DDOS 공격에 대비한 라우터 설정

김상정

최근에 유행하고 있는 DDOS(Distributed Denial of Service) 공격에 대비하여 라우터 설정하는 방법에 대해 알아본다.

1. ip verify unicast reverse-path interface 명령 사용

- ✓ 라우터로 유입되는 각각의 패킷을 검사하여 소스 IP 주소가 CEF 테이블에서 패킷이 도착한 인터페이스를 가리키는 경로를 갖고 있지 않을 경우, 패킷을 drop 한다.
- ✓ SMURF 공격과 같이 IP 주소 spoofing 을 이용하는 공격을 방지한다.
- ✓ 위의 명령을 사용하기 위해서는 라우터에서 "CEF(Cisco Express Forwarding) switching" 또는 "CEF distributed switching"이 동작하도록 설정해야 한다.
- ✓ CEF switching 을 라우터 입력 인터페이스에 대해 설정할 필요가 없다. CEF 가 동작중인 경우, 개별 인터페이스는 여러가지 다른 스위칭 모드로 설정가능하다

Unicast RPF 는 11.2 또는 11.3 이미지에서는 지원되지 않으며, CEF 를 지원하는 12.0 에서 지원한다. 그러므로, unicast RPF 는 AS5800 의 PSTN/ISDN dial-up 인터페이스에서 사용할 수 있다.

2. ACL(Access Control List)를 사용하여 RFC1918 address space 필터링

- ✓ 일반적으로 분산서비스 공격도구는 소스 IP 주소로 RFC1918 address space 를 주로 사용하는 것으로 알려진다. 그러므로, 아래 예제와 같이 라우터의 ACL 에 내용을 추가한다.

```
interface serial3/0/0
        ip access-group 101 in
        access-list 101 deny ip 10.0.0.0       0.255.255.255 any
        access-list 101 deny ip 192.168.0.0    0.0.255.255 any
        access-list 101 deny ip 172.16.0.0     0.15.255.255 any
        access-list 101 permit ip any any
```

3. ACL 에 ingress 및 egress filtering (RFC 2267) 적용

- ✓ ISP edge 라우터에서는 고객의 네트워크에 속하는 소스 주소를 갖고 있는 트래픽만 받아들이도록 하며, 고객의 네트워크는 자신의 네트워크 주소 이외의 소스 주소를 가지는 트래픽만 받아들인다.

{ ISP Core } -- ISP Edge Router -- Customer Edge Router -- { Customer network }

- ✓ ISP 쪽의 라우터를 다음과 같이 설정한다.

```
access-list 190 permit ip {customer network} {customer network mask} any
access-list 190 deny ip any any [log]

interface {ingress interface} {interface #}
   ip  access-group 190 in
```

- ✓ 고객쪽의 라우터를 다음과 같이 설정한다.

```
  access-list 187 deny ip {customer network} {customer network mask} any
  access-list 187 permit ip any any

  access-list 188 permit ip {customer network} {customer network mask} any
  access-list 188 deny ip any any

interface  {egress  interface}  {interface  #}
     ip  access-group 187 in
     ip  access-group 188 out
```

4. ICMP 패킷에 대한 rate limit 설정

✓ 다음과 같이 rate limit 를 설정한다.

```
        interface serial3/0/0
        rate-limit [input|output] access-group 2020 3000000 512000 786000 conform-action transmit exceed-action drop

        access-list 2020 permit icmp any any echo-reply
```

* 3000000 : maximum link bandwidth
  512000 : burst normal rate
  786000 : burst max rate

* 위의 설정은 ICMP echo-reply 패킷을 3Mbps bandwidth 와 512kbyte burst normal size 및 786kbyte 의 burst max size 로 제한한다.

* show interface [interface-name] rate-limit : rate-limiting 에 대한 통계
  clear counters [interface-name] : rate-limiting 에 대한 통계 초기화

✓ 이외에도 다양한 type 에 대한 rate limit 를 설정하여 사용한다.

5. SYN 패킷에 대한 limit 설정

✓ ICMP 패킷에 대한 limit 설정하는 방법과 같다. 다음과 같이 rate limit 를 설정한다.

```
        interface serial3/0/0
        rate-limit output access-group 153 45000000 100000 100000 conform-action transmit exceed-action drop
        rate-limit output access-group 152 1000000 100000 100000 conform-action transmit exceed-action drop

        access-list 152 permit tcp any host eq www
        access-list 153 permit tcp any host eq www established
```

* 45000000 : maximum link bandwidth
1000000 : syn flooding rate 의 30%내지 50% 사이의 값
100000 : burst normal and max rate

* 80 번 포트에 대한 TCP SYN 패킷을 1Mbps bandwidth 와 100kbyte burst normal size 및 100kbyte 의 burst max size 로 제한한다.

* 웹 연결 세션을 45Mbps bandwidth 와 100kbyte burst normal size 및 100kbyte burst max size 로 제한한다.

7. Random detect 설정

✓ WRED(Weighted Random Early Detection) 설정을 이용하여, 패킷의 양이 갑자기 증가할 경우 random detect 명령으로 패킷을 drop 할 수 있다. 이 설정은 drop 된 패킷에 대해 respond 하는 TCP 와 같은 프로토콜에서 유용하다.

```
interface serial3/0/0
    random-detect [weighting]

interface serial2/0/0
    no random-detect
```

✓ * weighting : exponential weighting 상수로서 1 부터 16 까지의 값을 가진다.
기본값은 10 으로 설정되어 있으며, 이 경우에는 2^{10} 마다 패킷 하나씩 drop 한다.

- "show" 명령어를 사용할 수 있는 레벨을 기본 레벨인 1이 아닌 관리자 권한 (15)으로 제한.

```
SHB_NET.shinhan.com# config terminal
SHB_NET.shinhan.com(config)# privilege exec level 15 show
SHB_NET.shinhan.com(config)# ^Z
```