OpenDNS 보안조치 가이드

V1.0

스마일서브
Korea first service

목차

1. OpenDNS로 인한 국제 트래픽 발생 / 대응 방안

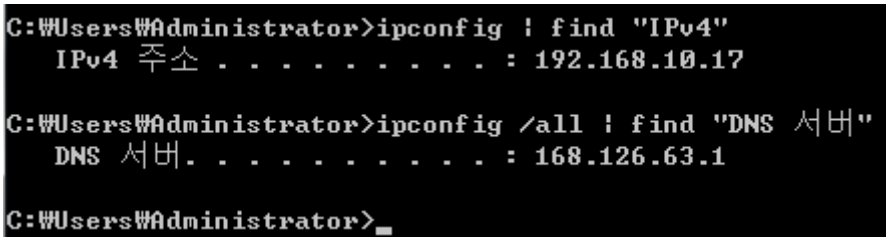
1-1. OpenDNS란?

OpenDNS란 모든 인터넷 사용자들에게 Recursive Query (재귀적 질의)에 대해 응답을 해주는 DNS를 말합니다. 이러한 OpenDNS는 캐시네임서버로 사용되지 않는다면 불필요한 설정입니다.

(* 또한 의도치 않은 해외트래픽 발생의 여지가 있습니다.)

참고 1 : 일반적으로 사용하는 도메인만 등록하여 자체 네임서버를 구성하는 경우 '재귀적 질의'의 사용은 불필요 합니다. (대표적인 캐시 네임서버 : KT 168.126.63.1 / SK 219.250.36.130)

리눅스(상) 윈도우(하) / (자체 네임서버 구성하였으나, 네트워크 네임서버는 KT 이용)



참고 2 : 자체 네임서버를 서버 네트워크에서 사용하는 네임서버로 사용시에는 '재귀적 질의'사용이 필요합니다.

1-2. 설정 변경

1-2-1. 리눅스

(1-1) Recursion 기능 비활성화

#참고 1의 경우 캐시네임서버로 사용되지 않으므로 Recursion 기능이 불필요 합니다. 아래 설정은 외부로부터의 모든 호스트들로부터 오는 '재귀적 질의'에 대해 응답하지 않는 예입니다.

설정은 named.conf의 Options 부분에 다음과 같은 내용을 추가합니다.

```
Options {
    recursion no;
};
```

(1-2) Recursion 서비스 호스트 제한

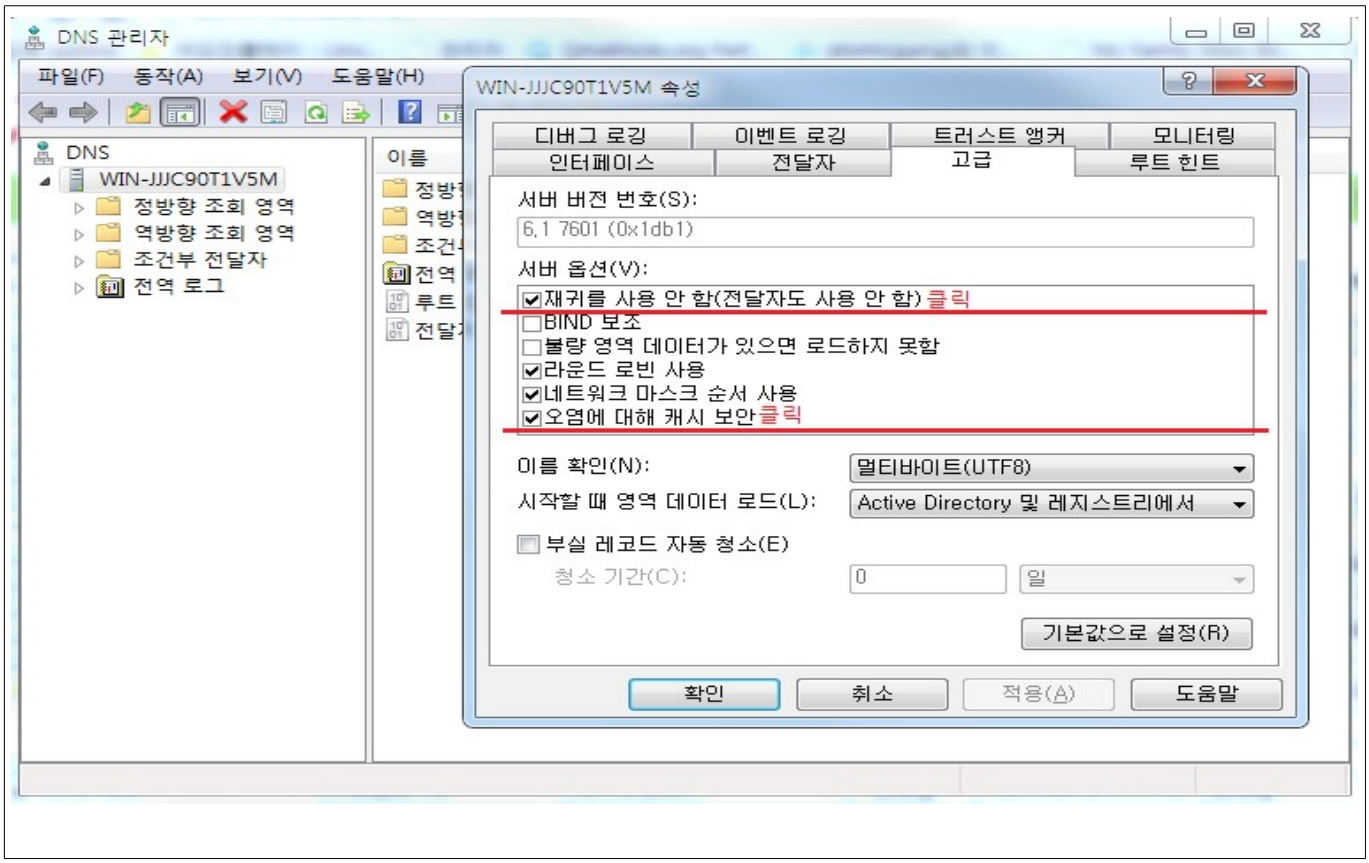
#참고 2의 경우처럼 자체 네임서버를 서버 네트워크에서 사용하는 네임서버로 사용시에는 Recursion 호스트를 제한하는 방법이 있습니다. 아래 설정은 192.168.10.0/24 에서만 Recursion 서비스 이용이 가능하도록 설정하는 예입니다.

설정은 named.conf에 다음과 같은 내용을 추가합니다.

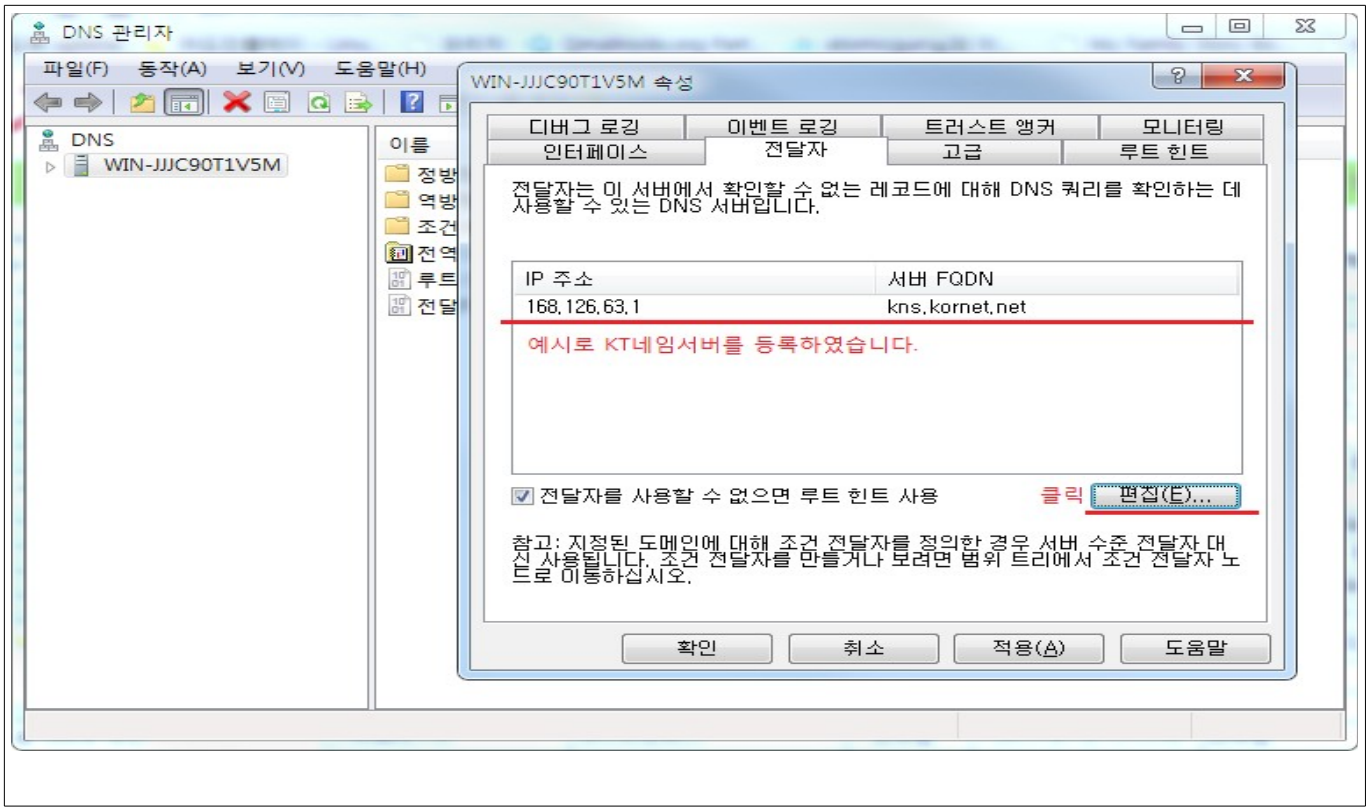
```
acl trust { 192.168.10.0/24; };

Options {
    allow-recursion { trust; };
};
```

1-3-2. 윈도우

(1-1) Recursion 기능 비활성화



(1-2) Recursion 서비스 호스트 제한



1-4. 추가 사항

현재 운영중인 서버가 OpenDNS 서버인지 확인하는 방법입니다.

기본 사용법은 아래 링크로 접속 후 IP 입력후에 바로 결과를 확인할 수 있습니다.

http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl/

OPEN RESOLVER TEST

This tool sends a single "recursion desired" query to one or more target addresses. If the queries are forwarded to our authoritative server, the host has an open resolver running at that address.

Enter up to 10 IPv4 Addresses:

115.68.62.210 예시로 스마일서브 1차 네임서버를 입력하였습니다.

제출 재설정

클릭

OPEN RESOLVER TEST RESULTS

Address	Status	Date Checked
115.68.62.210	open	2013-04-07 10:18:58

테스트 결과, 최근 2013-04-07 10:18분에 확인되었으며 해당 서버는 '재귀적 질의'가 허용되어 있음을 알 수 있습니다.

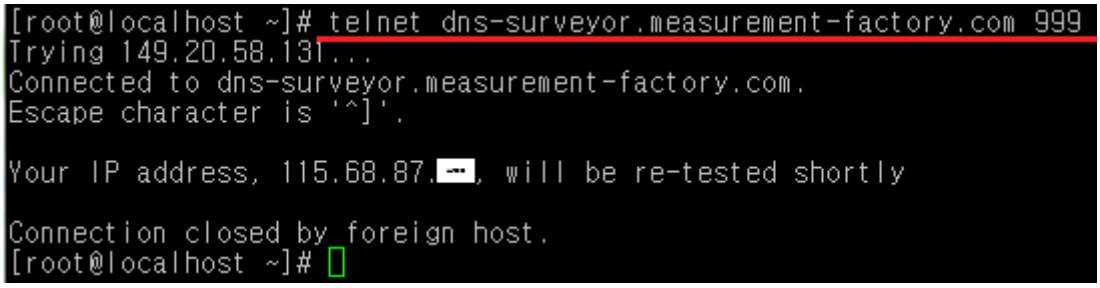
Notes

- Addresses marked closed may not even be running a resolver.
- If a resolver receives and transmits on different addresses, the transmitting address is shown in [brackets].
- Results are cached to avoid frequent probing. If you want your address to be re-tested, make a TCP connection to dns-surveyor.measurement-factory.com port 999 (e.g., with *telnet*) from the address to be tested.

만약 Recursive Query를 사용하지 않도록 설정한 후에 다시 테스트를 원한다면,

리눅스의 경우 쉘 상에서, 윈도우의 경우 '시작 > 실행 > CMD' 상에서 아래와 같이 입력합니다.

입력 후 잠시 기다리면 아래와 같은 응답을 받을 수 있습니다.



위 메세지 확인 후 빠르면 수 분 내에, 길면 하루 안에 다시 테스트가 완료되며 해당 사이트에서 다시 테스트시 설정 변경된것을 확인할 수 있습니다.