

FastNAC



CİHAZ PROFİLLEME

İçindekiler;

1. Başlangıç.....	3
2. Profil Ekleme.....	4
3. Profil Detay Sayfası.....	5
4. Profil Kuralı Ekleme.....	6
5. Profil Kural Tipleri.....	7
5.1. MAC Bilgisine Göre.....	7
5.1.1. MAC Adresi.....	7
5.1.2. MAC Üretici Bilgisi.....	7
5.2. IP Adresine Göre.....	8
5.3. Lokasyona Göre.....	9
5.3.1. Lokasyon Bilgisi.....	9
5.3.2. Switch/Port Bilgisi.....	10
5.4. Domain Kontrolü.....	10
5.4.1. Domain Cihaz Kontrolü.....	11
5.4.2. Domain Kullanıcı Kontrolü.....	11
5.5. Active Directory.....	12
5.6. HTTP/HTTPS.....	12
5.7. Telnet/SSH.....	14
5.7.1. Telnet.....	15
5.7.2. SSH.....	16
5.8. DHCP Fingerprint.....	17
5.8.1. Üretici Bilgisi.....	17
5.8.2. Cihaz Adı (Hostname).....	17
5.8.3. Parametreler.....	18
5.9. TCP/UDP Port.....	18
5.10. SNMP.....	19
5.11. Posture.....	19
5.11.1. Windows.....	20
5.11.1.1. İşletim Sistemi Kontrolü.....	20
5.11.1.2. Program Kontrolü.....	21
5.11.1.2.1. Program Adı.....	21
5.11.1.2.2. Program Versiyonu.....	22
5.11.1.3. Servis Kontrolü.....	22
5.11.2. Linux.....	23
5.11.2.1. İşletim Sistemi Kontrolü.....	23
5.11.2.2. Program Kontrolü.....	24
5.11.2.2.1. Program Adı.....	24
5.11.2.2.2. Program Versiyonu.....	25

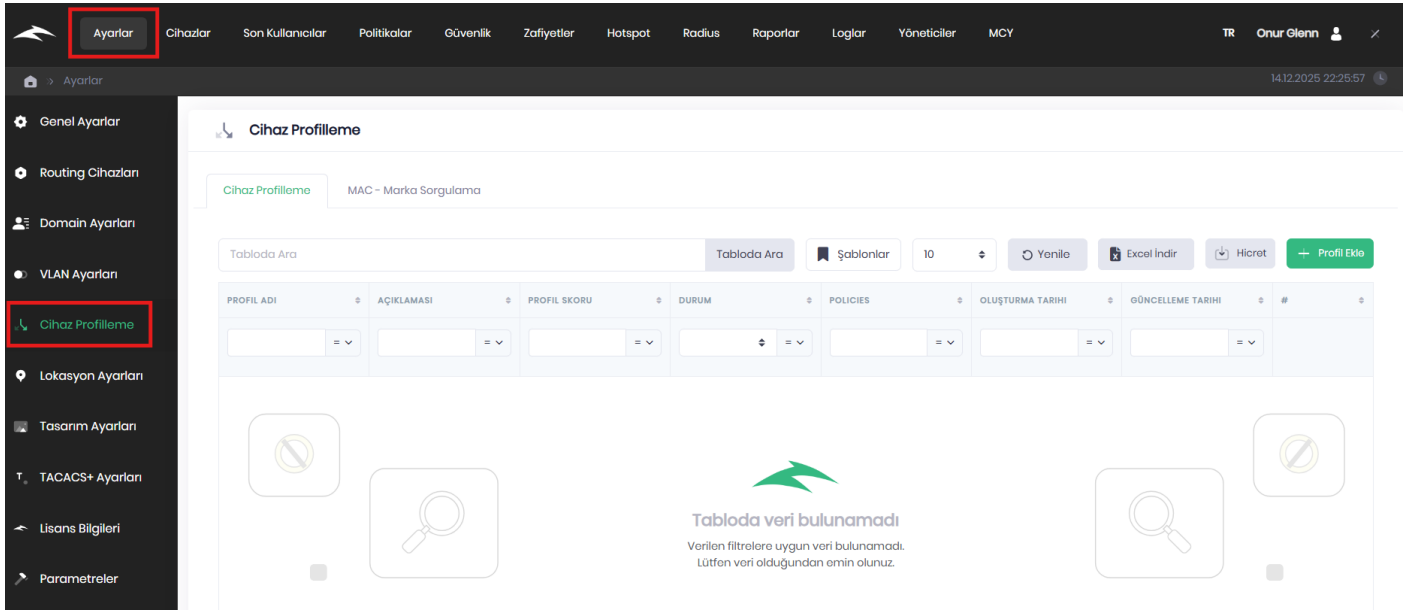
5.11.2.3. Servis Kontrolü.....	25
5.11.3. Dosya Takibi.....	26
5.11.4. Oturum Takibi.....	26
5.12. NMAP.....	27
6. Profil ve Skor Sistemi ve Örnekler.....	27
6.1. Örnek IP_Kamera Profili.....	28
6.2. Örnek Yazıcı Profili.....	30
6.3. Örnek IoT Cihaz Profili.....	33

1. Başlangıç

FastNAC ile Network üzerinde bulunan IoT veya benzer cihazları, bir çok profillemeye yöntemini aynı anda kullanarak sınıflandırma yapabilirsiniz. Cihazları;

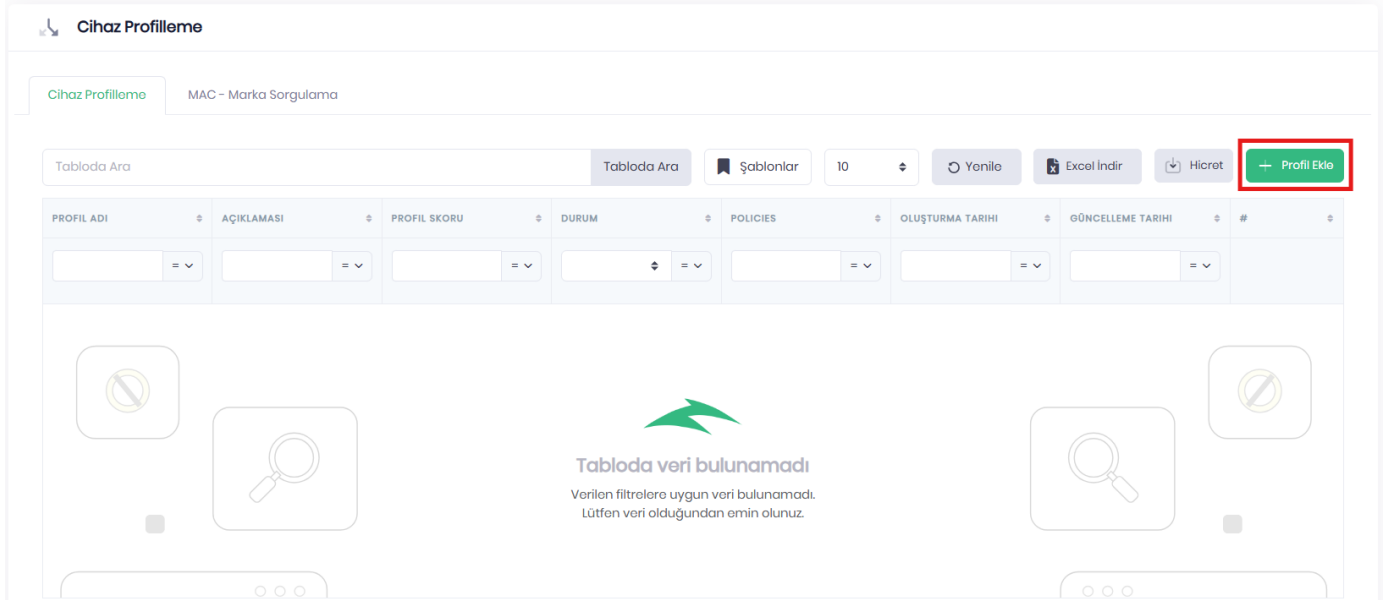
- MAC adresleri veya MAC üretici bilgisine göre,
- IP Adresi veya IP Bloklarına göre,
- Lokasyonuna veya Switch/Port bilgisine göre,
- Active Directory Öz Niteliklerine göre,
- HTTP/HTTPS yöntemi ile tarama yapıp içeriğe,
- Telnet/SSH ile komut çalıştırıp çıktısına göre,
- DHCP Fingerprint;
 - Üretici bilgisine göre,
 - Ana makine adına (hostname) göre,
 - Fingerprint parametrelerine göre
- TCP/UDP açık/kapalı/filtreli port durumlarına göre,
- SNMP isteği atarak gelen cevaba göre,
- Windows işletim sistemi için;
 - İşletim sistemi kontrolüne göre,
 - Windows içinde yüklü veya yüklü olmayan programa göre,
 - Windows içinde yüklü olan programın versiyon bilgisine göre,
 - Windows içinde çalışan/çalışmayan servislerin duruma göre,
- Linux işletim sistemi için;
 - İşletim sistemi kontrolüne göre,
 - Linux içinde yüklü veya yüklü olmayan programa göre,
 - Linux içinde yüklü olan programın versiyon bilgisine göre,
 - Linux içinde çalışan/çalışmayan servislerin duruma göre,
- İşletim sistemi içinde bulunan bir dosyanın yoluna göre,
- Oturum açılma süresine göre,
- NMAP taraması (özel parametreler kullanabilirsiniz) ile çıkan sonuca göre,

vb. yöntemleri kullanarak sınıflandırabilirsiniz. Cihaz Profillemeye ayarlarına; **Ayarlar** -> **Cihaz Profillemeye** menüsü altından ulaşabilirsiniz.



2. Profil Ekleme

Cihaz Profilleme ekranında bulunan “Profil Ekle” butonuna basarak yeni bir profil oluşturabilirsiniz.



Açılan pencerede;

Profil Ekle

Adı: *

IoT_Enerji

Açıklama:

Toplam Eşik Değeri: *

10

İptal Et

Ekle

Oluşturmak istediğiniz profilin Adını, Açıklamasını (opsiyonel) ve Toplam Eşik Değeri Puanını belirtmelisiniz. Profili oluşturduğunuzda otomatik olarak detay sayfasına yönlendirileceksiniz.

Önemli: Toplam Eşik Değeri Puanı, profilin içine eklenecek kuralların toplam puanını ifade etmektedir. Burada vereceğiniz puan profilin içine eklenen kurallara verdiğiniz puanların toplamı olmalıdır. “1.6) Profil Skor Sistemi ve Örnekler” konusunda bu bölüm daha detaylı anlatılmaktadır.

3. Profil Detay Sayfası

Profil detay sayfasına sağ üstte bulunan “Profil Düzenle” butonunu kullanarak ilgili profili düzenleyebilirsiniz;

IoT_Enerji

Listeye Dön

Profil Düzenle

Profil Kaldır

Adı: IoT_Enerji

Açıklama: -

Profil Skoru: 10

Durumu: Aktif

Oluşturma Tarihi: 12/14/2025, 10:41:11 PM

Güncelleme Tarihi: -

Tabloda Ara

Tabloda Ara

Şablonlar

10

Yenileme kapalı

Yenile

Kural Ekle

ADI	EŞİK DEĞERİ	DURUMU	OLUŞTURMA TARİHİ	GÜNCELLEME TARİHİ	#

Tabloda veri bulunamadı

Verilen filtrelere uygun veri bulunamadı. Lütfen veri olduğundan emin olunuz.

İlk

Önceki

1

Sonraki

Son

Toplam / Filtrelenmiş Sonuç: 0 / 0

10

Düzenleme ekranında Profilin Adını, Açıklamasını veya Toplam Eşik Değeri Puanını değiştirebilirsiniz.

4. Profil Kuralı Ekleme

Profil detay sayfasının sağında bulunan “Kural Ekle” butonuna basarak yeni bir kural ekleyebilirsiniz;

The screenshot shows the 'IoT_Enerji' profile page. On the left, there's a sidebar with profile details: Adı: IoT_Enerji, Açıklama: -, Profil Skoru: 10, Durumu: Aktif, Oluşturma Tarihi: 12/14/2025, 10:41:11 PM, Güncelleme Tarihi: -. On the right, there's a table with columns: ADI, EŞİK DEĞERİ, DURUMU, OLUŞTURMA TARİHİ, GÜNCELLEME TARİHİ, and #. The table is empty, and a message says 'Tabloda veri bulunamadı. Verilen filtrelere uygun veri bulunamadı. Lütfen veri olduğundan emin olunuz.' The 'Kural Ekle' button is highlighted in red in the top right corner.

Kural eklerken;

The 'Kural Ekle' form has the following fields: Adı (with a red error message: 'İsim boş bırakılamaz. Lütfen kontrol ediniz.'), Puanı, Durumu (dropdown), and Kural tipi (dropdown). At the bottom, there are two buttons: 'İptal Et' and 'Kural Ekle'.

Adı: Kural'a verebileceğiniz özel bir isim

Puanı: İlgili kuralın puanı (Profil skorunu etkiler)

Durumu: Kuralın aktif/pasif durumu

Kural Tipi: Profillemeye sınıfı

bilgilerini girerek yeni bir kural seti oluşturabilirsiniz.

Not: Kural tipini seç belirlediğinizde ilgili ekranda seçtiğiniz kural tipi için ekstra inputlar çıkmaktadır. Bunlar Kural Tipleri bölümünde anlatılmaktadır.

5. Profil Kural Tipleri

5.1. MAC Bilgisine Göre

Kural tipi olarak “**MAC Adresi**” seçildiğinde;

Kural tipi	MAC Adresi
Tipi	MAC Adresi Üretici

MAC adresinin kendisi veya üretici bilgisine göre profil kuralı oluşturabilirsiniz.

5.1.1. MAC Adresi

Kural tipi olarak MAC adresi seçildiğinde;

Tipi	MAC Adresi
MAC Adresi	? Kullanım Biçimleri 01:aa:02:bb:03:cc - 01:aa:02:*

MAC adresinin tamamını veya :* regexini kullanarak ile başlıyorsa şeklinde kural oluşturabilirsiniz. Örneğin;

- Network'e erişmeye çalışan cihazın MAC adresi 01:aa:02:bb:03:cc ise
- Network'e erişmeye çalışan cihazın MAC adresi 01:aa:02:* ile başlıyorsa

şeklinde kural tanımı yapabilirsiniz.

5.1.2. MAC Üretici Bilgisi

MAC üretici bilgisi tipinde;

Kural tipi	MAC Adresi
Tipi	Üretici
Üretici	
Kelime İçeriği	İçeriyorsa

“Üretici” bilgisi girildikten sonra girdiğiniz “**Kelime İçeriği**” “**Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa**” alt kural bilgisi seçilir. Örneğin üretici bilgisi olarak “**samsung**” ve kelime içeriği “**içeriyorsa**” seçildiğinde;

- Network’e erişmeye çalışan cihazın MAC üretici bilgisi “**samsung**” içeriyorsa şeklinde kural tanımı yapabilirsiniz.

5.2. IP Adresine Göre

Kural tipi olarak “**IP adresi**” seçildiğinde;

Kural Ekle

Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

IP_ADRES

Puanı

5

Durumu

Aktif

Kural tipi

IP Adresi

IP Adresi

?

Kullanım Biçimleri

192.168.1.0 - 192.168.1.0/24 - 192.168.1.* - 192.168.*.* - 192.168.*.[1-10] - 192.168.[1-5].[1-10]

<

İptal Et

Kural Ekle

Network’e bağlanana cihazın IP adresinin tamamı, IP bloğu, IP adresinin son oktet, IP adresinin son iki oktet, IP adres aralıklarına göre kural tanımlaması yapılabilir. Örneğin;

- Network’e erişmeye çalışan cihazın IP adresi 192.168.1.10 ise,
- Network’e erişmeye çalışan cihazın IP adresi 192.168.1.0/24 ip bloğu içindeyse,
- Network’e erişmeye çalışan cihazın IP adresi 192.168.1. ile başlayıp 4.oktetinde herhangi bir rakam geliyorsa (Maksimum 254) (192.168.1.*),
- Network’e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp son 3. ve 4. oktetinde herhangi bir rakam geliyorsa (Maksimum 254) (192.168.*.*),
- Network’e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp 3.oktetinde herhangi bir rakam (Maksimum 254) ile başlayıp [1-10] arasında bir ip adresi alıyorsa (192.168.*.[1-10])
- Network’e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp 3.oktetinde [1-5] arasında bir rakam alıyorsa ve 4.oktetinde [1-10] arasında bir ip adresi alıyorsa (192.168.[1-5].[1-10])

Rakort
Bilgi ve İletişim Teknolojileri

Rakort.com

info@rakort.com

0850 460 10 58

Mustafa Kemal Mah. 2139 Cad.
Ekim Plaza No: 2 Kat: 3 Daire: 16

Çankaya / Ankara

şeklinde kural tanımları yapabilirsiniz.

Not: IP adresi tipinde kuralın eşleşebilmesi için networke bağlanan cihazın IP adresi almış olması gerekmektedir.

5.3. Lokasyona Göre

Kural tipi olarak “**Lokasyon**” seçildiğinde;

 Kural Ekle 

Adı

 İsim boş bırakılamaz. Lütfen kontrol ediniz.

Puanı

Durumu

Kural tipi

Tipi

Lokasyon Bilgisi

Switch/Port Bilgisi

 İptal Et

 Kural Ekle

5.3.1. Lokasyon Bilgisi

Lokasyon tipinde;

Kural tipi

Tipi

Lokasyon

B_Lokasyonu

Genel

A_Lokasyonu

 İptal Et

 Kural Ekle

FastNAC üzerinde oluşturulan lokasyonları seçerek kural tanımlı yapabilirsiniz.

5.3.2. Switch/Port Bilgisi

Switch/Port Bilgisi Tipinde;

Kural tipi	Lokasyon
Tipi	Switch/Port Bilgisi
Switch	 Switch bilgisi ip adresi olmalıdır. Örneğin: 192.168.1.10
Port	 Port bilgisi interface description olarak girmeniz gerekmektedir. Örneğin: GigabitEthernet/0/1

Inputlara yazılan Switch/Port bilgisine göre kural tanımını yapabilirsiniz.

5.4. Domain Kontrolü

Kural tipi olarak “**Domain Kontrolü**” seçildiğinde;

 Kural Ekle ×

 Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı	 ⓘ İsim boş bırakılamaz. Lütfen kontrol ediniz.
Puanı	0
Durumu	
Kural tipi	Domain Kontrolü
Durumu	 Domaindeki Cihazlar

← İptal Et Kural Ekle

5.4.1. Domain Cihaz Kontrolü

Varsayılan olarak gelen profil tipidir.

Kural tipi	Domain Kontrolü
Durumu	Domaindeki Cihazlar
Tipi	Domain Cihaz Kontrolü Domain Kullanıcı Kontrolü

[← İptal Et](#)[Kural Ekle](#)

Parametre ayarlarına göre cihazınların domain kontrolünü sağlayan profildir.

5.4.2. Domain Kullanıcı Kontrolü

Domain Kullanıcı Kontrolü tipinde;

Kural tipi	Domain Kontrolü
Durumu	Domaindeki Cihazlar
Tipi	Domain Kullanıcı Kontrolü
Kullanıcı Adı	
Oturum Kontrolü	☒ Açık
Kaç Cihazda Oturum Açabilir	

[← İptal Et](#)[Kural Ekle](#)

Domainde olan kullanıcılara özel profil tanımlı yapabilirsiniz. Ayrıca kullanıcının kaç cihazda oturum açabileceğini “**Oturum Kontrolü**” ayarını açarak belirleyebilirsiniz. Örneğin;

- Network’e erişmeye çalışan cihazda “**onur**” kullanıcısı oturum açmışsa ve eğer oturum kontrolü açıksa ve herhangi bir cihazda 2.oturumu açmışsa (Kural tanımına uyması için inputun içine 3 yazılması gerekmektedir.)

şeklinde kural tanımlı yapabilirsiniz.

5.5. Active Directory

Kural tipi olarak “**Active Directory**” seçildiğinde;

Kural tipi	Active Directory
Attribute Adı	
Değer	
Kelime İçeriği	Eşitse
	Eşitse
	İçeriyorsa
	ile Başlıyorsa
	ile Bitiyorsa

[← İptal Et](#)

Active Directory kullanıcıları üzerinde bulunan Özniteliklere göre (Custom Attribute) profil tanımlı yapabilirsiniz. Öznitelik(Attribute) adı, Active Directory üzerinde bulunan öznitelik ismiyle aynı olmalıdır. Karşılığındaki değere göre kural tanımlı belirleyebilirsiniz. Örneğin;

Attribute Adı: **department**

Değer: **Bilgi İşlem**

Kelime İçeriği: **Eşitse**

- Network'e erişmeye çalışan cihazda “**onur**” kullanıcısı oturum açmışsa ve “**onur**” kullanıcısının department özniteliği “**Bilgi İşlem**” yazısına eşitse

şeklinde kural tanımlı yapabilirsiniz.

5.6. HTTP/HTTPS

Kural tipi olarak “**HTTP/HTTPS**” seçildiğinde ilgili cihazın eğer web arayüzü varsa (80/443), arayüzü tarayıp içeriğinde geçen kelimelere göre profil tanımlaması yapabilirsiniz.

Kural tipi

HTTP/HTTPS

URL

Portu URL üzerinden belirtilebilirsiniz. Örneğin: https://192.168.1.10:6000

Değer

Kelime İçeriği

Giriş Ekranı



URL: Eğer profillemek istediğiniz cihazın özel bir URL adresi varsa buraya girebilirsiniz. Eğer yoksa “/” girmeniz yeterli olacaktır.

Değer: Web arayüz tarandıktan sonra aranmak istenen değer buraya girilir.

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Giriş Ekranı: Açık/Kapalı

Taranmak istenen web arayüzüne Kullanıcı Adı ve Şifre ile giriş yapıldıktan sonra işlemlere devam edilmesi gerekiyorsa “Giriş Ekranı” bölümünü açıp aşağıdaki ayarları yapabilirsiniz;

Giriş Ekranı



Giriş URL

Kullanıcı Adı

Şifre

Basic Auth



Payload Kullanıcı

Payload Şifresi

Giriş URL: Kullanıcı girişi yapılacak URL (Örneğin: login.php)

Kullanıcı Adı: Sayfaya giriş yapacak Kullanıcı Adı

Şifre: Sayfaya giriş yapacak Şifre

Basic Auth: Açık/Kapalı

Basic Authentication, HTTP protokolünde kullanılan en basit kimlik doğrulama yöntemlerinden biridir. Eğer taranmak istenen web arayüzü Basic Authentication kullanıyorsa bu ayarı açtığınızda form üzerinde bulunan Kullanıcı Adı ve Şifre kullanılarak Basic Authentication denemesi yapılır.

Eğer Basic Authentication yoksa ilgili ayar Kapalı duruma getirilir. Sayfaya giriş yapılacak kullanıcı bilgileri Payload Username ile Payload Password bölümüne yazılması gerekir.

5.7. Telnet/SSH

Kural tipi olarak **"Telnet/SSH"** seçildiğinde;

 Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

İsim boş bırakılamaz. Lütfen kontrol ediniz.

Puanı

Durumu

Aktif

Kural tipi

Telnet/SSH

Tipi

TELNET

SSH

← İptal Et

 Kural Ekle

5.7.1. Telnet

Tipi	TELNET
Port	
Timeout	
Kullanıcı Adı	
Şifre	
Komut	 Komutu belirtiniz. Örneğin: show version
Kelime	 Komut çıktısında aranacak kelimeyi belirtiniz. Örneğin: Cisco
Kelime İçeriği	İçeriyorsa

Port: Telnet port bilgisi (Varsayılan port 23'tür.)

Timeout: Bağlantı zaman aşımı süresi (Belirtilmezse 30 saniyedir)

Kullanıcı Adı: Telnet bağlantısı için gerekli kullanıcı adı

Şifre: Telnet bağlantısı için gerekli şifre

Komut: Telnet bağlantısı yapıldıktan sonra çalıştırılacak komut

Kelime: Çalıştırılan komut sonrasında aranan çıktı

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Çalışma mantığı; ilgili cihaza verilen bilgilerle telnet üzerinden erişerek belirtilen komutun çıktısı sonucunda aranan kelimeye göre kural yazabilirsiniz.

5.7.2. SSH

Kural tipi	Telnet/SSH
Tipi	SSH
Port	
Kullanıcı Adı	
Şifre	
Komut	Komutu belirtiniz. Örneğin: show version
Kelime	Komut çıktısında aranacak kelimeyi belirtiniz. Örneğin: Cisco
Kelime İçeriği	İçeriyorsa

Port: Telnet port bilgisi (Varsayılan portu 22'dir)

Timeout: Bağlantı zaman aşımı süresi (Belirtilmezse 30 saniyedir)

Kullanıcı Adı: Telnet bağlantısı için gerekli kullanıcı adı

Şifre: Telnet bağlantısı için gerekli şifre

Komut: Telnet bağlantısı yapıldıktan sonra çalıştırılacak komut

Kelime: Çalıştırılan komut sonrasında aranan çıktı

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Çalışma mantığı; ilgili cihaza verilen bilgilerle SSH üzerinden erişerek belirtilen komutun çıktısı sonucunda aranan kelimeye göre kural yazabilirsiniz.

5.8. DHCP Fingerprint

Kural tipi olarak “**DHCP Fingerprint**” seçildiğinde;

 Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

 İsim boş bırakılamaz. Lütfen kontrol ediniz.

Puanı

Durumu

Aktif

Kural tipi

DHCP Fingerprint

Tipi

Üretici Bilgisi

Hostname

Parametreler

 İptal Et

 Kural Ekle

5.8.1. Üretici Bilgisi

Kural tipi

DHCP Fingerprint

Tipi

Üretici Bilgisi

Üretici Bilgisi

DHCP Fingerprint çıktısındaki üretici bilgisine göre kural tanımlı yapabilirsiniz.

5.8.2. Cihaz Adı (Hostname)

Kural tipi

DHCP Fingerprint

Tipi

Hostname

Hostname

DHCP Fingerprint çıktısındaki cihaz adına (hostname) göre kural tanımlı yapabilirsiniz.

5.8.3. Parametreler

Kural tipi

Tipi

Parametreler [Örnekler](#)

İŞLETİM SİSTEMİ	PARAMETRELER
Windows	1,3,6,15,31,33,43,44,46,47,119,121,249,252
Pardus	1,2,6,12,15,26,28,121,3,33,40,41,42,119,249,252,17
Android 11	1,3,6,15,26,28,51,58,59,43,114,108
Apple iOS	1,121,3,6,15,108,114,119,252

DHCP Fingerprint çıktısındaki parametrelere göre kural tanımlı yapabilirsiniz.

5.9. TCP/UDP Port

Kural tipi olarak **"TCP/UDP Port"** seçildiğinde;

Kural tipi

TCP Portları

UDP Portları

Port Durumu



Kullanım Biçimleri
80 - 80,8080 - 90,50,8081-9000

İlgili cihazın yukarıda belirtilen TCP / UDP portlarının durumuna göre profil tanımlı yapabilirsiniz. Port Durumları;

- Open (Açık)
- Closed (Kapalı)
- Open Filtered (Filtreli şekilde Açık)

Port tanımlamalarını yaparken tekil olarak port numarası (Örneğin: 80), birden fazla portta tarama yapmak için aralarında virgül ile (Örneğin: 80,8080), Port aralığını aramak için de arasına tire koyarak (Örneğin: 80-8080 arası) kural tanımlamasını yapabilirsiniz.

5.10. SNMP

Kural tipi olarak “**SNMP**” seçildiğinde;

Kural tipi	SNMP
SNMP Tipi	
Port	
SNMP OID	
Değer	
Kelime İçeriği	İçeriyorsa

Belirtilen SNMP OID'inin çıktısında gelen değerın içeriğine göre profil tanımlı yapabilirsiniz. SNMPv1, SNMPv2c ve SNMPv3 desteğı sunmaktadır. SNMPv3 için kabul edilen seçenekler;

Tip olarak noAuthNoPriv, authNoPriv, authPriv desteğı sunulmaktadır.

Auth tip olarak: No Auth Protocol, MD5, SHA128, SHA256, SHA384, SHA512 desteğı sunmaktadır.

Priv tip olarak: No Priv Protocol, DES, AES 128, AES 192, AES 256 desteğı sunmaktadır.

Örneğın girilen SNMP bilgilerine göre 1.3.6.1.2.1.1.1 (SNMP sysdesrc OID) OID'ine atılan istek karşılığında eğer içeriğinde “Cisco” geçiyorsa şeklinde bir kural tanımlı yapabilirsiniz.

Not: SNMP OID'lerine internet üzerinden arama yaparak ulaşabilirsiniz.

5.11. Posture

Kural tipi olarak “**Posture**” seçildiğinde;

Kural tipi	Posture
Tipi	Windows Linux Dosya Takibi Oturum Takibi

[← İptal Et](#)

Windows, Linux, Dosya Takibi, Oturum Takibi gibi özellikleri kullanarak kural tanımları gerçekleştirebilirsiniz.

5.11.1. Windows

Kural tipi olarak “**Windows**” seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	İşletim Sistemi Kontrolü Program Kontrolü Servis Kontrolü
← İptal Et Kural Ekle	

5.11.1.1. İşletim Sistemi Kontrolü

Posture tipi olarak “**İşletim Sistemi**” Kontrolü seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	İşletim Sistemi Kontrolü
OS Versiyonu	
Tipi	Küçük Eşit Büyük
← İptal Et Kural Ekle	

İşletim sistemi versiyonu “**OS Versiyonu**” inputuna yazdığınız versiyondan “**Küçük, Eşit, Büyük**” ise şeklinde kural tanımlı yapabilirsiniz.

5.11.1.2. Program Kontrolü

Posture tipi olarak **“Program Kontrolü”** seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Adı Program Versiyonu

5.11.1.2.1. Program Adı

Alt kural tipi **“Program Adı”** olarak seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Adı
Durumu	Yüklü Yüklü Değil

“Program Adı” inputuna yazdığınız program kontrol edilen cihazda **“Yüklü”** veya **“Yüklü Değil”** şeklinde bir kural tanımı yapabilirsiniz.

5.11.1.2.2. Program Versiyonu

Alt kural tipi “**Program Versiyonu**” olarak seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Versiyonu
Versiyon	
Tipi	Küçük Eşit Büyük
← İptal EtKural Ekle	

“**Program Adı**” inputuna yazılan programın versiyonu “**Versiyon**” inputuna yazacağınız değerden “**Küçük, Eşit, Büyük**” şeklinde kural tanımı yapabilirsiniz.

5.11.1.3. Servis Kontrolü

Posture tipi olarak “**Servis Kontrolü**” seçildiğinde;

Kural tipi	Posture
Tipi	Windows
Posture Tipi	Servis Kontrolü
Servis Adı	
Durumu	Çalışıyor Çalışmıyor

“**Servis Adı**” yazan inputa yazacağınız servisin “**Çalışıyor (Running)**” veya “**Çalışmıyor (Not Running)**” durumuna göre kural tanımı yapabilirsiniz.

5.11.2. Linux

Kural tipi olarak “**Linux**” seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	İşletim Sistemi Kontrolü Program Kontrolü Servis Kontrolü
← İptal Et Kural Ekle	

5.11.2.1. İşletim Sistemi Kontrolü

Posture tipi olarak “**İşletim Sistemi**” Kontrolü seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	İşletim Sistemi Kontrolü
OS Versiyonu	
Tipi	Küçük Eşit Büyük
← İptal Et Kural Ekle	

İşletim sistemi versiyonu “**OS Versiyonu**” inputuna yazdığınız versiyondan “**Küçük, Eşit, Büyük**” ise şeklinde kural tanımı yapabilirsiniz.

5.11.2.2. Program Kontrolü

Posture tipi olarak “**Program Kontrolü**” seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Adı Program Versiyonu

5.11.2.2.1. Program Adı

Alt kural tipi “**Program Adı**” olarak seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Adı
Durumu	Yüklü Yüklü Değil

“**Program Adı**” inputuna yazdığınız program kontrol edilen cihazda “**Yüklü**” veya “**Yüklü Değil**” şeklinde bir kural tanımı yapabilirsiniz.

5.11.2.2. Program Versiyonu

Alt kural tipi “**Program Versiyonu**” olarak seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Program Kontrolü
Program Adı	
Tipi	Program Versiyonu
Versiyon	
Tipi	Küçük Eşit Büyük
← İptal EtKural Ekle	

“**Program Adı**” inputuna yazılan programın versiyonu “**Versiyon**” inputuna yazacağınız değerden “**Küçük, Eşit, Büyük**” şeklinde kural tanımı yapabilirsiniz.

5.11.2.3. Servis Kontrolü

Posture tipi olarak “**Servis Kontrolü**” seçildiğinde;

Kural tipi	Posture
Tipi	Linux
Posture Tipi	Servis Kontrolü
Servis Adı	
Durumu	Running Dead Exited Failed
← İptal Et	

“**Servis Adı**” yazan inputa yazacağınız servisin “**Çalışıyor (Running)**”, “**Çalışmıyor (Dead)**”, “**Çıkış Yaptı (Exited)**” ve “**Hatalı (Failed)**” durumuna göre kural tanımı yapabilirsiniz.

5.11.3. Dosya Takibi

Kural tipi olarak “**Dosya Takibi**” seçildiğinde;

Kural tipi	Posture
Tipi	Dosya Takibi
Dosya Yolu	

Dosya yolunun tam halini girmelisiniz. Örneğin: C:\Program Files\Notepad++\notepad++.exe

“**Dosya Yolu**” inputunda belirtilen dosyanın var olup olmadığını cihaz üzerinde kontrol et şeklinde kural tanımı yapabilirsiniz.

5.11.4. Oturum Takibi

Kural tipi olarak “**Oturum Takibi**” seçildiğinde;

Kural tipi	Posture
Tipi	Oturum Takibi
Süre	

X gündür giriş yapmamış

Cihazda “**Süre**” inputunda belirtilen gün sayısına göre oturum açılmamışsa şeklinde kural tanımı yapabilirsiniz.

5.12. NMAP

Kural tipi olarak “**NMAP**” seçildiğinde;

Kural tipi	NMAP
Parametre	<button>Parametreler</button>
Kelime	

cihazda “**Parametre**” bölümüne yazılan NMAP parametreleri kullanarak bir tarama başlatır ve “**Kelime**” inputuna yazılan çıktıyı arar. Örneğin Parametre inputuna “**-Pn -O**” yazdım ve Kelime inputuna da “**Windows**” yazdım;

- İlgili cihazda belirtilen parametrelerle NMAP taraması başlat ve çıktısında “**Windows**” yazısı geçiyorsa

şeklinde kural tanımı yapabilirsiniz.

6. Profil ve Skor Sistemi ve Örnekler

Yeni bir profil oluşturulduğunda sizden Toplam Eşik Değeri (Profil Skoru) istenmektedir;

Profil Ekle ×

Adı: *	
	ⓘ İsim boş bırakılamaz. Lütfen kontrol ediniz.
Açıklama:	
Toplam Eşik Değeri: *	
	ⓘ Eşik değeri 1'den küçük olamaz.

İptal Et ► Ekle

Bu Profil Skoru, profilin detayına eklenen profil kurallarının puan toplamına eşit veya üzeri şeklinde ayarlanmalıdır. Aşağıdaki verilen örnek kuralların detayları “**1.5 Profil Kural Tipleri**” başlığı altında detaylı bir şekilde anlatılmaktadır.

6.1. Örnek IP_Kamera Profili

Profil Skor sistemini daha ayrıntılı anlamak için bir profil oluşturalım.

“IP_Kamera” adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını **10** olarak belirliyoruz;

Profil Ekle

Adı: *

IP_Kamera

Açıklama:

IP Kamera Profili

Toplam Eşik Değeri: *

10

İptal Et

Ekle

Şimdi oluşturduğumuz bu profile kural setleri ekleyerek Toplam Eşik Değeri puanını yakalamamız gerekiyor.

İlk kural olarak regex'li bir MAC adresi kural seti oluşturalım;

Kural Ekle

Adı

MAC_ADRES

Puanı

5

Durumu

Aktif

Kural tipi

MAC Adresi

Tipi

MAC Adresi

MAC Adresi

01:aa:02:*

Kullanım Biçimleri

01:aa:02:bb:03:cc - 01:aa:02:*

İptal Et

Kural Ekle

Yukardaki örneğe göre cihazın MAC adresi “**01:aa:02:***” ile başlıyorsa bu kural setinden 5 puan alacak şekilde yorumlanır.

Daha sonrasında yeni bir kural seti daha oluřturarak bu sefer Üretici seęelim;

Kural Ekle

Adı

MAC_VENDOR

Puanı

5

Durumu

Aktif

Kural tipi

MAC Adresi

Tipi

Üretici

Üretici

samsung

Kelime İçerięi

İçeriyorsa

İptal Et

Kural Ekle

Yukardaki örneęe göre cihazın MAC üretici bilgisi **“samsung”** içeriorsa bu kural setinden 5 puan daha alacak řekilde yorumlanır.

“IP_Kamera” profilinin Profil skorunu **10** olarak belirlemiřtik. Eęer yukarda yazdıęımız 2 kural setine çarpan bir cihaz olursa ilgili cihaza artık **“IP_Kamera”** profiline uyan bir cihaz diyebiliriz.

Yorumlamak gerekirse;

Network’e erişmeye çalıřan cihazın;

- MAC adresi **“01:aa:02:*”** ile bařlıyorsa 5 puan,
- MAC üretici bilgisi **“samsung”** içeriorsa 5 puan daha alacak.

Yani toplamda kural setlerinden **10** puan’a sahip olacak ve **“IP_Kamera”** profiline uyan bir cihaz olacak.

6.2. Örnek Yazıcı Profili

Bir örnek daha yaparak bu sefer bir Yazıcı profili oluşturalım.

“**Yazıcı**” adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını bu sefer **50** olarak belirliyoruz;

Profil Ekle

Adı: *

Yazıcı

Açıklama:

Yazıcı tipindeki cihazlar

Toplam Eşik Değeri: *

50

İptal Et

Ekle

İlk kural olarak yine regex’li bir MAC adresi kural seti oluşturalım;

Kural Ekle

Adı

canon_mac_regex

Puanı

15

Durumu

Aktif

Kural tipi

MAC Adresi

Tipi

MAC Adresi

MAC Adresi

88:87:17:*

?

Kullanım Biçimleri
01:aa:02:bb:03:cc - 01:aa:02:*

< İptal Et

Kural Ekle

Eğer cihazın MAC adresi “**88:87:17:***” ile başlıyorsa kural setinden **15** puan alacak şekilde yorumlayabiliriz.

Profil Skorunu **50** olarak belirtmiştik. Kuralımız işlerse cihaz **15** puan alacak ve cihaza “**Yazıcı**” profilindeki bir cihaz diyebilmemiz için **50-15=35** puanlık kural setleri daha gerekmektedir.

İkinci kural olarak MAC üretici bilgisi ekleyelim;

Adı	canon_mac_vendor
Puanı	15
Durumu	Aktif
Kural tipi	MAC Adresi
Tipi	Üretici
Üretici	canon
Kelime İçeriği	İçeriyorsa

[← İptal Et](#)[Kural Ekle](#)

Eğer cihazın MAC üreticisi “**canon**” içeriyorsa kural setinden 15 puan alacak şekilde yorumlayabiliriz.

Yine tekrar etmek gerekirse, Profil Skorunu **50** olarak belirtmiştik. Bize ilk kuralımız işlerse cihaz **15** puan alacak. İkinci kuralımızda işlerse **15** puan daha alacak ve toplamda **30** puan’a erişecek. Bizim **50** puana ihtiyacımız var ve **50-30=20** puanlık kural setleri daha gerekmektedir.

Devam edelim ve üçüncü kural olarak bu sefer TCP/UDP port bilgisi ekleyelim;

 Kural Ekle x

 Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

tcp_9100

Puanı

20

Durumu

Aktif

Kural tipi

TCP/UDP

TCP Portları

9100

UDP Portları

Port Durumu

Open

 Kullanım Biçimleri
80 - 80,8080 - 90,50,8081-9000

 İptal Et

 Kural Ekle

Eğer cihazın **“TCP 9100 portu açıksa”** (open) kural setinden de **20** puan alacak şekilde yorumlayabiliriz.

Sonuç olarak Network’e erişmeye çalışan cihazın;

- MAC adresi **“88:87:17:*”** ile başlıyorsa 15 puan,
- MAC üretici bilgisi **“canon”** içeriyorsa 15 puan,
- **“TCP 9100 portu açık”** ise 20 puan alacak.

Toplamda **50** puana ulaşacak ve Yazıcı profiline uygun bir cihaz olarak tanımlanacaktır.


Bilgi ve İletişim Teknolojileri

Rakort.com

info@rakort.com

0850 460 10 58

Mustafa Kemal Mah. 2139 Cad.
Ekim Plaza No: 2 Kat: 3 Daire: 16

Çankaya / Ankara

6.3. Örnek IoT Cihaz Profili

Bir örnek daha yaparak bu sefer daha kapsamlı ve sıkılaştırılmış bir profil oluşturalım.

“IoT” adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını bu seferde **50** olarak belirliyoruz;

Profil Ekle

Adı: *

IoT

Açıklama:

Toplam Eşik Değeri: *

50

İptal Et

Ekle

İlk kural olarak yine regex’li bir MAC adresi kural seti oluşturalım ve buna 5 puan verelim;

Kural Ekle

Adı

mac_regex

Puanı

5

Durumu

Aktif

Kural tipi

MAC Adresi

Tipi

MAC Adresi

MAC Adresi

01:aa:02:*

?

Kullanım Biçimleri
01:aa:02:bb:03:cc - 01:aa:02:*

< İptal Et

Kural Ekle

Cihazın MAC adresi “01:aa:02:*” ile başlıyorsa 5 puan alacak.

Devam edelim ikinci kural olarak bu sefer **TCP 1010** portunun açık olması kuralını ekleyelim ve buna da 10 puan verelim;

Kural Ekle

Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

tcp_1010

Puanı

10

Durumu

Aktif

Kural tipi

TCP/UDP

TCP Portları

1010

UDP Portları

Port Durumu

Open

?

Kullanım Biçimleri

80 - 80,8080 - 90,50,8081-9000

←

İptal Et

Kural Ekle

Cihazın **TCP 1010** portu açıksa buradan **10** puan alacak ve toplamda **15** puana erişecek.

Rakort
Bilgi ve İletişim Teknolojileri

Rakort.com

info@rakort.com

0850 460 10 58

Mustafa Kemal Mah. 2139 Cad.
Ekim Plaza No: 2 Kat: 3 Daire: 16

Çankaya / Ankara

Üçüncü kural olarak bir SNMP kuralı yapalım ve buna da **10** puan verelim;

Kural Ekle

Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

snmp

Puanı

10

Durumu

Aktif

Kural tipi

SNMP

SNMP Tipi

SNMP v2c

Community

Port

161

SNMP OID

1.3.6.1.2.1.1.1

Değer

IoT

Kelime İçeriği

İçeriyorsa

Cihaza **SNMPv2c** community ile **1.3.6.1.2.1.1.1** (SNMP sysdescr OID) istek atılacak ve cevabın içinde **IoT** geçiyorsa buradan da **10** puan alacak. Toplamda **25** puana erişecek.

Unutmayın, profili eklerken **50** puan vermiştik. Şu an **25** puandayız. Devam edelim ve dördüncü kuralı HTTP/HTTPS olarak ekleyelim ve buna **15** puan verelim;

Kural Ekle

Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

http_profil

Puanı

15

Durumu

Aktif

Kural tipi

HTTP/HTTPS

URL

/

Portu URL üzerinden belirtebilirsiniz. Örneğin: https://192.168.1.10:6000

Değer

Energy

Kelime İçeriği

İçeriyorsa

Giriş Ekranı

☐

← İptal Et

Kural Ekle

Cihazın web arayüzü taranacak ve içeriğinde **“Energy”** kelimesi geçiyorsa bu kuraldan da **15** puan daha alacak. Toplamda **45** puan’a ulaştık.

Cihaza IoT profilindeki bir cihaz diyebilmemiz için 5 puanlık kural setine ihtiyacımız kaldı.

Hemen beşinci kuralımızı ekleyelim. Bunun tipini de IP adresi olarak belirleyelim ve cihazın bir ip bloğunun içinde olması kuralını yapalım;

Kural Ekle

Bu profil işlenirken ilgili cihazın IP adresini almış olması gerekiyor.

Adı

ipaddr_rule

Puanı

5

Durumu

Aktif

Kural tipi

IP Adresi

IP Adresi

192.168.1.0/24

?

Kullanım Biçimleri

192.168.1.0 - 192.168.1.0/24 - 192.168.1.* - 192.168.*.* - 192.168.*.[1-10] - 192.168.[1-5].[1-10]

<

İptal Et

Kural Ekle

Cihazın IP adresi **192.168.1.0/24** network bloğu içindeyse bu kuraldan da **5** puan daha alacak. Toplamda **50** olacak.

Artık tüm kurallarımız hazır. Bir cihaza “**IoT**” profilinde diyebilmemiz için sıkı bir kural seti oluşturduk. Özetlemek gerekirse;

- Cihazın MAC adresi “**01:aa:02:***” ile başlıyorsa **5** puan,
- Cihazın “**TCP 1010 portu**” açıksa **10** puan,
- Cihazın **SNMPv2c** community ile “**1.3.6.1.2.1.1.1** (sysDescr)” SNMP OID’ine istek attığımızda gelen cevabın içinde “**IoT**” geçiyorsa **10** puan,
- Cihazın web arayüzü taranacak ve içeriğinde “**Energy**” kelimesi geçiyorsa **15** puan,
- Cihazın IP adresi “**192.168.1.0/24**” network bloğu içindeyse **5** puan alacak

toplamda **50** puana ulaşacak ve biz artık bu cihaza “**IoT**” profiline uygun bir cihaz olarak tanımlayacağız.

Cihaz profillemeye ile ilgili tüm detayları öğrendik. Cihazlar profillendikten sonra aksiyon alma işlemi Politikalar üzerinden gerçekleşmektedir. Bunun için **politikalar.docx** dökümanını inceleyebilirsiniz.

Rakort
Bilgi ve İletişim Teknolojileri

Rakort.com

info@rakort.com

0850 460 10 58

Mustafa Kemal Mah. 2139 Cad.
Ekim Plaza No: 2 Kat: 3 Daire: 16

Çankaya / Ankara