
FORTINET®

CISCO

TALOS

IP BLACKLIST

Entegrasyonu

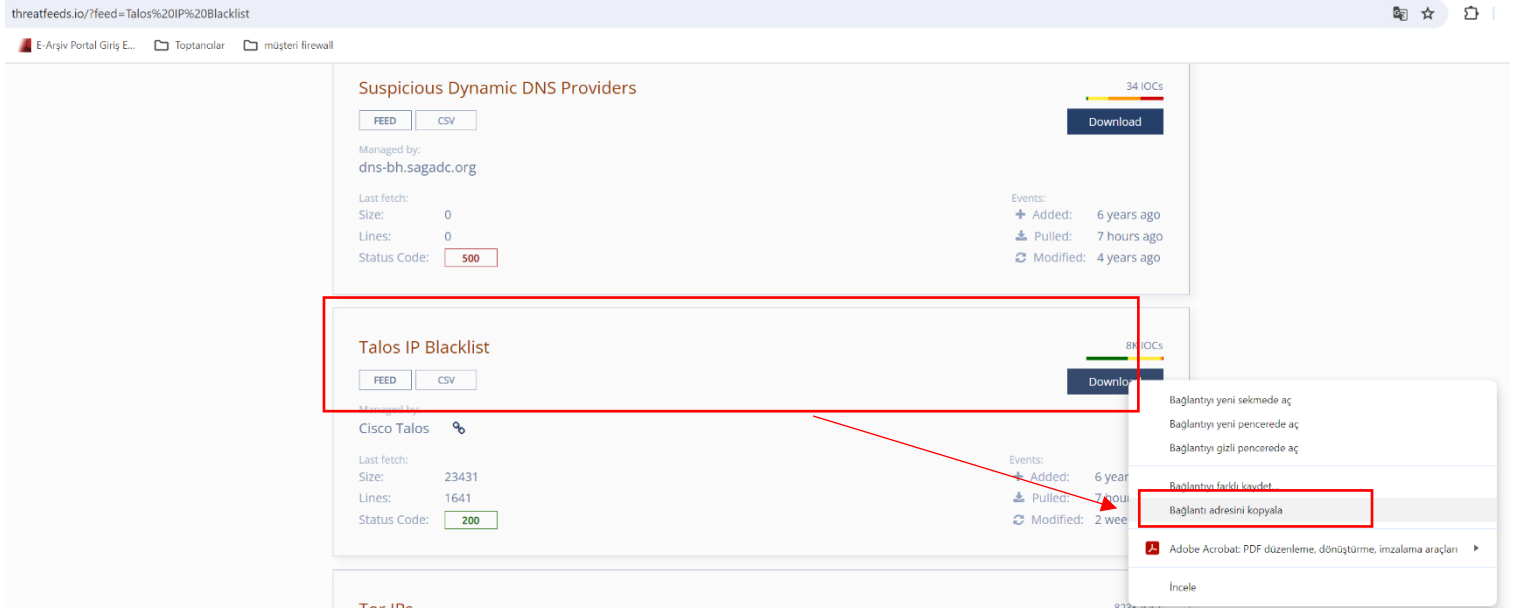
FORTIGATE firewall Cihazında 3.Taraf
Tehdit akışlarını ve ip listesini kullanma

Fortigate

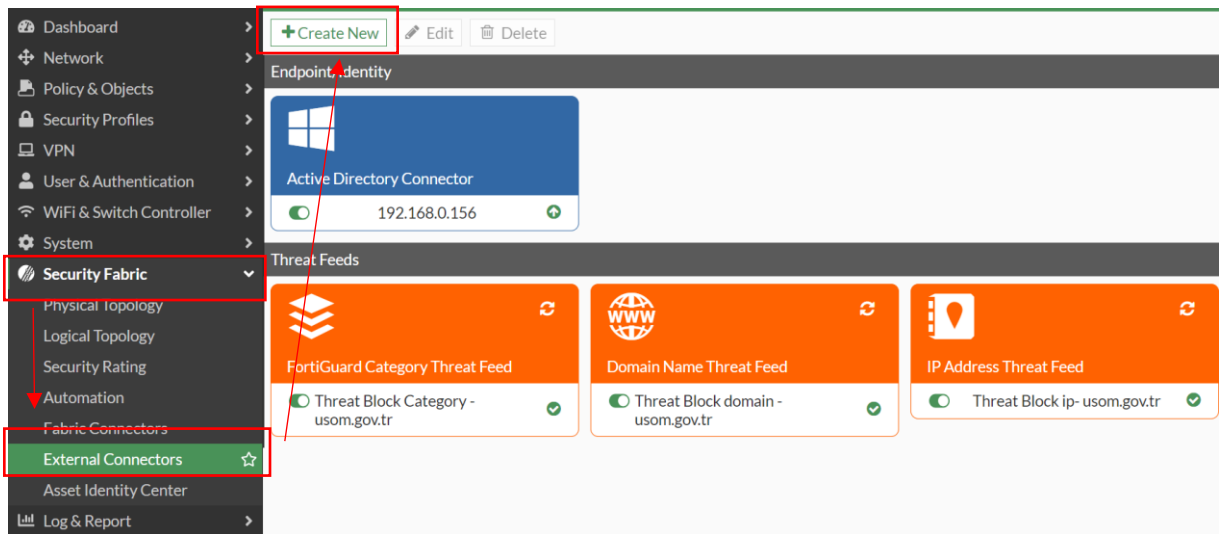
Security Fabric – External Connectors

İlk olarak ilgili aşağıdaki adres'e giditorum ve "Cisco Talos Intelligence Group" ip blacklist database bağlantı adresini kopyalıyorum.

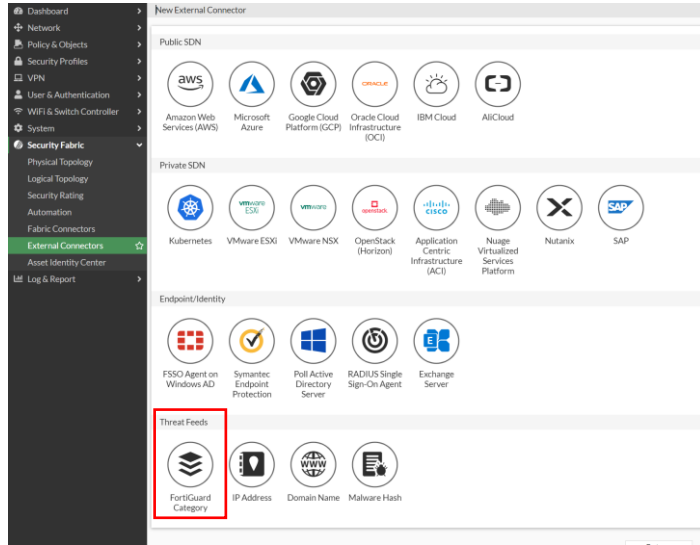
<https://threatfeeds.io/?feed=Talos%20IP%20Blacklist>



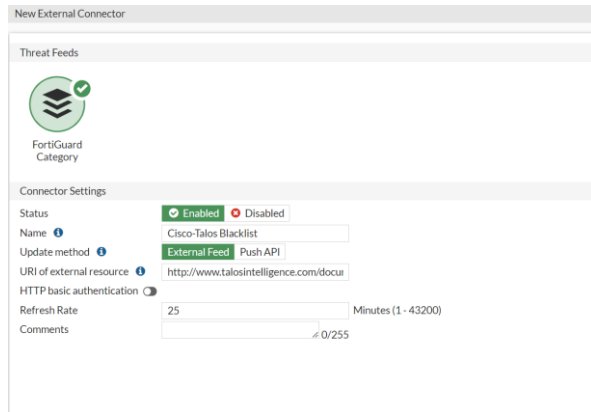
Sonraki adımda Firewall cihazıma gidiyor ve "security fabric" sekmesi altından "External Connectors" e tıklıyorum. Karşıma gelen sayfadan yeni bir connectors oluşturmak için "Create New" diyorum.



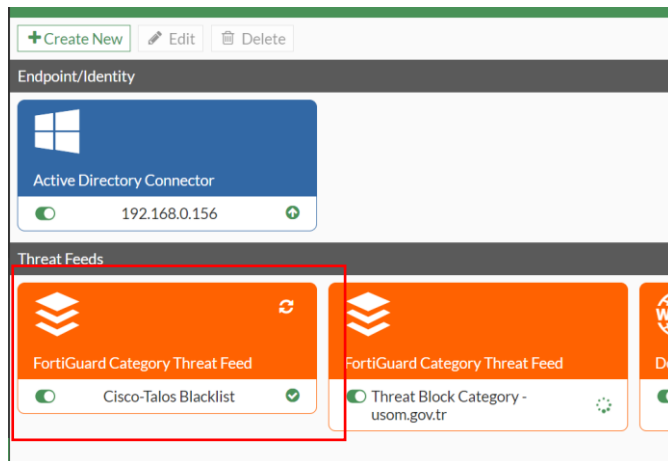
Karşıma gelen ekrandan “FortiGuard Category” seçeneğine tıklıyorum.



Yine karşıma gelen ekrandan Connector e bir isim veriyorum ve üst adımlarda kopyalama işlemini gerçekleştirdiğim bağlantımı External Resource bölümüne yapıştırıyorum. http Basic authentication kapalı tutuyorum ve tanımlama işlemimi tamamlıyorum.



Görüldüğü üzere Yeşil onay tik işareti çıktı bağlantı başarılı.



Sonraki adımda oluşturmuş olduğum connector ü kuralıma ekliyorum ve Action kısmını DENY seçerek kayıt ediyorum.

The screenshot shows the Fortinet Firewall Policy configuration interface. The 'Edit Policy' window is open, showing the following details:

- ID: 55
- Name: (empty)
- Incoming Interface: LAN (selected)
- Outgoing Interface: INTERNET (wan1)
- Source: all
- Negate Source: (unchecked)
- Destination: Threat Block ip- usom.gov.tr (selected)
- Negate Destination: (unchecked)
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (unchecked)
- Log Violation Traffic: (checked)
- Advanced: WCCP (unchecked), Exempt from Captive Portal (unchecked)
- Comments: Write a comment... (0/1023)
- Enable this policy: (checked)

The 'Select Entries' dialog is open on the right, showing a list of entries. The entry 'Threat Block ip- usom.gov.tr' is selected at the bottom of the list.

Kuralımı en yukarıya taşıyorum. Tüm firewalllarda hiyerarşi yukarıdan aşağıya doğrudur.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Talos Blacklist	lan ANA-DM ATIKSU HOSAB_GUEST Kamera SU_ARITMA	INTERNET (wan1)	all	Threat Block ip- usom.gov.tr	always	ALL	DENY			All