

FORTINET®



ABUSE | ch

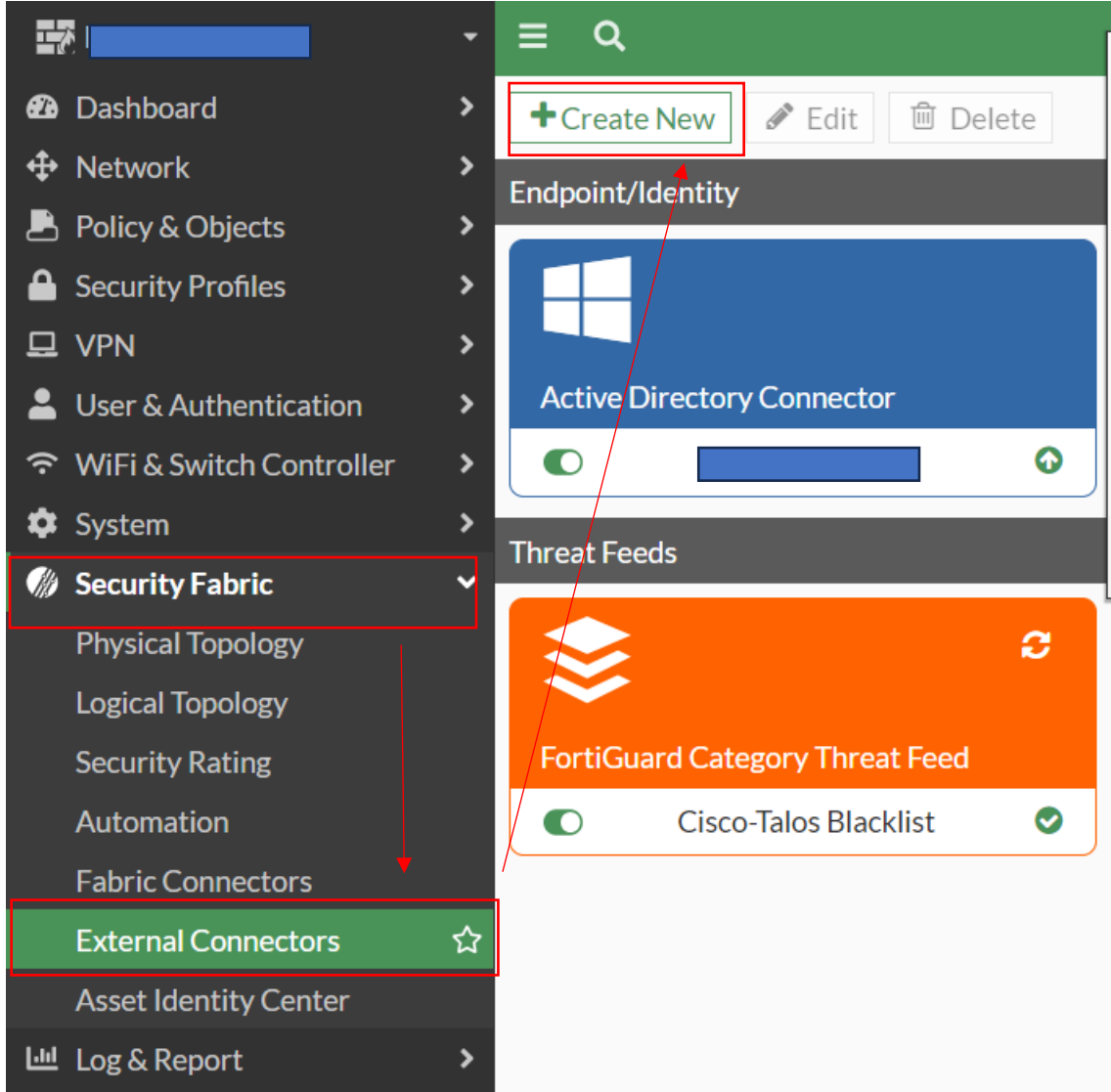


WARNING

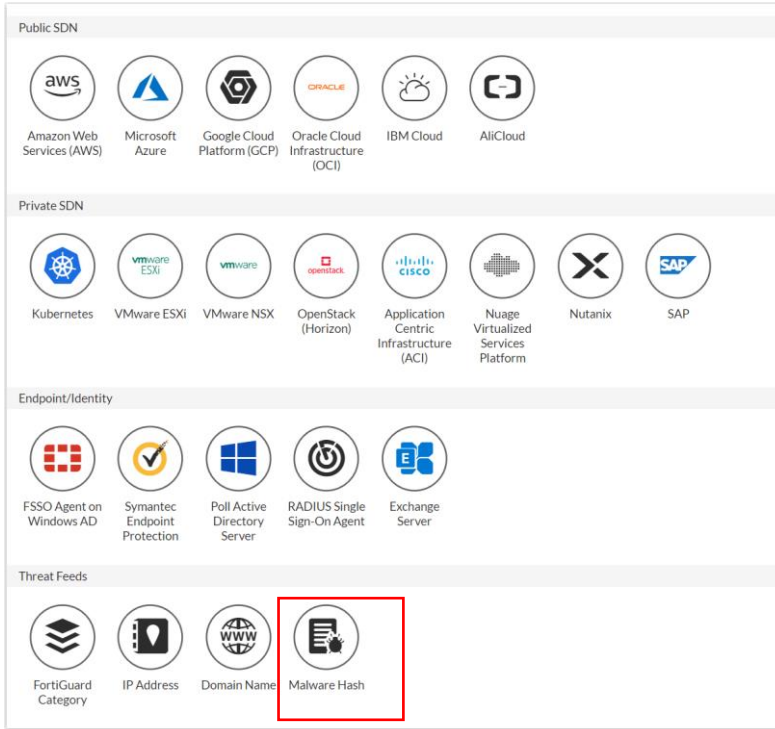
Fortigate

"Malware Hash Threat Feed"
Kullanımı

Öncelikle **“EXTERNAL CONNECTOR”** eklemek için firewall menüsünden **“Security Fabric”** altından **“External Connectors”** e tıklıyorum ve karşıma gelen menüden **“Creative New”** butonuna tıklıyorum.

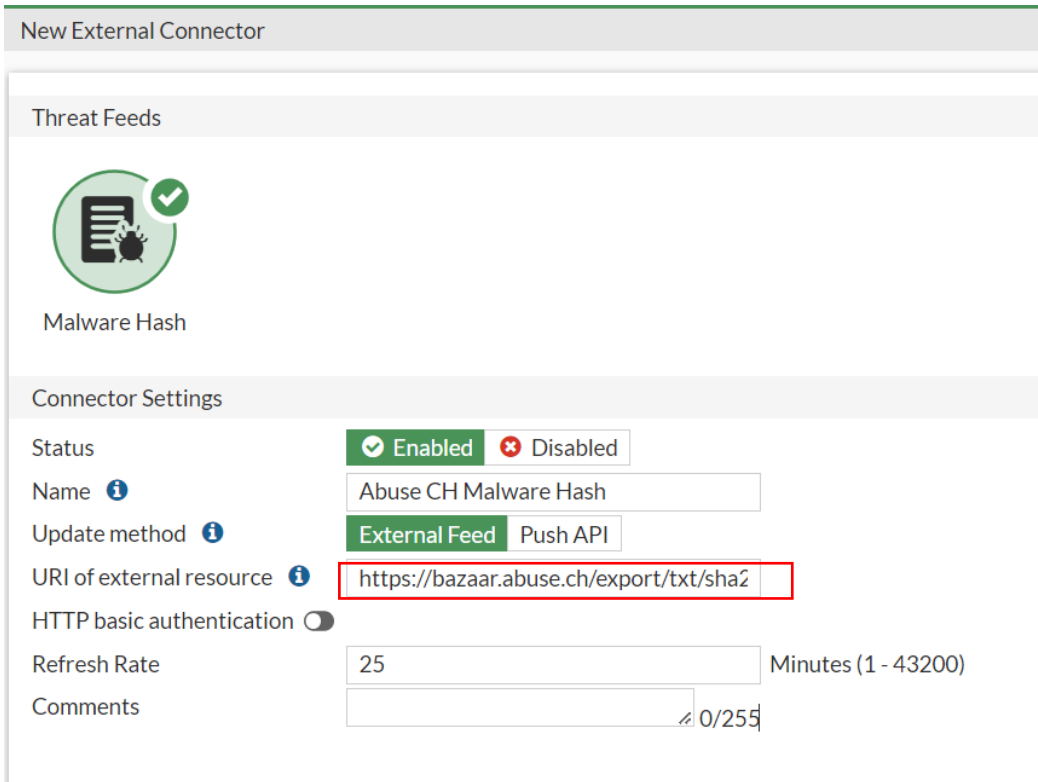


Karşıma gelen ekrandan "Malware Hash" a tıklıyorum.

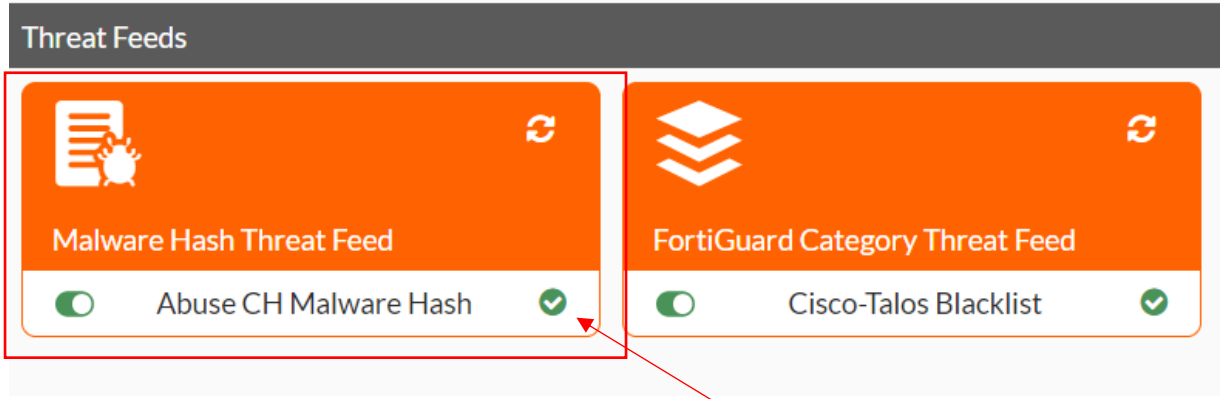


Karşıma gelen ekranı Abuse ch nin sunmuş olduğu ve Malware hash bilgilerinin olduğu linki kullanarak yapılandırıyor ve ok diyerek işlemimi tamamliyorum.

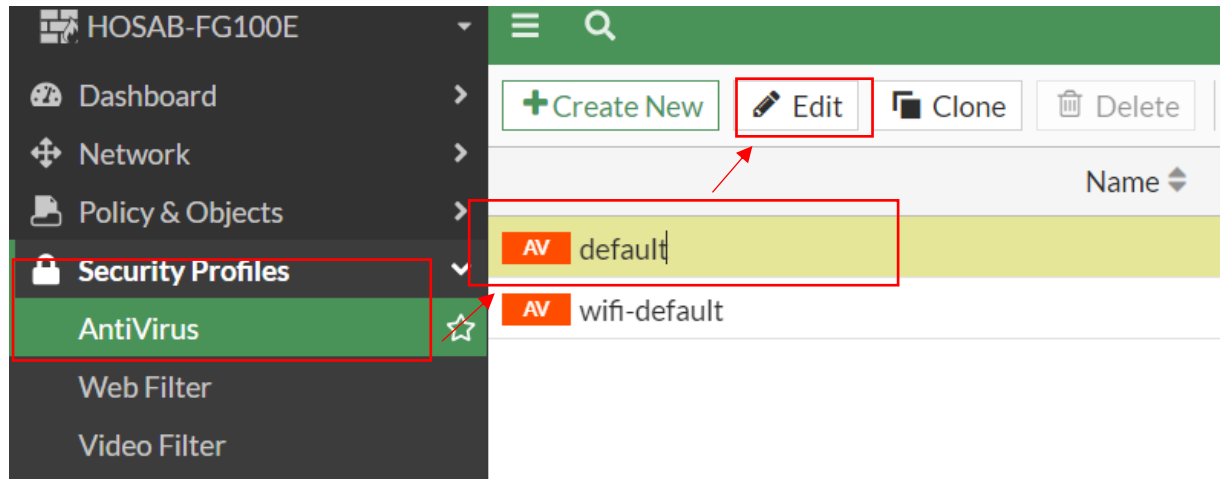
<https://bazaar.abuse.ch/export/txt/sha256/recent/>



Görüldüğü üzere External Connector bağlandım gerçekleşti.



Sonraki adımda firewall menüsünden **“security Profiles”** altından **“Antivirüs”** e tıklıyorum karşıma gelen ekrandan ben var olan default gelen politikaya edit diyorum. Siz yeni bir tane daha oluşturabilirsiniz.



Karşıma gelen ekrandan **“Use external malware block list”** butonunu aktif ediyorum ve ok diyerek işlemimi tamamliyorum. Böylece eklemiş olduğumuz malware connector otomatik olarak tanınacaktır.

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ☒ Block ☐ Monitor

Feature set: ☒ Flow-based ☐ Proxy-based

Inspected Protocols

HTTP ☒
SMTP ☒
POP3 ☒
IMAP ☒
FTP ☒
CIFS ☐

APT Protection Options

Treat Windows executables in email attachments as viruses ☒
Send files to FortiSandbox for inspection ☐
Include mobile malware protection ☒
Quarantine ☐

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database ☒ Block ☐ Monitor

Use external malware block list ☒ Block ☐ Monitor

All Specify

Use EMS threat feed ☐

OK Cancel



Bilgi Teknolojileri