셀 스크리닝 방식에 기반한 ATM Firewall Switch의 설계

홍 승 선[†] · 정 태 명[††] · 박 미 룡[†††] · 이 종 협[†††]

요 약

기존의 라우터 기반의 패킷 스크리닝 방식은 ATM 네트워크 상에서는 패킷 수준의 스크리닝 기능의 적용을 위하여 SAR(Segmentation And Reassembly) 과정을 필요로 하기 때문에 고속의 셀 처리를 수행하는 ATM Switch의 셀 처리 속도를 저하시킨다는 문제점을 안고 있다. 본 논문에서는 셀 스크리닝 방식에 기반한 병렬 처리 구조의 ATM Firewall Switch를 제안한다. 제안된 Enhanced ATM Firewall Switch는 셀 단위로 분할된 패킷의 1, 2번 셀들에 대한 검사만을 통하여 스크리닝 기능을 수행하기 때문에 셀 단위의 스크리닝 수행이 가능하며, 정책 캐쉬의 도입을 통해 셀 스크리닝 수행 속도를 향상하였다. 또한 독립적인 User Cells Filter 기능 블록의 설계를 통하여 병렬 처리 구조의 셀 스크리닝 수행이 가능하도록 구성하여 셀 지연 시간을 최소화하였다.

A Design of ATM Firewall Switch using Cell Screening

Seung S. Hong[†] · Tai M. Chung[††] · Mi-Ryong Park[†††] · Jong-Hyup Lee[†††]

ABSTRACT

A Router-based packet screening has the problem of increasing the cell processing time of an ATM switch which performs high-speed cell transmission because it incurs the overhead of SAR (Segmentation and Reassembly) to apply the packet-level filtering policy to ATM cells. In this paper, we propose the parallelized ATM Firewall Switch designed to perform the high-speed cell screening. The proposed Enhanced ATM Firewall Switch filters packets by looking up only the first two cells of a packet and improves the speed of cell screening process using the policy cache. Furthermore, the independent design of User Cells Filter functional block makes it possible to parallelize the cell screening processes. We expect that the Enhanced ATM Firewall Switch will not only increase scalability but also reduce the cell delay caused by the cell screening.

키워드 : ATM, Firewall(방화벽), Cell Screening(셀 스크리닝), Policy Cache(정책 캐쉬)

1. 서 론

ATM 기술이 고속의 네트워크와 다양한 형태의 네트워크 서비스를 지원하기 위한 주요 인프라 구조로서 자리잡음에 따라, 전통적인 TCP/IP 기반의 네트워크 서비스들을 ATM 네트워크 상에서 지원하기 위한 많은 노력이 이루어져 왔으며[1-5]. 이러한 노력들에 의하여 기존의 IP 네트워크에서 제공되던 서비스들이 ATM 네트워크 상에서도 제공 가능하게 되었다.

그러나, 인터넷과 같은 공중망이 가지고 있는 보안상의 문제점들이 ATM 네트워크에서도 여전히 문제점으로 제기되고 있는 상황이며, 이에 반해 ATM 네트워크 보안과 관련된 연구는 ATM 네트워크의 확산 속도에 미치지 못하는 실정이다. 뿐만 아니라, 보안 문제와 관련하여 상대적으로 많은 연구가 이루어진 IP 네트워크의 보안 기술은 ATM 기반의 네트워크에서는 기술적인 차이로 인하여 적용 불가능하다는 문제점을 안고 있다.

ATM Forum에서는 ATM Security Specification version 1.0 [6]에 명시된 것과 같이 암호와 기술과 인증 기술에 기반한 데이터 보호 기술을 통하여 ATM 보안 문제를 해결하고자 하였다. 이는 기존의 IP 기반의 네트워크 보안 기술이 암호화 및 인증 기술뿐만 아니라, 침입 탐지 및 차단 기술까지 광범위하게 연구 개발되어 있는 현실과 비교해 볼 때, ATM 네트워크에 적용 가능한 보안 기술의 한계성을 나타내는 예라고 할 수 있다.

IP 네트워크의 보안 기술인 침입 차단 기술은 네트워크의 경계에 위치하면서 이 지점을 거친 연결을 보안 정책에 따라 허가하거나 거부하는 방식을 통해 네트워크를 물리적으로 차단함으로써 불법적인 외부의 침입으로부터 내부의 네트워크

† 준 회 원 : 성균관대학교 대학원 전기전자및컴퓨터공학부
†† 종신회원 : 성균관대학교 전기전자및컴퓨터공학부 교수
††† 정 회 원 : 한국전자통신연구원
논문접수 : 2000년 11월 29일, 심사완료 : 2001년 6월 20일

를 보호하는 기술이다. 이러한 목적으로 정의된 시스템을 침입차단시스템 또는 방화벽(Firewall)이라 하며, 패킷 필터링(Packet Filtering) 또는 패킷 스크리닝(Packet Screening) 기술과 프락시(Proxy) 기술이 침입차단시스템의 기반 기술로 이용되고 있다.

현재 가장 광범위하게 적용되고 있는 라우터 기반의 패킷 스크리닝 기술은 인가되지 않은 연결로부터 네트워크를 보호하기 위한 효율적인 방법으로 알려져 있다. 그러나, 전통적인 라우터 기반의 패킷 스크리닝 기술이 ATM 네트워크에 적용되는 경우, 다음과 같은 문제점을 초래한다. 우선, ATM 네트워크 상에서 패킷 스크리닝 기술을 적용하는 경우에는 패킷 스크리닝 기술의 적용을 위하여 해당 IP 패킷을 셀로부터 추출해야 하기 때문에 종단 시스템간에 구성되는 ATM 연결이 단절되는 결과를 초래한다. 또한 패킷 스크리닝을 위한 IP 패킷의 추출 과정은 셀에 대한 대량의 SAR (Segmentation And Reassembly) 과정을 필요로 한다는 점에서 ATM 스위치에 오버헤드로 작용하게 된다.

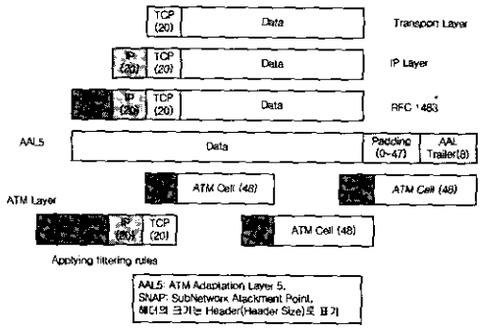
둘째로, ATM 네트워크가 고속의 데이터 전송을 수행하는 반면, 현재 적용되고 있는 패킷 스크리닝 기술의 처리 속도는 한계성을 보인다는 점이다. 일반적인 ATM 전송 속도는 OC-3c의 경우 155Mbps, OC-12c의 경우 622Mbps에 이르고 있지만, 일반적인 Firewall의 경우 100Mbps 이상의 대역폭을 갖는 네트워크 상에서 처리 속도의 한계성을 나타냄으로써 ATM 네트워크의 처리 속도를 저하시킨다. 이러한 현상은 대부분의 Firewall 시스템이 보안 정책 기반으로 동작하고, 패킷에 대한 스크리닝 여부를 결정하기 위해서는 Firewall 시스템이 관리하는 정책과의 비교 과정이 반드시 필요하기 때문이다. 따라서, 보안 정책 항목수의 증가는 Firewall 시스템의 처리 속도 저하와 직결되는 문제점을 내포하고 있다. 이와 같은 이유로 인하여 패킷 스크리닝 기술에 기반한 전통적인 라우터 기반의 Firewall 시스템은 ATM 네트워크에서는 적용하기 힘든 기술로 인식되고 있으며, ATM 네트워크에 적용 가능한 새로운 ATM Firewall의 구조를 필요로 한다.

본 논문은 ATM 네트워크에 적용 가능한 Enhanced ATM Firewall Switch를 설계, 제안함으로써 기존의 Firewall 시스템의 문제점을 해결하고자 한다. 제안된 Enhanced ATM Firewall Switch는 기존의 라우터 기반의 Firewall 시스템의 패킷 스크리닝 기술을 셀 스크리닝 기술로 대치시킴으로써, 처리 속도의 향상과 불필요한 SAR 과정을 제거할 수 있도록 구성되었다. 본 논문에서는 2장을 통하여 ATM Firewall 시스템의 연구 동향에 대하여 기술하며, 3장에서는 Enhanced ATM Firewall Switch의 구조에 대하여 기술한다. 마지막으로 본 연구를 통하여 추출된 결론과 향후 계획을 4장을 통하여 기술한다.

2. ATM Firewall Switch의 연구 동향

현재 ATM Firewall Switch에 대한 연구 동향은 Firewall 시스템의 기반 기술 가운데 패킷 스크리닝 기술에 주력하고 있는 경향을 보이고 있는데, 이는 기존의 라우터 기반의 Firewall 시스템들이 대부분 패킷 스크리닝 기술을 통하여 접근 제어를 수행하기 때문이다. 그러나, 패킷 스크리닝의 도입이 기술적인 이유로 ATM 네트워크에 적용하는 것이 비효율적이기 때문에 새롭게 셀에 기반한 셀 스크리닝 방식에 고안되었다[7].

셀 스크리닝은 전통적인 패킷 스크리닝 방식이 ATM 네트워크에 적용되는 경우에 발생하는 셀들에 대한 재조합(Reassembly)과 분할(Segmentation) 과정을 최소화함으로써 셀 지연 시간을 줄일 수 있다. (그림 1)은 셀 스크리닝 방식의 적용 방식을 간략히 도시한 것이다.



(그림 1) 셀 스크리닝 방식의 필터링

TCP/IP 계층을 통하여 생성된 IP 데이터그램은 Classical IP over ATM(CLIP) 프로토콜 스택에 의하여 8 바이트의 SNAP(SubNetwork Attachment Point) 헤더가 추가된다[8]. SANP 헤더가 추가된 IP 데이터그램은 AAL5 프레임으로 캡슐화되기 위하여 패딩과 트레일러가 추가된다. 생성된 AAL5 프레임은 정확히 48 바이트의 배수 크기를 갖는 프레임으로 구성되고, ATM Layer에 의하여 48바이트 크기의 셀로 분할되며, 분할된 셀에 ATM 헤더가 추가되어 가상 회선(Virtual Circuit)을 통하여 전송된다. 분할된 IP 데이터그램의 마지막 셀은 셀 헤더의 Payload Type 필드에 표시하여, 이 정보를 이용하여 셀의 재조합 과정을 거치지 않아도 데이터그램들의 경계를 알 수 있다.

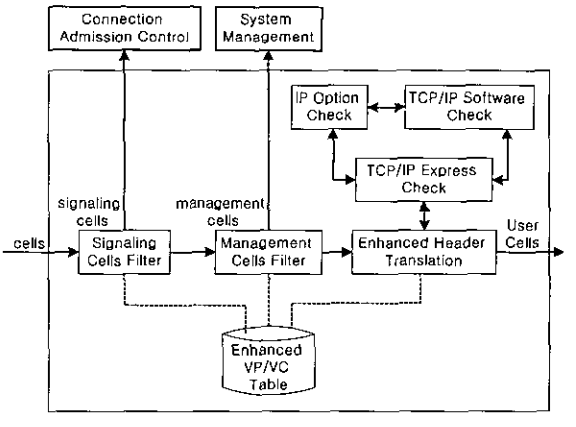
셀 스크리닝 방식에서는 유입되는 셀에 대하여 첫 번째 셀 정보만을 이용하여 필터링 규칙을 적용할 수 있는데, 이는 첫 번째 셀에 필터링 규칙의 적용을 위해 사용되는 20 바이트의 IP 헤더와 TCP 헤더가 모두 포함되기 때문이다. 셀 스크리닝은 데이터그램의 첫 번째 셀을 필터링 규칙에 적용해 봄으로써 셀이 속한 데이터그램에 대한 허가 여부를 판단할 수 있으며, 이러한 과정을 통하여 셀에 대한 SAR 과정을 생략할 수 있다.

이와 같은 셀 스크리닝 방식에 기반하여 제안된 ATM Firewall 시스템으로 StorageTek사에서 설계한 ATLAS (ATM Line Access & Security system)가 있다[9]. ATLAS는 셀 스크리닝에 기반하고 있으며, 정책 캐쉬를 사용한 시스템이다. 정책 캐쉬는 VPI/VCI, 근원지와 목적지의 IP 주소, 그리고 근원지 목적지 포트번호로 구성되며, 유입된 첫 번째 셀 정보와 일치하는 정보가 정책 캐쉬에 있는 경우에는 셀을 통과시킨다. 만일 첫 번째 셀 정보와 일치하는 정보가 정책 캐쉬에 존재하지 않는다면, 소프트웨어 스크리닝 프로세스에게 접근 제어 여부를 결정하도록 요구하고, 접근 제어 여부가 결정되기 이전에 도착하는 동일 데이터그램의 셀들은 모두 버퍼링된다. 접근 제어 판단 결과가 안전하지 않은 데이터그램으로 판단되는 경우에는 버퍼링된 셀들은 모두 폐기되며, 안전한 것으로 판단되는 경우에는 버퍼링된 셀들을 전송하고 정책 캐쉬에 해당 엔트리를 추가한다. ATLAS가 갖는 또 하나의 특징은 정책 캐쉬의 검색 속도를 향상하기 위하여 CAM (Content Addressable Memory)를 사용한다는 점이다. CAM 메모리는 동시에 병렬 메모리 검색이 가능하기 때문에, 검색 속도를 향상시킬 수 있다는 장점을 갖는다.

그러나, ATLAS 시스템은 만일 IP Option 필드가 사용된 데이터그램이 분할된 경우에는 해당 TCP 헤더가 데이터그램의 두 번째 셀로 분할되기 때문에, 이에 대한 처리가 불가능하며, 접근 제어 여부의 결정을 위하여 셀을 버퍼링하는 과정에서 셀의 처리가 지연된다는 단점을 갖는다. 또한 정책 캐쉬에 사용되는 CAM 메모리의 비용과 관리의 복잡성은 ATLAS의 적용을 어렵게 만드는 원인으로 작용한다. ATLAS의 또다른 문제점으로는 접근 제어 정책 관리가 정책의 추가를 위해서는 관리자가 직접 새롭게 생성된 가상 연결(Virtual Connection)에 대한 접근 제어 정책을 설정해야 한다는 것이다. 이러한 문제점은 현재 광범위하게 사용되고 있는 PVC(Permanent Virtual Connection) 구조에서는 적용 가능한 구조이지만, SVC(Switched Virtual Connection)의 관리를 위해서는 적용 불가능하다.

현재 제안된 또다른 ATM Firewall 구조로 Xu가 설계한 QoF (Quality of Firewalling) 시스템이 있다[10]. QoF 시스템은 스위치로 유입되는 트래픽을 A, B, C, D의 4 등급으로 구분하고, A 등급을 가장 안전한 트래픽으로 D 등급을 가장 위험한 트래픽으로 분류하여 등급에 상응하는 접근 제어를 수행한다. QoF 역시 정책 캐쉬를 사용하는데, 캐쉬의 각 엔트리는 4계층 스위칭(layer-4 Switching)을 위한 <src-IP, dst-IP, src-port, dst-port, protocol>의 튜플로 구성된다.

QoF는 ATLAS가 정책 캐쉬와 일치하지 않는 셀들에 대하여 버퍼링을 수행함으로써 발생하는 셀 지연을 줄이기 위하여 LCH(Last Cell Hostage) 기법을 사용하는데, LCH는 C와 D 등급으로 분류되는 트래픽에 대하여 적용된다. LCH는 정책 캐쉬와 일치하지 않은 셀들에 대한 접근 제어 여부를 판단하는 과정에서 해당 데이터그램의 가장 마지막 셀을 인질로 버퍼링하고 있게 되며, 안전하다고 판단되는 경우에는 마지막 셀을 전송하여 정상적인 전송이 이루어지도록 하는 방식이다. 또한, ATLAS의 또다른 문제점인 IP Option 필드에 대한 처리 문제를 해결하기 위하여 QoF 에서는 셀 처리 과정에 IP Option 필드의 처리를 위한 소프트웨어 모듈을 추가하였다. (그림 2)는 QoF 시스템의 물리적 구조를 나타내는데, ATM 스위치의 IM(Input Module)을 변형하여 Firewall 기능을 수행할 수 있도록 구성한 것이다.



(그림 2) QoF(Quality of Firewall)의 셀처리 방식

QoF는 ATM 스위치로 유입되는 트래픽에 대한 분류에 따라 차등적인 수준의 보안 기법을 사용하며, 셀 지연을 막기 위해 LCH 기법을 사용한다는 점에서 ATLAS의 문제점을 해결한 반면, LCH 기법의 적용을 위하여 IM(Input Module)과 OM(Output Module) 사이에 정보 교환으로 인해 전체 시스템의 오버헤드가 증가한다는 단점을 갖는다.

사용자 셀에 대한 스크리닝은 셀 처리과정에서 부하를 증가시키며, 추가적인 내부 태그(internal tag)의 사용이 수반하기 때문에 병렬 구조와 같은 셀 스크리닝 방식의 적용을 통하여 셀 처리 과정의 부하를 줄여주어야 한다. 본 논문에서 제안하는 Enhanced ATM Firewall Switch는 QoF의 LCH 기법의 사용으로 인해 발생하는 내부태그의 사용을 제거하고, 병렬 구조의 셀 스크리닝 방식의 적용이 가능하도록 독립적인 User Cells Filter 기능 블록을 포함하고 있다.

3. The Enhanced ATM Firewall Switch

ATM Firewall Switch는 고속의 셀 처리가 가능해야 함과 동시에, 일반적인 Firewall이 제공하는 기능을 ATM 네트워크 상에서도 제공할 수 있어야 하며, 패킷 스크리닝은 Firewall 시스템의 접근 제어 기능 수행을 위한 기반 기능으로서 ATM Firewall Switch 상에서도 동일한 기능을 제공할 수 있도록 설계되어야 한다. 앞서 기술한 것과 같이, ATM

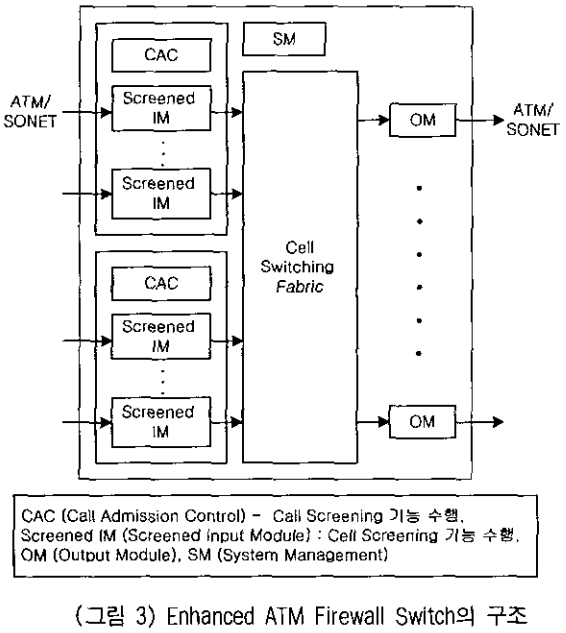
Firewall Switch는 패킷 단위의 스크리닝 기능 수행으로 인하여 발생할 수 있는 셀 처리 속도 저하를 최소화하기 위하여 셀 스크리닝 방식과 정책 캐쉬의 도입을 통해 보안 정책의 비교로 인한 부하를 줄이는 방법을 도입하고 있는 추세이다.

3.1 Enhanced ATM Firewall Switch의 구조

본 논문에서 제안하는 Enhanced ATM Firewall Switch 역시 셀 스크리닝 방식에 기반하고 있으며, 셀 스크리닝 속도 향상을 위하여 정책 캐쉬 구조를 사용한다. 또한, QoF의 경우와 마찬가지로 패킷의 마지막 셀을 해당 패킷에 대한 보안 정책을 결정하는 동안 셀 처리를 수행하지 않는 방식을 사용하여 인가되지 않은 패킷에 대한 차단 기능을 제공할 수 있도록 설계되었다.

ATM Firewall Switch에서 셀 스크리닝 기능의 구현은 IM(Input Module)의 셀 처리(Cell Processing) 기능 블록에서 이루어지는 것이 일반적이다. 이는 IM의 기능 블록중에서 셀 처리 기능 블록이 신호 셀(Signaling Cells), 관리 셀(Management Cells), 사용자 셀(User Cells)이 처음으로 구분되어 처리되는 기능 블록이며, Firewall 시스템의 정의와 마찬가지로 외부로부터의 패킷이 유입되는 경계 블록에 해당하기 때문이다.

ATM Switch는 일반적으로 연결 설정 신호 메시지가 수신되면, 메시지를 CAC(Connection Admission Control)로 전송하며, CAC는 연결 설정을 위한 자원 할당 여부를 결정하고, 연결 설정이 가능한 경우 해당 가상 연결에 상응하는 VPI/VCI 번호를 부여하게 된다. 따라서, CAC는 연결 설정시 연결에 대한 스크리닝을 수행할 수 있는 기능 블록으로 정의할 수 있다. (그림 3)은 Enhanced ATM Firewall Switch의 전체 구조를 간략히 도시한 것이다.



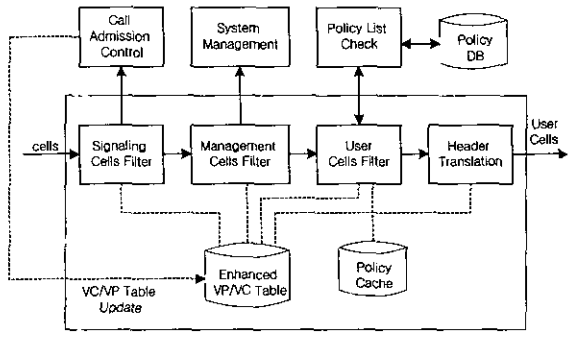
(그림 3) Enhanced ATM Firewall Switch의 구조

(그림 3)에서 나타난 바와 같이, Enhanced ATM Firewall Switch는 분산 형태의 CAC 모듈을 가지고 있다. 이러한 분산된 형태의 CAC 구조는 ATM 스위치의 확장성을 향상하며, 중앙 집중형 CAC 구조에서 나타나는 신호 처리를 위한 병목 현상을 방지할 수 있다는 특징을 갖는다.

몇 개의 IM 모듈 블록 단위의 연결 설정 제어 기능을 제공하는 CAC는 연결 스크리닝(Call Screening) 기능을 제공한다. 연결 스크리닝 기능은 연결 설정을 요구한 종단 시스템의 식별자를 이용하는데 해당 정보는 근원지와 목적지의 ATM 주소를 포함한다. 만일 인가되지 않은 종단 시스템간의 연결 설정 요구인 경우에는 연결 설정을 거부하게 되며, 연결 설정이 허가되는 경우에는 해당 가상 연결에 대한 보안 정책 정보를 결정한 후, 할당된 VPI/VCI 정보와 가상 회선 보안 정책 정보를 IM으로 전달한다. 연결 스크리닝 기능에 의하여 설정 가능한 보안 정책으로는 Bypass와 Apply가 있으며, Bypass는 설정된 가상 회선을 통해 수신되는 모든 셀들에 대한 통과를 의미하고, Apply는 수신되는 모든 패킷들에 대하여 셀 스크리닝 기능을 적용할 것을 의미한다.

3.2 User Cells Filter 기능 블록

CAC에 의해 연결 설정이 이루어진 이후에는 설정된 가상 회선의 보안 정책이 Apply로 설정되는 경우에 유입되는 모든 패킷들에 대한 패킷 수준의 스크리닝이 적용하기 위하여 셀 스크리닝 방식을 적용한다. 셀 스크리닝이 적용되는 기능 블록은 IM(Input Module)의 셀 처리 기능 블록이며, (그림 4)는 IM의 User Cells Filter 기능 블록을 포함하는 셀 처리 기능 블록을 도시한 것이다.



(그림 4) Enhanced ATM Firewall Switch를 위한 Input Module의 셀처리 기능 블록의 구조

앞서 기술한 것과 같이, IM의 셀 처리 기능 블록은 ATM 스위치로 유입되는 셀들에 대한 분류가 처음으로 이루어지는 기능 블록이다. 우선 연결 설정을 위하여 수신된 셀들은 Signaling Cells Filter 기능 블록에 의하여 CAC로 전송되어 연결 스크리닝을 수행하게 되며, 연결 설정된 가상 회선은 다시 IM의 VP/VC 테이블을 갱신하게 된다. Management Cells Filter 기능 블록에 의하여 관리 셀들이

필터링 된 후에는, 사용자 셀들이 User Cells Filter 블록으로 유입되는데, User Cells Filter 기능 블록은 유입되는 셀들에 대하여 Enhanced VP/VC Table 정보를 이용하여 셀 스크리닝 기능을 수행하게 된다. User Cells Filter 기능 블록을 통과한 패킷들은 마지막으로 Header Translation 기능 블록에 의하여 셀 스위칭을 위해 필요한 정보가 삽입된 후, CSF(Cell Switching Fabric)으로 전송된다.

User Cells Filter 기능 블록에 의하여 수행되는 셀 스크리닝 기능은 유입되는 셀들에 대하여 셀 스크리닝 기능을 적용하고, 적용 결과에 따라 셀이 포함되는 패킷을 Header Translation 기능 블록으로 전달하거나 폐기하는 기능을 제공하는 것이다. 우선 셀이 유입되면, User Cells Filter 기능 블록은 CAC에 의해 할당된 가상회선에 대하여 설정되어 있는 보안 정책을 얻기 위해 Enhanced VP/VC Table을 참조한다. 만일 가상 회선의 보안 정책이 Bypass인 경우에는 해당 셀을 바로 Header Translation 기능 블록으로 전달하고, 보안 정책이 Apply일 경우에는 해당 셀이 포함된 패킷에 대한 스크리닝 처리를 위하여 Enhanced VP/VC Table의 패킷 수준의 보안 정책 필드를 참조한다.

Enhanced VP/VC Table에 의해 반환될 수 있는 패킷 수준의 설정 값은 Apply, Bypass, Discard, IP_Option, Processing 이다. Apply는 패킷의 첫 번째 셀이 유입되는 경우에 설정되는 값으로 해당 패킷에 대한 보안 정책 설정이 존재하지 않으므로, 보안 정책 결정할 것을 의미한다. Bypass는 패킷에 대한 통과를 의미하며, Discard는 패킷에 대한 폐기를 의미한다. IP_Option은 해당 패킷이 IP_Option 필드를 사용하기 때문에 해당 패킷의 두 번째 셀 정보에 대한 참조가 요구됨을 의미한다. 마지막으로 Processing은 해당 패킷에 대한 보안 정책의 결정이 현재 처리 중임을 의미한다.

우선 설정되어 있는 값이 Bypass와 Discard인 경우에는 해당 패킷의 첫 번째 셀에 의하여 패킷에 대한 보안 정책이 결정된 상태를 의미하며, Bypass의 경우에는 해당 셀을 Header Translation 기능 모듈로 전달하고, Discard인 경우에는 해당 셀을 폐기하게 된다. 이러한 과정은 해당 패킷의 마지막 셀이 도착하는 시점까지 지속적으로 수행되며, 마지막 패킷에 대한 처리를 마치고 난 후에 설정 값을 Apply로 변경한다.

설정 값이 Apply인 경우는 수신된 셀이 패킷의 첫 번째 셀임을 의미하며, 패킷에 대한 보안 정책이 결정이 요구된다. Apply로 설정된 셀에 대한 처리 과정은 우선 해당 셀이 IP Option 필드를 사용하고 있는 패킷인지의 여부를 검사하는 것이다. 만일 사용하고 있다면, 첫 번째 셀을 버퍼에 복사하고 IP_Option으로 설정 값을 변경한 후, 패킷을 Header Translation 필드로 전달한다. IP Option 필드를 사용하지 않는 패킷의 경우에는 해당 패킷의 정책을 결정하기 위하여 정책 캐쉬를 확인한다.

만일 일치하는 보안 정책이 정책 캐쉬에 존재한다면, 정책 값에 따른 셀 처리를 수행한 후, 설정 값을 정책 캐쉬에 설정되어 있는 값으로 변경한다. 정책 캐쉬를 통하여 반환되는 값은 패킷을 허가할 것인지(Bypass), 차단할 것인지(Discard)에 대한 결정이다. 만일 정책 캐쉬 상에 일치하는 엔트리가 없는 경우에는 정책 결정을 Policy List Check 기능 블록에게 요구하게 되며, Policy List Check 블록으로부터 결과가 반환되기 전까지 설정 값을 Processing으로 유지하게 된다. 만일 Processing 상태에 있는 패킷의 마지막 셀이 결정 이전에 도착하게 되면, 마지막 셀은 User Cells Filter 모듈 내에 저장되며, Policy List Check 기능 모듈의 결정에 따라 셀을 폐기하거나, Header Translation 기능 블록으로 전달한다. 또한 다음 패킷에 대한 처리를 위하여 설정 값을 Apply로 초기화한다.

설정 값이 IP_Option 인 경우에는 해당 패킷의 두 번째 셀을 기다리고 있는 상태이다. 이 경우에는 해당 셀을 이전에 버퍼링된 첫 번째 셀과 함께 사용하게 되는데, 이는 IP Option 필드에 의하여 TCP 헤더의 정보가 두 번째 셀에 유지되기 때문이다. 두 개의 셀이 합쳐지면, 설정 값을 Apply로 변경하고, 정책 결정을 위하여 정책 캐쉬를 참조한다. 이후의 절차는 Apply의 처리 절차와 동일하다.

마지막으로 Processing의 경우에는 해당 패킷에 대한 보안 정책 결정이 아직 진행중인 상태를 의미한다. 따라서, 수신된 셀이 패킷의 마지막 셀에 해당하는지의 여부를 검사하게 된다. 마지막 셀에 해당하는 경우에는 패킷에 대한 처리 문제를 결정하는 시간 동안 마지막 셀을 처리하지 않고 버퍼에 저장한다. 마지막 셀이 아닌 경우에는 셀 처리 지연을 막기 위하여 셀을 Header Translation 기능 블록으로 전달하게 된다. 패킷에 속하는 모든 셀에 대한 처리를 마친 후에는 설정 값의 초기화를 위해 Apply로 설정한다.

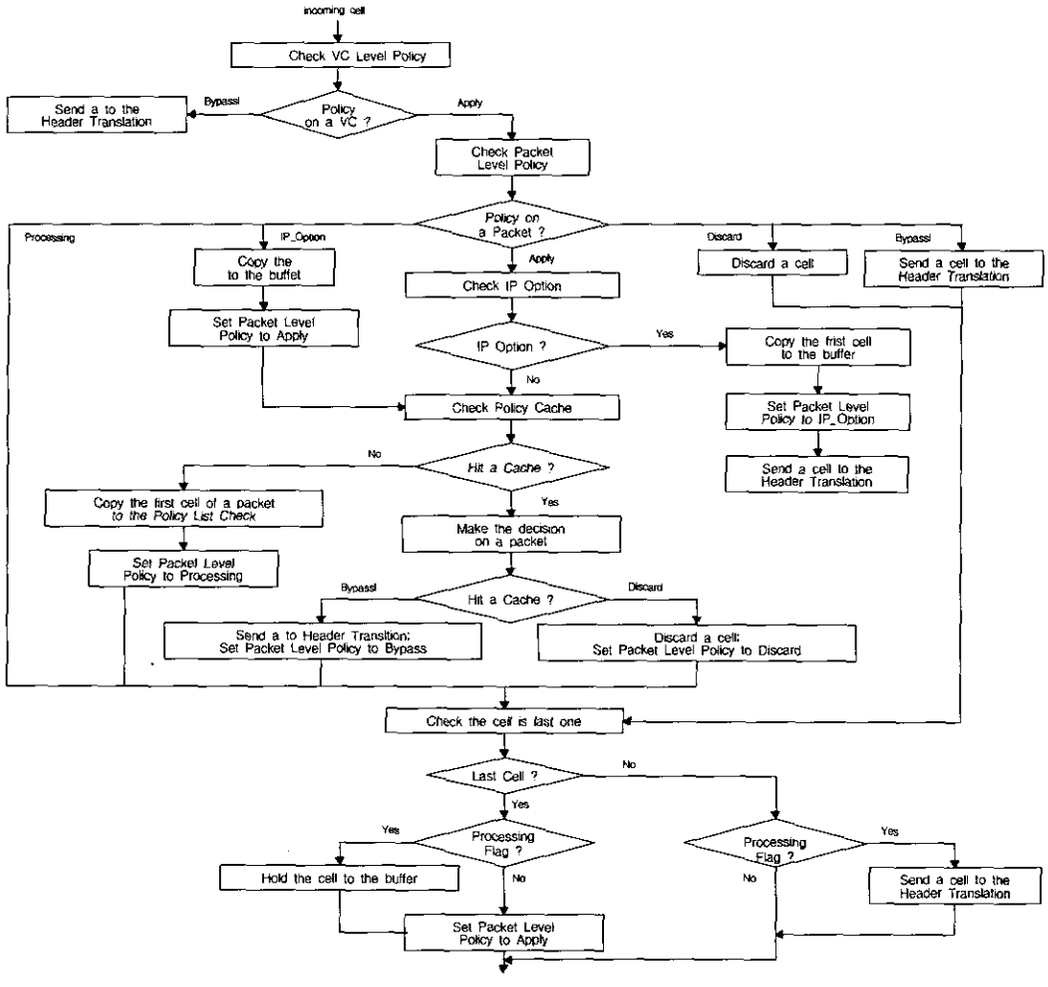
(그림 5)는 User Cells Filter 기능 블록의 셀 스크리닝을 위해 적용되는 알고리즘을 도시한 것이다.

3.3 Enhanced ATM Firewall Switch의 구조적 특성

본 논문에서 제안하는 Enhanced ATM Firewall Switch의 User Cells Filter 기능 블록은 다음과 같은 구조적 특성을 갖는다.

- 정책 캐쉬의 사용을 통한 고속의 셀 스크리닝 수행이 가능하다.
- 내부태그의 사용이 불필요하게 됨으로써 User Cells Filter 기능 블록의 독립성을 유지한다.
- 병렬 User Cells Filter 기능 블록을 통하여 시스템의 부하를 분산시킬 수 있기 때문에, 셀 스크리닝 성능 향상의 효과를 갖는다.

우선, Enhanced ATM Firewall Switch의 User Cells Filter 기능 블록은 셀 스크리닝 기능은 패킷에 대한 빠른



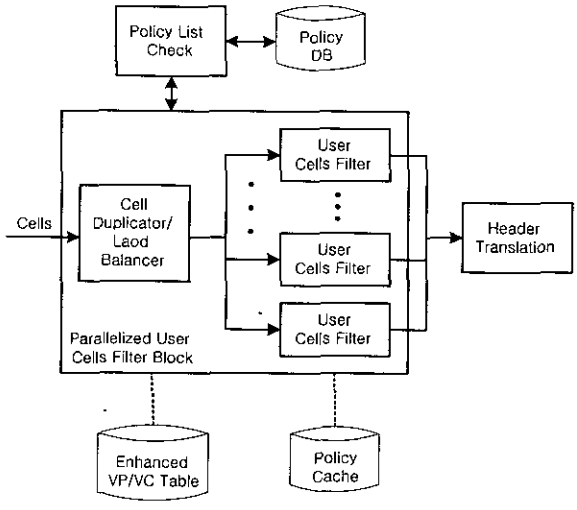
(그림 5) User Cells의 셀 스크리닝 알고리즘

보안 정책 결정을 위하여 정책 캐쉬를 사용한다는 점에서 장점을 갖는다. 정책 캐쉬의 사용은 셀 스크리닝 과정에서 셀에 대한 정책을 결정하는 과정에서 다수의 정책 목록과의 비교가 요구되는 경우에 발생할 수 있는 처리 속도의 저하를 막을 수 있는 방법으로 현재 많이 도입되고 있는 방식이다. 정책 캐쉬의 Hit Ratio를 향상함으로써 캐쉬 엔트리의 Replacement 상황을 최소화하고, 효율적인 Repalcement 알고리즘을 통하여 처리 속도를 향상할 수 있다.

둘째로, Enhanced ATM Firewall Switch의 Screened IM (Input Module)은 셀 스크리닝 기능 수행시 OM(Output Module)과 독립적으로 동작할 수 있도록 설계되어 IM과 OM 사이에 정보 교환을 위한 추가적인 내부태그의 사용이 불필요하다. 이는 앞서 언급한 QoF (Quality Of Firewall)의 LCH (Last Cell Hostage) 방식이 Last Cell의 통과를 차단하기 위하여 IM과 OM 사이에 정보 교환을 위한 내부태그들의 사용이 불가피하며, 이는 시스템의 불필요한 부하를 초래할 수 있다는 문제점을 해결한 것이다. 따라서 제안된 Enhanced ATM Firewall Switch의 독립적인 Screened IM의 셀 스크리닝 기능 수행은 시스템의 불필요한 오버헤드를 제거하고, 기존의 ATM Switch에 대한 변경을 최소화할 수 있다는 장점을 갖는다.

마지막으로, 독립적으로 구성된 User Cells Filter 기능 블록은 스위치의 처리 부하 정도에 따라 병렬 구조로도 구성이 가능하기 때문에, ATM Firewall Switch의 설계에 유동성을 갖는다. 병렬 User Cells Filter 전통적인 네트워크에서도 패킷 스크리닝 라우터의 병렬 구조는 처리 속도의 향상을 위하여 많은 연구가 이루어지고 있는 상황이다[7]. User Cells Filter 기능 블록을 병렬 처리 구조로 설계하기 위해서는 병렬 프로세스들을 스케쥴링 하기 위한 관리 구조가 필요하게 되며, (그림 6)은 이러한 병렬 처리 구조의 User Cells Filter 기능 블록의 구조를 보인다.

(그림 6)에 나타난 것과 같이 병렬 구조의 User Cells Filter 블록을 구성하는 경우에는 각각의 User Cells Filter 블록으로 셀을 분배하기 위한 분배기를 필요로 한다. 셀 분배 방식은 크게 Cell Duplicator를 사용하여 모든 User Cell Filter 블록으로 셀을 전달하는 방식과 Load Balancer를 이용하여 셀을 각 User Cell Filter 블록들에게 균형적으로 분배하는 방식을 고려할 수 있다.



(그림 6) 병렬 처리 구조의 User Cells Filter 블록

Cell Duplicator를 사용하는 방식에서는 유입되는 셀을 Cell Duplicator가 연결되어 있는 User Cells Filter 블록의 수만큼 복제한 후, 모든 User Cells Filter 블록들로 전달하는 방식이다. 따라서, 모든 User Cells Filter 블록은 동일한 셀에 대한 처리를 요구받게 되는데, 이 때 User Cells Filter는 자신의 처리 대상 셀만을 처리하고 그 이외의 셀들은 모두 폐기한다. 각 User Cells Filter 블록의 처리 대상 셀에 대한 결정은 셀 헤더의 특정 필드 정보를 이용하는 방식을 사용할 수 있는데, 예를 들어, 헤더의 VPI 필드를 식별자로 사용하여 자신의 처리 범위 VPI 필드 값을 할당받고, 유입되는 셀의 VPI 필드를 검사하여 처리 대상 범위 내의 셀만을 처리하는 방식이다. 이러한 방식을 사용할 경우, 각 User Cells Filter 블록은 자신의 처리 범위 내의 셀들에 대해서만 스크리닝 기능을 수행하면 되기 때문에, 처리 부하를 줄일 수 있는 장점이 있다.

Load Balancer를 사용하는 방식은 셀의 분배를 Load Balancer가 스케줄링을 통하여 User Cells Filter 모듈들에 대한 부하를 균일하게 분배하는 방식이다. Load Balancing을 위한 알고리즘은 가장 단순한 형태의 Round Robin 방식의 적용도 가능하며, 각 User Cells Filter 블록들의 현재 처리 대상 가상 회선 수를 고려하여 분배할 수도 있다.

병렬 처리 구조의 셀 스크리닝 방식은 단일 셀 스크리닝 방식보다 셀 처리 시간과 부하를 줄일 수 있는 장점이 있다. TCP 연결에 기반한 서비스는 연결 설정 과정에 수반되는 패킷들(SYN, FIN, ACK, RST 패킷들)이 데이터를 포함하지 않기 때문에 IP Option 필드가 사용되지 않을 경우, 해당 패킷이 하나의 셀로 포함될 수 있다. 이러한 연결 설정 요구들이 Apply 정책이 적용되는 가상회선을 통하여 많은 수의 연결 요청이 수신되는 경우에는 보안 정책의 결정을 위하여 많은 지연을 초래할 수 있다. 따라서, 병렬 처리 구조의 User Cell Filter 블록들로 처리 부하를 분배하는 방식을 통하여 연결 설정 패킷들에 대한 처리 속도를 향상시킬 수 있다.

4. 결론 및 향후 계획

기존의 라우터 기반의 패킷 스크리닝 방식은 전통적인 네트워크 상에서 Firewall 시스템의 기반 기술로서 사용되는 네트워크 보안 기술이다. 그러나, 패킷 스크리닝의 처리 속도가 고속의 데이터 전송을 지원하는 ATM 네트워크 상에서는 데이터 전송 속도의 저하 및 패킷 스크리닝을 위한 SAR(Segmentation And Reassembly) 과정을 필요로 하기 때문에 새로운 기술인 셀 스크리닝 방식의 도입이 확산되고 있다. 셀 스크리닝 방식은 패킷의 TCP/IP 헤더 부분만을 재조합하여 4계층 스위칭이 가능하도록 하여 셀 수준의 스크리닝이 가능하도록 구성된 기술이다.

본 논문에서는 ATM Firewall Switch의 구성을 위한 시스템 구조를 제안하였다. 제안된 Enhanced ATM Firewall Switch의 구조는 독립적으로 구성된 User Cells Filter 블록이 가상 회선을 통하여 유입되는 패킷에 대해 셀 스크리닝이 가능하다. 또한 회선 연결 단위의 스크리닝 기능을 수행하는 분산 형태의 CAC 기능 블록의 도입을 통하여 SVC 연결 설정에 대해서도 연결 설정에 대한 스크리닝 기능을 수행할 수 있도록 구성하였다. User Cells Filter 블록은 기존의 스위치 구조와 독립성을 유지할 수 있는 방식으로 구성하여 병렬 처리가 가능하도록 구성하였으며, 결과적으로 셀 스크리닝 기능의 처리 속도 향상과 처리 오버헤드를 줄일 수 있는 장점을 갖는다. 각 User Cells Filter 블록은 셀 스크리닝 기능의 적용을 가상 회선으로 유입되는 패킷 단위의 보안 정책 적용이 가능하도록 구성하였으며, 보안 정책 결정 시간을 단축하기 위하여 보안 정책 캐쉬를 사용하였다. ATLAS 시스템이 갖는 IP Option 필드를 포함하는 패킷의 처리 문제는 QoF의 경우와 마찬가지로 패킷의 두 번째 패킷까지의 검사가 가능하도록 스크리닝 알고리즘을 정의하여 해결하였으며, 또한, QoF의 셀 스크리닝을 위한 추가 Internal Tag의 사용으로 인한 복잡성을 제거하기 위하여 User Cells Filter 블록 내에 버퍼링 기능을 추가하였다.

본 연구를 통하여 설계된 Enhanced ATM Firewall Switch의 구조는 시스템의 확장성과 셀 스크리닝 처리 속도 향상을 목적으로 설계되었기 때문에, 대규모의 셀 처리가 요구되는 스위처 상에서의 Firewalling 기능 구현에 적합하다고 사료된다.

마지막으로 셀 스크리닝 처리 속도 향상을 위해서는 Enhanced ATM Firewall Switch의 User Cells Filter 기능 블록이 사용하는 정책 캐쉬의 정확도를 향상하여야 한다. 정책 캐쉬의 정확도는 가상 회선을 통해 유입되는 패킷들에 대한 보안 정책 결정 시간을 단축시킬 수 있기 때문에 보다 효율적인 정책 캐쉬 관리를 위한 메커니즘에 대한 연구가 필요하다.

참 고 문 헌

[1] M. Laubach, "Classical IP and ARP over ATM," RFC 1577, January. 1994.

[2] M. Laubach, J. Halpern, "Classical IP and ARP over ATM," RFC 2225, April. 1998.

[3] M. Perez, F. Liaw, et el, "ATM Signaling Support for IP over ATM," RFC 1755, February. 1995.

[4] M. Maher, "ATM Signaling Support for IP over ATM - UNI Sinaling 4.0 Update," RFC 2331, April. 1998.

[5] ATM Forum, MultiProtocol Over ATM (MPOA), Version 1.0, af-mpoa-0087.000, July. 1997.

[6] ATM Forum, "ATM Security Specification Version 1.0," af-sec-0100.001, February. 1999.

[7] Uwe Ellermann, Carsten Benecke, "Firewalls for ATM Networks," *Proceedings in INFOSEC'98, Paris France, June.* 4-5, 1998.

[8] Juha Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," RFC 1483, July. 1993.

[9] J. Hughes, "A High Speed Firewall Architecture for atm/oc-3c," *Interop Engineering Conference, Las Vegas USA,* 1996.

[10] Jun Xu, Mukesh Singhal, "Design of High-Performance ATM Firewall," ACM Transaction on Information and System Security, Vol.2, No.3, pp.269-294, August 1999.

홍 승 선

email : sshong@ece.skku.ac.kr

1998년 성균관대학교 정보공학과 졸업(석사)

2000년 성균관대학교 대학원 전기전자 및 컴퓨터공학부(공학석사)

현 재 성균관대학교 대학원 전기전자 및 컴퓨터공학부 박사과정 재학

관심분야 : 망관리, ATM 네트워크, Mobile Agents, 네트워크 보안

정 태 명

email : tmchung@ece.skku.ac.kr

1984년 일리노이주립대학 전자계산학과 졸업(학사)

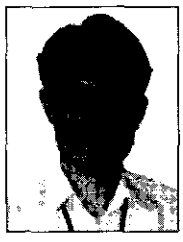
1987년 일리노이주립대학 대학원 컴퓨터 공학(공학석사)

1995년 Purdue대학교 대학원 컴퓨터공학과 (공학박사)

1995년~1999년 성균관대학교 전기전자 및 컴퓨터공학부 조교수

2000년~현재 성균관대학교 전기전자 및 컴퓨터공학부 부교수

관심분야 : 망관리, 네트워크 보안, 통합보안 관리, 액티브 네크워크



박 미 룡

email : mrpark@etri.re.kr

1993년 경북대학교 전자공학과 졸업(학사)

1998년 경북대학교 대학원 전자전기공학부 (공학석사)

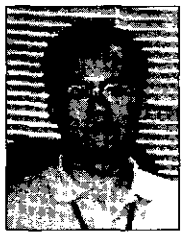
1993년~1994년 산업과학기술원(RIST) 전산개발과

1994년~1996년 영남대학교 전산정보원 학내망 담당

1998년~1999년 대구종합정보센터 개발팀

1999년~현재 한국전자통신연구원 선임연구원

관심분야 : ATM, Internet Protocol, IP Multicast, IP Routing, Router Technology, VoIP, Network Protocols, QoS



이 종 협

email : jhlee@etri.re.kr

1984년 고려재학교 산업공학과 졸업(학사)

1986년 한국과학기술원(KAIST) 대학원 산업공학과(공학석사)

1996년 한국과학기술원(KAIST) 대학원 산업공학과(공학박사)

1986년~현재 한국전자통신연구원 책임연구원, 라우터제어팀장

관심분야 : High-speed Network Design and Routing, Router Technology, Converged Network System, Network Protocols