ESET – Firewall – Windows update – RDP, printer, scanner i/ili druge mrežne usluge nisu dostupne

Tema

Ponekad se dogodi da mrežne usluge računala (RDP, mrežni printer, skener, …) nisu više dostupne nakon Windows Updatea.

Ovaj postupak može pomoći i kada ESET-ovi programi javljaju poruku “ARP Cache Poisoning attack” (“Napad onečišćenjem ARP predmemorije”).

Uzrok

ESET tijekom instalacije i temeljne konfiguracije namjesti svoj firewall da preuzme postavke Windowsa. No, ponekad Windows Update promijeni postavke filtriranja mrežnog prometa koje onda utječu i na postavke ESET-ovog program koje treba ažurirati. Također, ESET tijekom instalacije preuzima neke postavke Windows Firewalla, pa ovisi i o toj konfiguraciji.

Rješenje

Na jedan od sljedećih načina možete svoju lokalnu mrežu proglasiti sigurnom, pa se blokade ubuduće ne bi trebale odnositi na nju.

Opisane postupke treba obaviti na računalu koje ima scanner ili printer koji trebaju biti dostupni (svima) u mreži ili na računalu kojemu putem RDP-a pristupaju korisnici s lokalne mreže.

Važno: prije primjene pravila iz ovog članka provjerite želite li zaista dopustiti pristup baš svima iz svog LAN-a; možda se na neka računala treba (smije) pristup dopustiti samo određenim uređajima s mreže, pa ograničite sukladno popisu.

Prvi korak

Prvo morate dobiti podatke o svojoj mreži što je najlakše putem Powershella za Windows:

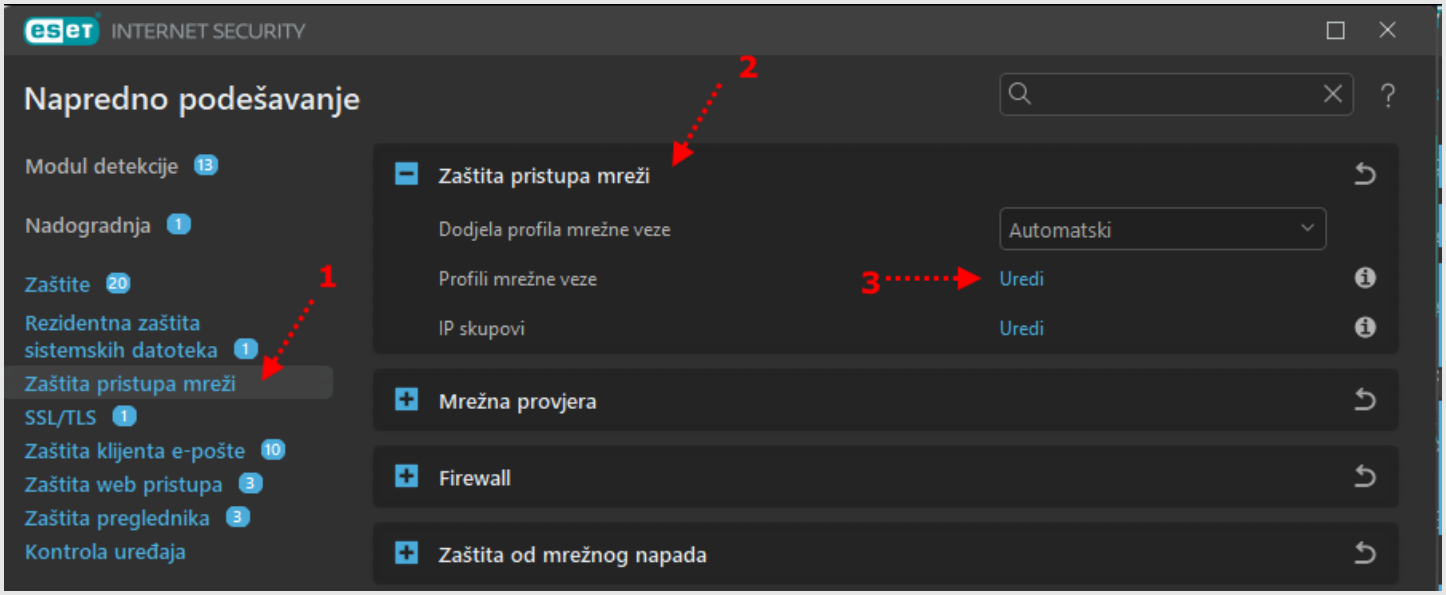
```
Get-NetIPAddress | Where-Object { $_.AddressFamily -eq "IPv4" -and $_.PrefixOrigin -ne "WellKnown" } | Select-Object IPAddress, PrefixLength, InterfaceAlias
```

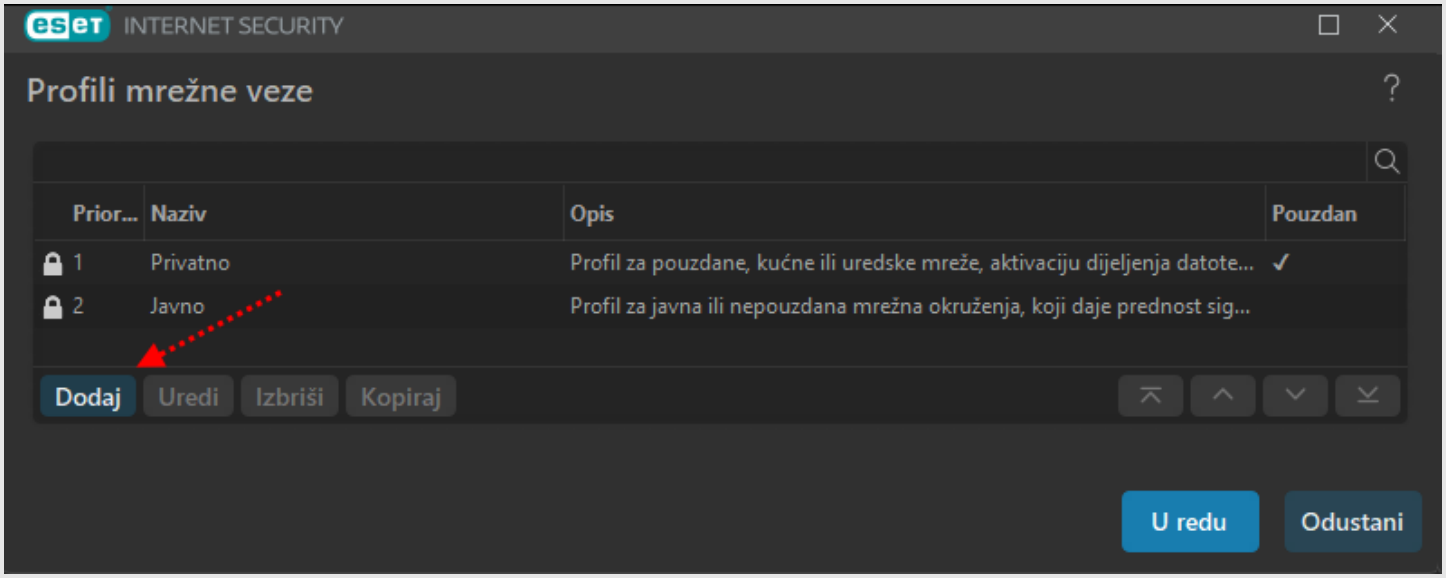
..ili Basha za Linux:

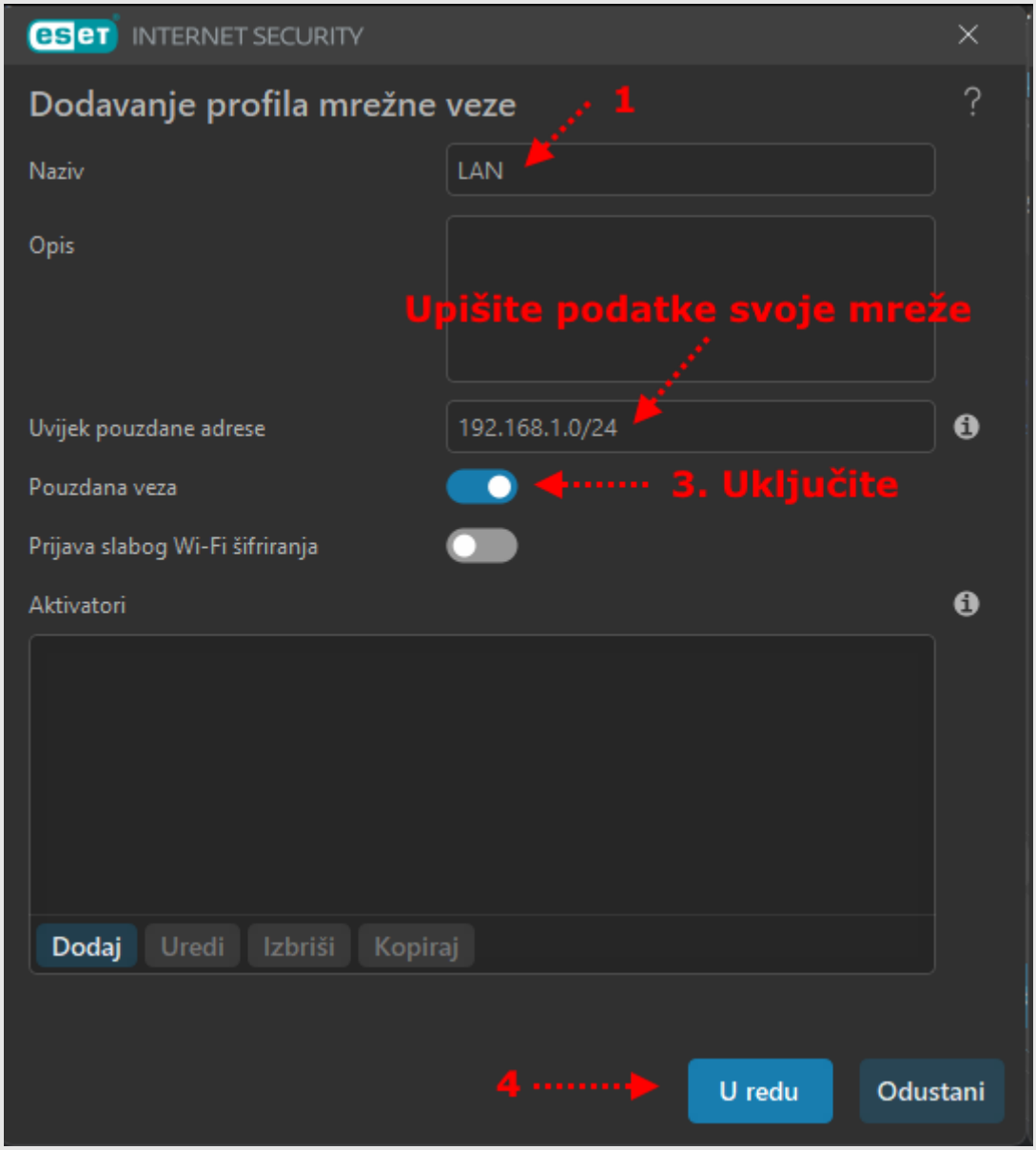
```
ip -o -f inet addr show
```

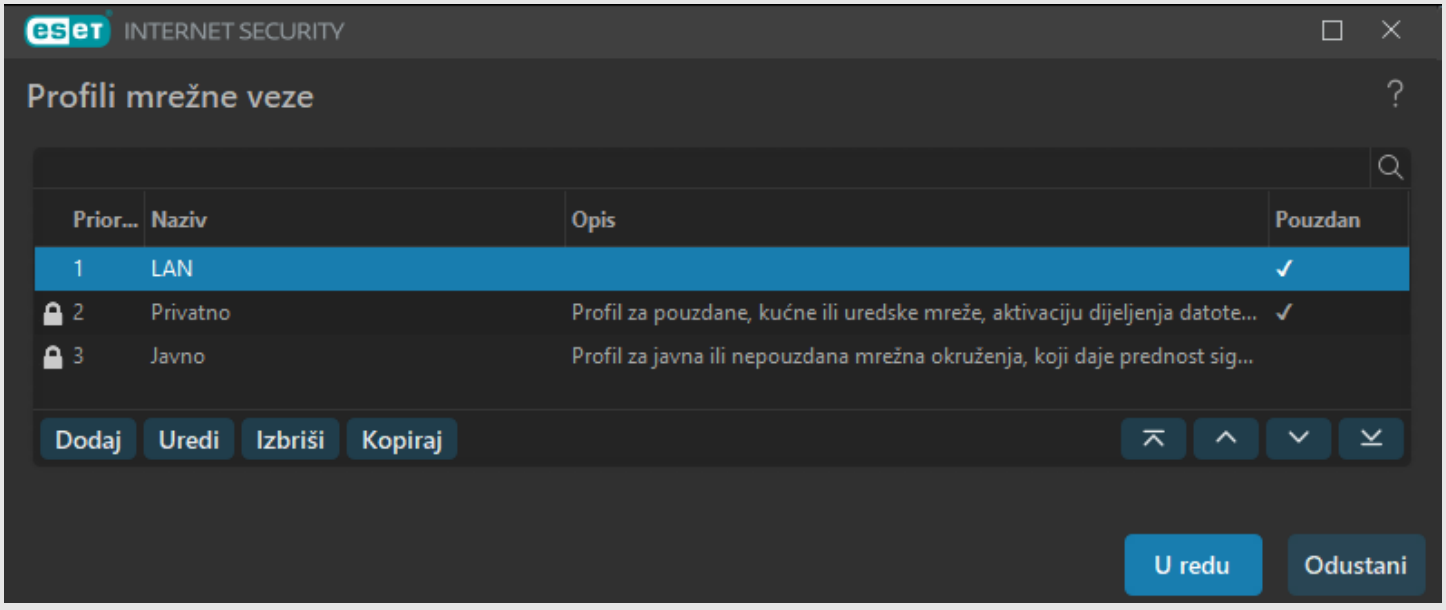
Home programi

Postupak 1 – Profili mrežne veze – Dopuštanje pristupa svima s lokalne mreže

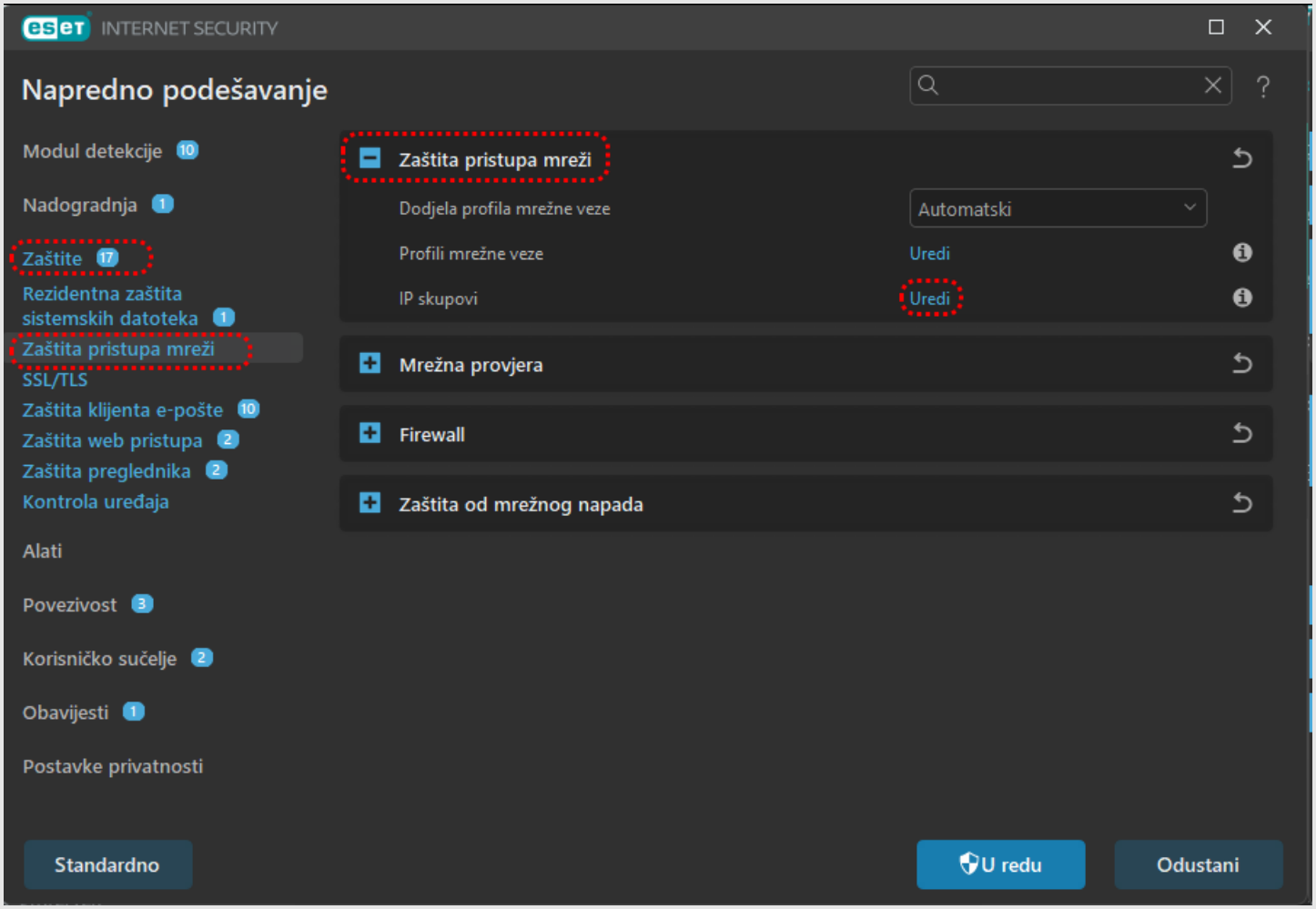


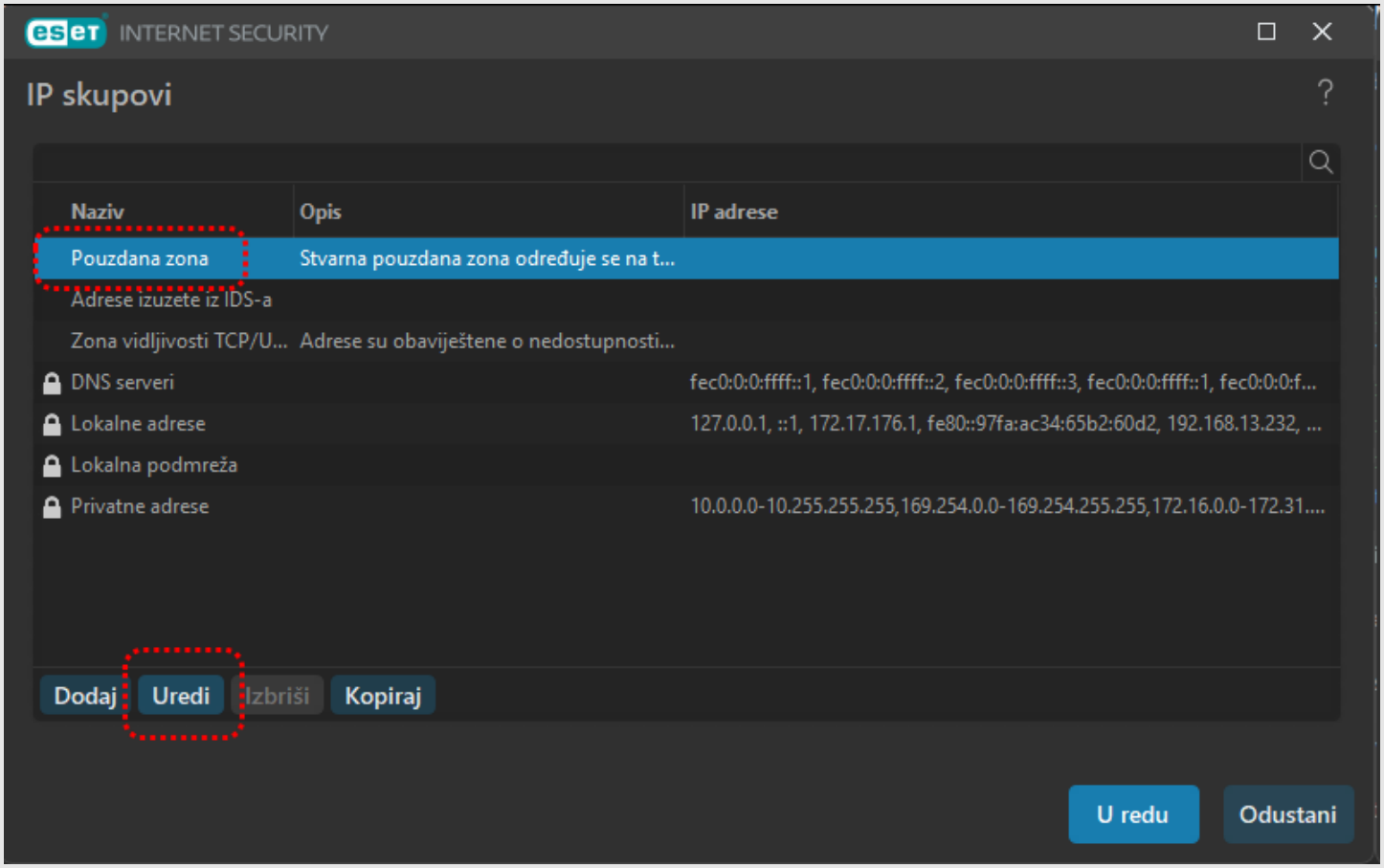


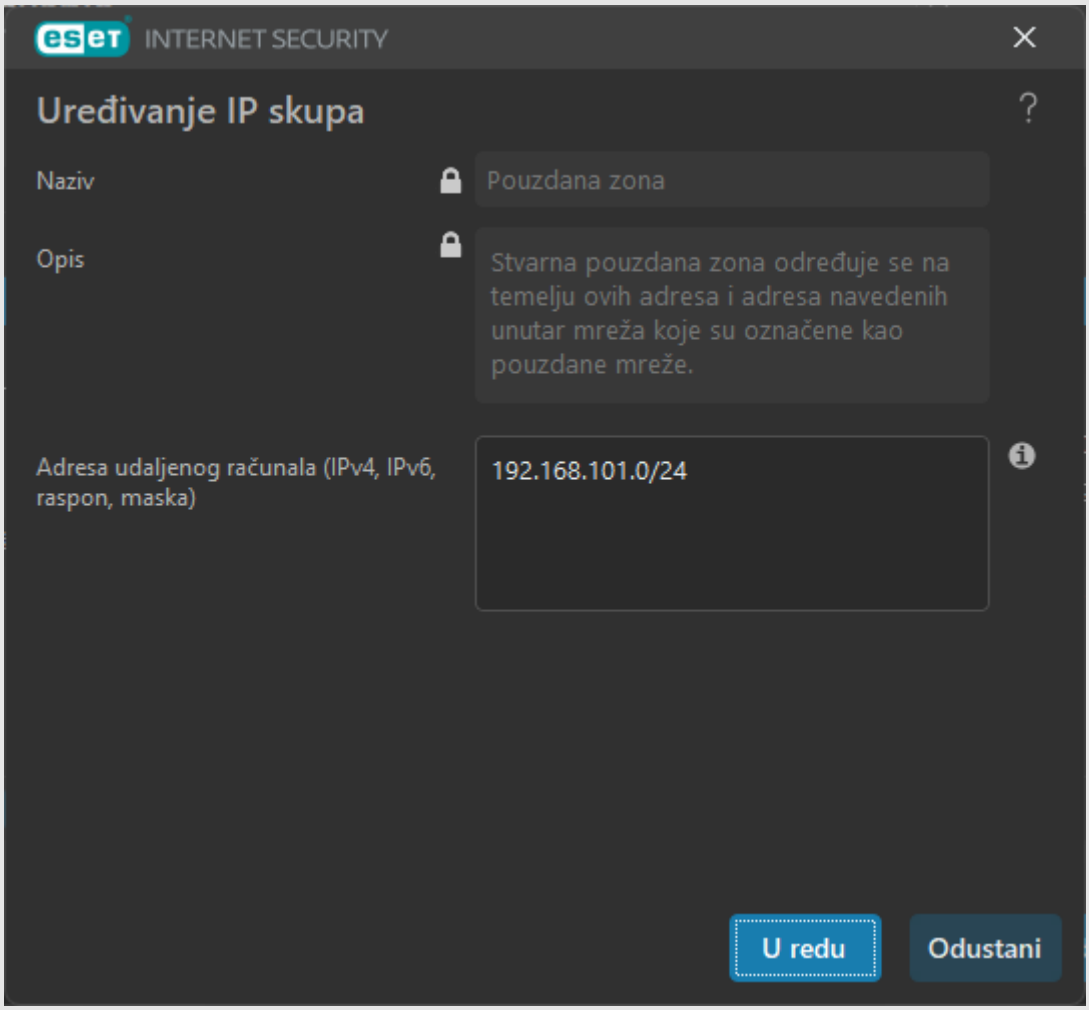

INTERNET SECURITY
Dodavanje profila mrežne veze
1
Naziv
LAN
Opis
Upišite podatke svoje mreže
Uvijek pouzdane adrese
192.168.1.0/24
Pouzdana veza
3. Uključite
Prijava slabog Wi-Fi šifriranja
Aktivatori
Dodaj
Uredi
Izbriši
Kopiraj
4
U redu
Odustani


INTERNET SECURITY
Profili mrežne veze
Prior...
Naziv
Opis
Pouzdan
1
LAN
2
Privatno
Profil za pouzdane, kućne ili uredske mreže, aktivaciju dijeljenja datote...
3
Javno
Profil za javna ili nepouzdana mrežna okruženja, koji daje prednost sig...
Dodaj
Uredi
Izbriši
Kopiraj
U redu
Odustani

Postupak 2A – Stavljanje “IP skupova” pod sigurnu zonu

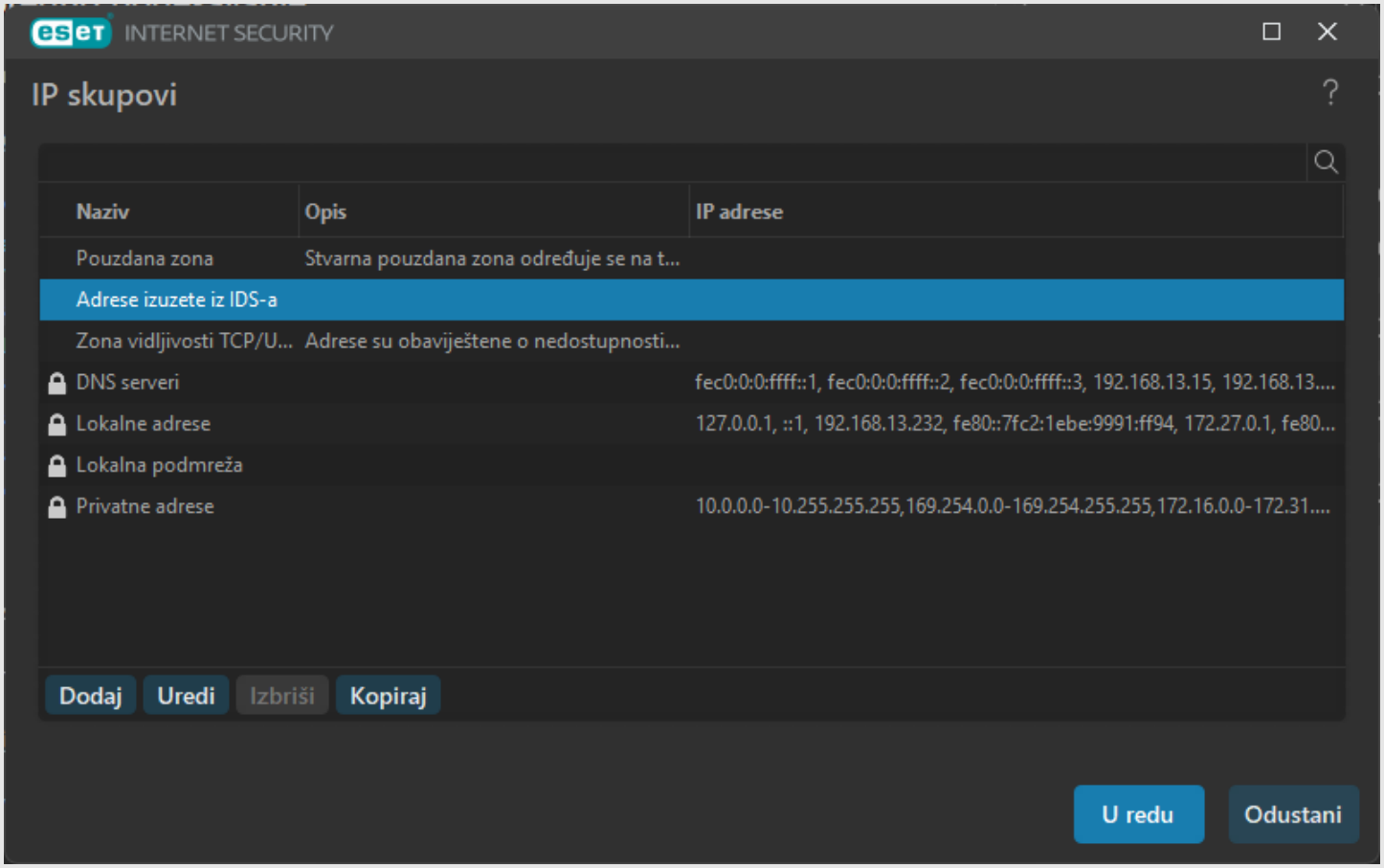



INTERNET SECURITY
IP skupovi
Naziv
Opis
IP adrese
Pouzdana zona
Stvarna pouzdana zona određuje se na t...
Adrese izuzete iz IDS-a
Zona vidljivosti TCP/U...
Adrese su obaviještene o nedostupnosti...
DNS serveri
fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3, fec0:0:0:ffff::1, fec0:0:0:f...
Lokalne adrese
127.0.0.1, ::1, 172.17.176.1, fe80::97fa:ac34:65b2:60d2, 192.168.13.232, ...
Lokalna podmreža
Privatne adrese
10.0.0.0-10.255.255.255,169.254.0.0-169.254.255.255,172.16.0.0-172.31....
Dodaj
Uredi
Izbriši
Kopiraj
U redu
Odustani

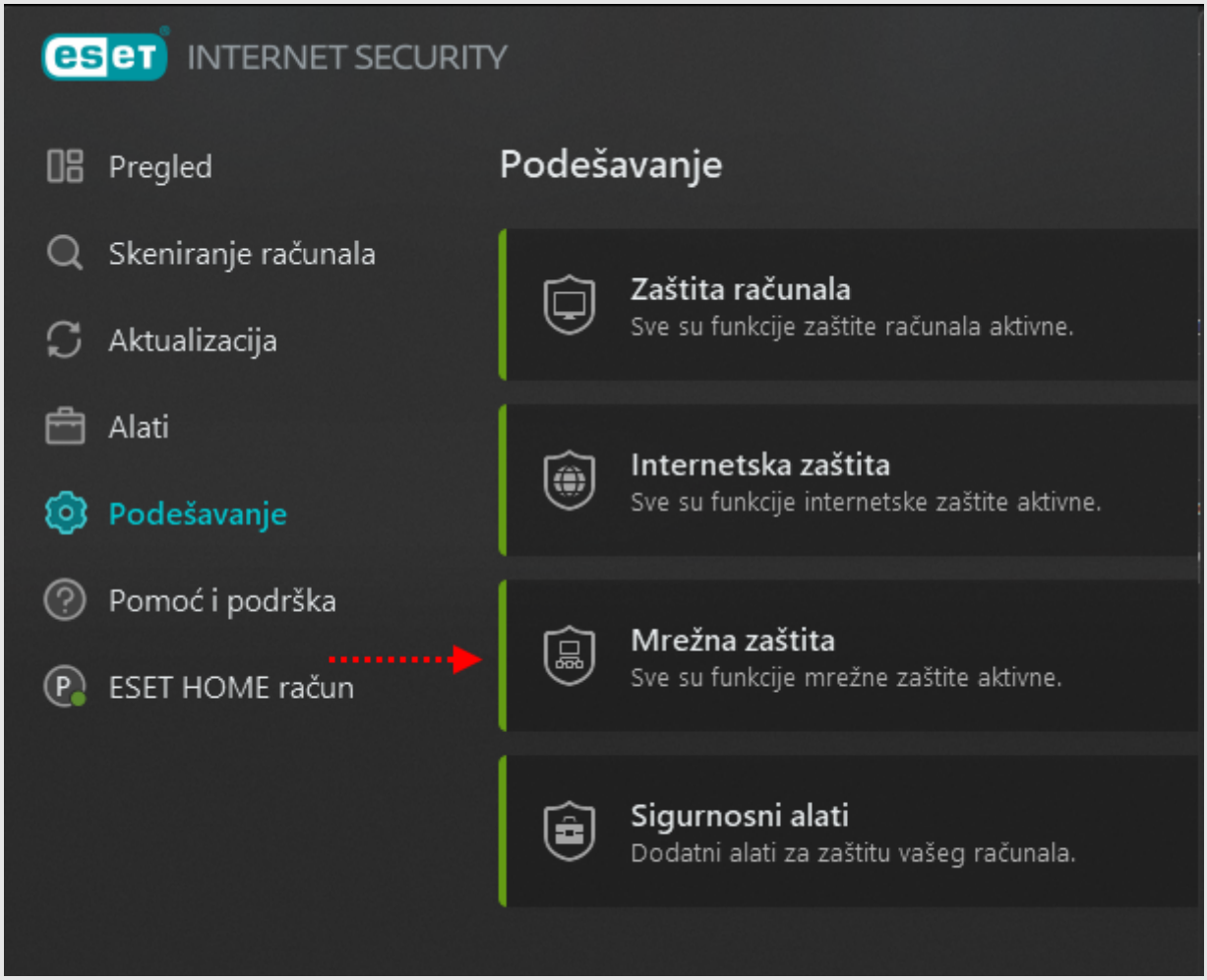

INTERNET SECURITY
Uređivanje IP skupa
Naziv
Pouzdana zona
Opis
Stvarna pouzdana zona određuje se na temelju ovih adresa i adresa navedenih unutar mreža koje su označene kao pouzdane mreže.
Adresa udaljenog računala (IPv4, IPv6, raspon, maska)
192.168.101.0/24
U redu
Odustani

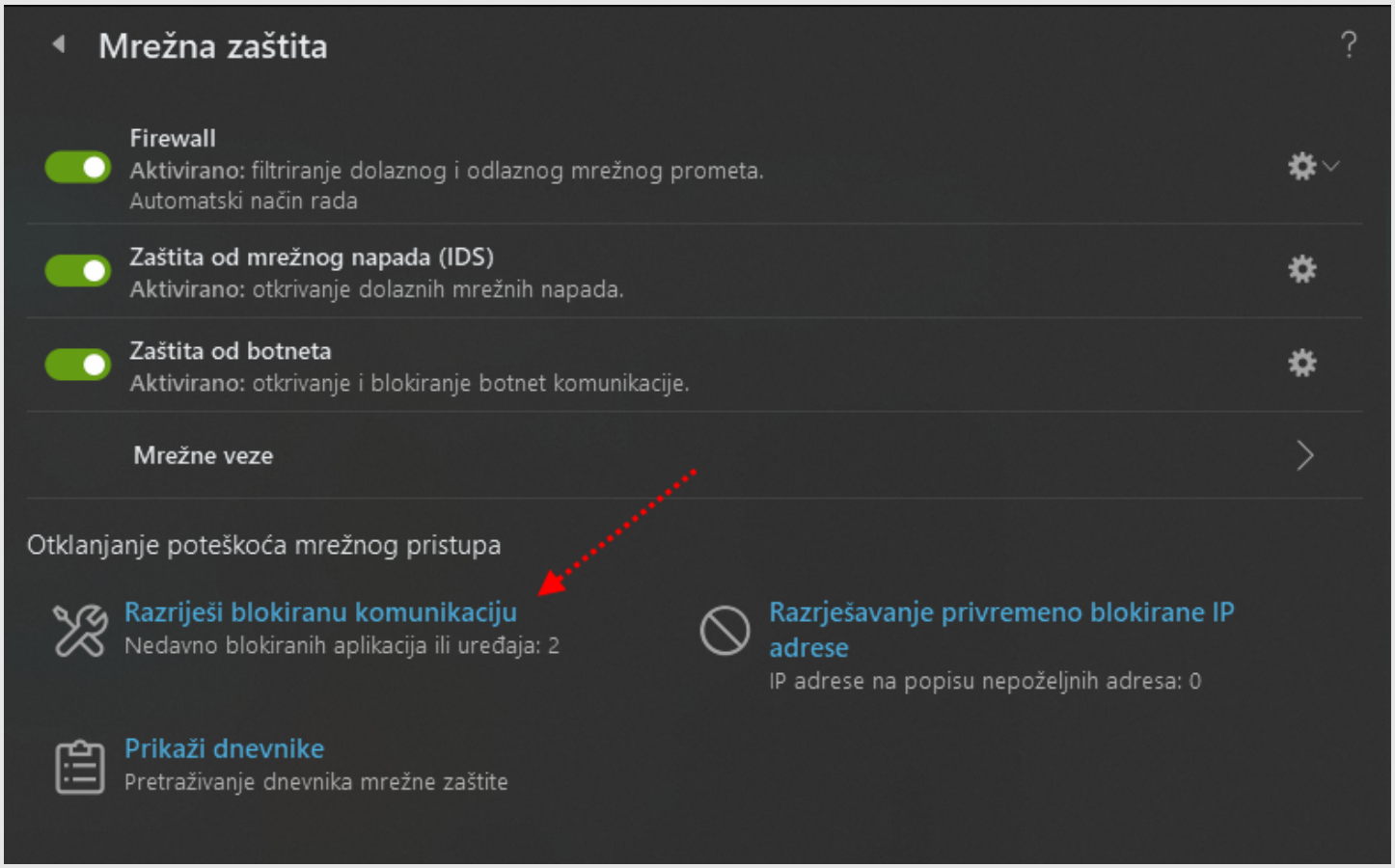
Postupak 2B – “IDS” – Izuzimanje adresa iz lokalne mreže od blokade

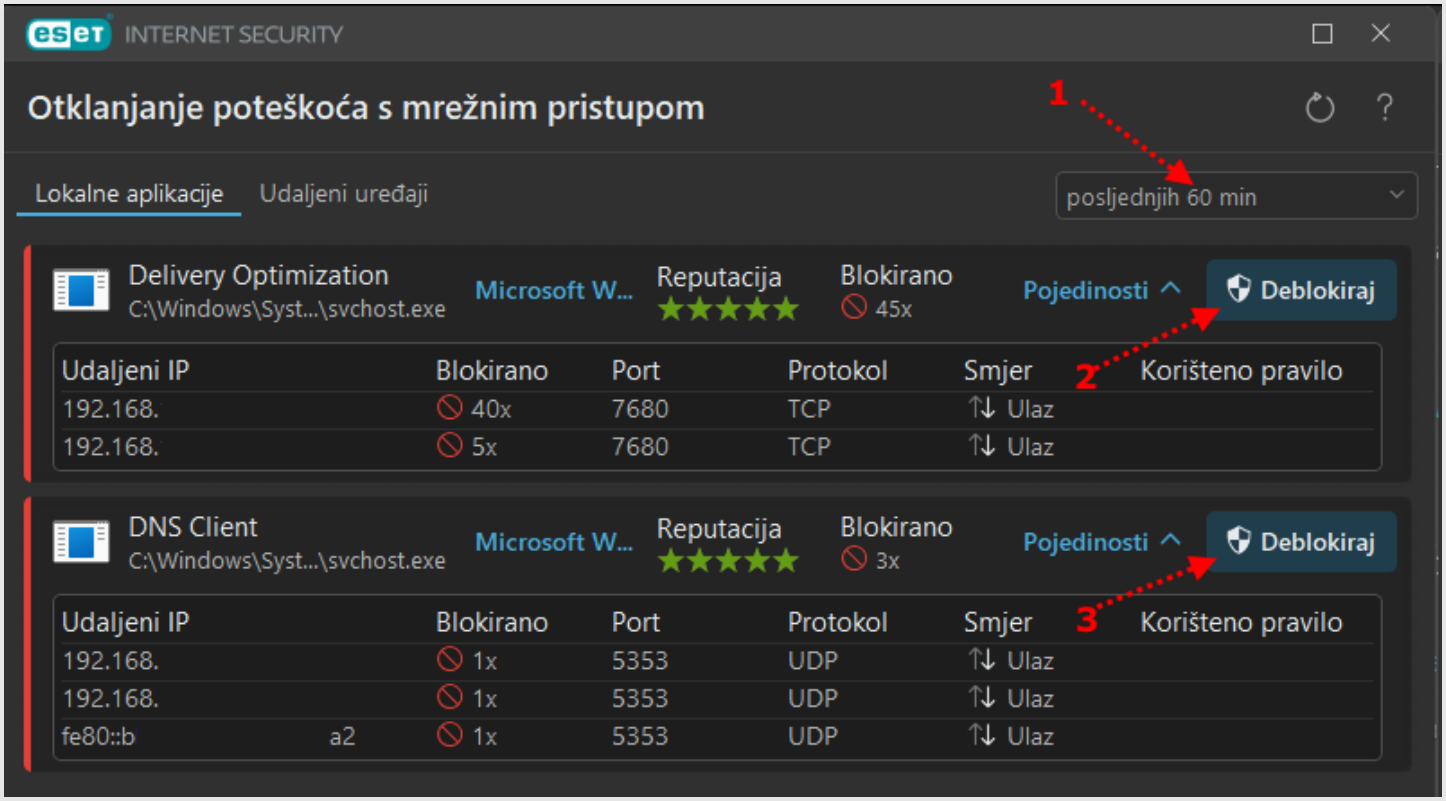
Sljedeća opcija je da na isti način svoju mrežu dodate u “Adrese izuzete iz IDS-a”:



Postupak 3 – Deblokiranje pojedinačnih događaja

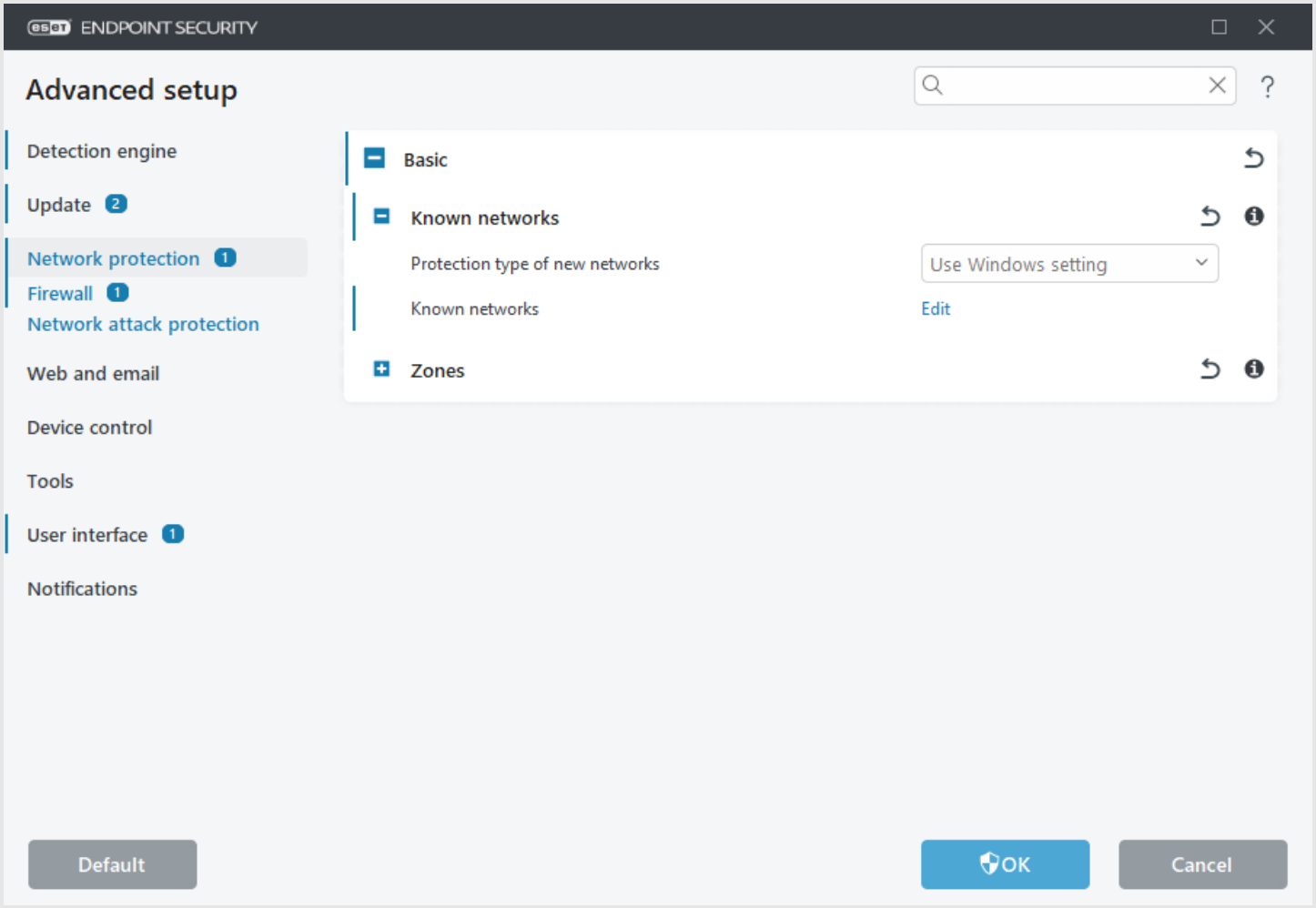

eset INTERNET SECURITY
Pregled
Skeniranje računala
Aktualizacija
Alati
Podešavanje
Pomoć i podrška
ESET HOME račun
Podešavanje
Zaštita računala
Sve su funkcije zaštite računala aktivne.
Internetska zaštita
Sve su funkcije internetske zaštite aktivne.
Mrežna zaštita
Sve su funkcije mrežne zaštite aktivne.
Sigurnosni alati
Dodatni alati za zaštitu vašeg računala.

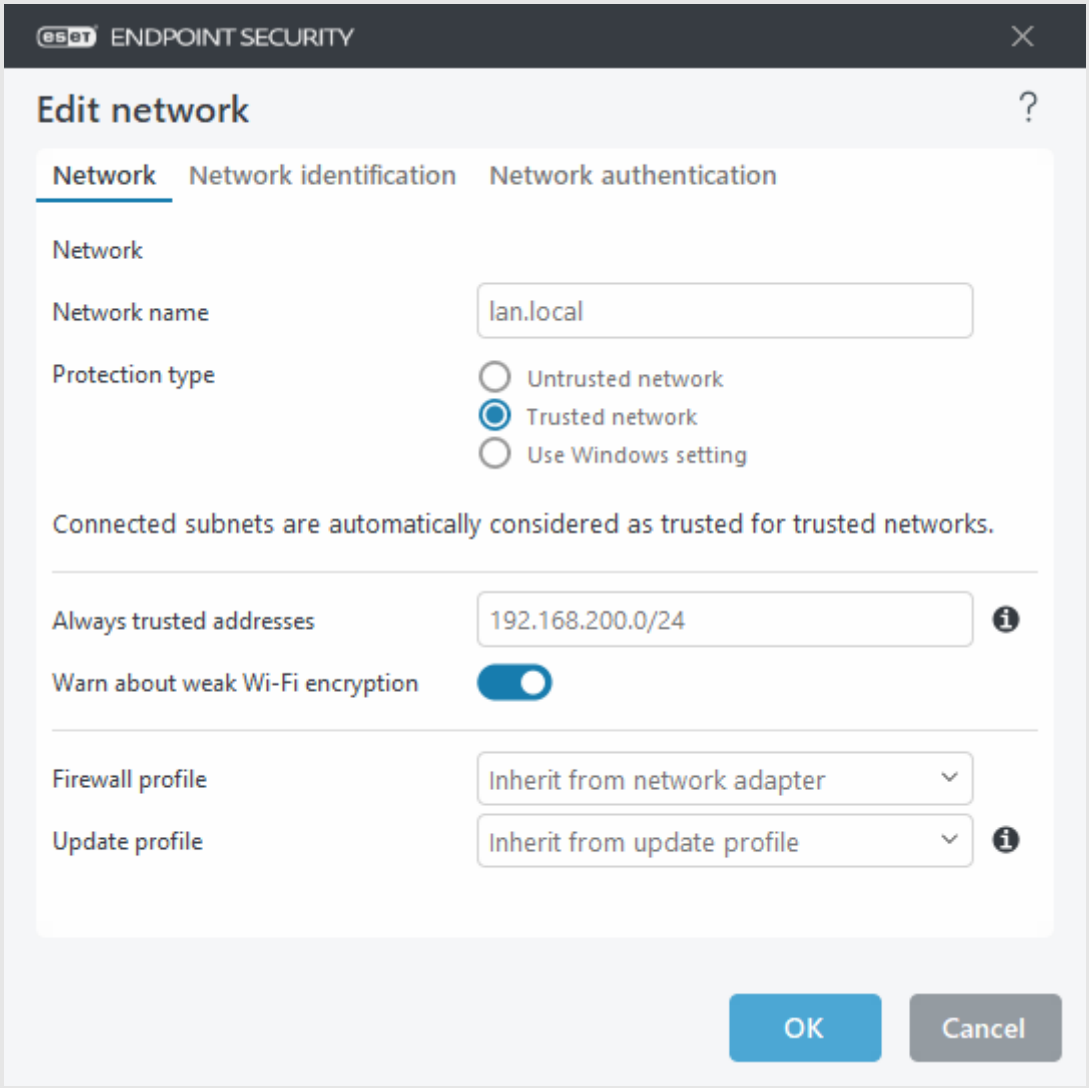

Mrežna zaštita
Firewall
Aktivirano: filtriranje dolaznog i odlaznog mrežnog prometa.
Automatski način rada
Zaštita od mrežnog napada (IDS)
Aktivirano: otkrivanje dolaznih mrežnih napada.
Zaštita od botneta
Aktivirano: otkrivanje i blokiranje botnet komunikacije.
Mrežne veze
Otklanjanje poteškoća mrežnog pristupa
Razriješi blokiranu komunikaciju
Nedavno blokiranih aplikacija ili uređaja: 2
Razrješavanje privremeno blokirane IP adrese
IP adrese na popisu nepoželjnih adresa: 0
Prikaži dnevnike
Pretraživanje dnevnika mrežne zaštite



Poslovni programi

Cjelina je nazvana “Known networks” (“Poznate mreže”)


ENDPOINT SECURITY
Advanced setup
Detection engine
Update 2
Network protection 1
Firewall 1
Network attack protection
Web and email
Device control
Tools
User interface 1
Notifications
Basic
Known networks
Protection type of new networks
Use Windows setting
Known networks
Edit
Zones
Default
OK
Cancel



Razno

U pravilu nije potrebno restartati računalo nakon ovih promjena.

ESET-ovi članci

Postupak 1 = Network connection profiles: https://help.eset.com/essp/17/en-US/?idh_config_epfw_profile.html

Postupak 2A = IP sets:
https://help.eset.com/essp/latest/en-US/idh_dialog_epfw_zones_page.html?idh_dialog_epfw_zones_page.html

Postupak 2B = Exclude an IP address from IDS in ESET Windows home products (verzija 15.x – 16.x):
https://support.eset.com/en/kb2939-exclude-an-ip-address-from-ids-in-eset-windows-home-products

Postupak 3 = Resolve blocked communication:

https://help.eset.com/essp/latest/en-US/idh_page_epfw_blacklist.html

---

firewall xfirewall fw xfw block xblock unblock xunblock iprange xiprange xrange xraspon raspon known xknown trusted xtrusted pouzdane xpouzdane izuzeće xizuzeće exclusion xexclusion xexclude exclude /24 24 x24 rule xrule lan xlan local network xlocal xnetwork blokiran xblokiran arp cache xarp xcache icmp xicmp known network xknown xnetwork razriješi blokiranu komunikaciju xrazriješi xblokiranu xkomunikaciju