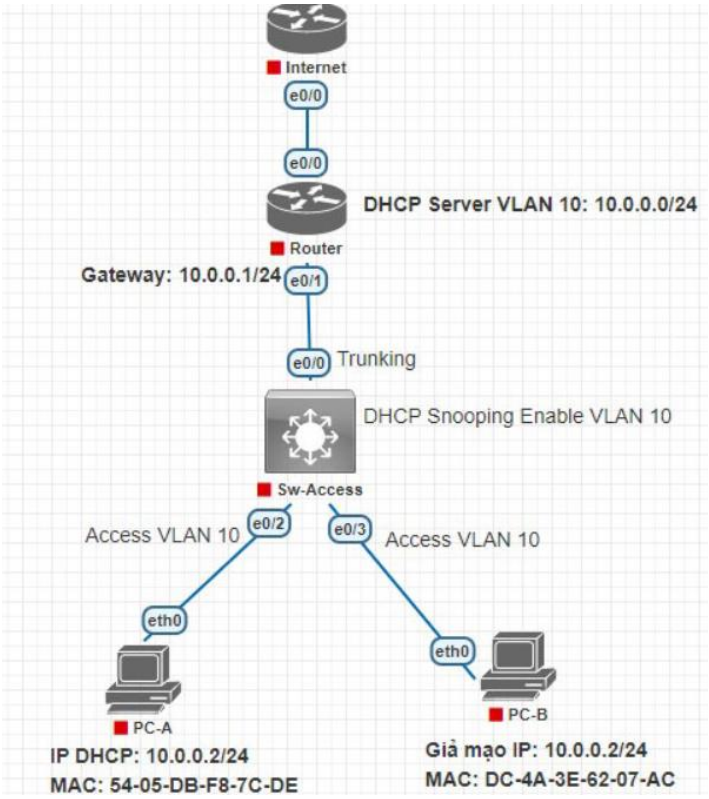
CƠ CHẾ HOẠT ĐỘNG CỦA IP SOURCE GUARD (IPSG)

(Bài lab này đã được phòng kỹ thuật VnPro thực hiện và kiểm tra thành công)

Mục lục

1. Giới thiệu

IP Source Guard hay thường gọi là **IPSG**, là 1 tính năng bảo mật lớp 2 để ngăn chặn các cuộc tấn công giả mạo địa chỉ IP, hoặc là cả địa chỉ IP và MAC. Các bạn có thể xem trong mô hình này:



Giả sử trong mạng của chúng ta có máy tính A, được cấp phát địa chỉ IP hợp lệ **10.0.0.2** và địa chỉ MAC **54-05-DB-F8-7C-DE** thông qua DHCP Server. Đây là hai thông tin xác thực giúp định danh thiết bị này trong hệ thống mạng. Tuy nhiên có 1 máy tính khác của hacker

cũng đặt địa chỉ IP này với MAC là **DC-4A-3E-62-07-AC**, nhằm giả mạo máy tính A để đánh cắp thông tin.

Trong thực tế hệ thống mạng chúng ta sẽ gặp rất nhiều trường hợp tương tự.

Giả sử bạn có một VLAN và trên firewall chỉ cho phép một số địa chỉ IP nhất định được truy cập internet, nhưng không kiểm tra địa chỉ MAC. Trong trường hợp này, một số người có thể cố tình cấu hình trùng địa chỉ IP được phép truy cập để đăng nhập vào mạng khi các thiết bị hợp lệ đang offline.

Hoặc một tình huống phổ biến khác: trong mạng của bạn có một số server sử dụng địa chỉ IP tĩnh. Các server này thường bật firewall để bảo vệ nên mặc định sẽ chặn các gói tin ICMP (ping). Nếu ai đó cần đặt một IP tĩnh cho thiết bị của họ, họ có thể ping thử đến IP của server. Do firewall chặn ping nên không nhận được phản hồi, họ nghĩ IP đó chưa được sử dụng và gán nó cho thiết bị của mình. Kết quả là mạng của bạn sẽ có hai thiết bị cùng dùng một IP, dẫn đến hiện tượng xung đột IP và làm gián đoạn kết nối đến server.

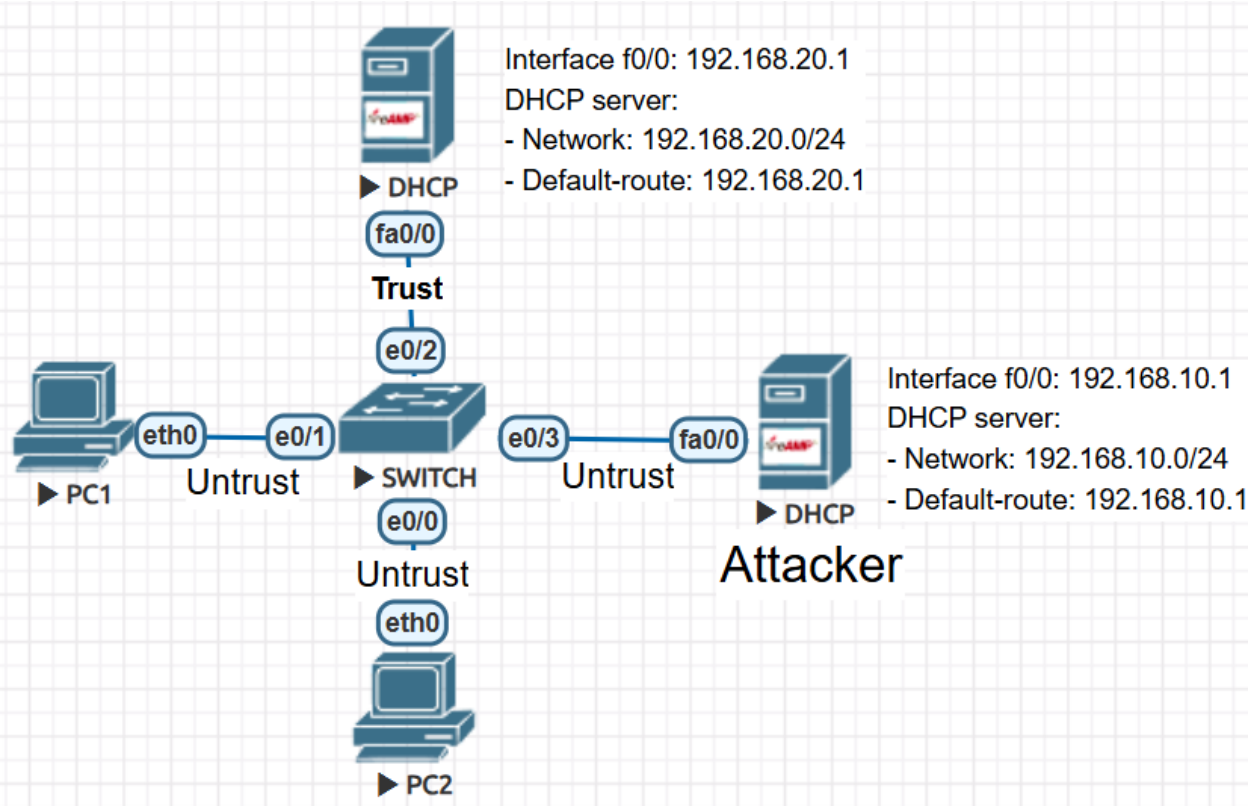
Khi xảy ra trùng IP, switch sẽ lưu địa chỉ MAC của thiết bị nào gửi gói tin gần nhất, nên tất cả lưu lượng đến IP đó sẽ được chuyển đến thiết bị này. Điều này rất nguy hiểm vì có thể làm gián đoạn các dịch vụ quan trọng nếu một thiết bị cố tình hoặc vô tình sử dụng địa chỉ IP đã được cấp phát. Tình trạng này càng nghiêm trọng hơn nếu IP tĩnh của server chưa được loại khỏi DHCP pool — khi server offline, DHCP vẫn có thể cấp IP này cho thiết bị khác.

Với những rủi ro như vậy, IP Source Guard (IPSG) là một giải pháp đơn giản nhưng cực kỳ hiệu quả để ngăn chặn tình trạng giả mạo và xung đột IP trong mạng.

2. Cấu hình IP Source Guard trên switch Cisco

Khi các bạn bật IP Source Guard lên, ban đầu nó sẽ deny toàn bộ traffic, chỉ cho phép các gói tin DHCP. Khi đó chỉ những Client nhận được IP DHCP hoặc đã được cấu hình binding tĩnh thì mới được phép đi qua.

IP Source Guard sẽ có 2 cách để cấu hình: dựa trên DHCP Snooping binding và static binding.



3. Cấu hình dựa trên DHCP Snooping database

Để có thể cấu hình được IP Source Guard theo bảng DHCP Snooping binding thì chúng ta cần có DHCP Snooping trước.

Đây là bảng DHCP Snooping binding

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:50:79:66:68:04   192.168.20.3     86341       dhcp-snooping   1     Ethernet0/1
Total number of bindings: 1
```

IP Source Guard sẽ sử dụng các thông tin này để tạo các Access list động và lọc traffic, các thông tin này tùy vào các bạn cấu hình, nó có thể là IP, hoặc MAC, VLAN, và interface cũng được.

Ví dụ như mô hình trên, các bạn bật IP Source Guard với thông tin kiểm tra là IP và MAC, thì khi đó chỉ có PC1 sẽ có thể truy cập mạng được, do nó nhận IP từ DHCP và thông tin này đã được binding trong DHCP Snooping database. Còn PC2 này sẽ bị deny do địa chỉ MAC của nó không khớp với địa chỉ IP và PC2 được đặt IP tĩnh nên sẽ không có trong bảng DHCP Snooping. Tất nhiên là khi PC2 nhận IP mới thông qua DHCP, thì IP Source

Guard cũng sẽ update Access list động của nó với thông tin mới trong DHCP Snooping database.

Cách hoạt động của nó chỉ đơn giản vậy thôi. Các bạn đưa các thông số nào vào check, thì nó sẽ kiểm tra các thông tin đó, nếu đúng thì cho phép truy cập.

Trước tiên mình sẽ cấu hình IP source guard cho cổng 0/1 trước.

Bật IP Source Guard bằng lệnh *ip verify source* trong mode Interface.

Switch(config)#int e0/1

Switch(config-if)#ip verify source

Để kiểm tra thì các bạn có thể show bằng lệnh ***show ip verify source***.

```
Switch(config)#do show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/1      ip           active       192.168.20.3                        1
Switch(config)#
```

Các bạn cũng có thể thêm bộ lọc dựa vào địa chỉ MAC. Để lọc theo MAC thì các bạn có thể thêm option port secure vào.

```
Switch(config)#interface ethernet 0/1
Switch(config-if)#ip verify source port-security
Switch(config-if)#do show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/1      ip-mac       active       192.168.20.3     permit-all         1
Switch(config-if)#
```

Khi đó thì switch sẽ check cả IP và MAC, tuy nhiên thì MAC hiện tại đang cho phép tất cả do mình chưa cấu hình Port secure, mình sẽ bật port secure trên cổng 0/1.

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#do show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/1      ip-mac       active       192.168.20.3     00:50:79:66:68:04  1
Switch(config-if)#
```

Bây giờ thì switch sẽ lọc các Client tương ứng với địa chỉ IP và địa chỉ MAC này.

Mình sẽ cấu hình tương tự cho cổng 0/0 nối xuống PC2

Switch(config)#int e0/0

Switch(config-if)#ip verify source

Switch(config-if)#ip verify source port-security

Switch(config-if)#switch mode access

Switch(config-if)#switchport port-security

```
Switch(config-if)#do show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/0      ip-mac       active       deny-all         deny-all           1
Et0/1      ip-mac       active       192.168.20.3     00:50:79:66:68:04  1
Switch(config-if)#
```

Các bạn có thể thấy do cổng 0/0 đang cấu hình IP tĩnh và nó không có thông tin trong bảng DHCP Snooping, nên nó sẽ deny toàn bộ traffic đến từ cổng này, trừ gói tin DHCP thôi. Nên chúng ta sẽ tránh được các trường hợp ai đó đặt trùng với các IP quan trọng trong hệ thống mạng. Các máy client lúc này tại cổng 0/0 cần phải nhận IP qua DHCP thì mới truy cập được. Còn trường hợp đặt tĩnh thì chúng ta sẽ cần static binding.

Như vậy PC2 dù có đặt trùng IP thì cũng không làm ảnh hưởng đến kết nối mạng của PC1.

4. Cấu hình Static binding

Ngoài sử dụng thông tin về client trong DHCP snooping Binding, thì IP Source Guard cũng hỗ trợ các cấu hình Static. Nó sẽ được sử dụng trong trường hợp Server cấu hình IP tĩnh và chúng ta chỉ muốn IP này được phép sử dụng trên 1 cổng nhất định, tránh trường hợp ai đó đặt trùng IP của server gây mất mạng chẳng hạn. Thì khi đó chúng ta không cần kết hợp với DHCP Snooping nữa

Trước tiên mình đã đổi IP của PC2 sang IP 192.168.20.10 để tránh trùng lặp với PC1.

Để cấu hình static binding, chúng ta quay lại vào mode global config và cấu hình bằng lệnh ip source binding, sau đó là các thông tin về MAC, VLAN, IP và cuối cùng là cổng kết nối. Đây là lệnh cấu hình:

Switch(config)#ip source binding 00:50:79:66:68:05 vlan 1 192.168.20.10 interface e0/0

Bây giờ thì các server tại cổng 0/0 với các thông tin này có thể truy cập mạng, mặc dù chúng không có trong bảng DHCP Binding.

```
Switch(config)#do show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/0      ip-mac       active       192.168.20.10    00:50:79:66:68:05  1
Et0/1      ip-mac       active       192.168.20.3     00:50:79:66:68:04  1
Switch(config)#do show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------
00:50:79:66:68:04   192.168.20.3     85244       dhcp-snooping   1     Ethernet0/1
Total number of bindings: 1
```

Kiểm tra

Để kiểm tra hoạt động của IP Source Guard (IPSG), có thể sử dụng lệnh show ip verify source như đã show ở trên, hoặc các bạn cũng có thể bật debug IPSG để xem chi tiết.

Mình sẽ bật debug IPSG trên switch lên trước. Lưu ý kết quả debug này là lúc mình chưa cấu hình static binding cho PC2 và PC2 vẫn đang đặt IP 192.168.20.3 trùng với PC1.

```
Switch#debug ip verify source packet
Ip source guard debug packet debugging is on
Switch#
```

Switch#debug ip verify source packet

Ip source guard debug packet debugging is on

ping từ PC-B đến gateway.

```
VPCS> ip 192.168.20.3/24 192.168.20.1
Checking for duplicate address...
PC1 : 192.168.20.3 255.255.255.0 gateway 192.168.20.1

VPCS> ping 192.168.20.1

host (192.168.20.1) not reachable

VPCS>
```

Có thể thấy 1 log đã được đẩy ra thông báo PC từ cổng 0/0, địa chỉ IP và MAC không có trên interface này, do vậy tất cả traffic này sẽ bị drop.

```
Switch#
*Mar 12 17:15:34.052: DHCP_SECURITY_SW: receive port security packet, recv port: Ethernet0/
0, recv vlan: 1, consume flag: 0, handle flag: 1.
*Mar 12 17:15:34.052: DHCP_SECURITY_SW: validate port security packet, recv port: Ethernet0
/0, recv vlan: 1, mac: 0050.7966.6805, invalid flag: 0.
*Mar 12 17:15:35.053: DHCP_SECURITY_SW: receive port security packet, recv port: Ethernet0/
0, recv vlan: 1, consume flag: 0, handle flag: 1.
*Mar 12 17:15:35.053: DHCP_SECURITY_SW: validate port security packet, recv port: Ethernet0
/0, recv vlan: 1, mac: 0050.7966.6805, invalid flag: 0.
Switch#
*Mar 12 17:15:36.055: DHCP_SECURITY_SW: receive port security packet, recv port: Ethernet0/
0, recv vlan: 1, consume flag: 0, handle flag: 1.
*Mar 12 17:15:36.055: DHCP_SECURITY_SW: validate port security packet, recv port: Ethernet0
/0, recv vlan: 1, mac: 0050.7966.6805, invalid flag: 0.
```

Tác giả: Quang Hòa – PKT VNPRO