ESET Bridge nginx proxy – Dijagnostika

Kao i uvijek, “Korak ” u aktivnostima na bilo kojem serveru: prije ikakve radnje napravite disk-image backup / snapshot / checkpoint / …

Što detaljnije provedete testove i što više preciznih podataka pošaljete “u prvom naletu” – to kraće će trajati dijagnosticiranje i to manje potpitanja ćemo imati.

Provjera konfiguracije

- Radi li servis?
- Zahtijeva li username/password za spajanje?
- Imaju li endpointi specificiran taj user/pass u policyju?
- Imate li drugi proxy putem kojega se ovaj spaja na internet? Je li sve u redu konfigurirano?
- Traži li drugi proxy username/password?
- Propušta li firewall sav promet s ovog proxyja?

Restart servera (ne samo servisa)

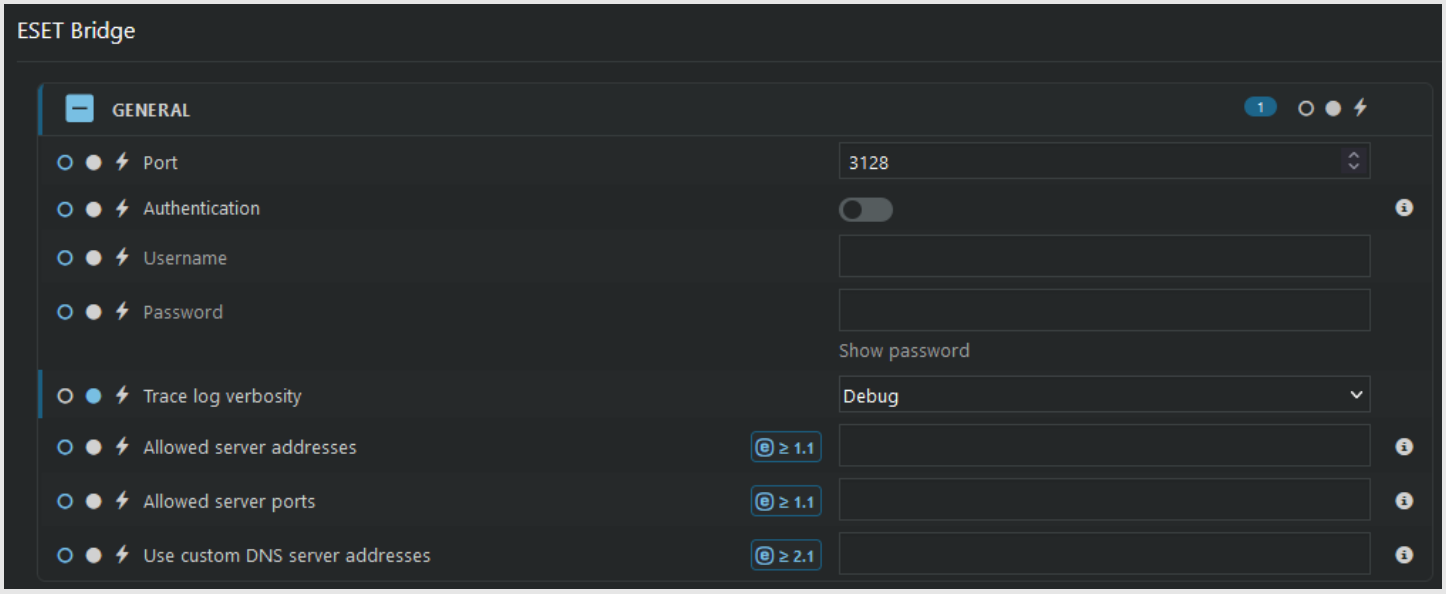
Prije nastavka – prvo restartajte cijeli ESET Protect server (nemojte restartati samo Bridge servis).

Ako se problem pojavljuje i dalje, slijedite donje upute.

Debug mode

Postavite ESET Protect (EPX) policy za ESET Bridge na

“`Trace log verbosity = Debug`“



Provjera proksija

Neki testovi se odrađuju Powershellom, pa testiranje pokrenite na Windows 10 / 11 računalu.

Windows

Bridge je instaliran na Windows serveru – test v1

Test

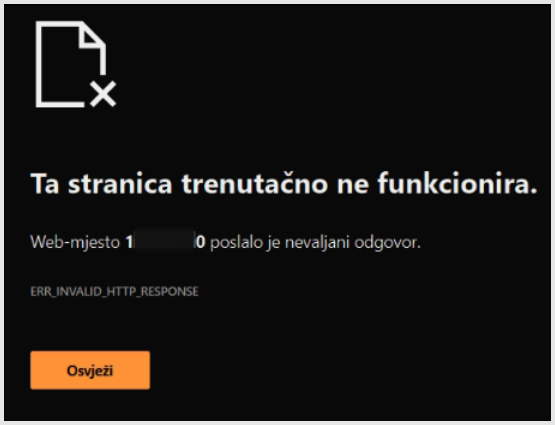
Pokrenite [Firefox | Chrome | MSEdge]
Otvorite stranicu

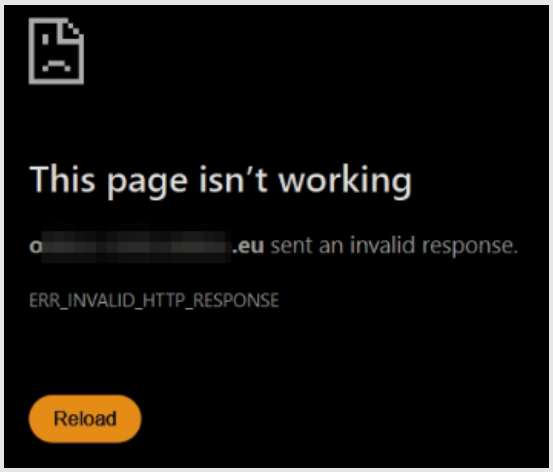
```
http://<$ProxyIP>:<$ProxyPort>/index.html
```

Rezultat

Mora se pojaviti tekst "`403 forbidden / nginx`" i to znači da je ovaj način povezivanja ispravan:

Ako kao rezultat dobijete nešto drugo – uzrok problemima je firewall ili upstream proxy. Npr. “This page isn’t working” error:





Bridge je instaliran na Windows – test v2

Test

```
powershell -command Test-NetConnection -ComputerName $ProxyIP -Port
$ProxyPort -InformationLevel Detailed | Format-List *
```

ili

```
pwsh -command Test-NetConnection -ComputerName $ProxyIP -Port $ProxyPort
-InformationLevel Detailed | Format-List *
```

Rezultat

Uspješan test će prikazati “`TcpTestSucceeded: True`“

```
ComputerName            : <$ProxyIP>
```

```
RemoteAddress           : <$ProxyIP>
RemotePort              : <$ProxyPort>
NameResolutionResults   : <$ProxyIP> <$ProxyComputerName>
MatchingIPsecRules      :
NetworkIsolationContext : Internet
IsAdmin                 : False
InterfaceAlias          : Ethernet
SourceAddress           : <$MojaIPadresa>
NetRoute (NextHop)      : <$GatewayIP>
TcpTestSucceeded        : True   <-----
```

Bridge je instaliran na Windows – test v3

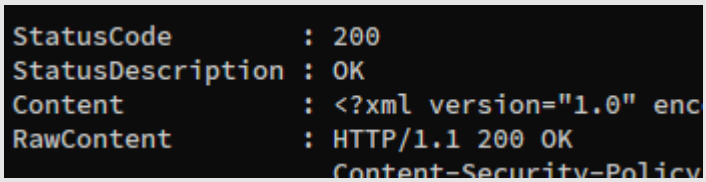
Spajanje na ESET-ove servere

Test

```
powershell -command Invoke-WebRequest -Proxy http://<$ProxyIP>:<$ProxyPort>
-uri https://edf.eset.com/edf -verbose
```

Rezultat

Uspješno povezivanje će vratiti kôd 200
(`StatusCode:200; StatusDescription:OK; RawContent:HTTP/1.1 200 OK`)

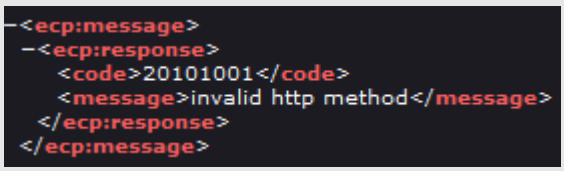


Neuspješno povezivanje uzrokovano firewallom ili upstream proxyjem će vratiti pogrešku “The connection was closed unexpectedly“

Test browserom

Namjestite browser da koristi vaš proxy i otvorite stranicu https://edf.eset.com/edf

Ovakav odgovor pokazuje da je povezivanje moguće:



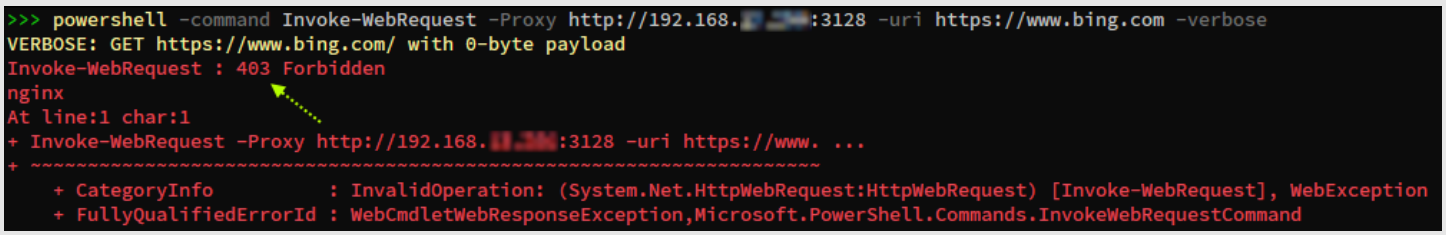
Spajanje na server koji nema veze s ESET-om

Test

```
powershell -command Invoke-WebRequest -Proxy http://<$ProxyIP>:<$ProxyPort>
-uri https://www.bing.com -verbose
```

Rezultat

će biti uspješan ako se pojavi pogreška "`Invoke-WebRequest : 403 Forbidden`" jer proxy u izvornoj konfiguraciji dopušta povezivanje samo s ESET-ovim serverima.



Bridge je instaliran na Windows – test v4

Pregled otvorenih portova

Test

```
Get-NetUDPEndpoint | select
LocalAddress,LocalPort,CreationTime,OwningProcess,@{Name="Process";Expression
={(Get-Process -Id $_.OwningProcess).ProcessName}} | Format-Table
```

Rezultat

```
LocalAddress  LocalPort CreationTime     OwningProcess Process
------------  --------- ------------     ------------- -------
::                55609 2024-06-19 13:18          2592 svchost
::                53873 2024-06-19 11:33          3768 svchost
::                 5355 2024-06-19 11:33          2592 svchost
::                 5353 2024-06-19 11:33          2592 svchost
::                 3702 2024-06-19 11:33          3768 svchost
::                 3389 2024-06-19 11:33          1080 svchost
::                 1434 2024-06-19 11:33          3596 sqlbrowser
::                  123 2024-06-19 11:33          3544 svchost
0.0.0.0           61839 2024-06-19 11:34          1944 ekrn
127.0.0.1         61324 2024-06-19 11:33          1988 svchost
0.0.0.0           54828 2024-06-19 13:18          1944 ekrn
0.0.0.0           53872 2024-06-19 11:33          3768 svchost
0.0.0.0           53505 2024-06-19 11:35          5588 nginx
127.0.0.1         51288 2024-06-19 11:33          3344 svchost
0.0.0.0            5355 2024-06-19 11:33          2592 svchost
0.0.0.0            5353 2024-06-19 11:33          2592 svchost
0.0.0.0            3702 2024-06-19 11:33          3768 svchost
0.0.0.0            3389 2024-06-19 11:33          1080 svchost
0.0.0.0            1434 2024-06-19 11:33          3596 sqlbrowser
192.168             138 2024-06-19 11:33             4 System
192.168             137 2024-06-19 11:33             4 System
0.0.0.0             123 2024-06-19 11:33          3544 svchost
```

Linux

Neke testove provedite iz Linux konzole (može i sa sâmog ESET Protect servera), a neke možete provesti i gornjim Powershell komandama.

Bridge je instaliran na Linux – test v1L

Spajanje na ESET-ove servere

Test

```
wget --no-check-certificate -e use_proxy=yes -e
https_proxy=<$proxyIP>:<$ProxyPort> https://edf.eset.com/edf -O edf.html
```

Rezultat

Mora se pojaviti poruka

```
"awaiting response... 200 OK"
```

```
: wget --no-check-certificate -e use_proxy=yes -e https_proxy=192.168.[redacted]:3128 https://edf.eset.com/edf -O edf.html
--2023-09-05 13:33:42--  https://edf.eset.com/edf
Connecting to 192.168[redacted]:3128... connected.
Proxy request sent, awaiting response... 200 OK
Length: 197 [text/xml]
Saving to: ‘edf.html’

edf.html                                                100%[=========================================================>

2023-09-05 13:33:43 (221 MB/s) - ‘edf.html’ saved [197/197]
```

Spajanje na server koji nema veze s ESET-om

Test

```
wget --debug --no-check-certificate -e use_proxy=yes -e
https_proxy=<$ProxyIP>:<$ProxyPort> https://www.bing.com -O bing.html
```

Rezultat

Mora se pojaviti tekst

```
"proxy responded with: [HTTP/1.1 403 Forbidden server: nginx <...cut...>"
```

```
---request end---
proxy responded with: [HTTP/1.1 403 Forbidden
Server: nginx
Date: Tue, 05 Sep 2023 11:40:51 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

]
```

Bridge je instaliran na Linux – test v2L

Pregled otvorenih portova

Test

```
netstat --all --wide --numeric-hosts --numeric-ports --verbose --extend
--listening --context
```

Rezultat

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name     Security Context
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      root       22697      841/sshd: /usr/sbin  system_u:system_r:sshd_t:s0-s0:c0.c1023
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      root       49918      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 0.0.0.0:2223            0.0.0.0:*               LISTEN      root       49922      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 0.0.0.0:10000           0.0.0.0:*               LISTEN      root       22222      1602/perl            system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4447          0.0.0.0:*               LISTEN      eset-bridge 21993      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4446          0.0.0.0:*               LISTEN      eset-bridge 21992      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4445          0.0.0.0:*               LISTEN      eset-bridge 21991      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4444          0.0.0.0:*               LISTEN      eset-bridge 21989      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4450          0.0.0.0:*               LISTEN      eset-bridge 21995      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:4448          0.0.0.0:*               LISTEN      eset-bridge 21994      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 0.0.0.0:3128            0.0.0.0:*               LISTEN      eset-bridge 21990      1236/nginx: master   system_u:system_r:unconfined_service_t:s0
tcp        0      0 127.0.0.1:50782         127.0.0.1:3306          ESTABLISHED root       53038      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50740         127.0.0.1:3306          ESTABLISHED root       54185      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50788         127.0.0.1:3306          ESTABLISHED root       53039      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50798         127.0.0.1:3306          ESTABLISHED root       53041      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50748         127.0.0.1:3306          ESTABLISHED root       53035      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:2222          127.0.0.1:48492         ESTABLISHED root       50735      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50760         127.0.0.1:3306          ESTABLISHED root       53036      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 192.168       :59460    91.228.167.172:8883     ESTABLISHED root       68868      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50776         127.0.0.1:3306          ESTABLISHED root       53037      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:50794         127.0.0.1:3306          ESTABLISHED root       53040      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        1      0 192.168       :60412    192.168       :3128     CLOSE_WAIT  root       49128      18079/ERAServer      system_u:system_r:eraserver_t:s0
tcp        0      0 127.0.0.1:2223          127.0.0.1:48664         ESTABLISHED root       59563      18079/ERAServer      system_u:system_r:eraserver_t:s0
```

Telnet test

```
telnet <$ProxyIP> <$ProxyPort>
```

ili upotrijebite Microsoftov PortQry.

PortQry test

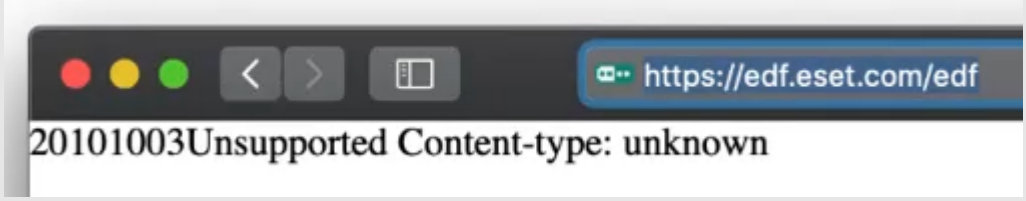
Download: https://www.microsoft.com/en-us/download/details.aspx?id=17148

portqry -sl -v -n <$ProxyIP> -p TCP -e <$ProxyPort>

---

macOS test EDF

Sljedeći odgovor je u redu, spajanje je moguće:



Konfiguracija

• C:\ProgramData\ESET\Bridge\Proxies\Nginx\Conf\nginx.conf

Logovi

Provjerite i dnevnike nginxa:

• C:\ProgramData\ESET\Bridge\Logs\bridge.log
• C:\ProgramData\ESET\Bridge\Logs\watchdog.log
• (watchdog.logYYYYMMDDHHMMSSms)

Napomena

U gornjim testovima zamijenite varijable odgovarajućim vrijednostima:

• `<$ProxyIP>` ... IP adresa ESET Bridge servera u vašem sustavu
• `<$ProxyPort>` ... port ESET Bridge servera u vašem sustavu; standardno je to 3128

Dodatne informacije

https://help.eset.com/ebe/latest/en-US/troubleshooting.html

---

proxy xproxy http xhttp bridge xbridge nginx xnginx test xtest check xcheck probe xprobe troubleshooting trblsht xtroubleshooting xtrblsht debug xdebug diagnostics xdiagnostics