

프록시 서버(Proxy Server) 개념

프록시 서버(Proxy Server)는 클라이언트(Client)가 자신을 통해서 다른 네트워크 서비스에 간접적으로 접속할 수 있게 해 주는 컴퓨터 시스템이나 응용 프로그램을 말합니다. Server와 Client 사이에 중계기로서 대리로 통신을 수행하는 것을 가리켜 'Proxy', 그 중계 기능을 하는 것을 Proxy Server라고 부릅니다. Proxy Server 중 일부는 Proxy Server에 요청된 내용들을 캐시(Cache)를 이용해 저장합니다.

프록시 서버는 다음과 같이 2가지 종류가 있습니다.

1. 포워드 프록시(Forward Proxy)
2. 리버스 프로시(Reverse Proxy)

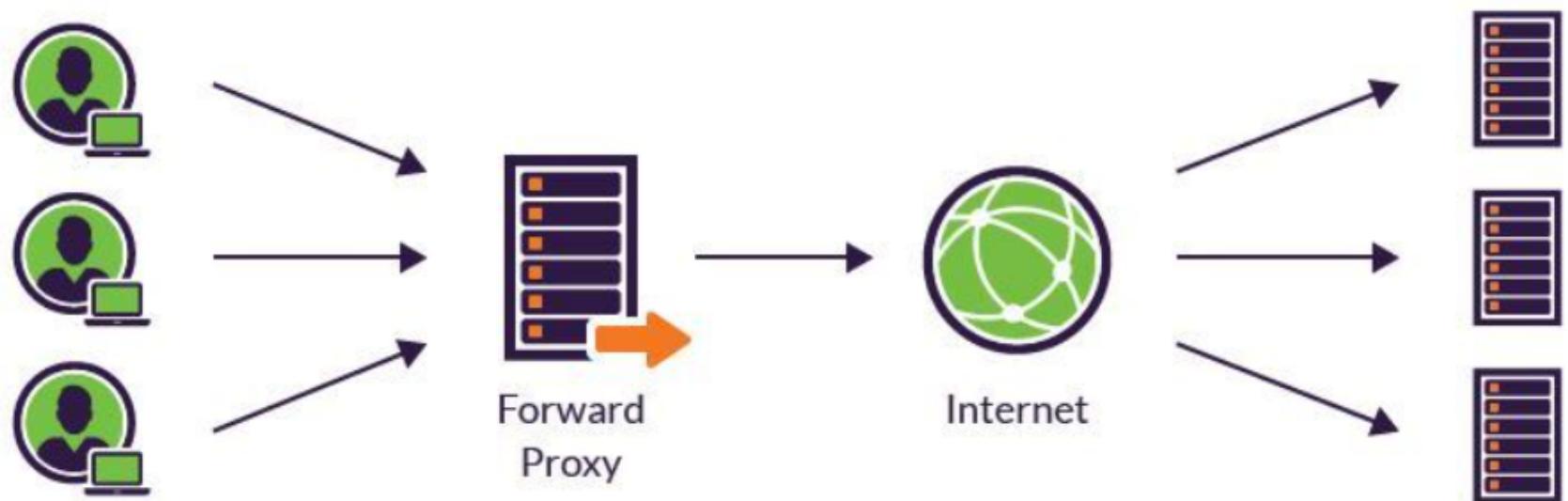


Web Server와 WAS에 대해 연동하려면 Reverse Proxy에 대한 이해가 필수입니다.

아파치 웹서버(apache web server)에는 mod_proxy라는 모듈에서 forward proxy와 reverse proxy 두 가지 기능을 제공하며 nginx는 필요한 기능만 제공하는 고성능 웹 서버에 맞게 reverse proxy 기능만 제공합니다.

웹서버가 Proxy 서버 역할을 수행함.

2. Forward Proxy



일반적으로 프록시라고 하면 포워드 프록시입니다.

클라이언트가 서버로 요청할 때 직접 요청하지 않고 먼저 프록시 서버를 통해 요청하는 방식입니다.

이 방식을 좀 더 쉽게 이해하자면 회사 내부 인트라넷에서 인터네트에 있는 서버에 요청할 때 먼저 프록시 서버를 호출하게 되는 데 이런 방식이 포워드 프록시입니다.

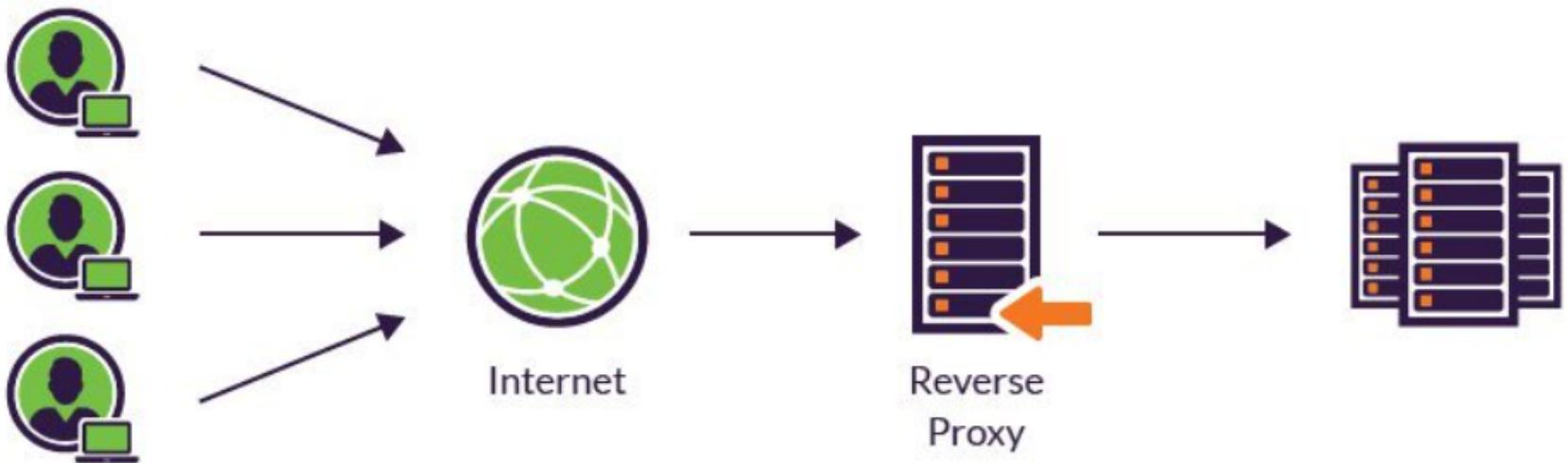


서버에게 클라이언트가 누구인지 감추는 역할을 해주죠.

서버가 응답받은 IP는 포워드 프록시 서버의 IP이기 때문에 클라이언트가 누군지 알 수 없습니다.

위 그림으로 이해하자면 인터넷보다 프록시 서버를 먼저 호출하게 되면 포워드 프록시입니다.

3. Reverse Proxy



리버스 프록시는 포워드 프록시와 반대 반향을 생각하면 됩니다.

클라이언트가 서버를 호출할 때 리버스 프록시를 호출하게 되고 프록시 서버가 서버를 요청하여 받은 응답을 클라이언트에게 전달하는 방식입니다.

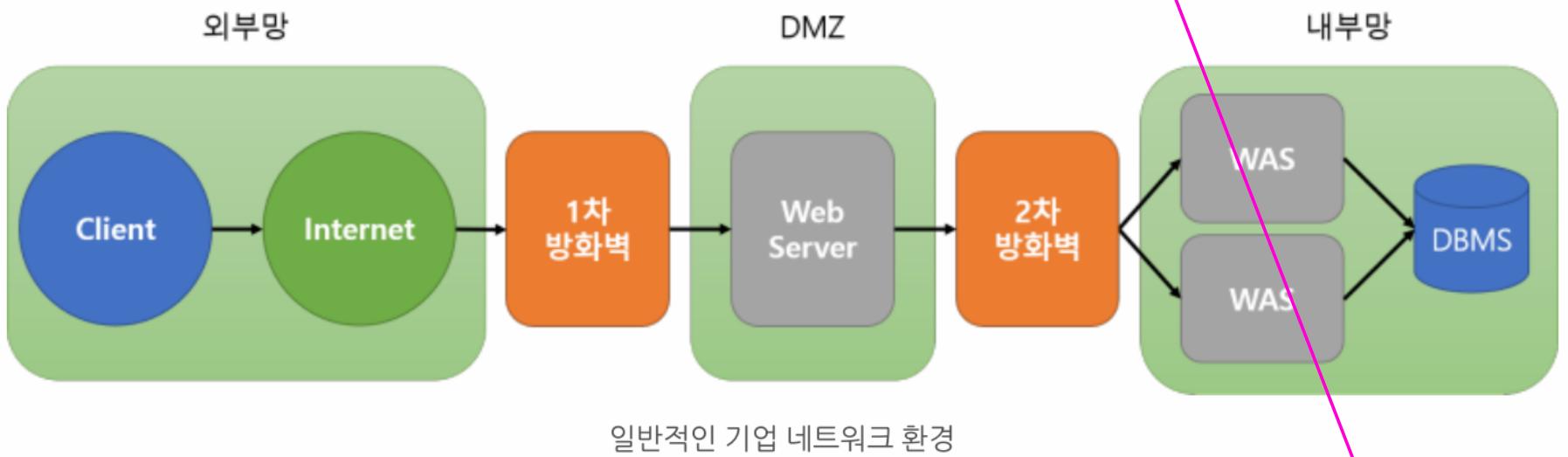
이 방식은 내부 인트라넷에 있는 서버를 호출하기 위해서 인터넷 망에 있는 클라이언트가 리버스 프록시 서버에 요청하여 응답을 받는 방식입니다.

리버스 프록시는 서버가 누구인지 감추는 역할을 해줍니다.

클라이언트는 리버스 프록시 서버를 먼저 호출하게 되기 때문에 실제 서버의 IP를 알 수 없습니다.

위 그림으로 이해하자면 인터넷망에 있는 클라이언트가 프록시 서버를 호출하여 내부망에 있는 서버를 호출하는 방식이리버스 프록시 입니다.

보통 기업의 네트워크 환경은 외부망(External Network)과 내부망(Internal Network) 사이에 DMZ(Demilitarize Zone)라고 하는 망이 존재합니다. 일반적으로 DMZ에는 외부망으로 서비스를 제공하는 서버(Mail Server, Web Server, DNS Server)를 배치하고, 내부망에는 WAS를 배치합니다. 만약 WAS가 최전방에 배치되어 있다고 했을 때 블랙햇 해커(Black Hat Hacker)에게 WAS가 터릴 경우 WAS는 DBMS와 직접적으로 연결되어 있기 때문에 DBMS Server까지 모두 터릴 수 있는 심각한 보안 취약점이 있습니다.

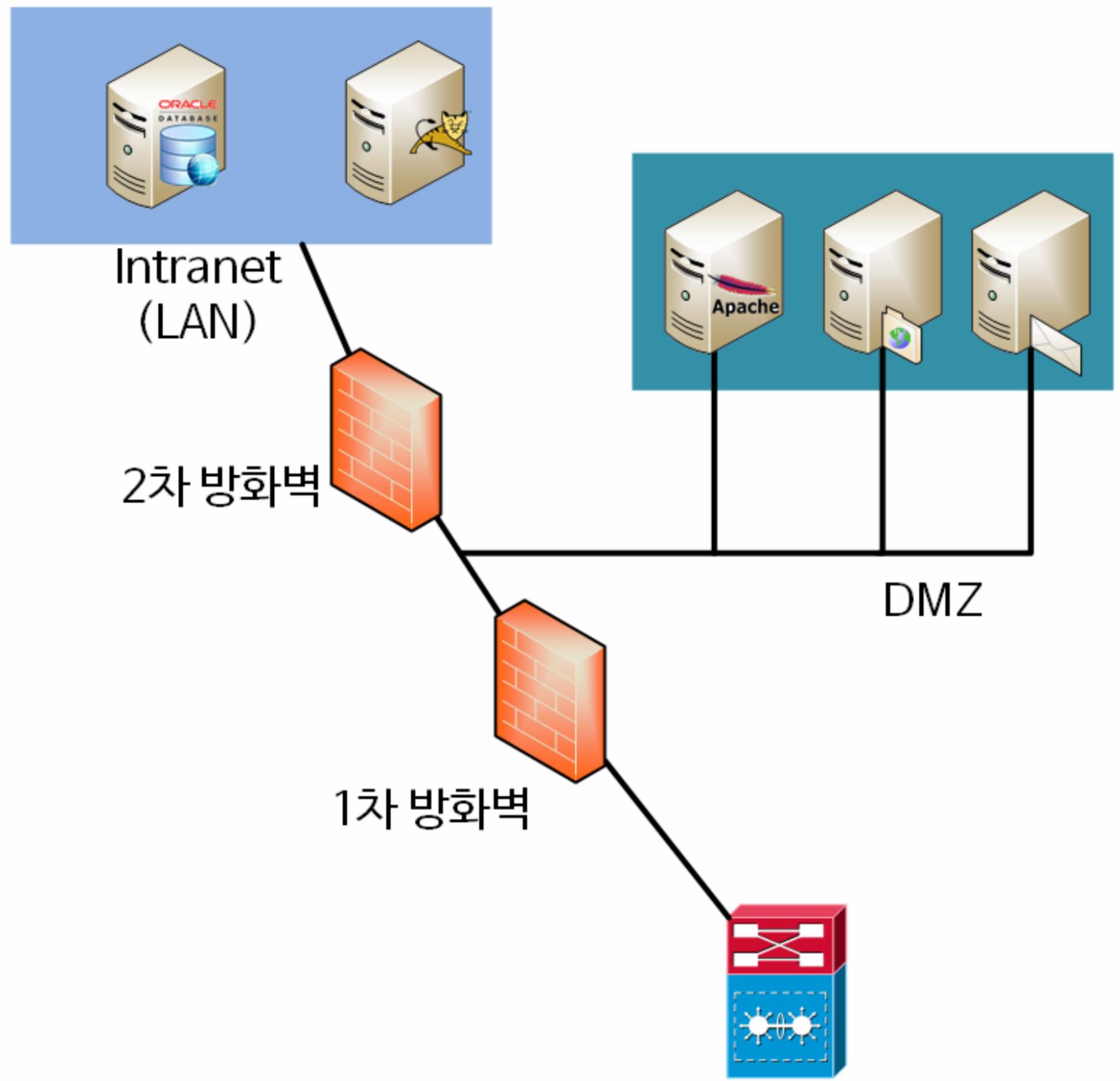


따라서 DMZ망에 Web Server를 두고 Reverse Proxy로 설정하고 WAS는 내부망에 배치합니다. Reverse Proxy로 동작하는 Web Server만 내부 WAS와 연결하도록 설정해서 Web Server가 해킹 당해도 2차 방화벽을 다시 뚫어야 하므로 보안에 강해질 수 있습니다.

Reverse Proxy Server 앞에 Cache Server를 붙이거나 SSL 하드웨어 가속기를 연동하면, 아키텍처 측면에서 성능 향상에도 용이합니다. 간단하게 생각하면 cloudflare 나 akamai 같은 CDN 도 Reverse Proxy로 동작하는 Cashe Server입니다. CDN 을 연동한다면 DDOS 공격을 효과적으로 방어하고 서비스를 빠르고 안정적으로 제공할 수 있습니다.

Reverse Proxy를 Cluster로 구성해 놓으면 가용성을 높일 수 있고, 사용자가 증가하는 상황에 맞게 Web Server 나 WAS를 유연하게 늘릴 수 있는 장점이 있습니다. Reverse Proxy 앞에 L4 Switch나 Load Balancer를 붙이면 Round Robin(RR), Least connection 등 상황에 맞는 분배 알고리즘을 적용해 서비스 신뢰성을 높일 수 있습니다.

보통 기업의 네트워크 환경은 비무장 지대(DMZ; Demilitarized Zone) 라고 하는 내부 네트워크와 외부 네트워크 사이에 위치하는 구간이 존재합니다.



위 그림과 같이 DMZ 내에 외부에 서비스를 제공하는 서버(메일 서버, 웹 서버, DNS 서버)를 배치하고 네트워크는 1, 2차 방화벽으로 보호합니다.

example.com 서비스를 제공하려면 WAS 를 DMZ 에 놓고 서비스해도 되지만 이런 서비스는 보통 내부의 DBMS 서버와 연결되어 있습니다.

만약 WAS 가 최전방에 있으면 WAS 가 털릴 경우 DBMS 와 관련 서버까지 모두 같이 털리는 심각한 보안 문제가 발생할 수 있습니다.

이때문에 DMZ 존에 웹 서버를 두고 리버스 프락시로 설정하고 WAS 는 내부망에 위치시키게 설정합니다.

리버스 프락시로 동작하는 웹 서버만 내부 WAS 와 연결하도록 설정하므로 웹 서버가 해킹당해도 2 차 방화벽을 다시 뚫어야 하므로 더 보안에 강해질 수 있습니다.

특히 Red Hat이나 CentOS라면 SELinux 를 켜 놓으면 SELinux 의 강제 접근 통제에 따라 웹 서버는 사전 정해진 포트(예: WAS 의 8080, 8009)만 접근 할 수 있으므로 웹 서버가 해킹당해도 2 차 피해를 최소화할 수 있습니다.

