(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년04월26일
(11) 등록번호 10-2390765
(24) 등록일자 2022년04월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 16/00* (2019.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 63/20 (2013.01)
G06F 16/22 (2019.01)
(21) 출원번호 10-2017-7010910
(22) 출원일자(국제) 2015년09월23일
심사청구일자 2020년09월15일
(85) 번역문제출일자 2017년04월21일
(65) 공개번호 10-2017-0060092
(43) 공개일자 2017년05월31일
(86) 국제출원번호 PCT/US2015/051783
(87) 국제공개번호 WO 2016/049228
국제공개일자 2016년03월31일
(30) 우선권주장
14/495,631 2014년09월24일 미국(US)
(56) 선행기술조사문헌
US7152240 B1
(뒷면에 계속)
전체 청구항 수 : 총 19 항

(73) 특허권자
넷플릭스, 인크.
미국 캘리포니아 로스 가토스 윈체스터 써클 100 (우:95032-7606)
(72) 발명자
찬, 제이슨
미국 95032 캘리포니아주 로스 가토스 윈체스터 서클 100
우두피, 푸나프라즈나
미국 95032 캘리포니아주 로스 가토스 윈체스터 서클 100
마다파, 샤시
미국 95032 캘리포니아주 로스 가토스 윈체스터 서클 100
(74) 대리인
양영준, 김연송, 백만기

심사관 : 홍기완

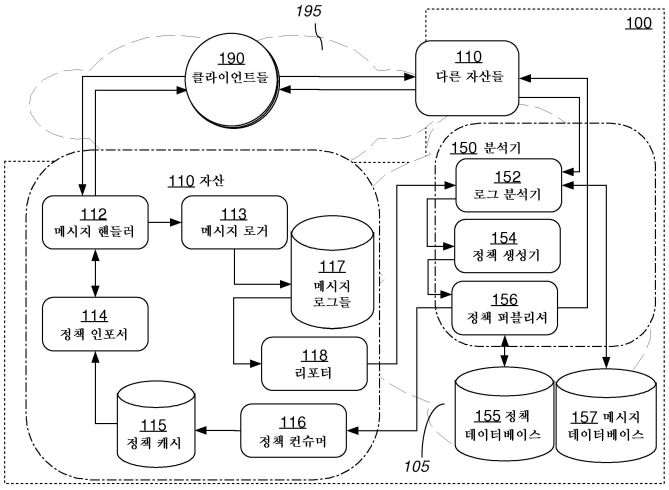
(54) 발명의 명칭 **분산형 트래픽 관리 시스템 및 기법들**

(57) 요 약

분산형 방화벽을 구현하기 위한 접근 방식들, 기법들 및 메커니즘들이 개시된다. 일 실시예에서, 많은 상이한 컴퓨터 자산들이 로컬 정책 데이터에 기초하여 들어오는 메시지들을 감시한다. 이 로컬 정책 데이터는 글로벌 정책 데이터와 동기화된다. 글로벌 정책 데이터는 하나 이상의 별개의 분석기들에 의해 생성된다. 각각의 분석

(뒷면에 계속)

대 표 도



기는 컴퓨터 자산들의 그룹들에 대하여 메시지 로그들 또는 그로부터 도출되는 정보에 대한 액세스를 가지며, 따라서 분리된 자산과는 대조적으로 전체적인 그룹으로부터의 인텔리전스에 기초하여 정책들을 생성할 수 있다. 다른 효과들 중에서, 접근 방식들, 기법들 및 메커니즘들 중 일부는 공격면 전반에 걸쳐 제한된 감독 기능을 갖는 컴퓨팅 환경들, 및/또는 다른 시스템 컴포넌트들에 대한 접속들에서의 레이턴시 및/또는 비신뢰성으로 인해 들어오는 메시지들이 어떻게 핸들링되어야 하는지에 대해 자산들이 독립적인 결정들을 내릴 필요가 있을 수 있는 컴퓨팅 환경들에서도 효과적일 수 있다.

(52) CPC특허분류
H04L 63/0227 (2013.01)
H04L 63/1408 (2013.01)
H04L 67/10 (2013.01)

(56) 선행기술조사문헌
US20040015719 A1
JP2003229913 A
JP2003273936 A
JP2004362581 A

명 세 서

청구범위

청구항 1

컴퓨터 시스템으로서,

정책들(policies)을 기술하는 글로벌 정책 데이터(global policy data)를 저장하는 데이터 리포지토리(data repository);

제1 컴퓨터 하드웨어에 의해 적어도 부분적으로 구현되는 복수의 컴퓨터 자산들(assets) - 상기 복수의 컴퓨터 자산들의 각각의 자산은, 클라이언트 디바이스들로부터 메시지들을 수신하고, 상기 자산을 구현하는 컴퓨팅 디바이스에서 상기 정책들을 기술하는 로컬 정책 데이터(local policy data)를 저장하고, 상기 정책들 중 어느 정책이 상기 메시지들 중 어느 메시지에 적용되는지를 결정하고, 상기 정책들 중 어느 정책이 상기 메시지들 중 어느 메시지에 적용되는지에 기초하여, 상기 메시지들에 대해 수행할 정책-기반 액션들을 식별하고, 상기 메시지들로부터 로그된 메시지 정보를 분석기 컴포넌트에 전송하고, 상기 글로벌 정책 데이터에 업데이트들을 반영하도록 상기 로컬 정책 데이터를 업데이트하도록 구성됨 -; 및

제2 컴퓨터 하드웨어에 의해 적어도 부분적으로 구현되는 분석기 컴포넌트 - 상기 분석기 컴포넌트는 상기 복수의 컴퓨터 자산들 각각으로부터 상기 메시지 정보를 수신하고, 상기 복수의 컴퓨터 자산들 각각으로부터의 상기 메시지 정보를 총괄적으로(collectively) 분석하고, 상기 메시지 정보를 총괄적으로 분석하는 것에 기초하여, 새로운 정책들을 생성하고, 상기 새로운 정책들을 기술하도록 상기 글로벌 정책 데이터를 업데이트하도록 구성됨 -

를 포함하고,

상기 복수의 컴퓨터 자산들의 각각의 자산은 제1 네트워크의 에지에 배치되고,

상기 클라이언트 디바이스들은 제2 네트워크 내에 배치되는 컴퓨터 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 복수의 컴퓨터 자산들 및 상기 분석기는 상기 컴퓨터 시스템의 제1 영역에 배치되고, 상기 컴퓨터 시스템은 하나 이상의 추가적인 영역들을 추가로 포함하고, 각각의 영역은 별개의 복수의 컴퓨터 자산들 및 별개의 분석기를 포함하고, 상기 데이터 리포지토리는 상기 제1 영역과 상기 하나 이상의 추가적인 영역들 사이에서 공유되는 컴퓨터 시스템.

청구항 4

제1항에 있어서, 상기 정책들의 각각의 정책은 상기 정책이 주어진 메시지에 적용되는지를 결정하기 위한 로직을 지시하는 데이터 구조일 뿐만 아니라, 상기 정책이 상기 주어진 메시지에 적용되는 경우 상기 주어진 메시지에 대해 수행할 하나 이상의 특정 정책-기반 액션들을 지시하는 하나 이상의 명령어들인 컴퓨터 시스템.

청구항 5

제1항에 있어서, 상기 분석기는 총괄적으로 분석된 메시지 정보로부터 시스템-레벨 정책에 의해 기술된 조건이 존재한다고 결정하는 것에 기초하여, 상기 새로운 정책들 중 하나 이상의 새로운 정책을 식별하고, 상기 기술된 조건을 고려하여 차단 또는 리다이렉트(redirect)할 메시지들을 식별하기 위한 로직을 포함하는 하나 이상의 자산-레벨 정책들을 생성하고, 상기 생성된 하나 이상의 자산-레벨 정책들을 포함하도록 상기 글로벌 정책 데이터를 업데이트하도록 추가로 구성되는 컴퓨터 시스템.

청구항 6

제1항에 있어서, 상기 분석기는 상기 총괄적으로 분석된 메시지 정보에 기초하여 상기 컴퓨터 시스템 상의 분산형 공격을 식별하고, 상기 분산형 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하고, 상기 제1 정책을 기술하도록 상기 글로벌 정책 데이터를 업데이트하도록 추가로 구성되는 컴퓨터 시스템.

청구항 7

제1항에 있어서,

상기 분석기는 상기 총괄적으로 분석된 메시지 정보에 기초하여: 상기 복수의 컴퓨터 자산들 중 제1 자산에서 발생하고 있는 공격을 식별하고, 상기 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하고, 상기 제1 정책을 기술하도록 상기 글로벌 정책 데이터를 업데이트하도록 추가로 구성되고,

상기 복수의 컴퓨터 자산들 중 제2 자산은 상기 업데이트된 글로벌 정책 데이터에 기초하여, 상기 제1 정책을 기술하도록 상기 제2 자산의 로컬 정책 데이터를 업데이트하고 - 상기 제2 자산은 상기 제2 자산의 상기 로컬 정책 데이터가 업데이트되는 시점에서는 상기 공격에 수반된 메시지들을 아직 수신하지 않음 -, 상기 제1 정책에 기초하여 상기 공격에 수반된 메시지를 차단 또는 리다이렉트하도록 구성되는 컴퓨터 시스템.

청구항 8

제1항에 있어서, 상기 메시지들은 수행할 상기 복수의 자산들에 대해 지정된 액션들을 지시하고, 각각의 자산은 상기 정책들이 적용되는 메시지들에 대해 상기 지시된 지정된 액션들 대신에 또는 이에 더하여 적용가능한 정책-기반 액션들을 수행하도록 구성되는 컴퓨터 시스템.

청구항 9

제1항에 있어서, 상기 정책들 중 주어진 정책에 의해 지시된 정책-기반 액션은 상기 주어진 정책이 적용되는 임의의 메시지를 차단하는 것, 상기 주어진 정책이 적용되는 임의의 메시지를 리다이렉트하는 것, 또는 상기 주어진 정책이 적용되는 임의의 메시지에 대해 자산이 정상적으로 응답하도록 허용하는 것 중 하나인 컴퓨터 시스템.

청구항 10

제1항에 있어서, 상기 복수의 컴퓨터 자산들의 자산은, 상기 분석기 컴포넌트 및 상기 데이터 리포지토리가 상기 자산에 액세스불가능할 때에도, 상기 자산의 상기 로컬 정책 데이터로부터 정책들을 메시지들에 적용하도록 구성되는 컴퓨터 시스템.

청구항 11

데이터 처리 방법으로서,

컴퓨터 자산에서, 정책들을 기술하는 로컬 정책 데이터를 저장하는 단계;

상기 컴퓨터 자산에서, 클라이언트 디바이스들로부터 메시지들을 수신하는 단계;

상기 컴퓨터 자산에서, 상기 정책들 중 어느 정책이 상기 메시지들 중 어느 메시지에 적용되는지를 결정하는 단계;

상기 컴퓨터 자산에서, 상기 정책들 중 어느 정책이 상기 메시지들 중 어느 메시지에 적용되는지에 기초하여, 상기 메시지들에 대해 수행할 정책-기반 액션들을 식별하는 단계;

상기 컴퓨터 자산으로부터, 상기 메시지들로부터 로그된 메시지 정보를 분석기 컴포넌트에 전송하는 단계; 및

상기 컴퓨터 자산에 의해, 상기 분석기 컴포넌트에 의해 생성된 글로벌 정책 데이터에 업데이트들을 반영하도록 상기 로컬 정책 데이터를 업데이트하는 단계

를 포함하고,

상기 컴퓨터 자산은 하나 이상의 컴퓨팅 디바이스들에 의해 구현되고,

상기 컴퓨터 자산은 제1 네트워크의 에지에 배치되고,

상기 클라이언트 디바이스들은 제2 네트워크 내에 배치되는 데이터 처리 방법.

청구항 12

제11항에 있어서, 상기 정책들의 각각의 정책은 상기 정책이 주어진 메시지에 적용되는지를 결정하기 위한 로직을 지시하는 데이터 구조일 뿐만 아니라, 상기 정책이 적용되는 경우 상기 주어진 메시지에 대해 수행할 하나 이상의 특정 정책-기반 액션들을 지시하는 하나 이상의 명령어들인 데이터 처리 방법.

청구항 13

제11항에 있어서, 상기 메시지들은 수행할 상기 컴퓨터 자산에 대해 지정된 액션들을 지시하고,

상기 방법은, 상기 정책들이 적용되는 메시지들에 대해 지시된 상기 지정된 액션들 대신에 또는 이에 더하여 적용가능한 정책-기반 액션들을 수행하는 단계를 추가로 포함하는 데이터 처리 방법.

청구항 14

제11항에 있어서, 상기 분석기 컴포넌트 및 상기 글로벌 정책 데이터가 상기 자산에 액세스불가능할 때에도, 상기 로컬 정책 데이터로부터 정책들을 메시지들에 적용하는 단계를 추가로 포함하는 데이터 처리 방법.

청구항 15

제11항에 있어서,

상기 분석기 컴포넌트에서, 상기 컴퓨터 자산을 포함하여 복수의 컴퓨터 자산들의 각각의 자산에서 로그된 메시지 정보를 수신하는 단계;

상기 분석기 컴포넌트에 의해, 상기 복수의 컴퓨터 자산들 각각에서 로그된 상기 메시지 정보를 총괄적으로 분석하는 단계;

상기 분석기 컴포넌트에 의해, 상기 메시지 정보를 총괄적으로 분석하는 것에 기초하여, 새로운 정책들을 생성하는 단계; 및

상기 분석기 컴포넌트에 의해, 상기 새로운 정책들을 기술하도록 상기 글로벌 정책 데이터를 업데이트하는 단계

를 추가로 포함하는 데이터 처리 방법.

청구항 16

데이터 처리 방법으로서,

복수의 컴퓨터 자산들의 각각의 자산으로부터 메시지 정보를 수신하는 단계 - 상기 메시지 정보는 상기 자산에 의해 수신된 메시지들을 기술함 -;

상기 복수의 컴퓨터 자산들 각각으로부터의 상기 메시지 정보를 총괄적으로 분석하는 단계;

상기 메시지 정보를 총괄적으로 분석하는 것에 기초하여 정책들을 생성하는 단계 - 상기 정책들은 상기 정책들이 적용되는 메시지들을 식별하기 위한 로직뿐만 아니라, 상기 정책들이 적용되는 메시지들에 대해 수행할 정책-기반 액션들을 기술함 -;

상기 정책들을 기술하도록 글로벌 정책 데이터 리포지토리를 업데이트하는 단계; 및

상기 복수의 컴퓨터 자산들에 정책 데이터를 전송하는 단계 - 상기 정책 데이터는 적어도 상기 글로벌 정책 데이터 리포지토리에 상기 정책들을 기술함 -;

를 포함하고,

상기 방법은 분석기 컴포넌트를 구현하는 하나 이상의 컴퓨터 디바이스들에 의해 수행되고,

상기 복수의 컴퓨터 자산들의 각각의 자산은 제1 네트워크의 에지에 배치되는 데이터 처리 방법.

청구항 17

제16항에 있어서,

상기 분석기 컴포넌트는 복수의 분석기들 중 하나의 분석기이고, 각각은 상이한 복수의 컴퓨터 자산들에 대해

제16항의 단계들을 수행하도록 구성되고,

상기 글로벌 정책 데이터 리포지토리는 적어도 상기 복수의 분석기들 사이에서 공유되는 데이터 처리 방법.

청구항 18

제16항에 있어서,

상기 메시지 정보로부터 시스템-레벨 정책에 의해 기술된 조건이 존재한다고 결정하는 것에 기초하여, 상기 정책들 중 하나 이상의 정책을 식별하는 단계;

상기 기술된 조건을 고려하여 차단 또는 리다이렉트할 메시지들을 식별하기 위한 로직을 포함하는 하나 이상의 자산-레벨 정책들을 생성하는 단계; 및

상기 생성된 하나 이상의 자산-레벨 정책들을 포함하도록 상기 글로벌 정책 데이터를 업데이트하는 단계

를 추가로 포함하는 데이터 처리 방법.

청구항 19

제16항에 있어서,

상기 메시지 정보를 총괄적으로 분석하는 것에 기초하여, 상기 복수의 컴퓨터 자산들을 포함하는 컴퓨터 시스템 상의 분산형 공격을 식별하는 단계;

상기 분산형 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하는 단계; 및

상기 제1 정책을 기술하도록 상기 글로벌 정책 데이터를 업데이트하는 단계

를 추가로 포함하는 데이터 처리 방법.

청구항 20

제16항에 있어서,

상기 메시지 정보에 기초하여, 상기 분석기 컴포넌트가 제1 컴퓨터 자산에서 발생되고 있는 공격을 식별하는 단계;

상기 복수의 컴퓨터 자산들 중 적어도 제2 자산에서 상기 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하는 단계 - 상기 분석기 컴포넌트는 상기 제2 자산이 상기 공격에 수반된 메시지들을 수신하였음을 지시하는 메시지 정보를 상기 제2 자산으로부터 아직 수신하지 않음 -; 및

상기 제1 정책을 기술하도록 상기 글로벌 정책 데이터를 업데이트하는 단계

를 추가로 포함하는 데이터 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 개시내용은 분산형 네트워크 자산들에서 네트워크 트래픽을 관리하는 것에 관한 것이다.

배 경 기 술

[0002] 본 부분에서 기술되는 접근 방식들은 수행될 수 있었던 접근 방식들이지만, 반드시 이전에 고안되었거나 수행되었던 접근 방식들일 필요는 없다. 따라서, 다르게 나타내지 않는 한, 본 부분에서 기술되는 접근 방식들 중 임의의 것이 단지 본 부분에 포함됨으로 인해 종래의 기술로서 한정되는 것으로 가정되지 않아야 한다.

[0003] 네트워크화된 컴퓨터 시스템의 공격면은 잠재적인 공격자에 의해 액세스되도록 노출되는, 해당 컴퓨터 시스템 내의 컴포넌트들로 이루어진다. 이러한 컴포넌트들은 예를 들어, 웹 서버에 의해 실행되는 애플리케이션들 및 다른 서버-기반형 애플리케이션들을 포함할 수 있다. 통상적으로, 사용자-동작형 클라이언트들은 하나 이상의 컴퓨터 네트워크들을 통해 이들 컴포넌트들과 상호작용하는 것이 바람직하다. 따라서, 컴포넌트들은 그 하나 이상의 네트워크들을 통해 클라이언트들과 상호작용하기 위한 다양한 인터페이스들을 특징짓는다. 예를 들어,

컴포넌트들은 사용자 입력 콘트롤들을 포함하는 웹-기반 그래픽 사용자 인터페이스("GUI")들, 하이퍼-텍스트 전송 프로토콜(Hyper-Text Transfer Protocol : "HTTP") 또는 단순 객체 접근 프로토콜(Simple Object Access Protocol : "SOAP")과 같은 미리 정의된 프로토콜들을 통해 사용자 입력을 수신하기 위한 인터페이스들, 커스터마이즈된 애플리케이션 프로그래밍 인터페이스("API")들, 및/또는 컴포넌트들이 사용자-동작형 클라이언트 디바이스들로부터 통신들을 수신하고 이에 반응하는 다른 서비스들을 노출할 수 있다.

[0004] 컴포넌트들에 대한 사용자 액세스는 통상적으로는 바람직하지만, 사용자 액세스가 때때로 컴포넌트들을 허가되지 않은 사용들에 취약한 상태로 둔다면, 허가되지 않은 사용자가 컴포넌트들로 하여금 컴퓨터 시스템의 소유자에 의해 의도되지 않거나 원치 않는 방식들로 실행되게 할 수 있다. "공격들"로도 알려진 허가되지 않은 사용들의 예들은 도청과 같은 수동적 공격들, 및 서비스 거부, 스크립트된 계정 생성, 서버 또는 계정 가로채기, 버퍼 오버플로우, 힙 오버플로우 및 포맷 스트링 공격들과 같은 적극적 공격들을 포함하지만, 이에 제한되지 않는다.

[0005] 본 명세서에서 기술되는 목적들을 위해, 공격은 반드시 의도적으로 악성일 필요는 없으며, 오히려 예를 들어, 사용자가 시스템 자원들을 의도치않게 과다 사용하는 것을 포함하는 임의의 바람직하지 않은 거동일 수 있다. 예를 들어, 컴퓨터 시스템은 매우 다양한 미디어 자원들에 대한 액세스를 제공할 수 있고, 사용자는 실행될 때 컴퓨팅 디바이스로 하여금 미디어 자원들에 대한 액세스를 반복적으로 그리고 체계적으로 요청하게 하여 미디어 자원들에 대한 정보의 라이브러리를 컴파일 및/또는 분석하게 하는 미디어 서버용 코드와 같은 소프트웨어 코드를 의도치않게 생성하거나 배치할 수 있다. 그러나, 이러한 거동은 컴퓨터 시스템에 바람직하지 않을 수 있는데, 이는 미디어 아이템들에 대해 보다 많은 통상적인 애드 혹 요청들에 응답하도록 시스템의 능력에 부정적으로 영향을 미칠 수 있기 때문이다. 이러한 바람직하지 않은 거동 및 다른 바람직하지 않은 거동을 해결하기 위하여 다양한 트래픽 관리 구조들이 고안될 수 있다.

[0006] 방화벽은 네트워크화된 컴퓨터 시스템의 예시적인 트래픽 관리 컴포넌트이다. 방화벽 컴포넌트들의 예들로는 전용 어플라이언스들, 시스템 내의 컴퓨터 디바이스들 상에서 실행되는 소프트웨어-기반 애플리케이션들, 또는 네트워크 트래픽에 대한 게이트웨이들로서 동작하는 임의의 다른 시스템 컴포넌트들이 포함된다. 많은 통상적인 네트워크화된 컴퓨터 시스템들은 컴퓨터 시스템 외부의 잠재적으로 신뢰되지 않은 클라이언트 디바이스들과 컴퓨터 시스템 내부의 신뢰된 컴포넌트들 사이에서 전송되는 메시지들의 전부 또는 적어도 대다수를 방화벽이 인터셉트하도록 구성된다. 메시지들은 하나의 레벨 또는 복수의 레벨들에서 인터셉트될 수 있다. 예를 들어, 일부 방화벽들은 메시지들을 TCP 또는 UDP 패킷들의 형태의 메시지들과 같이 네트워크 계층 또는 전송 계층에서, 및/또는 FTP, DNS 또는 HTTP 요청들의 형태의 메시지들과 같이 애플리케이션 계층에서 인터셉트한다. 다른 방화벽들은 매우 다양한 메시지 타입들 중 임의의 메시지 타입을 매우 다양한 계층들 중 임의의 계층에서 인터셉트한다.

[0007] 통상적으로, 방화벽은 하나 이상의 정책들과 인터셉트된 메시지들을 비교하여 인터셉트된 메시지들에 대해 취해질 하나 이상의 액션들을 결정하도록 구성된다. 메시지가 그 어드레스된 목적지에 도달할 수 있게 허용하는 것, 메시지를 리다이렉트하는 것, 메시지를 차단하는 것, 메시지를 조작하는 것, 메시지에 대한 특정 상세들에 로그하는 것 등과 같은 다양한 상이한 액션들이 취해질 수 있다. 정책들은 종종 원치 않는 메시지들을 전체적으로 차단함으로써 이 원치 않는 메시지들을 "필터링(filter out)"한다는 점에서 때때로 필터들로서 참조된다. 정책의 간단한 예로는 특정된 소스 어드레스 또는 목적지 포트와 같이 규칙에 의해 특정된 특정 기준과 매치하는 특징들을 갖는 메시지가 차단되어야 하는 규칙이 있다. 방화벽은 시스템 자산들 상의 공격들을 차단하거나 최소화하도록 의도되는 다양한 정책들을 적용하도록 구성될 수 있다. 일부 시스템들에서, 방화벽은 미리 수신된 트래픽으로부터 학습하고 그 정책들을 조정하여 미래의 공격들에 양호하게 반응하도록 구성된다는 점에서 좀 더 적응적일 수 있다.

[0008] 공격면이 매우 분산되는 네트워크화된 컴퓨터 시스템들에서는, 적응식 방화벽을 효과적으로 배치하는 것이 종종 어렵다. 단일의 공격이 매우 다양한 소스들로부터 거의 동시에 발생할 수 있고, 공격면 상의 많은 상이한 자산들에 영향을 미칠 수 있다. 따라서, 네트워크화된 컴퓨터 시스템을 통과하는 트래픽을 중점적으로 분석하여 특정 공격들을 인식하고 그 범위를 이해하는 것이 유용하다. 그러나, 각각의 메시지를 인터셉트하고 분석하기 위하여 단일의 중앙화된 방화벽 컴포넌트에 의존하는 것은 때때로 바람직하지 않거나 실행 불가능한 일이다.

발명의 내용

[0009] 첨부되는 청구항들은 본 발명을 요약하기 위하여 제공될 수 있다.

도면의 간단한 설명

[0010] 도 1은 기술되는 기법들이 실행될 수 있는 예시적인 네트워크화된 컴퓨터 시스템을 도시한다.

도 2는 상이한 자산들의 그룹들을 담당하는 복수의 분석기(analyzer)들을 포함하는 예시적인 네트워크화된 컴퓨터 시스템을 도시한다.

도 3은 분산형 트래픽 관리 시스템에서 로컬 정책들을 적용하기 위한 예시적인 흐름을 도시한다.

도 4는 분산형 트래픽 관리 시스템에서 정책들을 생성하고 발행하기 위한 예시적인 흐름을 도시한다.

도 5는 본 발명의 실시예가 구현될 수 있는 컴퓨터 시스템을 도시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하의 내용에서는, 설명의 목적을 위해, 많은 구체적인 상세들이 본 발명의 완전한 이해를 제공하기 위해 제시된다. 그러나, 본 발명이 이들 구체적인 상세들이 없어도 실시될 수 있음은 명백할 것이다. 다른 예들에서는, 본 발명을 불필요하게 모호하게 하는 것을 피하기 위하여 잘 알려진 구조들 및 디바이스들이 블록도 형태로 도시된다.

[0012] 실시예들은 이하의 개요에 따라 본 명세서에서 기술된다.

[0013] 1.0. 일반적 개관

[0014] 2.0. 구조적 개관

[0015] 2.1. 자산들

[0016] 2.2. 클라이언트들

[0017] 2.3. 메시지 핸들링

[0018] 2.4. 정책 시행(Policy Enforcement)

[0019] 2.5. 로그 보고 및 분석

[0020] 2.6. 정책 생성 및 발행

[0021] 2.7. 분산형 분석기들

[0022] 2.8. 중간-계층(Mid-Tier) 컴포넌트들

[0023] 2.9. 기타

[0024] 3.0. 기능적 개관

[0025] 3.1. 로컬 정책들 적용

[0026] 3.2. 정책 생성 및 발행

[0027] 4.0. 예시적인 구현 상세들

[0028] 4.1. 예시적인 정책 구조들

[0029] 4.2. 예시적인 정책 캐시들

[0030] 4.3. 예시적인 구성 옵션들

[0031] 4.4. 예시적인 메시지 로그들

[0032] 4.5. 예시적인 쿼리들

[0033] 5.0. 하드웨어 개관

[0034] 1.0. 일반적 개관

[0035] 네트워크화된 컴퓨터 시스템에서의 분산형 트래픽 관리를 위한 접근 방식들, 기법들 및 메커니즘들이 개시된다. 일 실시예에서, 많은 상이한 컴퓨터 자산들이 로컬 정책 데이터에 기초하여 들어오는 메시지들을 감시한다. 이

로컬 정책 데이터는 글로벌 정책 데이터와 동기화된다. 글로벌 정책 데이터는 하나 이상의 별개의 분석기들에 의해 생성된다. 각각의 분석기는 컴퓨터 자산들의 그룹들에 대하여 메시지 로그들 또는 그로부터 도출되는 정보에 대한 액세스를 가지며, 따라서 분리된 자산과는 대조적으로 전체적인 그룹으로부터의 인텔리전스에 기초하여 정책들을 생성할 수 있다. 다른 효과들 중에서, 접근 방식들, 기법들 및 메커니즘들 중 일부는 공격면 전반에 걸쳐 제한된 감독 기능을 갖는 컴퓨팅 환경들, 및/또는 다른 시스템 컴포넌트들에 대한 접속들에서의 레이턴시 및/또는 비신뢰성으로 인해 들어오는 메시지들이 어떻게 핸들링되어야 하는지에 대해 자산들이 독립적인 결정들을 내릴 필요가 있을 수 있는 컴퓨팅 환경들에서도 효과적일 수 있다.

[0036] 일 실시예에 따르면, 분산형 트래픽 관리를 구현하는 컴퓨터 시스템은 정책들을 기술하는 글로벌 정책 데이터를 저장하는 데이터 리포지토리(data repository)를 포함한다. 시스템은 제1 컴퓨터 하드웨어에 의해 적어도 부분적으로 구현되는 복수의 컴퓨터 자산들을 추가로 포함한다. 복수의 컴퓨터 자산들 중 각각의 자산은 클라이언트 디바이스들로부터 메시지를 수신하고, 자산을 구현하는 컴퓨팅 디바이스에서 정책들을 기술하는 로컬 정책 데이터를 저장하고, 정책들 중 어느 정책이 메시지들 중 어느 메시지에 적용되는지를 결정하고, 정책들 중 어느 정책이 메시지들 중 어느 메시지에 적용되는지에 기초하여, 메시지들에 대해 수행할 정책-기반 액션들을 식별하고, 메시지들로부터 로그된 메시지 정보를 분석기 컴포넌트에 전송하고, 글로벌 정책 데이터에 업데이트들을 반영하도록 로컬 정책 데이터를 업데이트하도록 구성된다. 시스템은 제2 컴퓨터 하드웨어에 의해 적어도 부분적으로 구현되는 분석기 컴포넌트를 추가로 포함한다. 분석기 컴포넌트는 복수의 컴퓨터 자산들 각각으로부터 메시지 정보를 수신하고, 복수의 컴퓨터 자산들 각각으로부터의 메시지 정보를 총괄적으로 분석하고, 메시지 정보를 총괄적으로 분석하는 것에 기초하여, 새로운 정책들을 생성하고, 새로운 정책들을 기술하도록 글로벌 정책 데이터를 업데이트하도록 구성된다.

[0037] 일 실시예에서, 복수의 컴퓨터 자산들의 각각의 자산은 제1 네트워크의 에지에 배치되고, 클라이언트 디바이스들은 제2 네트워크 내에 배치된다. 일 실시예에서, 복수의 컴퓨터 자산들의 자산은, 복수의 컴퓨터 자산들 내에 있지 않고 자산에 의해 수신되는 메시지들이 지향되는 서버 애플리케이션의 전방에 배치된다. 일 실시예에서, 복수의 컴퓨터 자산들의 자산은 자산에 의해 수신되는 메시지들에 응답하도록 구성되는 웹 서버 애플리케이션을 실행하도록 추가로 구성된다. 일 실시예에서, 복수의 컴퓨터 자산들 및 분석기는 컴퓨터 시스템의 제1 영역에 배치되고, 컴퓨터 시스템은 하나 이상의 추가적인 영역들을 추가로 포함하고, 각각의 영역은 별개의 복수의 컴퓨터 자산들 및 별개의 분석기를 포함하고, 데이터 리포지토리는 제1 영역과 하나 이상의 추가적인 영역들 사이에서 공유된다. 일 실시예에서, 제1 컴퓨터 하드웨어는 제2 컴퓨팅 하드웨어에 포함되지 않은 하나 이상의 컴퓨팅 디바이스들을 포함한다.

[0038] 일 실시예에서, 분석기는 총괄적인 메시지 정보로부터 시스템-레벨 정책에 의해 기술된 조건이 존재한다고 결정하는 것에 기초하여 새로운 정책들 중 하나 이상의 새로운 정책을 식별하고, 기술된 조건을 고려하여 차단 또는 리다이렉트할 메시지들을 식별하기 위한 로직을 포함하는 하나 이상의 자산-레벨 정책들을 생성하고, 생성된 하나 이상의 자산-레벨 정책들을 포함하도록 글로벌 정책 데이터를 업데이트하도록 추가로 구성된다.

[0039] 일 실시예에서, 분석기는 총괄적인 메시지 정보에 기초하여 컴퓨터 시스템 상의 분산형 공격을 식별하고, 분산형 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하고, 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하도록 추가로 구성된다. 일 실시예에서, 분석기는 총괄적인 메시지 정보에 기초하여, 복수의 컴퓨터 자산들 중 제1 자산에서 발생되고 있는 공격을 식별하고, 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하고, 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하도록 추가로 구성된다. 복수의 컴퓨터 자산들 중 제2 자산은 업데이트된 글로벌 정책 데이터에 기초하여, 제1 정책을 기술하도록 제2 자산의 로컬 정책 데이터를 업데이트하고 - 제2 자산은 제2 자산의 로컬 정책 데이터가 업데이트되는 시점에서는 공격에 수반된 메시지들을 아직 수신하지 않음 -, 제1 정책에 기초하여 공격에 수반된 메시지를 차단 또는 리다이렉트하도록 구성된다.

[0040] 일 실시예에서, 정책들의 각각의 정책은 정책이 주어진 메시지에 적용되는지를 결정하기 위한 로직을 지시하는 데이터 구조일 뿐만 아니라, 정책이 주어진 메시지에 적용되는 경우, 주어진 메시지에 대해 수행할 하나 이상의 특정 정책-기반 액션들을 지시하는 하나 이상의 명령어들이다. 일 실시예에서, 메시지들은 수행할 복수의 자산들에 대해 지정된 액션들을 지시하고, 각각의 자산은 정책이 적용되는 메시지들에 대해 지시된 지정된 액션들 대신에 또는 이에 더하여 적용가능한 정책-기반 액션들을 수행하도록 구성된다. 일 실시예에서, 정책들 중 주어진 정책에 의해 지시된 정책-기반 액션은 주어진 정책이 적용되는 임의의 메시지를 차단하는 것, 주어진 정책이 적용되는 임의의 메시지를 리다이렉트하는 것, 또는 주어진 정책이 적용되는 임의의 메시지에 대해 자산이

정상적으로 응답하도록 허용하는 것 중 하나이다.

[0041] 일 실시예에서, 로컬 정책 데이터를 업데이트하는 것은 분석기 컴포넌트로부터 글로벌 정책 데이터를 기술하는 정책 데이터를 수신하는 것, 또는 글로벌 정책 데이터를 공유된 데이터 리포지토리로부터 리트리브하는 것 중 하나를 포함한다.

[0042] 일 실시예에 따르면, 데이터 처리 방법은 컴퓨터 자산에서, 정책들을 기술하는 로컬 정책 데이터를 저장하는 단계를 포함한다. 방법은 컴퓨터 자산에서 메시지들을 클라이언트 디바이스들로부터 수신하는 단계를 추가로 포함한다. 방법은 컴퓨터 자산에서, 정책들 중 어느 정책이 메시지들 중 어느 메시지에 적용되는지를 결정하는 단계를 추가로 포함한다. 방법은 컴퓨터 자산에서, 정책들 중 어느 정책이 메시지들 중 어느 메시지에 적용되는지에 기초하여 메시지들에 대해 수행할 정책-기반 액션들을 식별하는 단계를 추가로 포함한다. 방법은 컴퓨터 자산으로부터, 메시지들로부터 로그된 메시지 정보를 분석기 컴포넌트로 전송하는 단계를 추가로 포함한다. 메시지는 컴퓨터 자산에 의해, 분석기 컴포넌트에 의해 생성된 글로벌 정책 데이터에 업데이트들을 반영하도록 로컬 정책 데이터를 업데이트하는 단계를 추가로 포함한다. 컴퓨터 자산은 하나 이상의 컴퓨팅 디바이스들에 의해 구현된다.

[0043] 일 실시예에서, 방법은 분석기 컴포넌트 및 글로벌 정책 데이터가 자산에 액세스불가능할 때에도, 로컬 정책 데이터로부터 정책들을 메시지들에 적용하는 단계를 추가로 포함한다. 일 실시예에서, 컴퓨터 자산은 컴퓨터 자산에 의해 수신된 메시지들이 지향되는 서버 애플리케이션의 전방에 배치된다. 일 실시예에서, 방법은 컴퓨터 자산에서, 컴퓨터 자산에 의해 수신된 메시지들 중 적어도 일부의 메시지에 응답하는 웹 서버 애플리케이션을 실행하는 단계를 추가로 포함한다. 일 실시예에서, 로컬 정책 데이터를 업데이트하는 단계는 분석기 컴포넌트로부터 글로벌 정책 데이터를 기술하는 정책 데이터를 수신하는 단계 또는 글로벌 정책 데이터를 공유된 데이터 리포지토리로부터 리트리브하는 단계 중 하나의 단계를 포함한다.

[0044] 일 실시예에서, 정책들의 각각의 정책은 정책이 주어진 메시지에 적용되는지를 결정하기 위한 로직을 지시하는 데이터 구조일 뿐만 아니라, 정책이 적용되는 경우, 주어진 메시지에 대해 수행할 하나 이상의 특정 정책-기반 액션들을 지시하는 하나 이상의 명령어들이다. 일 실시예에서, 정책들 중 주어진 정책에 의해 지시된 정책-기반 액션은 주어진 정책이 적용되는 임의의 메시지를 차단하는 것, 주어진 정책이 적용되는 임의의 메시지를 리다이렉트하는 것, 또는 주어진 정책이 적용되는 임의의 메시지에 대해 자산이 정상적으로 응답하도록 허용하는 것 중 하나이다. 일 실시예에서, 메시지들은 수행할 복수의 자산들에 대해 지정된 액션들을 나타내고, 방법은 정책이 적용되는 메시지들에 대해 지시된 지정된 액션들 대신에 또는 이에 더하여 적용가능한 정책-기반 액션들을 수행하는 단계를 추가로 포함한다.

[0045] 일 실시예에서, 방법은 분석기 컴포넌트에서, 컴퓨터 자산을 포함하여 복수의 컴퓨터 자산들의 각각의 자산에서 로그된 메시지 정보를 수신하는 단계를 추가로 포함한다. 방법은 분석기 컴포넌트에 의해, 복수의 컴퓨터 자산들 각각에서 로그된 메시지 정보를 총괄적으로 분석하는 단계를 추가로 포함한다. 방법은 분석기 컴포넌트에 의해, 메시지 정보를 총괄적으로 분석하는 것에 기초하여, 새로운 정책들을 생성하는 단계를 추가로 포함한다. 방법은 분석기 컴포넌트에 의해, 새로운 정책들을 기술하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0046] 일 실시예에서, 방법은 상기 인용된 컴퓨터 자산의 단계들을 수행하는 복수의 세트들의 컴퓨터 자산들을 실행하는 단계를 추가로 포함한다. 복수의 세트들 중 주어진 세트 내의 자산들은 복수의 분석기들 중 주어진 세트에 할당되는 동일한 분석기 컴포넌트에 그들 각각의 메시지 정보를 전송한다. 방법은 적어도 복수의 분석기들 사이에 공유된 데이터 리포지토리에 글로벌 정책 데이터를 저장하는 단계를 추가로 포함한다. 복수의 분석기들 각각은 별개로 새로운 정책들을 생성하고, 각각 생성된 새로운 정책들을 기술하도록 동일한 글로벌 정책 데이터를 업데이트한다.

[0047] 일 실시예에서, 방법은 분석기 컴포넌트에서, 총괄적인 메시지 정보로부터 시스템-레벨 정책에 의해 기술된 조건이 존재한다고 결정하는 것에 기초하여 새로운 정책들 중 하나 이상의 새로운 정책을 식별하는 단계를 추가로 포함한다. 방법은 기술된 조건을 고려하여 차단 또는 리다이렉트할 메시지들을 식별하기 위한 로직을 포함하는 하나 이상의 자산-레벨 정책들을 생성하는 단계를 추가로 포함한다. 방법은 생성된 하나 이상의 자산-레벨 정책들을 포함하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0048] 일 실시예에서, 방법은 분석기 컴포넌트에 의해, 총괄적인 메시지 정보에 기초하여 복수의 컴퓨터 자산들 상의 분산형 공격을 식별하는 단계를 추가로 포함한다. 방법은 분산형 공격에 수반된 메시지들을 식별하기 위한 로

직을 포함하는 제1 정책을 생성하는 단계를 추가로 포함한다. 방법은 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0049] 일 실시예에서, 방법은 총괄적인 메시지 정보에 기초하여, 분석기 컴포넌트가 컴퓨터 자산에서 발생되고 있는 공격을 식별하는 단계를 추가로 포함한다. 방법은 분석기 컴포넌트에 의해, 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하는 단계를 추가로 포함한다. 방법은 분석기 컴포넌트에 의해, 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다. 방법은 복수의 컴퓨터 자산들 중 다른 컴퓨터 자산에서, 업데이트된 글로벌 정책 데이터에 기초하여, 제1 정책을 기술하도록 다른 자산의 로컬 정책 데이터를 업데이트하는 단계를 추가로 포함하고, 다른 자산은 그 다른 자산이 그 다른 자산의 로컬 정책 데이터를 업데이트하는 시점에서는 공격에 수반된 메시지들을 아직 수신하지 않았다. 방법은 제1 정책에 기초하여, 다른 자산이 공격에 수반된 메시지를 차단 또는 리다이렉트하는 단계를 추가로 포함한다.

[0050] 일 실시예에 따르면, 데이터 처리 방법은 복수의 컴퓨터 자산들의 각각의 자산으로부터 메시지 정보를 수신하는 단계를 포함하고, 메시지 정보는 자산에 의해 수신된 메시지들을 기술한다. 방법은 복수의 컴퓨터 자산들 각각으로부터의 메시지 정보를 총괄적으로 분석하는 단계를 추가로 포함한다. 방법은 메시지 정보를 총괄적으로 분석하는 것에 기초하여 정책들을 생성하는 단계를 추가로 포함하고, 정책들은 정책들이 적용되는 메시지들을 식별하기 위한 로직뿐만 아니라, 정책들이 적용되는 메시지들에 대하여 수행할 정책-기반 액션들을 기술한다. 방법은 정책들을 기술하도록 글로벌 정책 데이터 리포지토리를 업데이트하는 단계를 추가로 포함한다. 방법은 복수의 컴퓨터 자산들에 정책 데이터를 전송하는 단계를 추가로 포함하고, 정책 데이터는 글로벌 정책 데이터 리포지토리에서 적어도 정책들을 기술한다. 방법은 분석기 컴포넌트를 구현하는 하나 이상의 컴퓨터 디바이스들에 의해 수행된다.

[0051] 일 실시예에서, 분석기 컴포넌트는 복수의 분석기들 중 하나의 분석기이고, 각각은 상이한 복수의 컴퓨터 자산들에 대해 이전 단락에서 인용된 단계들을 수행하도록 구성된다. 글로벌 정책 데이터 리포지토리는 적어도 복수의 분석기들 사이에서 공유된다.

[0052] 일 실시예에서, 방법은 메시지 정보로부터 시스템-레벨 정책에 의해 기술된 조건이 존재한다고 결정하는 것에 기초하여, 정책들 중 하나 이상의 정책들을 식별하는 단계를 추가로 포함한다. 방법은 기술된 조건을 고려하여 차단 또는 리다이렉트할 메시지들을 식별하기 위한 로직을 포함하는 하나 이상의 자산-레벨 정책들을 생성하는 단계를 추가로 포함한다. 방법은 생성된 하나 이상의 자산-레벨 정책들을 포함하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0053] 일 실시예에서, 방법은 메시지 정보를 총괄적으로 분석하는 것에 기초하여 컴퓨터 시스템 상의 분산형 공격을 식별하는 단계를 추가로 포함한다. 방법은 분산형 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하는 단계를 추가로 포함한다. 방법은 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0054] 일 실시예에서, 방법은 메시지 정보에 기초하여, 분석기 컴포넌트가 제1 컴퓨터 자산에서 발생되고 있는 공격을 식별하는 단계를 추가로 포함한다. 방법은 복수의 컴퓨터 자산들 중 적어도 제2 자산에서 공격에 수반된 메시지들을 식별하기 위한 로직을 포함하는 제1 정책을 생성하는 단계를 추가로 포함하고, 분석기 컴포넌트는 제2 자산이 공격에 수반된 메시지들을 수신하였음을 지시하는 메시지 정보를 제2 자산으로부터 아직 수신하지 않았다. 방법은 제1 정책을 기술하도록 글로벌 정책 데이터를 업데이트하는 단계를 추가로 포함한다.

[0055] 일 실시예에서, 정책들 중 주어진 정책에 의해 지시된 정책-기반 액션은 주어진 정책이 적용되는 임의의 메시지를 차단하는 것, 주어진 정책이 적용되는 임의의 메시지를 리다이렉트하는 것 또는 주어진 정책이 적용되는 임의의 메시지에 대해 자산이 정상적으로 응답하도록 허용하는 것 중 하나이다. 일 실시예에서, 정책 데이터를 전송하는 단계는 복수의 컴퓨터 자산들로부터 글로벌 데이터 리포지토리로의 직접적인 쿼리들에 응답하는 단계, 또는 분석기 컴포넌트에 의해, 글로벌 데이터 리포지토리로부터 정책 데이터를 리트리브하고, 분석기 컴포넌트로부터 복수의 컴퓨터 자산들로 정책 데이터를 전송하는 단계 중 하나의 단계를 포함한다. 일 실시예에서, 복수의 컴퓨터 자산들 중 제1 자산은 제1 자산에 의해 수신된 메시지들이 지향되는 서버 애플리케이션의 전방에 배치된다. 일 실시예에서, 복수의 컴퓨터 자산들 중 제1 자산은 제1 자산에 의해 수신된 적어도 일부 메시지들에 응답하는 웹 서버 애플리케이션을 실행시킨다.

[0056] 다른 양태들에서, 본 발명은 컴퓨터 장치 및 전술한 단계들을 수행하도록 구성된 컴퓨터-판독가능 매체를 포함한다.

[0057] 2.0. 구조적 개관

[0058] 도 1은 일 실시예에 따라 전술한 기법들이 실시될 수 있는 예시적인 네트워크화된 컴퓨터 시스템(100)을 도시한다. 시스템(100)은 하나 이상의 컴퓨팅 디바이스들을 포함한다. 이들 하나 이상의 컴퓨팅 디바이스들은 컴포넌트들(105-157)을 포함하여, 본 명세서에서 기술된 다양한 로직 컴포넌트들을 구현하도록 구성된 소프트웨어 및 하드웨어의 임의의 조합을 포함한다. 예를 들어, 하나 이상의 컴퓨팅 디바이스들은 본 명세서에서 기술된 다양한 컴포넌트들을 구현하기 위한 명령어들을 저장하는 하나 이상의 메모리들을 포함할 수 있고, 하나 이상의 하드웨어 프로세서들은 하나 이상의 메모리들, 및 다양한 컴포넌트들에 의해 사용되고 조작되는 데이터 구조들을 저장하는 하나 이상의 메모리들 내의 다양한 데이터 리포지토리들에 저장된 명령어들을 실행하도록 구성된다.

[0059] 일 실시예에서, 시스템(100)은 서버-사이드 프로세스들의 세트로서 시스템(100)의 다양한 컴포넌트들을 총괄적으로 구현하는 하나 이상의 서버 컴퓨터 디바이스들을 포함하는 서버 컴퓨터 시스템이다. 서버 컴퓨터 시스템은 웹 서버, 애플리케이션 서버, 데이터베이스 서버, 및/또는 도시된 컴포넌트들이 기술된 기능을 제공하기 위하여 이용하는 기타 통상적인 서버 컴포넌트들을 포함할 수 있다. 일 실시예에서, 특정 서버 컴포넌트들은 인터넷과 같은 하나 이상의 네트워크들에 의해 시스템(100)에 연결되는 "클라우드"-기반 시스템들을 이용하여 전체적으로 또는 부분적으로 구현될 수 있다. 클라우드-기반 시스템들은 이들이 시스템(100)의 컴포넌트들에 처리, 저장, 소프트웨어 및/또는 기타 자원들을 제공하는 인터페이스들을 노출시킬 수 있다. 일 실시예에서, 클라우드-기반 시스템들은 시스템(100)이 배치되는 다른 엔티티를 대신하여, 서드파티 엔티티에 의해 구현될 수 있다. 그러나, 다른 실시예들에서, 시스템(100)의 컴포넌트들은 단일의 엔티티에 의해 소유되고 동작되는 컴퓨터 시스템들에 의해 전체적으로 구현될 수 있다.

[0060] 2.1. 자산들

[0061] 본 명세서에서 사용됨에 있어서, 자산은 일반적으로 네트워크화된 컴퓨터 시스템의 논리적 또는 물리적 컴포넌트이다. 자산은 컴퓨팅 디바이스, 컴퓨팅 디바이스들의 시스템, 또는 이러한 컴퓨팅 디바이스들 또는 컴퓨팅 디바이스들의 시스템들에서 하드웨어 및/또는 소프트웨어의 임의의 조합에 의해 구현되는 컴포넌트일 수 있다. 일 실시예에서, 자산은 서버-기반 애플리케이션들이 하나 이상의 컴퓨터 네트워크들을 통해 클라이언트 컴퓨터들과 상호작용하는 하나 이상의 서버-사이드 인터페이스들을 포함한다. 예를 들어, 자산들은 웹 서버들, 애플리케이션 서버들, 특정 웹사이트들, 특정 애플리케이션들, 메일 서버들 등을 포함할 수 있다.

[0062] 시스템(100)은 다른 컴포넌트들 중에서, 네트워크(105) 또는 네트워크들(105)의 그룹에 의해 접속된 자산들(110)의 세트를 포함한다. 네트워크(105)는 예를 들어, 내부 네트워크 또는 인트라넷과 같은 신뢰된 네트워크일 수 있다. 시스템(100)은 실시예에 따라, 다른 자산들, 라우터들, 개인용 컴퓨터들, 개발 디바이스들, 백업 서버들 등과 같이 도시되지 않은 매우 다양한 타입들의 컴포넌트들을 포함할 수 있다. 네트워크(105)나 그에 직접 접속된 컴포넌트들은 모두 단일의 물리적 영역에 반드시 국한될 필요는 없다. 예를 들어, 일부 실시예들에서, 네트워크(105)는 상이한 지리적 영역들에 배치되지만, 전용 회선들, 가상 사설 네트워크들 및/또는 임의의 다른 적절한 메커니즘(들)을 통해 접속되는 복수의 서브-네트워크들을 포함할 수 있다.

[0063] 자산들(110)은 적어도 부분적으로 네트워크(105) 상의 네트워크 트래픽의 적어도 일부 양태를 관리할 책임이 있는 트래픽 관리 컴포넌트들로서 기능한다. 자산들(110)은 적어도 하나의 네트워크(195)를 통해 클라이언트들(190)과의 통신에 노출된다. 네트워크(105)와 반대로, 네트워크(195)는 시스템(100)의 소유자 또는 운영자가 제어를 실시하지 않는 공중 광역 네트워크 또는 인터넷과 같이 시스템(100)의 외부에 있는 신뢰되지 않고/않거나 감독되지 않는 네트워크일 수 있다. 따라서, 시스템(100)의 소유자 또는 운영자에 의해 사전-승인되지 않은 통신들이 클라이언트 컴퓨팅 디바이스로부터 네트워크(195)를 통해 수신될 수 있다. 적어도 하나의 이러한 실시예에서는, 메시지가 방화벽 또는 시스템(100) 내의 다른 트래픽 관리 컴포넌트를 먼저 통과하지 않고, 각각의 자산(110)이 네트워크(105)를 통해 하나 이상의 클라이언트들(190)로부터 직접 메시지들을 수신한다는 점에서, 각각의 자산(110)은 시스템(100)의 공격면의 일부를 형성한다. 그러나, 다른 실시예들에서, 메시지는 자산(110)에 도달하기 전에 라우터들, 로드 밸런서들, 다른 자산들(110) 또는 심지어 전용 방화벽들과 같은 임의의 수의 다른 컴포넌트들을 통과할 수 있다. 또한, 적어도 일부 실시예들에서는, 네트워크(195)와 네트워크(105) 간에 전혀 구별되지 않을 수 있다.

[0064] 일부 실시예들에서, 자산들(110)의 일부 또는 전부는 전용 방화벽 어플라이언스들, 전용 소프트웨어 방화벽들, 프록시 서버들, 에지 서비스 애플리케이션들, 로드 밸런서들, 게이트웨이 디바이스들, 및/또는 하나 이상의 다른 자산들의 전방에 배치되고, 다른 자산들로 지향되는 메시지들이 다른 자산들에 전달되기 전에 보안상 또는

다른 목적상 라우팅되는 다른 트래픽 관리 컴포넌트들일 수 있다. 다른 실시예들에서는, 별개의 트래픽 관리 컴포넌트들의 사용을 선행시켜, 자산들(110)의 일부 또는 전부가 그 자체로 메시지의 의도된 목적지이도록 하는 것이 유리할 수 있다. 예를 들어, 자산(110)은 웹 애플리케이션, API 서버, 또는 그 자신의 통합된 트래픽 관리 컴포넌트를 특징짓는 스트리밍 서버일 수 있다.

[0065] 일부 실시예들에서, 컴퓨팅 코드의 하나 이상의 라이브러리들이 기술되는 기법들을 구현하는 데에 이용가능할 수 있다. 하나 이상의 라이브러리들은 자산(110)에 의해 실행될 때, 자산(110)의 도시된 트래픽 관리 컴포넌트들의 일부 또는 전부를 구현하게 하는 명령어들을 포함한다. 각각의 자산(110)은 트래픽 관리 컴포넌트들을 구현하도록 동일한 하나 이상의 라이브러리들을 포함하거나 참조할 수 있다. 예를 들어, 하나 이상의 라이브러리들은 넷플릭스, 인크.에 의해 생성되는 에지 서비스들을 위한 Zuul 프레임워크와 같은 오픈 소스 웹 애플리케이션 프레임워크에 통합될 수 있고, 각각의 자산(110)은 그 인스턴스일 수 있다. 선택적으로, 각각의 자산(110)은 그때 메시지들에 대해 다른 기능들을 수행하기 위해 다른 도시되지 않은 추가적인 컴포넌트들을 구현하는 코드를 별개로 포함할 수 있다. 예를 들어, 일부 자산들(110)은 추가적인 웹 애플리케이션 컴포넌트들을 구현하는 코드를 실행할 수 있고, 다른 자산들(110)은 추가적인 API 서버 컴포넌트들을 구현하는 코드를 실행할 수 있다. 다른 실시예들에서, 자산들(110)은 라이브러리들의 공통 세트에 의존하기보다는, 도시된 트래픽 관리 컴포넌트들의 일부 또는 전부를 애드 혹 기반으로 구현할 수 있다.

[0066] 2.2. 클라이언트들

[0067] 클라이언트들(190)은 최종-사용자에 의해 종종 동작되는 개개의 컴퓨팅 디바이스들 또는 그 컴포넌트들일 수 있다. 예를 들어, 클라이언트(190)는 데스크탑 컴퓨터 상의 웹 브라우저, 셋-탑 미디어 박스, 모바일 디바이스 상에서 실행되는 애플리케이션 등일 수 있다. 네트워크(195)를 통해, 잠재적으로 자산들(110)을 포함하는 시스템(100)의 특정 컴포넌트들은 클라이언트들(190)에게 웹 페이지들 전달, 미디어 컨텐츠들 스트리밍, 이메일들 전송, 애플리케이션 프로그래밍 인터페이스("API") 호출들에 대한 응답 등과 같은 다양한 네트워크화된 서비스들을 제공한다. 이를 위해, 클라이언트들(190)은 다양한 메시지들을 자산들(110)에 전송하고/하거나 수신할 수 있다.

[0068] 2.3. 메시지 핸들링

[0069] 자산(110)은 적어도 하나의 메시지 핸들러 컴포넌트(112)를 포함한다. 메시지 핸들러(112)는 통신 인터페이스를 통해 클라이언트들(190)로부터 및/또는 클라이언트들(190)에 메시지들을 수신하도록 구성된다. 본 명세서에서 기술되는 목적들을 위해, 메시지는 클라이언트(190) 또는 자산(110)에 또는 그로부터 전송되는 임의의 데이터 구조를 포함할 수 있다. 메시지는 예를 들어, TCP 또는 UDP 패킷, HTTP 요청 또는 응답 또는 FTP 패킷과 같이, 매우 다양한 종류의 표준 네트워킹 프로토콜들 중 임의의 것에 따른 패킷 또는 데이터그램일 수 있지만, 이에 제한되지 않는다. 일 실시예에서, 메시지는 메시지의 컨텐츠들을 포함하는 "페이로드"뿐만 아니라, 전송자 및/또는 의도된 수신자에 대한 식별자들(예를 들어, IP 어드레스들, MAC 어드레스들, 도메인 네임들, 이메일 어드레스들 등), 메시지가 전달되고 있는 포트 번호, 메시지 타입 또는 다른 절대적 정보, 타임스탬프들, 라우팅 명령어들 등과 같은 "헤더" 또는 "트랜잭션" 정보를 포함하도록 구성된다. 그러나, 본 명세서에 기술되는 기법들은 임의의 특정 메시지 형태에 제한되지 않는다. 또한, 네트워크 계층 또는 전송 계층과 같은 하나의 계층 내의 관련된 메시지들의 그룹이 애플리케이션 계층과 같은 다른 계층에서 단일의 메시지를 형성하도록 구성되거나 해석된다는 점에서 복수의 계층들의 메시지들이 있을 수 있다. 실시예에 따라, 기술된 기법들은 매우 다양한 메시지 타입들 중 임의의 타입의 메시지들 및/또는 하나 또는 다수의 상이한 계층들에서의 메시지들에 적용될 수 있다.

[0070] 메시지 핸들러(112)는 메시지 수신에 응답하여 하나 이상의 지정된 액션들을 식별 및 수행하도록 구성될 수 있다. 예시적인 지정된 액션들로는 요청된 데이터 구조들을 리트리브 및 리턴하기, 메시지에 의해 특정된 파라미터들에 기초하여 데이터 구조들을 생성 및 저장 또는 리턴하기, 메시지에 의해 특정되거나 지시된 다른 자산에 메시지를 포워딩하기, 메시지를 포워딩할 자산을 선택하기 등이 포함되지만, 이에 제한되지 않는다. 지정된 액션은 메시지에서 특정될 수 있다. 예를 들어, 메시지 핸들러(112)는 웹 애플리케이션 서버일 수 있고, 메시지는 특정된 위치로부터 데이터를 리턴하거나 특정된 커맨드를 실행하라는 요청일 수 있다. 또는, 지정된 액션은 헤더 또는 트랜잭션 정보와 같은 메시지의 일부 양태로부터 암시적일 수 있다. 예를 들어, 목적지 IP 어드레스, 포트 번호 및/또는 URL 경로는 자산(110)에 메시지를 다른 자산으로 포워딩하라고 지시할 수 있다. 일부 실시예들에서, 지정된 액션은 자산(110)에 의해 수신된 모든 메시지들에 대해 동일할 수 있다. 예를 들어, 자산(110)은 항상 특정 서버 또는 애플리케이션에 메시지들을 포워딩하도록 구성되는 프록시 서버 컴포넌

트일 수 있다.

[0071] 그러나, 메시지에 대해 임의의 지정된 액션을 수행하기(또는 심지어는 지정된 액션을 식별하기) 전에, 메시지 핸들러(112)는 사전-처리를 위해 정책 인포서(policy enforcer)(114)에 수신된 메시지를 전송하여, 임의의 지정된 액션 전에 또는 그 대신에 임의의 정책-기반 액션이 수행되어야 하는지 여부를 결정하도록 구성된다. 정책 인포서(114)에 의한 이 사전-처리의 결과로서, 본 출원의 다른 곳에서 기술된 바와 같이, 일부 실시예들에서, 메시지 핸들러(112)는 메시지 핸들러(112)가 정상적인 방식으로 메시지를 계속해서 처리해야 하는지 여부에 대한 지시를 수신하고, 그에 따라, 지정된 액션(들)을 수행하거나, 메시지를 무시하거나, 또는 메시지를 리다이렉트하거나 지정된 상태 코드 또는 에러 메시지로 응답하는 것과 같은 다른 정책-기반 액션들을 수행할 수 있다. 다른 실시예들에서는, 정책 인포서(114)가 정책-기반 액션들의 수행을 담당할 수 있고, 그에 따라, 메시지 핸들러(112)는 단지 정상적인 방식으로 메시지를 계속해서 처리해야 하는지 여부에 대한 지시를 수신할 것이다.

[0072] 메시지 핸들러(112)는 수신된 메시지들, 또는 그로부터 도출된 정보를 메시지 로거 컴포넌트(message logger component)(113)에 전송하도록 추가로 구성된다. 메시지들 및/또는 메시지들로부터 도출된 정보는 그 후 메시지 로그들(message logs)(117)에 로그된다. 메시지 로그들(117)은 임의의 적절한 형태의 데이터 리포지토리에 저장될 수 있다. 메시지 로그들(117)은 헤더 필드 값들, 페이로드 컨텐츠들 등과 같이 메시지에 대한 임의의 적절한 특성들을 기술할 수 있다. 메시지 로그들(117)은 특정 양의 메시지들만이 저장되는 환형 캐시(circular cache)와 같은 임시 리포지토리일 수 있다. 또는, 메시지 로그들(117)은 더욱 영구적인 형태로 저장될 수 있다.

[0073] 주어진 메시지에 의해 지정된 액션 타입 및/또는 임의의 정책들이 적용되는지 여부에 따라, 클라이언트(190)는 주어진 메시지에 응답하여 응답 메시지를 수신할 수도 수신하지 않을 수도 있다. 응답 메시지는 메시지 핸들러(112) 또는 자산(110)의 다른 컴포넌트로부터 전송되거나 이를 통해 중계될 수 있다. 또는, 자산(110)이 원래 메시지를 시스템(100)의 다른 컴포넌트에 중계하였다면, 일부 실시예들에서, 응답 메시지는 그 다른 컴포넌트로부터 직접 수신될 수 있다. 메시지 로그들(117)은 주어진 메시지가 응답되었는지 여부, 주어진 메시지가 어떻게 응답되었는지를 추가로 지시할 수 있고, 및/또는 메시지 로그들(117)은 시스템 자원 사용과 같이 메시지를 처리하는 것에 관련된 운영 통계치(operating statistics)를 포함할 수 있다.

[0074] 2.4. 정책 시행

[0075] 자산(110)은 정책 인포서(114)를 추가로 포함한다. 정책 인포서(114)는 메시지들 및/또는 로컬 정책 캐시(115)에 기록된 정책들을 고려하여 메시지들과 연관된 정보를 분석하도록 구성된다. 로컬 정책 캐시(115)는 정책들을 자산(110)이 구현되는 컴퓨팅 디바이스 내에 또는 이에 직접 접속되는 저장 디바이스 상에 파일들, 파일들의 라인들(lines of files), 데이터베이스 기록들 등과 같은 데이터 구조들로서 저장하여, 정책 인포서(114)가 정책들을 쉽게 이용가능하도록 한다.

[0076] 정책은 정책이 메시지"에 적용되는지" 여부를 결정하기 위한 로직뿐만 아니라, 정책이 적용되는 경우, 메시지에 대해 수행되는 하나 이상의 정책-기반 액션들을 지시하는 하나 이상의 명령어들을 포함한다. 로직은 헤더 정보 또는 페이로드 컨텐츠와 같은 메시지의 고유 상세들에 기초할 수 있다. 선택적으로, 로직은, 특정 타입의 이전 메시지들의 개수와 같이 인스턴트 메시지에 관련될 수 있는 이전 메시지들에 대한 정보 또는 특정 지정된 소스를 갖는 이전 메시지들에 대한 정보에 추가로 기초될 수 있다. 이러한 타입의 정보는 예를 들어, 메시지 로그들(117)에 로그될 수 있다.

[0077] 일부 정책들에 있어서, 로직은, 매치되는 경우, 정책이 메시지에 적용됨을 지시하는 하나 이상의 값들 또는 값 범위들과 마찬가지로, 검사할 메시지의 특성(characteristic) 또는 특정 필드의 간단한 규격일 수 있다. 다른 정책들이 검사를 위해 추가적인 메시지 필드들 또는 특성들을 특정할 수 있다. 다른 예로서, 로직은 특정된 메시지 필드 또는 특성에 대해, 인스턴트 메시지와 동일한 값(또는 동일한 범위의 값들 내의 값)을 갖는 일정 기간 동안 수신된 모든 메시지들에 기초하여 통계치(statistic)를 계산하기 위한 함수를 특정할 수 있다. 로직은 정책이 적용되는지를 결정하기 위하여 계산된 통계치를 비교하기 위한 값을 추가로 지시할 수 있다. 물론, 본 명세서에 기술된 기법들은 정책을 표현하기 위한 임의의 특정 타입의 로직에 제한되지 않고, 변화하는 복잡도를 갖는 매우 다양한 정책들에 대해 사용될 수 있다.

[0078] 정책이 메시지에 적용된다고 결정되면, 실시예에 따라, 정책 인포서(114)는 메시지에 대해 취해야 하는 하나 이상의 정책-기반 액션들을 수행하거나, 메시지 핸들러(112)와 같은 다른 컴포넌트에게 하나 이상의 정책-기반 액션들을 수행하라고 명령할 수 있다.

[0079] 2.5. 로그 보고 및 분석

[0080] 시스템(100)은 적어도 하나의 분석기(150)를 추가로 포함한다. 분석기(150)는 자산들(110) 외부에 있다. 예를 들어, 분석기(150)는 자산들(110)의 일부 또는 전부와 상이한 세트의 하나 이상의 서버 컴퓨팅 디바이스들 상에서 실행될 수 있다. 분석기(150)는 복수의 자산들(110)에서 수신된 메시지들을 분석하고, 분석들에 기초하여 새로운 정책들을 식별하고, 복수의 자산들(110)에서 사용하도록 새로운 정책들을 발행하도록 구성된다.

[0081] 이를 위해, 각각의 자산(110)은 분석기(150)에 메시지들 및/또는 그 자산(110)에서 수신된 메시지들에 대한 정보를 전송하도록 구성된 보고 컴포넌트(118)를 포함한다. 도시된 바와 같이, 리포터(118)는 새로운 기록들에 대한 메시지 로그들(117)을 모니터하고, 필요에 따라, 이들 새로운 기록들을 반영하는 데이터를 분석기(150)에 스트리밍함에 있어서, 메시지 핸들러(112)와 관련하여 비동기적으로 동작한다. 그러나, 다른 실시예들에서, 메시지 핸들러(112) 또는 메시지 로거(113)는 리포터(118)가 반드시 메시지 로그들(117)에 액세스할 필요없이, 새로운 메시지를 처리할 때, 즉시 리포터(118)를 호출할 수 있다. 리포터(118)는 각각의 새로운 메시지에 대한 정보를 분석기(150)에 즉시 스트리밍할 수 있다. 또는, 리포터(118)는 복수의 메시지들에 대한 정보를 배치(batch)하고, 배치된 정보를 매우 다양한 규칙들 또는 프로토콜들 중 임의의 것에 따라 결정된 시점에 스트리밍하여, 자원 사용을 최적화할 수 있게 한다.

[0082] 일 실시예에서, 리포터(118)는 각각의 메시지의 로그를 전송한다. 다른 실시예들에서는, 메시지가 관심 대상임을 지시하는 일부 기준 또는 규칙을 메시지가 충족하는 경우에만 리포터(118)가 메시지에 대한 로그를 전송할 수 있다. 실시예에 따르면, 로그는 전체 메시지 또는 단지 특정 헤더 또는 트랜잭션 정보만을 포함할 수 있다. 일 실시예에서, 각각의 메시지에 대한 개개의 로그를 전송하는 대신에, 메시지들의 그룹들로부터 도출된 데이터가 다양한 통계치로 함께 집계되어 분석기(150)에 전송될 수 있다.

[0083] 분석기(150)는 메시지 데이터베이스(157)에 메시지 정보를 저장하도록 구성된다. 분석기(150)는 인터벌을 두고, 및/또는 조건들을 트리거하는 것에 응답하여, 계속적으로 메시지 데이터베이스(157) 내의 메시지 정보를 분석하도록 구성된 적어도 하나의 로그 분석기(152)를 추가로 포함한다.

[0084] 로그 분석기(152)는 분석기(150)의 정책 생성 컴포넌트(154)에 시스템(100)에 대한 상태 정보를 제공하도록 추가로 구성된다. 상태 정보는 실시예에 따라, 특정량의 시간 동안, 클라이언트(190)당 자산들(110)에 의해 수신된 특정 타입들의 메시지들의 개수, 각각의 자산(110)에 대한 활성 접속들의 횟수, 네트워크 자원 사용 트렌드들, 메모리 사용 트렌드들, 프로세서 사용 트렌드들, 기존의 정책들이 얼마나 빈번하게 적용되었는지의 표시 등과 같은 다양한 정보를 포함할 수 있다.

[0085] 일 실시예에서, 로그 분석기(152)는 메시지 정보에 기초하여 특정 클라이언트들(190)을 특징짓는 상태 정보 데이터를 포함하도록 추가로 구성될 수 있다. 예를 들어, 로그 분석기는 클라이언트(190)가 특정 기간 동안 특정 타입의 요청을 얼마나 자주 했는지에 기초하여, 클라이언트(190)를 현재 잠재적인 리스크인 것으로서 분류하는 로직을 구현할 수 있다. 정확한 특징화 로직은 관리자에 의해 구성가능하고, 및/또는 실시예에 따라 변할 수 있다.

[0086] 또한, 상태 정보가 이에 응답하여 정책 생성 컴포넌트(154)에 제공되는 빈도 또는 조건(들)은 실시예에 따라 변할 수 있다. 상태 정보는 동시에 전부 전송될 필요는 없다. 예를 들어, 로그 분석기(152)는 상태 정보의 개개의 아이템들이 식별됨에 따라 이들 아이템들을 보고할 수 있다.

[0087] 일 실시예에서, 로그 분석기(152)는 시스템(100) 내의 다른 컴포넌트들이 로그 분석기(152)가 이용가능한 다양한 상태 정보에 대해 쿼리할 수 있는 하나 이상의 서버 인터페이스들을 제공하도록 추가로 구성될 수 있다. 예를 들어, 시스템(100) 내의 자산은 (있다면) 특정 IP 어드레스 또는 도메인을 갖는 통신들과 관련된 정보에 대해 로그 분석기(152)에 쿼리할 수 있다. 이러한 쿼리는 다양한 이유때문에 유용할 수 있다 -- 예를 들어, 서버가 특정 IP 어드레스 또는 도메인으로부터 의심스러운 트래픽을 수신하였고, 쿼리의 결과들이 의심스러운 트래픽이 과거에 종종 발생했었다고 지시하는 경우, 서버는 그 IP 어드레스 또는 도메인을 블랙리스트화하는 것과 같은 액션들을 순행적으로(proactively) 취하도록 구성될 수 있다.

[0088] 2.6. 정책 생성 및 발행

[0089] 로그 분석기(152)로부터의 상태 정보에 기초하여, 정책 생성기(154)가 시스템(100)의 무결성에 대한 잠재적인 보안 위협들 또는 다른 리스크들을 식별하도록 구성된다. 식별된 리스크들에 기초하여, 정책 생성기(154)는 정책 데이터베이스(155)에 저장된 정책들을 생성, 수정 및/또는 삭제하여, 식별된 리스크들을 가장 최적으로 해결

하도록 (또한, 일부 실시예들에서는, 더 이상 존재하지 않는 리스크들을 해결하도록 의도된 정책들을 제거하도록) 추가로 구성된다. 리스크들을 식별하고 정책들을 생성하기 위한 다수의 기법이 존재하거나 가능하며, 정책 생성기(154)는 실시예에 따라 임의의 적절한 기법(들)을 사용할 수 있다.

[0090] 일 실시예에서, 정책 생성기(154)에 의해 생성된 정책은 분석기(150)가 담당하는 각각의 자산(110)에서의 애플리케이션을 위해 의도될 수 있다. 일 실시예에서, 일부 정책들은 특정 지리적 영역 또는 클러스터 내의 모든 자산들(110) 또는 특정 타입의 모든 자산들(110) 또는 심지어 단일의 특정된 자산(110)과 같은 특정 자산들(110)에서만의 애플리케이션을 위해 맞춰질 수 있다. 일 실시예에서, 정책 생성기(154)에 의해 생성된 정책은 주어진 자산(110)이 단지 자산(110)이 이미 이용가능한 정보에만 기초하여 그 정책에 적용가능한 메시지들을 충분히 식별하기에 충분한 로직을 포함한다. 예를 들어, 단일의 자산(110)이 다른 자산들(110)로부터의 메시지 로그들(117)에 대한 액세스가 부족한 경우에도, 및/또는 단일의 자산(110)이 시스템(100)의 임의의 다른 컴포넌트들과 메시지에 대해 통신하는 것이 요구되지 않고도, 정책은 그 단일의 자산(110)이 차단할 적용가능한 메시지를 식별하기에 충분한 정보를 가질 수 있다.

[0091] 일 실시예에서, 정책이 트래픽 정보에 기초하여 생성된 경우, 정책은 데이터 분석/수집에 실제적으로 기여하고 있지 않을 수 있는 임의의 종점들에 배포(distribute)될 수 있다. 예를 들어, 로그 분석기(152)는 주어진 IP 어드레스가 '불량'임을 발견할 수 있다. 그 후, 정책 생성기(154)는 그 IP 어드레스로부터의 메시지들을 차단하는 정책을 생성할 수 있다. 그 후, 정책은 다른 시스템들로 시스템(100)의 외부에서의 그 자신들의 독립적인 사용을 위해 배포될 수 있다. 예를 들어, 불량인 것으로 의심되는 IP들의 그레이리스트가 그 그레이리스트를 이용하여 리스크 또는 부정 스코어들을 계산하도록 구성된 다른 비접속 부정 검출 시스템에 주기적으로 발행될 수 있다.

[0092] 정책이 생성, 수정 또는 삭제되고 나면, 분석기(150)는 정책 데이터베이스(155)를 업데이트하여 생성되거나 수정된 정책을 포함하도록 또는 삭제된 정책을 제거하도록 한다. 그리고, 분석기(150)의 정책 퍼블리셔(156) 컴포넌트는 임의의 적절한 푸시-기반 및/또는 풀(pull)-기반 전달 기법(들)을 이용하여 각각의 자산(110)에 정책 데이터베이스(155) 내의 업데이트된 정책들을 발행하도록 구성된다. 차례로, 각각의 자산(110)은 정책 업데이트들을 수신하고 그에 따라 정책 캐시(115)를 업데이트하도록 구성된 정책 컨슈머 컴포넌트(116)를 포함한다. 일부 실시예들에서, 정책 퍼블리셔(156)는 단지 정책 데이터베이스(155)에 정책을 저장하는 역할만을 할 수 있으며, 각각의 정책 컨슈머(116)가 다양한 시점에서 정책 데이터베이스(155) 그 자체에 액세스하여, 대응하는 로컬 정책 캐시(115)를 정책 데이터베이스(155)와 동기화하도록 구성될 수 있다.

[0093] 일 실시예에서, 정책 생성기(154)가 자산들(110)에 대해 동적으로 정책들을 생성하는 한가지 방식은 언제 보다 많은 특정의 자산-레벨의 동적 정책들을 생성하는지를 결정하기 위하여 사용자-정의된 범용의 시스템-레벨 정책들의 세트를 사용하는 것이다. 예를 들어, 특정 타입의 요청이 특정 기간 동안 특정 횟수보다 많이 시스템(100)에서 (혹은 단일의 자산(110)에서 또는 조합하여 다수의 자산들(110)에서) 수신된 경우, 범용 정책은 특정 기간 동안 IP 어드레스를 블랙리스트화하고, 이 조건이 지속되는 경우, 그 IP 어드레스를 영구적으로 블랙리스트화하는 것일 수 있다. 정책 생성기(154)가 상태 정보로부터 이전 조건이 발생했음을 결정하면, 정책 생성기(154)는 각각의 자산(110)에게 특정 횟수 동안 그 IP 어드레스로부터의 메시지들을 차단하라고 명령하는 자산-레벨 정책을 동적으로 생성할 수 있다. 문제가 되는 조건이 중지되면, 정책 생성기(154)는 정책을 제거할 수 있다. 또는, 조건이 지속되면, 정책 생성기(154)는 영구적으로 시행될 자산-레벨 정책을 수정할 수 있다.

[0094] 단, 메시지 데이터베이스(157)가 복수의 상이한 자산들(110)로부터 수집된 메시지 정보를 포함하기 때문에, 분석기(150)의 컴포넌트들은 시스템(100) 내의 모든 자산들(110)에 대한 메시지 정보를 완전히 분석하여, 단지 개개의 자산들(110)에 영향을 미치는 위협들 대신에, 시스템(100)에 대한 위협들을 전체로서 식별할 수 있게 된다는 것에 유의한다. 이는 분석기(150)로 하여금 특정 타입들의 분산형 공격들을 각각의 자산의 로그들이 별개로 분석되었던 시스템에서 가능했던 것보다 더 빨리 식별할 수 있게 할 수 있다. 다시 말하지만, 상태 정보는 시스템(100)에 대한 네트워크 트래픽의 상태를 단순히 개개의 자산(110)에 대한 것과는 반대로 전체로서 기술하기 때문에, 정책 생성기(154)는 그렇지 않은 경우에 가능했던 것보다 더 빨리 분산형 공격들을 해결하는 정책들을 생성할 수 있고, 따라서, 전반적인 시스템(100) 상의 이러한 공격들에 대한 영향을 최소화할 수 있게 된다. 또한, 한가지 타입의 공격이 자산들(110) 중 하나 또는 작은 수의 자산들(110)에서 보이는 경우, 정책 생성기(154)는 공격을 해결하기 위하여 다른 자산들(110) 또는 심지어 전체 자산들(110)에 대해 정책들을 생성할 수 있고, 따라서 다른 자산들(110)로 하여금 이러한 자산들(110)이 아직 보지 못했을 수 있는 공격들에 대한 정책들을 선제적으로 배치할 수 있게 한다.

[0095] 2.7. 분산형 분석기들

[0096] 도 2는 일 실시예에 따라, 상이한 그룹들의 자산들(210)을 담당하는 복수의 분석기들(250)을 포함하는 예시적인 네트워크화된 컴퓨터 시스템(200)을 도시한다. 도 1의 시스템(100)에서와 같이, 시스템(200)은 하나 이상의 컴퓨팅 디바이스들을 포함한다. 이러한 하나 이상의 컴퓨팅 디바이스들은 컴포넌트들(210-255)을 포함하여, 본 명세서에서 기술된 다양한 로직 컴포넌트들을 구현하도록 구성된 소프트웨어 및 하드웨어의 임의의 조합을 포함한다.

[0097] 일 실시예에서, 각각의 자산(210)은 도 1의 자산(110)과 관련하여 기술된 것과 동일한 컴포넌트들을 포함할 수 있고, 각각의 분석기(250)는 도 1의 분석기(150)와 관련하여 기술된 것과 동일한 컴포넌트들을 포함할 수 있다. 따라서, 일 실시예에서, 시스템들(100 및 200)은 시스템(100)에 단지 단일의 영역만이 도시된 것을 제외하고는 실제로 동일한 시스템들일 수 있다. 다른 실시예들에서, 도 1에 도시된 것과 상이한 컴포넌트들 및/또는 그 구성을 사용하는 것을 제외하고, 자산들(210) 및/또는 분석기(250)는 대신에 자산들(110) 및/또는 분석기(150)와 관련하여 기술된 것과 유사한 기능을 제공하도록 구성될 수 있다. 시스템(200)은 복수의 분석기들(250)을 포함하지만, 본 명세서에서 기술된 기법들이 분석기(150)가 시스템(100) 내의 유일한 분석기 컴포넌트였던 경우에서와 같이, 단일의 중앙화된 분석기를 갖는 시스템들에 동일하게 적용될 수 있음에 유의하여야 한다.

[0098] 시스템(200)은 도시된 영역들(231 및 232)과 같이 2 이상의 영역들로 세분화된다. 영역들(231 및 232)은 지리적 영역들에 대응한다. 예를 들어, 영역(231)은 북아메리카의 데이터 센터에 대응할 수 있고, 영역(232)은 유럽의 데이터 센터에 대응할 수 있다. 그러나, 일 실시예에서, 영역들(231 및 232)은 임의의 그룹들의 자산들(210)일 수 있으며, 그 그룹들이 지리적 영역에 대응하는지와 상관없다.

[0099] 각각의 영역(231)은 하나 이상의 클러스터들을 포함할 수 있다. 예를 들어, 도시된 바와 같이, 영역(231)은 클러스터들(221) 및 클러스터들(222)을 포함하고, 영역(232)은 클러스터들(223 및 224)을 포함한다. 각각의 클러스터(221-224)는 복수의 자산들(210)을 포함한다. 클러스터는 자산들(210)의 어떤 임의의 하위-그룹일 수 있다. 예를 들어, 클러스터들(221 및 223)은 웹 서버 자산들인(또는 이를 보호하는) 그 각각의 영역들 내의 그 자산들(210)로 구성되는 "웹 클러스터들"일 수 있고, 클러스터들(222 및 224)은 API 서버 자산들인(또는 이를 보호하는) 그 각각의 영역들 내의 그 자산들(210)로 구성되는 "API 클러스터들"일 수 있다. 그러나, 다른 실시예들에서, 클러스터들은 다른 범주화 구조들, 지리적 근접도, 구현하는 컴퓨팅 디바이스들 또는 임의의 다른 적절한 그루핑 기준에 의해 그룹화될 수 있다.

[0100] 각각의 자산(210)은 수신된 메시지들에 관한 정보를 자산(210)이 속하는 영역(231/232)의 분석기(250)에 스트리밍하거나 그렇지 않으면 전송하도록 구성된다. 분석기들(250)은 공유된 다-영역 데이터 리포지토리(255)에 정책들을 발행하도록 구성된다. 예를 들어, 다-영역 데이터 리포지토리(255)는 정책 데이터베이스(155)를 저장할 수 있다. 다-영역 데이터 리포지토리(255)는 중앙 데이터 리포지토리일 수 있고, 또는 다-영역 데이터 리포지토리(255)는 각각의 영역(231/232) 전반에 걸쳐 분산될 수 있다. 예를 들어, 각각의 영역(231/232)은 임의의 적절한 동기화 기법(들)을 통해 다른 영역들(231/232) 내의 사본들과 동기화되는 다-영역 데이터 리포지토리(255)의 그 자신의 사본을 저장할 수 있다.

[0101] 각각의 자산(210)에서, 정책들의 로컬 사본은 다-영역 데이터 리포지토리(255)에서 찾아진 것과 동기화된 채로 유지된다. 자산(210)은 다-영역 데이터 리포지토리(255)에 직접 액세스할 수 있고, 또는 대응하는 분석기(250)를 통해 동기화가 발생할 수 있다. 각각의 자산(210)은 정책들의 로컬 사본을 유지하기 때문에, 자산이 그 대응하는 분석기(250)와의 컨택을 잃어버리거나, 일정 기간 동안 다-영역 데이터 리포지토리(255)와 통신할 수 없는 경우에도, 각각의 자산(210)은 비교적 최근의 정책들의 세트를 적용하는 것이 보장될 수 있다. 동기화가 발생하는 빈도는 예를 들어, 시스템 자원들의 이용가능성, 및 분석기(250)에서 정책을 생성하는 것과 자산(210)에서 정책을 시행하는 것 사이에 "래그(lag)" 시간이 얼마나 허용되는지에 기초하여 관리자에 의해 구성가능할 수 있다.

[0102] 일 실시예에서, 각각의 분석기(250)는 자산(210)이 속하는 영역(231/232) 내의 단지 그 자산들(210)로부터의 메시지 정보에 기초하여 정책들을 생성하도록 구성될 수 있다. 따라서, 그 각각의 영역(231/232) 내의 상이한 네트워크 트래픽 때문에, 일부 분석기들(250)은 다른 분석기들(250)이 생성할 수 없는 정책들을 생성할 수 있을 것이다. 다른 실시예에서는, 예를 들어, 메시지 데이터베이스(157)를 다-영역 데이터 리포지토리(255)에 공유된 데이터베이스로서 저장하는 것에 의해, 각각의 분석기(250)가 대응하는 영역(231/232)에 대한 메시지 정보를 다른 영역들로부터의 분석기들(250)과 공유한다. 이는, 각각의 분석기(250)가 유사하게 구성되는 경우, (상이한 영역들에서의 데이터 공유 프로세스들 간의 지연으로 인해, 하나의 분석기(250)가 다른 분석기(250) 전부터

정책을 생성할 수 있더라도) 이에 따라 각각의 분석기(250)가 결국 유사한 정책들을 생성할 수 있는 실시예들을 만들어낼 수 있다. 이는 분석기(250)가 불량이었던 이벤트에서 리던던시(redundancy)를 제공한다.

[0103] 2.8. 중간-계층(Mid-Tier) 컴포넌트들

[0104] 일 실시예에서, 시스템(200)은 하나 이상의 중간-계층 컴포넌트들(241)을 선택적으로 포함한다. 중간-계층 컴포넌트들(241)은 인간 운영자 및/또는 자산들(210)에 의해 적용되는 추가적인 정책들을 지시하며 시스템(200) 내에서 실행되는 자동화된 프로세스들로부터의 입력들을 허용하도록 구성된다. 이들 추가적인 정책들은 예를 들어, 고정된 정책들, 또는 분석기(250)가 동적으로 생성하지 않았을 수 있지만, 인간 운영자들 또는 자동화된 프로세스들이 다양한 기법들을 이용하여 식별한 비지니스 규칙들일 수 있다. 각각의 분석기(250)는 (예를들어, 로그 분석기(152)를 통해) 상태 정보 또는 메시지 로그들을 리트리브하거나, 현재 정책들의 세트를 리트리브하거나, 분석기(250)에게 새로운 정책을 수정 또는 생성하라고 명령하는 것과 같은 태스크들을 수행하기 위하여 중간-계층 컴포넌트들(241)에 대한 API를 노출하도록 구성될 수 있다. 예를 들어, 일 실시예에서, 하나의 중간-계층 컴포넌트(241)는 인간 운영자가 메시지 로그들에 관련된 통계치를 보고 이러한 통계치를 고려하여 새로운 정책을 구성하게 하는 웹 인터페이스를 제공한다. 다른 중간-계층 컴포넌트는 부정 검사들을 수행하기 위하여 분석기(250)가 이용가능한 것 이외의 데이터를 사용할 수 있고, 이에 기초하여, 새로운 정책들을 자동으로 생성하여 분석기(250)에 전송할 수 있다. 또 다른 중간-계층 컴포넌트(241)는 간단한 레이트-위반(rate-breach) 제한들을 이용하여 검출될 수 있는 것과 같은 특정 타입들의 공격들을 빠르게 식별하도록 설치되는, 자산(110) 내에 배치된 다른 도시되지 않은 컴포넌트들(예를 들어, 메시지 핸들러(112)의 전방에 배치된 전치-필터 컴포넌트)과 상호작용함으로써 정책들을 생성하는 데에 최적화된 컴포넌트일 수 있다.

[0105] 2.9. 기타

[0106] 시스템들(100 및 200)은 본 명세서에 기술된 기법들을 수행하는 데에 적합한 시스템들의 단지 예시들일 뿐이다. 다른 시스템들은 다양한 구성들에서 추가적이거나 또는 더 적은 컴포넌트들을 포함할 수 있다. 컴포넌트들 간의 기능들의 분리는 또한 실시예에 따라 상이할 수 있다. 도 1에 도시된 자산(110)과 분석기(150)의 하위컴포넌트들은 본 명세서에서 기술된 본 발명의 기법들을 설명할 의도로 기술된 로직 컴포넌트들이다. 하위컴포넌트들은 소프트웨어 애플리케이션들, 패키지들, 모듈들, 클래스들, 프로세스들 또는 객체들의 별개의 세트들에 실제로 대응할 수도 대응하지 않을 수도 있다. 예를 들어, 일부 실시예들에서, 리스크들을 식별하고 정책들을 생성하는 프로세스들은 밀접하게 연관되어, 로그 분석기(152) 및 정책 생성기(154)가 단일의 서버 애플리케이션으로서 구현될 수 있게 한다. 다른 예로서, 메시지 핸들러(112), 메시지 로거(113) 및 정책 인포서(114)는 일부 실시예들에서 단일의 소프트웨어 애플리케이션을 형성할 수 있다.

[0107] 본 명세서에 기술된 다양한 데이터 엘리먼트들은 다양한 방식들로 저장될 수 있다. 예를 들어, 각각의 정책 캐시(115), 메시지 로그들(117), 정책 데이터베이스(155) 및 메시지 데이터베이스(157)는 하나 이상의 데이터 리포지토리들에 별개의 하나 이상의 데이터베이스 테이블들, 데이터베이스들 또는 파일들로 저장될 수 있다. 다르게는, 다양한 데이터 엘리먼트들 중 일부는 하나 이상의 조합된 데이터베이스 테이블들, 데이터베이스들 및/또는 파일들 내에 함께 저장될 수 있다.

[0108] 3.0. 기능적 개관

[0109] 3.1. 로컬 정책들 적용

[0110] 도 3은 일 실시예에 따라, 분산형 트래픽 관리 시스템에 로컬 정책들을 적용하기 위한 예시적인 흐름(300)을 도시한다. 흐름(300)의 다양한 요소들은 전술한 시스템들(100 및 200)과 같은 시스템들을 포함하여 다양한 시스템들에서 수행될 수 있다. 일 실시예에서, 이하 기술되는 기능 블록들과 관련되어 기술되는 각각의 프로세스들은 하나 이상의 컴퓨터 프로그램들, 다른 소프트웨어 엘리먼트들 및/또는 범용 컴퓨터 또는 전용 컴퓨터 중 임의의 것의 디지털 로직을 사용하여 구현될 수 있고, 컴퓨터의 메모리의 물리적 상태와 상호작용하고 이를 변환시키는 것을 수반하는 데이터 리트리브, 변환 및 저장 동작들을 수행할 수 있다. 흐름(300)은 자산에서 로컬 정책들을 적용하는 것의 하나의 예시이다. 다른 흐름들은 다양한 구성들에서 더 적거나 추가된 요소들을 포함할 수 있다.

[0111] 블록(310)은 클라이언트(190)와 같은 클라이언트 디바이스 또는 메시지가 수신될 수 있는 임의의 다른 디바이스로부터 메시지를 수신하는 단계를 포함한다. 메시지는 HTTP 요청 또는 TCP 패킷과 같은 임의의 타입의 메시지일 수 있다. 메시지는 자산(110) 또는 임의의 다른 적절한 자산과 같은 자산에서 수신된다. 일 실시예에서, 메시지는 파일 리트리브, 애플리케이션 실행, 다른 시스템 컴포넌트로의메시지 포워딩 등과 같이, 수행되는 지

정된 액션을 특정하거나 그렇지 않으면 지시할 수 있다.

[0112] 블록(320)은 자산에 대한 로컬 정책 데이터에서 메시지가 테스트되어야 하는 정책들의 세트를 식별하는 단계를 포함한다. 예를 들어, 로컬 정책 데이터는 정책 캐시(115), 또는 정책들을 기술하고 자산에 로컬인 저장 디바이스 상에 저장되는 임의의 다른 적절한 데이터 구조(들)일 수 있다.

[0113] 블록(330)은 정책들에 의해 특정되는 하나 이상의 메시지 속성들에 대한 값들을 식별하는 단계를 포함한다. 예를 들어, 메시지 속성들은 소스 또는 목적지 IP 어드레스들, 요청되는 통합 자원 지시자(uniform resource indicator: URI), 참조 URI(referring URI), 메시지와 연관된 쿠키 또는 세션 데이터, 타임스탬프들, 트랜잭션 메타데이터, 페이로드 내의 특정 키워드들의 존재 등과 같은 헤더 필드들을 포함할 수 있지만, 이에 제한되지 않는다. 일 실시예에서, 메시지 속성들은 자산에 의해 수신되었고 하나 이상의 유사한 속성들을 가진 이전 메시지들로부터 적어도 부분적으로 도출된 통계치 또는 다른 정보를 포함할 수 있다. 이들 이전 메시지들은 이러한 목적 및 다른 목적을 위해, 예를 들어, 메시지 로그(117) 또는 임의의 다른 적절한 로컬 리포지토리에 로그되었을 수 있다. 메시지 속성들은 미리 정의되거나 잘 알려진 메시지 필드 또는 특성(characteristics)에 대응하여, 메시지 속성들을 도출하기 위한 로직이 이미 자산에 알려져 있게 할 수 있다. 다르게는, 정책은 다른 메시지 속성들로부터의 값을 계산하도록 구성된 함수들 또는 다른 실행가능한 로직을 특정함으로써 메시지 속성에 대한 값을 식별하는 방식을 특정할 수 있다.

[0114] 블록(340)은 식별된 값들에 기초하여, 정책이 메시지에 적용될지 여부를 결정하는 단계를 포함한다. 정책이 메시지에 적용될지 여부를 결정하기 위한 임의의 적절한 기법이 사용될 수 있다. 블록(340)은 예를 들어, 정책에 의해 특정된 값 또는 값들의 범위를 블록(330)에서 식별된 값 또는 값들과 비교하는 단계를 포함할 수 있다. 정책은 하나 이상의 조건들을 포함할 수 있다. 정책에 의해 특정된 로직에 따라, 정책이 적용되는 메시지가 하나의 조건과 이들 조건들 전부 사이의 어딘 가에 매치되도록 요구될 수 있다.

[0115] 블록(340)은 블록(320)에서 식별된 정책들 중 일부 또는 이들 전부에 대해 수행될 수 있다. 일부 실시예들에서, 블록들(320-340)은 다수의 반복들을 사용해서 수행된다. 예를 들어, 단일의 최고 우선순위의 정책이 제1 반복에서 로드될 수 있다. 그 정책에 필요한 값들은 블록(330)마다 계산된다. 그 후, 블록(340)의 결정이 그 단일의 정책에 대해 수행된다. 정책이 적용되지 않으면, 그 후 매치되는 정책이 발견될 때까지 또는 어느 정책도 적용되지 않는다고 결정될 때까지, 추가적인 반복들이 계속하여 각각의 다른 정책들에 대해 수행된다. 다른 실시예들에서는, 결정 트리들 또는 상태 머신들과 같은 다양한 최적화가 수행되어, 복수의 정책들 또는 심지어는 모든 정책들이 단일의 반복에서 고려되게 할 수 있다. 일 실시예에서, 매치되는 정책이 발견되고 나면, 어떠한 다른 정책들도 고려될 필요가 없고, 따라서, 블록(340)(및 선택적으로는 블록(330))이 다른 정책들에 대해 수행될 필요가 없다. 일 실시예에서, 매치되는 정책이 발견되었는지 여부에 관계없이 모든 정책들이 고려되고, 복수의 적용가능한 정책들에 의해 지시되는 임의의 충돌하는 정책-기반 액션들을 조정하기 위해 다양한 우선순위화 메커니즘들이 사용될 수 있다.

[0116] 블록(340)에서 정책이 메시지에 적용된다고 결정되었다면, 그 후 흐름은 블록(350)으로 진행한다. 블록(350)은 적용가능한 정책과 연관된 하나 이상의 정책-기반 액션들을 수행하는 단계를 포함한다. 정책-기반 액션들은, 예를 들어, 메시지 차단하기(예를 들어, "블랙리스트화"), 메시지를 메시지가 어드레스되는 목적지 이외의 목적지로 포워딩하기, 메시지가 어드레스된 목적지로 진행하도록 허용하기(예를 들어, "화이트리스트화"), 에러 메시지 또는 다른 적절한 메시지를 이용하여 메시지에 응답하기, 및/또는 자산이 구현하도록 구성될 수 있는 임의의 다른 적절한 타입의 액션을 포함할 수 있다. 다른 예로서, 액션은 (예를 들어, 후속하는 정책 결정 또는 생성 프로세스들에 유용하도록) 메시지에 대해 정상적으로 로그되지 않았던 상세한 메시지 정보에 로그하는 것일 수 있다.

[0117] 블록(360)은 메시지를 정상적인 방식으로 처리하는 것(예를 들어, 메시지에 의해 지시되는 지정된 액션을 수행하는 것)으로 진행할지 여부를 결정하는 단계를 포함한다. 메시지를 차단하거나 에러 메시지를 이용하여 응답하는 것과 같은 특정 정책-기반 액션들은 자산에게 메시지를 정상적인 방식으로 처리하는 것으로 진행하지 않게 암시적으로 또는 명시적으로 명령할 수 있고, 결과적으로 흐름은 메시지의 처리가 중지되는 블록(370)으로 진행한다. 메시지를 허용하거나 상세한 메시지 정보에 로그하는 것과 같은 다른 정책-기반 액션들은 자산에게 메시지를 정상적인 방식으로 처리하는 것으로 진행하라고 암시적으로 또는 명시적으로 명령할 수 있다. 결과적으로, 흐름은 블록(380)으로 진행한다.

[0118] 또한, 블록(340)에서 어떠한 정책도 메시지에 적용되지 않는다고 결정되었다면, 흐름은 블록(380)으로 진행한다. 블록(380)은 메시지에 의해 지시되는 지정된 액션을 수행하는 것에 의하는 것과 같이 메시지를 정상

적인 방식으로 처리하는 단계를 포함한다.

[0119] 3.2. 정책 생성 및 발행

[0120] 도 4는 일 실시예에 따라, 분산형 트래픽 관리 시스템에서 정책들을 생성하고 발행하기 위한 예시적인 흐름(400)을 도시한다. 흐름(400)의 다양한 요소들은 전술한 시스템들(100 및 200)과 같은 시스템들을 포함하여 다양한 시스템들에서 수행될 수 있다. 일 실시예에서, 이하 기술되는 기능 블록들과 관련되어 기술되는 각각의 프로세스들은 하나 이상의 컴퓨터 프로그램들, 다른 소프트웨어 엘리먼트들 및/또는 범용 컴퓨터 또는 전용 컴퓨터 중 임의의 것의 디지털 로직을 사용하여 구현될 수 있고, 컴퓨터의 메모리의 물리적 상태와 상호작용하고 이를 변환시키는 것을 수반하는 데이터 리트리브, 변환 및 저장 동작들을 수행할 수 있다.

[0121] 블록(410)은 복수의 자산들이 도 3의 블록(310)을 수행한 결과로서 발생하는 것과 같이, 자산들에서 메시지들을 수신하는 단계를 포함한다. 도시되지는 않았지만, 각각의 자산들은 자산이 수신하는 메시지들 중 일부 또는 전부에 응답하여 흐름(300)을 수행할 수 있다. 흐름(400)의 행위는 자산들이 흐름(300)을 수행하는 것과 관련하여 비동기적으로 블록(410)으로부터 진행할 수 있다.

[0122] 블록(420)은 자산들이 분석기(150)와 같은 분석기에 전송할 메시지 정보를 식별하는 단계를 포함한다. 블록(430)은 분석기에 메시지 정보를 전송하는 단계를 포함한다. 일부 실시예들에서, 메시지 정보는 본질적으로 각각의 메시지의 전체 사본이기 때문에, 블록(420)은 사소한 단계이다. 다른 실시예들에서, 블록(420)은 다양한 검출 기법들을 이용하여, 분석기(150)가 잠재적으로 관심을 갖는 메시지들을 식별하는 단계를 포함할 수 있다. 예를 들어, 자산은 분석기(150)에 의해 행해지는 정책 결정들에 영향을 줄 수 있는 특이한 메시지들을 식별하기 위한 다양한 규칙들 또는 머신 학습 로직으로 구성될 수 있다. 따라서, 모든 메시지들에 대한 메시지 정보를 전송하기보다는, 자산은 잠재적으로 관심있는 메시지들에 대해서만 메시지 정보를 전송할 것이다. 일 실시예에서, 메시지 정보는 분석기가 관심가질 수 있는 데이터(예를 들어, 필드들, 속성들, 통계치들 등)만을 포함하도록 추가로 필터링, 요약, 집계 또는 다르게 처리될 수 있다. 일 실시예에서, 메시지 정보는 자산 처리 시간량 또는 메시지에 응답하는 데 사용되는 자산 자원들 또는 임의의 정책들이 적용되었는지 여부와 같이, 주어진 메시지를 처리하는 것과 관련하여 수집된 데이터를 포함할 수 있다.

[0123] 일 실시예에서, 블록들(420-430)은 자산들에서 블록(410)에서의 메시지 수신과 관련하여 비동기적으로 실행하는 프로세스들에 의해 수행된다. 예를 들어, 각각의 자산은 주기적으로 또는 다른 방식으로 블록(410)에 응답하여 자산에 의해 생성되는 로컬 메시지 로그를 판독하고, 그 후 이에 기초하여 블록들(420-430)을 수행하는 리포터(118)와 같은 메시지 스트리밍 컴포넌트를 포함할 수 있다. 이러한 실시예들에서, 메시지 정보는 복수의 메시지들에 대해 동시에 함께 배치(batch)될 수 있다. 또는, 메시지 스트리밍 컴포넌트는 연속적으로 메시지 정보를 식별할 수 있지만, 네트워크 자원들이 이용가능해질 때까지 및/또는 다른 조건들이 충족될 때까지 메시지 정보를 전달하는 것을 대기할 수 있다. 다른 실시예들에서, 블록들(420-430)은 흐름(300)의 블록(310)에서 메시지의 수신시 또는 메시지에 대한 흐름(300)의 종료시와 같이, 메시지를 수신하는 것에 응답하여 즉시 수행된다.

[0124] 블록(440)은 분석기가 메시지 정보를 로그하는 단계를 포함한다. 분석기는 전체 메시지 정보에 로그할 수 있고, 또는 분석기는 메시지 정보를 처리하여, 오직 필터링, 요약화 또는 집계된 메시지 정보에만 로그할 수 있다. 메시지 정보는 메시지 데이터베이스(157) 및/또는 다-영역 데이터 리포지토리(255)와 같은 임의의 적절한 리포지토리에 저장될 수 있다.

[0125] 블록(450)은 분석기가 로그된 메시지 정보에 의해 지시된 바람직하지 않은 조건을 식별하는 단계를 포함한다. 예를 들어, 분석기는 특정 IP 어드레스 또는 IP 어드레스들의 그룹으로부터의 자산에 대한 공격, 복수의 시스템들에 영향을 미치고 있는 분산형 공격, 메시지의 타입 또는 바람직하지 않은 양의 시스템 자원들을 소비하고 있는 클라이언트들의 그룹 등을 식별할 수 있다. 분석기는 미리 정의된 규칙들 또는 패턴 인식에 입각한 로직과 같이 이러한 조건들을 검출하기 위한 임의의 적절한 로직을 채용할 수 있다. 선택적으로, 블록(450)은 서버 로드 통계치와 같은 시스템에 대한 다른 상태 정보에 기초하여 바람직하지 않은 조건들을 식별하는 단계(예를 들어, 오버로드되거나 불량인 서버로부터의 요청을 일시적으로 리다이렉트시키는 정책을 생성할지 여부를 지시함)를 추가로 또는 대신에 포함할 수 있다. 또한, 블록(450)은 더 이상 존재하지 않는 이전에 바람직하지 않았던 조건들을 식별하여, 불필요한 정책들이 제거될 수 있게 하는 단계를 선택적으로 포함할 수 있다.

[0126] 블록(460)은 분석기가 바람직하지 않은 조건을 해결하기 위하여 적어도 하나의 정책을 생성하는 단계를 포함한다. 정책은 IP 어드레스 또는 IP 어드레스들의 범위 차단하기, 특정 타입들의 요청들을 리다이렉트하기 등과 같은 임의의 적절한 방식으로 바람직하지 않은 조건을 해결할 수 있다. 임의의 적절한 적응식 정책 생성 기법

이 사용될 수 있다. 일 실시예에서, 정책은, 다른 자산들에서 무슨 메시지들이 수신되고 있는지에 대한 지식을 단일의 자산이 가질 필요없이, 또한 그 단일의 자산이 분석기와 통신할 필요 없이, 그 단일의 자산에서 적용할 수 있는 자산-레벨 정책이다.

[0127] 일 실시예에서, 분석기는 더 많은 범용 시스템-레벨 정책들에 기초하여 특정 자산-레벨 정책들을 생성할 수 있다. 시스템-레벨 정책들은, 잠재적으로는 복수의 자산들로부터의 메시지 정보를 반영하는 속성들을 포함하여 적어도 메시지 정보로부터 도출된 다양한 속성들의 함수들에 기초하여, 바람직하지 않은 조건을 지시하는 기준을 특정한다. 바람직하지 않은 조건이 발견될 때, 시스템-레벨 정책들은 어떤 자산-레벨 정책이 생성되어야 하는지를 추가로 나타낼 수 있다.

[0128] 일 실시예에서, 정책은 시간 기준을 포함할 수 있다. 분석기 및/또는 개개의 자산들은 그 각각의 시간 기준에 의해 지시된 바와 같이, 만료된 정책들을 자동으로 제거하도록 구성될 수 있다.

[0129] 블록(470)은 정책 데이터베이스(155) 및/또는 다-영역 데이터 리포지토리(255)와 같은 정책 데이터의 리포지토리에 정책을 기술하는 데이터를 저장하는 단계를 포함한다.

[0130] 흐름(400)의 나머지 부분으로 진행하기 전에, 블록(450-470)은 다수의 가능한 바람직하지 않은 조건들에 대해 반복될 수 있다.

[0131] 블록(480)은 자산들에 정책 업데이트들을 전송하는 단계를 포함한다. 블록(480)은 예를 들어, 자산들이 정책 데이터의 리포지토리부터 직접 정책 데이터를 리트리브하기, 자산들이 간격을 두고 분석기가 정책 업데이트들을 제공할 것을 요청하기, 및/또는 새로운 정책들이 생성될 때 또는 일부 다른 기준에 기초하여 분석기가 자산들에 새로운 정책 업데이트들을 푸시하기를 포함할 수 있다. 예를 들어, 각각의 자산은 정책 업데이트들을 청취하고/하거나 정책 업데이트들에 대해 분석기 또는 리포지토리를 폴링하는 정책 컨슈머(116)와 같은 컨슈머 컴포넌트를 포함할 수 있다.

[0132] 블록(490)은, 자산들이 임의의 종류의 동기화 수단을 사용하여 그 자신의 로컬 정책 데이터를 정책 업데이트들과 동기화시키는 단계를 포함한다. 단, 자산들은 흐름(400)과 관련하여 비동기적으로 흐름(300)의 다양한 반복들을 수행하고 있기 때문에, 자산은, 흐름(300)의 반복을 한 번 수행한 후에, 다른 메시지를 수신하기 전에, 블록(490)을 수행할 수 있음을 유의한다. 따라서, 그 자산에 대한 흐름(300)의 다음 반복은 흐름(300)의 이전 반복에서 고려되지 않았던 하나 이상의 새로운 정책들을 지시하는 업데이트된 정책 데이터에 기초할 것이다.

[0133] 흐름(400)은 정책을 생성하고 발행하는 일례이다. 다른 흐름들은 다양한 구성들에서 더 적거나 추가된 요소들을 포함할 수 있다. 예를 들어, 하나의 실시예에서, 블록(440)은 필요하지 않다. 다른 실시예에서, 블록들(450 및 460)은 조합될 수 있다. 다른 예로서, 흐름(400)은 예를 들어, 중간-계층 컴포넌트들(241/242)을 통해 수신될 수 있는 바와 같이, 외부 컴포넌트들에 의해 생성된 비지니스 규칙들 또는 필터들을 반영하는 고정된 정책들을 분석기가 수신하는 단계를 추가로 포함할 수 있다. 또한, 이들 고정된 정책들은 블록(470)에서 정책 데이터의 리포지토리에 추가될 수 있다.

[0134] 일 실시예에서, 블록들(410-440) 및/또는 블록들(480-490)은 흐름(400)의 나머지 요소들에 대해 비동기적으로, 실질적으로 연속하여 수행된다. 한편, 블록들(450-470)은 주기적으로 또는 다른 간격을 두고, 또는 특정 타입들 또는 특정 양들의 메시지 정보의 수신과 같이 다양한 트리거링 조건들에 응답하여 반복될 수 있다.

[0135] 일 실시예에서, 블록들(430-480)은 시스템(200) 또는 다른 분산형 시스템들과 같은 분산형 시스템에서 복수의 분석기들에 의해 수행될 수 있다.

[0136] 4.0. 예시적인 구현 상세들

[0137] 일 실시예에 따르면, 분석기는, 이에 제한되지는 않지만, 보안 정책들을 시행하기, 악의적이거나 사기적인 액티비티를 차단하기, 비지니스 규칙들을 시행하기, 레이트-제한들과 같은 특정 조건들에 기초하여 요청들에 대한 커스텀 액션 실행하기, 네트워크의 에지에서의 안티 크로스-사이트 요청 위조 보호, 네트워크의 에지에서의 안티 크로스-사이트 스크립팅 보호, 빠른 반응 시간들을 인에이블하기 위하여 실시간으로 사전적 보안 모니터링하기(경고 액션들, 및/또는 보안 공격 패턴들을 연구하기 위하여 샌드박스 클러스터에 악의적인 트래픽을 라우트하는 라우트 액션들의 구현 포함), 보안-관련 사고들에 기초하여 반응형 보안 모니터링하기, 임의의 인프라스트럭쳐 취약점들에 대한 통찰들을 도출하기 위하여 보안 관련 데이터를 애드혹 분석하기, 및/또는 자산이 덜 타겟이 되도록 공격자들을 유인하기 중 일부 또는 전부를 위해 구성된 자산-레벨 정책들을 생성할 수 있다.

[0138] 4.1. 예시적인 정책 구조들

[0139] 일 실시예에 따르면, 제1 정책 데이터베이스는 데이터베이스에 복수의 로우(row)들을 포함한다. 각각의 로우는 정책을 표현한다. 로우의 필수 필드들은 예를 들어, 정책 식별자, 경로 파라미터 및 액션 파라미터를 포함할 수 있다. 로우의 선택적인 필드들은 메소드 파라미터(methods parameter), 레이트 파라미터, 영역 파라미터, 클러스터 파라미터, 호스트 파라미터 및/또는 커스텀 파라미터(custom parameter)를 포함할 수 있다. 각각의 파라미터들은 상이한 메시지 속성에 대응하고, 단일 값, 값들의 범위 및/또는 값들의 리스트를 포함하여, 정책이 적용되는지를 결정하도록 대응하는 메시지 속성과 비교할 수 있다.

[0140] 일 실시예에 따르면, 제2 정책 데이터베이스는 로우들을 이용하여 정책들을 표현한다. 각각의 로우는 액션들을 시행할 대상(예를 들어, IP 어드레스, 디바이스 식별자, 사용자 에이전트(User Agent), 고객 ID(Customer ID) 등) 및 정책 ID를 특정한다. 각각의 로우는 경로, 메소드, 영역, 클러스터, 호스트 또는 커스텀과 같은 메시지 속성들에 대응하는 하나 이상의 필드들에 대한 값들을 추가로 포함한다. 실시예에 따라, 필드들 중 하나 이상은 정책이 적용될지 여부를 결정할 때 무시되는 메시지 속성들을 지시하는 공백으로 남겨둘 수 있다. 각각의 로우는 시작 시간, 종료 시간 및/또는 회귀 패턴과 같이 정책을 위한 스케줄을 지시하는 선택적인 필드들을 추가로 포함할 수 있다. 각각의 로우는 수행하는 액션을 특정하는 필드를 추가로 포함한다.

[0141] 제1 정책 데이터베이스 및 제2 정책 데이터베이스는 실시예에 따라, 서로 함께 또는 그들끼리만 사용될 수 있다. 일 실시예에서, 제1 정책 데이터베이스는 제2 정책 데이터베이스에 언제 정책들을 생성할지를 결정하기 위해 분석기에 의해 시스템 레벨에서 사용되는 반면, 제2 정책 데이터베이스는 들어오는 메시지들에 정책들을 시행하기 위하여 자산들에서 사용된다. 그러나, 다른 실시예에들에서, 로컬 정책 데이터는 제1 정책 데이터베이스 및 제2 정책 데이터베이스 모두를 포함할 수 있다.

[0142] 제1 정책 데이터베이스 및 제2 정책 데이터베이스는 단지 정책 데이터 구조들의 예들일 뿐이다. 또 다른 실시예들에서, 정책들은 임의의 다른 적절한 구조 또는 포맷으로 국지적으로 및/또는 전역적으로 저장될 수 있다.

[0143] 4.2. 예시적인 정책 캐시들

[0144] 일 실시예에 따르면, 자산은 하나 이상의 별개의 캐시들의 형태로 로컬 정책 데이터를 저장할 수 있다. 일 실시예에서, 제1 캐시는 글로벌 자원 캐시이다. 글로벌 자원 캐시는 자산들에 대한 자원 URI들을 이들 URI들에 적용되는 적절한 규칙들에 매핑하는 것을 포함한다. 다른 용도들 중에서, 글로벌 정책 캐시의 한가지 용도는 블랙리스트들 및 특정 URI들 대한 특정 규칙들을 시행하는 것이다. 예를 들어, 예시적인 사용 케이스에서, 고객 서비스 센터들은 이커머스 플랫폼에서 액세스-감지 종점들을 사용하도록 화이트리스트화된다. 그러나, 화이트리스트화는 고객 서비스 에이전트들로 하여금 모든 종점들에 대한 액세스를 허용하지만, 다른 내부 도구들, 개발자들 및 테스트 팀들에 의해서는 사용되도록 의도되고 고객 서비스 에이전트들에 대해서는 차단되어야 하는 몇몇 URI들이 있을 수 있다. 글로벌 자원 캐시에 이러한 자원들을 리스트화하고, 글로벌 자원 캐시에서의 매치를 위해 들어오는 요청 URI를 평가함으로써, 이러한 비지니스 규칙들이 시행될 수 있다. 일반적으로, 글로벌 자원 캐시는 워크플로우에서의 나머지 처리를 단락하기 위한 좋은 후보자들인 자원 규칙들을 포함한다.

[0145] 일 실시예에서, 제2 캐시는 대상 규칙들 캐시이다. 대상 규칙들 캐시는 대상(예를 들어, IP, 디바이스 식별자, 고객 Id)을 시행하는 즉각적인 규칙들에 매핑하는 것을 포함한다. 이 캐시는 각각의 URI에 대해 특정하게 다루지 않고, 대상에 절대적으로 적용될 수 있는 규칙들을 포함한다. 이러한 정책의 예로는 "고객 Id 12456689로부터의 모든 요청을 차단"하는 것이 있다.

[0146] 일 실시예에서, 제3 캐시는 대상 자원 캐시이다. 대상 자원 캐시는 대상(예를 들어, IP, 디바이스 식별자, 고객 Id)을 시행하는 자원-특정 규칙들에 매핑하는 것을 포함한다. 이 캐시는 특정 URI들에만 적용될 수 있는 정책들을 포함한다. 이러한 정책의 예로는 고객 Id 12456689로부터 URI 경로 /홈으로의 요청들을 차단"하는 것이 있다.

[0147] 이러한 캐시들 및/또는 다른 타입들의 캐시들의 다양한 조합들 중 임의의 것이 정책들을 저장하는 데에 사용될 수 있다. 특정 실시예에서, 이들 3개의 캐시들은 다음의 워크플로우를 이용하여 함께 사용된다. 먼저, 메시지가 수신된다. 그 후, 메시지는 정책 시행으로부터 메시지를 배제할지 여부를 결정하기 위하여 전역적 배제들(global exclusions)의 세트를 이용하여 처리된다. 메시지가 배제되지 않으면, 그 후 자산은 다음으로 메시지 URI가 글로벌 자원 캐시에 있는지 여부를 결정한다. 만약 없다면, 자산은 다음으로 메시지에 대응하는 고객 ID가 대상 규칙들 캐시 또는 대상 자원 캐시에 있는지 여부를 결정한다. 만약 없다면, 자산은 다음으로 메시지의 소스 IP 어드레스가 대상 규칙들 캐시 또는 대상 자원 캐시에 있는지 여부를 결정한다. 만약 없다면, 자산은

다음으로 메시지의 디바이스 식별자가 대상 규칙들 캐시 또는 대상 자원 캐시에 있는지 여부를 결정한다. 만약 없다면, 그 후 메시지는 정상적으로 처리된다. 그러나, 전술한 결정들 중 임의의 것이 긍정적이면, 대응하는 정책들에 대한 적절한 액션(들)이 시행된다.

[0148] 4.3. 예시적인 구성 옵션들

[0149] 일 실시예에 따르면, 자산의 특정 거동들은 이하의 구성 옵션들 중 일부 또는 전부를 이용하여 구성될 수 있다. 빈도 파라미터는 자산이 얼마나 종종 로컬 정책 캐시를 업데이트하는지를 제어한다. 예를 들어, 예시적인 빈도는 30초이다. 다양한 "인에이블된" 파라미터들은 자산의 개개의 하위컴포넌트들이 활성화되어 있는지 여부를 제어할 수 있어서, 예를 들어, 정책 시행 또는 로그 보고가 특정 자산들에 대해 디스에이블되게 할 수 있다. 모드 파라미터는 자산이 정책-기반 액션들을 실제로 수행하도록, 또는 자산이 테스트 모드에 있지 않은 경우 자산이 어떤 정책-기반 액션들을 수행했는지를 자산이 단순히 보고하는 테스트 모드에서 동작하도록 구성되는지를 제어한다. 로그 레벨 파라미터는 얼마나 많은 메시지 정보가 로그되는지 및/또는 분석기로 전송되는지를 제어할 수 있다. 화이트리스트 파라미터는 자산이 화이트리스트된 메시지들 상에 실제로 다른 정책들을 시행하는지 여부를 제어할 수 있다. 다른 실시예들에서, 어떠한 이러한 구성 파라미터들도 제공되지 않을 수도 있고, 및/또는 다양한 다른 구성 파라미터들도 가능하다.

[0150] 4.4. 예시적인 메시지 로그들

[0151] 일 실시예에 따르면, 메시지 정보는 JSON 블랍(blob) 또는 다른 적절한 데이터 구조로 로그되고/되거나 스트리밍될 수 있다. 데이터 구조는 디바이스 식별자, IP, 고객 ID, 애플리케이션 명, 지리적 위치 데이터, 요청 별명, 요청 URL, 응답 상태, 날짜, 호스트 명, 메시지 배치 ID, 검출된 정책 액션 등과 같은 필드들을 포함할 수 있지만, 이에 제한되지 않는다. 예를 들어, 하나의 이러한 로그는 다음과 같을 수 있다.

[0152] 표 1: 예시적인 메시지 로그


```
{
      "Ip": "127.0.0.1",
      "capp": "apiproxy",
      "customerId": "135048091",
      "detectaction": "BlockAction with status code 403\t
            message: Forbidden",
      "geoData": "[ zip=null, pmsa=reserved,
            network_type=reserved, dma=-1, bw=reserved,
            areacode=reserved, asnum=reserved,
            long=reserved, ipaddress=127.0.0.1,
            country_code=US, throughput=reserved,
            network=reserved, city=reserved,
            timezone=reserved, region_code=reserved,
            county=reserved,
            company=Internet_Assigned_Numbers_Authority,
            continent=reserved, domain=reserved,
            msa=reserved, fips=reserved, lat=reserved, ]",
      "log": "",
      "logLevel": "INFO",
      "request_alias": "/favicon.ico",
      "request_url":
            "http://movies.netflix.com:1234/favicon.ico",
      "response_status": "200",
      "rowId": "1392335738461-1"
}
1392335742847
mac-p.corp.netflix.com
20140213
23
merged_20140214T001750_1
```


[0153]

[0154] 물론, 다양한 다른 로그 구조들 및 필드들 또한 가능하다.

[0155] 4.5. 예시적인 쿼리들

[0156] 일 실시예에 따르면, 분석기는 로그된 메시지 정보를 수반하는 다양한 쿼리들을 사용하여 정책들을 생성할 대상들을 식별하도록 구성될 수 있다. 이러한 쿼리들의 예들은, 특정 영역(예를 들어, US)에서 상위 n개의 요청 IP 어드레스들을 식별하기, 특정 API를 호출한 특정 영역 내의 상위 n개의 요청 IP 어드레스들을 식별하기, 특정 API에 대해 POST 이외의 메소드를 호출한 특정 영역 내의 상위 n개의 요청 IP 어드레스들을 식별하기, 잠재적으로 개방되어 있는 관리 콘솔들에 대한 서비스들을 스캔하고 있는 특정 영역 내의 상위 n개의 요청 IP 어드레스들을 식별하기, 및 PHP 종점들에 대한 서비스들을 스캔하고 있는 특정 영역 내의 상위 n개의 요청 IP 어드레스들을 식별하기를 포함할 수 있지만, 이에 제한되지 않는다. 물론, 이들 예들은 표현될 수 있는 매우 다양한 쿼리들 중 단지 예시일 뿐이다.

[0157] 마찬가지로, 중간-계층 컴포넌트는 통계적 분석, 비지니스 규칙들 공식화 등과 같은 목적들을 위해 이들 및 다른 쿼리들을 분석기에 만들어낼 수 있다.

[0158] 5.0. 하드웨어 개관

[0159] 하나의 실시예에 따르면, 본 명세서에 기술된 기법들은 하나 이상의 전용 컴퓨팅 디바이스들에 의해 구현된다. 전용 컴퓨팅 디바이스들은 기법들을 수행하기 위해 하드-와이어드형일 수 있고, 또는 기법들을 수행하도록 지속적으로 프로그래밍되는 하나 이상의 주문형 집적 회로(application-specific integrated circuit : ASIC)들 또는 필드 프로그래머블 게이트 어레이(field programmable gate array : FPGA)들과 같은 디지털 전자 디바이스들을 포함할 수 있고, 펌웨어, 메모리, 다른 스토리지 또는 그 조합의 프로그램 명령어들에 따라 기법들을 수행하도록 프로그래밍되는 하나 이상의 범용 하드웨어 프로세서들을 포함할 수 있다. 이러한 전용 컴퓨팅 디바이스들은 또한 기법들을 달성하기 위해 커스텀 하드-와이어드형 로직, ASIC들 또는 FPGA들을 커스텀 프로그래밍과 결합할 수 있다. 전용 컴퓨팅 디바이스들은 데스크탑 컴퓨터 시스템들, 포터블 컴퓨터 시스템들, 핸드헬드 디바이스들, 네트워킹 디바이스들 또는 기법들을 구현하기 위해 하드-와이어드형 로직 및/또는 프로그램 로직을 포함하는 임의의 다른 디바이스일 수 있다.

[0160] 예를 들면, 도 5는 본 발명의 실시예가 구현될 수 있는 컴퓨터 시스템(500)을 도시하는 블록도이다. 컴퓨터 시스템(500)은 버스(502) 또는 정보를 전달하기 위한 다른 통신 메커니즘, 및 버스(502)와 연결되고 정보를 처리하기 위한 하드웨어 프로세서(504)를 포함한다. 하드웨어 프로세서(504)는 예를 들어, 범용 마이크로프로세서일 수 있다.

[0161] 또한, 컴퓨터 시스템(500)은 랜덤 액세스 메모리(RAM)와 같은 메인 메모리(506), 또는 버스(502)에 연결되고 정보 및 프로세서(504)에 의해 실행되는 명령어들을 저장하기 위한 다른 동적 저장 디바이스를 포함한다. 메인 메모리(506)는 또한 임시 변수들 또는 프로세서(504)에 의해 실행되는 명령어들의 실행 동안의 다른 중간 정보를 저장하는 데에 사용될 수 있다. 이러한 명령어들은, 프로세서(504)가 액세스가능한 비일시적 저장 매체에 저장될 때, 컴퓨터 시스템(500)을, 명령어들로 특정된 동작들을 수행하도록 커스터마이즈되는 전용 머신으로 렌더링한다.

[0162] 컴퓨터 시스템(500)은 판독 전용 메모리(ROM)(508), 또는 버스(502)에 연결되고 프로세서(504)를 위해 정적 정보 및 명령어들을 저장하기 위한 다른 정적 저장 디바이스를 추가로 포함한다. 자기 디스크 또는 광 디스크와 같은 저장 디바이스(510)가 제공되며, 버스(502)에 연결되어 정보 및 명령어들을 저장한다.

[0163] 컴퓨터 시스템(500)은 정보를 컴퓨터 사용자에게 디스플레이하기 위하여 음극선관(cathode ray tube : CRT)과 같은 디스플레이(512)에 버스(502)를 통해 연결될 수 있다. 영숫자 및 다른 키들을 포함하는 입력 디바이스(514)는 버스(502)에 연결되어 정보 및 커맨드 선택들을 프로세서(504)에 전달한다. 다른 타입의 사용자 입력 디바이스는 마우스, 트랙볼, 또는 방향 정보 및 커맨드 선택들을 프로세서(504)에 전달하고 디스플레이(512) 상에서 커서 이동을 제어하기 위한 커서 방향 키들과 같은 커서 컨트롤(516)이 있다. 이 입력 디바이스는 통상적으로 디바이스로 하여금 평면에서의 위치들을 특정하게 할 수 있는 2개의 축, 즉 제1 축(예를 들어, x) 및 제2 축(예를 들어, y)에서 2개의 자유도를 갖는다.

[0164] 컴퓨터 시스템(500)은, 커스터마이즈된 하드-와이어드형 로직, 하나 이상의 ASIC들 또는 FPGA들, 컴퓨터 시스템과 조합하여 컴퓨터 시스템(500)으로 하여금 전용 머신으로 되게 야기하거나 프로그래밍하는 펌웨어 및/또는 프로그램 로직을 사용하여 본 명세서에 기술된 기법들을 구현할 수 있다. 하나의 실시예에 따르면, 본 명세서의 기법들은 프로세서(504)가 메인 메모리(506)에 포함된 하나 이상의 명령어들의 하나 이상의 시퀀스들을 실행하는 것에 응답하여 컴퓨터 시스템(500)에 의해 수행된다. 이러한 명령어들은 저장 디바이스(510)와 같은 다른 저장 매체로부터 메인 메모리(506)로 판독될 수 있다. 메인 메모리(506)에 포함된 명령어들의 시퀀스들의 실행은 프로세서(504)로 하여금 본 명세서에 기술된 프로세스 단계들을 수행하게 한다. 다른 실시예들에서, 하드-와이어드형 회로는 소프트웨어 명령어들 대신에 또는 이와 결합하여 사용될 수 있다.

[0165] 본 명세서에서 사용된 "저장 매체"라는 용어는 머신으로 하여금 특정 방식으로 동작하게 하는 데이터 및/또는 명령어들을 저장하는 임의의 비일시적 매체를 지칭한다. 이러한 저장 매체는 비휘발성 매체 및/또는 휘발성 매체를 포함할 수 있다. 비휘발성 매체는 예를 들어, 저장 디바이스(510)와 같은 광 또는 자기 디스크를 포함한다. 휘발성 매체는 메인 메모리(506)와 같은 동적 메모리를 포함한다. 통상적인 형태들의 저장 매체는 예를 들어, 플로피 디스크, 플렉서블 디스크, 하드 디스크, 고상 드라이브, 자기 테이프, 또는 임의의 다른 자기 데이터 저장 매체, CD-ROM, 임의의 다른 광 데이터 저장 매체, 홀들의 패턴들을 갖는 임의의 물리적 매체, RAM, PROM, 및 EPROM, FLASH-EPROM, NVRAM, 임의의 다른 메모리 칩 또는 카트리지를 포함한다.

[0166] 저장 매체는 전송 매체와 구별되지만, 이와 함께 사용될 수 있다. 전송 매체는 저장 매체 사이에서 정보를 전달하는 역할을 한다. 예를 들어, 전송 매체는 버스(502)를 포함하는 배선들을 포함하여, 동축 케이블들, 구리 배선 및 광섬유들을 포함한다. 또한, 전송 매체는 전파 및 적외선 데이터 통신들 동안에 생성되는 것과 같은

광파 또는 음향파의 형태를 취할 수 있다.

[0167] 실행을 위해 프로세서(504)에 하나 이상의 명령어들의 하나 이상의 시퀀스들을 운반하는 데에 다양한 형태의 매체가 관련될 수 있다. 예를 들어, 명령어들은 초기에는 원격 컴퓨터의 자기 디스크 또는 고상 드라이브 상에서 운반될 수 있다. 원격 컴퓨터는 명령어들을 그 동적 메모리에 로드하고, 모뎀을 사용하여 전화 회선을 통해 명령어들을 전송할 수 있다. 컴퓨터 시스템(500)에 로컬인 모뎀은 전화 회선 상에서 데이터를 수신하고, 적외선 송신기를 사용하여 데이터를 적외선 신호로 변환할 수 있다. 적외선 검출기는 적외선 신호로 운반된 데이터를 수신할 수 있고, 적절한 회로가 버스(502) 상에 데이터를 배치할 수 있다. 버스(502)는 프로세서(504)가 명령어들을 리트리브하고 실행하는 메인 메모리(506)로 데이터를 운반한다. 메인 메모리(506)에 의해 수신된 명령어들은 프로세서(504)에 의한 실행 전 또는 후에 선택적으로 저장 디바이스(510)에 저장될 수 있다.

[0168] 컴퓨터 시스템(500)은 또한 버스(502)에 연결된 통신 인터페이스(518)를 포함한다. 통신 인터페이스(518)는 로컬 네트워크(522)에 접속되는 네트워크 링크(520)에 양방향 데이터 통신 커플링을 제공한다. 예를 들어, 통신 인터페이스(518)는 통합 서비스 디지털 네트워크(integrated services digital network : ISDN) 카드, 케이블 모뎀, 위성 모뎀 또는 데이터 통신 접속을 대응하는 타입의 전화 회선에 제공하는 모뎀일 수 있다. 다른 예로서, 통신 인터페이스(518)는 호환형 LAN에 데이터 통신 접속을 제공하는 근거리 네트워크(LAN) 카드일 수 있다. 무선 링크들 또한 구현될 수 있다. 임의의 이러한 구현에서, 통신 인터페이스(518)는 다양한 타입들의 정보를 표현하는 디지털 데이터 스트림들을 운반하는 전기, 전자기 또는 광 신호들을 송수신한다.

[0169] 네트워크 링크(520)는 통상적으로 데이터 통신을 하나 이상의 네트워크들을 통해 다른 데이터 디바이스들에 제공한다. 예를 들어, 네트워크 링크(520)는 접속을 로컬 네트워크(522)를 통해 호스트 컴퓨터(524)에 또는 인터넷 서비스 제공자(Internet Service Provider : ISP)(526)에 의해 운영되는 데이터 설비에 제공할 수 있다. 차례로, ISP(526)는 이제 관용적으로 "인터넷"(528)이라고 불리는 월드 와이드 패킷 데이터 통신 네트워크를 통해 데이터 통신 서비스들을 제공한다. 로컬 네트워크(522) 및 인터넷(528)은 둘 다 디지털 데이터 스트림들을 운반하는 전기, 전자기 또는 광신호들을 사용한다. 컴퓨터 시스템(500)으로/으로부터 디지털 데이터를 운반하는 다양한 네트워크들을 통한 신호들 및 네트워크 링크(520) 상의 그리고 통신 인터페이스(518)를 통한 신호들은 전송 매체의 예시적인 형태들이다.

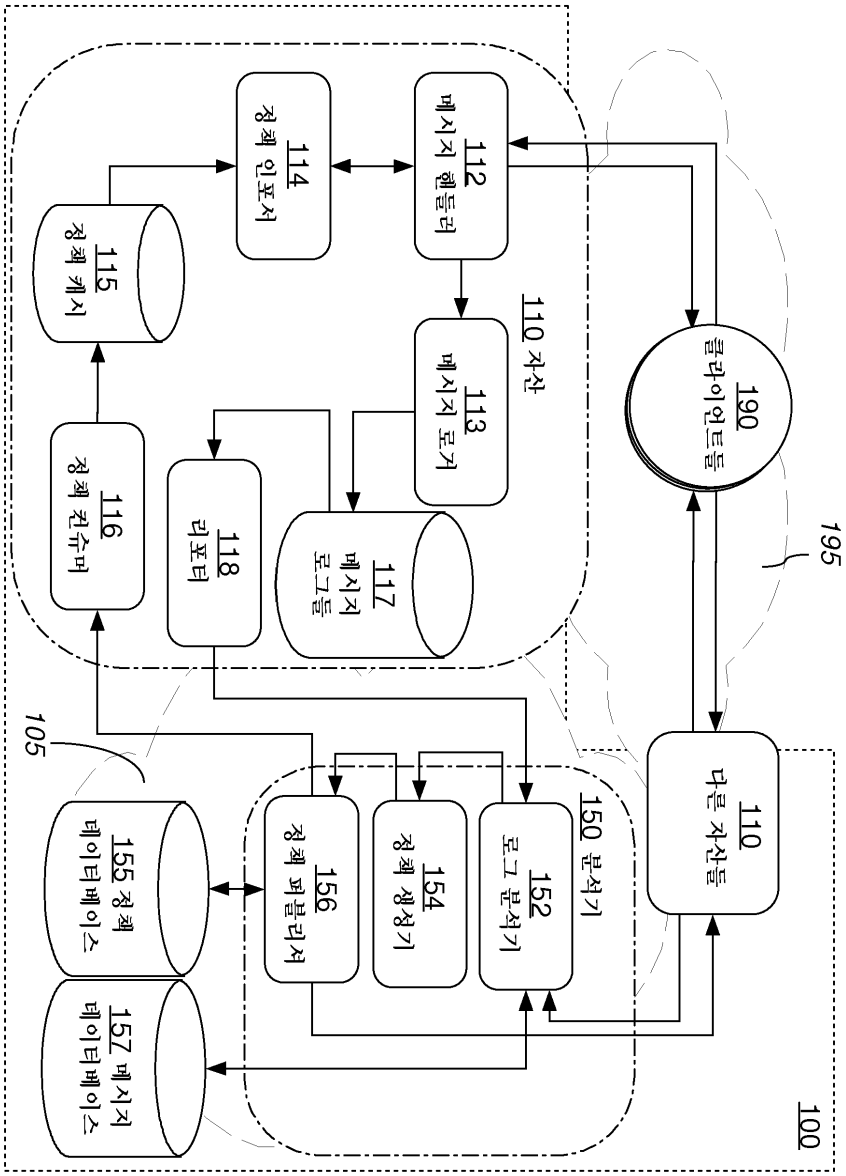
[0170] 컴퓨터 시스템(500)은 네트워크(들), 네트워크 링크(520) 및 통신 인터페이스(518)를 통해 메시지들을 전송하고 프로그램 코드를 포함한 데이터를 수신할 수 있다. 인터넷 예에서, 서버(530)는 인터넷(528), ISP(526), 로컬 네트워크(522) 및 통신 인터페이스(518)를 통해 애플리케이션 프로그램을 위한 요청된 코드를 전송할 수 있다.

[0171] 수신되는 코드는 코드가 수신됨에 따라 프로세서(504)에 의해 실행될 수 있고, 및/또는 저장 디바이스(510) 또는 나중의 실행을 위한 다른 비휘발성 스토리지에 저장될 수 있다.

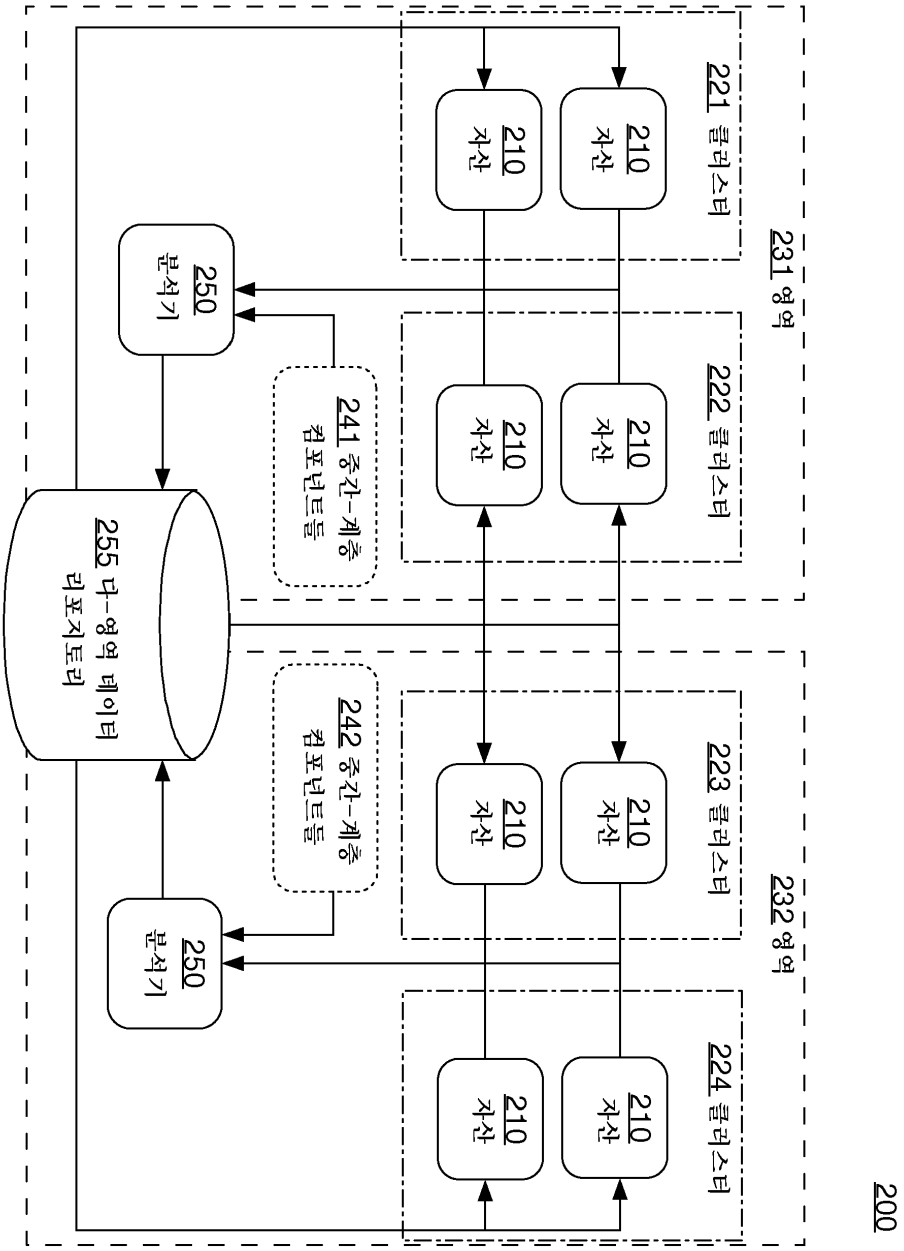
[0172] 전술한 명세서에서, 본 발명의 실시예들은 구현마다 변할 수 있는 다수의 특정 상세들을 참조하여 기술되었다. 따라서, 명세서 및 도면들은 제한적인 의미보다는 예시적인 것으로 고려된다. 본 발명의 범위의 유일하고 배타적인 지시자, 및 출원인들에 의해 본 발명의 범위인 것으로 의도되는 것은 임의의 후속적인 보정을 포함하여 본 출원으로부터 발행되는 청구범위의 세트가 발행하는 특정한 형태의 이러한 청구범위의 세트의 문자 그대로의 등가의 범위이다. 이와 관련하여, 본 출원의 청구범위에서는 특정 청구항 종속성이 개시되어 있지만, 본 출원의 종속 청구항들의 특징들은 단순히 청구범위의 세트에 인용된 특정 종속성들에만 따르지 않고, 본 출원의 다른 종속 청구항들의 특징들 및 독립 청구항들의 특징들과 적절히 결합될 수 있음에 유의한다.

도면

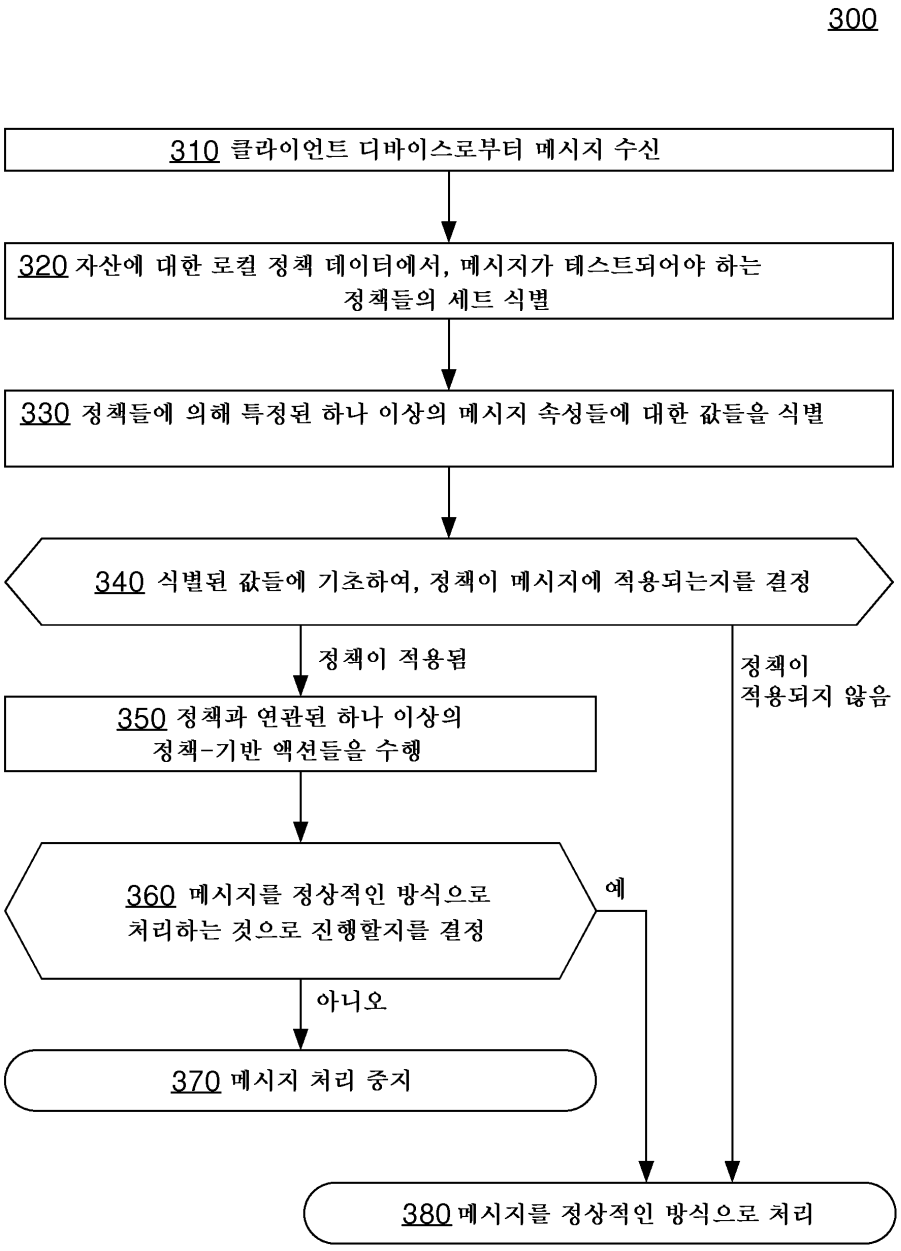
도면1


100
105
195
110 자산
112 메시지 핸들러
113 메시지 로거
114 정책 인포서
115 정책 캐시
116 정책 컨슈머
117 메시지 로그들
118 리포터
190 클라이언트들
110 다른 자산들
150 분석기
152 로그 분석기
154 정책 생성기
156 정책 퍼블리셔
155 정책 데이터베이스
157 메시지 데이터베이스

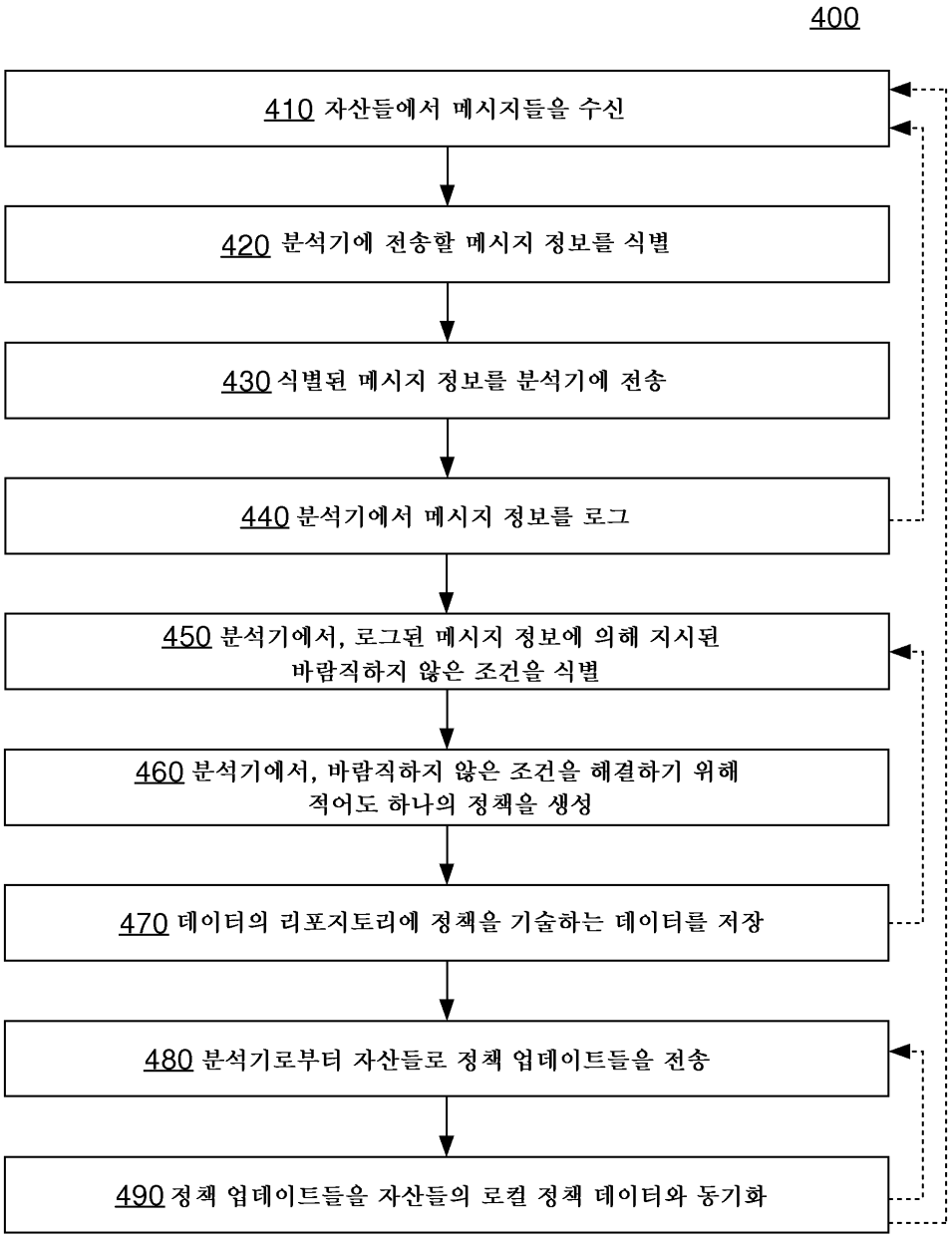
도면2


200
231 영역
221 클러스터
210 자산
210 자산
222 클러스터
210 자산
210 자산
232 영역
223 클러스터
210 자산
210 자산
224 클러스터
210 자산
210 자산
250 분석기
250 분석기
241 중간-계층 컴포넌트들
242 중간-계층 컴포넌트들
255 다-영역 데이터 리포지토리

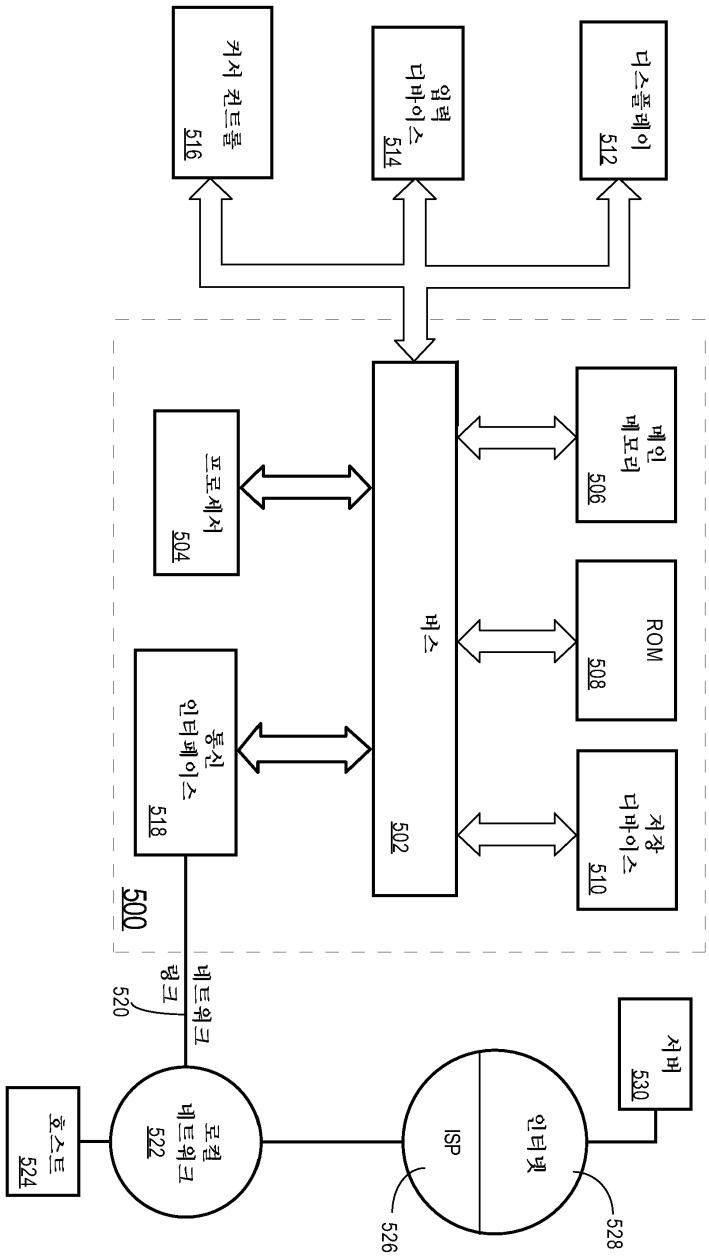
도면3


300
310 클라이언트 디바이스로부터 메시지 수신
320 자산에 대한 로컬 정책 데이터에서, 메시지가 테스트되어야 하는 정책들의 세트 식별
330 정책들에 의해 특정된 하나 이상의 메시지 속성들에 대한 값들을 식별
340 식별된 값들에 기초하여, 정책이 메시지에 적용되는지를 결정
정책이 적용됨
정책이 적용되지 않음
350 정책과 연관된 하나 이상의 정책-기반 액션들을 수행
360 메시지를 정상적인 방식으로 처리하는 것으로 진행할지를 결정
예
아니오
370 메시지 처리 중지
380 메시지를 정상적인 방식으로 처리

도면4


400
410 자산들에서 메시지들을 수신
420 분석기에 전송할 메시지 정보를 식별
430 식별된 메시지 정보를 분석기에 전송
440 분석기에서 메시지 정보를 로그
450 분석기에서, 로그된 메시지 정보에 의해 지시된 바람직하지 않은 조건을 식별
460 분석기에서, 바람직하지 않은 조건을 해결하기 위해 적어도 하나의 정책을 생성
470 데이터의 리포지토리에 정책을 기술하는 데이터를 저장
480 분석기로부터 자산들로 정책 업데이트들을 전송
490 정책 업데이트들을 자산들의 로컬 정책 데이터와 동기화

도면5


커서 컨트롤
516
입력
디바이스
514
디스플레이
512
메인
메모리
506
프로세서
504
버스
502
ROM
508
통신
인터페이스
518
저장
디바이스
510
500
네트워크
링크
520
서버
530
호스트
524
로컬
네트워크
522
ISP
인터넷
526
528