이것만은 알아야 할 네트워크 보안 이야기

Part 7. DDoS 3. DDoS 공격의 차단 방안

글. 이선응 아이크래프트 수석
Ka3211a@gmail.com

연재 목차

이번 호에서는 DDoS 공격 트래픽을 어떻게 차단하는지 설명하도록 하겠다. 일단 의심되는 트래픽이 탐지되면, 다양한 방식으로 해당 트래픽을 차단할 수 있는데 대략 4가지 정도의 방법이 존재한다.

번호	방식	내용
1	블랙홀(Blackhole) 방식 : null-routing using BGP	공격으로 의심되는 특정 목적지의 트래픽을 특정 라우터로 우회시켜 모든 트래픽을 패기
2	필터차단 방식	관리자가 공격 IP 및 포트 정보를 확인하여 라우터에서 조건에 해당하는 트래픽을 수동으로 필터를 생성하여 조건에 해당하는 트래픽만 차단
3	Flow Specification 이용방식	FlowSpec 기능이 동작하는 라우터에서 적용 가능하며 필터생성을 자동화시켜 신속하게 차단
4	전용 차단 장비 이용방식	공격으로 의심되는 모든 트래픽을 전용 차단 장비로 보내 실제 공격 트래픽은 차단하고, 정상으로 판단되는 트래픽은 원래 목적지로 전달

차단방식이 개발되던 초기에 나온 방식이 1번이다. 가장 쉽게 구현이 가능한 장점이 있지만 정상적인 트래픽도 차단되는 단점이 있다. 2번 방식은 트래픽을 처리하는 장비에 관리자가 직접 필터를 적용하여 트래픽을 처리하는 방식인데, 관리자가 수동으로 입력해야 해서 대응 속도가 느리고, 라우터의 처리 성능에 대한 고려가 필요한 방식이다. 3번 방식은 2번 방식을 자동화한 것으로, 관리자가 수동으로 필터를 입력하는 것이 아니고, 탐지 장비에서 확인한 트래픽의 목적지 IP 및 포트 정보를 이용하여 라우터에 자동으로 필터가 생성되어, 대응 속도를 높인 방식이다. 마지막으로 4번째 방식은 전용 차단 장비를 이용하는 방식으로 인라인타입 제품이나 아웃오브패스타입의 차단 장비 모두 이용이 가능하다. 이 방식은 의심되는 모든 트래픽을 차단하는 것이 아니고, 트래픽의 L3~L7 레벨을 다시 검사해서 정상으로 판별되는 트래픽은 원래 서버로 전송하고, 공격으로 판별되는 트래픽만 폐기하는 방식으로 동작한다.

초창기에는 대부분 1번 방식을 이용했지만 최근에는 대부분 4번 방식을 주로 적용하는 추세이다. 4번 방식은 공격으로 의심되는 정황이 탐지되면, 해당 공격대상으로 가는 모든 트래픽은 차단 장비로 우회시킨다고 했다. 여기서 의심되는 정황이라고 표현한 이유는 임계치 기반의 탐지방식이 100% 정확할 수가 없기 때문이다. 단지 평상시 트래픽 사용량 대비 통계적으로 충분히 비정상적인 상태를 탐지하고, 해당 목적지로 가는 트래픽을 좀 더 자세하게 검사하여 공격으로 의심되는 트래픽은 차단하고, 정상으로 판단되는 트래픽은 서버로 전달하겠다는 전략이 아웃오브패스방식 장비의 방어전략이다.

탐지 장비가 트래픽을 모니터링하는 방식이 라우터에서 보내주는 Netflow 기반 정보를 이용하기 때문에 해당 정보는 L3~L4 레벨 정보만 포함되어 있다. 그래서 용량기반 공격이나 자원 소모 공격은 비교적 정확하게 탐지가 가능할 수 있지만 L7 레벨을 이용하는 애플리케이션 기반 공격은 탐지가 부정확할 수 있다. 그래서 의심스러운 트래픽은 차단 장비로 우회시켜 직접 트래픽을 모니터링하면서 L3부터 L7까지 모든 레이어를 직접 검사하는 방식으로 작동한다.

그럼 차단 장비에서는 어떤 방식으로 정상 트래픽과 공격 트래픽을 구분하는지 알아보자. 차단 장비는 L3~L7까지 다양한 차단 필터를 가지고 있다. 각각의 필터는 특정 공격에 대해 식별 및 차단을 할 수 있는 기능을 가지고 있다. [그림 1]과 같이 왼쪽에 빨간색으로 표시된 공격 트래픽과 녹색으로 표시된 정상 트래픽이 있다고 가정해 보자. 차단 장비로 트래픽이 들어오면 제일 먼저 유입되는 패킷이 표준을 준수하는 정상적인 패킷인지, 블랙리스트에 등록된 IP 주소는 아닌지, 혹시 북한에서 들어오는 트래픽은 아닌지 등을 체크하여 설정에 따라 공격으로 판단된 트래픽은 차단되고, 정상으로 판단한 트래픽은 다음 필터로 넘어간다. 이런 방식을 이용하여 다양한 필터를 직렬로 배치하여 단계별로 공격 트래픽을 차단해 가다 보면 최종 필터를 통과한 트래픽만 정상으로 추정하여 서버로 전달하는 방식으로 차단을 수행한다. 공격의 종류가 다양해지고 공격의 크기가 증가하면서 이런 순차적인 다단계 차단 방식이 보다 효과적이며, 차단 수행 시 장비의 부하를 최소화해 같은 성능의 장비로 더 큰 용량의 공격을 차단할 수 있는 장점이 있다.

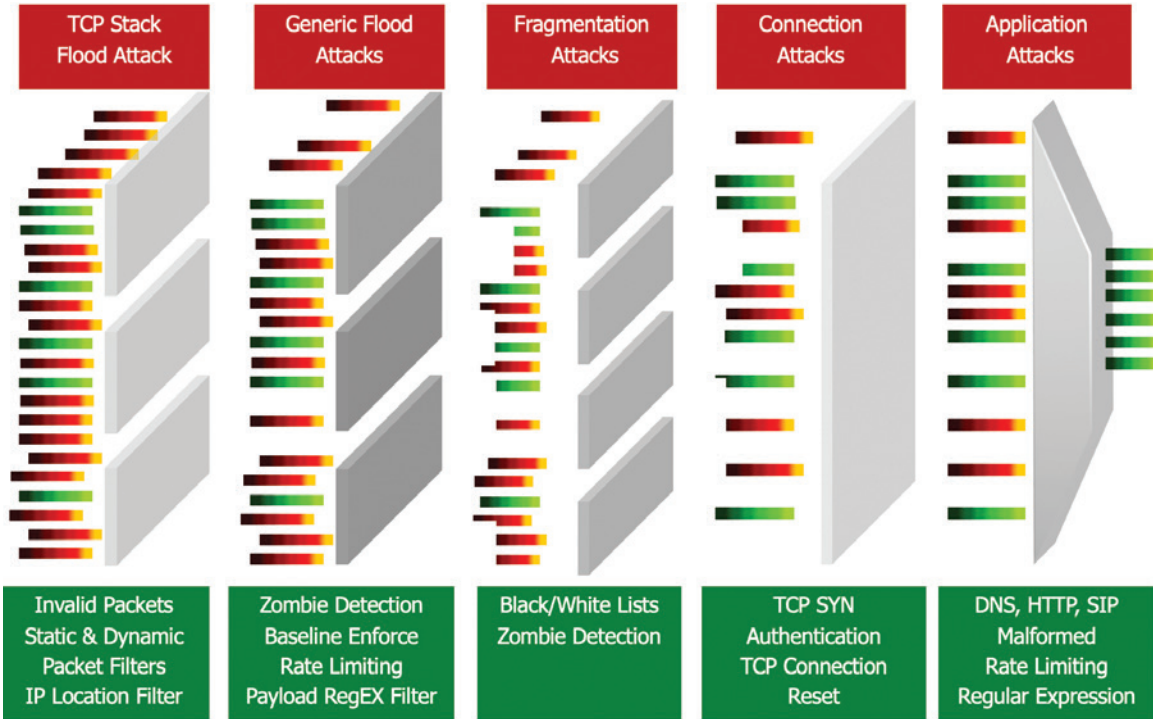

그림 1. DDoS 공격 방어를 위한 단계적 차단 체계

다음으로 공격을 식별하고 차단하기 위해 구체적으로 어떤 단계를 거쳐서 패킷을 검사하고 식별된 공격 트래픽을 차단하는지 알아보자. [그림 2]와 같이 단계적 차단을 위한 여러 차단단계를 표시하였다. 1번 Invalid Packets에서부터 12번 IP Location Policing까지 다양한 공격을 각각의 공격 특성에 맞추어서 효과적인 차단방식을 선택적으로 적용하여 공격 트래픽을 단계별로 순차적으로 걸러내게 구성되어 있다. 이는 마치 그림의 오른쪽과 같이 인터넷회선을 제일 상단부터 방화벽, IPS, Layer 7 스위치, QoS 장비를 거쳐서 직렬로 순차적으로 배치한 것과 동일한 효과를 발휘한다. 즉 네 가지의 독자적인 보안 장비의 기능을 하나의 장비에서 통합적으로 설정하고 모니터링이 가능하게 구성하여 더욱 유기적으로 각각의 기능을 발휘하게 구성한 것과 같다. 모든 단계에 대해 자세히 설명하기에는 지면이 허락되지 않아서 주요한 단계만 선별해서 설명하도록 하겠다.

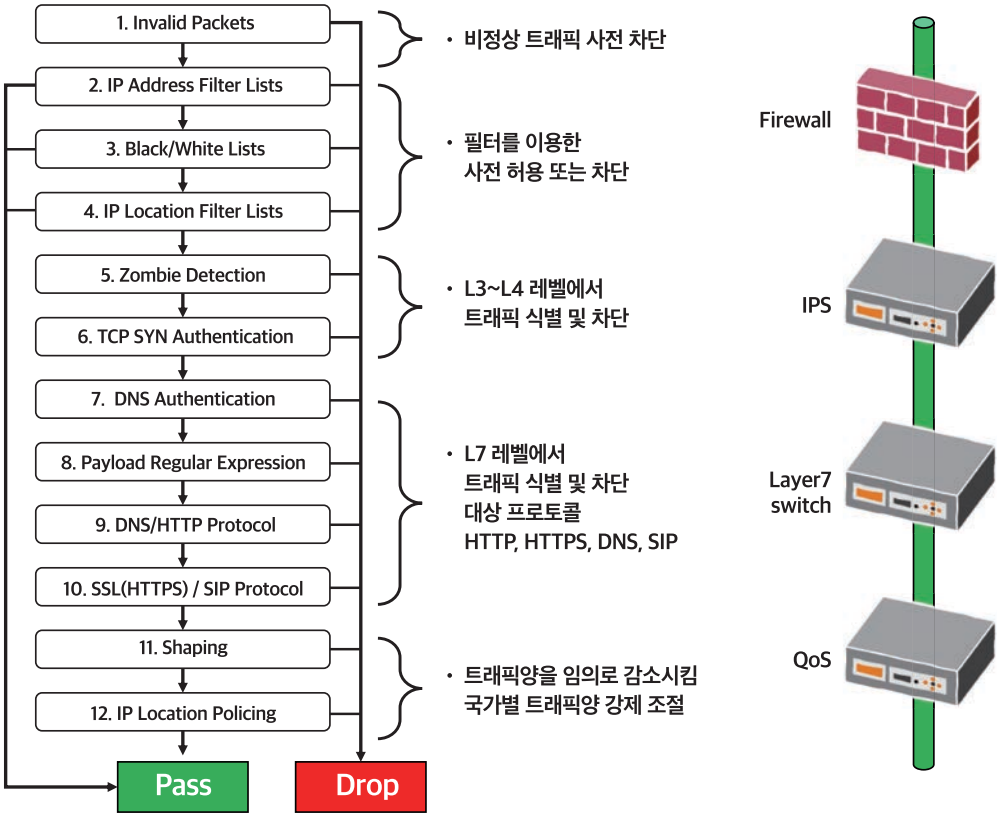

그림 2. 차단 장비의 공격 트래픽 검사 단계 및 순서

첫 번째 단계는 패킷이 표준에 맞게 구성되어 있는지 확인하는 단계이다. 정상적인 클라이언트에서 발생하는 트래픽은 단연히 서버와 통신을 위해서 표준에 맞추어서 생성되어 전달되게 된다. 표준에 위배되면 서버와 통신이 불가능하기 때문이다. 그러나 DDoS 공격 툴에서 만들어지는 패킷은 정상 통신이 아니고 공격을 목적으로 생성되기 때문에 표준에 위배되게 생성되는 경우가 있다. 이런 패킷은 사전에 차단하여 이후 단계를 거치면서 발생하는 부하를 최소화할 필요가 있어 제일 먼저 검사하는 것이다.

2~4번째 필터 단계는 공격이 발생한 이후 어느 정도 공격을 차단하면서 정상적인 트래픽으로 파악된 패킷의 출발지 IP나 포트 넘버를 필터에 적용하여 이후 단계를 거치지 않고 바로 서버로 전달하거나, 반대로 공격으로 이미 판별된 패킷에 대해 사전 차단을 수행하여 이후 단계에서 추가로 검사할 필요가 없을 때 사용하는 차단단계이다. 추가로 특정 대륙에 할당받은 공인 IP 대역 정보를 장비가 사전에 가지고 있다가 특정 대륙에서 오는 트래픽은 사전에 차단하고 싶을 때도 사용할 수 있다. 예를 들면 코로나 사태로 원격수업에 필요한 시스템의 경우 상식적으로 해외에서 접속

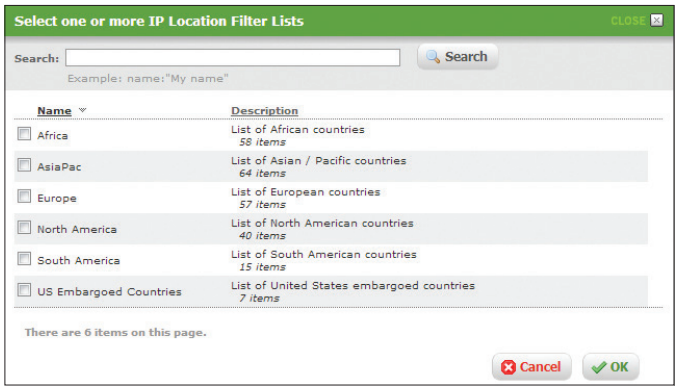

그림 3. 지리적 위치기반 차단 필터 리스트

할 경우는 매우 희박할 수 있다. 그래서 북미, 남미, 아프리카 등 대륙 단위로 서비스가 필요 없는 지역의 공인 IP는 처음부터 차단하고 싶을 때도 사용 가능하다. 이런 필터 단계가 필요한 이유도 필터차단 이후 즉 5단계 이후부터는 장비의 부하가 상대적으로 많이 사용되기 때문이다. 이미 정상 트래픽이나 공격으로 판별된 트래픽에 대해서는 굳이 장비의 자원이 소모하면서까지 추가적인 단계를 거쳐서 검사할 필요가 없기 때문이다.

5번째 단계는 좀비(Zombie) 단말에서 발생하는 비정상 트래픽을 차단하는 단계이다. 다양한 Flood 공격 등의 용량 기반 공격과 TCP SYN 등의 자원소모공격에 모두 효과적인 방어 단계이다. 동작 방식은 특정 출발지 IP를 기준으로 설정한 pps 혹은 bps 임계치를 설정하여, 트래픽이 임계치를 초과할 경우 해당 출발지 IP를 일정 시간 동안 차단하는 방식으로 동작한다. 여기서 모든 트래픽에 대한 총합을 임계치로 설정할 경우 정상적으로 트래픽을 많이 사용하는(Chatty) 호스트에 대해서도 차단이 될 수 있기에 특정 조건(패킷 길이, TCP flags 등)에 맞는 필터를 만들어서 필터별 임계치를 별도로 설정하면 좀 더 디테일하고 정확하게 공격 단말을 식별하여 차단할 수 있다.

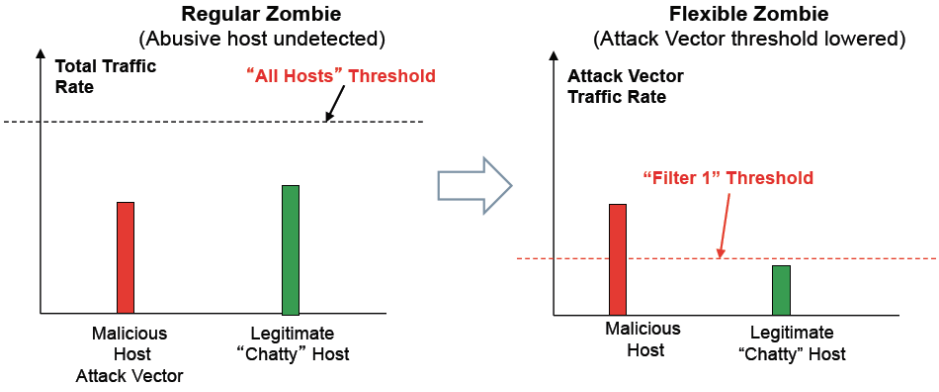

그림 4. Zombie Detection 차단 임계치 설정 개념도

6번째 단계는 TCP SYN 같이 자원소모공격에 특화된 차단단계이다. TCP 연결은 데이터를 전송하기 전에 두 장비 간 연결 준비를 사전에 하게 된다. 이 준비 단계를 3 way handshake라고 하여 서버와 단말 간 총 3번의 통신을 하여 연결 준비를 마치게 되는데, 이를 악용하여 서버의 TCP 연결 자원을 소모해 더는 신규 세션 연결을 못 하게 하는 것이 이 공격의 특징이다. [그림 5]와 같이 클라이언트와 서버 그리고 그 사이에 TMS라는 공격차단장비가 있다. 클라이언트는 서버로 TCP SYN 패킷을 보내면 중간의 TMS가 해당 패킷을 가로채서 서버 대신 클라이언트로 응답을 준다.
이때 기술적으로 더 들어가면 패킷을 주고받을 때 시퀀스넘버(seq)라는 고유번호를 사용하는데, 최초 클라이언트가 랜덤하게 만든 숫자에 TMS가 1을 더한 값을 SYN-ACK 패킷과 함께 보내면서 덧붙여 TMS가 랜덤하게 생성한 시퀀스넘버를 추가로 포함해 응답을 주게 된다. 만약 클라이언트가 정상적인 사용자라면 TMS가 랜덤하게 생성한 시퀀스넘버에 1을 더한 값을 응답하게 되는데, 이 시퀀스넘버가 정상적이면 출발지 IP를 정상사용자로 판단하여 이후 일정 시간 동안 서버와 패킷을 통과시키고, 만약 시퀀스넘버가 다르거나 응답이 없으면 공격자로 판단하여 해당 연결을 종료시키는 방식으로 동작한다.

다음 단계는 본격적으로 애플리케이션 기반 공격을 차단하는 단계이다. DNS Authentication은 애플리케이션 기반 공격 중의 하나인 DNS flooding 공격을 차단하기 위해 개발된 단계이다. DNS 서버란 도메인 네임(daum.net naver.com 등)을 브라우저에 입력하면 해당 도메인네임의 IP 주소를 알려주는 서비스로써 인터넷에 공개된 서버를 운영하는 조직은 모두 필수적으로 사용하는 서버이다. 만약에 DNS 서버가 DDoS 공격을 받아 정상적으로 응답하지 못하게 되면, 해당 조직의 공개 서버는 실제로는 아무 문제 없이 작동 중이라도, 외부에서 IP 주소를 확인할 수 없어 접속을 못 하게 되는 문제가 발생하게 된다. 2013년 6월 25일 대한민국 정부의 DNS 서버가 공격당해 정부 관련 온라인서비스가 정상적으로 접속되지 못한 일명 625 대란이라는 공격 사례가 있었다.

[그림 6]과 같이 DNS 공격에 대해 크게 2가지 방식으로 공격 트래픽을 식별하게 된다. 먼저 Passive 방식은 클라이언트에서 DNS 쿼리가 들어오면 TMS 장비는 해당 패킷을 차단한다. 설정한 timeout 시간(1분) 안에 동일한 출발지 IP에서 DNS 쿼리가 다시 들어올 경우 해당 IP를 정상으로 판단하여 이후 DNS 쿼리는 서버로 전달한다. 이 방식은 랜덤하게 출발지 IP를 변조하여 DNS 서버를 공격하는 행위에 대해 효과적인 차단방식이다. 두 번째 방식은 Active UDP 방식으로 클라이언

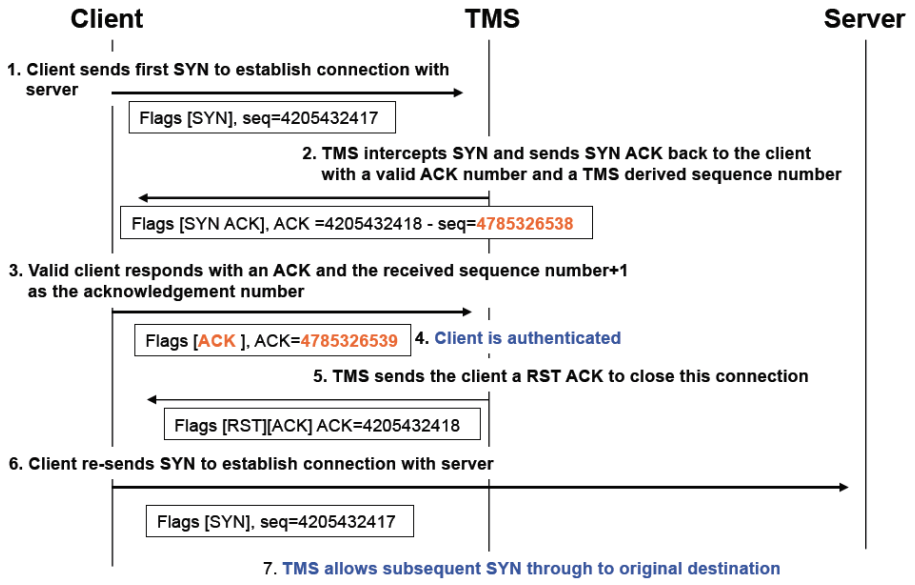

그림 5. TCP 기반 자원소모 공격에 대한 공격 단말 식별 방법

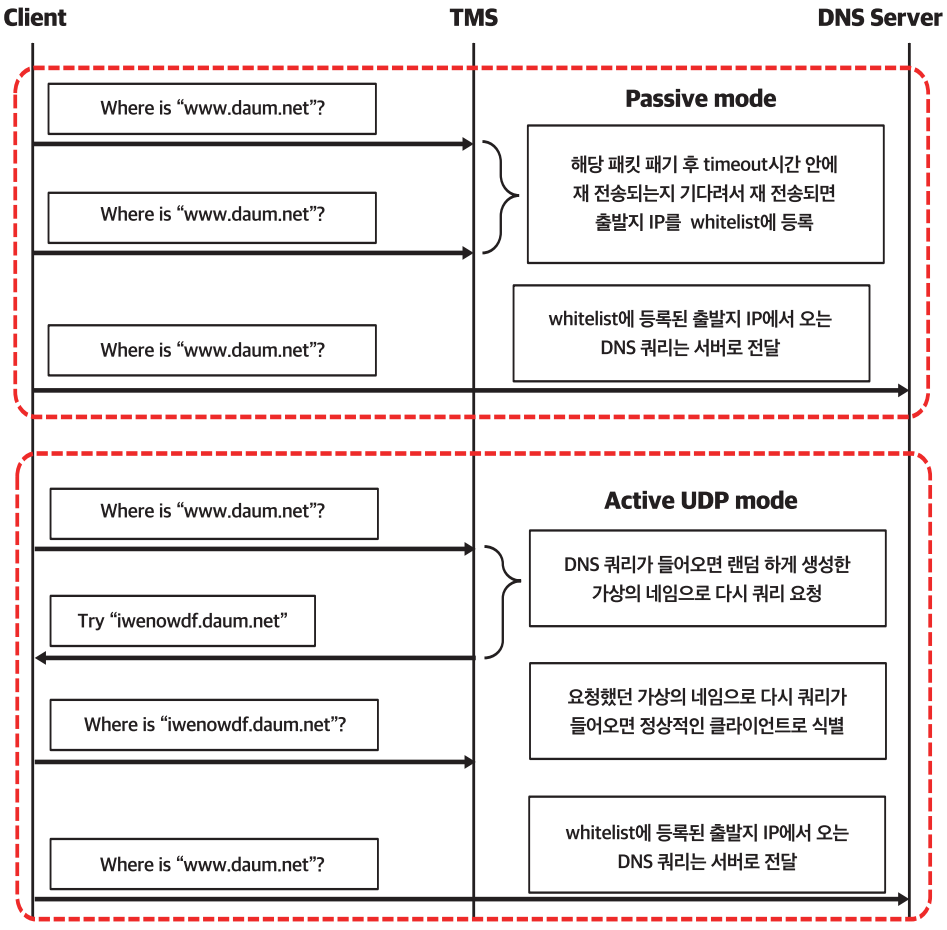

그림 6. DNS 기반 공격의 공격 단말 식별 방법

트에서 온 쿼리네임을 가상의 네임으로 변경하여 해당 클라이언트가 DNS 서버로 다시 쿼리하라고 요청한다. 이때 가상의 이름으로 다시 쿼리가 들어오면 정상적인 클라이언트로 식별하여 실제 DNS 서버로 전송하는 방식으로 작동한다.

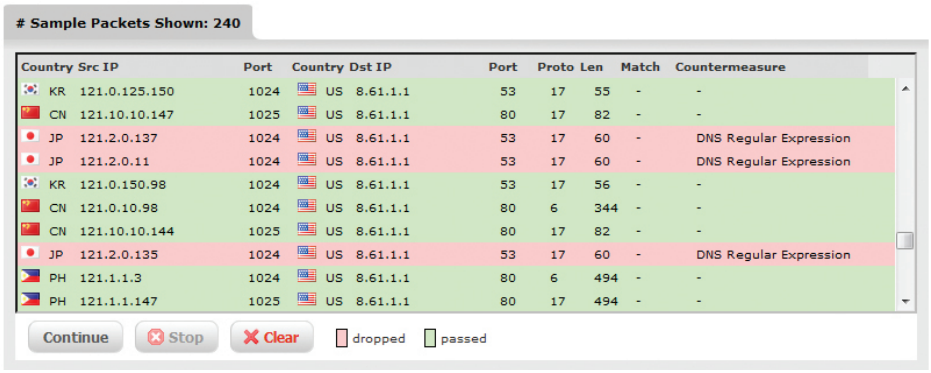

그림 7. DNS Regular Expression 방식으로 차단되는 공격패킷 현황

단말 식별 단계를 통과하면 다음으로 DNS Malformed와 DNS Regular Expression, DNS Rate Limiting, DNS NXDomain Rate Limiting 등 다양한 DNS 공격에 대한 차단단계가 기다리고 있다. 먼저 Malformed 탐지방식은 표준에 위배되는 정상적이지 않거나 비어 있는(내용이 없는) DNS 쿼리를 탐지하여 차단한다. Rate limiting은 정상적인 다량의 쿼리 요청이 들어올 경우 하나의 출발지 IP에서 초당 100개의 쿼리까지만 허용하고 100개를 넘으면 해당 IP를 일정 시간 동안 차단한다. 다음으로 NXDomain Rate Limiting은 존재하지 않는 도메인네임(NoneXistent)을 다량으로 보내 DNS 서버의 CPU를 소모하는 공격을 차단하기 위해, 초당 NXDomain으로 DNS 서버가 클라이언트로 응답하는 것을 모니터링하다가 초당 100개 이상의 NXDomain 응답이 있으면 해당 출발지 IP를 차단한다. 마지막으로 Regular Expression 단계는 관리자가 DNS 트래픽을 모니터링하고 있다가 특정한 패턴을 가지는 패킷이 빈번하게 보일 경우 수동으로 그 패턴을 등록하여 해당 DNS 패킷을 차단할 때 사용 가능한 차단단계이다. [그림 7]의 경우 이런 방식으로 차단된 DNS 기반 공격 패킷을 확인할 수 있다.

현재 가장 광범위하게 사용하는 프로토콜은 HTTP 프로토콜이다. 그만큼 HTTP 기반 DDoS 공격도 가장 빈번하게 발생하고 있어 여기에 대응하기 위한 여러 차단단계가 개발되었다. [그림 8]과 같이 서버와 클라이언트 사이에 TMS가 위치하여, 클라이언트에서 오는 HTTP 트래픽을 가로채서 대신 응답한다. 우선 최초 URI 요청을 임의로 변경하여 재접속요청을 클라이언트로 보낸다. 만약 TMS가 변경한 URI로 클라이언트가 연결을 요청하게 되면 정상적인 사용자로 인식하고, TMS가 다시 한번 최초 URI로 다시 재접속할 것을 클라이언트에 요청한다. 이후에는 해당 클라이언트의 요청을 서버까지 정상적으로 전달하게 된다.

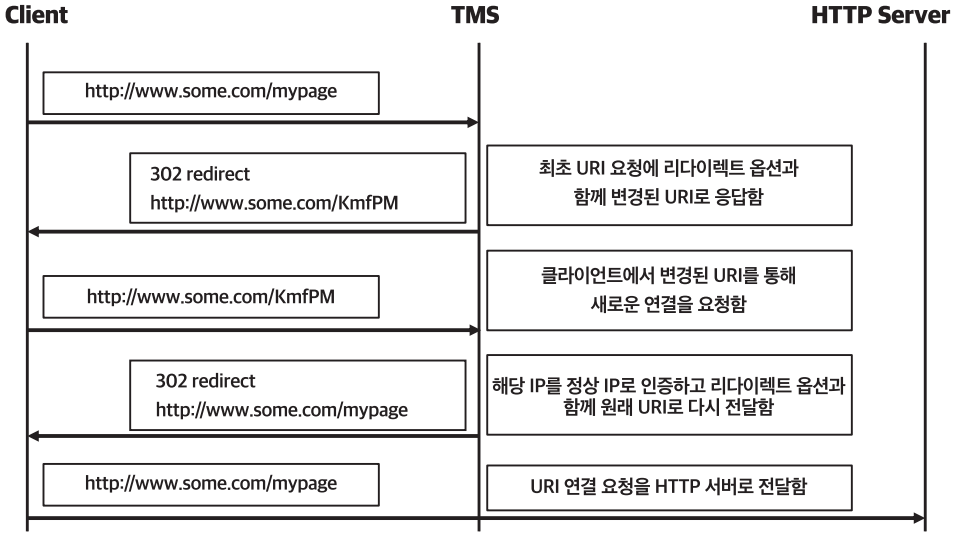

그림 8. HTTP 기반 공격의 단말 식별 방법

이 식별 단계를 통과하면 HTTP Malformed 단계에서 HTTP 내용이 표준에 위배되거나 비어있는 요청을 확인하여 출발지 IP를 차단한다. 다음으로 HTTP Rate Limiting 단계에서 특정한 한 개의 클라이언트가 특정 서버로 HTTP Request(get, put 등)를 초당 100개까지만 허용하고, HTTP object(index.html, /images/front.jpg)의 종류에 관계없이 초당 10개의 object까지만 허용하여 그 이상의 요청이 들어오면 해당 IP를 일정 시간 차단한다.

이 단계를 통과한 이후에도 HTTP 기반 DDoS 공격이 차단되지 않는다면 다음으로 HTTP/URL Regular Expression을 통해 HTTP Header를 검사하여 특정 값이 포함된 패킷을 차단하거나 인터넷에 공개된 공격툴이 발생시키는 공격 패킷의 특성을 패턴으로 등록하여 패턴에 매칭되는 패킷을 차단하고 해당 출발지 IP를 차단한다. [그림 9]는 벤더에서 제공하고 있는 다양한 공격툴의 트래픽 패턴을 등록하여, 차단하기 위한 설정 내역과 모니터링 화면을 보여준다.

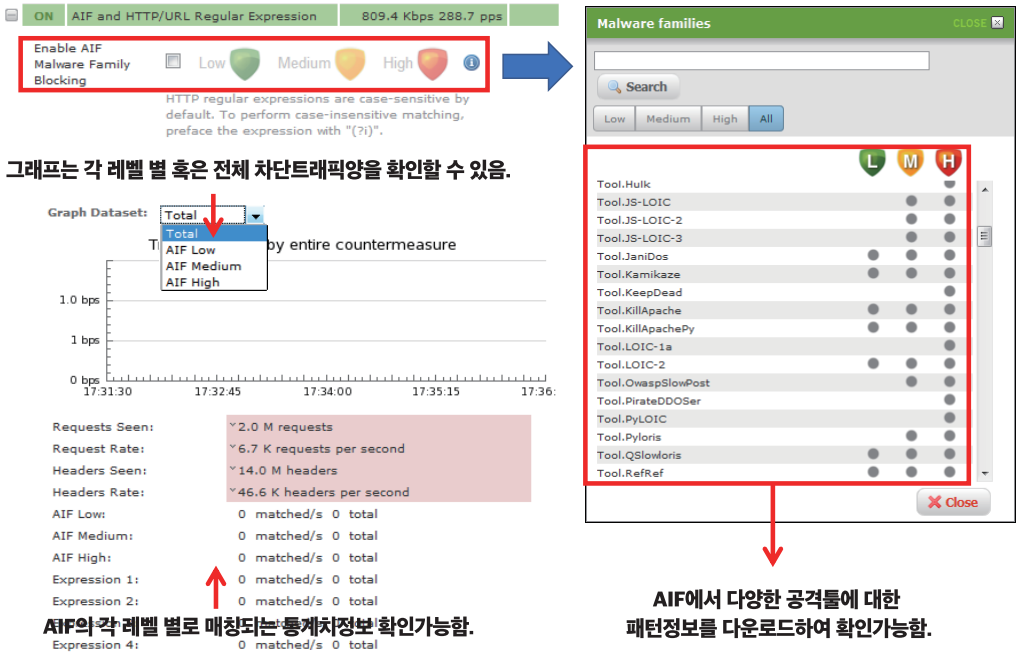

그림 9. 다양한 공격툴에 대한 패턴 리스트 및 공격 탐지 상태

최근 사무실에서 사용하는 전화기 라인이 UTP 라인으로 연결되어 있다면 기존의 전통적인 전화기가 아니고 IP 주소를 사용하는 VoIP 전화기라고 볼 수 있다. 이런 단말은 전화음성 혹은 화상회의 영상을 전달하기 위해 프로토콜(통신규약)이 필요한데 이때 가장 많이 사용되고 있는 것이 SIP(Session Initiation Protocol)이다. 이 프로토콜이 광범위하게 사용되면서 이 프로토콜도 DDoS 공격에 노출되어 있어, SIP 기반 DDoS 공격이 발생하면 전화는 물론 화상회의 등을 사용할 때 음성이나 화면이 끊어지거나 사용할 수 없게 된다. 이 공격도 HTTP, DNS와 동일한 방식으로 식별 차단이 가능하다. SIP Malformed 단계에서 표준에 위배되거나 비어있는 SIP 메시지를 식별하여 차단하게 되고, 다음으로 하나의 IP가 초당 100개의 과도한 SIP 메시지를 보낼 경우 공격으로 식별되어 차단이 가능하다.

이제 위의 모든 단계를 이용하여 차단을 수행하고 있는 상황에서도 서버로 트래픽이 과도하게 유입되고 있다면 마지막 수단으로 쉐이핑(shaping)을 사용할 수 있다. 이 단계는 보호 대상 서버가 감당할 수 있는 레벨의 트래픽 양만 전송하여 서버가 정상적인 응답이 가능하게 만들어 준다. 이 단계에서는 정상/비정상 트래픽을 구분하지 않고, 패킷을 랜덤하게 차단하여 서버로 가는 트래픽의 양을 설정값 이하로 강제로 낮추게 된다. 즉, 정상적인 트래픽도 차단이 되기 때문에 최후의 수단으로 사용할 수 있다. [그림 10]과 같이 최대 10개의 조건을 이용하여 트래픽 양을 줄일 수 있

다. 첫 번째 필터의 의미는 목적지 IP가 1.1.1.1이고 서비스 포트가 TCP80인 트래픽은 10bps 혹은 10pps까지의 양만 허용하고 그 이상의 트래픽은 차단하는 설정이다.

그림 10. 쉐이핑(Shaping) 설정 화면

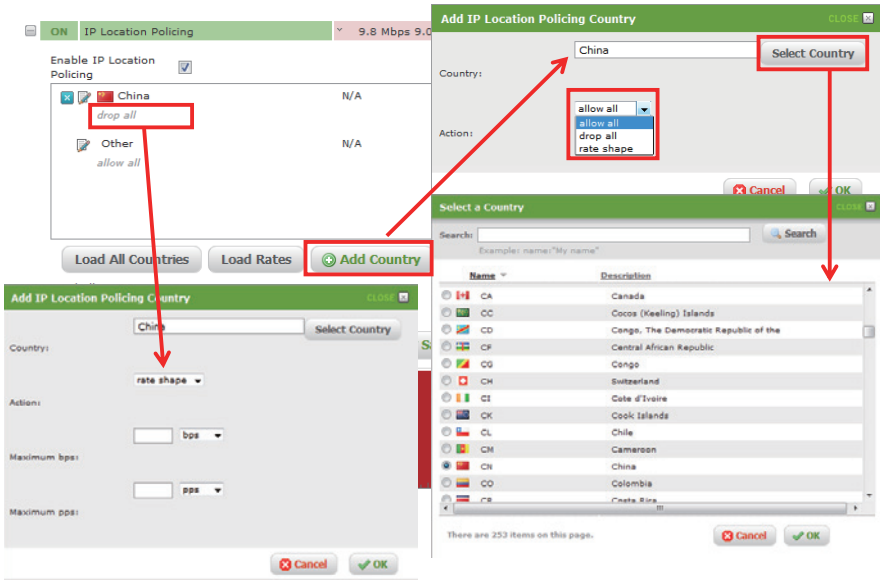

그림 11. 나라별로 트래픽을 모두 차단하거나 일정량으로 제한하는 설정 화면

쉐이핑의 두 번째 옵션은 나라 단위로 트래픽의 양을 제한할 수 있는 기능이다. [그림 11]과 같이 중국에서 오는 트래픽은 모두 차단하고 나머지 국가에서 오는 트랙만 통과시키거나 혹은 중국에서 오는 트래픽은 100Mbps 혹은 100kpps와 같이 특정량 이하로 트래픽 양을 제한할 수 있다. 중국 이외에도 북한이나 혹은 아프리카, 남미, 유럽의 나라처럼 각 조직에서 서비스하는 대상이 아닌 국가에서 오는 트래픽을 차단할 수 있는 옵션을 적용할 수 있다.

이상으로 DDoS의 마지막 편으로 공격 차단에 대해 설명해 드렸다. DDoS 공격이 다양화되면서 절대적인 하나의 방법으로 공격을 식별하고 차단하는 것은 불가능하게 되었다. 각각의 공격 특성에 효과적인 차단방식을 개발하여 순차적으로 적용하여 차근차근 공격 트래픽을 걸러 나가는 것이 효과적인 전략 중의 하나이기 때문에 이런 방법을 사용하는 것이지, 이 차단방식이 완벽한 방법이라고는 말할 수 없다.

앞에서 설명해 드린 여러 기능은 특정 벤더의 제품을 예로 들어 설명한 것으로, 모든 DDoS 방어 장비가 동일한 방식으로 공격을 차단하는 것은 아니다. 몇몇 기능은 공격 방어에 효과적이라 공통으로 많이 사용하는 단계가 있을 것이고, 또 다른 기능들은 특정 벤더에서만 고유하게 개발한 단계로 해당 벤더의 강점으로 내세우는 기능들도 있을 것이다.

모든 차단단계를 설명하기에는 지면의 한계가 있어서 여기서 줄이며, 다음 호에서는 DDoS 이후에 새로운 공격 패러다임으로 자리 잡고 있는 APT(Advanced Persistent Threat, 지능형 지속 공격)에 대해 알아보도록 하겠다.