IlmuKomputer.Com
Ikatlah ilmu dengan menuliskannya

MENGENAL SECURITY PORT PADA SWITCH CISCO

Firman Setya Nugraha

Someexperience.blogspot.com

Firmansetyan@gmail.com

Dalam bidang IT, keamanan jaringan sangatlah dibutuhkan karena hal tersebut menyangkut data pentingyang sifatnya rahasia, baik bagi personal maupun enterprise. Kali ini saya akan mencoba membahas tentang konfigurasi keamanan pada Switch Cisco.

Konfigurasi Port Security

Fitur ini dapat digunakan untuk membatasi masukan sebuah interface dengan melimit dan mengidentifikasi MAC address yang diperbolehkan untuk mengakses port. Jadi apabila MAC telah ditetapkan, maka port selain yang ditetapkan tidak akan dapat terkoneksi.

Perintah yang digunakan adalah:

Router(config) # switchport port-security (mac-address)

*NB: apabila port di shutdown, maka semua mac yang dipelajari secara dinamis akan terhapus.

Apabila seseorang mencoba melanggar dengan mecoba menghubungkan port dengan hardware dengan mac yang tidak terdaftar, maka kita dapat mengkonfigurasi interface dengan beberapa cara:

a. Membatasi: Sebuah pelanggaran port security membatasi data, hal tersebut menyebabkan security/violation counter naik, dan menyebabkan pemberitahuan SNMP dibangkitkan. Tingkat perangkap NSMP yang dibangkitkan dikontrol oleh

perintah **snmp-server enable traps port-security trap-rate**. Devault value-nya "0" menyebabkan SNMP trap akan dibangkitkan setiap pelanggaran security.

b. Shutdown- Pelanggaran security port akan menyebabkan interface untuk ditutup segera. Ketika sebuah port sudah aman dan dalam status error-disabled, kita dapat merubahnya dari status tersebut dengan memasukkan perintah konfigurasi global **errdisable recovery cause psecure_violation** atau dapat secara manual mengaktifkan kembali itu dengan mengetik **shutdown** dan **no shutdown** interface konfigurasi interface yang merupakan default mode.
Kita dapat menyesuaikan waktu untuk recover dari error tertentu dengan mematikan penyebabnya (default adalah 300 detik) dengan memasukkan **errdisable recovery interval** command.

Secara default konfigurasi port security adalah:

Feature	Default Seting
Port security	Disabled on a port
Maximum nomor security MAC address	1
Pelanggaran mode	Shutdown. Port akan shutdown ketika jumlah maksimum dari keamanan MAC address terlampaui, dan notifikasi perangkap SNMP terkirim.
Aging	Disabled
Aging type	Absolute
Static type	Disabled

Guidelines dan Pembatasan pada Port Security

- Secure port tidak bisa menjadi trunk port
- Secure port tidak bisa menjadi port tujuan untuk Switch Port Analyzer (SPAN)
- Secure port tidak dapat memiliki interface EtherChannel port channet
- Secure port tidak dapat menjadi port 802.1X. Jika mencoba untuk emngaktifkan 802.1X pada secure port, maka akan muncul pesan kesalahan dan 802.1X tidak diaktifkan. Jika mencoba untuk emngubah port 802.1X-enabled untuk secure port, pesan kesalahan muncul dan pengaturan keamanan tidak berubah.
- Secure port dan static MAC address terkonfigurasi saling terpisah.

Mengkonfigurasikan Port security pada interface:

Switch(config)# interface *interface_id*

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maxumum *value*

Switch(config-if)# switchport port-security violation {*restrict* | *shutdown*}

Switch(config-if)# switchport port-security limit rate invalid-sorce-mac

Switch(config-if)#switchport port-security mac-address *mac-address*

Switch(config-if)#end

Switch#show port-security address interface *interface_id*

Switch#show port-security address

Keterangan untuk yang bergaris miring:

- Interface_id: merupakan interface yang akan dijadikan port secure. Misal fa0/0.
- Value : merupakan jumlah secure mac address untuk interface. Rangenya 1 sampai 1024, akan tetapi defaultnya 1.
- Restrick/shutdown: merupakan mode pelanggaran, aksi yang akan dilakukan ketika pelanggaran keamanan terdeteksi:
  - Restrict: pelanggaran port security data dan menyebabkan pelanggaran keamanan menangani dengan menambah dan mengirim notifikasi perangkap SNMP
  - Shutdown: interface akan error-disabled ketikda pelanggaran keamanan dilakukan.
- Mac address: mac address yang akan dimasukkan ke dalam list

Kita dapat menggunakan port security aging untuk mengatur aging dan aging type untuk semua alamat yang aman pada port. Fitur ini dapat menghapus dan menambahkan PC pada port aman tanpa penghapusan manual MAC address yang sudah ada.

Switch (config)#interface *interface_id*

Switch(config-if)# switchport port-security [aging {static | time *aging_time* | type{absolute | inactivity}}]

Switch(config-if)#end

Switch# show port security [interface *interface_id*] [address]

Misal: menset aging time menjadi 2 jam untuk fast ethernet fa0/0

Switch (config)# interface fa0/0

Switch(config-if)# switchport port-security aging time 120

Untuk menunjukkan port security setting dengan cara:

- Switch# show port-security [interface *interface_id*]
- Switch# show port-security [interface *interface_id*] address

Bedanya adalah yang pertama menunjukkan portt security untuk switch atau untuk spesifik interface, terdapat maximum jumlah secure MAC address untuk tiap interface, jumlah secure MAC address pada interface, jumlah pelanggaran keamanan yang terjadi dan mode pelanggaran. Sedangkan yang kedua menunjukkan semua MAC address secure yang terkonfigurasi pada suma interface switch atau dalam interface spesifik dengan aging information untuk tiap alamat.

Pembatasan Layanan Jaringan

Yaitu dengan cara mematikan setiap service jaringan yang tidak perlu pada setiap switch. Ada perintah yang mempengaruhi secara global, akan tetapi ada juga yang hanya mempengaruhi satu interface. Banyak dari pengaturan konfigurasikan dapat pula digunakan untuk interface yang berbeda semisal fast ethernet, gigabitethernet.

Misal kita akan menset interface fastethernet 0/0 sampai 0/1

Switch(config)# interface range fa 0/0-1

1. Mendisable TCP dan UDP small server (TCP/UDP port 7,9,13,19) yang digunakan untuk serangan denial of service.
   Switch (config)# no service tcp-small-servers
   Switch (config)# no service udp-small-servers
2. Mendisable Bootp Server (UDP port 67) untuk meminimalkan pendistribusian gambar sistem untuk sistem Cisco yang lain.
   Switch(config)#no ip bootp server
3. Mendisable Finger (TCP port 79) untuk memberhentikan informasi tentang pengguna saat login ke switch.
   Switch(config)# no ip finger
   Switch(config)# no service finger
4. Konfigurasi autoload
   Switch(config)#no service config
   Switch(config)#no boot host
   Switch(config)#no boot network
   Switch(config)#no boot system
5. Packet assembler/disassembler (PAD)
   Switch(config)#no service pad
6. Address Resolution Protocol (ARP)
   Switch(config-if)#no ip proxy-arp
7. Internet Control Message Protocol (ICMP) Message
   Switch(config-if)#no ip unreachables
   Switch(config-if)#no ip redirects
   Switch(config-if)#no ip mask-reply
   Switch(config-if)#no ip direct-broadcast
8. Potentially Necessary Network Services
   Switch(config)#username admin privilege 0
   Switch(config)#username admin secret network
9. Domain Name System (TCP Port 53 dan UDP port 53)
   Switch(config)#ip name-server 10.1.200.97
   Switch(config)#ip domain-lookup

Switch(config)#no ip domain-lookup
Switch(config)#ip domain-name test.lab

10. Secure Shell (SSH) (TCP port 22)
    Switch(config)#hostname Switch
    Switch(config)#crypti key generate rsa
    Switch(config)#no access-list 101
    Switch(config)#access-list 101 remark Permit SSH access from administrators systems
    Switch(config)#access-list 101 permit tcp host 10.1.6.1 any eq 22 log
    Switch(config)#access-list 101 permit tcp host 10.1.6.2 any eq 22 log
    Switch(config)#access-list 101 deny ip any any log
    Switch(config)#line vty 0 4
    Switch(config-line)#access-class 101 in
    Switch(config-line)#transport input ssh
    Switch(config-line)#provilege level 0
    Switch(config-line)#exex-timeout 9 0
    Switch(config-line)#login local
11. Telnet Servet (TCP port23)

    Switch(config)# no access-list 102

    Switch(config)# access-list 102 remark Permit telnet access from administrators' systems

    Switch(config)# access-list 102 permit tcp host 10.1.6.1 any eq 23 log

    Switch(config)# access-list 102 permit tcp host 10.1.6.2 any eq 23 log

    Switch(config)# access-list 102 deny ip any any log

    Switch(config)# line vty 0 4

    Switch(config-line)# access-class 102 in

    Switch(config-line)# transport input telnet

    Switch(config-line)# privilege level 0

    Switch(config-line)# exec-timeout 9 0

    Switch(config-line)# login local

12. HTTP (TCP port80)
    Switch(config)# no ip http server
    Switch(config)# no access-list 11
    Switch(config)# access-list 11 remark Permit HTTP access from administrators' systems
    Switch(config)# access-list 11 permit host 10.1.6.1 log
    Switch(config)# access-list 11 permit host 10.1.6.2 log
    Switch(config)# access-list 11 deny any log
    Switch(config)# ip http server
    Switch(config)# ip http access-class 11

Switch(config)# ip http authentication local

13. SNMP (simple Network Management Protocol) (UDP port161,162)
    Switch(config)# no snmp-server community
    Switch(config)# no snmp-server enable traps
    Switch(config)# no snmp-server system-shutdown
    Switch(config)# no snmp-server
    Switch(config)# no access-list 12
    Switch(config)# access-list 12 permit 10.1.6.1
    Switch(config)# access-list 12 permit 10.1.6.2
    Switch(config)# snmp-server group admins v3 auth read adminview write adminview
    Switch(config)# snmp-server user root admins v3 auth md5 5ecret-5TR1N access 12
    Switch(config)# snmp-server view adminview internet included
    Switch(config)# snmp-server view adminview ipAddrEntry excluded
    Switch(config)# snmp-server view adminview ipRouteEntry excluded
    Switch(config)# no access-list 12
    Switch(config)# access-list 12 permit 10.1.6.1
    Switch(config)# access-list 12 permit 10.1.6.2
    Switch(config)# snmp-server community g00d-5tr1n9 ro 12
    Switch(config)# snmp-server host 10.1.6.1 traps g00d-5tr1n9-2
    Switch(config)# snmp-server host 10.1.6.2 traps g00d-5tr1n9-2
    Switch(config)# snmp-server trap-source Loopback0
    Switch(config)# snmp-server enable traps
14. Cisco Discovery protocol (CDP)
    Switch(config)# no cdp run
    Switch(config)# no cdp advertise-v2
    Switch(config)# interface range fastethernet 0/1 - 24
    Switch(config-if)# no cdp enable
    Switch(config)# cdp run
    Switch(config)# interface VLAN10
    Switch(config-if)# no cdp enable
    Switch(config)# interface VLAN101
    Switch(config-if)# cdp enable

Referensi:

- http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/19ew/configuration/guide/port_sec.pdf
- http://www.nsa.gov/ia/_files/switches/switch-guide-version1_01.pdf