بسمه تعالی

دانشگاه شهیدبهشتی
دانشکده مهندسی و علوم کامپیوتر
امنیت شبکه‌های کامپیوتری پیشرفته
تمرین چهارم

۱. با توجه به Firewall rule زیر در درست یا غلط بودن هر یک از جملات زیر را با دلیل توضیح دهید.

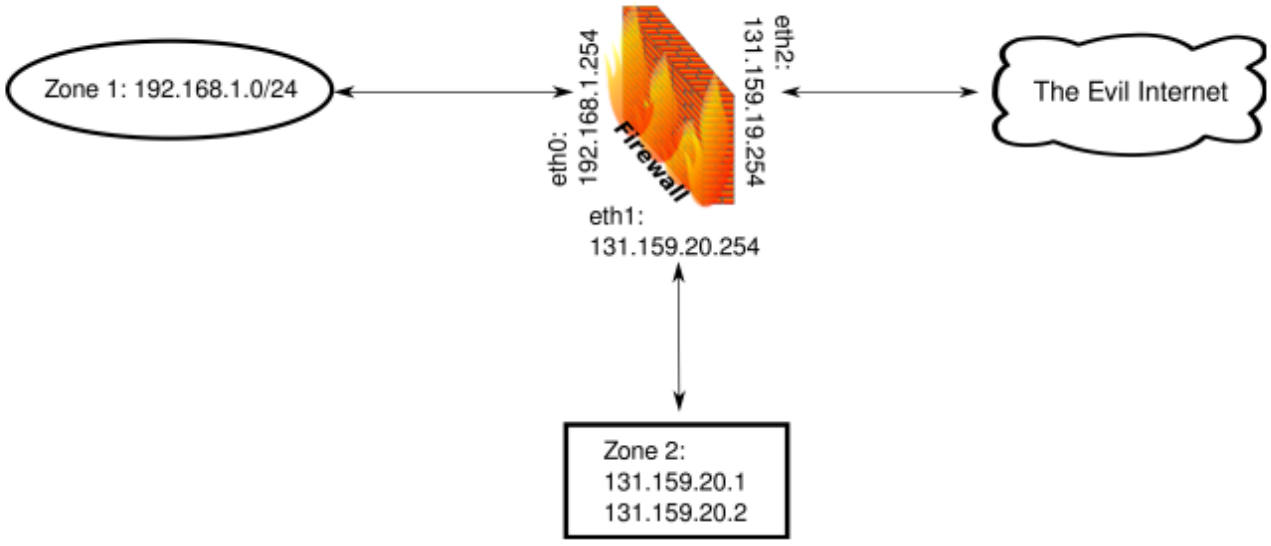
Action	Source IP	Destination IP	Protocol	Source Port	Destination Port
Accept	Any	192.168.0.2	TCP	Any	80

a. اجازه ارسال ترافیک از پورت ۸۰ به هر آدرس IP را می دهد.
b. ترافیک را از هر آدرس IP به سمت سرور در ۱۹۲/۱۶۸/۰/۲ می پذیرد.
c. ترافیک را از هر آدرس IP به سمت سرور وب در ۱۹۲/۱۶۸/۰/۲ می پذیرد.
d. امکان اتصال TCP را به هر پورت ۱۹۲/۱۶۸/۰/۲ فراهم می کند.

۲. چه نوع فایروال باید برای فیلتر کردن حملات به یک برنامه وب استفاده شود؟ توضیح دهید؟

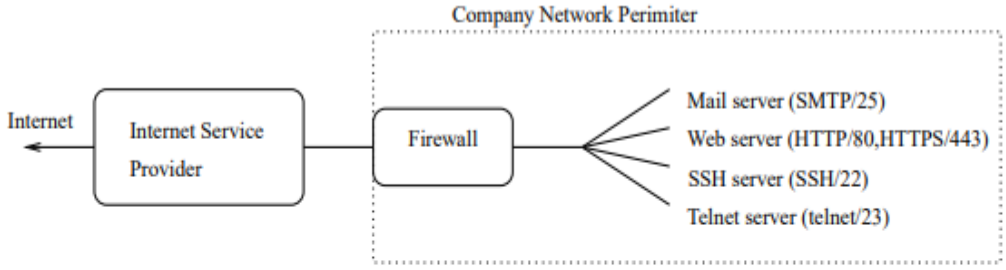
۳. در جدول، پیکربندی فایروال برای توپولوژی شبکه شکل زیر را مشاهده می کنید. مستقل از سیاست امنیتی، پیکربندی فایروال دارای نقص است. چهار اشتباه را بیابید که منجر به رفتاری می شود که احتمالاً نامطلوب است.

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	Zone 1 → *	*	*	TCP	*	*	New	Permit
B	* → *	Zone 2	Zone 1	*	*	*	New	Permit
C	Zone 1 → *	*	*	TCP	*	22	New	Drop
D	* → *	*	*	*	*	*	Est	Permit



امنیت شبکه‌های کامپیوتری پیشرفته
تمرین چهارم

۴. نمودار زیر معماری شبکه و اتصال دانشگاه شهید بهشتی به اینترنت را نشان می دهد.



IP addresses:

ISP router	2.2.2.1
Mail server	1.2.3.5
Web server	1.2.3.4
SSH server	1.2.3.3
Telnet server	1.2.3.2

Example rules:

```
allow * *:*/in -> *:*/out
drop * *:* -> *:*
```

دانشگاه شما در حال نصب فایروال فیلتر بسته است. در اینجا سیاست امنیتی پیشنهادی برای فایروال آمده است:

الف. به طور پیش فرض، تمام اتصالات ورودی را مسدود کنید.

ب. تمام اتصالات TCP ورودی به SMTP در سرور ایمیل مجاز است.

ج تمام اتصالات TCP ورودی به HTTP و HTTPS در وب سرور مجاز است.

د تمام اتصالات TCP ورودی به SSH در سرور SSH مجاز است.

ه. همه اتصالات خروجی را مجاز کنید.

ف. دسترسی به Telnet نباید مجاز باشد (زیرا رمزهای عبور را به صورت cleartext ارسال می کند).

A) مجموعه قوانین فایروال را برای فایروال دانشگاه خود بنویسید. برای هر قانون، توضیح مختصری از هدف آن ارائه دهید.

B) هکرها شبکه دانشگاه شما را با درخواست های مکرر برای تصاویر بزرگ در وب سرور دانشگاه هدف قرار می دهند. ماشین های هکرها در زیر شبکه 20.1.21.x هستند. چگونه می توانید مجموعه قوانین فایروال خود را برای جلوگیری از این حملات تغییر دهید؟

C) کارمندان شروع به دانلود بسیاری از تریلرهای فیلم از وب سایت جدید WebSiteFilm.com در آدرس 4.3.2.1:80 می کنند. چگونه می توانید قوانین فایروال خود را برای جلوگیری از دسترسی کارکنان به وب سایت تغییر دهید؟

امنیت شبکه‌های کامپیوتری پیشرفته
تمرین چهارم

۵. این سوال برخی از کاربردها و محدودیت های فایروال های فیلترینگ بسته (بدون وضعیت) را بررسی می کند.

a. ما یک وب سرور داخلی داریم که فقط برای اهداف آزمایشی به آدرس 5.6.7.8 در شبکه داخلی دانشگاه استفاده می شود. فیلتر بسته در نقطه انسداد بین شبکه داخلی ما و بقیه اینترنت قرار دارد. آیا چنین فیلتر بسته‌ای می‌تواند تمام تلاش‌های میزبان‌های خارجی برای شروع اتصال مستقیم TCP به این وب‌سرور داخلی را مسدود کند؟ اگر بله، یک مجموعه قوانین فیلترینگ بسته را نشان دهید که این قابلیت را فراهم می کند. اگر نه، توضیح دهید که چرا یک فیلتر بسته (بی حالت) نمی تواند این کار را انجام دهد.

b. آیا فیلتر بسته می‌تواند تمام ایمیل‌های دریافتی حاوی عبارت «با من تماس بگیرید!» را مسدود کند؟ اگر بله، یک مجموعه قوانین فیلترینگ بسته را نشان دهید که این قابلیت را فراهم می کند. اگر نه، توضیح دهید که چرا یک فیلتر بسته (بی حالت) نمی تواند این کار را انجام دهد.