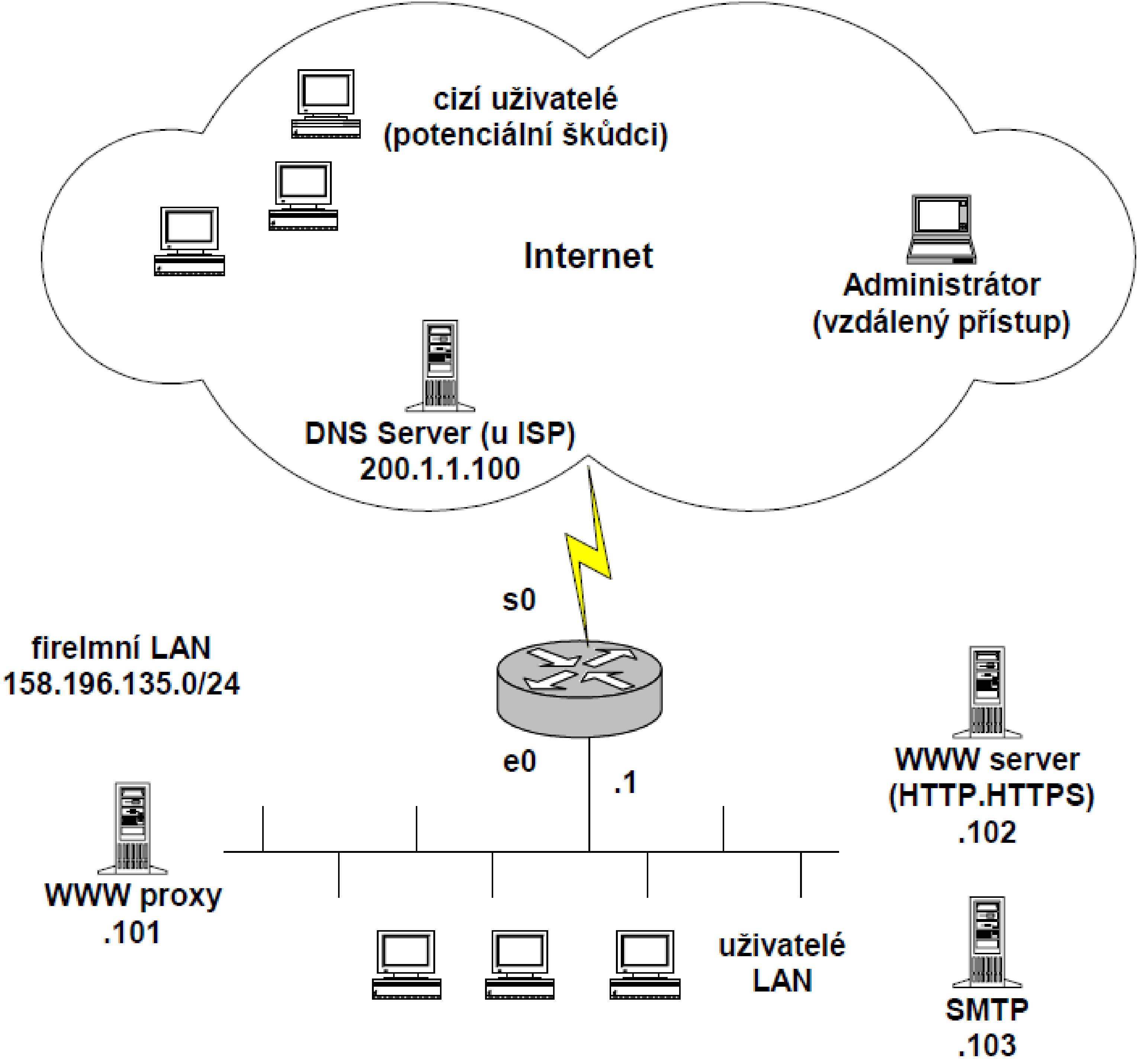
Example of ACL configuration

Situation

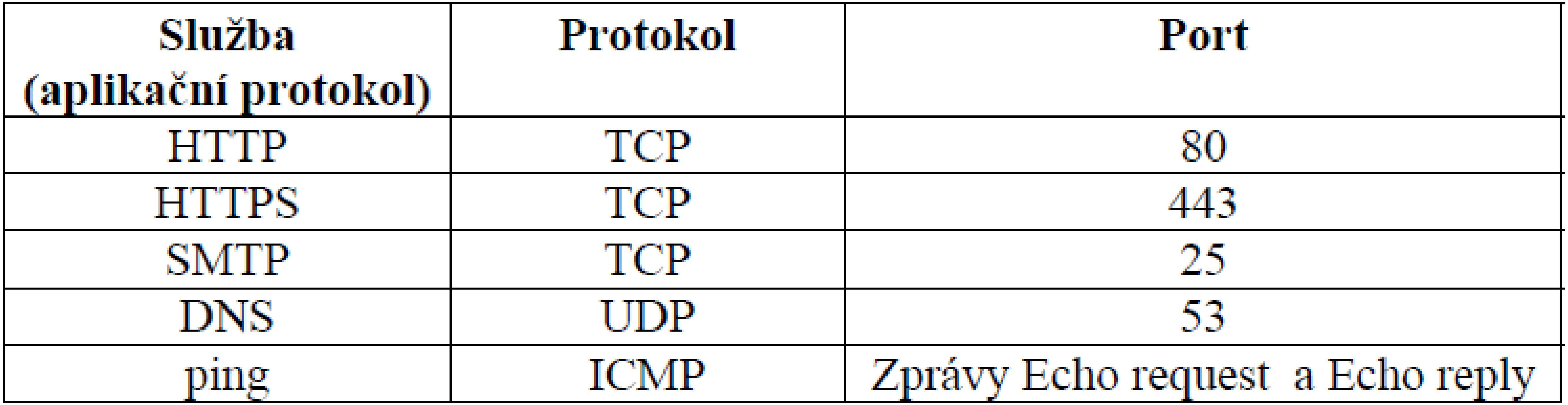
- We want to secure a company LAN connected to the Internet by a single line.
- We apply the ACL to the router that separates the LAN from the Internet (see figure).
- The company is assigned the address space 158.196.135.0/24.


cizí uživatelé
(potenciální škůdci)
Internet
Administrátor
(vzdálený přístup)
DNS Server (u ISP)
200.1.1.100
s0
firelmní LAN
158.196.135.0/24
e0
.1
WWW server
(HTTP.HTTPS)
.102
WWW proxy
.101
uživatelé
LAN
SMTP
.103

The requirements for traffic to be passed are as follows:

- The company operates its own mail server (SMTP) accessible from the outside at the address 158.196.135.103.
- The company operates its own WWW server (HTTP, HTTPS) accessible from the outside at the address 158.196.135.102.
- Local clients access the WWW service (HTTP and HTTPS) exclusively via a proxy with the address 158.196.135.101.
- Only SSH connections can be opened from LAN stations to the Internet.
- The DNS server performing recursive name lookups for all clients on the LAN is located at the Internet service provider (ISP) at 200.1.1.100.
- Ping from the LAN to the Internet is allowed, but not in the opposite direction for security reasons.
- A remote administrator can connect to the computer with the WWW server from anywhere on the Internet using SSH. Any other traffic is prohibited.

Application Analysis

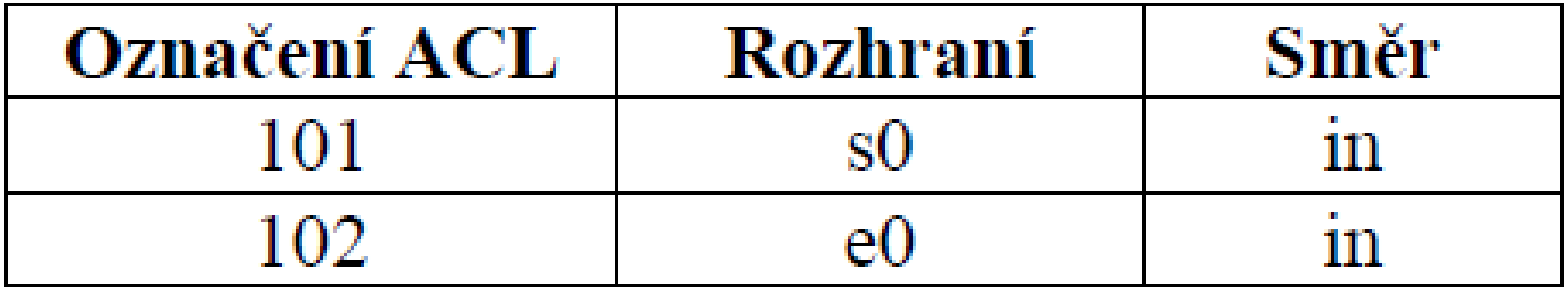


Služba (aplikační protokol)	Protokol	Port
HTTP	TCP	80
HTTPS	TCP	443
SMTP	TCP	25
DNS	UDP	53
ping	ICMP	Zprávy Echo request a Echo reply

Interface for applying the ACL

- Next, we need to decide on which router interface and for which direction of traffic we will apply the ACL.
- In this case, it seems most advantageous to control traffic to the LAN on interface s0 and from the LAN to the Internet on interface e0.
- This avoids unnecessary routing of packets that would be subsequently discarded anyway.

Interface for applying the ACL

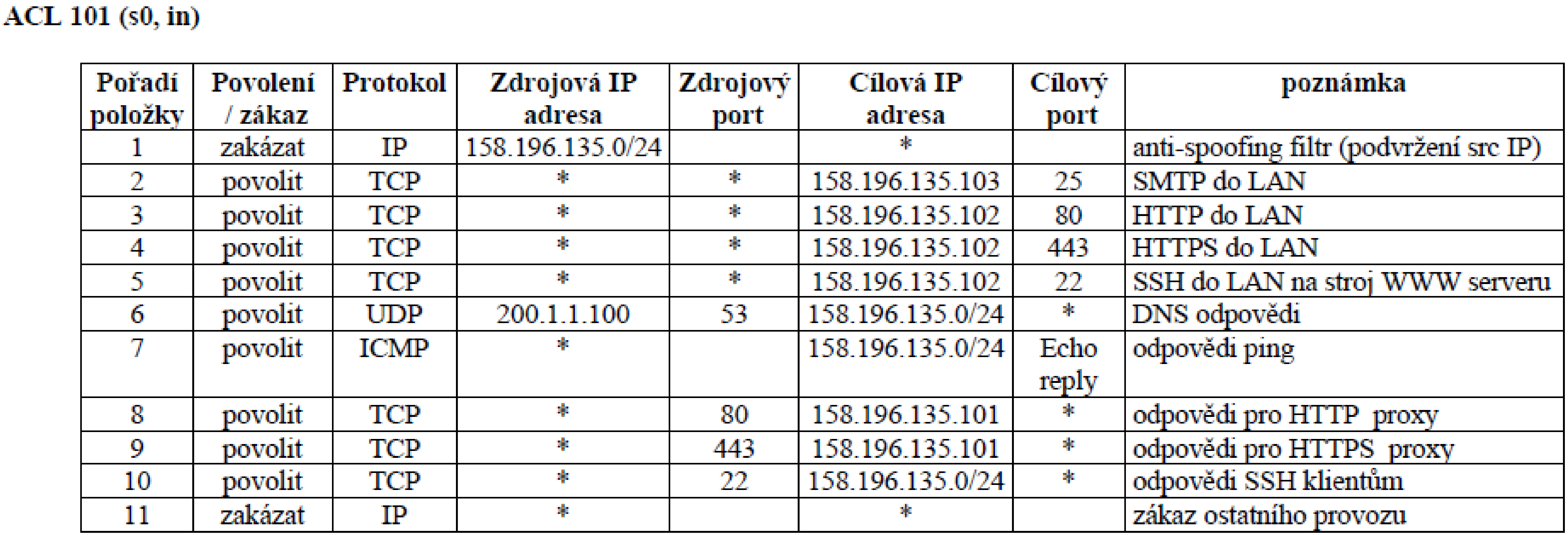


Označení ACL	Rozhraní	Směr
101	s0	in
102	e0	in

ACL marking

- When defining an ACL, we must remember that in each direction we must allow not only traffic towards permitted services located on the "opposite" side of the router, but also return traffic from services located on the "source side" of the ACL.
- An asterisk next to the source or destination address and port indicates any address or port. The source or destination port is only listed for TCP/UDP protocols; for the ICMP protocol, the Destination port column is used to define the message type.
- We could further increase the level of security by allowing only segments of already open TCP connections in the return traffic of the TCP protocol, i.e. filtering out segments with an active request to establish a connection (SYN=1, ACK=0}.

ACL 101

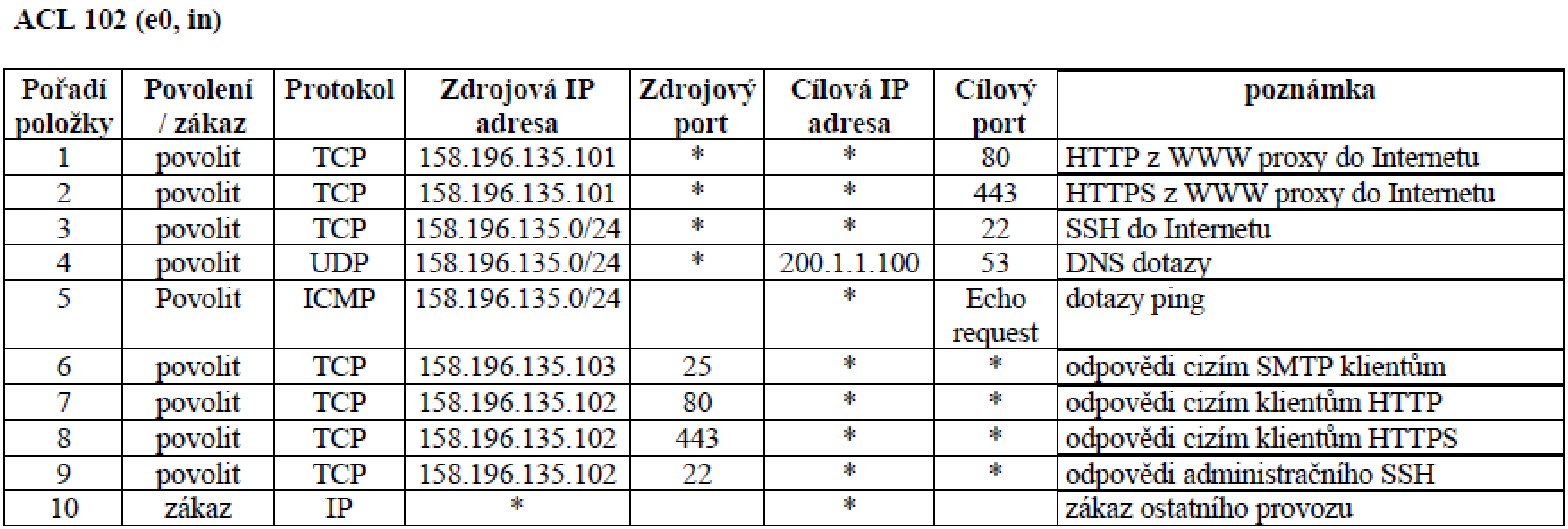


ACL 101 (s0, in)

Pořadí položky	Povolení / zákaz	Protokol	Zdrojová IP adresa	Zdrojový port	Cílová IP adresa	Cílový port	poznámka
1	zakázat	IP	158.196.135.0/24		*		anti-spoofing filtr (podvržení src IP)
2	povolit	TCP	*	*	158.196.135.103	25	SMTP do LAN
3	povolit	TCP	*	*	158.196.135.102	80	HTTP do LAN
4	povolit	TCP	*	*	158.196.135.102	443	HTTPS do LAN
5	povolit	TCP	*	*	158.196.135.102	22	SSH do LAN na stroj WWW serveru
6	povolit	UDP	200.1.1.100	53	158.196.135.0/24	*	DNS odpovědi
7	povolit	ICMP	*		158.196.135.0/24	Echo reply	odpovědi ping
8	povolit	TCP	*	80	158.196.135.101	*	odpovědi pro HTTP proxy
9	povolit	TCP	*	443	158.196.135.101	*	odpovědi pro HTTPS proxy
10	povolit	TCP	*	22	158.196.135.0/24	*	odpovědi SSH klientům
11	zakázat	IP	*		*		zákaz ostatního provozu

```
access-list 101 deny ip 158.196.135.0 0.0.0.255 any
access-list 101 permit tcp any host 158.196.135.103 eq 25
access-list 101 permit tcp any host 158.196.135.102 eq 80
access-list 101 permit tcp any host 158.196.135.102 eq 443
access-list 101 permit tcp any host 158.196.135.102 eq 22
access-list 101 permit udp host 200.1.1.100 eq 53 158.196.135.0 0.0.0.255
access-list 101 permit icmp any 158.196.135.0 0.0.0.255 echo-reply
access-list 101 permit tcp any eq 80 host 158.196.135.101 established
access-list 101 permit tcp any eq 443 host 158.196.135.101 established
access-list 101 permit tcp any eq 22 158.196.135.101 0.0.0.255 established
interface s0
ip access-group 101 in
```

ACL 102



ACL 102 (e0, in)

Pořadí položky	Povolení / zákaz	Protokol	Zdrojová IP adresa	Zdrojový port	Cílová IP adresa	Cílový port	poznámka
1	povolit	TCP	158.196.135.101	*	*	80	HTTP z WWW proxy do Internetu
2	povolit	TCP	158.196.135.101	*	*	443	HTTPS z WWW proxy do Internetu
3	povolit	TCP	158.196.135.0/24	*	*	22	SSH do Internetu
4	povolit	UDP	158.196.135.0/24	*	200.1.1.100	53	DNS dotazy
5	Povolit	ICMP	158.196.135.0/24		*	Echo request	dotazy ping
6	povolit	TCP	158.196.135.103	25	*	*	odpovědi cizím SMTP klientům
7	povolit	TCP	158.196.135.102	80	*	*	odpovědi cizím klientům HTTP
8	povolit	TCP	158.196.135.102	443	*	*	odpovědi cizím klientům HTTPS
9	povolit	TCP	158.196.135.102	22	*	*	odpovědi administračního SSH
10	zákaz	IP	*		*		zákaz ostatního provozu

```
access-list 102 permit tcp host 158.196.135.101 any eq 80
access-list 102 permit tcp host 158.196.135.101 any eq 443
access-list 102 permit tcp 158.196.135.0 0.0.0.255 any eq 22
access-list 102 permit udp 158.196.135.0 0.0.0.255 host 200.1.1.100 eq 53
access-list 102 permit icmp 158.196.135.0 0.0.0.255 any echo
access-list 102 permit tcp host 158.196.135.103 eq 25 any established
access-list 102 permit tcp host 158.196.135.102 eq 80 any established
access-list 102 permit tcp host 158.196.135.102 eq 443 any established
access-list 102 permit tcp host 158.196.135.102 eq 22 any established
interface e0
ip access-group 102 in
```