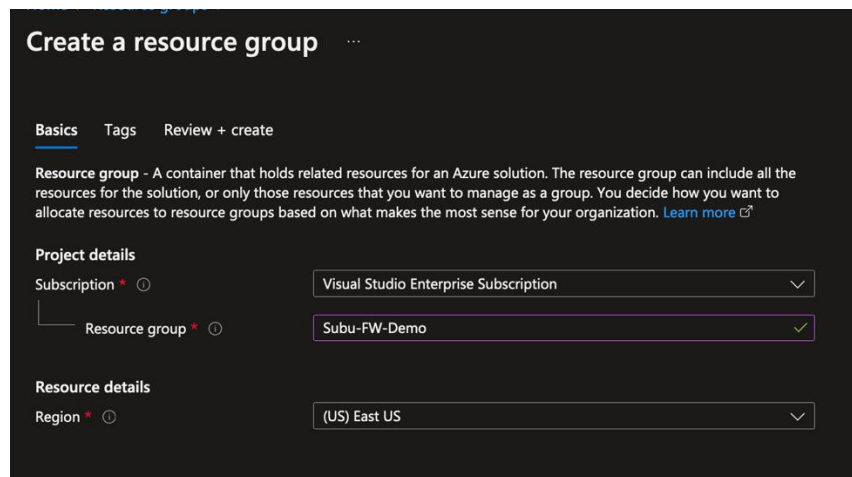


Azure Firewall Protection

In this Blog we will learn about how to implement the Azure Firewall protection for the Network/Application traffic and see the metrics.

Create a new Resource Group:

Login to Azure portal (<https://portal.azure.com/>) and then create a new RG



The screenshot shows the 'Create a resource group' page in the Azure portal. The page has a dark header with the title 'Create a resource group' and a three-dot menu. Below the header, there are three tabs: 'Basics' (selected), 'Tags', and 'Review + create'. A descriptive paragraph explains that a resource group is a container for related resources. Under the 'Project details' section, there are two dropdown menus: 'Subscription' (set to 'Visual Studio Enterprise Subscription') and 'Resource group' (set to 'Subu-FW-Demo' with a green checkmark). Under the 'Resource details' section, there is a 'Region' dropdown menu set to '(US) East US'.

Create a new Firewall Plan:

In the newly created RG, we need to create a new Firewall protection plan and then we will do the basic exercise to check if this plan is really protecting our VNET or not.

Create a firewall

fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#).

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

Availability zone ⓘ

Firewall tier

☒ Standard
☐ Premium

Firewall management

☒ Use a Firewall Policy to manage this firewall
☐ Use Firewall rules (classic) to manage this firewall

Firewall policy *

[Add new](#)
✖ The value must not be empty.

Choose a virtual network

☐ Create new
☒ Use existing

Virtual network

[Add new](#)
✖ This virtual network must have a subnet named AzureFirewallSubnet.

Public IP address *

[Add new](#)

Create a new Firewall Policy

This will create a new firewall policy with default settings. You can customize your policy after creation.

Policy name *

Region

Policy tier

☒ Standard
☐ Premium

Basics

Tags

Review + create

Summary

Basics

Subscription

Resource group

Region

Azure Firewall Sku

Firewall Policy Name

Firewall Policy Sku

Virtual network

Address space

Firewall public IP address

Availability zone

Visual Studio Enterprise Subscription

Subu-FW-Demo

East US

Standard

Subu-FW-policy

Standard

Subu-FW-Vnet

10.3.0.0/16

Subu-FW-pip

None

Tags

Resource type

Name

No results

Your deployment is complete

Deployment name: Microsoft.AzureFirewall-20220825073446

Subscription: [Visual Studio Enterprise Subscription](#)

Resource group: [Subu-FW-Demo](#)

Start time: 8/25/2022, 7:34:52 AM

Correlation ID: 767c699a-3d96-48d8-ab53-7c407f9d42df

Deployment details

Next steps

Go to resource

Create a new Virtual Network:

Create a new VNet in the same RG where we have created the new Firewall plan

Create virtual network ...

Basics

IP Addresses

Security

Tags

Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *

Visual Studio Enterprise Subscription

Resource group *

Subu-FW-Demo

Create new

Instance details

Name *

Subu-FW-Vnet

Region *

East US

Create virtual network

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.3.0.0/16 10.3.0.0 - 10.3.255.255 (65536 addresses)

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

Subnet name	Subnet address range	NAT gateway
default	10.3.0.0/24	-
AppSubnet	10.3.1.0/24	-

Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

✓ Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20220825072643
Subscription: Visual Studio Enterprise Subscription
Resource group: Subu-FW-Demo

Start time: 8/25/2022, 7:29:05 AM
Correlation ID: be55f414-8de0-4d73-bfe3-3fdd410ba590

Deployment details

Next steps

[Go to resource](#)

Enable the Firewall protection on the VNET we created:

In the Vnet we can check if the Firewall which we created is enabled or not.

Subu-FW-Vnet | Firewall

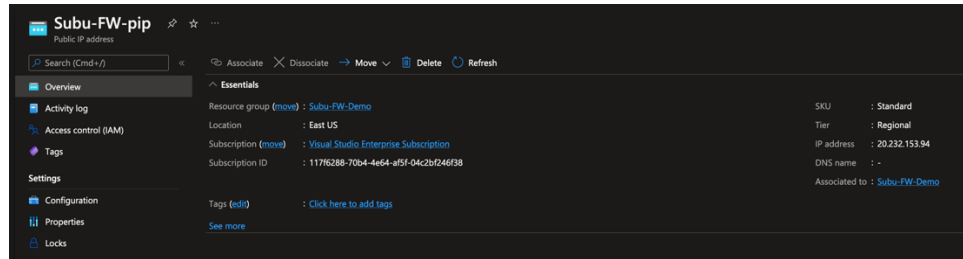
Search (Cmd+J)

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Address space Connected devices Subnets Bastion DDoS protection Firewall

Name	IP Address	Subnet
Subu-FW-Demo	10.3.2.4	AzureFirewallSubnet

Create a new Public IP:

Next step for us is to create a new Public IP so that we can link it with the Firewall to implement the rules.



Create a new VM to test the Firewall:

Create a new VM and add the same Vnet and Public IP to this VM so that we will be able to test the VM accordingly.

Create a virtual machine

✓ Validation passed

1 X Standard B1s
by Microsoft
[Terms of use](#) [Privacy policy](#)

Subscription credits apply ⓘ
0.0104 USD/hr
[Pricing for other VM sizes](#)

TERMS

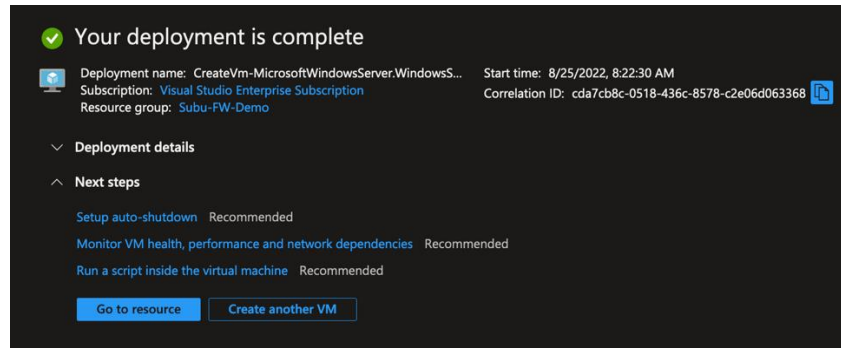
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	Visual Studio Enterprise Subscription
Resource group	Subu-FW-Demo
Virtual machine name	Subu-FW-demo-vm
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
Size	Standard B1s (1 vcpu, 1 GiB memory)
Username	testuser
Public inbound ports	None
Already have a Windows license?	Yes
License type	Windows Server
Azure Spot	No

Disks

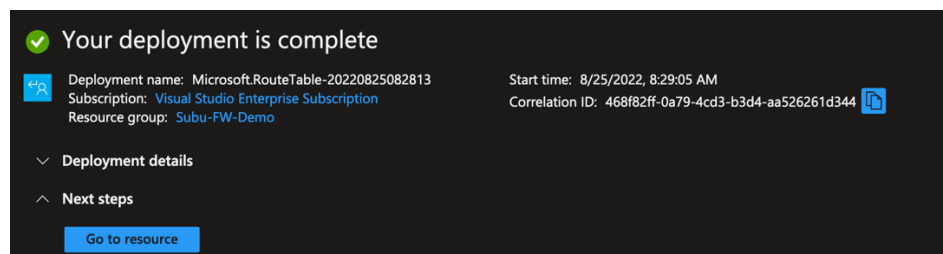
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No



Once the firewall is created then our work is to create the Route table and policies.

Create a new Route Table for Firewall:

Create a new Route Table to link the subnet and also the next hop to match the public IP of the firewall so that all the traffic will come and hit the firewall IP

A screenshot of the "Create Route table" form. The form has three tabs: "Basics", "Tags", and "Review + create". The "Basics" tab is selected. Under "Project details", there is a description: "Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources." Below this, there are two dropdown menus: "Subscription" (set to "Visual Studio Enterprise Subscription") and "Resource group" (set to "Subu-FW-Demo"). There is a "Create new" link next to the "Resource group" dropdown. Under "Instance details", there are two more dropdown menus: "Region" (set to "East US") and "Name" (set to "Demo-Route-FW"). At the bottom, there is a "Propagate gateway routes" section with two radio buttons: "Yes" (selected) and "No".

Associate subnet

Demo-Route-FW

Virtual network ⓘ

Subnet ⓘ

Demo-RT-FW

Demo-Route-FW

Address prefix destination ⓘ

IP Addresses

Destination IP addresses/CIDR ranges ⓘ

Next hop type ⓘ

Virtual appliance

Next hop address ⓘ

20.232.153.94

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Demo-Route-FW | Routes

Route table

Search (Cmd+/) Add Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Name	Address prefix	Next hop type
Demo-RT-FW	10.3.14/32	VirtualAppliance

Edit the Firewall Policies:

Next, we need to edit the firewall policies with different aspects.

Subu-FW-Demo

Resource group

Search (Cmd+/) Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Essentials

Subscription (move) : Visual Studio Enterprise Subscription

Subscription ID : 117f6288-70b4-4e64-af5f-04c2bf246f38

Tags (edit) : Click here to add tags

Deployments : 2 Succeeded

Location : East US

Resources Recommendations

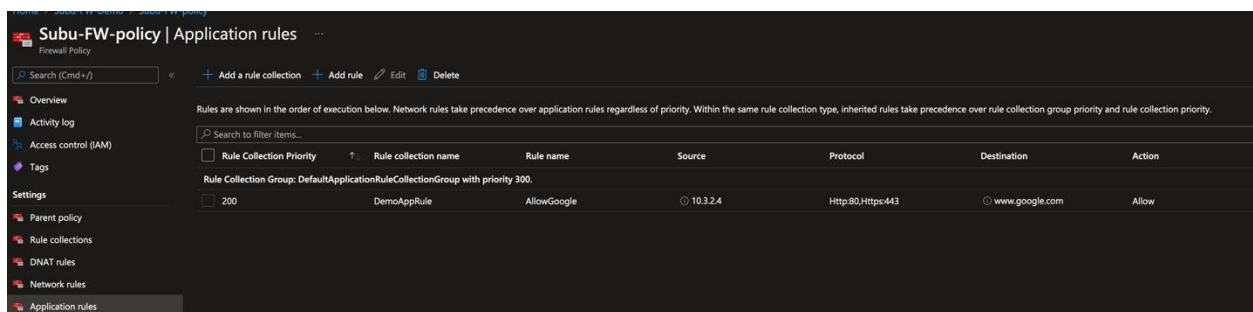
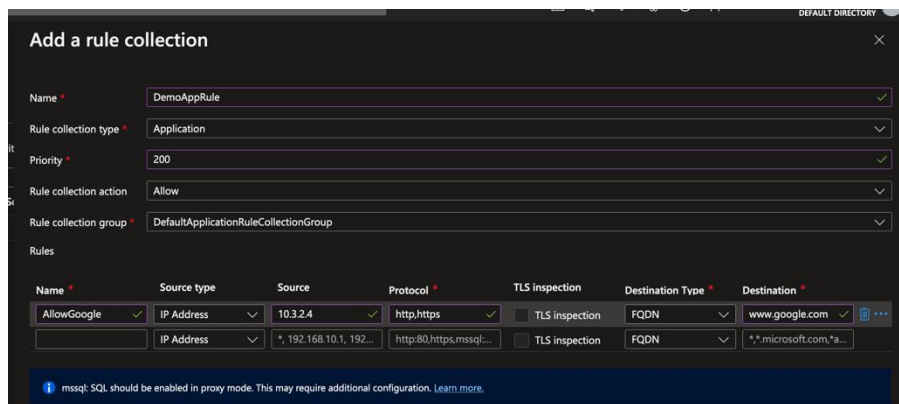
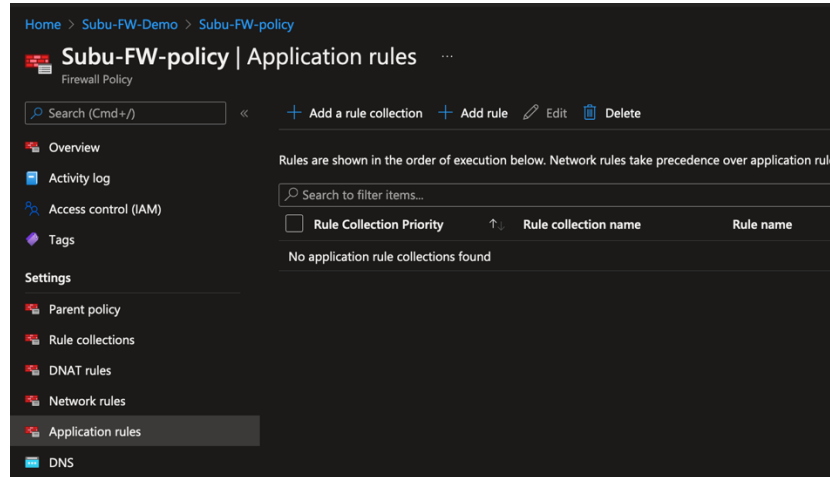
Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 4 of 4 records. Show hidden types

Name	Type	Location
Subu-FW-Demo	Firewall	East US
Subu-FW-pip	Public IP address	East US
Subu-FW-policy	Firewall Policy	East US
Subu-FW-Vnet	Virtual network	East US

Application Rules:

We can edit the Application rules to make sure that the corresponding websites with Allow and Deny rules.



Network Rules:

We can edit the Network rules to make sure that the corresponding websites with Allow and Deny rules.

Add a rule collection

Name *

DemoNetworkRule

✓

Rule collection type *

Network

✓

Priority *

200

✓

Rule collection action

Allow

✓

Rule collection group *

DefaultNetworkRuleCollectionGroup

✓

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Jenkins	IP Address	0.0.0.0/0	UDP	80	IP Address	10.3.1.4/32
Invalid argument: 'Prefix'. Reason: The prefix must be between 1 and 32.						
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*,10.0.0.1,10.1.0.0/1...

Subu-FW-policy | Network rules

Firewall Policy

Search (Cmd+V)

+ Add a rule collection

+ Add rule

Edit

Delete

Overview

Activity log

Access control (IAM)

Tags

Settings

Parent policy

Rule collections

DNAT rules

Network rules

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

<input type="checkbox"/>	Rule Collection Priority	Rule collection name	Rule name	Source	Port	Protocol	Destination	Action
Rule Collection Group: DefaultNetworkRuleCollectionGroup with priority 200.								
<input type="checkbox"/>	200	DemoNetworkRule	Jenkins	0.0.0.0/32	80	UDP	10.3.1.4/32	Allow

DNAT Rules:

We can edit the DNAT rules to make sure that the corresponding websites with Allow and Deny rules.

Add a rule collection

Name *

DemoDNATRule

✓

Rule collection type *

DNAT

✓

Priority *

200

✓

Rule collection action

Destination Network Address Translation (DNAT)

✓

Rule collection group *

DefaultDnatRuleCollectionGroup

✓

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *	Transla
RDP Rule	IP Address	0.0.0.0	2 selected	3389	IP Address	20.232.153.94	10.3.1
	IP Address	*, 192.168.10.1, 192...	0 selected	8080	IP Address	192.168.10.1	192.1

Subu-FW-policy | DNAT rules

Firewall Policy

Search (Cmd+J) + Add a rule collection + Add rule Edit Delete

Overview

Activity log

Access control (IAM)

Tags

Settings

Parent policy

Rule collections

DNAT rules

Network rules

Application rules

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection Priority	Rule collection name	Rule name	Source	Port	Protocol	Destination	Translated Address ...	Translated Port	Action
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.									
200	DemoDNATRule	RDP Rule	0.0.0.0	3389	TCP/UDP	20.232.153.94	10.3.1.4	3389	Dnat

Check the Firewall policies Real time:

Login to the VM using the RDP. We do not have the public IP of the VM, so we will use the Firewall IP to do the RDP to login to the Server.

Add PC

PC name: 20.232.153.94

User account: testuser

General Display Devices & Audio Folders

Friendly name: 20.232.153.94

Group: Saved PCs

Gateway: No gateway

☒ Bypass for local addresses

☒ Reconnect if the connection is dropped

☐ Connect to an admin session

☐ Swap mouse buttons

Cancel Add

Add a User Account

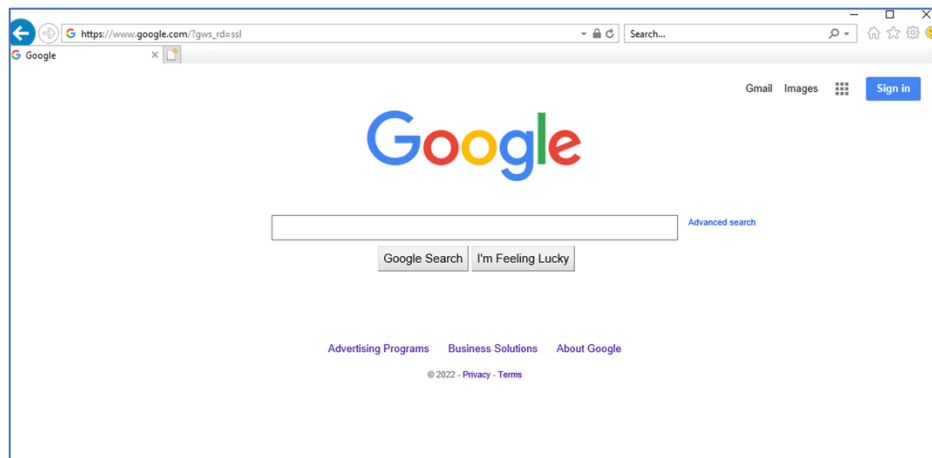
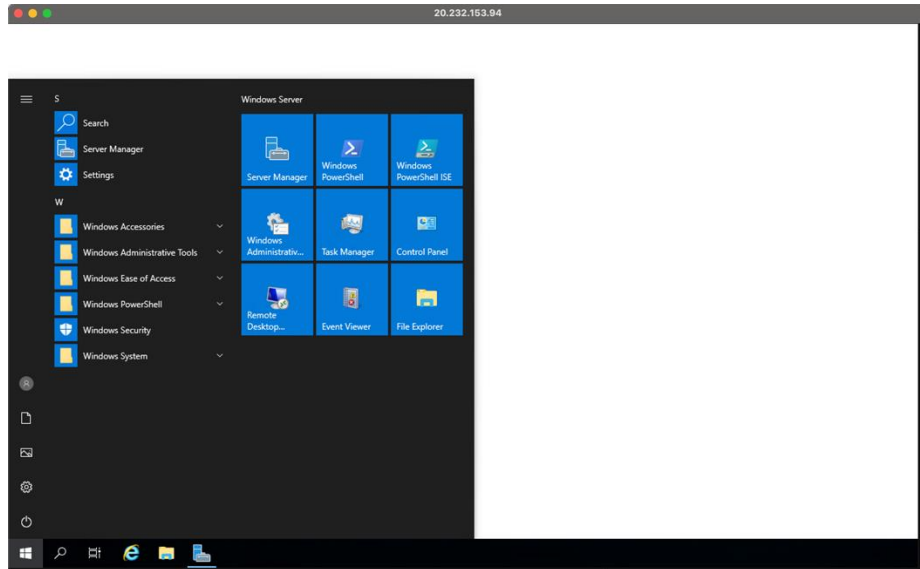
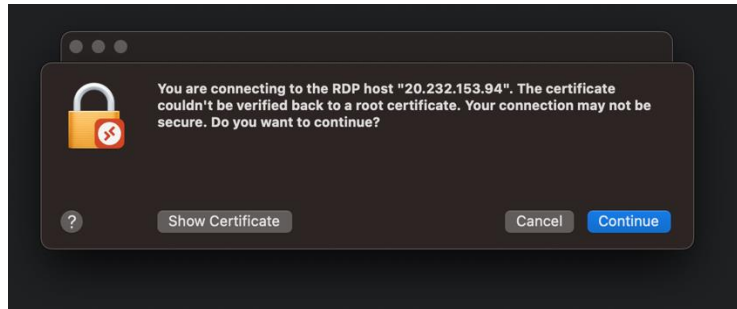
Username: testuser

Password: ●●●●●●●●

☐ Show password

Friendly name: 20.232.153.94

Cancel Add



When we try to access any other websites apart from allowed entry of Google.com then we will get the below error.

