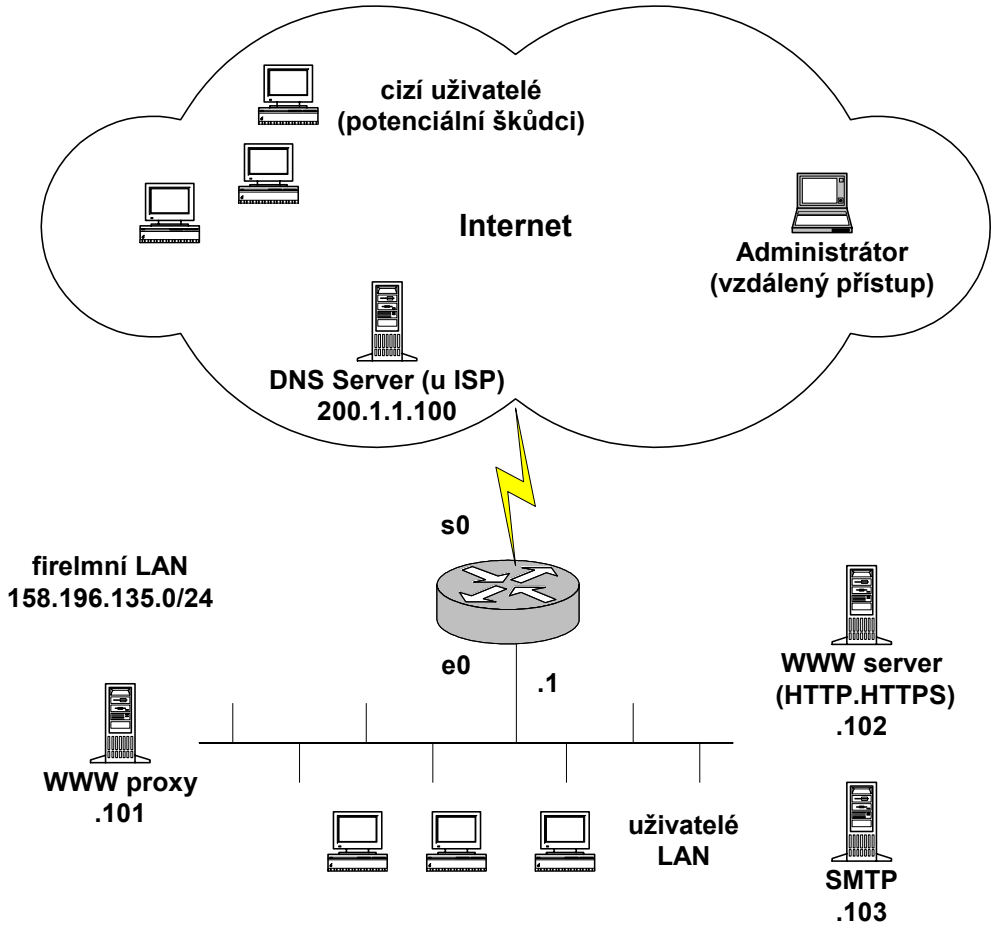
Příklad konfigurace ACL

petr.grygarek@vsb.cz

Situace

Chceme zabezpečit firemní LAN připojenou jednou linkou do Internetu. ACL aplikujeme na směrovači, který LAN od Internetu odděluje (viz obrázek). Firma má přidělen adresní prostor 158.196.135.0/24.



Požadavky na propouštěný provoz jsou následující:

- Firma provozuje svůj vlastní poštovní server (SMTP) přístupný zvenčí na adrese 158.196.135.103.
- Firma provozuje svůj vlastní WWW server (HTTP, HTTPS) přístupný zvenčí na adrese 158.196.135.102.
- Přístup lokálních klientů ke službě WWW (HTTP i HTTPS) jde výhradně přes proxy s adresou 158.196.135.101.
- Ze stanic LAN lze do Internetu otevírat pouze spojení SSH.
- DNS server provádějící rekurzivní vyhledávání jmen pro všechny klienty na LAN je u poskytovatele Internetu (ISP) na adrese 200.1.1.100.
- Je povolen ping z LAN do Internetu, v opačném směru však z bezpečnostních důvodů nikoli.
- Vzdálený administrátor je schopen připojit se odkudkoli z Internetu na počítač s WWW serverem pomocí služby SSH.

Jakýkoli jiný provoz je zakázán.

Analýza aplikací

Nejprve je nutné zvážit, jaké protokoly a jaké porty jednotlivé podporované služby používají:

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

Žádná z použitých služeb nevyužívá dynamicky přidělované porty.

Rozhraní pro aplikaci ACL

Dále musíme rozhodnout, na kterém rozhraní směrovače a pro který směr provozu budeme aplikovat ACL. V tomto případě se jeví nejvýhodnější provoz do LAN kontrolovat na rozhraní s0 a z LAN do Internetu na rozhraní e0. Tím se vyhneme zbytečnému směrování paketů, které by stejně byly následně zahozeny.

Označení ACL	**Rozhraní**	**Směr**
101	s0	in
102	e0	in

Definice ACL

Při definici ACL si musíme uvědomit, že v každém ze směrů musíme propustit nejen provoz směrem k povoleným službám nacházejícím se na „opačné“ straně směrovače, ale i zpětný provoz služeb umístěných na „zdrojové straně“ ACL.

Hvězdička u zdrojové nebo cílové adresy a portu vyjadřuje libovolnou adresu, resp. port. Zdrojový, resp. cílový port je uveden jen u protokolů TCP/UDP, u protokolu ICMP je sloupec Cílový port využit pro definici typu zprávy.

Úroveň zabezpečení bychom mohli ještě zvýšit tím, že u zpětného provozu protokolu TCP bychom vpouštěli pouze segmenty již otevřených TCP spojení, tedy odfiltrovali segmenty s aktivní výzvou k navázání spojení (SYN=1, ACK=0}.

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

Alternativně tabulku vyjádříme také syntaxí ACL používanou v Cisco IOS:

```
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 (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
```