PONIVA
FIREWALL

Kurulum ve Yönetim Kılavuzu

v5.0.0.7



İÇİNDEKİLER

KURULUM 5
Manuel Kurulum 6
FIREWALL KULLANICI REHBERİ 11
Dashboard 11
Genel Durum 11
Siber Harita 11
CPU/RAM Durumu 11
Bant Kullanımı 11
En Fazla Girilen Siteler 12
Download/Upload Grafikleri 12
Aktif Yöneticiler 12
Cihaz Listesi 13
Tehdit İzleme 13
Monitör 14
Network 14
VPN 14
Kontroller 15
Hotspot Kullanıcı 15
Log İzleme 15
Servisler 16
Network 16
Arayüz 16
WAN Ayarları 17
LAN Ayarları 18
PPPOE Ayarları 20
VLAN 21
Hardware Switch 21
Redundant 22
Loopback 23
Virtual Wire 24
Zone 25
DNS 25
DHCP 26
Dhcp Server 26
Dhcp Relay 27

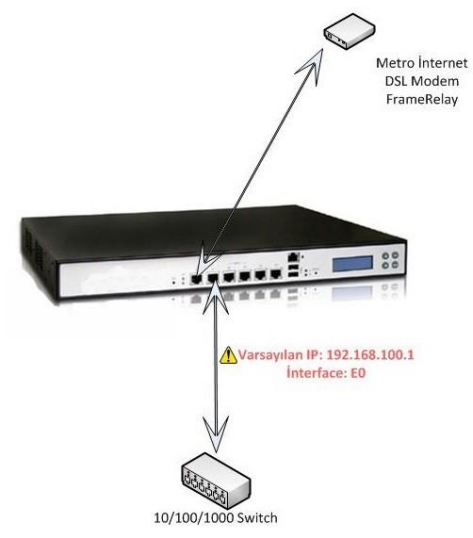
DHCPv6 28
Dhcpv6 Server 28
Dhcpv6 Relay 29
LLDP 30
IP-MAC 31
Ayarlar 31
IP-MAC Atama 32
SD-WAN 32
Ayarlar 32
Kural Bazlı Yönlendirme 33
Port Yönlendirme 34
Sanal IP 35
Yönlendirme 36
Virtual Routers 36
Netflow 37
Ayarlar 37
NAC 37
IDS/IPS 38
Bant Genişliği 39
Ayarlar 39
Tanım 39
Kurallar 40
Ayrıcalık 41
Firewall Kuralları 42
Grup Yönetimi 43
Web Filtreleme 45
DNS Firewall 45
Dosya Filtreleme 46
Uygulama Kontrol 46
Uygulama Engelle 46
Karantina 47
Tanımlar 47
Active Directory 48
Adresler 48
Adres Grupları 48
Dinamik Site Kategorileri 49
Güvenli Siteler 50

Güvenli IP'ler 50
Servisler 50
Site Kategorileri 50
SSL Ayrıcalık 51
Zaman Tanımları 51
VPN 52
SSL VPN 52
Ayarlar 52
Kullanıcılar 54
Sertifikalar 56
L2TP 56
Ayarlar 57
Kullanıcılar 57
IPSEC 57
Site to Site VPN 57
Cisco 59
IPSEC Remote Access 60
GIF Tunnel 61
GRE Tunnel 62
VPN Locatıon map 62
Turkuaz 62
Hotspot 62
Ayarlar 62
Ayrıcalık 64
Entegrasyon 64
Kullanıcılar 64
Kullanıcı Mac Kontrol 64
Anketler 64
Toplu İşlemler 64
İşlemler 64
CSV Import 65
Envanter 65
Cihaz Ayarları 65
Active Directory 65
Antivirüs 66
Bilgilendirme 67
Ayarlar 67

Mail 68
Telegram 68
Cihaz Yönetimi 69
Genel Ayarlar 69
Panel Yönetimi 70
Şifre Politikası 71
Güvenlik Ayarları 72
Servisler 73
Syslog Ayarları 74
Güncelleme 74
Kimlik Doğrulama Profili 75
Lisans 76
MFA Profili 76
Mobil Yönetim 77
Özelleştirme 77
Engelleme Sayfası 77
Bilgilendirme/Uyarı Sayfası 77
Sayfa Özelleştirme 77
Roller 77
Sertifika Yönetimi 78
Yedekleme 78
Yönetici Kullanıcılar 79
Sistem 80
Yeniden Başlat 80
Cihazı Kapat 80
Sistem Kayıtları 80
Web Log Arama 80
Yasal loglama 81
Log Transfer 81
Windows Transfer 82
FTP Transfer 82
USB Transfer 82
Zaman Damgası Sunucusu 83
Sistem Logları 83
Raporlar 84

KURULUM

1. Cihazın E0 Ethernet portundan DSL Modem/Router cihazınıza bir kablo takın.
2. Cihazın E1 portundan ağınızdaki Switch ya da bilgisayarınıza bir kablo takın.



Cihazınızın varsayılan IP adresi **192.168.100.1** 'dir.
Web Yönetim Paneline https://192.168.100.1:8401 veya http://192.168.100.1:8400 adresinden erişebilirsiniz.

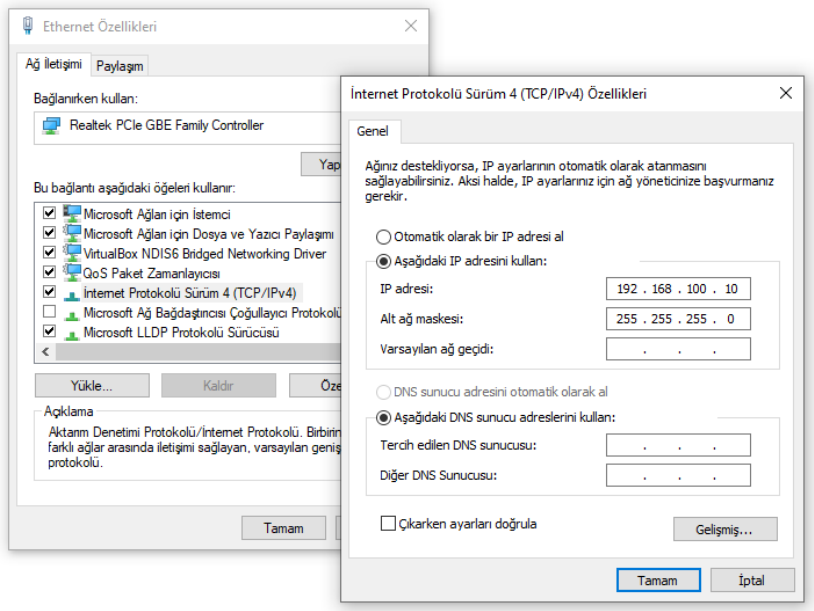
Varsayılan **Kullanıcı:** admin **Şifre:** admin 'dir.

Ağınızdaki IP bloğunuzu değiştirmek istemiyorsanız kuruluma başlamadan önce modeminizin IP adresini farklı bir blok ile değiştirmeniz gerekmektedir.

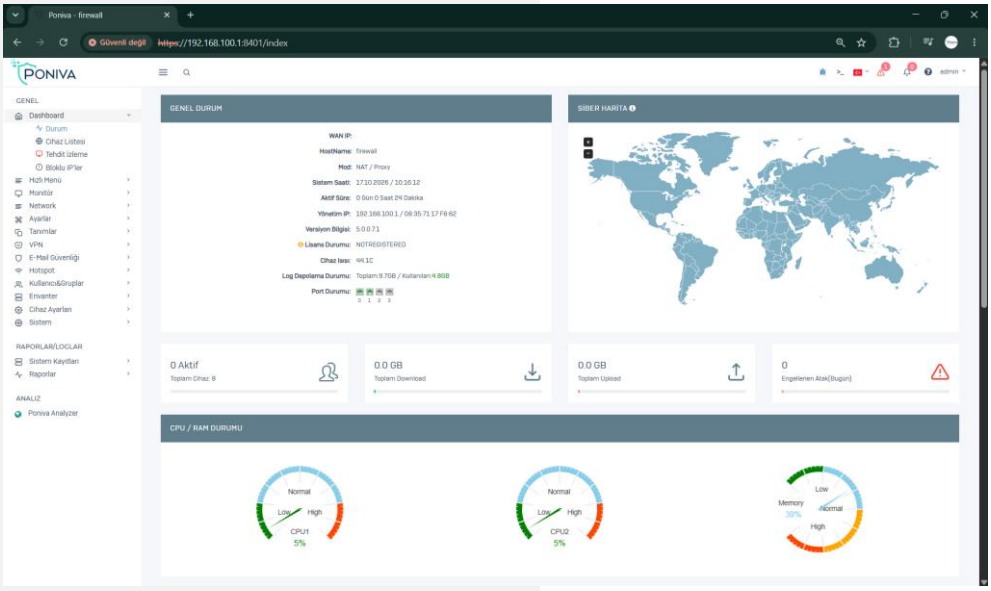
Örneğin; modeminizin IP adresi 192.168.1.1 ise Firewall cihazınızı devreye almadan önce modemin IP adresini 192.168.3.1 olarak değiştirin ve modeminizin ayarlarının aktif olması için kapatıp açın.

Bağlantı işlemimiz tamamlandı artık ilk kurulum ayarlarını yapabiliriz.

Kurulum için bilgisayarımızın IP adresi Firewall cihazının ağında bir IP adresine sahip olması gerekmektedir, bunun için bilgisayarımıza yeni otomatik IP aldırmalı ya da manuel olarak aşağıdaki gibi IP tanımlamamız gerekmektedir.



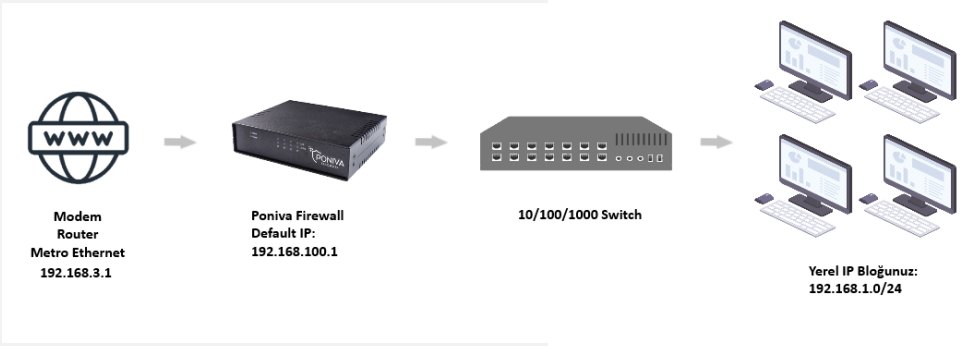
IP tanımlama işlemi bittikten sonra tarayıcımızı açıyoruz ve **https://192.168.100.1:8401** veya **http://192.168.100.1:8400** yazıyoruz. (Internet Explorer ile http üzerinden erişim sağlamak için "http:// " yazmanız gerekmektedir.)



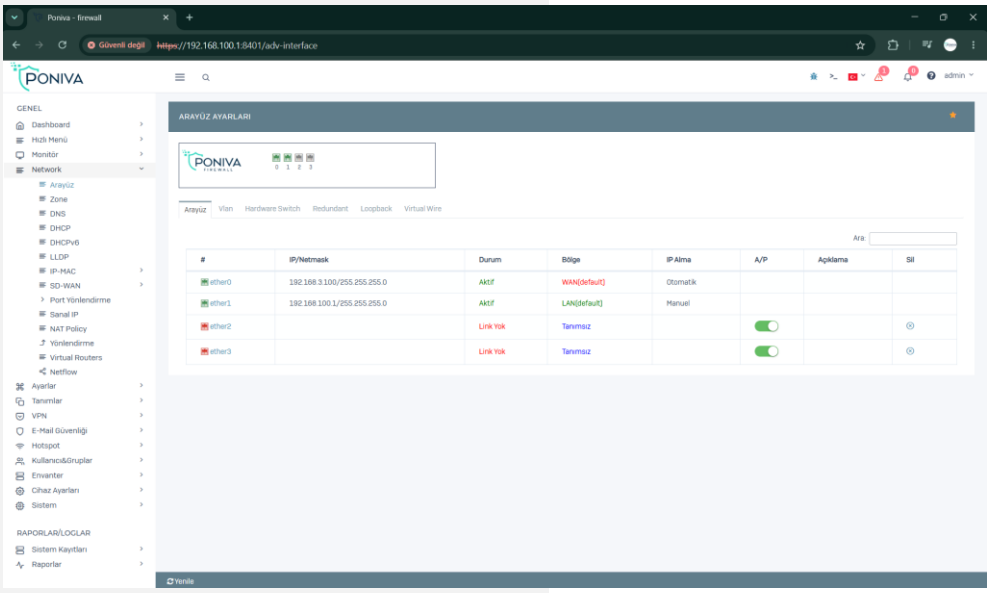
Firewall arayüzüne giriş yaptıktan sonra kuruluma "***Manuel***" olarak devam edebilirsiniz.

MANUEL KURULUM

Yerel ağınızın 192.168.1.0/24 ve modem IP adresinin 192.168.3.1 olduğu varsayılarak devam edilecektir.

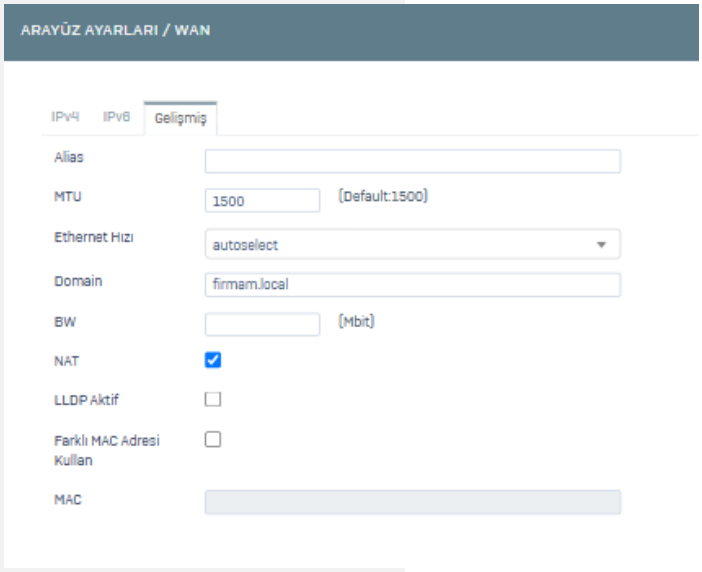


Network -> Arayüz menüsüne tıklıyoruz.



Açılan pencerede ether0 (Varsayılan WAN interface) üzerine tıklayarak ayarlarını yapılandırmaya başlıyoruz.





Network bölümünde,

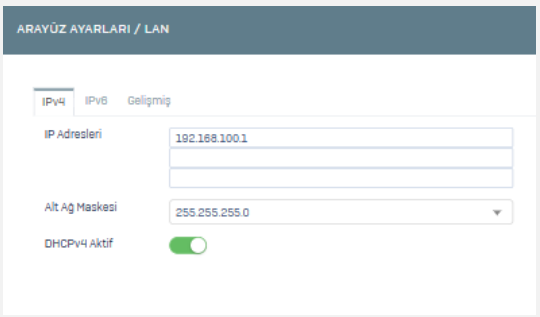
- Bağlantı türünü IP adresimizi otomatik, manuel ya da bridge mod tanımlaması için PPPOE seçiyoruz (biz bu örnekte manuel kurulum gerçekleştirdiğimiz için manuel seçerek devam ediyoruz),
- IP Adresi kısmına 192.168.3.100 giriyoruz (Siz 192.168.3.1 hariç bir IP tanımlayabilirsiniz.),
- Alt Ağ maskesi özel bir durum yok ise 255.255.255.0 giriyoruz,
- Varsayılan ağ geçidi Modem/Router IP adresidir, modemimizi 192.168.3.1 ayarladığımız için buraya modem IP adresini giriyoruz.
- Servisler bölümünde PING, WEB YÖNETİM varsayılan aktif gelir.

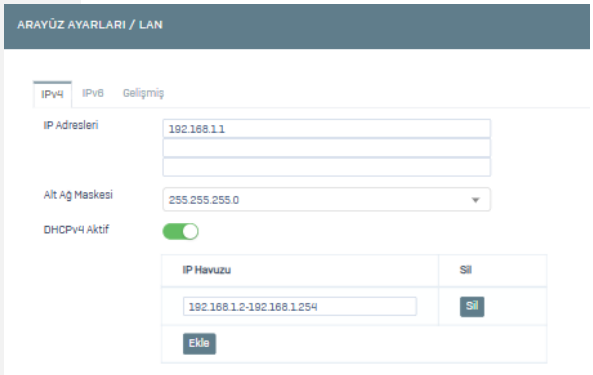
Gelişmiş bölümüne tıklayarak;

- Domain ismi kısmına Türkçe karakter kullanmadan bir tanım yapabilirsiniz. (örn: firmam.local)
- MTU değerini 1500 olarak kalıyor. (DSL hatlar için MTU değeri 1492 olmalıdır.),
- Kaydet diyerek bu ekrandan çıkıyoruz.

Network WAN ayarlarımız tamamlandı.

Şimdi sıra yerel ağımızın konfigürasyonunda, ether1 (Varsayılan LAN interface) üzerine tıklayarak ayarlarını yapılandırmaya başlıyoruz.

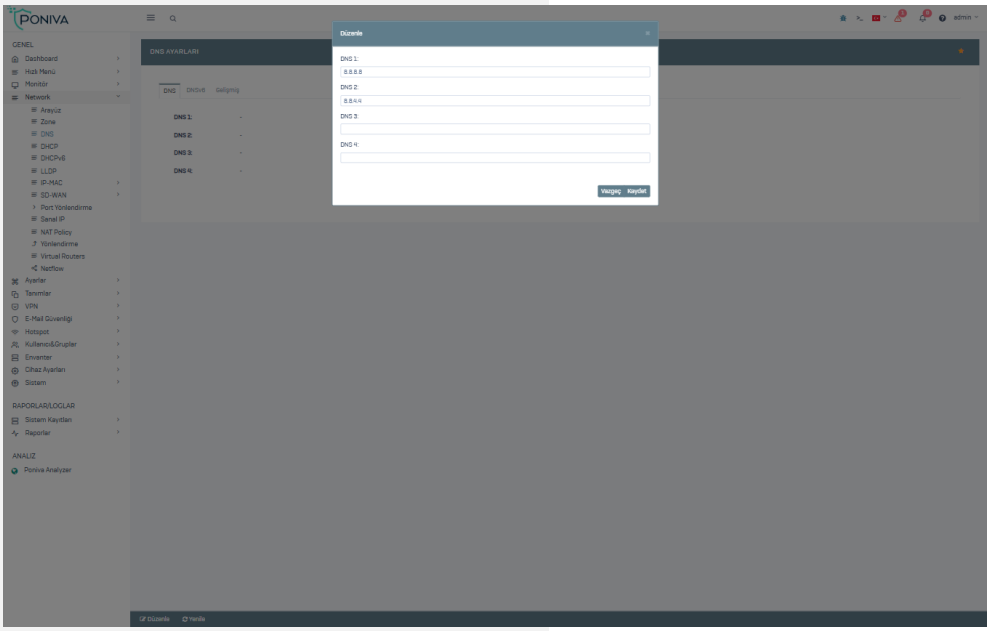




- Modemimizin eski IP adresi 192.168.1.1 olduğundan 192.168.100.1 yazan yeri 192.168.1.1 olarak değiştiriyoruz,
- Alt ağ maskesi özel bir durum yok ise 255.255.255.0 olarak kalmalıdır,
- DHCP servisini aktif edebilirsiniz, eğer IP adresinizi başka bir DHCP sunucusu dağıtacaksa ya da bu servisi çalıştırmak istemiyorsanız pasif olarak bırakabilirsiniz,
- Kaydet diyerek bu ekrandan çıkıyoruz.

Network LAN ayarlarımız tamamlandı.

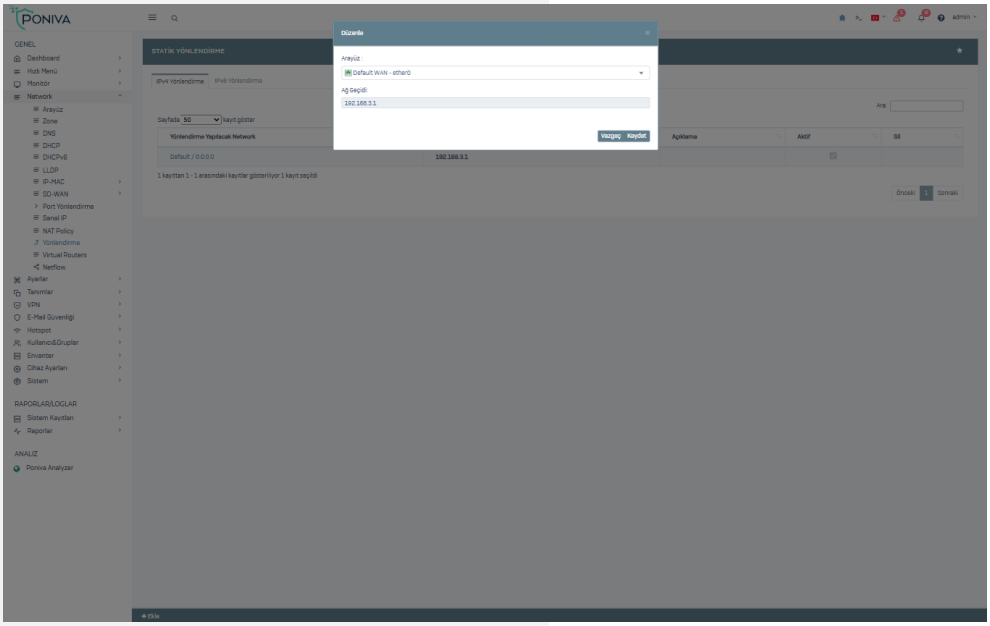
Network -> DNS menüsüne tıklayarak DNS ayarlarını yapılandırmaya başlıyoruz.



- DNS sunucuları kısmına Google sunucularını (8.8.8.8, 8.8.4.4), Modeminizi ya da farklı bir DNS sunucusu yazabilirsiniz. (Örneğin; Türk Telekom ya da Superonline sunucularını da yazabilirsiniz.)

DNS ayarlarımız tamamlandı.

Network -> Yönlendirme menüsüne tıklayarak Yönlendirme ayarlarını yapılandırmaya başlıyoruz.



- Burada Default değeri modem/Router ya da PPPOE ağ geçidi IP adresi yazmalıdır.

Yönlendirme ayarlarımız tamamlandı.

Eğer tanımlarımızda bir sorun yok ise cihazı yeniden başlattıktan sonra firewall'un interneti aktif hale gelecektir.

Artık yeni IP adresimizi (https://192.168.1.1:8401 veya http://192.168.1.1:8400) yazarak arayüze erişebiliriz.

Cihazın kurulum işlemi tamamlandıktan sonra lisans işlemleri için portala kaydının yapılması gerekmektedir.

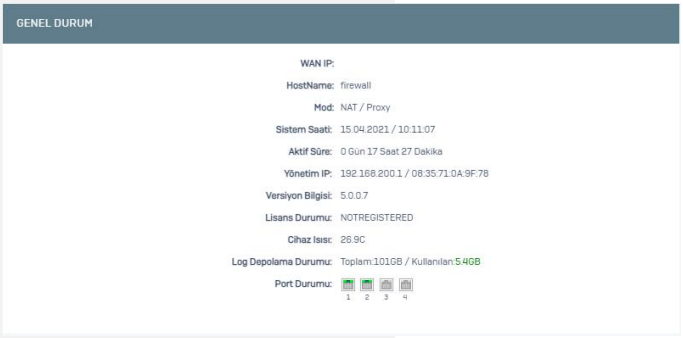


FIREWALL KULLANICI REHBERİ

DASHBOARD

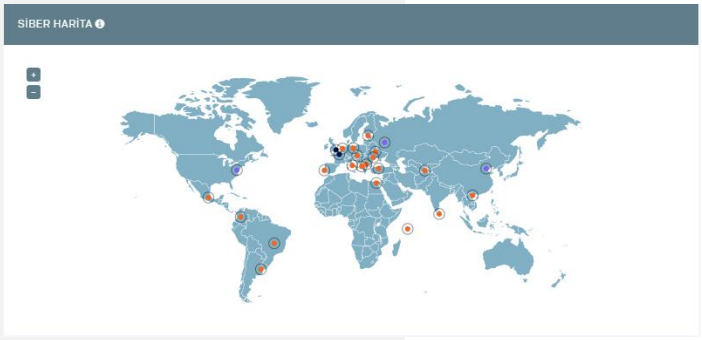
Genel Durum

Bu bölümde PONIVA Firewall cihazınıza ait genel sistem bilgilerini görüntüleyebilirsiniz. Yazılım sürümü, lisans durumu, disk depolama kullanımı ve aktif ağ portları gibi bilgilere buradan erişebilirsiniz.



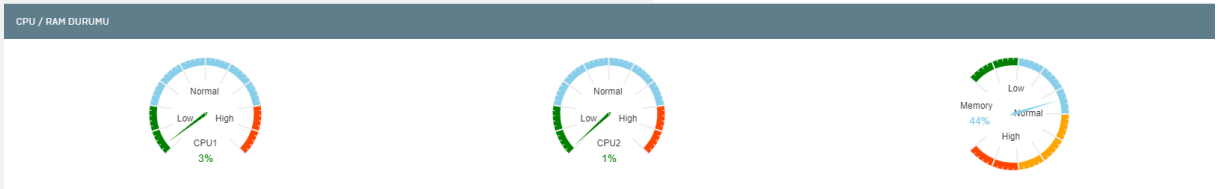
Siber Harita

Cihazınıza yönelik saldırı girişimlerinin hangi ülkelerden geldiğini günlük olarak harita üzerinden görüntüleyebilirsiniz. **Info** simgesine tıklayarak son 30 gün içinde ülkelere göre saldırı sayılarını inceleyebilirsiniz.



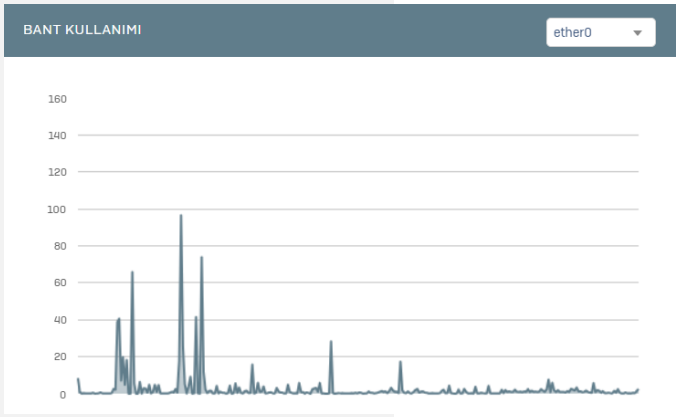
CPU/RAM Durumu

Cihazın işlemci (CPU) ve bellek (RAM) kullanım durumunu görüntüleyebilirsiniz.



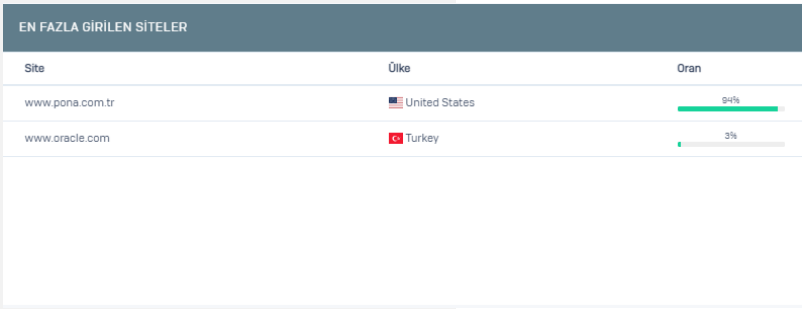
Bant Kullanımı

Seçili ağ portundan geçen bant genişliği kullanımını anlık olarak görüntüleyebilirsiniz. Örnekte ether0 portu gösterilmektedir; diğer aktif wan portlarınızı seçerek trafik durumlarını da inceleyebilirsiniz.



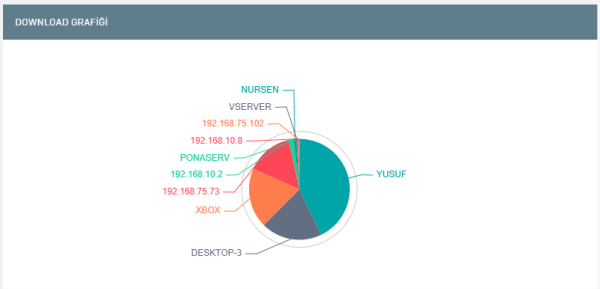
En Fazla Girilen Siteler

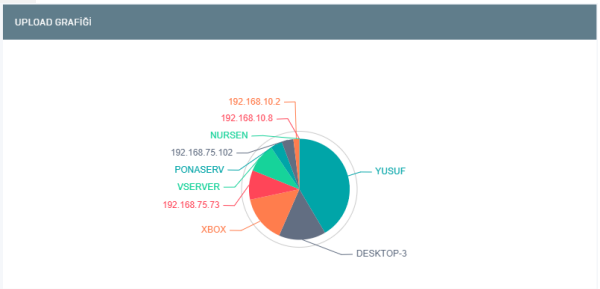
Ağınızdaki kullanıcılar tarafından en çok ziyaret edilen web sitelerini bu bölümden görüntüleyebilirsiniz.



Download/Upload Grafikleri

Yerel ağınızdaki kullanıcıların indirme (download) ve yükleme (upload) trafik miktarlarını görüntüleyebilirsiniz. Kullanıcılar, IP adreslerine göre veya isim tanımlanmışsa kullanıcı adlarıyla listelenir.





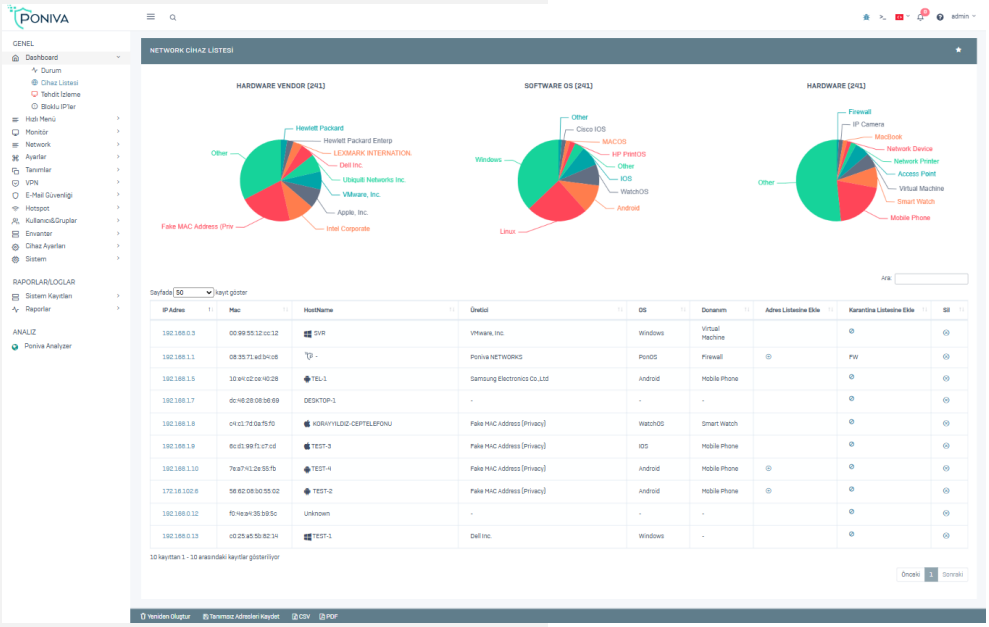
Aktif Yöneticiler

Cihazın yönetim arayüzünde oturum açmış olan aktif kullanıcıları görüntüleyebilirsiniz.



CİHAZ LİSTESİ

Ağınıza bağlı cihazları ve bu cihazlara ait ağ, üretici, işletim sistemi ve donanım bilgilerini görüntüleyebilirsiniz. Ayrıca cihazları adres listesine ekleyebilir veya karantina listesine alabilirsiniz.



	AÇIKLAMA
IP Adres	Cihaza atanmış IP adresini gösterir.
Mac	Cihazın ağ arayüzüne ait MAC adresini gösterir.
Hostname	Cihazın ağ üzerindeki ana bilgisayar adını gösterir.
Üretici	Cihazın üreticisini gösterir.
OS	Cihazda tespit edilen işletim sistemi bilgisini gösterir.
Donanım	Cihazın türünü veya donanım yapısını belirtir.

TEHDİT İZLEME

Bu menüden cihazınıza yönelik saldırılar hakkında ayrıntılı bilgi edinebilirsiniz. Aylık saldırı istatistiklerini, en çok saldırı alan portları ve saldırı tablosundaki IP adreslerini görüntüleyebilirsiniz.



MONİTÖR

NETWORK

MENU	AÇIKLAMA
Anlık Hat Kullanımı	Seçili ağ portundan geçen bant genişliği kullanımını anlık olarak görüntüleyebilirsiniz.
Aktif Aygıtlar	Ağınızda aktif olan aygıtları görüntüleyebilirsiniz.
Aktif Bağlantılar	Ağınızdaki aktif bağlantıları görüntüleyebilir ve gerekli durumlarda seçtiğiniz bağlantıları sonlandırabilirsiniz.
Kullanıcı Grafiği	Ağınızdaki kullanıcıların indirme (download) ve yükleme (upload) trafiklerini anlık görüntüleyebilirsiniz.
DHCP Cihazları	DHCP servisi üzerinden IP adresi almış cihazların listesini görüntüleyebilirsiniz.
LLDP Durumu	LLDP protokolü aracılığıyla yerel ağda tespit edilen komşu cihazları ve bunlara ilişkin bilgileri görüntüleyebilirsiniz.
Network Durumu	Ağ arayüzlerinin bağlantı durumlarını görüntüleyebilirsiniz.
Route Tablosu	Cihazın yönlendirme tablosunu görüntüleyerek ağ trafiğinin hangi ağ geçitleri ve arayüzler üzerinden yönlendirildiğini inceleyebilirsiniz.
ARP Tablosu	Aktif aygıtların IPv4 adresleri ile MAC adresleri arasındaki eşleştirmeleri görüntüleyebilirsiniz.
IPv6 Komşu Listesi	Yerel ağda IPv6 üzerinden tespit edilen komşu cihazların listesini görüntüleyebilirsiniz.

VPN

MENU	AÇIKLAMA

SSL VPN Kullanıcı	Aktif SSL VPN kullanıcı listenizi görüntüleyebilirsiniz.
L2TP/PPTP Kullanıcı	Aktif L2TP/PPTP kullanıcı listenizi görüntüleyebilirsiniz.
IPSEC VPN	Aktif IPSEC bağlantı listenizi görüntüleyebilirsiniz.

KONTROLLER

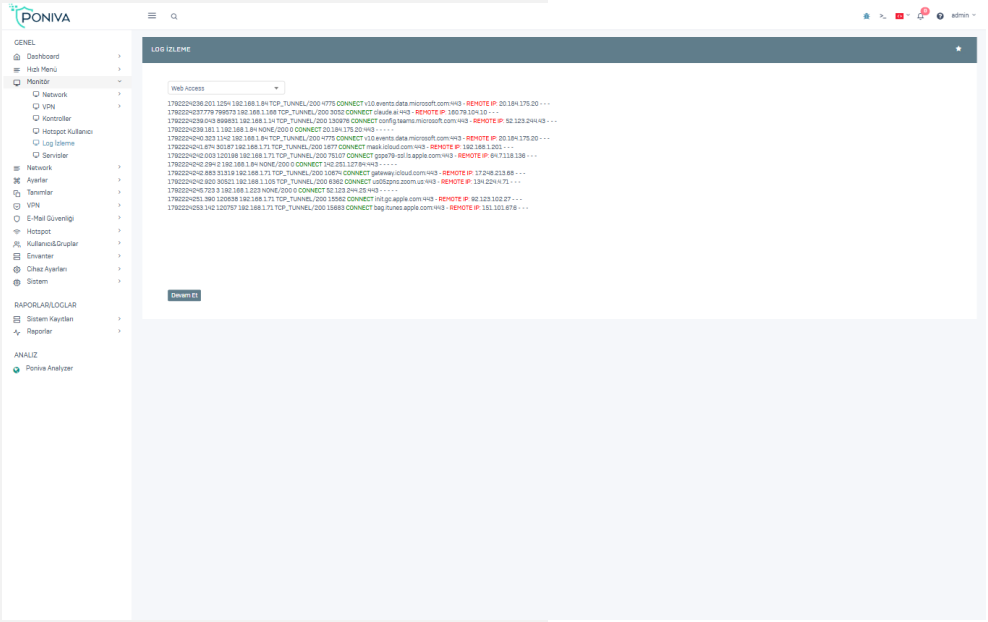
MENU	AÇIKLAMA
Cihaz Kontrol	Cihaz durumunu kontrol eder.
Network Kontrol	Belirtilen IP adresi ve port için ağ bağlantısını test etmenizi sağlar. Ping, Trace ve Telnet araçları ile bağlantı ve erişilebilirlik kontrolü yapabilirsiniz.
Website Kontrol	Firewall üzerinden bir web sitesine erişilip erişilemediğini test edebilirsiniz.
IPS Kontrol	Girilen IP adresiyle ilgili IPS olay kayıtlarını listeler. Kaynak veya hedef olarak bu IP'nin geçtiği tüm tetiklenmeler gösterilir.
IP Bilgisi	Girilen IP adresinin WHOIS kaydını sorgular.
Kullanıcı	Kullanıcının hangi grupta olduğunu ya da o kullanıcı için örneğin youtube.com yasak mı diye kontrol edebilirsiniz.
Domain Kontrol	Domain kategori listesini gösterir. Örneğin youtube.com domainin hangi kategorilerde olduğunu listeleyebilirsiniz.

HOTSPOT KULLANICI

Aktif Hotspot kullanıcı listesini görüntüleyebilirsiniz.

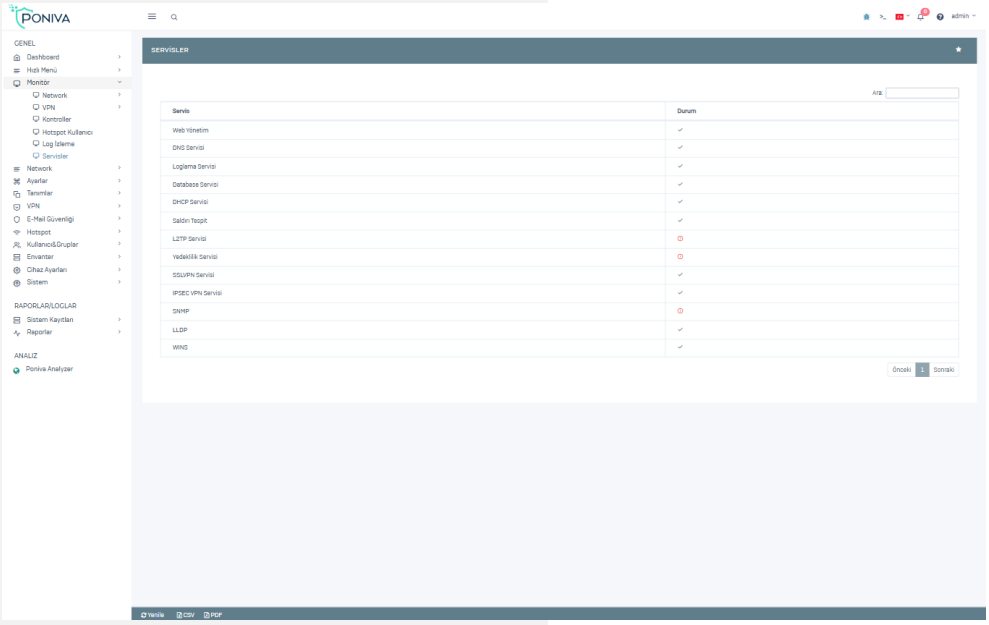
LOG İZLEME

Canlı olarak loglarınızı görüntüleyebilirsiniz.



SERVİSLER

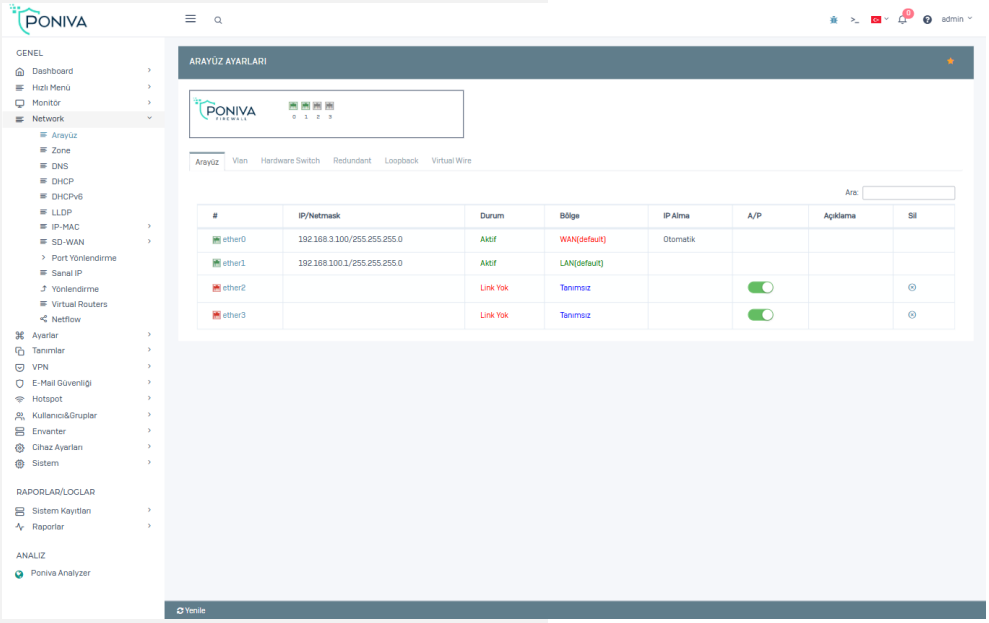
Servis durumlarını görüntüleyebilirsiniz.



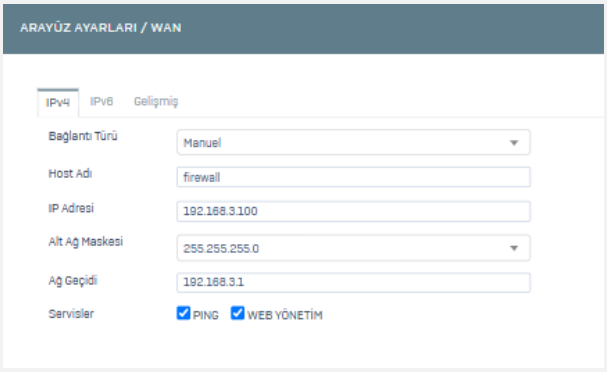
NETWORK

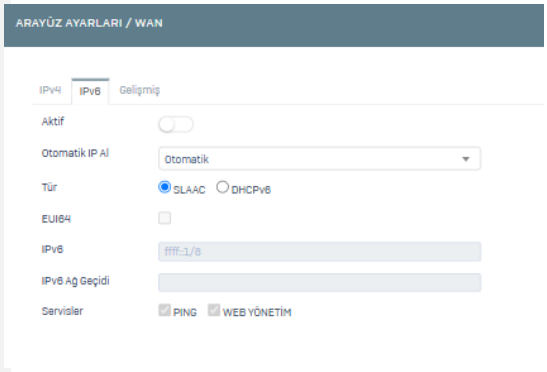
ARAYÜZ

Network ayarları bu bölümde tanımlanmaktadır. Birden fazla LAN, WAN arayüzü tanımlayabilirsiniz.



WAN Ayarları

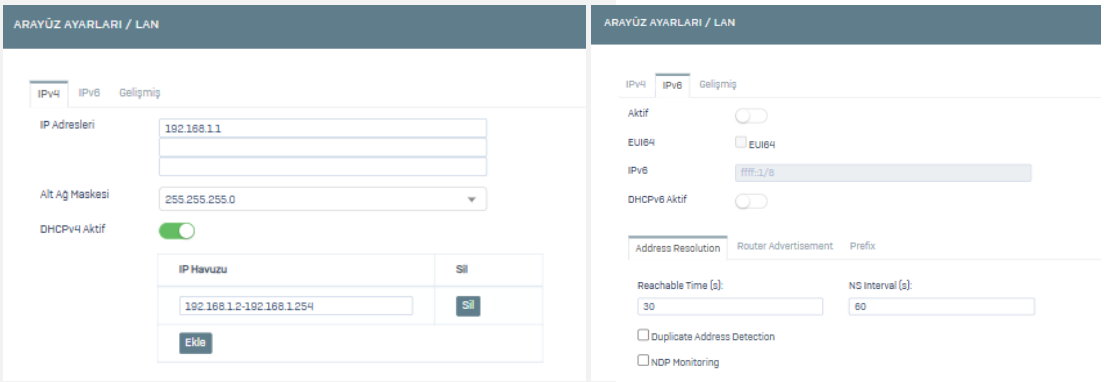


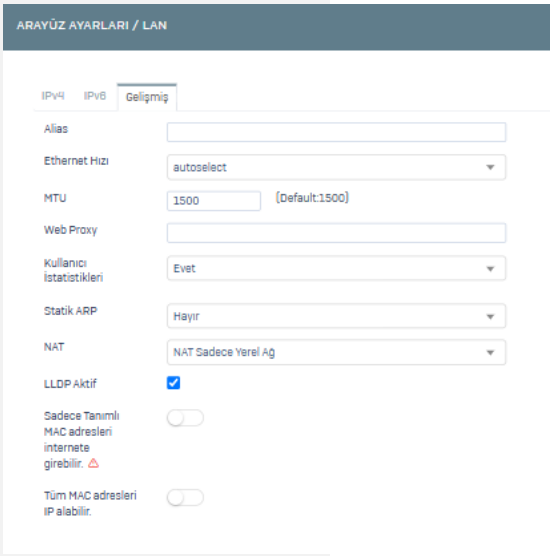


	AÇIKLAMA
IPv4 Sekmesi	
Bağlantı Türü	Yapılandırılacak ağ bağlantısının türünü belirtir.
Host Adı	Ağ arayüzü için kullanılacak ana bilgisayar adını belirtir.
IP Adres	Ağ arayüzüne atanacak IPv4 adresini belirtir.
Ağ Maskesi	IPv4 ağının alt ağ maskesini belirtir.
Ağ Geçidi	IPv4 trafiğinin diğer ağlara yönlendirilmesinde kullanılacak varsayılan ağ geçidini belirtir.
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.
IPv6 Sekmesi	
Aktif	Ağ arayüzünü etkinleştirir veya devre dışı bırakır
Otomatik IP Al	IP adresi ve ilgili ağ yapılandırma bilgilerinin DHCP üzerinden otomatik alınmasını sağlar.

EUI64	IPv6 adresinin ağ arayüzünün MAC adresinden türetilen EUI-64 yöntemiyle oluşturulmasını sağlar.
IPv6	Ağ arayüzüne atanacak IPv6 adresini belirtir.
Ağ Geçidi	IPv6 trafiğinin diğer ağlara yönlendirilmesinde kullanılacak ağ geçidini belirtir.
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.
Gelişmiş Sekmesi	
Alias	Ağ arayüzü için bir ad belirlemenizi sağlar.
MTU	Ağ arayüzü üzerinden tek bir pakette taşınabilecek maksimum veri boyutunu belirler.
Ethernet Hızı	Ağ arayüzünün bağlantı hızını ve çift yönlü iletişim modunu belirleyebilirsiniz. autoselect seçeneği, hız ve duplex ayarlarının otomatik olarak belirlenmesini sağlar.
Domain	Ağ arayüzü için kullanılacak etki alanı (domain) bilgisini belirtir.
BW	Ağ arayüzü için bant genişliği (bandwidth) değerini tanımlamanızı sağlar.
NAT	Ağ arayüzü için NAT (Ağ Adresi Çevirisi) özelliğini etkinleştirir veya devre dışı bırakır.
LLDP Aktif	Ağ arayüzünde LLDP protokolünü etkinleştirir veya devre dışı bırakır. Bu protokol, doğrudan bağlı ağ cihazlarının birbirlerini tanımasına yardımcı olur.
Farklı MAC Adresi Kullan	Ağ arayüzünde varsayılan MAC adresi yerine farklı bir MAC adresi kullanılmasını sağlar.
MAC	Ağ arayüzünde kullanılacak MAC adresini belirtir. Farklı MAC adresi kullanımı etkinleştirildiğinde bu alana ilgili adres girilir.

LAN Ayarları

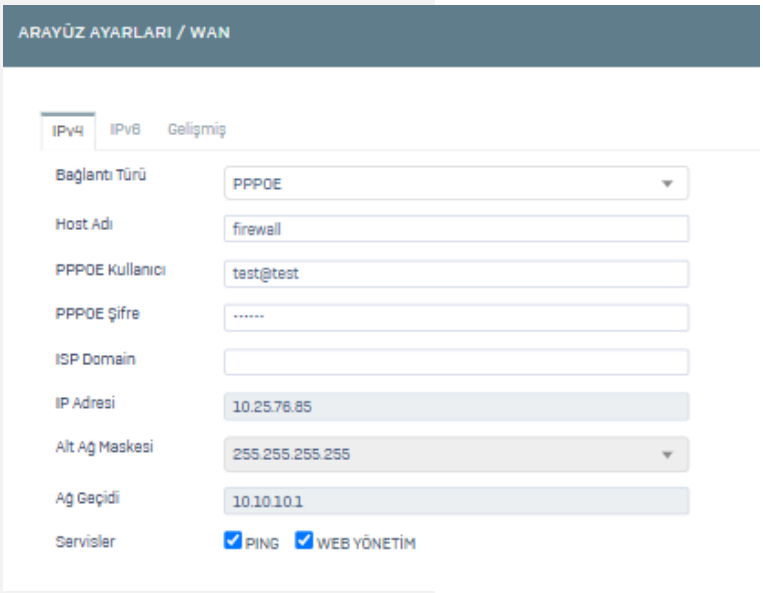




	AÇIKLAMA
IPv4 Sekmesi	
IPv4 Adresleri	Ağ arayüzüne atanacak IPv4 adresini tanımlayabilirsiniz. İhtiyaç halinde aynı arayüz için birden fazla IPv4 adresi ekleyebilirsiniz.
Alt Ağ Maskesi	IPv4 adresinin ait olduğu ağın alt ağ maskesini belirleyebilirsiniz.
DHCPv4 Aktif	IPv4 adresinin DHCP üzerinden otomatik alınıp alınmayacağını seçebilirsiniz.
IPv6 Sekmesi	
Aktif	Ağ arayüzünde IPv6 desteğini etkinleştirebilir veya devre dışı bırakabilirsiniz.
EUI64	Etkinleştirildiğinde, desteklenen yapılandırmalarda ağ arayüzünün MAC adresinden yararlanılarak 64 bitlik IPv6 arayüz kimliği oluşturulur.
IPv6 Adresleri	Ağ arayüzüne atanacak IPv6 adresini tanımlayabilirsiniz.
DHCPv6 Aktif	IPv6 adresi ve desteklenen ağ yapılandırma bilgilerinin DHCPv6 üzerinden otomatik alınıp alınmayacağını belirleyebilirsiniz.
Gelişmiş Sekmesi	
Alias	Ağ arayüzü için bir ad belirlemenizi sağlar.
Ethernet Hızı	Ağ arayüzünün bağlantı hızını ve çift yönlü iletişim modunu belirleyebilirsiniz. autoselect seçeneği, hız ve duplex ayarlarının otomatik olarak belirlenmesini sağlar.
MTU	Ağ arayüzü üzerinden tek bir pakette taşınabilecek maksimum veri boyutunu belirler.
Web Proxy	İlgili ağ arayüzü için Web Proxy özelliğinin kullanımını yapılandırmanızı sağlar.
Kullanıcı İstatistikleri	Ağ arayüzündeki kullanıcıların trafik ve kullanım istatistiklerinin izlenmesini sağlar.

Statik ARP	IP adresleri ile MAC adresleri arasındaki eşleştirmelerin statik olarak tanımlanmasını sağlar.
NAT	**NAT (Sadece Yerel Ağ):** NAT işleminin yalnızca yerel ağ trafiğine uygulanmasını sağlar. **NAT (Tüm Networkler):** NAT işleminin tüm ağlara yönelik trafik için uygulanmasını sağlar.
LLDP Aktif	LLDP protokolünü etkinleştirerek doğrudan bağlı ağ cihazlarının birbirlerini tanımasını sağlar.
Sadece Tanımlı MAC adresleri internete girebilir	Yalnızca MAC adresi tanımlanmış cihazların ağa erişmesine izin verilmesini sağlar.
Tüm MAC adresleri IP alabilir	MAC adresi önceden tanımlanmış olsun ya da olmasın, ağa bağlanan cihazların DHCP havuzundan IP adresi almasına izin verir.

PPPOE Ayarları

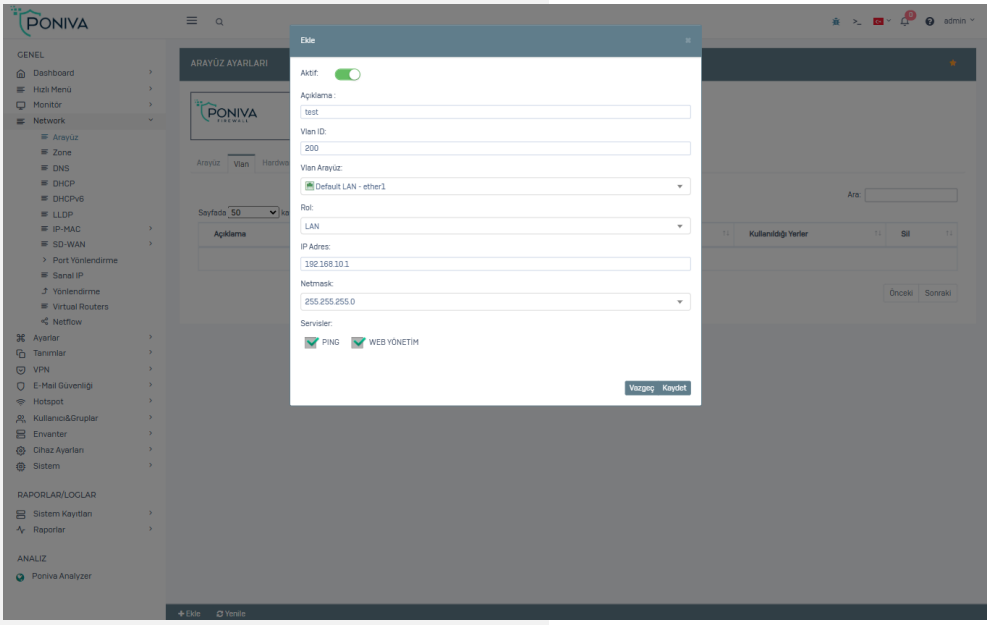


	AÇIKLAMA
Bağlantı Türü	PPPOE seçmelisiniz.
Host Adı	Varsayılan firewall
PPPOE Kullanıcı	İnternet servis sağlayıcınız tarafından verilen PPPoE kullanıcı adını girmenizi sağlar.
PPPOE Şifre	PPPoE bağlantısı için internet servis sağlayıcınız tarafından verilen şifreyi girmenizi sağlar.
ISP Domain	İnternet servis sağlayıcınızın (ISP) bağlantı için gerektirdiği etki alanı bilgisini belirtir.
IP Adres	Bu bölüm otomatik gelmektedir.
Ağ Maskesi	Bu bölüm otomatik gelmektedir.

Ağ Geçidi	Bu bölüm otomatik gelmektedir.
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.

VLAN

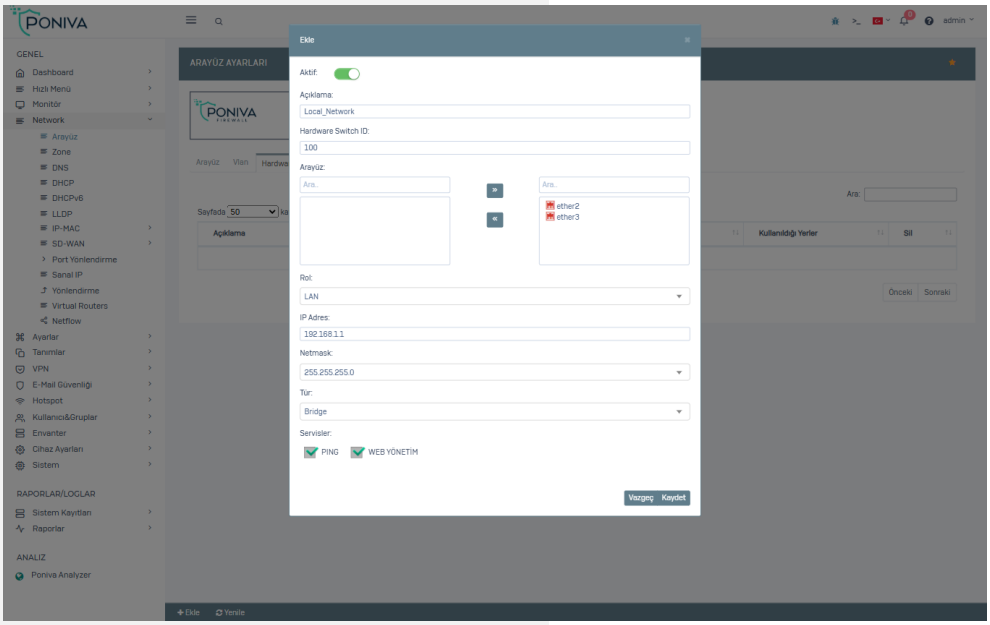
Lokal ağınız üzerinde VLAN (Sanal Yerel Alan Ağı) tanımlayarak ağınızı farklı mantıksal ağlara ayırabilirsiniz. Örneğin, VLAN destekli bir switch kullanarak farklı departmanların veya cihaz gruplarının ağ trafiğini birbirinden ayırabilir ve her VLAN'ı ayrı ayrı yönetebilirsiniz.



	AÇIKLAMA
VLAN Adı	Bir VLAN adı girmelisiniz.
VLAN ID	VLAN'ı tanımlayan, 1–4094 aralığında bir VLAN kimliği girmenizi sağlar.
VLAN Arayüz	VLAN'ın oluşturulacağı fiziksel ağ arayüzünü seçmenizi sağlar.
VLAN Tür	VLAN arayüzünün türünü veya çalışma biçimini belirlemenizi sağlar.
IP Adres	VLAN arayüzüne atanacak IP adresini belirtir.
Netmask	VLAN arayüzünün IPv4 alt ağ maskesini belirtir.
Ağ Geçidi	VLAN üzerinden diğer ağlara erişim için kullanılacak ağ geçidini belirtir.
NAT	VLAN trafiği için Ağ Adresi Çevirisi (NAT) özelliğini yapılandırmanızı sağlar.
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.

Hardware Switch

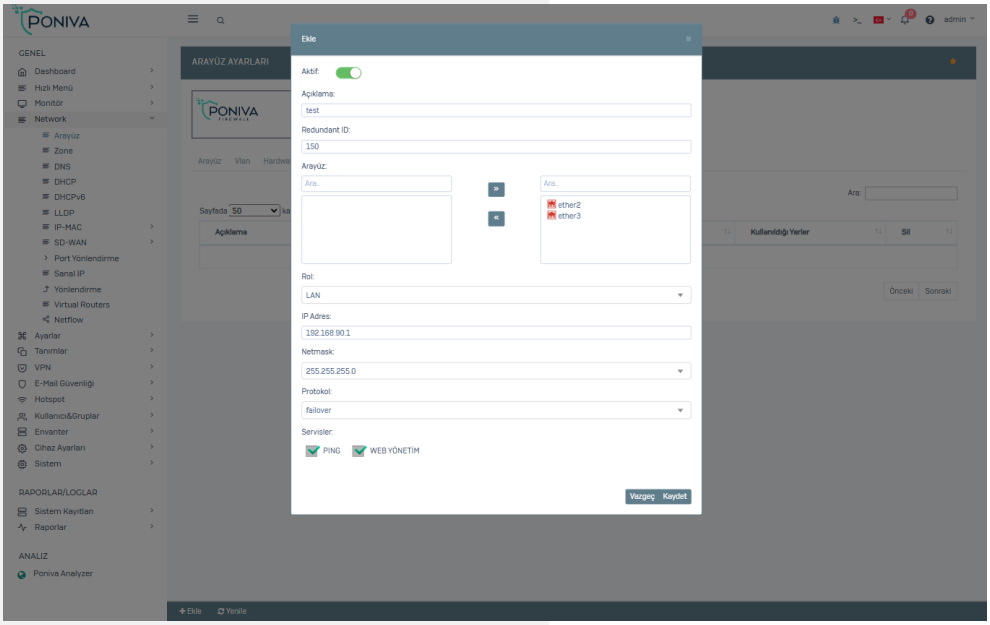
Hardware Switch, birden fazla fiziksel ağ arayüzünü donanım seviyesinde birleştirerek tek bir mantıksal ağ arayüzü gibi kullanmanızı sağlar.



	AÇIKLAMA
Aktif	Hardware Switch yapılandırmasını etkinleştirir veya devre dışı bırakır.
Açıklama	Hardware Switch yapılandırmasını tanımlamak için açıklama girmenizi sağlar.
Hardware Switch ID	Oluşturulan donanımsal switch'in kimlik numarasını belirtir.
Arayüz	Hardware Switch'e dahil edilecek fiziksel ağ arayüzlerini seçmenizi sağlar. Yapılandırma için en az iki farklı arayüz seçilmelidir.
Rol	Hardware Switch'in ağdaki rolünü belirler. LAN veya WAN olarak yapılandırılabilir.
IP Adres	Hardware Switch arayüzüne atanacak IP adresini belirtir.
Netmask	IP adresinin ait olduğu IPv4 ağının alt ağ maskesini belirtir.
Ağ Geçidi	Hardware Switch WAN rolünde kullanılıyorsa, ilgili bağlantı üzerinden diğer ağlara erişim için kullanılacak ağ geçidini belirtir.
Tür	Hardware Switch'in bağlantı veya yapılandırma türünü belirlemenizi sağlar. Bridge/Bridge(STP)
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.

Redundant

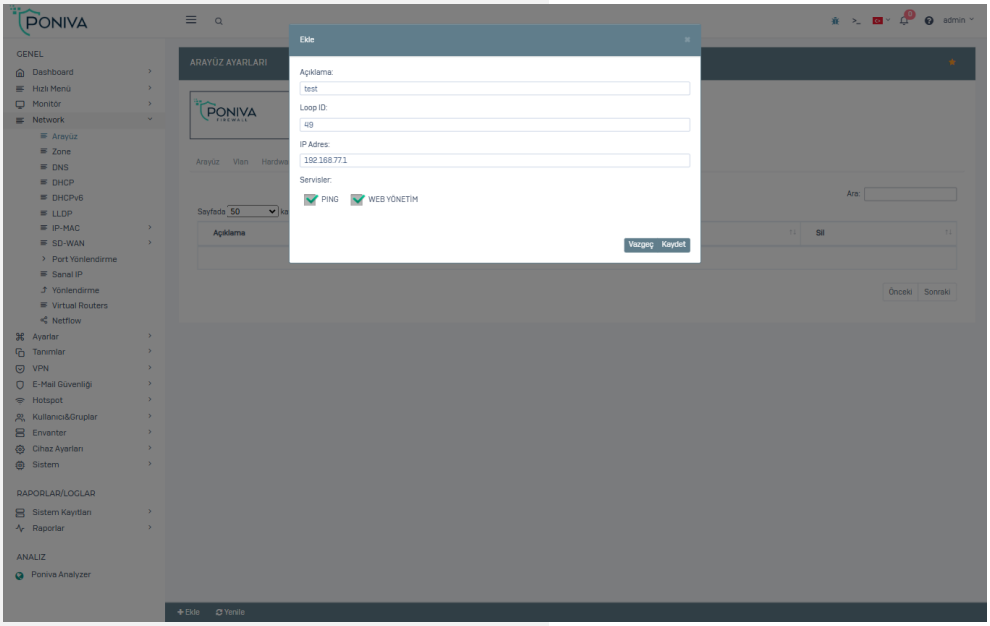
Redundant Switch, birden fazla fiziksel ağ arayüzünü tek bir mantıksal bağlantı altında birleştirmenizi sağlar. Seçilen protokole bağlı olarak bağlantı yedekliliği, yük dengeleme veya bağlantıların birlikte kullanılması gibi işlevler sunabilir.



	AÇIKLAMA
Aktif	Redundant Switch yapılandırmasını etkinleştirir veya devre dışı bırakır.
Açıklama	Redundant Switch yapılandırmasını tanımlamak için açıklama girmenizi sağlar.
Redundant ID	Redundant Switch yapılandırmasına ait kimlik numarasını belirtir.
Arayüz	Redundant Switch'e dahil edilecek fiziksel ağ arayüzlerini seçmenizi sağlar. Yapılandırma için en az iki farklı arayüz seçilmelidir.
Rol	Redundant Switch'in ağdaki rolünü belirler. LAN veya WAN olarak yapılandırılabilir.
IP Adres	Redundant Switch arayüzüne atanacak IP adresini belirtir.
Netmask	IP adresinin ait olduğu IPv4 ağının alt ağ maskesini belirtir.
Ağ Geçidi	Redundant Switch WAN rolünde kullanılıyorsa, ilgili bağlantı üzerinden diğer ağlara erişim için kullanılacak ağ geçidini belirtir.
Protokol	Fiziksel arayüzlerin nasıl birlikte çalışacağını belirler. Kullanılabilir seçenekler arasında Failover, FEC, LACP, Load Balance ve Round Robin bulunur.
Servisler	Arayüz üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.

Loopback

Loopback arayüzü, fiziksel bir ağ bağlantısına ihtiyaç duymadan cihaz üzerinde mantıksal bir ağ arayüzü oluşturmanızı sağlar. Bu arayüze IP adresi atayabilir ve ilgili servisleri yapılandırabilirsiniz.

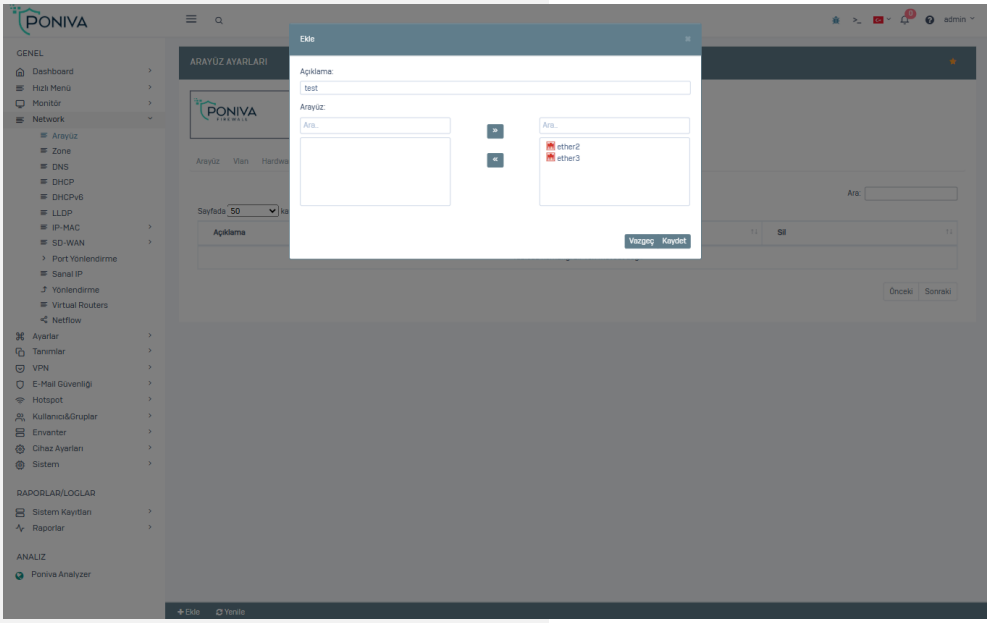


	AÇIKLAMA
Açıklama	Loopback arayüzünü tanımlamak için açıklama girmenizi sağlar.
ID	Loopback yapılandırmasına ait kimlik numarasını belirtir. 1-50 arasında bir değer girmelisiniz.
IP Adresi	Loopback arayüzüne atanacak IP adresini belirtir.
Servisler	Loopback arayüzü üzerinden erişime izin verilecek servisleri belirlemenizi sağlar.

Virtual Wire

Virtual Wire, iki fiziksel ağ arayüzünü birbiri arasında saydam bir bağlantı oluşturacak şekilde birleştirir. Bu yapılandırmada cihaz, ağ trafiğini IP adresi atamadan veya yönlendirme işlemi gerçekleştirmeden karşı arayüze aktarır. Trafik, yapılandırılmış güvenlik politikalarına bağlı olarak IPS, Uygulama Kontrolü, Web Filtreleme ve Antivirüs gibi güvenlik denetimlerinden geçirilebilir.

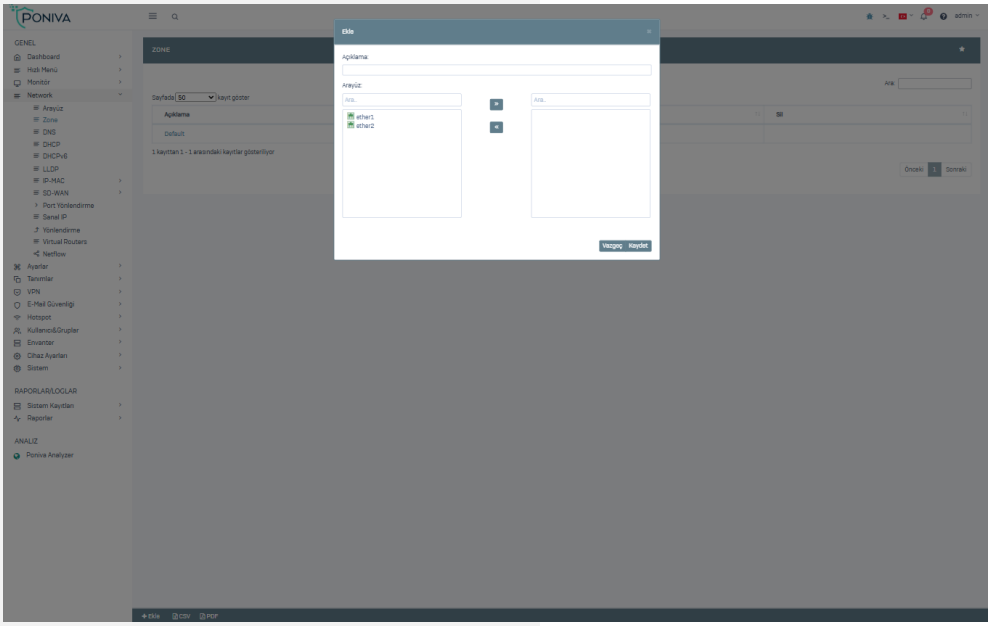
Virtual Wire bağlantısı, mevcut ağ topolojisini değiştirmeden ağ trafiğinin güvenlik duvarı üzerinden denetlenmesini sağlar. VLAN etiketleri gibi ağ bilgileri, yapılandırmaya bağlı olarak korunarak iletilir.



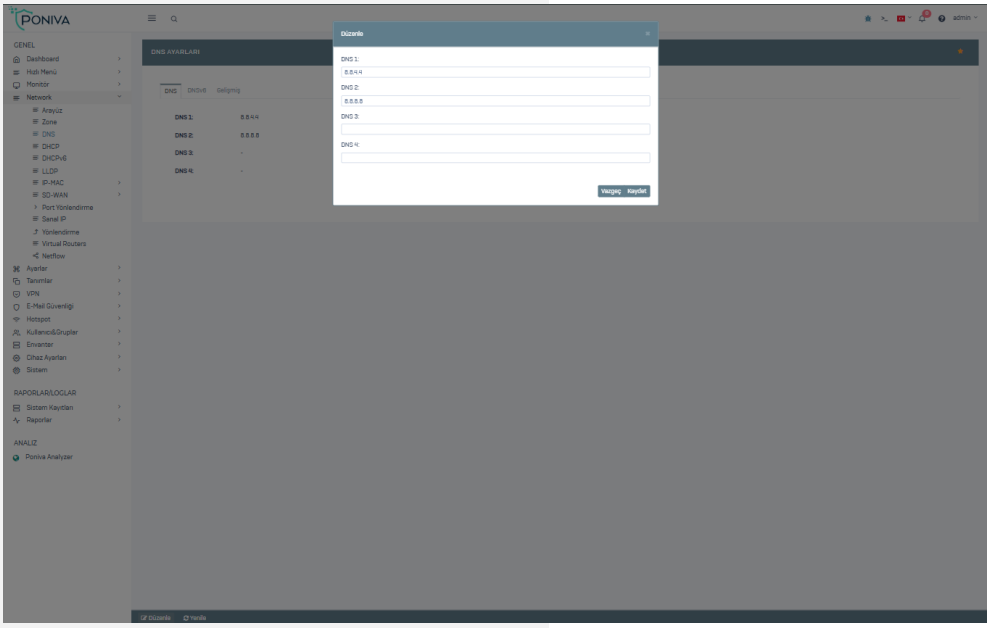
	AÇIKLAMA
Açıklama	Virtual Wire yapılandırmasını tanımlamak için açıklama girmenizi sağlar.
Arayüz	Virtual Wire bağlantısında kullanılacak iki fiziksel ağ arayüzünü seçmenizi sağlar.

ZONE

Zone, fiziksel ve sanal ağ arayüzlerini belirli gruplar altında toplamanızı sağlar. Bu sayede ağ arayüzlerini kullanım amaçlarına göre gruplandırabilir ve ilgili bölgeler arasındaki trafiği güvenlik politikaları üzerinden yönetebilirsiniz.



DNS

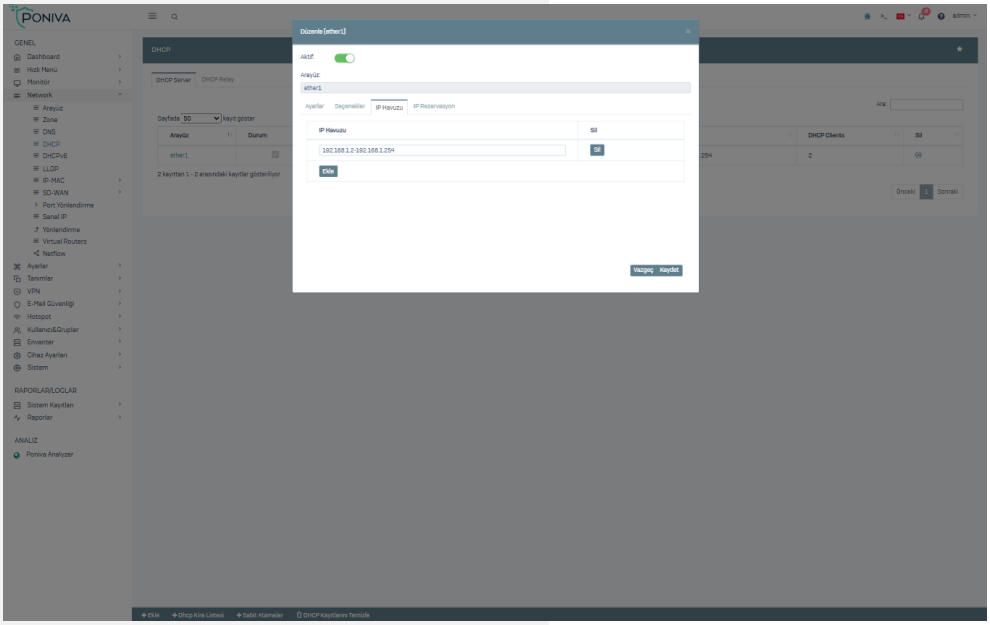


	AÇIKLAMA
DNS 1	Birincil DNS sunucusunun IP adresini belirtir.
DNS 2	İkincil DNS sunucusunun IP adresini belirtir.
DNS 3	Üçüncü DNS sunucusunun IP adresini belirtir.
DNS 4	Dördüncü DNS sunucusunun IP adresini belirtir.
PPPOE ile DNS Güncellenmesin	Etkinleştirildiğinde, PPPoE bağlantısı üzerinden otomatik olarak alınan DNS bilgilerinin mevcut DNS ayarlarını güncellemesini engeller.

DHCP

Dhcp Server

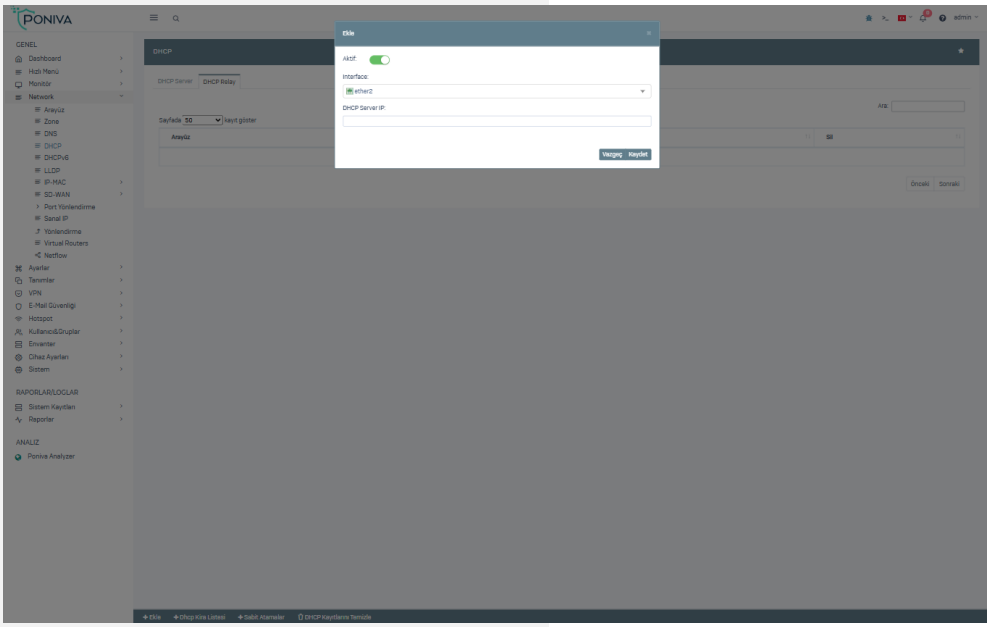
Sistemde kullanılan DHCPv4 ayarları bu bölümde yapılandırılır.



	AÇIKLAMA
Arayüz	DHCP sunucusunun hizmet vereceği ağ arayüzünü belirler.
IP Dağıtırken Pingle	Bir IP adresi dağıtılmadan önce adresin kullanımda olup olmadığını kontrol etmek için ping işlemi gerçekleştirir.
Sadece Tanımlı Cihazlara IP Dağıt	Yalnızca sistemde tanımlanmış cihazlara IP adresi dağıtılmasını sağlar.
Kira Süresi	Dağıtılan IP adresinin cihaz tarafından ne kadar süreyle kullanılabileceğini belirler.
Subnet	DHCP sunucusunun IP adresi dağıtacağı ağın alt ağını belirtir. Varsayılan 'firewall kullan' seçeneği aktiftir.
Ağ Geçidi	DHCP istemcilerine varsayılan ağ geçidi olarak iletilecek IP adresini belirler. Varsayılan 'firewall kullan' seçeneği aktiftir.
WINS	İstemcilere iletilecek WINS sunucusunun IP adresini belirtir. Varsayılan 'firewall kullan' seçeneği aktiftir.
DNS Son Eki	İstemcilere dağıtılacak DNS etki alanı son ekini belirler. Varsayılan 'firewall kullan' seçeneği aktiftir.
DNS	İstemcilere iletilecek DNS sunucularının IP adreslerini belirtir. Varsayılan 'firewall kullan' seçeneği aktiftir.
IP Havuzu	DHCP sunucusunun otomatik olarak dağıtabileceği IP adresi aralığını tanımlar. Birden fazla IP aralığı ekleyebilirsiniz.
IP Rezervasyon	Belirli cihazlara, genellikle MAC adresleri üzerinden, sürekli aynı IP adresinin atanmasını sağlar.
Network Tarama	Ağdaki cihazları tarayarak IP adreslerini ve cihazları listeler.

Dhcp Relay

DHCP Relay, yerel ağdaki cihazların farklı bir ağda bulunan DHCP sunucusundan IP adresi ve ağ yapılandırma bilgileri almasını sağlar. Bu bölümden DHCP Relay tanımı oluşturarak istemcilerden gelen DHCP isteklerinin belirtilen DHCP sunucusuna iletilmesini sağlayabilirsiniz.

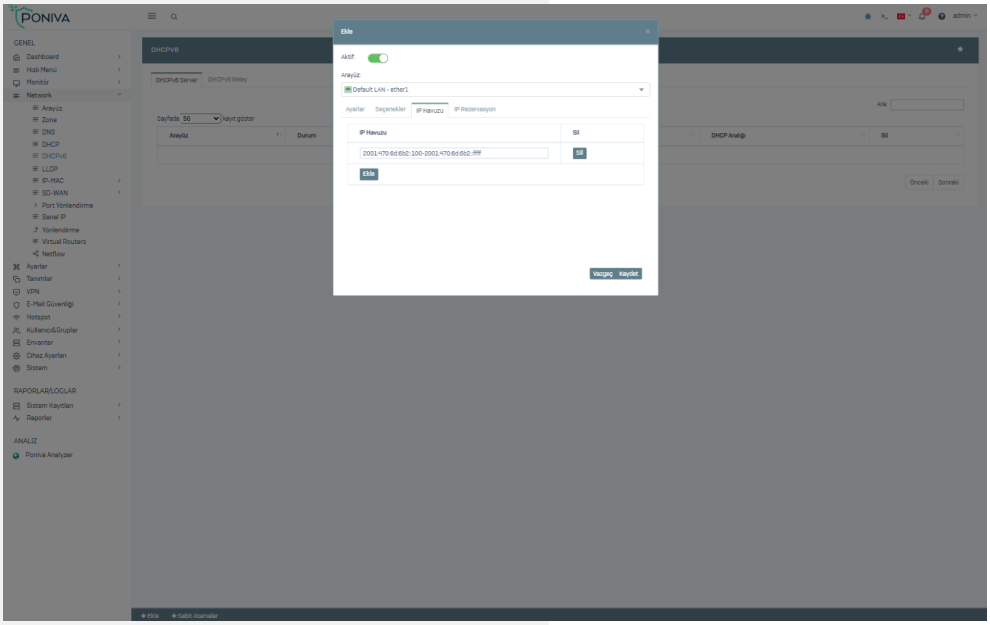


	AÇIKLAMA
Arayüz	DHCP isteklerinin alınacağı ve DHCP Relay işleminin gerçekleştirileceği ağ arayüzünü belirtir.
IPv4	DHCP isteklerinin iletileceği uzak DHCP sunucusunun IPv4 adresini belirtir.

DHCPV6

Dhcpv6 Server

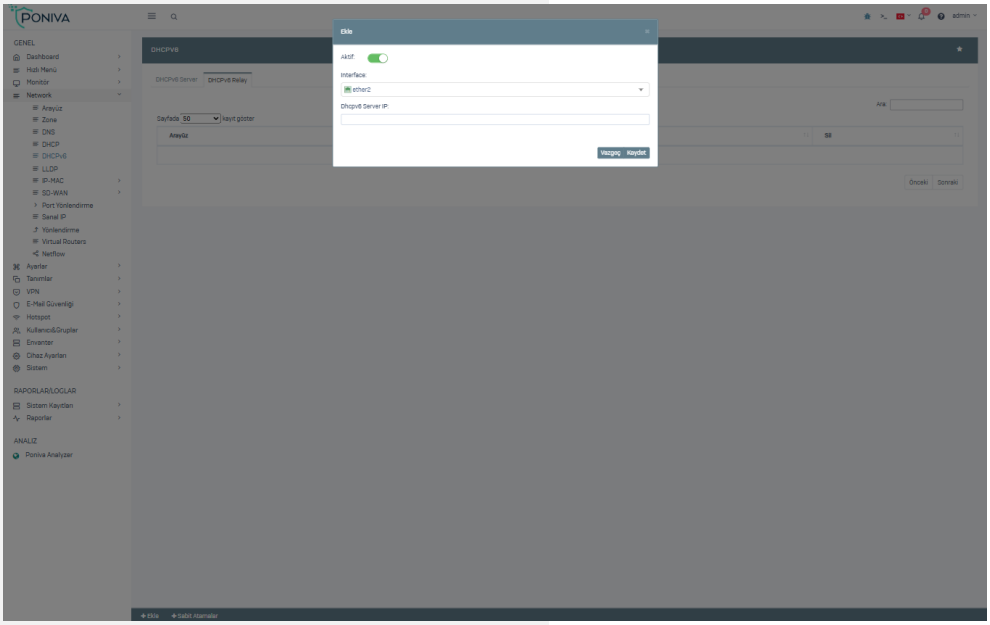
Sistemde kullanılan DHCPv6 ayarları bu bölümde yapılandırılır.



	AÇIKLAMA
Arayüz	DHCPv6 sunucusunun hizmet vereceği ağ arayüzünü belirler.
IP Dağıtırken Pingle	Bir IPv6 adresi dağıtılmadan önce adresin kullanımda olup olmadığını kontrol etmek için ping işlemi gerçekleştirir.
Sadece Tanımlı Cihazlara IP Dağıt	Yalnızca sistemde tanımlanmış cihazlara IPv6 adresi dağıtılmasını sağlar.
DNS Son Eki	İstemcilere iletilecek DNS etki alanı son ekini belirler. Varsayılan firewall kullan seçeneği aktiftir.
DNS	İstemcilere iletilecek DNS sunucularının IPv6 adreslerini belirtir. Varsayılan firewall kullan seçeneği aktiftir.
IP Havuzu	DHCPv6 sunucusunun dağıtabileceği IPv6 adres aralığını tanımlar.
IP Rezervasyon	Belirli cihazlara, desteklenen tanımlama yöntemi üzerinden, sürekli aynı IPv6 adresinin atanmasını sağlar.

Dhcpv6 Relay

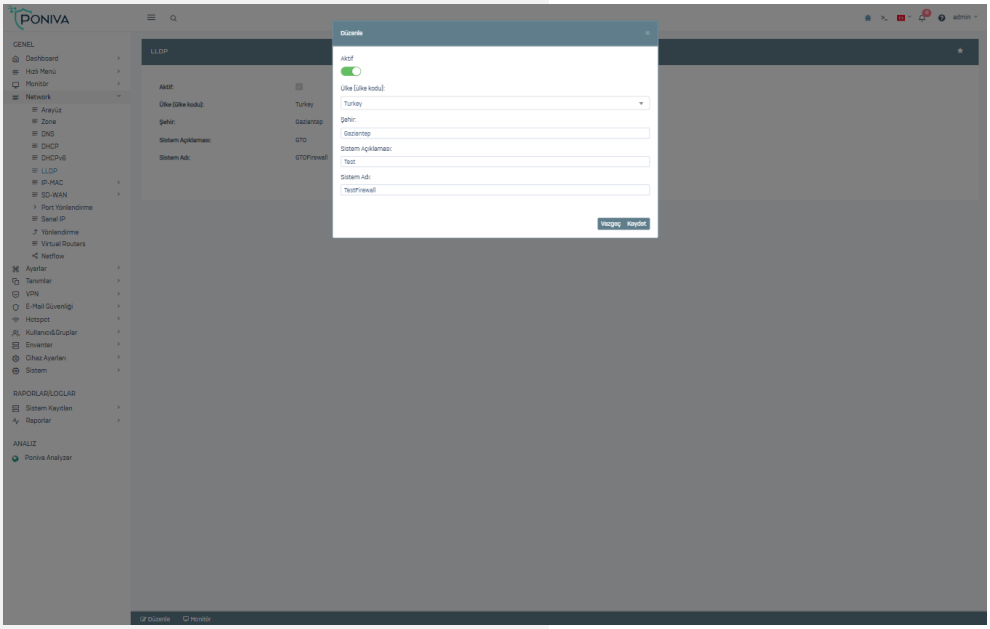
DHCPv6 Relay, yerel ağdaki cihazların farklı bir ağda bulunan DHCPv6 sunucusundan IPv6 adresi ve ağ yapılandırma bilgileri almasını sağlar. Bu bölümden DHCPv6 Relay tanımı oluşturarak istemcilerden gelen DHCPv6 isteklerinin belirtilen DHCPv6 sunucusuna iletilmesini sağlayabilirsiniz.



	AÇIKLAMA
Arayüz	DHCPv6 isteklerinin alınacağı ve DHCPv6 Relay işleminin gerçekleştirileceği ağ arayüzünü belirtir.
IPv6	DHCPv6 isteklerinin iletileceği uzak DHCPv6 sunucusunun IPv6 adresini belirtir.

LLDP

LLDP (Link Layer Discovery Protocol), aynı ağ üzerindeki doğrudan bağlı cihazların birbirleri hakkında bilgi paylaşmasını sağlayan bir protokoldür. Bu özellik sayesinde ağ cihazlarının kimlik ve konum bilgileri paylaşılabilir. LLDP üzerinden öğrenilen cihazları **Monitör** menüsünden görüntüleyebilirsiniz.

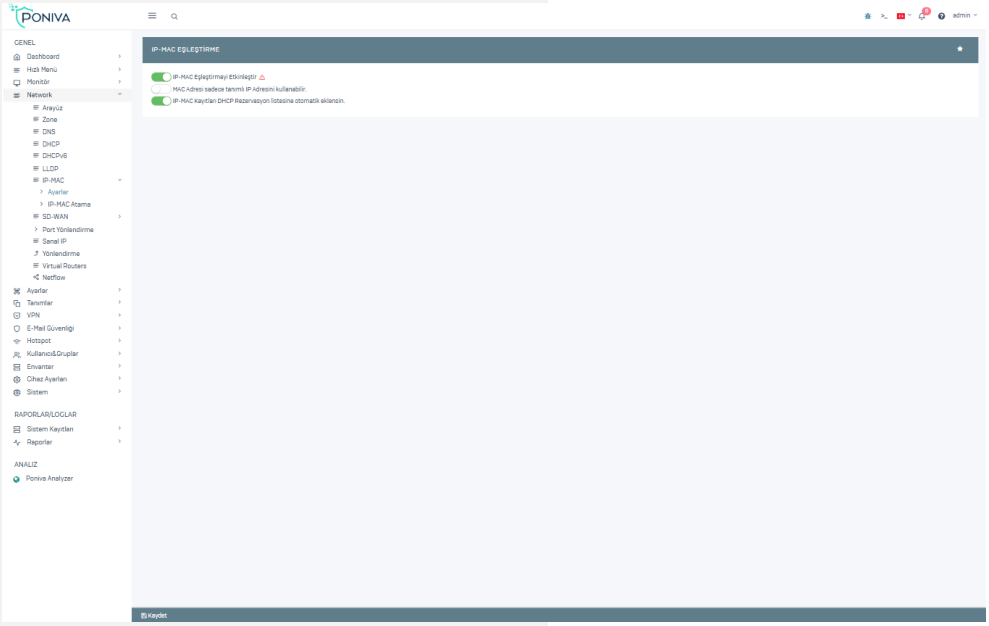


	AÇIKLAMA
Aktif	LLDP protokolünü etkinleştirir veya devre dışı bırakır.
Ülke	Cihazın bulunduğu ülke bilgisini belirtir.
Şehir	Cihazın bulunduğu şehir bilgisini belirtir.
Sistem Açıklaması	Cihazın işlevi veya donanımı hakkında açıklama girmenizi sağlar.
Sistem Adı	LLDP üzerinden diğer cihazlara bildirilecek sistem adını belirtir.

IP-MAC

IP-MAC eşleştirme, belirli bir MAC adresinin tanımlanan IP adresiyle eşleştirilmesini sağlar.

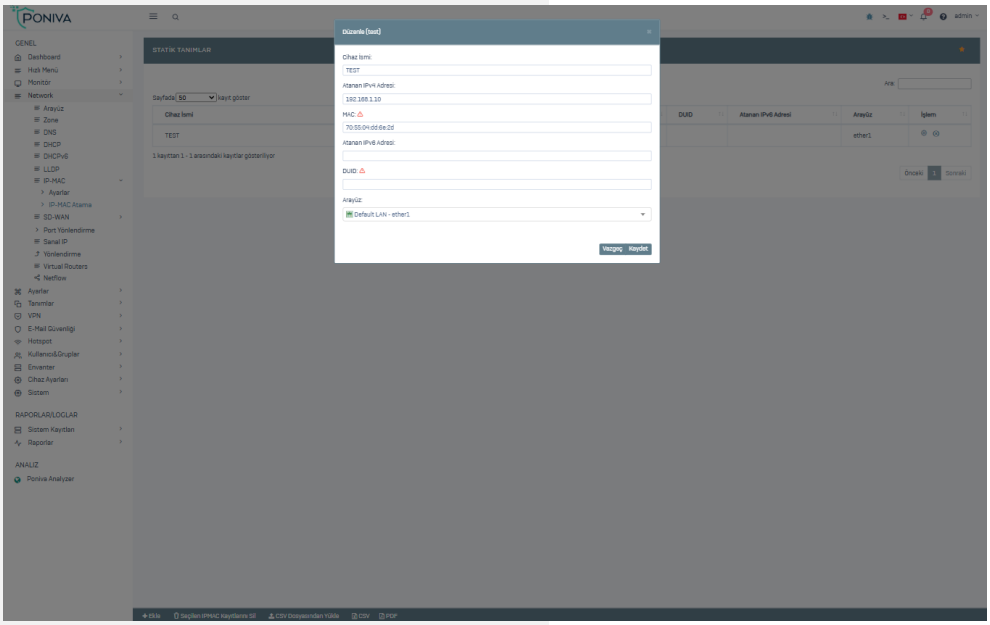
Ayarlar



	AÇIKLAMA
IP-MAC Eşleştirmeyi Etkinleştir	IP-MAC eşleştirme özelliğini etkinleştirir veya devre dışı bırakır.
Sadece Tanımlı MAC Adresleri İnternete Girebilir	Yalnızca sistemde tanımlı MAC adreslerine sahip cihazların internete erişmesine izin verir.
IP-MAC Kayıtları DHCP Rezervasyon Listesine Otomatik Eklensin	Oluşturulan IP-MAC eşleştirmelerinin DHCP rezervasyon listesine otomatik olarak eklenmesini sağlar.

*Varsayılan pasif gelir.

IP-MAC Atama

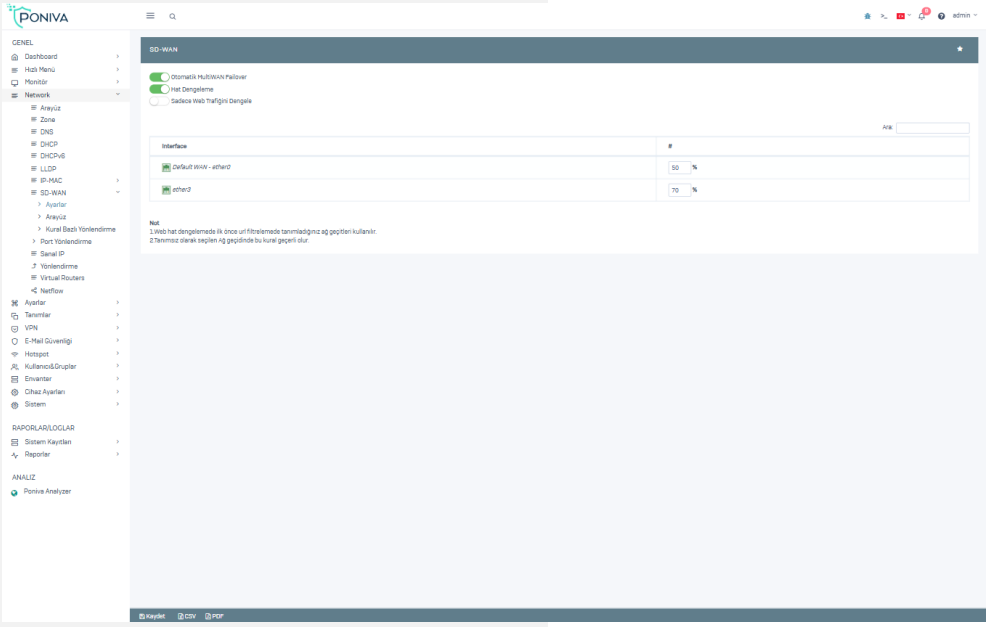


	AÇIKLAMA
Cihaz İsmi	Eşleştirme yapılacak cihazın adını belirtir.
Cihaz MAC Adresi	Cihazın ağ arayüzüne ait MAC adresini belirtir.
Atanan IPv4 Adresi	Cihaza atanacak IPv4 adresini belirtir.
Atanan IPv6 Adresi	Cihaza atanacak IPv6 adresini belirtir.
DUID	DHCPv6 işlemlerinde cihazı tanımlamak için kullanılan DHCP Unique Identifier bilgisini belirtir.
Arayüz	IP-MAC eşleştirmesinin geçerli olacağı ağ arayüzünü belirler.

SD-WAN

SD-WAN, birden fazla internet hattını tek bir yapı altında yönetmenizi sağlar. Bu bölümden internet hatları arasında yük dengeleme yapabilir ve hatlardan birinde bağlantı kesintisi yaşandığında trafiğin diğer aktif hat üzerinden devam etmesini sağlayabilirsiniz.

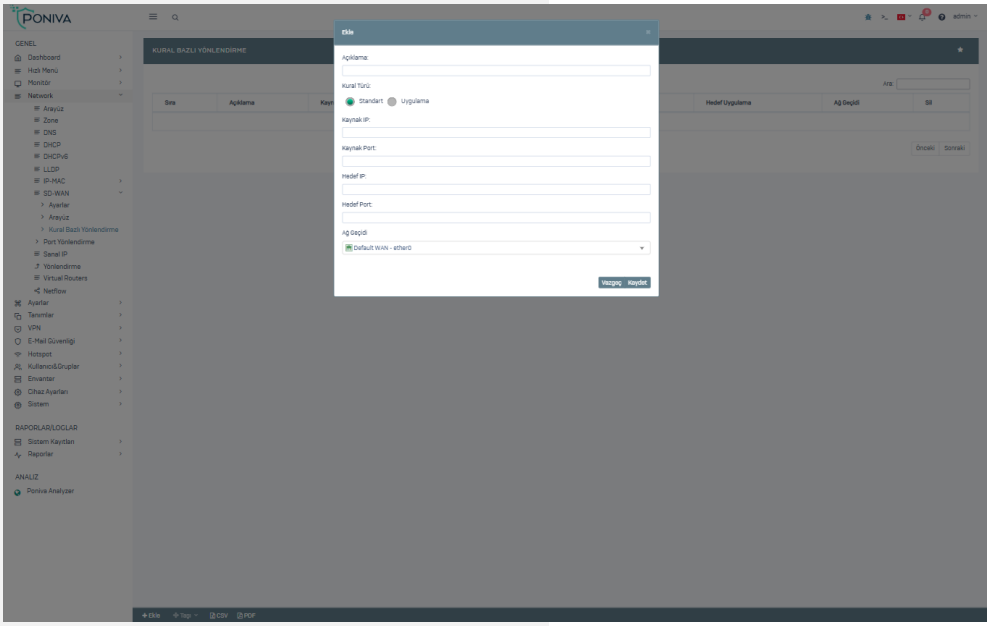
Ayarlar



	AÇIKLAMA
Otomatik Multiwan Failover	Etkinleştirildiğinde, internet hatlarından biri devre dışı kaldığında ilgili hattan geçen trafiğin aktif olan diğer hat üzerinden devam etmesini sağlar.
Hat Dengeleme	İnternet trafiğinin birden fazla hat arasında belirlenen oranlara göre dağıtılmasını sağlar. Örneğin, iki hat arasında %50-%50 oranında dağıtım yapılabilir.
Sadece Web Trafiğini Dengele	Etkinleştirildiğinde, hat dengeleme işleminin yalnızca web gezintisi trafiğine uygulanmasını sağlar.

Kural Bazlı Yönlendirme

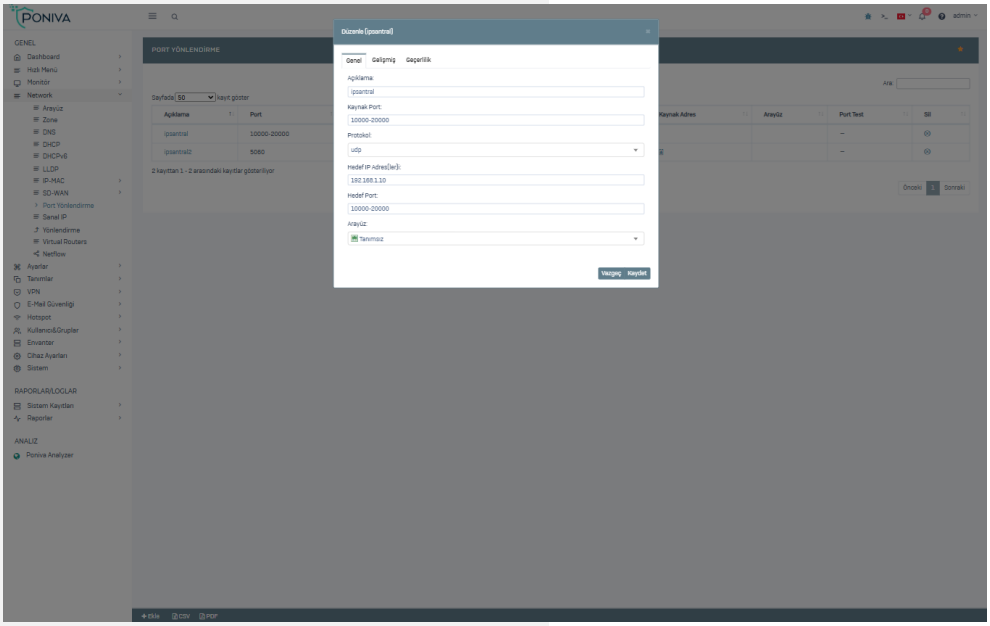
Kural Bazlı Yönlendirme, ağ trafiğinin belirlenen koşullara göre uygun ağ geçidine yönlendirilmesini sağlar. Kaynak ve hedef IP adresi, port bilgileri ve kural türü gibi ölçütler tanımlayarak belirli trafiklerin hangi ağ geçidi üzerinden iletileceğini belirleyebilirsiniz.



	AÇIKLAMA
Açıklama	Yönlendirme kuralını tanımlamak için açıklama girmenizi sağlar.
Kural Türü	Yönlendirme kuralının hangi trafik türüne veya koşula göre uygulanacağını belirler.
Kaynak IP Adresi	Kuralın uygulanacağı trafiğin kaynak IP adresini belirtir.
Kaynak Port	Trafiğin kaynak portunu belirtir. (Port aralığı için örneğin 10000-20000 gibi kullanabilirsiniz.)
Hedef IP Adresi	Trafiğin ulaşacağı hedef IP adresini belirtir.
Hedef Port	Trafiğin hedef portunu belirtir. (Port aralığı için örneğin 10000-20000 gibi kullanabilirsiniz.)
Ağ Geçidi	Belirtilen koşullara uyan trafiğin yönlendirileceği ağ geçidini belirler.

PORT YÖNLENDİRME

Port Yönlendirme, dış ağdan gelen belirli port ve protokoldeki bağlantı isteklerini yerel ağınızdaki bir sunucuya veya cihazın ilgili servisine yönlendirmenizi sağlar. Bu sayede Web Servisi, RDP gibi hizmetlere dış ağ üzerinden erişim sağlayabilirsiniz.



	AÇIKLAMA
Açıklama	Port yönlendirme kuralını tanımlamak için açıklama girmenizi sağlar.
Kaynak Port	Dış ağdan gelen bağlantı isteklerinin hedeflediği port numarasını belirtir. (Port aralığı için örneğin 10000-20000 gibi kullanabilirsiniz.)
Protokol	Yönlendirme kuralının uygulanacağı iletişim protokolünü belirler. Örneğin TCP veya UDP.
Hedef IP Adresi	Gelen bağlantı isteklerinin yönlendirileceği yerel ağ cihazının IP adresini belirtir.
Hedef Port	Bağlantı isteklerinin hedef cihazda yönlendirileceği port numarasını belirtir.
Sadece Bu Adreslerden Kabul Et	Port yönlendirme kuralı üzerinden bağlantı kurulmasına izin verilecek kaynak IP adreslerini sınırlar.
Geçerlilik	Port yönlendirme kuralının uygulanacağı zaman aralığını belirler.
Firewall Kurallarını Otomatik Ekle	Port yönlendirme işleminin çalışması için gerekli firewall kurallarının otomatik olarak oluşturulmasını sağlar.

SANAL IP

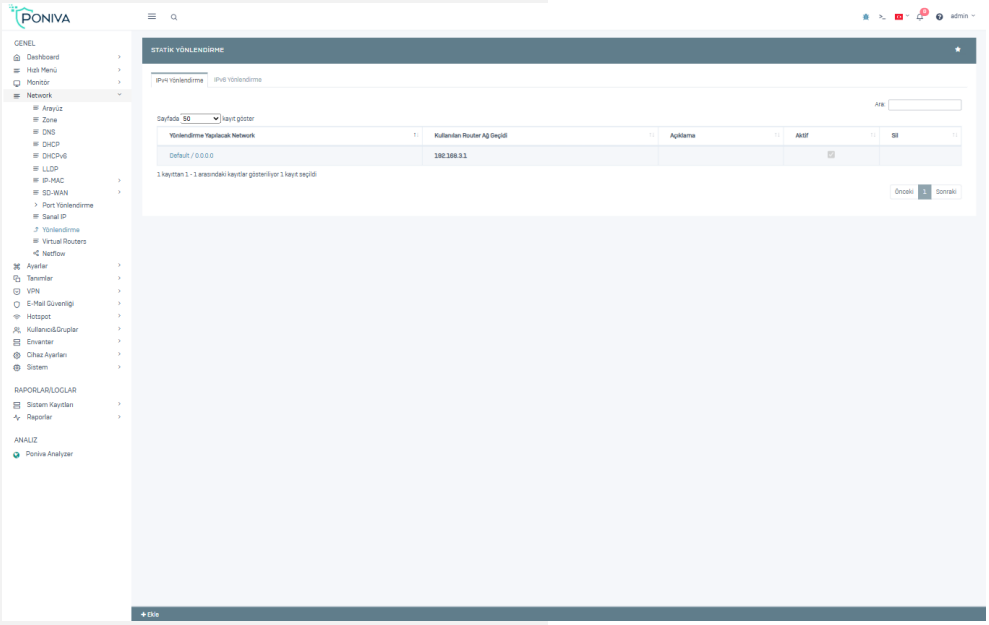
Sanal IP, belirli IP adresleri için ağ üzerinden gelen bağlantıların karşılanmasını ve bu bağlantıların tanımlanan gerçek IP adreslerine yönlendirilmesini sağlar.

	AÇIKLAMA
Açıklama	Sanal IP tanımını tanımlamak için açıklama girmenizi sağlar.
Tür	Sanal IP eşleştirme türünü belirler. **Shared** veya **One-to-one** seçeneklerinden biri seçilebilir.

Gerçek IP Adresi	Trafiğin yönlendirileceği gerçek IP adresini belirtir.
Yerel IP Adresi	Sanal IP tanımında kullanılacak yerel ağ IP adresini belirtir.
Arayüz	Sanal IP tanımının ilişkilendirileceği ağ arayüzünü belirler.

YÖNLENDİRME

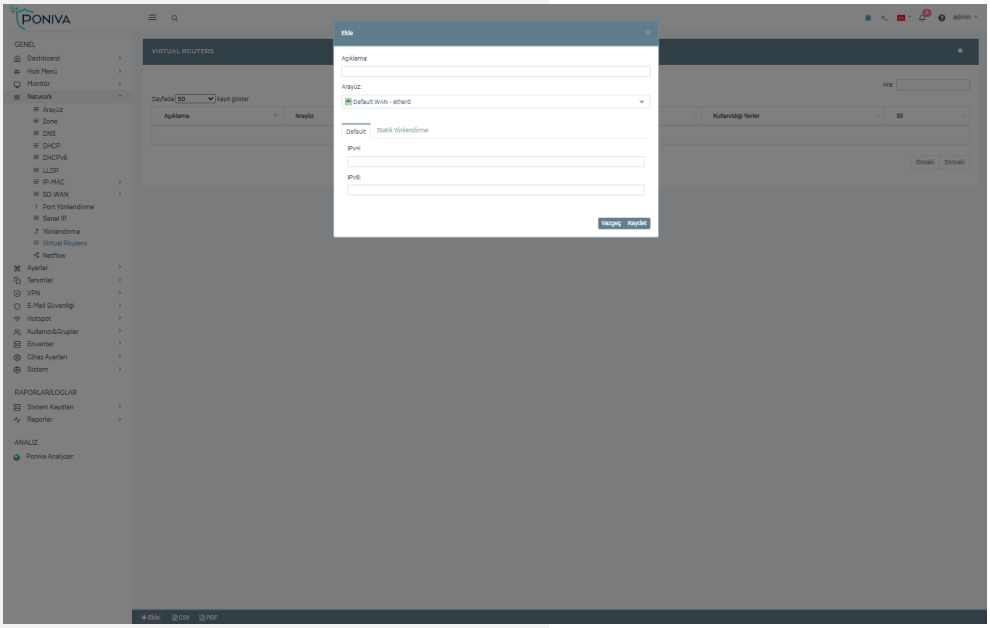
Yönlendirme bölümünden IPv4 ve IPv6 ağları için yönlendirme kuralları tanımlayabilirsiniz.



VIRTUAL ROUTERS

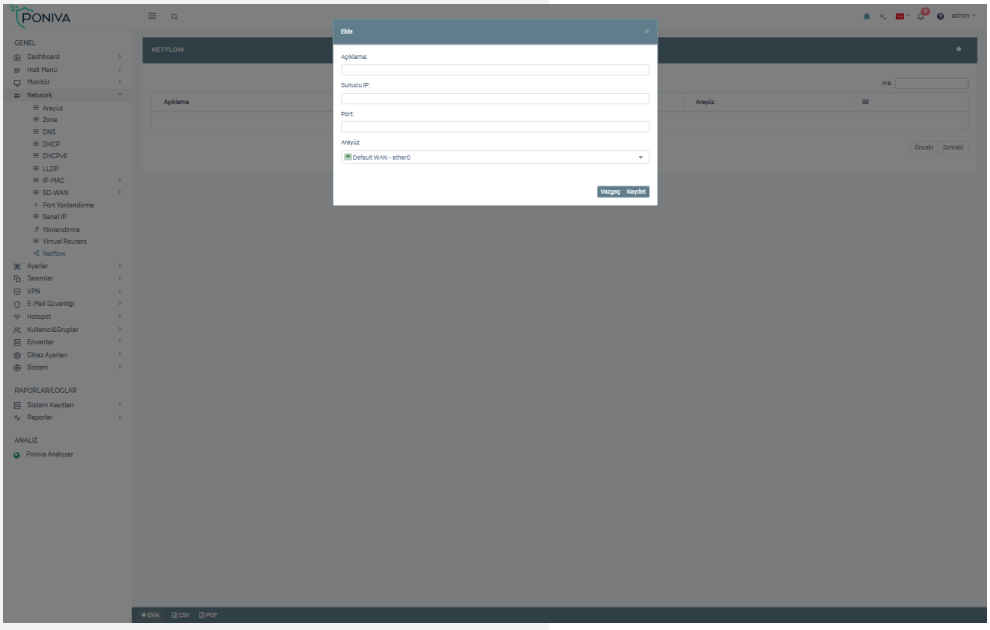
Virtual Router, firewall cihazı üzerinde farklı ağların yönlendirme işlemlerini birbirinden bağımsız olarak yönetmeyi sağlayan bir özelliktir.

Bu özellik sayesinde aynı fiziksel firewall üzerinde birden fazla sanal yönlendirme alanı oluşturulabilir. Her Virtual Router, kendisine tanımlanan ağlar ve yönlendirme kuralları doğrultusunda trafik iletimini gerçekleştirir.



NETFLOW

NetFlow, ağ üzerinden geçen IP trafiğine ilişkin akış bilgilerini toplayarak trafik yoğunluğunun, kaynak ve hedef IP adreslerinin, kullanılan protokollerin ve veri miktarlarının analiz edilmesini sağlayan bir ağ izleme teknolojisidir.



AYARLAR

NAC

Yetkili Switchler

Bu bölümde, firewall ile haberleşmesine izin verilen switch cihazlarını tanımlayabilirsiniz. Tanımlanan switchlerin, karşılıklı iletişimin sağlanabilmesi için ilgili yapılandırmanın switch tarafında da yapılması gerekir.

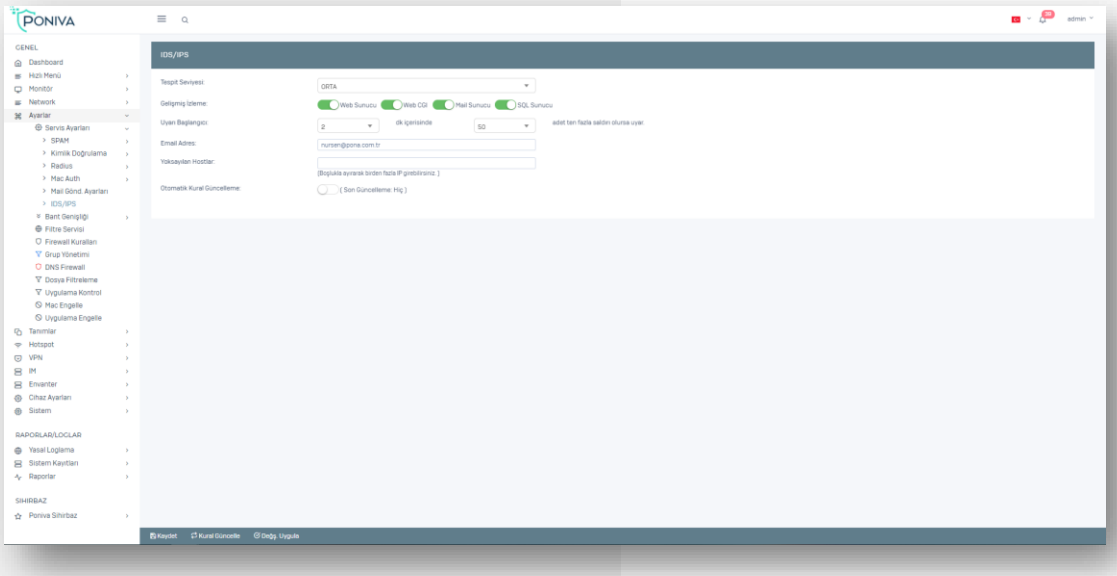
İzinli MAC

Bu bölümde tanımlanan MAC adreslerine sahip cihazların firewall tarafından izinli olarak değerlendirilmesini sağlayabilirsiniz.

IDS/IPS

Ayarlar

Sisteme yönelik saldırı girişimleri, Saldırı Tespit Sistemi (IDS) ve Saldırı Önleme Sistemi (IPS) tarafından izlenir ve yapılandırmaya bağlı olarak engellenir. Belirlediğiniz zaman aralığında saldırı sayısı tanımlanan eşiğe ulaştığında, sistem tarafından kayıtlı e-posta adresine bilgilendirme mesajı gönderilir.



Dos Koruma

DoS Koruma, firewall üzerinden geçen ağ trafiğinde hizmetlerin erişilebilirliğini olumsuz etkileyebilecek aşırı trafik, bağlantı isteği ve tarama faaliyetlerinin tespit edilmesine ve sınırlandırılmasına yardımcı olan bir güvenlik özelliğidir. DoS koruma parametreleri, ilgili trafik türüne ait eşik değerlerinin belirlenmesini ve yapılandırmaya bağlı olarak eşik aşımı durumlarında gerekli koruma işlemlerinin uygulanmasını sağlar.

	AÇIKLAMA
ip_src_session	Kaynak IP adresi bazında IP trafiğine ait oturum veya bağlantı yoğunluğunun kontrol edilmesini sağlar.
ip_dst_session	Hedef IP adresi bazında IP trafiğine ait oturum veya bağlantı yoğunluğunun kontrol edilmesini sağlar.

tcp_syn_flood	TCP bağlantı başlangıç isteklerinin (SYN) aşırı artmasıyla oluşabilecek SYN Flood saldırılarına karşı koruma sağlar.
tcp_port_scan	TCP portlarına yönelik tarama faaliyetlerinin tespit edilmesine yardımcı olur.
tcp_src_session	Kaynak IP adresi bazında TCP oturum sayısının kontrol edilmesini sağlar.
tcp_dst_session	Hedef IP adresi bazında TCP oturum sayısının kontrol edilmesini sağlar.
udp_flood	Aşırı miktarda UDP paketi gönderilmesiyle oluşabilecek UDP Flood saldırılarına karşı koruma sağlar.
udp_scan	UDP portlarına yönelik tarama faaliyetlerinin tespit edilmesine yardımcı olur.
udp_src_session	Kaynak IP adresi bazında UDP oturum veya trafik yoğunluğunun kontrol edilmesini sağlar.
udp_dst_session	Hedef IP adresi bazında UDP oturum veya trafik yoğunluğunun kontrol edilmesini sağlar.
icmp_flood	Aşırı miktarda ICMP paketi gönderilmesiyle oluşabilecek ICMP Flood saldırılarına karşı koruma sağlar.
icmp_sweep	Birden fazla IP adresine yönelik ICMP tarama veya keşif faaliyetlerinin tespit edilmesine yardımcı olur.
icmp_src_session	Kaynak IP adresi bazında ICMP trafik yoğunluğunun kontrol edilmesini sağlar.
icmp_dst_session	Hedef IP adresi bazında ICMP trafik yoğunluğunun kontrol edilmesini sağlar.

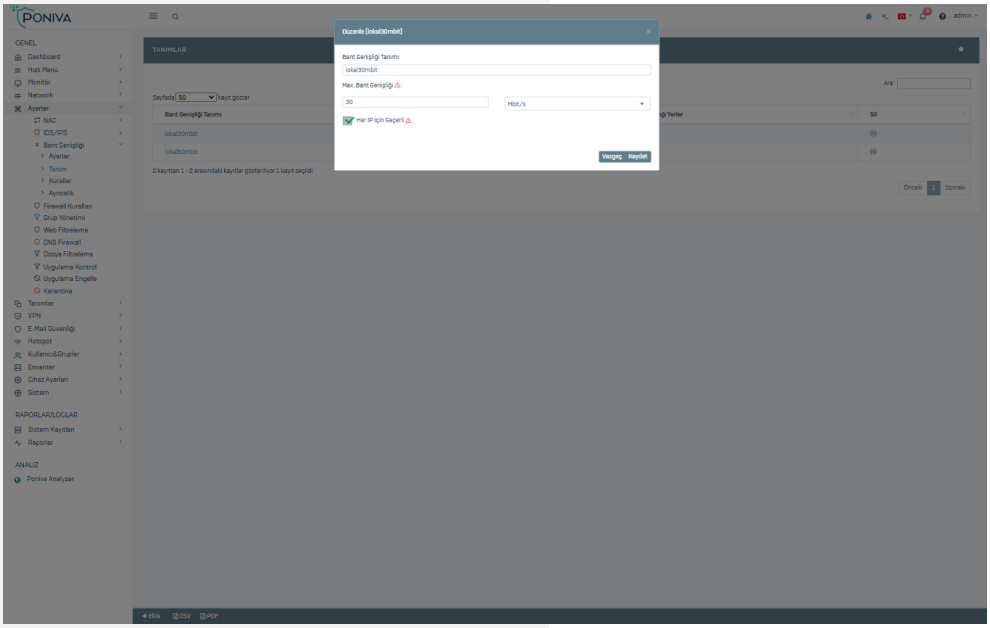
BANT GENİŞLİĞİ

Bant Genişliği bölümünden kullanıcıların veya belirli ağ trafiğinin internet kullanım hızını sınırlandırabilirsiniz. Tanımladığınız kurallar ile indirme ve yükleme hızlarını kontrol edebilir, ağ ve protokol bilgilerine göre bant genişliği limitleri belirleyebilirsiniz.

Ayarlar

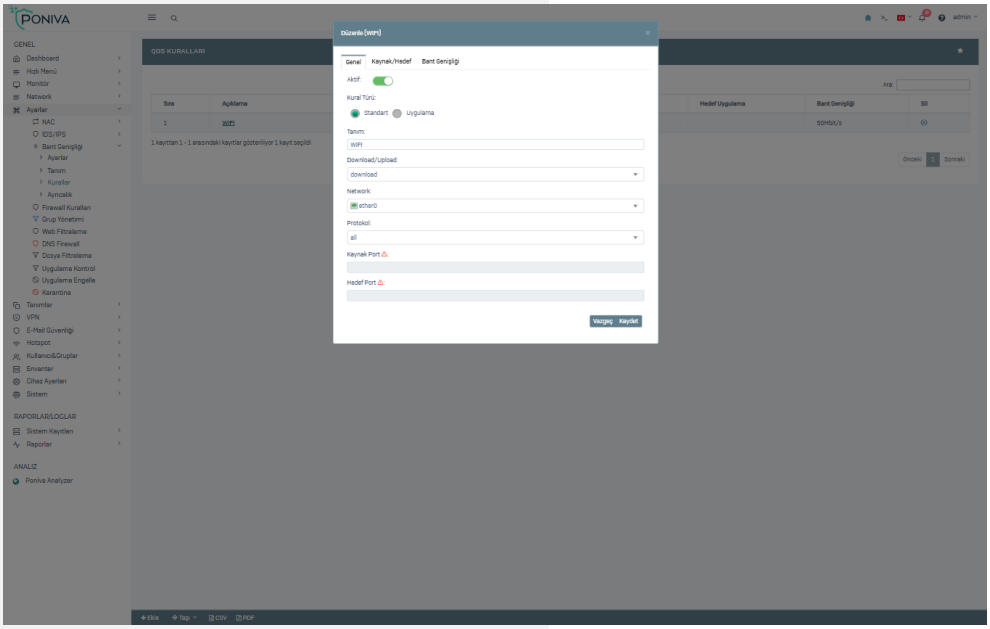
Bu bölümden bant genişliği yönetimi servisini etkinleştirebilir veya devre dışı bırakabilirsiniz.

Tanım



	AÇIKLAMA
Açıklama	Bant genişliği yapılandırmasını tanımlamak için açıklama girmenizi sağlar.
Max. Bant Genişliği	Bant genişliği kurallarında kullanılabilecek azami bant genişliğini belirler. (kbit/s, kbyte/s, mbit/s, mbte/s)
Her IP İçin Geçerli	Etkinleştirildiğinde belirlenen bant genişliği limitinin her IP adresi için ayrı ayrı uygulanmasını sağlar.

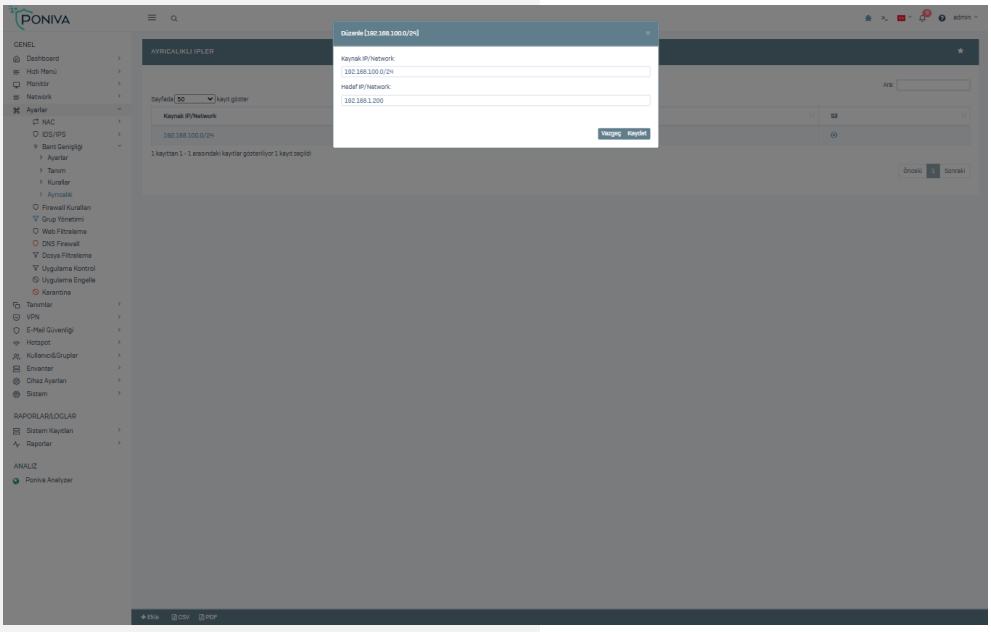
Kurallar



	AÇIKLAMA
Aktif	Kuralı etkinleştirir veya devre dışı bırakır.
Kural Türü	Kuralın hangi trafik türüne veya koşula göre uygulanacağını belirler.
Tanım	Kuralı tanımlamak için açıklama girmenizi sağlar.
Download/Upload	Kuralın indirme, yükleme veya her iki yöndeki trafik için uygulanacağını belirler.
Network	Kuralın geçerli olacağı ağı belirtir.
Protokol	Kuralın uygulanacağı iletişim protokolünü belirler.
Kaynak Port	Trafiğin kaynak portunu belirtir. (Port aralığı için örneğin 10000-20000 gibi kullanabilirsiniz.)
Hedef Port	Trafiğin hedef portunu belirtir.
Kaynak	Kuralın uygulanacağı trafiğin kaynak IP adresini veya kaynak ağını belirtir. Tüm adresler için checkboxı işaretleyin ya da belirli adresleri seçebilirsiniz.
Hedef	Kuralın uygulanacağı trafiğin hedef IP adresini veya hedef ağını belirtir. Tüm adresler için checkboxı işaretleyin ya da belirli adresleri seçebilirsiniz.
BW Limit	Kural kapsamında uygulanacak bant genişliği limitini belirler.
Öncelik	Bant genişliği kurallarının uygulanma önceliğini belirler.
Bu Kuraldan Sonraki Kuralları Uygulama	Bu kural eşleştiğinde kendisinden sonra gelen kuralların değerlendirilmesini durdurur.

Ayrıcalık

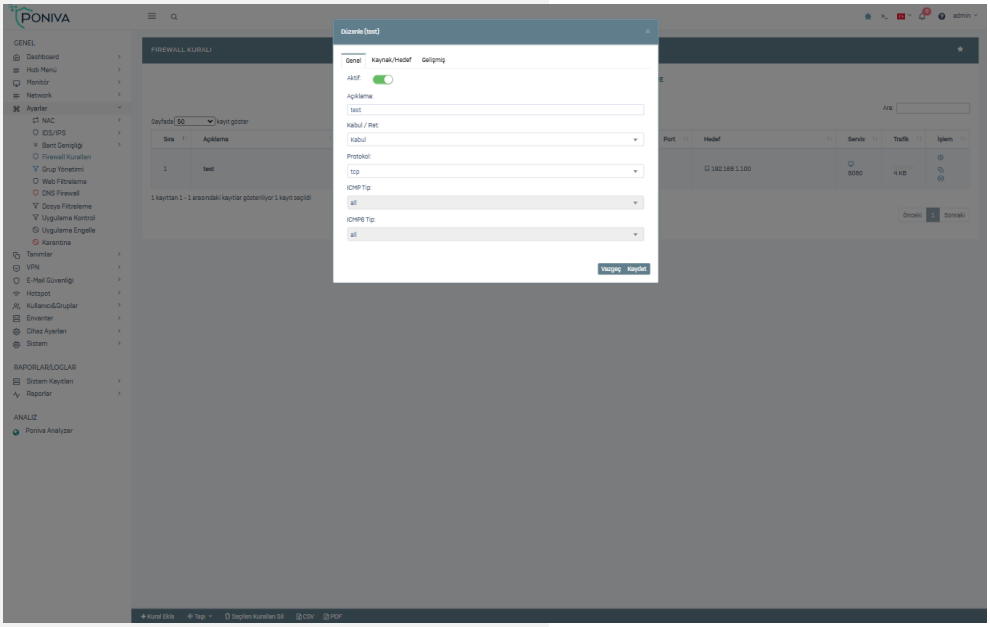
Ayrıcalık tanımları, belirli kaynak ve hedef IP adresleri arasındaki trafiğin bant genişliği kısıtlamalarından muaf tutulmasını sağlar. Bu sayede tanımlanan IP adresleri arasındaki trafik için bant genişliği limitleri uygulanmaz.



FİREWALL KURALLARI

Firewall kuralları, ağ trafiğinin kabul edilmesini, reddedilmesini veya kayıt altına alınmasını (log) kontrol etmenizi sağlar. Kurallar; kaynak ve hedef IP adresleri, protokol, port ve diğer trafik kriterlerine göre tanımlanabilir.

Kuralların sıralaması önemlidir. Ağ trafiği, tanımlanan kuralların sırasına göre değerlendirilir ve eşleşen kurala bağlı olarak ilgili işlem uygulanır. Birden fazla kural oluşturarak ağ trafiğinin nasıl yönetileceğini belirleyebilirsiniz. Bu nedenle kuralların doğru sıralanması, güvenlik politikalarının beklenen şekilde uygulanması açısından önem taşır.



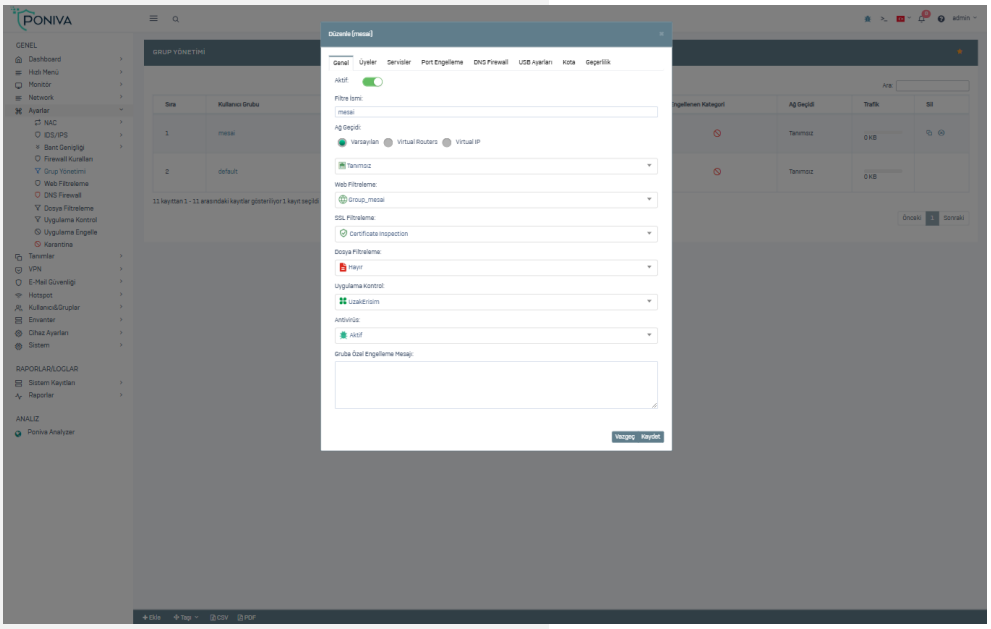
	AÇIKLAMA
Aktif	Firewall kuralını etkinleştirir veya devre dışı bırakır.
Açıklama	Kuralın amacını belirtmek için açıklama girmenizi sağlar.
Kabul / Red / Log	Kuralla eşleşen trafik için uygulanacak işlemi belirler. **Kabul** trafiğe izin verir, **Red** trafiği engeller, **Log** ise trafiğin kayıt altına alınmasını sağlar.
Protokol	Kuralın uygulanacağı ağ protokolünü belirler.
Kaynak Adres	Trafiğin kaynak adresini tanımlamak için kullanılacak adres nesnesini, adres grubunu, active directory kullanıcısını, dinamik kategoriyi ya da grup yönetimindeki ilgili grubu belirtir.
Kaynak IP	Kaynak adres manuel seçilirse bu bölüm aktif olur ve kaynak IP veya Network girmelisiniz. Birden fazla IP veya Network için ‘virgül’ kullanabilirsiniz. Tümü için ‘any’ girmelisiniz.
Kaynak Port	Trafiğin kaynak portunu belirtir. Birden fazla port için ‘virgül’ , port aralığı için ‘–‘ kullanabilirsiniz.
Hedef Adres	Trafiğin hedef adresini tanımlamak için kullanılacak adres nesnesini, adres grubunu, active directory kullanıcısını,

	dinamik kategoriyi ya da grup yönetimindeki ilgili grubu belirtir.
Hedef IP	Hedef adres manuel seçilirse bu bölüm aktif olur ve hedef IP veya Network girmelisiniz. Birden fazla IP veya Network için 'virgül' kullanabilirsiniz. Tümü için 'any' girmelisiniz.
Hedef Port	Trafiğin hedef portunu belirtir. Birden fazla port için 'virgül' , port aralığı için '–' kullanabilirsiniz.
IP Limit	Kural kapsamında IP adresleri veya trafik için uygulanacak sınırlandırmayı belirler.
Koşul Yön (Opsiyonel)	Kuralın uygulanacağı trafik yönüne ilişkin koşulu belirler.
Geliş Arayüz	Trafiğin firewall'a giriş yaptığı ağ arayüzünü belirtir.
Çıkış Arayüz	Trafiğin firewall üzerinden çıkacağı ağ arayüzünü belirtir.
Geçerlilik	Kuralın uygulanacağı zaman aralığını belirler.
Statefull	Etkinleştirildiğinde bağlantı durumunu takip ederek trafik için durum bilgisine dayalı denetim uygulanmasını sağlar.
Kayıt Tut	Kuralla eşleşen trafikle ilgili kayıtların oluşturulmasını sağlar.

GRUP YÖNETİMİ

Grup Yönetimi, kullanıcılar için farklı güvenlik ve filtreleme politikaları oluşturmanızı sağlar. Kullanıcıları IP adreslerine, adres gruplarına veya Active Directory hesaplarına göre gruplandırabilir; her grup için web, SSL, dosya ve uygulama filtreleme gibi özellikleri ayrı ayrı yapılandırabilirsiniz.

Birden fazla grup oluşturarak filtreleme politikalarını öncelik sırasına göre düzenleyebilirsiniz. Herhangi bir gruba dahil olmayan kullanıcılar **Default** grubuna dahil edilir ve bu grupta tanımlanan kurallara tabi olur.

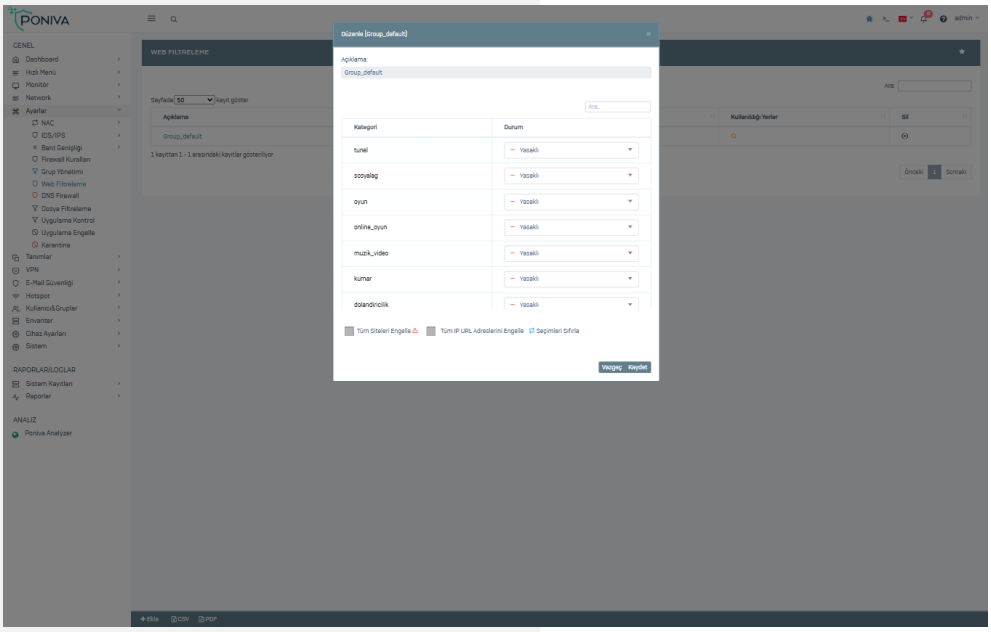


	AÇIKLAMA
Aktif	Grubu etkinleştirir veya devre dışı bırakır.
Filtre İsmi	Filtreleme grubuna verilecek adı belirtir.
Ağ Geçidi	Birden fazla internet hattı bulunması durumunda, grup üyelerinin internet trafiğinin hangi ağ geçidi üzerinden çıkacağını belirler.
Web Filtreleme	Seçilen web filtreleme tanımındaki izinli ve yasaklı kategorilerin grup üyelerine uygulanmasını sağlar. İstenirse bu grup için web filtreleme devre dışı bırakılabilir.
SSL Filtreleme	Grup üyelerinin HTTPS trafiğine uygulanacak SSL filtreleme yöntemini belirler. Deep Inspection veya Certificate Inspection seçeneklerinden biri seçilebilir. Deep Inspection kullanıldığında ilgili sertifikanın istemci bilgisayarlara yüklenmesi gerekir. İstenirse SSL filtreleme devre dışı bırakılabilir.
Dosya Filtreleme	Seçilen dosya filtreleme tanımında belirtilen dosya türlerinin veya uzantılarının engellenmesini sağlar.
Uygulama Kontrol	Seçilen uygulama kontrolü tanımındaki kuralların grup üyelerinin trafiğine uygulanmasını sağlar.
Antivirüs	Etkinleştirildiğinde, desteklenen trafik ve protokoller üzerinde antivirüs denetimi uygulanmasını sağlar.
Gruba Özel Engelleme Mesajı	Grup üyeleri engellenen bir siteye erişmeye çalıştığında gösterilecek mesajı tanımlamanızı sağlar.
Filtreleme Türü	Filtrelemenin IP adreslerine veya Active Directory kullanıcılarına göre uygulanacağını belirler.
Grup Üyeleri	Gruba dahil edilecek adresleri, adres gruplarını veya Active Directory kullanıcılarını seçmenizi sağlar.
Servisler	İlgili grup için sadece belirli servislere izin verebilmenizi sağlar.
Port Engelleme	Seçilen portlara veya port gruplarına erişimi engeller. Tüm çıkışların engellenmesi seçildiğinde grup üyelerinin ağ erişimi kapsamlı biçimde kısıtlanabilir.
DNS Firewall	Seçilen DNS Firewall tanımındaki kuralların grup üyelerine uygulanmasını sağlar.
USB Bellek Kullanımı	Grup üyelerinin USB bellek kullanımını kontrol etmenizi sağlar. Bu özellik Windows bilgisayarlarda ek istemci yazılımı gerektirir.
USB 3G Modem	Grup üyelerinin USB 3G modem kullanımını kontrol etmenizi sağlar. Bu özellik Windows bilgisayarlarda ek istemci yazılımı gerektirir.
Kota Yönetimi	Kullanıcıların belirlenen veri kullanım kotasına ulaşması veya kotayı aşması durumunda uyarı gösterilmesini ve yapılandırmaya bağlı olarak internet erişiminin kısıtlanmasını sağlar.
Toplam Limit /KB	Grup üyelerinin tamamı için geçerli olacak toplam bant genişliği limitini belirtir.
Kullanıcı Limiti /KB	Her bir grup üyesi için ayrı ayrı uygulanacak bant genişliği limitini belirtir.

Geçerlilik	Filtreleme kurallarının hangi gün ve saatlerde uygulanacağını belirler.

WEB FİLTRELEME

Web Filtreleme, kullanıcıların internet erişimini belirlenen site kategorilerine göre kontrol etmenizi sağlar. İzin verilen veya engellenen kategorileri tanımlayarak kullanıcıların hangi web sitelerine erişebileceğini yönetebilirsiniz.



	AÇIKLAMA
Açıklama	Web filtreleme tanımını açıklamak için bir metin girmenizi sağlar.
Kategoriler	Filtreleme kapsamında uygulanacak site kategorilerini seçmenizi sağlar. Seçilen kategorilere göre ilgili web sitelerine erişime izin verilebilir veya erişim engellenebilir.

DNS FİREWALL

DNS Firewall, DNS sorgularını denetleyerek zararlı veya istenmeyen alan adlarına erişimi kontrol etmenizi sağlar. Tanımlanan kurallar doğrultusunda belirli alan adlarına yönelik DNS sorgularını engelleyerek kullanıcıların bu alan adlarına erişmesini kısıtlayabilirsiniz.

	AÇIKLAMA
Açıklama	DNS firewall tanımını açıklamak için bir metin girmenizi sağlar.
Botnet C&C İsteğini Blok Portalına Yönlendir	Etkinleştirildiğinde, botnet komuta-kontrol (C&C) adreslerine yönelik DNS isteklerinin engellenmesini ve yapılandırmaya bağlı olarak blok portalına yönlendirilmesini sağlar.

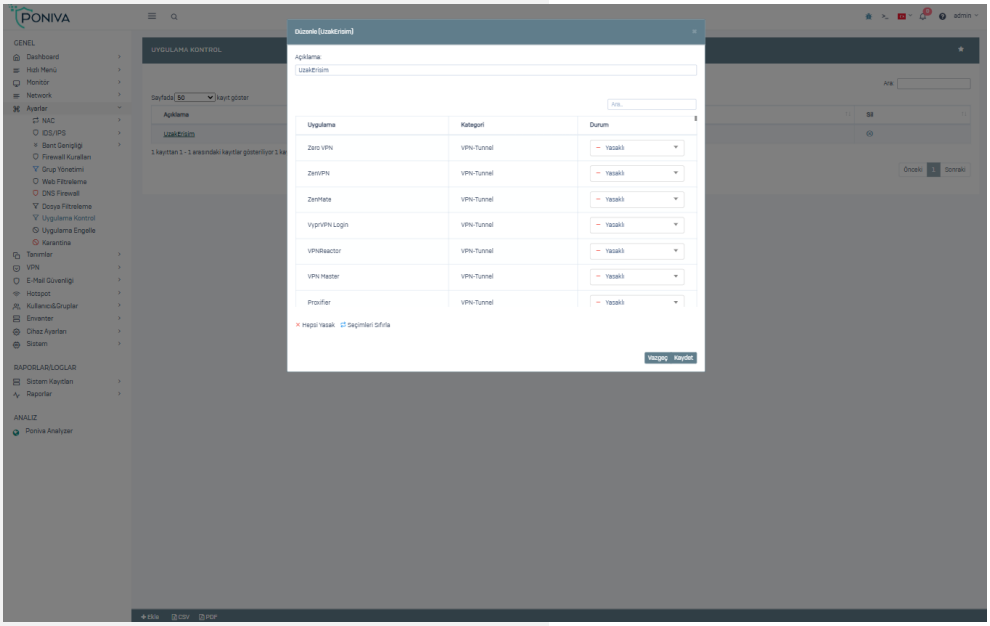
Google, Bing için Güvenli Aramaya Zorla	Etkinleştirildiğinde, Google ve Bing arama motorlarında Güvenli Arama özelliğinin kullanılmasını sağlar. Böylece uygunsuz içeriklerin arama sonuçlarında görüntülenmesi sınırlandırılır.
Youtube için Güvenli Aramaya Zorla	Etkinleştirildiğinde, YouTube'un kısıtlı içerik filtrelemesini uygulamasını sağlar.
Domain Filtreleme	Belirli alan adlarına (domain) izin vermek veya bu alan adlarına erişimi engellemek için yerel statik domain filtreleri tanımlamanızı sağlar.
DNS Translation	Belirli bir alan adı için döndürülen IP adresinin, tanımlanan farklı bir IP adresiyle değiştirilmesini sağlar. Örneğin, www.example.com alan adı için 192.168.3.4 IP adresinin döndürülmesini sağlayabilirsiniz.
Name Server	DNS sorgularının çözümlenmesinde kullanılacak ad DNS sunucularını tanımlamanızı sağlar.

DOSYA FİLTRELEME

Bu bölümde, engellenmesini istediğiniz dosya uzantılarını ve türlerini tanımlayabilirsiniz. Oluşturduğunuz filtreleri Grup Filtreleme bölümünden ilgili gruba atayarak, belirtilen dosya türlerinin o gruptaki kullanıcılar tarafından indirilmesini veya aktarılmasını engelleyebilirsiniz.

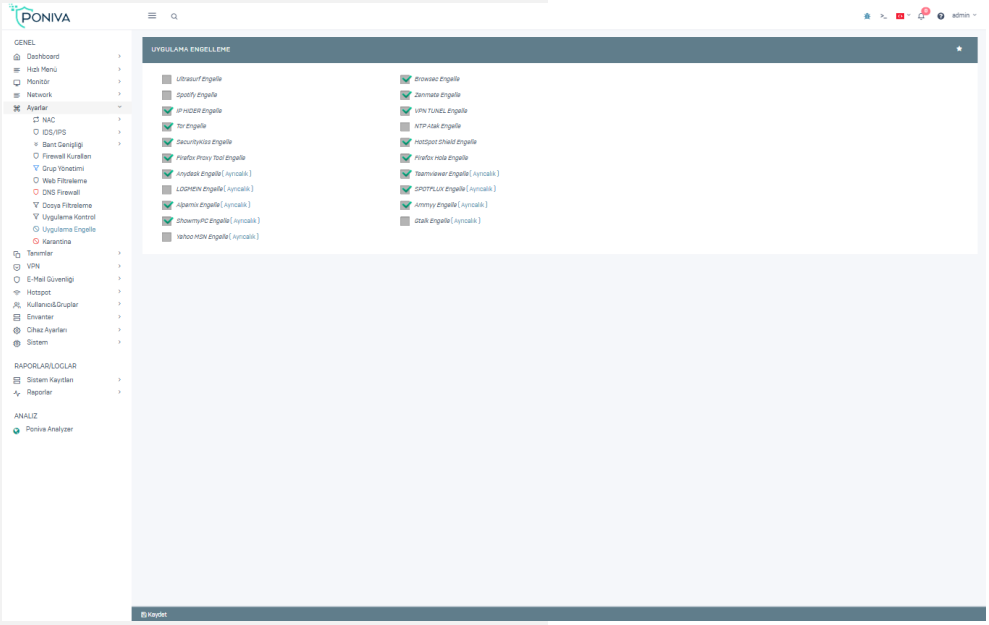
UYGULAMA KONTROL

Bu bölümde, Layer 7 (Uygulama Katmanı) üzerinden kontrol etmek veya engellemek istediğiniz uygulamaları seçerek kaydedebilirsiniz. Oluşturduğunuz uygulama filtrelerini Grup Filtreleme bölümünden ilgili gruba atayarak, seçilen uygulamaların o gruptaki kullanıcılar tarafından kullanılmasını engelleyebilirsiniz.



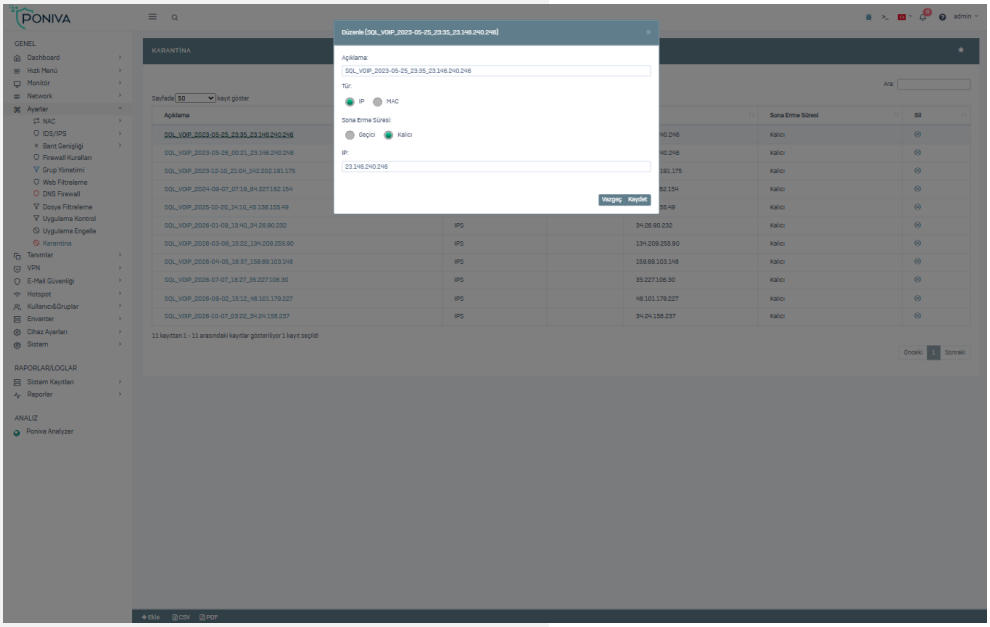
UYGULAMA ENGELLE

Bu bölümde seçilen uygulamalar, sistem tarafından otomatik olarak tespit edilerek engellenir. Örneğin, AnyDesk uygulaması seçildiğinde, ilgili trafik engellenerek AnyDesk bağlantısı kısıtlanır. Ayrıcalık listesinde tanımlanan istisnalar bu uygulamanın dışında tutulur.



KARANTİNA

Bu bölümde, IP adresi veya MAC adresi bazında cihazları karantinaya alabilirsiniz. Engelleme işlemi kalıcı veya belirli bir süreyle sınırlı olacak şekilde yapılandırılabilir. Karantinaya alınan cihazların ağ erişimi kısıtlanır.



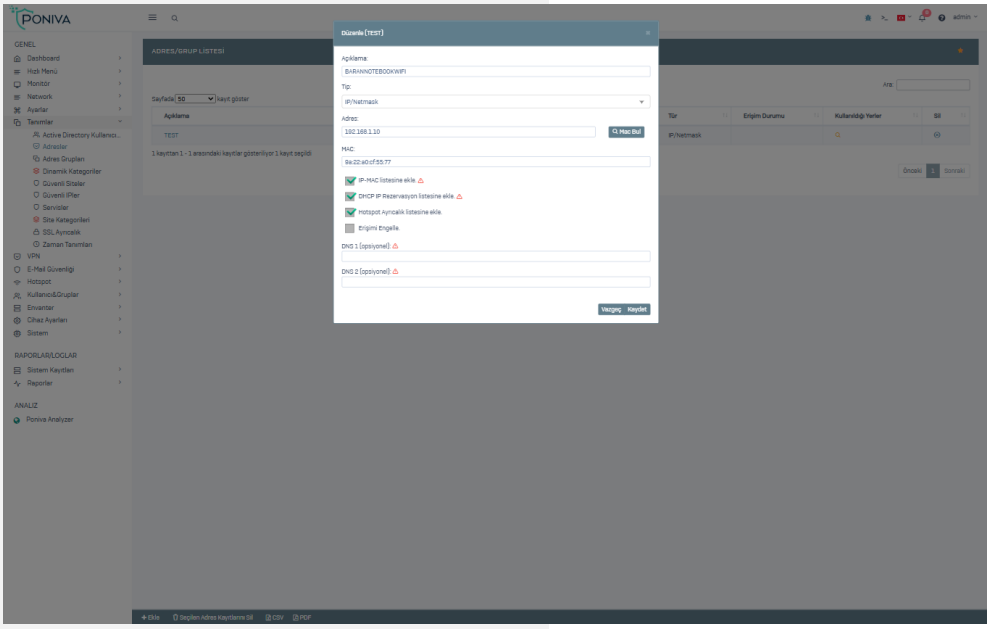
TANIMLAR

ACTIVE DIRECTORY

Active Directory kullanıcılarınızı görüntüleyebilirsiniz. Active Directory yapılandırma ayarları Cihaz Ayarları -> Active Directory menüsünden yapılmaktadır.

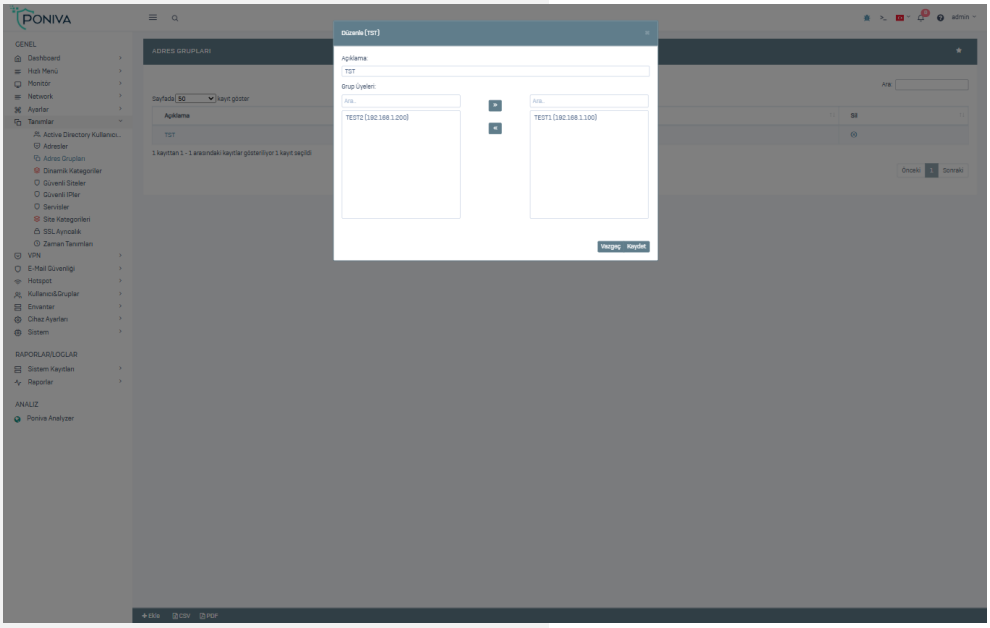
ADRESLER

Adres tanımlamalarını bu bölümde yapabilirsiniz. IP adresi, network, IP aralığı veya ülke tanımlayabilirsiniz. Bu tanımlar firewall kuralları, bant genişliği, grup yönetimi veya port yönlendirmede '**üyeler**' bölümünde kullanabilirsiniz. Buraya eklediğiniz kayıtları IP-MAC, DHCP IP Rezervasyon ya da Hotspot Ayrıcalık listesine de ekle diyerek kayıtları oraya da kolayca tanımlayabilirsiniz.



ADRES GRUPLARI

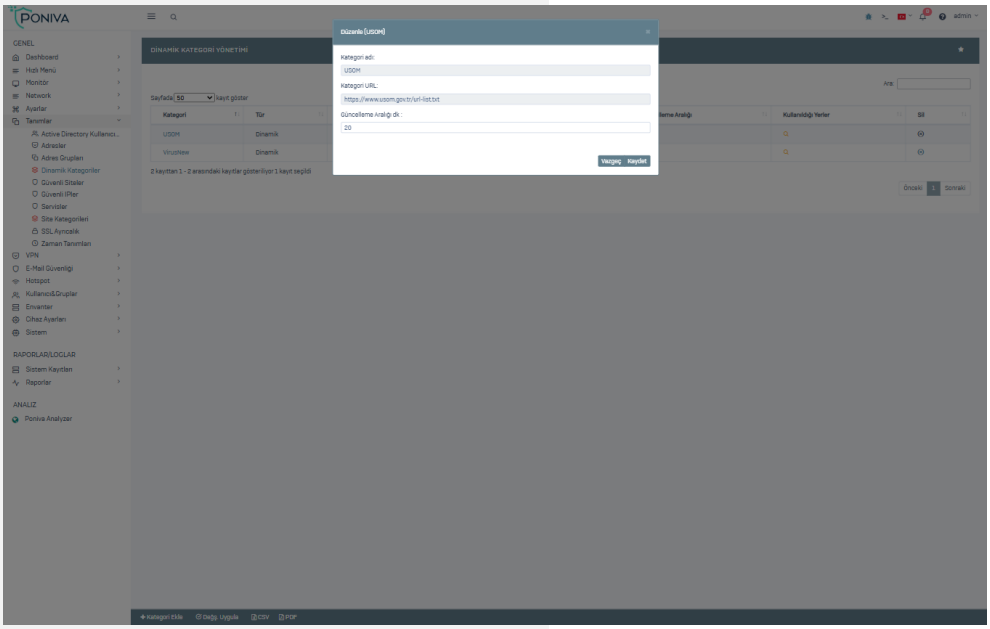
Adresler bölümünde yaptığınız tanımları bu bölümde gruplandırma yapabilirsiniz. Bu gruplandırmaları firewall kuralları, grup yönetimi veya port yönlendirmede '**üyeler**' bölümünde kullanabilirsiniz.



DİNAMİK SİTE KATEGORİLERİ

Bu bölümde, belirli URL kaynaklarından otomatik olarak güncellenen site kategorileri oluşturabilir, bu kategorilere erişim izni verebilir veya erişimi engelleyebilirsiniz. Tanımladığınız URL listesinin güncelleme aralığını belirleyerek listenin manuel işlem gerektirmeden yenilenmesini sağlayabilirsiniz.

Sistemde varsayılan olarak USOM kategorisi bulunmaktadır. USOM tarafından sağlanan zararlı ve erişimi engellenmesi önerilen adres listesi, güncelleme aralıklarına bağlı olarak PONIVA Firewall'a otomatik aktarılır. Grup Yönetimi bölümünden USOM kategorisini ilgili gruba atayarak listedeki adreslere erişimi engelleyebilirsiniz.



GÜVENLİ SİTELER

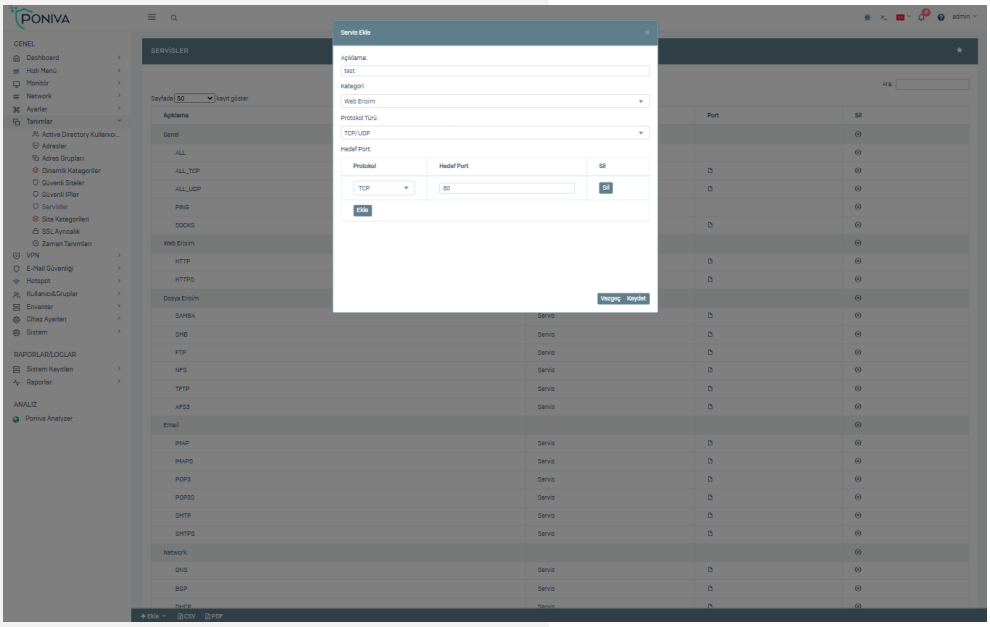
Bu bölümde tanımlanan siteler, ilgili yapılandırma kapsamında filtreleme ve loglama işlemlerinin dışında tutulur. 5651 sayılı Kanun ve ilgili mevzuat kapsamındaki yükümlülüklerinizi yerine getirmek için gerekli trafik kayıtlarının tutulduğundan emin olun.

GÜVENLİ IP'LER

Bu bölümde tanımlanan yerel ağ IP adreslerinin HTTP trafiği filtreleme ve loglama işlemlerinin dışında tutulmasını sağlayabilirsiniz. 5651 sayılı Kanun ve ilgili mevzuat kapsamındaki yükümlülüklerinizi yerine getirmek için gerekli trafik kayıtlarının tutulduğundan emin olun.

SERVİSLER

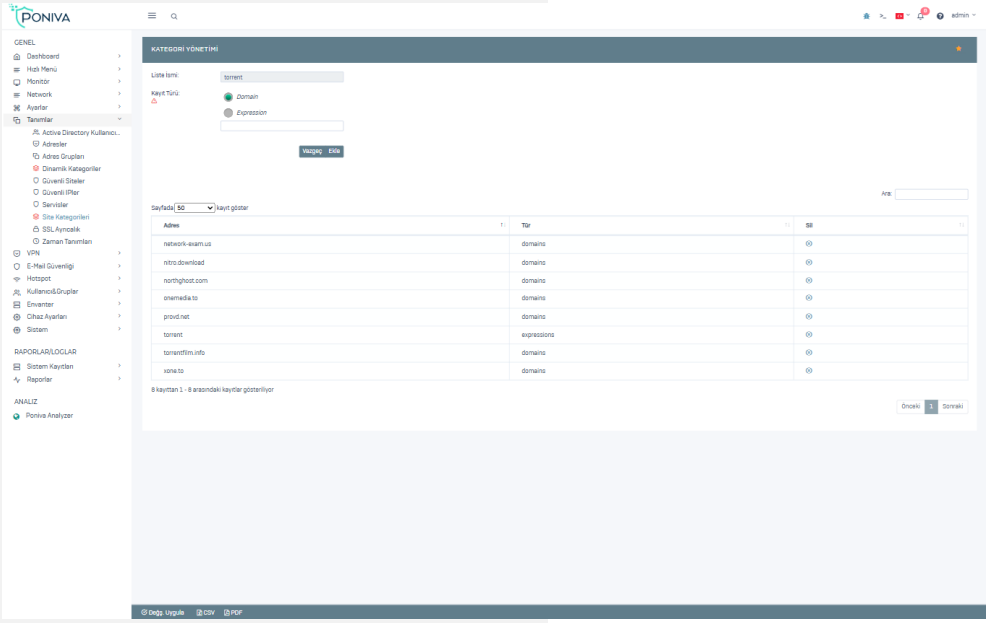
Bu bölümde, ağ trafiğini protokol ve hedef port bilgilerine göre tanımlayarak servisler oluşturabilirsiniz. Her servise açıklama ve kategori atayabilir, TCP, UDP gibi protokolleri ve hedef port numaralarını belirleyebilirsiniz. Oluşturulan servisler, grup yönetiminde kullanılarak ilgili grup için belirli servislere izin verebilirsiniz.



SİTE KATEGORİLERİ

Bu bölümde, belirli sitelere izin vermek veya erişimi engellemek amacıyla site kategorileri oluşturabilirsiniz. Kategori tanımlarında alan adı (domain) veya adres çubuğunda geçen belirli kelimelere göre eşleştirme yapan ifadeler (expression) kullanabilirsiniz. Örneğin, adresinde "oyun" kelimesi geçen siteleri eşleştirebilirsiniz.

Oluşturduğunuz kategorilere ilişkin izin ve engelleme işlemlerini Web Filtreleme bölümünden yapılandırabilirsiniz.



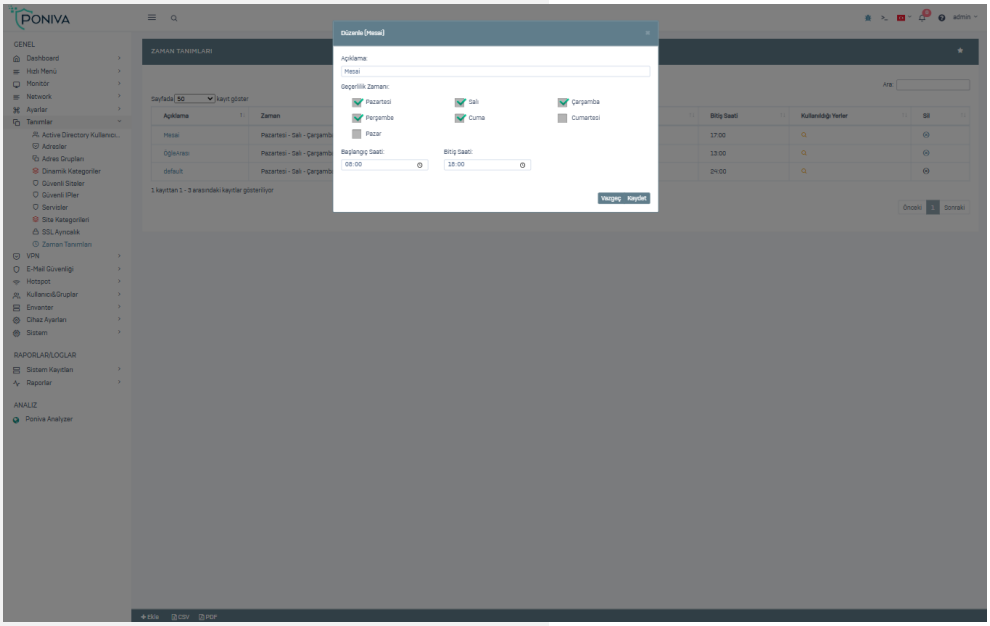
SSL AYRICALIK

Bu bölümde, SSL trafiği filtreleme ve loglama işlemlerinin dışında tutulacak yerel ağ (LAN) IP adreslerini tanımlayabilirsiniz.Tanımlanan IP adreslerine ait **HTTPS trafiği, SSL filtreleme ve loglama işlemlerine dahil edilmez.** 5651 sayılı Kanun ve ilgili mevzuat kapsamındaki yükümlülüklerinizi yerine getirmek için gerekli trafik kayıtlarının tutulduğundan emin olun.

ZAMAN TANIMLARI

Bu bölümde, belirli gün ve saat aralıkları için zaman tanımlamaları oluşturabilirsiniz. Oluşturduğunuz zaman tanımlarını, diğer menülerde **Geçerlilik** kriteri olarak kullanarak erişim ve kullanım sürelerini sınırlandırabilirsiniz.

Örnek: SSL VPN kullanıcı tanımında, geçerlilik kriteri olarak *Mesai Saatleri* seçildiğinde kullanıcının VPN erişimi yalnızca tanımlanan mesai saatleri içerisinde geçerli olur.

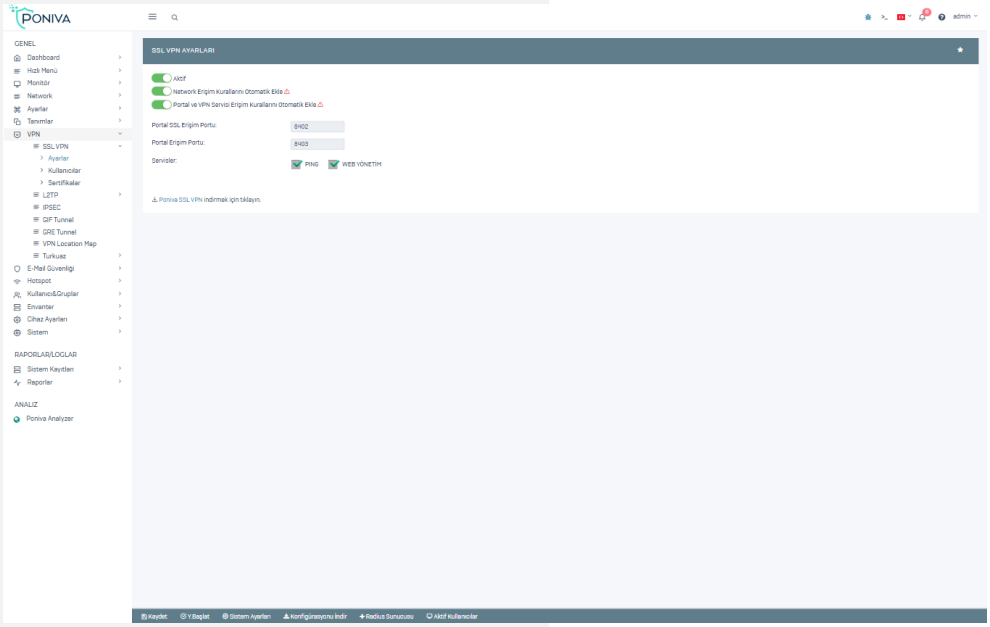


VPN

SSL VPN

Uzak kullanıcılar, bilgisayarlarına **Poniva SSL** uygulamasını kurarak firewall cihazına güvenli bir VPN bağlantısı oluşturabilir ve yetkilendirildikleri ağ kaynaklarına uzaktan erişebilirler.

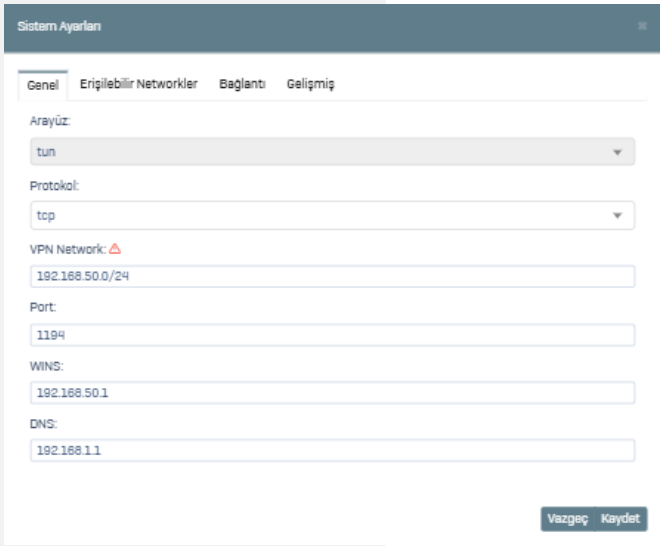
Ayarlar



	AÇIKLAMA
Aktif	SSL VPN servisini etkinleştirir veya devre dışı bırakır.

Network Kurallarını Otomatik Ekle	SSL VPN bağlantıları için gerekli ağ kurallarının otomatik olarak eklenmesini sağlar.
Portal ve VPN Servisi Erişim Kurallarını	Portal ve VPN servislerine erişim için kullanılacak kuralların yapılandırılmasını sağlar.
Konfigürasyonu İndir	VPN bağlantısı için gerekli yapılandırma dosyasını indirmenizi sağlar.
Aktif Kullanıcılar	SSL VPN üzerinden cihaza bağlı olan kullanıcıları görüntülemenizi sağlar.

Sistem Ayarları

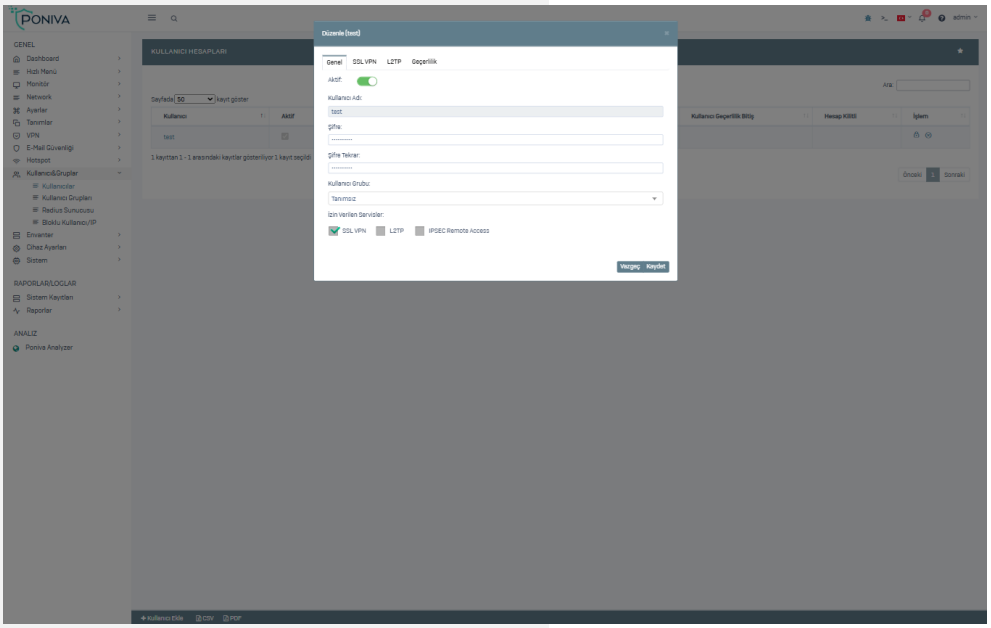


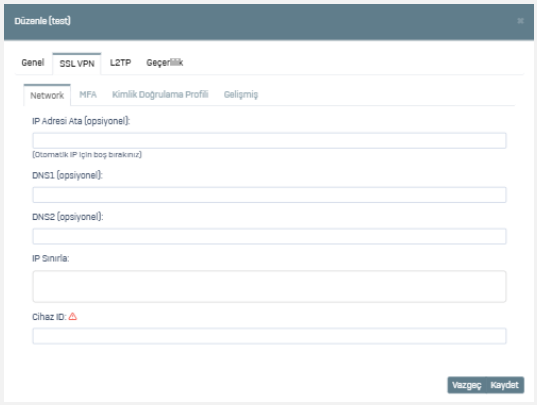
	AÇIKLAMA
Arayüz	Varsayılan ‘tun’ seçilidir.
Protokol	SSL VPN bağlantısında kullanılacak iletişim protokolünü (TCP veya UDP) seçebilirsiniz.
VPN Network	VPN bağlantısı kuran istemcilere atanacak IP adreslerinin bulunduğu ağ bloğunu tanımlayabilirsiniz. Bu ağ, yerel ağınızdan farklı olmalıdır. (Örneğin 192.168.50.0/24)
Port	SSL VPN bağlantılarında kullanılacak port numarasını belirleyebilirsiniz. Varsayılan port **1194** olarak ayarlanmıştır.
WINS	VPN istemcilerinin kullanacağı WINS sunucusunun IP adresini tanımlayabilirsiniz.
DNS	VPN istemcilerinin alan adlarını IP adreslerine çözümlemek için kullanacağı DNS sunucusunu tanımlayabilirsiniz. Yerel kaynaklara erişim için firewall cihazınızın veya ağınızdaki DNS sunucusunun IP adresini girebilirsiniz.
Erişilebilir Networkler	VPN bağlantısı kuran kullanıcıların erişebileceği ağları belirleyebilirsiniz. **Manuel** seçeneğini tercih ederek kullanıcıların erişmesine izin vermek istediğiniz ağları tanımlayabilirsiniz.

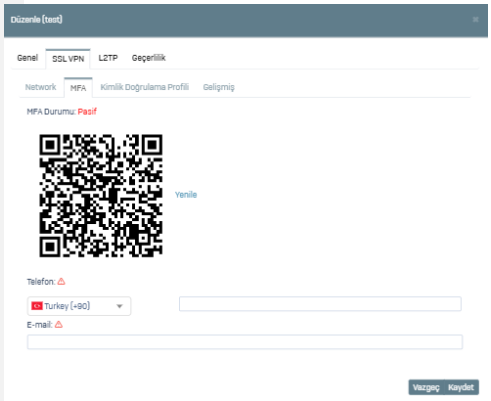
Clientlar birbirlerini görebilir	Bu seçenek etkinleştirildiğinde, VPN bağlantısı kuran istemcilerin birbirleriyle iletişim kurmasına izin verilir. Devre dışı bırakıldığında istemciler arasındaki doğrudan iletişim engellenir.
Aynı sertifika ile birden fazla bağlantı yapılabilir	Bu seçenek etkinleştirildiğinde, aynı sertifika kullanılarak birden fazla VPN bağlantısı kurulabilir.
Kullanıcılar bu sunucu üzerinden çıkış yapsın	Bu seçenek etkinleştirildiğinde, VPN kullanıcılarının internet trafiği firewall üzerinden yönlendirilir. Böylece kullanıcılar internete firewall cihazının bağlantısı üzerinden erişebilir.
Auth Digest Algorithm (Kimlik Doğrulama Özet Algoritması)	VPN bağlantısında veri bütünlüğünü doğrulamak ve verilerin aktarım sırasında değiştirilmediğini kontrol etmek için kullanılacak özeti (hash) algoritmasını belirleyebilirsiniz. **Default** seçeneği, sistemin varsayılan algoritma ayarlarının kullanılmasını sağlar.
Data Encryption Algorithms (Veri Şifreleme Algoritmaları)	VPN bağlantısı sırasında aktarılan verilerin şifrelenmesinde kullanılacak algoritmaları belirleyebilirsiniz. **Default** seçeneği, sistemin varsayılan şifreleme algoritması ayarlarının kullanılmasını sağlar.

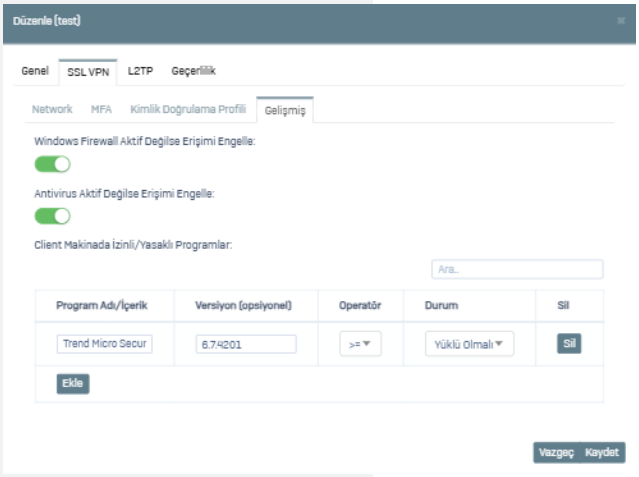
*Kullanıcılar bu sunucu üzerinden çıkış yapsın ‘evet’ seçilirse, Erişilebilir Networkler pasif olur.

Kullanıcılar









	AÇIKLAMA
Aktif	Kullanıcı hesabını etkinleştirir veya devre dışı bırakır.
Kullanıcı Adı	SSL VPN bağlantısında kimlik doğrulama için kullanılacak kullanıcı adını belirtir.
Şifre	Kullanıcının SSL VPN bağlantısı sırasında kimlik doğrulaması yapabilmesi için kullanılacak şifreyi belirler.
Kullanıcı Grubu	Kullanıcı grubu tanımları üzerinden genel kimlik doğrulama profilini ve geçerlilik süresini merkezi olarak yönetebilirsiniz.
İzin Verilen Servisler	Kullanıcının erişebileceği servisleri seçmelisiniz. SSL VPN bağlantısı için **SSL VPN** seçeneğini etkinleştirmelisiniz.
IP Adresi Ata (Opsiyonel)	Kullanıcıya sabit bir IP adresi atayabilir veya otomatik IP atanması için bu alanı boş bırakabilirsiniz.
DNS1 (Opsiyonel)	VPN bağlantısında kullanılacak birincil DNS sunucusunun IP adresini belirleyebilirsiniz.
DNS2 (Opsiyonel)	VPN bağlantısında kullanılacak ikincil DNS sunucusunun IP adresini belirleyebilirsiniz.
IP Sınırla	Kullanıcı yalnızca belirtilen IP adreslerinden VPN bağlantısı sağlayabilir.
Cihaz ID	Kullanıcının VPN bağlantısını belirli bir cihazın MAC adresiyle ya da mobil uygulama için uuid ile sınırlandırabilirsiniz.

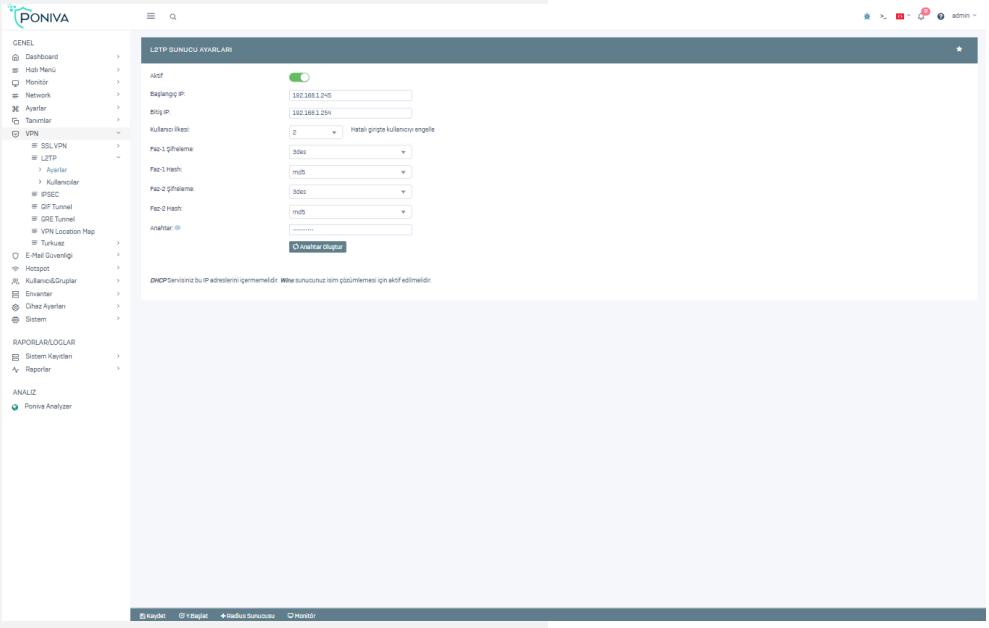
MFA	Etkinleştirildiğinde kullanıcı, Google/Microsoft Authenticator uygulaması, sms ya da email aracılığıyla ek doğrulama yapmalıdır.
Telefon	2 Faktörlü doğrulamayı telefonunuz ile yapacaksanız girmelisiniz.
E-mail	2 Faktörlü doğrulamayı email ile yapacaksanız girmelisiniz.
Geçerlilik	Kullanıcının VPN bağlantısı kurabileceği gün ve saat aralığını belirleyebilirsiniz.
Geçerlilik Bitiş	Kullanıcı hesabının geçerlilik süresini belirleyebilirsiniz. Tanımlanan tarihten sonra kullanıcı hesabı geçersiz olur.
Kimlik Doğrulama Profili	Kullanıcı için uygulanacak kimlik doğrulama profilini seçebilirsiniz. Eğer kullanıcı bir gruba üye ise bu alan pasif olur.
Windows Firewall Aktif Değilse Erişimi Engelle	Etkinleştirildiğinde, istemci bilgisayarda Windows Güvenlik Duvarı aktif değilse VPN erişimi engellenir.
Antivirüs Aktif Değilse Erişimi Engelle	Etkinleştirildiğinde, istemci bilgisayarda antivirüs koruması aktif değilse VPN erişimi engellenir.
Client Makinada İzinli/Yasaklı Programlar	İstemci bilgisayarda çalıştırılmasına izin verilen veya engellenen programları belirleyebilirsiniz.

Sertifikalar

Kullanıcılar için ayrı sertifikalar oluşturabilir ve bu sertifikaların geçerlilik sürelerini belirleyebilirsiniz. Böylece kullanıcıların güvenli bağlantı kurmasını sağlayabilir, sertifikaların kullanım süresini yönetebilirsiniz.

L2TP

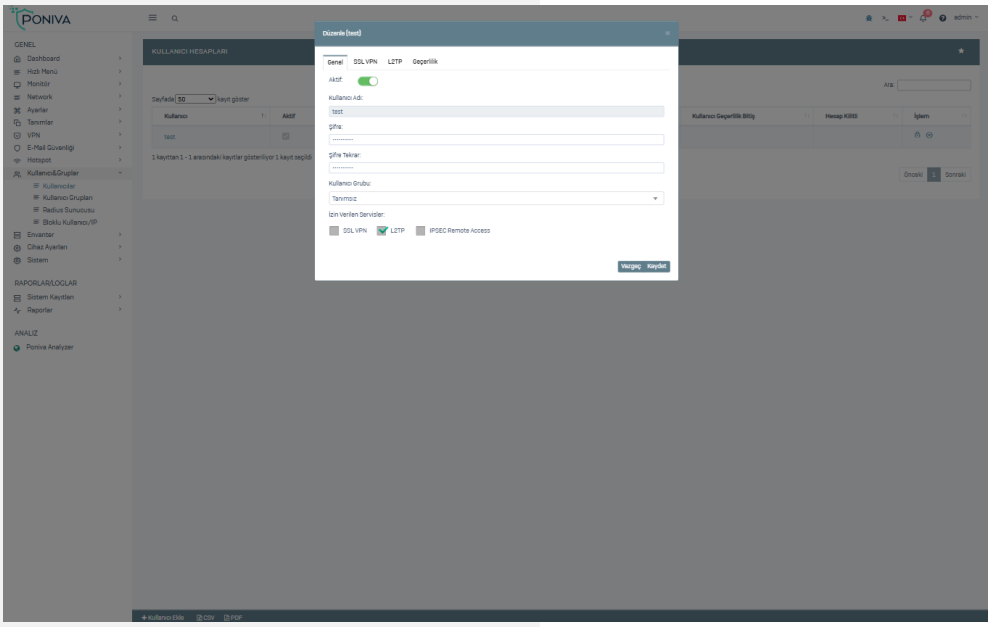
Diğer VPN protokollerinden farklı olarak, L2TP (Layer 2 Tunnel Protocol) üzerinden geçen trafik ile ilgili herhangi bir gizlilik veya şifreleme sağlamaz.



Ayarlar

	AÇIKLAMA
Aktif	L2TP servisini etkinleştirir veya devre dışı bırakır.
Başlangıç IP	Kullanıcılarına dağıtılacak IP adresi aralığının başlangıç adresini belirtir.
Bitiş IP	Kullanıcılarına dağıtılacak IP adresi aralığının bitiş adresini belirtir.
Kullanıcı İlkesi	Kullanıcının kaç hatalı girişte engelleneceğini seçebilirsiniz.

Kullanıcılar

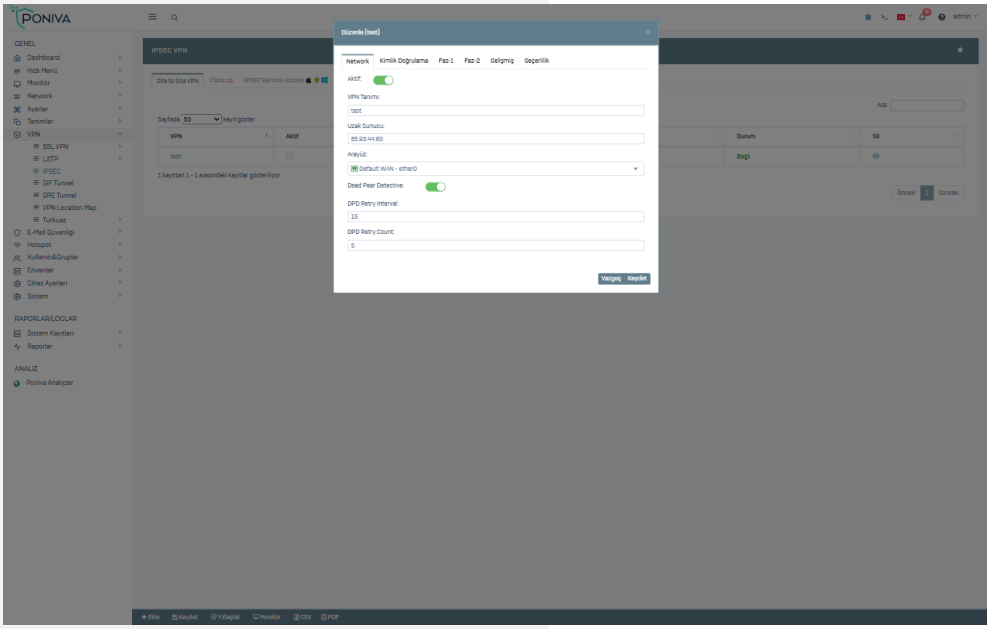


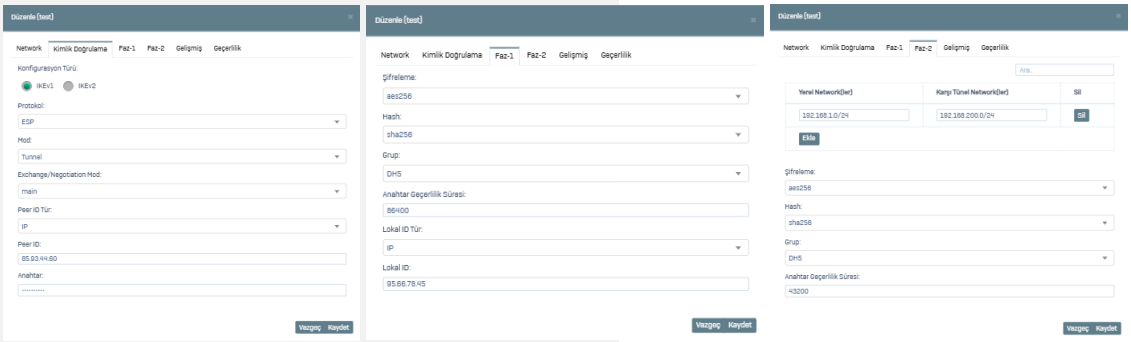
	AÇIKLAMA
Aktif	Kullanıcı hesabını etkinleştirir veya devre dışı bırakır.
Kullanıcı Adı	SSL VPN bağlantısında kimlik doğrulama için kullanılacak kullanıcı adını belirtir.
Şifre	Kullanıcının SSL VPN bağlantısı sırasında kimlik doğrulaması yapabilmesi için kullanılacak şifreyi belirler.
İzin Verilen Servisler	Kullanıcının erişebileceği servisleri seçmelisiniz. L2TP bağlantısı için **L2TP** seçeneğini etkinleştirmelisiniz.
IP Adresi Ata (Opsiyonel)	Kullanıcıya sabit bir IP adresi atayabilir veya otomatik IP atanması için bu alanı boş bırakabilirsiniz.

IPSEC

Site to Site VPN

Site to Site VPN, farklı konumlarda bulunan iki veya daha fazla ağı güvenli bir VPN bağlantısı üzerinden birbirine bağlamanızı sağlar. Bu sayede farklı lokasyonlardaki yerel ağlar arasında şifreli iletişim kurabilir ve ağ kaynaklarına uzaktan erişim sağlayabilirsiniz. Bağlantının kurulabilmesi için her iki tarafta da VPN yapılandırmasının yapılması gerekir.





	AÇIKLAMA
Aktif	VPN tanımını etkinleştirir veya devre dışı bırakır.
VPN Tanımı	Bir VPN tanımı girmelisiniz.
Uzak Sunucu	Bağlantı kurulacak uzak VPN sunucusunun IP adresini veya alan adını belirtir.
Arayüz	VPN bağlantısının kullanılacağı yerel ağ arayüzünü belirler.
Dead Pear Detective	Uzak VPN cihazının erişilebilirliğini kontrol eder.
DPD Retry Interval	Uzak cihazdan yanıt alınamadığında yeniden kontrol için beklenecek süreyi belirler.
DPD Retry Count	Uzak cihazın yanıt vermemesi durumunda yapılacak kontrol sayısını belirler.
Konfigurasyon Türü	VPN bağlantısında kullanılacak yapılandırma türünü belirler.

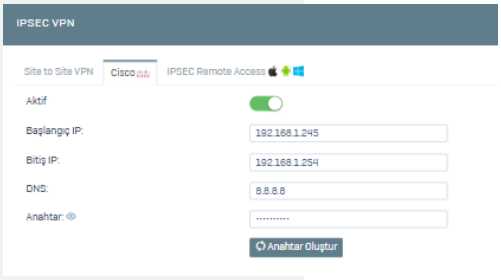
Protokol	VPN bağlantısında kullanılacak IPsec protokolünü belirler.
Mod	VPN bağlantısında kullanılacak çalışma modunu belirler.
Exchange/Negotiation Mod	Faz 1 anahtar değişimi ve kimlik doğrulama sürecinde kullanılacak müzakere modunu belirler.
Peer ID Tür	Uzak VPN cihazının kimliğinin hangi türde doğrulanacağını belirler.
Peer ID	Uzak VPN cihazının kimlik bilgisini belirtir.
Anahtar	VPN bağlantısında kullanılacak önceden paylaşılan anahtarı (PSK) belirtir.
Faz1/Şifreleme	Faz 1 aşamasında kullanılacak şifreleme algoritmasını belirler.
Faz1/Hash	Faz 1 aşamasında kullanılacak bütünlük doğrulama algoritmasını belirler.
Faz1/Grup	Faz 1 anahtar değişiminde kullanılacak Diffie-Hellman grubunu belirler.
Faz1/Anahtar Geçerlilik Süresi	Faz 1 güvenlik ilişkisinin (SA) geçerlilik süresini belirler.
Faz1/Lokal ID Tür	Yerel VPN cihazının (Poniva'nın) kimliğinin hangi türde tanımlanacağını belirler.
Faz1/Lokal ID	Yerel VPN cihazının (Poniva'nın) karşı tarafa bildireceği kimlik bilgisini belirtir.
Faz2/Yerel Network-Karşı Tünel Network	VPN üzerinden birbirine erişecek yerel ve uzak ağları tanımlar.
Faz2/Şifreleme	Faz 2 aşamasında veri trafiği için kullanılacak şifreleme algoritmasını belirler.
Faz2/Hash	Faz 2 aşamasında veri bütünlüğü doğrulamasında kullanılacak algoritmayı belirler.
Faz2/Grup	Faz 2 anahtar değişiminde kullanılacak Diffie-Hellman grubunu belirler.
Faz2/Anahtar Geçerlilik Süresi	Faz 2 güvenlik ilişkisinin (SA) geçerlilik süresini belirler.
Ping Kontrol	VPN bağlantısının erişilebilirliğini belirli aralıklarla kontrol eder.
Interface Oluştur	VPN bağlantısı için gerekli sanal arayüzün oluşturulmasını sağlar.
Firewall Kuralını Otomatik Ekle	VPN trafiği için gerekli firewall kurallarının otomatik oluşturulmasını sağlar.
Failover	Birincil VPN bağlantısı kullanılamadığında yedek bağlantıya geçişi sağlar.
Geçerlilik	VPN tanımının hangi süre boyunca geçerli olacağını belirler.

*VPN bağlantısının kurulabilmesi için aynı ayarların karşı taraftaki cihazda da tanımlanması gerekir.

*Yerel ve uzak ağların IP adresi aralıkları birbiriyle çakışmamalıdır.

Cisco

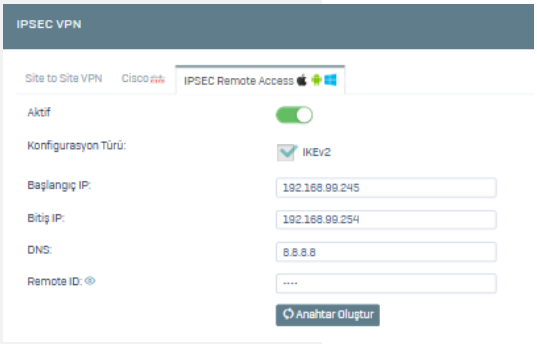
Cisco uyumlu IPsec VPN bağlantısı için gerekli ayarları bu bölümden yapılandırabilirsiniz.



	AÇIKLAMA
Aktif	IPsec Cisco VPN yapılandırmasını etkinleştirir veya devre dışı bırakır.
Başlangıç IP	VPN bağlantısı için kullanılacak IP adres aralığının başlangıç adresini belirler.
Bitiş IP	VPN bağlantısı için kullanılacak IP adres aralığının son adresini belirler.
DNS	VPN bağlantısı üzerinden kullanılacak DNS sunucusunun IP adresini belirtir.
Anahtar	VPN bağlantısında kimlik doğrulama amacıyla kullanılacak anahtarı belirler.
Anahtar Oluştur	VPN bağlantısında kullanılmak üzere yeni bir anahtar oluşturur.

IPSEC Remote Access

Bu bölümden, uzak kullanıcıların IPsec VPN protokolü üzerinden kurum ağına güvenli bir şekilde erişebilmesini sağlayabilirsiniz. IKEv2 protokolü sayesinde, bu özelliği destekleyen modern işletim sistemleri ve cihazlar üzerinden ek bir VPN istemcisi kurmadan bağlantı oluşturabilirsiniz.



	AÇIKLAMA
Aktif	IPsec Remote Access VPN yapılandırmasını etkinleştirir veya devre dışı bırakır.
Konfigürasyon Türü	VPN bağlantısında kullanılacak IKE protokolünü belirler. IKEv2, anahtar değişimi ve kimlik doğrulama işlemlerinde kullanılır.
Başlangıç IP	VPN bağlantısı için kullanılacak IP adres aralığının başlangıç adresini belirler.

Bitiş IP	VPN bağlantısı için kullanılacak IP adres aralığının son adresini belirler.
DNS	VPN bağlantısı üzerinden kullanılacak DNS sunucusunun IP adresini belirtir.
Remote ID	Uzak VPN istemcisinin kimlik doğrulama sürecinde kullanılacak kimlik bilgisini belirtir.
Anahtar Oluştur	VPN bağlantısında kullanılmak üzere yeni bir Remote ID oluşturur.

IPsec Remote Access ayarlarını yapılandırdıktan sonra VPN bağlantısı kuracak kullanıcıları oluşturmanız veya mevcut kullanıcılarınızı düzenlemeniz gerekir.

Bunun için sol menüden **Kullanıcı & Gruplar → Kullanıcılar** bölümüne gidin. Yeni bir kullanıcı oluştururken veya mevcut bir kullanıcıyı düzenlerken **IPsec Remote Access** servisinin etkin olduğundan emin olun.

GIF TUNNEL

GIF Tunnel, iki ağ uç noktası arasında IP paketlerinin tünel üzerinden taşınmasını sağlayan bir tünelleme yöntemidir. Trafik şifrelenmediği için gizlilik ve veri güvenliği sağlamaz. Doğrudan bağlantısı bulunmayan ağlar arasında paket yönlendirmek veya Hurricane Electric gibi tünel sağlayıcıları üzerinden IPv6 bağlantısı elde etmek amacıyla kullanılabilir.

Not: GIF Tunnel, veri şifrelemesi sağlamadığından güvenli iletişim gerektiren bağlantılarda IPsec gibi şifreleme sağlayan yöntemler tercih edilmelidir.

	AÇIKLAMA
Aktif	VPN tünelini aktif veya pasif duruma getirebilirsiniz.
Açıklama	Tüneli tanımlamak için açıklama girebilirsiniz.
Yerel IP (WAN)	Tünel bağlantısında kullanılacak yerel WAN arayüzünü seçmelisiniz.
Uzak IP	Karşı uçtaki cihazın dış (WAN) IP adresini girmelisiniz. Örneğin: 88.176.43.57
Tunnel Tür	Tünelde kullanılacak IP protokolünü IPv4 veya IPv6 olarak seçmelisiniz.
Lokal Tunel IP	Yerel tünel ucuna atanacak IPv4 veya IPv6 adresini girmelisiniz.
Uzak Tunel IP	Karşı tünel ucuna atanacak IPv4 veya IPv6 adresini girmelisiniz.
Tür	Tünel bağlantısı için kullanılacak türü seçmelisiniz.
Karşı Tünel Ucundaki Lokal Network/Router Ağ Geçidi	Tünel türüne göre karşı uçta bulunan yerel ağın adresini veya kullanılacak yönlendirici ağ geçidini girmelisiniz.
Prefix	Tünel türü IPv6 olarak seçildiğinde, IPv6 adresi için kullanılacak ağ önek uzunluğunu belirtmelisiniz.

GRE TUNNEL

GRE Tunnel, iki uç nokta arasında IP paketlerinin tünel üzerinden taşınmasını sağlayan bir tünelleme yöntemidir. Trafik şifrelenmediği için veri gizliliği sağlamaz. Doğrudan bağlı olmayan ağlar arasında paket yönlendirmek ve farklı ağları birbirine bağlamak amacıyla kullanılabilir.

GRE Tunnel üzerinden IPv4, IPv6 veya her iki trafik türü de taşınabilir. Güvenli iletişim gerektiren bağlantılarda GRE, IPsec gibi şifreleme sağlayan protokollerle birlikte kullanılabilir.

	AÇIKLAMA
Aktif	VPN tünelini aktif veya pasif duruma getirebilirsiniz.
Açıklama	Tüneli tanımlamak için açıklama girebilirsiniz.
Yerel IP (WAN)	Tünel bağlantısında kullanılacak yerel WAN arayüzünü seçmelisiniz.
Uzak IP	Karşı uçtaki cihazın dış (WAN) IP adresini girmelisiniz. Örneğin: 88.176.43.57
Tunnel Tür	Tünelde kullanılacak IP protokolünü IPv4 veya IPv6 olarak seçmelisiniz.
Lokal Tunel IP	Yerel tünel ucuna atanacak IPv4 veya IPv6 adresini girmelisiniz.
Uzak Tunel IP	Karşı tünel ucuna atanacak IPv4 veya IPv6 adresini girmelisiniz.
Tür	Tünel bağlantısı için kullanılacak türü seçmelisiniz.
Karşı Tünel Ucundaki Lokal Network/Router Ağ Geçidi	Tünel türüne göre karşı uçta bulunan yerel ağın adresini veya kullanılacak yönlendirici ağ geçidini girmelisiniz.
Prefix	Tünel türü IPv6 olarak seçildiğinde, IPv6 adresi için kullanılacak ağ önek uzunluğunu belirtmelisiniz.

VPN LOCATION MAP

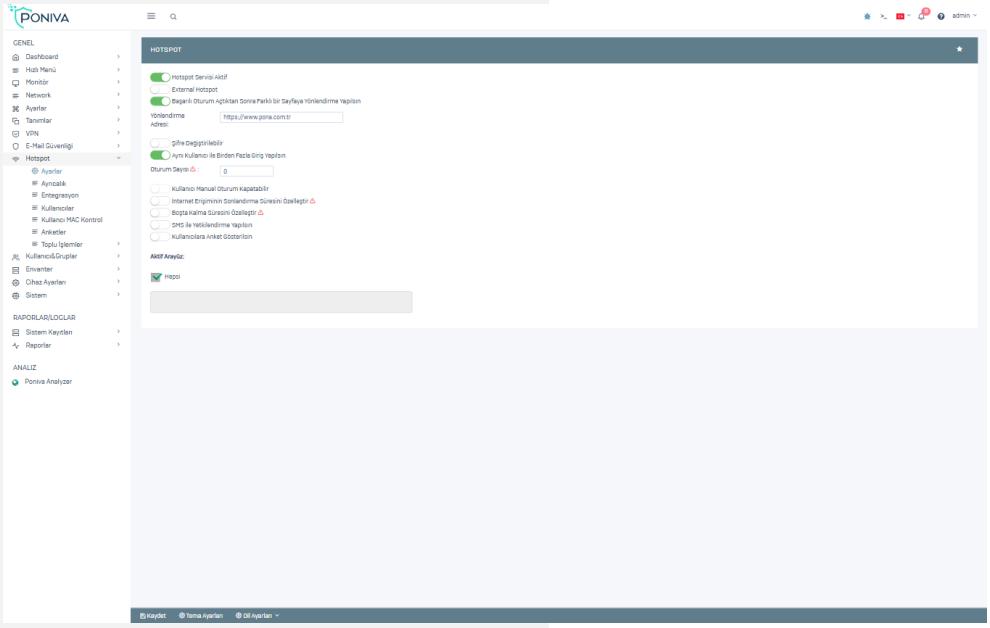
Bu bölümde, VPN bağlantısı üzerinden ağa erişim sağlayan kullanıcıları harita üzerinde görüntüleyebilirsiniz.

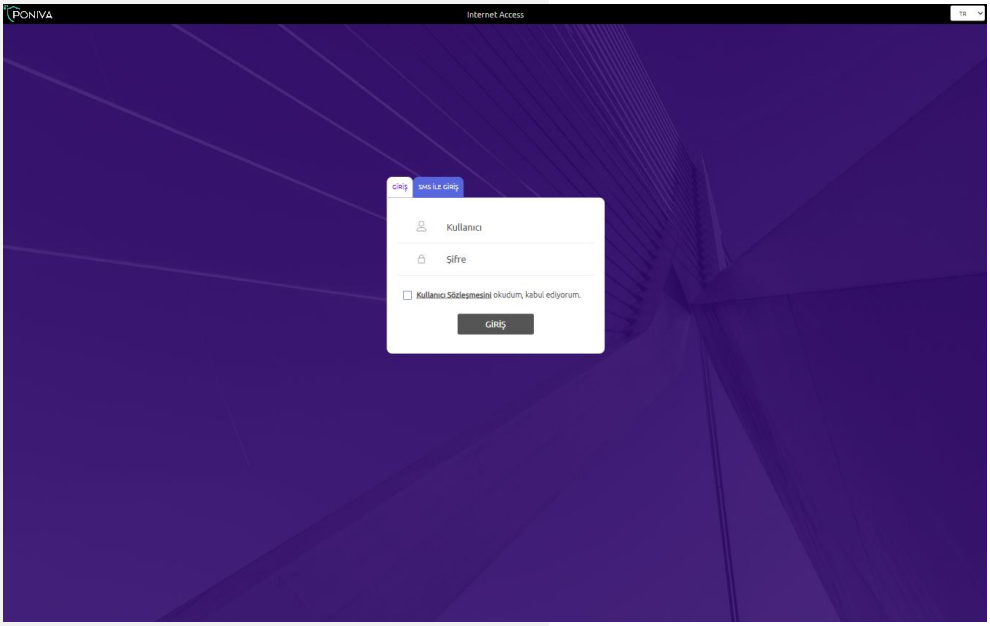
TURKUAZ

Turkuaz VPN, şube tarafında hiçbir yapılandırma gerektirmeyen (Zero-Touch) yerli tünelleme cihazı serisidir. Cihazın E0 portu internete bağlandığı anda merkezdeki PONIVA Firewall ile otomatik olarak eşleşir ve şubeyi merkez ağına dahil eder; şubede sabit IP adresine veya teknik personele ihtiyaç yoktur. Turkuaz VPN cihazlarına ait bağlantı ve yapılandırma ayarlarını bu bölümden yönetebilirsiniz.

HOTSPOT

AYARLAR





	AÇIKLAMA
Hotspot Servisi Aktif	Hotspot hizmetini aktif veya pasif duruma getirebilirsiniz.
External Hotspot	Hotspot kimlik doğrulama işlemlerinin harici bir sistem üzerinden gerçekleştirilmesini sağlar. (https://gatefi.io)
Başarılı Oturum Açıktan Sonra Farklı bir Sayfaya Yönlendirme Yapılsın	Kullanıcı başarılı bir şekilde oturum açıktan sonra yönlendirileceği web adresini belirleyebilirsiniz.
Şifre Değiştirilebilir	Hotspot kullanıcılarının mevcut şifrelerini değiştirebilmesine izin verir.
Aynı Kullanıcı ile Birden Fazla Giriş Yapılsın	Aynı kullanıcı hesabıyla birden fazla oturum açılmasına izin verir.

Kullanıcı Manuel Oturum Kapatabilir	Kullanıcıların hotspot oturumlarını kendilerinin sonlandırabilmesini sağlar.
İnternet Erişiminin Sonlandırma Süresini Özelleştir	Kullanıcının internet erişiminin sonlandırılacağı süreyi özelleştirmenizi sağlar.
Boşta Kalma Süresini Özelleştir	Kullanıcının belirli bir süre etkinlik göstermemesi durumunda oturumun sonlandırılacağı süreyi belirlemenizi sağlar.
SMS ile Yetkilendirme Yapılsın	Hotspot kullanıcılarının SMS doğrulaması aracılığıyla kimliklerini doğrulamasını sağlar.
Kullanıcılara Anket Gösterilsin	Hotspot kullanıcılarına oturum açma sürecinde veya yapılandırılan aşamada anket gösterilmesini sağlar.
Aktif Arayüz	Hotspot hizmetinin kullanılacağı ağ arayüzünü seçebilirsiniz.
Tema Ayarları	Hotspot giriş sayfasının görünümünü ve tasarımını yapılandırabilirsiniz.
Dil Ayarları	Hotspot giriş sayfasında kullanılacak dil ile ilgili özelleştirmeler yapabilirsiniz.

*Wi-Fi kullanıcılarının hotspot özelliğini kullanabilmesi için firewall cihazınıza veya switch'inize bir Access Point bağlamanız gerekmektedir.

AYRICALIK

Bu bölümde IP adresi veya MAC adresi üzerinden tanımladığınız cihazlar için Hotspot giriş ekranı gösterilmez. Bu cihazlar, şifre girişi yapmadan doğrudan internete erişebilir.

ENTEGRASYON

Otel ve benzeri işletmelerde, işletmenin kullandığı yönetim sisteminde (PMS) kayıtlı kullanıcı bilgilerini Hotspot sistemine hızlı ve kolay bir şekilde aktarabilirsiniz. Bu sayede misafirler, kablosuz ağa bağlanırken T.C. kimlik numarası veya pasaport numarası ile oda numarasını girerek internet erişimi sağlayabilir. Sistem; **XML, MSSQL, Sispar, Zeus PMS ve Oracle** ile entegrasyonu destekler.

KULLANICILAR

Bu bölümde, Hotspot sistemine kayıtlı kullanıcıları görüntüleyebilir, mevcut kullanıcıları silebilir veya yeni kullanıcılar ekleyebilirsiniz.

KULLANICI MAC KONTROL

Bu bölümde kullanıcıya bir MAC adresi tanımlandığında, kullanıcı yalnızca belirtilen MAC adresine sahip cihaz üzerinden Hotspot sistemine giriş yapabilir. Diğer cihazlardan giriş yapması engellenir.

ANKETLER

Bu bölümde, kullanıcılara gösterilecek anketleri oluşturabilir ve yönetebilirsiniz. Oluşturduğunuz anketler aracılığıyla kullanıcılardan geri bildirim toplayabilirsiniz.

TOPLU İŞLEMLER

İşlemler

Bu bölümde, kullanıcı kayıtları üzerinde toplu silme işlemi gerçekleştirebilir; kayıtların başlangıç ve bitiş tarihlerini toplu olarak temizleyebilir veya güncelleyebilirsiniz.

CSV Import

Kullanıcı bilgilerini CSV dosyası aracılığıyla sisteme toplu olarak aktarabilirsiniz.

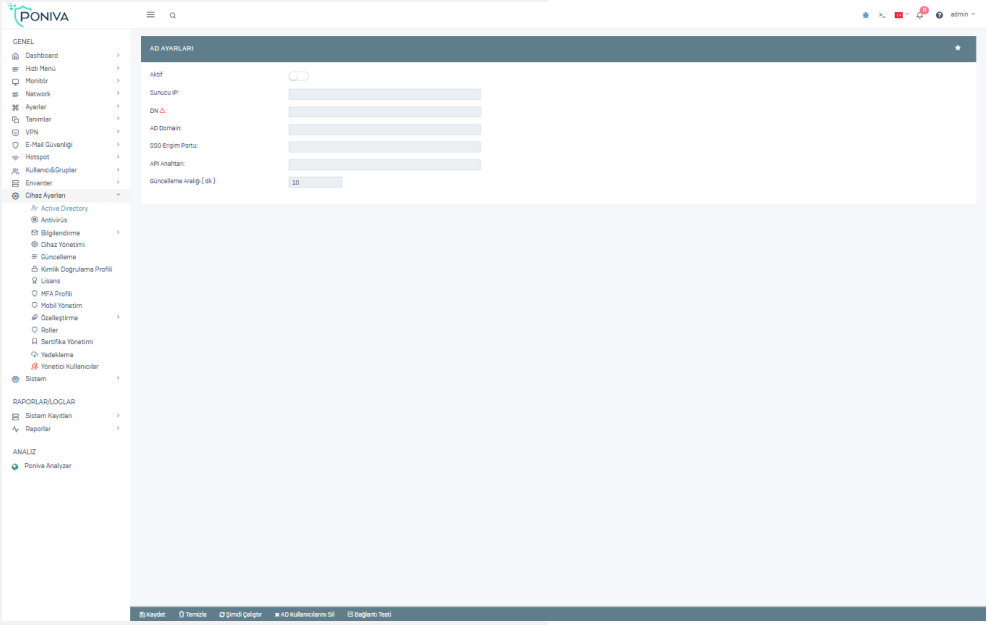
ENVANTER

Poniva Client yazılımının yüklü olduğu bilgisayarların donanım bilgilerini, yüklü yazılımlarını ve sürümlerini firewall üzerinden takip edebilirsiniz. Ayrıca, USB engelleme özelliğinin kullanılabilmesi için de Poniva Client yazılımının ilgili bilgisayarlarda yüklü olması gerekmektedir.

CİHAZ AYARLARI

ACTIVE DIRECTORY

Bu bölümden, Active Directory entegrasyonuna ilişkin bağlantı ve senkronizasyon ayarlarını yapılandırabilirsiniz. Entegrasyonun çalışabilmesi için sunucuda **PONIVA SSO uygulamasının** kurulu ve yapılandırılmış olması gerekir.

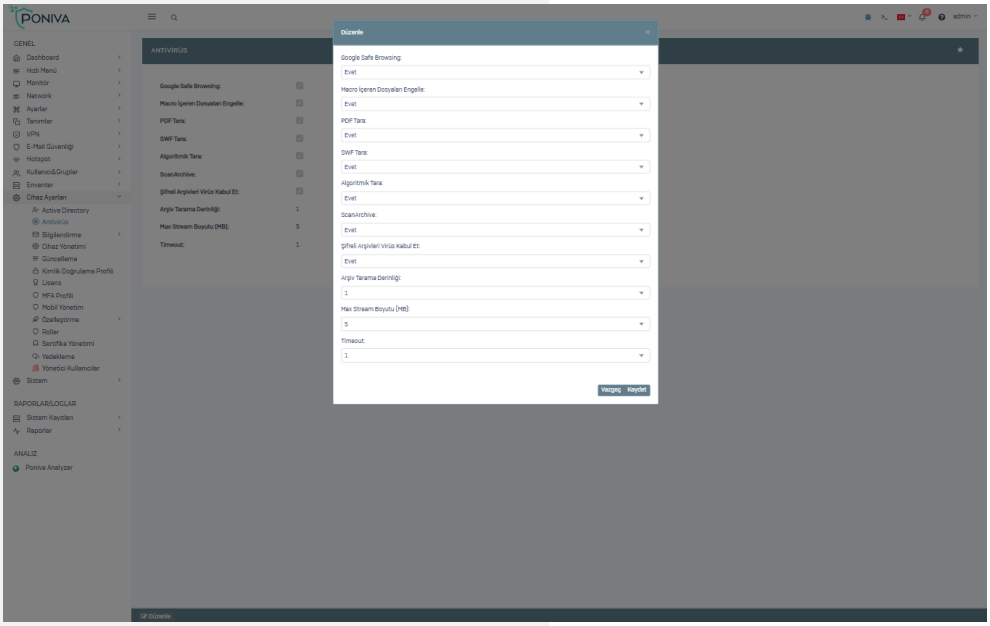


	AÇIKLAMA
Aktif	Active Directory entegrasyonunu aktif veya pasif duruma getirebilirsiniz.
Sunucu IP	Active Directory sunucusunun IP adresini girmelisiniz.
DN	Active Directory bağlantısı için kullanılacak Distinguished Name (DN) bilgisini girmelisiniz.
AD Domain	Active Directory etki alanı adını girmelisiniz.

SSO Erişim Portu	PONIVA SSO uygulamasına erişim için kullanılan port numarasını belirtmelisiniz.
API Anahtarı	PONIVA Firewall ile PONIVA SSO uygulaması arasındaki iletişimin doğrulanması için kullanılan API anahtarını girmelisiniz.
Güncelleme Aralığı (dk)	Active Directory bilgilerinin güncellenmesi için kullanılacak aralığı dakika cinsinden belirlemelisiniz.

ANTİVİRÜS

Bu bölümde yapılandırılan antivirüs ayarları, Grup Yönetimi bölümünde Antivirüs özelliği **aktif** olarak tanımlanmış gruplara uygulanır.



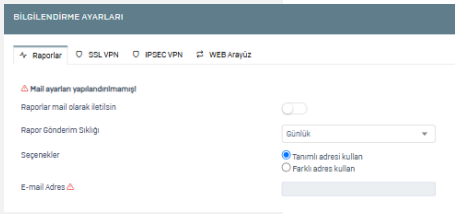
	AÇIKLAMA
Google Safe Browsing	Google Safe Browsing hizmeti aracılığıyla zararlı veya tehlikeli olarak tanımlanan web sitelerine karşı koruma sağlar.
Macro İçeren Dosyaları Engelle	Makro içeren dosyaların ağ üzerinden aktarılmasını engeller.
PDF Tara	PDF dosyalarının zararlı içeriklere karşı taranmasını sağlar.
SWF Tara	SWF dosyalarının zararlı içeriklere karşı taranmasını sağlar.
Algoritmik Tara	Dosyaların bilinen tehditlerin yanı sıra algoritmik analiz yöntemleriyle de incelenmesini sağlar.
ScanArchive	Arşiv dosyalarının içeriğinin zararlı yazılımlara karşı taranmasını sağlar.
Şifreli Arşivleri Virüs Kabul Et	İçeriği taranamayan şifreli arşiv dosyalarının virüslü olarak değerlendirilmesini sağlar.
Arşiv Tarama Derinliği (MB)	Arşiv dosyalarının taranması sırasında incelenecek içerik miktarına ilişkin sınırı megabayt (MB) cinsinden belirler.

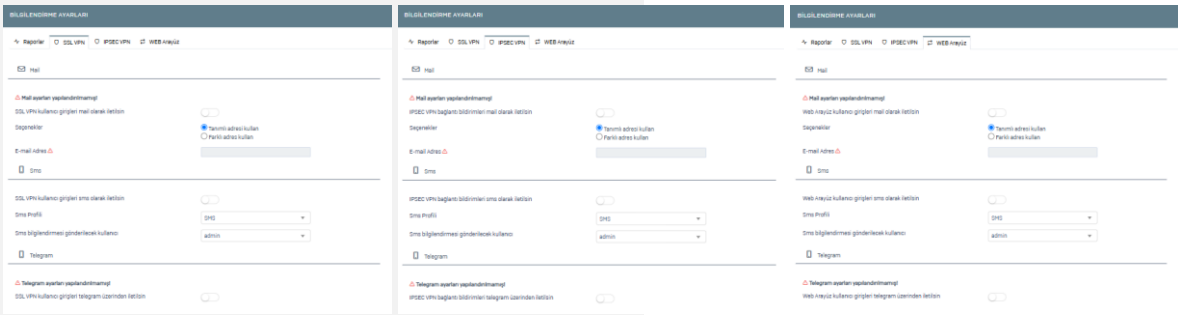
Max. Stream Boyutu (MB)	Tarama işleminde işlenecek maksimum veri akışı boyutunu megabayt (MB) cinsinden belirler.
Timeout	Dosya tarama işlemi için izin verilen maksimum süreyi belirler. Süre aşıldığında tarama işlemi zaman aşımına uğrar.

BİLGİLENDİRME

Bu bölümden, rapor ve sistem olaylarına ilişkin bildirimlerin hangi kanallar üzerinden, hangi alıcılara ve hangi sıklıkta iletileceğini yapılandırabilirsiniz.

Ayarlar





	AÇIKLAMA
Raporlar	Belirlediğiniz gönderim sıklığına göre kullanıcıların ziyaret ettiği web sitelerine ilişkin raporların iletilmesini sağlayabilirsiniz.
SSL VPN	SSL VPN bağlantılarına ilişkin bildirimlerin belirlediğiniz e-posta adresine veya yönetici kullanıcıya e-posta, SMS ya da Telegram üzerinden gönderilmesini sağlayabilirsiniz.
IPSEC VPN	IPsec VPN bağlantılarına ilişkin bildirimlerin belirlediğiniz e-posta adresine veya yönetici kullanıcıya e-posta, SMS ya da Telegram üzerinden gönderilmesini sağlayabilirsiniz.
WEB Arayüz	Yönetim web arayüzüne yapılan girişlere ilişkin bildirimlerin belirlediğiniz e-posta adresine veya yönetici kullanıcıya e-posta, SMS ya da Telegram üzerinden gönderilmesini sağlayabilirsiniz.
Mail Tanımı	Bildirimlerin e-posta yoluyla iletilmesi için kullanılacak e-posta adreslerini tanımlayabilirsiniz.

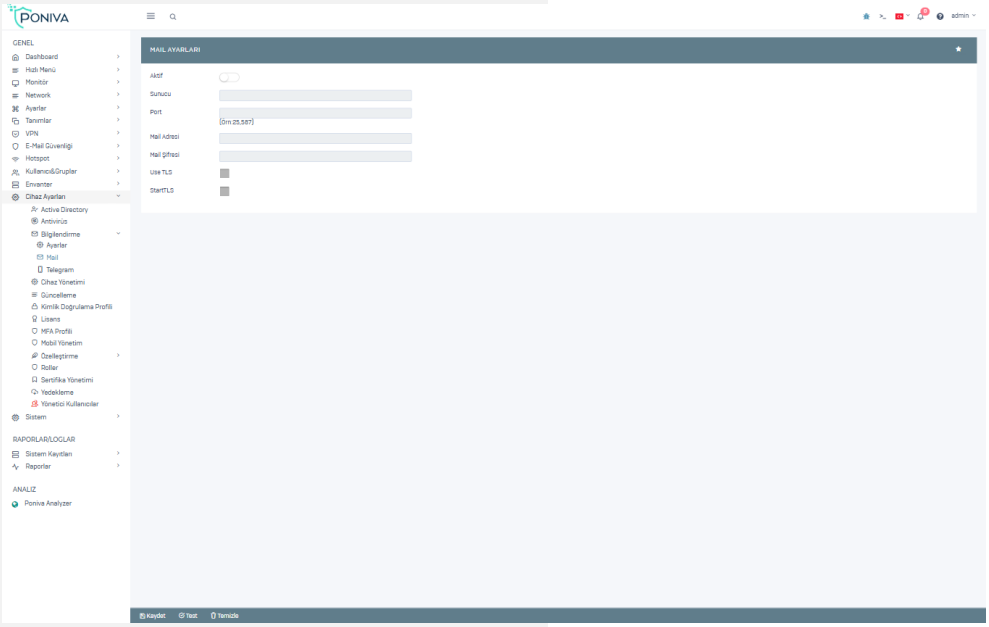
*E-posta bildirimlerinin gönderilebilmesi için mail ayarlarının yapılandırılmış olması gerekir.

*SMS bildirimlerinin gönderilebilmesi için aktif bir SMS profilinin bulunması gerekir.

*Telegram bildirimlerinin gönderilebilmesi için Telegram ayarlarının yapılandırılmış olması gerekir.

Mail

Bu bölümden, gönderilecek e-posta bildirimleri ve raporlar için gerekli SMTP sunucu ayarlarını yapılandırabilirsiniz.



	AÇIKLAMA
Aktif	E-posta gönderim servisini aktif veya pasif duruma getirebilirsiniz.
Sunucu	E-posta gönderiminde kullanılacak SMTP sunucusunun adresini girmelisiniz.
Port	SMTP sunucusuna bağlantı için kullanılacak port numarasını belirtmelisiniz.
Mail Adresi	E-posta gönderiminde kullanılacak hesabın e-posta adresini girmelisiniz.
Mail Şifresi	E-posta hesabının kimlik doğrulaması için gerekli şifreyi girmelisiniz.
Use TLS	E-posta sunucusuyla TLS üzerinden şifreli bağlantı kurulmasını sağlar.
StartTLS	Sunucuyla bağlantı kurulduktan sonra bağlantının STARTTLS komutuyla şifreli hale getirilmesini sağlar.

Telegram

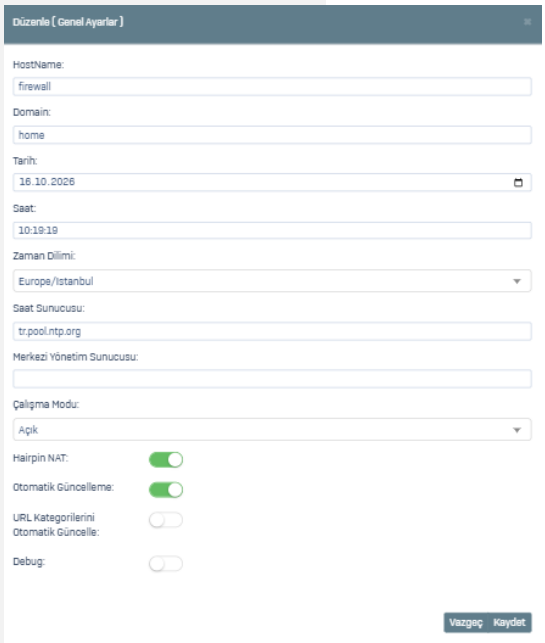
Bu bölümden, gönderilecek telegram bildirimleri için gerekli ayarları yapılandırabilirsiniz. Bildirimlerin iletilebilmesi için Telegram entegrasyonunun kurulmuş ve gerekli yapılandırmaların tamamlanmış olması gerekir.

Kurulum ve yapılandırma adımları hakkında ayrıntılı bilgi almak için Telegram Üzerinden Nasıl Bildirim Gönderilir? başlıklı dokümanı inceleyebilirsiniz.

CİHAZ YÖNETİMİ

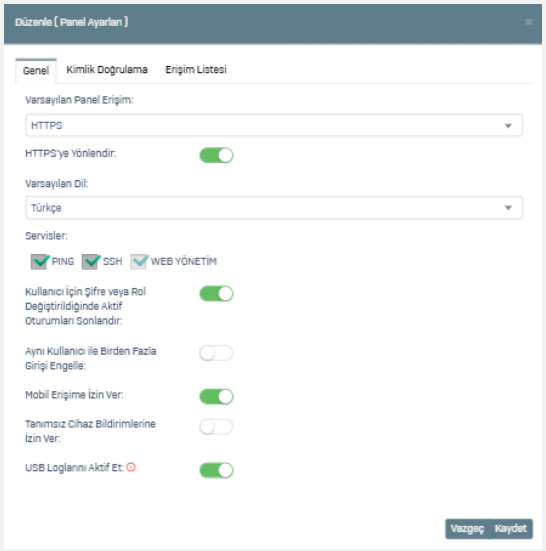
Cihazın genel ayarlarını bu bölümde yapılandırabilirsiniz.

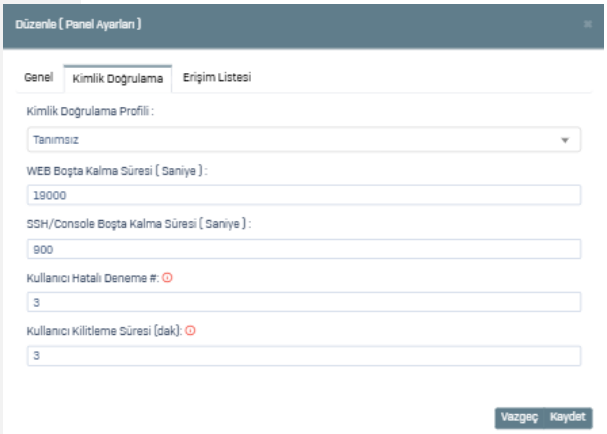
Genel Ayarlar



	AÇIKLAMA
HostName	Firewall cihazının ağ üzerinde tanınmasını sağlayan ana bilgisayar adını belirtir. Varsayılan firewall.
Domain	Cihazın bağlı olduğu veya kullanacağı etki alanını belirtir. Örneğin, firmam.local
Tarih	Firewall cihazının sistem tarihini ayarlamanızı sağlar.
Saat	Firewall cihazının sistem saatini ayarlamanızı sağlar.
Zaman Dilimi	Cihazın kullanacağı zaman dilimini belirlemenizi sağlar.
Saat Sunucusu	Sistem tarih ve saatinin senkronize edileceği NTP veya desteklenen saat sunucusunu tanımlamanızı sağlar.
Merkezi Yönetim Sunucusu	Firewall cihazının merkezi yönetim işlemleri için kullanılacak sunucu bilgilerini belirtir.
Çalışma Modu	Firewall cihazının çalışma şeklini belirler. Kullanılabilir modlar, cihazın desteklediği yapılandırmaya göre değişebilir.
Hairpin NAT	Yerel ağdaki cihazların, dış IP adresi üzerinden erişilen ve aynı yerel ağda bulunan bir sunucuya ulaşmasını sağlayan NAT davranışını etkinleştirir veya devre dışı bırakır.
Otomatik Güncelleme	Etkinleştirildiğinde, sistem güncellemelerinin otomatik olarak kontrol edilmesini sağlar.
URL Kategorilerini Otomatik Güncelle	URL kategorilerinin otomatik olarak güncellenmesini sağlar. Böylece web filtreleme kategorilerinin güncel tutulmasına yardımcı olur.

Panel Yönetimi





	AÇIKLAMA
	Genel Sekmesi
Varsayılan Panel Erişim	Yönetim paneline erişimde kullanılacak bağlantı türünü belirler. HTTP veya HTTPS seçeneklerinden biri seçilebilir.
HTTPS'ye Yönlendir	Etkinleştirildiğinde, HTTP üzerinden yapılan yönetim paneli erişimlerinin HTTPS bağlantısına yönlendirilmesini sağlar.
Varsayılan Dil	Yönetim panelinde varsayılan olarak kullanılacak dili belirler.
Servisler	Yönetim için kullanılabilecek servisleri etkinleştirmenizi veya devre dışı bırakmanızı sağlar. PING, SSH ve Web Yönetimi gibi servisler bu bölümden yapılandırılabilir.
Kullanıcı İçin Şifre veya Rol Değiştirildiğinde Aktif Oturumları Sonlandır	Bir kullanıcının şifresi veya rolü değiştirildiğinde, kullanıcıya ait mevcut oturumların sonlandırılmasını sağlar.
Aynı Kullanıcı ile Birden Fazla Girişi Engelle	Etkinleştirildiğinde, aynı kullanıcı hesabıyla eş zamanlı birden fazla oturum açılmasını engeller.
Mobil Erişime İzin Ver	Etkinleştirildiğinde Poniva Manager ile erişime izin verir.
Tanımsız Cihaz Bildirimlerine İzin Ver	Tanımlanmamış cihazlarla ilgili bildirimlere izin verir.
USB Loglarını Aktif Et	USB aygıtlarıyla ilgili olayların kayıt altına alınmasını etkinleştirir. Ek lisans gerekebilir.
	Kimlik Doğrulama Sekmesi
Kimlik Doğrulama Profili	Yönetim erişiminde kullanılacak kimlik doğrulama profilini belirler.
WEB Boşta Kalma Süresi (Saniye)	Yönetim panelinde belirlenen süre boyunca işlem yapılmadığında oturumun zaman aşımına uğramasını ve kullanıcının yeniden giriş ekranına yönlendirilmesini sağlar.

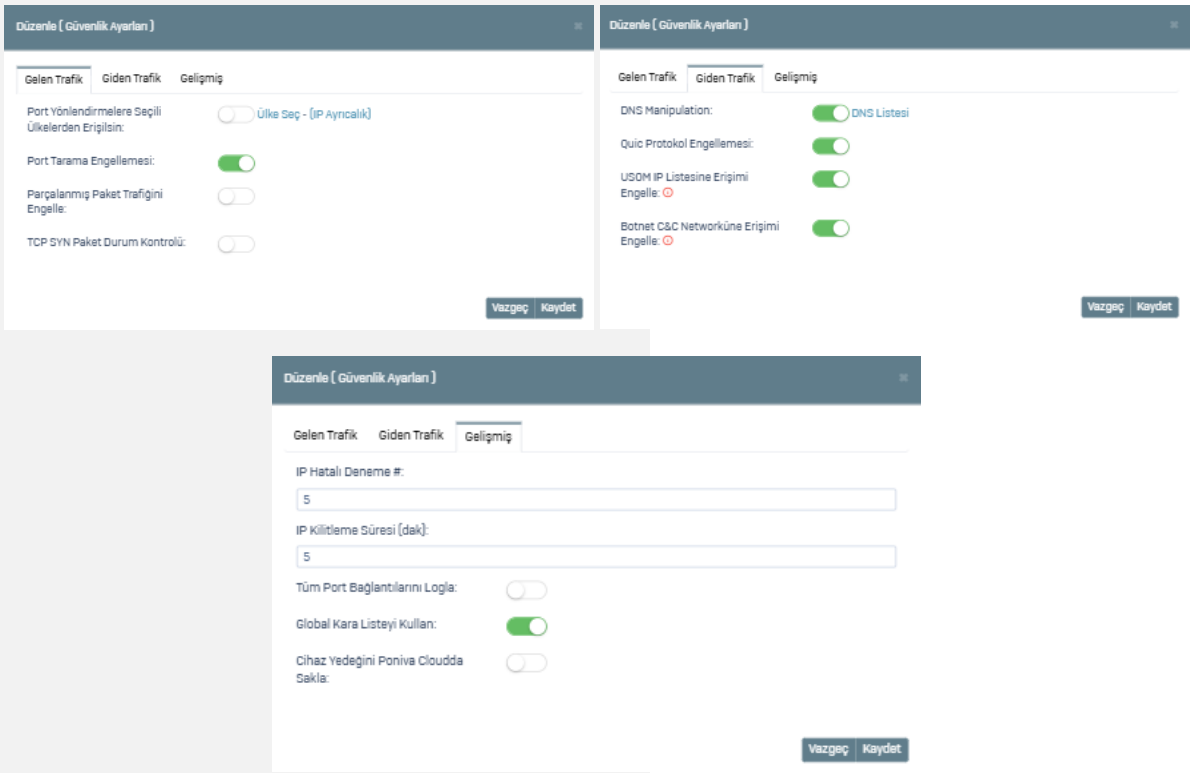
SSH/Console Boşta Kalmas Süresi (Saniye)	SSH veya konsol oturumlarında işlem yapılmadan geçirilebilecek azami süreyi belirler. Süre dolduğunda oturumun sonlandırılması veya zaman aşımına uğraması sağlanabilir.
Kullanıcı Hatalı Deneme	Kullanıcı hesabının kilitlenmesine neden olacak hatalı kimlik doğrulama denemesi sayısını belirler.
Kullanıcı Kilitleme Süresi (dak)	Hatalı giriş denemeleri nedeniyle kilitlenen kullanıcı hesabının ne kadar süreyle kilitli kalacağını belirler.
Erişim Listesi Sekmesi	
Web Arayüzüne Erişimi Sınırlandır	Yönetim paneline erişimi belirli IP adresleri veya ağlarla sınırlandırmanızı sağlar. Bu özellik kullanıldığında, erişim izni verilecek adreslerin doğru tanımlanması önemlidir.

Şifre Politikası



	AÇIKLAMA
Min. Uzunluk	Şifrelerin sahip olması gereken minimum karakter sayısını belirler.
Min. Büyük Harf	Şifrede bulunması gereken minimum büyük harf sayısını belirler.
Min. Küçük Harf	Şifrede bulunması gereken minimum küçük harf sayısını belirler.
Min. Rakam	Şifrede bulunması gereken minimum rakam sayısını belirler.
Min. Özel Karakter	Şifrede bulunması gereken minimum özel karakter sayısını belirler.
Şifre Hatırlatma	Kullanıcılara şifrelerini değiştirmeleri gerektiğini hatırlatmak için kullanılacak hatırlatma periyodunu belirler.
Şifre Değiştirme Periyodu	Kullanıcıların şifrelerini hangi aralıklarla değiştirmeleri gerektiğini belirler.

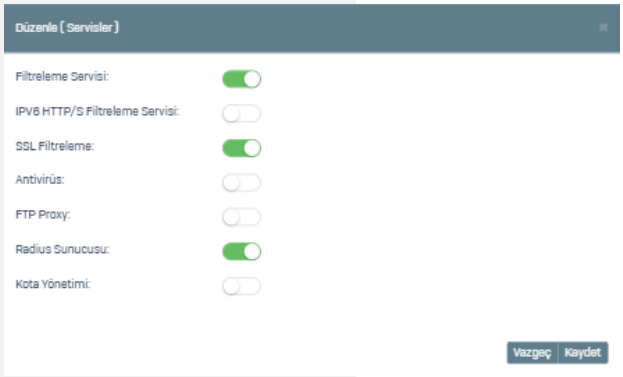
Güvenlik Ayarları



	AÇIKLAMA
Gelen Trafik Sekmesi	
Port Yönlendirmelere Sadece Seçili Ülkelerden Erişilsin	Port yönlendirme kuralları üzerinden sunuculara erişebilecek ülkeleri sınırlandırmanızı sağlar. Varsayılan olarak Türkiye seçilidir.
Port Tarama Engellemesi	Ağ üzerindeki açık portları tespit etmek amacıyla yapılan port tarama girişimlerinin engellenmesini sağlar.
Parçalanmış Paket Trafiğini Engelle	Parçalanmış IP paketlerinden oluşan trafiğin engellenmesini sağlar.
TCP SYN Paket Durum Kontrolü	TCP bağlantılarının başlangıç aşamasındaki SYN paketlerini denetleyerek şüpheli veya kurallara uymayan bağlantı girişimlerinin tespit edilmesine yardımcı olur.
Giden Trafik Sekmesi	
DNS Manipulation	DNS sorgularına yönelik manipülasyon veya değiştirme girişimlerine karşı koruma sağlayan güvenlik denetimini etkinleştirir.
Quic Protokol Engellemesi	QUIC protokolü üzerinden gerçekleştirilen bağlantıların engellenmesini sağlar.
USOM IP Listesine Erişimi Engelle	USOM tarafından yayımlanan IP adresleri listesine yönelik erişimlerin kontrol edilmesini sağlar.
Botnet C&C Networküne Erişimi Engelle	Botnet komuta-kontrol (C&C) altyapılarıyla iletişim kurulmasını engellemeye yönelik güvenlik denetimini etkinleştirir.
Gelişmiş Sekmesi	

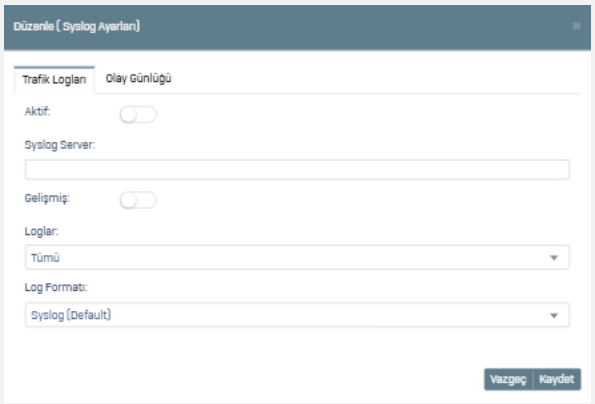
IP Hatalı Deneme	Bir IP adresinden gelen başarısız veya şüpheli denemelerin kaç kez gerçekleşmesinden sonra IP adresinin kilitleneceğini belirler.
IP Kilitleme Süresi (dak)	Belirlenen deneme sınırı aşıldığında IP adresinin ne kadar süreyle kilitli kalacağını belirler.
Tüm Port Bağlantılarını Logla	Port bağlantılarına ilişkin kayıtların tutulmasını sağlar.
Global Kara Listeyi Kullan	Sistem genelinde kullanılan kara listeyi etkinleştirerek listedeki IP adresleri veya diğer tanımlayıcılar için ilgili güvenlik kurallarının uygulanmasını sağlar.
Cihaz Yedeğini Poniva Cloudda Sakla	Firewall cihazına ait yedeklerin PONIVA Cloud üzerinde saklanmasını sağlar.

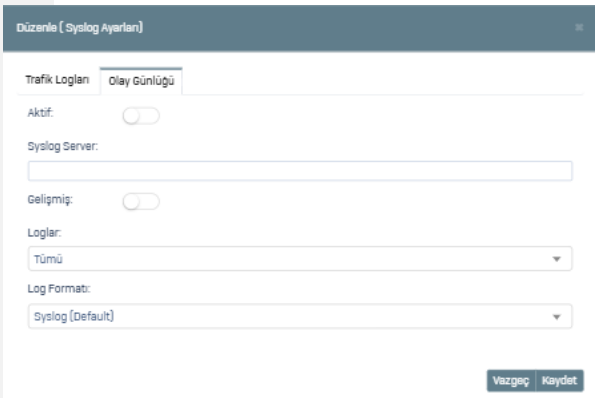
Servisler



	AÇIKLAMA
Filtreleme Servisi	Etkinleştirildiğinde, Grup Yönetimi bölümünde tanımlanan filtreleme politikalarının uygulanmasını sağlar. Devre dışı bırakıldığında filtreleme ve loglama uygulanmaz.
IPV6 HTTP/S Filtreleme Servisi	IPv6 üzerinden gerçekleşen HTTP ve HTTPS trafiğinin filtrelenmesini sağlar.
SSL Filtreleme	SSL/TLS trafiğinin yapılandırılan filtreleme politikalarına göre denetlenmesini sağlar.
Antivirüs	Etkinleştirildiğinde, Grup Yönetimi bölümünde seçilen antivirüs politikalarının uygulanmasını sağlar. Devre dışı bırakıldığında, grup bazında antivirüs seçilmiş olsa bile antivirüs denetimi gerçekleştirilemez.
FTP Proxy	FTP trafiğinin proxy servisi üzerinden iletilmesini ve yapılandırmaya bağlı olarak denetlenmesini sağlar.
Radius Suncusu	RADIUS protokolü üzerinden merkezi kimlik doğrulama ve erişim yönetimi hizmeti sunar.
Kota Yönetimi	Etkinleştirildiğinde, Grup Yönetimi bölümünde tanımlanan internet kullanım kotası politikalarının uygulanmasını sağlar. Devre dışı bırakıldığında, grup bazında kota tanımlanmış olsa bile kota yönetimi işlemleri uygulanmaz.

Syslog Ayarları

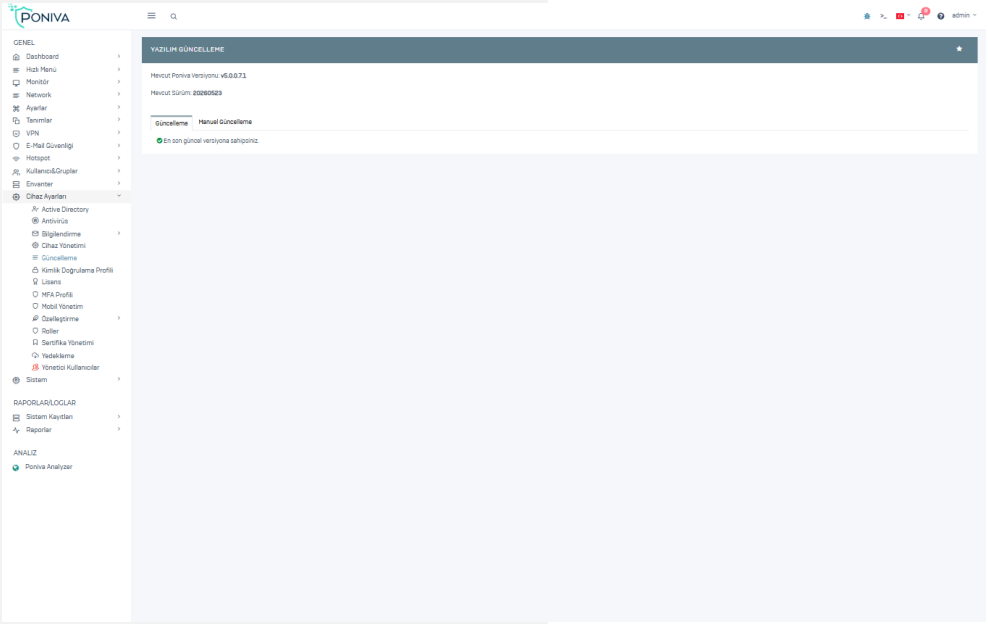




	AÇIKLAMA
	Trafik Logları Sekmesi
Aktif	Trafik loglarının Syslog sunucusuna gönderilmesini etkinleştirir veya devre dışı bırakır.
Syslog Server	Trafik loglarının gönderileceği Syslog sunucusunu belirtir.
Gelişmiş	Trafik loglarının gönderimine ilişkin ek yapılandırma seçeneklerini içerir.
Loglar	Syslog sunucusuna aktarılacak trafik kayıtlarını belirlemenizi sağlar.
Log Formatı	Trafik loglarının Syslog sunucusuna hangi formatta gönderileceğini belirler.
	Olay Günlüğü Sekmesi
Aktif	Sistem olay günlüklerinin Syslog sunucusuna gönderilmesini etkinleştirir veya devre dışı bırakır.
Syslog Server	Olay günlüklerinin gönderileceği Syslog sunucusunu belirtir.
Gelişmiş	Olay günlüklerinin gönderimine ilişkin ek yapılandırma seçeneklerini içerir.
Loglar	Syslog sunucusuna aktarılacak olay günlüklerini belirlemenizi sağlar.
Log Formatı	Olay günlüklerinin Syslog sunucusuna hangi formatta gönderileceğini belirler.

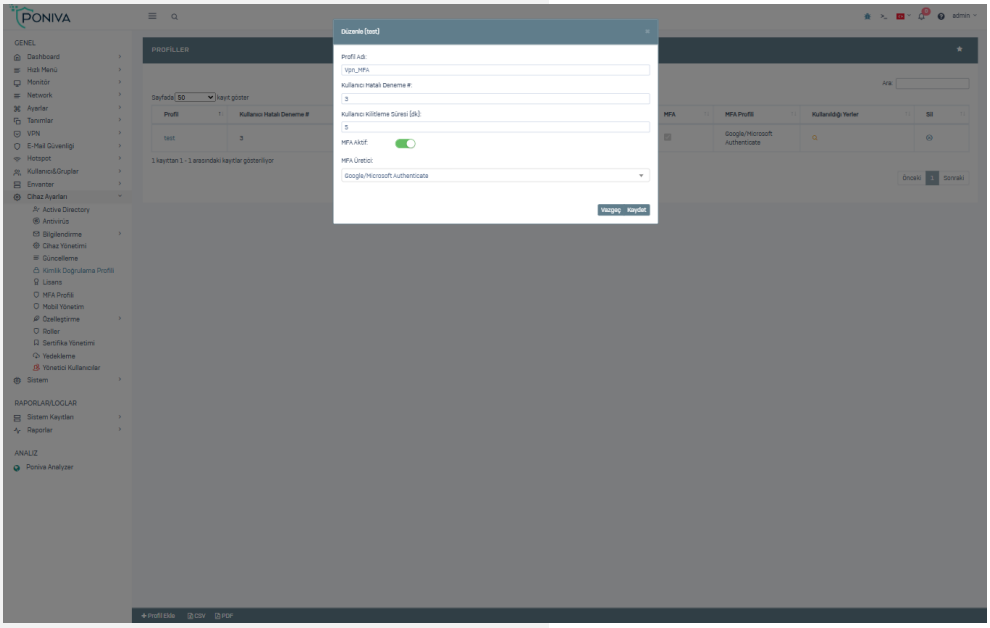
GÜNCELLEME

Bu bölümden, cihazınızın mevcut yazılım sürümünü ve güncelleme durumunu kontrol edebilirsiniz. Mevcut güncellemeleri görüntüleyerek cihazınızın yazılımını güncel tutabilir ve sunulan yeni sürümlere ilişkin bilgileri takip edebilirsiniz.



KİMLİK DOĞRULAMA PROFİLİ

Bu bölümden, kullanıcılarınız için kimlik doğrulama profili oluşturabilir ve güvenlik ayarlarını yapılandırabilirsiniz.



	AÇIKLAMA
Profil Adı	Kimlik doğrulama profilini tanımlamak için bir ad girmelisiniz.
IP Hatalı Deneme	Bir IP adresinden izin verilen hatalı kimlik doğrulama denemesi sayısını belirleyebilirsiniz.
IP Kilitleme Süresi (dk)	Belirlenen hatalı deneme sayısına ulaşıldığında IP adresinin ne kadar süreyle kilitleneceğini dakika cinsinden belirleyebilirsiniz.

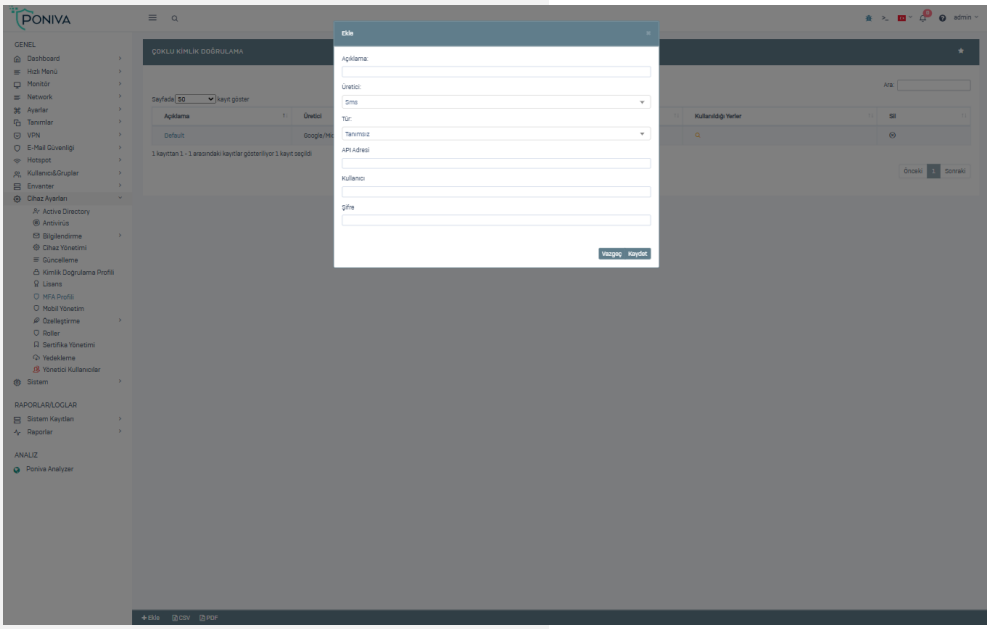
MFA Aktif	Çok faktörlü kimlik doğrulama (MFA) özelliğini aktif veya pasif duruma getirebilirsiniz.
MFA Üretici	Çok faktörlü kimlik doğrulama için kullanılacak yöntemi veya üreticiyi seçebilirsiniz. Bu kısımdaki tanımlamalar MFA Profili menüsünden yönetilmektedir.

LİSANS

Bu bölümden, cihazınıza ait lisans bilgilerini görüntüleyebilirsiniz. Lisans kapsamında tanımlanan kullanıcı sayısı ve diğer lisans detaylarını inceleyebilirsiniz. Lisans süreniz bittiğinde Loglama, Filtreleme, Uygulama Kontrol, Hotspot, Turkuaz VPN özellikleri devredışı kalır.

MFA PROFİLİ

Bu bölümden, farklı doğrulama yöntemleri ve SMS sağlayıcıları için birden fazla çok faktörlü kimlik doğrulama (MFA) profili oluşturabilirsiniz. Oluşturduğunuz profilleri, **Kimlik Doğrulama Profili** bölümünde ilgili kullanıcıların doğrulama süreçlerinde kullanabilirsiniz.



	AÇIKLAMA
Üretici	Çok faktörlü kimlik doğrulama kodlarının gönderileceği yöntemi seçebilirsiniz. E-posta veya SMS seçenekleri kullanılabilir.
Tür	SMS üreticisi olarak kullanılacak servis sağlayıcısını seçebilirsiniz. Desteklenen sağlayıcılar Verimor, Teknomart, Posta Güvercini, Netgsm, JetSMS ve Telsam'dır.
Kullanıcı	SMS sağlayıcısına ait API kullanıcı adını girmelisiniz.
Şifre	SMS sağlayıcısına ait API şifresini girmelisiniz.

Başlık	Gönderilecek SMS mesajlarında kullanılacak gönderici başlığını belirtmelisiniz.

MOBİL YÖNETİM

Bu bölümden, admin dışındaki kullanıcıların Poniva Manager uygulamasında erişebileceği menüleri ve yetkilerini yapılandırabilirsiniz.



ÖZELLEŞTİRME

Engelleme Sayfası

Bir web sitesi engellendiğinde, kullanıcılara varsayılan olarak PONIVA Firewall engelleme mesajı gösterilir. Bu bölümden varsayılan mesajı özelleştirerek kendi bilgilendirme metninizi oluşturabilirsiniz. Mesaj içeriğini HTML formatında da düzenleyebilirsiniz.

Bilgilendirme/Uyarı Sayfası

Kullanıcılara belirli konularda bilgilendirme mesajları göstermek için bu bölümü kullanabilirsiniz. Örneğin, internet erişim kayıtlarının 5651 sayılı Kanun kapsamında tutulduğuna ilişkin bir bilgilendirme mesajı hazırlayabilirsiniz. Sayfa içeriğini HTML formatında özelleştirebilirsiniz.

Sayfa Özelleştirme

Engelleme Sayfası: Engellenen web sitelerine erişim sırasında görüntülenen sayfadaki varsayılan PONIVA logosu yerine kurumunuza veya firmanıza ait logoyu ekleyebilirsiniz.

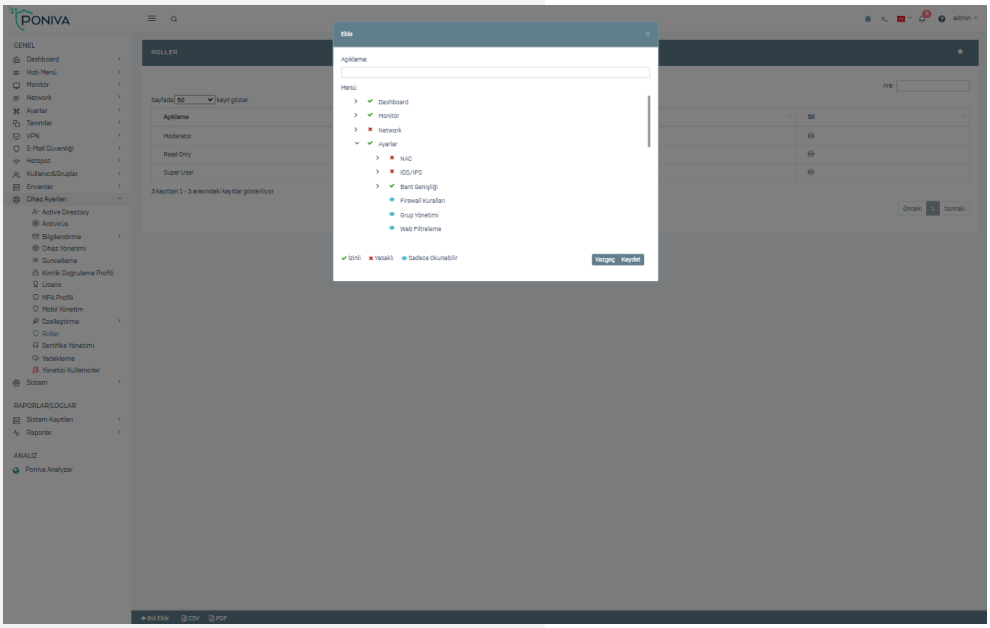
Bilgilendirme/Uyarı Sayfası: Uyarı sayfası giriş ekranında görüntülenen varsayılan PONIVA logosu yerine kurumunuza veya firmanıza ait logoyu ekleyebilirsiniz.

Hotspot Sayfası: Hotspot kullanıcı giriş ekranında görüntülenen varsayılan PONIVA logosu yerine kurumunuza veya firmanıza ait logoyu ekleyebilirsiniz.

*Logo boyutlarının kare formatında olduğundan emin olunuz. İdeal logo boyutu 400x400 piksel olmalıdır.

ROLLER

Bu bölümden, oluşturduğunuz kullanıcılar için roller tanımlayabilir ve yönetim arayüzünde erişebilecekleri menüleri ve işlem yetkilerini belirleyebilirsiniz. Oluşturduğunuz rolleri **Yönetici Kullanıcılar** bölümünde ilgili kullanıcılara atayabilirsiniz.



	AÇIKLAMA
Açıklama	Rol tanımını açıklamak için bir metin girebilirsiniz.
Menü	Kullanıcıların yönetim arayüzündeki menülere erişim ve işlem yetkilerini belirleyebilirsiniz. **İzinli:** Kullanıcı ilgili menüyü görüntüleyebilir ve değişiklik yapabilir. **Yasaklı:** Kullanıcı ilgili menüye erişemez. **Sadece Okuyabilir:** Kullanıcı ilgili menüyü görüntüleyebilir ancak herhangi bir değişiklik yapamaz.

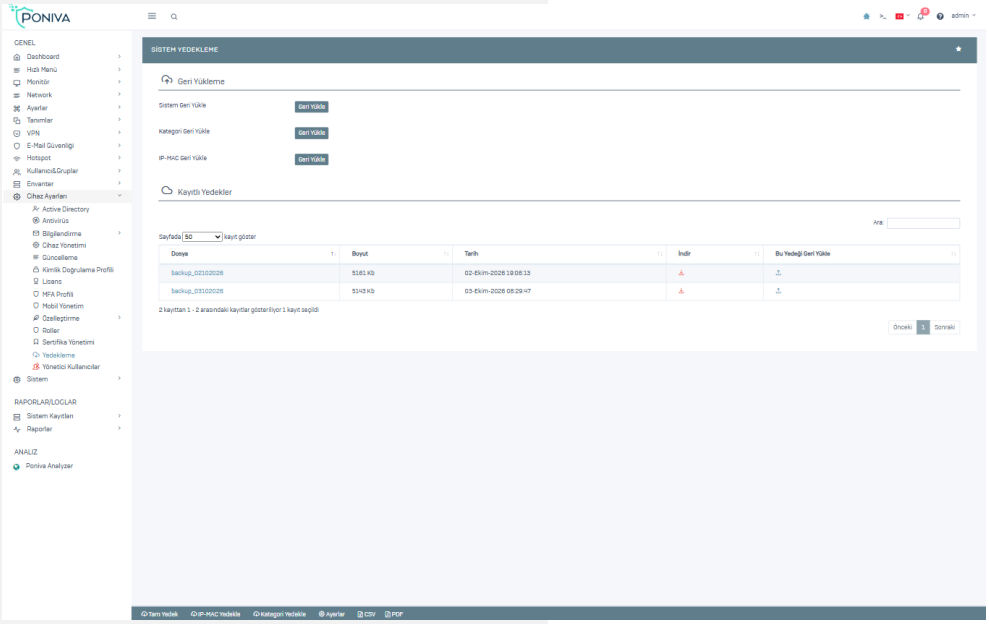
SERTİFİKA YÖNETİMİ

Bu bölümden, cihaz üzerinde kullanılan sertifikaları yeniden oluşturabilirsiniz. Sertifikaların yenilenmesi veya yeniden oluşturulması gereken durumlarda bu bölümü kullanabilirsiniz.



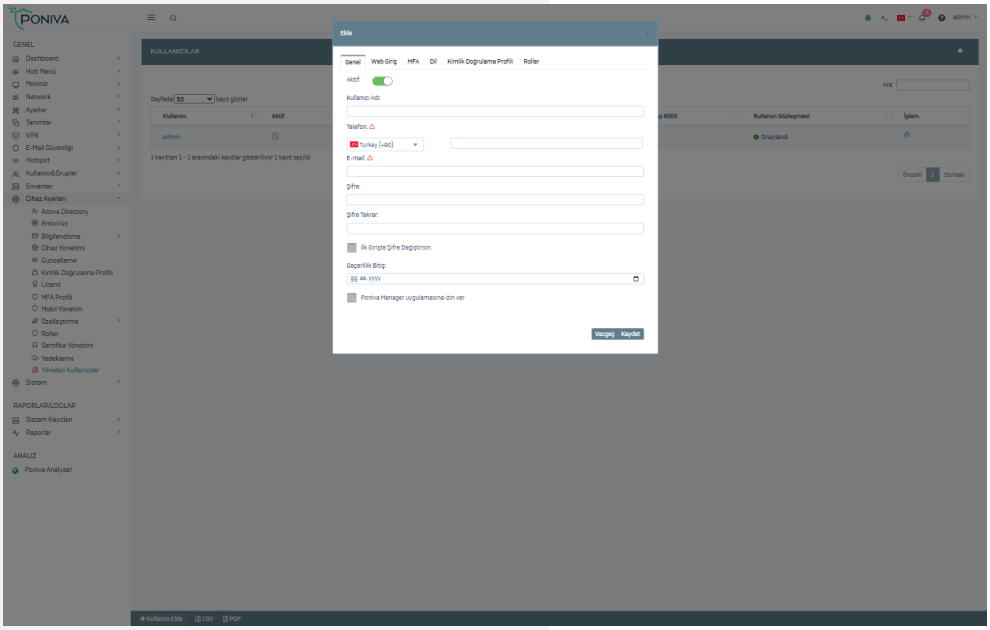
YEDEKLEME

Bu bölümden, PONIVA Firewall cihazınızın konfigürasyon yedeğini alabilir ve ihtiyaç duyduğunuzda daha önce oluşturduğunuz yedekleri cihaza geri yükleyebilirsiniz. Yedekleme ve geri yükleme işlemlerinde **FTP, WEB ve Loglama** modüllerine ait ayarlar yedek kapsamına dahil değildir.



YÖNETİCİ KULLANICILAR

PONIVA Firewall üzerinde varsayılan yönetici kullanıcı adı **admin**'dir. Bunun yanı sıra, yönetim arayüzüne erişim sağlayacak yeni kullanıcılar oluşturabilir ve bu kullanıcılara uygun roller ve yetkiler atayabilirsiniz.



	AÇIKLAMA

Aktif	Kullanıcının aktif veya pasif durumunu belirleyebilirsiniz.
Kullanıcı Adı	Yönetim arayüzüne girişte kullanılacak kullanıcı adını girmelisiniz.
Telefon	Kullanıcının telefon numarasını girebilirsiniz. Kimlik doğrulama profilinde SMS doğrulaması kullanılacaksa bu alanın doldurulması gerekir.
E-mail	Kullanıcının e-posta adresini girebilirsiniz. Kimlik doğrulama profilinde e-posta doğrulaması kullanılacaksa bu alanın doldurulması gerekir.
Şifre	Kullanıcının yönetim arayüzüne girişte kullanacağı şifreyi belirlemelisiniz.
İlk Girişte Şifre Değiştirilsin	Etkinleştirildiğinde kullanıcı, ilk girişinde şifresini değiştirmek zorundadır.
Geçerlilik Bitiş	Kullanıcı hesabının erişim yetkisinin sona ereceği tarihi belirleyebilirsiniz.
Poniva Manager Uygulamasına İzin Ver	Etkinleştirildiğinde kullanıcının PONIVA Manager mobil uygulamasına erişmesine izin verilir.
Web Giriş	Kullanıcının yönetim arayüzüne erişebileceği IP adreslerini tanımlayabilirsiniz.
MFA	Çok faktörlü kimlik doğrulama özelliğini yapılandırabilirsiniz. Kullanılabilmesi için ilgili kimlik doğrulama profilinde MFA'nın etkin olması gerekir.
Dil	Kullanıcının yönetim arayüzünde kullanacağı dili Türkçe veya İngilizce olarak seçebilirsiniz.
Kimlik Doğrulama Profili	Kullanıcı için uygulanacak kimlik doğrulama profilini seçebilirsiniz.
Roller	Kullanıcıya atanacak rolleri belirleyerek yönetim arayüzündeki menü ve işlem yetkilerini yapılandırabilirsiniz.

SİSTEM

YENİDEN BAŞLAT

Bu menüden PONIVA Firewall cihazını yeniden başlatabilirsiniz. Yeniden başlatma işlemi sırasında cihazın ağ ve güvenlik hizmetlerinde geçici kesinti yaşanabilir.

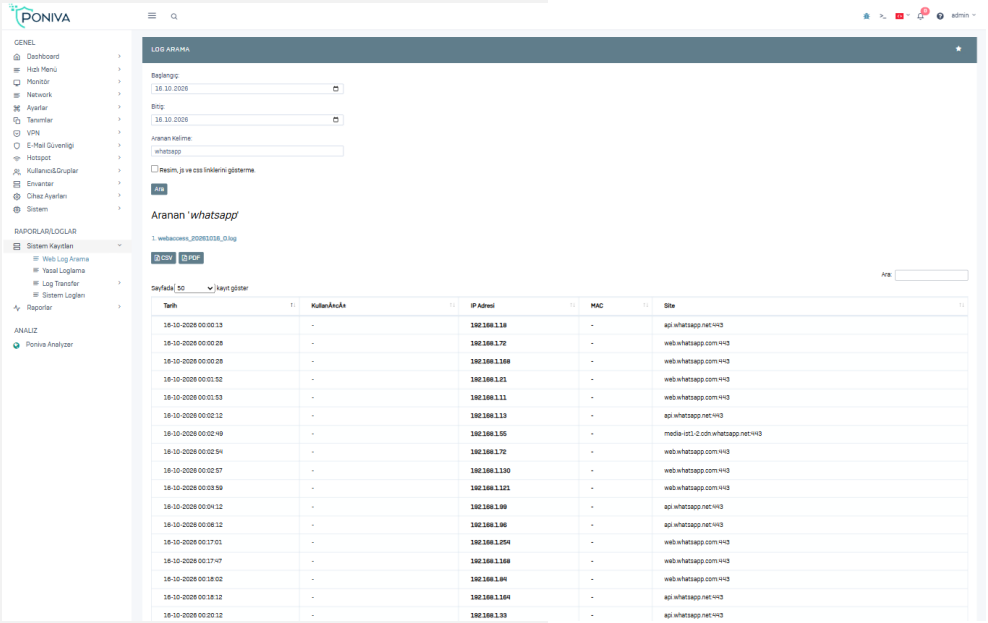
CİHAZI KAPAT

Bu menüden PONIVA Firewall cihazını kapatabilirsiniz. Kapatma işlemi sonrasında cihaz, manuel olarak veya desteklenen başka bir yöntemle yeniden başlatılana kadar hizmet vermez.

SİSTEM KAYITLARI

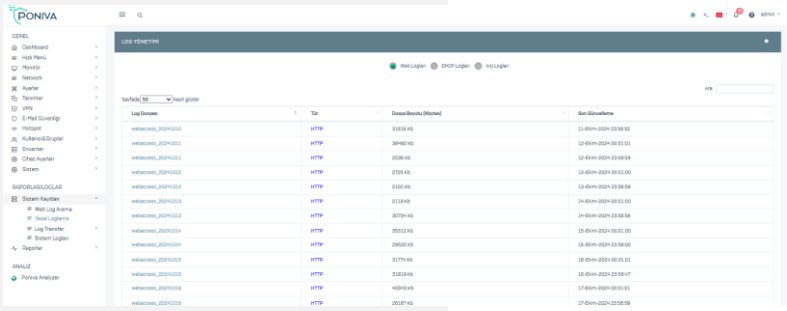
WEB LOG ARAMA

Belirlediğiniz tarih aralığında, aradığınız kelimeye göre filtreleme yaparak ilgili log kayıtlarını görüntüleyebilirsiniz.



YASAL LOGLAMA

5651 sayılı Kanun kapsamında tutulan log kayıtlarına bu menüden erişebilir, ihtiyaç duyduğunuzda kayıtları bilgisayarınıza indirerek inceleyebilirsiniz.





LOG TRANSFER

Windows Transfer

Log kayıtlarınızı, belirlediğiniz saatte Windows Transfer aracılığıyla ağınızdaki bir bilgisayarda bulunan paylaşımlı klasöre günlük olarak otomatik şekilde aktarabilirsiniz.

Windows Transfer kurulumu ve log aktarımının nasıl yapılandırılacağı hakkında detaylı bilgiye Windows Transfer ile Log Aktarımı dokümanından ulaşabilirsiniz.

	AÇIKLAMA
Aktif	Otomatik log aktarımını etkinleştirir veya devre dışı bırakır.
Loglama Saati	Log kayıtlarının her gün aktarılacağı saati belirler.
PC IP Adresi	Paylaşımlı klasörün bulunduğu bilgisayarın IP adresini belirtir.
Kullanıcı Adı	Paylaşımlı klasöre erişmek için kullanılacak kullanıcı adını belirtir.
Şifre	İlgili kullanıcı hesabının şifresini belirtir.
Domain/Workgroup	Hedef bilgisayarın bağlı olduğu etki alanını (Domain) veya çalışma grubunu (Workgroup) belirtir.
Paylaşım Adı	Log kayıtlarının aktarılacağı paylaşımlı klasörün adını belirtir.
Koyulacak Dizin	Log kayıtlarının paylaşım klasörü içerisinde kaydedileceği alt dizini belirtir.

FTP Transfer

Log kayıtlarınızı, belirlediğiniz saatte FTP sunucunuza günlük olarak otomatik şekilde aktarabilirsiniz.

FTP Transfer yapılandırması ve log aktarımının nasıl yapılacağı hakkında detaylı bilgiye FTP Transfer ile Log Aktarımı dokümanından ulaşabilirsiniz.

	AÇIKLAMA
Aktif	Otomatik log aktarımını etkinleştirir veya devre dışı bırakır.
Loglama Saati	Log kayıtlarının her gün aktarılacağı saati belirler.
FTP Server	Log kayıtlarının aktarılacağı FTP sunucusunun adresini belirtir.
FTP Kullanıcı Adı	FTP sunucusuna bağlanmak için kullanılacak kullanıcı adını belirtir.
FTP Şifre	FTP sunucusuna bağlanmak için kullanılacak şifreyi belirtir.
FTP Dizin	Log kayıtlarının FTP sunucusunda kaydedileceği dizini belirtir.

USB Transfer

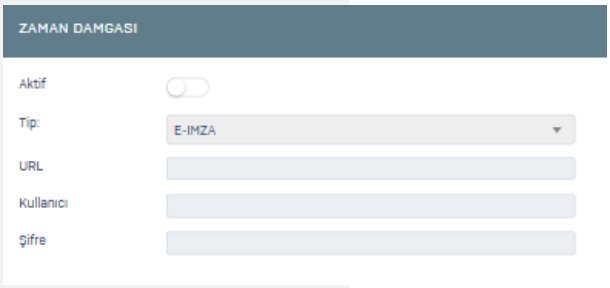
Log kayıtlarınızı, belirlediğiniz saatte USB diske günlük olarak otomatik şekilde aktarabilirsiniz. Aktarım için USB diskin cihazınıza bağlı olması gerekir.

USB Transfer yapılandırması ve log aktarımının nasıl yapılacağı hakkında detaylı bilgiye USB Transfer ile Log Aktarımı dokümanından ulaşabilirsiniz.

	AÇIKLAMA
Aktif	Otomatik log aktarımını etkinleştirir veya devre dışı bırakır.
Loglama Saati	Log kayıtlarının her gün aktarılacağı saati belirler.
USB	Log kayıtlarının aktarılacağı USB diski seçmenizi sağlar.

Zaman Damgası Sunucusu

5651 sayılı Kanun kapsamında tutulan log kayıtlarının bütünlüğünü doğrulamak amacıyla zaman damgası hizmeti kullanabilirsiniz. **TÜBİTAK**, **E-İmza** ve **TURKTRUST** gibi zaman damgası hizmet sağlayıcılarını kullanmak için bu servisi etkinleştirmeniz ve ilgili bağlantı ile erişim bilgilerini tanımlamanız gerekir.



SİSTEM LOGLARI

	AÇIKLAMA
Saldırı Tespit	Sisteminize yönelik saldırı girişimleri ve engellenen trafikle ilgili kayıtları görüntüleyebilirsiniz.
Bağlantılar	Ağınızdan gerçekleştirilen bağlantılara ilişkin kayıtları görüntüleyebilirsiniz.
Servis Logları	Firewall üzerindeki servislerin çalışması ve durumlarıyla ilgili kayıtları görüntüleyebilirsiniz.
Web Engelleme	Engellenen web sitelerini ve engelleme nedenlerini içeren kayıtları görüntüleyebilirsiniz.
Önemli Olaylar	Lisans durumu ve saldırı kayıtları gibi önemli sistem olaylarını görüntüleyebilirsiniz.
Arp Logları	IP-MAC adres eşleştirmeleri ve IP adresi çakışmalarıyla ilgili kayıtları görüntüleyebilirsiniz.
Network Durumu	Ağ bağlantılarının ve fiziksel ağ arayüzlerinin durumuyla ilgili kayıtları görüntüleyebilirsiniz.
SSL VPN Logları	SSL VPN bağlantılarına ilişkin kayıtları görüntüleyebilirsiniz.

Trojan Logları	Ağınızda P2P veya tünel bağlantısı kullanan kullanıcılarla ilgili kayıtları görüntüleyebilirsiniz.
Hotspot Logları	Hotspot kullanıcılarının giriş ve çıkış işlemlerine ilişkin kayıtları görüntüleyebilirsiniz.
Sistem Giriş Logları	Cihaza yapılan başarılı ve başarısız kullanıcı girişlerini görüntüleyebilirsiniz.
USB Logları	PONIVA Monitor servisi aracılığıyla kullanıcıların hangi cihazlara USB bellek taktığını ve hangi dosyaları eklediğini görüntüleyebilirsiniz. (Ek lisans gerektirebilir)
Audit Logları	Firewall üzerinde gerçekleştirilen ekleme, silme ve güncelleme işlemlerinin ayrıntılı kayıtlarını görüntüleyebilirsiniz.

RAPORLAR

Bu menüden istediğiniz rapor türünü seçerek belirlediğiniz tarih aralığı için rapor oluşturabilirsiniz. Raporları tüm kullanıcılar için veya belirli bir IP adresine göre filtreleyerek görüntüleyebilirsiniz.