

Firewall

Contents

1.	Purpose	1
2.	Procedure	2
1)	pfSense	2
2)	Kerio	94
3)	Fortinet	169
3.	Conclusion	207
4.	Evaluation	207

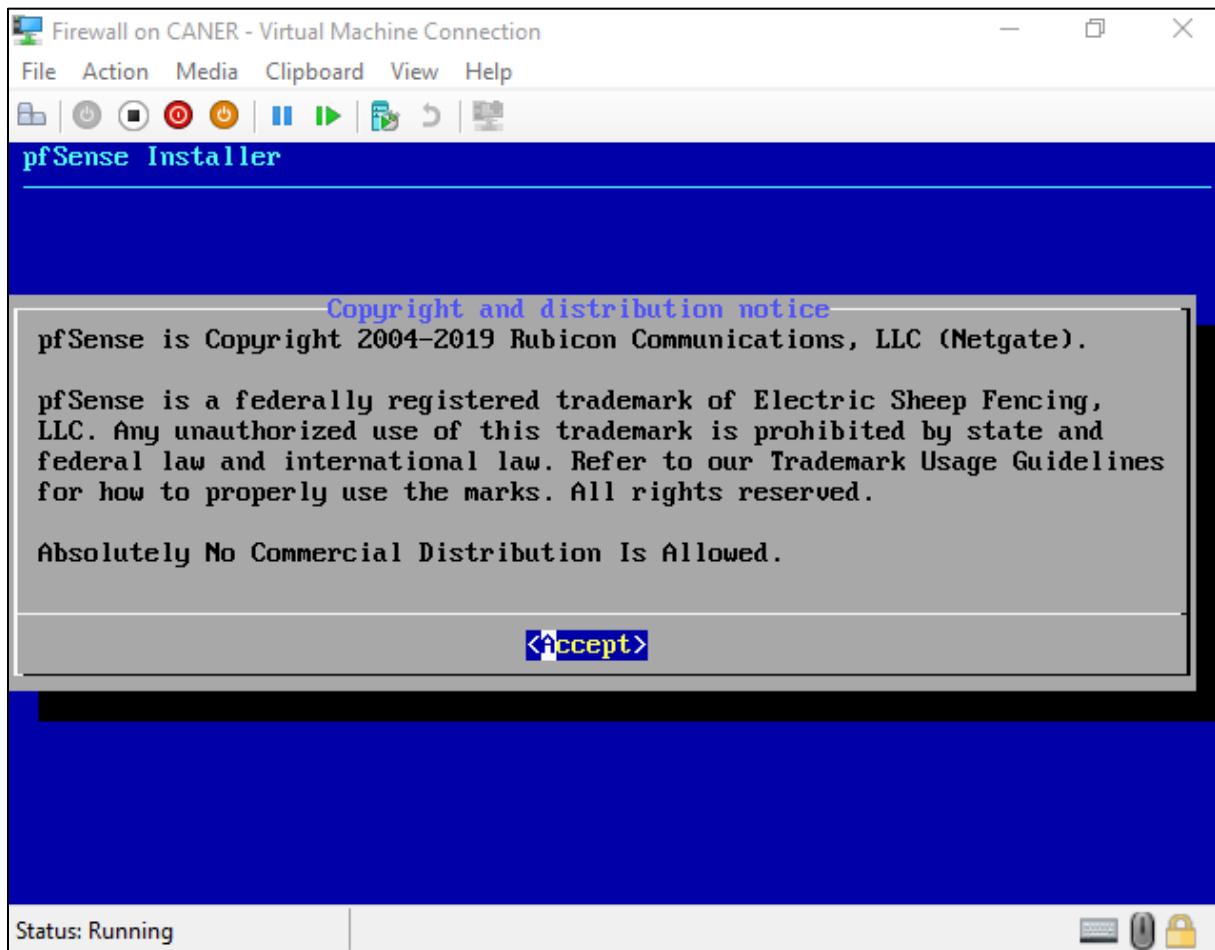
1. Purpose

The purpose of this project is to set up various firewalls and get familiar with them. We establish Captive Portals along with Radius' for an extra layer of security to get to the internet for our enterprise users and also use VPNs and IPSec tunnels for safe connections. We write rules to block access to certain websites and protocols. We utilize port forwarding for secure remote access to our servers through the firewalls. In this project, we use pfSense, Kerio and Fortinet firewalls.

2. Procedure

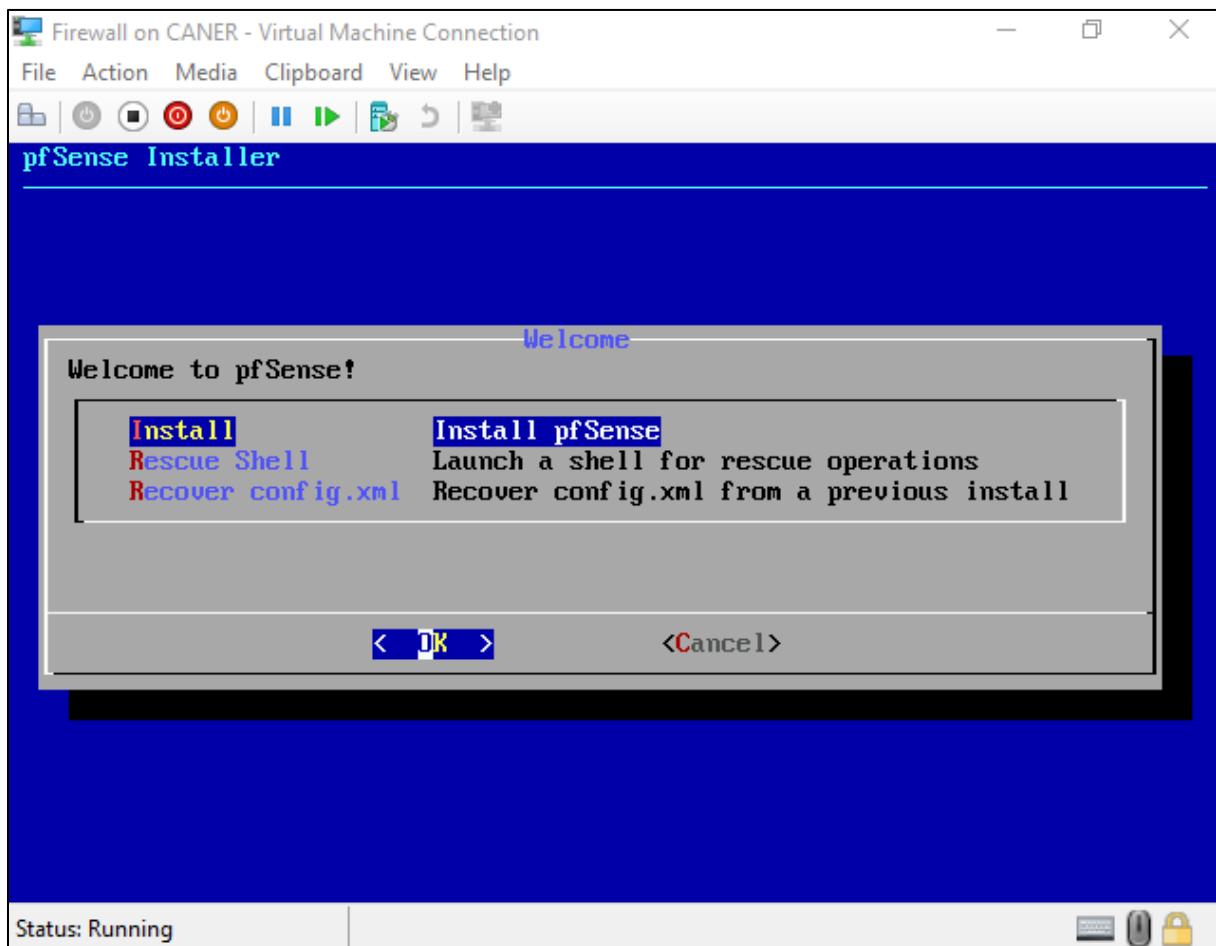
1) pfSense

The first firewall we'll demonstrate is pfSense. Once we set up a virtual machine with the PfSense image on the media drive and start it, the pfSense Installer runs. Please note that you must have at least 2 network interface cards for a firewall to properly work; one for your internal topology and one for accessing the internet via an external virtual switch.

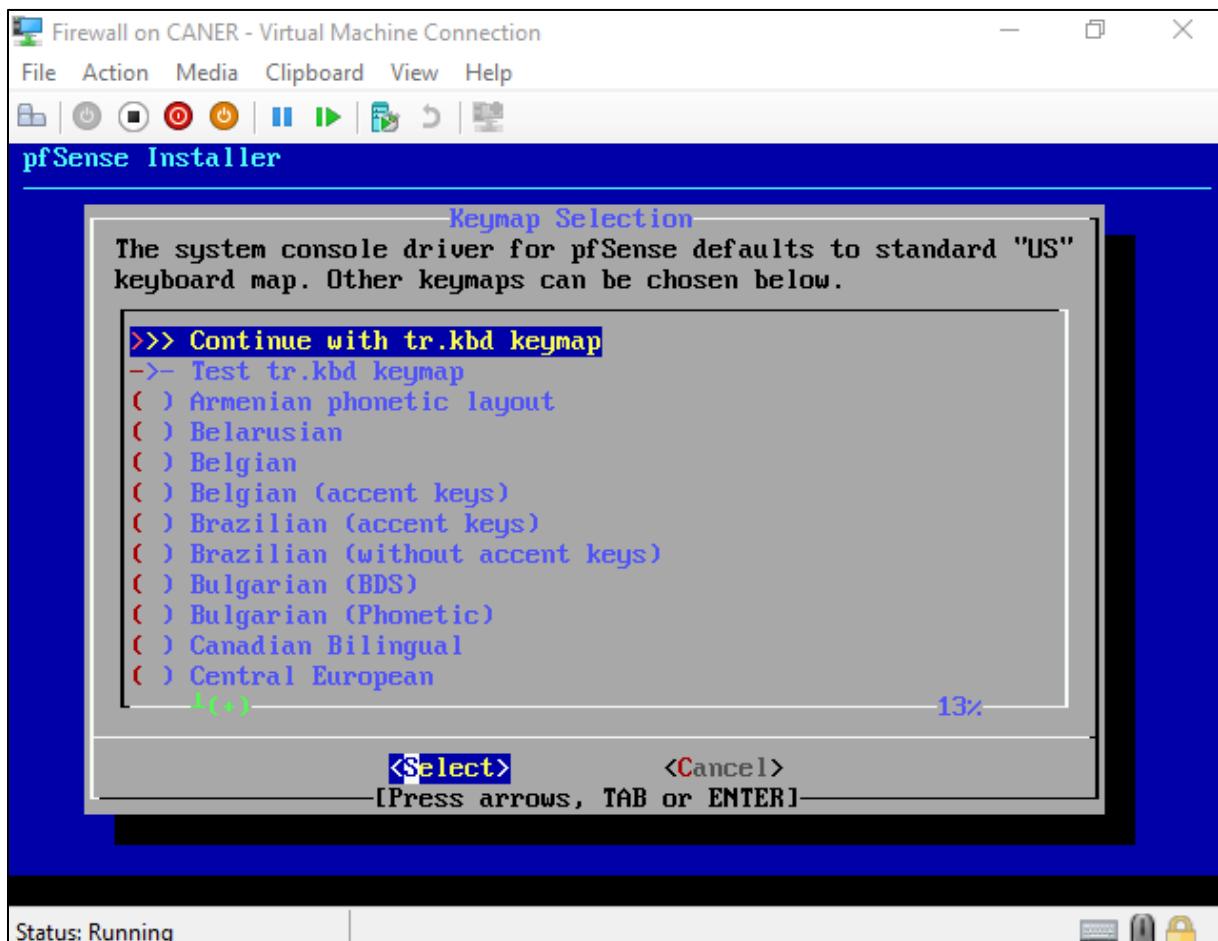


20.1.2020

We select Install pfSense.

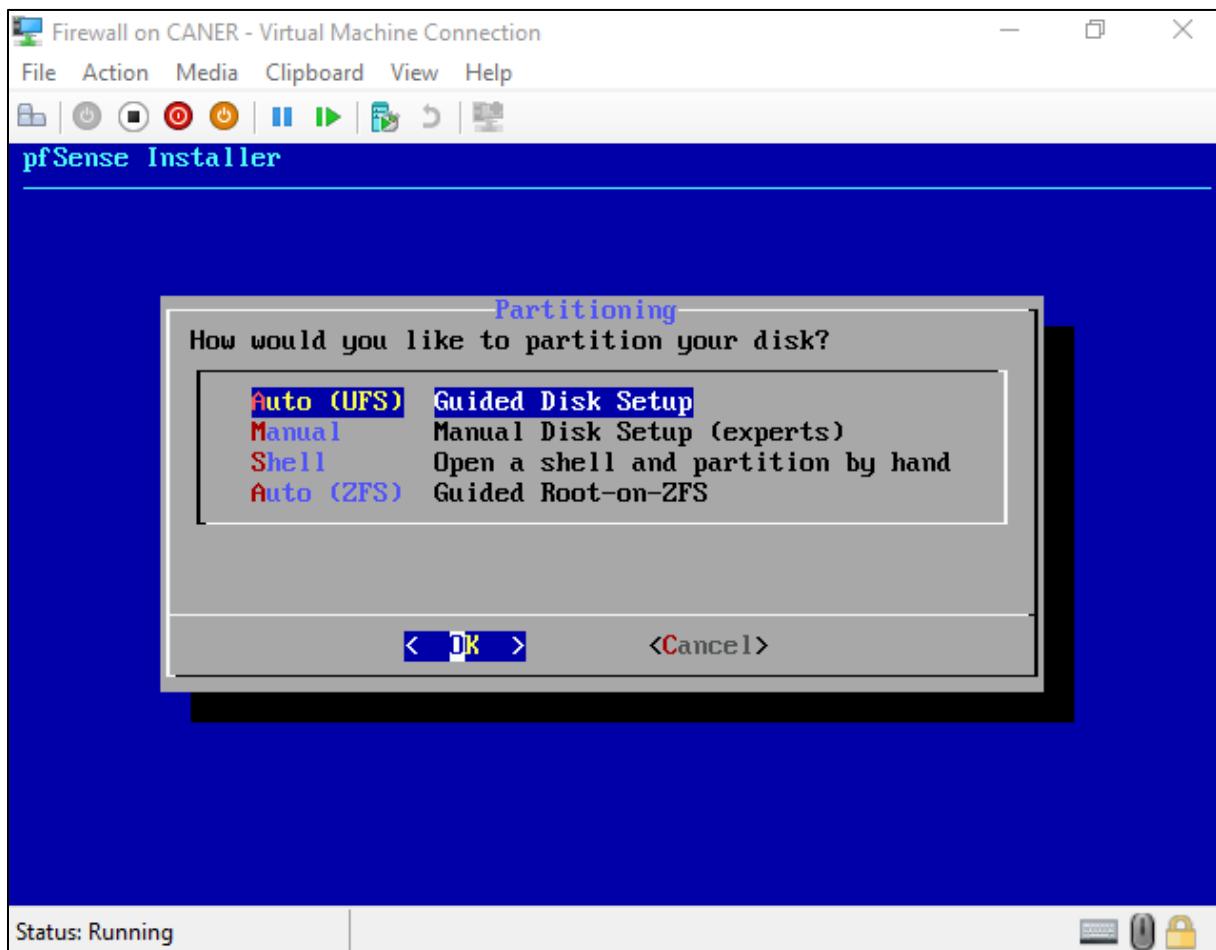


We determine which keyboard we will be using.



20.1.2020

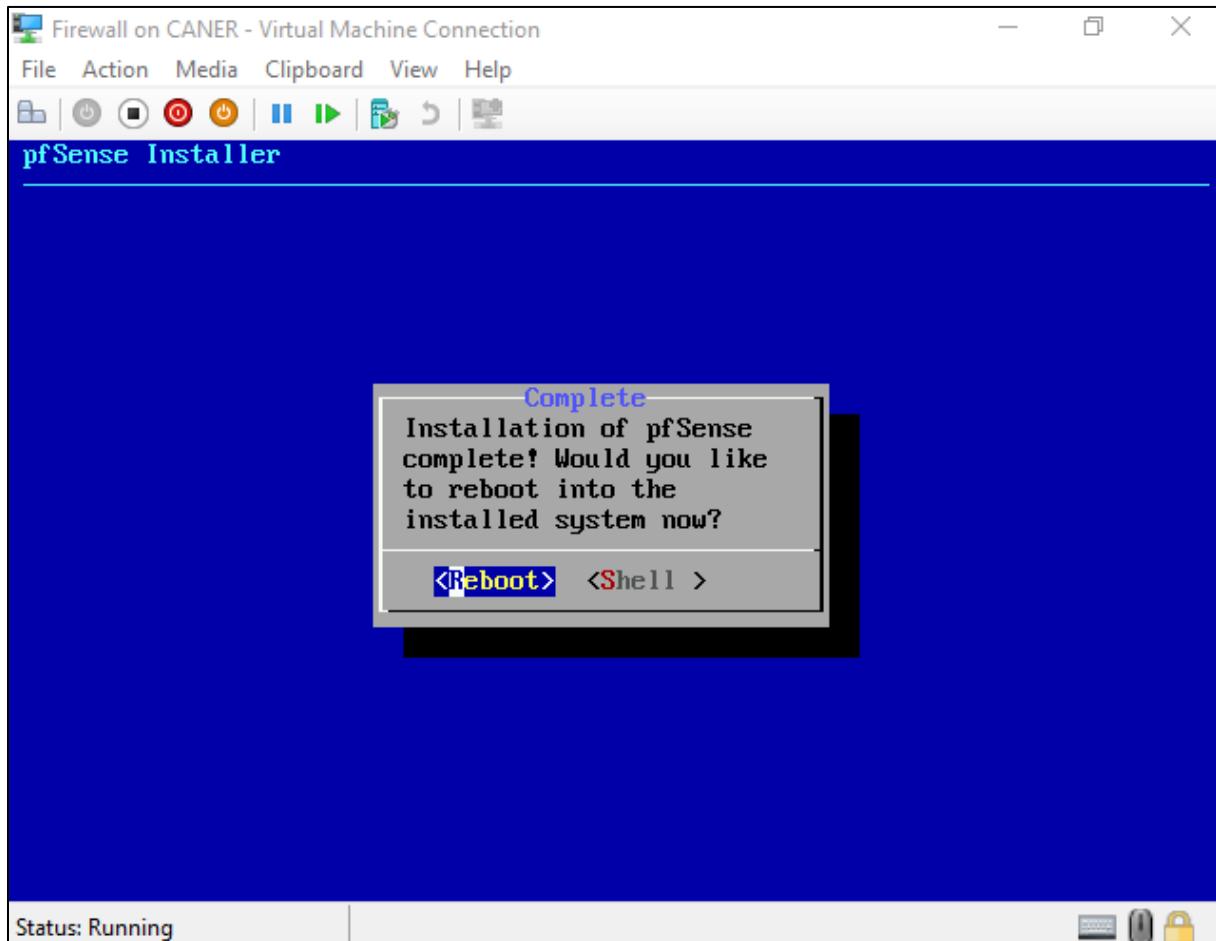
We use Guided Disk Setup.



After installation finishes, we refuse to open a shell to make any modifications.



Then, we reboot the system. However, make sure to remove the image disk before you reboot.



It starts to initialize.

```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
AMD Features=0x28100800<SYSCALL,MX,RDTSCP,LM>
AMD Features2=0x1<LAHF>
Structured Extended Features=0x281<FSGSBASE,SMEP,ERMS>
XSAVE Features=0x1<XSAVEOPT>
Hypervisor: Origin = "Microsoft Hv"
Done.
..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em0 em1
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:
hn0      00:15:5d:02:8f:23 (down) Hyper-V Network Interface
hn1      00:15:5d:02:8f:24 (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n
Status: Running
```

It automatically recognizes the 2 NICs but since they are not assigned IPs yet, they only have MAC addresses. Note that it even recognized that we're using Hyper-V to create it.

It asks whether we want to set up VLANs and we refuse.

20.1.2020

We assign the interfaces for WAN and LAN.

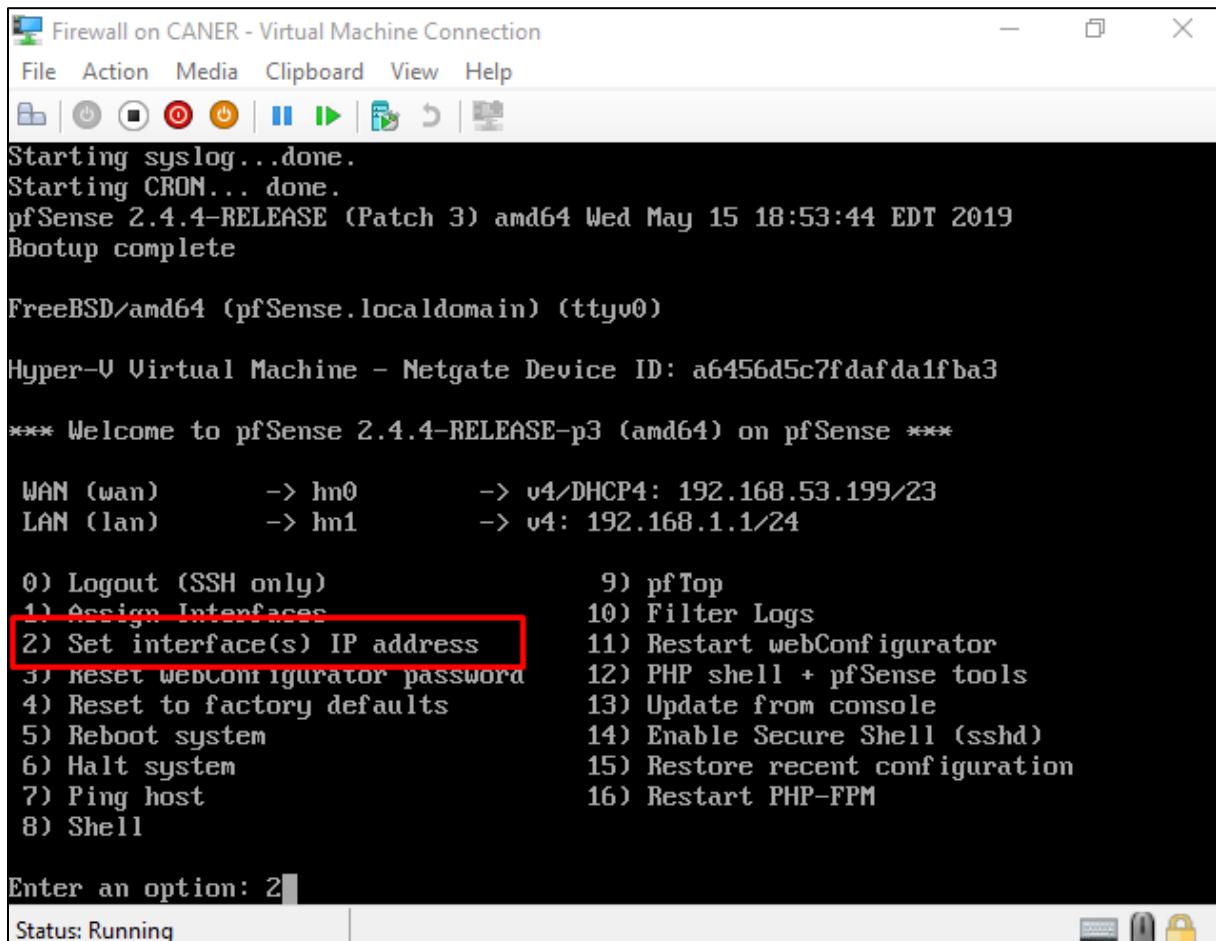
The screenshot shows a terminal window with the following text:

```
No link-up detected.  
Enter the WAN interface name or 'a' for auto-detection  
(hm0 hm1 or a): hm0  
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(hm1 a or nothing if finished): hm1: link state changed to UP  
hm1  
The interfaces will be assigned as follows:  
WAN -> hm0  
LAN -> hm1  
Do you want to proceed [y\?n]? |
```

The status bar at the bottom left shows "Status: Running". The top bar has icons for file operations like copy, paste, and search.

We proceed.

In this example our WAN IP is the IP that BAU's internal network distributes via DHCP. We use them to get to the internet. The LAN IP is ours to create. To do so, in the menu that pfSense presents we select 2 to set an interface's IP address.



```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

Hyper-V Virtual Machine - Netgate Device ID: a6456d5c7fdafda1fba3

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> hn0          -> v4/DHCP4: 192.168.53.199/23
LAN (lan)      -> hn1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

Status: Running

And select that we want to change the IP address of the LAN interface.

```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Hyper-V Virtual Machine - Netgate Device ID: a6456d5c7fdafda1fba3

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4/DHCP4: 192.168.53.199/23
LAN (lan)      -> hn1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 2
Status: Running
```

We give it an IP address and subnet mask. Since it's a LAN we don't have to give it an upstream gateway address. We don't have to assign an IPv6 address. And lastly, we do enable DHCP in our internal NIC so that the enterprise hosts can get IP addresses from the firewall itself.

```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
File | Power | Stop | Reset | Start | Stop | Eject | Help

1 - WAN (hm0 - dhcp, dhcp6)
2 - LAN (hm1 - static)

Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 173.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

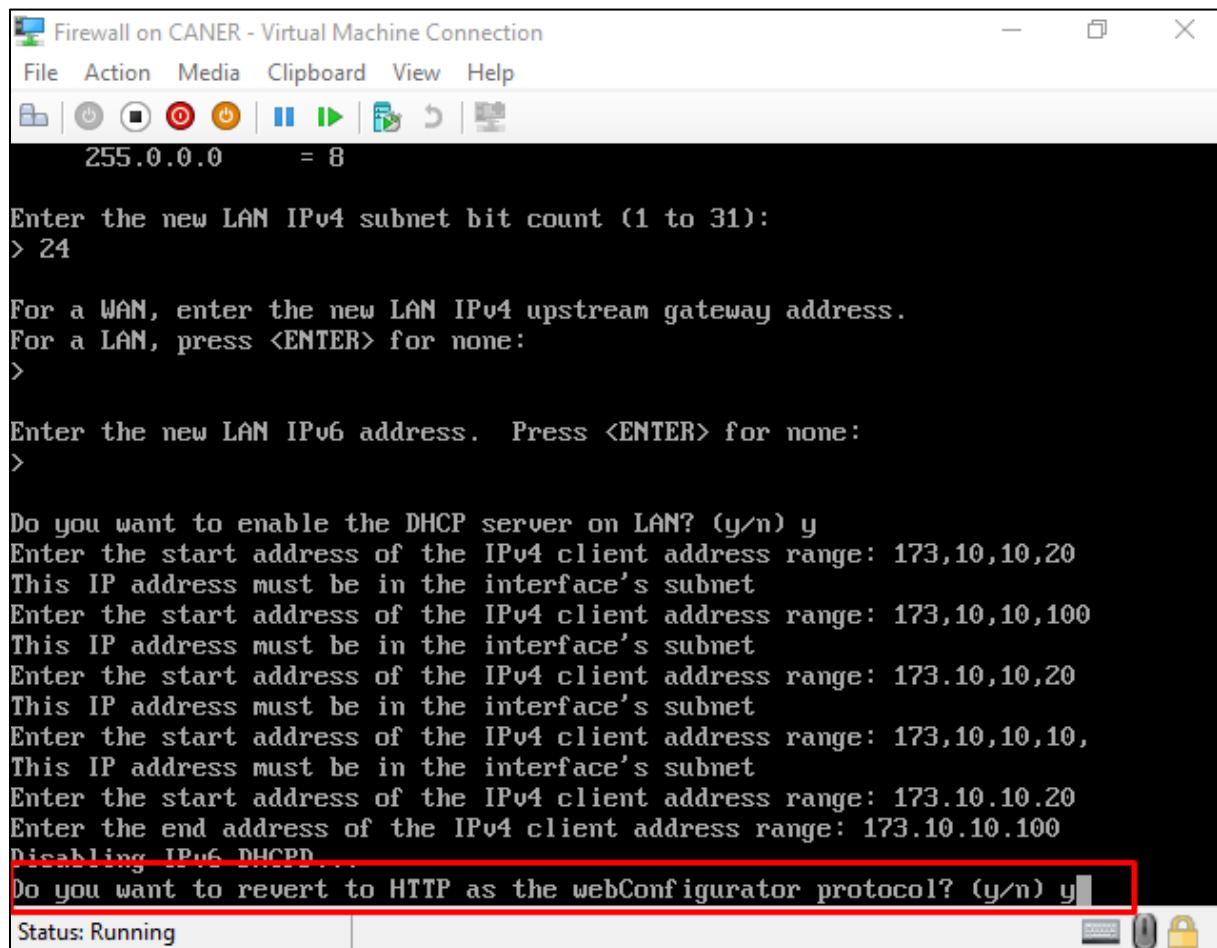
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Status: Running
```

We determine the DHCP pool and say yes to the next question to use HTTP as the webConfigurator protocol to access pfSense.



```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
File | Open | Save | Print | Stop | Refresh | Stop | Help
255.0.0.0      = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

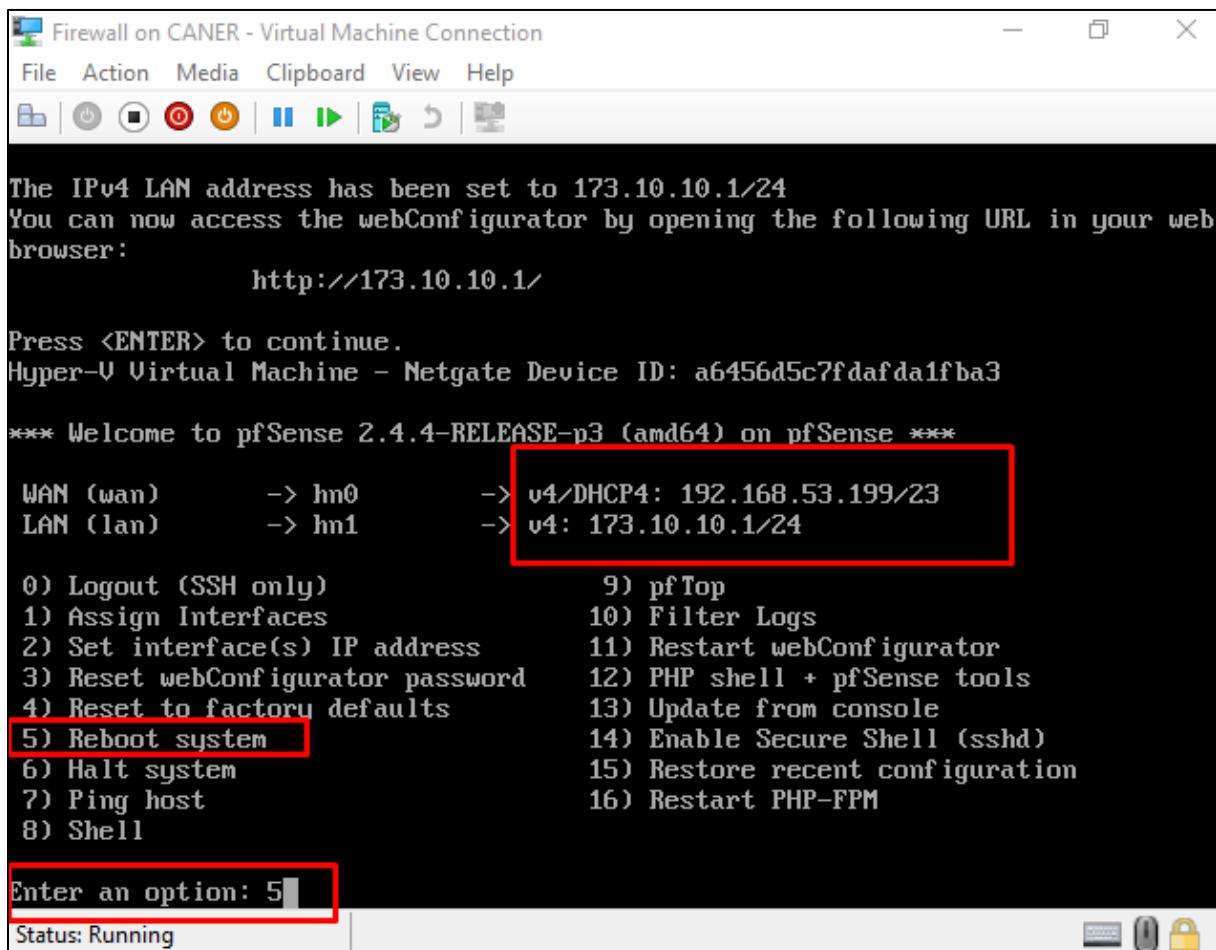
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 173.10.10.20
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 173.10.10.100
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 173.10.10.20
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 173.10.10.10,
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 173.10.10.20
Enter the end address of the IPv4 client address range: 173.10.10.100
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

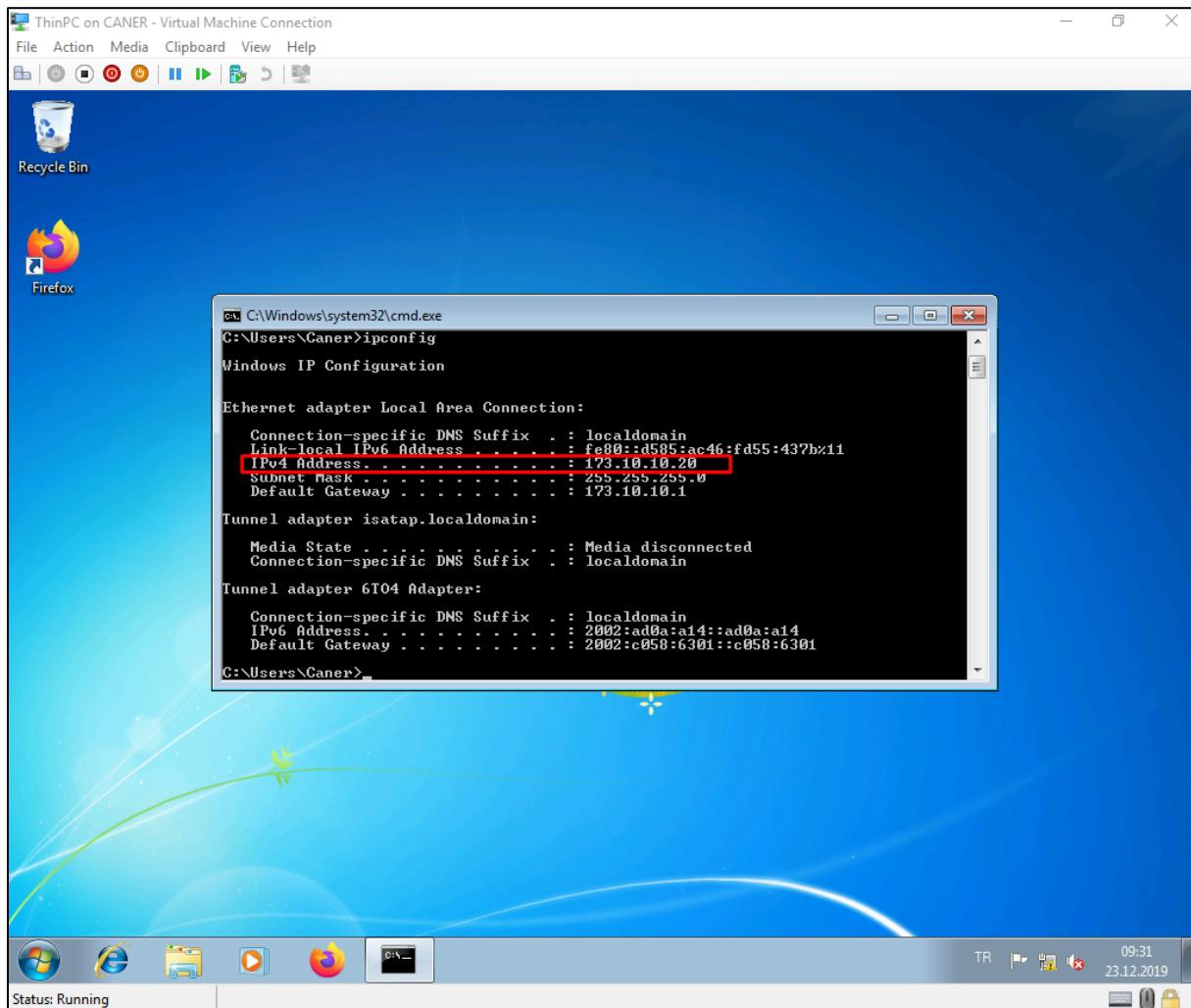
Status: Running
```

After the initial configuration is over, we must reboot it.

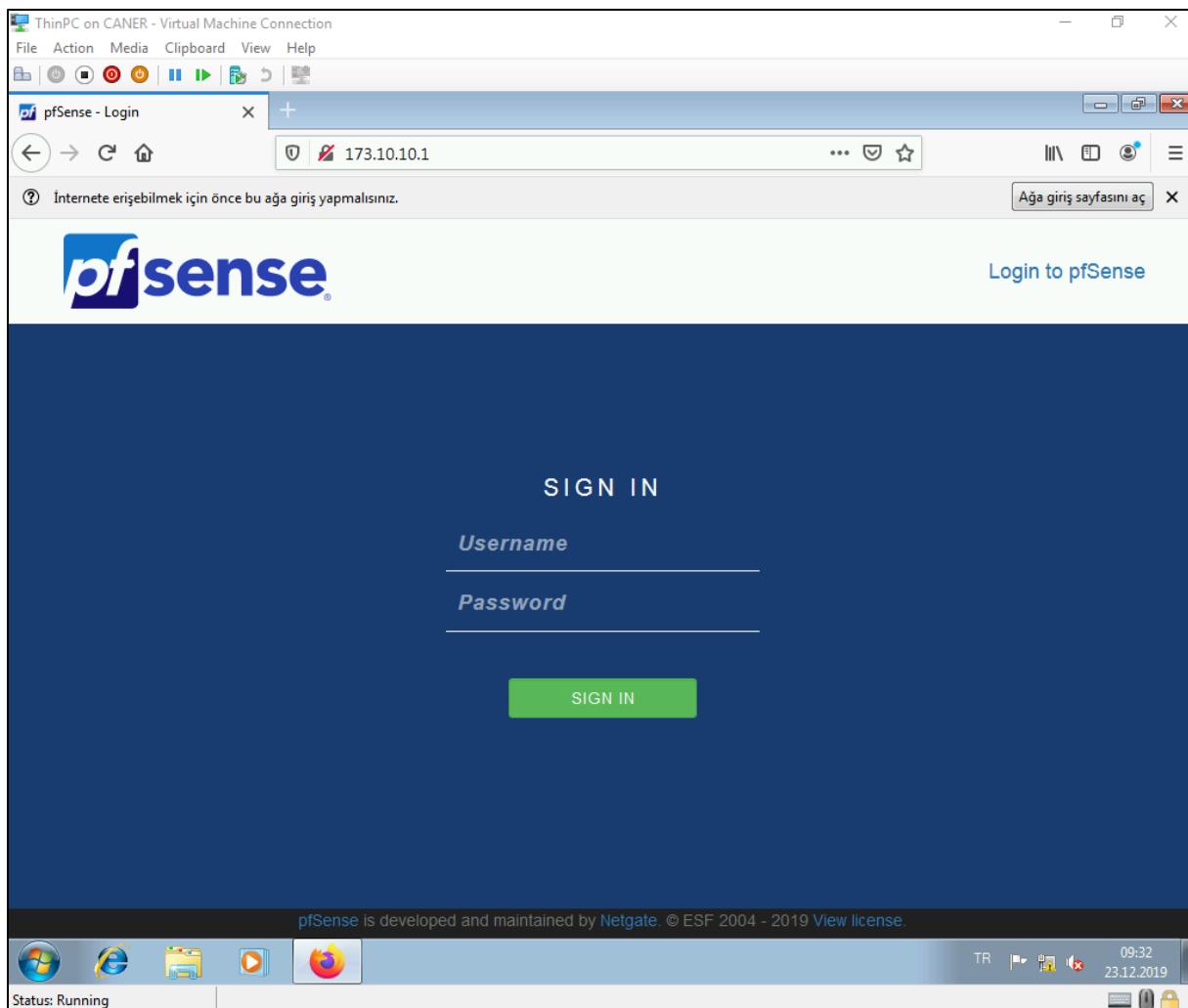


Note the LAN IP address, we will be using it to connect to it via a web browser and further configure security settings.

Next, we create another virtual machine, we used ThinPC image, but any client or even server system would work. This machine has only one NIC and it is set to internal setting. It receives its IP address from the DHCP of pfSense.

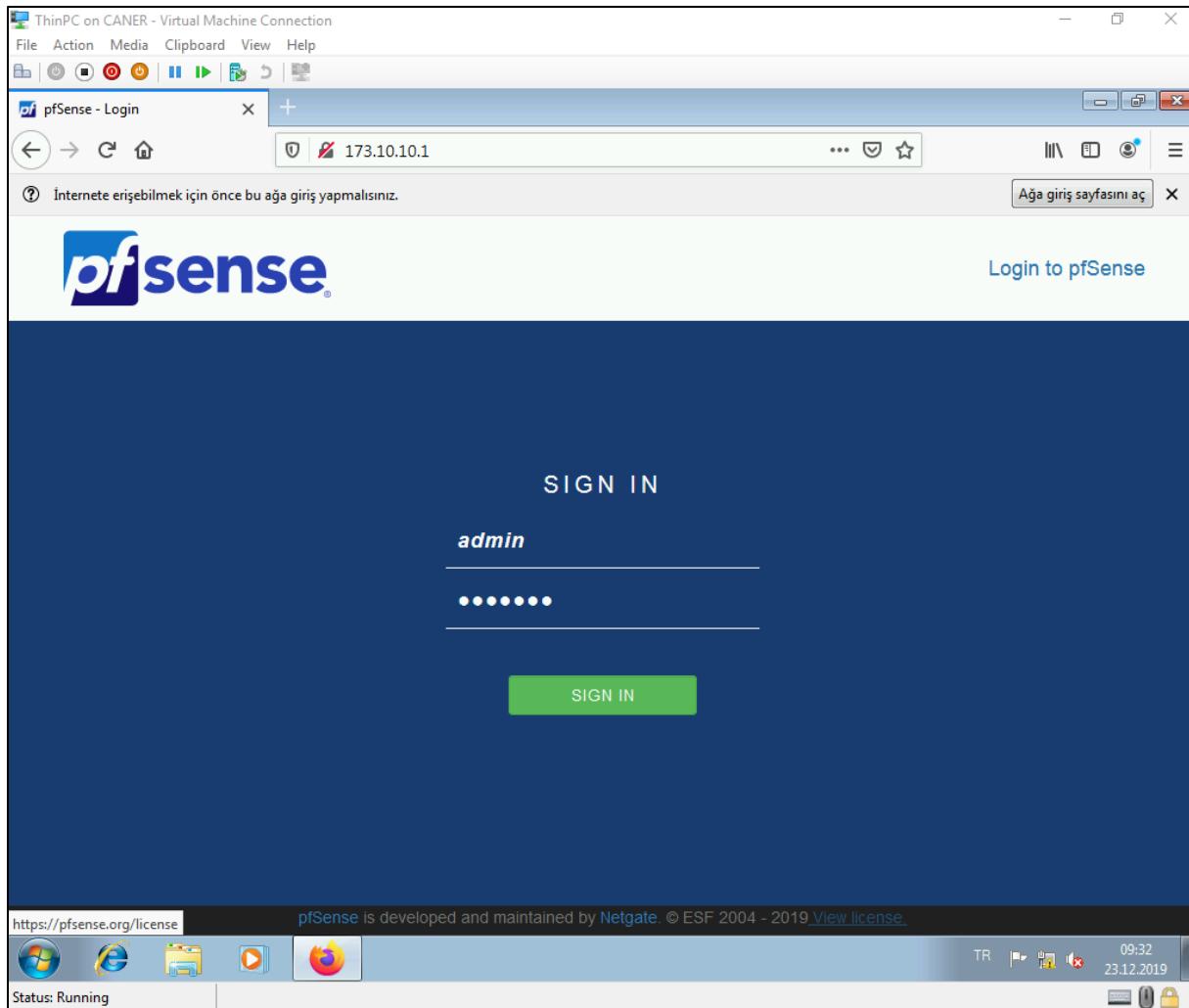


When we enter the LAN IP address to the web browser. We connect to the firewall.



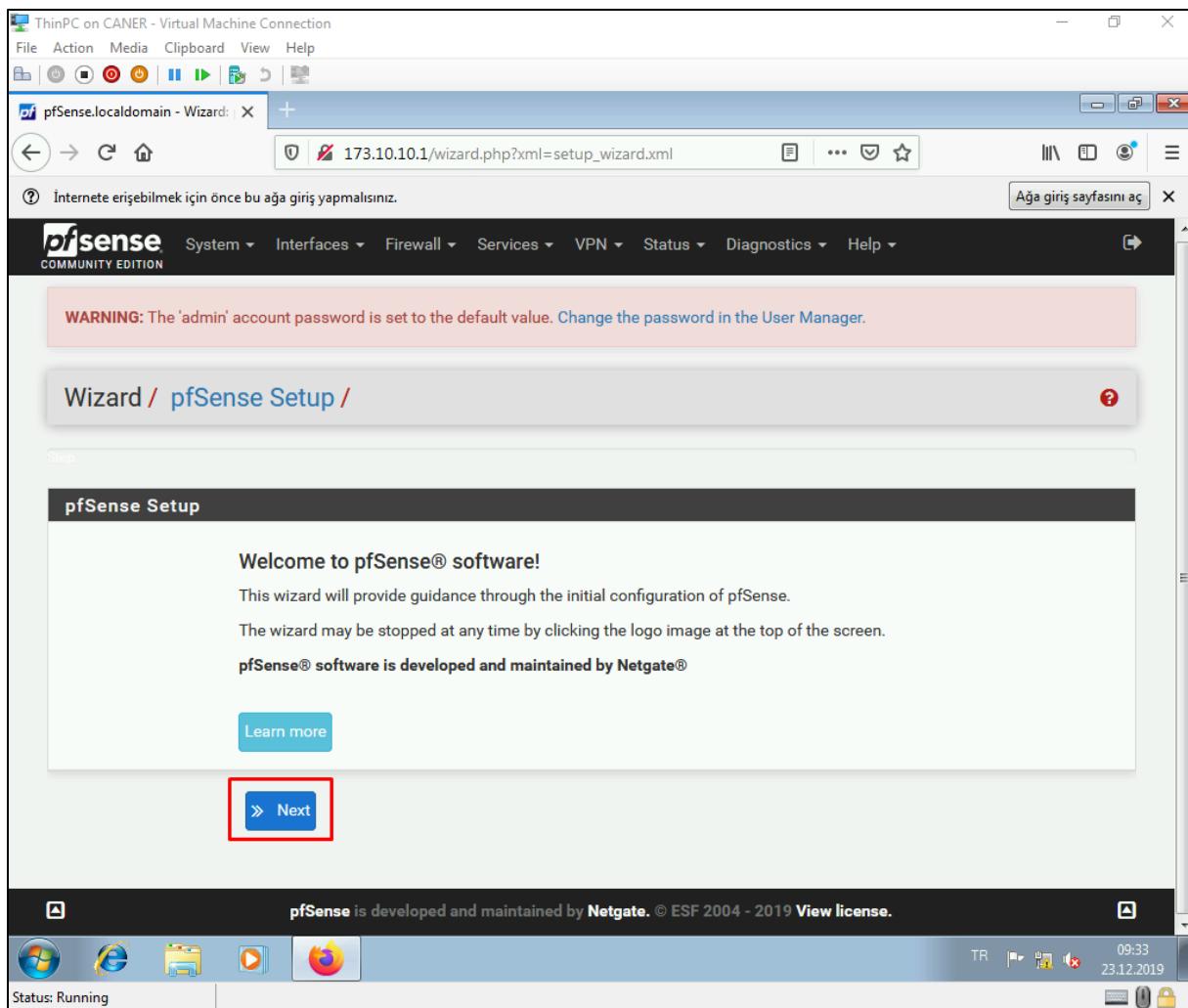
20.1.2020

We haven't set up any users yet but admin user with the password pfSense works.



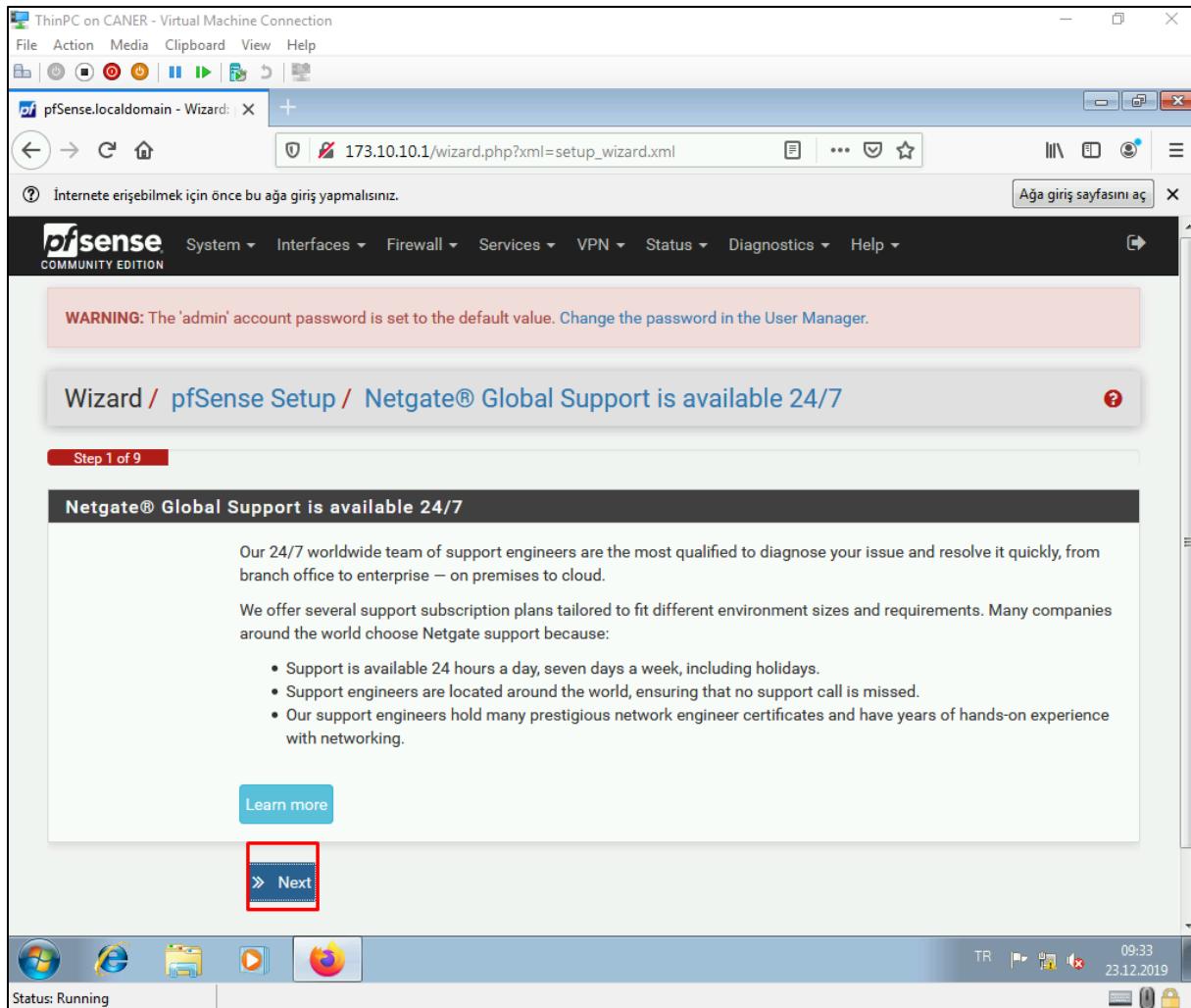
It will require us to change this password later during the configuration.

A setup wizard pops up and we simply need to follow its steps.

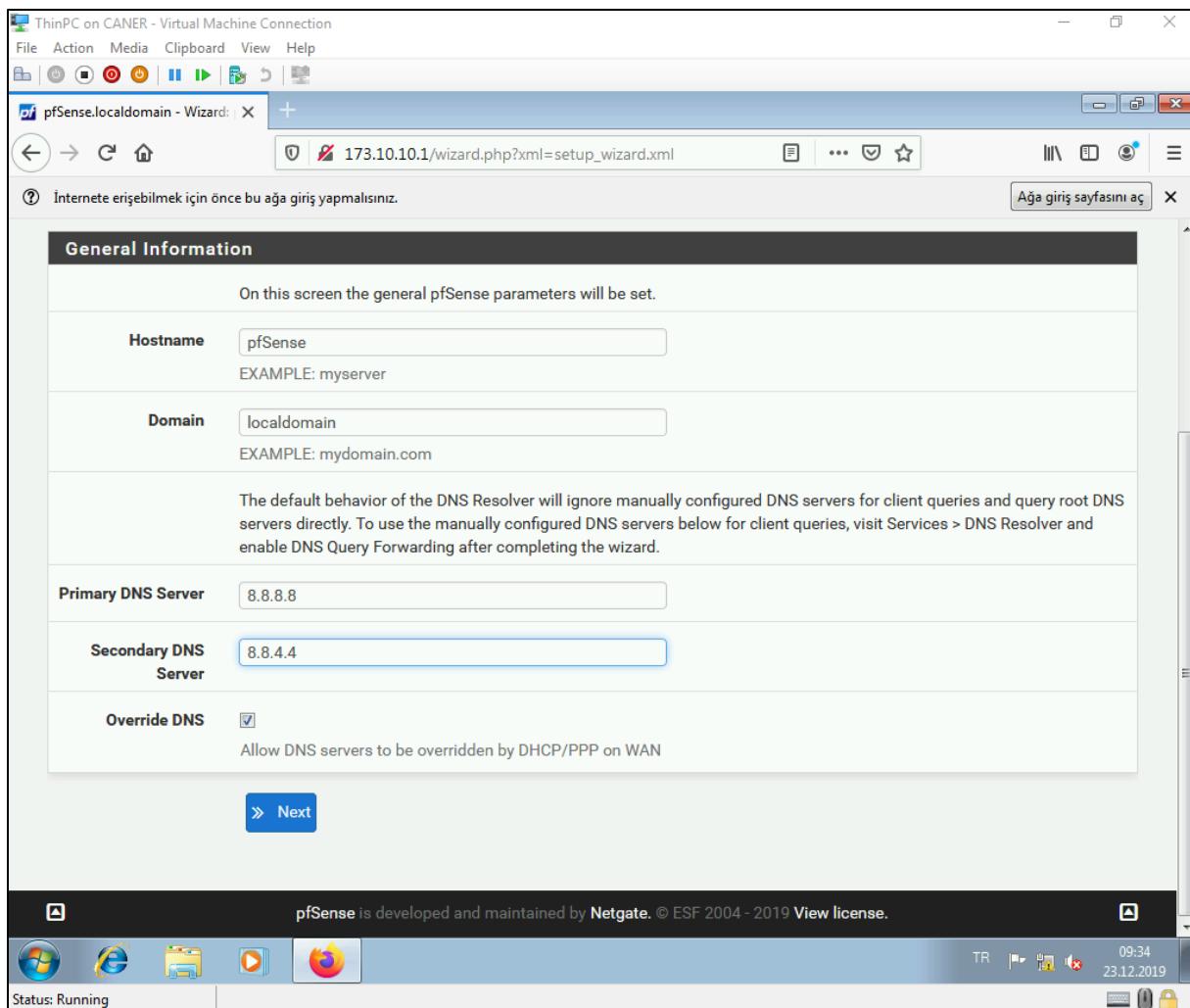


20.1.2020

We proceed.

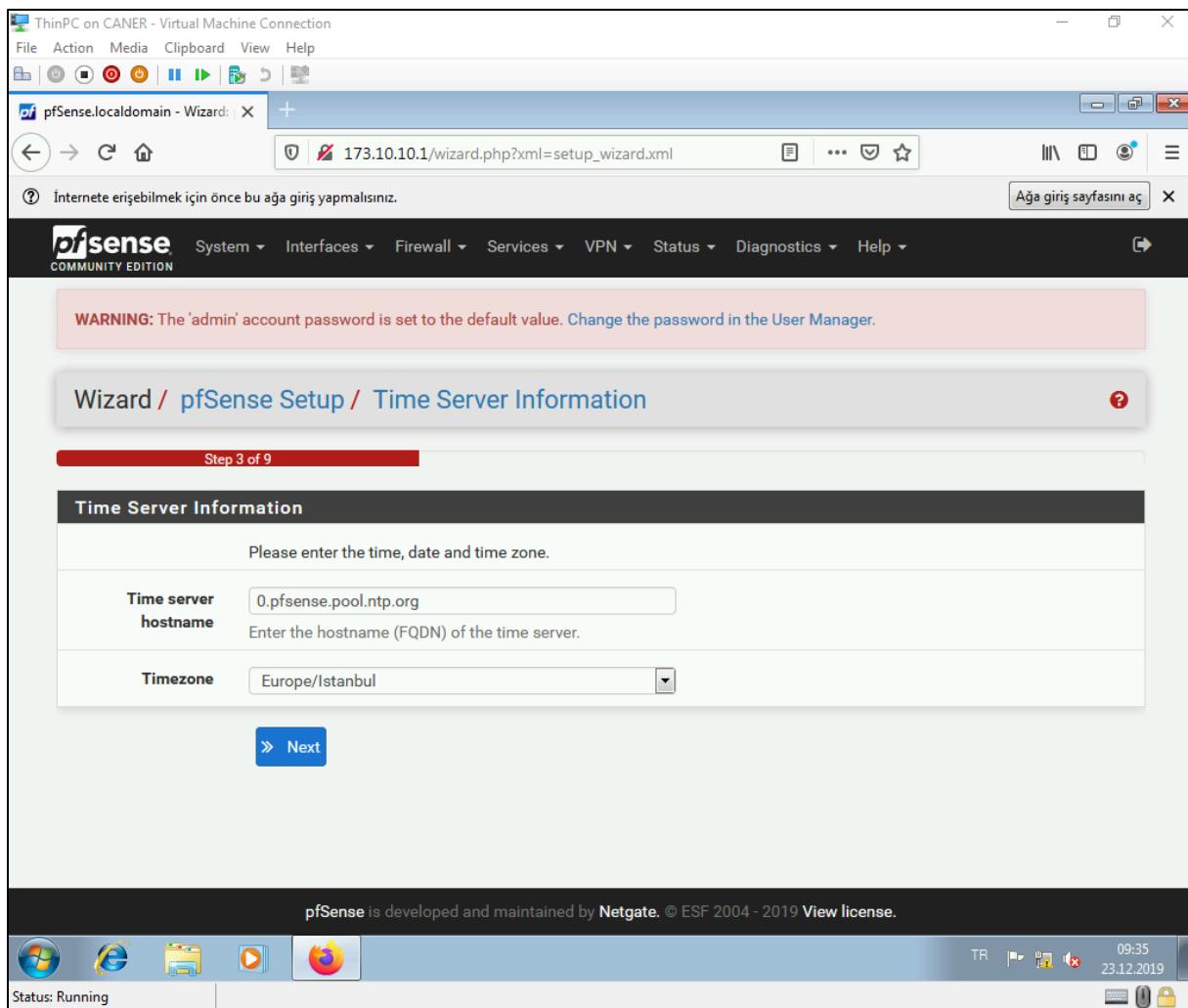


We name the local domain and select DNS servers. In this case, we used Google's DNS.

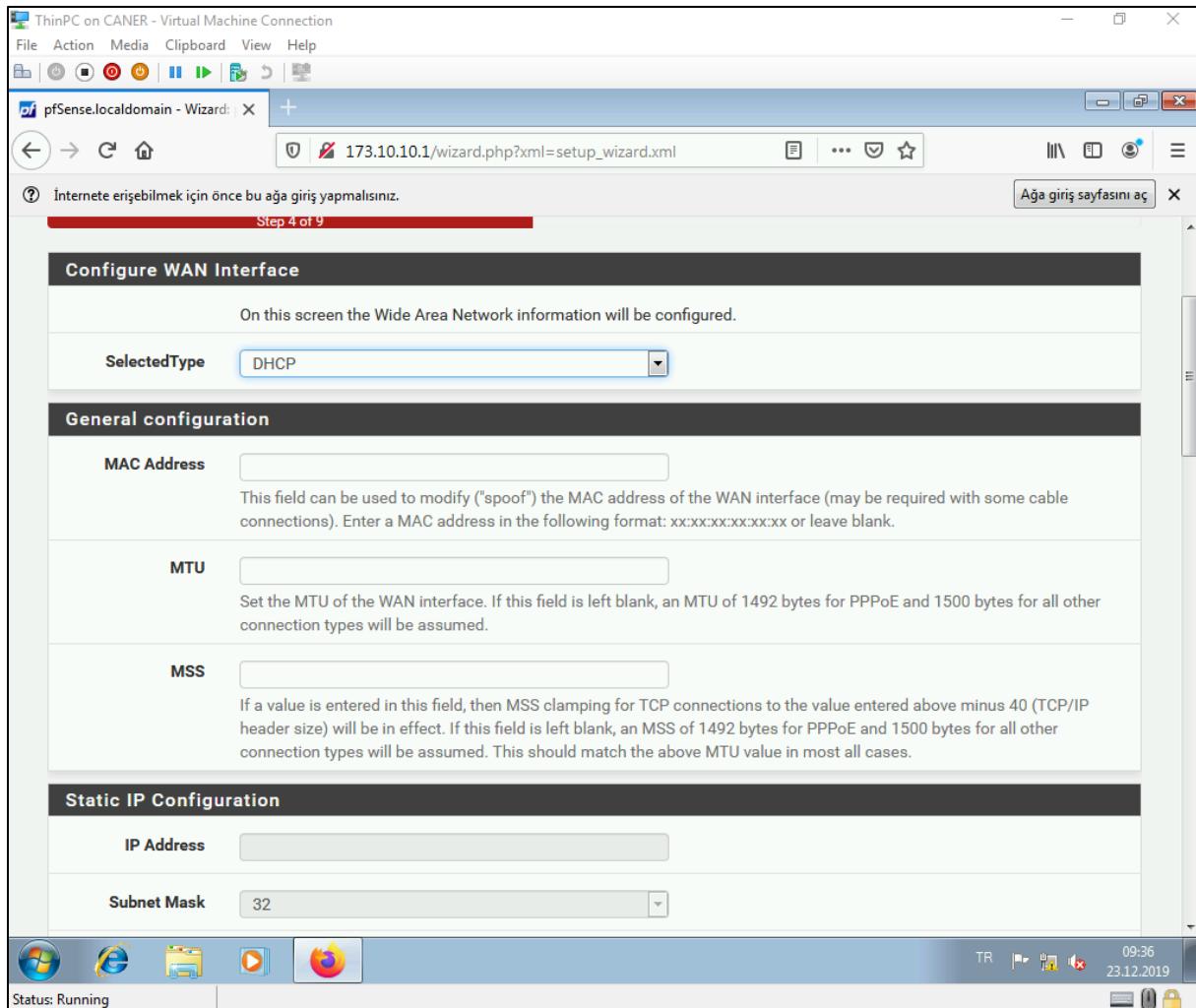


20.1.2020

We choose the time zone as Istanbul.

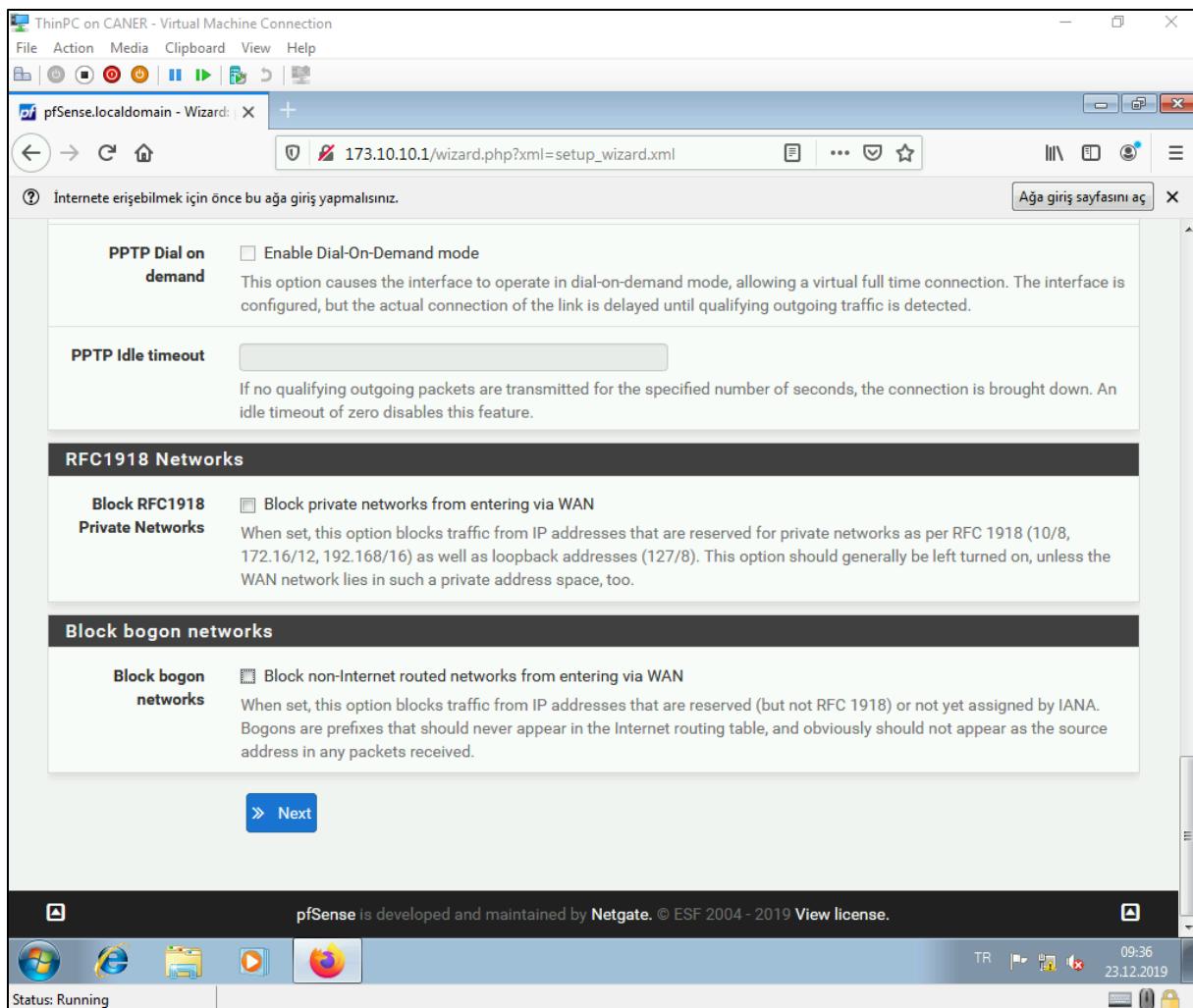


The WAN interface remains at DHCP since we need BAU's network to reach the internet.

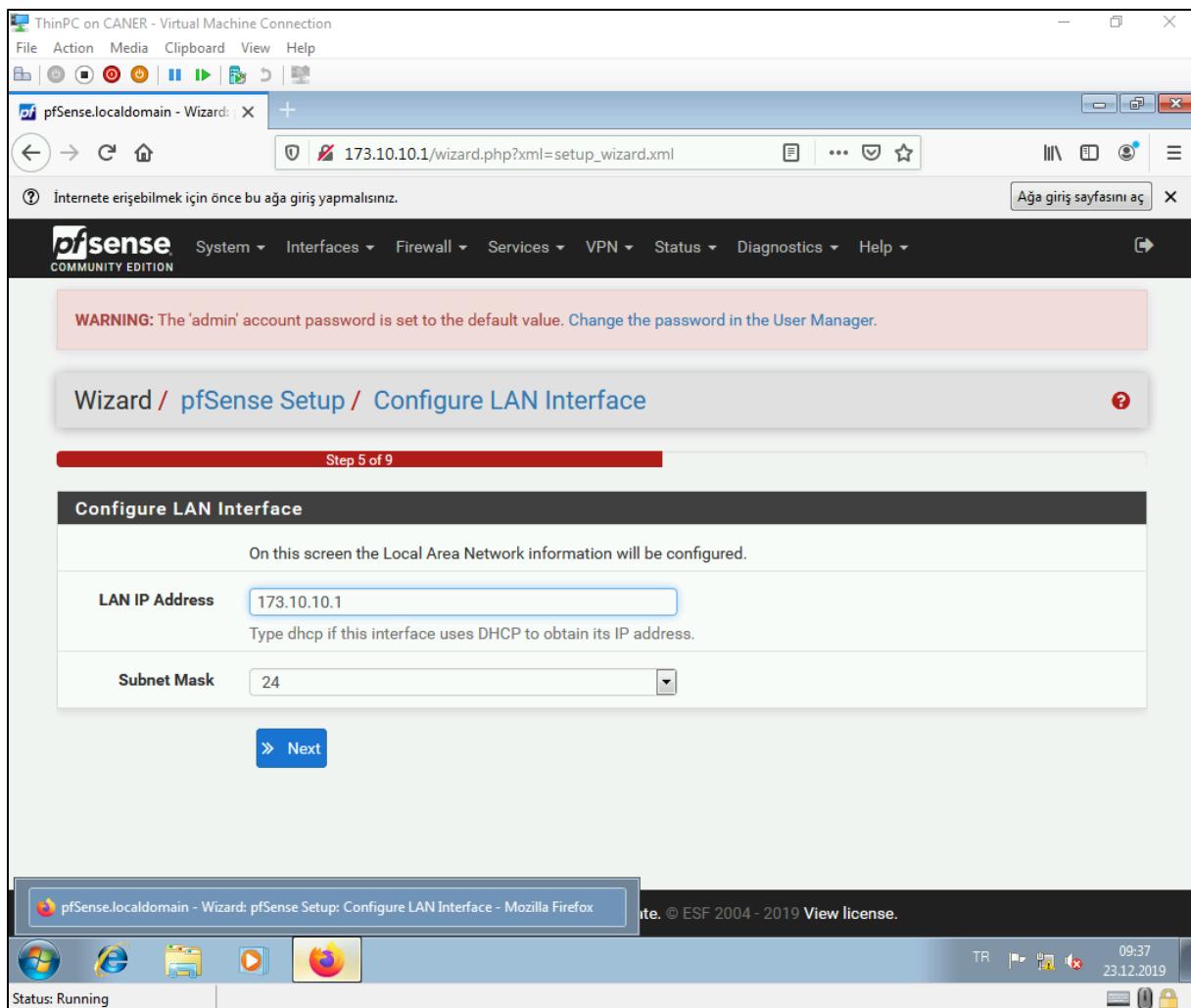


20.1.2020

And we don't change any other setting from there.

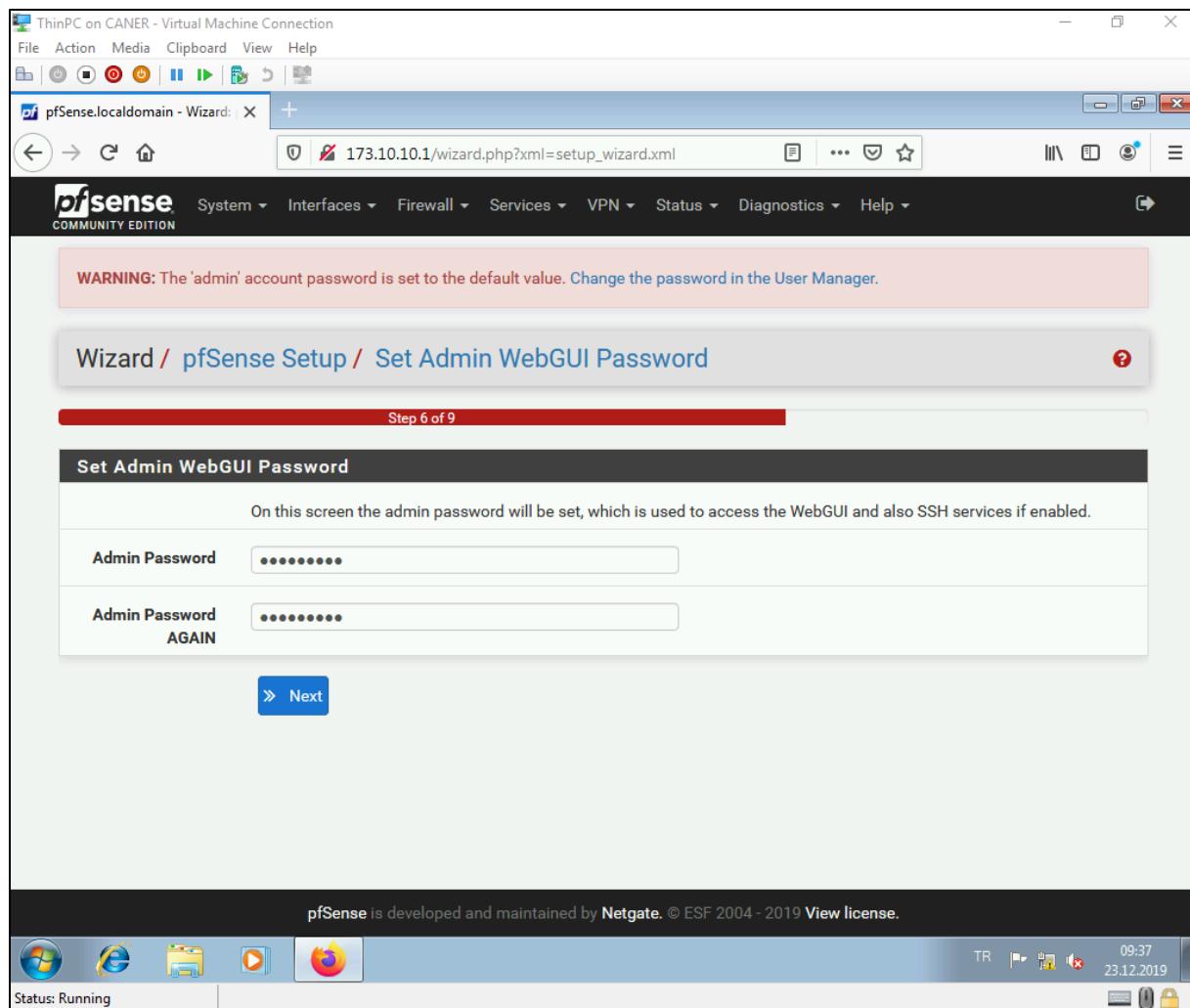


On the next step, we confirm our setup of the LAN interface. Again we change nothing.

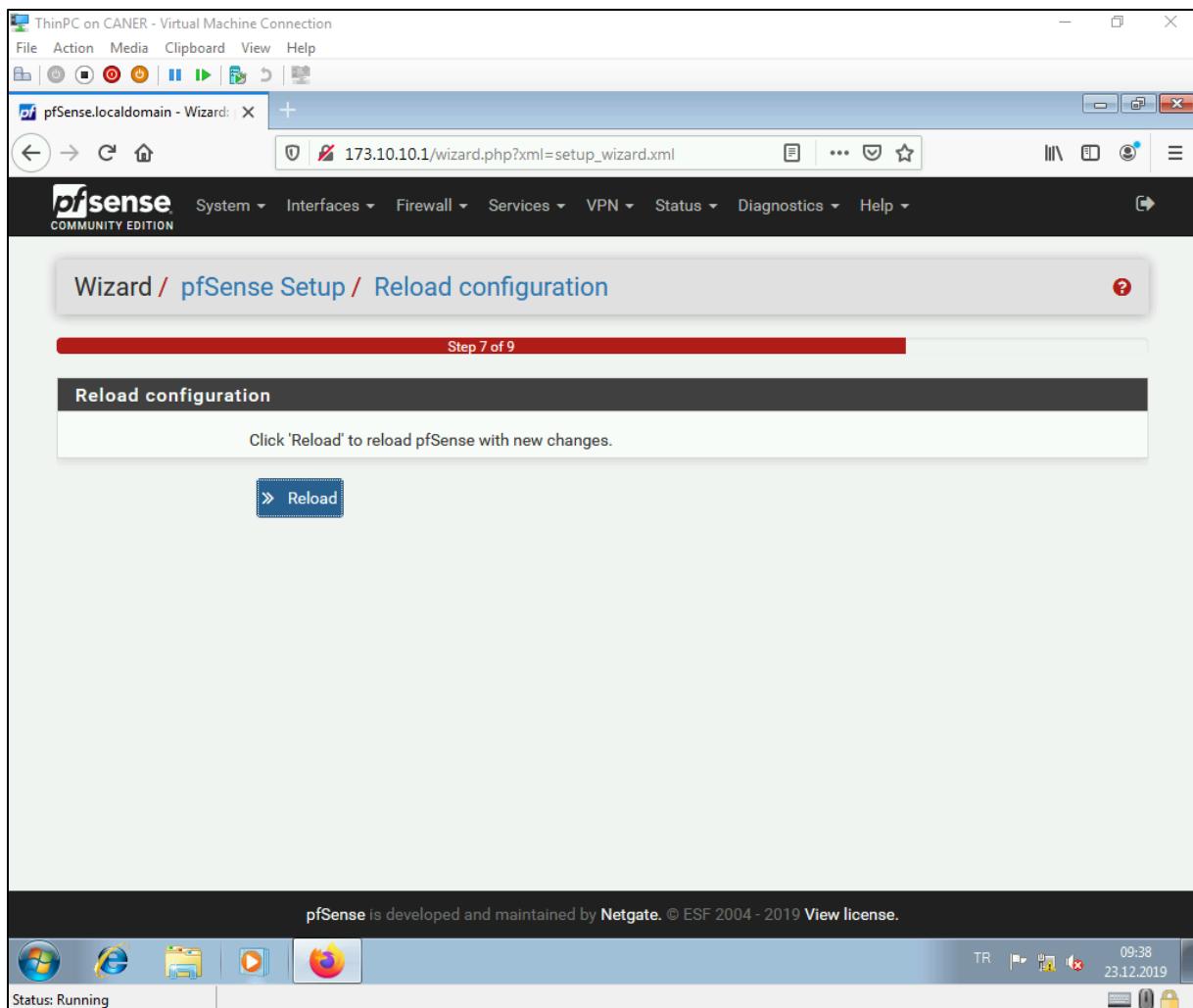


20.1.2020

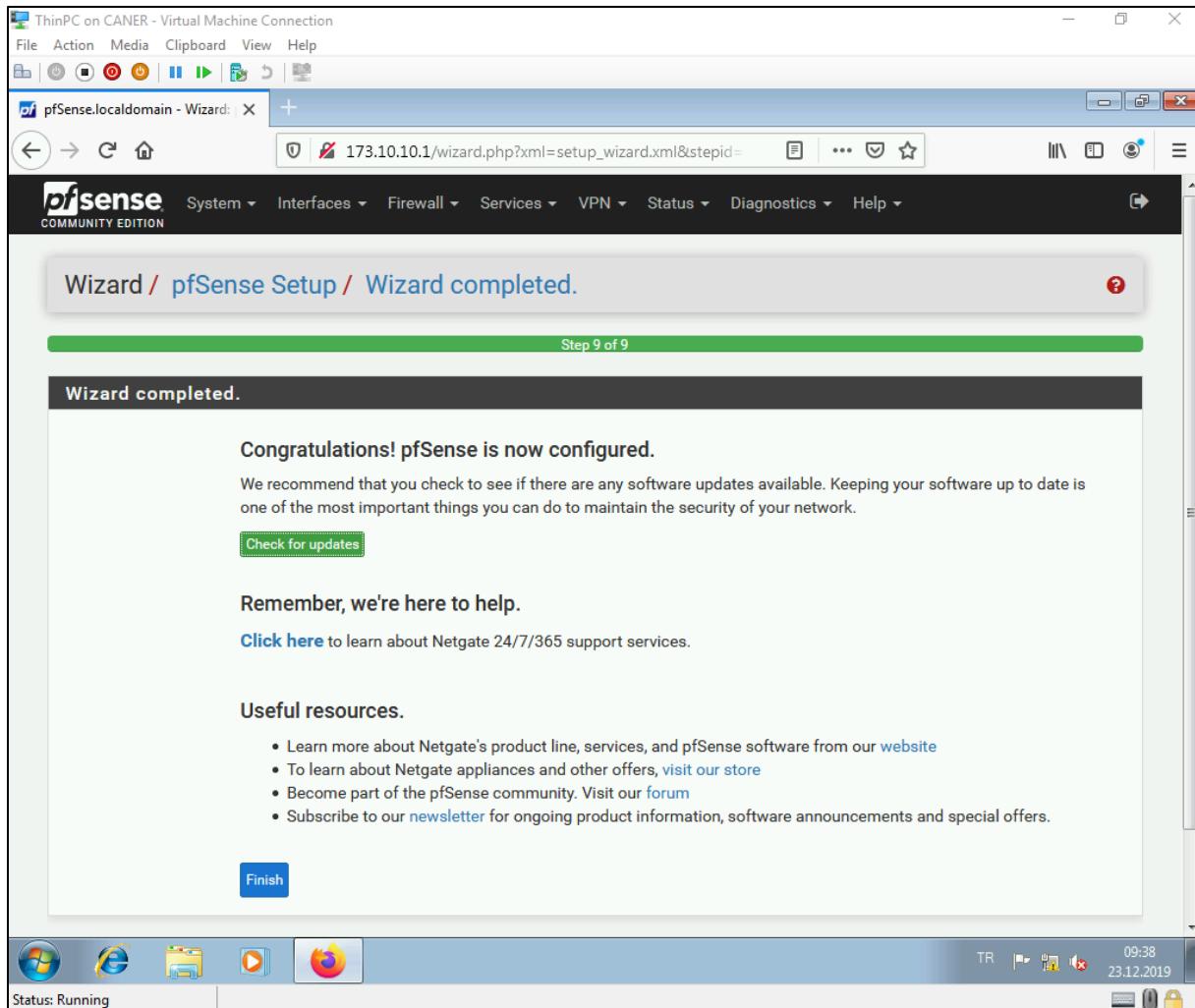
Then, it asks for a new admin password.



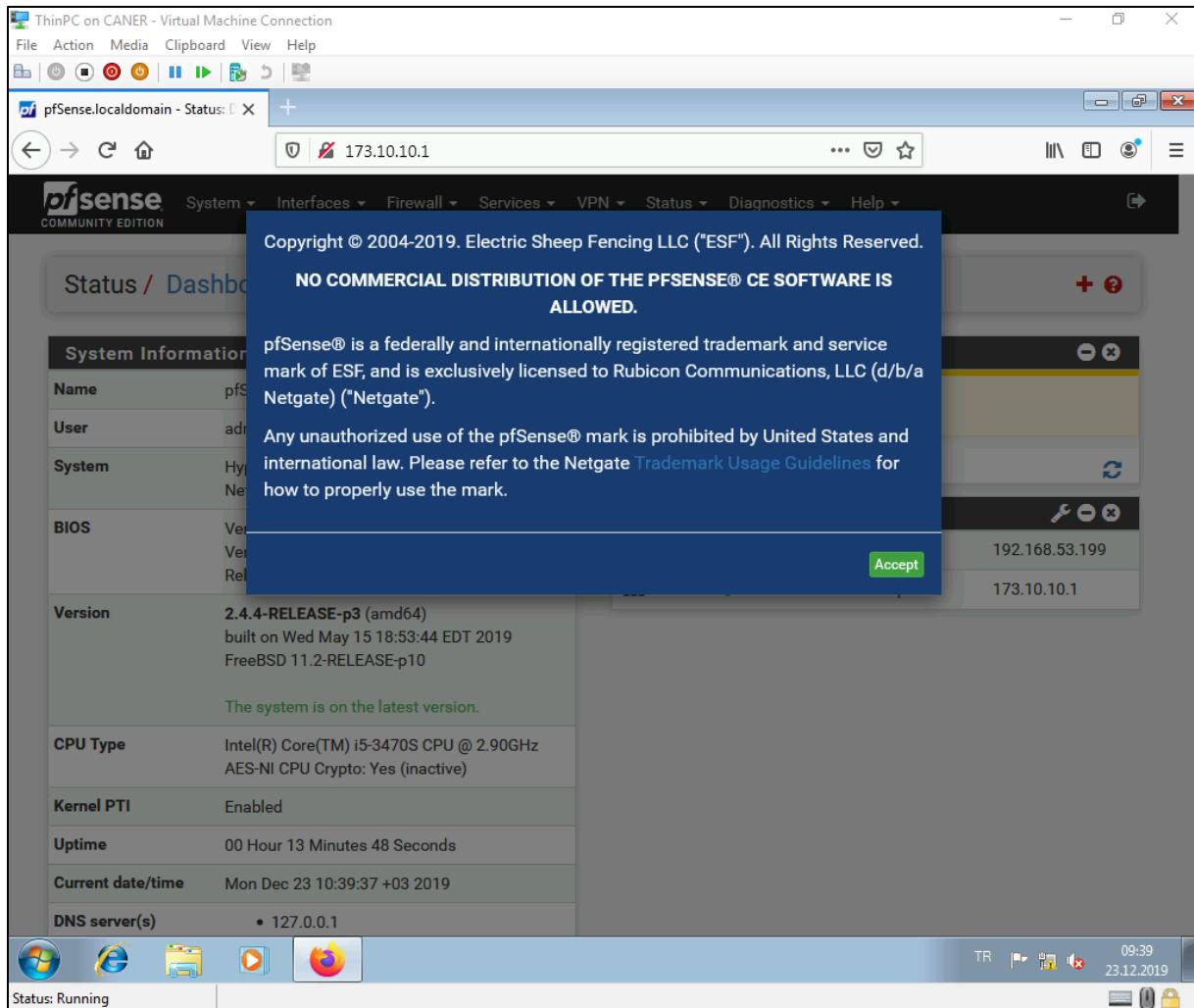
We now need to reload the configuration to save it.



This completes the setup and wizard is done.



Then, we're sent to the Status Dashboard where this screen welcomes us.



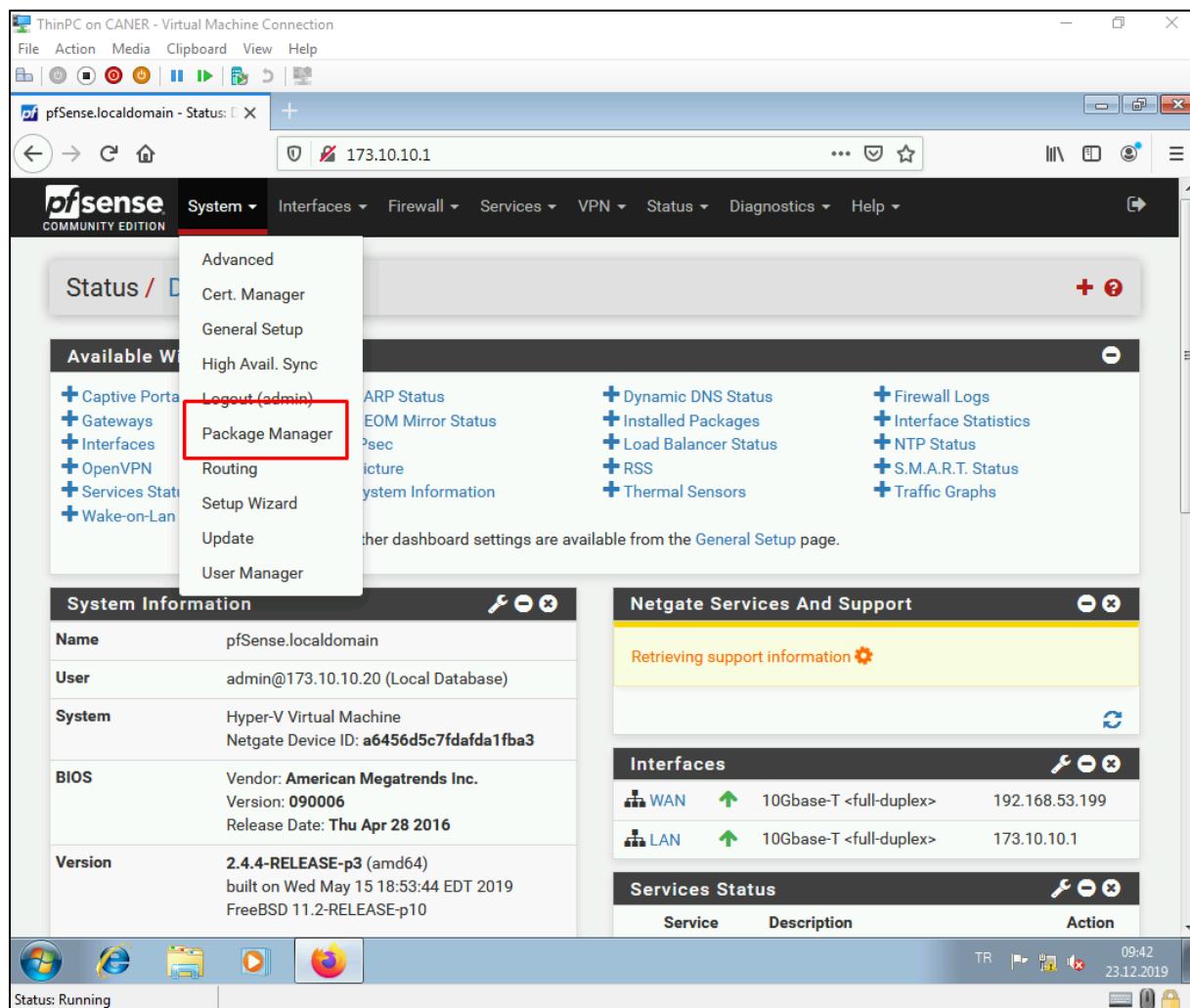
We add services status to the dashboard and look at the services that are currently running.

The screenshot shows the pfSense dashboard interface. At the top left, it says "ThinPC on CANER - Virtual Machine Connection". The main title is "pfSense.localdomain - Status" with the IP "173.10.10.1". The left sidebar has a menu with "Services Status" highlighted by a red box. The dashboard includes sections for System Information, Netgate Services And Support (showing "Retrieving support information"), Interfaces (listing WAN and LAN ports), and Services Status. The Services Status section is also highlighted with a red box and contains a table with the following data:

Service	Description	Action
dhcpcd	DHCP Service	
dpinger	Gateway Monitoring Daemon	
ntpd	NTP clock sync	
syslogd	System Logger Daemon	
unbound	DNS Resolver	

At the bottom, there are browser icons (IE, Firefox) and a status bar showing "Status: Running" and the date "23.12.2019".

Now let's start a Radius service so that our internal users must enter their credentials to connect to the internet. We don't want anyone to get to the internet easily we want to track when they connect and how long they stay connected. Firstly, we need to get to the Package Manager.



20.1.2020

Under Available Packages...

The screenshot shows the pfSense Package Manager interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the title "System / Package Manager / Available Packages" is displayed. There are two tabs: "Installed Packages" and "Available Packages", with "Available Packages" being the active tab and highlighted with a red box. A search bar is present with a placeholder "Enter a search string or *nix regular expression to search package names and descriptions." Below the search bar is a table titled "Packages" with columns for Name, Version, and Description. The table lists three packages: acme, apcupsd, and arping. Each package row includes a "Install" button with a green plus sign. The "acme" package is described as "Automated Certificate Management Environment, for automated use of LetsEncrypt certificates." Its dependencies are listed as pec-ssh2-1.1.2, socat-1.7.3.2_3, php72-7.2.10, and php72-ftp-7.2.10. The "apcupsd" package is described as "apcupsd" can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN. Its dependency is listed as apcupsd-3.14.14_2. The "arping" package is described as "Broadcasts a who-has ARP packet on the network and prints answers." Its dependency is listed as arp-1.1.2. At the bottom left, the status "Status: Running" is shown, and at the bottom right, there are icons for desktop, lock, and help.

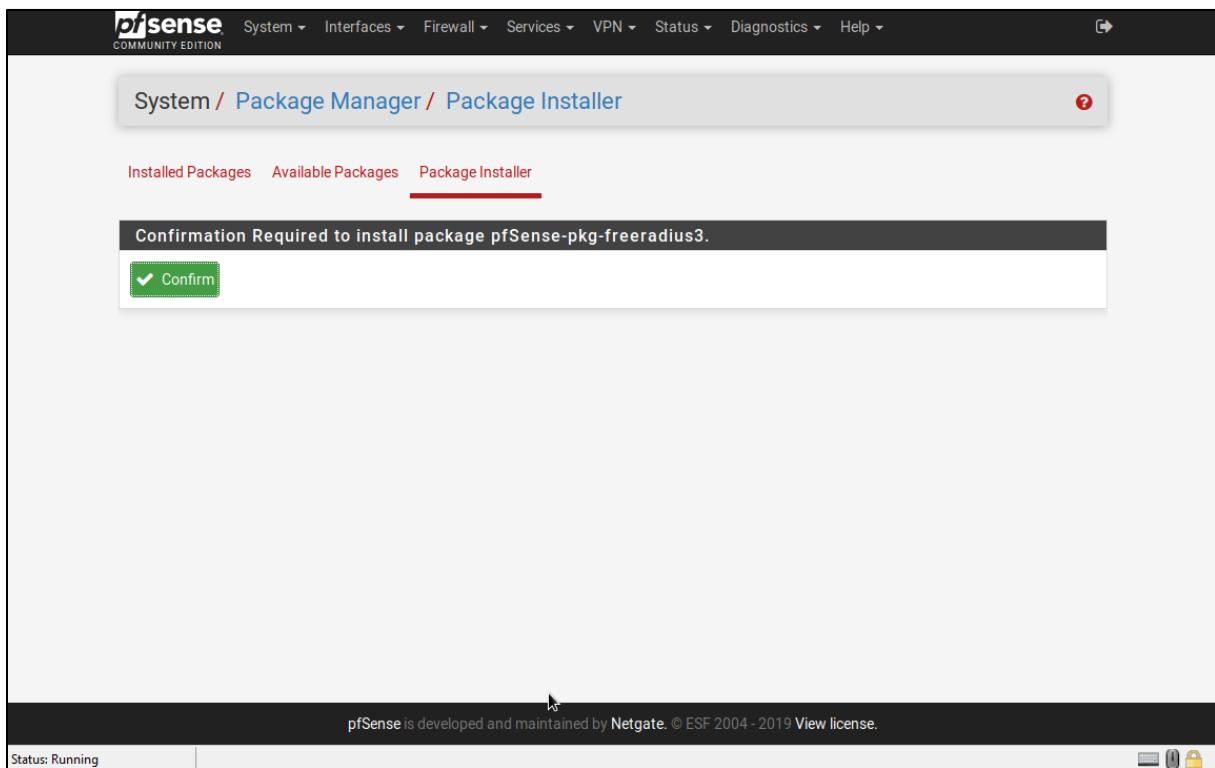
Name	Version	Description
acme	0.6.4	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pec-ssh2-1.1.2 socat-1.7.3.2_3 php72-7.2.10 php72-ftp-7.2.10
apcupsd	0.3.91_8	"apcupsd" can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN. Package Dependencies: apcupsd-3.14.14_2
arping	1.2.2_1	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arp-1.1.2

We install freeradius3.

Cron	0.3.7_3	The cron utility is used to manage commands on a schedule.	+ Install
darkstat	3.1.3_4	darkstat is a network statistics gatherer. It's a packet sniffer that runs as a background process on a cable/DSL router, gathers all sorts of statistics about network usage, and serves them over HTTP. Package Dependencies: darkstat-3.0.719	+ Install
Filer	0.60.6_1	Allows you to create and overwrite files from the GUI.	+ Install
freeradius3	0.15.7_7	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos. Package Dependencies: bash-4.4.23 freeradius3-3.0.17 python27-2.7.16	+ Install
frr	0.6.3_1	FRR routing daemon for BGP, OSPF, and OSPF6 Conflicts with Quagga OSPF and OpenBGPD. These packages cannot be installed at the same time. Package Dependencies: frf6-6.0.2_1	+ Install
FTP_Client_Proxy	0.3_3	Basic FTP Client Proxy using ftp-proxy from FreeBSD.	+ Install
gwled	0.2.4_1	Allows you to use LEDs for monitoring gateway status on supported platforms (ALIX, WRAP, Soekris, etc.)	+ Install
haproxy	0.59_21	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching. Package Dependencies: haproxy17-1.7.12	+ Install
haproxy-devel	0.59_22	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Contains AOL, examples, documentation, and more.	+ Install

20.1.2020

We confirm to install it.



After a little while the installation is complete.

The screenshot shows the pfSense Package Manager interface. At the top, the pfSense logo and navigation menu (System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help) are visible. Below the menu, the title "System / Package Manager / Package Installer" is displayed. A green notification bar at the top of the main content area states "pfSense-pkg-freeradius3 installation successfully completed." Below this, there are three tabs: "Installed Packages" (red), "Available Packages" (grey), and "Package Installer" (blue, underlined). The main content area is titled "Package Installation". It contains a message from the package: "Useful configuration advice can be found in the FreeRADIUS Wiki at <http://wiki.freeradius.org>". Below this, a message from "pfSense-pkg-freeradius3-0.15.7_7:" is shown, instructing the user to visit the "FreeRADIUS" menu in the Services section to configure the package. It also mentions that EAP certificate configuration is required and provides instructions for creating a CA and server certificates. The message concludes with "Success". At the bottom left, the status "Status: Running" is shown, along with system icons for power, network, and security.

Then, we must reboot the firewall again.

```
Firewall on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
WAN (wan)    -> hm0      -> v4/DHCP4: 192.168.53.199/23
LAN (lan)    -> hm1      -> v4: 173.10.10.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 5

pfSense will reboot. This may take a few minutes, depending on your hardware.
Do you want to proceed?

Y/y: Reboot normally
R/r: Reroot (Stop processes, remount disks, re-run startup sequence)
S: Reboot into Single User Mode (requires console access!)
F: Reboot and run a filesystem check

Enter an option: y
Status: Running
```

We confirm that the package is installed after the reboot.

The screenshot shows a web browser window titled "ThinPC on CANER - Virtual Machine Connection". The address bar displays "173.10.10.1/pkg_mgr_installed.php". The page is the "Installed Packages" section of the pfSense Package Manager. The table lists one package:

Name	Category	Version	Description	Actions
✓ freeradius3	net	0.15.7_7	A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.	

Below the table, it says "Package Dependencies:" followed by "bash-4.4.23", "freeradius3-3.0.17", and "python27-2.7.16". At the bottom of the table, there are legends: "⟳ = Update" and "✓ = Current" for the checkmark icon; "trash = Remove" and "info = Information" for the trash bin and info icons; and "reinstall = Reinstall" for the circular arrow icon. A note says "Newer version available" and "Package is configured but not (fully) installed or deprecated".

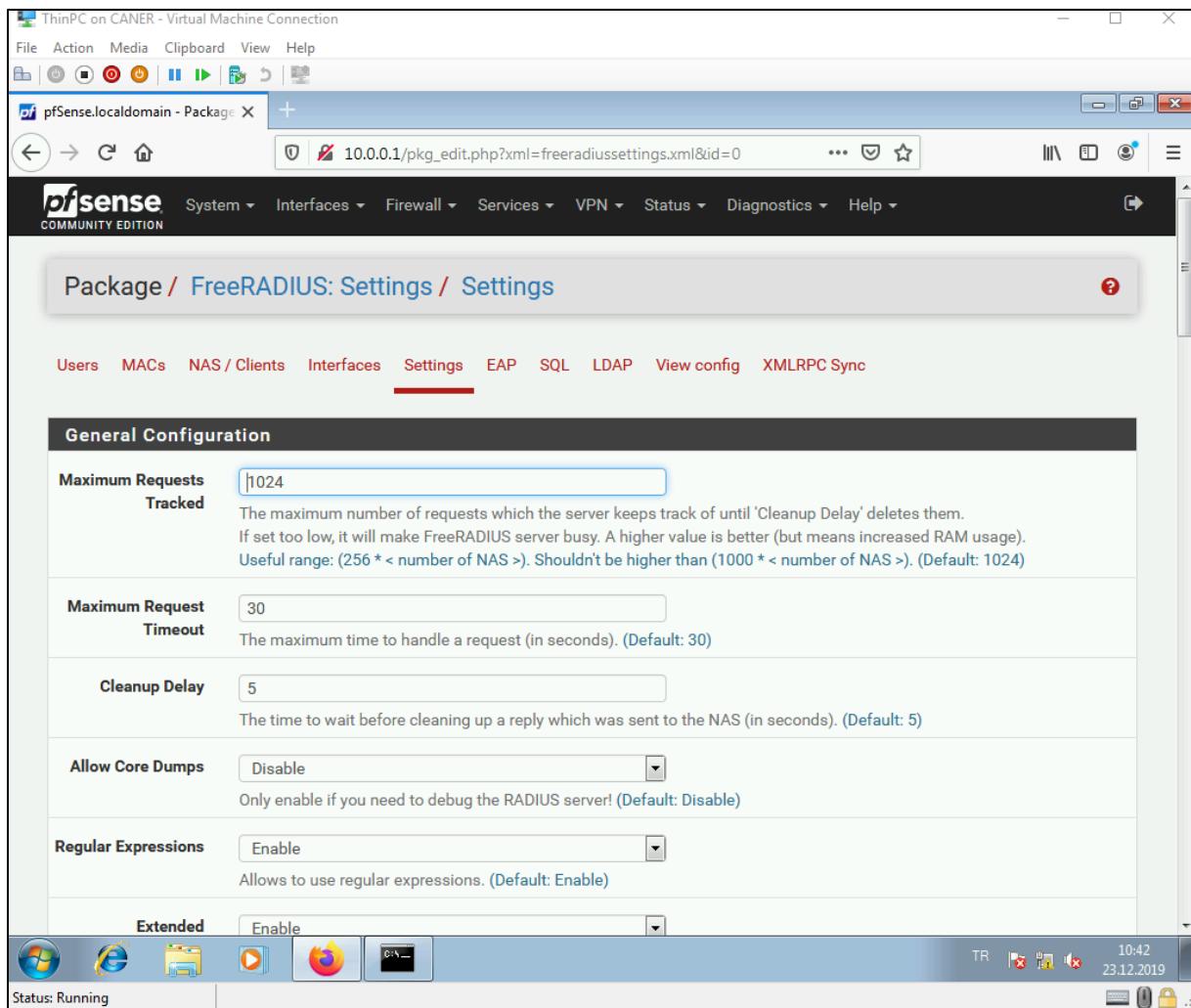
At the bottom of the screen, the pfSense footer states "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." The status bar shows "Status: Running" and the system time "10:32 23.12.2019".

20.1.2020

Then to configure the Radius we select it under Services.

The screenshot shows the pfSense 2.4.4 RELEASE-p3 dashboard. The Services menu is open, and the FreeRADIUS option is highlighted with a red box. The dashboard also displays system information such as Name (pfSense.localdomain), User (admin@10.0.0.20), System (Hyper-V Virtual Machine), BIOS (American Megatrends Inc.), Version (2.4.4-RELEASE-p3), CPU Type (Intel(R) Core(TM) i5-3470S CPU @ 2.90GHz), Kernel PTI (Enabled), Uptime (00 Hour 12 Minutes 14 Seconds), and Current (Mon Dec 23 11:42:23 +03 2019). The status bar at the bottom indicates "Status: Running".

We go under Settings...



... and enable MAC Authentication.

pfSense.localdomain - Package

Miscellaneous Configuration

Plain MAC Auth Enable Plain MAC Authentication
The Calling-Station-Id in an Access-Request is first checked against the authorized_macs list, before all other authorization methods. If the NAS is not able to convert the MAC address to the 802.1X format, this field can be enabled.
Leave this disabled (unchecked) unless absolutely necessary. (Default: Disabled)

Disable Acct_Unique Disable the 'rlm_acct_unique' module in FreeRADIUS "preacct" section.
If you encounter problems with some counters when using 'Amount of Download/Upload/Time', you can check this to disable the module. (Default: Enabled)

Save

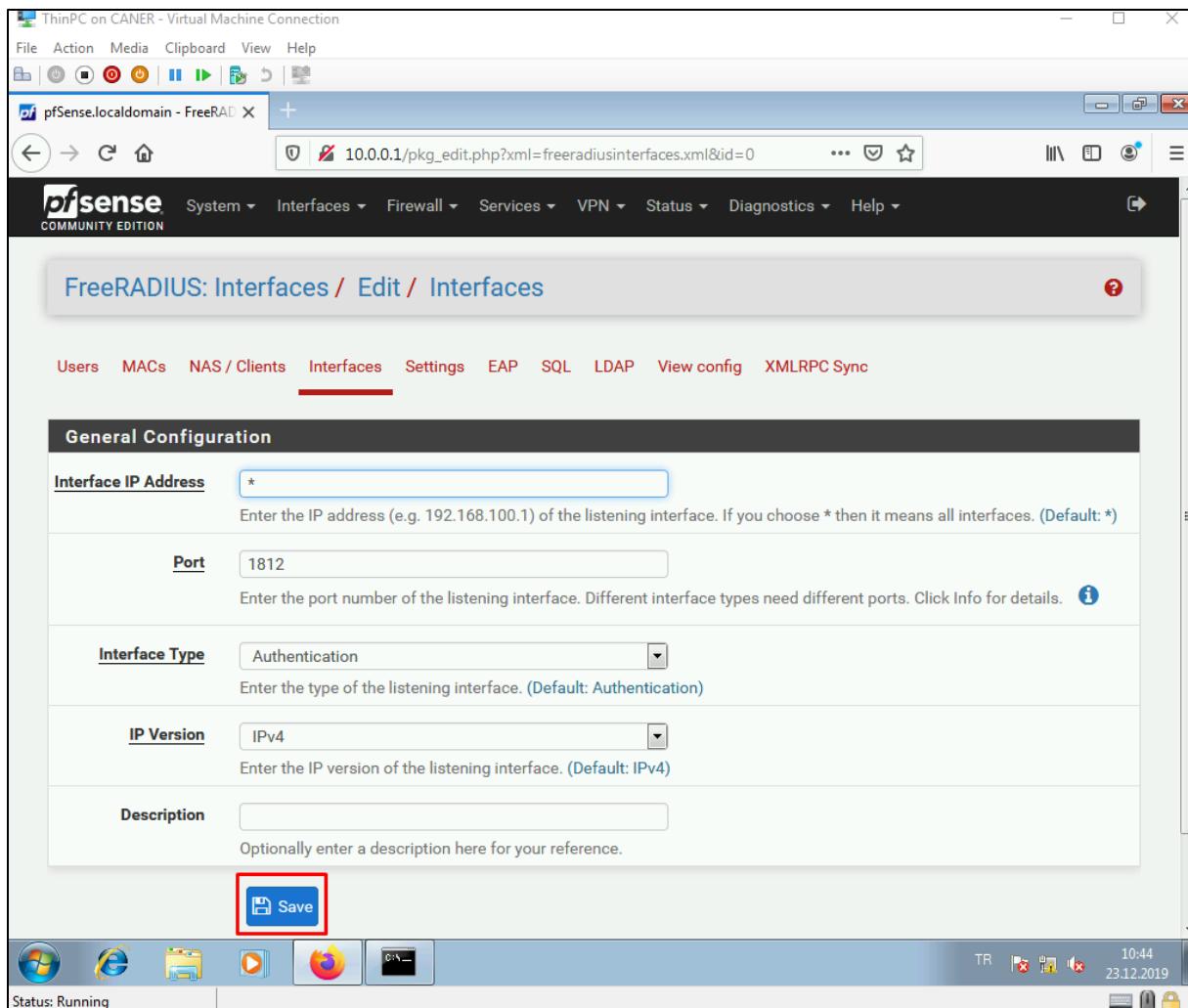
Status: Running

We go under Interfaces and add a new one.

The screenshot shows the pfSense web interface running on a ThinPC virtual machine. The browser title is "ThinPC on CANER - Virtual Machine Connection". The address bar shows the URL "10.0.0.1/pkg.php?xml=freradiusinterfaces.xml". The pfSense logo is at the top left, followed by navigation links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help. Below the navigation is a breadcrumb trail: Package / FreeRADIUS: Interfaces / Interfaces. A red box highlights the "Interfaces" tab in the top menu. Another red box highlights the green "Add" button with a plus sign in the bottom right corner of the table header. The table has columns: Interface IP Address, Port, Interface Type, IP Version, Description. A "Save" button is located below the table. At the bottom, a footer states "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." The taskbar at the bottom includes icons for File Explorer, Internet Explorer, Task Manager, and others, along with system status indicators like battery level and network connection.

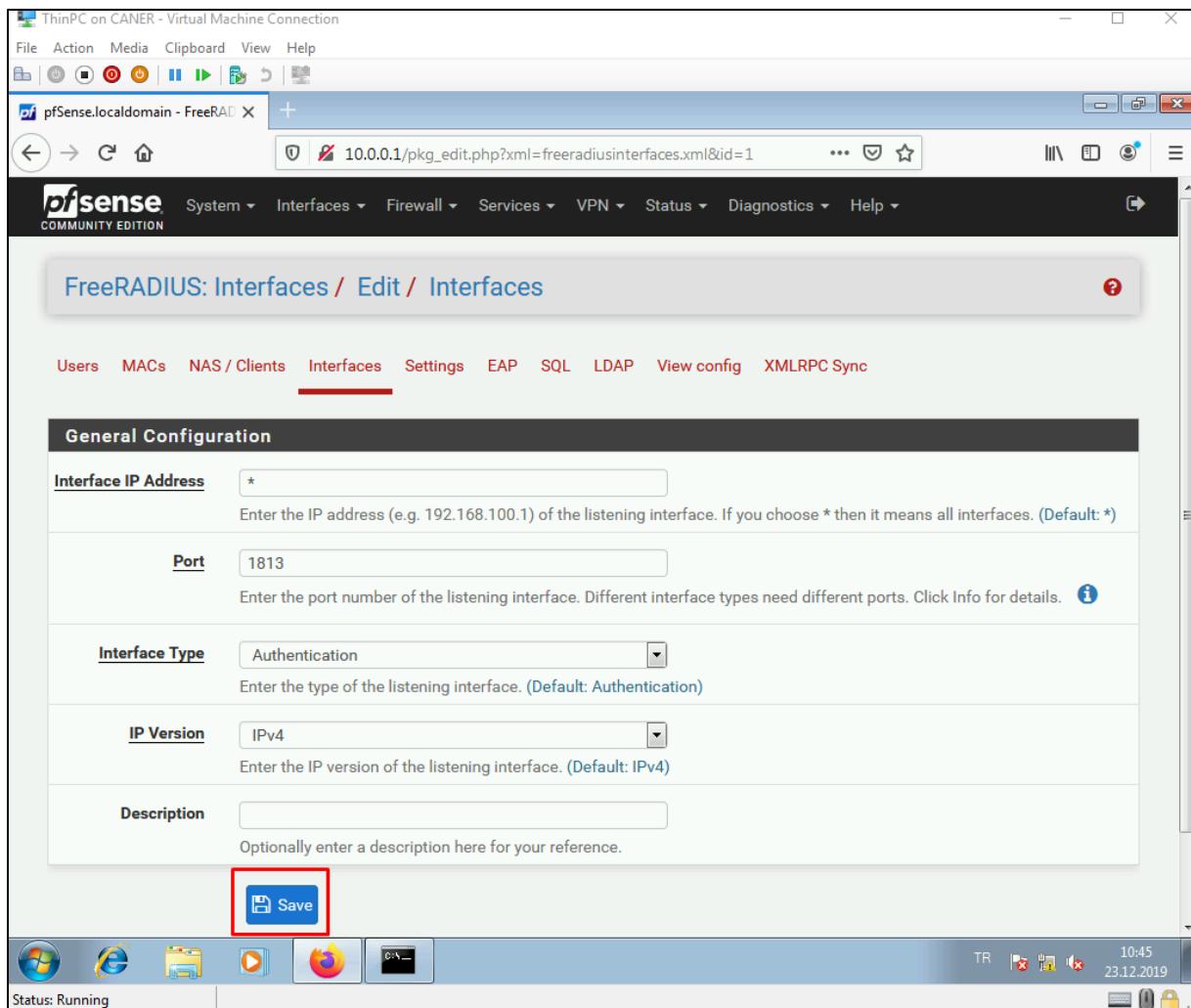
20.1.2020

Port 1812 must be specified.



Then, we save.

We do the same for port 1813 as well.



20.1.2020

We save once again.

The screenshot shows the pfSense web interface for managing FreeRADIUS interfaces. The URL in the browser is `10.0.0.1/pkg.php?xml=freeradiusinterfaces.xml`. The main menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The sub-menu for Interfaces is currently selected. The page title is "Package / FreeRADIUS: Interfaces / Interfaces". Below the title, there are tabs for Users, MACs, NAS / Clients, Interfaces (which is underlined), Settings, EAP, SQL, LDAP, View config, and XMLRPC Sync. The main content area displays a table with the following data:

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	
*	1813	auth	ipaddr	

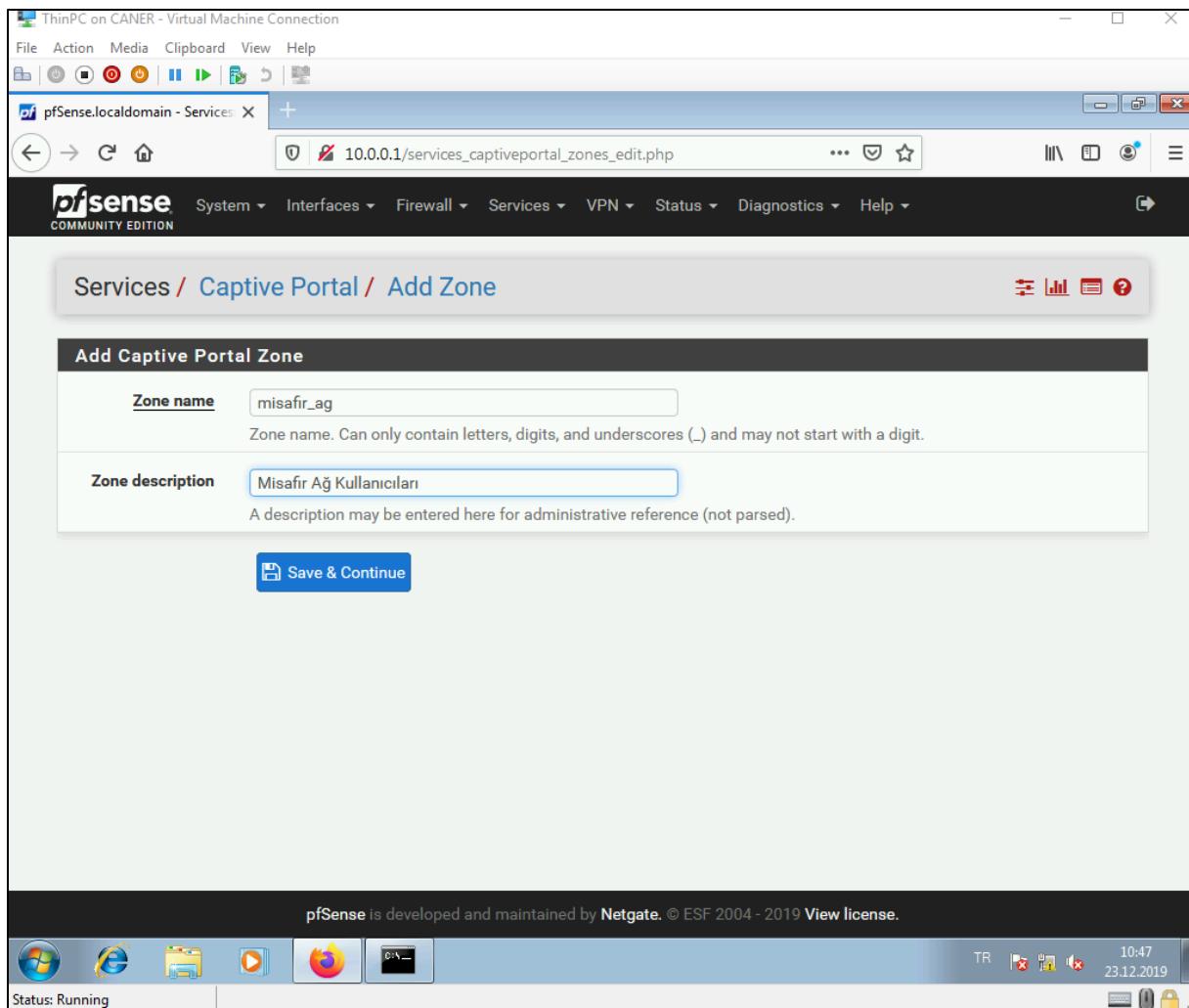
At the bottom left of the table area, there is a blue "Save" button with a white outline, which is highlighted with a red box. At the bottom right of the table area, there is a green "Add" button with a white outline. The status bar at the bottom of the browser window shows "Status: Running".

We then get to the Captive Portal Service.

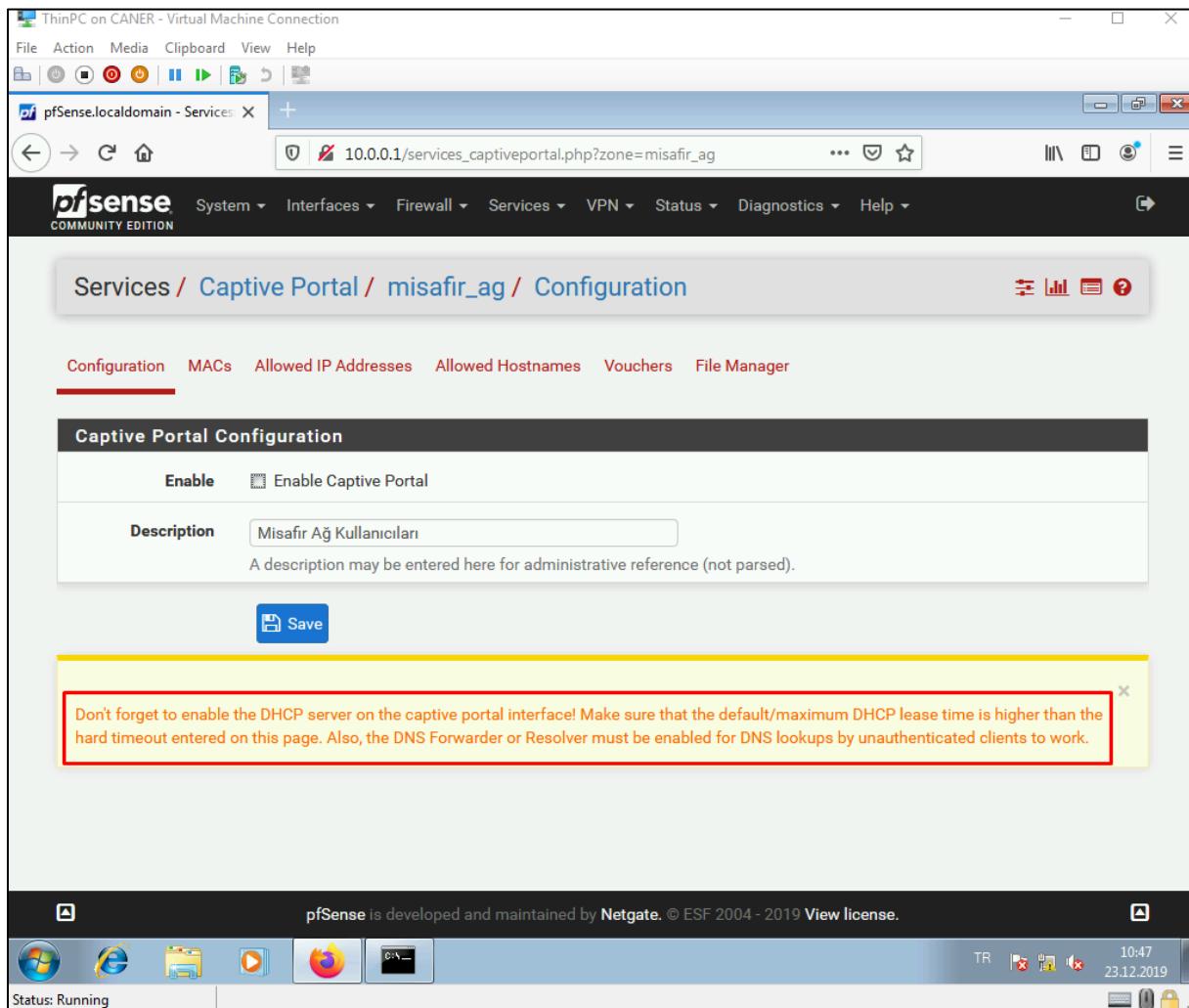
The screenshot shows the pfSense web interface. The URL in the browser is `10.0.0.1/pkg.php?xml=freeradiusinterfaces.xml`. The main menu bar includes File, Action, Media, Clipboard, View, Help, and several icons. The navigation bar has links for pfSense.localdomain - Package, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Package / FreeRADIUS: Interfaces". On the left, there are tabs for Users, MACs, NAS / Clients, Interfaces (which is selected), and Settings. Below the tabs is a table with columns: Interface IP Address, Port, and Int. The table contains two rows, both marked with an asterisk (*). A blue "Save" button is located at the bottom left of this section. To the right of the table is a sidebar with a list of services: Auto Config Backup, Captive Portal (highlighted with a red box), DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, FreeRADIUS, IGMP Proxy, Load Balancer, NTP, PPPoE Server, SNMP, UPnP & NAT-PMP, and Wake-on-LAN. Below the sidebar is a table with columns: IP Version and Description. It lists two entries: "ipaddr" and another "ipaddr". Each entry has edit and delete icons. A green "Add" button is located at the bottom right of this table. At the bottom of the interface, there is a footer with the pfSense logo, a copyright notice (pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.), and a status bar showing "Status: Running". The system tray on the right shows icons for battery, signal strength, and date/time (23.12.2019, 10:46).

20.1.2020

We name the zone we want to use.



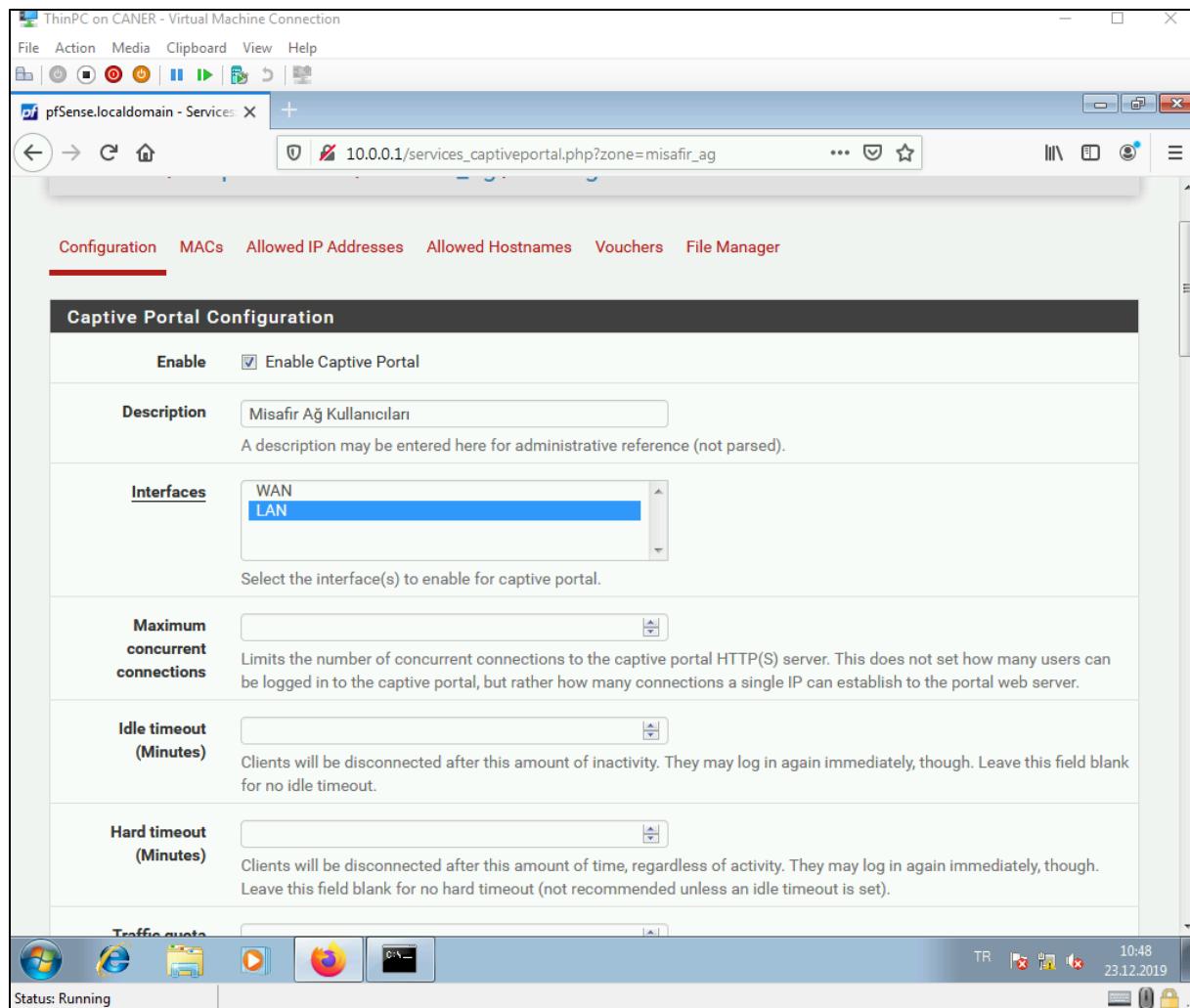
pfSense reminds us to use DHCP for the interface we will be using for the portal. Luckily, that is already case for us.



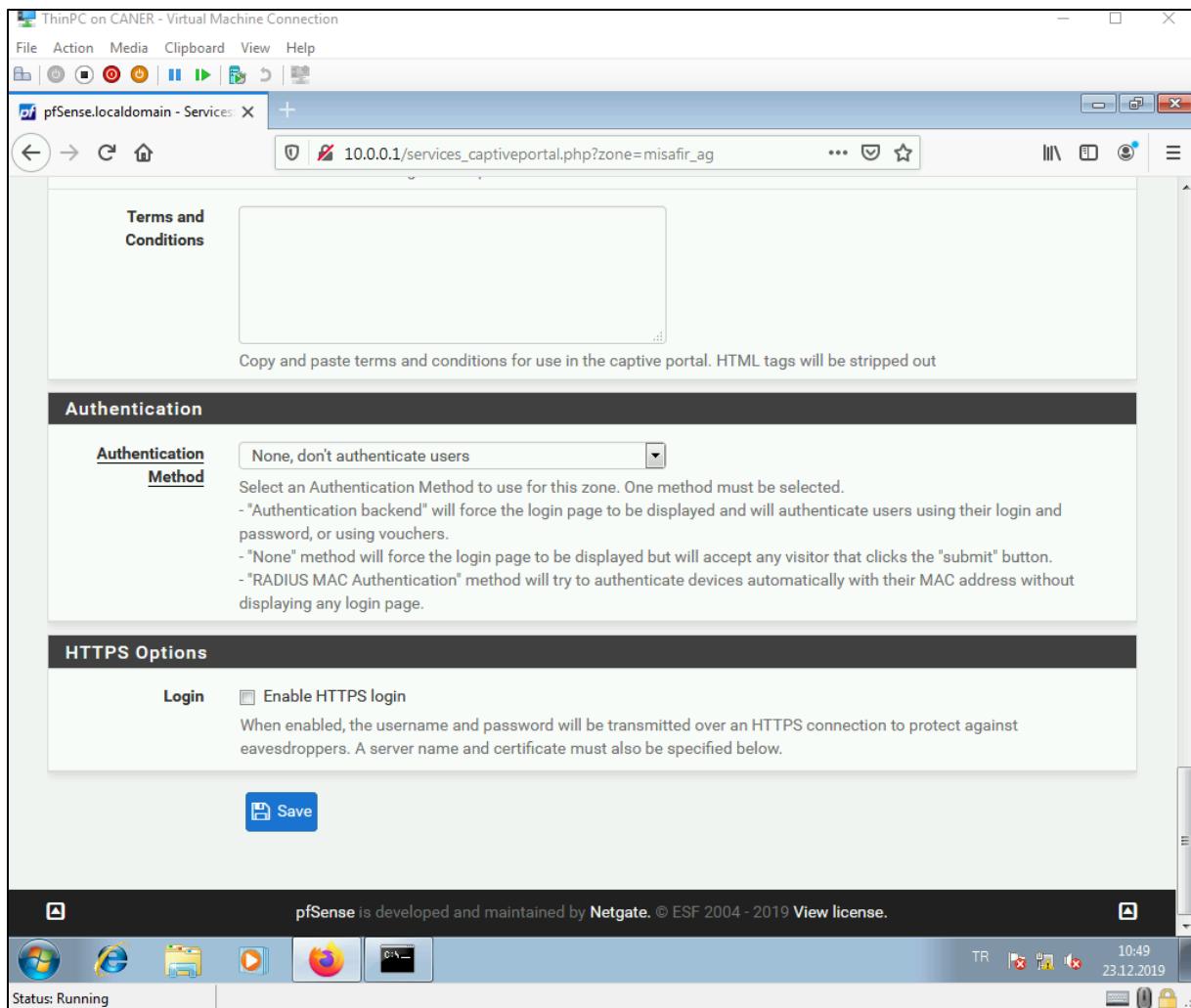
Once we enable the service...

20.1.2020

... many configuration settings pop up. We must select the LAN interface here.



And for now, we don't change anything else.



We will come back to these settings and modify them in a bit.

20.1.2020

This creates the zone.

The screenshot shows the pfSense Services / Captive Portal interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the main content area has a title "Services / Captive Portal". Underneath the title is a table titled "Captive Portal Zones". The table has columns for Zone, Interfaces, Number of users, Description, and Actions. There is one entry in the table:

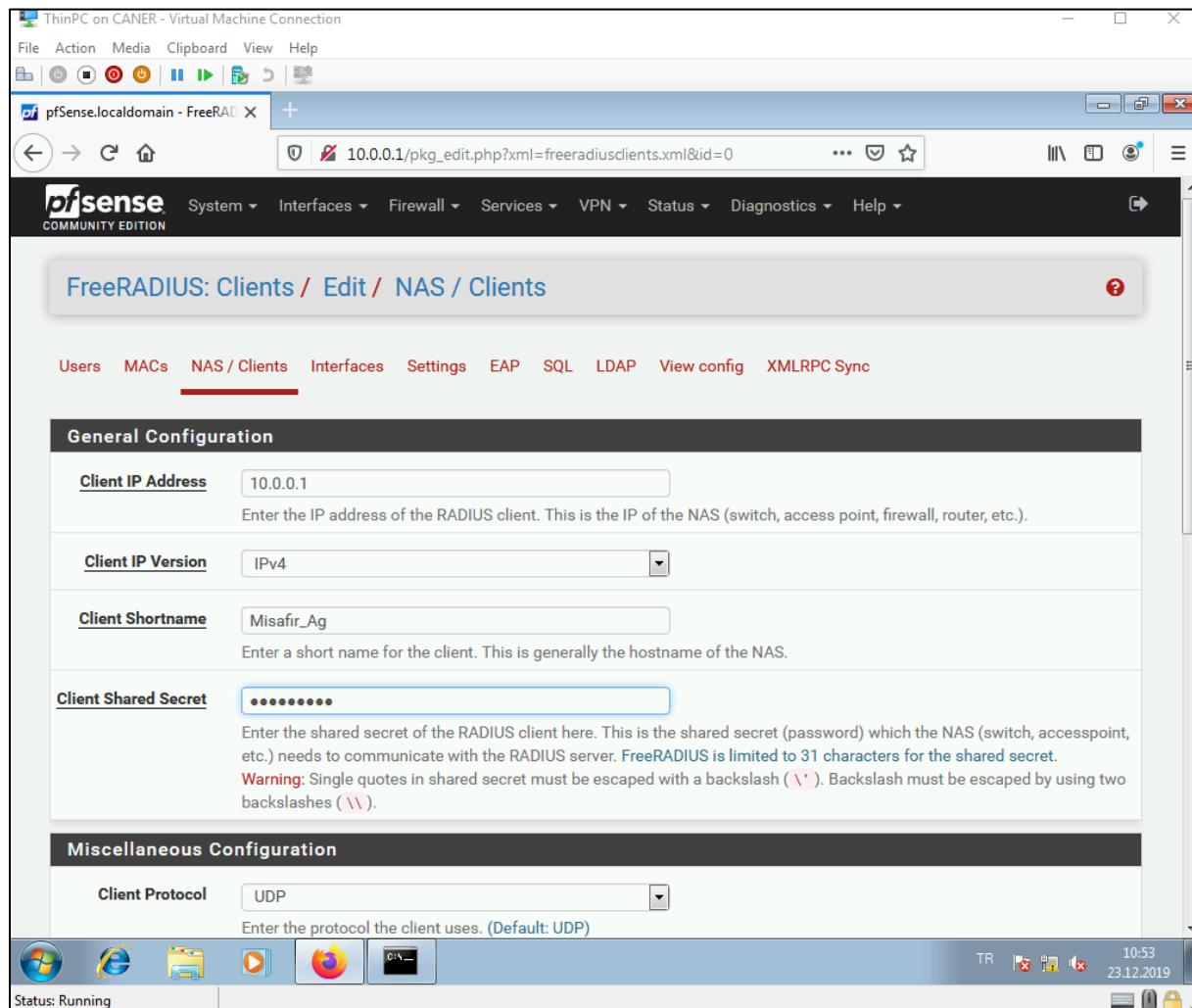
Zone	Interfaces	Number of users	Description	Actions
misafir_ag	LAN	0	Misafir Ağ Kullanıcıları	

At the bottom right of the table, there is a green "Add" button with a plus sign. The status bar at the bottom of the window shows "Status: Running" and the date and time "23.12.2019 10:50".

We now need to create some NAS clients.

The screenshot shows the pfSense web interface on a ThinPC virtual machine. The URL in the browser is `10.0.0.1/pkg.php?xml=freeradiusclients.xml`. The main title is "Package / FreeRADIUS: Clients / NAS / Clients". Below it, there is a navigation bar with tabs: Users, MACs, **NAS / Clients**, Interfaces, Settings, EAP, SQL, LDAP, View config, and XMLRPC Sync. The "NAS / Clients" tab is highlighted with a red box. A table below lists client configurations with columns: Client IP Address, Client IP Version, Client Shortname, Client Protocol, Client Type, Require Message Authenticator, Max Connections, and Description. A green "Add" button is at the top right of the table. At the bottom left is a "Save" button. The pfSense footer at the bottom states "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." The status bar at the bottom shows "Status: Running" and the date/time "23.12.2019 10:50".

We determine a private IP address. We must enter a “Shared Secret” here. It is crucial to remember this secret as it will be mandatory that we use the same string later.



This creates the client.

The screenshot shows the pfSense web interface on a ThinPC virtual machine. The URL in the browser is `10.0.0.1/pkg.php?xml=freeradiusclients.xml`. The page title is "Package / FreeRADIUS: Clients / NAS / Clients". The "NAS / Clients" tab is selected. A table lists a single client entry:

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
10.0.0.1	ipaddr	Misafir_Ag	udp	other	no	16	

Below the table is a green "Add" button with a plus sign. At the bottom left is a "Save" button. The pfSense footer indicates it is developed by Netgate, © ESF 2004 - 2019, and shows the license status as "View license". The system tray at the bottom right shows the date and time as 10:54, 23.12.2019, and various system icons.

20.1.2020

We now need to create some users to login to the portal.

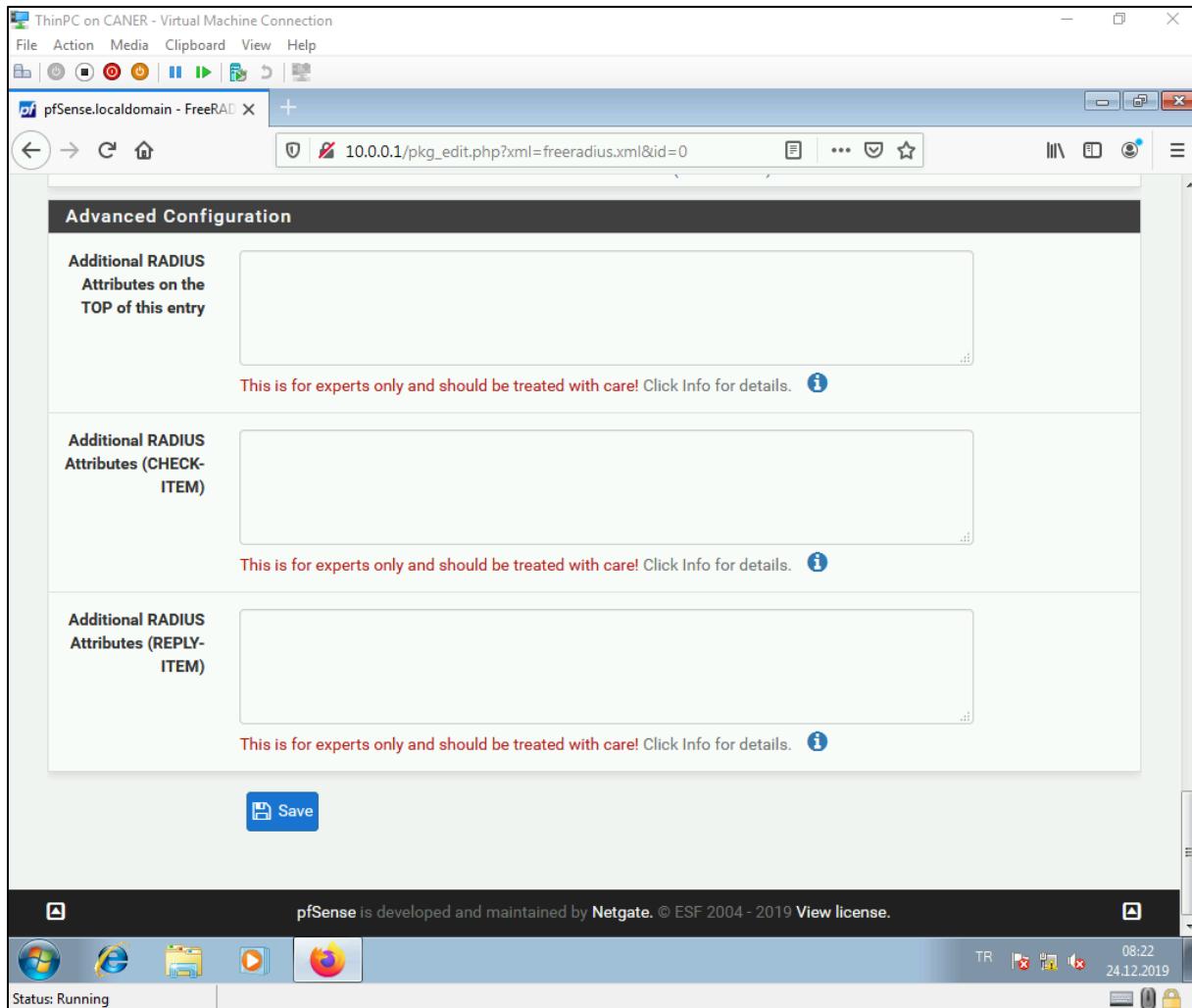
The screenshot shows the pfSense web interface for managing users. The browser title is "pfSense.localdomain - Package X". The URL in the address bar is "10.0.0.1/pkg.php?xml=freeradius.xml". The main navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu, the pfSense logo and "COMMUNITY EDITION" are displayed. The current page is "Package / FreeRADIUS: Users / Users". The "Users" tab is selected and highlighted with a red box. Other tabs include MACs, NAS / Clients, Interfaces, Settings, EAP, SQL, LDAP, View config, and XMLRPC Sync. A filter bar at the top allows filtering by Username, with a dropdown for "Filter field" set to "Username" and a "Filter" button. Below the filter is a table header with columns: Username, Password, Use One Time, Simult. Connections, IP Address, Expiration Date, Session Timeout, Possible Login Times, VLAN ID, and Description. The "Add" button in the bottom right corner of the table area is also highlighted with a red box. A "Save" button is located below the table. At the bottom of the page, a footer states "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." The system status bar at the bottom shows "Status: Running" and various system icons.

We give them usernames and passwords.

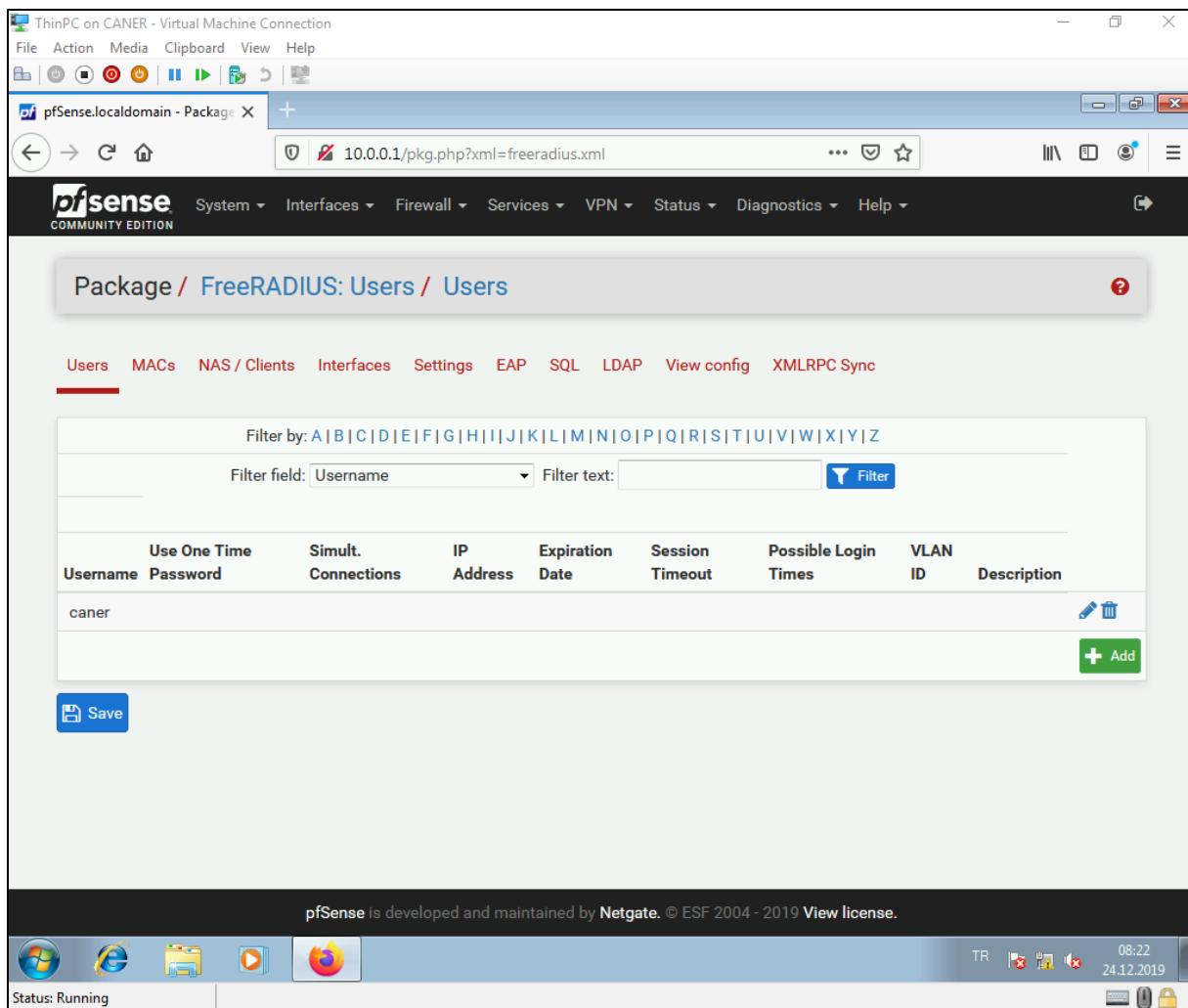
The screenshot shows a web browser window titled "pfSense.localdomain - FreeRAD X" with the URL "10.0.0.1/pkg_edit.php?xml=freeradius.xml&id=0". The page is titled "FreeRADIUS: Users / Edit / Users" and displays a "General Configuration" section. In the "Username" field, "caner" is entered. Below it, a note says "Enter the username. Whitespace is allowed. Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP." In the "Password" field, a masked password is shown. Below it, a note says "Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password." Under "Password Encryption", "Cleartext-Password" is selected. A "One-Time Password Configuration" section follows, containing a checkbox for enabling OTP. A note states: "This enables the possibility to authenticate with username and one-time-password. The client used to generate OTP can be installed on various mobile device platforms like Android, iOS and others. (Default: unchecked)" and "IMPORTANT: For MOTP, mOTP must be enabled at FreeRADIUS > Settings. The RADIUS NAS / Client must use PAP otherwise the authenticator script cannot use the authentication data." The bottom status bar shows "Status: Running" and system icons.

20.1.2020

We do not change of the settings.



And, now we have a new user.



20.1.2020

We now need to get to the User Manager.

The screenshot shows the pfSense web interface on a ThinPC virtual machine. The URL in the address bar is `10.0.0.1/pkg.php?xml=freeradius.xml`. The main menu is visible at the top, and the left sidebar shows 'Package /' with 'Users' selected. The main content area is titled 'Users / Users' and displays a table of users. A red box highlights the 'User Manager' link in the 'Actions' column of the table. The table columns are: Username, Password, Actions, IP Address, Expiration Date, Session Timeout, Possible Login Times, VLAN ID, and Description. At the bottom of the table, there are 'Save' and 'Add' buttons. The status bar at the bottom shows 'Status: Running' and the date '24.12.2019'.

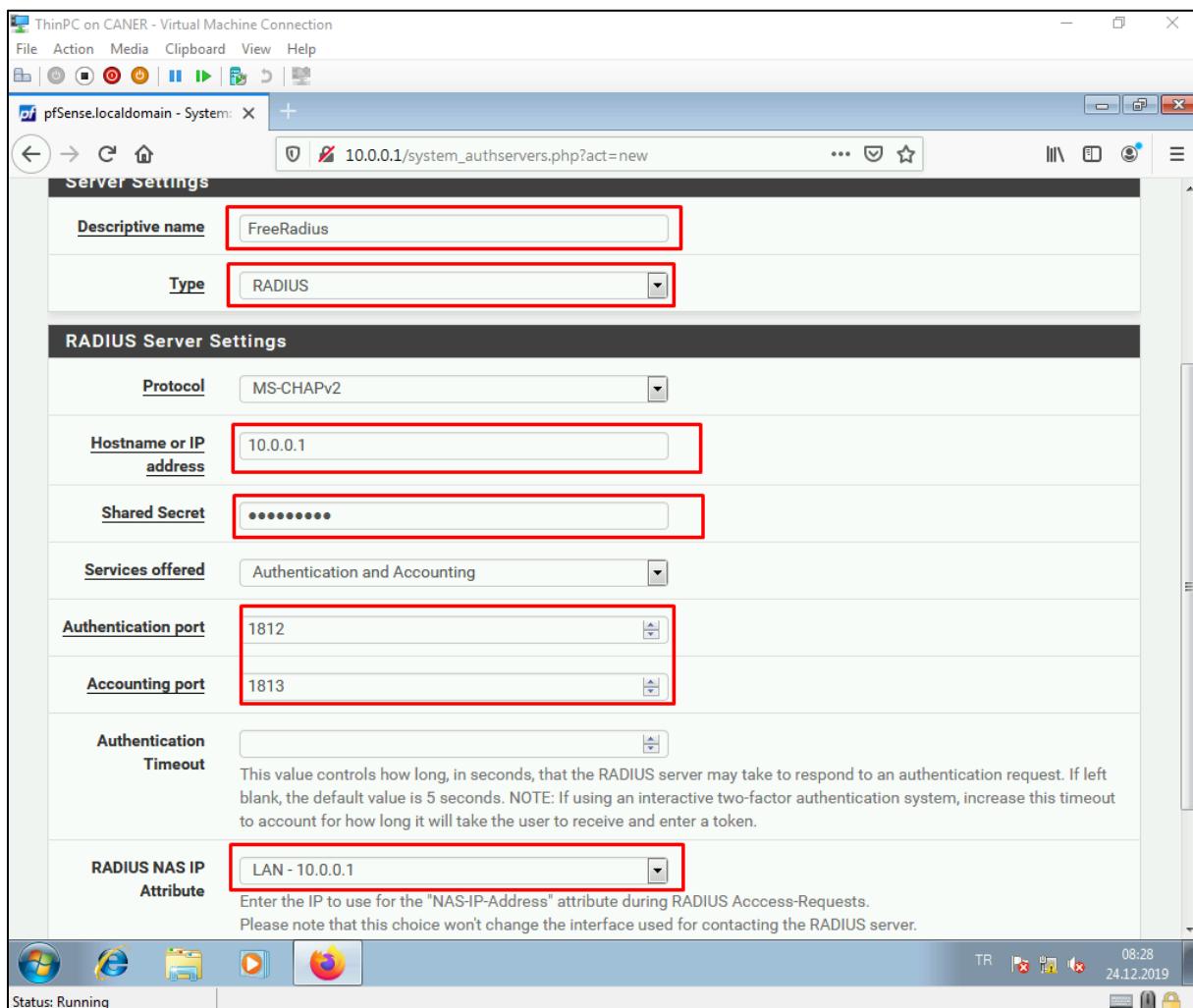
We select the Authentication Servers tab and create a new one.

The screenshot shows a web browser window titled "pfSense.localdomain - System" with the URL "10.0.0.1/system_authservers.php". The browser has a standard toolbar with icons for file operations, navigation, and search. The pfSense navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the breadcrumb trail reads "System / User Manager / Authentication Servers". A red box highlights the "Authentication Servers" tab in the top navigation menu, which is currently active. The main content area displays a table titled "Authentication Servers" with the following data:

Server Name	Type	Host Name	Actions
Local Database		pfSense	Edit

A green "Add" button with a plus sign is located at the bottom right of the table. At the bottom of the page, there is a footer bar with icons for various services and a status message "Status: Running". The footer also includes copyright information: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." and system details like "08:23 24.12.2019".

We create it with specific details that we have set up previously. The type is Radius. The ports are 1812 and 1813 and hostname IP is the NAS client IP address. Finally, the secret is the same “Shared Secret” that we used in NAS client. All of these are very important to set the same; otherwise, the portal wouldn’t work and the internet access would be crippled.



Once we save, we have the new Authentication Server.

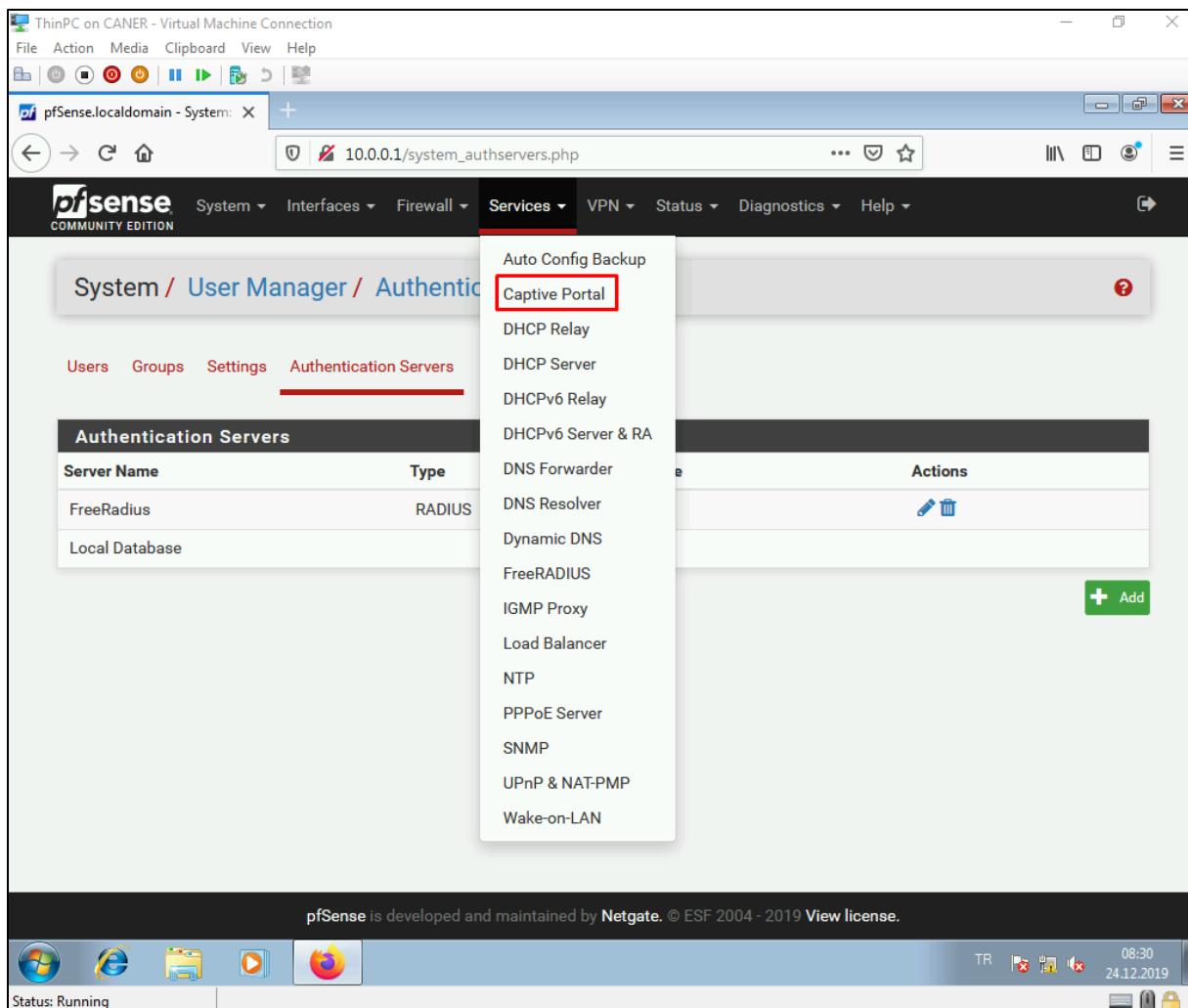
The screenshot shows the pfSense User Manager / Authentication Servers page. The page title is "System / User Manager / Authentication Servers". Below the title, there are tabs for "Users", "Groups", "Settings", and "Authentication Servers", with "Authentication Servers" being the active tab. A table titled "Authentication Servers" lists two entries:

Server Name	Type	Host Name	Actions
FreeRadius	RADIUS	10.0.0.1	
Local Database		pfSense	

At the bottom right of the table, there is a green "Add" button with a plus sign. The pfSense footer includes the text "pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license." and a status bar showing "Status: Running" and system icons.

20.1.2020

Now, we need to get to the Captive Portal again to start the authentication process.



We edit the previously created portal zone.

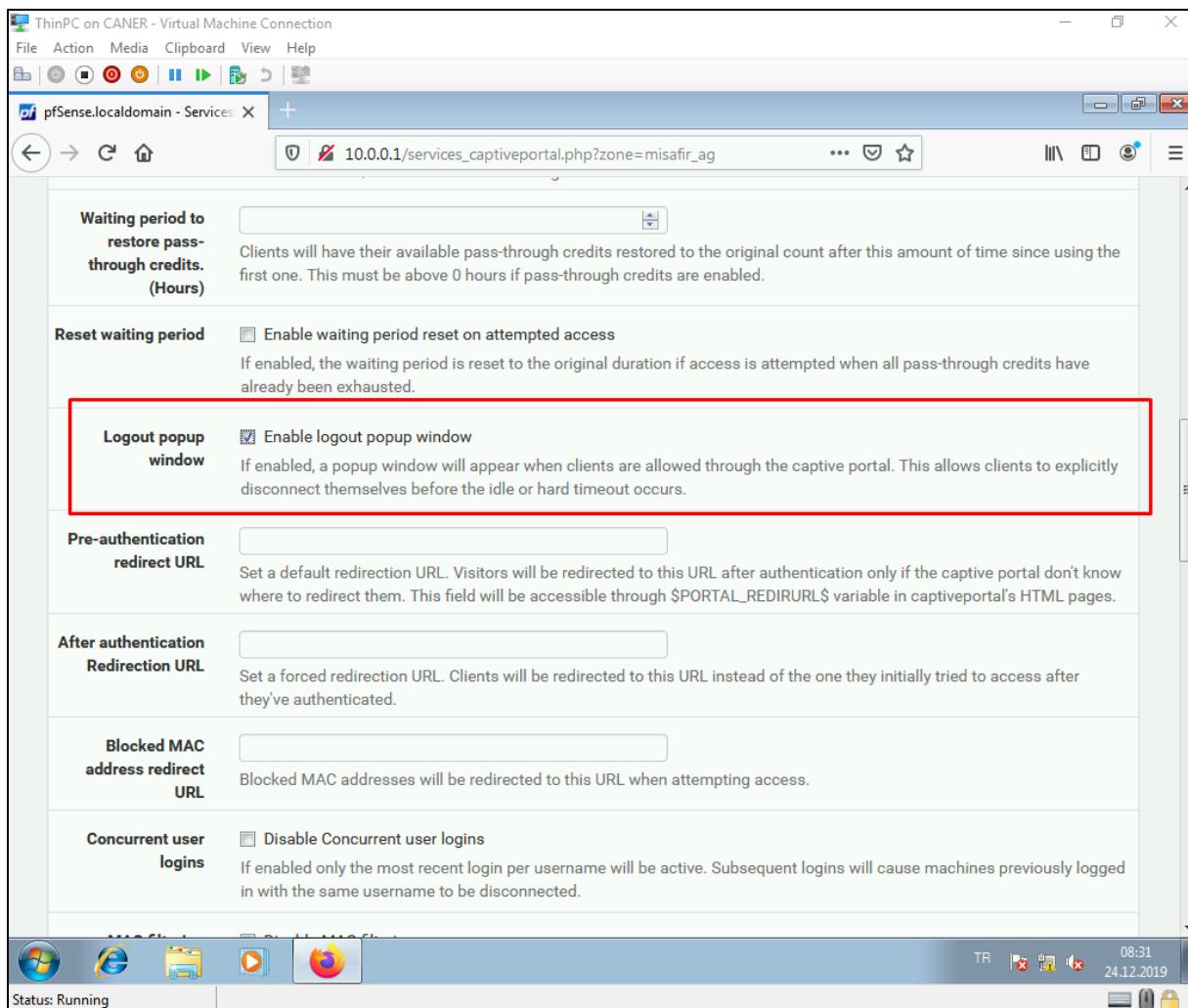
The screenshot shows a pfSense web interface titled "Services / Captive Portal". The "Captive Portal Zones" table lists one zone:

Zone	Interfaces	Number of users	Description	Actions
misafir_ag	LAN	1	Misafir Ağ Kullanıcıları	

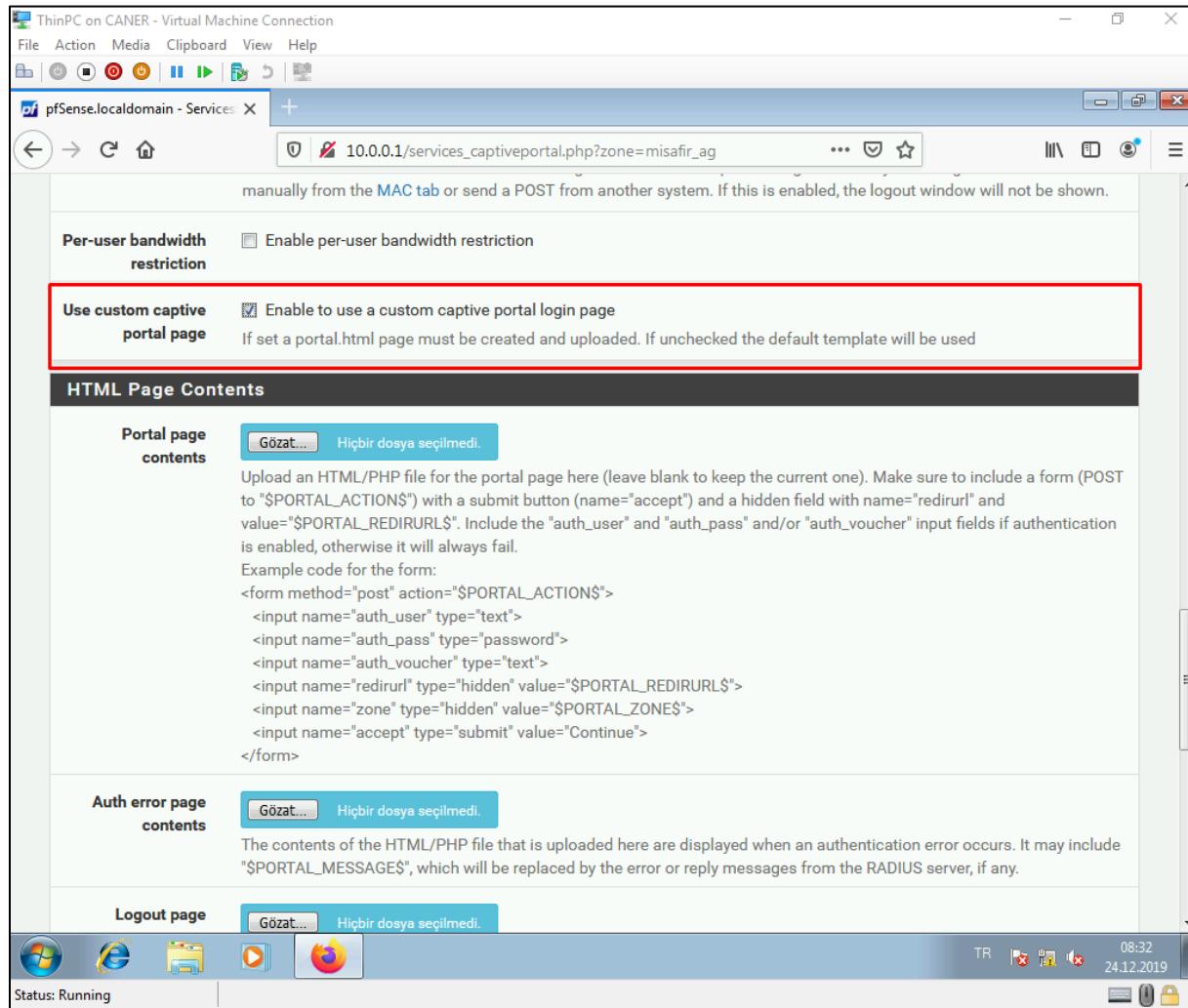
A red box highlights the edit icon (pencil) in the "Actions" column for the "misafir_ag" row. The browser address bar shows "10.0.0.1/services_captiveportal_zones.php". The pfSense navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The bottom status bar shows "Status: Running", network information "Network 3 No Internet access", and a date/time stamp "24.12.2019 08:30".

20.1.2020

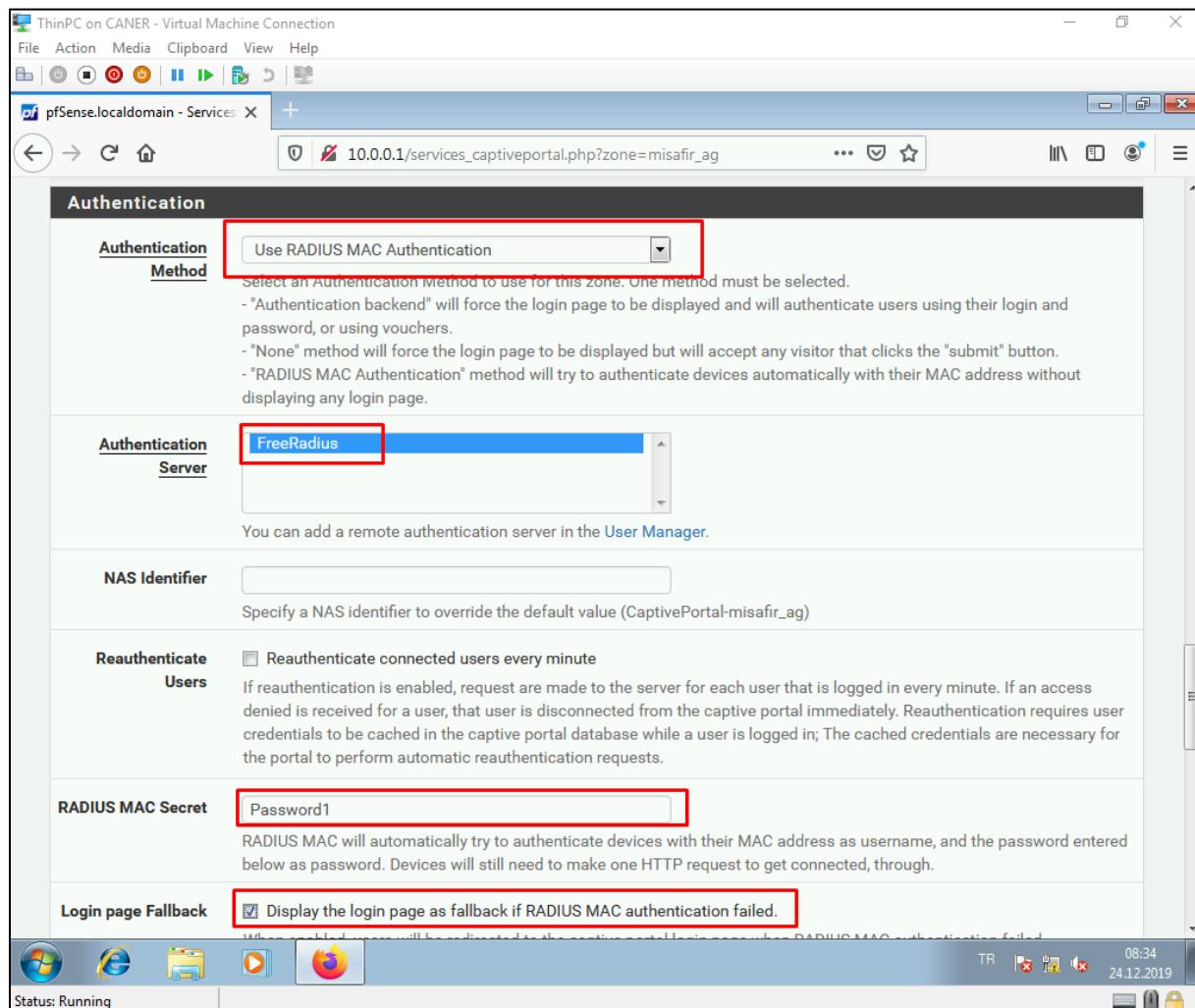
We enable the logout popup window.



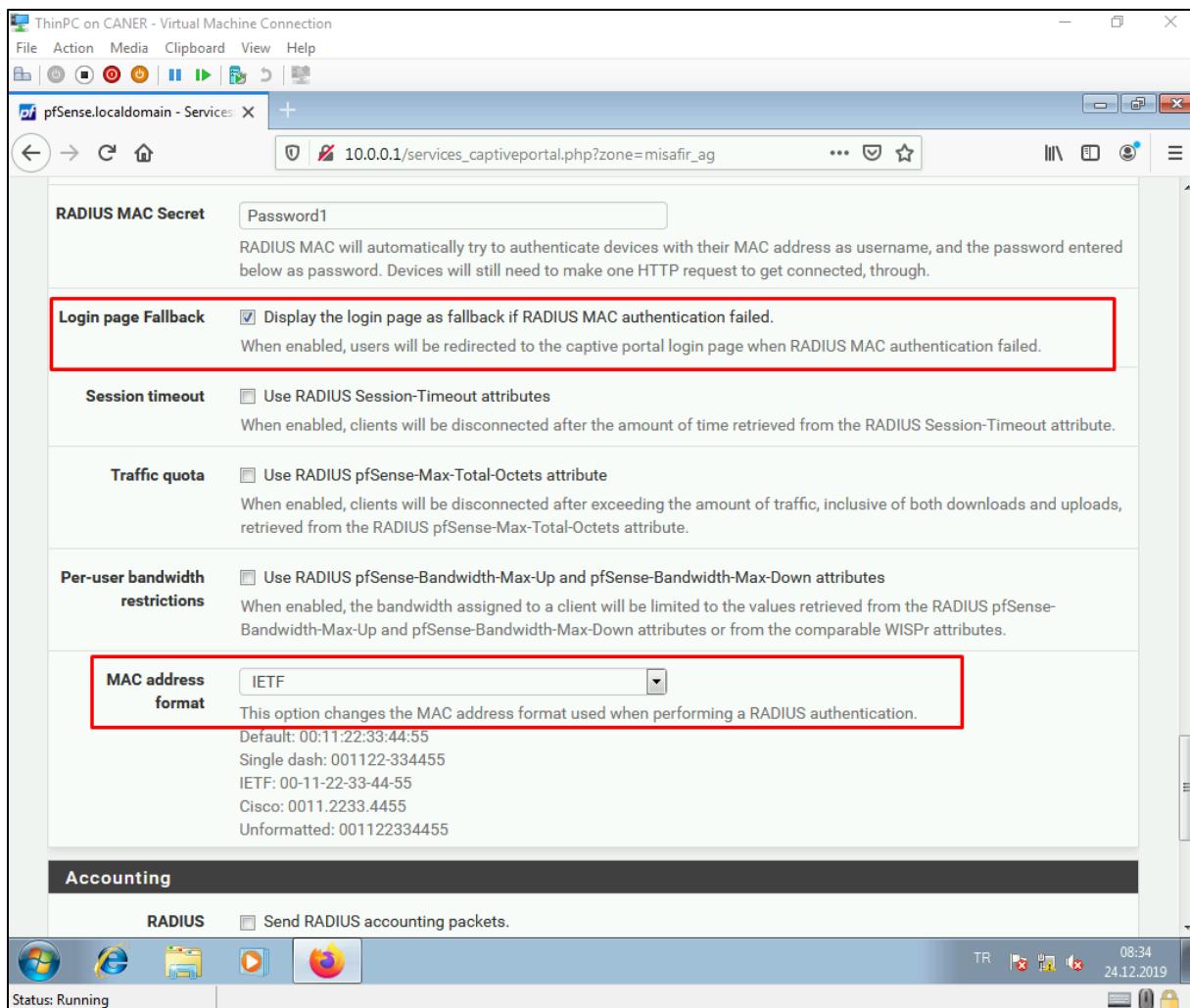
We can enable the custom captive portal login page to design it as we like. We use the default one but this changes nothing in the security of the portal.



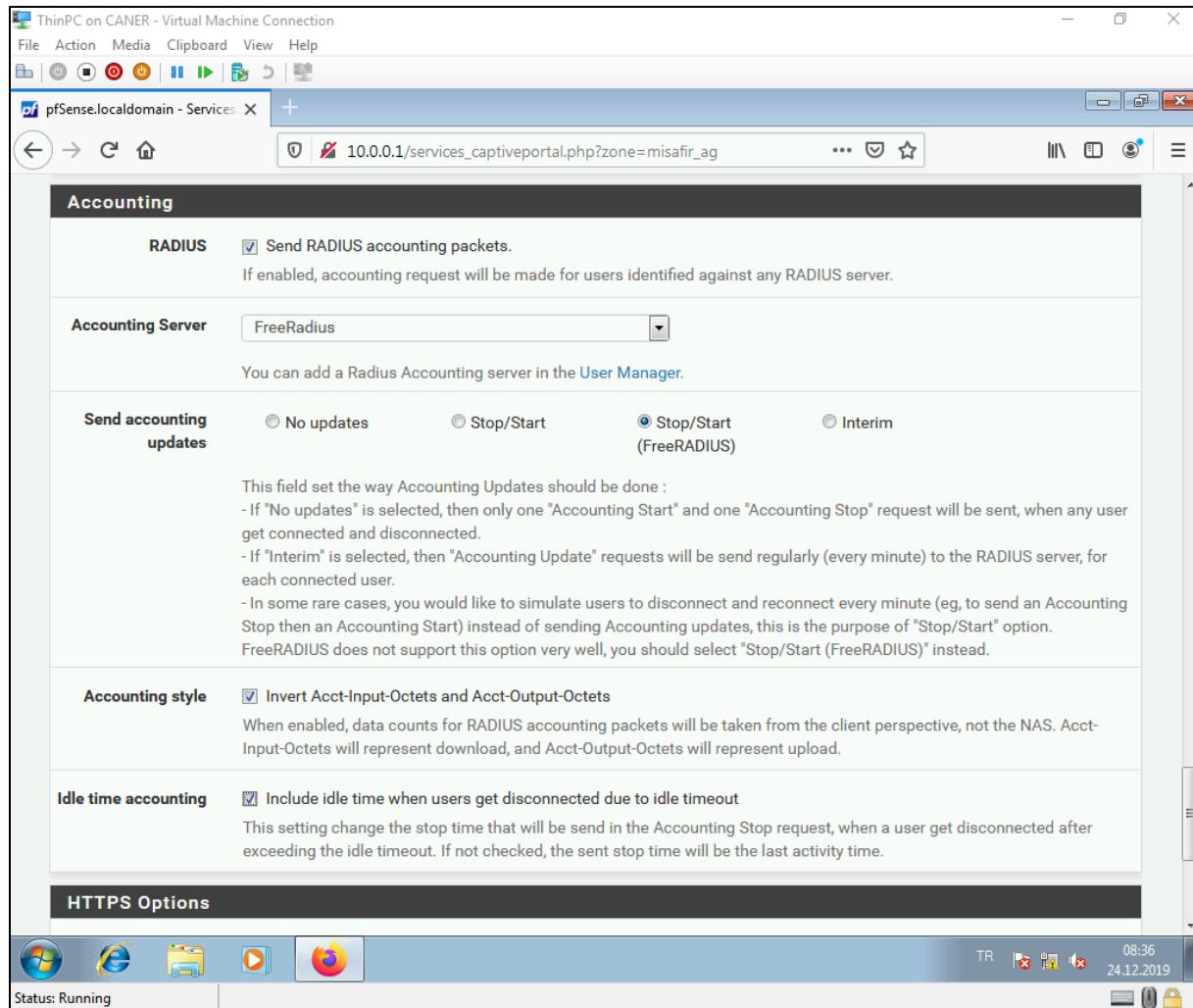
We choose the Radius MAC Authentication and choose our previously created Authentication Server. We enter the same secret.



We select the following options as well.

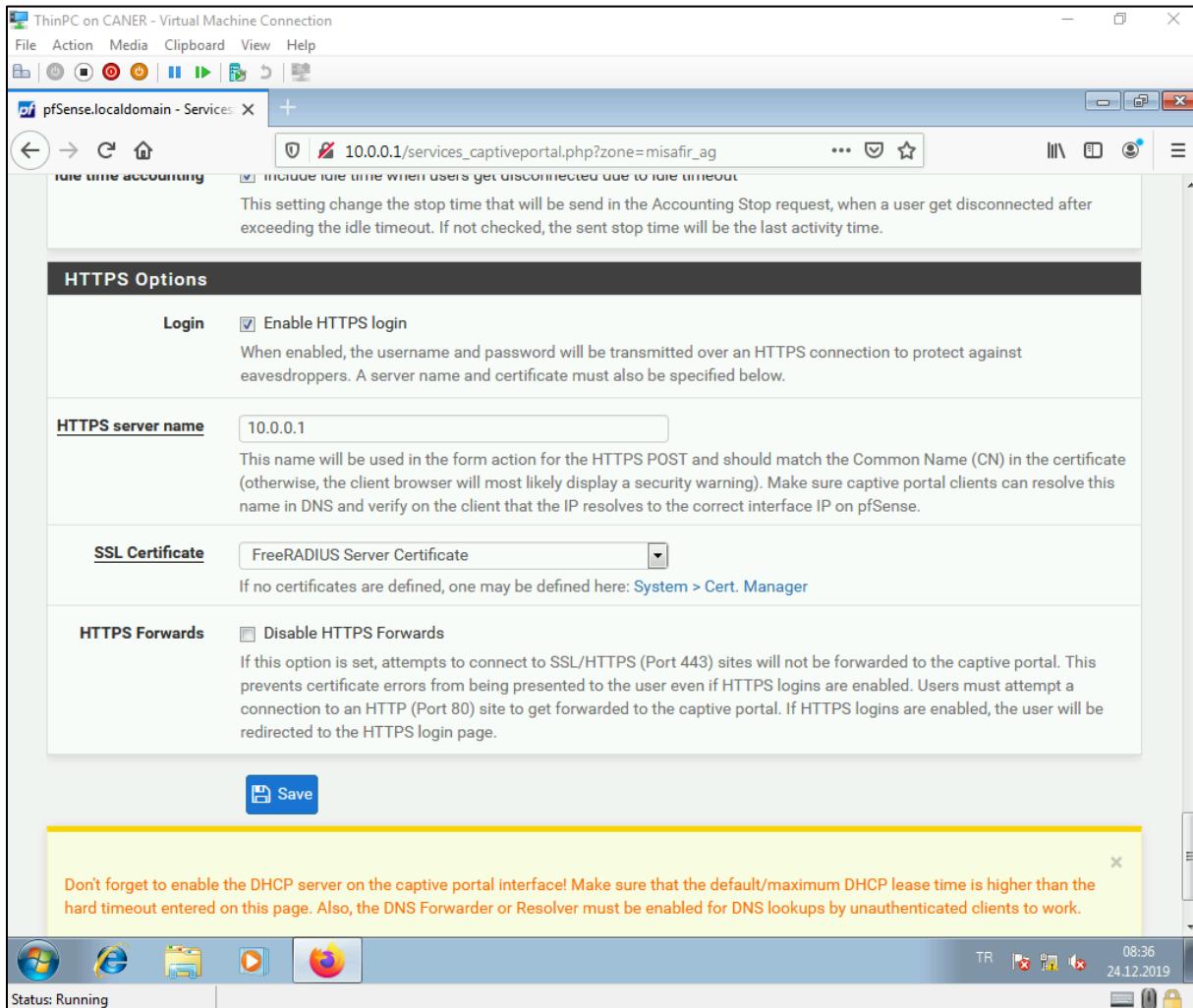


We set it up to send Radius accounting packets with the following specifications.

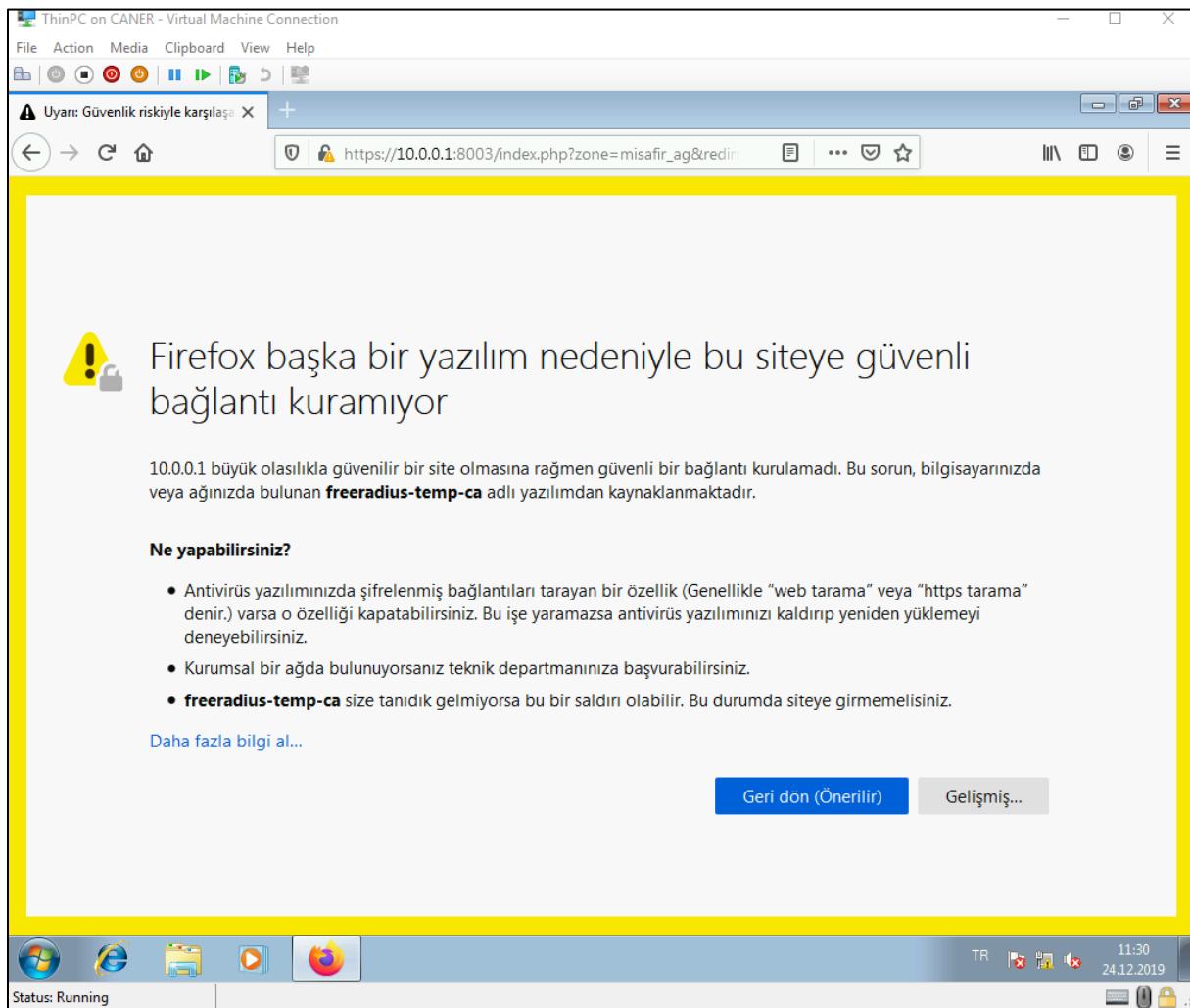


And, finally we enable HTTPS login with our NAS client's IP and FreeRADIUS Server

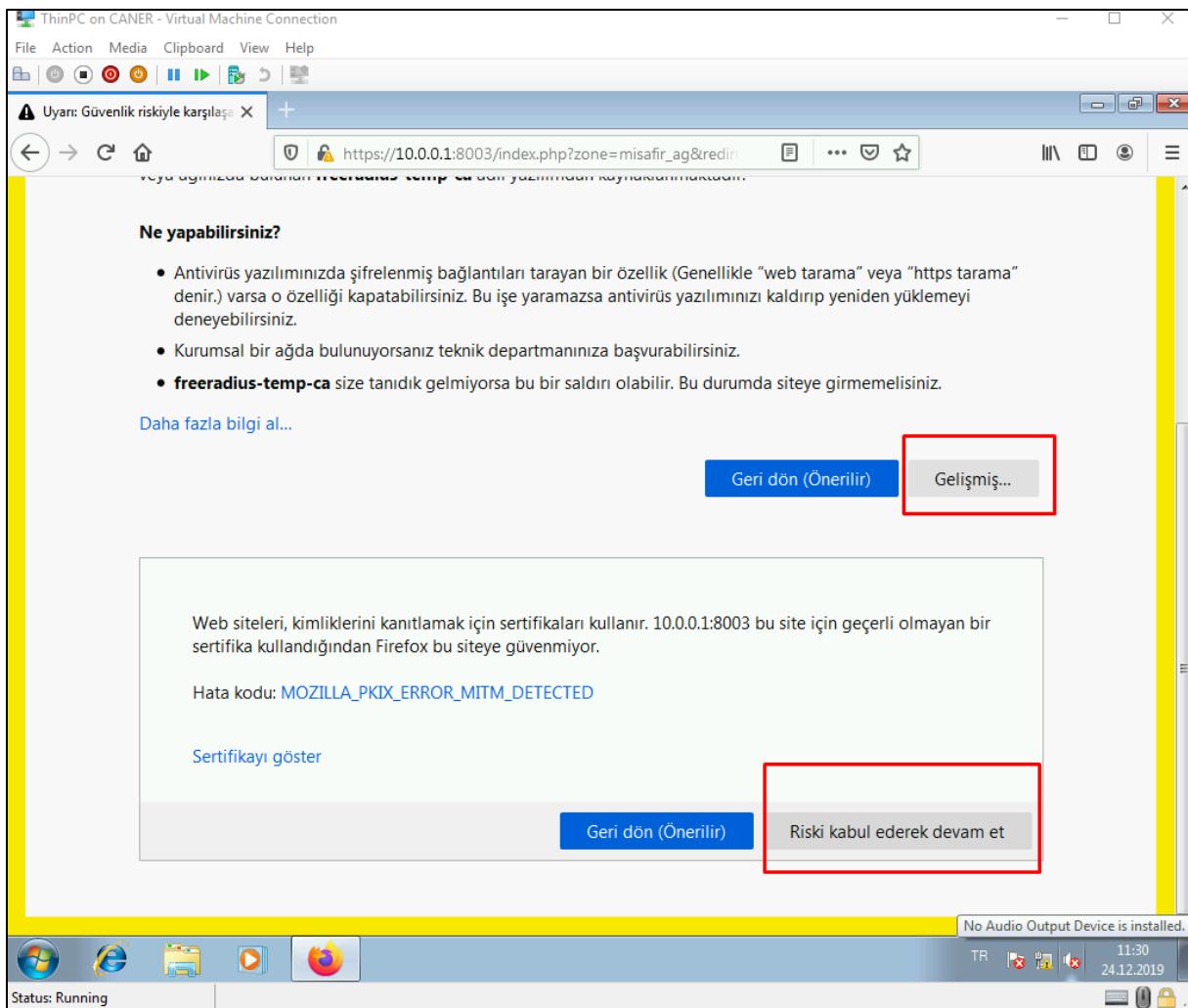
Certificate for SSL. Once we save, our portal is working.



When we start the web browser and attempt to go anywhere, like perhaps youtube.com we are redirected to this page.

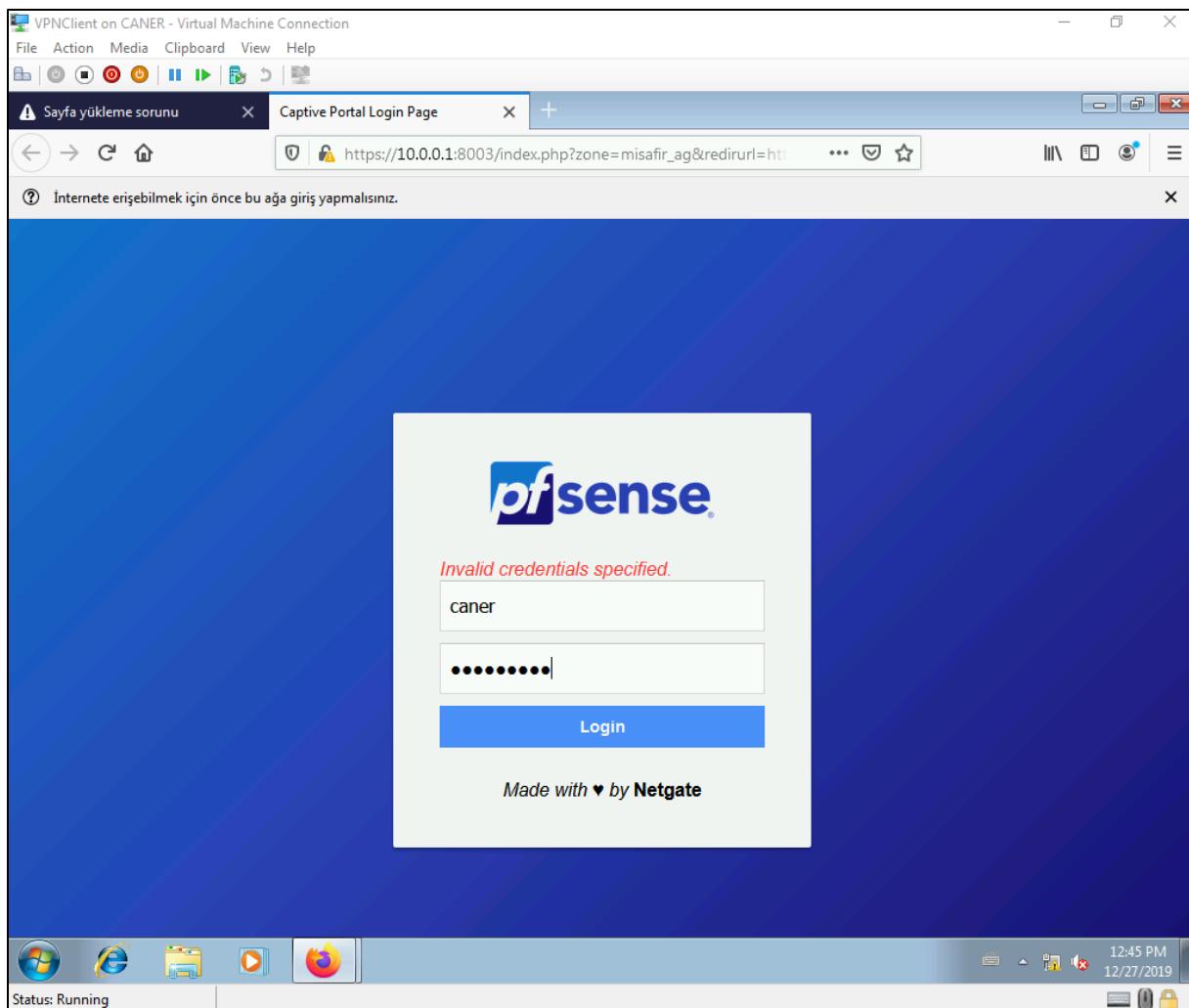


From the advanced settings option we select to proceed with accepting the risks.



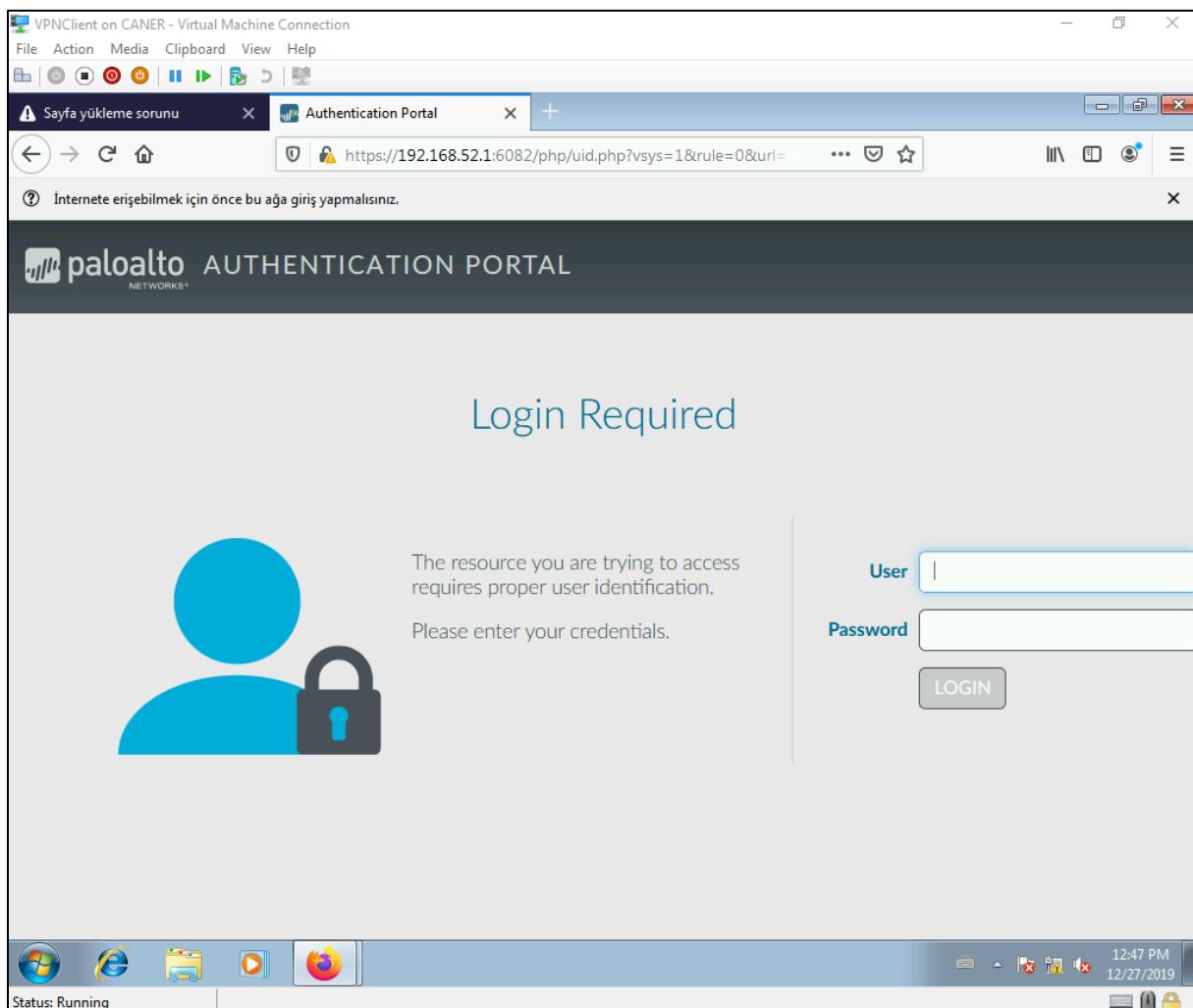
20.1.2020

And we find ourselves at the default Captive Portal page.



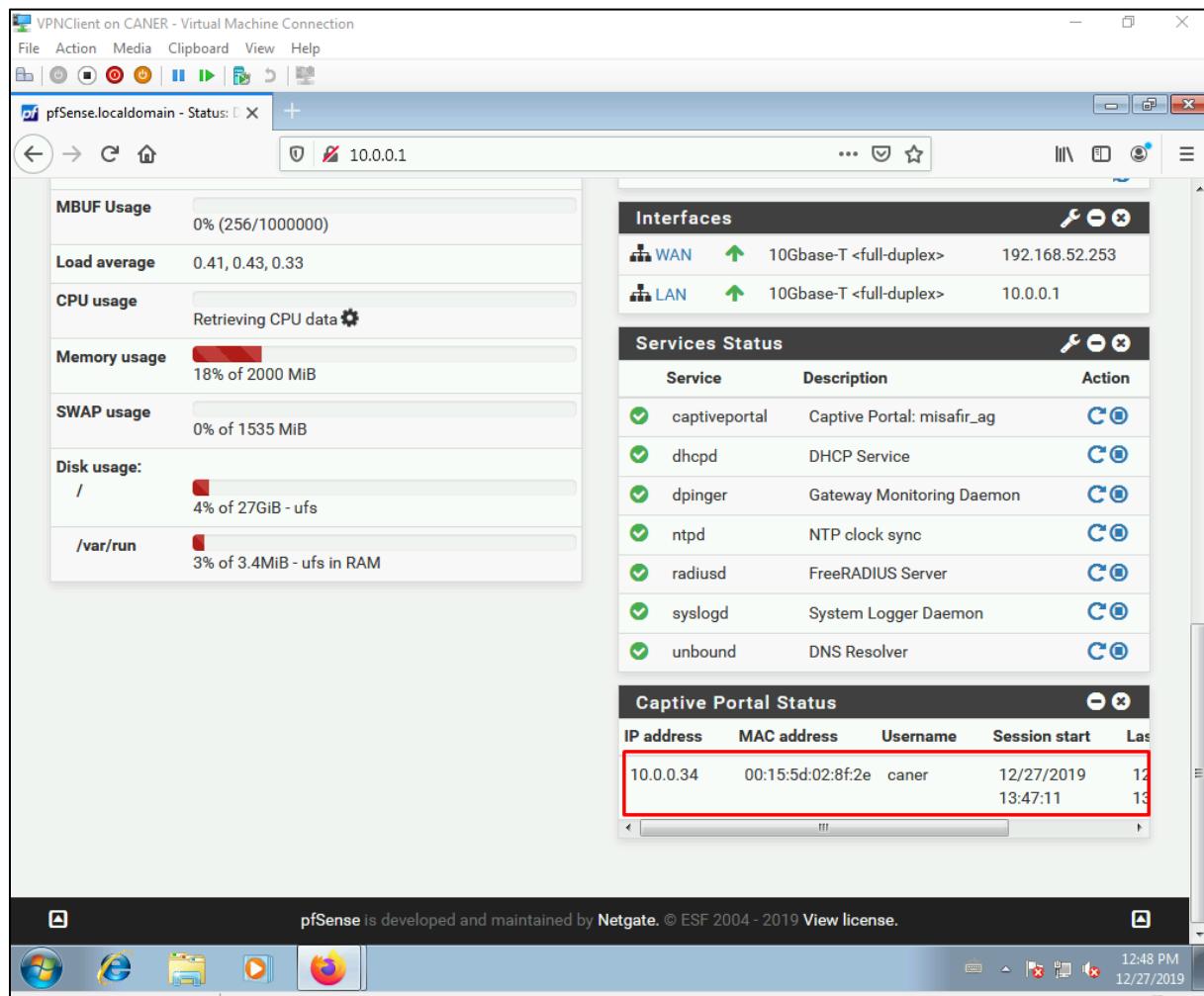
After we login using the previously set password...

... we find ourselves at another Captive Portal. The one BAU uses for its own internal network but this means we basically accessed to the WAN interface of the firewall and reached the internet. To get to the actual youtube.com page we'd have to login to this portal as well but this is completely irrelevant.

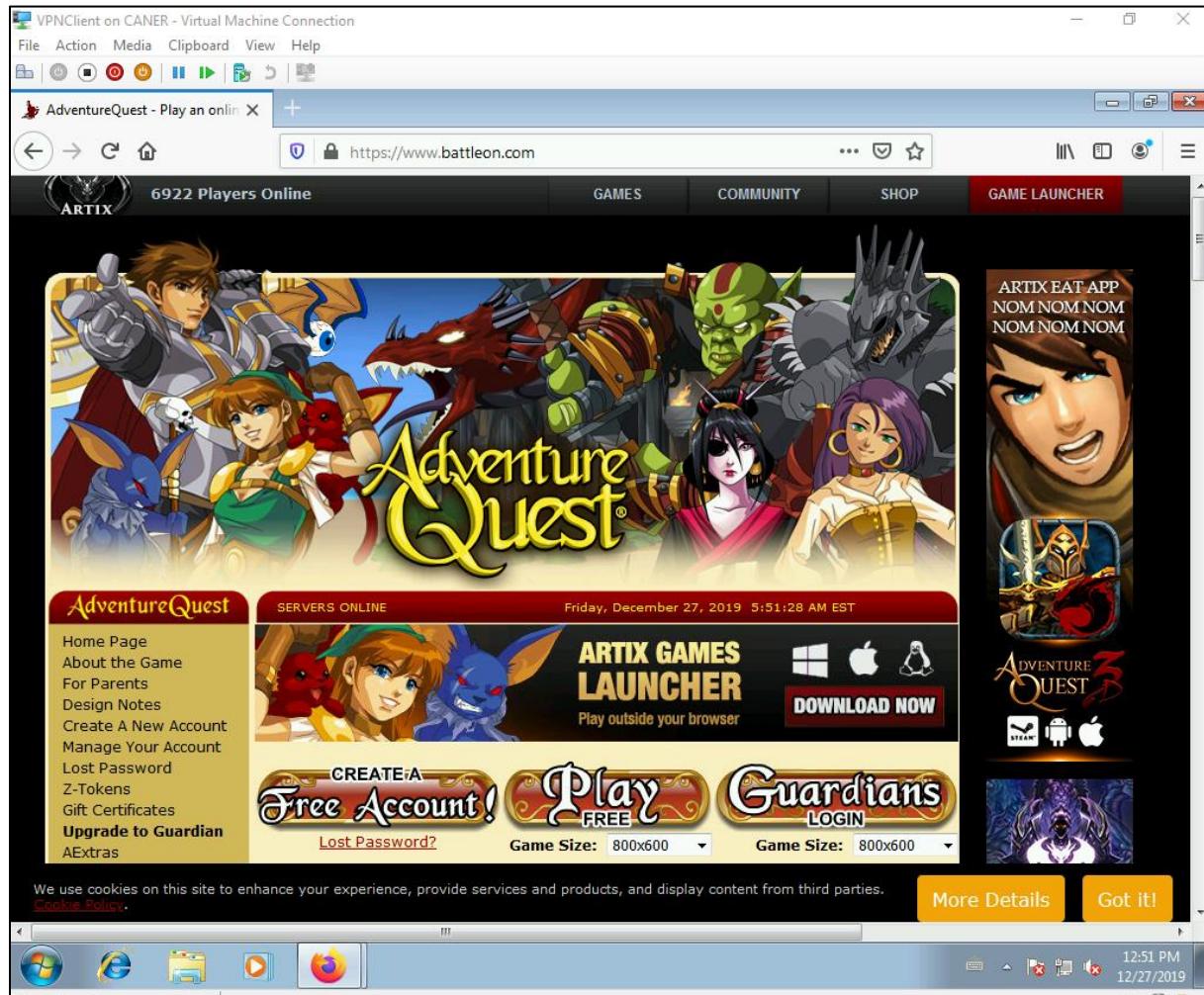


20.1.2020

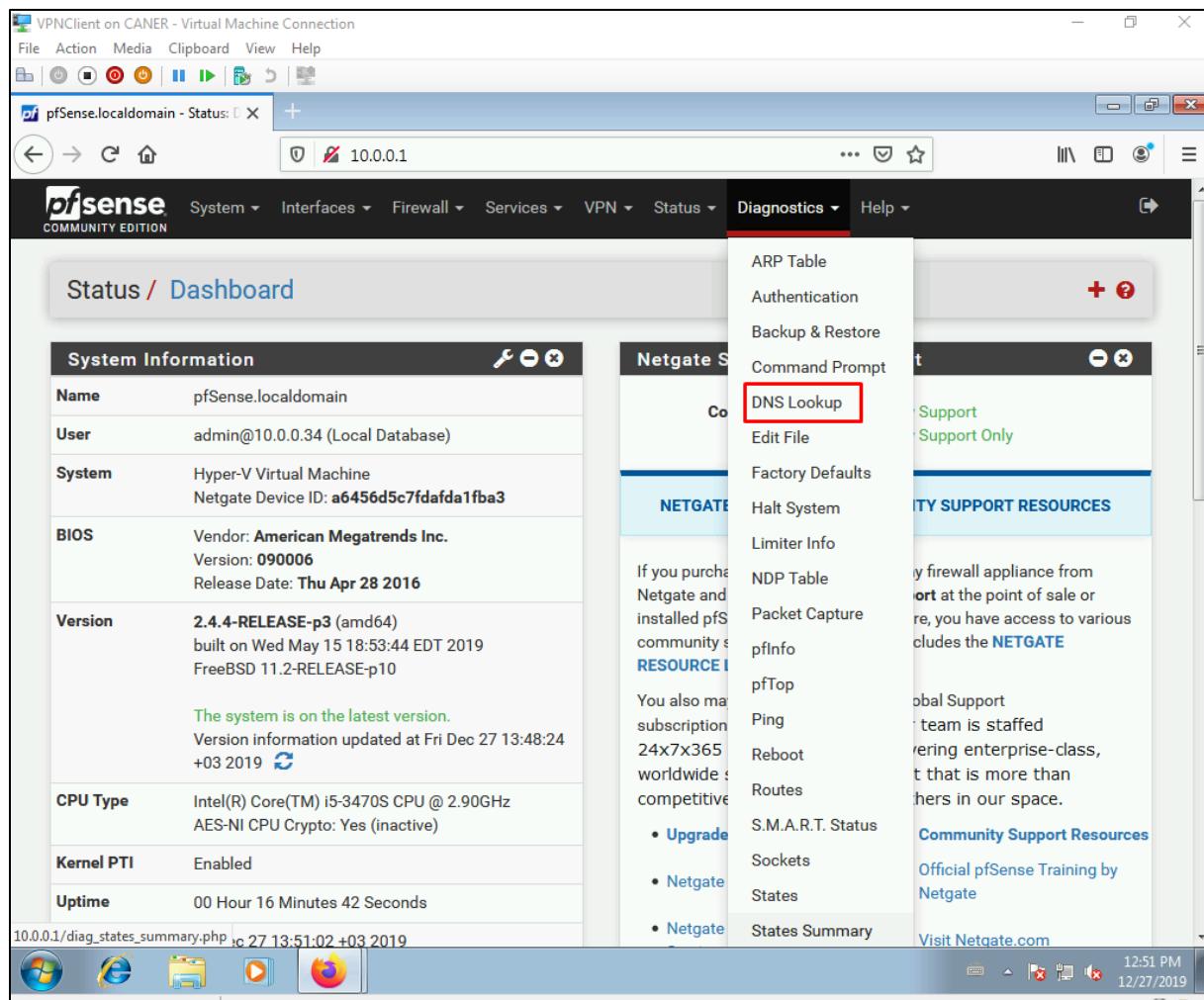
When we look at the Captive Portal Status from the pfSense dashboard we can see the information of our user logging in.



Now, let's ban access to a specific website for our users. We decide to ban this online based game website so that our employees cannot play while at work.



We first need to get to the DNS Lookup under Diagnostics.



With the DNS Lookup we get the IP addresses of the website. Fortunately, it's not Facebook and it only has 2 IP addresses.

The screenshot shows the pfSense Diagnostics / DNS Lookup interface. In the 'Hostname' field, 'battleon.com' is entered. The 'Lookup' button is highlighted with a red box. The 'Results' section displays two entries:

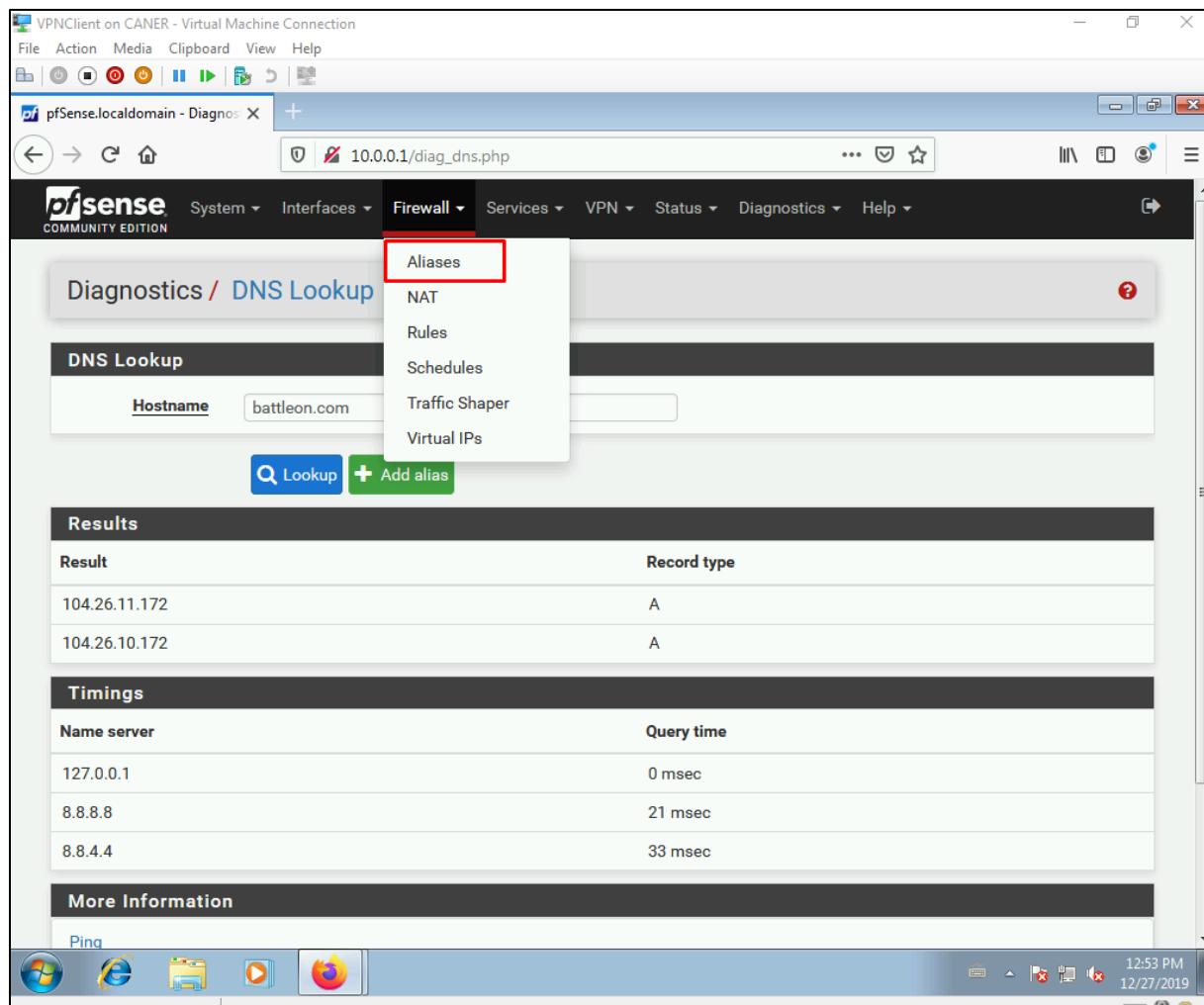
Result	Record type
104.26.11.172	A
104.26.10.172	A

The 'Timings' section shows query times for different name servers:

Name server	Query time
127.0.0.1	0 msec
8.8.8.8	21 msec
8.8.4.4	33 msec

20.1.2020

We go to Aliases under Firewall to create an alias.

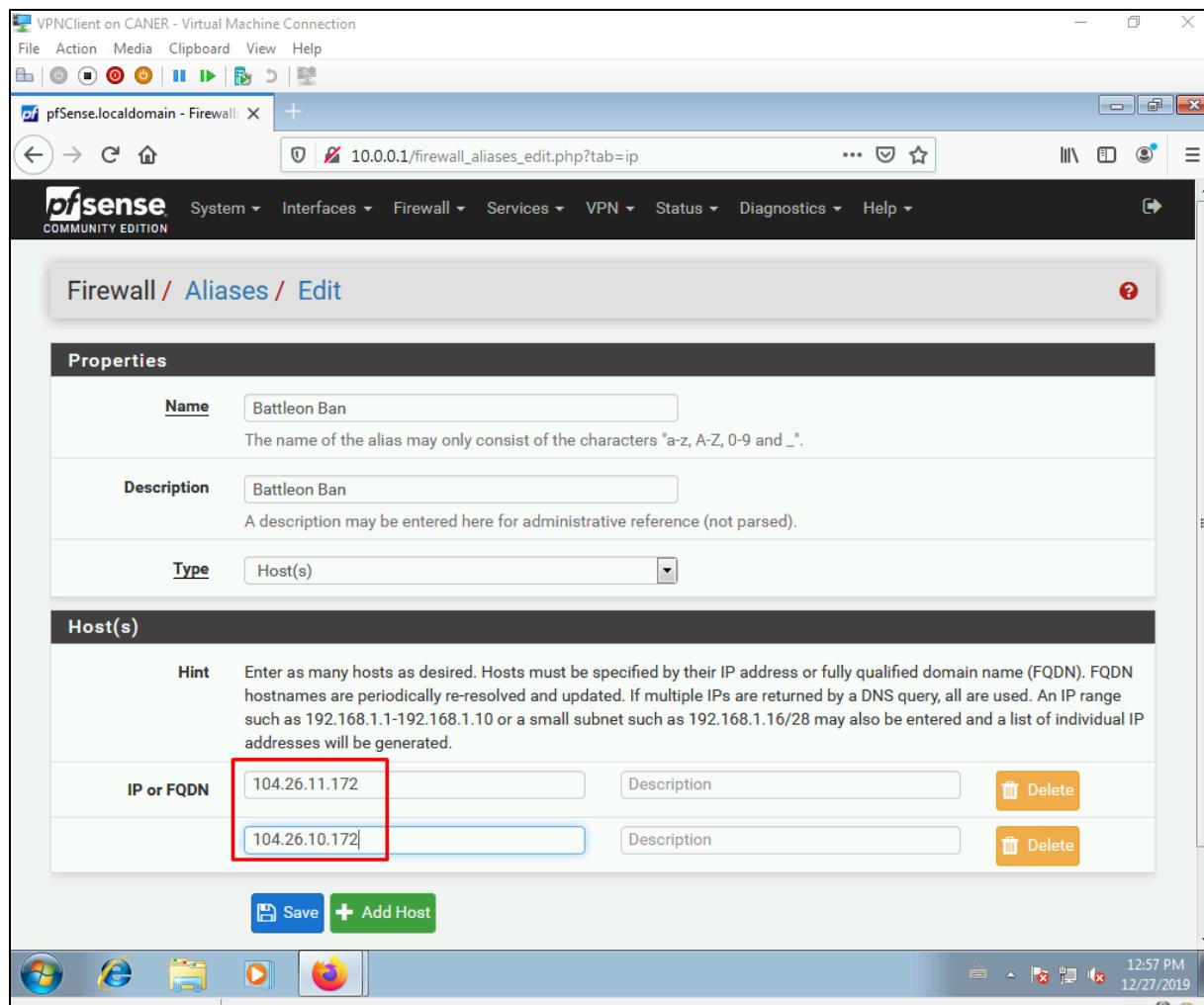


We create an alias for IPs.

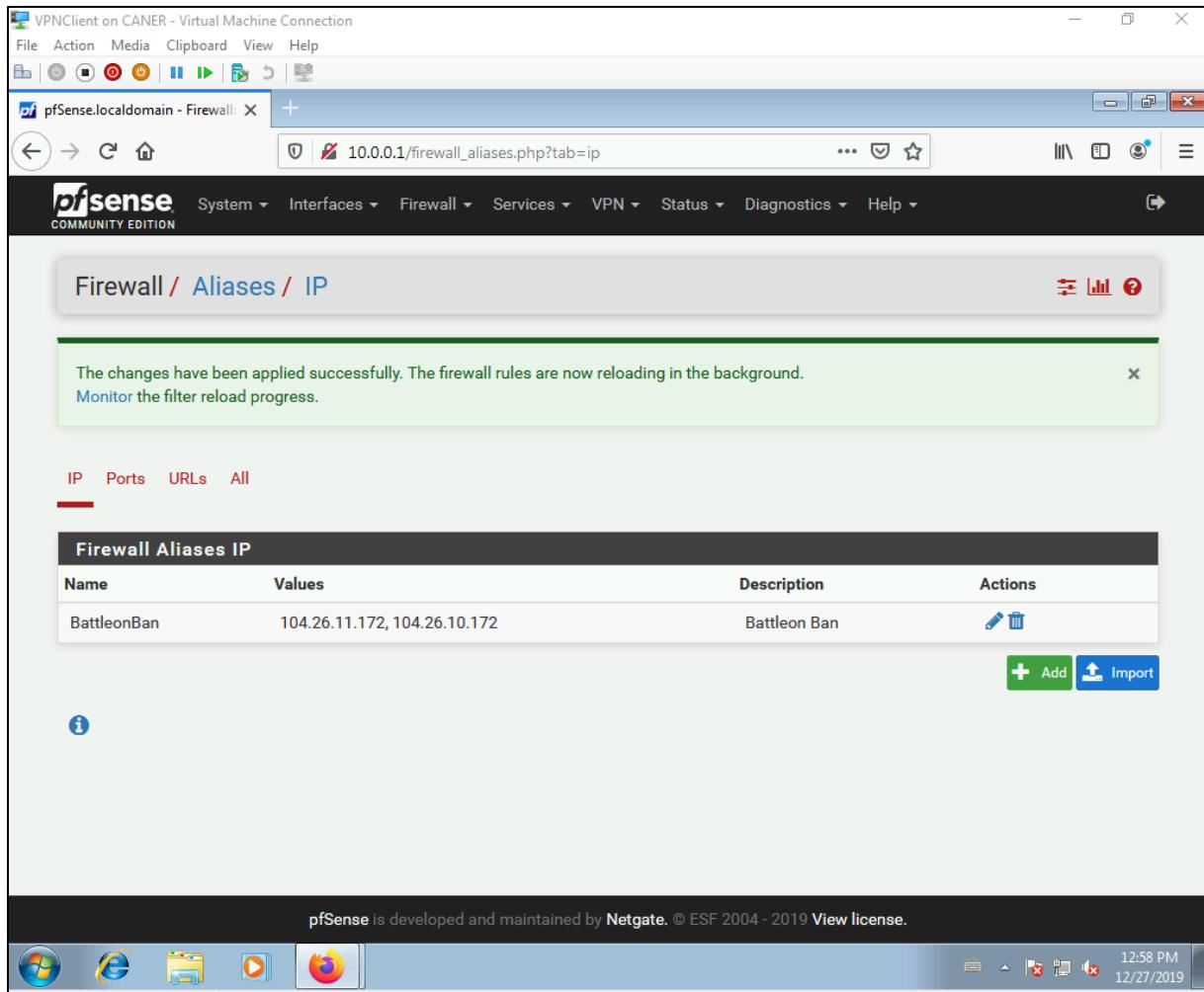
The screenshot shows the pfSense Firewall Aliases IP configuration page. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the title is "Firewall / Aliases / IP". There are tabs for IP, Ports, URLs, and All, with IP selected. A table titled "Firewall Aliases IP" lists columns for Name, Values, Description, and Actions. In the Actions column, there is a green "Add" button with a red box drawn around it, and a blue "Import" button. At the bottom of the page, there is a footer with the pfSense license information and the date Friday, December 27, 2019.

20.1.2020

We name the alias and enter the website's IP addresses here.



Once we save, we have an alias neatly named as BattleOnBan.



20.1.2020

Now, we get to the Rules under Firewall.

The screenshot shows the pfSense Firewall / Aliases / IP interface. The 'Rules' option in the sidebar is highlighted with a red box. A table lists a single rule named 'BattleonBan' with values '104.26.11.172, 104.26.10.172'. The table has columns for Name, Values, Description, and Actions. The Actions column contains edit and delete icons. Below the table are 'Add' and 'Import' buttons. The pfSense logo and copyright information are visible at the bottom.

Name	Values	Description	Actions
BattleonBan	104.26.11.172, 104.26.10.172	Battleon Ban	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

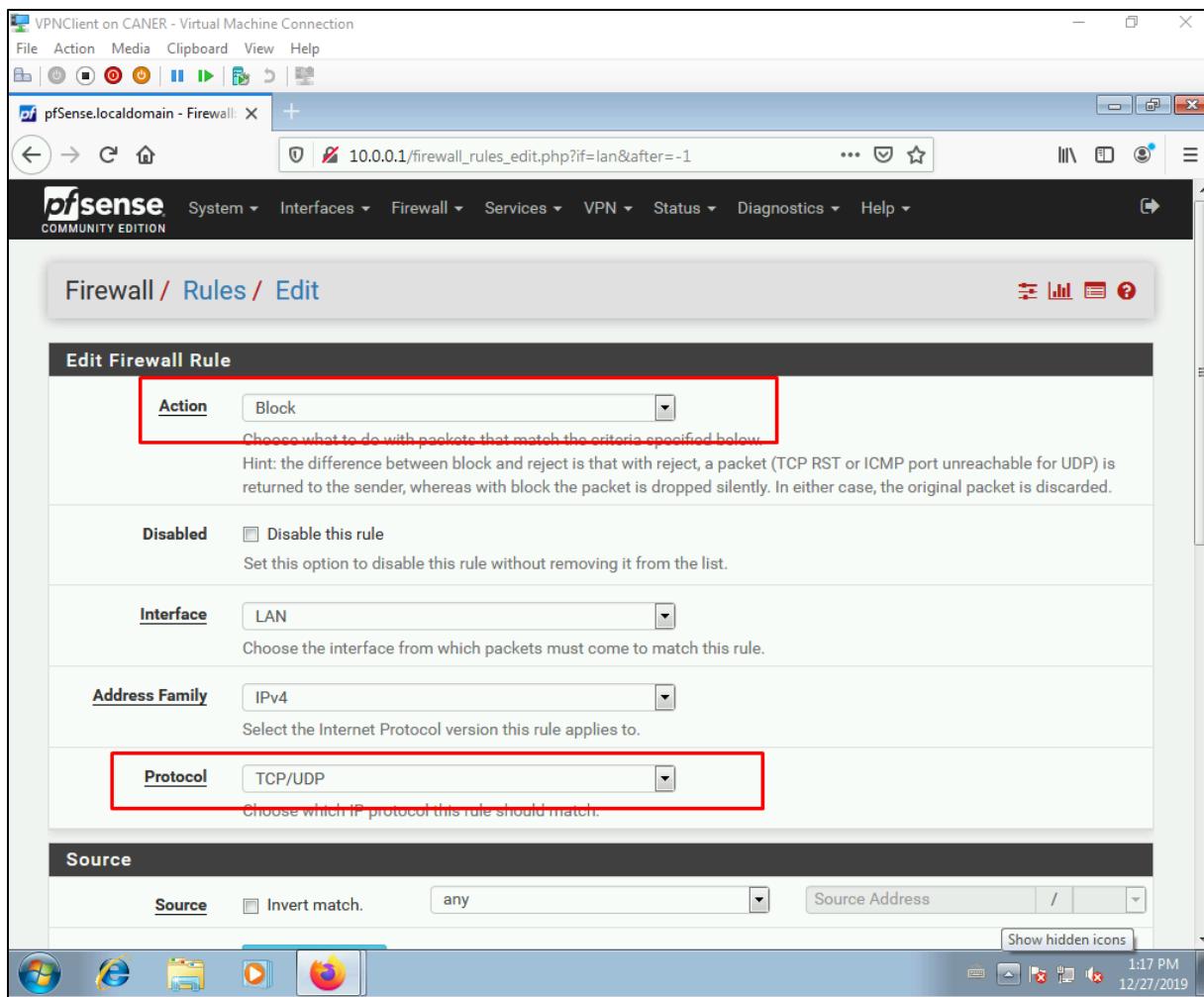
We create a new rule.

The screenshot shows the pfSense Firewall Rules LAN page. The 'LAN' tab is selected. A table lists existing rules:

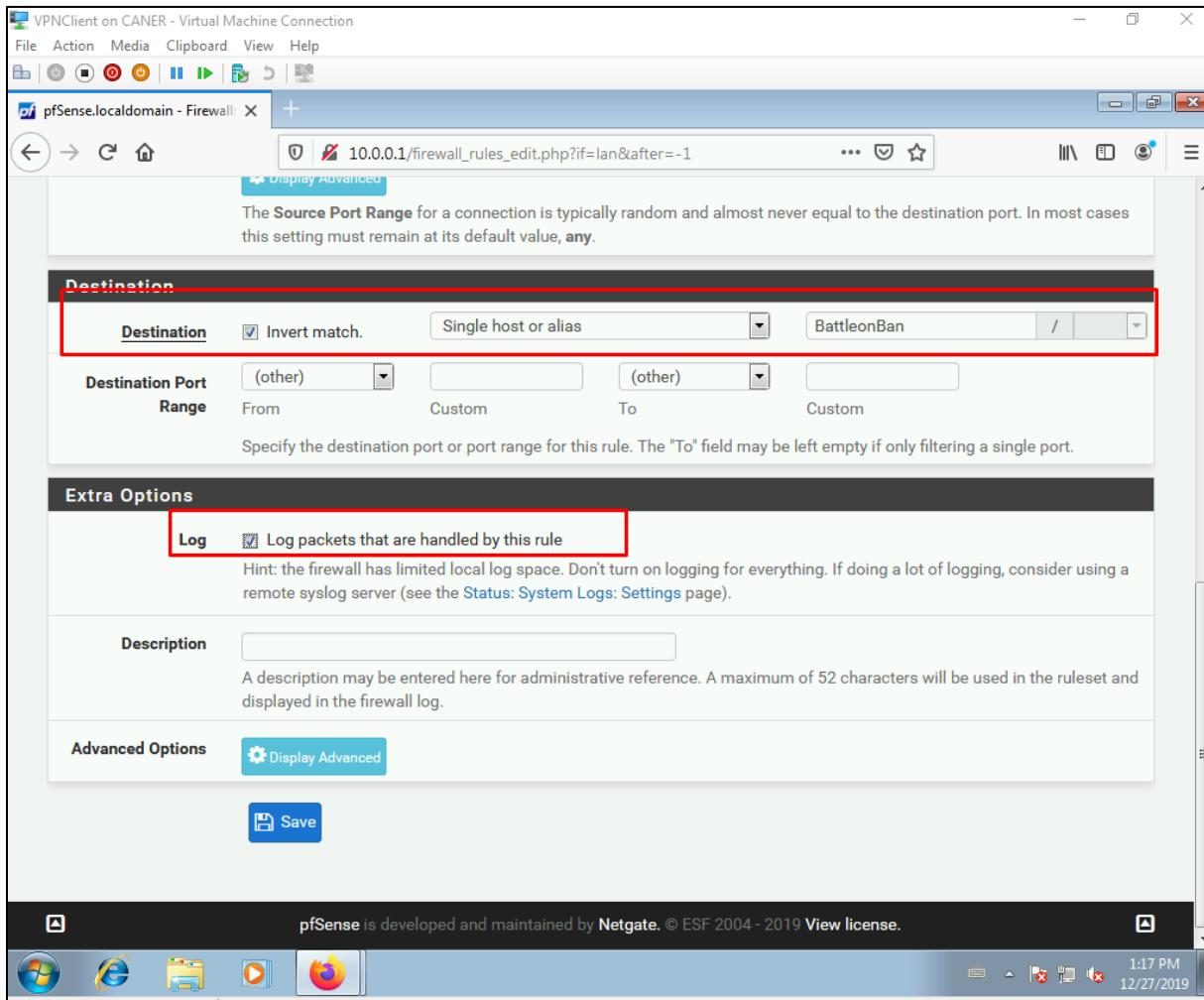
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 /217 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 16 /2.33 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

A green 'Add' button is located at the bottom right of the table, with a red box drawn around it. Below the table, there is a status bar with icons and the text 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.'

We choose to block, both TCP and UDP protocols from any source...



... to BattleOn.com's IP addresses as displayed by the alias.



We also take a log of anyone attempting to log into the banned website so that we can reprimand those employees if necessary.

20.1.2020

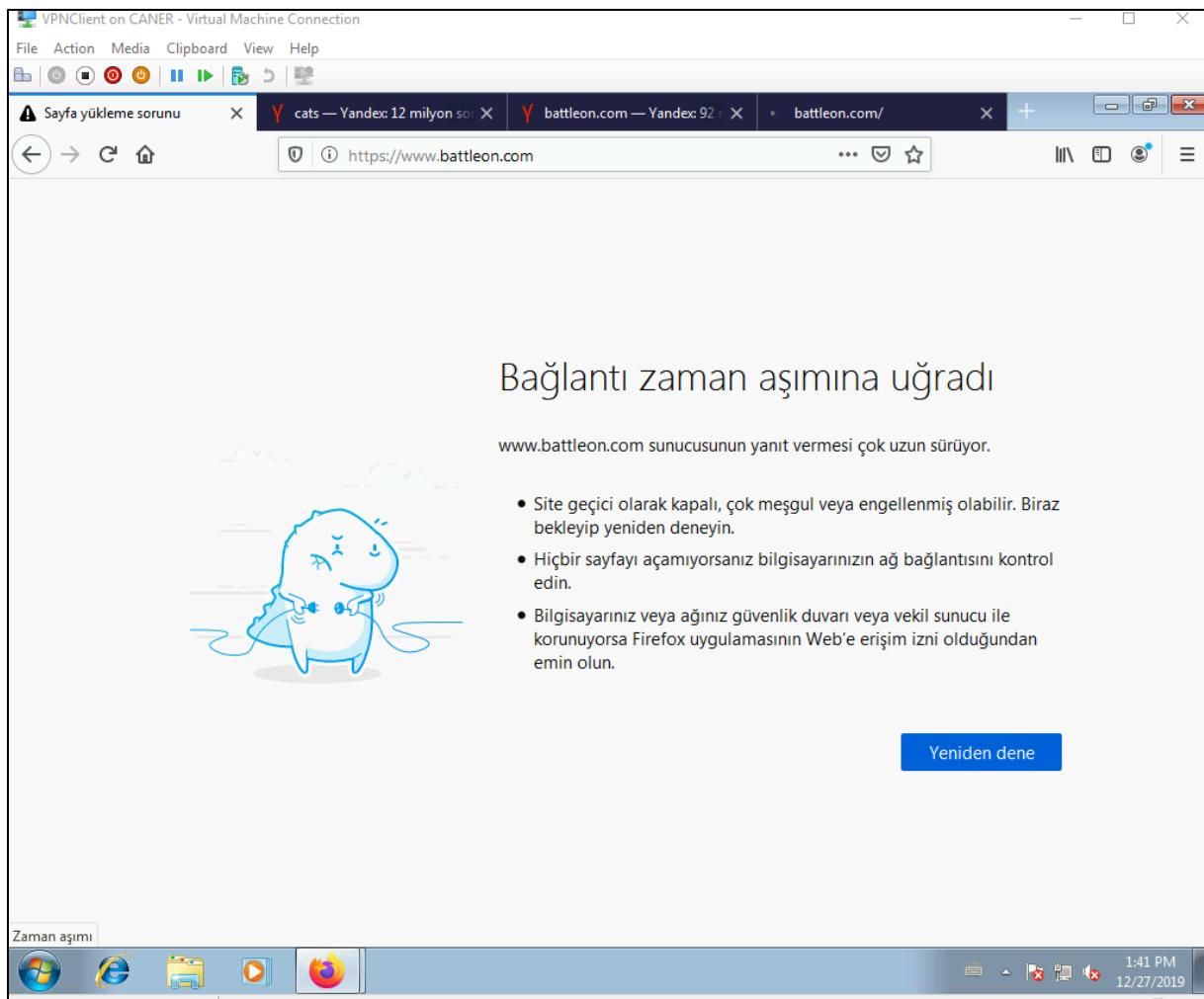
Now the rule is set.

The screenshot shows the pfSense Firewall Rules LAN page. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, and LAN, with LAN selected. The main table displays firewall rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 / 263 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0 / 0 B	IPv4 TCP/UDP	*	*	! BattleonBan	*	*	none			
✓ 11 / 2.33 MiB	IPv4	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0 / 0 B	IPv6	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

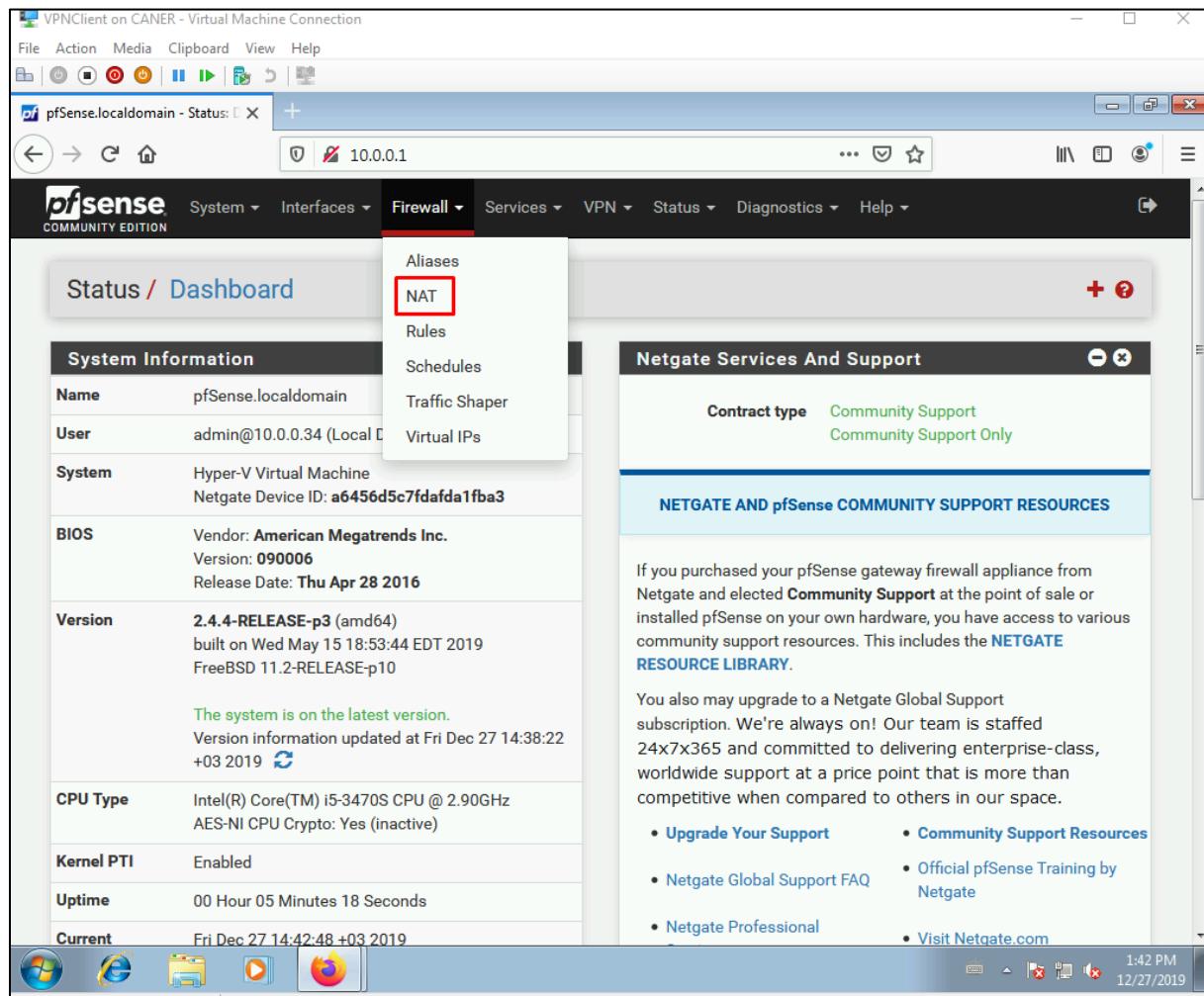
At the bottom, there are buttons for Add, Delete, Save, and Separator. The taskbar at the bottom of the window shows icons for Internet Explorer, File Explorer, and Mozilla Firefox, along with system status icons.

Now, when we try to play the game, we cannot connect.

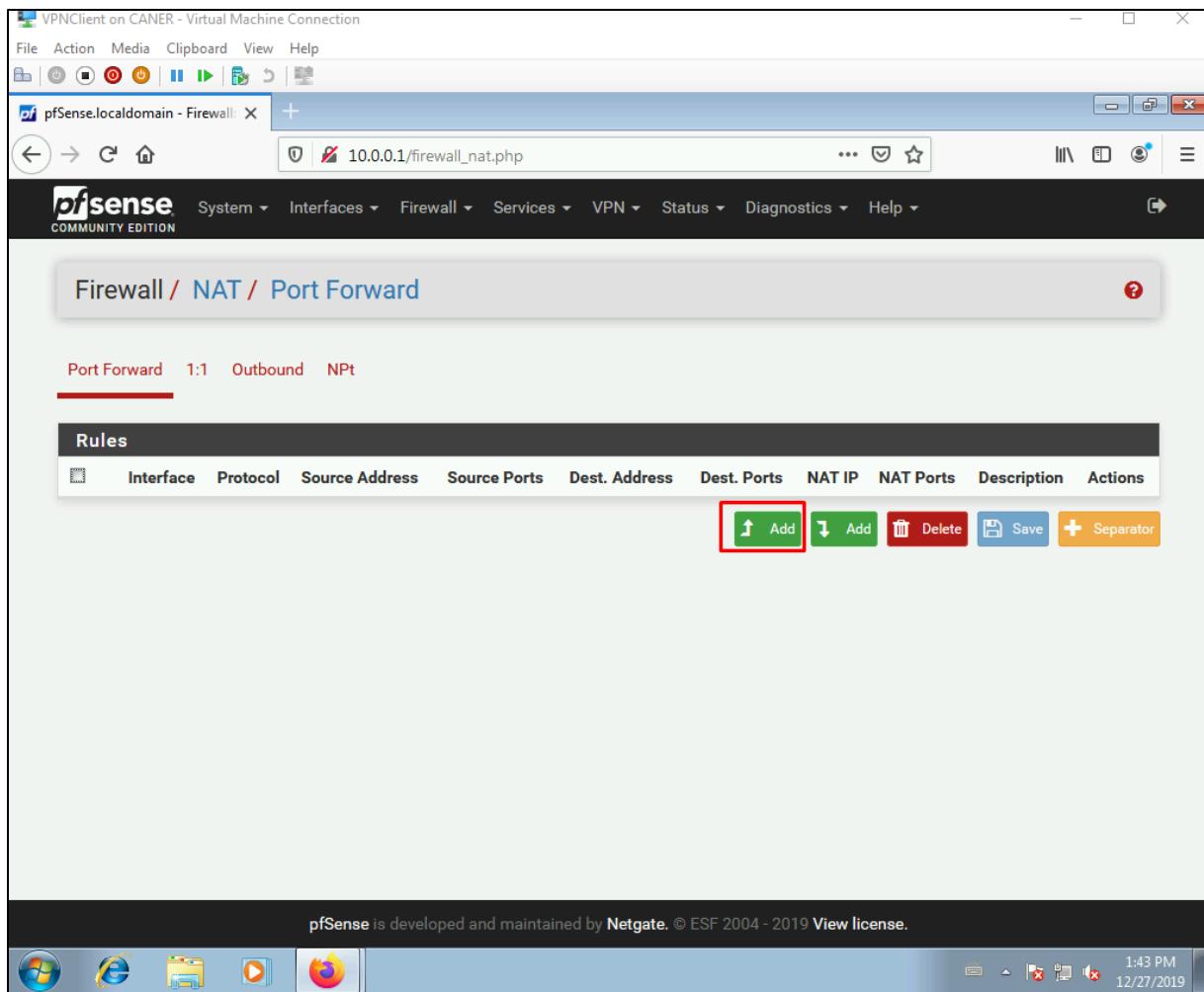


This ends the captive portal demonstration.

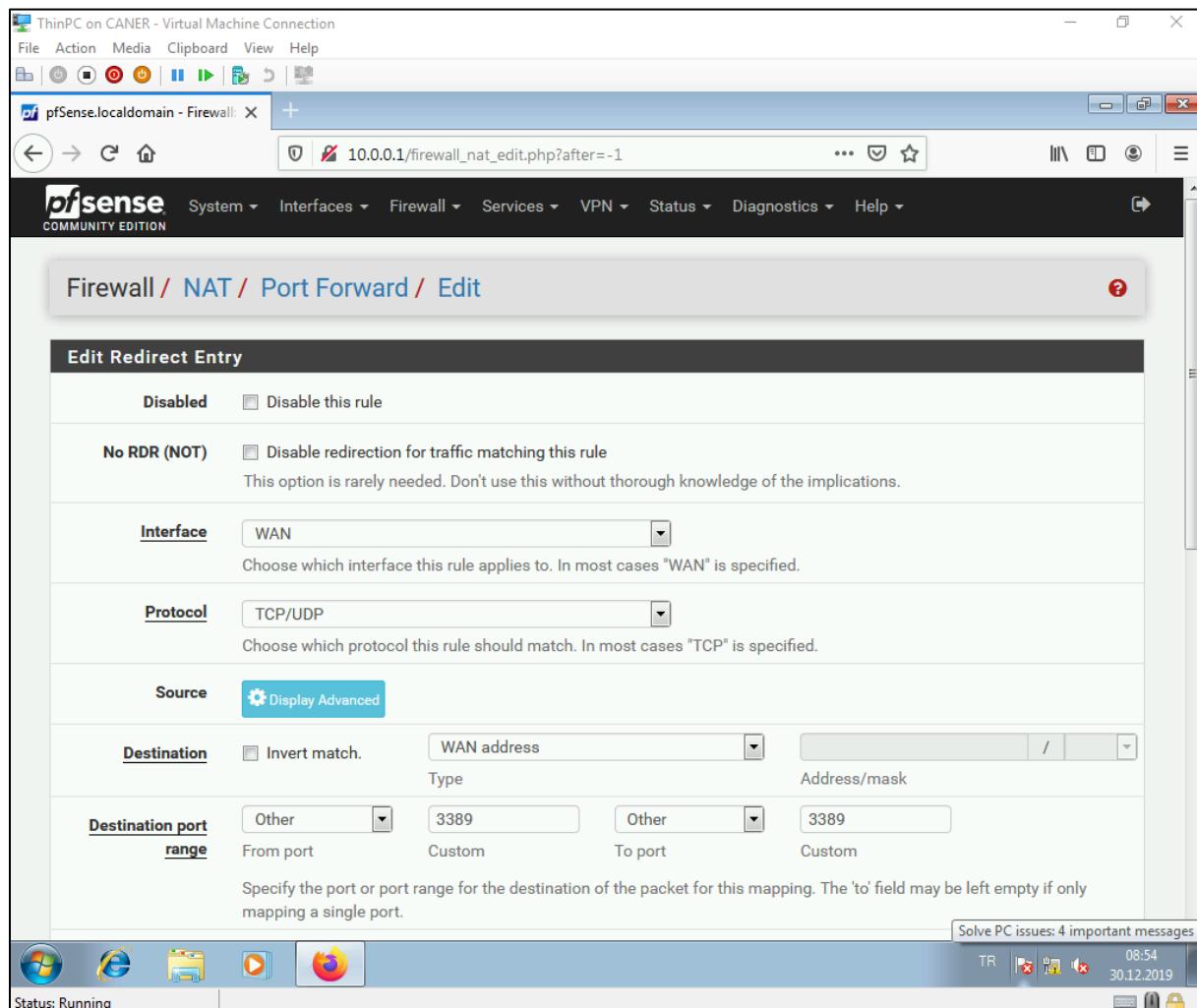
Now let's do an example of port forwarding and remotely connect to the internal PC. First, we need to get to NAT settings.



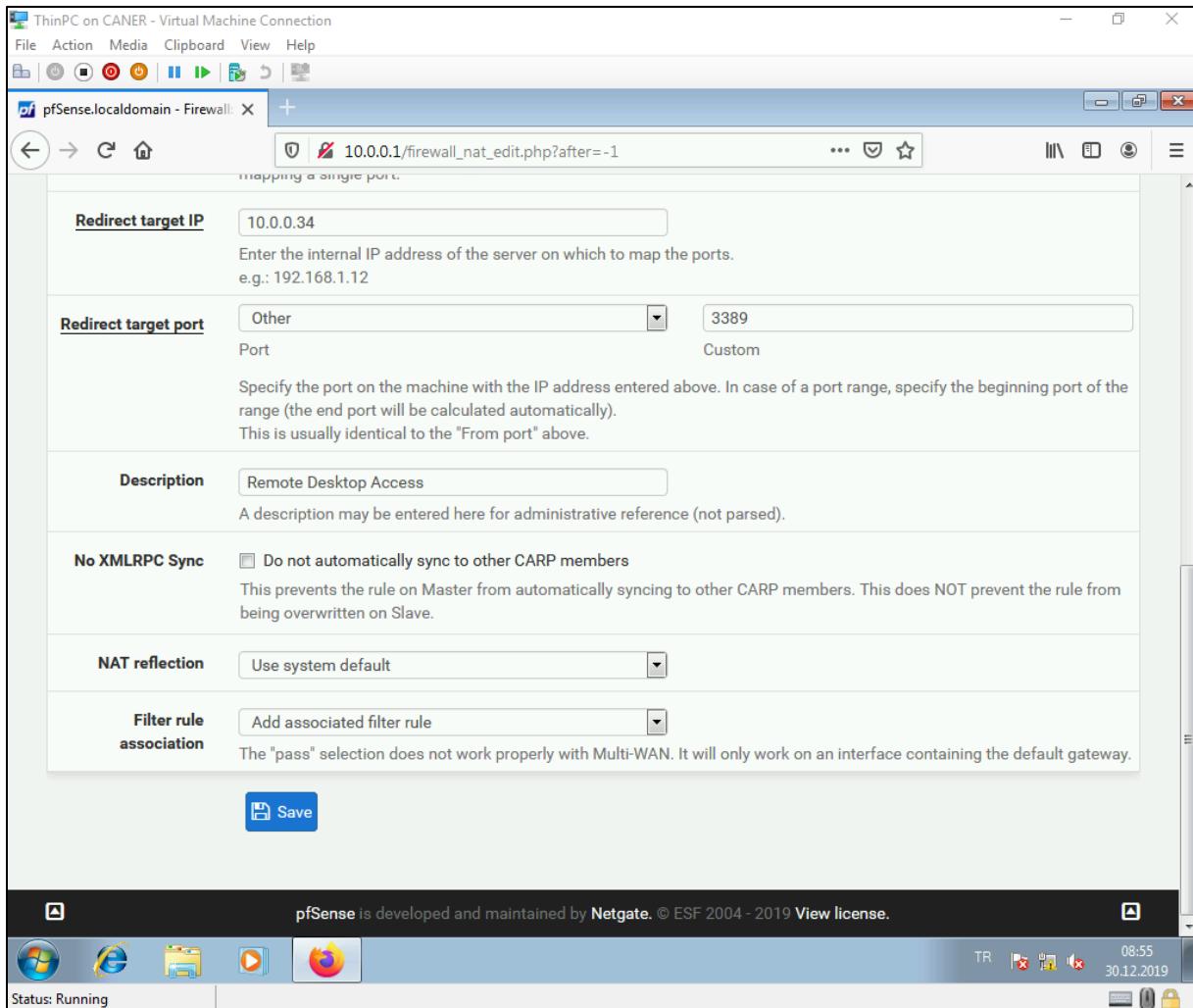
We then, add a new Port Forwarding rule.



We choose the interface as WAN, protocols at both TCP and UDP, write 3389 for destination port to allow Remote Desktop ...

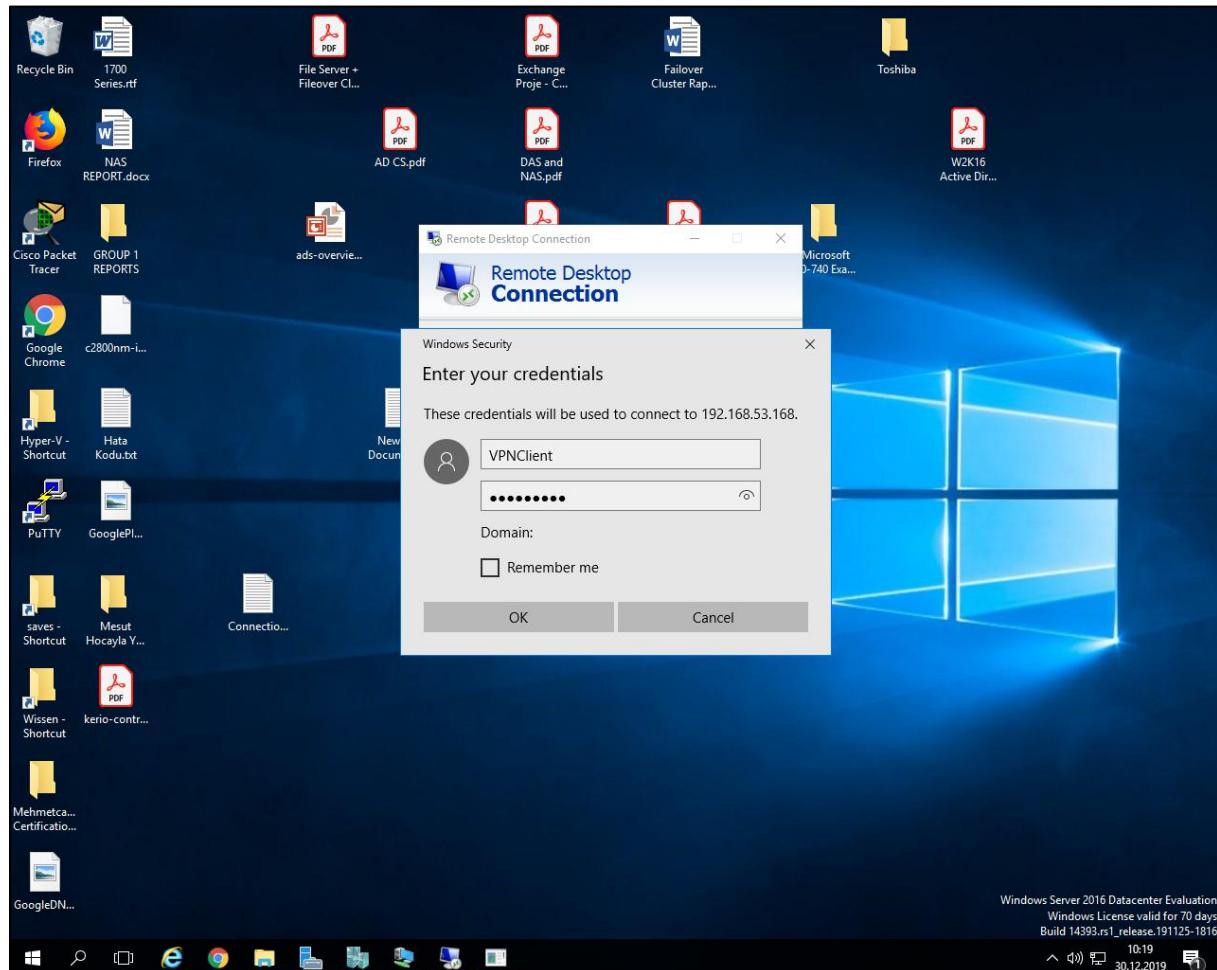


... and enter the IP address of the server we want to forward the Remote Desktop request to.

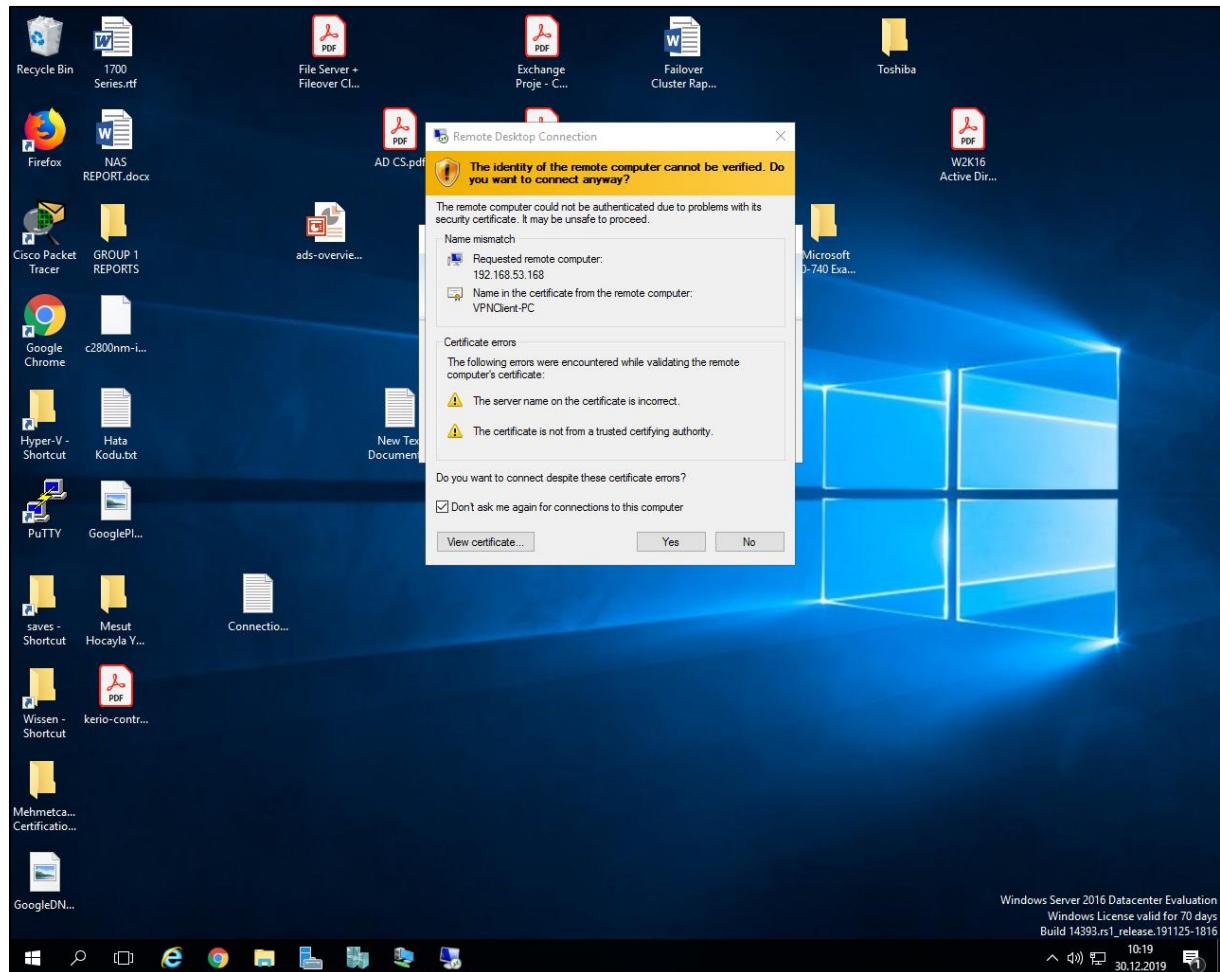


20.1.2020

Then, when we enter the WAN address of the Firewall to connect via Remote Desktop, we get to log in as an account on the server that we specified.

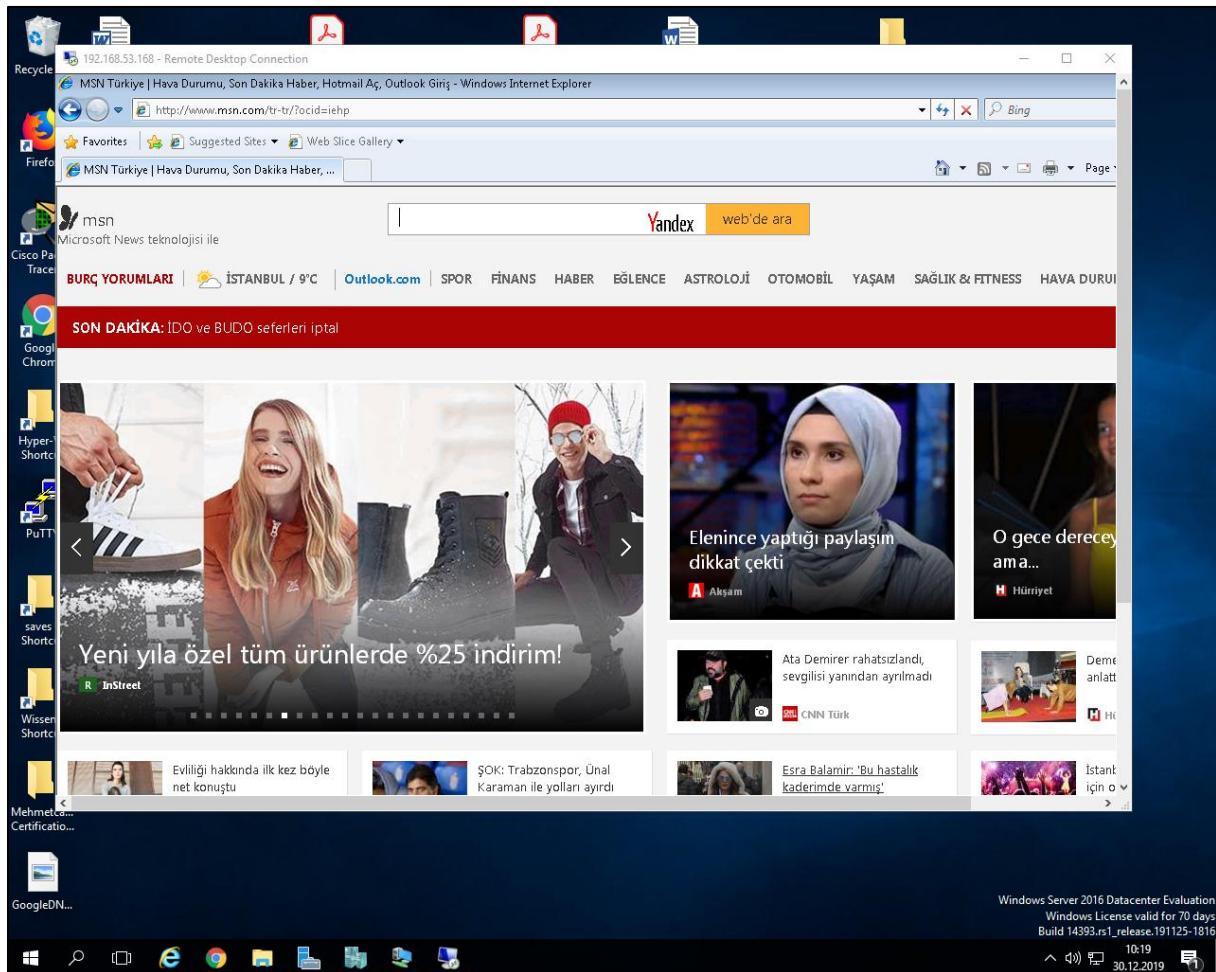


A confirmation page pops up.



20.1.2020

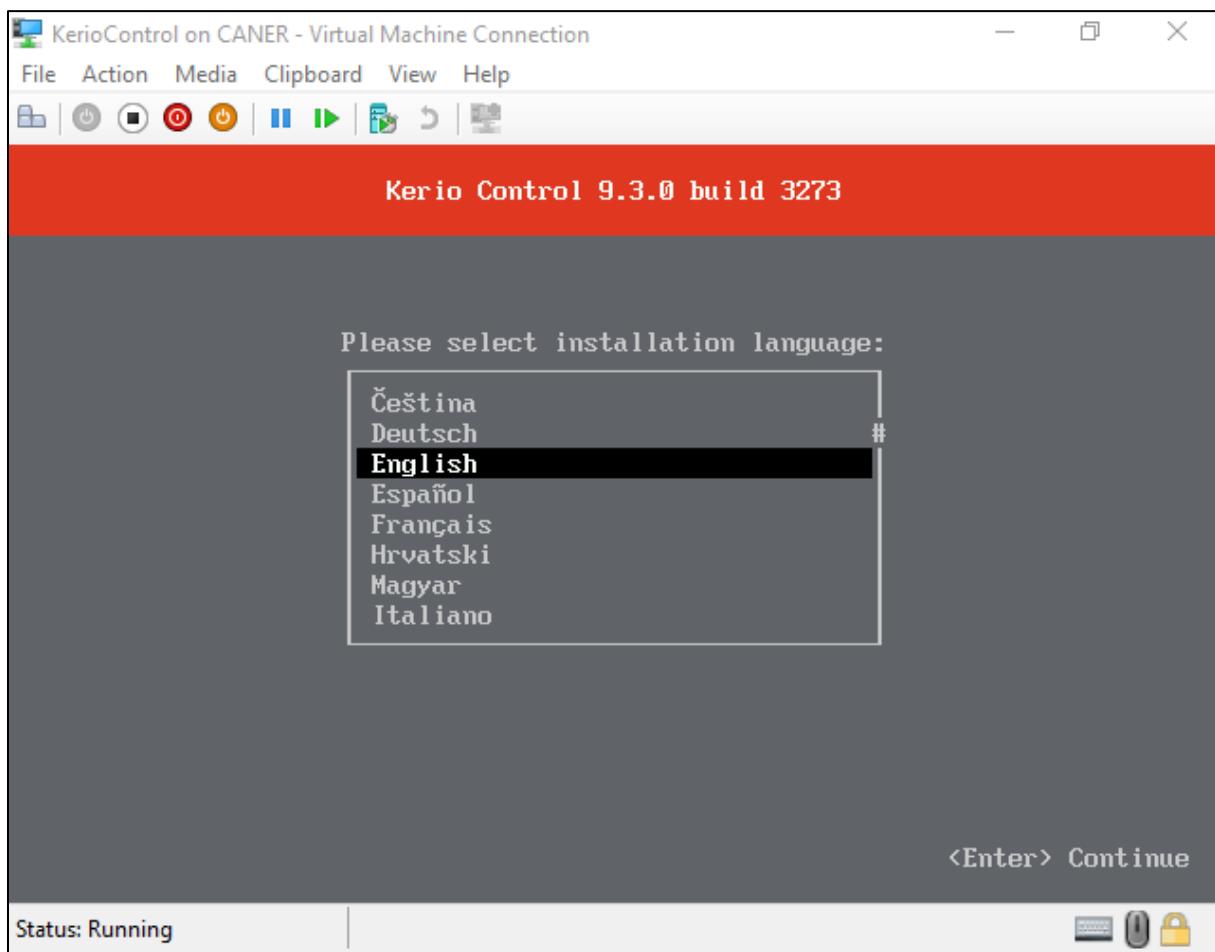
And then, we're in.



This finishes the pfSense part of this project.

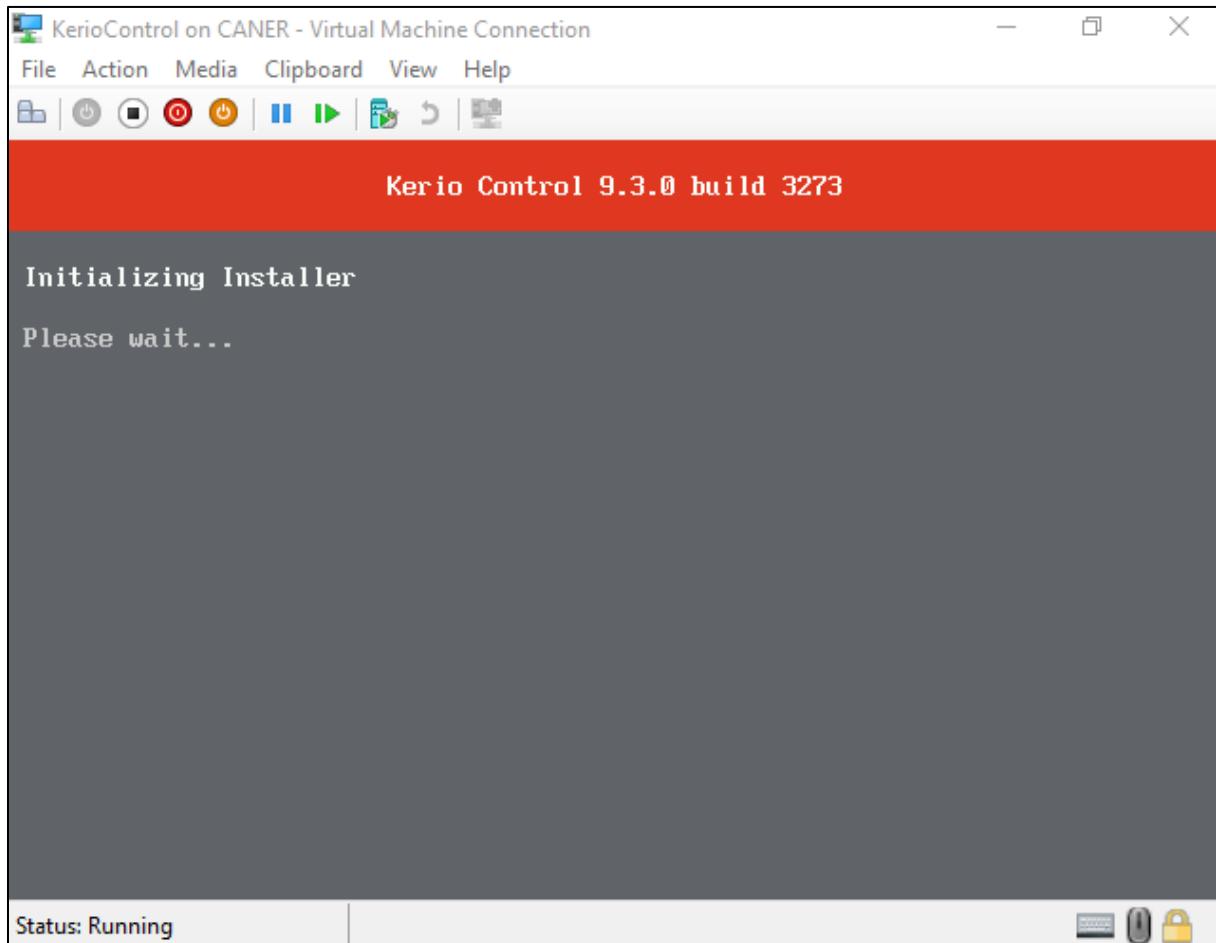
2) Kerio

Similar to the pfSense set up, we create a new virtual machine with two NICs for the Kerio Firewall and start the image on the installation media. Then, the installer starts and the first thing we select is the language.

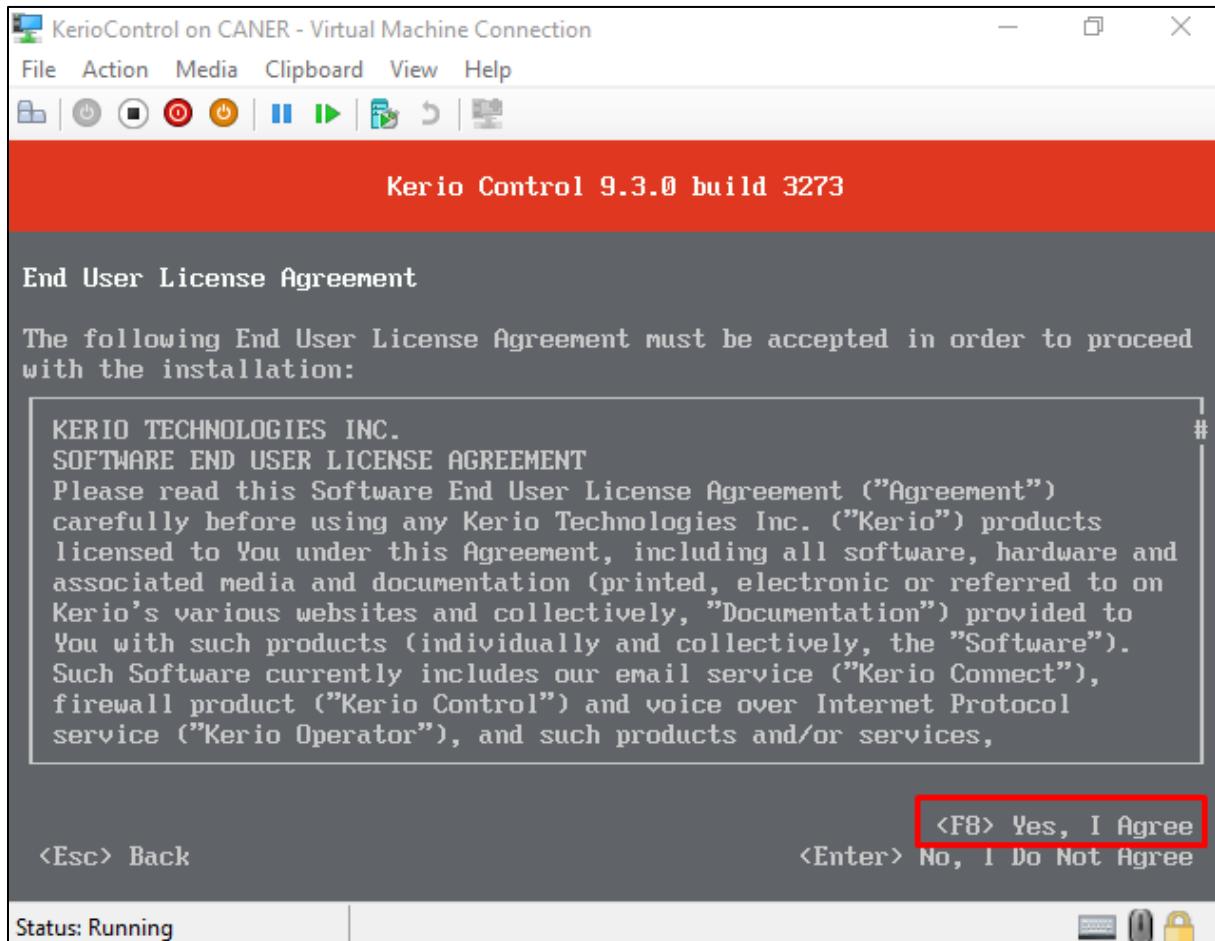


20.1.2020

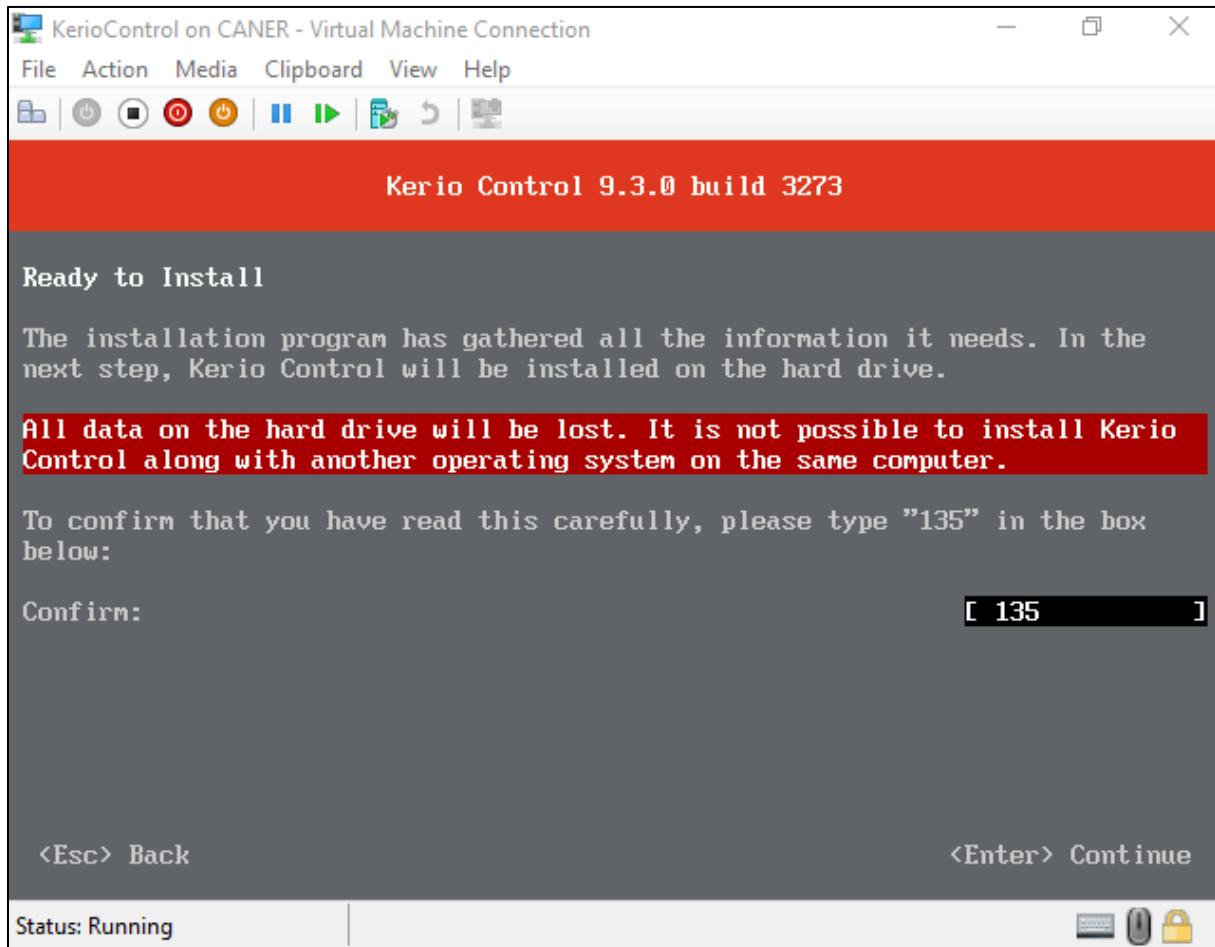
The installer starts to initialize.



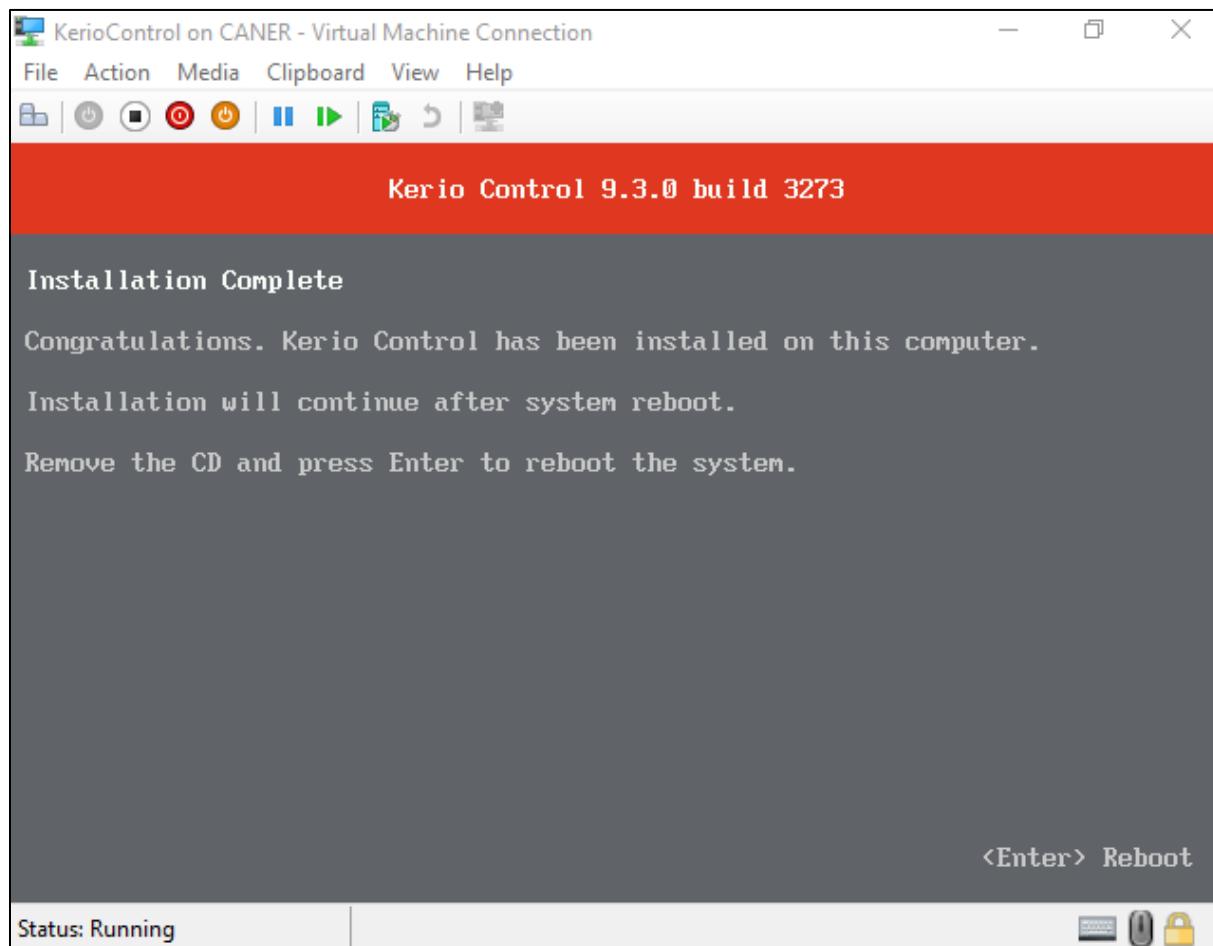
We agree to the user agreement and proceed.



We type 135 to proceed.

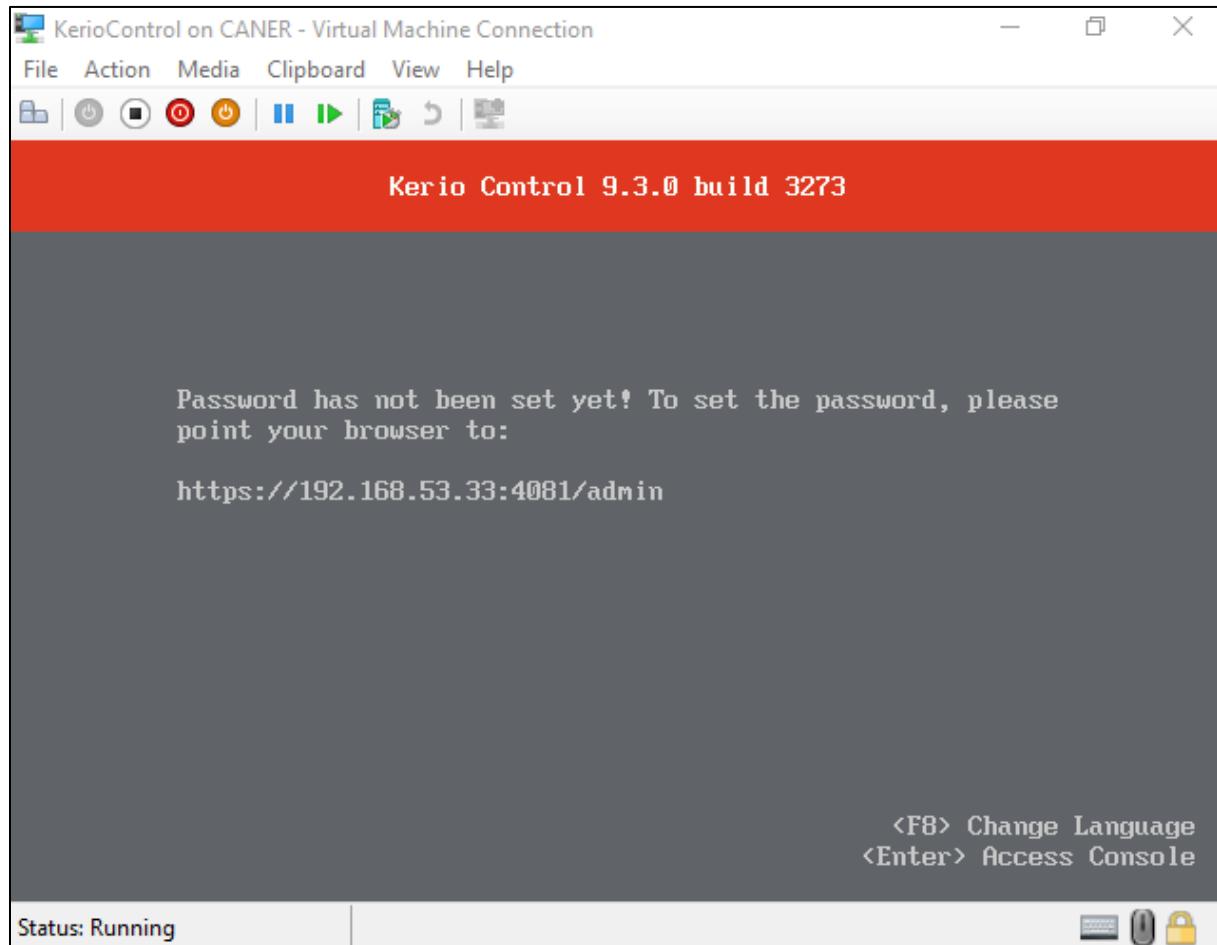


After the installation is complete, we again remove the image disk and reboot.

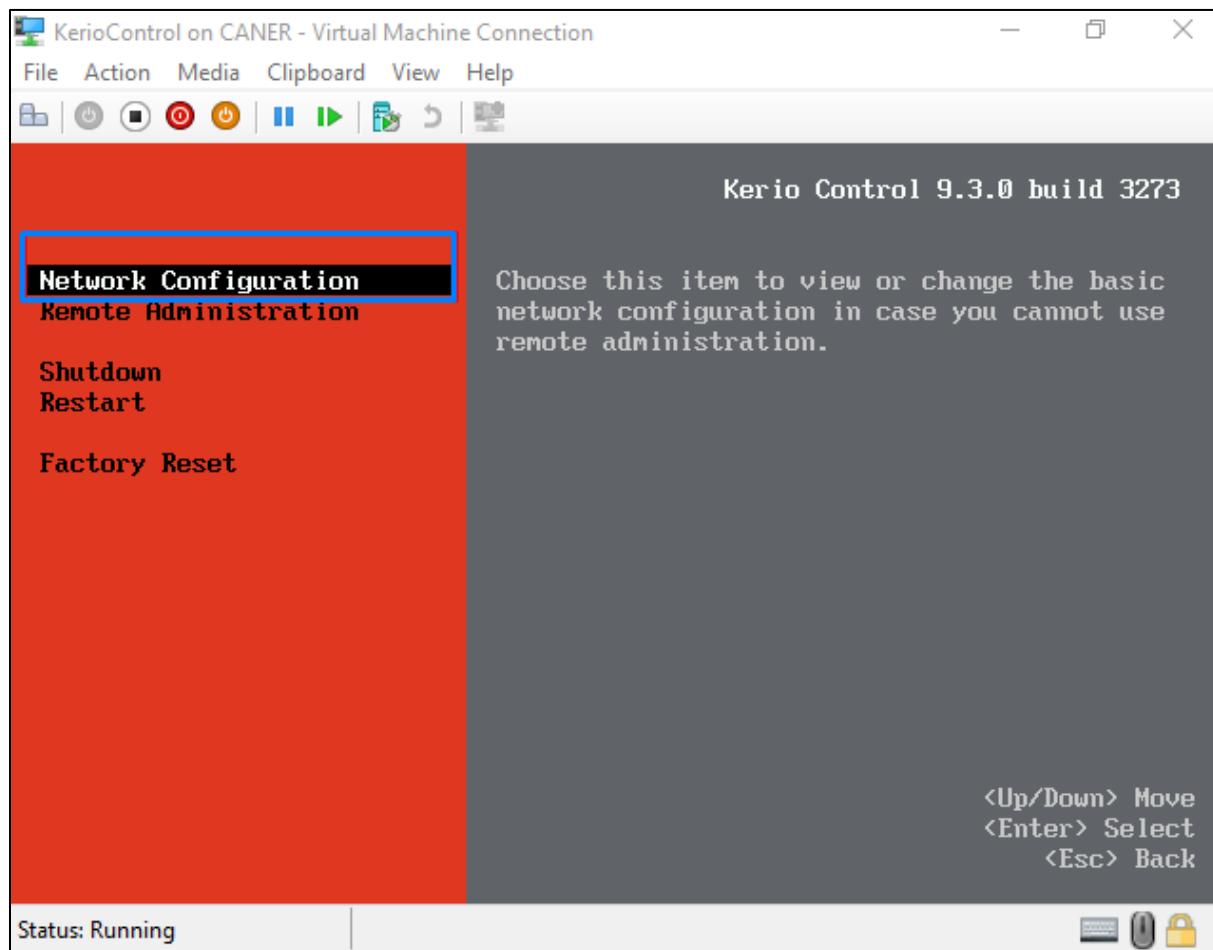


20.1.2020

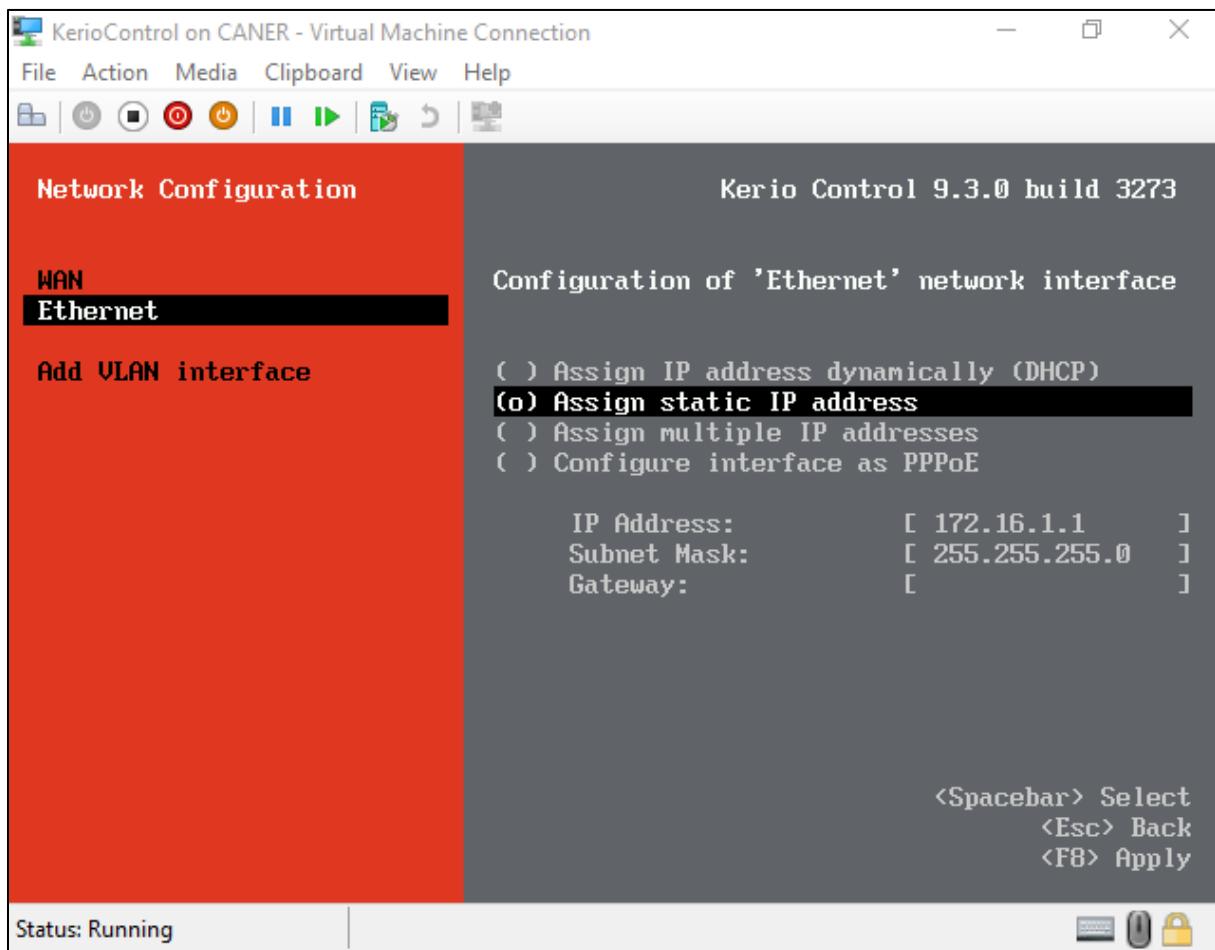
And the firewall is working. We get to the access console by pressing Enter.



We want to do the network configuration.

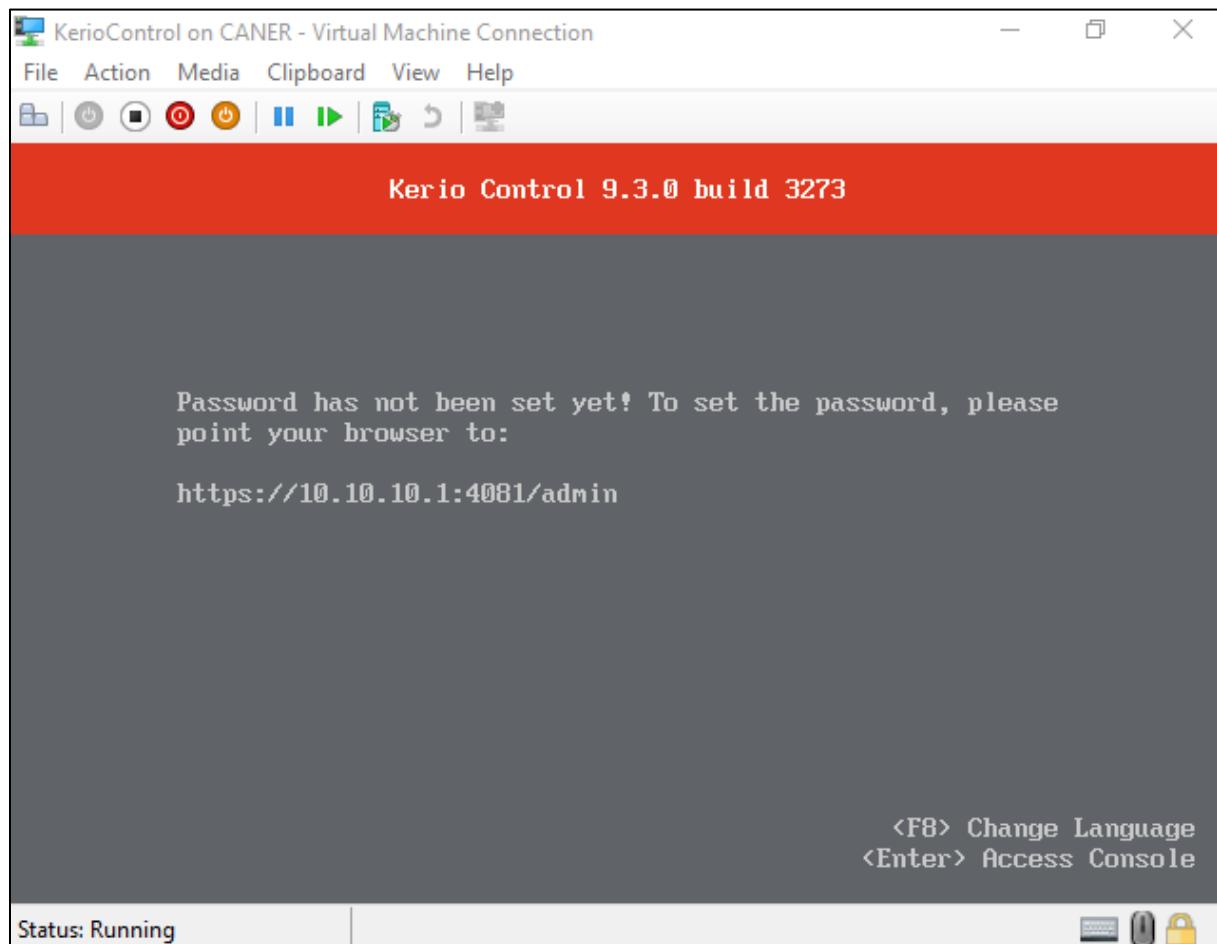


We assign a static IP address to the internal Ethernet interface.



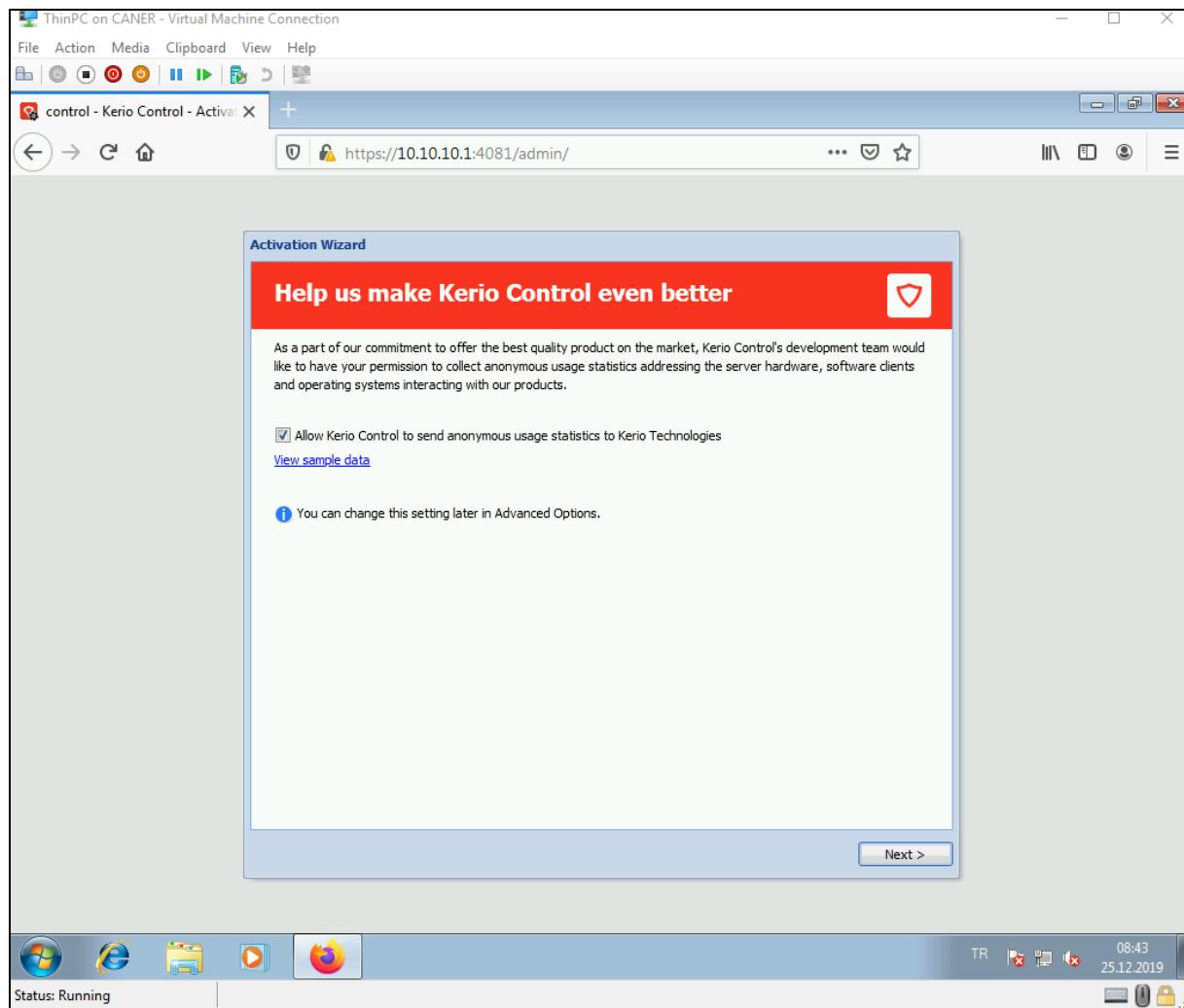
The WAN interface is automatically receiving IP from the BAU DHCP and we don't have to do anything there.

After we set our internal IP address of 10.10.10.1/24 and reboot the firewall. This screen once again welcomes us but now the access IP is the internal interface's IP address.

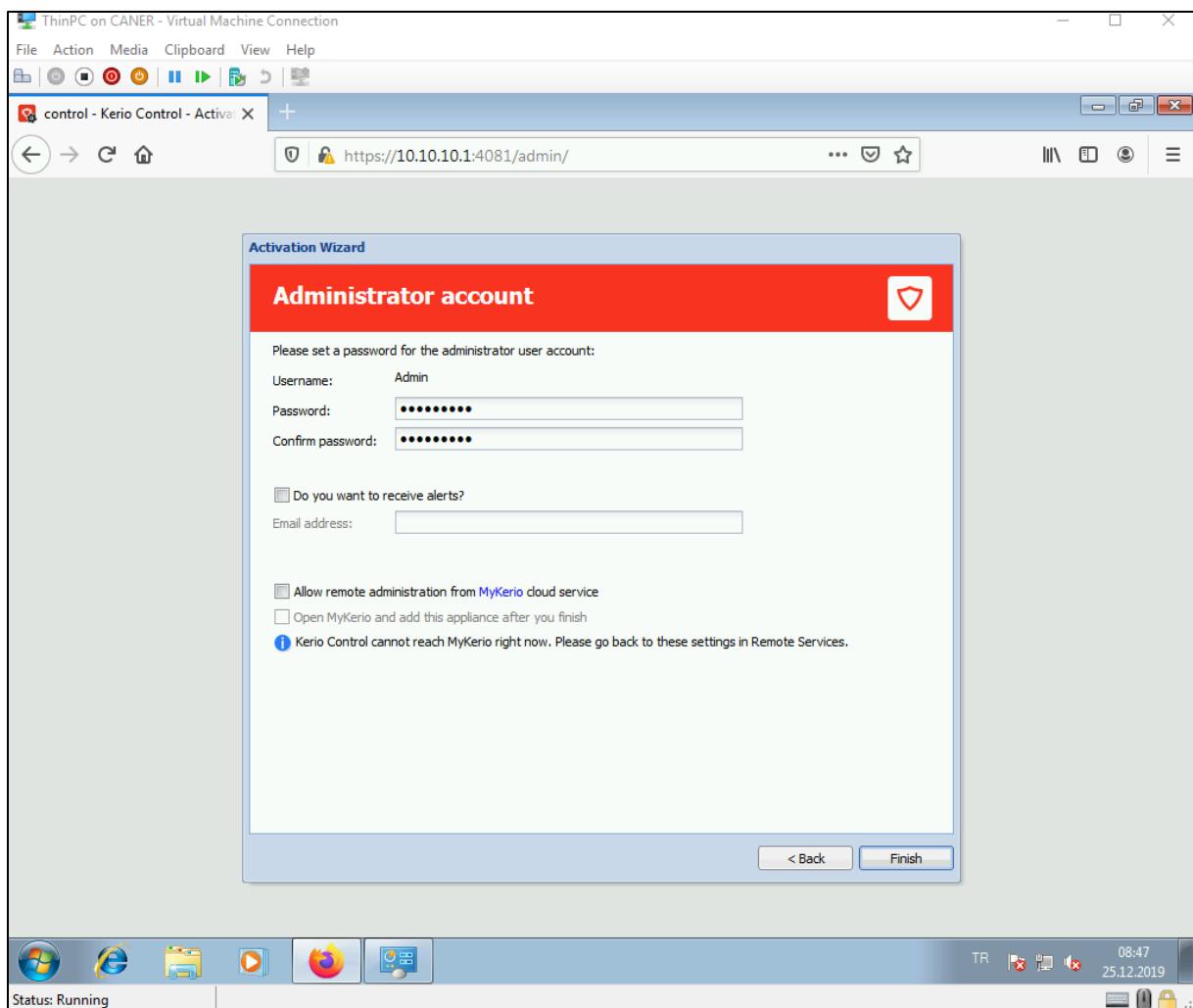


20.1.2020

Similar to how we have done it with pfSense we enter this address to our web browser.

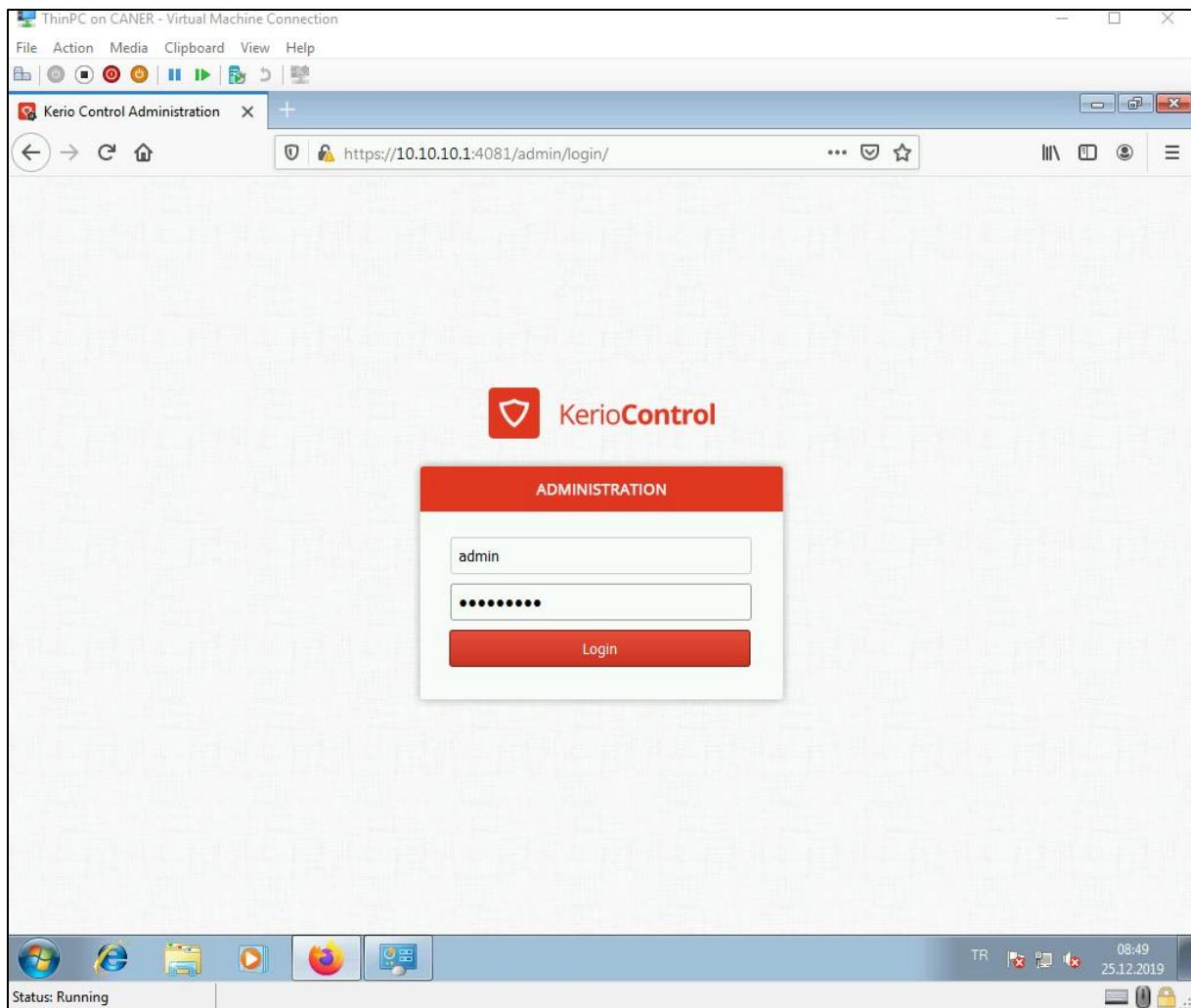


It wants us to set a password for admin.

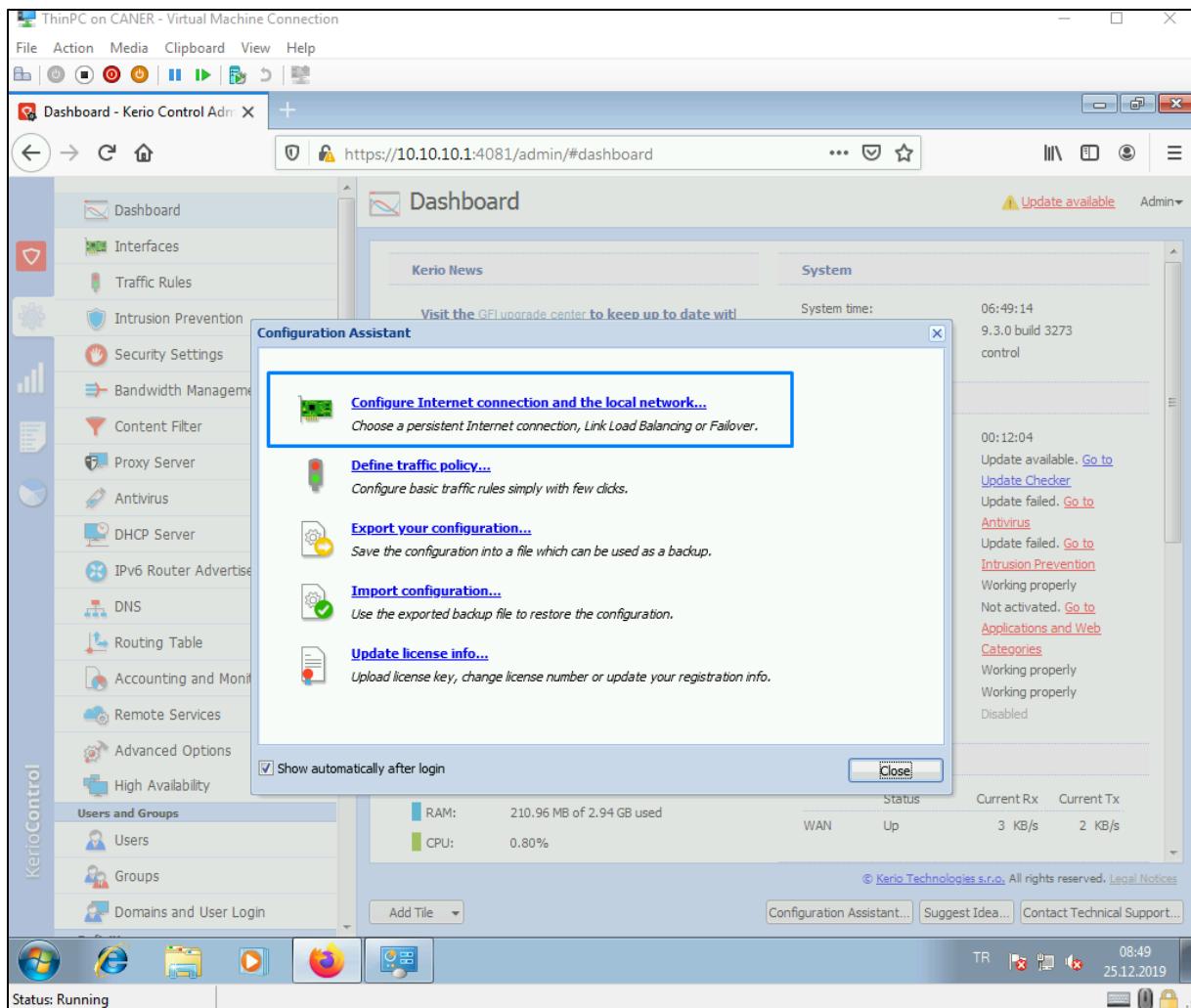


20.1.2020

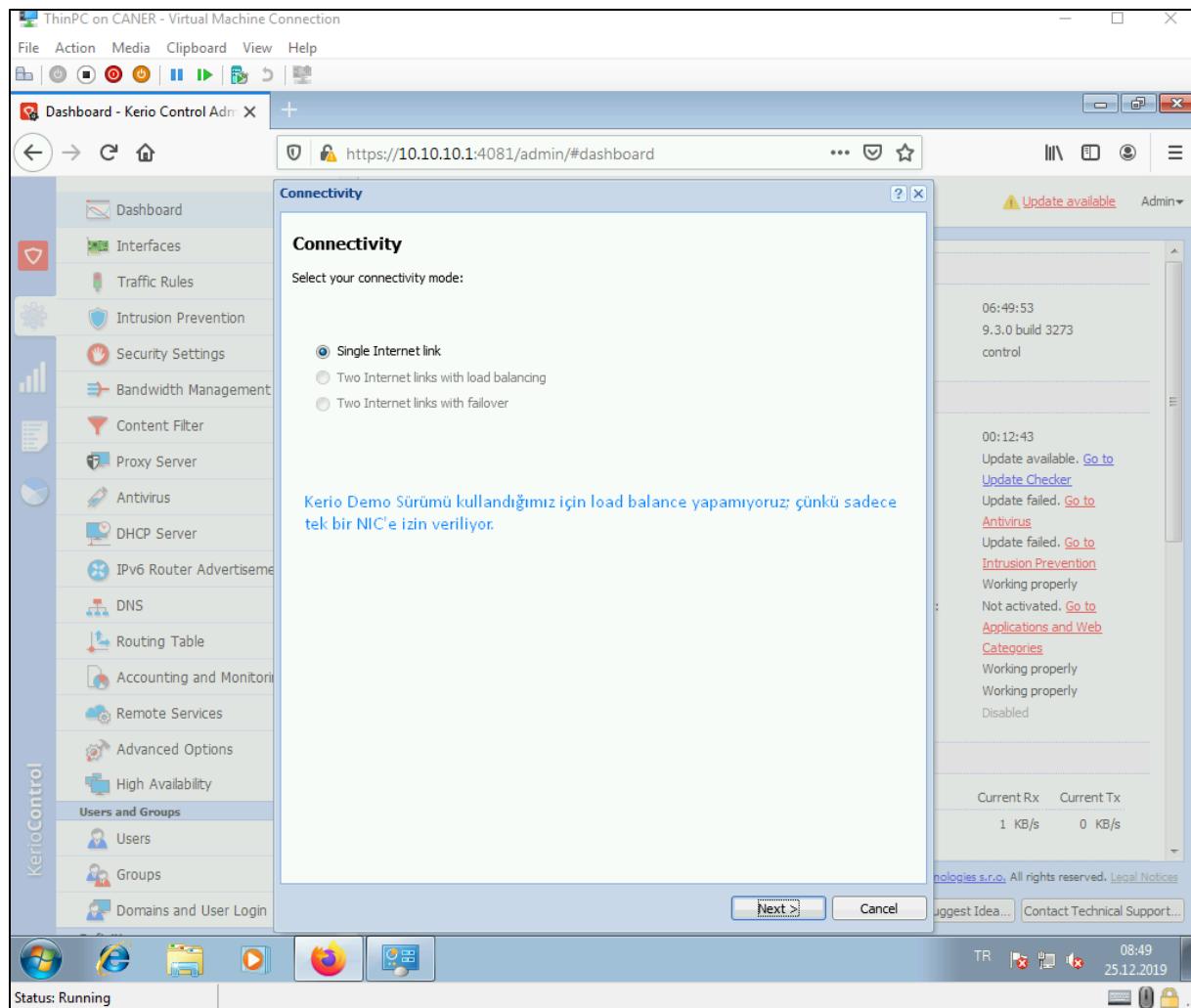
We log in using the newly set password.



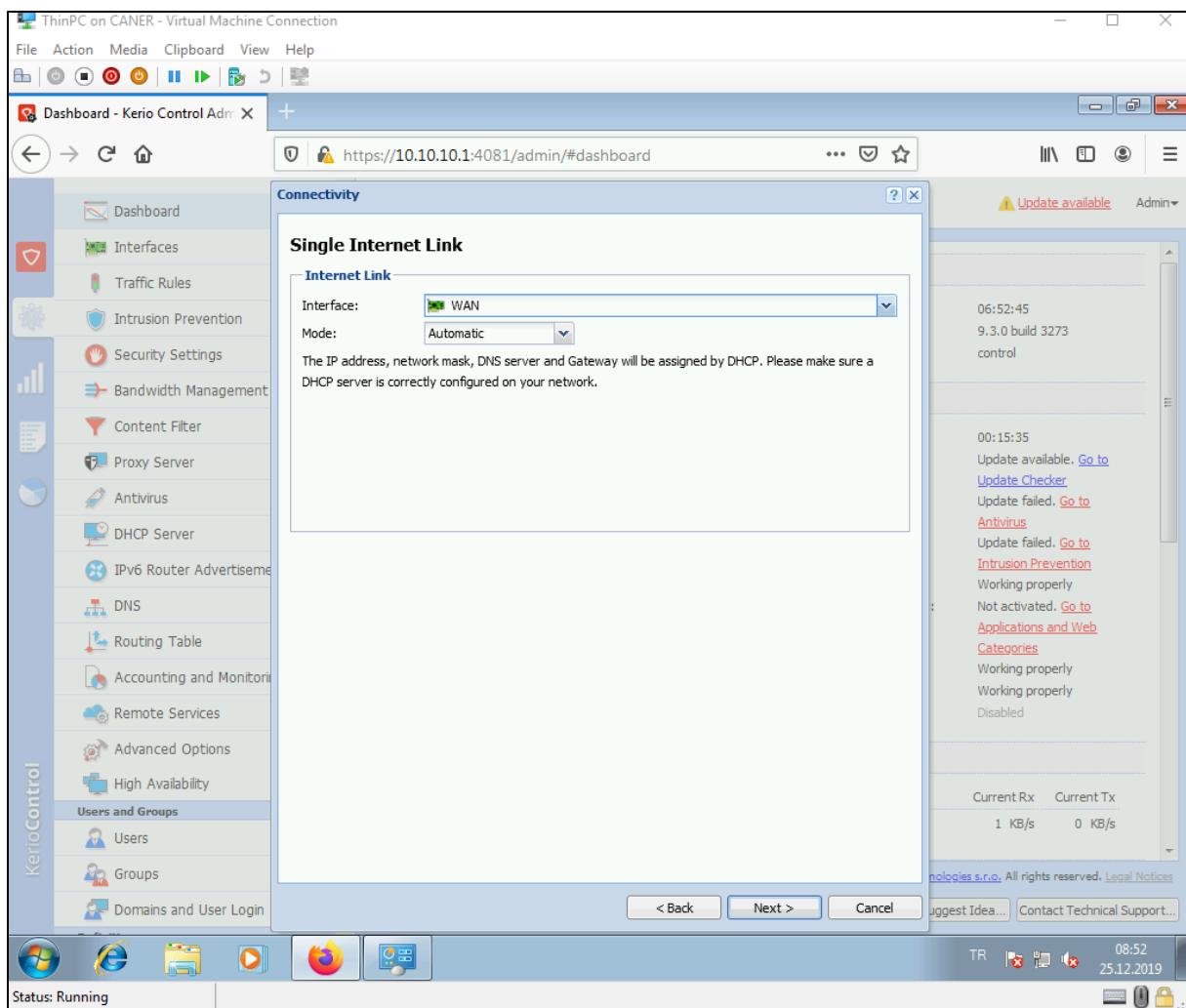
We configure the network settings.



We use single link since this is a Demo Edition.

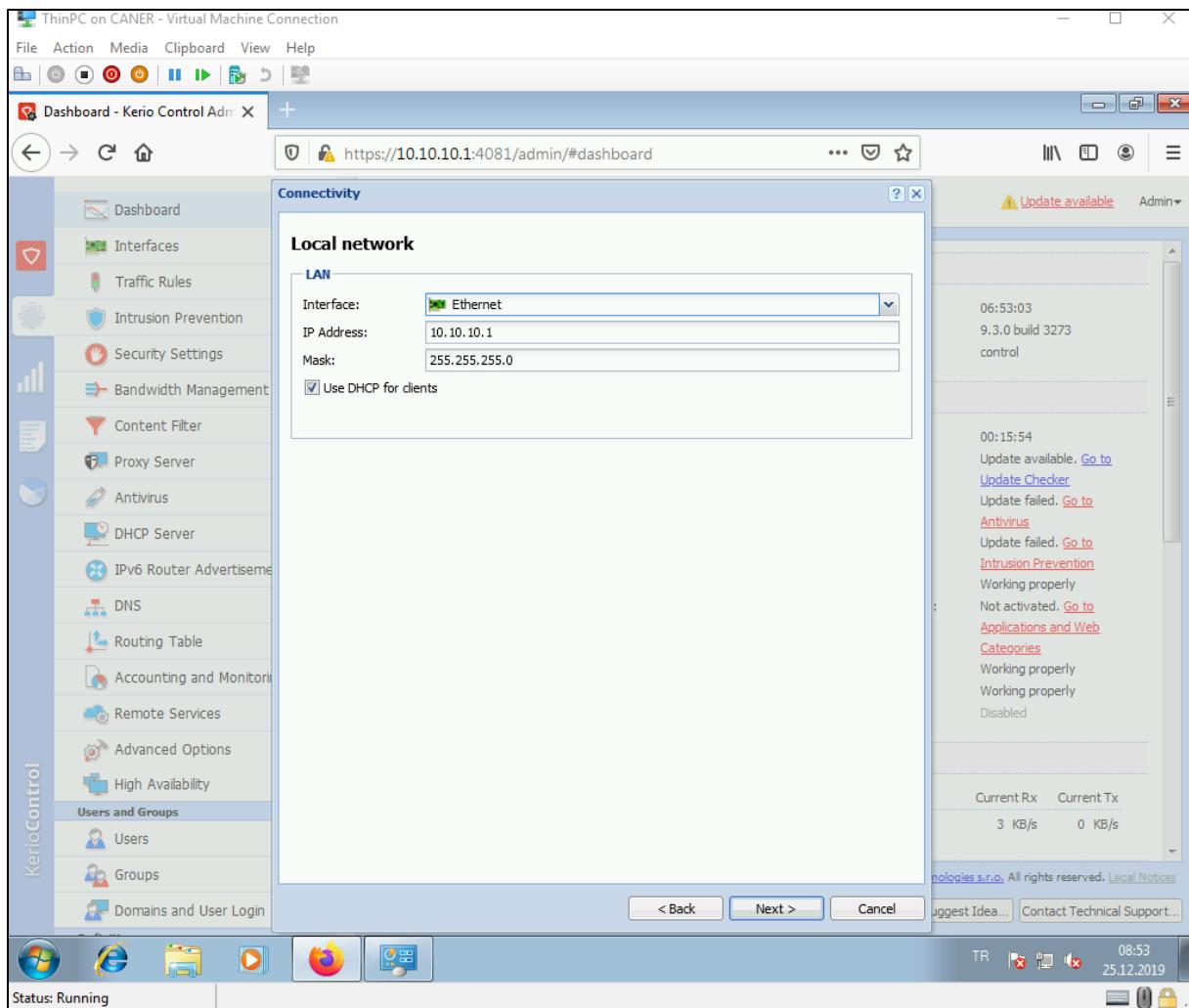


We keep WAN interface at automatic.

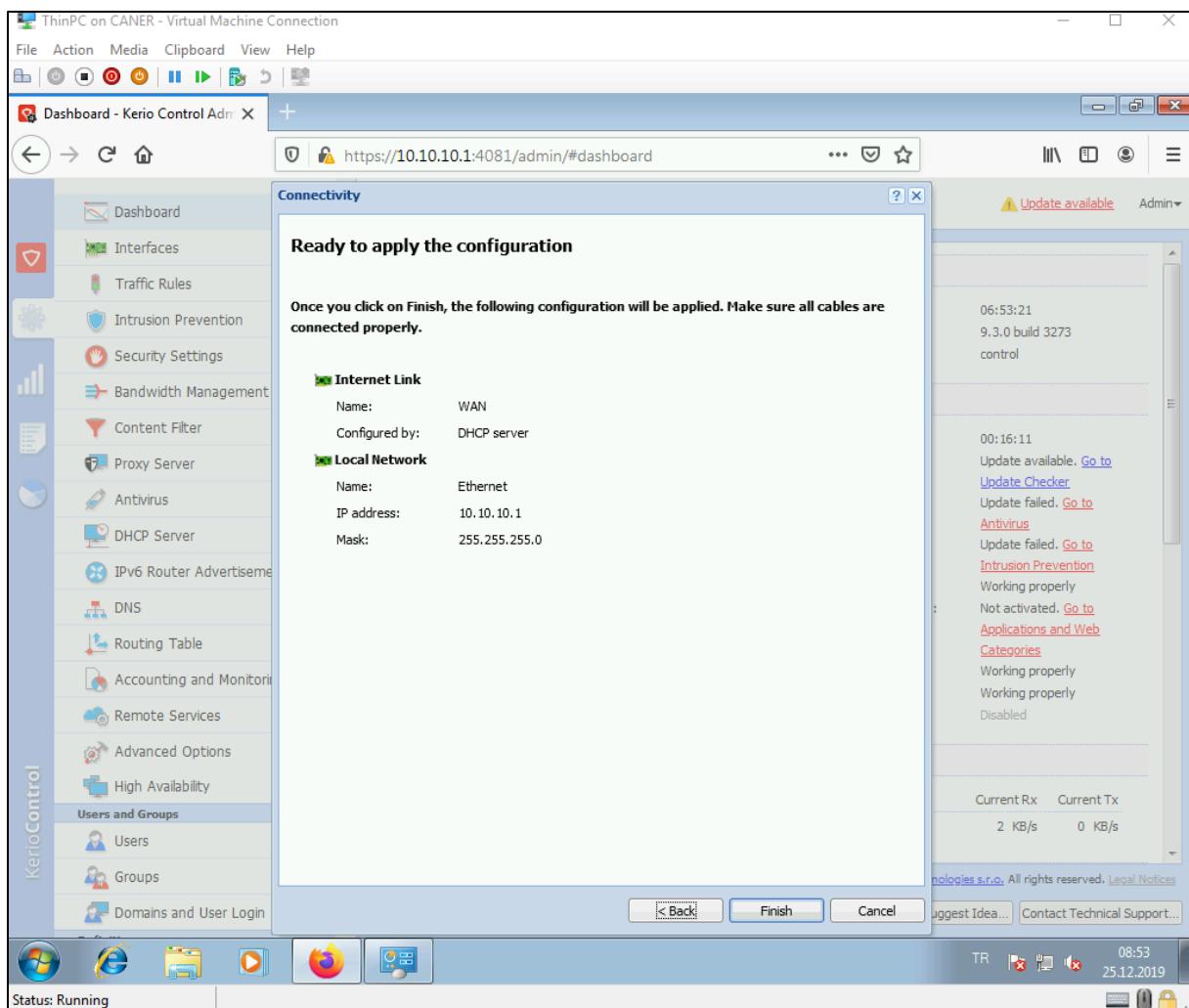


20.1.2020

We set the Ethernet interface at the IP address we have set before and enable DHCP.

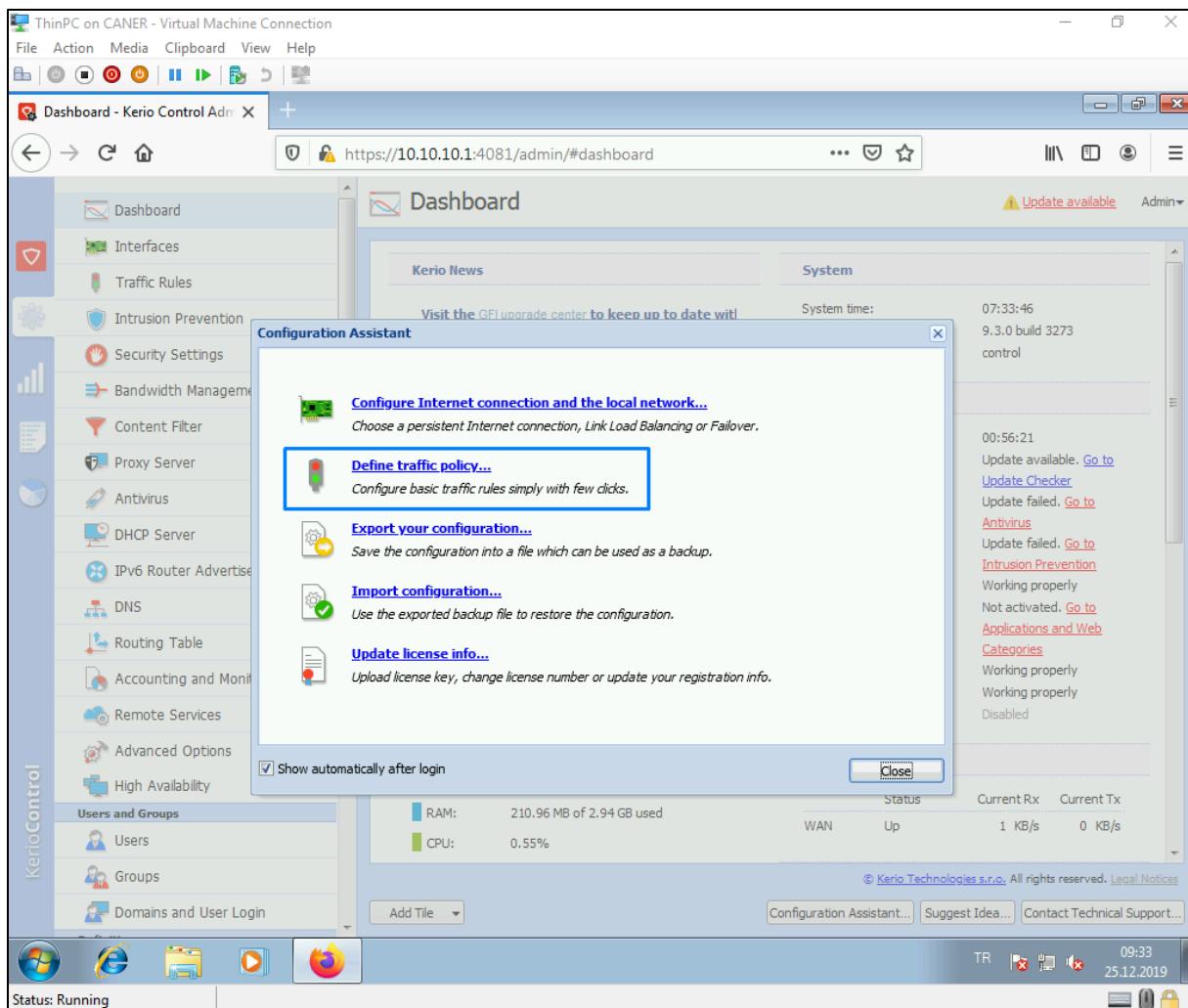


We review and finish.

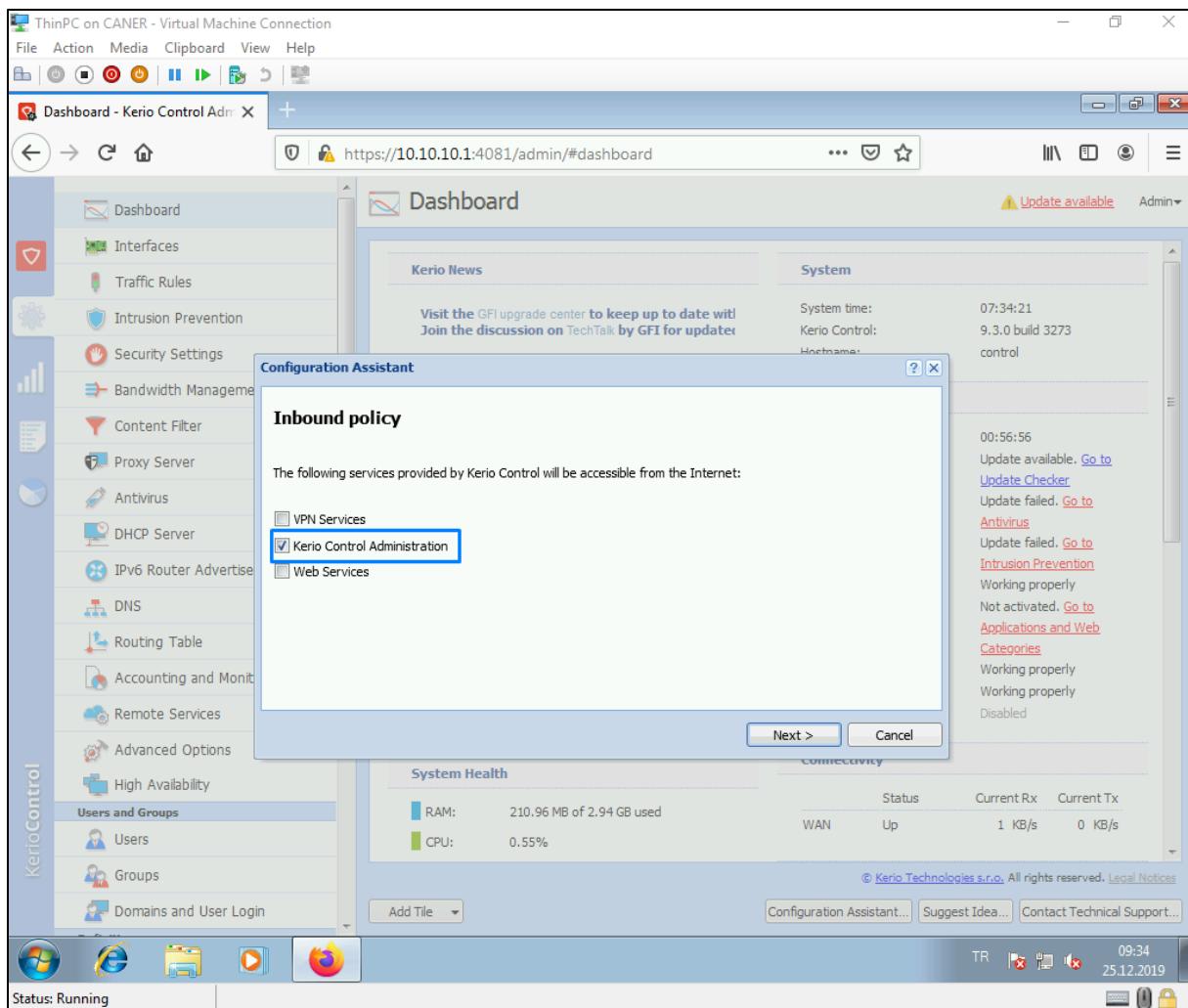


20.1.2020

The next step of the wizard is to set traffic rules.

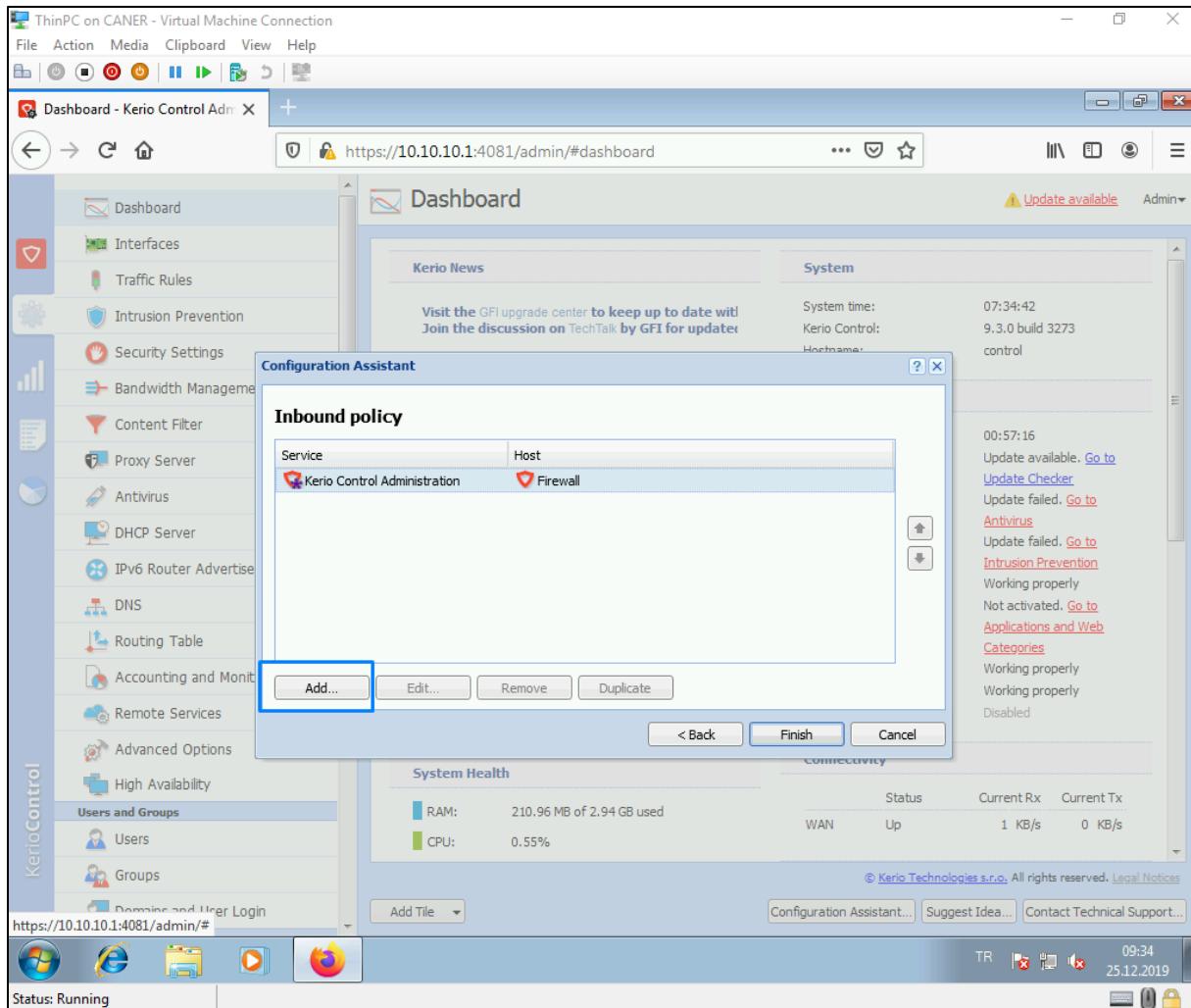


We choose to set the rules for Kerio Control Administration.

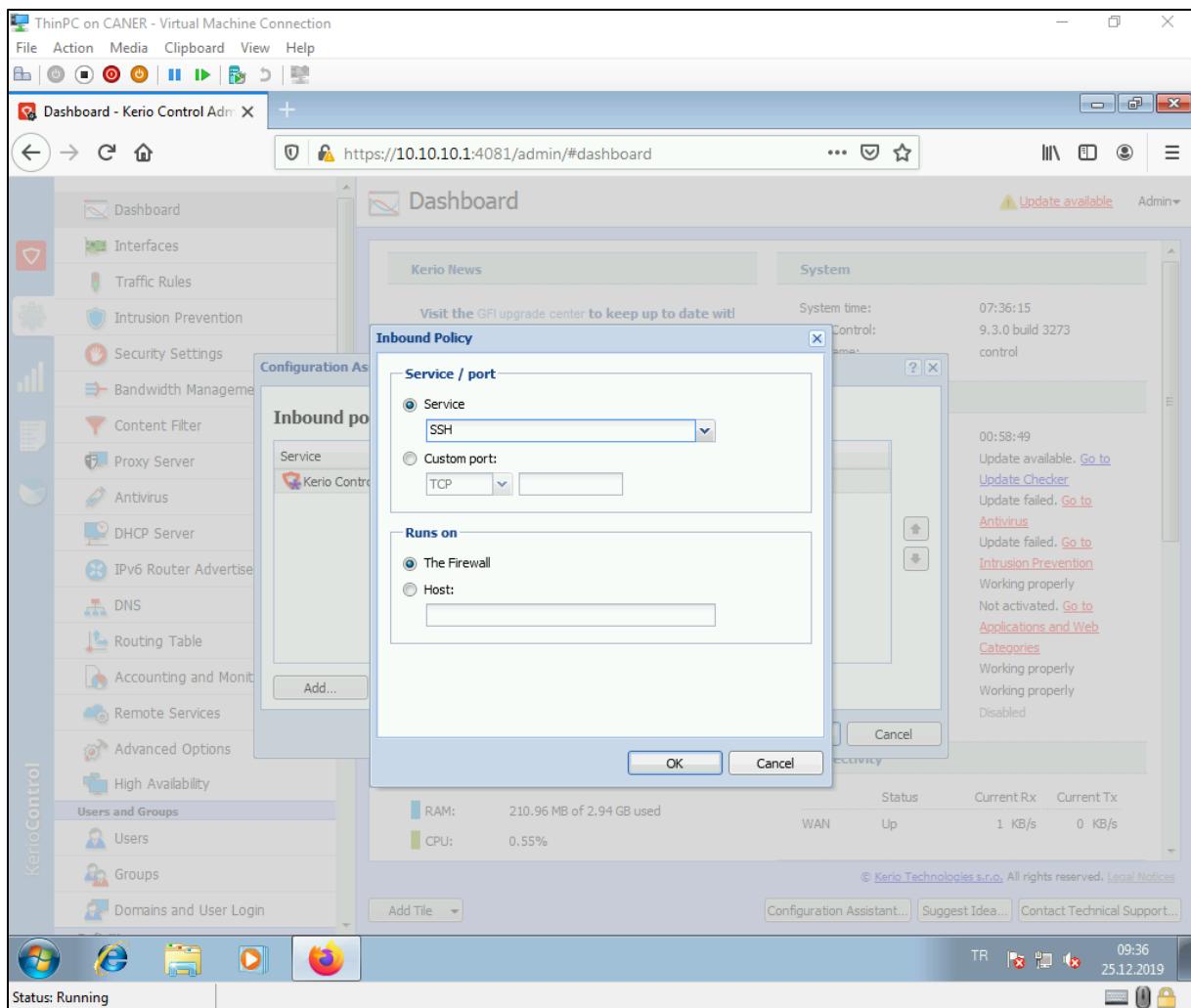


20.1.2020

We select the firewall itself and add inbound policies.

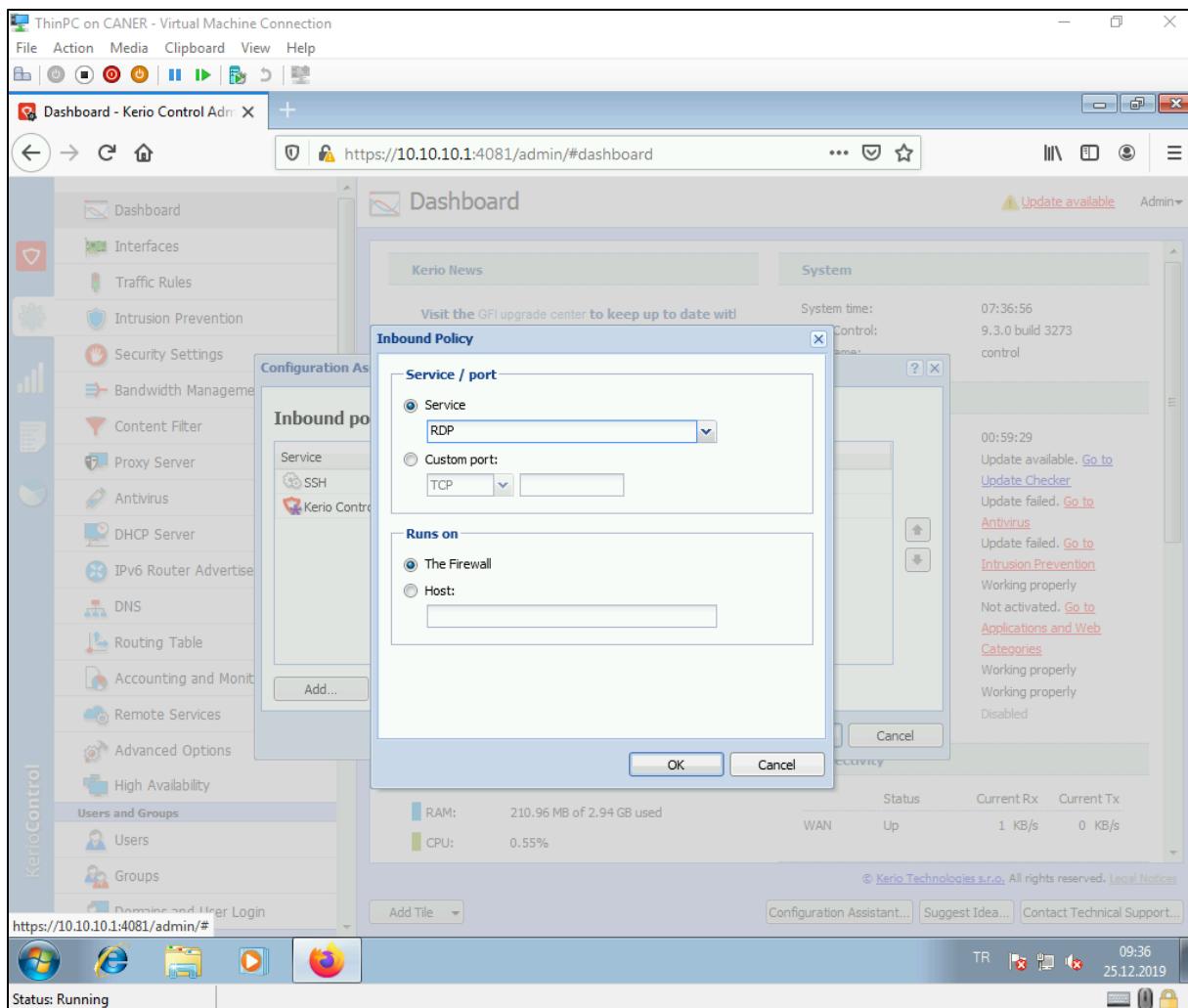


We enable SSH.



20.1.2020

We enable RDP.



We also enable Telnet and proceed.

The screenshot shows the Kerio Control Admin interface running on a ThinPC virtual machine. The main window displays the Dashboard with various system status indicators and a Configuration Assistant dialog box in the foreground.

Configuration Assistant - Inbound policy

Service	Host
Telnet	Firewall
RDP	Firewall
SSH	Firewall
Kerio Control Administration	Firewall

Buttons at the bottom of the dialog: Add..., Edit..., Remove, Duplicate, < Back, Finish, Cancel.

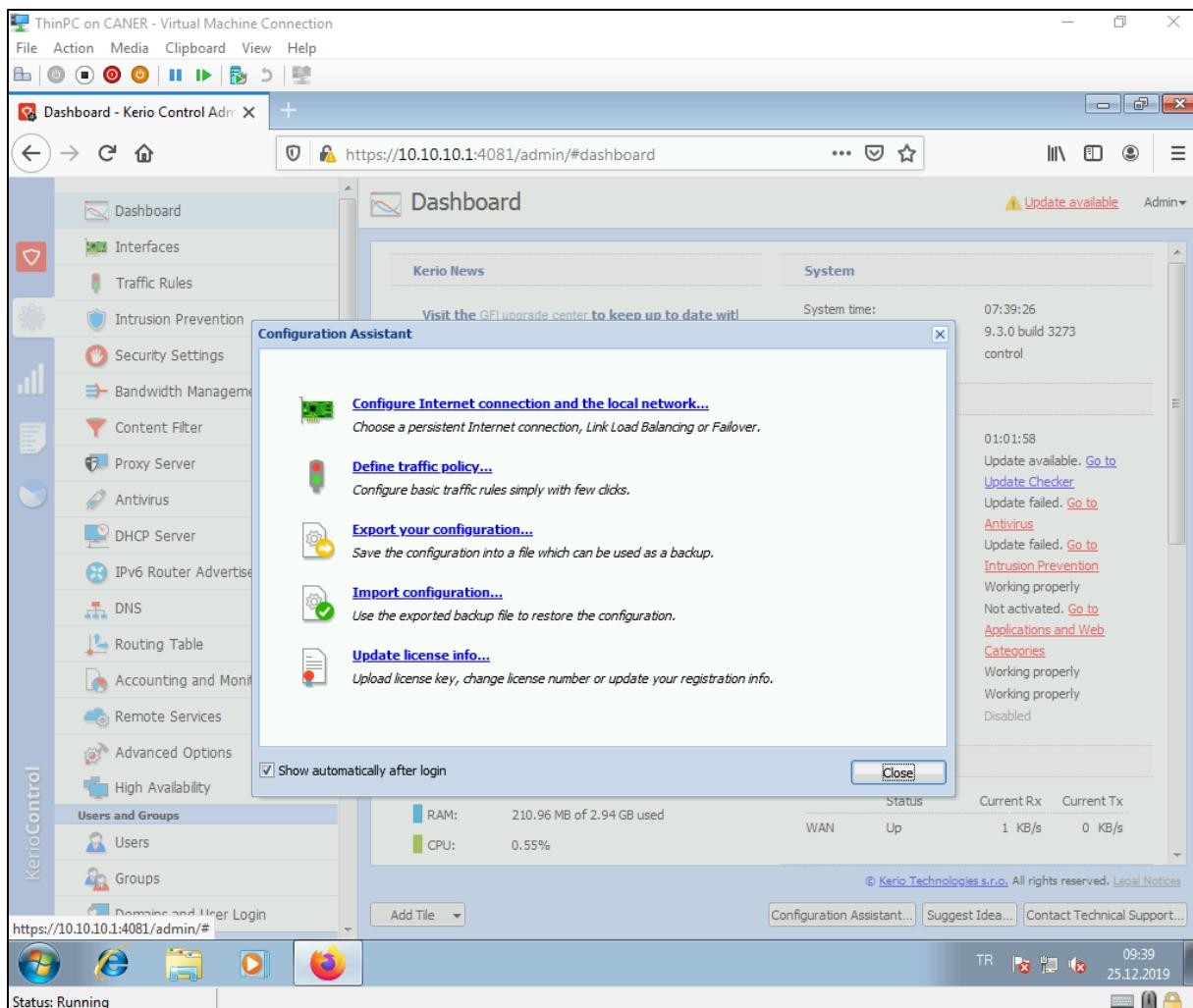
System Health

RAM:	210.96 MB of 2.94 GB used	Status	Current Rx	Current Tx
CPU:	0.55%	WAN	Up	1 KB/s 0 KB/s

Other visible elements include the left sidebar with categories like KerioControl, Dashboard, Interfaces, Traffic Rules, etc., and a bottom toolbar with browser icons and a status bar showing "Status: Running".

20.1.2020

We are done with network configuration and can close the wizard.



We get to users to create a new user.

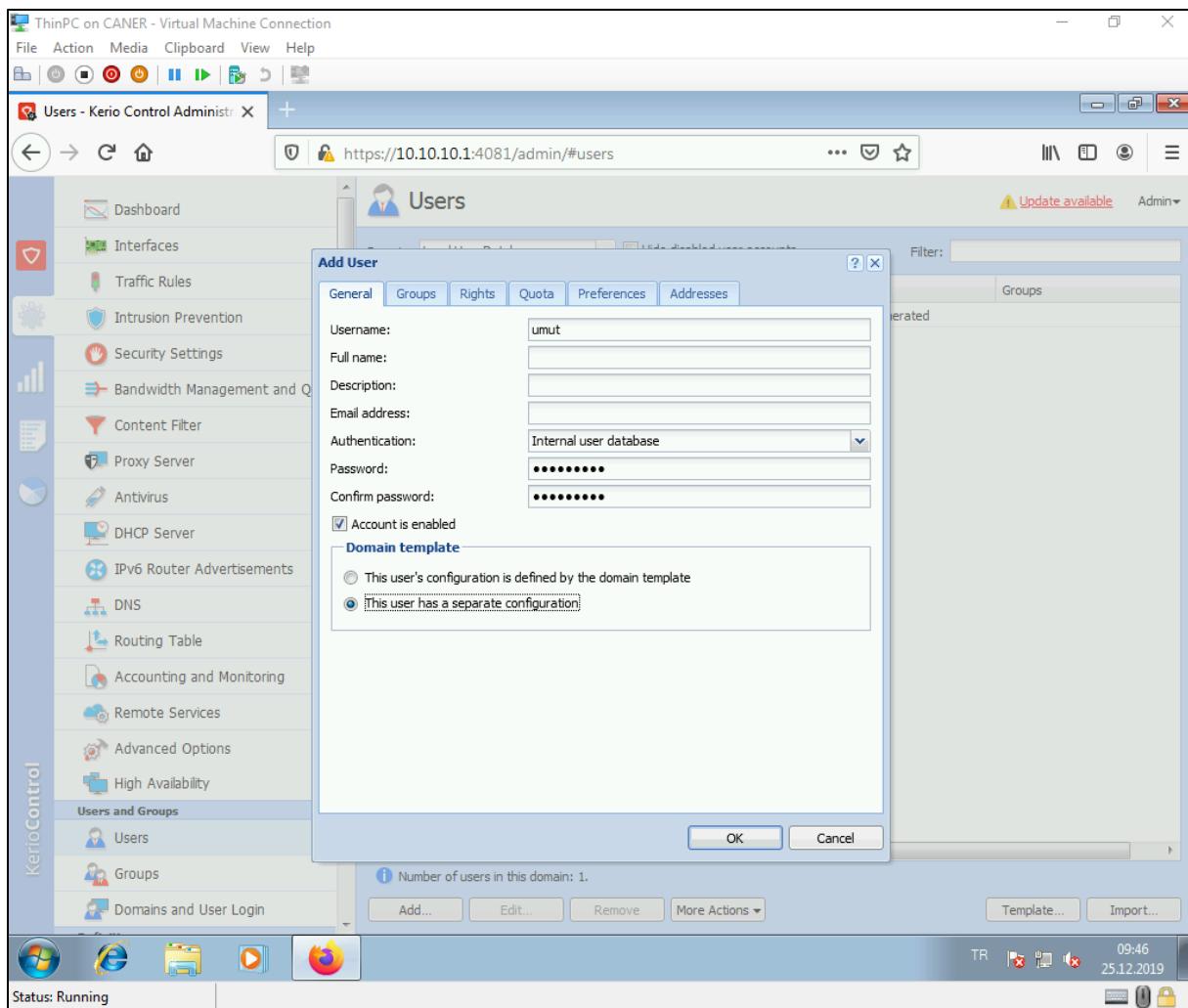
The screenshot shows the Kerio Control Admin interface running on a ThinPC virtual machine. The main window title is "Users - Kerio Control Admin". The URL in the address bar is <https://10.10.10.1:4081/admin/#users>. The left sidebar has a "KerioControl" section with various icons and a "Users and Groups" section where "Users" is selected. The main content area is titled "Users" and shows a table with one row:

Username	Full Name	Description	Groups
Admin		Automatically generated	

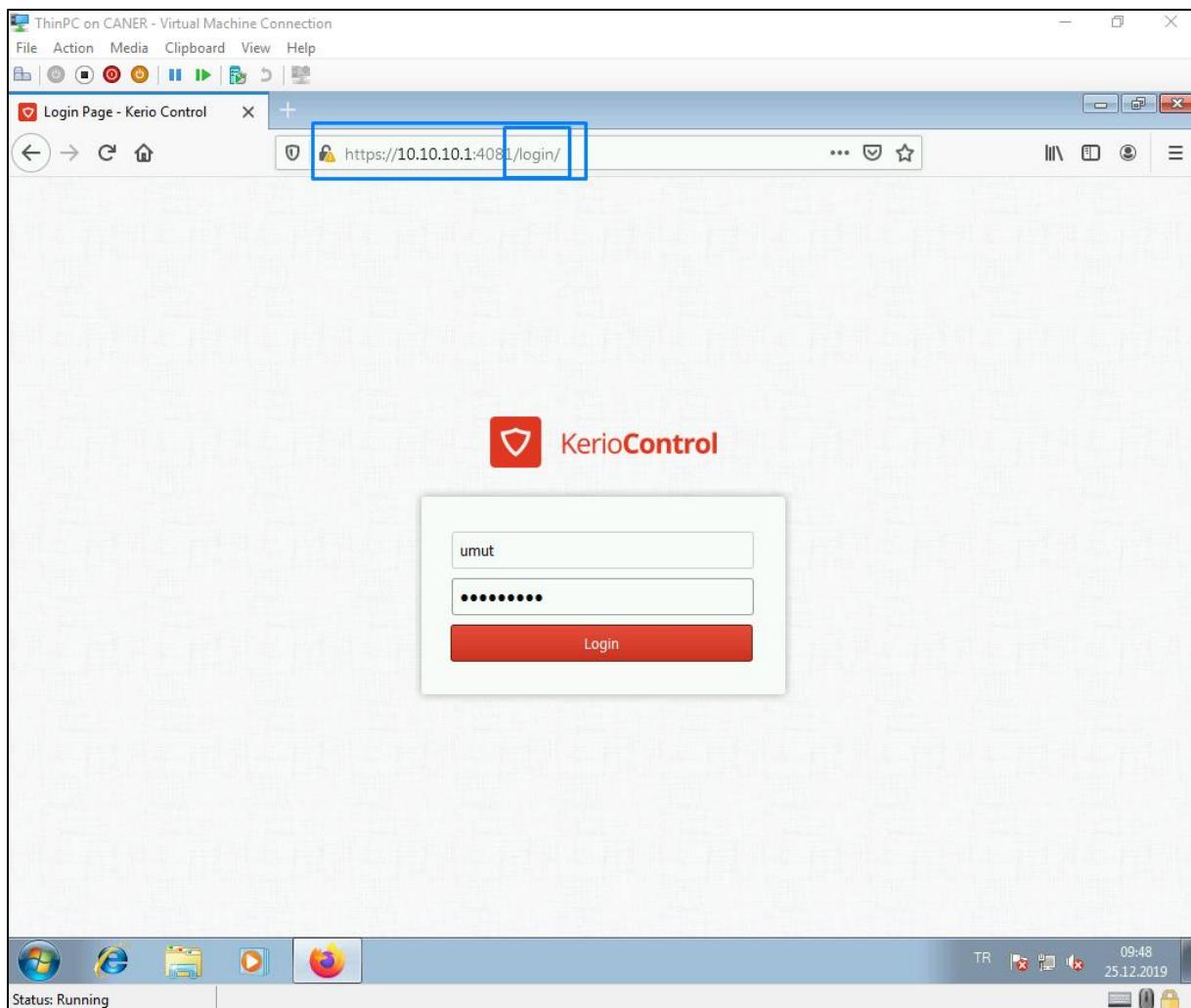
At the bottom of the main window, there are buttons for "Add...", "Edit...", "Remove", and "More Actions". The status bar at the bottom shows "Status: Running" and the system tray includes icons for Taskbar, Firewall, and a lock.

20.1.2020

We enter the user's information.

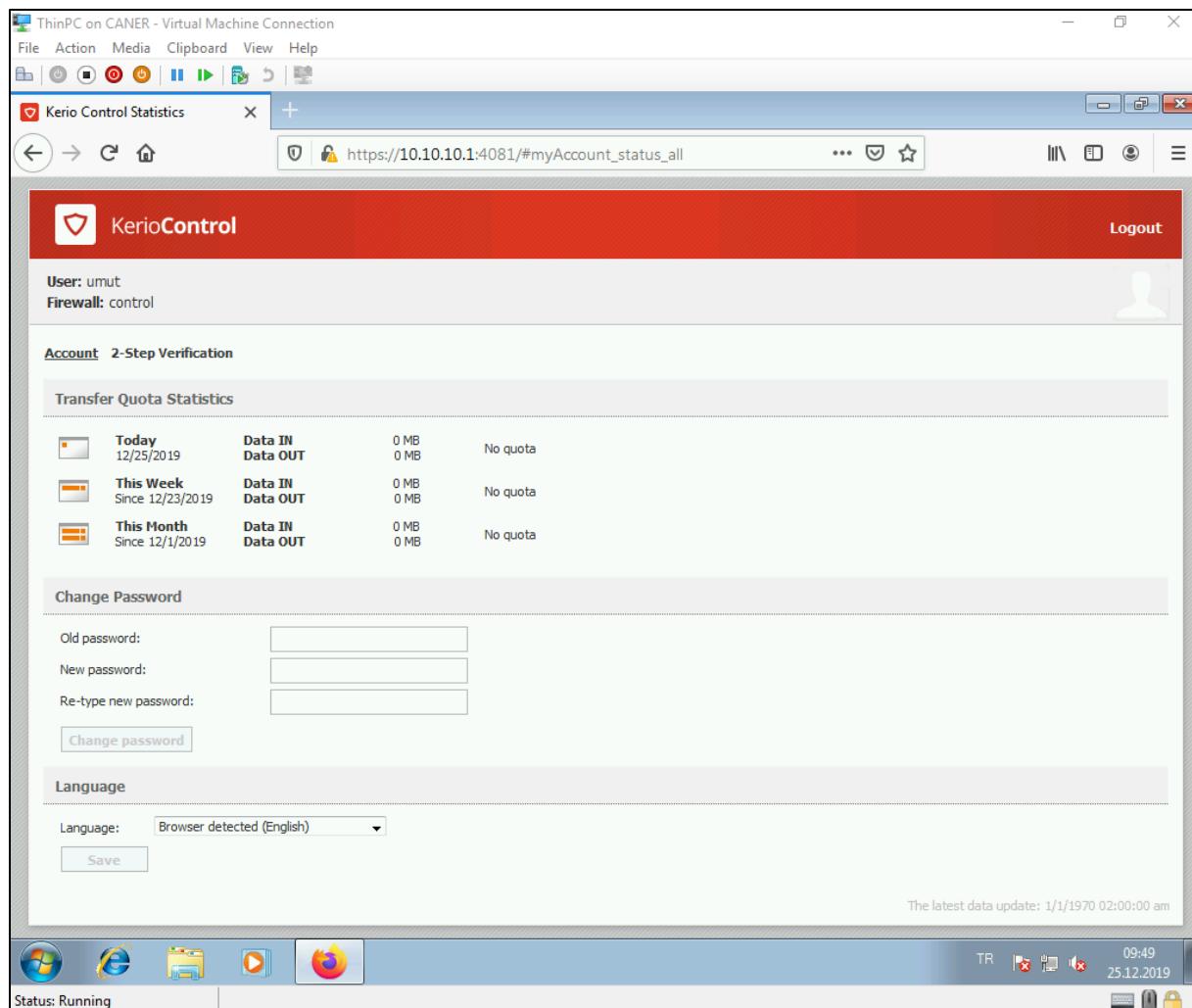


Then, we test logging in as the new user.



20.1.2020

As you can see, a simple user doesn't have access to the admin controls.



But it's possible to change the password.

Now, we want to do port mapping to connect to an internal host via the internet through the firewall. Hence, we get to the traffic rules and add a new one.

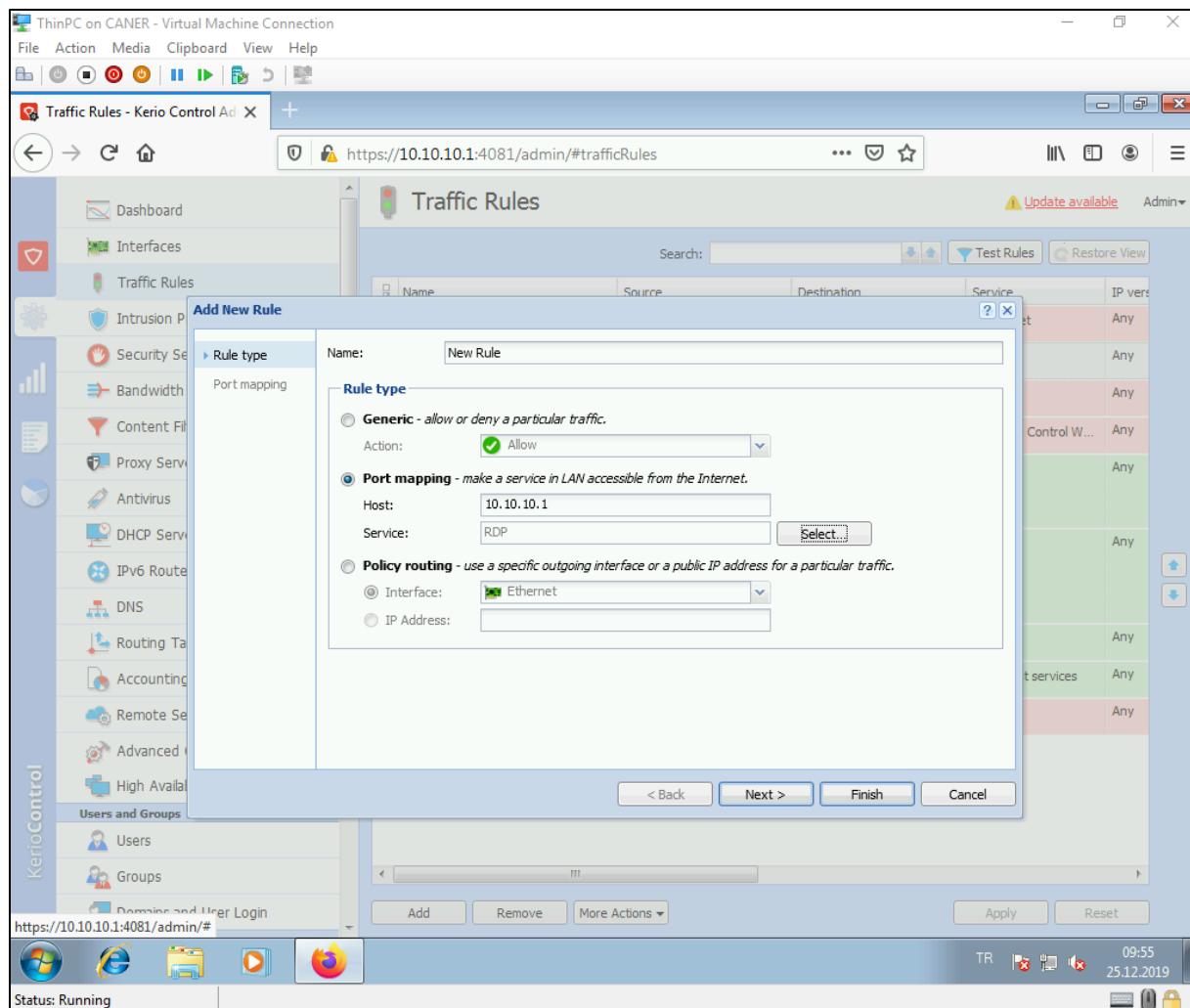
The screenshot shows the Kerio Control Admin interface with the title "Traffic Rules - Kerio Control Admin". The left sidebar has a blue header "KerioControl" and lists various management sections: Dashboard, Interfaces (selected), Traffic Rules (highlighted with a blue box), Intrusion Prevention, Security Settings, Bandwidth Management and QoS, Content Filter, Proxy Server, Antivirus, DHCP Server, IPv6 Router Advertisements, DNS, Routing Table, Accounting and Monitoring, Remote Services, Advanced Options, and High Availability. Below these are "Users and Groups" sections for Users, Groups, and Domains and User Login. The main content area is titled "Traffic Rules" and displays a table of current rules:

Name	Source	Destination	Service	IP version
Service Telnet on Firewall	Any	Firewall	Telnet	Any
Service RDP on Firewall	Any	Firewall	RDP	Any
Service SSH on Firewall	Any	Firewall	SSH	Any
Kerio Control Administration	Any	Firewall	Kerio Control W...	Any
Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any
Local traffic	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Firewall Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any
Firewall traffic	Firewall	Any	Any	Any
Guests traffic	Guest Interfaces	Firewall	Guest services	Any
Block other traffic	Any	Any	Any	Any

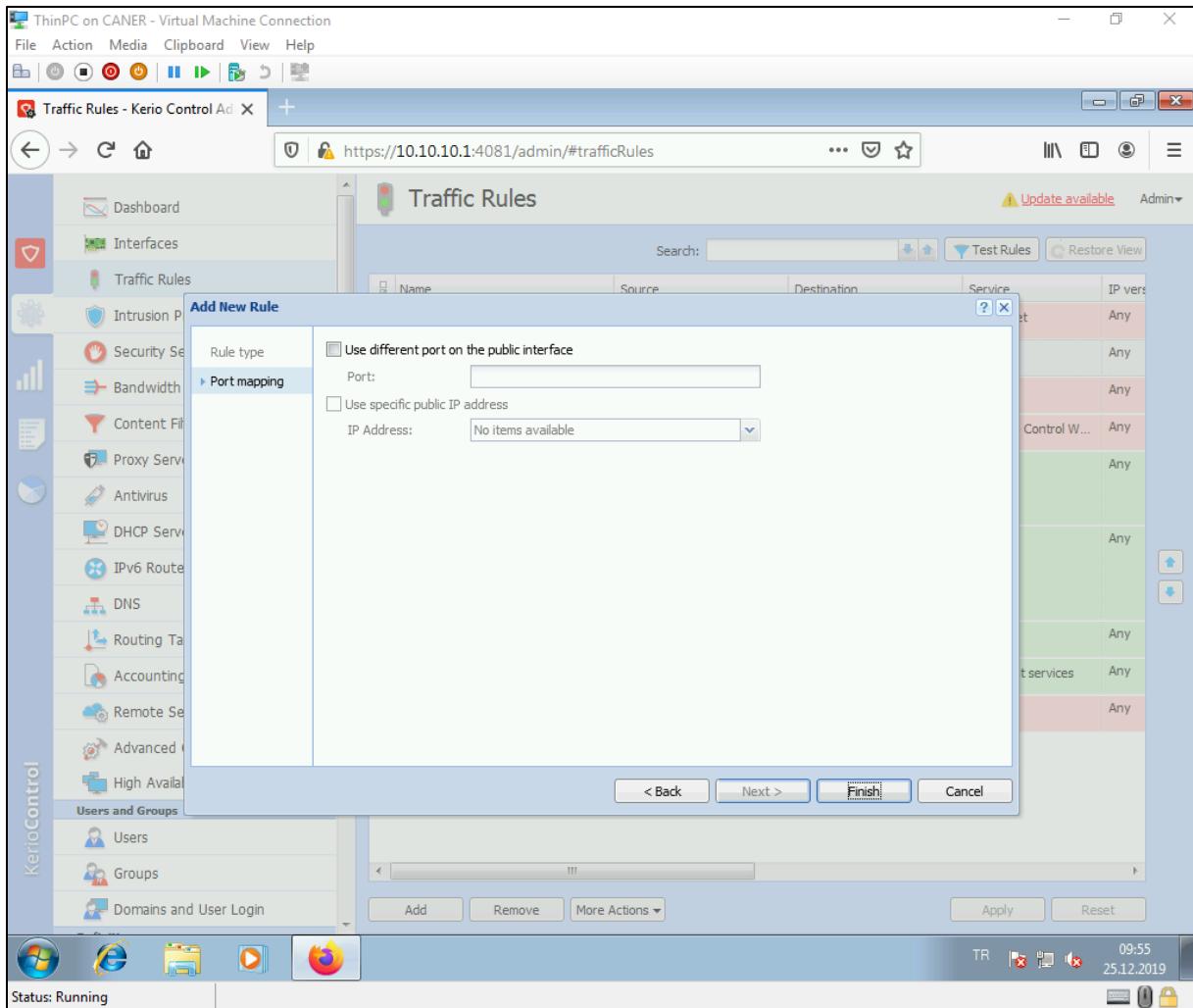
At the bottom of the table are buttons for "Add" (highlighted with a blue box), "Remove", and "More Actions". To the right of the table are "Apply" and "Reset" buttons. The status bar at the bottom shows "Status: Running" and the date/time "09:54 25.12.2019".

20.1.2020

We map every RDP request to a specific host. This was called port forwarding in pfSense.



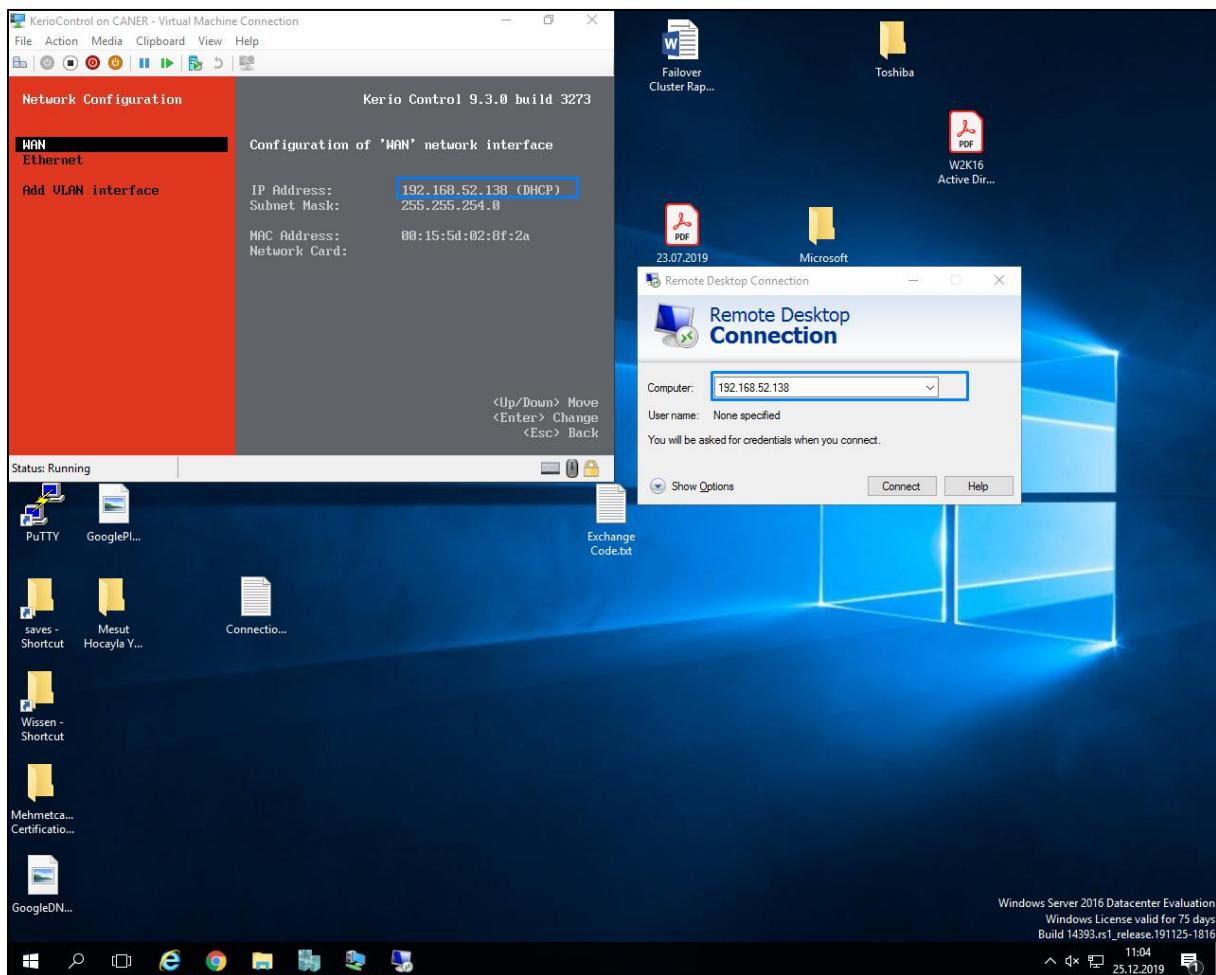
We could even use different port outside or inside of the firewall.



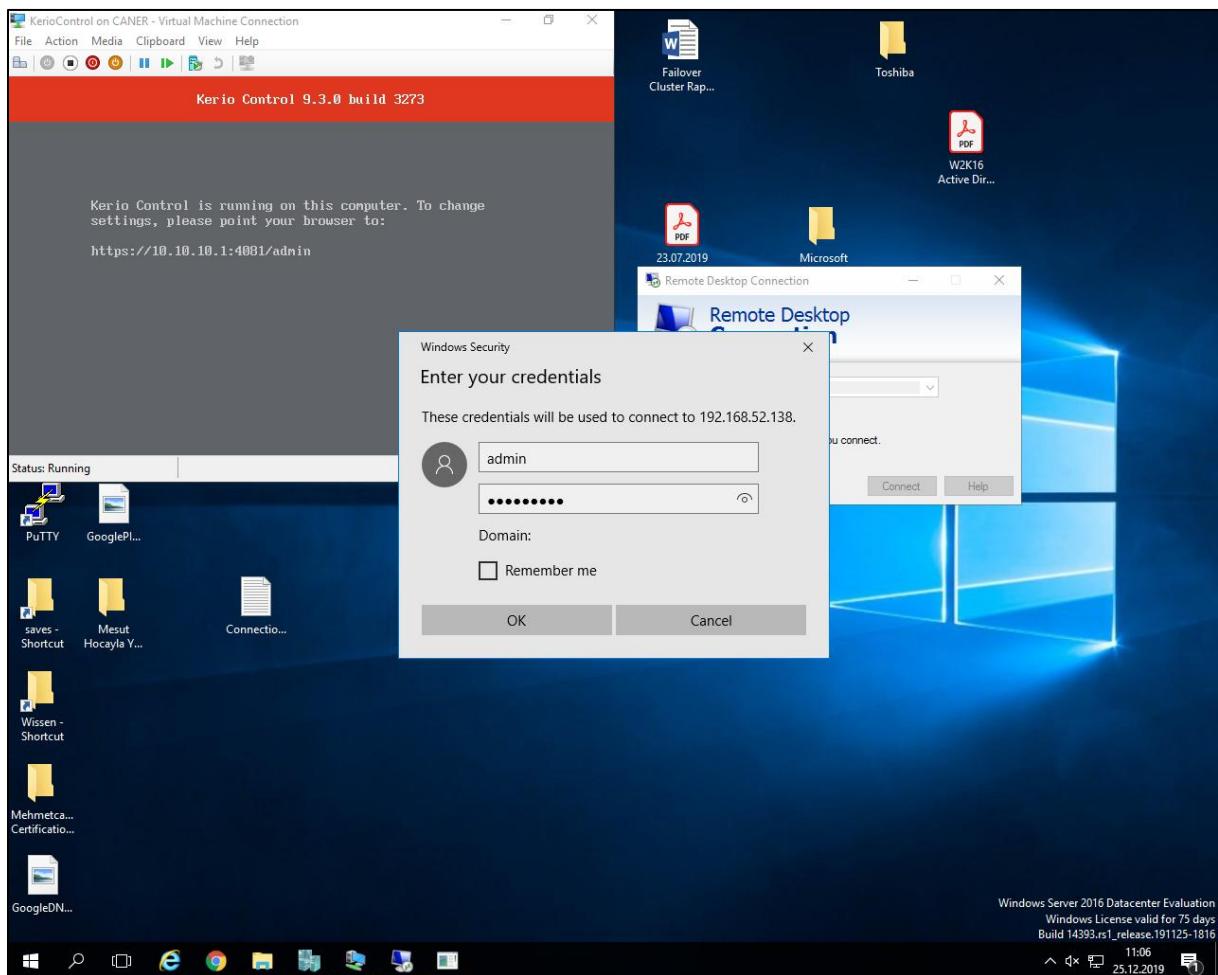
But we choose not to overcomplicate it.

20.1.2020

When we use RDP using the WAN IP address of the firewall, ...

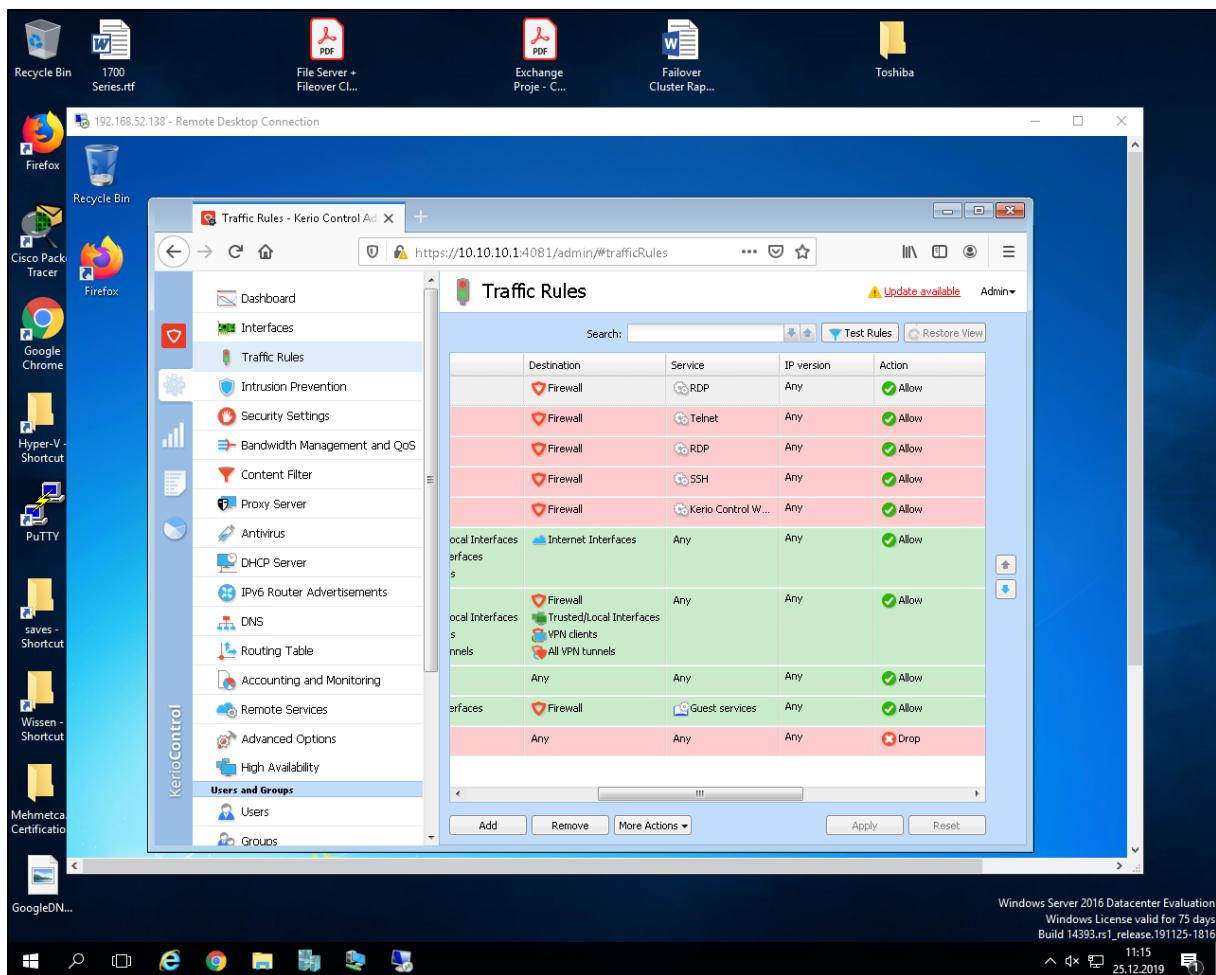


... we are asked to log in as an account of the host.

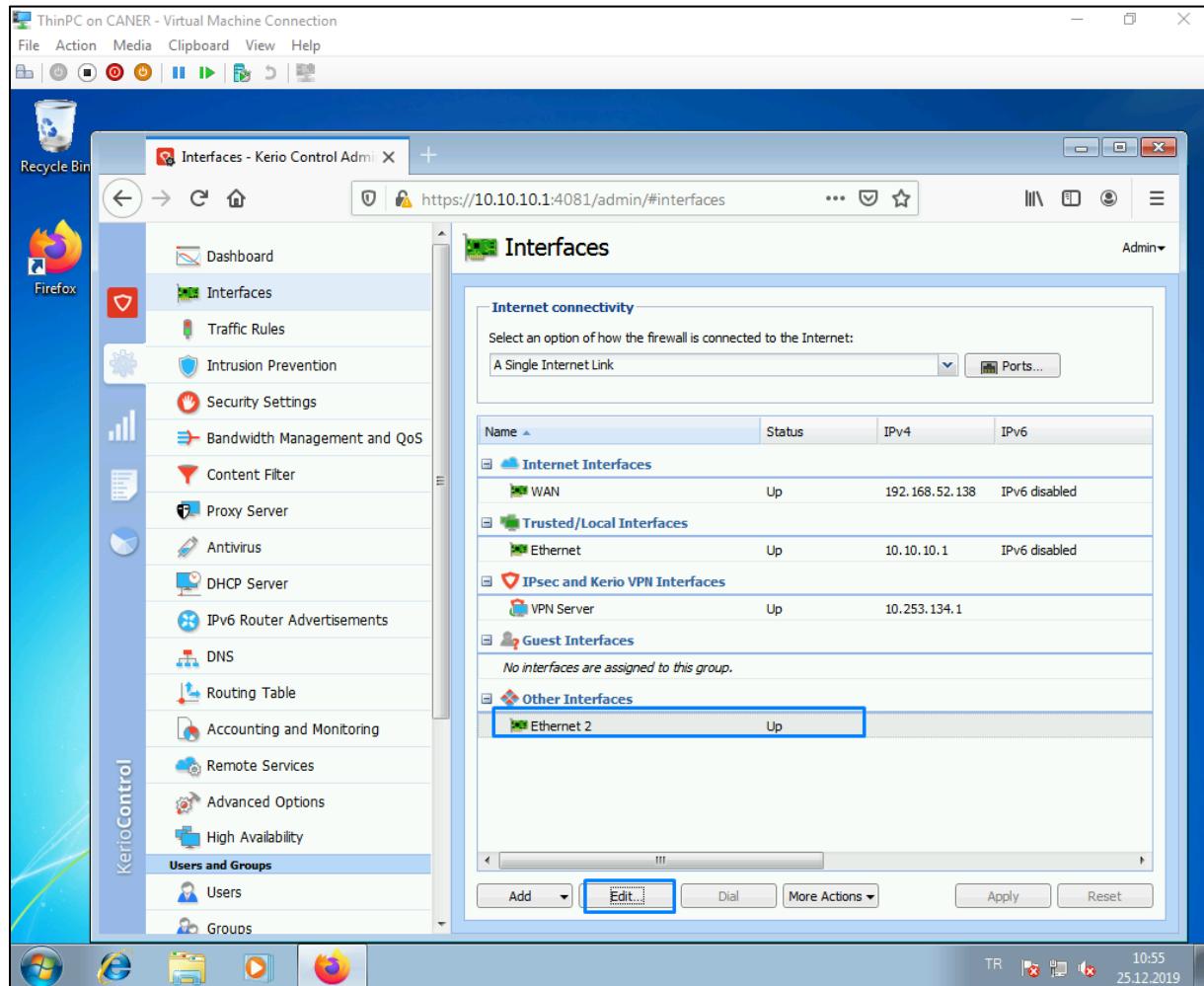


20.1.2020

Then, we're in.

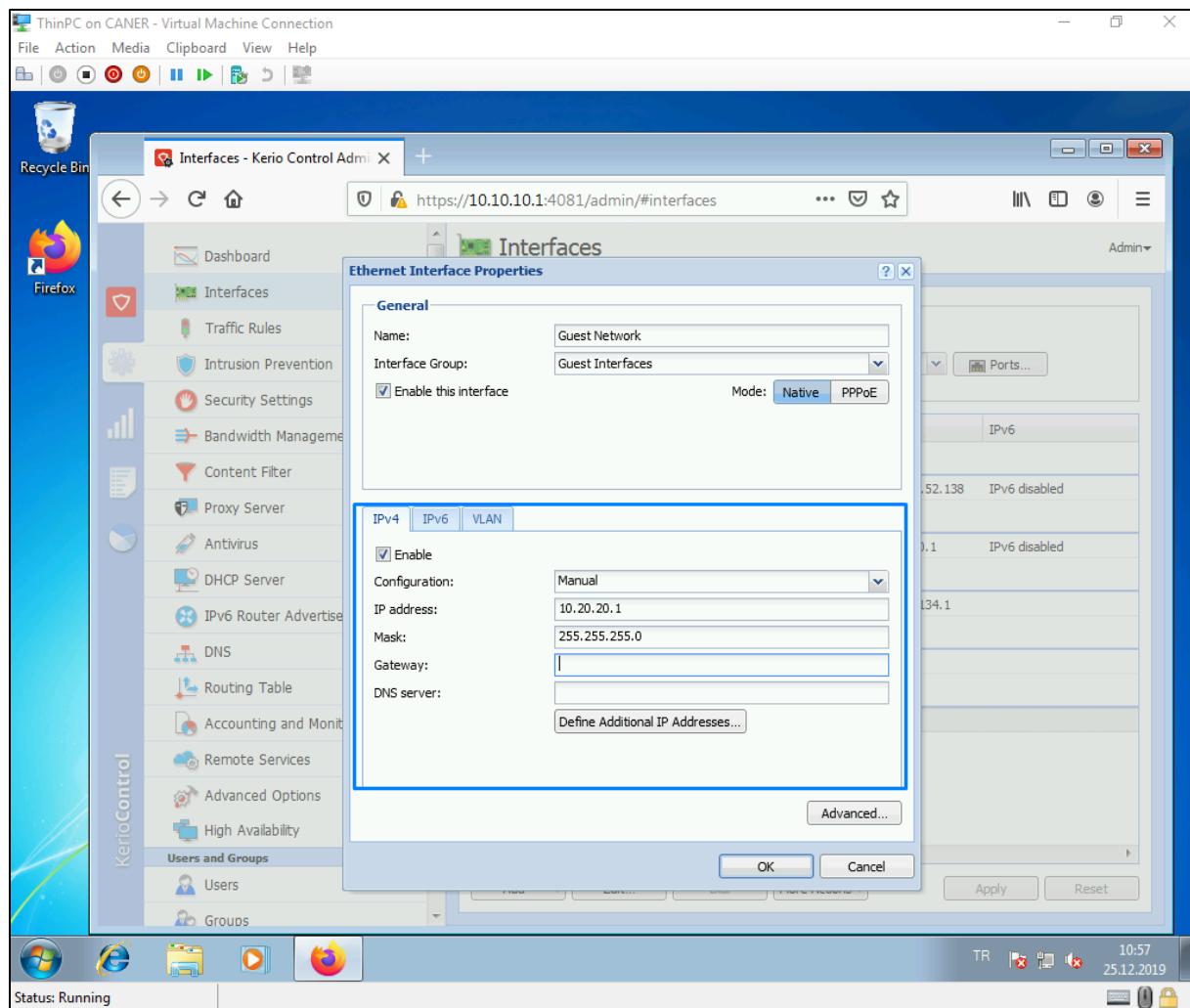


Now, we have a portal for our users but what if we also want to enable guest users to come and use the wi-fi of our company. We create a new interface.

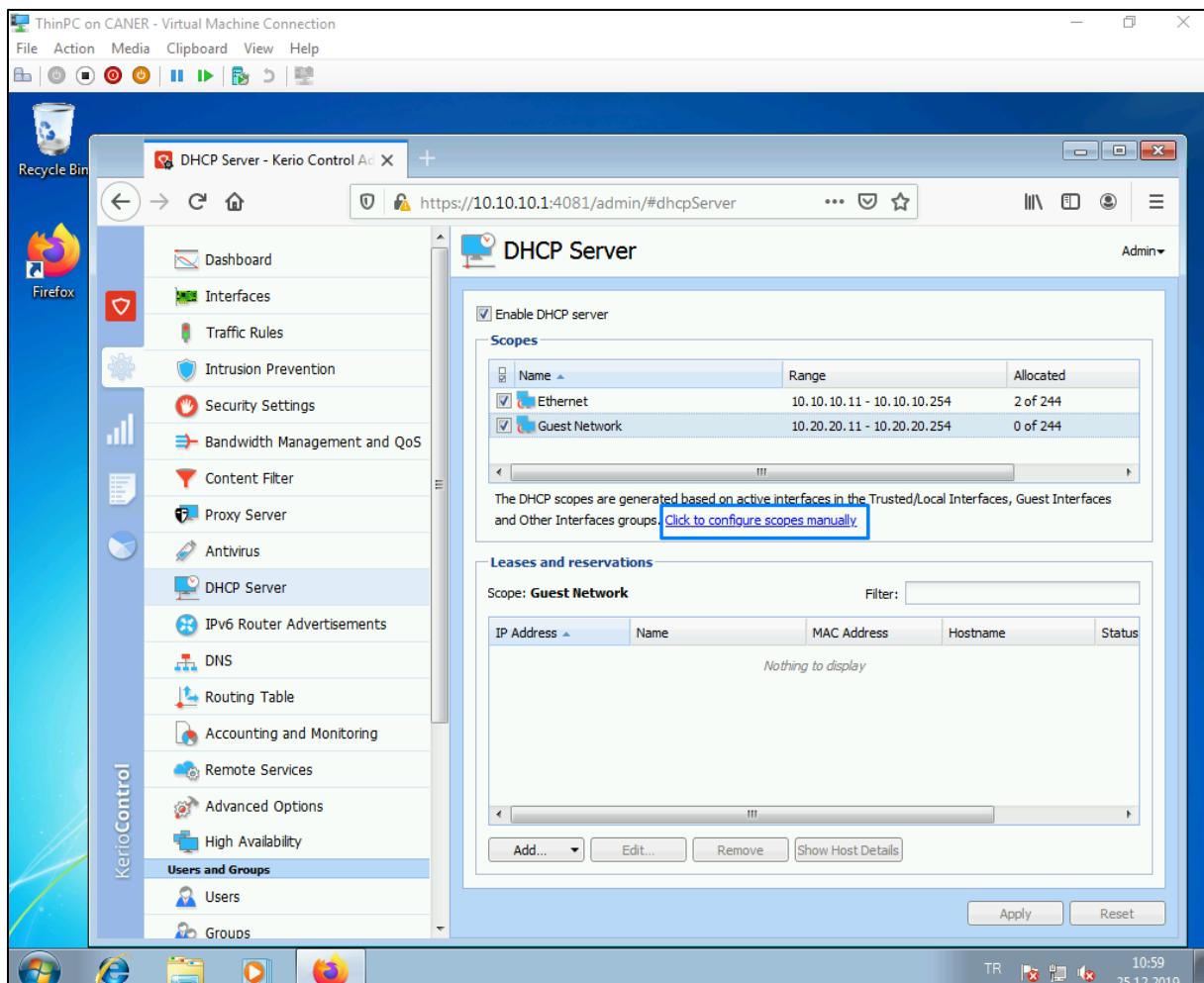


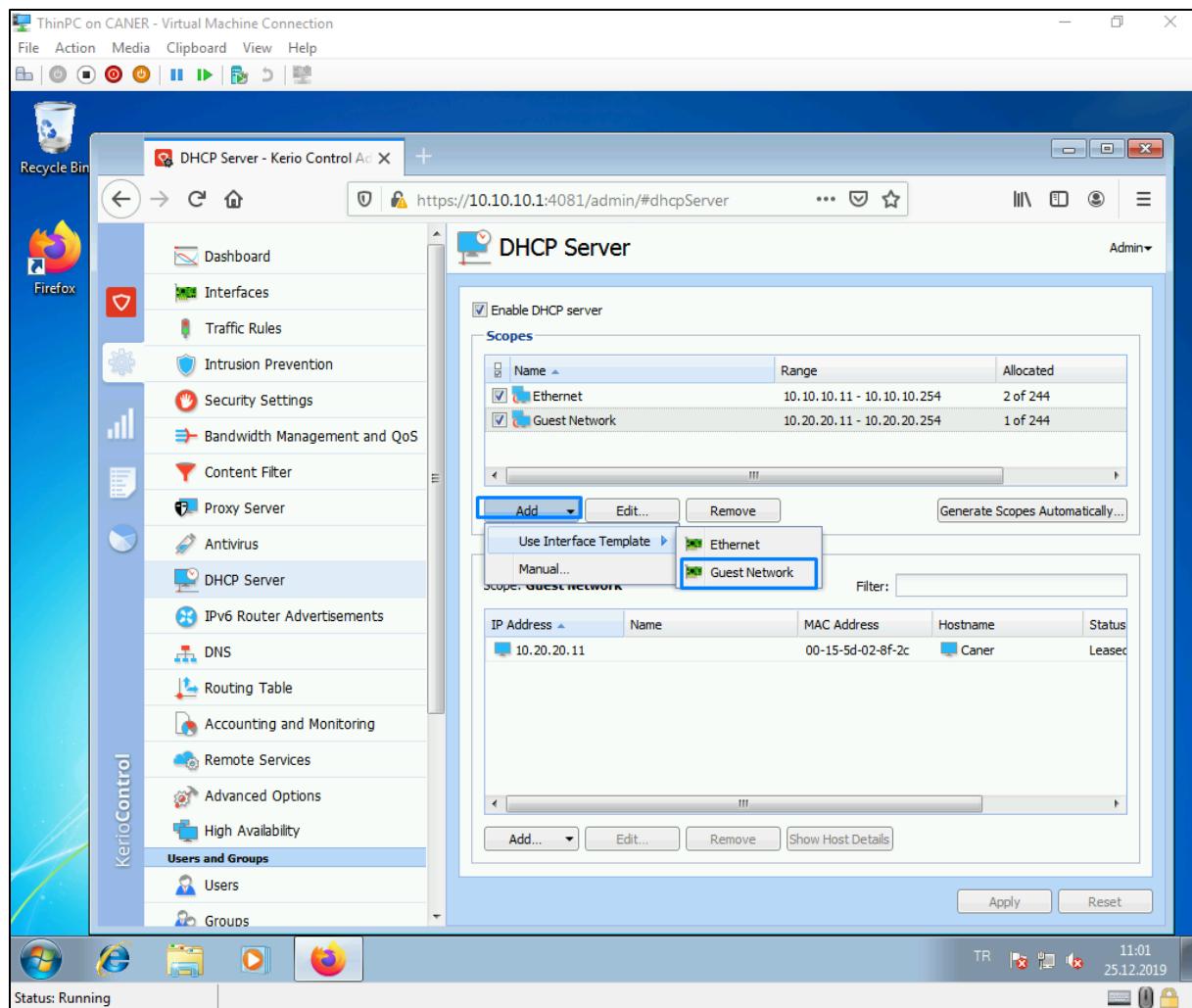
20.1.2020

We edit it to be a guest interface and give a determined guest subnetwork.

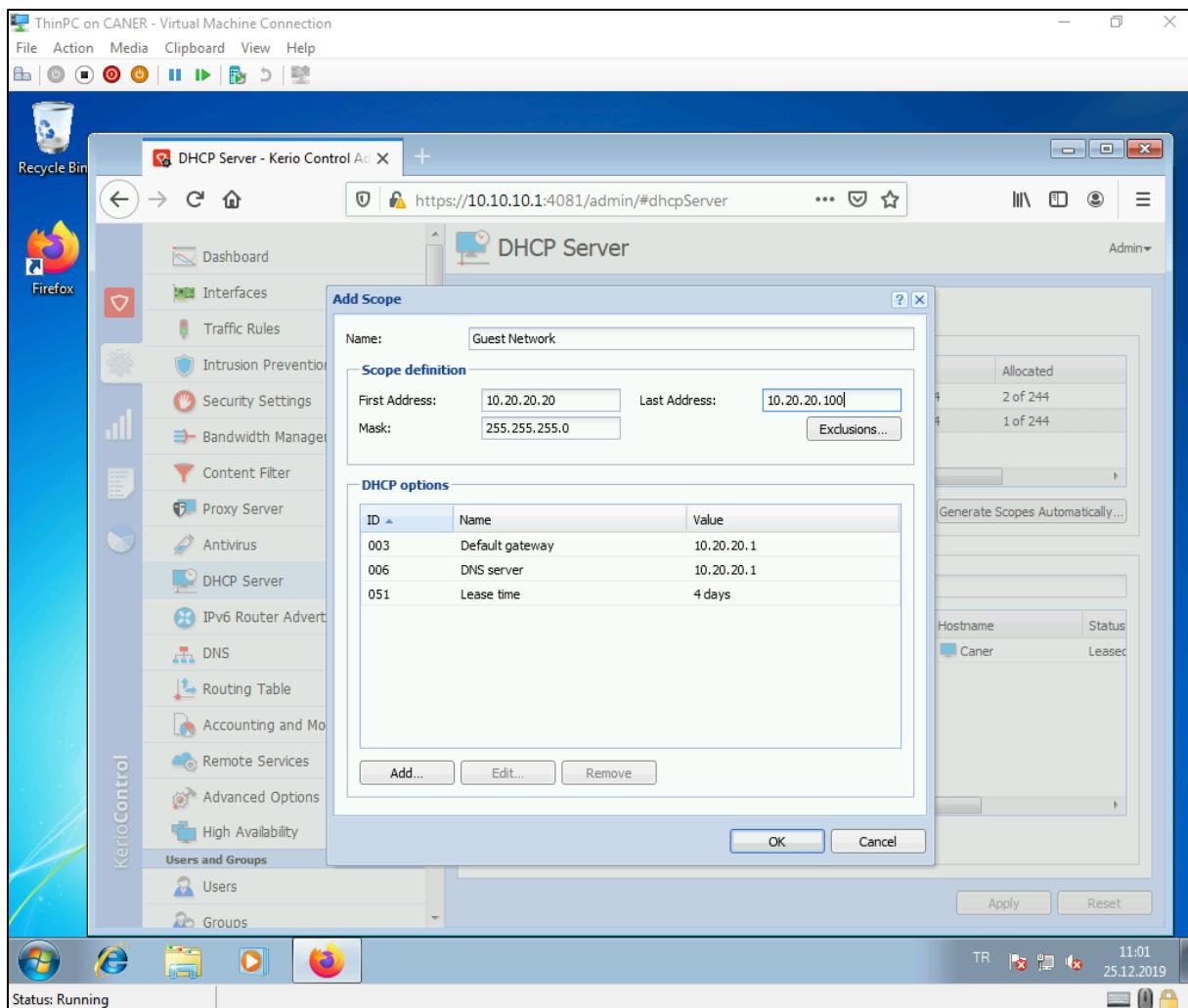


We get to the DHCP server to start a scope for the guest network as well.



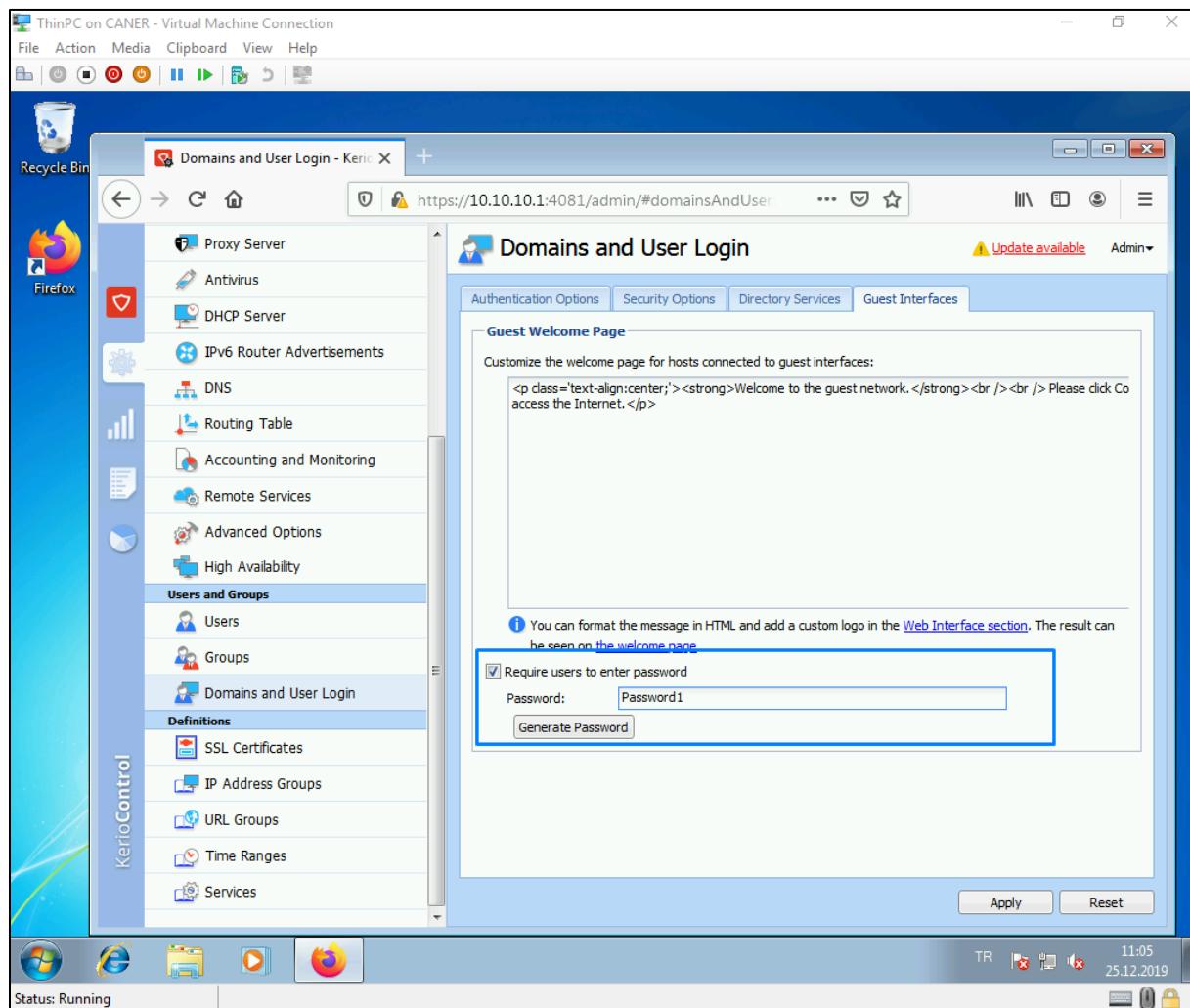


We determine the start and the end of the scope.



20.1.2020

We, then require all of the guests to enter a password to connect.



Now, let's ban access to some certain gaming websites so that work efficiency is optimal.

The screenshot shows the Kerio Control Content Filter interface. The left sidebar lists various system settings like Dashboard, Interfaces, Traffic Rules, and Content Filter (which is selected). The main content area is titled "Content Filter" and displays a table of "Content Rules".

Name	Detected content	Source	Action
<input checked="" type="checkbox"/> Kerio sites	kerio.com	Any	<input checked="" type="checkbox"/> Allow <input type="checkbox"/> Block
<input checked="" type="checkbox"/> Advertisements and banners	Ads/banners	Any	<input type="checkbox"/> Deny <input checked="" type="checkbox"/> Allow
<input checked="" type="checkbox"/> Updates and MS Windows activa...	Automatic Updates	Any	<input checked="" type="checkbox"/> Allow <input type="checkbox"/> Block
<input checked="" type="checkbox"/> Kerio Control Web Filter categori...	<ul style="list-style-type: none"> ⚠️ Anonymizer ⚠️ Botnet ⚠️ Command and Control Centers ⚠️ Compromised ⚠️ Criminal Skills ⚠️ Hacking ⚠️ Malware Call-Home ⚠️ Malware Distribution Point ⚠️ Phishing/Fraud ...and 3 more 	Any	<input type="checkbox"/> Deny <input checked="" type="checkbox"/> Allow
<input type="checkbox"/> Audio and video files	<ul style="list-style-type: none"> ⚠️ Audio files ⚠️ Video files 	Any	<input type="checkbox"/> Deny <input checked="" type="checkbox"/> Allow
<input type="checkbox"/> Peer-to-Peer traffic	⚠️ Peer-to-Peer	Any	<input type="checkbox"/> Deny <input checked="" type="checkbox"/> Allow
<input type="checkbox"/> Allow other traffic	Any	Any	<input checked="" type="checkbox"/> Allow

At the bottom, there are buttons for "Add", "Remove", and "More Actions".

20.1.2020

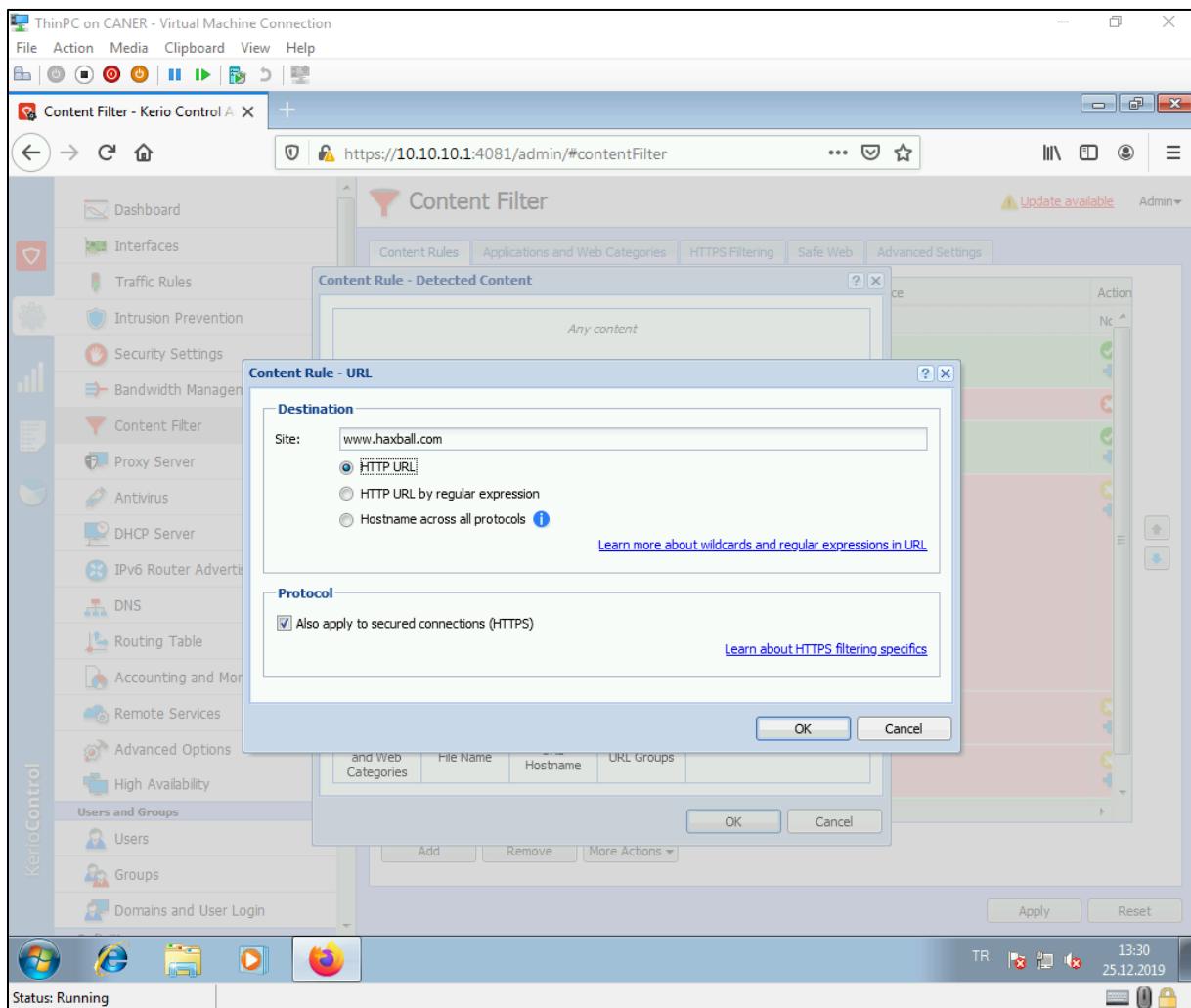
We create a new content rule and edit it.

The screenshot shows the Kerio Control Content Filter interface. The left sidebar lists various system management options like Dashboard, Interfaces, Traffic Rules, and Content Filter. The Content Filter section is selected. The main pane displays a table of content rules:

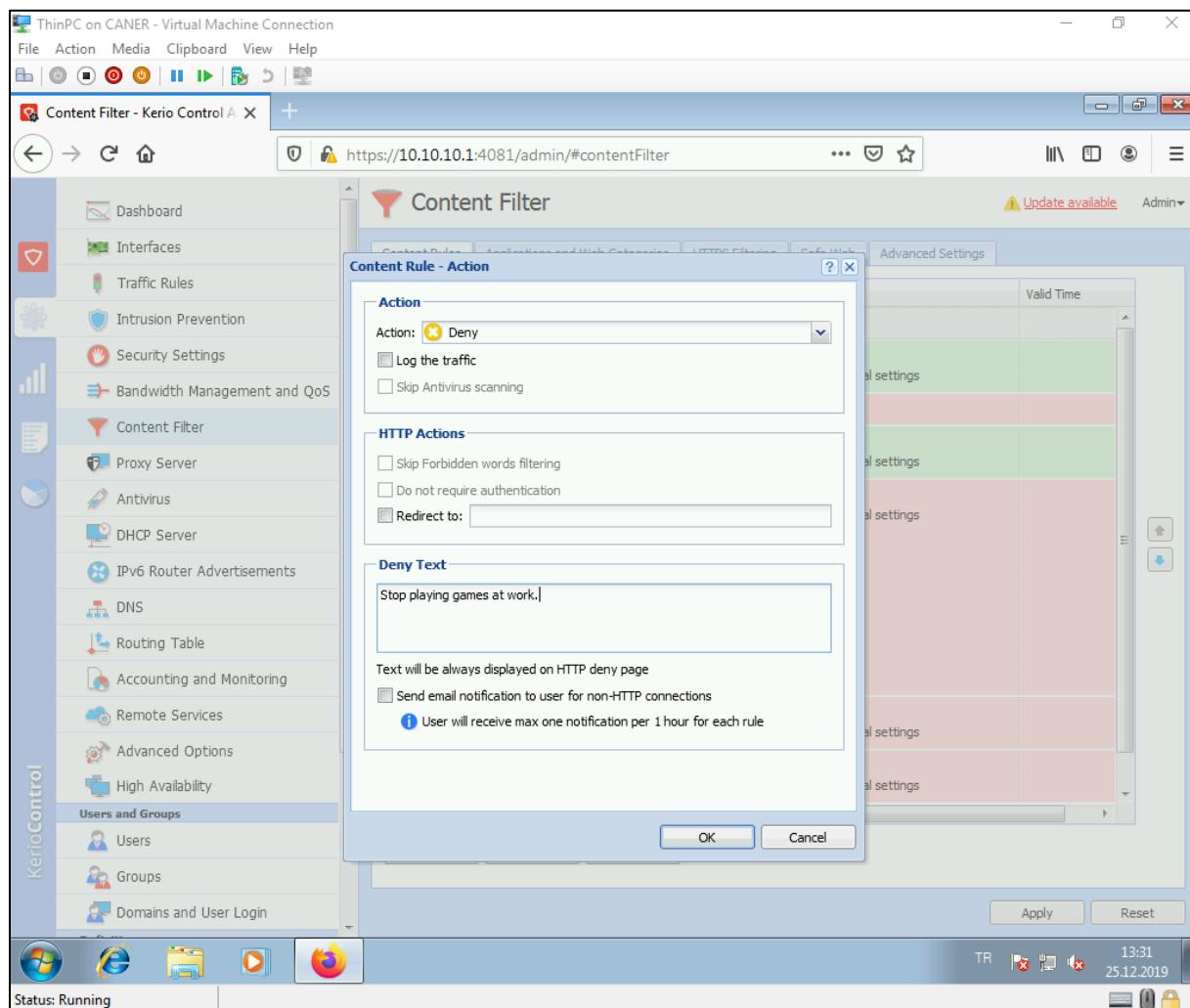
Name	Detected content	Source	Action
Haxball Ban	Any	Any	[Edit]
Kerio sites	kerio.com	Any	[Edit]
Advertisements and banners	Ads/banners	Any	[Edit]
Updates and MS Windows activ...	Automatic Updates	Any	[Edit]
Kerio Control Web Filter categor...	Anonymizer Botnet Command and Control Centers Compromised Criminal Skills Hacking Malware Call-Home Phishing/Fraud ...and 3 more	Any	[Edit]
Audio and video files	Audio files Video files	Any	[Edit]
Peer-to-Peer traffic	Peer-to-Peer	Any	[Edit]

At the bottom, there are buttons for Add, Remove, More Actions, Apply, and Reset. The status bar at the bottom indicates "Status: Running".

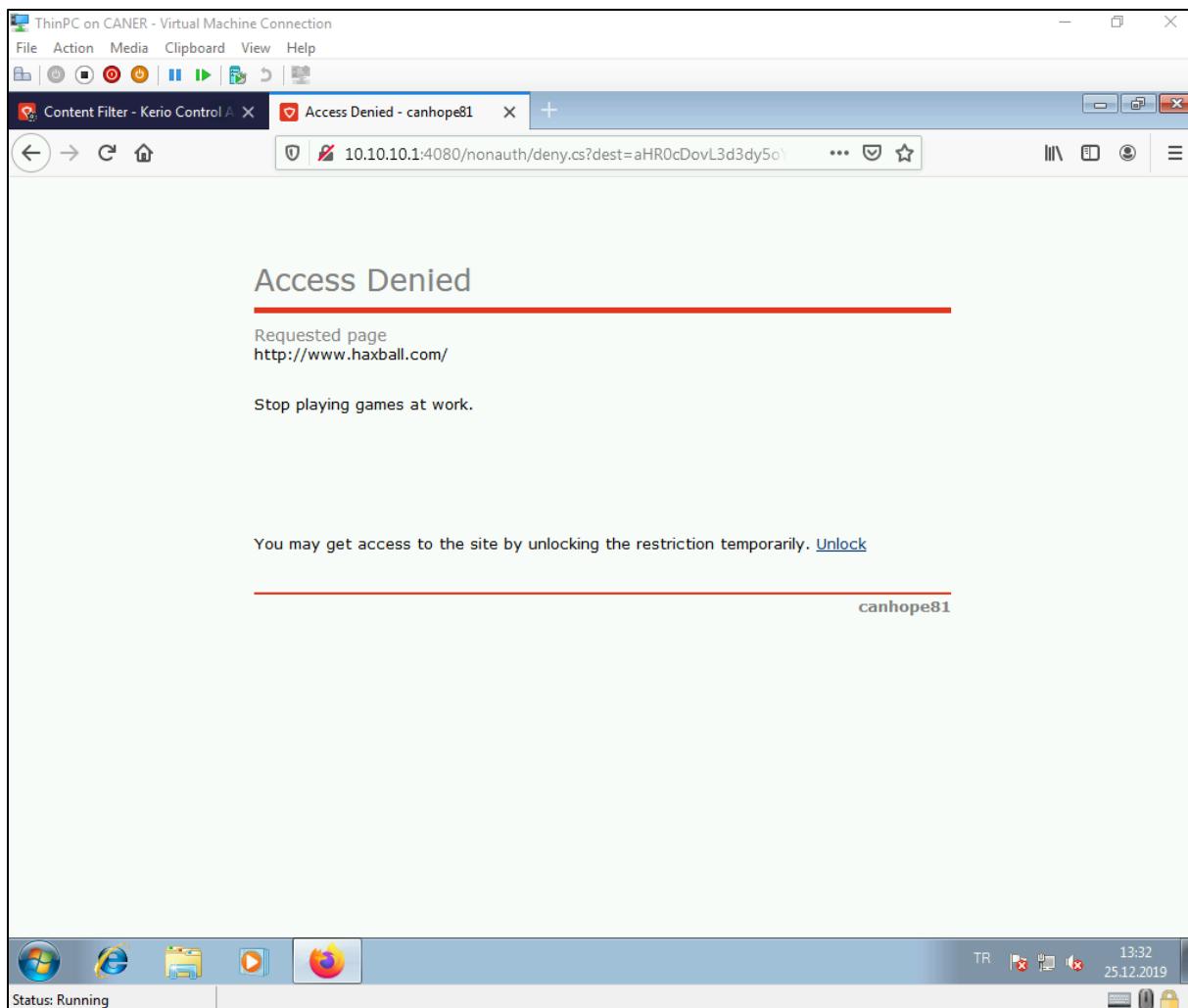
We apply it to the destination of www.haxball.com.



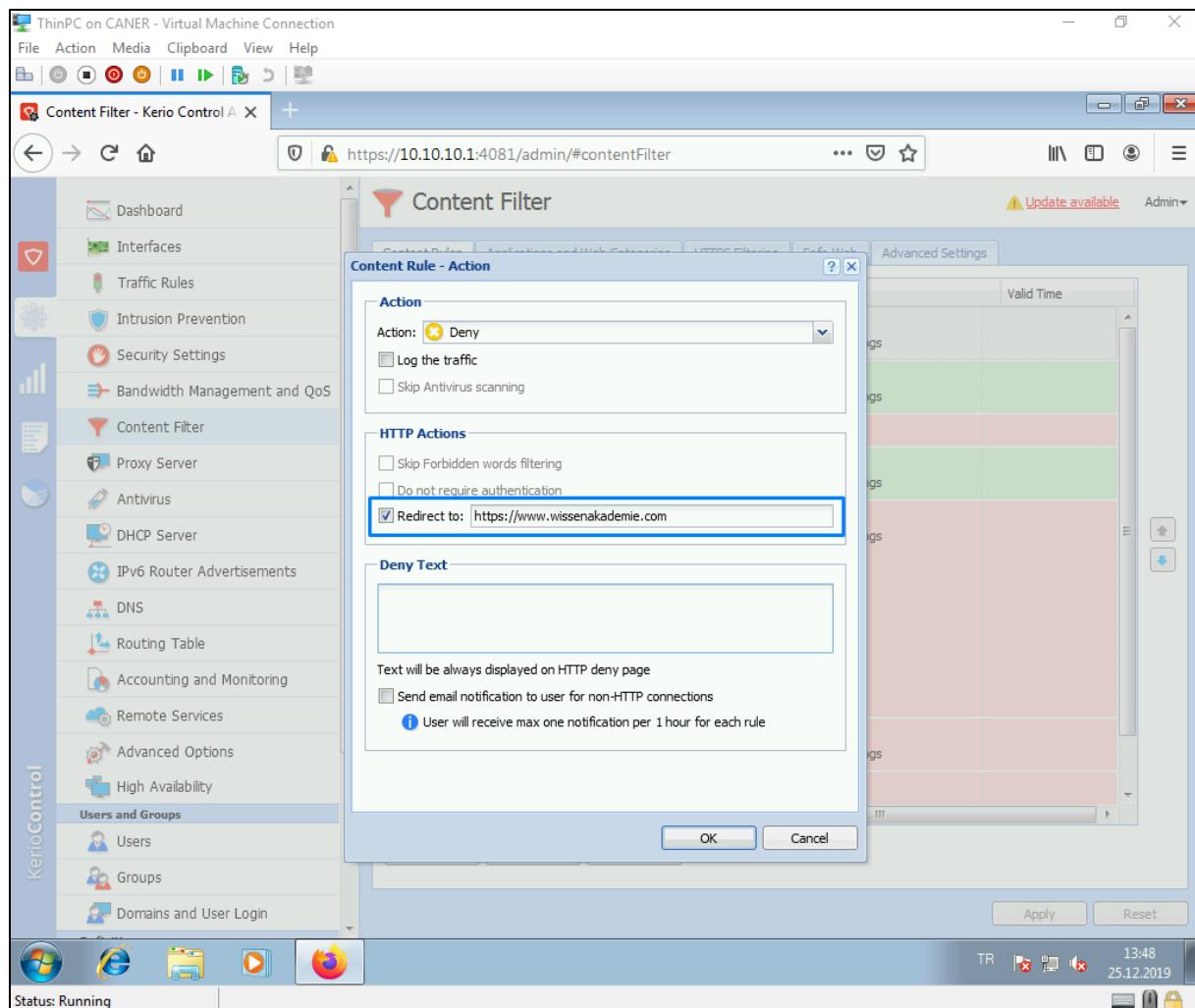
We choose the action to DENY access and let them know that we know they just tried to play games while at work. We could also use the action to DROP to not show a page that says we blocked access. That might also frustrate them to try over and over again. Since we believe that would be a waste of valuable production time, we decided to simply DENY.

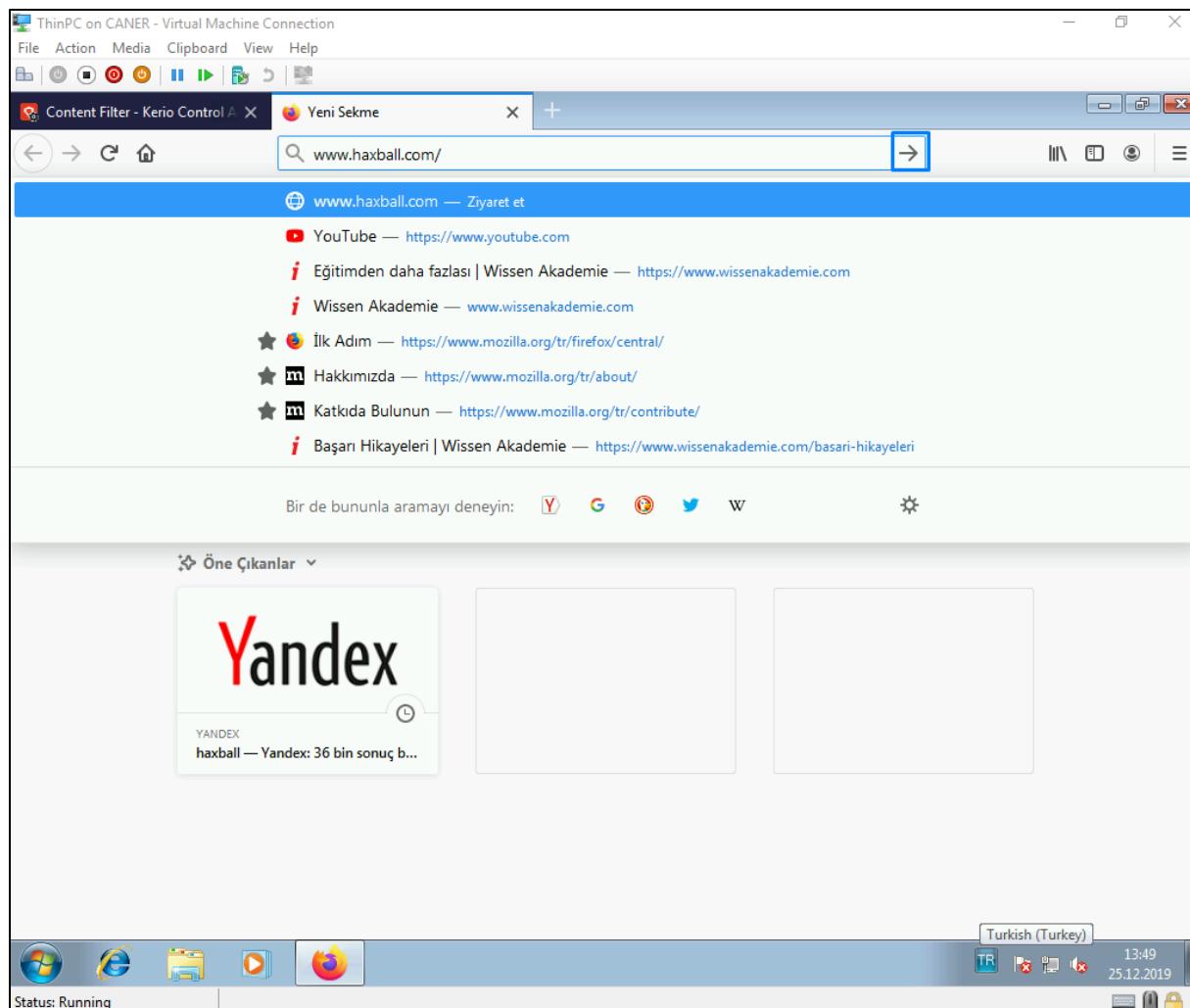


When the user tries to connect to the website, they see this page instead.



We could also redirect the traffic to our company's website.





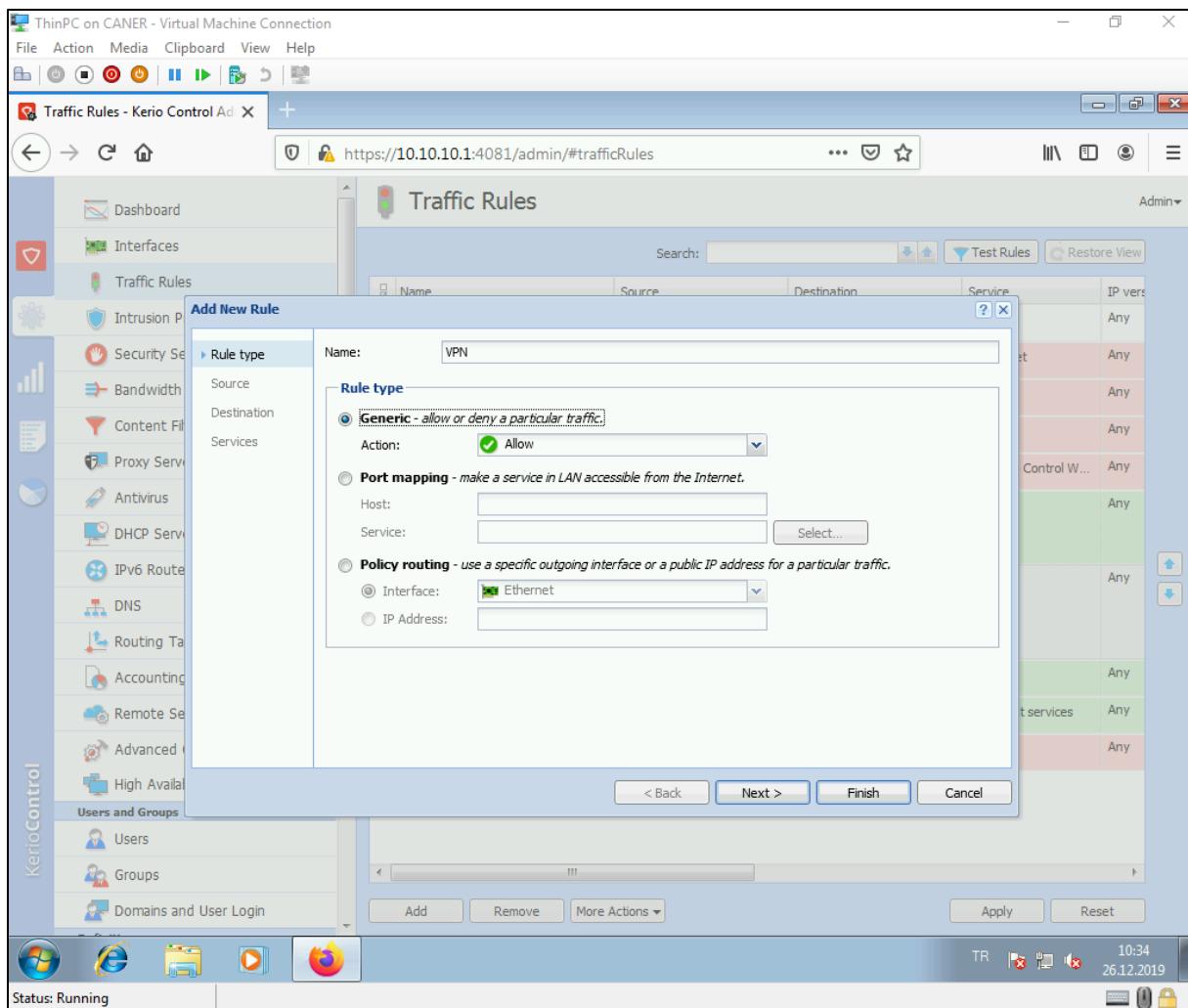
The screenshot shows a web browser window titled "ThinPC on CANER - Virtual Machine Connection". The address bar displays "Content Filter - Kerio Control A" and the URL "https://www.wissenakademie.com". The page content is the homepage of Wissen Akademie, featuring a red header with the logo and navigation links: WISSEN, EĞİTİM PROGRAMLARIMIZ, REFERANSLARIMIZ, PARTNERLERİMİZ, BLOG, IK, İLETİŞİM. Below the header, there is a search bar with the placeholder "Ara" and a list of filter categories: YAZILIM, MOBİL, SİSTEM, NETWORK, ARAYÜZ, TEKNİK ÇİZİM, OFİS, ERP, CMS, ANİMASYON, GÜVENLİK, YÖNETİM, CLOUD. To the right, there is a contact form with fields for Adınız Soyadınız, Telefon, E-Posta, Mesajınız, and a checkbox for KVKK kapsamında kişisel bilgilerimi paylaştığımı kabul ediyorum. At the bottom right of the page, there is a "GÖNDER" button. On the left side, there is a section titled "Etkinlik Takvimi" (Event Calendar) showing two events: "Python ile Yapay Zeka Uygulamaları" on Saturday, December 21st, and "Proje Yönetimi" on Sunday, December 18th. The browser status bar at the bottom shows "static.hotjar.com okunuyor" and various system icons.

Now, let's try setting a VPN connection to another site that uses Kerio Control also known as a site-to-site VPN. First thing to do is to allow the traffic rules for it.

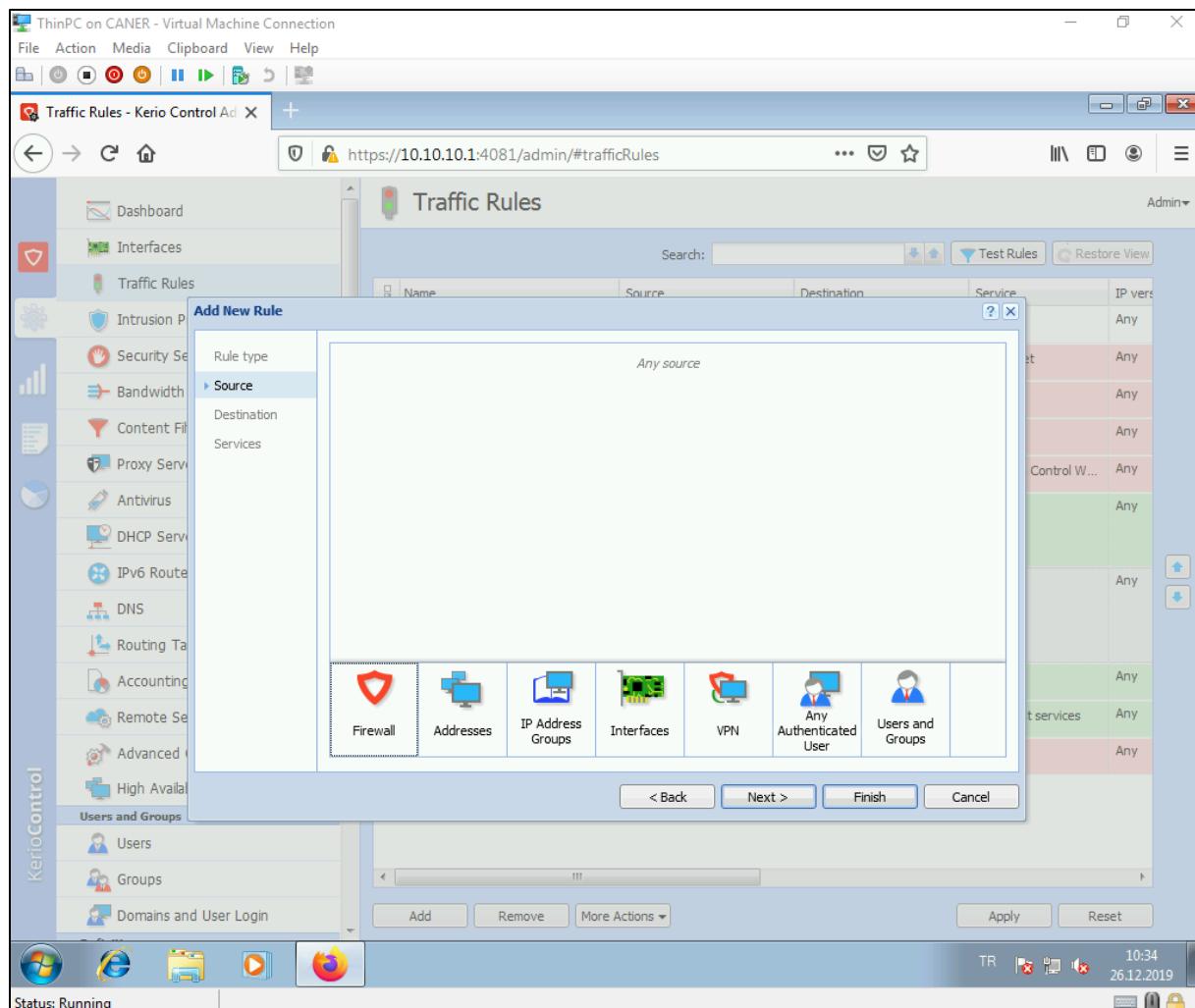
The screenshot shows the Kerio Control Admin interface with the title "Traffic Rules - Kerio Control Admin". The left sidebar lists various system components like Dashboard, Interfaces, Traffic Rules, and others. The main pane displays a table of traffic rules with columns for Name, Source, Destination, Service, and IP version. Several rules are listed, including "RDP Port Mapping to ThinPc", "Service Telnet on Firewall", "Service RDP on Firewall", "Service SSH on Firewall", "Kerio Control Administration", "Internet access (NAT)", "Local traffic", "Firewall traffic", "Guests traffic", and "Block other traffic". At the bottom of the table, there are buttons for "Add", "Remove", and "More Actions". A red box highlights the "Add" button. The status bar at the bottom indicates "Status: Running" and the date/time "26.12.2019 10:33".

20.1.2020

We set ALLOW as the action, ...

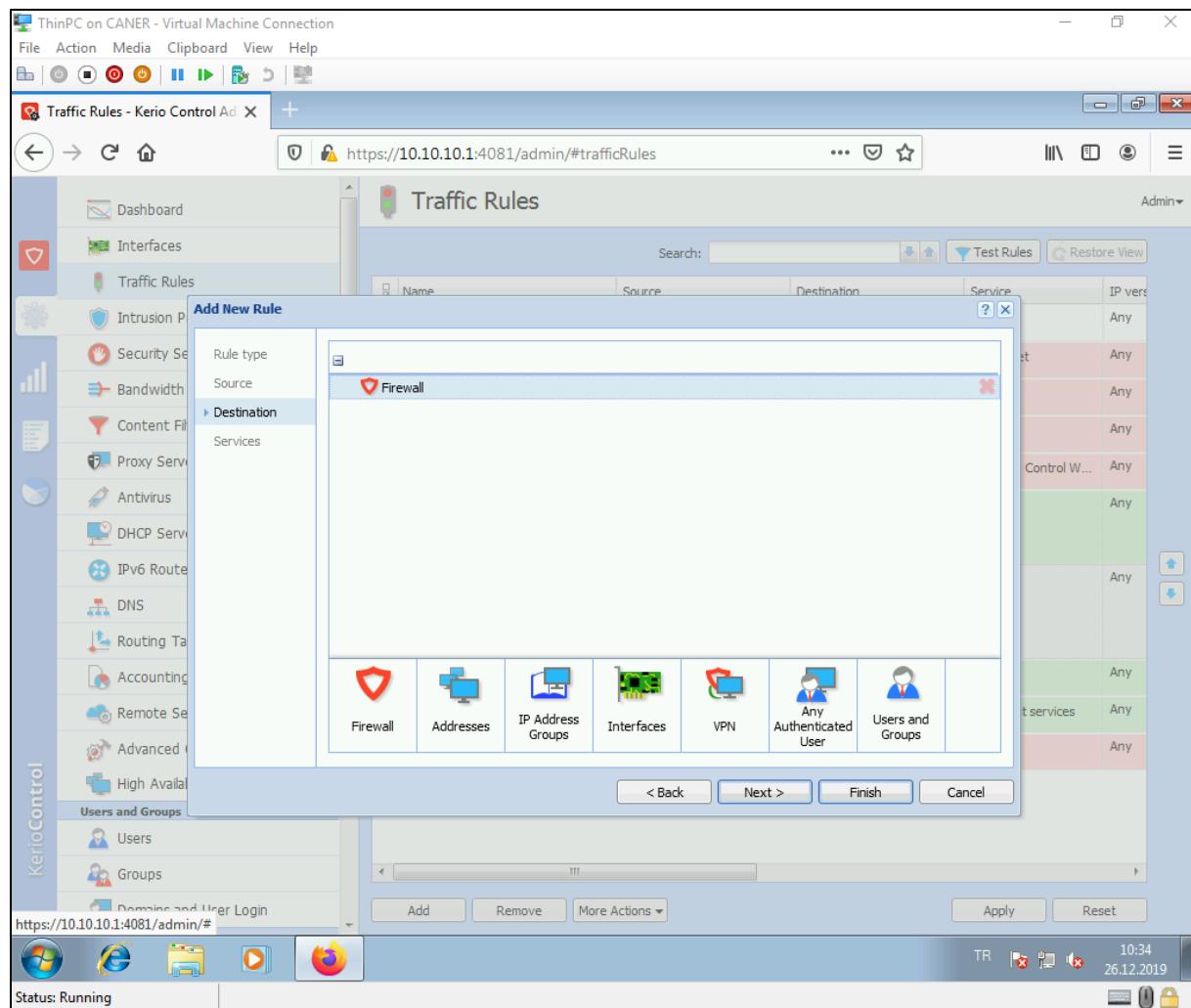


... source as any, ...

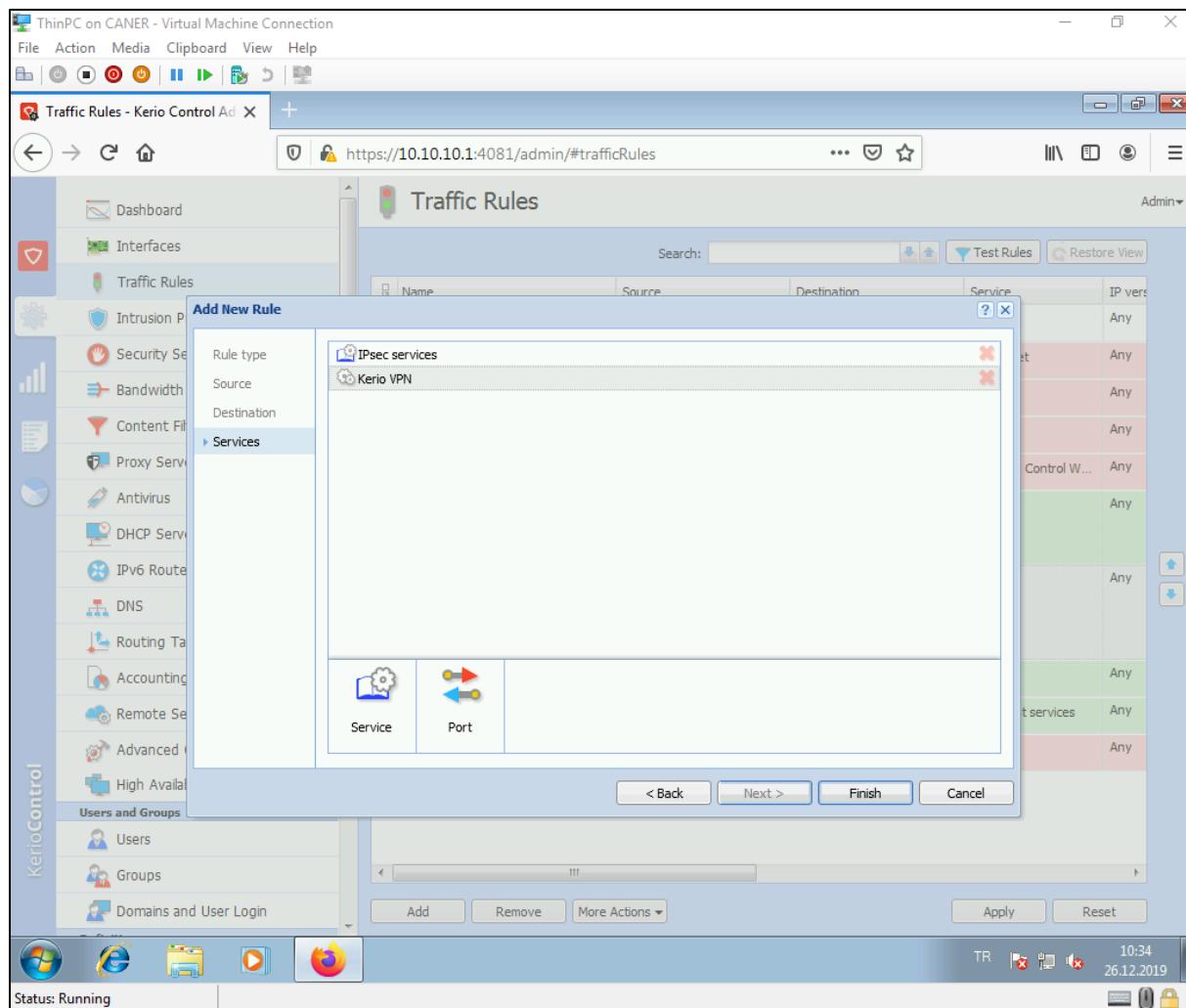


20.1.2020

... this firewall as destination ...



... and only Kerio VPN and IPsec as services for this rule.



We also allow the local traffic as demonstrated. This completes the necessary rules.

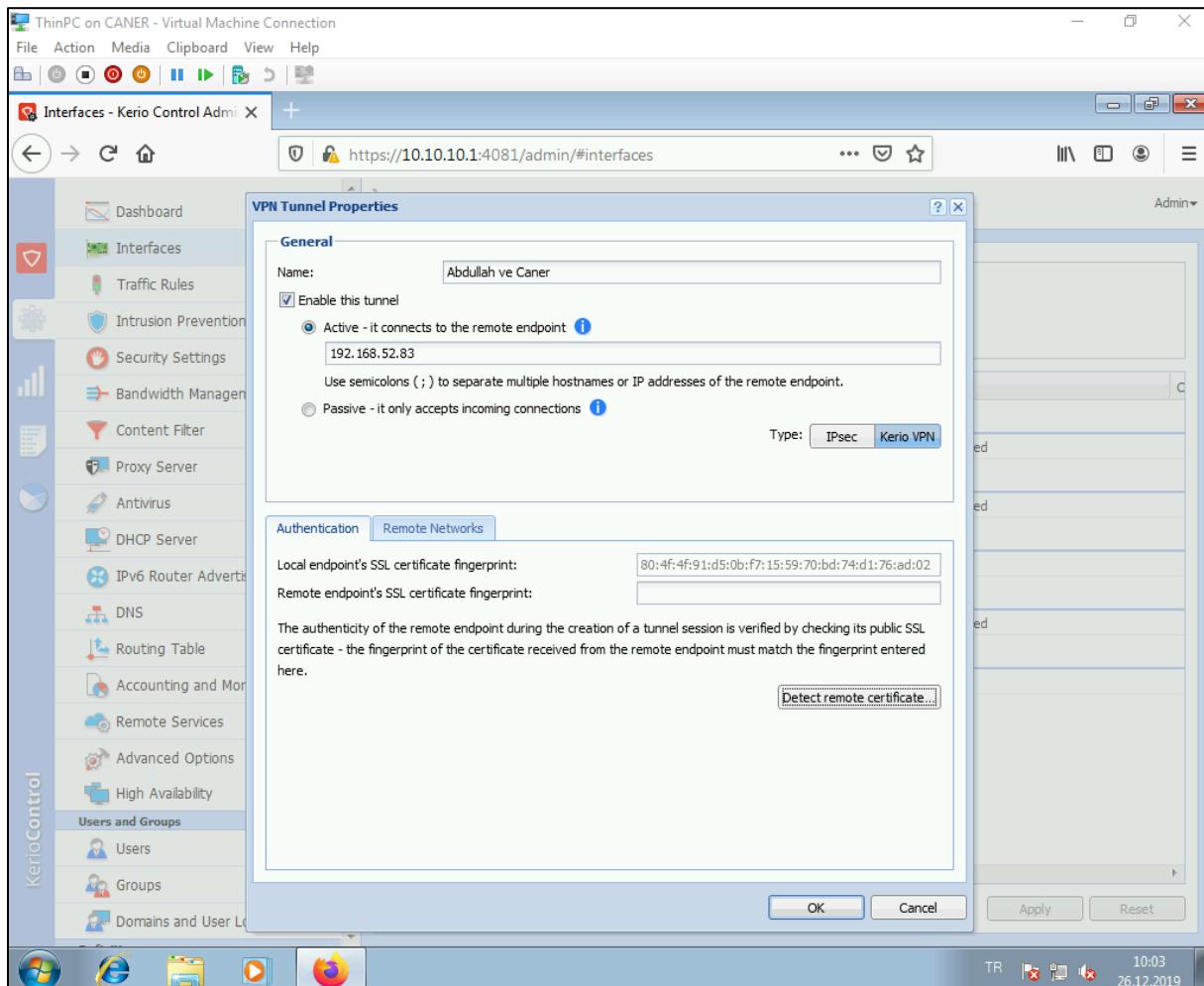
The screenshot shows the Kerio Control Admin interface with the 'Traffic Rules' page open. The left sidebar lists various management options like Dashboard, Interfaces, Traffic Rules, and Intrusion Prevention. The main area displays a table of traffic rules with columns for Name, Source, Destination, Service, IP version, and Action. A red box highlights the 'Local traffic' rule, which allows traffic from 'Firewall' to 'Firewall' via 'Any' service. Below it is another rule for 'VPN' traffic.

Name	Source	Destination	Action
RDP Port Mapping to ThinPc	Any	Firewall	Allow
Service Telnet on Firewall	Any	Firewall	Allow
Service RDP on Firewall	Any	Firewall	Allow
Service SSH on Firewall	Any	Firewall	Allow
Kerio Control Administr...	Any	Firewall	Allow
Internet access (NAT)	Trusted/Local In... Guest Interfaces VPN clients	Internet Interfaces	Allow
Local traffic	Firewall Trusted/Local In... VPN clients All VPN tunnels	Firewall	Allow
VPN	Any	Firewall	Allow
Firewall traffic	Firewall	Any	Allow
Guests traffic	Guest Interfaces	Firewall	Allow
Block other traffic	Any	Any	Drop

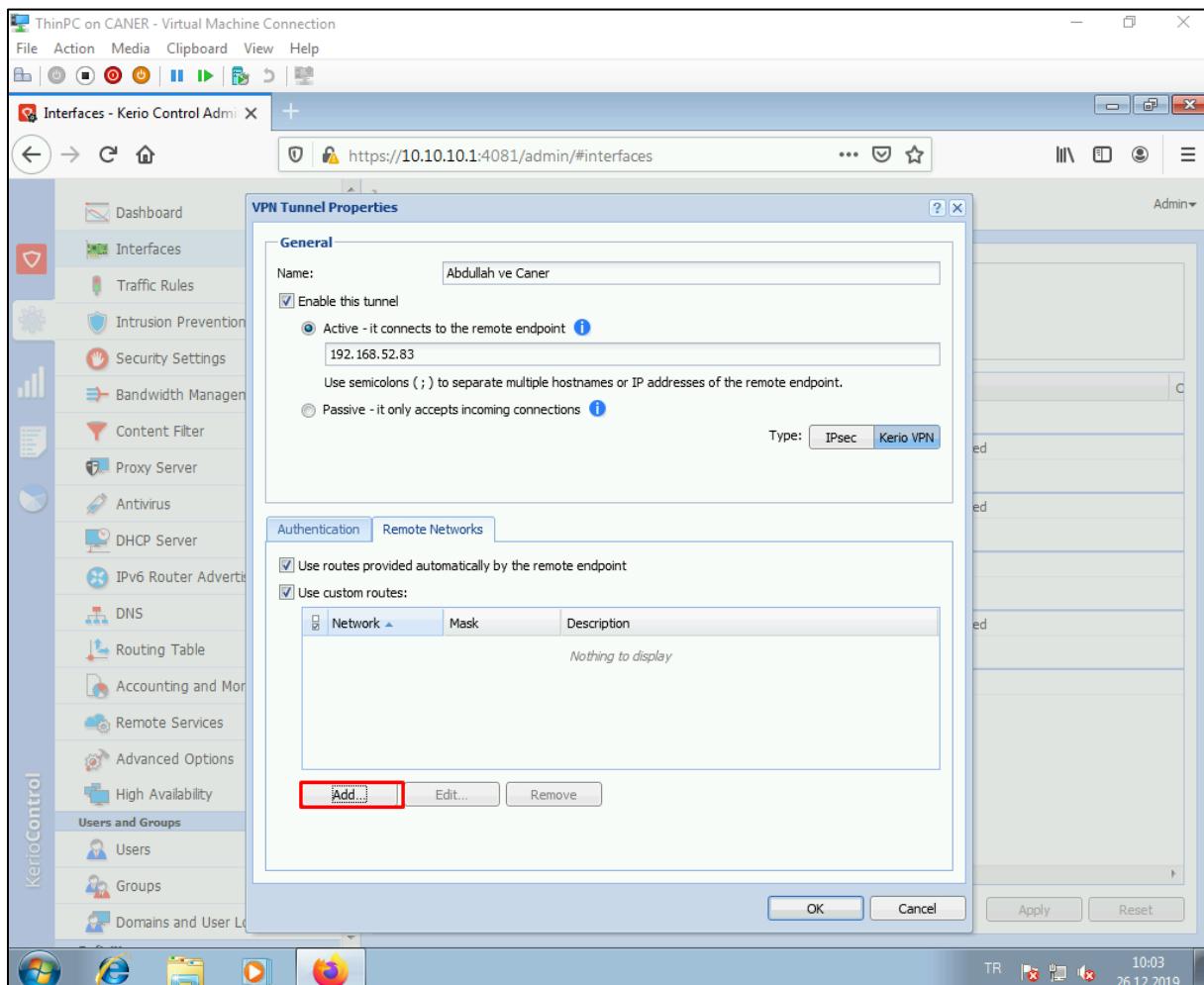
After that, we need to add a new interface for our tunnel.

The screenshot shows the Kerio Control Admin interface running on a ThinPC virtual machine. The left sidebar contains navigation links for Dashboard, Interfaces, Traffic Rules, Intrusion Prevention, Security Settings, Bandwidth Management and QoS, Content Filter, Proxy Server, Antivirus, DHCP Server, IPv6 Router Advertisements, DNS, Routing Table, Accounting and Monitoring, Remote Services, Advanced Options, and High Availability. Under 'Users and Groups', there are links for Users, Groups, and Domains and User Login. The main content area is titled 'Interfaces' and shows 'Internet connectivity' settings. It lists several interface types: Internet Interfaces (WAN), Trusted/Local Interfaces (Ethernet), IPsec and Kerio VPN Interfaces (VPN Server), Guest Interfaces (Guest Network), and Other Interfaces. A red box highlights the 'Add...' button at the bottom left of the interface list. The status bar at the bottom right shows the date and time as 26.12.2019 10:01.

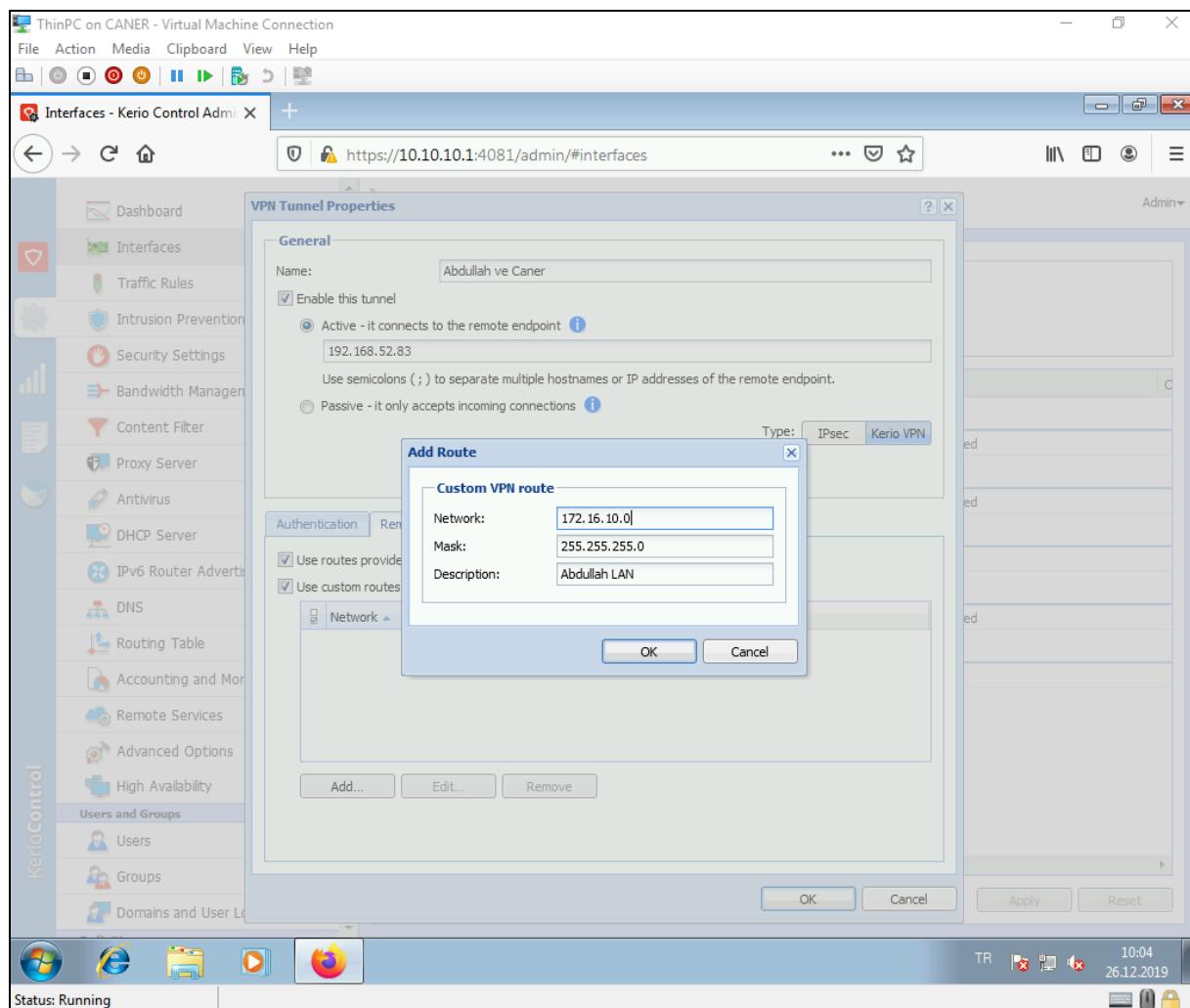
We name the tunnel and enable it. Depending on your network topology, the site might be active or passive. If it's an active site then you need to enter the public IP address of the other site. At least, one of the sites must be active to establish the connection.



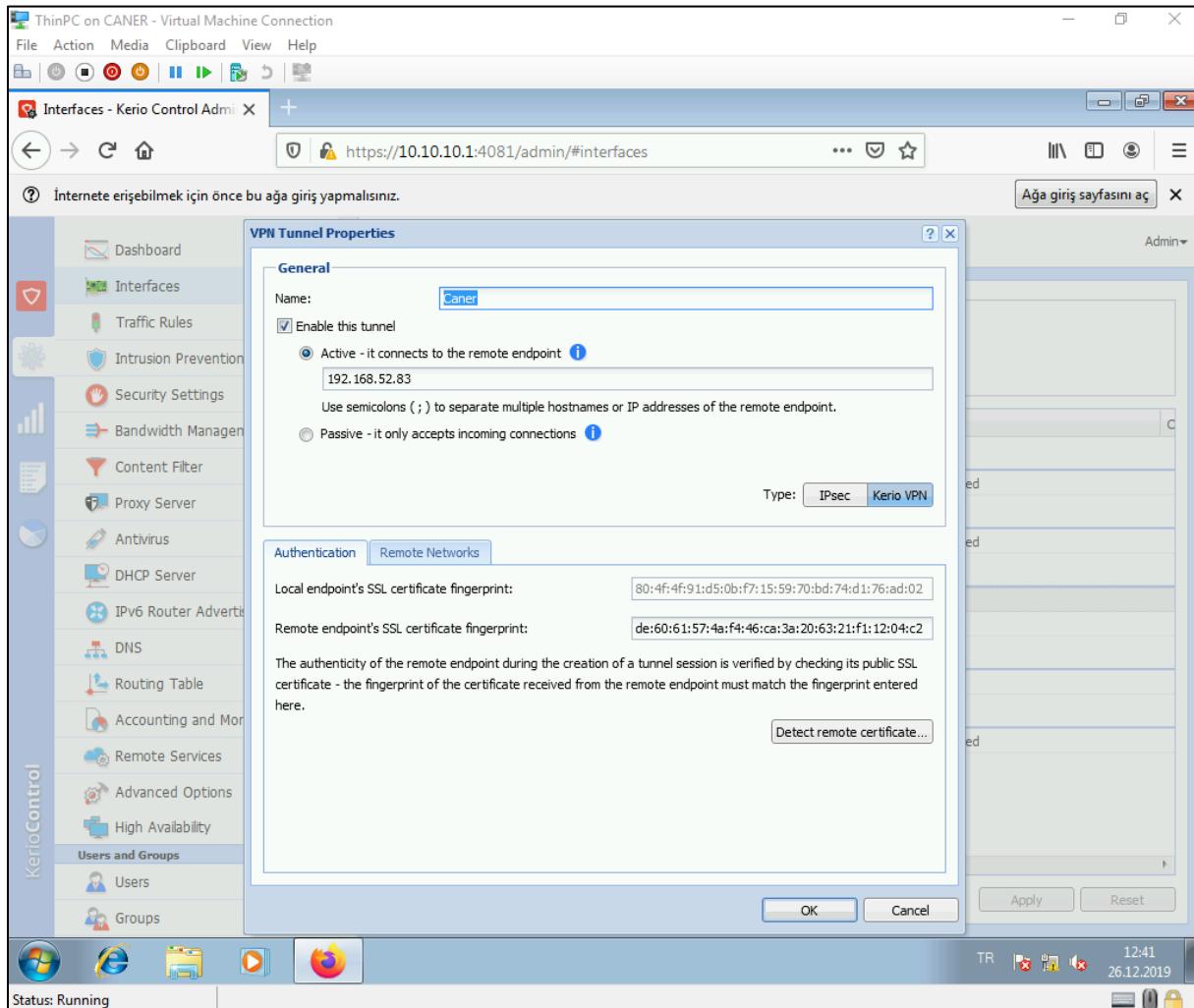
We then get to the remote networks tab and add the unknown internal networks of the partner site that you want to establish the VPN with.



This is the LAN network of the partner site.



We do the vice versa at the other site and click on detect remote certificate. It should get their certificate and you do the vice versa at the other site.



Note that we changed the tunnel's name only for cosmetic reasons. The network settings are still the same. Both sites still have all the relevant network information and each other's certificate.

20.1.2020

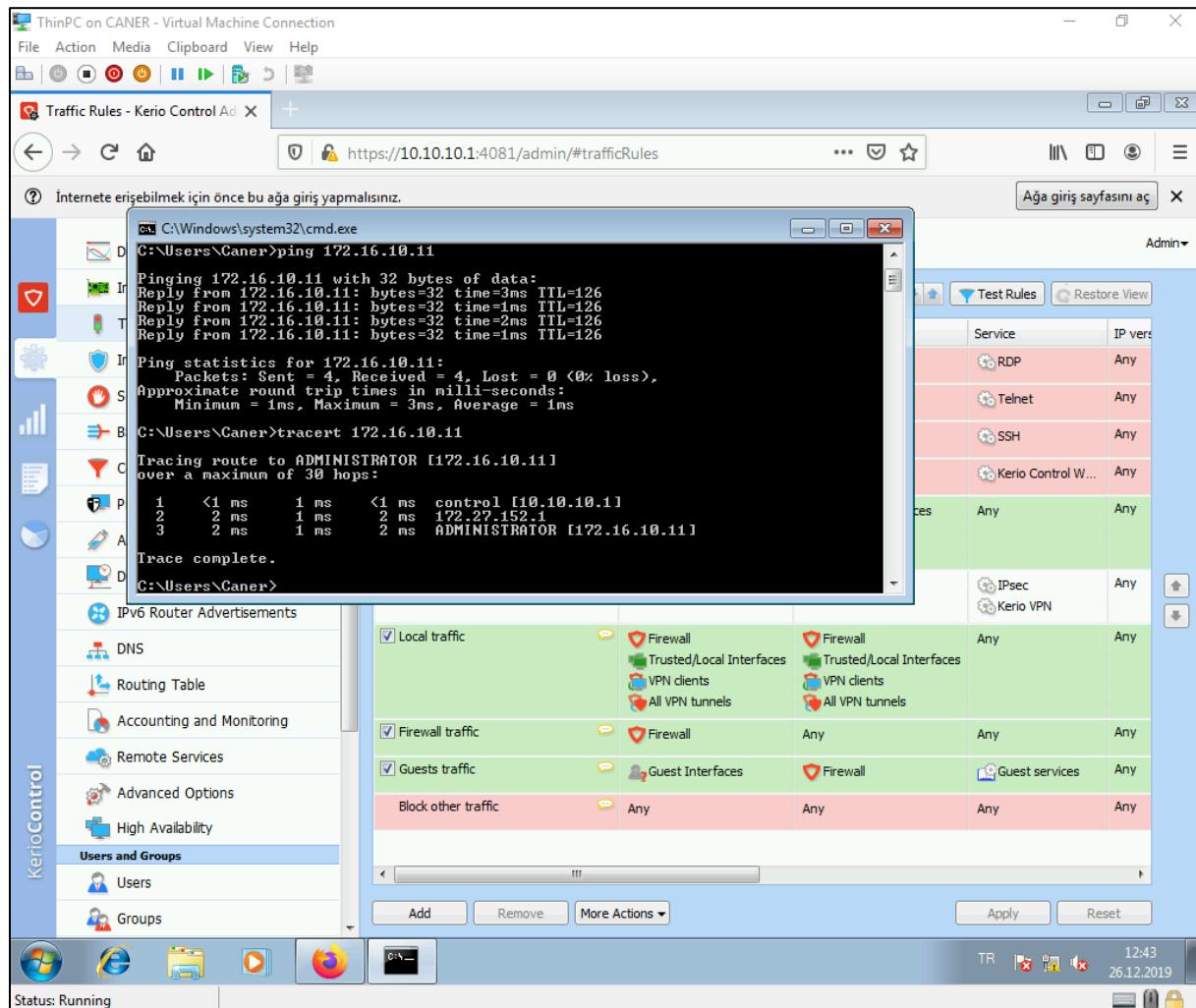
After we click finish and wait a while our VPN connection is up.

The screenshot shows the Kerio Control Admin interface with the title "Interfaces - Kerio Control Admin". The left sidebar contains a navigation menu with items like Dashboard, Interfaces (which is selected), Traffic Rules, Intrusion Prevention, Security Settings, Bandwidth Management and QoS, Content Filter, Proxy Server, Antivirus, DHCP Server, IPv6 Router Advertisements, DNS, Routing Table, Accounting and Monitoring, Remote Services, Advanced Options, High Availability, Users and Groups, Users, and Groups. The main content area is titled "Interfaces" and includes a section for "Internet connectivity" where it says "Select an option of how the firewall is connected to the Internet: A Single Internet Link". Below this is a table of interfaces:

Name	Status	IPv4	IPv6
WAN	Up	192.168.52.182	IPv6 disabled
Ethernet	Up	10.10.10.1	IPv6 disabled
Caner	Up		
VPN Server	Up	10.253.134.1	

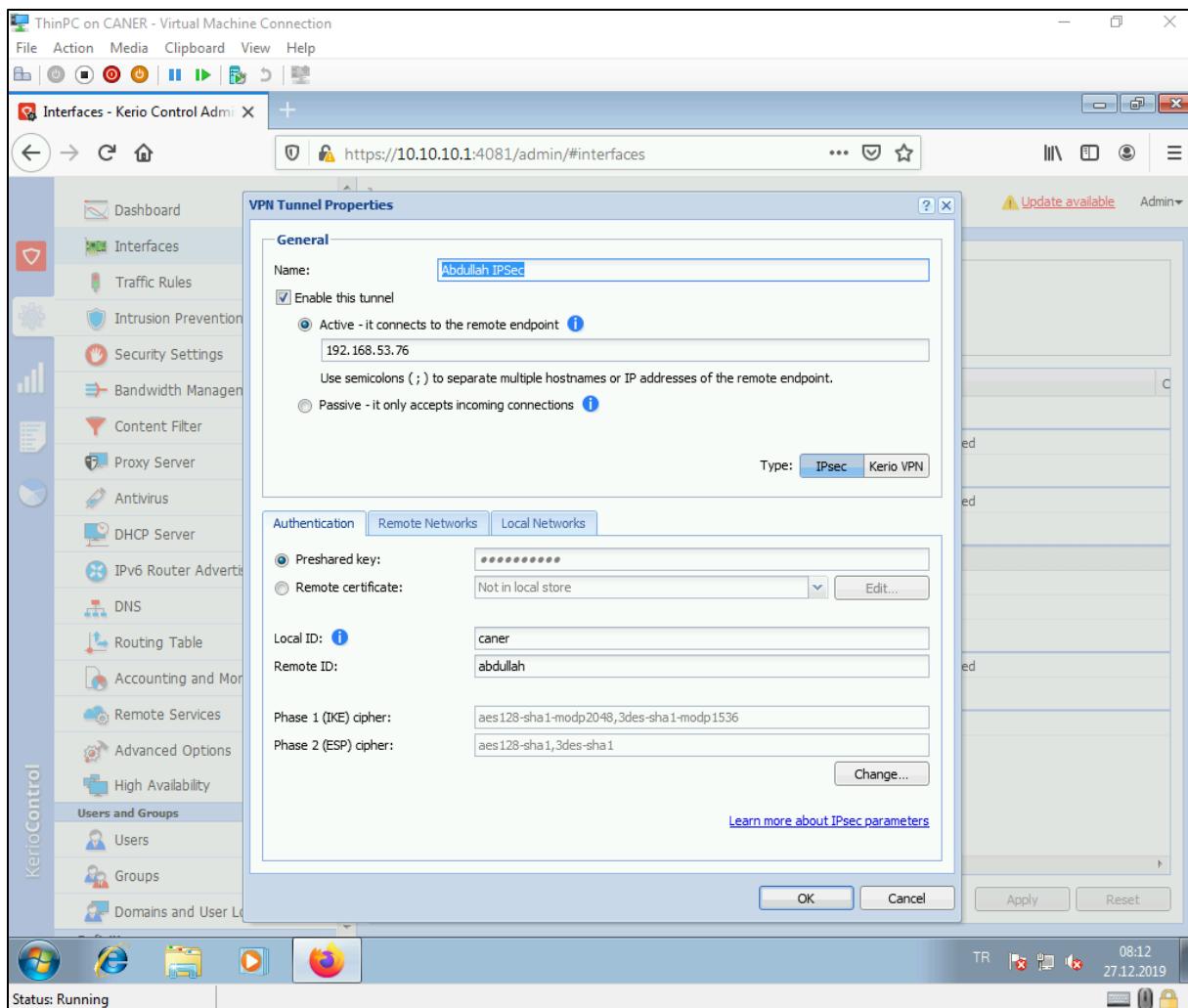
At the bottom of the interface, there are buttons for Add, Edit..., Dial, More Actions, Apply, and Reset. The status bar at the bottom shows "Status: Running", the date and time "TR 12:42 26.12.2019", and icons for network, battery, and lock.

That means a host on site 1's internal network can ping or RDP a host on site 2's internal network and when we trace the route it directly goes from one internal to the other's VPN server and to the other's internal network.



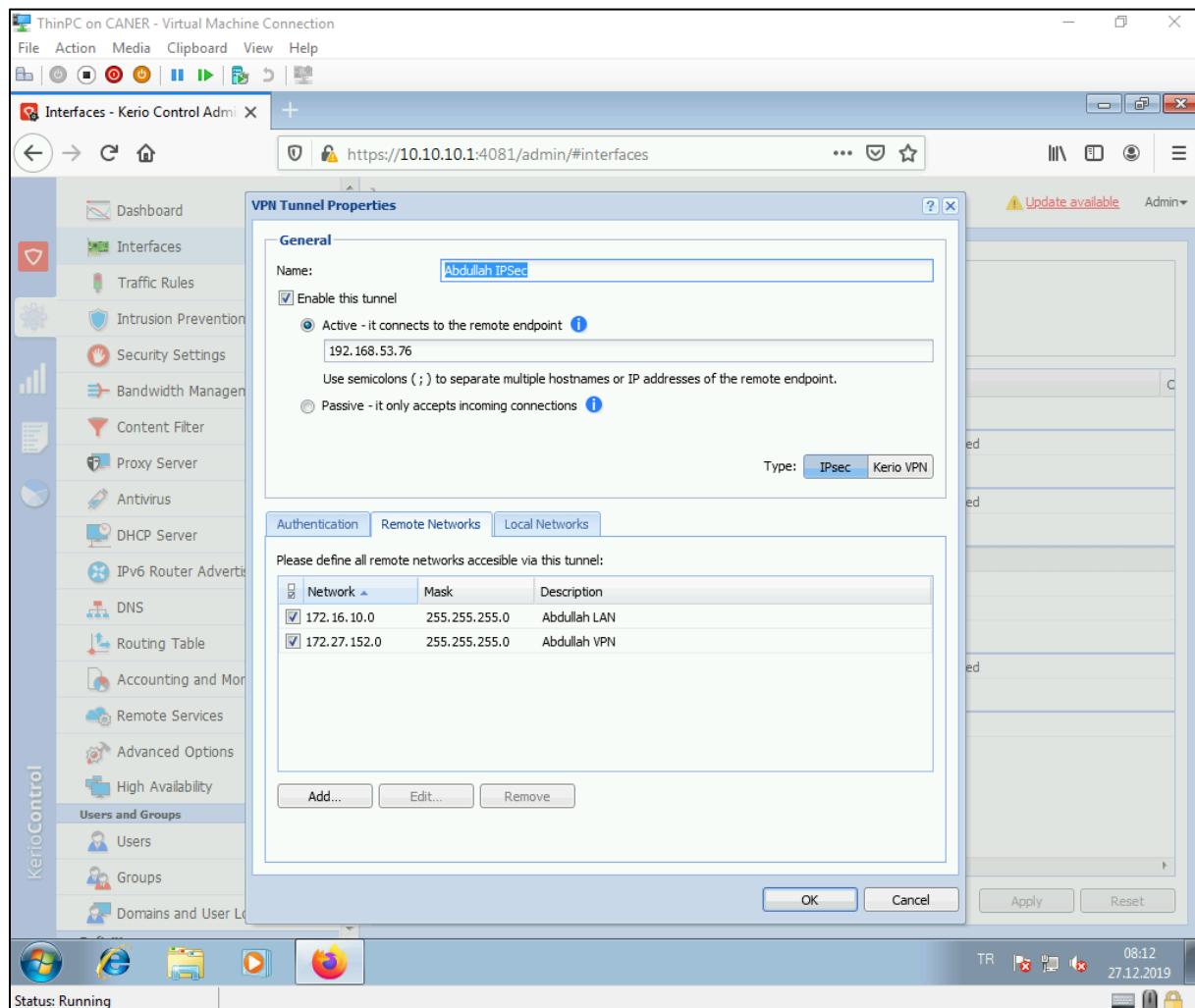
This completes the VPN.

We could also use IPSec instead of the VPN and get more security due to encryption.

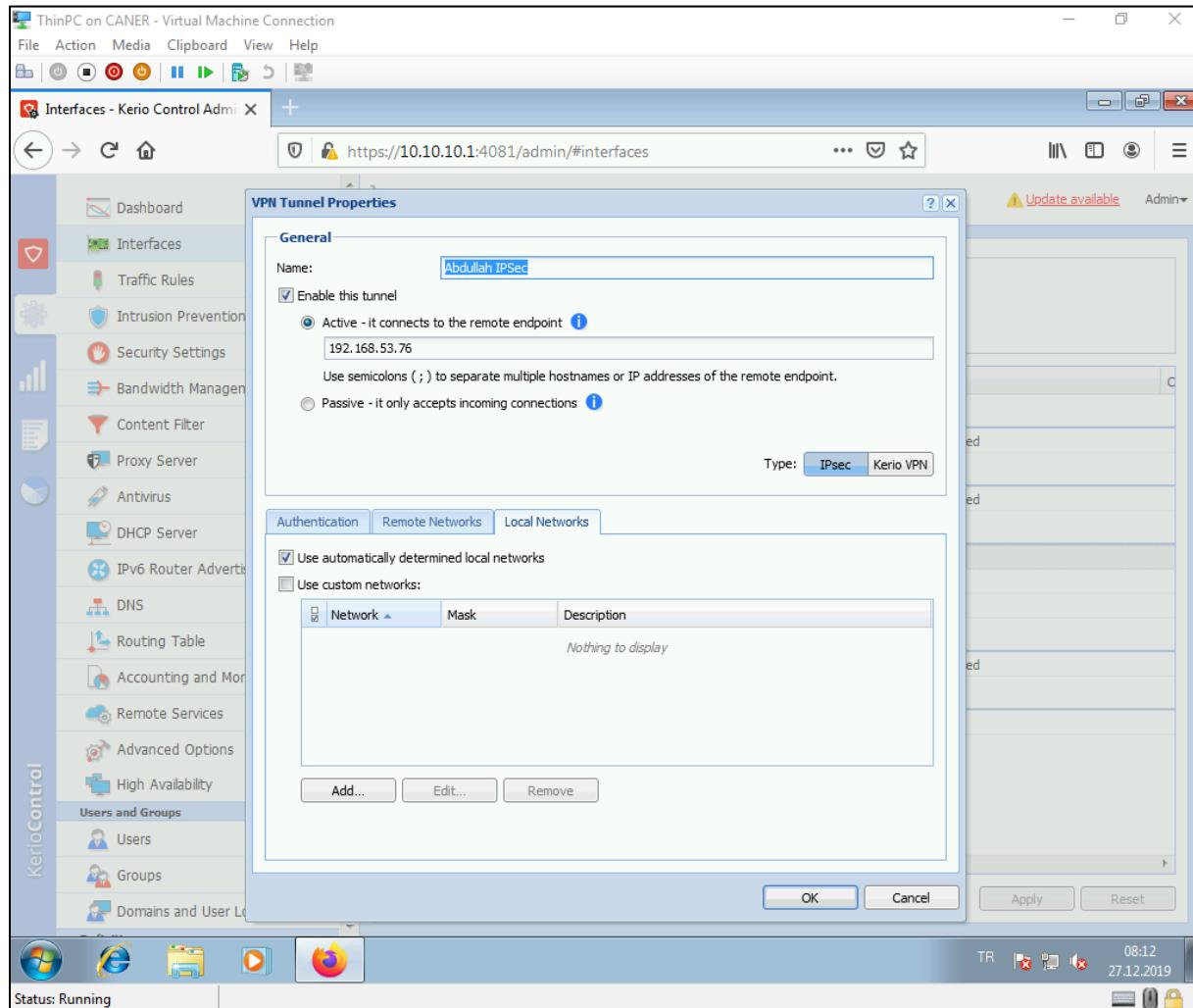


For an IPSec tunnel a pre-shared key can be used as another layer of security. The local and remote IDs must match to the partners, in reverse obviously and the IKE and ESP ciphers' details MUST be the same. An IPSec tunnel cannot be established if you use different encryption and/or hash algorithms. Everything must be the same.

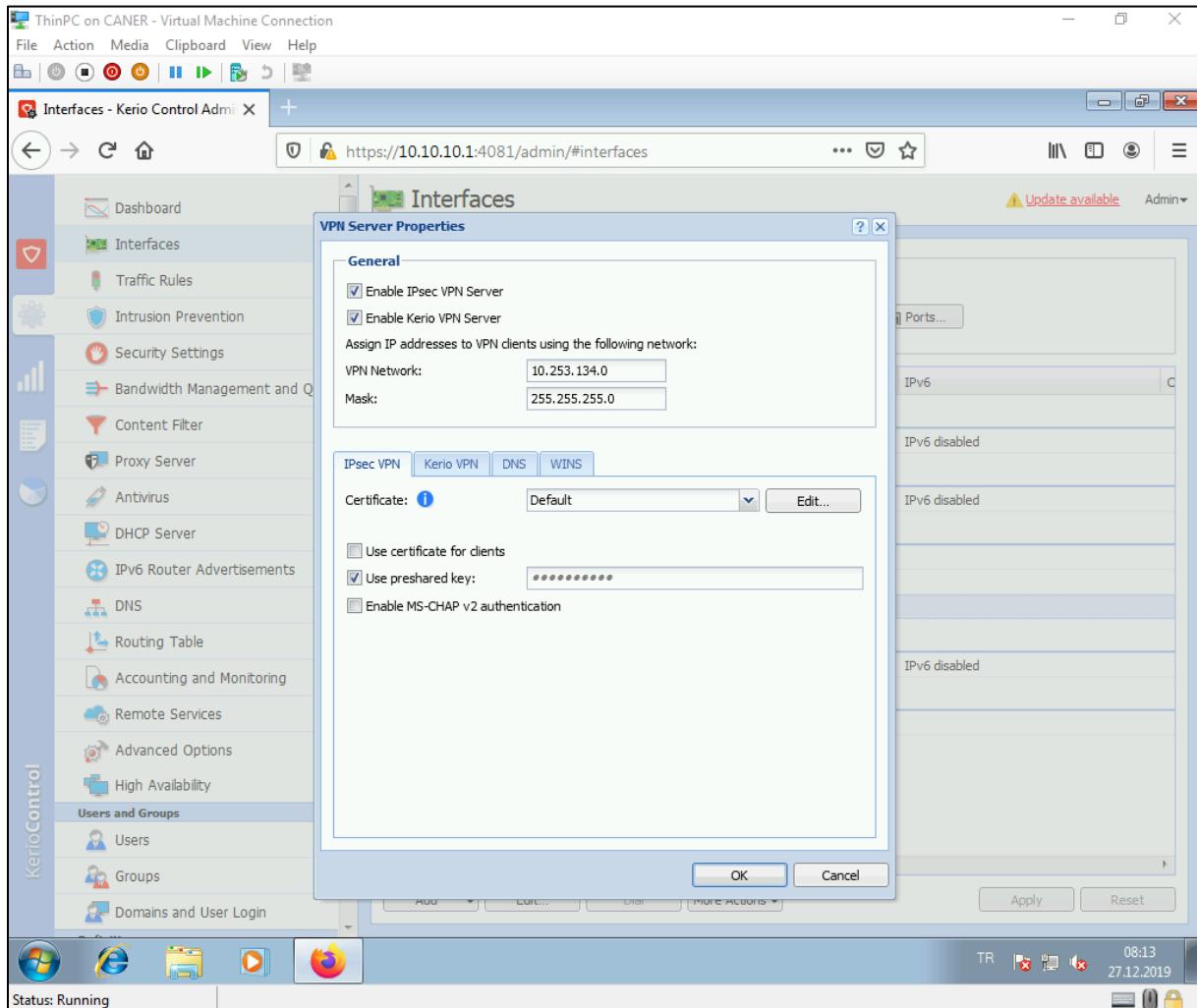
Another detail is that remote networks site 1 enters must match the local networks site 2 enters exactly and vice versa.



For this basic topology, the simplest way to accomplish this is to add every internal network of the other site as remote networks and connect all local networks.

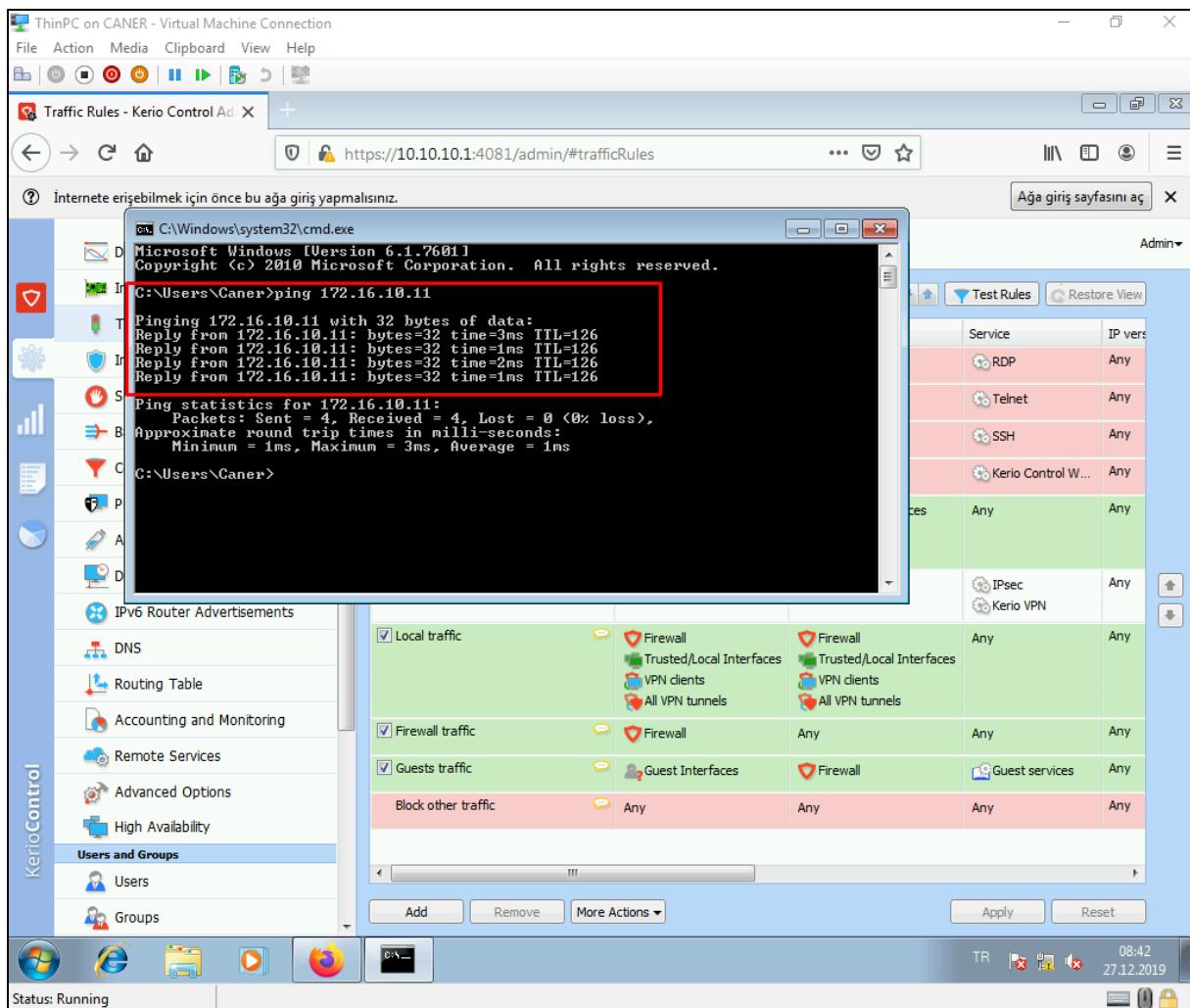


Also, if you use the pre-shared key mention it on the VPN Server Settings as well. Of course, it must be the same everywhere.

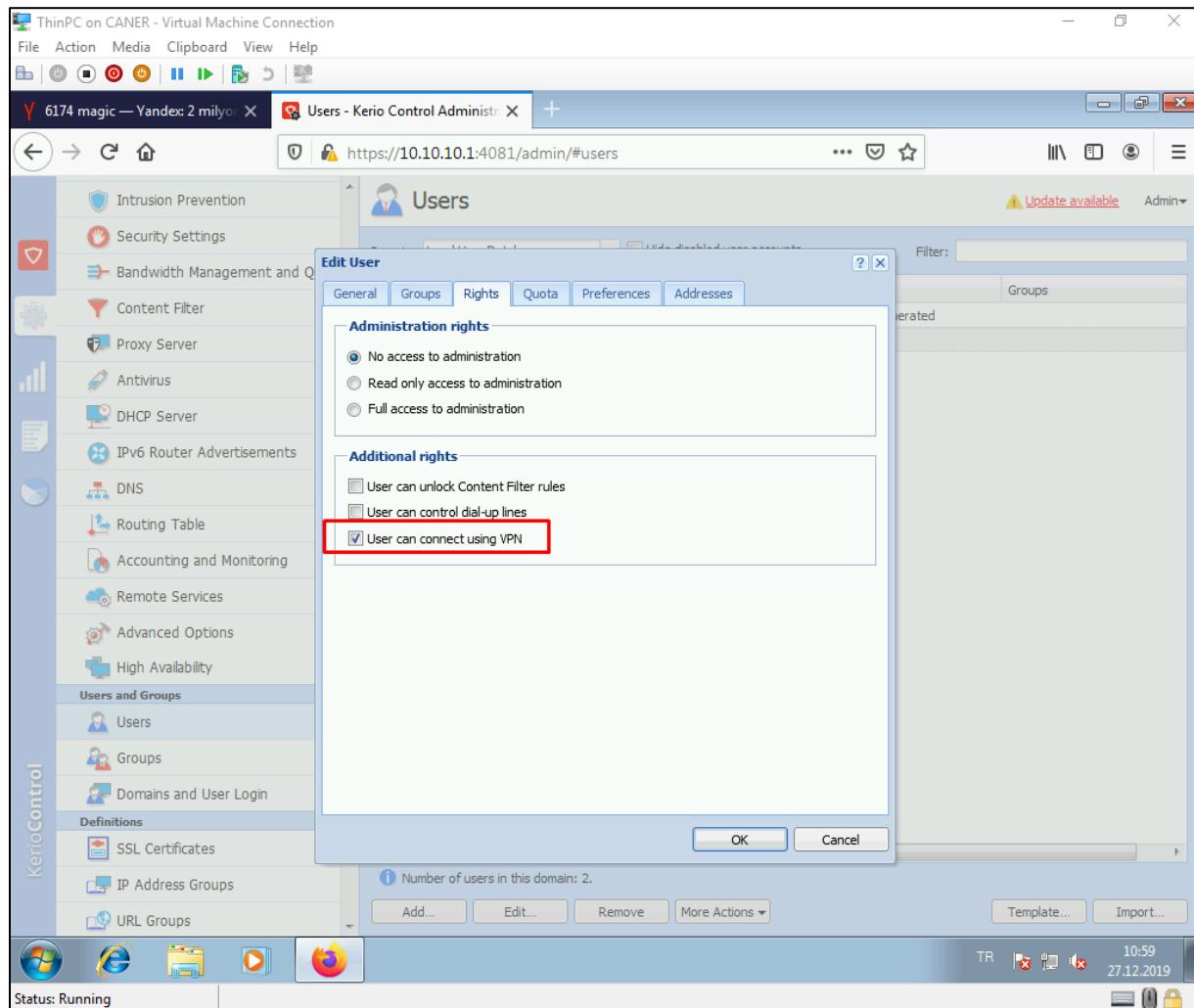


20.1.2020

Then, the tunnel works again.

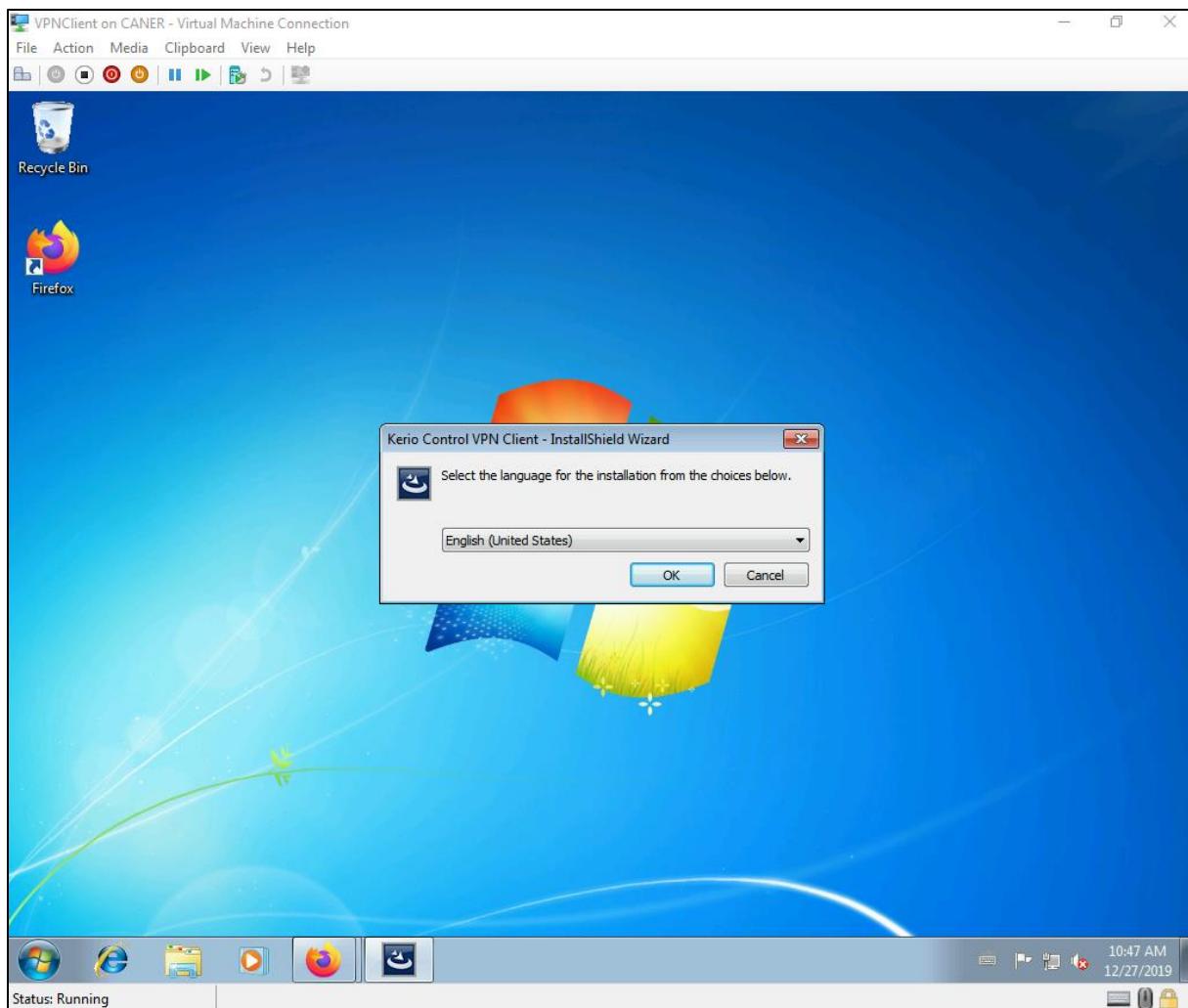


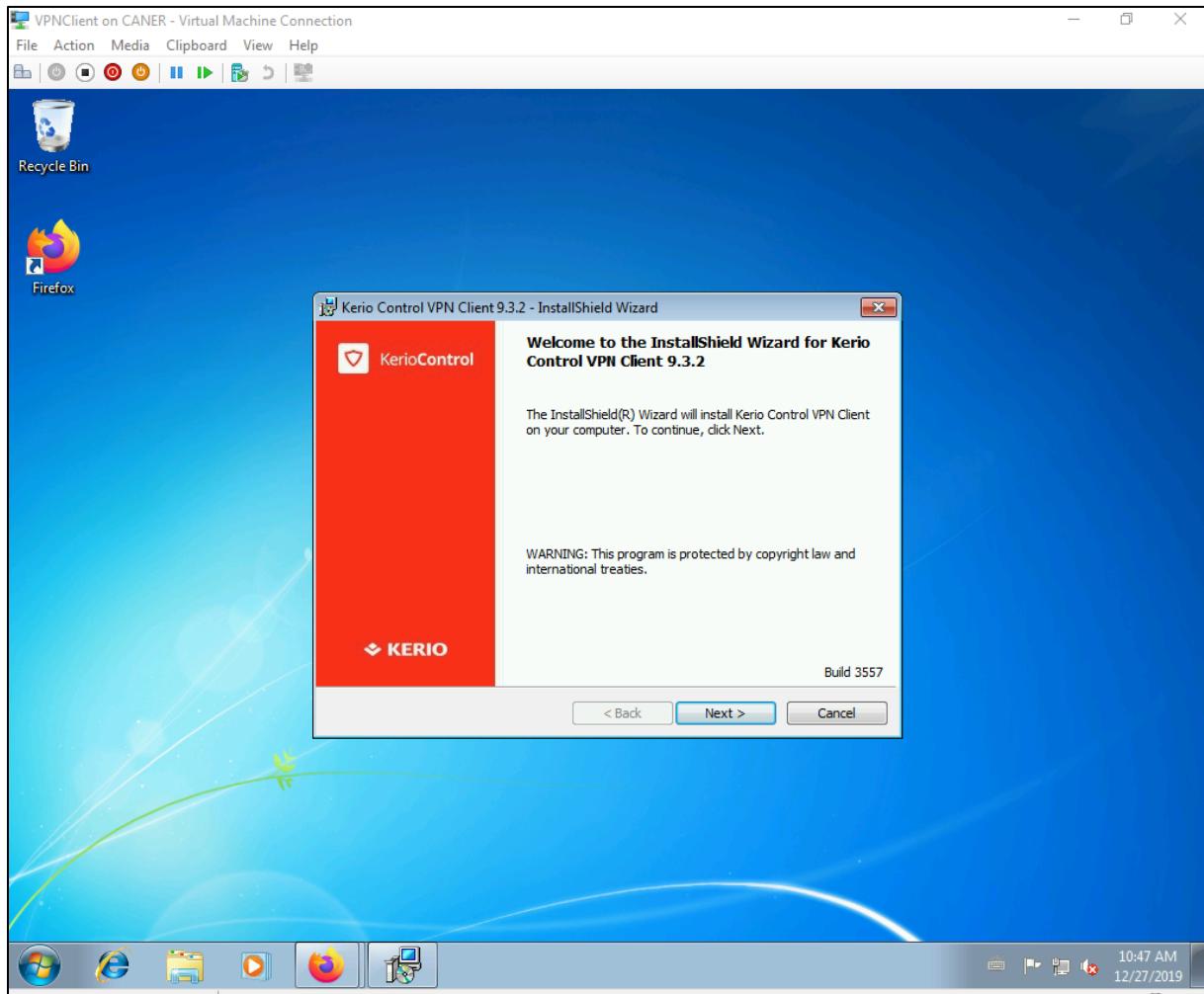
Now, let's do a client to site VPN connection. The very first thing we need to do is enable a user to connect via VPN under administration right of the user's rights. We can easily get there by editing the user.

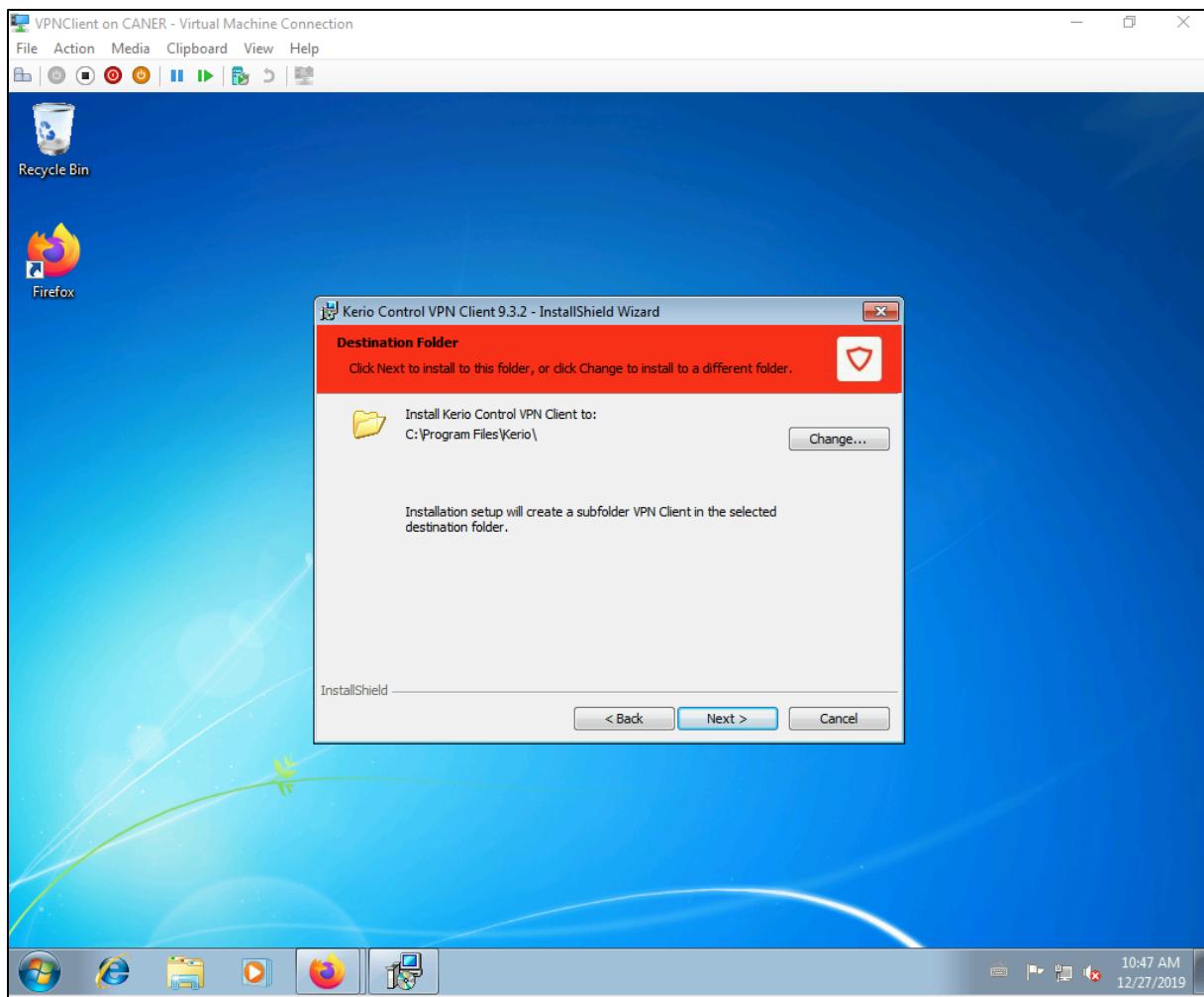


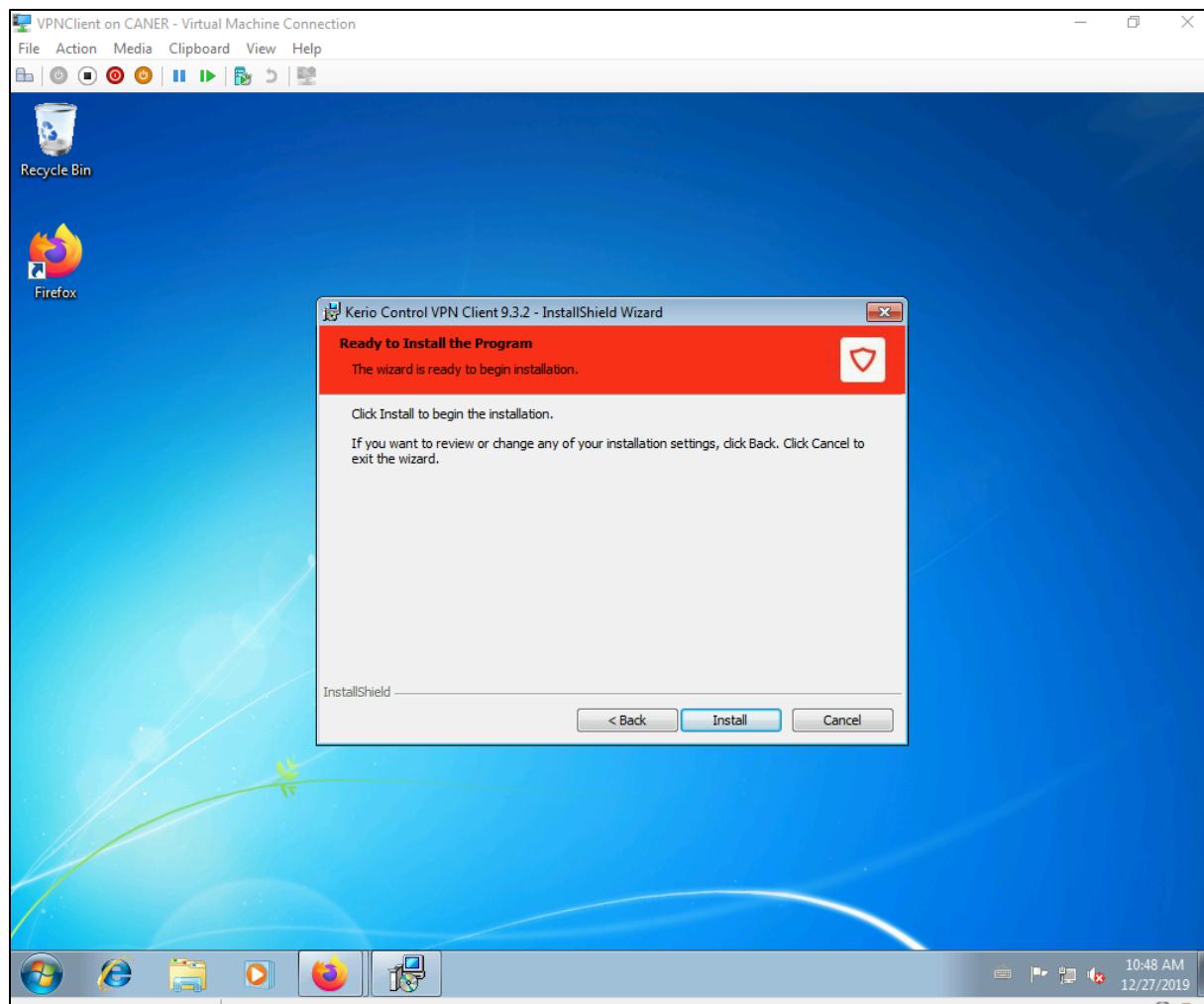
20.1.2020

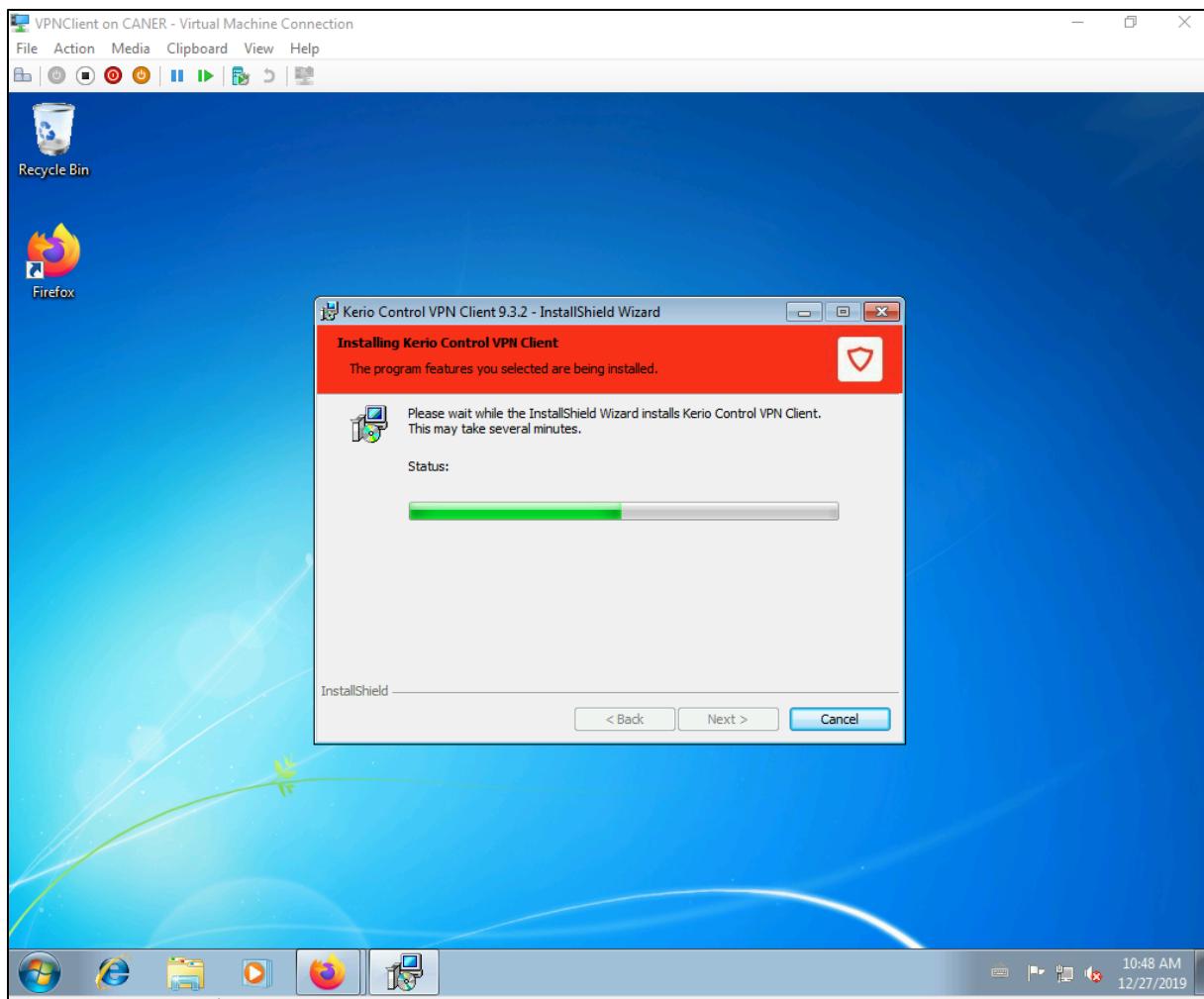
Then, from Kerio Control website the user must download the Kerio VPN Client application.



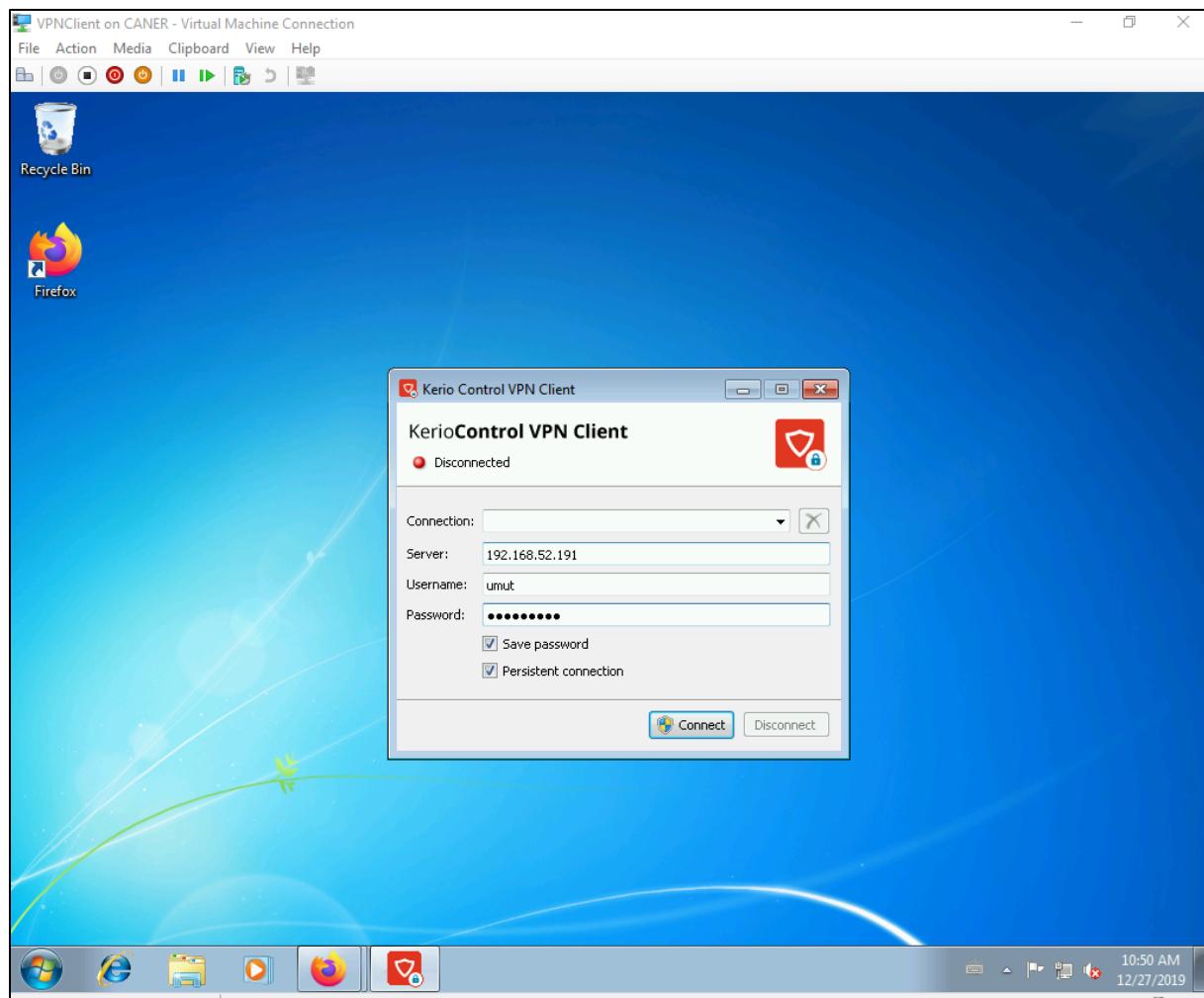






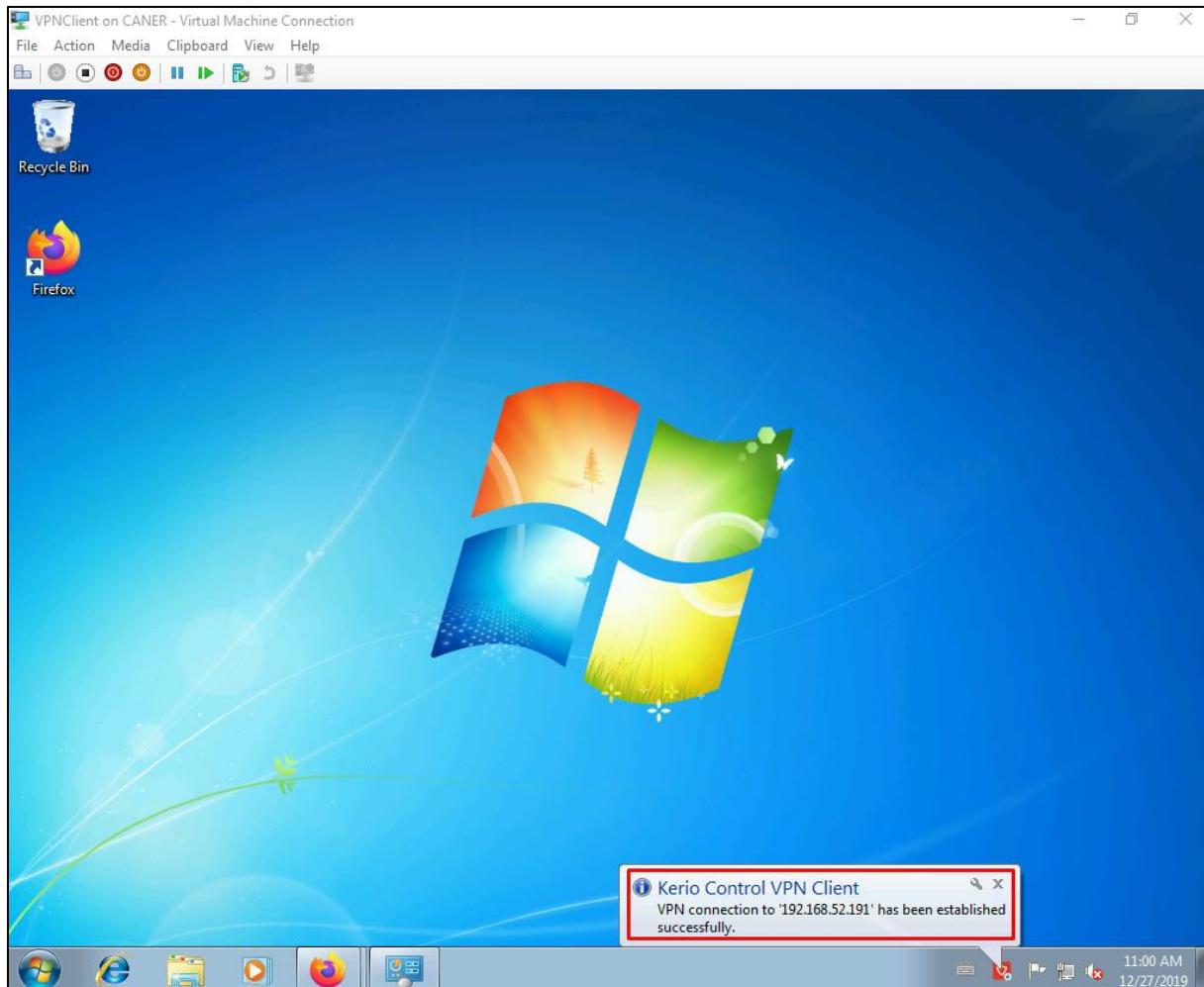


After the installation is done, the user logs in with WAN IP address mentioned for the server.



20.1.2020

And the connection established.



The admin can also see that the user has been connected via the VPN.

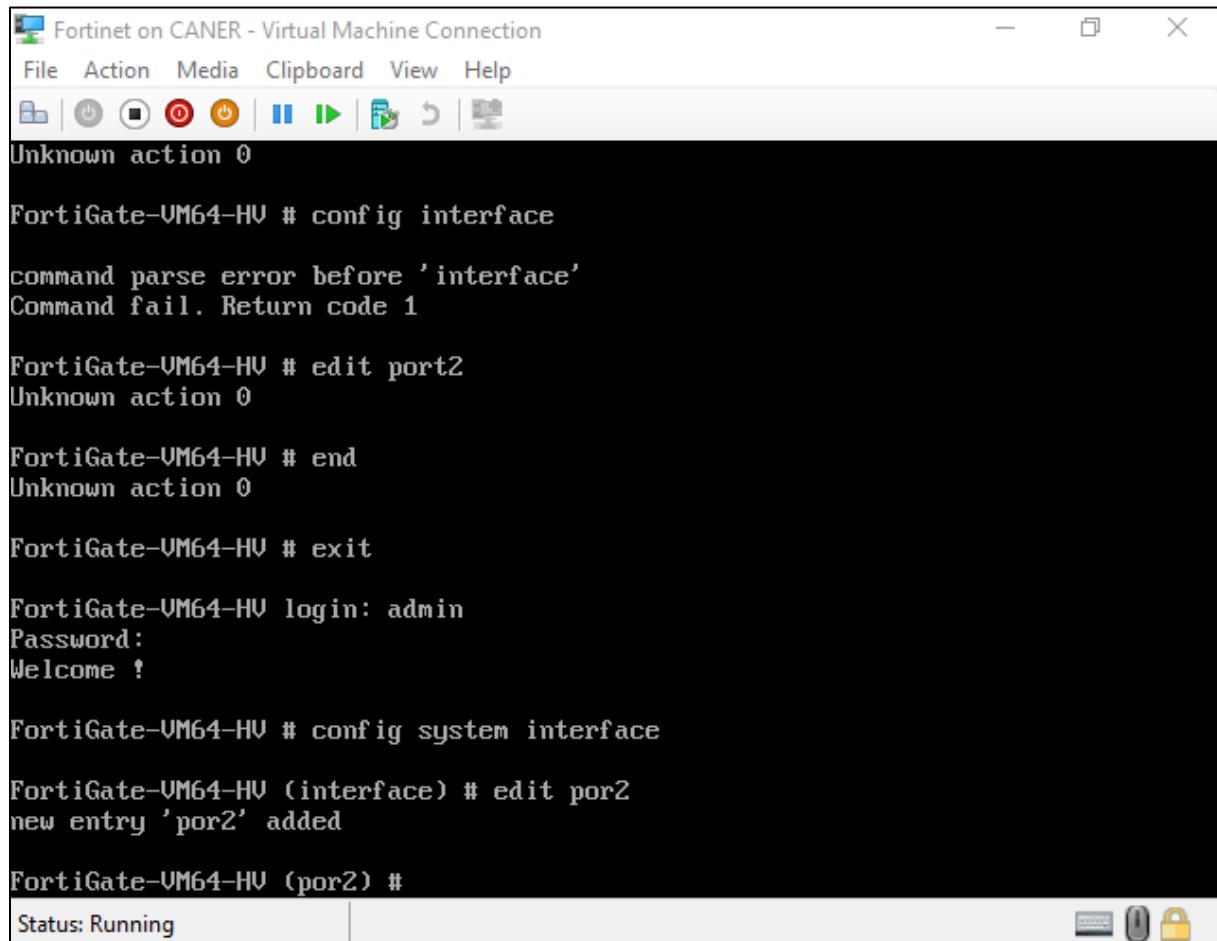
The screenshot shows the Kerio Control Admin interface. On the left, there's a vertical sidebar with icons for Active Hosts, Active Connections, VPN Clients (which is selected), User Statistics, Traffic Charts, Alert Messages, System Health, and IP Tools. The main area is titled "VPN Clients" and displays a table with one item: "umut". The table columns are Username, Tunnel Type, Operating System, Hostname, and Client IP. The "Client IP" column shows "10.253.134.3". A red box highlights this row. At the bottom of the main window, there's a status bar with "Auto-refresh" checked. The taskbar at the bottom of the screen shows several icons, including a Yandex browser tab and the Kerio Control icon.

Username	Tunnel Type	Operating System	Hostname	Client IP
umut	Kerio VPN	Windows 7	192.168.53.149	10.253.134.3

This finishes the Kerio Control part of this project.

3) Fortinet

We set up another virtual machine with two NICs similar to the previous cases and this time load up a Fortinet image. We log in with the user name admin and no password.



```
Fortinet on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Unknown action 0

FortiGate-VM64-HV # config interface
command parse error before 'interface'
Command fail. Return code 1

FortiGate-VM64-HV # edit port2
Unknown action 0

FortiGate-VM64-HV # end
Unknown action 0

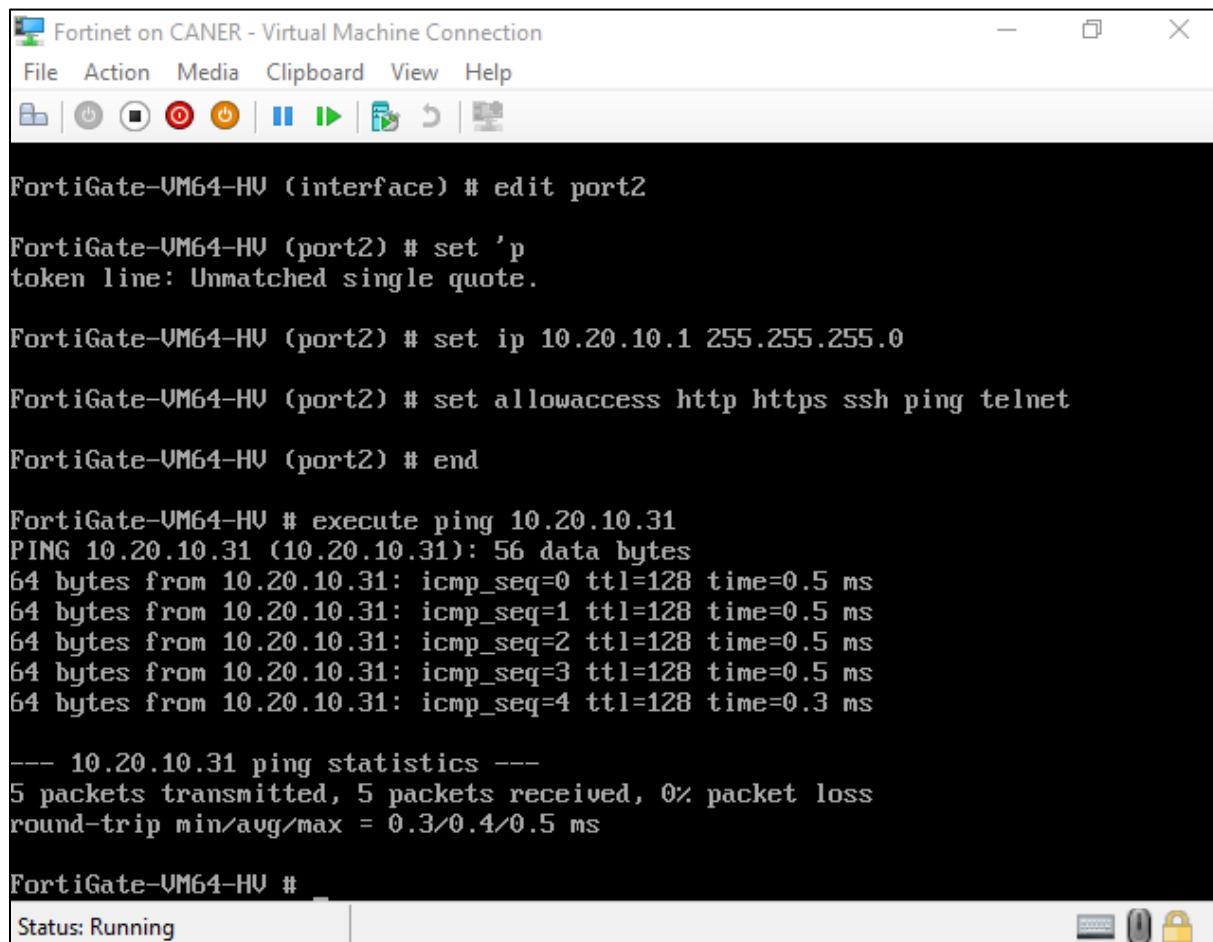
FortiGate-VM64-HV # exit

FortiGate-VM64-HV login: admin
Password:
Welcome !

FortiGate-VM64-HV # config system interface
FortiGate-VM64-HV (interface) # edit por2
new entry 'por2' added

FortiGate-VM64-HV (por2) #
Status: Running |
```

Then, we type edit port2, since it's our internal card, to get into the interface and assign an IP address. We also allow SSH, HTTP, HTTPS, PING and TELNET protocols.



The screenshot shows a terminal window titled "Fortinet on CANER - Virtual Machine Connection". The window contains the following command-line session:

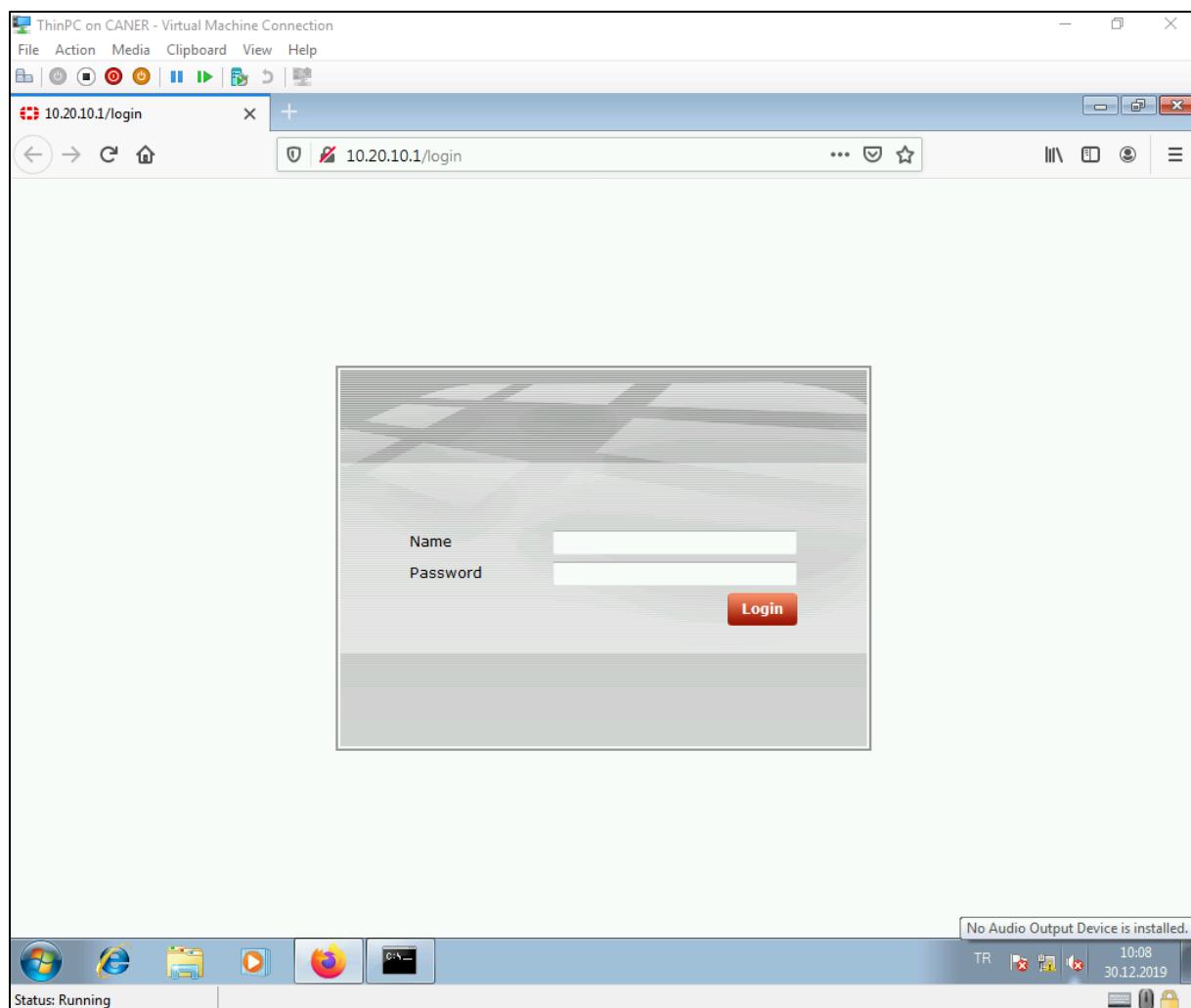
```
FortiGate-VM64-HV (interface) # edit port2
FortiGate-VM64-HV (port2) # set 'p
token line: Unmatched single quote.
FortiGate-VM64-HV (port2) # set ip 10.20.10.1 255.255.255.0
FortiGate-VM64-HV (port2) # set allowaccess http https ssh ping telnet
FortiGate-VM64-HV (port2) # end
FortiGate-VM64-HV # execute ping 10.20.10.31
PING 10.20.10.31 (10.20.10.31): 56 data bytes
64 bytes from 10.20.10.31: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 10.20.10.31: icmp_seq=1 ttl=128 time=0.5 ms
64 bytes from 10.20.10.31: icmp_seq=2 ttl=128 time=0.5 ms
64 bytes from 10.20.10.31: icmp_seq=3 ttl=128 time=0.5 ms
64 bytes from 10.20.10.31: icmp_seq=4 ttl=128 time=0.3 ms
--- 10.20.10.31 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.5 ms
FortiGate-VM64-HV #
```

The status bar at the bottom indicates "Status: Running".

We then test pinging a host on the same internal network.

20.1.2020

With the web browser we log in using the previous log in information.



This is the FortiGate VM64-HV Dashboard.

The screenshot shows the FortiGate VM64-HV dashboard interface. The top navigation bar includes薄 PC on CANER - Virtual Machine Connection, File, Action, Media, Clipboard, View, Help, and a toolbar with various icons. The main title is FortiGate - FortiGate-VM64-HV X, and the URL is 10.20.10.1/index.

System Information:

- Host Name: FortiGate-VM64-HV [Change]
- Serial Number: FGMEV0000000000
- Operation Mode: NAT [Change]
- HA Status: Standalone [Configure]
- System Time: Mon Dec 30 03:08:24 2019 (FortiGuard)
- Firmware Version: v5.0.build0292 (GA Patch 9) [Update] [Details]
- System Configuration: [Backup] [Restore] [Revisions]
- Current Administrator: admin [Change Password] /2 in Total [Details]
- Uptime: 0 day(s) 0 hour(s) 24 min(s)
- Virtual Domain: Disabled [Enable]

System Resources:

- CPU Usage: 20%
- Memory Usage: 29%

Features:

- Basic Features:** Advanced Routing (ON), IPv6 (OFF), VPN (ON), WAN Opt. & Cache (OFF)
- Security Features:** Preset: NGFW + ATP
 - AntiVirus (ON)
 - Application Control (ON)
 - DLP (OFF)
 - Email Filter (OFF)
 - Endpoint Control (ON)
 - Explicit Proxy (ON)

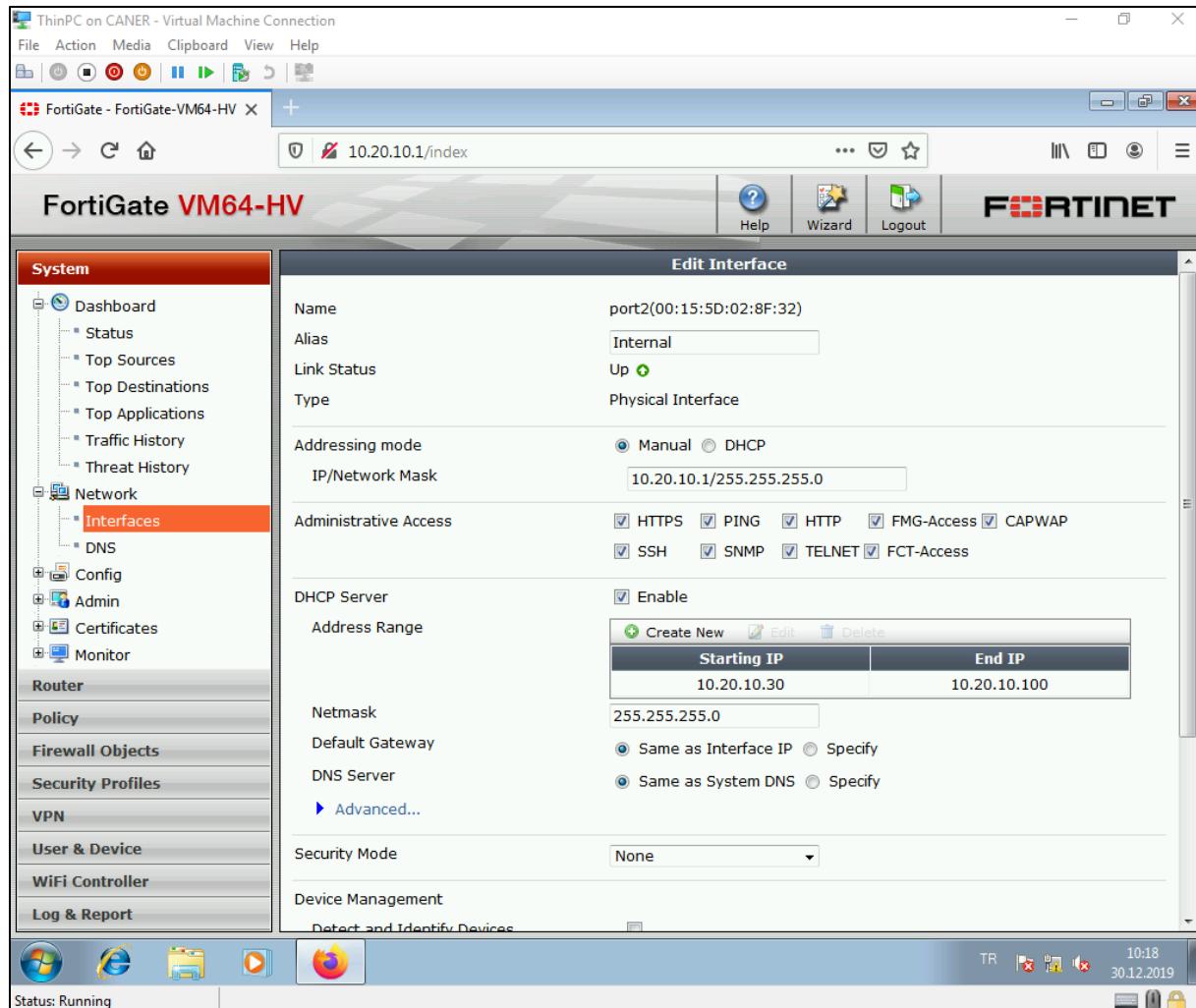
Licenses:

- VM License:** Registration Status: Valid [Update], CPUs Detected: 1 / 1, Evaluation License Expires: Tue Jan 14 02:44:31 2020
- Support Contract:** Registration: Unreachable
- FortiGuard Services:** Next Generation Firewall: IPS & Application Control Unreachable [Configure]

Network Status: Network 5, No Internet access

The bottom taskbar includes icons for ThinPC, Internet Explorer, File Explorer, Task View, and Firefox, along with a clock showing 10:08 and the date 30.12.2019.

As usual, we want to set up the interfaces.



The internal interface starts a DHCP pool but keeps the previously given static IP.

The external interface stays in DHCP mode to receive an IP address from BAU.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a 'System' section with 'Dashboard', 'Network' (selected), 'Config', 'Admin', 'Certificates', and 'Monitor'. Below these are sections for 'Router', 'Policy', 'Firewall Objects', 'Security Profiles', 'VPN', 'User & Device', 'WiFi Controller', and 'Log & Report'. The main content area is titled 'Edit Interface' for 'port1(00:15:5D:02:8F:31)'. The interface details include:

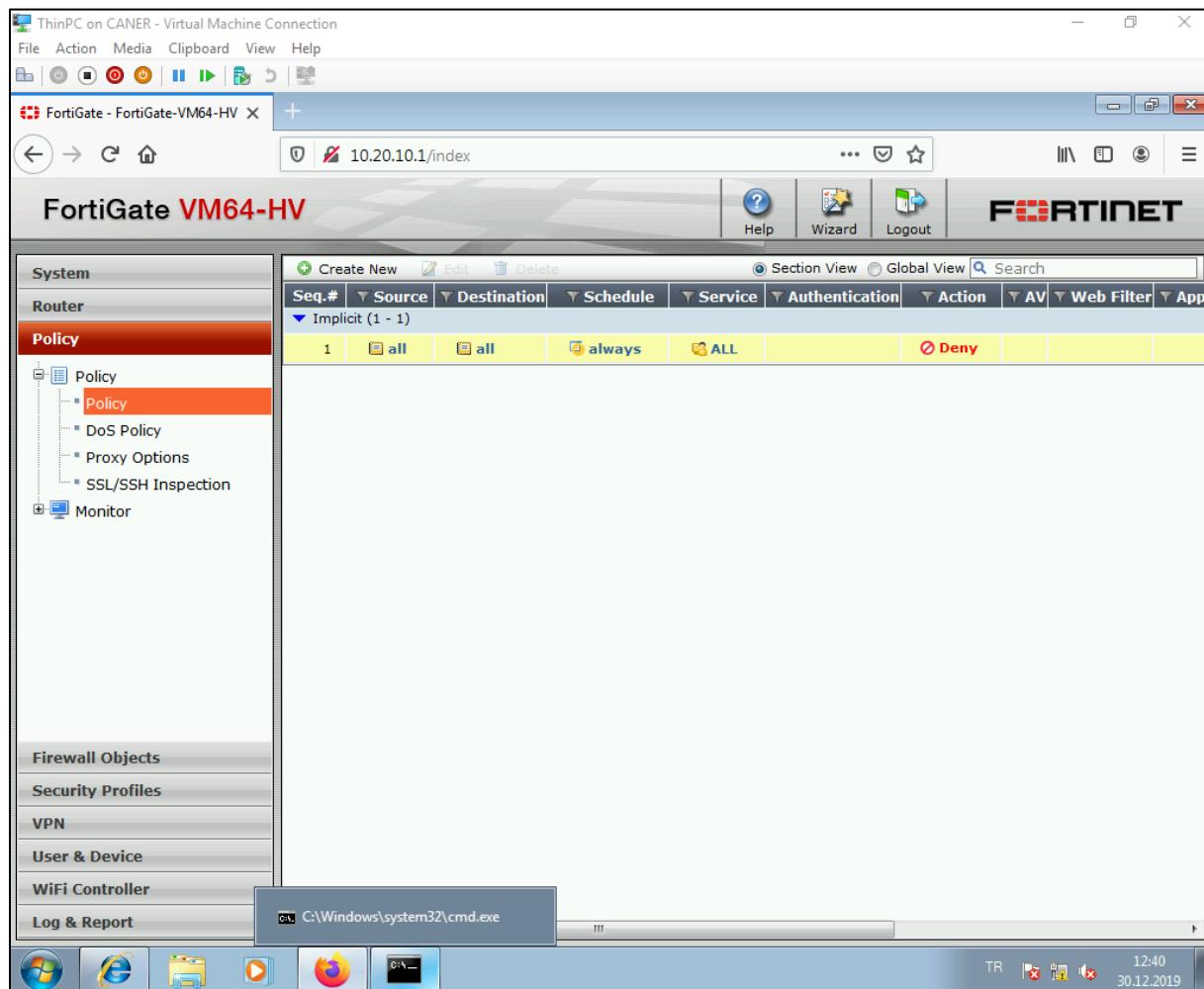
- Name:** port1(00:15:5D:02:8F:31)
- Alias:** External
- Link Status:** Up
- Type:** Physical Interface
- Addressing mode:** DHCP (radio button selected)
- Distance:** (empty input field)
- Administrative Access:** Checkboxes for HTTPS, PING, HTTP, FMG-Access, CAPWAP, SSH, SNMP, TELNET, and FCT-Access are all checked.
- Device Management:** Checkboxes for Detect and Identify Devices and Broadcast Discovery Messages are both unchecked.
- Comments:** A text input field with placeholder 'Write a comment...' and character count '0/255'.
- Administrative Status:** Radio buttons for 'Up' (selected) and 'Down' are shown.

At the bottom right of the interface window, it says '30 Aralık 2019 Pazartesi' (Sunday, December 30, 2019). The bottom status bar shows icons for Task View, Internet Explorer, File Explorer, Taskbar, and Firefox, along with the date '30.12.2019' and time '10:19'.

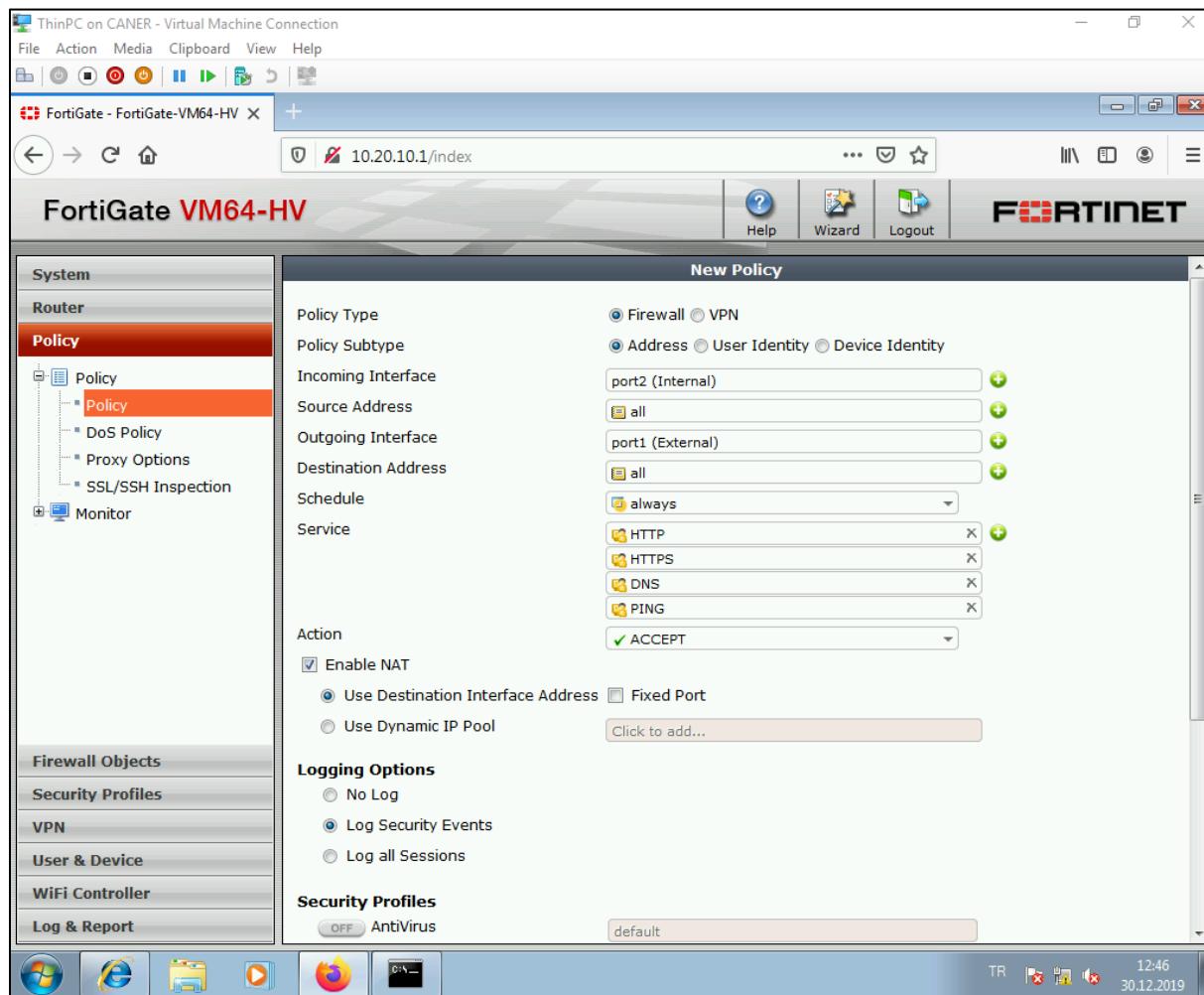
We can allow additional protocols here.

20.1.2020

We get to policies to create a new policy. Currently the only active policy is the (implicit) deny at the end.

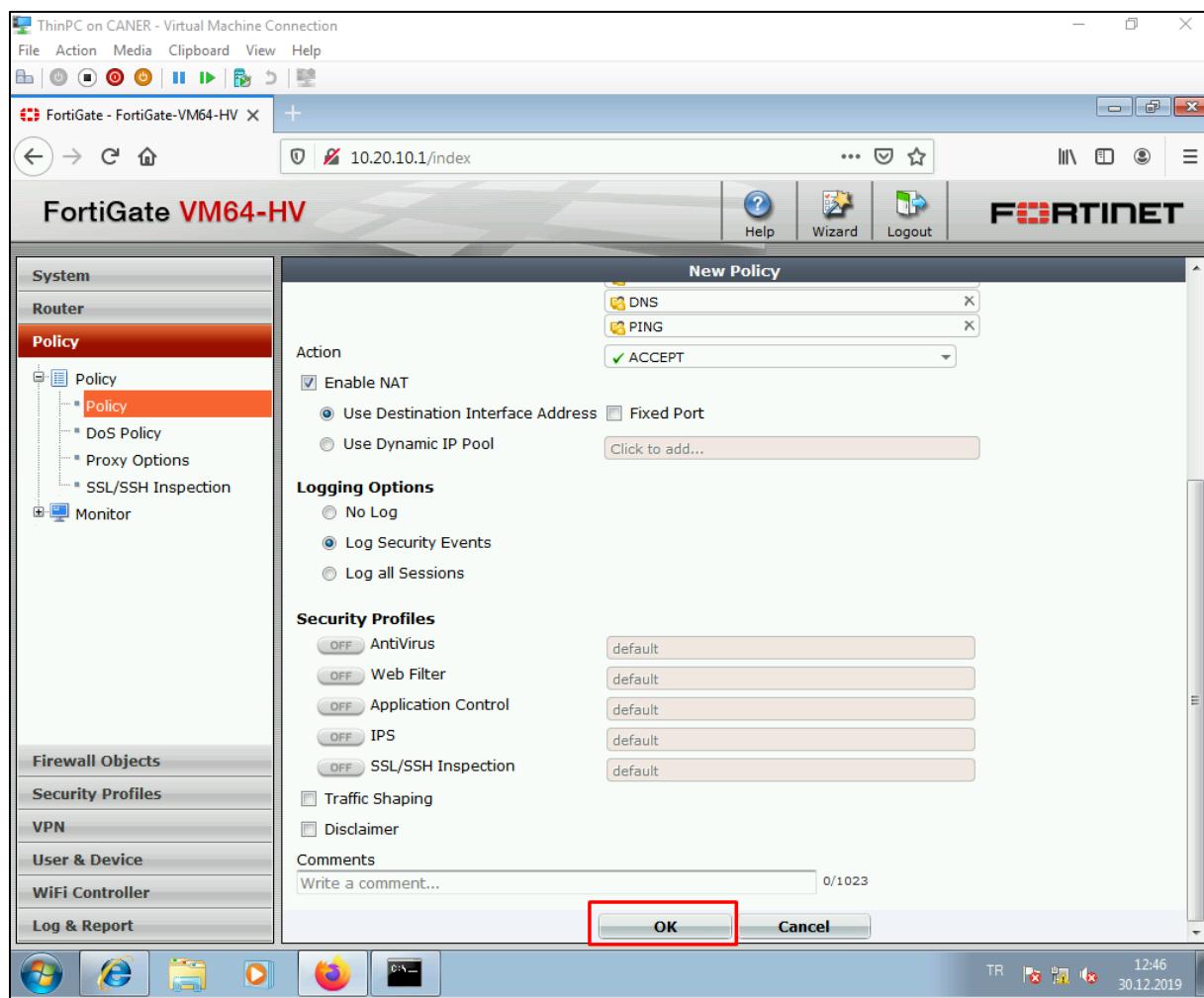


We enable NAT between the internal port2 and external port1 and allow HTTP, HTTPS, PING and DNS.

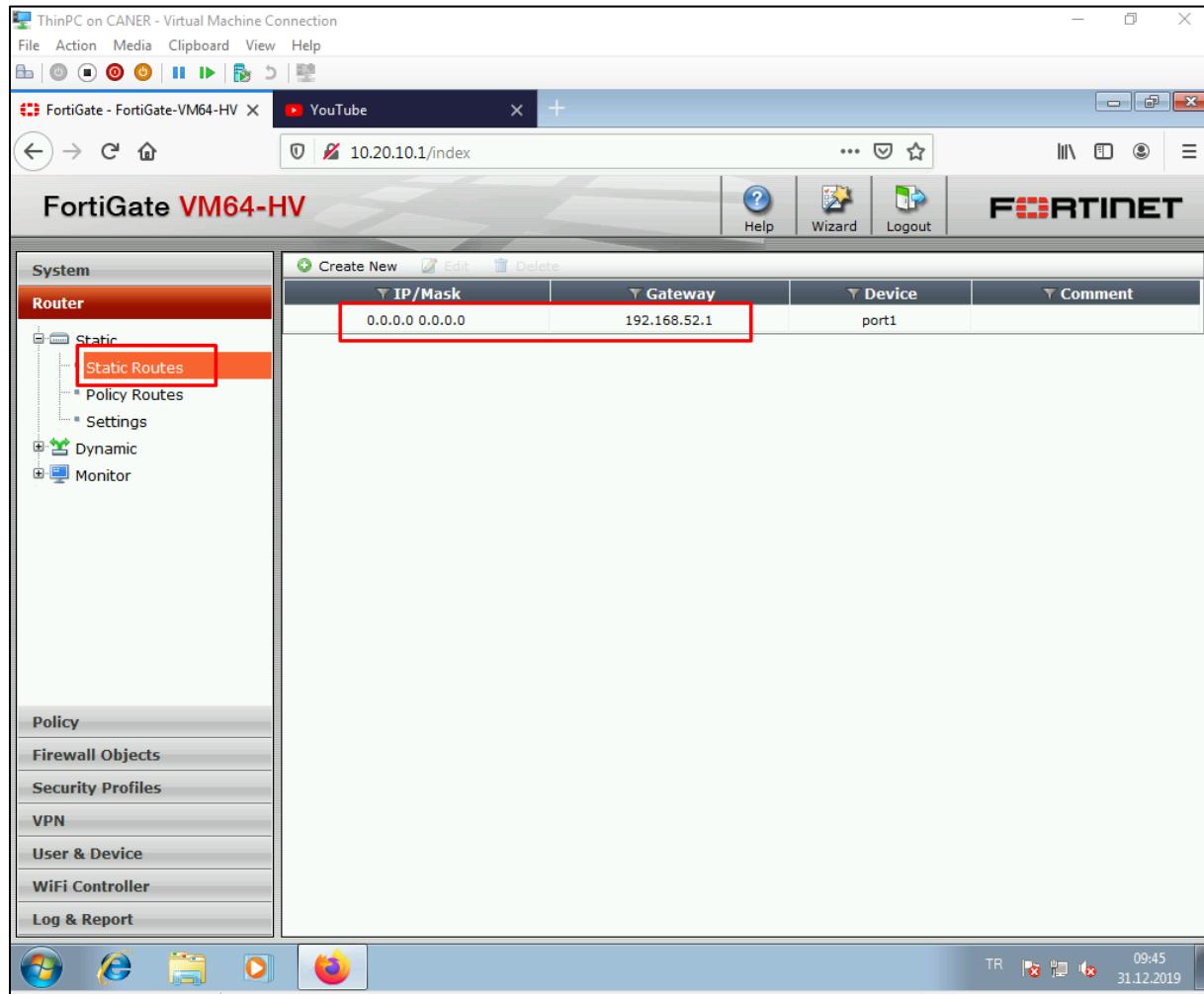


20.1.2020

Then, click OK without changing anything else.

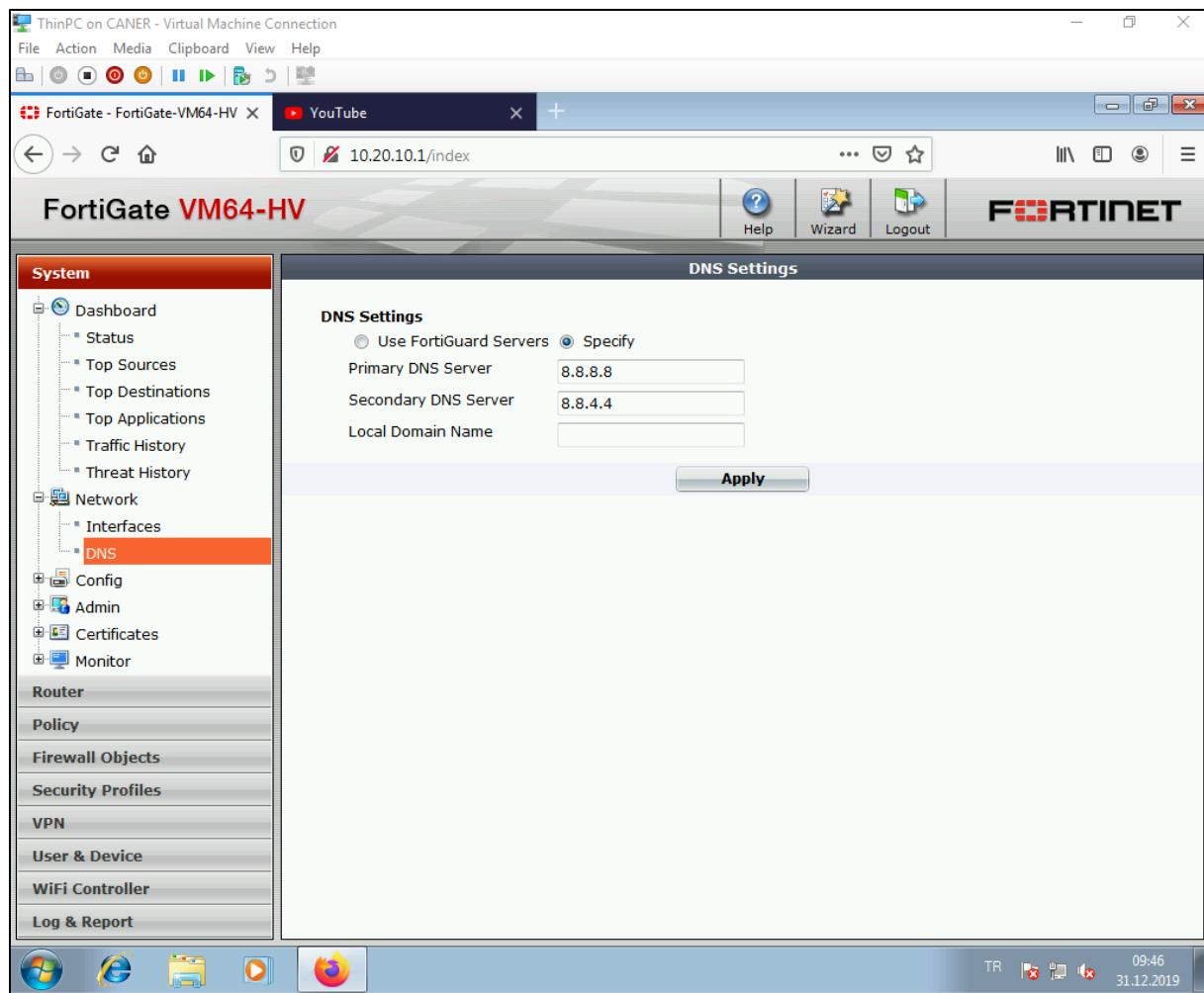


Since Fortinet didn't receive the information directly from BAU, we add a default route to the gateway of BAU's network to access the internet.

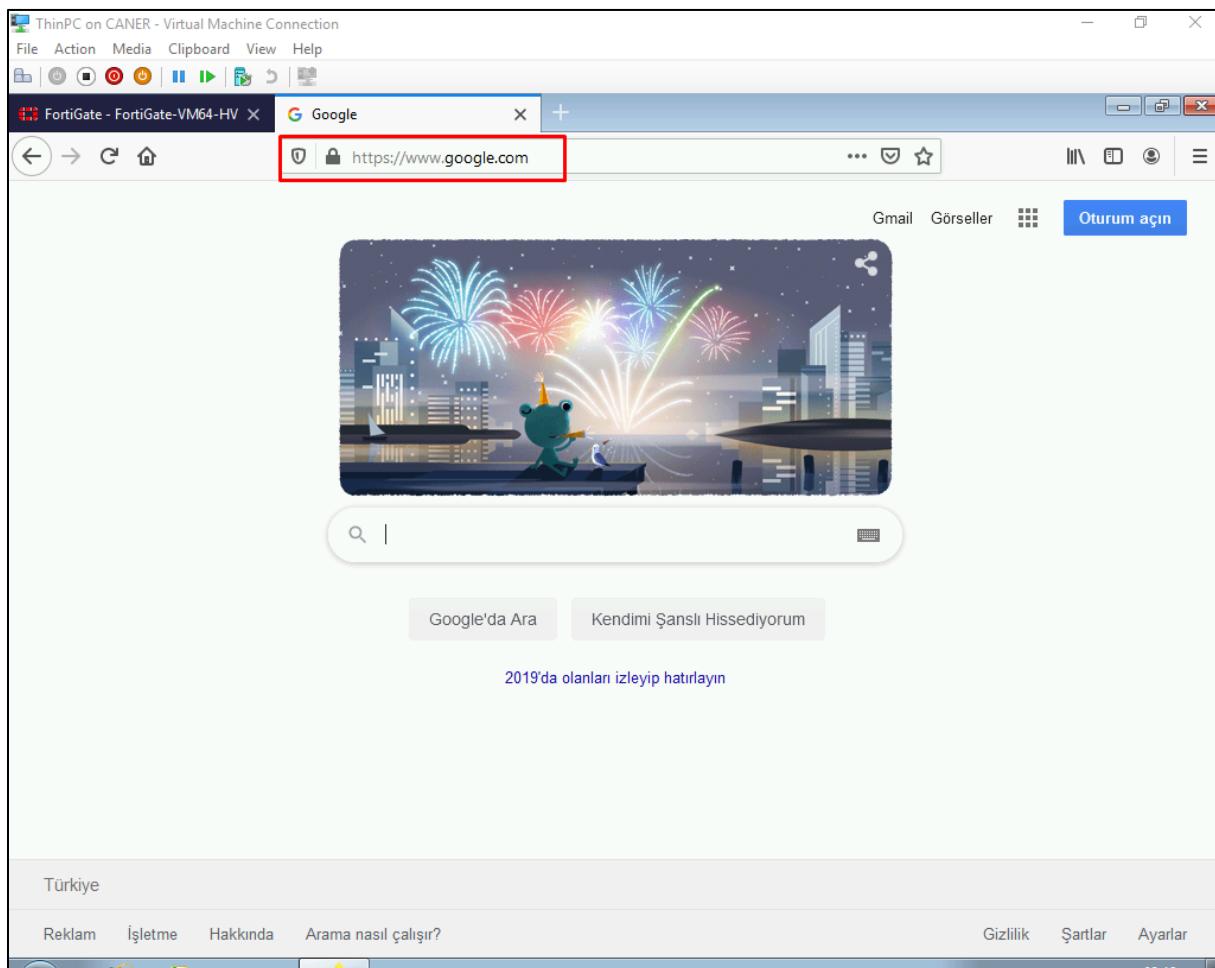


20.1.2020

We change the DNS settings to use Google's DNS.



And now we can connect to the internet since NAT is enabled and access is allowed.



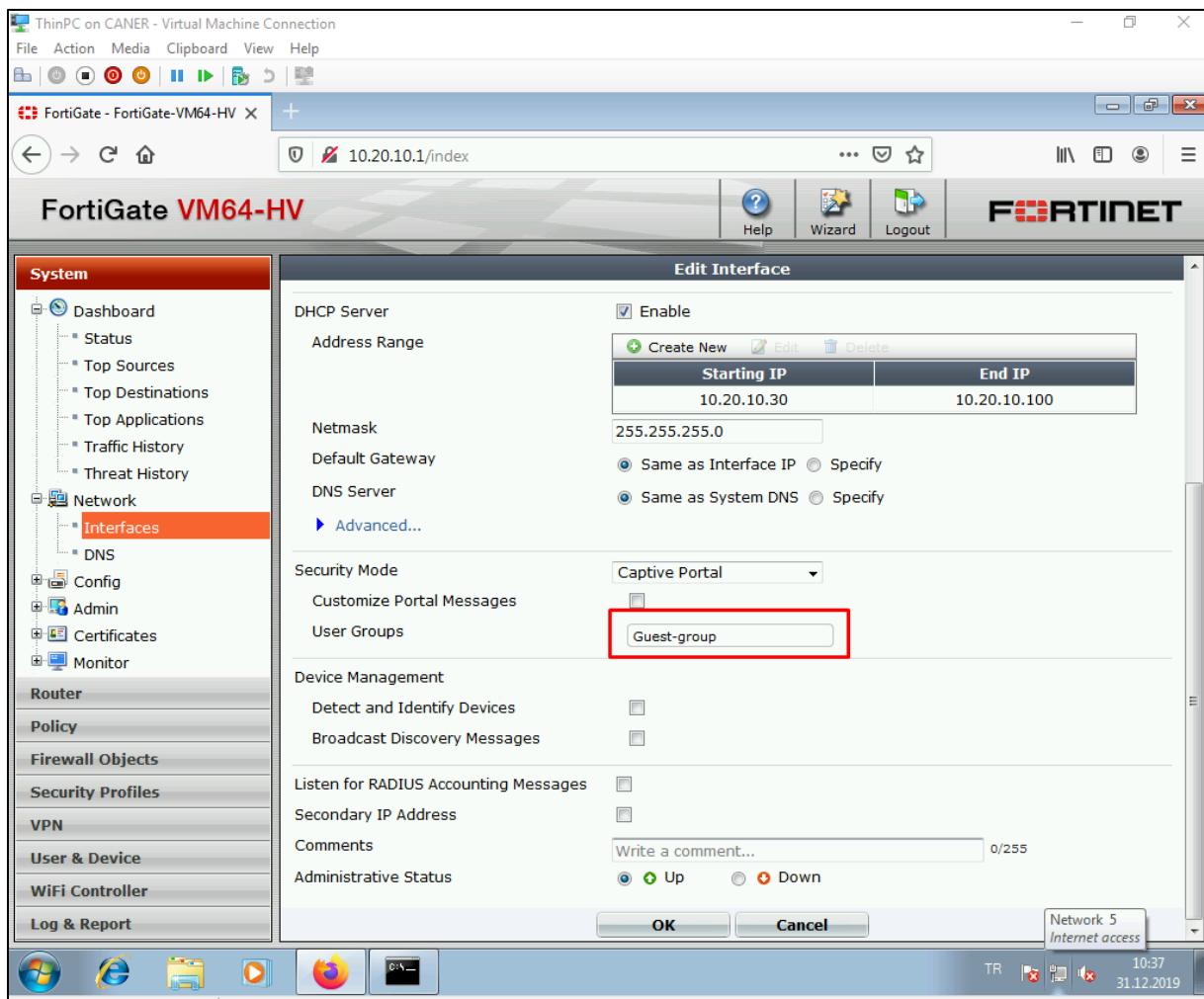
To create a Captive Portal we get to the internal interface and set the security mode.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a 'System' section with 'Dashboard', 'Network' (selected), 'Config', 'Admin', 'Certificates', and 'Monitor'. Under 'Router', there are 'Policy', 'Firewall Objects', 'Security Profiles', 'VPN', 'User & Device', 'WiFi Controller', and 'Log & Report'. The main content area is titled 'Edit Interface' for 'port2(00:15:5D:02:8F:32)'. The interface details include:

- Name:** port2(00:15:5D:02:8F:32)
- Alias:** Internal
- Link Status:** Up
- Type:** Physical Interface
- Addressing mode:** Manual (radio button selected)
- IP/Network Mask:** 10.20.10.1/255.255.255.0
- Administrative Access:** Checkboxes for HTTPS, PING, HTTP, FMG-Access, CAPWAP, SSH, SNMP, TELNET, and FCT-Access are all checked.
- DHCP Server:** Enabled (checkbox checked). Address Range table:

Starting IP	End IP
10.20.10.30	10.20.10.100
- Netmask:** 255.255.255.0
- Default Gateway:** Same as Interface IP (radio button selected)
- DNS Server:** Same as System DNS (radio button selected)
- Security Mode:** A dropdown menu is open, with 'Captive Portal' selected (highlighted by a red box). Other options in the dropdown are: Normal, Wired LAN, Wireless LAN, WAN, Trunk, and Loopback.
- Customize Portal Messages:** Click to add...
- User Groups:** Click to add...

We state a user group. In this case we used the Guest-group but we will change it soon.



20.1.2020

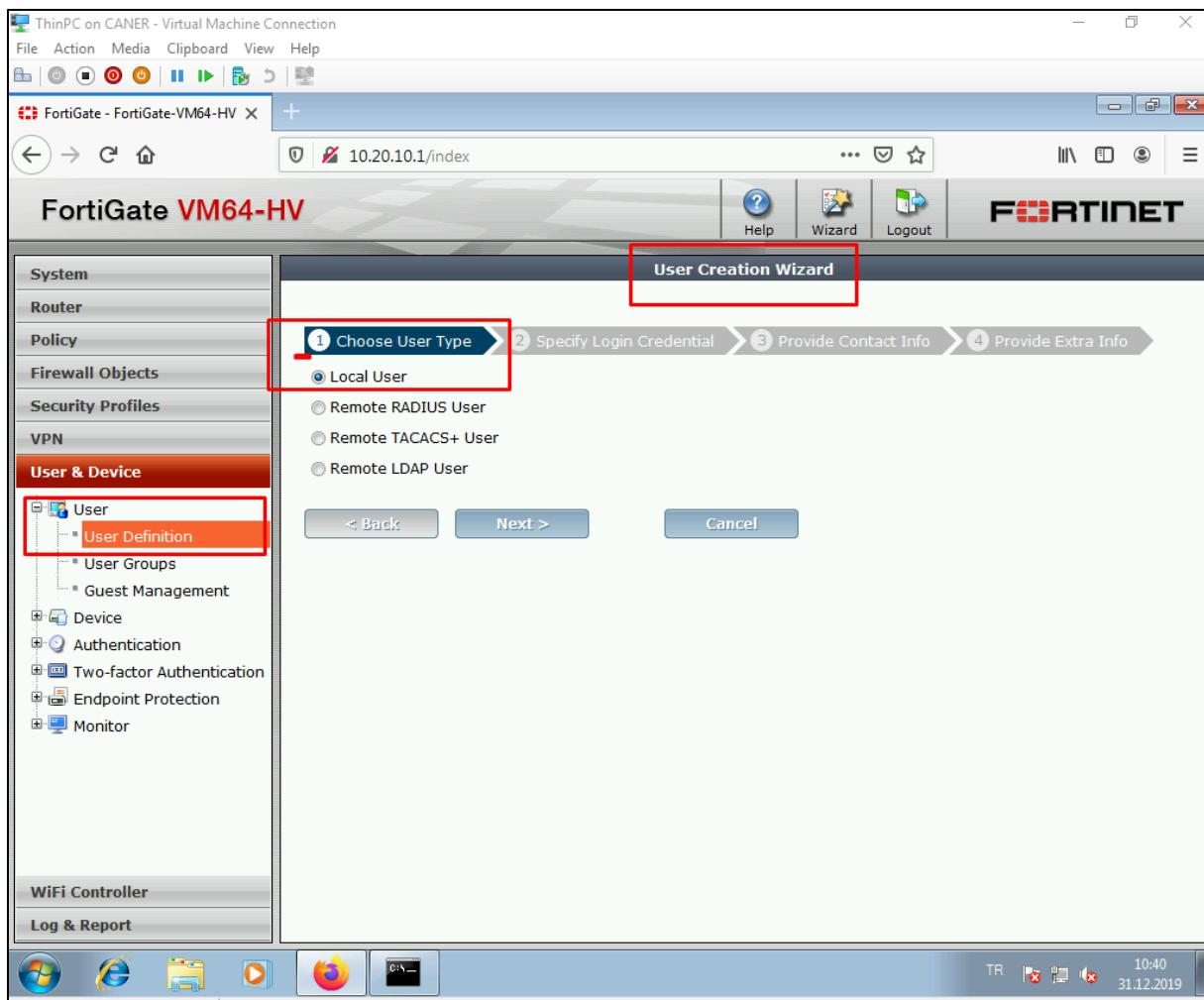
We can manage and peruse the user groups in detail under User & Device tab.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a tree view with 'User & Device' selected. Under 'User & Device', 'User Groups' is also selected and highlighted with a red box. The main content area displays a table of user groups:

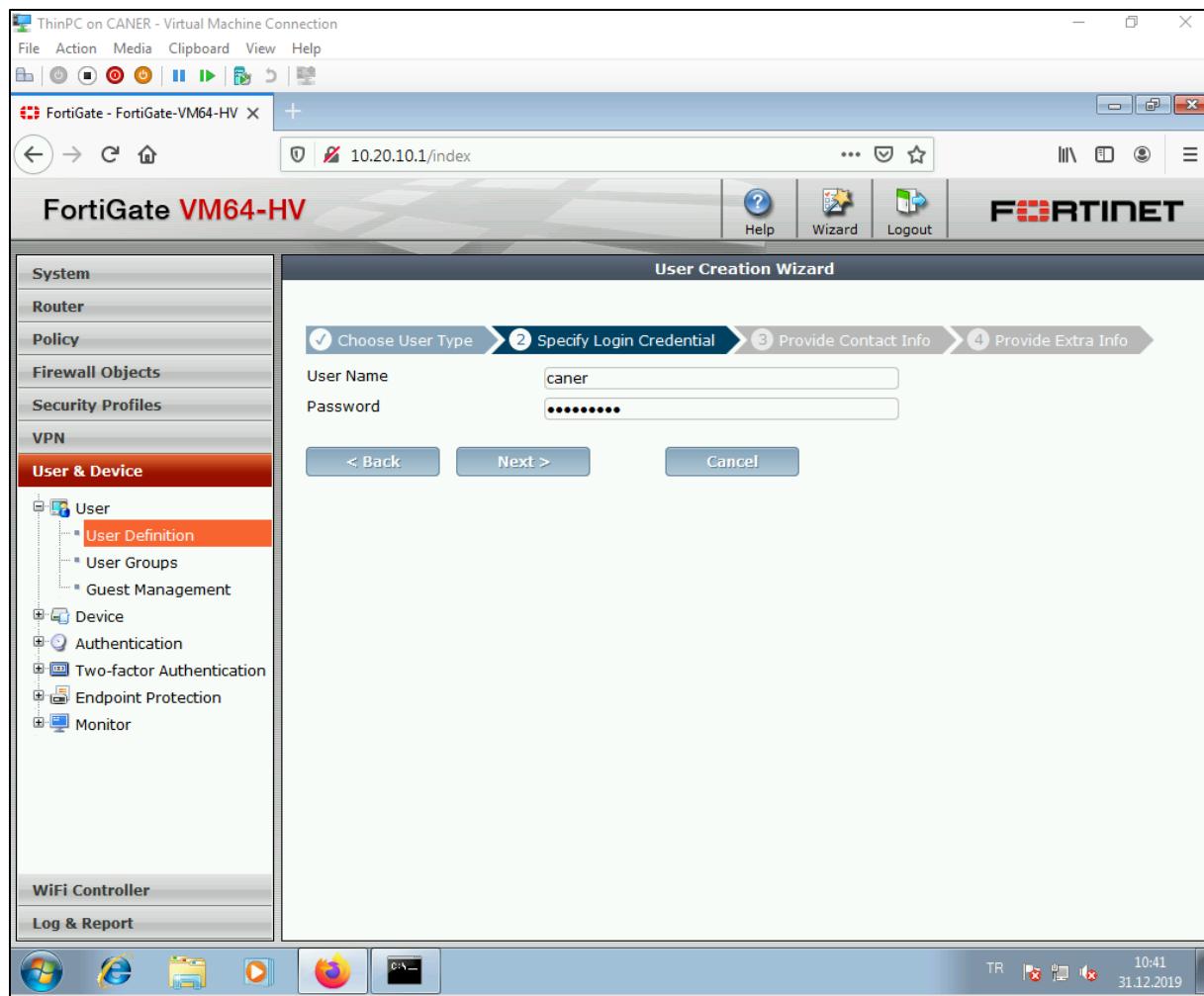
Group Name	Group Type	Members	Ref.
FSSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)	0	
Guest-group (1 Members)	Firewall	guest	0

The 'Guest-group' row is also highlighted with a red box. The status bar at the bottom right shows the time as 10:38 and the date as 31.12.2019.

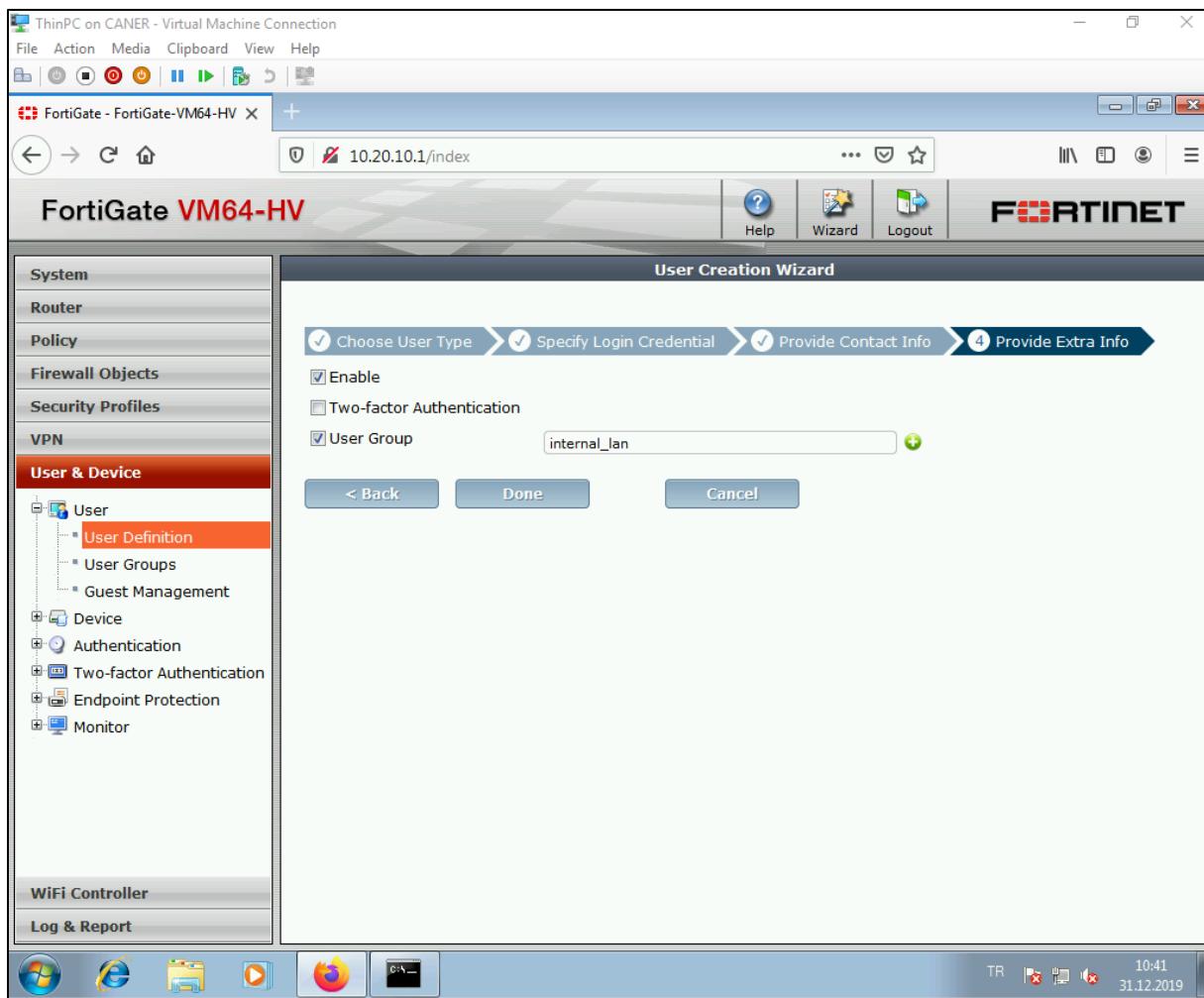
Let's now create a new user to utilize the captive portal.



We choose local user and define the login credentials.



We put this user into the new user group internal_lan.



20.1.2020

Now, when we look at the new group, we can see our new users.

The screenshot shows the FortiGate VM64-HV interface. The left sidebar has a red highlight over the 'User & Device' section, specifically on the 'User Groups' item under 'User'. The main window displays a table of user groups:

Group Name	Group Type	Members	Ref.
FSSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)	0	
Guest-group (1 Members)	Firewall	guest	0
internal_lan (2 Members)	Firewall	caner umut	0

The 'internal_lan' group is highlighted with a red border. The status bar at the bottom right shows the date and time: 10:42 31.12.2019.

We add the internal_lan to the captive portal rules as well.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar is the navigation menu:

- System
 - Dashboard
 - Status
 - Top Sources
 - Top Destinations
 - Top Applications
 - Traffic History
 - Threat History
- Network
 - Interfaces
 - DNS
- Config
- Admin
- Certificates
- Monitor

The main content area is titled "Edit Interface". It shows the configuration for a network interface:

- DHCP Server**: Enabled, Address Range: Starting IP 10.20.10.30, End IP 10.20.10.100, Netmask 255.255.255.0, Default Gateway Same as Interface IP, DNS Server Same as System DNS.
- Security Mode**: Captive Portal.
- User Groups**: internal_lan (highlighted with a red box), Guest-group.
- Device Management**: Detect and Identify Devices, Broadcast Discovery Messages.
- Comments**: Write a comment... 0/255.

The bottom status bar shows system icons and the time: 10:42 31.12.2019.

20.1.2020

When we get to the Firewall Objects, under addresses. internal_lan should be already there automatically but we could also create it easily.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a 'Firewall Objects' section with 'Address' selected, which is further expanded to show 'Addresses'. The main content area displays a table of addresses:

Name	Address/FQDN	Interface	Type	Show in Address List
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	IP Range	✓
all	0.0.0.0/0.0.0.0	Any	Subnet	✓
internal_lan	10.20.10.0/255.255.255.0	Any	Subnet	✓

The 'internal_lan' row is highlighted with a red border. The interface includes standard browser navigation buttons (back, forward, search) and a Fortinet logo at the top right.

Now, we modify the policies to allow internal_lan specifically to access to the internet.

The screenshot shows the FortiGate VM64-HV interface. The left sidebar has a tree view with 'Policy' selected. The main area displays a table of firewall policies:

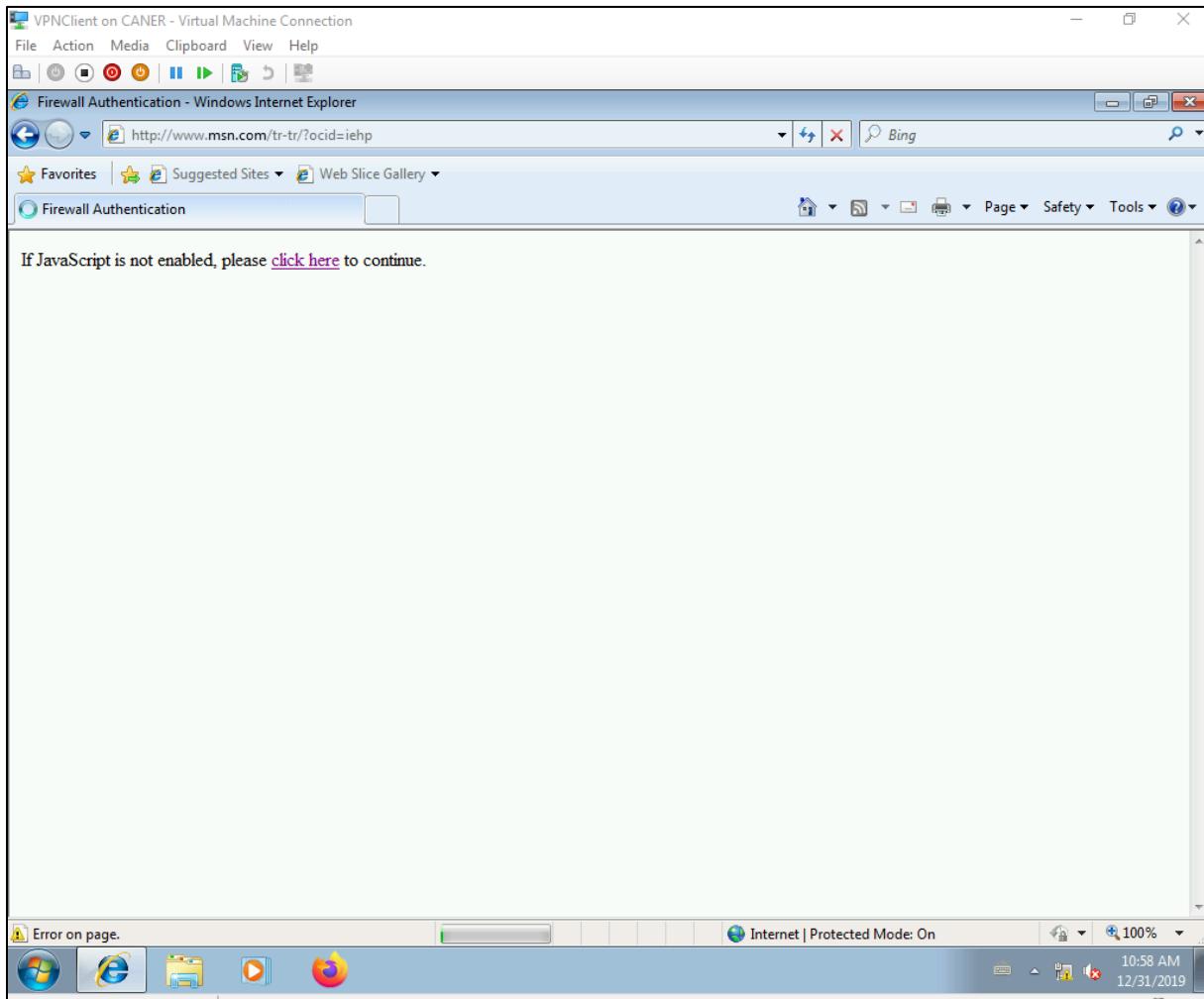
Seq.#	Source	Destination	Schedule	Service	Action
1	internal_lan	all	always	ALL	✓ Accept
2	all	all	always	ALL	✓ Accept
3	all	all	always	ALL	✗ Deny

The first two rows (Seq# 1 and 2) have a red border around them, indicating they are the specific rules being modified. The third row (Seq# 3) is implicitly defined by the system.

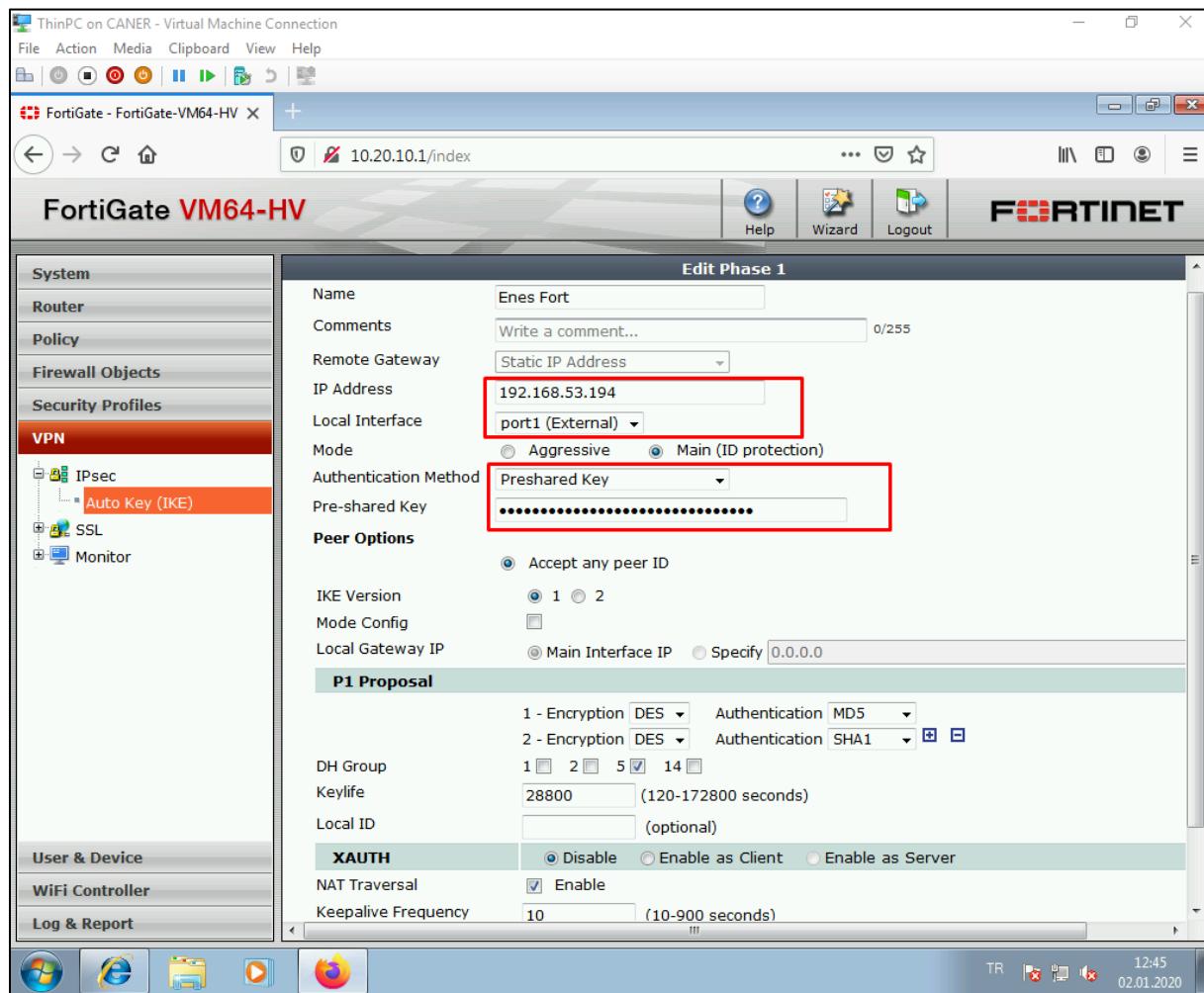
When a host tries to connect to the internet using the internal _lan group's IP addresses. This Captive Portal page pops up. We log in using a user's credentials.



Then, we can access the internet. However, I don't recommend IE.

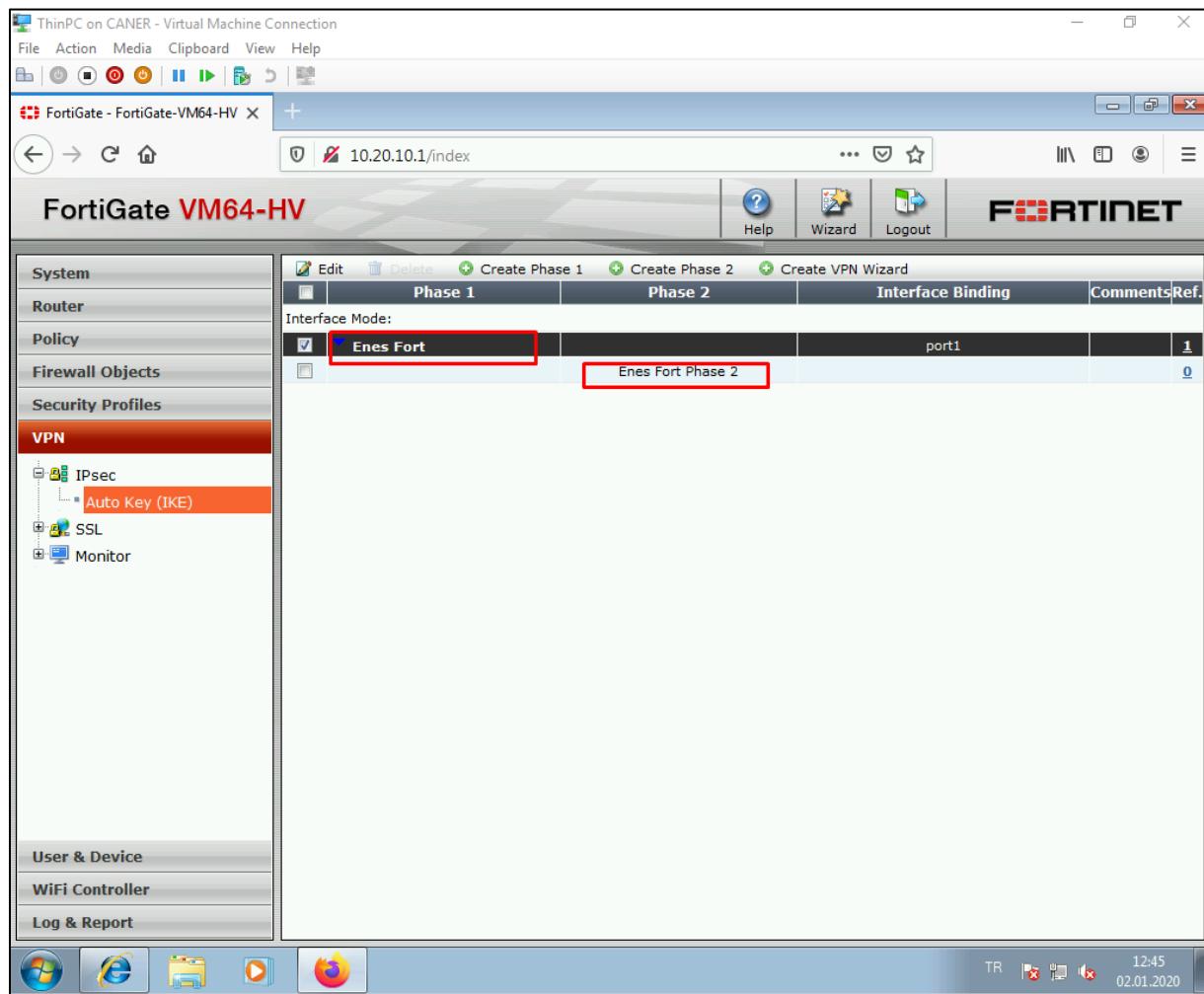


Now that the unstimulating stuff is out of the way, let's establish an IPSec Tunnel. We go to the VPN tab and click on Create Phase 1 to start the wizard.



We name the tunnel and use the other site's public IP address and our port1 (WAN interface) for the local interface. We describe a pre-shared key and leave every other encryption setting to default. The other site must do the vice versa with out IP address, their WAN port and the same pre-shared key and encryption details.

We then select freshly created Phase 1 to create a Phase 2 related to that. The default settings are sufficient. The Phase 2 should look like this:



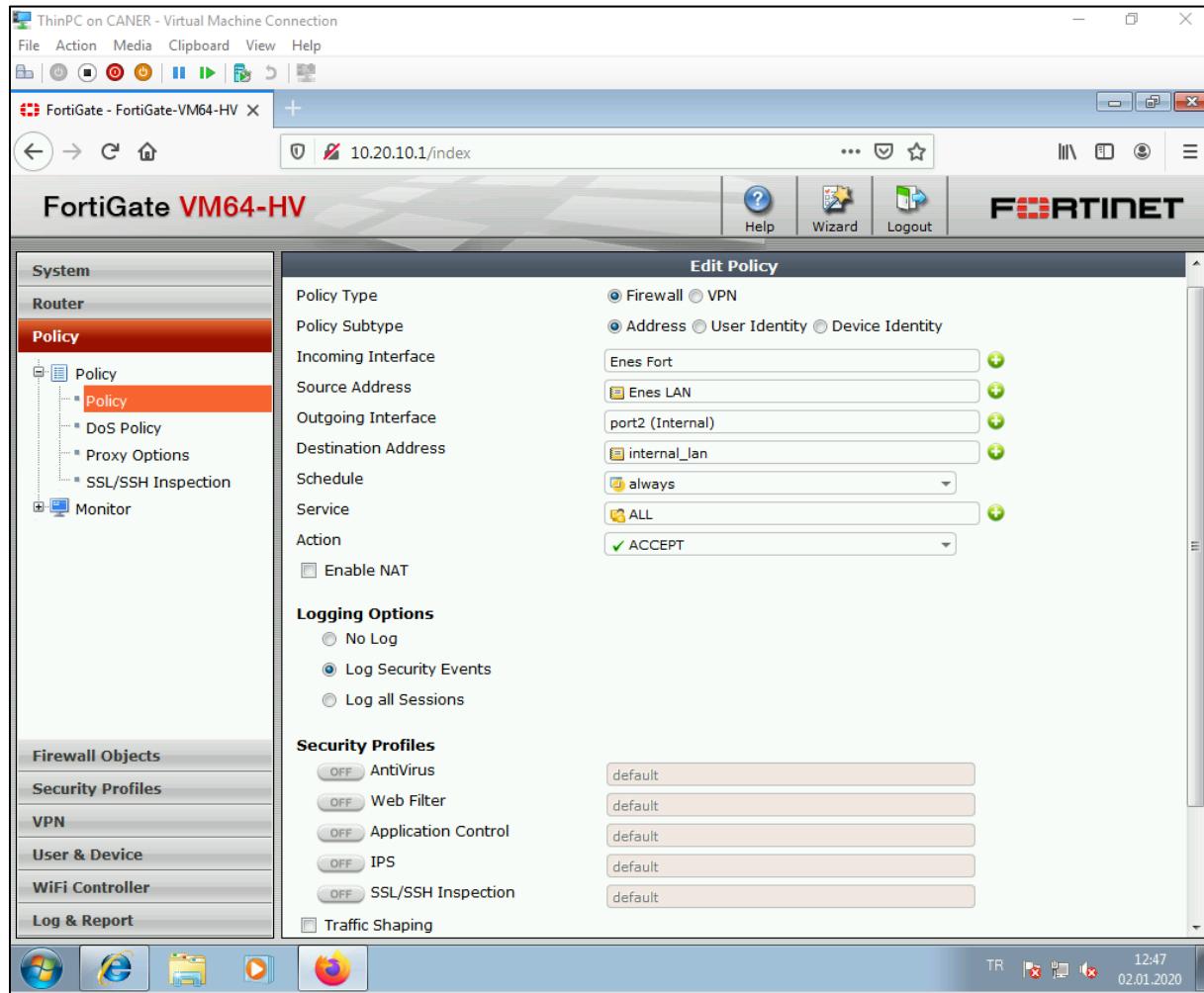
We add the other site's internal networks under Addresses under Firewall Objects so that defining policies is simpler.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a red highlight over the 'Firewall Objects' section, which is expanded to show 'Address' and 'Addresses'. The 'Addresses' item is also highlighted with a red box. The main content area displays a table of addresses:

Name	Address/FQDN	Interface	Type	Show in Address List
Enes LAN	10.30.10.0/255.255.255.0	Any	Subnet	<input checked="" type="checkbox"/>
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	IP Range	<input checked="" type="checkbox"/>
all	0.0.0.0/0.0.0.0	Any	Subnet	<input checked="" type="checkbox"/>
internal_lan	10.20.10.0/255.255.255.0	Any	Subnet	<input checked="" type="checkbox"/>

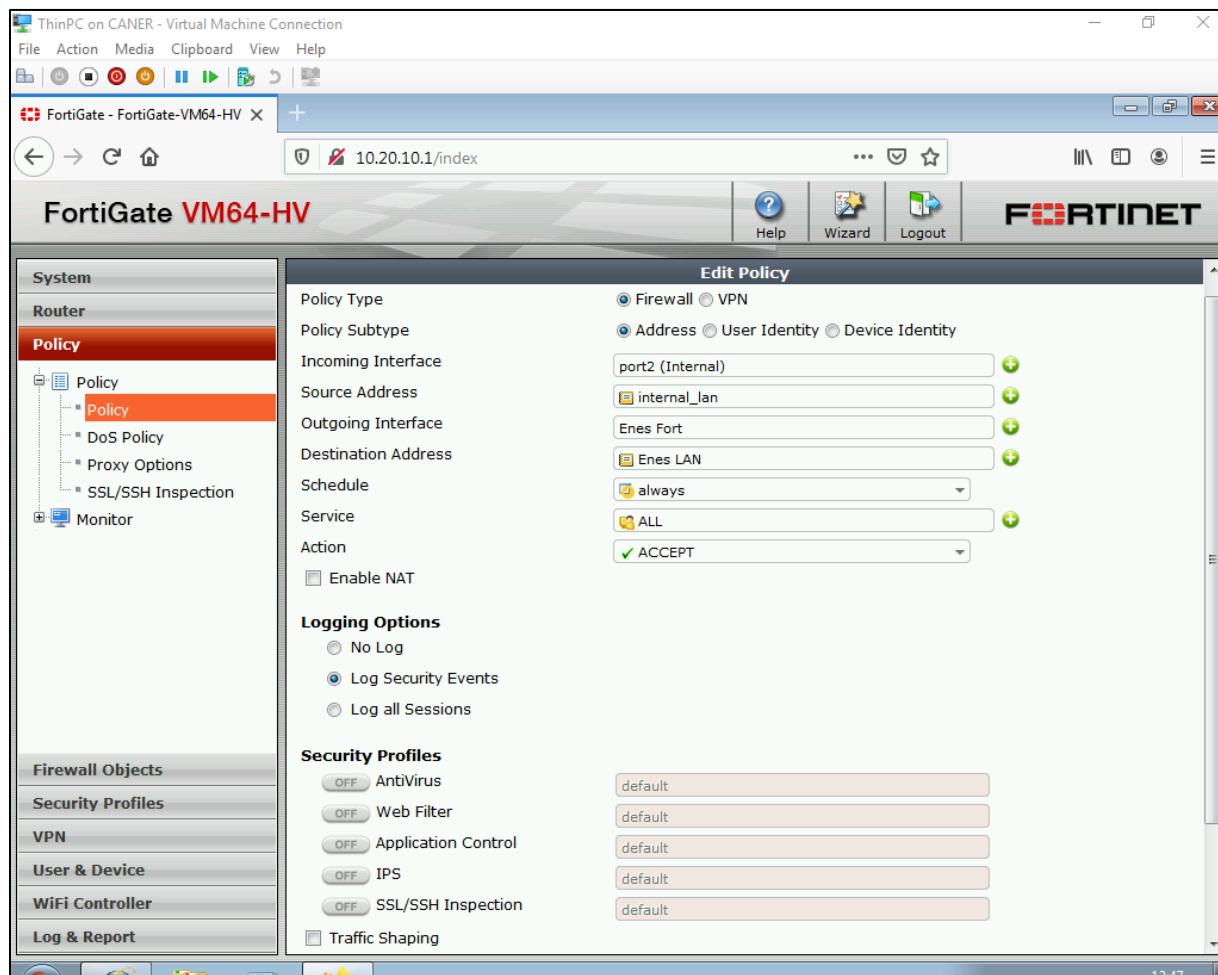
The bottom status bar shows the date and time: 02.01.2020 12:46.

We state the following rules since FortiGate VM64-HV doesn't really support site-to-site tunnels as a pre set rules system. I'd definitely not recommend using this outside of a lab.



Note that we chose the tunnel as an interface.

And the vice versa rule is also necessary.



The policies should like this.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar navigation bar includes: System, Router, Policy (selected), Firewall Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The main content area displays a table of security policies:

Seq.#	Source	Destination	Schedule	Service	Action
1	Enes LAN	internal_lan	always	ALL	✓ Accept
2	internal_lan	Enes LAN	always	ALL	✓ Accept
3	internal_lan	all	always	ALL	✓ Accept
4	all	all	always	ALL	✓ Accept
5	all	all	always	ALL	✗ Deny

The first two rows (Seq# 1 and 2) are highlighted with a red box. The last row (Seq# 5) has a yellow background.

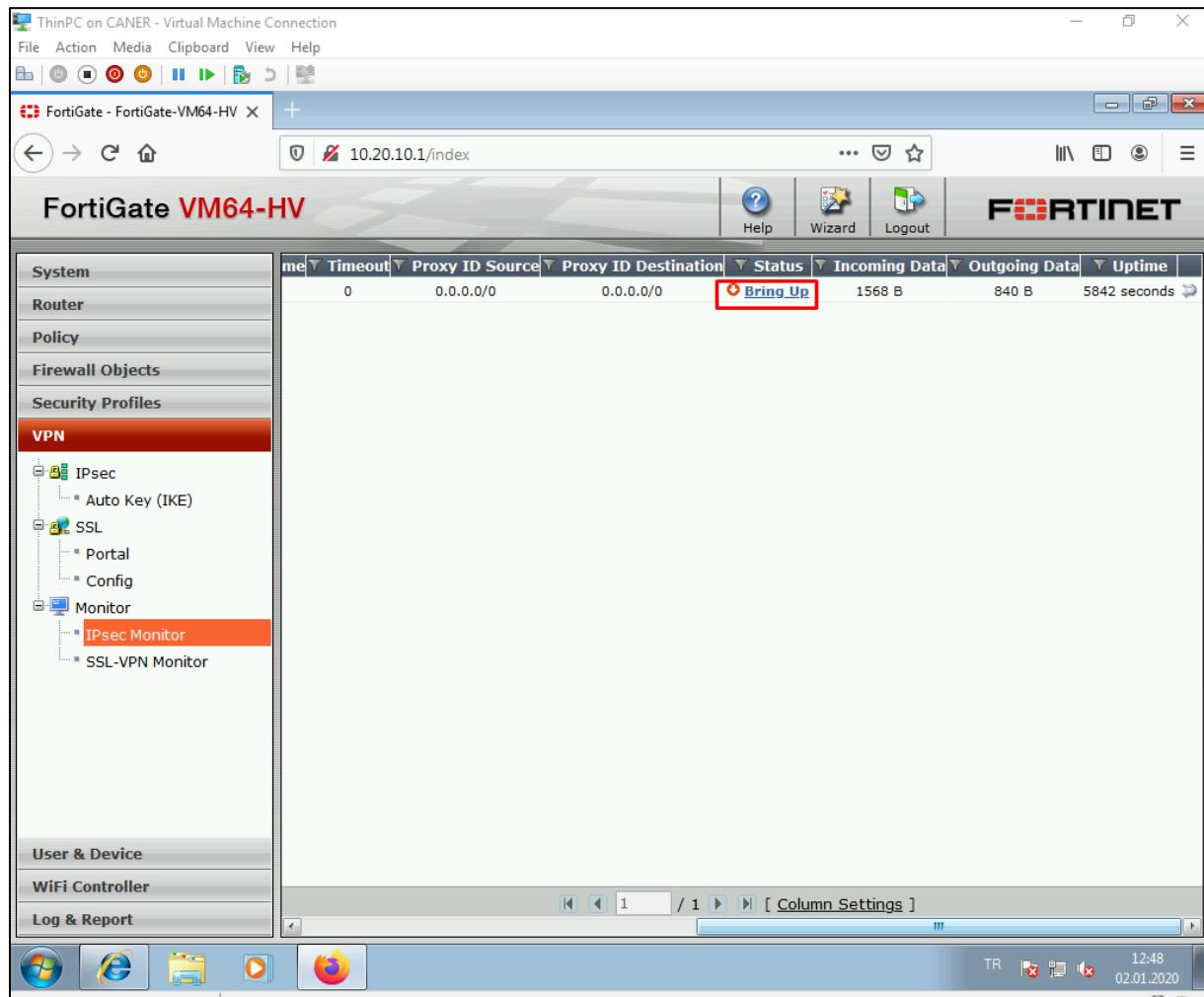
20.1.2020

Now, when we get to the VPN tab and click on Monitor we should see the tunnel that we named.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar has a 'VPN' section highlighted in orange, containing 'IPsec', 'SSL', and 'Monitor' sub-sections. The 'IPsec Monitor' item under 'Monitor' is also highlighted with a red box. The main content area displays a table titled 'IPsec Monitor'. The table has columns: Name, Type, Remote Gateway, Remote Port, Username, Timeout, Proxy ID Source, and Proxy. One row in the table is highlighted with a red box, showing 'Enes Fort' as the name, 'Static IP or Dynamic DNS' as the type, '192.168.53.194' as the remote gateway, and '0' as the remote port. The table also includes a 'Column Settings' link at the bottom.

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source	Proxy
Enes Fort	Static IP or Dynamic DNS	192.168.53.194	0		0		0.0.0.0/0

Currently, it's down; however, if we have set everything correctly on both ends, mirroring each other, and made sure that the pre-shared key and the encryption details are the same when we click on Bring Up, it should work.

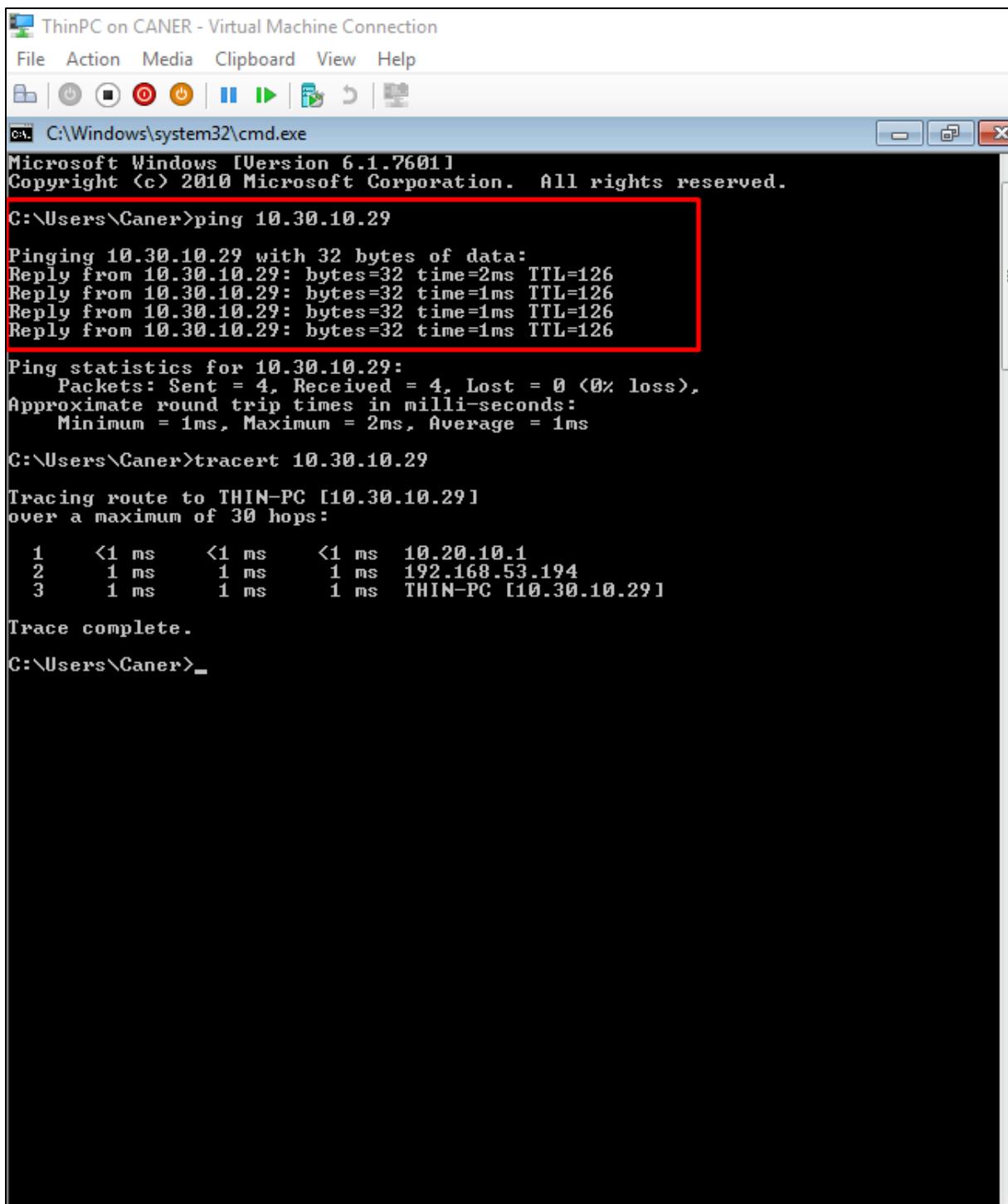


20.1.2020

It works beautifully.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar contains navigation links: System, Router, Policy, Firewall Objects, Security Profiles, VPN (selected), User & Device, WiFi Controller, and Log & Report. Under the VPN section, IPsec, SSL, Monitor (selected), and SSL-VPN Monitor are listed. The main content area displays a table with the following columns: Timeout, Proxy ID Source, Proxy ID Destination, Status, Incoming Data, Outgoing Data, and Uptime. A single row is present with values: 1743, 0.0.0.0/0, 0.0.0.0/0, **Bring Down** (button highlighted with a red box), 1712 B, 900 B, and 5903 seconds. The status column shows a green icon and the text "Bring Down".

Now, we can ping from site 1's internal LAN to site 2's internal LAN.



ThinPC on CANER - Virtual Machine Connection

File Action Media Clipboard View Help

cmd C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright © 2010 Microsoft Corporation. All rights reserved.

```
C:\Users\Caner>ping 10.30.10.29
Pinging 10.30.10.29 with 32 bytes of data:
Reply from 10.30.10.29: bytes=32 time=2ms TTL=126
Reply from 10.30.10.29: bytes=32 time=1ms TTL=126
Reply from 10.30.10.29: bytes=32 time=1ms TTL=126
Reply from 10.30.10.29: bytes=32 time=1ms TTL=126

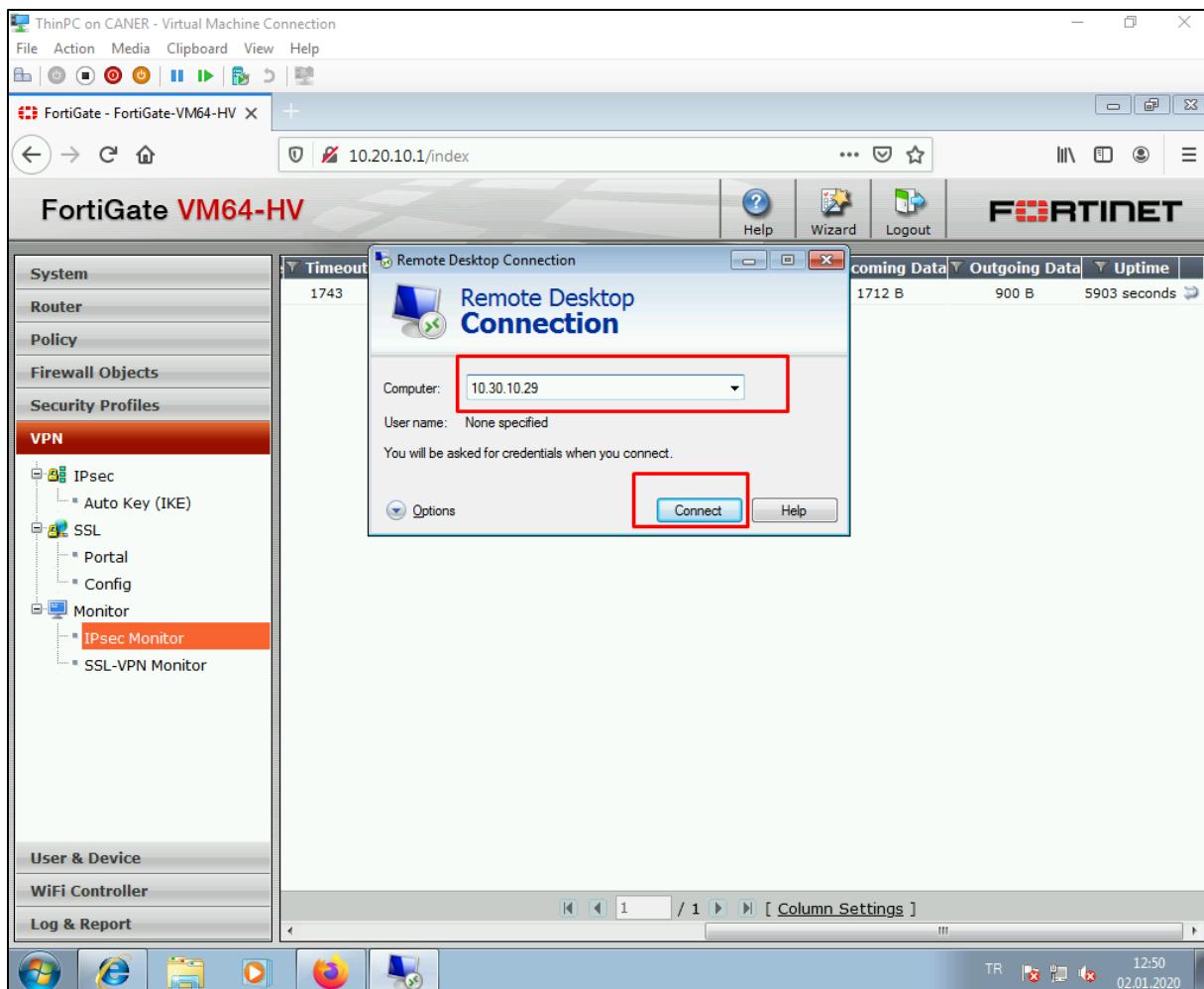
Ping statistics for 10.30.10.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

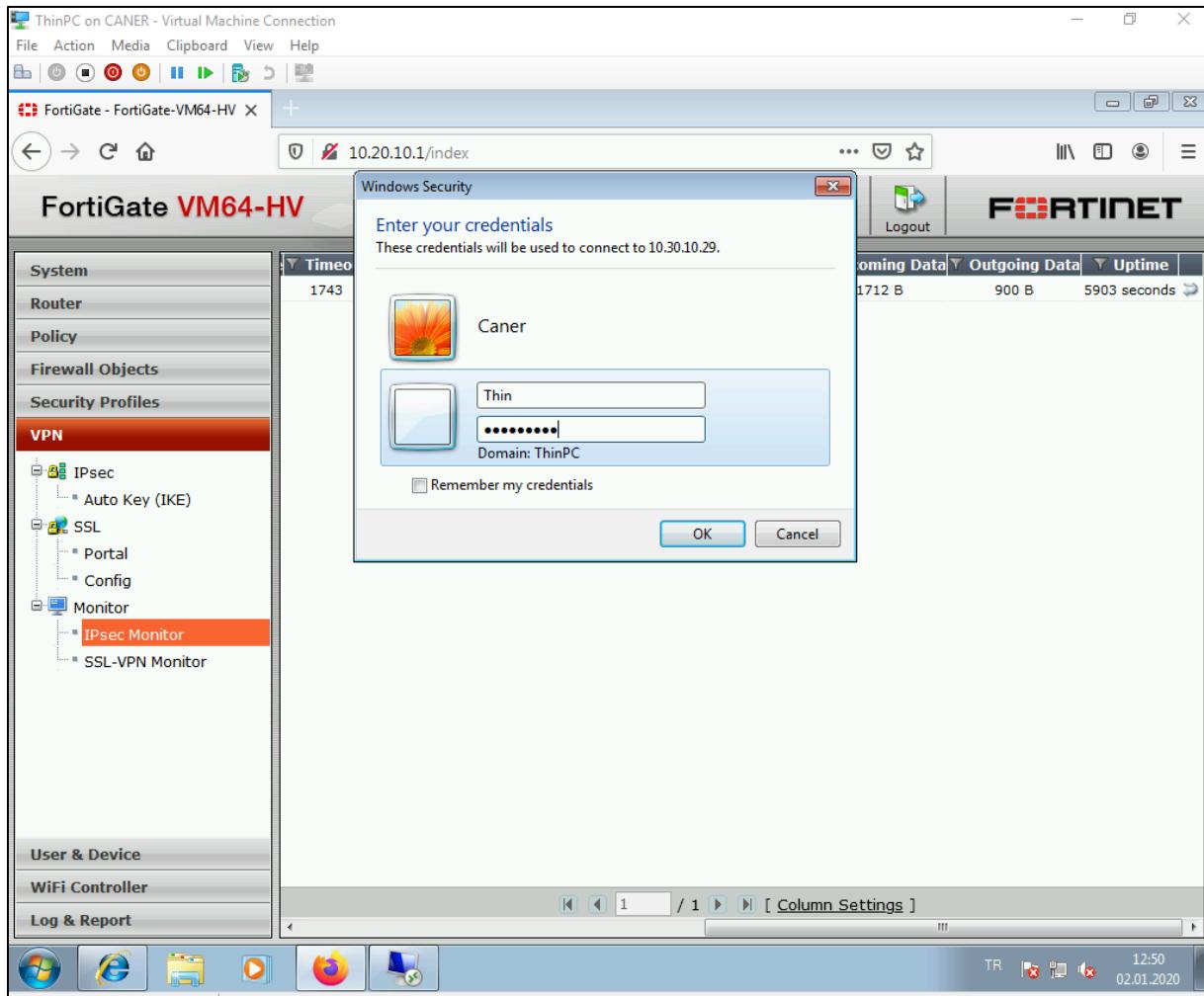
C:\Users\Caner>tracert 10.30.10.29
Tracing route to THIN-PC [10.30.10.29]
over a maximum of 30 hops:
  1    <1 ms      <1 ms      <1 ms  10.20.10.1
  2      1 ms      1 ms      1 ms  192.168.53.194
  3      1 ms      1 ms      1 ms  THIN-PC [10.30.10.29]

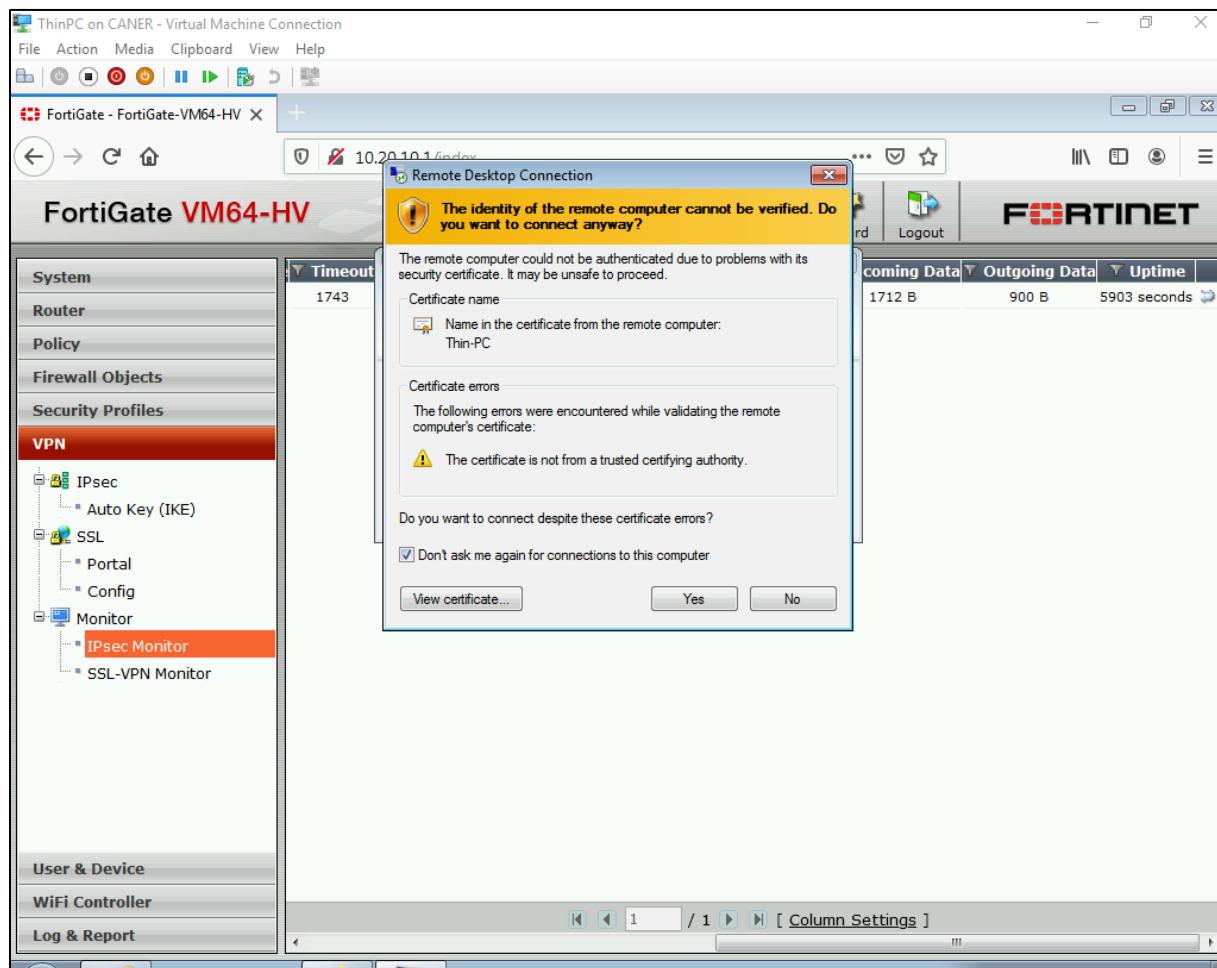
Trace complete.

C:\Users\Caner>
```

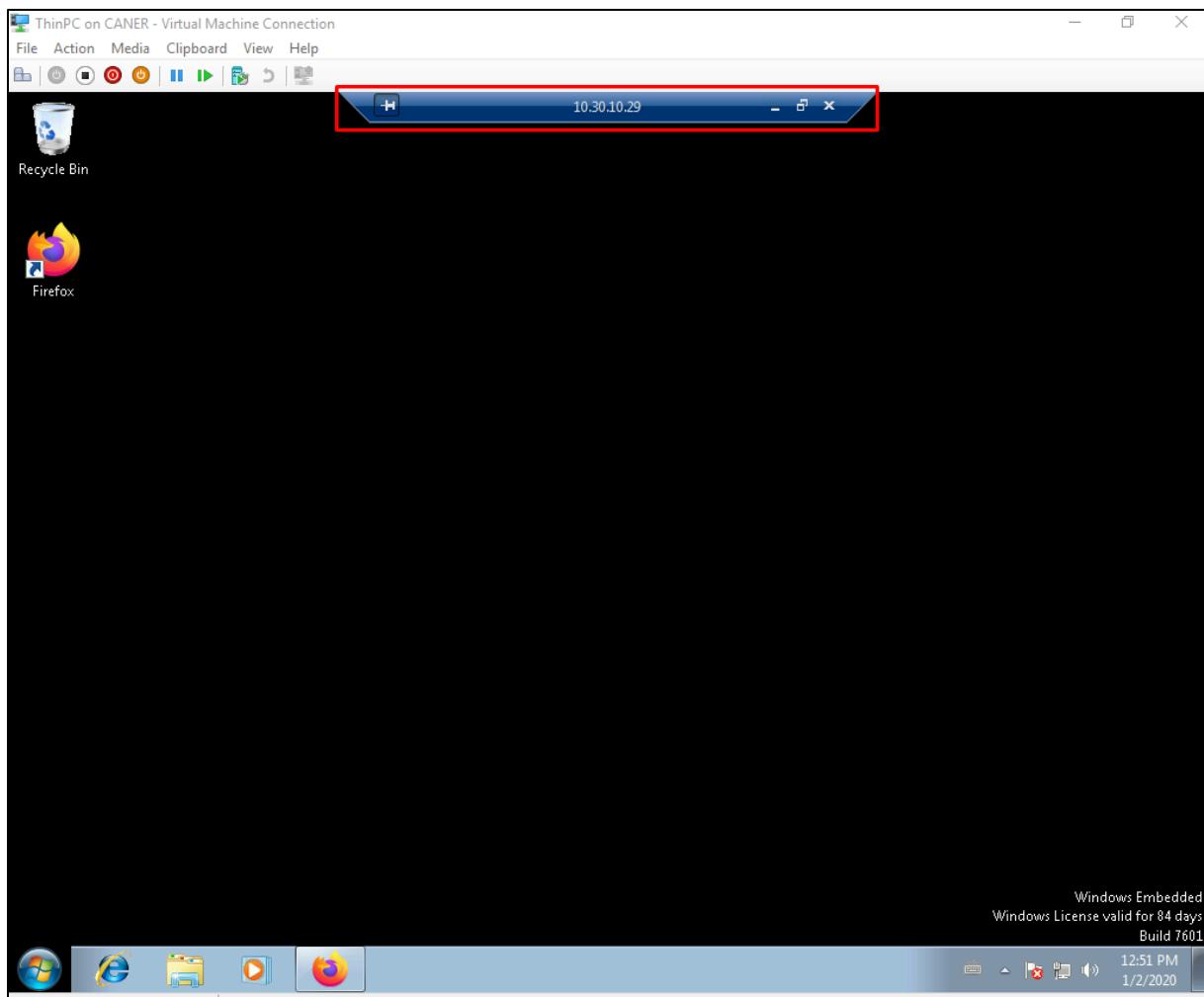
We can also easily do RDP by entering the local IP addresses of the other site.







We're in!



This demonstrates the IPSec Tunnel working and completes the Fortinet part of this project.

3. Conclusion

Firewalls are powerful but delicate tools in network connectivity and safety. Customization of networking rules and being able to block or allow access to certain networks websites or even hosts is brilliant in a knowledgeable administrator's hand. However, it's also very easy to set up a traffic on a wrong order and completely block tunneling or internet access. Fortunately, I have been quite meticulous with policy and rule setting that I never faced such a problem. Utilizing Captive Portals adds another layer of security that we all can appreciate.

4. Evaluation

FortiGate VM64-HV didn't allow multiple NICs so we couldn't test complex topologies as we originally intended to. It also doesn't seem to implicitly support site-to-site tunnels as it does client-to-site tunnels. A different version should definitely be tested to compare.

Kerio Control is easy to use, write rules and it establishes a default internal DHCP pool.

pfSense's webConfigure user interface is a design nightmare. It's not harder to use compared to the other firewalls but the user interface is very unintuitive and just ugly.