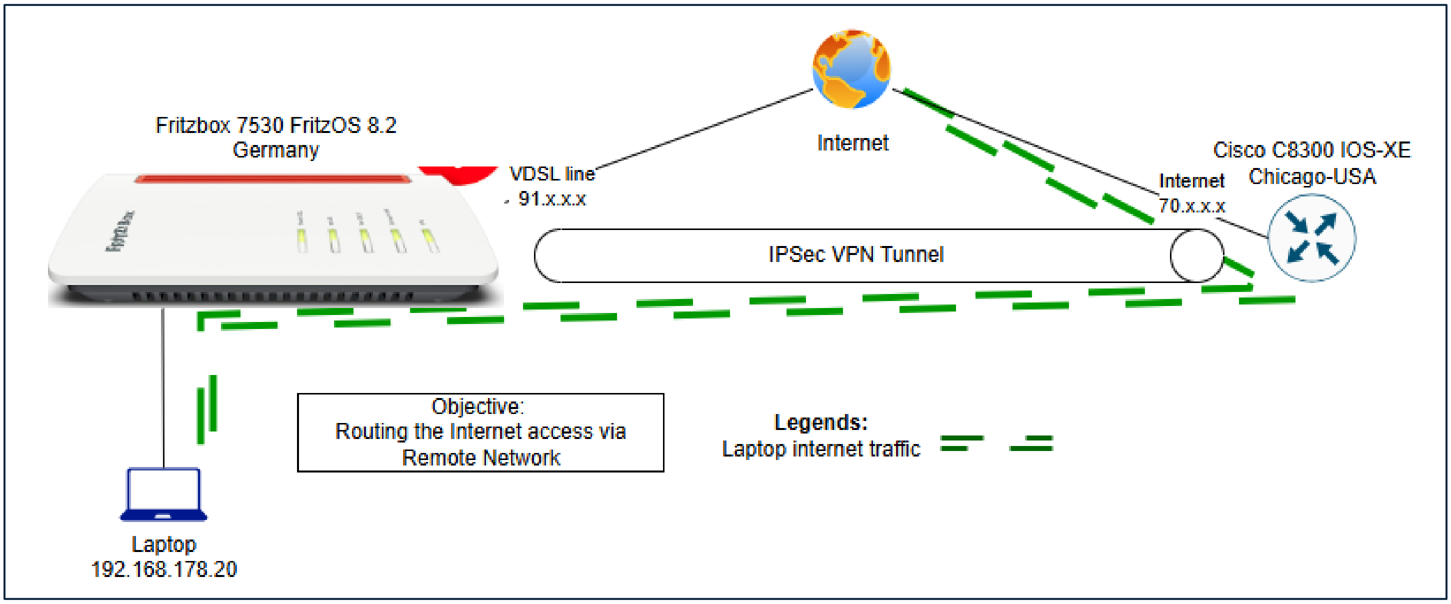
IPSec VPN configuration between Fritzbox and Cisco Router

Objective:

The Objective of this project is to route Laptop internet browsing traffic via Remote Cisco Router via IPSec VPN Tunnel. This way Laptop can access the content which are available in the remote Geography.

Topology:



Components involved in this Project:

1. Fritzbox 7530 with FritzOS 8.2; it is very popular consumer grade Broadband Router in Germany
2. Cisco C8300 Router with IOS 17.12
3. Windows 11 Laptop

IPSec VPN configuration between Fritzbox and Cisco Router

Configuration/ Programming:

Cisco Router configuration:

! aaa configuration

```
aaa new-model

aaa authentication login vpn local

aaa authorization network vpn local

aaa session-id common
```

! vpn user account for X-Auth

```
username testing1 password 0 Testing1234
```

! ISAKMP policy for phase 1 negotiation

```
 crypto isakmp policy 1

encryption aes 256

hash sha256

authentication pre-share

group 14

lifetime 3600

crypto isakmp policy 2

encryption aes

hash sha

authentication pre-share

group 14
```

!ISAKMP Client profile configuration

```
crypto isakmp client configuration group cisco
```

IPSec VPN configuration between Fritzbox and Cisco Router

```
key Testing1234
pool vpn
save-password
max-logins 3

! VPN pool creation of IP address offering to VPN Client
ip local pool vpn 192.168.143.5 192.168.143.10

! ISAKMP profile configuration
crypto isakmp profile vpn
  match identity group cisco
  client authentication list vpn
  isakmp authorization list vpn password Testing1234
  client configuration address respond
  virtual-template 1

! IPSec Configuration for the Phase 2 communication

crypto ipsec transform-set vpn esp-aes esp-sha-hmac
mode tunnel
crypto ipsec profile vpn
set transform-set vpn

! Virtual-Template 1 interface configuration for the IPSec Traffic

interface Virtual-Template1 type tunnel
```

```
ip unnumbered GigabitEthernet0/0/1

ip nat inside

tunnel mode ipsec ipv4

tunnel protection ipsec profile vpn

ip virtual-reassembly

End
```

! INTERNET INTERFACE Configuration

```
interface GigabitEthernet0/0/1

description ->Chicago INTERNET

ip address 70.x.x.x 255.255.255.252

ip nat outside

ip access-group OUTSIDE in

load-interval 30

negotiation auto

End
```

!Update the ACL to allow the Fritzbox public IP to have IPSec VPN traffic

```
ip access-list extended OUTSIDE

91 permit udp host 92.1.2.3 any eq non500-isakmp

92 permit udp host 92.1.2.3 any eq isakmp
```

!Update the NAT ACL to perform the NAT translation for internet bound traffic

IPSec VPN configuration between Fritzbox and Cisco Router

```
ip access-list extended NAT
```

```
11 permit ip 192.168.143.0 0.0.0.255 any --> This is the VPN pool address range
```

! Router Global NAT configuration

```
ip nat inside source list NAT interface GigabitEthernet0/0/1 overload
```

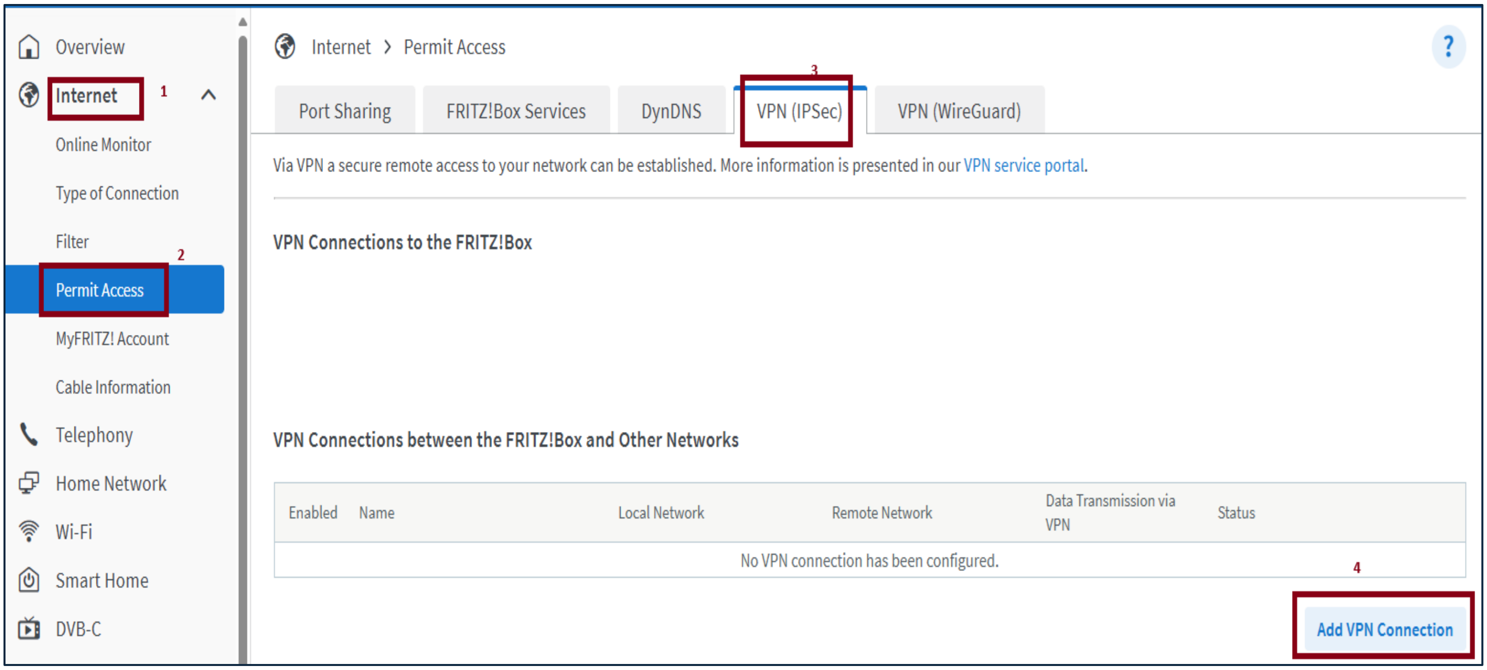
FRITZBOX configuration

Login to Fritzbox webUI

https://fritz.box

Navigate to **INTERNET** --> **Permit Access** --> **VPN (IPSec)**

Under “**VPN Connections between the FRITZ!Box and Other Networks**” --> **Add VPN Connection**



Via VPN a secure remote access to your network can be established. More information is presented in our VPN service portal.

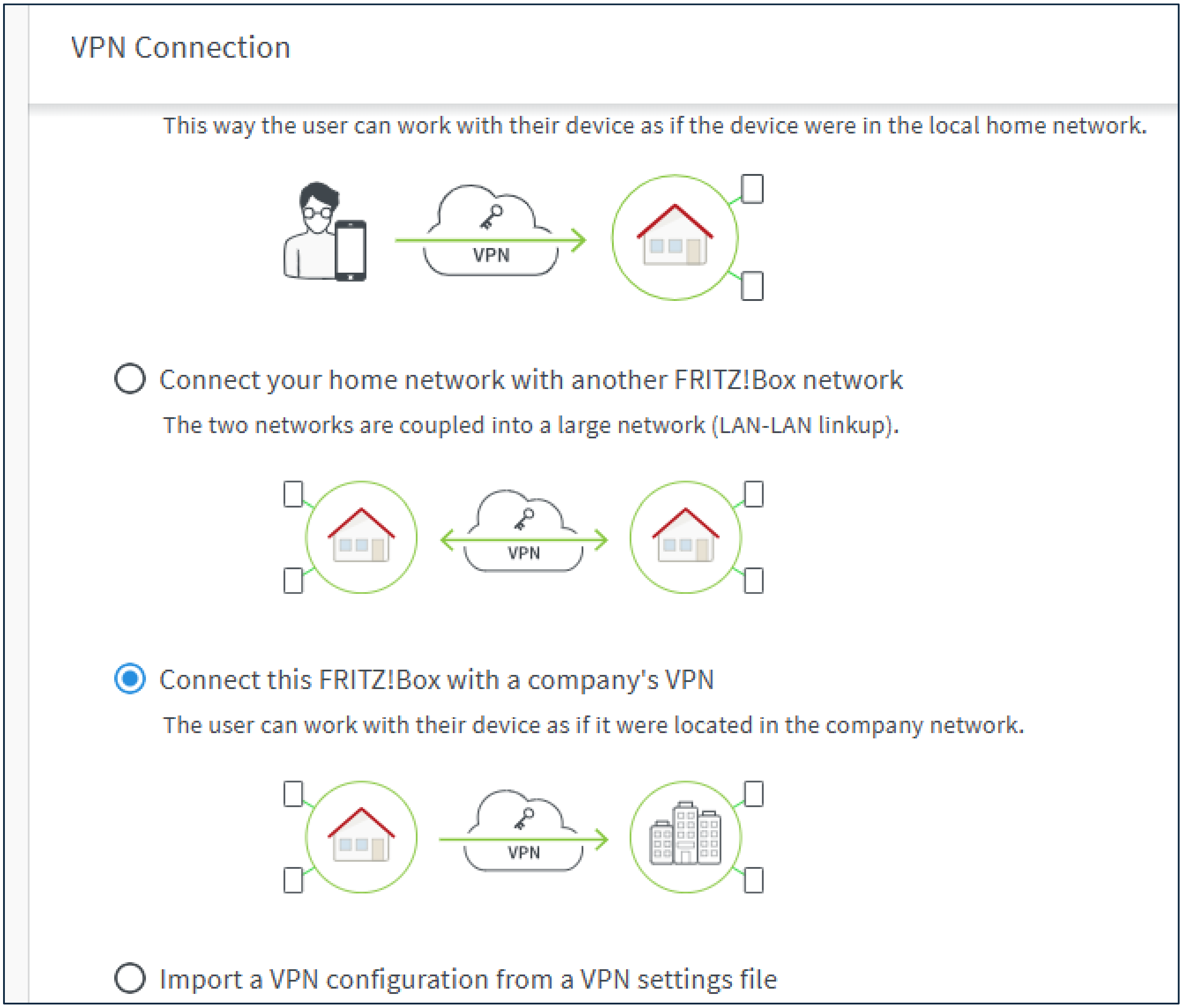
VPN Connections to the FRITZ!Box

VPN Connections between the FRITZ!Box and Other Networks

Enabled	Name	Local Network	Remote Network	Data Transmission via VPN	Status
No VPN connection has been configured.					

Click on “**Connect this FRITZ!Box with a company's VPN**”

IPSec VPN configuration between Fritzbox and Cisco Router



VPN Connection

This way the user can work with their device as if the device were in the local home network.

○ Connect your home network with another FRITZ!Box network

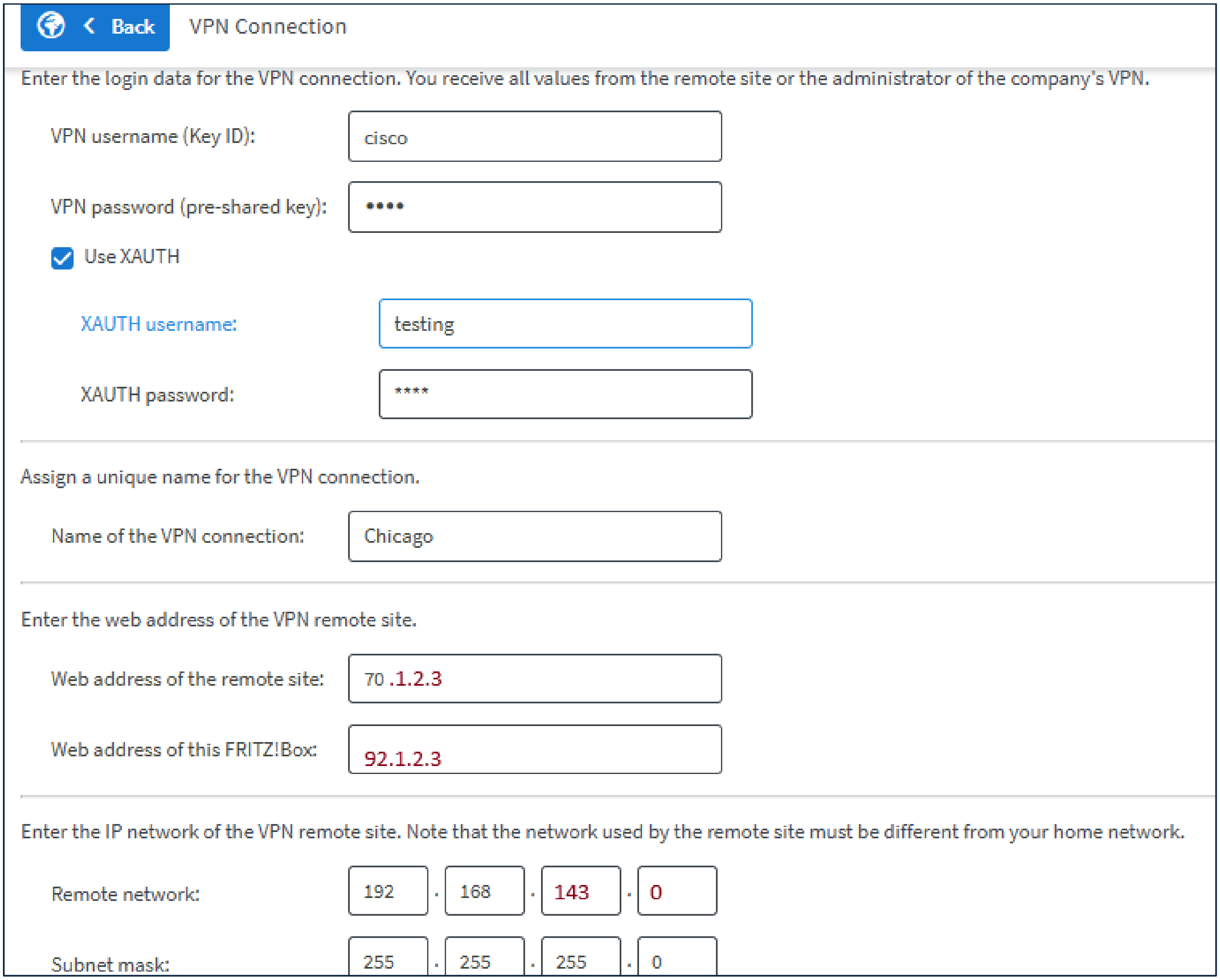
The two networks are coupled into a large network (LAN-LAN linkup).

● Connect this FRITZ!Box with a company's VPN

The user can work with their device as if it were located in the company network.

○ Import a VPN configuration from a VPN settings file

IPSec VPN configuration between Fritzbox and Cisco Router



VPN Connection

Enter the login data for the VPN connection. You receive all values from the remote site or the administrator of the company's VPN.

VPN username (Key ID): cisco

VPN password (pre-shared key): ••••

☑ Use XAUTH

XAUTH username: testing

XAUTH password: ****

Assign a unique name for the VPN connection.

Name of the VPN connection: Chicago

Enter the web address of the VPN remote site.

Web address of the remote site: 70 .1.2.3

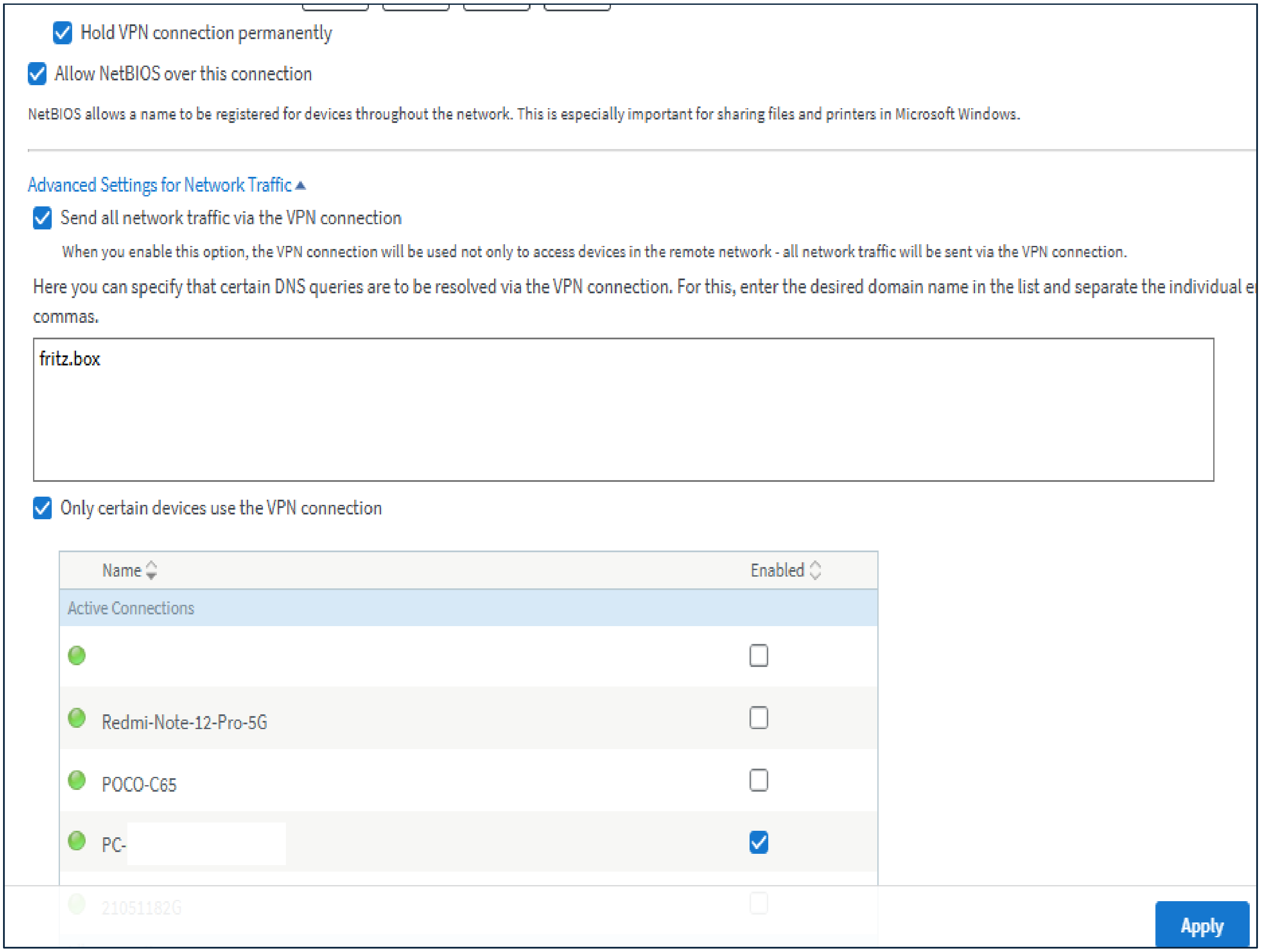
Web address of this FRITZ!Box: 92.1.2.3

Enter the IP network of the VPN remote site. Note that the network used by the remote site must be different from your home network.

Remote network: 192 . 168 . 143 . 0

Subnet mask: 255 . 255 . 255 . 0

IPSec VPN configuration between Fritzbox and Cisco Router



☑ Hold VPN connection permanently

☑ Allow NetBIOS over this connection

NetBIOS allows a name to be registered for devices throughout the network. This is especially important for sharing files and printers in Microsoft Windows.

Advanced Settings for Network Traffic ▲

☑ Send all network traffic via the VPN connection

When you enable this option, the VPN connection will be used not only to access devices in the remote network - all network traffic will be sent via the VPN connection.

Here you can specify that certain DNS queries are to be resolved via the VPN connection. For this, enter the desired domain name in the list and separate the individual e commas.

fritz.box

☑ Only certain devices use the VPN connection

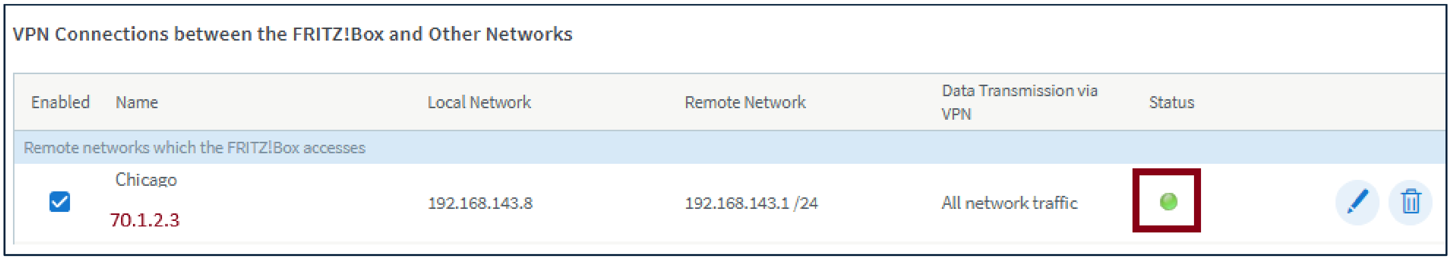
Name	Enabled
Active Connections	
●	□
● Redmi-Note-12-Pro-5G	□
● POCO-C65	□
● PC-	☑
● 21051182G	□

I have selected only my Laptop “PC” to be able to route All traffic via this VPN Tunnel,

Validation, Testing:

Once this has been successfully configured, we can see the VPN Status on both Fritzbox and Cisco Router as per below.

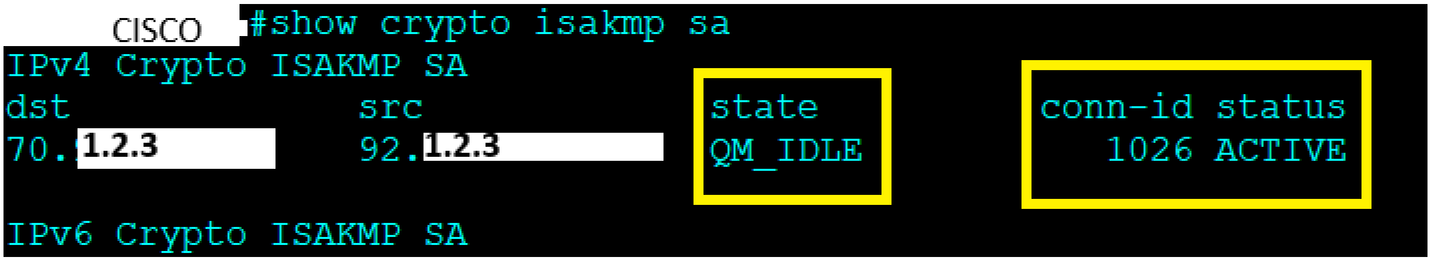
IPSec VPN configuration between Fritzbox and Cisco Router



VPN Connections between the FRITZ!Box and Other Networks

Enabled	Name	Local Network	Remote Network	Data Transmission via VPN	Status
Remote networks which the FRITZ!Box accesses					
☑	Chicago 70.1.2.3	192.168.143.8	192.168.143.1 /24	All network traffic	●

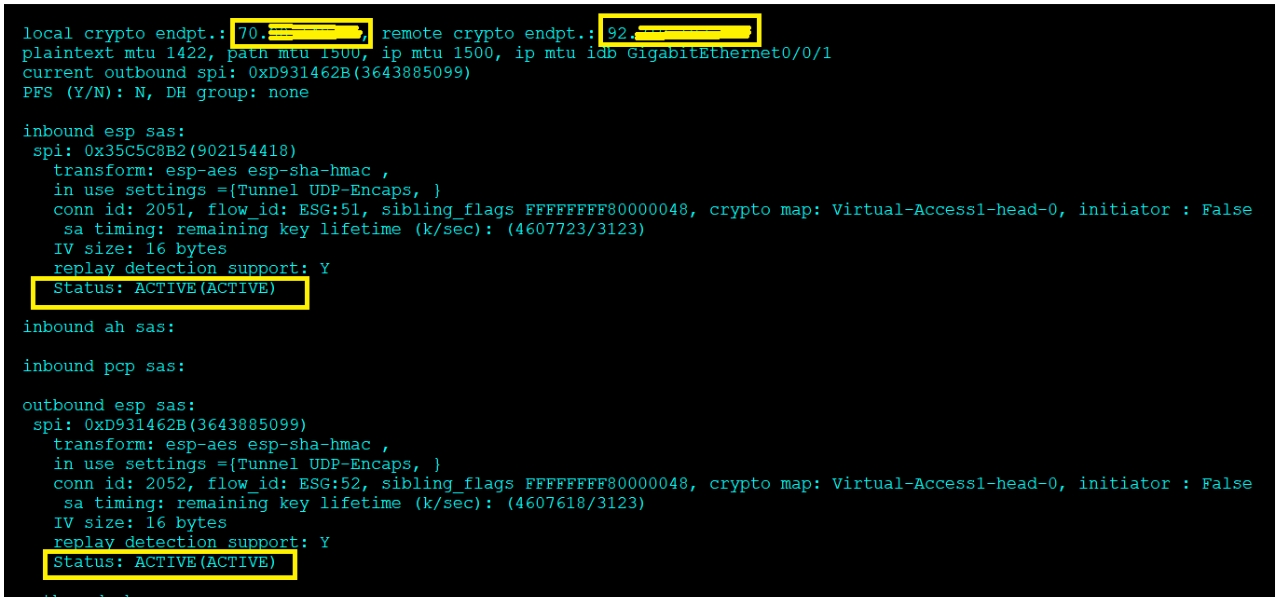
Cisco Router IPSec Phase 1 status (ISAKMP)



```
CISCO   #show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state       conn-id status
70.1.2.3        92.1.2.3        QM_IDLE        1026 ACTIVE

IPv6 Crypto ISAKMP SA
```

Cisco Router IPSec Phase 2 status (IPSec Tunnel)



```
local crypto endpt.: 70.[redacted], remote crypto endpt.: 92.[redacted]
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/1
current outbound spi: 0xD931462B(3643885099)
PFS (Y/N): N, DH group: none

inbound esp sas:
 spi: 0x35C5C8B2(902154418)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Tunnel UDP-Encaps, }
   conn id: 2051, flow_id: ESG:51, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-head-0, initiator : False
    sa timing: remaining key lifetime (k/sec): (4607723/3123)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xD931462B(3643885099)
   transform: esp-aes esp-sha-hmac ,
   in use settings ={Tunnel UDP-Encaps, }
   conn id: 2052, flow_id: ESG:52, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-head-0, initiator : False
    sa timing: remaining key lifetime (k/sec): (4607618/3123)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)
```