پاکستان سِول ایوی ایشن اتھارٹی

Prepared by – Sohail Ahmed

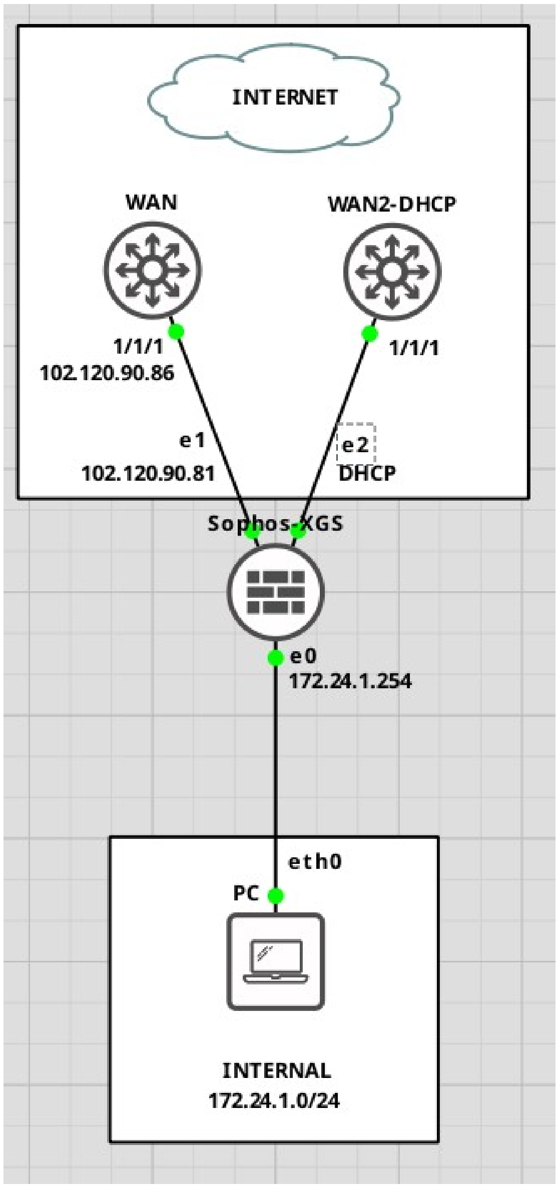
Position – IT Intern

Assignment Title –Sophos XGS2300 and Sophos Firewall Base Configuration & Adding Exception

Supervisor – Sir Noman Rajput, Sr. Assistant Director IT

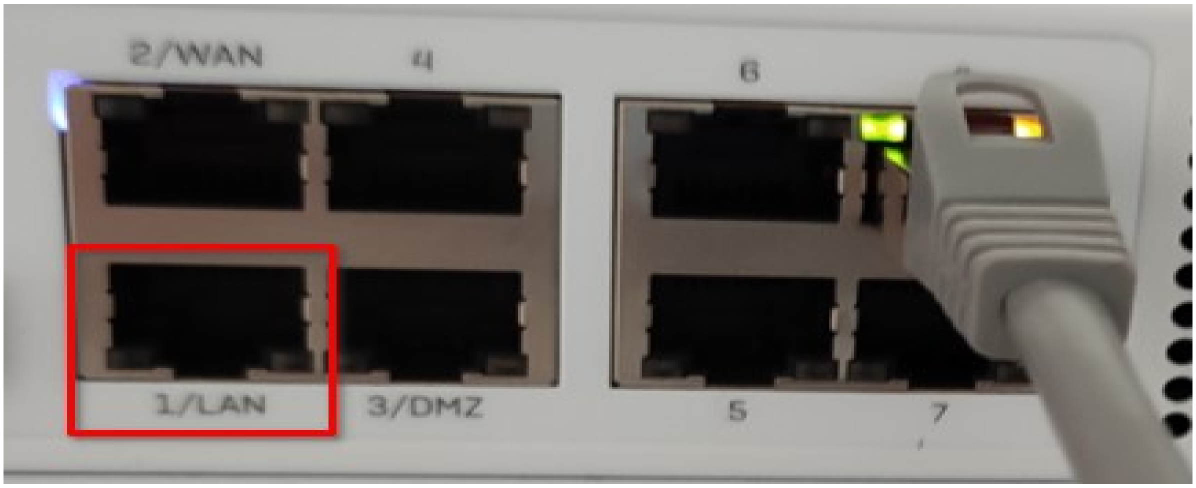
Sophos XGS2300 and Sophos Firewall Base

Configuration & Adding Exception



Initial Setup

Let's begin with the initial setup. Once the hardware is powered up, we can access the WebUI through port 1 (LAN).



The default IP set on the Sophos XG/XGS is always “172.16.16.16/24”, so we have to set an IP on our local device.

I am using GNS3 for this. The client I will use to access Sophos is the “webterm” appliance for GNS3.
First, we will set the IP on the client.

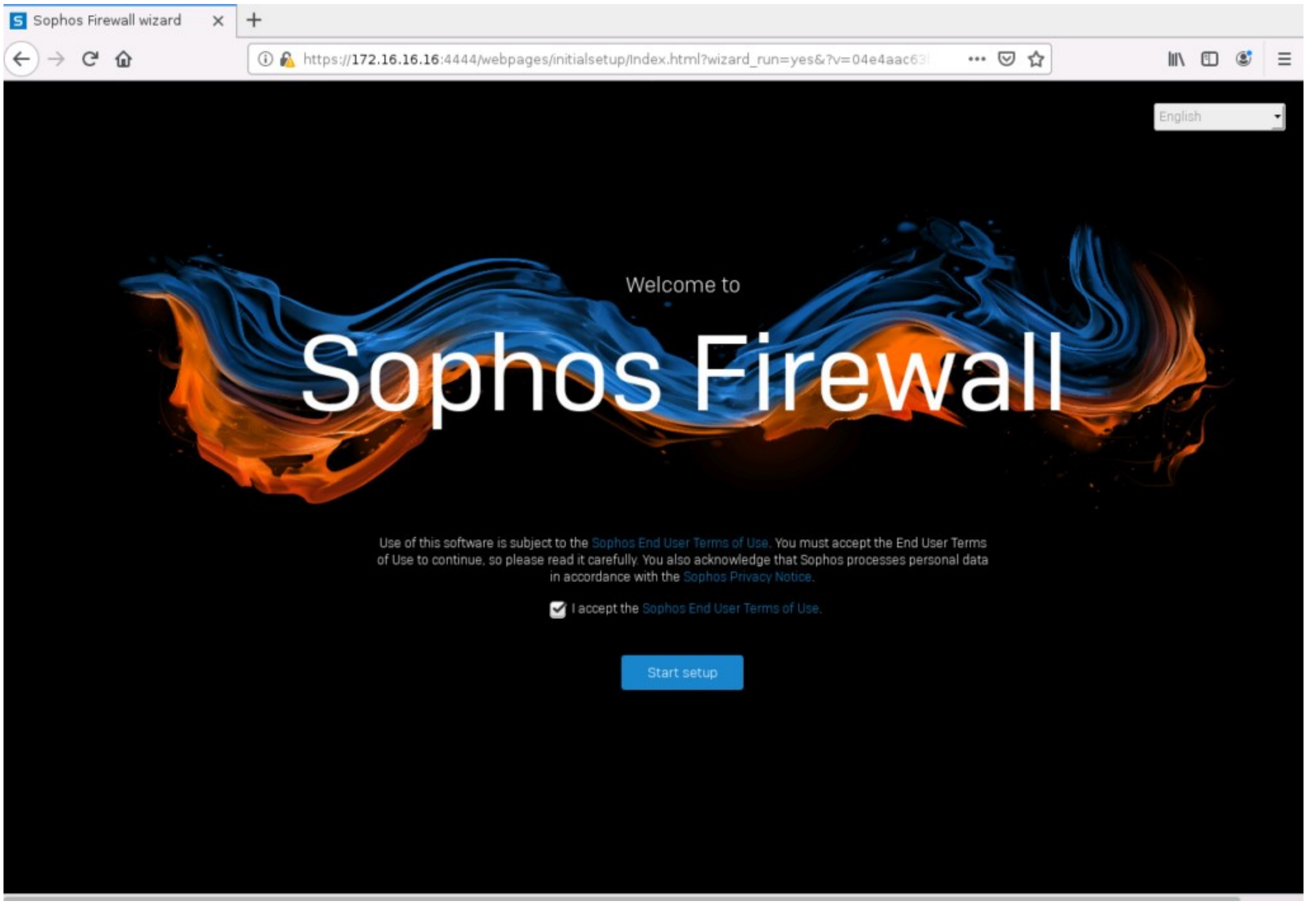
List the interfaces. “lo” is the loopback interface. “eth0” is the one we want.

```
fedora-kde :: ~ » ifconfig
eth0      Link encap:Ethernet  HWaddr 4e:21:aa:73:1b:05
          inet6 addr: fe80::4c21:aaff:fe73:1b05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:726 (726.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31784 (31.0 KiB)  TX bytes:31784 (31.0 KiB)
```

Next, set the IP for eth0.

```
fedora-kde :: ~ » ifconfig eth0 172.16.16.10/24
```

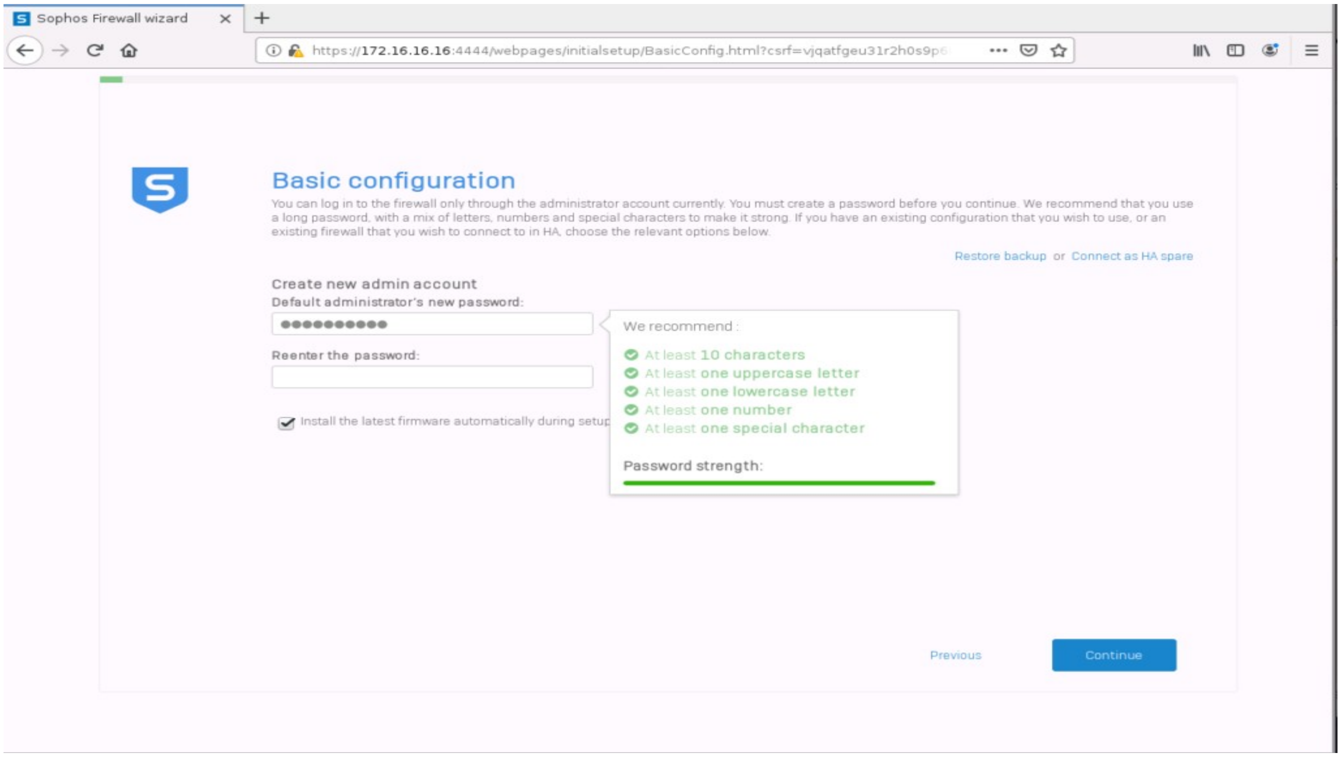
Now we can access the WebUI. Open a browser and enter “https://172.16.16.16:4444”.
Accept the terms and click on “Start setup”.


Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/Index.html?wizard_run=yes&?v=04e4aac63
English
Welcome to
Sophos Firewall
Start setup

Use of this software is subject to the Sophos End User Terms of Use. You must accept the End User Terms of Use to continue, so please read it carefully. You also acknowledge that Sophos processes personal data in accordance with the Sophos Privacy Notice.

☑ I accept the Sophos End User Terms of Use.

The first step is to set a password for the “admin” user. I will deselect the “install the latest firmware automatically during setup” since this is from a VM without internet access. Click on “Continue”.


Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/BasicConfig.html?csrf=vjqatfgeu31r2h0s9p6

Basic configuration

You can log in to the firewall only through the administrator account currently. You must create a password before you continue. We recommend that you use a long password, with a mix of letters, numbers and special characters to make it strong. If you have an existing configuration that you wish to use, or an existing firewall that you wish to connect to in HA, choose the relevant options below.

Restore backup or Connect as HA spare

Create new admin account

Default administrator's new password: ●●●●●●●●●●●

Reenter the password:

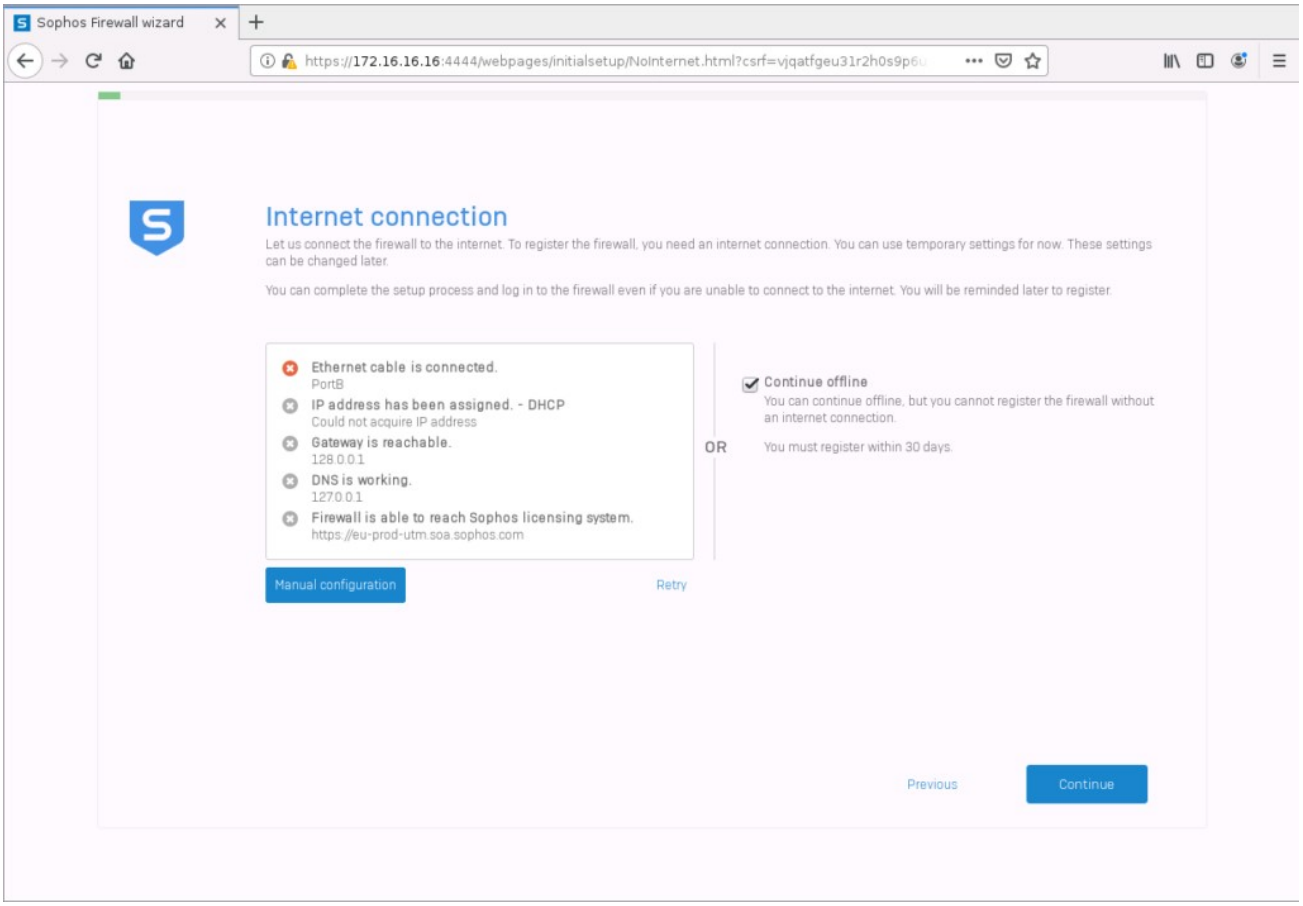
☑ Install the latest firmware automatically during setup

We recommend :

- ✓ At least 10 characters
- ✓ At least one uppercase letter
- ✓ At least one lowercase letter
- ✓ At least one number
- ✓ At least one special character

Password strength:

Here we set up the internet connection. I tend to skip this step by selecting “Continue offline”.


Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/NoInternet.html?csrf=vjqatfgeu31r2h0s9p6u

Internet connection

Let us connect the firewall to the internet. To register the firewall, you need an internet connection. You can use temporary settings for now. These settings can be changed later.

You can complete the setup process and log in to the firewall even if you are unable to connect to the internet. You will be reminded later to register.

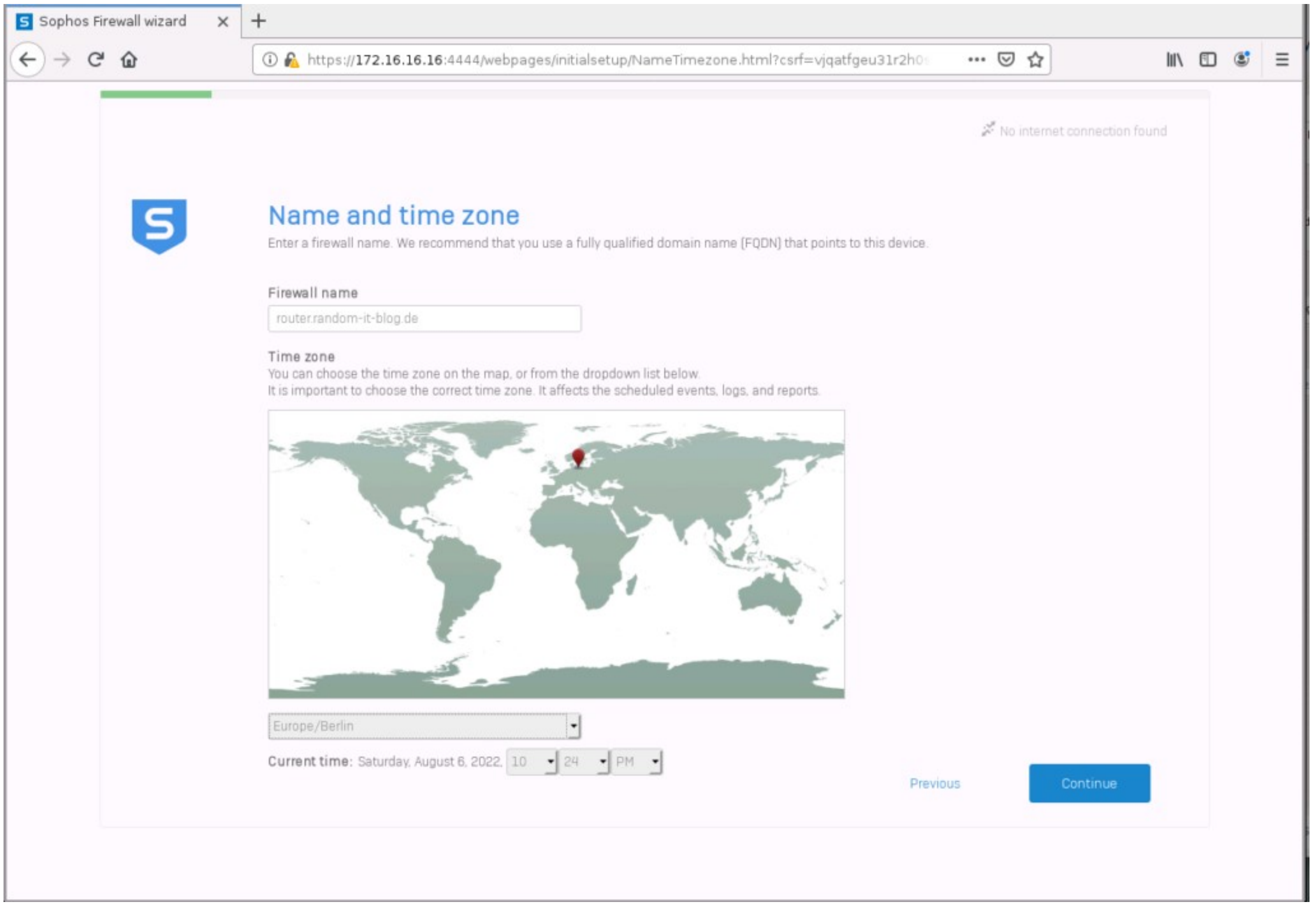
- ☒ Ethernet cable is connected.
  PortB
- ☒ IP address has been assigned. - DHCP
  Could not acquire IP address
- ☒ Gateway is reachable.
  128.0.0.1
- ☒ DNS is working.
  127.0.0.1
- ☒ Firewall is able to reach Sophos licensing system.
  https://eu-prod-utm.soa.sophos.com

OR

☑ Continue offline
You can continue offline, but you cannot register the firewall without an internet connection.

You must register within 30 days.

Type in the hostname and select the timezone for the firewall.


Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/NameTimezone.html?csrf=vjqatfgeu31r2h0
No internet connection found
Previous
Continue

Name and time zone

Enter a firewall name. We recommend that you use a fully qualified domain name (FQDN) that points to this device.

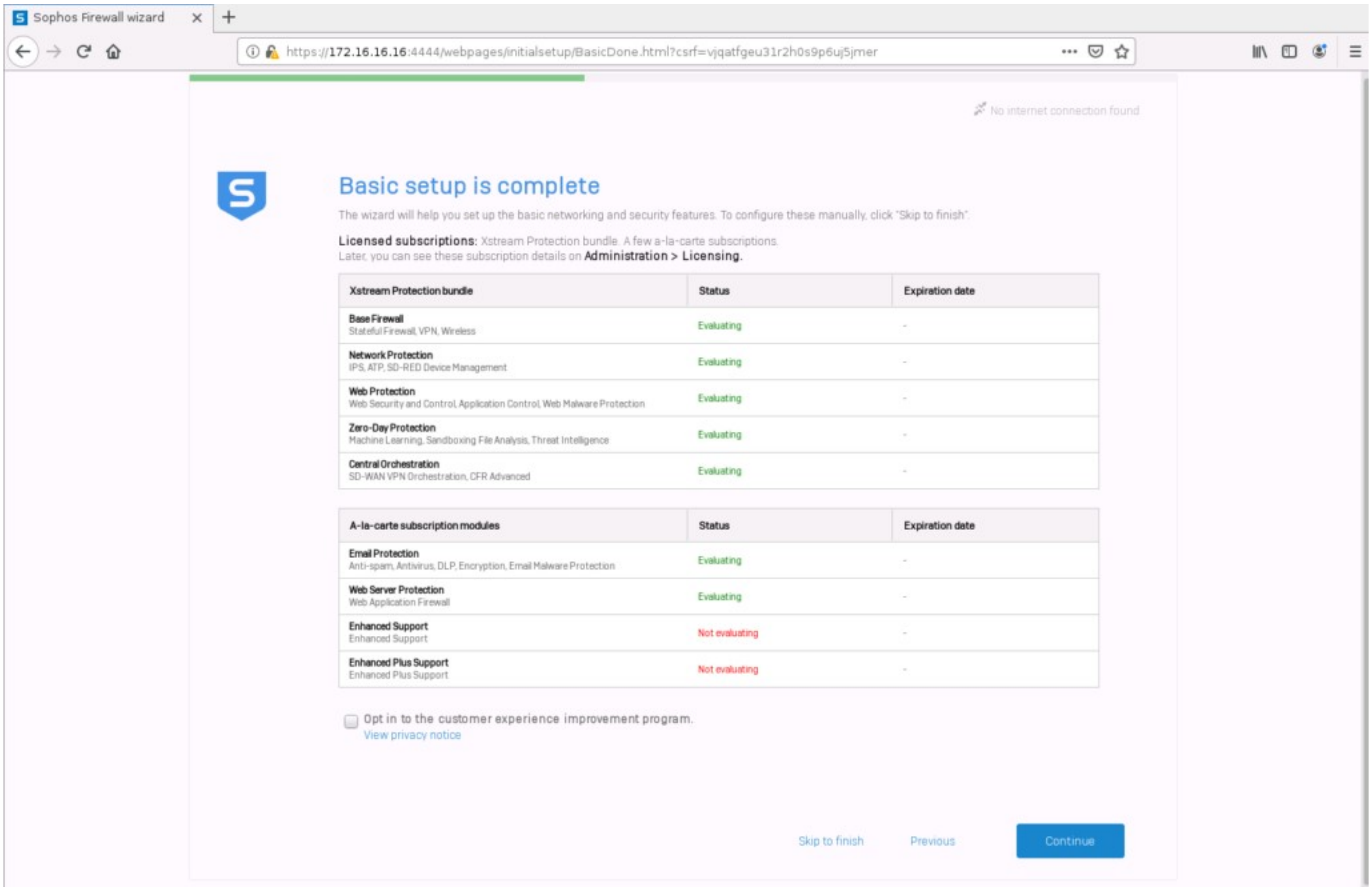
Firewall name: router.random-it-blog.de

Time zone
You can choose the time zone on the map, or from the dropdown list below.
It is important to choose the correct time zone. It affects the scheduled events, logs, and reports.

Europe/Berlin

Current time: Saturday, August 6, 2022, 10 24 PM

Now we are technically done. We can select “Skip to finish” which would restart the firewall and greet us with a login screen.
We could also continue with the configuration. This would allow us to enable a few things like the web filter and firewall rules, but I like to set this up myself.



Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/BasicDone.html?csrf=vjqatfgeu31r2h0s9p6uj5jmer
No internet connection found

Basic setup is complete

The wizard will help you set up the basic networking and security features. To configure these manually, click "Skip to finish".

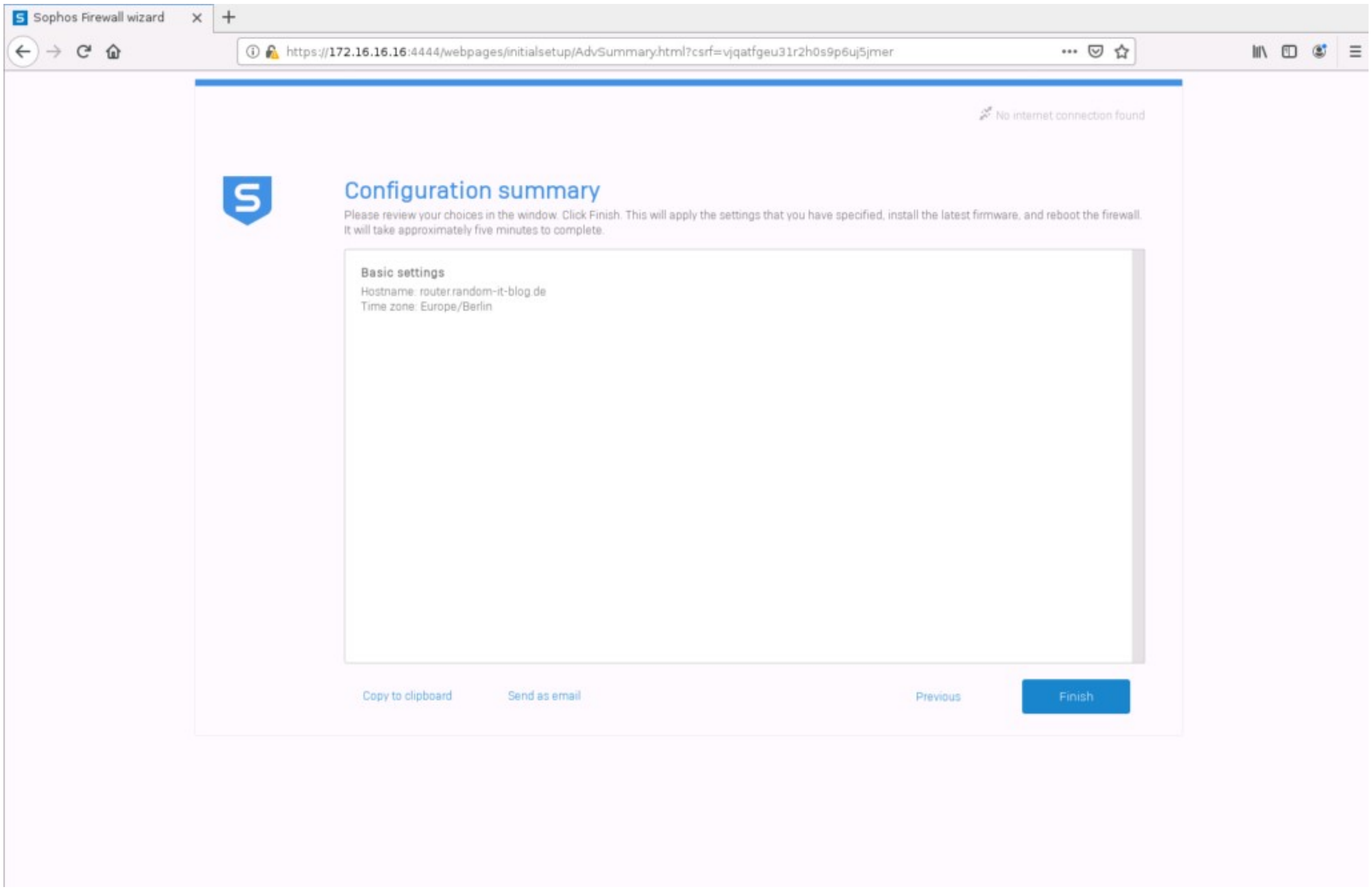
Licensed subscriptions: Xstream Protection bundle. A few a-la-carte subscriptions.
Later, you can see these subscription details on **Administration > Licensing.**

Xstream Protection bundle	Status	Expiration date
Base Firewall Stateful Firewall, VPN, Wireless	Evaluating	-
Network Protection IPS, ATP, SD-RED Device Management	Evaluating	-
Web Protection Web Security and Control, Application Control, Web Malware Protection	Evaluating	-
Zero-Day Protection Machine Learning, Sandboxing File Analysis, Threat Intelligence	Evaluating	-
Central Orchestration SD-WAN VPN Orchestration, CFR Advanced	Evaluating	-

A-la-carte subscription modules	Status	Expiration date
Email Protection Anti-spam, Antivirus, DLP, Encryption, Email Malware Protection	Evaluating	-
Web Server Protection Web Application Firewall	Evaluating	-
Enhanced Support Enhanced Support	Not evaluating	-
Enhanced Plus Support Enhanced Plus Support	Not evaluating	-

☐ Opt in to the customer experience improvement program.
View privacy notice

Click “Finish” to complete the setup and restart.


Sophos Firewall wizard
https://172.16.16.16:4444/webpages/initialsetup/AdvSummary.html?csrf=vjqatfgeu31r2h0s9p6uj5jmer
No internet connection found

Configuration summary

Please review your choices in the window. Click Finish. This will apply the settings that you have specified, install the latest firmware, and reboot the firewall. It will take approximately five minutes to complete.

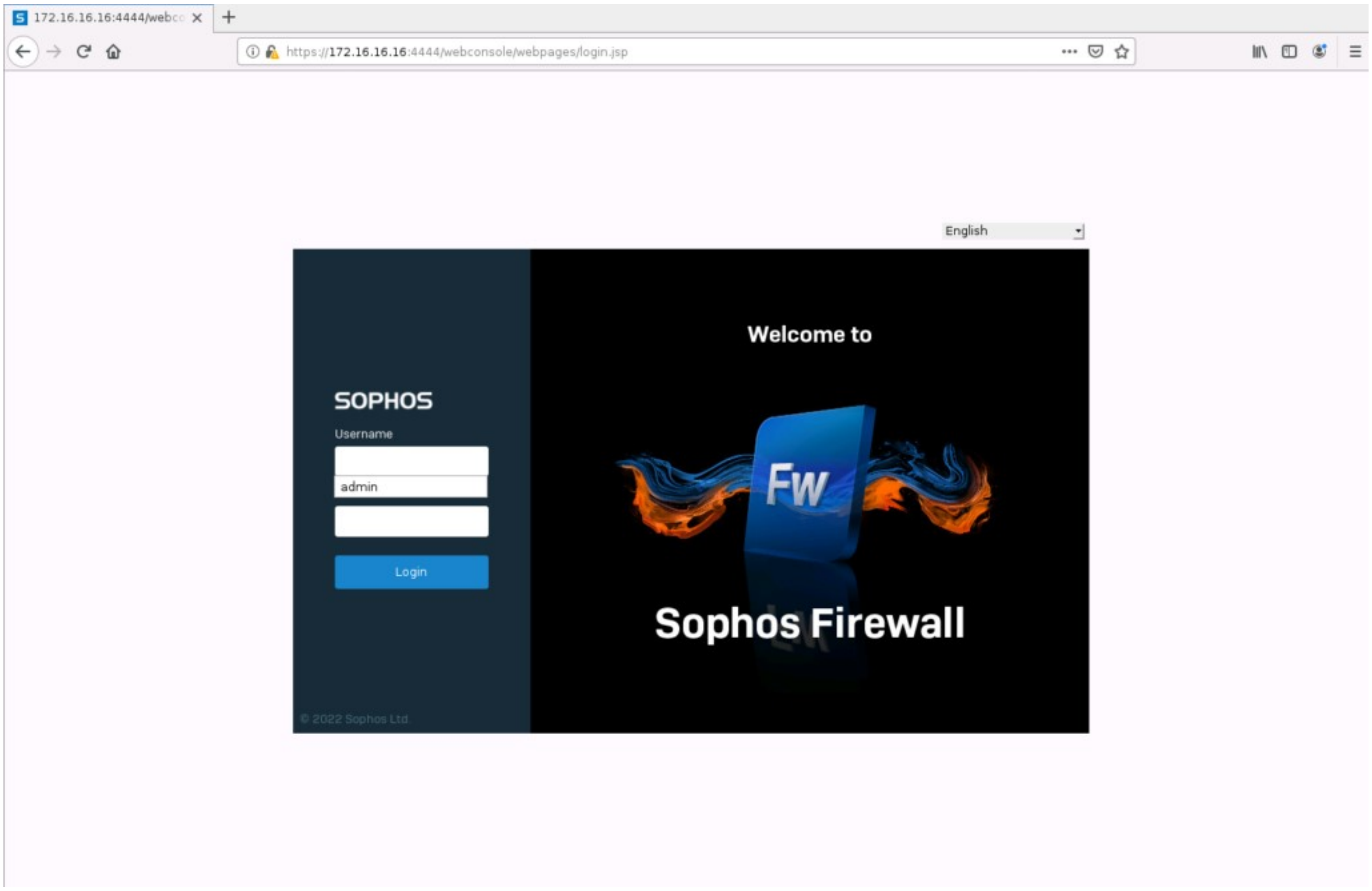
Basic settings
Hostname: router.random-it-blog.de
Time zone: Europe/Berlin

Copy to clipboard
Send as email
Previous
Finish

Basic Setup

Interface configuration

OK, after a couple of minutes the system should be up and running. We can log in with the username "admin" and the password we set earlier. Let us get through a basic setup, enough to be able to (somewhat) safely access the internet.

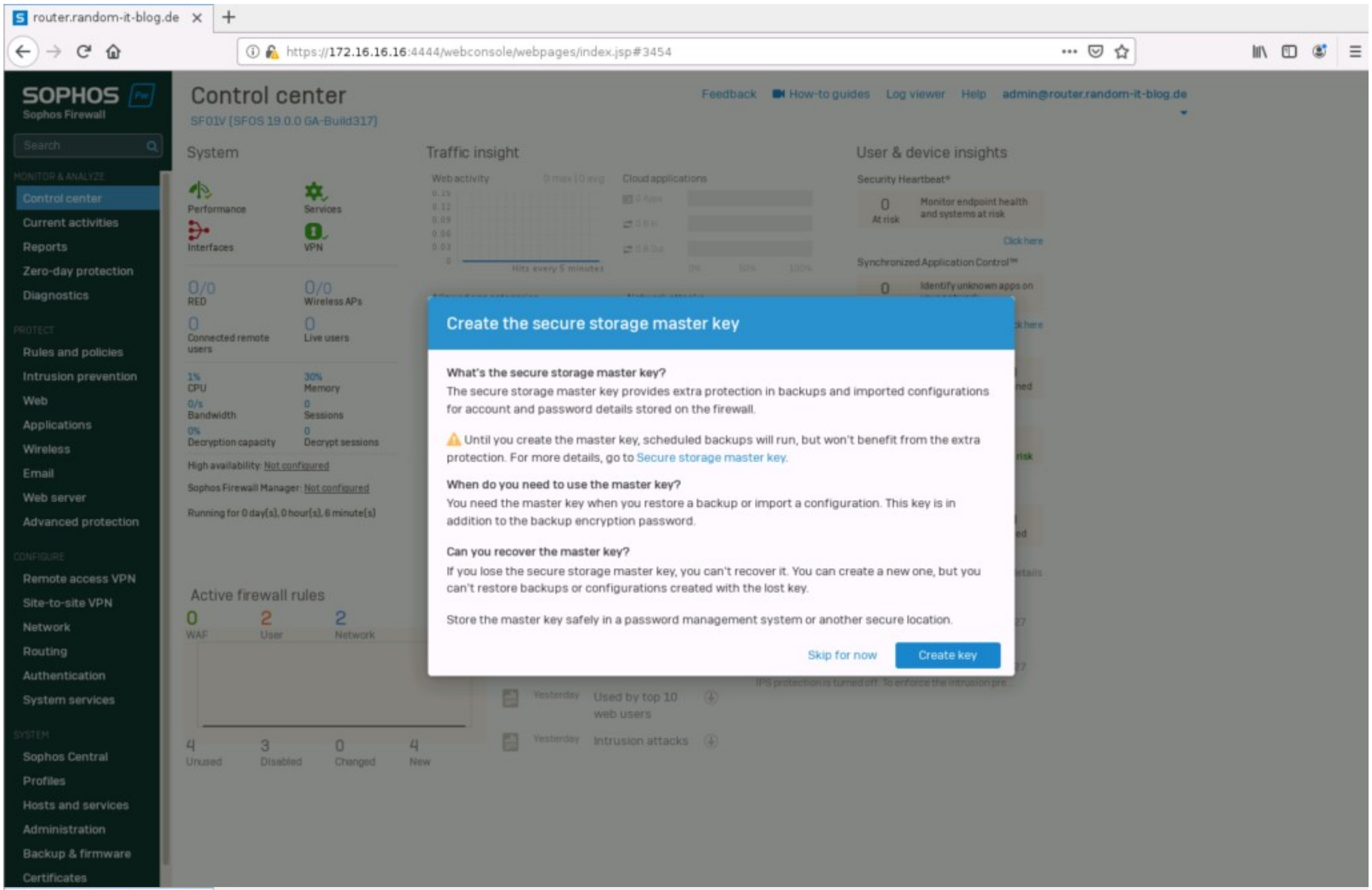


https://172.16.16.16:4444/webconsole/webpages/login.jsp

Username: admin

Once we are in, we are greeted by a pop-up, which asks us to create a “Storage Master Key”. This is an additional password for your Sophos backups. We will create one now.

Do not lose this password, since we cannot recover it. You can always set a new one for new backups, though.



Create the secure storage master key

What's the secure storage master key?

The secure storage master key provides extra protection in backups and imported configurations for account and password details stored on the firewall.

⚠ Until you create the master key, scheduled backups will run, but won't benefit from the extra protection. For more details, go to Secure storage master key.

When do you need to use the master key?

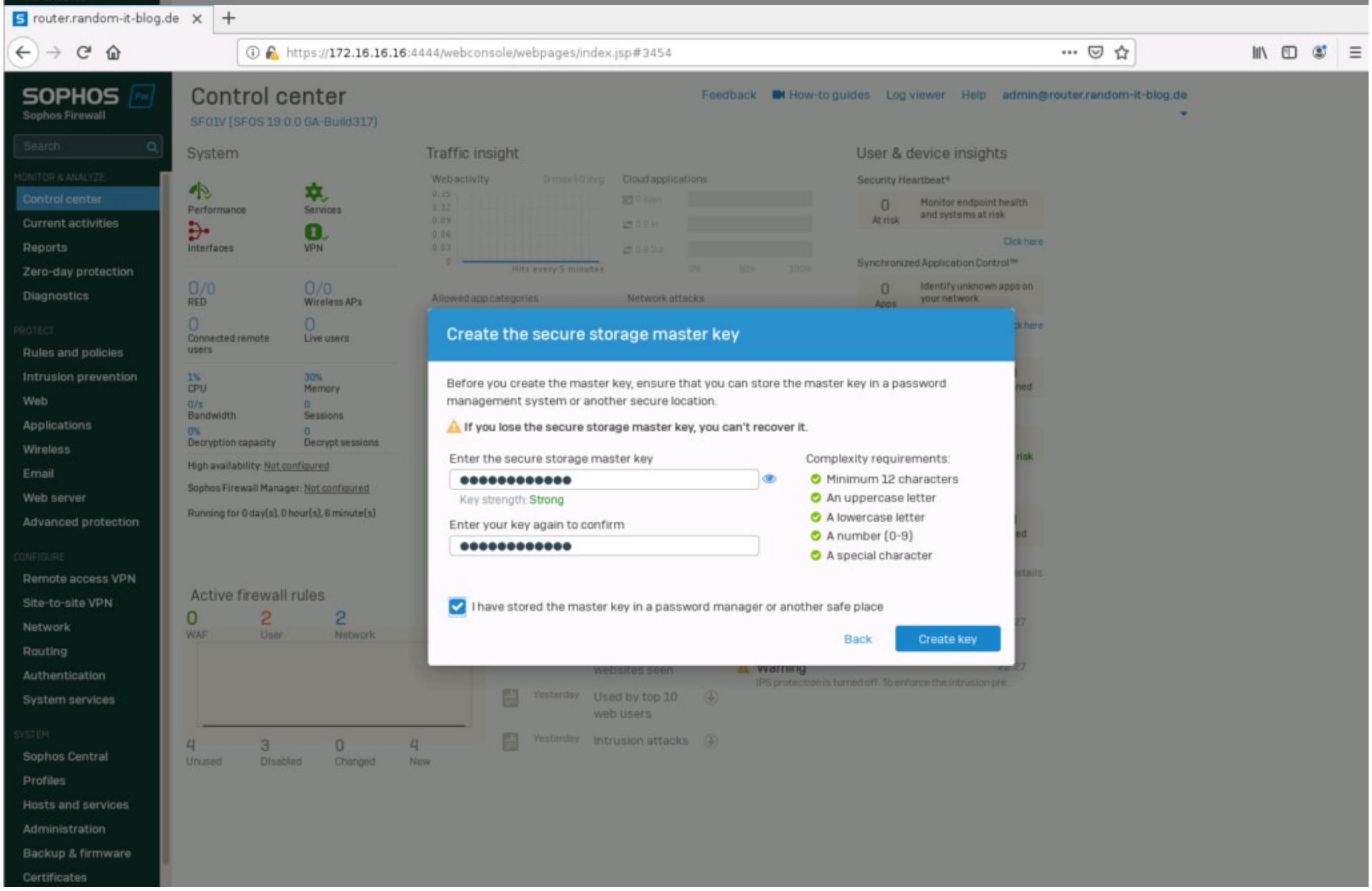
You need the master key when you restore a backup or import a configuration. This key is in addition to the backup encryption password.

Can you recover the master key?

If you lose the secure storage master key, you can't recover it. You can create a new one, but you can't restore backups or configurations created with the lost key.

Store the master key safely in a password management system or another secure location.

Skip for now | Create key



Create the secure storage master key

Before you create the master key, ensure that you can store the master key in a password management system or another secure location.

⚠ **If you lose the secure storage master key, you can't recover it.**

Enter the secure storage master key: ●●●●●●●●●●●●●

Key strength: Strong

Enter your key again to confirm: ●●●●●●●●●●●●●

Complexity requirements:

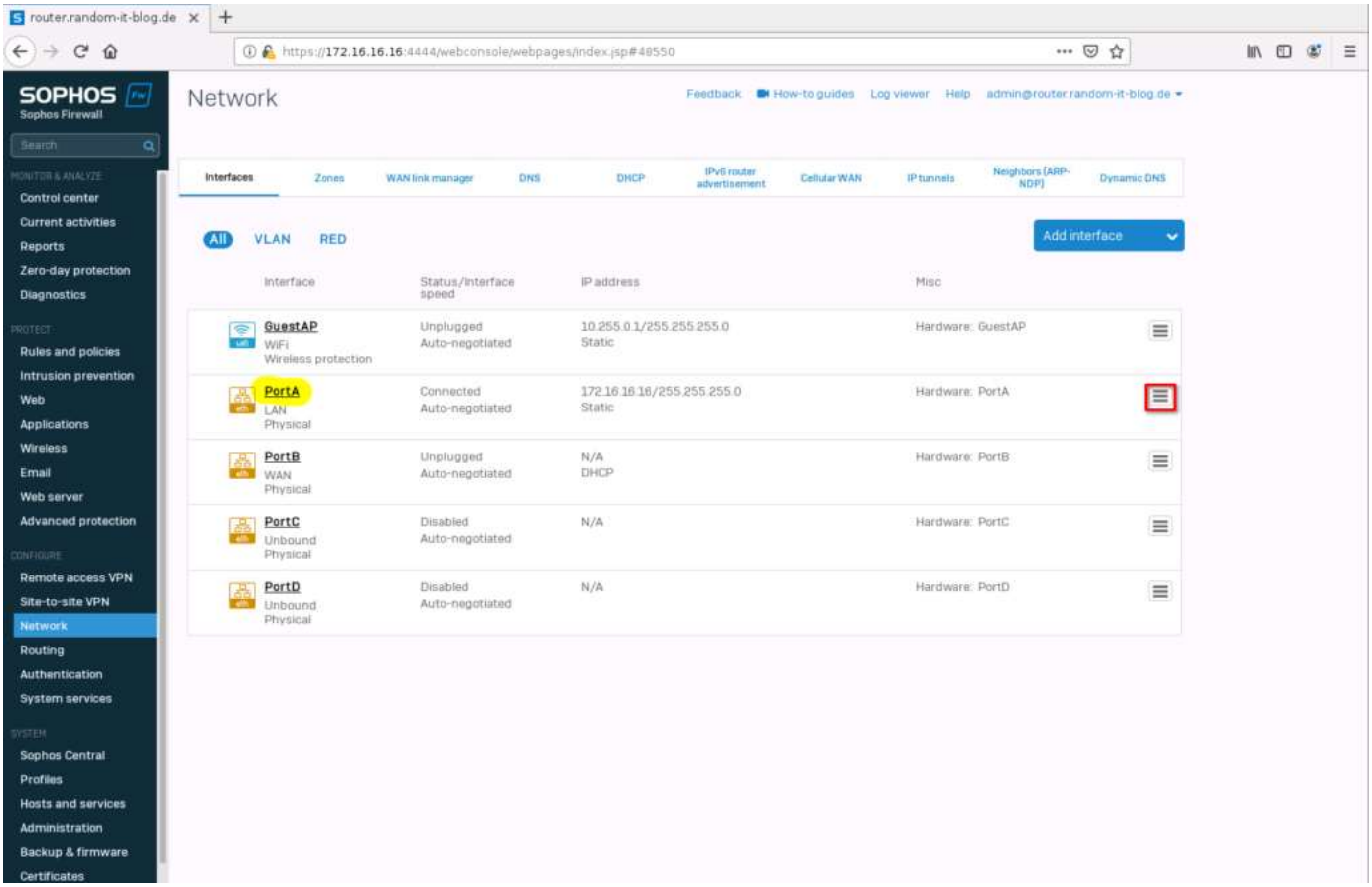
- ✓ Minimum 12 characters
- ✓ An uppercase letter
- ✓ A lowercase letter
- ✓ A number (0-9)
- ✓ A special character

☑ I have stored the master key in a password manager or another safe place

Back | Create key

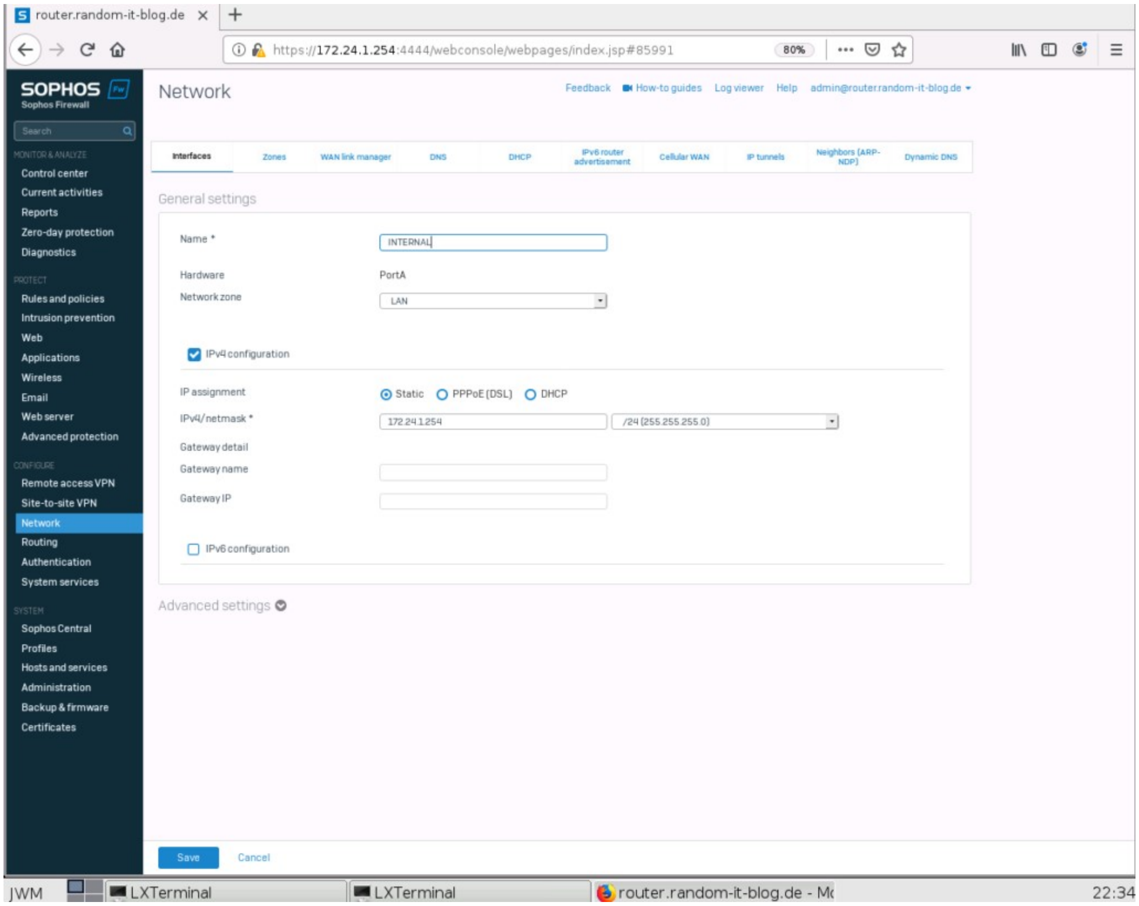
Now we are in. The first step for me is to set the interfaces. So let's begin there.

Select “Network” on the left. Depending on the hardware you are using, the interface page might look slightly different. We will ignore the “GuestAP” interface. I will begin with the internal interface, so select “PortA” or click on the collapsed menu on the right.



Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	Hardware: GuestAP
PortA LAN Physical	Connected Auto-negotiated	172.16.16.16/255.255.255.0 Static	Hardware: PortA
PortB WAN Physical	Unplugged Auto-negotiated	N/A DHCP	Hardware: PortB
PortC Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortC
PortD Unbound Physical	Disabled Auto-negotiated	N/A	Hardware: PortD

Choose a fitting name, I will use “INTERNAL” and set the IP address. “172.24.1.254/24” in my case. Click on Save to confirm.



Network

General settings

Name * INTERNAL

Hardware PortA

Network zone LAN

☑ IPv4 configuration

IP assignment ● Static ○ PPPoE (DSL) ○ DHCP

IPv4/netmask * 172.24.1.254 /24 (255.255.255.0)

Gateway detail

Gateway name

Gateway IP

□ IPv6 configuration

Advanced settings

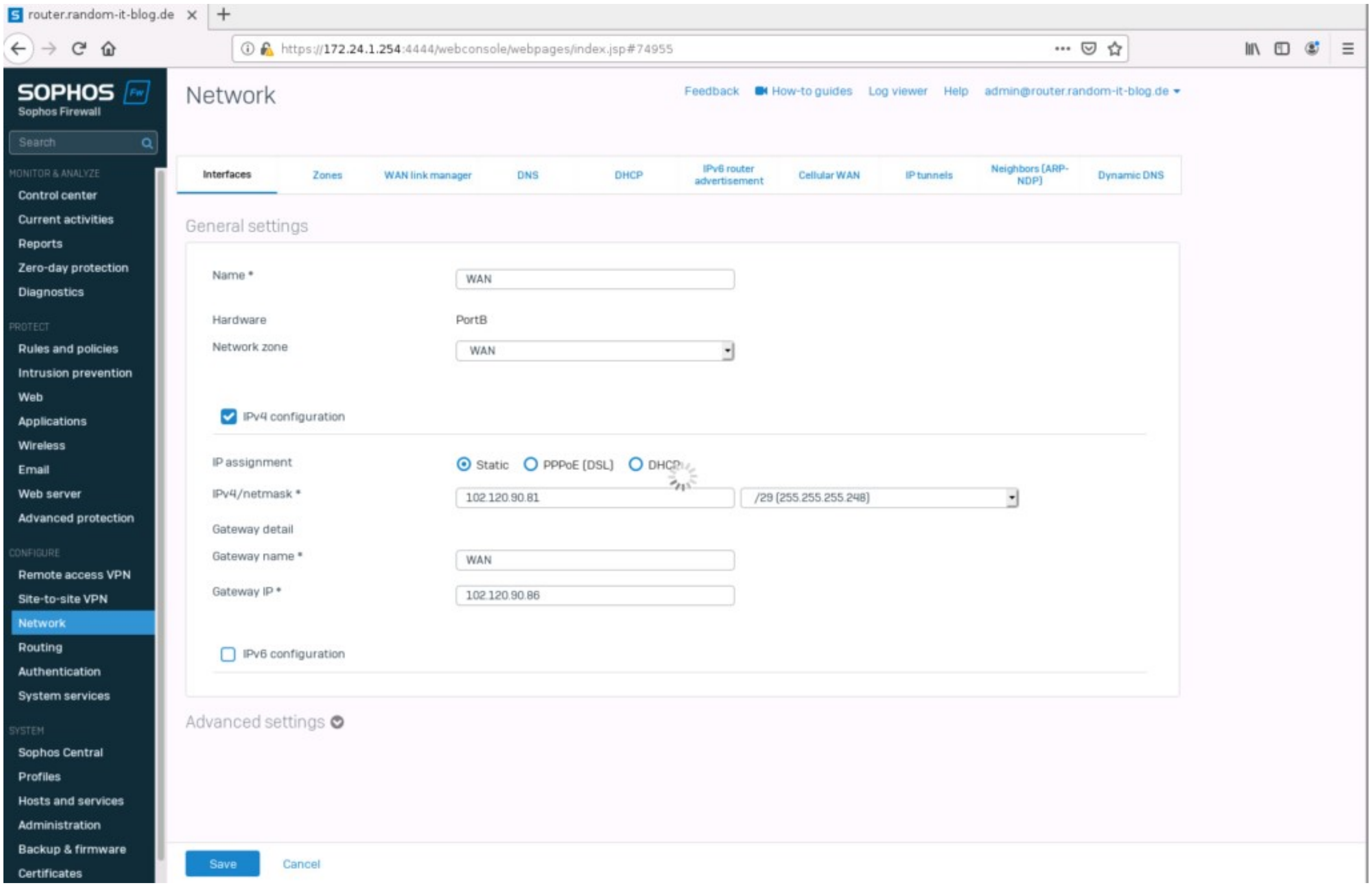
To be able to access the system again, we have to change the IP of our device. And while we are at it, let's set the gateway.

```
fedora-kde :: ~ » ifconfig eth0 172.24.1.1/24

fedora-kde :: ~ » ip route add default via 172.24.1.254

fedora-kde :: ~ » ip route

default via 172.24.1.254 dev eth0

172.24.1.0/24 dev eth0  proto kernel  scope link  src 172.24.1.1
```

OK. Now let's log back in.

Let us set up the "WAN" interface. I will be using the second port for this. So click on "PortB".

Let's just assume that my provider assigned the network 102.120.90.80/29 to me and the gateway is the last IP in that subnet. So 102.120.90.86. I will be using the first possible IP, 102.120.90.81. The interface will be named "WAN".



Network

General settings

Name * WAN

Hardware PortB

Network zone WAN

☑ IPv4 configuration

IP assignment ● Static ○ PPPoE (DSL) ○ DHCP

IPv4/netmask * 102.120.90.81 /29 (255.255.255.248)

Gateway detail

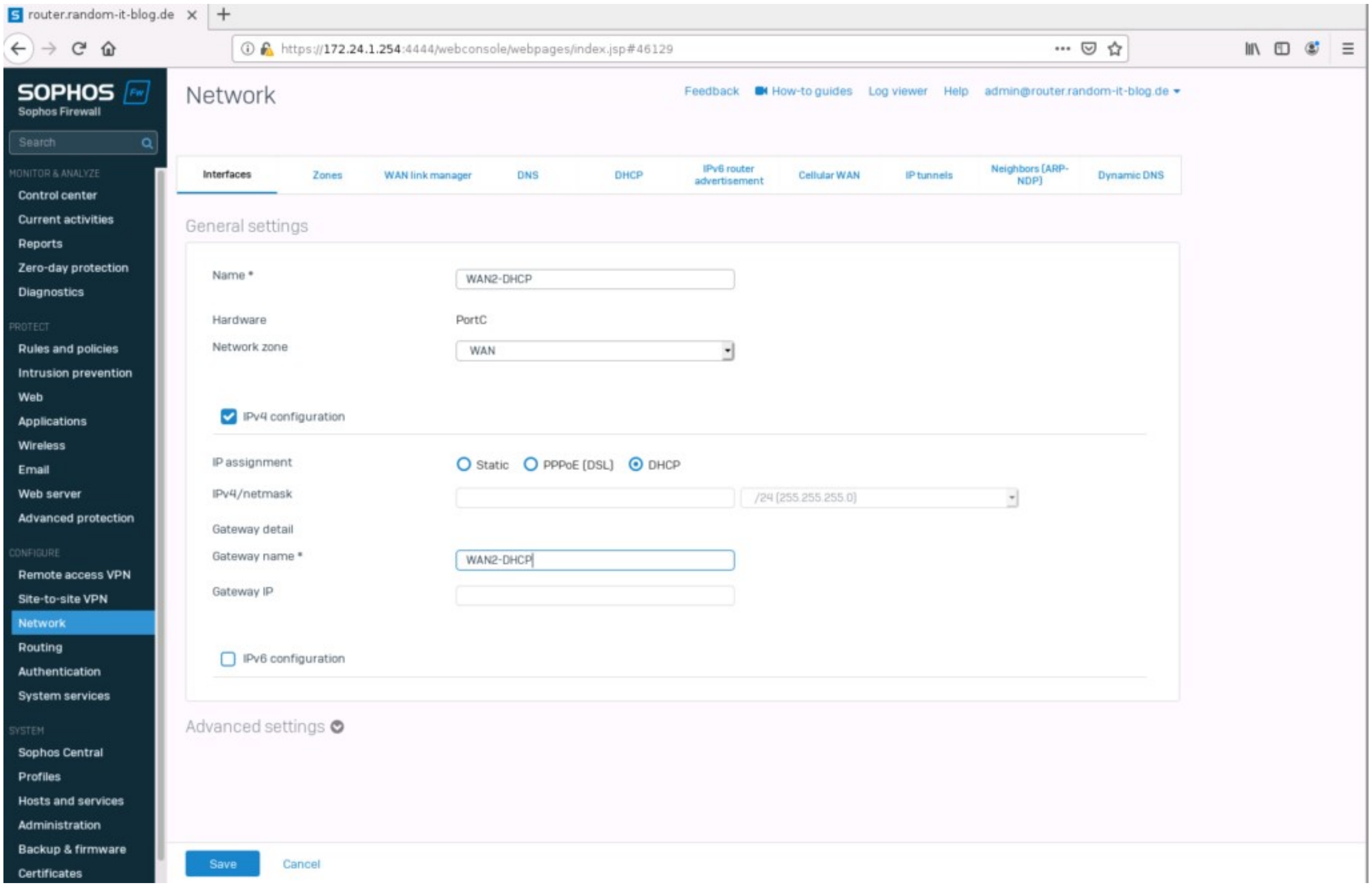
Gateway name * WAN

Gateway IP * 102.120.90.86

☐ IPv6 configuration

This customer has also a second ISP, so we have to configure another interface. Select “PortC”. For this, we will assume the ISP assigned the IPs via DHCP, so no additional configuration is needed.

Select the “Network Zone” WAN and give it a pretty name. I will choose “WAN2-DHCP”.



Name * WAN2-DHCP

Hardware PortC

Network zone WAN

☑ IPv4 configuration

IP assignment ○ Static ○ PPPoE (DSL) ● DHCP

IPv4/netmask /24 (255.255.255.0)

Gateway detail

Gateway name * WAN2-DHCP

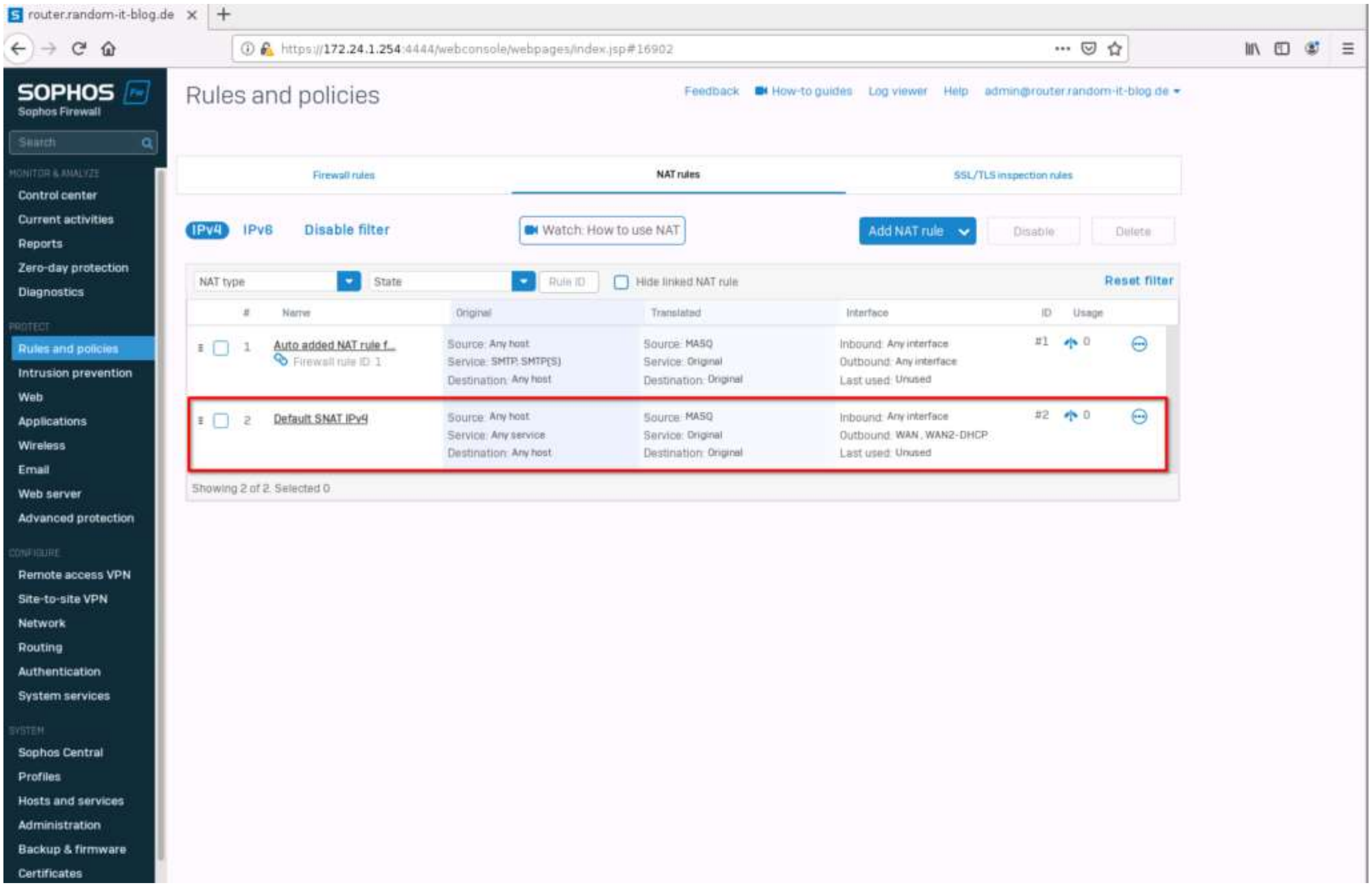
Gateway IP

□ IPv6 configuration

Checking NAT/Masq

Great. Next, we should check if there is a SNAT/Masq rule set. Normally it should be created automatically, but just to make sure. Click on “Rules and policies” and select “NAT rules” in the top bar.

We can see that the second rule is a “SNAT/MASQ” rule and includes both wan interfaces for the “outbound”.
If you don’t have that entry, create a new NAT rule and set the settings identically to the ones listed below.



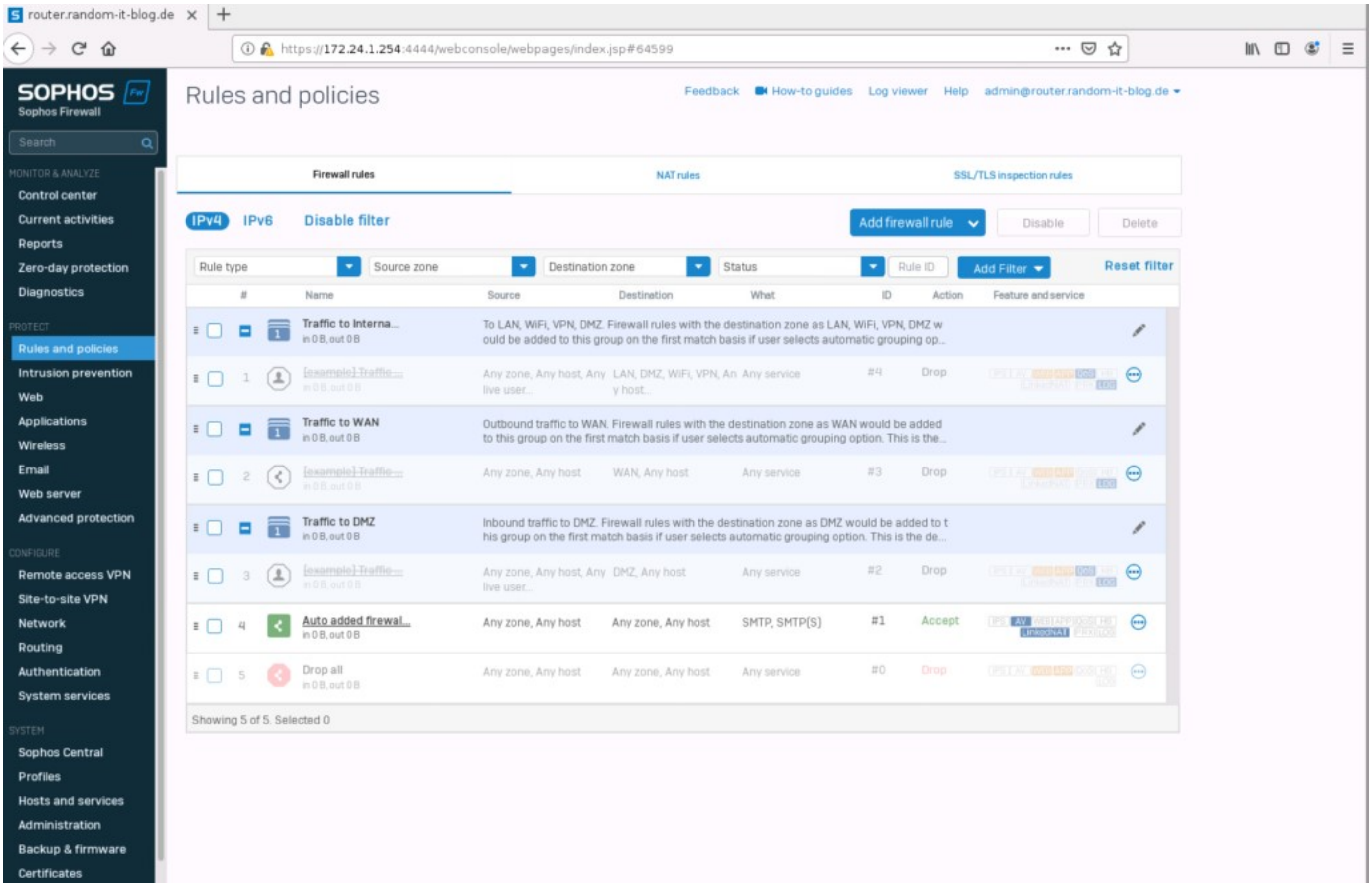
Rules and policies

#	Name	Original	Translated	Interface	ID	Usage
1	Auto added NAT rule f... Firewall rule ID: 1	Source: Any host Service: SMTP, SMTP(S) Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#1	0
2	Default SNAT IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: WAN , WAN2-DHCP Last used: Unused	#2	0

Showing 2 of 2. Selected 0

Firewall Configuration

Let's check the firewall rules. There are no active rules (except SMTP) since we skipped the end of the "initial setup".

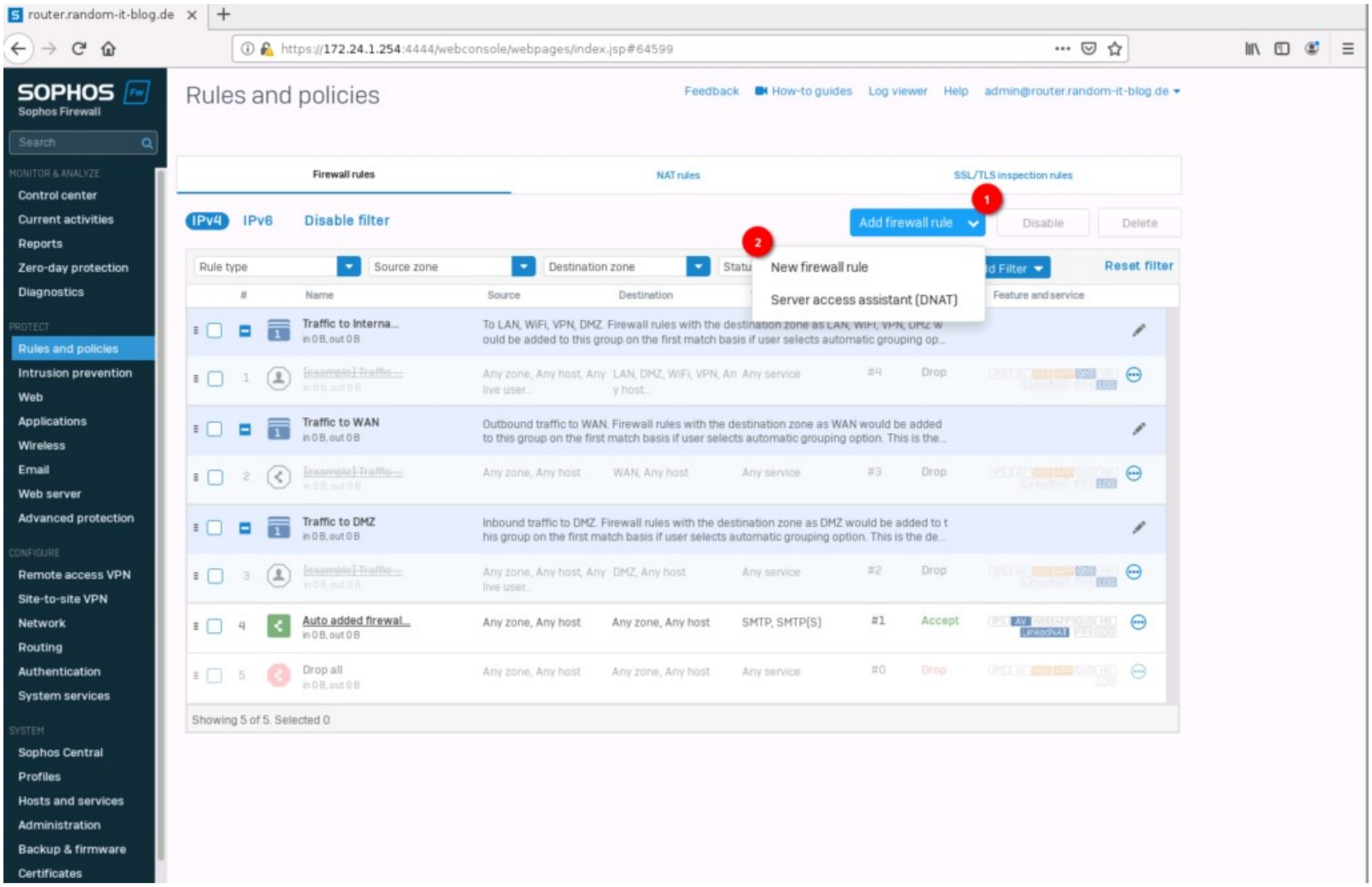


Rules and policies

#	Name	Source	Destination	What	ID	Action	Feature and service
	Traffic to Interna... in 0 B, out 0 B	To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping op...					
1	~~[example] Traffic ...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	LAN, DMZ, WiFi, VPN, Any host...	Any service	#4	Drop	IPS AV WEB APP QOS HB LinkedNAT FRX LOG
	Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the...					
2	~~[example] Traffic ...~~ in 0 B, out 0 B	Any zone, Any host	WAN, Any host	Any service	#3	Drop	IPS AV WEB APP QOS HB LinkedNAT FRX LOG
	Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...					
3	~~[example] Traffic ...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	DMZ, Any host	Any service	#2	Drop	IPS AV WEB APP QOS HB LinkedNAT FRX LOG
4	Auto added firewal... in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	IPS AV WEB APP QOS HB LinkedNAT FRX LOG
5	Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	IPS AV WEB APP QOS HB LOG

Showing 5 of 5. Selected 0

Let’s create one. Select “Add firewall rule” and click on “New firewall rule”.



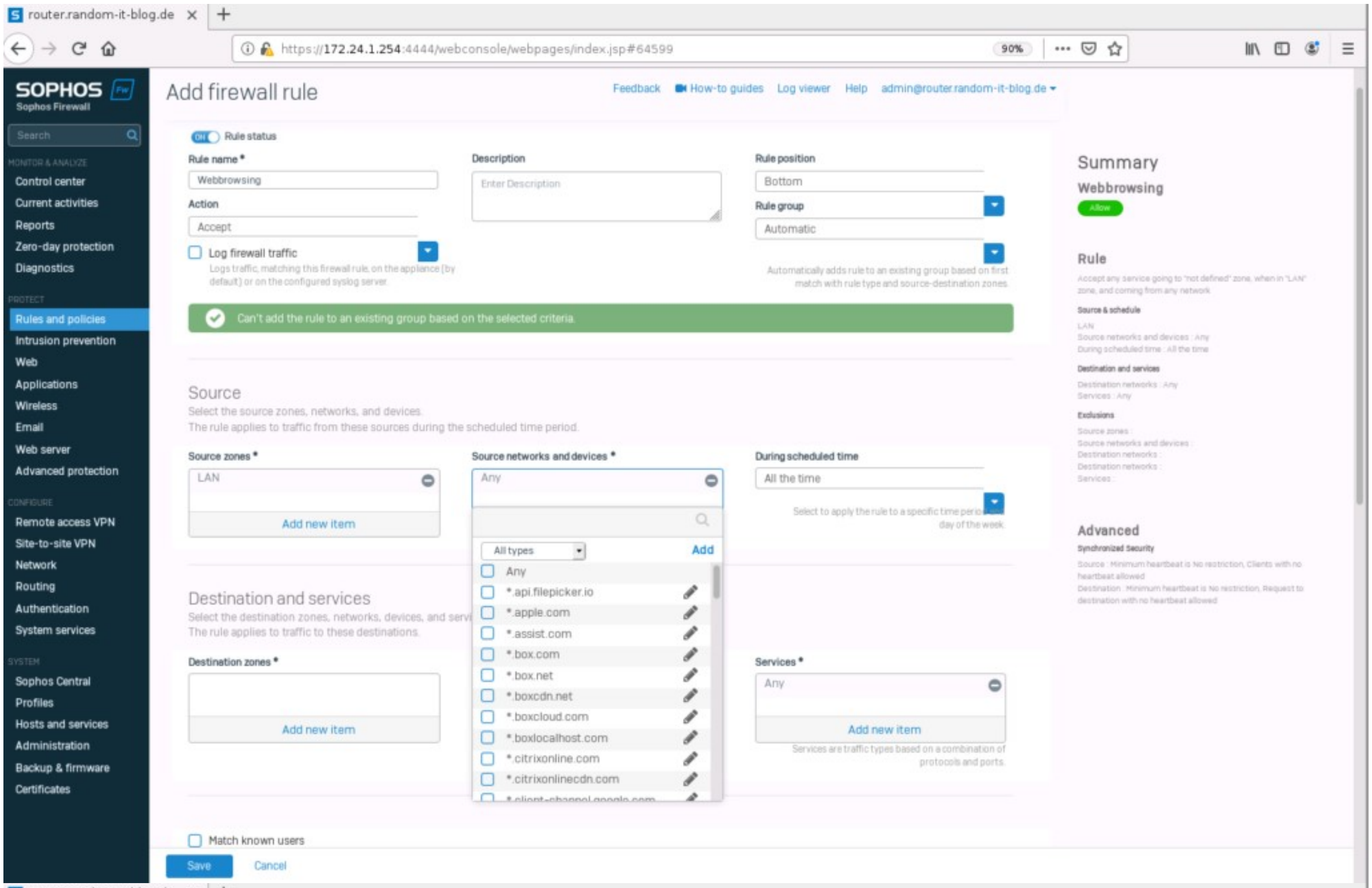
Rules and policies

#	Name	Source	Destination				Feature and service
	Traffic to Interna... in 0 B, out 0 B	To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping op...					
1	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	LAN, DMZ, WiFi, VPN, Any host...	Any service	#4	Drop	
	Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the...					
2	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host	WAN, Any host	Any service	#3	Drop	
	Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...					
3	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	DMZ, Any host	Any service	#2	Drop	
4	Auto added firewal... in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	
5	Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	

Showing 5 of 5. Selected 0

Give the new rule a name. I will create one for “webbrowsing”. For the “source zone” select “LAN”. In “Source networks and devices” remove “Any” and create a new “network” item.

Type in the internal network you use, in my case 172.24.1.0/24, and click on “Save”.



Add firewall rule

ON Rule status

Rule name * Webbrowsing

Action Accept

Description Enter Description

Rule position Bottom

Rule group Automatic

Automatically adds rule to an existing group based on first match with rule type and source-destination zones.

□ Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Can't add the rule to an existing group based on the selected criteria.

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones * LAN

Add new item

Source networks and devices * Any

All types Add

□ Any
□ *.api.filepicker.io
□ *.apple.com
□ *.assist.com
□ *.box.com
□ *.box.net
□ *.boxcdn.net
□ *.boxcloud.com
□ *.boxlocalhost.com
□ *.citrixonline.com
□ *.citrixonlinecdn.com
□ *.client-channel.google.com

During scheduled time All the time

Select to apply the rule to a specific time period or day of the week

Destination and services

Select the destination zones, networks, devices, and servi
The rule applies to traffic to these destinations.

Destination zones *

Add new item

Services * Any

Add new item

Services are traffic types based on a combination of protocols and ports.

□ Match known users

Save Cancel

Summary

Webbrowsing

Allow

Rule

Accept any service going to "not defined" zone, when in "LAN" zone, and coming from any network

Source & schedule

LAN
Source networks and devices : Any
During scheduled time : All the time

Destination and services

Destination networks : Any
Services : Any

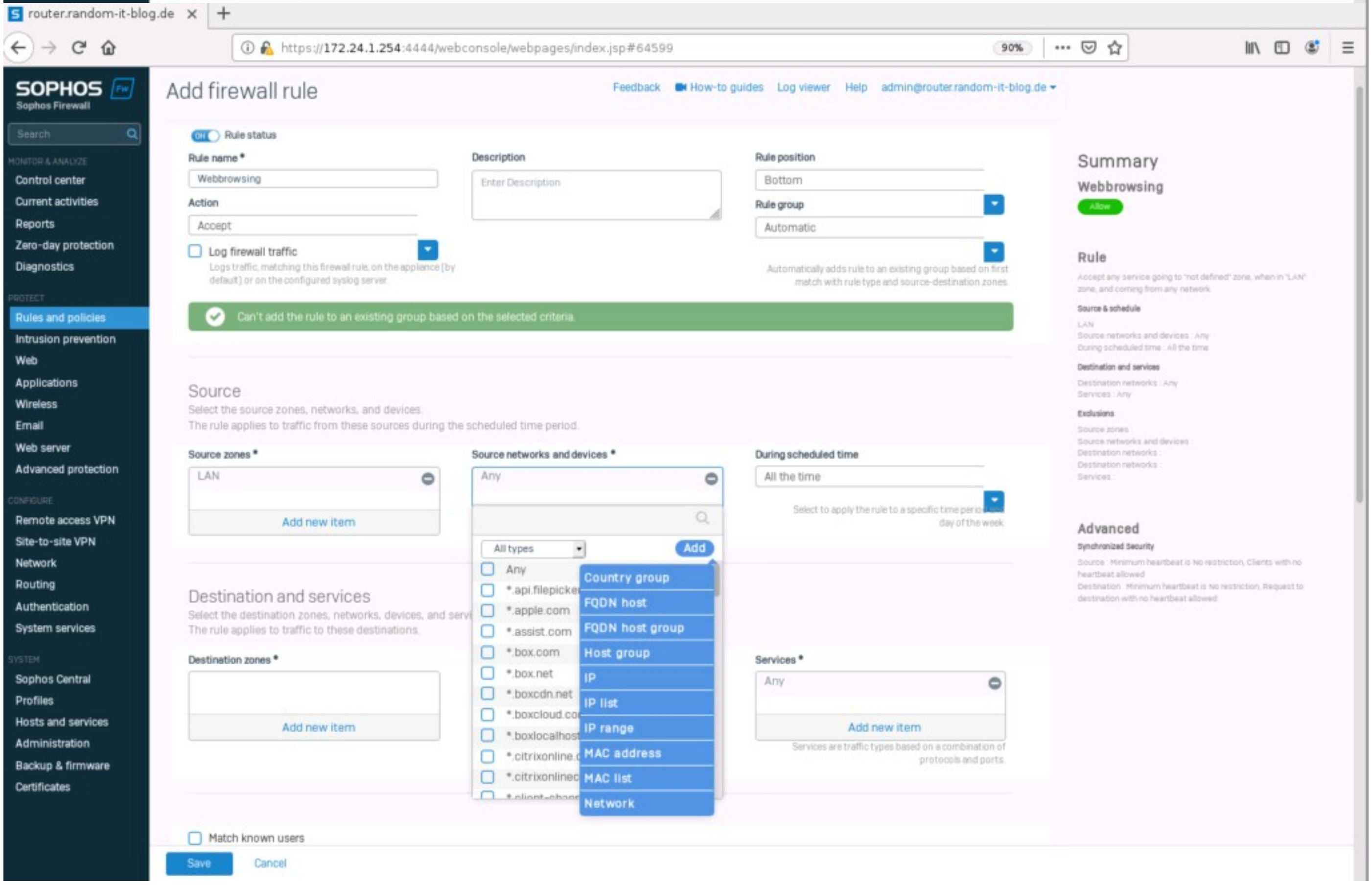
Exclusions

Source zones :
Source networks and devices :
Destination networks :
Destination networks :
Services :

Advanced

Synchronized Security

Source : Minimum heartbeat is No restriction, Clients with no heartbeat allowed
Destination : Minimum heartbeat is No restriction, Request to destination with no heartbeat allowed


Add firewall rule

ON Rule status

Rule name * Webbrowsing

Action Accept

Description Enter Description

Rule position Bottom

Rule group Automatic

Can't add the rule to an existing group based on the selected criteria.

Source

Source zones * LAN

Source networks and devices * Any

During scheduled time All the time

Destination and services

Destination zones *

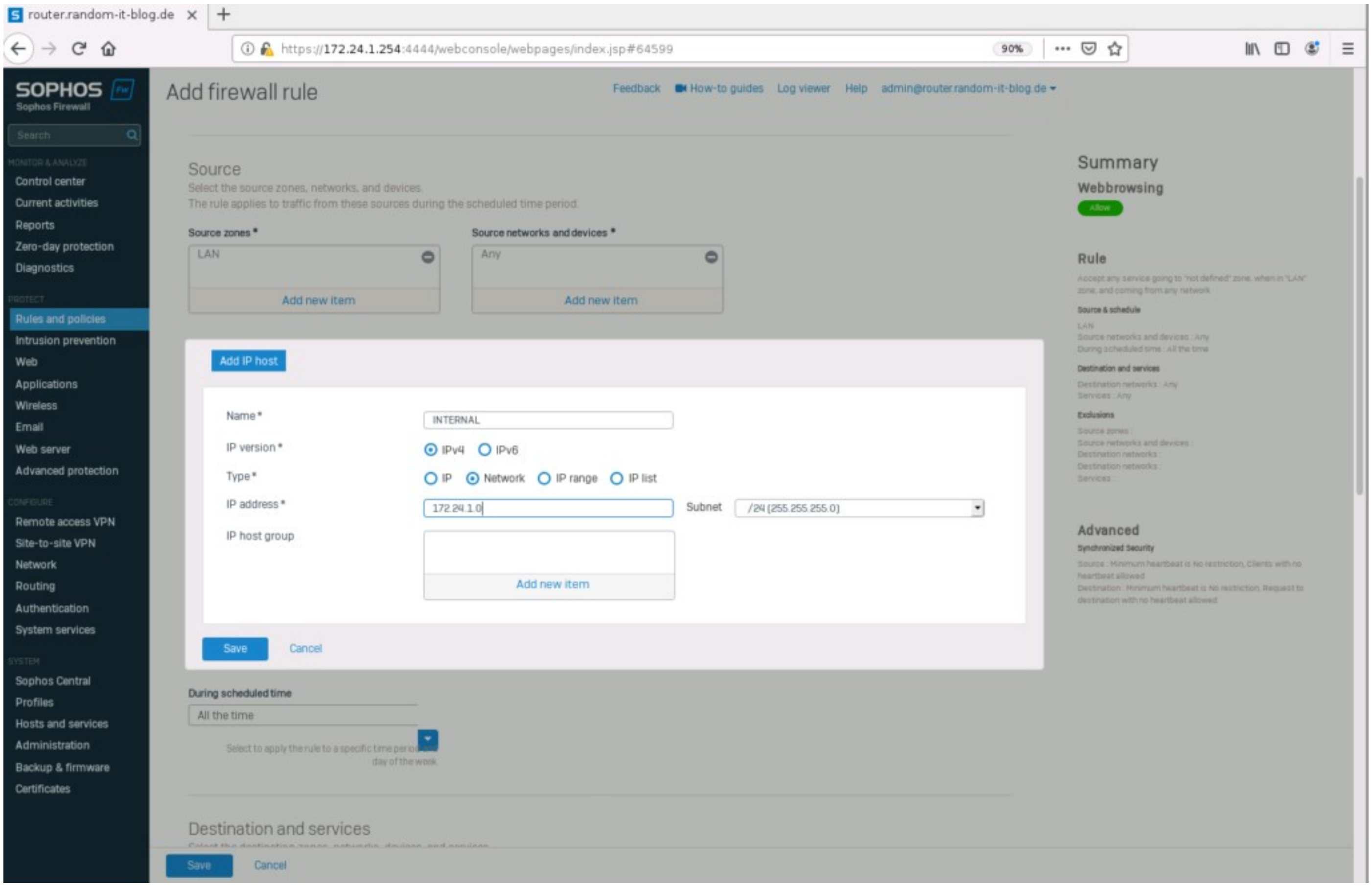
Services * Any

□ Match known users

Save Cancel

All types Add

Country group
FQDN host
FQDN host group
Host group
IP
IP list
IP range
MAC address
MAC list
Network



Source zones *: LAN

Source networks and devices *: Any

Add IP host

Name *: INTERNAL

IP version *: ● IPv4 ○ IPv6

Type *: ○ IP ● Network ○ IP range ○ IP list

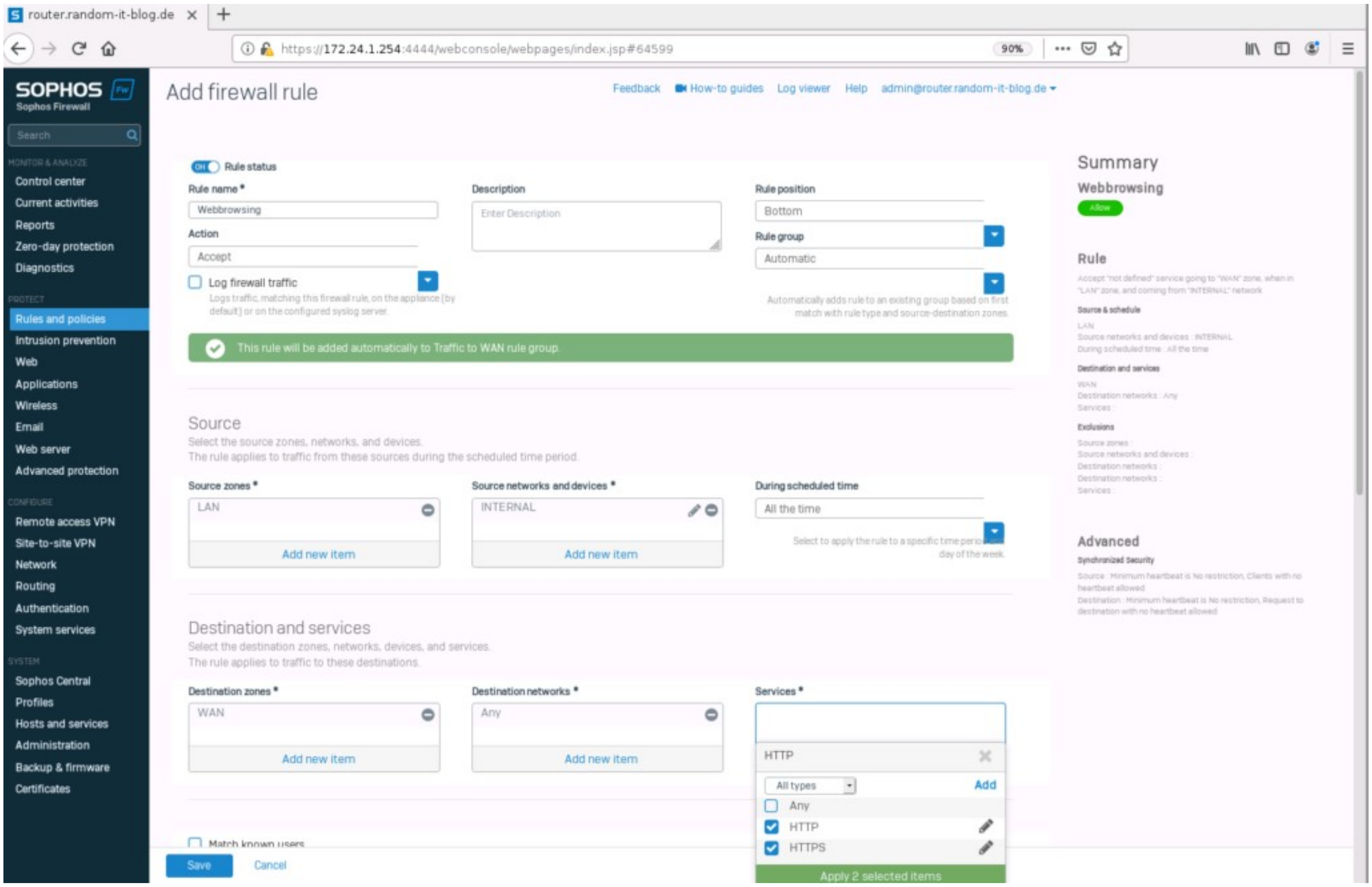
IP address *: 172.24.1.0 Subnet: /24 (255.255.255.0)

IP host group: Add new item

Save Cancel

During scheduled time: All the time

Choose “WAN” for the “destination zone”. Leave “Any” in the “destination networks”. Remove “Any” from the “Services” and click on “Add new item”. Here you can search for the protocol. Type in HTTP and select both “HTTP” and “HTTPs”.



Add firewall rule

ON Rule status

Rule name *: Webbrowsing

Action: Accept

□ Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description: Enter Description

Rule position: Bottom

Rule group: Automatic

Automatically adds rule to an existing group based on first match with rule type and source-destination zones.

This rule will be added automatically to Traffic to WAN rule group.

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *: LAN

Source networks and devices *: INTERNAL

During scheduled time: All the time

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *: WAN

Destination networks *: Any

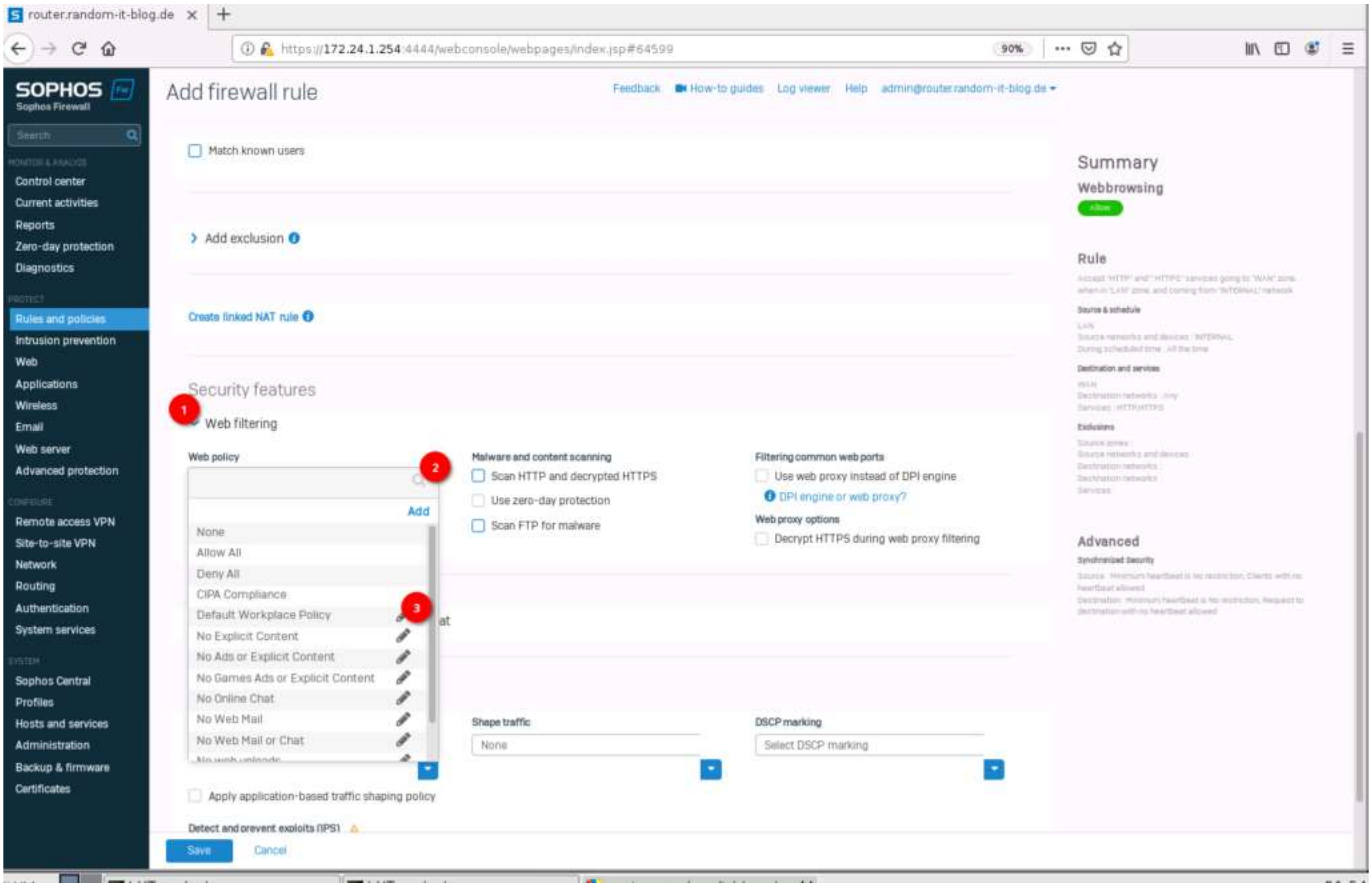
Services *: HTTP

□ Any
☑ HTTP
☑ HTTPS

Apply 2 selected items

□ Match known users

Scroll down until you see the “Security features”. Select “Web filtering” and click on “Default Workplace Policy”. We will set this up later.



Add firewall rule

□ Match known users

Add exclusion

Create linked NAT rule

Security features

Web filtering

Web policy

- None
- Allow All
- Deny All
- CIPA Compliance
- Default Workplace Policy
- No Explicit Content
- No Ads or Explicit Content
- No Games Ads or Explicit Content
- No Online Chat
- No Web Mail
- No Web Mail or Chat
- No web uploads

Malware and content scanning

□ Scan HTTP and decrypted HTTPS

□ Use zero-day protection

□ Scan FTP for malware

Filtering common web ports

□ Use web proxy instead of DPI engine

DPI engine or web proxy?

Web proxy options

□ Decrypt HTTPS during web proxy filtering

Shape traffic: None

DSCP marking: Select DSCP marking

□ Apply application-based traffic shaping policy

Detect and prevent exploits (IPS)

Summary

Webbrowsing

Allow

Rule

Source & schedule

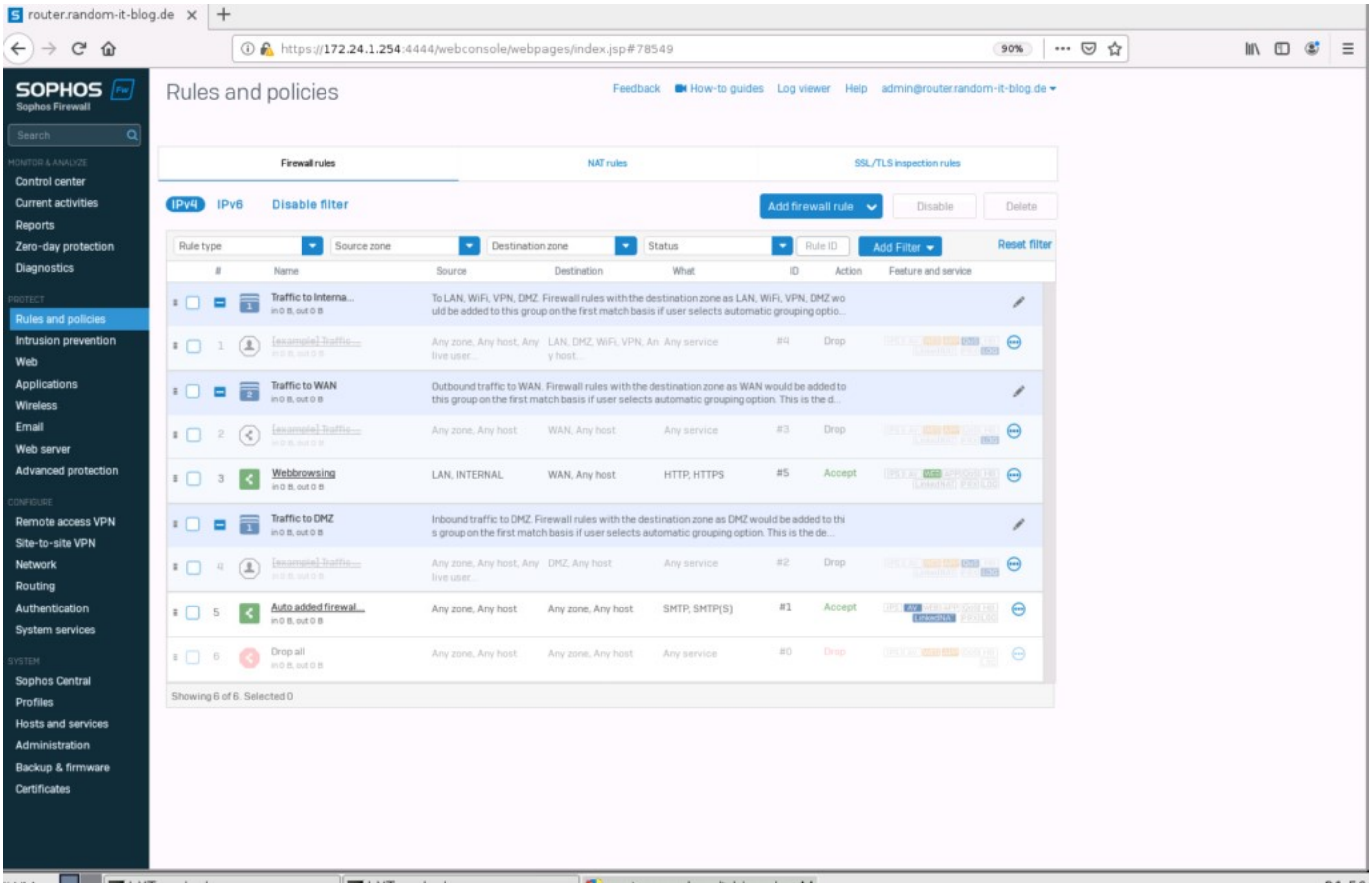
Destination and services

Exclusions

Advanced

Synchronized Security

That’s it. Click on Save.



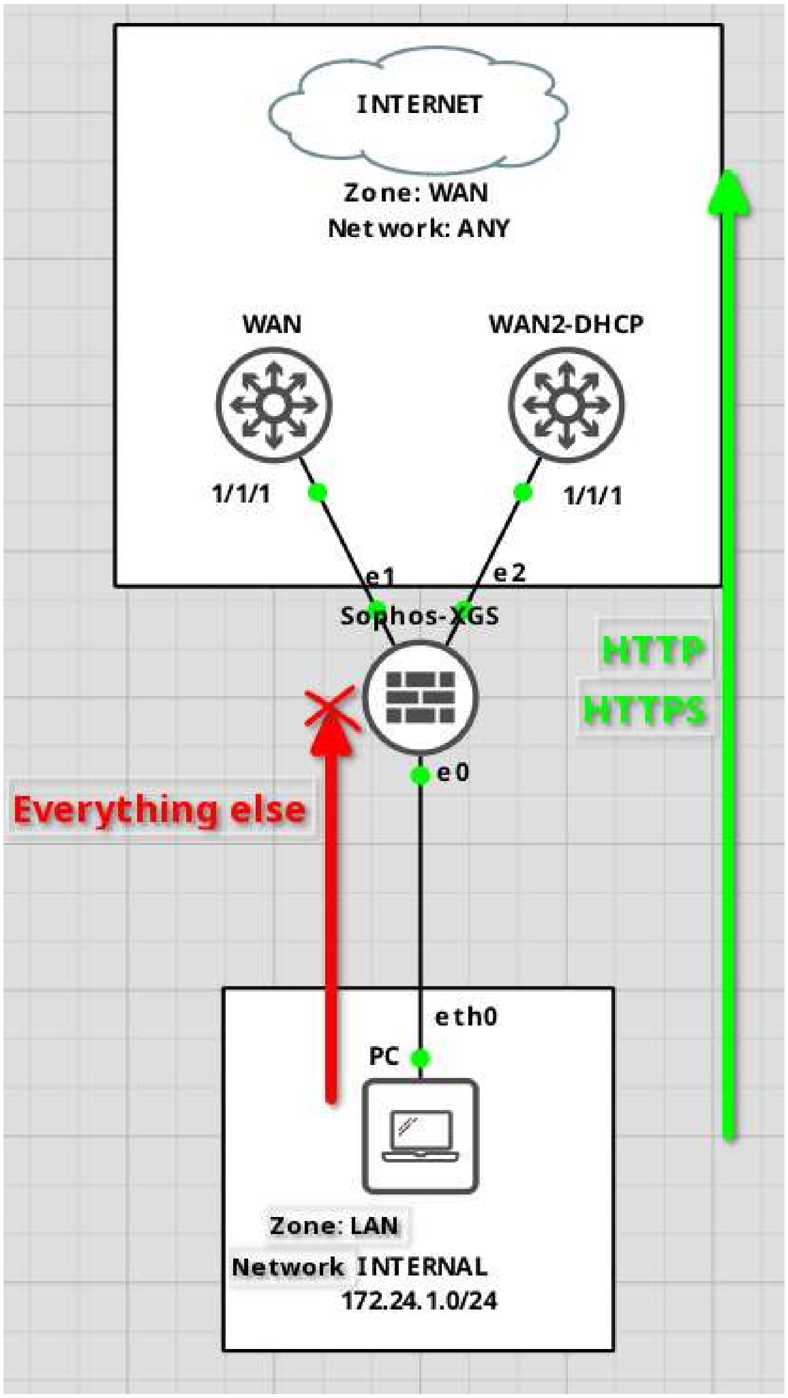
#	Name	Source	Destination	What	ID	Action	Feature and service
	Traffic to Interna... in 0 B, out 0 B	To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping optio...					
1	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	LAN, DMZ, WiFi, VPN, Any host...	Any service	#4	Drop	[illegible]
	Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...					
2	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host	WAN, Any host	Any service	#3	Drop	[illegible]
3	Webbrowsing in 0 B, out 0 B	LAN, INTERNAL	WAN, Any host	HTTP, HTTPS	#5	Accept	[illegible]
	Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...					
4	~~[example] Traffic...~~ in 0 B, out 0 B	Any zone, Any host, Any live user...	DMZ, Any host	Any service	#2	Drop	[illegible]
5	Auto added firewal... in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	[illegible]
6	Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	[illegible]

Showing 6 of 6. Selected 0

This rule allows any system from the “LAN” zone with an IP from the “INTERNAL” network to access “Any” IP in the “WAN” zone (basically the internet) with the protocols HTTP (80/TCP) and HTTPs (443/TCP).

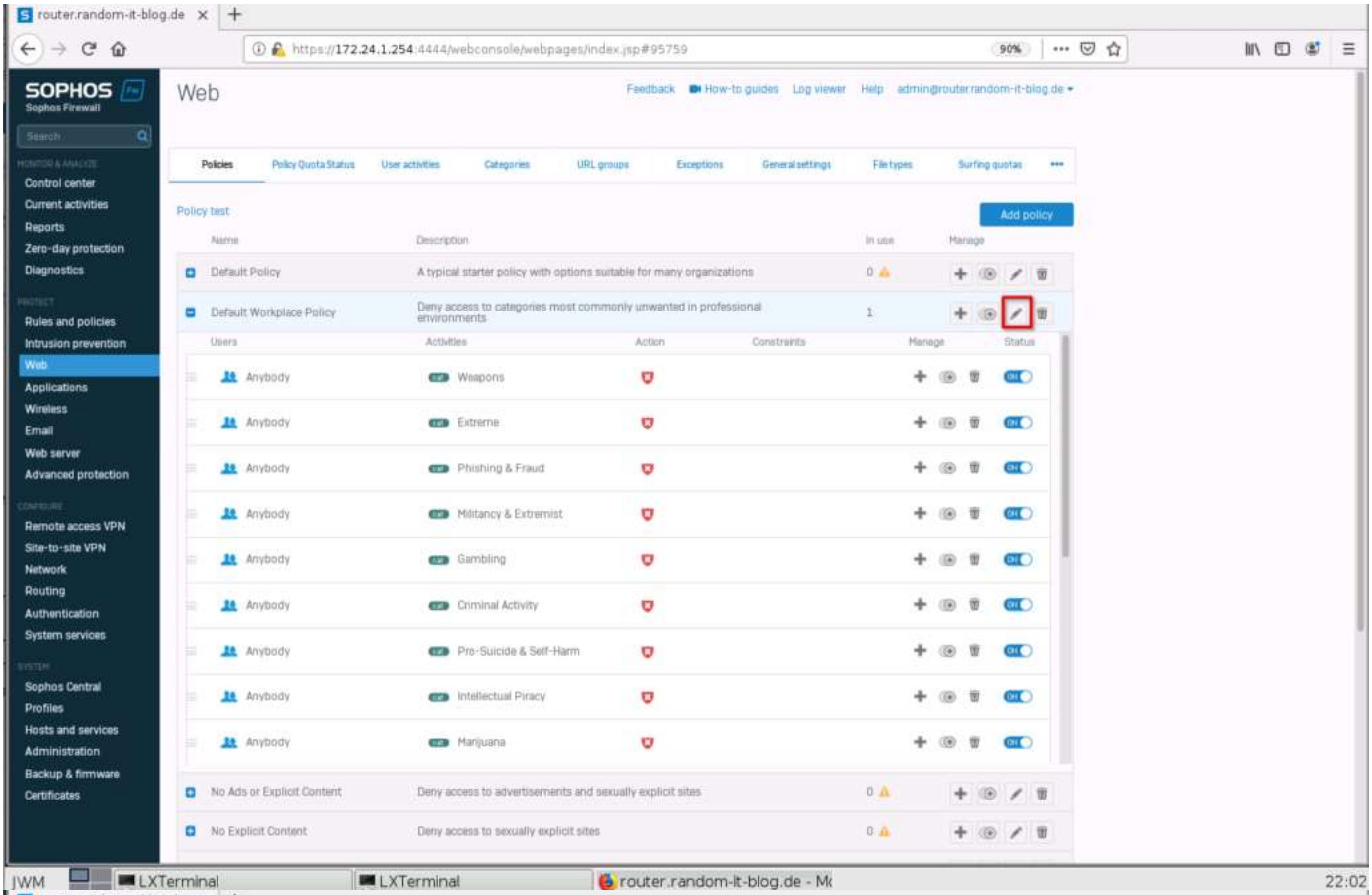
The default is to block everything.

Maybe this helps to understand the concept a little bit?



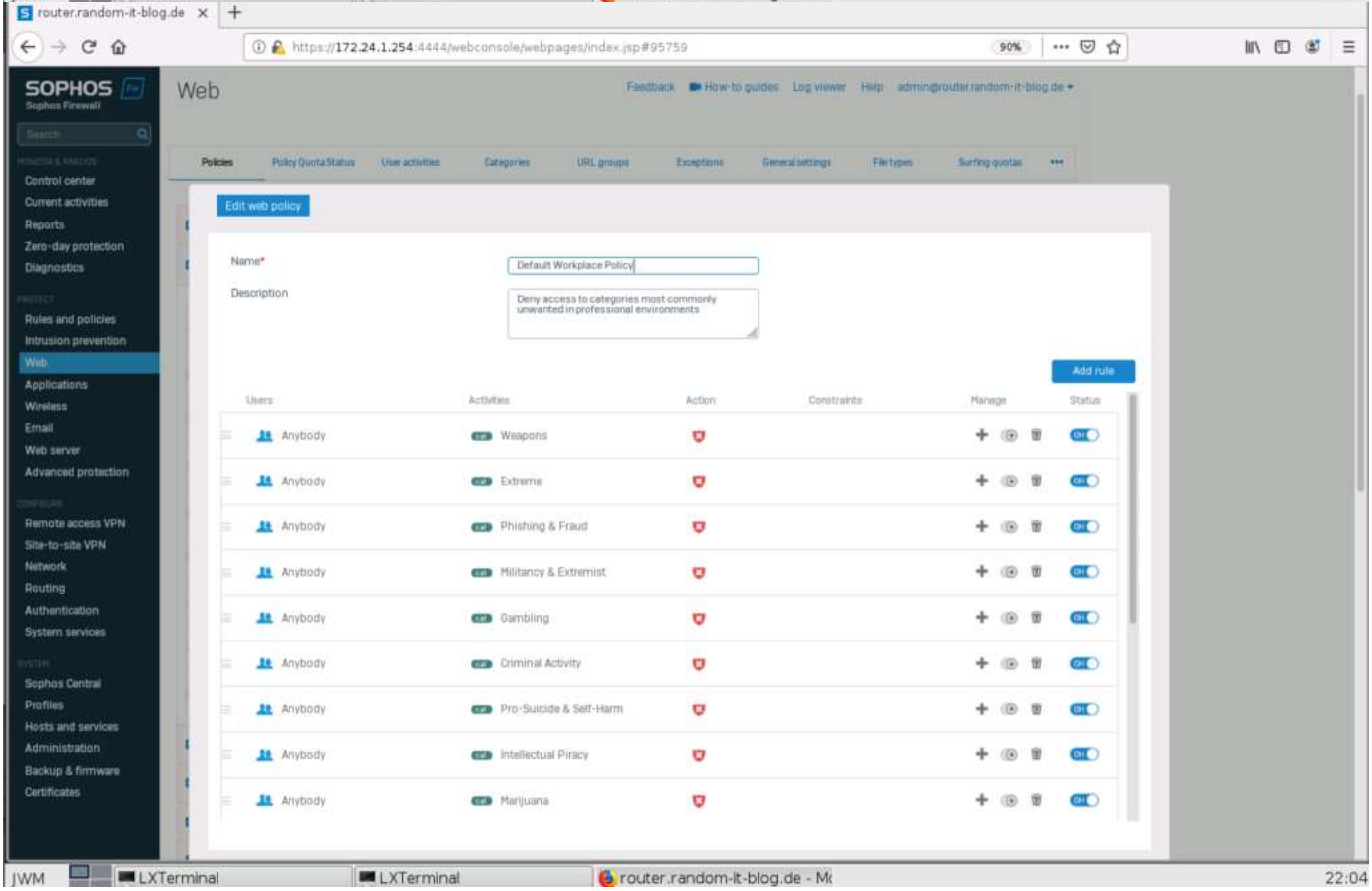
Webfilter Configuration

Onto the Webfilter configuration. Click on “Web” and select “Default Workplace Policy”.
For the most part, this filter is actually fine, but let’s just add another rule. Click on the pen symbol and select “Add rule”.



Name	Description	In use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	0	
Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	1	
No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0	
No Explicit Content	Deny access to sexually explicit sites	0	

Users	Activities	Action	Constraints	Manage	Status
Anybody	Weapons				ON
Anybody	Extreme				ON
Anybody	Phishing & Fraud				ON
Anybody	Militancy & Extremist				ON
Anybody	Gambling				ON
Anybody	Criminal Activity				ON
Anybody	Pro-Suicide & Self-Harm				ON
Anybody	Intellectual Piracy				ON
Anybody	Marijuana				ON



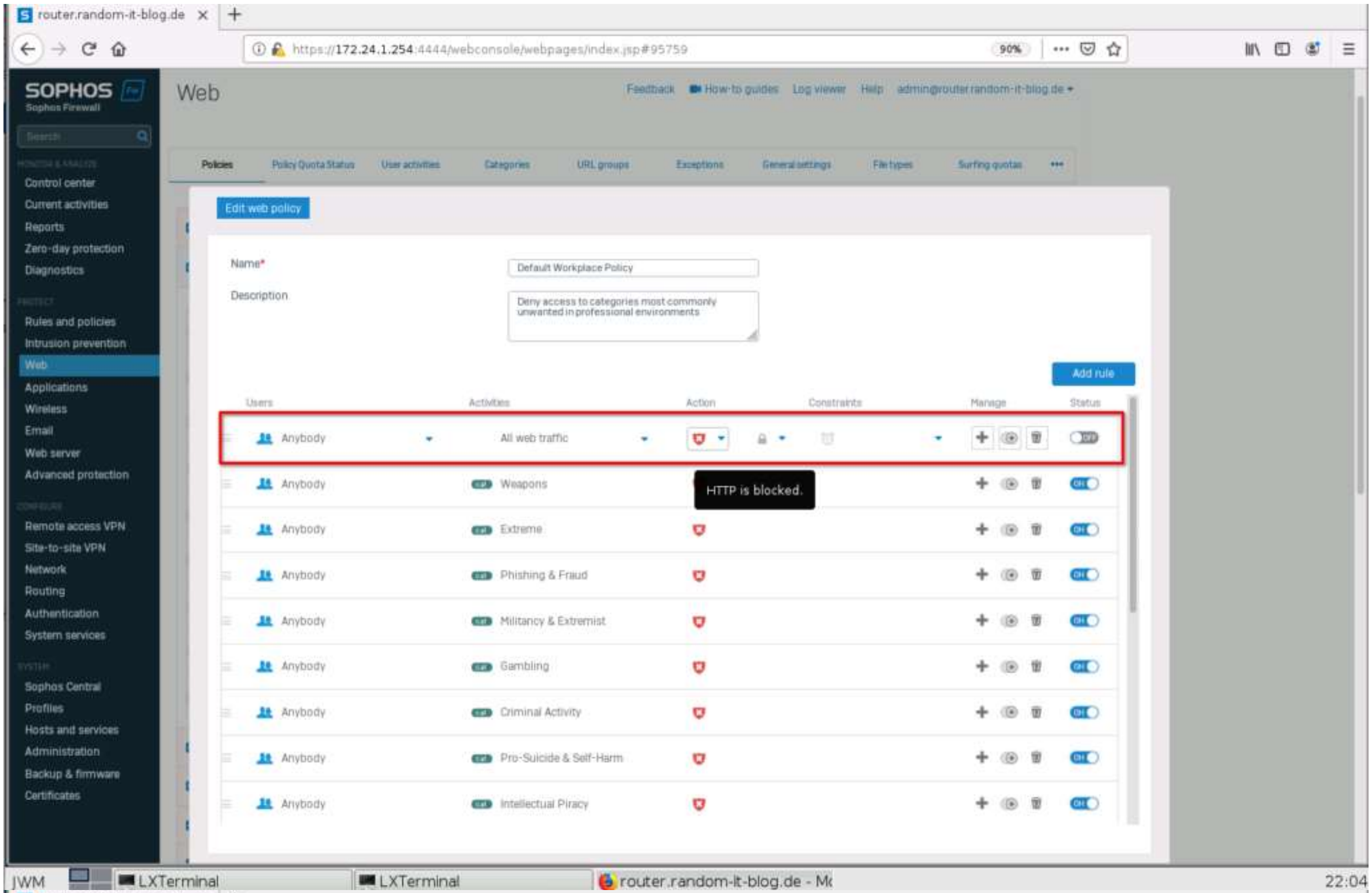
Name* Default Workplace Policy

Description Deny access to categories most commonly unwanted in professional environments

Users	Activities	Action	Constraints	Manage	Status
Anybody	Weapons				ON
Anybody	Extreme				ON
Anybody	Phishing & Fraud				ON
Anybody	Militancy & Extremist				ON
Anybody	Gambling				ON
Anybody	Criminal Activity				ON
Anybody	Pro-Suicide & Self-Harm				ON
Anybody	Intellectual Piracy				ON
Anybody	Marijuana				ON

This will add a new line at the top of the list. Here you can choose what kind of activities should be filtered, what kind of action should be taken and during what time (only weekends for instance).

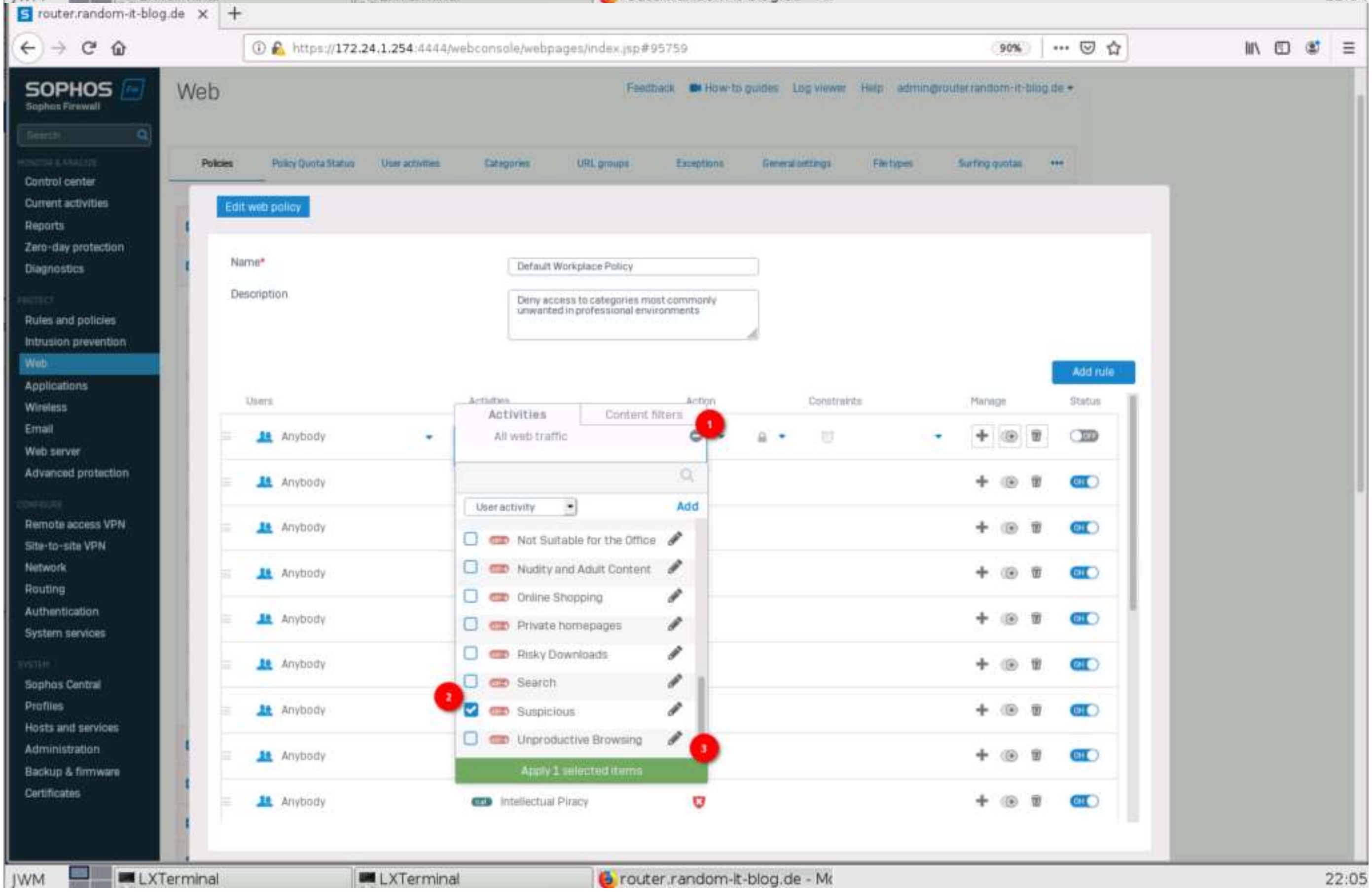
Click on “All web traffic” under “Activities”, deselect it, and select something more specific. I will choose “User activity” “Suspicious”. You could also choose something more specific, by switching to “All types” in the drop-down above. Enable the rule with the switch on the right.



Name* Default Workplace Policy

Description Deny access to categories most commonly unwanted in professional environments

Users	Activities	Action	Status
Anybody	All web traffic		OFF
Anybody	Weapons		ON
Anybody	Extreme		ON
Anybody	Phishing & Fraud		ON
Anybody	Militancy & Extremist		ON
Anybody	Gambling		ON
Anybody	Criminal Activity		ON
Anybody	Pro-Suicide & Self-Harm		ON
Anybody	Intellectual Piracy		ON



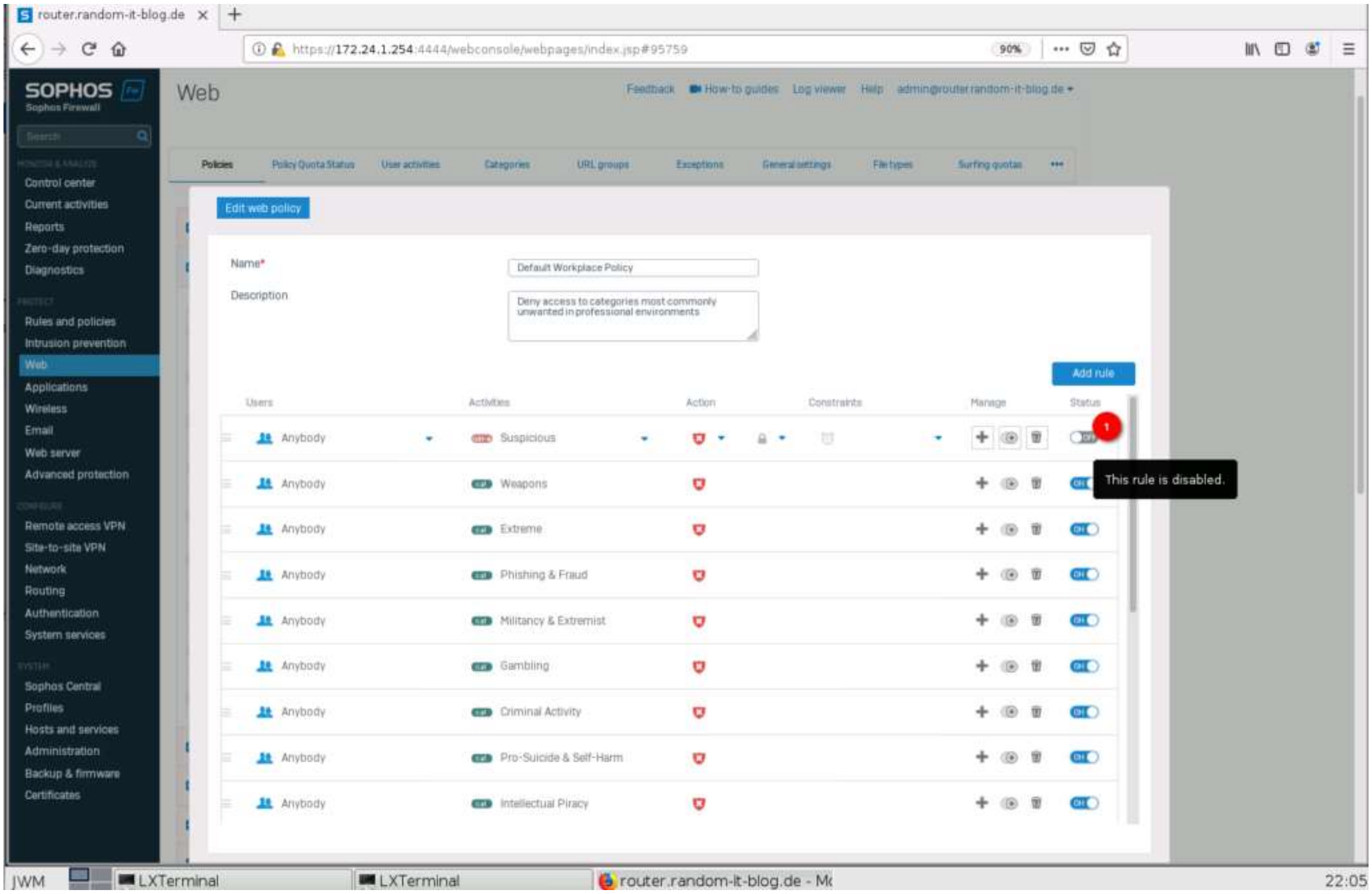
Name* Default Workplace Policy

Description Deny access to categories most commonly unwanted in professional environments

Anybody — All web traffic — OFF

- ☐ Not Suitable for the Office
- ☐ Nudity and Adult Content
- ☐ Online Shopping
- ☐ Private homepages
- ☐ Risky Downloads
- ☐ Search
- ☑ Suspicious
- ☐ Unproductive Browsing

Anybody — Intellectual Piracy — ON



Name* Default Workplace Policy

Description Deny access to categories most commonly unwanted in professional environments

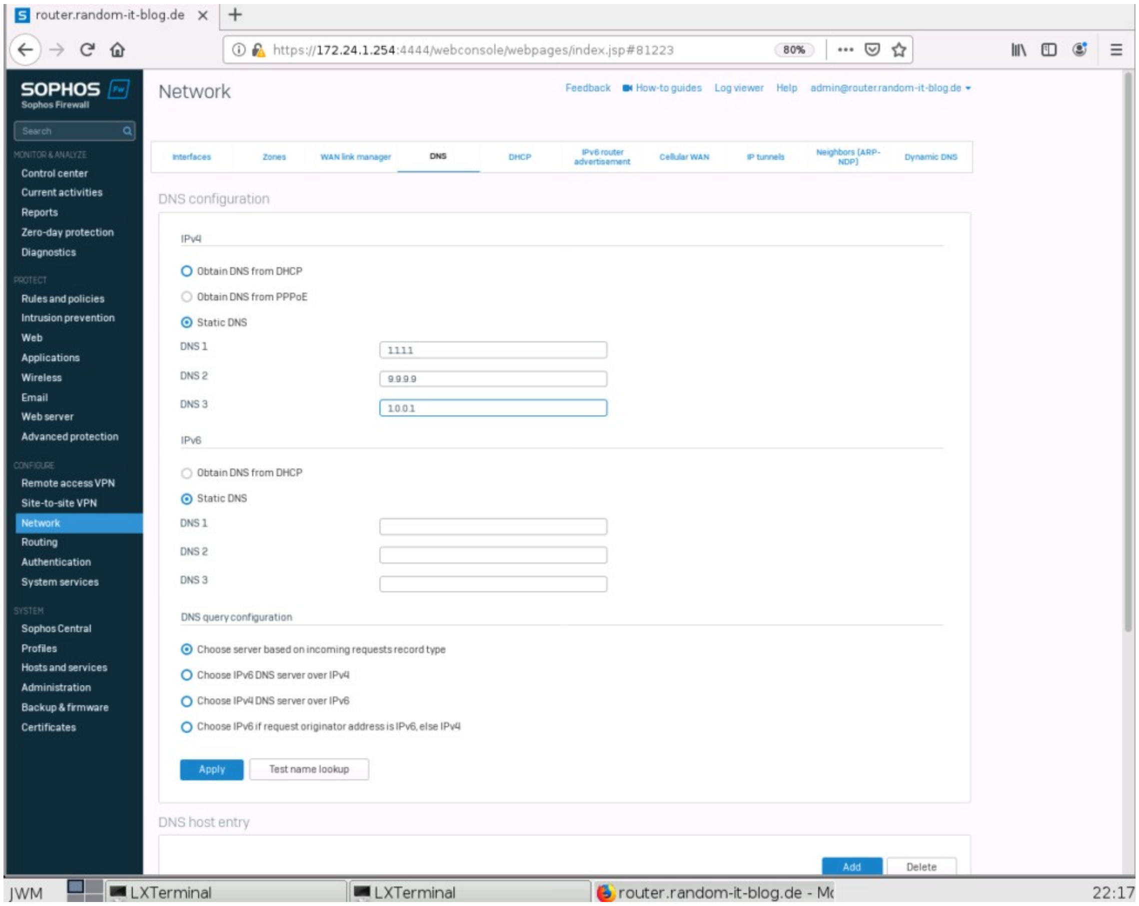
Users	Activities	Action	Constraints	Manage	Status
Anybody	Suspicious	🛡		✚	OFF
Anybody	Weapons	🛡		✚	ON
Anybody	Extreme	🛡		✚	ON
Anybody	Phishing & Fraud	🛡		✚	ON
Anybody	Militancy & Extremist	🛡		✚	ON
Anybody	Gambling	🛡		✚	ON
Anybody	Criminal Activity	🛡		✚	ON
Anybody	Pro-Suicide & Self-Harm	🛡		✚	ON
Anybody	Intellectual Piracy	🛡		✚	ON

This rule is disabled.

DNS Configuration

DNS is next on the list.

Select “Network” -> “DNS”. Here we can set the nameservers we want to use. I will use a few public DNS servers. Two are from Cloudflare and the other one is Quad9. Apply the configuration.



DNS configuration

IPv4

○ Obtain DNS from DHCP
○ Obtain DNS from PPPoE
● Static DNS

DNS 1: 1.1.1.1
DNS 2: 9.9.9.9
DNS 3: 1.0.0.1

IPv6

○ Obtain DNS from DHCP
● Static DNS

DNS 1:
DNS 2:
DNS 3:

DNS query configuration

● Choose server based on incoming requests record type
○ Choose IPv6 DNS server over IPv4
○ Choose IPv4 DNS server over IPv6
○ Choose IPv6 if request originator address is IPv6, else IPv4

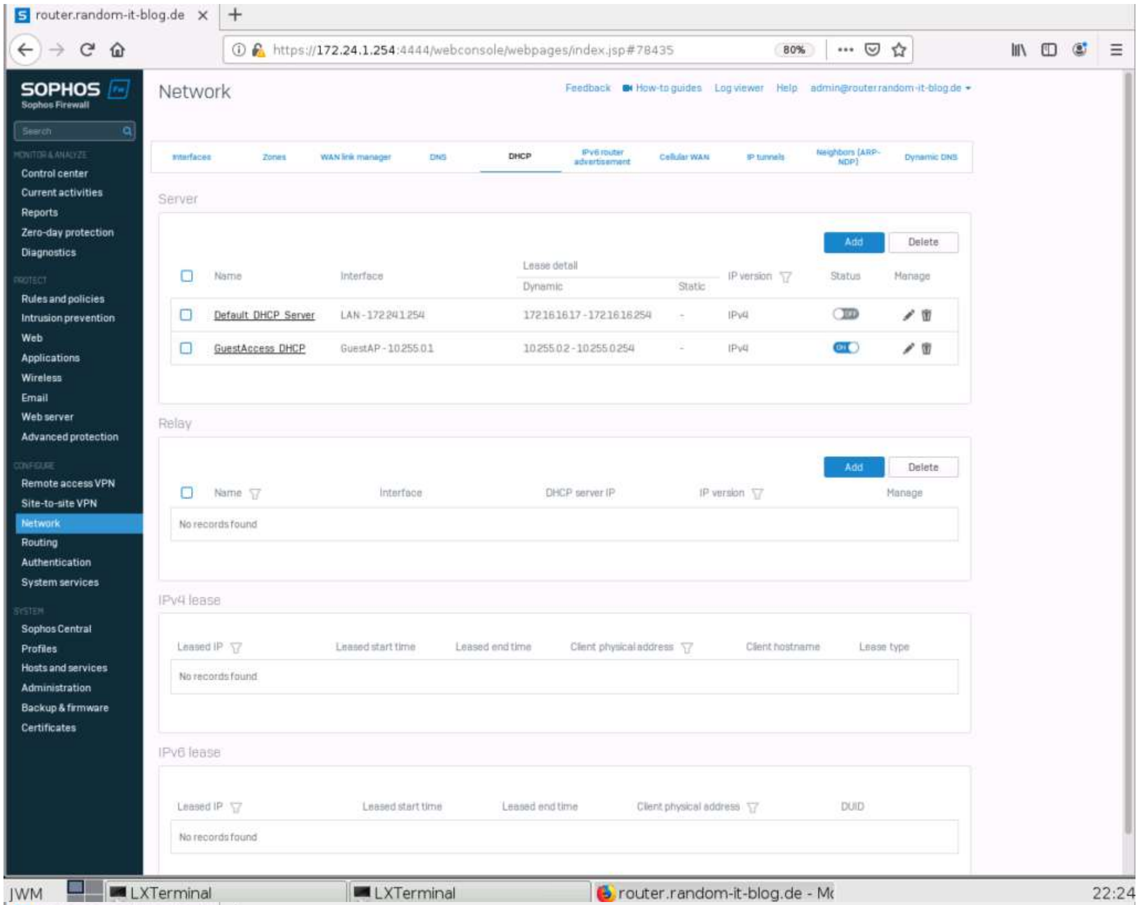
DNS host entry

DHCP Configuration

This should be the last setting. DHCP is disabled in the default configuration. This will stay disabled for the customer, but we will enable it for this demonstration.

Select “Network” -> “DHCP” and just click on the “Default DHCP Server”. Change the IP range to the correct subnet and the desired range. Enter the DNS server you want to distribute and click on “Save”.

Now switch the “off” button on the right to enable the DHCP Server. That’s it.



Network

Server

□	Name	Interface	Lease detail		IP version	Status	Manage
			Dynamic	Static			
□	Default_DHCP_Server	LAN - 172.24.1.254	172.16.16.17 - 172.16.16.254	-	IPv4	OFF	
□	GuestAccess_DHCP	GuestAP - 10.255.0.1	10.255.0.2 - 10.255.0.254	-	IPv4	ON	

Relay

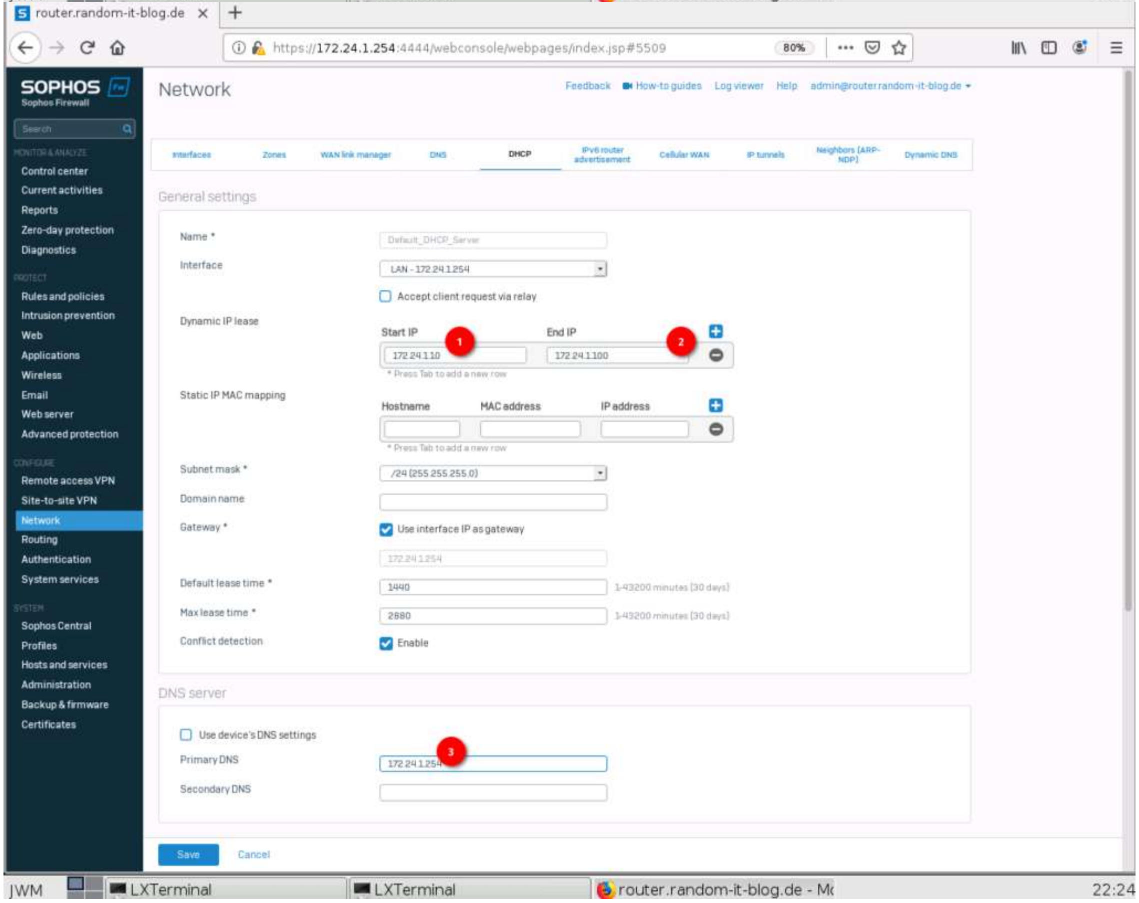
□	Name	Interface	DHCP server IP	IP version	Manage
No records found					

IPv4 lease

Leased IP	Leased start time	Leased end time	Client physical address	Client hostname	Lease type
No records found					

IPv6 lease

Leased IP	Leased start time	Leased end time	Client physical address	DUID
No records found				



Network

General settings

Name * Default_DHCP_Server

Interface LAN - 172.24.1.254

□ Accept client request via relay

Dynamic IP lease
Start IP 172.24.1.10 End IP 172.24.1.100
* Press Tab to add a new row

Static IP MAC mapping
Hostname MAC address IP address
* Press Tab to add a new row

Subnet mask * /24 (255.255.255.0)

Domain name

Gateway * ☑ Use interface IP as gateway
172.24.1.254

Default lease time * 1440 1-43200 minutes (30 days)

Max lease time * 2880 1-43200 minutes (30 days)

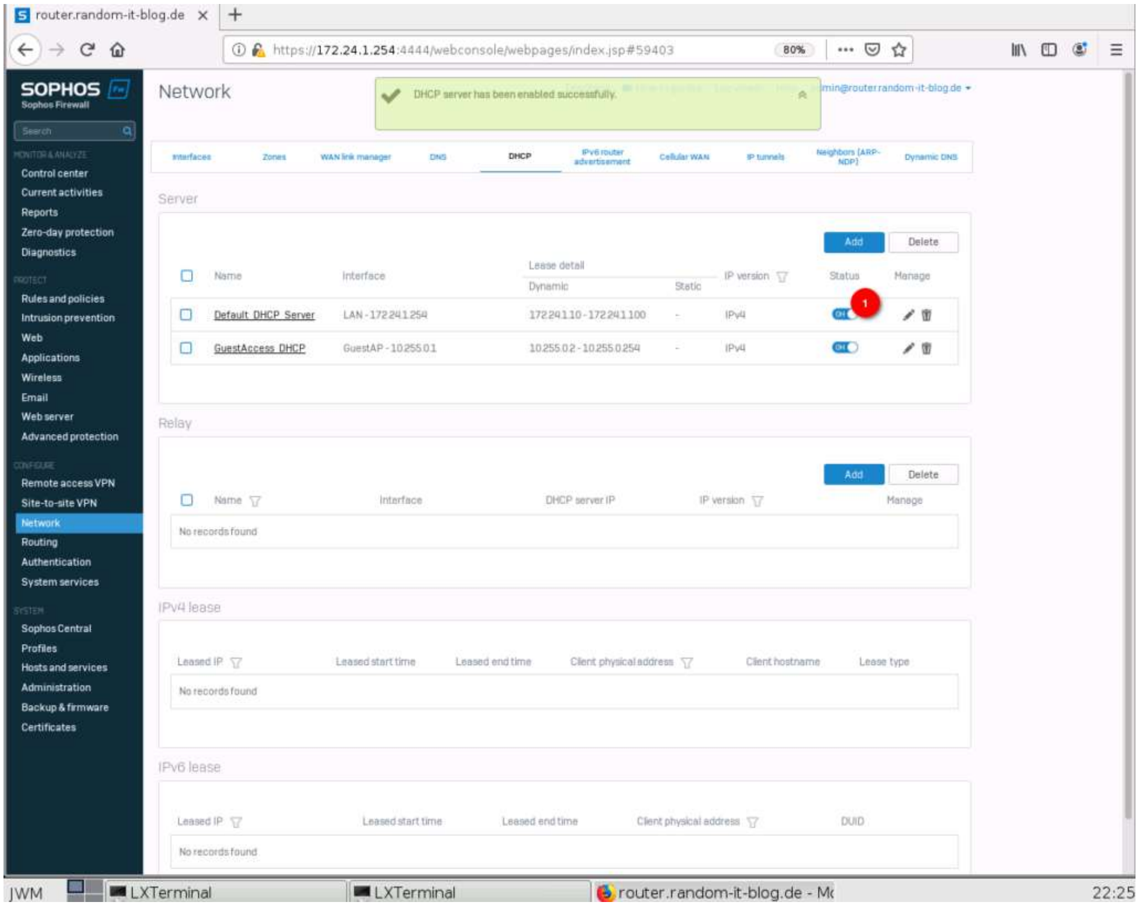
Conflict detection ☑ Enable

DNS server

□ Use device's DNS settings

Primary DNS 172.24.1.254

Secondary DNS



Network

DHCP server has been enabled successfully.

Server

□	Name	Interface	Lease detail		IP version	Status	Manage
			Dynamic	Static			
□	Default DHCP Server	LAN - 172.24.1.254	172.24.1.10 - 172.24.1.100	-	IPv4	ON	
□	GuestAccess DHCP	GuestAP - 10.255.0.1	10.255.0.2 - 10.255.0.254	-	IPv4	ON	

Relay

□	Name	Interface	DHCP server IP	IP version	Manage
No records found					

IPv4 lease

Leased IP	Leased start time	Leased end time	Client physical address	Client hostname	Lease type
No records found					

IPv6 lease

Leased IP	Leased start time	Leased end time	Client physical address	DUID
No records found				

Add Exceptions to WAF on Sophos XG Firewall

To add exceptions or exclusions to the Web Application Firewall (WAF) on a Sophos XG Firewall, you typically need to create specific rules that bypass the WAF inspection for certain web traffic or URLs. Here's a general guide on how to add exceptions to the WAF on a Sophos XG Firewall:

Access the Sophos XG Firewall Interface: Log in to the Sophos XG Firewall's web-based administration interface using your administrator credentials.

Navigate to the WAF Configuration: Go to the section of the administration interface where you can configure the Web Application Firewall settings. This is typically found under the "Protection" or "Firewall" menu.

Create a New WAF Policy: If you haven't already created a separate policy for managing exceptions, you may want to do so. This will allow you to keep exception rules separate from your regular WAF rules.

Add an Exception Rule: Within the WAF policy or rule set, locate the option to add a new rule. Depending on the interface design of the Sophos XG Firewall, this may involve clicking on a "Add Rule" button or similar action.

Configure the Exception Rule:

Define the criteria for the exception rule. This could include specifying the source IP addresses, destination URLs, or other attributes that identify the traffic you want to exclude from WAF inspection.

Specify the action for the rule. In this case, you would typically select an action that bypasses or excludes the traffic from WAF inspection. This may be labeled as "Bypass", "Exclude", or similar.

Optionally, provide a description or comment to document the purpose of the exception rule for future reference.

Save the Rule: Once you have configured the exception rule, save your changes to apply the rule to the WAF policy.

Test the Exception Rule: Before deploying the exception rule in a production environment, test it to ensure that it effectively bypasses WAF inspection for the intended traffic without unintended consequences.

Monitor and Maintain: Regularly monitor the WAF logs and reports to verify that the exception rules are working as expected and are not being abused or misused. Make any necessary adjustments to the exception rules based on changes in your network environment or security requirements.

By following these steps, you can add exceptions to the Web Application Firewall on a Sophos XG Firewall to allow certain web traffic to bypass WAF inspection when necessary.