SSL VPN Distribution and MEP

Christian Abraham Castillo Porras
Cloud Security Architect | LATAM
March 2020

Needs

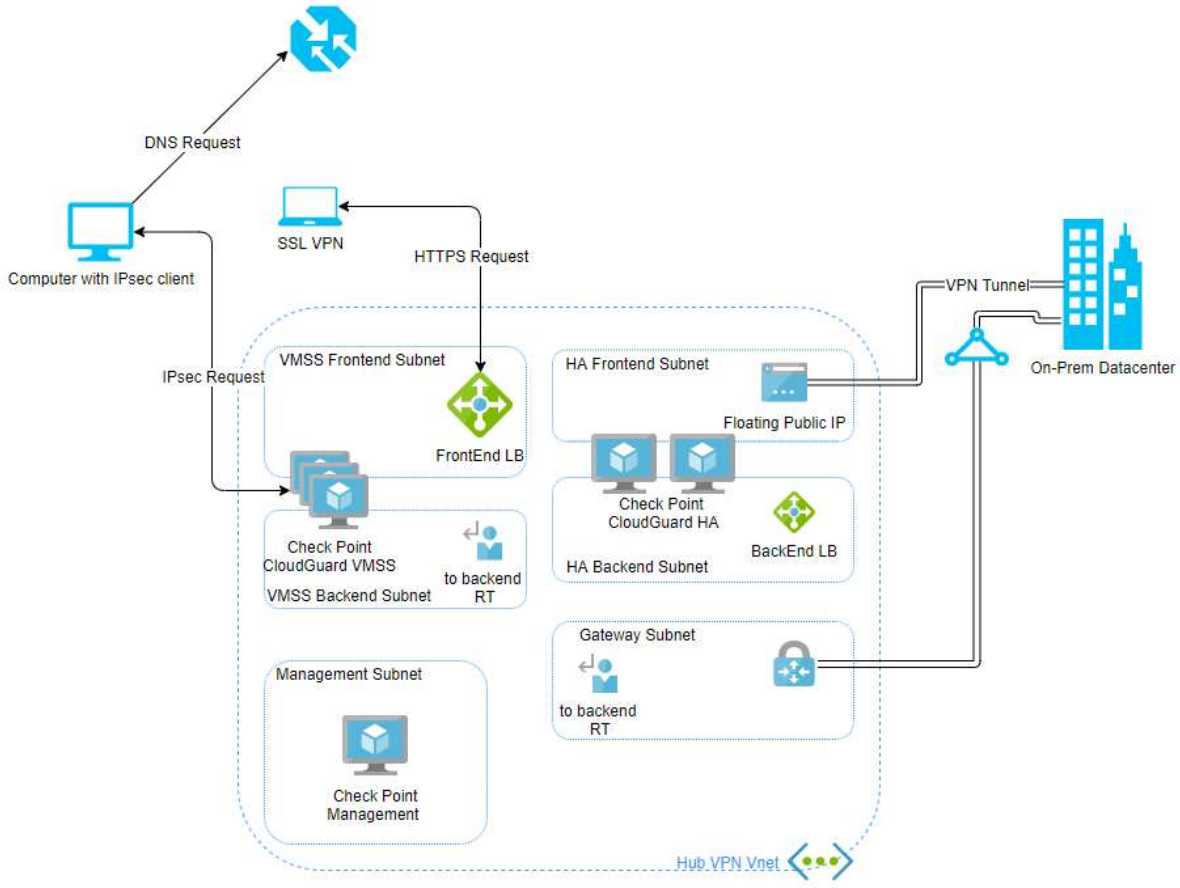
A scalable (not automated) way to add GW to do SSL VPN and distribute it between users of the corporation, also add a way to enable new points of access (GW with VPN P2S support) to the end user with less interactions.

Also the need to connect several On-Prem datacenters to give access to the users of SSL VPN or IPsec Client.

Technologies we use

Azure Cloud to offer the connectivity to on-prem and fast growing deployment to offer entry points to remote users, but any single Gateway deployment works the same.

Proposed design



Implementation

Used the ARM preconfigured templates from Check Point, following the Admin Guide (https://sc1.checkpoint.com/documents/IaaS/WebAdminGuides/EN/CP_VMSS_for_Azure/Content/Topics/Overview.htm) this for the VMSS part of the diagram, this GW will receive the Remote Access requests from the users, we deployed only with external LB because we will not use it to outbound traffic.

Also used HA pair following the Admin Guide (https://sc1.checkpoint.com/documents/IaaS/WebAdminGuides/EN/CP_CloudGuard_IaaS_High_Availability_for_Azure/Content/Topics/Check_Point_CloudGuard_IaaS_High_Availability_for_Azure.htm) to establish the center of a star community to communicate with all the on-prem datacenters that the user can have.

Also can use ExpressRoute with the proper set of Route Tables.

Explanation of the flows

DNS request can be handled from the Traffic Manager, since this feature don't balance the traffic to the app just the resolution of the IP address to a given URL, allow us to directly connect the IPsec clients and SNX to one of the GW, since this lacks of persistence is better to use with non-interactive browser features.

HTTPS request for Mobile Access Portal (reverse proxy feature) are handled by the frontend load balancer deployed from the VMSS ARM template, since the load balancer in Azure have the feature of persistence the Mobile Access portal requests from the browser will be maintained by hashing algorithm.

Communication to On-Prem datacenter is done by the HA pair, this by manipulating the VMSS backend Route Table and pointing the On-Prem CIDR Blocks to the Backend LB deployed by the HA ARM template.

MEP

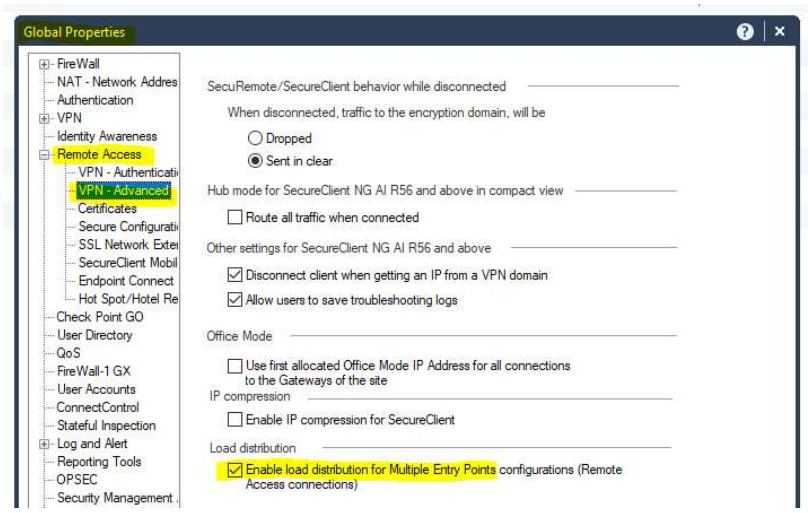
The MEP feature from Check Point is explained in the Admin Guide (https://sc1.checkpoint.com/documents/R80.10_andhigher/WebAdminGuides/EN/CP_RemoteAccessVPN_AdminGuide/html_frameset.htm), this allow to any Gateway member of the same RemoteAccess Community to be part of the list on an IPSec Client from Check Point (Endpoint VPN or Check Point Mobile are supported sk67820) .

The main feature is globally enabled under Remote Access options and is not needed to enable on each GW; this is explained on the next title.

Multi Entry Point feature

When use the IPsec Client there is a method to detect new GW on the list and uses it to distribute traffic, this is done by the Check Point's algorithm and not by the Load Balancer, in this case to provide direct access to end users to GW can use Traffic Manager, this Azure's feature will resolve a name directly to a public IP and allow to connect.

To enable MEP for Load Sharing need to mark this checkbox on the SmartConsole, under General Properties.

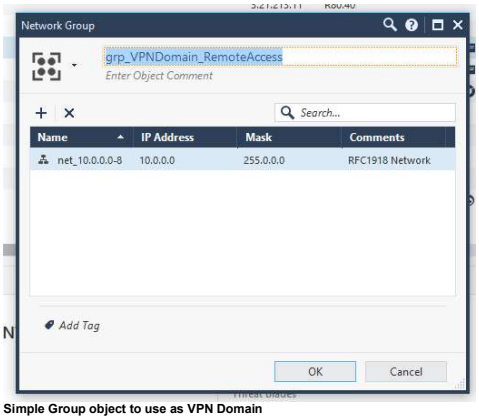


Manual configuration

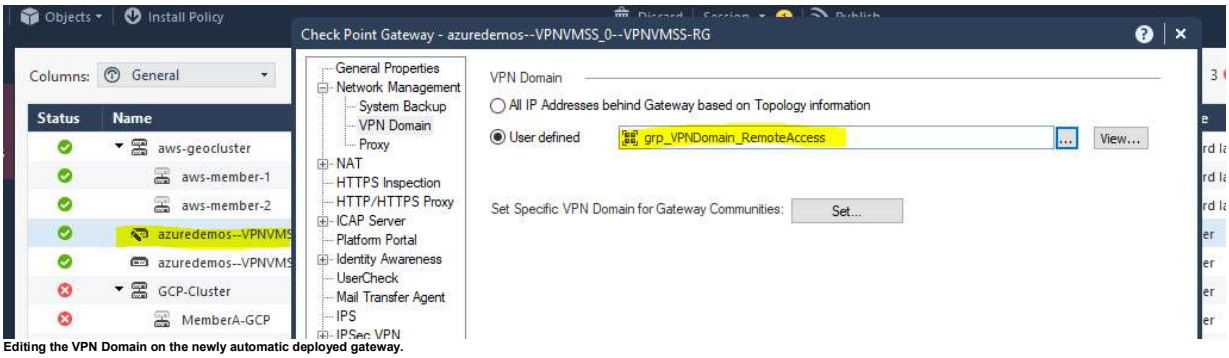
Every newly added GW need to be tuned by hand, here are the configuration to enable it as VPN remote access Gateway.

General configuration, needed for both, Remote Access by SNX and Client;

- Set the VPN domain, this GW will advertise all the networks from on-premises and clouds, so a super net is a good option, my example will use 10.0.0.0/8, also we encourage using a Group because if the networks grows we can just attach to a group and can automate it.



Simple Group object to use as VPN Domain

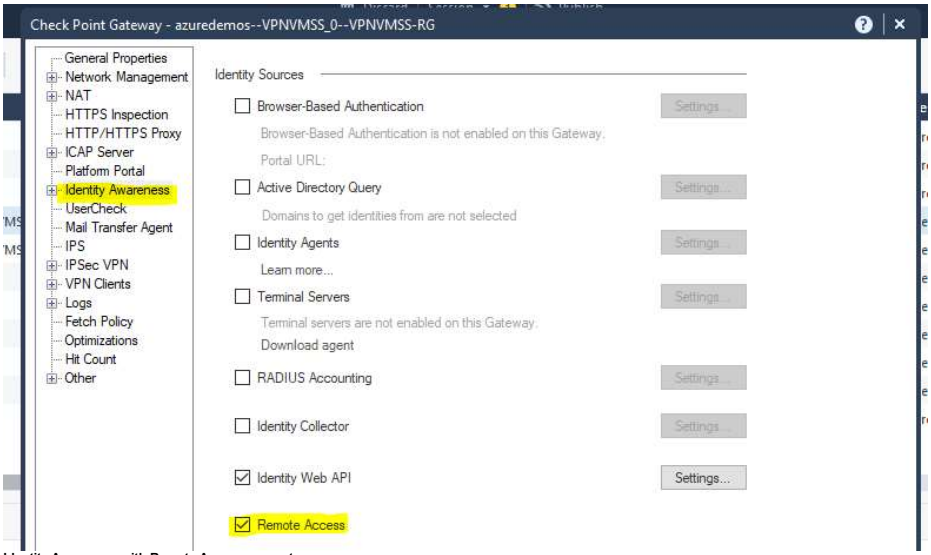


Editing the VPN Domain on the newly automatic deployed gateway.

- Change the portal port, since we will use HTTPS default port to connect the VPN.

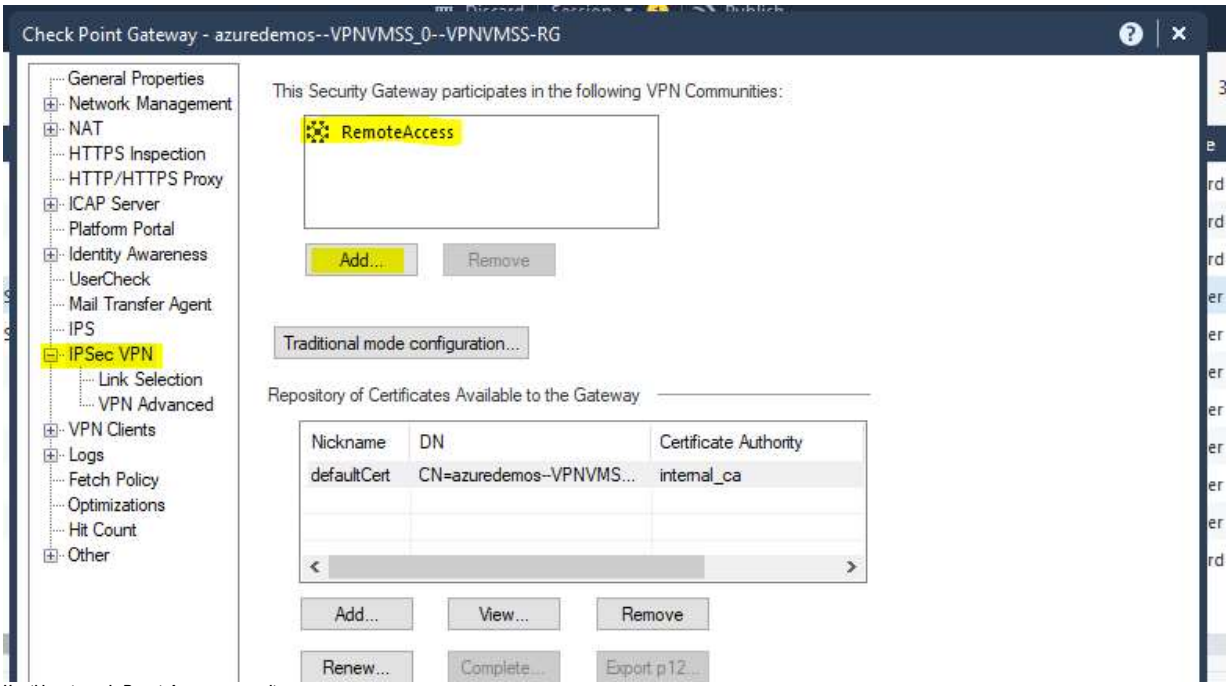
Modifying Platform Portal port to 4434 (use any port adding it at the end)

- Add the support to Remote Access in Identity Awareness feature, this allow us to connect an AD to obtain the users



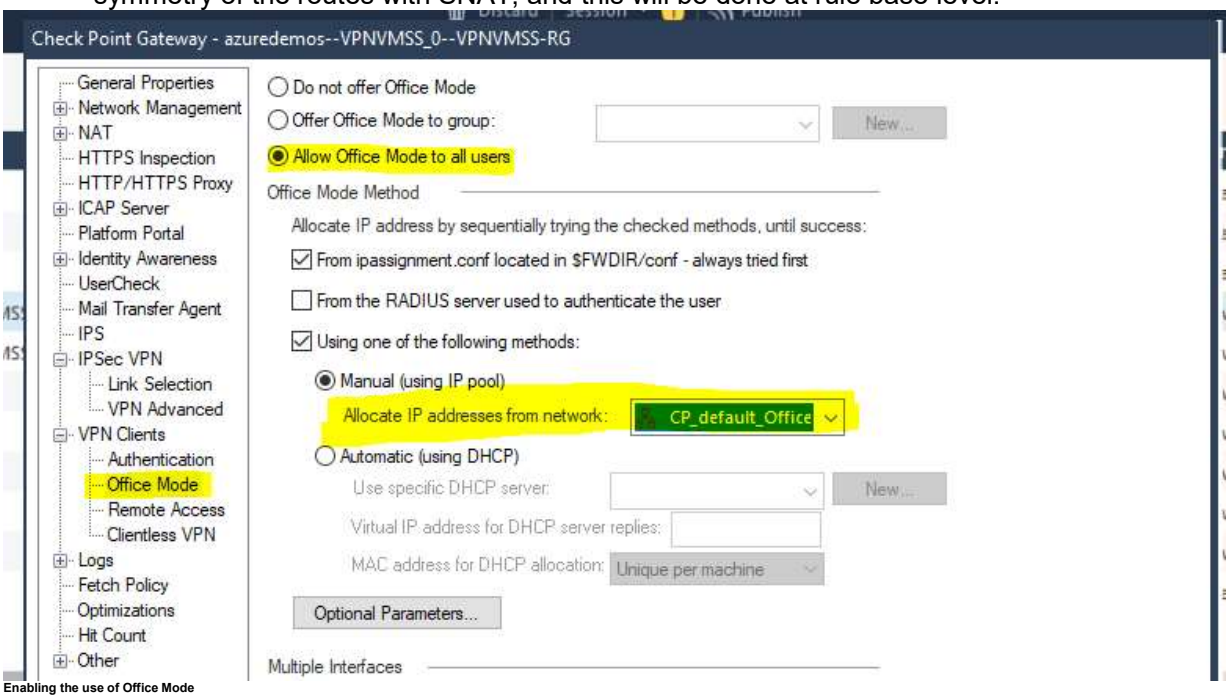
Identity Awareness with Remote Access support

- Add the gateway to RemoteAccess VPN community



Use this gateway in RemoteAccess community

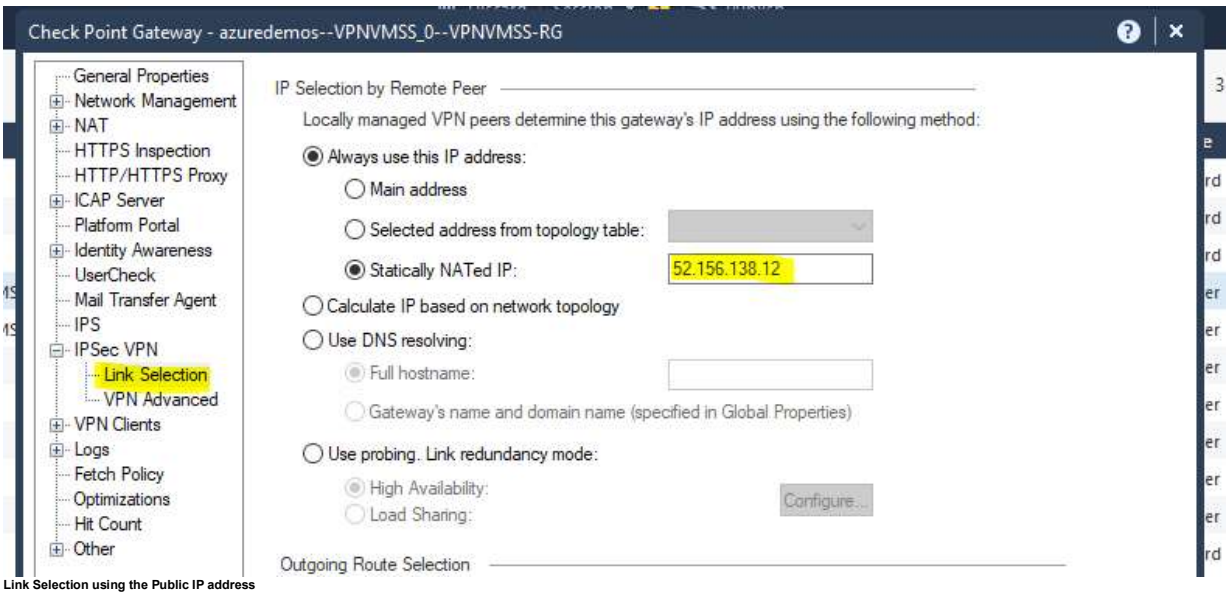
- We will use the same Office Mode IP Pool for all the Gateways, going to manage the symmetry of the routes with SNAT, and this will be done at rule base level.



Enabling the use of Office Mode

Specific configuration for IPSec clients support with MEP

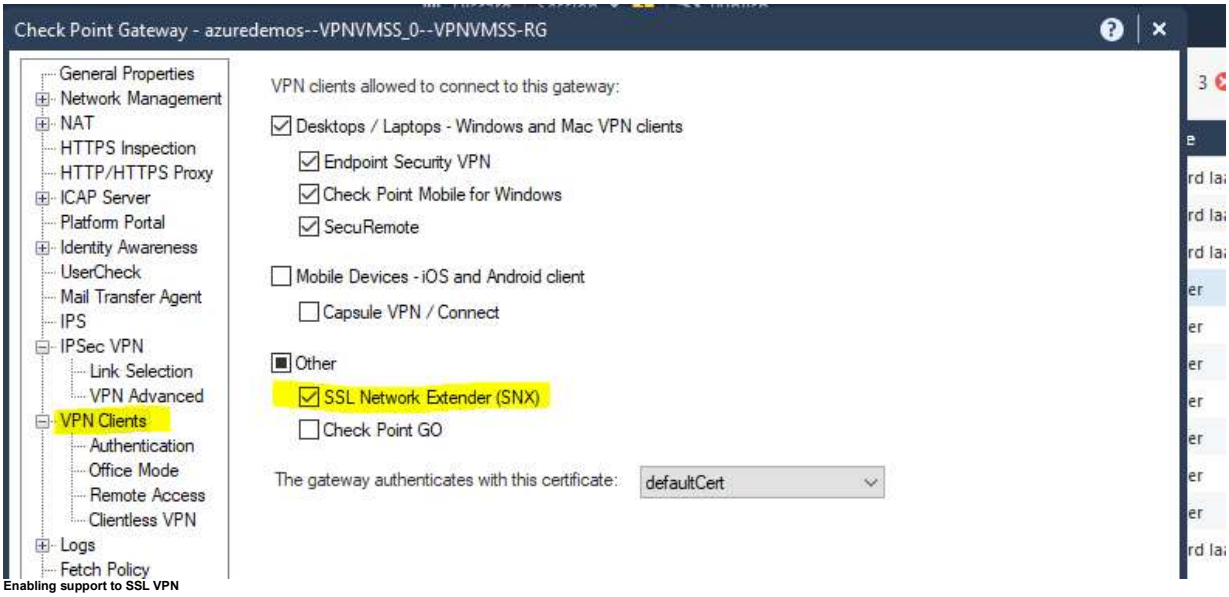
- In Check Point VPN the GW will advertise the IP address to use to the connected VPN Clients by the Link Selection option inside VPN configuration; you need to use Statically NATed IP since Azure offers you private IP address to the machine.



Link Selection using the Public IP address

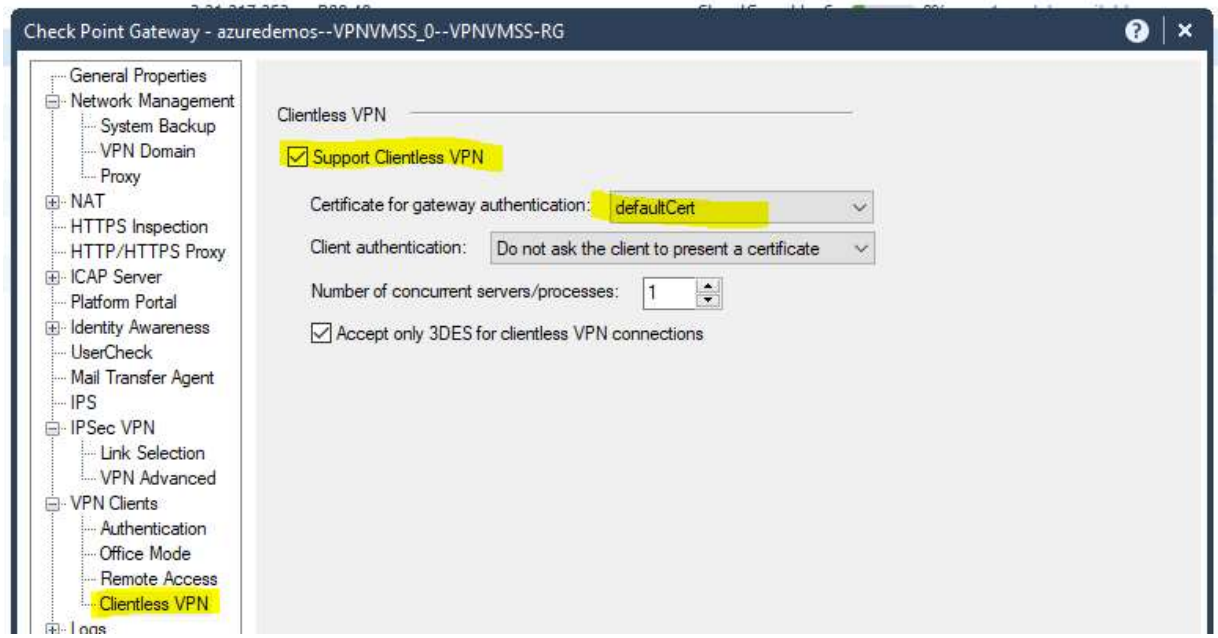
Configuration needed for SSL VPN support (SNX)

- In VPN Clients enable SSL Network Extender, the IPsec Clients are supported by default.



Enabling support to SSL VPN

- Enable the support for Clientless VPN



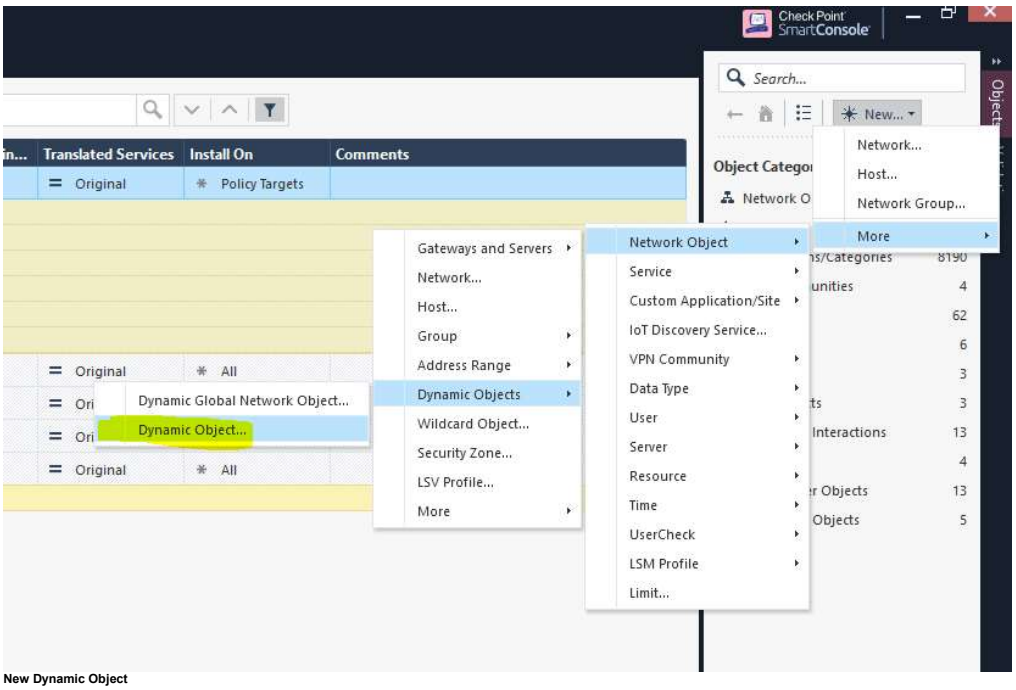
This set of configurations are done on each deployed GW, this enables the GW to be fully operable as VPN Remote Access Gateway for SSL VPN and IPsec Clients (Endpoint VPN)

Rulebase criteria

Since the gateways will be deployed under demand of modifying the VMSS parameters, is a good option to use a rulebase that works for every GW and not use static IP address because we will never know what address will be offered by Azure to newly deployed machines, in the Check Point VMSS admin guide explain the use of “Dynamic Objects” this is the one that we will use on the rulebase.

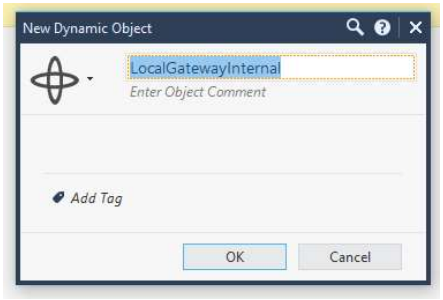
The only rule we need (other than the proper ones for remote access, that’s under customer criteria) is the NAT rule, all the incoming communication from the remote users will use a pool declared on Office Mode configuration, since will be the same for all GW will use the NAT rules to hide the packets in the backend (ETH1) interface of the GW.

Therefore, we will create that object;



New Dynamic Object

In addition, will use exactly this name “LocalGatewayInternal”

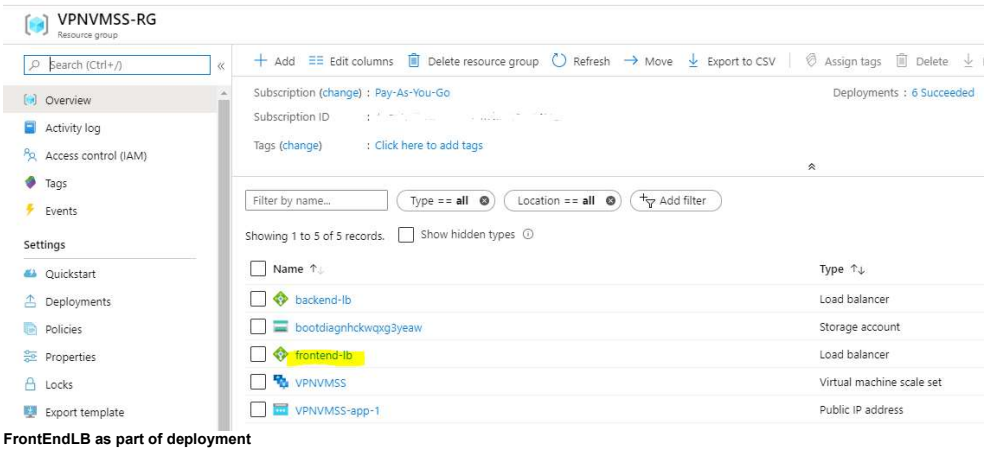


Load Balancer on Azure

As we said the VMSS template launch a Load Balancer called FrontendLB, this can be used to distribute access evenly for SSLVPN and Mobile Access.

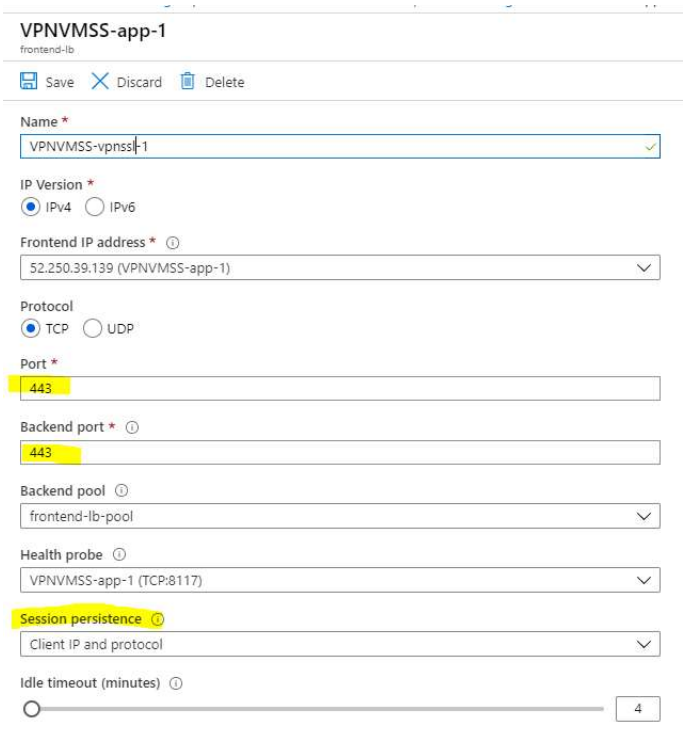
The load balancing rule MUST have persistence, on the past steps we deploy the GW listening for SSLVPN on port 443, so I left some images on how I configured the LB.

In the resource group of the deployment of VMSS you will find it, if use multiple single GW you can create it.



FrontEndLB as part of deployment

We will use it and create a Load Balancing Rule for port 443.



Load Balancing rule for port 443 and persistence

