

epati



















Dinamik Raporlar

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

Dinamik Raporlar

18 farklı rapor çeşidi dinamik olarak buradan görüntülenmekte ve listelenmektedir.

- Anti Spam Raporları
- Cluster Raporları
- DNS Filtreleme Raporları
- Hotspot Logları
- IPsec Servis Raporları
- Paket Filtreleme Raporları
- PPP Debug Logları
- PPP Raporları
- AV, AppID, IPS, DoS Logları
- SSH Denetimi Raporları
- SSH Koruma Raporları
- Trafik Oturum Raporları
- Sanal Kablo Raporları
- Web Erişim Raporları
- Web Sunucu Güvenliği Raporları
- WF (Web Filtreleme) İçerik ve Antivirüs Tarama Raporları
- WF (Web Filtreleme) Sayfa Yasaklama Raporları
- Yasaklanan Kullanıcılar Raporları

 Anti Spam Raporları	 Cluster Raporları	 DNS Filtreleme Raporları
 Hotspot Logları	 IPsec Servis Raporları	 Paket Filtreleme Raporları
 PPP Debug Logları	 PPP Raporları	 AV, AppID, IPS, DoS Logları
 SSH Denetimi Raporları	 SSH Koruma 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

Cluster Raporları

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

Cluster Raporları

[← Raporlara Dön](#)[CSV](#) [PDF](#) [XLS](#) [HTML](#)

Sayfa Başı 50

Kayıt Göster

Göster/Gizle

Sıralama

Filtreleme

#	Zaman Damgası	İşlem	Son Görev	Önceki Görev	Açıklama	Detaylar
1	2022-10-19 09:29:47.385494+03	Görev Değiştirdi	AKTIF	PASIF	Diğer cihaz PASIF olduğu için...	{\"Yerel Cihaz Bilgileri\": {\"gorev\": \"AKTIF\", \"ipAdresi\": \"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}, \"kabloTakiliOlmayanEthSayisi\": 0}, \"aktiflikUptime\": 2325}, \"Diğer Cihaz Bilgileri\": {\"gorev\": \"PASIF\", \"ipAdresi\": \"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}, \"kabloTakiliOlmayanEthSayisi\": 0}, \"aktiflikUptime\": -1}}

Kullanıcılar bu raporları [csv](#), [pdf](#), [xls](#) ve [html](#) formatlarında indirebilmektedir.

PPP Debug Logları

[← Raporlara Dön](#)[CSV](#) [PDF](#) [XLS](#) [HTML](#)

Sayfa Başı 50

Kayıt Göster

Göster/Gizle

Sıralama

Filtreleme

#	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

Her sayfada kaç kayıt gösterileceği [Sayfa Başı](#)ndan sonra değer girilip, kayıt göster butonuna basıldığında; sayfa başı kullanıcının girdiği değer kadar veri gösterilir. (Varsayılan 50 olarak gelmektedir.)

AV, AppID, IPS, DoS Logları

[← Raporlara Dön](#)[CSV](#) [PDF](#) [XLS](#) [HTML](#)

Sayfa Başı 50

Kayıt Göster

Göster/Gizle

Sıralama

Filtreleme

#	Zaman Damgası	İşlem	Karar	Protokol	Kaynak Kullanıcı Adı	Kaynak Adres	Kaynak Port	Hedef Kullanıcı Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	AppID	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-TR&source=appxmanifest&tenant=amp&vertical=s
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-TR&source=appxmanifest&tenant=amp&vertical=s
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-TR&source=appxmanifest&tenant=amp&vertical=s
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/ivivite/preinstall?region=TR&appid=C98EA5B0842DBB94058BF071E1DA76512D21FE368&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/ivivite/preinstall?region=TR&appid=C98EA5B0842DBB94058BF071E1DA76512D21FE368&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/ivivite/preinstall?region=TR&appid=C98EA5B0842DBB94058BF071E1DA76512D21FE368&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/singletile/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/singletile/summary/alias/experiencebyname/today/market-tr-TR&source=appxmanifest&tenant=amp&vertical=news

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

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	

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.

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 çöp simgesine sahip butonlar ile sütuna ait sıralama filtresini kaldırabilirsiniz.

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

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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/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 /dwwa/vulnerabilities/x...	REQUEST-APPLICATION-ATTACK-XSS	XSS Attack Detected via libinjection	Matched Data: XSS data fou...	2	application-multi, language...

Filtreleme

X

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

A

İçeren

Filtreleme



Zaman Damgası

Temizle + Ekle

18.10.2022 09:44:52,728

Tarihinde

İstemci

A

İçeren

İçeren

İle Başlayan

İle Biten

Tam Olarak

Virgüle Ayrılmış

Host

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 ! Temizle

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 Bgı 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/singlefile/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/singlefile/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/singlefile/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/livestile/preinstall?region=TR&appid=C98EA5B0842DB89405BBF071E1DA76512D21FE36&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/livestile/preinstall?region=TR&appid=C98EA5B0842DB89405BBF071E1DA76512D21FE36&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/livestile/preinstall?region=TR&appid=C98EA5B0842DB89405BBF071E1DA76512D21FE36&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/singlefile/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/singlefile/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/singlefile/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://f1est.com/

Tabloya yeni gelen değerleri görmek için yenile butonuna butonuna basılmalıdır.

#	Zaman Damgası	İşlem	Karar	Protokol	Kaynak Kullanıcı Adı	Kaynak Adres	Kaynak Port	Hedef Kullanıcı Adı	Hedef Adres	Hedef Port	Ağ Arayüzü	VLAN	AppID	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		

Raporlara Dön butonu ile dinamik raporlar menüsüne geri dönebilir, başka raporlara göz atabilirsiniz.

Web Erişim Raporları

Raporlara Dön

#	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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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:aa:d8		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 Kullanıcı Raporlarına log düşmesi için;

- Log Ayarlarında Arayüze Erişimi Yasaklanan Ipler Log çeşidinin Cihazda Tut seçili olması gerekir.

Http(s) Sunucu Yönlendirme 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
SSH ve Konsol Oturum 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
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
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
Web Arayüzü 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
Cluster Logları	<input checked="" type="checkbox"/> Cihazda Tut <input type="checkbox"/> Cihazda Tutma
Web Filtreleme - İçerik ve Antivirüs Tarama Logları	<input checked="" type="checkbox"/> Cihazda Tut <input type="checkbox"/> Cihazda Tutma
Antispam Logları	<input checked="" type="checkbox"/> Cihazda Tut <input type="checkbox"/> Cihazda Tutma
SSH Koruma Servisi Logları	<input checked="" type="checkbox"/> Cihazda Tut <input type="checkbox"/> Cihazda Tutma
Arayüze Erişimi Yasaklanan İpler	<input checked="" type="checkbox"/> Cihazda Tut <input type="checkbox"/> Cihazda Tutma

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

Oturum Ayarları

Trafik Logla Kapalı

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

- 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

