

epati

Log İzleme

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

title: Log izleme

Log İzleme

20 farklı rapor çeşidi dinamik olarak buradan görüntülenmekte ve listelenmektedir.

- Anti Spam Logları
- Cluster Logları
- DHCPv4 Logları
- DHCPv6 Logları
- Dışa Atılan İstek Logları
- DNS Filtreleme Logları
- Doğrulama Logları
- Güvenlik Kuralları Kullanım Logları
- Hotspot Logları
- IPsec Servis Logları
- Oturum Geçmişi Logları
- Paket Filtreleme Logları
- PPP Debug Logları
- PPP Logları
- AV, AppID, IPS, DoS Logları
- SSH Denetimi Logları
- SSH Koruma Logları
- SSL VPN Logları
- Trafik Oturum Logları
- Sanal Kablo Logları
- Web Erişim Logları
- Web Sunucu Güvenliği Logları
- WF İçerik ve Antivirüs Tarama Logları
- WF Sayfa Yasaklama Logları
- Yasaklanan Kullanıcılar Logları

Anti Spam Raporları	Cluster Raporları	DNS Filtreleme Raporları
Güvenlik Kuralları Kullanım Raporu	Hotspot Logları	IPsec Servis Raporları
Paket Filtreleme Raporları	PPP Debug Logları	PPP Raporları
AV, ApplID, IPS, DoS Logları	SSH Denetimi Raporları	SSH Koruma Raporları
SSL VPN Raporları	Trafik Oturum Raporları	Sanal Kablo Raporları
Web Erişim Raporları	Web Sunucu Güvenliği Raporları	WF İçerik ve Antivirüs Tarama Raporları
WF Sayfa Yasaklama Raporları	Yasaklanan Kullanıcılar Raporları	

Anti Spam Logları

Anti-spam raporları, e-postaların spam filtrelerinden geçme sürecini detaylandıran kayıtlardır.

Anti Spam Raporları									
CSV PDF XLS HTML Sayfa Bağı 50 Kayıt Göster Göster/Gizle Sıralama Filtreleme									
#	Zaman Damgası	Kimden	Kimlere	Konu	SMTP Adresi	Skor	Eylem	Semboller	
« « » » Giriş									

Alan	Açıklama
Zaman Damgası	E-postanın işlendiği tarih bilgisini gösterir.
Kimden	E-postayı gönderen kişinin veya sistemin e-posta adresini belirtir.
Kimlere	E-postanın gönderildiği alıcı veya alıcıların e-posta adreslerini gösterir.
Konu	E-postanın içerik bilgisini içerir.
SMTP Adresi	E-postayı gönderen sunucunun IP adresi veya alan adını belirtir.
Skor	E-postanın spam olasılığını gösteren sayısal bir değerdir.
Eylem	Anti-spam sisteminin e-postaya uyguladığı işlemi belirtir.
Semboller	E-postanın spam olarak işaretlenmesine katkıda bulunan belirli anti-spam kontrollerinin sonuçlarını gösteren kodlardır.

Cluster Logları

Cluster ile ilgili oluşan durumları ve durumların gerçekleştiği arayüzleri tarihe göre raporlamaktadır.

[← Raporlara Dön](#)

#	Zaman Damgası	İşlem	Son Görev	Önceki Görev	Açıklama	Detaylar
		🔄🔄🔄 🔄	🔄🔄 🔄🔄	🔄🔄🔄 🔄	🔄🔄🔄	🔄🔄🔄
1	2022-10-19 09:29:47.385494+03	Görev Değiştii	AKTİF	PASİF	Diğer cihaz PASİF olduđu için...	{“Yerel Cihaz Bilgileri”: {“gorev”: “AKTİF”, “İpAdresi”: “99.99.99.40”, “sistemAdi”: “Antikor NGFW - 1.Cihaz”, “kabloDurum”: {“detaylar”: {“vmx0”: 0, “vmx1”: 0, “vmx2”: 0, “vmx3”: 0, “vmx6”: 0, “vmx7”: 0, “vmx8”: 0, “vmx9”: 0}, “kabloTakılıOlmayanEthSayisi”: 0}, “aktiflikUptime”: 2325}, “Diğer Cihaz Bilgileri”: {“gorev”: “PASİF”, “İpAdresi”: “99.99.99.41”, “sistemAdi”: “Antikor NGFW - 2.Cihaz”, “kabloDurum”: {“detaylar”: {“vmx0”: 0, “vmx1”: 0, “vmx2”: 0, “vmx3”: 0, “vmx6”: 0, “vmx7”: 0, “vmx8”: 0, “vmx9”: 0}, “kabloTakılıOlmayanEthSayisi”: 0}, “aktiflikUptime”: -1}}}

Alan	Açıklama
Zaman Damgası	Zaman damgası, olayın tam olarak ne zaman gerçekleştiğini gösterir.
İşlem	Cluster üzerindeki işlemlerin neler olduğu açıklanmaktadır. (Ne yapılmış).
Son Görev	Cluster içindeki ilgili node'un şu anda bulunduğu durumu veya en son gerçekleştirdiği geçişi gösterir.
Önceki Görev	Bu node'un önceki rolü neydi, hangi durumdan geldiğini gösterir.
Açıklama	Bu kısımda olayın kısa özeti yer alır.
Detaylar	Bu bölümde olayın arka planı yani teknik ayrıntılar yer alır.

DHCPv4 Logları

Seçilen tarih için DHCPv4 servisi tarafından IPv4 adresi atanmış olan istemcilere ait DHCPv4 raporlarını gösterir.

#	IP Adresi	MAC Adresi	Network	Kayıtlı Bilgisayar Adı	Görünen Bilgisayar Adı	Kira Başlangıcı	Kira Bitişi	Toplam Kira Süresi

ALAN	AÇIKLAMA
IP Adresi	DHCP servisi tarafından istemciye atanmış IPv4 adresini gösterir.
MAC Adresi	IPv4 adresini alan istemciye ait MAC adresini gösterir.
Network	İstemcinin bağlı olduğu IPv4 ağı (network) gösterir.
Kayıtlı Bilgisayar Adı	İstemci Tanımlarında kayıtlı olan bilgisayar adını gösterir.
Görünen Bilgisayar Adı	Bilgisayarın işletim sisteminde tanımlı olan bilgisayar adını gösterir.
Kira Başlangıcı	IPv4 adresinin istemciye atanma tarihini gösterir.
Kira Bitişi	IPv4 adresinin istemci tarafından bırakıldığı tarihi gösterir.
Toplam Kira Süresi	İstemcinin IPv4 adresini toplamda ne kadar süre kullandığını gösterir.

Filtreleme

IP Adresi	IPv6		Kapsayan		☐ Ters
MAC Adresi	MAC	11:11:11:11:11:11	İçeren		☐ Ters
Network	Filtre Yok				☐ Ters
Kayıtlı Bilgisayar Adı			İçeren		☐ Ters
Görünen Bilgisayar Adı			İçeren		☐ Ters
Kira Başlangıcı			Tarihinde		☐ Ters
Kira Bitişi			Tarihinde		☐ Ters

Filtrele

DHCPv6 Logları

Seçilen tarih için DHCPv6 servisi tarafından IPv6 adresi atanmış olan istemcilere ait DHCPv6 raporlarını gösterir.

DHCPv6 Raporları

Tarih03.04.2020 - 03.04.2020Yükle

XLS CSV PDF

Göster/Gizle Sayfa Başı Kayıt SayısıTamamFiltreleFiltreyi Temizle

IP AdresiMAC AdresiNetworkKayıtlı Bilgisayar AdıGörünen Bilgisayar AdıKira BaşlangıcıKira BitişiToplam Kira Süresi

Gör

ALAN	AÇIKLAMA
IP Adresi	DHCP servisi tarafından istemciye atanmış IPv6 adresini gösterir.
MAC Adresi	IPv6 adresini alan istemciye ait MAC adresini gösterir.
Network	İstemcinin bağlı olduğu IPv6 ağı (network) gösterir.
Kayıtlı Bilgisayar Adı	İstemci Tanımlarında kayıtlı olan bilgisayar adını gösterir.
Görünen Bilgisayar Adı	Bilgisayarın işletim sisteminde tanımlı olan bilgisayar adını gösterir.
Kira Başlangıcı	IPv6 adresinin istemciye atanma tarihini gösterir.
Kira Bitişi	IPv6 adresinin istemci tarafından bırakıldığı tarihi gösterir.
Toplam Kira Süresi	İstemcinin IPv6 adresini toplamda ne kadar süre kullandığını gösterir.

Dışa Atılan İstek Logları

Dışa Atılan İstek Logları, sistem tarafından dış sistemlere yapılan isteklerin ve bu isteklere ait yanıtların detaylarını kayıt altına alır.

IP Adresi	IPv6		Kapsayan	☐ Ters
MAC Adresi	MAC	11:11:11:11:11:11	İçeren	☐ Ters
Network	Filtre Yok			☐ Ters
Kayıtlı Bilgisayar Adı			İçeren	☐ Ters
Görünen Bilgisayar Adı			İçeren	☐ Ters
Kira Başlangıcı			Tarihinde	☐ Ters
Kira Bitişi			Tarihinde	☐ Ters

Filtrele

DNS Filtreleme Logları

DNS filtreleme logları, bir ağda yapılan DNS sorgularını ve bu sorgulara verilen yanıtları takip eder.

DNS Filtreleme Raporları

[← Raporlara Dön](#)

#	Zaman Damgası	Tip	Sorgu Adı	Sorgu Tipi	İstemci IP	Yanıt	Karar
1	2025-04-30 12:07:40	Response	dns.msftncsi.com.	A	192.168.2.102	[object Object]	allow
2	2025-04-30 12:07:40	Query	dns.msftncsi.com.	A	192.168.2.102		allow
3	2025-04-30 12:07:14	Response	boot.net.anydesk.com.	A	192.168.2.102	[object Object], [object Object], [object Object]...	allow
4	2025-04-30 12:07:14	Query	boot.net.anydesk.com.	A	192.168.2.102		allow
5	2025-04-30 12:04:40	Response	client.wns.windows.com.	A	192.168.2.102	[object Object], [object Object]	allow
6	2025-04-30 12:04:40	Query	client.wns.windows.com.	A	192.168.2.102		allow
7	2025-04-30 12:01:49	Response	boot.net.anydesk.com.	A	192.168.2.102	[object Object], [object Object], [object Object]...	allow
8	2025-04-30 12:01:49	Query	boot.net.anydesk.com.	A	192.168.2.102		allow
9	2025-04-30 12:01:43	Response	geover.prod.do.dsp.mp.microsoft.com.	A	192.168.2.102	[object Object], [object Object], [object Object]	allow
10	2025-04-30 12:01:43	Query	geover.prod.do.dsp.mp.microsoft.com.	A	192.168.2.102		allow

Alan	Açıklama
Zaman Damgası	DNS filtrelemesinin sistemde gerçekleştiği tarih ve saattir.
Tip	DNS filtrelemesinin türünü belirtir
Sorgu Adı	Erişilmek istenen alan adını (domain) gösterir.
Sorgu Tipi	Yapılan DNS sorgusunun tipidir.
İstemci IP	DNS sorgusunu yapan cihazın IP adresidir.
Yanıt	DNS sunucusunun bu sorguya verdiği cevaptır.
Karar	Sorguya izin verildi mi yoksa engellendi mi, bunu belirtir.

Doğrulama Logları

Doğrulama Logları, sistem üzerinde yapılan kullanıcı doğrulama (authentication / validation) işlemlerine ait kayıtları gösterir. Bu loglar sayesinde hangi kullanıcı tarafından, hangi sayfa veya URL üzerinde, hangi metot ile doğrulama hatası olduğu detaylı olarak izlenebilir.

#	Zaman Damgası	Kullanıcı Adı	Sayı Adı	Metod	Doğrulama Hataları	URL

Alan	Açıklama
#	Log kaydının tablo üzerindeki sıra numarasını gösterir.
Zaman Damgası	Doğrulama işleminin gerçekleştiği tarih ve saat bilgisidir.
Kullanıcı Adı	Doğrulama işlemini gerçekleştiren kullanıcı hesabını gösterir.
Sayfa Adı	Doğrulama işleminin yapıldığı sayfanın adını gösterir.
Metod	Doğrulama sırasında kullanılan HTTP metodunu gösterir (GET, POST vb.).
Doğrulama Hataları	Doğrulama sırasında oluşan hata veya hata mesajlarını gösterir.
URL	Doğrulama işleminin gerçekleştiği tam URL bilgisini gösterir.

Güvenlik Kuralları Kullanım Logları

Güvenlik kuralı kullanım logları, [Güvenlik Kuralları](#) sayfasında oluşturduğumuz kuralların kullanım loglarıdır.

Güvenlik Kuralları Kullanım Raporu

CSV

PDF

XLS

HTML

Sayfa Başı

50

Kayıt Göster

Göster/Gizle

Sıralama

Filtreleme

#	Grup ID	Grup Adı	Kural ID	Sıra No	Açıklama	Hit sayısı	İlk kullanım	Son kullanım
1	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	c1qW3H8qgUn	1	çoklu özellik kontrolü	38	2025-04-30 09:34:12.551571+03	2025-04-30 11:25:42.221011+03
2	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	c1sdOF0toxwu	2	ip-adresi-kuralı	98	2025-04-30 08:41:05.401168+03	2025-04-30 09:21:59.958441+03
3	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	Açq8PnhQKCj	3	uygulama_tanima_paket_testi	8	2025-04-29 21:47:56.76646+03	2025-04-30 08:31:05.001721+03
4	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	c1oLSpt6Dh8	4	kullanici_seccil_kural	4959	2025-04-29 14:08:03.270749+03	2025-04-29 16:36:02.90927+03
5	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	c1juMWXC0GE	5	icmp	18840	2025-04-28 13:35:21.091507+03	2025-04-29 11:32:35.611544+03
6	c1Cn76P3ah9	Ana Kural Seti Ana Grubu	c1CMUnLCupjp	6	sshdenetimi	263183	2025-04-24 21:30:46.052857+03	2025-04-28 13:32:14.380987+03

Alan	Açıklama
Grup ID	Bu kuralın ait olduğu grubun benzersiz kimlik numarasını belirtir.
Grup Adı	Kuralın yer aldığı güvenlik grubunun adını belirtir.
Kural ID	Her bir güvenlik kuralının kendine ait benzersiz kimlik numarasını gösterir.
Sıra No	Kuralın sıralandığı yerin numarasını belirtir. En düşük numara ilk dikkate alınan kural.
Açıklama	Bu güvenlik kuralının ne işe yaradığını açıklayan kısa bir tanımlamadır.
Hit Sayısı	Bu güvenlik kuralının kaç kez tetiklendiğini veya kaç kez kullanıldığını gösteren sayıdır.
İlk Kullanım	Kuralın ilk kez ne zaman tetiklendiğini veya uygulandığını gösterir.
Son Kullanım	Kuralın son kez ne zaman tetiklendiğini veya kullanıldığını gösterir.

Hotspot Logları

CSV PDF XLS HTML Sayfa Bazi 50 Kayıt Göster Göster/Gizle Sıralama Filtreleme

#	Kullanıcı Adı	IP Adresi	Giriş Zamanı	Çıkış Zamanı
1	system			
2	merkezyonetimkullanicisi	10.2.1.34	2026-01-12 22:02:07.105522+03	2026-01-12 22:04:46+03
3	merkezyonetimkullanicisi	10.2.1.34	2026-01-12 22:02:11.316245+03	2026-01-12 22:04:46+03
4	merkezyonetimkullanicisi	10.2.1.34	2026-01-12 22:02:56.868922+03	2026-01-12 22:04:46+03
5	merkezyonetimkullanicisi	10.2.1.34	2026-01-12 22:03:31.892487+03	2026-01-12 22:04:46+03

Alan	Açıklama
#	Log kaydının tablo üzerindeki sıra numarasını gösterir.
Kullanıcı Adı	Oturum açan kullanıcı hesabını gösterir.
IP Adresi	Kullanıcının oturum açtığı istemci IP adresini gösterir.
Giriş Zamanı	Kullanıcının sisteme giriş yaptığı tarih ve saat bilgisidir.
Çıkış Zamanı	Kullanıcının sistemden çıkış yaptığı tarih ve saat bilgisidir.

Paket Filtreleme Logları

Paket filtreleme logları, ağdan geçen veri paketlerinin hangi kurallara göre işlendiğini, izin verilip verilmediğini ve paketin yönünü gösteren güvenlik kayıtlarıdır. Bu raporlar sayesinde, ağ trafiği gerçek zamanlı olarak analiz edilir ve olası tehditler tespit edilebilir.

Paket Filtreleme Raporları

Raporlara Dön

CSV PDF XLS HTML

Sayfa Bazi 50 Kayıt Göster Göster/Gizle Sıralama Filtreleme

#	Zaman Damgası	İşlem	Protokol	Giriş	Çıkış	Kaynak IP	K. Port	Hedef IP	H. Port	K. Kullanıcı	H. Kullanıcı	K. NAT Tipi	K. NAT Portu	H. NAT Tipi	H. NAT IP	H. NAT Portu	Giriş Kural Seti	Giriş Kural ID	Çıkış Kural Seti	Çıkış Kural ID	TCP Flags	Analiz
1	2025-04-30 13:14:16.971661+03	pass	TCP	vmx2 - LAN2	vmx0 - WAN1	192.168.2.102	54700	20.106.86.13	443	-	-	src-nat	10.2.1.177	56445			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn	-----S	Connection establish reques...
2	2025-04-30 13:14:16.962299+03	pass	UDP	vmx2 - LAN2	vmx0 - WAN1	192.168.2.102	49500	1.1.1.1	53	-	-	src-nat	10.2.1.177	60220			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn		
3	2025-04-30 13:14:16.945216+03	pass	UDP	vmx2 - LAN2	vmx1 - LAN1	192.168.2.102	49500	192.168.1.6	53	-	-	src-nat	192.168.1.2	56278			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn		
4	2025-04-30 13:13:51.545207+03	pass	TCP	vmx2 - LAN2	vmx0 - WAN1	192.168.2.102	54699	217.20.58.98	80	-	-	src-nat	10.2.1.177	65459			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn	-----S	Connection establish reques...
5	2025-04-30 13:13:51.537019+03	pass	UDP	vmx2 - LAN2	vmx0 - WAN1	192.168.2.102	57475	1.1.1.1	53	-	-	src-nat	10.2.1.177	61532			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn		
6	2025-04-30 13:13:50.537012+03	pass	UDP	vmx2 - LAN2	vmx1 - LAN1	192.168.2.102	57475	192.168.1.7	53	-	-	src-nat	192.168.1.2	63579			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn		
7	2025-04-30 13:13:50.516441+03	pass	UDP	vmx2 - LAN2	vmx1 - LAN1	192.168.2.102	57475	192.168.1.6	53	-	-	src-nat	192.168.1.2	64959			cCin76P3an9	cIqzw3H8ggUn	cCin76P3an9	cIqzw3H8ggUn		

Alan	Açıklama
Zaman Damgası	Paketin işlendiği tarih ve saat bilgisidir.
İşlem	Pakete uygulanan işlem türünü belirtir.(pass/block)
Protokol	Paket iletişiminin gerçekleştiği ağ protokolünü (örneğin TCP, UDP) gösterir.
Giriş	Paket ağda hangi arayüzden (interface) içeri girmişse onu belirtir.
Çıkış	Paket ağdan hangi arayüzden çıkmışsa onu gösterir.
Kaynak IP	Paketin geldiği cihazın IP adresidir.
K.Port	Paketi gönderen cihazın kullandığı port numarasıdır.
Hedef IP	Paketin ulaşmak istediği hedef IP adresidir.
H.Port	Paketin ulaştığı hedefteki port numarasıdır.
K.Kullanıcı	Kaynak tarafındaki oturumda kullanılan kullanıcı bilgisidir (varsa).
H.Kullanıcı	Hedef sistemdeki kullanıcı kimliğidir (varsa).
K.NAT Tipi	Kaynak tarafında uygulanan NAT (adres çevirme) türüdür.
K.NAT IP	NAT işleminde kullanılan yeni kaynak IP adresidir.
K.NAT Portu	NAT işleminde kullanılan yeni kaynak port numarasıdır.
H.NAT Tipi	Hedef tarafında uygulanan NAT türüdür.
H.NAT IP	NAT işleminde hedefe atanmış yeni IP adresidir.
H.NAT Portu	NAT işleminde hedefe atanmış yeni port numarasıdır.
Giriş Kural Seti	Paketin girişte karşılaştığı kural grubunun adıdır.
Giriş Kural ID	Girişte uygulanan belirli güvenlik kuralının kimlik numarasıdır.
Çıkış Kural Seti	Paketin çıkışta karşılaştığı kural grubunun adıdır.
Çıkış Kural ID	Çıkışta uygulanan belirli güvenlik kuralının kimlik numarasıdır.
TCP Flags	TCP paketleri için iletişim durumunu belirten bayrak (flag) bilgilerini gösterir.
Analiz	Bu paketin güvenlik açısından sistem tarafından yapılmış olan yorum veya işlem notudur.

PPP Debug Logları

PPP (Point-to-Point Protocol) Debug logları, iki cihaz arasında yapılan PPP bağlantısının kurulum, kimlik doğrulama ve veri iletim süreçlerini ayrıntılı olarak izleyen hata ayıklama kayıtlarıdır. Bu loglar, bağlantı hataları, oturum açma süreçleri ve iletişim adımlarını adım adım analiz etmek için kullanılır.

#	Zaman Damgası	Mesaj
1	2020-10-07 10:05:46	tun0(ppp7): Phase: Signal 15, terminate.
2	2020-10-07 10:05:46	tun0(ppp7): Phase: deflink: Disconnected!
3	2020-10-07 10:05:46	tun0(ppp7): Phase: deflink: opening -> closed
4	2020-10-07 10:05:46	tun0(ppp7): Warning: Delete route failed: 127.127.0.7: errno: Address already in use
5	2020-10-07 10:05:46	tun0(ppp7): Phase: bundle: Dead
6	2020-10-07 10:05:46	tun0(ppp7): Phase: PPP Terminated (normal).
7	2020-10-07 10:05:45	tun0(ppp7): Command: ppp7: iface clear
8	2020-10-07 10:05:45	tun0(ppp7): Warning: deflink: Unable to set physical to speed 0
9	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: Disconnected!
10	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: lcp -> logout
11	2020-10-07 10:05:45	tun0(ppp7): Warning: deflink: Unable to set physical to speed 0
12	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: Disconnected!
13	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: logout -> hangup
14	2020-10-07 10:05:45	tun0(ppp7): Warning: deflink: Unable to set physical to speed 0
15	2020-10-07 10:05:45	tun0(ppp7): Warning: deflink: tcsetattr: Unable to restore device settings
16	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: Connect time: 2953 secs: 124514228 octets in, 4448898 octets out
17	2020-10-07 10:05:45	tun0(ppp7): Phase: deflink: 96395 packets in, 54678 packets out

Not: Kullanıcılar bu raporları **csv, pdf, xls ve html** formatlarında indirebilmektedir.

PPP (Point-to-Point Protocol) raporları, ağ üzerindeki PPP bağlantılarının genel durumu hakkında bilgi verir; özellikle IP atamaları ve bağlantı arayüzleri gibi detayları içerir.

Alan	Açıklama
Zaman Damgası	PPP bağlantı işleminin gerçekleştiği tarih ve saat bilgisidir.
İşlem	PPP bağlantısı için yapılan işlemi belirtir.
Ethernet Adı	PPP oturumunun bağlı olduğu fiziksel Ethernet arayüzünün adıdır.
Açıklama	Bağlantıya dair sistem tarafından girilen durum veya bilgilendirici nottur.
Arayüz	PPP oturumunun kurulduğu mantıksal arayüz adıdır.
IPv4 Adresi	PPP bağlantısı sırasında istemciye atanan IPv4 adresidir.
IPv4 Ağ Geçidi	PPP oturumu için kullanılan varsayılan ağ geçidinin IPv4 adresidir.

Antivirüs (AV), Uygulama Tanımlama (AppID), Saldırı Önleme Sistemi (IPS) ve Hizmet Dışı Bırakma (DoS) olaylarına ilişkin güvenlik kayıtlarıdır. Ağdaki tehditleri, riskli uygulamaları ve saldırı girişimlerini tespit ederek yöneticilere detaylı güvenlik görünürlüğü sağlar.

Alan	Açıklama
Zaman Damgası	Olayın veya güvenlik işleminin gerçekleştiği tarih ve saat bilgisidir.
İşlem	Sistem tarafından yapılan güvenlik müdahalesinin türünü belirtir.
Karar	Olay sonucunda sistemin izin verip vermediğini veya engellediğini belirtir.
Protokol	İletişimin gerçekleştiği ağ protokolünü (örneğin TCP, UDP) gösterir.
Kaynak Kullanıcı	Olayın çıktığı istemcideki oturum açmış kullanıcıyı belirtir.
Kaynak IP	Trafiği başlatan cihazın IP adresidir.
Kaynak Port	Trafiği başlatan cihazın kullandığı port numarasıdır.
Hedef Kullanıcı	Trafiğin ulaştığı cihazda oturum açmış olan kullanıcı bilgisidir.
Hedef IP	Trafiğin yönlendirildiği hedef IP adresidir.
Hedef Port	Hedefte kullanılan servis port numarasıdır.
Servis	Belirli bir porta bağlı çalışan uygulama veya servis bilgisidir.
Ağ Arayüzü	Trafiğin geçtiği bağlantı noktasıdır.
VLAN	Olayın geçtiği sanal yerel ağıdır.
AppID	Tanımlanan veya tespit edilen uygulama adıdır
Kural	Uygulanan güvenlik politikasının adıdır.
Açıklama	Olayla ilgili sistemin oluşturduğu açıklayıcı bilgidir.
Sistem	Olayı işleyen veya kaydeden güvenlik sistemi bileşenidir.
Kayıt ID	Her olaya özel oluşturulmuş benzersiz kimlik numarasıdır.
QoS Bilgisi	Olayın geçtiği trafiğe ait hizmet kalitesi seviyesidir.
Severity	Olayın önem derecesini ifade eder.

SSH Denetim Raporları

SSH denetim raporları, ağ üzerindeki cihazlara yapılan **SSH (Secure Shell)** bağlantı girişimlerini ve yönetim aktivitelerini izlemek amacıyla kaydedilen güvenlik kayıtlarıdır.

SSH Denetimi Raporları [Raporlara Dön](#)

CSV PDF XLS HTML

Sayfa Bapı 50 Kayıt Göster Göster/Göster Sıralama Filtreleme

#	Zaman Damgası	Kaynak Adres	Kaynak Port	Hedef Adres	Hedef Port	Kullanıcı Adı	İşlem
---	---------------	--------------	-------------	-------------	------------	---------------	-------

Get

Alan	Açıklama
Zaman Damgası	SSH işleminin gerçekleştiği tarih ve saat bilgisidir.
Kaynak Adres	Bağlantıyı başlatan istemci cihazın IP adresidir.
Kaynak Port	İstemcinin SSH bağlantısı için kullandığı port numarasıdır.
Hedef Adres	Bağlantı kurulmak istenen sunucunun IP adresidir.
Hedef Port	SSH erişimi için hedef sistemde dinlenen port numarasıdır.
Kullanıcı Adı	SSH oturumu için kimlik doğrulama sırasında girilen kullanıcı hesabıdır.
İşlem	Gerçekleşen SSH işleminin türünü belirtir.

SSH Koruma Raporları

SSH koruma raporları, yetkisiz veya şüpheli SSH bağlantı girişimlerini tespit edip engelleyen güvenlik önlemlerini kayıt altına alan raporlardır.

SSH Koruma Raporları

[← Raporlara Dön](#)

#	Zaman Damgası	İşlem	IP Adresi	Sıralama Yapılmamış
1	2020-10-06 15:48:15	release	10.10.99.10	
2	2020-10-06 15:45:32	block	10.10.99.10	

Alan	Açıklama
Zaman Damgası	SSH işleminin gerçekleştiği tarih ve saat bilgisidir.
İşlem	Sistem tarafından alınan güvenlik aksiyonunu belirtir; örneğin IP engellendi, erişim reddedildi gibi.
IP Adresi	Kısıtlanan veya engellenen kaynak cihazın IP adresidir.

SSL VPN Logları

Kullanıcılar için tanımlanmış SSL VPN bağlantılarına ait oturum kayıtları sistem tarafından detaylı şekilde tutulmaktadır. Bu kayıtlar; bağlantı zamanı, kullanıcı bilgileri, IP adresi, bağlantı süresi ve veri trafiği gibi bilgileri içermektedir. Bu sayede hem güvenlik takibi yapılabilir hem de kullanıcı aktiviteleri denetlenebilir.

SSL VPN Raporları

Yenile

XLS CSV PDF

Göster/Gizle

Sayfa Başı Kayıt Sayısı

Tamam

Filtrele

Filtreyi Temizle

#	Bağlantı Tarihi	Kaynak IP Adresi	Kaynak Port	CN	Vpn IPv4 Adresi	Bağlantı Bitiş Tarihi	Toplam Vpn Süresi	Yükleme Boyut	İndirme Boyut
1	11/11/2019 02:00:58	94.122.153.199	19206		10.255.4.100	11/11/2019 02:01:33	35	8 KB	3 KB
2	11/11/2019 09:35:49	94.122.153.199	16645		10.255.4.100			0 BYTE	0 BYTE
3	11/11/2019 14:05:53	37.154.57.197	34342		10.255.4.6	11/11/2019 14:17:53	720	2 MB	15 MB
4	11/11/2019 14:18:55	37.154.57.197	33302		10.255.4.6	11/11/2019 14:29:00	605	508 KB	557 KB
5	11/11/2019 14:28:59	37.154.57.197	33893		10.255.4.6	11/11/2019 14:30:02	63	15 KB	20 KB
6	11/11/2019 14:39:55	37.154.57.197	33396		10.255.4.6	11/11/2019 15:35:36	3341	4 MB	10 MB
7	11/11/2019 17:55:55	78.180.10.167	64612		10.255.4.6	11/11/2019 17:56:57	62	108 KB	172 KB
8	11/11/2019 20:36:04	78.180.10.167	63799		10.255.4.6	11/11/2019 20:43:27	443	202 KB	1 MB
9	12/11/2019 02:47:06	94.122.153.199	17725		10.255.4.100	12/11/2019 02:47:41	35	6 KB	3 KB
10	12/11/2019 07:44:54	94.122.153.199	19160		10.255.4.100			0 BYTE	0 BYTE
11	12/11/2019 10:44:04	46.155.243.144	58195		10.255.4.3	12/11/2019 10:59:49	945	1 MB	9 MB
12	12/11/2019 11:12:59	46.155.243.144	57894		10.255.4.3	12/11/2019 11:18:59	360	536 KB	4 MB
13	12/11/2019 11:32:13	46.155.243.144	58185		10.255.4.3	12/11/2019 11:35:57	224	363 KB	3 MB

« < 1 > »

Gör

ALAN	AÇIKLAMA
Bağlantı Tarihi	SSL VPN bağlantısının ne zaman bağlandığını gösterilmektedir.
Kaynak IP Adresi	Hangi IP adresi ile VPN bağlantısı oluşturduğunu gösterilmektedir.
Kaynak Port	Hangi port ile bağlantı kurulduğunu gösterilmektedir.
CN	Sertifika adı gösterilmektedir.
Vpn IPv4 Adresi	Bağlantı esnasında kullanılan IP adresi gösterilmektedir.
Bağlantı Bitiş Tarihi	SSL VPN bağlantısının ne zaman sonlandığını gösterilmektedir.
Toplam Vpn Süresi	Bağlantı boyunca geçen toplam süre(saniye cinsinden) gösterilmektedir.
Yükleme Boyutu	SSL VPN bağlantısı esnasında ne kadar yükleme yapıldığını gösterilmektedir.
İndirme Boyutu	SSL VPN bağlantısı esnasında ne kadar indirme yapıldığını gösterilmektedir.

Trafik Oturum Logları

Trafik Oturum Logları, belirli bir zaman aralığında ağ üzerinde gerçekleşen kaynak ve hedef IP'ler arasında kurulan oturumları ve protokol bazlı iletişim bilgilerini incelemek için kullanılan bir rapordur. Bu rapor sayesinde, sistem yöneticileri ağ trafiğini detaylı şekilde analiz edebilir, güvenlik ya da performans açısından olağandışı davranışları tespit edebilir.

Dinamik Raporlar

Trafik Oturum Raporları

CSV PDF XLS HTML

Filtreleme

Başlangıç Tarihi (Zorunlu)

Bitiş Tarihi (Zorunlu)

Protokol

Kaynak Adres

Kaynak Port

Hedef Adres

Hedef Port

Tanımları Uygula

Sayfa Başı

50

Kayıt Göster

Göster/Gizle

Sıralama

Filtreleme

Raporlara Dön

#	Başlangıç Tarihi	Bitiş Tarihi	Protokol	Hedef Port	Gelen Paket	Giden Paket	Gelen Byte	Giden Byte
---	------------------	--------------	----------	------------	-------------	-------------	------------	------------

Alan	Açıklama
Başlangıç Tarihi	Trafik oturumlarının izlenmeye başlanacağı ilk tarih ve saat bilgisidir (zorunlu olarak girilmelidir).
Bitiş Tarihi	Oturum kayıtlarının alınacağı son tarih ve saat bilgisidir (zorunlu olarak tanımlanmalıdır).
Protokol	İzlenen oturumun gerçekleştiği iletişim protokolüdür (örneğin TCP, UDP, ICMP).
Kaynak Adres	Oturumu başlatan cihazın IP adresidir.
Kaynak Port	Oturumu başlatan cihazın kullandığı port numarasıdır.
Hedef Adres	Oturumun yöneldiği hedef sistemin IP adresidir.
Hedef Port	Hedef cihazda kullanılan servis port numarasıdır.

Sanal Kablo Logları

Sanal Kablo Logları sistem üzerinde sanal bağlantı üzerinden geçen ağ trafiğini izleyip, hangi cihazlar ve kullanıcılar arasında nasıl bir iletişim kurulduğunu gösteren ayrıntılı kayıtlardır.

Sanal Kablo Raporları															Raporlara Dön
CSV PDF XLS HTML															Sayfa Sayısı: 50 Kayıt Göster Göster/Göster Sıralama Filtreleme
#	Zaman Damgası	Karar	Protokol	Kaynak K. Adı	Kaynak Adres	Kaynak Port	Hedef K. Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	Kural	Açıklama	Sistem	Kayıt ID

Alan	Açıklama
Zaman Damgası	Sanal kablo olayının veya trafiğinin gerçekleştiği tarih ve saat bilgisidir.
Karar	Trafik için verilen izin (allow) veya engelleme (deny) gibi sistemin uyguladığı karardır.
Protokol	Sanal kablo üzerinden taşınan verinin iletişim protokolüdür (örnek: TCP, UDP).
Kaynak K. Adı	Trafiği başlatan uçta yer alan kullanıcının adıdır.
Kaynak Adres	Bağlantıyı başlatan cihazın IP adresidir.
Kaynak Port	Kaynak cihazın kullandığı port numarasıdır.
Hedef K. Adı	Trafiğin yönlendirildiği uçtaki kullanıcı adıdır.
Hedef Adres	Trafiğin ulaştığı hedef sistemin IP adresidir.
Hedef Port	Hedefteki servisin çalıştığı port numarasıdır.
Ağ Arayüzü	Trafiğin geçtiği fiziksel veya sanal ağ bağlantı noktasıdır.
VLAN	Bağlantının geçtiği sanal yerel ağ (Virtual LAN) kimliğidir.
Kural	Trafiğe uygulanan güvenlik veya yönlendirme politikasının adıdır.
Açıklama	Olay hakkında sistemin oluşturduğu özet veya açıklayıcı bilgidir.
Sistem	Olayı kaydeden veya işleyen güvenlik modülü ya da sistem bileşenidir.
Kayıt ID	Her olay için oluşturulmuş benzersiz tanımlayıcı numaradır.

Web Erişim Logları

Web erişim Logları, kullanıcıların ağ üzerinden internete yaptıkları web isteklerinin detaylarını kayıt altına alan loglardır. Bu raporlar, kim hangi internet adresine, ne zaman ve ne kadar veri kullanarak erişti sorularını yanıtlamaya yardımcı olur.

Web Erişim Raporları

Raporlara Dön

CSVPDFXLSHTML

Sayfa Baş50Kayıt GösterGöster/GösterilemezSıralamaFiltreleme

#	Tarih Saat	İstemci IP Adresi	İstemci Portu	İstemci Mac Adresi	Kullanıcı Adı	Sunucu IP Adresi	Alan Adı	Adres	SSL SNI	HTTP Metodu	HTTP Kodu	İçerik	Tüketim	Geçen Süre	Başlangıç Zamanı	Bitiş Zamanı
1	2025-04-30 13:13:11.771+03	192.168.2.102	54697				kv801.prod.do.dsp.mp.microsoft.com	https://kv801.prod.do.dsp.m...	kv801.prod.do.dsp.mp.microsoft.com	GET	0		0		2025-04-30 13:13:11.771+03	
2	2025-04-30 13:13:05.314+03	192.168.2.102	54696	00:0c:29:ad:8d:7a	192.168.2.102	184.28.154.41	disc801.prod.do.dsp.mp.microsoft.com	https://disc801.prod.do.dsp...	disc801.prod.do.dsp.mp.microsoft.com	GET	200	text/json	480		2025-04-30 13:13:05.314+03	
3	2025-04-30 13:13:04.992+03	192.168.2.102	54696	00:0c:29:ad:8d:7a	192.168.2.102	184.28.154.41	184.28.154.41	184.28.154.41:443	disc801.prod.do.dsp.mp.microsoft.com	CONNECT	0		0	00:00:00.206	2025-04-30 13:13:04.992+03	2025-04-30 13:13:05.198+03
4	2025-04-30 13:13:03.959+03	192.168.2.102	54697	00:0c:29:ad:8d:7a	192.168.2.102	184.28.154.41	184.28.154.41	184.28.154.41:443	kv801.prod.do.dsp.mp.microsoft.com	CONNECT	0		0	00:00:00.201	2025-04-30 13:13:03.959+03	2025-04-30 13:13:04.16+03
5	2025-04-30 13:13:03.735+03	192.168.2.102	54696				geover.prod.do.dsp.mp.microsoft.com	https://geover.prod.do.dsp...	geover.prod.do.dsp.mp.microsoft.com	GET	0		0		2025-04-30 13:13:03.735+03	
6	2025-04-30 13:12:56.27+03	192.168.2.102	54696	00:0c:29:ad:8d:7a	192.168.2.102	184.28.153.210	184.28.153.210	184.28.153.210:443	geover.prod.do.dsp.mp.microsoft.com	CONNECT	0		0	00:00:00.231	2025-04-30 13:12:56.27+03	2025-04-30 13:12:56.501+03
7	2025-04-30 13:12:55.766+03	192.168.2.102	54692				disc801.prod.do.dsp.mp.microsoft.com	https://disc801.prod.do.dsp...	disc801.prod.do.dsp.mp.microsoft.com	GET	0		0		2025-04-30 13:12:55.766+03	
8	2025-04-30 13:12:55.561+03	192.168.2.102	54689	00:0c:29:ad:8d:7a	192.168.2.102			195.181.174.173	https://195.181.174.173:443	CONNECT	0		0	00:00:59.576	2025-04-30 13:12:55.561+03	2025-04-30 13:13:55.137+03
9	2025-04-30 13:12:50.462+03	192.168.2.102	54693	00:0c:29:ad:8d:7a	192.168.2.102		*.events.data.microsoft.com	52.168.117.170:443	v10.events.data.microsoft.com	CONNECT	0		0	00:00:00.451	2025-04-30 13:12:50.462+03	2025-04-30 13:12:50.913+03
10	2025-04-30 13:12:47.4+03	192.168.2.102	54692	00:0c:29:ad:8d:7a	192.168.2.102	184.28.154.41	184.28.154.41	184.28.154.41:443	disc801.prod.do.dsp.mp.microsoft.com	CONNECT	0		0	00:00:00.201	2025-04-30 13:12:47.4+03	2025-04-30 13:12:47.601+03

Alan	Açıklama
Tarih Saat	Web erişiminin gerçekleştiği gün ve saat bilgisidir.
İstemci IP Adresi	Web isteğini başlatan cihazın IP adresidir.
İstemci Portu	İstemci cihazın web erişimi için kullandığı port numarasıdır.
İstemci Mac Adresi	Web erişimini gerçekleştiren cihazın donanımsal MAC adresidir.
Kullanıcı Adı	Web erişimini yapan kullanıcının hesabıdır.
Sunucu IP Adresi	Erişim sağlanan internet sitesinin IP adresidir.
Alan Adı	Bağlantı kurulan web sitesinin alan adı (örnek: google.com) bilgisidir.
Adres	Tam erişilen URL ya da web sayfası adresidir.
SSL SNI	HTTPS bağlantılarında belirtilen Sunucu Adı Göstergesi (Server Name Indication) bilgisidir.
HTTP Metodu	Yapılan web isteğinin türünü gösterir; örneğin GET, POST gibi.
HTTP Kodu	Web sunucusunun verdiği yanıt durum kodudur.
İçerik	Erişilen web içeriğinin türüdür.
Tüketim	Web erişimi sırasında kullanılan toplam veri miktarıdır.
Geçen Süre	Web bağlantısının ne kadar süre aktif kaldığını gösterir.
Başlangıç Zamanı	Web oturumunun başladığı ilk zaman damgasıdır.
Bitiş Zamanı	Web oturumunun bittiği zaman damgasıdır.

Web Sunucu Güvenliği Logları

Web Sunucu Güvenliği Logları, kurum içinden veya dışından gelen web isteklerinin sunucu üzerinde oluşturabileceği potansiyel tehditleri ve güvenlik açıklarını analiz eden loglardır.

Web Sunucu Güvenliği Raporları									
Raporlara Dön CSV PDF XLS HTML Sayfa Bp: 50 Kayıt Göster Göster/Göle Sıralama Filtreleme Gör									
#	Zaman Damgası	İstemci	Host	İstek	Kategori	Tespit	Analiz	Önem Derecesi	Etiketler
Gör									

Alan	Açıklama
Zaman Damgası	Güvenlik olayının veya tehdidin tespit edildiği tarih ve saat bilgisidir.
İstemci	Web sunucusuna istekte bulunan kaynak cihazın IP adresidir.
Host	İsteğin gönderildiği web sunucusunun alan adı veya IP adresidir.
İstek	İstemciden gelen HTTP isteğinin tam URI veya yöntem bilgisidir.
Kategori	Tespit edilen güvenlik olayının sınıflandırıldığı tehdit türüdür.
Tespit	Güvenlik sisteminin algıladığı şüpheli veya zararlı davranış bilgisidir.
Analiz	Olayla ilgili yapılan teknik inceleme ve açıklayıcı yorumlardır.
Önem Derecesi	Tespit edilen tehdidin ciddiyet seviyesini belirtir.
Etiketler	Olayla ilişkilendirilen anahtar kelimeler veya sınıflandırıcı ifadelerdir.

WF WF İçerik ve Antivirüs Tarama Logları

Bu log, Web Filtreleme (WF) ve Antivirüs motoru tarafından taranan içeriklerin kayıtlarını içerir; kullanıcıların erişmeye çalıştığı adreslerde zararlı içerik, uygunsuz kategori ya da politika ihlali olup olmadığını analiz eder.

WF İçerik ve Antivirüs Tarama Raporları									
Raporlara Dön CSV PDF XLS HTML Sayfa Bp: 50 Kayıt Göster Göster/Göle Sıralama Filtreleme Gör									
#	Zaman Damgası	İstemci IP Adresi	Kullanıcı	Adres	HTTP Cevap Boyutu	WF Politikası	Kategori	Mesaj	
Gör									

Alan	Açıklama
Zaman Damgası	Tarama olayının gerçekleştiği tarih ve saat bilgisidir.
İstemci IP Adresi	Web erişimini yapan istemci cihazın IP adresidir.
Kullanıcı	İçeriğe erişim girişiminde bulunan kullanıcı hesabıdır.
Adres	Tarama yapılan web adresi ya da dosya URL'sidir.
HTTP Cevap Boyutu	Web sunucusundan gelen içeriğin boyutudur.
WF Politikası	Uygulanan Web Filtreleme kural veya politikasıdır.
Kategori	Erişilen içeriğin WF sistemi tarafından sınıflandırıldığı içerik türüdür.
Mesaj	Tarama sonucunda oluşan bilgilendirici veya uyarı mesajıdır.

WF Sayfa Yasaklama Logları

WF (Web Filtreleme) Sayfa Yasaklama Logları, kullanıcıların erişmeye çalıştığı ancak filtre politikaları nedeniyle engellenen web sayfalarını kaydeder. Bu rapor, yasaklanan içeriklerin ne zaman, kim tarafından ve hangi kategoriye göre engellendiğini göstererek içerik denetimi ve kullanıcı kontrolü sağlar.

WF Sayfa Yasaklama Raporları

Raporlara Dön

CSVPDFXLSHTML

Sayfa Sayı50Kayıt GösterGöster/GösterSıra SıralamaFiltreleme

#	Zaman Damgası	İşlem	Kullanıcı	İstemci IP Adresi	WF Profili	Kategori	HTTP Metodu	URL
1	2025-04-30 13:13:04	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	Varsayilan Izini	GET ip4+host	https://dsc001.prod.do.dsp.mi.microsoft.com/v2/comen0a6f7c9a9d56eeefcd46f20d3cf0a40cbb1878...
2	2025-04-30 13:13:04	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	184.28.154.41:443
3	2025-04-30 13:13:03	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	184.28.154.41:443
4	2025-04-30 13:12:55	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	184.28.153.210:443
5	2025-04-30 13:12:50	PASS	-	#####	Varsayilan Izini	GET hostname	http://www.microsoft.com/pki/certs/MicRoCerAut2011_2011_03_22.crt	
6	2025-04-30 13:12:50	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	52.168.117.70:443
7	2025-04-30 13:12:46	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	184.28.154.41:443
8	2025-04-30 13:12:36	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	2.22.114.43:443
9	2025-04-30 13:12:36	PASS	-	#####	Varsayilan Izini	GET hostname	http://www.microsoft.com/pkips/certs/Microsoft%20ECN%20Product%20Root%20Certificate%20Authority%202018.crt	
10	2025-04-30 13:12:36	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	52.149.43.87:443
11	2025-04-30 13:11:55	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	195.181.174.173:443
12	2025-04-30 13:10:23	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	150.171.27.10:443
13	2025-04-30 13:10:06	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	89.238.73.97:443
14	2025-04-30 13:10:06	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	89.238.73.97:443
15	2025-04-30 13:09:55	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	57.129.19.230:443
16	2025-04-30 13:09:50	PASS	192.168.2.102	192.168.2.102	varsayilan - Genel Web Filtreleme Politikasi	IP Adresi	CONNECT ip4+host	20.199.58.43:443

AV, ApplD, IPS, DoS Logları

Raporlara Dön

#	Zaman Damgası	İşlem	Karar	Protokol	Kaynak Kullanıcı Adı	Kaynak Adres	Kaynak Port	Hedef Kullanıcı Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	ApplD	Kural	Açıklama	Sistem	Kayıt ID	QoS Bilgisi
1	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
2	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
3	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	
4	2022-10-19 09:29:44.989636	alert	allow	ARP							vmx1 - DMZ1 (inline)	0		(arp_spoof) ethernet/ARP mismatch request for source		ips	serviskontrol	

Göster/Gizle butonu ile sütunlar gizlenip, gizlenen sütunlar tekrar gösterilebilmektedir. Yukarı aşağı ok butonları ile aynı zamanda sütunların yeri de değiştirilebilmektedir.

WF Sayfa Yasaklama Raporları

Raporlara Dön

#	Zaman Damgası	İşlem	Kullanıcı	İstemci IP Adresi	WF Politikası	Kategori	HTTP Metodu	URL
1	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singletile/su
2	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singletile/su
3	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singletile/su
4	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
5	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
6	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
7	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/iv
8	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/iv
9	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/iv
10	2020-10-06 10:43:16	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today/market=tr-
11	2020-10-06 10:43:16	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today/market=tr-

Aşağıdaki ekran görüntüsünde sırala simgesine tıkladığımızda sütundaki değerlere göre tüm tablo sıralanmış olacaktır.

SSH Koruma Raporları

Raporlara Dön

#	Zaman Damgası	İşlem	IP Adresi
1	2020-10-06 15:48:15	release	10.10.99.10
2	2020-10-06 15:45:32	block	10.10.99.10

SSH Koruma Raporları

Raporlara Dön

#	Zaman Damgası	İşlem	IP Adresi
1	2020-10-06 15:45:32	block	10.10.99.10
2	2020-10-06 15:48:15	release	10.10.99.10

Sıralamada bulunan yukarı aşağı ok butonları ile sütun sıralama önceliğini değiştirebilirsiniz.

#	Zaman Damgası	İşlem	IP Adresi
1	2020-10-06 15:45:32	block	10.10.99.10
2	2020-10-06 15:48:15	release	10.10.99.10

Sıralamada bulunan çöp simgesine sahip butonlar ile sütuna ait sıralama filtresini kaldırabilirsiniz.

#	Zaman Damgası	İşlem	IP Adresi
1	2020-10-06 15:45:32	block	10.10.99.10
2	2020-10-06 15:48:15	release	10.10.99.10

Filtreleme butonu ile tabloda bulunan verileri belirlenen kriterlere göre filtreleyebilirsiniz.

Web Sunucu Güvenliği Raporları

Raporlara Dön

#	Zaman Damgası	İstemci	Host	İstek	Kategori	Tespit	Analiz	Önem Derecesi	Etiketler
1	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
2	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
3	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
4	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
5	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
6	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
7	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
8	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
9	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
10	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...
11	2020-10-06 10:17:17	10.10.30.10	10.10.99.11	POST /dvw/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...

Filtreleme



Zaman Damgası

Temizle

Ekle

İstemci

Temizle

Ekle

Host

Temizle

Ekle

İstek

Temizle

Ekle

Kategori

Temizle

Ekle

Tespit

Temizle

Ekle

Analiz

Temizle

Ekle

Önem Derecesi

Temizle

Ekle

Etiketler

Temizle

Ekle

Tanımları Uygula

Kriterleri girerken yanında bulunan açılır listeye göre filtreleyeceğinden, azami dikkat etmeniz gerekmektedir.

Filtreleme



Zaman Damgası

Temizle

Ekle



18.10.2022 09:44:52,728



Tarihinde



Tarihinde

Tarihinden Önce

Tarihinden Sonra

İstemci

Temizle

Ekle

A

İçeren



Filtreleme



Zaman Damgası

Temizle

Ekle



18.10.2022 09:44:52,728



Tarihinde



İstemci

Temizle

Ekle

A

İçeren



İçeren

İle Başlayan

İle Biten

Tam Olarak

Virgülle Ayrılmış

Host

Temizle

Ekle

A

Etiketler

Temizle

Ekle

Kapsanan

Kapsanan

Kapsayan

Tam Olarak

İçeren

Uygula

Tablo için gereken filtreler girildikten sonra **Tanımları Uygula** butonuna basılmalıdır.

Filtreleme

Zaman Damgası

Temizle

Ekle

18.10.2022 09:44:52,728

Tarihinden Önce

İstemci

Temizle

Ekle

Host

Temizle

Ekle

İstek

Temizle

Ekle

Kategori

Temizle

Ekle

Tespit

Temizle

Ekle

Analiz

Temizle

Ekle

Önem Derecesi

Temizle

Ekle

Etiketler

Temizle

Ekle

Tanımları Uygula

Tablo için yapılan filtrelemeleri kaldırmak için silgi simgesi olan butona tıklamanız yeterli olacaktır.

WF Sayfa Yasaklama Raporları

Raporlara Dön

CSV PDF XLS HTML

Sayfa Bp: 50 Kayıt Göster Göster/Gizle Sıralama Filtreleme

#	Zaman Damgası	İşlem	Kullanıcı	İstemci IP Adresi	WF Politikası	Kategori	HTTP Metodu	URL
1	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=sports
2	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=sports
3	2020-10-06 11:00:15	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=sports
4	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
5	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
6	2020-10-06 10:56:47	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://kurumsal.turk.net/
7	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/livesite/preinstall?region=TR&appid=C98EASB0842DB89405BBF071E1DA76512D21FE36&FORM=Threshold
8	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/livesite/preinstall?region=TR&appid=C98EASB0842DB89405BBF071E1DA76512D21FE36&FORM=Threshold
9	2020-10-06 10:45:18	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://tile-service.weather.microsoft.com/tr-TR/livesite/preinstall?region=TR&appid=C98EASB0842DB89405BBF071E1DA76512D21FE36&FORM=Threshold
10	2020-10-06 10:43:16	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=news
11	2020-10-06 10:43:16	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=news
12	2020-10-06 10:43:16	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://cdn.content.prod.cms.msn.com/singlestore/summary/alias/experiencebyname/today/market=tr-TR&source=appxmanifest&tenant=amp&vertical=news
13	2020-10-06 10:43:01	PASS	16211717590	10.10.30.10	Genel Web Filtreleme Politikası	Varsayılan İzinli	GET	http://fast.com/

Tabloya yeni gelen deęerleri g rmek i in yenile butonuna butonuna basılmalıdır.

AV, AppID, IPS, DoS Logları

Raporlara D n

CSVPDFXLSHTML

Sayfa Başı50Kayıt G sterG ster/GizleSıralamaFiltreleme

<

Raporlara D n butonu ile dinamik raporlar men s ne geri d nebilir, ba ka raporlara g z atabilirsiniz.

Web Erişim Raporları

Raporlara Dön

CSVPDFXLSHTML

Sayfa Bapı50Kayıt GösterGöster/GizleSıralamaFiltreleme

#	Tarih Saat	İstemci IP Adresi	İstemci Portu	İstemci Mac Adresi	Kullanıcı Adı	Sunucu IP Adresi	Alan Adı	Adres	SSL SNI	HTTP Metodu	HTTP Kodu	İçerik	Tüketim	Geçen Süre	Başlangıç Zamanı	Bitiş Zamanı
1	2020.10.06 07:10	10.10.30.10	50679	00:0c:29:fb:aad8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:56.000	2020.10.06 07:10:56.007
2	2020.10.06 07:10	10.10.30.10	50678	00:0c:29:fb:aad8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.008	2020.10.06 07:10:53.000	2020.10.06 07:10:53.008
3	2020.10.06 07:10	10.10.30.10	50645	00:0c:29:fb:aad8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.016	2020.10.06 07:10:14.000	2020.10.06 07:10:14.016
4	2020.10.06 07:10	10.10.30.10	50680	00:0c:29:fb:aad8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:56.000	2020.10.06 07:10:56.007
5	2020.10.06 07:10	10.10.30.10	50681	00:0c:29:fb:aad8		10.10.99.1	www.aliexpress.com	10.10.99.1:8801	www.aliexpress.com	CONNECT	200		2293	00:00:00.008	2020.10.06 07:10:56.000	2020.10.06 07:10:56.008
6	2020.10.06 07:10	10.10.30.10	50676	00:0c:29:fb:aad8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		1268	00:00:00.007	2020.10.06 07:10:47.000	2020.10.06 07:10:47.007
7	2020.10.06 07:10	10.10.30.10	50660	00:0c:29:fb:aad8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		2293	00:00:00.009	2020.10.06 07:10:25.000	2020.10.06 07:10:25.009
8	2020.10.06 07:10	10.10.30.10	50663	00:0c:29:fb:aad8		10.10.99.1	www.n11.com	10.10.99.1:8801	www.n11.com	CONNECT	200		156	00:00:00.002	2020.10.06 07:10:34.000	2020.10.06 07:10:34.002
9	2020.10.06 06:10	10.10.30.10	49683	00:0c:29:fb:aad8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.042	2020.10.06 06:10:50.000	2020.10.06 06:10:50.042
10	2020.10.06 06:10	10.10.30.10	49823	00:0c:29:fb:aad8		10.10.99.1	www.bing.com	10.10.99.1:8801	www.bing.com	CONNECT	200		1268	00:00:00.049	2020.10.06 06:10:34.000	2020.10.06 06:10:34.049
11	2020.10.06 05:10	10.10.30.10	52288	00:0c:29:fb:aad8		10.10.99.1	www.hepsiburada.com	10.10.99.1:8801	www.hepsiburada.com	CONNECT	200		1268	00:00:00.009	2020.10.06 05:10:49.000	2020.10.06 05:10:49.009

Not: Yasaklanan Kullanıcılar Loglarına d  mesi i in;

- Log Ayarları'nda Aray ze Eri imi Yasaklanan IPler Log  e idinin Cihazda Tut se ili olması gerekir.

Http(s) Sunucu Yönlendirme Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Web Erişim Logları	☒ Cihazda Tut ☐ Cihazda Tutma
SSH ve Konsol Oturum Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Karadeli Servisi Logları	☒ Cihazda Tut ☐ Cihazda Tutma
VPN - SSL VPN Logları	☒ Cihazda Tut ☐ Cihazda Tutma
VPN - PPTP / L2TP Logları	☒ Cihazda Tut ☐ Cihazda Tutma
RADIUS Logları	☒ Cihazda Tut ☐ Cihazda Tutma
VPN - IPsec VPN Logları	☒ Cihazda Tut ☐ Cihazda Tutma
DHCP Olay Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Web Oturum Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Web Arayüzü Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Hotspot Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Cluster Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Web Filtreleme - İçerik ve Antivirüs Tarama Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Antispam Logları	☒ Cihazda Tut ☐ Cihazda Tutma
SSH Koruma Servisi Logları	☒ Cihazda Tut ☐ Cihazda Tutma
Arayüze Erişimi Yasaklanan IPler	☒ Cihazda Tut ☐ Cihazda Tutma

- Erişim / Oturum Ayarları'nda Trafiği Logla seçeneğinin aktifleştirilmesi gerekir.

Oturum Ayarları

Trafiği Logla ☒ Açık ☐

Sertifika Bazlı Kimlik Doğrulama ☐ Kapalı ☒

Harici Kaynaklardan Kimlik Doğrulama ☐ Kapalı ☒

Eş Zamanlı Oturum Açma ☒ Açık ☐

Çalışma Modu Kısıtlı Erişim

Giriş Feragatnamesi ☐ Kapalı ☒

SSH Karşılama Ekran Durumu ☐ Kapalı ☒

Kaydet

- Bu ayarların yapılmadığı durumda ürün Common Criteria EAL4+ sertifika kapsamından çıkmaktadır.

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

