# 지능형 ATM 방화벽의 설계

○
서 병 기, 김 태 연†
서남대학교 전산정보학과†

# A Design for an Intelligent ATM Firewall

**Byung_Gi Seo† Tae_Yeon Kim†**
*Dept. of Computer Science and Information Communications, Seonnam University†*

## 요 약

본 논문에서는 정보의 비밀성과 지능적인 접근제어가 제공되는 방화벽의 구조에 대해서 기술한다. 몇몇 연구에서는 서비스의 중요도에 따라 선별적으로 패킷을 검사하는 방법을 채택하고 있기 때문에 정당한 사용자가 서비스를 효율적으로 사용하는데 적잖은 제약을 받게 된다. 따라서 보안 접근제어가 서비스의 중요도와 사용자의 보안등급, 사용자의 신뢰도, 그리고 침입 탐지에 관한 정보에 따라 이루어지도록 하였다. 지능형 방화벽은 다양한 정보에 따라 다른 퍼지 제어 규칙을 사용하여 안전한 서비스를 보장하고 정당한 사용자의 서비스 사용율을 극대화한다.

## 1. 서 론

인터넷의 상업성과 광대역 망 기술이 발전함에 따라 다양한 장비 및 서비스개발에 대한 연구가 활발히 진행 중에 있다. 특히, ATM과 같은 광대역 서비스의 출현은 음성뿐만 아니라 비디오, 데이터, 트랜잭션 처리 등에 많은 영향을 주었다. 따라서 ATM 망과 기존의 인터넷간에 호환성도 보장되어야 한다. 또한 이러한 구조에 귀중한 정보를 보호할 수 있도록 보안 메카니즘이 요구된다. 망과 망 사이에 보안 메카니즘을 첨가하더라도 종단 사용자에 대해 투명하여야 하고, 기존의 스위치 망 서비스에 seamless하게 연결되어야 한다.

본 논문에서는 정보의 비밀성과 지능적인 접근제어가 제공되는 방화벽의 구조에 대해서 기술한다. 제안된 방법은 기존의 구조에 비해 더 강한 접근제어를 수행하는 구조로 간주된다. 망 보안은 데이터의 비밀성과 신뢰되지 않는 망으로부터 접근을 고려한다. 비밀성은 중요한 데이터가 비 인가된 사용자에 노출을 막는 것이기 때문에 데이터의 암호화에 의해서 보장될 수 있다. 접근제어는 신뢰되지 않는 망으로부터 신뢰된 망으로의 접근을 막기 위해서 사용자를 인증해야할 뿐만 아니라 전송되고 있는 서비스를 감시하는 장치에 의해서 호스트간에 신뢰된 연결과 안전한 서비스를 보장하는 기능을 수행할 수 있다.

ATM 포럼에서는 방화벽을 통과하는 모든 패킷의 내용을 검사하는 것을 지양하고 있다. 기존의 연구들은 서비스의 중요도에 따라 선별적으로 패킷을 검사하는 방법을 채택하고 있어 정당한 사용자가 서비스

를 효율적으로 사용하는데 적잖은 제약을 받게 된다. 따라서 보안정책을 수행하는데 있어서 지능적인 기능이 지원될 수 있는 방화벽을 사용하여 서비스의 중요도에 관계없이 정당한 사용자에게는 양질의 서비스를 지원할 수 있어야 한다. 본 논문에서 제안한 지능형 방화벽은 다양한 정보에 따라 다른 퍼지 제어 규칙을 사용하여 안전한 서비스를 보장하고 정당한 사용자에게는 서비스 사용율을 극대화한다.

2장에서는 트래픽 필터링 서비스와 퍼지 제어규칙을 서술하고, 3장에서는 개선된 ATM 방화벽 구조를 기술하며 마지막으로 4장에서는 결론을 기술한다.

## 2. 트래픽 필터링 서비스와 제어규칙

### 2.1 트래픽 필터링 서비스

일반적으로 패킷 필터링은 라우터에서 필터링 규칙에 따라 처리하는 메카니즘이다. 패킷이 패킷 필터링 라우터에 도착하면 패킷 해더로 부터 정보(송신측 주소와 수신측 주소, 송신측과 수신측 TCP/UDP 포트, ICMP 메시지 타입, 켑슐화된 프로토콜 정보)를 추출하여 패킷을 전달할 것인지 폐기할 것인지를 결정하는 하는 기능을 수행한다. 이러한 기능은 방화벽에서 구현될 수도 있고 서버에 의해서 구현될 수 있다.

패킷 필터링 규칙은 다음과 같은 망 보안 정책을 기반으로 한다.

[정책1] 명시적으로 허용하지 않는 모든 트래픽은 거절한다.

[정책2] 명시적으로 거절하지 않는 모든 트래픽은 허용한다.

보안 정책에 의해서 필터링하는 방법은 서비스 종류에 의한 필터링과 송신측과 수신측 주소에 의한 필터링, 보안 메카니즘에 의한 필터링, 그리고 패킷의 페이로드 검사등을 포함한 혼합 방법에 의한 필터링이 있다.

### 2.2. 퍼지 제어 규칙

자원의 접근 여부에 대한 판단은 서비스의 중요도와 사용자의 보안등급, 사용자의 신뢰도, 그리고 모니터링 결과에 의한 위반감지와 시스템에 대한 침입 탐지기에 의한 시스템의 침입탐지 결과에 의해서 이루어진다. 여기에서 사용자의 보안 등급과 사용자 신뢰도는 고정적인 값이 아닌 동적인 값으로 정의하고, 사용자의 보안 등급은 모든 망에서의 신용을 나타내는 것으로 인증서버에 의해서 발급되며, 사용자 신뢰도는 특정 망에 대한 신용을 나타내는 것으로 방화벽이 독자적으로 관리하기 때문에 별개의 것으로 간주한다. 퍼지 제어기는 목적지 서버의 사용에 있어서의 사용자 신뢰도와 다른 사용자들에 의한 서버의 침입 상황들을 수치화하여 오차의 변환분을 계산하고 퍼지화를 수행한다. 즉, 입력 데이터를 적절한 언어적인 값으로 변환시킨다. 서비스의 중요도는 "low"와 "medium", "high" 등의 언어적 변수를 사용하고, 사용자의 보안 등급은 인증 증명서에 의해서 기록된 것으로 "low", "medium", "high" 등의 변수를 사용하고, 사용자의 신뢰도는 "zero"와 "low", "medium", "high" 등의 언어적 변수를 사용하며, 침입 탐지에 관한 정보는 탐지되지 않는 경우와 무시할 수 있는 경우, 다소 문제가 발생한 경우, 치명적인 경우를 "zero"와 "low", "medium", "high" 등의 변수를 사용한다.

출력 퍼지 값은 실제 제어 입력 전체 집합에 맞게 변환시켜야 한다. 즉, 비 퍼지화(defuzzify)는 무게중심법을 이용하여 실제 제어 입력으로 사용할 수 있는 명확한 비 퍼지 값으로 변환시킨다[1,2].

본 논문에서 사용된 퍼지 규칙은 식(1)과 같은 "if - then" 형식의 규칙으로 구성된다.

규칙 : If <u>보안등급</u> and <u>신뢰도</u> and <u>침입탐지</u> then <u>출력변수</u> (1)

예를 들어 서비스의 소속 정도 값이 medium인 경우에 표1과 같이 퍼지 제어 규칙을 따라 필터링 정책을 수행한다. ANY는 침입탐지의 모든 경우를 나타낸다.

위 규칙들의 기본 개념은 서비스 질이 낮은 경우에 목적지 서버 망에 침입이 확인되면 모든 사용자의 패킷을 검사하고, 서비스 질이 높더라도 목적지 서버 망에 침입 흔적이 없는 경우나 클라이언트 측의 사용자 보안 등급이 낮고 사용자 신뢰도가 높으면 패킷을 필터링하지 않고 그대로 전송하는 것이다. 이러한 제어 규칙에 의한 출력 변수는 P(pass)와 M(monitoring), F(filtering), X(proxy)로 정의하였다.

표 1. 퍼지 제어 규칙 예

| 번호 | 보안등급 | 신뢰도 | 침입 탐지 | 출력변수 |
|---|---|---|---|---|
| 1 | low | low | ANY | X |
| 2 | low | medium | zero. low | F |
| 3 | low | medium | medium, high | X |
| 4 | low | high | zero, low, medium | F |
| 5 | low | high | high | X |
| 6 | medium | low | zero, low, medium | F |
| 7 | medium | low | high | X |
| 8 | medium | medium | zero | M |
| 9 | medium | medium | low,medium | F |
| 10 | medium | medium | high | X |
| 11 | medium | high | zero | M |
| 12 | high | high | low | P |
| 13 | medium | high | medium, high | F |
| 14 | high | low | zero, low | M |
| 15 | high | low | medium, high | F |
| 16 | high | medium | zero, low | P |
| 17 | high | medium | medium | M |
| 18 | high | medium | high | F |
| 19 | high | high | zero, low, medium | P |
| 20 | high | high | high | M |

# 3. 개선된 ATM 방화벽의 구조

개선된 ATM 방화벽의 물리적인 구조는 그림 1과 같이 트래픽 모니터링 서버와 필터링 서버, Proxy 서버, 방화벽 관리 서버로 구성되어 있다.

### 3.1 트래픽 모니터링 서버

트래픽 모니터링 서버는 퍼지 제어 규칙에 따라 전송되고 있는 패킷의 헤더 정보(송신자 IP 주소, 수신자 IP 주소, TCP/UDP 송신 포트, TCP/UDP 수신 포트, 프로토콜 서비스, ICMP 메시지 유형)를 필터링하는 역할을 한다. 다시 말해서 전송중인 셀을 패킷 단위로 조립한 다음 헤더 부분만을 복사한 다음 즉시 헤더를 포함한 모든 셀을 전송하고, 헤더 정보를 분석하여 보안을 위반했는지를 모니터링하는 방식이다. 보안에 위반된 경우에는 침입 정보를 방화벽 관리 서버에 전달하여 조치를 취할 수 있도록 한다. 트래픽 모니터링 서비스는 패킷을 보낸 후 보안 검사를 하기 때문에 침입을 사전에 막을 수는 없고 사후처리에 국한된 방법이다.

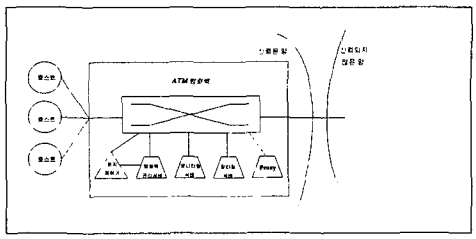


그림1. 개선된 ATM방화벽의 물리적인 구조

### 3.2 패킷 필터링 서버

패킷 필터링은 트래픽 모니터링 서비스와 같이 퍼지 제어 규칙에 따라 전송되고 있는 패킷의 헤더 정보를 필터링 하지만 패킷의 마지막 셀을 보내지 않는 방식이다. 다시 말해서 전송중인 셀을 패킷 단위로 조립한 다음 헤더 부분을 필터링하는 것은 유사하지만 보안을 위반하지 않는 경우에 마지막 셀을 전송하고 위반한 경우에는 셀을 폐기한다. 필터링하는 시간만큼 셀이 지연되는 문제가 발생하지만 보안에 위반한 경우에는 마지막 셀을 폐기함으로써 침입을 막을 수 있게 된다.

### 3.3 응용 수준 게이트웨이(Proxy)

응용 수준 게이트웨이는 목적지 서버에 전달되기 전에 패킷의 헤더뿐만 아니라 패킷의 페이로드(서비스의 내용)를 퍼지 제어 규칙에 따라 필터링하여 망 간에 데이터 트래픽을 제어하는 역할을 한다. 게이트웨이를 통과하는 특정 서비스를 관리하기 위해서 Proxy 코드가 게이트웨이 서버에 설치된다. 따라서 Proxy는 클라이언트에 대해서는 서버의 역할을, 목적지 서버에 대해서는 클라이언트의 역할을 한다. Proxy의 기능은 클라이언트와 목적지 서버의 관점에서는 투명하게 이루어진다.

### 3.4 방화벽 관리 서버

방화벽 관리 서비스는 다른 방화벽 보안 서버를 제어·관리하고 침입 탐지기에 의해서 탐지된 침입 정보를 관리하며, 망 관리자에 사용자에 관련된 관리 도구를 제공한다. 이러한 도구는 사용자의 비정상적인 활동을 감시하고 보안 정책을 위반한 사용자의 연결 설정을 중지시키는 기능을 수행한다.

방화벽 관리 서버는 보안 정책의 위반에 사항과 연결설정에 관한 프로파일 정보를 기록 보관한다. 보안 정책의 위반에 사항은 시그널 메시지 처리 과정에서의 보안 위반 정보나 트래픽 모니터링 서버와 필터링 서버, Proxy 서버에 의해서 탐지된 안전하지 않는

패킷 정보와 침입 탐지기에 의해서 탐지된 침입 정보 등이다. 이러한 정보는 어떠한 유형의 침입이 있는지의 분석하는데 사용된다. 연결설정에 관한 프로파일 정보는 통신하고자하는 클라이언트와 목적지 서버의 식별자와 연결 설정의 시작과 종료 시간, 한 주기 동안 전송된 셀의 수 등이 포함된다. 이러한 정보로서 각 클라이언트로부터 불법적인 접근 유형이나 언제 연결설정을 얼마나 많이 요구하고 어느 시간대에 얼마나 많은 량의 데이터가 전송되었는지를 분석할 수 있기 때문에 특정 클라이언트의 접근에 대해서는 더 강한 접근 정책을 수행할 수 있다.

### 3.5 방화벽 알고리즘

전송되는 패킷에 대한 보안 검사를 하는 알고리즘은 그림 2와 같다.

```
while ()
{
  scan (1'st cell of packet)
  if a cell is 1'st cell
    switch (kind of packet)
    {
      signaling : check (s1, s2, p, AH, .. )
                  save s1 ,s2, p
                  pass a cell
      information : defuzzify (출력변수)
      switch (출력변수)
      {
       P : pass all the cells
       M : pass all the cells
           extract (1'st cell of packet)
           check (s1, s2, p, AH, .. )
           if not validate
              notify firewall manager
       F : pass all the cells except last cell
           extract (1'st cell of packet)
           check (s1, s2, p, AH, .. )
           if not validate
             notify firewall manager
             drop the last cell
                 else pass the last cell of a
                          packet
        X :  assemble all the cells
             check (s1, s2, p, AH,  .. ,
                    Payload)
             if not validate
                notify firewall manager
                drop the packet
             else pass all the cells

      }
  }
}
```

그림 2. 방화벽 알고리즘

## 4. 결 론

패킷 필터링 라우터에서의 SAR의 처리로 인한 지연이 발생하기 때문에 ATM 포럼에서는 호 연결 설정 시에만 접근 제어를 수행하도록 권고하고 있지만 망을 보호하는데 많은 문제가 발생한다. 따라서 신뢰되지 않는 망들로부터 안전한 망으로의 접근을 효율적으로 막기 위해서는 패킷 필터링 ATM 방화벽이 필수적이다. 그러나 특정 서비스의 내용을 필터링할 수 없기 때문에 완벽한 방화벽의 역할을 할 수 없다. 그리고 기존의 필터링 방화벽은 서비스 종류와 사용자 수준의 제어만을 지원하고 있지만 시스템의 침입 상태 등에 관해서는 고려하고 있지 않고 있다. 따라서 본 논문에서는 응용 수준의 필터링과 현재 망의 불확실하고 애매한 환경을 고려하여 안전하게 망을 보호할 수 있는 지능적인 ATM 방화벽을 설계하였다.

### 참 고 문 헌


[1] Hans Hellendoom, Christoph Thomas, "Defuzzification in fuzzy Controller", Journal of Intelligent and Fuzzy Systems, Vol.1, pp.109-123, 1993.

[2] Kickart, W. J. M. and Mandani, E. H., "Analysis of fuzzy logic controller", Fuzzy sets and system, Vol.1, No.1, pp.29-44,1978.

[3] J. Hughes, "A High Speed Firewall Architecture for ATM/OC-3c", StorageTek Corp., MN, 1996 : http://www.network.com.

[4] T. Smith, and J. Stidd, "Requrements and Methodlogy for Authenticated Signaling", ATM Forum/94-1213.

[5] L. Pierson, and T. Tarman, "Requirements for Security Signaling", ATM Forum/95-0137.

[6] T. Tarman, "Phase I ATM Security Specification", ATM Forum BTD-SECURITY -01.13, July, 1997.

[7] Secant Network Technologyies Inc., "Encrypting ATM Firewall", Celotek Corporation Research Triangle Park, NC: http://www.celotek.com.

[8] 서병기, 김태연, "패킷 필터링을 지원하는 ATM 방화벽", 한국정보처리학회 추계 학술발표논문집, 제6권 제 2호, 1999