

WAPPLES SA 운영 방안

펜타시큐리티시스템 웹보안부

- I. X-Forwarded-For
- II. Proxy by DNS lookup 기능
- III. Multi domain nat 기능
- IV. Sync(다중 동기화) 기능

WAPPLES SA 운영 방안

I. X-Forwarded-For

1. Proxy 환경에서의 Client ip

- 1) 클라우드 환경에서는 Proxy 동작으로 인해 대부분 앞단 장비의 IP가 소스 IP가 됨
- 2) HTTP request header filed 중 X-Forwarded-for를 확인하여 client IP 확인 가능



A. Block by X-Forwarded-for IP

- ① 설정 ON이면, HttpDoS와 IP Block에 한해서 누적 IP를 X-Forwarded-For 헤더의 IP를 보고 counting
- ② 누적치가 설정된 값에 부합하게 되면 X-Forwarded-For 헤더의 IP를 보고 해당 IP만 탐지엔진에서 Block
- ③ 만약 X-Forwarded-For IP Header가 없다면, Block되지 않음

B. Detect by X-Forwarded-for IP

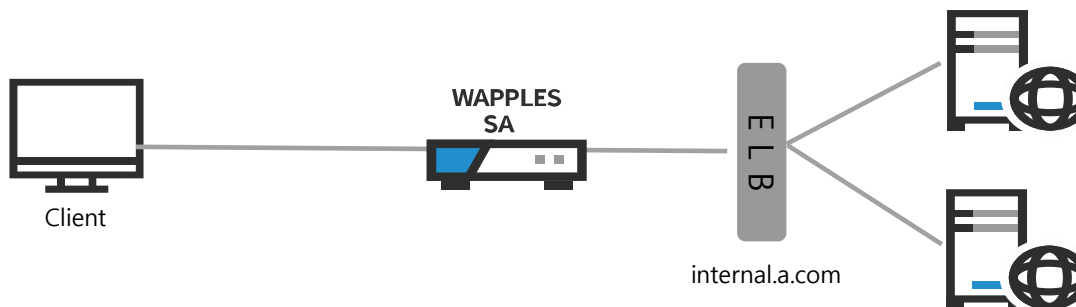
- ① 설정 ON이면, "UriAccessControl 신뢰하는 IP, 예외설정, AccessControl, Suspicious Bot ip 판단기준, IP Filtering, Unlogging 기능, IP Block 위험도별, IP Block 지연 패킷"에 대해 Client IP가 실제 들어온 Network IP가 아닌, X-Forwarded-For IP로 검사
- ② 만약 X-Forwarded-For Header가 없다면, Network IP 그대로 검사

WAPPLES SA 운영 방안

II. Proxy by DNS lookup 기능

1. 개요

- 1) 클라우드 환경에서는 웹 서버의 고정 IP가 DHCP인 경우가 대부분
- 2) 웹 서버 혹은 Internal LB에서 IP가 아닌 Domain을 가지고 있음
- 3) WAPPLES 웹 서버 설정에서 IP 설정이 아닌, 도메인으로 설정 가능
- 4) WAPPLES은 DNS기반 통신하여, 능동적으로 Domain 에 맞춰 filter를 갱신 할 수 있도록 기능 개발



A. 이경우 WAPPLES의 웹서버는 internal.a.com으로 설정

B. DNS 예시

▼ 인스턴스 요약 정보		
인스턴스 ID i-0ef5a50ed00335ab (3.server1_안랩)	퍼블릭 IPv4 주소 3.34.44.6 개방 주소법	프라이빗 IPv4 주소 172.31.29.15
인스턴스 상태 실행 중	퍼블릭 IPv4 DNS ec2-3-34-44-6.ap-northeast-2.compute.amazonaws.com 개방 주소법	프라이빗 IPv4 DNS ip-172-31-29-15.ap-northeast-2.compute.internal
인스턴스 유형 m4.large	탄력적 IP 주소 -	VPC ID vpc-0395776a

WAPPLES SA 운영 방안

II. Proxy by DNS lookup 기능(계속)

2. 설정 방법

- 1) 보호대상 IP 입력하는 부분에 도메인 명 입력
- 2) Proxy 모드일 경우에만 도메인명 입력 가능, Proxy 모드가 아닌 경우 IP 형식만 입력 가능
- 3) DNS Query를 통해 얻어진 결과값은 dnat-ip 에서 관리됨

서버 모드

Inline Proxy T.Proxy 단일 호스트 LB 다중 호스트 LB

프록시 IP 172.31.31.132

프록시 포트 80

단일 다중

웹 서버 IP ip-172-31-29-15.ap-northeast-2.compute.internal

웹 서버 포트 80

헬스 체크 사용 안 함

```
pentasec@ip-172-31-31-132:(dpi)# show filter
Session Filter Info
40000 - TCP 000.000.000.000[000.000.000.000]:00000/00000 => 172.031.031.132[255.255.255.255]:00080/00080 - NAT<400
00> DETECT ENABLE
L 40000 - NAT-TYPE(DOMAINNAME_DNAT) snat_ip(172.031.031.132) domainName(ip-172-31-29-15.ap-northeast-2.
compute.internal) dnat_port(00080)
pentasec@ip-172-31-31-132:(dpi)# show nat
Session Nat Info
40000 - NAT-TYPE(DOMAINNAME_DNAT) snat_ip(172.031.031.132) hostname(none) domainName(ip-172-31-29-15.ap-northeast-2.c
ompute.internal) health_check_type(none) dnat_port(00080) gw_ip(172.031.016.001) gw_ip_mac(0a:19:fd:0d:b5:21) local_
ip(000.000.000.000) localMacEnable(DISABLE) sspi->count(55001) ref_cnt(1) lb(NONE)
L 40000 - dnat_ip(172.031.029.015) dnat_mac(00:00:00:00:00:00) ref_count(0) will_del(NO_DEL) status(up) type(dy
namic) hashkey(544530754244222016) weight(0)
pentasec@ip-172-31-31-132:(dpi)# show dnat-ip
40000 - Selected-IP(172.031.029.015) count(1)
L 40000 - dnat_ip(172.031.029.015) dnat_mac(00:00:00:00:00:00) ref_count(0) will_del(NO_DEL) status(up) type(dy
namic) hashkey(544530754244222016) weight(0)
pentasec@ip-172-31-31-132:(dpi)#
```

WAPPLES SA 운영 방안

II. Proxy by DNS lookup 기능(계속)

3. 동작 방식

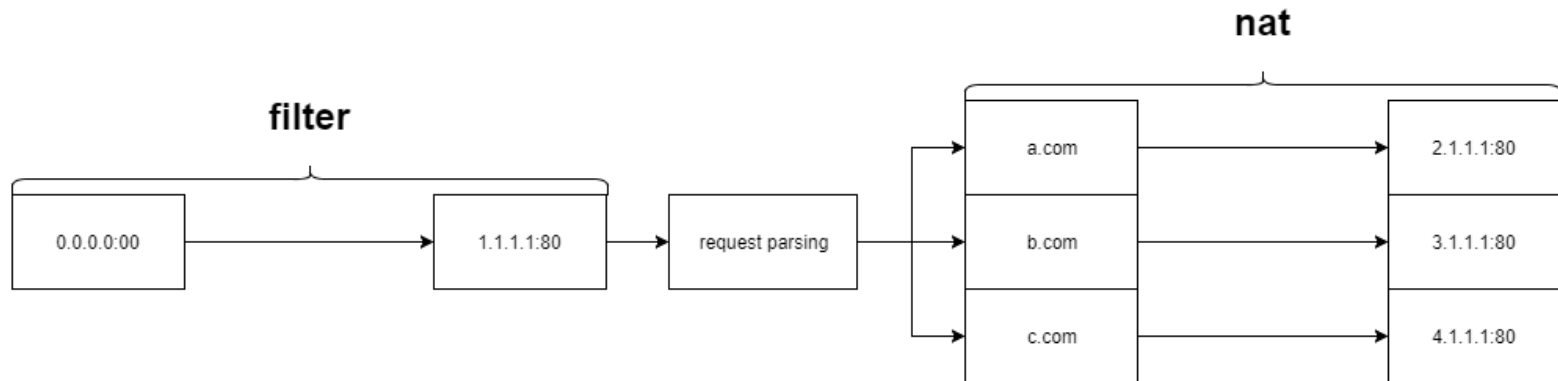
- 1) NAT 필터에 있는 Domain 을 DNS Query 요청을 한다.
- 2) 여러 개의 DNS가 있는 경우
 - 1) 헬스체크 선택한 경우 : 선택한 헬스체크 방식으로 health check 진행 후 Selected IP 선정
 - 2) 헬스체크 선택하지 않은 경우 : 쿼리 응답이 온 IP를 그대로 선정
- 3) Selected IP로 통신 되는 방식

WAPPLES SA 운영 방안

III. Multi domain nat 기능

1. 개요

- 1) v6.0.4 이상 버전에서만 사용 가능
- 2) L7 (hostname) 기반 1:N NAT 기능
- 3) 보호대상 서버 설정에서 Proxy -> 다중 선택하여 사용 가능



WAPPLES SA 운영 방안

III. Multi domain nat 기능(계속)

2. 설정 방법

- 1) 보호 대상 서버 -> Proxy -> 다중
- 2) 호스트명 입력 후 대상 웹서버 지정(IP 또는 DNS 주소)
- 3) 헬스 체크는 DNS 주소로 입력했을 때만 설정 가능하며, 보통 사용 안함으로 체크

서버 모드

Inline Proxy T.Proxy 단일 호스트 LB 다중 호스트 LB

프록시 IP 172.31.31.132

프록시 포트 80

단일 다중

+

검색...

	호스트명	대상 웹 서버	포트	헬스 체크	적... ↑
수정 삭제	www.abc.com	1.1.1.1	80	사용 안 함	1
수정 삭제	www.def.com	2.2.2.2	80	사용 안 함	2
수정 삭제	www.xyz.com	3.3.3.3	80	사용 안 함	3

```
pentasec@ip-172-31-31-132:~$ sudo show filter
Session Filter Info
40000 - TCP 000.000.000.000[000.000.000.000]:00000/00000 => 172.031.031.132[255.255.255.255]:00080/00080 - NAT<40000><40001><40002> DETECT ENABLE
L 40000 - NAT-TYPE(SINGLE_DNAT|HOSTNAME_DNAT) snat_ip(172.031.031.132) hostname(www.abc.com) dnatIp(001.001.001.001) dnat_port(00080)
L 40001 - NAT-TYPE(SINGLE_DNAT|HOSTNAME_DNAT) snat_ip(172.031.031.132) hostname(www.def.com) dnatIp(002.002.002.002) dnat_port(00080)
L 40002 - NAT-TYPE(SINGLE_DNAT|HOSTNAME_DNAT) snat_ip(172.031.031.132) hostname(www.xyz.com) dnatIp(003.003.003.003) dnat_port(00080)
pentasec@ip-172-31-31-132:~$ sudo show nat
```

WAPPLES SA 운영 방안

IV. Sync(다중 동기화) 기능

1. 개요

- 1) Auto Scaling에서 서비스 되기 위한 다중 동기화 기능(설정 동기화) 제공
- 2) 관리도구 설정에 대한 Master / Slave 설정
 - A. Master
 - ① 설정에 대한 주체가 되는 WAPPLES SA
 - ② Master WAPPLES SA는 한 대만 지원
 - B. Slave
 - ① Master에서 설정 변경 시, 설정 동기화 되는 WAPPLES SA
 - ② Slave 설정 된 WAPPLES는 관리도구 설정 변경 불가능
- 3) 1:1 또는 1:N 운영 가능
- 4) 다중 동기화 설정은 CouchDB 동기화에 한정
- 5) 로그 동기화 불가능

WAPPLES SA 운영 방안

IV. Sync(다중 동기화) 기능(계속)

2. 설정 방법

- 1) CLI wapples -> sync 탭에서 설정 가능
- 2) Master 설정
 - A. sync set master
- 3) Slave 설정
 - A. sync set slave default 1.1.1.1(master ip) 5984
 - B. Master를 바라볼 수 있도록 master ip 및 5984 port 설정

```
pentasec@ip-172-31-31-132: (wapples-sync)# show config
current sync mode : master enable
-----
[CONFIG]
  MASTER : on
  SLAVE : off
  WCC : off
-----
[MASTER]
  IP :
  PORT :
-----
[AWS]
  INSTANCE_ID :
  REGION_NAME :
  ACCESS_KEY_ID :
  SECRET_ACCESS_KEY :
-----
pentasec@ip-172-31-31-132: (wapples-sync)#
```

<Master>

```
pentasec@ip-172-31-31-132: (wapples-sync)# show config
current sync mode : slave enable
-----
[CONFIG]
  MASTER : off
  SLAVE : on
  WCC : off
-----
[MASTER]
  IP : 1.1.1.1
  PORT : 5984
-----
[AWS]
  INSTANCE_ID :
  REGION_NAME :
  ACCESS_KEY_ID :
  SECRET_ACCESS_KEY :
-----
pentasec@ip-172-31-31-132: (wapples-sync)#
```

<Slave>

WAPPLES SA 운영 방안

IV. Sync(다중 동기화) 기능(계속)

3. 참고 사항

- 1) Sync 설정은 라이선스가 반영된 상태에서 진행 되어야 하며, 관리도구 설정이 아무것도 없는 상태에서 진행
- 2) Slave 설정된 WAPPLES SA를 Auto Scaling 이미지로 사용
- 3) Slave 설정 WAPPLES은 관리도구 설정 변경 할 수 없음
 - A. 예외 항목
 - ① 탐지/감사로그 내보내기, 관리도구 sw-bypass, 보고서 생성, 백업/복원 실행 메뉴
- 4) Couchdb에 저장되는 내용은 모두 동기화 대상이며, couchdb 포트인 5984 포트 사용