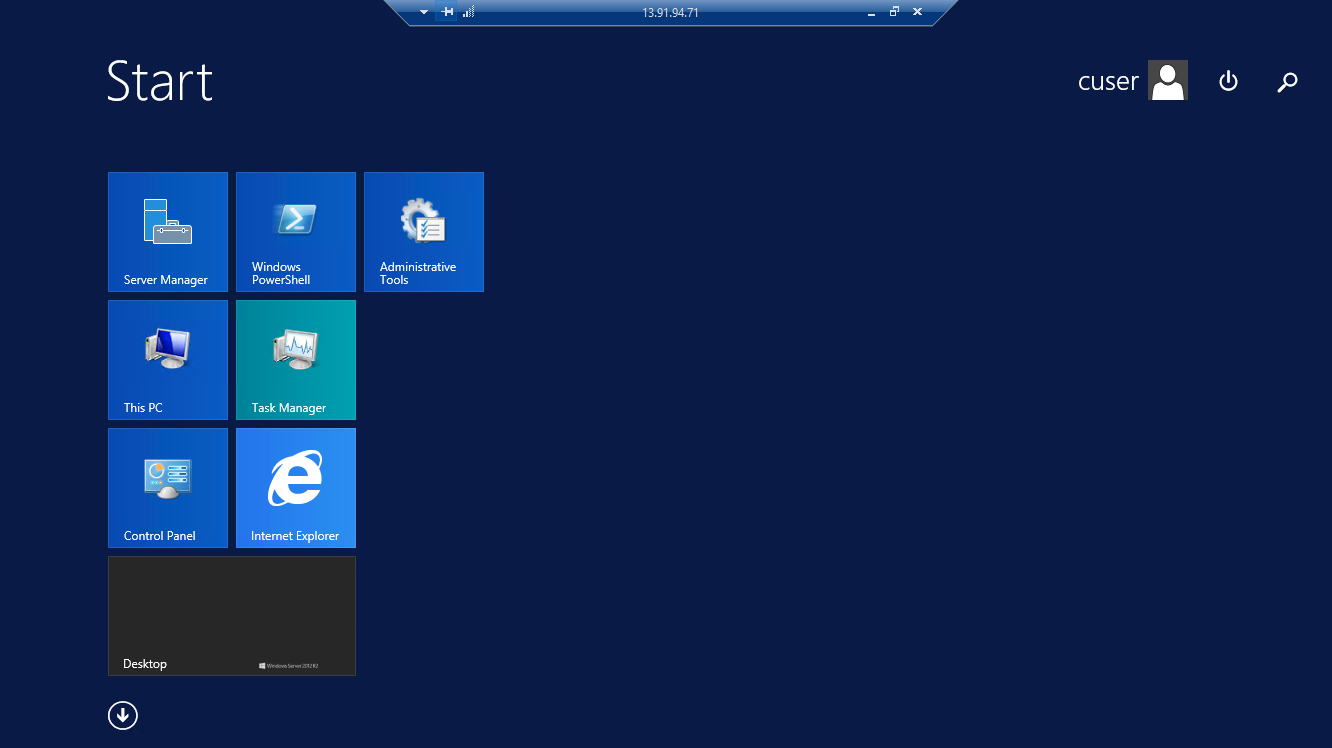


# Access RDP and check for Blocked website

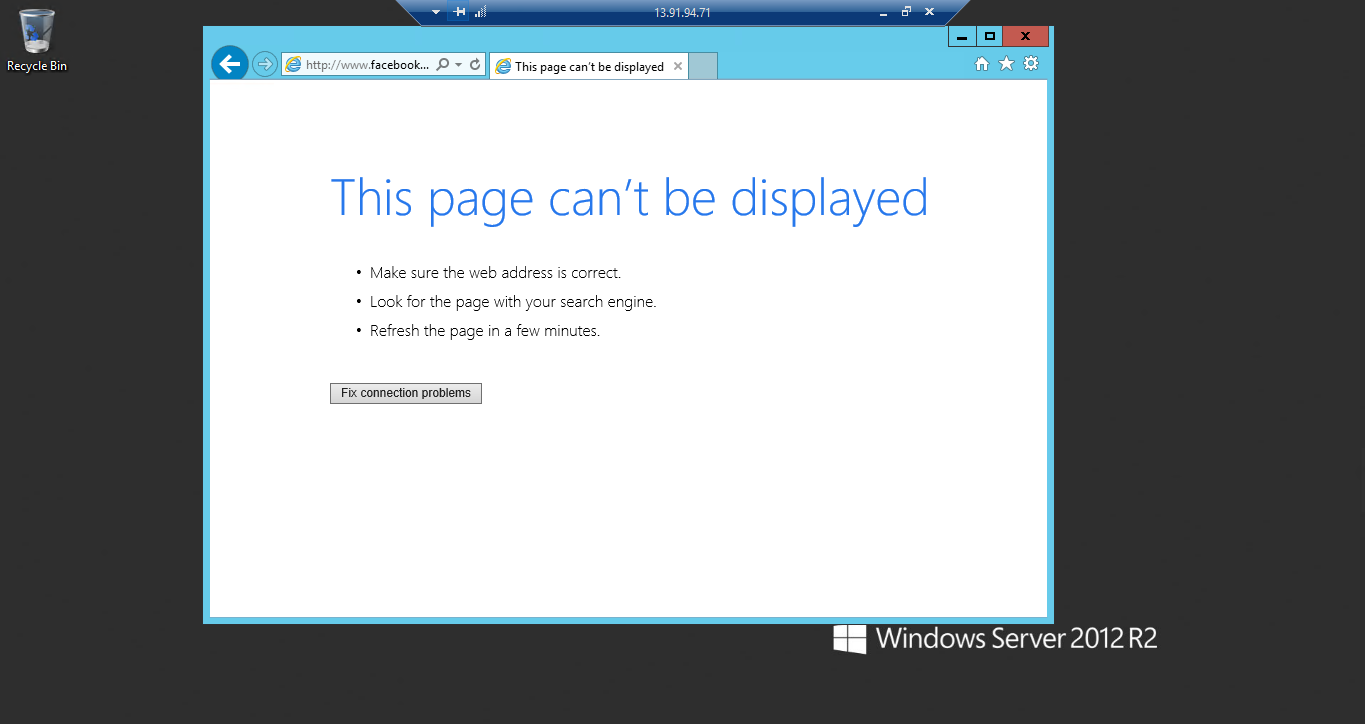
1. RDP into Firewall VM using windows server credentials.



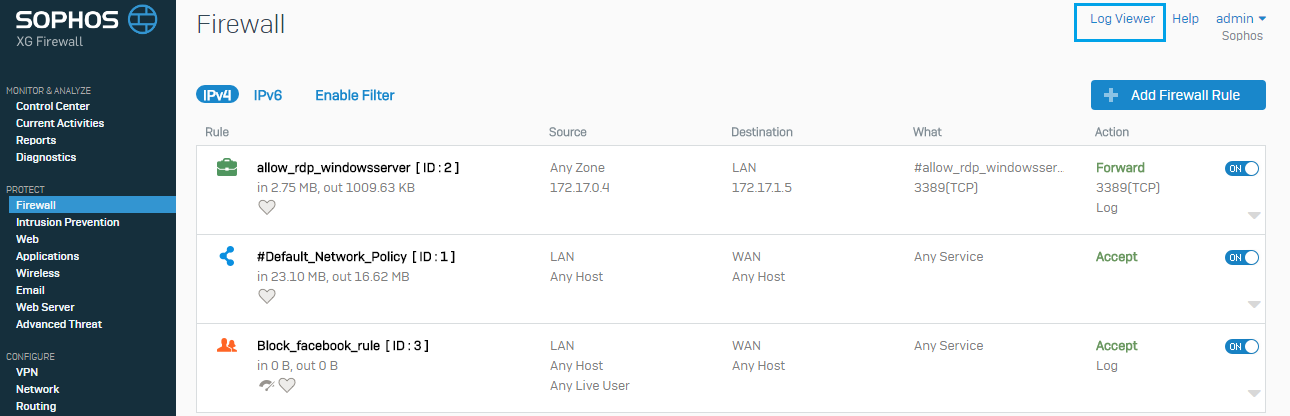


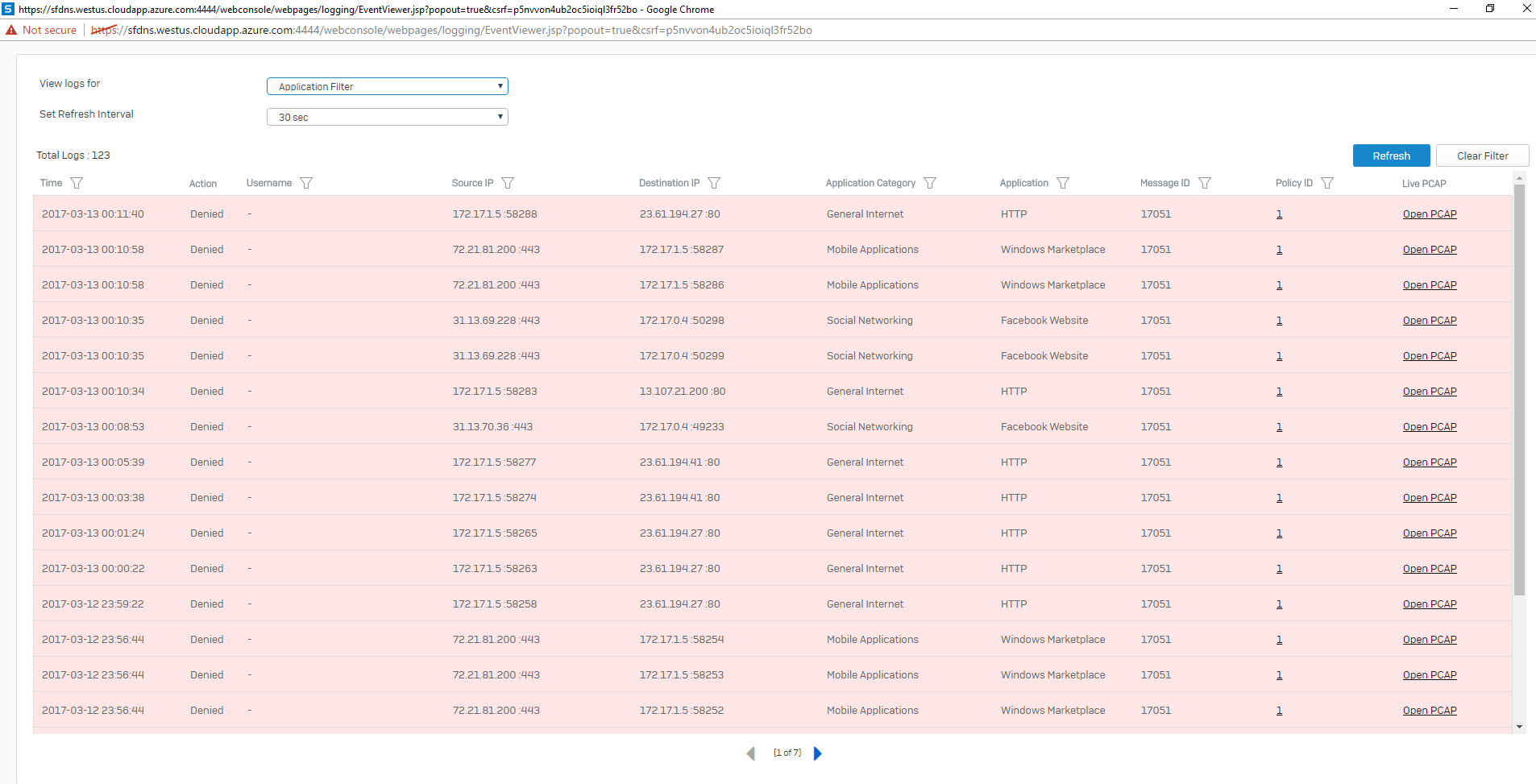


1. Browse the website [www.facebook.com](http://www.facebook.com) in a browser and check .The page will not be displayed as the web policy and a firewall is created.



1. We can check the log in by clicking on **Log Viewer**.





1. The above documentation shows that the Sophos XG Firewall can block access to a particular website.
2. Similarly the procedure can be followed to block any website.