(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년06월11일
(11) 등록번호 10-2263755
(24) 등록일자 2021년06월04일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 12/859* (2013.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 67/2814 (2013.01)
H04L 47/2475 (2013.01)
(21) 출원번호 10-2019-0128326
(22) 출원일자 2019년10월16일
심사청구일자 2019년10월16일
(65) 공개번호 10-2021-0045545
(43) 공개일자 2021년04월27일
(56) 선행기술조사문헌
KR101523253 B1
(뒷면에 계속)
전체 청구항 수 : 총 14 항

(73) 특허권자
(주)소만사
서울특별시 영등포구 영신로 220 (영등포동8가)
(72) 발명자
김태완
서울특별시 마포구 월드컵북로 502-36 1010동 901호 (상암동,상암월드컵파크10단지아파트)
최일훈
서울특별시 양천구 목동서로 340 909동 401호 (신정동,신시가지9단지아파트)
(74) 대리인
윤재승

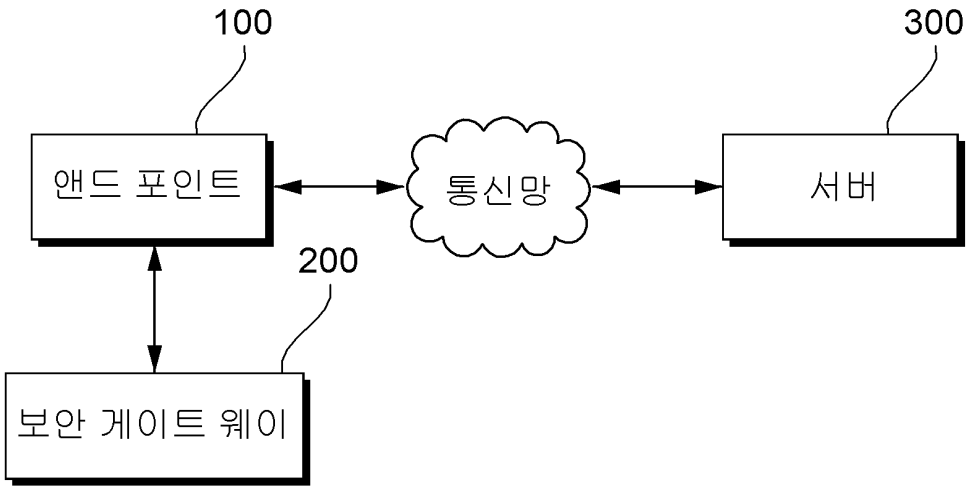
심사관 : 장상배

(54) 발명의 명칭 **엔드포인트의 트래픽에 대한 포워딩 시스템 및 방법**

(57) 요 약

본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 시스템은 애플리케이션에서 생성되는 트래픽을 서버로 전송하는 엔드포인트; 및 상기 트래픽을 상기 엔드포인트로부터 전달받아서, 상기 트래픽 중 SSL 트래픽의 정보 보안과 관련한 데이터 분석을 수행하는 보안 게이트웨이를 포함하고, 상기 엔드포인트는, 상기 트래픽을 상기 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하고, 상기 트래픽의 전송과 관련한 리다이렉션을 수행하는 로컬 리다이렉션 모듈; 및 상기 로컬 리다이렉션 모듈의 리다이렉션에 따라, 상기 로컬 리다이렉션 모듈에서 전달받은 상기 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행한 후에, 복호화 SSL 트래픽을 상기 보안 게이트웨이로 포워딩하는 로컬 프록시 모듈을 포함하는 것을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 63/18 (2013.01)
H04L 69/162 (2013.01)
H04L 69/22 (2013.01)

(56) 선행기술조사문헌
KR1020140110058 A
KR1020170106694 A
KR1020190048943 A
KR1020190083160 A

이 발명을 지원한 국가연구개발사업

과제고유번호	2016-0-00078
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원 (IITP)
연구사업명	정보보호핵심원천기술개발사업
연구과제명	맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발
기 여 율	1/1
과제수행기관명	한국전자통신연구원
연구기간	2019.01.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

애플리케이션에서 생성되는 트래픽을 서버로 전송하는 엔드포인트; 및

상기 트래픽을 상기 엔드포인트로부터 전달받아서, 상기 트래픽 중 SSL 트래픽의 정보 보안과 관련한 데이터 분석을 수행하는 보안 게이트웨이를 포함하고,

상기 엔드포인트는,

상기 트래픽을 상기 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하고, 상기 트래픽의 전송과 관련한 리다이렉션을 수행하는 로컬 리다이렉션 모듈; 및

상기 로컬 리다이렉션 모듈의 리다이렉션에 따라, 상기 로컬 리다이렉션 모듈에서 전달받은 상기 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행한 후에, 복호화 SSL 트래픽을 상기 보안 게이트웨이로 포워딩하는 로컬 프록시 모듈을 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 2

청구항 1에 있어서,

상기 로컬 리다이렉션 모듈은,

네트워크 커널기반의 연결 리다이렉션 방식 및 애플리케이션 소켓연결 API 후킹방식 중 적어도 어느 하나의 방식을 이용하여, 상기 트래픽에 대한 리다이렉션을 수행하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 3

청구항 1에 있어서,

상기 로컬 리다이렉션 모듈은,

상기 리다이렉션 정보로서, 상기 서버에 대한 서버 IP 주소정보 및 포트정보와 상기 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 저장하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 4

청구항 1에 있어서,

상기 로컬 프록시 모듈은,

상기 로컬 리다이렉션 모듈의 리다이렉션에 의해 상기 로컬 리다이렉션 모듈과 연결되며, 상기 로컬 리다이렉션 모듈에 저장된 상기 리다이렉션정보를 조회하고,

조회에 따라 상기 리다이렉션정보에 포함된 서버 IP 주소정보 및 포트정보를 이용하여 상기 서버와의 TCP 연결을 수행하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 5

청구항 1에 있어서,

상기 로컬 프록시 모듈은,

상기 복호화 SSL 트래픽을 재암호화하고, 재암화SSL 트래픽을 상기 서버로 전송하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 6

청구항 5에 있어서,

상기 로컬 프록시 모듈은,

상기 트래픽 중 상기 SSL 트래픽이 아닌 Non-SSL 트래픽 또는 상기 복호화 SSL 트래픽의 페이로드 데이터에 대해서 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 상기 보안 게이트웨이로 포워딩하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 7

청구항 1에 있어서,

상기 보안 게이트웨이는,

상기 로컬 프록시 모듈로부터 포워딩된 상기 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 상기 로컬 프록시 모듈로 전송하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 시스템.

청구항 8

엔드포인트를 구성하는 로컬 리다이렉션 모듈은 애플리케이션에서 생성되는 트래픽을 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하는 단계;

상기 로컬 리다이렉션 모듈은 상기 트래픽의 전송과 관련한 리다이렉션을 수행하는 단계;

상기 엔드포인트를 구성하는 로컬 프록시 모듈은 상기 로컬 리다이렉션 모듈의 리다이렉션에 따라, 전달받은 상기 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행하는 단계; 및

상기 로컬 프록시 모듈은 복호화 SSL 트래픽을 보안 게이트웨이로 포워딩하는 단계를 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 9

청구항 8에 있어서,

상기 리다이렉션정보를 저장하는 단계는,

상기 서버에 대한 서버 IP 주소정보 및 포트정보와 상기 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 상기 리다이렉션정보로서 저장하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 10

청구항 8에 있어서,

상기 리다이렉션을 수행하는 단계는

네트워크 커널기반의 연결 리다이렉션 방식 및 애플리케이션 소켓연결 API 후킹방식 중 적어도 어느 하나의 방식을 이용하여, 상기 트래픽에 대한 리다이렉션을 수행하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 11

청구항 8에 있어서,

상기 로컬 프록시 모듈은 상기 로컬 리다이렉션 모듈의 리다이렉션에 의해 상기 로컬 리다이렉션 모듈과 연결되며, 상기 로컬 리다이렉션 모듈에 저장된 상기 리다이렉션정보를 조회하는 단계; 및

상기 로컬 프록시 모듈은 조회에 따라 상기 리다이렉션정보에 포함된 서버 IP 주소정보 및 포트정보를 이용하여 상기 서버와의 TCP 연결을 수행하는 단계를 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 12

청구항 8에 있어서,

상기 로컬 프록시 모듈은 상기 복호화 SSL 트래픽을 재암호화하고, 재암화SSL 트래픽을 상기 서버로 전송하는 단계를 더 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 13

청구항 12에 있어서,

상기 로컬 프록시 모듈은, 상기 트래픽 중 상기 SSL 트래픽이 아닌 Non-SSL 트래픽 또는 상기 복호화 SSL 트래픽의 페이로드 데이터에 대해서 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 상기 보안 게이트웨이로 포워딩하는 단계를 더 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

청구항 14

청구항 12에 있어서,

상기 보안 게이트웨이는, 상기 로컬 프록시 모듈로부터 포워딩된 상기 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 상기 로컬 프록시 모듈로 전송하는 단계를 더 포함하는 것을 특징으로 하는 엔드포인트의 트래픽에 대한 포워딩 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 클라우드 기반의 정보유출 방지솔루션을 제공하기 위하여 엔드포인트에서 트래픽을 클라우드로 포워딩하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 네트워크 정보유출 방지솔루션의 보안 게이트웨이는 프록시 방식으로 네트워크 트래픽을 중계하면서 SSL 인터셉션, 프로토콜을 분석하여 메일, 메시지, 파일 등 인터넷으로 전송되는 데이터에 개인정보 및 기밀정보가 포함되어 있는지 검사한다. 온프레미스 환경의 보안 게이트웨이는 사내 네트워크와 인터넷 사이에 위치하며, 스위치 SPAN(SwitchPortANalyzer) 포트 또는 네트워크 TAP(Tess Access Point)을 이용하여 패킷을 모니터링하는 스니핑방식, 브라우저 등에 HTTP 프록시 설정을 보안 게이트웨이로 설정하는 명시적 프록시 방식, 네트워크를 물리적으로 절체하는 투명한 인라인 프록시 방식, L4 스위치 또는 방화벽을 통한 포트 리다이렉션방식 등으로 구성될 수 있다. 사내에 위치하지 않는 클라우드 기반의 보안 게이트웨이의 경우에는, 브라우저 등에 HTTP 프록시 설정을 보안 게이트웨이로 설정하는 명시적 프록시 방식, 방화벽 또는 라우터를 사용하여 사내-인터넷 트래픽을 보안 게이트웨이로 포워딩하는 GRE 또는 IPSEC 터널링 방식, 엔드포인트의 트래픽을 보안 게이트웨이로 전송하는 일반적인 엔드포인트 트래픽 포워딩방식으로 구성될 수 있다.

[0003] 명시적 프록시방식의 경우에는 인터넷 익스플로러, 크롬, 사파리, 파이어폭스 등 브라우저의 HTTP 프록시 설정을 이용하므로 브라우저 이외의 메신저 등 애플리케이션의 트래픽을 보안 게이트웨이로 포워딩하지 못하는 한계가 있다. 스니핑방식, 투명한 인라인 프록시방식, 포트리다이렉션 방식, GRE 또는 프록시방식의 경우에는 사내 네트워크에서 물리적인 장비 또는 구성이 필요하기 때문에, 노트북 등을이용하여 사외 네트워크환경의 엔드포인트의 트래픽을 보안 게이트웨이로 포워딩하지 못하는 한계가 있다. 일반적인 엔드포인트 트래픽 포워딩 방식의 경우에는 엔드포인트의 트래픽이 클라우드 상에 위치한 보안 게이트웨이의 중계를 거쳐 인터넷으로 송수신되므로 과도한 인터넷 지연이 발생하며, 클라우드 네트워크 사용에 따른 과다한 네트워크 과금이 발생하는 문제가 있다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국 공개특허공보 10-2010-0018022호(공개일 2010년2월16일)

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 과제는, 메일, 메시지, 파일 등 인터넷으로 전송되는 트래픽(데이터)에 개인정보 및 기밀정보가 포함되어 있는지 검사할 수 있도록 엔드포인트에서 브라우저 등 애플리케이션의 인터넷 연결을 로컬 프록시로 리다이렉트하여, Non- SSL 트래픽 및 복호화한 SSL 트래픽을 아웃오브 패스방식으로 클라우드로 포워딩하는 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0006] 상기의 과제를 해결하기 위한 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 시스템은 애플리케이션에서 생성되는 트래픽을 서버로 전송하는 엔드포인트; 및 상기 트래픽을 상기 엔드포인트로부터 전달받아서, 상기 트래픽 중 SSL 트래픽의 정보 보안과 관련한 데이터 분석을 수행하는 보안 게이트웨이를 포함하고, 상기 엔드포인트는, 상기 트래픽을 상기 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하고, 상기 트래픽의 전송과 관련한 리다이렉션을 수행하는 로컬 리다이렉션 모듈; 및 상기 로컬 리다이렉션 모듈의 리다이렉션에 따라, 상기 로컬 리다이렉션 모듈에서 전달받은 상기 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행한 후에, 복호화 SSL 트래픽을 상기 보안 게이트웨이로 포워딩하는 로컬 프록시 모듈을 포함하는 것을 특징으로 한다.

[0007] 상기 로컬 리다이렉션 모듈은, 네트워크 커널기반의 연결 리다이렉션 방식 및 애플리케이션 소켓연결 API 후킹 방식 중 적어도 어느 하나의 방식을 이용하여, 상기 트래픽에 대한 리다이렉션을 수행하는 것을 특징으로 한다.

[0008] 상기 로컬 리다이렉션 모듈은, 상기 리다이렉션 정보로서, 상기 서버에 대한 서버 IP 주소정보 및 포트정보와 상기 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 저장하는 것을 특징으로 한다.

[0009] 상기 로컬 프록시 모듈은, 상기 로컬 리다이렉션 모듈의 리다이렉션에 의해 상기 로컬 리다이렉션 모듈과 연결되며, 상기 로컬 리다이렉션 모듈에 저장된 상기 리다이렉션정보를 조회하고, 조회에 따라 상기 리다이렉션정보에 포함된 서버 IP 주소정보 및 포트정보를 이용하여 상기 서버와의 TCP 연결을 수행하는 것을 특징으로 한다.

[0010] 상기 로컬 프록시 모듈은, 상기 복호화 SSL 트래픽을 재암호화하고, 재암화SSL 트래픽을 상기 서버로 전송하는 것을 특징으로 한다.

[0011] 상기 로컬 프록시 모듈은, 상기 트래픽 중 상기 SSL 트래픽이 아닌 Non-SSL 트래픽 또는 상기 복호화 SSL 트래픽의 페이로드 데이터에 대해서 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 상기 보안 게이트웨이로 포워딩하는 것을 특징으로 한다.

[0012] 상기 보안 게이트웨이는, 상기 로컬 프록시 모듈로부터 포워딩된 상기 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 상기 로컬 프록시 모듈로 전송하는 것을 특징으로 한다.

[0014] 상기의 과제를 해결하기 위한 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 방법은 엔드포인트를 구성하는 로컬 리다이렉션 모듈은 애플리케이션에서 생성되는 트래픽을 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하는 단계; 상기 로컬 리다이렉션 모듈은 상기 트래픽의 전송과 관련한 리다이렉션을 수행하는 단계; 상기 엔드포인트를 구성하는 로컬 프록시 모듈은 상기 로컬 리다이렉션 모듈의 리다이렉션에 따라, 전달받은 상기 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행하는 단계; 및 상기 로컬 프록시 모듈은 복호화 SSL 트래픽을 상기 보안 게이트웨이로 포워딩하는 단계를 포함하는 것을 특징으로 한다.

[0015] 상기 리다이렉션정보를 저장하는 단계는, 상기 서버에 대한 서버 IP 주소정보 및 포트정보와 상기 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 상기 리다이렉션정보로서 저장하는 것을 특징으로 한다.

[0016] 상기 리다이렉션을 수행하는 단계는 네트워크 커널기반의 연결 리다이렉션 방식 및 애플리케이션 소켓연결 API 후킹방식 중 적어도 어느 하나의 방식을 이용하여, 상기 트래픽에 대한 리다이렉션을 수행하는 것을 특징으로 한다.

[0017] 상기 로컬 프록시 모듈은 상기 로컬 리다이렉션 모듈의 리다이렉션에 의해 상기 로컬 리다이렉션 모듈과 연결되며, 상기 로컬 리다이렉션 모듈에 저장된 상기 리다이렉션정보를 조회하는 단계; 및 상기 로컬 프록시 모듈은 조회에 따라 상기 리다이렉션정보에 포함된 서버 IP 주소정보 및 포트정보를 이용하여 상기 서버와의 TCP 연결을 수행하는 단계를 포함하는 것을 특징으로 한다.

[0018] 상기 로컬 프록시 모듈은 상기 복호화 SSL 트래픽을 재암호화하고, 재암화SSL 트래픽을 상기 서버로 전송하는 단계를 더 포함하는 것을 특징으로 한다.

[0019] 상기 로컬 프록시 모듈은, 상기 트래픽 중 상기 SSL 트래픽이 아닌 Non-SSL 트래픽 또는 상기 복호화 SSL 트래픽의 페이로드 데이터에 대해서 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 상기 보안 게이트웨이로 포워딩하는 단계를 더 포함하는 것을 특징으로 한다.

[0020] 상기 보안 게이트웨이는, 상기 로컬 프록시 모듈로부터 포워딩된 상기 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 상기 로컬 프록시 모듈로 전송하는 단계를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0021] 본 발명에서 엔드포인트 트래픽은 아웃오브패스(Out-Of-Path) 방식으로 아웃바운드트래픽 또는 인바운드트래픽을 선택적으로 보안 게이트웨이로 전송하여 분석할 수 있도록 한다.

[0022] 또한, 보안 게이트웨이를 경유하여 모든 아웃바운드 및 인바운드 트래픽을 인터넷으로 송수신하는 일반적인 엔드포인트 트래픽포워딩 방식에 비하여, 과다한 네트워크 지연이나 트래픽 과금 발생 없이 클라우드 기반의 네트워크 정보유출 방지기능을 제공할 수 있다.

[0023] 이에 따라, 사내 네트워크에서의 물리적인 장비 또는 구성 없이, 사내뿐만 아니라 사외의 엔드포인트의 트래픽을 과도한 네트워크 지연 및 네트워크 과금 발생 없이 엔드포인트의 트래픽을 클라우드 상의 보안 게이트웨이 포워딩하여 정보유출 방지를 위한 분석을 수행할 수 있으며, 이러한 정보 유출 방지 분석에도 불구하고, 네트워크 지연이나 트래픽 과금 발생이 최소화될 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 시스템의 구성 블록도이다.

도 2는 도 1에 도시된 엔드포인트를 설명하기 위한 세부 구성블록도이다.

도 3은 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩을 설명하기 위한 각 구성요소들의 동작 수행 참조도이다.

도 4는 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 방법을 설명하기 위한 일 실시예의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명의 실시예들은 당해 기술 분야에서 통상의 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공되는 것이며, 아래의 실시예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 아래의 실시예들로 한정되는 것은 아니다. 오히려, 이들 실시예는 본 개시를 더욱 충실하고 완전하게 하며 당업자에게 본 발명의 사상을 완전하게 전달하기 위하여 제공되는 것이다.

[0026] 본 명세서에서 사용된 용어는 특정 실시예를 설명하기 위하여 사용되며, 본 발명을 제한하기 위한 것이 아니다. 본 명세서에서 사용된 바와 같이 단수 형태는 문맥상 다른 경우를 분명히 지적하는 것이 아니라면, 복수의 형태를 포함할 수 있다. 또한, 본 명세서에서 사용된 바와 같이, 용어 "및/또는"은 해당 열거된 항목 중 어느 하나 및 하나 이상의 모든 조합을 포함한다.

[0028] 이하, 본 발명의 실시예들은 본 발명의 실시예들을 개략적으로 도시하는 도면들을 참조하여 설명한다.

[0029] 도 1은 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 시스템의 구성 블록도이다.

[0030] 도 1을 참조하면, 엔드포인트의 트래픽에 대한 포워딩 시스템은 엔드포인트(100) 및 보안 게이트웨이(200)를 포함하며, 아울러, 이와 연관되는 구성요소로서 서버(300)를 포함할 수 있다.

[0031] 엔드포인트(100)는 애플리케이션에서 생성되는 통신망을 통해 트래픽을 서버(300)로 전송하는 단말기이다. 애플

리케이션은 트래픽을 생성하는 프로그램을 의미할 수 있으며, 메일, 메시지, 파일 등의 생성을 위한 프로그램을 포함할 수 있다. 통신망은 엔드포인트(100)와 서버(300) 사이에서 데이터의 송수신을 위한 네트워크를 형성한다. 통신망은 LAN, WAN 또는 유선 인터넷을 포함하며, 무선인터넷, 휴대인터넷, 3G 이동통신망, 4G 이동통신망 또는 5G 이동통신망을 포함할 수 있다. 엔드포인트(100)에 대한 구체적인 내용은 후술한다.

[0032] 보안 게이트웨이(200)는 트래픽을 엔드포인트(100)로부터 전달받아서, 트래픽 중 SSL 트래픽의 정보 보안과 관련한 데이터 분석을 수행한다. 보안 게이트웨이(200)는 엔드포인트(100)로부터 전송된 트래픽 중에서 SSL 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 엔드포인트(100)로 전송한다. 보안 게이트웨이(200)의 구체적인 동작 내용은 후술한다.

[0033] 서버(300)는 엔드포인트(100)와 연결되어, 엔드포인트(100)로부터 전송된 트래픽을 수신하고, 자신이 생성한 트래픽을 엔드포인트(100)로 전송한다.

[0035] 도 2는 도 1에 도시된 엔드포인트(100)를 설명하기 위한 세부 구성블록도이다.

[0036] 도 2를 참조하면, 엔드포인트(100)는 로컬 리다이렉션 모듈(110) 및 로컬 프록시 모듈(120)을 포함한다.

[0037] 로컬 리다이렉션 모듈(110)은 애플리케이션에 의해 생성된 트래픽을 서버(300)로 전송하기 위한 리다이렉션을 수행한다.

[0038] 애플리케이션의 실행에 따라 서버(300)로 전송하기 위한 트래픽(예를 들어, 메일, 메시지, 파일 등)이 생성되면, 로컬 리다이렉션 모듈(110)은 생성된 트래픽의 전송을 위한 해당 서버(300)의 서버연결정보를 포함하는 리다이렉션정보를 메모리(미도시)에 저장한다.

[0039] 예를 들어, 로컬 리다이렉션 모듈(110)은 애플리케이션의 트래픽 발생에 따른 해당 서버(300) 연결 요청에 대응하여, 서버(300)에 대한 서버 IP 주소정보 및 포트정보에 해당하는 서버연결정보와 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 포함하는 리다이렉션정보를 메모리에 저장한다.

[0040] 로컬 리다이렉션 모듈(110)은 네트워크 커널기반의 연결 리다이렉션 방식 또는 애플리케이션 소켓연결 API 후킹 방식 중 적어도 어느 하나의 방식을 이용하여, 애플리케이션에서 생성된 트래픽에 대한 리다이렉션을 수행한다. 로컬 리다이렉션 모듈(110)은 서버(300)와의 API 연결을 위한 서버연결정보 즉, 서버 IP 주소정보 및 포트정보를 로컬 프록시 모듈(120)에서 서비스하는 루프백 IP 주소정보 및 포트정보로 변경하여 트래픽에 대한 리다이렉션을 수행한다.

[0041] 네트워크 커널기반의 연결 리다이렉션 방식은 Windows WFP(Windows FilteringPlatform), macOS NKE(Network KernelExtensions) 등 네트워크 커널에서 애플리케이션의 인터넷 연결시 로컬 프록시 모듈(120)에서 서비스하는 루프백 IP 주소 및 포트정보로 리다이렉션하는 방식이다. 또한, 애플리케이션 소켓연결 API 후킹방식은 애플리케이션의 connect() 등 소켓연결 API를 후킹하여 애플리케이션에서 인터넷 연결시 로컬 프록시 모듈(120)에서 서비스하는 루프백 IP주소 및 포트정보로 리다이렉션하는 방식이다.

[0042] 로컬 프록시 모듈(120)은 로컬 리다이렉션 모듈(110)의 리다이렉션에 따라, 로컬 리다이렉션 모듈(110)에서 전달받은 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행한 후에, 복호화 SSL 트래픽을 보안 게이트웨이(200)로 전송한다. 또한, 로컬 리다이렉션 모듈(110)에서 전달받은 트래픽 중 Non-SSL 트래픽을 그대로 보안 게이트웨이(200)로 아웃오브패스(Out-Of-Path) 방식으로 포워딩한다. 로컬 프록시 모듈(120)에 대한 상세히 설명하면 다음과 같다.

[0043] 우선, 로컬 프록시 모듈(120)은 로컬 리다이렉션 모듈(110)의 리다이렉션에 의해 로컬 리다이렉션 모듈(110)과 접속된다. 이에 따라, 로컬 프록시 모듈(120)은 로컬 리다이렉션 모듈(10)에 저장된 리다이렉션를 조회하고, 조회에 따라 리다이렉션정보 중에서 추출된 서버 IP 주소정보 및 포트정보를 이용하여 서버(300)와의 TCP 연결을 수행한다. 이때, 로컬 프록시 모듈(120)은 서버(300)와의 TCP 연결에 대한 트래픽정보를 보안 게이트웨이(200)로 포워딩할 수 있다.

[0044] 그 후, 로컬 프록시 모듈(120)은 로컬 리다이렉션 모듈(110)에 의해 리다이렉트 TCP 연결이 발생하면, getpeername() 소켓 API를 이용하여 TCP 연결의 클라이언트인 애플리케이션 IP주소 및 포트정보를 로컬 리다이렉션 모듈(110)의 리다이렉션정보로부터 조회한다. 또한, 로컬 프록시 모듈(120)은 로컬 리다이렉션 모듈(110)이 저장하고 있는 리다이렉션정보로부터 연결하고자 하는 서버 IP 주소 및 포트정보를 조회하여 해당 서버(300)에 TCP 연결을 수행한다.

[0045] 그 후, 로컬 프록시 모듈(120)은 애플리케이션 또는 서버(300)로부터 전송된 트래픽을 수신한다. 이때, 로컬 프록시 모듈(120)은 애플리케이션으로부터 SSL ClientHello 메시지를 수신한 경우에는 SSL 트래픽을 위한 연결로 판단하고, 서버(300) 측 SSL 핸드쉐이크와 클라이언트측 SSL 핸드쉐이크를 수행한다.

[0046] SSL 핸드쉐이크 수행 후에, 로컬 프록시 모듈(120)은 SSL 트래픽에 대한 인터셉션 동작을 수행한다. 즉, 로컬 프록시 모듈(120)은 애플리케이션 또는 서버(300)가 전송한 암호화 SSL 트래픽을 수신하고 이를 복호화한다. 로컬 프록시 모듈(120)은 복호화된 복호화 SSL 트래픽을 보안 게이트웨이(200)로 포워딩한다. 그 후, 로컬 프록시 모듈(120)은 복호화 SSL 트래픽을 재암호화하고, 재암호화 SSL 트래픽을 서버(300)로 전송한다.

[0047] 한편, 로컬 프록시 모듈(120)은 애플리케이션으로부터 제공된 트래픽이 SSL 트래픽이 아닌 경우에(즉, Non-SSL 트래픽), 제공된 Non-SSL 트래픽을 그대로 보안 게이트웨이(200)로 포워딩하고, 아울러 서버(300)로 전송한다.

[0048] 이때, 로컬 프록시 모듈(120)은 Non-SSL 트래픽 또는 복호화 SSL 트래픽의 페이로드 데이터에 대해서 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 보안 게이트웨이(200)로 아웃오브패스(Out-Of-Path) 방식으로 포워딩할 수 있다. 예를 들어, 로컬 프록시 모듈(120)은 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 서버(300)에 대한 TCP 연결시 TCP 3-핸드쉐이크 패킷(SYN, SYN-ACK, ACK)을 생성하고, Non-SSL 트래픽 및 복호화 SSL 트래픽의 페이로드 데이터에 대해서 TCP 패킷을 생성하고, TCP 연결종료시 TCP 연결종료(FIN 또는 RST) 패킷을 생성하여 보안 게이트웨이(200)로 포워딩한다. 이더넷 헤더의 출발지 및 목적지 MAC 주소는 특정값을 지정할 수 있으며, IP 헤더의 출발지 및 목적지 IP 주소는 애플리케이션 및 서버의 IP주소를 지정하며, TCP 헤더의 출발지 및 목적지 포트정보는 애플리케이션 및 서버의 포트정보를 지정하며, TCP 헤더의 Seq/Ack정보를 페이로드 데이터의 송수신에 따라 증가시킨다.

[0049] 로컬 프록시 모듈(120)은 보안 게이트웨이(200)로 포워딩하는 대상으로 트래픽포워딩 정책에 따라 특정 서버의 IP주소 또는 특정 애플리케이션의 프로세스인 트래픽을 포함하거나 제외할 수 있으며, 트래픽 아웃바운드 트래픽 또는 인바운드 트래픽을 포함하거나 제외할 수 있다.

[0050] 보안 게이트웨이(200)는 엔드포인트(100)의 로컬 프록시 모듈(120)에서 포워딩한 TCP 패킷 형태의 트래픽을 수신하여, 콜백 함수 또는 콜백 데이터로 전달하거나, PCAP(PacketCapture) 포맷의 파일로 저장한다. 또한, 보안 게이트웨이(200)는 수신된 트래픽에 대하여 프로토콜 분석 및 메일, 메시지, 파일 등 포워딩된 트래픽에 대한 개인정보 및 기밀정보를 검사한다. 보안 게이트웨이(200)는 포워딩된 트래픽에 대한 검사결과로 해당 트래픽의 차단이 필요할 경우 애플리케이션 및 서버(300)의 IP주소 및 포트정보로 구성된 차단할 주소연결정보를 포함하는 검사결과정보를 로컬 프록시 모듈(120)로 전송한다.

[0051] 이에 따라, 엔드포인트(100)의 로컬 프록시 모듈(120)은 보안 게이트웨이(200)의 검사결과정보로부터 차단 대상이 되는 애플리케이션 및 서버(300)의 IP주소 및 포트정보를 확인하고, 해당 애플리케이션 연결과 서버(300)와의 연결을 종료한다.

[0053] 도 3은 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩을 설명하기 위한 각 구성요소들의 동작 수행 참조도이다.

[0054] 먼저, 엔드포인트(100)에 구비된 애플리케이션이 서버(300)로 전송하기 위한 트래픽을 생성하여 로컬 리다이렉션 모듈(110)로 TCP 연결을 요청하면, 로컬 리다이렉션 모듈(110)은 서버(300)와의 연결을 위한 서버연결정보를 포함하는 리다이렉션정보를 저장하며, 트래픽을 로컬 프록시 모듈(120)로 전달을 위한 리다이렉션 동작을 수행한다.

[0055] 그 후, 로컬 프록시 모듈(120)은 리다이렉션정보를 조회하여 서버 연결정보에 대응하는 서버(300)와 TCP 연결을 수행하며, 이때, 서버(300)에 대한 TCP 연결에 대한 트래픽 정보를 보안 게이트웨이(200)로 포워딩할 수 있다. 로컬 프록시 모듈(120)은 애플리케이션 및 서버(300)와 각각 SSL 핸드쉐이크를 수행한 후에, 애플리케이션으로부터 암호화 SSL 트래픽을 수신한다. 그 후, 로컬 프록시 모듈(120)은 수신된 암호화 SSL 트래픽을 복호화하여, 복호화 SSL 트래픽을 보안 게이트웨이(200)로 포워딩하며, 아울러, 복호화 SSL 트래픽을 재암호화하여, 서버(300)로 전송한다.

[0056] 그 후, 보안 게이트웨이(200)는 암호화 SSL 트래픽을 로컬 프록시 모듈(120)로 포워딩할 수 있으며, 이에 따라, 로컬 프록시 모듈(120)은 보안 게이트웨이(200)로부터 수신된 암호화 SSL 트래픽을 복호화 한 후에, 이를 재암호화하여 애플리케이션으로 전달할 수 있다.

[0057] 또한, 보안 게이트웨이(200)는 로컬 프록시 모듈(120)로부터 포워딩된 복호화 SSL 트래픽 또는 Non-SSL 트래픽

에 대한 검사결과정보를 로컬 프록시 모듈(120)로 전송할 수 있다. 이에 따라, 로컬 프록시 모듈(120)은 검사결과정보에 따라 해당 애플리케이션 연결과 서버(300)와의 연결을 종료시킨 후에, TCP 연결 종료에 대한 트래픽 정보를 보안 게이트웨이(200)로 포워딩한다.

[0059] 도 4는 본 발명에 따른 엔드포인트의 트래픽에 대한 포워딩 방법을 설명하기 위한 일 실시예의 흐름도이다.

[0060] 엔드포인트를 구성하는 로컬 리다이렉션 모듈은 애플리케이션에서 생성되는 트래픽을 서버로 전송하기 위한 서버연결정보를 포함하는 리다이렉션정보를 저장한다(200 단계). 로컬 리다이렉션 모듈은 서버에 대한 서버 IP 주소정보 및 포트정보와 애플리케이션에 대한 애플리케이션 IP 주소정보 및 포트정보를 리다이렉션정보로서 저장한다.

[0061] 200 단계 후에, 로컬 리다이렉션 모듈은 트래픽의 서버로의 전송과 관련한 리다이렉션을 수행한다(202 단계). 로컬 리다이렉션 모듈은 네트워크 커널기반의 연결 리다이렉션 방식 또는 애플리케이션 소켓연결 API 후킹방식 중 적어도 어느 하나의 방식을 이용하여, 상기 트래픽에 대한 리다이렉션을 수행한다. 로컬 리다이렉션 모듈은 서버와의 API 연결을 위한 서버연결정보 즉, 서버 IP 주소정보 및 포트정보를 로컬 프록시 모듈에서 서비스하는 루프백 IP 주소정보 및 포트정보로 변경하여 트래픽에 대한 리다이렉션을 수행한다.

[0062] 202 단계 후에, 로컬 프록시 모듈은 로컬 리다이렉션 모듈의 리다이렉션에 의해 로컬 리다이렉션 모듈과 연결되며, 트래픽의 서버로의 전송을 위해 로컬 리다이렉션 모듈에 저장된 리다이렉션정보를 조회한다(204 단계).

[0063] 204 단계 후에, 로컬 프록시 모듈은 리다이렉션정보의 조회에 따라 추출된 서버 IP 주소정보 및 포트정보를 이용하여 서버와의 TCP 연결을 수행한다(206 단계). 그 후, 로컬 프록시 모듈은 애플리케이션 또는 서버로부터 전송된 트래픽을 수신한다.

[0064] 206 단계 후에, 로컬 프록시 모듈은 수신된 트래픽이 SSL 트래픽인가를 판단한다(208 단계). 로컬 프록시 모듈은 애플리케이션으로부터 SSL ClientHello 메시지를 수신한 경우에는 SSL 트래픽으로 판단한다.

[0065] 208 단계 후에, 로컬 프록시 모듈은 로컬 리다이렉션 모듈의 리다이렉션에 따라, 전달받은 트래픽 중 SSL 트래픽에 대한 데이터 복호화를 수행한다(210 단계). SSL 트래픽을 위한 연결로 판단되면, 로컬 프록시 모듈은 서버측 SSL 핸드쉐이크와 클라이언트측 SSL 핸드쉐이크를 수행한다. SSL 핸드쉐이크 수행 후에, 로컬 프록시 모듈은 SSL 트래픽에 대한 인터셉션 동작을 수행한다. 즉, 로컬 프록시 모듈은 애플리케이션 또는 서버가 전송한 암호화 SSL 트래픽을 수신하고 이를 복호화한다.

[0066] 210 단계 후에, 로컬 프록시 모듈은 복호화 SSL 트래픽을 보안 게이트웨이로 포워딩한다(212 단계).

[0067] 212 단계 후에, 로컬 프록시 모듈은 복호화 SSL 트래픽을 재암호화하고, 재암호화 SSL 트래픽을 서버로 전송한다(214 단계).

[0068] 214 단계 후에, 보안 게이트웨이는, 로컬 프록시 모듈로부터 포워딩된 트래픽에 대한 개인정보 및 기밀정보와 관련한 데이터 검증절차를 수행하고, 데이터 검증절차에 따른 검사결과정보를 로컬 프록시 모듈로 전송한다(216 단계).

[0069] 216 단계 후에, 엔드포인트의 로컬 프록시 모듈은 보안 게이트웨이의 검사결과정보로부터 차단 대상이 되는 애플리케이션 및 서버의 IP주소 및 포트정보를 확인하고, 해당 애플리케이션 연결과 서버와의 연결을 종료한다(218 단계).

[0070] 한편, 208 단계에서, 애플리케이션으로부터 수신된 트래픽이 SSL 트래픽이 아니라고 판단되면, 로컬 프록시 모듈은, SSL 트래픽이 아닌 Non-SSL 트래픽에 대해 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 보안 게이트웨이로 포워딩한다(220 단계). 이때, 로컬 프록시 모듈은 복호화 SSL 트래픽의 페이로드 데이터에 대해서도 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 보안 게이트웨이로 포워딩할 수 있다.

[0071] 220 단계 후에, 로컬 프록시 모듈은 Non-SSL 트래픽에 대해 이더넷 헤더, IP 헤더, TCP 헤더를 추가하여 서버로 전송한다(222 단계).

[0073] 본 발명은 소프트웨어적인 프로그램으로 구현하여 컴퓨터로 읽을 수 있는 소정 기록매체에 기록해 둠으로써 다양한 재생장치에 적용할 수 있다. 다양한 재생장치는 PC, 노트북, 휴대용 단말 등일 수 있다. 예컨대, 기록매체는 각 재생장치의 내장형으로 하드디스크, 플래시 메모리, RAM, ROM 등이거나, 외장형으로 CD-R, CD-RW와 같은 광디스크, 콤팩트 플래시 카드, 스마트 미디어, 메모리 스틱, 멀티미디어 카드일 수 있다.

[0074] 이상과 같이 본 발명의 실시예를 설명하였으나, 본 발명의 명세서에 개시된 실시예들은 본 발명을 한정하는 것이 아니다. 본 발명의 범위는 아래의 특허청구범위에 의해 해석되어야 하며, 그와 균등한 범위 내에 있는 모든 기술도 본 발명의 범위에 포함되는 것으로 해석해야 할 것이다.

부호의 설명

[0075] 100: 엔드포인트

110: 로컬 리다이렉션 모듈

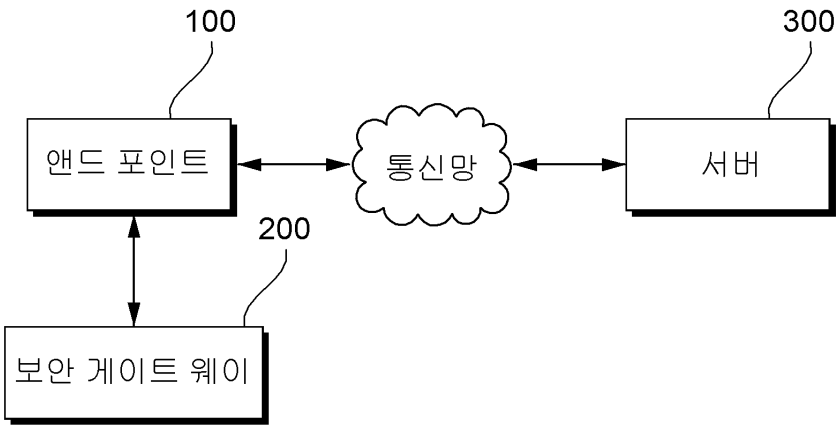
120: 로컬 프록시 모듈

200: 보안 게이트웨이

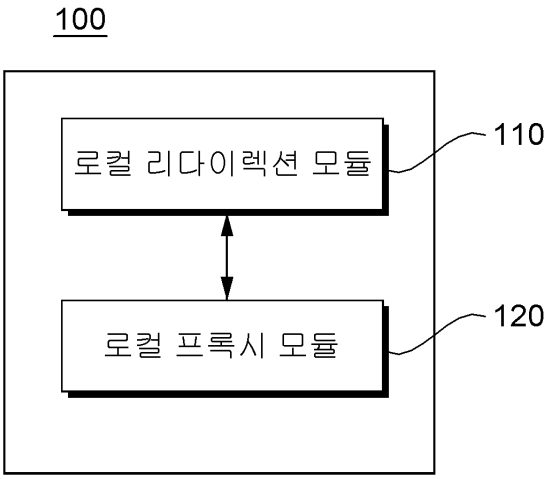
300: 서버

도면

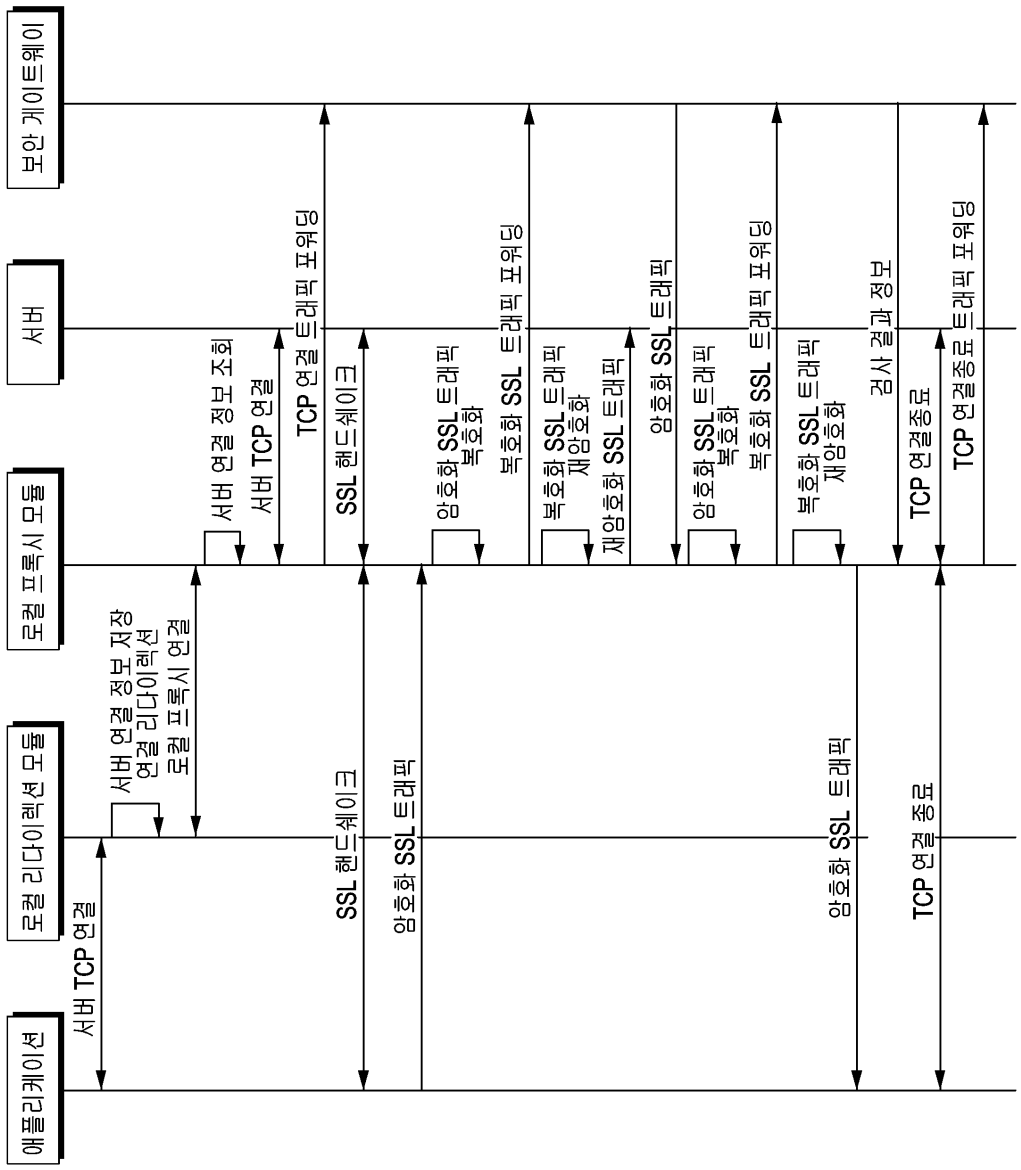
도면1



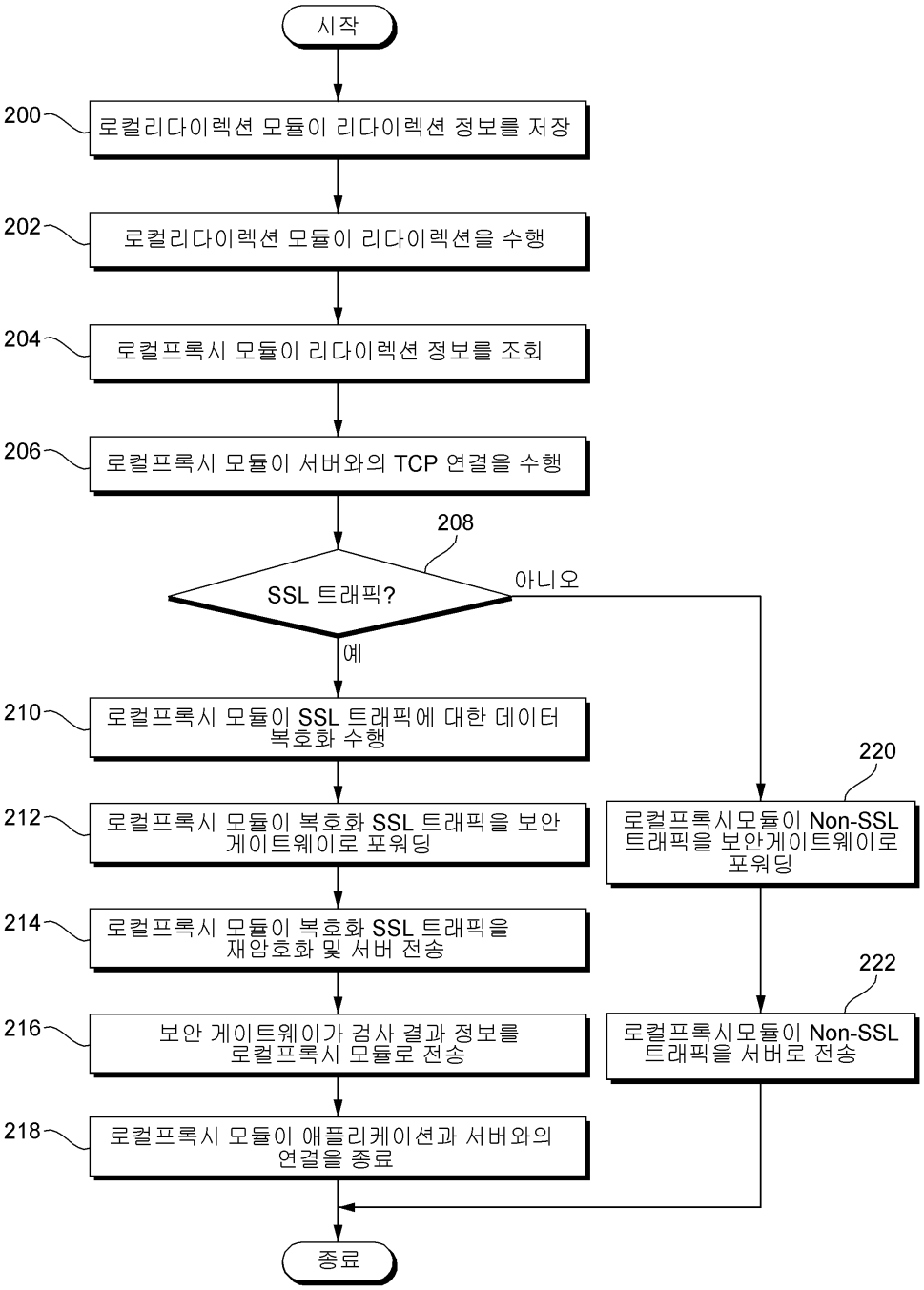
도면2



도면3


애플리케이션
로컬 리다이렉션 모듈
로컬 프록시 모듈
서버
보안 게이트웨이
서버 TCP 연결
서버 연결 정보 저장
연결 리다이렉션
로컬 프록시 연결
서버 연결 정보 조회
서버 TCP 연결
TCP 연결 트래픽 포워딩
SSL 핸드쉐이크
암호화 SSL 트래픽
암호화 SSL 트래픽
복호화
복호화 SSL 트래픽 포워딩
복호화 SSL 트래픽
재암호화
재암호화 SSL 트래픽
암호화 SSL 트래픽
암호화 SSL 트래픽
복호화
복호화 SSL 트래픽 포워딩
복호화 SSL 트래픽
재암호화
검사 결과 정보
TCP 연결종료
TCP 연결종료
TCP 연결종료 트래픽 포워딩
SSL 핸드쉐이크
암호화 SSL 트래픽
암호화 SSL 트래픽
TCP 연결 종료

도면4


시작
200
로컬리다이렉션 모듈이 리다이렉션 정보를 저장
202
로컬리다이렉션 모듈이 리다이렉션을 수행
204
로컬프록시 모듈이 리다이렉션 정보를 조회
206
로컬프록시 모듈이 서버와의 TCP 연결을 수행
208
SSL 트래픽?
아니오
예
210
로컬프록시 모듈이 SSL 트래픽에 대한 데이터 복호화 수행
212
로컬프록시 모듈이 복호화 SSL 트래픽을 보안 게이트웨이로 포워딩
214
로컬프록시 모듈이 복호화 SSL 트래픽을 재암호화 및 서버 전송
216
보안 게이트웨이가 검사 결과 정보를 로컬프록시 모듈로 전송
218
로컬프록시 모듈이 애플리케이션과 서버와의 연결을 종료
220
로컬프록시모듈이 Non-SSL 트래픽을 보안게이트웨이로 포워딩
222
로컬프록시모듈이 Non-SSL 트래픽을 서버로 전송
종료