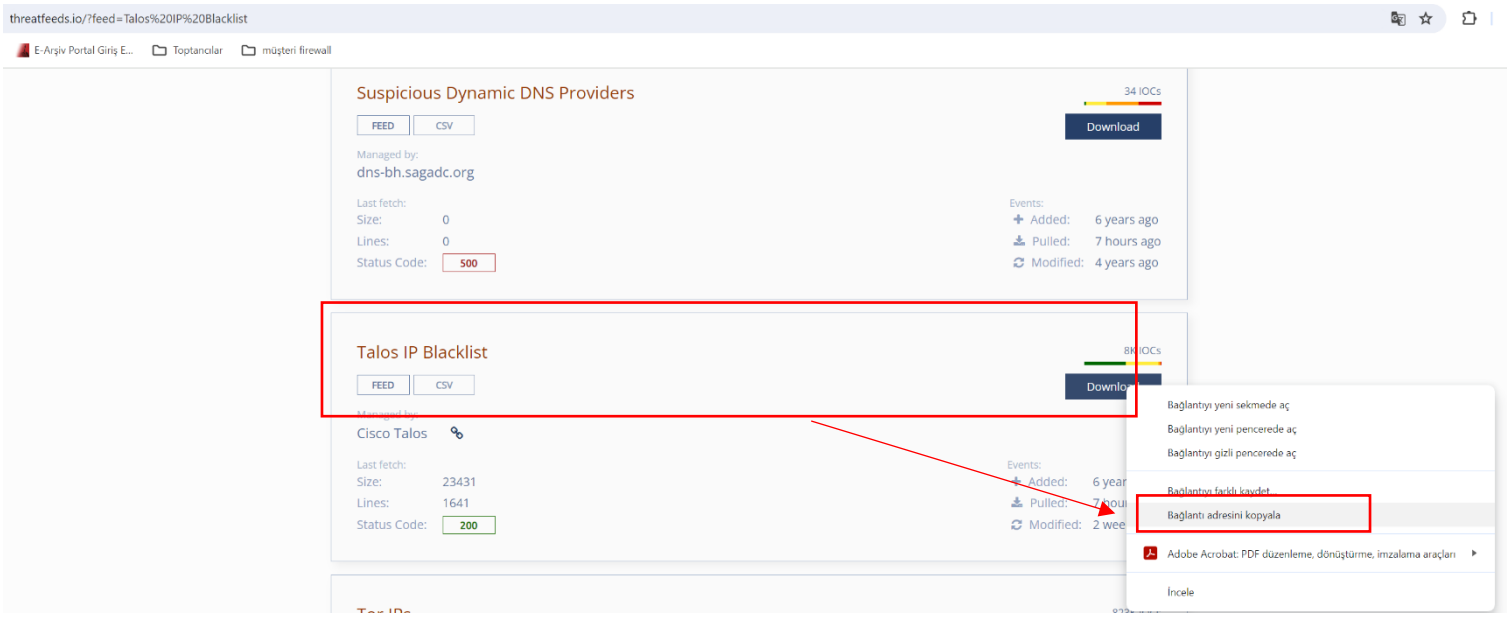
IP BLACKLIST
Entegrasyonu

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

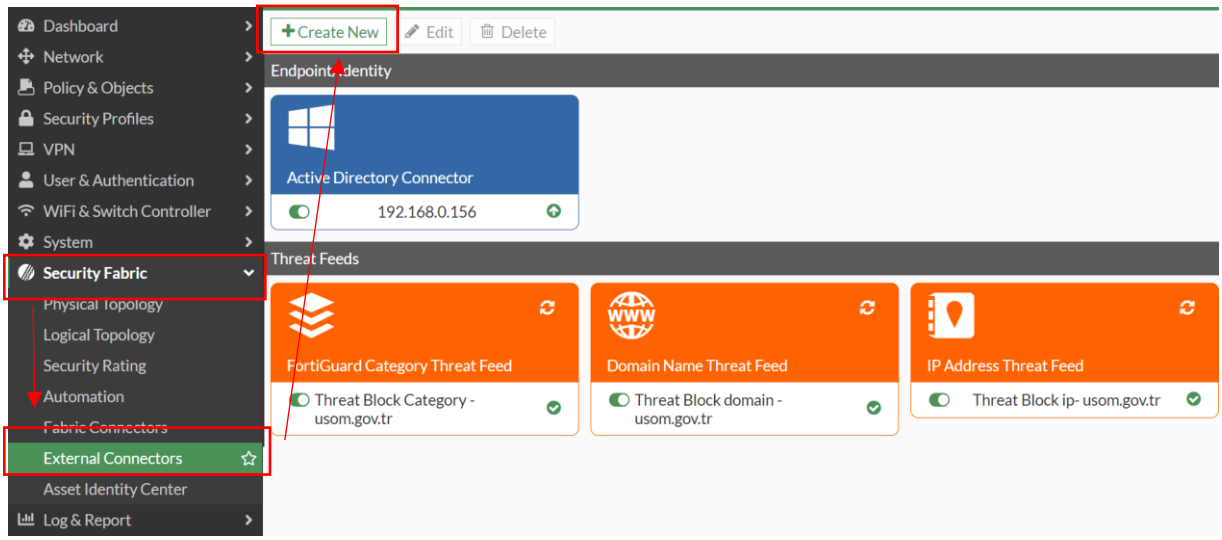
Fortigate
Security Fabric – External Connectors

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

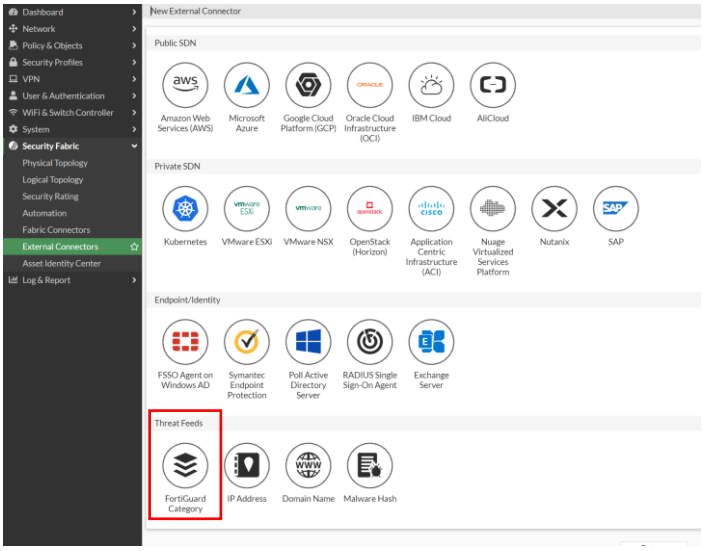
https://threatfeeds.io/?feed=Talos%20IP%20Blacklist



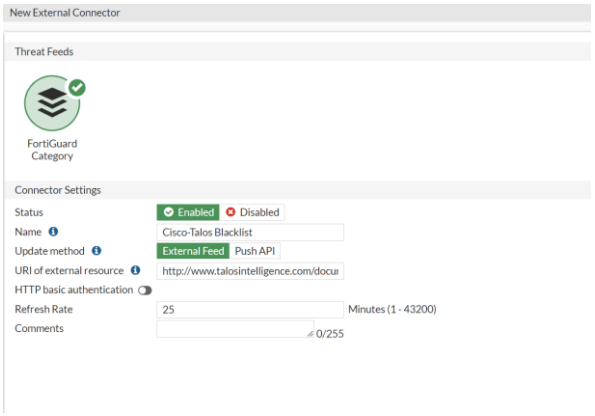
Sonraki adımda Firewall cihazıma gidiyor ve "security fabric" sekmesi altından "Extarnal Connectors" e tıklıyorum. Karşıma gelen sayfadan yeni bir connectors oluşturmak için "Create New" diyorum.



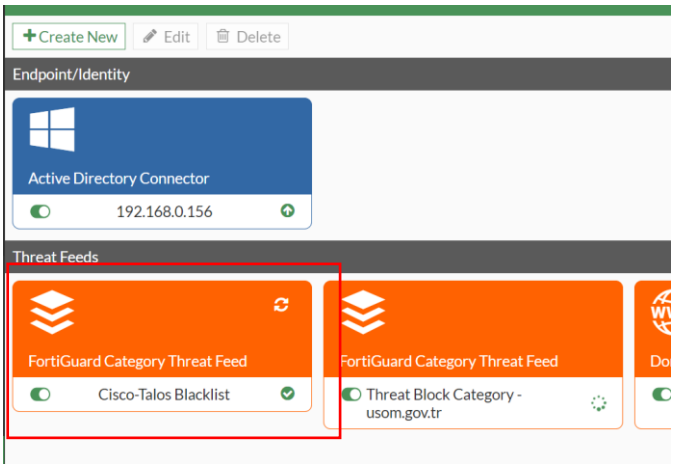
Karşıma gelen ekrandan “FortiGuard Category” seçeneğine tıklıyorum.



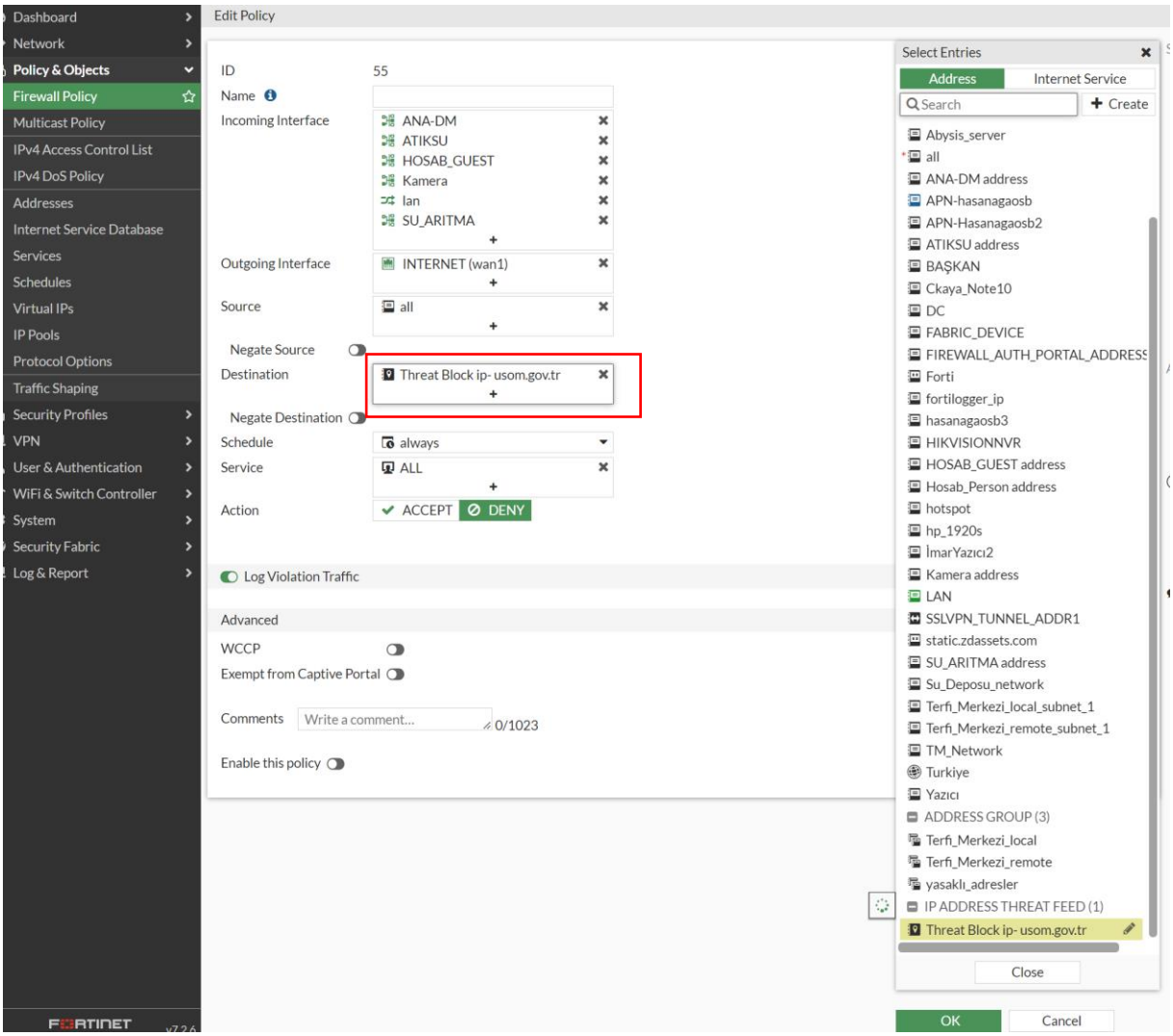
Yine karşıma gelen ekrandan Connector e bir isim veriyorum ve üst adımlarda kopyalama işlemini gerçekleştrdiğim bağlantımı External Resource bölümğne yapıştırıyorum. http Basic authentication kapalı tutuyor ve tanımlama işlememi tamamlıyorum.



Görüldüğü üzere Yeşil onay tik işareti çıktı bağlantı başarılı.



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



Kuralımı en yukarıya taşıyorum. Tüm firewallarda 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