		Document No.
		SKInfosec-Tech-001

UDP Flooding Attack
공격과 방어

황 교 국
(fullc0de@gmail.com)

SK Infosec Co., Inc
MSS Biz. Security Center

Table of Contents

1. 소개

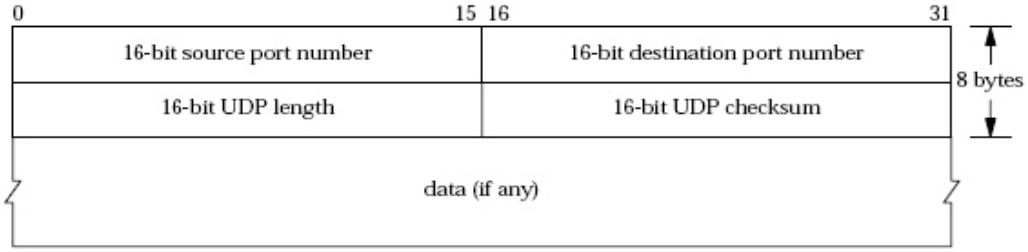
UDP Flooding Attack이란 다양한 DoS(Denial of Service) 공격의 일종으로 대량의 UDP 패킷을 이용하여 대상 호스트의 네트워크 자원을 소모시키는 공격을 말한다. 최근 인터넷에서 발생하는 DDoS 형태 중 UDP Flooding Attack이 큰 부분을 차지하고 있다. 따라서, 본 문서에서는 UDP의 특성과 이를 이용한 Flooding 공격이 어떻게 이루어 지는지 테스트을 통해서 알아보며 이에 대한 방어 대책을 F/W과 ID/PS(Intrusion Detection/ Preventing System)등과 같은 보안 장비 관점에서 알아보고 적용해 볼 것이다.

2. 공격 관련 Protocols Overview

UDP Flooding Attack은 UDP와 ICMP Protocol의 동작 메커니즘에 밀접한 관련이 있다. 따라서 공격을 이해하기 위해서는 두 프로토콜의 동작 원리에 대한 이해가 필요하다. ICMP Protocol의 경우는 UDP Flooding Attack와 관련 된 기능에 한해 언급할 것이다.

2.1. UDP Protocol

UDP Protocol은 John Postel이 작성한 RFC768[3]에서 제안되었다. 이 Protocol을 사용하는 호스트간에 통신 효율성을 제공해주는 반면 비 연결 지향적이기 때문에 통신 간의 신뢰성을 제공해주지 못한다. 따라서, 데이터 전송 간의 신뢰성이 보장되어야 하는 서비스에서는 사용하지 않는다.



[그림2.1] UDP Diagram

[그림2.1]에서 보는 바와 같이 데이터 전송에 가장 기본적인 요소만을 가지고 있음을 확인할 수 있다. 하지만 기본적인 에러 컨트롤을 제공하기 위해 ICMP(Internet Control Message

Protocol)[9] Error Control 기능을 이용한다.

2.2. ICMP Protocol

신뢰성을 제공해주지 못하는 IP Protocol 통신 환경에서 발생할 수 있는 문제에 대한 Feedback을 제공하기 위해 설계되었다. 따라서, 프로토콜 컨트롤을 위해 다양한 형태의 메시지를 포함하고 있다. 그 중 잘못된 서비스 Port로 UDP 패킷이 전달 되었을 때 발생되는 ICMP Destination Port Unreachable메시지는 UDP Flooding 공격과 밀접한 관련이 있다.

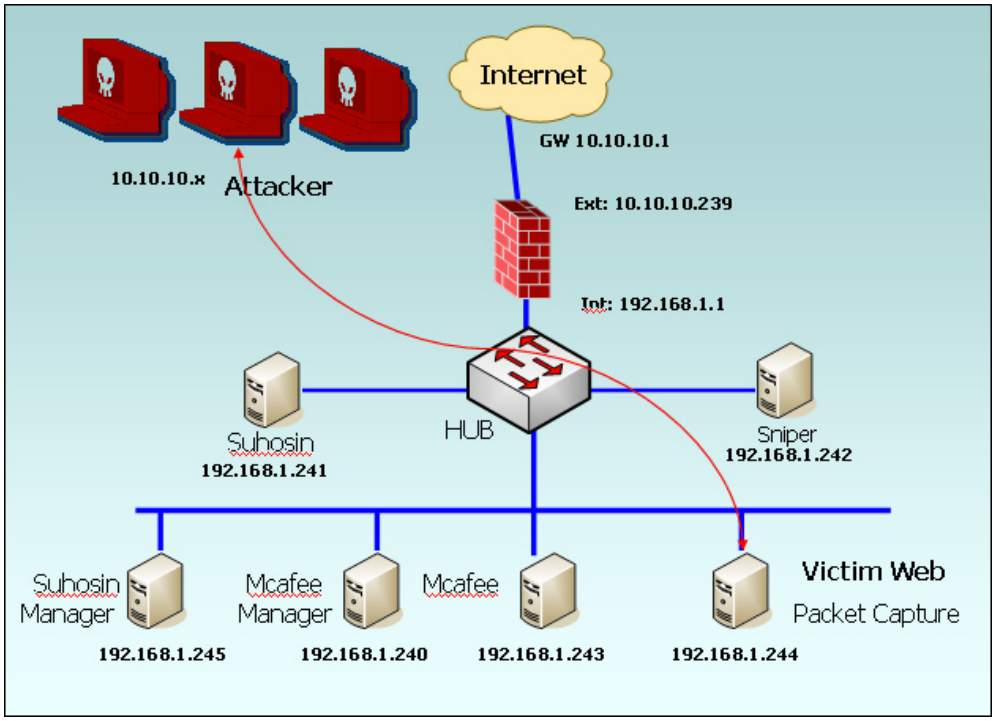
[표2.1]는 ICMP Protocol에서 발생하는 메시지 중 3번 Destination Unreachable이 가질 수 있는 15가지 코드를 보여준다.

Type 3. Destination Unreachable	
Code	Name
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect

[표2.1] ICMP Destination Unreachable Type.3 코드표

3. UDP Flood Test Environment

UDP Flood 공격을 수행하고 이를 모니터링 하기 위해 [그림3.1]과 같은 네트워크 환경을 준비하였다.



[그림3.1] UDP Flood 공격 실험을 위한 네트워크 구성

공격의 효율을 위해 다중 호스트들에 의한 DDoS로 진행이 되며 이를 위해서 rBot을 이용하게 된다. IRCBot은 DDoS를 보다 간편하게 수행할 수 있는 장점을 가지고 있다. 하지만 Bot자체의 논의는 본 문서의 주제에서 벗어나므로 언급하지 않겠다.

[표3.1]은 테스트에 사용된 장비들의 리스트이다.

용도	종류
Attacker	Windows XP SP2 Windows 2000 SP4
Victim Web	Windows 2000 Server Edition
ID/PS	Suhosin, sniper, Mcafee
Firewall	NetScreen 5GT

[표3.1] 테스트 장비 목록

Attacker들과 Victim 사이에 Router가 존재하지 않는다. 따라서 UDP Packet은 방화벽을 지나 Victim으로 유입될 것이며 그 때 발생하는 방화벽 트래픽 변화와 Victim의 네트워크 상태는 네트워크 트래픽 모니터링 도구를 통해 확인한다. 또한, 방화벽 정책을 통해 UDP Flood 공격이 얼마나 완화 될 수 있는지 확인 할 것이다.

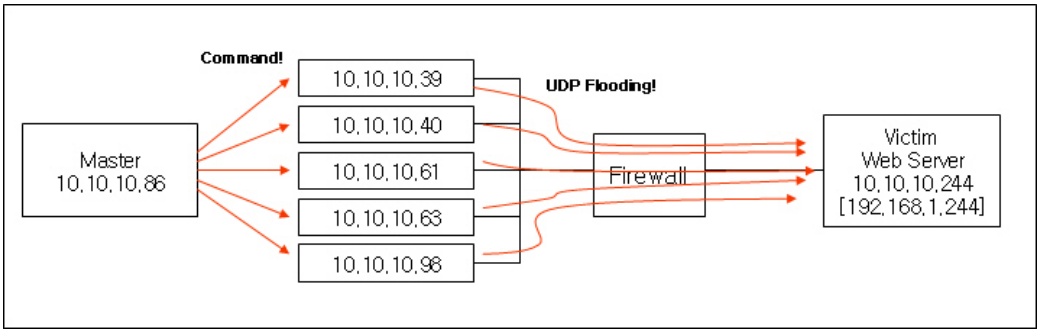
본 문서는 Firewall이나 ID/PS의 성능을 테스트 하기 위함이 목적이 아니다. UDP Flood가 발생했을 때 네트워크의 변화와 이에 대응하여 Firewall에서 기본적인 방어를 하였을 때 공격이 얼마나 완화되는가를 확인하는 것이 목적이다. 따라서, 다양한 방화벽을 이용한 성능 테스트는 하지 않는다.

4. Attack Monitoring

공격을 수행하기 전 네트워크 상태와 공격을 수행 한 후 네트워크 상태를 분리해서 비교 해 본다. 먼저, 공격을 수행하기 전 네트워크 상태를 확인한다.

4.1. Before Attacking

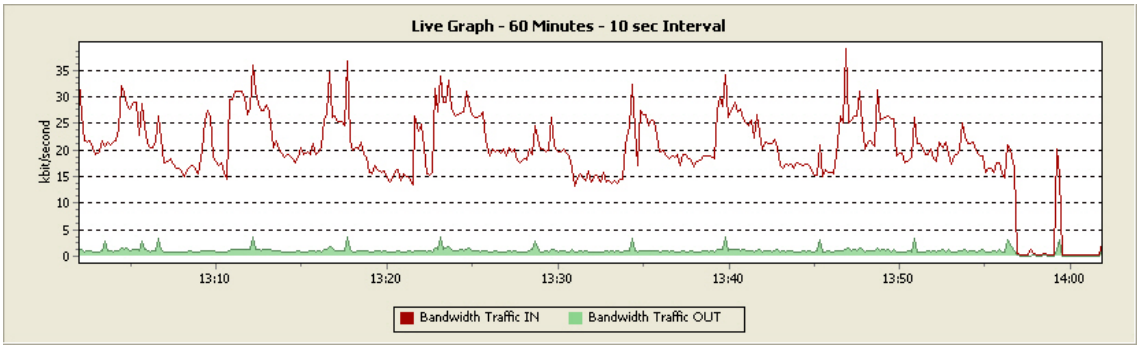
UDP공격의 경우 SYNFlood 공격과는 달리 네트워크 bandwidth를 소모시키는 것이 목적이다. 따라서, 단일 공격 호스트로는 효과를 볼 수 없기 때문에 DDoS로 구성해서 공격이 이루어 진다. 보통, DDoS를 수행하기 위해 최소 수 백대 이상의 Zombie 호스트가 필요하지만 본 문서에서는 UDP Flooding 공격이 발생했을 때 네트워크 bandwidth의 변화가 어떻게 발생하는지 확인하기 위함이므로 5대의 샘플 호스트를 이용할 것이다.



[그림4.1] UDP Flood를 이용한 DDoS 개념도

먼저 트래픽을 확인하기 위해 Firewall에서 제공하는 정보를 모니터링 한다.

공격을 수행하지 않았을 때 방화벽을 통해 발생하는 네트워크 트래픽은 [그림4.2]과 같다.



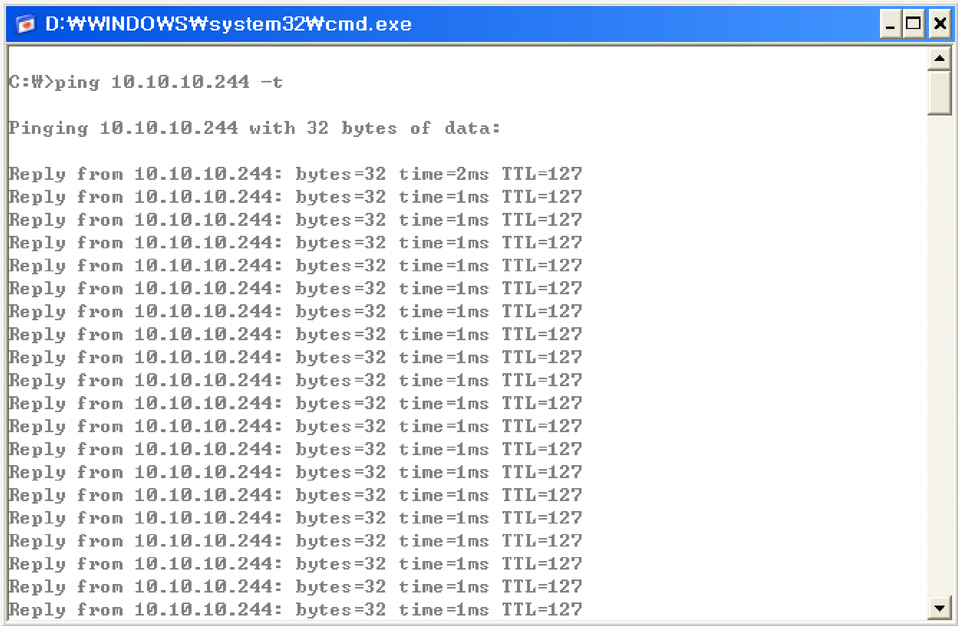
[그림4.2] 정상 네트워크 트래픽

테스트의 편의를 위해서 victim에 대한 원격 연결 트래픽을 제외하고는 네트워크를 이용하지 않았다. [그림4.3]는 정상 네트워크 트래픽 양를 보여준다.

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
2007-02-14 오후 2:00 - 오후 3:00	1.889	0.240	0.000	0.000	1.889	0.240	2
2007-02-14 오후 1:00 - 오후 2:00	8,986.098	20.461	451.329	1.028	9,437.427	21.489	100
2007-02-14 오후 12:00 - 오후 1:00	9,912.262	22.571	548.070	1.248	10,460.332	23.819	100

[그림4.3] 정상 네트워크 트래픽 양

즉, 1시간동안 발생한 평균 트래픽 양은 21.489Kbit/Second가 발생하였다.
다음 10.10.10.86 호스트에서 방화벽을 지나 10.10.10.244로 가는 ping의 response 는 [그림4.4]와 같다.



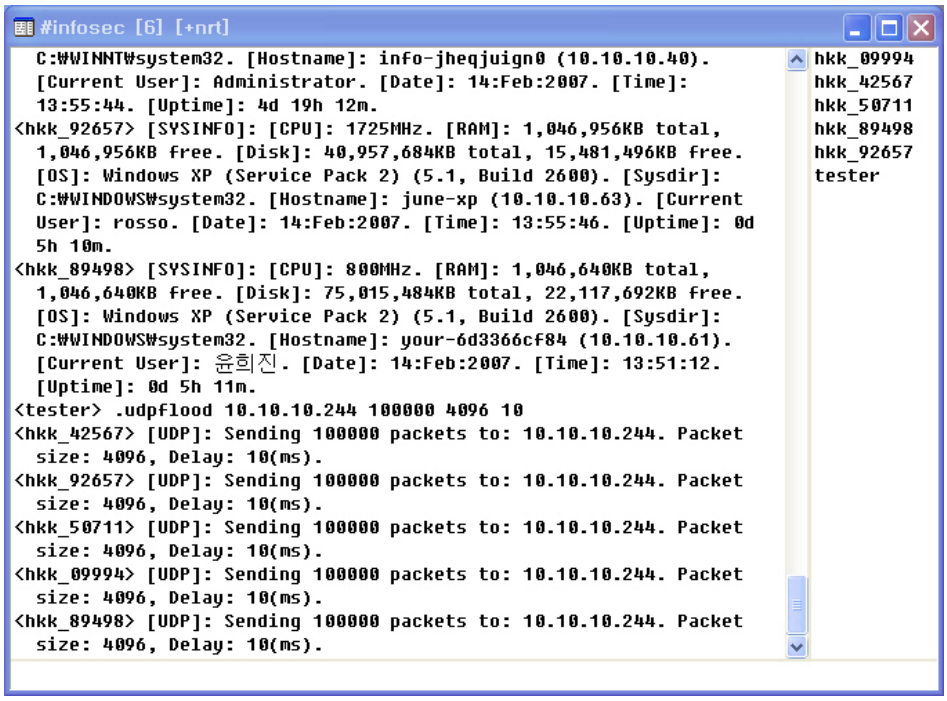
[그림4.4] victim에 대한 ping 테스트

DDoS 공격이 이루어지지 않은 상황에서는 모든 네트워크 상태가 양호함을 확인할 수 있다.

4.2. After Attacking

테스트를 위한 DDoS 공격 환경을 구성하기 위해 5대의 샘플 호스트와 rBot으로 잘 알려져 있는 IRC Bot을 이용할 것이다.

[그림4.1]에서 보는 바와 같이 10.10.10.86이 IRC 서버 역할을 하는 동시에 Master가 된다. [그림4.5]는 Master에서 IRC를 이용해 Client를 컨트롤 하는 화면이다.



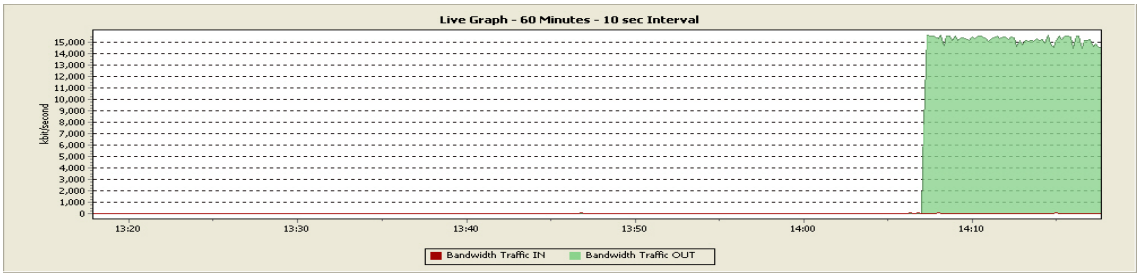
[그림4.5] IRC 제어 화면

Agent에게 UDP Flood 공격을 내리기 위해 다음과 같이 IRC 창에 입력을 한다

```
.udpflood 10.10.10.244 100000 4096 10
```

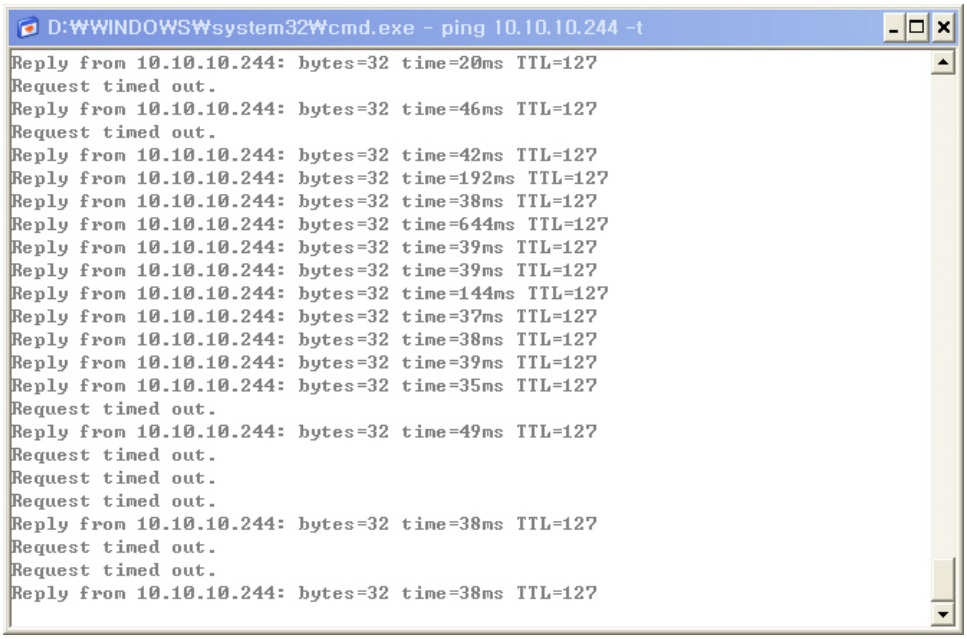
위 명령은 rBot 계열에서 통용되는 명령어로써 무작위로 선택 된 포트를 향해 패킷 당 4096Bytes씩 100000개를 10ms 단위로 전송하라는 것이다. 하지만 4096Byte씩 전송되므로 IP Fragmentation 과정을 거치게 되므로 더 짧은 시간 간격으로 공격이 수행될 것이라 예상된다.

[그림4.6]은 공격이 수행되었을 때 그래프이다.



[그림4.6] 1차 공격 화면

네트워크는 100Mbps의 bandwidth를 가지고 있다. 1차 공격을 통해 15Mbps 가량 소모되었으며 해당 트래픽이 모두 victim으로 몰리게 되어 [그림4.7]과 같은 ping 테스트 결과를 가져오게 된다.



[그림4.7] 1차 공격 시 victim에 대한 ping 테스트 결과

공격 시 victim에서 발생한 패킷은 다음과 같다.

No.	Time	Source	Destination	Protocol	Info
35	6.920372	10.10.10.63	192.168.1.244	UDP	Source port: 7115 Destination port: 14511
36	6.920453	192.168.1.244	10.10.10.63	ICMP	Destination unreachable (Port unreachable)
37	6.921591	10.10.10.97	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
38	6.922900	10.10.10.97	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=1480)
39	6.923861	10.10.10.97	192.168.1.244	UDP	Source port: 1824 Destination port: 10422
40	6.923936	192.168.1.244	10.10.10.97	ICMP	Destination unreachable (Port unreachable)
41	6.925094	10.10.10.40	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=1480)
42	6.926083	10.10.10.40	192.168.1.244	UDP	Source port: 3899 Destination port: 29870
43	6.926218	192.168.1.244	10.10.10.40	ICMP	Destination unreachable (Port unreachable)
44	6.927293	10.10.10.98	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
45	6.928508	10.10.10.98	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=1480)
46	6.929460	10.10.10.98	192.168.1.244	UDP	Source port: 3954 Destination port: 7919
47	6.929545	192.168.1.244	10.10.10.98	ICMP	Destination unreachable (Port unreachable)
48	7.014053	10.10.10.61	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
49	7.015126	10.10.10.61	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=1280)
50	7.016190	10.10.10.61	192.168.1.244	IP	Fragmented IP protocol (proto=UDP 0x11, off=2560)
51	7.016402	10.10.10.61	192.168.1.244	UDP	Source port: 3724 Destination port: 4696

[그림4.8] 1차 공격 시 victim에서 감지한 패킷들

[그림4.8]을 보면 victim 시스템에 fragmentation된 UDP 패킷과 무작위 포트 공격으로 인해 발생한 ICMP Destination Port Unreachable 메시지가 주기적으로 발생했음을 확인할 수 있다.

대량의 UDP 패킷과 더불어 victim에서 생성시키는 ICMP 에러 메시지는 victim의 네트워크

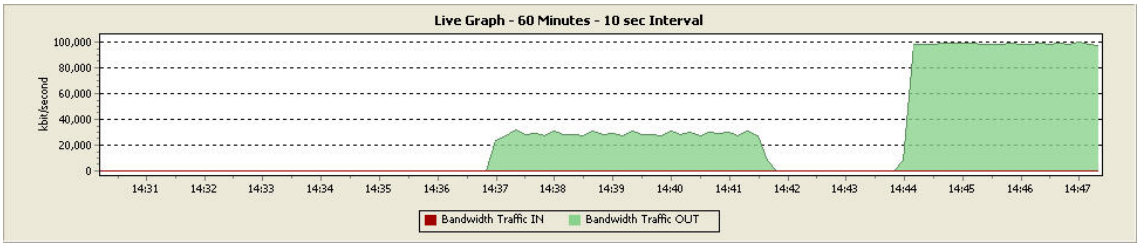
자원을 소모하게 하여 웹 서버로써의 원래 기능을 원활하게 하지 못하는 결과를 초래하게 된다.

테스트 환경의 bandwidth는 100Mbs를 가진다. 따라서 100Mbs에 가까운 공격을 수행하였을 경우 네트워크에 어떤 변화가 발생하는 지 확인해 본다.

```
.udpflood 10.10.10.244 1000000 60000 3
```

이번에는 전체 전송 패킷 개수와 payload 크기를 늘리고 전송 간격을 3ms로 줄여본다.

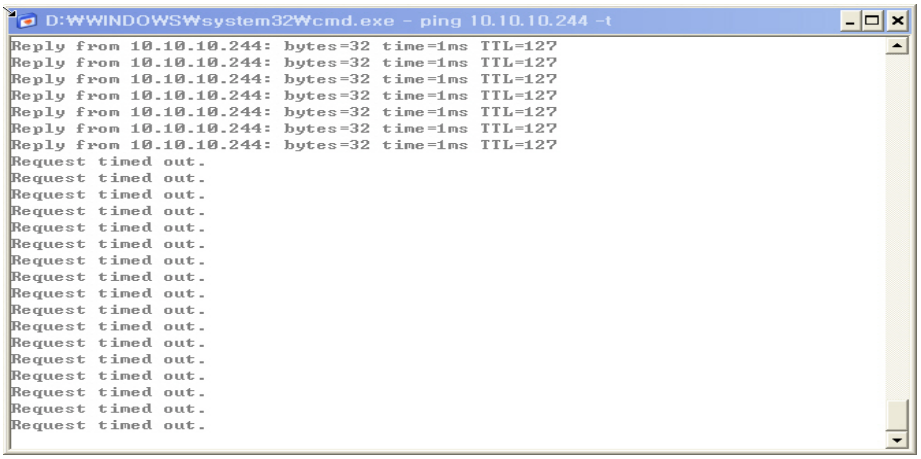
[그림4.9]는 공격이 수행되었을 때 그래프이다.



[그림4.9] 2차 공격 화면

[그림4.9]를 보면 공격에 의해서 이미 100Mbs에 근접한 네트워크 트래픽이 발생하고 있음을 확인할 수 있다. 이 그래프는 victim으로 가는 길목에 위치하고 있는 Firewall에 걸리는 트래픽이므로 실질적으로 victim에서 제공하는 웹 서비스와 같은 네트워크 관련 서비스는 할 수 없을 것으로 판단된다.

[그림4.10]은 victim에 대한 ping 테스트 화면이다.



[그림4.10] 2차 공격 시 victim에 대한 ping 테스트 결과

[그림4.7]과는 달리 2차 공격 시에는 victim의 ping 응답이 전혀 없음을 확인 할 수 있다.

결과적으로 Firewall에서부터 victim으로 연결되는 네트워크는 bandwidth를 최대 한도까지 소모하게 되어 정상적인 서비스를 하지 못하는 DoS상태에 빠지게 된다.

다음 절에서는 UDP Flood 공격에 대응하기 위한 Firewall과 ID/PS 관점에서의 대응방안을 알아본다.

5. Defense and Mitigation

5.1. DDoS 탐지

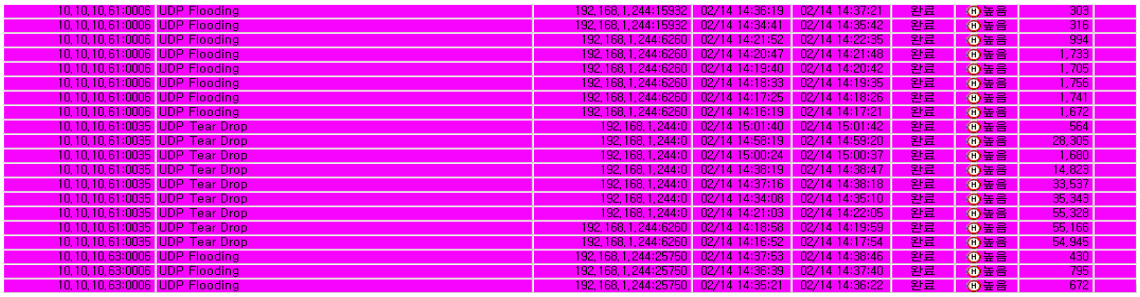
DDoS를 방어하기 위한 기법은 DDoS 기술 별, 네트워크 장비 별 기타 여러 가지 요인에 따라 다르게 적용된다. 특히 본 문서에서 다루고 있는 UDP Flood의 경우, 정상적인 트래픽(normal traffic)과 비 정상적인 트래픽(anomaly traffic)간의 차이를 분석하고 적절한 대응을 하는 것이 DoS를 방어하는 주요 점이 된다.

일반적으로 UDP Flood 공격을 수행할 때 단일 Zombie 에서 발생시키는 패킷은 그 크기가 다양하며 전송 간격 또한 다양화 하게 된다. 하지만 Firewall로 모든 패킷이 몰리게 되어 단일 시간(보통 초 단위)에 대량의 패킷이 몰릴 수 밖에 없다.

따라서, 방어 및 완화를 위해 Firewall의 Threshold 설정 기능을 이용할 것이다.

Firewall에서의 Threshold 기능 설정을 수행하여 DDoS 공격을 방어하는 테스트를 수행하기 전에 ID/PS에서 UDP Flood에 대한 탐지가 가능한 지 확인해 본다.

[그림5.1]은 공격이 수행되었을 때 윈스테크넷의 Sniper에서는 다음과 같은 경고를 발생시켰다.



10.10.10.61:0006	UDP Flooding	192.168.1.244:15932	02/14 14:36:19	02/14 14:37:21	완료	H 높음	303
10.10.10.61:0006	UDP Flooding	192.168.1.244:15932	02/14 14:34:41	02/14 14:35:42	완료	H 높음	316
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:21:52	02/14 14:22:35	완료	H 높음	994
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:20:47	02/14 14:21:48	완료	H 높음	1,733
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:19:40	02/14 14:20:42	완료	H 높음	1,705
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:18:33	02/14 14:19:35	완료	H 높음	1,756
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:17:25	02/14 14:18:26	완료	H 높음	1,741
10.10.10.61:0006	UDP Flooding	192.168.1.244:6260	02/14 14:16:19	02/14 14:17:21	완료	H 높음	1,672
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 15:01:40	02/14 15:01:42	완료	H 높음	564
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 14:58:19	02/14 14:59:20	완료	H 높음	28,305
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 15:00:24	02/14 15:00:37	완료	H 높음	1,680
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 14:38:19	02/14 14:38:47	완료	H 높음	14,823
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 14:37:16	02/14 14:38:18	완료	H 높음	33,537
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 14:34:08	02/14 14:35:10	완료	H 높음	35,343
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:0	02/14 14:21:03	02/14 14:22:05	완료	H 높음	55,328
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:6260	02/14 14:18:58	02/14 14:19:59	완료	H 높음	55,166
10.10.10.61:0035	UDP Tear Drop	192.168.1.244:6260	02/14 14:16:52	02/14 14:17:54	완료	H 높음	54,945
10.10.10.63:0006	UDP Flooding	192.168.1.244:25750	02/14 14:37:53	02/14 14:38:46	완료	H 높음	430
10.10.10.63:0006	UDP Flooding	192.168.1.244:25750	02/14 14:36:39	02/14 14:37:40	완료	H 높음	795
10.10.10.63:0006	UDP Flooding	192.168.1.244:25750	02/14 14:35:21	02/14 14:36:22	완료	H 높음	672

[그림5.1] Sniper IDS에서 UDP Flood 탐지 화면

최초 DDoS 발생 시 IDS가 [그림5.1]과 같이 적절한 탐지를 해 네트워크 관리자에게 통보를 한다면 관리자는 방화벽을 통해 적절한 대응이 가능 할 것이다. 물론 IPS의 경우 실시간으로 이 모든 작업이 가능하도록 하기 때문에 IPS에 DDoS에 대한 대응 정책을 잘 설정하면 될 것이다.

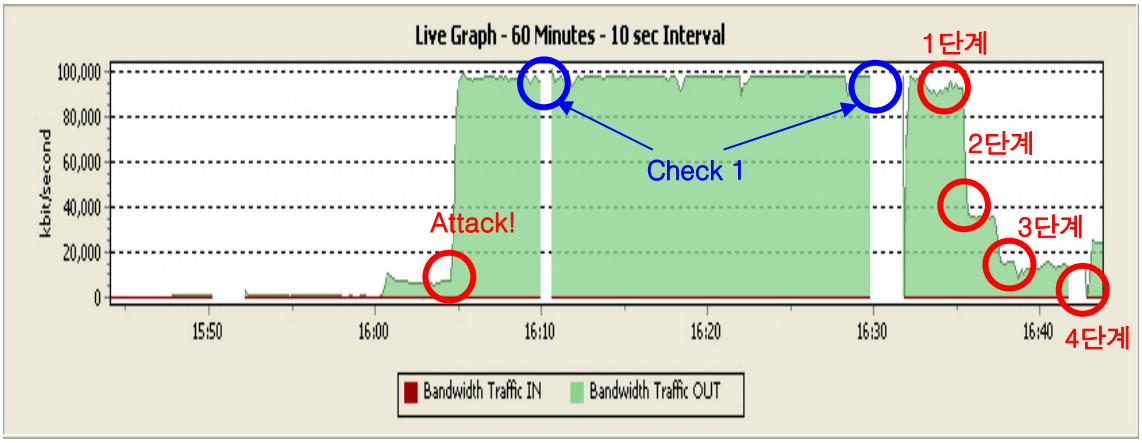
5.2. Threshold를 이용한 방어

공격은 테스트 네트워크가 처리할 수 있는 최대 용량인 100Mbp에 근접하게 이루어진다. 4절에서 확인할 수 있듯이 최대 용량에 근접한 공격을 수행했을 경우 네트워크 서비스가 마비되는 현상이 발생하였다.

Threshold에 따른 트래픽 변화를 쉽게 확인하기 위해 아래와 같이 단계적으로 차단 Threshold를 조정하여 테스트한다.

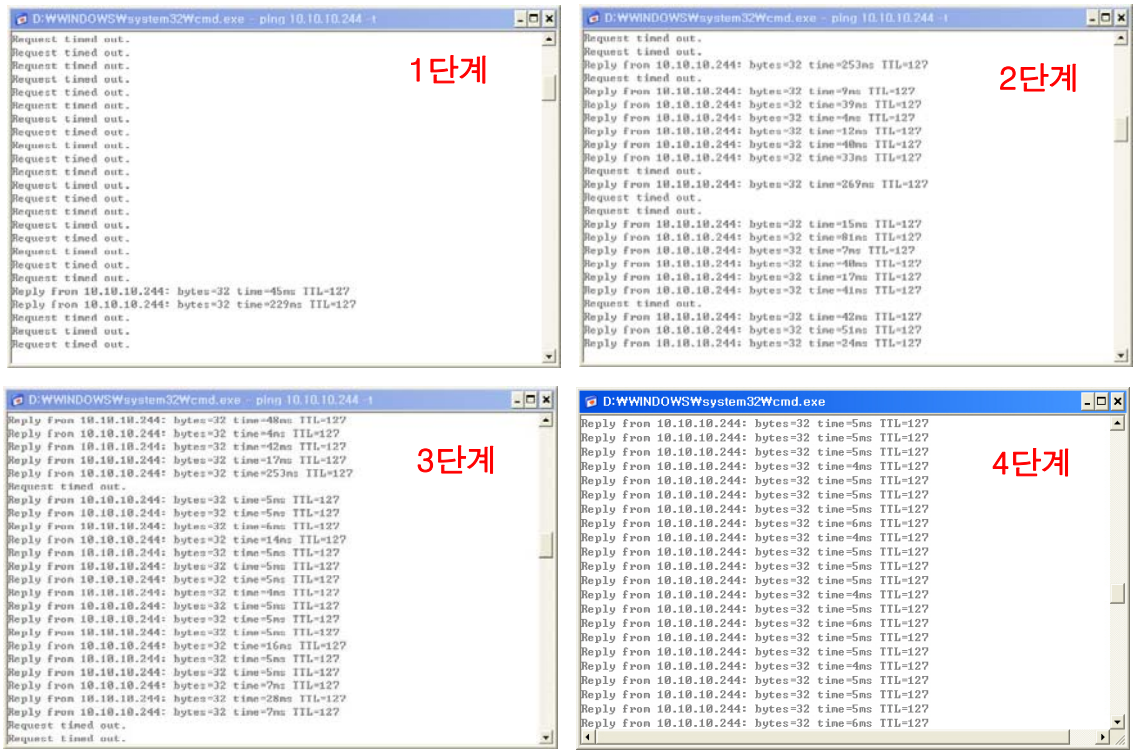
- 1단계: 200 pps (packet per second)
- 2단계: 100 pps
- 3단계: 50 pps
- 4단계: 20 pps

먼저, 결론적으로 Threshold 조정을 통한 DDoS 방어 및 완화는 효과적이다. [그림5.2]는 단계별 트래픽 변화는 보여준다.



[그림5.2] Threshold변화에 따른 트래픽 변화량

다음은 각 단계별 Ping 테스트 결과를 보여준다.



[그림5.3] 각 단계별 Ping 테스트 결과 화면

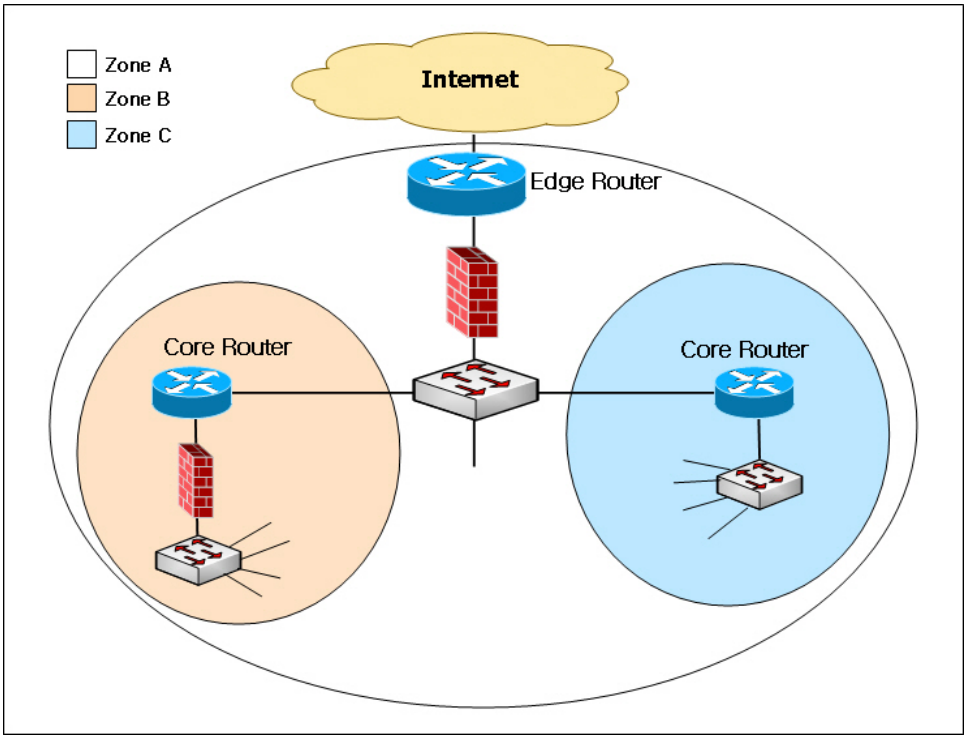
Ping 테스트에서 확인 할 수 있듯이 초당 Threshold 값을 낮게 설정할수록 네트워크 bandwidth가 안정되고 있음을 확인할 수 있다.

결과적으로 보호하고자 하는 네트워크에서 ***가장 민감한 곳***에 위치하고 있는 Firewall이 얼마나 차단 역할을 적절하게 해주는가가 UDP Flood DDoS를 방어할 수 있는 관건이 될 것

이다.

5.3. 방화벽의 위치에 따른 대응

[그림 5.4]는 가상의 네트워크에 설치 된 방화벽들을 보여준다. 이를 통해 위에서 언급한 방화벽의 민감한 위치를 알아본다.



[그림5.4] 가상 네트워크 구성도

[그림5.4]에서의 가상 네트워크는 크게 3개의 Zone으로 구성된다.

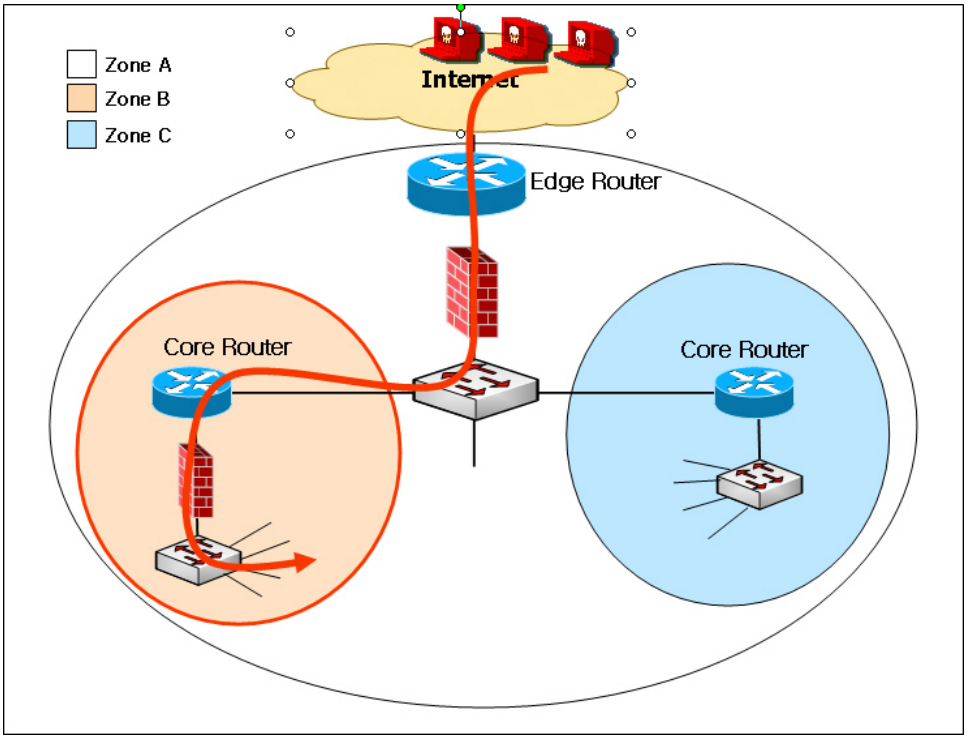
- Zone A: 인터넷으로 통하는 BackBone망과 연결되는 전체 가상 네트워크
- Zone B: Firewall으로 보호되고 있는 Sub 네트워크
- Zone C: Firewall으로 보호되고 있지 않는 Sub 네트워크

가상 네트워크 구성에서 IDS는 생략한다. 왜냐 하면 DDoS를 방어하기 위한 직접적인 대응은 Firewall을 통해서 이루어지기 때문이다.

여기서 보호하고자 하는 대상이 Zone B에 존재한다고 할 때 DDoS 공격은 크게 1)Internet을 통한 외부 유입과 2)내부 유입으로 나눠 생각할 수 있다.

1) 외부 유입

Internet을 포함한 망 외부에서 DDoS공격이 발생 할 경우 [그림5.5]와 같이 생각해 볼 수 있다.



[그림5.5] 외부로부터의 공격

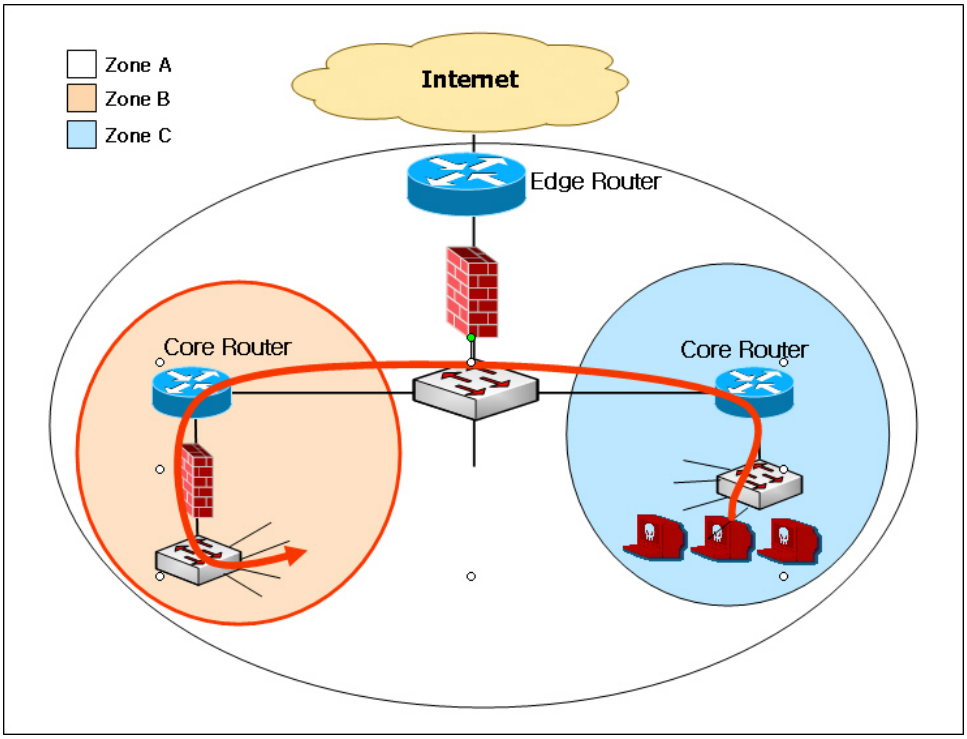
이와 같은 공격이 진행 될 경우 트래픽에 가장 큰 영향을 받는 부분은 Edge Router와 인접한 Firewall이다. 물론 공격자로부터 Edge Router를 통해 victim으로 가는 모든 네트워크의 자원이 소모되므로 DoS 상태에 빠지게 된다.

이를 방어하기 위해서는 Core Router 쪽의 Firewall이 아닌 Edge Router쪽의 Firewall에서 Threshold 설정을 해주어야 한다. 그 이유는 victim과 가까이에 있는 firewall에서 설정 해주었다 하더라도 Edge Router에서부터 bandwidth 소모가 일어나므로 결과적으로는 DoS 상태를 빠져나올 수 없기 때문이다. 물론 가장자리(perimeter)쪽의 장비 가용성이 뛰어날 경우에는 문제를 발생시키는 Core Router쪽에서 방어를 해도 상관은 없다. 하지만 이러한 판단은 각 네트워크 관리자가 해야 할 과제이다.

다시 말해, 굉장히 큰 bandwidth를 소모시키는 DDoS가 발생할 경우 Edge Router쪽에 있는 Firewall에서의 방어가 가장 효과적일 것이다.

2) 내부 유입

[그림5.6]은 Zone B가 아닌 내부의 다른 Zone에서 DoS 공격이 시작되는 모습을 보여주고 있다.



[그림5.6] 내부로부터의 공격

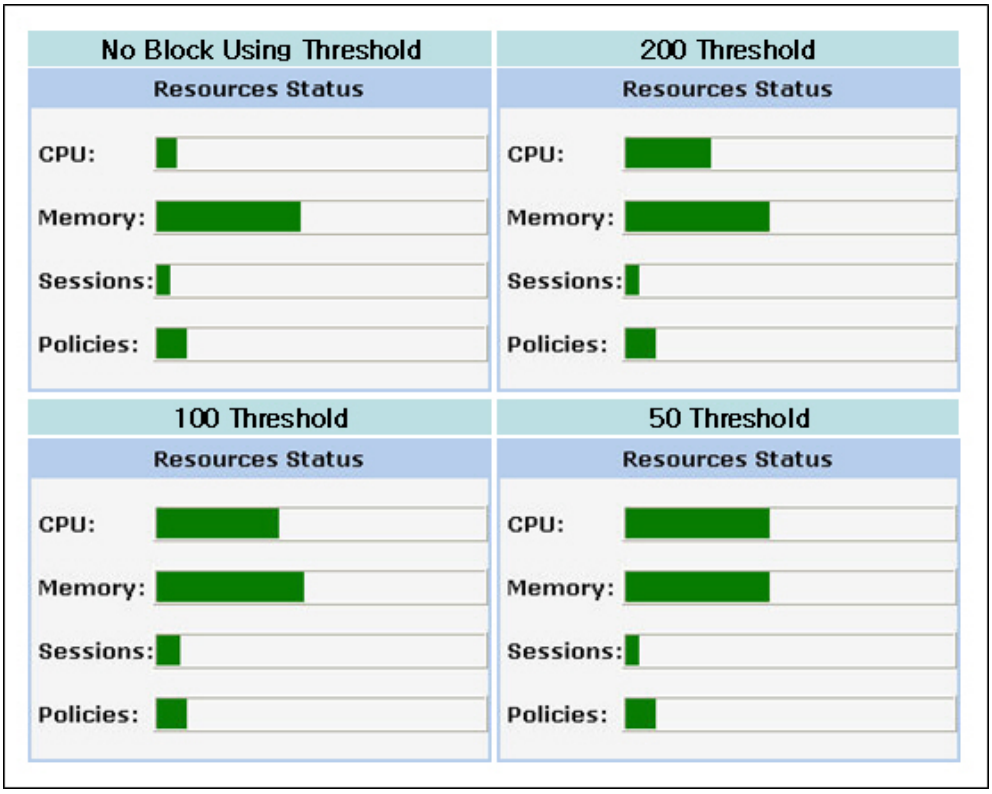
이러한 형태의 공격은 기본적으로 Threshold 설정을 어디에 할 것인가와 부가적으로 Router에서의 Ingress/Egress Filter를 어떻게 할 것인가와 관련이 있다.

먼저, victim의 서비스를 정상화 시키기 위해 Zone A에 위치한 방화벽에서 적절한 Threshold 설정을 해야 한다. 다음, NMS이나 ID/PS를 이용하여 트래픽 분석을 실시한 후 DoS의 진원지를 파악해야 한다. 위치가 파악되면 DoS의 진원지와 가장 근접한 Router에서의 Filter 설정과 Firewall 설정하여 다른 Zone으로 비정상적인 UDP packet이 흐르지 못하도록 해야 한다. 마지막으로, 진원지 Zone에 위치한 Host를 조사하여 DoS를 발생시키는 악성 프로그램을 찾아서 제거해야 할 것이다.

위에서 살펴본 것처럼 UDP Flood 공격은 관리자의 적절한 대응이 피해를 줄이는 가장 큰 요인이 됨을 확인할 수 있다.

5.4. Against The Other Problem

지금까지 살펴본 내용에서는 모든 DDoS가 Firewall의 가용 한계치 내에서 이루어 진다고 가정하고 있다. 하지만 실제 공격에서는 가용 한계치 이상의 공격이 발생하고 있다. 따라서, DDoS가 발생하였을 때 Firewall에서는 적절한 Threshold 설정을 하게 되면 상대적으로 Firewall에 프로세싱 부하가 걸리게 된다.



[그림5.7] Threshold 설정 강도에 따른 Firewall CPU 사용량

[그림5.7]에서는 확인할 수 있듯이 동일한 공격 강도에 대해 Threshold 값이 변화함에 따라 Firewall의 CPU가 어떻게 변화하는지 보여주고 있다.

또한, 공격 강도가 강해짐에 따라 CPU 사용량은 증가하게 되며 이 증가폭은 Firewall에서 Block 설정을 하는 정도에 따라 높아진다.

[그림5.2]의 Check 1을 보면 모니터링 Host로 전해지는 트래픽 정보가 끊어짐을 확인 할 수 있다. 결과적으로 Firewall의 가용 한계치를 초과한 공격이 들어 올 경우 Block을 하여도 DoS 상황에 빠지는 결과를 초래하게 된다.

이는 네트워크 bandwidth와 Firewall의 가용성과 관련된 문제이다. 따라서 Edge Router에

인접한 Firewall이나 기타 보호하고자 하는 구역에 위치한 Firewall의 성능을 업그레이드 시키거나 네트워크의 트래픽을 분산하여 ***병렬 구성*** 할 수 있는 방향을 문제 해결의 방향을 잡아가야 한다.

6. 결론

일반적으로 운영체제나 응용 프로그램의 취약점을 이용하는 공격에 비해 DoS라는 공격은 다루기가 쉽지 않다. 또 가져오는 효과가 큰데 비해 조작하기가 쉬우며 분산된 환경에서 이루어지기 때문에 추적 또한 용의하지 않다. 보안 업데이트를 통해 방어가 가능한 공격이 아니기 때문에 지속적인 네트워크 상태 분석 및 가용성 체크, 사고 대응 프로세스를 마련해야 한다.

결론적으로 분산된 형태의 DoS인 DDoS 형태로 UDP Flood 공격이 발생하였을 때 아래와 같은 준비가 필요하다.

- 가동중인 네트워크 보안 장비의 가용 한계치 파악
- 네트워크에 위치하고 있는 Firewall의 위치 분석을 통한 Critical Location 추출
- 보안 담당자와 네트워크 관리자 간의 유기적인 협조 체제

항상 네트워크 보안 장비의 한계치 영역 내로 공격이 이루어지지 않는다. 보통은 한계치를 초과한 공격이 이루어 지며, 최근에는 대부분의 공격이 이에 해당한다. 따라서 보안 담당자와 네트워크 관리자는 보호하고 있는 네트워크와 보안 장비의 가용 한계치를 파악하여 공격을 받을 시 보안 장비가 DoS 상태에 빠지지 않도록 대비해야 할 것이다.

또한, 네트워크 곳곳에 위치하고 있는 Firewall의 위치를 분석하고 이를 토대로 DDoS 방어를 위한 적절한 Critical Location을 파악하여 공격 발생 시 Threshold 설정 과 같은 보안 정책을 빠르게 적용할 수 있도록 준비해야 한다.

끝으로, DDoS 공격이 발생했을 때 대다수의 1차 발견이 보안 담당자가 아닌 네트워크 관리자에 의해서 이루어지고 있다. 따라서, 보안 담당자의 입장에서 DDoS 공격을 판별하고 대응하기 위해서는 네트워크 관리자로부터 충분한 정보를 획득해야 한다.

7. 참고 자료

[1] Michael Glenn, 2003, “A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment”

[2] Cisco, 2004, “Worm Mitigation Technical Details”

[3] J. Postel, 1980, “USER DATAGRAM PROTOCOL”

[4] Juniper Networks, 2006, “FIPS 140-2 Security Policy”

[5] Milutinovic, Milic, Savic, “Denial of Service Attacks: Methods, Tools, and Defenses”

[6] Konstantinos, Brian, Hyoseon Kim, “The Detection & Defense of DDoS Attack”

[7] Cisco, 2004, “Defeating DDoS Attacks”

[8] Ross Oliver, “Countering SYN Flooding Denial of Service (DOS) Attack”

[9] J. Postel, 1981, “INTERNET CONTROL MESSAGE PROTOCOL”