[MODULE 5]

Firewall Filters

Read Me

Ini adalah modul gratis, boleh digunakan oleh siapa saja untuk keperluan belajar (non-komersial) dan hal serupa lainnya tanpa menghapus footer credit dari webiptek.com.

Penjelasan dalam bentuk video (Bahasa Indonesia), silakan cek di Youtube:
https://www.youtube.com/playlist?list=PLnZp9Zjr0jNt84A7BFFUztsPILawYuIC0

by Rizqi Aldi Prayugo (xdnroot@gmail.com)

xdnroot

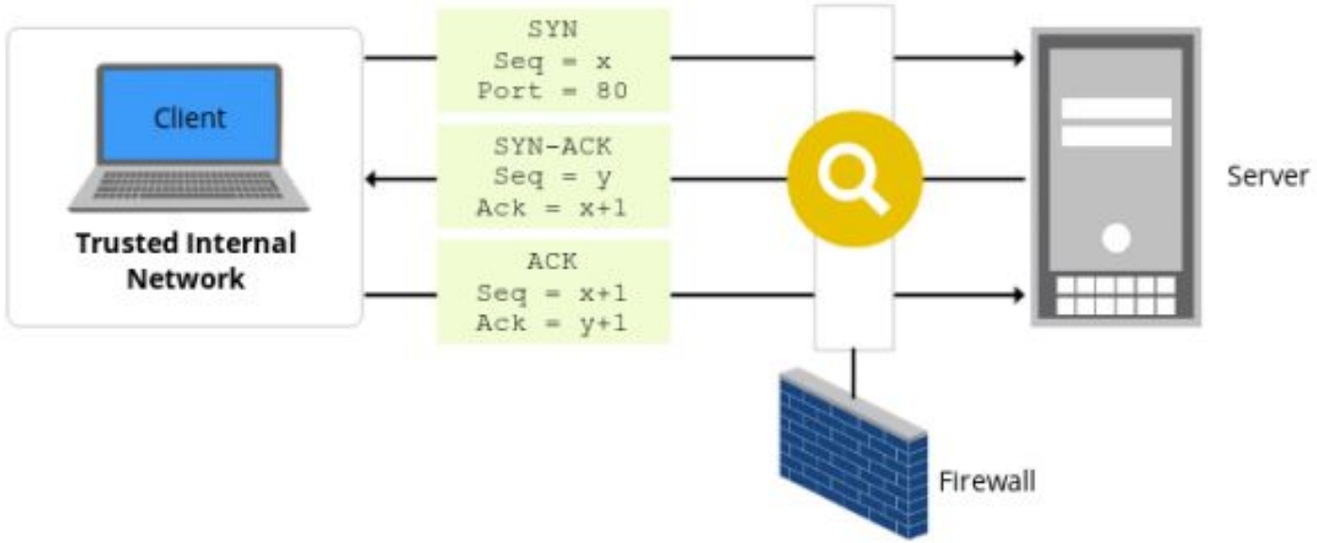
Last Update: 16/06/2020

What is Firewall Filters?

- Firewall filters merupakan fitur yang memungkinkan router untuk mengontrol traffic yang masuk dan/atau keluar.
- Firewall filters biasanya digunakan untuk melindungi perangkat dari serangan dengan cara membatasi akses layanan tertentu.
- Firewall filters bekerja pada layer 3 dan 4 model OSI. Dia akan membandingkan tcp dan ip header dengan rule firewall yang telah dikonfigurasikan, kemudian memberi tindakan jika paketnya cocok dengan rule firewall.

Stateless Firewall Filters

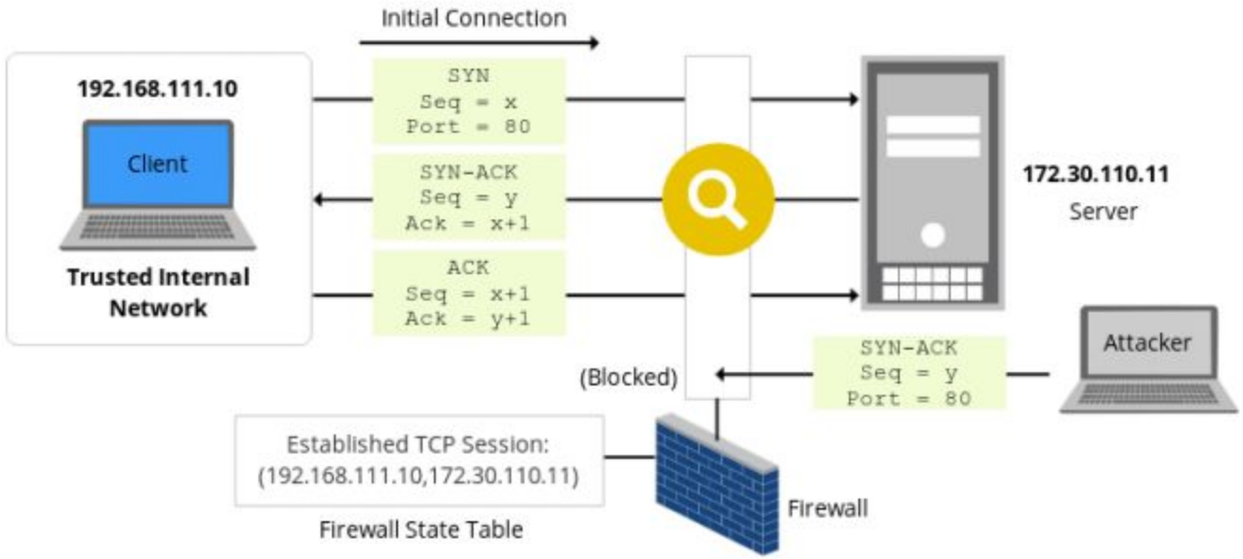
Pada dasarnya firewall filters bersifat stateless. Maksudnya firewall filter akan mengecek paket yang lewat satu per satu.
Misalnya ketika kita mengirim file, paket kita dibagi menjadi 10 paket. Maka stateless firewall filter akan melakukan pengecekan di setiap paket artinya ada 10x.
Pengecekan di sini artinya paket



Stateful Firewall Filters

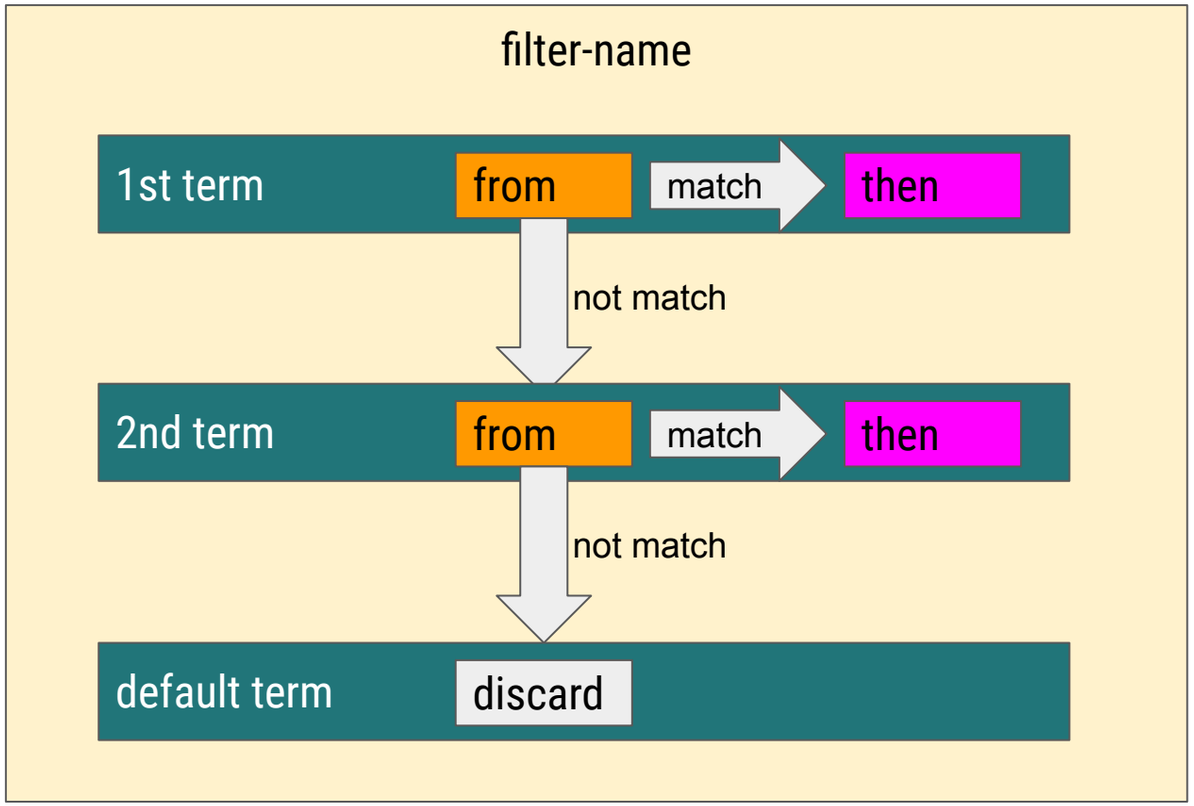
Stateful firewall filter akan mengecek connection-state setiap paket sebelum memeriksanya.

Misalnya ketika kita mentransfer sebuah file, paket kita dibagi menjadi 10 paket. Stateful firewall filter hanya akan mengecek paket pertama (*initial connection)* atau paket yang connection-statenya new. Dan paket berikutnya yang statusnya established atau related, akan otomatis mengikuti action yang diberikan firewall filter ke paket pertama tadi.



Firewall Filters Hierarchy

- Firewall filter menggunakan prinsip mirip if else statement. Paket yang masuk akan dicocokan L3 dan L4 headernya dengan term pertama, apakah ada kecocokan dengan kriteria yang didefinisikan di form, jika cocok maka akan diputuskan sebuah atau beberapa action yang telah didefinisikan pada then.
- Jika tidak cocok paket ada periksa dengan term berikutnya, jika tidak ada yang cocok maka paket akan diabaikan.



Firewall Filter Actions

Terminating Action
Action untuk mengakhiri proses pencocokan paket terhadap firewall.

Flow Control
Action untuk meneruskan paket ke term berikutnya setelah melakukan action.

Action Modifiers
Action untuk kebutuhan monitoring. Dapat dikombinasikan dengan satu atau lebih terminating action atau flow control. Jika tidak ada terminating / flow control action, paket akan diterima (accepted).

Action: Terminating

accept: paket diterima.

discard: paket dibuang tanpa pemberitahuan ICMP message.

reject: paket ditolak dengan pemberitahuan dengan mengirimkan ICMP message kepada pengirim.

tcp-reset: sistem akan membalas dengan TCP reset, tetapi balasan itu tidak akan dikirim jika bukan paket TCP.

Action: Flow Control

next-term: meneruskan paket ke term berikutnya.

Action: Modifiers

count, log, syslog: untuk merekam/menyimpan informasi tentang paket.

forwarding-class and **loss-priority**: untuk mendefinisikan class of service (CoS).

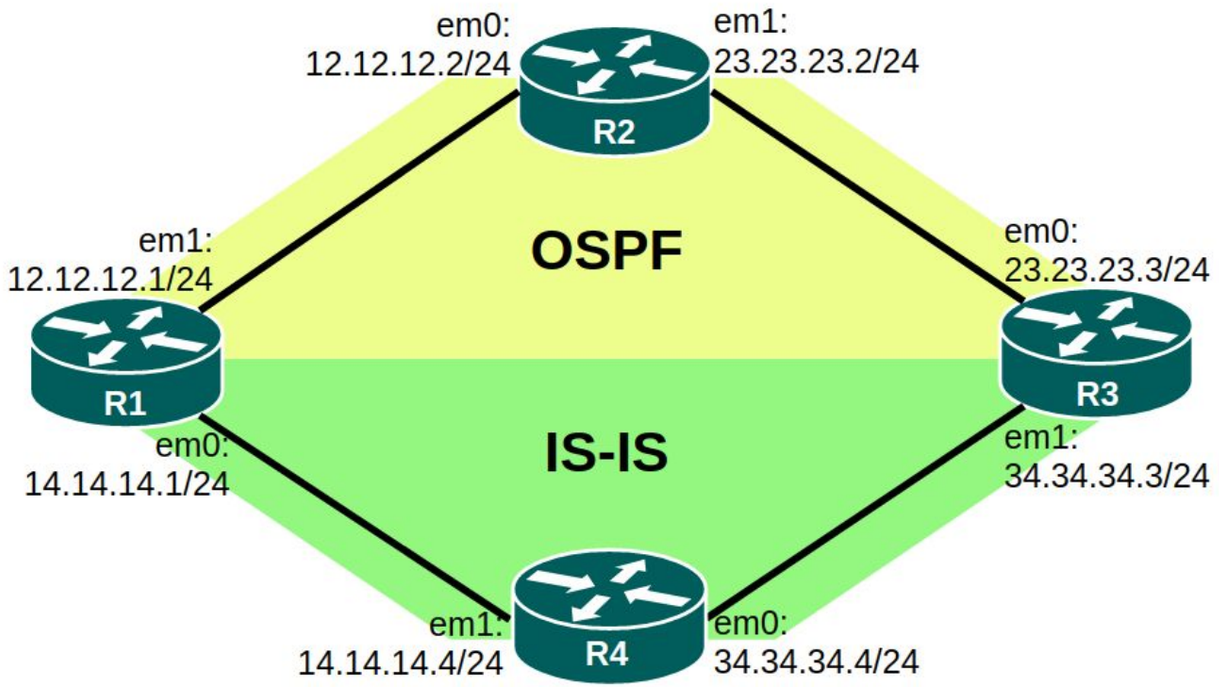
policers: paket akan ditangani traffic policer.

Firewall Filter Reference

https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-stateless-overview.html

[LAB 7]

Basic Firewall Filters



WebIPTEK.com

JUNIPER NETWORKS

Tasks

Aktifkan remote access ssh pada R1. Kemudian buat firewall filter pada R1 dengan ketentuan:

1. Reject akses ping ke R1 (1.1.1.1) dari network 23.23.23.0/24
2. Discard akses ssh ke R1 dari semua IP, kecuali network 23.23.23.0/24 dan 14.14.14.0/24.
3. Masukan ke dalam log setiap ada percobaan akses ssh.

Basic Firewall Filters

1. Reject akses ping ke R1 dari network 23.23.23.0/24

buat firewall filter
[edit firewall filter ping-in term 1]
root@R1# **set from source-address 23.23.23.0/24**
root@R1# **set from destination-address 1.1.1.1**
root@R1# **set from protocol icmp**
root@R1# **set then reject**

[edit firewall filter ping-in term 2]
root@R1# **set then accept**

apply firewall filter ke interface em0 filter input
[edit]
root@R1# **set interfaces lo0 unit 0 family inet filter input ping-in**

Basic Firewall Filters

1. Reject akses ping ke R1 dari network 23.23.23.0/24

Pengujian

Prefix List

2. Discard akses ssh ke R1 dari semua IP, kecuali network 23.23.23.0/24 dan 14.14.14.0/24.

buat prefix-list untuk trusted address yang nantinya akan diaccept.
[edit]
root@R1# **set policy-options prefix-list** trusted-ssh **23.23.23.0/24**
root@R1# **set policy-options prefix-list** trusted-ssh **14.14.14.0/24**

buat firewall filter
[edit firewall filter ssh-in term 1]
root@R1# **set from source-address 0.0.0.0/0**
root@R1# **set from source-prefix-list** trusted-ssh **except**
root@R1# **set from destination-address 1.1.1.1/32**
root@R1# **set from protocol tcp port 22**
root@R1# **set then discard**

[edit firewall filter ssh-in term 1]
root@R1# **set then accept**

apply firewall filter ke interface em0 filter input
[edit]
root@R1# **set interfaces lo0 unit 0 family inet filter input ssh-in**

Prefix List

2. Discard akses ssh ke R1 dari semua IP, kecuali network 23.23.23.0/24 dan 14.14.14.0/24.

Pengujian

Firewall Log

3. Masukan ke dalam log setiap ada percobaan akses ssh.

edit filter ssh-in buat firewall filter
[edit firewall filter ssh-in term 1]
root@R1# **set then log**