(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월15일
(11) 등록번호 10-1553264
(24) 등록일자 2015년09월09일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/26* (2006.01)
(21) 출원번호 10-2014-0178226
(22) 출원일자 2014년12월11일
심사청구일자 2014년12월11일
(56) 선행기술조사문헌
KR1020140051776 A*
KR1020020062071 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
조진용
대전광역시 유성구 노은로 353, 303동 1003호 (하기동, 송림마을3단지아파트)
공정욱
대전광역시 유성구 상대로 17, 303동 1001호 (상대동, 도안신도시 한라비발디 아파트)
이경민
대전광역시 유성구 어은로57번길 29, 301호 (어은동)
(74) 대리인
특허법인(유)화우

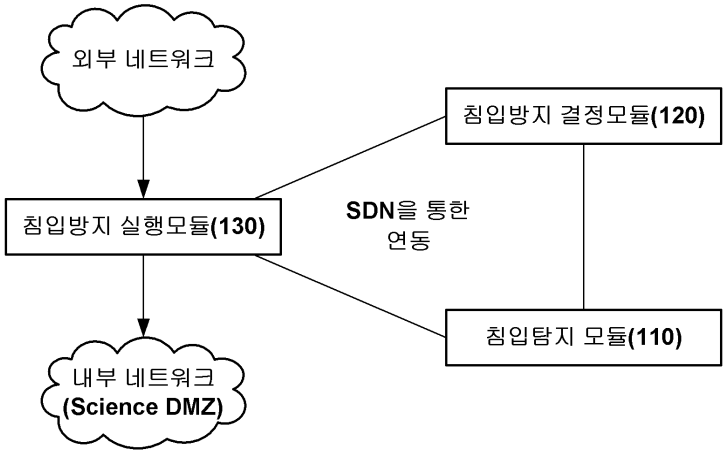
전체 청구항 수 : 총 17 항 심사관 : 윤태섭

(54) 발명의 명칭 **네트워크 침입방지 시스템 및 방법**

(57) 요 약

본 발명은 침입탐지프로그램과 연계하여 동작하며 보안위협을 분석하고, 침입이 탐지되면 침입방지결정모듈에게 위협정보를 전달하는 침입탐지모듈, 패킷 플로우에 대한 침입방지를 결정하며, 상기 침입탐지모듈과 침입방지실행모듈에 대한 접근제어 기능을 갖는 침입방지결정모듈, 내부 네트워크에 대한 침입방지 기능을 수행하며, SDN 기술에 의해 상기 침입방지결정모듈에 제어되는 침입방지실행모듈을 포함하는 네트워크 침입방지 시스템 및 방법에 관한 것이다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

침입탐지프로그램과 연계하여 동작하며, 보안위협을 분석하고 침입이 탐지되면 침입방지결정모듈에 위협정보를 전달하는 침입탐지모듈;

상기 침입탐지모듈과 침입방지실행모듈에 대한 접근제어를 수행하며, 패킷 플로우에 대한 침입방지를 결정하는 침입방지결정모듈;

상기 침입방지결정모듈과 SDN(Software defined networking)에 의해 상호 연동되어, 상기 침입방지결정모듈이 결정한 접근 허락 여부에 따라 내부 네트워크에 대한 외부의 침입 방지를 수행하는 침입방지실행모듈;

을 포함하고,

상기 침입방지실행모듈은,

패킷의 시그니처(signature)를 미리 저장하고, 시그니처 기반의 패킷 처리 국지화를 위한 블룸 필터(Bloom filter)를 사용하며,

플로우(f)가 입력되면 침입방지결정모듈에 테이블 조회를 요청하여 SDN 메시지를 통해 상기 플로우에 대한 완전일치 정합 엔트리를 송신받고, 피드백 플로우(f')를 시그니처 정합 테이블에 등록할 것인지 결정하여 피드백 플로우(f')가 입력되면 시그니처 정합을 이루며, 시그니처 정합 엔트리에서 완전일치 정합 엔트리로 규칙 복사(rule clone)를 수행하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 2

제 1항에 있어서,

상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN에 의해 상호 연동되는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 3

제 1항에 있어서,

상기 침입탐지모듈은,

침입탐지프로그램과 연계하여, 내부 네트워크의 보안 위협을 실시간으로 분석하는 위협분석부;

상기 분석 결과를 침입방지결정모듈에 보고하는 위협보고부;

를 포함하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 4

제 3항에 있어서,

상기 위협분석부는,

상기 내부 네트워크 및 시스템의 보안위협을 취합하고 침입 방지 시스템의 보안 정책에 따라 보안 위협을 분류하며, 보안 위협을 단계별로 재분류하고,

상기 위협보고부는,

E2N(End to Network) 메시지를 구성한 후 상기 침입방지결정모듈에 보고하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 5

제 1항에 있어서,

상기 침입방지결정모듈은,

상기 침입탐지모듈이 위협정보를 제공하고 상기 침입방지실행모듈이 패킷 플로우 테이블 조회를 요청하면, 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하고, 결과를 플로우 엔트리에 반영하여 상기 침입방지실행모듈에 설치하고 동작지침에 따라 플로우를 처리하도록 하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 6

제 1항에 있어서,

상기 침입방지결정모듈은,

보안 규정에 따라 내부네트워크에 대한 접근 허가 또는 접근 거부를 결정하는 침입방지 결정부;

침입탐지모듈과 침입방지실행모듈을 직접 연결하는 경우 네트워크 간 환경을 설정하는 시스템 연동부;

비인가 침입방지실행모듈과 비인가 침입탐지모듈이 침입방지결정모듈에 접근하는 것을 차단하기 위해 IP주소 기반의 접근 제어를 수행하는 접근 제어부;

상기 침입탐지모듈에 의해 확인된 위협 정보가 저장되는 보안위협 데이터베이스;

를 포함하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 7

제 6항에 있어서,

상기 시스템 연동부는,

시스템 명령을 이용하여 패킷 필터링과, IP 패킷의 네트워크 주소와 포트 주소를 변경하며, IP패킷의 캡슐화 및 역캡슐화 하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 8

제 7항에 있어서,

상기 시스템 명령은,

FORWARD, DROP, SET_FIELD, SET_TUNNEL 명령 중 하나 이상을 포함하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 9

제 6항에 있어서,

상기 시스템 연동부는,

침입탐지프로그램 또는 방화벽의 운용환경을 모사하여, 네트워크 주소변경 방식을 통해 자동적으로 네트워크간 환경을 설정하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 10

제 6항에 있어서,

상기 시스템 연동부는,

공격자의 IP 주소를 포함하는 보안 위협 정보를 수집, 개방 또는 공유하여 다수의 서버에 대한 공격을 협력적으로 방지하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 11

제 1항에 있어서,

상기 침입방지실행모듈은,

패킷이 수신되면 정합 테이블의 우선순위에 따라 플로우 엔트리를 검색하고, 할당된 동작지침에 따라 패킷을 처리하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 12

제 11항에 있어서,

상기 정합 테이블은,

완전일치 정합(exact match), 시그니처 정합(signature match), 와일드카드 정합(wildcard match)의 순으로 우선순위인 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 13

삭제

청구항 14

제 1항에 있어서,

상기 침입방지실행모듈은,

활성 블룸 필터와 대기 블룸 필터를 포함하여 플로우 엔트리를 구성하고, (수학식 1)에 따라 상기 활성 블룸 필터에 t개 이상의 플로우가 기록되면 해당 필터를 초기화한 후 대기 상태로 전환하며, 대기 블룸 필터를 활성 상태로 전환하는 것을 특징으로 하는 네트워크 침입방지 시스템.

(수학식 1)

$$t = \frac{-m(\ln 2)^2}{\ln \alpha} \leq n$$

(m: 블룸 필터의 비트 수, n: 플로우 시그니처의 수, α: 기대 위양성 확률)

청구항 15

제 1항에 있어서,

상기 침입방지실행모듈은,

n이 (수학식 2)의 조건에 맞는 경우, 활성 블룸 필터와 대기 블룸 필터 모두에 시그니처를 남기는 것을 특징으로 하는 네트워크 침입방지 시스템.

(수학식 2)

$$\beta \cdot t < n < t, (0 < \beta < 1)$$

(β : 기대 위양성 계수)

청구항 16

삭제

청구항 17

제 1항에 있어서,

상기 침입방지실행모듈은,

상기 블룸 필터의 시그니처를 삭제하는 경우, 다른 정합 테이블에 기록된 역 플로우(f^{-1})의 처리규칙을 변경하여 삭제하는 것을 특징으로 하는 네트워크 침입방지 시스템.

청구항 18

(a) 침입탐지모듈이 침입을 탐지하고, 침입방지결정모듈로 위협정보를 전달하는 단계;

(b) 침입방지실행모듈이 입력된 패킷에 대하여 플로우 테이블 조회를 요청하는 단계;

(c) 침입방지결정모듈이 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하는 단계;

(d) 상기 침입방지결정모듈이 결정된 결과를 플로우 엔트리에 반영하여 상기 침입방지실행모듈에 동작지침을 설치하는 단계;

(e) 상기 침입방지실행모듈이 동작지침에 따라 플로우를 처리하는 단계;

를 포함하고,

상기 침입방지실행모듈은,

패킷의 시그니처(signature)를 미리 저장하고, 시그니처 기반의 패킷 처리 국지화를 위한 블룸 필터(Bloom filter)를 사용하며,

플로우(f)가 입력되면 침입방지결정모듈에 테이블 조회를 요청하여 SDN 메시지를 통해 상기 플로우에 대한 완전일치 정합 엔트리를 송신받고, 피드백 플로우(f')를 시그니처 정합 테이블에 등록할 것인지 결정하여 피드백 플로우(f')가 입력되면 시그니처 정합을 이루며, 시그니처 정합 엔트리에서 완전일치 정합 엔트리로 규칙 복사(rule clone)를 수행하는 것을 특징으로 하는 네트워크 침입방지 방법.

청구항 19

제 18항에 있어서,

상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN(Software defined networking)에 의해 상호 연동되는 것을 특징으로 하는 네트워크 침입처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 침입탐지프로그램과 연계하여 동작하며 보안위협을 분석하고, 침입이 탐지되면 침입방지결정모듈에게 위협정보를 전달하는 침입탐지모듈, 패킷 플로우에 대한 침입방지를 결정하며, 상기 침입탐지모듈과 침입방지실행모듈에 대한 접근제어 기능을 갖는 침입방지결정모듈, 내부 네트워크에 대한 침입방지 기능을 수행하며, SDN 기술에 의해 상기 침입방지결정모듈에 제어되는 침입방지실행모듈을 포함하는 네트워크 침입방지 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷 백본 대역폭의 폭발적 증가에도 불구하고, 복잡도가 증가된 일반 목적 망(general-purpose network)은 데이터 전송성능의 병목 지점으로 작용하고 있다. 특히, 상태기반 방화벽(stateful firewall)으로 인한 사용자 망(last-mile network)의 병목은 패킷손실을 유발해 대용량 과학기술데이터(scientific data)의 전송 성능을 크게 저하시킨다.

[0003] 방화벽 등으로 인한 사용자 망의 성능병목 문제를 완화하고 대용량 과학기술데이터의 고속 전송을 담보하기 위해 Science DMZ와 같은 네트워크 완충 영역에 대한 연구가 진행되어 왔다. 특히 근래에는 DMZ 내부 및 외부 네트워킹 자원을 유연하게 연동하기 위해 SDN(Software Defined Networking) 기술을 DMZ 환경에 적용하는 방안이 모색되고 있다. 하지만, SDN의 적용 범위가 가상회선(virtual circuit)의 설정 등 네트워킹 유연성 확보에 초점을 두고 있는 단계로써 DMZ 환경의 보안 강화 방안에 대해서는 고려되지 않고 있다.

[0004] 따라서, 내부 네트워크에 대한 침입 방지 시스템은 데이터 처리성능 및 저비용 구조와 정책규칙 설정의 유연성 및 관리의 용이성을 가져야 한다. 네트워크 내·외부 간 데이터 전송 속도와 침입 방지 시스템의 적용 사이에는 트레이드오프 관계가 존재하며, 고성능 침입 방지 시스템의 적용을 통해 전송 속도 저하와 관련된 문제를 일부 해결할 수 있지만 관련 장비가 고가인 단점이 있으므로, 적용되는 침입 방지 시스템은 데이터 전송 속도의 저하를 초래하지 않아야 하며 시스템 확장성(extensibility)의 확보를 통해 초기 구축비용을 줄일 수 있어야 한다.

[0005] 또한, 방화벽 사용으로 인해 네트워크 자원에 대한 접근 제어가 데이터 통신의 단절을 야기할 수 있다. 방화벽에서 접근제어 규칙을 정적으로 적용하면 임의의 포트번호를 사용하는 UDP 응용의 통신 단절을 야기하며, 다수 응용의 통신 단절문제를 해결하기 위해서는 방화벽 설정의 빈번한 변경이 요구되지만 이는 시스템 관리비용의 증가를 초래하게 되므로, 침입 탐지 시스템은 관리운영 측면의 유연성 확보를 통해 운영비용을 줄일 수 있어야 한다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 DMZ 환경에서 유연한 보안 적용을 가능하게 하는 SDN 기반의 침입 방지 프레임워크인 SAFE(SDN-Assisted Firewall Environment)를 이용하는 네트워크 침입방지 시스템을 제안한다. 네트워크 침입 방지 시스템은, 침입 방지 시스템 (IPS, Intrusion Prevention System)의 침입 탐지, 방지 결정, 침입 방지 등의 기능을 물리적으로 분산하고 SDN을 이용해 상호 연동시키는 것을 해결 과제로 한다.

[0007] 이와 같이 기존 방화벽이 갖는 침입 탐지, 침입 방지 결정, 침입 방지 실행 등 기능을 물리적으로 분리시키고, SDN 기술을 이용하여 상호 연동시킴으로써 보안 정책의 유연한 적용과 보안시스템 관리운영의 자동화가 가능하게 된다.

[0008] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 이하에서 설명할 내용으로부터 통상의 기술자에게 자명한 범위 내에서 다양한 기술적 과제가 포함될 수 있다.

과제의 해결 수단

[0009] 상기와 같은 과제를 해결하기 위한 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템은, 침입탐지프로그램과 연계하여 동작하며, 보안위협을 분석하고 침입이 탐지되면 침입방지결정모듈에 위협정보를 전달하는 침입탐지모듈; 상기 침입탐지모듈과 침입방지실행모듈에 대한 접근제어를 수행하며, 패킷 플로우에 대한 침입방지를 결정하는 침입방지결정모듈; 상기 침입방지결정모듈과 SDN(Software defined networking)에 의해 상호 연동되어, 상기 침입방지결정모듈이 결정한 접근 허락 여부에 따라 내부 네트워크에 대한 외부의 침입 방지를 수행하는 침입방지실행모듈; 을 포함한다.

[0010] 이 때, 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템은, 상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN에 의해 상호 연동되는 것을 특징으로 한다.

[0011] 또한, 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 상기 침입탐지모듈은, 침입탐지프로그램과 연계하여, 내부 네트워크의 보안 위협을 실시간으로 분석하는 위협분석부; 상기 분석 결과를 침입방지결정모듈에 보고하는 위협보고부; 를 더 포함하는 것을 특징으로 한다.

[0012] 이 때, 상기 위협분석부는, 상기 내부 네트워크 및 시스템의 보안위협을 취합하고 침입 방지 시스템의 보안 정책에 따라 보안 위협을 분류하며, 보안 위협을 단계별로 재분류하고, 상기 위협보고부는, E2N(End to Network) 메시지를 구성한 후 상기 침입방지결정모듈에 보고하는 것을 특징으로 한다.

[0013] 또한, 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 상기 침입방지결정모듈은, 상기 침입탐지모듈이 위협정보를 제공하고 상기 침입방지실행모듈이 패킷 플로우 테이블 조회를 요청하면, 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하고, 결과를 플로우 엔트리에 반영하여 상기 침입방지실행모듈에 설치하고 동작지침에 따라 플로우를 처리하도록 하는 것을 특징으로 한다.

[0014] 이 때, 상기 침입방지결정모듈은, 보안 규정에 따라 내부네트워크에 대한 접근 허가 또는 접근 거부를 결정하는 침입방지 결정부; 침입탐지모듈과 침입방지실행모듈을 직접 연결하는 경우 네트워크 간 환경을 설정하는 시스템 연동부; 비인가 침입방지실행모듈과 비인가 침입탐지모듈이 침입방지결정모듈에 접근하는 것을 차단하기 위해 IP주소 기반의 접근 제어를 수행하는 접근 제어부; 상기 침입탐지모듈에 의해 확인된 위협 정보가 저장되는 보안위협 데이터베이스; 를 더 포함하는 것을 특징으로 한다.

[0015] 아울러, 상기 시스템 연동부는, 시스템 명령을 이용하여 패킷 필터링과, IP 패킷의 네트워크 주소와 포트 주소를 변경하며, IP패킷의 캡슐화 및 역캡슐화 하는 것을 특징으로 하며, 상기 시스템 명령은, FORWARD, DROP, SET_FIELD, SET_TUNNEL 명령 중 하나 이상을 포함하고, 상기 시스템 연동부는, 침입탐지프로그램 또는 방화벽의 운용환경을 모사하여, 네트워크 주소변경 방식을 통해 자동적으로 네트워크간 환경을 설정하는 것을 특징으로 한다.

[0016] 또한, 상기 시스템 연동부는, 공격자의 IP 주소를 포함하는 보안 위협 정보를 수집, 개방 또는 공유하여 다수의 서버에 대한 공격을 협력적으로 방지하는 것을 특징으로 한다.

[0017] 이어, 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 상기 침입방지실행모듈은, 패킷이 수신되면 정합 테이블의 우선순위에 따라 플로우 엔트리를 검색하고, 할당된 동작지침에 따라 패킷을 처리하는 것을 특징으로 한다. 이 때, 상기 정합 테이블은, 완전일치 정합(exact match), 시그니처 정합(signature match), 와일드카드 정합(wildcard match)의 순으로 우선순위인 것을 특징으로 한다.

[0018] 또한, 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 상기 침입방지실행모듈은, 패킷의 시그니처(signature)를 미리 저장하고, 시그니처 기반의 패킷 처리 국지화를 위한 블룸 필터(Bloom filter)를 사용하는 것을 특징으로 한다.

[0019] 이 때, 상기 침입방지실행모듈은, 활성 블룸 필터와 대기 블룸 필터를 포함하여 플로우 엔트리를 구성하고, (수학식 1)에 따라 상기 활성 블룸 필터에 t개 이상의 플로우가 기록되면 해당 필터를 초기화한 후 대기 상태로 전환하며, 대기 블룸 필터를 활성 상태로 전환하는 것을 특징으로 한다.

[0020] (수학식 1)

[0021] $$t = \frac{-m(\ln 2)^2}{\ln \alpha} \leq n$$

[0022] (m: 블룸 필터의 비트 수, n: 플로우 시그니처의 수, α: 기대 위양성 확률)

[0023] 또한, 상기 침입방지실행모듈은, n이 (수학식 2)의 조건에 맞는 경우, 활성 블룸 필터와 대기 블룸 필터 모두에 시그니처를 남기는 것을 특징으로 한다.

[0024] (수학식 2)

[0025] $$\beta \cdot t < n < t, (0 < \beta < 1)$$

[0026] (β: 기대 위양성 계수)

[0027] 또한, 상기 침입방지실행모듈은, 플로우(f)가 입력되면 침입방지결정모듈에 테이블 조회를 요청하여 SDN 메시지를 통해 상기 플로우에 대한 완전일치 정합 엔트리를 송신받고, 피드백 플로우(f')를 시그니처 정합 테이블에 등록할 것인지 결정하여 피드백 플로우(f')가 입력되면 시그니처 정합을 이루며, 시그니처 정합 엔트리에서 완전일치 정합 엔트리로 규칙 복사(rule clone)를 수행하는 것을 특징으로 한다.

[0028] 또한, 상기 침입방지실행모듈은, 상기 블룸 필터의 시그니처를 삭제하는 경우, 다른 정합 테이블에 기록된 역플로우(f^{-1})의 처리규칙을 변경하여 삭제하는 것을 특징으로 한다.

[0029] 한편, 본 발명의 일 실시 예에 따른 네트워크 침입방지 방법은, (a) 침입탐지모듈이 침입을 탐지하고, 침입방지결정모듈로 위협정보를 전달하는 단계; (b) 침입방지실행모듈이 입력된 패킷에 대하여 플로우 테이블 조회를 요청하는 단계; (c) 침입방지결정모듈이 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하는 단계; (d) 상기 침입방지결정모듈이 결정된 결과를 플로우 엔트리에 반영하여 상기 침입방지실행모듈에 동작지침을 설치하는 단계; (e) 상기 침입방지실행모듈이 동작지침에 따라 플로우를 처리하는 단계; 를 포함한다.

[0030] 이 때, 상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN(Software defined networking)에 의해 상호 연동되는 것을 특징으로 한다.

발명의 효과

[0031] 종래의 침입방지시스템들이 이메일, 그룹웨어, 웹 등을 주요 응용으로 갖는 일반 목적 네트워크에서의 보안 강화를 목적으로 개발되었기 때문에 대용량 데이터전송 시 성능저하를 초래하는 등 과학기술 네트워크에서 응용성능에 부정적인 영향을 주는 단점이 있으나, 본 발명은 모니터링 채널과 데이터 채널을 분리시킴으로써 성능저하의 문제를 완화하며, SDN을 통해 연동함으로써 기존 보안 시스템들과의 정보 공유가 가능하여 다양한 보안위협 정보들이 중앙에서 유지 관리되므로 보안위협에 대한 효과적인 대처가 가능하여 상태기반 방화벽 사용으로 인한 성능병목을 해소할 수 있다.

[0032] 또한, 종래의 침입방지시스템들은 침입탐지, 방지결정, 침입방지의 기능이 하나의 보안장치 내에 통합되어 있기 때문에 장치의 개발 및 구매 비용이 높은 단점이 있으나, 본 발명은 침입방지 기능의 모듈화를 통해 다양한 방화벽 기능을 쉽게 적용하며 오픈소스 침입탐지프로그램 등과 용이하고 유연하게 연동될 수 있으므로 침입 방지 시스템의 구축비용 절감 및 확장성 (extensibility) 향상을 기대할 수 있다.

[0033] 또한, 다수의 침입방지시스템들을 중앙에서 제어할 수 있으므로 보안시스템의 빈번한 설정 변경으로 야기되는 운영비용(operational cost)을 절감하는 효과가 있다.

도면의 간단한 설명

[0034] 도 1, 2는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템을 나타내는 구성도이다.

도 3, 4는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템이 동작하는 방법을 나타내는 순서도이다.

도 5는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 침입방지실행모듈이 패킷 플로우의 국지적 처리를 위해 블룸 필터와 규칙 복사를 이용하는 과정을 나타내는 예시도이다.

도 6은 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 희생자 서버의 수에 따른 공격 교차율을 나타

내는 도표이다.

도 7은 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 블룸 필터 적중률을 나타내는 도표이다.

도 8은 본 발명의 일 실시예에 따른 네트워크 침입방지 방법을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0035] 이하, 첨부된 도면들을 참조하여 본 발명에 따른 '네트워크 침입방지 시스템'을 상세하게 설명한다. 설명하는 실시 예들은 본 발명의 기술 사상을 통상의 기술자가 용이하게 이해할 수 있도록 제공되는 것으로 이에 의해 본 발명이 한정되지 않는다. 또한, 첨부된 도면에 표현된 사항들은 본 발명의 실시 예들을 쉽게 설명하기 위해 도식화된 도면으로 실제로 구현되는 형태와 상이할 수 있다.

[0036] 한편, 이하에서 표현되는 각 구성부는 본 발명을 구현하기 위한 예일 뿐이다. 따라서, 본 발명의 다른 구현에서는 본 발명의 사상 및 범위를 벗어나지 않는 범위에서 다른 구성부가 사용될 수 있다. 또한, 각 구성부는 순전히 하드웨어 또는 소프트웨어의 구성만으로 구현될 수도 있지만, 동일 기능을 수행하는 다양한 하드웨어 및 소프트웨어 구성들의 조합으로 구현될 수도 있다. 또한, 하나의 하드웨어 또는 소프트웨어에 의해 둘 이상의 구성부들이 함께 구현될 수도 있다.

[0037] 또한, 어떤 구성요소들을 '포함'한다는 표현은, '개방형'의 표현으로서 해당 구성요소들이 존재하는 것을 단순히 지칭할 뿐이며, 추가적인 구성요소들을 배제하는 것으로 이해되어서는 안 된다.

[0038] 또한, '제1, 제2' 등과 같은 표현은, 복수의 구성들을 구분하기 위한 용도로만 사용된 표현으로써, 구성들 사이의 순서나 기타 특징들을 한정하지 않는다.

[0039] 한편, 이상에서 살펴본 본 발명의 일 실시 예에 따른 '네트워크 침입방지 시스템'은, 카테고리는 상이하지만 본 발명의 일 실시 예에 따른 '네트워크 침입방지 방법'과 실질적으로 동일한 기술적 특징을 포함할 수 있다.

[0040] 따라서, 중복 기재를 방지하기 위하여 자세히 기재하지는 않았지만, 상기 '네트워크 침입방지 시스템'과 관련하여 상술한 특징들은, 본 발명은 일 실시 예에 따른 '네트워크 침입방지 방법'에도 당연히 유추 적용될 수 있다. 또한, 반대로, 상기 '네트워크 침입방지 방법'과 관련하여 상술한 특징들은 상기 '네트워크 침입방지 시스템'에도 당연히 유추 적용될 수 있다.

[0041] 도 1, 2는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템을 나타내는 구성도이다.

[0042] 도 1을 참조하면, 네트워크 침입방지 시스템(110)은 침입탐지모듈(110), 침입방지결정모듈(120), 침입방지실행모듈(130)을 포함하며, 침입탐지모듈은 위협분석부(111)와 위협보고부(112), 침입방지결정모듈은 침입방지 결정부(121), 시스템 연동부(122), 접근 제어부(123), 데이터베이스(124)를 포함할 수 있다.

[0043] 침입탐지모듈(110)은 소프트웨어 에이전트이며, logwatch, OSSEC(Open Source SECurity) 등 침입탐지프로그램과 연계하여, 내부 네트워크의 보안 위협을 실시간으로 분석하는 위협분석부(111) 및 분석 결과를 침입방지결정모듈에 보고하는 위협보고부(112) 를 포함한다. 이 때, 위협분석부는 rsyslog 등을 이용해 내부 네트워크 및 시스템의 보안위협을 취합하고 침입 방지 시스템의 보안 정책에 따라 보안 위협을 분류하며, 보안 위협을 단계별로 재분류하고, 위협보고부는, E2N(End to Network) 메시지를 구성한 후 상기 침입방지결정모듈에 보고하게 된다.

[0044] 침입방지결정모듈(120)은 침입탐지모듈이 위협정보를 제공하고 침입방지실행모듈이 패킷 플로우 테이블 조회를 요청하면, 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하고, 결과를 플로우 엔트리에 반영하여 침입방지실행모듈에 설치하고 동작지침에 따라 패킷 플로우를 처리하도록 한다.

[0045] 이 때, 침입방지결정모듈은 보안 규정에 따라 내부네트워크에 대한 접근 허가 또는 접근 거부를 결정하는 침입방지 결정부(121), 침입탐지모듈과 침입방지실행모듈을 직접 연결하는 경우 네트워크 간 환경을 설정하는 시스템 연동부(122), 비인가 침입방지실행모듈과 비인가 침입탐지모듈이 침입방지결정모듈에 접근하는 것을 차단하기 위해 IP주소 기반의 접근 제어를 수행하는 접근 제어부(123), 상기 침입탐지모듈에 의해 확인된 위협 정보가 저장되는 보안위협 데이터베이스(124)를 포함한다.

[0046] 또한, 시스템 연동부는 침입탐지프로그램 또는 방화벽의 운용환경을 모사하여, 네트워크 주소변경 방식을 통해 자동적으로 네트워크간 환경을 설정할 수 있으며, 시스템 연동부는, 공격자의 IP 주소를 포함하는 보안 위협 정보를 수집, 개방 또는 공유하여 다수의 서버에 대한 공격을 협력적으로 방지할 수 있다.

[0047] 침입방지실행모듈(130)은 설치된 플로우 엔트리의 동작지침에 따라 침입 방지를 실행한다. 침입방지실행모듈의 시스템 소프트웨어는 CPU 포트로 FORWARD된 패킷에 임시 플로우 엔트리를 할당해 데이터평면에 설치한 후 침입방지결정모듈에게 테이블 조회를 요청한다. 즉, 침입방지실행모듈은 문제점을 해결하기 위해 패킷을 '선 포워드 후 조회' 한다. 이후 침입방지결정모듈은 초기 연결 설정 시 상기 플로우 처리 과정을 침입방지실행모듈에 설정한다.

[0048] 한편, 상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN(Software defined networking)에 의해 상호 연동된다.

[0049] SDN은 네트워크 제어와 포워딩 기능을 분리하고 오픈플로우 등 개방형 API(Application Programming Interface)를 통해 제어 기능과 포워딩 기능을 상호 연동시키는 것을 특징으로 갖는 네트워킹 접근방식이다. 중앙 집중화된 컨트롤러에서 패킷 플로우에 대한 제어와 네트워크 인프라에 대한 환경 설정(configuration)이 가능하기 때문에 네트워크 상황 변화에 민첩히 대응할 수 있다. 또한, 네트워크 자원에 대한 설정, 관리, 보호, 최적화 등의 프로세스들을 SDN 프로그램화함으로 네트워크 운영 업무를 자동화할 수 있다.

[0050] SDN에서 패킷 플로우에 대한 출력 포트 검색 절차는 다음과 같다. 패킷이 도착하면 네트워크 스위치는 로컬 플로우 테이블에서 플로우 엔트리를 조회하고 지정된 동작지침(action)에 따라 패킷을 처리한다. 플로우 엔트리가 존재하지 않으면 수신된 패킷을 캡슐화한 후 컨트롤러에게 전달함으로써 일종의 플로우 테이블 조회(flow table lookup)과정을 수행한다. 컨트롤러의 SDN 프로그램은 전달받은 패킷의 동작지침을 결정한 후 개방형 API를 통해 네트워크 스위치에 플로우 엔트리를 설치한다.

[0051] 침입탐지모듈(110)은 침입탐지프로그램과 연계하여 동작하며 보안위협을 분석하고, 침입이 탐지되면 침입방지결정모듈에게 위협정보를 전달한다. 침입방지결정모듈(120)은 패킷 플로우에 대한 침입방지를 결정하며, 상기 침입탐지모듈과 침입방지실행모듈에 대한 접근제어 기능을 갖는다. 침입방지실행모듈(130)은 내부 네트워크에 대한 침입방지 기능을 수행하며, SDN 기술에 의해 상기 침입방지결정모듈에 제어된다. 위와 같은 네트워크 침입방지 시스템은, 외부 네트워크로부터 내부 네트워크로 침입을 시도할 때, 접근 허가 여부를 결정하게 된다.

[0052] 이 때, 내부 네트워크는 특히 Science DMZ를 이용하는 것을 특징으로 할 수 있다. Science DMZ는 독자적인 전송장비, 네트워크 구성 및 보안 정책을 갖는 일종의 부분망으로써 기업 등의 사설망(intranet)과 인터넷 망의 중간 지역에 구축되어 데이터 전송 성능을 가속시키는 역할을 한다. 대용량 과학기술데이터의 전송 속도를 향상시키기 위해 상태기반 방화벽의 사용이 지양되며 광역 데이터전송시 전송 성능 가속을 위해 전용 데이터전송노드(DTN, Data Transfer Node)를 이용한다. WAN과 LAN의 접점에 DTN을 설치하고 전송 구간을 분리해 데이터를 수신 받는다면 LAN 구간에서 발생하는 패킷 손실이 WAN 구간에 영향을 주지 않으므로 TCP 성능의 간접적 향상을 기대할 수 있다.

[0053] 한편, SDN에서 각 모듈을 물리적으로 분리함으로써, HOF(Head-Of-Flow delay) 문제와 플로우 테이블 조회 병목(lookup bottleneck)이 발생하게 된다. HOF 문제는 SDN 스위치가 플로우에 속한 최초 패킷에 대해 플로우 테이블 조회를 수행하면서 소요되는 SDN 메시지의 왕복시간 및 처리시간 등으로 인해 발생하며, 플로우 테이블 조회 병목은 네트워크 스위치에서 발생하는 요청 병목과 컨트롤러의 SDN 메시지 처리 병목으로 구분할 수 있다. 위의 HOF와 조회 병목 문제는 TCP의 RTO(Retransmission TimeOut)에 부정적인 영향을 주기 때문에 TCP 성능 저하를 초래할 수 있다.

[0054] 따라서, 본 발명의 네트워크 침입방지 시스템은, 인가된 패킷의 시그니처(signature)를 침입방지실행모듈에 미리 저장한 후 해당 패킷의 처리를 침입방지실행모듈에게 위임함으로써 HOF 문제와 조회 병목을 완화시킨다. 또한 시그니처 기반의 패킷 처리 국지화를 위해 블룸 필터를 적용하며, 블룸 필터에 대한 자세한 설명은 도 5를 참조하기로 한다.

[0055] 도 3, 4는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템이 동작하는 방법을 나타내는 순서도이다.

[0056] 도 3을 참조하면, 네트워크 침입방지 시스템은, 침입탐지모듈, 침입방지결정모듈, 침입방지실행모듈을 포함한다. 먼저 침입탐지모듈이 침입을 탐지하고, 침입방지결정모듈로 위협정보를 전달한다. 이어, 침입방지실행모듈이 입력된 패킷에 대하여 플로우 테이블 조회를 요청하고, 침입방지결정모듈이 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정한다. 침입방지결정모듈은 결정된 결과를 플로우 엔트리에 반영하여 침입방지실행모듈에 동작지침을 설치하고, 동작지침에 따라 플로우를 처리하게 된다.

[0057] 이 때, 네트워크 침입방지 시스템을 구성하는 각 모듈들은 물리적으로 분리된 상태에서 SDN 기술을 이용해 상호 연동시키는 비용효율적 침입 방지 프레임워크이다. 침입방지실행모듈은, 방지 결정 기능 등을 침입방지결정모듈에게 이관함으로써 그 기능을 간소화할 수 있으며, 기능 간소화는 장비 가격을 낮추고 성능 병목 문제를 해결하는데 효과적이고, 침입방지결정모듈에 의한 방지 결정을 통해 탐지된 보안 위협에 대한 신속하고 동적인 대처가 가능하다. 또한, 탐지된 공격자 정보를 집중화하고 유관 컨트롤러, IPS, 방화벽 등과 공유함으로써 DDoS등 분산 서비스 공격 등에 효과적으로 대응할 수 있다.

[0058] 한편, 네트워크 침입방지 시스템은 탐지 기능을 분리시킴으로써 DPI(Deep Packet Inspection) 등 복잡한 기능 수행으로 야기되는 모듈의 성능 저하 문제를 해결한다. 또한, Snort, OSSEC, Modsecurity 등 침입탐지프로그램 및 방화벽들과의 연계가 용이해지기 때문에 초기 구축비용을 절감하고 시스템 확장성을 높일 수 있으며, 호스트 IDS(HIDS), 네트워크 IDS(NIDS), 또는 혼합 IDS(Hybrid IDS) 등 다양한 형태의 IDS(Intrusion Detection System)를 조합해 침입 탐지에 활용 가능하므로 각 IDS가 갖는 단점을 상쇄할 수 있다.

[0059] 도 5는 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 침입방지실행모듈이 패킷 플로우의 국지적 처리를 위해 블룸 필터와 규칙 복사를 이용하는 과정을 나타내는 예시도이다.

[0060] 도 5를 참조하면, 침입방지실행모듈은 패킷이 수신되면 정합 테이블의 우선순위에 따라 플로우 엔트리를 검색하고, 할당된 동작지침에 따라 패킷을 처리한다. 이 때, 정합의 우선순위는 완전일치 정합(exact match), 시그니처(signiture) 정합, 와일드카드 정합(wildcard match)의 순으로, 패킷이 수신되면 침입방지실행모듈은 각 정합 테이블의 우선 순위에 따라 플로우 엔트리를 검색하고 할당된 동작지침에 따라 패킷을 처리한다.

[0061] 또한, 침입방지실행모듈은, 패킷의 시그니처(signature)를 미리 저장하고, 시그니처 기반의 패킷 처리 국지화를 위한 블룸 필터(Bloom filter)를 사용할 수 있다.

[0062] 블룸 필터(133, 134)는 위양성(false positive)과 공간-효율성 간에 상반관계를 갖는 확률적 데이터 구조이다. 이 때, 시그니처 정합을 위한 플로우 엔트리는 위양성 문제를 해결하기 위해 활성 블룸 필터와 대기 블룸 필터를 포함하는 2개의 블룸 필터를 교대로 이용하여 구성한다. 이는 위양성 확률을 기대 위양성 확률 이하로 유지하기 위해 블룸 필터에 n개 이하의 플로우 시그니처만 남기는 방식에 해당한다.

[0063] 활성 블룸 필터에 t개 이상의 플로우가 기록되면, 해당 필터를 초기화한 후 대기 상태로 전환하며, 대기 블룸 필터를 활성 상태로 전환한다.

[0064] $$t = \frac{-m(\ln 2)^2}{\ln \alpha} \leq n$$ (수학식 1)

[0065] (m: 블룸 필터의 비트 수, n: 플로우 시그니처의 수, α: 기대 위양성 확률)

[0066] 또한, 규칙 복사가 수행되지 않은 플로우의 시그니처 정보를 삭제하는 문제점을 해결하기 위하여, 침입방지실행모듈은 플로우 시그니처의 수인 n이 (수학식 2)의 조건에 맞는 경우, 활성 블룸 필터와 대기 블룸 필터 모두에 시그니처를 남김으로써 필터 초기화로 인한 문제를 해결할 수 있다.

[0067] $$\beta \cdot t < n < t, (0 < \beta < 1)$$ (수학식 2)

[0068] (β: 기대 위양성 계수)

[0069] 이 때, 확률 α=0.001, 계수 β=1인 것이 바람직하다.

[0070] 이어, 침입방지실행모듈은 외부 네트워크로부터 플로우(f)가 입력되면 침입방지결정모듈에 테이블 조회를 요청하여 SDN 메시지를 통해 플로우에 대한 완전일치 정합 엔트리를 송신받고, 피드백 플로우(f')를 시그니처 정합 테이블에 등록할 것인지 결정한다. 이 때 SDN 메시지에 피기백(piggyback)하여 함께 전달한다.

[0071] 피드백 플로우(f')가 입력되면 시그니처 정합을 이루며, 시그니처 정합 엔트리에서 완전일치 정합 엔트리로 규칙 복사(rule clone)를 수행하게 되며, 규칙 복사를 통하여 제한된 하드웨어 자원을 비용 효과적으로 사용할 수 있게 된다. 예를 들어, 하나의 통신 세션이 데이터 플로우와 피드백 플로우로 구성된다고 가정하면, 블룸 필터와 규칙 복사를 적용하여 N개의 통신 세션에 대해 테이블 조회 횟수가 2N에서 N으로 50% 줄고 SDN 메시지의 발생도 4N에서 2N으로 감소하기 때문에 조회 병목 문제와 메시지 부하를 줄일 수 있다. 한 번의 테이블 조회는 SDN 메시지를 2번씩(요청과 응답) 발생시킨다.

[0072] 한편, 블룸 필터의 사용은 네트워킹 상태에 대한 일관성(consistency) 문제를 발생할 수 있다.

[0073] 먼저, 블룸 필터가 시그니처 삭제를 지원하지 않기 때문에 플로우의 상태 변화가 요구될 때, 필터에서 시그니처를 삭제할 수 없는 문제가 발생할 수 있으며, 이는 침입방지실행모듈은 블룸 필터의 시그니처를 삭제하는 경우, 다른 정합 테이블에 기록된 역 플로우(f-1)의 처리규칙을 변경하여 삭제하여 문제를 해결할 수 있다.

[0074] 두번째로, 네트워크 침입방지 시스템은, 위양성 문제를 완화하기 위해 블룸 필터를 초기화시키며, 블룸 필터는 국지적으로 초기화되기 때문에 침입방지결정모듈이 유지하는 플로우 테이블에 일관성 문제가 발생할 수 있다. 이는 블룸 필터에 의해 시그니처 정합된 플로우는 규칙 복사되어 최종적으로 완전일치 테이블에 저장하고, 네트워크 침입방지 시스템은 완전일치 테이블에 저장된 플로우 엔트리 중 접근 허가된 플로우에 대해서 타임아웃(timeout)시키는 방법으로 일관성 문제를 해결할 수 있다.

[0075] 도 6은 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 희생자 서버의 수에 따른 공격 교차율을 나타내는 도표이다.

[0076] 본 발명의 성능 평가 수행에 있어서, 동일한 서브넷에 구축된 총 7대의 희생자(victim) 서버가 OSSEC 서버에게 로그 정보를 전달하면 침입탐지모듈은 무작위 대입 공격(brute force attack)을 시도한 공격자 IP 주소를 추출해 침입방지결정모듈에게 전달한다. 도 6의 공격자 정보는 약 50일 간 수집되었으며, 수집 기간 동안 관측된 서버 별 총 공격자(IP 주소) 수는 평균 158개이다. 단, 공격자 수는 공격의 횟수 또는 공격 성공의 횟수를 의미하지 않는다.

[0077] 공격 교차율은 임의의 희생자 서버 에 대한 공격 가 다른 희생자 서버 중 한 곳 이상을 공격하는 비율로 정의한다. 도 6에서, 희생자 서버의 수가 증가함에 따라 공격 교차율도 높아짐을 확인할 수 있다. 따라서 공격 정보를 공유하고 경계선에서 방어함으로써 교차율이 높은 보안 위협에 대해 효과적으로 대응할 수 있다. 바꿔 말하면, 네트워크 침입방지 시스템은 교차율이 높은 공격들로부터 내부 네트워크가 포함하는 서버들을 효과적으로 방어할 수 있다.

[0078] 도 7은 본 발명의 일 실시예에 따른 네트워크 침입방지 시스템의 블룸 필터 적중률을 나타내는 도표이다.

[0079] 본 발명의 성능 수행 평가에 있어서, 패킷을 국지적으로 처리하기 위해 적용된 블룸 필터의 높은 적중률은 상대적으로 낮은 조회 병목과 네트워크 대역폭 소비를 의미한다. 적중률을 측정하기 위해 희생자 서버에서 발생된 웹 플로우(HTTP flow)들을 침입방지결정모듈에서 분석하며, 침입방지결정모듈은 외부 접근이 허가된 플로우의 역 플로우 정보를 침입방지실행모듈의 블룸 필터에 등록한다. 블룸 필터에 의해 국지적으로 처리되지 못한 플로우의 동작지침을 얻기 위해 플로우 테이블 조회가 요구된다.

[0080] 도 7을 참조하면, 4회에 걸친 측정 결과 94% 이상의 블룸 필터 적중률을 보였다. 바꿔 말하면 네트워크 침입방지 시스템의 응용 시나리오에서 시그니처 정합 엔트리를 이용하면 메시지 발생회수가 완전일치 정합 엔트리를 이용했을 때보다 최소 46.9% 이상 감소한다. 소개된 네트워크 침입방지 시스템의 응용 시나리오에서 메시지 발생회수와 대역폭 소비에 대한 최대 성능이득은 50%이다. 플로우 테이블 조회 요청 메시지와 응답 메시지의 크기가 동일하다고 가정하면 네트워크 대역폭 소비도 동일한 비율로 감소한다.

[0081] 블룸 필터에 비 적중(missed flows)된 플로우가 발생하는 이유는 역 플로우 정보가 블룸 필터에 등록되기 이전

에 해당 역 플로우가 침입방지실행모듈에 도착했기 때문이며, 희생자 서버와 접속 요청한 웹서버의 왕복지연시간이 플로우 테이블 조회시간 보다 짧을 경우 비 적중 풀로우가 발생한다.

[0082] 도 8은 본 발명의 일 실시예에 따른 네트워크 침입방지 방법을 나타내는 순서도이다.

[0083] 도 8을 참조하면, 본 발명의 일 실시예에 따른 네트워크 침입방지 방법은, (a) 침입탐지모듈이 침입을 탐지하고, 침입방지결정모듈로 위협정보를 전달하는 단계; (b) 침입방지실행모듈이 입력된 패킷에 대하여 플로우 테이블 조회를 요청하는 단계; (c) 침입방지결정모듈이 설정된 보안 정책에 따라 접근 허락 또는 거부를 결정하는 단계; (d) 상기 침입방지결정모듈이 결정된 결과를 플로우 엔트리에 반영하여 상기 침입방지실행모듈에 동작지침을 설치하는 단계; (e) 상기 침입방지실행모듈이 동작지침에 따라 플로우를 처리하는 단계; 를 포함한다.

[0084] 이 때, 상기 침입탐지모듈, 상기 침입방지결정모듈, 상기 침입방지실행모듈은 물리적으로 분리되어 있으며, SDN(Software defined networking)에 의해 상호 연동되는 것을 특징으로 한다.

[0085] 위에서 설명된 본 발명의 실시 예들은 예시의 목적을 위해 개시된 것이며, 이들에 의하여 본 발명이 한정되는 것은 아니다. 또한, 본 발명에 대한 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 사상과 범위 안에서 다양한 수정 및 변경을 가할 수 있을 것이며, 이러한 수정 및 변경은 본 발명의 범위에 속하는 것으로 보아야 할 것이다.

부호의 설명

[0086] 100: 네트워크 침입방지 시스템

110: 침입탐지모듈

111: 위협분석부

112: 위협보고부

120: 침입방지결정모듈

121: 침입방지 결정부

122: 시스템 연동부

123: 접근 제어부

124: 데이터베이스

130: 침입방지 실행모듈

131: 완전정합 테이블

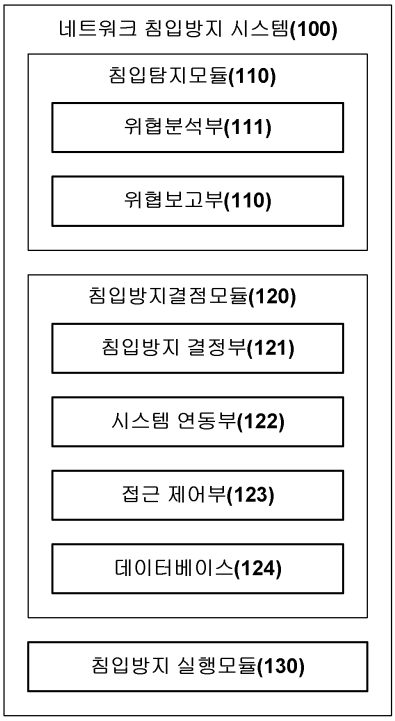
132: 시그니처 정합 테이블

133: 활성 블룸필터

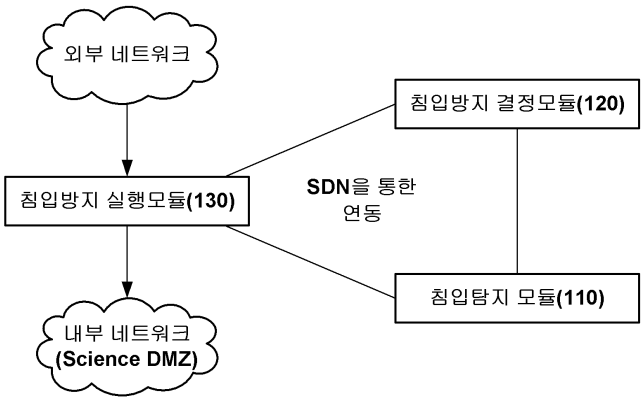
134: 대기 블룸필터

도면

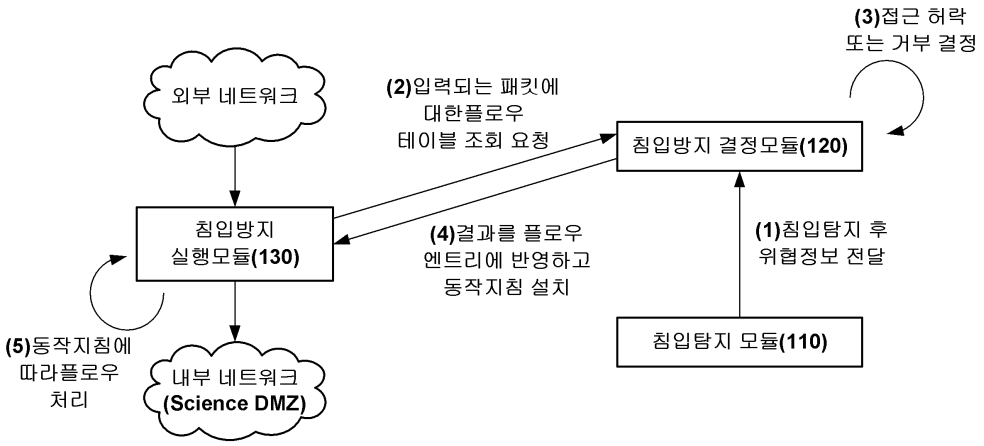
도면1


네트워크 침입방지 시스템(100)
침입탐지모듈(110)
위협분석부(111)
위협보고부(110)
침입방지결정모듈(120)
침입방지 결정부(121)
시스템 연동부(122)
접근 제어부(123)
데이터베이스(124)
침입방지 실행모듈(130)

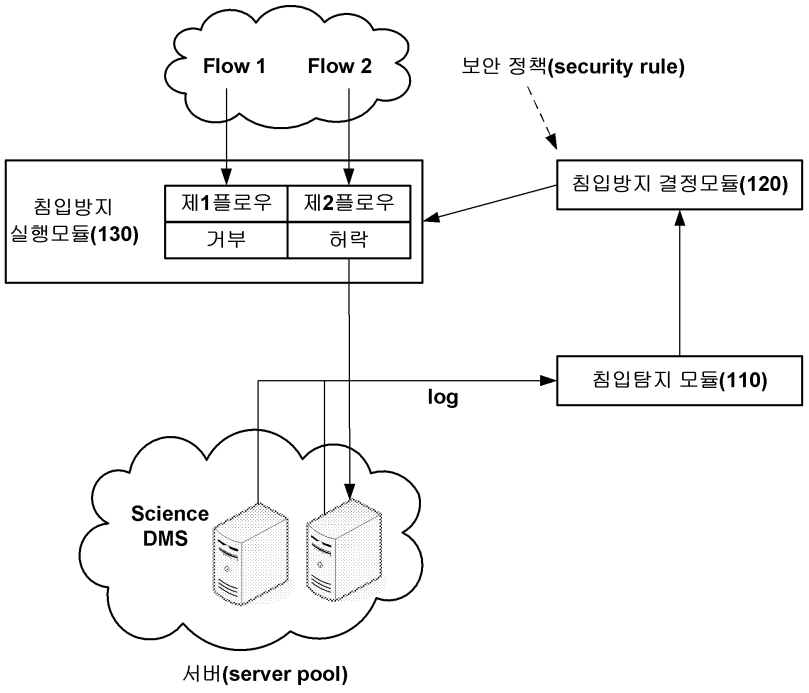
도면2


외부 네트워크
침입방지 결정모듈(120)
침입방지 실행모듈(130)
SDN을 통한
연동
침입탐지 모듈(110)
내부 네트워크
(Science DMZ)

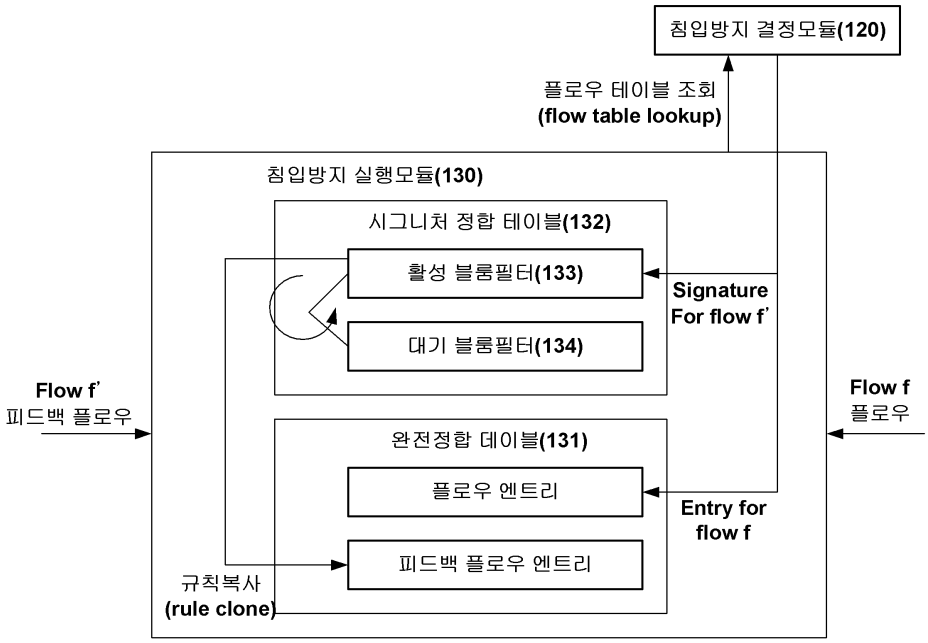
도면3


(3)접근 허락
또는 거부 결정
외부 네트워크
(2)입력되는 패킷에
대한플로우
테이블 조회 요청
침입방지 결정모듈(120)
침입방지
실행모듈(130)
(4)결과를 플로우
엔트리에 반영하고
동작지침 설치
(1)침입탐지 후
위협정보 전달
(5)동작지침에
따라플로우
처리
내부 네트워크
(Science DMZ)
침입탐지 모듈(110)

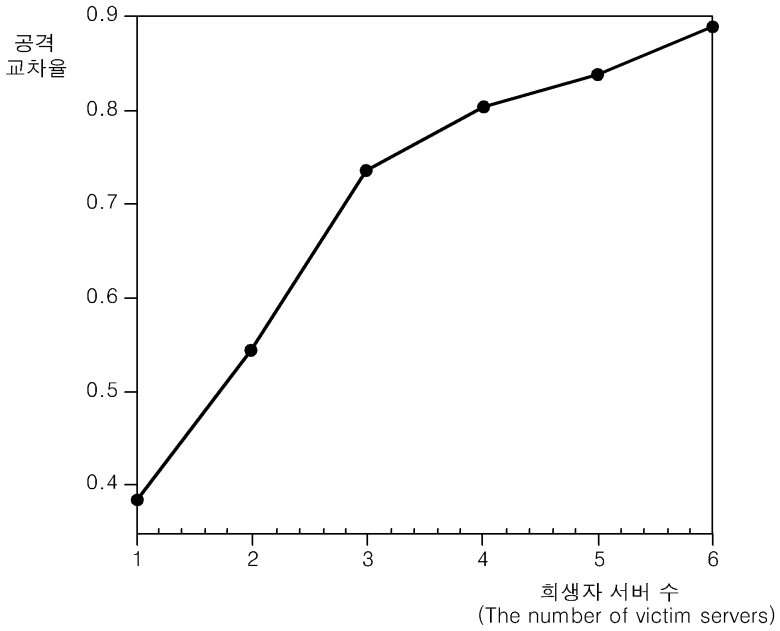
도면4


Flow 1
Flow 2
보안 정책(security rule)
침입방지
실행모듈(130)
제1플로우
제2플로우
거부
허락
침입방지 결정모듈(120)
침입탐지 모듈(110)
log
Science
DMS
서버(server pool)

도면5


침입방지 결정모듈(120)
플로우 테이블 조회
(flow table lookup)
침입방지 실행모듈(130)
시그니처 정합 테이블(132)
활성 블룸필터(133)
대기 블룸필터(134)
Signature
For flow f'
Flow f'
피드백 플로우
Flow f
플로우
완전정합 데이블(131)
플로우 엔트리
Entry for
flow f
피드백 플로우 엔트리
규칙복사
(rule clone)

도면6


공격
교차율
0.9
0.8
0.7
0.6
0.5
0.4
1
2
3
4
5
6
희생자 서버 수
(The number of victim servers)

도면7

총 플로우 수 (total flow)	비적중된 플로우 (missed flow)	블룸 필터 적중률(%) (hit rate)
37,953	2,277	94.0
20,269	466	97.7
65,467	916	98.6
56,372	394	99.3

도면8