

DDOS 공격 유형별 대응방안 설명

2008. 4.

Contents

I DDOS 공격 개요

II DDOS 공격 대비 사전 준비

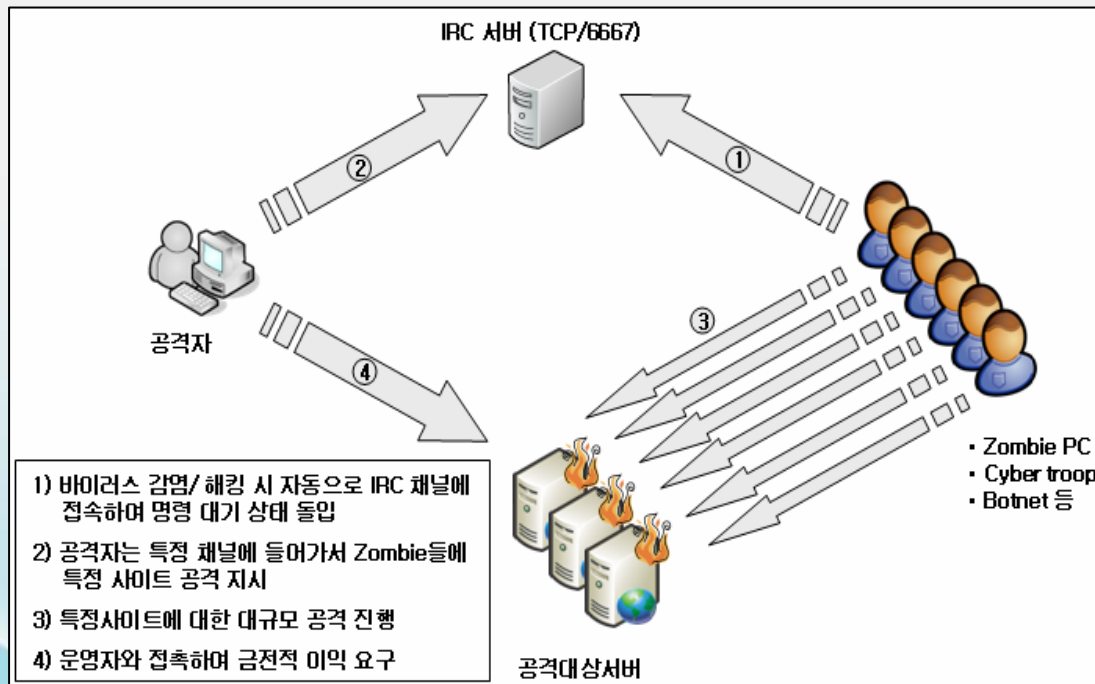
III DDOS 공격 대응 방안

IV 기타 고려 사항

V DDOS 공격 대응 전용 시스템 시험

I. DDOS 공격 개요

1. DDOS 공격 방식



o Agent 유포 방식

- P2P : 정상 S/W에 악성 코드 (DDOS Agent) 삽입
- 웜/바이러스 : 웜/바이러스에 악성 코드 (DDOS Agent) 삽입
- 사회공학 : 이메일 등을 통한 악성 코드(DDOS Agent) 전파
- 홈페이지 : 취약한 사이트 해킹을 통한 악성 코드 (DDOS Agent) 유포

I. DDOS 공격 개요

2. 공격 유형 분석

	PPS 증가 (PPS Consuming)	웹서비스 지연 (http Flooding)	대용량 트래픽 전송 (Bandwidth Consuming)
사용 프로토콜	TCP	HTTP	주로 UDP/ICMP
공격 PC 위치	국내/국외	국내/국외	국내
IP변조여부	변조/실제IP	실제IP	변조/실제IP
공격 유형	64byte 이하 100Mbyte 수십만~수백만 PPS	동일 URL 접속 시도	1000~1500byte 1Gbyte 수십만 PPS
공격 효과	네트워크 장비, 보안장비, 서버 등의 부하 발생	웹서버 부하 발생	회선 대역폭 초과
피해 시스템	공격 대상 시스템 또는 동 일 네트워크에서 사용 중 인 모든 시스템	공격 대상 시스템	동일 네트워크에서 사용 중인 모든 시스템

I. DDOS 공격 개요

3. DDOS 공격의 진화

o 계측기 공격

예) 스마트비트 : 초당 148만 PPS 이상 발생

o Slow TCP Connection Flooding 공격

예) 다수의 PC에서 초당 10 Connection 이하

o http를 이용한 공격

예) 공격 대상 사이트 분석을 통한 URL, 파라미터 변조

o 기본 DDOS 공격 기술의 응용

예) 잘 알려진 IP로 Source IP 변조

II. DDOS 공격 대응 사전 준비

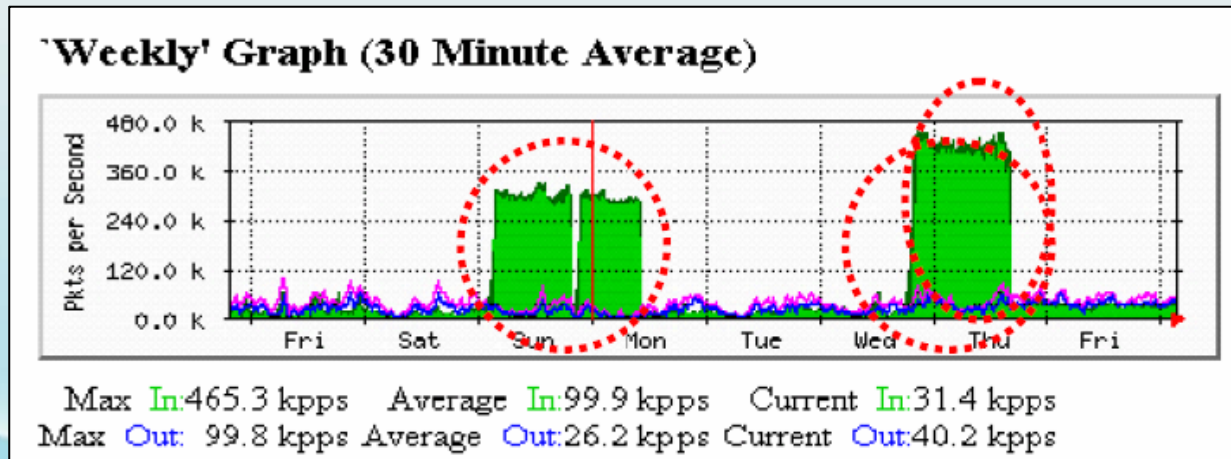
1. 기 설치된 시스템을 이용한 모니터링 체계 구축

① MRTG를 이용한 네트워크 모니터링

MRTG 등을 이용하여 PPS, BPS 등 모니터링 수행

o PPS(Packet per Second) 모니터링

- 목적 : 공격 징후 및 유형 파악 등(PPS 증가 공격)
- 공격징후 : 평상시 보다 2~3배 이상 많은 PPS가 10분 이상 지속될 경우
- 모니터링 : mrtg 등을 이용한 PPS 모니터링(라우터, L3/L4 스위치 등)

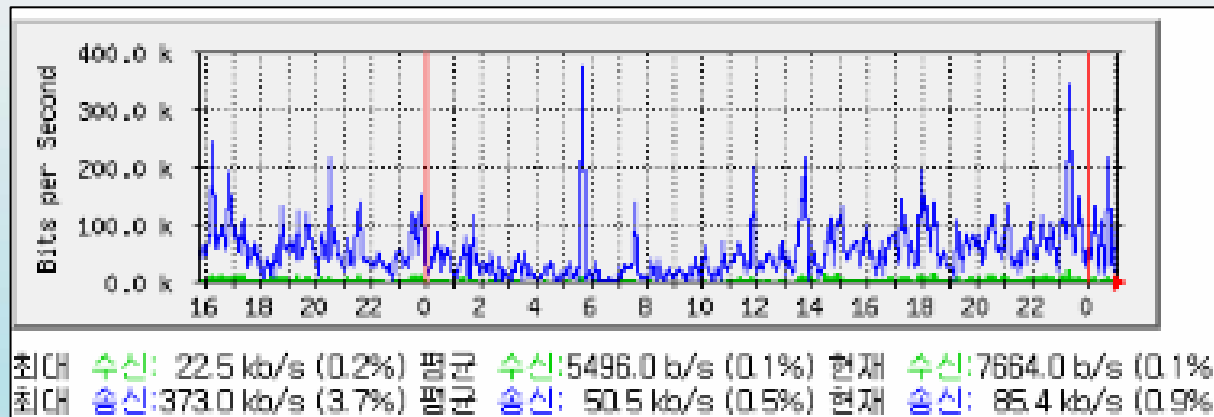


II. DDOS 공격 대응 사전 준비

1. 기 설치된 시스템을 이용한 모니터링 체계 구축

o BPS(Bits per Second) 모니터링

- 목적 : 공격 징후 및 유형 파악 등(대량 트래픽 전송 공격)
- 공격징후 : 평소보다 트래픽 양이 증가하여 사용하고 있는 전용선 대역폭의 90% 이상 사용될 경우
- 모니터링 : mrtg 등을 이용한 BPS 모니터링(라우터, L3/L4 스위치 등)



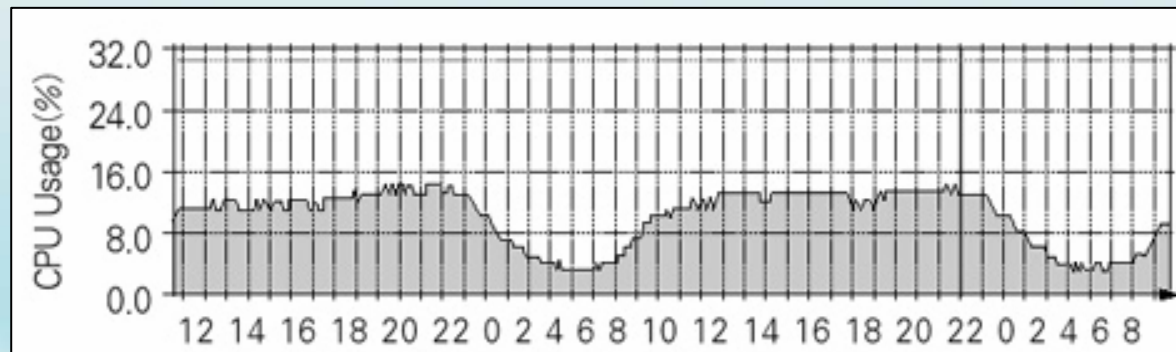
II. DDOS 공격 대응 사전 준비

1. 기 설치된 시스템을 이용한 모니터링 체계 구축

② 네트워크 장비 및 서버 성능 모니터링
기존 네트워크 장비 및 서버에 대한 성능(CPU, 메모리, 세션 사용량 등) 모니터링 수행

o 각종 네트워크/보안 장비 및 서버에 대한 성능 모니터링

- 목적 : 장애 포인트 점검을 위한 기본 자료
- 공격징후 : 서버 및 네트워크 장비의 CPU 및 메모리 사용량이 급격히 증가
- 모니터링 : mrtg(네트워크 장비) 및 SMS(서버) 등을 이용한 모니터링



II. DDOS 공격 대응 사전 준비

1. 기 설치된 시스템을 이용한 모니터링 체계 구축

0 서버 모니터링

- 목적 : 웹서버 모니터링
- 공격징후 : SYN_RECEIVED 상태가 급격히 증가(IP변조 SYN Flooding)하거나, 동일 IP에서 대량의 세션 연결(ESTABLISHED 상태) 발생

TCP	20.20.20.2:80	192.168.1.232:1081	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.233:1080	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.233:1081	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.234:1080	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.234:1081	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.235:1080	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.235:1081	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.236:1080	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.236:1081	SYN_RECEIVED			
TCP	20.20.20.2:80	192.168.1.237:1080	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43705	ESTABLISHED
TCP	20.20.20.2:80	192.168.1.237:1081	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43706	ESTABLISHED
TCP	20.20.20.2:80	192.168.1.238:1080	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43707	ESTABLISHED
TCP	20.20.20.2:80	192.168.1.238:1081	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43708	ESTABLISHED
TCP	20.20.20.2:80	192.168.1.239:1080	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43709	ESTABLISHED
TCP	20.20.20.2:80	192.168.1.239:1081	SYN_RECEIVED	20.20.20.2:80	20.20.0.100:43710	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43711	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43712	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43713	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43714	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43715	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43716	ESTABLISHED
TCP	20.20.20.2:80			20.20.20.2:80	20.20.0.100:43717	ESTABLISHED

IP 변조 Syn Flooding 공격 시

실제 IP를 이용한 Syn Flooding 공격 시

II. DDOS 공격 대응 사전 준비

1. 기 설치된 시스템을 이용한 모니터링 체계 구축

③ 로그 분석을 통한 모니터링

기존 네트워크 장비(L3/L4 스위치, 라우터, 방화벽 등)에서 제공하는 로깅 기능을 이용하여 모니터링 수행

o 출발지 및 목적지 IP

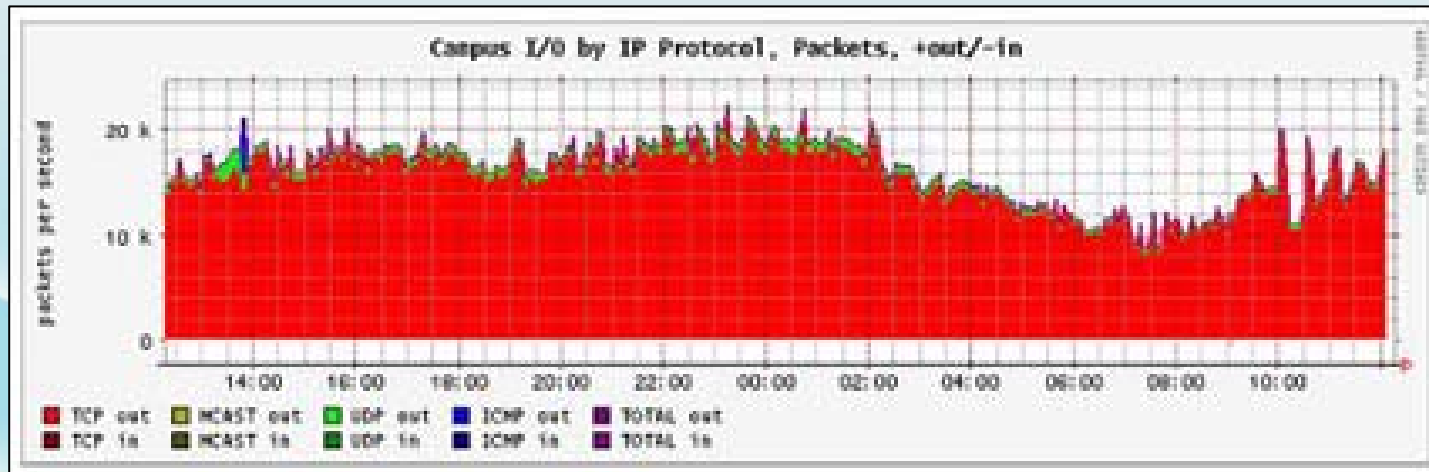
- 목적 : 공격 대상 확인 및 공격 IP(국내/국외/변조여부) 등 파악
- 모니터링 : L3/L4 스위치, 라우터, 방화벽 등

N.	Date	Time	O...	Act	Source	Src. Port	Dst.	Service
648502	7Apr2008	20:59:16	FW-2	Drop	TCP 181,53,254,42	12345	168	http
648503	7Apr2008	20:59:16	FW-2	Drop	TCP 64,64,139,1	12345	168	http
648504	7Apr2008	20:59:16	FW-2	Drop	TCP 182,56,88,174	12345	168	http
648505	7Apr2008	20:59:16	FW-2	Drop	TCP 154,208,45,192	12345	168	http
648506	7Apr2008	20:59:16	FW-2	Drop	TCP 180,184,96,165	12345	168	http
648507	7Apr2008	20:59:16	FW-2	Drop	TCP 40,105,157,23	12345	168	http
648508	7Apr2008	20:59:16	FW-2	Drop	TCP 216,23,182,230	12345	168	http
648509	7Apr2008	20:59:16	FW-2	Drop	TCP 135,127,250,68	12345	168	http
648510	7Apr2008	20:59:16	FW-2	Drop	TCP 87,112,61,135	12345	168	http
648511	7Apr2008	20:59:16	FW-2	Drop	TCP 143,226,101,28	12345	168	http
648512	7Apr2008	20:59:16	FW-2	Drop	TCP 216,126,45,185	12345	168	http
648513	7Apr2008	20:59:16	FW-2	Drop	TCP 80,211,164,218	12345	168	http
648514	7Apr2008	20:59:16	FW-2	Drop	TCP 27,203,73,148	12345	168	http
648515	7Apr2008	20:59:16	FW-2	Drop	TCP 95,6,9,41	12345	168	http
648516	7Apr2008	20:59:16	FW-2	Drop	TCP 214,114,103,238	12345	168	http
648517	7Apr2008	20:59:16	FW-2	Drop	TCP 82,145,146,247	12345	168	http
648518	7Apr2008	20:59:16	FW-2	Drop	TCP 226,58,58,101	12345	168	http
648519	7Apr2008	20:59:16	FW-2	Drop	TCP 136,8,85,17	12345	168	http
648520	7Apr2008	20:59:16	FW-2	Drop	TCP 151,202,75,50	12345	168	http
648521	7Apr2008	20:59:16	FW-2	Drop	TCP 45,81,21,143	12345	168	http
648522	7Apr2008	20:59:16	FW-2	Drop	TCP 115,53,74,134	12345	168	http
648523	7Apr2008	20:59:16	FW-2	Drop	TCP 125,235,56,140	12345	168	http
648524	7Apr2008	20:59:16	FW-2	Drop	TCP 1,55,135,112	12345	168	http
648525	7Apr2008	20:59:16	FW-2	Drop	TCP 71,185,222,193	12345	168	http

II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

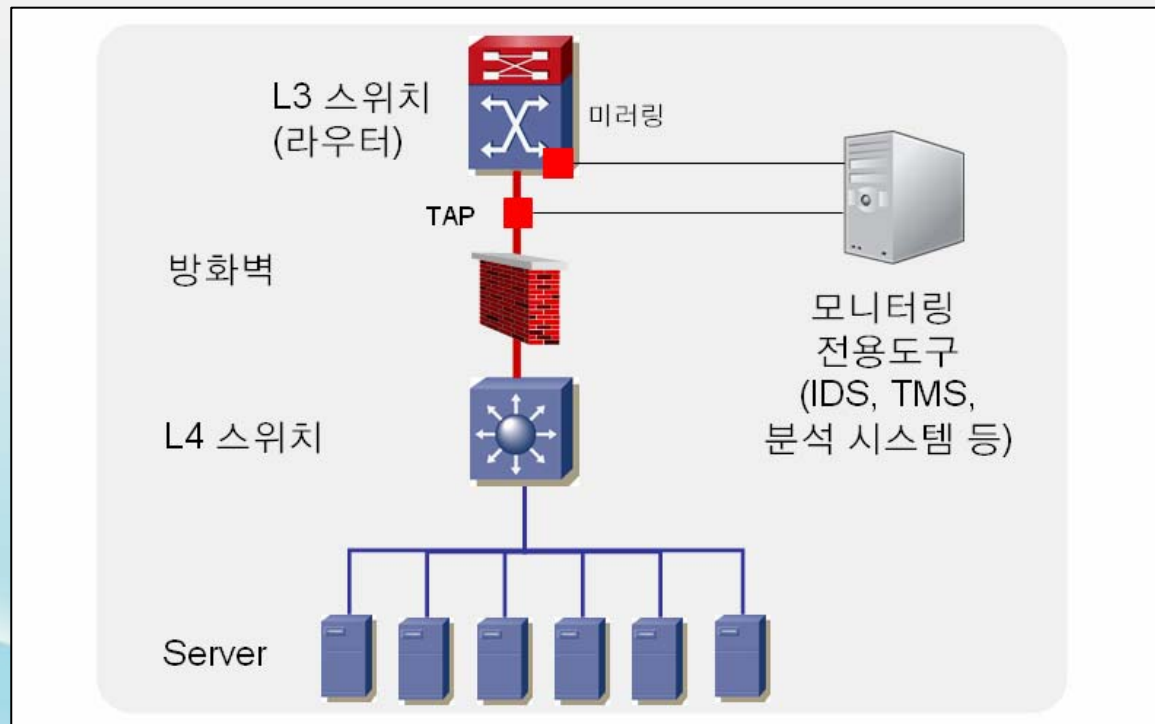
- ① Netflow, FlowScan 등을 이용한 모니터링
가장 많은 트래픽을 유발하는 IP, FPS(Flows per Second), IP/서비스 프로토콜별 사용량 등에 대한 모니터링
- ※ Netflow를 사용 시, 네트워크 장비의 부하 발생 가능하므로 적용 시 주의
- o IP 프로토콜(TCP, UDP, ICMP 등) 분포
- 목적 : 공격 징후 및 유형 파악 등
 - 공격징후 : 특정 프로토콜의 사용량이 평소의 사용량 보다 급격히 증가하는 경우
 - 모니터링 : L3스위치, 라우터에서 제공하는 모니터링 기능을(netflow, cflow) 이용하여 IP 프로토콜별 bps, fps, pps 등을 모니터링



II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

- ② 모니터링 시스템을 이용한 모니터링
- IDS, TMS, 네트워크 분석 시스템 등과 같은 모니터링 시스템 이용
 - 네트워크에 대한 분석 및 공격 유형 모니터링
 - 네트워크 **최상단**에 TAP 설치 및 미러링을 이용한 실시간 모니터링 필요

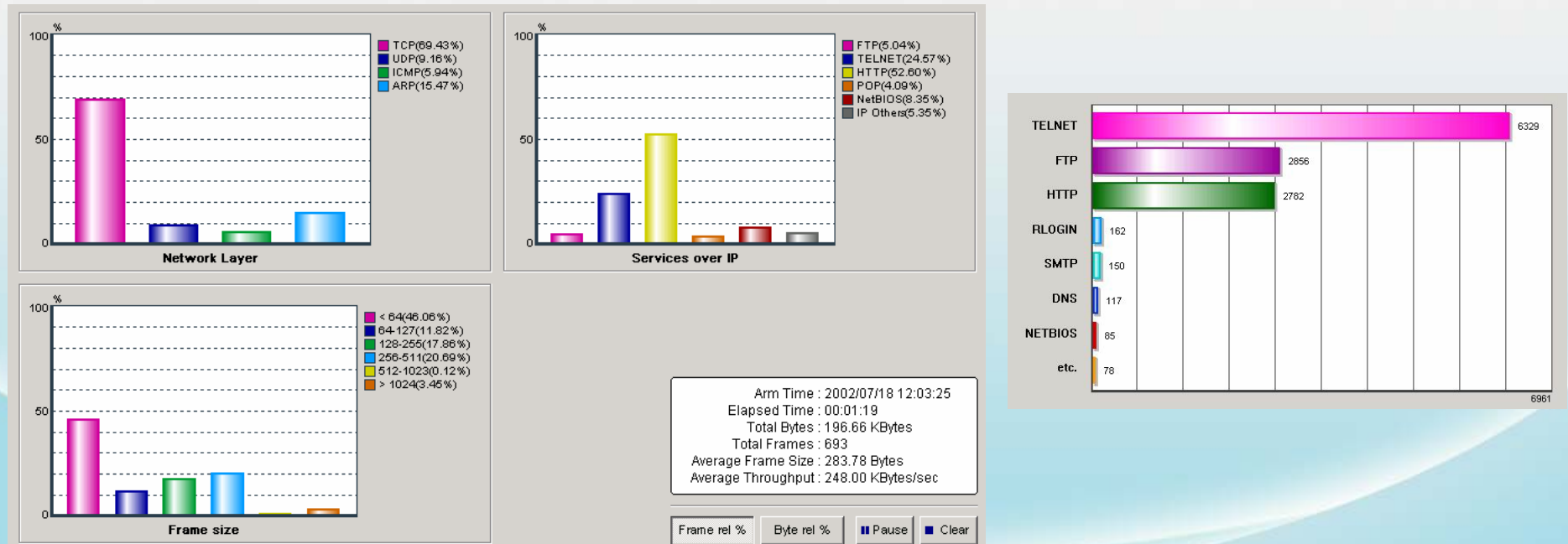


II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

0 네트워크 현황 분석

- 목적 : 공격 징후 및 유형 파악 등
- 모니터링 : 모니터링 시스템을 이용하여, 프로토콜/서비스 별 사용현황 및 **Frame Size** 등에 대한 현황을 모니터링

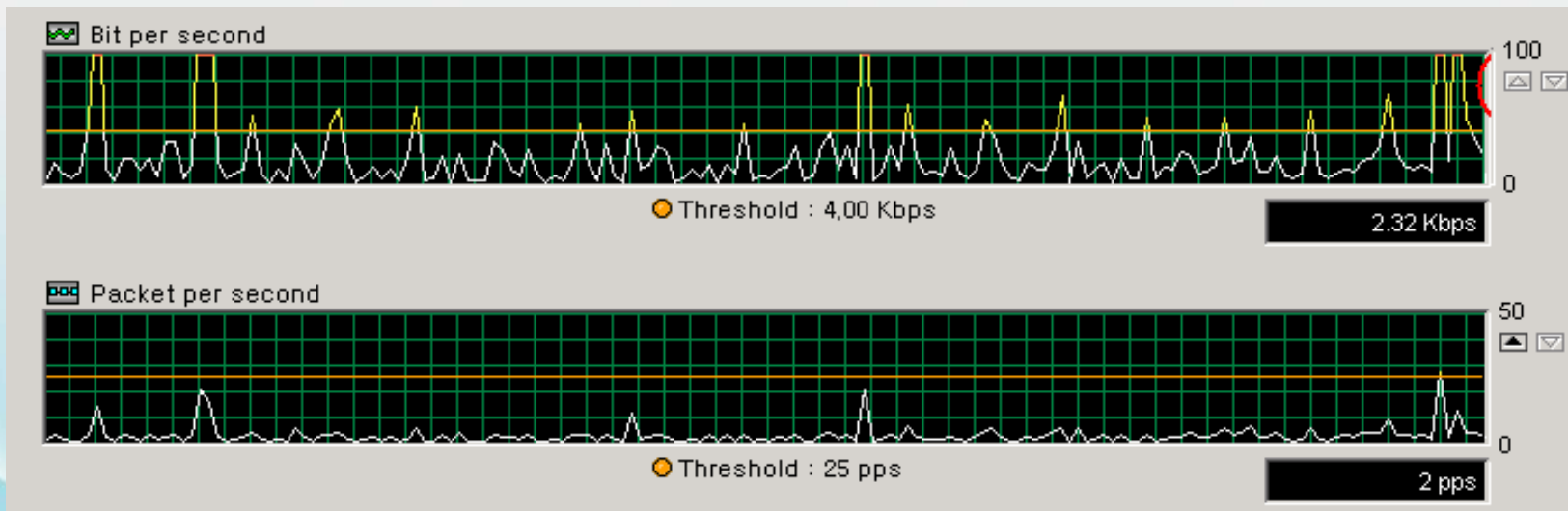


II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

0 임계치 설정을 통한 알림 기능 사용

- 목적 : 공격 징후 파악
- 모니터링 : 프로토콜별/서비스별/대역폭별/PPS별 사용량에 대한 임계치를 설정하여 설정된 임계치를 초과할 경우 알림 기능을 통한 모니터링

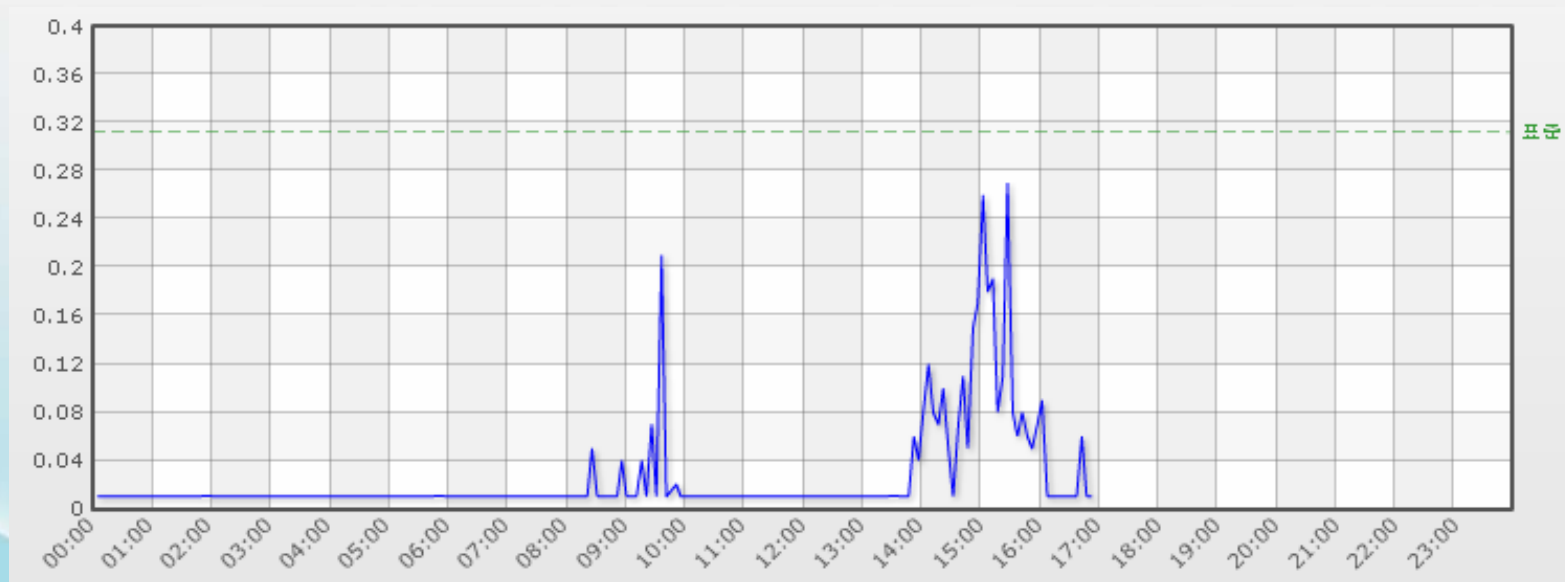


II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

o 응답 시간(Response Time) 측정

- 목적 : 사용자 응답 속도 측정을 통한 장애 여부 파악
- 공격징후 : 서버 응답 속도가 현저하게 올라가는 경우
- 모니터링 : 외부에서 웹서버 등의 응답 속도 모니터링



II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

0 패킷 분석

- 목적 : 공격 유형 및 패턴 분석(IP 변조 여부 파악 등)
- 모니터링 : IDS, TMS, 네트워크 분석 시스템 등을 이용하여 캡처된 **패킷을 분석**
- 대응 : 캡처된 패킷을 통하여 패턴을 분석하고 생성된 패턴(TTL, Frame size, 기타 패킷 헤더 옵션)을 **IPS, IDS, L7 스위치 등에 적용**하여 탐지/차단 수행

30492	274.404845	51.171.21.49	20.20.20.2	TCP	1024	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30493	274.404848	240.51.204.116	20.20.20.2	TCP	1024	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30494	274.404852	186.163.171.28	20.20.20.2	TCP	1024	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30495	274.404856	128.68.242.115	20.20.20.2	TCP	3072	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30496	274.404859	75.37.169.3	20.20.20.2	TCP	3072	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30497	274.404863	92.27.200.40	20.20.20.2	TCP	3072	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30498	274.404866	116.20.30.18	20.20.20.2	TCP	3072	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30499	274.404870	157.60.248.93	20.20.20.2	TCP	3072	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30500	274.404872	29.236.7.113	20.20.20.2	TCP	1024	>	http	[SYN]	Seq=0	Len=0	MSS=1460
30501	274.404875	236.55.54.		Differenziated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)							
30502	274.404876	123.8.166.		Total Length: 48							
30503	274.404878	160.220.16		Identification: 0x02fe (766)							
30504	274.404879	70.130.10.		Flags: 0x04 (Don't Fragment)							
30505	274.404883	86.128.90.		Fragment offset: 0							
30506	274.404887	203.192.19		Time to live: 128							
30507	274.404895	229.252.13		Protocol: TCP (0x06)							
				Header checksum: 0x86d8 [correct]							
				Source: 51.171.21.49 (51.171.21.49)							
				Destination: 20.20.20.2 (20.20.20.2)							
				Transmission Control Protocol, Src Port: 1024 (1024), Dst Port: http (80), Seq: 0, Len: 0							
				Source port: 1024 (1024)							
				Destination port: http (80)							
				Sequence number: 0 (relative sequence number)							
				Header length: 28 bytes							
				Flags: 0x0002 (SYN)							
				window size: 8192							
				Checksum: 0x7d93 [correct]							
				Options: (8 bytes)							

II. DDOS 공격 대응 사전 준비

2. 모니터링 시스템 및 DDOS 공격 대응 시스템 활용

③ DDOS 공격 대응 시스템

- NBA 기반의 DDOS 공격 대응 전용 시스템
- DDOS 공격 대응 기능이 추가된 IPS
- 웹 가속기, L7 보안스위치
- 기타 보안 시스템 등

III. 공격 유형 별 대응 방안

1. PPS 증가 (PPS Consuming)

o IP Spoofed Syn Flooding 공격

특징

IP 변조 후 다량의 Syn 패킷을 공격 대상 서버로 전송
공격 받은 서버는 다수의 SYN_RECEIVED 세션 상태가 발생
서버의 CPU 및 Connection 자원의 고갈을 유발

대응 방안

1) 비정상 IP에 대한 ACL 적용

RFC1918에서 지정한 비공인 IP
특정 목적을 가진 IP 및 IANA에서 reserved한 IP

2) 해외 트래픽 차단 (NULL 라우팅 적용)

ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단(NULL 라우팅)
라우터 간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도

3) Syn Proxy 또는 Cookie 기능 사용

Syn Proxy/Cookie 기능을 제공하는 보안 장비 및 네트워크 장비 이용
단, 장비의 성능 파악 후, 적용 필요

III. 공격 유형 별 대응 방안

1. PPS 증가 (PPS Consuming)

o TCP Connection Flooding 공격 (3 way handshaking 정상 완료)

특징

IP를 변조하지 않고, 다량의 Syn 패킷을 공격 대상 서버로 전송
공격 받은 서버는 다수의 **ESTABLISHED** 세션 상태가 발생
서버의 CPU 및 Connection 자원의 고갈을 유발

대응 방안

1) 공격의 진원지가 국외일 경우

ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단(**NULL 라우팅**)
라우터간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도

2) 공격의 진원지가 국내일 경우

C&C 서버의 조정을 받고 있는 봇넷 PC에 의한 경우가 대부분
대외기관에 공격 IP를 제공하여 봇넷 **샘플 확보**
샘플 분석을 통하여 **C&C 서버와 봇넷 PC와의 통신 차단**(대외기관 등 협조)
긴급한 **보안 프로그램 업데이트** 수행(보안업체 협조)
공격 소스 IP가 소수일 경우, **ACL을 이용하여 차단**

3) DDOS 대응 시스템 사용

민원 접수 및 모니터링을 통하여 장애 발생 가능성에 대비

III. 공격 유형 별 대응 방안

1. PPS 증가 (PPS Consuming)

o TCP Out-of-State Packet Flooding 공격 (ACK/SYN+ACK/FIN 등)

특징

다량의 **ACK/SYN+ACK/FIN/RST** 등의 패킷을 공격 대상 서버로 전송
방화벽이나 L4 등과 같이 세션을 관리하는 장비에서 차단
일부 네트워크 장비 및 서버의 CPU 사용량이 올라가는 등 오작동 발생 가능

대응 방안

1) IP가 변조된 경우

IP Spoofed Syn Flooding 공격 대응 방안과 동일

2) IP가 변조되지 않았을 경우

TCP Connection Flooding 공격 대응 방안과 동일

3) 보안 패치 및 장비 교체

취약한 네트워크 장비 및 서버에 대한 **패치 및 교체 진행**

III. 공격 유형 별 대응 방안

2. 웹 서비스 지연(http Flooding)

0 동일 URL 반복 접속 시도(웹서버 부하 발생)

특징

IP를 변조하지 않고, 정상적인 3 way handshake 후 동일한 URL 반복 요청
(get /index.jsp 등)일부
웹서버의 CPU 및 Connection 자원의 고갈을 유발

대응 방안

- 1) 공격의 진원지가 해외일 경우
TCP Connection Flooding 공격 대응 방안과 동일
- 2) 공격의 진원지가 국내일 경우
TCP Connection Flooding 공격 대응 방안과 동일
- 3) 서버 설정 변경(임시방안)
KeepAlive를 off로 변경
MaxClient를 최대수치로 조정
- 4) 웹서버 증설
- 5) DDOS 대응 시스템 사용

III. 공격 유형 별 대응 방안

2. 웹 서비스 지연(http Flooding)

o 조회(로그인) 반복 시도(웹서버 및 DB 서버 부하 발생)

특징

정상적인 3 way handshake 후 로그인 및 상품 조회와 같은 요청 반복 전송
웹서버 및 DB 서버의 CPU 및 Connection 자원의 고갈을 유발

대응 방안

‘동일 URL 반복 접속 시도’ 대응 방안과 동일

III. 공격 유형 별 대응 방안

3. 대용량 트래픽 전송(Bandwidth Consuming)

o UDP/ICMP Flooding

특징

1000~1500byte 정도의 큰 패킷을 공격 대상 서버(네트워크)로 전송
네트워크 회선 대역폭 고갈
공격 대상 서버와 같은 네트워크에서 운영 중인 모든 서버의 접속 장애 유발

대응 방안

- 1) 불필요한 UDP/ICMP 서비스 차단
가능한 최상위 구간(국제 GW, IDC 라우터 등)에서 차단
- 2) 공격 대상 서버에 대한 NULL 라우팅 적용(임시방안)
공격 대상 서버에 대한 NULL 라우팅을 적용하여 점진적으로 공격 트래픽 감소
동일네트워크에서 운영중인 다른 서버/서비스 보호
- 3) DNS 서버의 다중화
다중 DNS 서버를 운영
제3의 등록기관에 DNS를 등록
- 4) DNS 전용 회선 준비
서비스 네트워크 회선과 별도로 우회할 수 있는 DNS 전용 회선 마련

III. 공격 유형 별 대응 방안

4. 기타

0 특정 패턴을 가진 DOS 공격

대응 방안

1) 보안 시스템 사용

IDS, TMS 등과 같은 모니터링 시스템을 통하여 공격 트래픽에 대한 분석
생성된 패턴을 IPS, L7 스위치 등에 적용하여 차단

0 네트워크 장비, 서버 등의 취약점을 이용한 DOS 공격

대응 방안

1) 보안 패치

취약한 네트워크 장비 및 서버에 대한 패치를 진행

2) 보안 시스템 사용

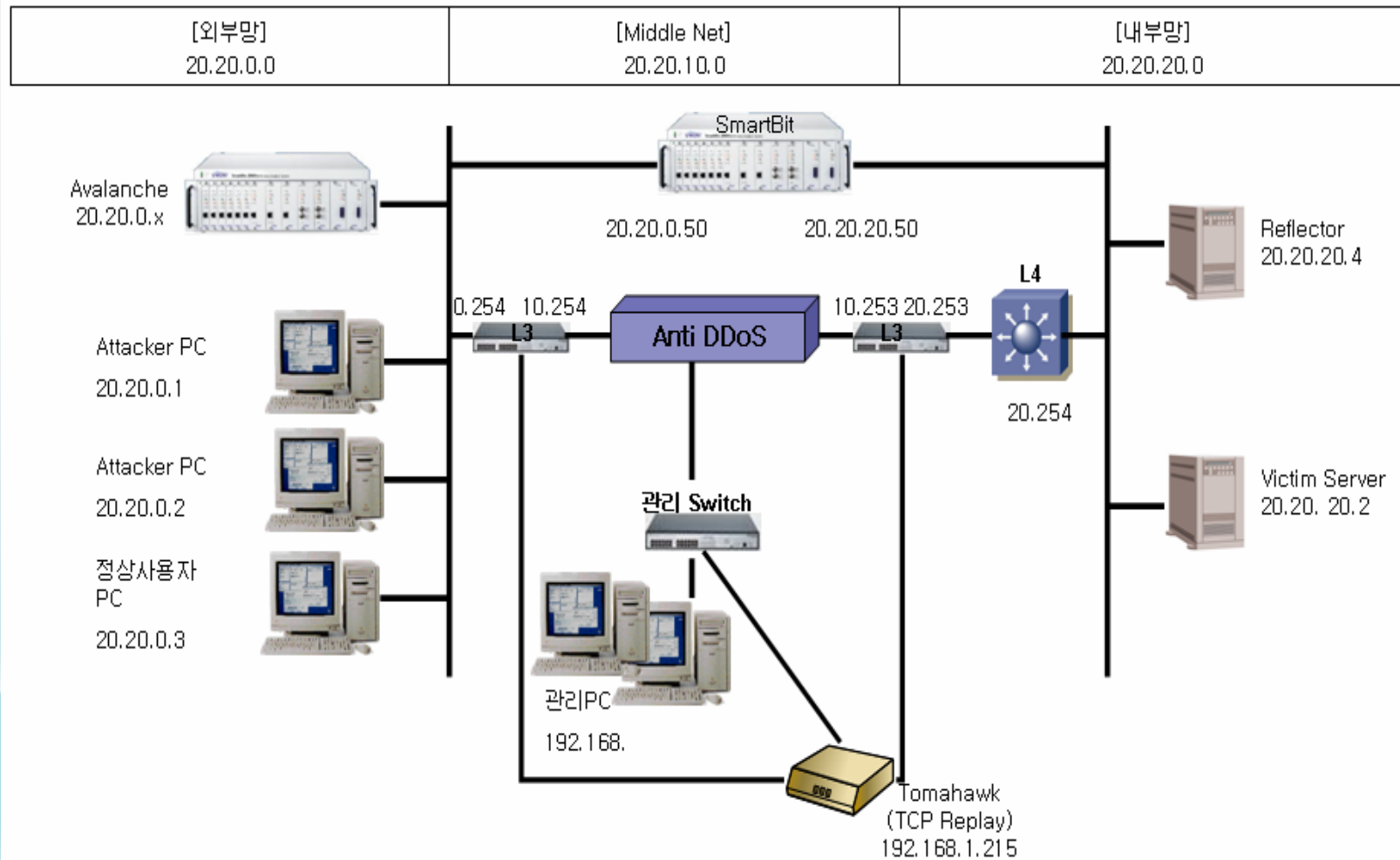
IDS, TMS 등과 같은 모니터링 시스템을 통하여 공격 트래픽에 대한 분석
생성된 패턴을 IPS, L7 스위치 등에 적용하여 차단

IV. 기타 고려 사항

0 공격에 대비한 사전 준비	0 공격 발생시
<ul style="list-style-type: none"> - 모니터링 체계 구축 공격 징후 및 공격 발생 시, 즉시 인지 및 분석 가능 - 공격에 대비한 업무 분장을 통한 단일 명령 체계 확립 - 대외 협력 기관과의 협조 체계 및 비상 연락망 사전 구축 	<ul style="list-style-type: none"> - 공격 확산 방지 대응방안에 따른 초동 대응 네트워크 수준으로의 공격 확산 방지 - ISP/IDC 등과의 적극적인 협력 실시간 정보 공유 및 공동 대응 방안 마련 - 대외 협력 기관과의 협력 샘플 확보 및 분석 보안 프로그램(백신) 업데이트, 봇넷 제거 등

V. DDOS 공격 대응 전용 시스템 시험

1. 시험 환경



V. DDOS 공격 대응 전용 시스템 시험

2. 기능 시험 항목

시험항목		설명
1	IP Spoofed Syn Flooding	변조된 IP를 이용하여 다량의 TCP Syn 패킷을 전송하는 공격
2	TCP Connection Flooding	실제 IP를 이용하여 다량의 TCP Syn 패킷을 전송하는 공격
3	TCP Out-of-State Packet Flooding	변조 또는 실제 IP를 이용하여 다량의 TCP 패킷(ACK, SYN+ACK, ACK, FIN 등)을 전송하는 공격
4	http Flooding	동일한 URL을 반복적으로 요청하는 공격 웹페이지의 파라미터를 변조하여 반복적으로 요청하는 공격
5	UDP/ICMP Flooding	변조 또는 실제 IP를 이용하여 다량의 UDP/ICMP 패킷을 전송하는 공격
6	IP Flooding	변조된 IP주소와 헤더정보를 가진 패킷을 Fragmentation하여 전송하는 공격

※ Spoofed SYN Flooding 등 DDOS 공격 유형별 대응 여부 점검(21종)

V. DDOS 공격 대응 전용 시스템 시험

3. 성능 시험 항목

시험항목		설명
1	Response time	<ul style="list-style-type: none"> - Smartbit 이용 100M씩 SYN 트래픽 증가시키며 Reflector로 전송 - 최대 800M Syn 패킷 생성(소스IP 변조)하여 Reflector(20.20.20.4)로 공격 시 정상 세션 (1000 connection) 생성 여부 확인 - Response time 측정(증가여부)
2	CPS	<ul style="list-style-type: none"> - Avalanche 이용 측정 (예 : 초당 6만개 생성 가능 여부)
3	Max Connection	<ul style="list-style-type: none"> - Avalanche 이용 측정 (예 : 150만개 세션 생성 유지 여부)
4	Latency, Throughput	<ul style="list-style-type: none"> - SmartBit 이용
5	계측기 공격	<ul style="list-style-type: none"> - SmartBit에서 하나 또는 다수의 IP를 이용 - 단방향 1G SYN 트래픽(약148만개/초)을 생성 - 장비의 부하를, 차단률 여부 확인

V. DDOS 공격 대응 전용 시스템 시험

4. 부하 발생시 기능 시험

- o 기본 시험환경(Tomahawk, Avalanche)에서 SmartBit을 이용하여 양방향 1G 트래픽을 추가 생성하여 Background 환경 구성 후 기능시험항목을 시험
- o 기능 시험 시와 동일한 작동 여부 파악

5. Bypass 시험

- o 기존 세션(ftp, ssh 등) 유지 및 패킷(ping) 손실량 측정

V. DDOS 공격 대응 전용 시스템 시험

6. 선정시 고려사항

- o 학습기반 시스템의 경우, 모의환경에서 정확한 시험 결과 측정 어려움
- o 일부 시스템의 경우, 특정 공격(대용량 트래픽 포함) 발생시 시스템의 부하(CPU, 메모리 등) 발생으로 인하여 1G 이상의 성능을 제공하지 못함
- o BYPASS 기능 정상 작동 시, 장애 포인트로의 위험성 감소(In-line 기반 시스템)
- o 금융회사의 운영 환경을 고려하여 DDOS 대응 시스템 선정 필요
 - DDOS 전용 장비, Web 가속기, IPS 등
 - In-line 방식 또는 out-of-path 방식
 - 네트워크 구성 및 성능 등
- o DDOS 대응 시스템 운영 시, 적절한 커스터마이징(임계치 설정, 차단 시간 등) 필요
 - 공격 대응 시, 정상 서비스에 대한 가용성 보장 여부 파악 필요



감사합니다