

Panduan Singkat Extended Access List Pada Cisco c3640

Author : Antonius Robotsoft

www.robotsoft.co.id – www.freenergi.com – www.jasaplus.com

github : <https://github.com/antoniusrobotsoft>

Access list pada cisco router masih bisa dibypass dengan beberapa metode seperti paket terfragmentasi, SNMP spoof, dll akan tetapi cisco access list masih merupakan fitur paket filtering yang cukup handal digunakan. Access list dasar di cisco, hanya akan menyaring paket berdasarkan alamat ip. Jika komunikasi data menggunakan udp misal pada saat cisco router akan menerima paket snmp yang merupakan udp based protocol, seperti kita ketahui bersama bahwa udp merupakan connectionless yang mana kita bisa memalsukan source address maka kita bisa membypass access list pada cisco (misal kita kirimkan paket snmp dengan source address yang diijinkan).

Untuk itu kita perlu menggunakan yang namanya extended access list. Dengan menggunakan extended access list pada cisco, kita tidak hanya menyaring paket berdasarkan source address tapi juga berdasarkan nomor port, alamat tujuan, dll.

Kali ini kita akan mencoba menggunakan extended access list secara singkat pada cisco c3640.

Pertimbangan Dalam Penggunaan Extended Access List

Sebelum menerapkan extended access list, berikut ini beberapa contoh pertimbangan rule yang bisa kita terapkan : alamat2 ip apa saja yang diijinkan untuk outbound dan inbound traffic ? Nomor port berapa saja yang diijinkan untuk inbound dan outbound traffic ? Pada interface apa kita akan menerapkan extended access list ?

Pada contoh kali ini, kebetulan saya memiliki suatu router c3640 dengan access listnya, mari kita cek dengan perintah : "show access lists" atau bisa juga dengan perintah : "show running-config" atau bisa disingkat : "show run"

```

cr0security@cr0security-Vostro1310:~$ telnet 192.168.99.225
Trying 192.168.99.225...
Connected to 192.168.99.225.
Escape character is '^]'.

User Access Verification

Password:
Router35>ena
Password:
Router35#show access-lists
Standard IP access list 1
  10 permit 10.200.0.0, wildcard bits 0.0.0.255
Extended IP access list 102
  10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
Router35#

```

Pada contoh kali ini, kita bisa melihat kita punya 1 standard access list dan 1 extended access list. Extended access list selalu memiliki nomor antara 100 sampai dengan 199.

```

Router35#show running-config
Building configuration...
=====snip=====
access-list 1 permit 10.200.0.0 0.0.0.255
access-list 102 permit ip 10.200.0.0 0.0.0.255 any
=====snip=====
Router35#

```

10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
 extended access list dengan nomor 102 di atas akan mengizinkan trafik dengan ip range :
 10.200.0.1-255, di mana access list ini diaplikasikan pada dua interface, seperti kita lihat di bawah ini :

```

Router35#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router35(config)#int FastEthernet0/0
Router35(config-if)#do show access-list
Standard IP access list 1
  10 permit 10.200.0.0, wildcard bits 0.0.0.255
Extended IP access list 102
  10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
Router35(config-if)#int FastEthernet1/0
Router35(config-if)#do show access-list
Standard IP access list 1
  10 permit 10.200.0.0, wildcard bits 0.0.0.255
Extended IP access list 102
  10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
Router35(config-if)#

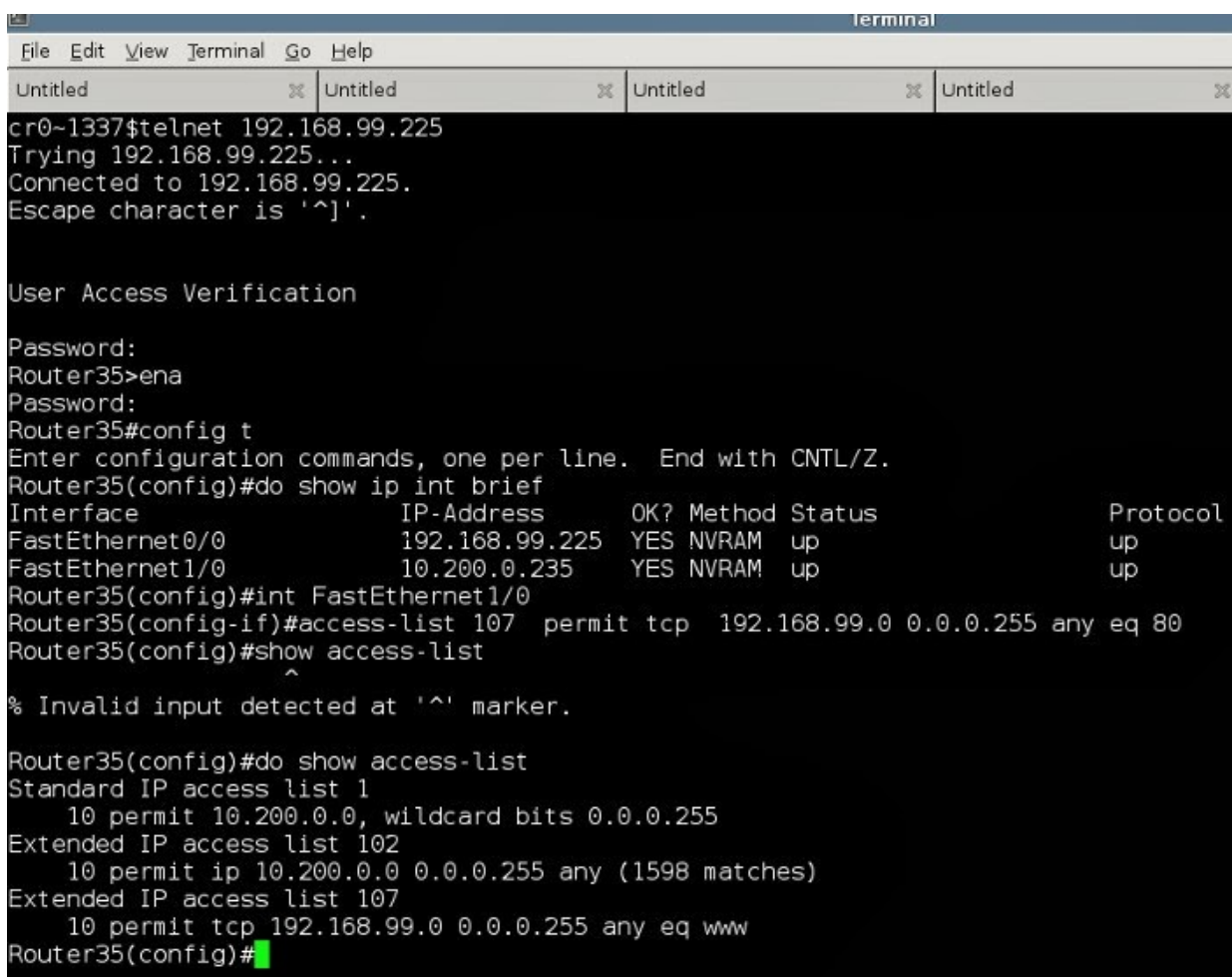
```

Menambah dan Mengurangi Extended Access List

Sintaks access list :

access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard
[precedence precedence]

di mana sudah disebutkan di atas bahwa extended access list selalu bernomor antara 100 sampai dengan 199. Misal kita akan membuat satu extended access list baru untuk mengizinkan paket tcp dari subnet 192.168.99 dengan destination port 80 yang akan diterapkan pada interface FastEthernet1/0:



```
cr0~1337$telnet 192.168.99.225
Trying 192.168.99.225...
Connected to 192.168.99.225.
Escape character is '^]'.

User Access Verification

Password:
Router35>ena
Password:
Router35#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router35(config)#do show ip int brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          192.168.99.225  YES NVRAM    up          up
FastEthernet1/0          10.200.0.235   YES NVRAM    up          up
Router35(config)#int FastEthernet1/0
Router35(config-if)#access-list 107 permit tcp 192.168.99.0 0.0.0.255 any eq 80
Router35(config)#show access-list
^
% Invalid input detected at '^' marker.

Router35(config)#do show access-list
Standard IP access list 1
 10 permit 10.200.0.0, wildcard bits 0.0.0.255
Extended IP access list 102
 10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
Extended IP access list 107
 10 permit tcp 192.168.99.0 0.0.0.255 any eq www
Router35(config)#
```

Berikut ini konfigurasi access list yang kita tambahkan :

```
Router35#config t
```

```
Router35(config)#int FastEthernet1/0
```

```
Router35(config-if)#access-list 107 permit tcp 192.168.99.0 0.0.0.255 any eq 80
```

Pada contoh di atas kita telah menambahkan access list dengan nomor 107 untuk mengizinkan paket tcp dari source address subnet 192.168.99 dengan port tujuan 80. Untuk melakukan verifikasi :

```
Router35(config)#do show access-list
```

```
Standard IP access list 1
```

```
 10 permit 10.200.0.0, wildcard bits 0.0.0.255
```

```
Extended IP access list 102
```

```
 10 permit ip 10.200.0.0 0.0.0.255 any (1598 matches)
```

```
Extended IP access list 107
```

```
 10 permit tcp 192.168.99.0 0.0.0.255 any eq www
```

```
Router35(config)#
```

Untuk menghapus extended access list sangat mudah, misal kita akan hapus access list dengan nomor 107:

```
Router35(config)#no access-list 107
```

Referensi

<https://learningnetwork.cisco.com/docs/DOC-7514>