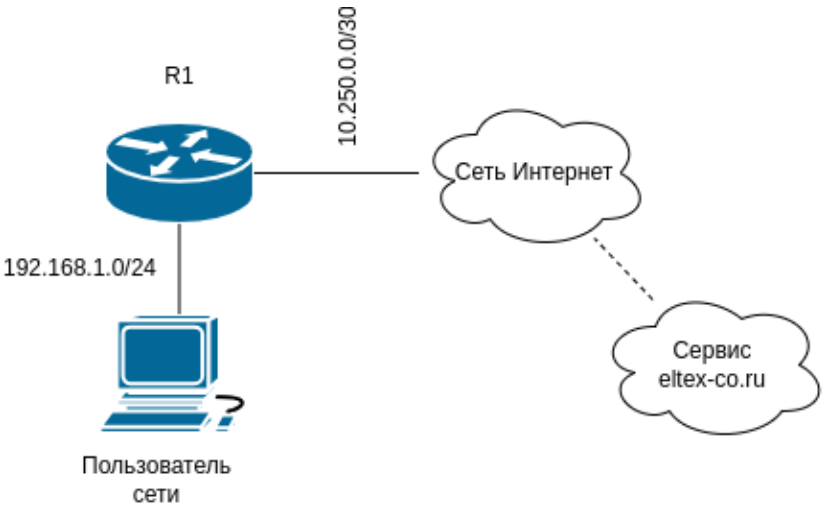
# DNS-  IPS




: IPS/IDS etlex-co.ru.

, . gi1/0/1 :

```
interface gigabitethernet 1/0/1
  security-zone untrusted
  ip address 10.0.0.1/30
exit
```

gi1/0/2 :

```
interface gigabitethernet 1/0/2
  security-zone trusted
  ip address 192.168.1.1/24
exit
```

IPS/IDS, . . :

```
esr# show licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    ESR-200
S/N:     NP00000000
MAC:     00:00:00:00:00:00
Features:
 IPS - Intrusion Prevention System
```

. object-groupe :

```
object-group network NET_IPS
  ip prefix 192.168.1.0/24
exit

security ips policy POL_IPS
  protect network-group NET_IPS
exit

security ips
  policy POL_IPS
  enable
exit
```

, dns- . etlex-co.ru.

```
security ips-category user-defined DNS_DENY
  rule-advanced 10
    enable
    rule-text 'drop dns any any -> any any (msg:"DNS Signature detected"; dns_query; content:"eltex-co.ru";
nocase; sid:10002;)'
  exit
exit
```

, . :

```
esr# config
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# service-ips inline
esr(config-if-gi)# end
esr# commit
esr# confirm
```

***dns- ,*** DNS - . eltex-co.ru, .

, . ESR Surikata 4.0. : https://docs.suricata.io/en/suricata-4.0.5/index.html