Firewall

Contents

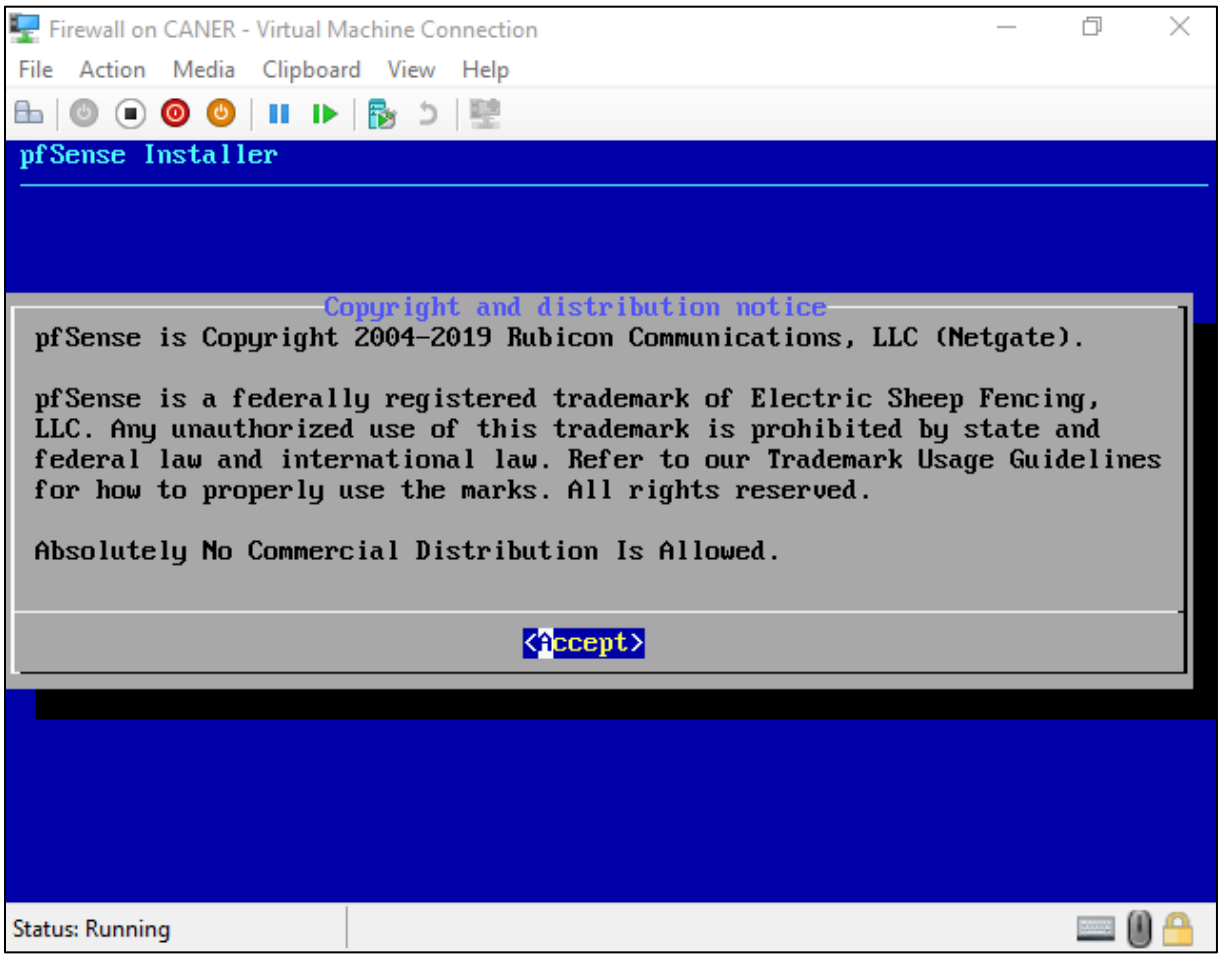
1. Purpose

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.

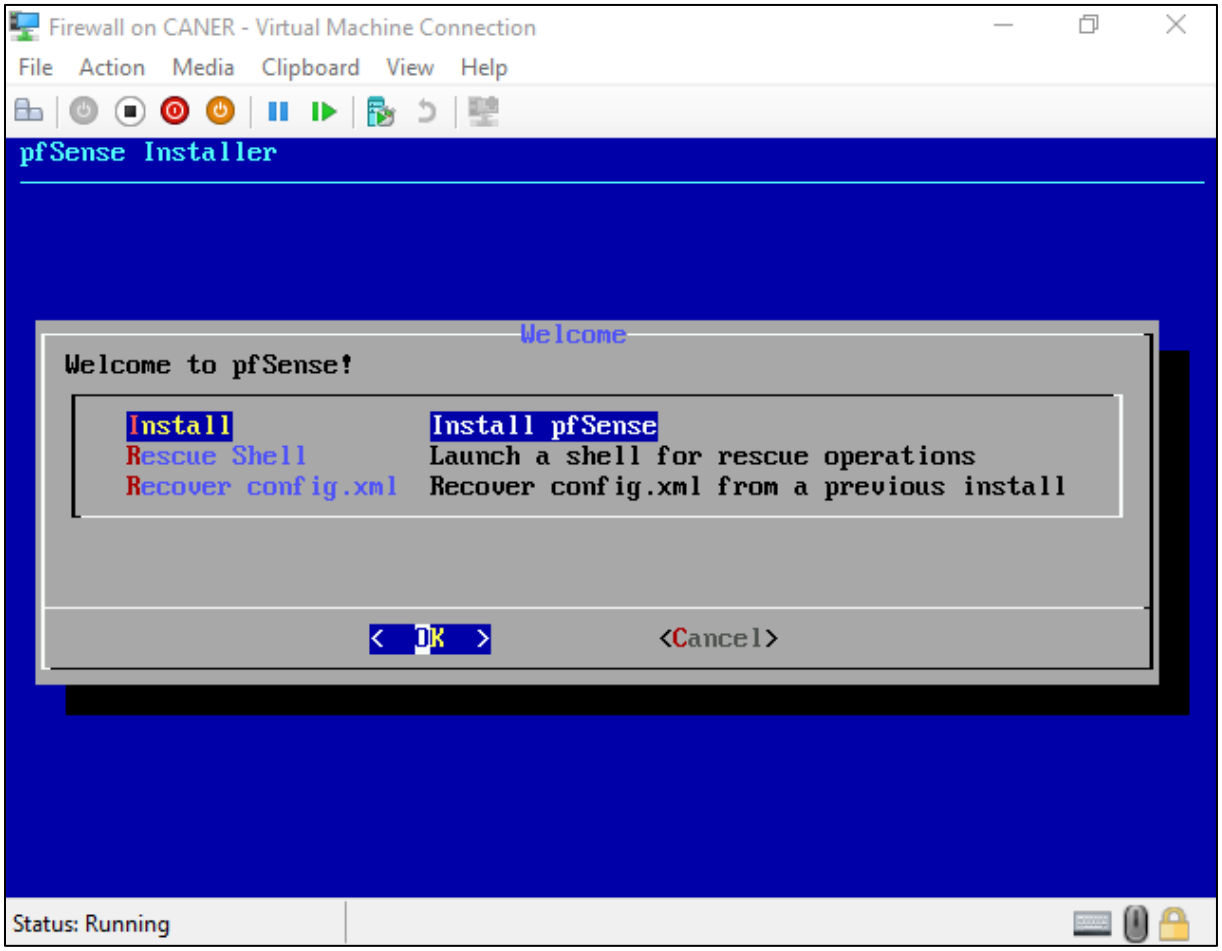
2. Procedure

1) pfSense

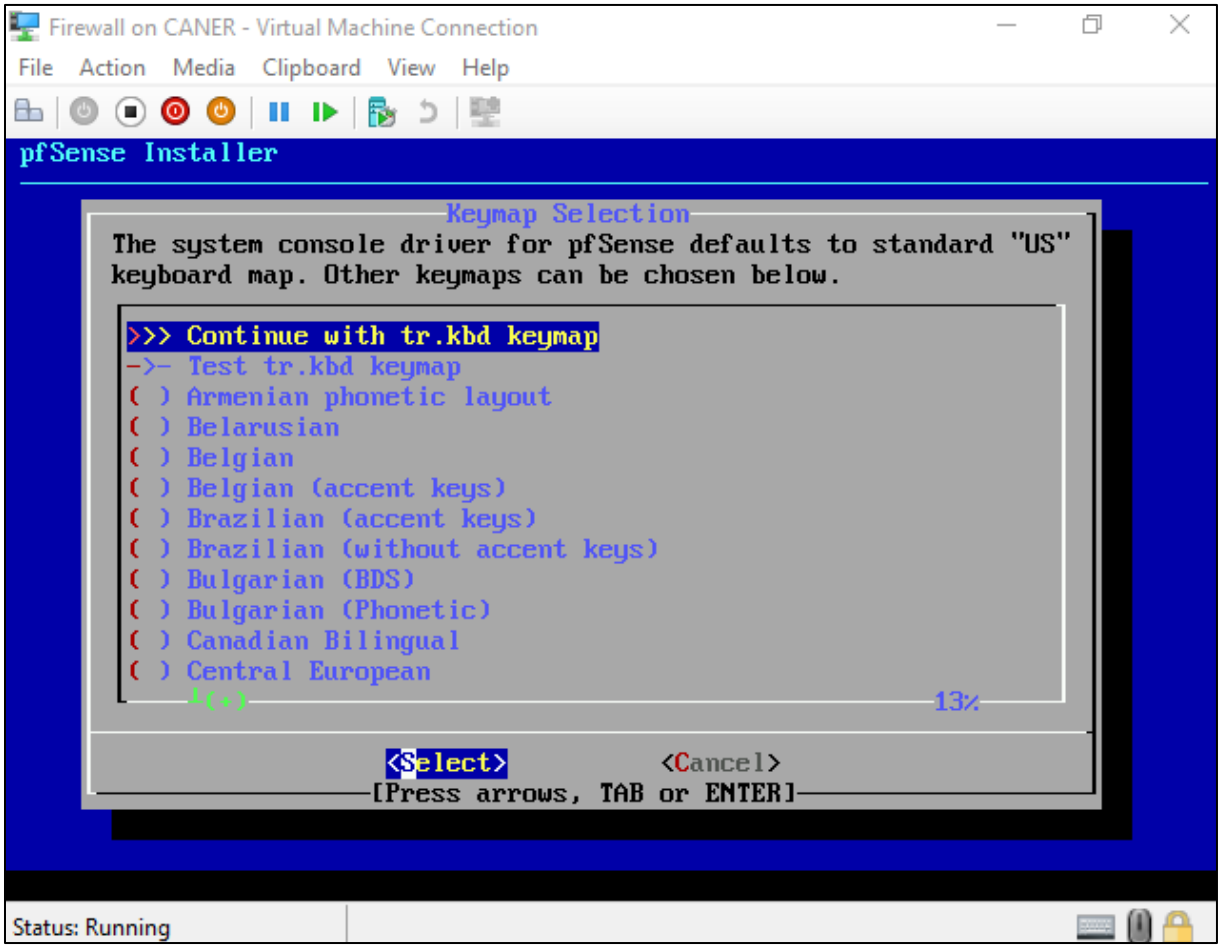
The first firewall we'll demonstrate is pfSense. Once we set up a virtual machine with the PfSense image on the media drive and start it, the pfSense Installer runs. Please note that you must have at least 2 network interface cards for a firewall to properly work; one for your internal topology and one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



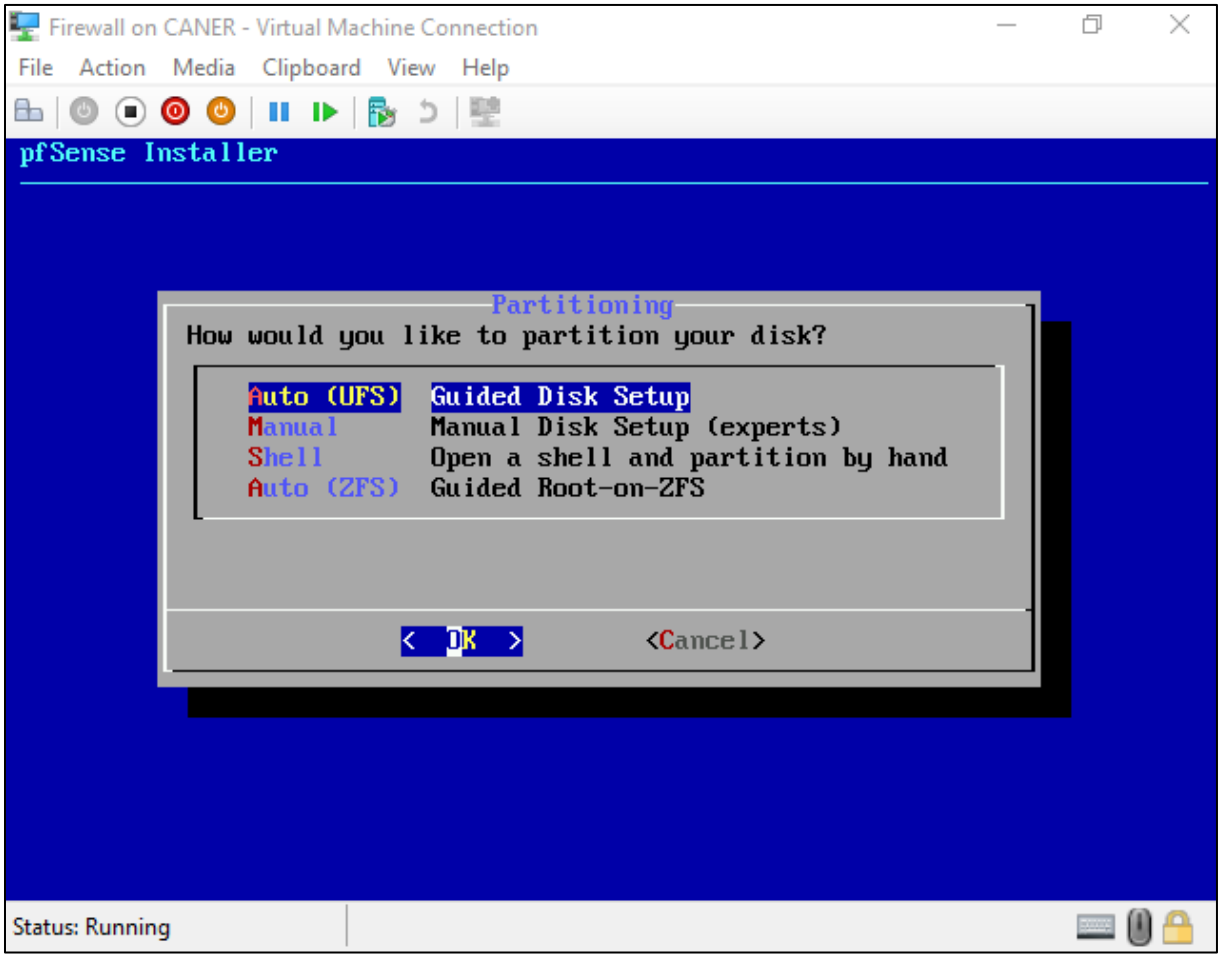
We select Install pfSense.



We determine which keyboard we will be using.

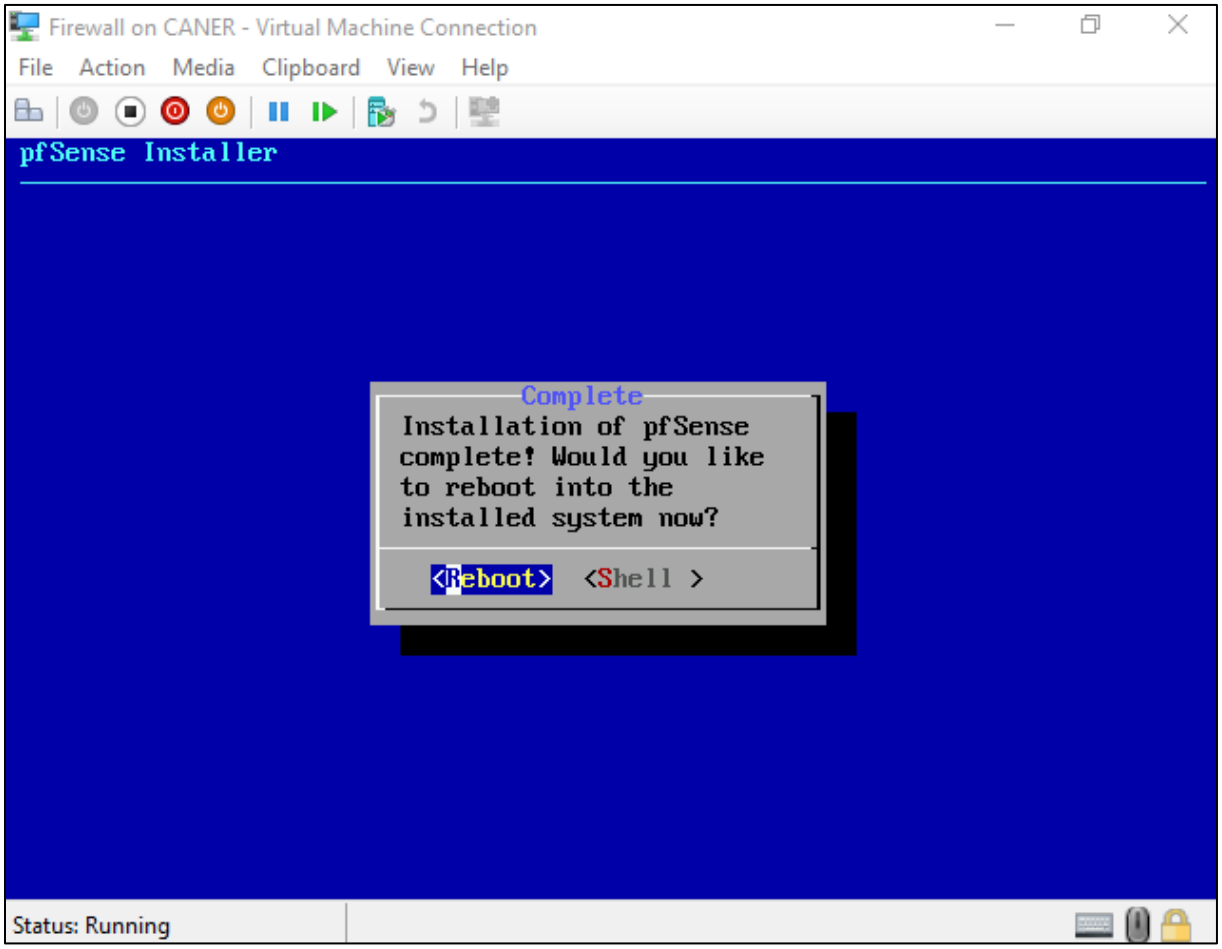


We use Guided Disk Setup.

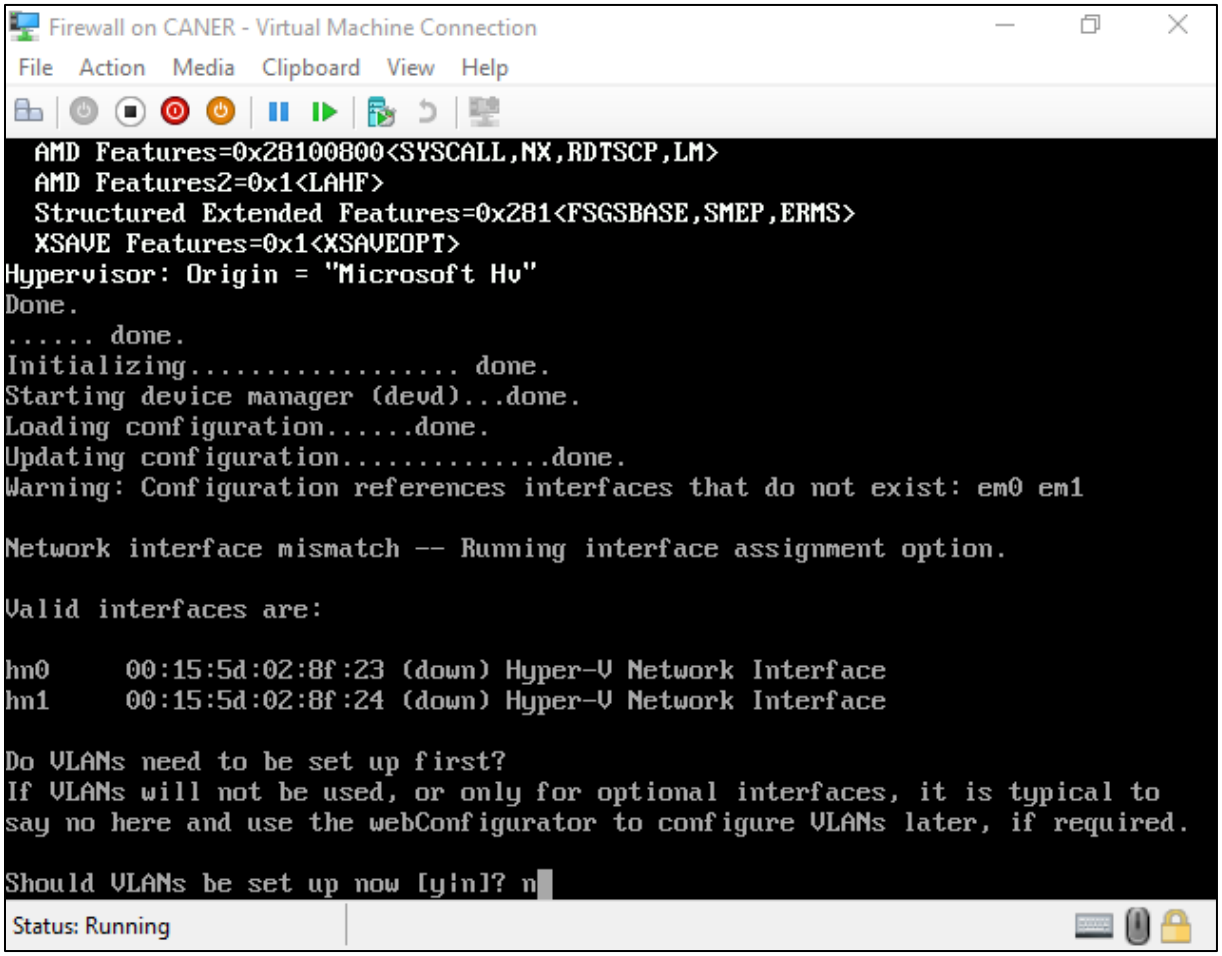


After installation finishes, we refuse to open a shell to make any modifications.

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



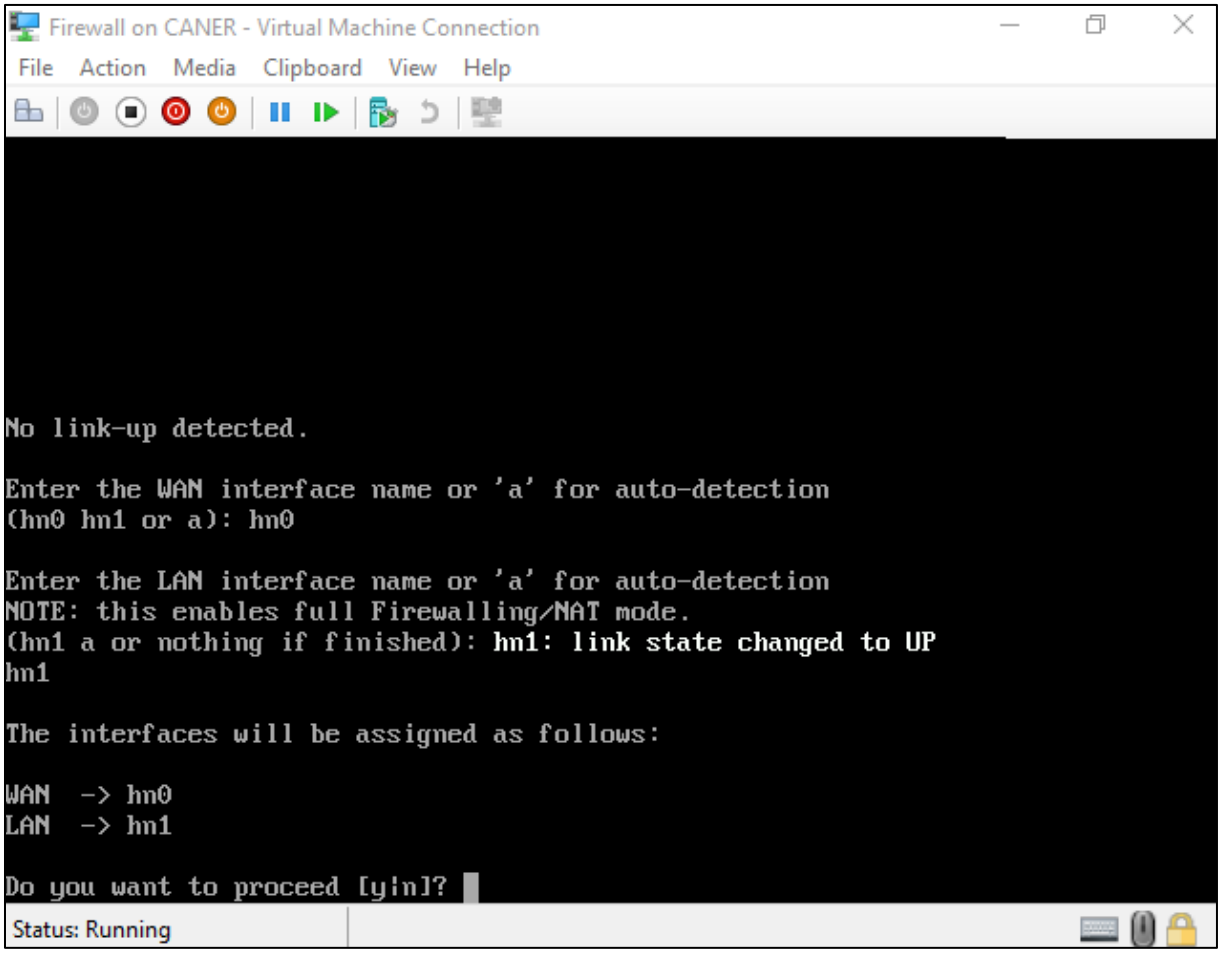
It starts to initialize.



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.

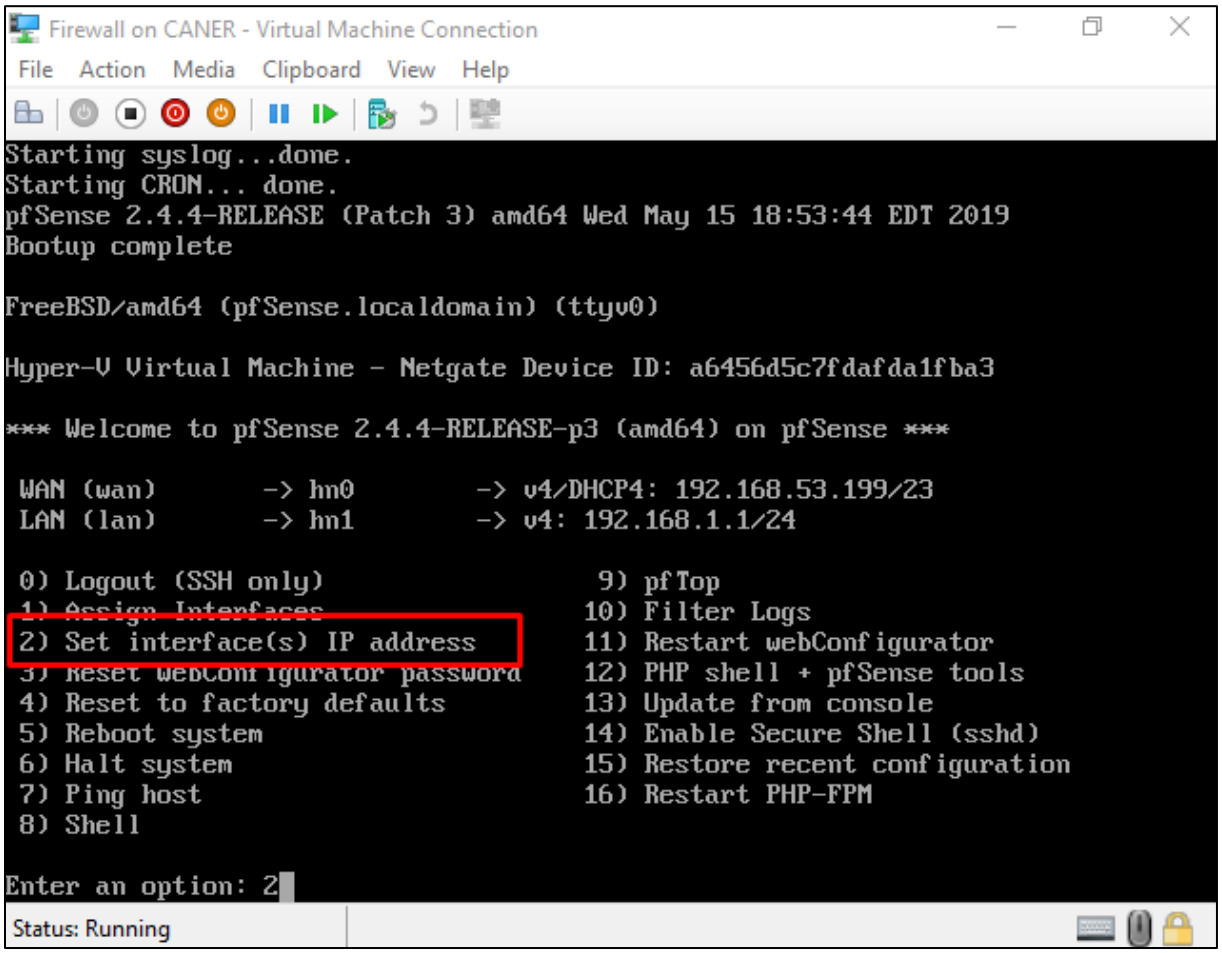
It asks whether we want to set up VLANs and we refuse.

We assign the interfaces for WAN and LAN.

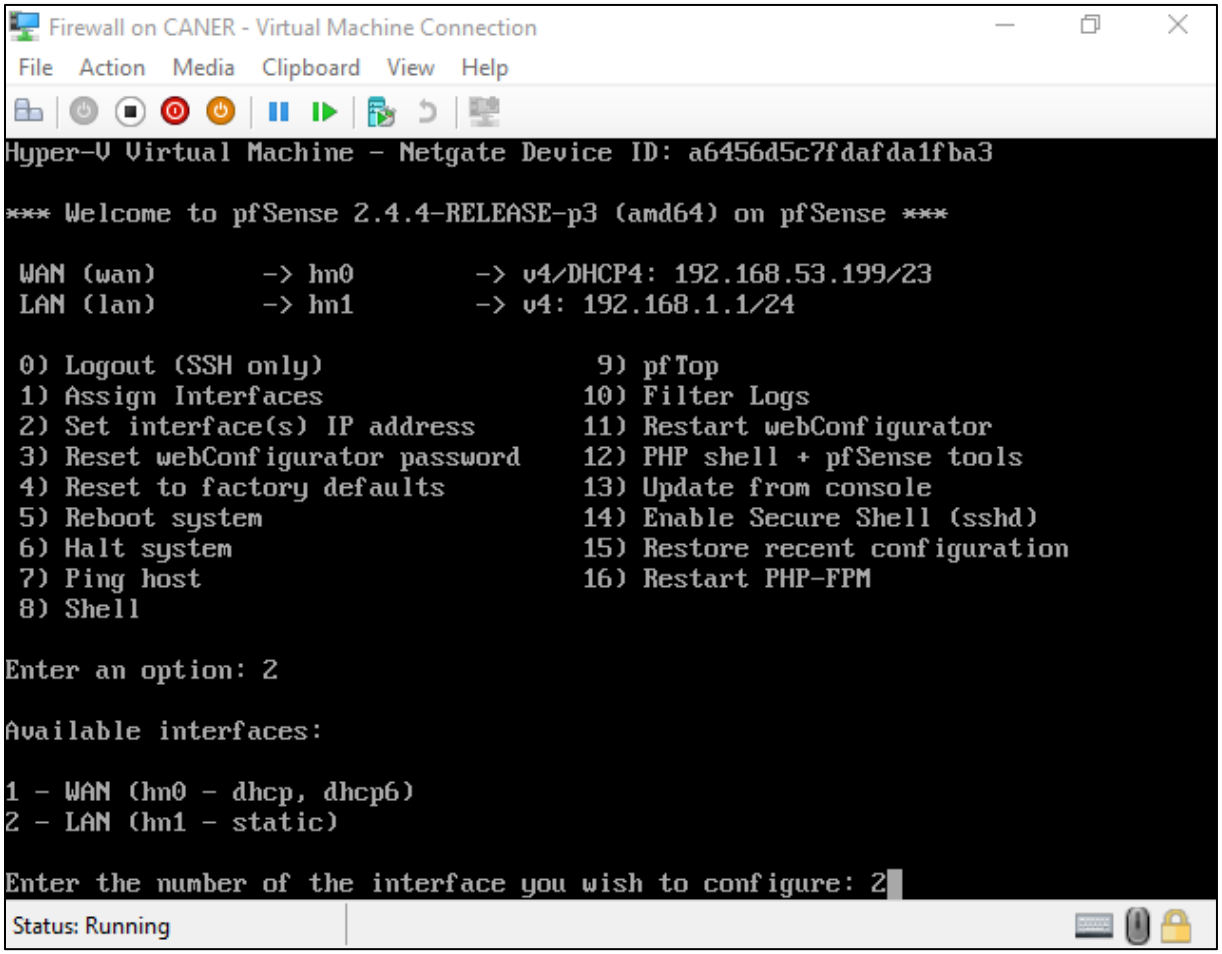


We proceed.

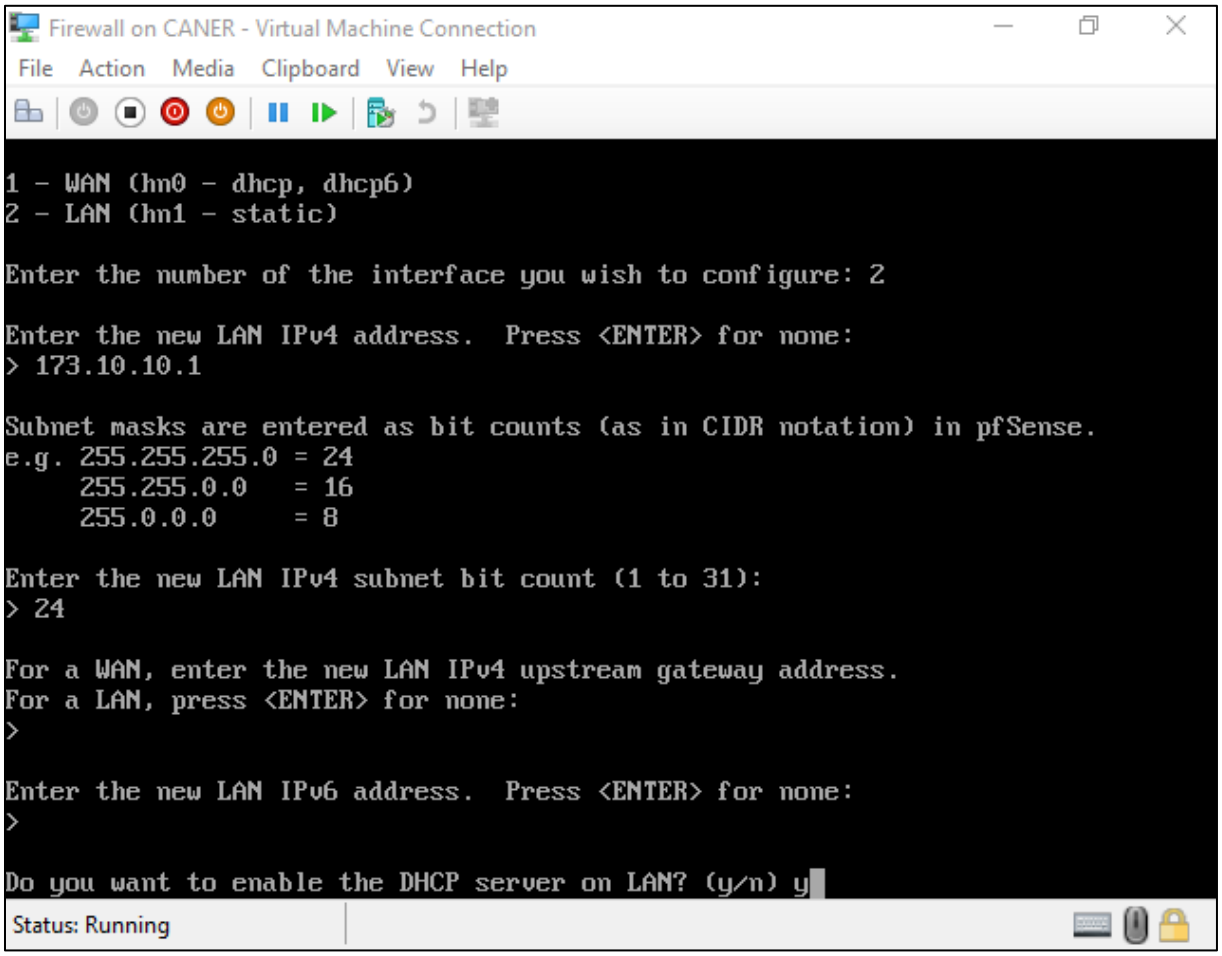
In this example our WAN IP is the IP that BAU's internal network distributes via DHCP. We use them to get to the internet. The LAN IP is ours to create. To do so, in the menu that pfSense presents we select 2 to set an interface's IP address.



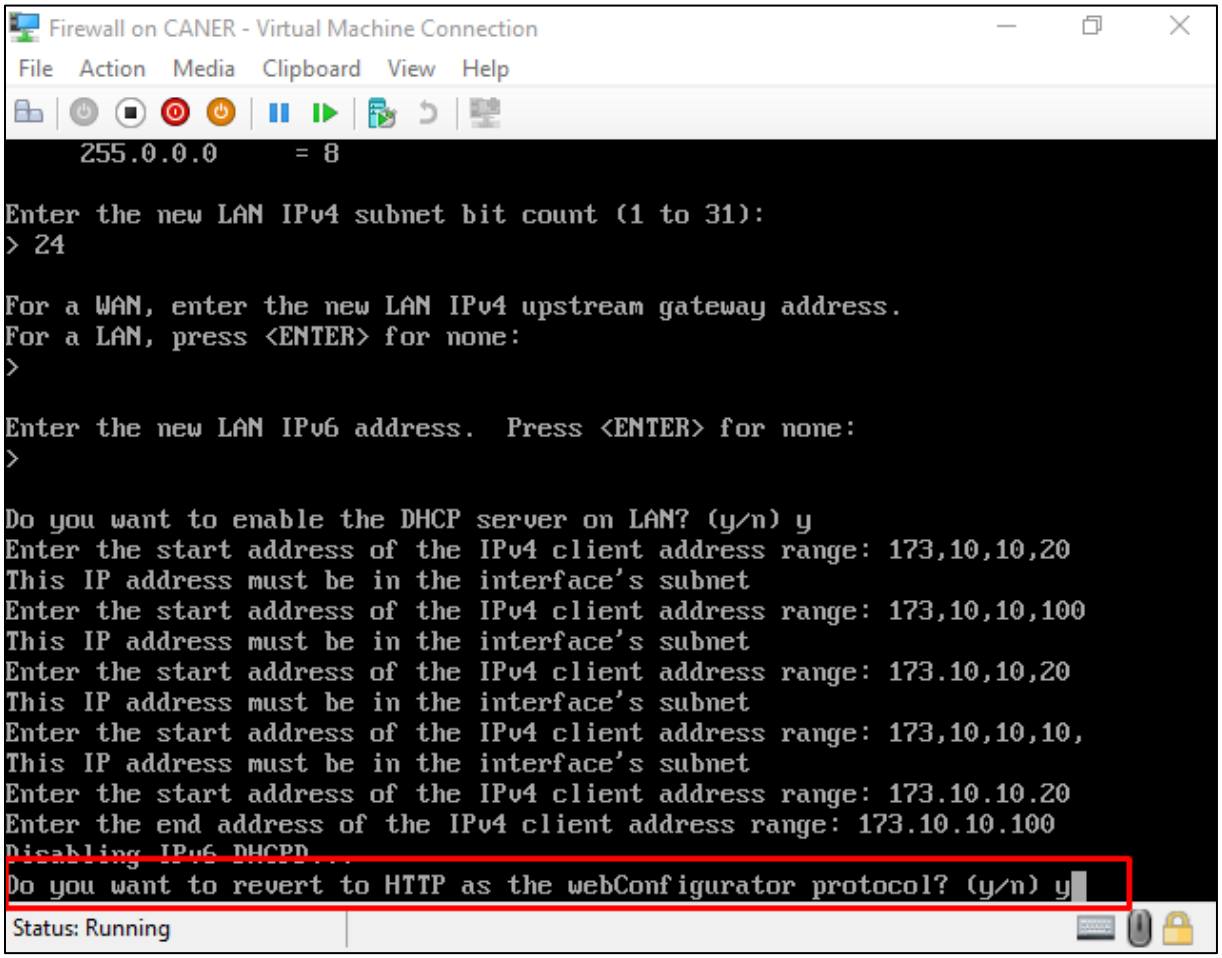
And select that we want to change the IP address of the LAN interface.



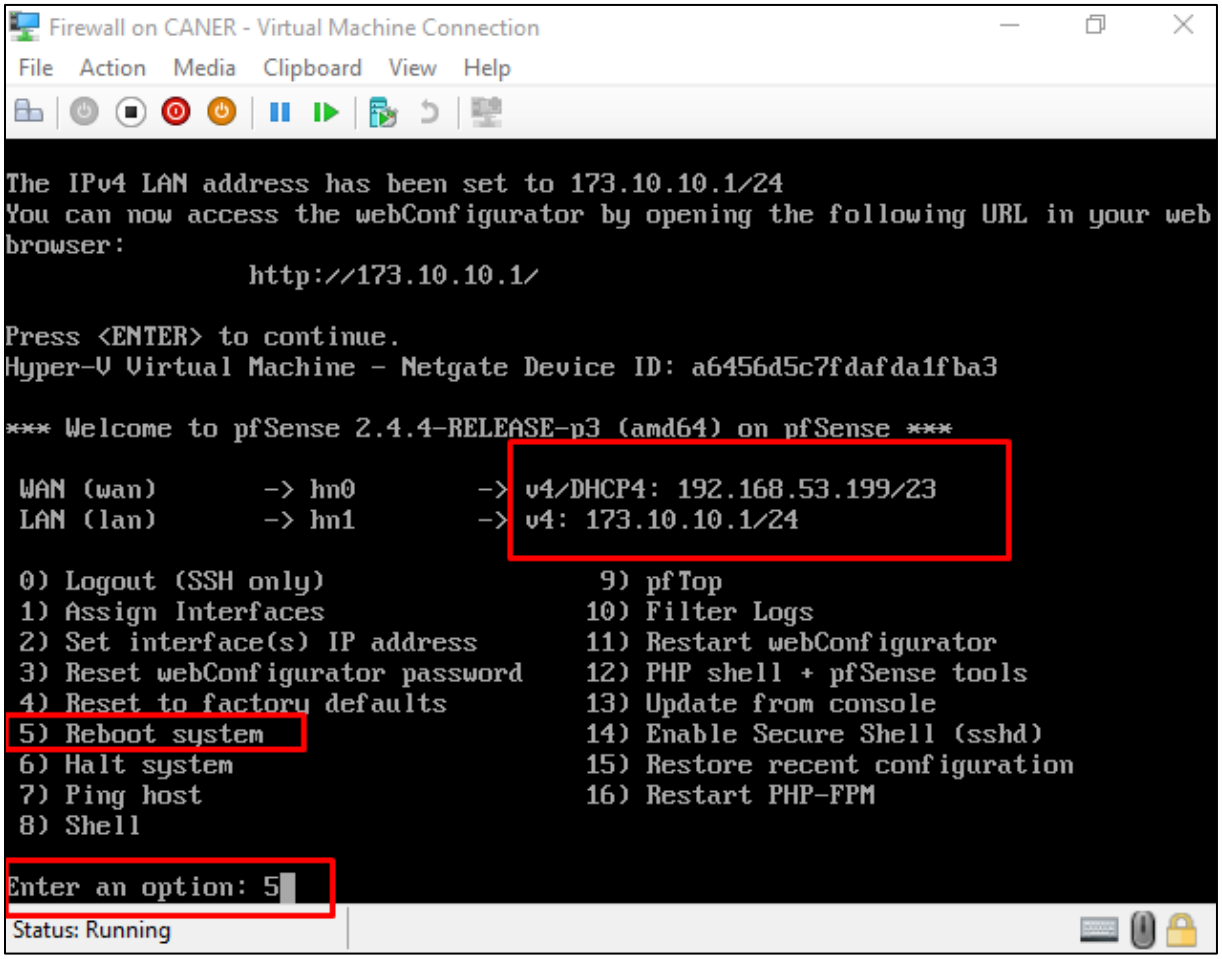
We give it an IP address and subnet mask. Since it's a LAN we don't have to give it an upstream gateway address. We don't have to assign an IPv6 address. And lastly, we do enable DHCP in our internal NIC so that the enterprise hosts can get IP addresses from the firewall itself.



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

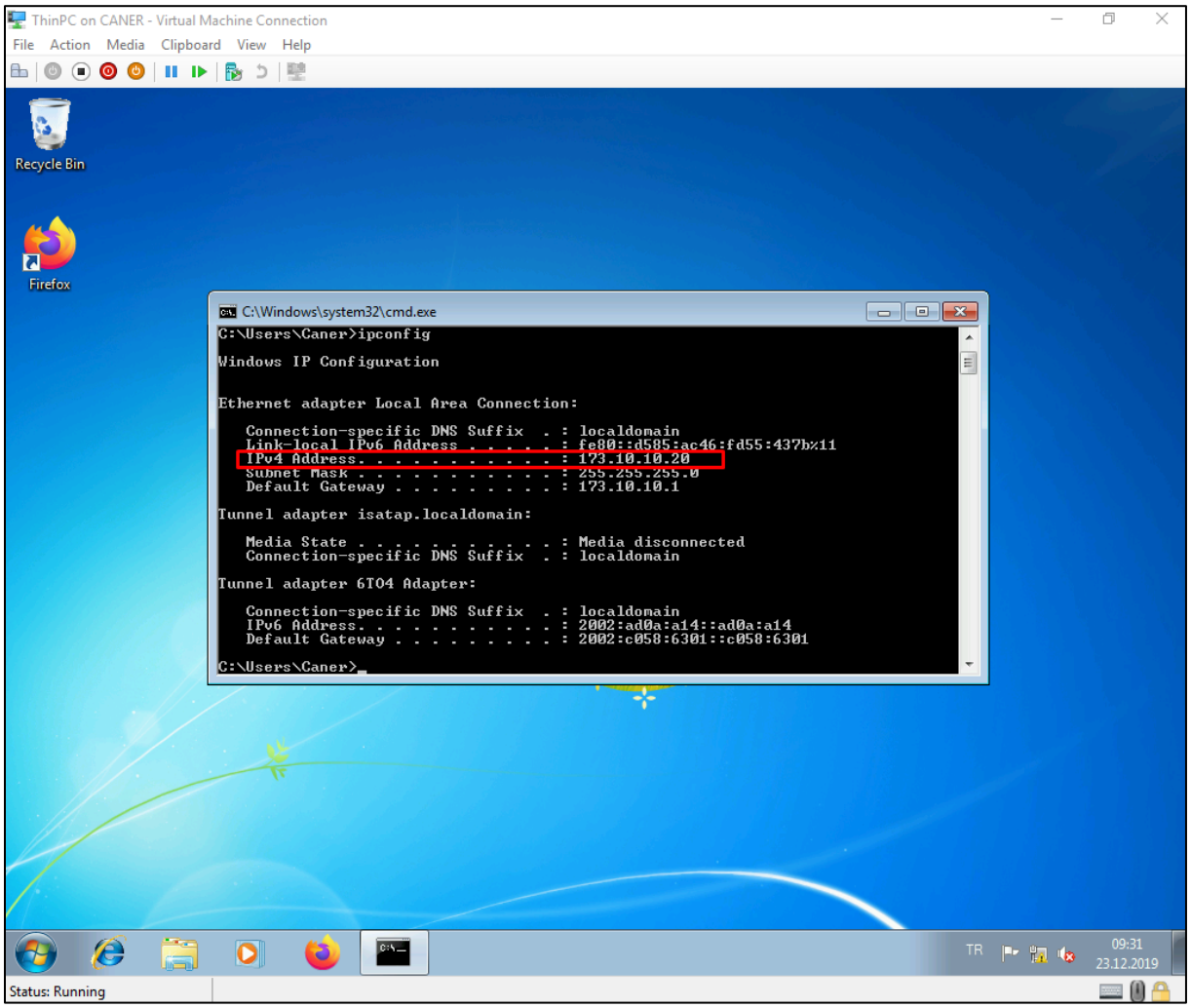


After the initial configuration is over, we must reboot it.

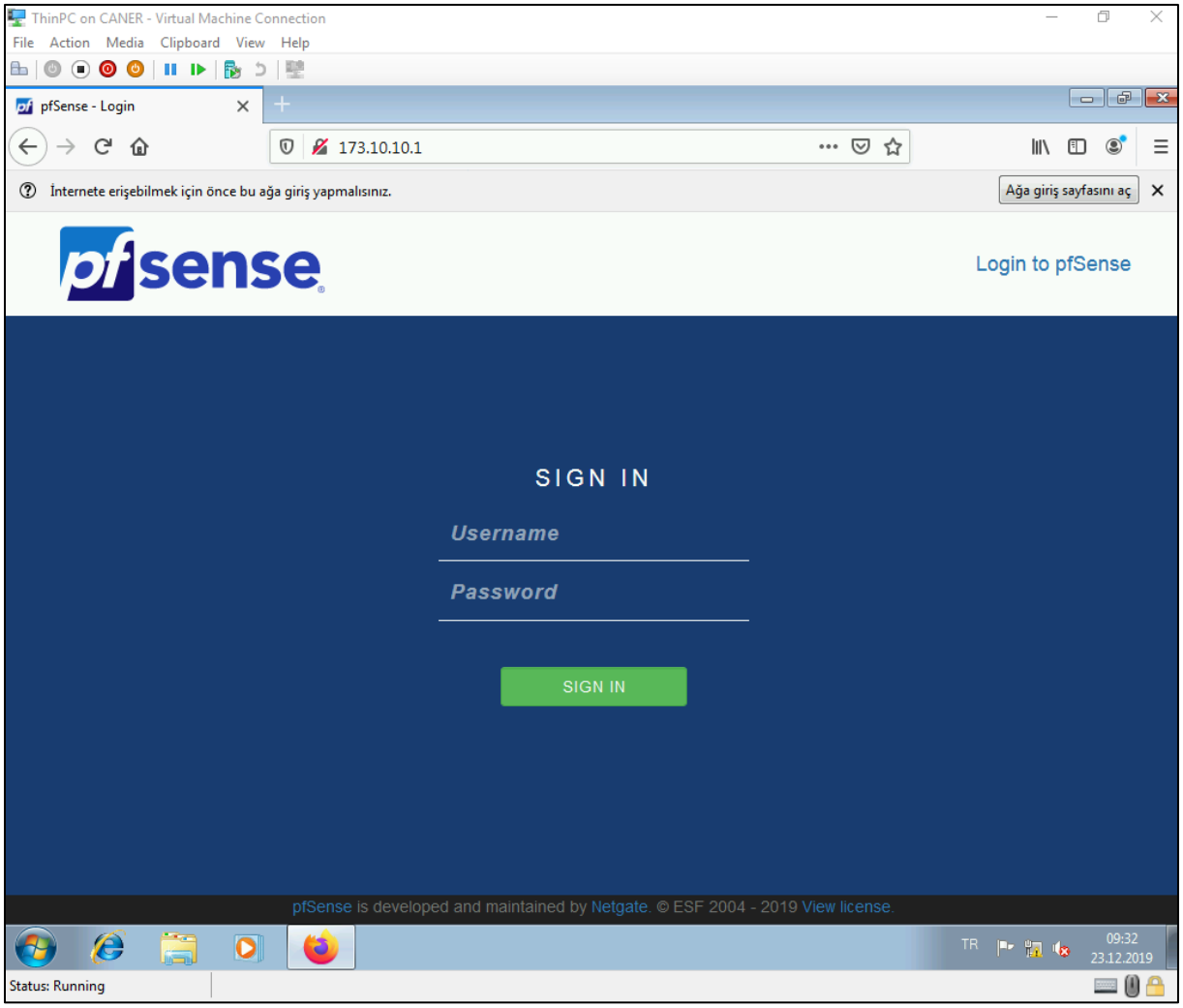


Note the LAN IP address, we will be using it to connect to it via a web browser and further configure security settings.

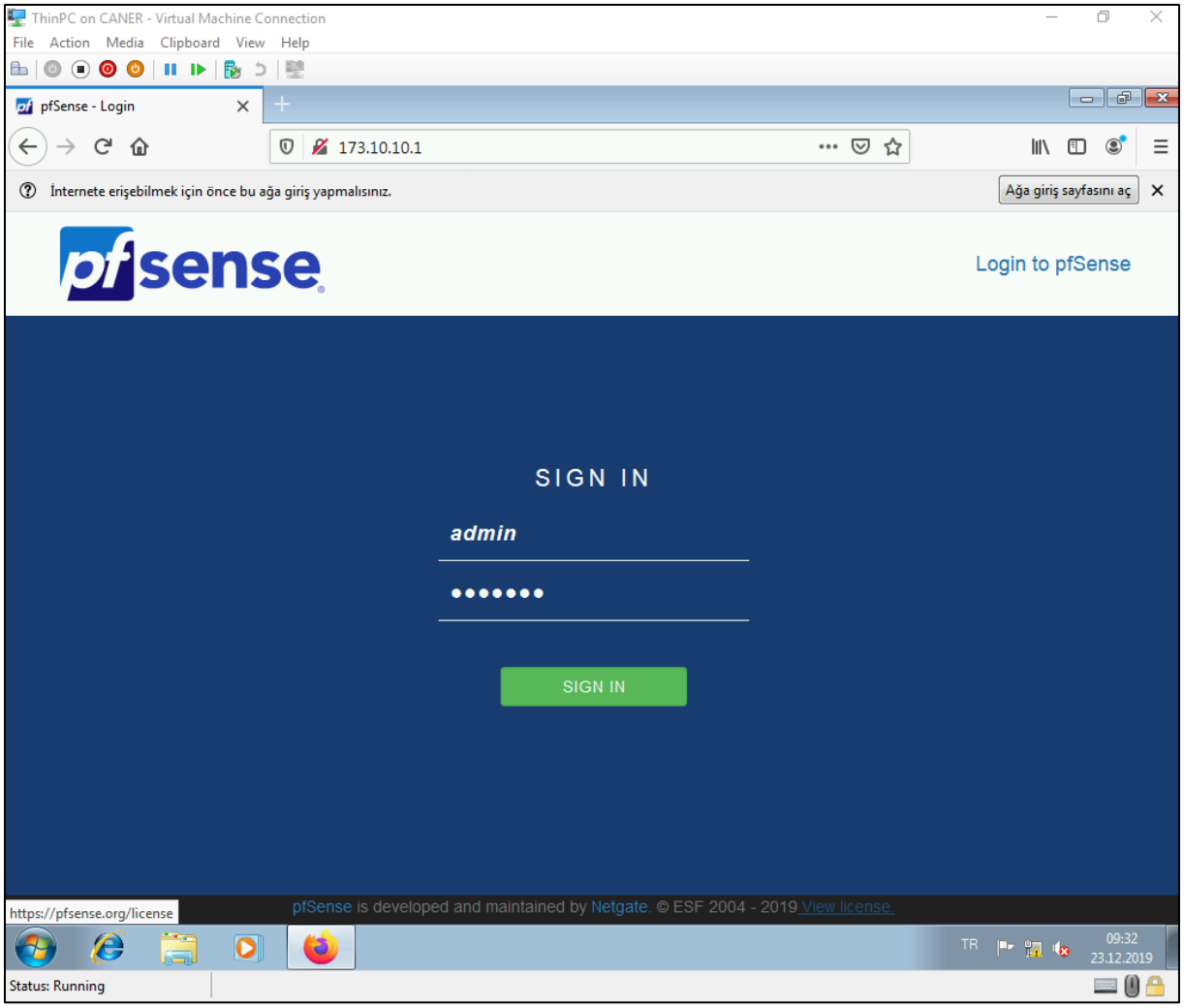
Next, we create another virtual machine, we used ThinPC image, but any client or even server system would work. This machine has only one NIC and it is set to internal setting. It receives its IP address from the DHCP of pfSense.



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

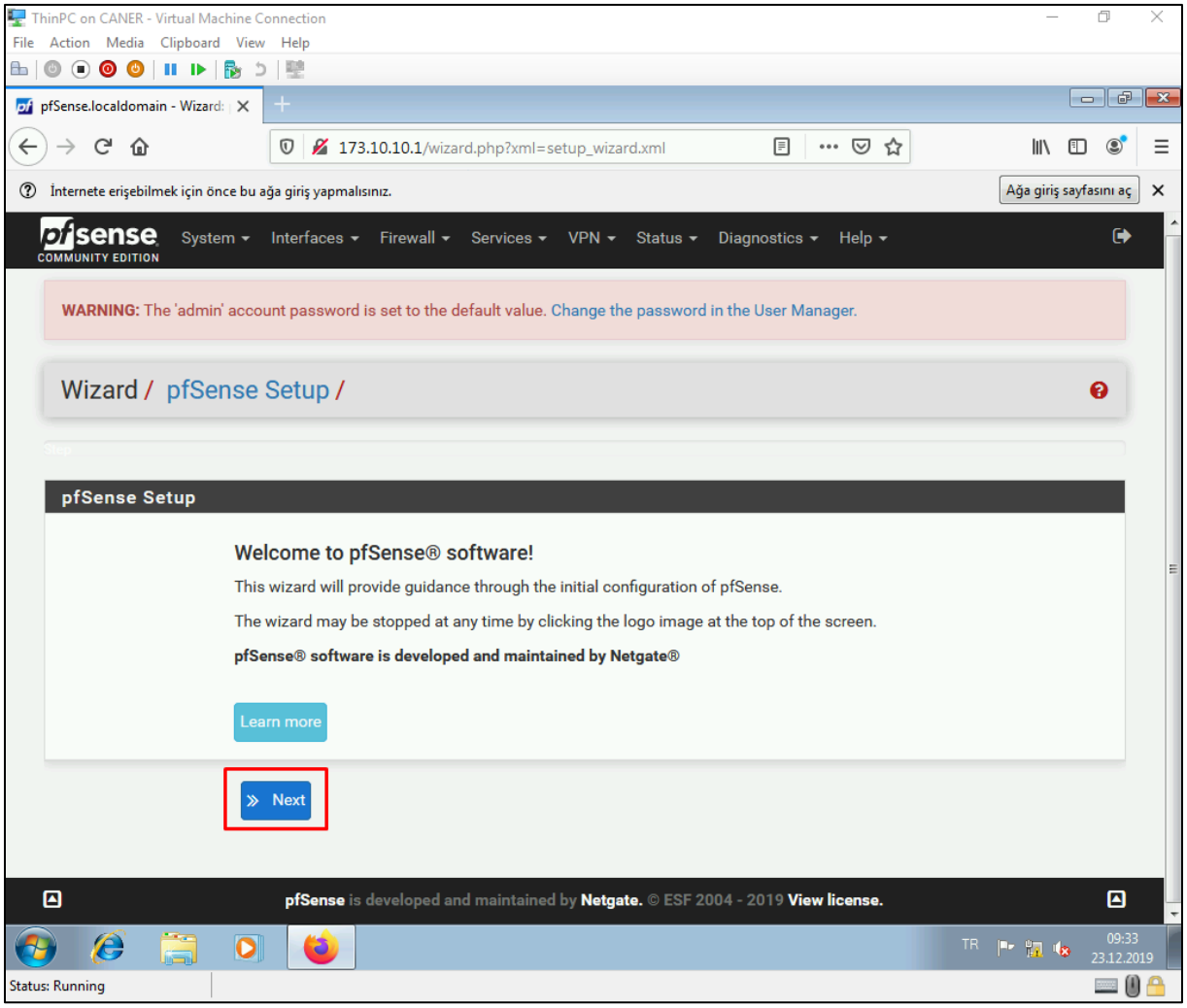


We haven’t set up any users yet but admin user with the password pfSense works.

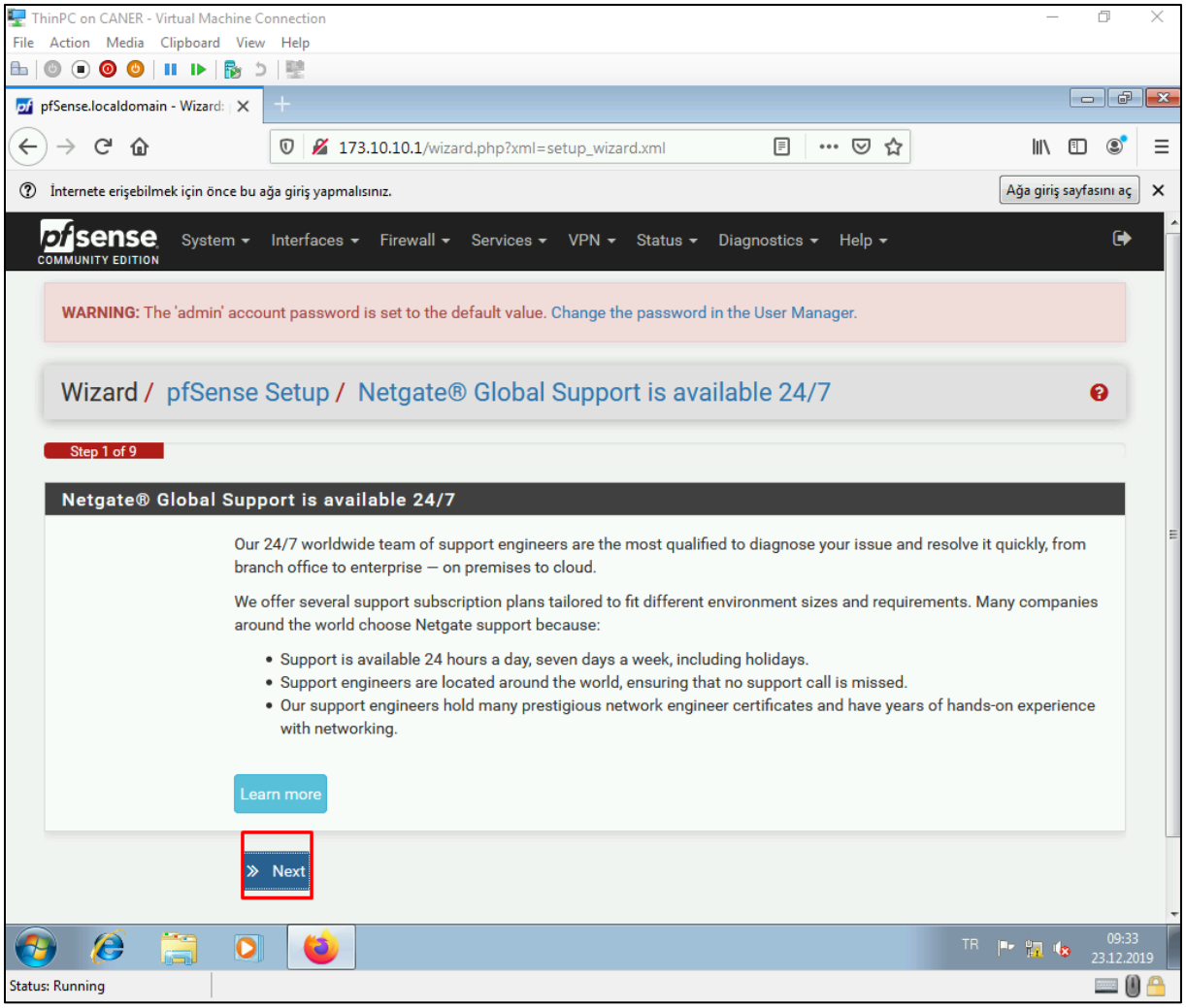


It will require us to change this password later during the configuration.

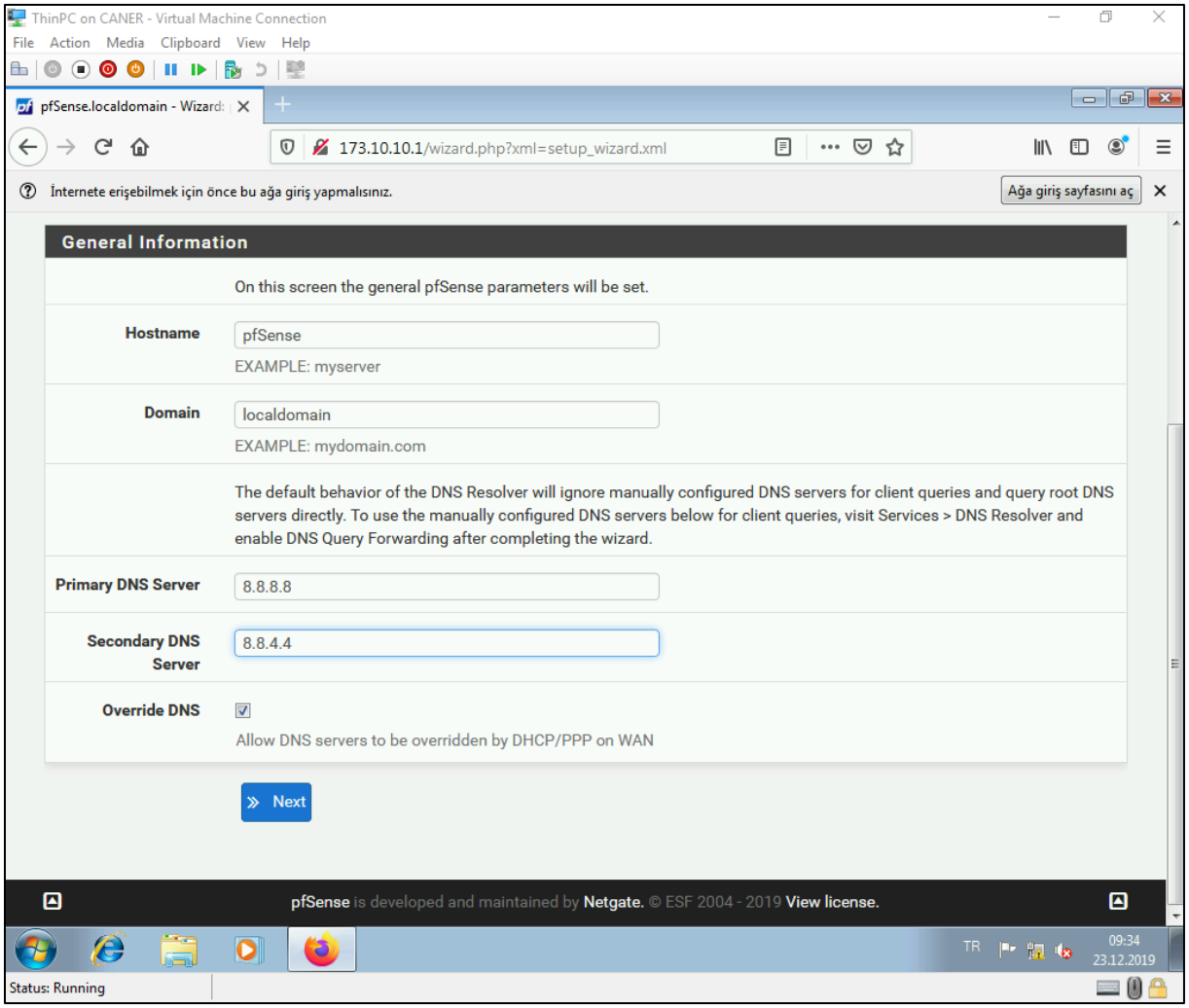
A setup wizard pops up and we simply need to follow its steps.



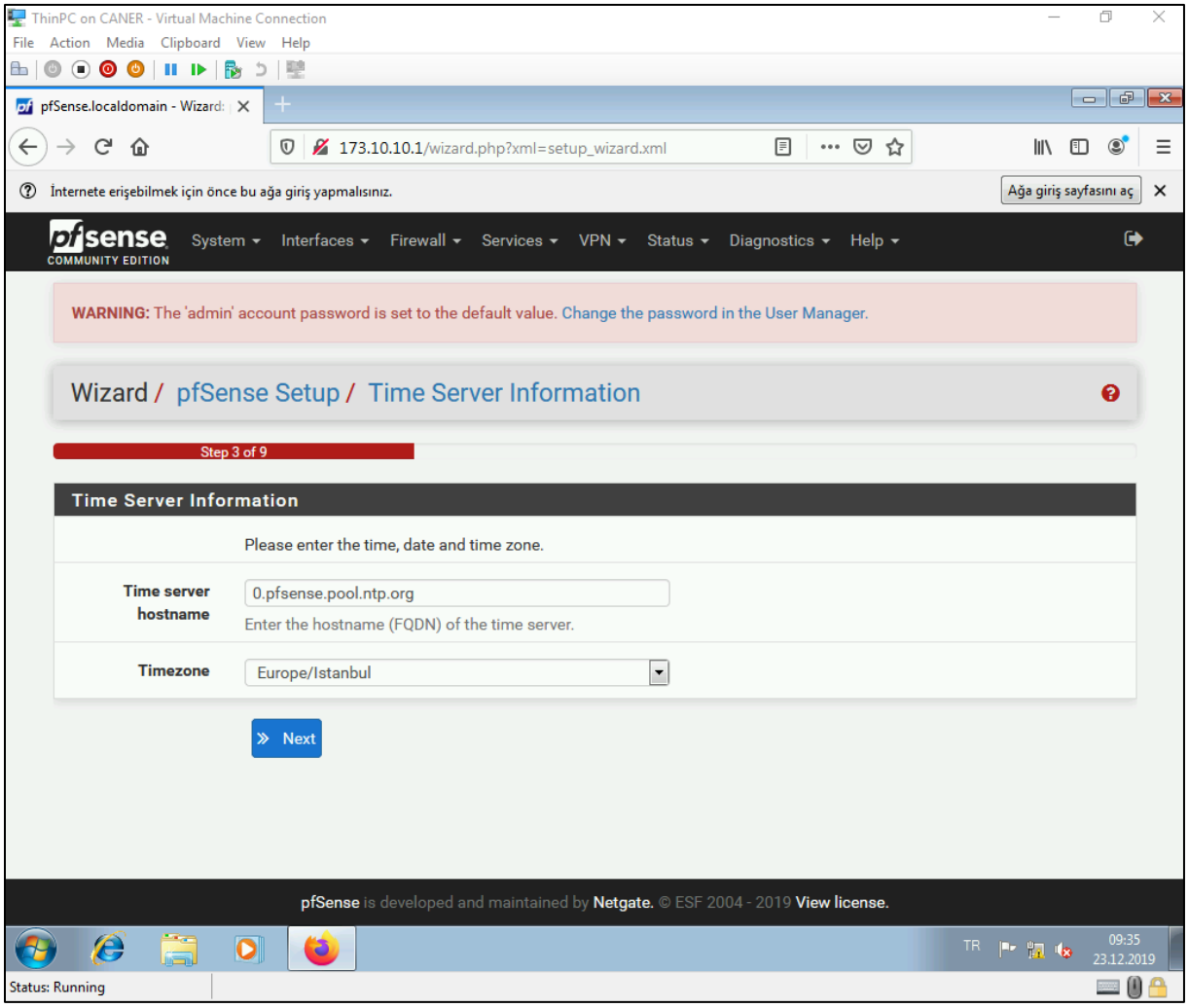
We proceed.


ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
pfSense.localdomain - Wizard:
173.10.10.1/wizard.php?xml=setup_wizard.xml
İnternete erişebilmek için önce bu ağa giriş yapmalısınız.
Ağa giriş sayfasını aç
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Netgate® Global Support is available 24/7
Step 1 of 9
Netgate® Global Support is available 24/7
Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.
We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:
Support is available 24 hours a day, seven days a week, including holidays.
Support engineers are located around the world, ensuring that no support call is missed.
Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.
Learn more
Next
TR
09:33
23.12.2019
Status: Running

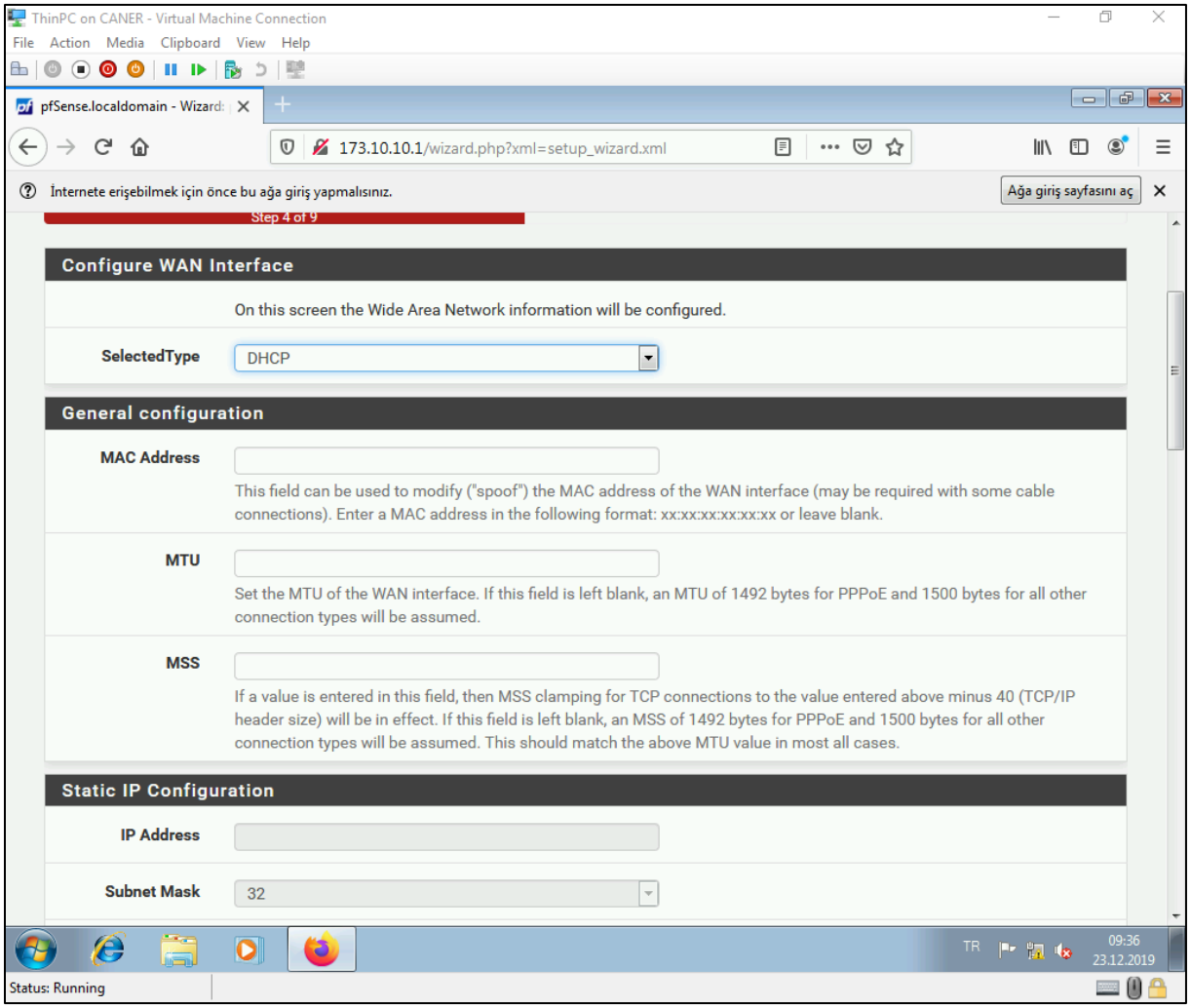
We name the local domain and select DNS servers. In this case, we used Google's DNS.



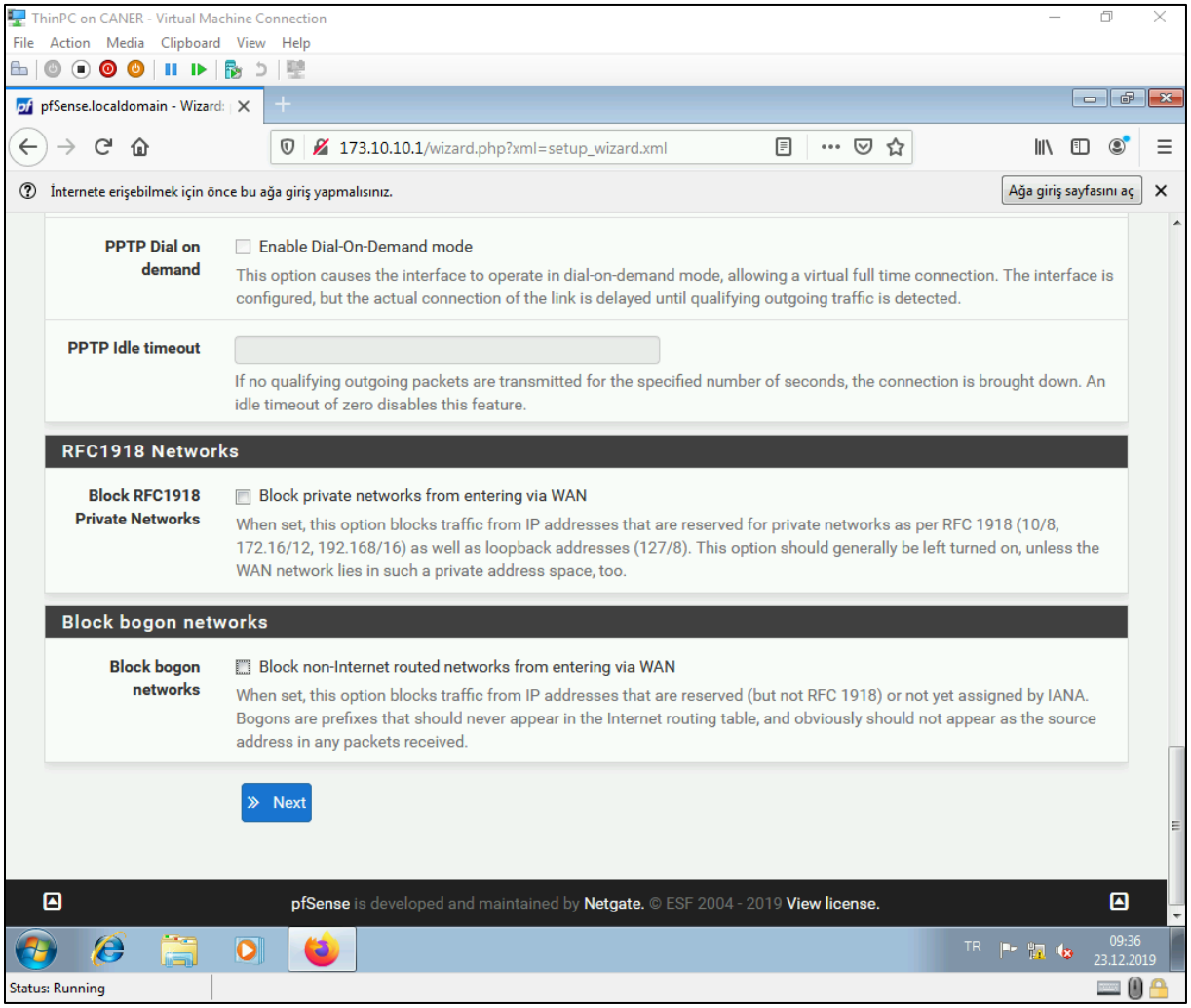
We choose the time zone as Istanbul.



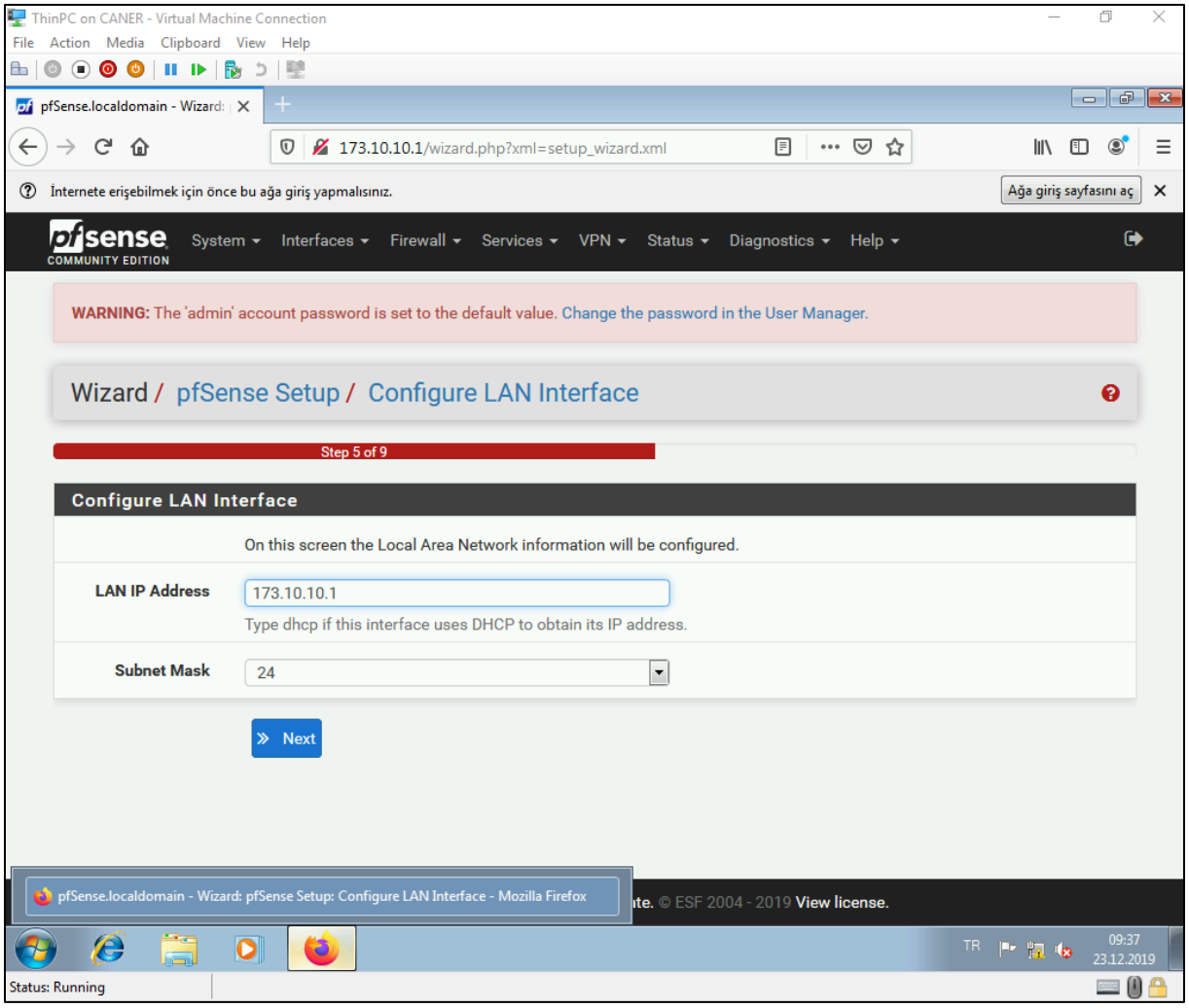
The WAN interface remains at DHCP since we need BAU's network to reach the internet.



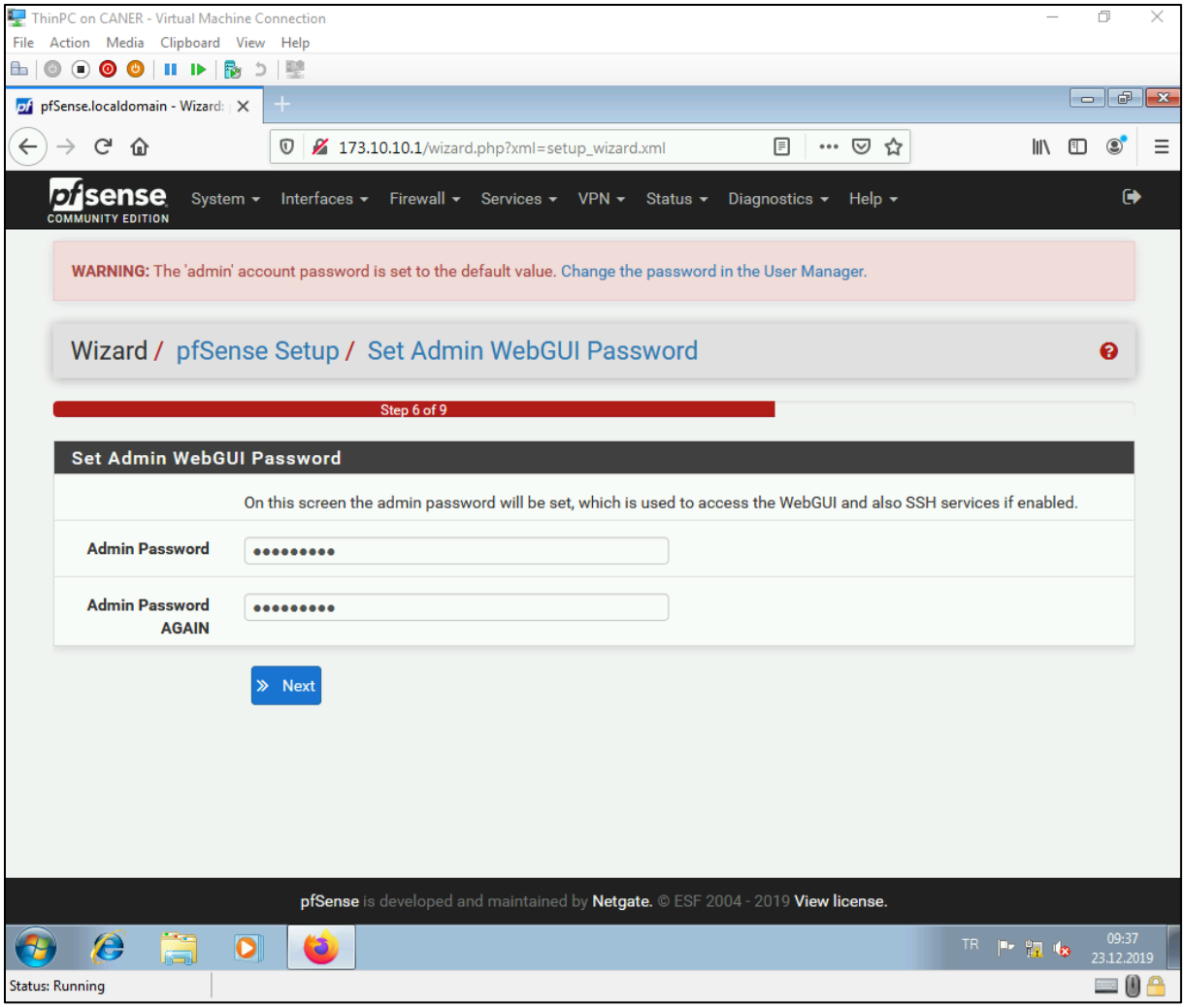
And we don’t change any other setting from there.



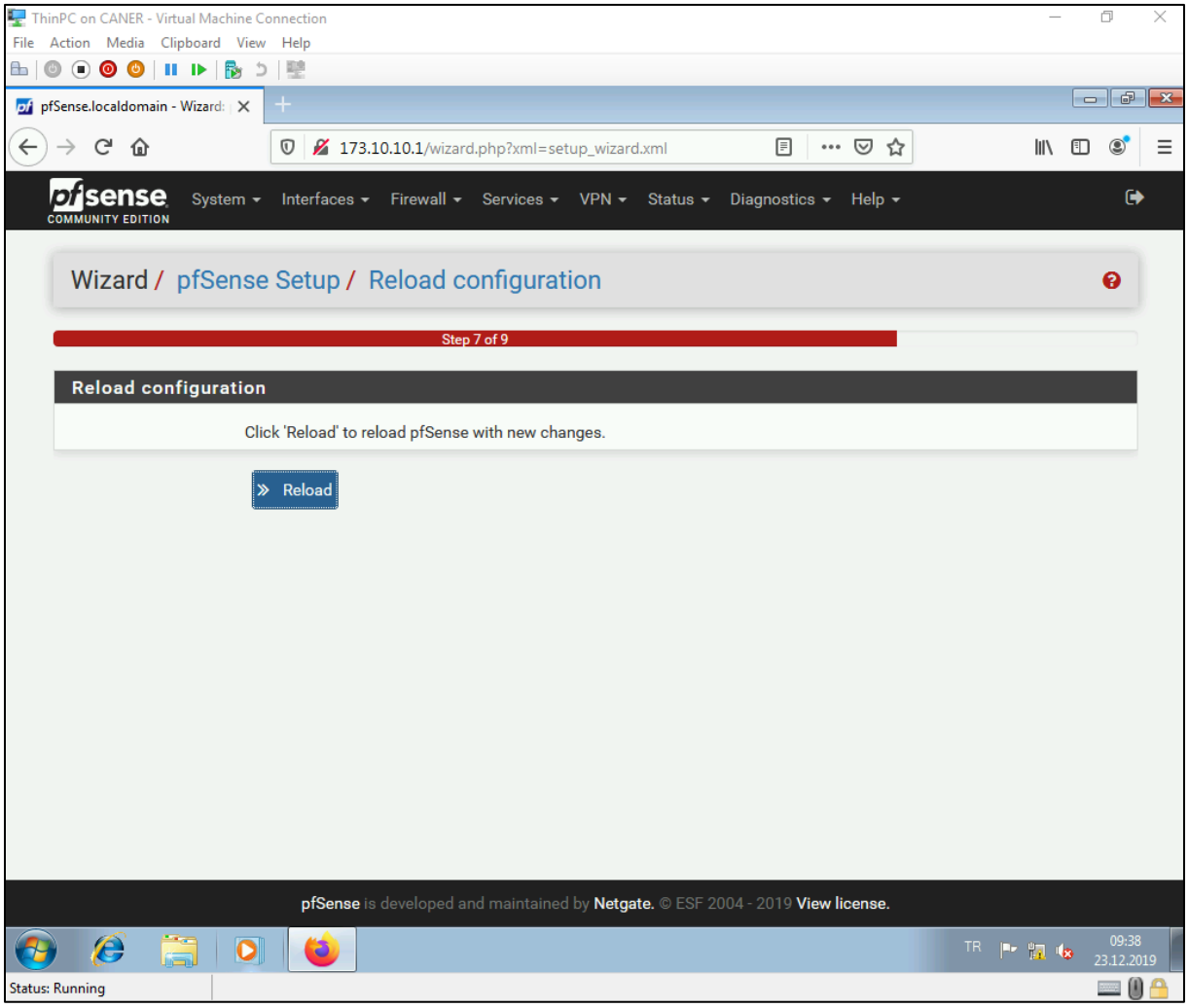
On the next step, we confirm our setup of the LAN interface. Again we change nothing.



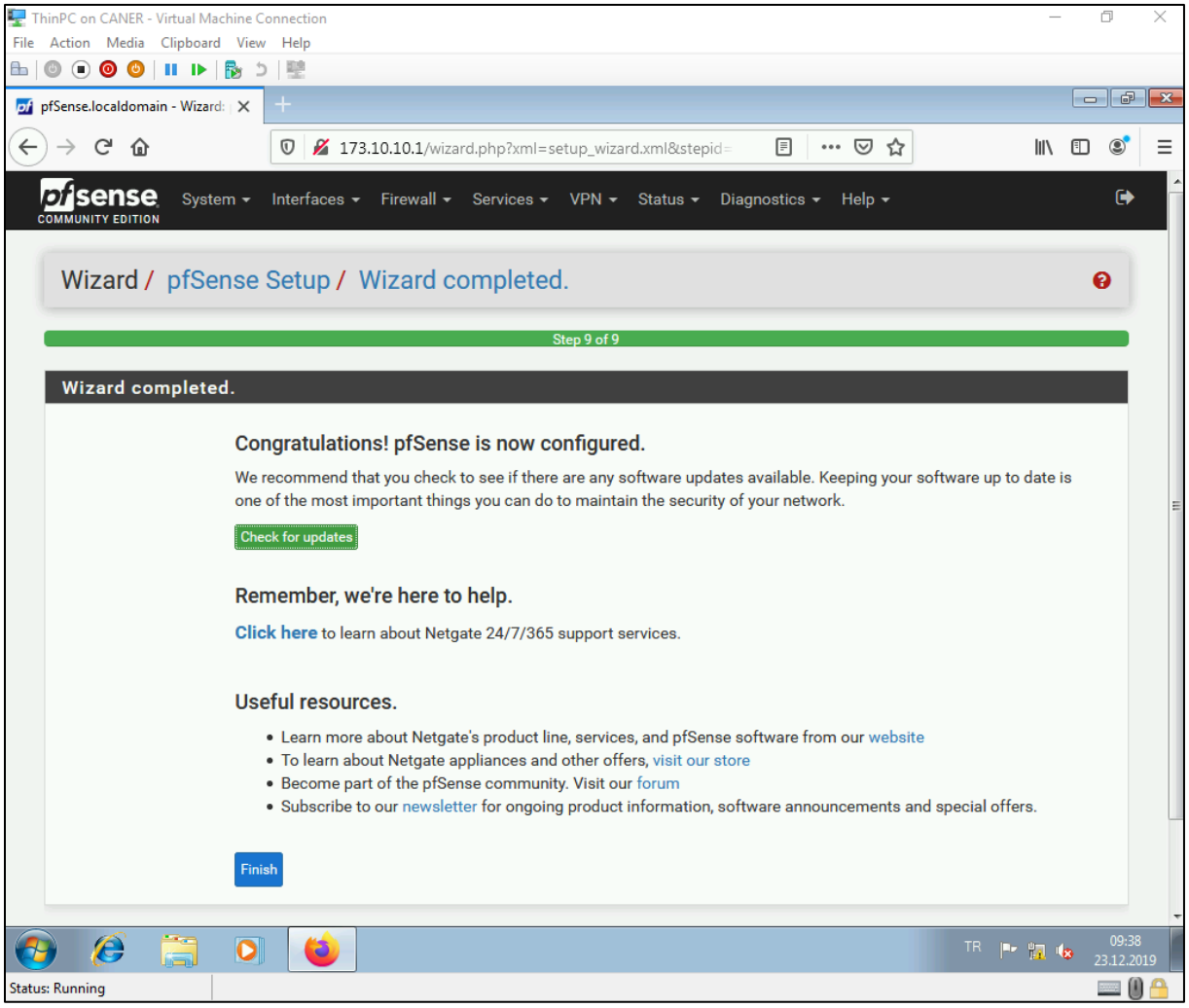
Then, it asks for a new admin password.



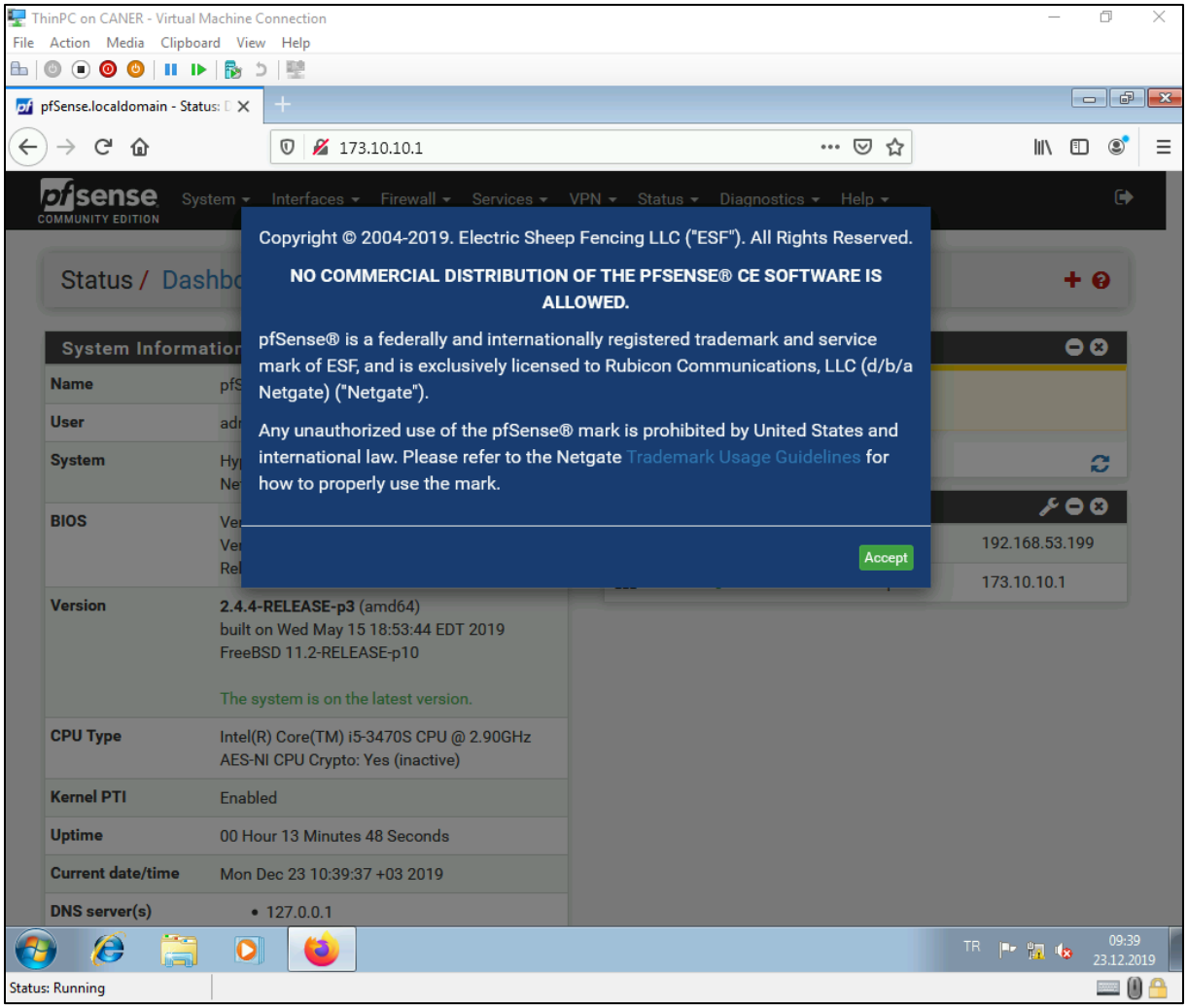
We now need to reload the configuration to save it.



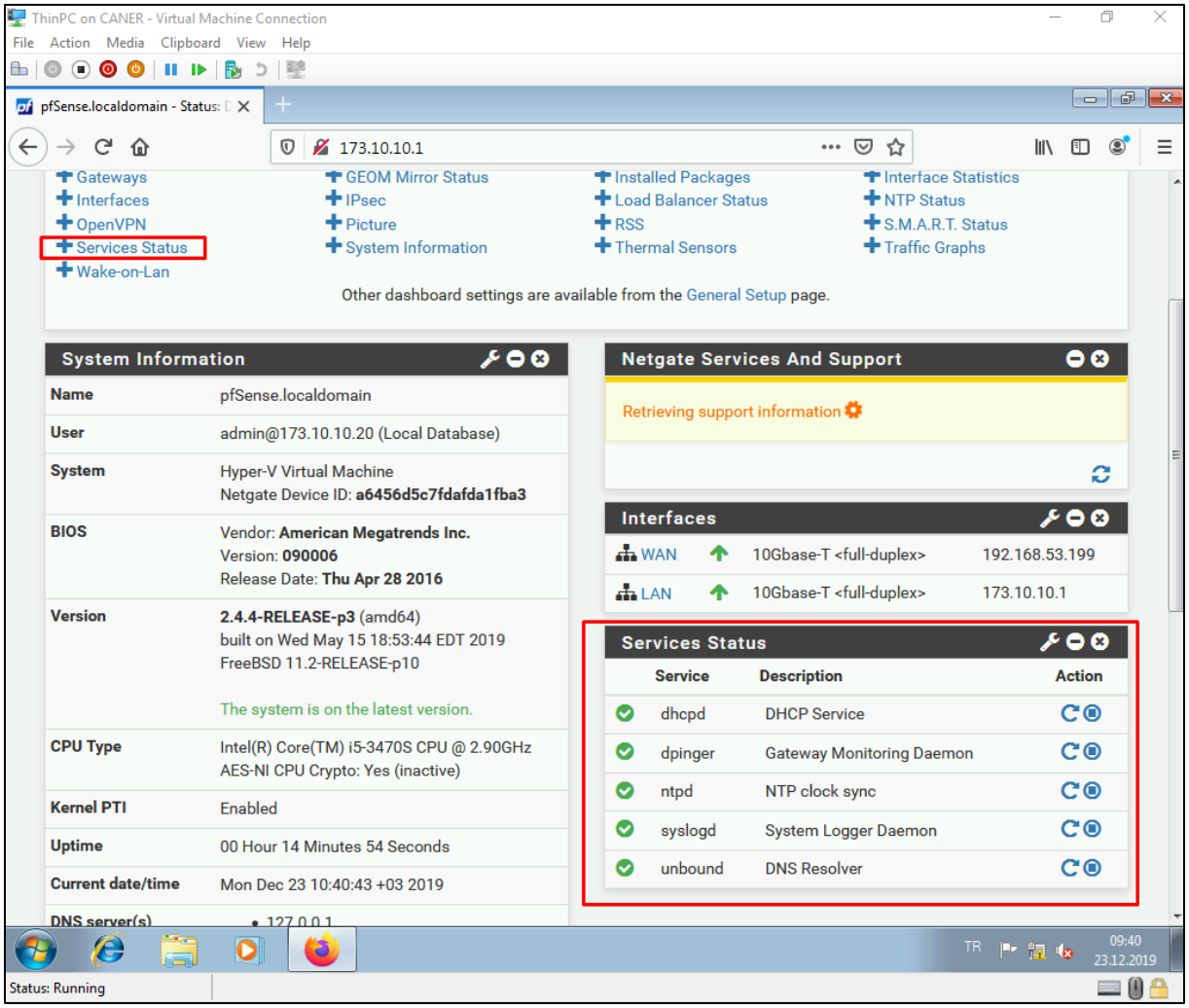
This completes the setup and wizard is done.



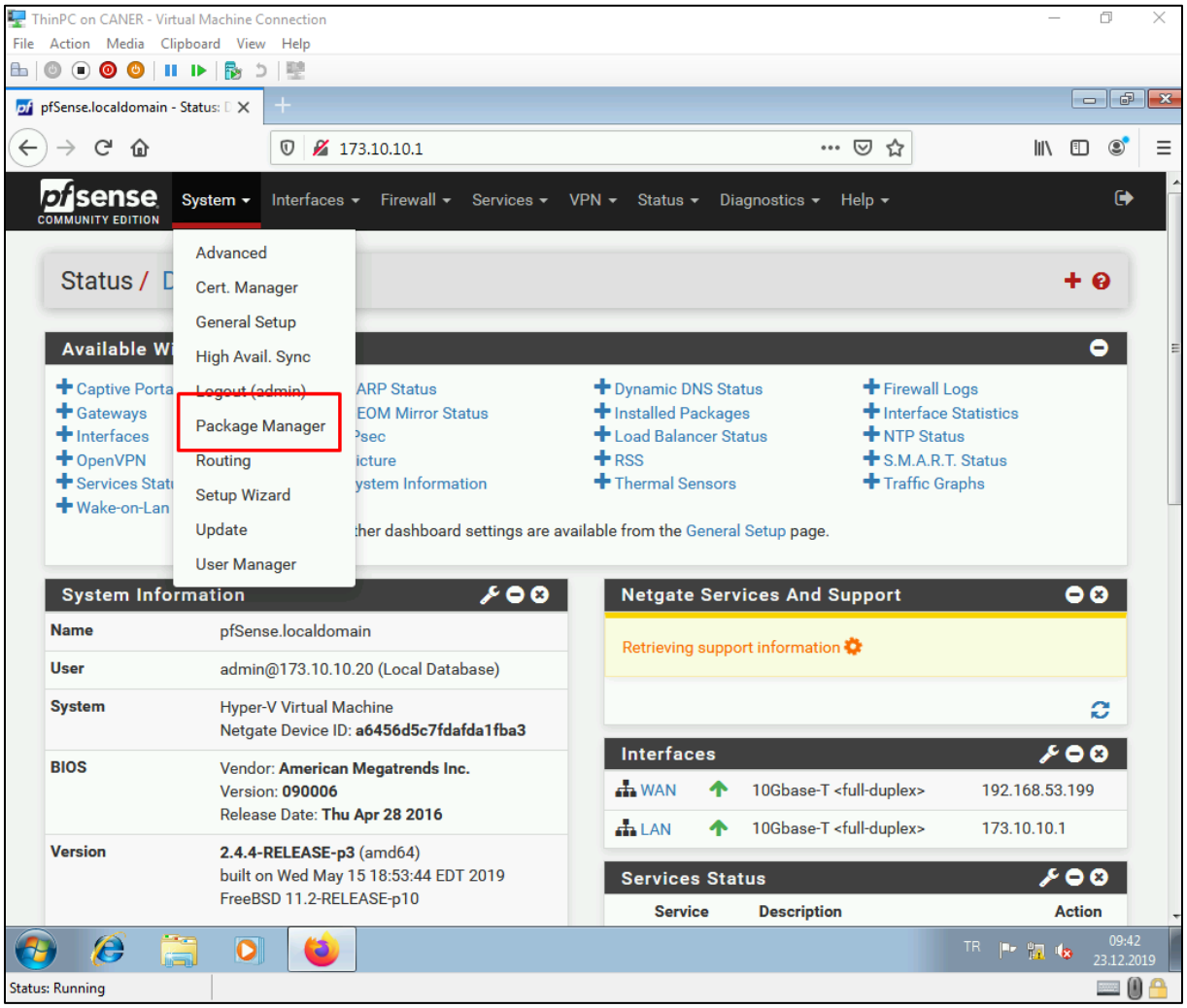
Then, we're sent to the Status Dashboard where this screen welcomes us.



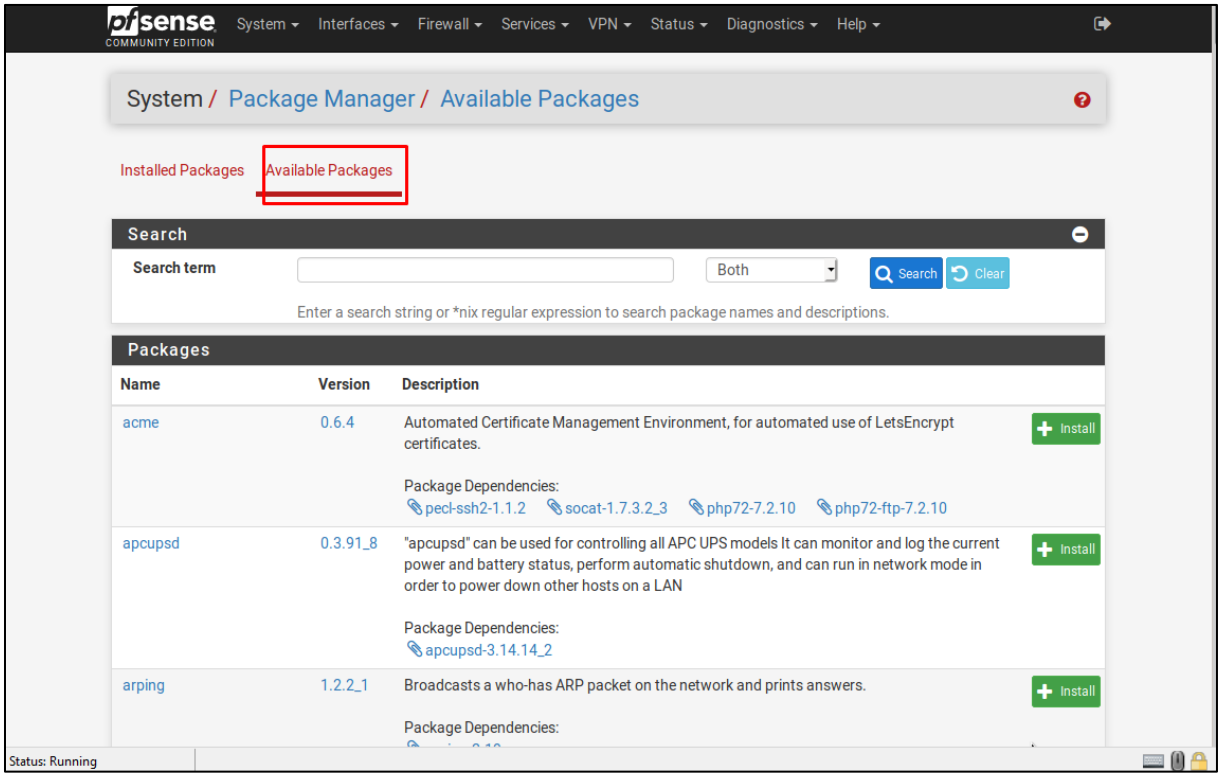
We add services status to the dashboard and look at the services that are currently running.



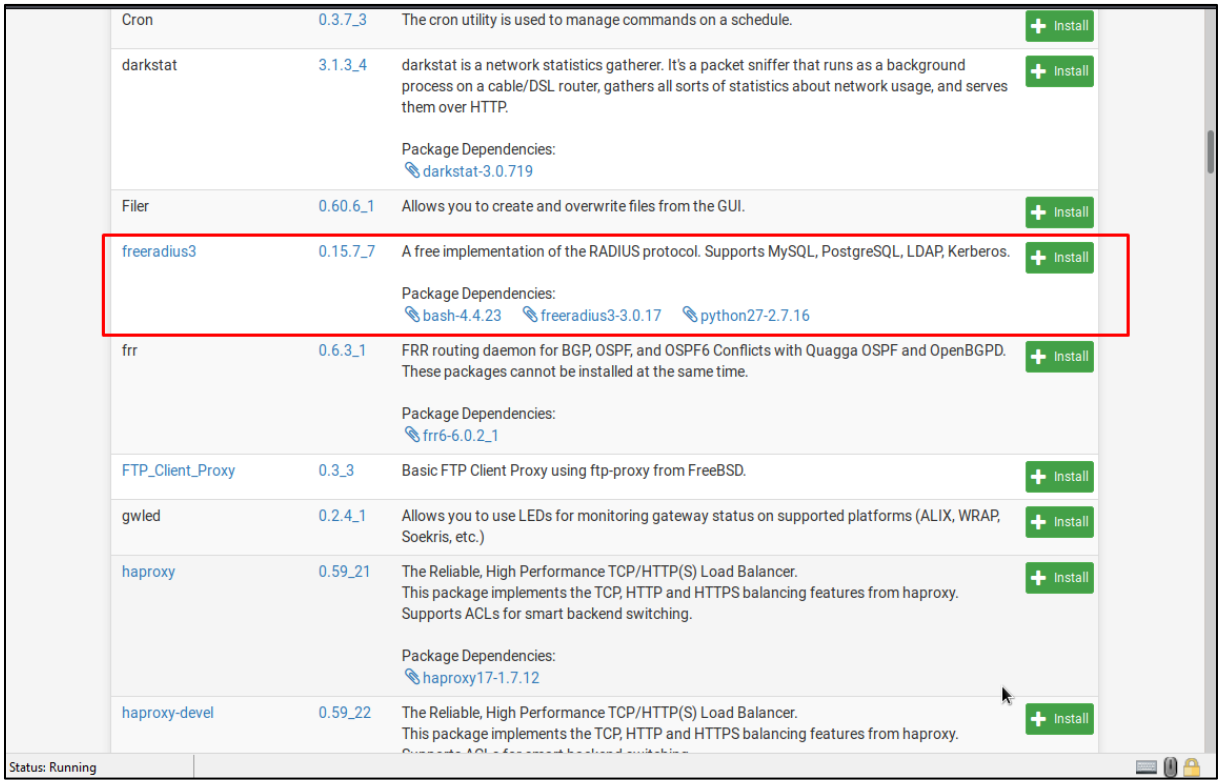
Now let’s start a Radius service so that our internal users must enter their credentials to connect to the internet. We don’t want anyone to get to the internet easily we want to track when they connect and how long they stay connected. Firstly, we need to get to the Package Manager.



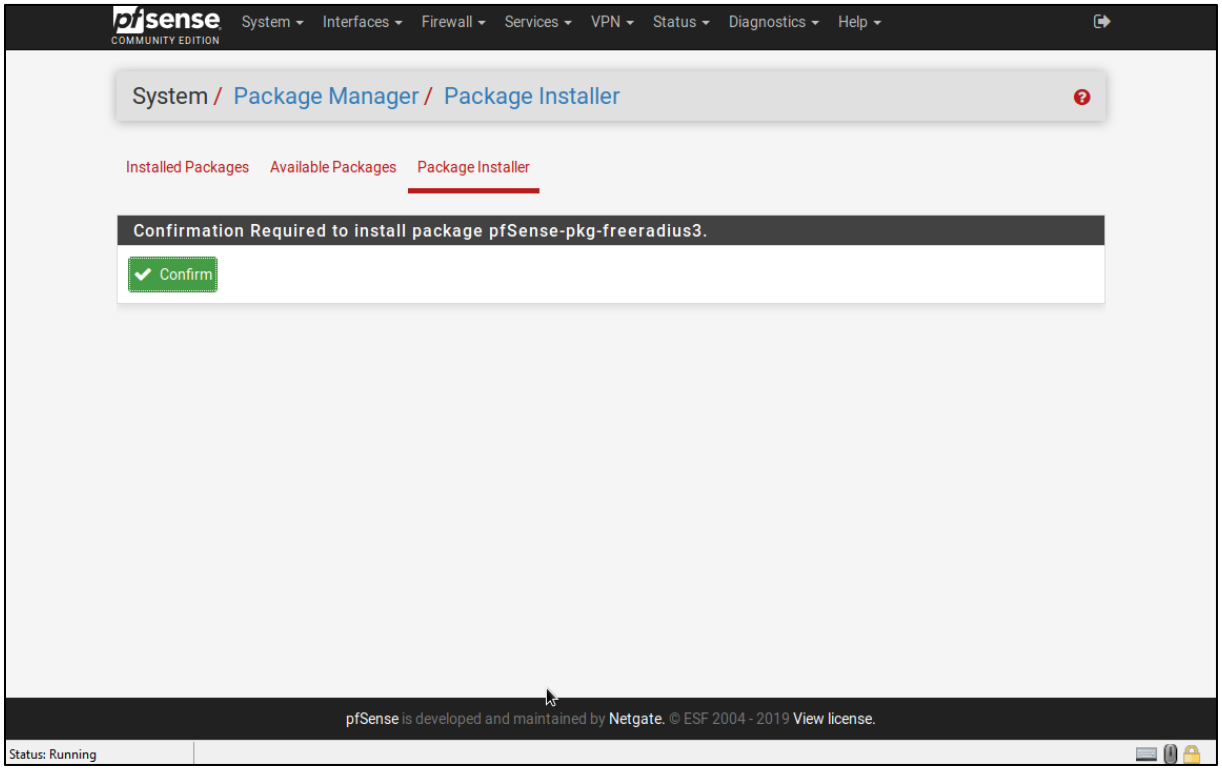
Under Available Packages…



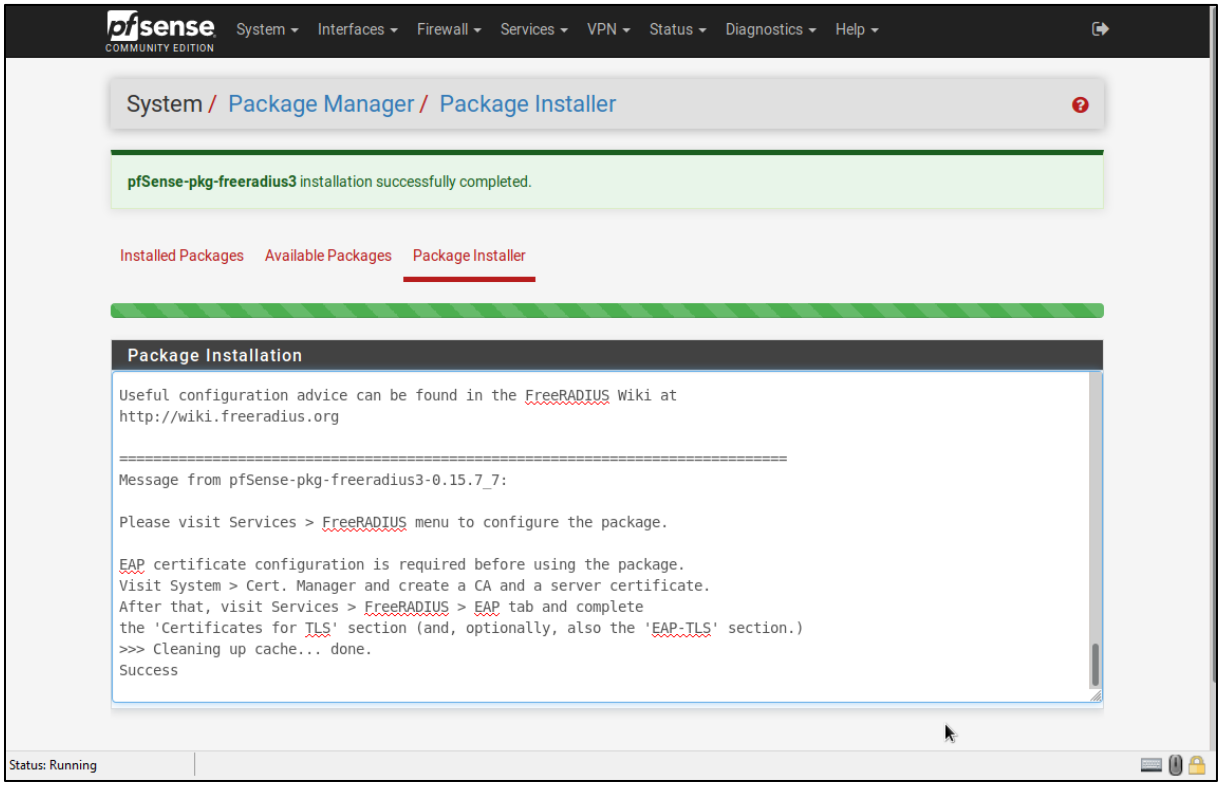
We install freeradius3.



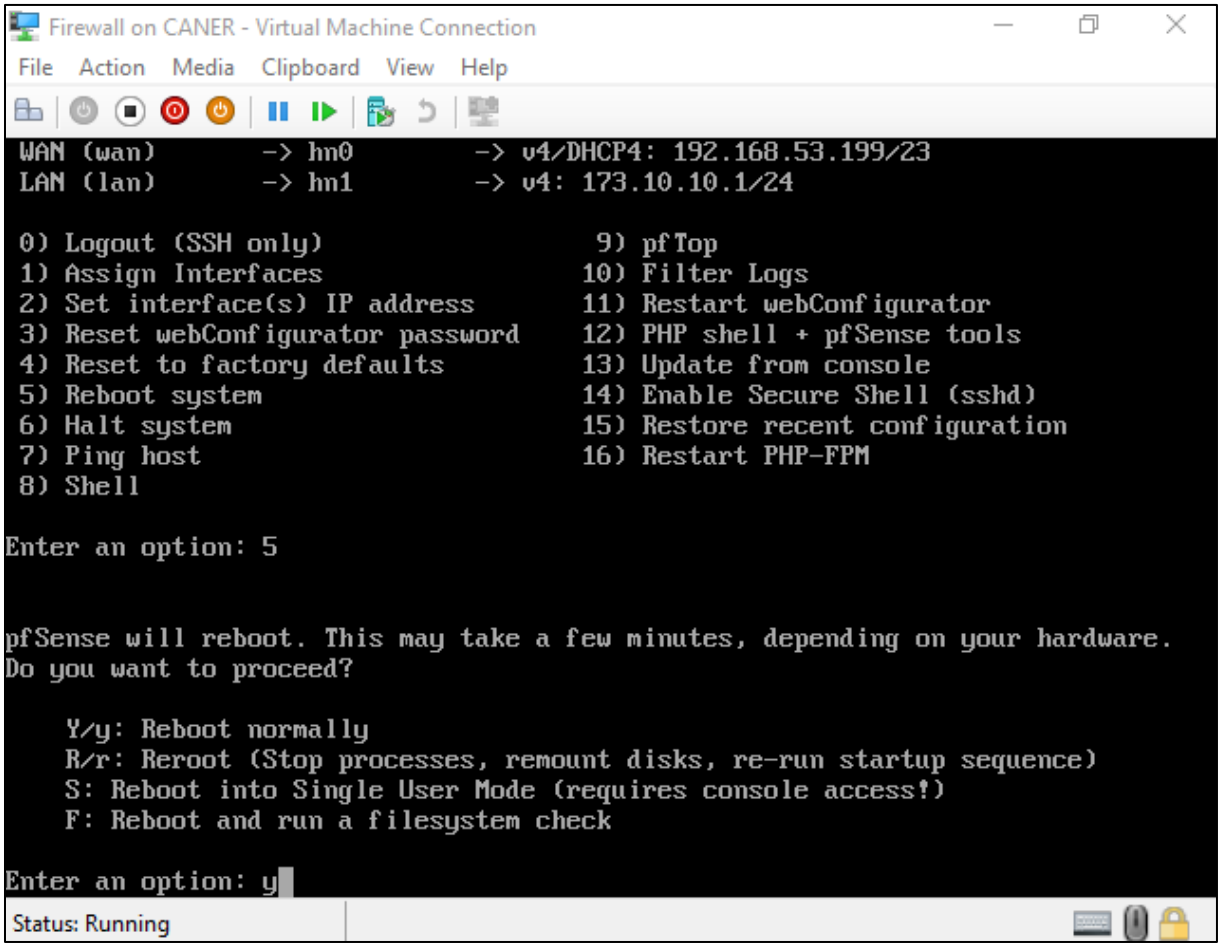
We confirm to install it.



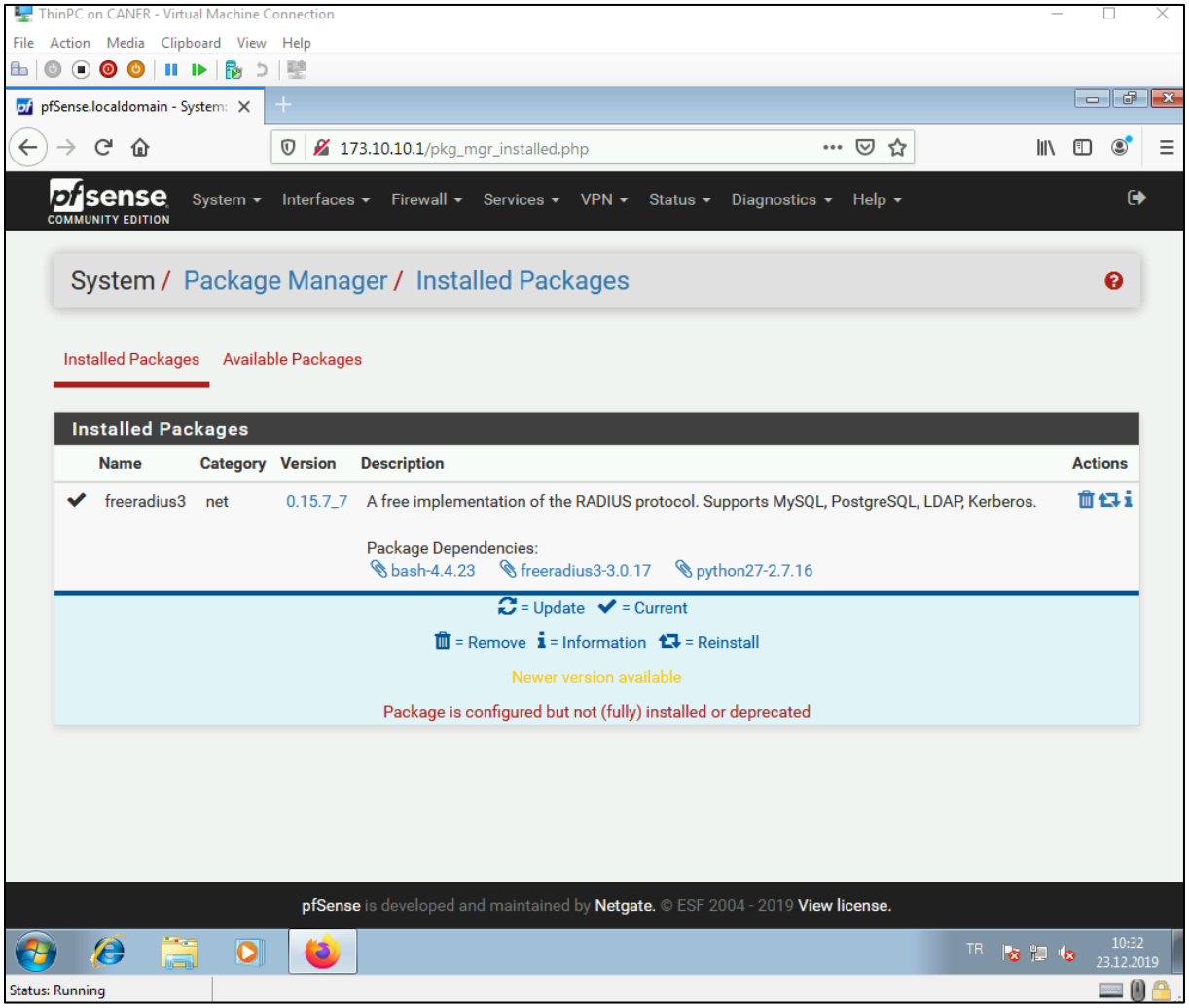
After a little while the installation is complete.



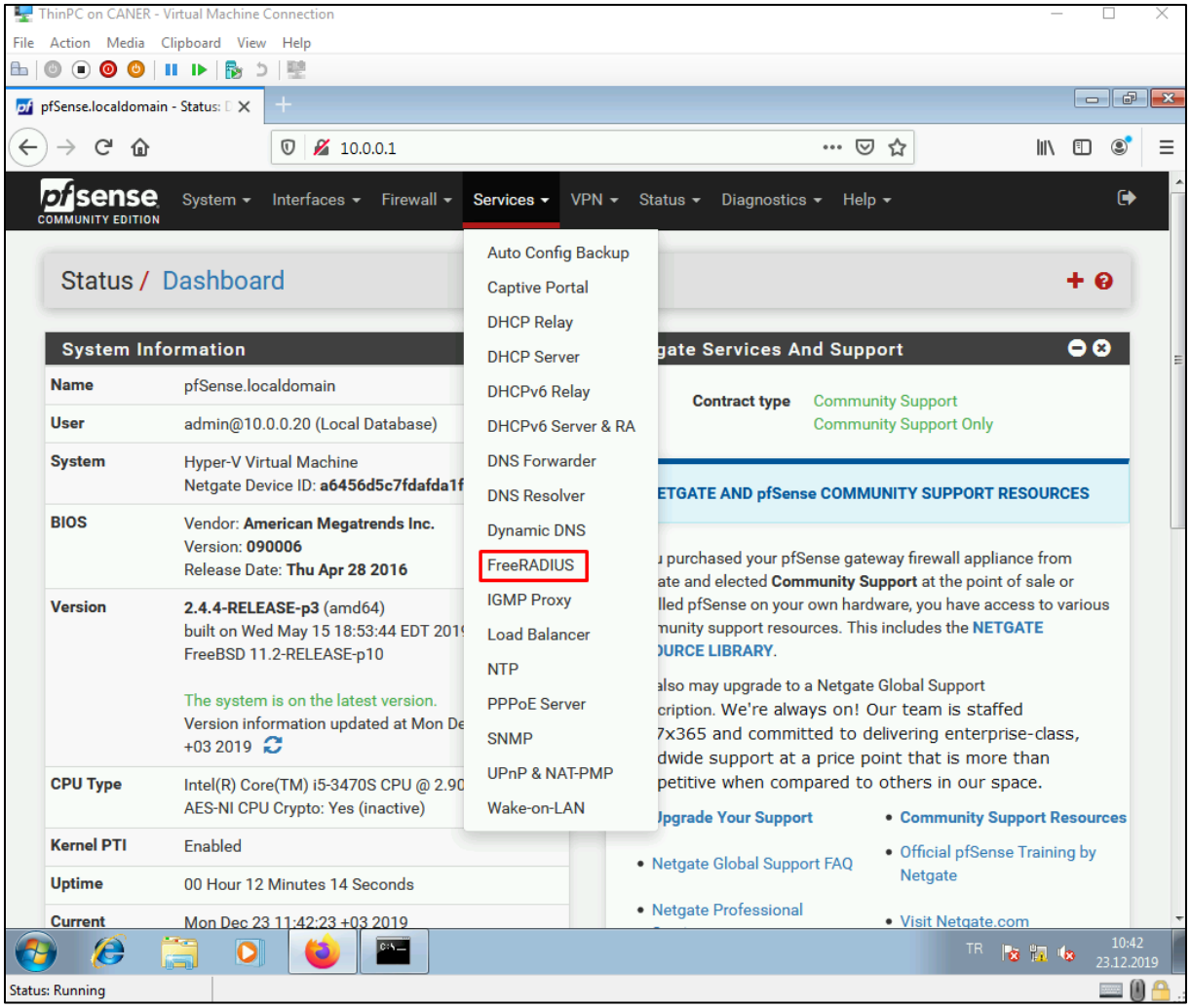
Then, we must reboot the firewall again.



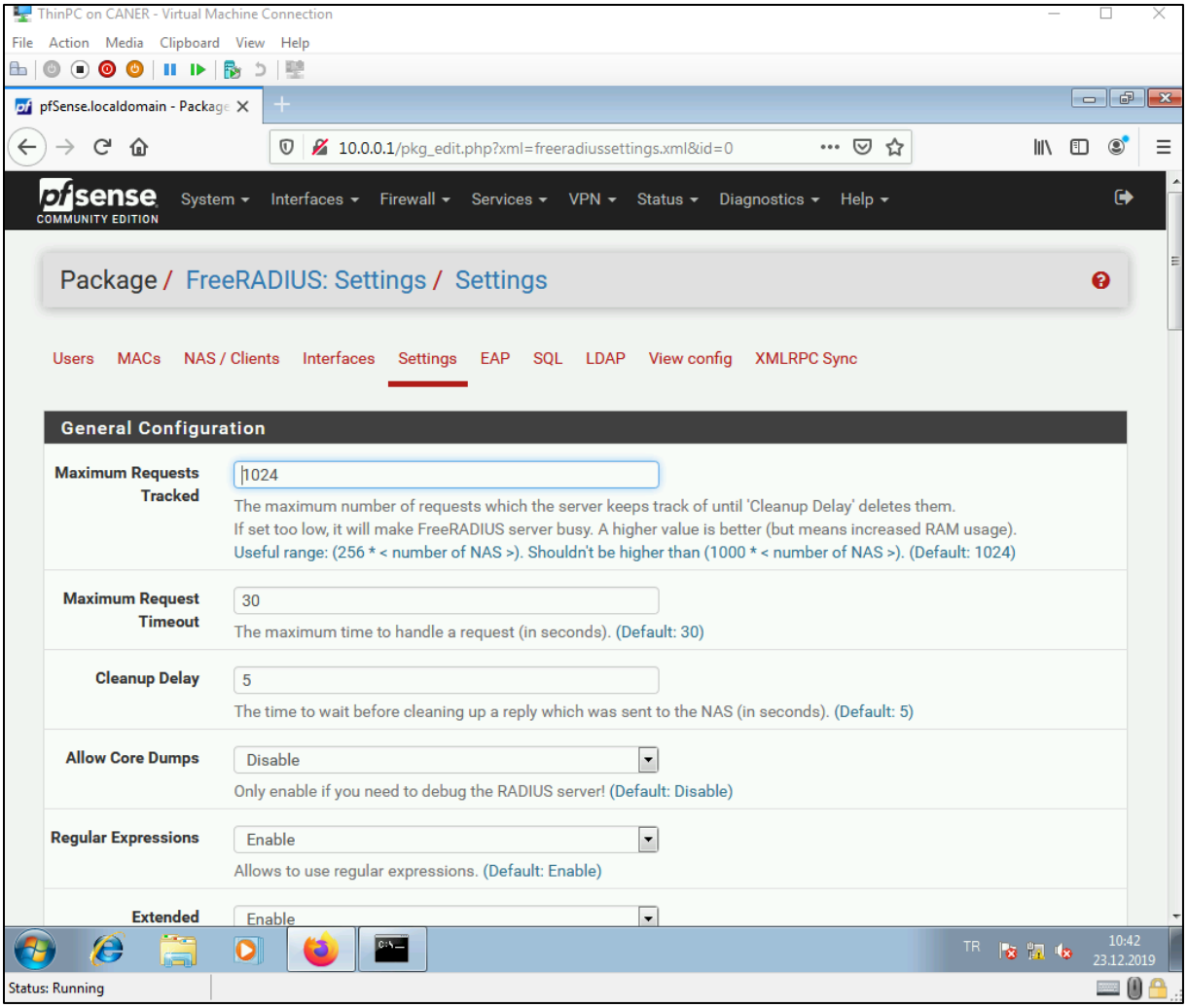
We confirm that the package is installed after the reboot.



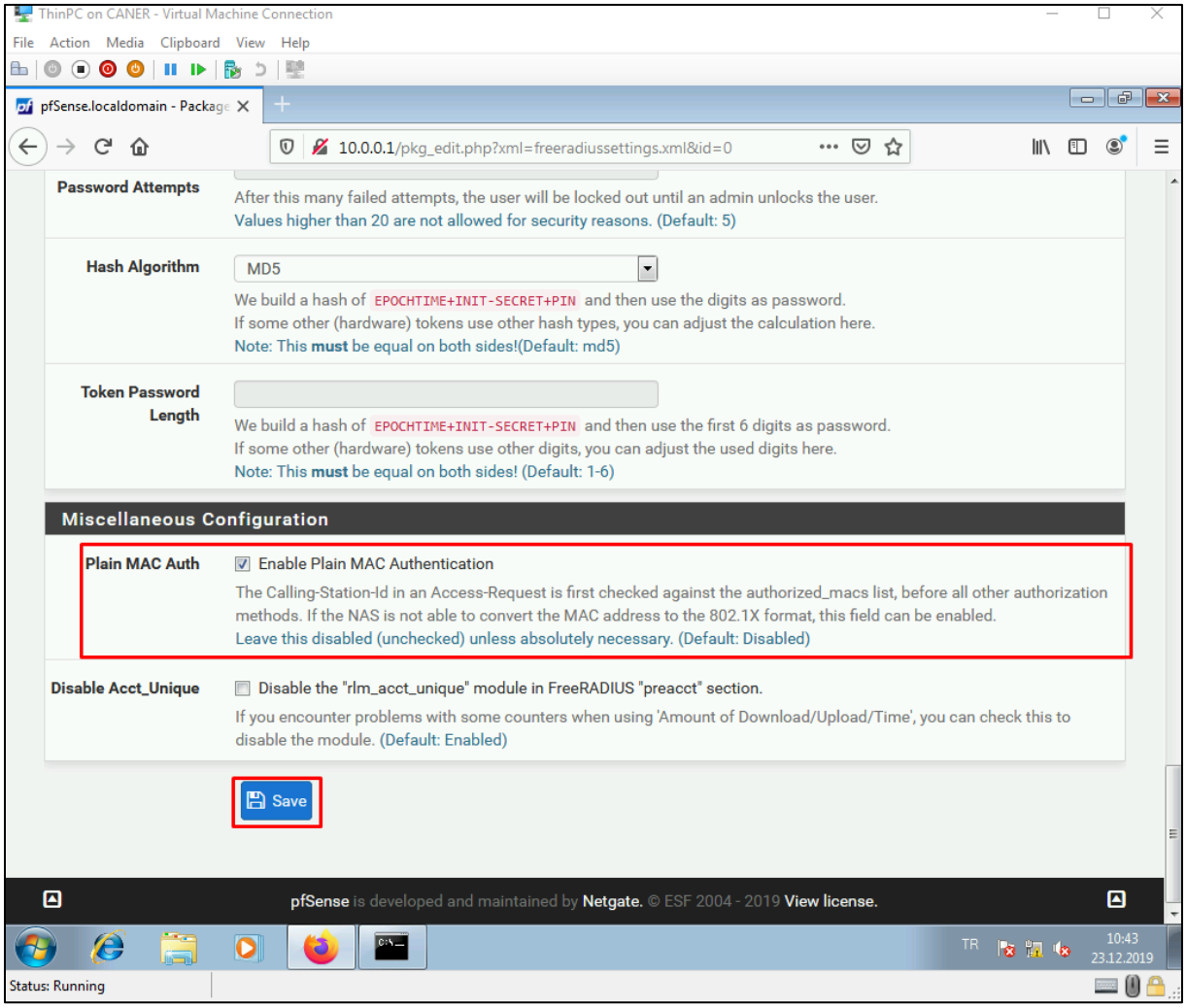
Then to configure the Radius we select it under Services.



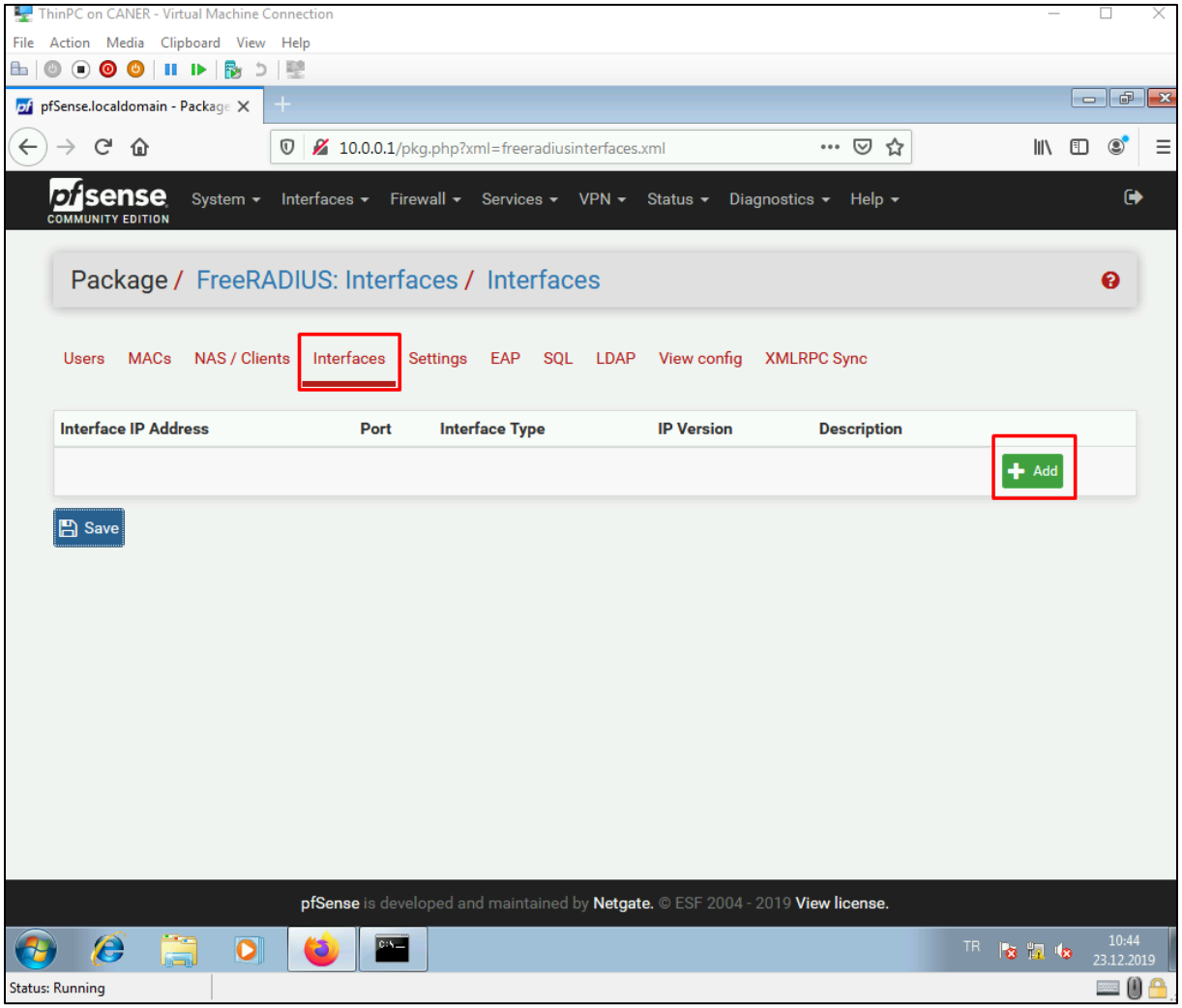
We go under Settings…



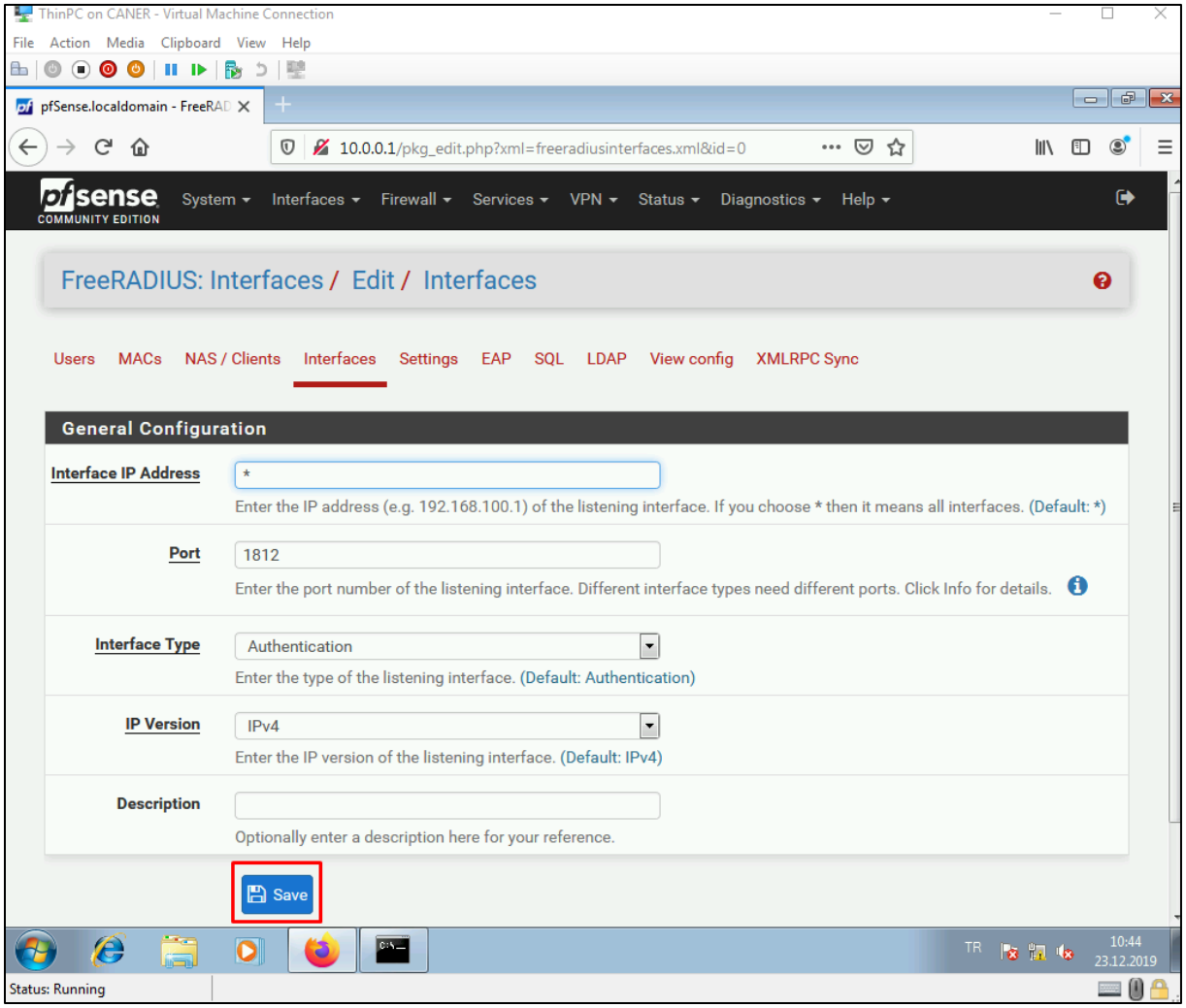
… and enable MAC Authentication.



We go under Interfaces and add a new one.

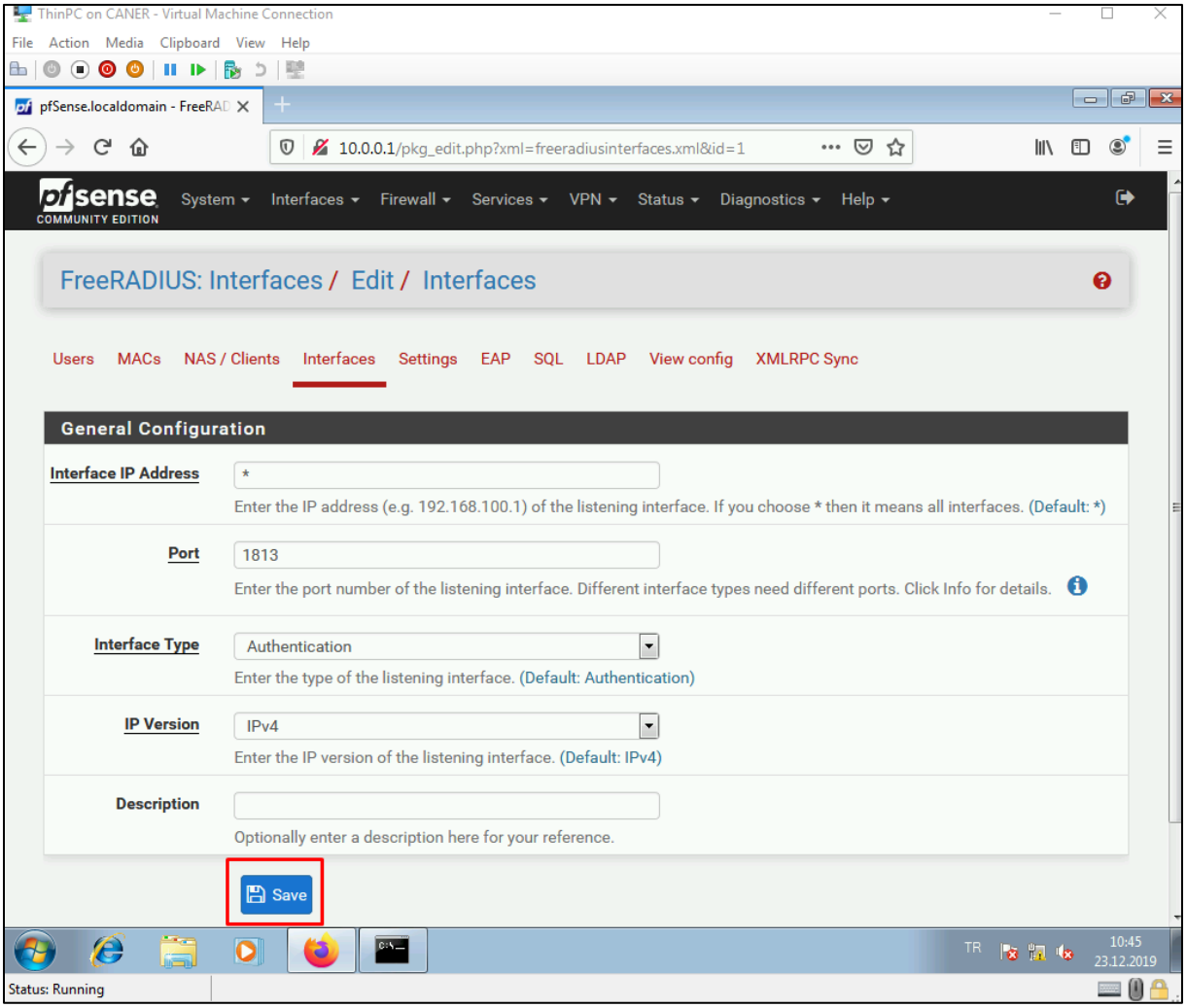


Port 1812 must be specified.

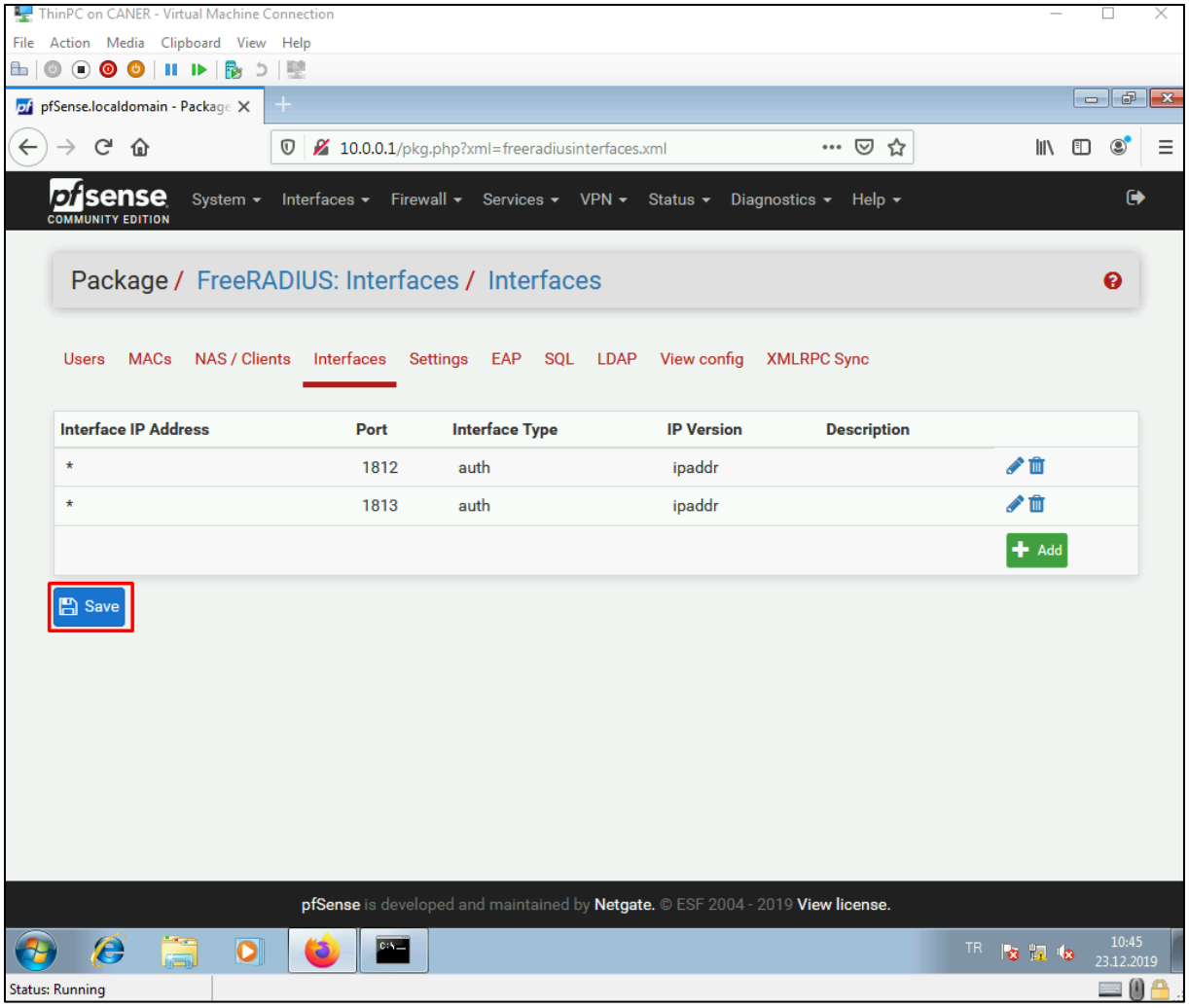


Then, we save.

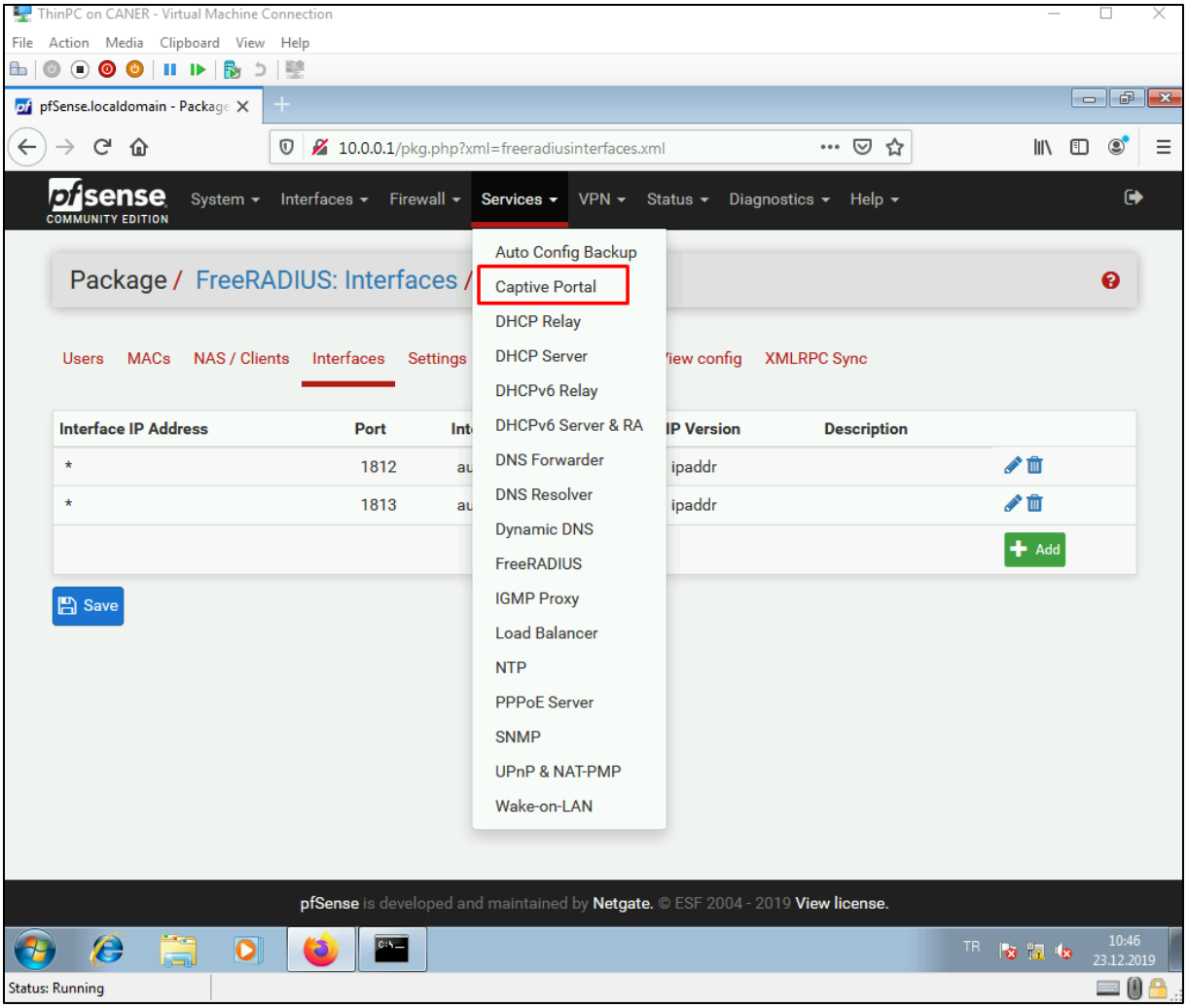
We do the same for port 1813 as well.



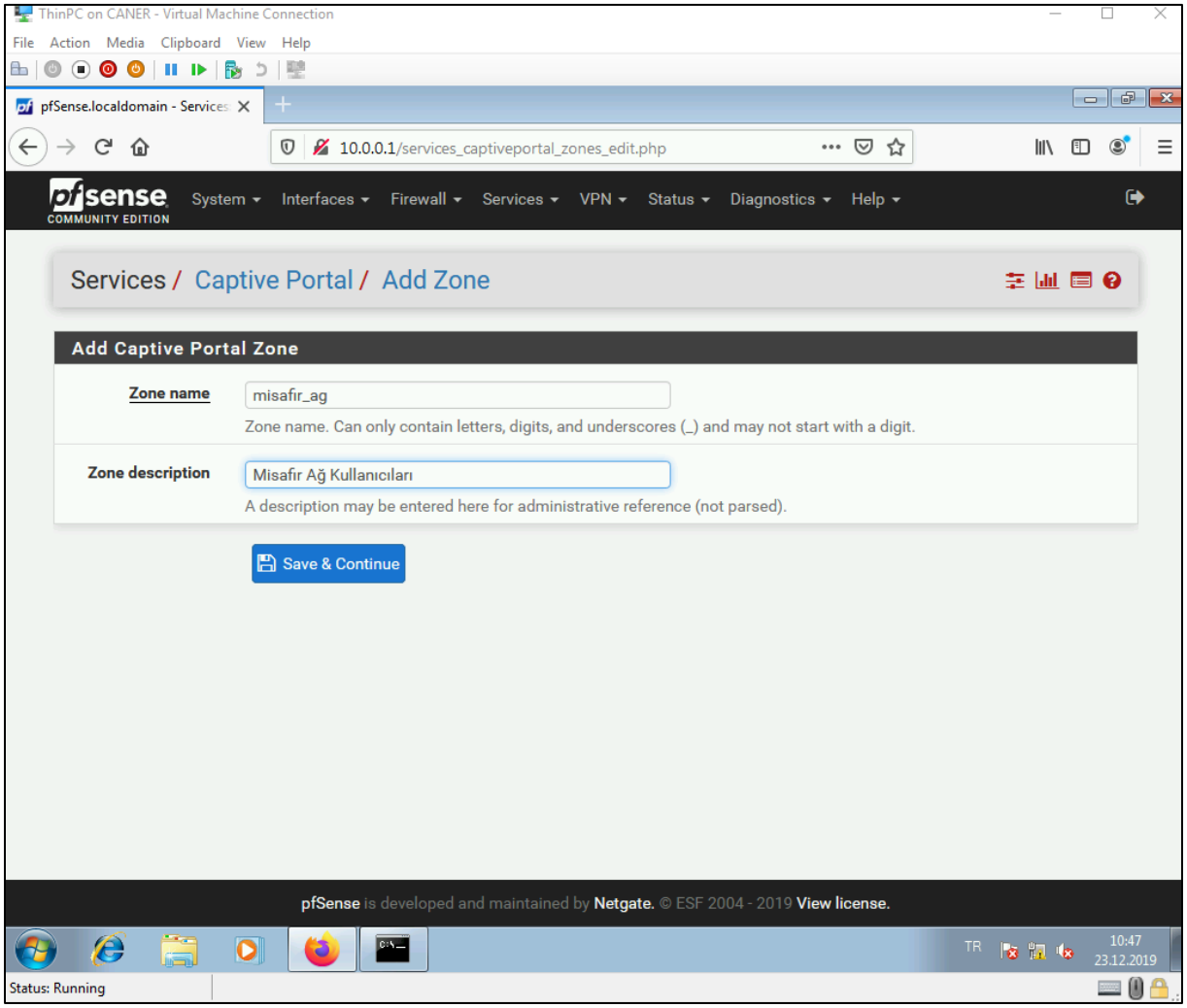
We save once again.



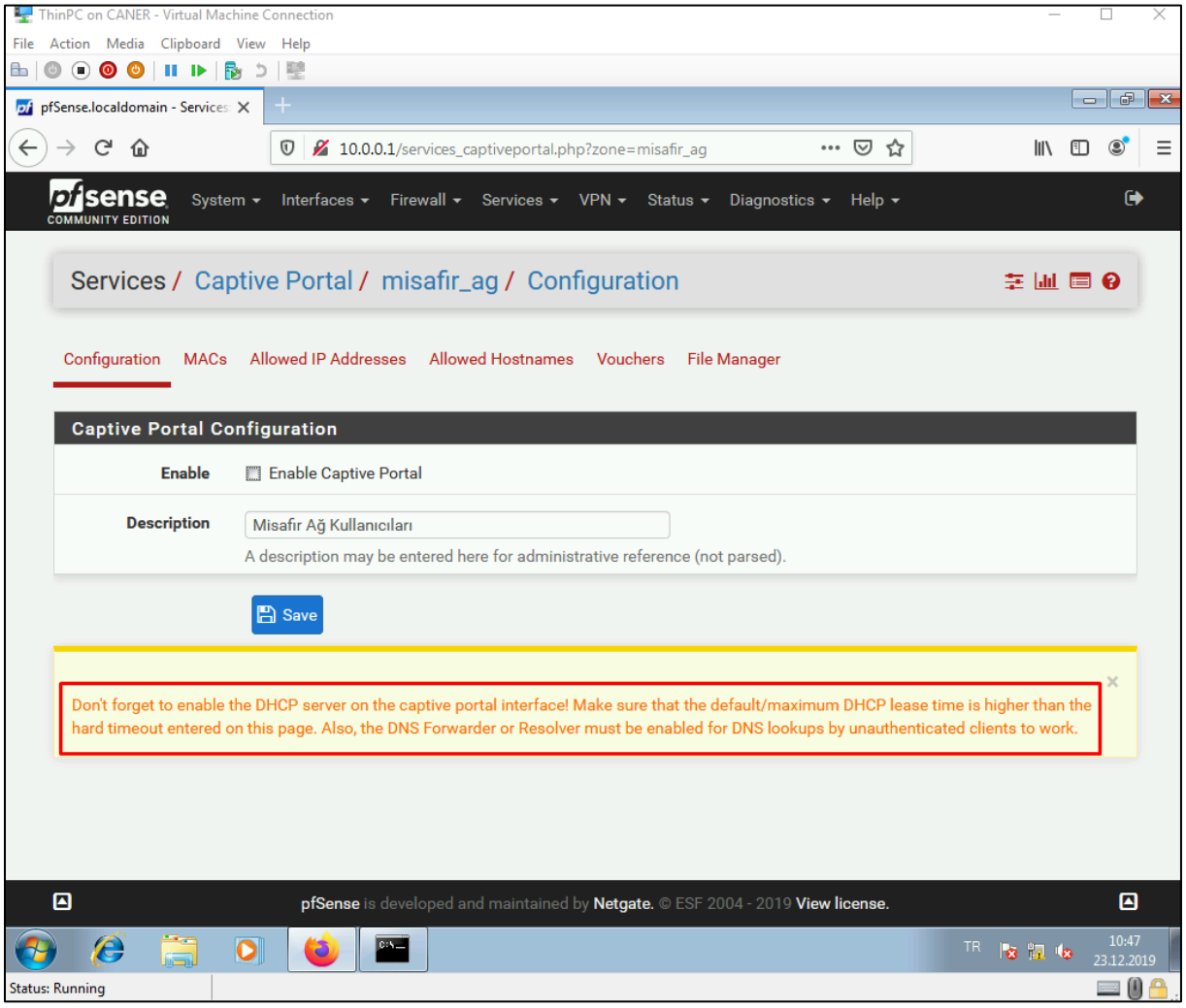
We then get to the Captive Portal Service.



We name the zone we want to use.

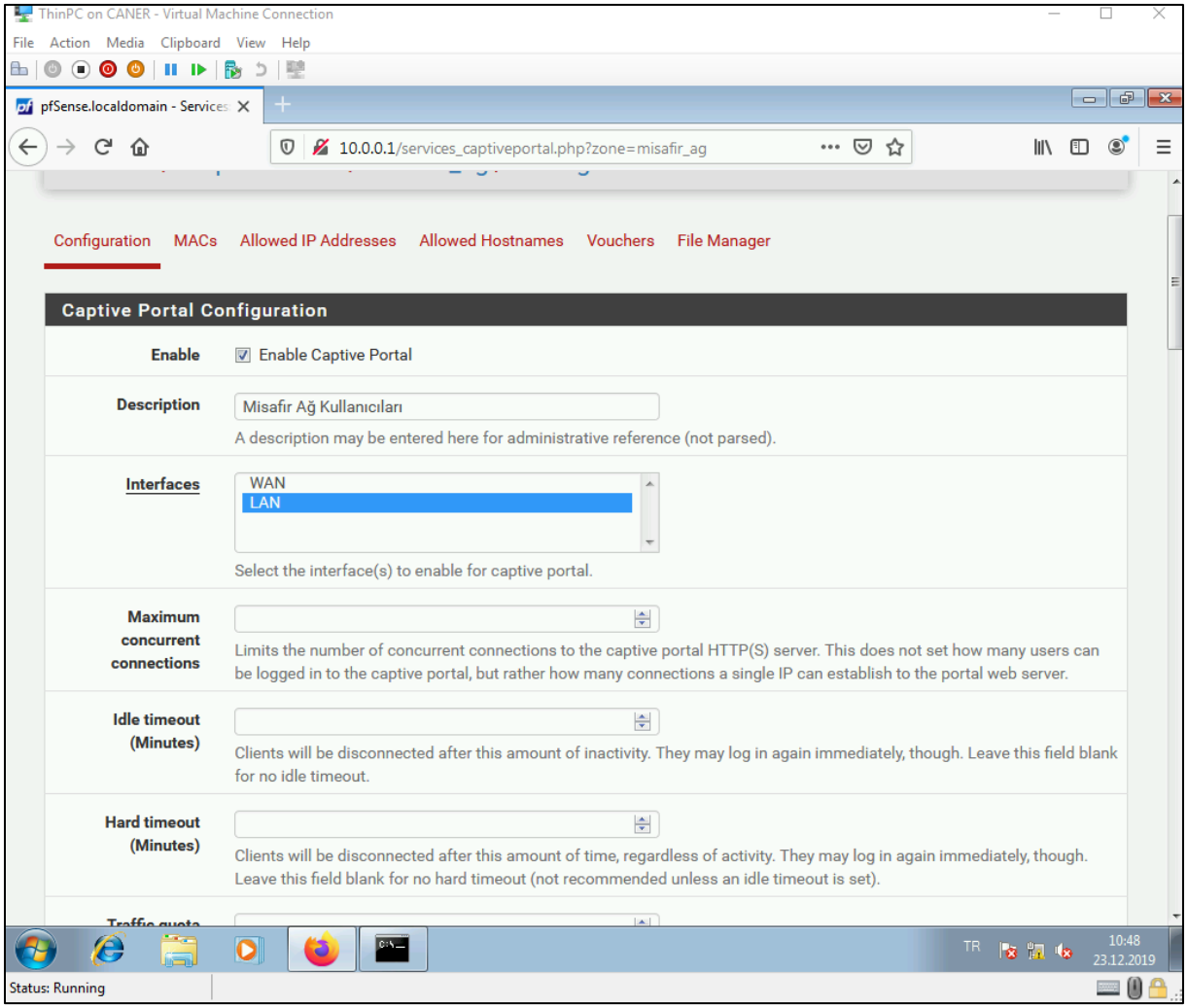


pfSense reminds us to use DHCP for the interface we will be using for the portal. Luckily, that is already case for us.

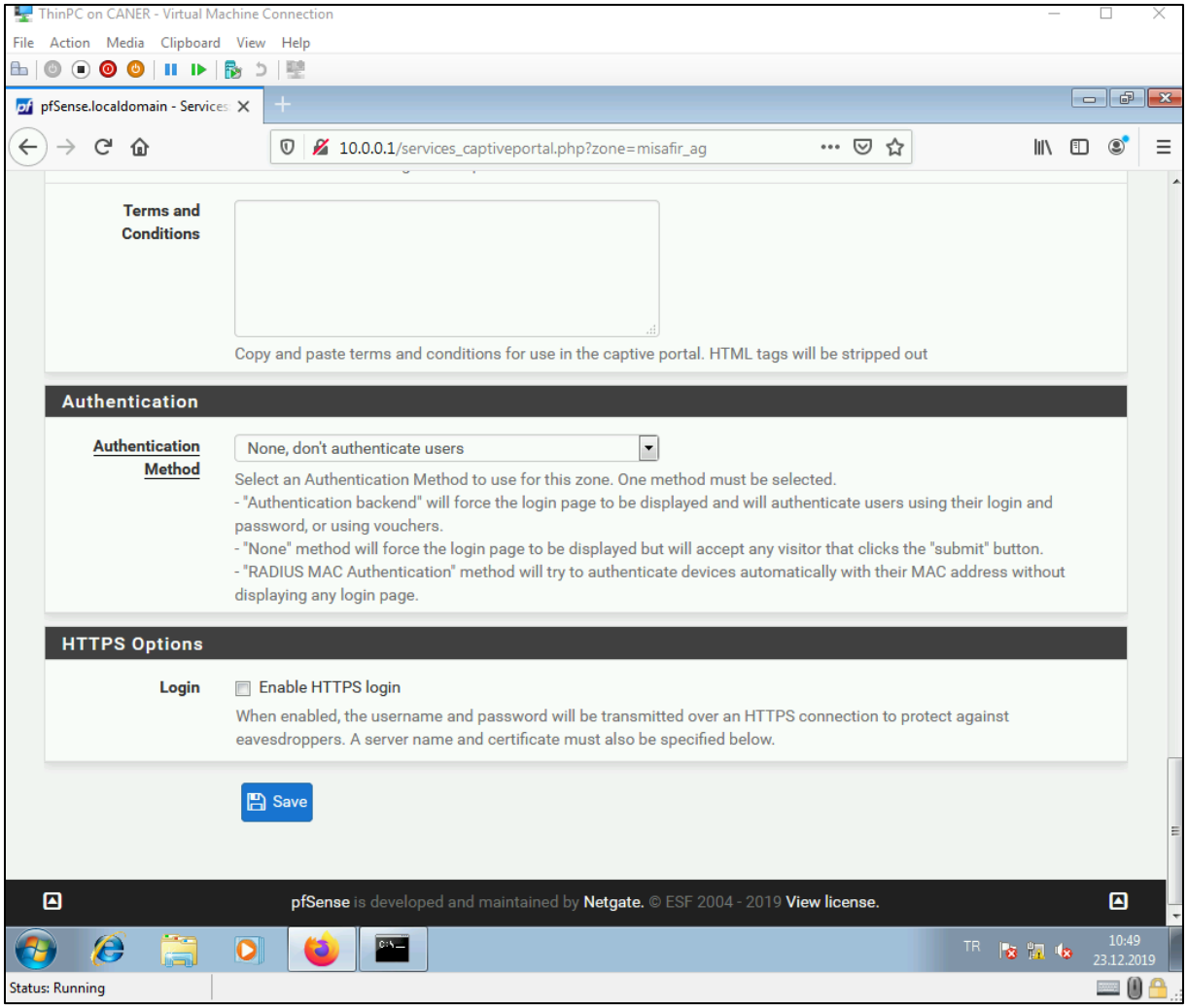


Once we enable the service…

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

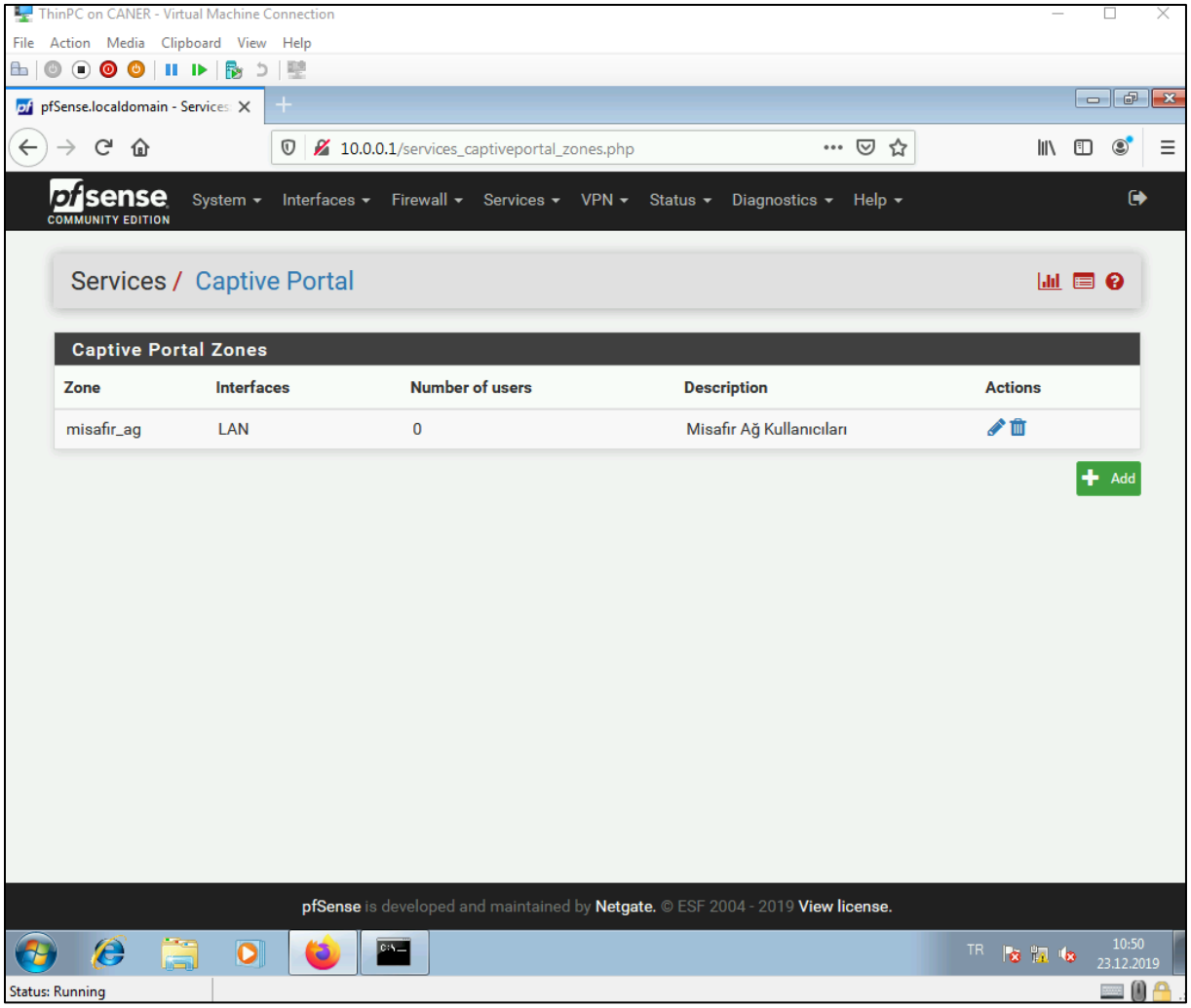


And for now, we don’t change anything else.

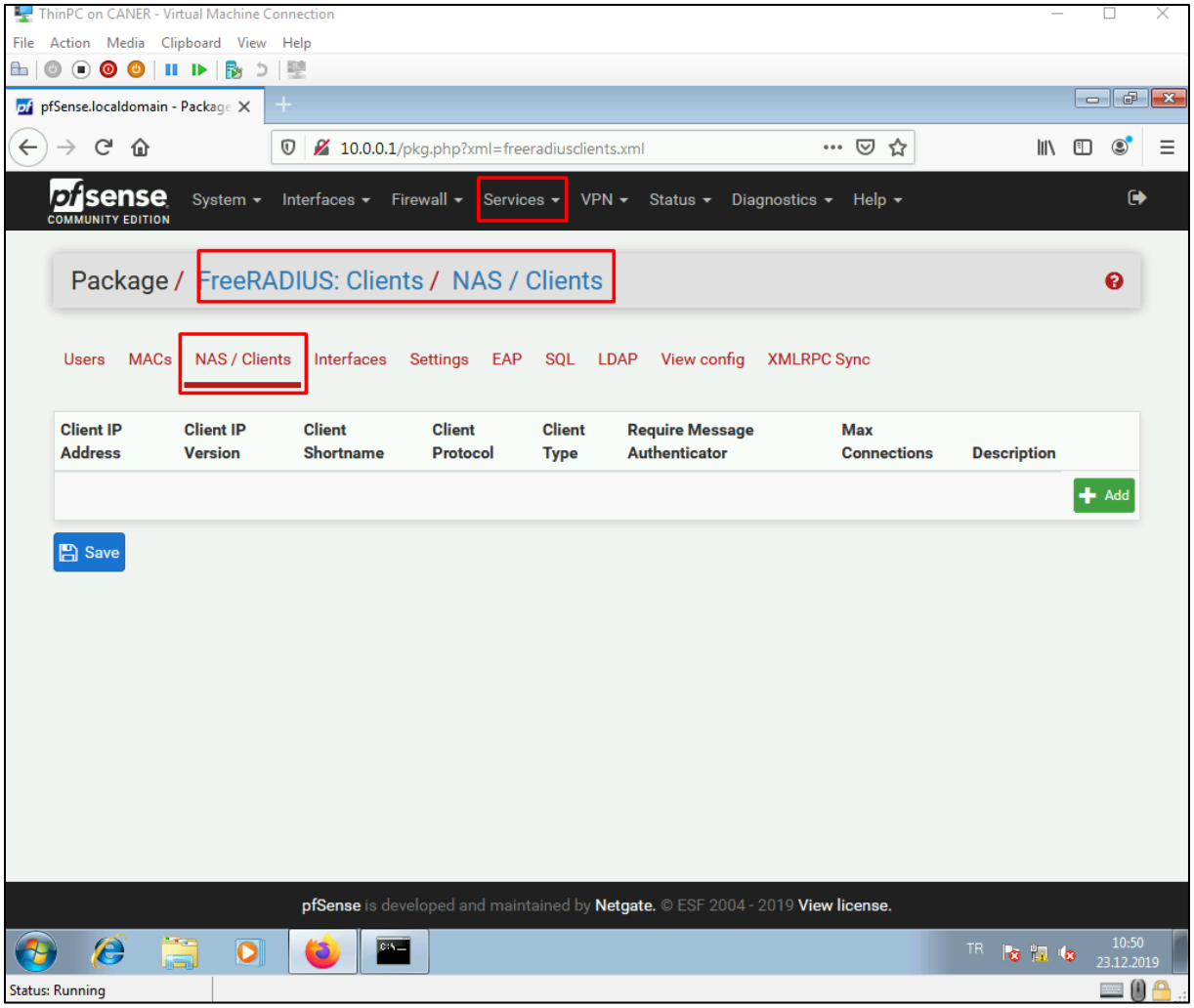


We will come back to these settings and modify them in a bit.

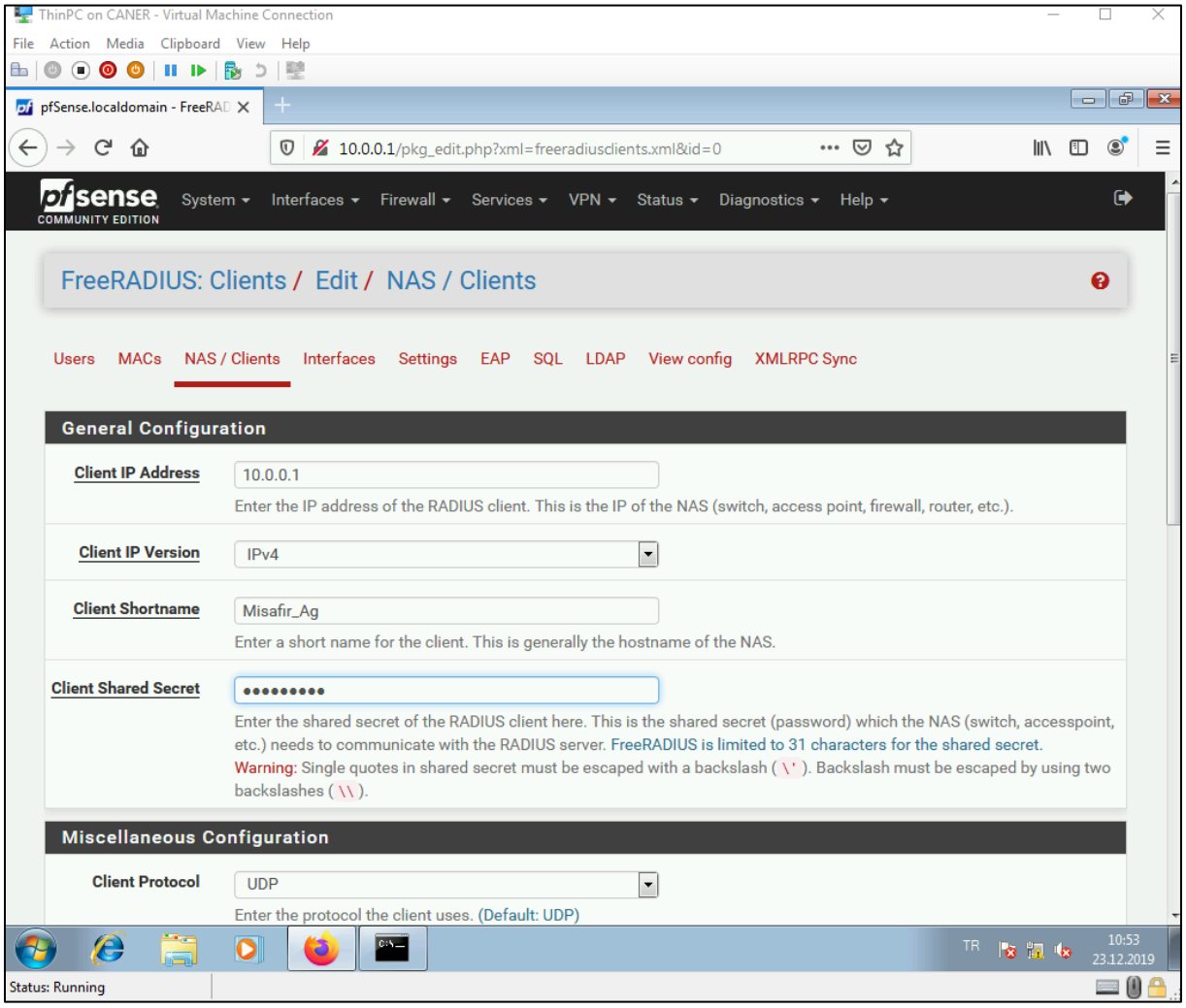
This creates the zone.



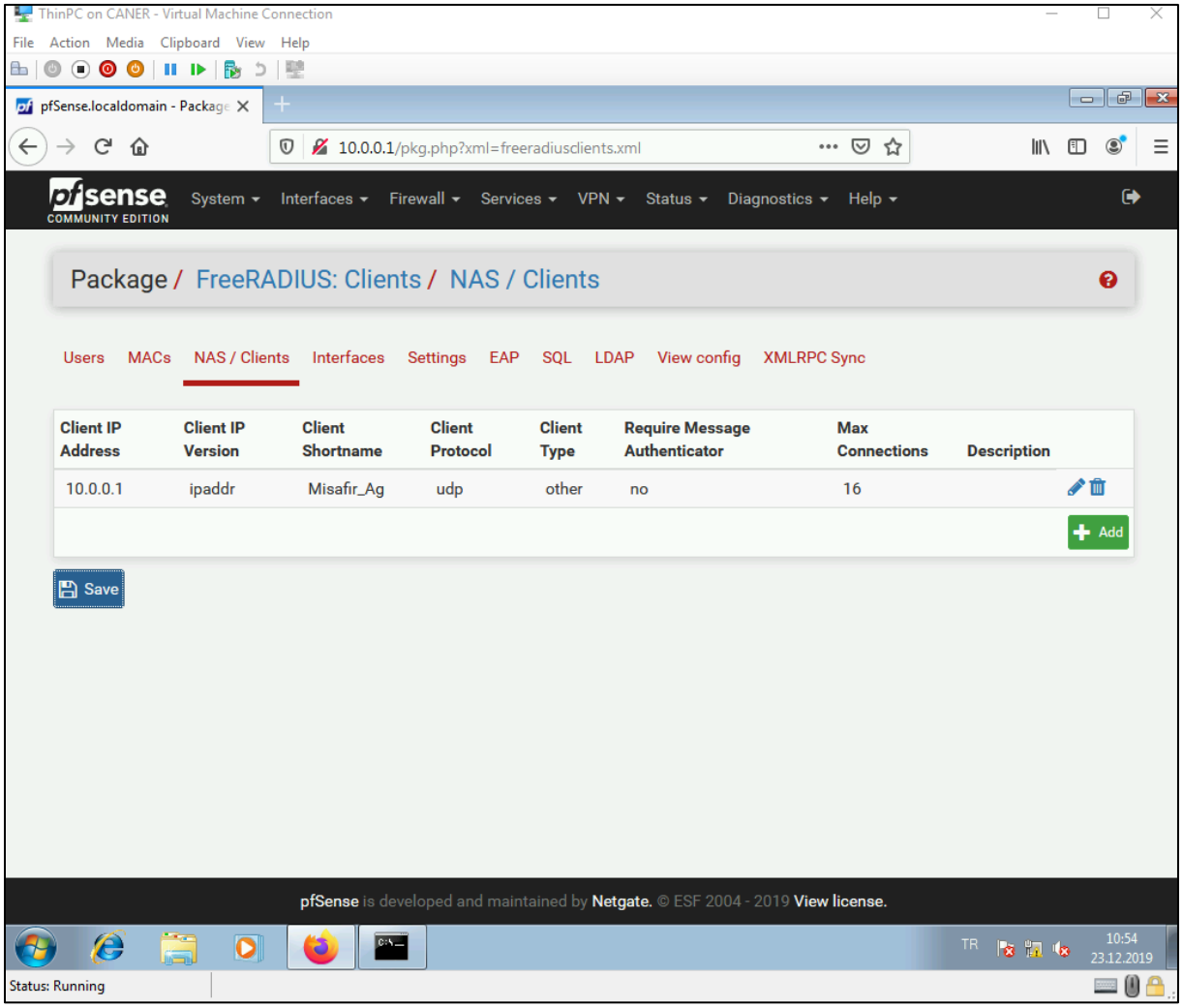
We now need to create some NAS clients.



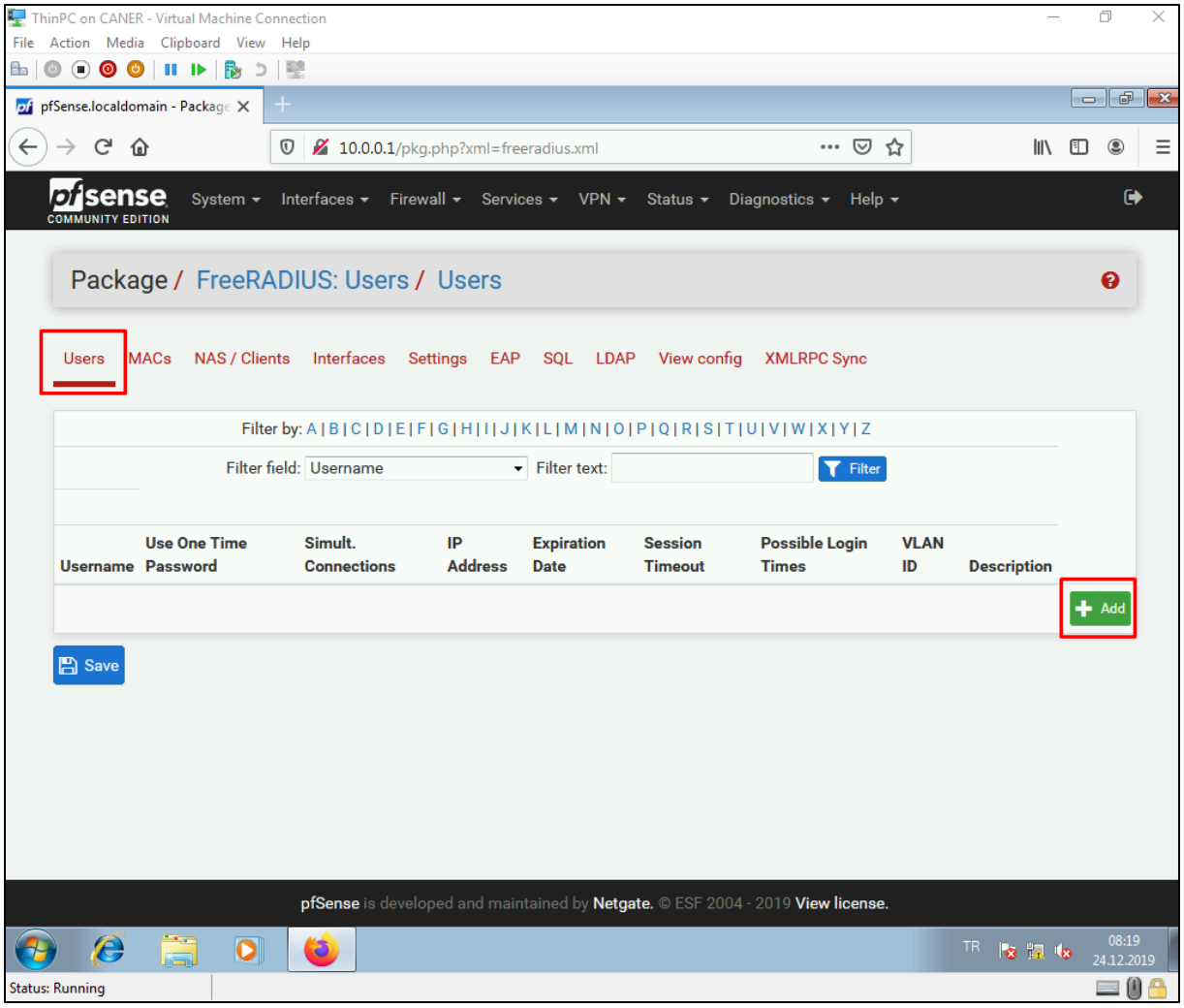
We determine a private IP address. We must enter a “Shared Secret” here. It is crucial to remember this secret as it will be mandatory that we use the same string later.



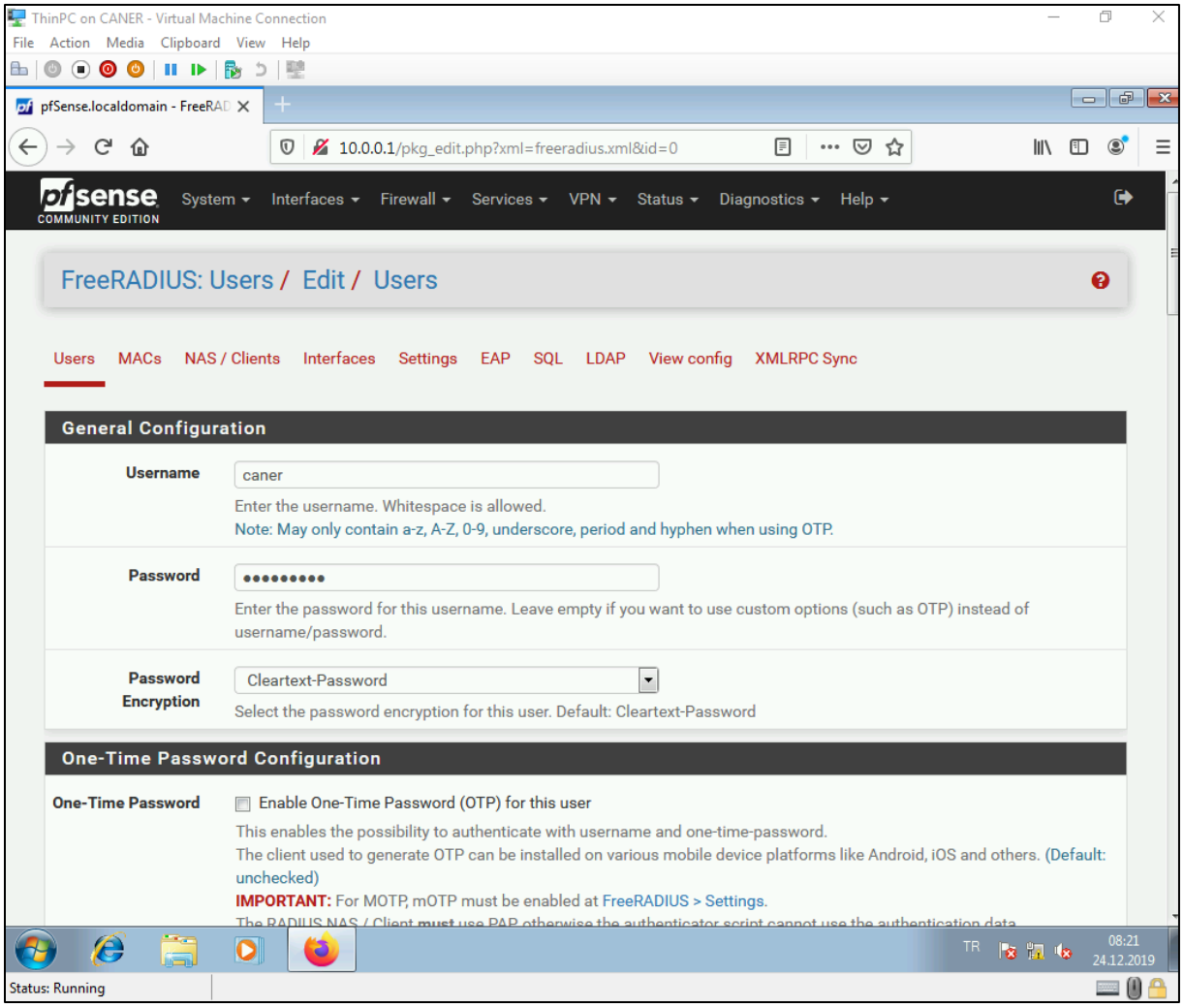
This creates the client.



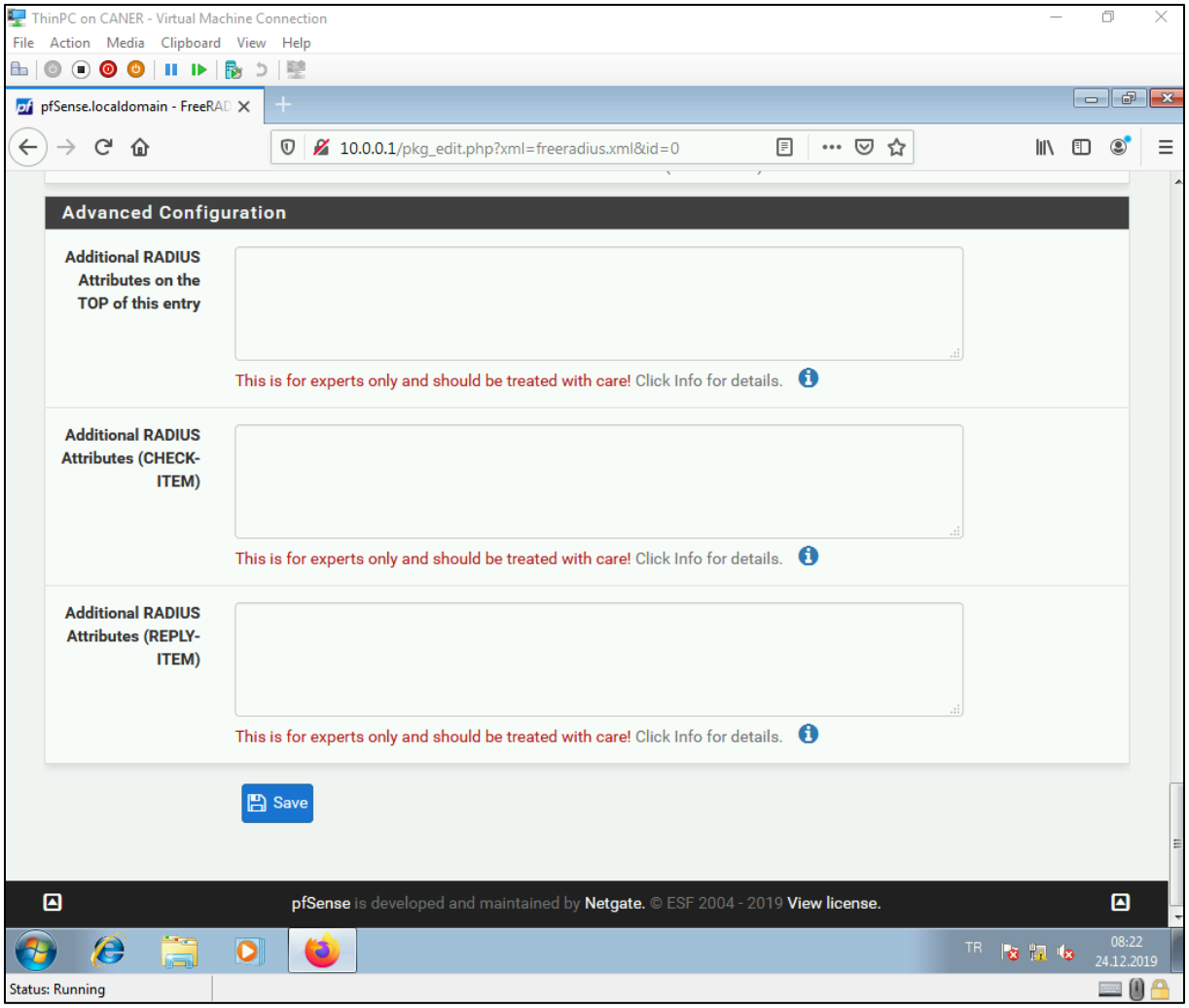
We now need to create some users to login to the portal.



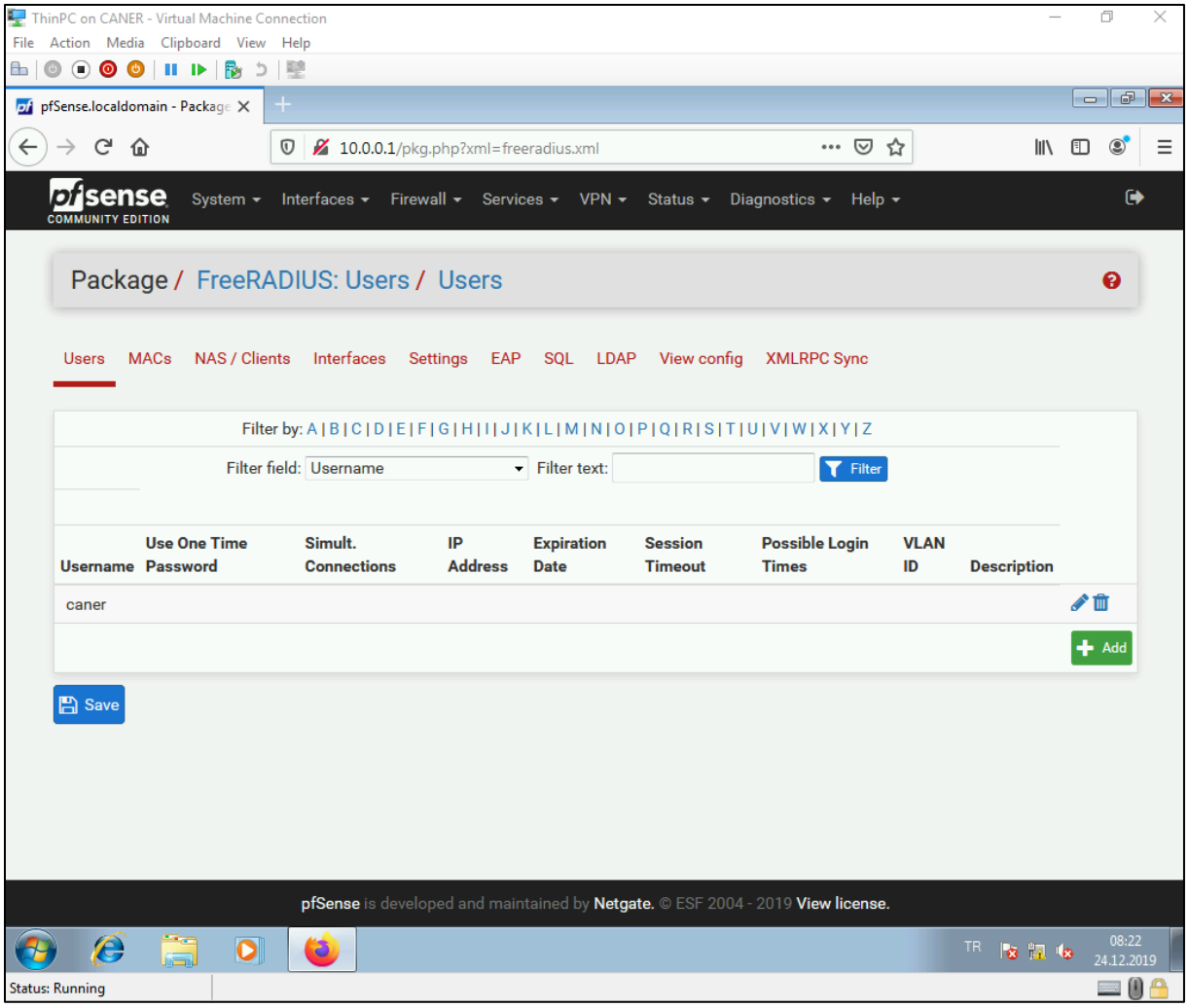
We give them usernames and passwords.



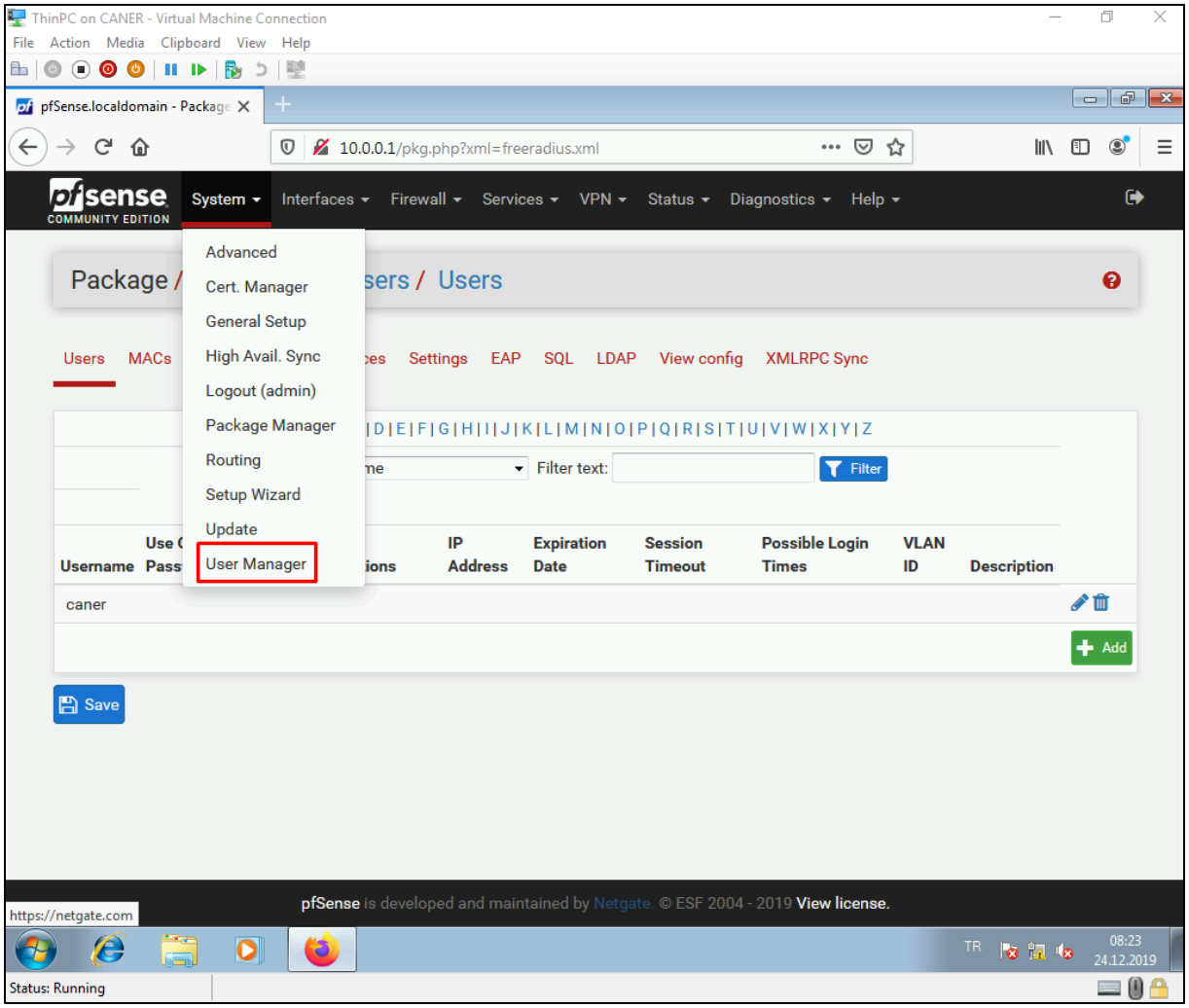
We do not change of the settings.



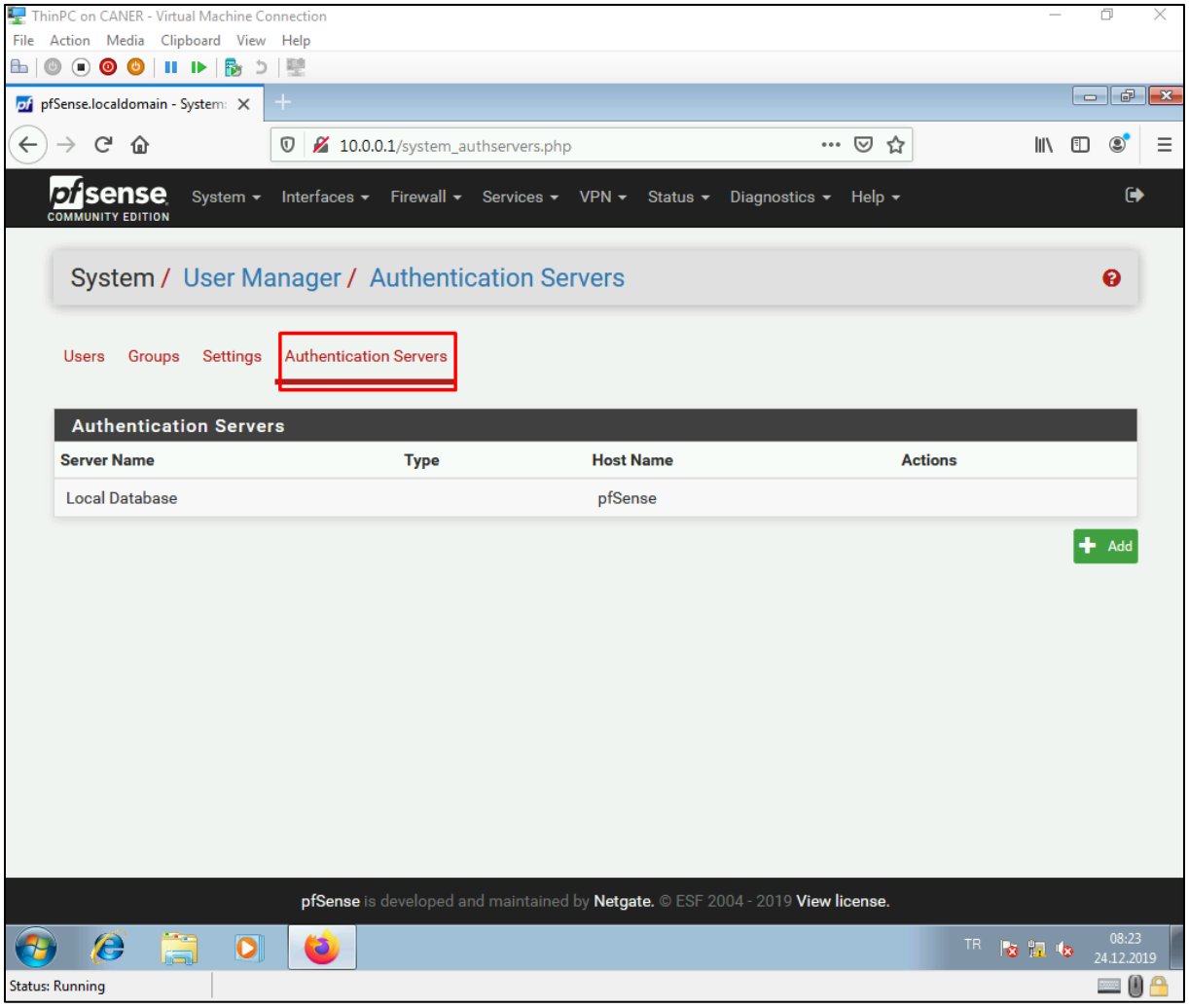
And, now we have a new user.



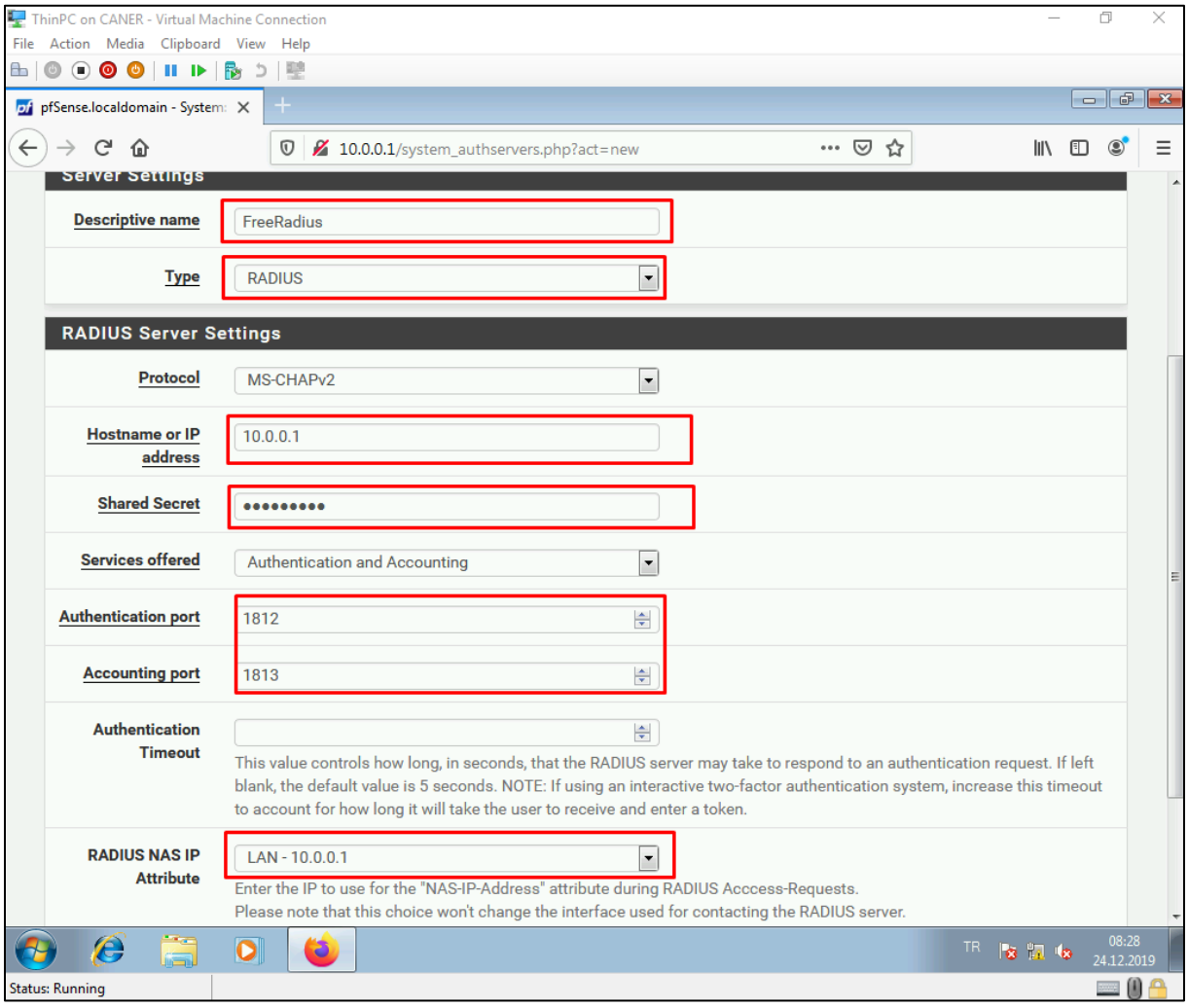
We now need to get to the User Manager.



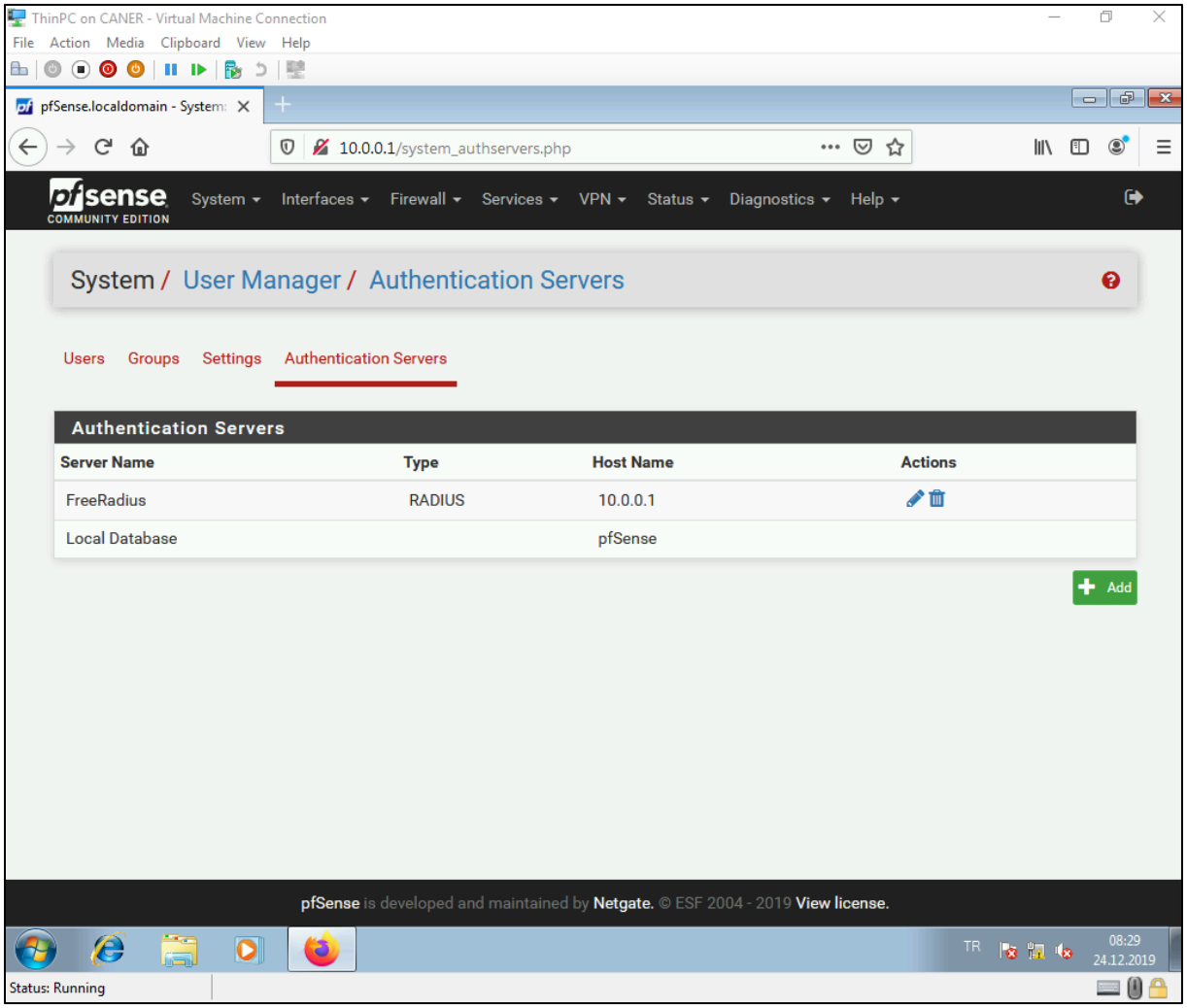
We select the Authentication Servers tab and create a new one.



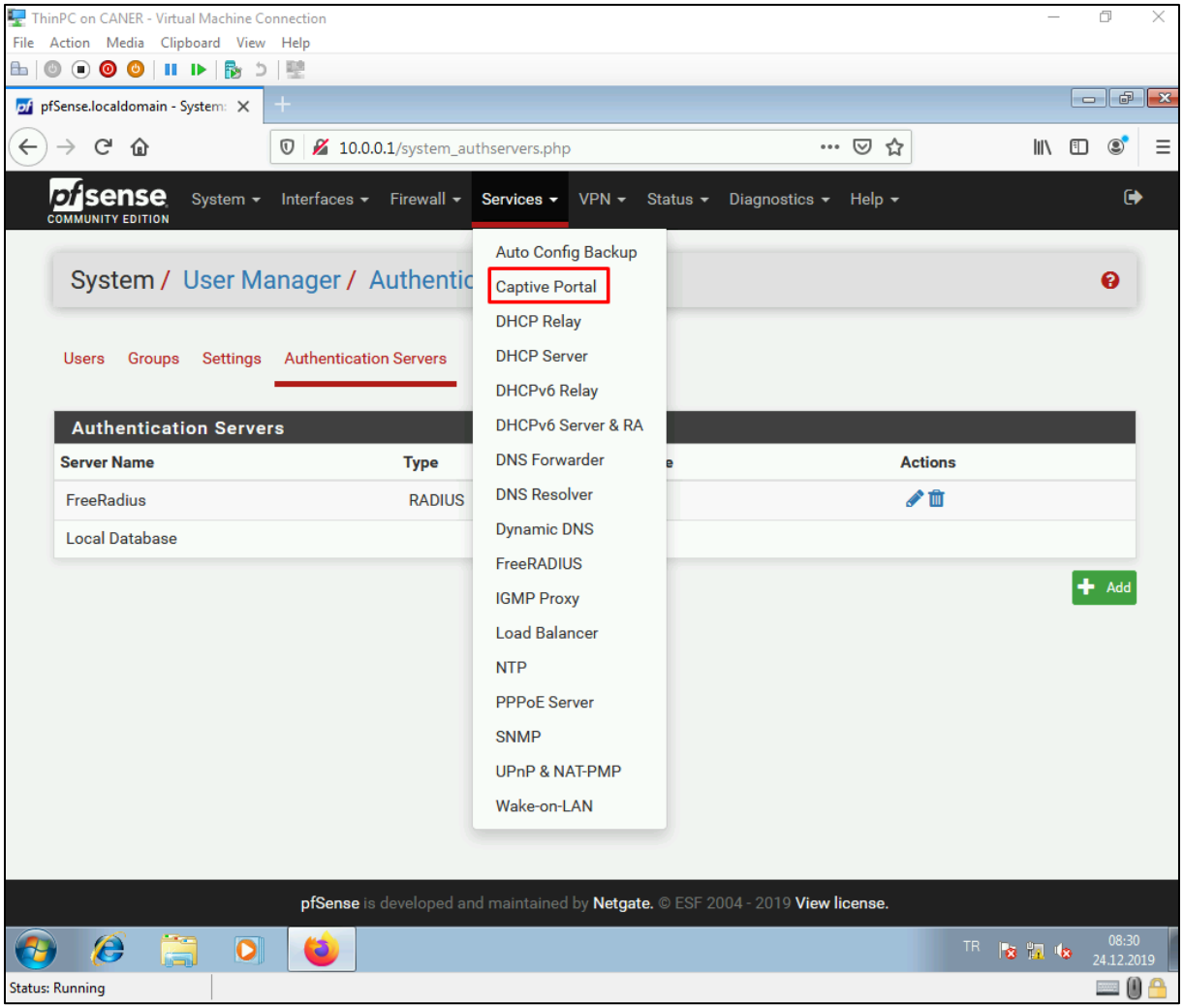
We create it with specific details that we have set up previously. The type is Radius. The ports are 1812 and 1813 and hostname IP is the NAS client IP address. Finally, the secret is the same “Shared Secret” that we used in NAS client. All of these are very important to set the same; otherwise, the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



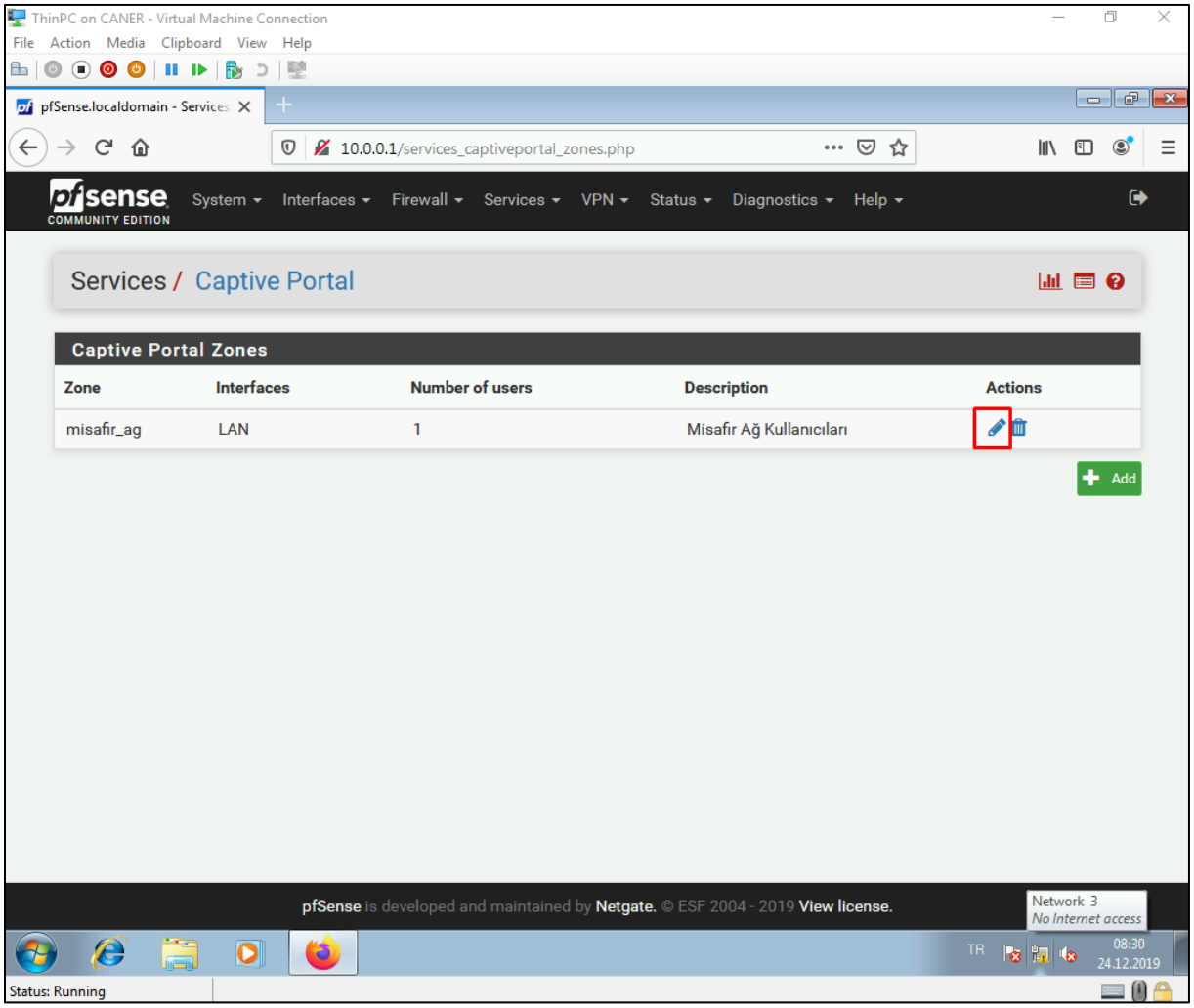
Once we save, we have the new Authentication Server.



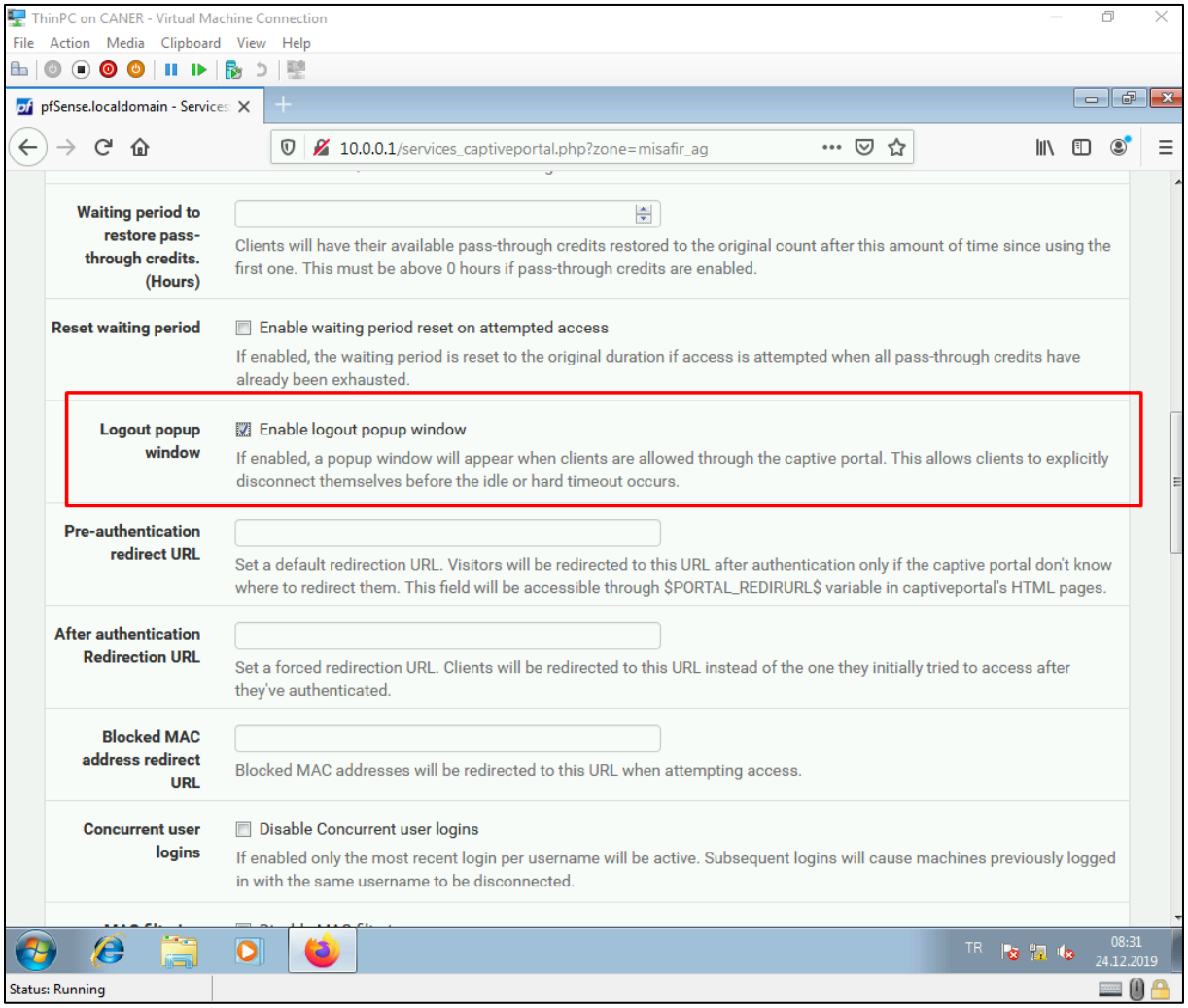
Now, we need to get to the Captive Portal again to start the authentication process.



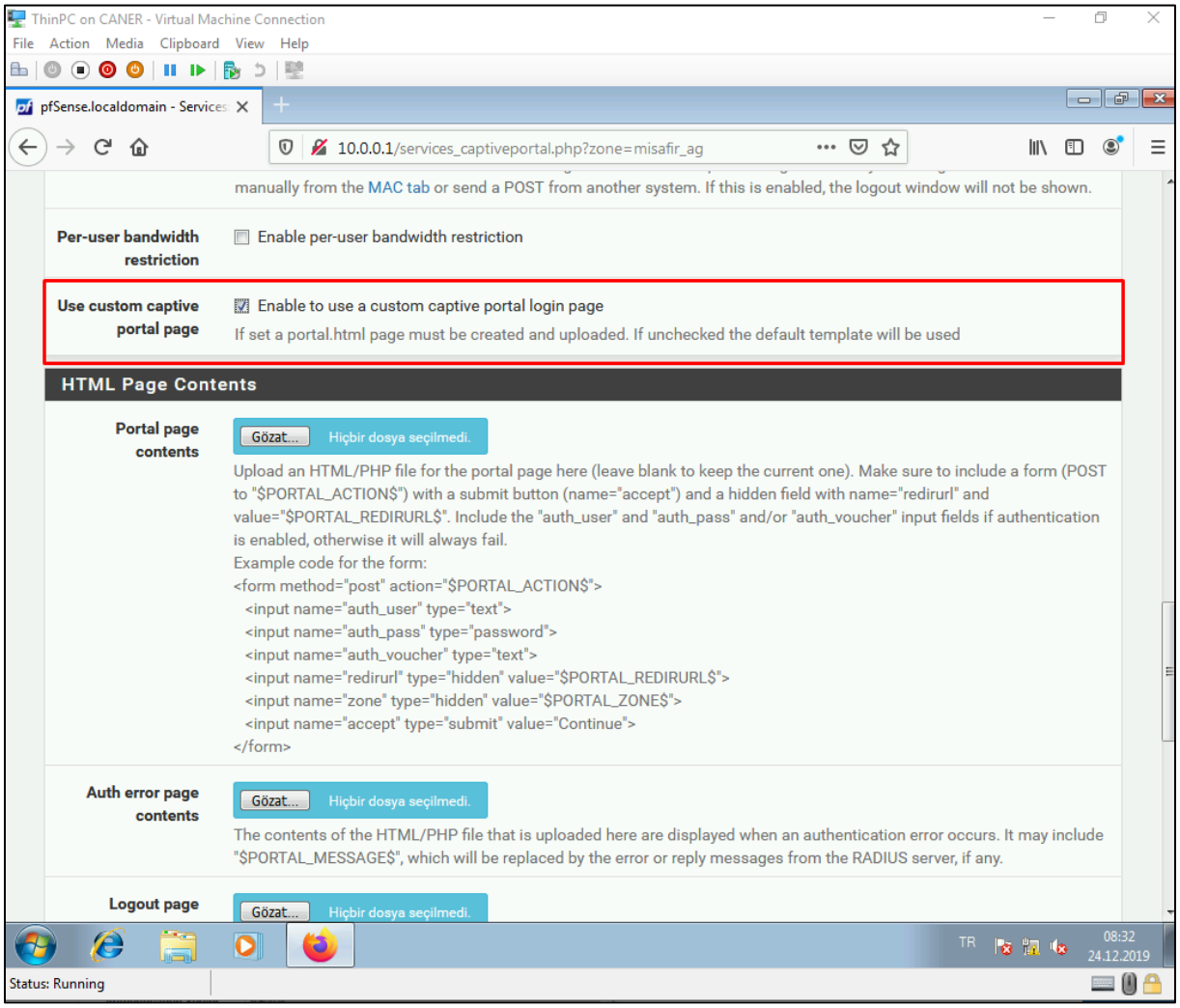
We edit the previously created portal zone.



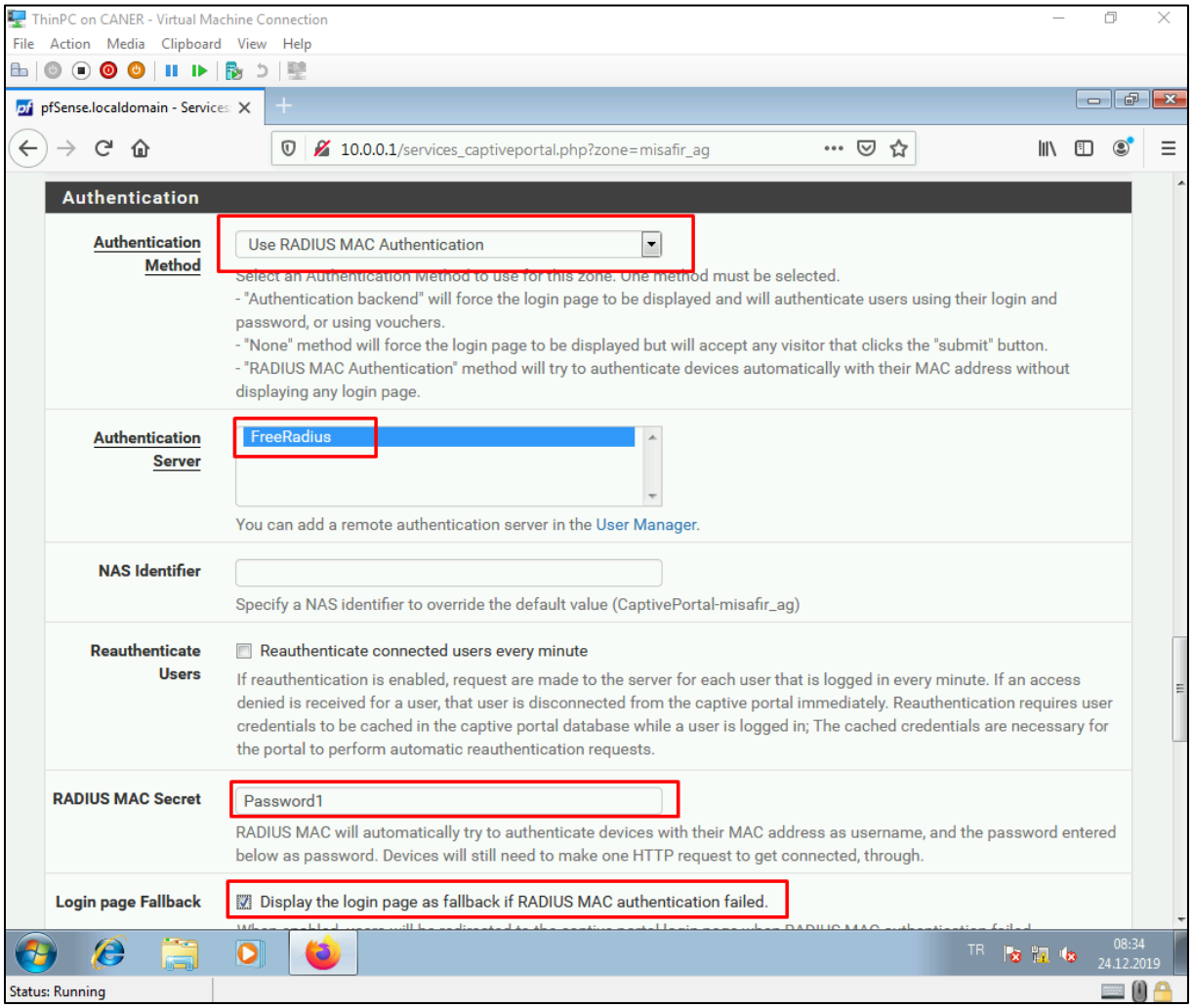
We enable the logout popup window.



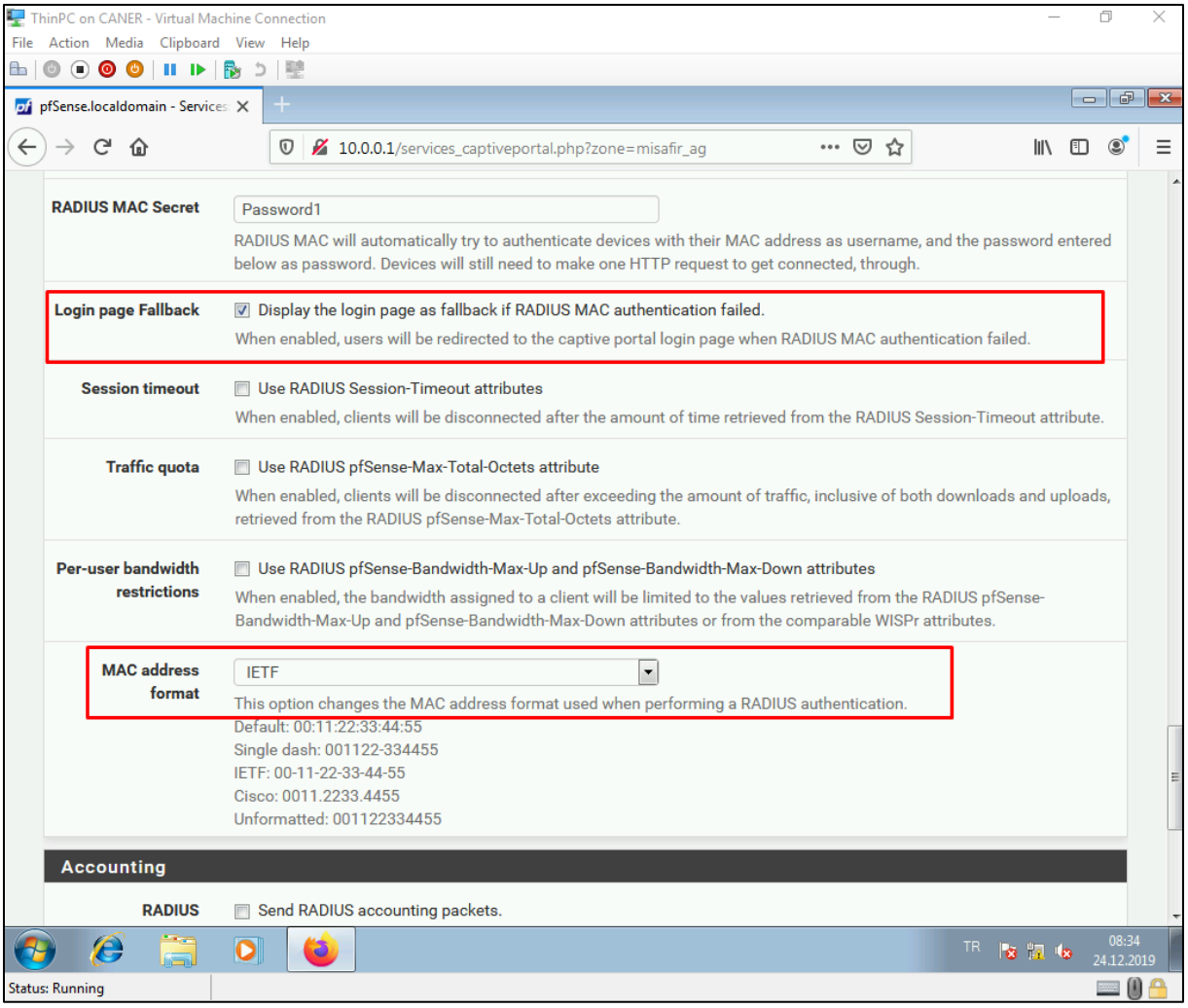
We can enable the custom captive portal login page to design it as we like. We use the default one but this changes nothing in the security of the portal.



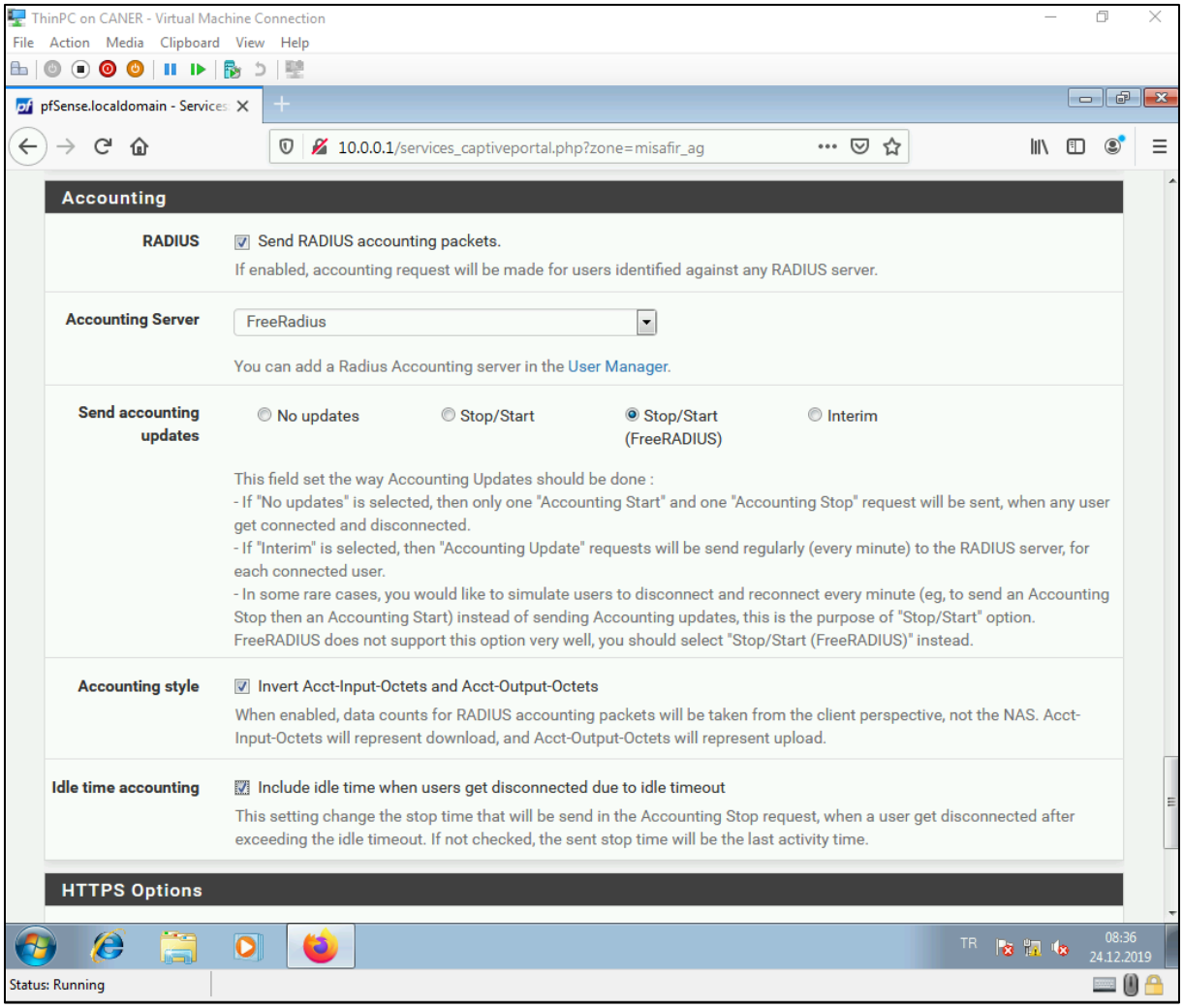
We choose the Radius MAC Authentication and choose our previously created Authentication Server. We enter the same secret.



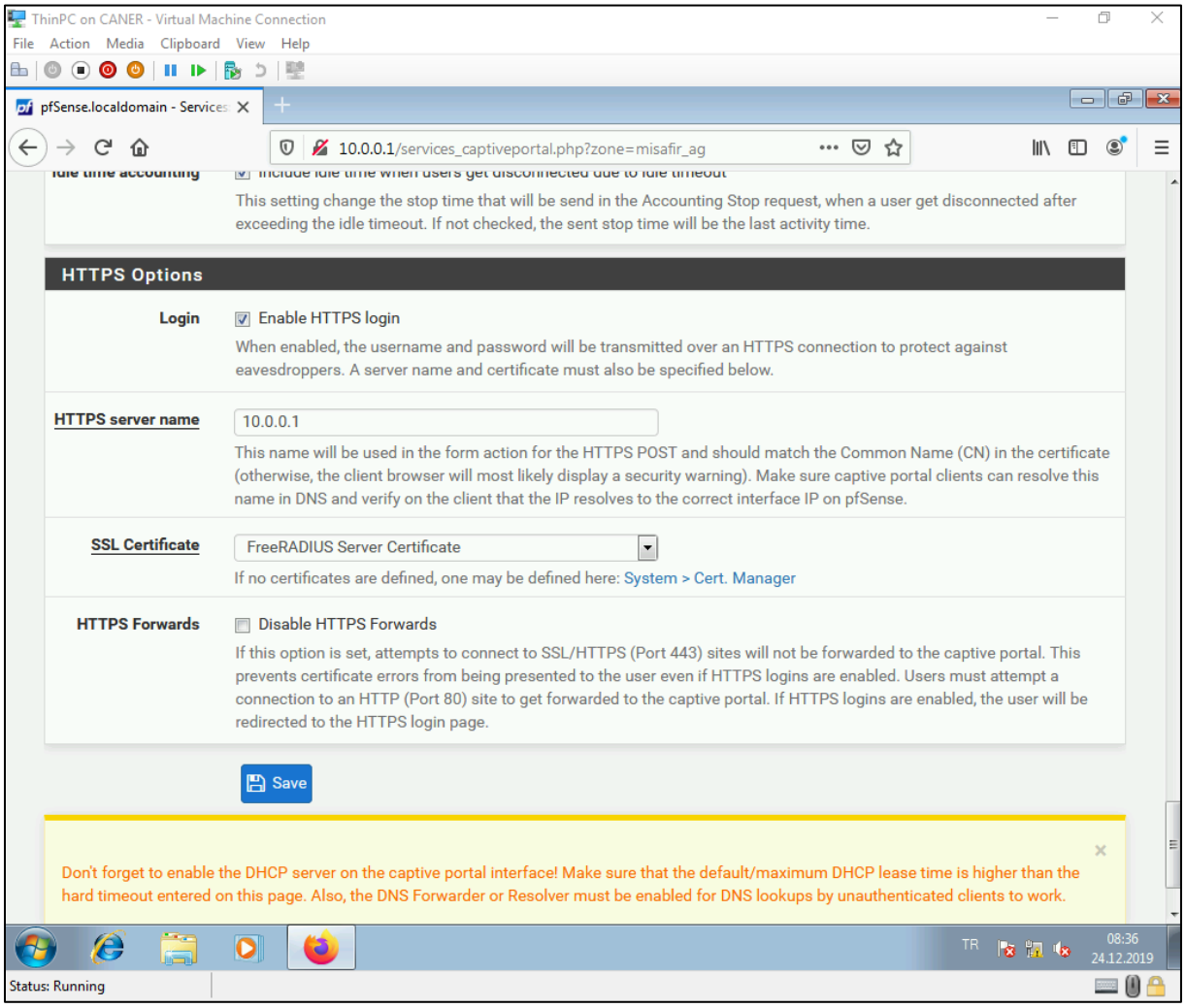
We select the following options as well.



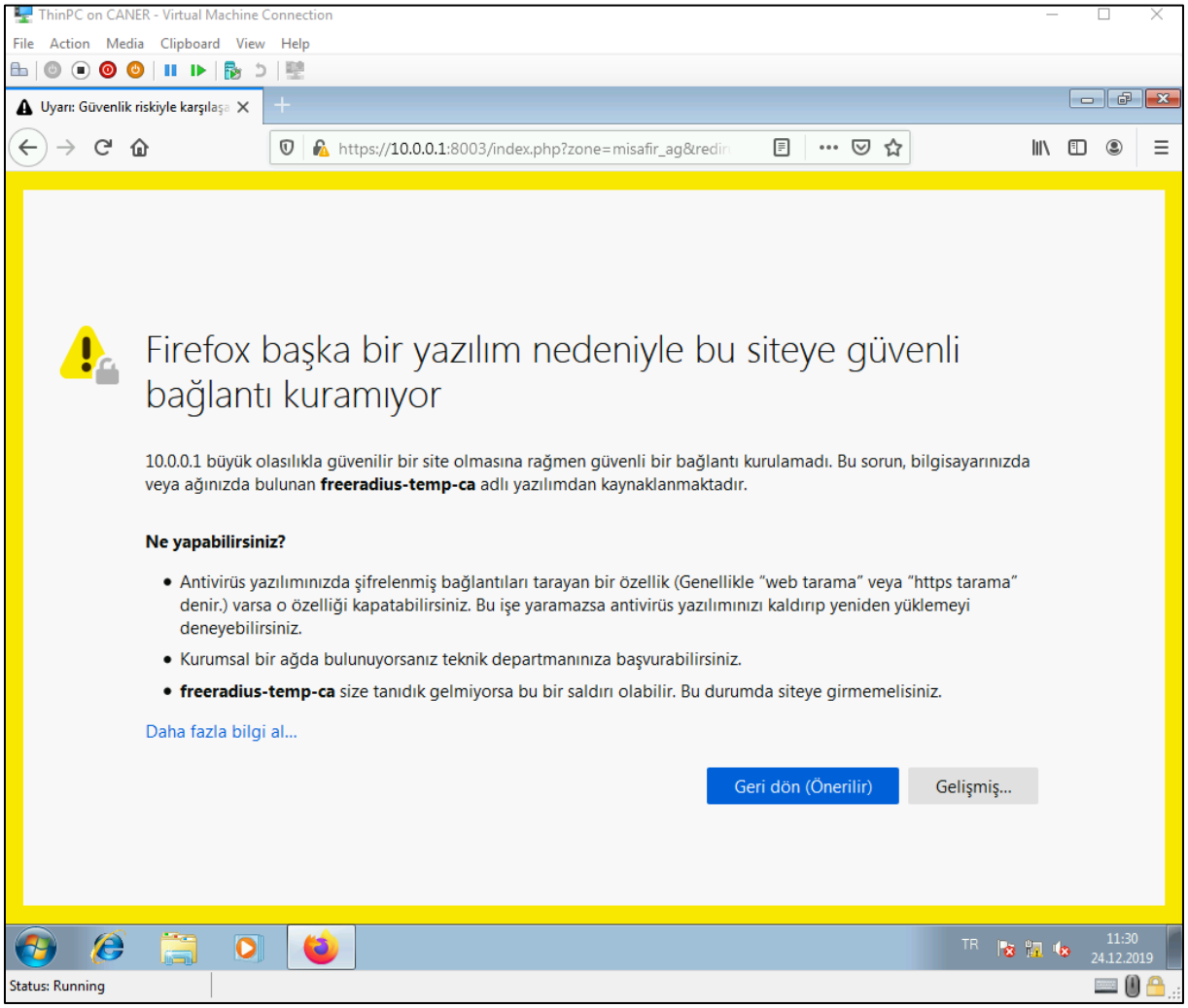
We set it up to send Radius accounting packets with the following specifications.



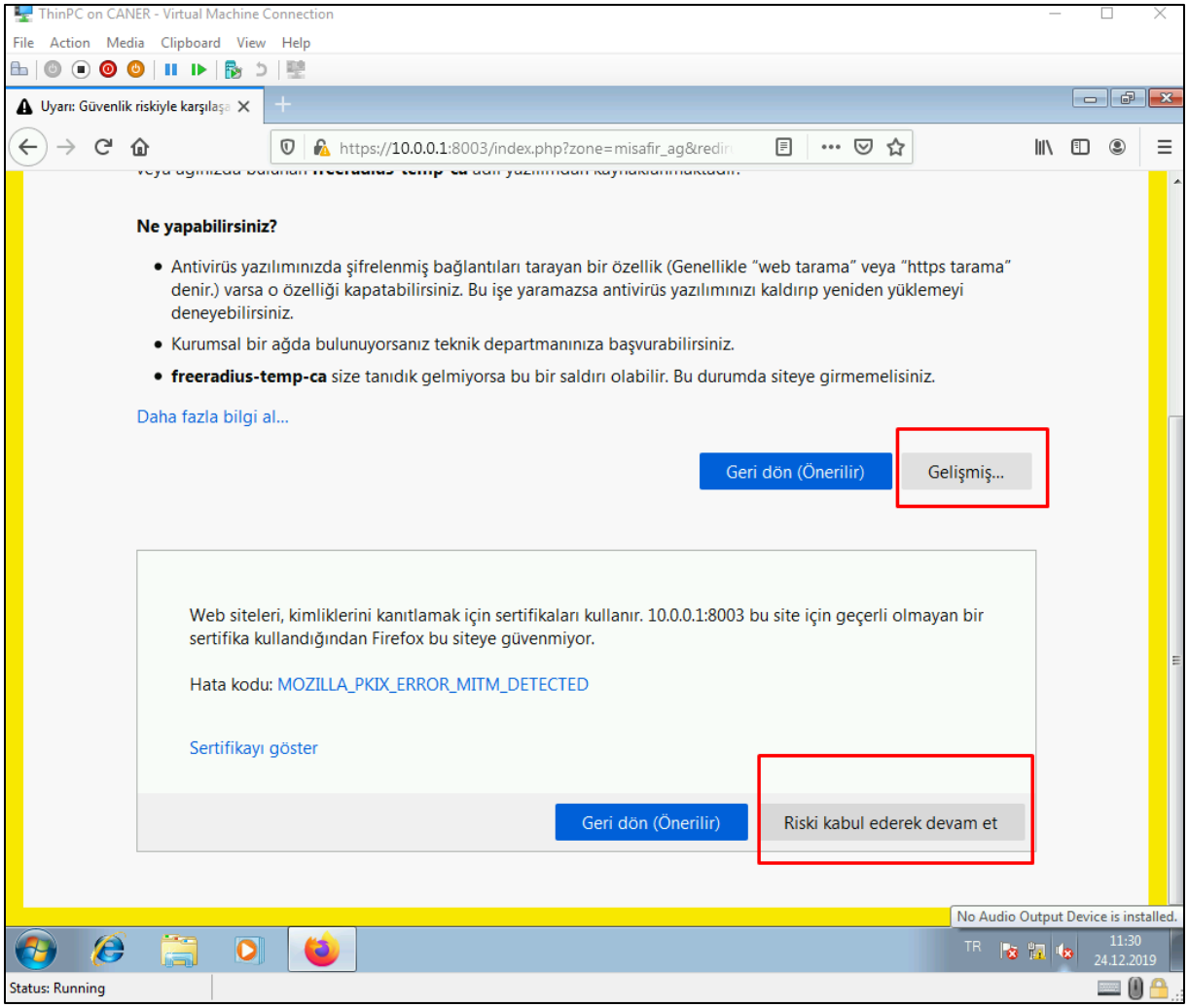
And, finally we enable HTTPS login with our NAS client's IP and FreeRADIUS Server Certificate for SSL. Once we save, our portal is working.



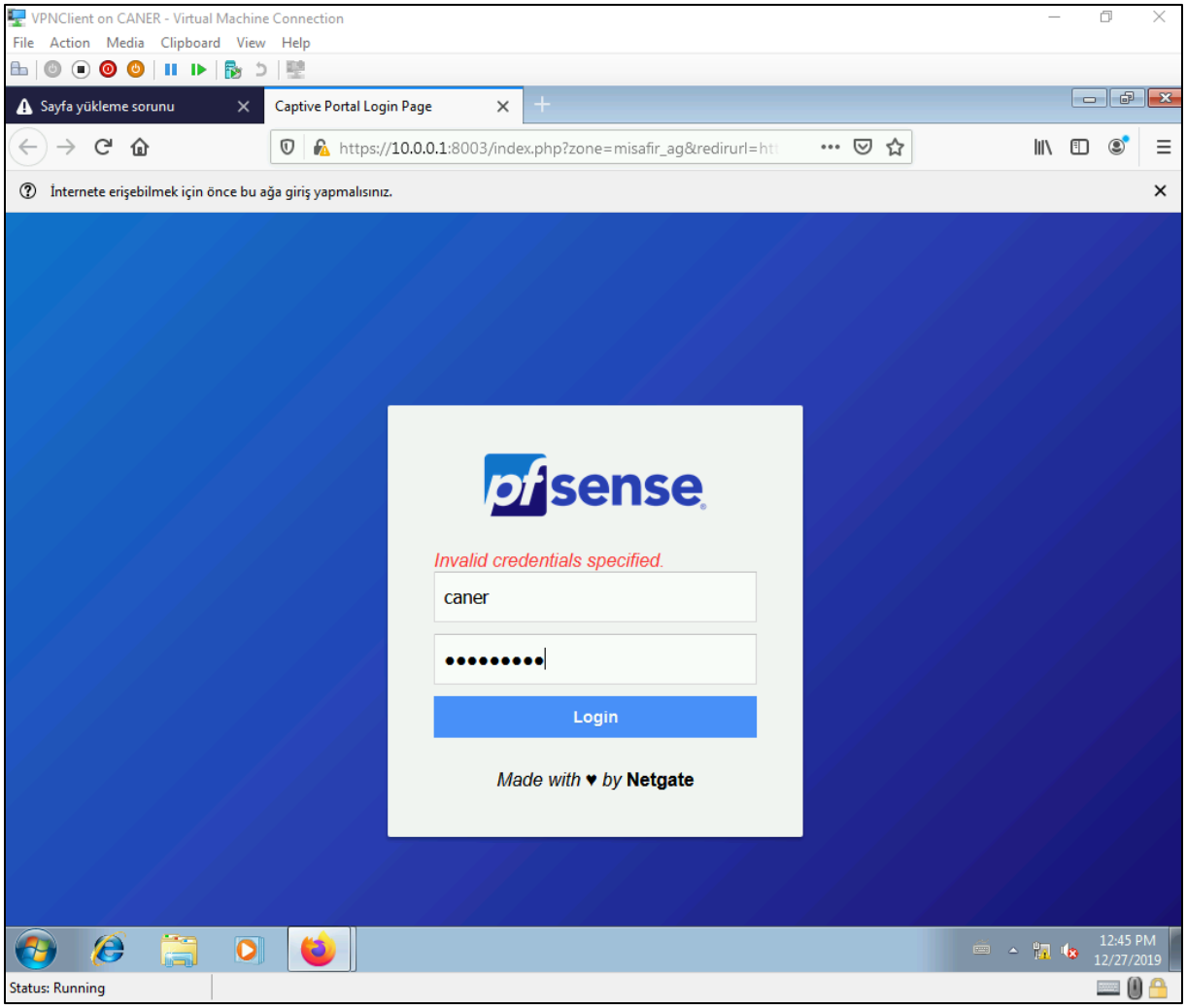
When we start the web browser and attempt to go anywhere, like perhaps youtube.com we are redirected to this page.



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

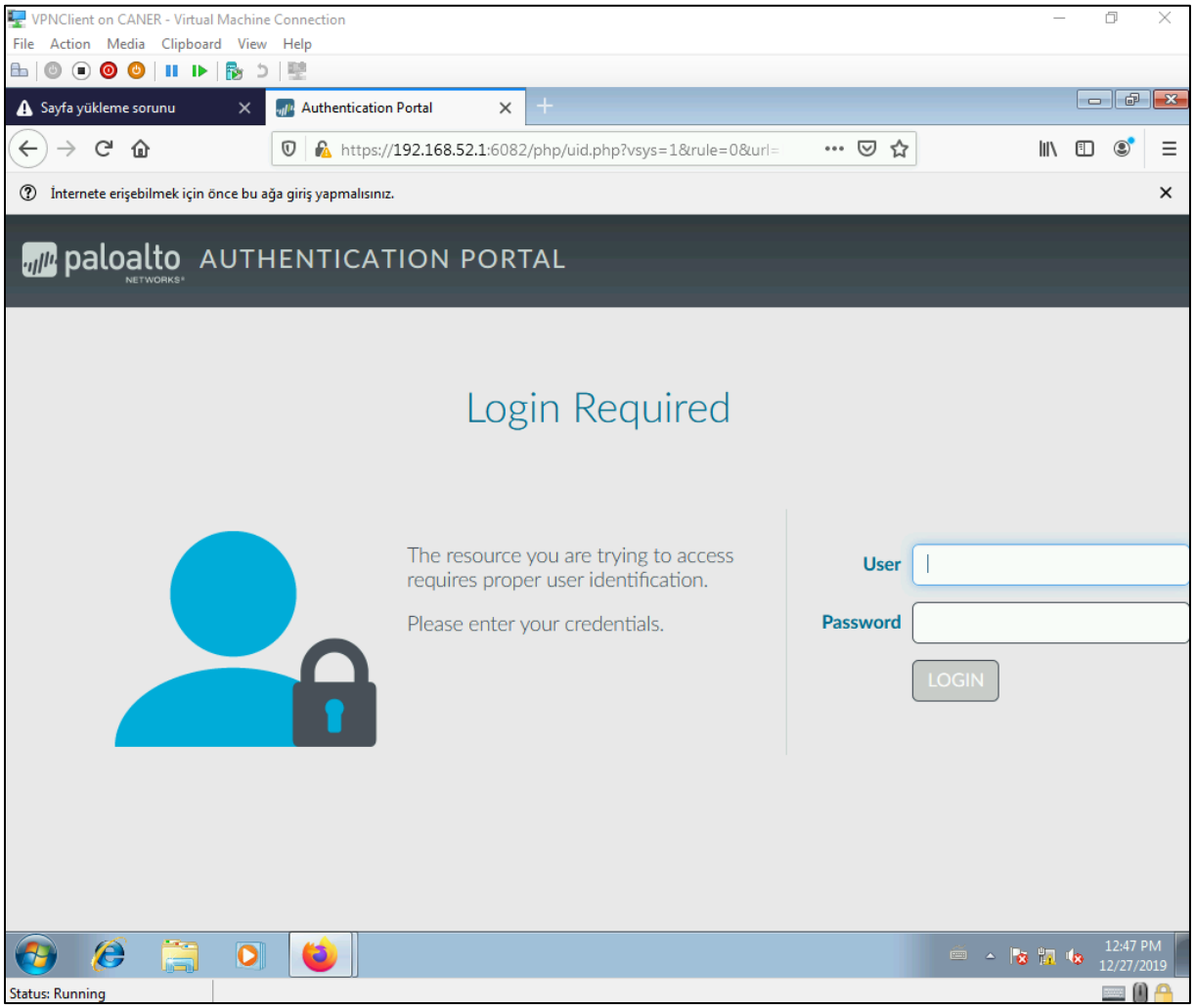


And we find ourselves at the default Captive Portal page.

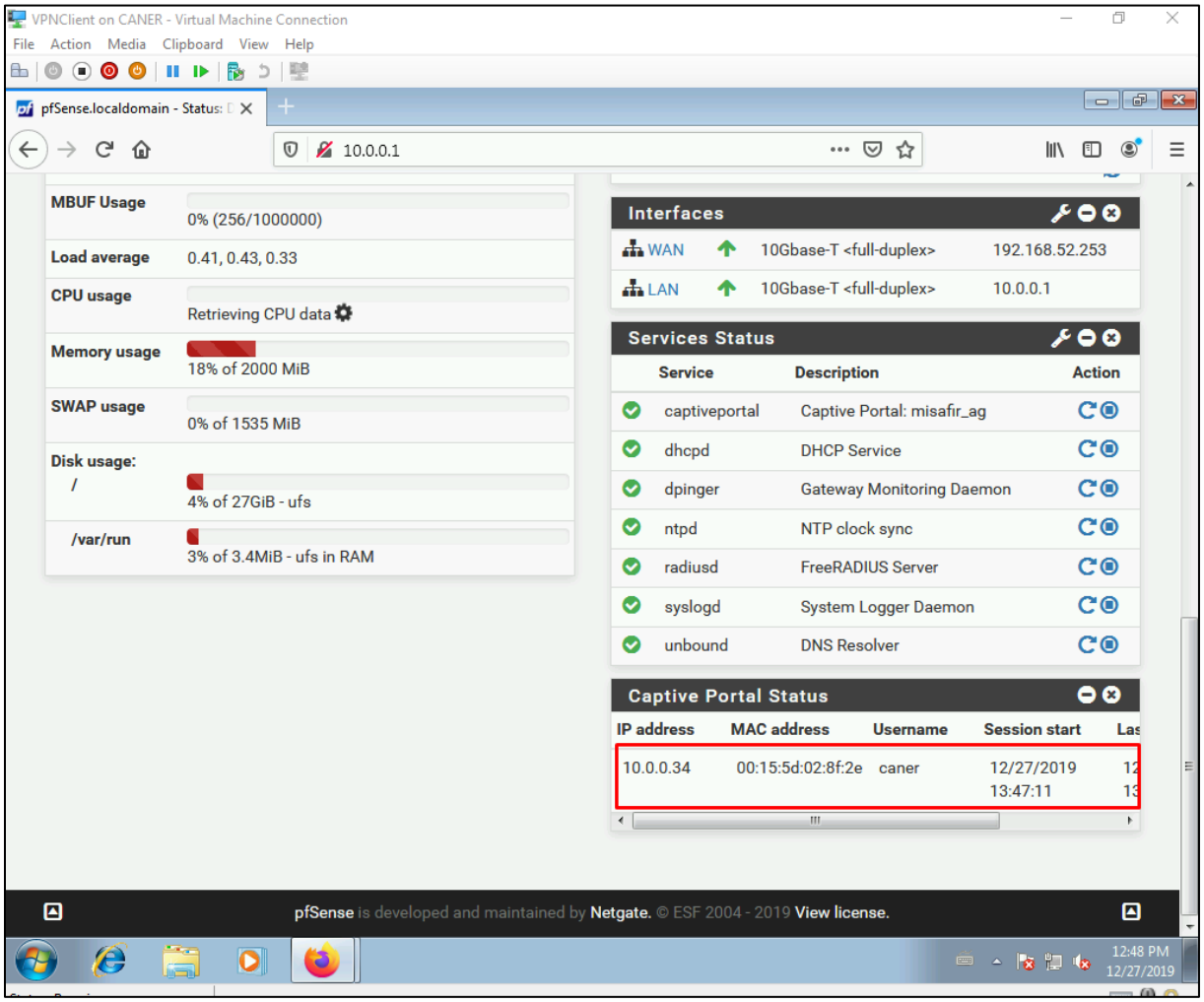


After we login using the previously set password…

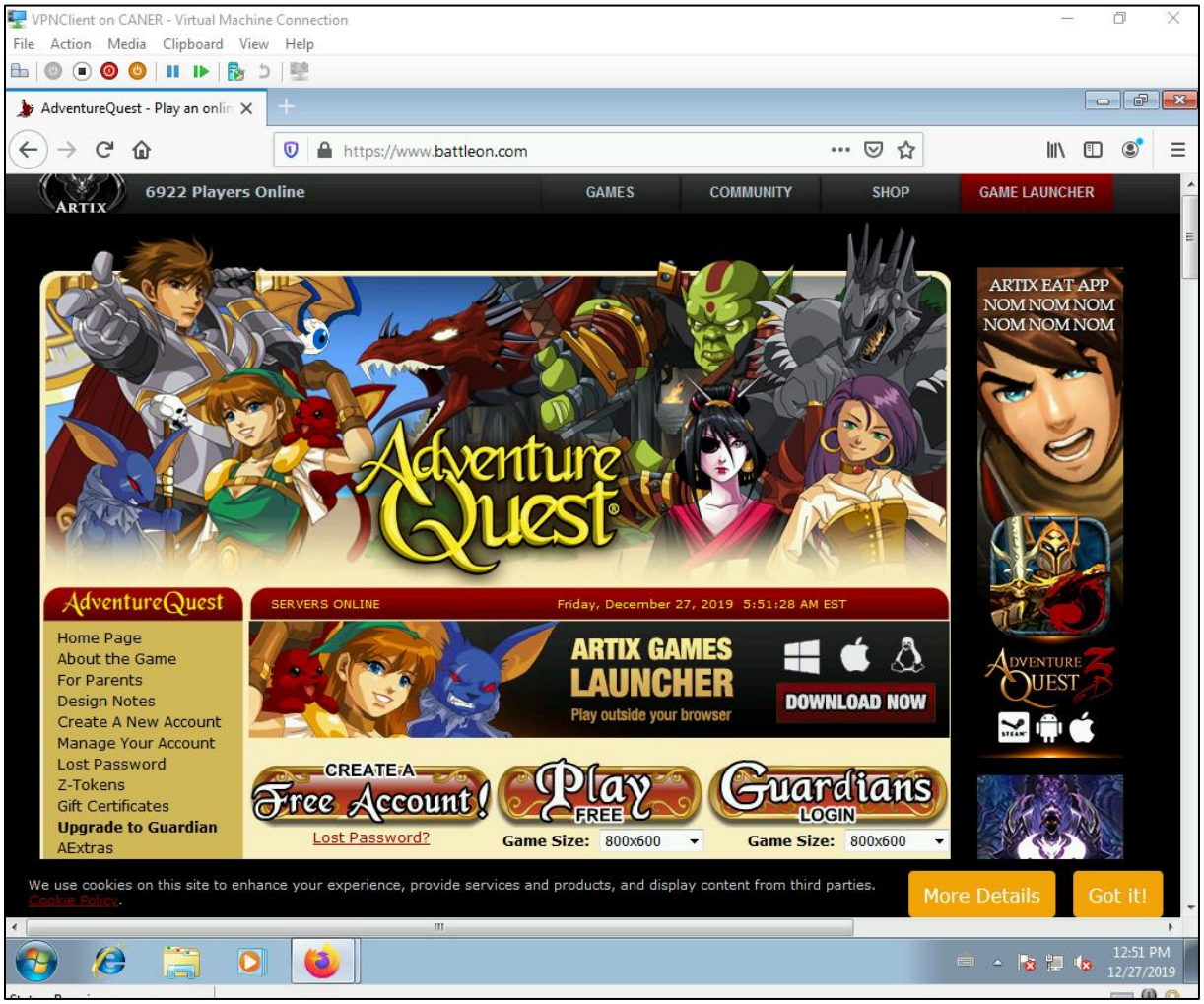
… we find ourselves at another Captive Portal. The one BAU uses for its own internal network but this means we basically accessed to the WAN interface of the firewall and reached the internet. To get to the actual youtube.com page we'd have to login to this portal as well but this is completely irrelevant.



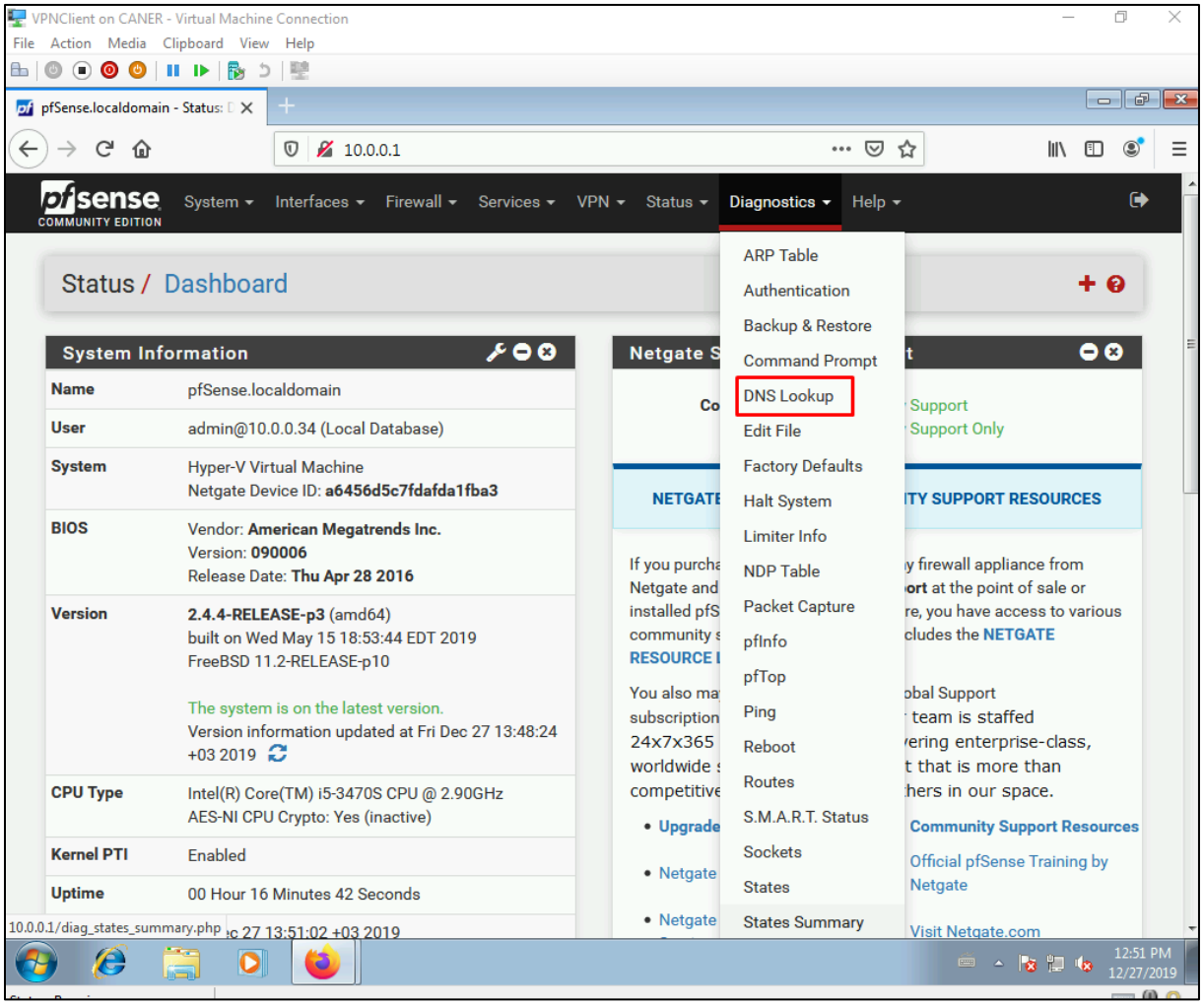
When we look at the Captive Portal Status from the pfSense dashboard we can see the information of our user logging in.



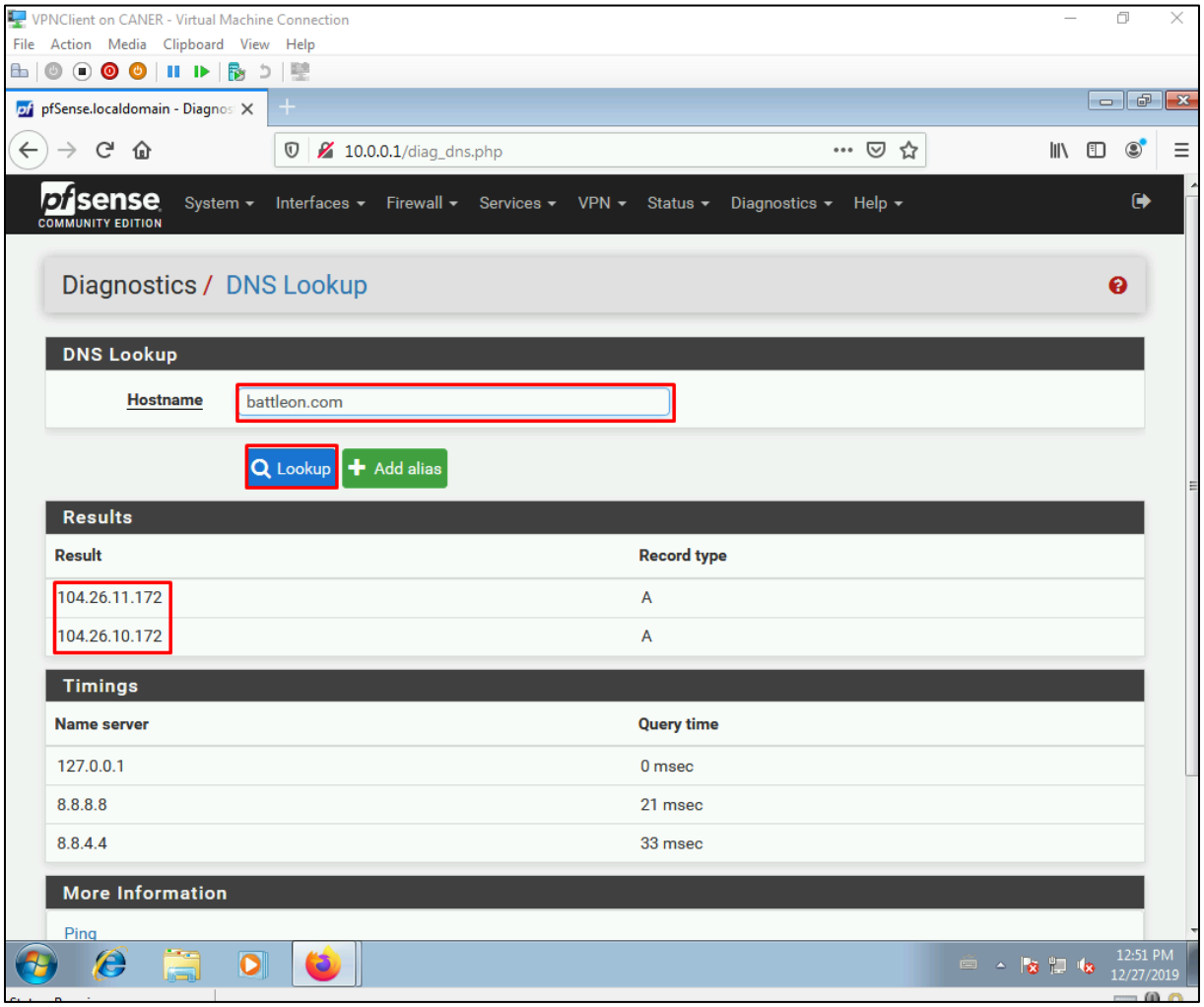
Now, let’s ban access to a specific website for our users. We decide to ban this online based game website so that our employees cannot play while at work.



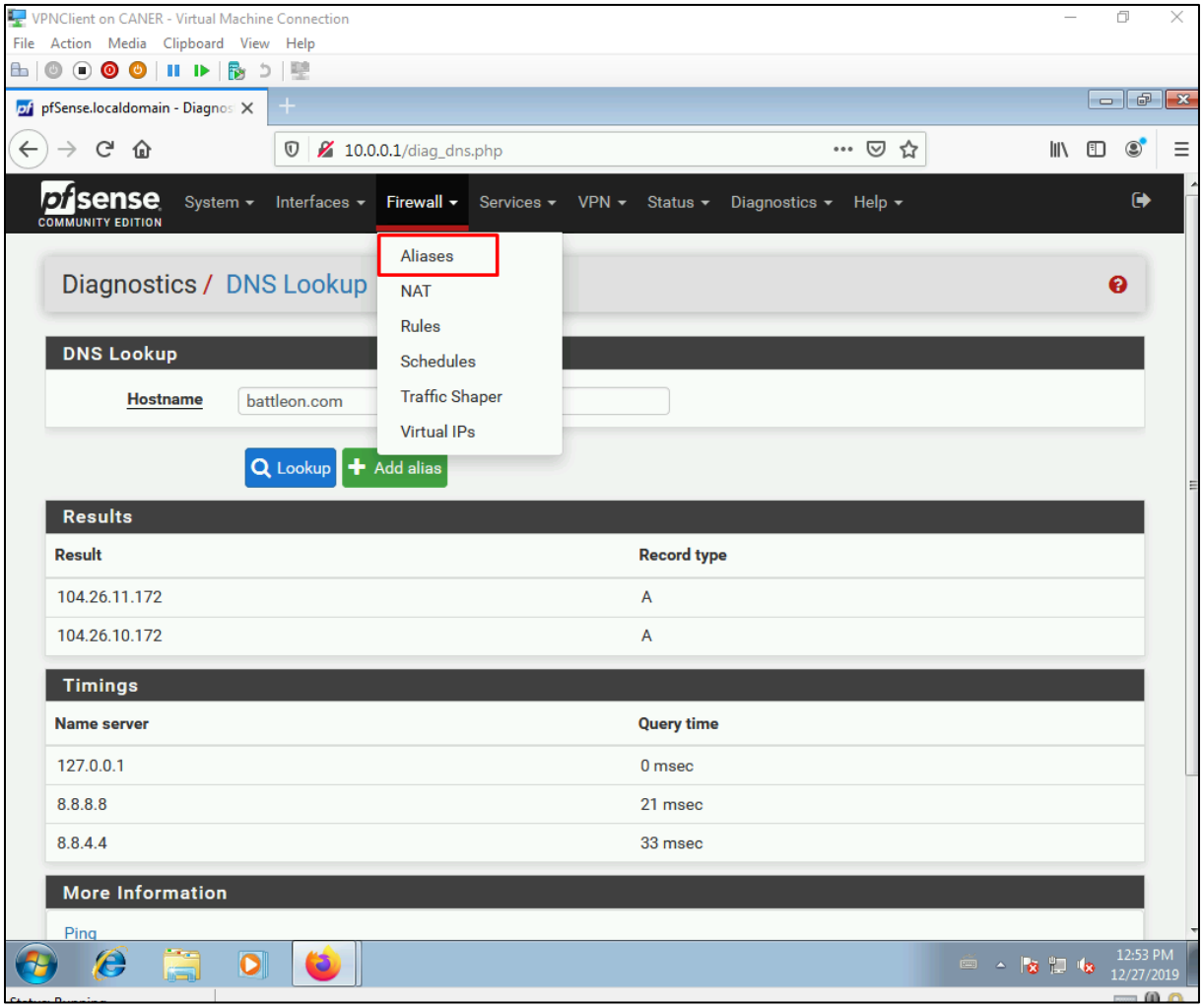
We first need to get to the DNS Lookup under Diagnostics.



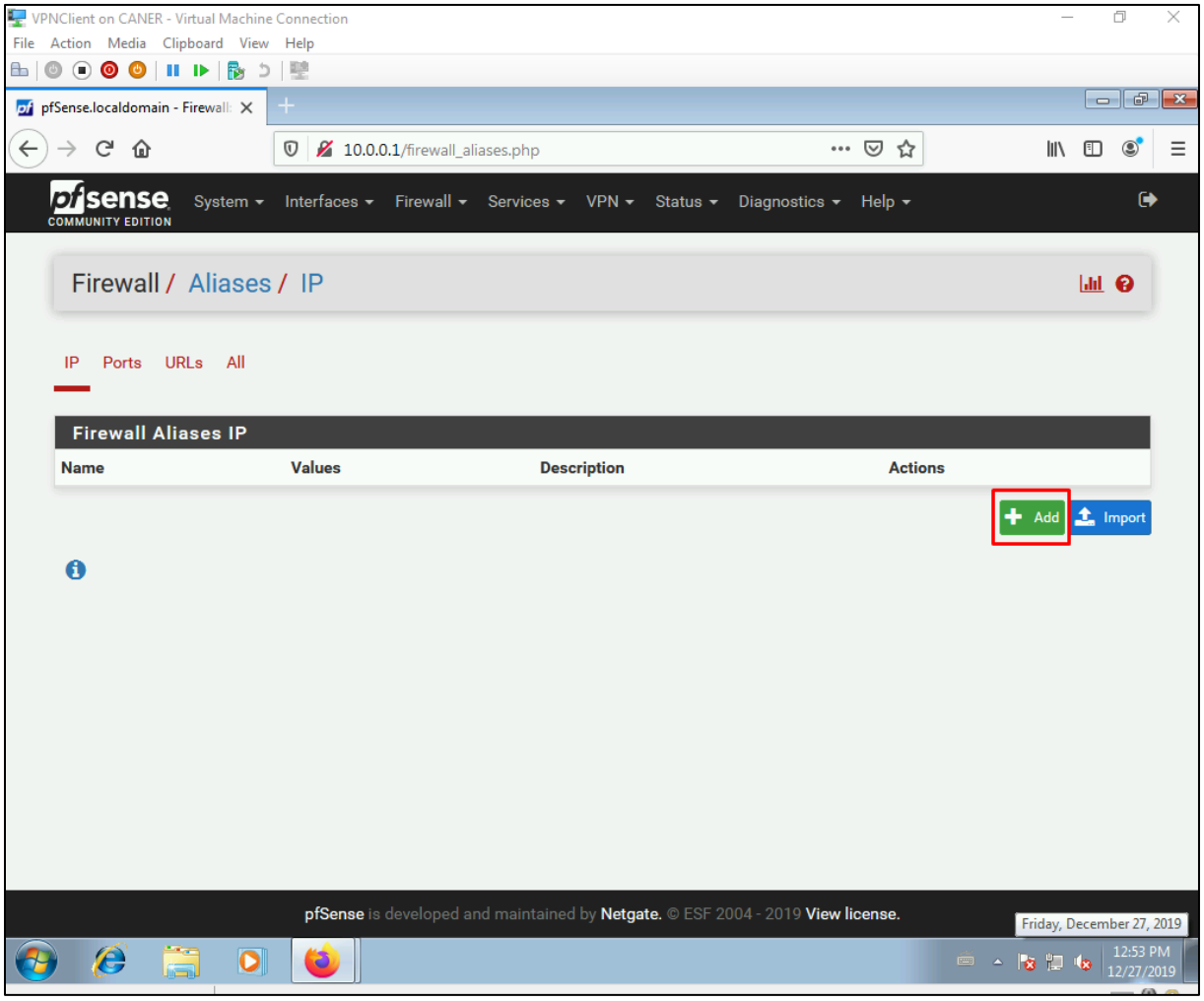
With the DNS Lookup we get the IP addresses of the website. Fortunately, it's not Facebook and it only has 2 IP addresses.



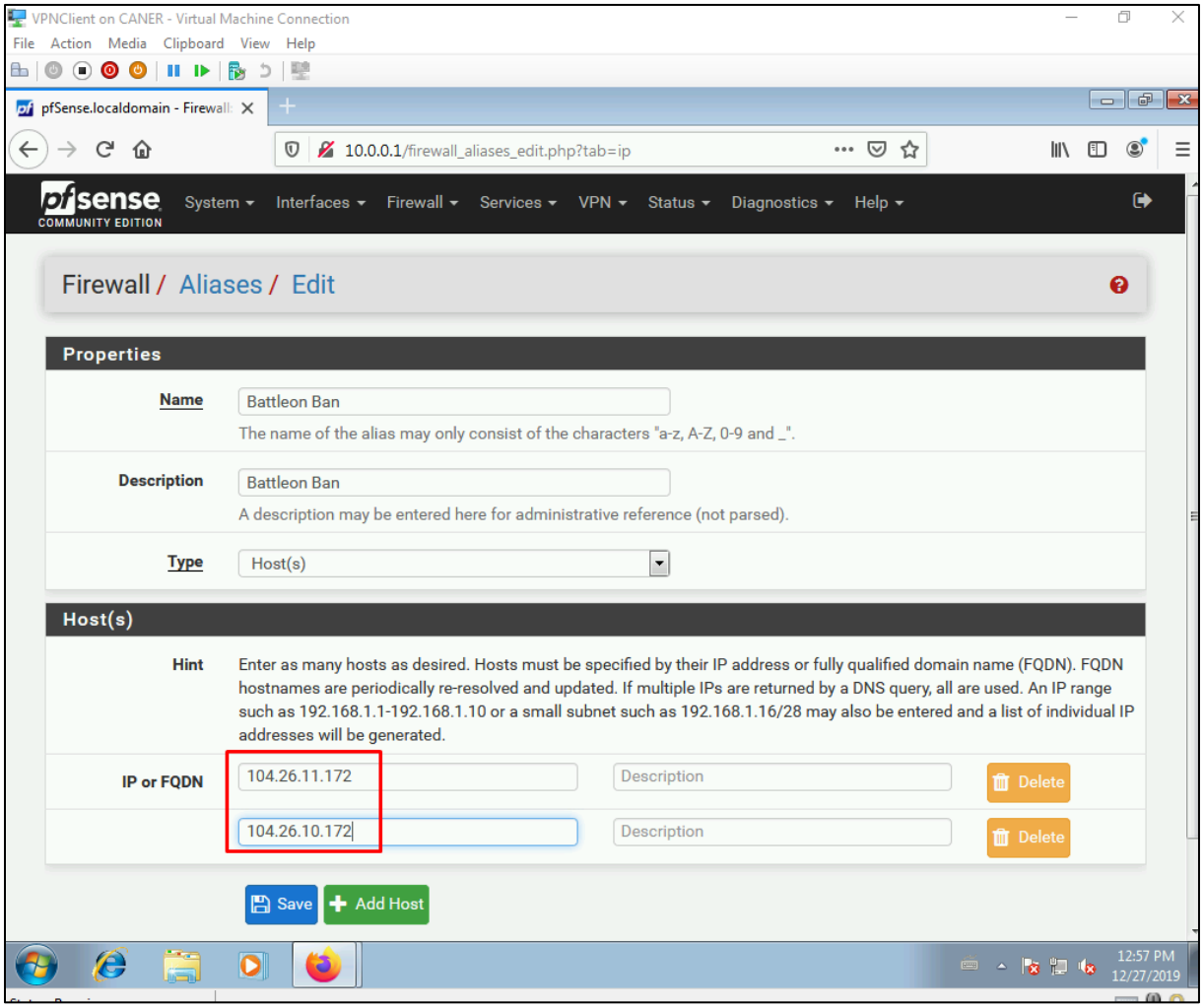
We go to Aliases under Firewall to create an alias.



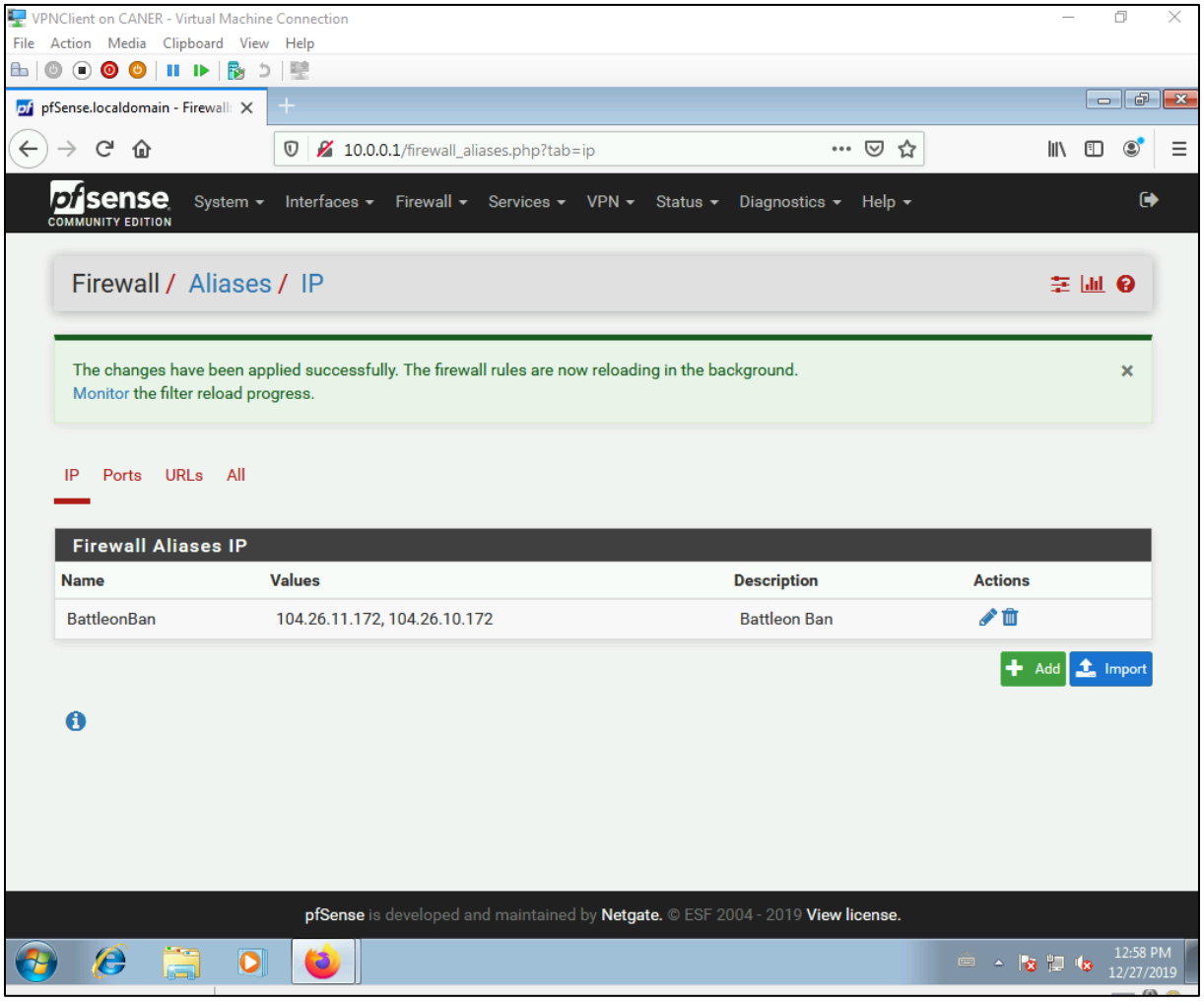
We create an alias for IPs.



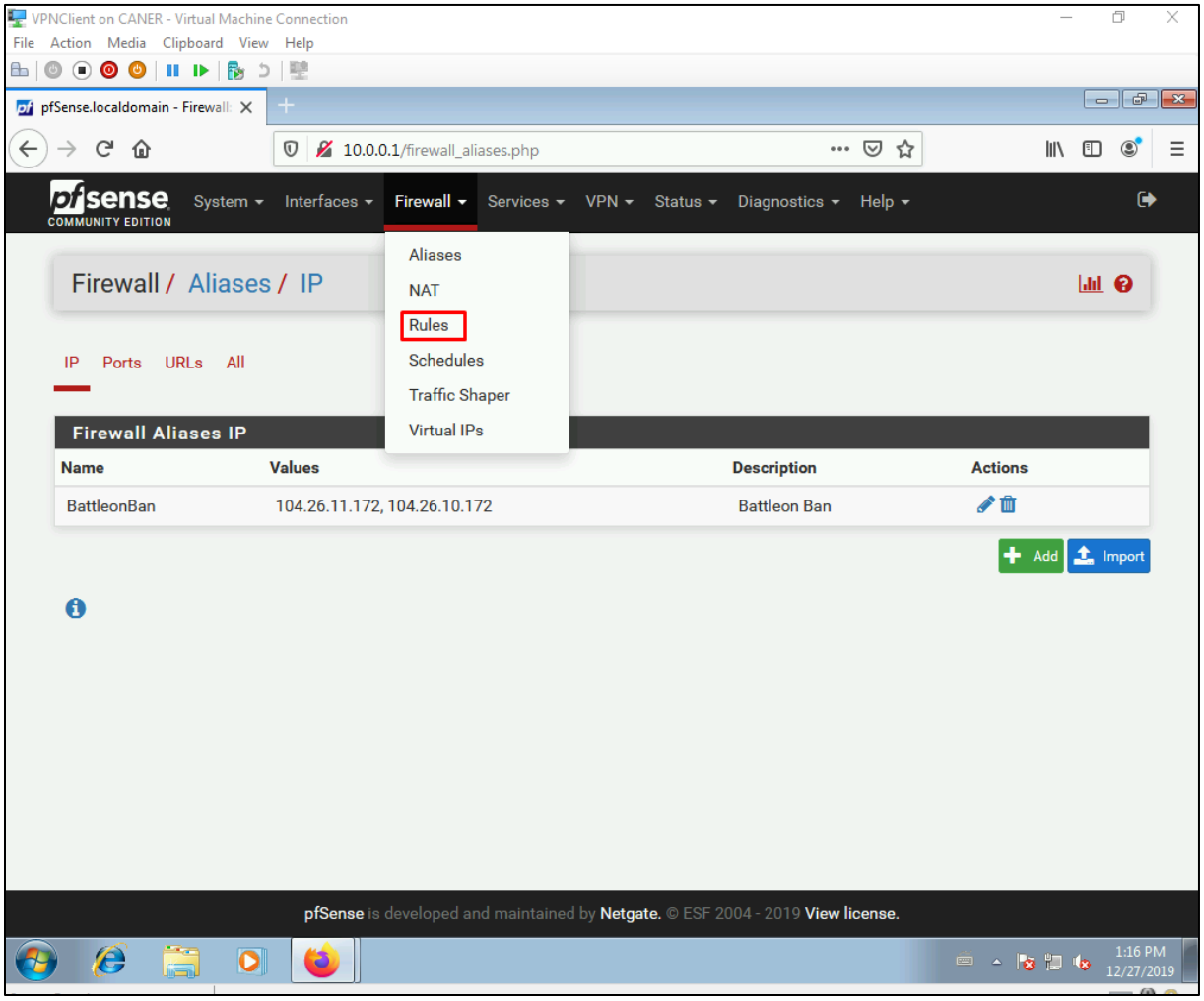
We name the alias and enter the website's IP addresses here.



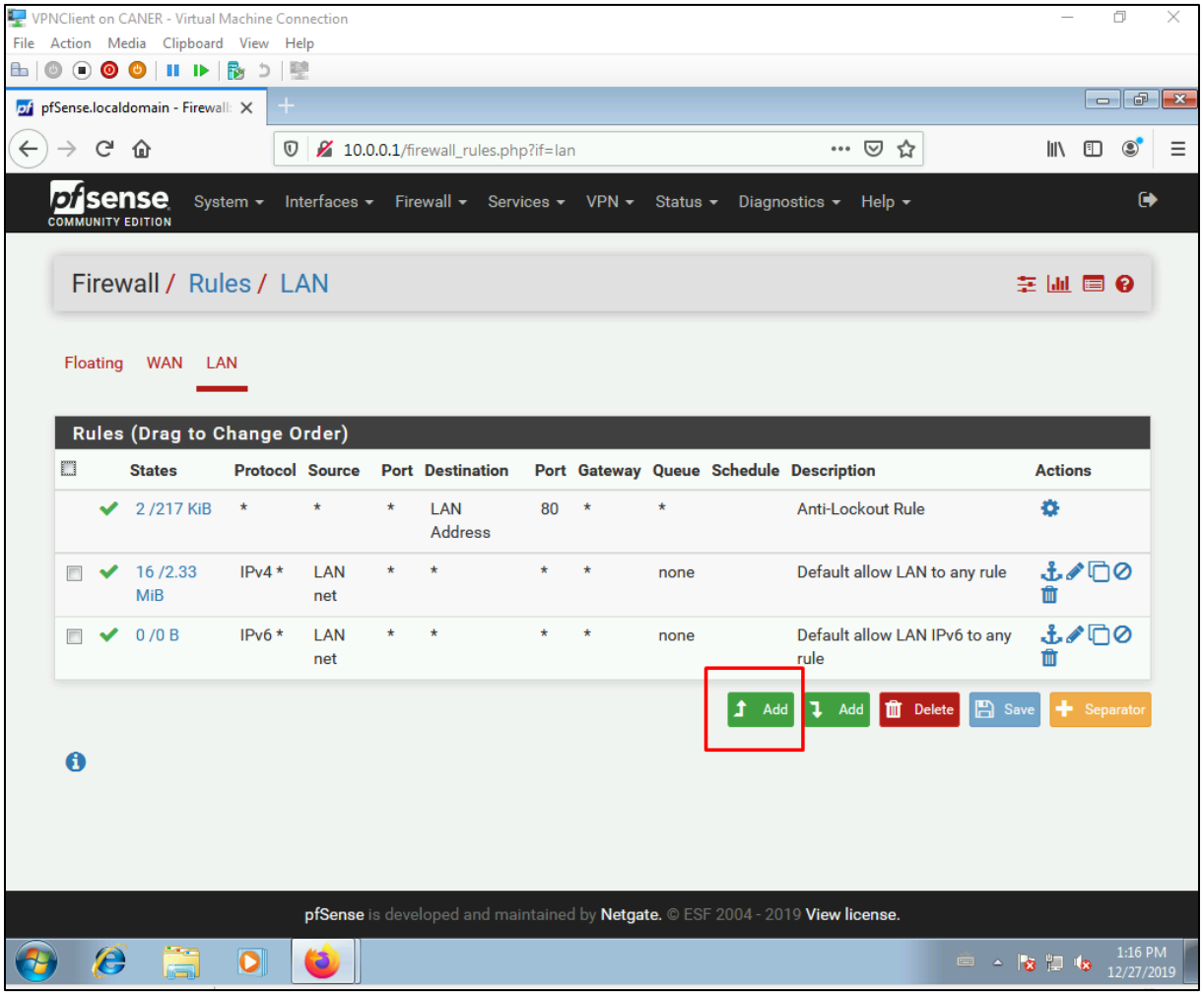
Once we save, we have an alias neatly named as BattleOnBan.



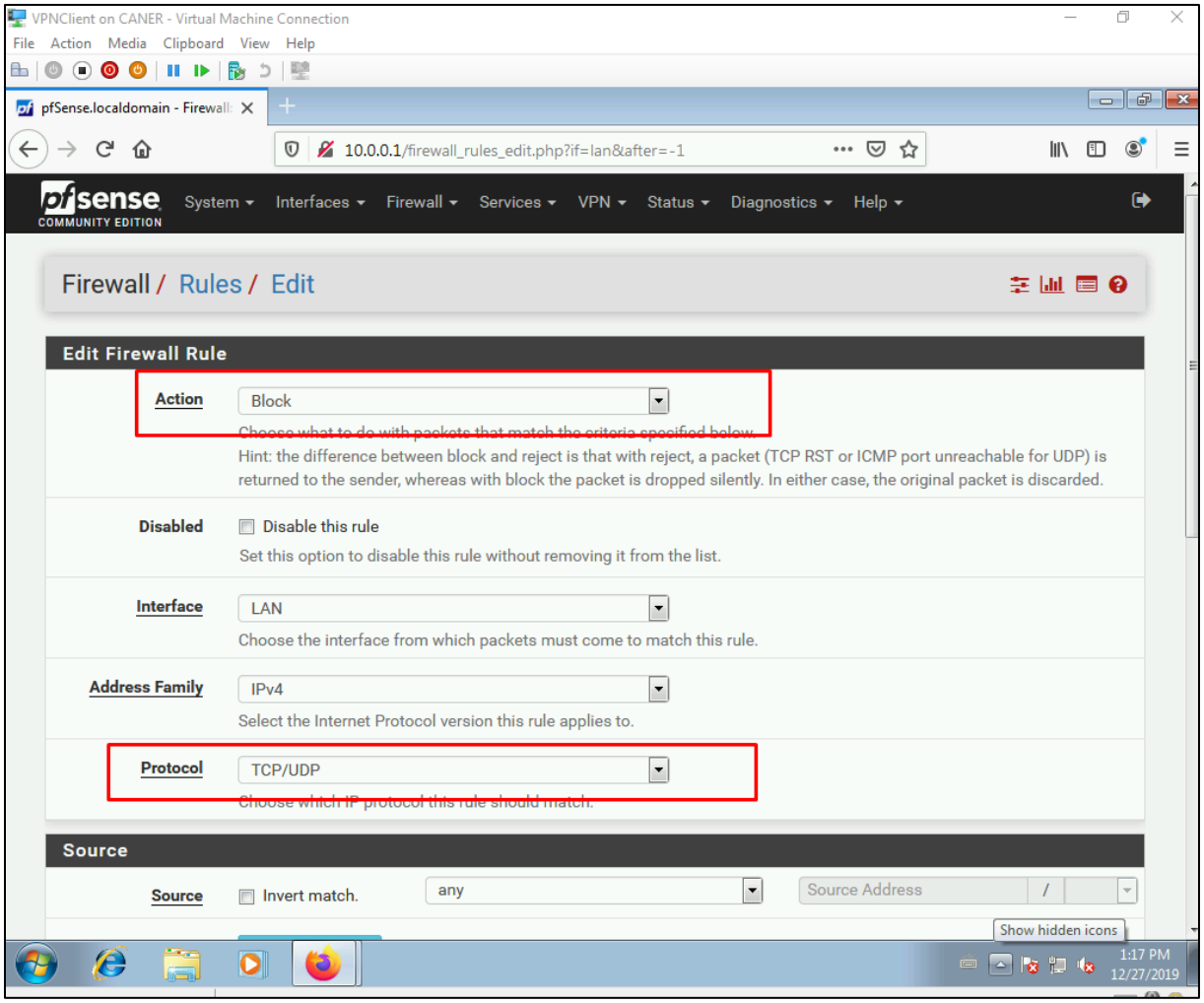
Now, we get to the Rules under Firewall.



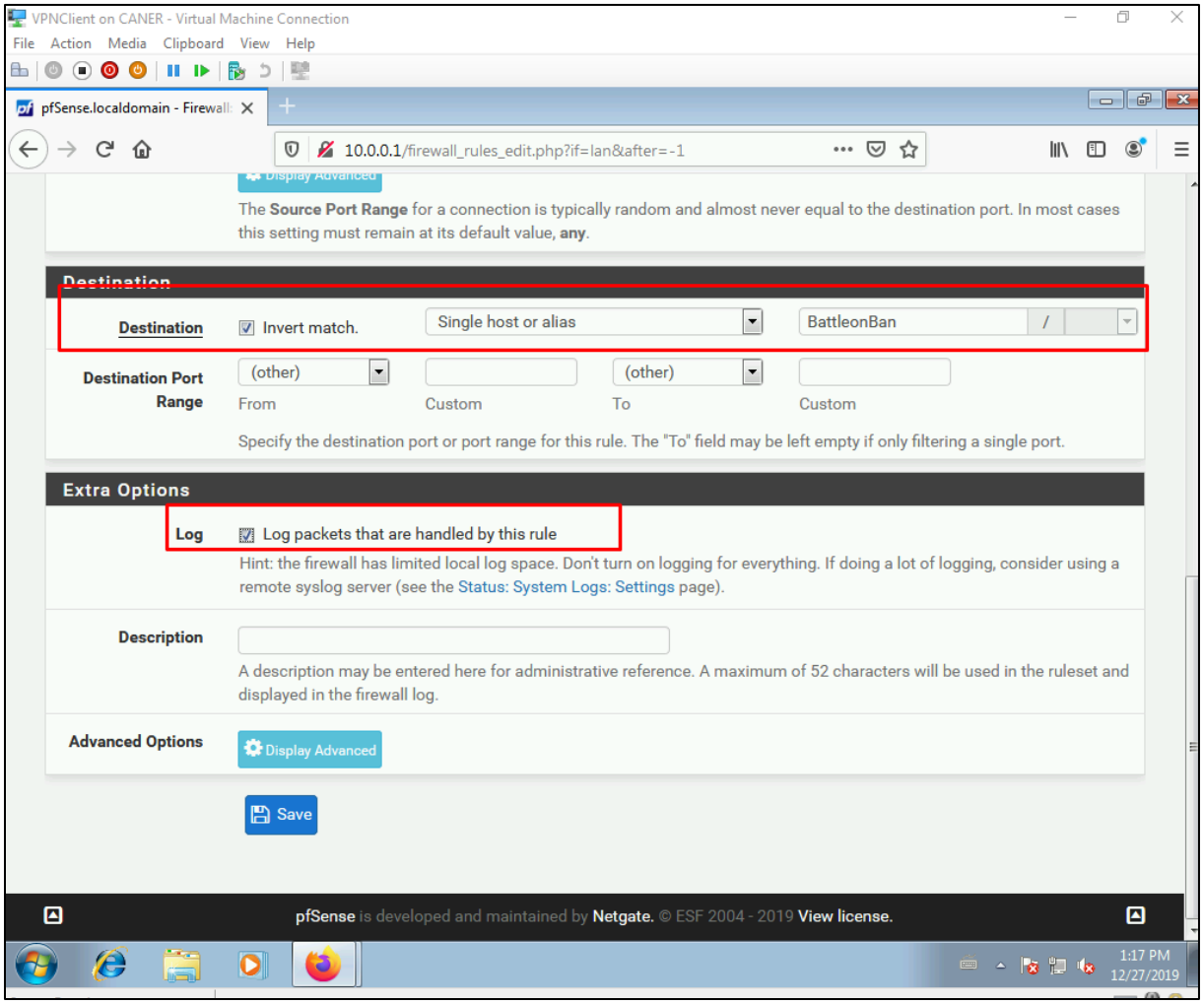
We create a new rule.



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

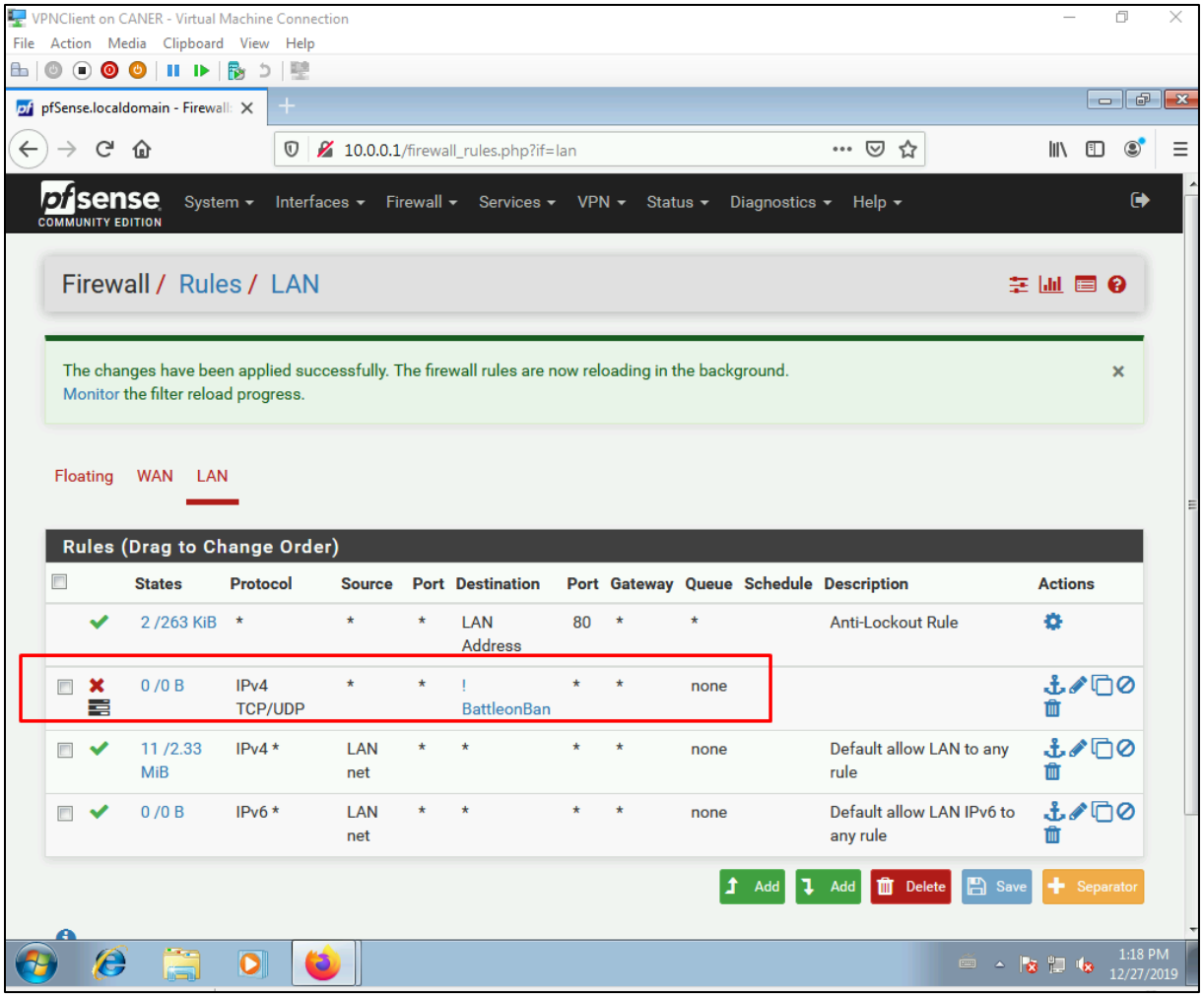


… to BattleOn.com's IP addresses as displayed by the alias.

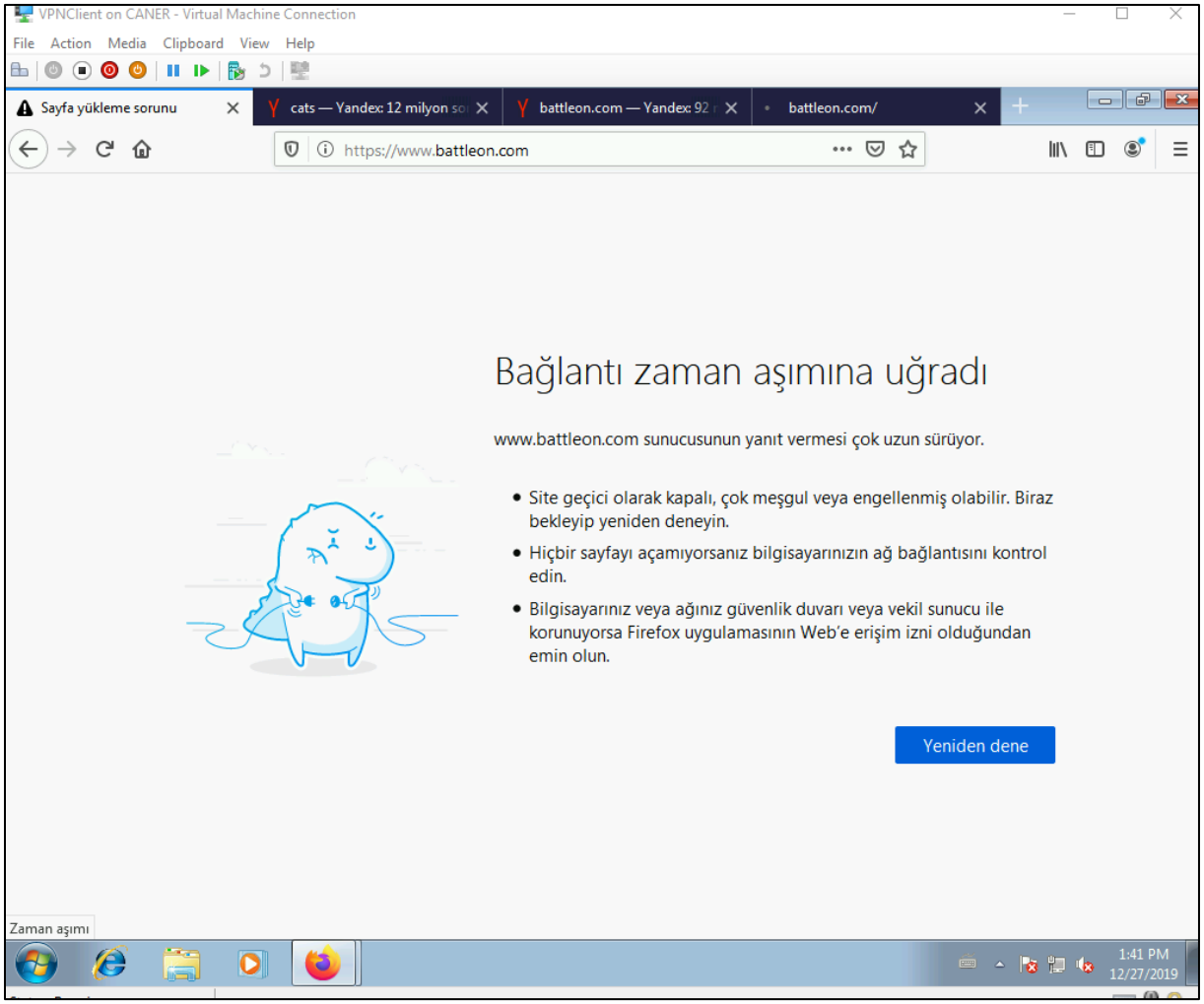


We also take a log of anyone attempting to log into the banned website so that we can reprimand those employees if necessary.

Now the rule is set.

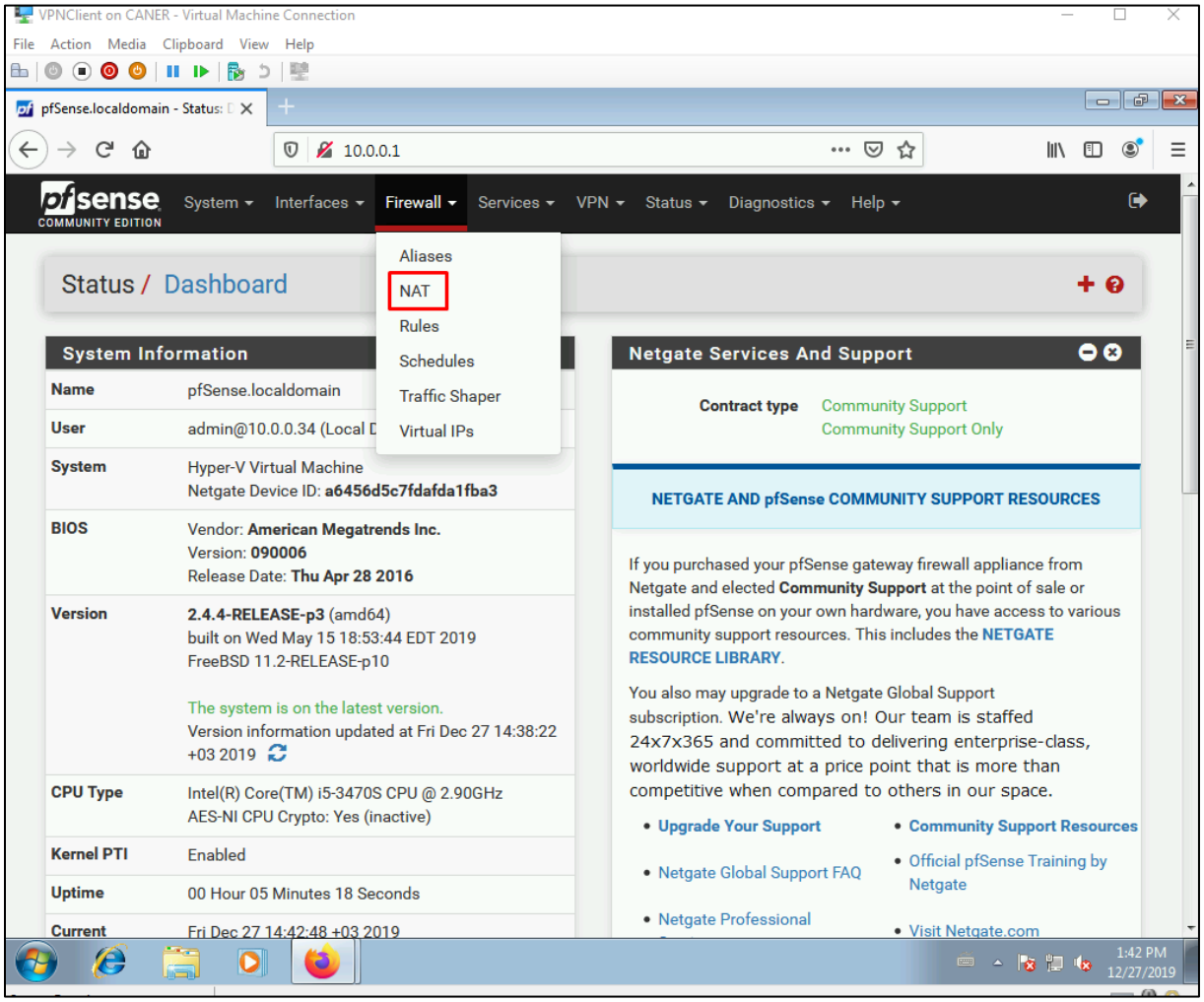


Now, when we try to play the game, we cannot connect.

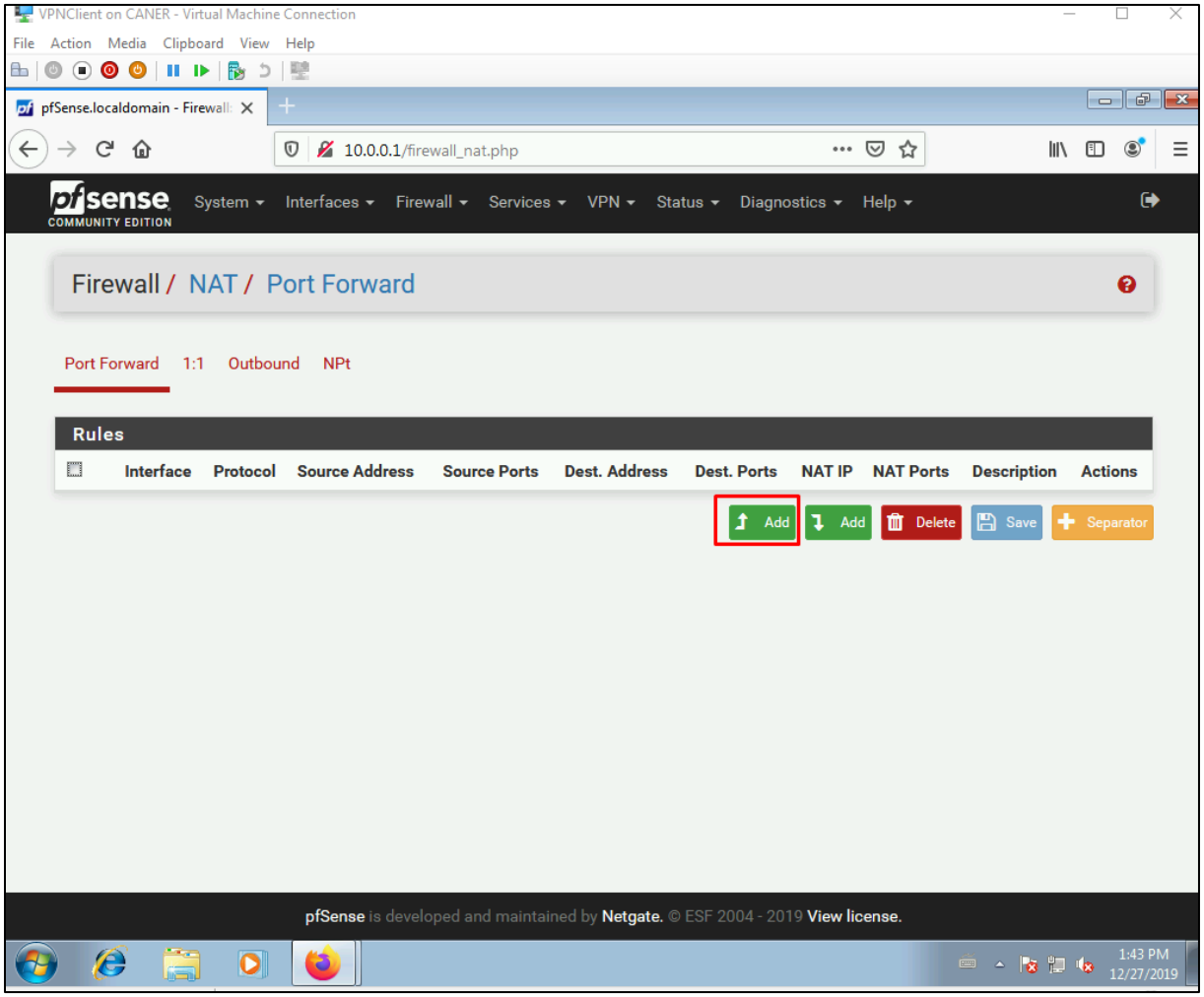


This ends the captive portal demonstration.

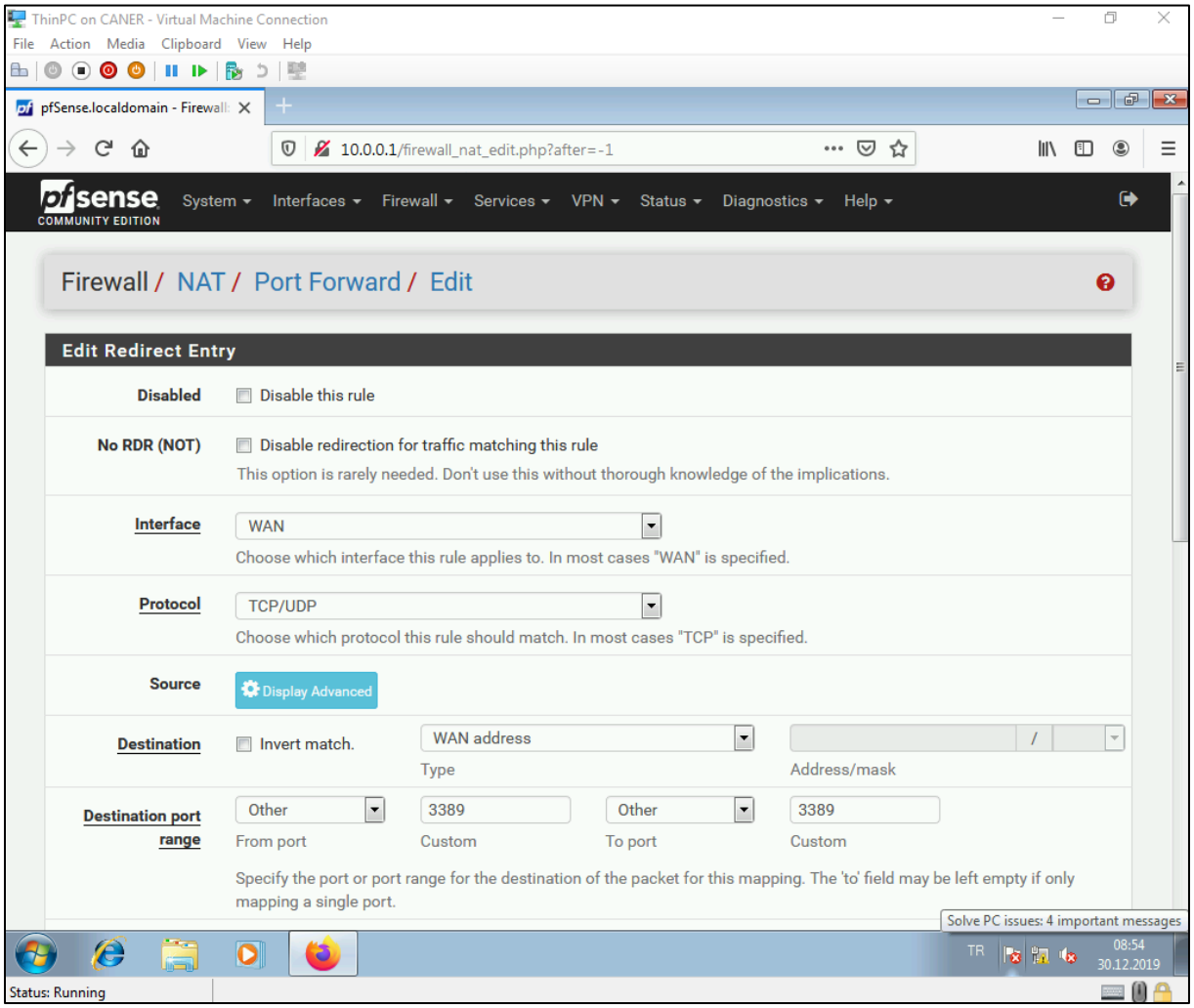
Now let’s do an example of port forwarding and remotely connect to the internal PC. First, we need to get to NAT settings.



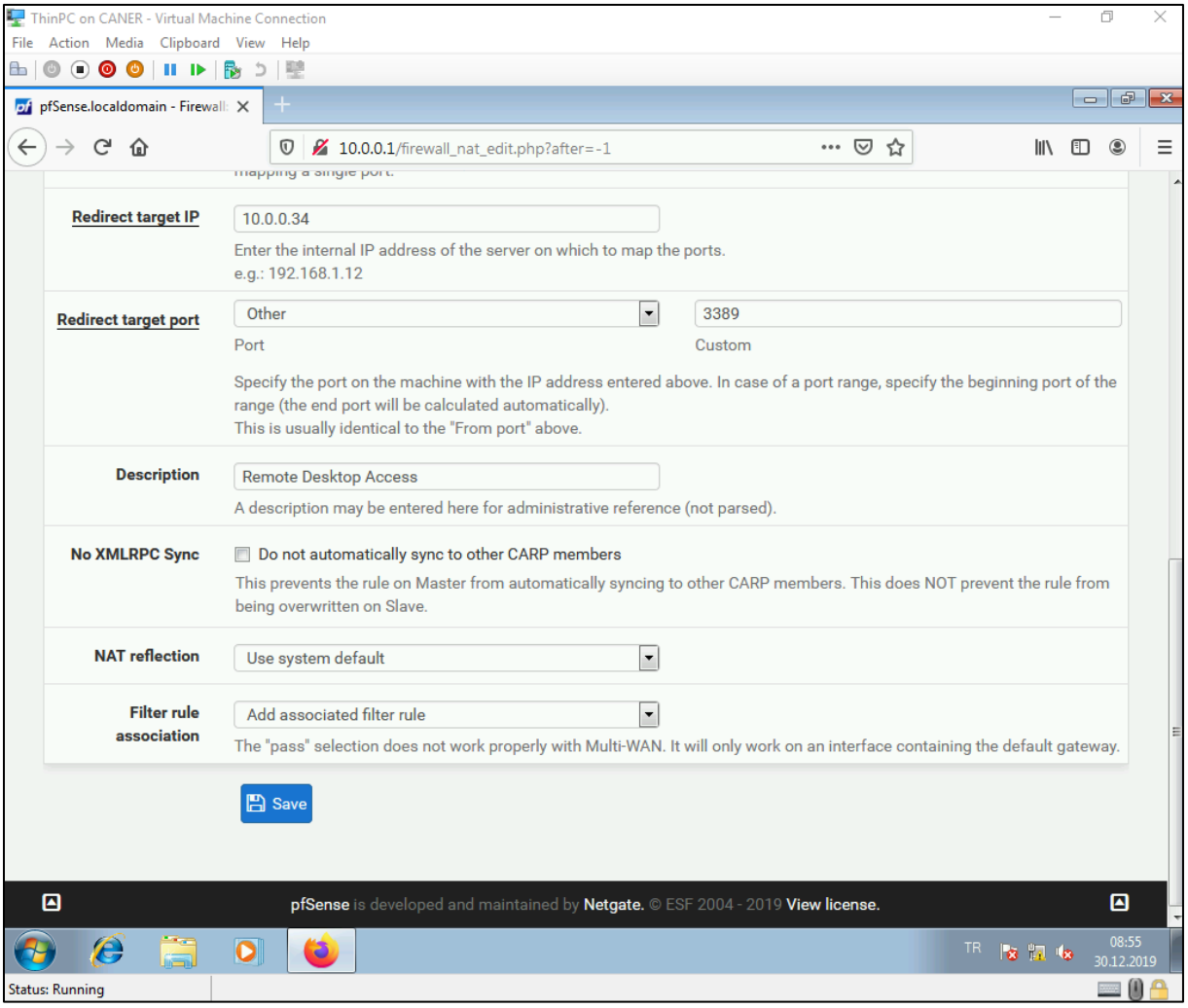
We then, add a new Port Forwarding rule.



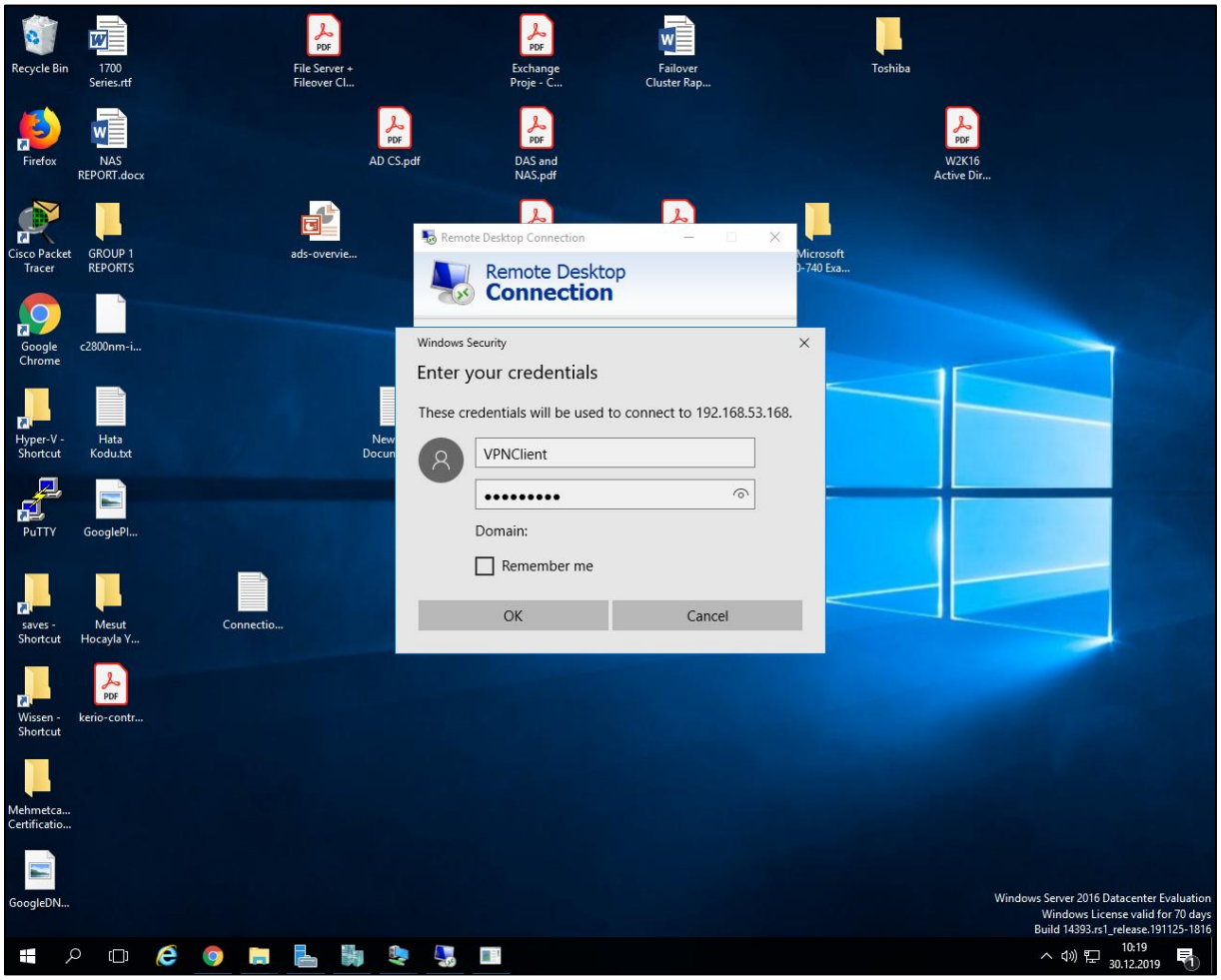
We choose the interface as WAN, protocols at both TCP and UDP, write 3389 for destination port to allow Remote Desktop …



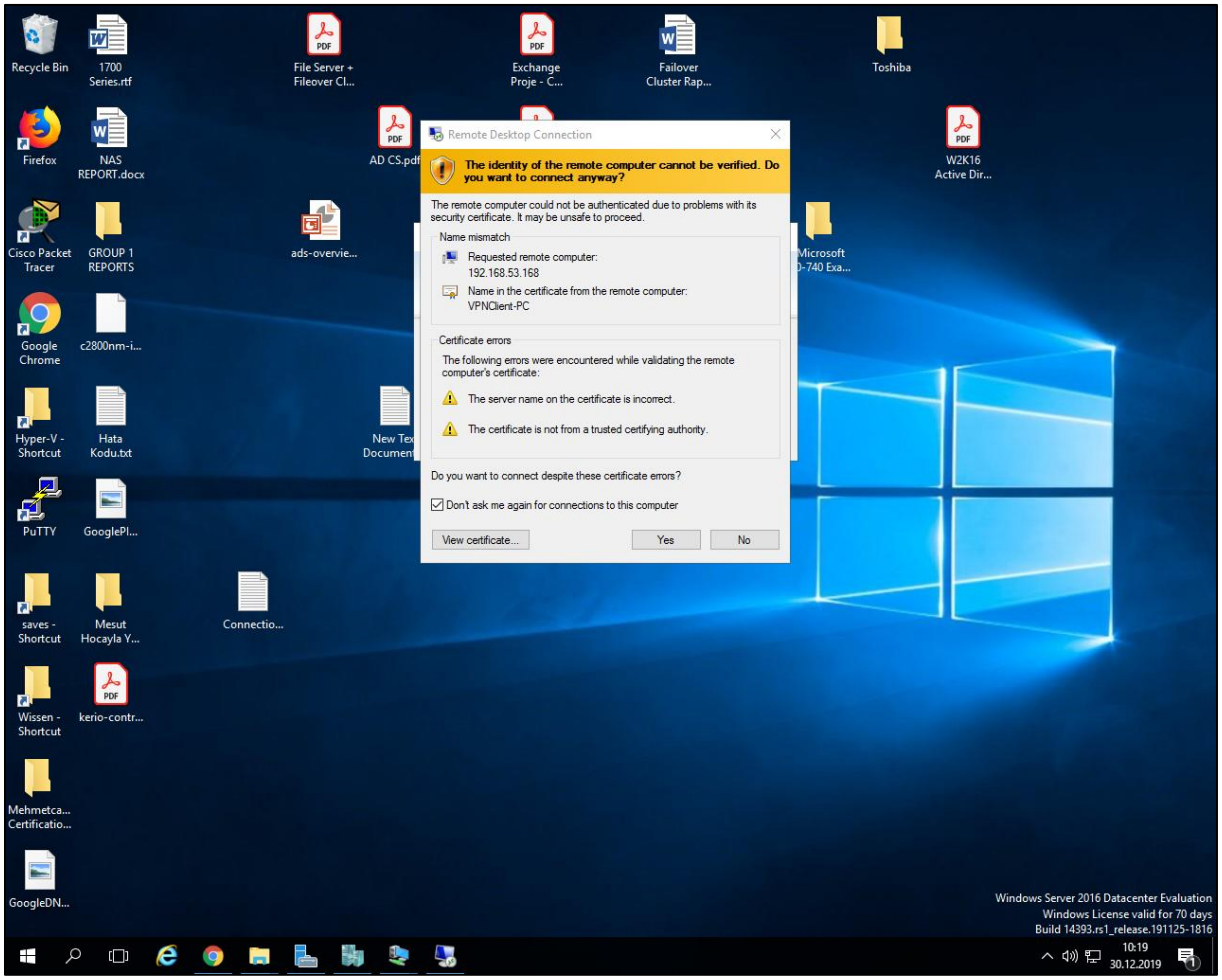
… and enter the IP address of the server we want to forward the Remote Desktop request to.



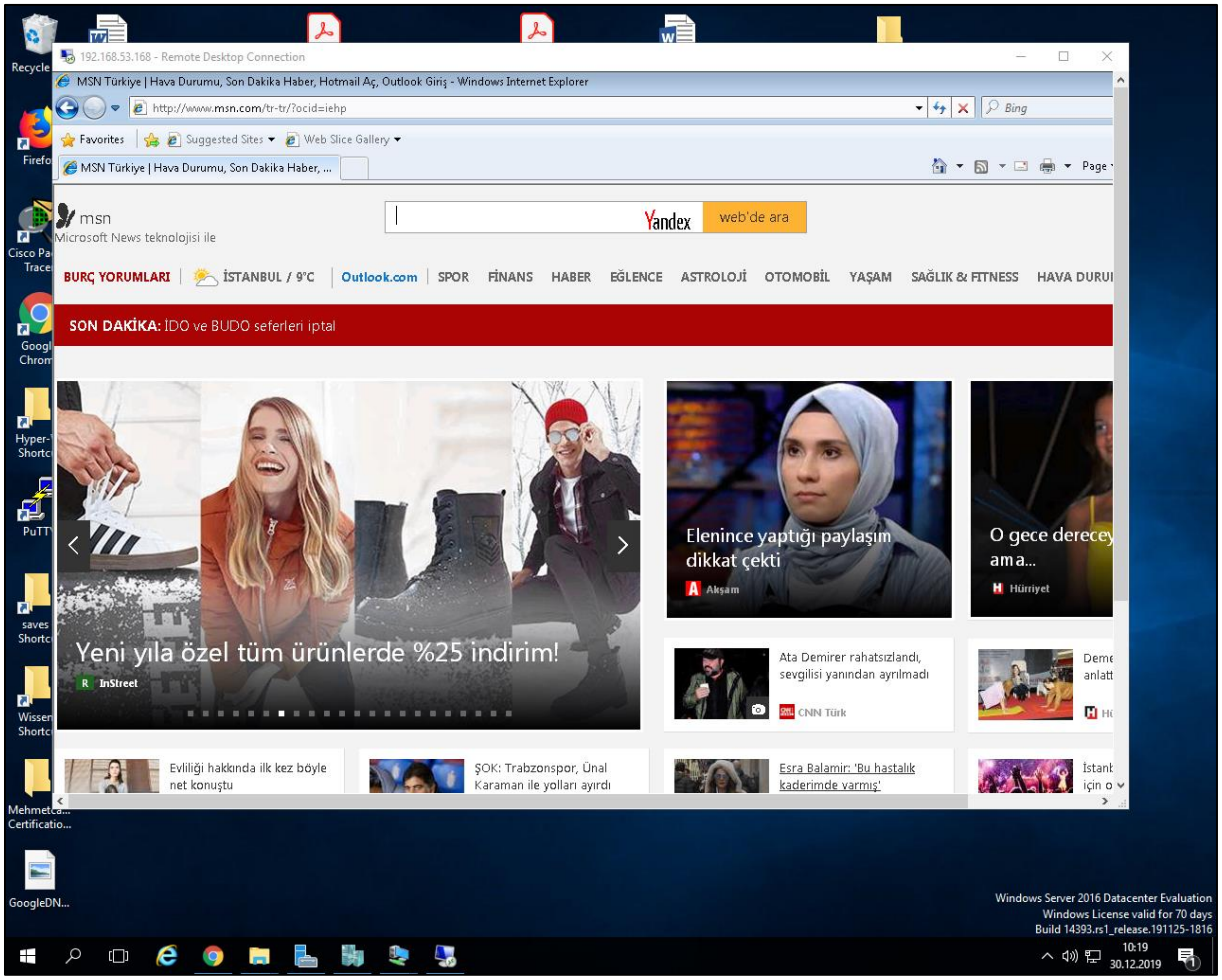
Then, when we enter the WAN address of the Firewall to connect via Remote Desktop, we get to log in as an account on the server that we specified.



A confirmation page pops up.



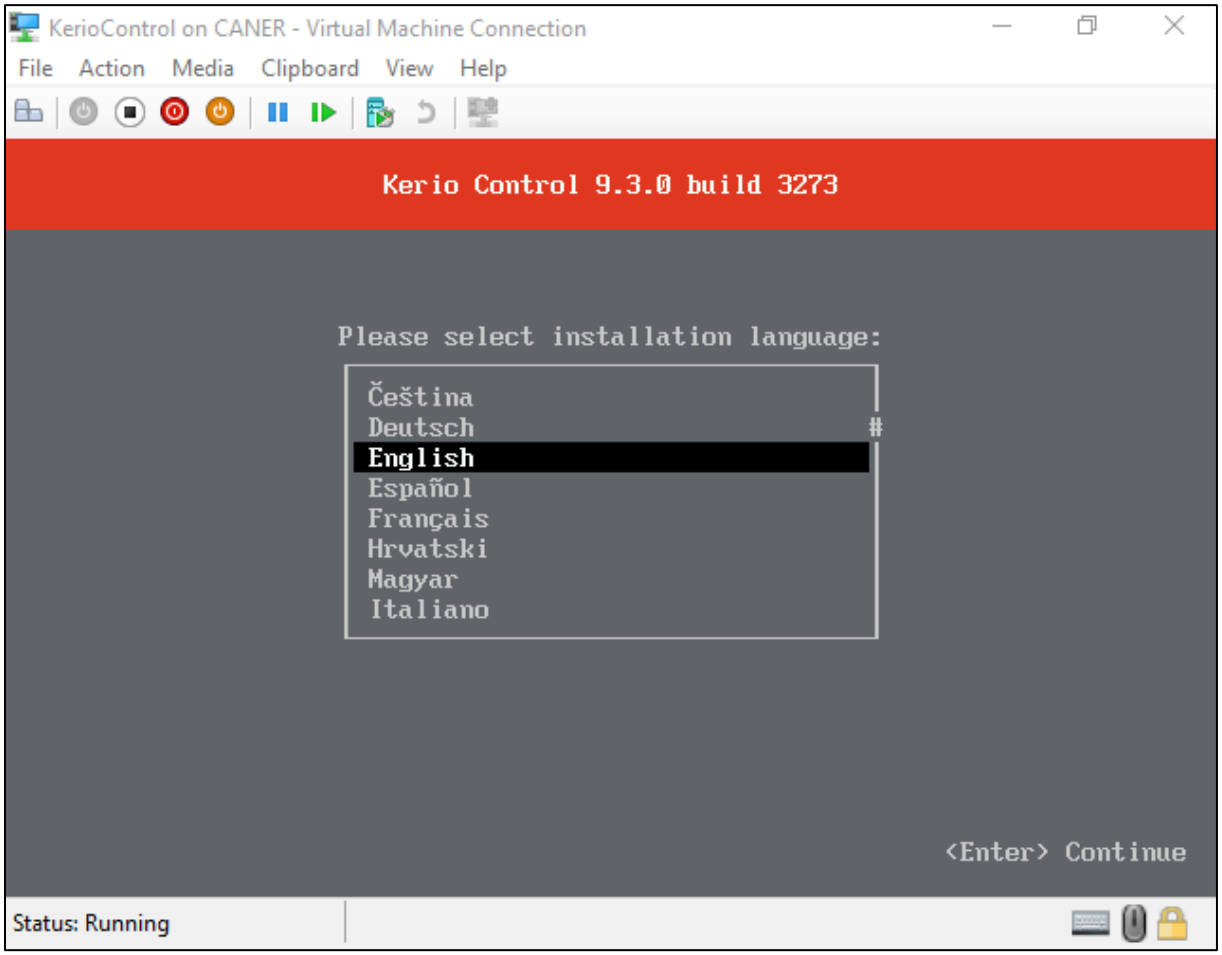
And then, we’re in.



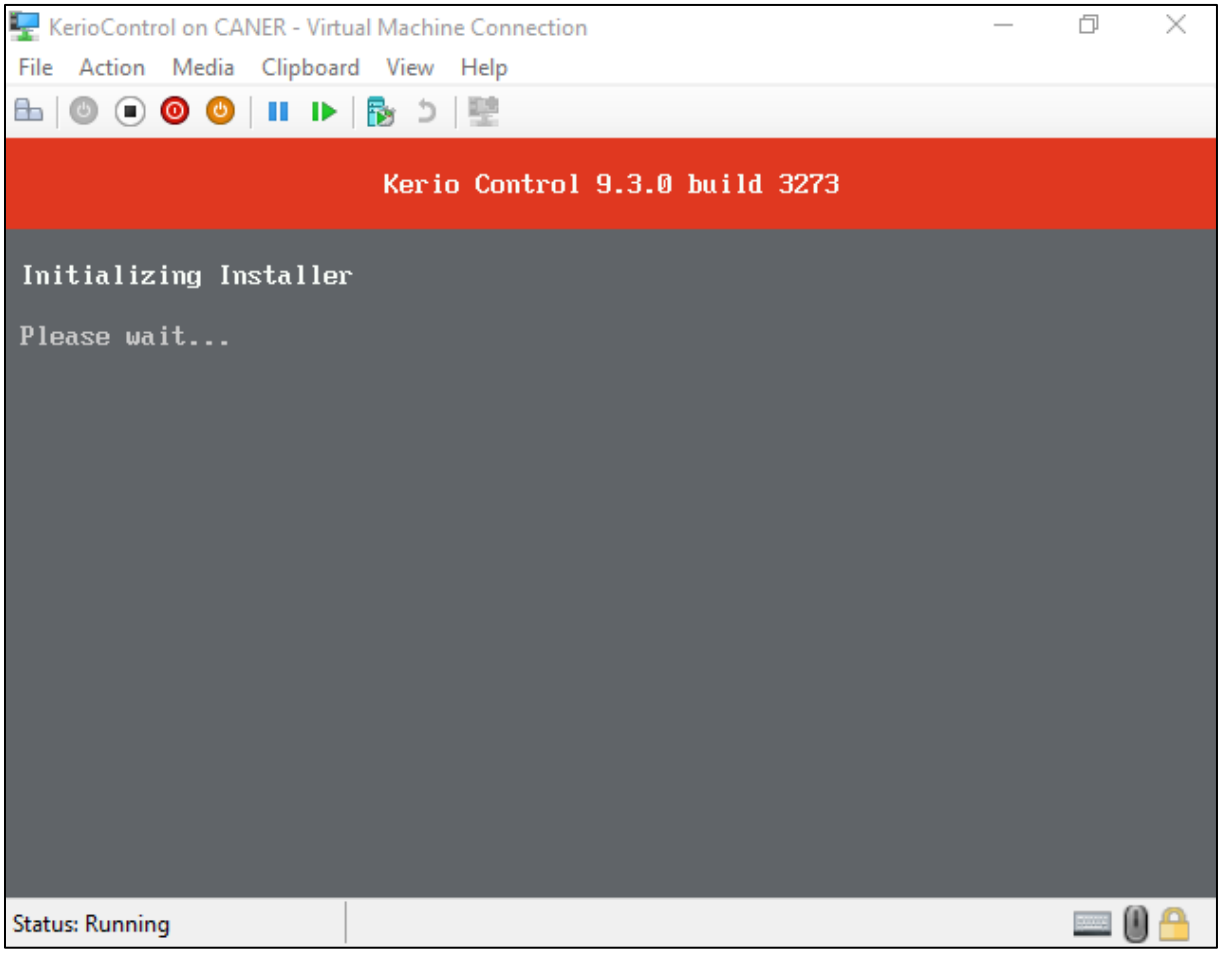
This finishes the pfSense part of this project.

2) Kerio

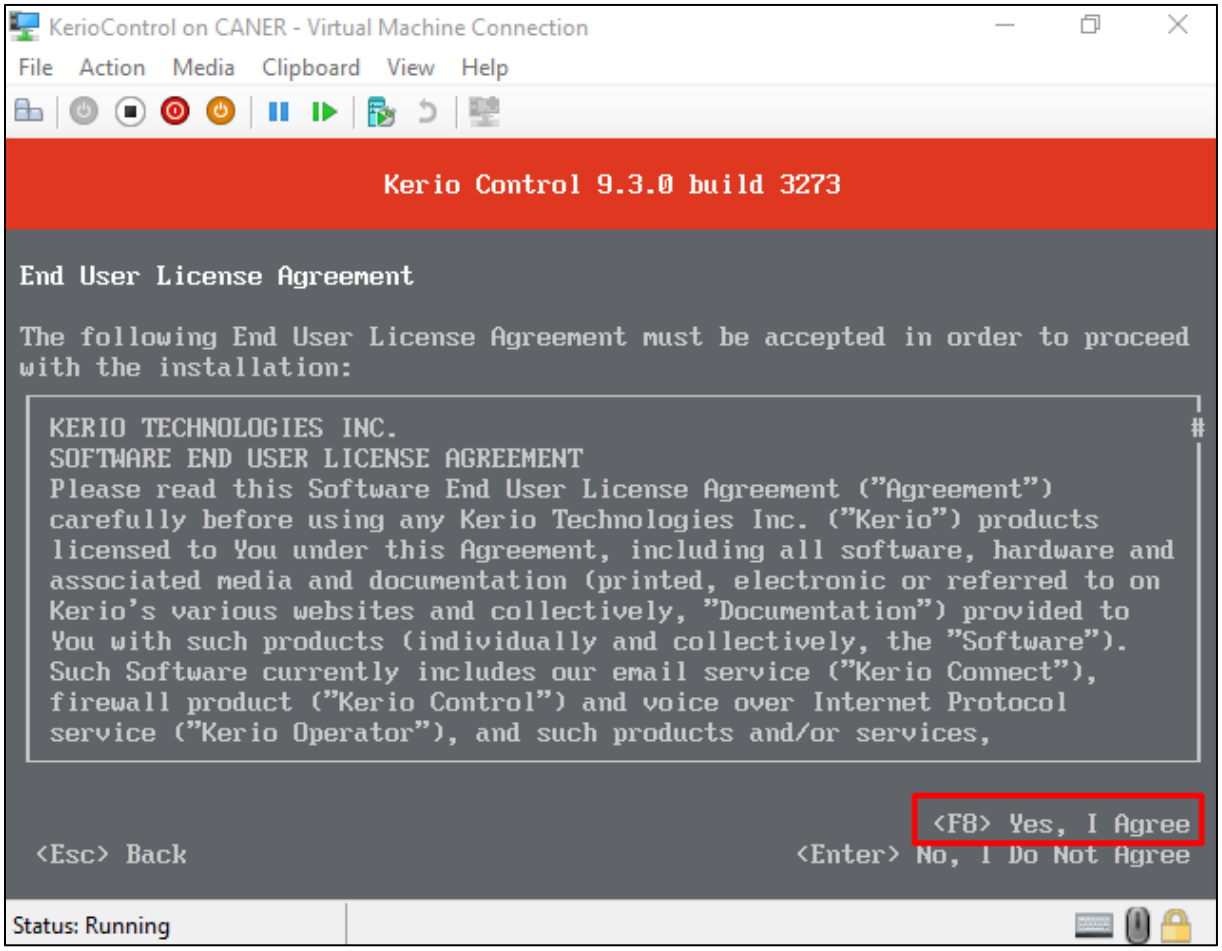
Similar to the pfSense set up, we create a new virtual machine with two NICs for the Kerio Firewall and start the image on the installation media. Then, the installer starts and the first thing we select is the language.



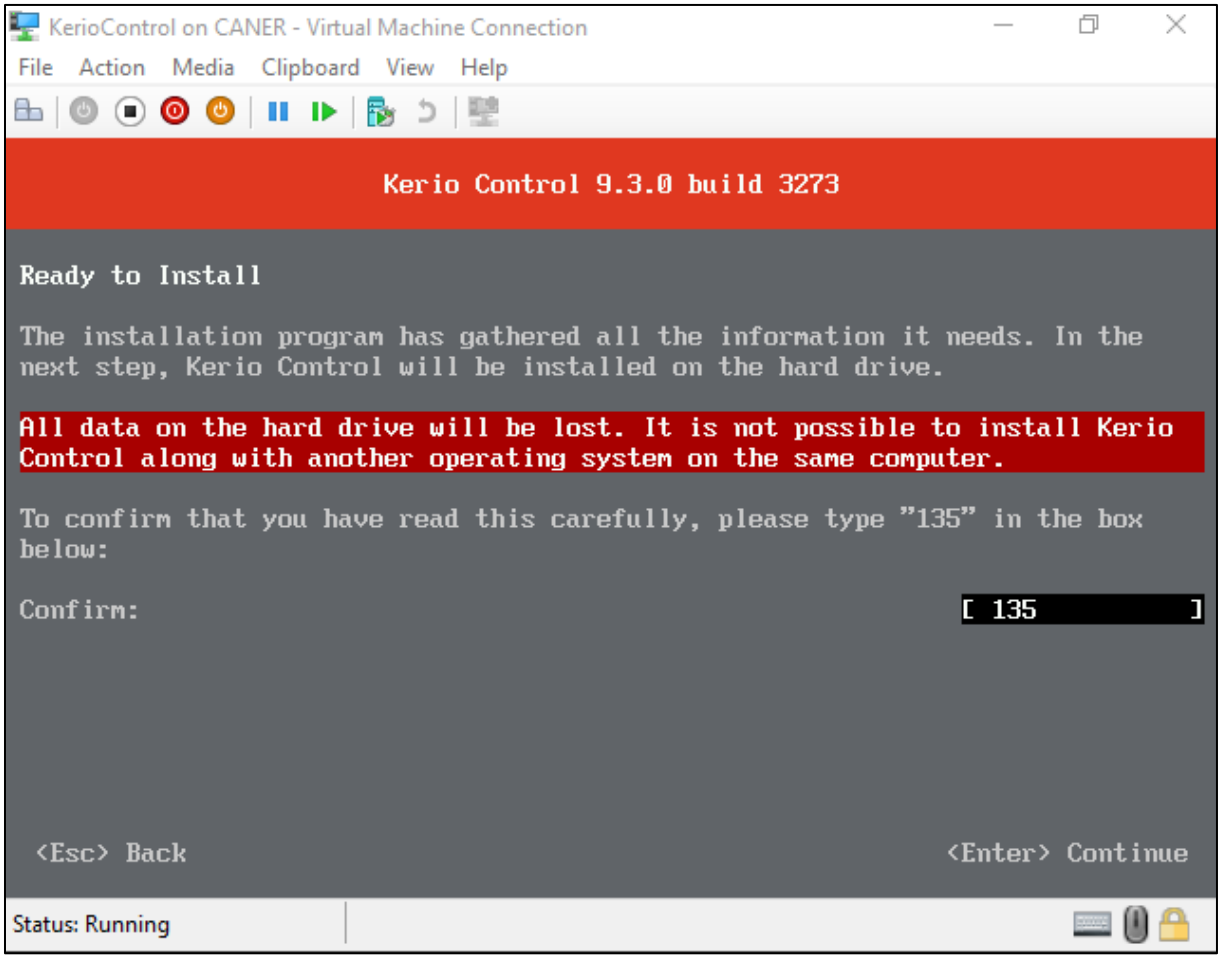
The installer starts to initialize.



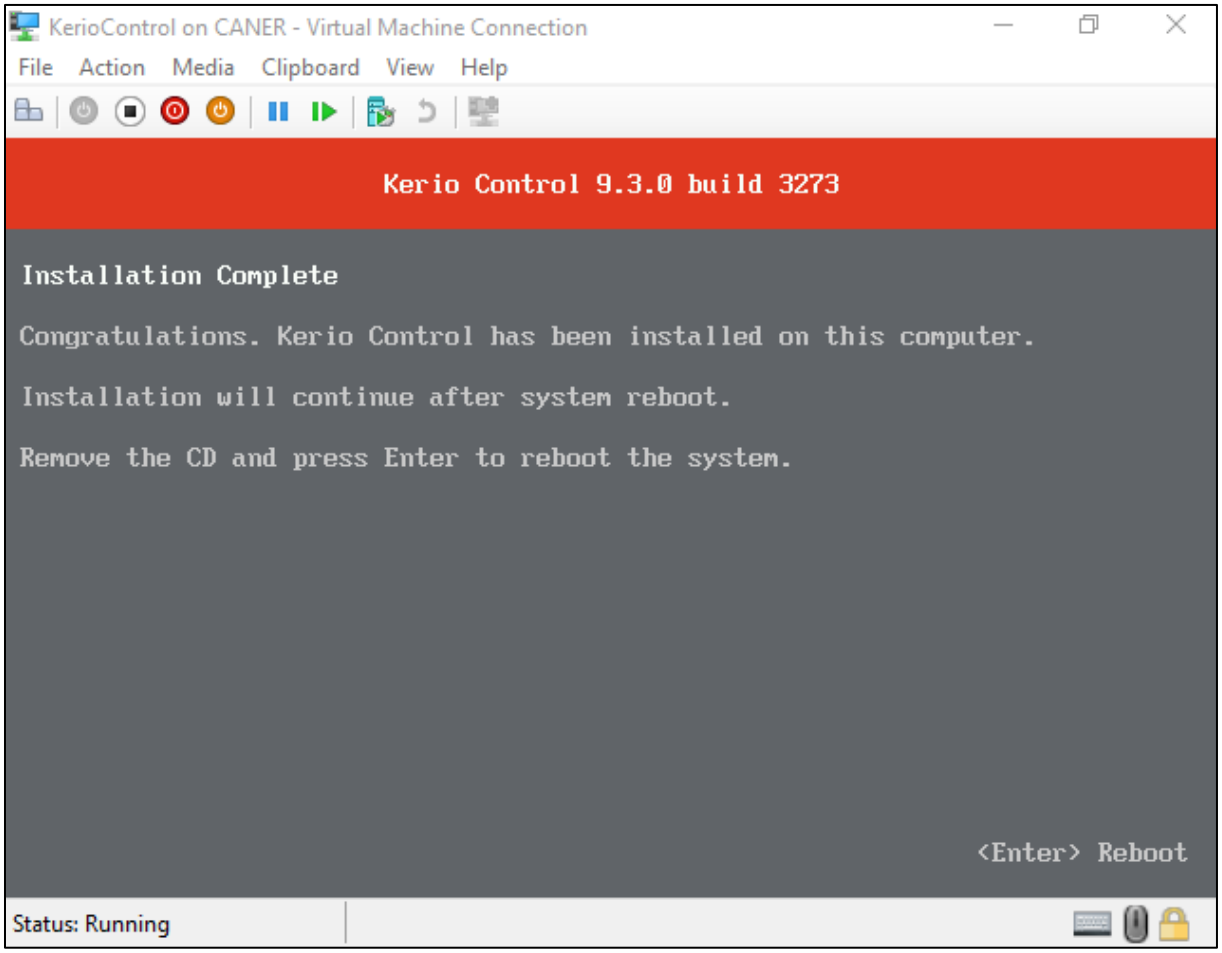
We agree to the user agreement and proceed.



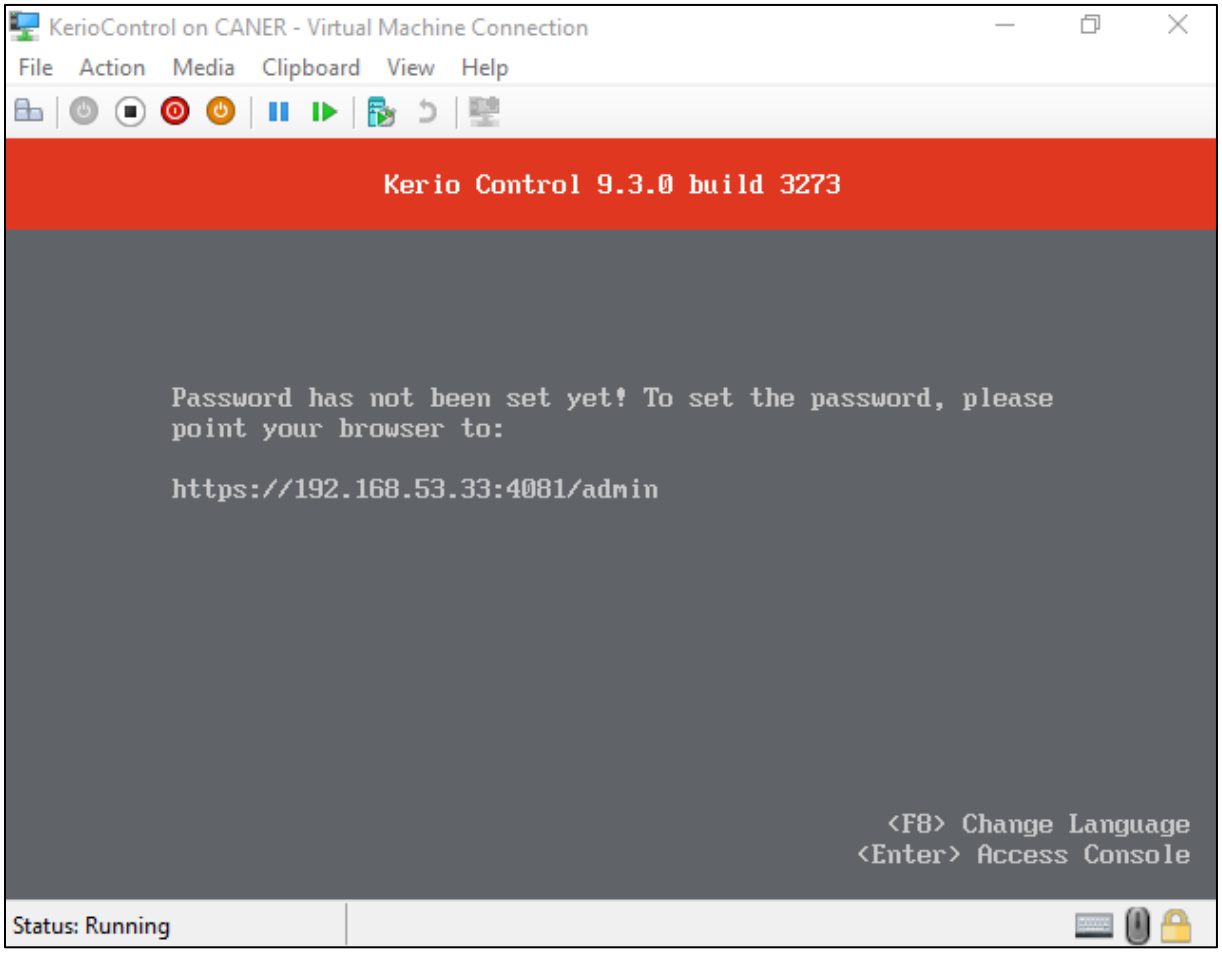
We type 135 to proceed.



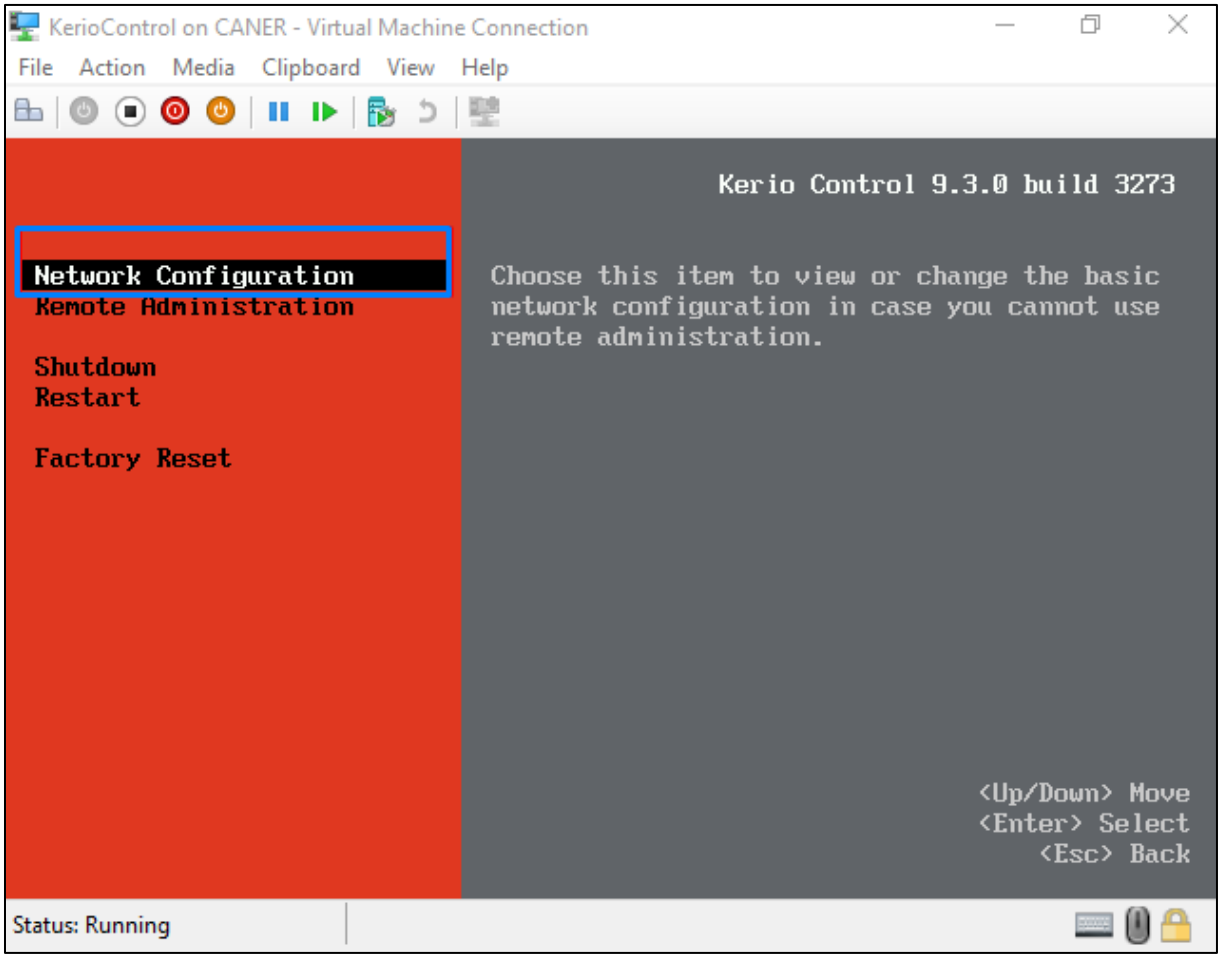
After the installation is complete, we again remove the image disk and reboot.



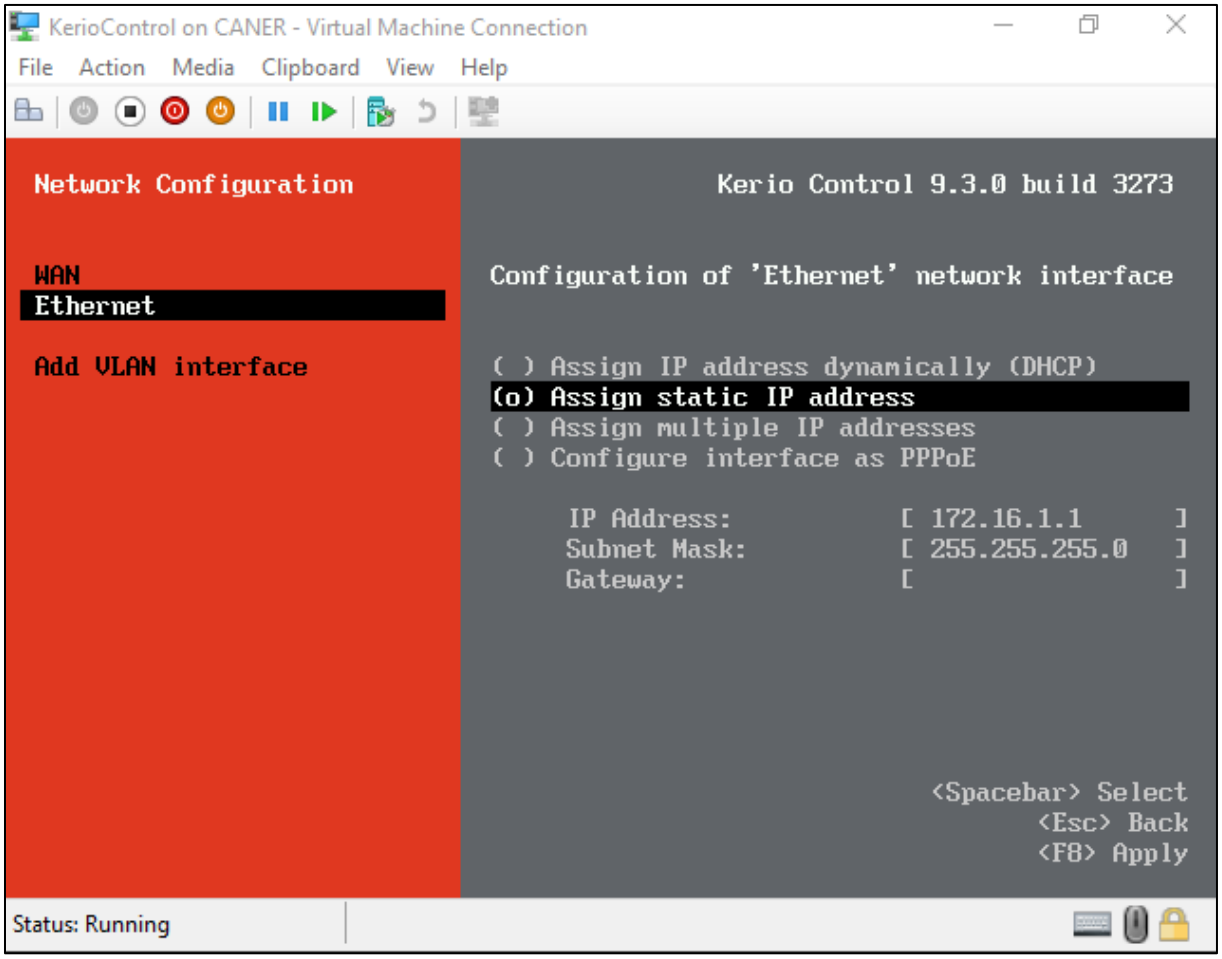
And the firewall is working. We get to the access console by pressing Enter.



We want to do the network configuration.

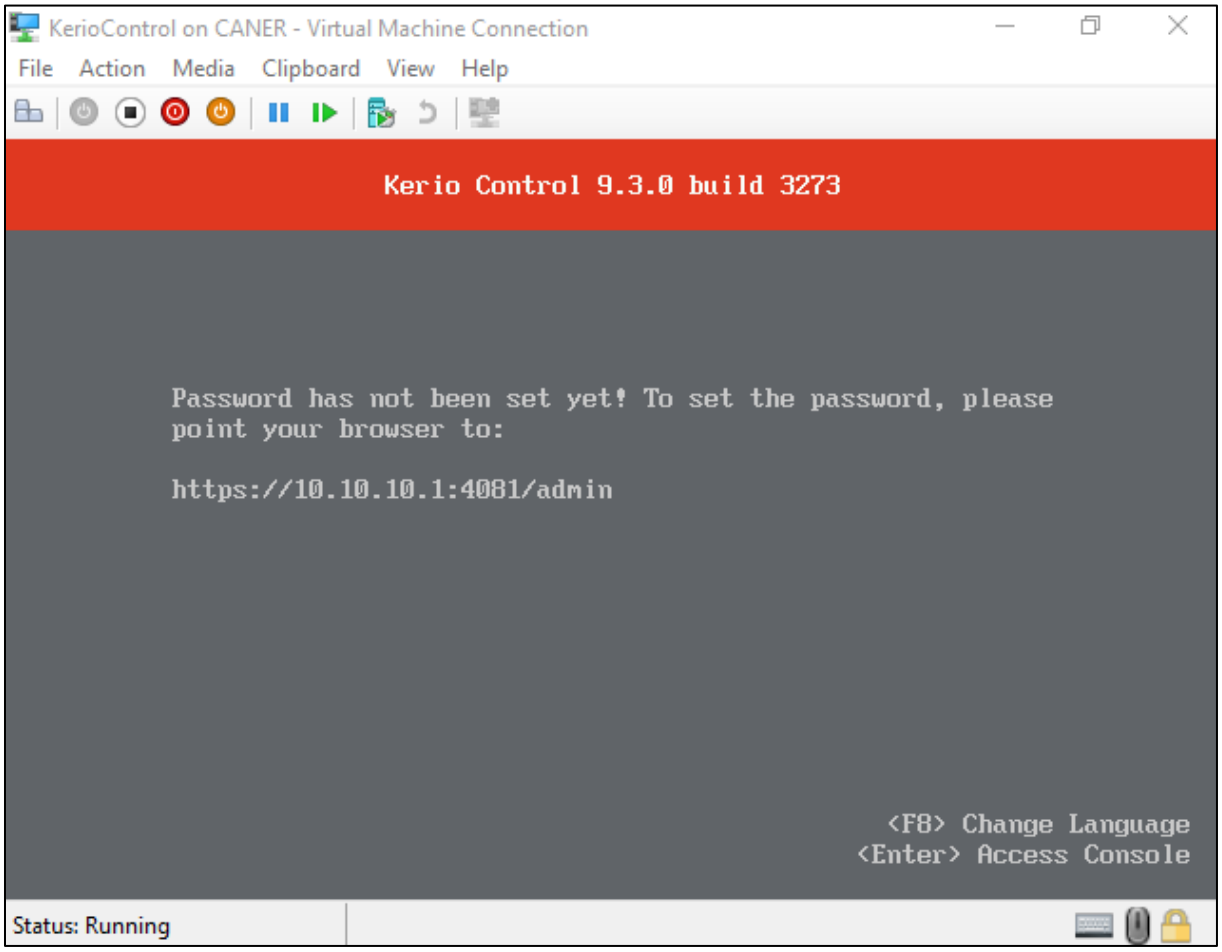


We assign a static IP address to the internal Ethernet interface.

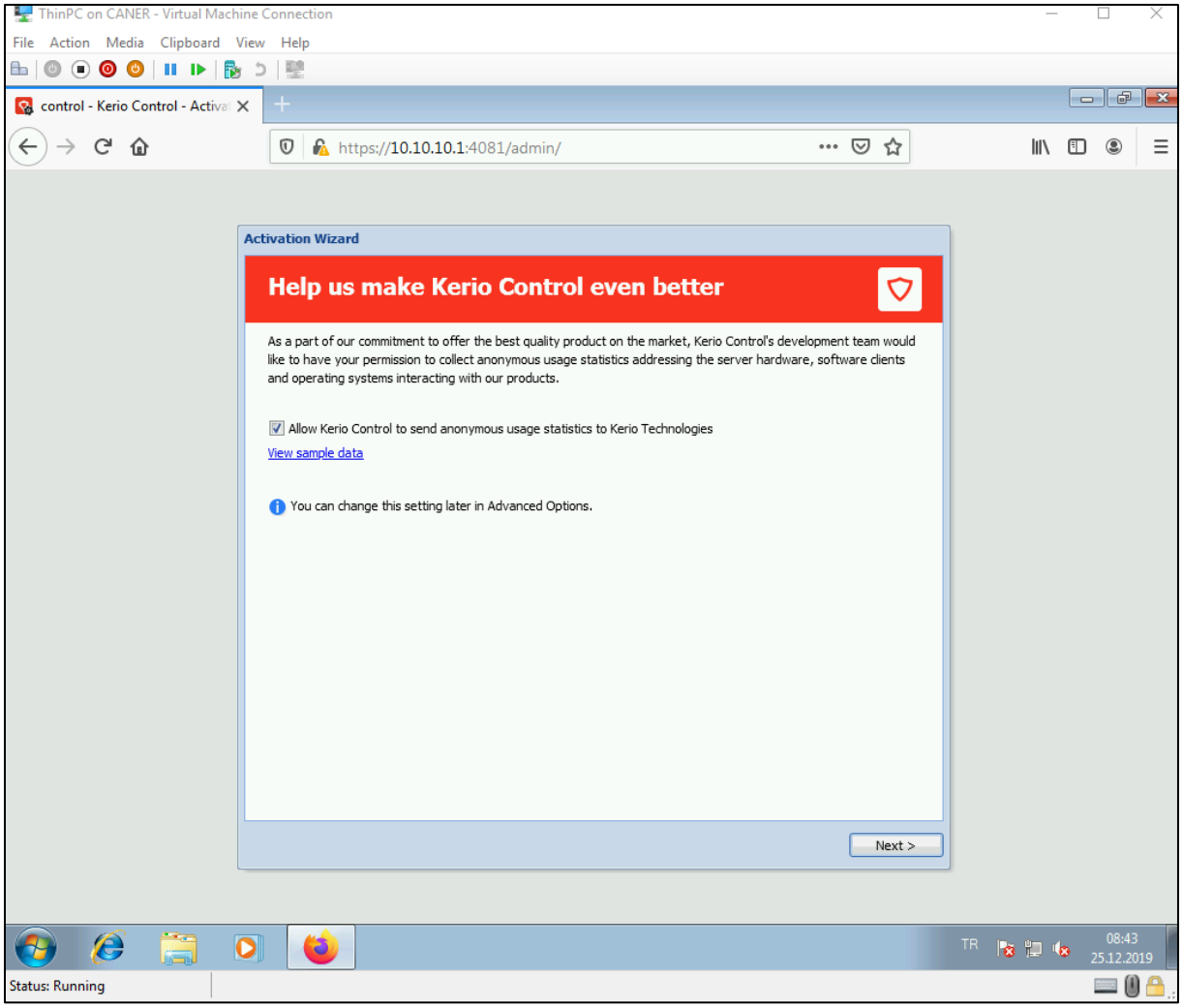


The WAN interface is automatically receiving IP from the BAU DHCP and we don't have to do anything there.

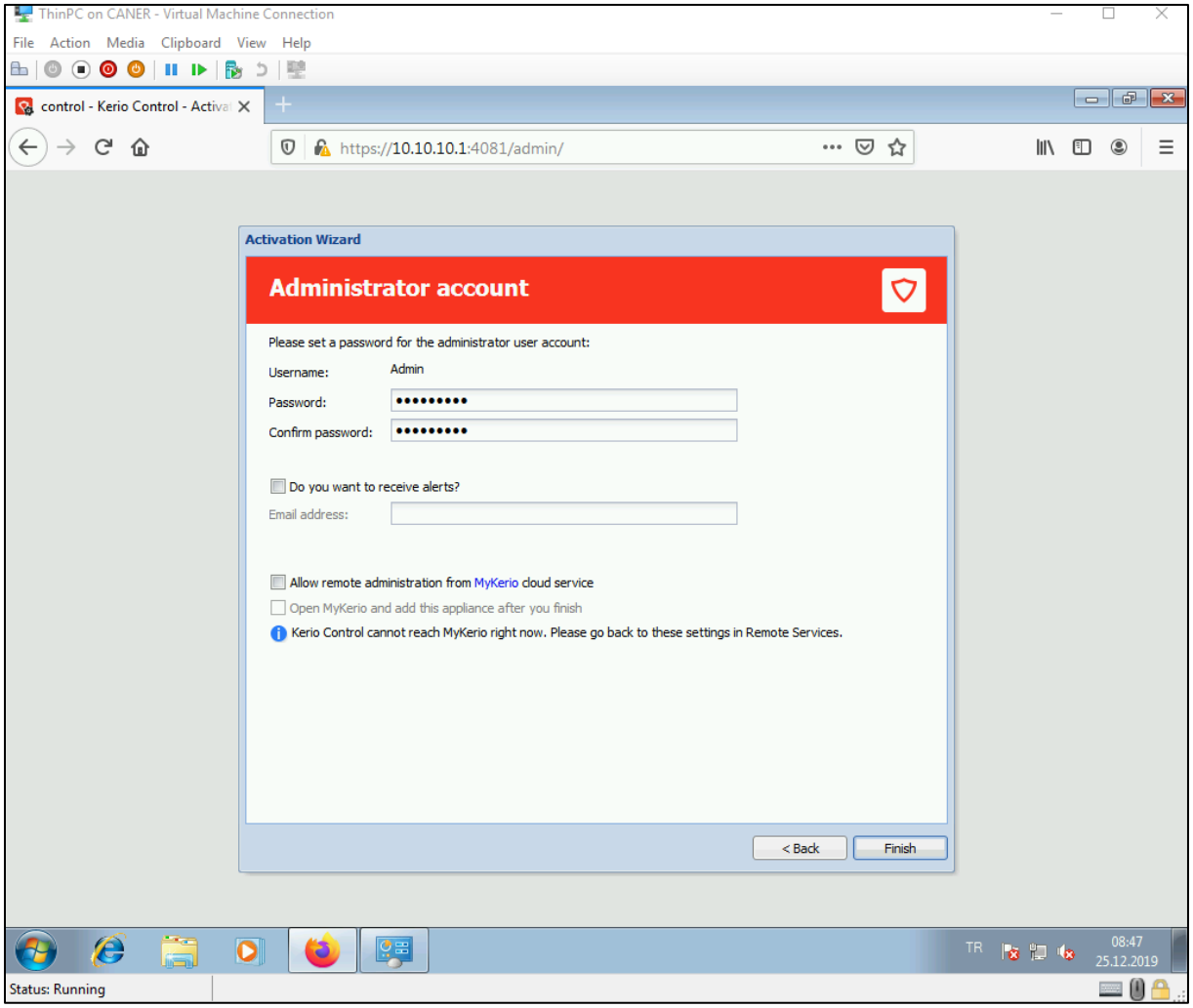
After we set our internal IP address of 10.10.10.1/24 and reboot the firewall. This screen once again welcomes as but now the access IP is the internal interface's IP address.



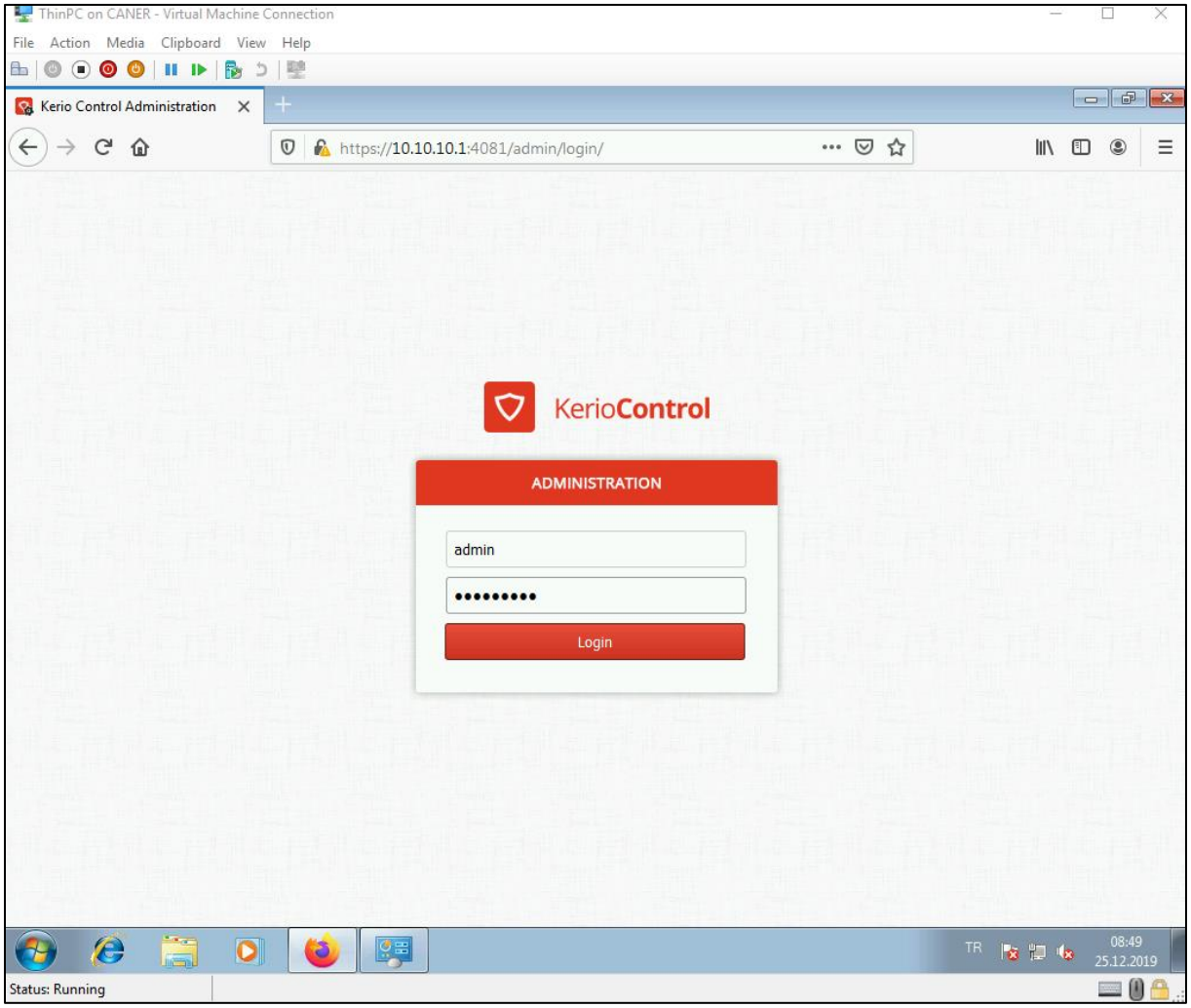
Similar to how we have done it with pfSense we enter this address to our web browser.



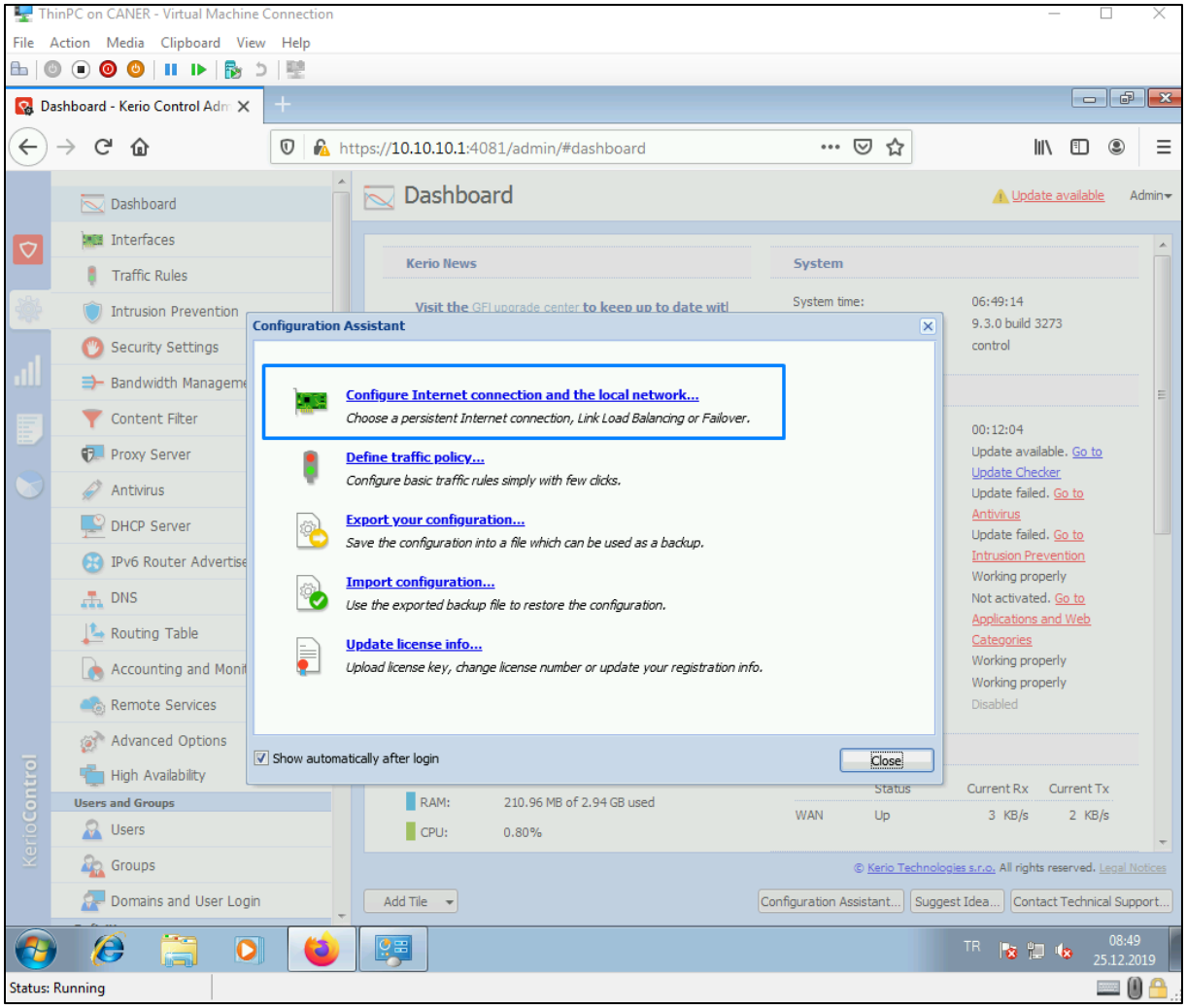
It wants us to set a password for admin.



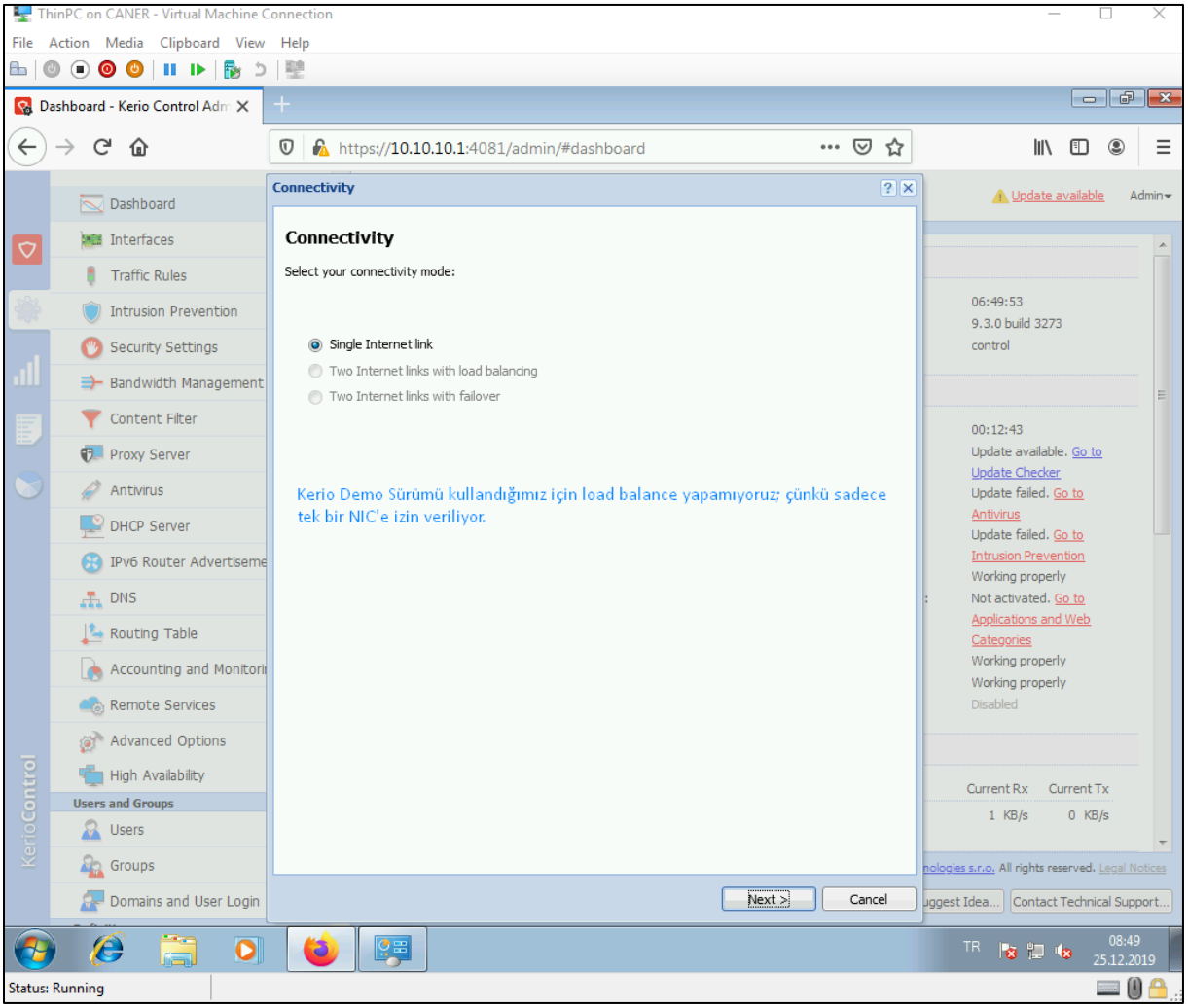
We log in using the newly set password.



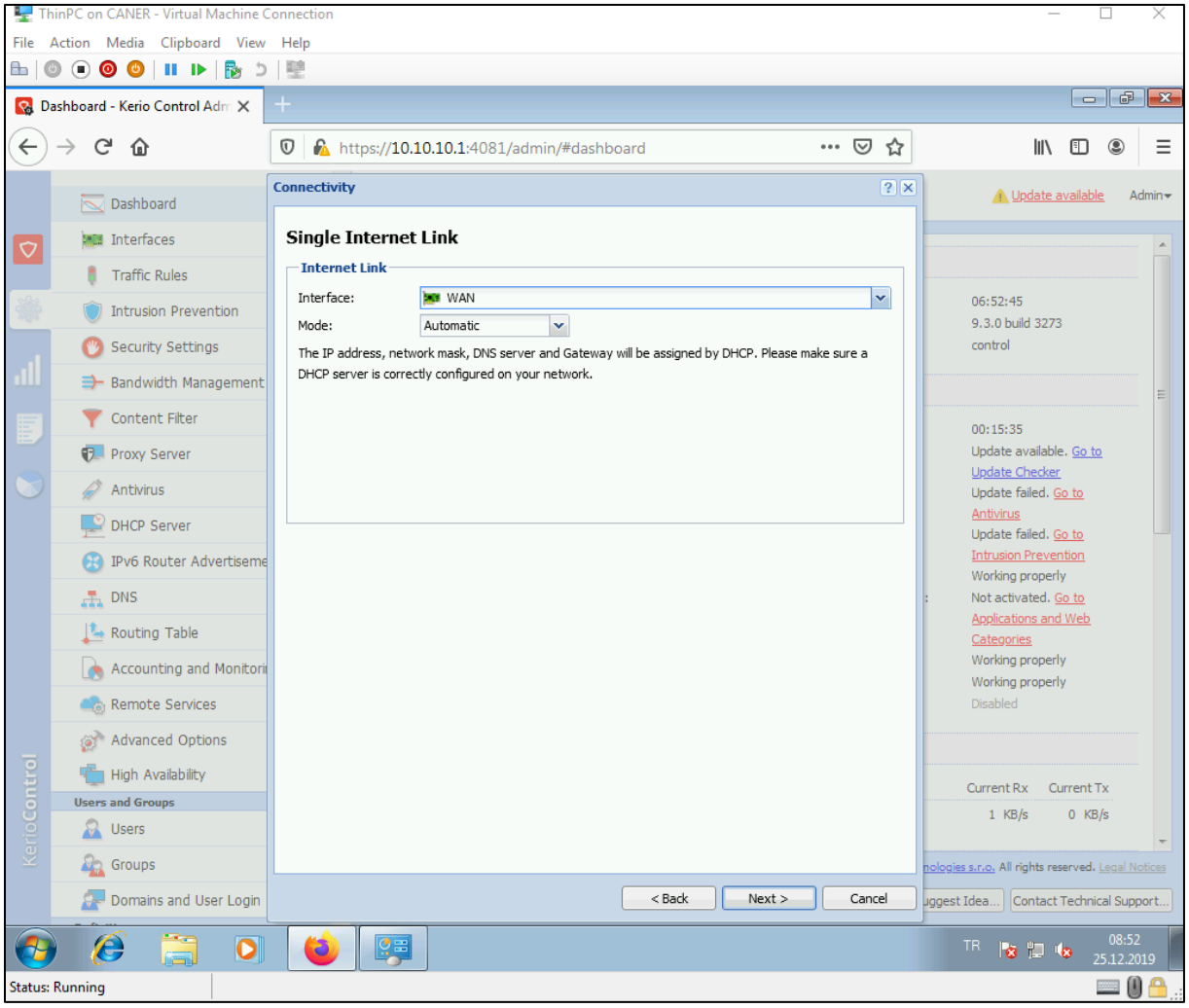
We configure the network settings.



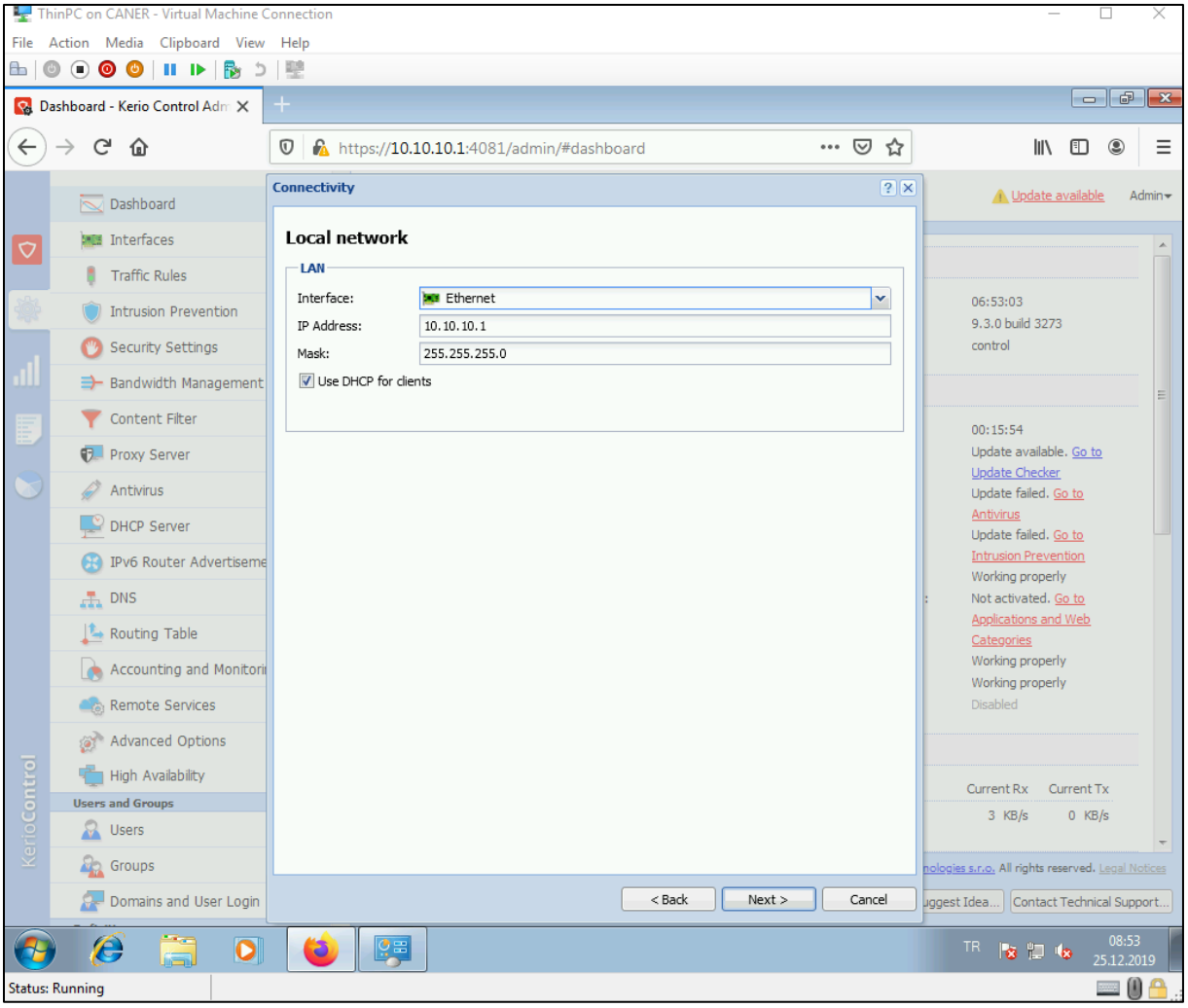
We use single link since this is a Demo Edition.



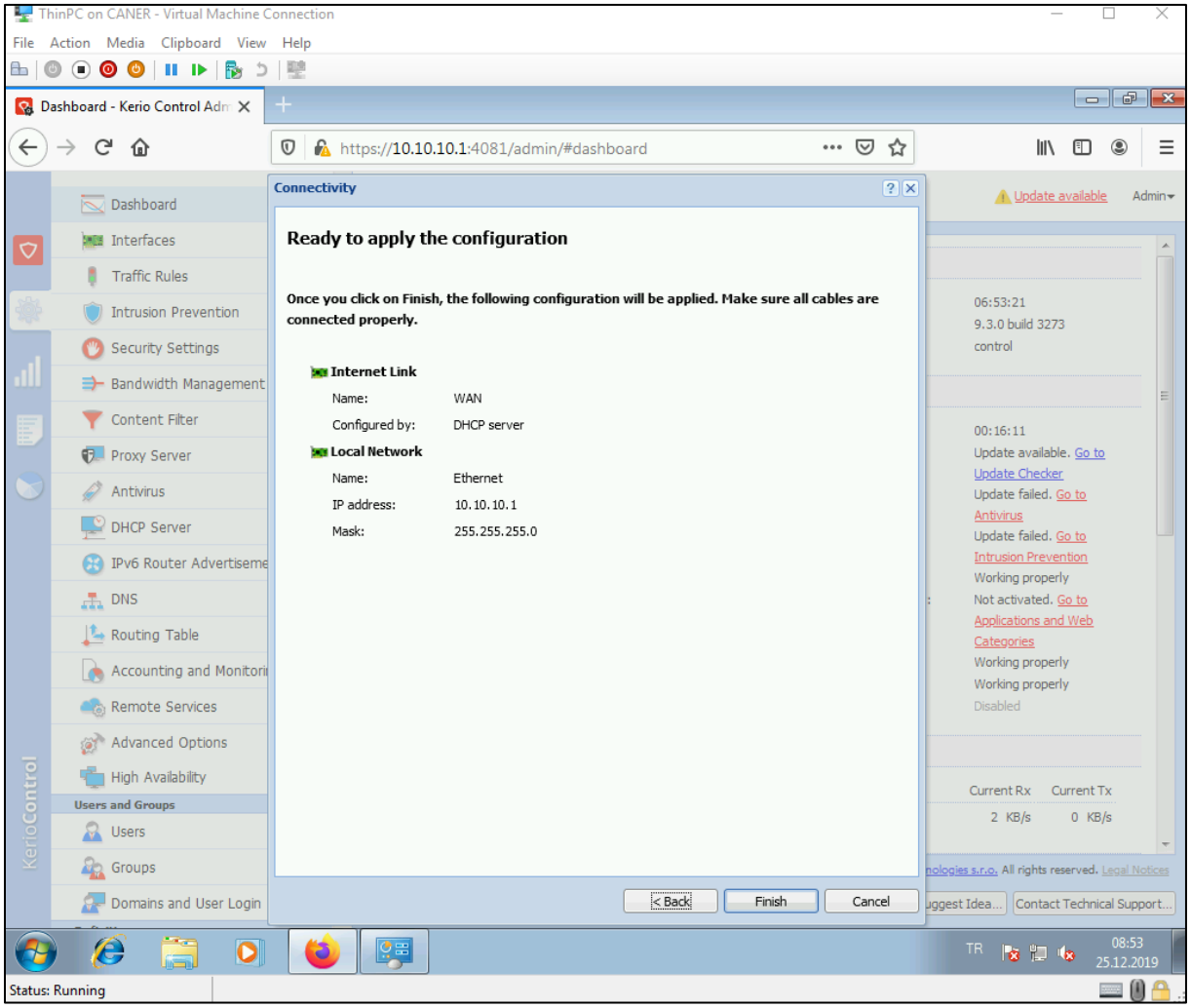
We keep WAN interface at automatic.



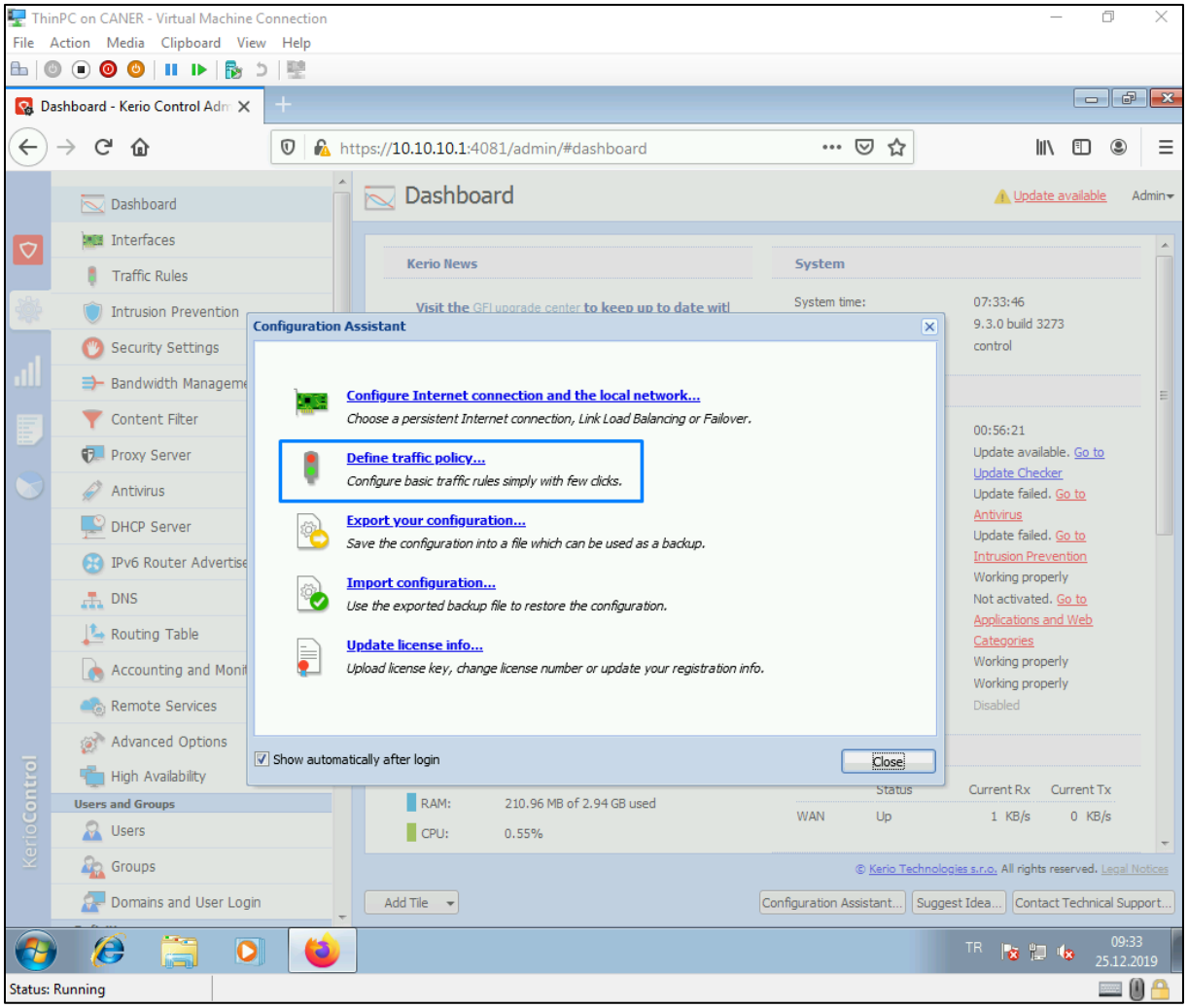
We set the Ethernet interface at the IP address we have set before and enable DHCP.



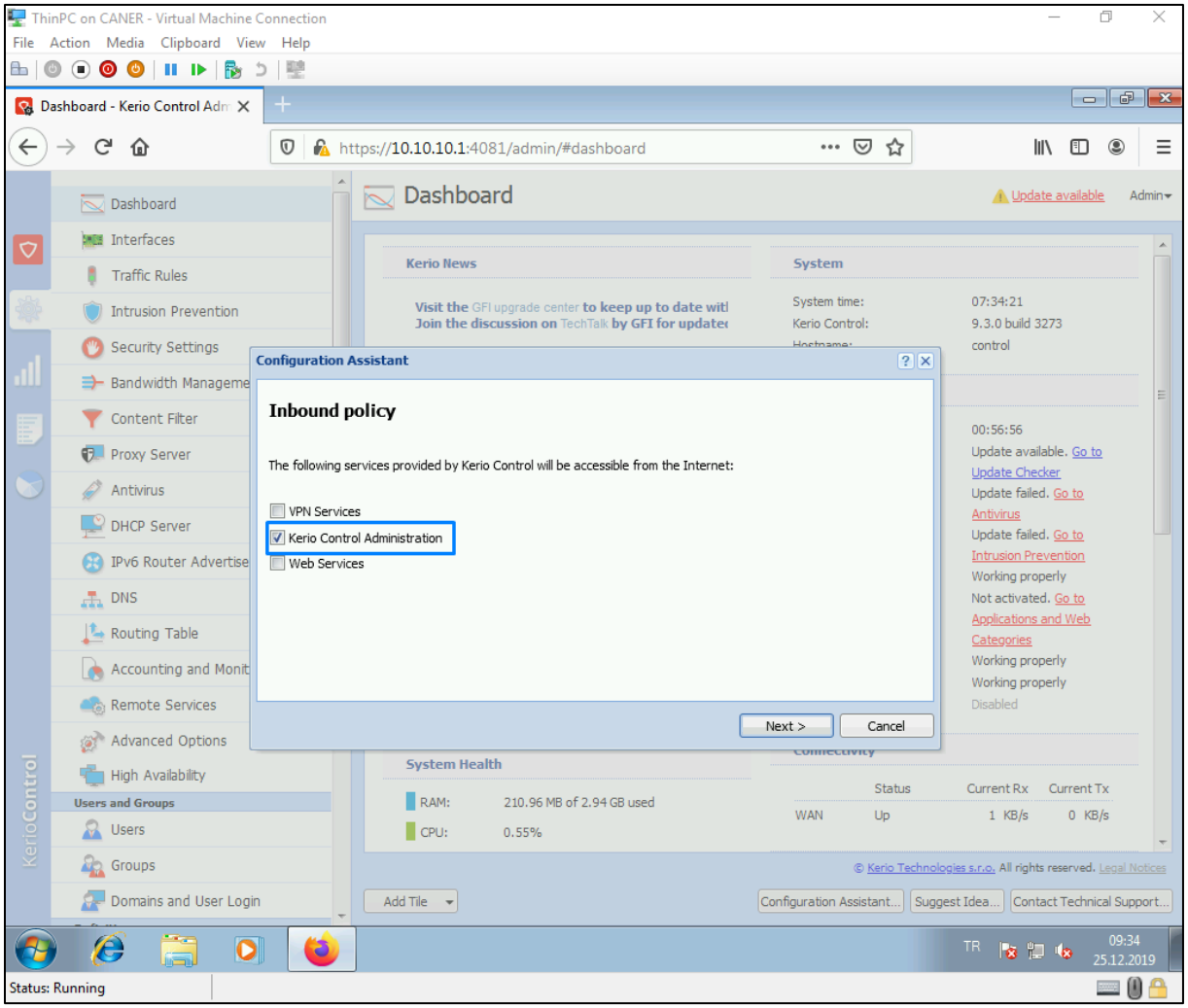
We review and finish.



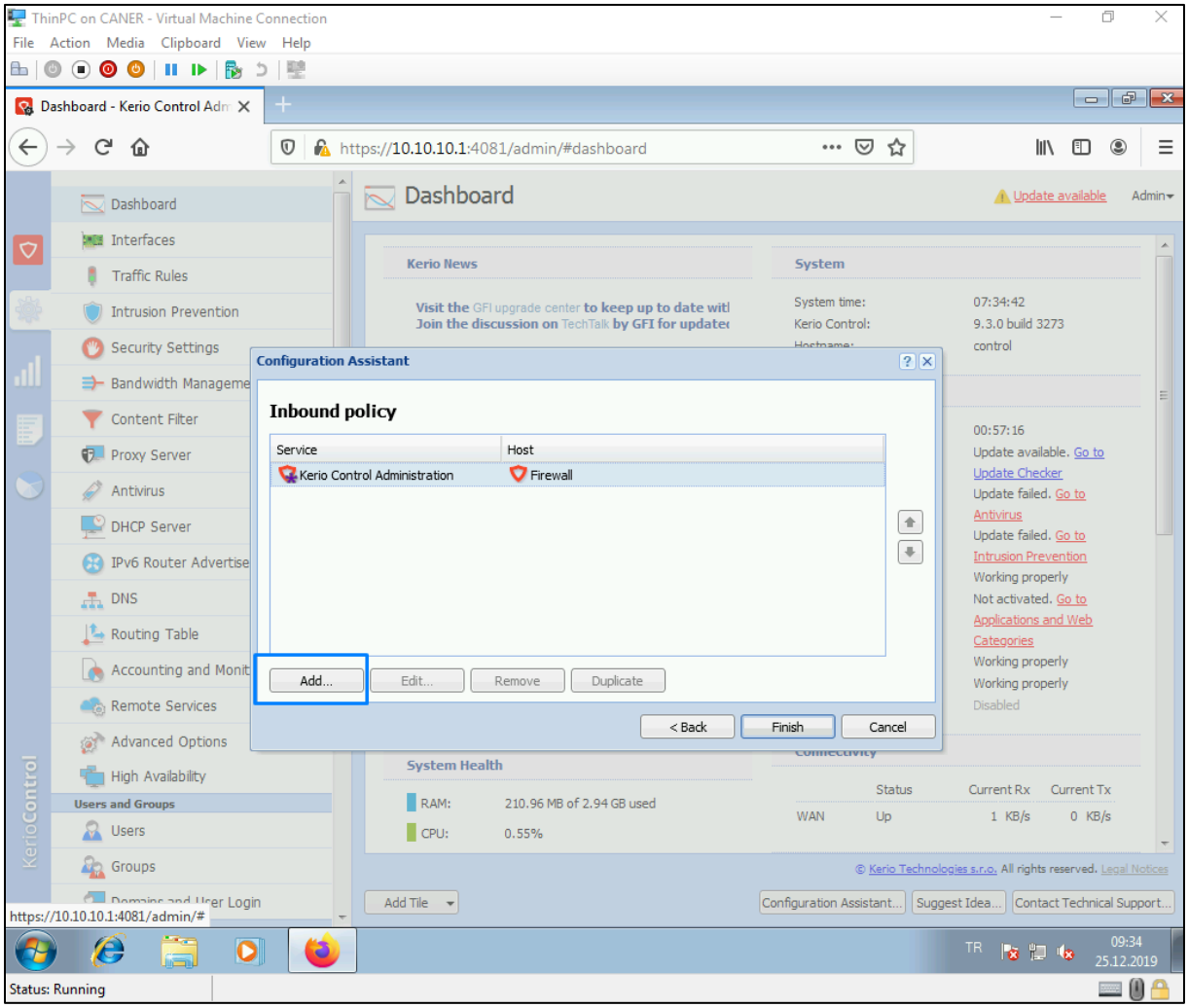
The next step of the wizard is to set traffic rules.



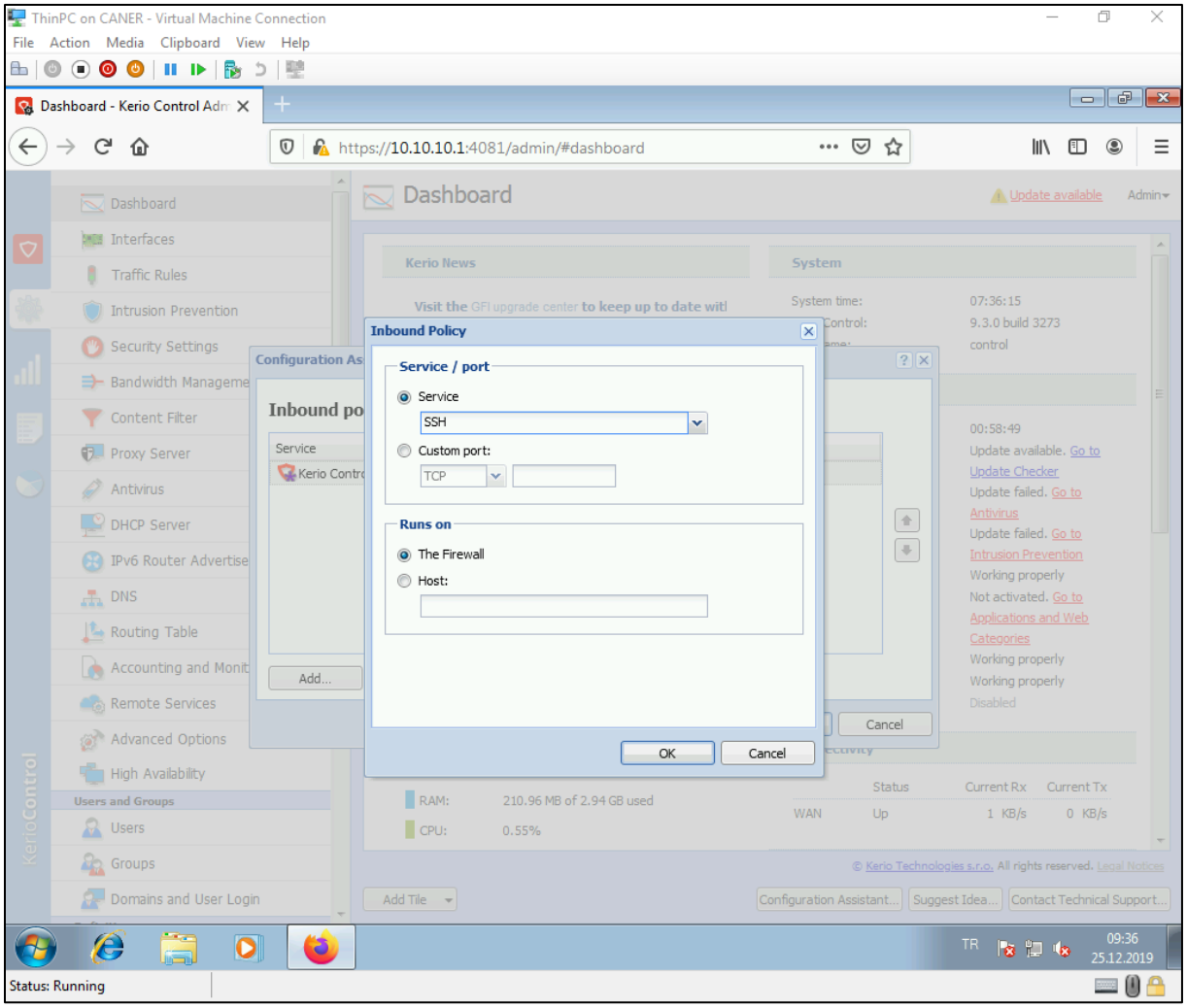
We choose to set the rules for Kerio Control Administration.



We select the firewall itself and add inbound policies.

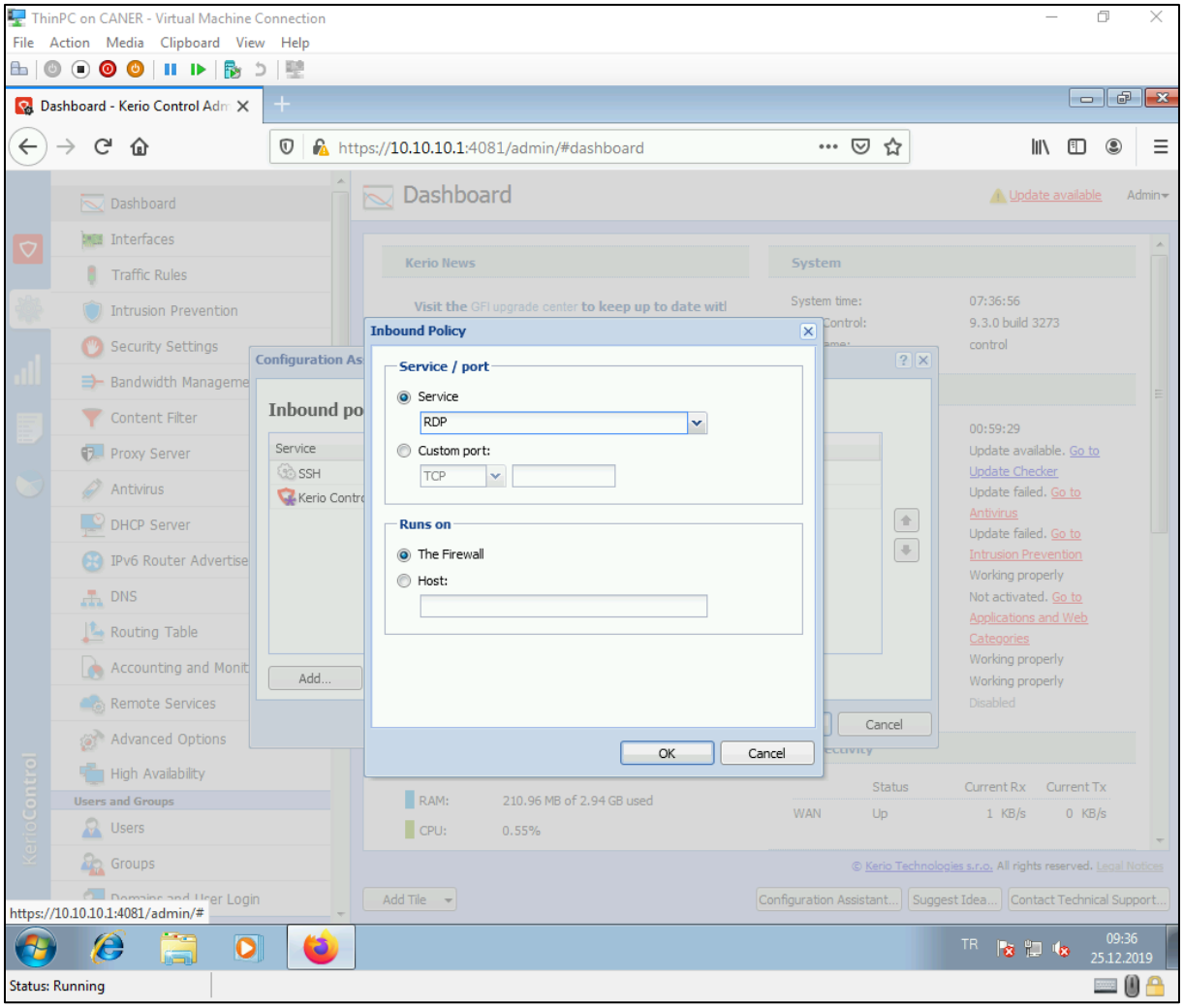


We enable SSH.

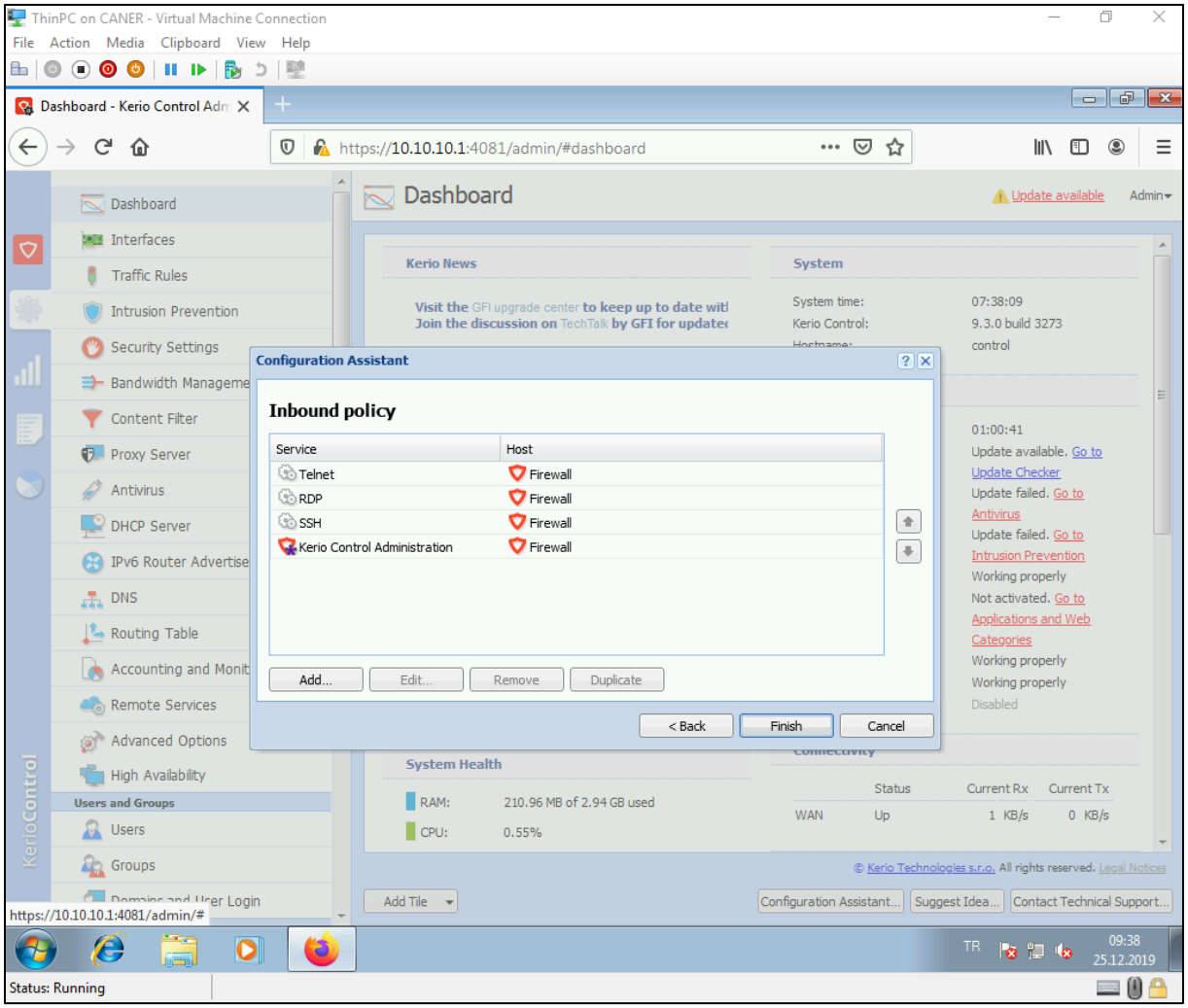


20.1.2020

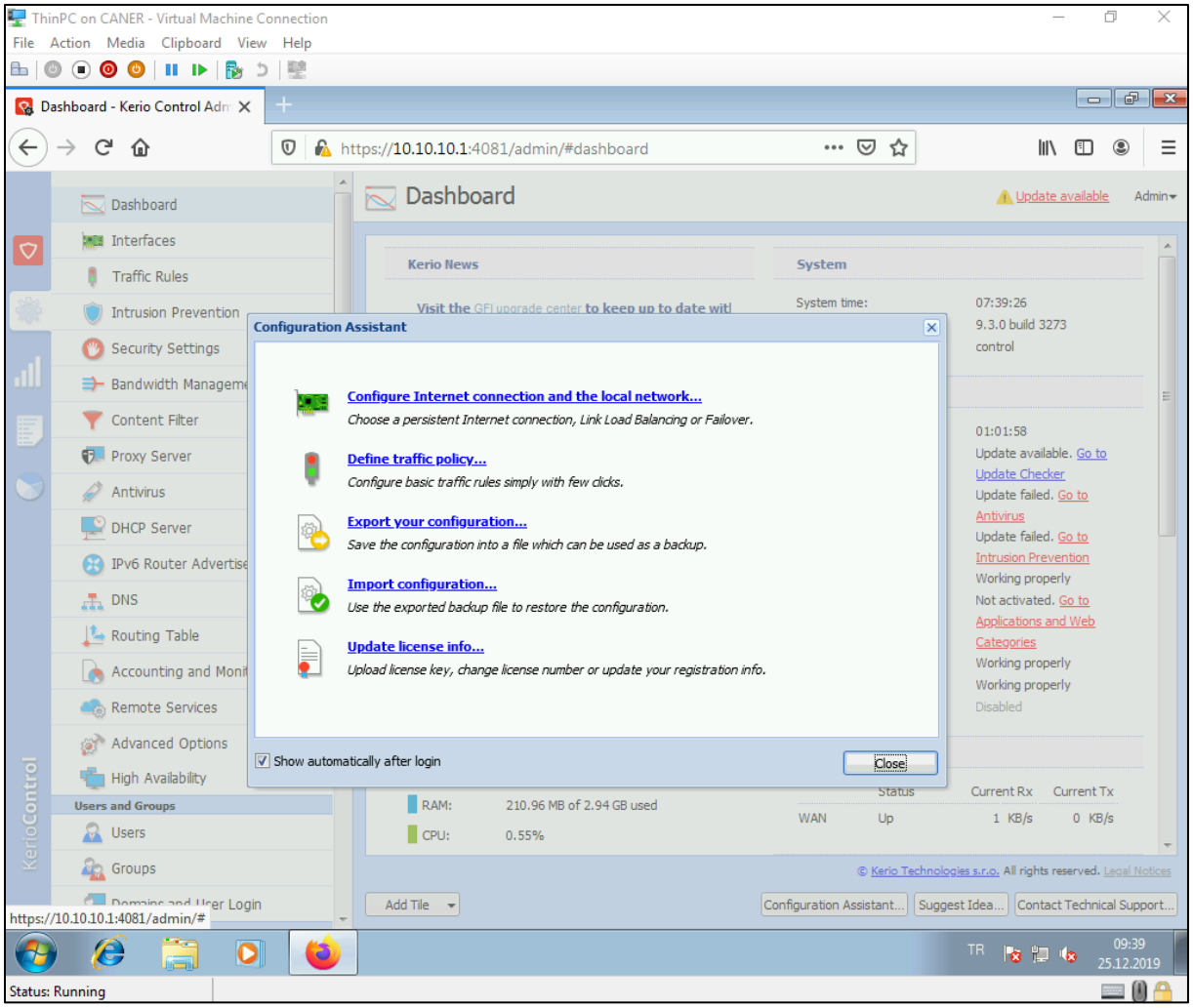
We enable RDP.



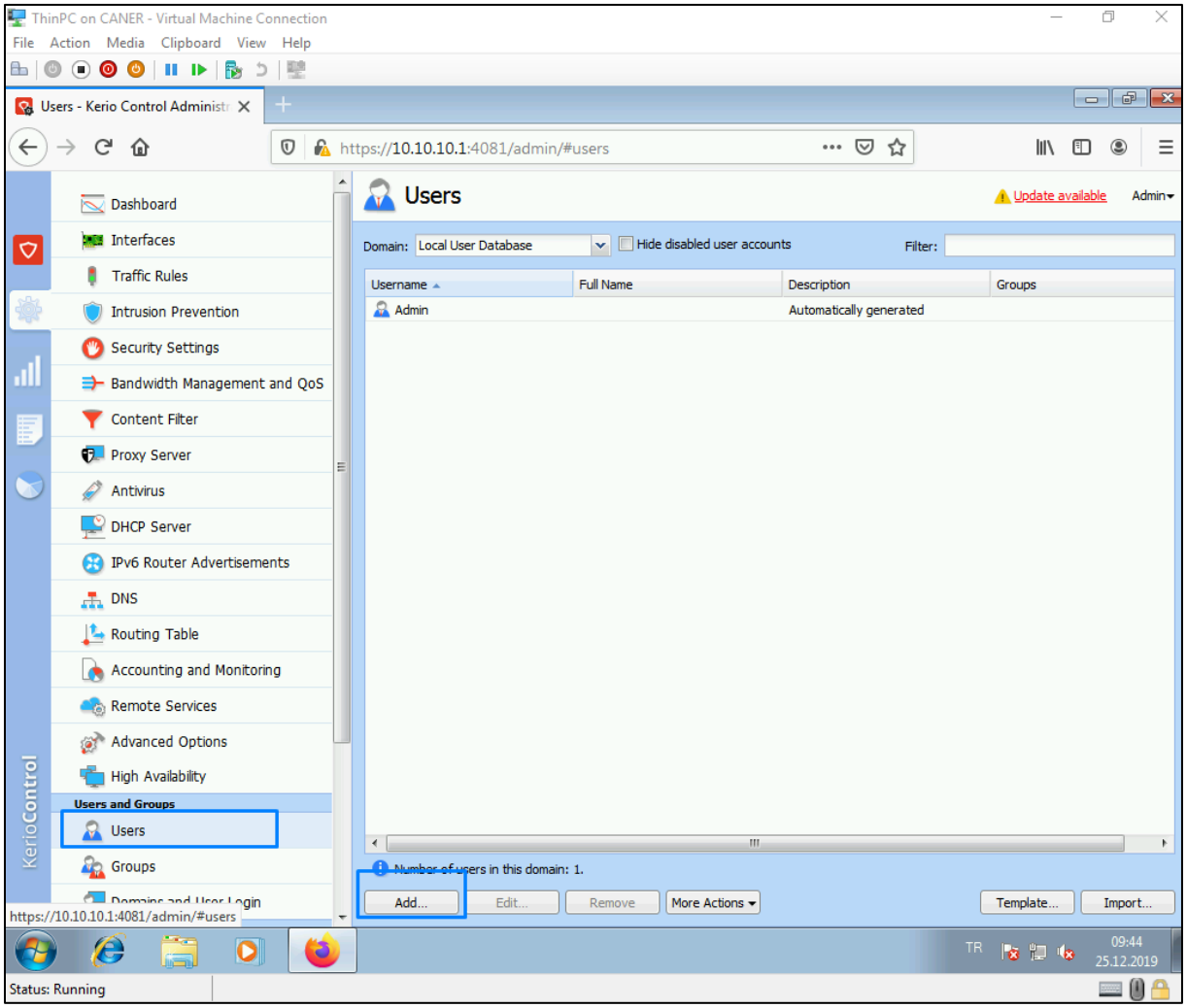
We also enable Telnet and proceed.



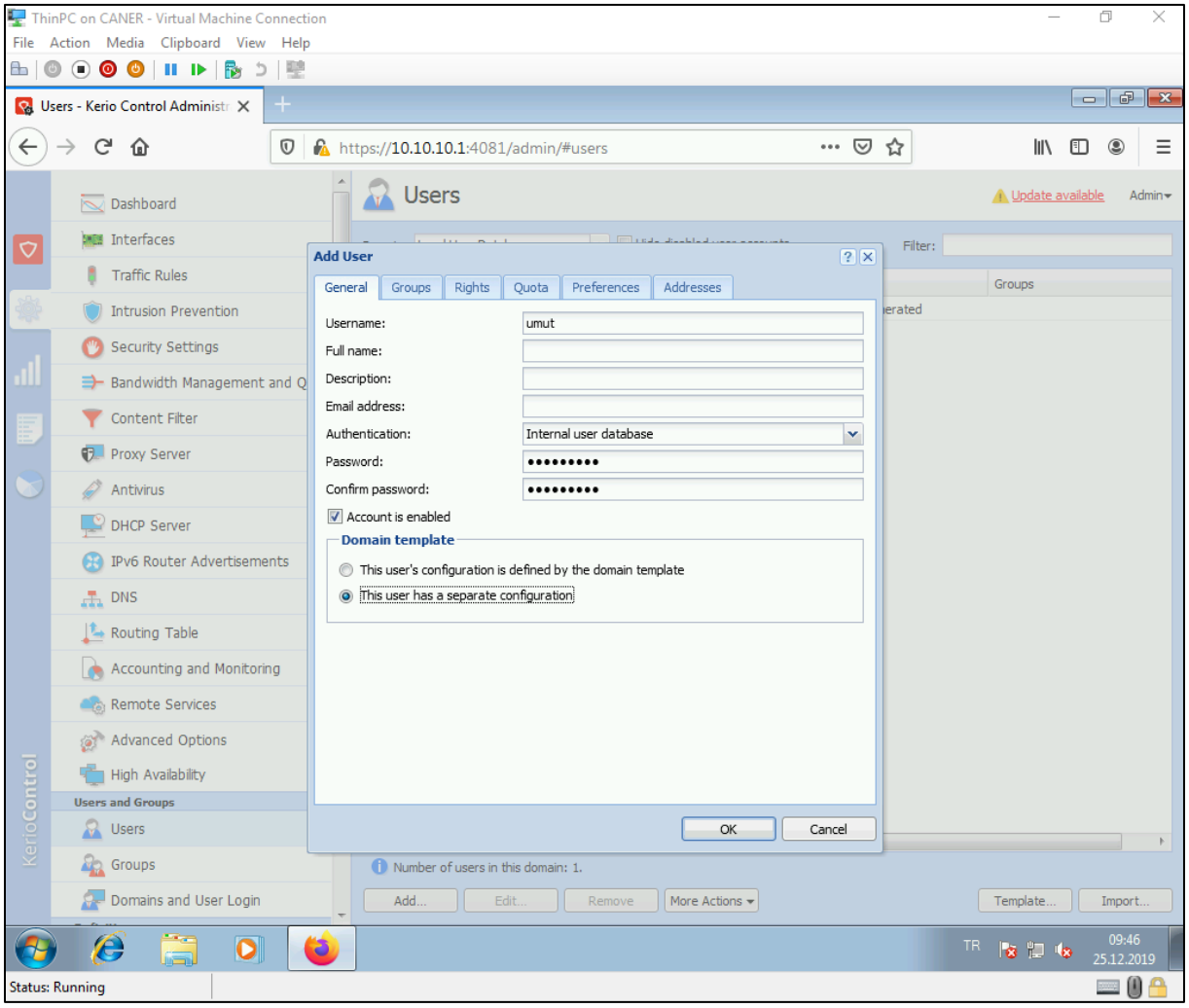
We are done with network configuration and can close the wizard.



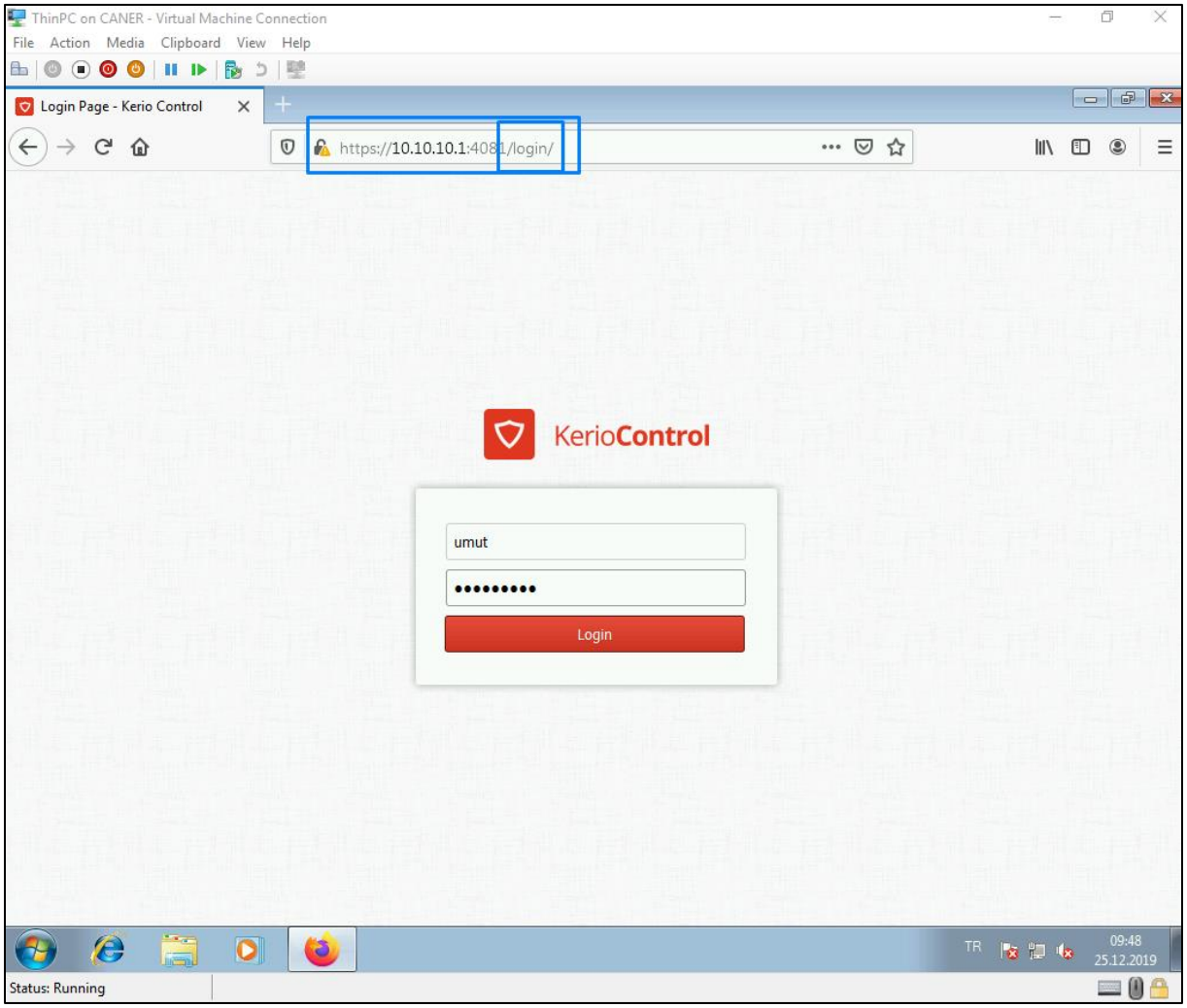
We get to users to create a new user.



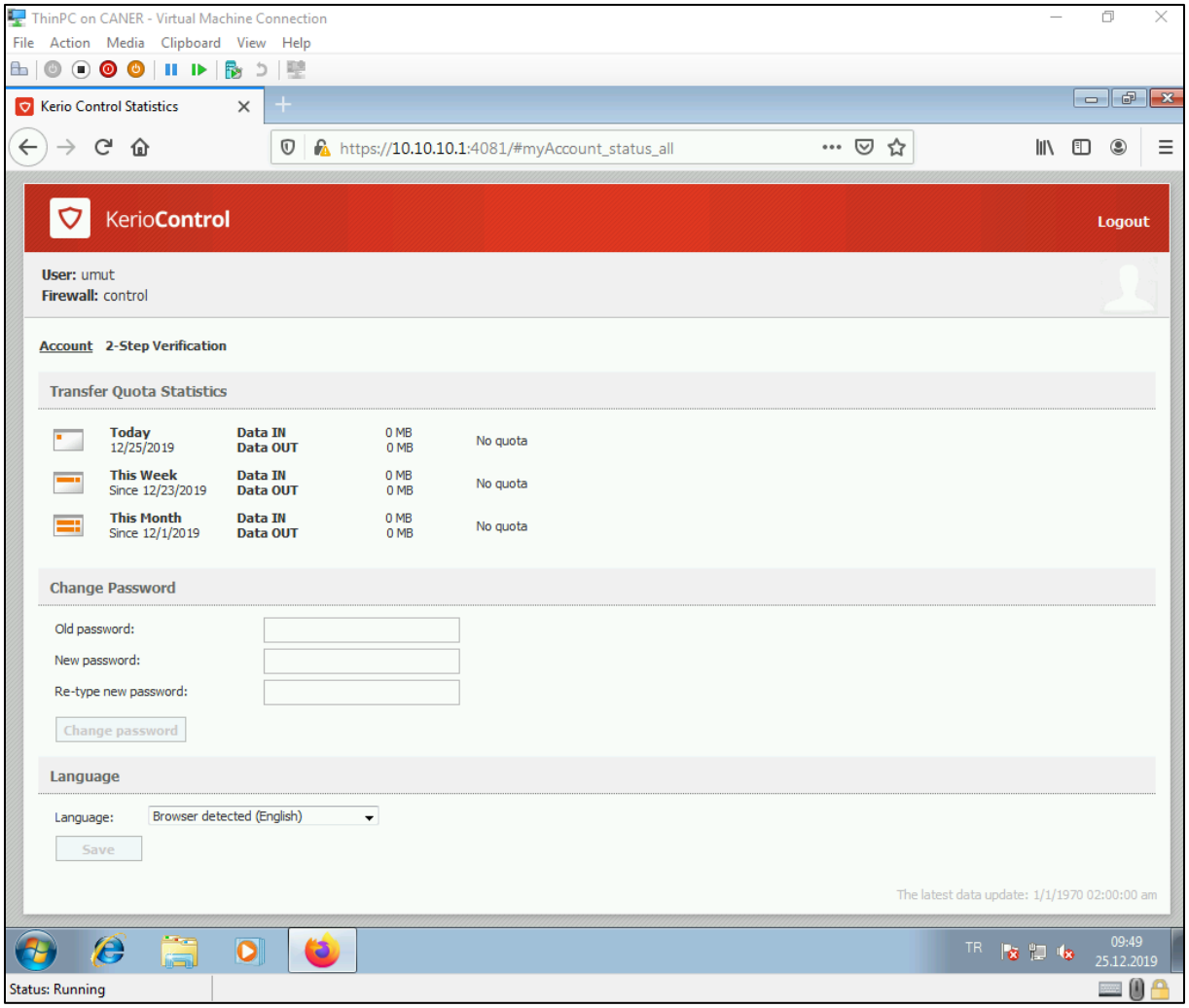
We enter the user's information.



Then, we test logging in as the new user.

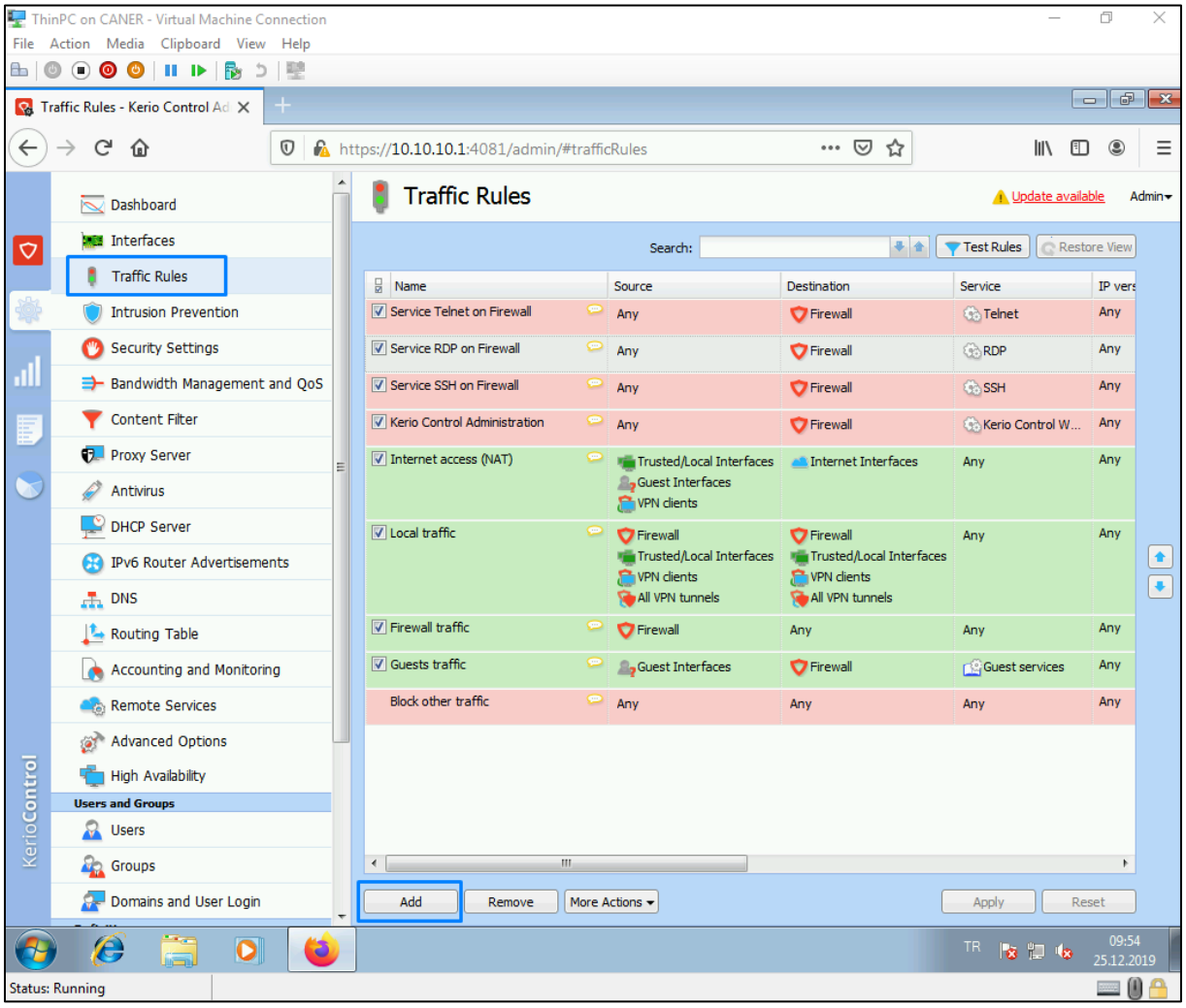


As you can see, a simple user doesn’t have access to the admin controls.

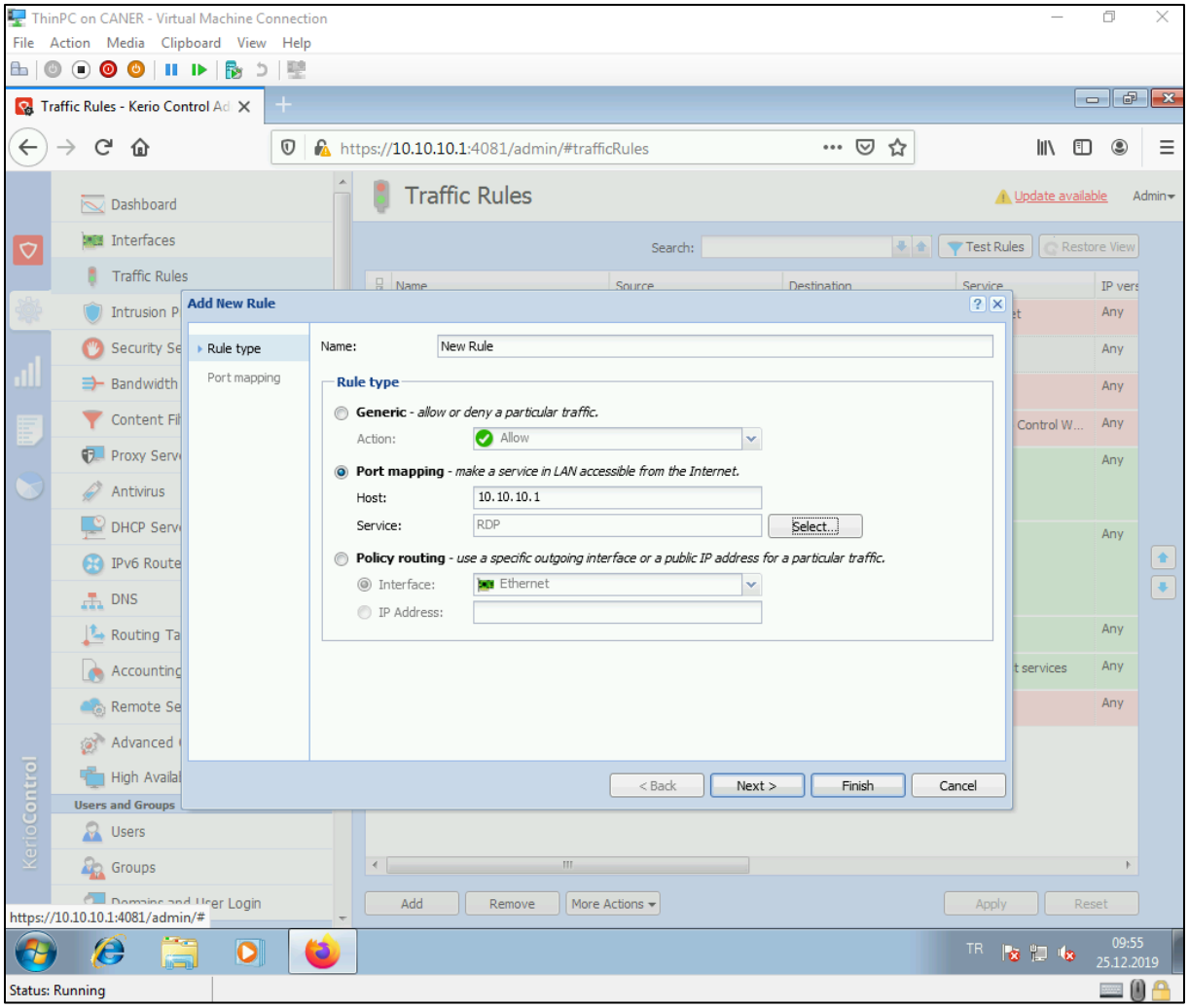


But it’s possible to change the password.

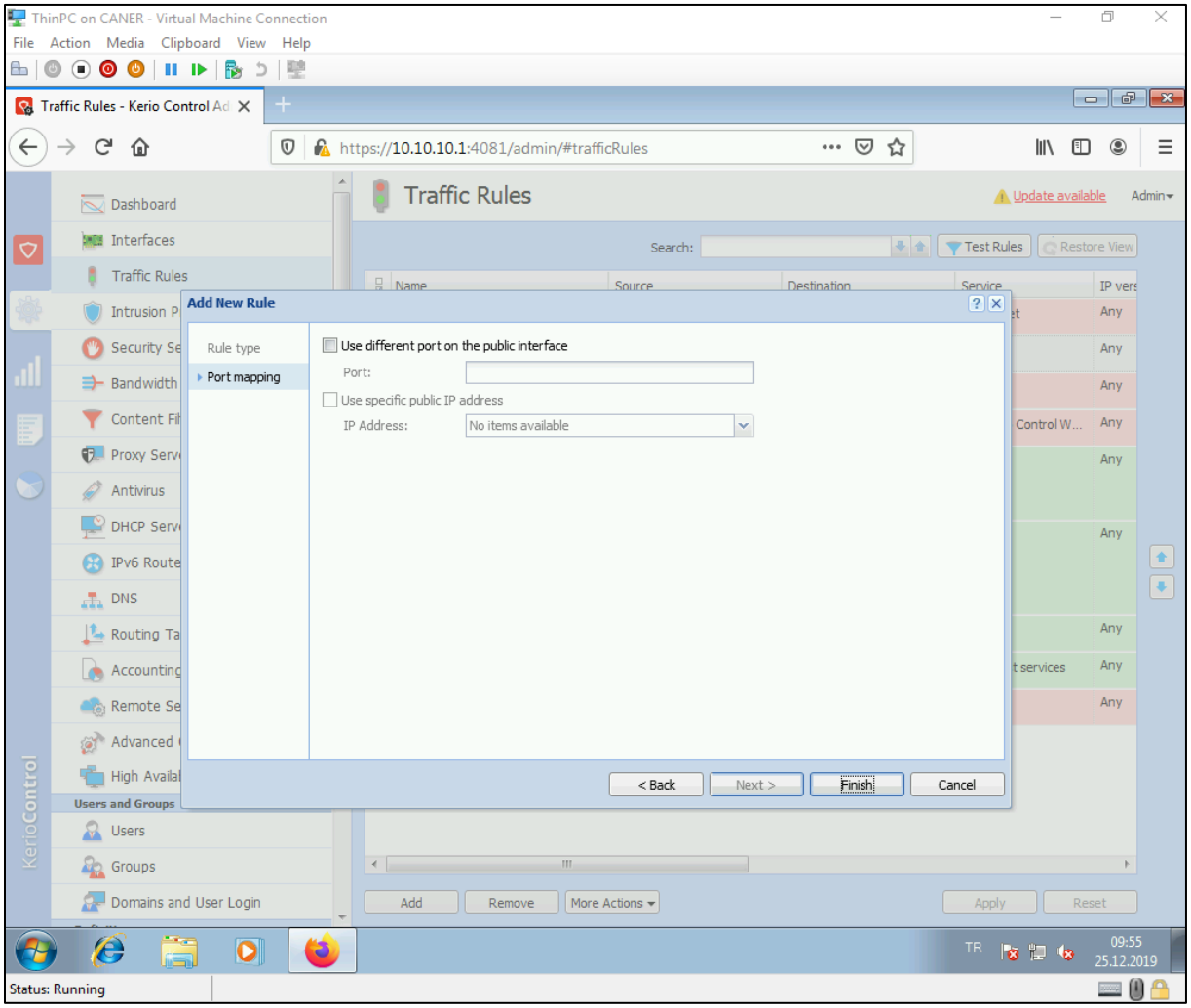
Now, we want to do port mapping to connect to an internal host via the internet through the firewall. Hence, we get to the traffic rules and add a new one.



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

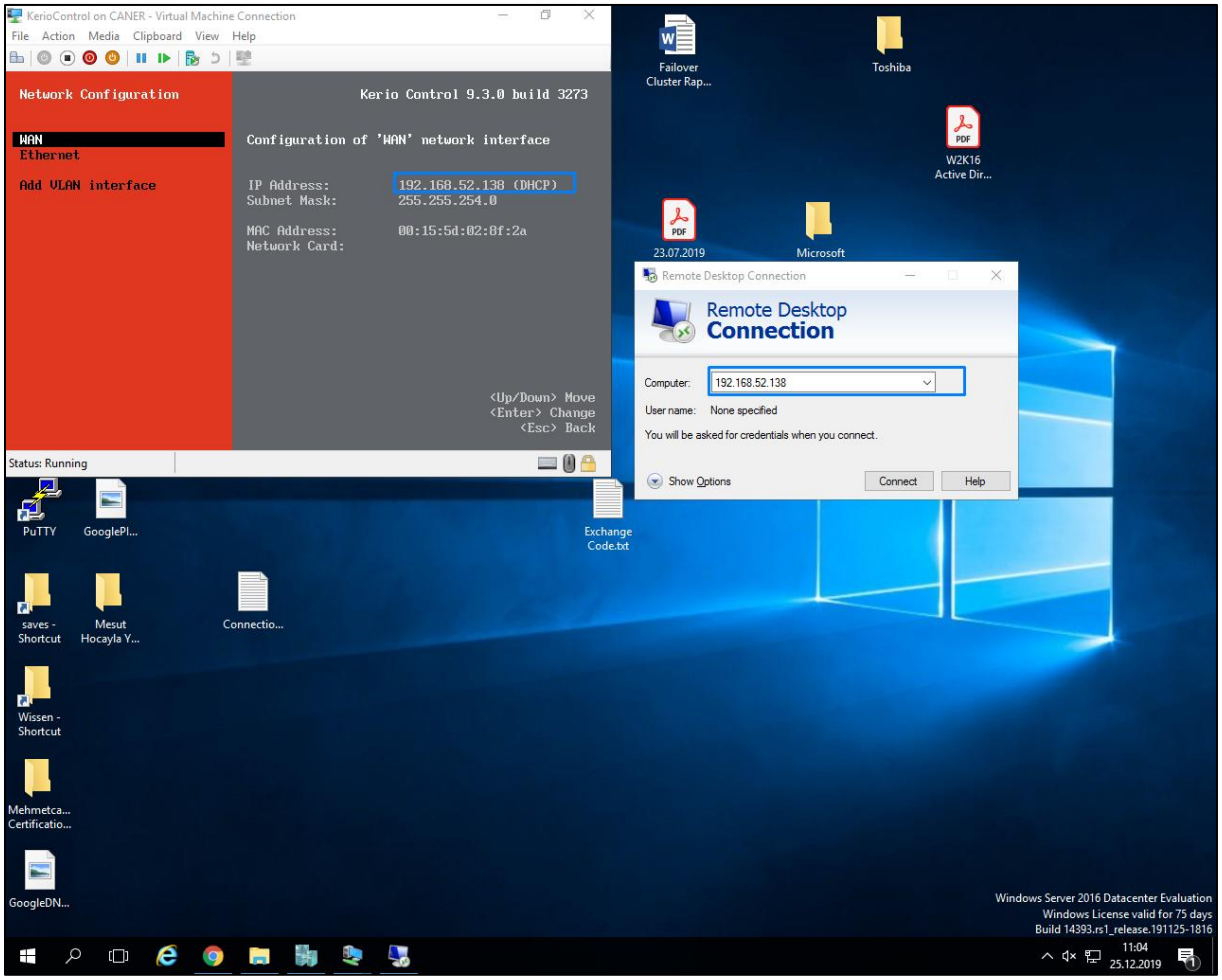


We could even use different port outside or inside of the firewall.

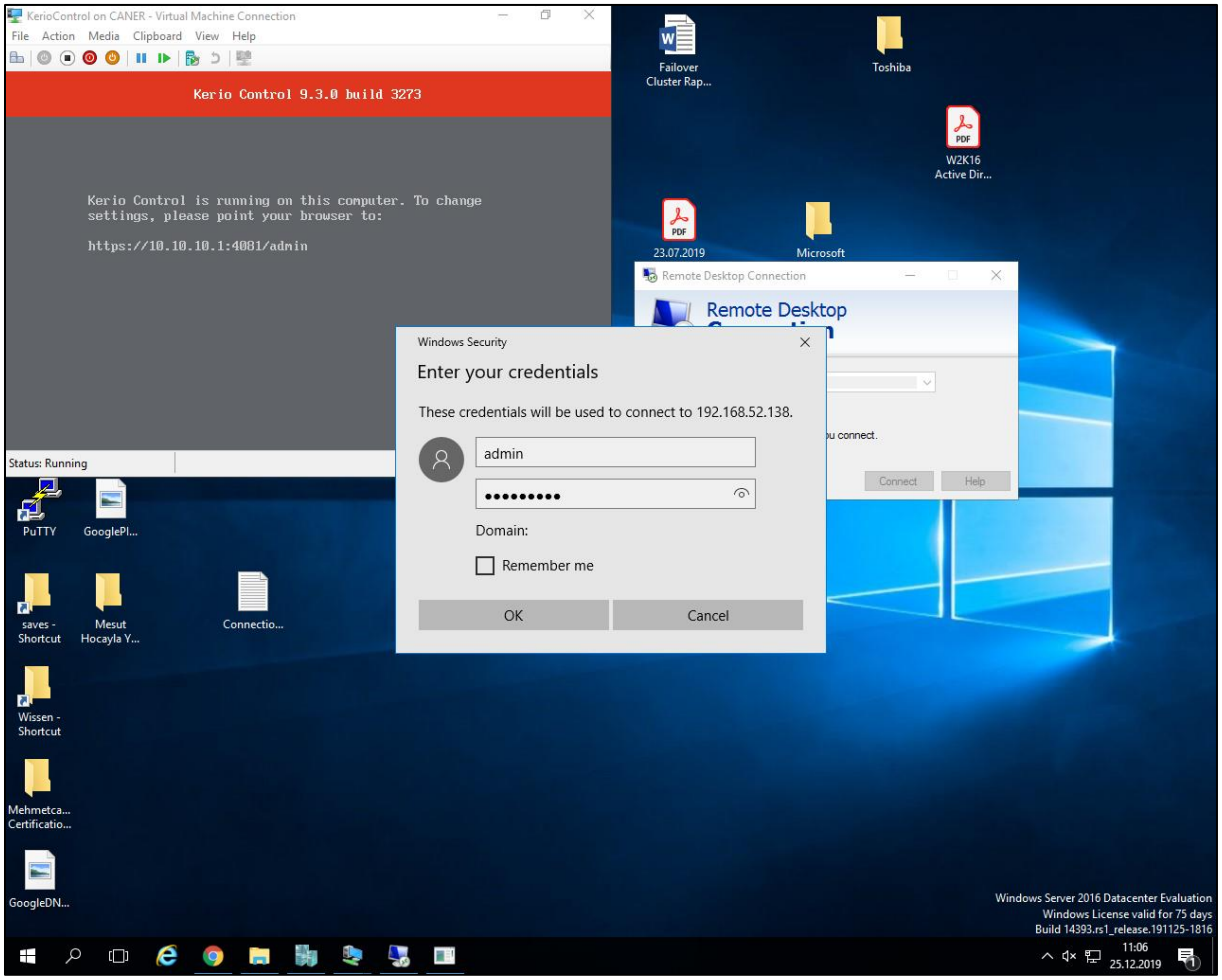


But we choose not to overcomplicate it.

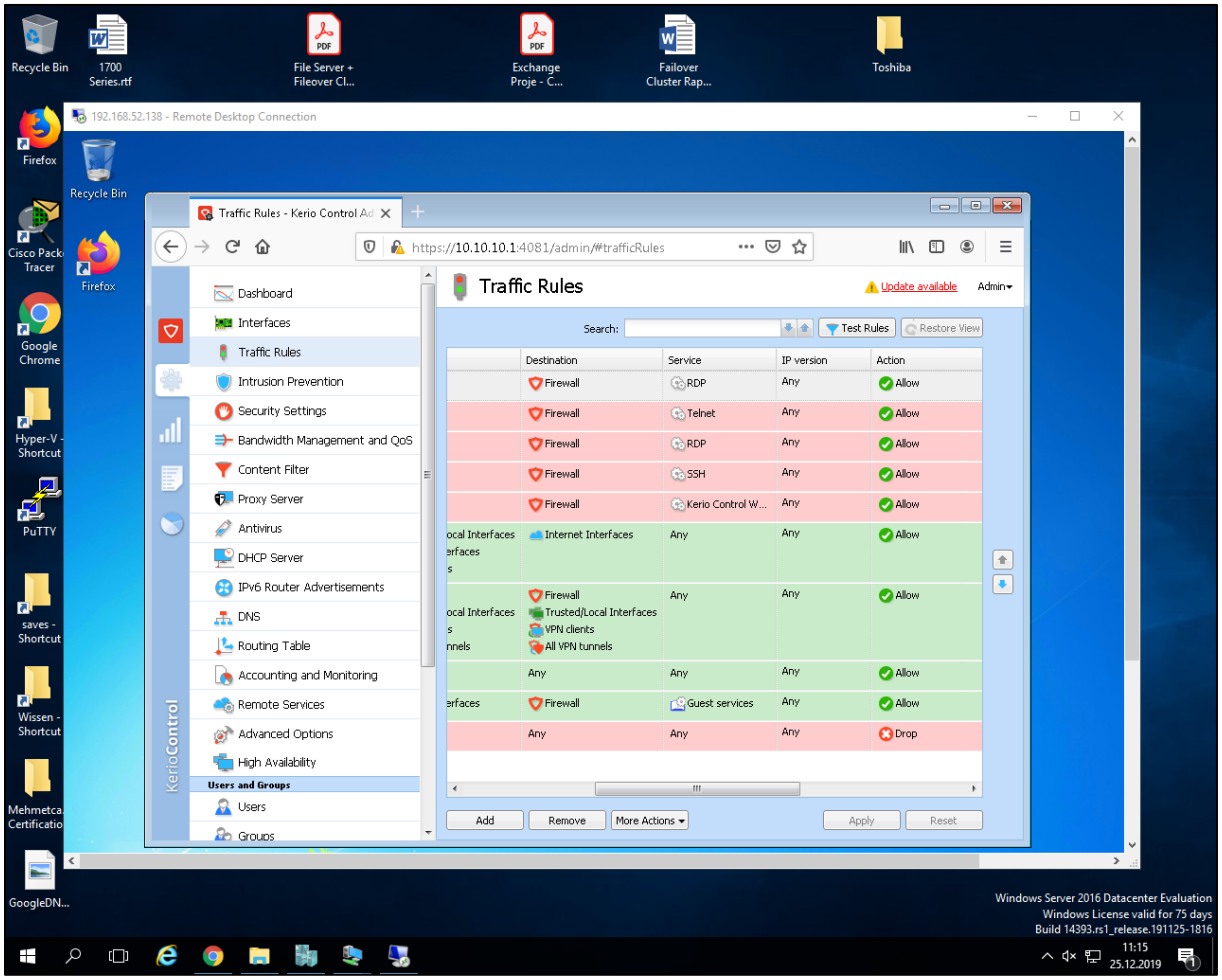
When we use RDP using the WAN IP address of the firewall, …



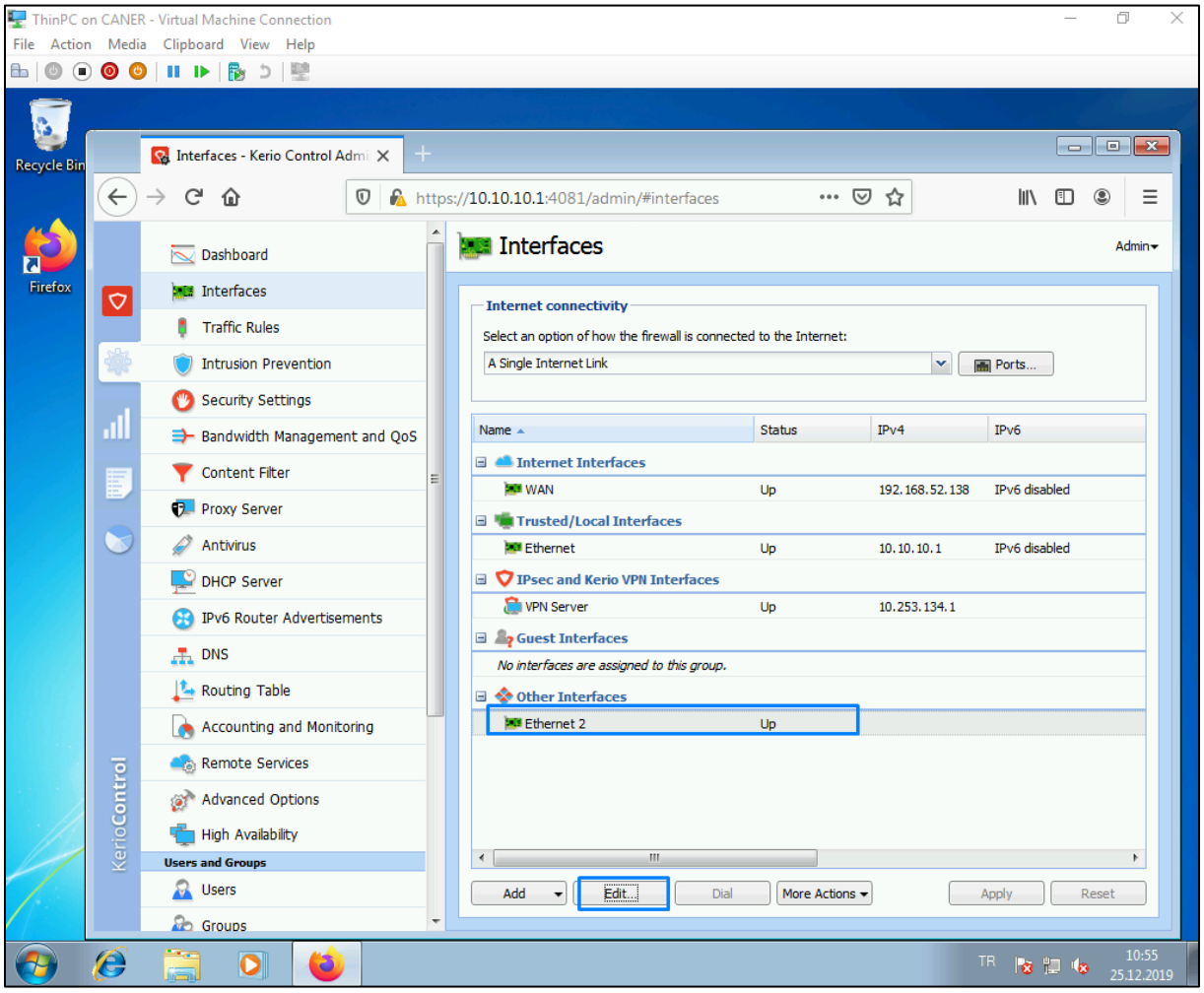
… we are asked to log in as an account of the host.



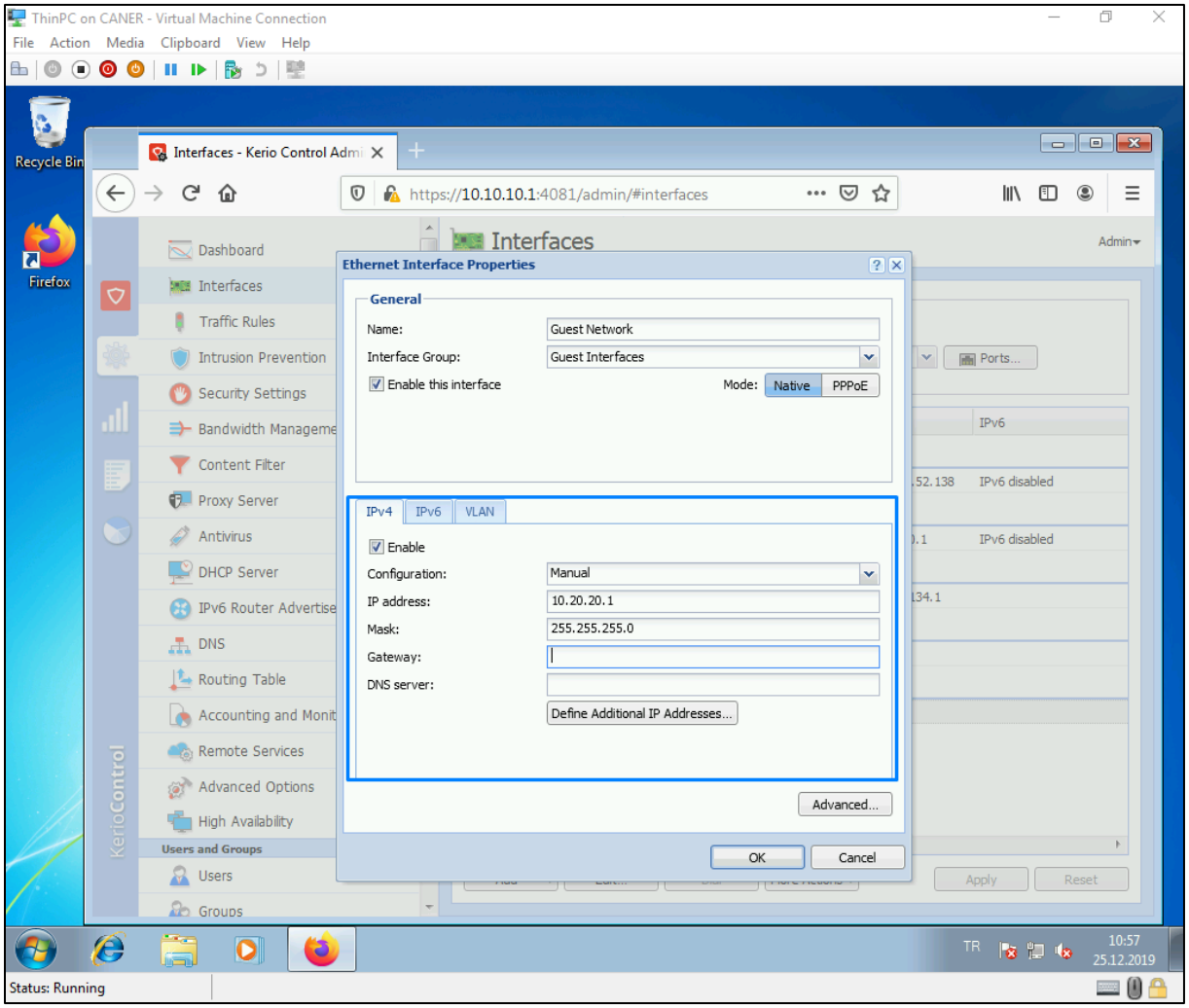
Then, we're in.


Recycle Bin
1700 Series.rtf
File Server + Fileover Cl...
Exchange Proje - C...
Failover Cluster Rap...
Toshiba
192.168.52.138 - Remote Desktop Connection
Traffic Rules - Kerio Control
https://10.10.10.1:4081/admin/#trafficRules
Traffic Rules
Update available
Admin
Search:
Test Rules
Restore View
Destination
Service
IP version
Action
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
High Availability
Users and Groups
Users
Groups
KerioControl
Add
Remove
More Actions
Apply
Reset
Windows Server 2016 Datacenter Evaluation
Windows License valid for 75 days
Build 14393.rs1_release.191125-1816
11:15
25.12.2019

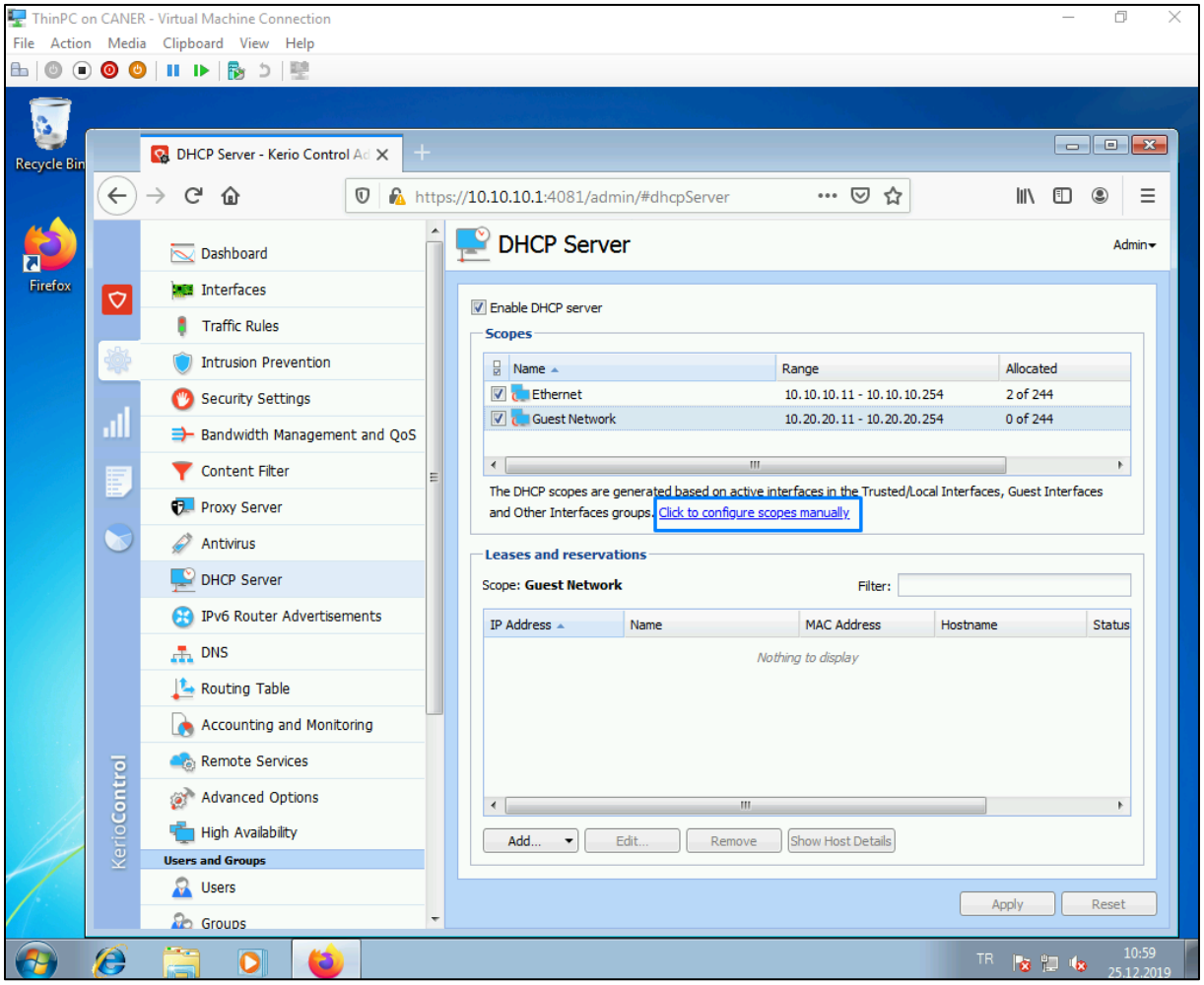
Now, we have a portal for our users but what if we also want to enable guest users to come and use the wi-fi of our company. We create a new interface.

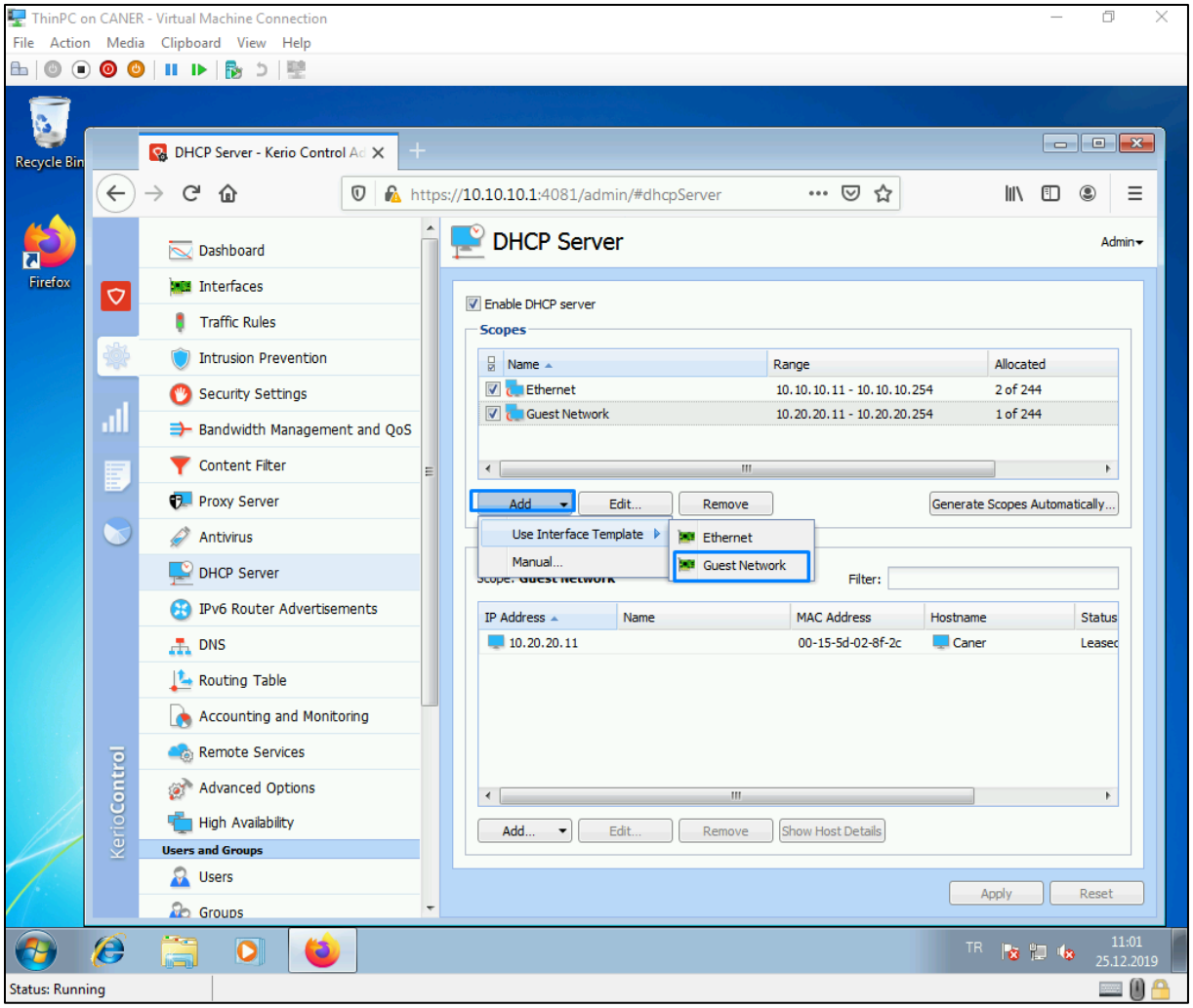


We edit it to be a guest interface and give a determined guest subnetwork.

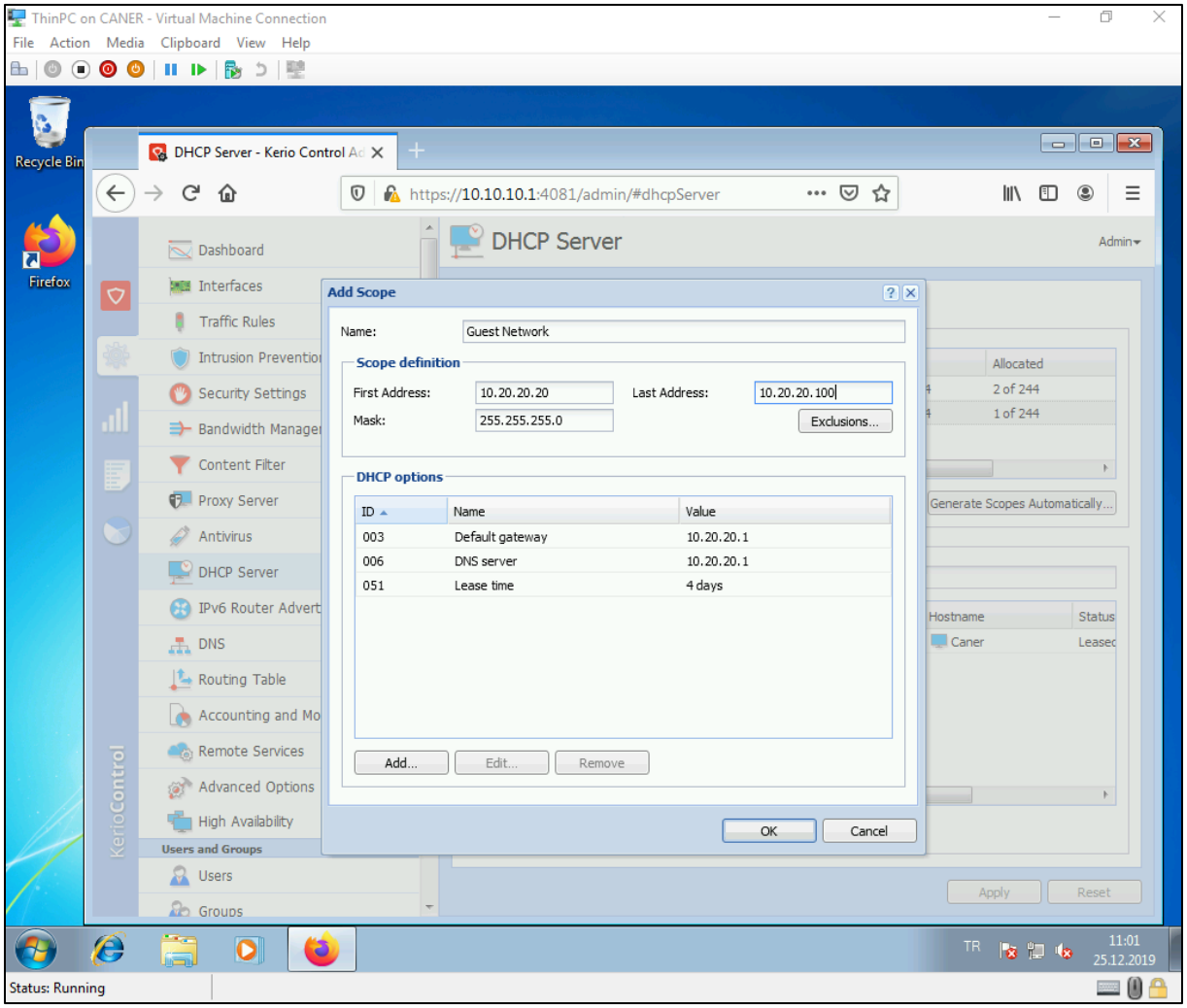


We get to the DHCP server to start a scope for the guest network as well.

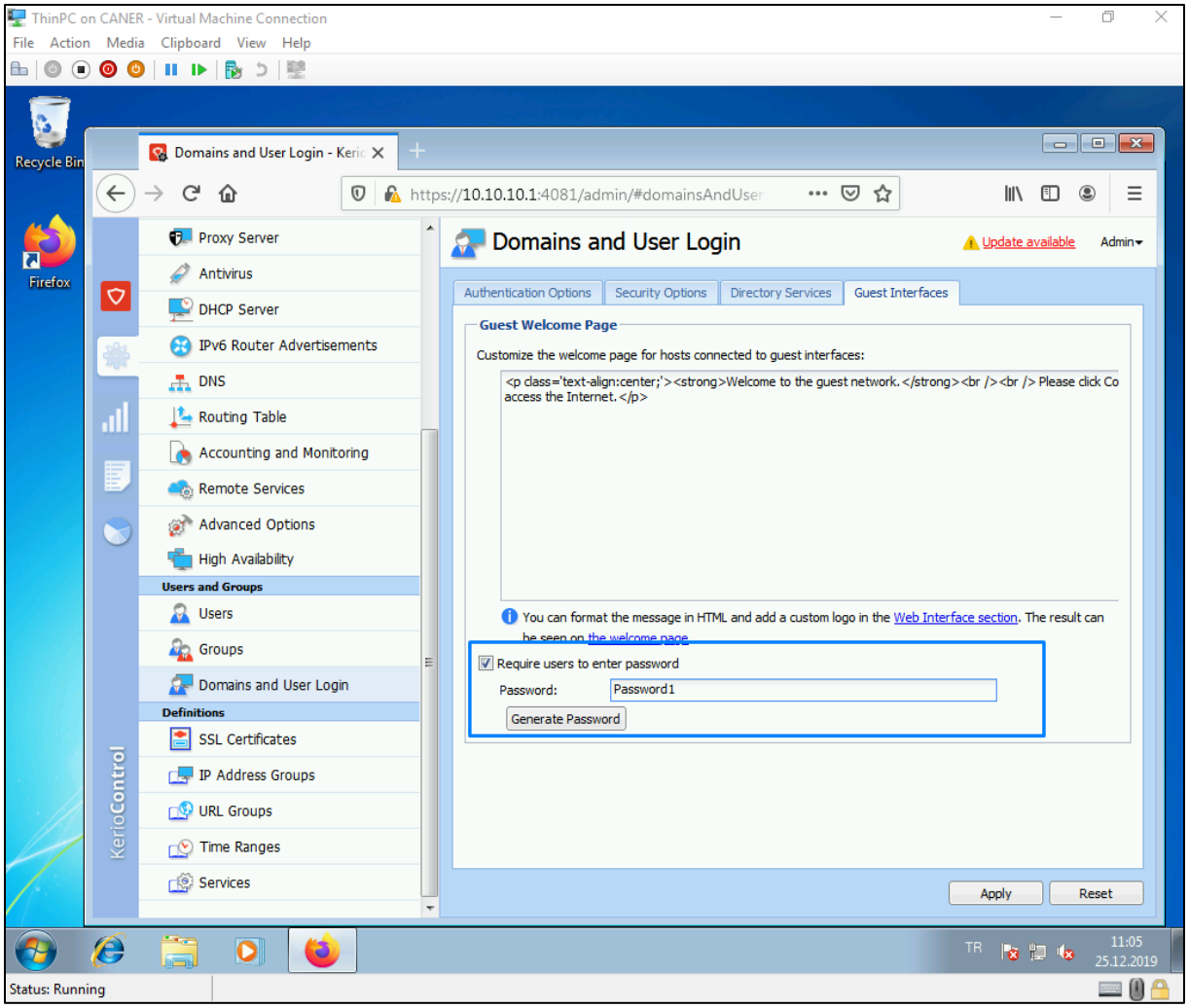



ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Firefox
DHCP Server - Kerio Control
https://10.10.10.1:4081/admin/#dhcpServer
Dashboard
Interfaces
Traffic Rules
Intrusion Prevention
Security Settings
Bandwidth Management and QoS
Content Filter
Proxy Server
Antivirus
DHCP Server
IPv6 Router Advertisements
DNS
Routing Table
Accounting and Monitoring
Remote Services
Advanced Options
High Availability
Users and Groups
Users
Groups
KerioControl
DHCP Server
Admin
Enable DHCP server
Scopes
Name
Range
Allocated
Ethernet
10.10.10.11 - 10.10.10.254
2 of 244
Guest Network
10.20.20.11 - 10.20.20.254
1 of 244
Add...
Edit...
Remove
Generate Scopes Automatically...
Use Interface Template
Manual...
Ethernet
Guest Network
Filter:
IP Address
Name
MAC Address
Hostname
Status
10.20.20.11
00-15-5d-02-8f-2c
Caner
Leased
Add...
Edit...
Remove
Show Host Details
Apply
Reset
TR
11:01
25.12.2019
Status: Running

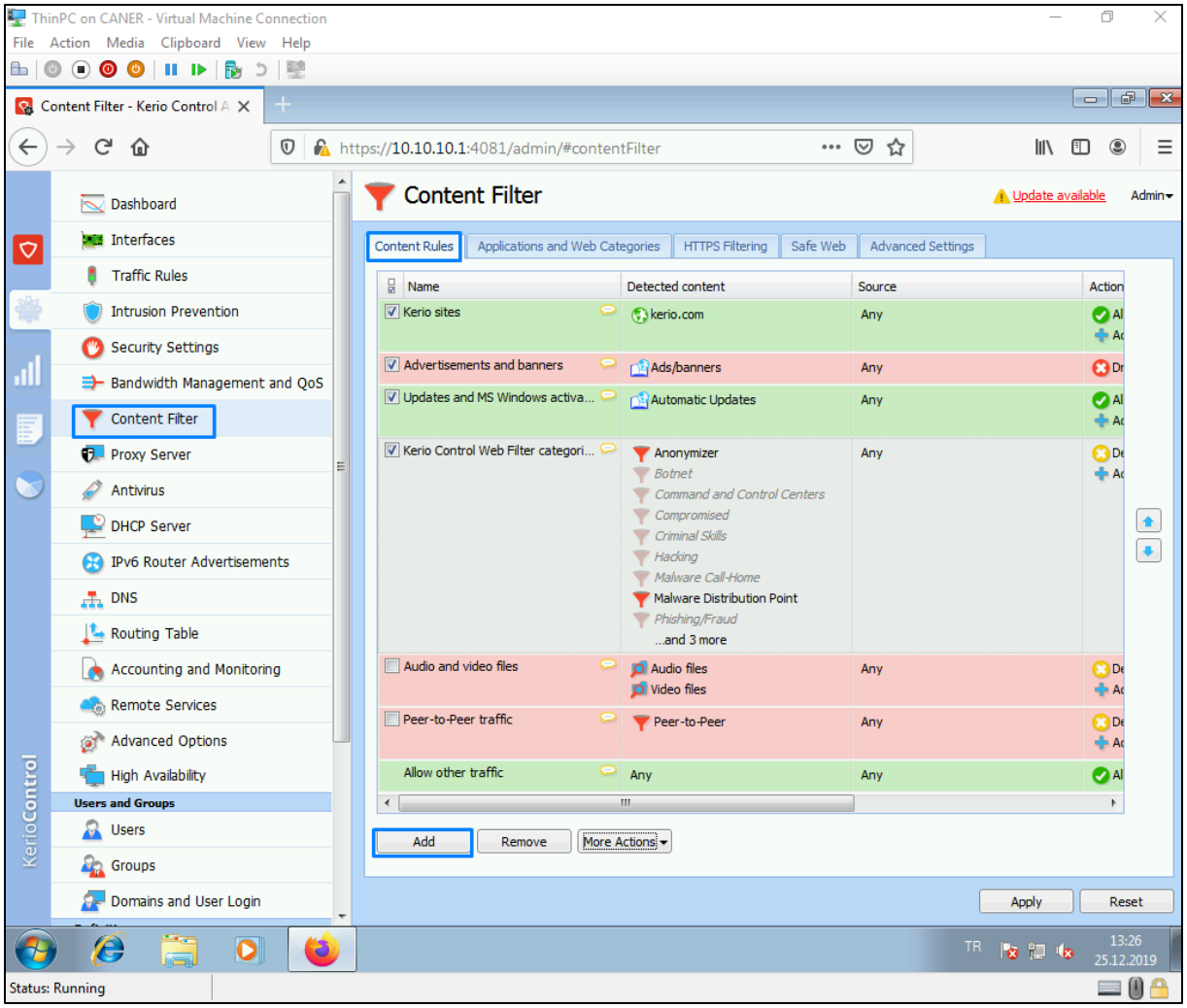
We determine the start and the end of the scope.



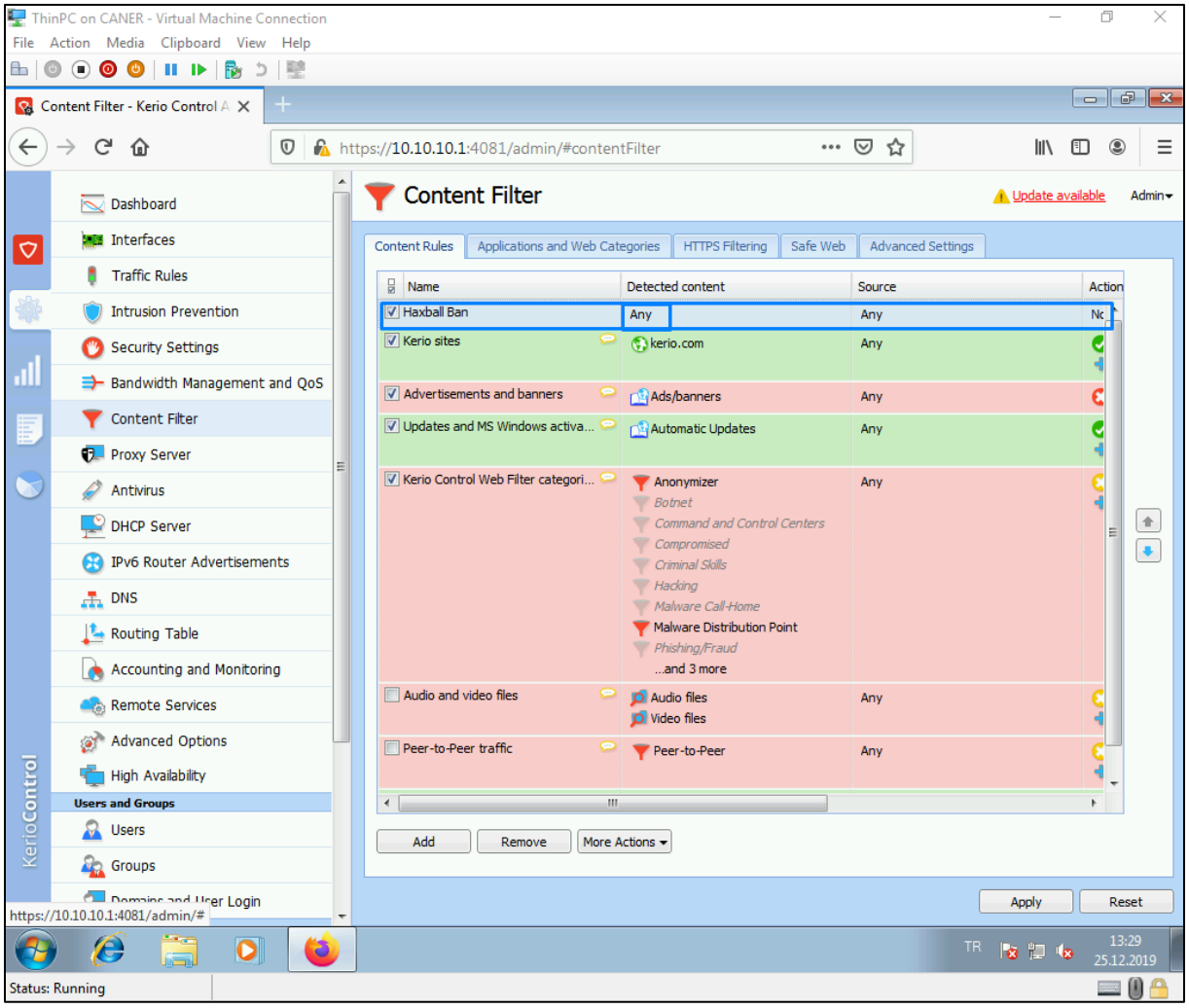
We, then require all of the guests to enter a password to connect.



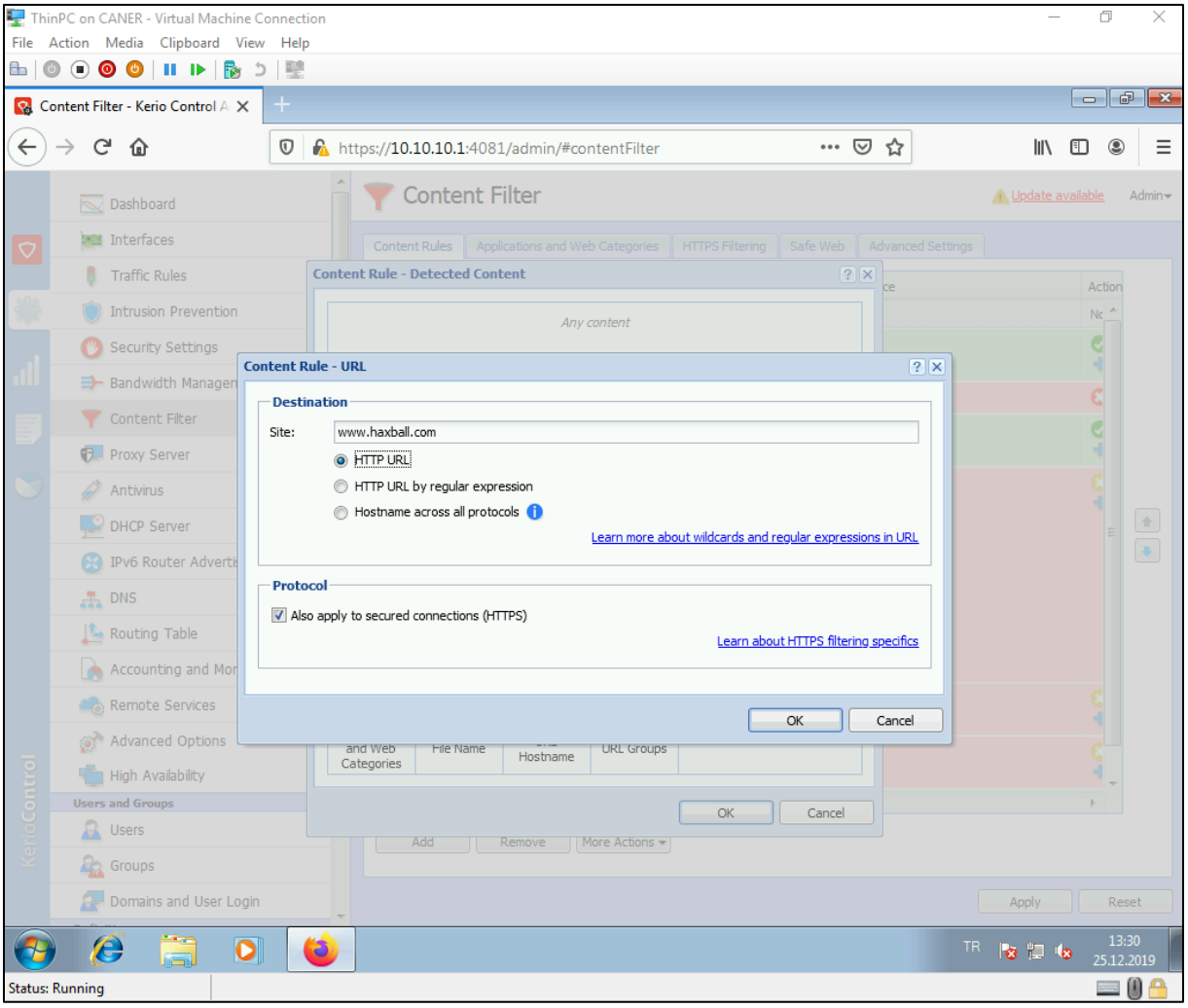
Now, let’s ban access to some certain gaming websites so that work efficiency is optimal.



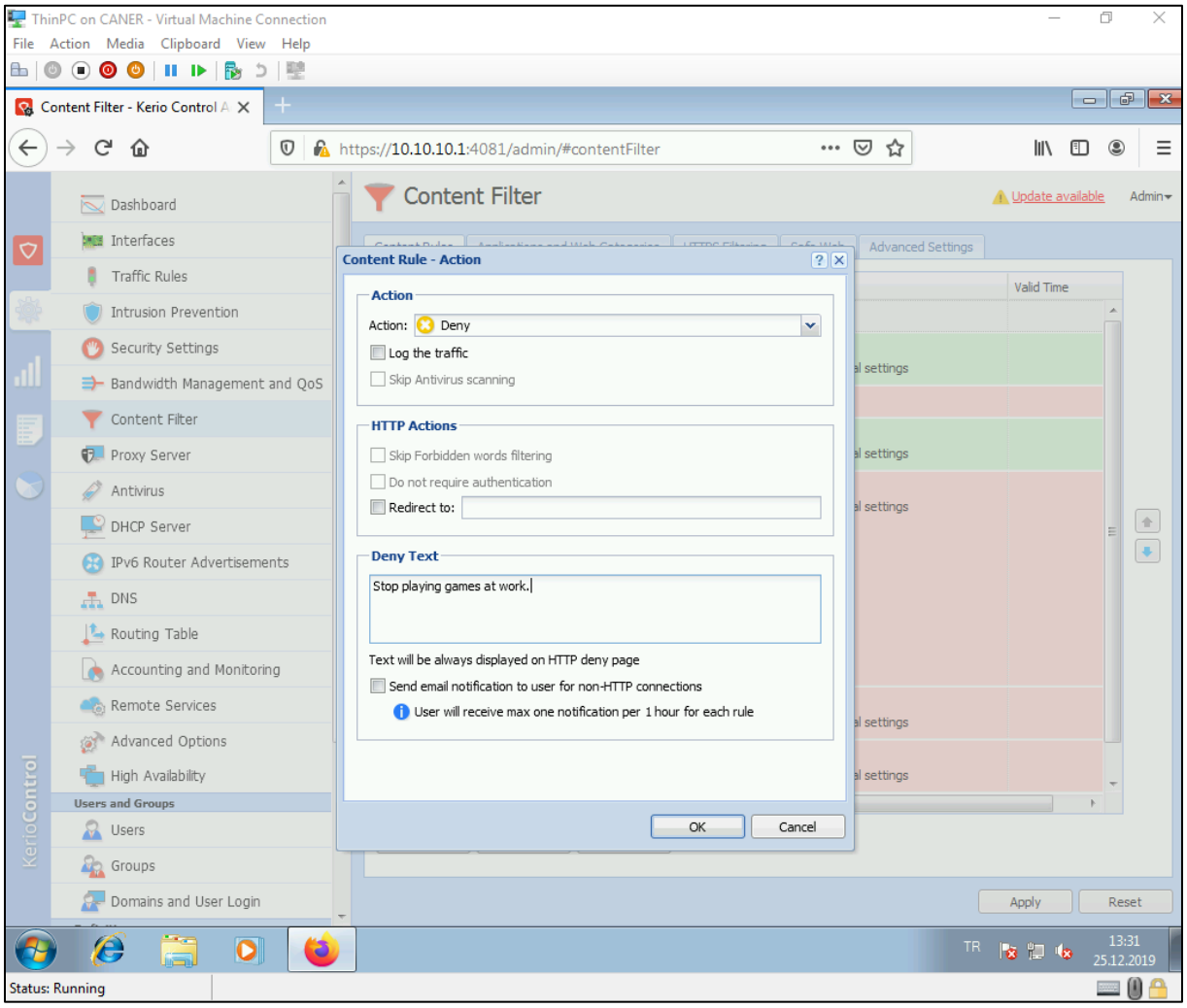
We create a new content rule and edit it.



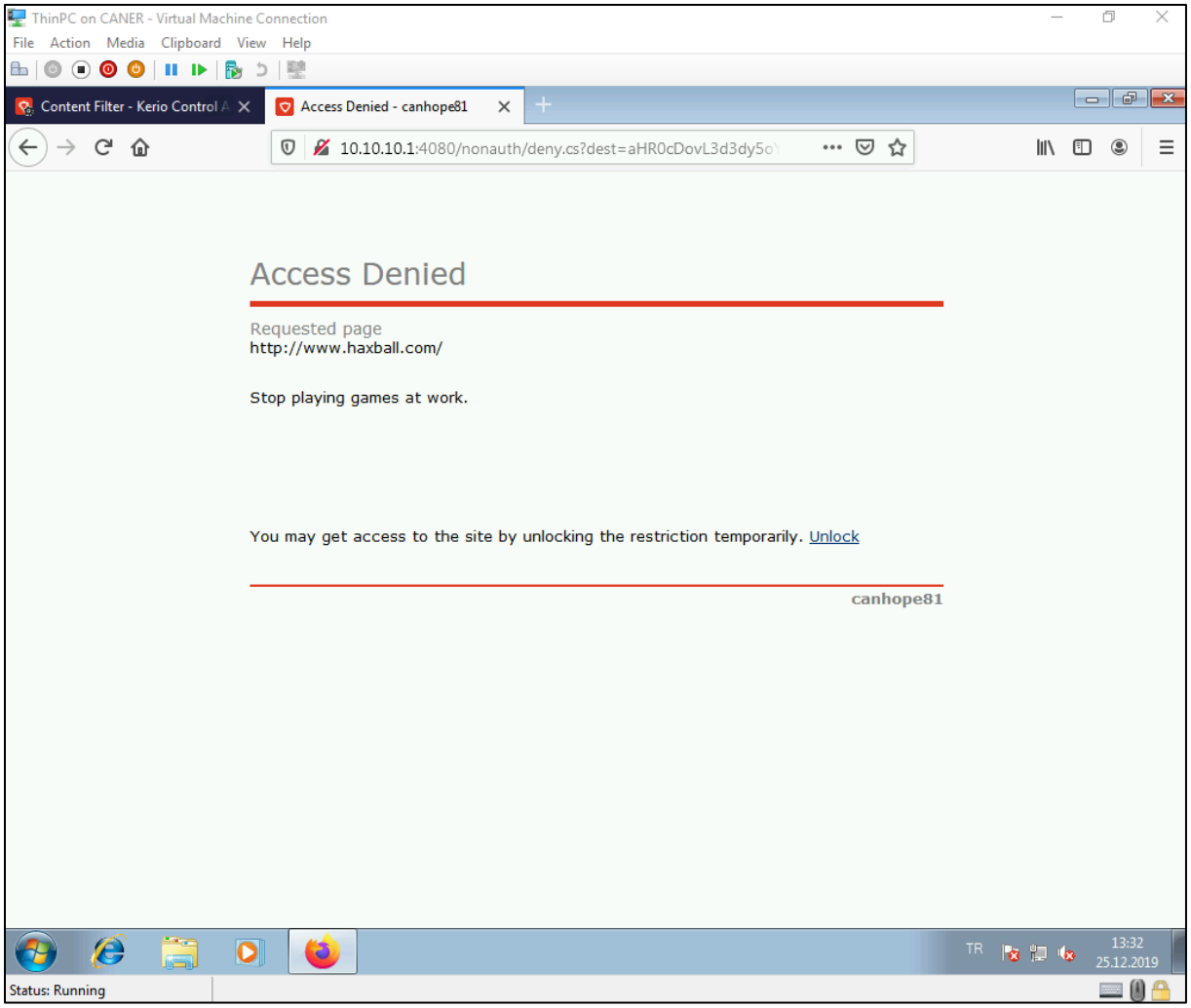
We apply it to the destination of www.haxball.com .



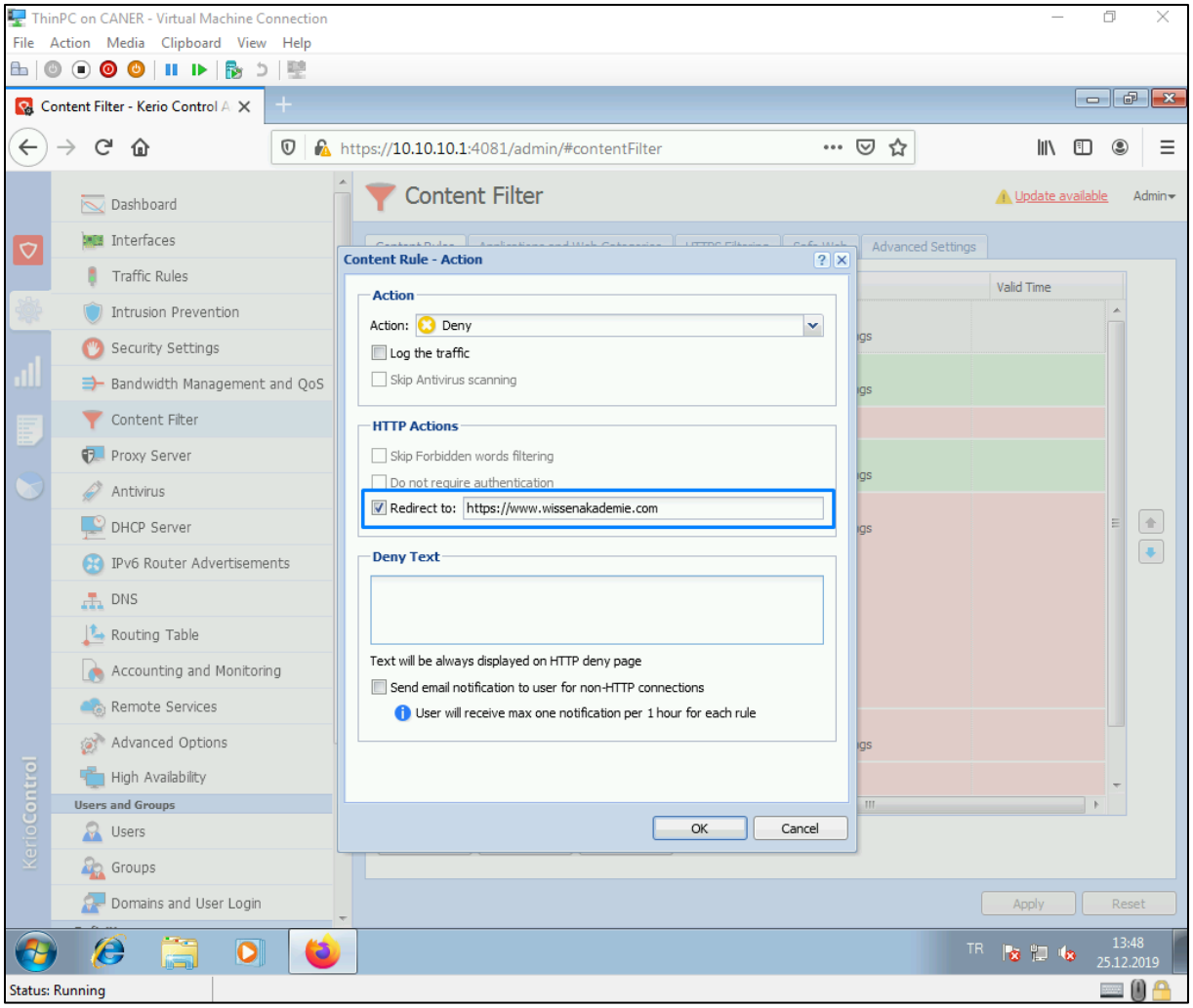
We choose the action to DENY access and let them know that we know they just tried to play games while at work. We could also use the action to DROP to not show a page that says we blocked access. That might also frustrate them to try over and over again. Since we believe that would be a waste of valuable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

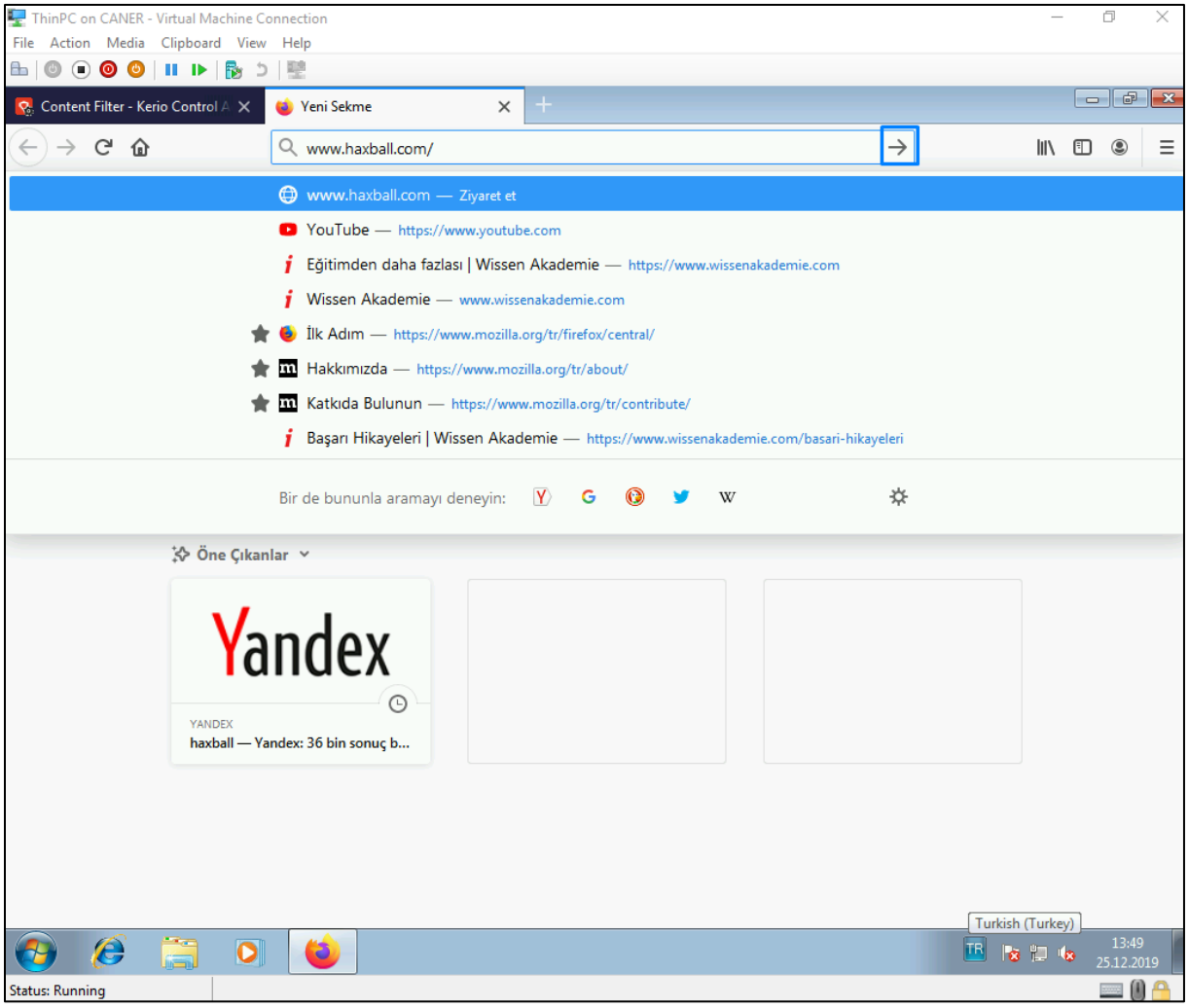


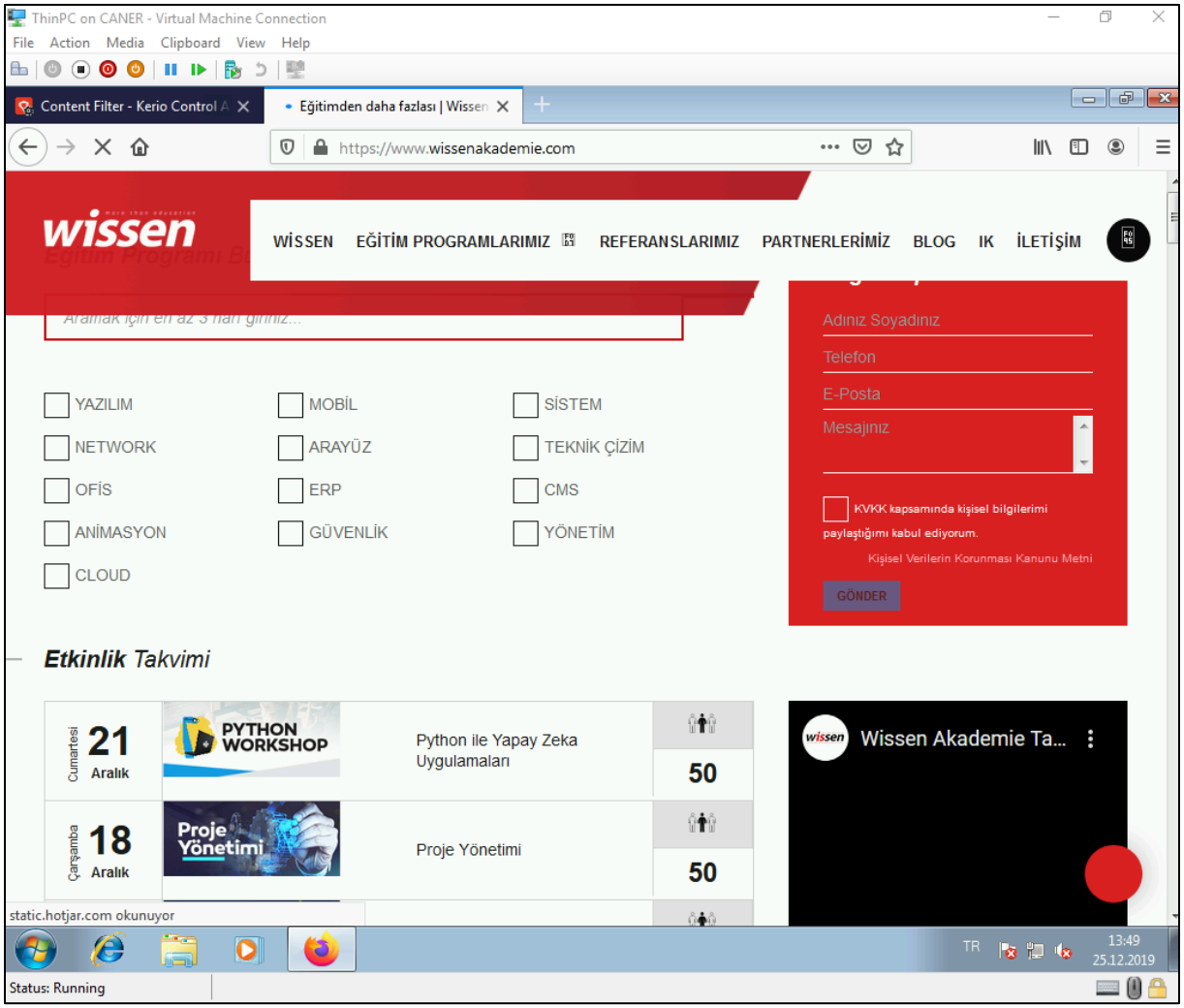
When the user tries to connect to the website, they see this page instead.



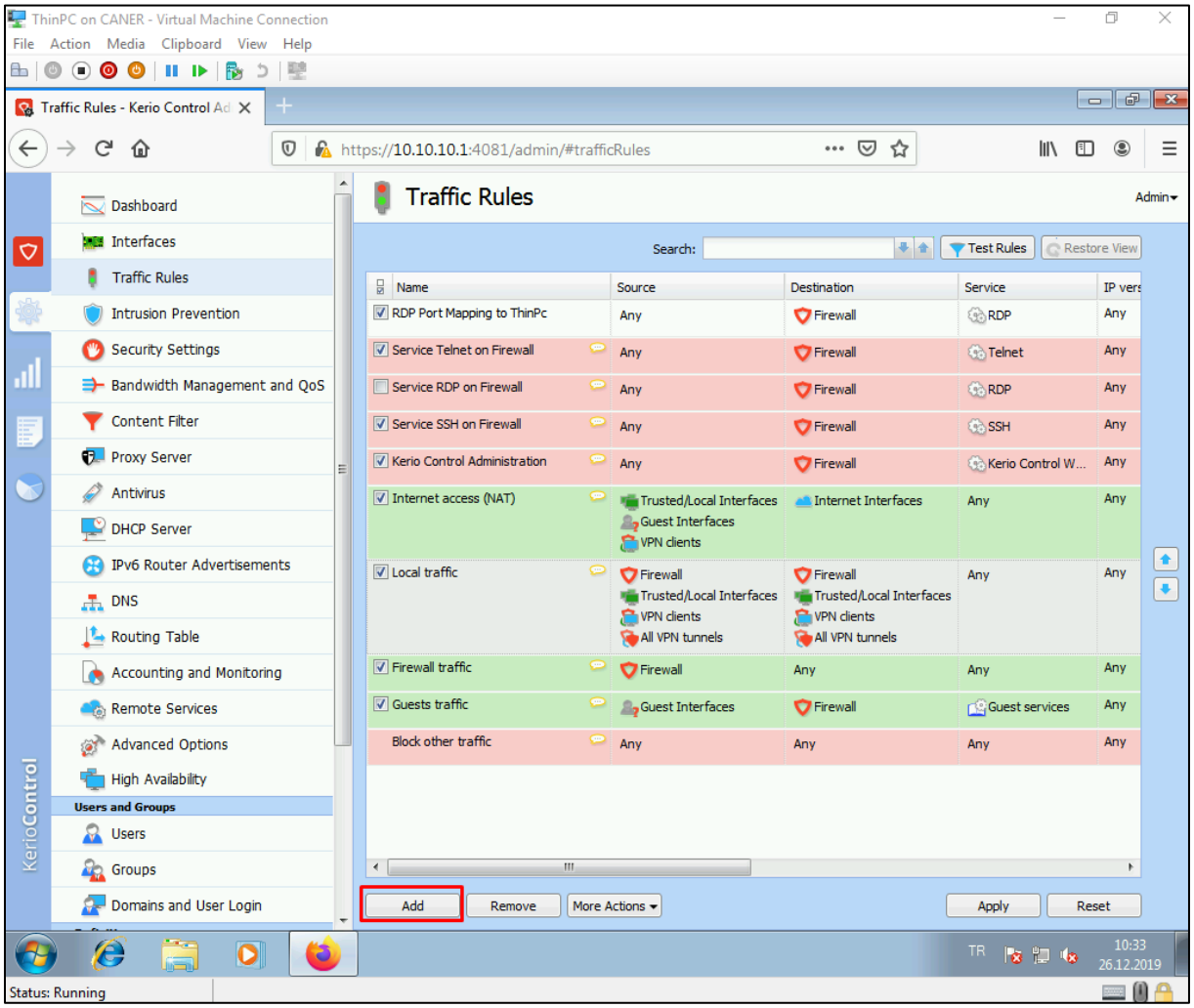
We could also redirect the traffic to our company's website.



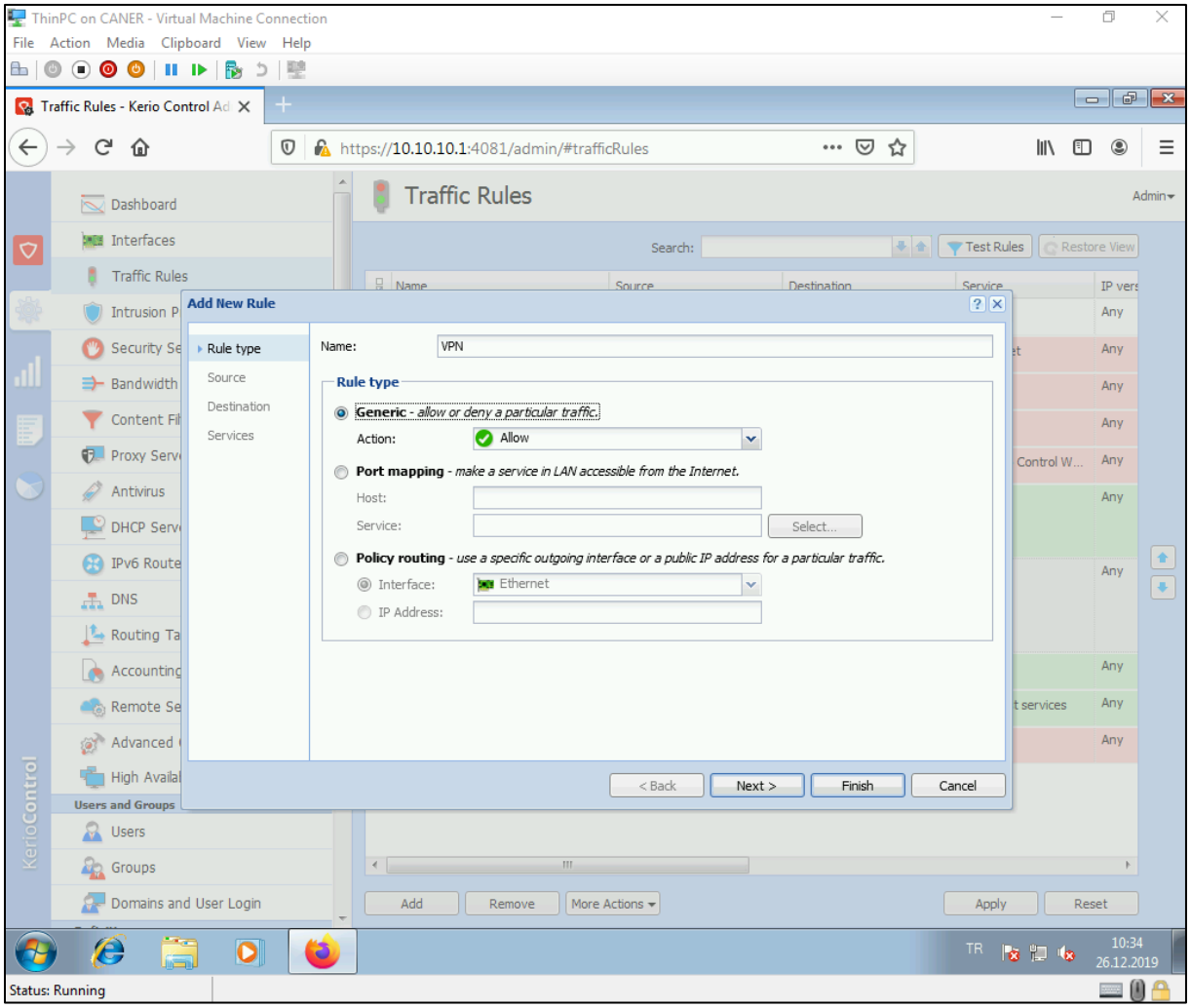

ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Content Filter - Kerio Control
Yeni Sekme
www.haxball.com/
www.haxball.com — Ziyaret et
YouTube — https://www.youtube.com
Eğitimden daha fazlası | Wissen Akademie — https://www.wissenakademie.com
Wissen Akademie — www.wissenakademie.com
İlk Adım — https://www.mozilla.org/tr/firefox/central/
Hakkımızda — https://www.mozilla.org/tr/about/
Katkıda Bulunun — https://www.mozilla.org/tr/contribute/
Başarı Hikayeleri | Wissen Akademie — https://www.wissenakademie.com/basari-hikayeleri
Bir de bununla aramayı deneyin:
Öne Çıkanlar
Yandex
YANDEX
haxball — Yandex: 36 bin sonuç b...
Turkish (Turkey)
TR
13:49
25.12.2019
Status: Running


ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Content Filter - Kerio Control
Eğitimden daha fazlası | Wissen
https://www.wissenakademie.com
wissen
WİSSEN EĞİTİM PROGRAMLARIMIZ REFERANSLARIMIZ PARTNERLERİMİZ BLOG IK İLETİŞİM
YAZILIM
MOBİL
SİSTEM
NETWORK
ARAYÜZ
TEKNİK ÇİZİM
OFİS
ERP
CMS
ANİMASYON
GÜVENLİK
YÖNETİM
CLOUD
Adınız Soyadınız
Telefon
E-Posta
Mesajınız
KVKK kapsamında kişisel bilgilerimi paylaştığımı kabul ediyorum.
Kişisel Verilerin Korunması Kanunu Metni
GÖNDER
Etkinlik Takvimi
Cumartesi 21 Aralık
PYTHON WORKSHOP
Python ile Yapay Zeka Uygulamaları
50
Çarşamba 18 Aralık
Proje Yönetimi
Proje Yönetimi
50
Wissen Akademie Ta...
static.hotjar.com okunuyor
TR
13:49
25.12.2019
Status: Running

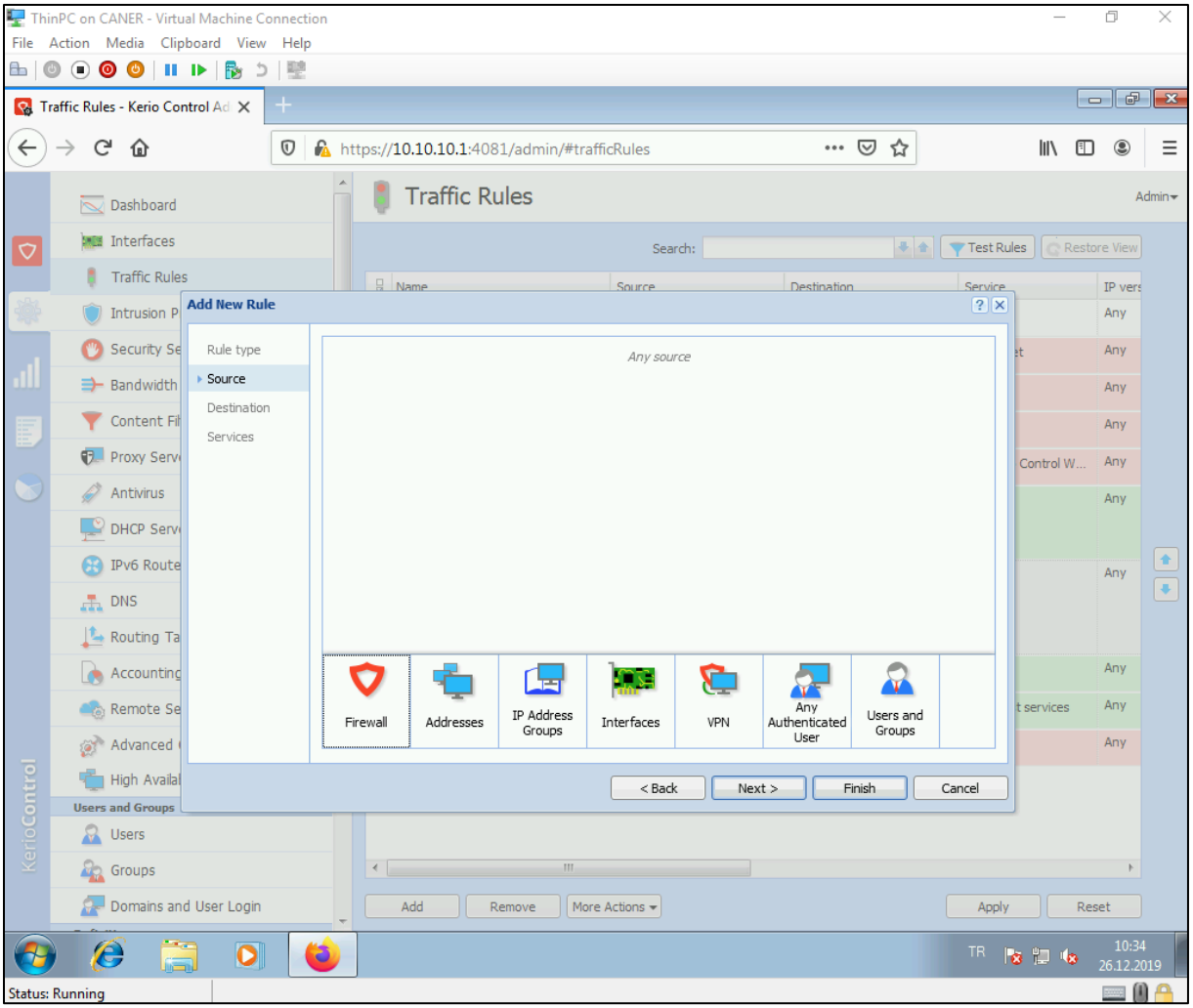
Now, let’s try setting a VPN connection to another site that uses Kerio Control also known as a site-to-site VPN. First thing to do is to allow the traffic rules for it.



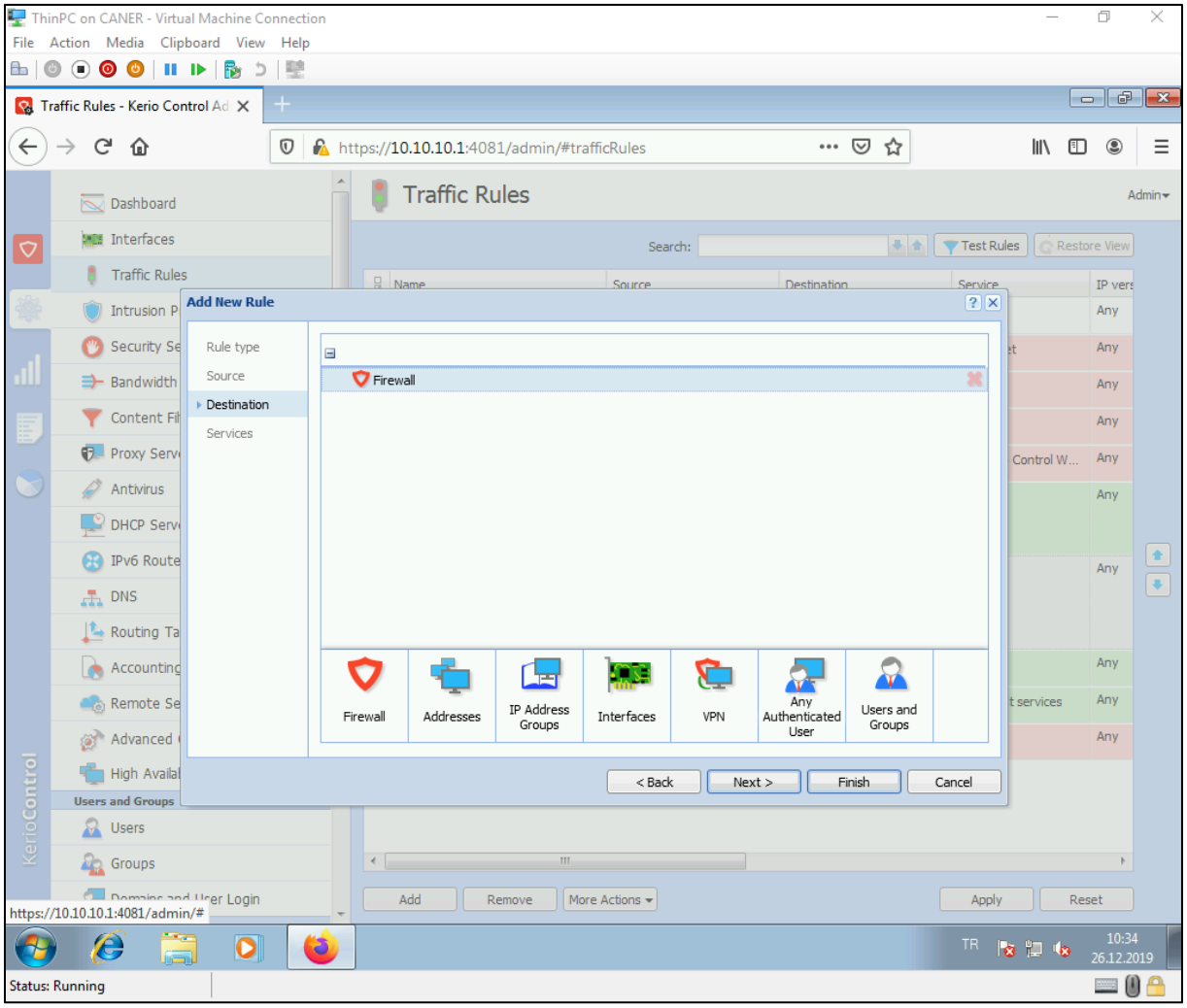
We set ALLOW as the action, …



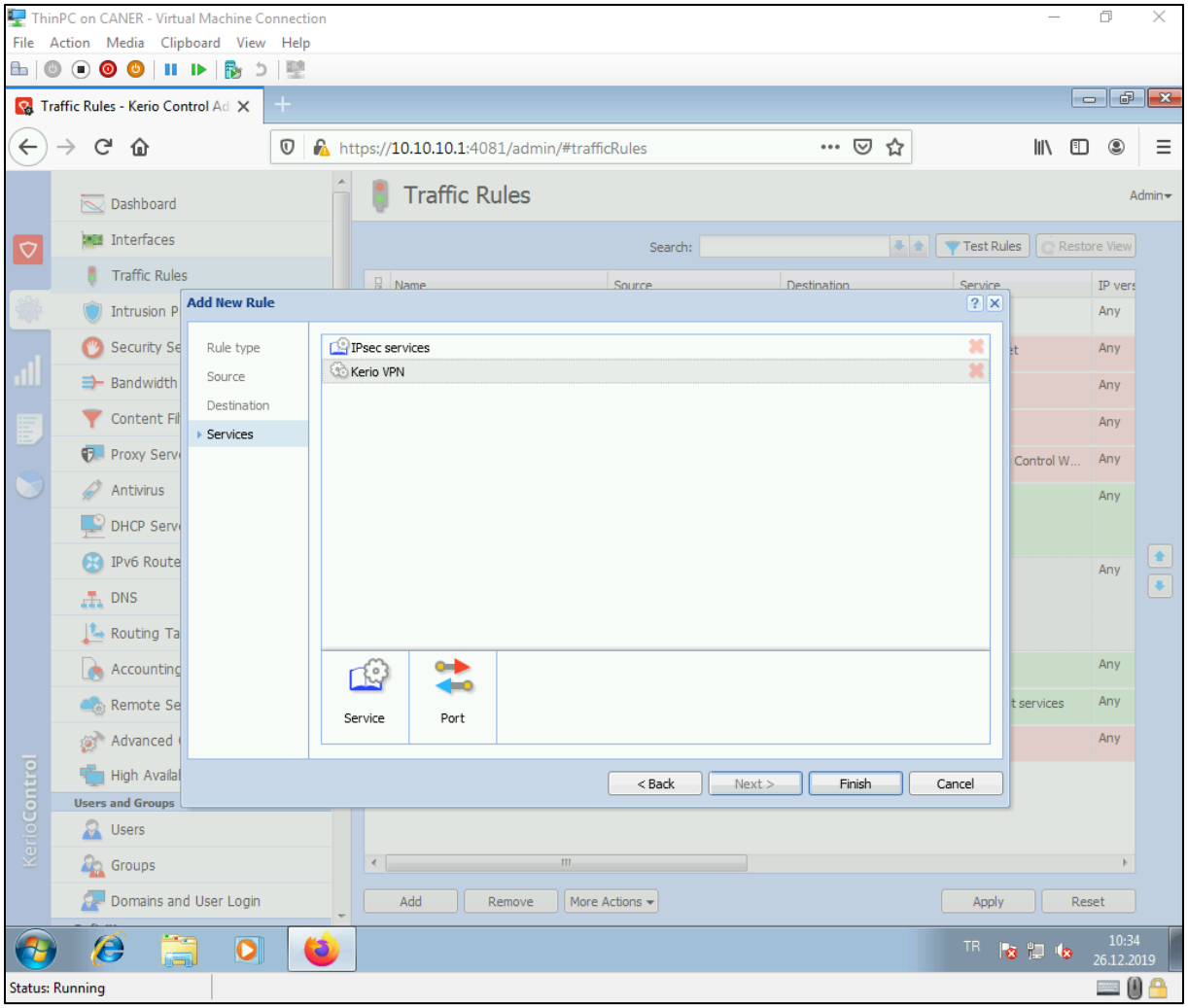
… source as any, …



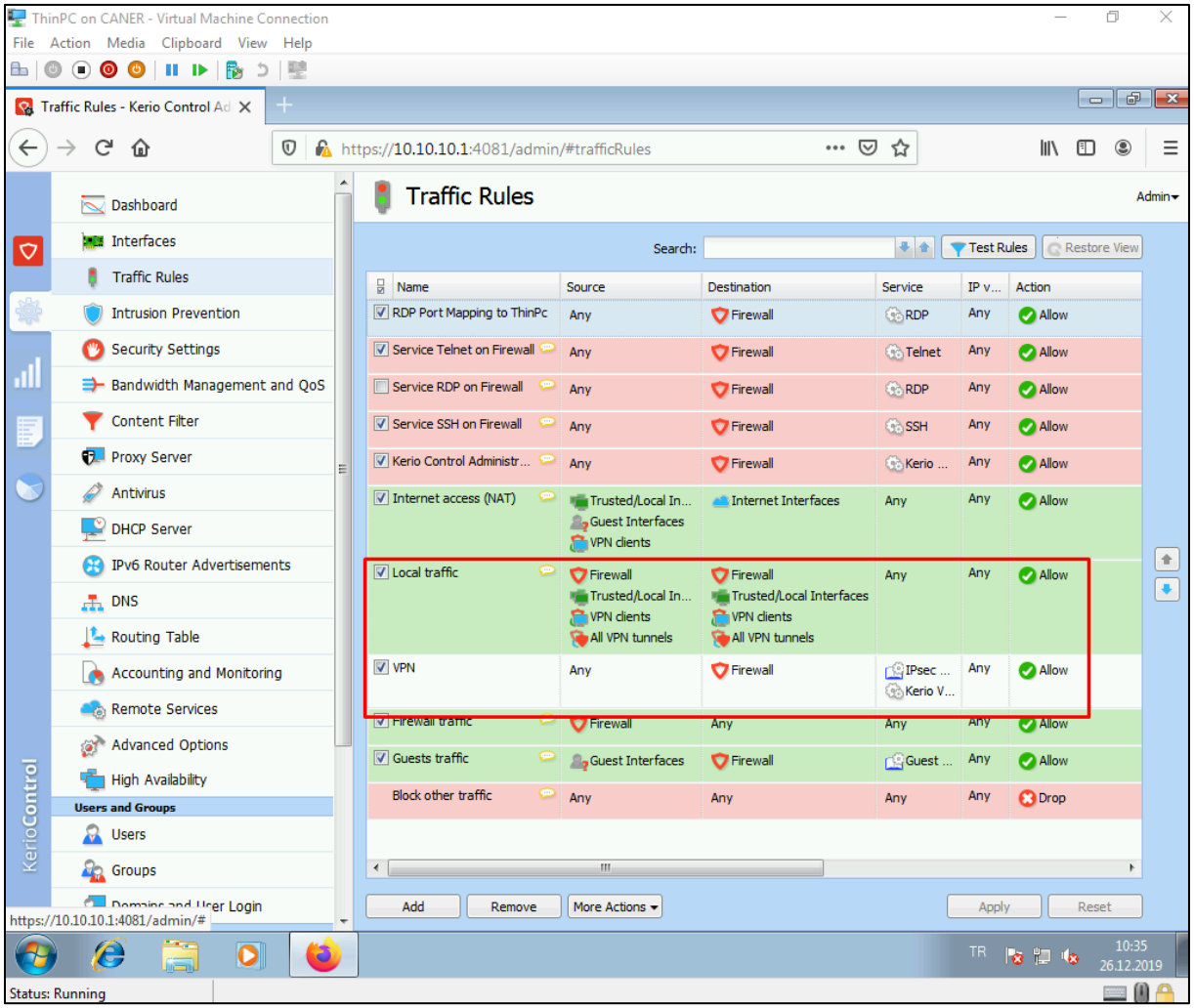
… this firewall as destination …



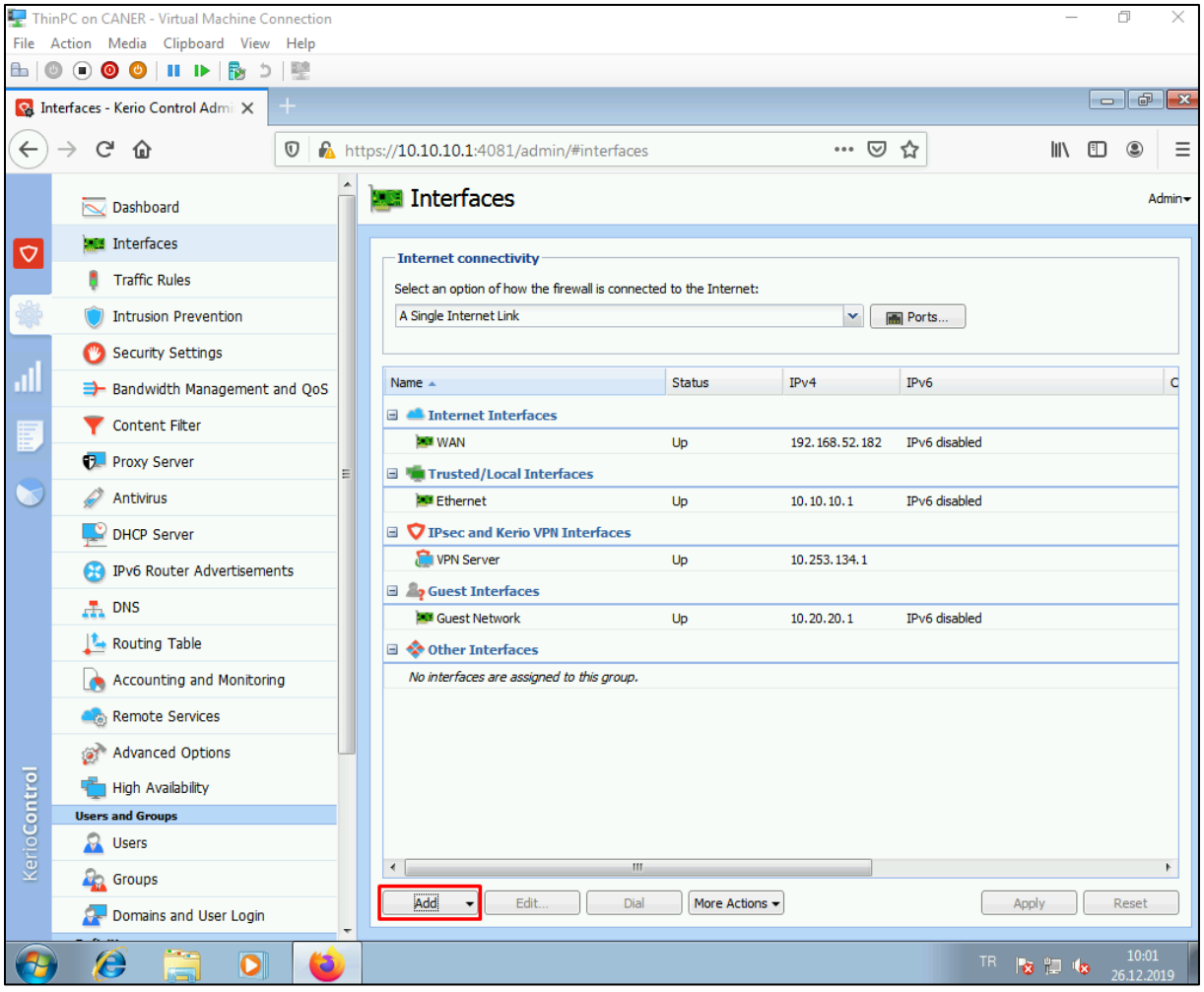
… and only Kerio VPN and IPSec as services for this rule.



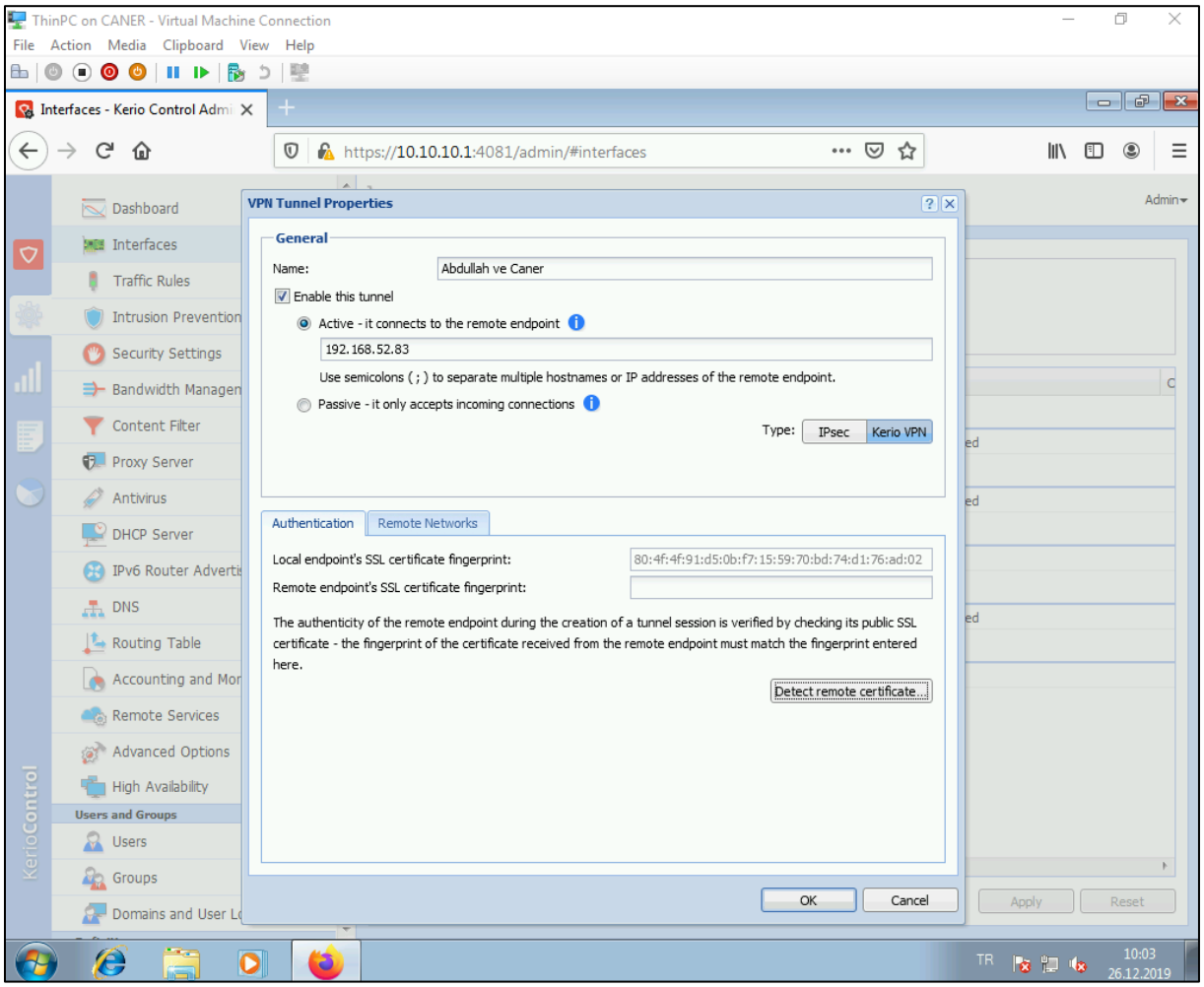
We also allow the local traffic as demonstrated. This completes the necessary rules.



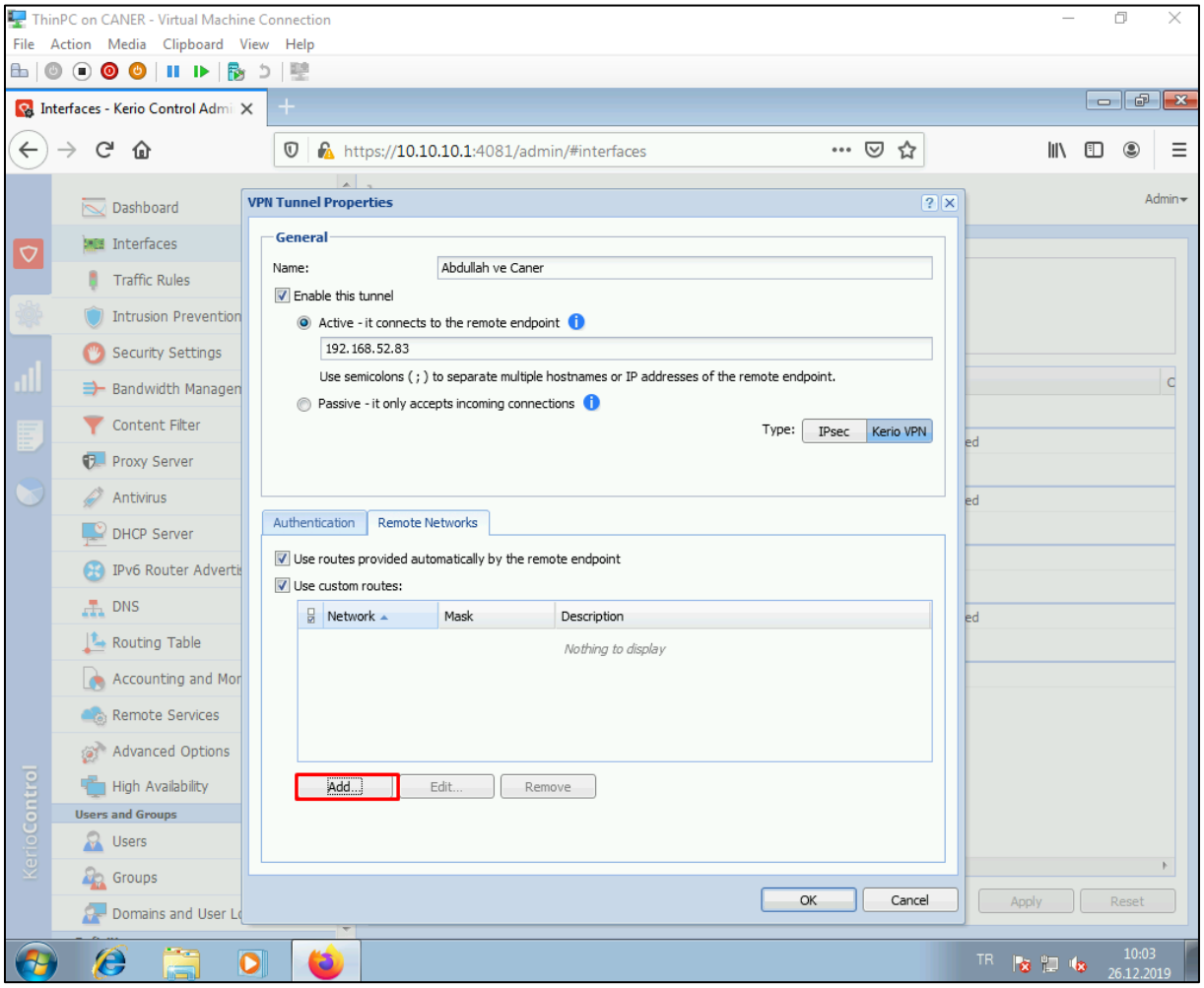
After that, we need to add a new interface for our tunnel.



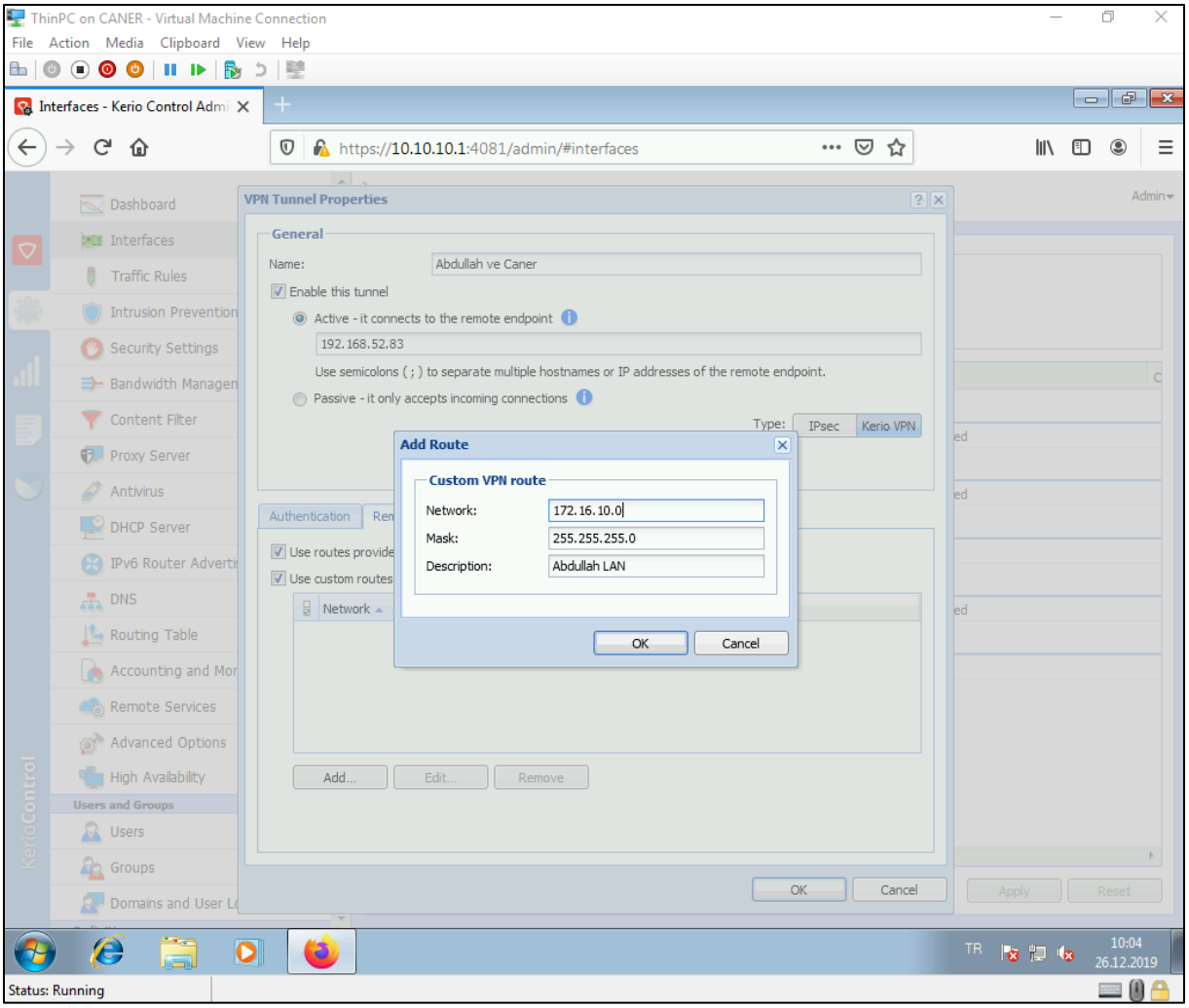
We name the tunnel and enable it. Depending on your network topology, the site might be active or passive. If it’s an active site then you need to enter the public IP address of the other site. At least, one of the sites must be active to establish the connection.



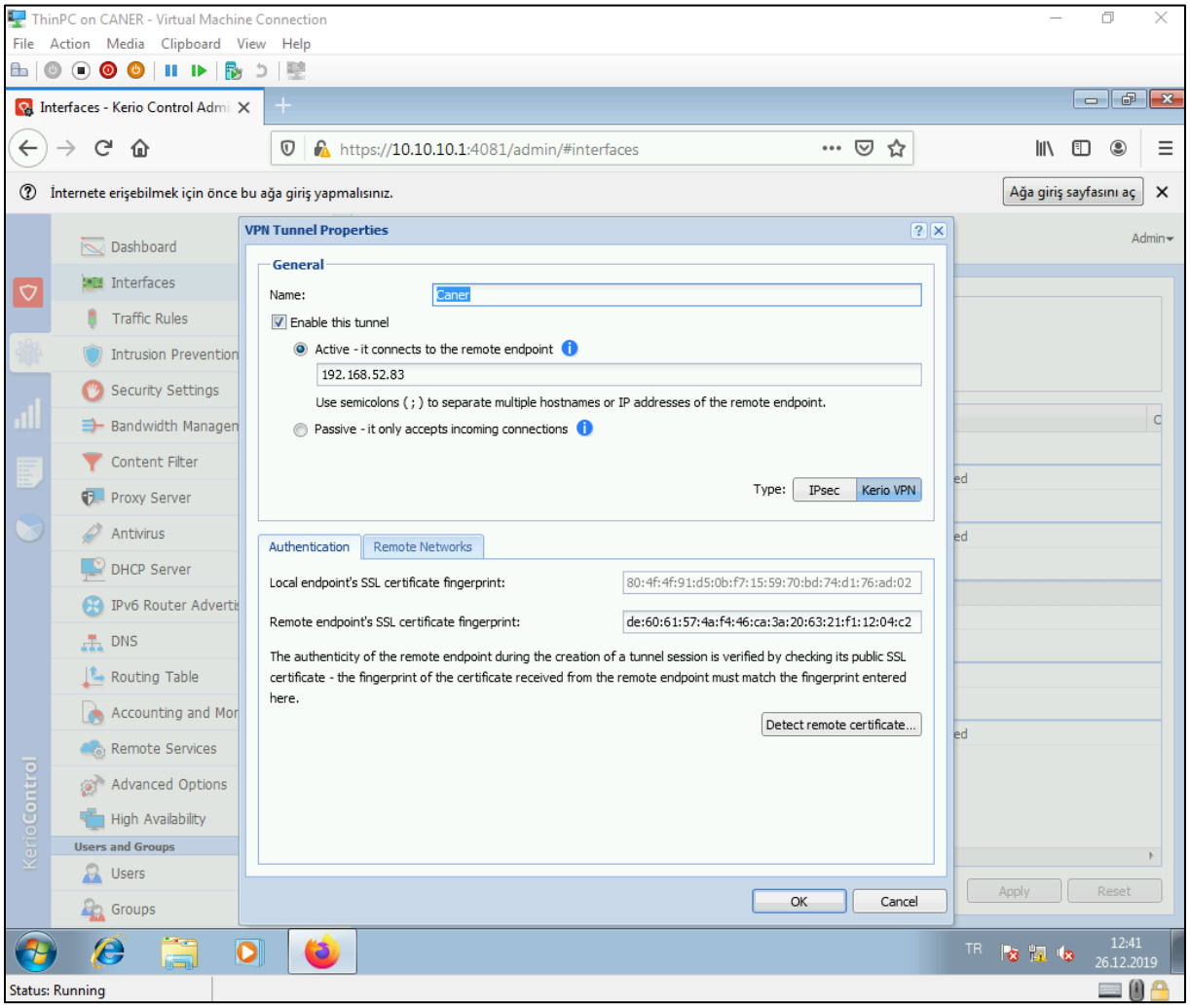
We then get to the remote networks tab and add the unknown internal networks of the partner site that you want to establish the VPN with.



This is the LAN network of the partner site.

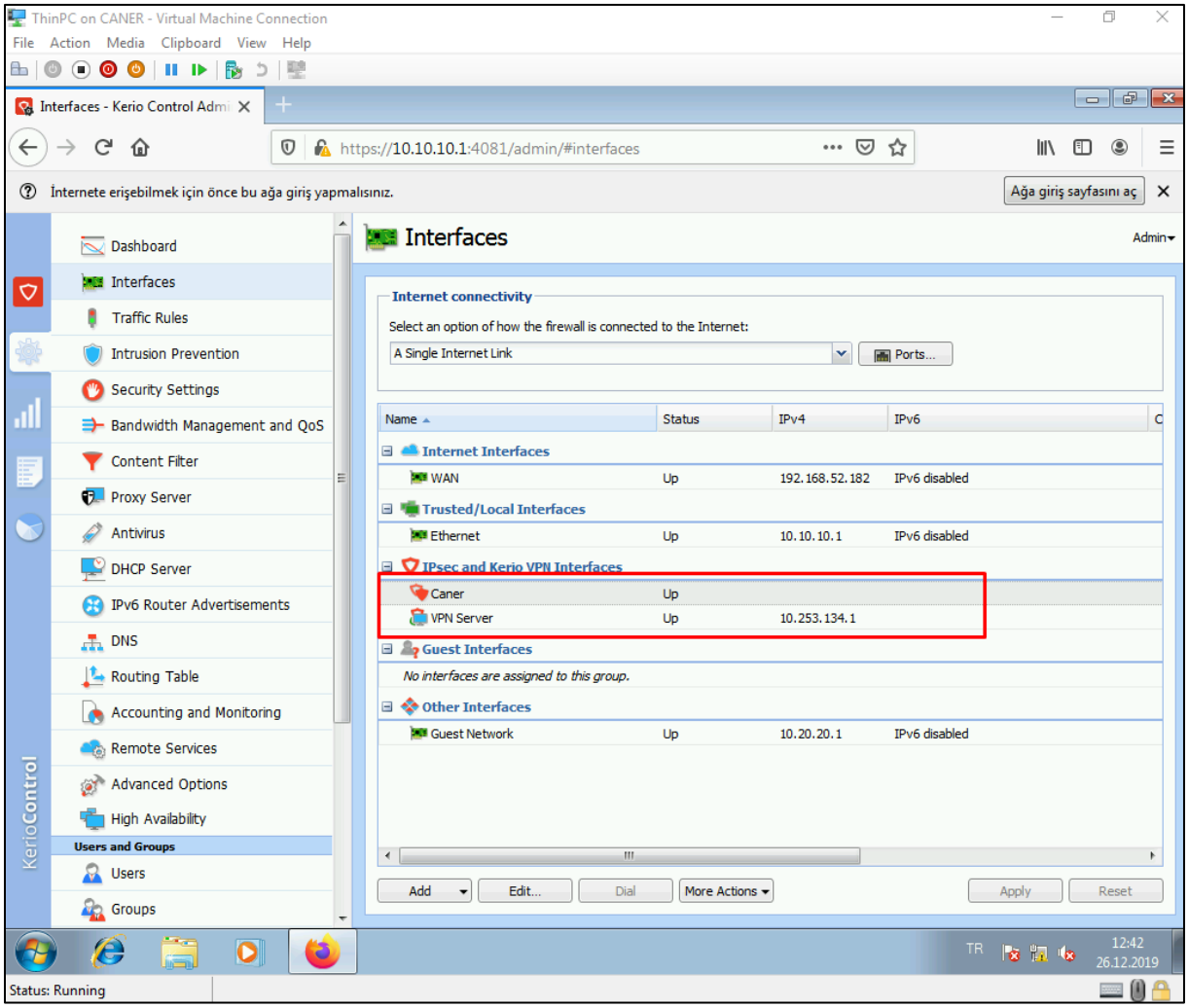

ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Interfaces - Kerio Control Adm
https://10.10.10.1:4081/admin/#interfaces
Dashboard
Interfaces
Traffic Rules
Intrusion Prevention
Security Settings
Bandwidth Managen
Content Filter
Proxy Server
Antivirus
DHCP Server
IPv6 Router Advert
DNS
Routing Table
Accounting and Mor
Remote Services
Advanced Options
High Availability
Users and Groups
Users
Groups
Domains and User L
KerioControl
VPN Tunnel Properties
General
Name:
Abdullah ve Caner
Enable this tunnel
Active - it connects to the remote endpoint
192.168.52.83
Use semicolons (;) to separate multiple hostnames or IP addresses of the remote endpoint.
Passive - it only accepts incoming connections
Type:
IPsec
Kerio VPN
Add Route
Custom VPN route
Network:
172.16.10.0
Mask:
255.255.255.0
Description:
Abdullah LAN
OK
Cancel
Authentication
Use routes provide
Use custom routes
Network
Add...
Edit...
Remove
OK
Cancel
Apply
Reset
Admin
TR
10:04
26.12.2019
Status: Running

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.

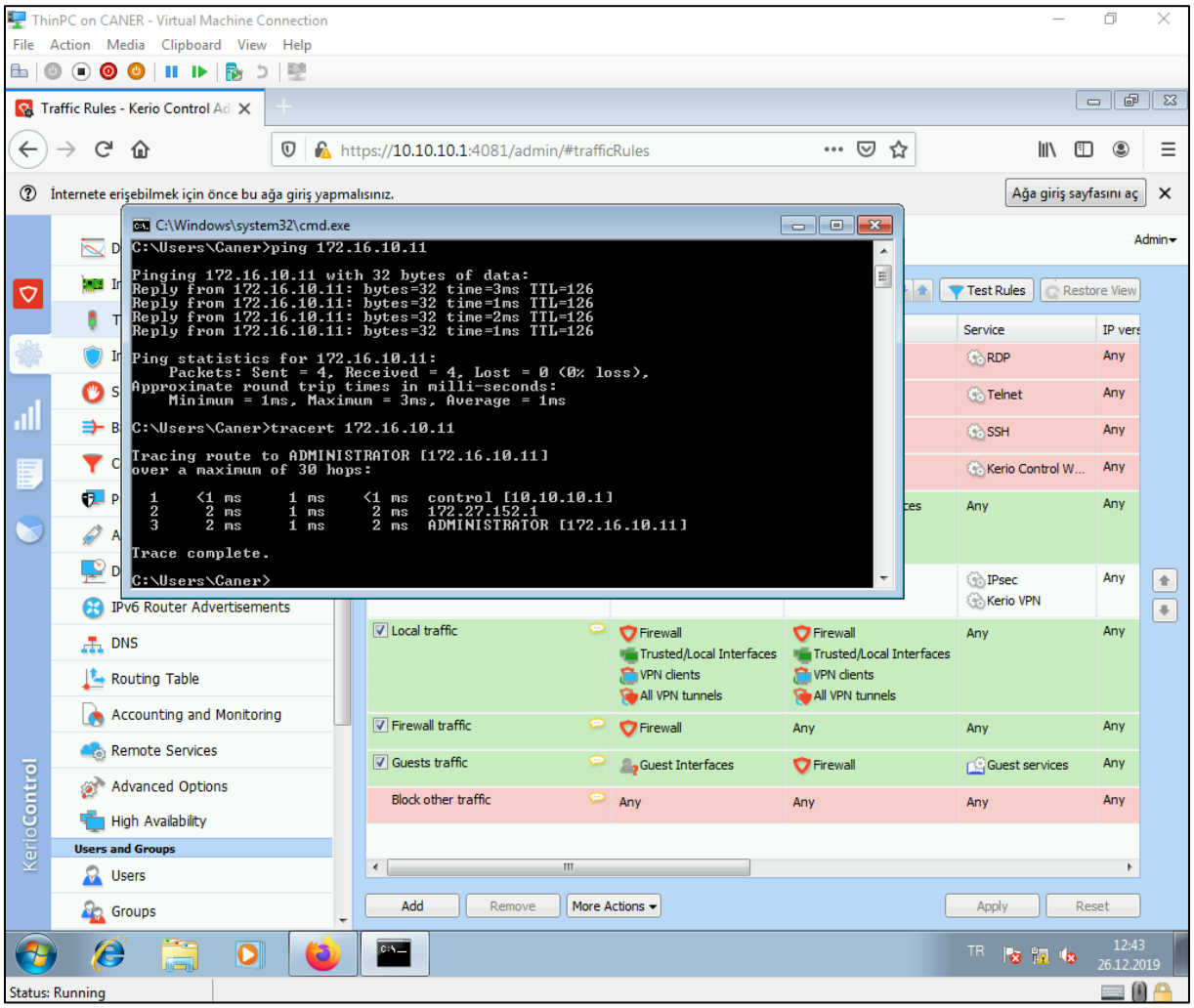


Note that we changed the tunnel's name only for cosmetic reasons. The network settings are still the same. Both sites still have all the relevant network information and each other's certificate.

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

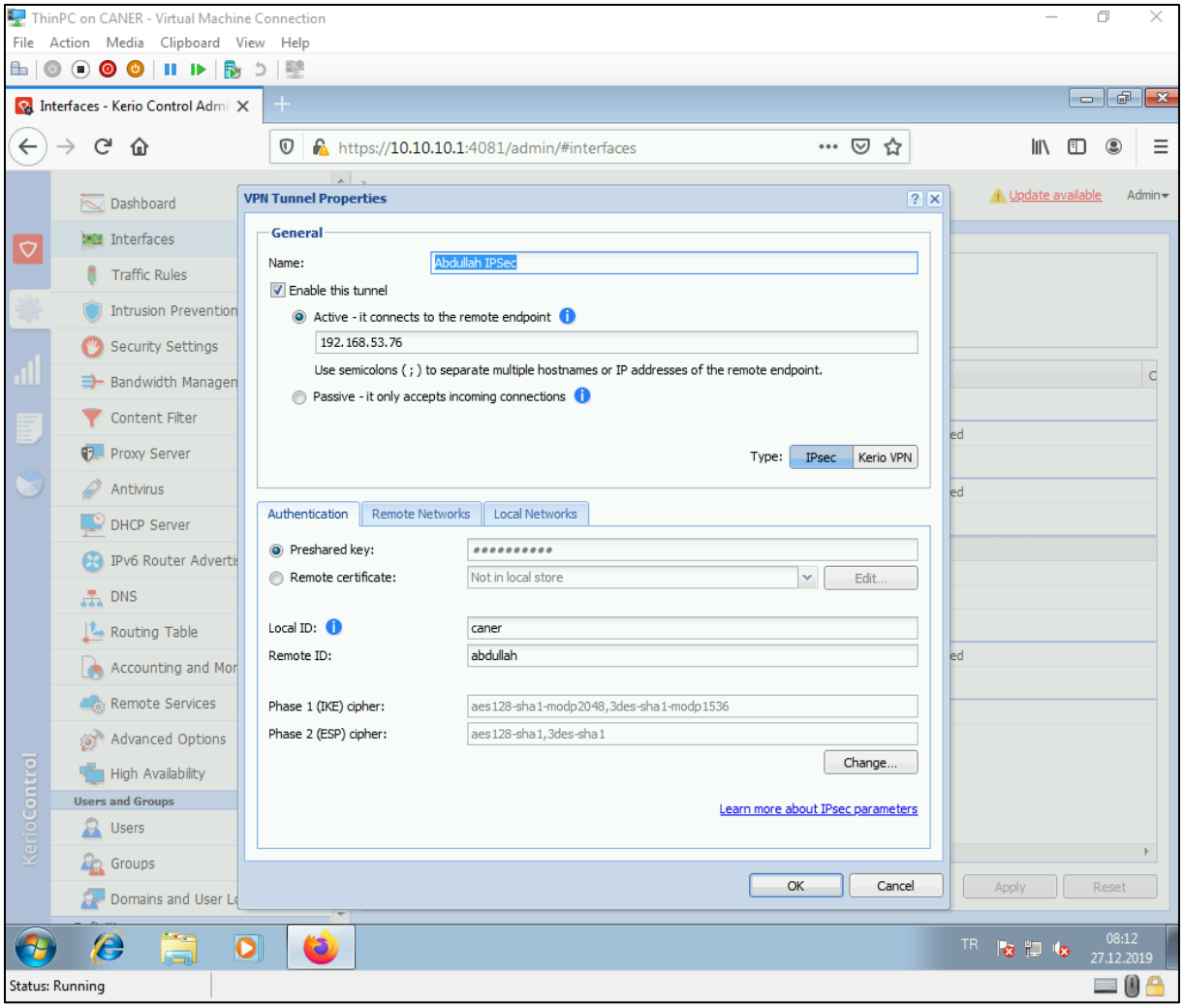


That means a host on site 1's internal network can ping or RDP a host on site 2's internal network and when we trace the route it directly goes from one internal to the other's VPN server and to the other's internal network.



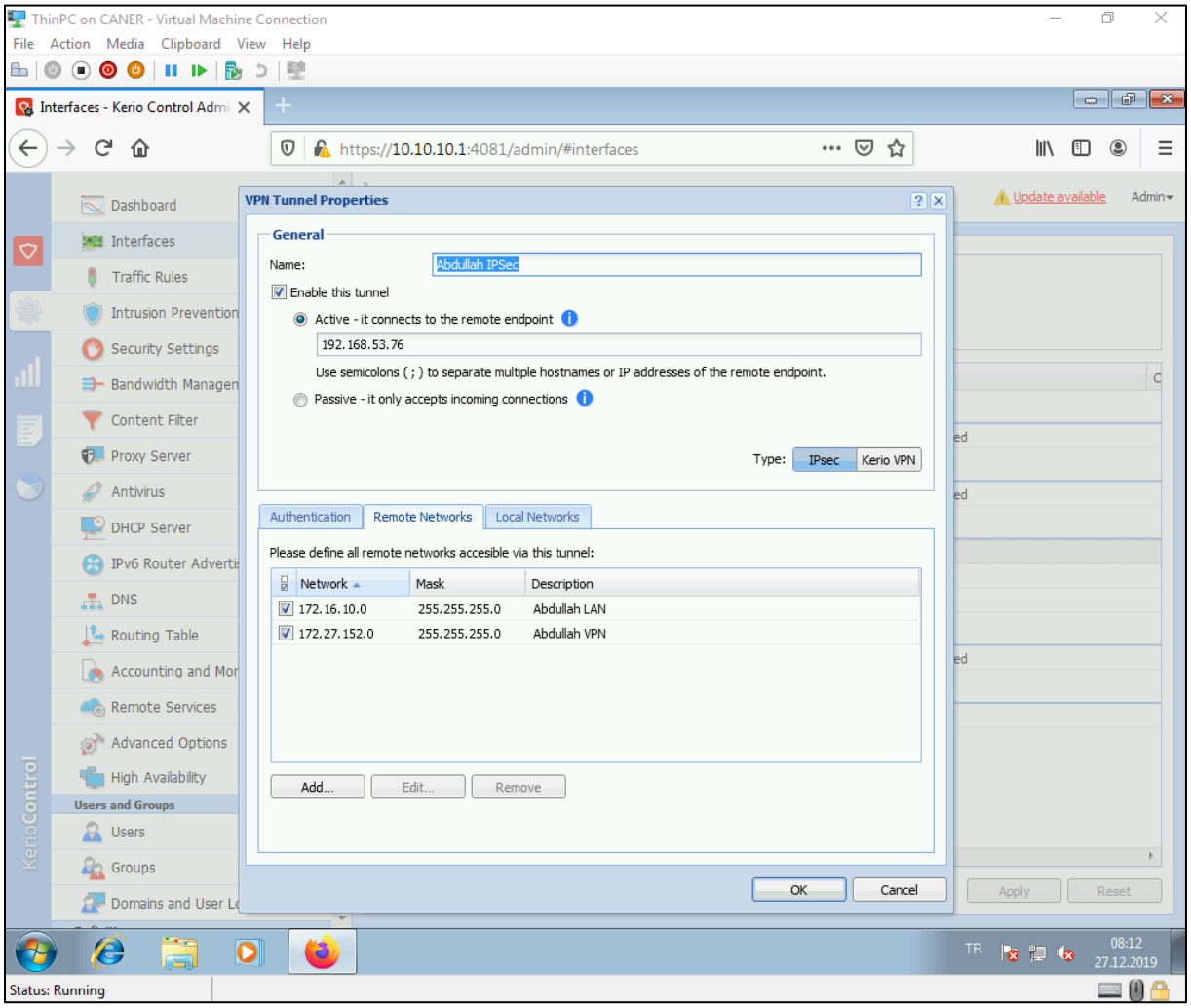
This completes the VPN.

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

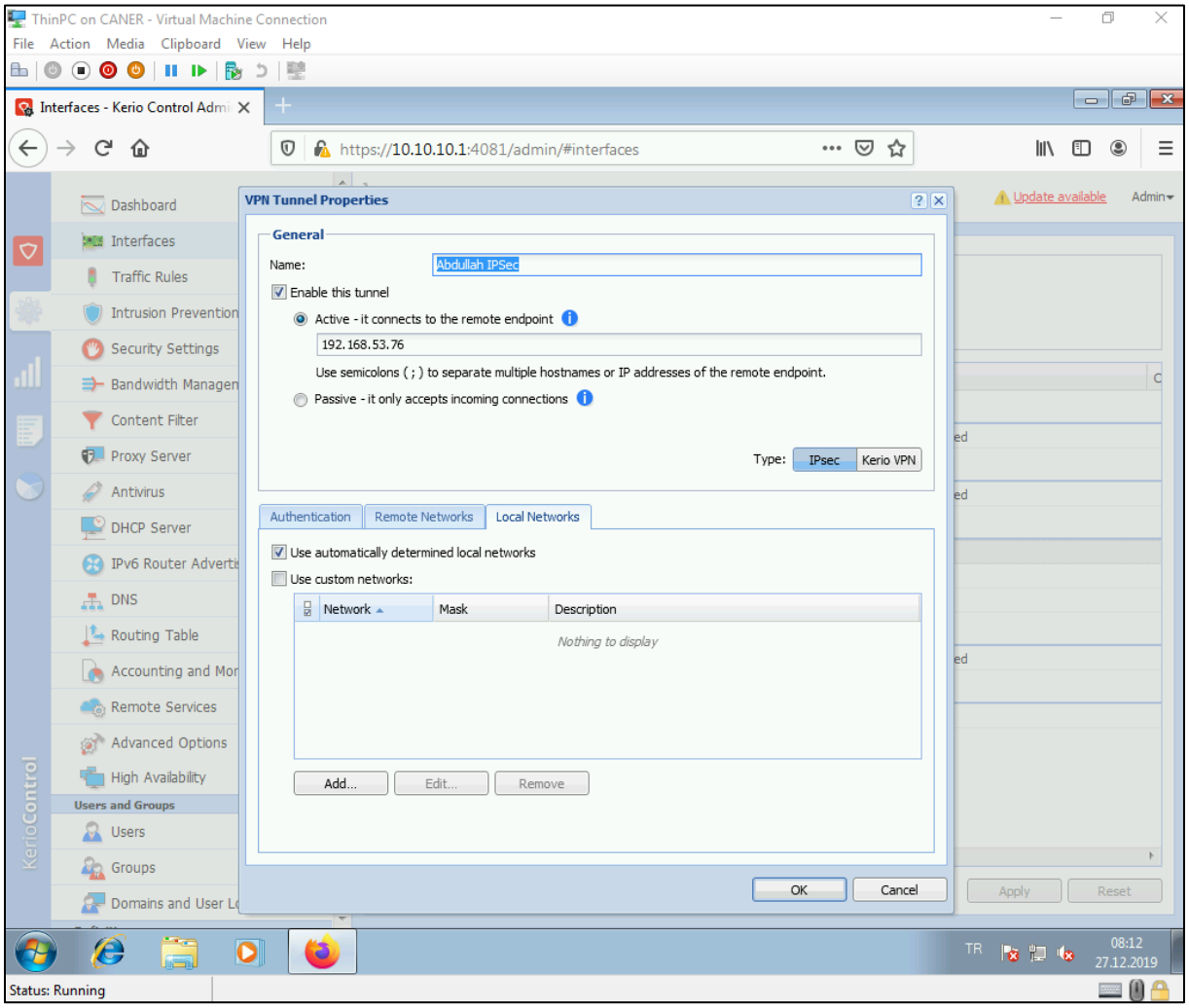


For an IPSec tunnel a pre-shared key can be used as another layer of security. The local and remote IDs must match to the partners, in reverse obviously and the IKE and ESP ciphers' details MUST be the same. An IPSec tunnel cannot be established if you use different encryption and/or hash algorithms.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

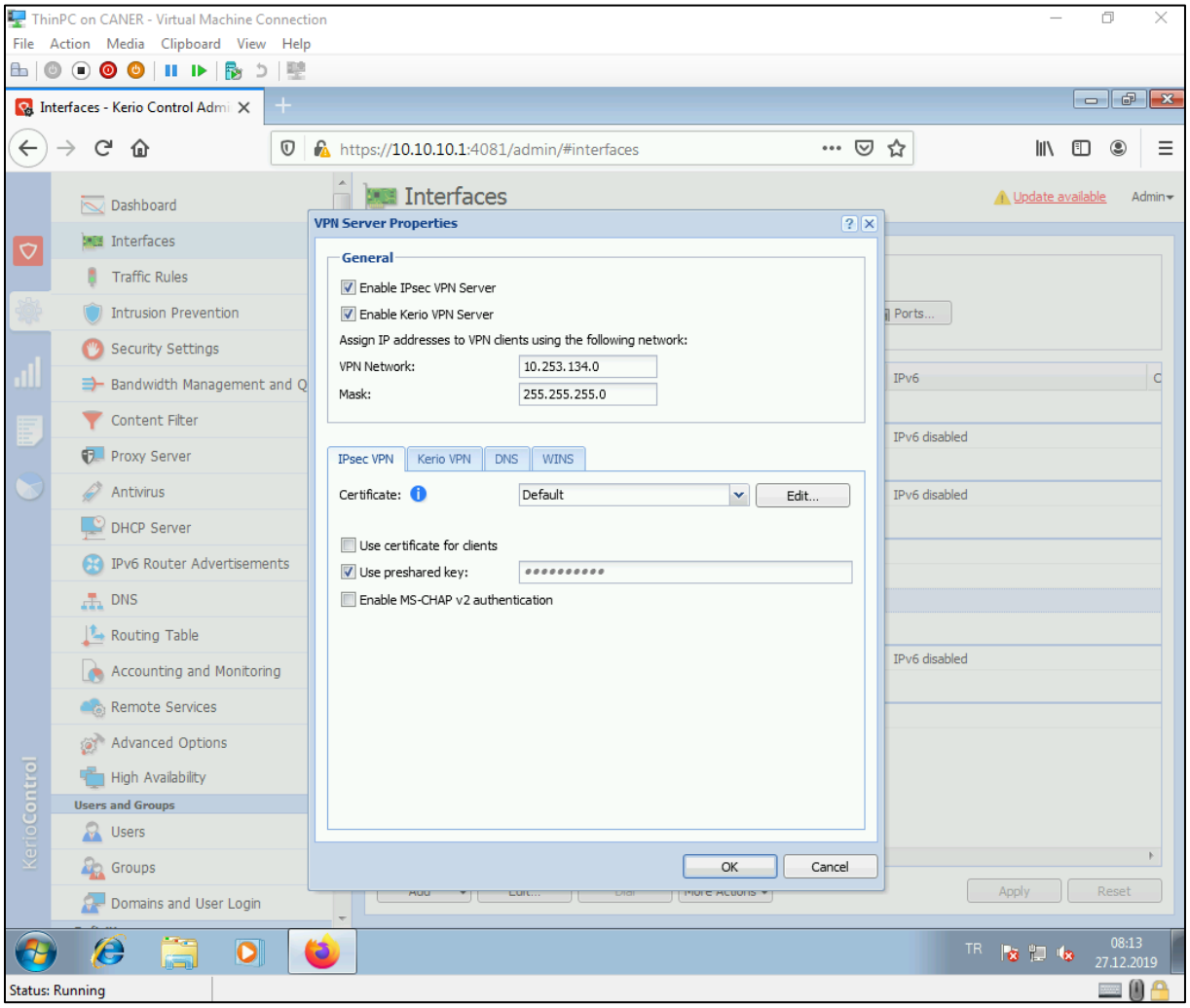
Another detail is that remote networks site 1 enters must match the local networks site 2 enters exactly and vice versa.



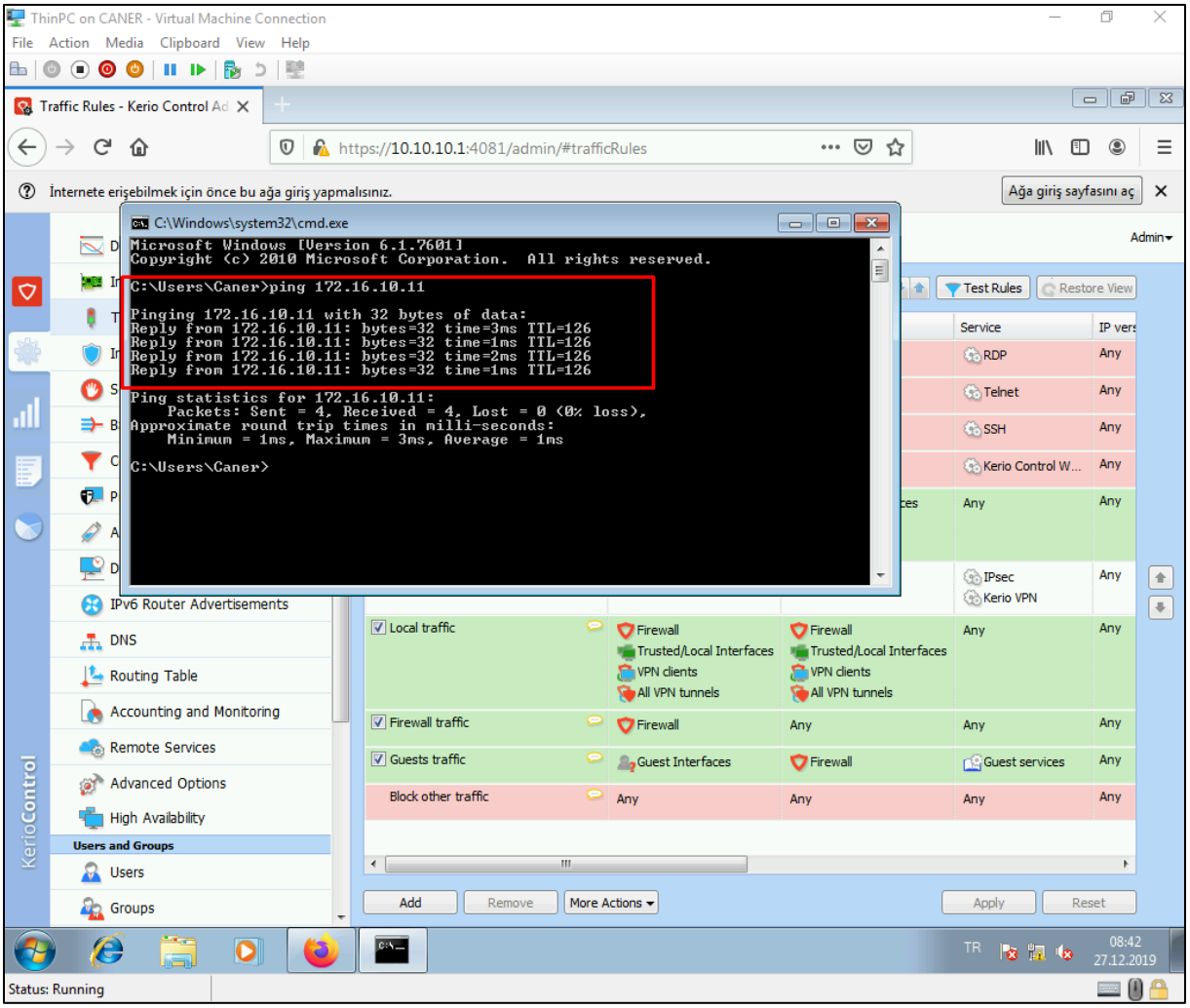
For this basic topology, the simplest way to accomplish this is to add every internal network of the other site as remote networks and connect all local networks.



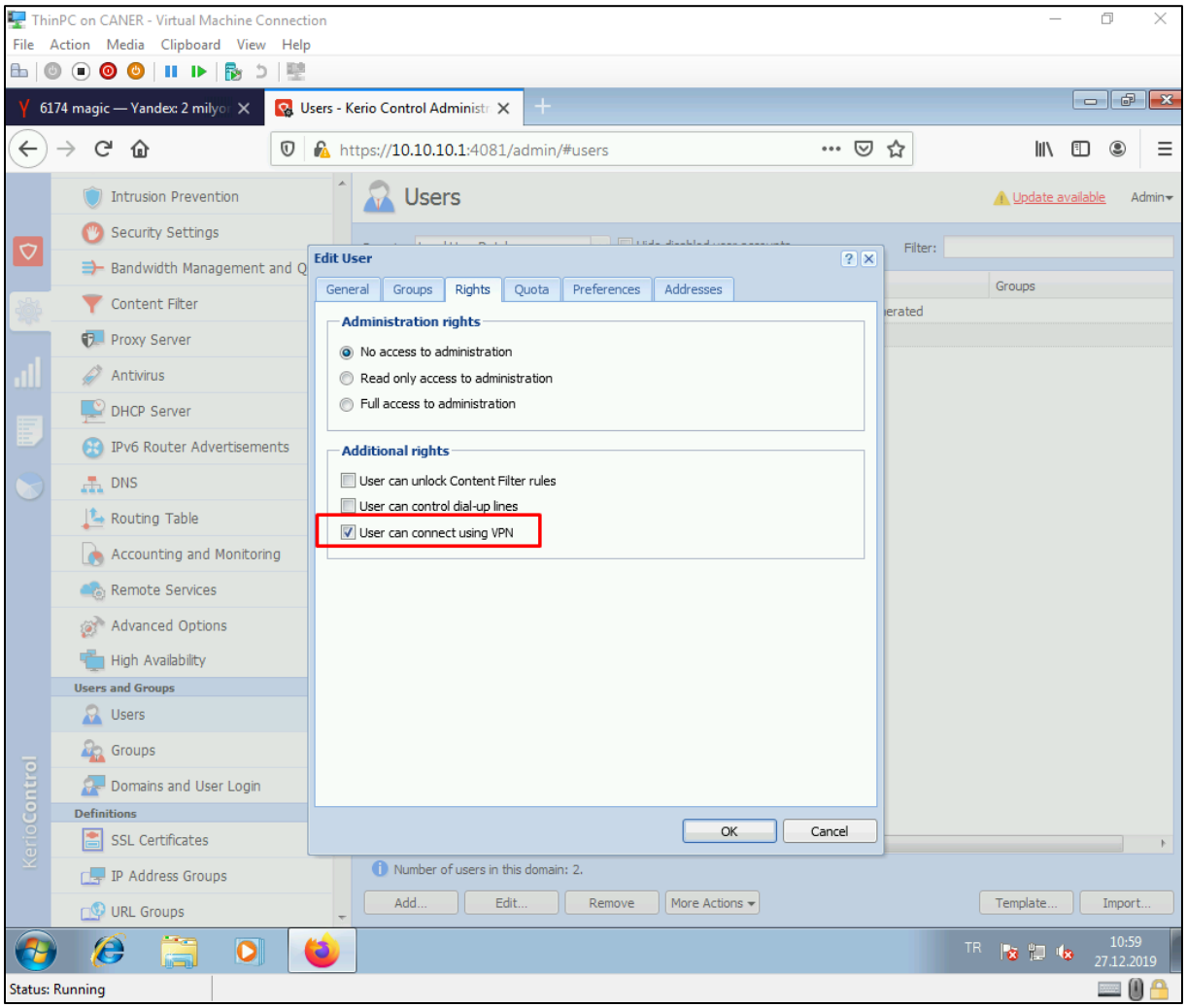
Also, if you use the pre-shared key mention it on the VPN Server Settings as well. Of course, it must be the same everywhere.



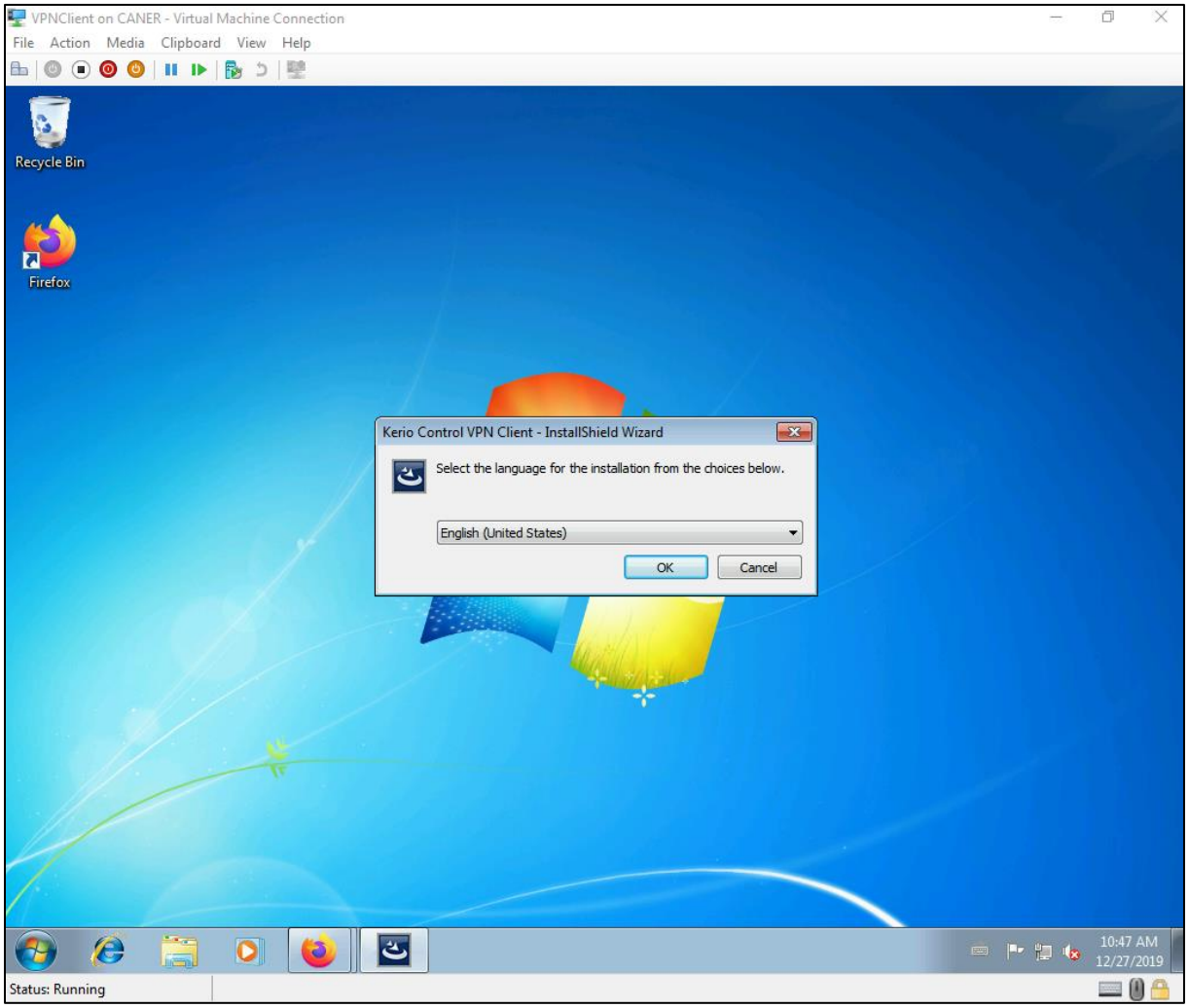
Then, the tunnel works again.

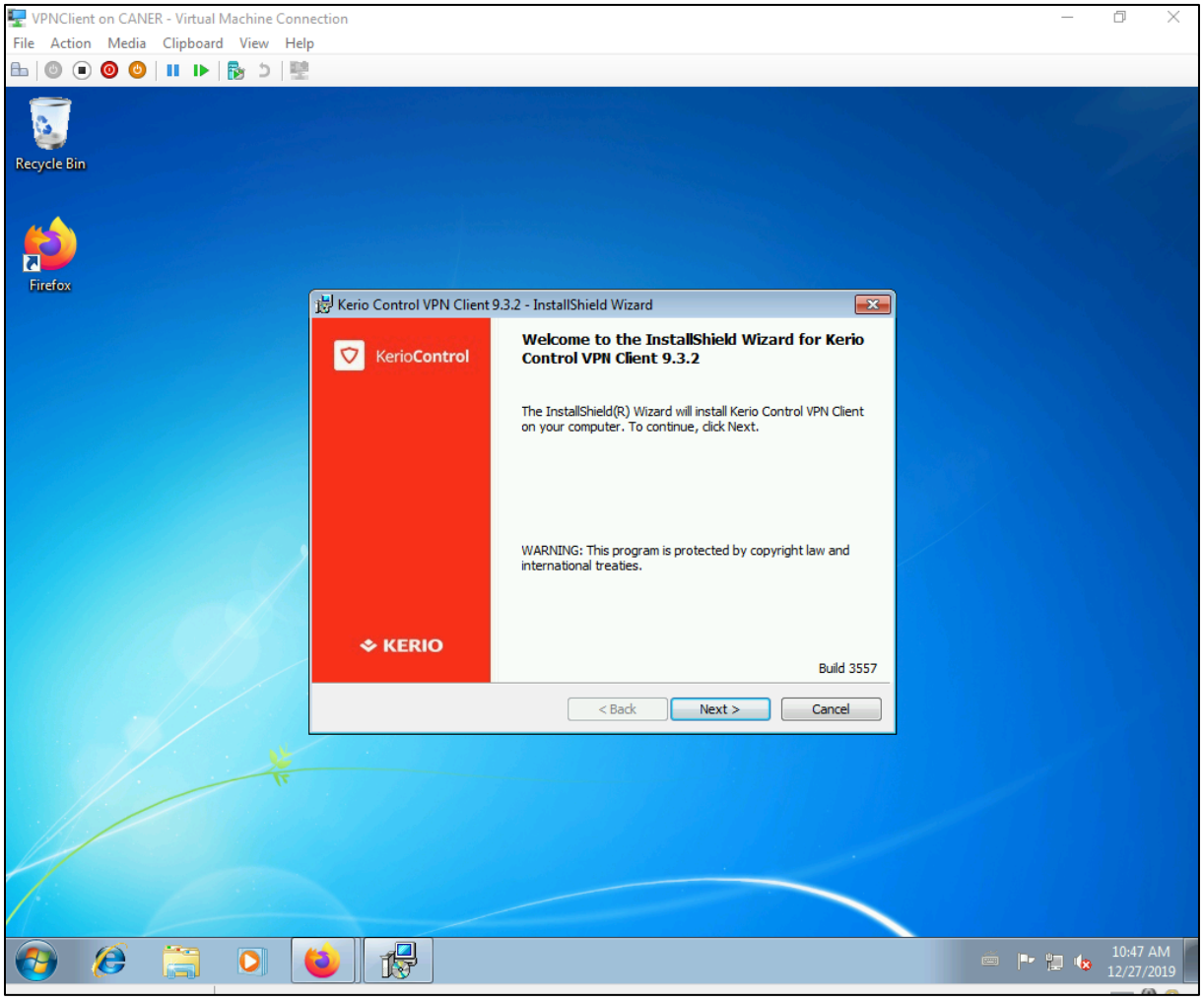


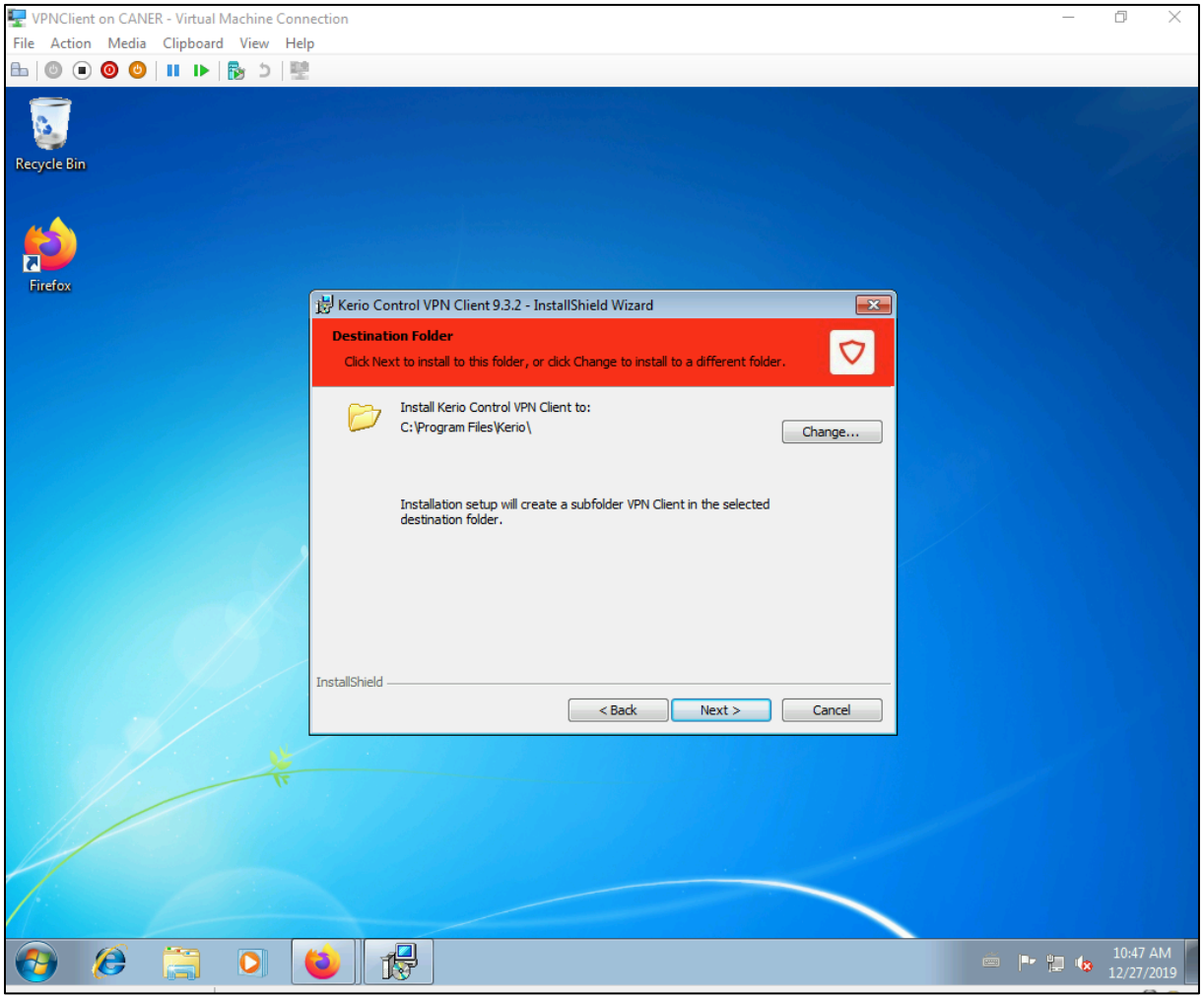
Now, let’s do a client to site VPN connection. The very first thing we need to do is enable a user to connect via VPN under administration right of the user’s rights. We can easily get there by editing the user.

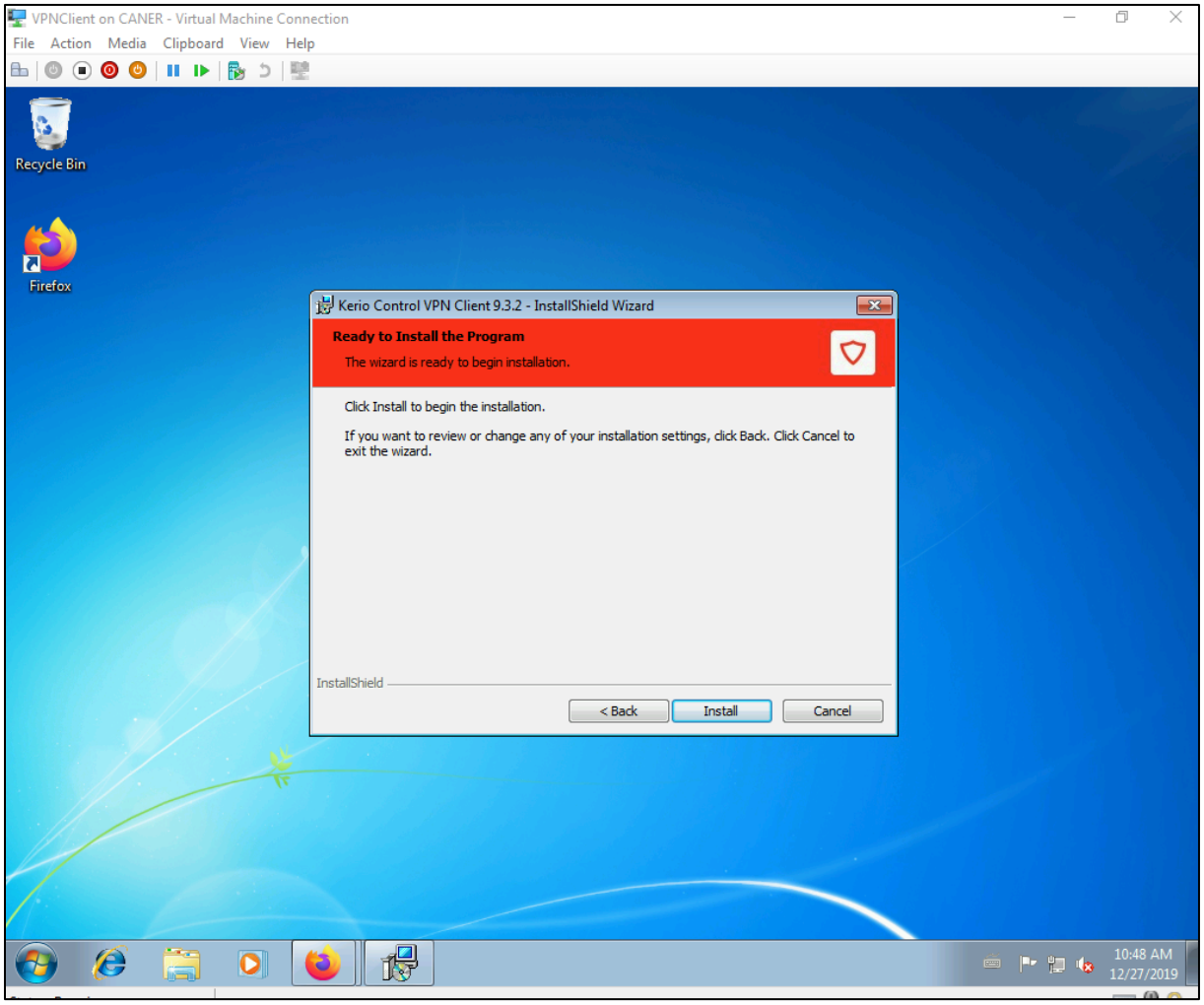


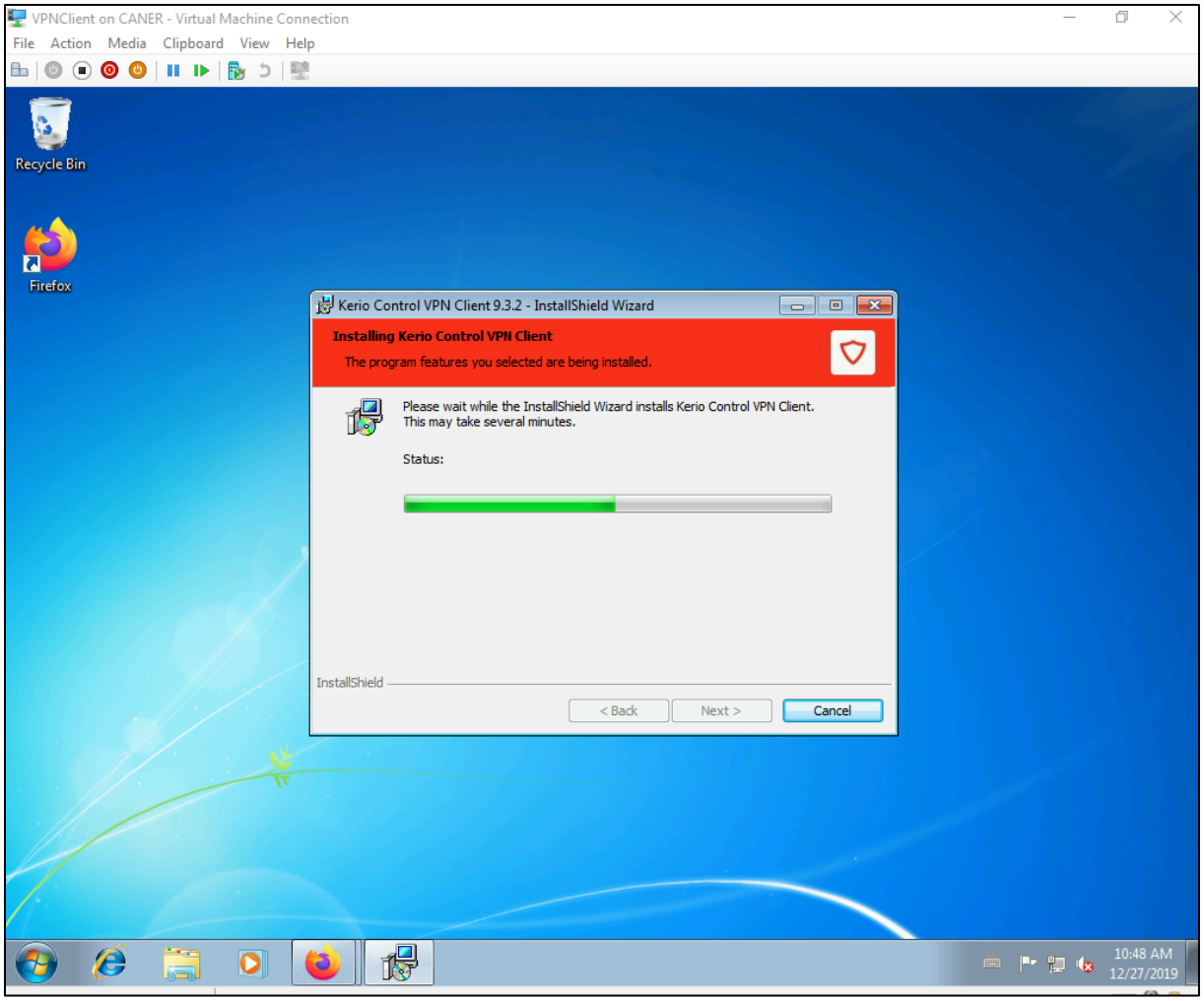
Then, from Kerio Control website the user must download the Kerio VPN Client application.



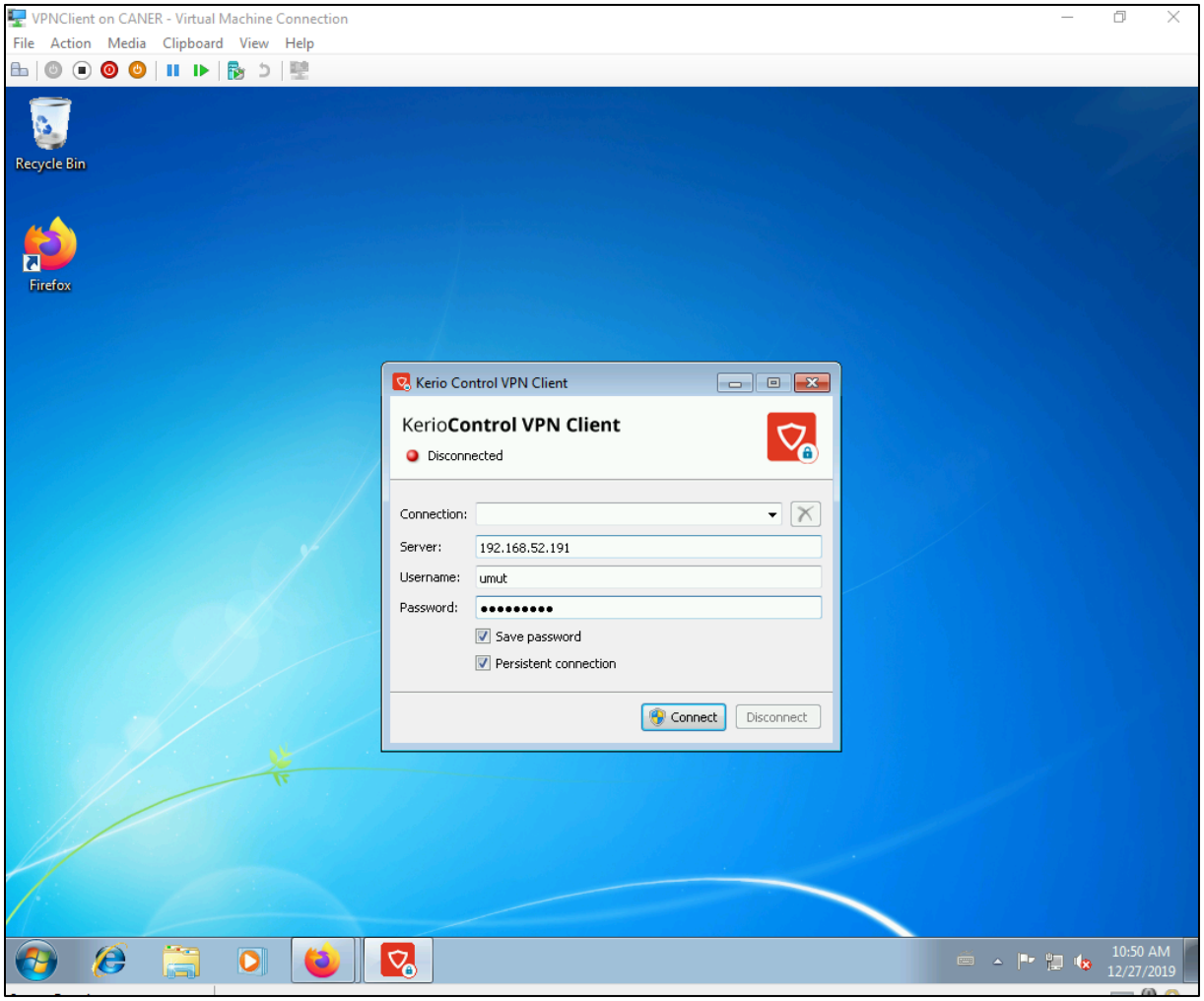

VPNClient on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Firefox
Kerio Control VPN Client 9.3.2 - InstallShield Wizard
KerioControl
Welcome to the InstallShield Wizard for Kerio Control VPN Client 9.3.2
The InstallShield(R) Wizard will install Kerio Control VPN Client on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
KERIO
Build 3557
< Back
Next >
Cancel
10:47 AM
12/27/2019


VPNClient on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Firefox
Kerio Control VPN Client 9.3.2 - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Kerio Control VPN Client to:
C:\Program Files\Kerio\
Change...
Installation setup will create a subfolder VPN Client in the selected destination folder.
InstallShield
< Back
Next >
Cancel
10:47 AM
12/27/2019

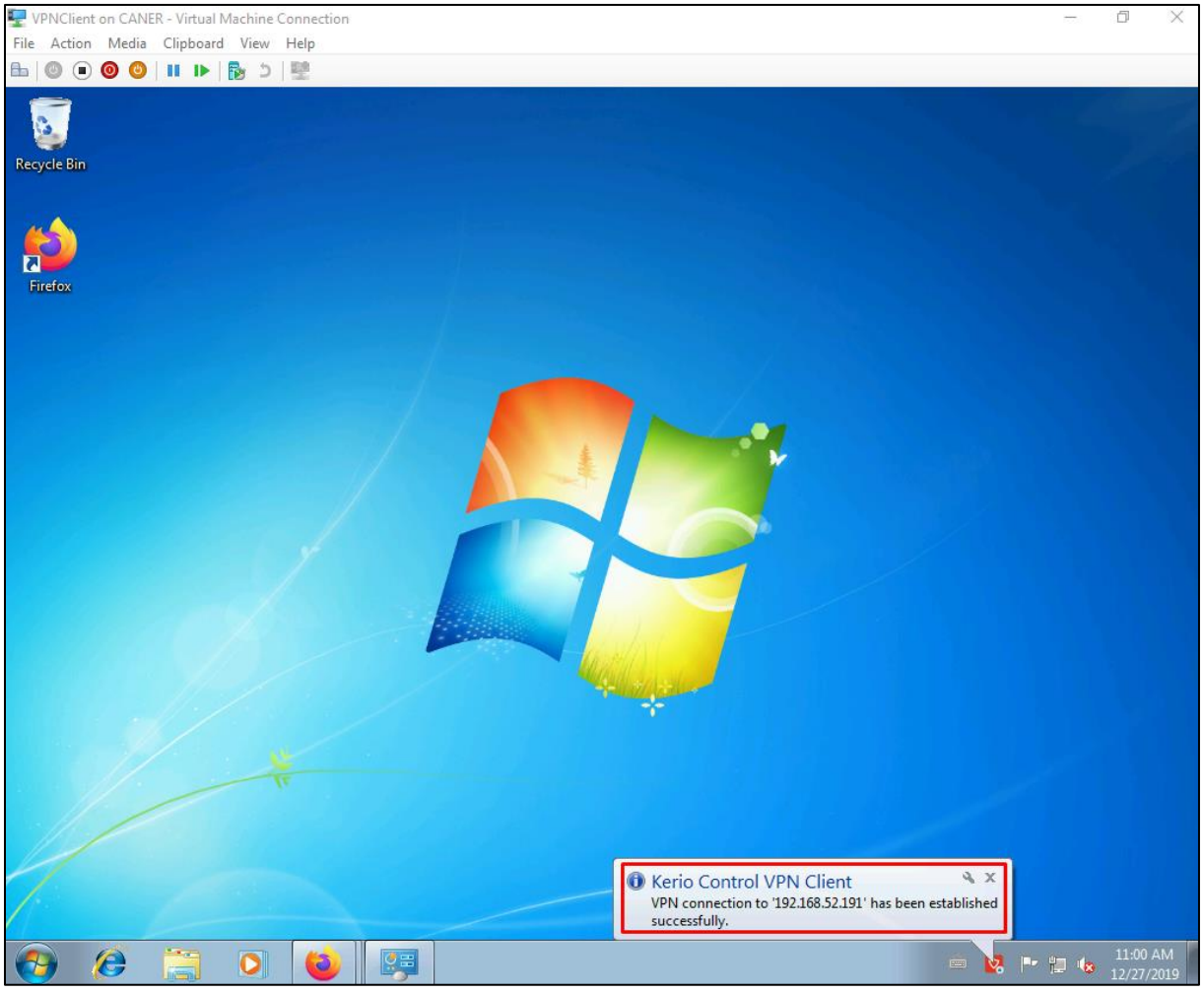

VPNClient on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Firefox
Kerio Control VPN Client 9.3.2 - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel
10:48 AM
12/27/2019


VPNClient on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Firefox
Kerio Control VPN Client 9.3.2 - InstallShield Wizard
Installing Kerio Control VPN Client
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Kerio Control VPN Client.
This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel
10:48 AM
12/27/2019

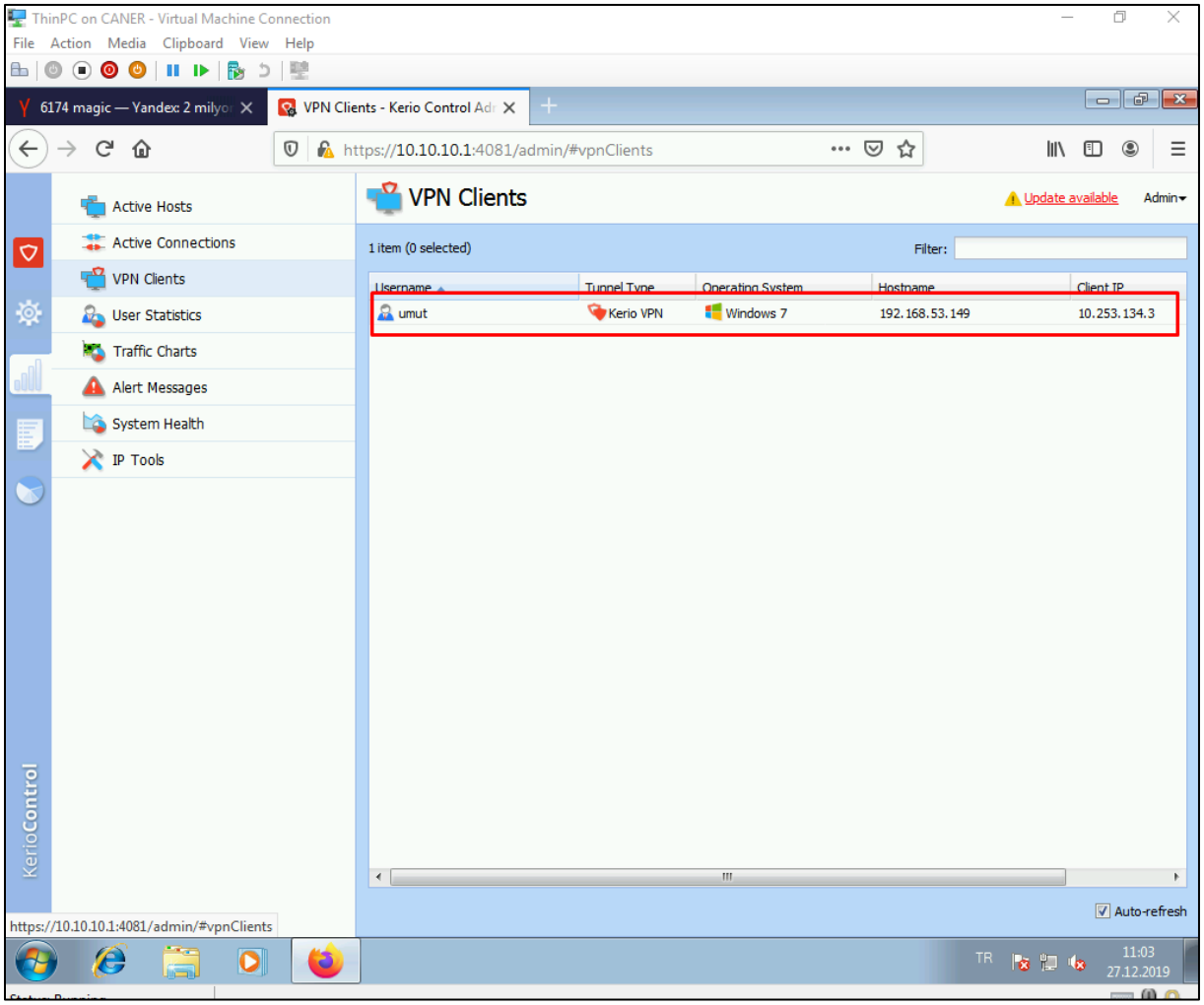
After the installation is done, the user logs in with WAN IP address mentioned for the server.



And the connection established.



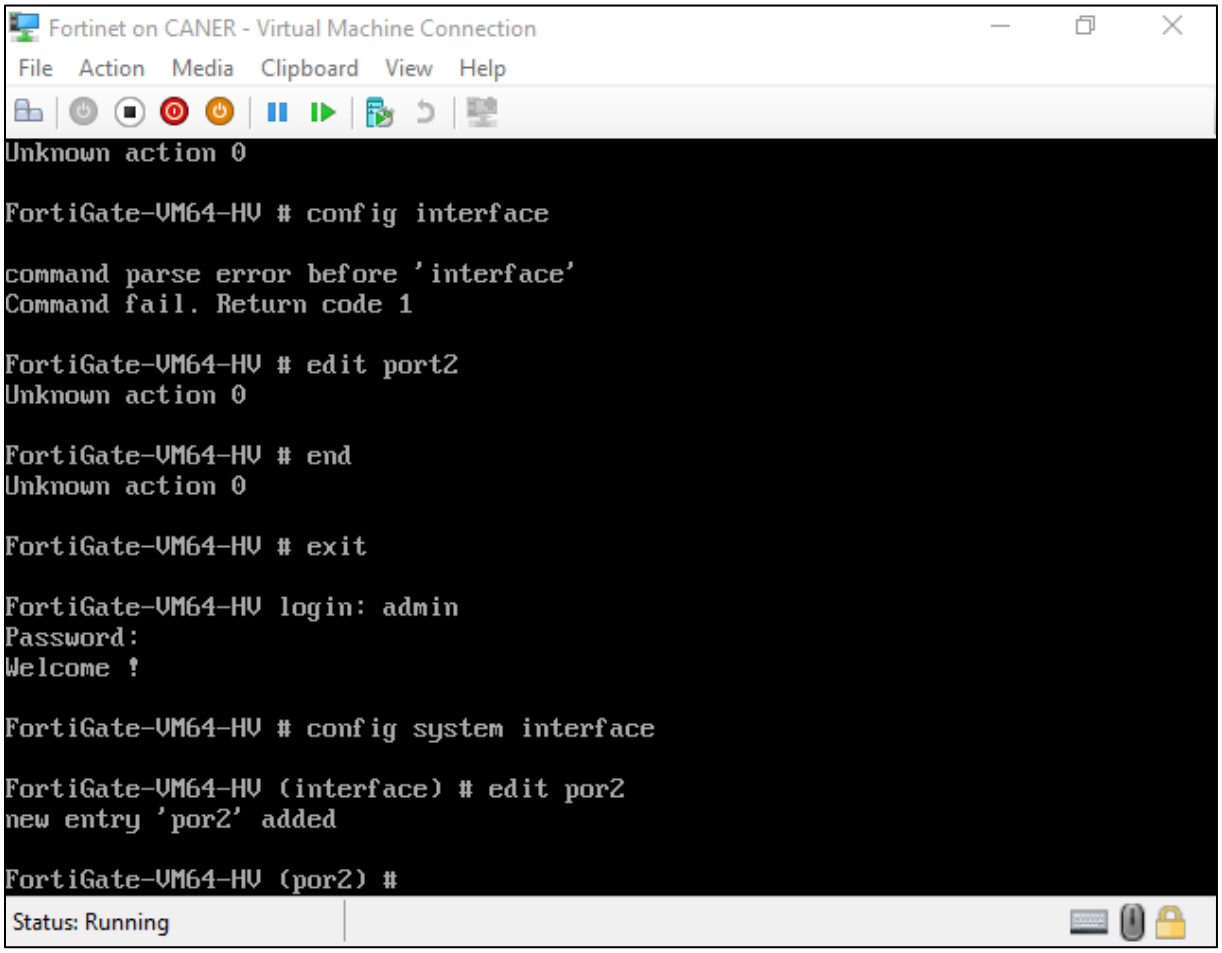
The admin can also see that the user has been connected via the VPN.



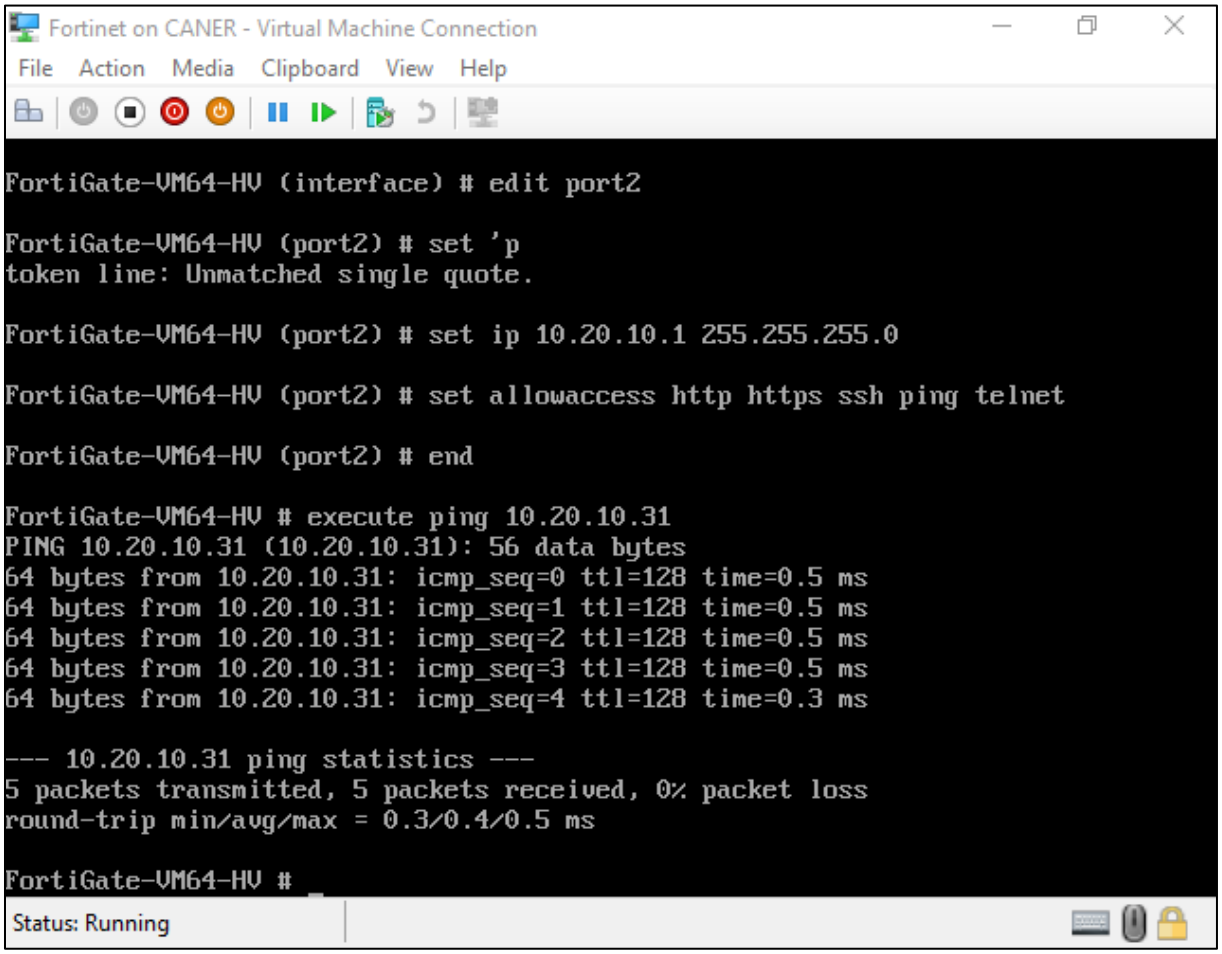
This finishes the Kerio Control part of this project.

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.

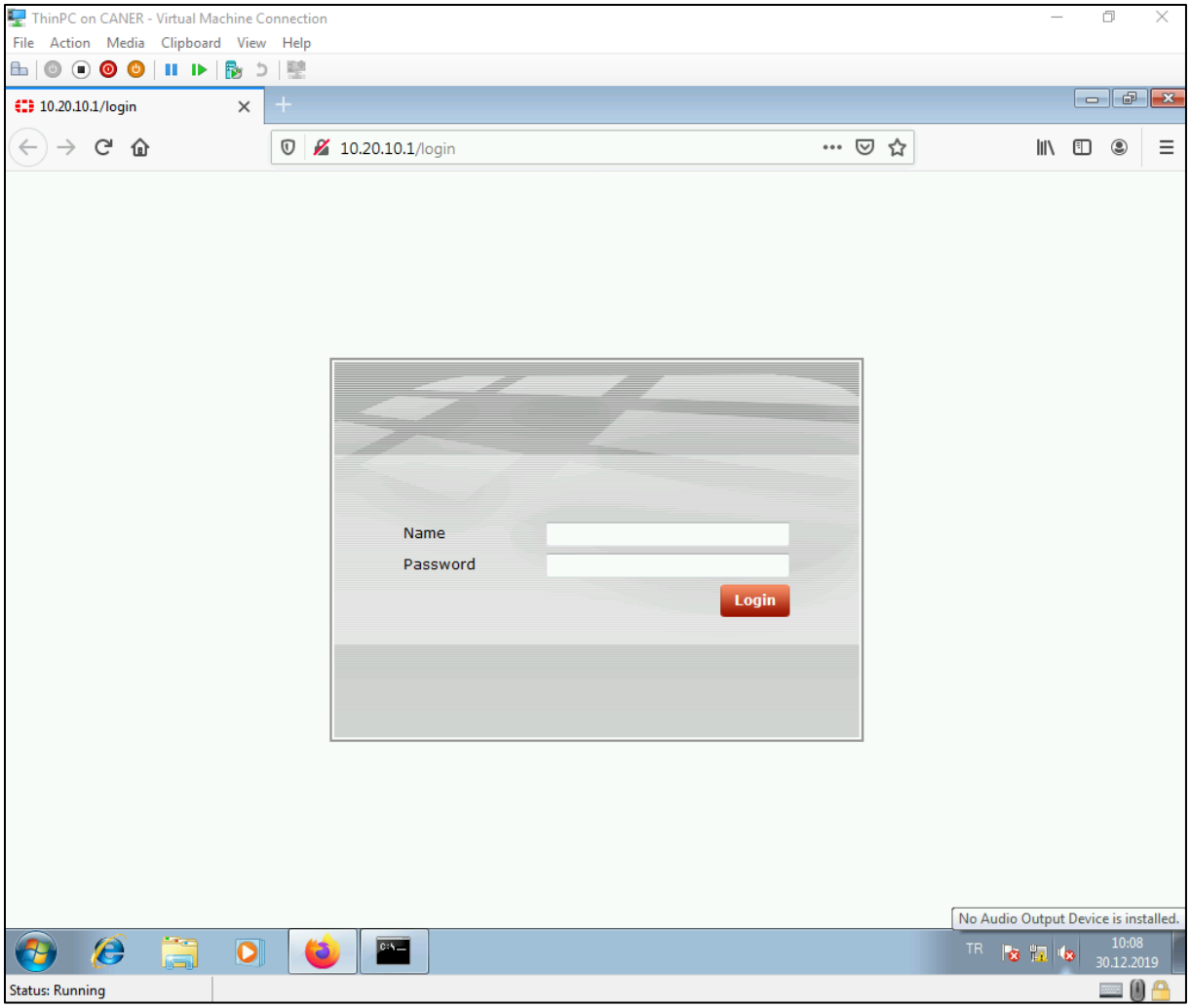


Then, we type edit port2, since it's our internal card, to get into the interface and assign an IP address. We also allow SSH, HTTP, HTTPS, PING and TELNET protocols.

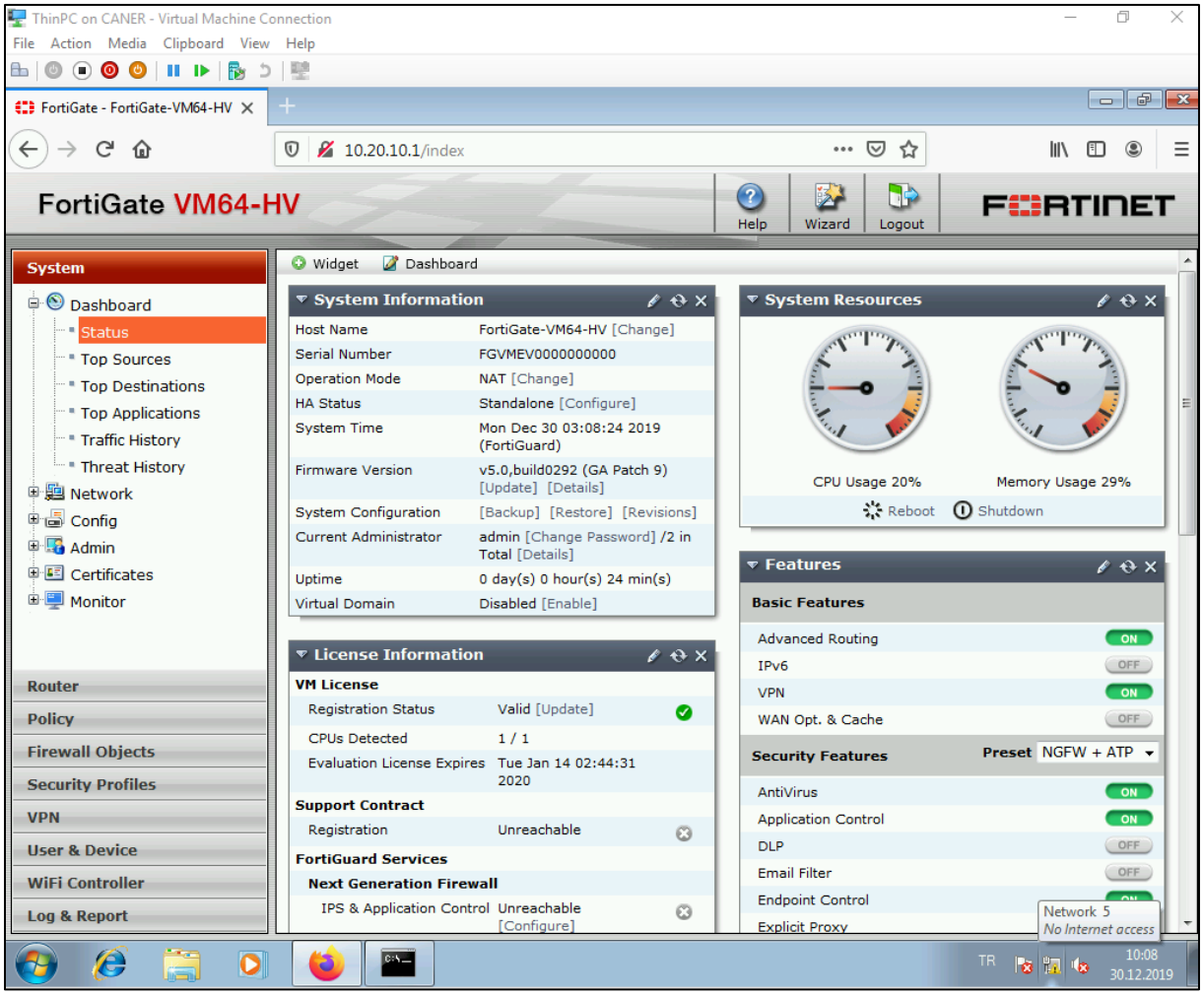


We then test pinging a host on the same internal network.

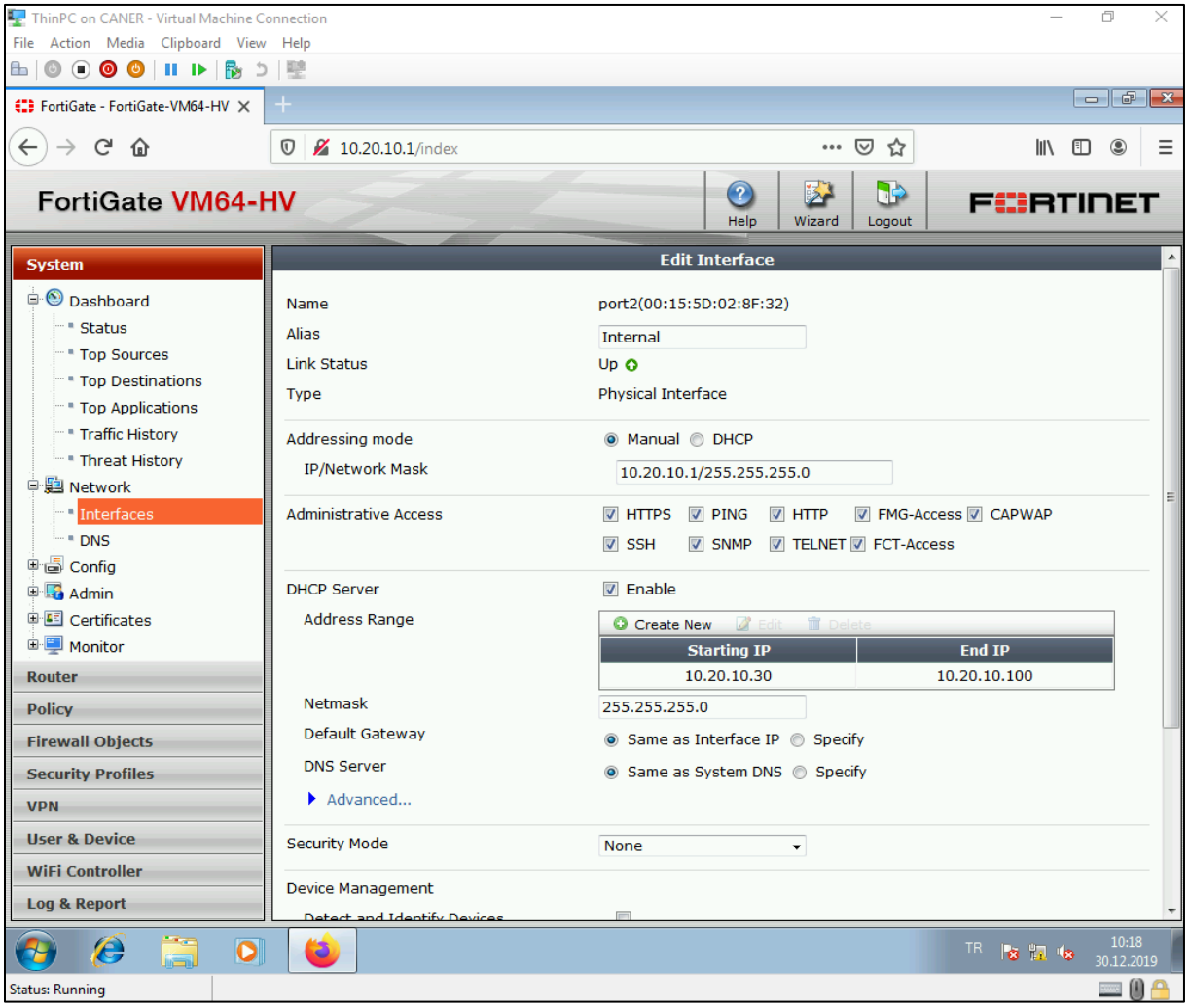
With the web browser we log in using the previous log in information.



This is the FortiGate VM64-HV Dashboard.

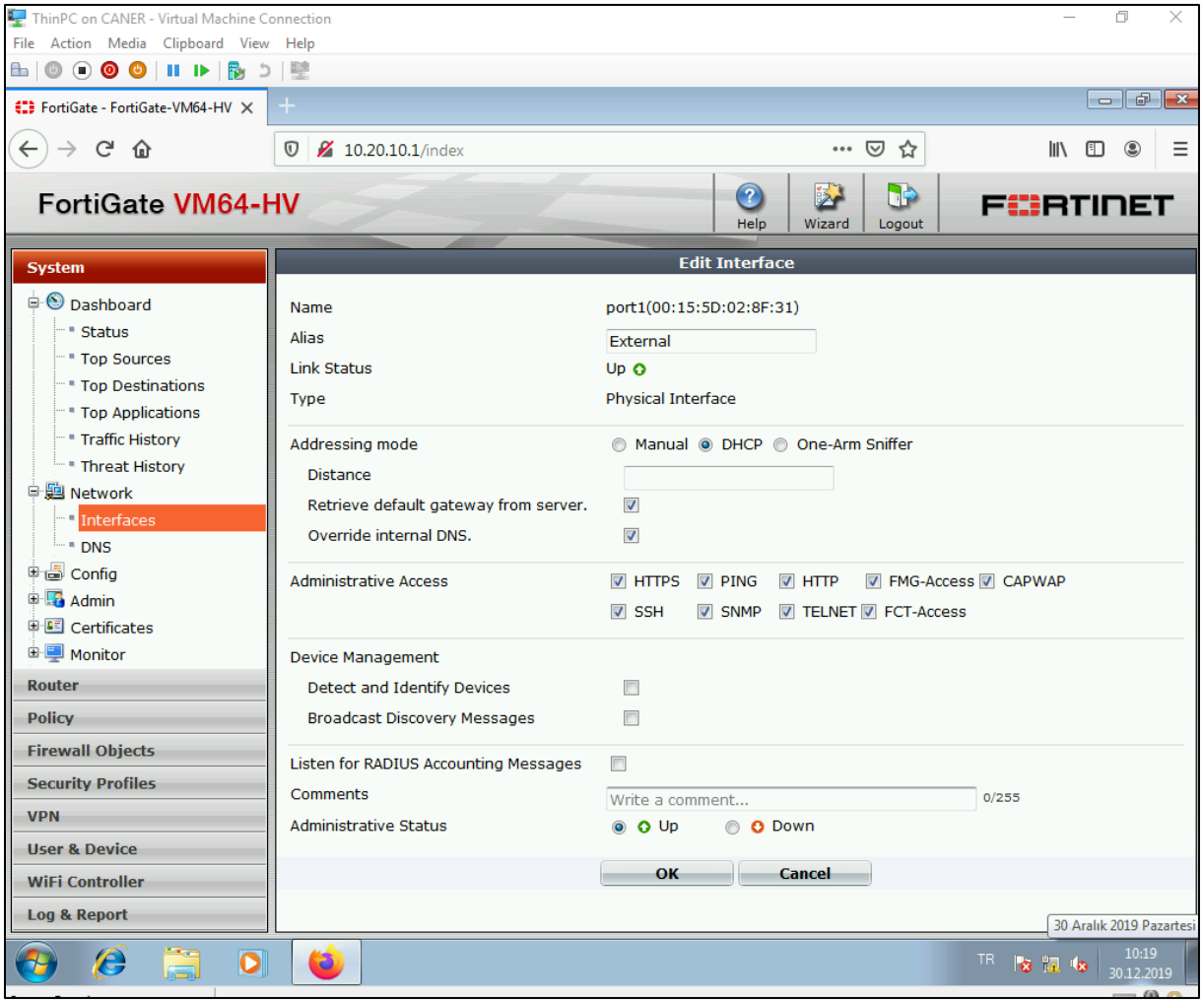


As usual, we want to set up the interfaces.



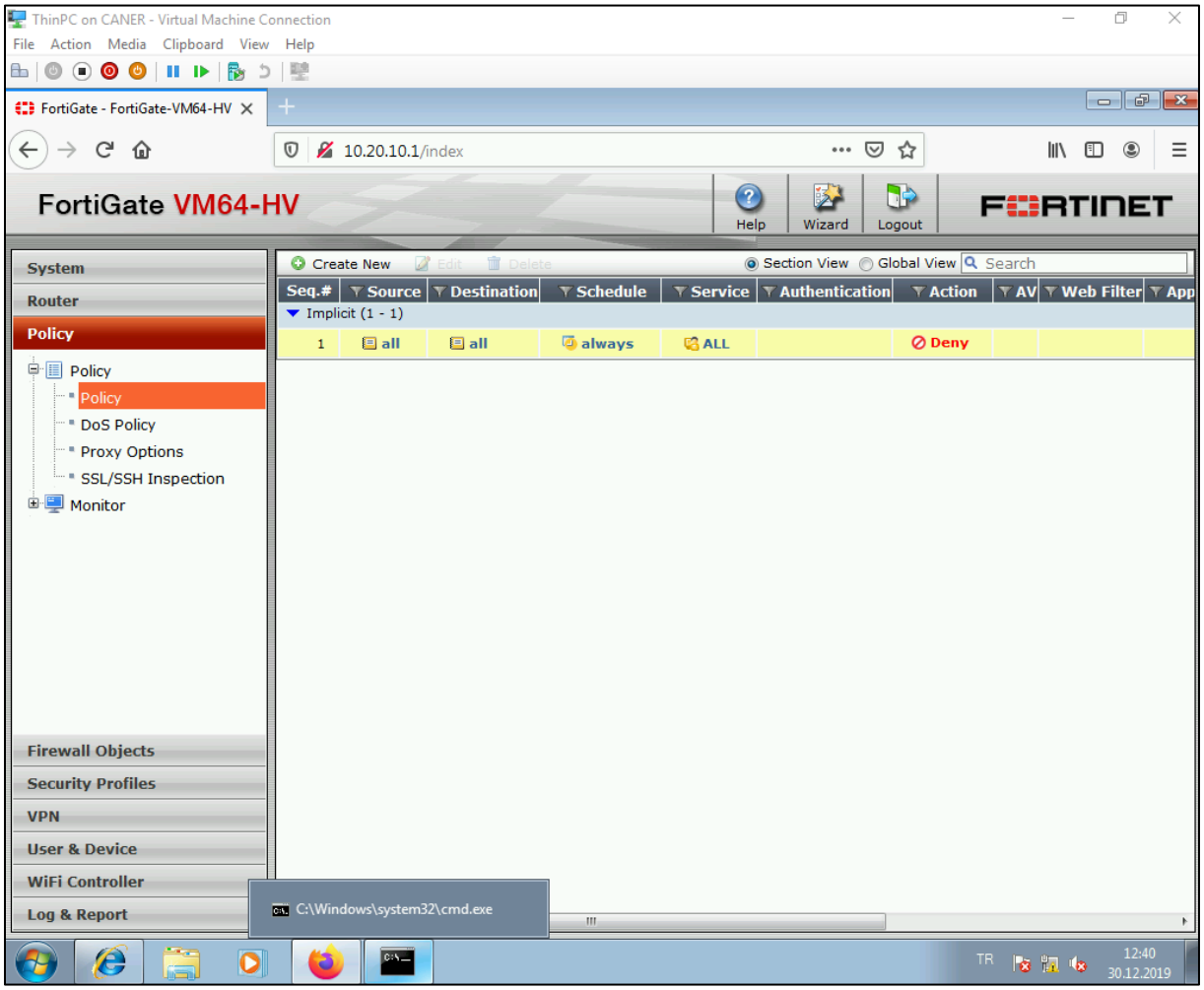
The internal interface starts a DHCP pool but keeps the previously given static IP.

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

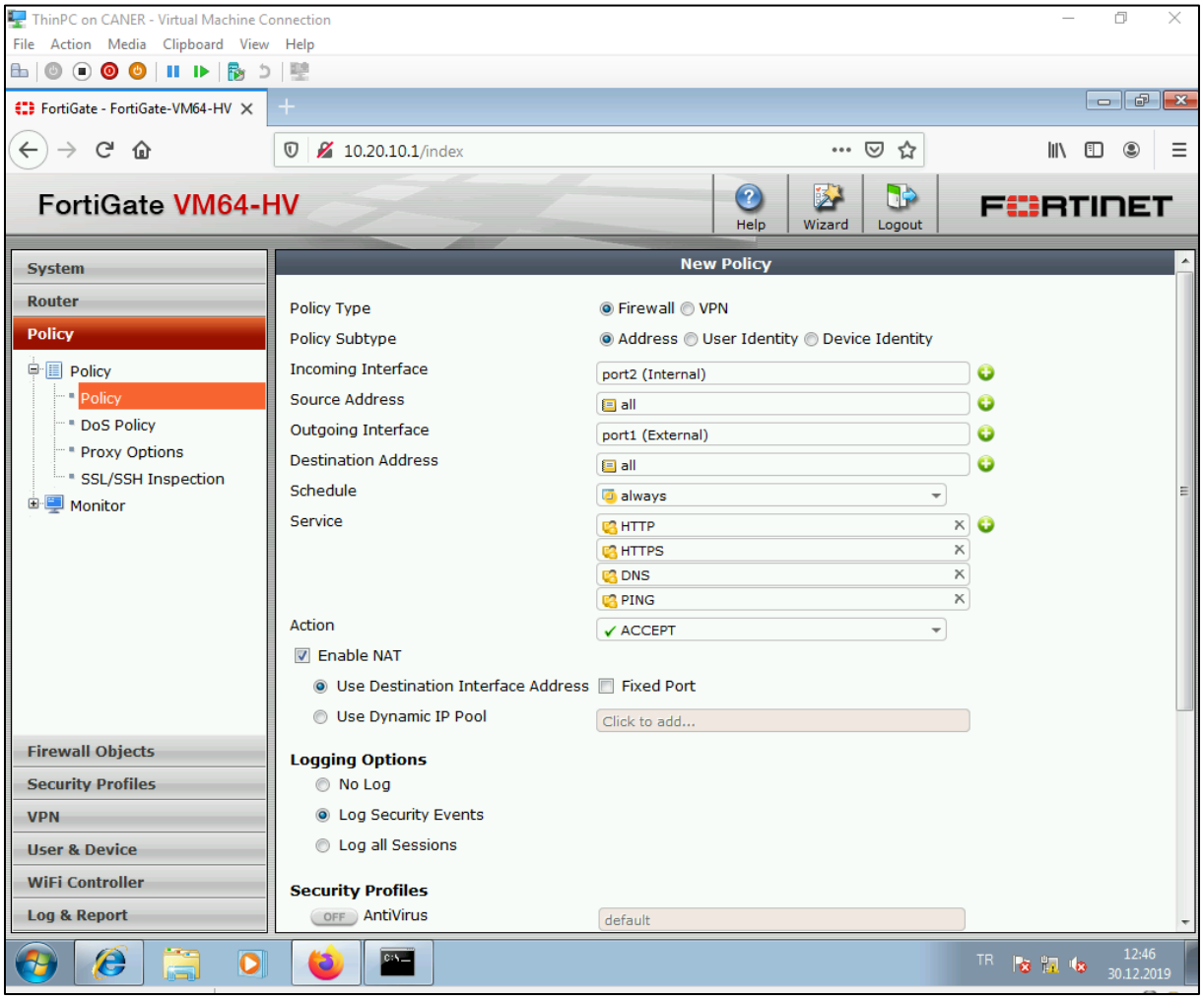


We can allow additional protocols here.

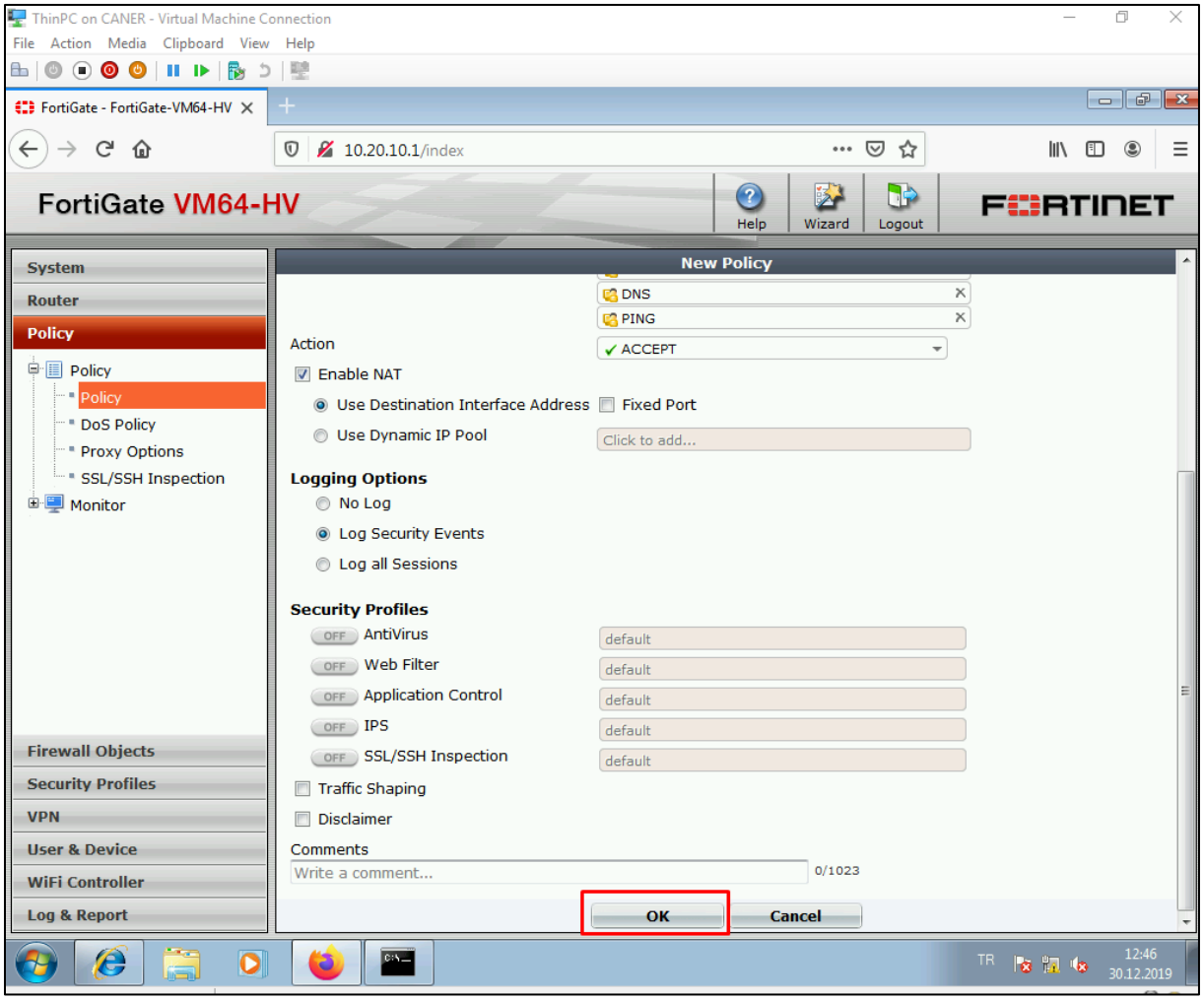
We get to policies to create a new policy. Currently the only active policy is the (implicit) deny at the end.



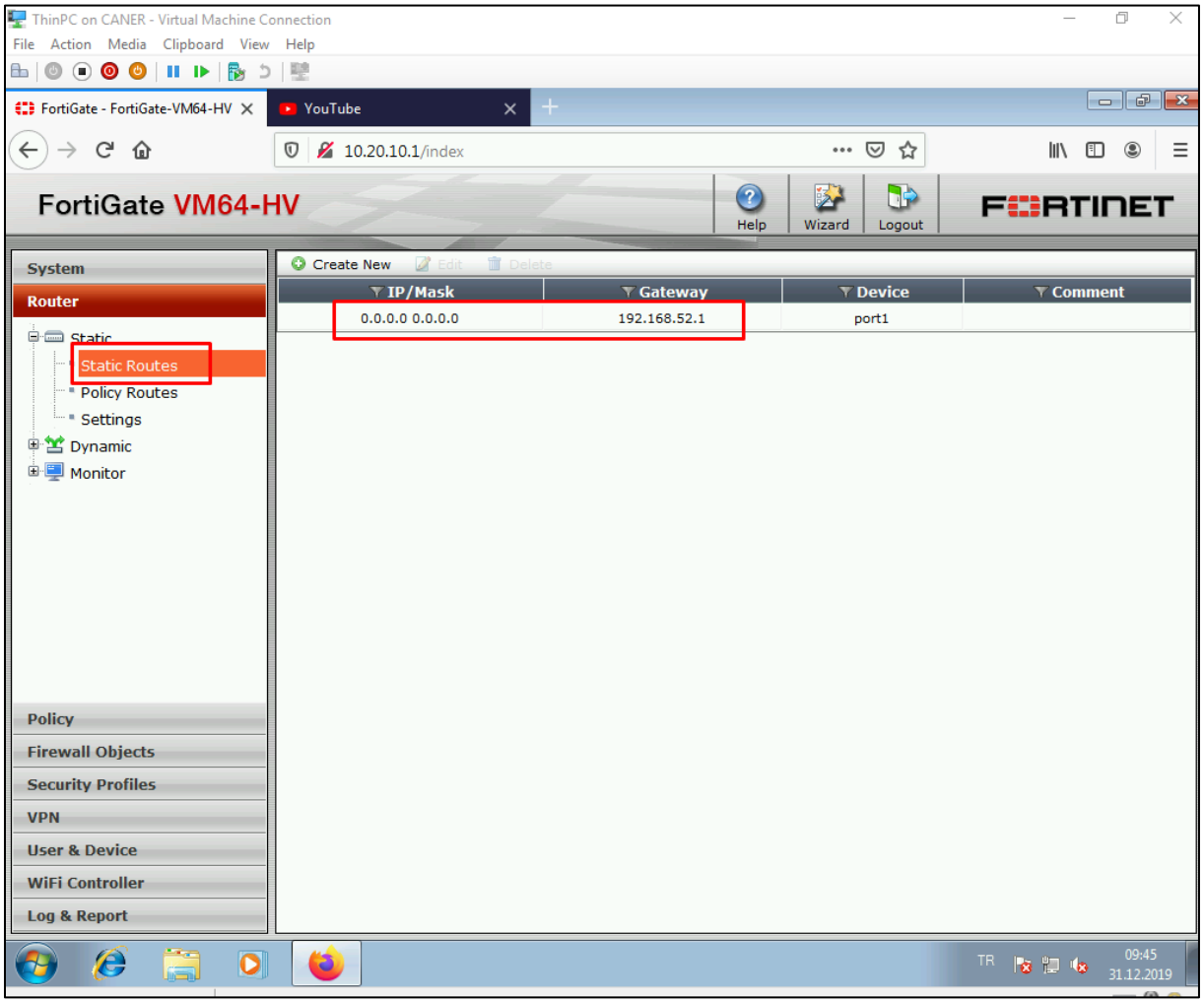
We enable NAT between the internal port2 and external port1 and allow HTTP, HTTPS, PING and DNS.



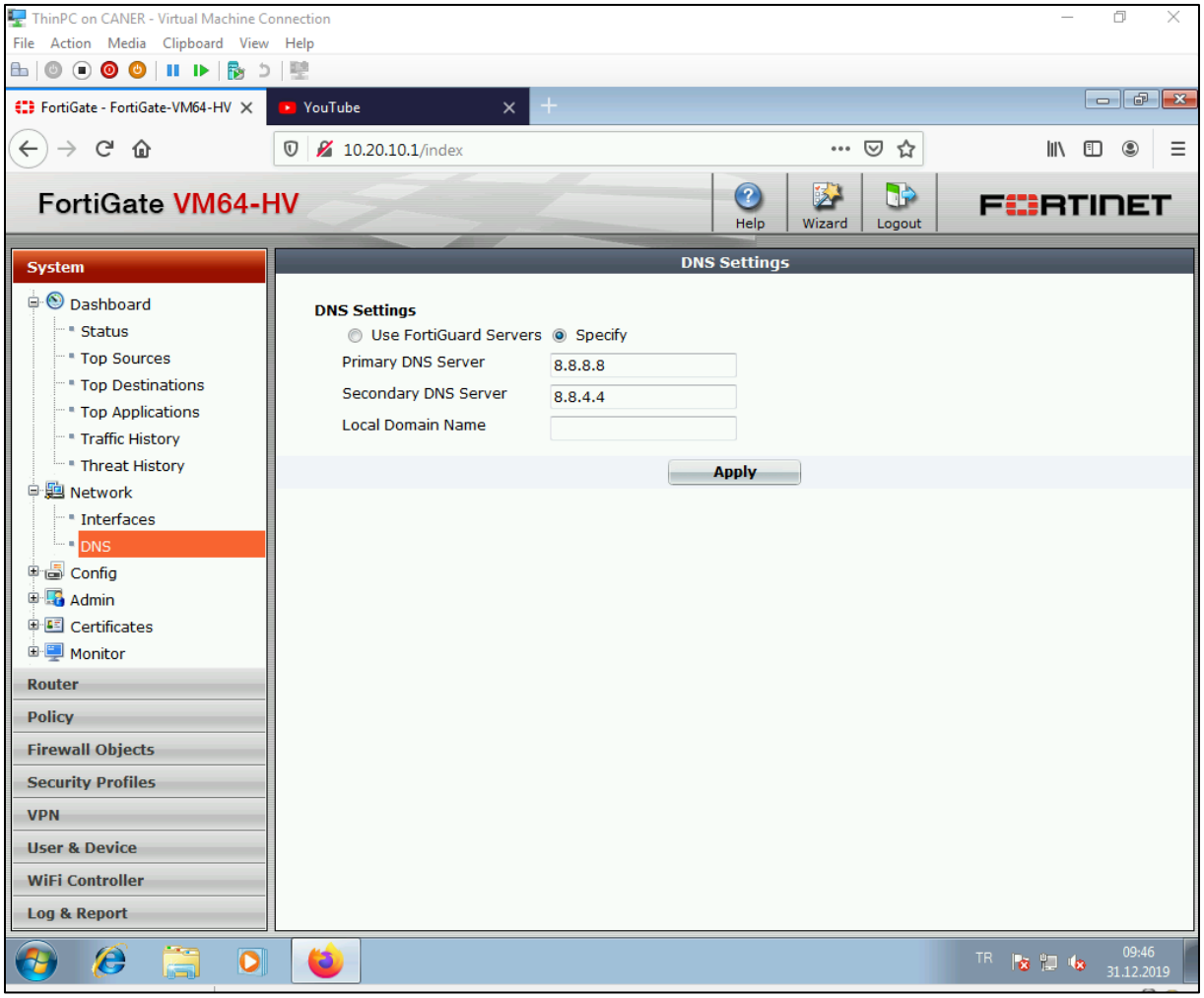
Then, click OK without changing anything else.



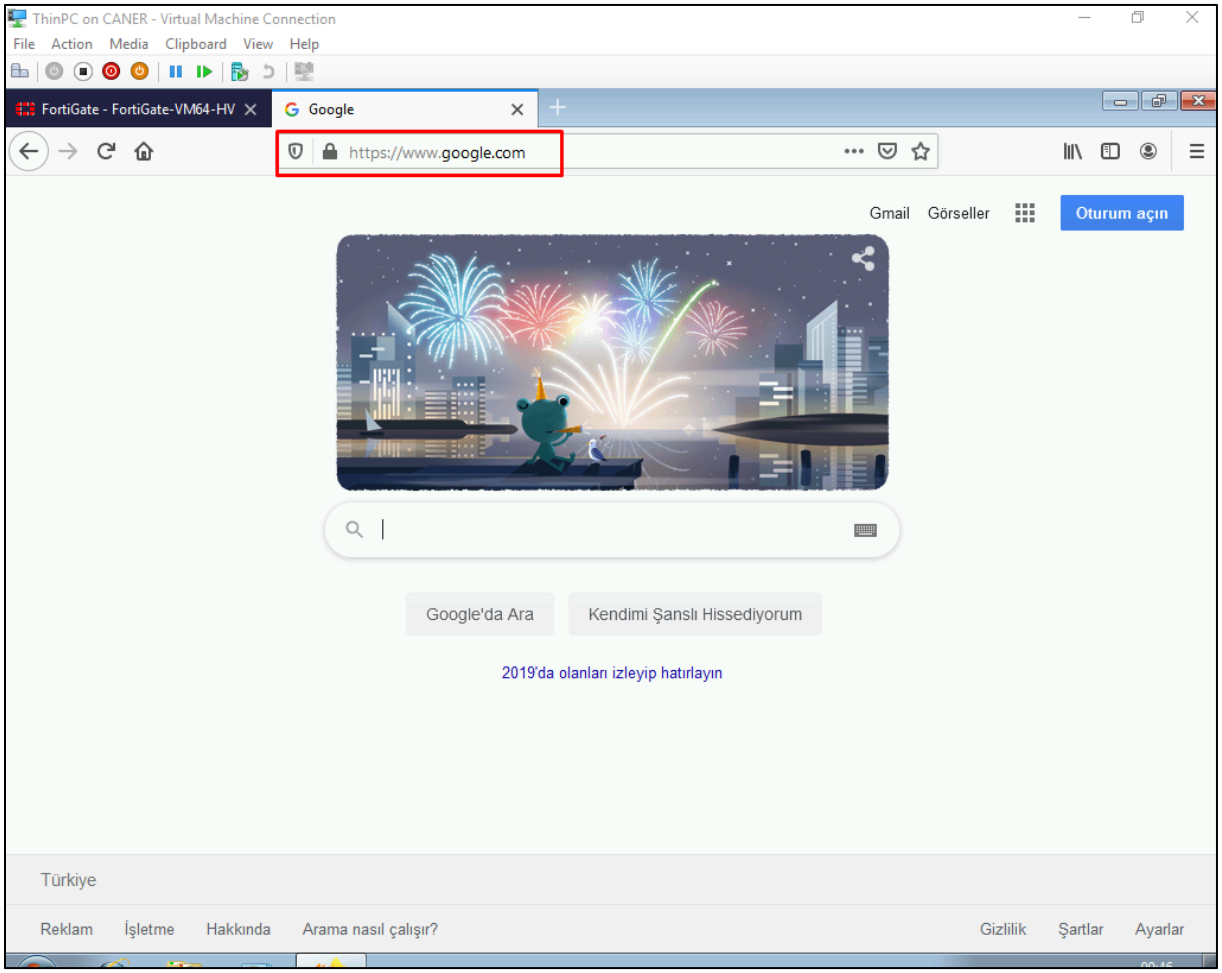
Since Fortinet didn't receive the information directly from BAU, we add a default route to the gateway of BAU's network to access the internet.



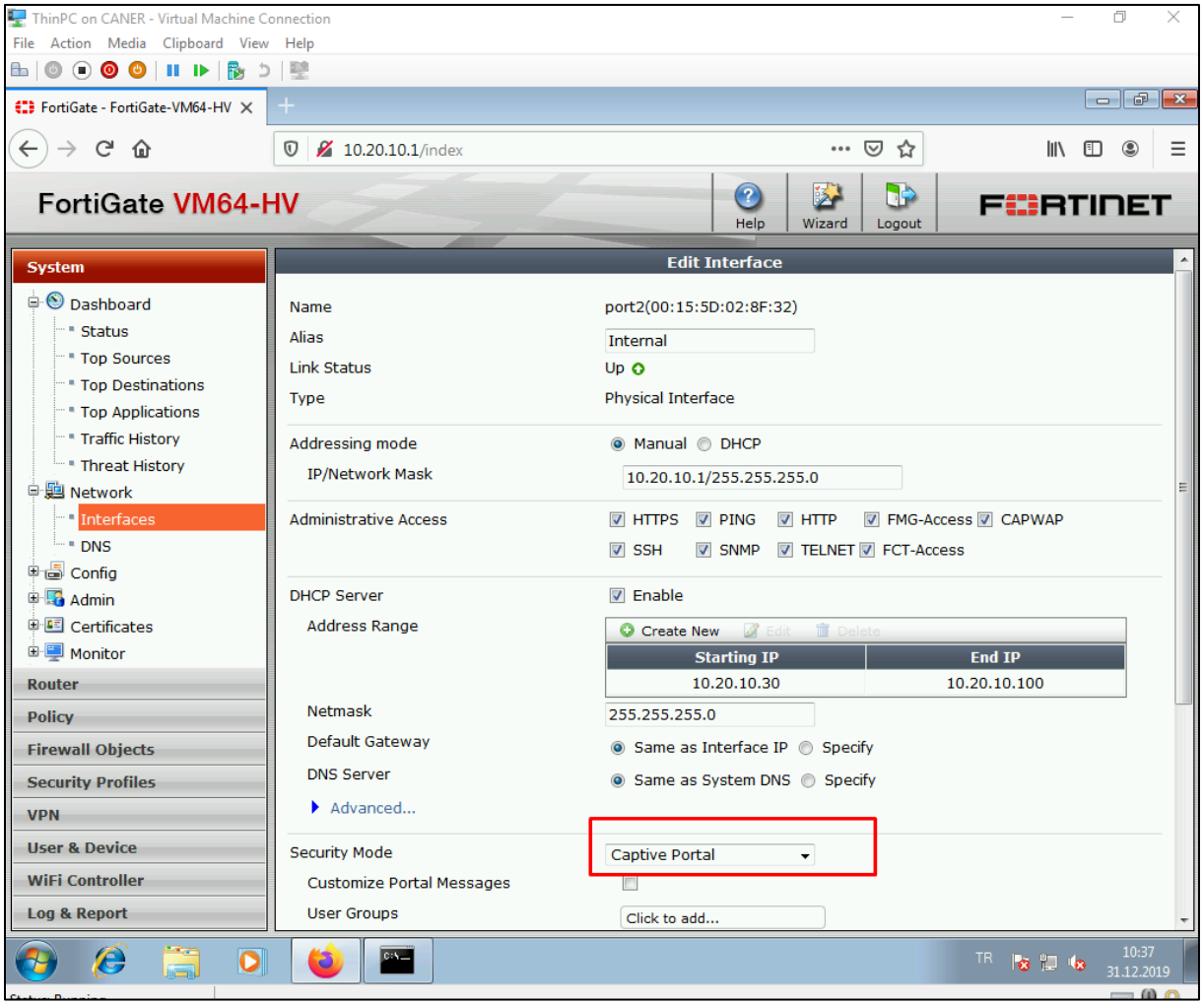
We change the DNS settings to use Google's DNS.



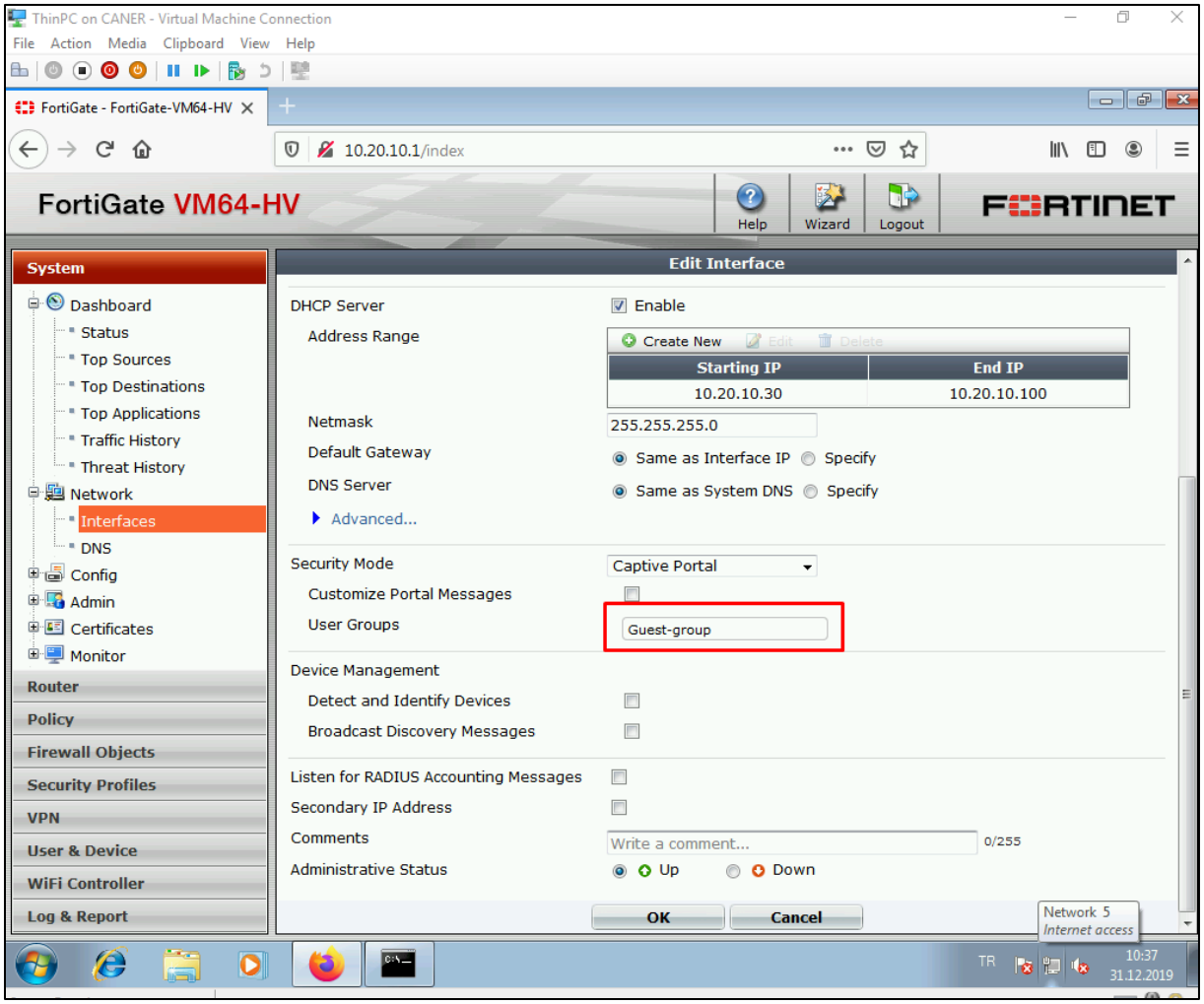
And now we can connect to the internet since NAT is enabled and access is allowed.



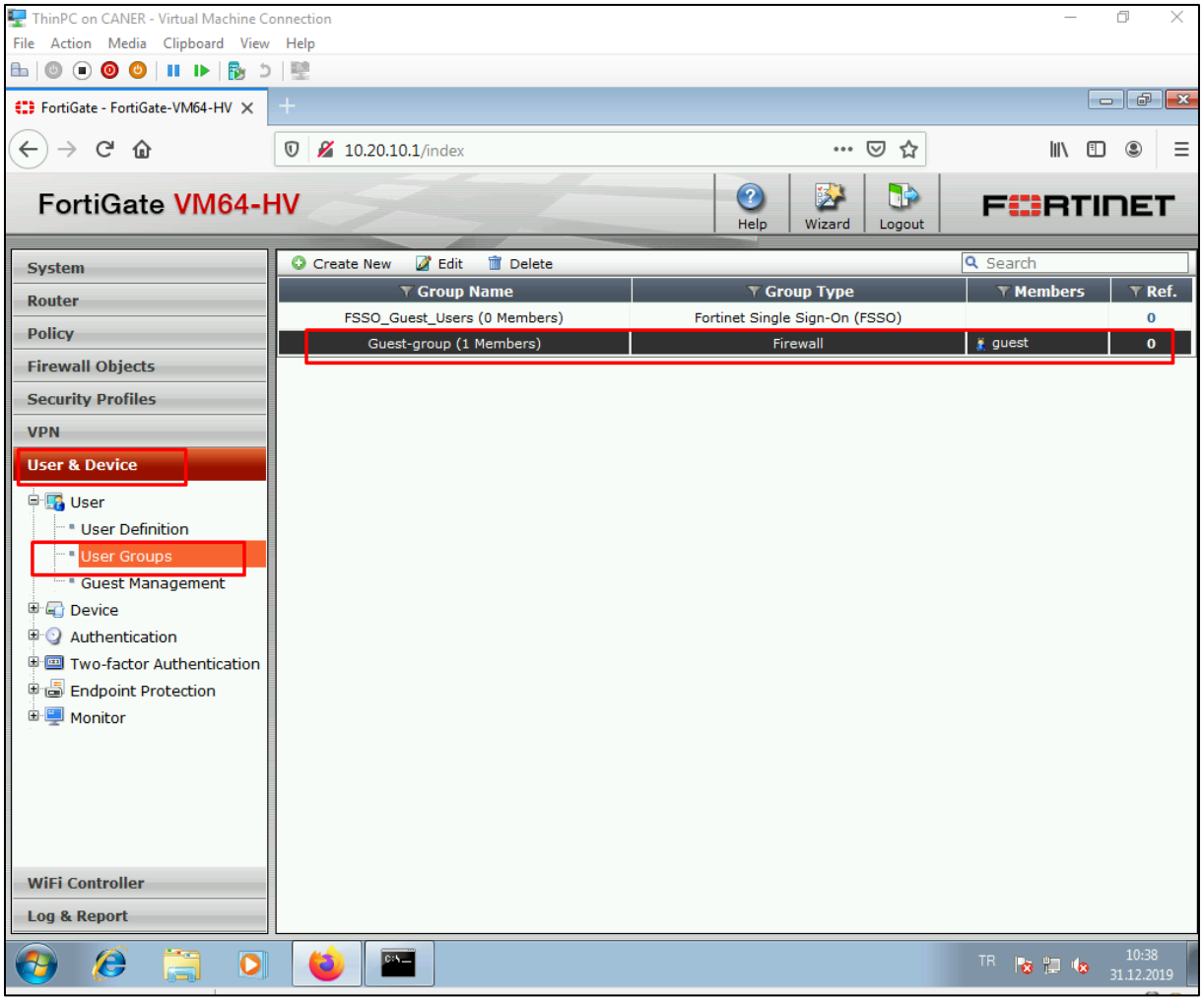
To create a Captive Portal we get to the internal interface and set the security mode.



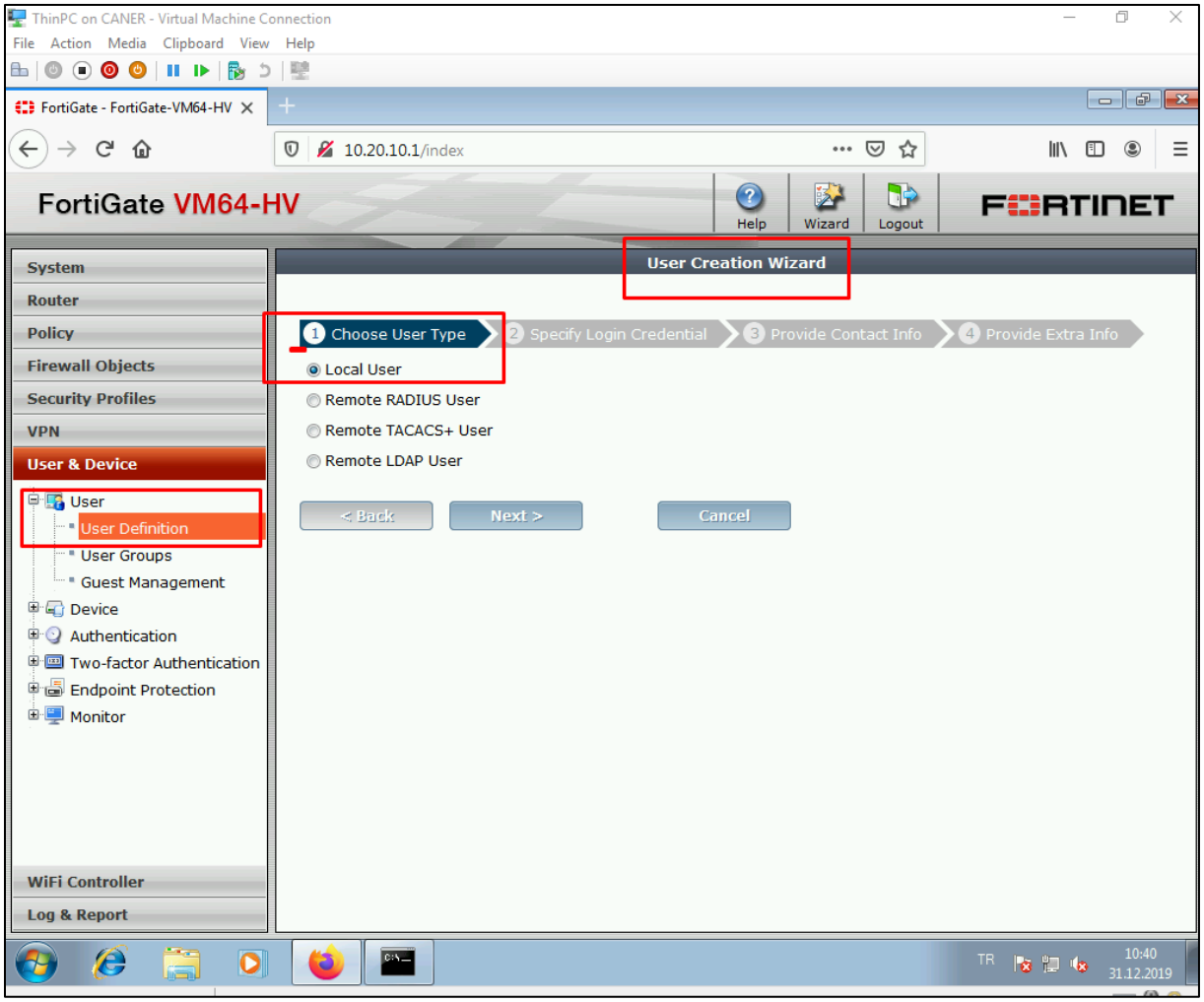
We state a user group. In this case we used the Guest-group but we will change it soon.



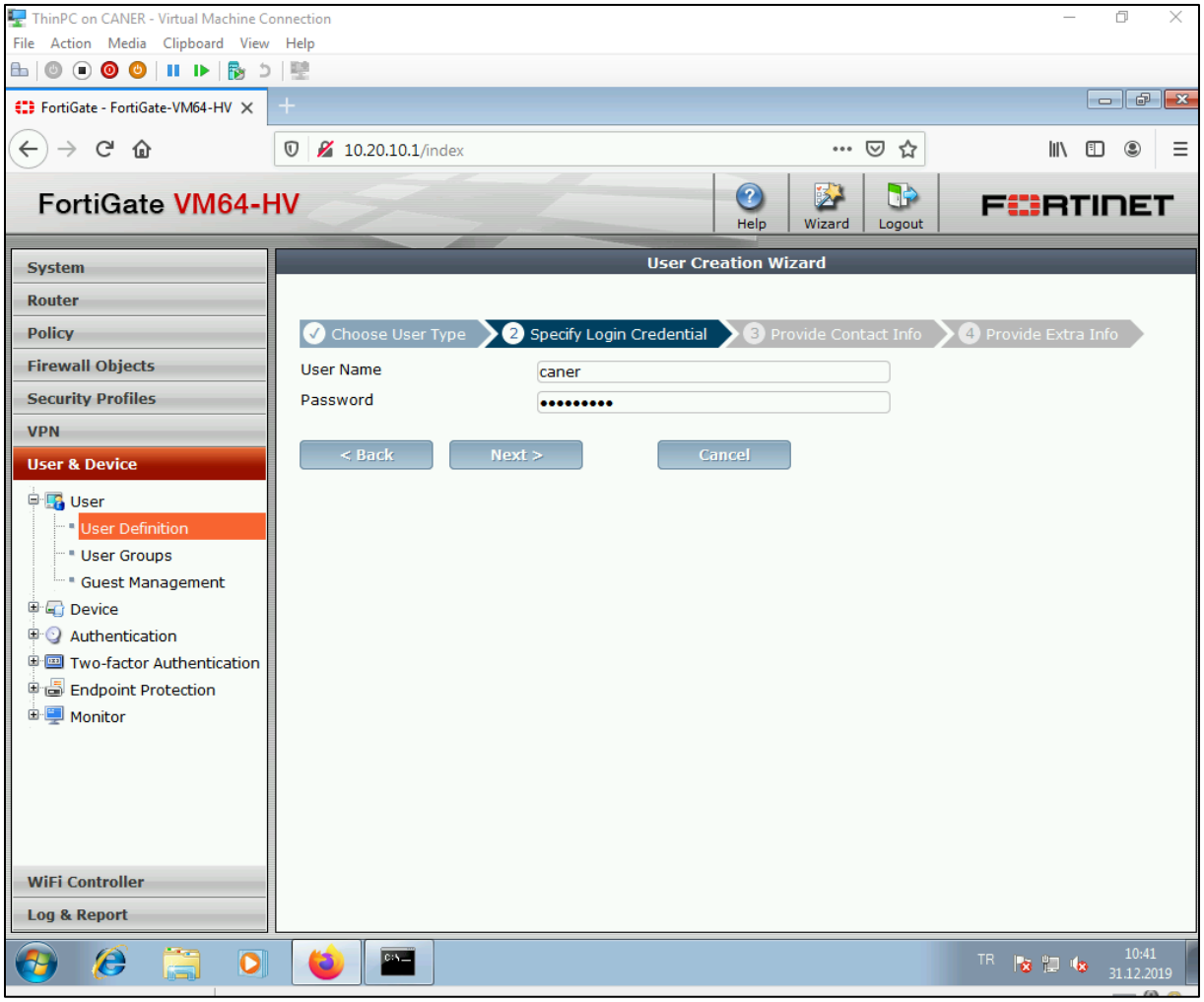
We can manage and peruse the user groups in detail under User & Device tab.



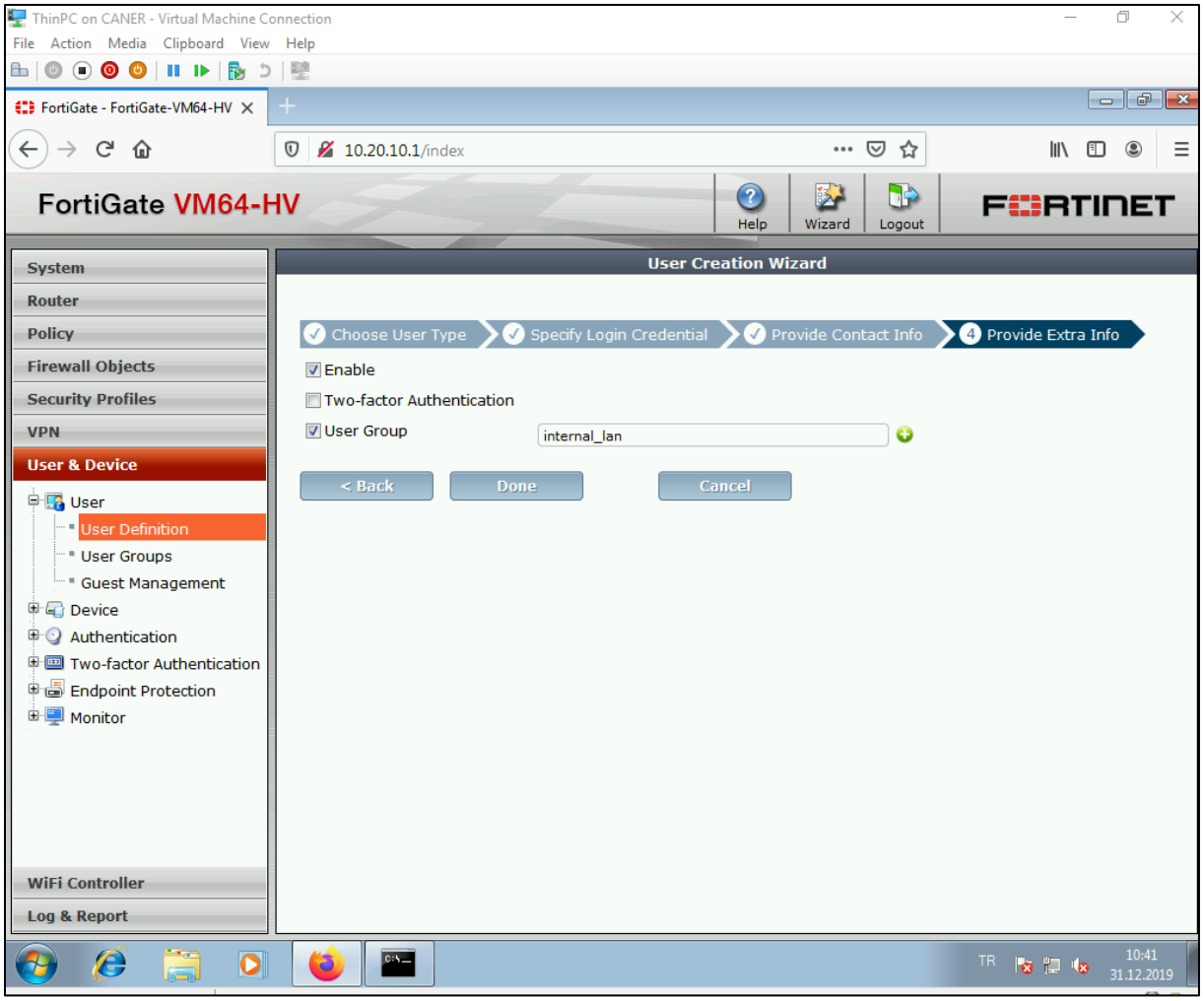
Let’s now create a new user to utilize the captive portal.



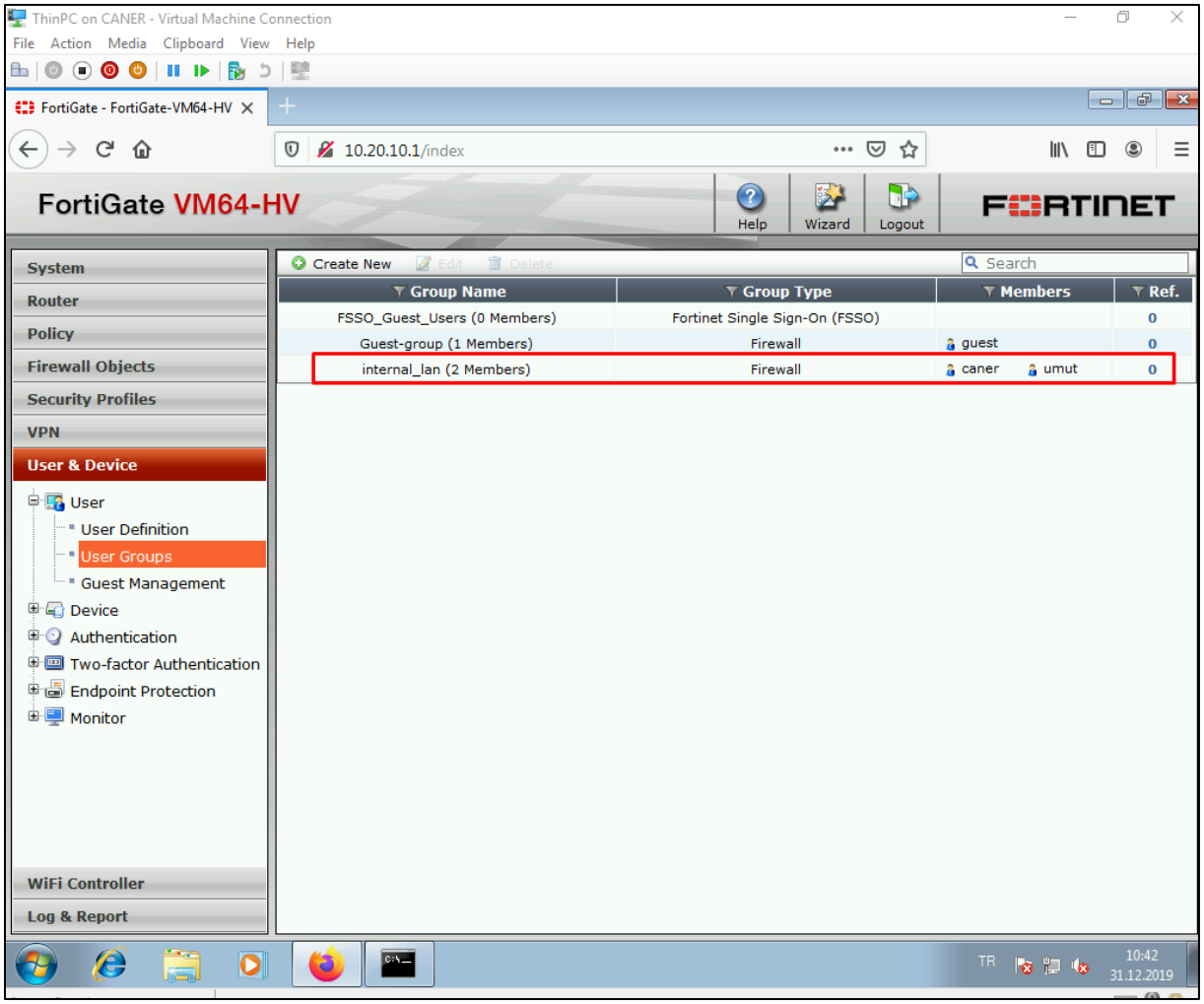
We choose local user and define the login credentials.



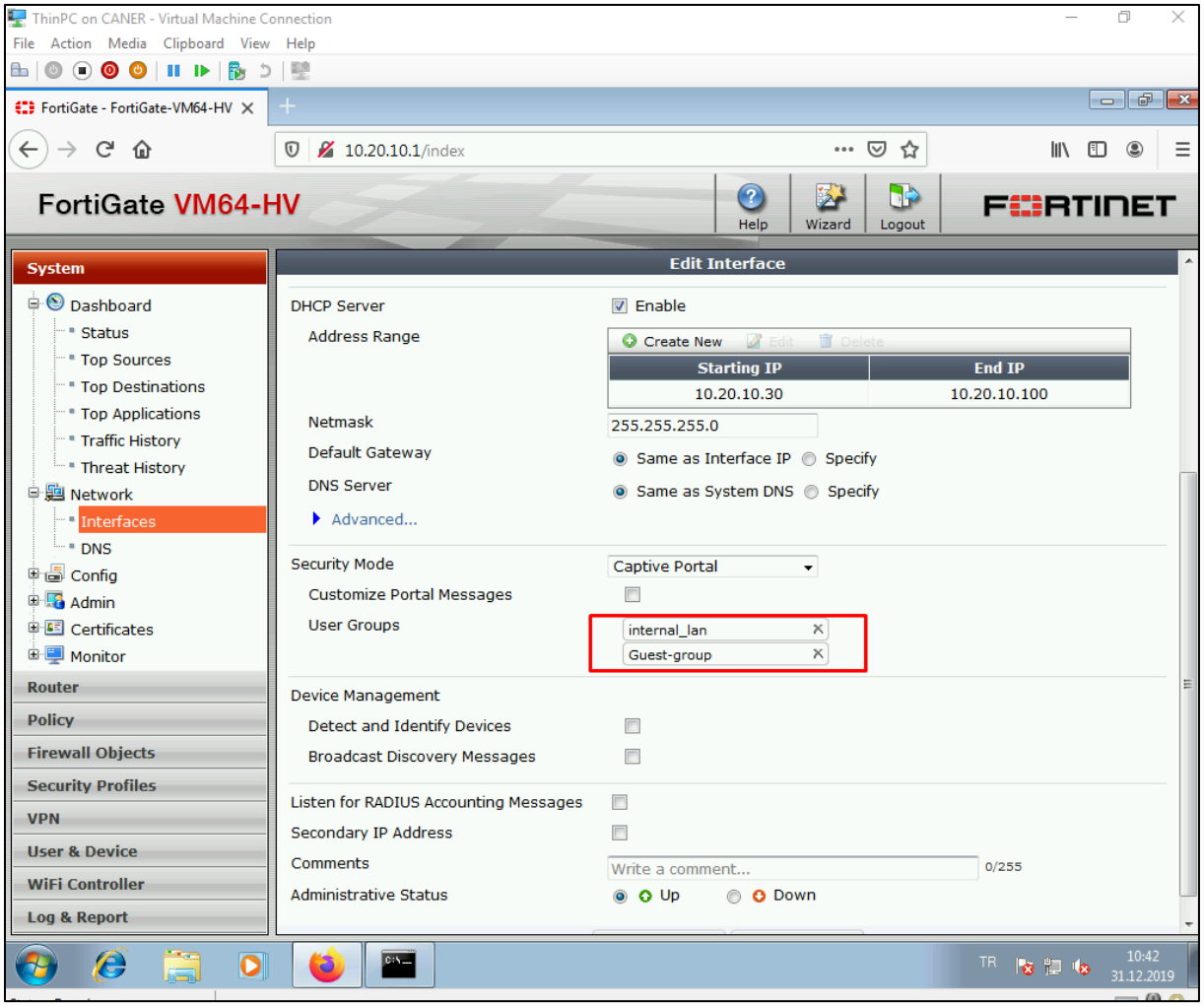
We put this user into the new user group internal_lan.



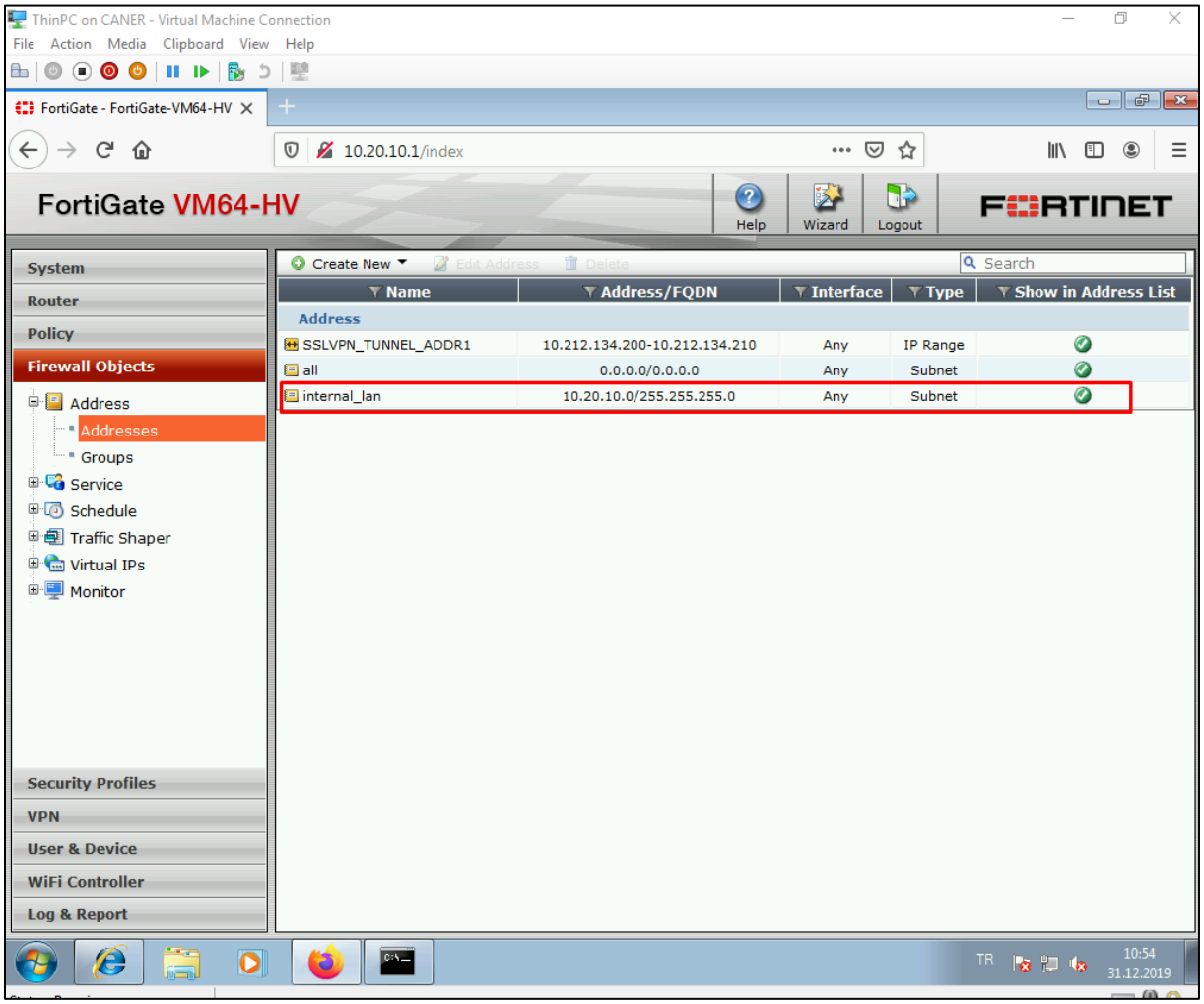
Now, when we look at the new group, we can see our new users.



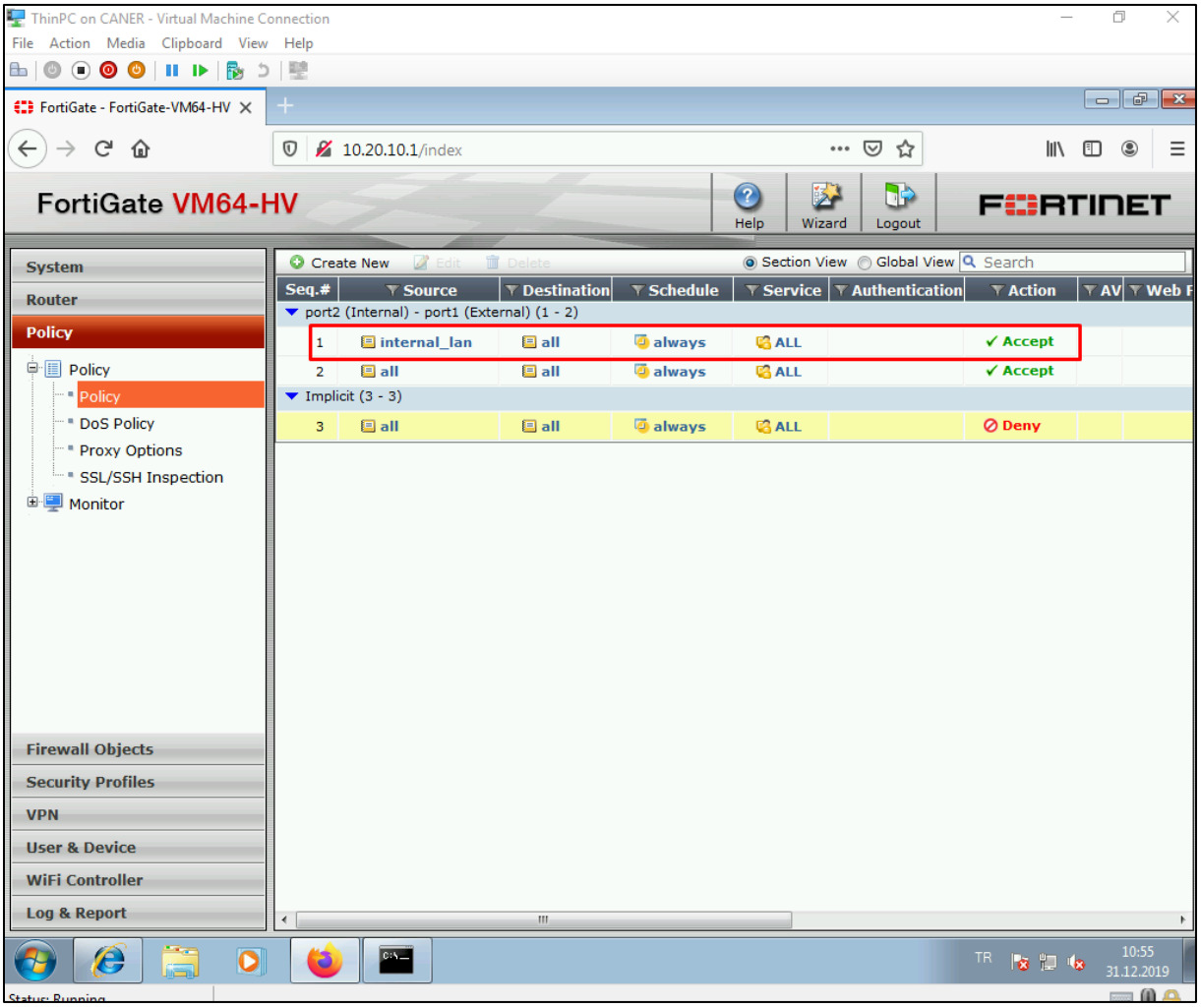
We add the internal_lan to the captive portal rules as well.



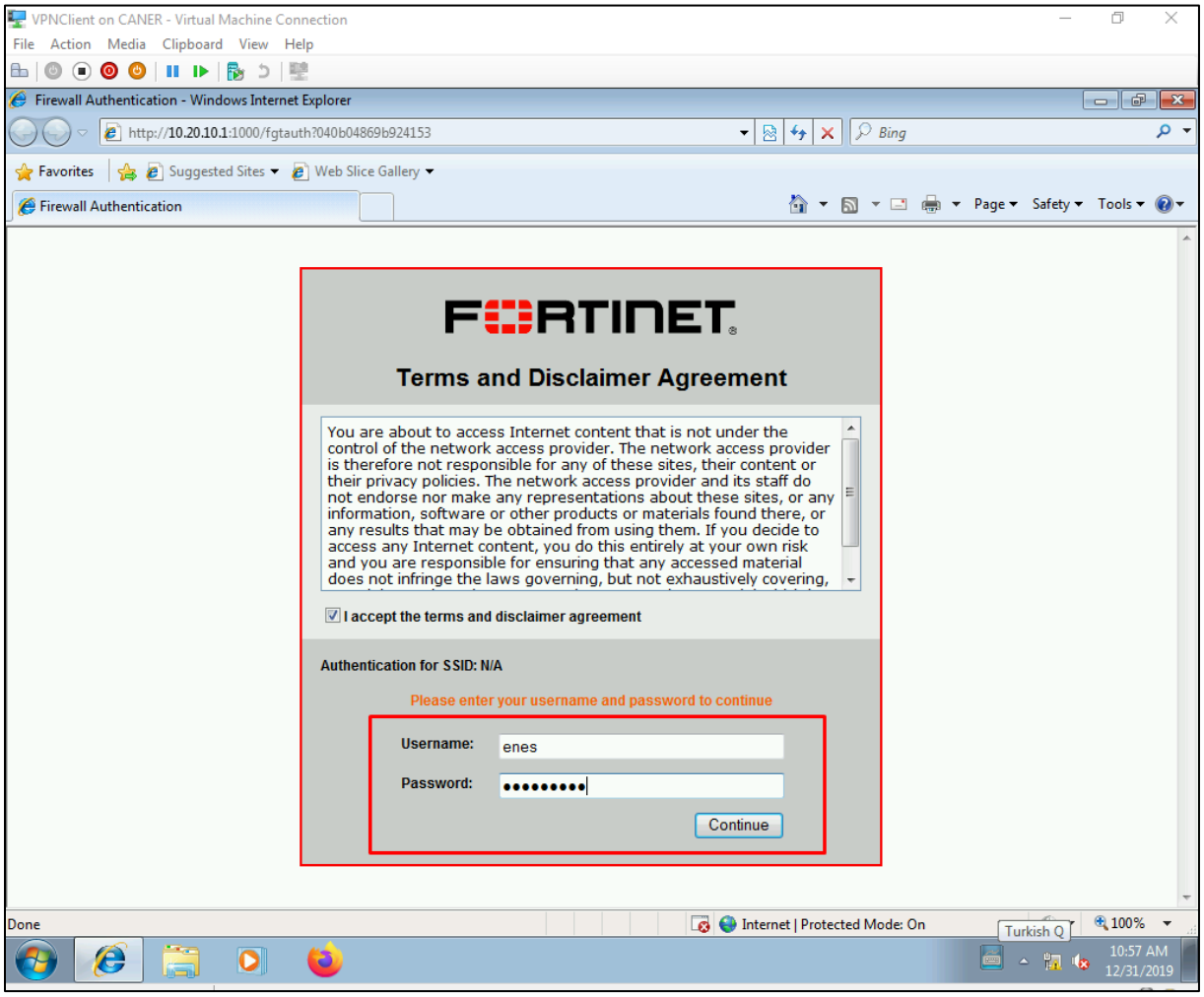
When we get to the Firewall Objects, under addresses. internal_lan should be already there automatically but we could also create it easily.



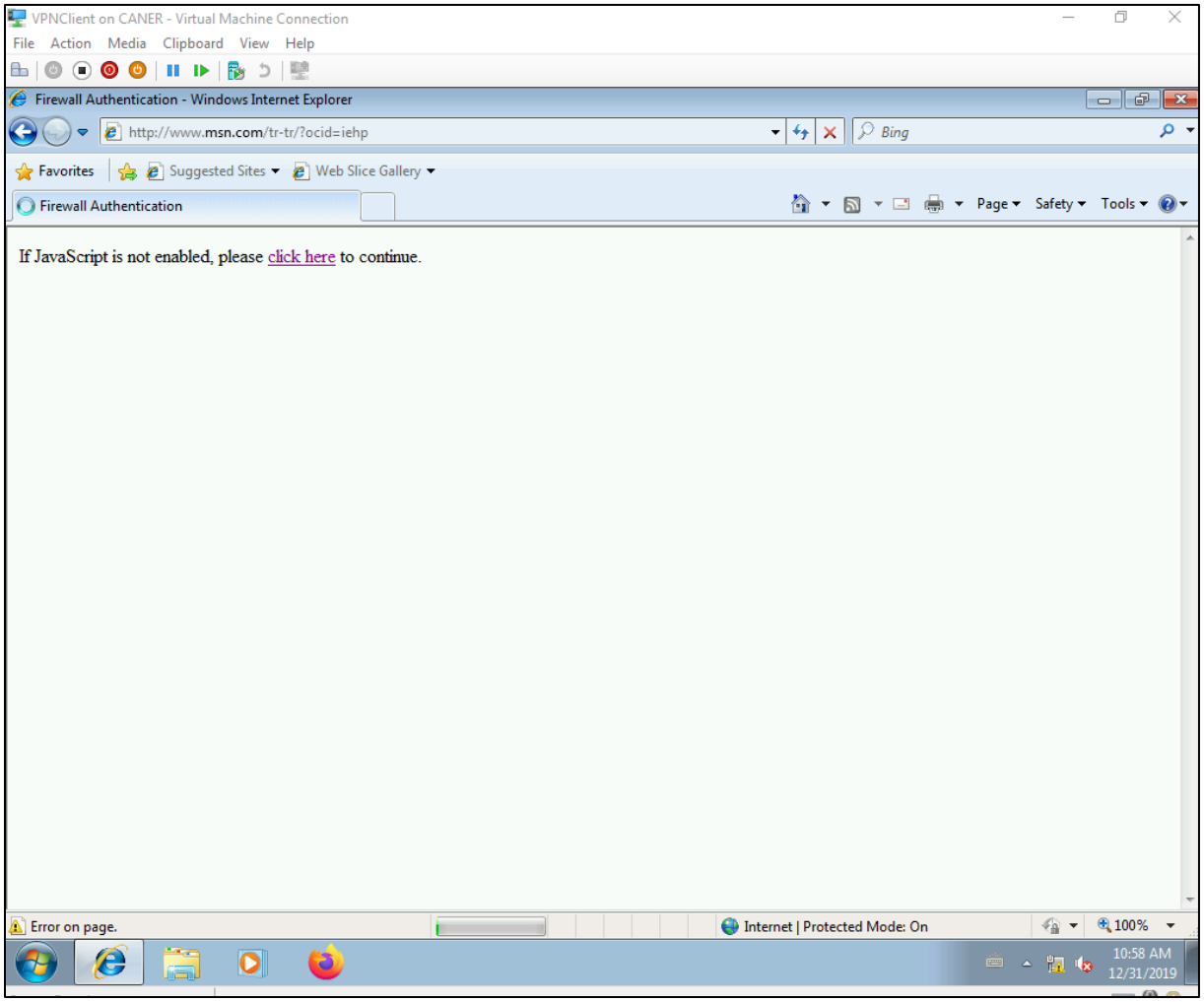
Now, we modify the policies to allow internal_lan specifically to access to the internet.



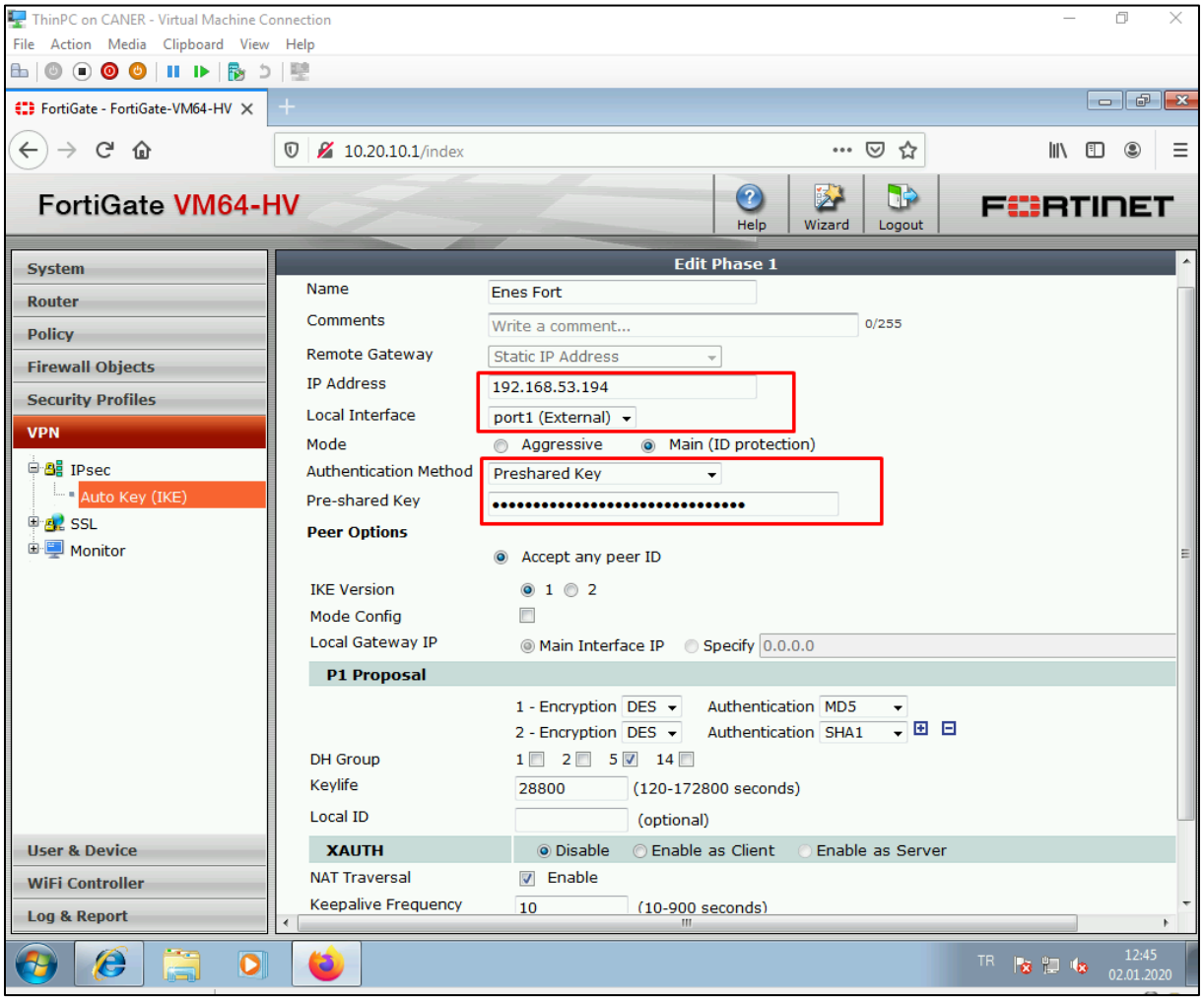
When a host tries to connect to the internet using the internal_lan group's IP addresses. This Captive Portal page pops up. We log in using a user's credentials.



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

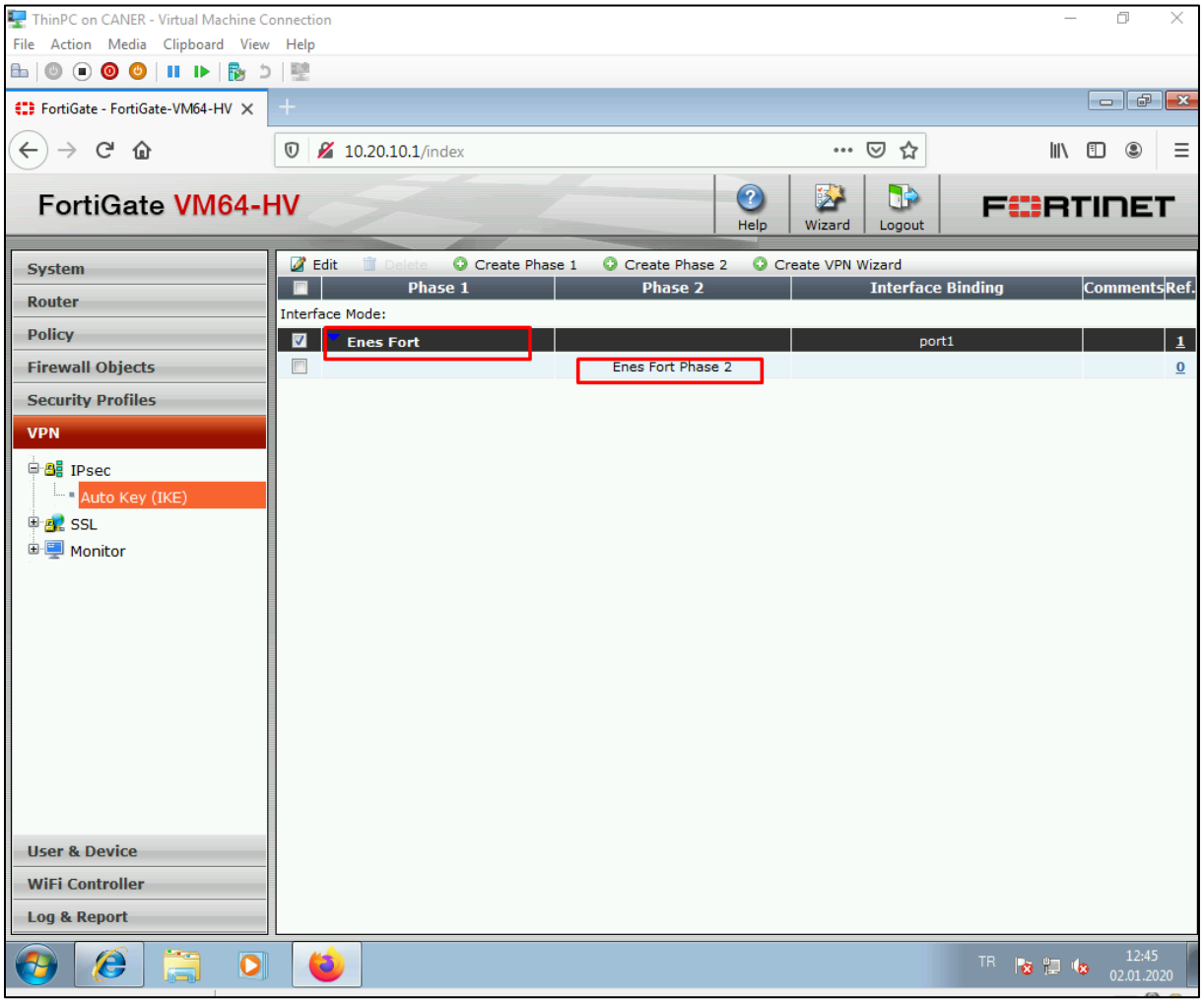


Now that the unstimulating stuff is out of the way, let's establish an IPSec Tunnel. We go to the VPN tab and click on Create Phase 1 to start the wizard.

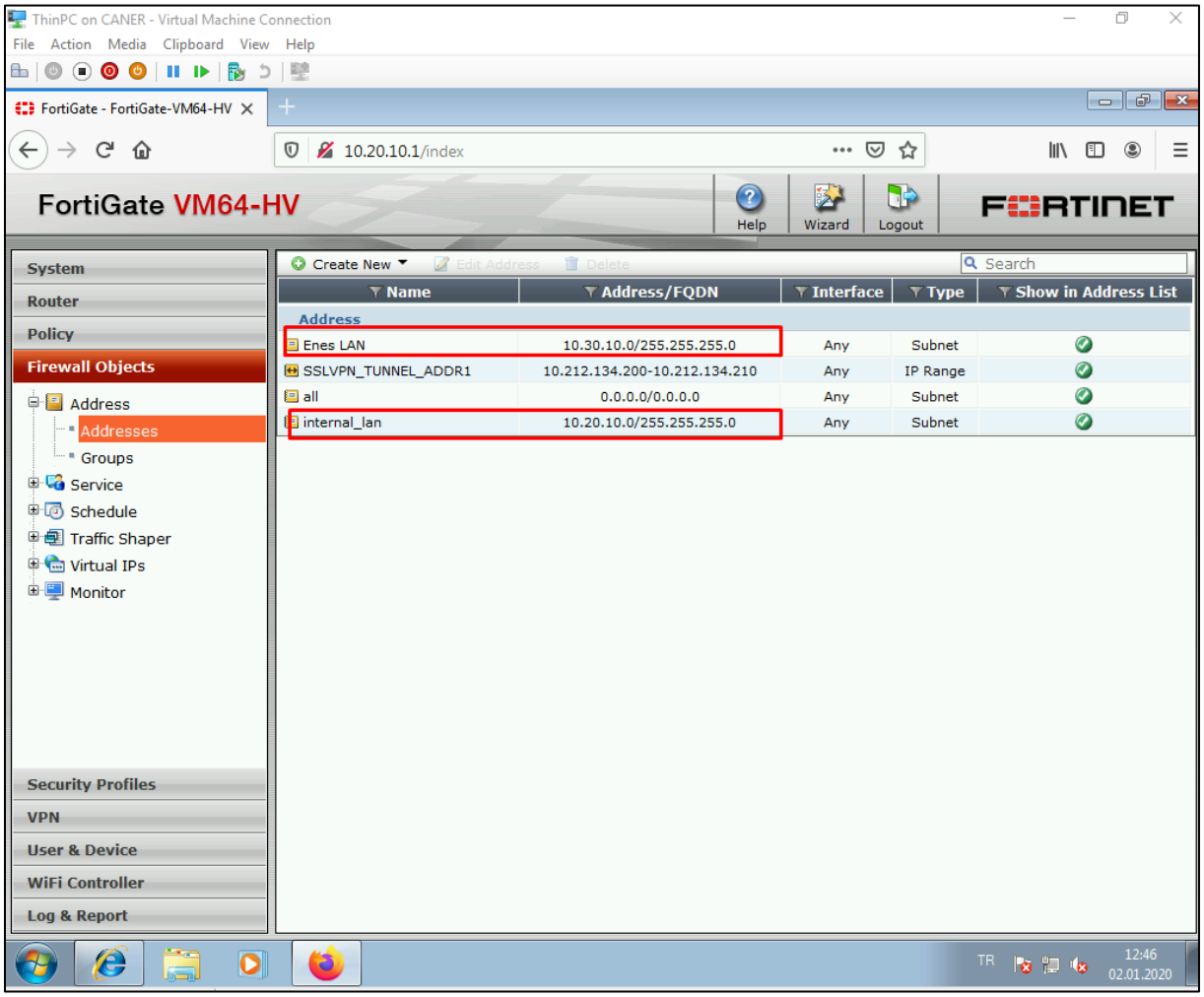


We name the tunnel and use the other site's public IP address and our port1 (WAN interface) for the local interface. We describe a pre-shared key and leave every other encryption setting to default. The other site must do the vice versa with out IP address, their WAN port and the same pre-shared key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

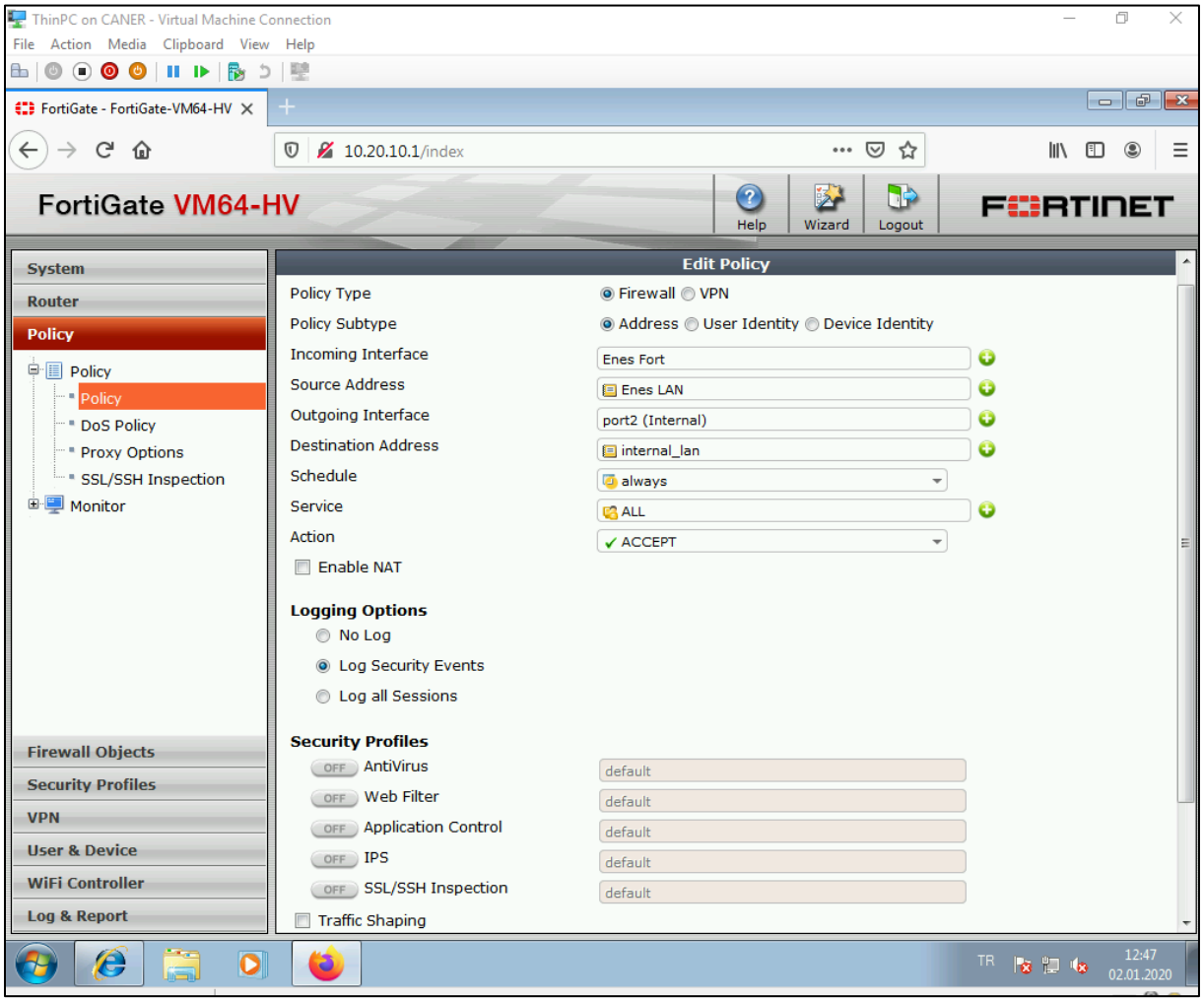
We then select freshly created Phase 1 to create a Phase 2 related to that. The default settings are sufficient. The Phase 2 should look like this:



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

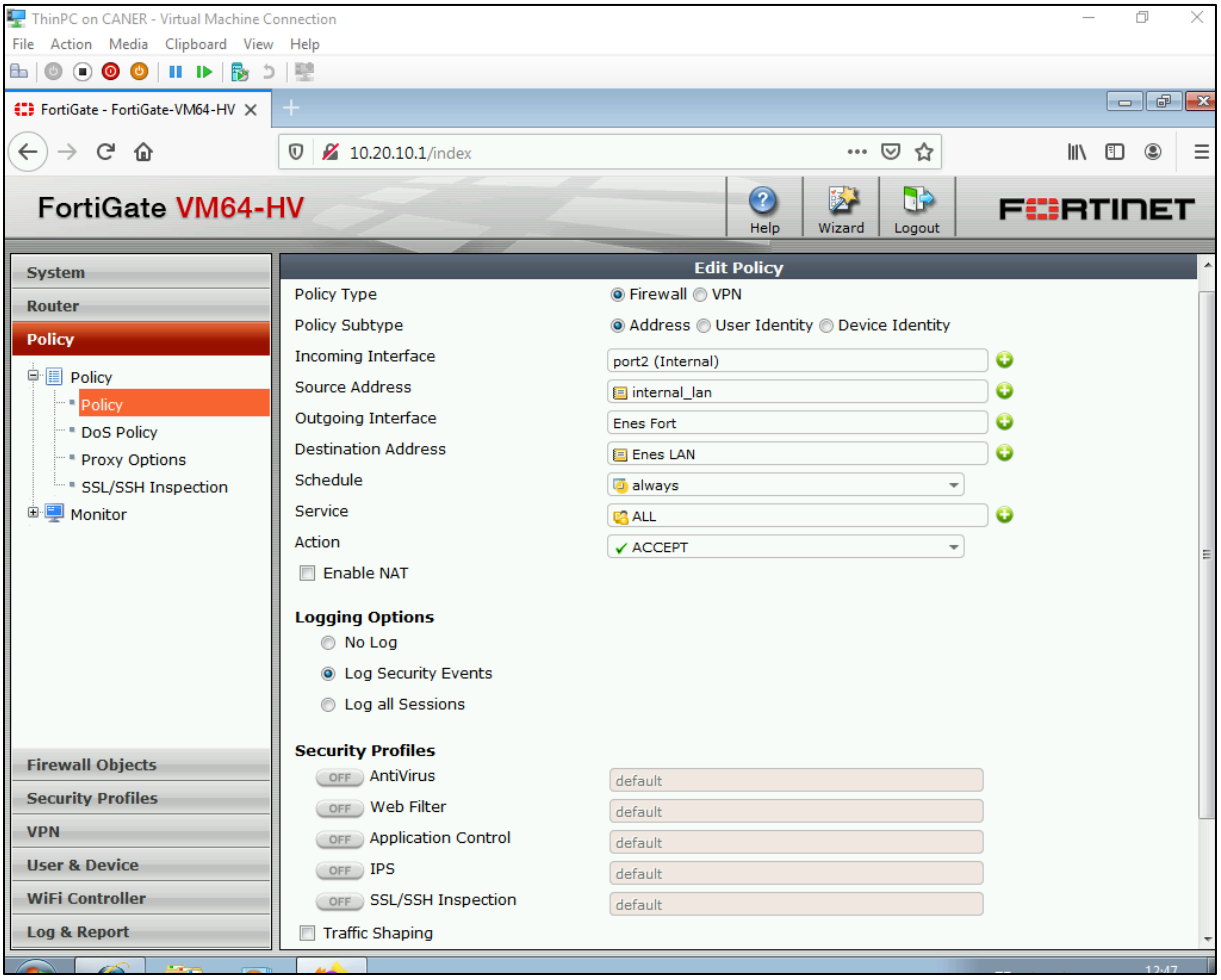


We state the following rules since FortiGate VM64-HV doesn't really support site-to-site tunnels as a pre set rules system. I'd definitely not recommend using this outside of a lab.

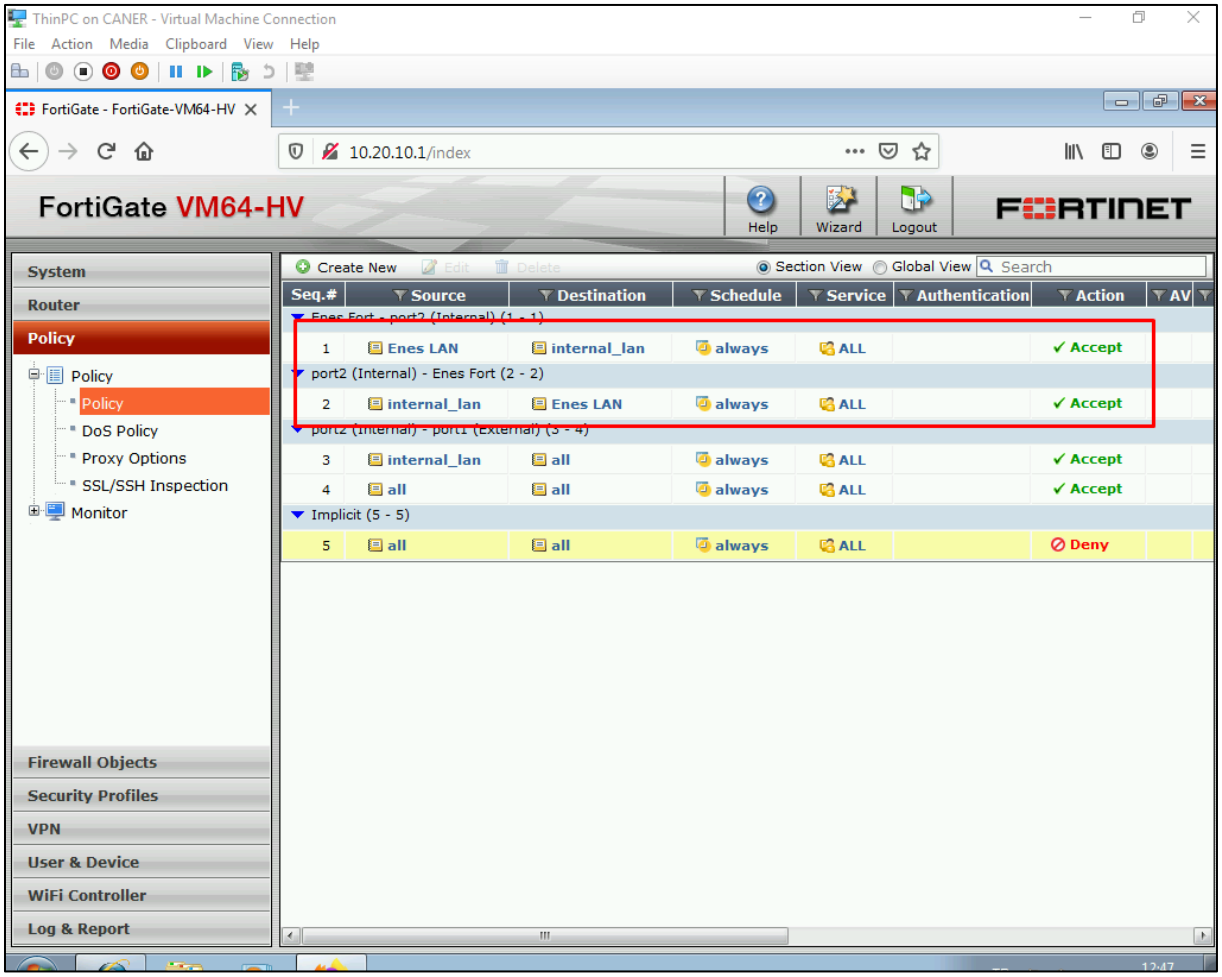


Note that we chose the tunnel as an interface.

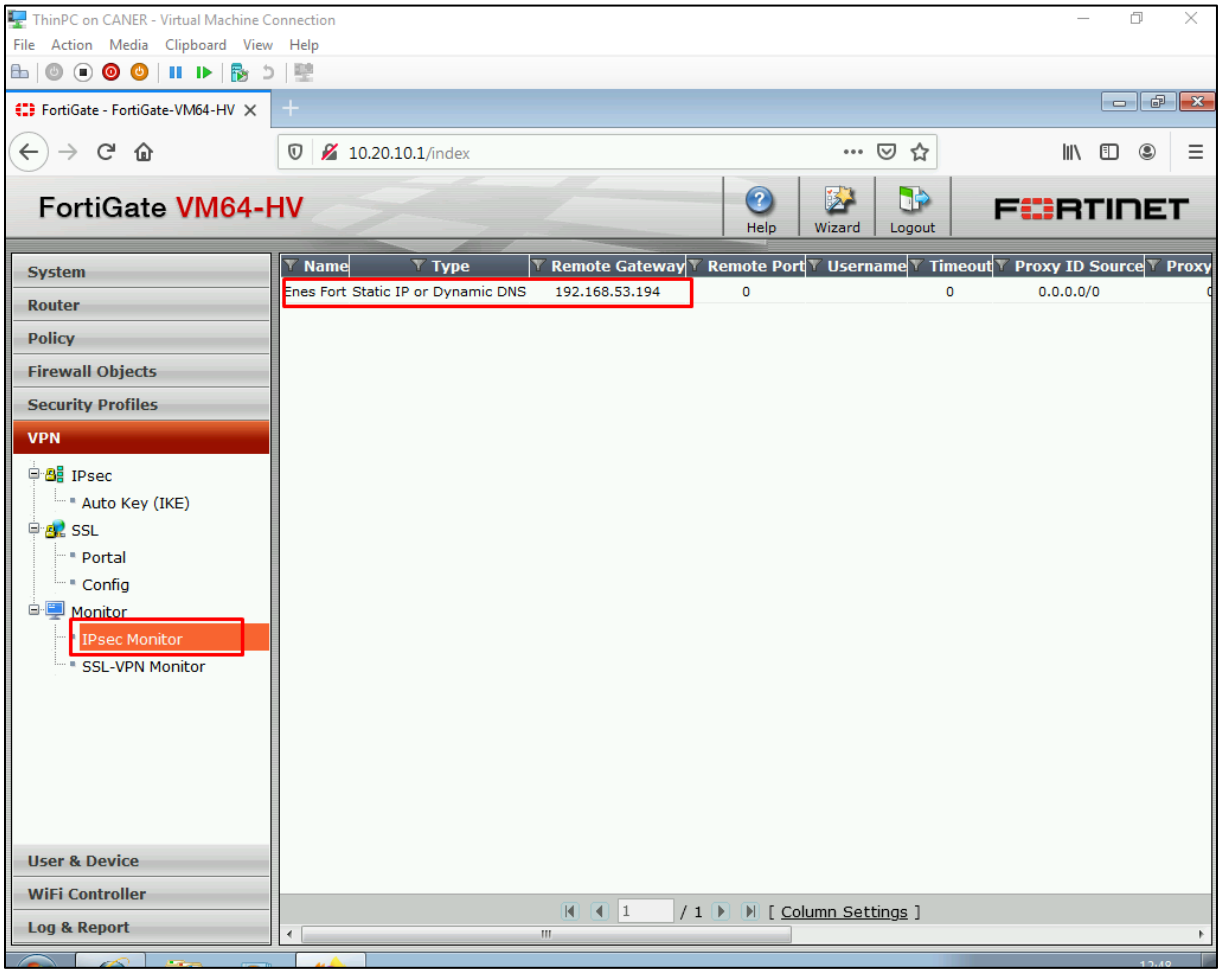
And the vice versa rule is also necessary.



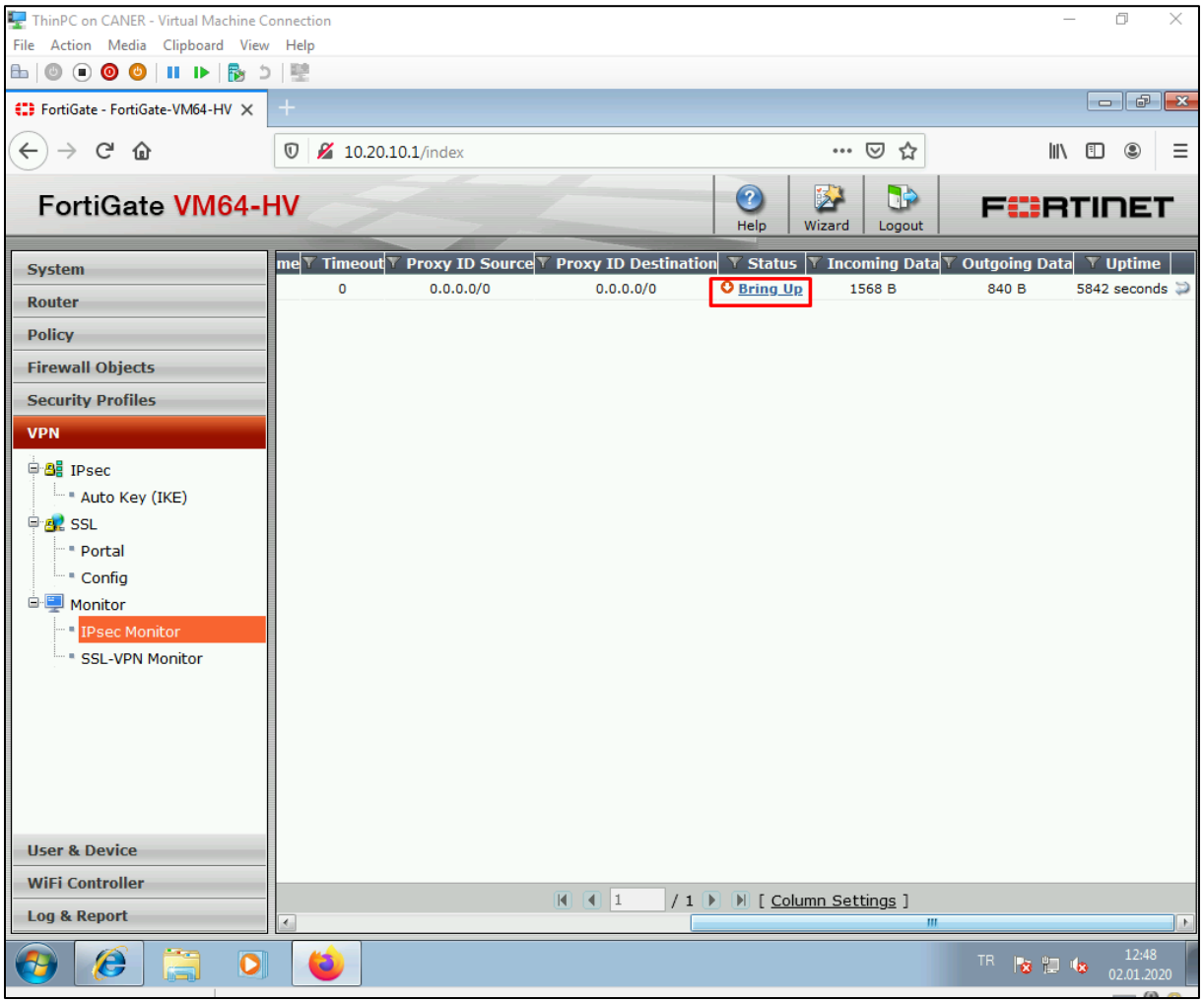
The policies should like this.



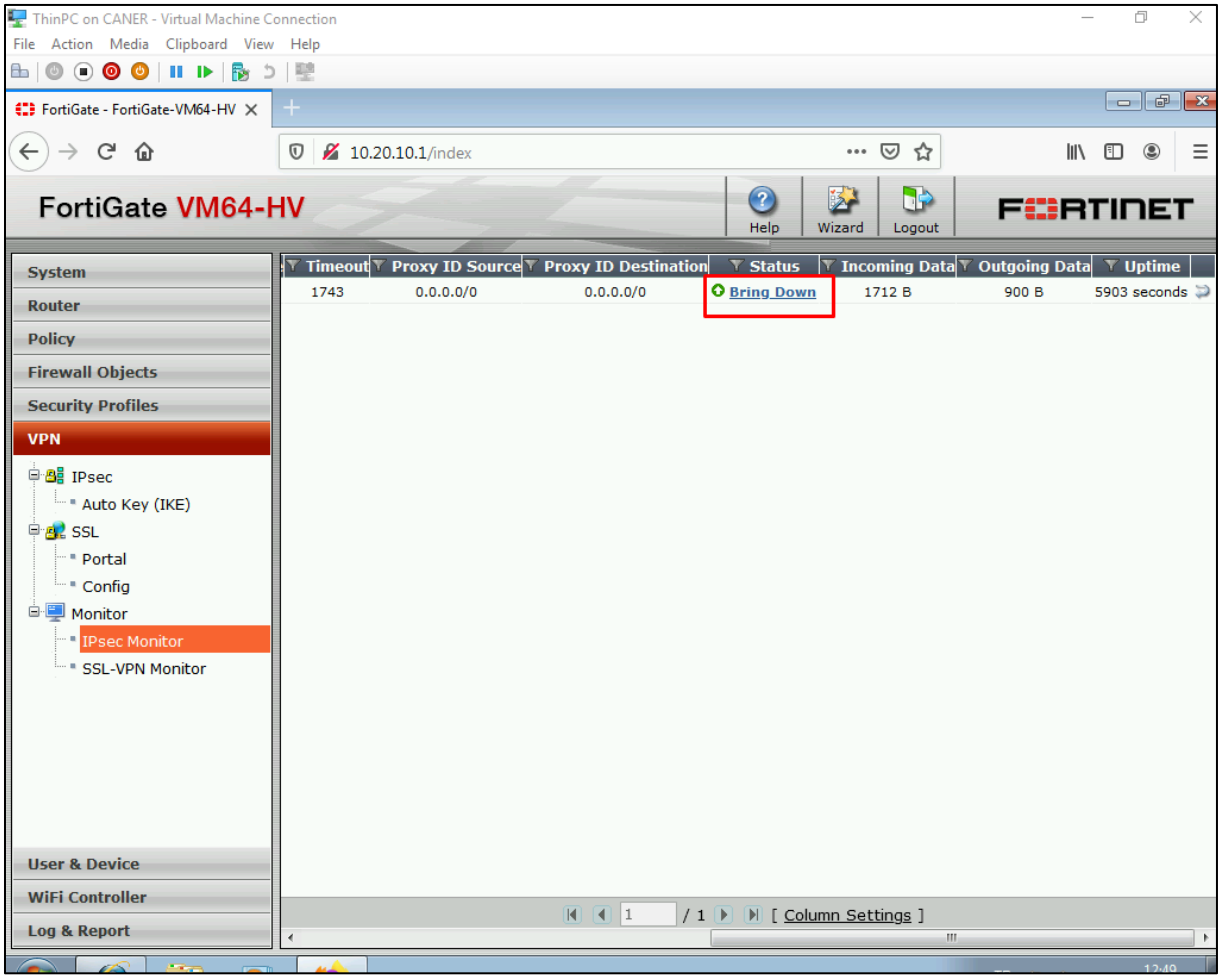
Now, when we get to the VPN tab and click on Monitor we should see the tunnel that we named.



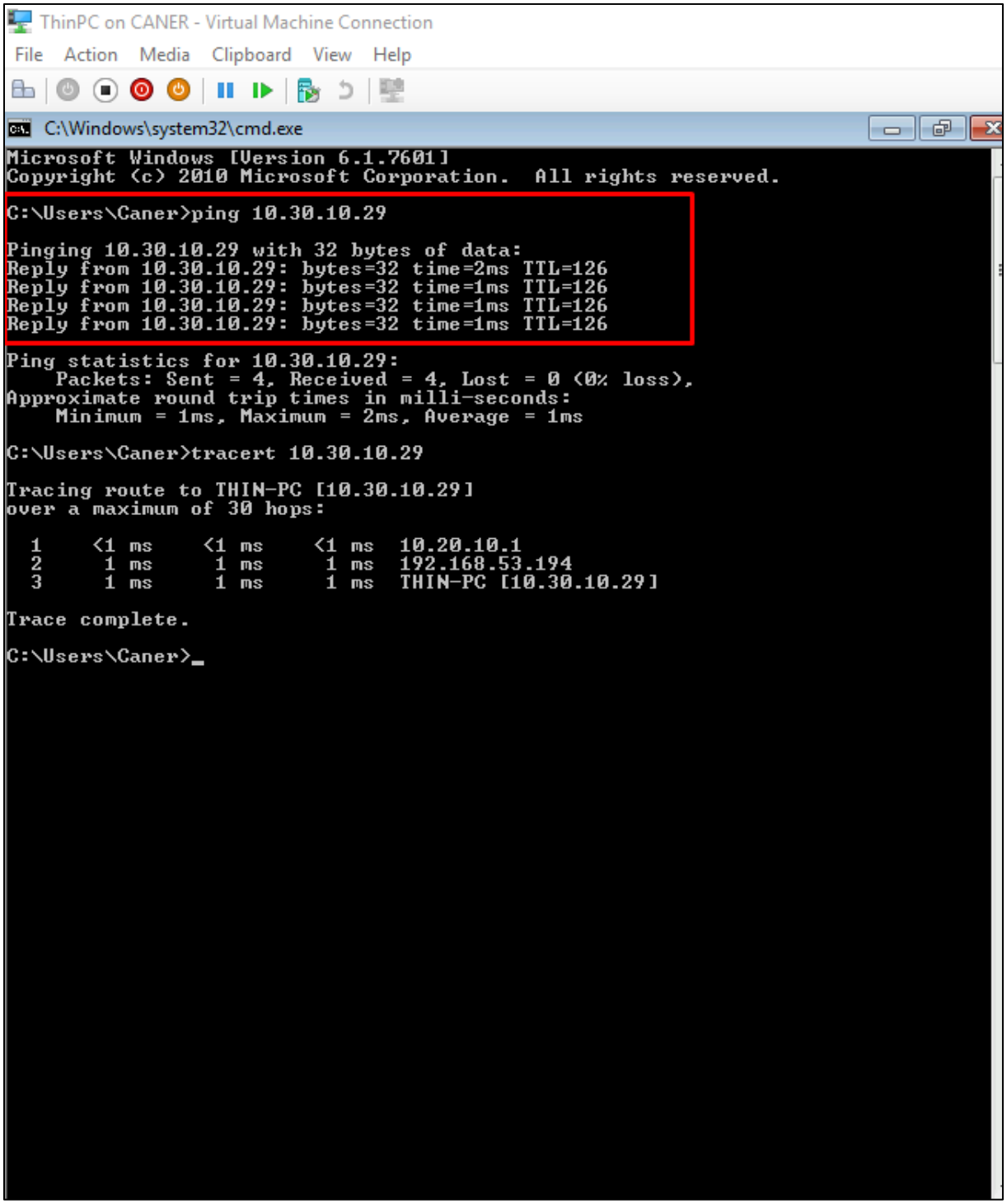
Currently, it's down; however, if we have set everything correctly on both ends, mirroring each other, and made sure that the pre-shared key and the encryption details are the same when we click on Bring Up, it should work.



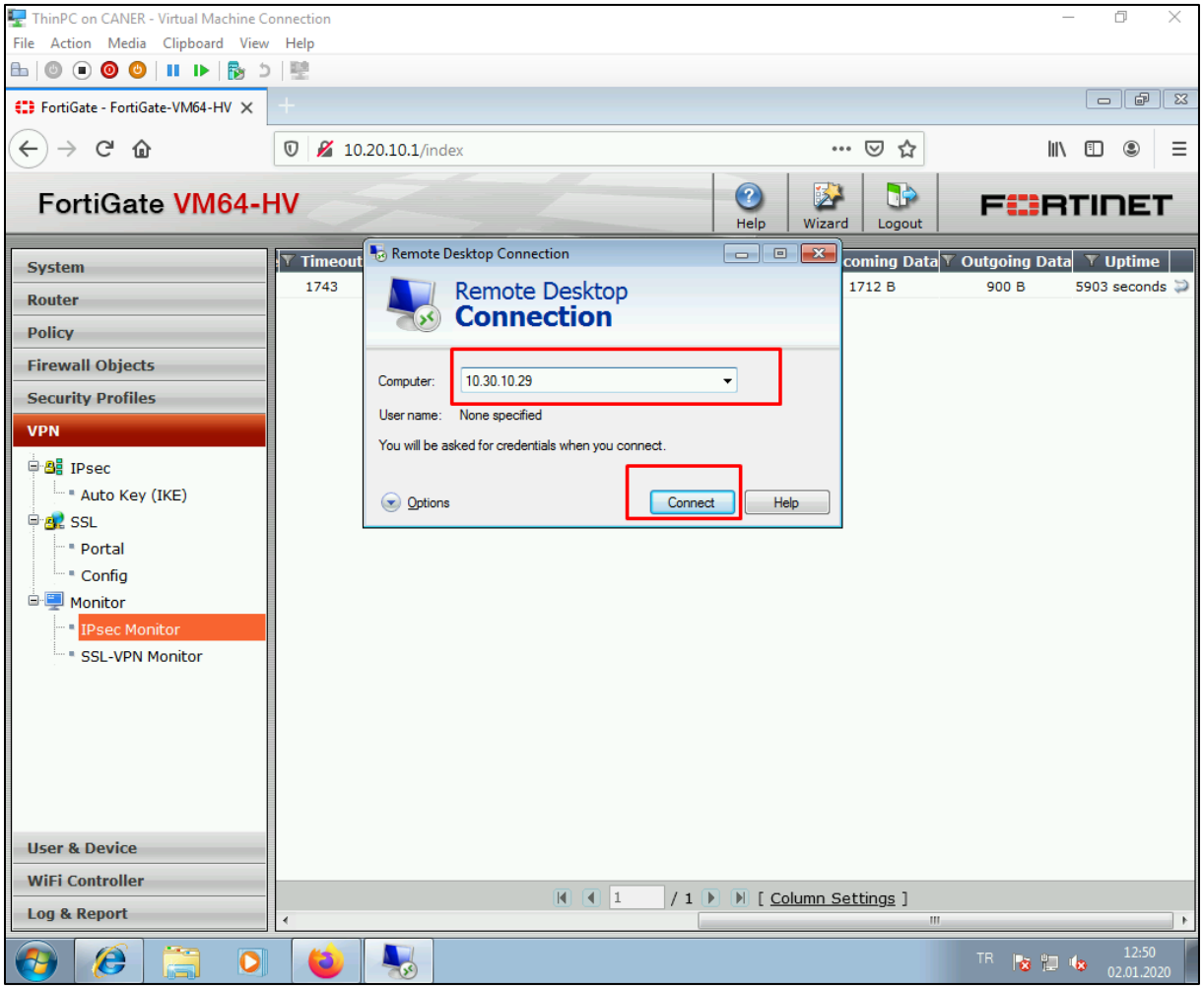
It works beautifully.

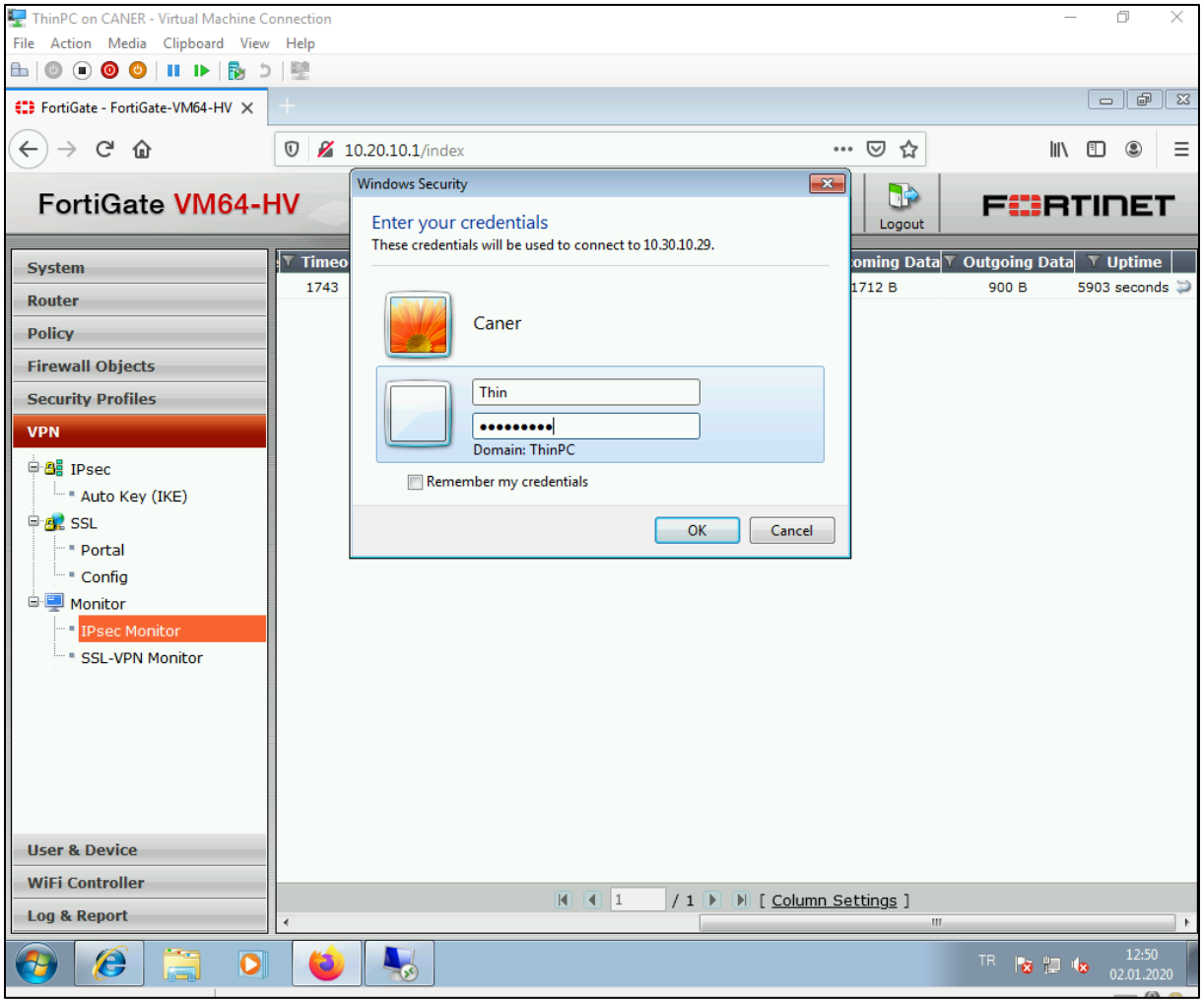


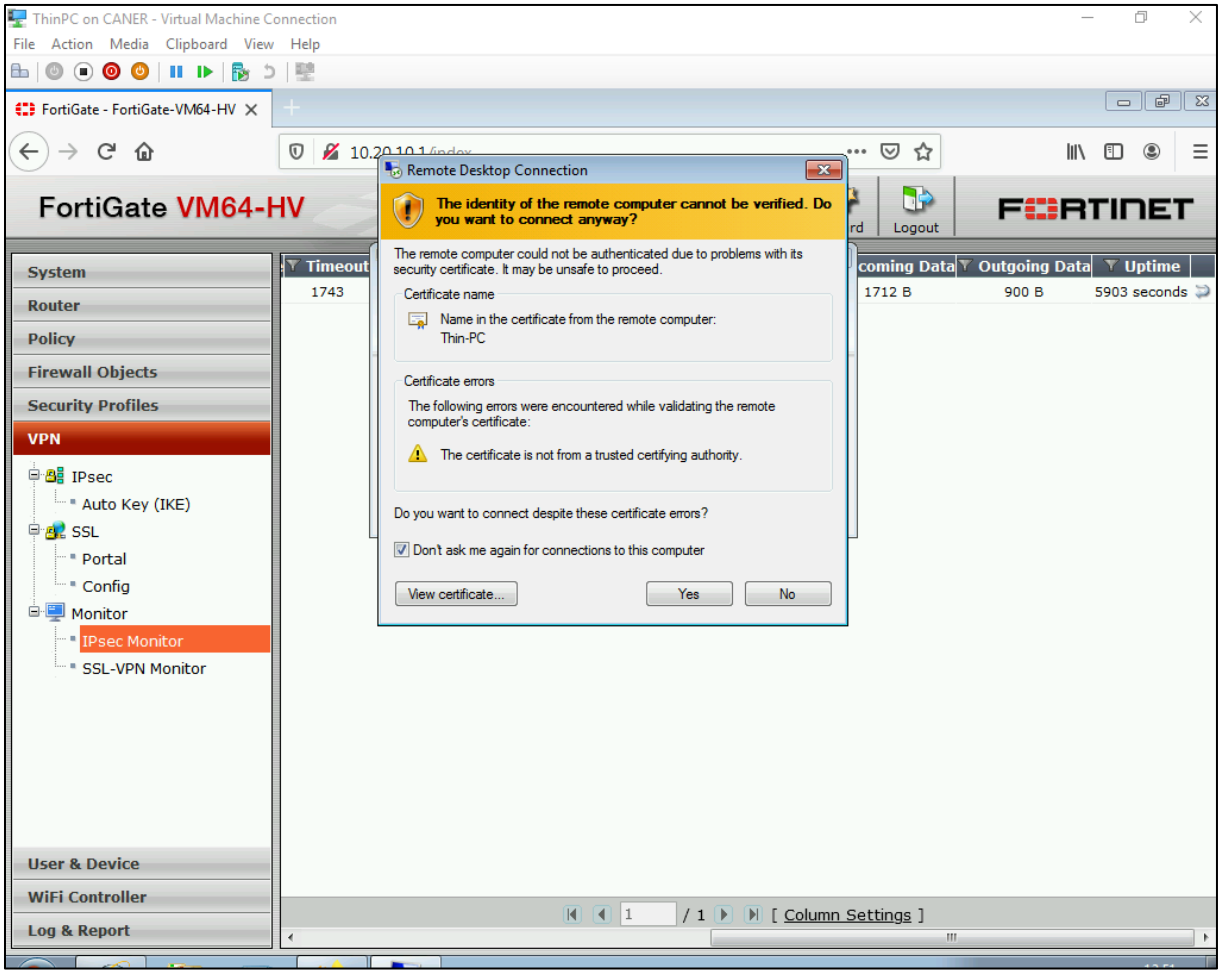
Now, we can ping from site 1's internal LAN to site 2's internal LAN.



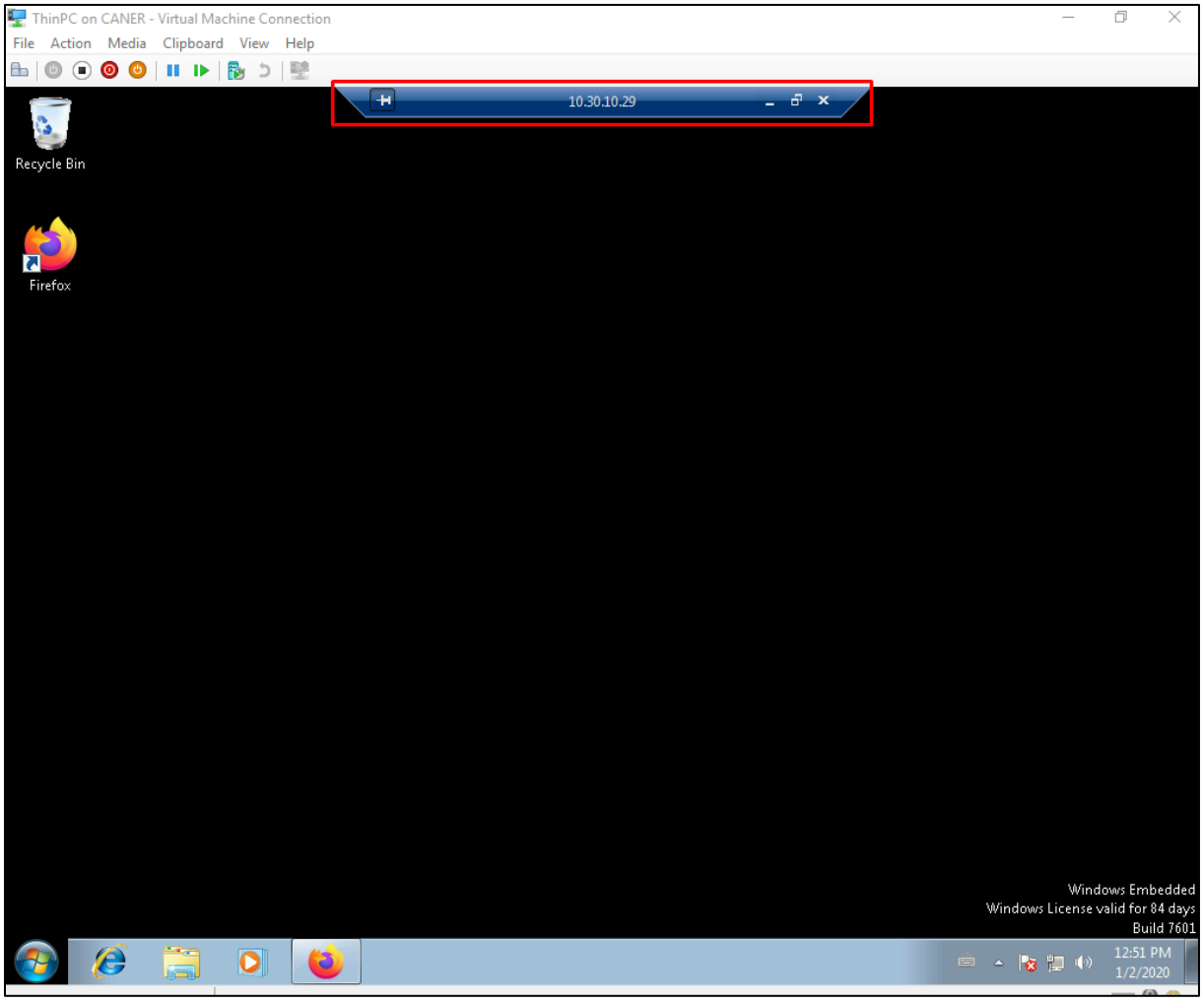
We can also easily do RDP by entering the local IP addresses of the other site.




ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
FortiGate - FortiGate-VM64-HV
10.20.10.1/index
FortiGate VM64-HV
Logout
FORTINET
System
Router
Policy
Firewall Objects
Security Profiles
VPN
IPsec
Auto Key (IKE)
SSL
Portal
Config
Monitor
IPsec Monitor
SSL-VPN Monitor
User & Device
WiFi Controller
Log & Report
Timeo
Outgoing Data
Uptime
1743
1712 B
900 B
5903 seconds
Windows Security
Enter your credentials
These credentials will be used to connect to 10.30.10.29.
Caner
Thin
Domain: ThinPC
Remember my credentials
OK
Cancel
[Column Settings]
TR
12:50
02.01.2020


ThinPC on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
FortiGate - FortiGate-VM64-HV
FortiGate VM64-HV
Logout
FORTINET
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
Thin-PC
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
System
Router
Policy
Firewall Objects
Security Profiles
VPN
IPsec
Auto Key (IKE)
SSL
Portal
Config
Monitor
IPsec Monitor
SSL-VPN Monitor
User & Device
WiFi Controller
Log & Report
Timeout
Outgoing Data
Uptime
1743
1712 B
900 B
5903 seconds
[Column Settings]

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.