PONIVA

FIREWALL

Installation & Administration Guide

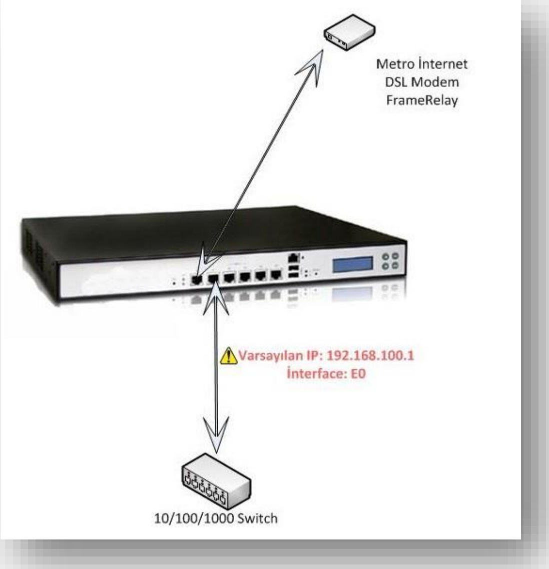
CONTENTS

TECHNICIAL SPECIFICATIONS

10/100/1000 Mbps Ethernet Port	6
USB Port	2nd
Internal Storage	128GB SSD
Firewall Throughput (Gbps)	6
IPSEC Throughput (Gbps)	3
SSL VPN Throughput (Gbps)	2.5
URL Throughput (Gbps)	4
Antivirus Throughput (Gbps)	3
Power source	one
Certification	CE/FCC
Dimensions	438x292.1x44 mm

SETUP

1. From the device's IGB0 Ethernet portPlug a cable into your DSL Modem/Router.
2. Plug a cable from the device's IGB1 port to your Switch or computer in your network.



Your device's default IP its address is 192.168.100.1.
You can access the Web Management Panel at http://192.168.100.1:8400.

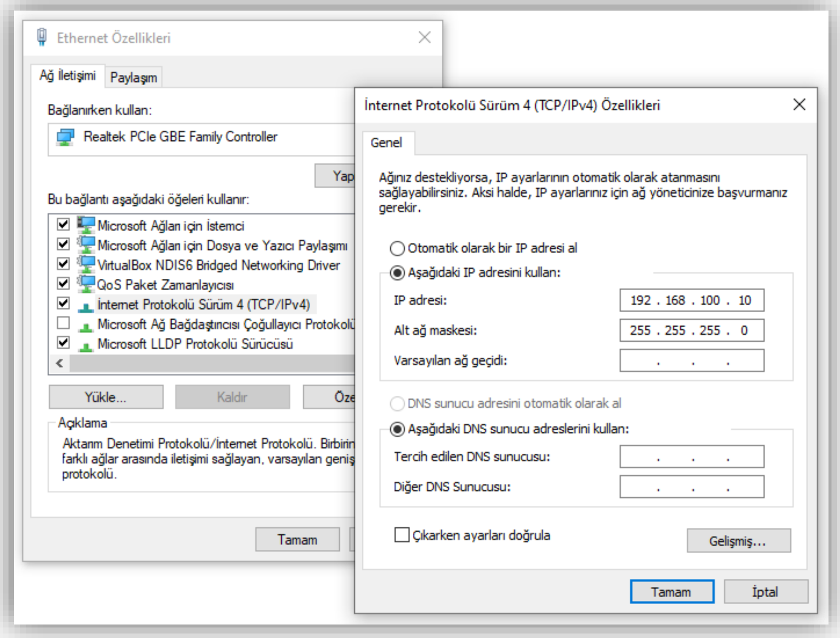
Default User:admin Password: admin.

in your networkIf you do not want to change your IP block, you must change your modem's IP address to a different block before starting the installation.

E.g;If your modem's IP address is 192.168.1.1, before activating your Firewall device, change the modem's IP address to 192.168.3.1 and turn it off and on so that your modem's settings are active.

ConnectionOur process is complete, now we can make the initial setup settings.

For the installation of our computer IP address Firewall device must have an IP address in its network, for this we need to get a new IP automatically for our computer or we need to define an IP manually as follows.



Ethernet Özellikleri

Ağ İletişimi | Paylaşım

Bağlanırken kullan:

Realtek PCIe GBE Family Controller

Bu bağlantı aşağıdaki öğeleri kullanır:

- ☑ Microsoft Ağları için İstemci
- ☑ Microsoft Ağları için Dosya ve Yazıcı Paylaşımı
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Paket Zamanlayıcısı
- ☑ İnternet Protokolü Sürüm 4 (TCP/IPv4)
- □ Microsoft Ağ Bağdaştırıcısı Çoğullayıcı Protokolü
- ☑ Microsoft LLDP Protokolü Sürücüsü

Açıklama

Aktarım Denetimi Protokolü/İnternet Protokolü. Birbirin farklı ağlar arasında iletişimi sağlayan, varsayılan geniş protokolü.

İnternet Protokolü Sürüm 4 (TCP/IPv4) Özellikleri

Genel

Ağınız destekliyorsa, IP ayarlarının otomatik olarak atanmasını sağlayabilirsiniz. Aksi halde, IP ayarlarınız için ağ yöneticinize başvurmanız gerekir.

○ Otomatik olarak bir IP adresi al

● Aşağıdaki IP adresini kullan:

IP adresi: 192 . 168 . 100 . 10

Alt ağ maskesi: 255 . 255 . 255 . 0

Varsayılan ağ geçidi: . . .

○ DNS sunucu adresini otomatik olarak al

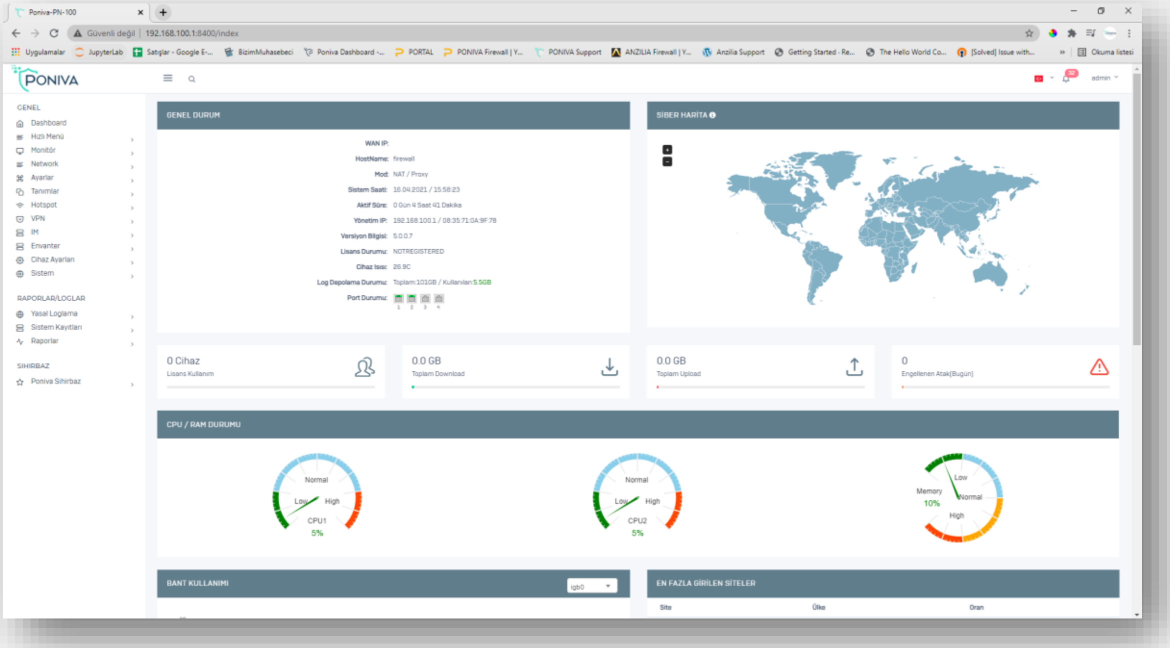
● Aşağıdaki DNS sunucu adreslerini kullan:

Tercih edilen DNS sunucusu: . . .

Diğer DNS Sunucusu: . . .

□ Çıkarken ayarları doğrula

After the IP identification process is finished, we open our browser and write http://192.168.100.1:8400. (You must type "http://" to access via Internet Explorer.)



Güvenli değil | 192.168.100.1:8400/index

GENEL DURUM

WAN IP:

HostName: firewall

Mod: NAT / Proxy

Sistem Saati: 16.04.2021 / 15:58:23

Aktif Süre: 0 Gün 4 Saat 41 Dakika

Yönetim IP: 192.168.100.1 / 08:35:71:0A:9F:78

Versiyon Bilgisi: 5.0.0.7

Lisans Durumu: NOTREGISTERED

Cihaz Isısı: 26.9C

Log Depolama Durumu: Toplam:101GB / Kullanılan:5.5GB

Port Durumu: 1 2 3 4

0 Cihaz Lisans Kullanım

0.0 GB Toplam Download

0.0 GB Toplam Upload

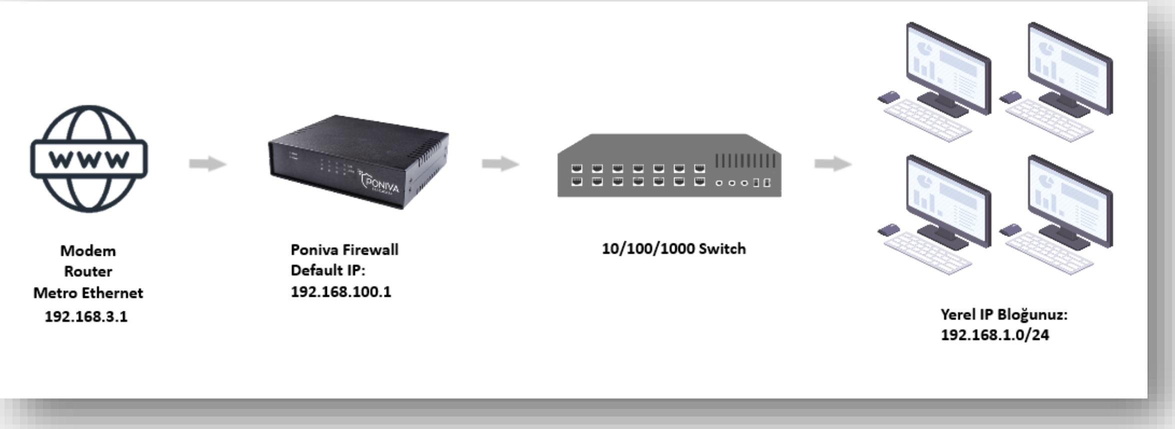
0 Engellenen Atak(Bugün)

Introduction to the firewall interface After you have done the installation, you can continue with the help of "Wizard" or "Manual".

SETUP WİZARD

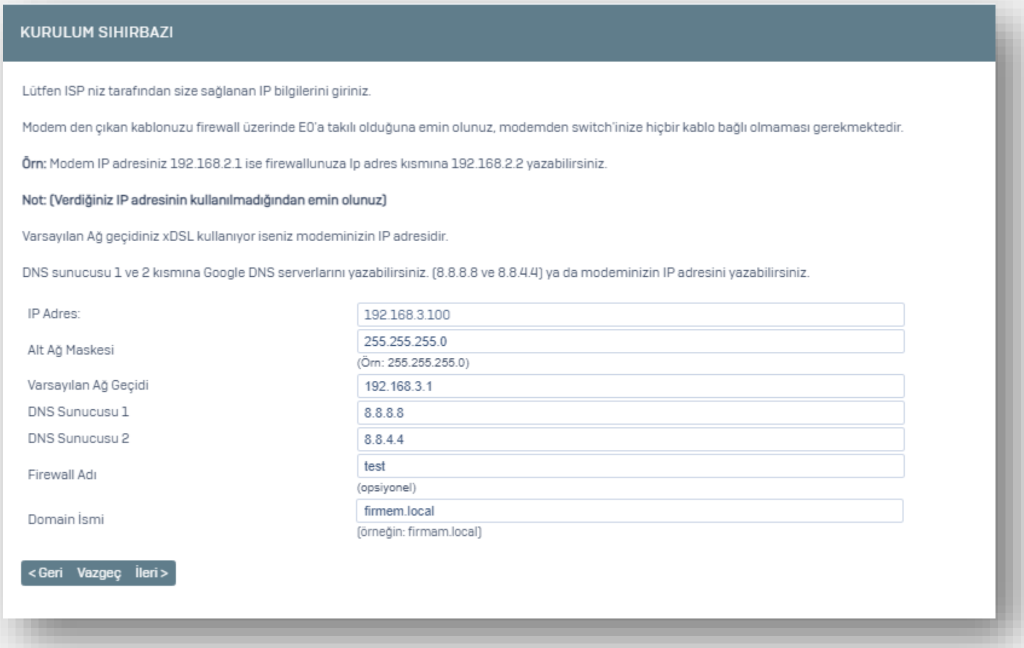
Setup wizardwith automatic configuration process; Firewall will help you to activate your device.

It will continue assuming your local network is 192.168.1.0/24 and the modem IP address is 192.168.3.1.



Let's start the process by clicking Poniva Wizard->Installation Wizard on the interface screen.

WAN (internet) settings are configured after passing the first screen.
(ManualIP assignment is recommended, port forwarding etc. for)



KURULUM SIHIRBAZI

Lütfen ISP niz tarafından size sağlanan IP bilgilerini giriniz.

Modem den çıkan kablonuzu firewall üzerinde E0'a takılı olduğuna emin olunuz, modemden switch'inize hiçbir kablo bağlı olmaması gerekmektedir.

Örn: Modem IP adresiniz 192.168.2.1 ise firewallunuza Ip adres kısmına 192.168.2.2 yazabilirsiniz.

Not: (Verdiğiniz IP adresinin kullanılmadığından emin olunuz)

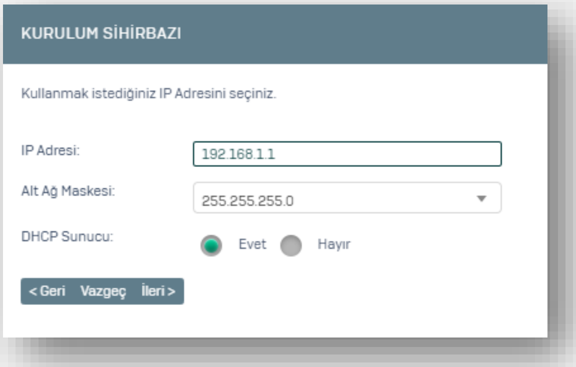
Varsayılan Ağ geçidiniz xDSL kullanıyor iseniz modeminizin IP adresidir.

DNS sunucusu 1 ve 2 kısmına Google DNS serverlarını yazabilirsiniz. (8.8.8.8 ve 8.8.4.4) ya da modeminizin IP adresini yazabilirsiniz.

IP Adres:	192.168.3.100
Alt Ağ Maskesi	255.255.255.0 (Örn: 255.255.255.0)
Varsayılan Ağ Geçidi	192.168.3.1
DNS Sunucusu 1	8.8.8.8
DNS Sunucusu 2	8.8.4.4
Firewall Adı	test (opsiyonel)
Domain İsmi	firmem.local (örneğin: firmam.local)

- In the IP Address section, we enter the IP address 192.168.2.200 that we want the modem to give to the firewall device,
- If there is no special subnet mask, we enter 255.255.255.0,
- Defaultgateway is Modem/Router IP address, we set this IP address because we set our modem to 192.168.3.1,
- We add Türk Telekom servers to the DNS servers section (195.175.39.39, 195175.39.40), you can also write your modem or a different dns server (for example: 8.8.8.8 / 8.8.4.4)
- You can make a definition in the domain name section without using Turkish characters, (eg:firmam.local)

On the next screen we will set up our local network.



KURULUM SİHİRBAZI

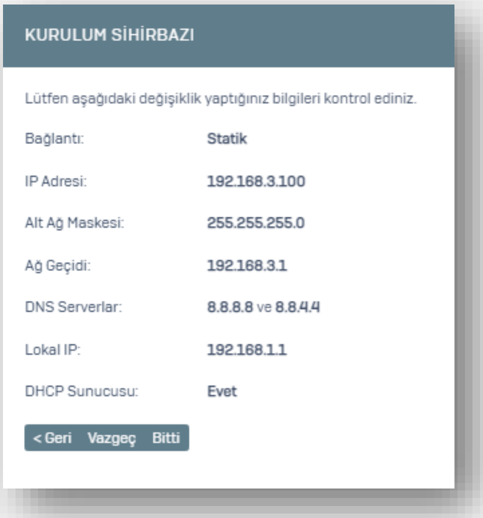
Kullanmak istediğiniz IP Adresini seçiniz.

IP Adresi: 192.168.1.1

Alt Ağ Maskesi: 255.255.255.0

DHCP Sunucu: ● Evet ○ Hayır

- In the IP address section, we define the IP address 192.168.1.1 that we want to give to the Firewall (The Firewall interface will now be accessed from the IP address http://192.168.1.1:8400),
- Subnet Mask should remain 255.255.255.0 if there is no special case,
- DHCPservice is active by default, if another DHCP server will distribute your IP address or if you do not want to run this service, you can continue the installation by saying no,
- After defining the time zone, you can check your settings again in the window that opens by clicking the "done" button and you can make your new settings active by clicking the finished button.



KURULUM SİHİRBAZI

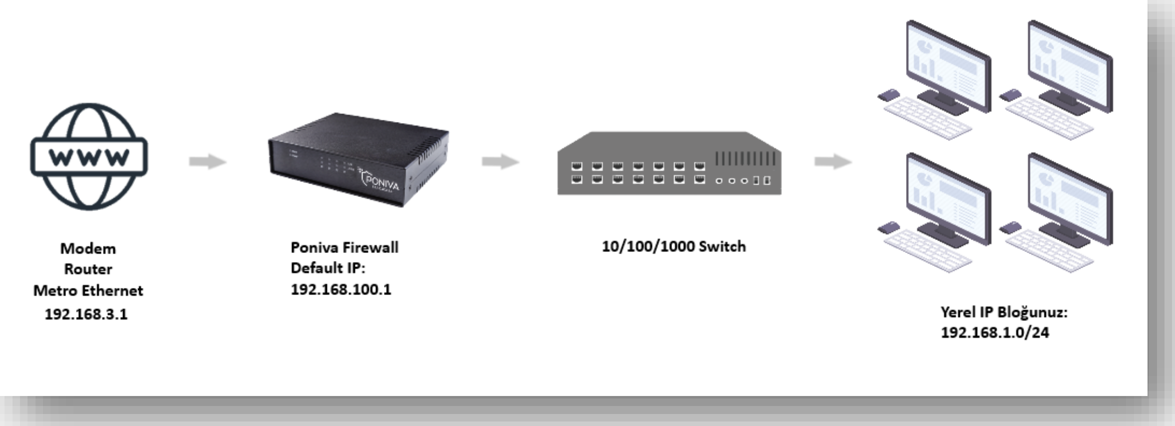
Lütfen aşağıdaki değişiklik yaptığınız bilgileri kontrol ediniz.

Bağlantı:	Statik
IP Adresi:	192.168.3.100
Alt Ağ Maskesi:	255.255.255.0
Ağ Geçidi:	192.168.3.1
DNS Serverlar:	8.8.8.8 ve 8.8.4.4
Lokal IP:	192.168.1.1
DHCP Sunucusu:	Evet

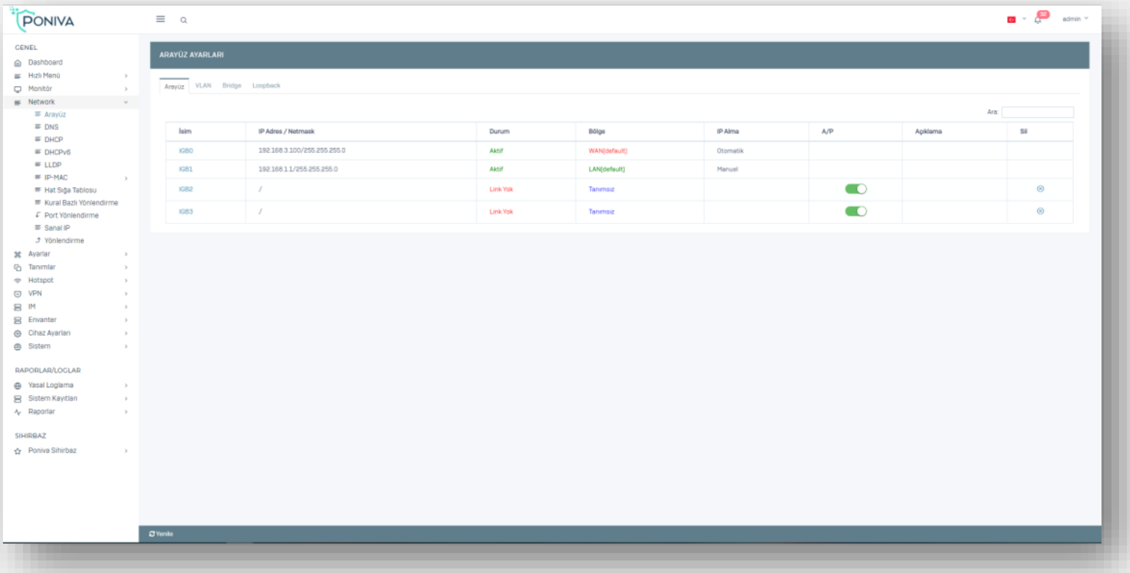
Your installation settings are complete, you need to restart the device.

MANUAL INSTALLATİON

It will continue assuming your local network is 192.168.1.0/24 and the modem IP address is 192.168.3.1.



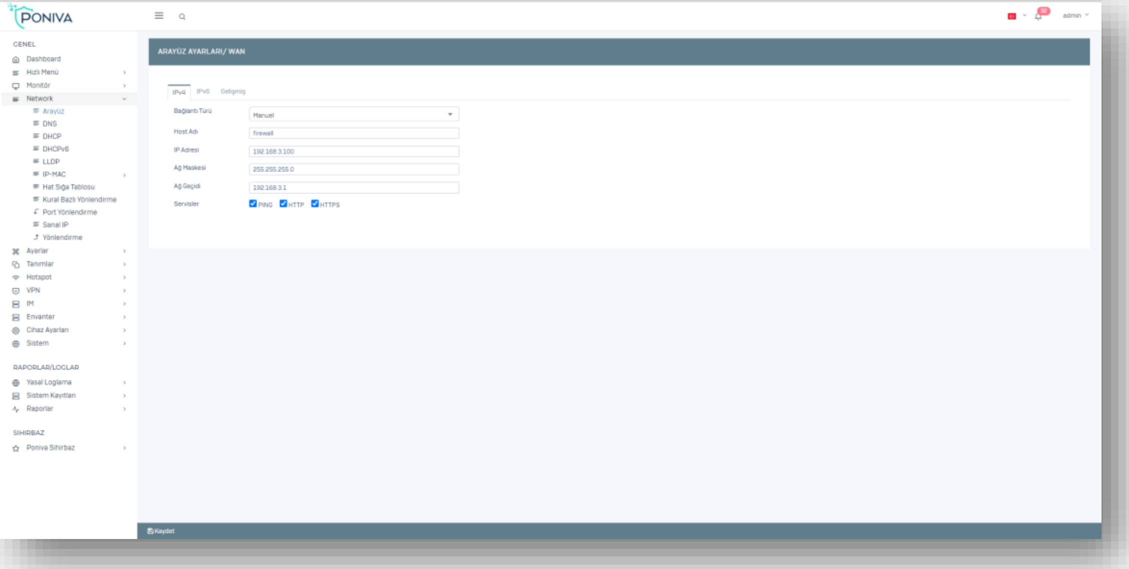
Network -> Interface Click on the menu.



ARAYÜZ AYARLARI

İsim	IP Adres / Netmask	Durum	Bölge	IP Alma	A/P	Açıklama	Sil
IGB0	192.168.3.100/255.255.255.0	Aktif	WAN(default)	Otomatik			
IGB1	192.168.1.1/255.255.255.0	Aktif	LAN(default)	Manuel			
IGB2	/	Link Yok	Tanımsız		●		⊗
IGB3	/	Link Yok	Tanımsız		●		⊗

In the window that opens, IGB0 Clicking on (Default WAN interface) we start configuring its settings.



ARAYÜZ AYARLARI/ WAN

Bağlantı Türü: Manuel

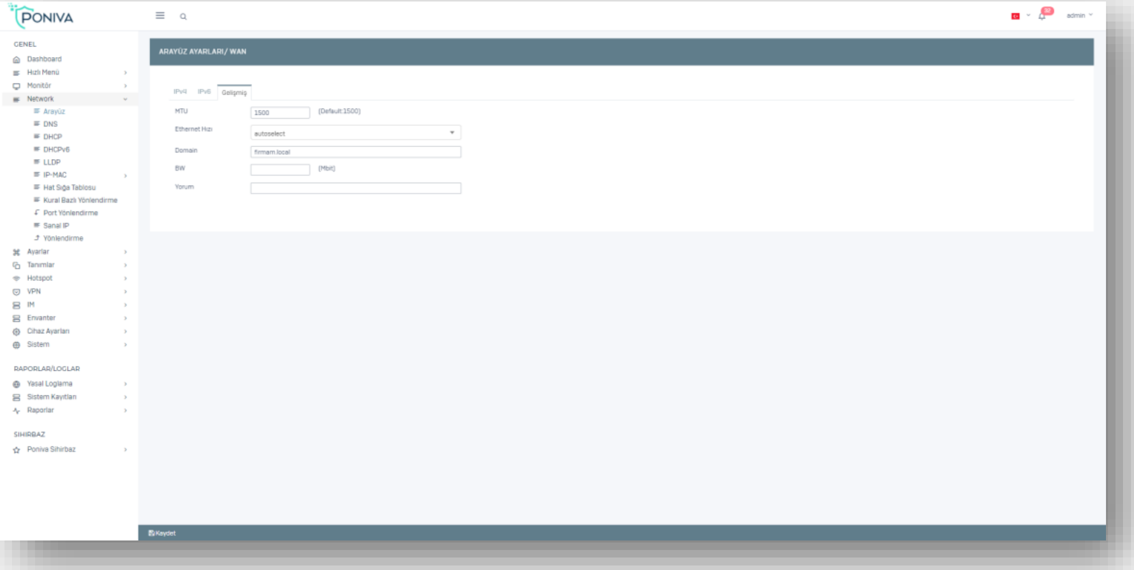
Host Adı: firewall

IP Adresi: 192.168.3.100

Ağ Maskesi: 255.255.255.0

Ağ Geçidi: 192.168.3.1

Servisler: ☑ PING ☑ HTTP ☑ HTTPS



ARAYÜZ AYARLARI/ WAN

MTU: 1500 (Default:1500)

Ethernet Hızı: autoselect

Domain: firmam.local

BW: (Mbit)

Yorum:

In the network section,

- IP type of connection We choose PPPOE for automatic, manual or bridge mode definition of our address,
- Enter 192.168.2.200 in the IP Address section.(You can define an IP except 192.168.3.1.),
- If there is no special subnet mask, we enter 255.255.255.0,
- DefaultThe gateway is the Modem/Router IP address, since we set our modem to 192.168.3.1, we enter the modem IP address here.

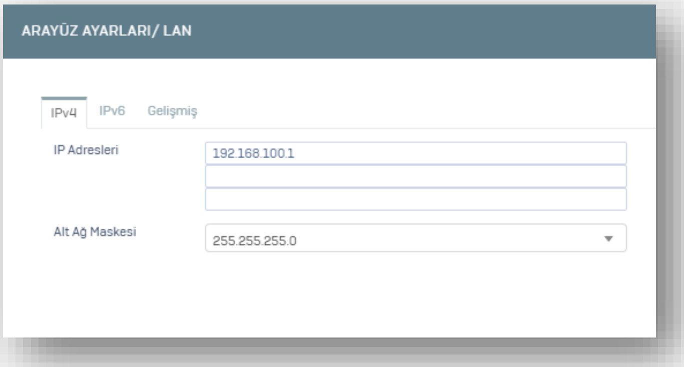
Clicking on the Advanced section;

- You can make a definition in the domain name section without using Turkish characters. (eg:firm.local)
- Its MTU value remains at 1500. (For DSL lines, the MTU value should be 1492.),
- Save we exit this screen.

Our Network WAN settings are complete.

Now it's time to configure our local network, IGB1 Clicking on (Default LAN interface) we start configuring its settings.

]



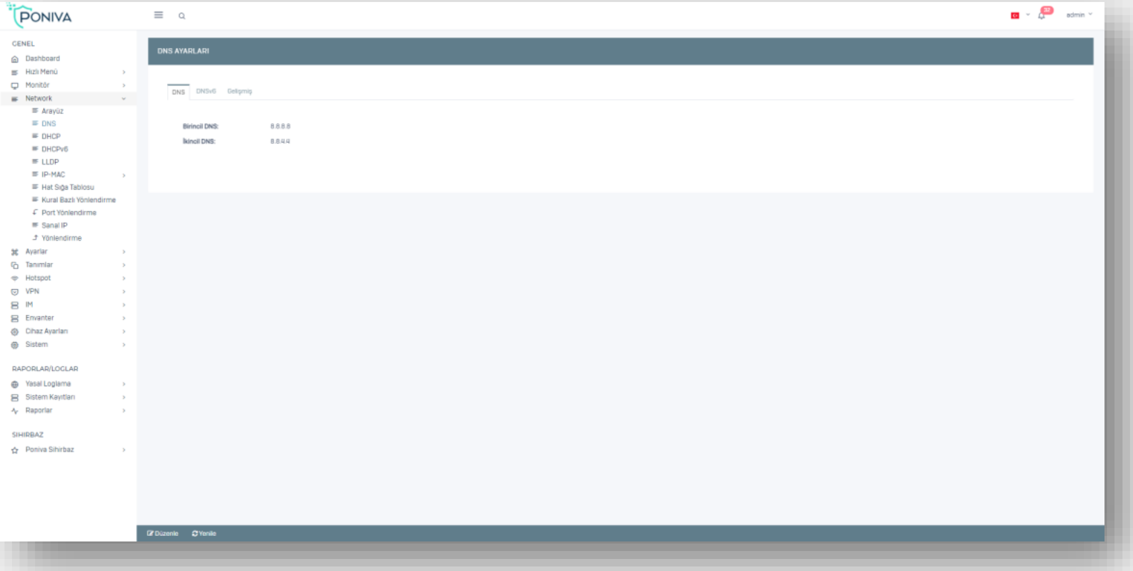
ARAYÜZ AYARLARI / LAN

IP Adresleri	192.168.100.1
Alt Ağ Maskesi	255.255.255.0

- The old IP of our modemSince the address is 192.168.1.1, we change the place where it says 192.168.100.1 to 192.168.1.1,
- The subnet mask should remain as 255.255.255.0 if there is no special case,
- DHCPYou can activate the service, if another DHCP server will distribute your IP address or if you do not want to run this service, you can leave it passive,
- Save we exit this screen.

Our Network LAN settings are complete.

Network -> DNS We start configuring DNS settings by clicking on the menu.



DNS AYARLARI

Birincil DNS:	8.8.8.8
İkincil DNS:	8.8.4.4

- In the DNS servers section, you can write Türk Telekom servers (195.175.39.39,195175.39.40), your modem or a different DNS server. (For example; 8.8.8.8 / 8.8.4.4)

Our DNS settings are complete.

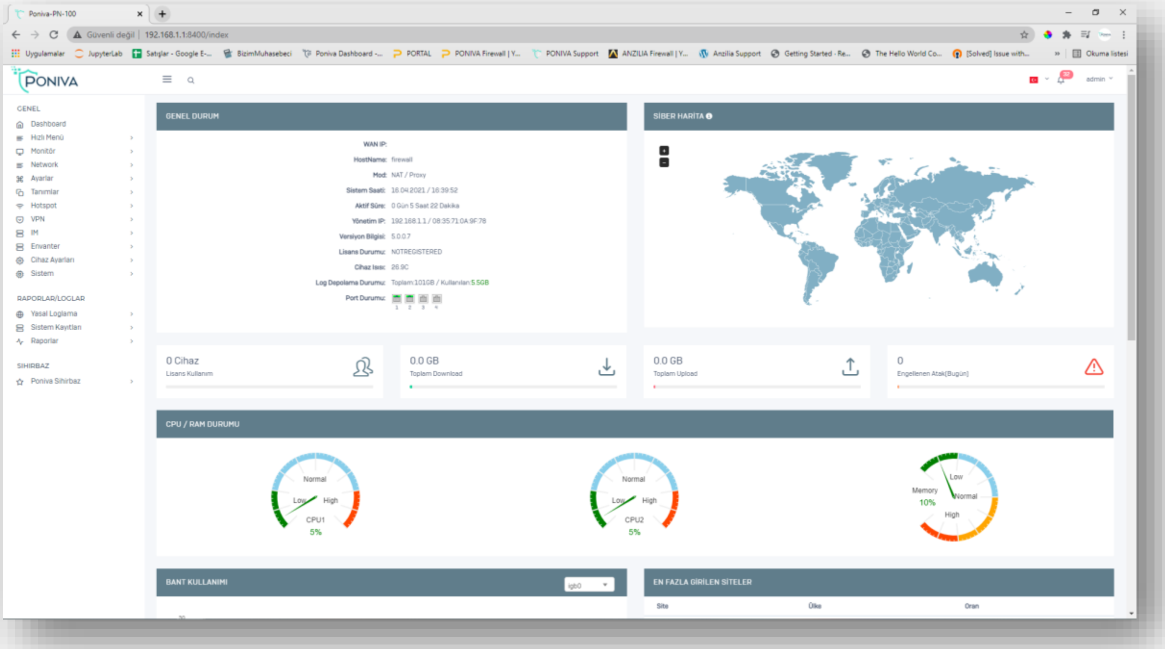
Network -> Routing By clicking on the menu, we start configuring the Forwarding settings.

- Here, Default value should write modem/Router or PPPOE gateway IP address.

Our forwarding settings are complete.

ifIf there is no problem in our definitions, after restarting the device, the firewall's internet will be active.

Now we can access the interface by typing our new IP address (http://192.168.1.1:8400).



WAN IP:
HostName: firewall
Mod: NAT / Proxy
Sistem Saati: 16.04.2021 / 16:39:52
Aktif Süre: 0 Gün 5 Saat 22 Dakika
Yönetim IP: 192.168.1.1 / 08:35:71:0A:9F:78
Versiyon Bilgisi: 5.0.0.7
Lisans Durumu: NOTREGISTERED
Cihaz Isısı: 26.9C
Log Depolama Durumu: Toplam:101GB / Kullanılan:5.5GB
Port Durumu: 1 2 3 4

0 Cihaz
Lisans Kullanım

0.0 GB
Toplam Download

0.0 GB
Toplam Upload

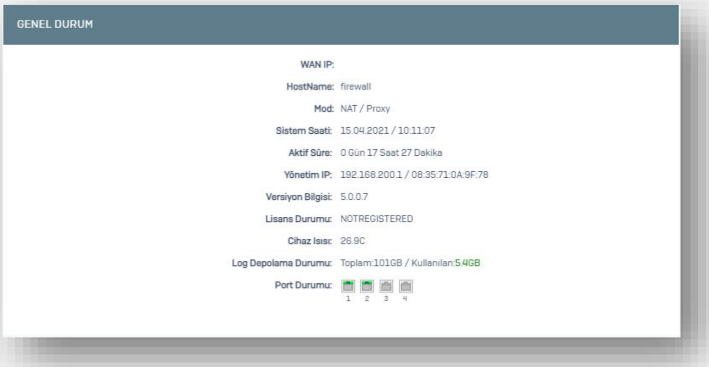
0
Engellenen Atak[Bugün]

Site	Ülke	Oran

DASHBOARD

General situation

System information about the device; You can view information such as version, license, disk storage, active ports.

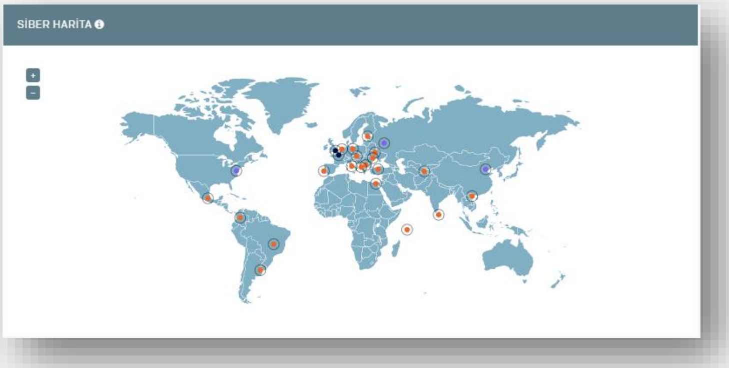


GENEL DURUM

WAN IP:
HostName: firewall
Mod: NAT / Proxy
Sistem Saati: 15.04.2021 / 10:11:07
Aktif Süre: 0 Gün 17 Saat 27 Dakika
Yönetim IP: 192.168.200.1 / 08:35:71:0A:9F:78
Versiyon Bilgisi: 5.0.0.7
Lisans Durumu: NOTREGISTERED
Cihaz Isısı: 26.9C
Log Depolama Durumu: Toplam:101GB / Kullanılan:5.4GB
Port Durumu: 1 2 3 4

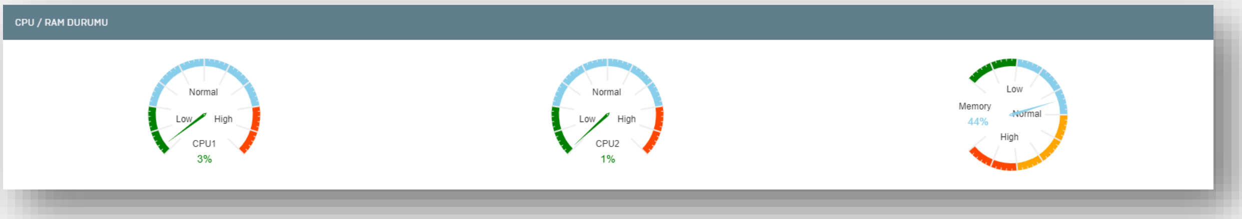
Cyber Map

You can view which countries the attacks (daily) are coming from. You can also view the number of countries and attacks in the last 30 days by clicking on the Info icon.



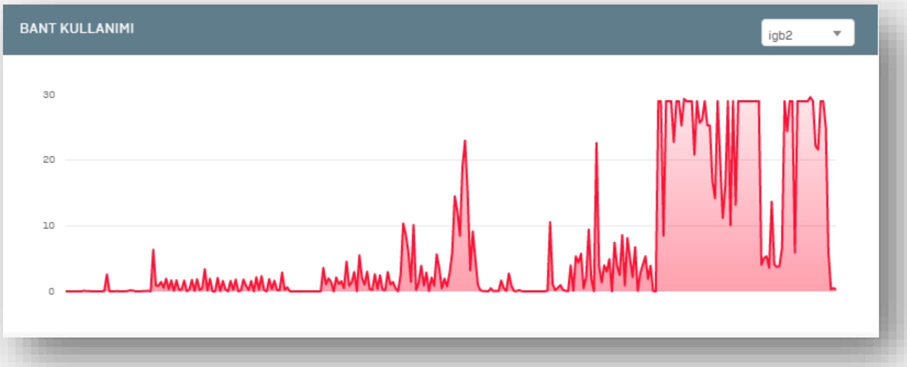
CPU/RAM Status

You can view the processor and memory status of the device.



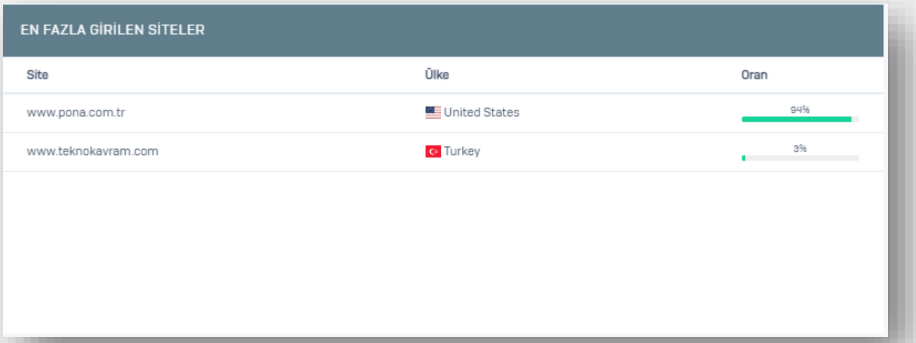
Tape Usage

You can instantly observe the bandwidth traffic passing through the igb2 port below. (You can also selectively examine your other active ports.)



Most Visited Sites

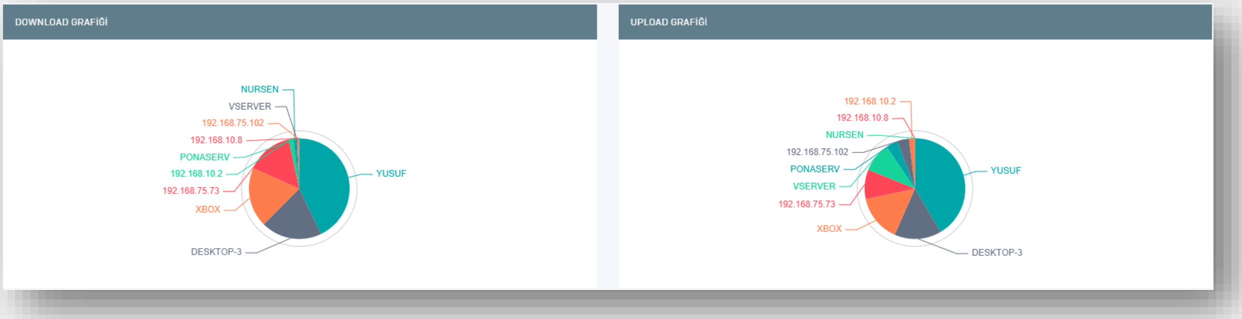
You can view the most visited websites here.


EN FAZLA GİRİLEN SİTELER

Site	Ülke	Oran
www.pona.com.tr	United States	94%
www.teknokavram.com	Turkey	3%

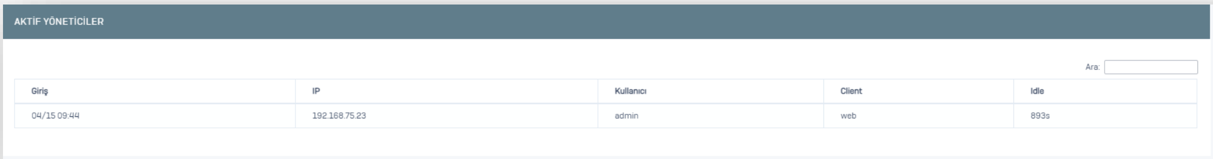
Download/Upload Graphics

You can also view the download/upload information of the people in your local network as IP or name if defined.



Active Managers

You can view the active users in the device interface.



AKTİF YÖNETİCİLER

Ara:

Giriş	IP	Kullanıcı	Client	Idle
04/15 09:44	192.168.75.23	admin	web	893s

MONITOR

NETWORK

MENU	EXPLANATION
Instant Line Usage	You can view the band usage graph of your lines.
Active Devices	You can view your active devices.
Active Links	You can view the connections in your network and terminate the connections you want.
User Chart	You can view the download/upload graphics of all users.
DHCP Devices	You can view the devices that receive IP in the DHCP list.
LLDP Status	You can view the list of devices available in your local network.
Network Status	You can view the download and upload graphics of all users.
Route Table	
ARP Table	You can view the IP and MAC addresses of Active Devices.
IPv6 Neighbor List	You can view the IPv6 list.

VPN

MENU	EXPLANATION
SSL VPN User	You can view your active SSL VPN user list.
L2TP/PPTP User	You can view your active L2TP/PPTP user list.
IPSEC VPN	You can view your active IPSEC connection list.

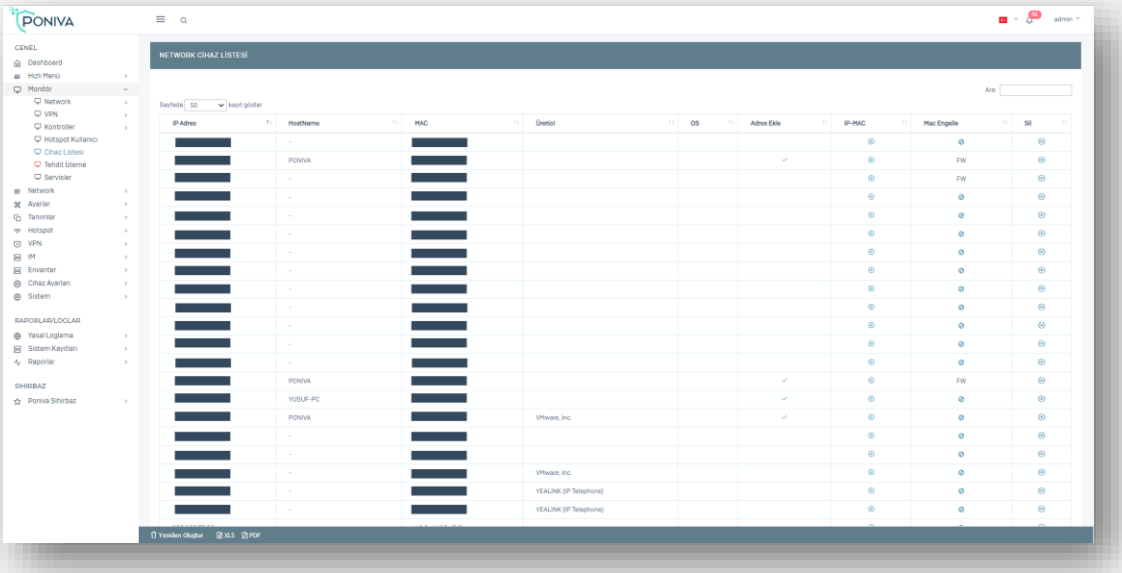
CONTROLS

MENU	EXPLANATION
Domain	Shows the domain category list. For example, you can list which categories the youtube.com domain is in.
User	You can check which group the user is in or whether youtube.com is banned for that user.
network	You can view the connections in your network and terminate the connections you want.

HOTSPOT USER

You can view the active Hotspot user list.

DEVICE LIST



NETWORK CİHAZ LİSTESİ

Sayfada 50 kayıt göster

Ara:

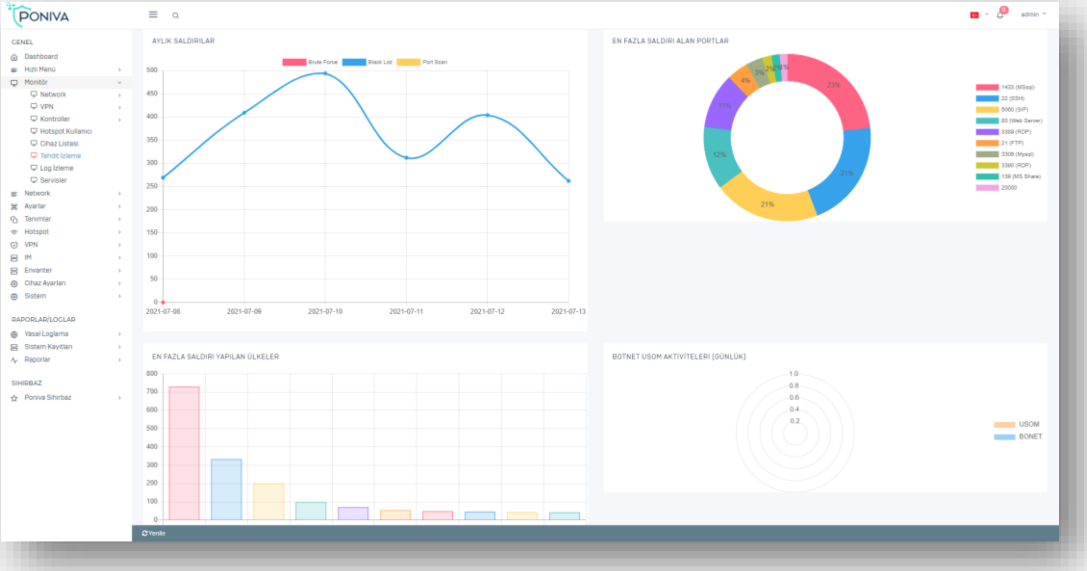
IP Adres	HostName	MAC	Üretici	OS	Adres Ekle	IP-MAC	Mac Engelle	Sil
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	PONIVA	[redacted]			✓	⊕	FW	⊗
[redacted]	-	[redacted]				⊕	FW	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	PONIVA	[redacted]			✓	⊕	FW	⊗
[redacted]	YUSUF-PC	[redacted]			✓	⊕	⊘	⊗
[redacted]	PONIVA	[redacted]	VMware, Inc.		✓	⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]				⊕	⊘	⊗
[redacted]	-	[redacted]	VMware, Inc.			⊕	⊘	⊗
[redacted]	-	[redacted]	YEALINK (IP Telephone)			⊕	⊘	⊗
[redacted]	-	[redacted]	YEALINK (IP Telephone)			⊕	⊘	⊗

	EXPLANATION

IP Address	IP list connected to the firewall device.
Hostname	Hostname list connected to the firewall device.
Match	List of Macs connected to the firewall device.
Producer	List of Manufacturers connected to the firewall device.
OS	List of OS connected to firewall device.
Add Address	You can define the Hostname, IP and Mac Address in the Device List in the Defines->Addresses menu.
IP-MAC	You can define the IP and MAC Address in the Device List in the Network->IP-MAC menu.
Mac Block	You can define the MAC Address in the Device List in the Settings->Mac Block menu.

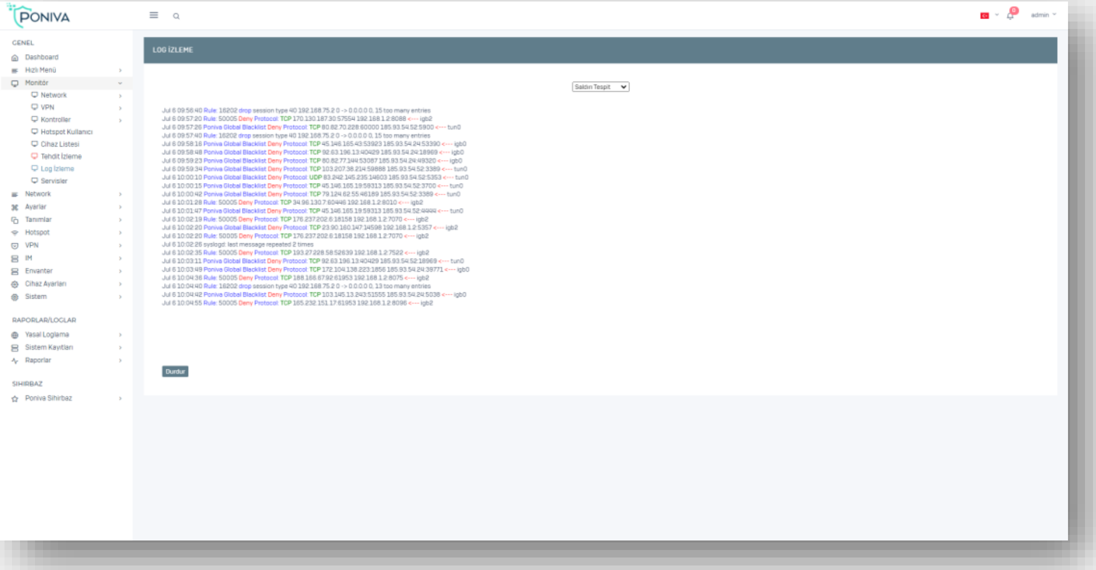
THREAT MONITORING

You can learn more about attacks in the threat watch menu. You can view the monthly attacks, the most attacked ports, or the IP addresses in the attack table.



LOG VIEWER

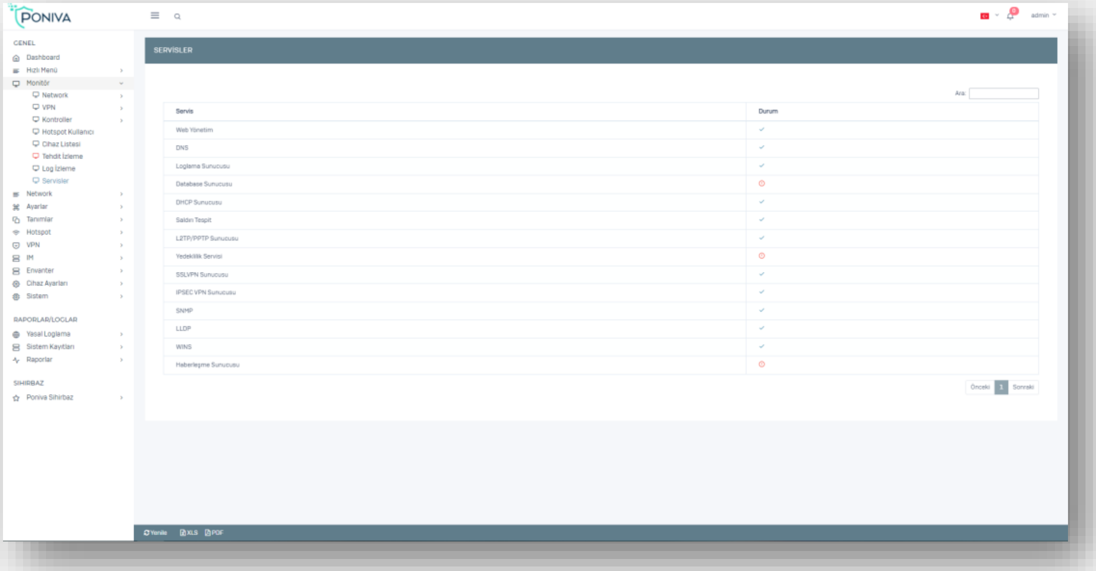
You can view your logs live.



```
Jul 6 09:56:40 Rule: 16202 drop session type 40 192.168.75.2 0 -> 0.0.0.0 0, 15 too many entries
Jul 6 09:57:20 Rule: 50005 Deny Protocol: TCP 170.130.187.30:57554 192.168.1.2:8088 <--- igb2
Jul 6 09:57:26 Poniva Global Blacklist Deny Protocol: TCP 80.82.70.228:60000 185.93.54.52:5900 <--- tun0
Jul 6 09:57:40 Rule: 16202 drop session type 40 192.168.75.2 0 -> 0.0.0.0 0, 15 too many entries
Jul 6 09:58:16 Poniva Global Blacklist Deny Protocol: TCP 45.146.165.43:53923 185.93.54.24:53390 <--- igb0
Jul 6 09:58:48 Poniva Global Blacklist Deny Protocol: TCP 92.63.196.13:40429 185.93.54.24:18969 <--- igb0
Jul 6 09:59:23 Poniva Global Blacklist Deny Protocol: TCP 80.82.77.144:53087 185.93.54.24:49320 <--- igb0
Jul 6 09:59:34 Poniva Global Blacklist Deny Protocol: TCP 103.207.38.214:59888 185.93.54.52:3389 <--- tun0
Jul 6 10:00:10 Poniva Global Blacklist Deny Protocol: UDP 83.242.145.235:14603 185.93.54.52:5353 <--- tun0
Jul 6 10:00:15 Poniva Global Blacklist Deny Protocol: TCP 45.146.165.19:59313 185.93.54.52:3700 <--- tun0
Jul 6 10:00:42 Poniva Global Blacklist Deny Protocol: TCP 79.124.62.55:46189 185.93.54.52:3389 <--- tun0
Jul 6 10:01:28 Rule: 50005 Deny Protocol: TCP 34.96.130.7:60446 192.168.1.2:8010 <--- igb2
Jul 6 10:01:47 Poniva Global Blacklist Deny Protocol: TCP 45.146.165.19:59313 185.93.54.52:4444 <--- tun0
Jul 6 10:02:19 Rule: 50005 Deny Protocol: TCP 176.237.202.6:18158 192.168.1.2:7070 <--- igb2
Jul 6 10:02:20 Poniva Global Blacklist Deny Protocol: TCP 23.90.160.147:14598 192.168.1.2:5357 <--- igb2
Jul 6 10:02:20 Rule: 50005 Deny Protocol: TCP 176.237.202.6:18158 192.168.1.2:7070 <--- igb2
Jul 6 10:02:26 syslogd: last message repeated 2 times
Jul 6 10:02:35 Rule: 50005 Deny Protocol: TCP 193.27.228.58:52639 192.168.1.2:7522 <--- igb2
Jul 6 10:03:11 Poniva Global Blacklist Deny Protocol: TCP 92.63.196.13:40429 185.93.54.52:18969 <--- tun0
Jul 6 10:03:49 Poniva Global Blacklist Deny Protocol: TCP 172.104.138.223:1856 185.93.54.24:39771 <--- igb0
Jul 6 10:04:36 Rule: 50005 Deny Protocol: TCP 188.166.67.92:61953 192.168.1.2:8075 <--- igb2
Jul 6 10:04:40 Rule: 16202 drop session type 40 192.168.75.2 0 -> 0.0.0.0 0, 13 too many entries
Jul 6 10:04:42 Poniva Global Blacklist Deny Protocol: TCP 103.145.13.243:51555 185.93.54.24:5038 <--- igb0
Jul 6 10:04:55 Rule: 50005 Deny Protocol: TCP 165.232.151.17:61953 192.168.1.2:8096 <--- igb2
```

SERVICES

You can view the service statuses.

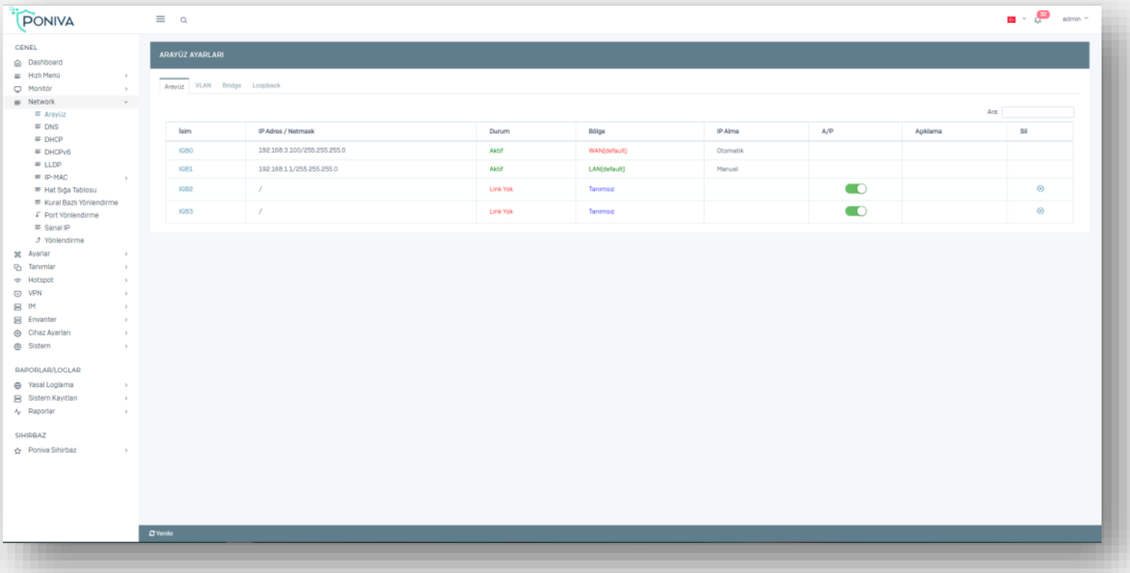


Servis	Durum
Web Yönetim	✓
DNS	✓
Loglama Sunucusu	✓
Database Sunucusu	⚠
DHCP Sunucusu	✓
Saldırı Tespit	✓
L2TP/PPTP Sunucusu	✓
Yedeklilik Servisi	⚠
SSLVPN Sunucusu	✓
IPSEC VPN Sunucusu	✓
SNMP	✓
LLDP	✓
WINS	✓
Haberleşme Sunucusu	⚠

NETWORK

INTERFACE

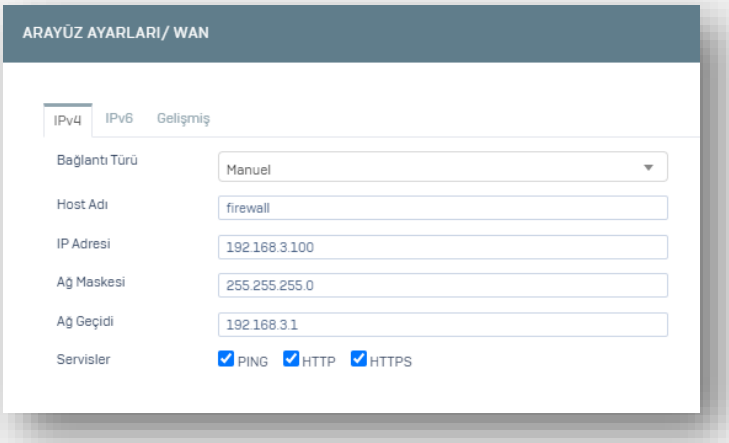
Ethernet (LAN, WAN and PPPOE) settings are defined in this section. You can define more than one LAN, WAN interface.



ARAYÜZ AYARLARI

İsim	IP Adres / Netmask	Durum	Bölge	IP Alma	A/P	Açıklama	Sil
IGB0	192.168.3.100/255.255.255.0	Aktif	WAN(default)	Otomatik			
IGB1	192.168.1.1/255.255.255.0	Aktif	LAN(default)	Manuel			
IGB2	/	Link Yok	Tanımsız		●		⊗
IGB3	/	Link Yok	Tanımsız		●		⊗

WAN Settings



ARAYÜZ AYARLARI/ WAN

Bağlantı Türü: Manuel

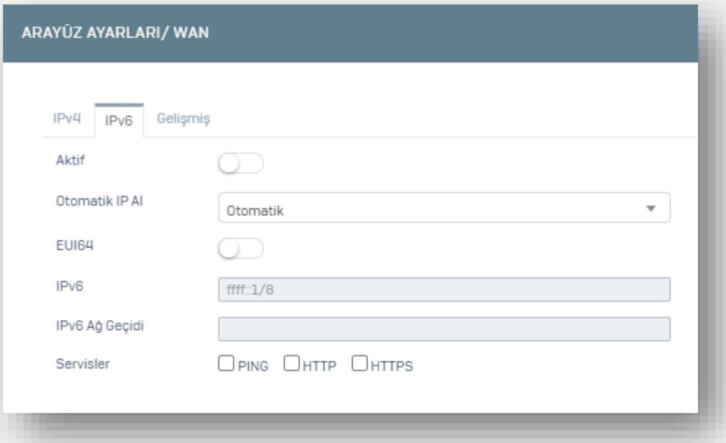
Host Adı: firewall

IP Adresi: 192.168.3.100

Ağ Maskesi: 255.255.255.0

Ağ Geçidi: 192.168.3.1

Servisler: ☑ PING ☑ HTTP ☑ HTTPS



ARAYÜZ AYARLARI/ WAN

Aktif: ○

Otomatik IP Al: Otomatik

EUI64: ○

IPv6: ffff::1/8

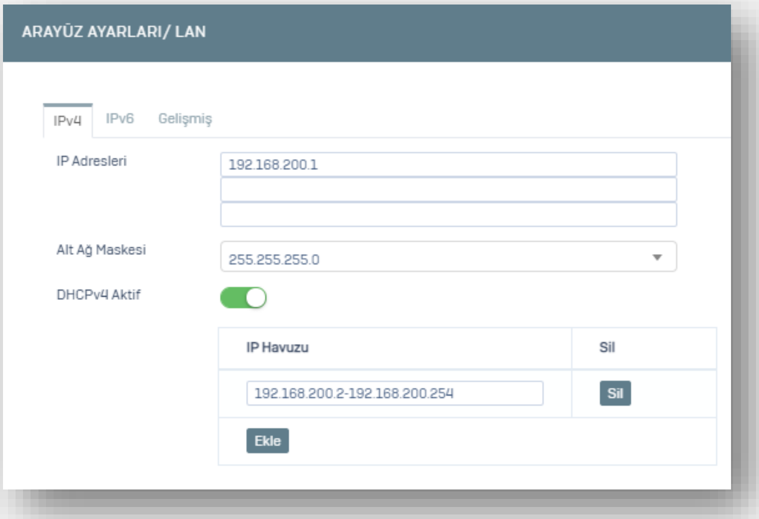
IPv6 Ağ Geçidi:

Servisler: □ PING □ HTTP □ HTTPS

	EXPLANATION
Connection Type	You must select a connection type.
Host Name	Default firewall
IP Address	Enter the IPv4 Address.
Netmask	Enter the netmask.
Gateway	You must enter the gateway.
Services	You can select the services you want to activate.
Active	You can enable IPv6.
Get IP Automatically	You can select Auto/Manual.
EUI64	When enabled, the Extended Unique Identifier places 16 bits in the middle of this 48-bit address to create a 64-bit Interface ID using the client's 48-bit Ethernet MAC address.
IPv6	You must enter an IPv6 address.
Gateway	You must enter the IPv6 Gateway.

Services	You can select the services you want to activate.

LAN Settings



ARAYÜZ AYARLARI/ LAN

IPv4 IPv6 Gelişmiş

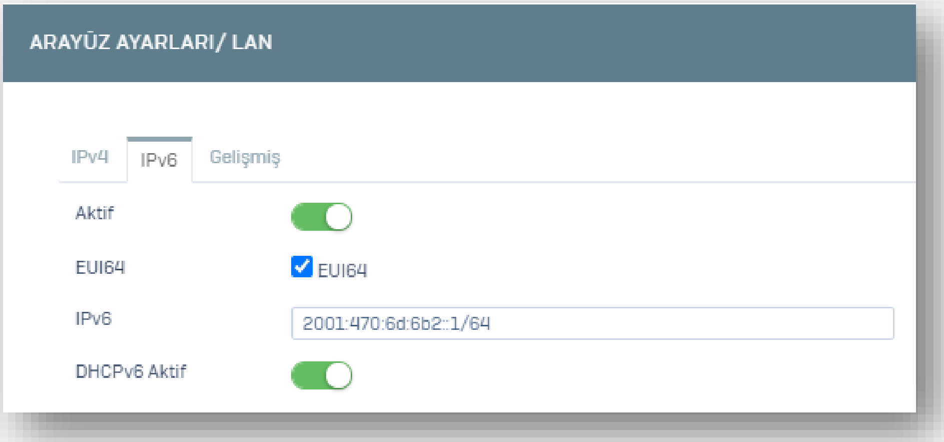
IP Adresleri: 192.168.200.1

Alt Ağ Maskesi: 255.255.255.0

DHCPv4 Aktif

IP Havuzu	Sil
192.168.200.2-192.168.200.254	Sil

Ekle



ARAYÜZ AYARLARI/ LAN

IPv4 IPv6 Gelişmiş

Aktif

EUI64: ☑ EUI64

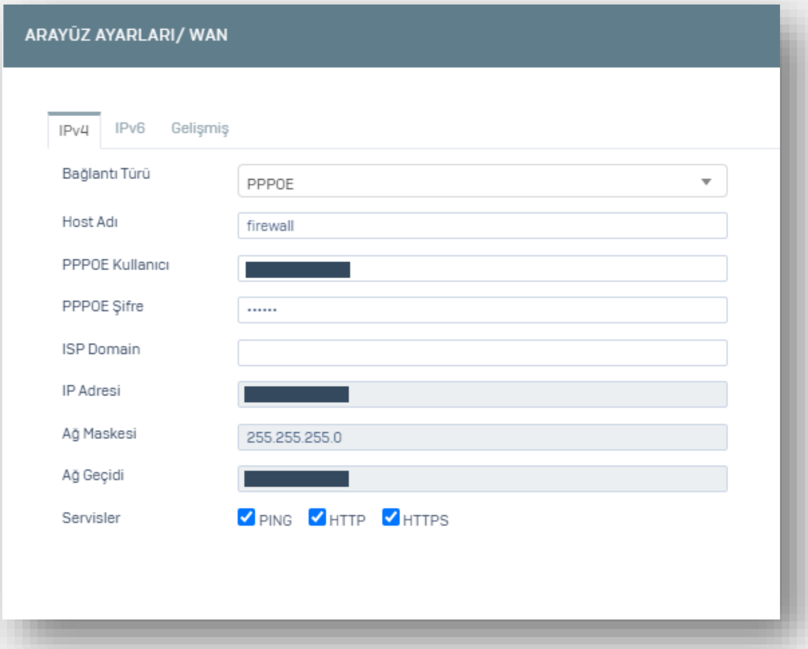
IPv6: 2001:470:6d:6b2::1/64

DHCPv6 Aktif

	EXPLANATION
IPv4 Addresses	You must enter an IPv4 address. You can define more than one IPv4 for access.
Subnet Mask	You must select a subnet mask.
DHCPv4 Active	You must choose whether to use DHCPv4.
Active	You can enable IPv6.
EUI64	When enabled, the Extended Unique Identifier places 16 bits in the middle of this 48-bit address to create a 64-bit Interface ID using the client's 48-bit Ethernet MAC address.

IPv6 Addresses	You must enter an IPv6 address.
DHCPv6 Active	You must choose whether to use DHCPv6.

PPPOE Settings



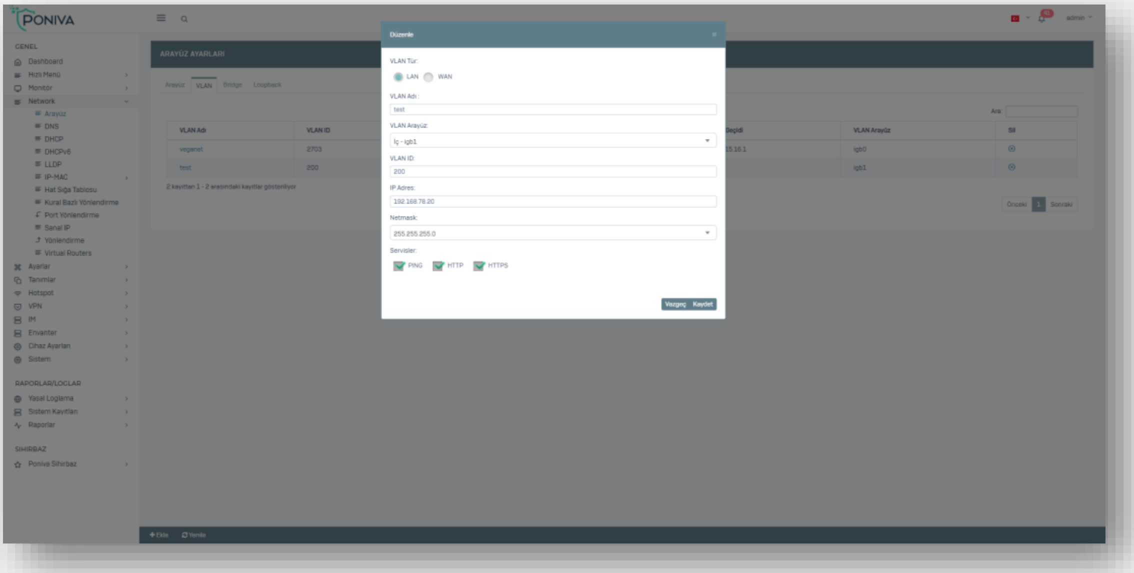
ARAYÜZ AYARLARI/ WAN

Bağlantı Türü	PPPOE
Host Adı	firewall
PPPOE Kullanıcı	[redacted]
PPPOE Şifre	••••••
ISP Domain	
IP Adresi	[redacted]
Ağ Maskesi	255.255.255.0
Ağ Geçidi	[redacted]
Servisler	☑ PING ☑ HTTP ☑ HTTPS

	EXPLANATION
Connection Type	You must choose PPPOE.
Host Name	Default firewall
PPPOE User	You must enter the user information given to you by your internet provider.
PPPOE Password	You must enter the password information given to you by your internet provider.
ISP Domain	-
IP Address	This section comes automatically.
Netmask	This section comes automatically.
Gateway	This section comes automatically.
Services	You can select the services you want to activate.

VLAN

If you want to create a virtual network behind your local network, you can define a vlan here. For example, you have a switch with vlan support and if you want to separate the networks inside, you can manage it by defining vlan.



Düzenle

VLAN Tür:

● LAN ○ WAN

VLAN Adı : test

VLAN Arayüz: İç - igb1

VLAN ID: 200

IP Adres: 192.168.78.20

Netmask: 255.255.255.0

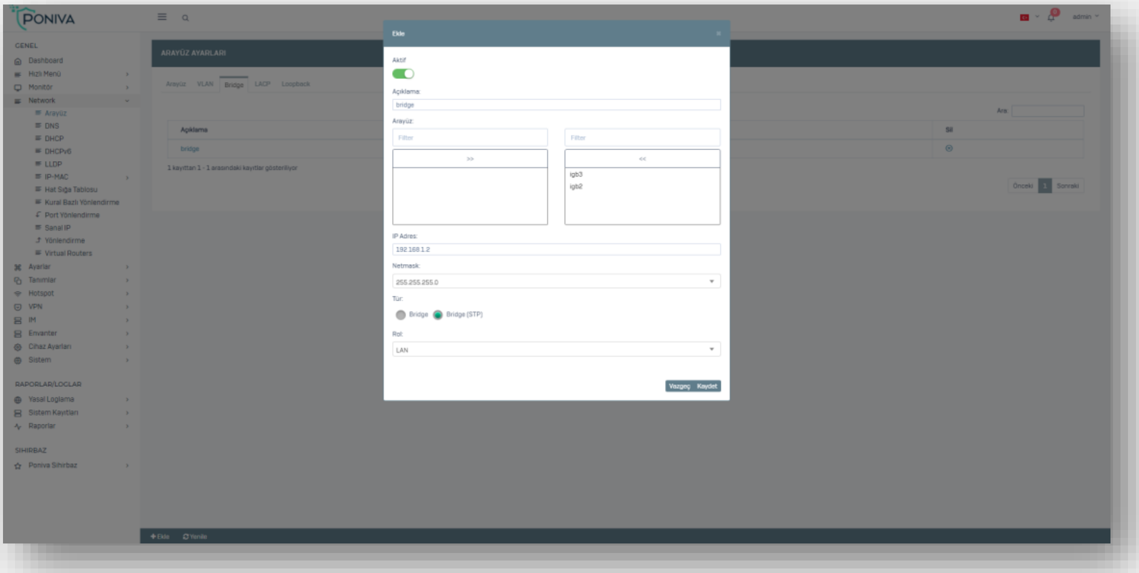
Servisler:

☑ PING ☑ HTTP ☑ HTTPS

	EXPLANATION
VLAN Type	You must select the VLAN type. (LAN/WAN)
VLAN Name	You must enter a VLAN name.
VLAN Interface	You must choose VLAN interface.
VLAN ID	You must enter the VLAN ID.
IP Address	You must enter the IP Address.
netmask	You must enter a netmask.
Gateway	You must enter the gateway.
NAT	-
Services	You can select the services you want to activate PING, HTTP, HTTPS.

Bridge

The bridge definition is the same as the switch logic. You can enable multiple ports to exit over a single IP.



Aktif

Açıklama: bridge

Arayüz:

Filter | Filter

igb3
igb2

IP Adres: 192.168.1.2

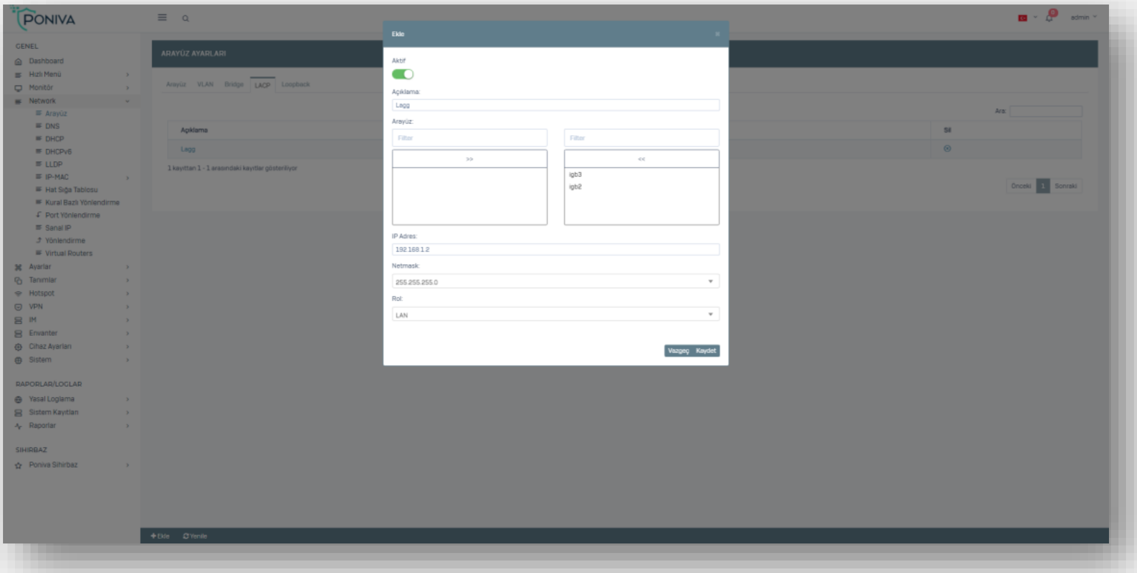
Netmask: 255.255.255.0

Tür: ○ Bridge ● Bridge (STP)

Rol: LAN

	EXPLANATION
Active	You can Active/Passive.
Description	You must enter a description.
Interface	You must choose at least two different interfaces.
IP Address	List of Macs connected to the firewall device.
netmask	You must enter a netmask. (Default: 255.255.255.0)
Kind	Bridge/Bridge(STP)
Role	LAN/WAN

LACP



Ekle

Aktif

Açıklama: Lagg

Arayüz:

Filter | Filter

>> | <<

igb3
igb2

IP Adres: 192.168.1.2

Netmask: 255.255.255.0

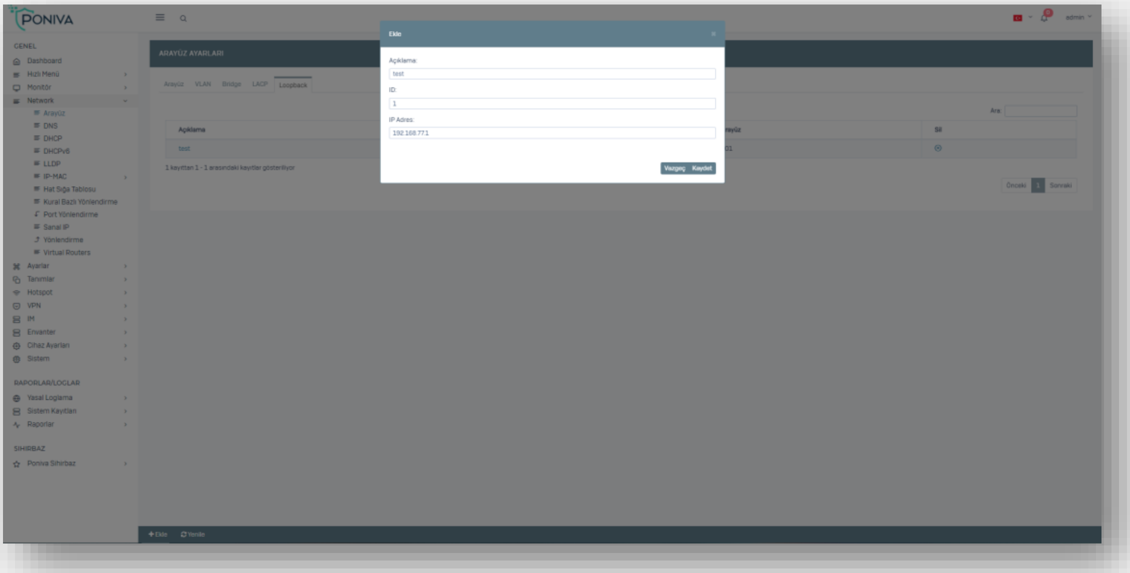
Rol: LAN

Vazgeç Kaydet

	EXPLANATION
Active	You can Active/Passive.
Description	You must enter a description.
Interface	You must choose at least two different interfaces.
IP Address	List of Macs connected to the firewall device.
netmask	You must enter a netmask. (Default: 255.255.255.0)
Role	LAN/WAN

Loopback

You can define loopback to create a local Ethernet within yourself.



Ekle

Açıklama: test

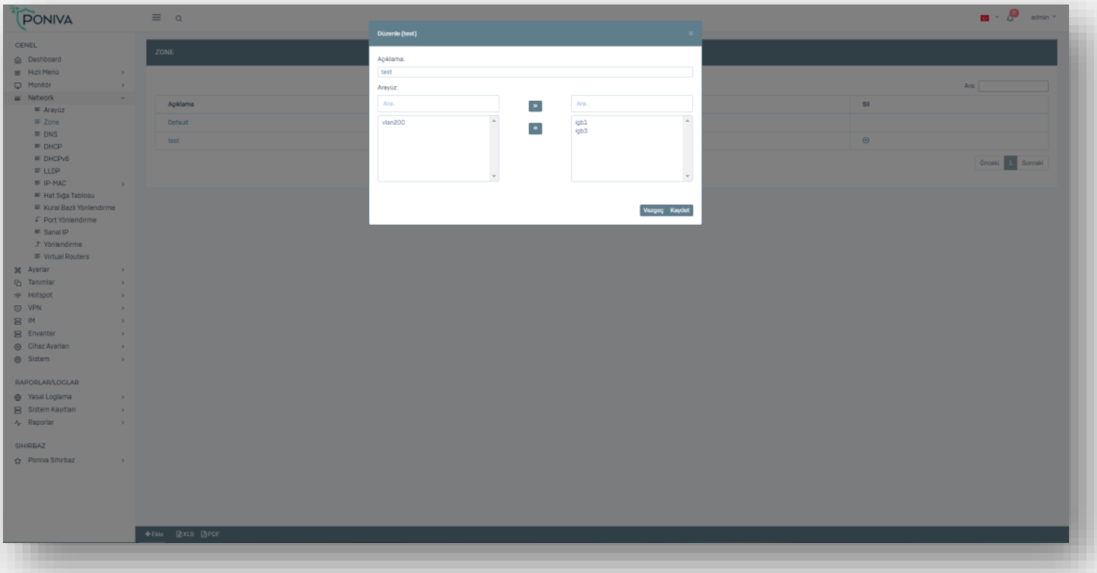
ID: 1

IP Adres: 192.168.77.1

	EXPLANATION
Description	You must enter a description.
ID	You must enter a value between 1-50.
IP Address	You must enter an IP address.

ZONE

You can group physical and virtual interfaces to control traffic passing through specific interfaces in your network.



Düzenle (test)

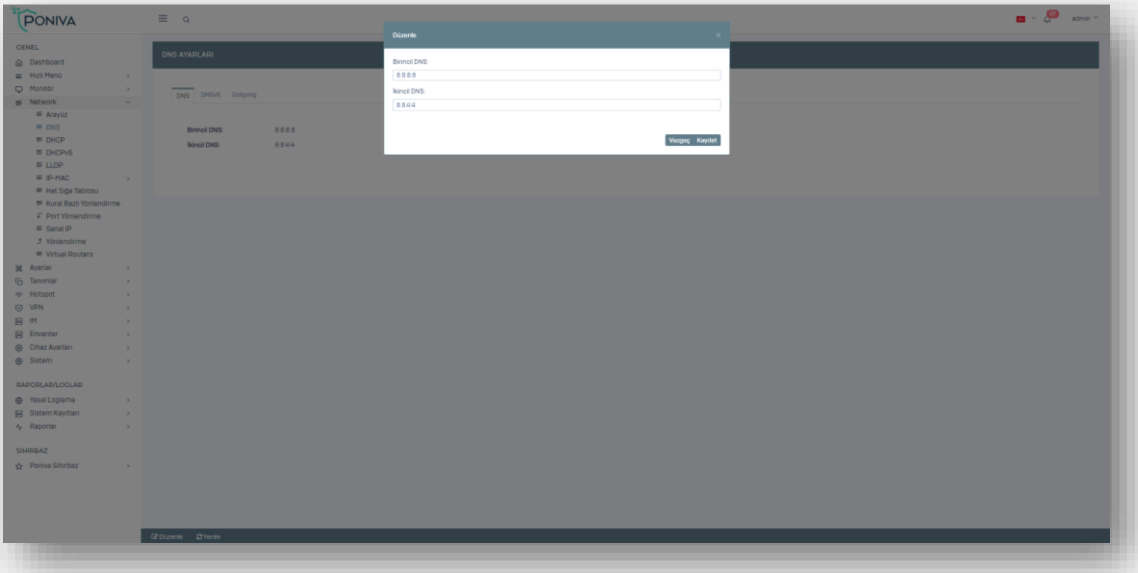
Açıklama: test

Arayüz:

vlan200

igb1
igb3

DNS



Birincil DNS: 8.8.8.8

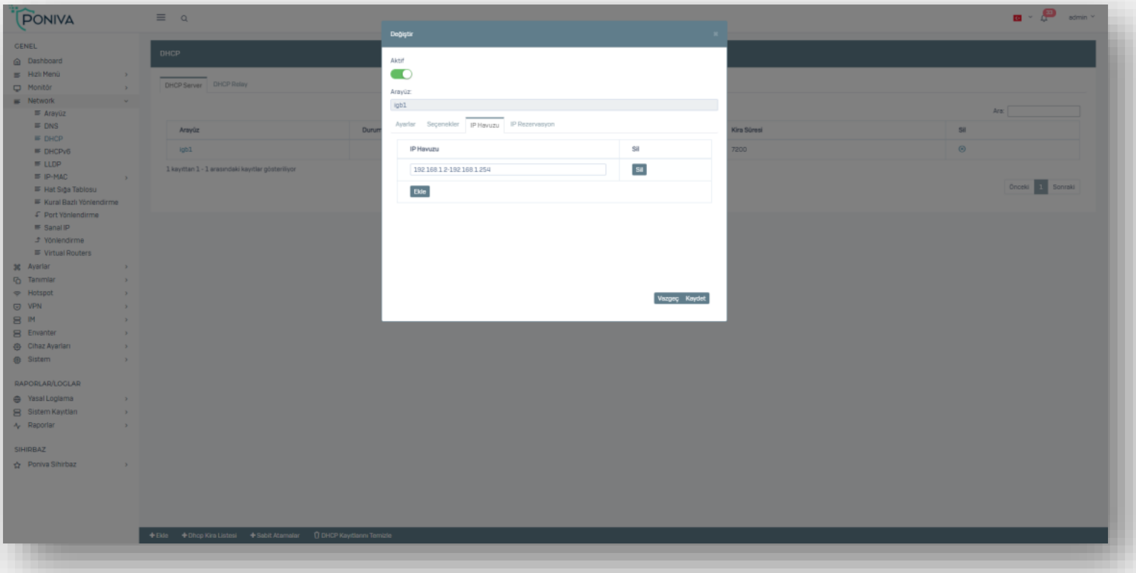
İkincil DNS: 8.8.4.4

	EXPLANATION
Primary DNS	The default is 8.8.8.8 (your modem or differentyou can also write a dns server.)
Secondary DNS	Default 8.8.4.4 (your modem or differentyou can also write a dns server.)
Don't Update DNS with PPPOE	When activated, DNS is not automatically updated.

DHCP

DHCP Server

DHCPv4 settings used in the system are configured in this section.



Aktif: ●

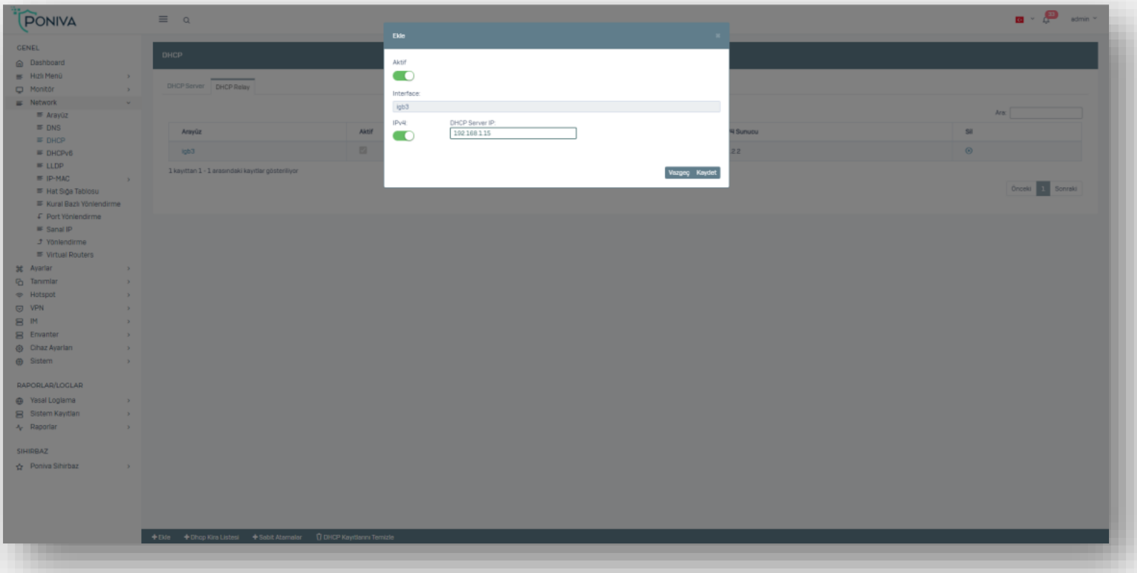
Arayüz: igb1

IP Havuzu	Sil
192.168.1.2-192.168.1.254	Sil

	EXPLANATION
Interface	You must choose the interface.
Pingle While Distributing IP	When it is activated, it checks whether that IP is used by pinging while distributing an IP.
Distribute IP Only to Defined Devices	When activated, no device can get IP except reservation.
Rental Period	It is the validity period of the distributed IP addresses.
Subnet	The default 'use firewall' option is active.
Gateway	The default 'use firewall' option is active.
WINS	The default 'use firewall' option is active.
DNS Suffix	The default 'use firewall' option is active.
DNS	The default 'use firewall' option is active.
IP Pool	You must enter a DHCP IP range. You can add multiple IP ranges.
IP Reservation	You can define the IPs you want to reserve in DHCP.
Network Scanning	Lists the devices found in your local network.

DHCP Relay

If you want to provide IP distribution from a different DHCP Server, you can do so by adding a new DHCP Relay definition.



Arayüz	Aktif	…N Sunucu	Sil
igb3	☑	…2.2	

1 kayıttan 1 - 1 arasındaki kayıtlar gösteriliyor

Ekle

Aktif: ●

Interface: igb3

IPv4: ●

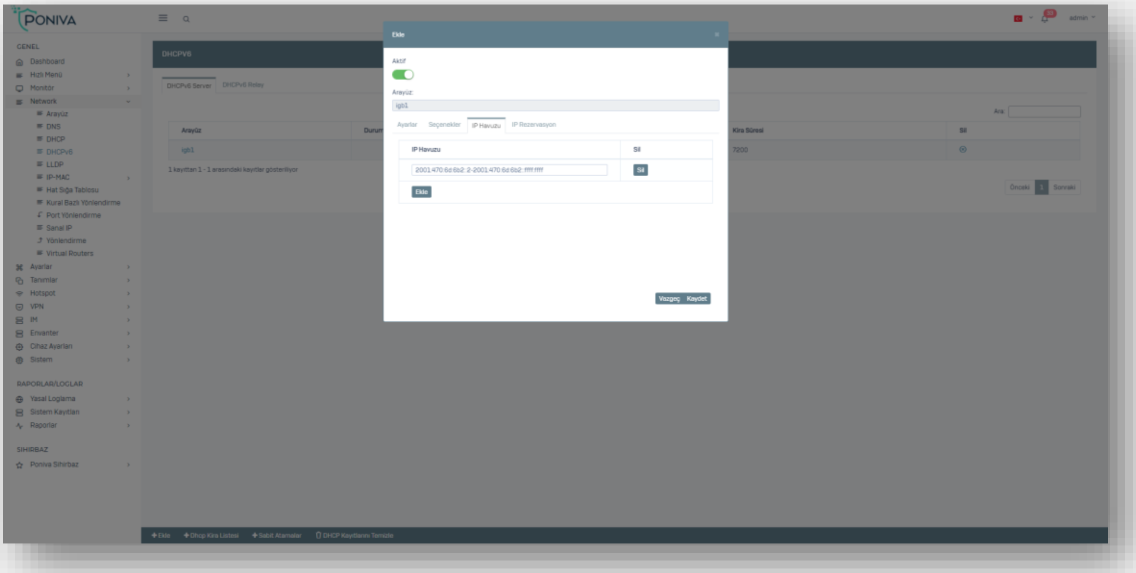
DHCP Server IP: 192.168.1.15

	EXPLANATION
Interface	You must choose the interface.
IPv4	You must enter your DHCP Server IP address.

DHCPV6

Dhcpv6 Server

DHCPv6 settings used in the system are configured in this section.



Aktif: ●

Arayüz: igb1

IP Havuzu	Sil
2001:470:6d:6b2::2-2001:470:6d:6b2::ffff:ffff	Sil

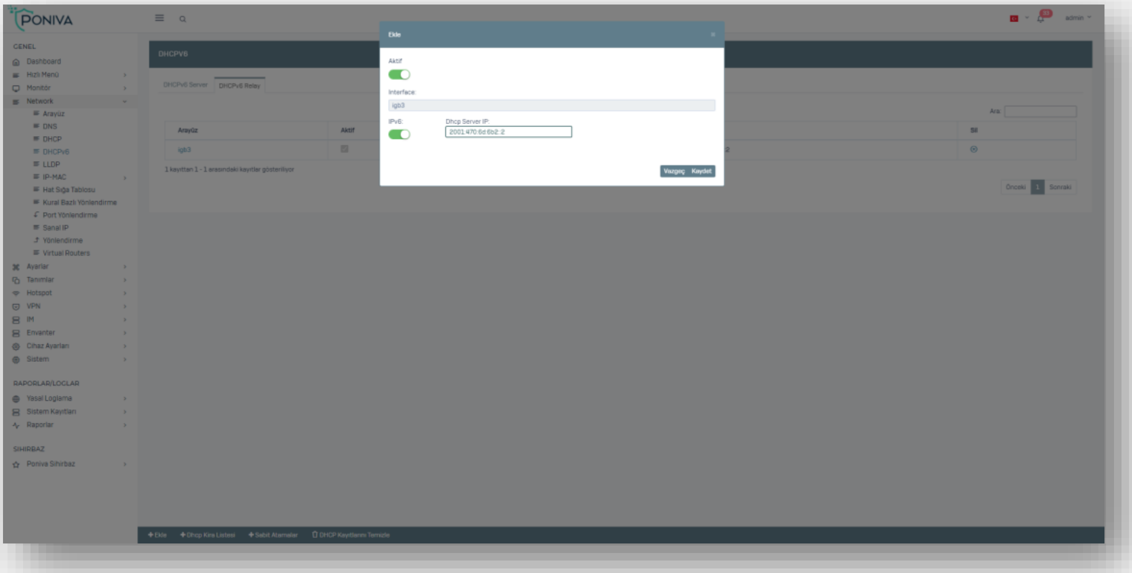
Arayüz	Durum	Kira Süresi	Sil
igb1		7200	⊗

1 kayıttan 1 - 1 arasındaki kayıtlar gösteriliyor

	EXPLANATION
Interface	You must choose the interface.
Pingle While Distributing IP	When it is activated, it checks whether that IP is used by pinging while distributing an IP.
Distribute IP Only to Defined Devices	When activated, no device can get IP except reservation.
DNS Suffix	Use default firewall option is active.
DNS	Use default firewall option is active.
IP Pool	You must enter a DHCPv6 IP range in IPv6 format. You can add multiple IP ranges.
IP Reservation	You can define the IPs you want to reserve in DHCPv6.

Dhcpv6 Relay

If you want to provide IPv6 distribution from a different DHCP Server, you can do so by adding a new DHCP Relay definition.



Aktif

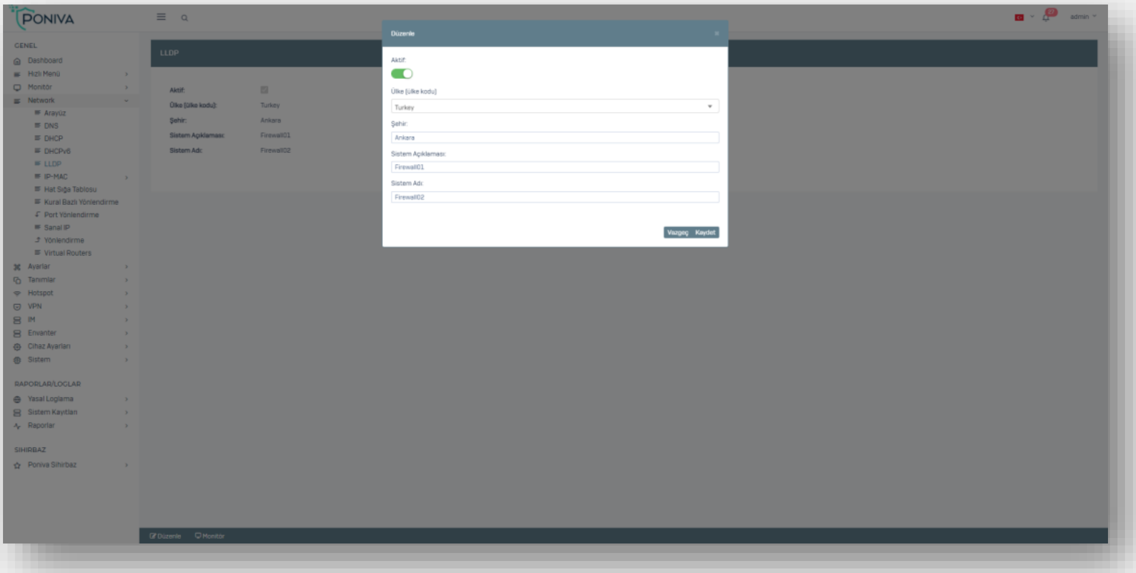
Interface: igb3

IPv6: Dhcp Server IP: 2001:470:6d:6b2::2

	EXPLANATION
Interface	You must choose the interface.
IPv6	You must enter your DHCP Server IP address in IPv6 format.

LLDP

It is a method by which it broadcasts to other devices on the network and has information. You can view devices from the monitor menu.



Aktif:

Ülke [ülke kodu]: Turkey

Şehir: Ankara

Sistem Açıklaması: Firewall01

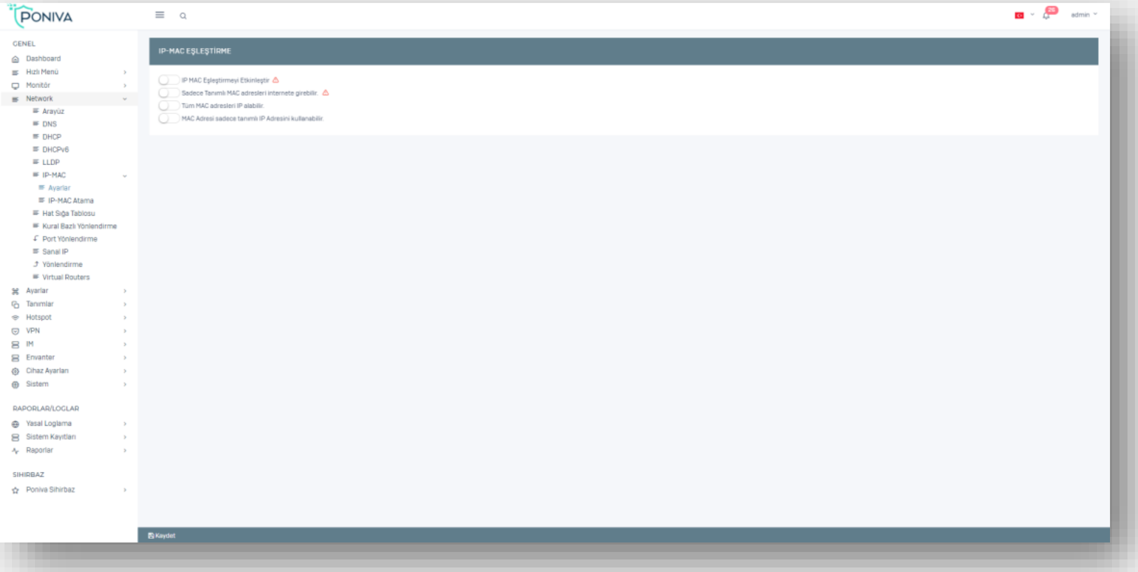
Sistem Adı: Firewall02

	EXPLANATION
Active	You can enable/disable LLDP status.
Country	You must select a country.
City	You must enter a city.
System Description	You must enter a system description.
System Name	You must enter a system name.

IP-MAC

The Mac address you add with IP-MAC mapping will only get the IP address you specify.

Settings



IP-MAC EŞLEŞTİRME

○ IP MAC Eşleştirmeyi Etkinleştir ⚠

○ Sadece Tanımlı MAC adresleri internete girebilir. ⚠

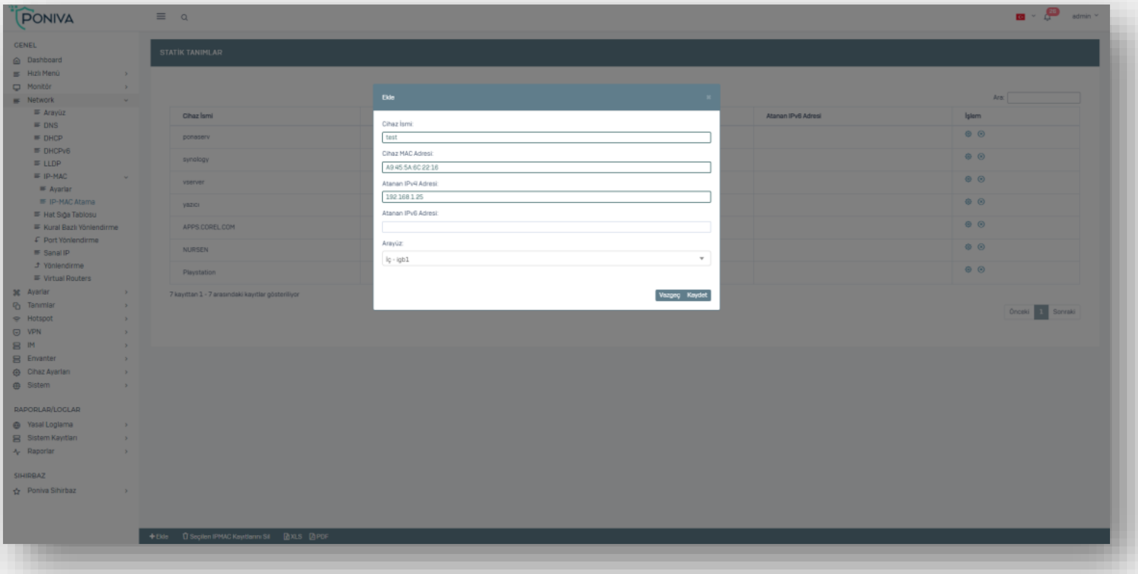
○ Tüm MAC adresleri IP alabilir.

○ MAC Adresi sadece tanımlı IP Adresini kullanabilir.

	EXPLANATION
Enable IP-MAC Pairing	You can enable/disable the service.
Only Defined MAC Addresses Can Access the Internet	When activated sOnly the MAC addresses you have mapped in the IP-MAC section can go to the internet.
All MAC Addresses Can Get IP	When enabled, MAC addresses other than IP-MAC mapping can also receive IP.
MAC Address Can Only Use Defined IP Address	When activated MAC addresses can only use the IP address you define in the IP-MAC section.

*Default passive income.

IP-MAC Assignment



Cihaz İsmi: test

Cihaz MAC Adresi: A9:45:5A:6C:22:16

Atanan IPv4 Adresi: 192.168.1.25

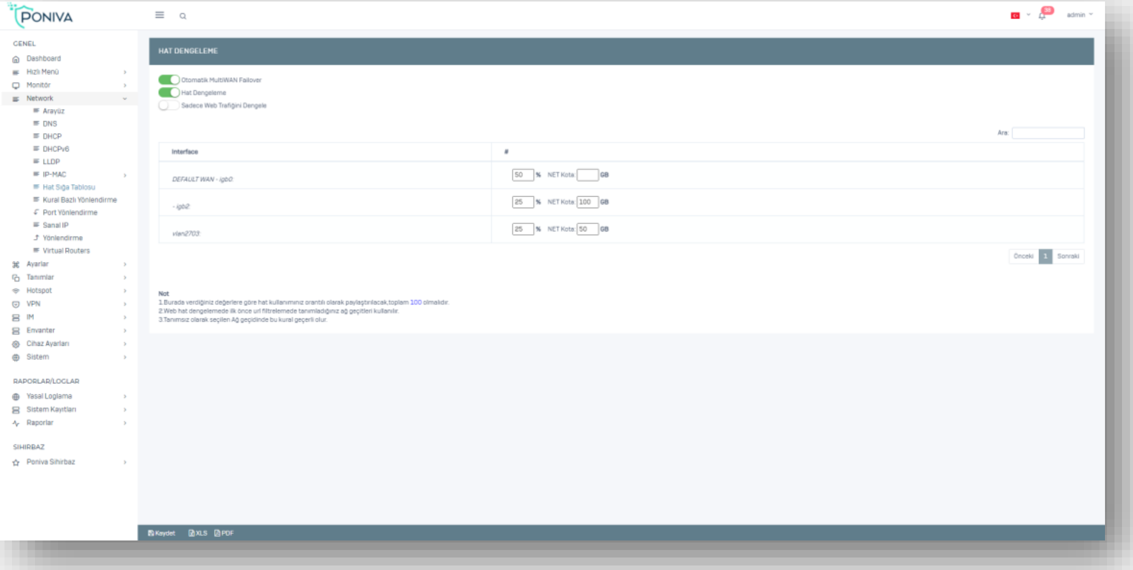
Atanan IPv6 Adresi:

Arayüz: İç - igb1

	EXPLANATION
Device Name	You must enter a device name.
Device MAC Address	You must enter the MAC address of the device.
Assigned IPv4 Address	You must enter the IP address you want the device to receive.
Assigned IPv6 Address	You can enter the IPv6 address you want the device to receive or leave it blank.
Interface	The interface is selected. (The IP you assign must be within the network you selected.)

LINE CAPACITANCE TABLE

Suddenly If you have more internet lines, you can define load balancing here.



HAT DENGELEME

- ● Otomatik MultiWAN Failover
- ● Hat Dengeleme
- ○ Sadece Web Trafiğini Dengele

Ara:

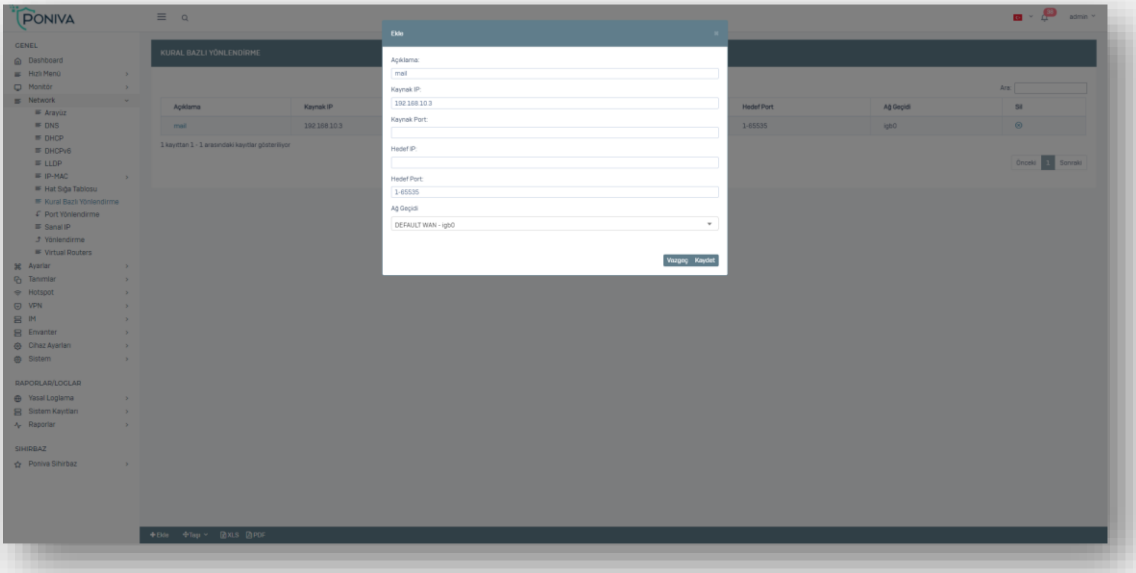
Interface	#
DEFAULT WAN - igb0:	50 % NET Kota: GB
- igb2:	25 % NET Kota: 100 GB
vlan2703:	25 % NET Kota: 50 GB

Not
1.Burada verdiğiniz değerlere göre hat kullanımınız orantılı olarak paylaştırılacak,toplam 100 olmalıdır.
2.Web hat dengelemede ilk önce url filtrelemede tanımladığınız ağ geçitleri kullanılır.
3.Tanımsız olarak seçilen Ağ geçidinde bu kural geçerli olur.

	EXPLANATION
Automatic Multiwan Failover	When this option is active, if one of your internet lines is disabled, all outputs there will continue over your active line.
Line Balancing	With this option, the use of your internet lines is shared equally. For example, you can use 50% from one line and 50% from the other line.
Just Balance Web Traffic	When this option is active, the stabilization settings you will make are applied only to 'Web Crawls'.
Default Wan	If you want the percentage of the line to be used, you must write that value.
Net Quota	When the line reaches the traffic quota you specified, it is automatically deactivated.

* If you have more than one line, you should apply these procedures to your other lines.

RULE BASED ROUTING



Ekle

Açıklama: mail

Kaynak IP: 192.168.10.3

Kaynak Port:

Hedef IP:

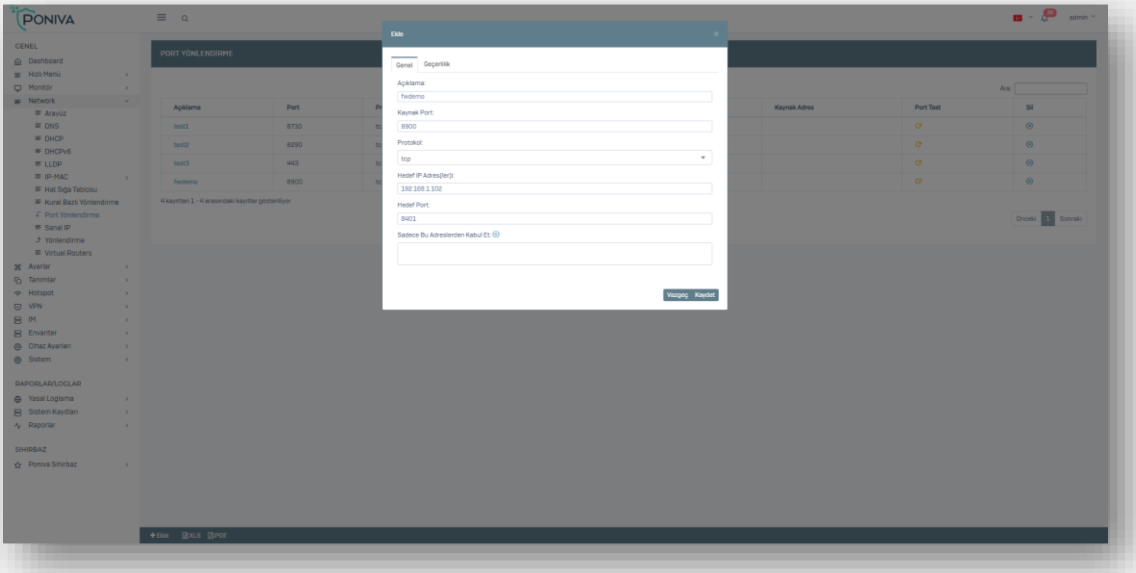
Hedef Port: 1-65535

Ağ Geçidi: DEFAULT WAN - igb0

	EXPLANATION
Description	You must enter a description.
Source IP Address	You must enter the IP Address you want to forward.
Source Port	You can enter the port or port range you want to forward or leave it blank. (For port range, you can use, for example, 10000-20000.)
Destination IP Address	You can enter the IP Address you will forward to or leave it blank.
Target Port	You must enter the port or port range you will forward. (For port range, you can use, for example, 10000-20000.)
Gateway	You must select the gateway where the rule will be active.

PORT FORWARDİNG

from the outside It is used to direct any incoming request to the service of another internal server. For example Web Service, RDP Service.



Açıklama: fwdemo

Kaynak Port: 8900

Protokol: tcp

Hedef IP Adres[ler]i: 192.168.1.102

Hedef Port: 8401

Sadece Bu Adreslerden Kabul Et:

	EXPLANATION
Description	You must enter a port description.
Source Port	You must enter the port or port range you want to forward. (For port range, you can use, for example, 10000-20000.)
Protocol	You must choose whether you want to forward TCP, UDP or TCP/UDP protocols.
Destination IP Address	You must enter the IP Address you will forward to. (You can use commas for multiple IP definitions.)
Target Port	You must enter the port or port range you will forward.
Only Accept From These Addresses	The port is accessed only from certain IP Addresses.
Validity	You can choose when port forwarding will be active.
Add Firewall Rules Automatically	When activated, it automatically adds the firewall rule for port forwarding.

VIRTUAL IP

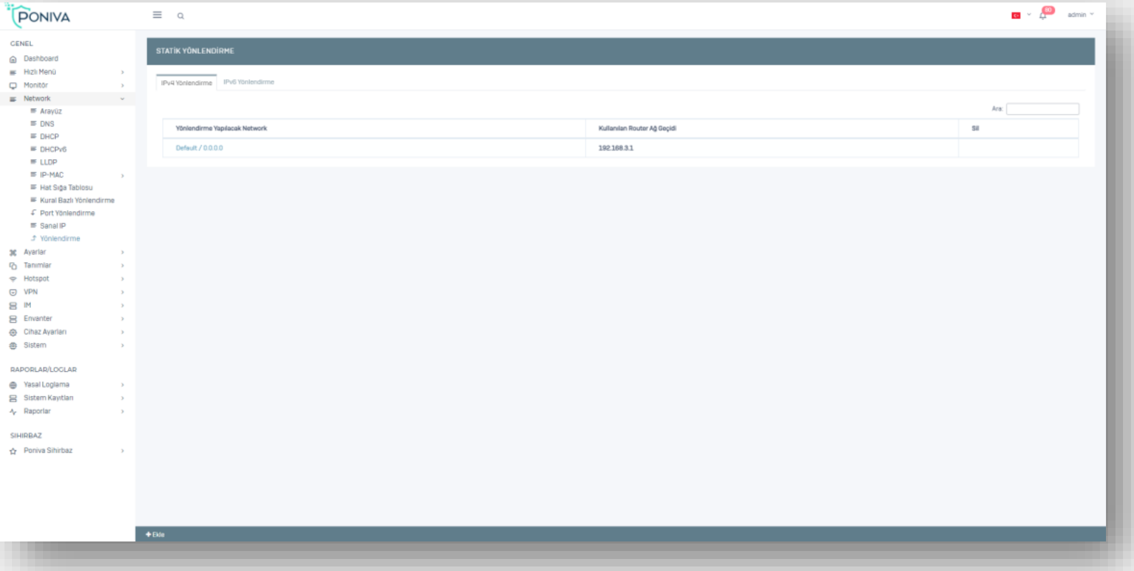
It responds to the ARP (Address Resolution Protocol) messages broadcast over the network for the definitions we made in the Virtual IP section, and ensures that the packets related to that IP are received.

	EXPLANATION
Description	You must enter a description.
Real IP Address	You must enter the real IP Address.

Local IP Address	You must enter an IP Address in your local network.
Interface	You must choose the interface.

ORIENTATION

You can define your IPv4 and IPv6 routings in this section.



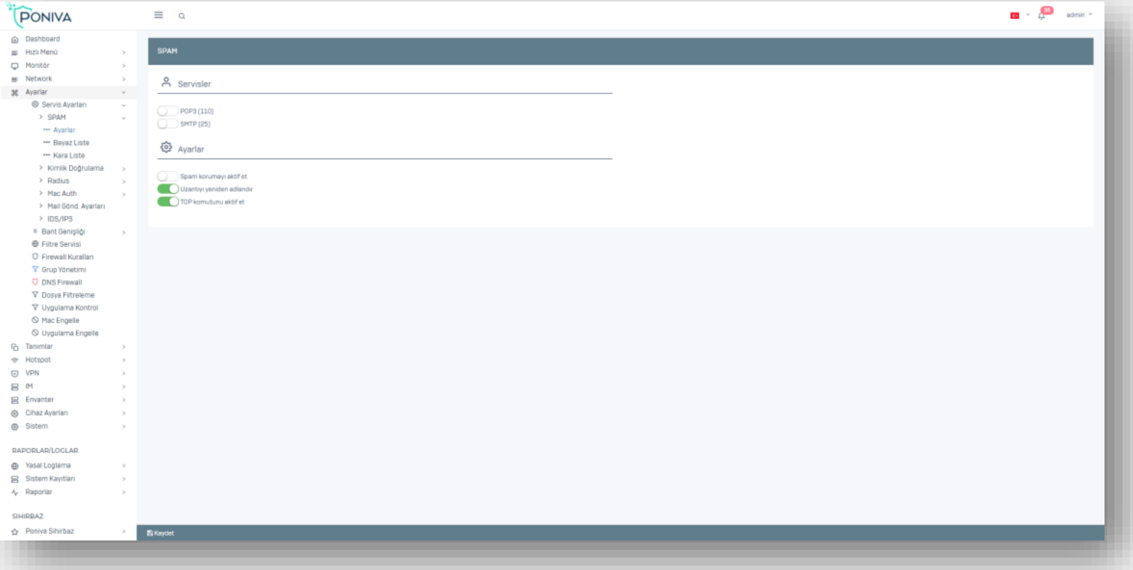
Yönlendirme Yapılacak Network	Kullanılan Router Ağ Geçidi	Sil
Default / 0.0.0.0	192.168.3.1	

SETTINGS

SERVICE SETTINGS

SPAM

You can enable/disable spam service settings.



SPAM

Servisler

○ POP3 (110)
○ SMTP (25)

Ayarlar

○ Spam korumayı aktif et
● Uzantıyı yeniden adlandır
● TOP komutunu aktif et

White List

The mail is sent to the user without checking for spam at the Mail/Domain addresses you add.

Black List

It does not forward the mail to the user without checking for spam in the Mail/Domain addresses you add and rejects it directly.

Authentication

You can define active directory server settings in this section.

Radius

Network Access Server (NAS) acts as RADIUS user and transfers user request to RADIUS server. Other RADIUS users can be wireless hotspots, routers or switches. RADIUS server performs authenticate, authorization, accounting (AAA) operations after receiving requests from users.

Mac Auth

on your firewallYou can do 802.1x Authentication with your smart switches. You prevent MAC addresses that you do not define in your firewall from entering your network, no one can attach a device to the network without your knowledge.

Authorized Switches

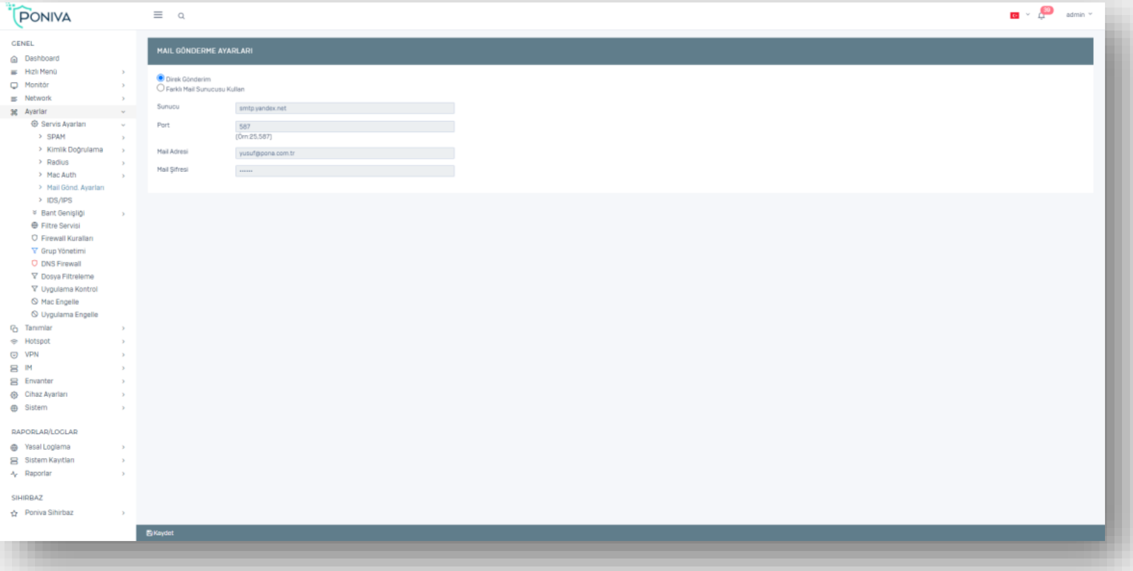
HereThe switches you write can only communicate with the firewall, the password defined here must be defined in the switch.

Allowed MAC

The MAC addresses you define here are allowed by the firewall.

Mail Sending Settings

You can define the mail sending settings here. If you wish, you can use direct sending or Use a different mail server option.



MAIL GÖNDERME AYARLARI

● Direk Gönderim
○ Farklı Mail Sunucusu Kullan

Sunucu: smtp.yandex.net

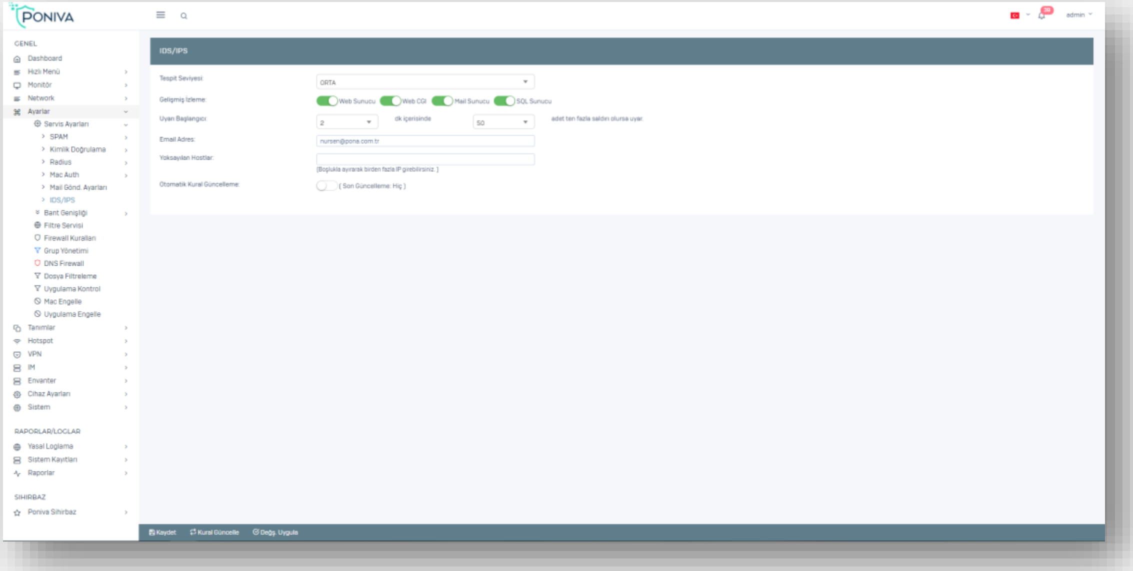
Port: 587 (Örn:25,587)

Mail Adresi: yusuf@pona.com.tr

Mail Şifresi: ••••••

IDS/IPS

to the systemIntrusion detection (IDS) and Intrusion prevention (IPS) systems are activated when there is an attack. When your e-mail address reaches the number of attacks within the period you specify, it will send you a notification e-mail.



IDS/IPS

Tespit Seviyesi: ORTA

Gelişmiş İzleme: Web Sunucu, Web CGI, Mail Sunucu, SQL Sunucu

Uyarı Baglangıcı: 2 dk içerisinde 50 adet ten fazla saldırı olursa uyar.

Email Adres: nursen@pona.com.tr

Yoksayılan Hostlar: (Boşlukla ayırarak birden fazla IP girebilirsiniz.)

Otomatik Kural Güncelleme: (Son Güncelleme: Hiç)

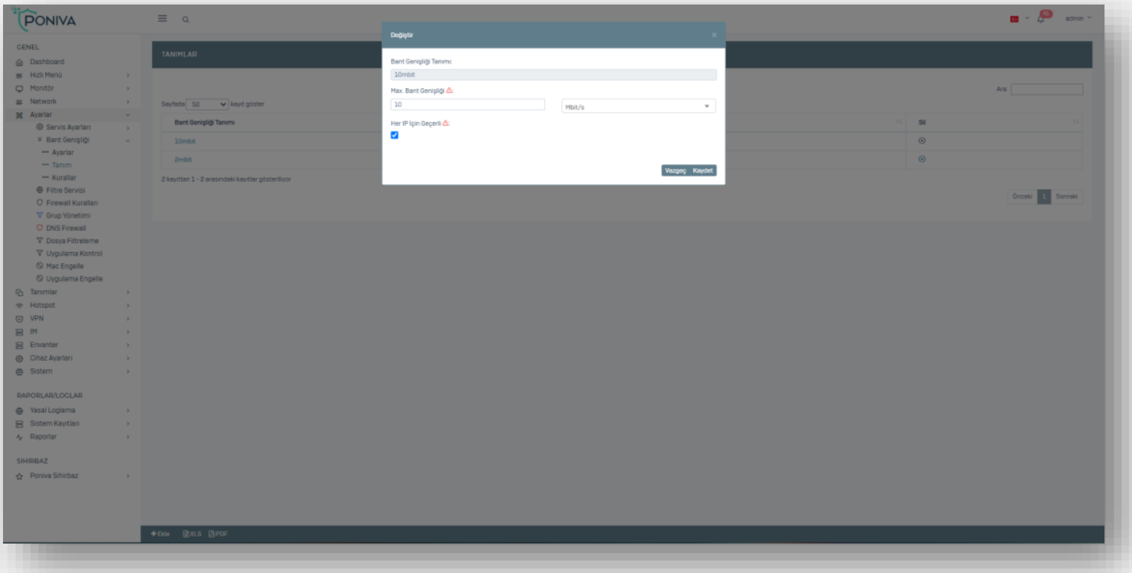
BANDWIDTH

You can limit internet speeds by defining bandwidth rules for your users.

Settings

You can enable/disable the service status.

Definition



Değiştir

Bant Genişliği Tanımı: 10mbit

Max. Bant Genişliği: 10 Mbit/s

Her IP İçin Geçerli: ☑

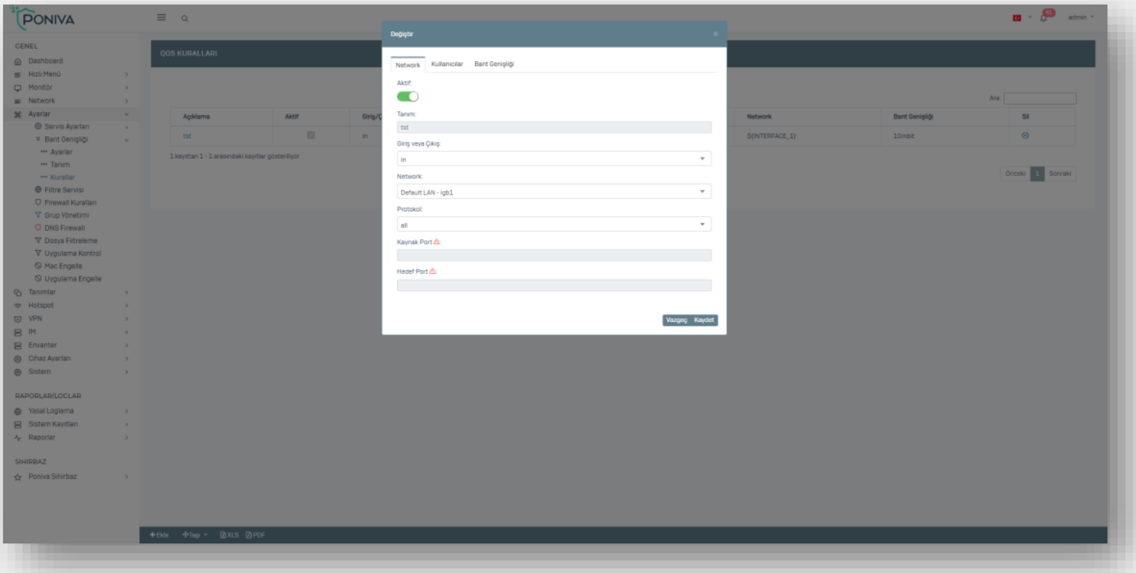
Sayfada 50 kayıt göster

Bant Genişliği Tanımı
10mbit
2mbit

2 kayıttan 1 - 2 arasındaki kayıtlar gösteriliyor

	EXPLANATION
Description	You must enter a description.
Max. Band width	You have to enter a number and choose how many kbit/s, kbyte/s, mbit/s, mbte/s.
Valid for Any IP	You must enter an IP Address in your local network.

Rules



Değiştir

Network | Kullanıcılar | Bant Genişliği

Aktif: ●

Tanım: tst

Giriş veya Çıkış: in

Network: Default LAN - igb1

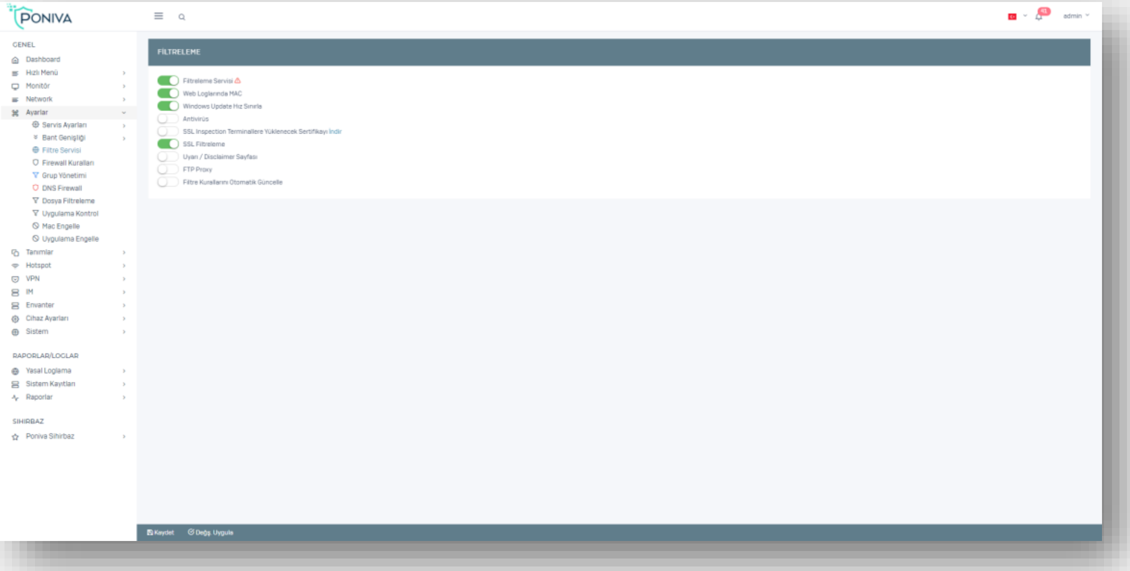
Protokol: all

Kaynak Port:

Hedef Port:

	EXPLANATION
Active	You can enable/disable the bandwidth status.
Definition	You must enter a description.
Entry or Exit	You must select the packet direction.
network	You should choose which network you want to apply bandwidth to.
Protocol	You must select the protocol.
Source Port	You must enter the port or port range you want to forward. (For port range, you can use, for example, 10000-20000.)
Target Port	You must enter the port or port range you will forward.
Users	You can type 'any' for all users or add IP addresses.
BW Limit	You must select the bandwidth definition you created in the Definition section.
Priority	You must enter a value between 1-100. (Default is 1.)
Enforce Rules After This Rule	When this option is activated, other rules become invalid.

FILTER SERVICE



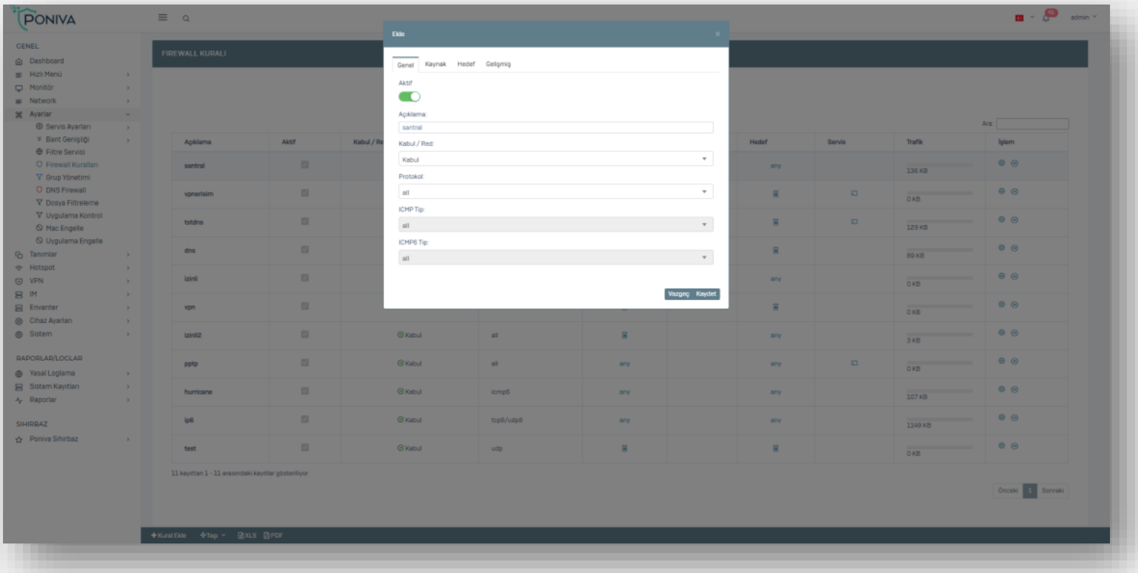
FİLTRELEME

- ● Filtreleme Servisi ⚠
- ● Web Loglarında MAC
- ● Windows Update Hız Sınırla
- ○ Antivirüs
- ○ SSL Inspection Terminallere Yüklenecek Sertifikayı İndir
- ● SSL Filtreleme
- ○ Uyarı / Disclaimer Sayfası
- ○ FTP Proxy
- ○ Filtre Kurallarını Otomatik Güncelle

	EXPLANATION
Filtering Service	The service status must be active for the logging service and filtering feature to work.
MAC in Web Logs	When activated, MAC records are also kept in the web logs.
Windows Update Rate Limit	When activated, it limits the Windows update speed.
antivirus	When activated, it scans the sites you access for antivirus.
SSL Inspection Download Certificate to be Installed on Terminals	When activated, you need to download and install the certificate on all your computers.
SSL Filtering	This option must be active in order to filter HTTPS sites.
Warning/Disclaimer Page	When activated, you can show a warning/information when your users open their browsers.

FIREWALL RULES

These are the rules we create to provide acceptance/rejection/log control of incoming packets to the Firewall. The order of the rules is important here. You can specify which one to prioritize by typing multiple rules one after the other.



Ekle

Aktif: ●

Açıklama: santral

Kabul / Red: Kabul

Protokol: all

ICMP Tip: all

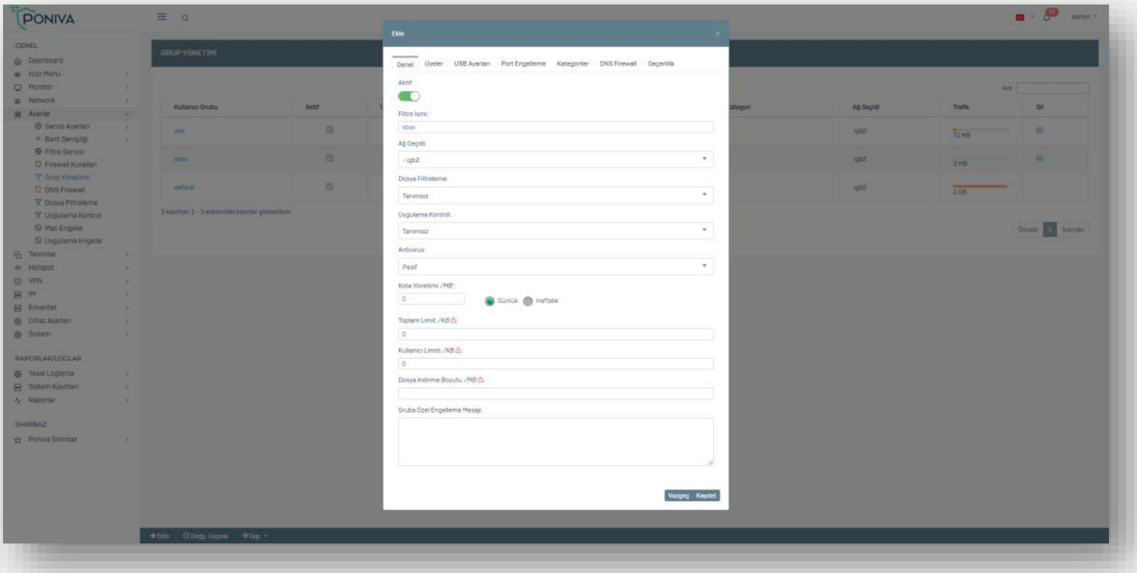
ICMP6 Tip: all

	EXPLANATION
Active	You can make the rule status active/passive.
Description	You must enter a description.
Accept / Reject / Log	Accept -> accept all packages. Red -> rejects all packets. Log -> just logs.
Protocol	You must select the protocol to which the rule will be applied.
Source Address	You must select the source address to which the rule will be applied.
Source IP	If the source address is selected manually, this section becomes active and you must enter the source IP or Network. You can use 'comma' for multiple IPs or Networks. You must enter 'any' for all.
Source Port	You can write the source port to which the rule will be applied. You can use 'comma' for multiple ports and '–' for port range.
Destination Address	You must select the destination address to which the rule will be applied.
Destination IP	If the destination address is selected manually, this section becomes active and you must enter the destination IP or Network. You can use 'comma' for multiple IPs or Networks. You must enter 'any' for all.
Target Port	You can type the destination port to which the rule will be applied. You can use 'comma' for multiple ports and '–' for port range.
IP Limit	You can enter the number of simultaneous connections from the same IP address.
Condition Direction (Optional)	You can choose in which direction the rule will work.

Arrival Interface	If the condition direction is 'in', you should choose the interface from here.
Output Interface	If the condition direction is 'out', you should choose the interface from here.
Validity	You can specify the day and time the rule will run.
stateful	
Keep Record	When activated, rule logs are kept.

GROUP MANAGEMENT

In this section, you can filter your users. By creating multiple groups one after the other, you can determine which one to prioritize. (Users who are not members of any group are included in the default group and the rules there apply.)



Aktif: ●

Filtre İsmi: xbox

Ağ Geçidi: - igb2

Dosya Filtreleme: Tanımsız

Uygulama Kontrol: Tanımsız

Antivirüs: Pasif

Kota Yönetimi /MB: 0 ● Günlük ○ Haftalık

Toplam Limit /KB: 0

Kullanıcı Limiti /KB: 0

Dosya İndirme Boyutu /MB:

Gruba Özel Engelleme Mesajı:

	EXPLANATION
Active	You can make the group active/passive.
Filter Name	You must enter a filter name.
Gateway	If you have more than one internet and you want users to exit only on that line, you can select the relevant network. If you want to use all lines in common, you should choose 'UNDEFINED'.
File Filtering	File types and extensions in the file filtering you choose. you can block.
Application Control	You can block the application extensions within the application control you selected.

antivirus	When you activate it, you can check the Antivirus when users enter the sites.
Quota Management	When users exceed the specified quota, you can turn off their internet by showing a warning screen by the system.
Total Limit /KB	Expresses the speed limit of the sum of all members of the group.
User Limit /KB	Indicates the speed limit for each member of the group.
File Download Size /MB	You can specify the 'MAX' file size allowed to be downloaded.
Group Specific Blocking Message	You can show a message here when the user accesses a blocked site.
Filtering Type	You can filter based on IP or User.
Group members	You can choose from the list you defined in Addresses and Address groups.
USB Memory Usage	You can control USB usage. (This feature is only valid for Windows PCs and additional software needs to be installed on the client side.)
USB 3G Modem	You can control the use of USB 3G Modem. (This feature is only valid for Windows PCs and additional software needs to be installed on the client side.)
Port Block	Turns off the outputs of the option you selected and prevents group members from accessing it. (When the Close all outputs option is activated, the user will not have access to any location.)
categories	For Monitor -> Category, it only monitors. Whitelist -> Allows category. Banned -> Blocks the category.
DNS Firewall	The definitions in the DNS firewall you selected are applied.
Validity	You can specify the day and time the filtering will run.

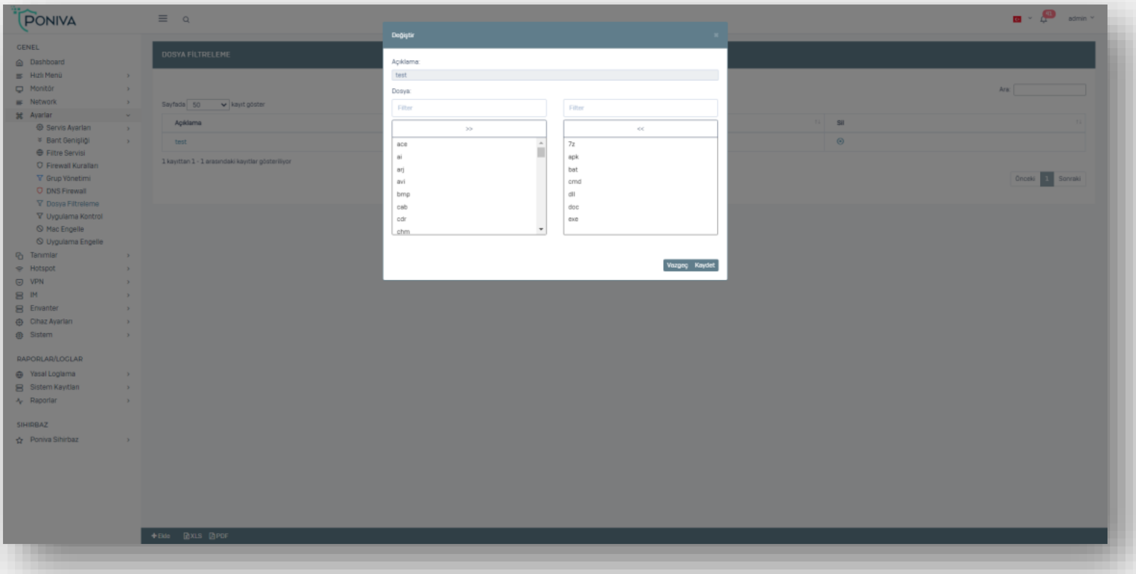
DNS FIREWALL

	EXPLANATION
Description	You must enter a description.
Redirect Botnet C&C Request to Block Portal	During the DNS name resolution phase, the botnet may block website access. This option provides additional protection for your network.
Google Force SafeSearch for Bing	When activated, harmful content is blocked for Google, bing.
Force SafeSearch for Youtube	When activated, harmful content on youtube is prevented from being displayed.
Domain Filtering	You can also define your own local static domain filter to allow or block specific domains.
DNS Translation	Forced to translate 1.2.3.4 (www.example.com) to 192.168.3.4 with DNS translation. When internal network users make a DNS query for www.example.com, they do not get the original

	IP address of www.example.com which is 1.2.3.4. Instead, they get the IP address 192.168.3.4.
NameServer	

FILE FILTERING

After saving the file extensions and types you choose in this section, you can assign them to any group in the group filtering section, so the system automatically detects them and blocks them for the users of that group.



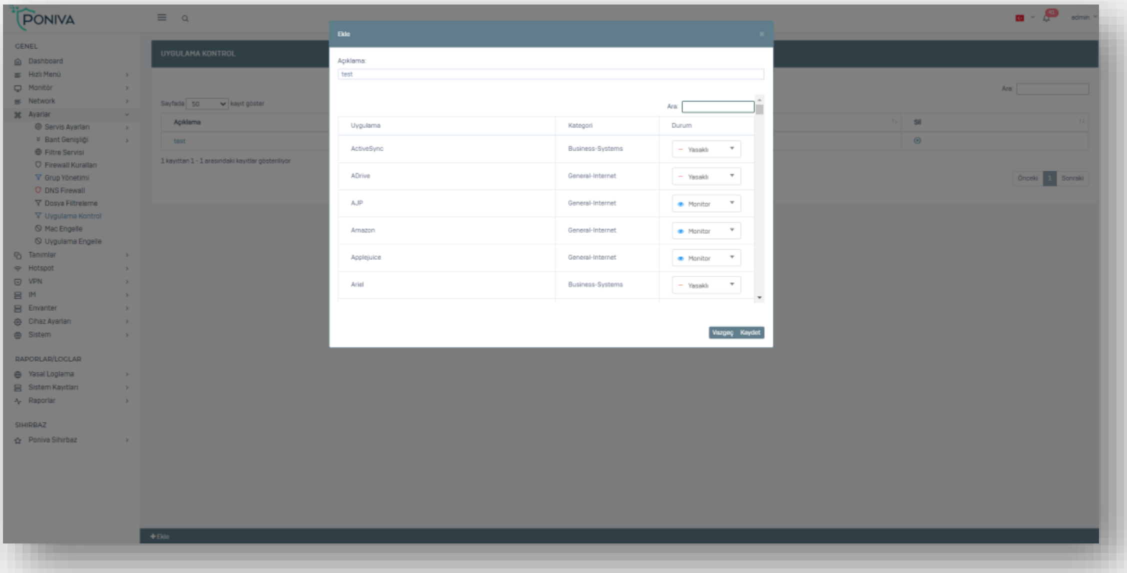
Açıklama: test

Dosya:

ace	7z
ai	apk
arj	bat
avi	cmd
bmp	dll
cab	doc
cdr	exe
chm	

APPLICATION CONTROL

After saving the applications you selected in this section, you can assign them to any group in the group filtering section, so the system automatically detects them and blocks them for the users of that group.



Ekle

Açıklama: test

Ara:

Uygulama	Kategori	Durum
ActiveSync	Business-Systems	− Yasaklı
ADrive	General-Internet	− Yasaklı
AJP	General-Internet	Monitor
Amazon	General-Internet	Monitor
Applejuice	General-Internet	Monitor
Ariel	Business-Systems	− Yasaklı

MAC BLOCK

You can block internet access by defining the MAC addresses of the devices here.

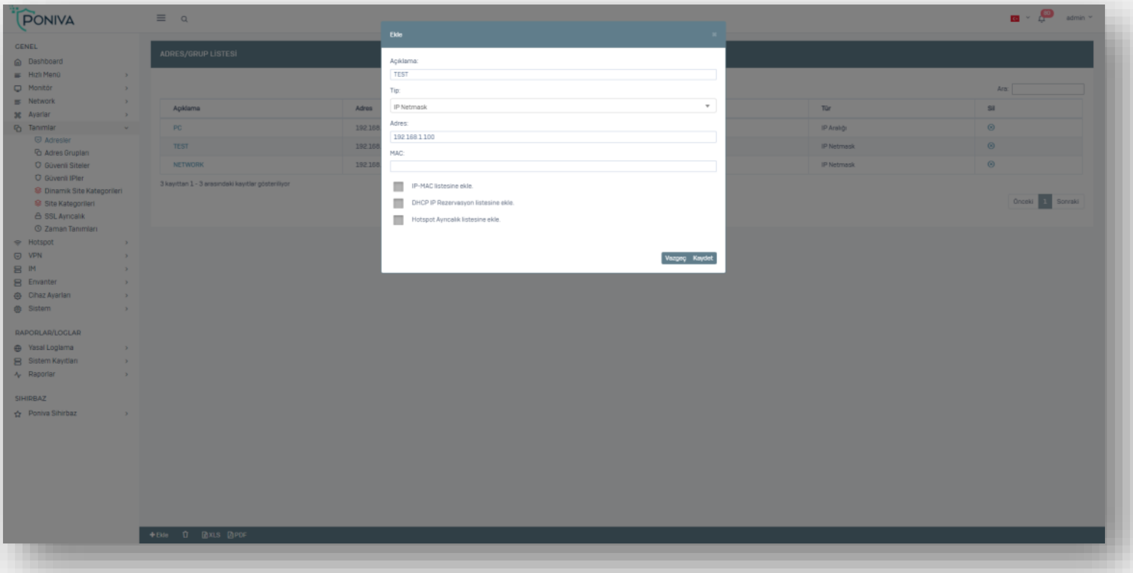
BLOCK APPLICATION

The system automatically detects and blocks the applications you select in this section. For example: When you select Anydesk, your computer can no longer connect to Anydesk. Except for definitions in the privilege list.

DEFINITIONS

ADDRESSES

You can make address definitions in this section. You can define IP address, network or IP range. You can use these definitions in the 'members' section in group management or port forwarding. You can easily define the records you add here by adding them to the IP-MAC, DHCP IP Reservation or Hotspot Privilege list.



Ekle

Açıklama: TEST

Tip: IP Netmask

Adres: 192.168.1.100

MAC:

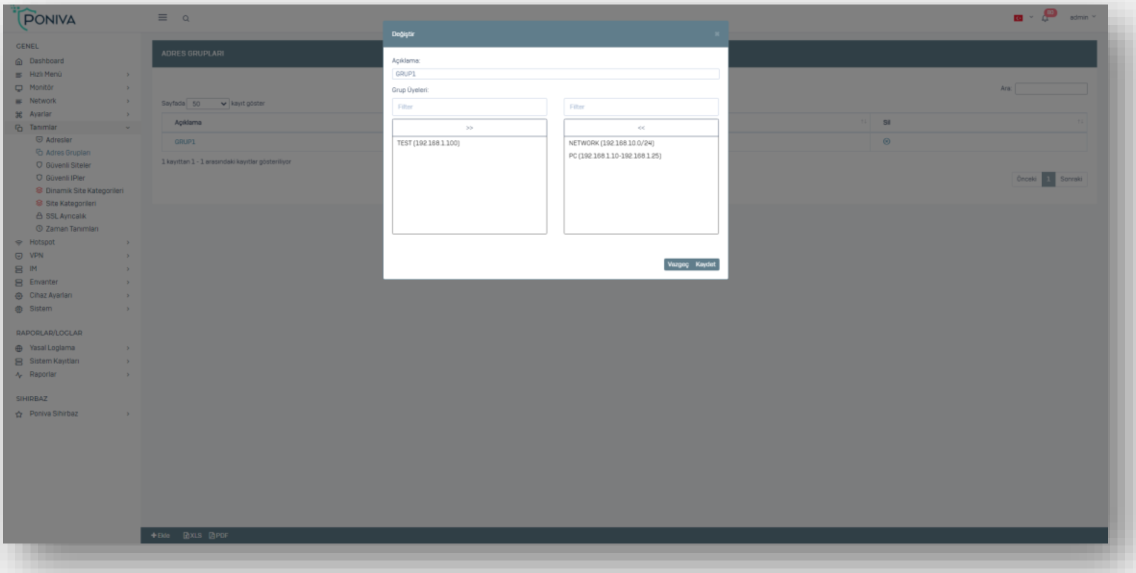
□ IP-MAC listesine ekle.

□ DHCP IP Rezervasyon listesine ekle.

□ Hotspot Ayrıcalık listesine ekle.

ADDRESS GROUPS

You can group the definitions you made in the Addresses section in this section. You can use these groupings in the 'members' section in group management or port forwarding.



Değiştir

Açıklama: GRUP1

Grup Üyeleri:

TEST (192.168.1.100)

NETWORK (192.168.10.0/24)
PC (192.168.1.10-192.168.1.25)

SAFE SITES

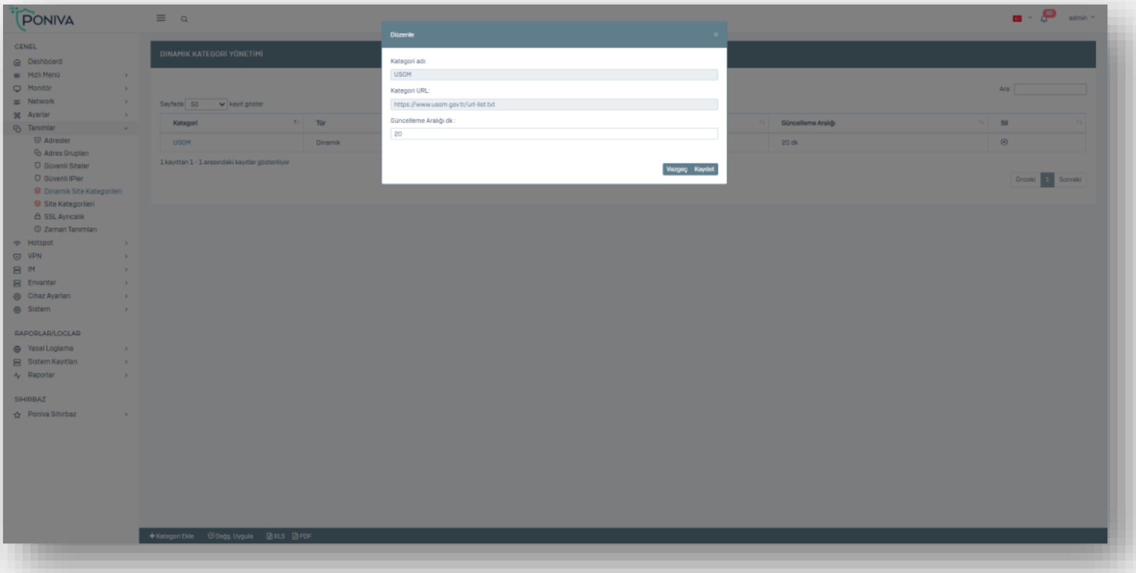
No logging or filtering is done about the sites you add in this section.

SECURE IPS

The local network IP addresses you add in this section, '**http**' traffic is excluded from filtering and logging. (According to the law no 5651, you must log for all IP Addresses.)

DYNAMIC SITE CATEGORIES

You can allow or block by creating dynamic site categories on your device. The url list is updated with the update intervals you specify from the url address you add without the need for any manual action in dynamic site categories. The default USOM is attached in the system. USOM is a government-provided service.As the list of blocked and prohibited sites by the USOM is updatedIn Poniva firewall, this url list is updated automatically. You can block this url list by selecting the USOM category in group management.



Kategori adı: USOM

Kategori URL: https://www.usom.gov.tr/url-list.txt

Güncelleme Aralığı dk : 20

Sayfada 50 kayıt göster

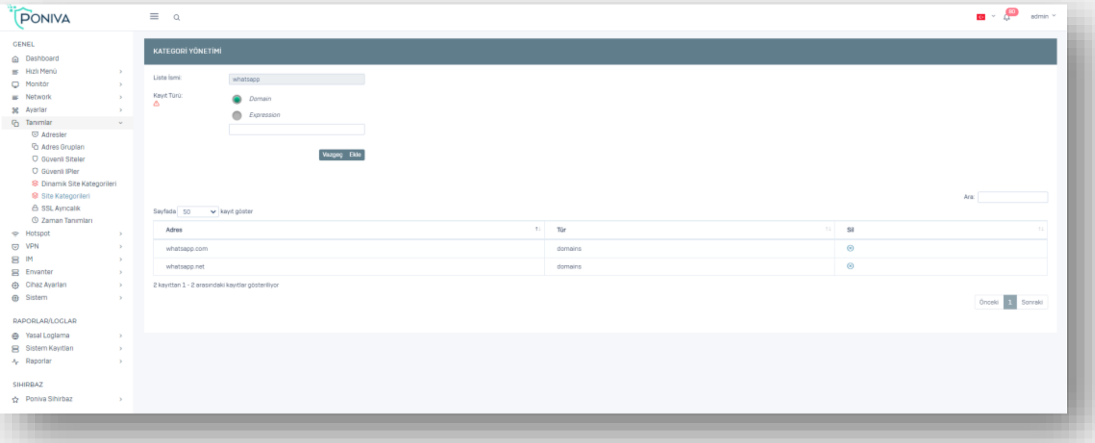
Ara:

Kategori	Tür	Güncelleme Aralığı	Sil
USOM	Dinamik	20 dk	⊗

1 kayıttan 1 - 1 arasındaki kayıtlar gösteriliyor

SITE CATEGORIES

You can allow or block the sites you want by creating site categories on your device. You can use a domain name in category definitions as well as an expression (based on the word in the address bar). For example, sites with "game" in the address bar. You should make the allowed/forbidden selections for the site categories you created here from the group management.



Liste İsmi: whatsapp

Kayıt Türü: ● Domain ○ Expression

Sayfada 50 kayıt göster

Ara:

Adres	Tür	Sil
whatsapp.com	domains	⊗
whatsapp.net	domains	⊗

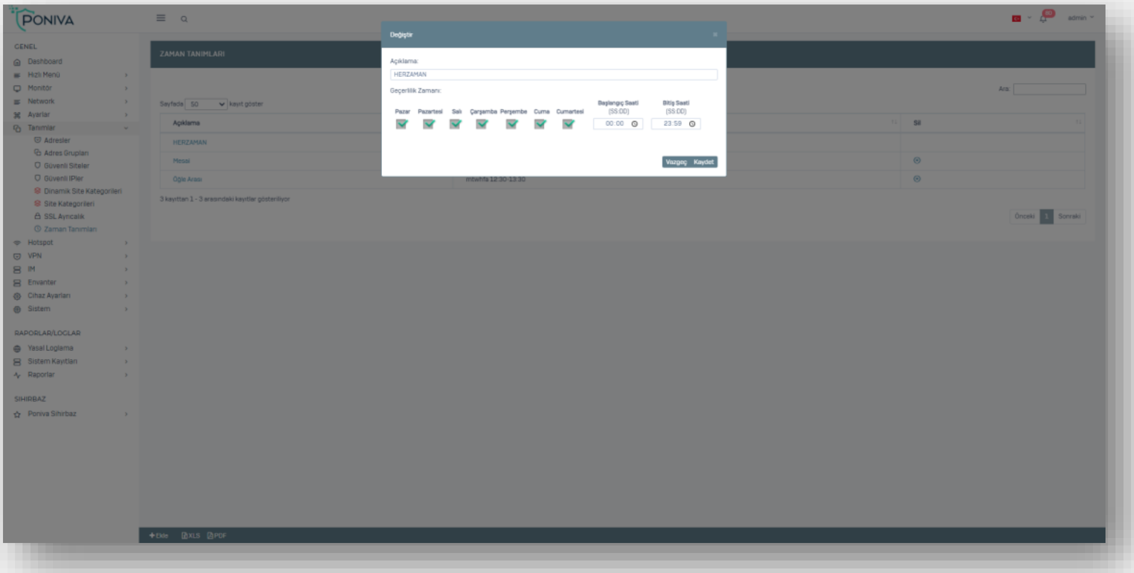
2 kayıttan 1 - 2 arasındaki kayıtlar gösteriliyor

SSL PRIVILEGE

The local network IP addresses you add in this section, '**https**' traffic is excluded from filtering and logging. (According to the law no 5651, you must log for all IP Addresses.)

TİME DEFINITIONS

In this section, you can make time definitions and use them as 'validity' in other menus. For example, you can restrict the access of a user you define in SSL VPN by selecting 'Operating Hours'.



Açıklama: HERZAMAN

Geçerlilik Zamanı:

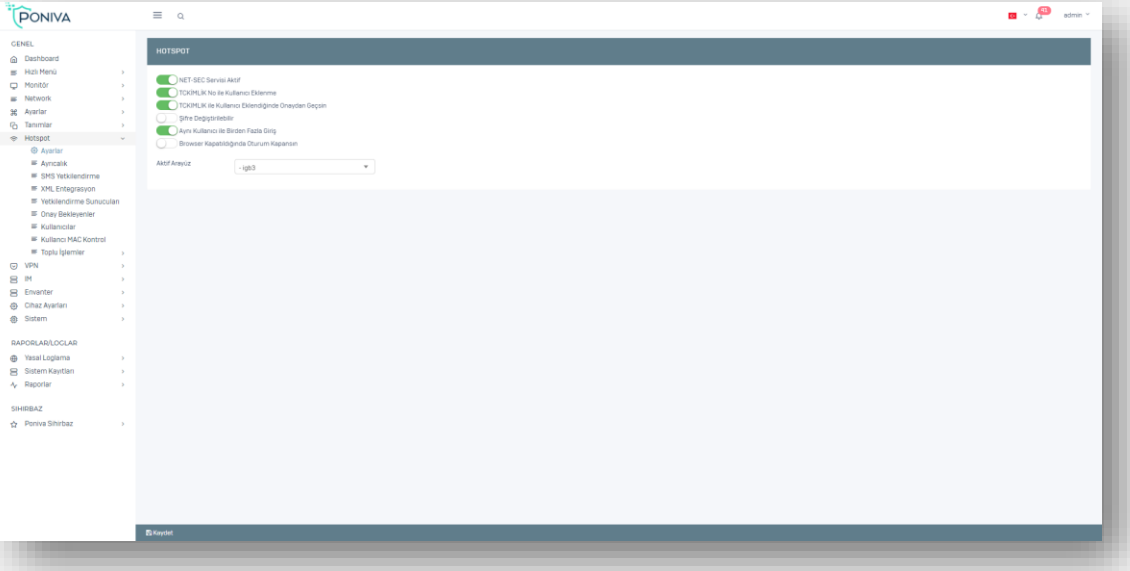
Pazar	Pazartesi	Salı	Çarşamba	Perşembe	Cuma	Cumartesi	Başlangıç Saati (SS:DD)	Bitiş Saati (SS:DD)
☑	☑	☑	☑	☑	☑	☑	00:00	23:59

Açıklama	
HERZAMAN	
Mesai	
Öğle Arası	mtwhfa 12:30-13:30

3 kayıttan 1 - 3 arasındaki kayıtlar gösteriliyor

HOTSPOT

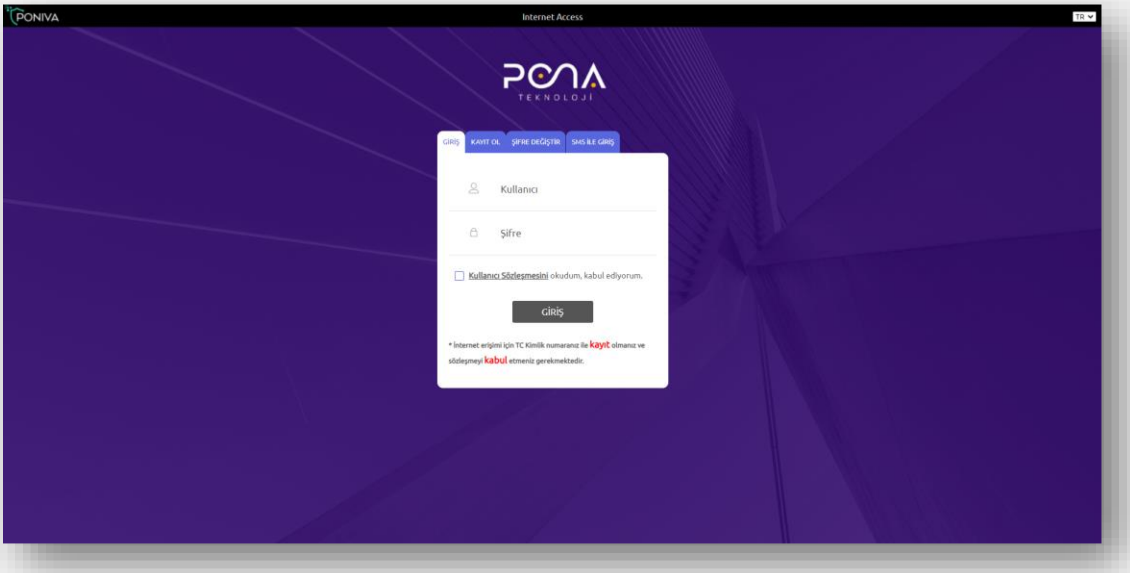
SETTINGS



HOTSPOT

- ● NET-SEC Servisi Aktif
- ● TCKİMLİK No ile Kullanıcı Eklenme
- ● TCKIMLIK ile Kullanıcı Eklendiğinde Onaydan Geçsin
- ○ Şifre Değiştirilebilir
- ● Aynı Kullanıcı ile Birden Fazla Giriş
- ○ Browser Kapatıldığında Oturum Kapansın

Aktif Arayüz: - igb3



* İnternet erişimi için TC Kimlik numaranız ile kayıt olmanız ve sözleşmeyi kabul etmeniz gerekmektedir.

	EXPLANATION
NET-SEC Service Active	You can enable/disable Hotspot Service.
Adding User with TCKID Number	When activated, users hotspot They can register with their TCID number on the registration screen.
Approval When User Added With TCKIMLIK Number	When activated, users cannot access the internet unless you give consent after registration.
Password Changeable	When activated, users can change their passwords on the Hotspot change password screen.
Multiple Logins with the Same User	Users can access from multiple devices with the same username and password.
Logout When Browser Is Closed	If the window that opens after logging in is closed, your session will be terminated automatically.
Active Interface	You must choose the interface where the hotspot will be active.

*In order to use the Hotspot feature, you must connect an Access point to your Firewall or Switch.

PRIVILEGE

The HOTSPOT password screen does not appear for the IPs you define here. Internet directly.

SMS AUTHORİZATION

When the SMS module is activated, the user registers with the mobile phone on the hotspot screen and the password is sent to the user as an SMS.

*You must purchase an SMS API to use this feature.

XML INTEGRATION

hotel etc. You can transfer the information of all users defined in the system in enterprises to the hotspot system quickly and easily with the Poniva Integration software. In this way, when users want to access the wireless network, they provide internet access by entering their TC and Passport number information.

AUTHORIZATION SERVERS

It can perform firewall user control in MSSQL, POP3, FTP protocols. You can also add multiple authorization servers to Firewall.

AWAİTİNG APPROVAL

If 'Confirm when a user is added with TCID' is activated in the HOTSPOT settings section, users will fall into this section when they register and cannot access the internet unless you give your consent.

USERS

In this section, you can see the list of registered users in the Hotspot, delete existing users or add a new user.

USER MAC CONTROL

User defined in this section he can only log in from the specified MAC address, he is prevented from logging in from other systems.

BATCH ACTIONS

Transactions

You can perform operations such as mass deletion, cleaning/updating start-end dates for records in the Users section.

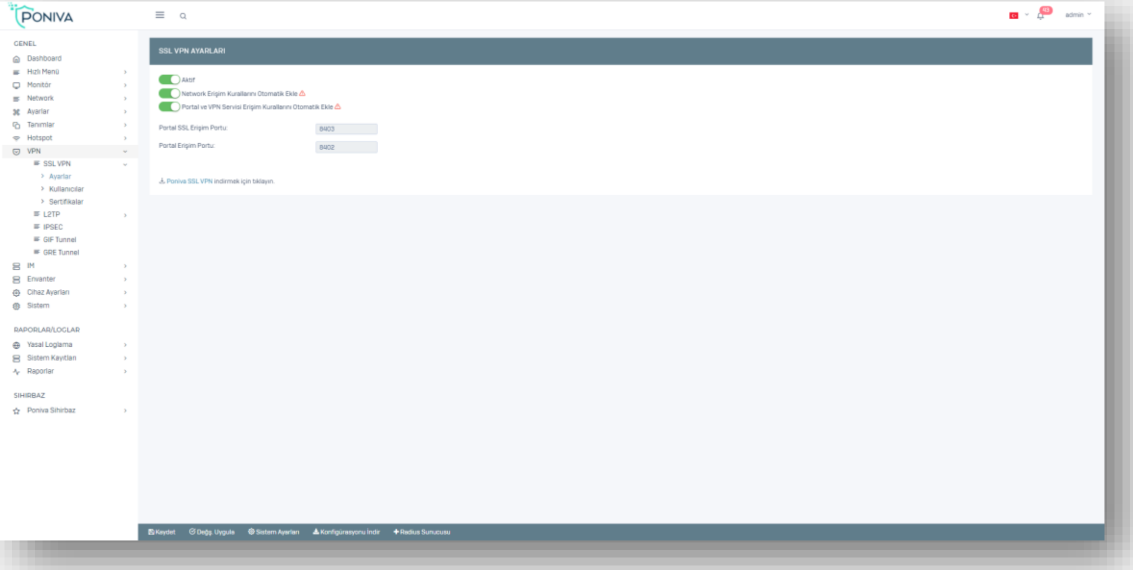
CSV Import

You can import your users from csv file.

VPN

SSL VPN

A remote user can establish a secure connection with the Poniva SSL application he will install on his computer.



SSL VPN AYARLARI

Aktif

Network Erişim Kurallarını Otomatik Ekle ⚠

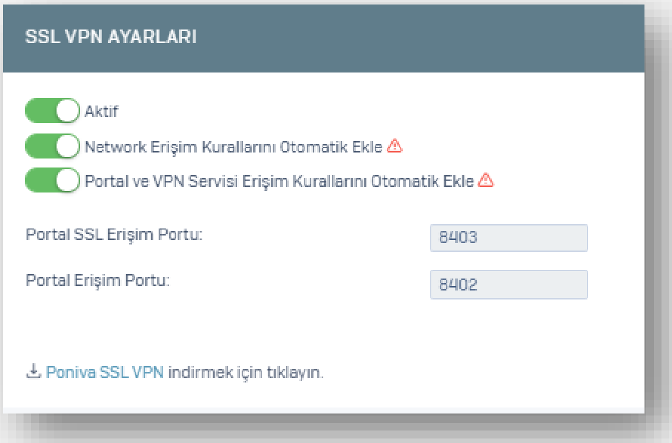
Portal ve VPN Servisi Erişim Kurallarını Otomatik Ekle ⚠

Portal SSL Erişim Portu: 8403

Portal Erişim Portu: 8402

Poniva SSL VPN indirmek için tıklayın.

Settings



SSL VPN AYARLARI

Aktif

Network Erişim Kurallarını Otomatik Ekle ⚠

Portal ve VPN Servisi Erişim Kurallarını Otomatik Ekle ⚠

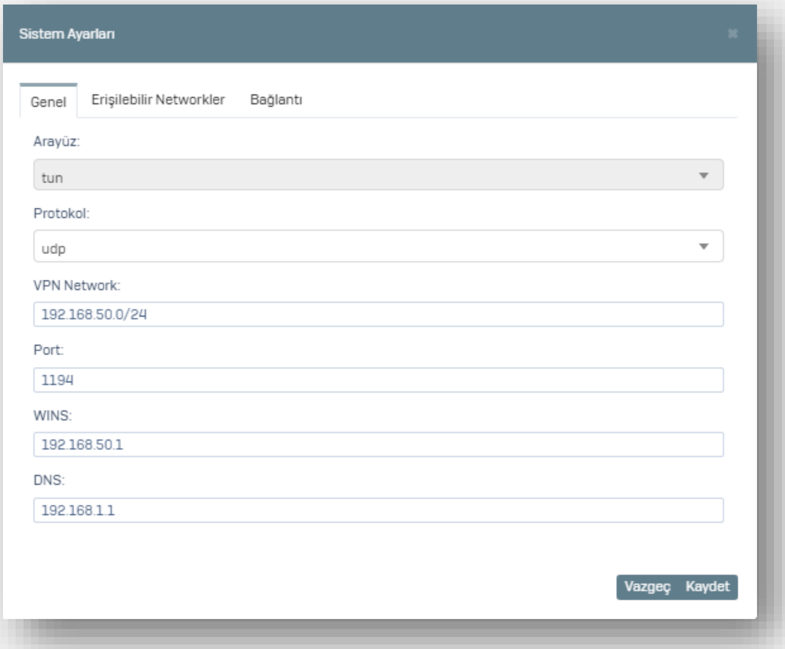
Portal SSL Erişim Portu: 8403

Portal Erişim Portu: 8402

Poniva SSL VPN indirmek için tıklayın.

	EXPLANATION
Active	You can enable/disable the service.
Add Network Rules Automatically	It automatically adds the network rules you define.
Portal and VPN Service Access Rules	You must enter the ending IP address.

System Settings



Arayüz: tun

Protokol: udp

VPN Network: 192.168.50.0/24

Port: 1194

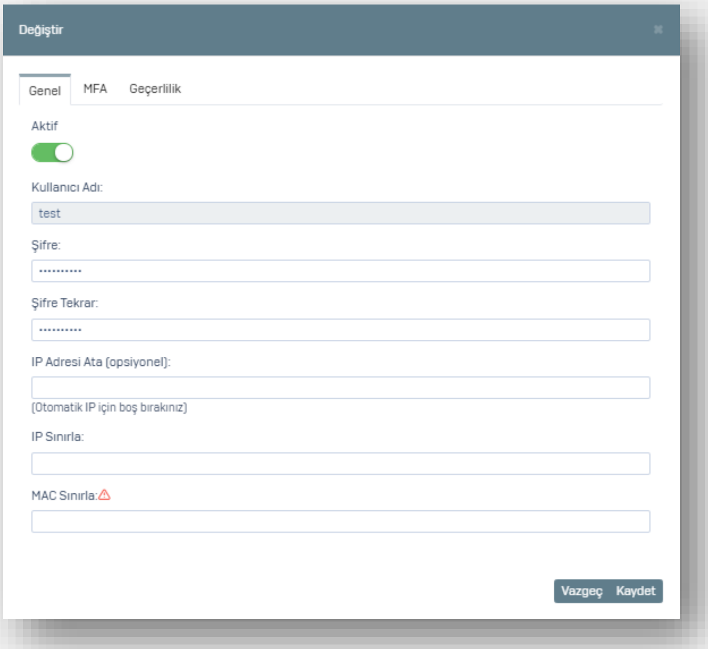
WINS: 192.168.50.1

DNS: 192.168.1.1

	EXPLANATION
Interface	The default 'tun' is selected.
Protocol	If you have more than one internet line, you should choose TCP.
VPN Network	You do not define a VPN network. (For example 192.168.50.0/24)
port	Default port 1194
WINS	You can type the IP you defined in the VPN network. (For example 192.168.50.1)
DNS	You must type the Firewall IP address. (For example 192.168.1.1)
Accessible Networks	When you select Manual in this section, you can write the networks you want users coming from VPN to access.
Clients can see each other	Default is 'Yes' is selected.
Multiple connections can be made with the same certificate	Default is 'Yes' is selected.
Users log out from this server	Default is 'Yes'is selected.

*If 'yes' is selected for users to log out through this server, Accessible Networks will be disabled.

Users



Aktif ●

Kullanıcı Adı: test

Şifre: ••••••••••

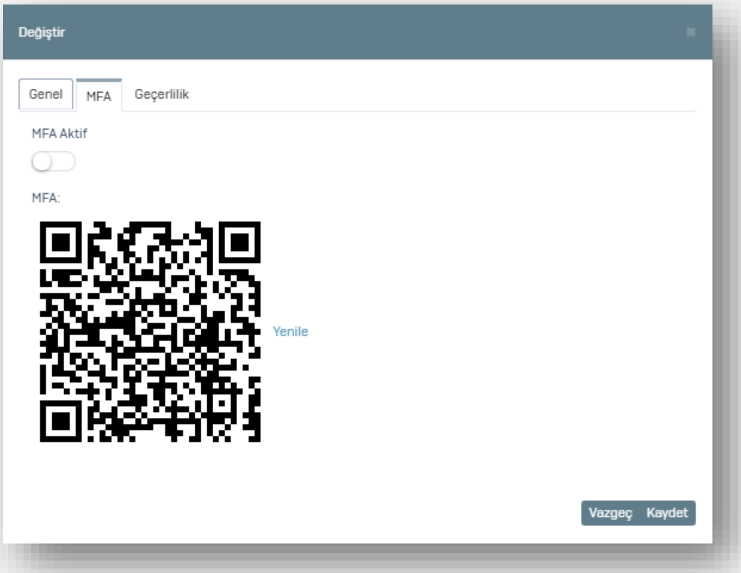
Şifre Tekrar: ••••••••••

IP Adresi Ata (opsiyonel):

(Otomatik IP için boş bırakınız)

IP Sınırla:

MAC Sınırla:⚠



MFA Aktif ○

MFA:

	EXPLANATION
Active	You can make the user active/passive.
User name	You must enter a username.
Password	You must enter a password for the user.
Assign IP Address (Optional)	You can assign an IP to the user or leave it blank for automatic IP.
IP Limit	The user can only connect from the IP you specify.

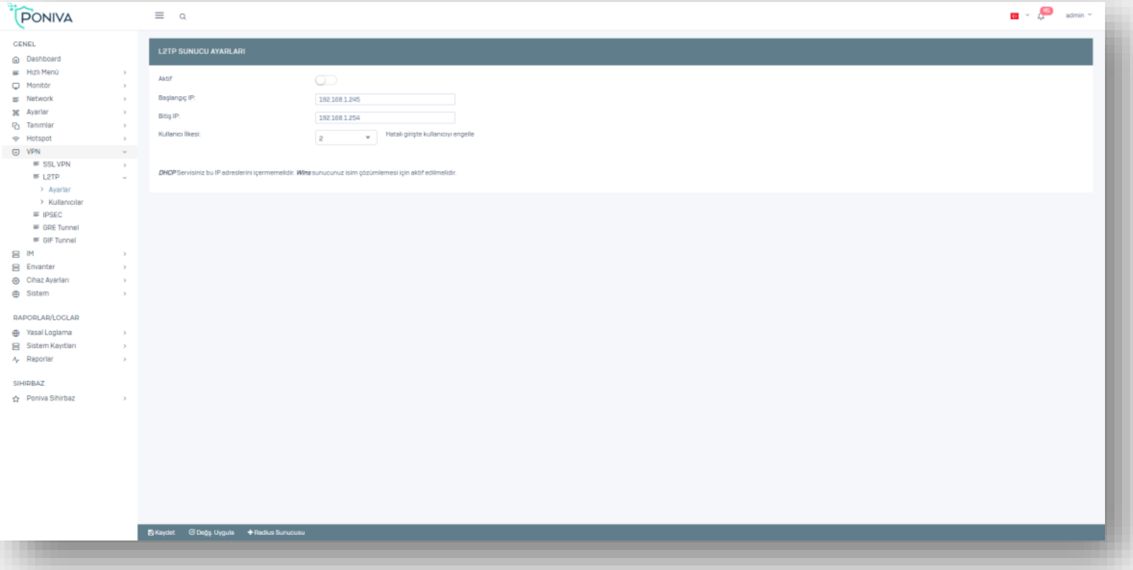
Limit MAC	The user can only connect from the MAC you specify.
MFA	When activated, you need to introduce the QR code through the Google Authenticate application.
Validity	The user can make a vpn connection on the days and times you specify.
Validity Expiry	You can define a duration for the user. After the date you set, this user becomes invalid.

Certificates

Users can connect with the certificate you created.

L2TP

Unlike other VPN protocols, L2TP (Layer 2 Tunnel Protocol) does not provide any privacy or encryption regarding traffic passing over it.



L2TP SUNUCU AYARLARI

Aktif:

Başlangıç IP: 192.168.1.245

Bitiş IP: 192.168.1.254

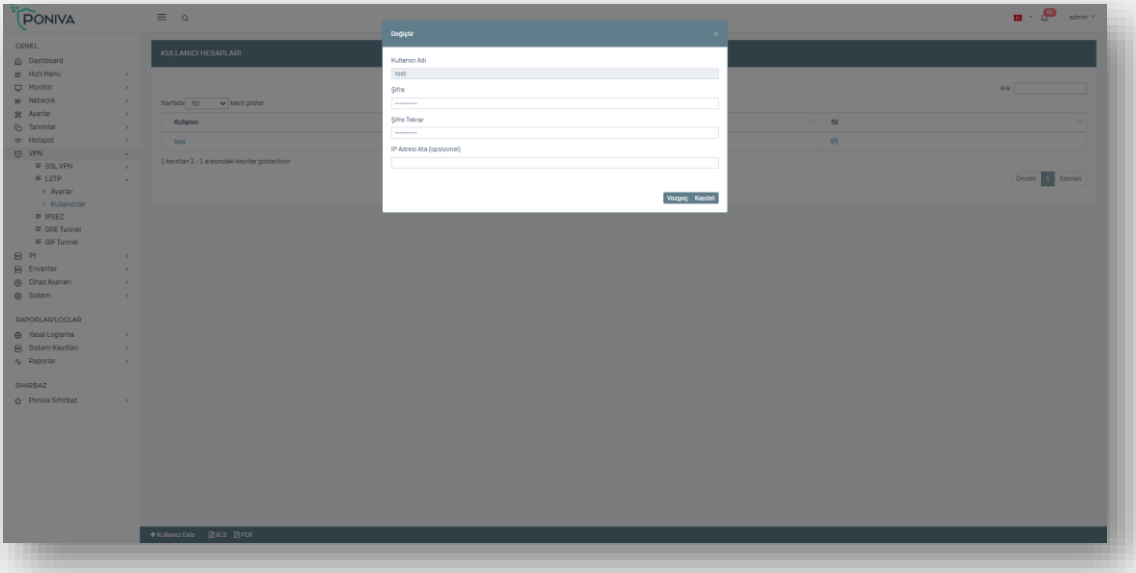
Kullanıcı İlkesi: 2 Hatalı girişte kullanıcıyı engelle

DHCP Servisiniz bu IP adreslerini içermemelidir. *Wins* sunucunuz isim çözümlemesi için aktif edilmelidir.

Settings

	EXPLANATION
Active	You can enable/disable the service.
Starting IP	You must enter a starting IP address.
End IP	You must enter the ending IP address.
User Policy	You can choose how many incorrect logins the user will be blocked.

Users



KULLANICI HESAPLARI

Sayfada 50 kayıt göster

Kullanıcı
test

1 kayıttan 1 - 1 arasındaki kayıtlar gösteriliyor

Değiştir

Kullanıcı Adı: test

Şifre: ••••••••••

Şifre Tekrar: ••••••••••

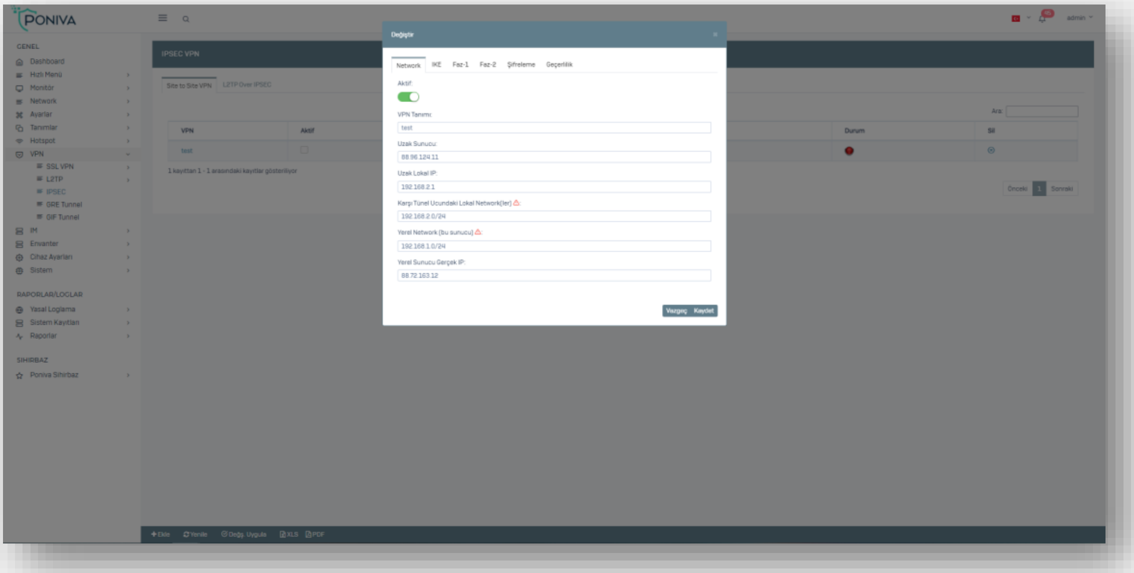
IP Adresi Ata (opsiyonel):

	EXPLANATION
User name	You must enter a username.
Password	You must enter a password.
Assign IP Address (Optional)	You can assign an IP address to the user.

IPSEC

Site to Site VPN

You can connect an entire network to a network in another location.



Aktif:

VPN Tanımı: test

Uzak Sunucu: 88.96.124.11

Uzak Lokal IP: 192.168.2.1

Karşı Tünel Ucundaki Lokal Network(ler): 192.168.2.0/24

Yerel Network (bu sunucu): 192.168.1.0/24

Yerel Sunucu Gerçek IP: 88.72.163.12

	EXPLANATION
Active	You can make the VPN status active/passive.
VPN Definition	You must enter a VPN description.
Remote Server	You must enter the remote server external IP. (For example 88.176.43.57)
Remote Local IP	You must enter the remote local IP. (For example 192.168.1.1)
Local Network at the Opposite Tunnel End	You must enter remote local network. (For example 192.168.1.0/24)
Local Network	You must enter your local network. (For example 192.168.10.0/24)
Local Server Real IP	You must enter the Local Server external IP. (For example 176.88.92.24)
IKE	Default is active.
Output Network	You must select the output network. (Default IGB0)
Protocol	The default ESP is selected.
mode	Default Tunnel is selected.
Exchange/Negotiation Mod	The default main is selected.
Phase-1	3des – md5 – DH1
Phase-2	3des – md5 – NONE
ID Type	ROPE
ID	You must enter an ID in an IP format.
Key	You must enter a key.

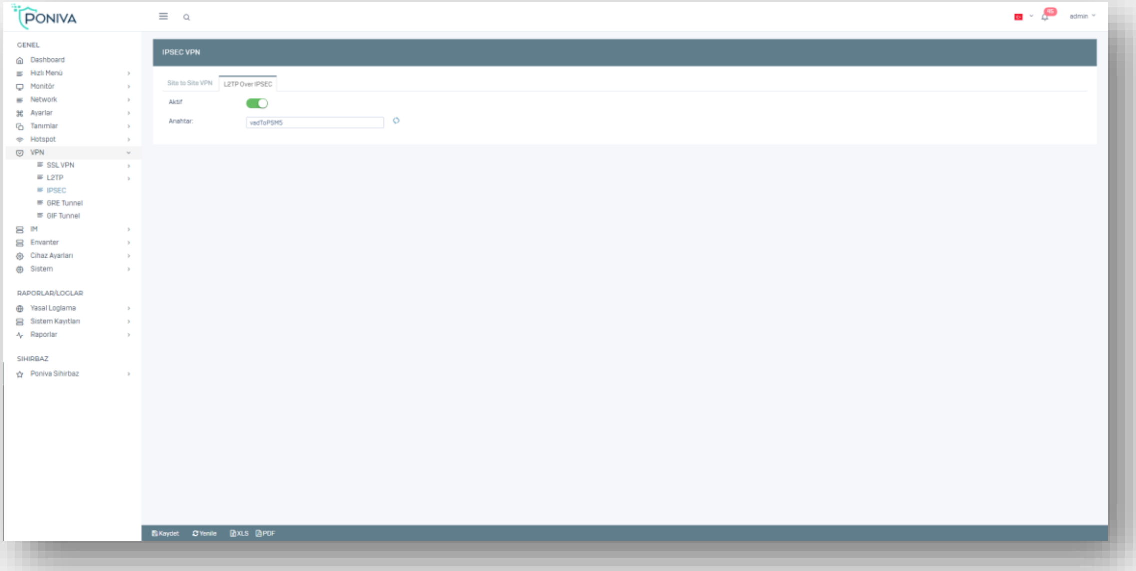
Key Validity Period	You must enter the key validity period. (Default 86400)
Debug Log	Default is Passive. (Activate in any case.)
Validity	The VPN connection works on the days and times you specify.

*You need to make the same settings for the other side.

**Local IPs must not be on the same network.

L2TP Over IPSEC

You can easily create a connection using a Key with the user you will create from the L2TP user section. All modern VPN compatible devices and operating systems have L2TP/IPSEC built in.

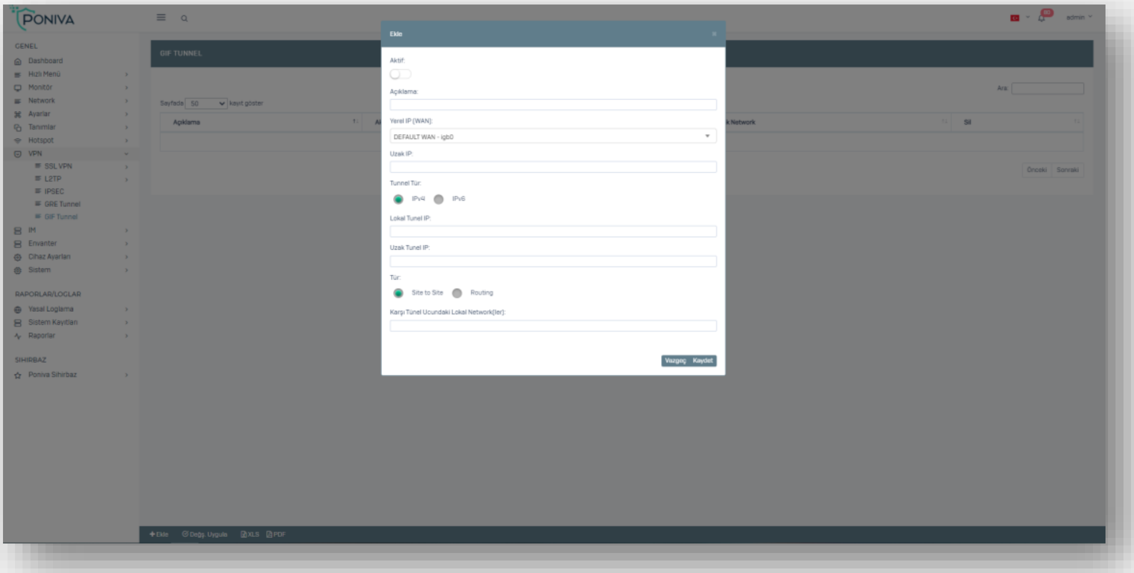


Aktif: ●

Anahtar: vadToPSM5

GIF TUNNEL

It is a method of tunneling traffic between two endpoints without encryption. You can use it to route packets between two locations that are not directly connected and do not require encryption. The GIF tunnel can be used to obtain IPv6 connectivity to a tunnel agent such as Hurricane Electric where IPv6 connectivity is not available.



Ekle

Aktif:

Açıklama:

Yerel IP (WAN): DEFAULT WAN - igb0

Uzak IP:

Tunnel Tür: ● IPv4 ○ IPv6

Lokal Tunel IP:

Uzak Tunel IP:

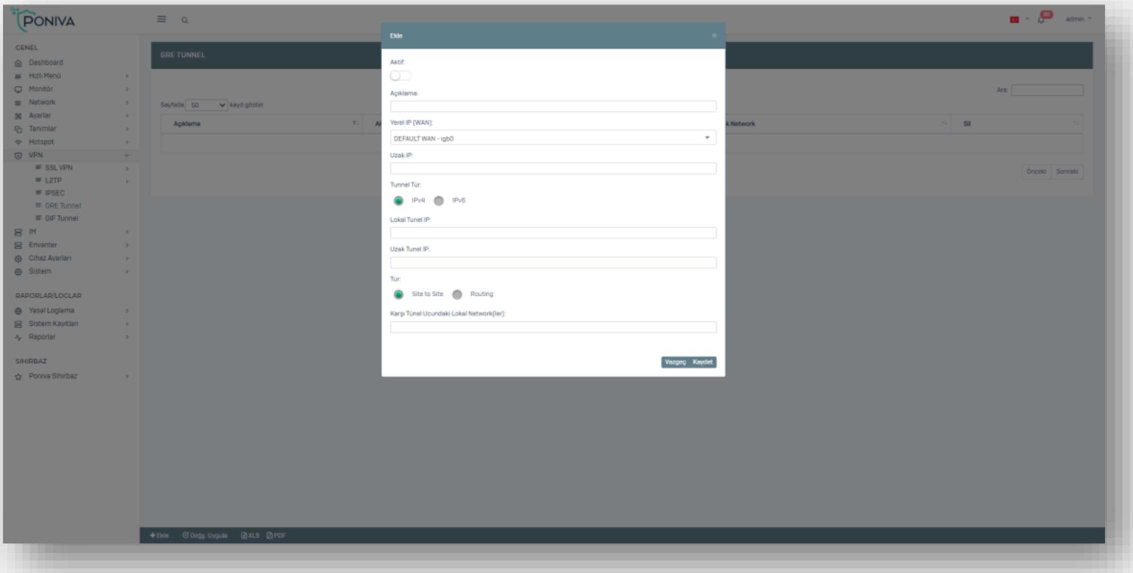
Tür: ● Site to Site ○ Routing

Karşı Tünel Ucundaki Lokal Network(ler):

	EXPLANATION
Active	You can make the VPN status active/passive.
Description	You must enter a description.
Local IP (WAN)	You must choose an interface.
Remote IP	You must enter the remote server external IP. (For example 88.176.43.57)
Tunnel Type	You must select IPv4/IPv6.
Local Tunnel IP	You must enter local tunnel IPv4/IPv6.
Remote Tunnel IP	You must enter the remote tunnel IPv4/IPv6.
Kind	You must select a connection type.
Local Network/Router Gateway at the Opposite Tunnel End	You must enter IPv4/IPv6 according to the tunnel type.
Prefix	If Tunnel type IPv6 is selected, you must select Prefix.

GRE TUNNEL

It is a method of tunneling traffic between two endpoints without encryption. You can use it to route packets between two locations that are not directly connected and do not require encryption. GRE tunnel can carry IPv4, IPv6 or both traffic types at the same time.



Ekle

Aktif:

Açıklama:

Yerel IP (WAN): DEFAULT WAN - igb0

Uzak IP:

Tunnel Tür: ● IPv4 ○ IPv6

Lokal Tunel IP:

Uzak Tunel IP:

Tür: ● Site to Site ○ Routing

Karşı Tünel Ucundaki Lokal Network(ler):

Vazgeç Kaydet

	EXPLANATION
Active	You can make the VPN status active/passive.
Description	You must enter a description.
Local IP (WAN)	You must choose an interface.
Remote IP	You must enter the remote server external IP. (For example 88.176.43.57)
Tunnel Type	You must select IPv4/IPv6.
Local Tunnel IP	You must enter local tunnel IPv4/IPv6.
Remote Tunnel IP	You must enter the remote tunnel IPv4/IPv6.
Kind	You must select a connection type.
Local Network/Router Gateway at the Opposite Tunnel End	You must enter IPv4/IPv6 according to the tunnel type.
Prefix	If Tunnel type IPv6 is selected, you must select Prefix.

IM

With this service, you can activate MSN style communication server and define users.

INVENTORY

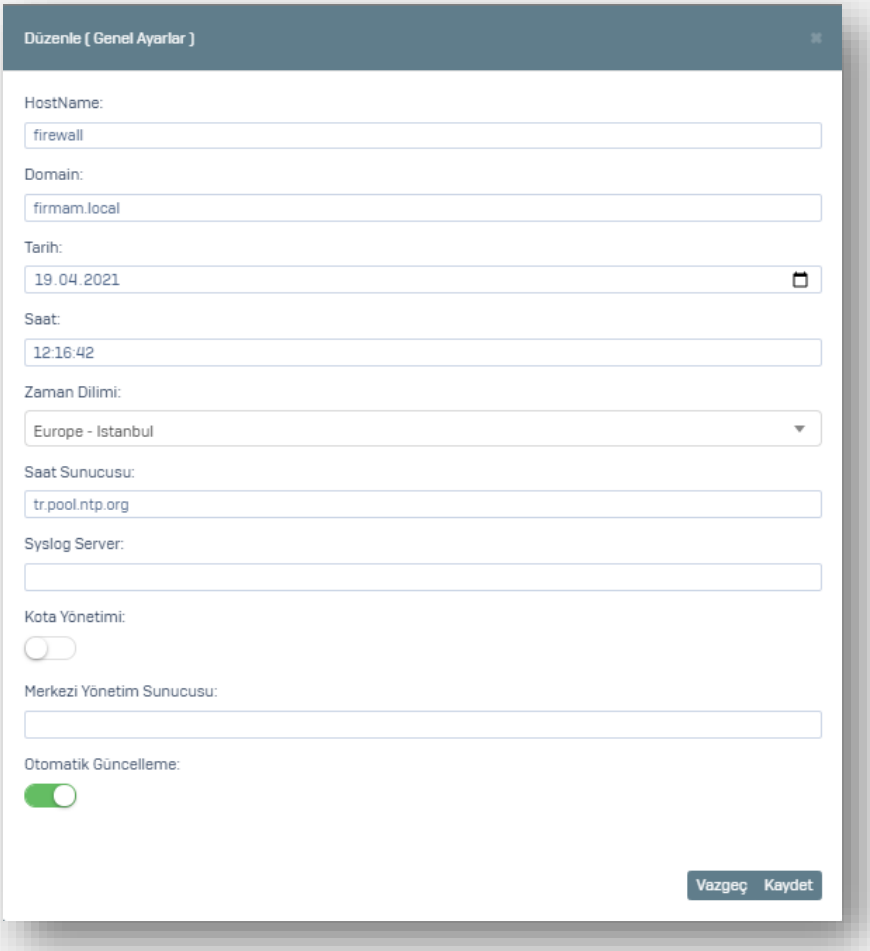
Poniva Client You can monitor the hardware information, installed software and versions on the PCs installed with the software through the firewall.

DEVICE SETTINGS

DEVICE MANAGEMENT

You can configure the general settings of the device in this section.

General Settings



Düzenle (Genel Ayarlar)

HostName: firewall

Domain: firmam.local

Tarih: 19.04.2021

Saat: 12:16:42

Zaman Dilimi: Europe - Istanbul

Saat Sunucusu: tr.pool.ntp.org

Syslog Server:

Kota Yönetimi: ○

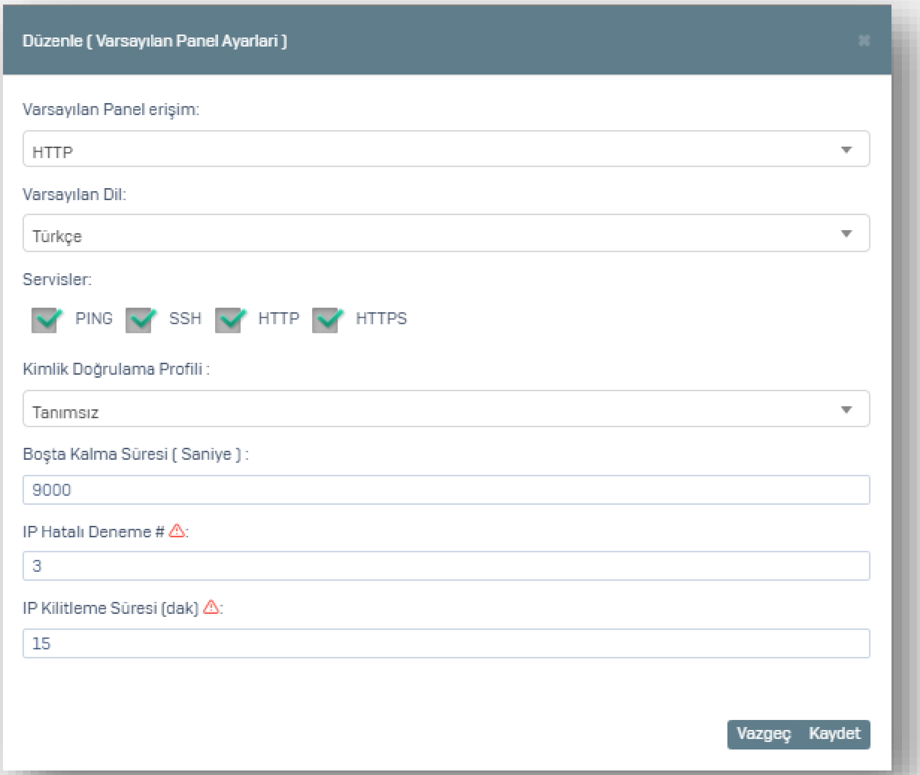
Merkezi Yönetim Sunucusu:

Otomatik Güncelleme: ●

	EXPLANATION
Hostname	firewall
Domain	You must enter a domain. (For example mycompany.local)
Date	You can update your date settings.
Hour	You can update your clock settings.
Time period	You can choose the time zone.
Time Server	You can add a time server.
SyslogServer	You can integrate your Syslog Server.

Quota Management	You can make quota management active/passive.
Central Management Server	You can enter Central Management server.
Automatic Update	When activated, updates are automatically checked.

Panel Management



Düzenle (Varsayılan Panel Ayarları)

Varsayılan Panel erişim: HTTP

Varsayılan Dil: Türkçe

Servisler:

☑ PING ☑ SSH ☑ HTTP ☑ HTTPS

Kimlik Doğrulama Profili : Tanımsız

Boşta Kalma Süresi (Saniye) : 9000

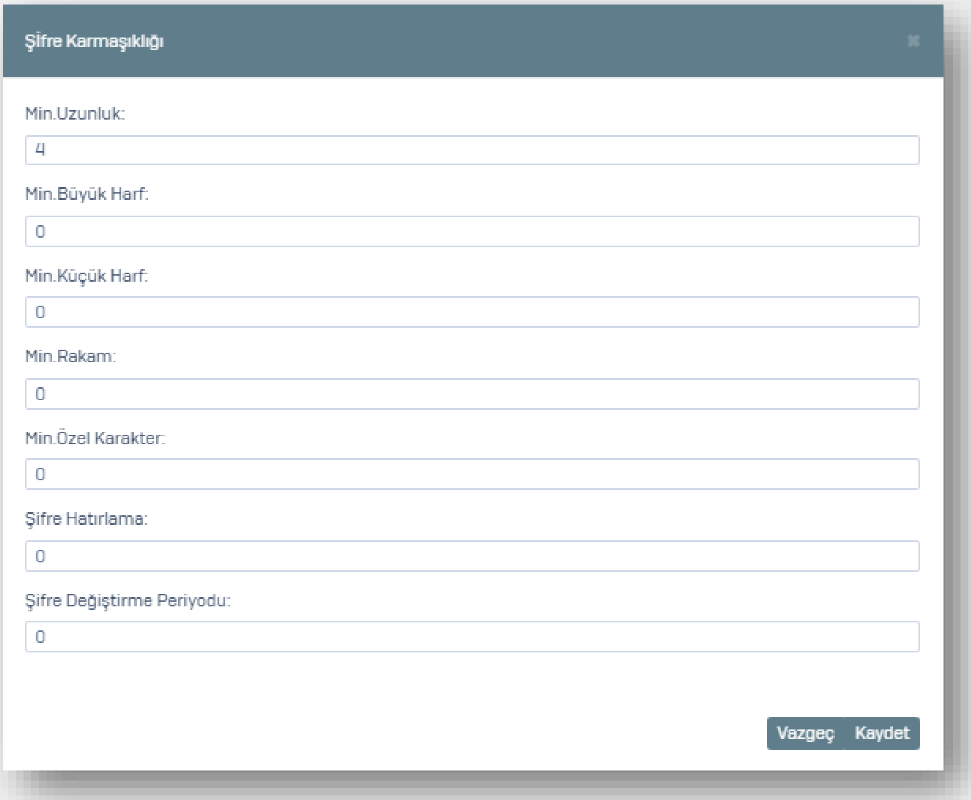
IP Hatalı Deneme # ⚠: 3

IP Kilitleme Süresi (dak) ⚠: 15

	EXPLANATION
Panel Access	You can select the panel access type (HTTP/HTTPS).
Tongue	You can select the default language of the Administration Panel.
Services	You can select the services you want to activate.
Authentication Profile	You can select an authentication profile for default panel accesses.
Idle Time	If no action is taken on the Administration Panel, the time you set will expire and you will be directed to the login screen.
IP Failed Attempt	If no Authentication profile is selected, you may enter an incorrect number of attempts.

IP Lockout Time	If no Authentication profile is selected, you can enter the duration of the ban for the user who filled in the number of incorrect logins.

Password Policy


Şifre Karmaşıklığı

Min.Uzunluk: 4

Min.Büyük Harf: 0

Min.Küçük Harf: 0

Min.Rakam: 0

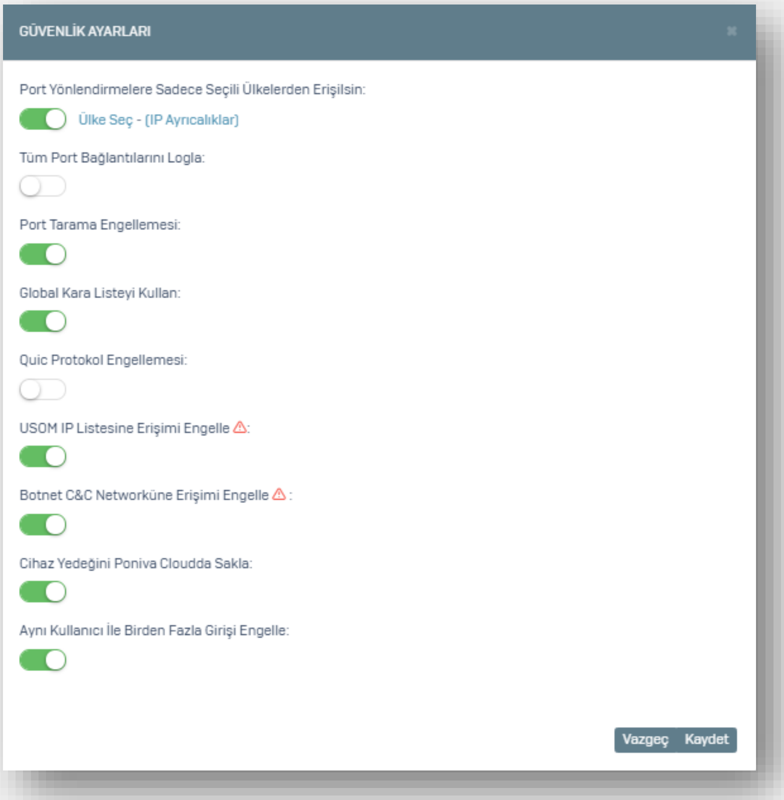
Min.Özel Karakter: 0

Şifre Hatırlama: 0

Şifre Değiştirme Periyodu: 0

	EXPLANATION
min. Length	Min. You can specify the length.
min. Uppercase letter	Min. You can specify the number of Capital Letters.
min. Lower case	Passwords min. You can specify the number of Lowercase Letters.
min. Figure	Min. You can specify the number of digits.
min. Special Character	Min. You can specify the number of Special Characters.
Password Reminder	You can specify the Reminder period of passwords.
Password Change Period	You can specify the Change period of the passwords.

Security Settings



GÜVENLİK AYARLARI

Port Yönlendirmelere Sadece Seçili Ülkelerden Erişilsin:

☑ Ülke Seç - (IP Ayrıcalıklar)

Tüm Port Bağlantılarını Logla:

☐

Port Tarama Engellemesi:

☑

Global Kara Listeyi Kullan:

☑

Quic Protokol Engellemesi:

☐

USOM IP Listesine Erişimi Engelle ⚠:

☑

Botnet C&C Networküne Erişimi Engelle ⚠ :

☑

Cihaz Yedeğini Poniva Cloudda Sakla:

☑

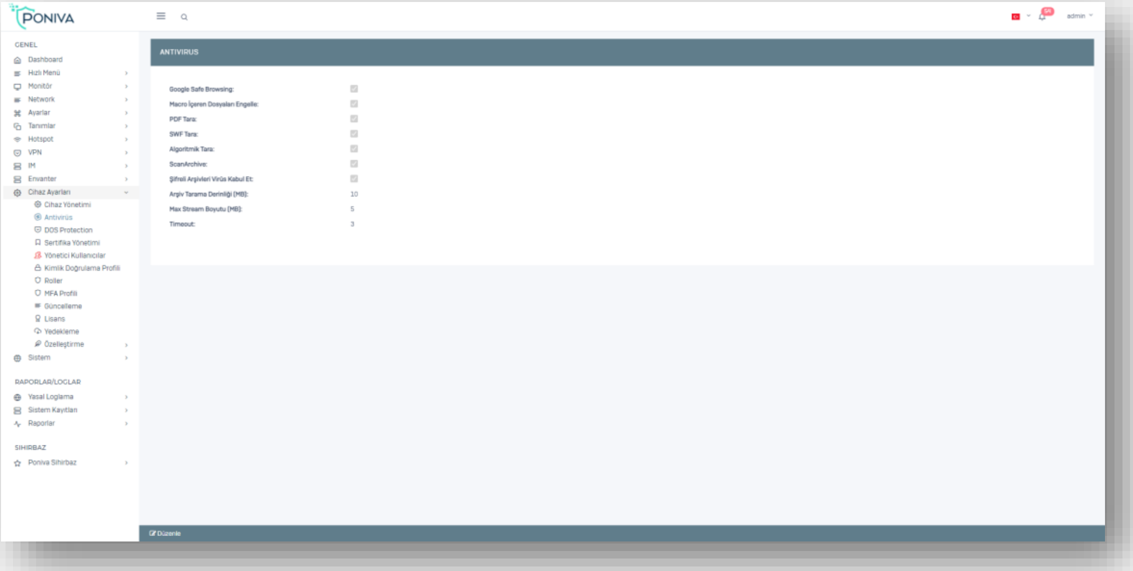
Aynı Kullanıcı İle Birden Fazla Girişi Engelle:

☑

	EXPLANATION
Access Port Forwarding Only from Selected Countries	When activated You can only allow access to the servers you refer to from the countries you choose and prevent attacks from outside. (Default Turkey)
Log All Port Connections	When activated, all port connections are logged.
Port Scan Blocking	When enabled, port scans are blocked.
Use Global Blacklist	When activated, blacklist control is performed for IP addresses.
Quick Protocol Blocking	
Block Access to USOM IP List	When activated, Poniva does not update the USOM IP list.
Block Access to Botnet C&C Network	
Store Device Backup in Poniva Cloud	When activated, your backups are automatically stored in the Poniva Cloud.
Block Multiple Logins with the Same User	When activated, a single login can be made with the same user.

ANTIVIRUS

The settings you configure in this section are applied to groups in which Antivirus is active in group management.



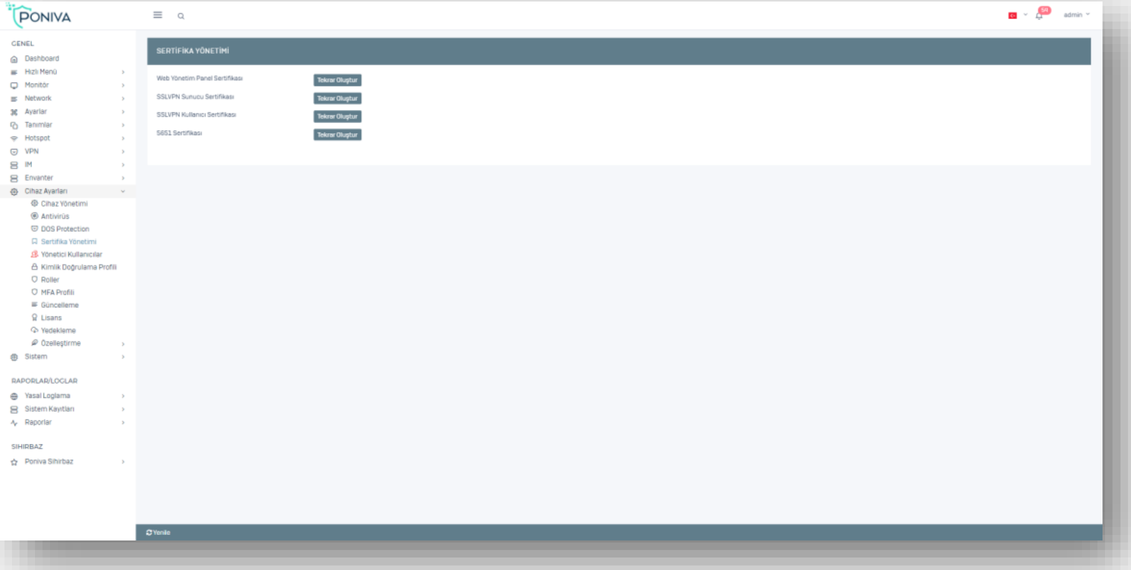
ANTIVIRUS

Google Safe Browsing: ☑
Macro İçeren Dosyaları Engelle: ☑
PDF Tara: ☑
SWF Tara: ☑
Algoritmik Tara: ☑
ScanArchive: ☑
Şifreli Arşivleri Virüs Kabul Et: ☑
Arşiv Tarama Derinliği (MB): 10
Max Stream Boyutu (MB): 5
Timeout: 3

	EXPLANATION
Google Safe Browsing	You can choose to enable/disable the use of the Google safe browsing database.
Block Files Containing Macros	You can block files containing macros.
Scan to PDF	You can change the PDF scan settings.
Scan SWF	You can change ShockWave Flash scan settings.
Algorithmic Scan	You can change algorithmic scan settings.
ScanArchive	You can change the archive scan settings.
Treat Encrypted Archives as Virus	You can treat encrypted archives as viruses.
Archive Scan Depth (MB)	You can select consecutive archive scan depth settings.
Max. Stream Size (MB)	You can specify the size of the archives to be scanned.
timeout	You can set a timeout.

CERTIFICATE MANAGEMENT

In this section you can regenerate your certificates.

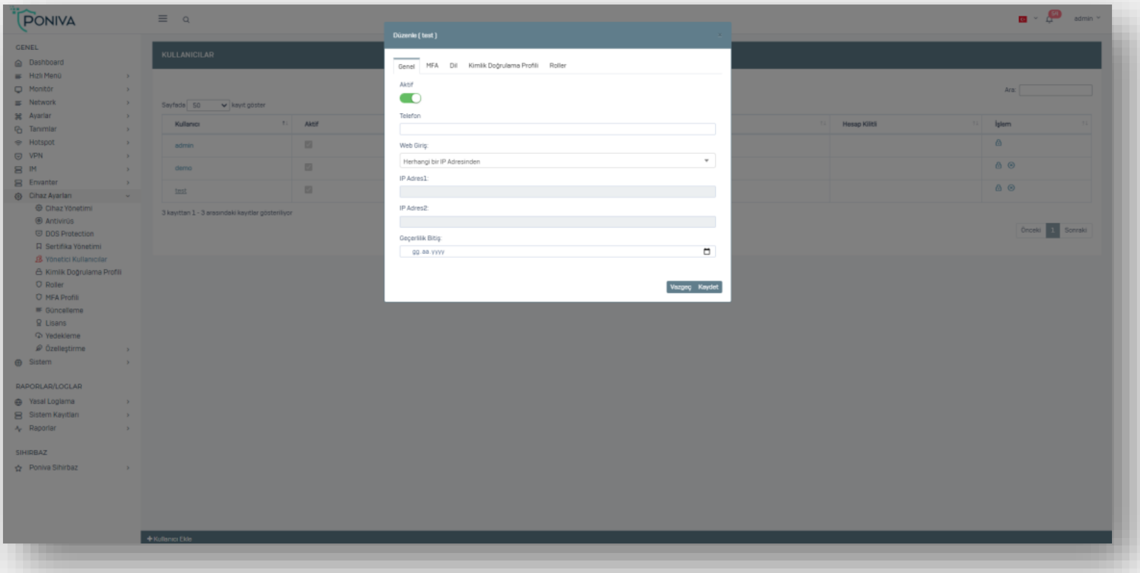


SERTİFİKA YÖNETİMİ

Web Yönetim Panel Sertifikası	Tekrar Oluştur
SSLVPN Sunucu Sertifikası	Tekrar Oluştur
SSLVPN Kullanıcı Sertifikası	Tekrar Oluştur
5651 Sertifikası	Tekrar Oluştur

ADMIN USERS

Poniva Firewall default administrator user is admin. However, you can also define new users for the administration panel and define authorization and roles for these users.



KULLANICILAR

Sayfada 50 kayıt göster

Ara:

Kullanıcı	Aktif	Hesap Kilitli	İşlem
admin	☑		
demo	☑		
test	☑		

3 kayıttan 1 - 3 arasındaki kayıtlar gösteriliyor

Düzenle (test)

Genel | MFA | Dil | Kimlik Doğrulama Profili | Roller

Aktif: ●

Telefon:

Web Giriş: Herhangi bir IP Adresinden

IP Adres1:

IP Adres2:

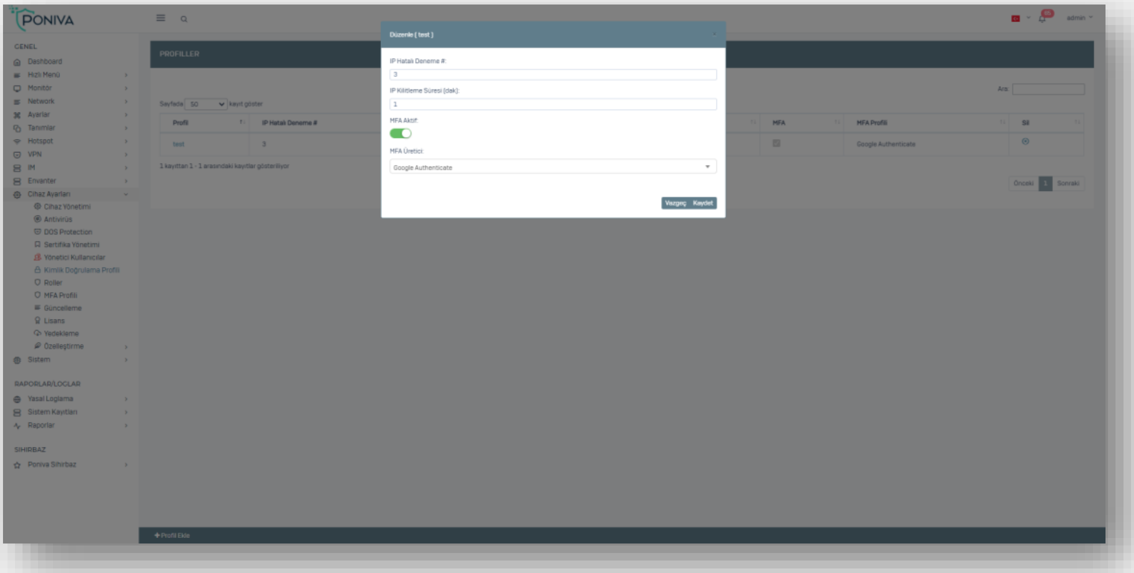
Geçerlilik Bitiş: gg.aa.yyyy

	EXPLANATION
Active	You can select the active/inactive state of the user.
User name	You must enter a username.
Telephone	This field is not required. However, if you are going to use SMS as an authentication profile, you must enter a phone.

Password	You must enter a password for the user.
Change Password on First Login	When activated, the user is directed to the password screen at the first login.
Validity Expiry	You can define a date when the user expires.
Web Login	You can enable the user to access the Administration panel from certain IPs.
MFA	You can use this feature if MFA is active in the authentication profile.
Tongue	You can select the language of the administration panel Turkish/English.
Authentication Profile	You can create a profile for the user.
Roles	You can define authorization and role for the user.

AUTHENTICATION PROFILE

You can create an authentication profile for your users.



Düzenle (test)

IP Hatalı Deneme #: 3

IP Kilitleme Süresi (dak): 1

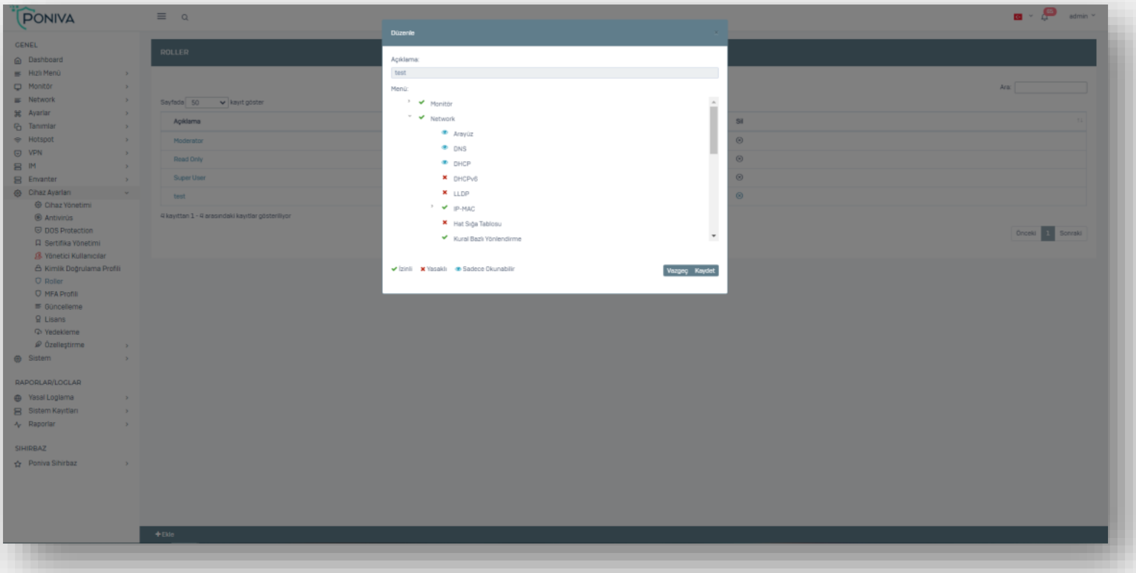
MFA Aktif: ●

MFA Üretici: Google Authenticate

	EXPLANATION
IP Failed Attempt	You can set the number of failed attempts.
IP Lock Time (min)	You can determine how long the system access ban will be after the wrong attempt you have set.
MFA Active	You can choose multi-factor authentication status.
MFA Manufacturer	You can select the definitions in the MFA profile. (Default Google Authenticate)

ROLES

You can define roles for the users you create. Authorizations and sections of the roles can be selected. For example, you can select Allowed, prohibited or readable. You can use the roles you created here in the 'Admin Users' section.



Düzenle

Açıklama: test

Menü:

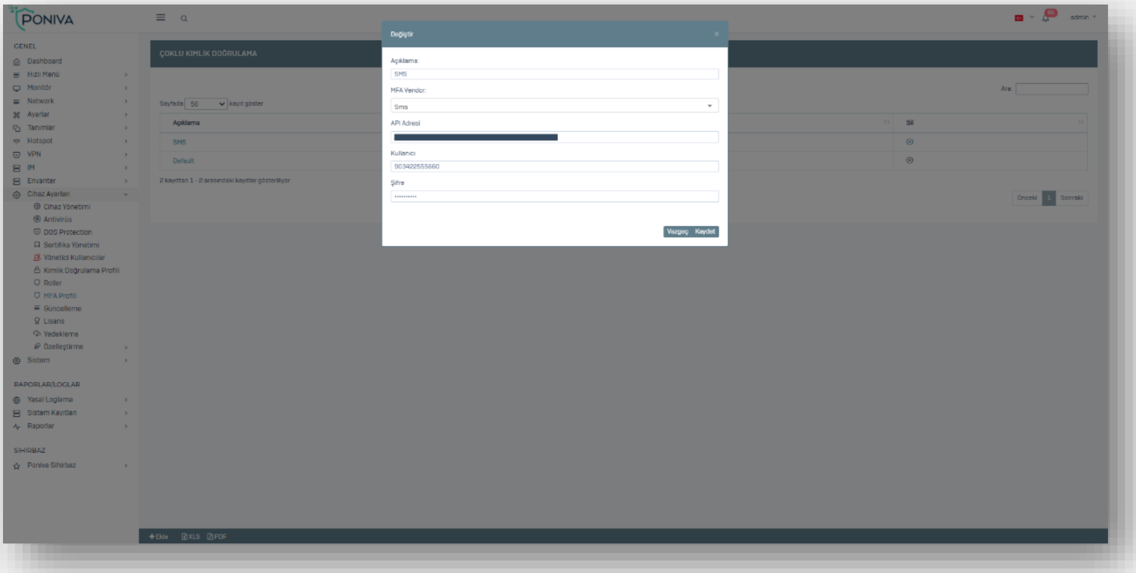
- ✓ Monitör
- ✓ Network
  - 👁 Arayüz
  - 👁 DNS
  - 👁 DHCP
  - ✗ DHCPv6
  - ✗ LLDP
  - ✓ IP-MAC
  - ✗ Hat Sığa Tablosu
  - ✓ Kural Bazlı Yönlendirme

✓ İzinli ✗ Yasaklı 👁 Sadece Okunabilir

	EXPLANATION
Description	You must enter a description.
Menu	In this section, you can select the states of the menus. Allowed -> User can view and make changes. Banned -> User cannot access this page. Can Read Only -> User can view only. It cannot make any changes.

MFA PROFİLE

You can create multiple two-factor authentication profiles in this section. You can use the MFA profiles you created here in the 'Authentication Profile' section.



Değiştir

Açıklama: SMS

MFA Vendor: Sms

API Adresi [redacted]

Kullanıcı 903422555660

Şifre ••••••••••

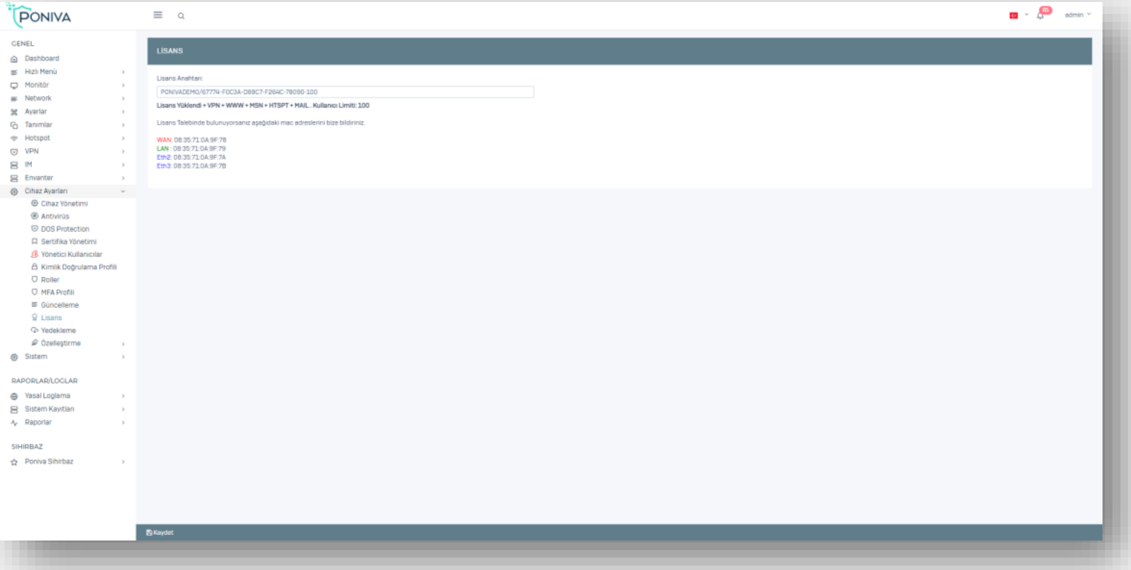
	EXPLANATION
Active	You can select the active/passive status of the profile.
MFA Vendor	You can choose the MFA type. You need to enter the information of the MFA type you have chosen.

UPDATE

You can check the update status of the device from this section.

LICENCE

You can view device license information. (Number of users, features included in the license, etc.)



LİSANS

Lisans Anahtarı:

PONIVADEMO/67774-F0C3A-D89C7-F264C-78090-100

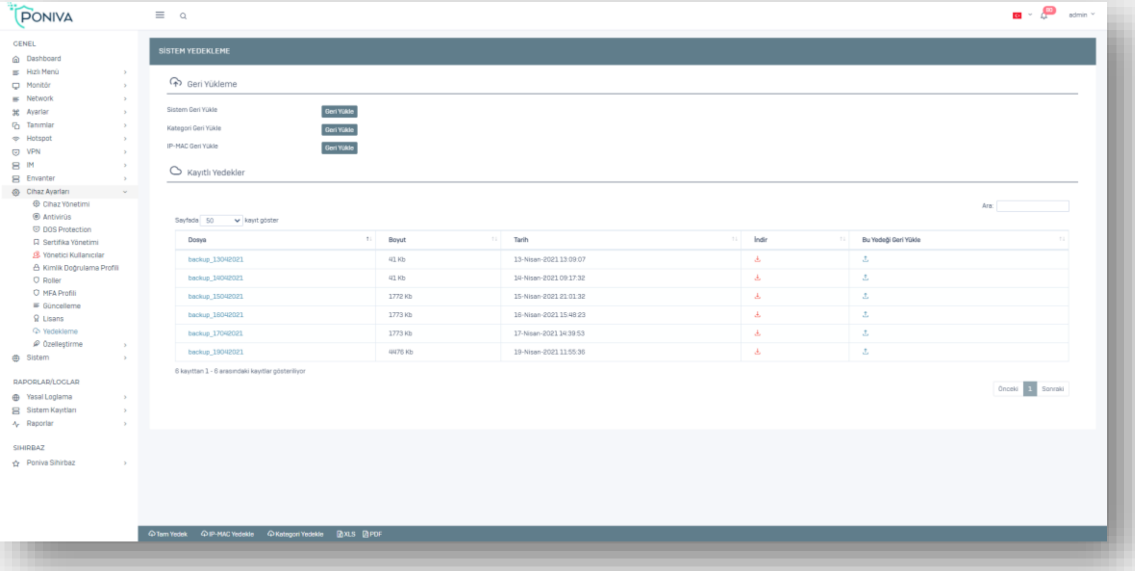
Lisans Yüklendi + VPN + WWW + MSN + HTSPT + MAIL . Kullanıcı Limiti: 100

Lisans Talebinde bulunuyorsanız aşağıdaki mac adreslerini bize bildiriniz.

WAN: 08:35:71:0A:9F:78
LAN : 08:35:71:0A:9F:79
Eth2: 08:35:71:0A:9F:7A
Eth3: 08:35:71:0A:9F:7B

BACKUP

Can backup device configurationand in any case you can easily upload your backups. Messenger records, FTP, WEB and Logging modules are not backed up in backup processes.



SİSTEM YEDEKLEME

Geri Yükleme

Sistem Geri Yükle — Geri Yükle
Kategori Geri Yükle — Geri Yükle
IP-MAC Geri Yükle — Geri Yükle

Kayıtlı Yedekler

Ara:

Sayfada 50 kayıt göster

Dosya	Boyut	Tarih	İndir	Bu Yedeği Geri Yükle
backup_13042021	41 Kb	13-Nisan-2021 13:09:07	⤓	⤒
backup_14042021	41 Kb	14-Nisan-2021 09:17:32	⤓	⤒
backup_15042021	1772 Kb	15-Nisan-2021 21:01:32	⤓	⤒
backup_16042021	1773 Kb	16-Nisan-2021 15:48:23	⤓	⤒
backup_17042021	1773 Kb	17-Nisan-2021 14:39:53	⤓	⤒
backup_19042021	4476 Kb	19-Nisan-2021 11:55:36	⤓	⤒

6 kayıttan 1 - 6 arasındaki kayıtlar gösteriliyor

Önceki 1 Sonraki

CUSTOMIZE

Blocking Page

When a site is blocked, a Firewall blocking message is displayed by default, a message written by you is displayed to users in this section, you can also write a message in html format.

Page Customization

Blocking Page: You can add your own corporate/company logo instead of the default Poniva logo on the blocking screens.

Information Page:You can use this menu for the messages you want to make a diary. For example, you can show users a message that the sites they visit are logged due to law no. 5651. You can also use it here in html format.

Hotspot Page: You can add your own corporate/company logo to the hotspot login screen.

Warning Page

In this section, the message written by you is displayed to the users, you can also write a message in html format.

SYSTEM

SUPPORT

If you have any problems or questions, you can contact our technical team from this section.

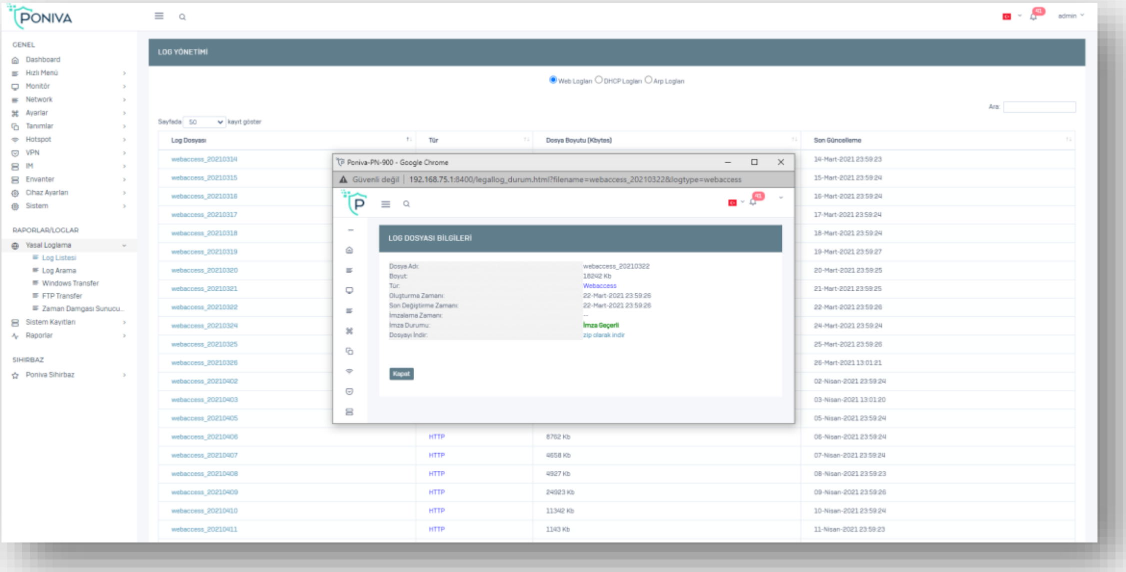
RESTART

You can restart your device from this menu.

LEGAL LOGGING

LOG LIST

Law No. 5651 You can access the appropriate log list here, download and review it on your computer when necessary.



LOG YÖNETİMİ

● Web Logları ○ DHCP Logları ○ Arp Logları

Ara:

Sayfada 50 kayıt göster

Log Dosyası	Tür	Dosya Boyutu (Kbytes)	Son Güncelleme
webaccess_20210314			14-Mart-2021 23:59:23
webaccess_20210315			15-Mart-2021 23:59:24
webaccess_20210316			16-Mart-2021 23:59:24
webaccess_20210317			17-Mart-2021 23:59:24
webaccess_20210318			18-Mart-2021 23:59:24
webaccess_20210319			19-Mart-2021 23:59:27
webaccess_20210320			20-Mart-2021 23:59:25
webaccess_20210321			21-Mart-2021 23:59:25
webaccess_20210322			22-Mart-2021 23:59:26
webaccess_20210324			24-Mart-2021 23:59:24
webaccess_20210325			25-Mart-2021 23:59:26
webaccess_20210326			26-Mart-2021 13:01:21
webaccess_20210402			02-Nisan-2021 23:59:24
webaccess_20210403			03-Nisan-2021 13:01:20
webaccess_20210405			05-Nisan-2021 23:59:24
webaccess_20210406	HTTP	8762 Kb	06-Nisan-2021 23:59:24
webaccess_20210407	HTTP	4658 Kb	07-Nisan-2021 23:59:24
webaccess_20210408	HTTP	4927 Kb	08-Nisan-2021 23:59:23
webaccess_20210409	HTTP	24923 Kb	09-Nisan-2021 23:59:26
webaccess_20210410	HTTP	11342 Kb	10-Nisan-2021 23:59:24
webaccess_20210411	HTTP	1143 Kb	11-Nisan-2021 23:59:23

Poniva-PN-900 - Google Chrome

Güvenli değil | 192.168.75.1:8400/legallog_durum.html?filename=webaccess_20210322&logtype=webaccess

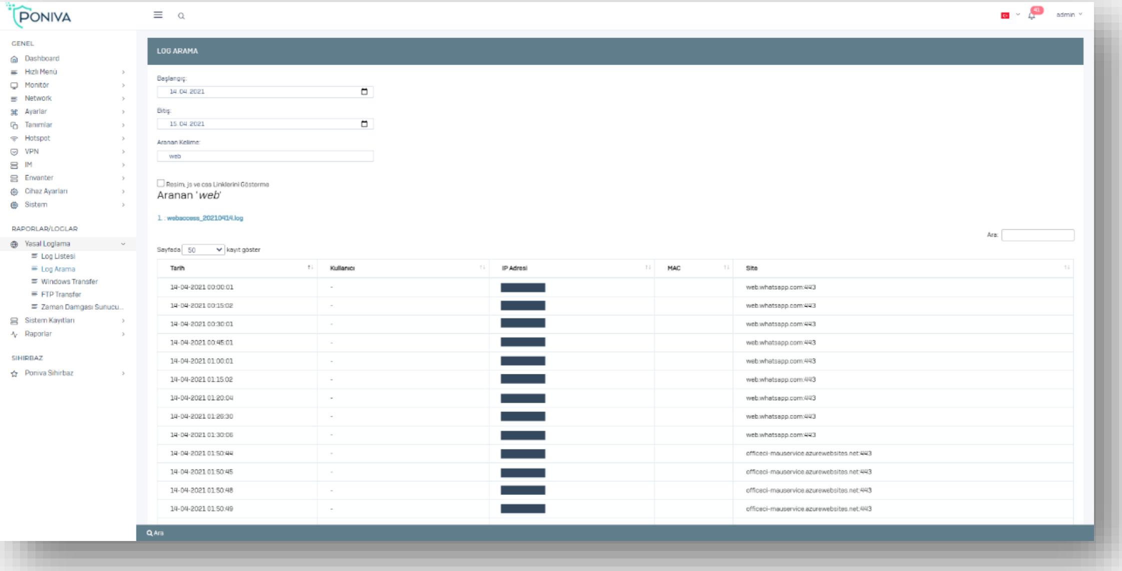
LOG DOSYASI BİLGİLERİ

Dosya Adı:	webaccess_20210322
Boyut:	18242 Kb
Tür:	Webaccess
Oluşturma Zamanı:	22-Mart-2021 23:59:26
Son Değiştirme Zamanı:	22-Mart-2021 23:59:26
İmzalama Zamanı:	--
İmza Durumu:	İmza Geçerli
Dosyayı İndir:	zip olarak indir

Kapat

LOG SEARCH

You can view your logs by filtering the words you are looking for between the dates you specify.



LOG ARAMA

Başlangıç: 14.04.2021

Bitiş: 15.04.2021

Aranan Kelime: web

☐ Resim, js ve css Linklerini Gösterme

Aranan '*web*'

1. : webaccess_20210414.log

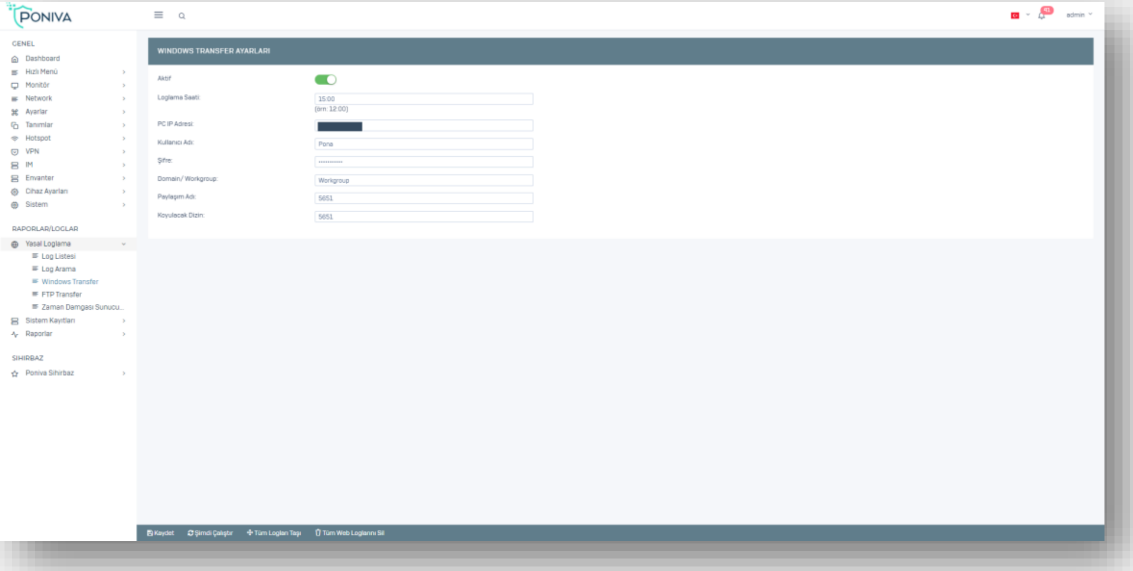
Sayfada 50 kayıt göster

Ara:

Tarih	Kullanıcı	IP Adresi	MAC	Site
14-04-2021 00:00:01	-	[redacted]		web.whatsapp.com:443
14-04-2021 00:15:02	-	[redacted]		web.whatsapp.com:443
14-04-2021 00:30:01	-	[redacted]		web.whatsapp.com:443
14-04-2021 00:45:01	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:00:01	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:15:02	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:20:04	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:26:30	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:30:06	-	[redacted]		web.whatsapp.com:443
14-04-2021 01:50:44	-	[redacted]		officeci-mauservice.azurewebsites.net:443
14-04-2021 01:50:45	-	[redacted]		officeci-mauservice.azurewebsites.net:443
14-04-2021 01:50:48	-	[redacted]		officeci-mauservice.azurewebsites.net:443
14-04-2021 01:50:49	-	[redacted]		officeci-mauservice.azurewebsites.net:443

WINDOWS TRANSFER

your logs You can transfer it daily to a PC share on your network via Windows Transfer at the time you specify automatically.



WINDOWS TRANSFER AYARLARI

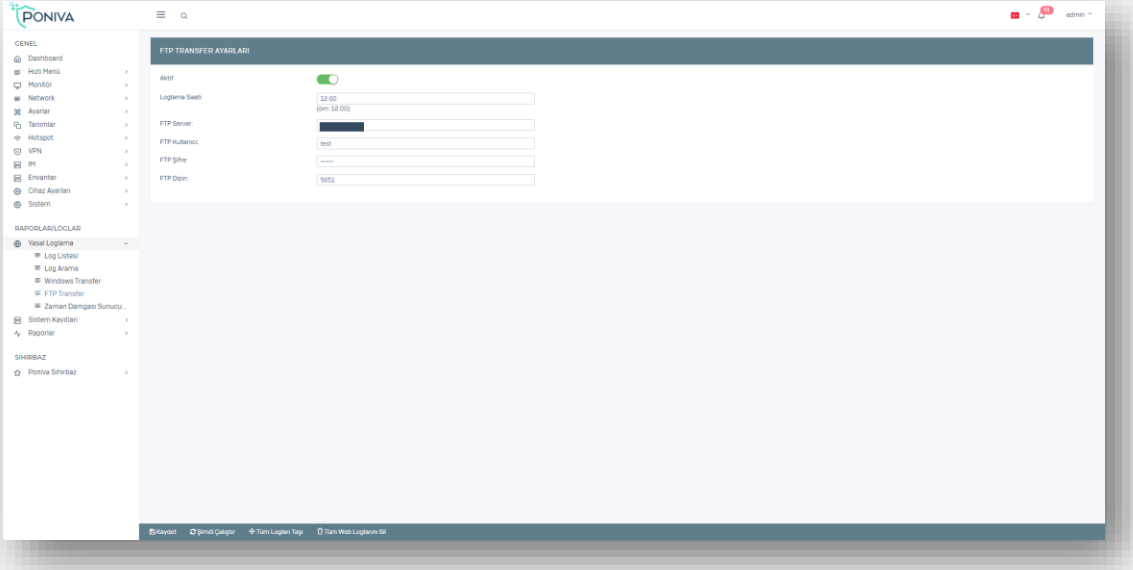
Aktif	●
Loglama Saati:	15:00 (örn: 12:00)
PC IP Adresi:	[redacted]
Kullanıcı Adı:	Pona
Şifre:	··········
Domain/ Workgroup:	Workgroup
Paylaşım Adı:	5651
Koyulacak Dizin:	5651

	EXPLANATION
Active	You can enable/disable the service.
Logging Hour	You can make the transfer at the time you specify.

PC IP Address	You must enter your computer's IP address.
User name	You must enter the Username on your computer.
Password	You must enter your computer password. If you do not have a password, you must create one.
Domain/Workgroup	You must enter your computer's Domain/Workgroup information.
Share Name	You must enter the name of the share folder on your computer where you will save the logs.
Index to Put	You must enter the directory information on your computer where you will save the logs.

FTP TRANSFER

your logs You can automatically transfer it to your FTP server at the time you specify.



FTP TRANSFER AYARLARI

Aktif: ●

Loglama Saati: 12:00 (örn: 12:00)

FTP Server: [redacted]

FTP Kullanıcı: test

FTP Şifre: ••••••

FTP Dizin: 5651

	EXPLANATION
Active	You can enable/disable the service.
Logging Hour	You can make the transfer at the time you specify.
FTP Server	You must enter the FTP Server IP address.
FTP Username	You must enter the FTP username.
FTP Password	You must enter your FTP password.
FTP Directory	You must enter the directory information where you will save the logs on your FTP Server.

TIMESTAMP SERVER

If you want to use a different timestamp server (an approved timestamp like TUBITAK), you must activate this service and fill in the required fields.

SYSTEM LOGS

	EXPLANATION
Attack Detection	A list of incoming and blocked traffic to your system.
Links	A log list of connections made from your system.
Service Logs	Firewall services related log list.
Web Blocking	List of Blocked Sites and records related to the reason for being blocked.
Important Events	License, List of Attack records.
Harp Logs	IP-MAC mapping, list of IP conflict related records.
Network Status	List of records related to the status of your network cable.
SSL VPN Logs	List of SSL VPN connections.
Trojan Logs	List of records related to users using P2P/Tunel on your network.
NETSEC Logs	List of hotspot login/logout records.
Incorrect Mail Entries	List of records related to incorrect mail, password attempts.
Mail Logins	List of IP based mail login records.
Audit Logs	Detailed list of records of firewall operations (add, delete, update).

REPORTS

Here you can generate a report for the type of reporting you want, for the time period you specify, and for all users/a specific IP.

	EXPLANATION
Total Traffic	Creates a graph of the total Inbound/Outbound traffic.
Average Traffic (bytes/sec)	Generates a graph of average Inbound/Outbound traffic.
Http(s) Traffic	Creates a graph of Inbound/Outbound Https traffic.
DNS Traffic	Generates a graph of Inbound/Outbound DNS traffic.
Mail Traffic	Creates a graph of Incoming/Outgoing Mail traffic.
FTP Traffic	Generates a graph of Inbound/Outbound FTP traffic.
Other Traffic	Creates a graph of other incoming/outgoing traffic.
Top 10 User Traffic	Graphs the traffic generated by the top 10 users (IP).
Top 10 User Traffic (bytes/sec)	Graphs the traffic generated by the top 10 users (IP).

Total Transfer	It generates a report with Clock, Outgoing, Incoming and Total transferred bytes.
User Traffic	It generates a report containing traffic information generated by users (IP).
Detailed User Site Logins	Generates a report of users' detailed web logins.
Real Time Usage	You can monitor instant web logins.

INFORMATION

When you activate the service, it automatically sends your reports to your e-mail address as often as you specify.

PONIVA WIZARD

If you want to make a quick installation on the device, you can do it by following the steps in this section.