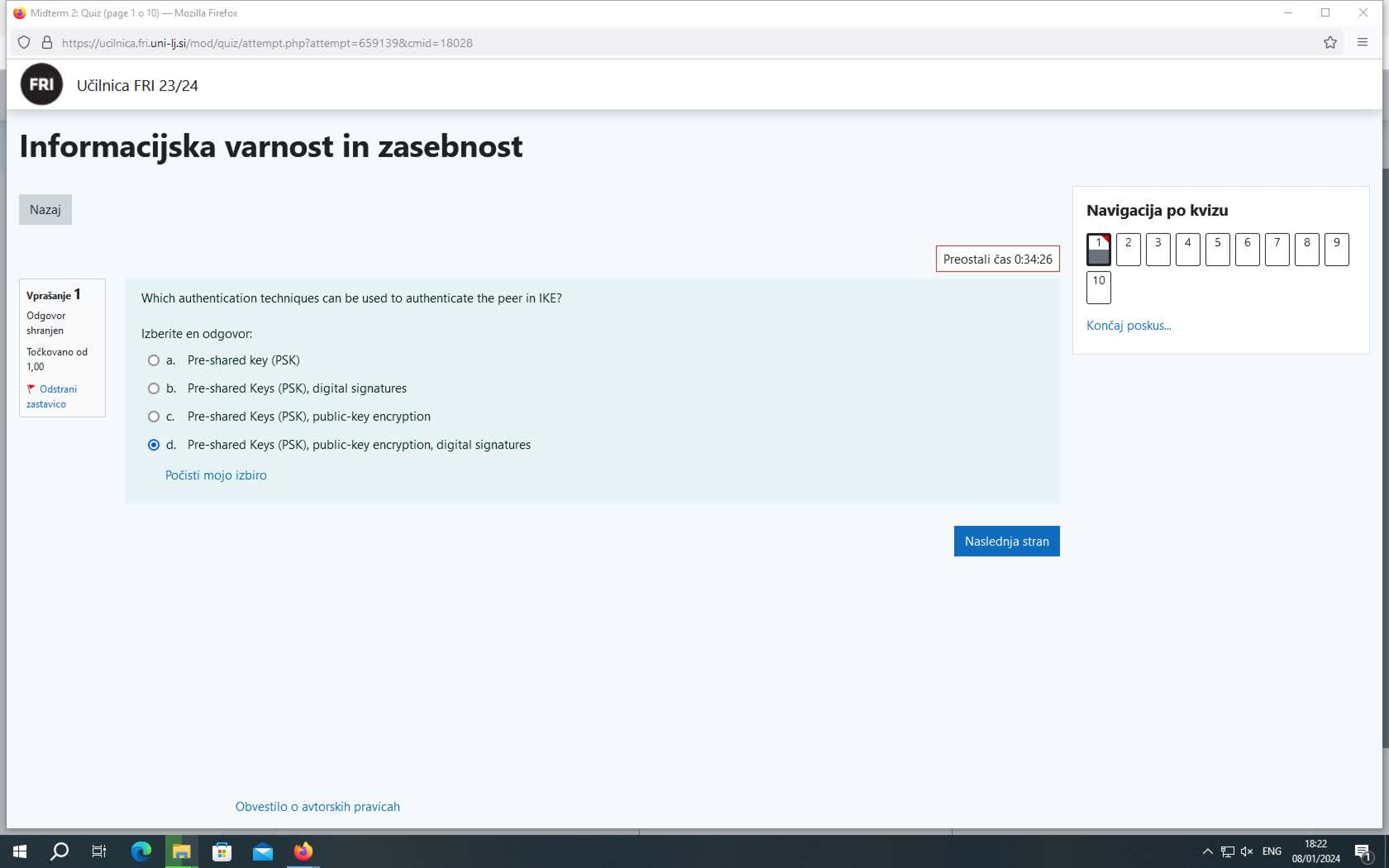

Midterm 2: Quiz (page 1 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028
FRI
Učilnica FRI 23/24

Informacijska varnost in zasebnost

Preostali čas 0:34:26

Vprašanje 1

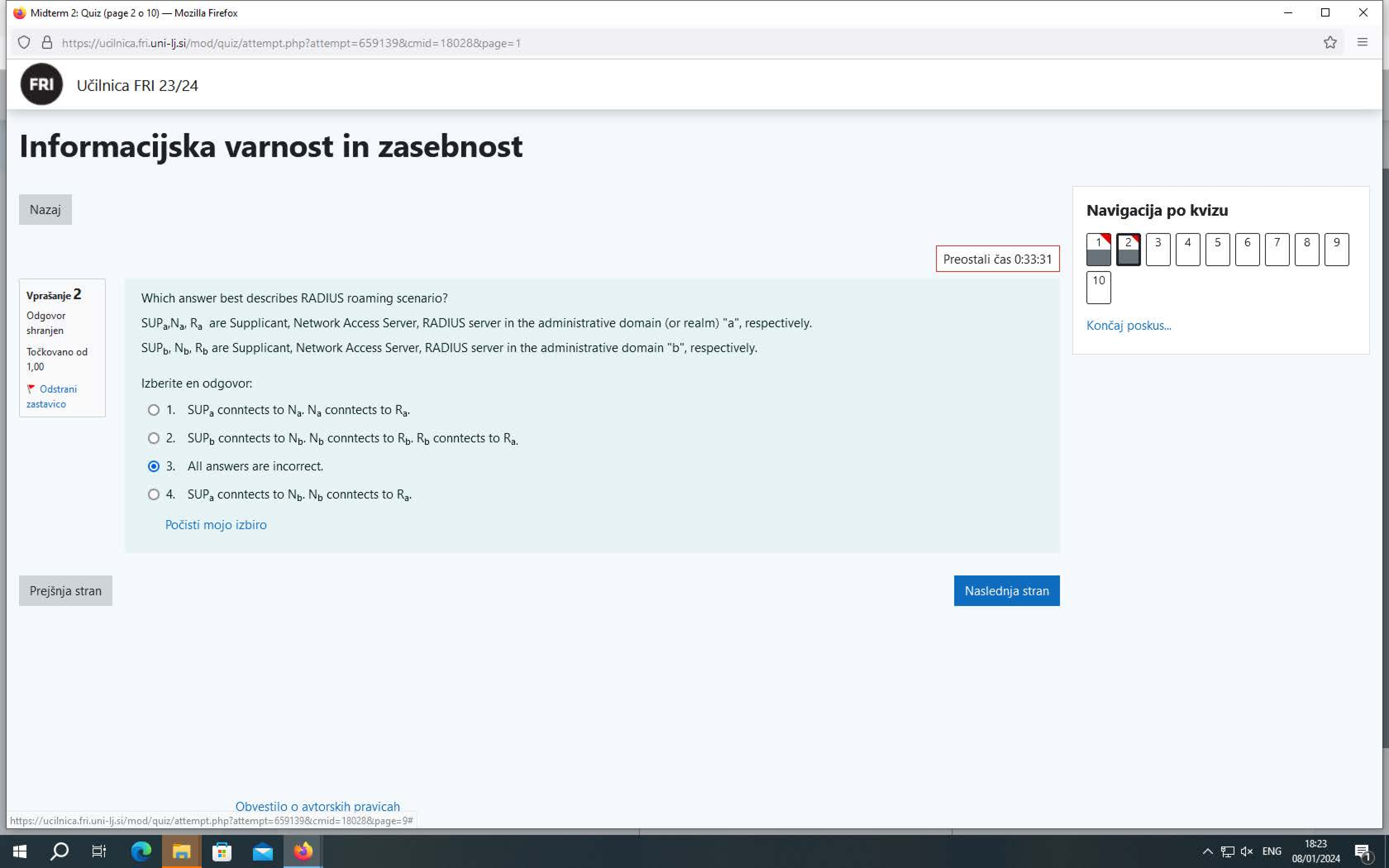
Odgovor shranjen

Točkovano od 1,00

Which authentication techniques can be used to authenticate the peer in IKE?

Izberite en odgovor:

- ○ a. Pre-shared key (PSK)
- ○ b. Pre-shared Keys (PSK), digital signatures
- ○ c. Pre-shared Keys (PSK), public-key encryption
- ● d. Pre-shared Keys (PSK), public-key encryption, digital signatures



Midterm 2: Quiz (page 2 o 10) — Mozilla Firefox

https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=1

FRI Učilnica FRI 23/24

Informacijska varnost in zasebnost

Nazaj

Preostali čas 0:33:31

Vprašanje 2

Odgovor shranjen

Točkovano od 1,00

Odstrani zastavico

Which answer best describes RADIUS roaming scenario?

SUP_a,N_a, R_a are Supplicant, Network Access Server, RADIUS server in the administrative domain (or realm) "a", respectively.

SUP_b, N_b, R_b are Supplicant, Network Access Server, RADIUS server in the administrative domain "b", respectively.

Izberite en odgovor:

○ 1. SUP_a conntects to N_a. N_a conntects to R_a.

○ 2. SUP_b conntects to N_b. N_b conntects to R_b. R_b conntects to R_a.

● 3. All answers are incorrect.

○ 4. SUP_a conntects to N_b. N_b conntects to R_a.

Počisti mojo izbiro

Prejšnja stran

Naslednja stran

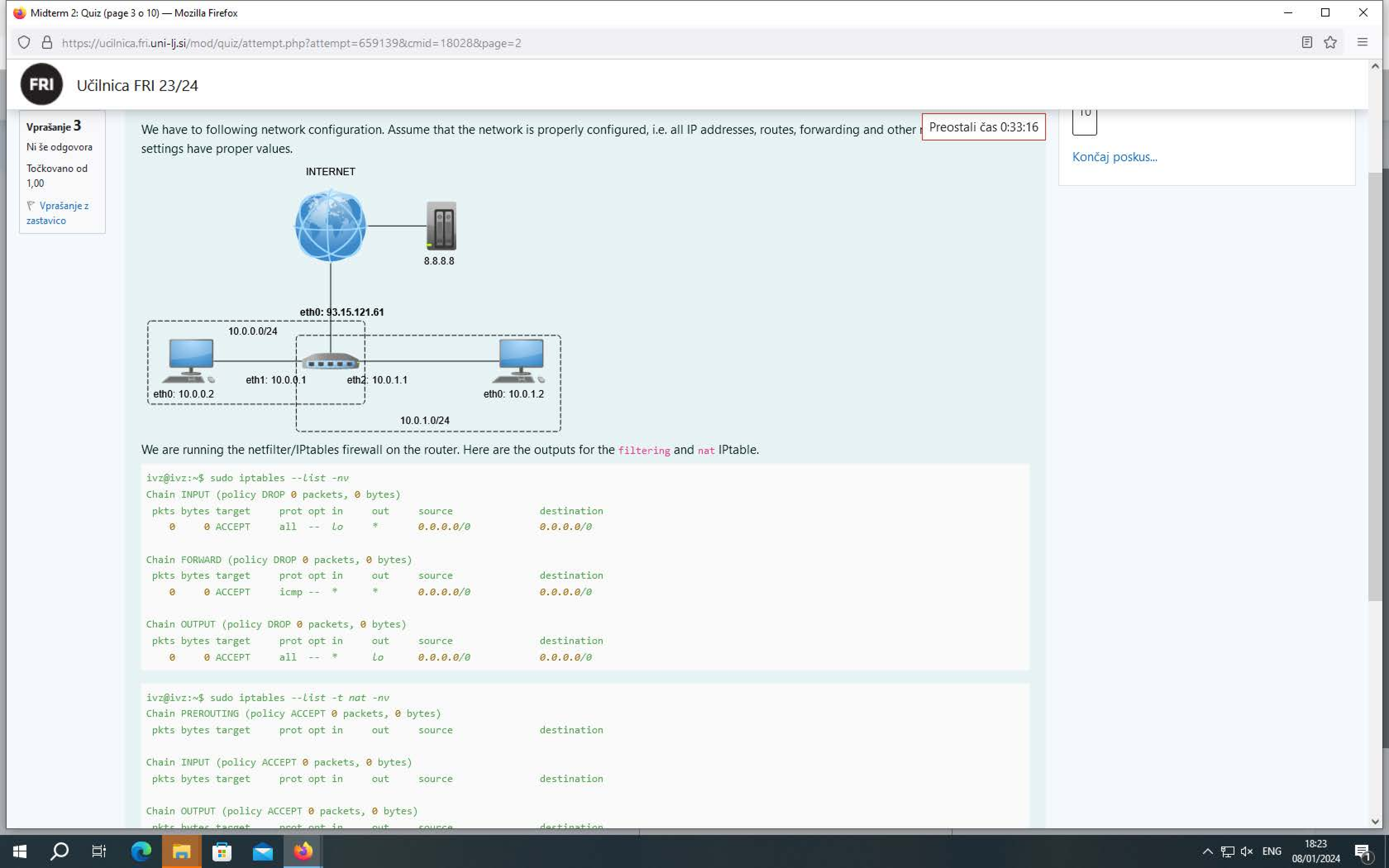
Navigacija po kvizu

1 2 3 4 5 6 7 8 9 10

Končaj poskus...

Obvestilo o avtorskih pravicah

https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=9#


Midterm 2: Quiz (page 3 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=2
FRI
Učilnica FRI 23/24
Preostali čas 0:33:16
10
Končaj poskus...

Vprašanje 3

Ni še odgovora

Točkovano od 1,00

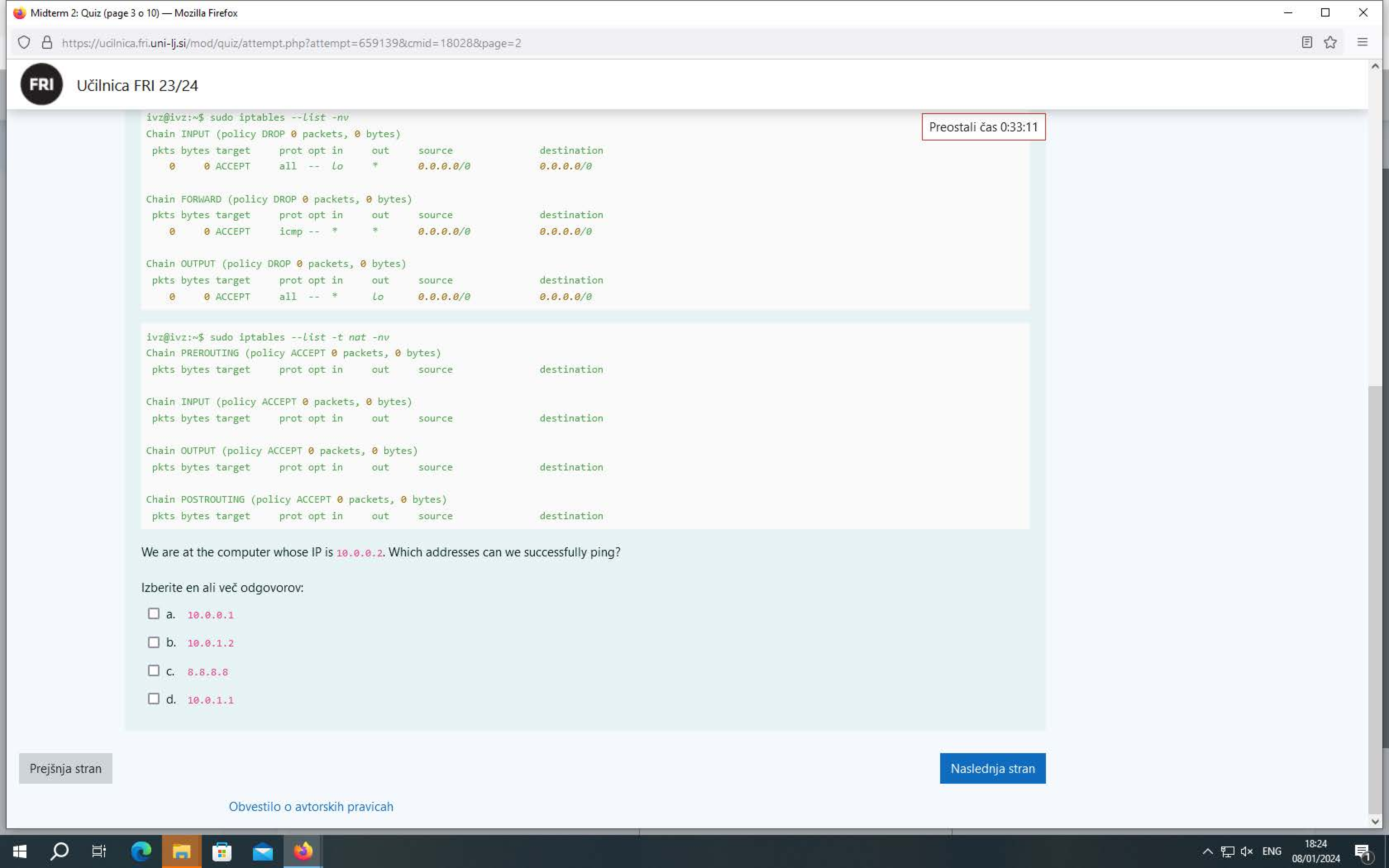
Vprašanje z zastavico

We have to following network configuration. Assume that the network is properly configured, i.e. all IP addresses, routes, forwarding and other r settings have proper values.

We are running the netfilter/IPtables firewall on the router. Here are the outputs for the `filtering` and `nat` IPtable.

```
ivz@ivz:~$ sudo iptables --list -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

```
ivz@ivz:~$ sudo iptables --list -t nat -nv
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```



Midterm 2: Quiz (page 3 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=2
FRI
Učilnica FRI 23/24
Preostali čas 0:33:11

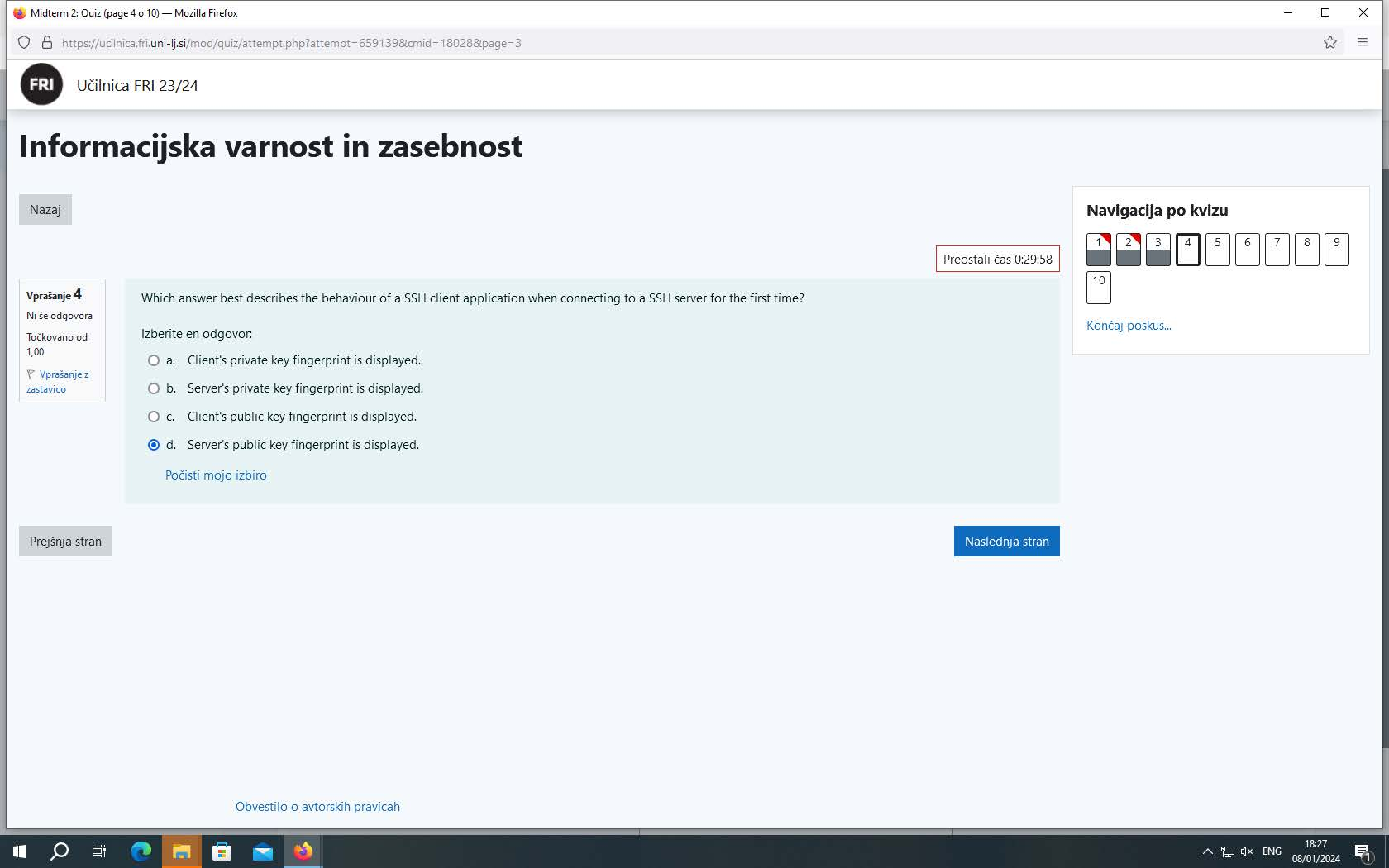
```
ivz@ivz:~$ sudo iptables --list -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

```
ivz@ivz:~$ sudo iptables --list -t nat -nv
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We are at the computer whose IP is `10.0.0.2`. Which addresses can we successfully ping?

Izberite en ali več odgovorov:

- □ a. `10.0.0.1`
- □ b. `10.0.1.2`
- □ c. `8.8.8.8`
- □ d. `10.0.1.1`


Midterm 2: Quiz (page 4 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=3
FRI
Učilnica FRI 23/24
Nazaj
Navigacija po kvizu
1
2
3
4
5
6
7
8
9
10
Končaj poskus...
Preostali čas 0:29:58
Vprašanje z zastavico
Prejšnja stran
Naslednja stran
Obvestilo o avtorskih pravicah
ENG
18:27
08/01/2024

Informacijska varnost in zasebnost

Vprašanje 4
Ni še odgovora
Točkovano od 1,00

Which answer best describes the behaviour of a SSH client application when connecting to a SSH server for the first time?

Izberite en odgovor:

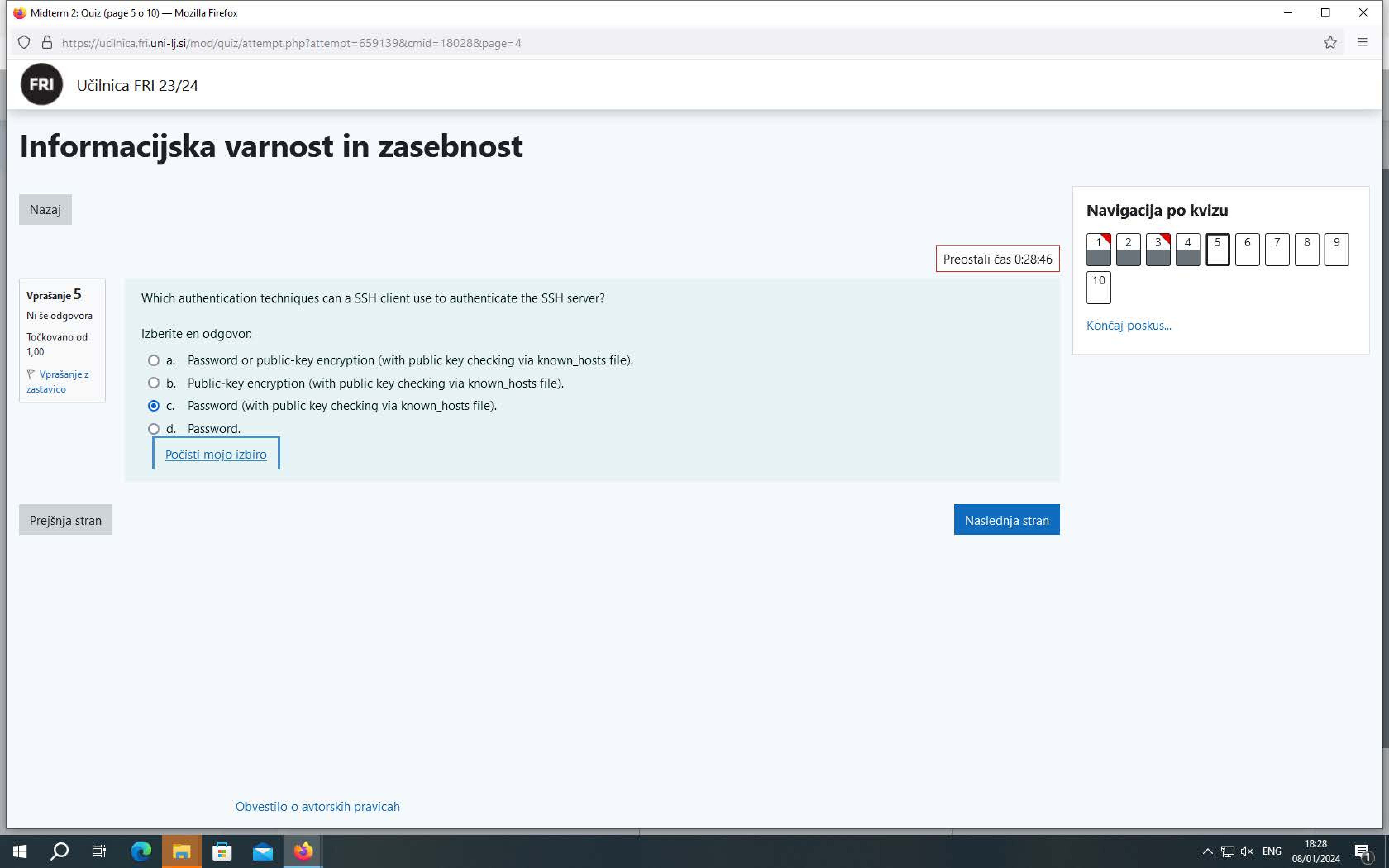
○ a. Client's private key fingerprint is displayed.

○ b. Server's private key fingerprint is displayed.

○ c. Client's public key fingerprint is displayed.

● d. Server's public key fingerprint is displayed.

Počisti mojo izbiro



Midterm 2: Quiz (page 5 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=4
FRI
Učilnica FRI 23/24

Informacijska varnost in zasebnost

Preostali čas 0:28:46

Vprašanje 5

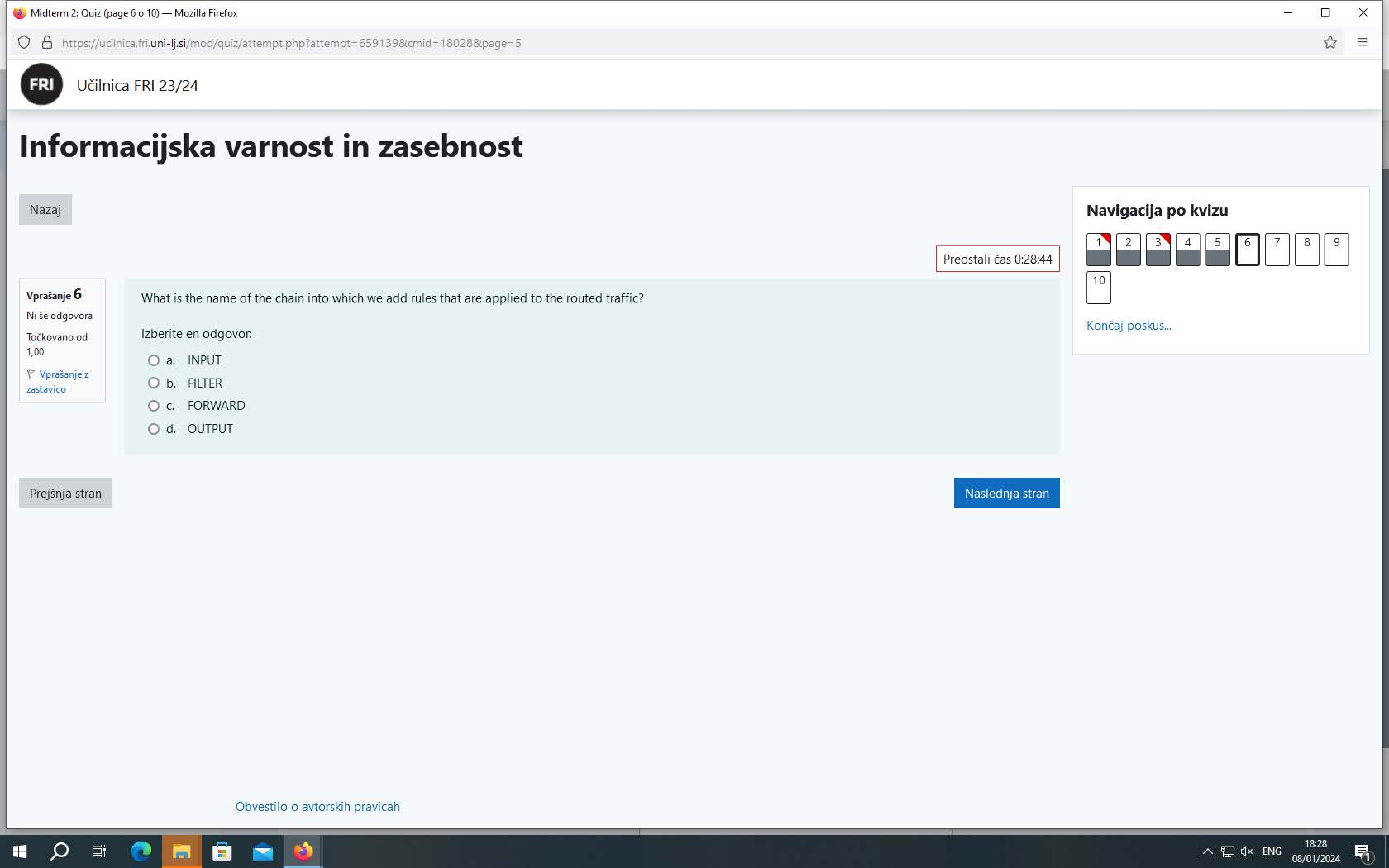
Ni še odgovora

Točkovano od 1,00

Which authentication techniques can a SSH client use to authenticate the SSH server?

Izberite en odgovor:

- ○ a. Password or public-key encryption (with public key checking via known_hosts file).
- ○ b. Public-key encryption (with public key checking via known_hosts file).
- ● c. Password (with public key checking via known_hosts file).
- ○ d. Password.


Midterm 2: Quiz (page 6 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=5
FRI
Učilnica FRI 23/24
Nazaj
Navigacija po kvizu
1 2 3 4 5 6 7 8 9 10
Končaj poskus...
Preostali čas 0:28:44
Prejšnja stran
Naslednja stran
Obvestilo o avtorskih pravicah
ENG
18:28
08/01/2024

Informacijska varnost in zasebnost

Vprašanje 6

Ni še odgovora

Točkovano od 1,00

Vprašanje z zastavico

What is the name of the chain into which we add rules that are applied to the routed traffic?

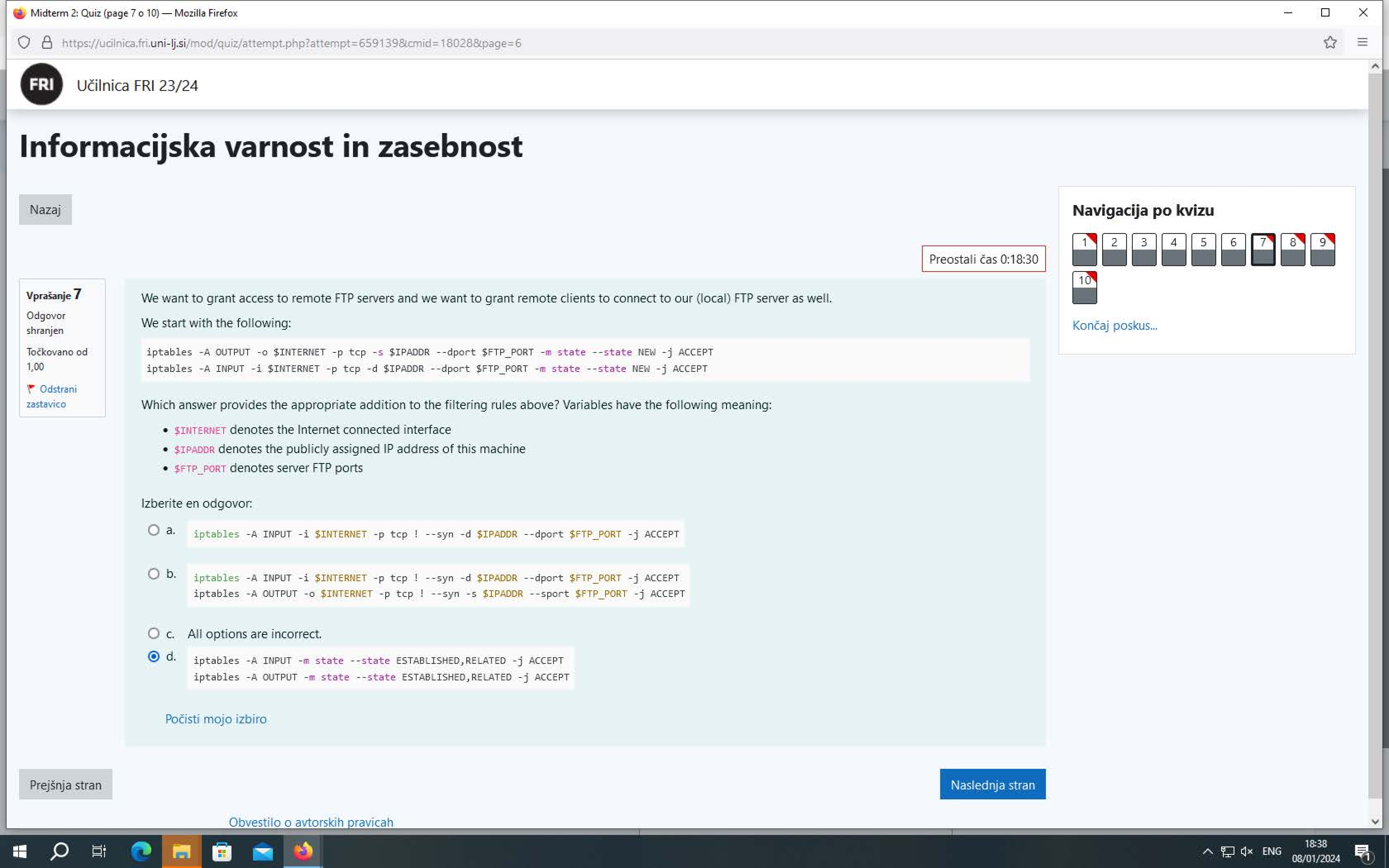
Izberite en odgovor:

○ a. INPUT

○ b. FILTER

○ c. FORWARD

○ d. OUTPUT


Midterm 2: Quiz (page 7 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=6
FRI
Učilnica FRI 23/24
ENG
18:38
08/01/2024

Informacijska varnost in zasebnost

Nazaj

Preostali čas 0:18:30

Vprašanje 7

Odgovor shranjen

Točkovano od 1,00

Odstrani zastavico

We want to grant access to remote FTP servers and we want to grant remote clients to connect to our (local) FTP server as well.

We start with the following:

```
iptables -A OUTPUT -o $INTERNET -p tcp -s $IPADDR --dport $FTP_PORT -m state --state NEW -j ACCEPT
iptables -A INPUT -i $INTERNET -p tcp -d $IPADDR --dport $FTP_PORT -m state --state NEW -j ACCEPT
```

Which answer provides the appropriate addition to the filtering rules above? Variables have the following meaning:

- `$INTERNET` denotes the Internet connected interface
- `$IPADDR` denotes the publicly assigned IP address of this machine
- `$FTP_PORT` denotes server FTP ports

Izberite en odgovor:

○ a.

```
iptables -A INPUT -i $INTERNET -p tcp ! --syn -d $IPADDR --dport $FTP_PORT -j ACCEPT
```

○ b.

```
iptables -A INPUT -i $INTERNET -p tcp ! --syn -d $IPADDR --dport $FTP_PORT -j ACCEPT
iptables -A OUTPUT -o $INTERNET -p tcp ! --syn -s $IPADDR --sport $FTP_PORT -j ACCEPT
```

○ c. All options are incorrect.

● d.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Počisti mojo izbiro

Navigacija po kvizu

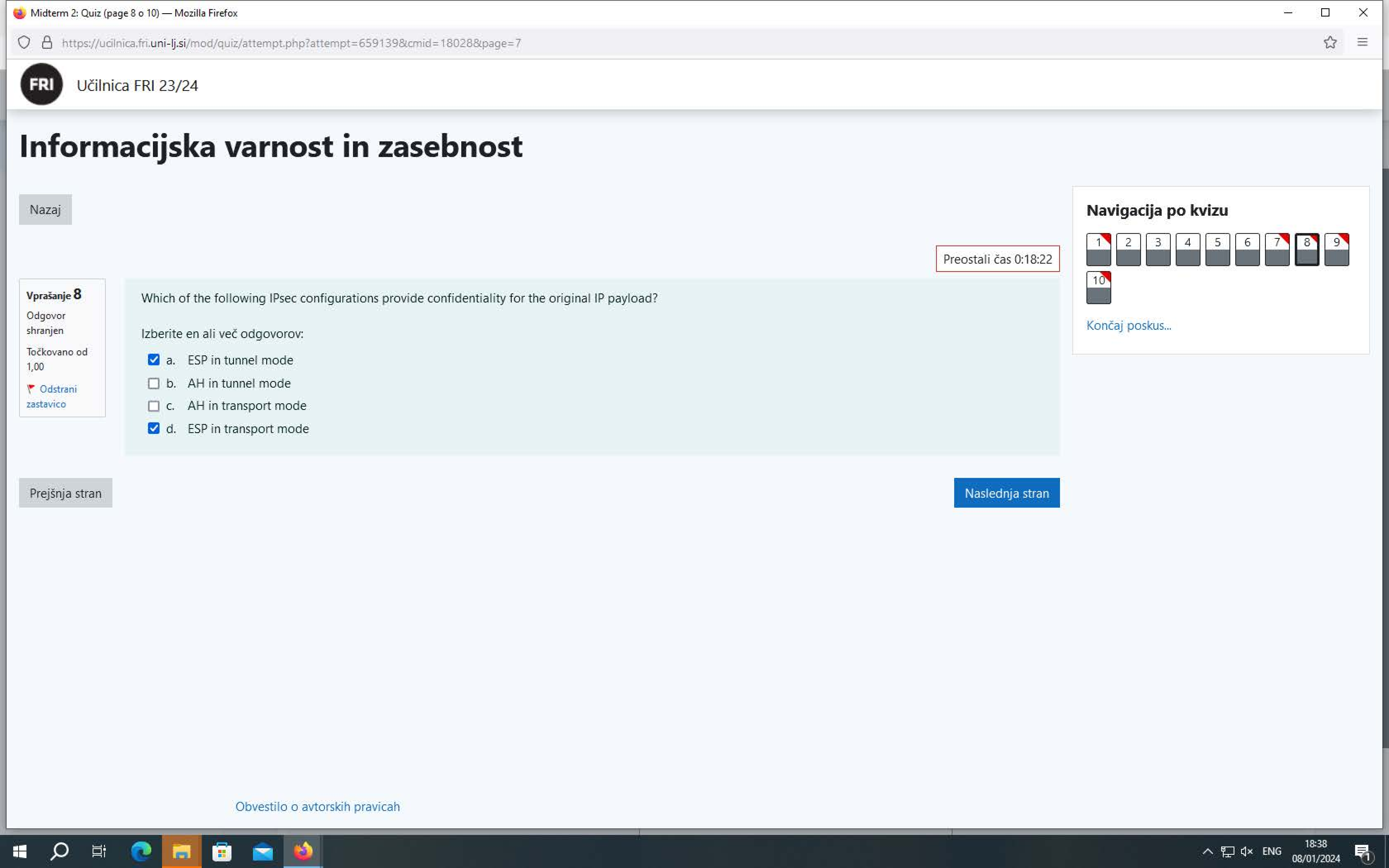
1 2 3 4 5 6 7 8 9 10

Končaj poskus...

Prejšnja stran

Naslednja stran

Obvestilo o avtorskih pravicah



Midterm 2: Quiz (page 8 o 10) — Mozilla Firefox

https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=7

Učilnica FRI 23/24

Informacijska varnost in zasebnost

Preostali čas 0:18:22

Vprašanje 8

Odgovor shranjen

Točkovano od 1,00

Odstrani zastavico

Which of the following IPsec configurations provide confidentiality for the original IP payload?

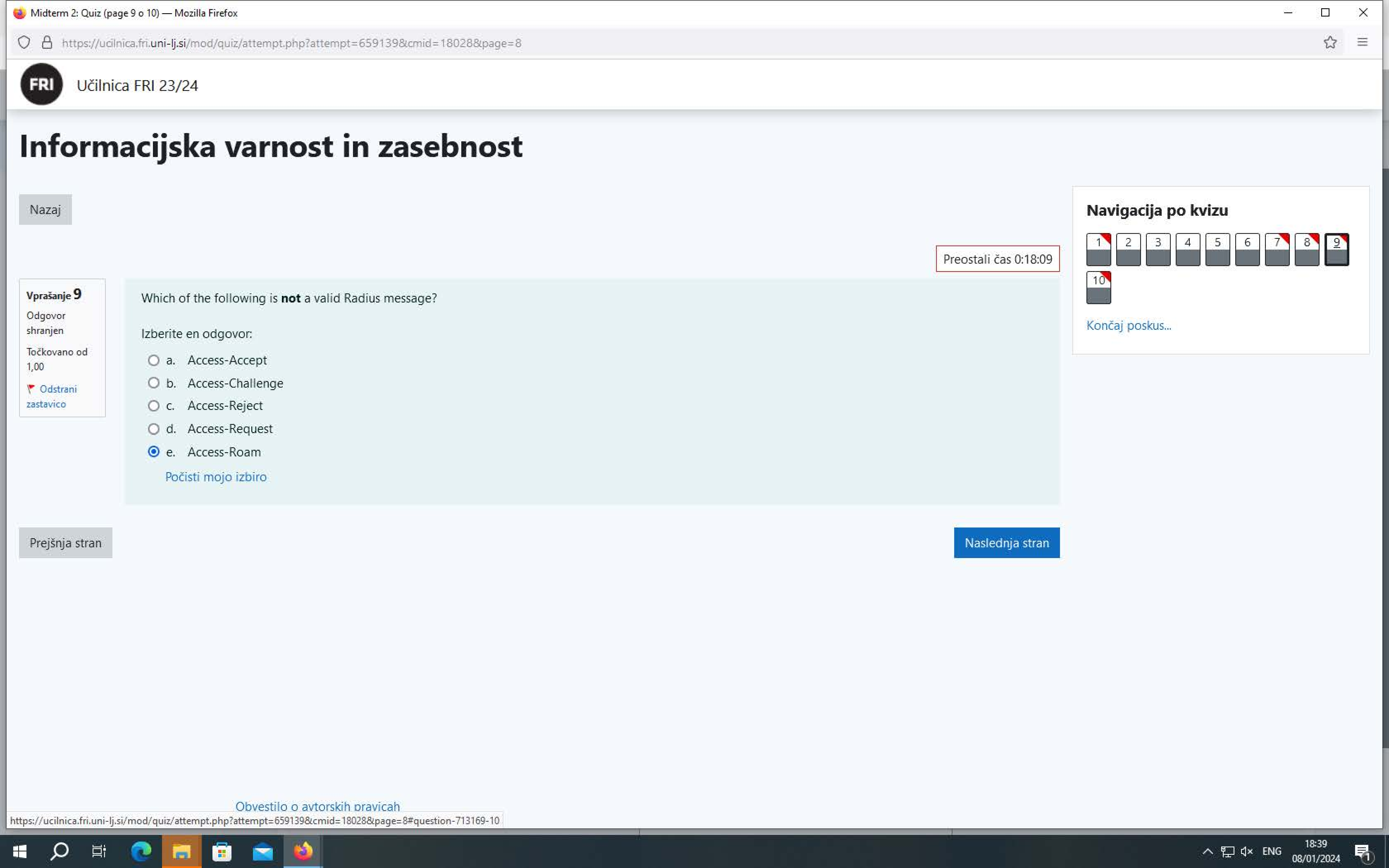
Izberite en ali več odgovorov:

- ☑ a. ESP in tunnel mode
- □ b. AH in tunnel mode
- □ c. AH in transport mode
- ☑ d. ESP in transport mode

Navigacija po kvizu

Končaj poskus...

Obvestilo o avtorskih pravicah


Midterm 2: Quiz (page 9 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=8
FRI
Učilnica FRI 23/24

Informacijska varnost in zasebnost

Preostali čas 0:18:09

Vprašanje 9

Odgovor shranjen

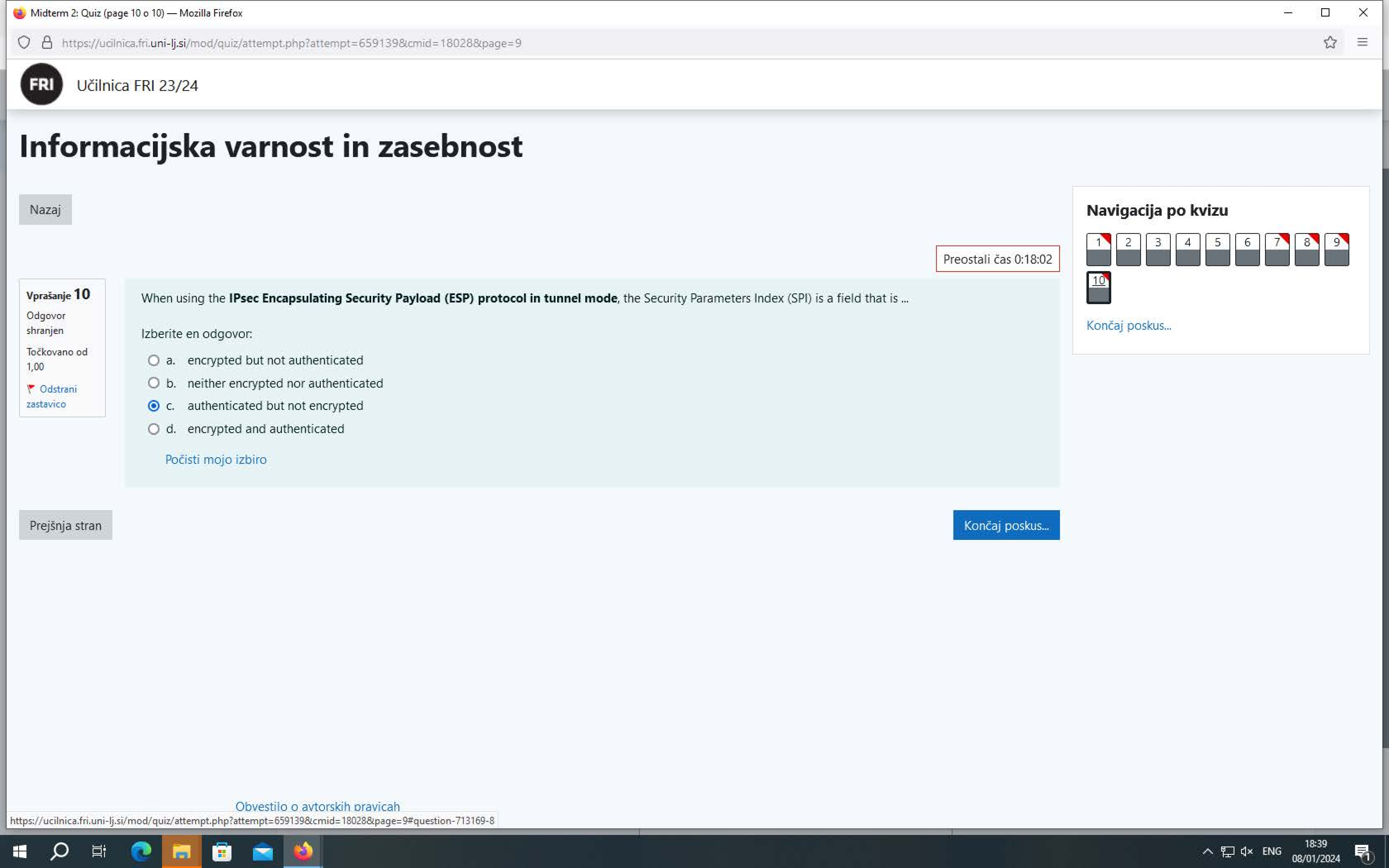
Točkovano od 1,00

Which of the following is **not** a valid Radius message?

Izberite en odgovor:

- ○ a. Access-Accept
- ○ b. Access-Challenge
- ○ c. Access-Reject
- ○ d. Access-Request
- ● e. Access-Roam

Počisti mojo izbiro
Prejšnja stran
Naslednja stran
Navigacija po kvizu
1
2
3
4
5
6
7
8
9
10
Končaj poskus...
Obvestilo o avtorskih pravicah
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=8#question-713169-10
ENG
18:39
08/01/2024


Midterm 2: Quiz (page 10 o 10) — Mozilla Firefox
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=9
FRI
Učilnica FRI 23/24

Informacijska varnost in zasebnost

Nazaj
Preostali čas 0:18:02
Navigacija po kvizu
1 2 3 4 5 6 7 8 9 10
Končaj poskus...

Vprašanje 10
Odgovor shranjen
Točkovano od 1,00
Odstrani zastavico

When using the **IPsec Encapsulating Security Payload (ESP) protocol in tunnel mode**, the Security Parameters Index (SPI) is a field that is ...

Izberite en odgovor:

○ a. encrypted but not authenticated
○ b. neither encrypted nor authenticated
● c. authenticated but not encrypted
○ d. encrypted and authenticated

Počisti mojo izbiro
Prejšnja stran
Končaj poskus...
Obvestilo o avtorskih pravicah
https://ucilnica.fri.uni-lj.si/mod/quiz/attempt.php?attempt=659139&cmid=18028&page=9#question-713169-8
ENG
18:39
08/01/2024

Set up a company's internal network, its gateway, and an example road warrior according to the specifications.

Preostali čas 1:08:27

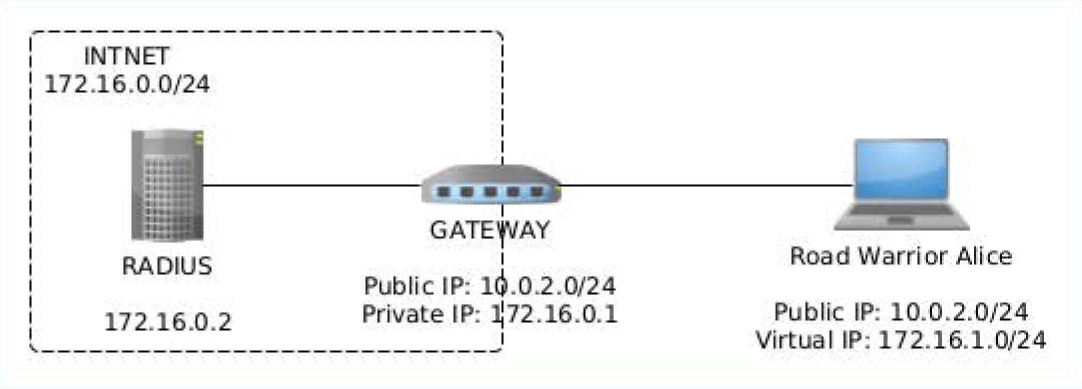


Figure 1: The specification diagram

1 Gateway network [7 points]

Computer `gateway` is connected to the *public* (IP `10.0.2.0/24`) and the private network (IP `172.16.0.1/24`). The gateway acts as a **router** and performs **masquerading** (network address translation) for all traffic that is bound to the Internet. For instance, Radius machine (configured next) should be able to `ping google.com`. You can simulate the public IP network either with a `NAT network` or with `Bridged network` adapter; note that in this case, your *public* IP addresses will be different.

2 Radius [11 points]

The Radius machine is connected to the private network with static IP `172.16.0.2`.

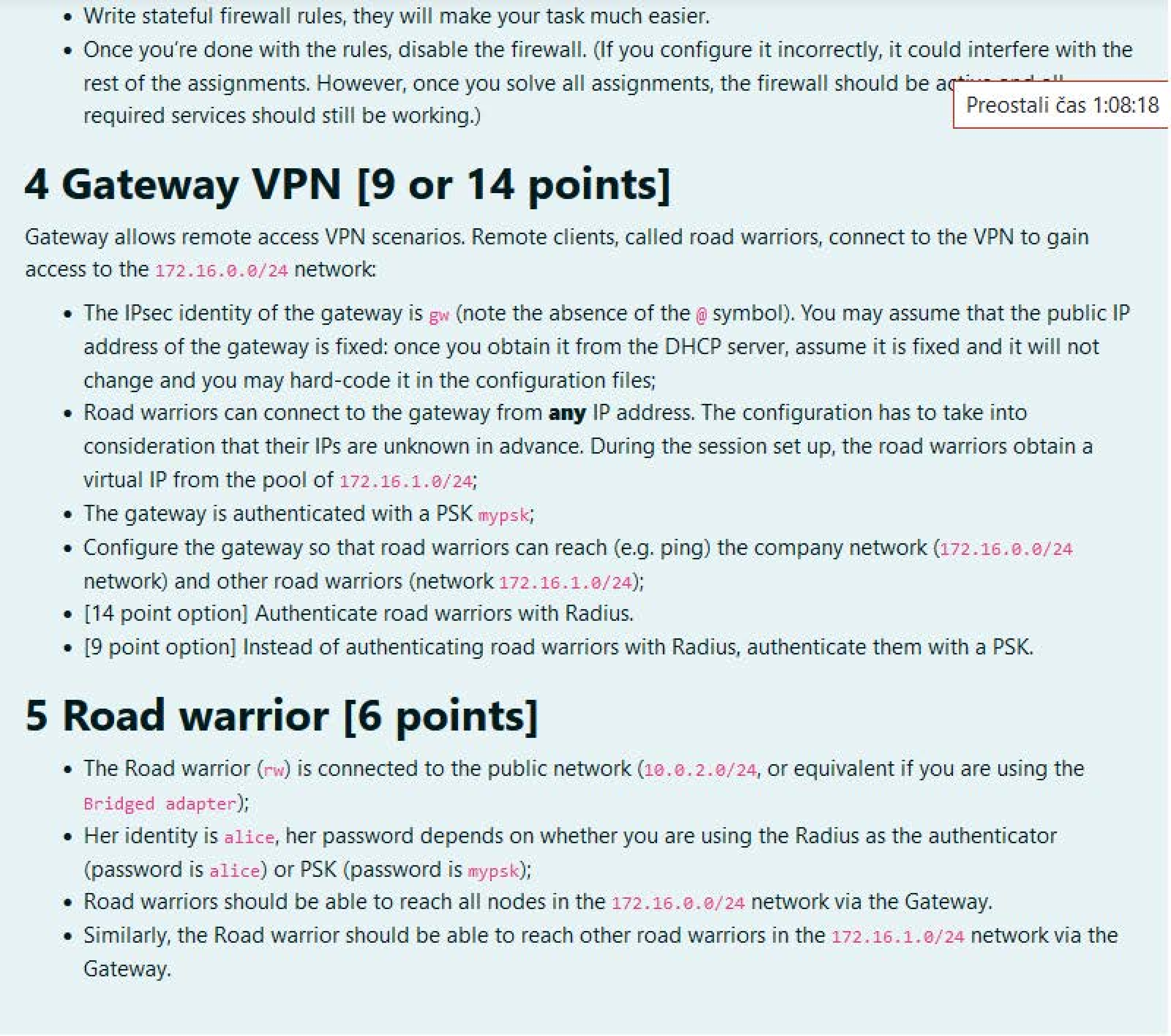
- Machine is running a Freeradius server. Configure it to allow NAS requests from `172.16.0.1`. Authenticate NAS clients with PSK `radiuspassword`.
- Add a user `alice` with password `alice` to the local Freeradius (file-based) database.

3 Gateway firewall [12 points]

Set up a firewall on `gateway` that allows all routed traffic to pass through, but imposes strict limitations on the Internet bound interface regarding the incoming and outgoing traffic. In particular, the following is the only traffic that should be allowed on the Internet bound interface:

- Incoming: ICMP, ISAKMP, IPsec (ESP) and NAT-T.
- Outgoing: ICMP, DNS.

Hints:



- Write stateful firewall rules, they will make your task much easier.
- Once you're done with the rules, disable the firewall. (If you configure it incorrectly, it could interfere with the rest of the assignments. However, once you solve all assignments, the firewall should be active and all required services should still be working.)

Preostali čas 1:08:18

4 Gateway VPN [9 or 14 points]

Gateway allows remote access VPN scenarios. Remote clients, called road warriors, connect to the VPN to gain access to the `172.16.0.0/24` network:

- The IPsec identity of the gateway is `gw` (note the absence of the `@` symbol). You may assume that the public IP address of the gateway is fixed: once you obtain it from the DHCP server, assume it is fixed and it will not change and you may hard-code it in the configuration files;
- Road warriors can connect to the gateway from **any** IP address. The configuration has to take into consideration that their IPs are unknown in advance. During the session set up, the road warriors obtain a virtual IP from the pool of `172.16.1.0/24`;
- The gateway is authenticated with a PSK `mypsk`;
- Configure the gateway so that road warriors can reach (e.g. ping) the company network (`172.16.0.0/24` network) and other road warriors (network `172.16.1.0/24`);
- [14 point option] Authenticate road warriors with Radius.
- [9 point option] Instead of authenticating road warriors with Radius, authenticate them with a PSK.

5 Road warrior [6 points]

- The Road warrior (`rw`) is connected to the public network (`10.0.2.0/24`, or equivalent if you are using the `Bridged adapter`);
- Her identity is `alice`, her password depends on whether you are using the Radius as the authenticator (password is `alice`) or PSK (password is `mypsk`);
- Road warriors should be able to reach all nodes in the `172.16.0.0/24` network via the Gateway.
- Similarly, the Road warrior should be able to reach other road warriors in the `172.16.1.0/24` network via the Gateway.