

epati

Anlık Log Monitörü

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

Anlık Log Monitörü

Arayüzde canlı olarak logları görüntüleyebileceğimiz menüdür.

Anlık Log Monitörü

AV, AppID, IPS, DoS Logları	Antispam Logları	Arayüze Erişimi Yasaklanan İPler
DHCP Olay Logları	DNS Filtreleme Logları	Http(s) Sunucu Yönlendirme Logları
PPP Debug Logları	PPP Logları	Paket Filtreleme Logları
RADIUS Logları	SSH Denetimi Logları	SSH Koruma Servisi Logları
Sanal Kablo Logları	VPN - SSL VPN Logları	Web Erişim Logları
Web Filtreleme - Sayfa Yasaklama Logları	Web Filtreleme - İçerik ve Antivirüs Tarama Logları	Web Uygulama Güvenliği Logları

Anlık Log Monitöründe, **Yönetim Paneli Trafik Erişim Logları** arayüzde görüntülenmek isteniyorsa;

Erişim / Oturum Ayarları sayfası açılır **Trafiği Logla** aktif edilir ve **Sistem Ayarları** sayfasında ilgili kayıt için cihazda tut ayarı seçilir, tanımlar uygulanır.

Erişim/Oturum Ayarları

Oturum Ayarları

Trafiği Logla Açık

Sertifika Bazlı Kimlik Doğrulama Kapalı

Harici Kaynaklardan Kimlik Doğrulama Kapalı

Eş Zamanlı Oturum Açma Açık

Çalışma Modu

Giriş Feragatnamesi Kapalı

SSH Karşılama Ekran Durumu Kapalı

Erişebilen Ağlar

#	IP Adresi	Açıklama	İşlemler
1	0.0.0.0/0	Arayüz Erişim	<input type="button" value="Düzenle"/> <input type="button" value="Sil"/>

Log Ayarları

Güvenlik Duvarı - Hotspot Varsayılan Engel Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Balküüpü Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Karadelik Servisi Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
VPN - SSL VPN Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Web Erişim Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Web Arayüzü Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Uygulama Güvenliği Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Http(s) Sunucu Yönlendirme Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
VPN - PPTP / L2TP Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
RADIUS Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
VPN - IPsec VPN Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Güvenlik Kuralları Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - DMZ Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Global NAT Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Port Yönlendirme Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Statik NAT Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Hedefe Göre NAT Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Dinamik NAT Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Antispoof Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Yönetim Paneli Erişim Trafik Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
DHCP Olay Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Web Oturum Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Hotspot Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Güvenlik Duvarı - Trafik Normalizasyonu	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
SSH ve Konsol Oturum Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma
Cluster Logları	<input checked="" type="checkbox"/> Cihazda Tut	<input type="checkbox"/> Cihazda Tutma

Yönetim Paneli Erişim Log çıktıları resimdeki gibi görüntülenecektir.

Yönetim Paneli Erişim Trafik Logları

Listeye Göz

Parametreler

Filtre (Düzenli İfade)

En üstteki satır en son gelen gibidir. Çıktı geçmişi maksimum 100 satır gösterilir.

```
2020-12-14 11:23:21.803068 pass in em0 TCP 10.2.1.152 6310 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:21.827986 pass in em0 TCP 10.2.1.152 6315 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:24.603885 pass in em0 TCP 10.2.1.152 6305 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:24.972077 pass in em0 TCP 10.2.1.152 6305 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:24.369127 pass in em0 TCP 10.2.1.152 6304 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:20.864078 pass in em0 TCP 10.2.1.152 6299 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.768666 pass in em0 TCP 10.2.1.152 6289 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.763874 pass in em0 TCP 10.2.1.152 6288 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.768674 pass in em0 TCP 10.2.1.152 6287 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.765464 pass in em0 TCP 10.2.1.152 6285 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.755474 pass in em0 TCP 10.2.1.152 6285 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.754593 pass in em0 TCP 10.2.1.152 6284 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.754166 pass in em0 TCP 10.2.1.152 6283 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.752929 pass in em0 TCP 10.2.1.152 6282 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.761978 pass in em0 TCP 10.2.1.152 6281 10.2.4.20 8880 18 kural-paneliris 1 - - -
2020-12-14 11:23:18.187423 pass in em0 TCP 10.2.1.152 6280 10.2.4.20 8880 18 kural-paneliris 1 - - -
...
```

DMZ Trafik Logları, monitörde gözlemlenmek isteniyorsa sırasıyla, **Sistem Ayarları > Log Ayarları > Paket Filtreleme Logları** cihazda tut seçilir.

SSH Denetimi Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Web Filtreleme - Sayfa Yasaklama Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Web Uygulama Güvenliği Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
AV, AppID, IPS, DoS Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
DNS Filtreleme Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
PPP Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
PPP Debug Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Sanal Kablo Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Paket Filtreleme Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma

Daha sonra DMZ Yönetimi > DMZ Sunucu Yönetimi logu tutulması istenilen DMZ Sunucusuna ait Erişimlere tıklanır. Erişimler içerisindeki kurallardan logu tutulacak kural düzenle tıklanarak açılan pencerede Trafik Logu açılmalıdır.

DMZ Sunucu Yönetimi - Kayıt Düzeltme

Durum Aktif

DMZ Türü NAT Yapma, Olduğu Gibi Erişim

Adres Ailesi IPv4 IPv6

DMZ IP Arayüzü [Redacted]

DMZ IP Adresi IPv4 [Redacted]

Loglama Aktif

Erişim Denetimi Bu Ekrandan Yönet

Açıklama [Redacted]

Güvenlik Kuralları logları için sırasıyla, **Sistem Ayarları > Log Ayarları > Paket Filtreleme Logları** cihazda tut seçilir.

SSH Denetimi Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Web Filtreleme - Sayfa Yasaklama Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Web Uygulama Güvenliği Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
AV, AppID, IPS, DoS Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
DNS Filtreleme Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
PPP Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
PPP Debug Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Sanal Kablo Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma
Paket Filtreleme Logları	<input checked="" type="radio"/> Cihazda Tut <input type="radio"/> Cihazda Tutma

Güvenlik Kurallarında, log tutulması istenilen kuralda **Loglama** aktif edilir.

Güvenlik Kuralları - Kayıt Düzeltme

Genel Kurallar

Grubu: ANA KURAL SETİ ANA GRU...
Sıra No: 5
Durum: Aktif
İşlem: Engelle, Reddet, İzin Ver
Loglama: Aktif
Ağ Geçidi: Varsayılan
Açıklama: Psiphon
İnceleme Yöntemi: Aktif, STATEFULL

NAT: Kapalı, Çıkış Adresi, NAT Havuzu, Global NAT

IP Kuralları

Kaynak Güvenlik Bölgesi: Tümü
Kaynak Adres: 10.50.1.0/24
Hedef Güvenlik Bölgesi: Tümü
Hedef Adres: Psiphon3 IP List (190)
Servisler: Tümü
Zaman Dilimleri: Seçiniz...

Güvenlik Profilleri

DoS / Bağlantı Limitleme: Pasif
Web Filtreleme: Pasif
Antivirus: Pasif
DNS Filtreleme: Pasif
Uygulama Kontrolü: Pasif
IPS: Pasif
SSH Denetimi: Pasif
WAF: Pasif

İptal Kaydet

Benzer şekilde logu tutulması istenilen diğer servislerde de **Trafiği Logla** aktif edilmelidir. **Trafiği logla** seçeneği olmayan menülerde, servisin açılması yeterlidir.

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

