방화벽 로그를 이용한 네트워크 공격유형 분석

윤성종, 김정호
한밭대학교 정보통신대학원 컴퓨터공학과
e-mail : yunsungjong@hanmail.net, jhkim@hanbat.ac.kr

Analysis of Network Attack Pattern using Firewall Log

Sung-Jong Yoon, Jeung-Ho Kim
Dept. of Computer Engineering, Hanbat National University

요 약

다양한 정보보호체계가 운영되고 있지만, 방화벽과 침입탐지시스템이 가장 많이 운영되고 있는 실정에서, 본 논문에서는 방화벽 관리자의 차단로그 분석을 효율적으로 지원하면서, 방화벽에 의해 차단되어 침입탐지시스템이 탐지하지 못해 관리자가 지나칠 우려가 있는 공격행위를 방화벽을 통해 인지할 수 있는 방안을 구성했다. 이를 통해 관리자는 침입탐지시스템과 함께 네트워크를 통한 스캔 및 DOS 등의 공격을 방화벽을 통해 인지할 수 있어 안정적인 네트워크 운영이 가능하다.

1. 서 론

현대 사회의 기반구조가 시공간적 제한이 있는 실환경에서 제한요인의 영향을 받지 않는 인터넷 기반의 가상환경으로 전환되고 있다. 이에 따라 다수의 사회 인프라가 가상환경 안에 현실과 동등한 수준으로 구축되었고, 사용자는 가상환경 안에서 자신이 필요한 정보를 획득하고, 이용할 수 있게 되었다. 그러나, 모든 정보가 집중되어 대단위로 이동하기 때문에 해킹과 같은 침해사고 발생시, 정보유출 및 유실에 따른 피해가 예전과는 비교할 수 없을 정도로 커지게 되었다.

이러한 피해를 예방하기 위해 다양한 방식의 정보보호체계가 구축되어 운영되고 있다. 현재, 많이 활용되고 있는 보호체계에는 침입차단시스템(방화벽), 네트워크용 침입탐지시스템(NIDS), 침입방지시스템(IPS), 바이러스 방역시스템(AVS) 및 이를 통합관리하는 통합관제시스템(ESM)이 있다. 그리고, 대규모 전산실이 아닌 곳에서 이러한 보호시스템을 구축하는 것은 비용대 효과측면에서 낭비이기 때문에 중·소규모의 전산실에서는 방화벽과 NIDS를 병행운영하면서, AVS 구축하고 있다. 그런데, 보호체계에서 생성된 탐지 로그를 종합해주는 ESM을 구비하지 않을 경우 보호체계 관리자는 침입 이벤트를 점검하는데 상당한 부담을 가질 수밖에 없다. 특히, 대부분의 방화벽에서 보여지는 로그의 형태가 단순히 패킷 차단 내역을 목록 상태로 보여주기 때문에, 관리자가 침입시도를 인지하기 위해서는 별도의 통계 S/W를 이용해야 한다. 이는 침해상태를 바로 알려주는 IDS 로그와 비교해 볼 때에 상대적으로 덜 중요하게 인식되는 요인이 된다.

그러나, 다음과 같은 이유로 방화벽의 차단로그는 NIDS의 탐지로그와 같이 중요하게 관리되어야 한다. 첫째, NIDS는 방화벽을 통과한 패킷을 대상으로 분석하기 때문에 방화벽에 의해 차단된 공격시도는 NIDS에 탐지되지 않는다. 둘째, NIDS는 순간 네트워크 소통량이 많을 경우 패킷 처리량의 한계로 탐지율이 70%~100% 정도에 머무르게 된다.[1] 따라서, 방화벽에서 불필요 패킷을 엄격하게 차단하고 선행 분석을 실시하여, NIDS의 패킷 처리량을 안정적으로 낮춰 NIDS의 탐지율을 높일 수 있도록 해야 한다.

따라서 본 논문에서는 방화벽 관리자의 침입 인지율 향상을 위해 방화벽 차단로그 분석결과를 기반으로 스캔, DOS 등의 네트워크 공격행위의 인지를 NIDS에 앞서 탐지해 안정적인 네트워크 운영을 보장하고자 한다.

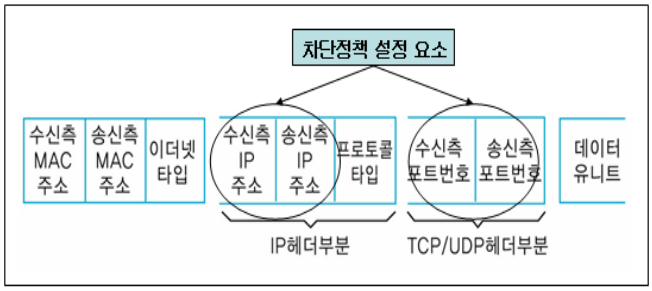
2. 방화벽의 기능과 차단정책

2.1 방화벽(Firewall)의 기능

방화벽은 관리자가 사전에 설정한 통제 정책에 따라 내·외부간 네트워크 트래픽을 제어한다. 이를 통해

방화벽의 가장 중요한 기능인 외부 네트워크로부터의 내부 네트워크 보호를 수행한다.[2]

방화벽의 통제 요소인 차단정책 설정 주요 요소로는 [그림 2-1]에서 보는바와 같이 '수신측 IP 주소', '수신측 포트 번호'와 '송신측 IP 주소', '송신측 포트 번호'가 있으며, 이외에도 사용자 등급, 접속시간 등이 사용될 수 있다.



[그림 2-1 패킷 내용]

방화벽의 주요기능은 다음과 같이 정리할 수 있다.[3]

- 외부의 불법침입으로부터 내부 네트워크 보호
- 비인가 된 서비스 접속 허용 및 차단
- 내·외부간 네트워크 소통을 원하는 사용자 통제
- 내·외부간 네트워크 트래픽 감시

2.2 차단 정책 설정

방화벽의 차단정책은 2.1에서 언급한 4가지의 주요 요소를 가지고 만들게 된다.

순번	출발지 IP	출발지 PORT	도착지 IP	도착지 PORT	프로토콜	허용 여부	사용자	허용 시간
1	any	any	1.1.1.1	80	TCP	허용	any	any
2	2.1.*.*	any	any	any	TCP	차단	any	any
3	3.1.*.*	any	any	any	TCP	허용	any	any
4	any	any	any	any	any	허용	any	any
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
99	any	any	any	any	any	차단	any	any

[그림 2-2 차단정책 내용]

[그림 2-2]는 차단정책 내용을 기록한 것으로서 해석하면 다음과 같다.

- 순번 1 : 외부 모든 IP는 내부 1.1.1.1의 80번 Port에 접근할 수 있다.
- 순번 2 : 외부 IP 2.1.1.1 ~ 2.1.255.255는 내부에 대한 모든 접근이 차단된다.

방화벽을 통과하려는 패킷은 상기와 같이 차단정책과 패킷의 해더 정보를 각각 비교한다. 만약, 2번행의 내용과 해더정보가 같다면 해당 패킷은 버려지게 되고, 1번 또는 3번행과 같다면 방화벽을 통과해서 내부로 들어오게 된다. 일치하지 않는 패킷의 경우에는 마지막 행인 99번에 의해 차단되어 버려지게 된다.[3]

차단정책 설정시 가장 주의해야 할 사항은 4번행과 같이 모든 패킷의 내부 유입을 허용하는 정책을 적용해서는 안된다는 것이다. 이러한 정책을 적용하게 되면 4번행 이후에 수립된 정책의 효력이 상실되기 때문이다. [그림 2-3]는 실제 방화벽의 차단로그를 보여주는 화면을 저장한 그림으로, '차단시간', '패킷종류', '허용여부', '방향성', '발신지주소', '수신지주소', '발신지포트', '수신지포트'의 항목이 저장되는 것을 볼 수 있다.

번 호	시 간	패킷종류	허용여부	방 향 성	발신지주소	수신지주소	발신지포트	수신지포트
257	2005/09/14 14:05:44	ICMP	차단	외==>내	67,2,1,21	48,1,1,14	3	
258	2005/09/14 14:05:44	UDP	차단	외==>내	48,16,1,176	48,1,2,79	1029	53
259	2005/09/14 14:02:24	ICMP	차단	외==>내	67,8,1,13	54,12,12,111	3	
260	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,14	1661	80
261	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,15	1662	80
262	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,13	1660	80
263	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,20	1667	80
264	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,21	1668	80
265	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,18	1665	80
266	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,19	1666	80
267	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,16	1663	80
268	2005/09/14 14:00:27	TCP	차단	외==>내	8,153,1,230	54,6,1,17	1664	80
269	2005/09/14 14:00:27	ICMP	차단	외==>내	67,3,1,9	54,6,5,252	3	
270	2005/09/14 14:00:27	ICMP	차단	외==>내	5,5,1,249	54,6,7,107	8	
271	2005/09/14 14:00:27	ICMP	차단	외==>내	67,3,1,9	54,6,6,23	3	
272	2005/09/14 14:13:23	TCP	차단	외==>내	48,2,126,12	54,9,12,63	2359	80
273	2005/09/14 14:03:53	TCP	차단	외==>내	54,2,4,42	54,8,11,98	2187	2186
274	2005/09/14 14:05:49	ICMP	차단	외==>내	67,2,1,21	48,1,1,14	3	
275	2005/09/14 14:05:49	UDP	차단	외==>내	48,16,1,176	48,1,2,79	1029	53
276	2005/09/14 14:02:29	ICMP	차단	외==>내	67,8,1,13	54,12,12,111	3	
277	2005/09/14 14:00:32	TCP	차단	외==>내	48,2,1,63	50,1,1,30	48759	34454
278	2005/09/14 14:00:32	TCP	차단	외==>내	8,153,1,230	54,6,1,22	1669	80
279	2005/09/14 14:00:32	ICMP	차단	외==>내	67,3,1,9	54,6,5,252	3	
280	2005/09/14 14:13:28	TCP	차단	외==>내	48,2,126,12	54,9,12,63	2359	80

[그림 2-3 차단로그 내용]

3. 차단로그를 활용한 공격유형 분석

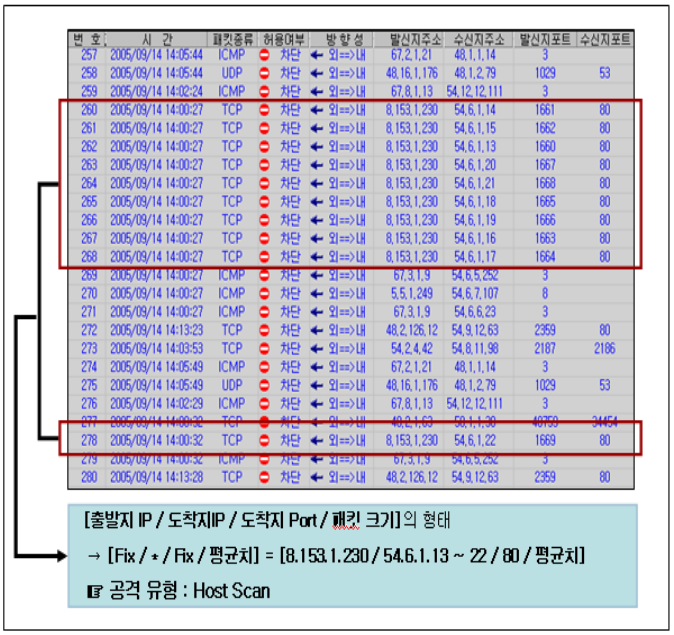
네트워크에서 소통되는 패킷 중에서 해킹 공격에 사용되는 유해 패킷을 '출발지 IP주소', '도착지 IP주소', '도착지 Port', '패킷크기'의 4가지 필드를 기준으로 분석하여 보면, [표 3-1]과 같은 공격 유형으로 구분되어 질 수 있다.[4]

공격형태	필드 구성				설 명
	출발지 IP	도착지 IP	도착지 Port	패킷 크기	
Dos	Fix	Fix	Fix	평균 이상	출발지가 일정한 DOS 공격
DDos	*	Fix	Fix	평균 이상	출발지가 다른 DOS 공격
Port Scan	Fix	Fix	*	평균치	도착지의 Port를 순차적으로 Scan
Host Scan	Fix	*	Fix	평균치	취약점을 지닌 Port를 보유한 Host를 찾기 위해 순차적으로 Scan
Worm Scan	*	*	Fix	특정값	웜을 전파하기 위한 취약점 Scan

[표 3-1 IP 해더정보에 따른 공격 유형]

위와 같은 공격 유형을 기반으로[그림 2-3]의 차단

로그를 분석할 수 있는데, 이를 통하여 스캔 및 DOS 공격 등을 탐지할 수 있다.



[그림 3-1 침입차단 로그 유형 분석]

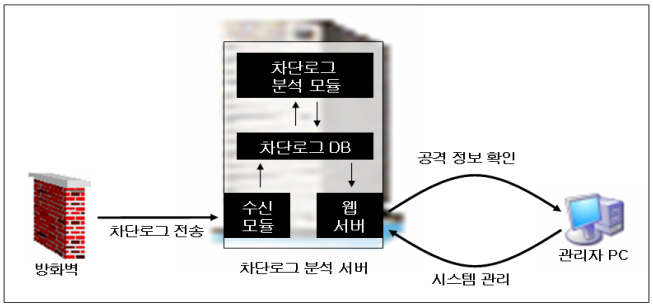
[그림 3-1]에서 보여지는 바와 같이 차단로그의 260~268번, 278번행을 살펴보면, 출발지 IP주소가 '8.153.1.230'이면서 도착지 Port번호가 '80번'으로 고정된 가운데 도착지 IP주소가 '54.6.1.13'에서 '54.6.1.22'로 변한 것을 볼 수 있다. 이를 공격 유형 정보와 비교해 보면 Host Scan 임을 판별할 수 있게 된다.

4. 공격 유형 분석

방화벽 차단로그를 활용하여 네트워크를 통한 공격 유형 분석을 위해서는 차단로그 중 공격 성향이 있는 패킷 정보를 식별하고, 이를 축약해서 시스템 구현에 필요한 최소한의 데이터만 제공하는 데이터 관리 기법이 요구된다. 본 논문에서는 DB에 저장된 차단로그를 대상으로 SQL 질의문을 적용하여 공격유형을 분석하는 방안을 제시하였다.

4.1 분석체계 구성

본 논문에서 시도된 구성도는 [그림 4-1]과 같다. [그림 4-1]에서 차단로그를 '분석서버'의 '수신모듈'로 전송하고, '수신 모듈'은 전송받은 로그를 '차단로그 DB'에 저장한다. DB에 저장된 차단로그는 '차단로그 분석모듈'에 의해 공격유형이 판별되고, 공격으로 판별된 정보는 다시 '차단로그 DB'에 저장되어 관리자가 웹서버를 통해 볼 수 있도록 설계되었다.



[그림 4-1 로그분석체계 구성도]

4.2 차단로그 분석모듈

방화벽 차단로그를 분석할 때, 차단로그 DB에 대한 효율적인 검색을 수행하기 위해서 공격 유형에 따라 분석에 필요한 필드값을 가지는 테이블을 [표 4-1]처럼 각각 구성할 필요가 있다. 이것은 한국전자통신연구원에서 개발한 상황인식 기반의 침입탐지 방법인 NASA(Network Attacks Situation Analysis)의 공격유형 중에서 차단로그를 활용해서 분석가능한 공격유형인 [1-2], [2-1], [2-4], [2-5]을 선택한 것이다.[4]

구 분	출발지 IP	도착지 IP	도착지 Port	탐지가능한 공격유형
TYPE_0	○	○	○	공격자 IP 및 대상자 IP/Port가 명확한 공격
TYPE_1	○		○	Host Scan, Worm Scan
TYPE_2	○	○		DOS
TYPE_3		○	○	Port Scan

[표 4-1 공격 유형에 따른 테이블 구성]

각 TYPE별 테이블 생성 방법은 다음과 같다. TYPE_0 테이블은 전체 차단로그DB 중 TCP와 UDP 패킷을 대상으로 추출하되, 위/아래 레코드가 같을 경우 카운터만 증가시키고, 하나로 합쳐 불필요한 정보의 차단로그를 제외한다. TYPE_1/2/3 테이블은 TYPE_0 테이블을 기반으로 생성하며, 각각 [표 4-1]의 해당 요소를 SELECT하여 [그림 4-2]와 같이 구성한다.

- **TYPE_0** : insert into TYPE_0_table
  select Protocol_type, 출발지 IP, 도착지 IP, 도착지 Port,
  sum(packet_num), sum(packet_size) from 차단로그 DB
  group by Protocol_type, 출발지 IP, 도착지 IP, 도착지 Port;
- **TYPE_1** : insert into TYPE_1_table
  select Protocol_type, 출발지 IP, 도착지 Port,
  sum(packet_num), sum(packet_size) from 차단로그 DB
  group by Protocol_type, 출발지 IP, 도착지 Port;
- **TYPE_2** : insert into TYPE_2_table
  select Protocol_type, 출발지 IP, 도착지 IP,
  sum(packet_num), sum(packet_size) from 차단로그 DB
  group by Protocol_type, 출발지 IP, 도착지 IP;
- **TYPE_3** : insert into TYPE_1_table
  select Protocol_type, 도착지 IP, 도착지 Port,
  sum(packet_num), sum(packet_size) from 차단로그 DB
  group by Protocol_type, 도착지 IP, 도착지 Port;

[그림 4-2 테이블 구성을 위한 SQL문]

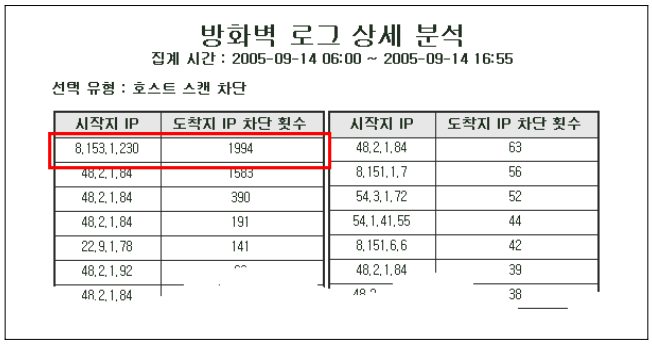
위와 같이 구성된 테이블을 대상으로 아래와 같이 SQL문을 주기적으로 실행하여, 차단로그에서 공격유형을 추출할 수 있다. [5,6]

- **DOS 공격 차단 유무 확인**
  : select 도착지IP, count(출발지IP) as cnt from TYPE_2_table
  group by 도착지IP having count(출발지IP) > 100
  order by cnt desc;
- **Port Scan 차단 유무 확인**
  : select 도착지IP, count(도착지Port) as cnt from TYPE_3_table
  group by 도착지IP having count(도착지Port) > 20
  order by cnt desc
- **Host Scan 차단 유무 확인**
  : select 출발지IP, count(도착지IP) as cnt from TYPE_2_table
  group by 출발지IP having count(도착지IP) > 20
  order by cnt desc
- **Worm Scan 차단 유무 확인**
  : select 출발지IP, 도착지Port, count(도착지Port) as cnt
  from TYPE_1_table, Worm_Port_table
  where TYPE_1_table.도착지Port = Worm_Port_table.port
  group by 출발지IP, 도착지Port having count(도착지Port) > 10
  order by cnt desc;

[그림 4-3 공격유형 분석을 위한 SQL문]

4.3 차단로그 분석 결과

위의 방식으로 [그림 2-3]의 차단로그 분석한 결과 [그림 4-4]와 같이 축약된 정보가 생성됨을 확인할 수 있게 되었다. 분석된 결과를 보면 '8.153.1.230'에서 총 1994건의 Host Scan이 차단됨을 알 수 있다.



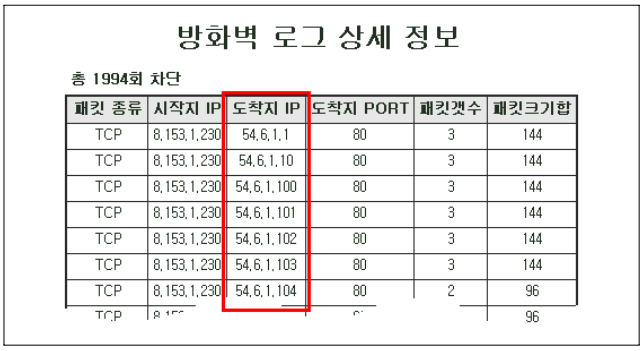
방화벽 로그 상세 분석

집계 시간 : 2005-09-14 06:00 ~ 2005-09-14 16:55

선택 유형 : 호스트 스캔 차단

시작지 IP	도착지 IP 차단 횟수	시작지 IP	도착지 IP 차단 횟수
8.153.1.230	1994	48.2.1.84	63
48.2.1.84	1583	8.151.1.7	56
48.2.1.84	390	54.3.1.72	52
48.2.1.84	191	54.1.41.55	44
22.9.1.78	141	8.151.6.6	42
48.2.1.92		48.2.1.84	39
48.2.1.84			38

[그림 4-4 차단로그 분석 결과]



방화벽 로그 상세 정보

총 1994회 차단

패킷 종류	시작지 IP	도착지 IP	도착지 PORT	패킷갯수	패킷크기합
TCP	8.153.1.230	54.6.1.1	80	3	144
TCP	8.153.1.230	54.6.1.10	80	3	144
TCP	8.153.1.230	54.6.1.100	80	3	144
TCP	8.153.1.230	54.6.1.101	80	3	144
TCP	8.153.1.230	54.6.1.102	80	3	144
TCP	8.153.1.230	54.6.1.103	80	3	144
TCP	8.153.1.230	54.6.1.104	80	2	96
TCP					96

[그림 4-5 세부 차단정보]

5. 결론 및 향후 연구

본 논문에서는 방화벽 차단로그를 이용하여 네트워크 공격행위를 인지함에 따라 안정성이 보유된 운영을 제안했다. 이를 통해 방화벽 관리자는 효율적인 차단로그와 스캔/DOS/Worm 등의 공격을 쉽게 인지할 수 있게 되었다. 이것은 방화벽에 의해 차단되어 NIDS가 탐지하지 못해 관리자가 지나칠 우려가 있는 공격행위를 인지시켜준다는 측면에서 의의를 찾을 수 있다.

또한, 본 논문에서 제안하는 DB Query문을 이용한 차단로그 분석은 대용량의 로그를 실시간으로 분석할 때와 TCP 80/135/139/445/3127번 Port를 순차적으로 스캔하는 Agobot 웜 같은 악성 패킷을 찾고자 할 때에는 제한이 따른다. 향후, 이를 보완하기 위한 데이터 마이닝 기법 중에서 대량의 데이터들의 상관관계를 처리하여 불규칙성 속에서 새로운 특징을 추출하는 연관규칙(association rule) 기법을 이용한 차단로그 분석 연구가 요구된다.

참 고 문 헌

[1] 문종욱외 5명, "IDS의 성능 향상을 위한 패킷 폐기 방안", 정보처리학회논문지, 8. 2002.
[2] 국가사이버안전센터, "방화벽 관리 및 침입기록 분석 방법", 5. 2005.
[3] "최신 정보보호개론", 홍릉과학출판사, 2005.
[4] 국가보안기술연구소, "테이터마이닝을 이용한 침입 이벤트 분석 기술", 9. 2004.
[5] 소진, 이상훈, "연관 규칙을 이용한 네트워크 기반 침입 탐지 패턴생성 기술", 한국정보과학회논문지, 11. 2002.
[6] 유일선, 조경산, "네트워크 취약점 검색공격에 대한 개선된 탐지시스템", 정보처리학회논문지, 10. 2001.