Configuring the Oracle SBC hosted on Azure Cloud with Microsoft Teams Direct Routing

Technical Application Note

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Added MSTeams specific configuration on Azure Cloud and SBC.	10-10-2019

Table of Contents

Introduction

This document describes how to connect the Oracle SBC in Azure cloud to Microsoft Teams Direct Routing environment. This paper is intended for IT or telephony professionals.

Configuring the SBC

Like the on-premises SBC, the VMSBC can also be connected to the Microsoft Teams Direct Routing. Here the platform is called as VME.

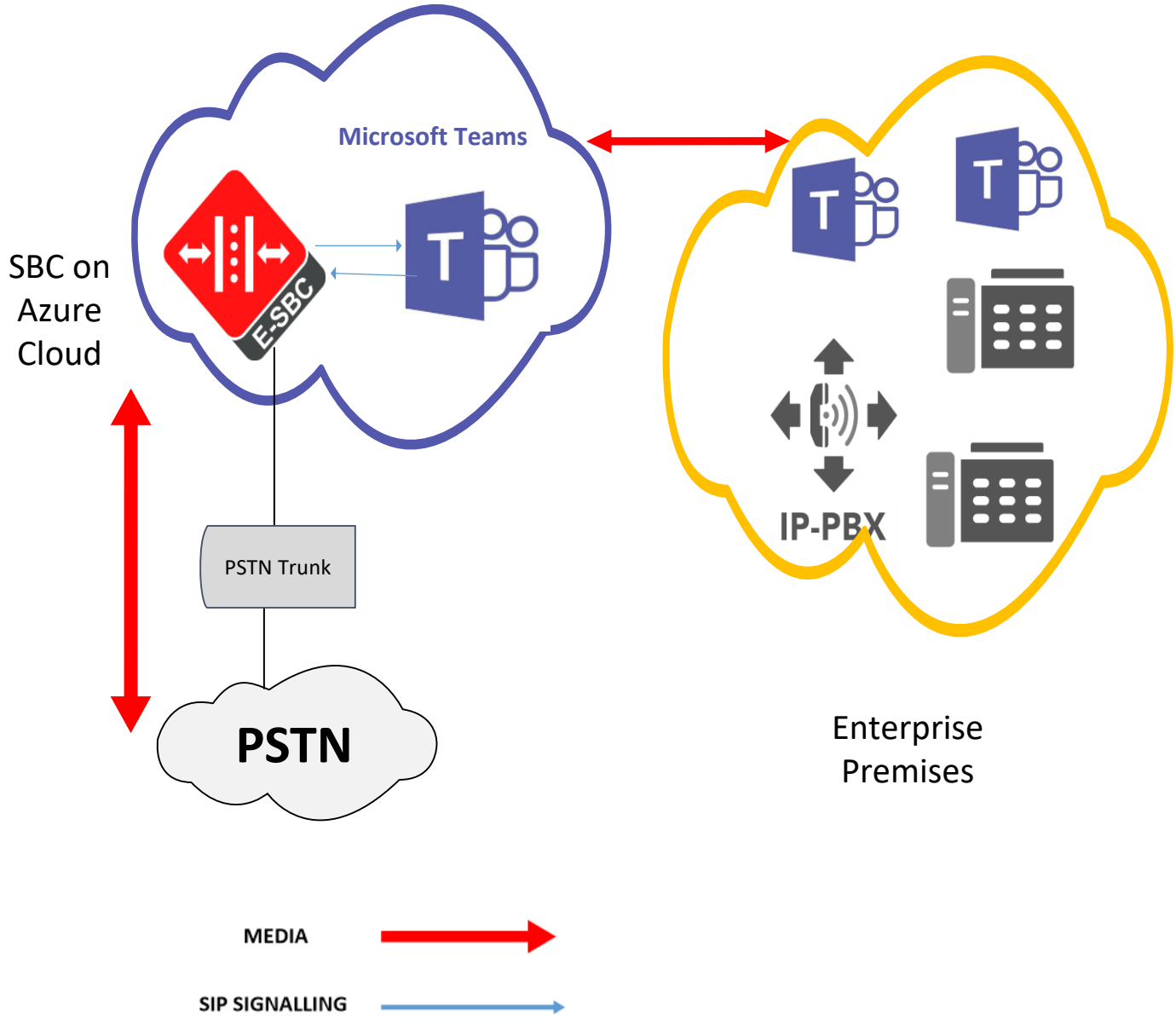


Figure :1: Signaling & media flow with media-bypass disabled

There are several connection entities on the picture:

- Enterprise network consisting of Teams client
- SBC on Azure Cloud
- Microsoft Teams Direct Routing Interface
- PSTN trunk from a 3rd party provider

These instructions cover configuration steps between the Oracle SBC and Microsoft Teams Direct Routing Interface. The interconnection of other entities, such as connection of the PSTN trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of respective components.

Deploying Oracle SBC on the Azure Cloud

This document assumes that Oracle SBC is up and running in the Azure cloud. If the customer is looking to deploy a new SBC on the Azure cloud, please follow the documentation here.

https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/OCSBC-Deployed-In-Azure.pdf

Configuring the Azure Cloud to support Direct Routing

To support direct routing on Azure cloud, the following configuration changes are required to the Oracle SBC instance running on the Azure cloud

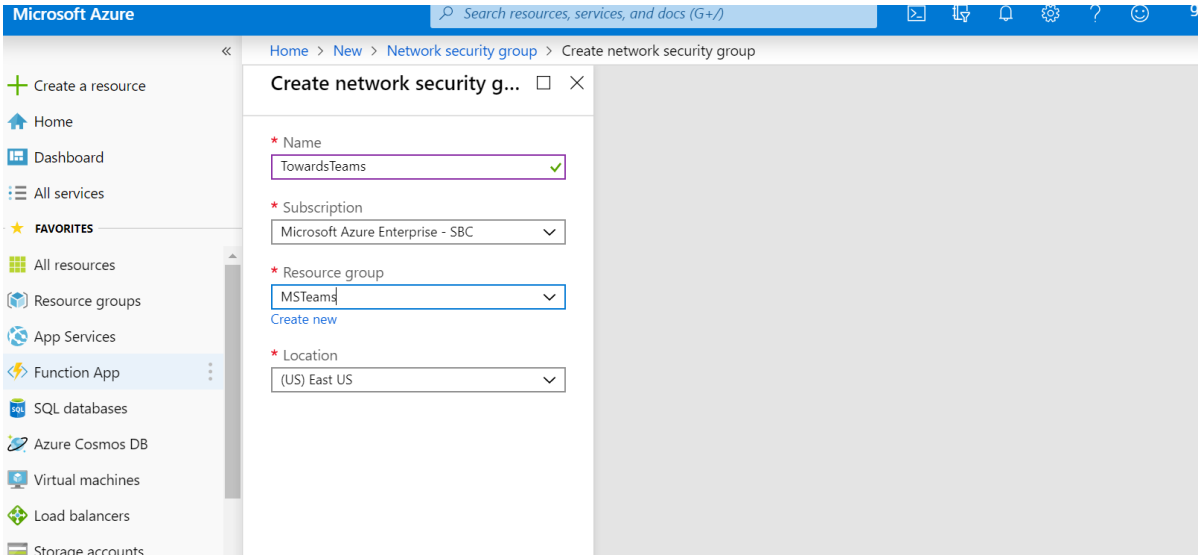
- Network security configuration
- Network Interfaces with a static public IP
- Attaching network interfaces to the Oracle SBC

Network Security configuration

Network Security Group for Media Interfaces

Create network security group for media interfaces. Here we will be creating two network security groups.

- Towards MS Teams
- Towards PSTN



From Azure's navigation list on the left side of the portal, click Create a resource, Networking, Network Security Group Configure the following for the Media Interface Network Security Group:

- Name
- Resource Group
- Location
- Click Create

Note: The Resource group and location should be the same used in deploying the Oracle SBC in Azure.

The following TCP/UDP protocols and/or ports should be opened for the Media Interface NSG "TowardsTeams"

Inbound Rules for network interface facing Teams

The below table shows the ports to be opened for **Non-Media bypass Configuration.**

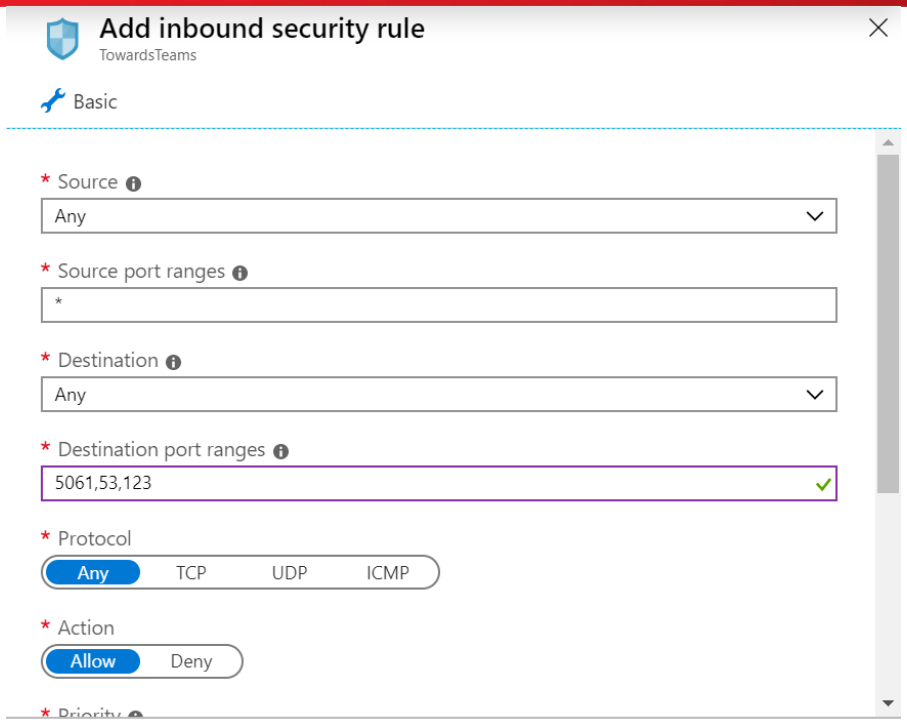
Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	*	Any	5061	TCP
Any	*	Any	53	*
Any	49152-53247	Any	10000-20000*	UDP
Any	*	Any	123	UDP

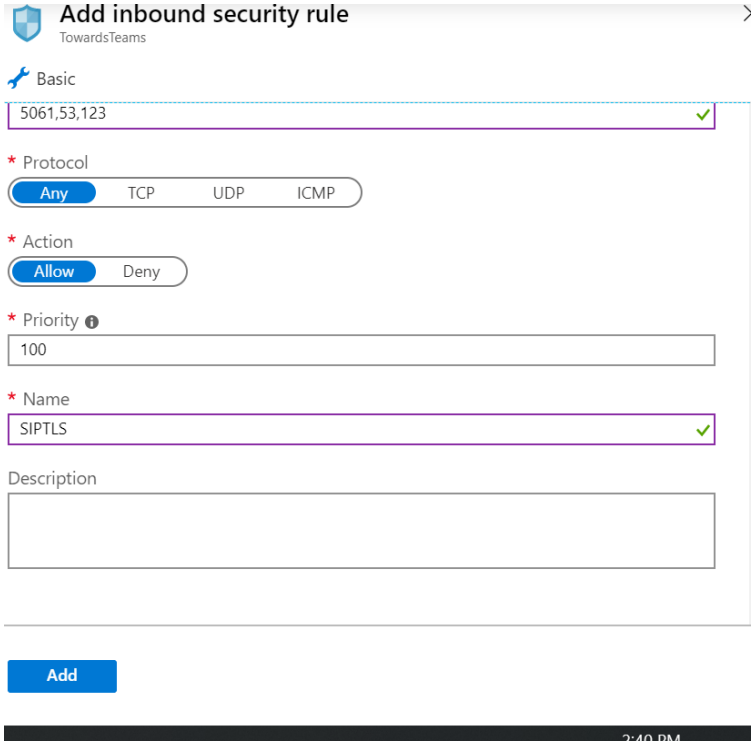
Here 10000-20000* specifies the steering pool configured on the SBC.(i.e the media port range of the SBC)
The ports 49152-53247 are defined as per Microsoft documentation for non-media bypass configuration
For more information on the ports to be configured for non-media bypass configuration, please click on the link below..
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-ports

Please use the table below for **Media bypass configuration**

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	*	Any	5061	TCP
Any	*	Any	53	*
Any	50000-50019	Any	10000-20000*	UDP
Any	*	Any	123	UDP

Similarly ,10000-20000* specifies the steering pool configured on the SBC.
The ports 49152-53247 are defined as per Microsoft documentation for media bypass configuration
For more information on the ports to be configured for media bypass configuration, please click on the link below.
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass





Refer the above tables and create inbound media rule according to your environment.
Note: Set priority as 110 for the media rules.

Outbound Rules for network interface facing Teams

The below table shows the ports to be opened for **Non-Media bypass Configuration.**

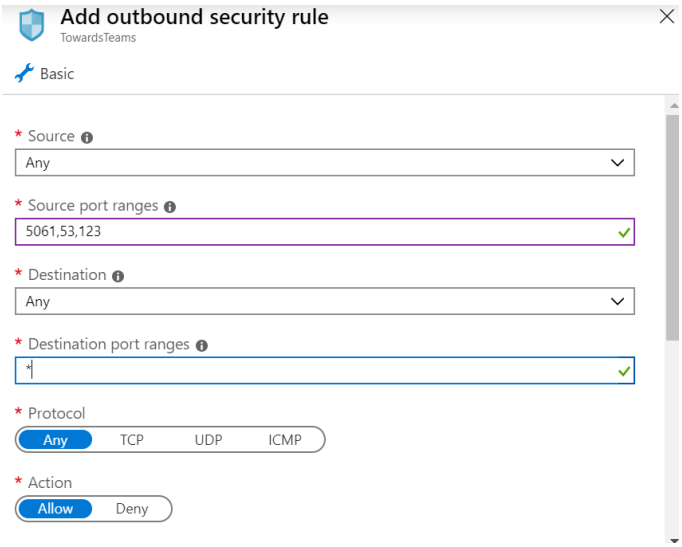
Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	5061	Any	*	TCP
Any	53	Any	*	*
Any	10000-20000*	Any	49152-53247	UDP
any	123	Any	*	UDP

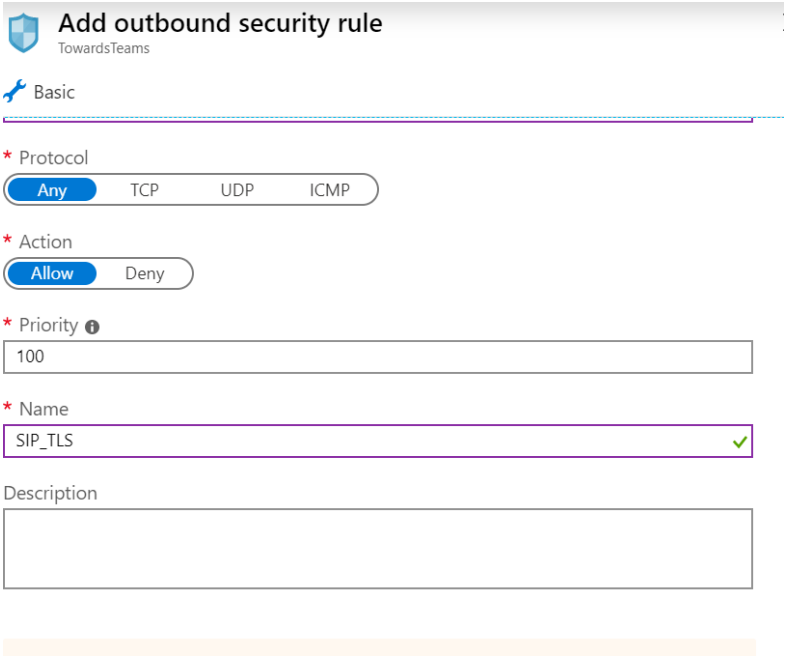
Here 10000-20000* specifies the steering pool configured on the SBC.(i.e the media port range of the SBC)
The ports 49152-53247 are defined as per Microsoft documentation for non-media bypass configuration
For more information on the ports to be configured for non-media bypass configuration, please click on the link below.
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-ports

Please use the table below for **Media bypass configuration**

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	5061	Any	*	TCP
Any	53	Any	*	*
Any	10000-20000*	Any	50000-50019	UDP
Any	123	Any	*	UDP

Similarly ,10000-20000* specifies the steering pool configured on the SBC.
The ports 49152-53247 are defined as per Microsoft documentation for media bypass configuration
For more information on the ports to be configured for media bypass configuration, please click on the link below.
https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass





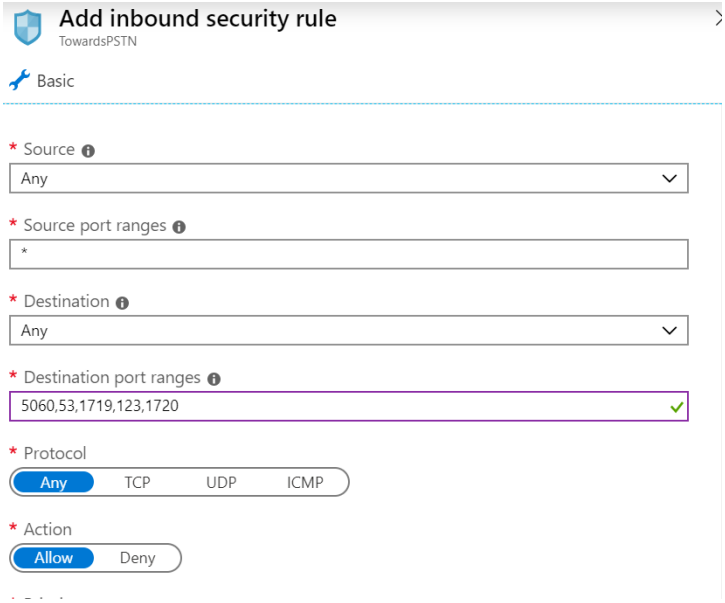
Refer the above tables and create outbound media rule according to your environment.
Note: Set priority as 110 for the media rules.

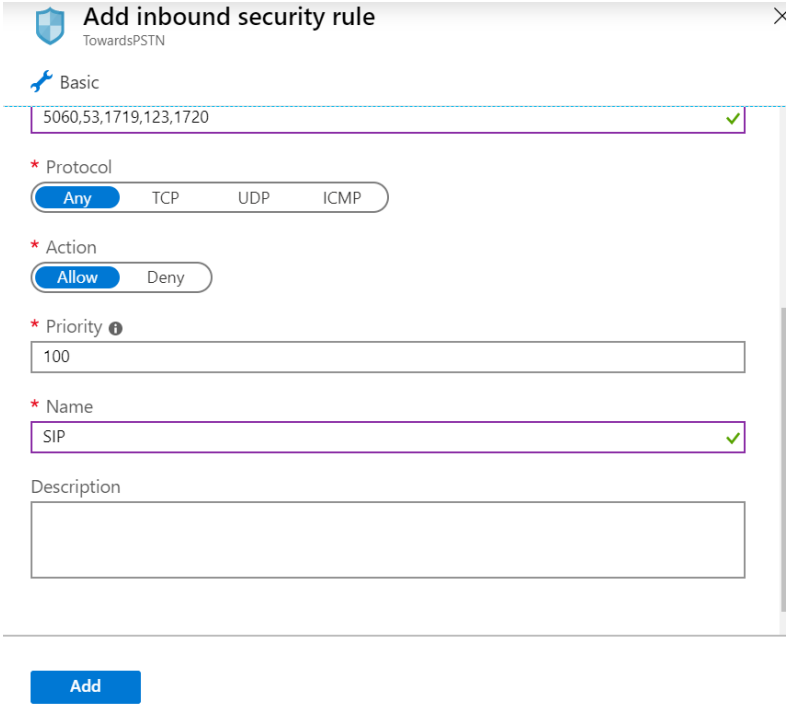
Inbound Rules for network interface facing PSTN

For the NSG "TowardsPSTN",create the following inbound rules.
Please note, the port matrix below is an example only. The ports opened during installation should depend on the environment needs and user preferences.

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	*	Any	5060	UDP
Any	*	Any	53	*
Any	*	Any	1719	UDP
Any	*	Any	123	UDP
Any	*	Any	1720	UDP
Any	*	Any	20000-30000*	UDP

Here 20000-30000 is the steering pool for PSTN side configured on SBC.





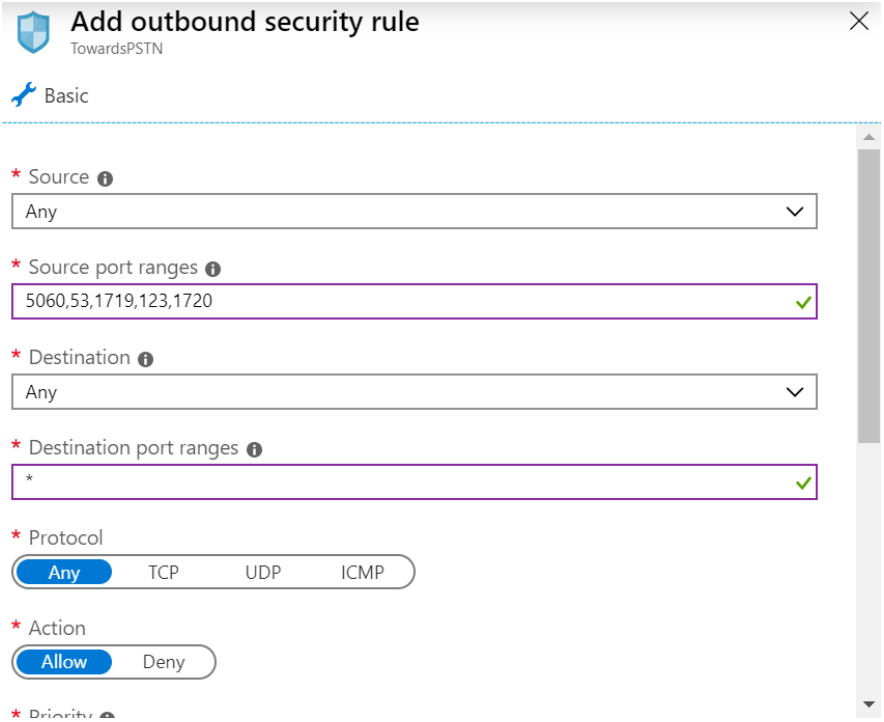
Refer the above tables and create inbound media rule according to your environment.
Note: Set priority as 110 for the media rules.

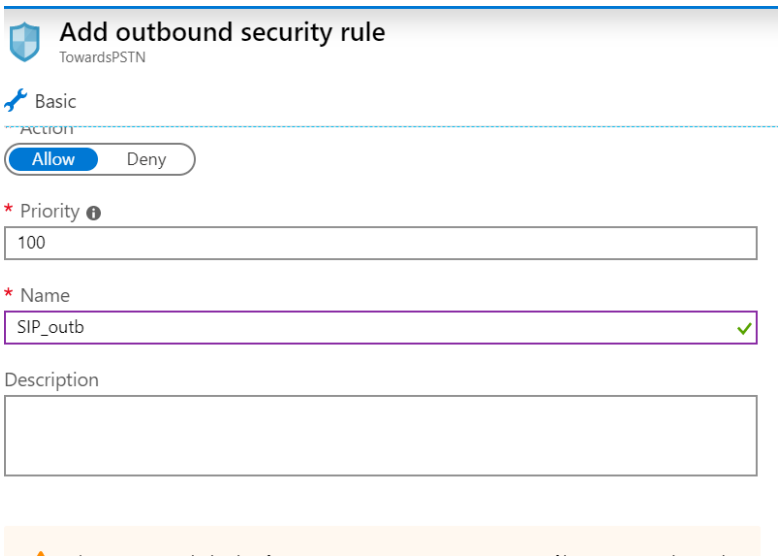
Outbound Rules for network interface facing PSTN

For the NSG “TowardsPSTN”,create the following outbound rules.

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	5060	Any	*	UDP
Any	53	Any	*	*
Any	1719	Any	*	UDP
Any	123	Any	*	UDP
Any	1720	Any	*	UDP
Any	20000-30000*	Any	*	UDP

Here 20000-30000 is the steering pool for PSTN side configured on SBC.





Refer the above tables and create outbound media rule according to your environment.
Note: Set priority as 110 for the media rules.

Create Network Interfaces on Azure cloud

For MS Teams deployment, we have to create two network interfaces

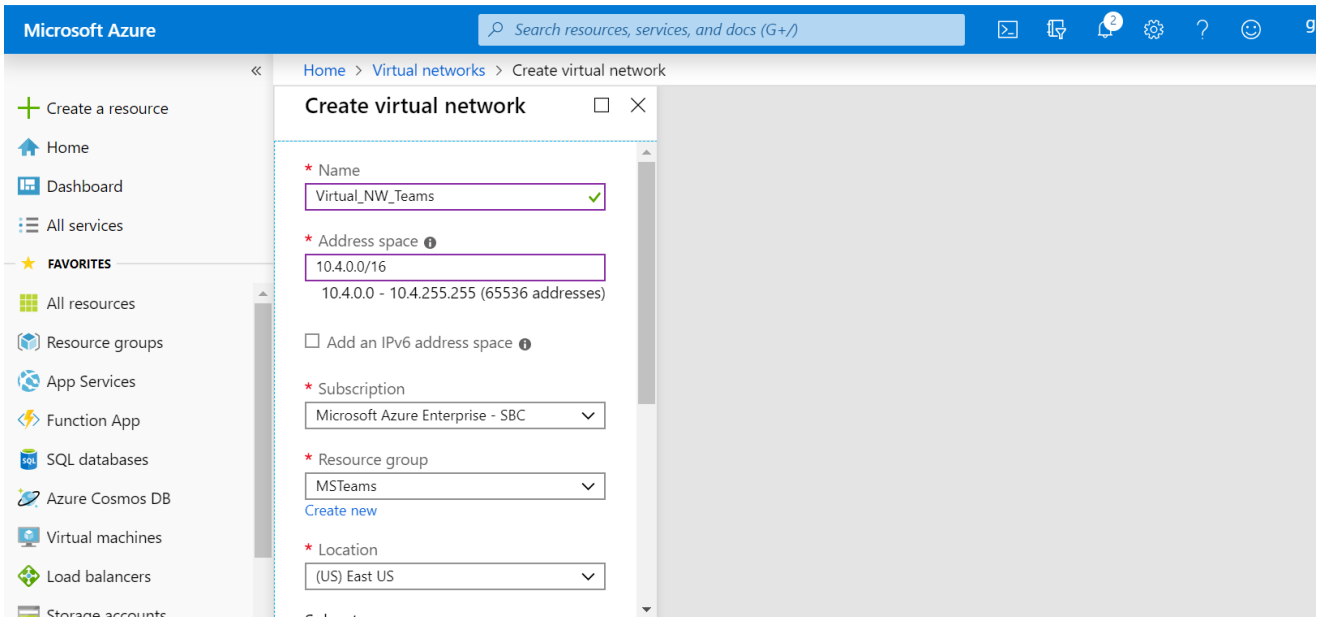
- S0P0-Facing the PSTN trunk
- S0P1-Facing the MS Teams

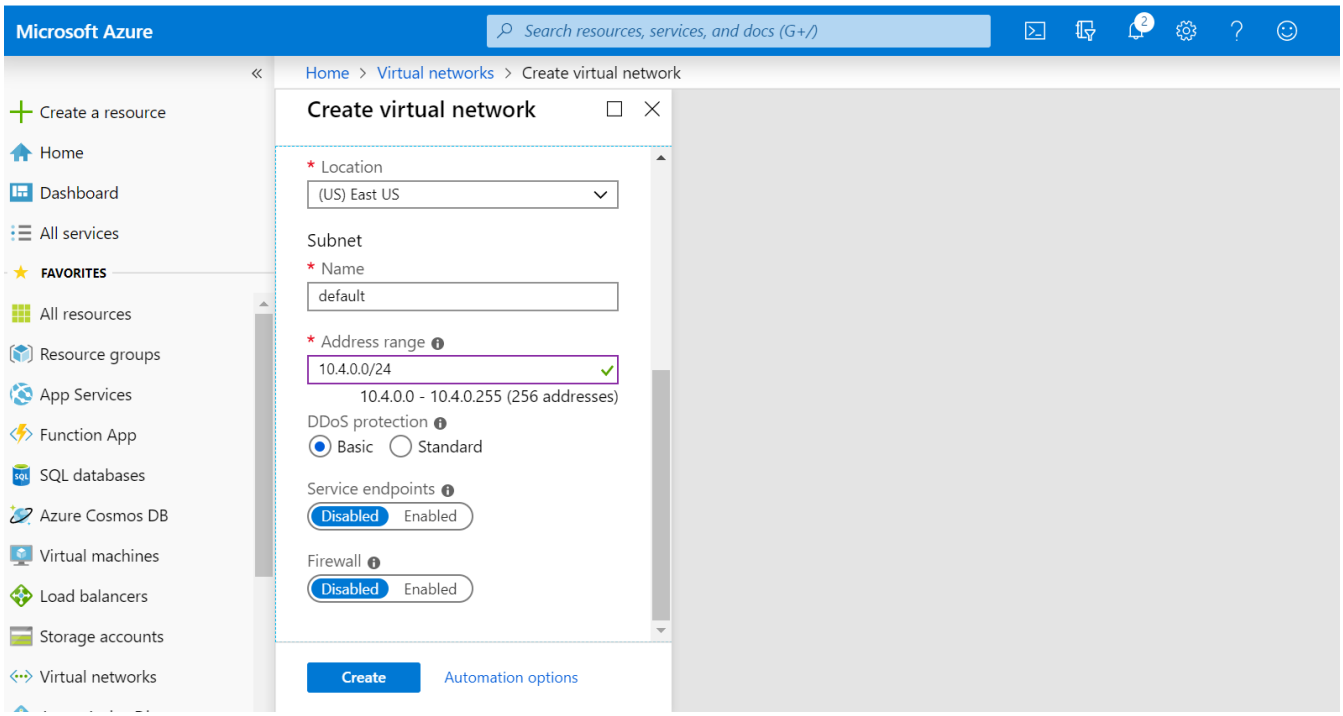
Before creating the network interface ,create virtual networks to be associated with network interfaces.

Create virtual Network

Provide the following information in the designated fields:

- Virtual Network Name
- Address Space: (below example is Azure provided)
- Subscription
- Resource Group (created above)
- Location (same as Resource Group location)





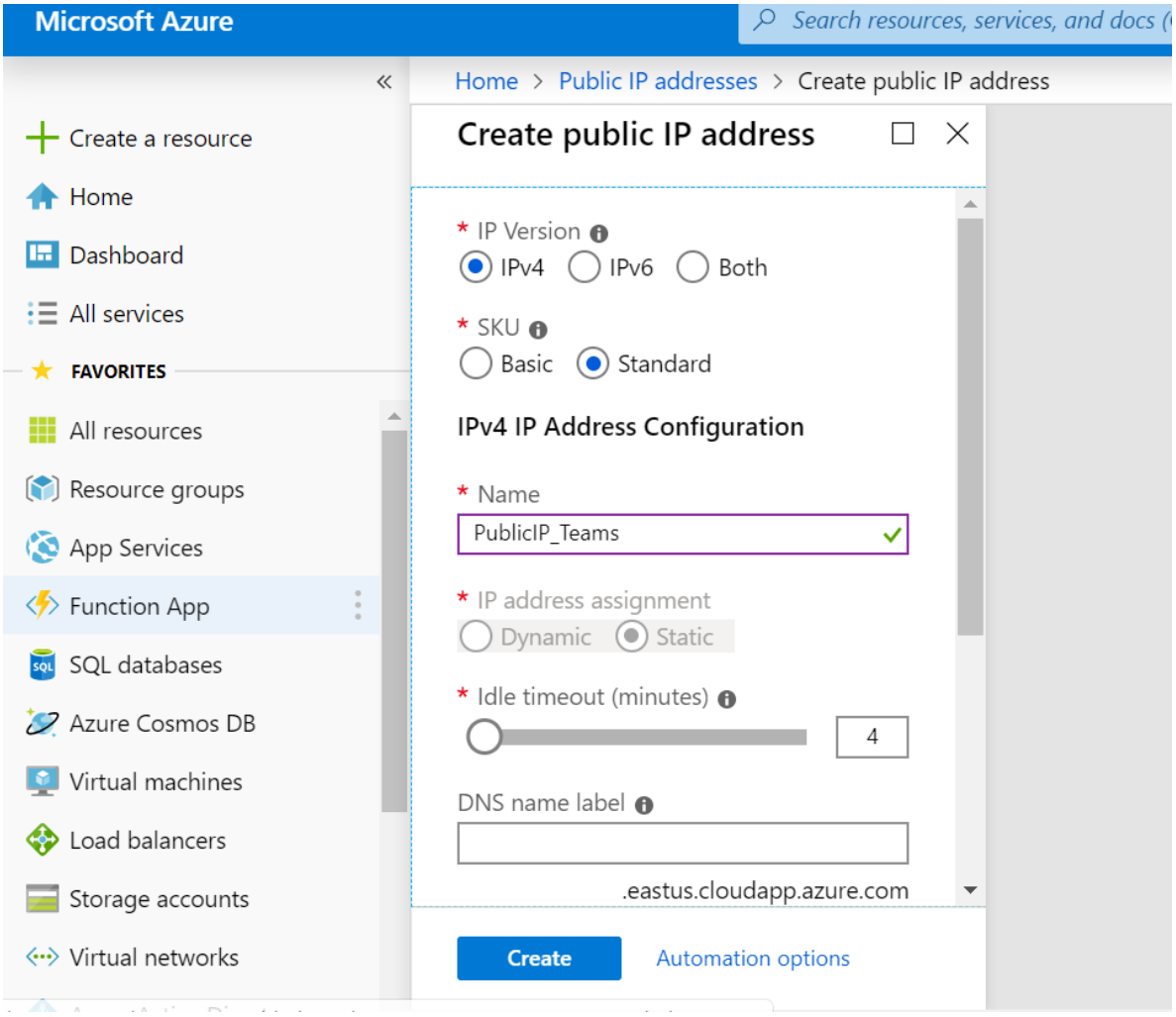
Similarly, create a virtual network for the PSTN side.

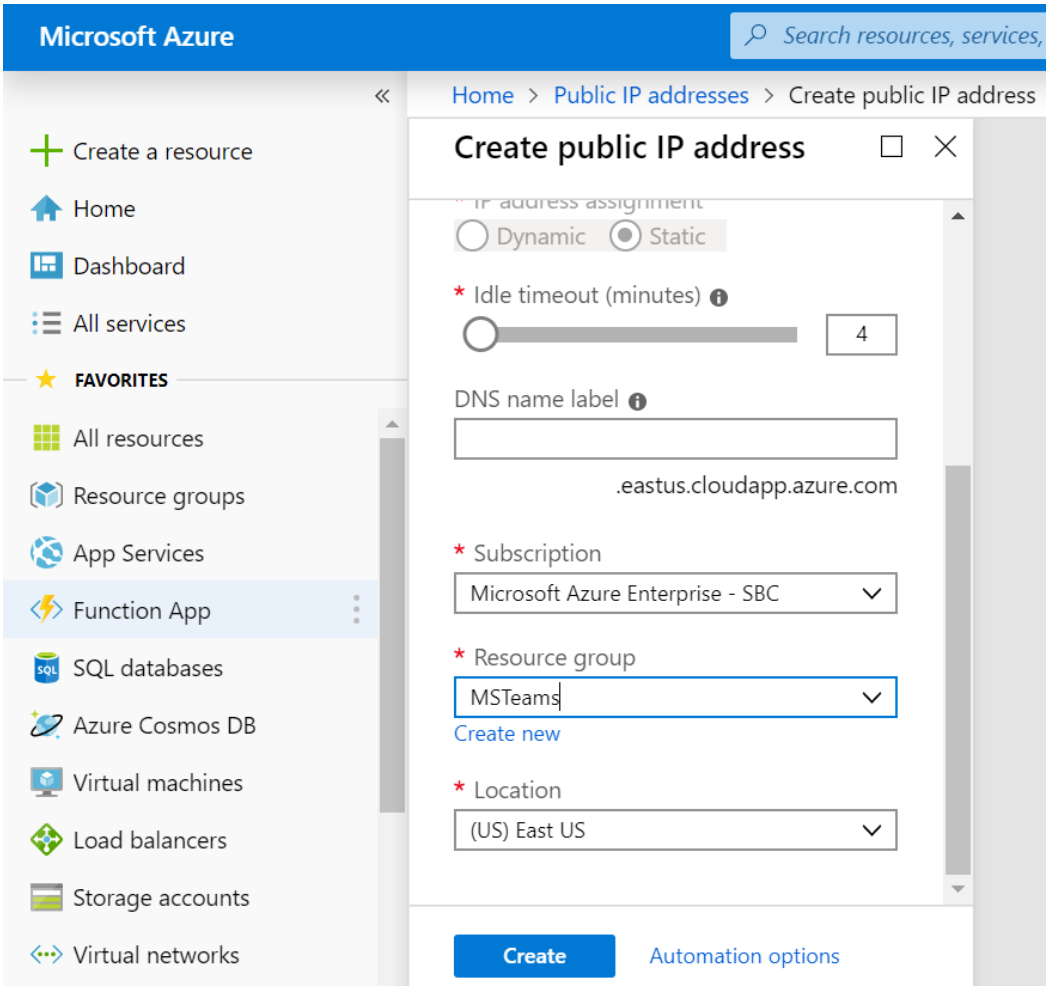
Creating Public IP

Create Public IP in the resource groups to be associated with the network interfaces.

Provide the following information in the designated fields:

- Name of the Public IP address
- Subscription
- Resource Group (created above)
- Location (same as Resource Group location)
- SKU type as Standard





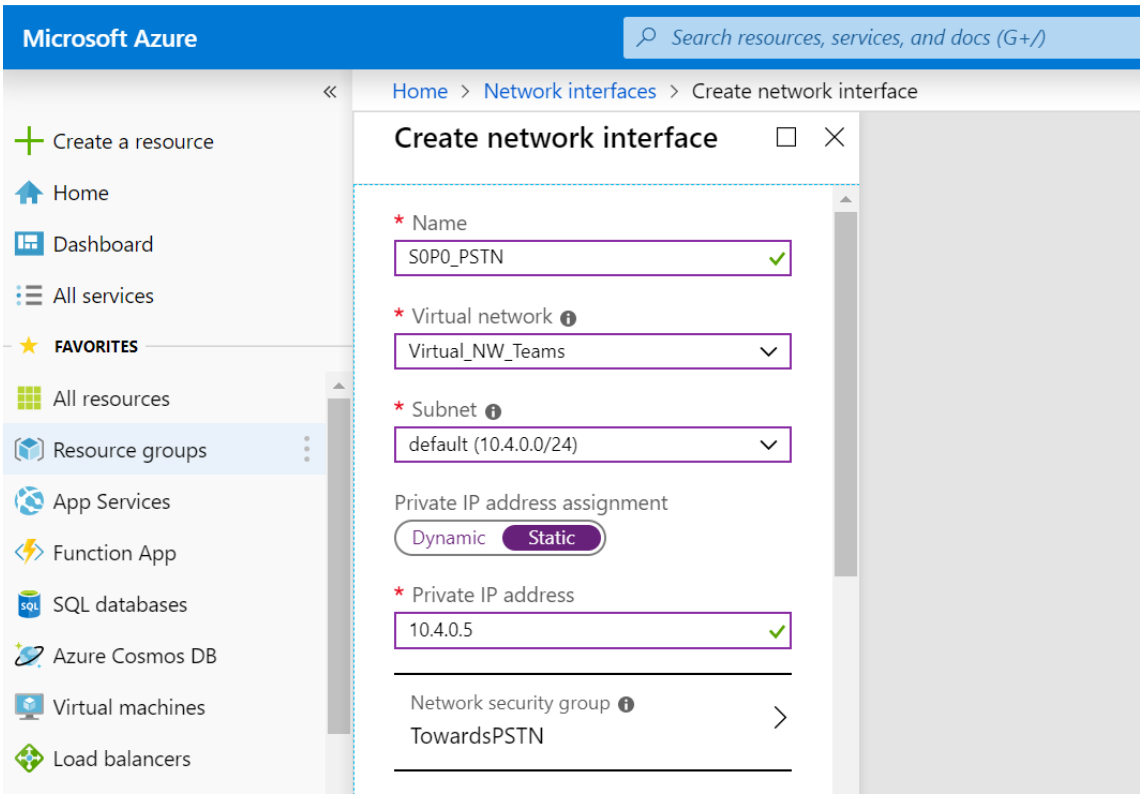
Creating network interfaces

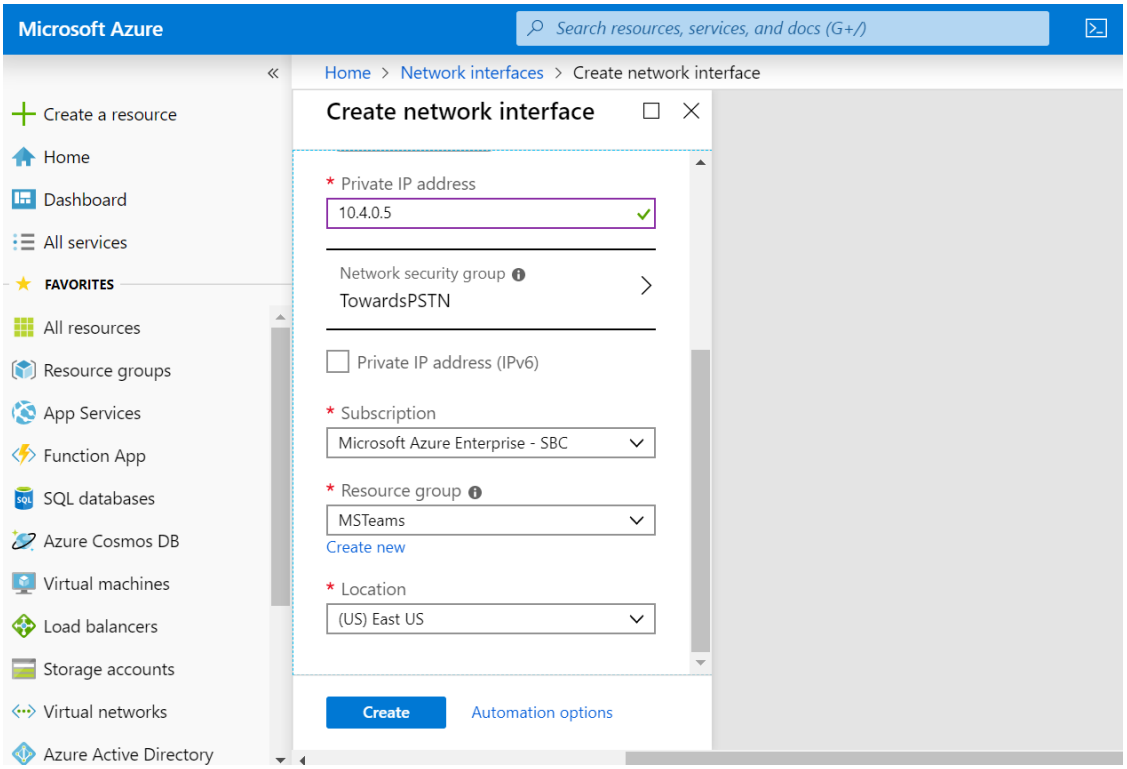
For MS Teams deployment, we have to create two network interfaces

- S0P0-Facing the PSTN trunk
- S0P1-Facing the MS Teams

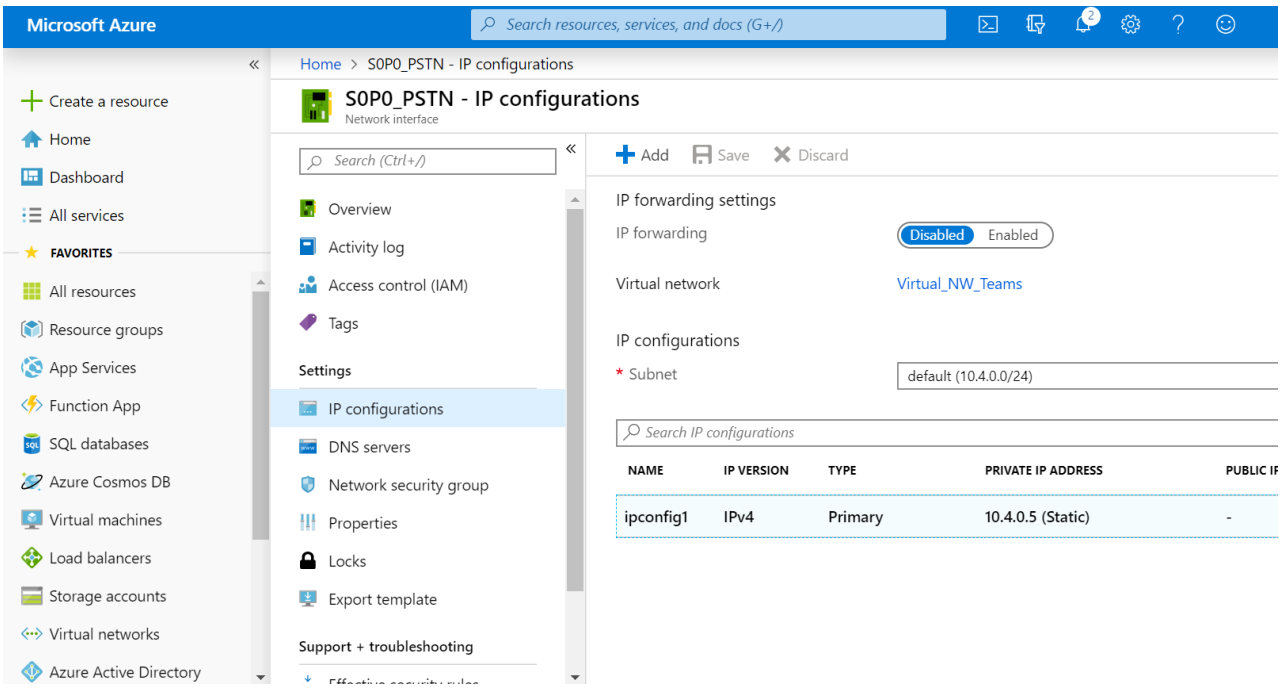
Configure the applicable Create Network interface fields, including:

- Name: S0P0_PSTN
- Subnet: From the drop down, select the subnet created for S0P0 interface
- Private IP: Set to static
- Private IP Address: Set to an address within the subnet, in this case, we're using 10.4.0.5
- Network Security Group: Select the group configured for SBC media Interfaces

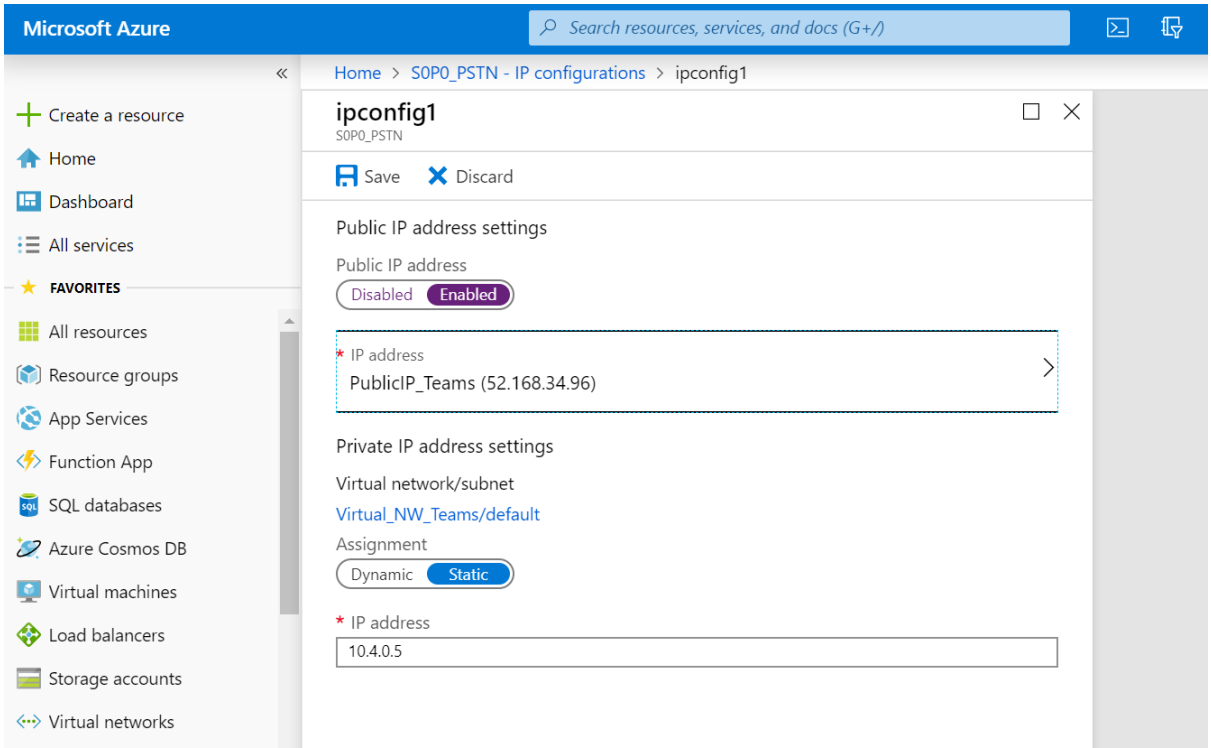

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Network interfaces > Create network interface
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Create network interface
* Name
S0P0_PSTN
* Virtual network
Virtual_NW_Teams
* Subnet
default (10.4.0.0/24)
Private IP address assignment
Dynamic
Static
* Private IP address
10.4.0.5
Network security group
TowardsPSTN



After the network interfaces are created ,go to the network interface and click on IP configurations.



Enable the Public IP address and associate the Public IP created previously.Save the config after that.



Follow the above procedure and create S0P1 interface facing the Teams side.

Attaching network interfaces to the Oracle SBC

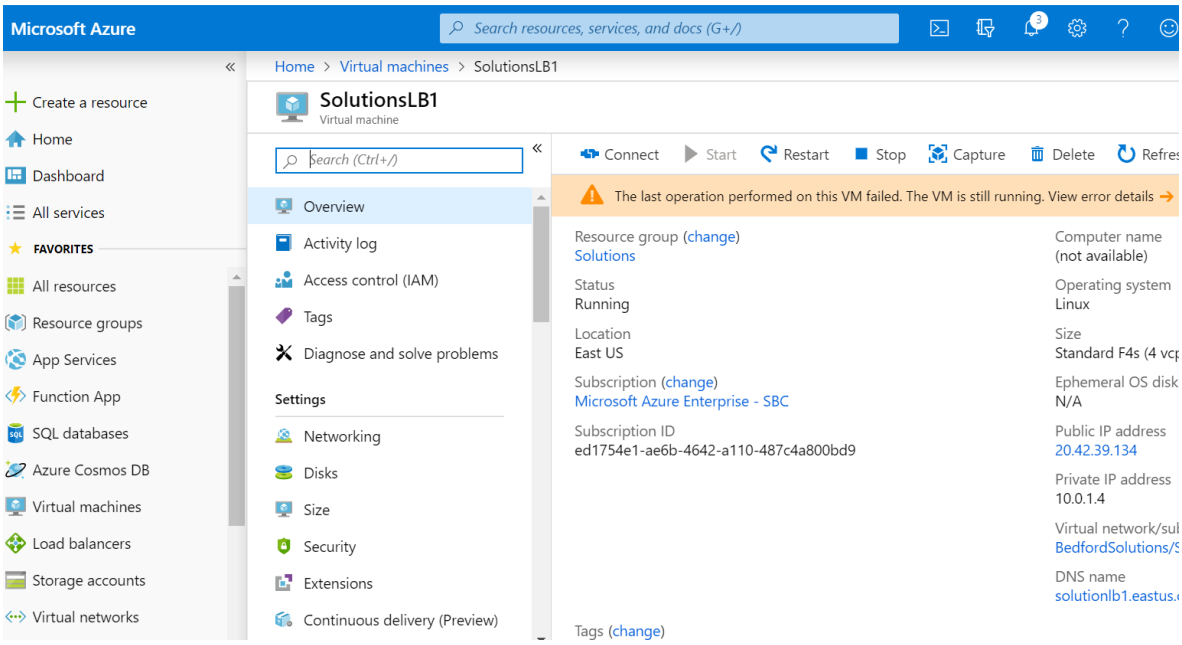
Once the network interfaces are created ,they have to be attached to the Oracle VM running on Azure.

Azure requires that we stop the SBC instance before we can create or attach additional networking interfaces for Media.

From Azure's navigation list, on the left side of the portal, Select “Virtual machines”

Select the instance we created previously . Once you select it, you will see displayed an instance-specific navigation pane on the left side of the dialog

- At the top, click on “Stop”
- Once the VM is stopped and deallocated, click on Networking under Settings in the instance specific navigation menu.



Next, “Attach Network Interface” and attach the two previously created network interfaces S0P0-PSTN and S0P1-MSTeams

Start your instance after creating and attaching all interfaces.

About Microsoft Teams Direct Routing

Microsoft Teams Direct Routing allows a customer provided SBC to connect to Microsoft Phone System. The customer provided SBC can be connected to almost any telephony trunk or interconnect 3rd party PSTN equipment. The scenario allows:

- Use virtually any PSTN trunk with Microsoft Phone System;
- Oracle Enterprise Session Border Controllers are Microsoft certified to work for Direct Routing. Additional information can be found at

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers

Planning Direct Routing

If you are planning to configure direct routing with Oracle SBC , you must ensure that the following prerequisites are completed before proceeding further

- Licensing and DNS requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs

Licensing Requirements

Make sure that the following license requirements are met by the Direct routing users.(ie the users must be assigned the following licenses in Office 365)

- Microsoft Phone System
- Microsoft Teams + Skype for Business Plan 2 if included in Licensing Sku

DNS Requirements

Create DNS records for domains in your network that resolve to your SBC .

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address (Assigned to the MS Teams interface on Azure cloud)
- FQDN name resolving to the above mentioned Public IP address

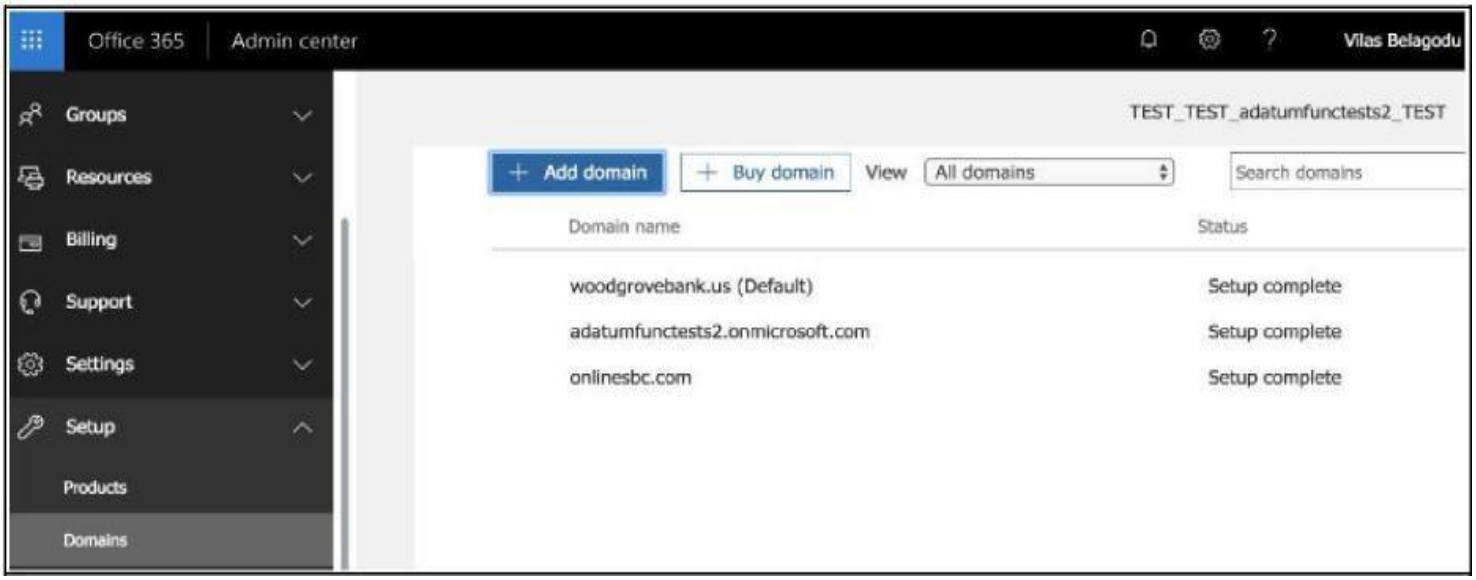
SBC Domain Names

The SBC domain name must be from one of the names registered in “Domains” of the tenant. You cannot use the *.onmicrosoft.com tenant for the domain name.

For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can be used for SBC FQDN	Examples of FQDN names
woodgrovebank.us	Yes	Valid names: • sbc1.woodgrovebank.us • ussbcs15.woodgrovebank.us • europe.woodgrovebank.us Non-Valid name: • sbc1.europe.woodgrovebank.us (requires registering domain name europe.atatum.biz in "Domains" first)
woodgrovebankus.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names
hybrdvoice.org	Yes	Valid names: • sbc1. hybridvoice.org • ussbcs15. hybridvoice.org • europe. hybridvoice.org Non-Valid name: • sbc1.europe.hybridvoice.org (requires registering domain name europe. hybridvoice.org in "Domains" first)

Please activate and register the domain of tenant.



In this document the following FQDN and IP is used as an example:

Here 52.168.x.x is the public IP of the Azure cloud configured for interface facing MS Teams side

Public IP	FQDN
52.168.x.x	oracleesbc2.woodgrovebank.us

Public trusted certificate for the SBC

It is necessary to setup a public trusted certificate for direct routing. This certificate is used to establish TLS connection between Oracle SBC and MS Teams. The certificate needs to have the SBC FQDN in the subject, common name, or subject alternate name fields. For root certificate authorities used to generate SBC certificate ,refer to Microsoft documentation. https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

Please refer to the Oracle SBC with Microsoft Teams documentation suitable for your environment (media bypass/non-media bypass) and model (enterprise and carrier) for the steps to configure the following,

- Configure Direct Routing –For pairing the SBC with direct routing
- Microsoft Teams Direct Routing Interface characteristics
- Requirements to SIP messages “Invite” and “Options” – For SIP syntax changes according to MS Teams requirements

The links for the documentation are provided here

SBC configuration

This document explains specific changes on the SBC in the Azure cloud environment.

For detailed configuration of Oracle SBC with Microsoft Teams Media Bypass refer to

Oracle ESBC with Microsoft Teams Media Bypass - Enterprise Mode
https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB-Enabled.pdf

For detailed configuration of Oracle SBC with Microsoft Teams Non-Media Bypass – Enterprise mode refer to
https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-NON-MB.pdf

For detailed configuration of Oracle SBC with Microsoft Teams Non- Media Bypass – Carrier Model refer to
https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/ESBC%20with%20MS%20Teams%20CarrierModel.pdf

Interface Mapping

The final step in deploying the Oracle SBC in Azure Public cloud is to verify the network interfaces have MAC addresses assigned to them.

- Access the serial console through the Azure portal under support + troubleshooting
- Log into enable mode
- Run the command

```
>show interface mapping
Interface Mapping Info
-----------------------------------------
Eth-IF  MAC-Addr                Label
wancom0 00:0D:3A:10:5D:FB       #generic
wancom1 00:0D:3A:17:F0:38       #generic
s0p0    00:0D:3A:17:FB:EF       #generic
wancom2 FF:FF:FF:FF:FF:FF       #dummy
spare   FF:FF:FF:FF:FF:FF       #dummy
s1p0    FF:FF:FF:FF:FF:FF       #dummy
s0p1    FF:FF:FF:FF:FF:FF       #dummy
s1p1    FF:FF:FF:FF:FF:FF       #dummy
s0p2    FF:FF:FF:FF:FF:FF       #dummy
s1p2    FF:FF:FF:FF:FF:FF       #dummy
s0p3    FF:FF:FF:FF:FF:FF       #dummy
s1p3    FF:FF:FF:FF:FF:FF       #dummy
```

- As you can see above, since we have not configured all eight network interfaces possible on the SBC, we'll need to correct the interface to MAC address mappings.
- The interface mapping branch on the SBC includes a swap command, which allows us to make those adjustments. A reboot is required for the changes to take effect.
- While in enable mode in the SBC CLI, type:

```
> # interface-mapping (enter)
> (interface-mapping)# swap wancom1 s1p0
Interface Mapping Info after swapping
-----------------------------------------
Eth-IF  MAC-Addr                Label
wancom0 00:0D:3A:10:5D:FB       #generic
wancom1 FF:FF:FF:FF:FF:FF       #dummy
s0p0    00:0D:3A:17:FB:EF       #generic
wancom2 FF:FF:FF:FF:FF:FF       #dummy
spare   FF:FF:FF:FF:FF:FF       #dummy
s1p0    00:0D:3A:17:F0:38       #generic
s0p1    FF:FF:FF:FF:FF:FF       #dummy
s1p1    FF:FF:FF:FF:FF:FF       #dummy
s0p2    FF:FF:FF:FF:FF:FF       #dummy
s1p2    FF:FF:FF:FF:FF:FF       #dummy
s0p3    FF:FF:FF:FF:FF:FF       #dummy
s1p3    FF:FF:FF:FF:FF:FF       #dummy
Changes could affect service, and Requires Reboot to become effective.
Continue [y/n]?: y (enter)
```

When the SBC comes back up from reboot, it is now ready for full configuration.

Note: This setting is available only through the CLI now. GUI will be enhanced in the near future to support this feature.

Also note that the usage of “swap” command is based on customer environment. Depending on the setup ,the mapping may vary.

System-Config in SBC

The CLI users can access the configuration by accessing configure terminal->system->system-config .

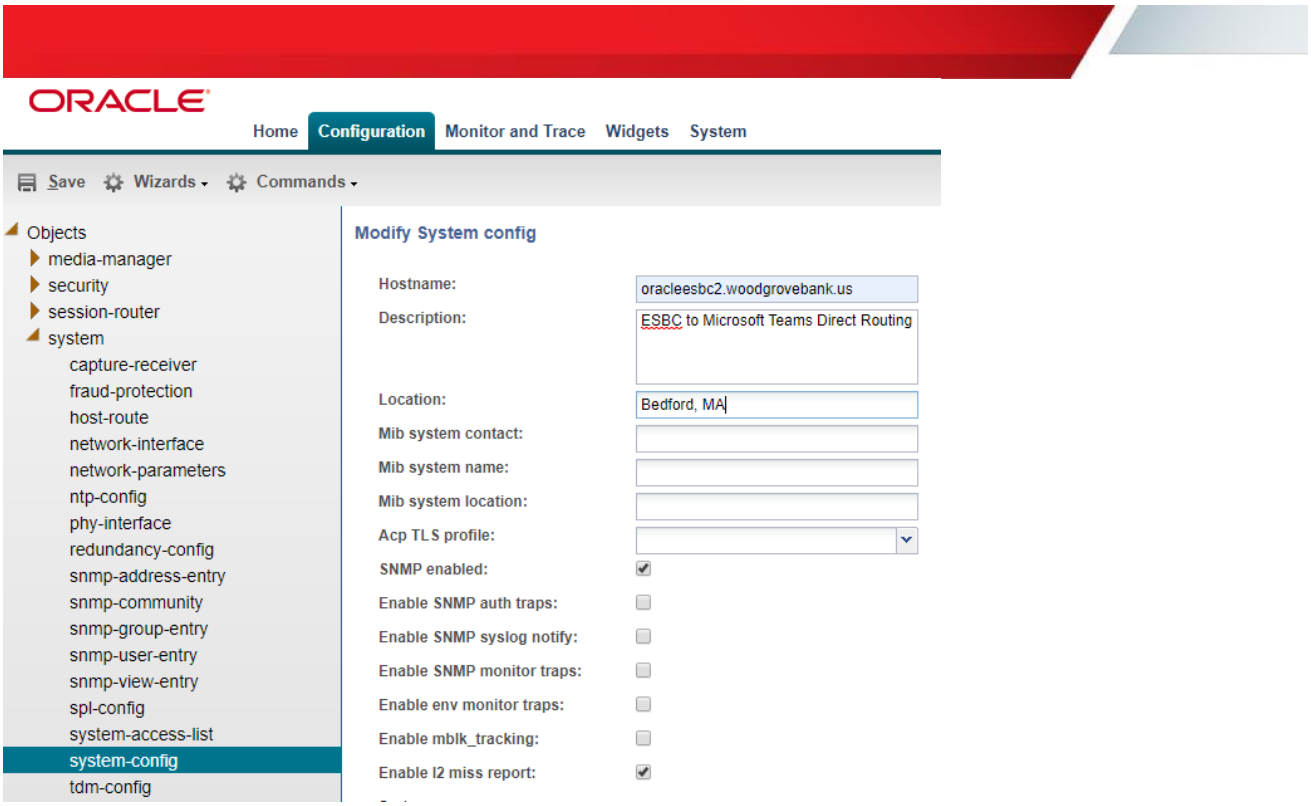
```
NN3900-101(system-config)# hostname SBC1
NN3900-101(system-config)# location Cloud
NN3900-101(system-config)# done
```

```
NN3900-101(system-config)# done
system-config
        hostname                                SBC1
        description
        location                                Cloud
        mib-system-contact
        mib-system-name
        mib-system-location
        acp-tls-profile
        snmp-enabled                            enabled
        enable-snmp-auth-traps                  disabled
        enable-snmp-syslog-notify               disabled
        enable-snmp-monitor-traps               disabled
        enable-env-monitor-traps                disabled
        enable-mblk_tracking                    disabled
        enable-l2-miss-report                   enabled
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        system-log-level                        NOTICE
        process-log-level                       NOTICE
        process-log-ip-address                  0.0.0.0
```

```
restart                                 enabled
exceptions
telnet-timeout                          0
console-timeout                         0
remote-control                          enabled
cli-audit-trail                         enabled
source-routing                          disabled
cli-more                                disabled
terminal-height                         24
debug-timeout                           0
trap-event-lifetime                     0
ids-syslog-facility                     -1
pko-rake-pkt                            0
pko-rake-burst                          0
options
default-v6-gateway                      ::
ipv6-signaling-mtu                      1500
ipv4-signaling-mtu                      1500
cleanup-time-of-day                     00:00
snmp-engine-id-suffix
snmp-agent-mode                         v1v2
forwarding-cores                        1
dos-cores                               1
transcoding-cores                       2
last-modified-by                        admin@172.18.0.105
last-modified-date                      2019-09-25 07:37:52
```

For WebGUI users, Go to system->system-config

Note: Please follow the link below for steps to activate the WebGUI.
https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB-Enabled.pdf.



For SBC, if transcoding is required, transcoding cores have to be set in system-config. Please refer to documentation here for more information and set cores according to your environment.

https://docs.oracle.com/cd/E85213_01/doc/sbc_scz739_essentials.pdf

Deploying SBC behind Azure NATing

The SPL-configuration is a must for SBC deployed in Cloud Environments.

Here,the SBC is placed behind the Azure NAT. The SBC behind SPL NAT plugin is essential for proper signaling and voice path between the SBC deployed on Azure cloud and PSTN
The plug-in changes information in SIP messages to hide the end point located inside the private network of Azure SBC. Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface on the SBC. Here there are two interfaces, one on the side facing Teams and the other on the PSTN side. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

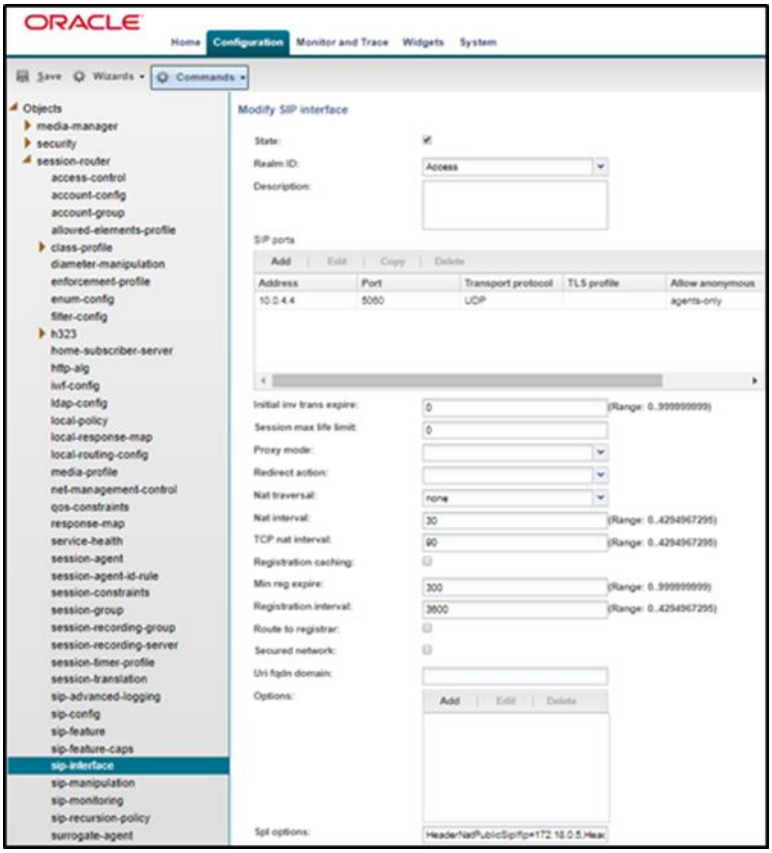
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address configured in Azure Cloud for particular network interface.

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Teams side SIP interface.

To configure SBC Behind NAT SPL Plug in using the GUI, Go to session-router->sip-interface->spl-options and input the following value, save and activate.

HeaderNatPublicSipIfIp=<Public IP of the Interface facing Teams>,HeaderNatPrivateSipIfIp=<Private IP of the interface facing Teams>

Here HeaderNatPublicSipIfIp is the public interface ip and HeaderNatPrivateSipIfIp is the private ip.



Similarly configure the PSTN side as well.

To configure SBC Behind NAT SPL Plug in using the CLI, Go to configure terminal-> session-router->sip-interface-> Select the sip-interface

```
spl-options + HeaderNatPublicSipIfIp=<Public IP of the Interface facing
Teams>,HeaderNatPrivateSipIfIp=<Private IP of the interface facing Teams>
```

Click on done. Save and activate the config.

```
SBCCUCMTLS(sip-interface)# sp-
SBCCUCMTLS(sip-interface)# spl-options +HeaderNatPublicSipIfIp=<Public IP of the Interface facing Teams>,HeaderNatPrivateSipIfIp=<Private IP of the interface
 facing Teams>
```

```
AzureSBC1# sh con sip-interface sh
sip-interface
        realm-id                                Access
        sip-port
                address                                 10.0.4.4
                port                                    5065
        sip-port
                address                                 10.0.4.4
                port                                    5065
                transport-protocol                      TCP
                allow-anonymous                         agents-only
        options                                 strip-route-headers
        spl-options                             HeaderNatPublicSipIfIp=172.18.0.5,Header
NatPrivateSipIfIp=10.0.4.4
```


Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services