

OPTIMASI NETWORK FIREWALL DAN LIMITASI BANDWITH UNTUK PRIORITAS VIDEO CONFERENCE MENGGUNAKAN ROUTER MIKROTIK

Numan Musyaffa

Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, Jakarta

E-mail: numan.nmf@nusamandiri.ac.id

Abstrak

Dengan perkembangan teknologi, kebutuhan akan jaringan komunikasi semakin meningkat dan selama pandemic virus covid-19 berlangsung dari satu tahun yang lalu memaksa masyarakat dari berbagai kalangan tidak untuk melakukan kontak fisik menyebabkan berbagai kegiatan banyak dilakukan dirumah secara daring atau yang lebih populer dengan sebutan *Work From Home (WFH)* atau bekerja dari rumah. Kegiatan belajar dan mengajar baik di sekolah maupun perguruan tinggi merupakan salah satu kegiatan yang menggunakan belajar secara daring dari rumah di masa pandemi Covid-19 ini. Kegiatan belajar mengajar dan bekerja yang digelar dalam jaringan (online) selama pandemi membuat lalu lintas data melesat tajam, aplikasi *video conference* yang ada, zoom berada di deretan paling atas dari sisi banyaknya pengguna. Hal tersebut tidak lepas dari banyaknya fitur yang ditawarkan aplikasi ini kepada penggunanya namun Salah satu hambatan yang harus dihadapi adalah terbatasnya *bandwith* internet di Indonesia. Muncul masalah koneksi lambat jika banyak klien menggunakan secara bersamaan sehingga penggunaan *video conference* menjadi tersendat-sendat dikarenakan pemakaian *bandwith* yang tidak sesuai, diperlukan penandaan paket data yang masuk sebagai *browsing* internet atau sebagai paket data untuk *video conference* setelah itu membatasi paket data yang akan digunakan sebagai *browsing* sehingga akan memprioritaskan paket data yang akan digunakan untuk *video conference* menggunakan fitur dari Router Mikrotik yaitu menggunakan *firewall mangle* dan membuat limitasi *bandwith* menggunakan *Simple Queue*.

Kata kunci: *firewall*, *video conference*, *router*

Abstract

With the development of technology, the need for communication networks has increased and during the Covid-19 pandemic, which took place one year ago, forcing people from various backgrounds not to make physical contact, causing many activities to be carried out at home online or more popularly known as *Work From Home (WFH)* or working from home. Teaching and learning activities both in schools and colleges are activities that use online learning from home during the Covid-19 pandemic. Teaching and learning activities that were held online during the pandemic made data traffic skyrocket, existing *video conferencing* applications, zooming were in the top row in terms of the number of users. This is inseparable from the many features that this application offers to its users. One of the obstacles that must be faced is the limited internet bandwidth in Indonesia. Slow connection problems arise if many clients use simultaneously so that the use of *video conferencing* becomes choked up due to inappropriate bandwidth usage, it is necessary to mark incoming data packets as internet browsing or as data packets for *video conferencing* after that limit the data packets to be used as browsing so that it will prioritize data packets that will be used for *video conferencing* using the features of the Mikrotik Router, namely using a *firewall mangle* and making bandwidth limitations using *Simple Queue*.

Key word: *firewall*, *video conference*, *router*

1. Pendahuluan

Dengan perkembangan teknologi, kebutuhan akan jaringan komunikasi semakin meningkat (Musyaffa & Ryansyah, 2020), Perkembangan pengguna di internet terus mengalami peningkatan secara signifikan, berdasarkan hasil survey *We Are Social* pada Januari 2020 pengguna internet di Indonesia sebanyak 172,4 juta, pengguna *social*

media di Indonesia sebanyak 160 juta dan koneksi seluler di Indonesia mencapai 338,2 juta jumlahnya 124% dari total penduduk Indonesia (Indonesia, 2020) dan selama pandemic virus covid 19 berlangsung dari satu tahun yang lalu memaksa masyarakat dari berbagai kalangan tidak untuk melakukan kontak fisik (Harun, 2020), menyebabkan berbagai kegiatan banyak dilakukan

dirumah secara daring atau yang lebih populer dengan sebutan *Work From Home (WFH)* atau bekerja dari rumah. Kegiatan belajar dan mengajar baik di sekolah maupun perguruan tinggi merupakan salah satu kegiatan yang menggunakan belajar secara daring dari rumah di masa pandemi Covid-19 ini. Kegiatan belajar mengajar dan bekerja yang digelar dalam jaringan (online) selama pandemi membuat lalu lintas data melesat tajam (Rahman, 2020).

Diantara sekian banyak aplikasi *video conference* yang ada, zoom berada di deretan paling atas dari sisi banyaknya pengguna. Hal tersebut tidak lepas dari banyaknya fitur yang ditawarkan aplikasi ini kepada penggunaanya (Andi, 2020), untuk digunakan baik pembelajaran daring maupun webinar namun Salah satu hambatan yang harus dihadapi adalah terbatasnya *bandwith* internet di Indonesia. *Bandwith* (lebar pita) merupakan istilah yang digunakan untuk menggambarkan berapa banyak informasi dapat dikirim melalui koneksi jaringan computer (Fitriastuti & Utomo, 2014), Kebutuhan akan pemakaian internet yang banyak akan membutuhkan *bandwith (lebar pita)* pada Router mikrotik yang besar juga, terlebih untuk melakukan *video conference* pada masa pandemic covid 19 saat ini, Muncul masalah koneksi lambat jika banyak klien menggunakan secara bersamaan (Hasan & Dkk, 2016), sehingga penggunaan video conference menjadi tersendat-sendat dikarenakan pemakaian *bandwith* yang tidak sesuai.

Dari permasalahan diatas diperlukan penandaan paket data yang masuk sebagai *browsing* internet atau sebagai paket data untuk *video conference* setelah itu membatasi paket data yang akan digunakan sebagai *browsing* sehingga akan memprioritaskan paket data yang akan digunakan untuk *video conference* menggunakan fitur dari Router Mikrotik yaitu menggunakan *firewall mangle* dan membuat limitasi *bandwith* menggunakan *Simple Queue*

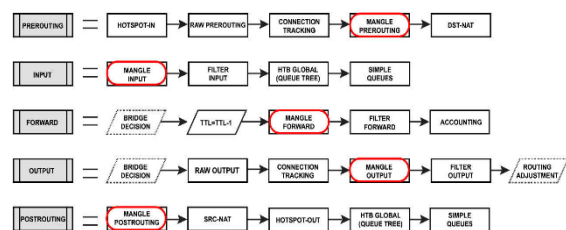
2. Metode Penelitian

2.1 Mikrotik Router

Router Mikrotik merupakan sebuah perangkat keras yang terdapat didalamnya system operasi berbasis linux yang berfungsi sebagai router dalam jaringan, Sistem operasi yang terdapat dalam mikrotik disebut juga MikroTik RouterOS. MikroTik RouterOS memiliki beberapa kelebihan dan mudah dalam konfigurasi karenaterdapat aplikasi pada Sistem Operasi Windows yang disebut Winbox. Kelebihan lainnya juga dapat dipasang pada PC dan hanya memerlukan sumber daya yang sedikit (Musyaffa & Sastra, 2019).

2.2 Firewall Mangle

Firewall mangle merupakan salah satu fitur firewall yang terdapat dalam MikroTik Router OS yang berfungsi sebagai penanda paket maupun koneksi data yang di *request* oleh *user*, Dalam prakteknya firewall mangle ini memiliki banyak fitur yang dapat dipergunakan (Fitriastuti & Utomo, 2014). *Firewall mangle* mempunyai *rules* seperti pada gambar 1.



Gambar 1. Firewall Mangle rules

(Sumber: <https://help.mikrotik.com/docs/display/ROS/Mangle>)

2.3 Address List

Address list adalah “tempat” untuk mengelompokkan IP yang akan dijadikan sebuah group (Paul, 2004). Dengan menggunakan *address list* ini lebih memudahkan apabila ingin menggunakan beberapa IP saja dari dalam satu segmen IP. IP yang akan di daftarkan nantinya dapat secara acak, hanya saja penamaan group dari IP tersebut harus sama apabila ingin masuk dalam satu group. Fungsinya adalah apabila memerlukan pembatasan kecepatan akses secara group, dapat menggunakan fitur ini untuk melakukan pendataan IP.(Fitriastuti & Utomo, 2014)

2.4 Metode Simple Queue

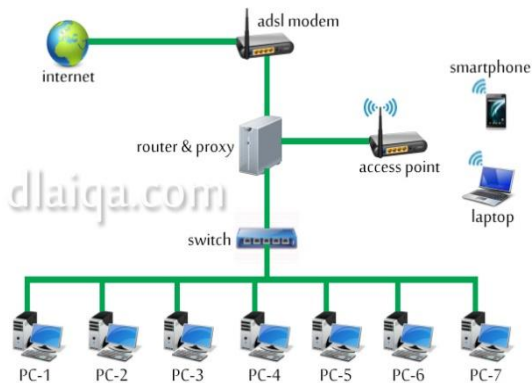
Metode *Simple Queue* merupakan metode yang cukup sederhana dalam melakukan konfigurasi. Pada metode *simple queue* kita tidak bisa mengalokasikan *bandwith* khusus buat *Internet Control Message Protocol* (ICMP) sehingga apabila pemakaian *bandwith* pada klien sudah penuh *ping time* nya akan naik dan bahkan *Request Time Out* (RTO) (Ilham, 2018).

2.5 winbox

WinBox adalah sebuah utility yang digunakan untuk melakukan remote ke server mikrotik dalam mode GUI Jika untuk mengkonfigurasi mikrotik dalamtext mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan winbox ini dapat melakukan konfigurasi mikrotik melalui komputer client. (Fitriastuti & Utomo, 2014).

2.6 Perancangan Topologi

Pada perancangan optimasi network firewall dan limitasi bandwith ini membutuhkan hanya 1 router mikrotik dan juga *Access Point* dan sedikit perangkat lainnya yang berguna untuk menyebarkan sinyal wireless jika klien tidak membutuhkan kabel untuk koneksinya, topologi ini dapat disebut juga dengan topologi *Small Office Home Office* (SOHO) yang bisa dilihat pada gambar 2 di bawah ini:



Gambar 2. Topologi Jaringan LAN SOHO
(Sumber: <https://www.dlaiaqa.com/2016/11/topologi-jaringan-soho-small-office.html>)

2.7 Sumber Data

Sumber data yang peneliti ambil pada penelitian ini dengan mendapatkan data ip dan protocol jaringan yang digunakan pada situs *video conference zoom meeting* itu sendiri seperti pada table di bawah ini.

Tabel 1. Protocol Jaringan zoom meeting

Protocol	Ports	Sum ber	Tujuan
TCP	80, 443	Klien Zoom dan Konektor Rapat	Zoom web
TCP	3478,3479,5090,5091,8801-8810	Semua klien zoom	MeetingConnector.IP
UDP	3478,3479,5090,5091,8801-8810	Semua klien zoom	MeetingConnector.IP

Pada gambar dibawah ini peneliti juga mengambil data IP Address yang digunakan untuk melakukan *video conference zoom meeting*.

To configure your network firewall, please see the following table. The following rules should be applied to outbound traffic. Zoom will communicate to the destination port received when the client makes its connection. The firewall should be configured to allow these return connections.

Protocol	Ports	Source	Destination
TCP	80,443	All Zoom clients	*zoomus
			IPv4:
			3.7.35.0/25
			3.21.137.128/25
			3.22.11.0/24
			3.23.93.0/24
			3.25.41.128/25
			3.25.42.0/25
			3.25.49.0/24
			3.80.20.128/25
			3.96.19.0/24
			3.101.32.128/25
			3.101.52.0/25
			3.104.34.128/25
			3.120.121.0/25
			3.127.194.128/25
			3.208.72.0/25
			3.211.241.0/25

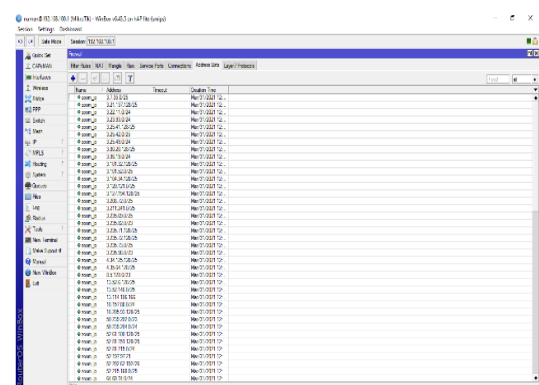
Gambar 3. Ip address server zoom meeting
(Sumber: <https://support.zoom.us/hc/en-us/articles/201362683-Network-firewall-or-proxy-server-settings-for-Zoom>)

3. Hasil Penelitian dan Pembahasan

3.1. Konfigurasi Address List

Langkah Pertama peneliti memasukan Address List Ip Server zoom meeting yang didapatkan dari website resmi video conference zoom meeting dengan cara :

1. Masuk kedalam menu winbox
2. pilih IP pada Tab menu samping Kiri di winbox
3. pilih **Firewall**, kemudian pilih tab **Address List** pada bagian atas menu Firewall tersebut
4. lalu pilih tanda + atau add, lalu masukan semua *ip address server zoom* yang sudah di dapatkan pada web resmi zoom meeting seperti pada gambar contoh dibawah ini:



Gambar 4. Tampilan address List pada Winbox

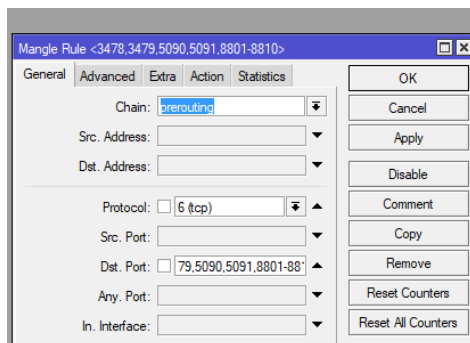
Namun *Ip address* yang ditambahkan pada gambar diatas tidak semua *Ip Server zoom* ada, maka harus menambahkan *rule firewall mangle* agar terisi List secara otomatis.

3.2. Konfigurasi Firewall Mangle untuk meng-update address list zoom

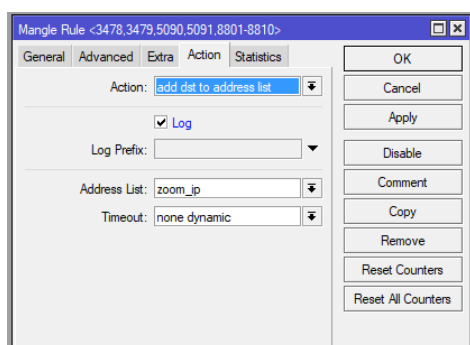
Karena *video conference zoom* menggunakan 2 protocol jaringan yaitu **TCP** dan **UDP** maka kita tambahkan pada **Firewall mangle** satu persatu :

1. Buka winbox, pilih **IP** pada tab di samping kiri
2. Pada tab **firewall** kemudian pilih **Mangle** dan pilih add atau tanda +
3. Setelah terbuka jendela **Mangle** pada tab **General** pada kolom **chain** pilih **Prerouting**
4. Pada kolom **protocol** pilih **TCP** dan pada kolom **dst (destination) port** isikan port **3478,3479,5090,5091,8801-8810**.
5. Kemudian pilih tab **Action** lalu pada kolom **Action** dibawah pilih **add dst to address list**.
6. Lalu pada kolom **address list** pilih **Zoom_ip** (atau ip address list yang sudah kita setting sebelumnya). Kemudian pilih **Apply** dan **OK**.
7. Lakukan hal yang sama seperti Langkah diatas untuk membuat settingan **UDP** nya. Cuma bedanya adalah pada kolom **protocol** pilih **UDP**.

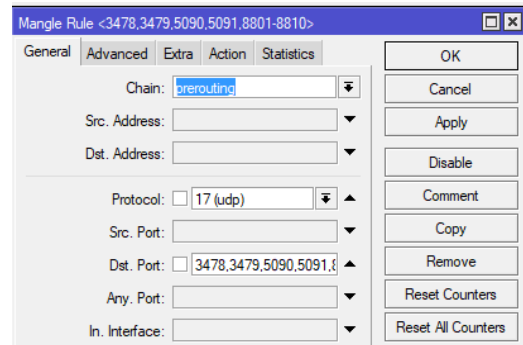
Settingan **protocol** yang kita buat seperti gambar di bawah ini baik untuk **protocol TCP** maupun **UDP**:



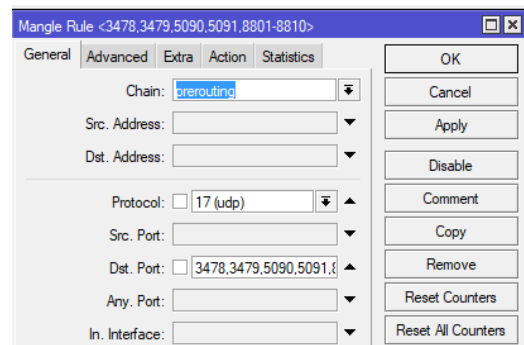
Gambar 5. Tab General Firewall Mangle TCP



Gambar 6. Tab Action Firewall Mangle TCP



Gambar 7. Tab General Firewall Mangle UDP



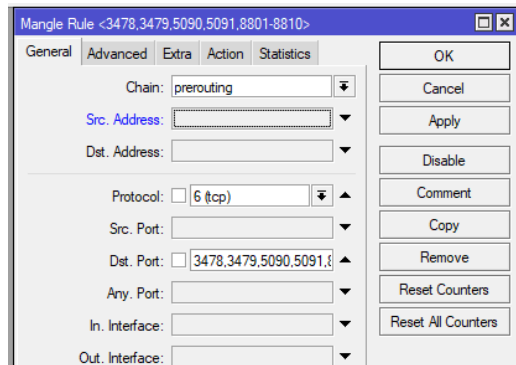
Gambar 8. Tab Action Firewall Mangle UDP

3.3 Konfigurasi Firewall Mangle Untuk Mark Connection video conference zoom.

Setelah memberikan konfigurasi parameter untuk menambahkan secara otomatis **address list** pada **video conference zoom**, sekarang tambahkan parameter untuk menandai koneksi **video conference zoom**, berikut Langkah-langkahnya :

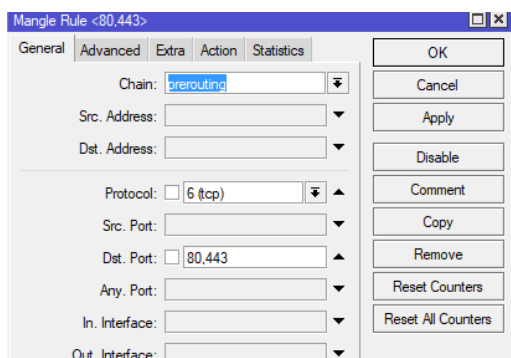
1. Buka **winbox** Buka winbox, pilih **IP** pada tab di samping kiri.
2. Pada tab **firewall** kemudian pilih **Mangle** dan pilih add atau tanda +
3. Setelah terbuka jendela **Mangle** pada tab **General** pada kolom **chain** pilih **Prerouting**.
4. Pada kolom **protocol** pilih **TCP** dan pada kolom **dst (destination) port** isikan port **3478,3479,5090,5091,8801-8810**.
5. Kemudian pilih tab **Advance** dan pilih **dst address list** dengan **Zoom_ip**.
6. Kemudian pilih tab **Action** lalu pada kolom **Action** dibawah pilih **Mark-Connection** dan pada kolom **new connection Mark** di isi **koneksi_zoom**.
7. Lalu pada kolom **address list** pilih **Zoom_ip** (atau ip address list yang sudah kita setting sebelumnya). Kemudian pilih **Apply** dan **OK**.

8. Karena **zoom** dapat di akses menggunakan **web** maka tambahkan **mark** koneksi **zoom** dengan **protocol TCP** yang **portnya** berisi **80, 443** namun untuk **tab action** sama seperti konfigurasi yang diatas, seperti pada gambar berikut :

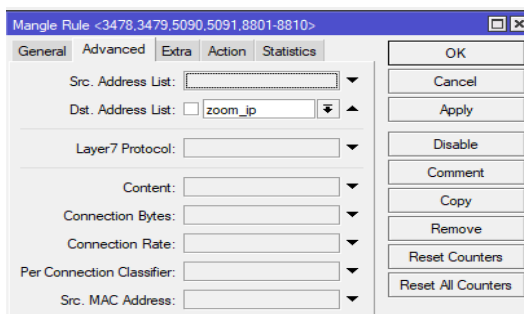


Gambar 9. Tab General konfigurasi Firewall Mangle TCP web Zoom

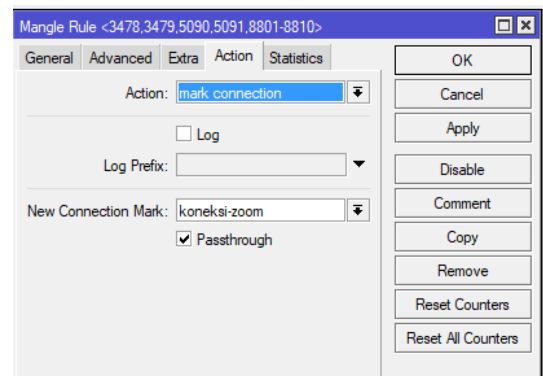
9. Lakukan hal yang sama seperti Langkah diatas untuk membuat settingan **UDP** nya Cuma bedanya adalah pada kolom **protocol** pilih **UDP**. Settingan **protocol** yang kita buat seperti gambar di bawah ini baik untuk **protocol TCP** maupun **UDP**:



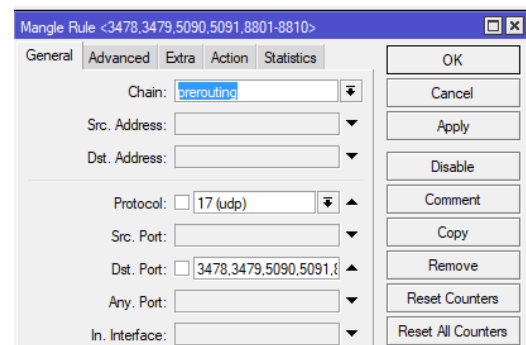
Gambar 10. Tab General Firewall Mangle TCP



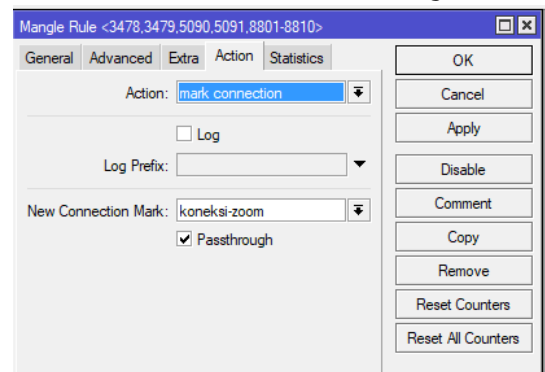
Gambar 11. Tab Advance Firewall Mangle TCP



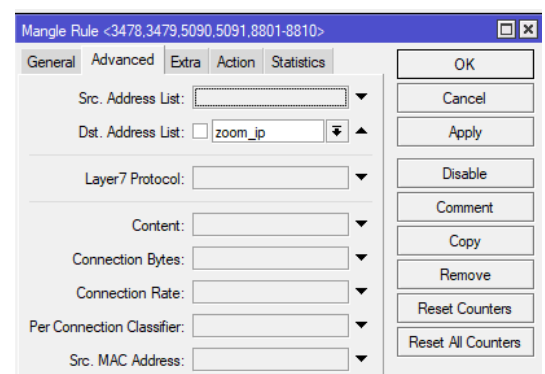
Gambar 12. Tab Action Firewall Mangle TCP



Gambar 13. Tab General Firewall Mangle UDP



Gambar 14. Tab Advance Firewall Mangle UDP



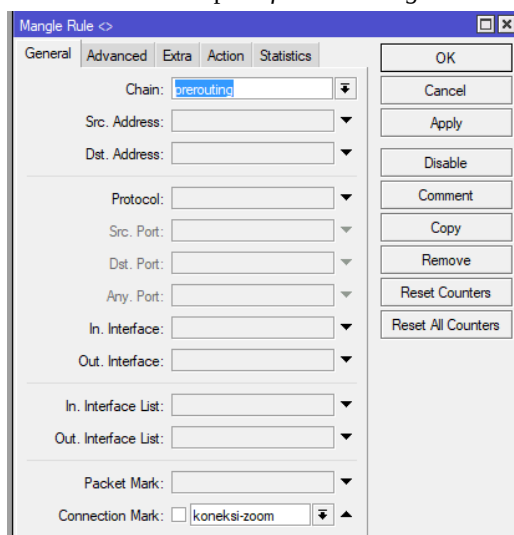
Gambar 15. Tab Action Firewall Mangle UDP

3.4 Konfigurasi Firewall Mangle Untuk Mark Packet video conference zoom.

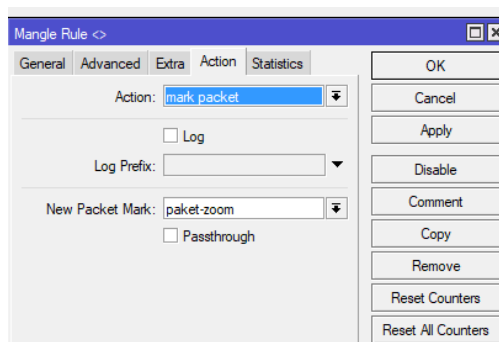
Parameter berikut ini akan menandakan paket **video conference zoom** yang akan melewati **router** dengan tujuan nanti nya akan terbaca Ketika nantinya sudah diberikan limitasi **bandwith** agar paket **zoom** ini akan terdeteksi prioritas dibandingkan dengan **bandwith browsing**, berikut konfigurasi **parameter** nya:

1. Buka **winbox**, pilih **IP** pada **tab** di samping kiri.
2. Pada tab **firewall** kemudian pilih **Mangle** dan pilih **add** atau tanda +.
3. Setelah terbuka jendela **Mangle** pada **tab General** pada kolom **chain** pilih **Prerouting**
4. Kemudian pada **kolom Connection Mark** pilih **Koneksi_zoom**.
5. Pada Tab **Action** pilih **Action** isi kolom **Mark Packet**.
6. Kemudian pilih **APPLY** dan **OK**

Berikut adalah gambar dari konfigurasi mark Packet zoom pada firewall mangle :



Gambar 16. Tab General Firewall Mangle TCP Mark Packet zoom



Gambar 17. Tab Action Firewall Mangle TCP Mark Packet Zoom

Pada gambar di bawah ini adalah hasil dari beberapa **rule** pada **mangle** yang telah dikonfigurasi

Mangle Rules															
Mangle Rules		ACT	Template	Flow	Service Ports	Connections	Address Lists	Language	Protocol						
															
Reset Counters															
Reset All Counters															
First															
id															
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Sec. Ad.	Dst. Ad.	Bytes	Packets
0	add address list zoom				6 (tcp)	3478,347								0.0	0
1	add src to address list	prerouting			17 (udp)	3478,347								0.0	0
2	mark koneksi zoom														
3	mark connection	prerouting			6 (tcp)	3478,347						zoom_ip		0.0	0
4	mark connection	prerouting			17 (udp)	3478,347						zoom_ip		0.0	0
5	mark connection	prerouting			6 (tcp)	3478,347						zoom_ip		0.0	0
6	mark packet														
7	mark packet	prerouting												0.0	0

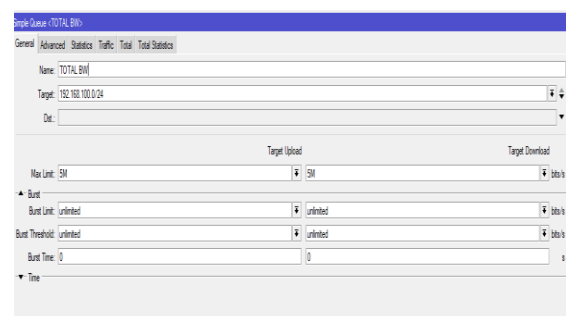
Gambar 18. Hasil Konfigurasi firewall Mangle

3.5 Konfigurasi Simple Queue Untuk Alokasi bandwith video conference zoom.

Selanjutnya konfigurasi limitasi bandwith dengan metode **simple queue** untuk memprioritaskan **bandwith video conference zoom**, seperti dibawah ini langkahnya:

1. Buka **winbox** pilih **Queues**.
2. Pada tab **queue** kemudian pilih **add** atau tanda +
3. Setelah terbuka jendela **queue** pada tab **General**, kolom **Name** kita isikan nama limitasi sebagai contoh **BW TOTAL**
4. Kemudian pada kolom target isikan **IP** dari **LAN** yang menuju internet dari **Mikrotik** sebagai contoh **192.168.100.0/24**.
5. Kemudian pada **kolom target Upload** dan **target Download** dimisalkan memberikan **Bandwith 5MB**
6. Kemudian Pilih **APPLY** dan **OK**.

Berikut adalah gambar dari hasil konfigurasi nya :

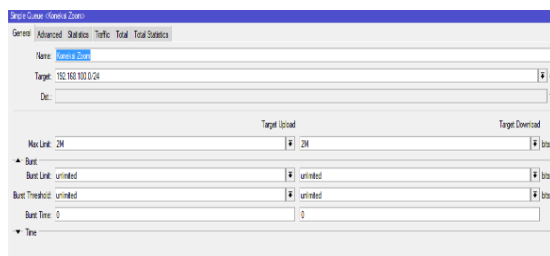


Gambar 19. Konfigurasi Limitasi Badwith Total

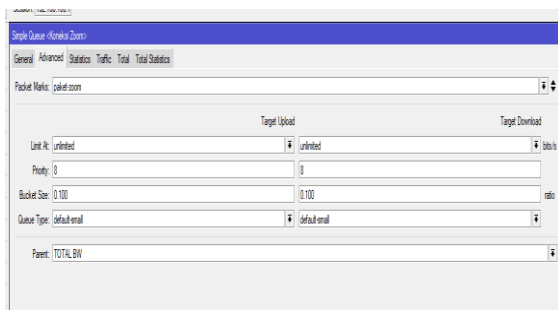
Untuk selanjutnya adalah memisahkan Bandwith **video Conference**, berikut adalah konfigurasi parameternya :

1. Buka **winbox** pilih **Quees**.
2. Pada tab **quee** kemudian pilih **add** atau tanda +
3. Setelah terbuka jendela **quee** pada tab **General**, kolom **Name** kita isikan nama limitasi sebagai contoh **Koneksi Zoom**.
4. Kemudian pada kolom target isikan **IP** dari **LAN** yang menuju internet dari **Mikrotik** sebagai contoh **192.168.100.0/24**.
5. Kemudian pada kolom target **Upload** dan **target Download** dimisalkan memberikan **Bandwith 3MB**
6. Kemudian pilih **Tab Advance** dan isi **Packet Marks** dengan memilih **Paket-zoom**
7. Kemudian Pilih **APPLY** dan **OK**.

Berikut adalah gambar dari hasil konfigurasi nya :



Gambar 20. Tab General Limitasi Badwith video Conference Zoom



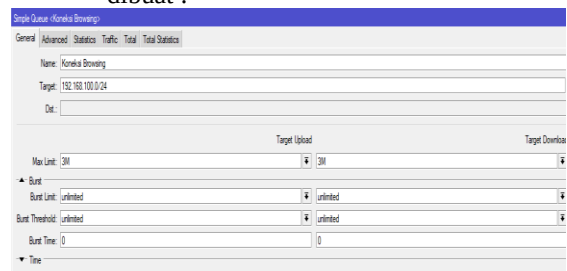
Gambar 21. Tab Advance Limitasi Badwith video Conference Zoom

Untuk selanjutnya adalah memisahkan Bandwith **Koneksi Browsing**, berikut adalah konfigurasi parameternya :

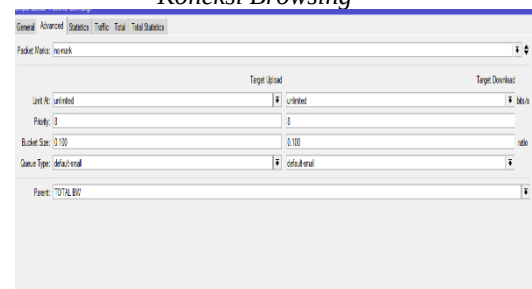
1. Buka **winbox** pilih **Quees**.
2. Pada tab **quee** kemudian pilih add atau tanda +
3. Setelah terbuka jendela **quee** pada tab **General**, kolom **Name** kita isikan nama limitasi sebagai contoh **Koneksi Browsing**.

4. Kemudian pada kolom target isikan **IP** dari **LAN** yang menuju internet dari Mikrotik sebagai contoh **192.168.100.0/24**.
5. Kemudian pilih **Tab Advance** dan isi **Packet Marks** dengan memilih **Paket-zoom**
6. Kemudian Pilih **APPLY** dan **OK**.

Dan berikut ini adalah gambar dari hasil konfigurasi limitiasi bandwith yang sudah dibuat :



Gambar 22. Tab General Limitasi Badwith Koneksi Browsing



Gambar 23. Tab Advance Limitasi Badwith Koneksi Browsing

Dan di bawah ini adalah gambar dari hasil konfigurasi limitiasi bandwith yang sudah dibuat keseluruhan :

Queue List						
Simple Queues						
#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bits/s)
0	TOTAL BW	192.168.100.0/24	5M	5M		
1	Koneksi Zoom	192.168.100.0/24	2M	2M	paket-zoom	
2	Koneksi Browsing	192.168.100.0/24	3M	3M	no-mark	

Gambar 24. Hasil Konfigurasi limitasi Bandwith

3.6 Tahap Pengujian

Disini peneliti melakukan pengujian pertama untuk Pembagian **Bandwith** yang sudah dilimitasi menggunakan **simple quee** dan di tandai menggunakan untuk prioritas **Video Conference**, Ketika sedang ada aktifitas webinar ataupun penggunaan zoom maka **bandwith** dan paket yang digunakan adalah **bandwith Koneksi_Zoom** seperti gambar di bawah ini :

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Download Avg. R.	Total Max Limit (bits/s)
0	TOTAL BW	192.168.100.0/24	5M	5M		26.4 kbps	
1	Koneksi Zoom	192.168.100.0/24	3M	3M	paket.zoom	1302 kbps	
2	Koneksi Browsing	192.168.100.0/24	2M	2M	no-mark	38.3 kbps	

Gambar 25. Hasil Pengujian limitasi *Bandwith video conference zoom*

Pada pengujian kedua, peneliti melakukan pengujian apabila Ketika bandwith yang digunakan adalah selain video conference zoom, maka akan menggunakan bandwith yang sudah di berikan limitasi nya agar Ketika melakukan browsing tidak mengganggu kualitas dari bandwith yang digunakan video conference zoo, berikut adalah hasil dari pengujian yang dilakukan:

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Download Avg. R.	Total Max Limit (bits/s)
0	TOTAL BW	192.168.100.0/24	5M	5M		1762.5 kbps	
1	Koneksi Zoom	192.168.100.0/24	3M	3M	paket.zoom	95 kbps	
2	Koneksi Browsing	192.168.100.0/24	2M	2M	no-mark	1173.4 kbps	

Gambar 25. Hasil Pengujian limitasi *Bandwith Koneksi_browsing*.

4. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa, optimasi network firewall dan limitasi bandwith untuk prioritas video conference dapat menjadi solusi Ketika melakukan video conference tidak menjadi terhambat dikarenakan paket data video conference sudah di pisahkan dan bandwith untuk melakukan video conference juga sudah dipisahkan sehingga Ketika melakukan kegiatan seperti

browsing dan membuka web lain nya juga tidak mengganggu bandwith yang sudah diberikan pada limitasi bandwith diatas.

5. Referensi

- Andi. (2020). Aplikasi Video Conference Terbaik Untuk Menunjang WFH. Retrieved March 31, 2021, from <https://qwords.com/blog/video-conference/>
- Fitriastuti, F., & Utomo, D. P. (2014). IMPLEMENTASI BANDWDITH MANAGEMENT DAN FIREWALL SYSTEM MENGGUNAKAN MIKROTIK OS. *Jurnal Teknik*, 4(1), 1–9.
- Harun, M. (2020). Evaluasi Kualitas Perangkat Lunak Pada Aplikasi Zoom Cloud Meetings Untuk Pembelajaran Elearning. *Journal of Chemical Information and Modeling*, 5(9), 1689–1699.
- Hasan, M., & Dkk. (2016). Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V.5.20 Di Sekolah Dasar Negeri 24 Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer*, 2(1), 10–19. Retrieved from stmik-binamulia.ac.id
- Ilham, D. N. (2018). Implementasi Metode Simple Queue Dan Queue Tree Untuk Optimasi Manajemen Bandwith Jaringan Komputer Di Politeknik Aceh Selatan. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 2(1), 43–50.
- Indonesia, D. (2020). we are social, “Digital 2020 Indonesia,.” Retrieved March 31, 2021, from <https://datareportal.com/reports/digital-2020-indonesia>
- Musyaffa, N., & Ryansyah, M. (2020). Implementation of VPN Using Router MikroTik at Al-Basyariah Education Foundation Bogor, 12(2), 49–55.
- Musyaffa, N., & Sastra, R. (2019). Analisa Kinerja Kualitas Layanan (QoS) Virtual Router Redundancy Protocol (VRRP) Menggunakan Mikrotik Routerboard, V(1), 1–5.
- Rahman, A. (2020). IMPLEMENTASI MANAJEMEN BANDWITH UNTUK VIDEO CONFERENCE DENGAN METODE FIREWALL MANGLE PADA, (Ciastech), 341–350.