DDoS 공격 비상, 어떻게 대처할 것인가?
- 7.7 DDoS 공격 유형 분석 및 대응방안 -

Date : 2009.07.16

Cisco Systems Korea

7.7 DDoS 대란 요약 분석

7.7 DDoS Summary
시간대별 요약

1차 DDoS 공격 (2009.07.05 ~ 07.06)

미국 21개 주요 정부기관,금융,인터넷 포털 사이트 대상으로 대규모 공격 감행

2차 DDoS 공격 (2009.07.07 ~ 07.08)

국내 12개/미국 14개 주요 정부기관,금융,인터넷 포털 사이트 대상으로 대규모 공격 감행

3차 DDoS 공격 (2009.07.08 ~ 07.09)

국내 15개/미국 1개 주요 정부기관,금융,인터넷 포털 사이트 대상으로 대규모 공격 감행

4차 DDoS 공격 (2009.07.09 ~ 07.10)

국내 7개 주요 정부기관,금융,인터넷 포털 사이트 대상으로 대규모 공격 감행

DDoS 공격 종료 (2009.07.10 18:00)

7.7 DDoS Summary
1차 미국 사이트 공격 분석 요약

공격 발생 시점

- 07.05 22:00 ~ 07.06 18:00 까지 미국 공공.언론.금융.포털 사이트 중심으로 대규모 트래픽 발생

공격 목표

- 21개 미국 주요 정부기관, 미국 금융기관, 미국 포털 사이트 공격

특이 사항

- 1차 공격 발생 이전에 이미 07.05 02:00 ~ 14:00 까지 미국 정부 기관 3군데를 공격한 것으로 보임
- 21개 공격 목표 전체는 사이트 접속 불능 상태로 해당 사이트는 접속 불능 상태

7.7 DDoS Summary
1차 미국 사이트 공격 분석 요약

공격목표	Site	해당 국가	산업군 분류	공격 시작 시간	공격 종료 시간	특이사항
미국백악관	www.whitehouse.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
미국 문화재부	www.ustreas.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
미국 국토안보부	www.dhs.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 접속불가 (미국에서는 접속 가능) 한국 IP 전체 차단으로 보임
미국 국무부	www.state.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
미국 교통부	www.dot.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 접속불가 (미국에서는 접속 가능) 한국 IP 전체 차단으로 보임
미국 연방통상 위원회	www.ftc.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 접속불가 (미국에서는 접속 가능) 한국 IP 전체 차단으로 보임
미국 국가안전보장국	www.nsa.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
미국 우정국	www.usps.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
미국의 소리	www.voanews.com	미국	언론	2009-07-05 22:00	2009-07-06 18:00	
미국국방부	www.defenselink.mil	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 접속불가 (미국에서는 접속 가능) 한국 IP 전체 차단으로 보임
미국 국무부 영사사업부	travel.state.gov	미국	공공기관	2009-07-05 22:00	2009-07-06 18:00	
뉴욕증권거래소	www.nyse.com	미국	금융	2009-07-05 22:00	2009-07-06 18:00	
나스닥	www.nasdaq.com	미국	금융	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 접속불가 (미국에서는 접속 가능) 한국 IP 전체 차단으로 보임
US뱅크	www.usbank.com	미국	금융	2009-07-05 22:00	2009-07-06 18:00	
야후 금융정보 사이트	finance.yahoo.com	미국	금융	2009-07-05 22:00	2009-07-06 18:00	
야후닷컴	www.yahoo.com	미국	인터넷포털	2009-07-05 22:00	2009-07-06 18:00	
International Investment Portal&Research	www.site-by-site.com	미국	인터넷포털	2009-07-05 22:00	2009-07-06 18:00	
마켓워치	www.marketwatch.com	미국	인터넷포털	2009-07-05 22:00	2009-07-06 18:00	
미국 옥션 라이브	www.usauctionslive.com	미국	인터넷포털	2009-07-05 22:00	2009-07-06 18:00	2009-07-12 14:00 현재 전세계 모든 지역에서 접속불가 사이트 폐쇄 조치를 취한것으로 보임
아마존닷컴	www.amazon.com	미국	인터넷포털	2009-07-05 22:00	2009-07-06 18:00	

7.7 DDoS Summary
2차 한국/미국 사이트 공격 분석 요약

공격 발생 시점

- 07.07 18:00 ~ 07.08 18:00 까지 한국/미국 공공.언론.금융.포털 사이트 중심으로 대규모 트래픽 발생

공격 목표

- 국내 12개 / 미국 14개 주요 정부기관, 금융기관, 포털 사이트 공격

특이 사항

- 국내에서 7.7 DDoS 대란 1차 공격으로 알려져 있음.
- 대부분의 공격 목표 사이트가 접속 불능 상태에 빠짐.
- 미국 주요 사이트들에서는 한국 IP의 접속을 차단함.

7.7 DDoS Summary
7월 7일 국내/외 2차 공격지 요약

공격목표	Site	해당 국가	산업군 분류	공격 시작 시간	공격 종료 시간	특이사항
청와대	www.president.go.kr	한국	공공기관	2009-07-07 18:00	2009-07-08 18:00	
국방부	www.mnd.go.kr	한국	공공기관	2009-07-07 18:00	2009-07-08 18:00	
외교통상부	www.mofat.go.kr	한국	공공기관	2009-07-07 18:00	2009-07-08 18:00	
대한민국국회	www.assembly.go.kr	한국	공공기관	2009-07-07 18:00	2009-07-08 18:00	
네이버블로그	blog.naver.com	한국	인터넷포털	2009-07-07 18:00	2009-07-08 18:00	
네이버메일	mail.naver.com	한국	인터넷포털	2009-07-07 18:00	2009-07-08 18:00	
옥션	www.auction.co.kr	한국	인터넷포털	2009-07-07 18:00	2009-07-08 18:00	
농협인터넷뱅킹	banking.nonghyup.com	한국	금융	2009-07-07 18:00	2009-07-08 18:00	
신한은행인터넷뱅킹	ezbank.shinhan.come	한국	금융	2009-07-07 18:00	2009-07-08 18:00	
외환은행인터넷뱅킹	bank.keb.co.kr	한국	금융	2009-07-07 18:00	2009-07-08 18:00	
한나라당	www.hannara.or.kr	한국	정당	2009-07-07 18:00	2009-07-08 18:00	
조선일보	www.chosun.com	한국	언론	2009-07-07 18:00	2009-07-08 18:00	
주한미군	www.usfk.mil	미국	공공기관	2009-07-07 18:00	2009-07-08 18:00	2009-07-12 14:00 현재 전세계 모든 지역에서 접속불가 사이트 폐쇄 조치를 취한것으로 보임
미국백악관	www.whitehouse.gov	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
미국연방항공청	www.faa.gov	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	
미국 국토안보부	www.dhs.gov	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	2009-07-12 14:00 현재 접속불가(미국에서는 접속 가능) 한국 IP 전체 차단으로 보임 1차 해외 공격에도 포함된 사이트
미국 국무부	www.state.gov	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
미국 문화재부	www.ustreas.gov	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
미국 국방부	www.defenselink.mil	미국	공공기관	2009-07-07 21:00	2009-07-08 7:00	2009-07-12 14:00 현재 접속불가(미국에서는 접속 가능) 한국 IP 전체 차단으로 보임 1차 해외 공격에도 포함된 사이트
미국 증권거래소	www.nyse.com	미국	금융	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
나스닥	www.nasdaq.com	미국	금융	2009-07-07 21:00	2009-07-08 7:00	2009-07-12 14:00 현재 접속불가(미국에서는 접속 가능) 한국 IP 전체 차단으로 보임 1차 해외 공격에도 포함된 사이트
US 뱅크	www.usbank.com	미국	금융	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
야후 금융정보 사이트	finance.yahoo.com	미국	인터넷포털	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
옥션 라이브	www.usauctionslive.com	미국	인터넷포털	2009-07-07 21:00	2009-07-08 7:00	2009-07-12 14:00 현재 전세계 모든 지역에서 접속불가 사이트 폐쇄 조치를 취한것으로 보임 1차 해외 공격에도 포함된 사이트
미국의 소리	www.voanews.com	미국	언론	2009-07-07 21:00	2009-07-08 7:00	1차 해외 공격에도 포함된 사이트
워싱턴포스트	www.washingtonpost.com	미국	언론	2009-07-07 21:00	2009-07-08 7:00	2009-07-12 14:00 현재 전세계 모든 지역에서 접속불가 사이트 폐쇄 조치를 취한것으로 보임

7.7 DDoS Summary
3차 한국/미국 사이트 공격 분석 요약

공격 발생 시점

- 07.08 18:00 ~ 07.09 18:00 까지 한국/미국 공공.언론.금융.포털 사이트 중심으로 대규모 트래픽 발생

공격 목표

- 국내 13개 / 미국 1개 주요 정부기관, 금융기관, 포털 사이트 공격

특이 사항

- 국내에서 7.7 DDoS 대란 2차 공격으로 알려져 있음.
- 일부 사이트들에서 DDoS 대응 장비 및 Site 주소 변경, GSLB 구성등으로 서비스
- 미국 주요 사이트들에서는 한국 IP의 접속 지속적으로 차단한 기관들 있음
- 감염된 Zombie 에서 HDD를 손상시키는 변종 발견 (실제 피해는 크지 않음)

7.7 DDoS Summary
3차 한국/미국 사이트 공격 분석 요약

공격목표	Site	해당 국가	산업군 분류	공격 시작 시간	공격 종료 시간	특이사항
청와대	www.president.go.kr	한국	공공기관	2009-07-08 18:00	2009-07-09 18:00	7월 7일 공격 목표에 포함된 사이트
국방부	www.mnd.go.kr	한국	공공기관	2009-07-08 18:00	2009-07-09 18:00	7월 7일 공격 목표에 포함된 사이트
국정원 사이버안전센터	www.ncsc.go.kr	한국	공공기관	2009-07-08 18:00	2009-07-09 18:00	
전자민원 G4C	www.egov.go.kr	한국	공공기관	2009-07-08 18:00	2009-07-09 18:00	
네이버메일	mail.naver.com	한국	인터넷포털	2009-07-08 18:00	2009-07-09 18:00	7월 7일 공격 목표에 포함된 사이트
다음 메일	mail.daum.net	한국	인터넷포털	2009-07-08 18:00	2009-07-09 18:00	
파란 메일	mail.paran.com	한국	인터넷포털	2009-07-08 18:00	2009-07-09 18:00	
옥션	www.auction.co.kr	한국	인터넷포털	2009-07-08 18:00	2009-07-09 18:00	7월 7일 공격 목표에 포함된 사이트
알툴	www.altools.co.kr	한국	보안포털	2009-07-08 18:00	2009-07-09 18:00	
안철수연구소	www.ahnlab.com	한국	보안포털	2009-07-08 18:00	2009-07-09 18:00	
기업은행	www.ibk.co.kr	한국	금융	2009-07-08 18:00	2009-07-09 18:00	
하나은행	www.hanabank.com	한국	금융	2009-07-08 18:00	2009-07-09 18:00	
우리은행	www.wooribank.com	한국	금융	2009-07-08 18:00	2009-07-09 18:00	
국민은행	www.kbstar.com	한국	금융	2009-07-08 18:00	2009-07-09 18:00	
조선일보	www.chosun.com	한국	언론	2009-07-08 18:00	2009-07-09 18:00	7월 7일 공격 목표에 포함된 사이트
주한미군	www.usfk.mil	미국	공공기관	2009-07-08 18:00	2009-07-09 18:00	2009-07-12 14:00 현재 전세계 모든 지역에서 접속불가 사이트 폐쇄 조치를 취한것으로 보임

7.7 DDoS Summary
4차 한국사이트 공격 분석 요약

공격 발생 시점

- 07.09 18:00 ~ 07.10 18:00 까지 한국 공공.언론.금융.포털 사이트 중심으로 대규모 트래픽 발생

공격 목표

- 국내 7개 주요 정부기관, 금융기관, 포털 사이트 공격

특이 사항

- 국내에서 7.7 DDoS 대란 3차 공격으로 알려져 있음.
- 일부 사이트들에서 DDoS 대응 장비 및 Site 주소 변경, GSLB 구성등으로 대부분 정상 서비스
- 미국 주요 사이트들에서는 한국 IP의 접속 지속적으로 차단한 기관들 있음
- 공격 목표가 줄어 듦에 따라, 공격 목표의 트래픽 유입량이 크게 증가함
- Zombie List가 최대 18만대 이상으로 파악됨

7.7 DDoS Summary
4차 한국사이트 공격 분석 요약

공격목표	Site	해당 국가	산업군 분류	공격 시작 시간	공격 종료 시간	특이사항
전자민원 G4C	www.egov.go.kr	한국	공공기관	2009-07-09 18:00	2009-07-10 18:00	7월 8일 공격 목표에 포함된 사이트
네이버메일	mail.naver.com	한국	인터넷포털	2009-07-09 18:00	2009-07-10 18:00	7월 7일 ~8일 공격목표에 포함된 사이트
다음 메일	mail.daum.net	한국	인터넷포털	2009-07-09 18:00	2009-07-10 18:00	7월 8일 공격 목표에 포함된 사이트
파란 메일	mail.paran.com	한국	인터넷포털	2009-07-09 18:00	2009-07-10 18:00	7월 8일 공격 목표에 포함된 사이트
옥션	www.auction.co.kr	한국	인터넷포털	2009-07-09 18:00	2009-07-10 18:00	7월 7일 ~8일 공격목표에 포함된 사이트
국민은행	www.kbstar.com	한국	금융	2009-07-09 18:00	2009-07-10 18:00	7월 8일 공격 목표에 포함된 사이트
조선일보	www.chosun.com	한국	언론	2009-07-09 18:00	2009-07-10 18:00	7월 7일 ~8일 공격목표에 포함된 사이트

7.7 DDoS Issue Summary
Zombie IP 분석

Zombie IP 수량

- 대략 20만 대 내외로 추정
- A은행 Cisco Guard를 통한 Zombie IP 분석 – 188,000대 Zombie IP 추출

국내외 IP 분포

- 대부분 국내 IP로 추정되며, 3만대의 IP는 지속적인 공격을 수행하는 것으로 보임
- A은행 Cisco Guard를 통한 Zombie 공격 시도 횟수 분석 결과
  – 3만대의 IP는 HTTP Getflooding을 매우 높은 횟수로 시도함
  - 대부분 국내 IP로 추정됨

특이 사항

- 샘플링 IP를 무작위로 분석한 결과 대부분 인터넷 일반 사용자 IP

7.7 DDoS Issue Summary
Zombie Traffic 분석

Zombie Traffic 유형 분석

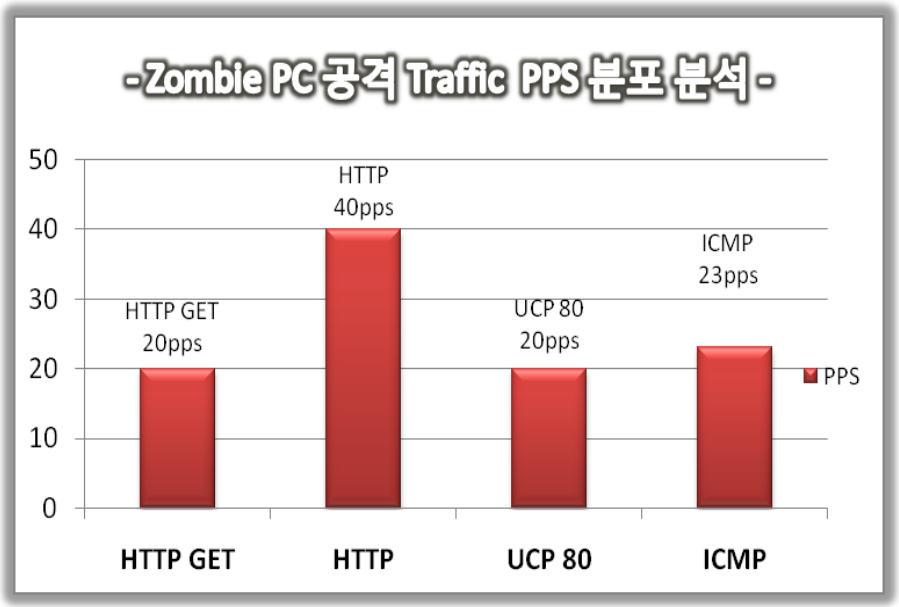
- Zombie PC 당 : 103pps , 18.5Kbyte/sec 전송
  - HTTP Get Flooding : 20pps , 12Kbyte/sec 전송
  - HTTP (TCP 80)Flooding : 40pps ,3.6Kbyte/sec 전송
  - UDP 80 Flooding : 20pps , 1.4Kbyte/sec 전송
  - ICMP Flooding : 23pps , 1.5Kbyte/sec 전송

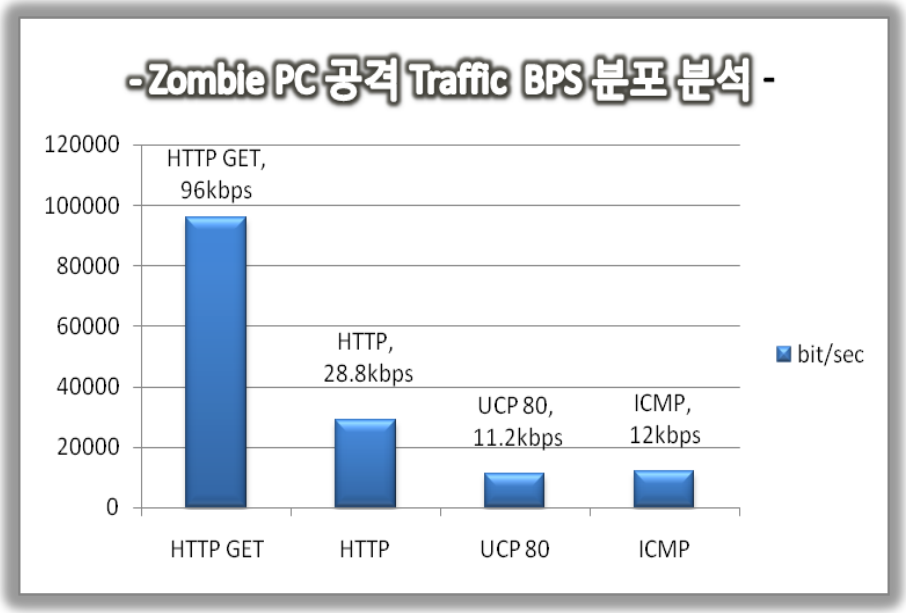
  - 안철수연구소 분석 결과 요약 -

특이 사항

- 대부분 국내 IP로 추정되며, 3만대의 IP는 지속적인 공격을 수행하는 것으로 보임
- A은행 Cisco Guard를 통한 Zombie 공격 시도 횟수 분석 결과
  – 3만대의 IP는 HTTP Getflooding을 매우 높은 횟수로 시도함
  - 대부분 국내 IP로 추정됨

7.7 DDoS Issue Summary
Zombie 분석

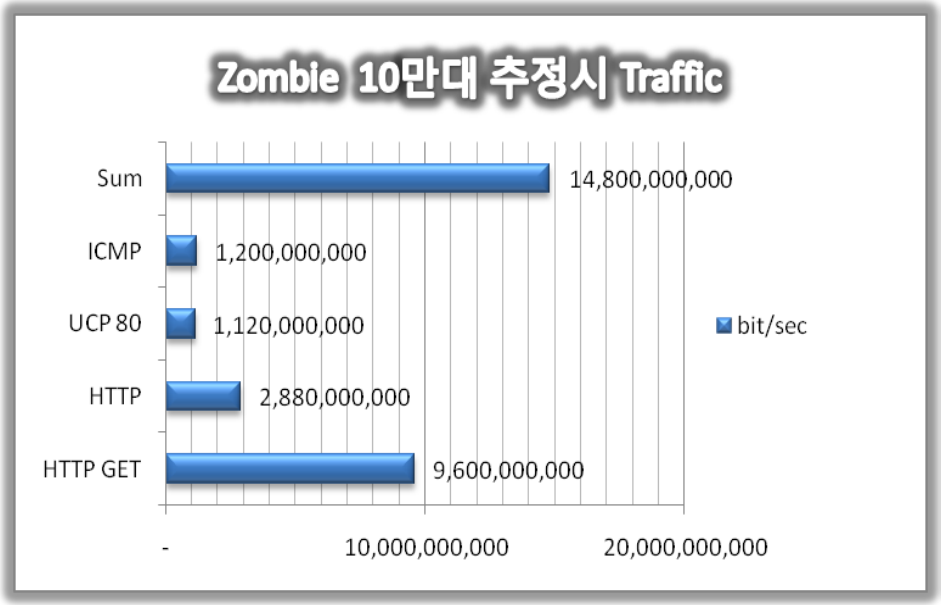


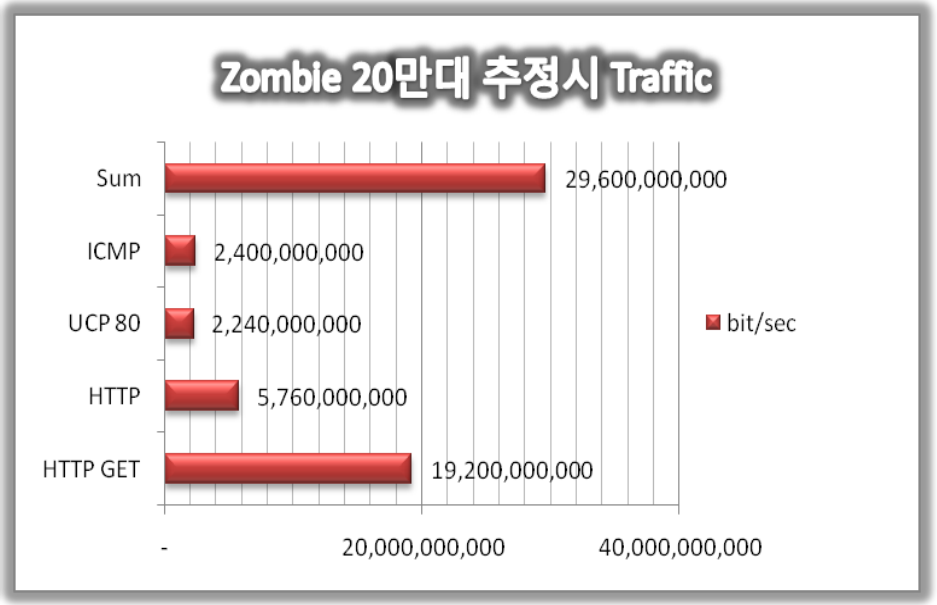


Zombie 분석 요약

1. **HTTP GET**
   - ① 일반적인 HTTP GET Flooding.
   - ② HTTP CC 공격 – 일반적인 CC Attack 유형이 포함 되어 있음.
2. **HTTP – TCP 80 으로 Connection Flooding**
3. **UDP 80 Flooding**
4. **ICMP Flooding**

7.7 DDoS Issue Summary
Zombie 분석에 따른 공격 트래픽 추정





Zombie Traffic 분석

1. Traffic Total Size
   - ① 2009.07.09 ~ 07.10 국내 공격지 분석 결과 Site 당 최대 2.x Gbps ~ 500Mbps 유지
     - Cisco Guard 분석 결과 (은행,포털 사이트)
   - ② Zombie 규모는 10만대 ~ 20만대 정도의 규모로 추정됨.
2. 특징
   - ① 공격 Site 수가 줄어 들 수록 , 공격지에 대한 Traffic의 크게 증가함.
   - ② 2009.07.09 이전에 공격 사이트의 피해 트래픽 보다 증가함.

7.7 DDoS 공격 상세 분석

7.7 DDoS 공격 특징

대규모 Zombie PC 와 Low level attack

1. 10만대 이상으로 추정되는 대규모 Zombie 의 Traffic.
2. Zombie PC의 Low level Size 공격으로 기존 시스템에서 탐지 어려움.

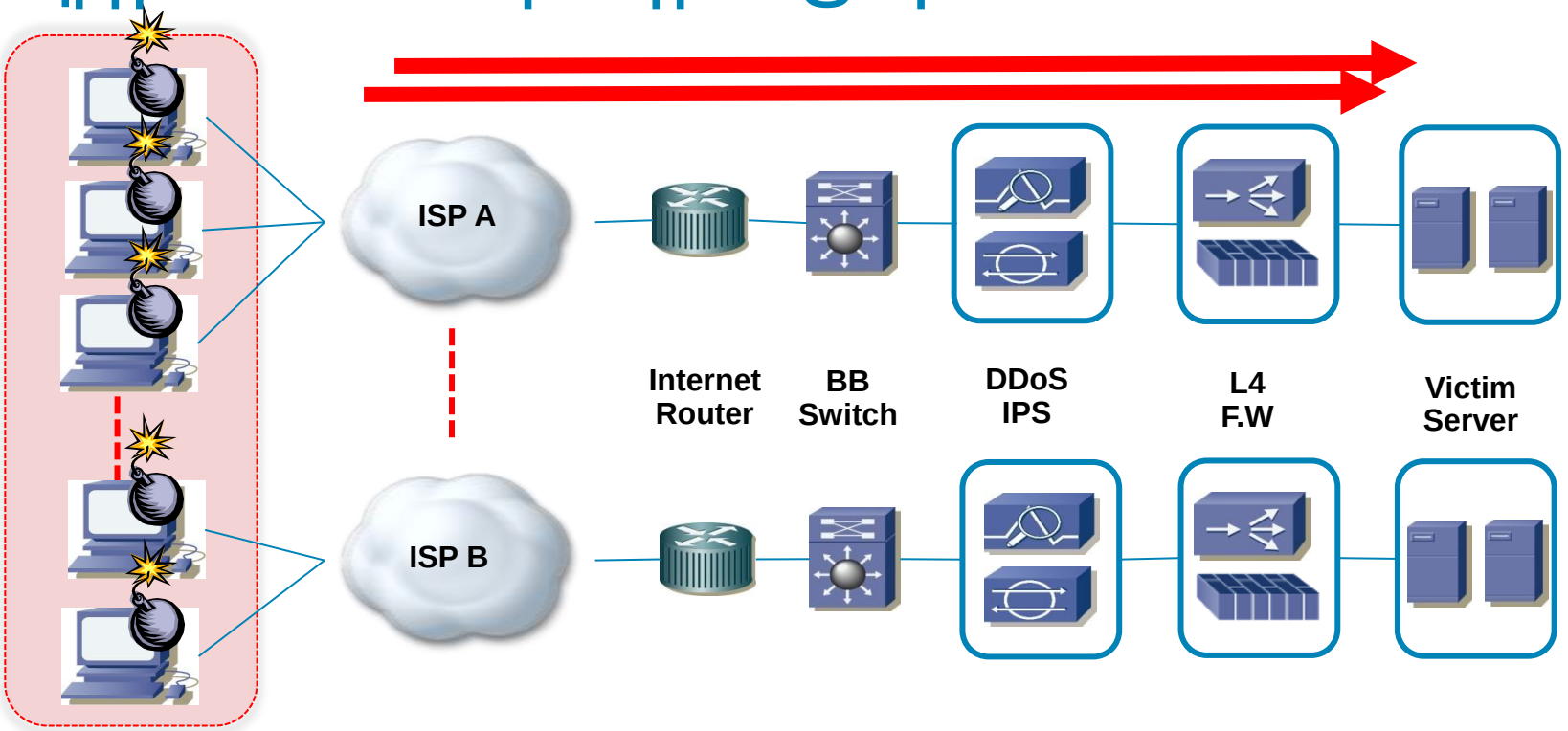
C&C Server가 없는 새로운 공격 형태

1. C&C Server가 없는 새로운 DDoS 공격 형태.
2. 추적 및 명령채널 차단이 어려워, 방어에 매우 어려움.

정교한 TCP/HTTP Attack

1. HTTP Get Flooding과 CC Attack을 혼합하여 공격

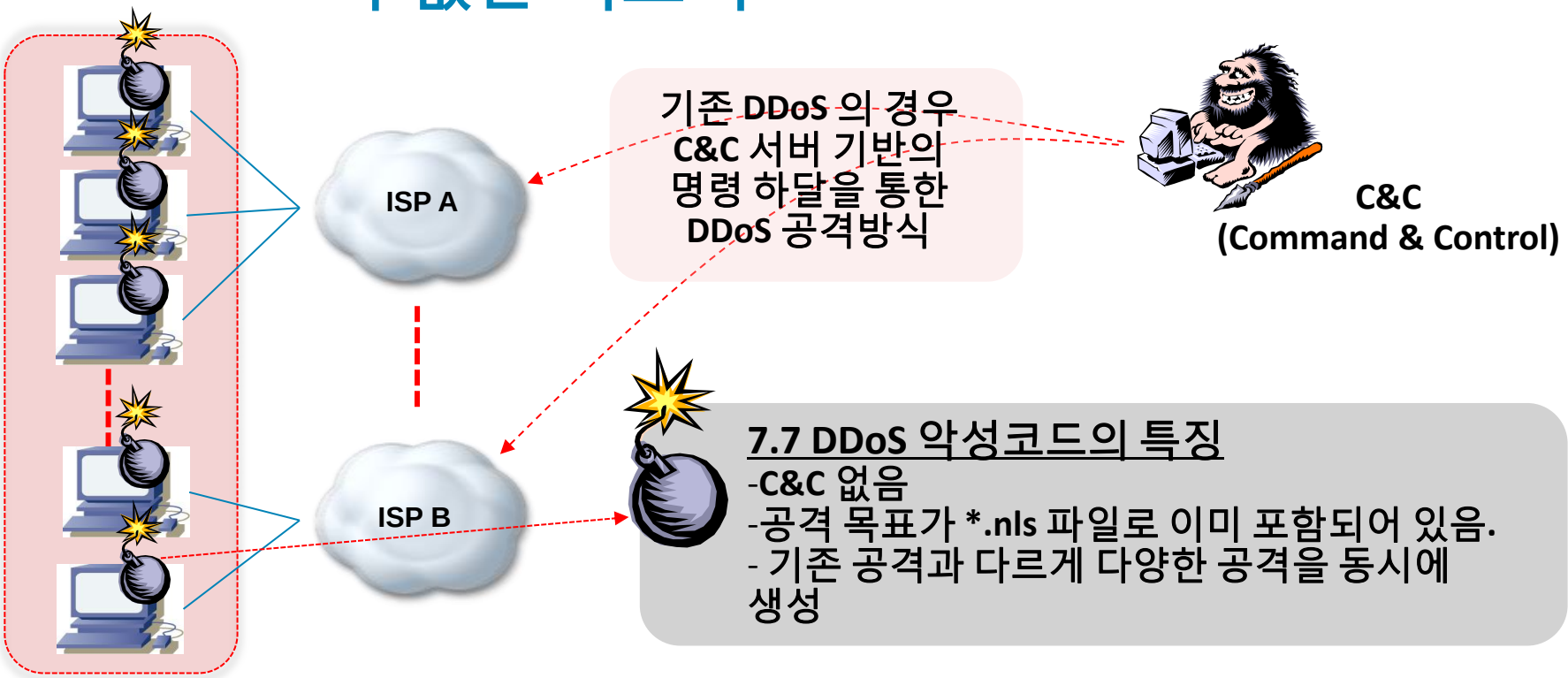
7.7 DDoS 공격 특징
대규모 Zombie와 소규모 공격



대규모 Zombie & 소규모 공격

1. **대규모 Zombie**
   ① 최소 수만대에서 최대 수십만대의 Zombie가 동원된 최대규모의 DDoS 공격
2. **소유모 공격**
   ① Zombie PC 당 매우 소량의 공격(100pps,1Mbps 이하)의 공격으로 기존 보안 장비를 우회하도록 구성됨
3. **실제 이러한 유형으로 인해 국내 1차 공격에 초기 대응이 늦어짐**

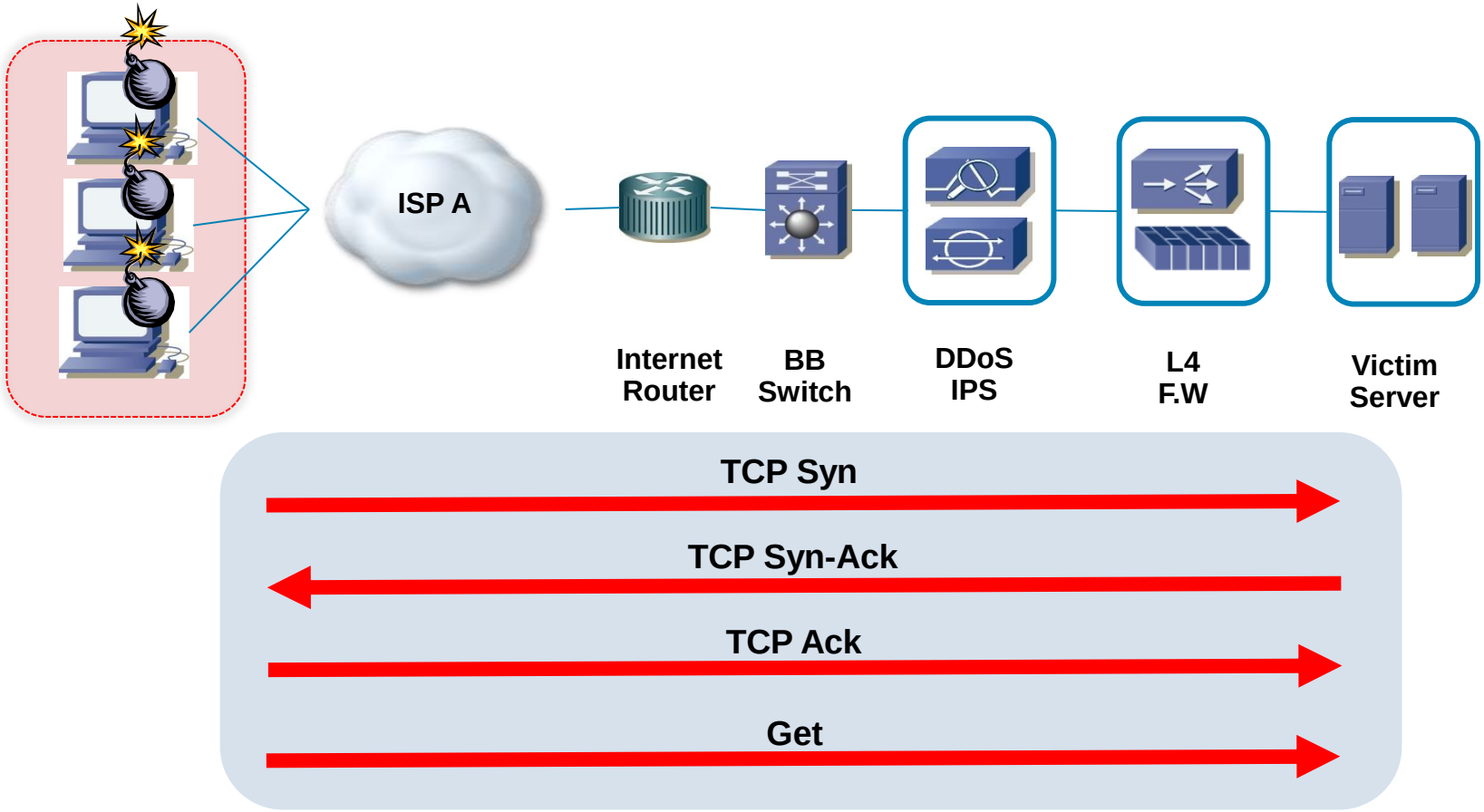
7.7 DDoS 공격 특징
C&C Server가 없는 최초의 DDoS



7.7 DDoS 공격의 특징

1. **C&C Server가 없는 공격 방식**
   ① C&C Server 가 없어서, 명령채널을 차단할 수 없는 DDoS 방식
2. **다양한 공격이 동시 발송**
   ① 4~5개 이상의 공격이 동시에 발송되는 특징을 띄고 있음
   ② **공격목표가 이미 *.nls 파일에 리스트를 담고 있음.**
   ③ **특정 날짜에 공격을 실행하도록 하고, 업데이트 함.**

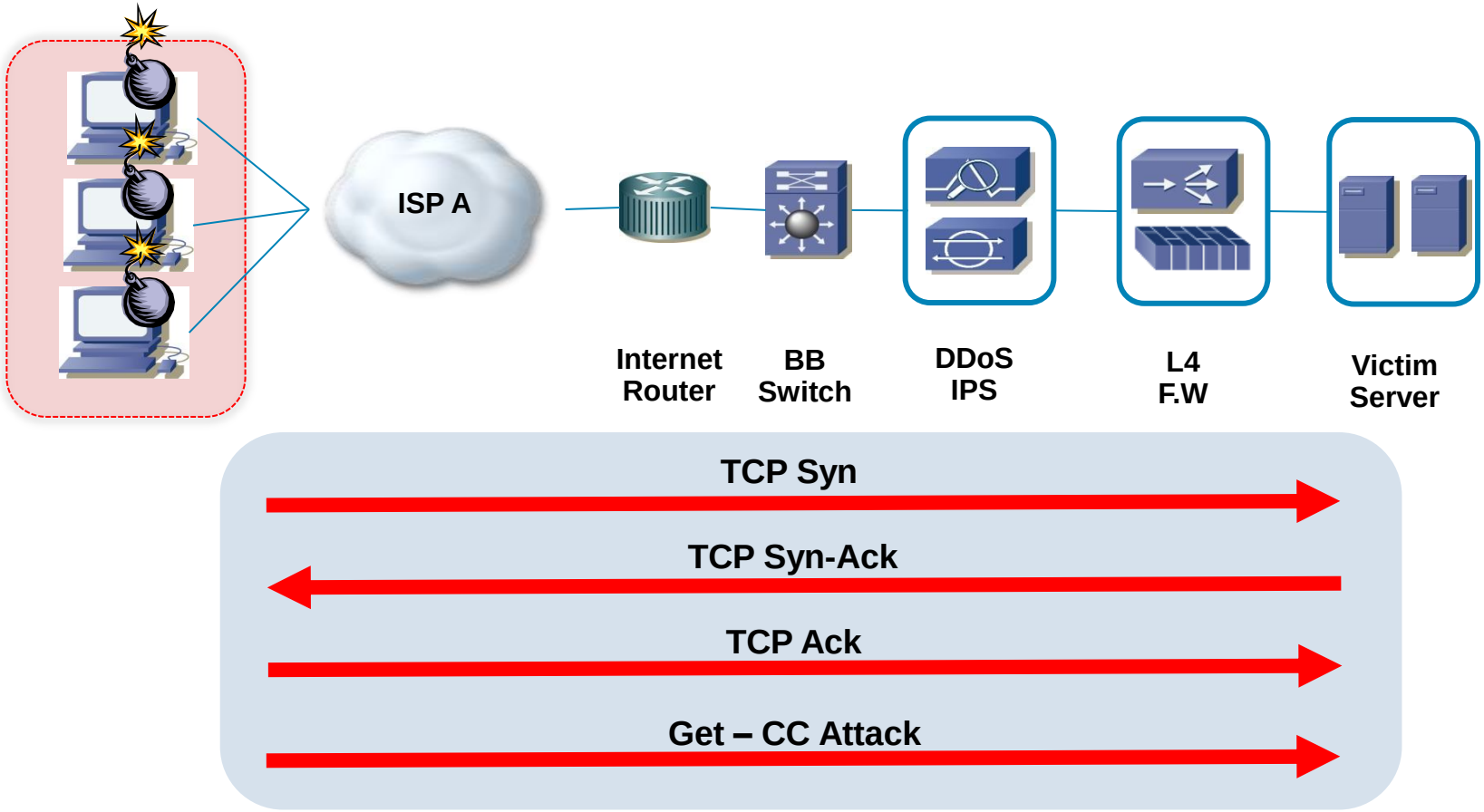
7.7 DDoS 공격 특징
정교한 TCP 공격 방식1



정교한 TCP HTTP 공격 방식

1. 매우 소량의 공격으로 보안 장비를 우회하는 방식
   ① 초당 40pps 미만의 TCP 80 공격 – TCP Syn Cookie에도 응답하는 방식 존재
   ② 초당 20pps 미만의 HTTP Get 공격 – Web Server의 부하 유발

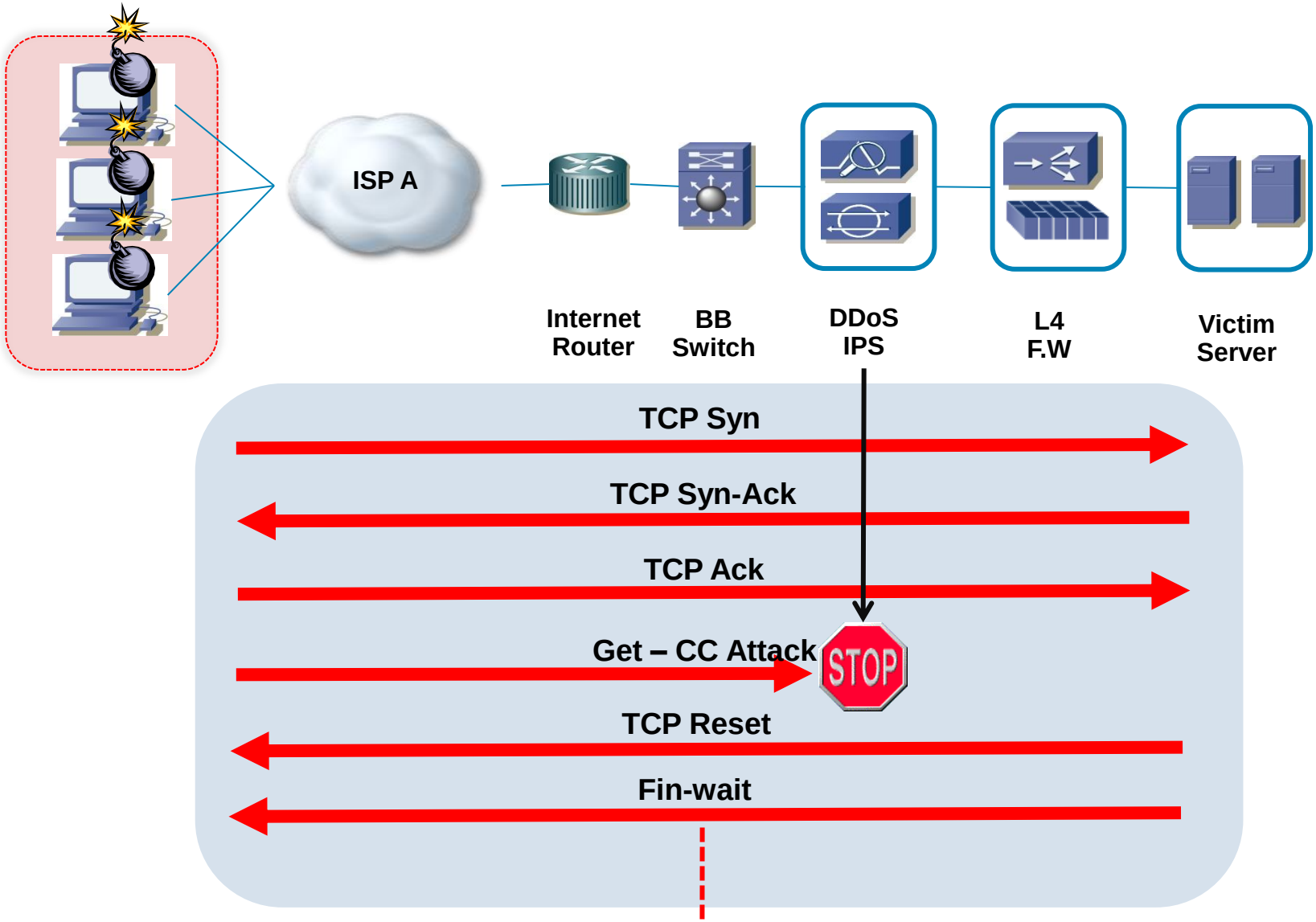
7.7 DDoS 공격 특징
정교한 TCP 공격 방식2 – HTTP CC Attack



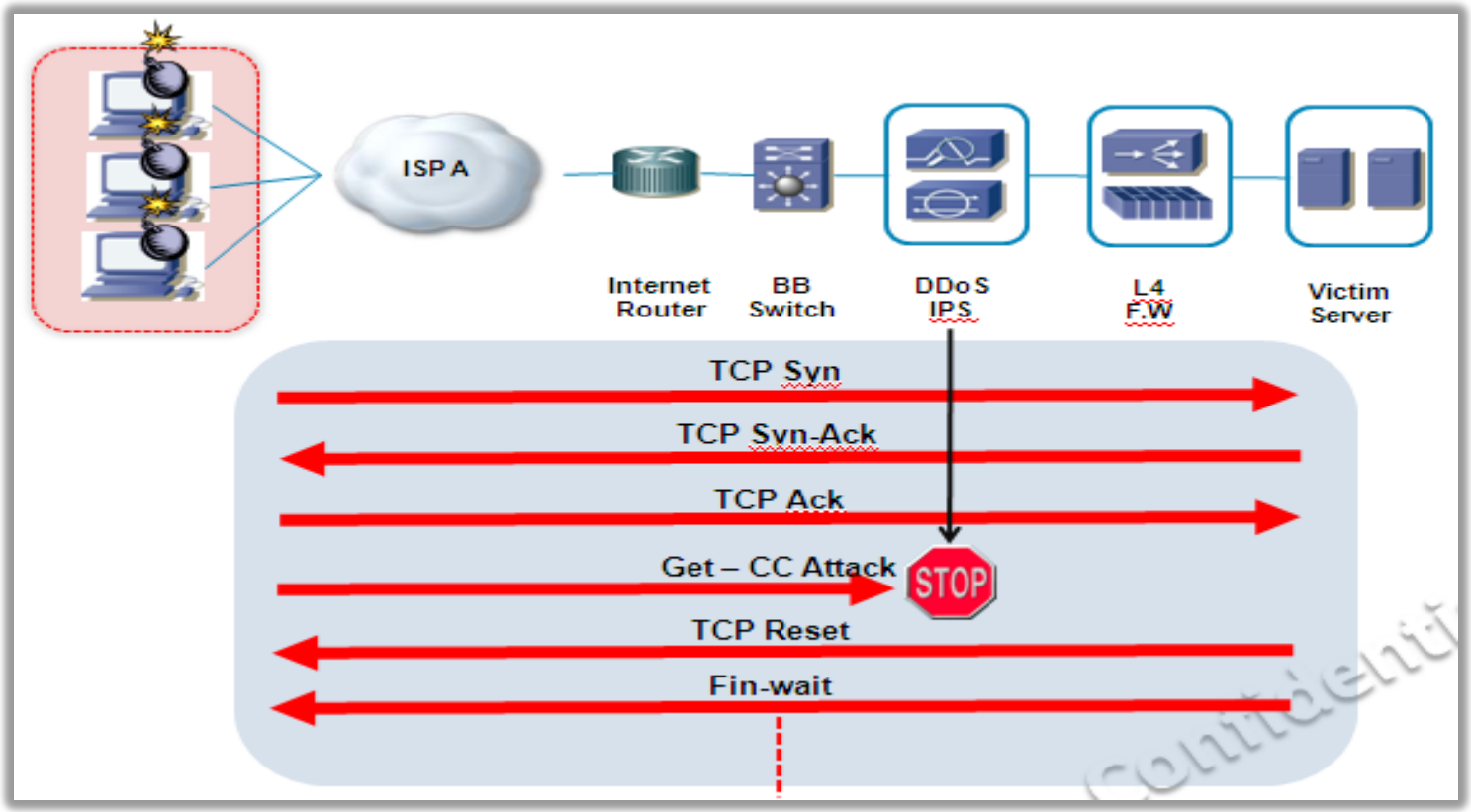
HTTP CC Attack

1. **HTTP CC Attack**
   - ① HTTP Get 내부에 CC Attack 정보 포함 공격
   - ② HTTP Get flooding과 동일한 증상이 발생하여, Victim Server Down

7.7 DDoS 공격 특징
정교한 TCP 공격 방식2 – HTTP CC Attack



7.7 DDoS 공격 특징
정교한 TCP 공격 방식2 – HTTP CC Attack

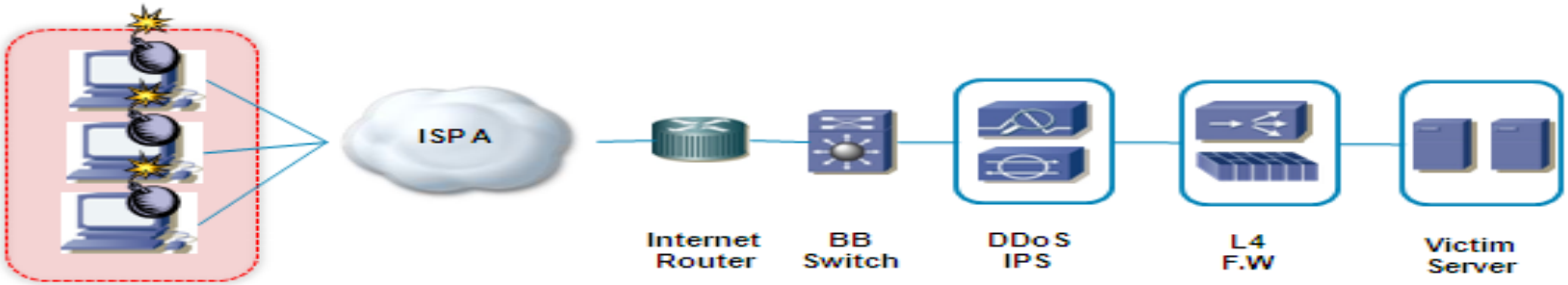


Signature 기반의 HTTP CC Attack 방어 시 발생하는 문제점.

1. **CC Attack 으로 인한 예기치 못한 사고 발생 가능성.**
   - ① CC Attack을 방어할 경우 Victim Server의 Fin-Wait 다량 발생으로, Victim Server,방화벽,L4 Switch 장애가 발생
   - ② CC Attack을 방어하지 않을 경우 HTTP Get Flooding으로 Server Down 하는 방식

7.7 DDoS Attack 방어 솔루션

7.7 DDoS 공격 방어 솔루션 Overview



Router/Switch

- 1Mpps 이상 처리 용량 장비로 구성 권고
- 적절한 ACL을 통한 사전 방어 필요
- Fragment 공격 차단 설정

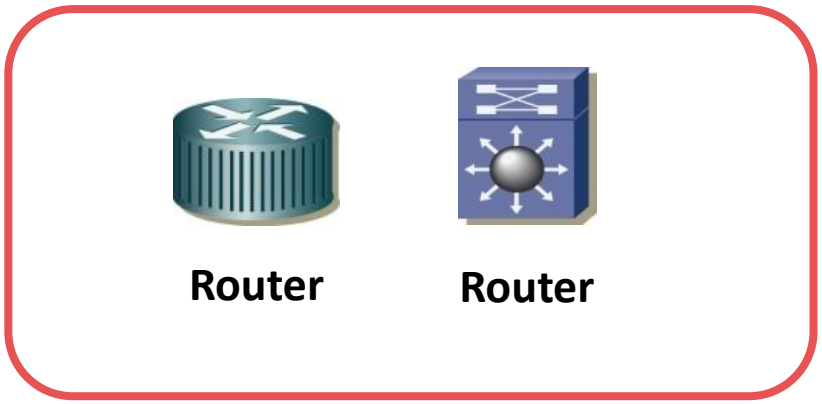
Cisco Guard/Detector

- Guard 기반의 정책 설정
- TCP Connection 정책 설정
- HTTP Syn 정책 설정
- HTTP Request 정책 설정
- HTTP Zomibe 메커니즘 설정
- Flex Filer 기반의 CC 공격 방어

Victim SVR

- GSLB 기반의 부하 분산 기법 설정
- SVR 보안 도구 설정

7.7 DDoS 공격 방어 솔루션
Router/Switch



1. **적절한 Network 장비 구성**
   - 고성능 Router/Switch

2. **Router/Switch ACL 설정**
   -불필요한 UDP Traffic Filter
   -불필요한 ICMP Traffic Filter
   -Fragment Attack Filter

Network 장비 기반의 ACL 설정

Cisco IOS 기반 Sample Config

```
ip access-list extended fragment
deny ip any any fragments
      ! UDP,ICMP fragment 우회를 방어하기 위한 Config
deny udp any any
      ! 불필요한 UDP Traffic 유입 방지
deny  icmp any any
      ! 불필요한 ICMP Traffic 유입 방지
permit ip any any
```

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

6가지 정책 설정에 앞서…

시스코 Guard 의 경우 기본적으로 Anti Spoofing 메커니즘으로, TCP Syn cookie에 의해 변조된 IP를 방어 수행한다.

다만, 금번 7.7 DDoS 공격의 경우 Zombie IP들이 TCP Syn Cookie 메커니즘에 동작하도록 구성되어 있으므로, 6가지의 추가적인 정책 Tuning을 통해 DDoS 공격에 적극방어 수행하도록 한다.

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – UDP/ICMP/Fragment Drop

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

1. UDP/ICMP/Fragment Drop 설정

Cisco Guard 기반의 Drop Policy 설정

user-filter 1 drop * * * fragments rate-limit 1 1 pps

! Fragment packet 이 특정 Src IP 에서 초당 1pps 이상 유입되면 Src IP의 트래픽 중 Fragment 만 Drop

user-filter 2 drop * 17 * no-fragments rate-limit 10 10 pps

! UDP packet 이 특정 Src IP 에서 초당 10pps 이상 유입되면 Src IP 의 트래픽 중 UDP만 Drop

user-filter 3 drop * 1 * no-fragments rate-limit 1 1 pps

! ICMP packet 이 특정 Src IP 에서 초당 1pps 이상 유입되면 Src IP 의 트래픽 중 ICMP만 Drop

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – UDP/ICMP/Fragment Drop

Cisco Guard

Cisco Detector

1. **UDP/ICMP/Fragment Drop 설정**
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

Src IP	Protocol	Dst Port	Fragments	Rate	Burst	Action	Rate (pps)
*	1	*	without			drop	0.00
*	17	80	without			drop	0.00
*	6	80	without			basic/redirect	205,365.00
*	6	8080	without			basic/redirect	0.00
*	6	8000	without			basic/redirect	0.00
*	6	8181	without			basic/redirect	0.00
*	6	8081	without			basic/redirect	0.00
*	6	3128	without			basic/redirect	0.00
*	6	53	without			basic/tcp-dns	0.00
*	6	25	without			basic/safe-reset	0.00
*	6	110	without			basic/safe-reset	0.00
*	6	143	without			basic/safe-reset	0.00
*	6	6667	without			basic/safe-reset	0.00
*	6	443	without			basic/safe-reset	0.00
*	6	*	without			basic/reset	0.00
*	17	5060	without			basic/sip	0.00

ICMP/UDP Traffic에 대해 Drop

Add Delete

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – TCP Connection 정책 설정


Cisco Guard


Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. **TCP Connection 정책 설정**
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

2. TCP Connection 정책 설정

Cisco Guard 기반의 Drop Policy 설정

policy tcp_connections_ns/any/basic/in_nodata_conns/src_ip 5.00 filter/drop 600 active 1 0

! TCP Connection 을 맺고 Data 가 전송되지 않는 Src IP에 대해 Drop
! 특정 Src IP 에서 초당 5pps Connection 을 맺는 불법 행위에 대해서만 Drop
! 해당 Rule 에 적용된 IP에 대해서는 600Sec간 정책 유지

TCP Connection Oriented 공격 방어에 매우 효과적 !!!

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – TCP Connection 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. **TCP Connection 정책 설정**
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

Home > Zone > Policies

Screen filter:

Path: tcp_connections/ * / * / * / * State: All Action: All

Policies: Current configuration Device: Guard Set screen

Src IP 당 TCP Connection 5pps 초과시 Drop

Config selection | Add service | Remove service | View Detector

	Policy Templ...	Service	Level	Type	Key	State	Action	Threshold	Proxy Th...	Thres...	Time...	Fixed	Learning ...	Detection T...
☐	tcp_connectio...	any	anal...	in_nodata_co...	global	▶	to-user-filters	945212.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	anal...	in_nodata_co...	src_ip	▶	to-user-filters	17884.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	basic	in_nodata_co...	global	▶	notify	945212.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	basic	in_nodata_co...	src_ip	▶	filter/drop	5.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	basic	num_sources	global	▶	redirect/zo...	7546.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	strong	in_conns	global	▶	notify	945594.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	strong	in_conns	src_ip	▶	filter/drop	200.0	170.0	0	600	✕	1.0	N/A
☐	tcp_connectio...	any	strong	in_nodata_co...	global	▶	notify	945212.0	0.0	-	600	✕	1.0	N/A
☐	tcp_connectio...	any	strong	in_nodata_co...	src_ip	▶	filter/drop	100.0	126.0	0	600	✕	1.0	N/A

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Syn 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. **HTTP Syn 정책 설정**
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

3. HTTP Syn 정책 설정

Cisco Guard 기반의 Drop Policy 설정

policy http/80/basic/syns/src_ip 5.00 filter/drop 600 active 1 0

! 특정 Src IP에서 TCP 80 포트로 TCP Flag Syn을 초당 5 pps 이상 보내면 Drop
! 해당 Rule 에 적용된 IP에 대해서는 600Sec간 정책 유지

TCP Connection Oriented 공격 방어에 매우 효과적 !!!

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Syn 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. **HTTP Syn 정책 설정**
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

Home > Zone > Policies

Screen filter:

Path: http/ * / * / * / *

Policies: Current configuration

State: All

Action: All

Set screen filter

Src IP 당 HTTP Syn 5pps 초과시 Drop

Config selection | Add service | Remove service | View Detector

Policy Templ...	Service	Level	Type	Key	State	Action	Threshold	Proxy Th...	Thres...	Time...	Fixed	Learning ...	Detection
http	80	anal...	syns_pph	src_ip		to-user-filters	5000.0	0.0	-	3600		1.0	
http	80	basic	pkts	dst_ip	▶	notify	89711.96	0.0	0	600		1.0	N
http	80	basic	pkts	global	▶	notify	95712.66	0.0	-	600		1.0	N
http	80	basic	pkts	src_ip	▶	filter/strong	4611.94	0.0	-	600		1.0	N
http	80	basic	reqs	dst_ip	▶	notify	29610.66	0.0	0	600		1.0	N
http	80	basic	reqs	global	▶	notify	29609.66	0.0	-	600		1.0	N
http	80	basic	reqs	src_ip	▶	filter/drop	20.0	0.0	-	600		1.0	N
http	80	basic	reqs_pph	src_ip		filter/strong	5000.0	0.0	-	3600		1.0	
http	80	basic	syns	dst_ip	▶	notify	64888.54	0.0	0	600		1.0	N
http	80	basic	syns	global	▶	notify	64888.54	0.0	-	600		1.0	N
http	80	basic	syns	src_ip	▶	filter/drop	5.0	0.0	-	600		1.0	N
http	80	basic	syns_pph	src_ip		filter/strong	5000.0	0.0	-	3600		1.0	
http	80	strong	http_reqs	dst_ip	▶	notify	29584.0	0.0	0	600		1.0	N

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Request 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. **HTTP Request 정책 설정**
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

4. HTTP Request 정책 설정

Cisco Guard 기반의 Drop Policy 설정

policy http/80/basic/reqs/src_ip 20.00 filter/drop 600 active 1 0

! 특정 Src IP에서 HTTP Request 패킷을 초당 20 pps 이상 전송할 경우 해당 Src IP Drop
! 해당 Rule 에 적용된 IP에 대해서는 600Sec간 정책 유지

HTTP Get Flooding 공격 방어에 매우 효과적 !!!

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Request 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. **HTTP Request 정책 설정**
5. HTTP Zombie 정책 설정
6. Flex Filter 설정

Src IP 당 HTTP Request 20pps 초과시 Drop

Home > Zone > Policies

Screen filter:

Path: http/*/*/*/* State: All Action: All

Policies: Current configuration Device: Guard

Set screen filter

Config selection | Add service | Remove service | View Detector

Policy Templ...	Service	Level	Type	Key	State	Action	Threshold	Proxy Th...	Thres...	Time...	Fixed	Learning ...	Detection
http	80	anal...	syns_pph	src_ip	⏻	to-user-filters	5000.0	0.0	-	3600	×	1.0	
http	80	basic	pkts	dst_ip	▶	notify	89711.96	0.0	0	600	×	1.0	N
http	80	basic	pkts	global	▶	notify	95712.66	0.0	-	600	×	1.0	N
http	80	basic	pkts	src_ip	▶	filter/strong	4611.94	0.0	-	600	×	1.0	N
http	80	basic	reqs	dst_ip	▶	notify	29610.66	0.0	0	600	×	1.0	N
http	80	basic	reqs	global	▶	notify	29609.66	0.0	-	600	×	1.0	N
http	80	basic	reqs	src_ip	▶	filter/drop	20.0	0.0	-	600	×	1.0	N
http	80	basic	reqs_pph	src_ip	⏻	filter/strong	5000.0	0.0	-	3600	×	1.0	
http	80	basic	syns	dst_ip	▶	notify	64888.54	0.0	0	600	×	1.0	N
http	80	basic	syns	global	▶	notify	64888.54	0.0	-	600	×	1.0	N
http	80	basic	syns	src_ip	▶	filter/drop	5.0	0.0	-	600	×	1.0	N
http	80	basic	syns_pph	src_ip	⏻	filter/strong	5000.0	0.0	-	3600	×	1.0	
http	80	strong	http_reqs	dst_ip	▶	notify	29584.0	0.0	0	600	×	1.0	N

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Zombie 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. **HTTP Zombie 정책 설정**
6. Flex Filter 설정

5. HTTP Zombie 정책 설정

Cisco Guard 기반의 Drop Policy 설정

policy tcp_connections/any/basic/num_sources/global 500.00 redirect/zombie 600 active 1 0

! Web Server로 초당 1000 개 이상의 Client 가 접속 요청시, 정상적인 Web Browser가 동작하는지 검증
! 해당 Rule 에 적용된 IP에 대해서는 600Sec간 정책 유지

공격자가 정상적인 Web Browser를 실행하고 있는 지 1차 검증하여, Filtering 하는 데 매우 효과적!!

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Zombie 정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. **HTTP Zombie 정책 설정**
6. Flex Filter 설정

Victim으로 Src IP 가 동시 500개 이상 Web 요청시 HTTP Cookie 검증

Home > Zone > Policies

Screen filter:

Path: tcp_connections/ * / * / * / *

Policies: Current configuration

State: All Action: A

Device: Guard

Set screen

Config selection | Add service | Remove service | View Detector

Policy Templ...	Service	Level	Type	Key	State	Action	Threshold	Proxy Th...	Thres...	Time...	Fixed	Learning ...	Detection T...
tcp_connectio...	any	anal...	in_nodata_co...	global	▶	to-user-filters	945212.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	anal...	in_nodata_co...	src_ip	▶	to-user-filters	17884.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	basic	in_nodata_co...	global	▶	notify	945212.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	basic	in_nodata_co...	src_ip	▶	filter/drop	5.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	basic	num_sources	global	▶	redirect/zo...	500	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	strong	in_conns	global	▶	notify	945594.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	strong	in_conns	src_ip	▶	filter/drop	200.0	170.0	0	600	×	1.0	N/A
tcp_connectio...	any	strong	in_nodata_co...	global	▶	notify	945212.0	0.0	-	600	×	1.0	N/A
tcp_connectio...	any	strong	in_nodata_co...	src_ip	▶	filter/drop	100.0	126.0	0	600	×	1.0	N/A

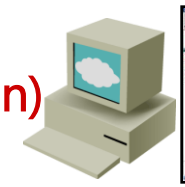
7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – HTTP Zombie 정책 설정

IP 192.168.1.1

Client (Source)

Guard (Scrubber)

Zone (Destination)



SYN
(SrcIP=192.168.1.1;seq=x)

SYN ACK
(seq=cookie;ack=x+1)

ACK
(seq=x+1;ack=cookie+1)

GET
(http://www.cisco.com)

Fin+Refresh
URL=cookie

TCP 검증 프로세스

HTTP code= 302
SYN

SYN ACK

ACK
GET URL = Cookie

Fin+Refresh
URL=orig URL

Guard 기반의 HTTP Cookie 검증

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – Flex Filter정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. **Flex Filter 설정**

No.	Time	Source	Destination	Protocol	Info
123	1.076804			HTTP	GET /shop/big_section.php?cno1=1009 HTTP/1.1
127	1.076817			HTTP	GET /shop/big_section.php?cno1=1009 HTTP/1.1
130	1.076826			HTTP	GET /shop/big_section.php?cno1=1009 HTTP/1.1
131	1.077800			HTTP	GET /shop/big_section.php?cno1=1009 HTTP/1.1

```
⊞ Frame 15 (287 bytes on wire, 287 bytes captured)
⊞ Raw packet data
⊞ Internet Protocol, Src:                                  ), Dst:                    )
⊞ Transmission Control Protocol, Src Port: 1101 (1101), Dst Port: http (80), Seq: 0, Ack: 0, Len: 247
⊟ Hypertext Transfer Protocol
  ⊟ GET /shop/big_section.php?cno1=1009 HTTP/1.1\r\n
      Request Method: GET
      Request URI: /shop/big_section.php?cno1=1009
      Request Version: HTTP/1.1
    Host:                    \r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; MyIE 3.01)Cache-Control: no-store, must-revalidate\r\n
    Referer: http://                    \r\n
    Connection: Close\r\n
    \r\n
```

CC Attack의 경우

User Agent filed에 Cache-Control: no-store, must-revalidate를 추가 시킴.

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – Flex Filter정책 설정

Cisco Guard

Cisco Detector

1. UDP/ICMP/Fragment Drop 설정
2. TCP Connection 정책 설정
3. HTTP Syn 정책 설정
4. HTTP Request 정책 설정
5. HTTP Zombie 정책 설정
6. **Flex Filter 설정**

Flex-Content Filter Form

Description: CC Attack

Protocol: 6 Dst Port: 80

Expression: Protocol : TCP Port : HTTP 80

Pattern: Cache-Control: no-store, must-revalidate Match Case

Start Offset: 0 End Offset:

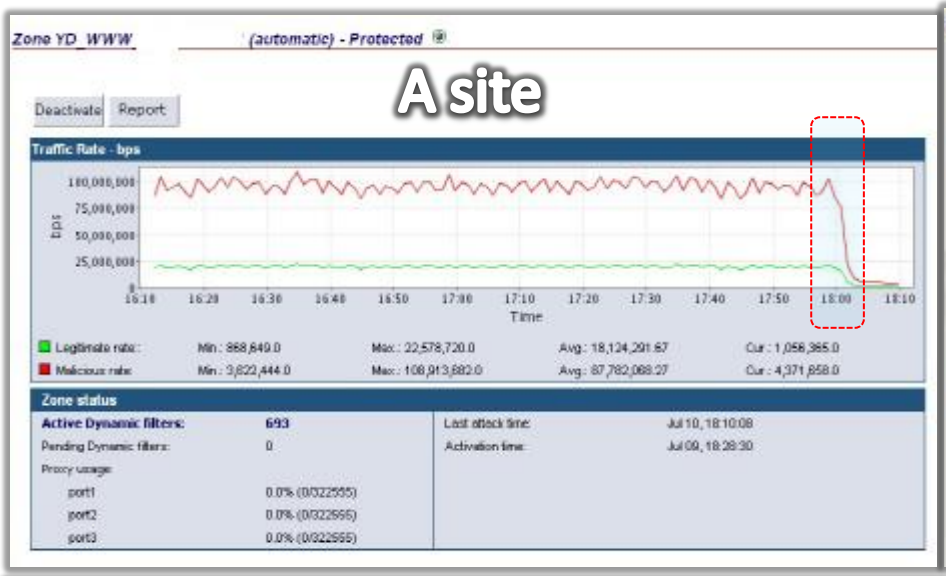
Action: drop

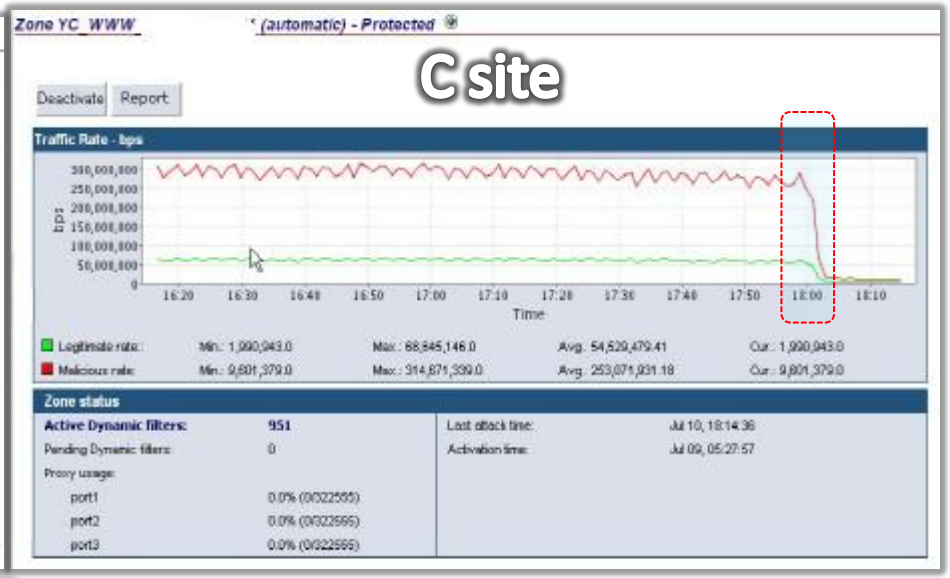
State: Enable

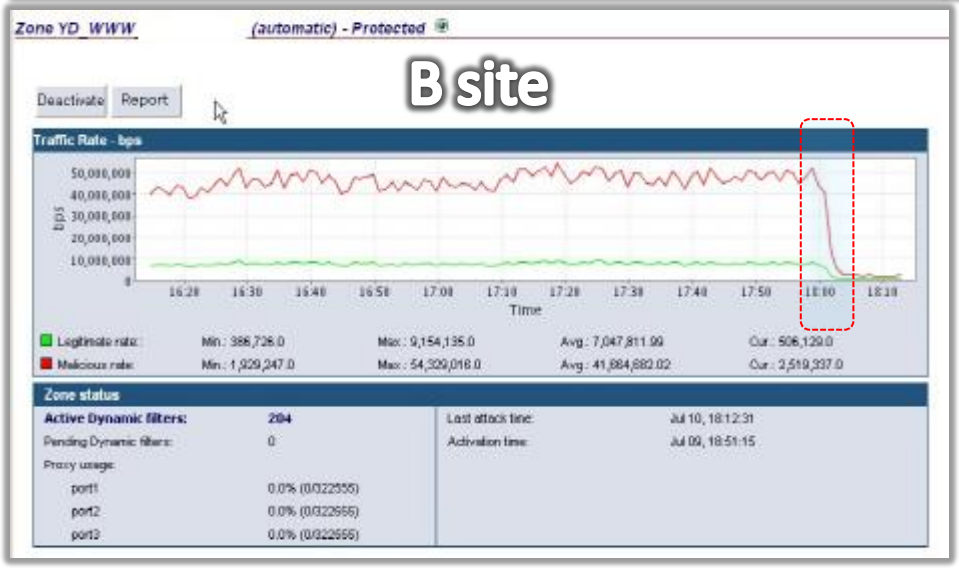
OK Clear Cancel

Cache-Control: no-store, must-revalidate
문자열에 대한 필터링 선언

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – 7.7 DDoS 공격방어 실제사례







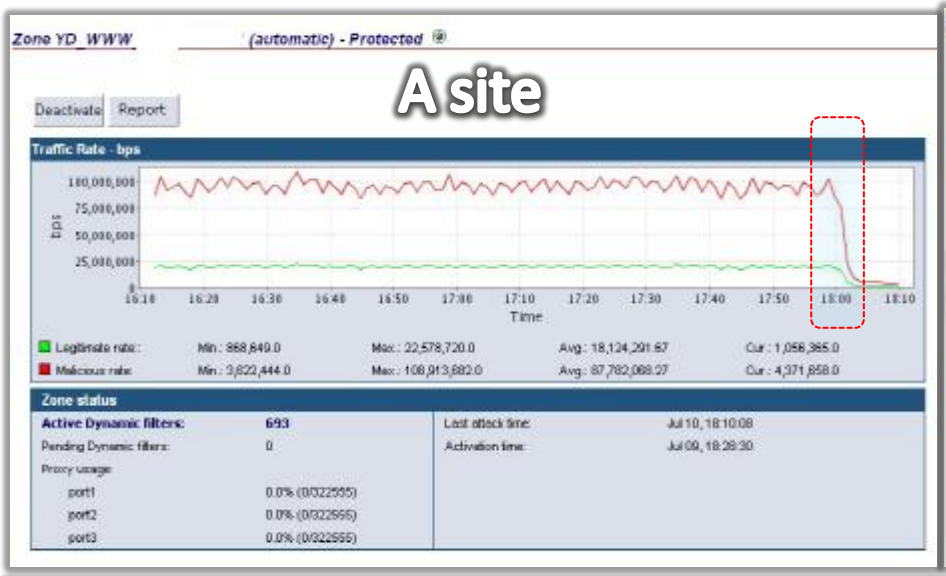
7월 9일 ~ 10일 피해 시스템 실제 사례

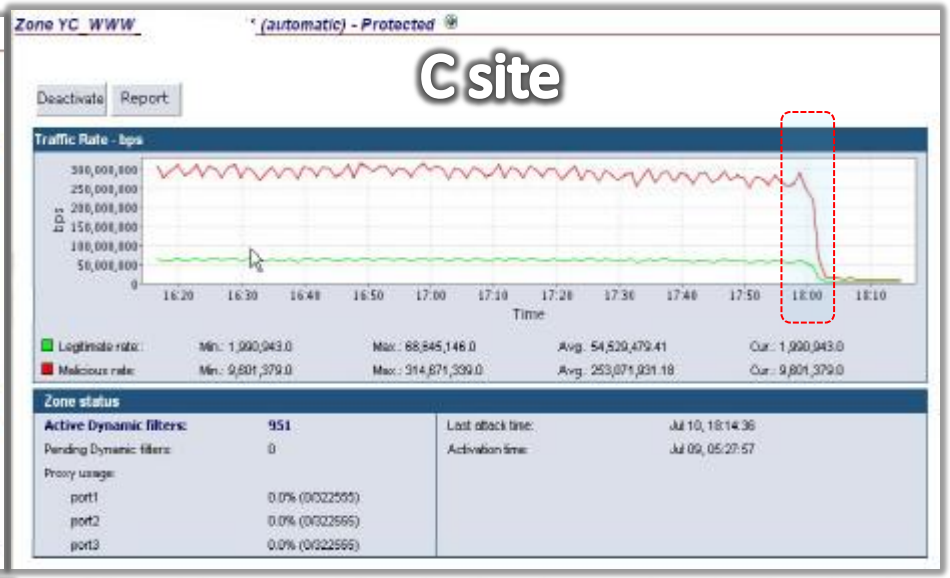
최대 **2.5Gbps** 공격 유입

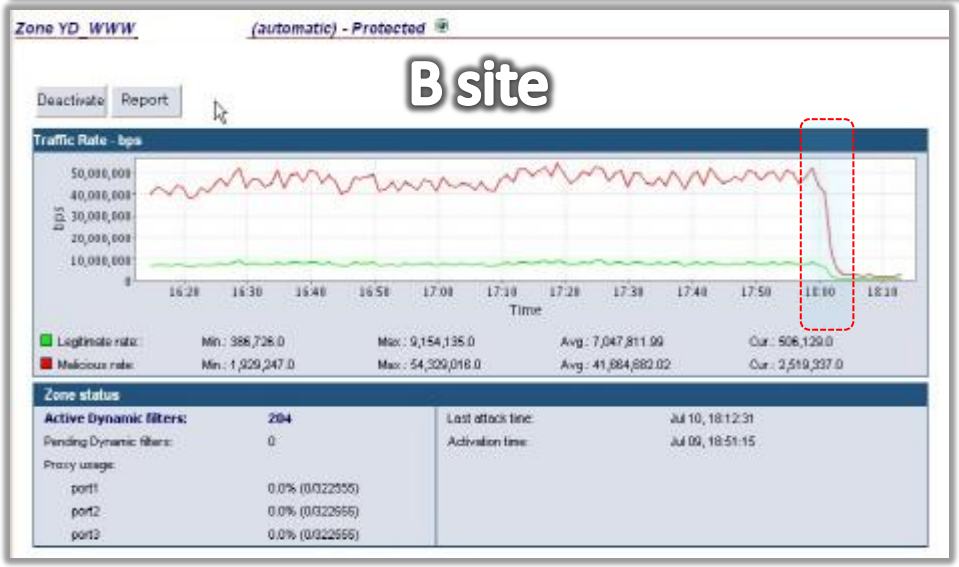
7월 9일 저녁 8시 기점 – 500Mbps 공격 꾸준히 유지
Cisco Guard Filtering 기반으로 정상 서비스 유지

Guard 기반의 좀비 **List 18만대** 확보
→ 보안 기관,업체,**ISP** 공유

7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – 7.7 DDoS 공격방어 실제사례







7월 9일 ~ 10일 피해 시스템 실제 사례

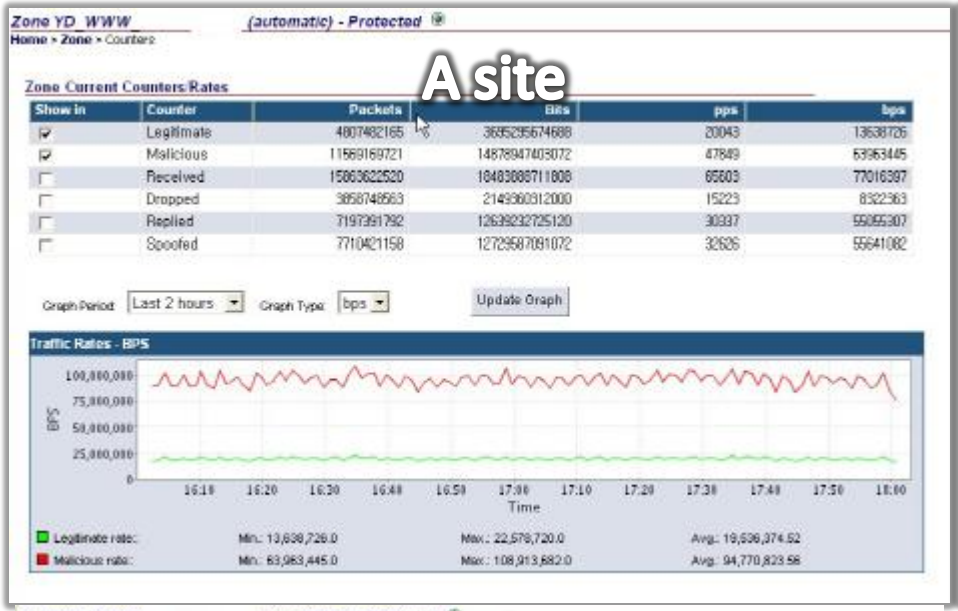
최대 **2.5Gbps** 공격 유입

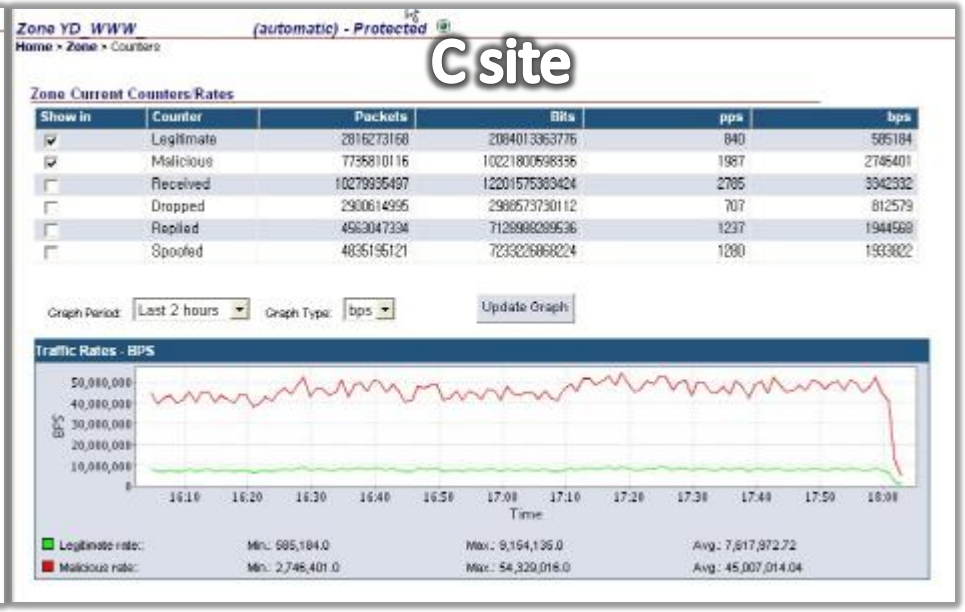
7월 **9**일 저녁 **8**시 기점 – **500Mbps** 공격 꾸준히 유지
Cisco Guard Filtering 기반으로 정상 서비스 유지

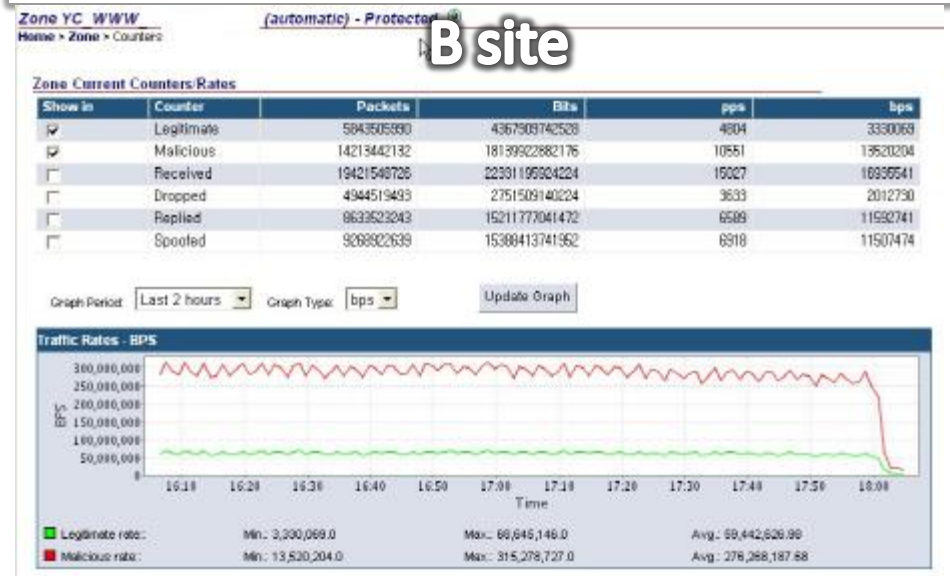
Guard 기반의 좀비 **List 18**만대 확보
→ 보안 기관,업체,**ISP** 공유

7.7 DDoS 공격 방어 솔루션

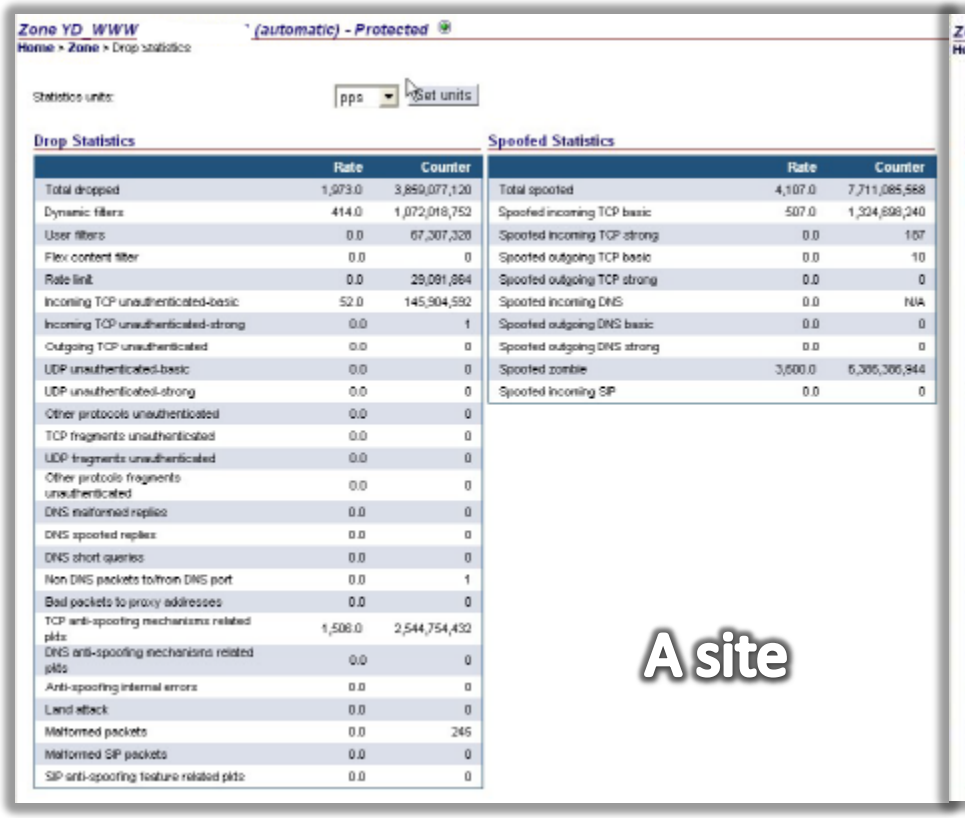
Cisco Guard/Detector – 7.7 DDoS 공격방어 실제사례

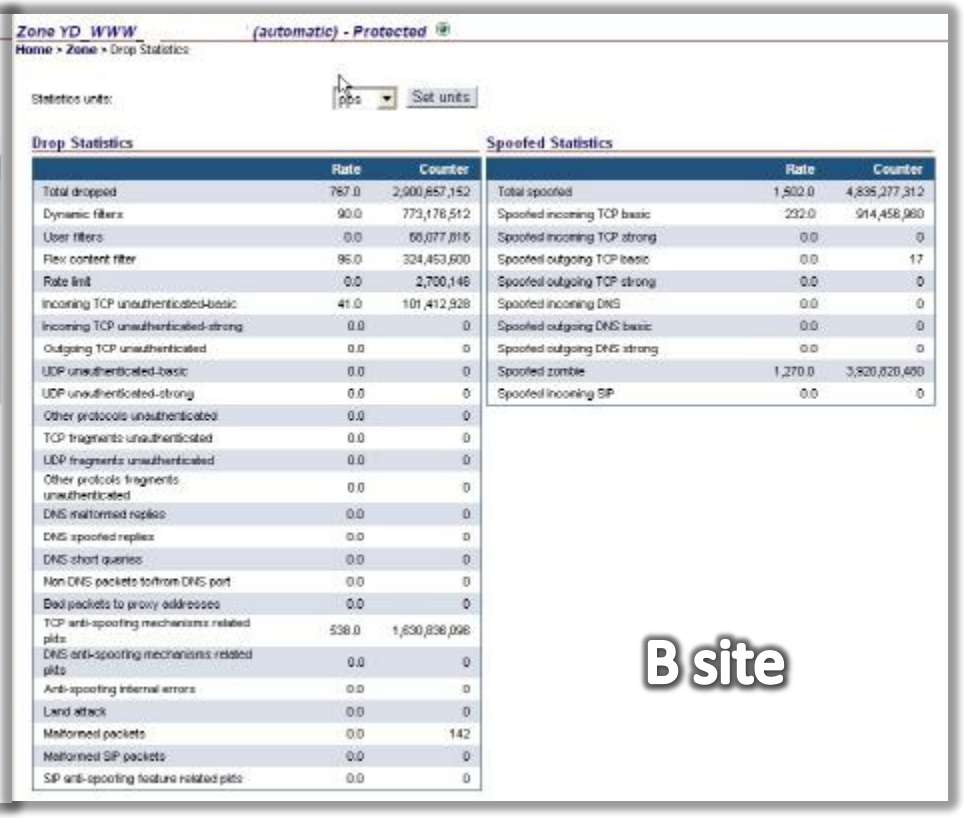






7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – 7.7 DDoS 공격방어 실제사례





7.7 DDoS 공격 방어 솔루션
Cisco Guard/Detector – 7.7 DDoS 공격방어 실제사례

1. 공공,언론 기관–3개 기관 지원
   - 3개 사이트 모두 긴급 장비 투입 지원
2. 포털 사이트–3개 기업 구성 지원
   - 1개 사이트 탐지 모드 동작
   - 1개 사이트 탐지/방어 서비스 지원
   - 1개 사이트 탐지/방어 구성 후 DDoS 공격 대비
3. 금융권–5개 은행 구성 지원
   - 4개 은행 탐지/방어 서비스 지원
   - 1개 은행 긴급 장비 투입 지원

왜 Cisco Guard & Detector 입니까?

1. HTTP에 가장 정교하게 방어할 수 있는 솔루션

2. 가장 많은 경험과 노하우 … 그리고 지원체계

3. Out Of Path 기반의 탁월한 DDoS 방어 디자인

4. 대용량 설계기반을 통한 높은 성능

5. 검증된 솔루션 – 국내 70여개의 대형 레퍼런스


CISCO