IVZ KVIZ 2 2018/2019

SHARING IS CARING

DON'T HOLD WHAT YOU HAVE TO YOURSELF
SHARE IT WITH OTHERS!

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

Izberite enega ali več odgovorov:

- [ ] a. AH in transport mode
- [ ] b. ESP in transport mode
- [ ] c. ESP in tunnel mode
- [ ] d. AH in tunnel mode

Which of the following IPsec configurations can be used in a network that performs network address translation at least once?

Izberite enega ali več odgovorov:

- [ ] a. Authentication Headers in transport mode
- [ ] b. Encapsulating Security Payload in transport mode
- [ ] c. Authentication Headers in tunnel mode
- [ ] d. Encapsulating Security Payload in tunnel mode

We want to grant access to remote HTTPS server. We start with the following:

```
iptables -A OUTPUT -o $INTERNET -p tcp -s $IPADDR --dport 443 -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

Izberite enega:

a.

```
iptables -A INPUT  -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i $INTERNET -p tcp -d $IPADDR --dport 443 -m state --state NEW -j ACCEPT
```

b.

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

c.

```
iptables -A INPUT -i $INTERNET -p tcp -d $IPADDR --dport 443 -m state --state NEW -j ACCEPT
```

d. All answers are incorrect.

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 enega:

- 1. SUP_b conntects to N_a. N_a conntects to R_b.
- 2. SUP_b conntects to N_b. N_b conntects to R_b.
- 3. SUP_b conntects to N_a. N_a conntects to R_a. R_a connects to R_b.
- 4. SUP_a conntects to N_a. N_a conntects to R_a. R_a conntects to R_b.

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

Izberite enega:

- a. FILTER
- b. FORWARD
- c. OUTPUT
- d. INPUT

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

Izberite enega:

- a. Client's public key fingerprint is displayed.
- b. Server's public key fingerprint is displayed.
- c. Client's private key fingerprint is displayed.
- d. Server's private key fingerprint is displayed.

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

Izberite enega:

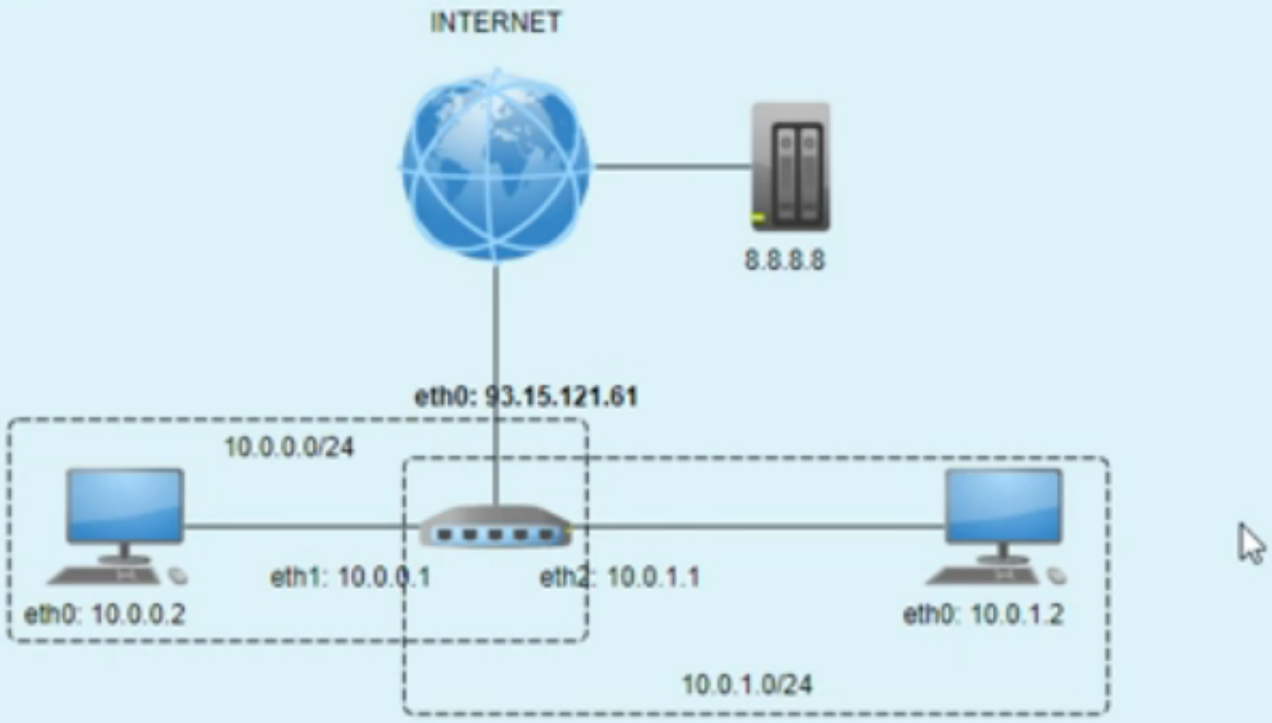
- a. encrypted and authenticated
- b. authenticated but not encrypted
- c. neither encrypted nor authenticated
- d. encrypted but not authenticated

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

Izberite enega:

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

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

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 enega ali več odgovorov:

- [ ] a. `8.8.8.8`
- [ ] b. `10.0.1.2`
- [ ] c. `10.0.1.1`
- [ ] d. `10.0.0.1`

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

Izberite enega:

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