JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 26, No. 9: 1374~1381, Sep. 2022

Edge 라우터 기반 네트워크 공격에 대응하는 보안기술 연구

황성규*

Research on security technology to respond to edge router-based network attacks

Seong-Kyu Hwang*

*Associate Professor, Department of Information & Commnincation Engg., Chosun College University of Science & Technology, Gwangju, 61453 Korea

요 약

네트워크 공격 대응에 관한 보안기술의 기존 연구들은 하드웨어적 네트워크 보안 기술을 이용하여 네트워크의 보안성을 높이는 방법이나 바이러스 방역 백신과 바이러스 방역 시스템이 주로 제안 설계되어왔다. 많은 사용자는 라우터의 보안 기능을 충분히 활용하지 못하고 있어 이러한 문제점을 극복하기 위해 네트워크 보안 수준에 따라 분리함으로써 계층화된 보안 관리를 통하여 외부에서의 공격을 차단할 수 있음을 계층별 실험을 통해 분류하였다. 연구의 범위는 Edge 라우터의 보안기술 동향을 살펴봄으로 Edge 라우터 기반의 네트워크 공격에 관한 위협으로부터 보호하는 방법과 구현 사례를 제시한다.

ABSTRACT

Existing research on security technology related to network attack response has focused on research using hardware network security technology, network attacks that wiretap and wiretap network packets, denial of service attack that consumes server resources to bring down the system, and network by identifying vulnerabilities before attack. It is classified as a scanning attack. In addition, methods for increasing network security, antivirus vaccines and antivirus systems have been mainly proposed and designed.

In particular, many users do not fully utilize the security function of the router. In order to overcome this problem, it is classified according to the network security level to block external attacks through layered security management through layer-by-layer experiments. The scope of the study was presented by examining the security technology trends of edge routers, and suggested methods and implementation examples to protect from threats related to edge router-based network attacks.

키워드 : Edge 라우터, 네트워크 공격, 보안기술, 라우터의 보안 기능

Keywords : Edge router, network attack, security technology, security function of router

Received 29 August 2022, **Revised** 4 September 2022, **Accepted** 12 September 2022

*** Corresponding Author** Seong-Kyu Hwang (E-mail:okhsk@cst.ac.kr, Tel:+82-62-230-8840)
Associate Professor, Department of Information & Commnincation Engg., Chosun College University of Science & Technology, Gwangju, 61453 Korea

Open Access http://doi.org/10.6109/jkiice.2022.26.9.1374 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

네트워크 보안을 보장하기 위해 Edge 라우터의 네트워크 장비에서의 보안은 완벽하지는 않지만 다양한 방법이 제공되고 있다[1].

지금까지의 대부분의 연구를 살펴보면 네트워크 패킷을 도청, 감청하는 네트워크 공격과 서버의 자원을 소비시켜 시스템을 다운 시키는 서비스 거부 공격과 공격 전 취약점 파악을 네트워크 스캐닝 공격 등으로 구분하고 있다[2].

본 논문에서는 라우터의 보안 기능을 충분히 활용하지 못하고 있어 이러한 문제점을 극복하기 위해 네트워크 보안 수준에 따라 분리함으로써 계층화된 보안 관리를 통하여 외부에서의 공격을 차단할 수 있음을 계층별 실험을 통해 분류하였다.

네트워크 공격유형 4가지 중 특히, 스푸핑(Spoofing)과 서비스 거부(Denial of Service) 공격 외에 네트워크 공격유형 3가지는 OSI 7 Layer 기준으로 2~4계층의 공격으로 발현된다[3]. 따라서 본 연구는 Layer 2계층의 MAC Limiting, MAC Address Filtering, Layer 2계층 기반의 NBT(NetBIOS Over TCP/IP) Control 보안과 Layer 3계층 기반의 IP Packet Filtering, Multicast Traffic Limiting과 Layer 4계층의 IP/TCP/UDP Port Filtering과 Port Rate- Limit로 구분하여 네트워크의 공격 대응에 관한 보안기술로 실험을 통해 구현해 보았다. 본 논문의 구성은 다음과 같다. 2장에서는 라우터 보안 구현 기술을 구현해 보고 실험 결과에 대해 논하고 3장에서는 결론으로 마무리한다.

Ⅱ. Edge 라우터 보안 구현 기술

2.1. MAC Limiting

MAC 제한기능(MAC Limiting)은 이더넷 스위칭 테이블의 플러딩을 차단하며 Layer 2 인터페이스에서 활성화된다[4]. MAC Limiting은 VLAN 내에서 학습할 수 있는 MAC 주소의 수를 제한하여 인터페이스 보안을 강화한다. MAC 주소의 수를 제한함으로써 이더넷 MAC 테이블의 플로딩으로부터 LAN을 보호한다. 플러딩은 학습한 새 MAC 주소의 수가 이더넷 MAC 테이블을 오버플로우하게 하고 이전에 학습한 MAC 주소가 테이블에서 플러시 되는 경우 발생한다.

MAC 주소 수 제한은 인터페이스당 동적 학습 될 수 있는 최대 MAC 주소 수를 구성한다. 새로운 MAC 주소가 있는 수신 패킷은 제한 사항을 초과할 때 무시, 삭제할 수 있다.

```
switchport port-security maximum 10
switchport port-security aging time 1
switchport port-security violation protect
```

Fig. 1 MAC Address Limiting Configuration

MAC Address Limiting을 위해 그림 1의 configuration의 maximum 10은 시스템의 인터페이스에 MAC Address의 Max Count를 10으로 제한했으며 aging time 1은 Mac 테이블에 저장된 정보는 1분 동안 유지되게 하였다. violation protect는 위반한 MAC 주소를 가진 장비의 모든 Frame을 Drop 하는 방법이다.

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 1 mins
Aging Type                 : Absolute
Maximum MAC Addresses      : 10
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
Last Source Address VlanId : 0
Security Violation Count   : 0
```

Fig. 2 Check MAC Address Limiting function

그림 1에서 MAC Address Limiting Configuration을 통한 결과는 그림 2에서 VLAN 내에서 학습할 수 있는 MAC 주소의 수를 Maximum MAC Addresses :10을 통해 10으로 제한됨을 확인할 수 있다.

2.2. MAC Address Filtering

특정 MAC 주소에서 모든 수신 패킷을 차단하려면 MAC 주소 필터링을 활성화할 수 있다[5]. 대상 MAC 주소를 동적으로 학습하도록 이더넷 인터페이스를 구성해야 한다. 소스 주소 필터링을 구현하기 위해서는 통합 이더넷 인터페이스에서 소스 주소 필터링을 통해 특정 MAC 주소에서 모든 수신 패킷을 차단할 수 있다. 또는 특정 디바이스에 대한 네트워크를 허용할 수 있다.

```
mac-address-table static 0000.0000.0001 vlan 100 drop
mac-address-table static 0000.0000.0002 vlan 100 drop
mac-address-table static 0000.0000.0003 vlan 100 drop
mac-address-table static 0000.0000.0004 vlan 100 drop
mac-address-table static 0000.0000.0005 vlan 100 drop
mac-address-table static 0000.0000.0006 vlan 100 drop
mac-address-table static 0000.0000.0007 vlan 100 drop
mac-address-table static 0000.0000.0008 vlan 100 drop
mac-address-table static 0000.0000.0009 vlan 100 drop
mac-address-table static 0000.0000.000a vlan 100 drop
mac-address-table static 0000.0000.000b vlan 100
```

Fig. 3 MAC Address Configuration

그림 3에서 실험을 위해 특정 MAC 주소를 임의로 48bit 할당하였으며 vlan 100으로 할당하여 해당 MAC 주소를 차단하여 보았다.

```
Router#show mac-address-table static
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age      ports
------+---------------+--------+-----+----------+--------
*  ---  0000.0000.aaaa    static  No          -   Switch
*  100  0000.0000.0004    static  No          -   <drop>
*  100  0000.0000.0005    static  No          -   <drop>
*  100  0000.0000.0006    static  No          -   <drop>
*  100  0000.0000.0007    static  No          -   <drop>
*  100  0000.0000.0001    static  No          -   <drop>
*  100  0000.0000.0002    static  No          -   <drop>
*  100  0000.0000.0003    static  No          -   <drop>
*  100  0000.0000.0008    static  No          -   <drop>
*  100  0000.0000.0009    static  No          -   <drop>
*  100  0000.0000.000a    static  No          -   <drop>
*  100  0000.0000.000b    static  No          -   <drop>
```

Fig. 4 Check MAC Address Configuration function

그림 4를 통해 특정 MAC 주소에서 수신 패킷을 차단하는 MAC 주소 필터링 실험에서 MAC 주소 필터링이 활성화됨을 알 수 있다.

2.3. Multicast Traffic Limiting

트래픽 스톰 (Storm traffic)이 생성되면 수신 노드가 네트워크에서 자체 메시지를 브로드캐스트하여 응답하라는 메시지를 요구한다[6]. 명령 응답을 통해 LAN 패킷의 트래픽이 생성되어 네트워크 성능이 저하되거나 네트워크 서비스가 손실된다. 스톰 컨트롤(Storm control level)은 지정된 트래픽 수준이 초과하면 스위치가 트래픽 수준을 모니터링하고 브로드캐스트와 멀티캐스트 등을 drop할 수 있다. 이를 통해 패킷이 LAN의 비정상적인 작동을 방지할 수 있다.

Multicast, Unicast, Brodcast 트래픽을 지정할 수 있는데 본 논문에서는 Multicast 트래픽을 지정하였다.

storm-control multicast level 0이라는 configuration으로 모든 Multicast를 Limiting을 한 다음 계측기에서 Multicast Traffic을 인가하여 Limiting을 확인하였다.

```
* Before changing settings
Port        UcastSupp %     McastSupp %     BcastSupp %  TotalSuppDiscards
Fa3/1           100.00          100.00          100.00                  0

* After changing the settings
Port        UcastSupp %     McastSupp %     BcastSupp %  TotalSuppDiscards
Fa3/1           100.00            0.00          100.00                  0
```

Fig. 5 Check Multicast Traffic Limiting function

그림 5의 멀티캐스트 트래픽(McastSupp)이 수신될 경우 Storm-control 기술을 사용하여 수신하는 멀티캐스트 처리양을 제어 및 관리할 수 있으며 그림 5에서 멀티캐스트 트래픽이 100%에서 0%로 수신이 차단됨을 알 수 있다.

2.4. Layer 2 기반의 NBT(NetBIOS Over TCP/IP) Control 보안

NetBIOS는 서로 다른 단말이 네트워크를 통해 데이터를 전송하며 라우팅이 불가능하여 TCP를 통해 광역 통신을 하는 프로토콜이다[7].

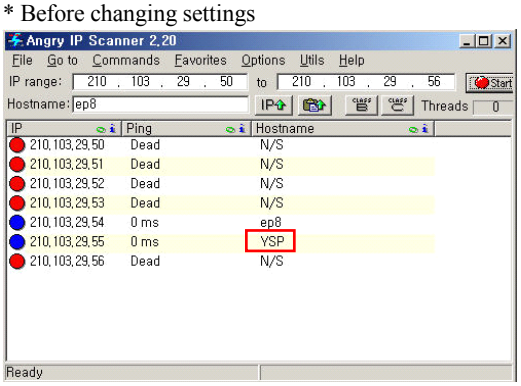
TCP, IP, IPX, NetBIEU 등 네트워크와 전달 계층 프로토콜을 연결하는 역할을 하는 프로그램이다. 즉 각각의 컴퓨터를 구분하기 위해 사용하는 이름이라 할 수 있다. 그림 6에서 L2 기반의 보안 기능을 위해 NBT Control 기능을 활성화하여 보안 기능을 실험해 본다.

```
vlan access-map netbios 10 match ip address 102
 action drop

access-list 102 permit tcp any any eq 137
access-list 102 permit tcp any any eq 138
access-list 102 permit tcp any any eq 139
access-list 102 permit udp any any eq netbios-ns
access-list 102 permit udp any any eq netbios-dgm
access-list 102 permit udp any any eq netbios-ss
```

Fig. 6 NBT control Configuration

* Before changing settings



* After changing the settings

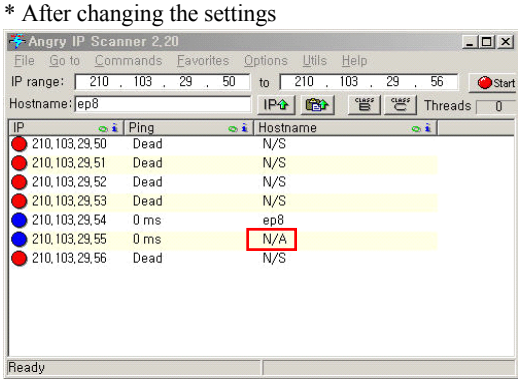


Fig. 7 Check NBT control function

그림 7을 통해 NBT 기능으로 Before changing the settings에서 각각의 컴퓨터가 구분(Hostname)됨을 확인할 수 있다. 그림 7의 After changing the settings는 NBT Control 보안기술을 통해 컴퓨터가 구분되는 것이 적용되어 실현되는 것을 확인하였다.

2.5. IP Packet Filtering

필터링은 출발지, 목적지 IP주소와 포트를 이용한다. 그러나 이것들만 가지고는 세밀한 제어가 힘들다. 데이터 흐름을 제어하는 것은 보안에서 중요하다[8]. 접근제어(Access Control List)를 통해 정의한 필터를 구성하고 비교검사를 수행하여 패킷을 허용하거나 거부한다. 본 논문에서는 IP Packet Filtering을 100개 이상 지원이 적용되는지 실험을 통해 확인하였다.

그림 8은 IP Address 10.2.1.2~10.2.1.101까지 100개의 IP Address를 Filtering을 실험하였으며 그림 8의 아래 그림 계측기에서 IP-Traffic을 인가하였으며 그림 9에서 IP Packet Filter를 설정한 후 해당 Packet이 폐기되

```
interface FastEthernet1/3
 ip address 10.2.1.1 255.255.255.0
 ip access-group 105 in
 load-interval 30
 duplex full

access-list 105 deny   ip host 10.2.1.2 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.3 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.4 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.5 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.6 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.7 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.8 host 10.3.1.2
access-list 105 deny   ip host 10.2.1.9 host 10.3.1.2
```

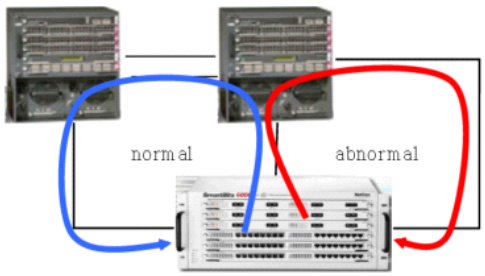
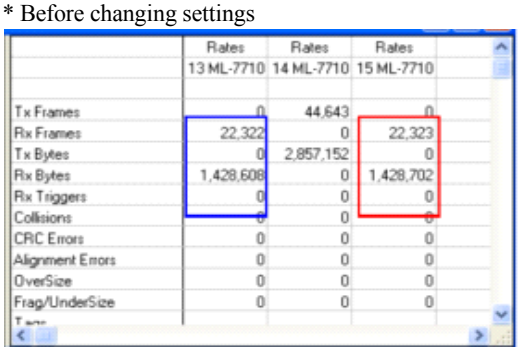


Fig. 8 IP Address Filtering Configuration

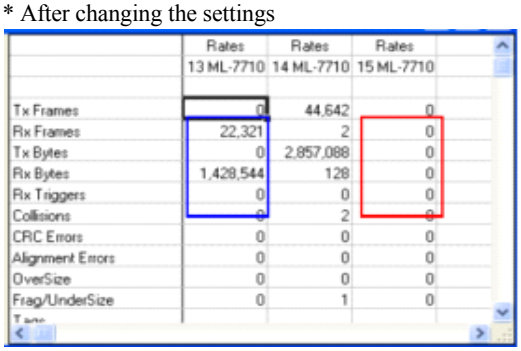
는 것을 확인한다. 그리고 Filtering Rule과 관계없는 Traffic은 정상적으로 수신되는 것을 확인하였다.

* Before changing settings



	Rates 13 ML-7710	Rates 14 ML-7710	Rates 15 ML-7710
Tx Frames	0	44,643	0
Rx Frames	22,322	0	22,323
Tx Bytes	0	2,857,152	0
Rx Bytes	1,428,608	0	1,428,702
Rx Triggers	0	0	0
Collisions	0	0	0
CRC Errors	0	0	0
Alignment Errors	0	0	0
OverSize	0	0	0
Frag/UnderSize	0	0	0

* After changing the settings



	Rates 13 ML-7710	Rates 14 ML-7710	Rates 15 ML-7710
Tx Frames	0	44,642	0
Rx Frames	22,321	2	0
Tx Bytes	0	2,857,088	0
Rx Bytes	1,428,544	128	0
Rx Triggers	0	0	0
Collisions	0	2	0
CRC Errors	0	0	0
Alignment Errors	0	0	0
OverSize	0	0	0
Frag/UnderSize	0	1	0

Fig. 9 Check IP Packet Filtering

2.6. IP/TCP/UDP Port의 Filtering

포트 필터링은 특정 UDP 및 TCP 서비스에 대해 활성화된 일 년의 포트가 있다. 호스트가 이러한 포트에 연결되어 요청을 처리하는데, CPU 용량이 사용된다. 단일 공격 디바이스에서 서로 다른 랜덤 소스 IP주소를 사용하여 대량의 요청을 전송하는 경우 오버 헤딩 되거나 속도가 느려지거나 실패할 수 있다. 그러므로 UDP 및 TCP의 서비스가 있는 장치는 보호되거나 서비스를 비활성화해야 한다.

```
ip addr 1.1.1.1 255.255.255.0
access-list 110 deny tcp any any eq 23
access-list 110 permit ip any any

access-group 110 in
```

Fig. 10 Port Filtering Configuration

그림 10 Port Filtering configuration에서 IP Address 1.1.1.1 255.255.255.0을 설정하여 TCP 23번 포트 Telnet을 차단한다.

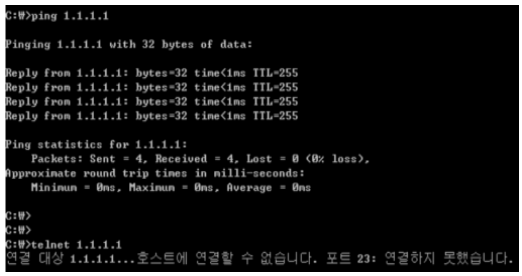


Fig. 11 Check Port Filtering

그림 11에서 IP Address 1.1.1.1의 Test PC와 ping으로 통신 확인 후 Telnet 23번 포트접근을 확인하여 Port Filtering이 되었음을 확인하였다.

2.7. TCP/UDP (Layer 4) Port Rate-Limit

대역폭은 통신 경로를 통해 성공적으로 전송된 데이터의 평균량을 나타낸다. 대역폭 쉐이핑과 관리, 상한 설정 및 할당 설정은 대역폭을 변경할 수 있다. 소수의 포트가 스위치 대역폭의 많은 부분을 차지하지 않도록 특정 포트의 대역폭을 제한하는 기술을 적용한다.

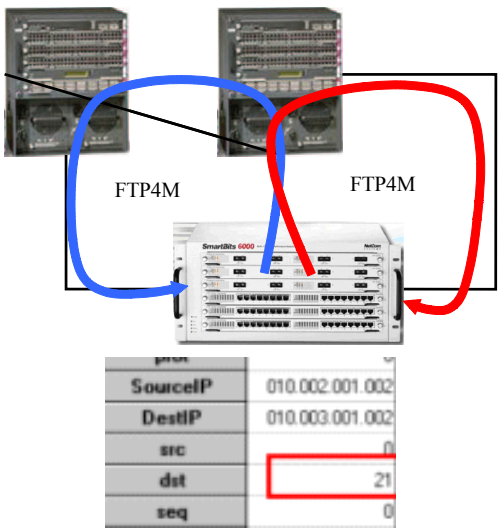


Fig. 12 Port Rate-Limit Configuration

그림 12는 Layer 4의 Port에 대한 Rate-Limit를 2M Bytes로 설정하여 소수의 포트가 스위치 대역폭을 많이 차지하지 않게 하려고 Traffic Drop을 확인한다.

* Before changing settings

	Rates 13 ML-7710	Rates 14 ML-7710	Rates 15 ML-7710
Tx Frames	0	16,667	0
Rx Frames	8,333	0	8,333
Tx Bytes	0	1,066,688	0
Rx Bytes	533,312	0	533,312
Rx Triggers	0	0	0
Collisions	0	0	0

* After changing the settings

	Rates 13 ML-7710	Rates 14 ML-7710	Rates 15 ML-7710
Tx Frames	0	16,667	0
Rx Frames	8,333	0	3,875
Tx Bytes	0	1,066,688	0
Rx Bytes	533,312	0	248,000
Rx Triggers	0	0	0
Collisions	0	0	0

Fig. 13 Check Port Rate-Limit

그림 13에서 특정 포트의 대역폭을 제한하는 기술인 Rate Limit Filtering 기능을 설정하여 Traffic이 2M

Bytes로 제한되는지 실험하기 위해 ftp 4M Bytes로 Packet을 전송하여 그림 13에서 2M Bytes로 Drop 됨을 확인하였다.

2.8. Direct Broadcast Filtering

Direct Broadcast는 대상 주소가 네트워크 또는 서브넷의 브로드캐스트 주소인 IP패킷이다. 모든 호스트가 응답하도록 한다. 또한 네트워크의 모든 활성 호스트 목록을 얻을 수 있다. 이를 악용하여 네트워크에서 서비스 거부 공격을 할 수 있다.

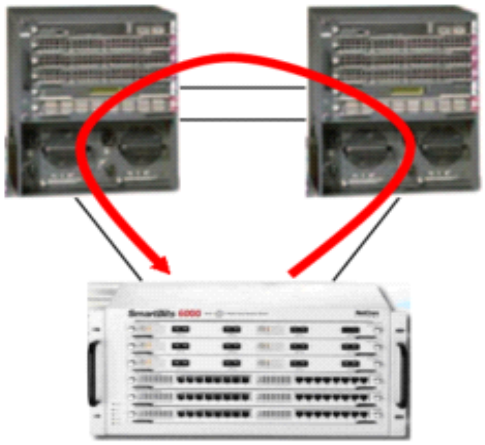


Fig. 14 Direct Broadcast Filtering Configuration

Direct Broadcast Filtering 실험하기 위해 그림 14에서 아래 계측기에서 Direct Broadcast Traffic을 인가한다. 그리고 Direct Broadcast Traffic을 Filtering을 확인하였다.

* Before changing settings

	Rates 13 ML-7710	Rates 14 ML-7710
Tx Frames	0	7,441
Rx Frames	7,429	0
Tx Bytes	0	476,224
Rx Bytes	475,456	0
Rx Triggers	0	0
Collisions	0	0
CRC Errors	0	0
Alignment Errors	0	0
OverSize	0	0
Frag/UnderSize	0	0

* After changing the settings

	Rates 13 ML-7710	Rates 14 ML-7710
Tx Frames	0	7,441
Rx Frames	0	1
Tx Bytes	0	476,224
Rx Bytes	0	94
Rx Triggers	0	0
Collisions	0	0
CRC Errors	0	0
Alignment Errors	0	0
OverSize	0	0
Frag/UnderSize	0	0

Fig. 15 Check Direct Broadcast Filtering

Direct Broadcast Filtering의 실험결과를 그림 15를 통해서 적용 전과 적용 후에서 Filtering을 확인하였다.

2.9. TCP SYN Attack

TCP SYN Flooding 공격은 DoS 공격의 한 종류이며 TCP 연결과정에서 취약점을 이용한 공격기법이다. TCP의 연결 가능한 자원을 모두 소진하게 되고, 외부 사용자는 TCP 연결을 할 수가 없게 되는 공격기법이다.

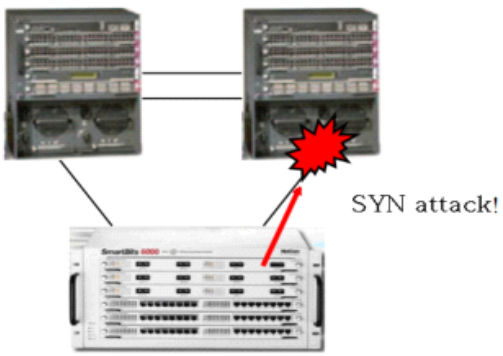


Fig. 16 TCP SYN Attack Configuration

그림 16은 TCP SYN Attack Packet을 수신할 때 정상동작을 실험하기 위해 그림 16 하단의 계측기에서 TCP SYN Attack Traffic을 인가하여 동작 여부를 확인한다.

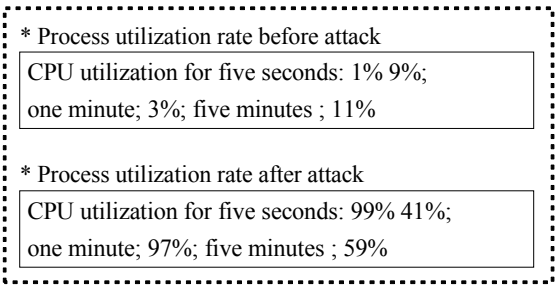


Fig. 17 Check TCP SYN Attack

TCP SYN Attack을 수신할 때 공격 차단 솔루션을 통하여 Intercept 모드나 Watch 모드 등 포워딩시켜주거나 SYN 패킷을 차단하여 그림 17과 같이 Attack 전 프로세스 사용율이 11%에서 Attack 후 프로세스 사용율이 59%까지 상승하나 정상 동작함을 확인하였다.

Ⅲ. 결 론

본 연구에서는 네트워크 공격유형을 OSI 7 Layer 기준으로 2~4계층의 공격으로 발현됨으로 라우터의 보안

Table. 1 comparison analysis

Security implementation technology	purpose	blocking effect	Classification of attacks by layer
MAC Limiting technology	MAC Address Limiting	MAC Address Limiting attack, normal behavior	Layer 2
MAC Address Filtering technology	MAC Address Filtering	MAC Address Filtering attack, normal behavior	Layer 2
Multicast Traffic Limiting technology	Multicast Traffic Limiting	Multicast Traffic Limiting attack, normal behavior	Layer 2
NBT Control technology	NetBIOS Over TCP/IP Control	NBT Control attack, normal behavior	Layer 2
IP Packet Filtering technology	IP Packet Filtering	Packet Filtering attack, normal behavior	Layer 3
IP/TCP/UDP Port Filtering technology	IP/TCP/UD P Port Filtering	IP/TCP/UDP Port Filtering attack, normal behavior	Layer 4
TCP/UDP Port Rate-Limit technology	TCP/UDP Port Packet volume control	TCP/UDP Port Rate-Limit attack, normal behavior	Layer 3
Direct Broadcast Filtering technology	Direct Broadcast Filtering	Direct Broadcast Filtering attack, normal behavior	Layer 3

기능을 충분히 활용하여 계층화된 보안 관리를 하여 외부 공격을 차단할 수 있음을 계층별 실험을 통해 나타내었다. 이를 위해 Layer 2계층부터 4계층까지 네트워크의 공격 대응에 관한 보안기술을 통해 차단 결과를 나타내었다. 본 논문에서 실험한 방법들이 모든 유형의 침해사고나 네트워크 공격유형에 대한 해결방안은 될 수 없겠지만 Edge 라우터가 포함된 네트워크 보안의 위협으로부터 보호할 수 있는 라우터의 보안기술 활용을 보다 높일 수 있을 것으로 생각한다.

REFERENCES

[1] M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395 – 411, May. 2018.

[2] K. Yang, Q. Li, and L. Sun, “Towards automatic fingerprinting of IoT devices in the cyberspace,” *Computer Networks*, vol. 148, pp. 318 – 327, Jan. 2019.

[3] Bitdefender, Bitdefender IoT Security Platform [Internet]. Available: https://www.bitdefender.com/iot/.

[4] Fing, Business Solutions: Device Recognition [Internet]. Available: https://www.fing.com/business/.

[5] S. E. Yang, I. S. Kang, B. O. Go, and H. K. Jung, “A Realtime Traffic Shaping Method for VPN Tunneling on Smart Gateway Supporting IoT,” *The Journal of Korea Institute of Information and Communication Engineering*, vol. 21, no. 6, pp. 1121-1126, Jun. 2017.

[6] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, “Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges," *IEEE Communication & Surveys Tutorials*, vol. 22, no. 1, pp. 320-351, Mar. 2020

[7] M. Lotfollahi, M. J. Siavoshani, R. S. H. Zade, and M.

Saberian, “Deep packet: a novel approach for encrypted traffic classification using deep learning,” *Soft Computing*, vol. 24, no. 3, pp. 1999-2012, May. 2019.

[8] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, “Mobile Encrypted Traffic Classification Using Deep Learning,” in *Proceedings of 2018 Network Traffic Measurement and Analysis Conference (TMA)*, Vienna, Austria, pp.1-8, 2018.

황성규 (Seong-Kyu Hwang)

정보통신공학과 공학박사

※관심분야 : 통신 프로토콜, 네트워크 설계, 통신 네트워크