ICAP protokoll alapú kiegészítő biztonsági szolgáltatás *Zorp Gateway* mellé

2022. július 28.

Az alábbi use case lépésről lépésre mutatja be, hogyan lehet a *Zorp Gatewayt* és a Zorp Content Vectoring Systemet kiegészíteni Internet Content Adaptation Protocol (ICAP) alapú Data Loss Prevention (DLP) és egyéb antivírus megoldással.

Tartalom

1. A probléma bemutatása

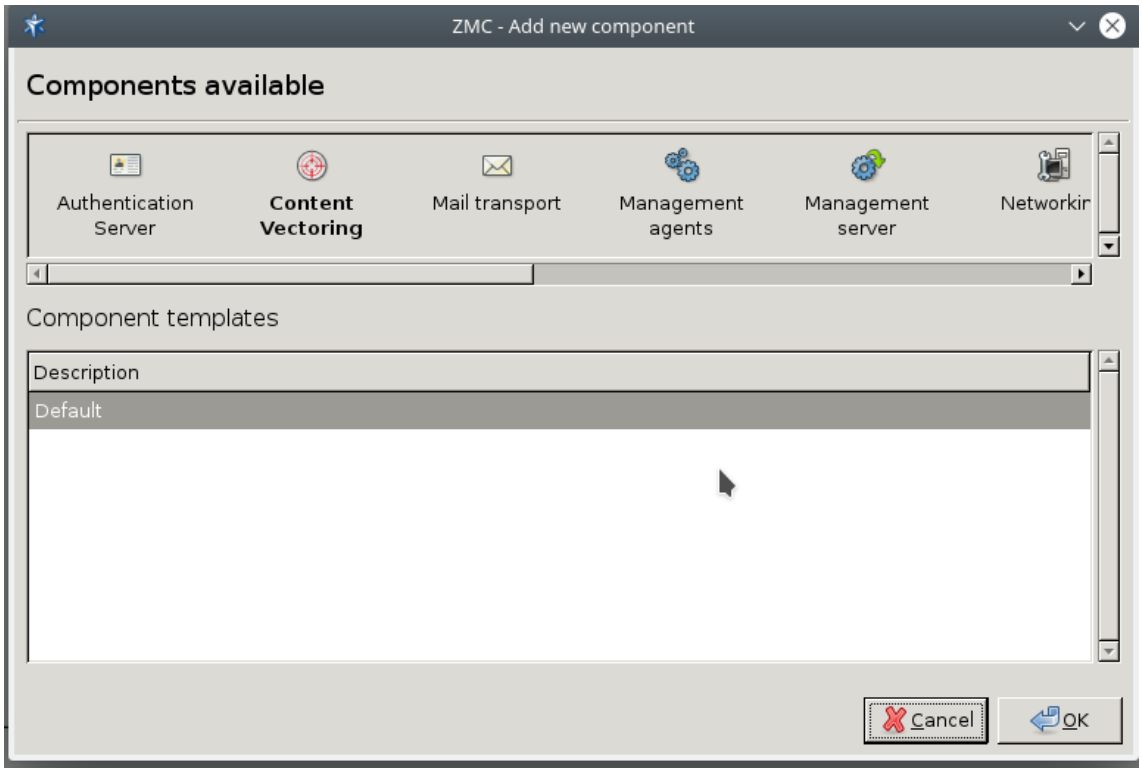
Nagyvállalati szinten end-to-end biztonsági megoldás eléréséhez a kockázatok és támadási felületek csökkentése érdekében többrétegű, integrált biztonsági infrastruktúrát érdemes kiépíteni. A harmadik féltől származó, kiegészítő biztonsági eszközök integrálása azonban nem triviális.

2. A megoldás bemutatása

A *Zorp* keretrendszer támogatja az ICAP protokollt, melyen keresztül tetszőleges gyártótól származó, - ICAP protokollt szintén támogató - DLP vagy egyéb alapú antivírus megoldással egészíthető ki a meglévő, *Zorp* alapú hálózatbiztonsági rendszer.

3. Technikai megvalósítás

1. Hozza létre a *Zorp Management Console (ZMC)* felületen a *Zorp Content Vectoring System (ZCV)* modult (licencköteles):

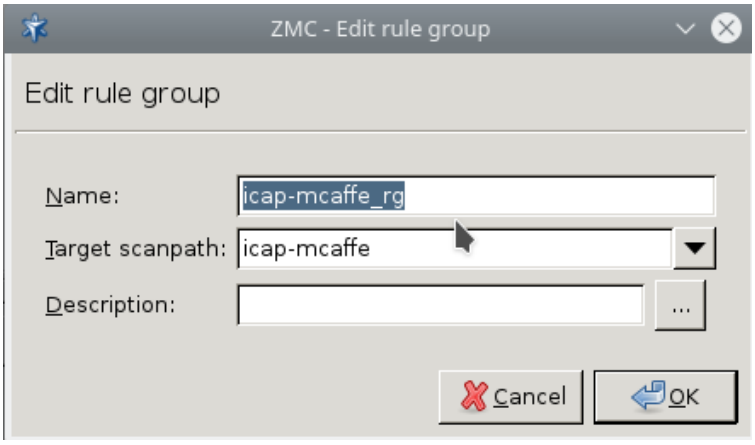


1. ábra - Zorp Management Console modulok

2. Helyezze be a licenc modulba a *Zorp Content Vectoring System* licencet.
3. Hozzon létre a *Zorp Management Console* modulban egy új rule groupot:

```
Name: icap-mcaffe_rg
Target scanpath: ACCEPT
```

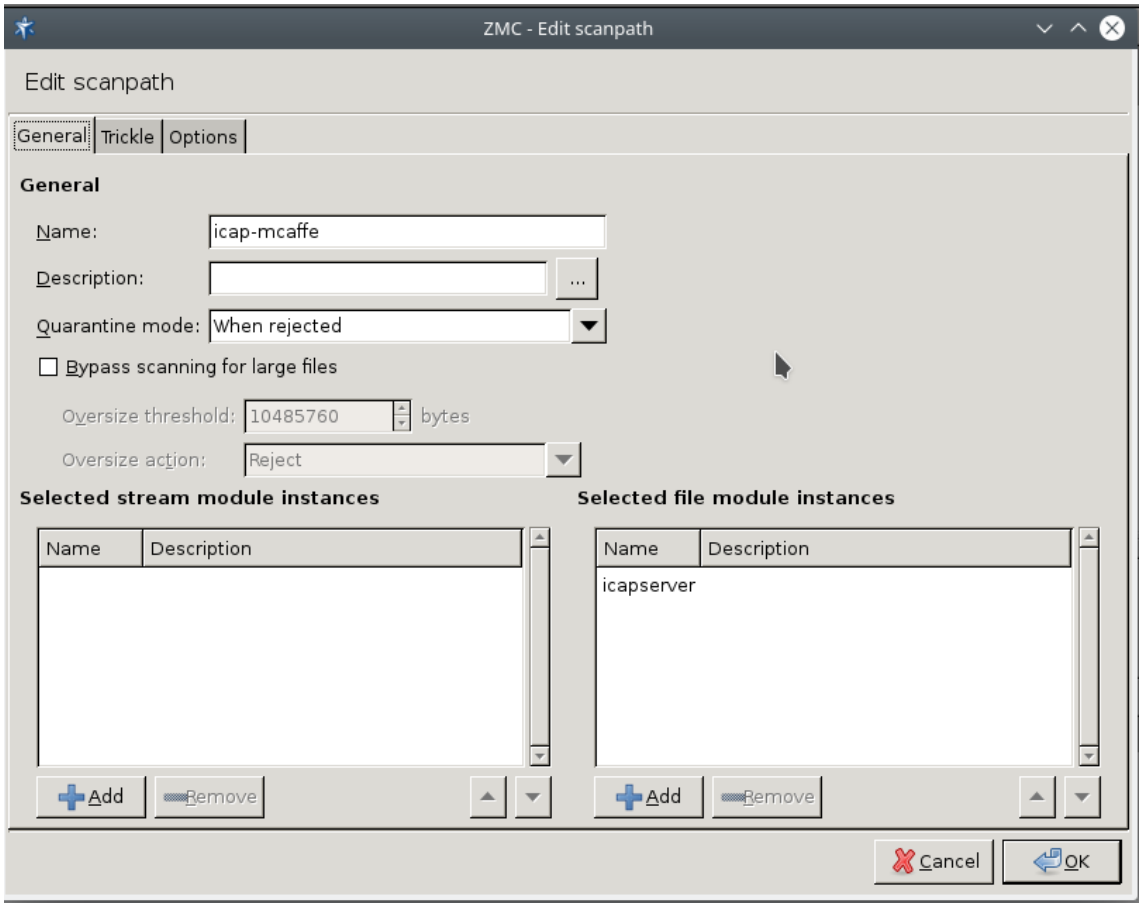
(A *Target scanpath* egy későbbi lépésben (6. lépés) megváltoztatható.)



2. ábra - Új Rule group létrehozása

4. Hozzon létre egy új *scanpath*-t:

```
Name: icap-mcaffe
Quarantine mode: When rejected
```

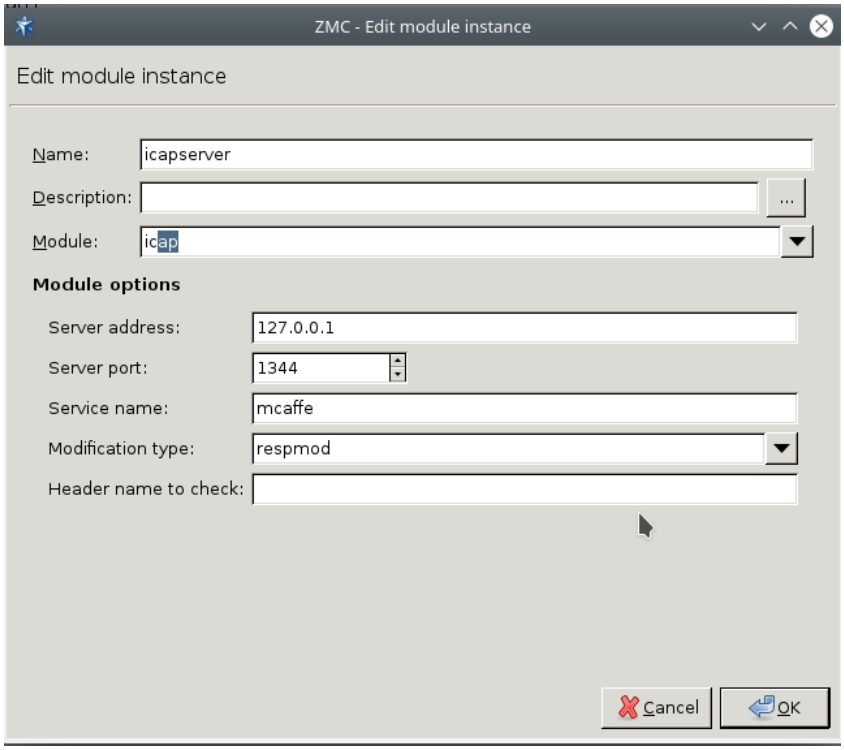


3. ábra - Új scanpath létrehozása

5. Hozzon létre egy új *modul instances*-t:

```
Name: icapserver
Module: icap
Server address: DLP vagy AV szerver címe, ami ICAP protokollt használ.
Modification type: respmod/reqmod
```

(respmod: milyen irányú kommunikációt szűrjön)



4. ábra - Új module instance létrehozása

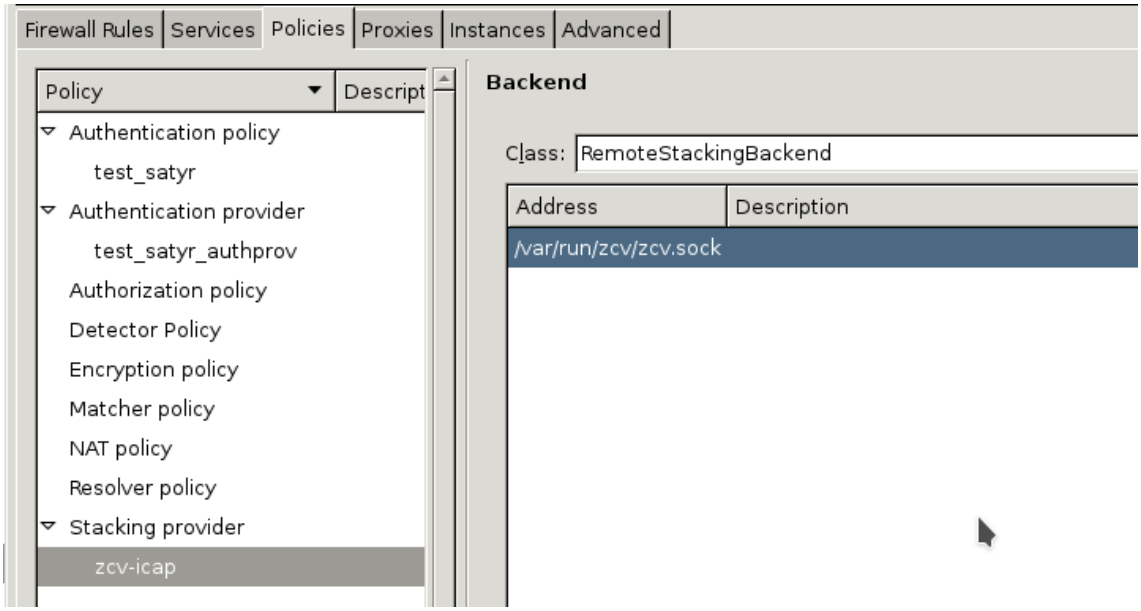
6. Szerkessze a *rule group*ban létrehozott sémát:

```
Target scanpath: icap-mcaffe
```

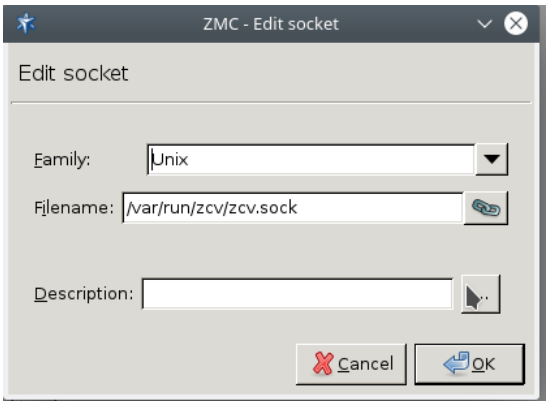
(az előző lépésekben lett létrehozva)

7. Hozzon létre egy új szabályrendszert (policy):
Stacking provider létrehozása:

```
zcv-icap
Backend:
Class: RemoteStackingBackend
```



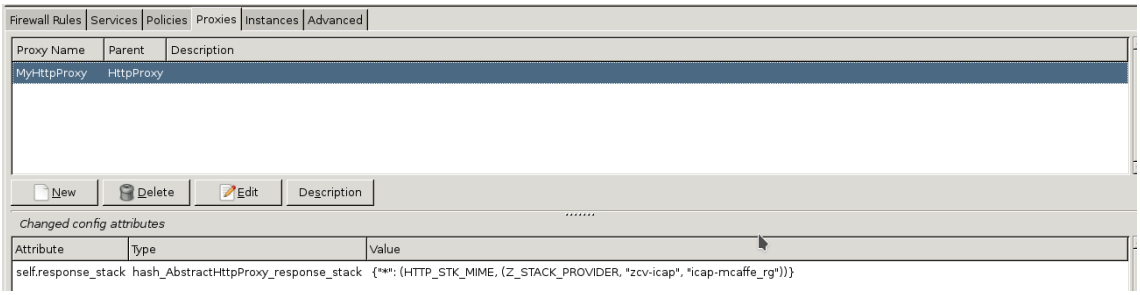
5. ábra - Új szabályrendszer létrehozása



6. ábra - Új socket létrehozása

Újdonság: Kiválaszthatjuk, hogy lokálisan fusson-e vagy másik szerveren.

8. Hozzon létre proxyt a proxy tablón.
HttpProxy template létrehozása:



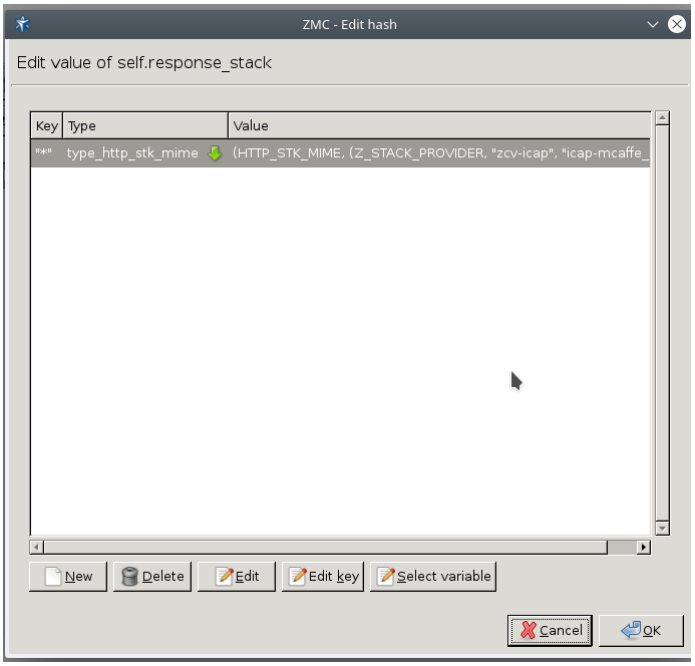
7. ábra - HttpProxy létrehozása

9. Szerkessze az attribútumokat.

- Válassza ki, majd szerkessze a *self.response_stacket*.
  Új elem létrehozása: Válassza az *OK-t*.

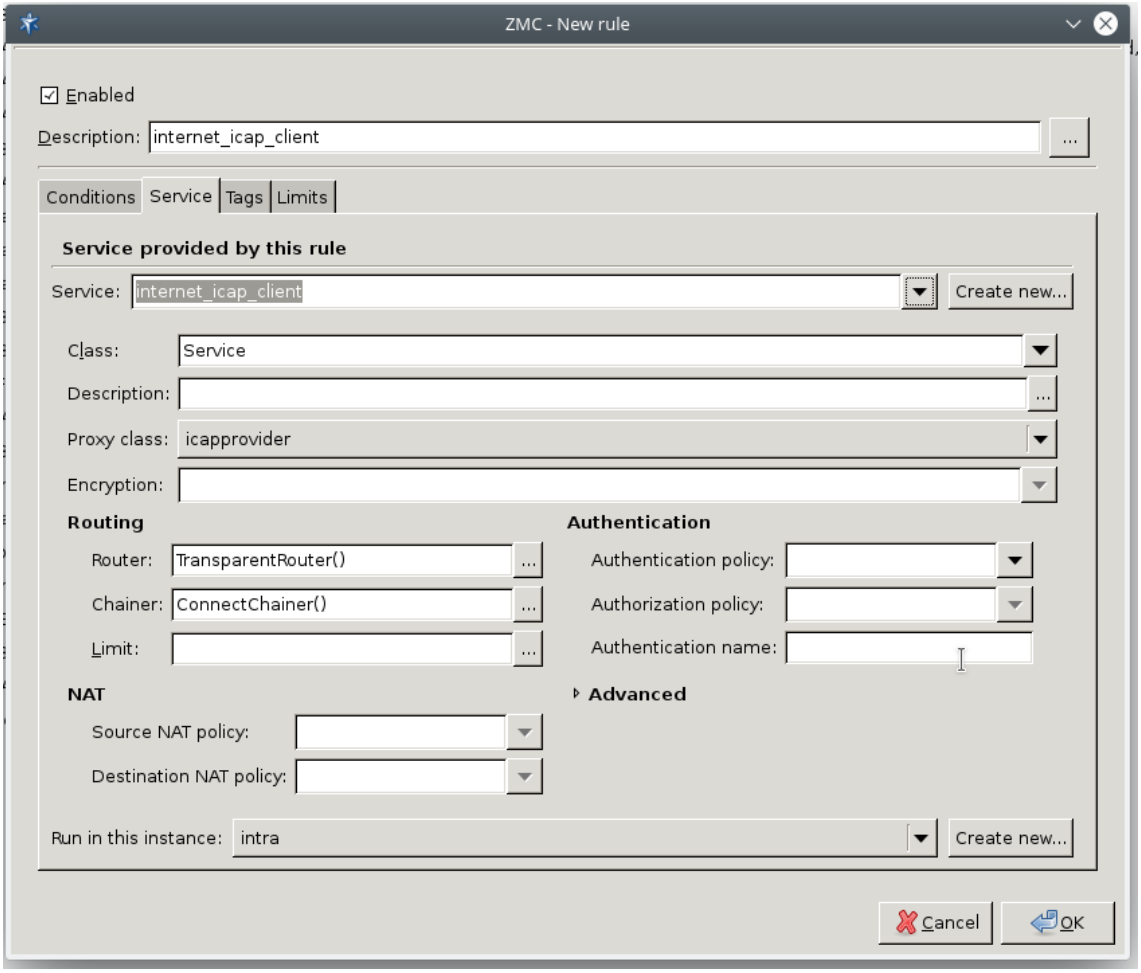
- Válassza ki a *type_http_stk_mime-t*:

```
Value: Zorp_stack
            Stacking_provider: zcv-icap (amit létrehoztunk)
            rule group: icap-mcaffe_rg (amit létrehoztunk)
```

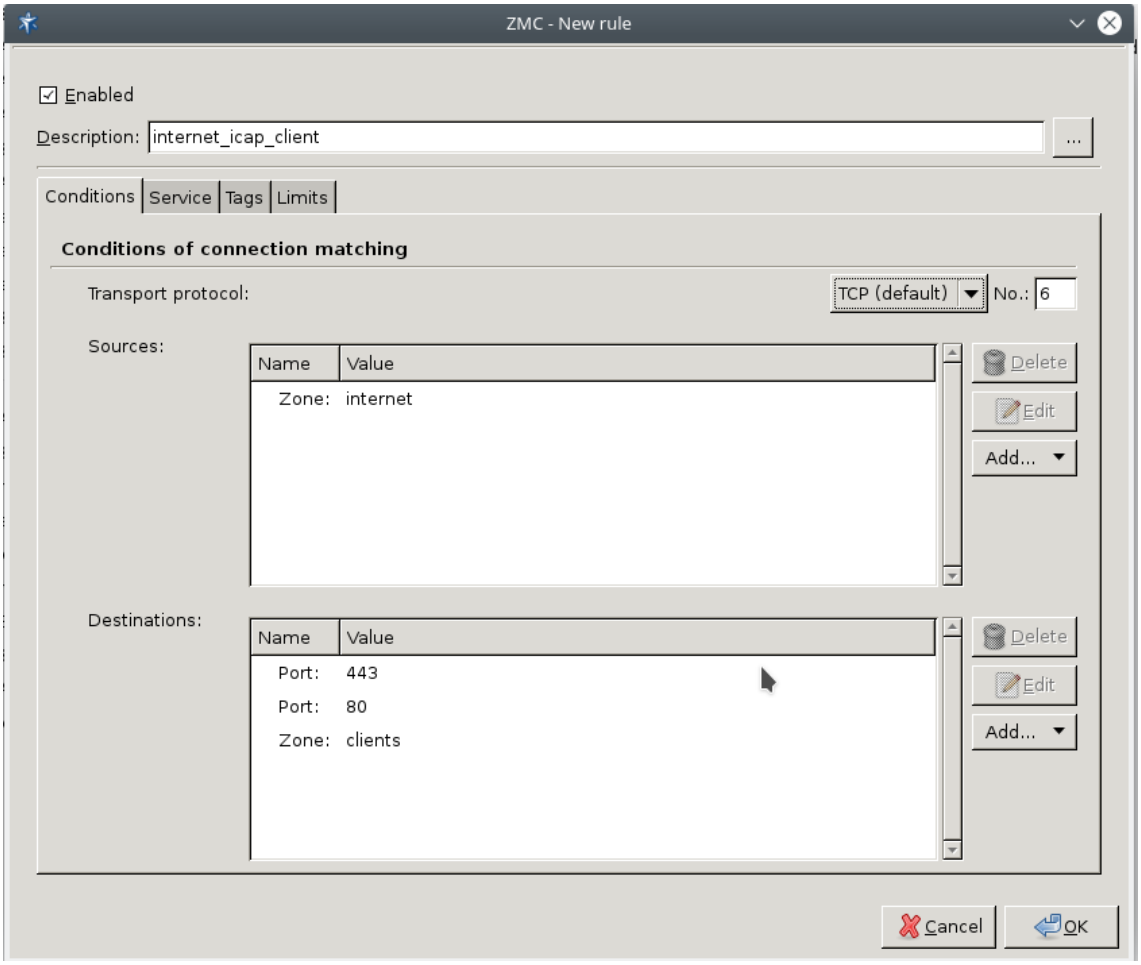


8. ábra - A self.response_stack szerkesztése

10. Hozzon létre új szabályt:



9. ábra - Új szabály létrehozása - service



10. ábra - Új szabály létrehozása - feltételek

4. Konklúzió

A *Zorp* hálózatbiztonsági szolgáltatásait egyszerűen ki lehet egészíteni harmadik féltől származó, ICAP protokollt támogató tartalomszűrő megoldásokkal (Kaskersky, Mcaffe, Norton, ESET, stb.). A fenti beállítási lehetőségek révén bármely, ICAP protokollt ismerő, DLP vagy antivírus alapú termék tetszés szerint illeszthető a *Zorp Content Vectoring System* modulhoz. A fenti megoldással már a hálózati határponton megállíthatjuk a gyanús forgalmakat.