



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0064102
(43) 공개일자 2020년06월05일

- (51) 국제특허분류(Int. Cl.)
H04L 12/715 (2013.01) H04L 12/14 (2006.01)
H04L 12/24 (2006.01) H04L 12/26 (2006.01)
H04L 12/28 (2006.01) H04L 12/46 (2006.01)
H04L 12/721 (2013.01) H04L 12/741 (2013.01)
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
H04L 29/12 (2006.01)
- (52) CPC특허분류
H04L 45/04 (2013.01)
H04L 41/0803 (2013.01)
- (21) 출원번호 10-2020-7012165
- (22) 출원일자(국제) 2018년10월01일
심사청구일자 2020년04월27일
- (85) 번역문제출일자 2020년04월27일
- (86) 국제출원번호 PCT/US2018/053811
- (87) 국제공개번호 WO 2019/070611
국제공개일자 2019년04월11일
- (30) 우선권주장
15/972,086 2018년05월04일 미국(US)
(뒷면에 계속)

- (71) 출원인
브이엠웨어, 인코포레이티드
미국 캘리포니아 94304 팔로 알토 힐뷰 애브뉴 3401
- (72) 발명자
시돈, 이스라엘
미국 94304 캘리포니아주 팔로 알토 힐뷰 애비뉴 3401
- 다르, 첸
이스라엘 5691000 마그쉬뎀 로템 스트리트 4
(뒷면에 계속)
- (74) 대리인
양영준, 김연송, 백만기

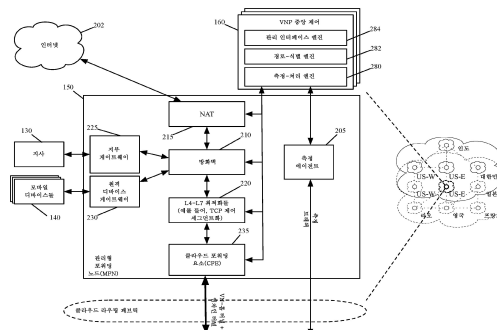
전체 청구항 수 : 총 40 항

(54) 발명의 명칭 복수의 공용 클라우드에 걸쳐 있는 가상 네트워크의 생성

(57) 요약

일부 실시예들은 여러 공용 클라우드 제공자의 여러 공용 클라우드를 통해 및/또는 여러 지역에서 엔티티를 위해 가상 네트워크를 확립한다. 일부 실시예들에서, 가상 네트워크는, 하나 이상의 사설 네트워크(예를 들어, 엔티티의 지부들, 부문들, 부서들 또는 그들의 연관된 데이터센터들 내의 네트워크들), 모바일 사용자들, 및 SaaS(Software as a Service) 제공자 머신들, 및 엔티티의 다른 웹 애플리케이션들을 상호접속하기 위해 여러 공용 클라우드들에 걸쳐 있는 오버레이 네트워크이다. 일부 실시예들에서의 가상 네트워크는, 최상의 종단간 성능, 신뢰성 및 보안을 위해 목적지로의 엔티티의 데이터 메시지의 라우팅을 최적화하면서, 인터넷을 통한 이러한 트래픽의 라우팅을 최소화하려고 시도하도록 구성될 수 있다. 또한, 일부 실시예들에서의 가상 네트워크는 네트워크를 통과하는 데이터 메시지 흐름의 계층 4 처리를 최적화하도록 구성될 수 있다.

대표도



(52) CPC특허분류

H04L 43/0829 (2013.01)
H04L 43/0852 (2013.01)
H04L 43/0888 (2013.01)
H04L 45/12 (2013.01)
H04L 45/14 (2013.01)
H04L 45/64 (2013.01)
H04L 45/745 (2013.01)
H04L 61/1511 (2013.01)
H04L 61/2514 (2013.01)

(72) 발명자

베누고팔, 프라샨스

미국 94304 캘리포니아주 팔로 알토 힐뷰 애비뉴 3401

조하르, 예알

이스라엘 17906 쉘쉬트 피.오. 박스 345

마르쿠제, 알렉스

이스라엘 5252328 라마트 간 에이피 33 비알리크 134

베르그만, 아란

이스라엘 5339513 기바타임 케렌 카예메트 르이스 라엘 44에이

(30) 우선권주장

15/972,083	2018년05월04일	미국(US)
62/566,524	2017년10월02일	미국(US)
15/972,088	2018년05월04일	미국(US)
15/972,090	2018년05월04일	미국(US)
15/972,091	2018년05월04일	미국(US)
15/972,093	2018년05월04일	미국(US)
15/972,095	2018년05월04일	미국(US)
15/972,098	2018년05월04일	미국(US)
15/972,100	2018년05월04일	미국(US)
15/972,102	2018년05월04일	미국(US)
15/972,103	2018년05월04일	미국(US)
15/972,104	2018년05월04일	미국(US)

명세서

청구범위

청구항 1

복수의 공용 클라우드 데이터센터를 통해 가상 네트워크들을 확립하는 방법으로서,

제1 엔티티에 대한 제1 가상 광역 네트워크(wide area network)(WAN)를 구현하기 위해 제1 및 제2 복수-임차인 공용 클라우드 데이터센터들 내의 제1 세트의 포워딩 요소들을 구성하는 단계 - 상기 제1 가상 WAN은 상기 제1 엔티티의 2개 이상의 머신 위치들의 세트에서 동작하는 복수의 머신을 접속함 -; 및

제2 엔티티에 대한 제2 가상 광역 네트워크를 구현하기 위해 제1 및 제2 복수-임차인 공용 클라우드 데이터센터들 내의 제2 세트의 포워딩 요소들을 구성하는 단계 - 상기 제2 가상 WAN은 상기 제2 엔티티의 2개 이상의 머신 위치들의 세트에서 동작하는 복수의 머신을 접속함 -

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 2개 이상의 사무실 위치를 포함하는 방법.

청구항 3

제2항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 적어도 하나의 데이터센터 위치를 더 포함하는 방법.

청구항 4

제3항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 원격 디바이스 위치들을 더 포함하는 방법.

청구항 5

제1항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 사무실 위치 및 데이터센터 위치를 포함하는 방법.

청구항 6

제5항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 SaaS(Software as a Service) 제공자의 복수의 머신을 포함하는 위치를 더 포함하는 방법.

청구항 7

제1항에 있어서, 상기 머신들은 가상 머신들, 컨테이너들, 또는 독립형 컴퓨터들 중 적어도 하나를 포함하는 방법.

청구항 8

제1항에 있어서, 상기 제1 세트의 포워딩 요소들 중의 적어도 서브세트의 포워딩 요소들은 또한 상기 제2 세트의 포워딩 요소들 중에 있는 방법.

청구항 9

제8항에 있어서, 상기 제1 세트의 포워딩 요소들 중의 적어도 또 다른 서브세트의 포워딩 요소들은 상기 제2 세트의 포워딩 요소들 중에 있지 않은 방법.

청구항 10

제1항에 있어서,

상기 제1 세트의 포워딩 요소들을 구성하는 단계는, 상이한 머신 위치들의 제1 엔티티 머신들 사이에서 교환되는 데이터 메시지들을 캡슐화하기 위해 제1 세트의 오버레이 가상 WAN 헤더들을 이용하도록 상기 제1 세트의 포

워딩 요소들을 구성하는 단계를 포함하고;

상기 제2 세트의 포워딩 요소들을 구성하는 단계는, 상이한 머신 위치들의 제2 엔티티 머신들 사이에서 교환되는 데이터 메시지들을 캡슐화하기 위해 제2 세트의 오버레이 가상 WAN 헤더들을 이용하도록 상기 제2 세트의 포워딩 요소들을 구성하는 단계를 포함하며;

상기 제1 세트의 오버레이 가상 WAN 헤더들은 상기 제1 엔티티를 식별하는 제1 엔티티 식별자를 저장하고, 상기 제2 세트의 오버레이 가상 WAN 헤더들은 상기 제2 엔티티를 식별하는 제2 엔티티 식별자를 저장하는 방법.

청구항 11

제10항에 있어서, 상기 제1 및 제2 세트들의 포워딩 요소들은 적어도 하나의 포워딩 요소가 양쪽 세트들의 포워딩 요소들에 있도록 중첩되는 방법.

청구항 12

제1항에 있어서, 상기 제1 및 제2 세트들의 포워딩 요소들의 구성 단계는, 상이한 공용 클라우드 제공자들의 공용 클라우드 데이터센터들을 통해 그리고 상이한 지역들에서, 상이한 엔티티들에 대한 상이한 가상 WAN들을 배치하는 가상 네트워크 제공자의 하나 이상의 제어기의 세트에 의해 수행되는 방법.

청구항 13

제1항에 있어서, 상기 제1 및 제2 세트들의 포워딩 요소들은 컴퓨터들에서 실행되는 복수의 소프트웨어 포워딩 요소를 포함하는 방법.

청구항 14

제1항에 있어서, 상기 제1 및 제2 세트들의 포워딩 요소들은 상기 데이터센터들의 호스트 컴퓨터들에서 실행되는 복수의 소프트웨어 포워딩 요소를 포함하는 방법.

청구항 15

제14항에 있어서, 상기 복수의 소프트웨어 포워딩 요소는 상기 호스트 컴퓨터들에서 실행되는 머신들인 방법.

청구항 16

제15항에 있어서, 상기 복수의 소프트웨어 포워딩 요소를 구현하는 머신들의 적어도 서브세트는 다른 머신들과 함께 호스트 컴퓨터들에서 실행되는 방법.

청구항 17

제15항에 있어서, 상기 복수의 소프트웨어 포워딩 요소를 구현하는 머신들의 적어도 서브세트는 가상 머신들인 방법.

청구항 18

복수의 공용 클라우드 데이터센터를 통해 가상 네트워크들을 확립하기 위한 프로그램을 저장한 비일시적인 머신 판독가능한 매체로서, 적어도 하나의 하드웨어 처리 유닛에 의한 실행을 위한 상기 프로그램은 명령어 세트들을 포함하고, 상기 명령어 세트들은:

제1 엔티티에 대한 제1 가상 광역 네트워크(WAN)를 구현하기 위해 제1 및 제2 복수-임차인 공용 클라우드 데이터센터들 내의 제1 세트의 포워딩 요소들을 구성하는 단계 - 상기 제1 가상 WAN은 상기 제1 엔티티의 2개 이상의 머신 위치들의 세트에서 동작하는 복수의 머신을 접속함 -; 및

제2 엔티티에 대한 제2 가상 광역 네트워크를 구현하기 위해 제1 및 제2 복수-임차인 공용 클라우드 데이터센터들 내의 제2 세트의 포워딩 요소들을 구성하는 단계 - 상기 제2 가상 WAN은 상기 제2 엔티티의 2개 이상의 머신 위치들의 세트에서 동작하는 복수의 머신을 접속함 -

를 위한 것인 비일시적인 머신 판독가능한 매체.

청구항 19

제18항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 적어도 하나의 사무실 위치, 하나의 데이터센터 위치 및 복수의 원격 사용자 위치를 포함하는 비밀시적인 머신 판독가능한 매체.

청구항 20

제19항에 있어서, 상기 제1 엔티티의 머신 위치들의 세트는 SaaS(Software as a Service) 제공자의 복수의 머신을 포함하는 위치를 더 포함하는 비밀시적인 머신 판독가능한 매체.

청구항 21

적어도 2개의 상이한 공용 클라우드 제공자의 적어도 2개의 공용 클라우드 데이터센터를 통해 데이터 메시지 흐름들을 포워딩하는 방법으로서,

제1 공용 클라우드 데이터센터 내의 유입 포워딩 요소(ingress forwarding element)에서:

상기 공용 클라우드 데이터센터들 외부의 제1 외부 머신으로부터, 상기 공용 클라우드 데이터센터들 외부의 제2 외부 머신으로 어드레싱된 데이터 메시지를 수신하는 단계 - 상기 제2 외부 머신은 제2 공용 클라우드 데이터센터에 있는 유출 포워딩 요소(egress forwarding element)를 통해 도달가능함 -;

상기 유입 및 유출 포워딩 요소들에 대한 네트워크 주소들을 소스 및 목적지 주소들로서 포함하는 제1 헤더로 상기 데이터 메시지를 캡슐화하는 단계; 및

소스 및 목적지 네트워크 주소들을, 상기 유입 포워딩 요소의 네트워크 주소, 및 공용 클라우드 데이터센터에 있고 상기 유출 포워딩 요소로의 경로 상의 다음 홉인 다음 홉 포워딩 요소(next hop forwarding element)의 네트워크 주소로서 명시하는 제2 헤더로 상기 데이터 메시지를 캡슐화하는 단계

를 포함하는 방법.

청구항 22

제21항에 있어서, 상기 다음 홉 포워딩 요소는 제3 공용 클라우드 데이터센터에 있는 방법.

청구항 23

제22항에 있어서, 상기 제1, 제2 및 제3 공용 클라우드 데이터센터들은 3개의 상이한 공용 클라우드 제공자에 속하는 방법.

청구항 24

제22항에 있어서, 상기 제1 및 제2 공용 클라우드 데이터센터는 제1 공용 클라우드 제공자에 속하는 반면, 상기 제3 공용 클라우드 데이터센터는 상이한 제2 공용 클라우드 제공자에 속하는 방법.

청구항 25

제22항에 있어서, 상기 제1 및 제2 공용 클라우드 데이터센터들은 상이한 2개의 공용 클라우드 제공자들에 속하는 반면, 상기 제3 공용 클라우드 데이터센터는 상기 제1 공용 클라우드 데이터센터 또는 상기 제2 공용 클라우드 데이터센터의 공용 클라우드 제공자에 속하는 방법.

청구항 26

제22항에 있어서,

상기 다음 홉 포워딩 요소는 제1 다음 홉 포워딩 요소이고,

상기 제1 다음 홉 포워딩 요소는, 상기 경로를 따른 제2 다음 홉 포워딩 요소를 상기 데이터 메시지에 대한 다음 홉으로서 식별하고, 상기 제2 헤더에서, 소스 및 목적지 네트워크 주소들을 상기 제1 다음 홉 포워딩 요소 및 상기 제2 다음 홉 포워딩 요소의 네트워크 주소들로서 명시하는 방법.

청구항 27

제26항에 있어서, 상기 제2 다음 홉 포워딩 요소는 상기 유출 포워딩 요소인 방법.

청구항 28

제27항에 있어서, 상기 캡슐화된 데이터 메시지를 수신한 후, 상기 유출 포워딩 요소는 상기 제1 헤더 내의 상기 목적지 네트워크 주소로부터, 상기 캡슐화된 데이터 메시지가 상기 유출 포워딩 요소에 어드레싱되어 있다고 결정하고, 상기 데이터 메시지에서 상기 제1 및 제2 헤더들을 제거하며, 상기 데이터 메시지를 상기 제2 외부 머신에 포워딩하는 방법.

청구항 29

제26항에 있어서, 상기 제2 다음 홉 포워딩 요소는 상기 제2 포워딩 요소와는 상이한 제4 포워딩 요소인 방법.

청구항 30

제21항에 있어서, 상기 다음 홉 포워딩 요소는 상기 제2 포워딩 요소인 방법.

청구항 31

제21항에 있어서,

상이한 임차인들에 대해 공용 클라우드 데이터센터들을 통한 상이한 가상 네트워크들을 정의하는 가상 네트워크 제공자의 상이한 임차인들에 속하는 데이터 메시지들을 유입 및 유출 포워딩 요소들에서 처리하는 단계; 및

상기 수신된 메시지의 제1 헤더를 캡슐화하는데 있어서, 상기 제1 및 제2 외부 머신들과 연관된 임차인을 식별하는 임차인 식별자를 저장하는 단계

를 더 포함하는 방법.

청구항 32

제31항에 있어서, 상기 제1 및 제2 헤더들을 이용한 상기 데이터 메시지의 캡슐화는, 상기 제1 임차인에 대해, 상기 제1 및 제2 공용 클라우드 데이터센터들을 포함하는 그룹 공용 클라우드 데이터센터들의 네트워크들의 그룹에 걸쳐 있는 오버레이 가상 네트워크(overlay virtual network)를 정의하는 방법.

청구항 33

제32항에 있어서, 상기 임차인들은 회사들이고, 상기 가상 네트워크들은 회사 광역 네트워크(WAN)들인 방법.

청구항 34

제21항에 있어서,

상기 제1 외부 머신은 제1 지사 내의 머신, 사설 제1 데이터센터 내의 머신, 또는 원격 머신 중 하나이고,

상기 제2 외부 머신은 제2 지사 내의 머신 또는 사설 제2 데이터센터 내의 머신인 방법.

청구항 35

엔터티를 위한 가상 네트워크를 확립하기 위한 시스템으로서,

제1 공용 클라우드 제공자에 의해 운영되는 제1 복수-임차인 공용 클라우드 내의 제1 세트의 포워딩 요소들; 및
상기 제1 공용 클라우드 제공자와는 상이한 제2 공용 클라우드 제공자에 의해 운영되는 제2 복수-임차인 공용 클라우드 내의 제2 세트의 포워딩 요소들

을 포함하고,

상기 제1 및 제2 세트의 포워딩 요소들은 가상 네트워크 제공자의 제1 및 제2 임차인들에 대한 제1 및 제2 오버레이 가상 네트워크들을 확립하고, 상기 각각의 오버레이 가상 네트워크는 상기 제1 및 제2 복수-임차인 공용 클라우드들 양쪽 모두에 걸쳐 있으며,

각각의 오버레이 가상 네트워크는 각각의 데이터 메시지를 제1 및 제2 헤더들로 캡슐화함으로써 확립되고, 상기 제1 헤더는 상기 데이터 메시지에 대한 상기 가상 네트워크 내의 유입/유출 인터페이스들을 식별하고, 상기 제2 헤더는 상기 데이터 메시지에 대한 상기 오버레이 네트워크 내의 다음 홉을 식별하는 시스템.

청구항 36

제35항에 있어서, 상기 다음 홉 포워딩 요소는 제3 공용 클라우드 데이터센터에 있는 시스템.

청구항 37

제36항에 있어서, 상기 제1, 제2 및 제3 공용 클라우드 데이터센터들은 3개의 상이한 공용 클라우드 제공자에 속하는 시스템.

청구항 38

제36항에 있어서, 상기 제1 및 제2 공용 클라우드 데이터센터는 제1 공용 클라우드 제공자에 속하는 반면, 상기 제3 공용 클라우드 데이터센터는 상이한 제2 공용 클라우드 제공자에 속하는 시스템.

청구항 39

제36항에 있어서, 상기 제1 및 제2 공용 클라우드 데이터센터들은 상이한 2개의 공용 클라우드 제공자에 속하는 반면, 상기 제3 공용 클라우드 데이터센터는 상기 제1 공용 클라우드 데이터센터 또는 상기 제2 공용 클라우드 데이터센터의 공용 클라우드 제공자에 속하는 시스템.

청구항 40

제36항에 있어서,

상기 다음 홉 포워딩 요소는 제1 다음 홉 포워딩 요소이고,

제1 다음 홉 포워딩 요소는, 상기 경로를 따른 제2 다음 홉 포워딩 요소를 상기 데이터 메시지에 대한 다음 홉 으로서 식별하고, 상기 제2 헤더에서, 소스 및 목적지 네트워크 주소들을 상기 제1 다음 홉 포워딩 요소 및 상기 제2 다음 홉 포워딩 요소의 네트워크 주소들로서 명시하는 시스템.

발명의 설명

기술 분야

배경 기술

- [0001] 오늘날 회사 기업 네트워크(corporate enterprise network)는 회사의 상이한 사무실들과 부서들을 보안 접속하는 통신 백본(communication backbone)이다. 이 네트워크는 전형적으로, (1) 지사(branch office) 및 지역 캠퍼스의 사용자들, (2) 비즈니스 애플리케이션, 인터넷, 및 그들의 대응하는 데이터를 호스팅하는 회사 데이터 센터들, 및 (3) 회사 방화벽 및 DMZ(demilitarized zone; 비무장 지대)를 통해 글로벌 인터넷을 접속하는 광역 네트워크(WAN)이다. 기업 네트워크는, Frame Relay 및 MPLS(multiprotocol label switching) 등의, 고가의 임대 회선에 의해 상호접속된 스위치, 라우터, 및 미들박스 기기들 등의 전문화된 하드웨어를 포함한다.
- [0002] 지난 몇 년간, 회사들이 통신 서비스를 제공하고 소비하는 방식에 있어서 패러다임 전환이 있었다. 첫째, 이동성 혁명은, 사용자가, 모바일 디바이스를 이용하여, 대개는 스마트폰을 이용하여, 언제 어디서나 서비스에 액세스하는 것을 허용했다. 이러한 사용자들은 공용 인터넷 및 셀룰러 네트워크를 통해 비즈니스 서비스에 액세스한다. 동시에, 제3자 SaaS(Software as a Service) 벤더(예를 들어, Salesforce, Workday, Zendesk)는, 기존의 온-프레미스 애플리케이션(on-premise application)을 대체한 반면, 사실 데이터센터에서 호스팅되는 다른 애플리케이션들은 공용 클라우드로 재배치되었다. 이 트래픽은 여전히 기업 네트워크 내에서 운반되지만, 트래픽의 상당 부분은 회사 네트워크 경계 외부에서 시작되고 종료되며, 회사 네트워크뿐만 아니라 공용 인터넷 양쪽 모두를 통과해야 한다(한번 또는 2번). 최근의 연구에 따르면, 회사 네트워크들의 40%가 백홀링된 트래픽(즉, 회사 네트워크에서 관찰된 인터넷 트래픽)의 비율이 80% 이상인 것으로 나타났다. 이것은, 대부분의 회사 트래픽이 고가의 임대 회선과 소비자 인터넷 양쪽 모두를 통해 운반된다는 것을 의미한다.
- [0003] 소비자-중심의 서비스로서, 인터넷 자체는 비즈니스 트래픽에 대해서는 좋지 않은 매체이다. 인터넷은, 중요한 비즈니스 애플리케이션이 기대하는 신뢰성, QoS(서비스 품질) 보장 및 보안이 결여되어 있다. 또한, 계속 증가하는 소비자 트래픽 수요, 순-중립성 규정 및 주요 업체(예를 들어, Netflix, Google, 공용 클라우드)의 인터넷

바이패스의 생성은, 트래픽 단위당 수익률을 저하시켰다. 이러한 추세는, 소비자의 수요를 신속하게 따라잡고 적절한 비즈니스 서비스를 제공하기 위한 서비스 제공자의 동기부여를 감소시켰다.

[0004] 공용 클라우드의 성장에 따라, 회사들은 그들의 더 많은 컴퓨팅 인프라스트럭처를 공용 클라우드 데이터센터로 이전시키고 있다. 공용 클라우드 제공자들은, 컴퓨팅 및 네트워킹 인프라스트럭처 투자의 선두에 서 있다. 이들 클라우드 서비스는 전 세계에 많은 데이터센터를 구축했으며, Azure, AWS, IBM 및 Google은 2016 년에 각각 전세계 38, 16, 25 및 14개 지역들로 확장되었다. 각각의 공용 클라우드 제공자는, 잠수함에 의해 배치된 다크 파이버(dark fiber) 및 해저 케이블을 채용하는 고가의 고속 네트워크를 이용함으로써 자체 데이터센터들을 상호접속했다.

[0005] 오늘날, 이들 변화에도 불구하고, 회사 네트워크 정책은, 종종, 모든 회사 트래픽이 보안 WAN 게이트웨이를 통과하도록 강제한다. 사용자들이 모바일화되고 애플리케이션들이 SaaS 및 공용 클라우드로 이전됨에 따라, 회사 WAN은 모든 회사 통신을 느려지게 하는 비용이 많이 드는 우회로가 된다. 대부분의 회사 WAN의 트래픽은 인터넷으로부터 제공되거나 인터넷으로 전송된다. 인터넷을 통해 이 트래픽을 전송하는 대안적인 보안 솔루션들은 그들의 불량하고 신뢰할 수 없는 성능 때문에 적절하지 않다.

발명의 내용

[0006] 일부 실시예들은, 하나 이상의 지역(예를 들어, 여러 도시, 주, 국가 등)에서 하나 이상의 공용 클라우드 제공자의 여러 공용 클라우드 데이터센터를 통해 가상 네트워크를 엔티티를 위해 확립한다. 이러한 가상 네트워크가 확립될 수 있는 엔티티의 예는, 비즈니스 엔티티(예를 들어, 회사), 비영리 엔티티(예를 들어, 병원, 연구기관 등) 및 교육 엔티티(예를 들어, 종합 대학, 단과 대학 등) 또는 기타 임의의 유형의 엔티티를 포함한다. 공용 클라우드 제공자의 예는, AWS(Amazon Web Services), Google Cloud Platform(GCP), Microsoft Azure 등을 포함한다.

[0007] 일부 실시예들에서, 고속의 신뢰성있는 사설 네트워크는 2개 이상의 공용 클라우드 데이터센터(공용 클라우드)를 상호접속한다. 일부 실시예들은, 가상 네트워크를, 하나 이상의 사설 네트워크(예를 들어, 엔티티의 지부들, 부문들, 부서들 또는 그들의 연관된 데이터센터들 내의 네트워크), 모바일 사용자, SaaS(Software as a Service) 제공자 머신, 공용 클라우드(들) 내의 머신 및/또는 서비스, 및 기타의 웹 애플리케이션을 상호접속하기 위해 여러 공용 클라우드에 걸쳐 있는 오버레이 네트워크로서 정의한다.

[0008] 일부 실시예들에서의 가상 네트워크는, 최상의 종단간 성능, 신뢰성 및 보안을 위해 목적지로의 엔티티의 데이터 메시지의 라우팅을 최적화하면서, 인터넷을 통한 이러한 트래픽의 라우팅을 최소화하려고 시도하도록 구성될 수 있다. 또한, 일부 실시예들에서의 가상 네트워크는, 네트워크를 통과하는 데이터 메시지 흐름의 계층 4 처리를 최적화하도록 구성될 수 있다. 예를 들어, 일부 실시예들에서, 가상 네트워크는 레이트 제어 메커니즘을 접속 경로에 걸쳐 분할함으로써 TCP(Transport Control Protocol) 접속의 종단간 레이트를 최적화한다.

[0009] 일부 실시예들은 여러 공용 클라우드에 배치된 여러 컴포넌트를 구성함으로써 가상 네트워크를 확립한다. 이들 컴포넌트들은, 일부 실시예들에서 소프트웨어-기반의 측정 에이전트, 소프트웨어 포워딩 요소들(예를 들어, 소프트웨어 라우터, 스위치, 게이트웨이 등), 계층-4 접속 프록시 및 미들박스 서비스 머신(예를 들어, 기기, VM, 컨테이너 등)를 포함한다. 일부 실시예들에서의 이들 컴포넌트들 중 하나 이상은, Open vSwitch, OpenVPN, strong Swan 및 Ryu 등의, 표준화되거나 흔하게 이용가능한 솔루션을 이용한다.

[0010] 일부 실시예들은, 여러 공용 클라우드에 걸쳐 가상 네트워크를 구현하도록 공용-클라우드 컴포넌트들을 구성하는 논리적으로 중앙 집중형의 제어기 클러스터(예를 들어, 한 세트의 하나 이상의 제어기 서버들)를 이용한다. 일부 실시예들에서, 이 클러스터 내의 제어기들은, 리던던시 및 높은 가용성을 향상시키기 위해 다양한 상이한 위치들에 있다(예를 들어, 상이한 공용 클라우드 데이터센터들에 있다). 일부 실시예들에서의 제어기 클러스터는, 가상 네트워크를 확립하는데 이용되는 공용 클라우드 컴포넌트들의 수, 또는 이들 컴포넌트에 할당된 컴퓨팅 또는 네트워크 자원들의 수를 확장 또는 축소한다.

[0011] 일부 실시예들은, 동일한 공용 클라우드 제공자들의 동일한 세트의 공용 클라우드들을 통해 및/또는 동일하거나 상이한 공용 클라우드 제공자들의 상이한 세트들의 공용 클라우드들을 통해 상이한 엔티티들에 대해 상이한 가상 네트워크들을 확립한다. 일부 실시예들에서, 가상 네트워크 제공자는, 상이한 임차인들이 동일하거나 상이한 공용 클라우드를 통해 상이한 가상 네트워크를 정의하는 것을 허용하는 소프트웨어 및 서비스를 제공한다. 일부 실시예들에서, 동일한 제어기 클러스터 또는 상이한 제어기 클러스터들은, 여러 상이한 엔티티들에 대해 동일하거나 상이한 세트들의 공용 클라우드들을 통해 상이한 가상 네트워크들을 구현하도록 공용 클라우드 컴포

넛트들을 구성하는데 이용될 수 있다.

[0012] 하나 이상의 공용 클라우드를 통해 임차인에 대한 가상 네트워크를 배치하기 위해, 제어기 클러스터는, (1) 임차인의 지사, 데이터센터, 모바일 사용자, 및 SaaS 제공자의 위치에 기초하여 임차인에 대한 가상 네트워크에 출입하기 위한 가능한 유입 및 유출 라우터들을 식별하고, (2) 가상 네트워크를 구현하는 다른 중간 공용 클라우드 라우터를 통해 식별된 유입 라우터들로부터 식별된 유출 라우터들로 횡단하는 경로들을 식별한다. 이들 경로들을 식별한 후, 제어기 클러스터는 이들 경로들을 공용 클라우드(들) 내의 가상 네트워크 라우터들의 포워딩 테이블들에 전파한다. OVS-기반의 가상 네트워크 라우터를 이용하는 실시예들에서, 제어기는 OpenFlow를 이용함으로써 경로들을 분산시킨다.

[0013] 전술된 요약은, 본 발명의 일부 실시예들에 대한 간략한 소개로서 역할하도록 의도되었다. 전술된 요약은, 본 문서에 개시된 모든 본 발명의 주제의 소개 또는 개요를 의미하는 것은 아니다. 이하의 상세한 설명 및 상세한 설명에서 참조되는 도면들은, 요약에서 설명된 실시예들뿐만 아니라 다른 실시예들도 추가로 설명할 것이다. 따라서, 본 문서에 설명된 모든 실시예들을 이해하기 위해, 요약, 상세한 설명, 도면 및 청구항들에 대한 완전한 검토가 필요하다. 더욱이, 청구된 주제는, 요약, 상세한 설명 및 도면의 예시적인 상세사항에 의해 제한되지 않아야 한다.

도면의 간단한 설명

[0014] 본 발명의 신규한 피처들은 첨부된 청구항들에 개시되어 있다. 그러나, 설명의 목적을 위해, 본 발명의 여러 실시예들이 아래의 도면들에 개시된다.

도 1a는 2개의 공용 클라우드 제공자들의 여러 공용 클라우드 데이터센터들을 통해 회사에 대해 정의된 가상 네트워크를 제시한다.

도 1b는 공용 클라우드들을 통해 배치된 2개의 회사 임차인들에 대한 2개의 가상 네트워크의 한 예를 나타낸다.

도 1c는 2개의 가상 네트워크의 한 예를 대안적으로 나타내며, 여기서, 하나의 네트워크는 공용 클라우드들을 통해 배치되고 다른 가상 네트워크는 또 다른 쌍의 공용 클라우드들을 통해 배치된다.

도 2는 본 발명의 일부 실시예들의 관리형 포워딩 노드 및 제어기 클러스터의 한 예를 나타낸다.

도 3은 일부 실시예들에서 제어기 측정-처리 계층이 생성하는 측정 그래프의 한 예를 나타낸다.

도 4a는 일부 실시예들에서 제어기 경로-식별 계층이 측정 그래프로부터 생성하는 라우팅 그래프의 한 예를 나타낸다.

도 4b는 2개의 SaaS 제공자들의 데이터센터들에 가장 가까운 데이터센터들에 있는 라우팅 그래프 내의 2개의 노드에 이들 2개의 SaaS 제공자에 대한 알려진 IP를 추가하는 한 예를 나타낸다.

도 4c는 2개의 SaaS 제공자를 나타내는 2개의 노드를 추가함으로써 생성되는 라우팅 그래프를 나타낸다.

도 4d는 2개의 공용 클라우드에 각각 접속된 알려진 IP 주소를 가진 지사와 데이터센터를 나타내도록 추가 노드가 추가되어 있는 라우팅 그래프를 나타낸다.

도 5는 제어기 경로-식별 계층이 제어기 측정 계층으로부터 수신된 측정 그래프로부터 라우팅 그래프를 생성하기 위해 이용하는 프로세스를 나타낸다.

도 6은 일부 실시예들의 IPsec 데이터 메시지 포맷을 나타낸다.

도 7은 일부 실시예들의 2개의 캡슐화 헤더의 한 예를 나타내는 반면, 도 8은 일부 실시예들에서 이들 2개의 헤더가 어떻게 이용되는지를 나타내는 한 예를 제시한다.

도 9 내지 도 11은, 유입, 중간 및 유출 MFN들이 2개의 상이한 지사에 있는 2개의 컴퓨팅 디바이스들 사이에서 전송되는 메시지를 수신할 때 이들 MFN들에 의해 각각 수행되는 메시지-처리 프로세스를 나타낸다.

도 12는 유입 및 유출 MFN들 사이에 중간 MFN을 포함하지 않는 한 예를 나타낸다.

도 13은 유입 MFN의 CFE가 지사 내의 회사 컴퓨팅 디바이스로부터 또 다른 지사 내의 또는 SaaS 제공자 데이터센터 내의 또 다른 디바이스에 전송되는 메시지를 수신할 때 그 CFE에 의해 수행되는 메시지-처리 프로세스를 나타낸다.

도 14는 유출 라우터에서 수행되는 NAT 동작을 나타낸다.

도 15는 SaaS 제공자 머신으로부터 임차인 머신으로 전송되는 메시지를 수신하는 유입 라우터에 의해 수행되는 메시지-처리 프로세스를 나타낸다.

도 16은 인터넷으로의 가상 네트워크의 유출 경로 상에 있는 각각의 가상-네트워크 게이트웨이에 배치된 TM 엔진을 나타낸다.

도 17은 도 16에 나타낸 단일 NAT 접근법 대신에 일부 실시예들에서 이용되는 이중-NAT 접근법을 나타낸다.

도 18은 유입 NAT 엔진의 소스 포트 변환을 나타내는 한 예를 제시한다.

도 19는 도 18의 데이터 메시지의 처리에 대한 응답으로서 SaaS 머신이 전송하는 응답 메시지의 처리를 나타낸다.

도 20은 하나 이상의 공용 클라우드 제공자의 N개 공용 클라우드에서 네트워크 인프라스트럭처와 제어기 클러스터(들)를 갖는 가상 네트워크 제공자의 M개의 임차인에 대한 M개의 가상 회사 WAN을 보여주는 한 예를 제시한다.

도 21은 특정한 임차인에 대한 가상 WAN을 배치하고 관리하기 위해 가상 네트워크 제공자의 제어기 클러스터에 의해 수행되는 한 프로세스를 개념적으로 나타낸다.

도 22는 본 발명의 일부 실시예들에서 구현되는 컴퓨터 시스템을 개념적으로 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0015] 본 발명의 이하의 상세한 설명에서, 본 발명의 수 많은 상세사항, 예, 및 실시예가 개시되고 설명된다. 그러나, 본 발명은 개시된 실시예들로 제한되지 않으며 본 발명은 논의된 특정한 상세사항들 및 예들의 일부 없이도 실시될 수 있다는 것이 본 기술분야의 통상의 기술자에게 명백하고 뚜렷할 것이다.
- [0016] 일부 실시예들은, 하나 이상의 지역(예를 들어, 여러 도시, 주, 국가 등)에서 하나 이상의 공용 클라우드 제공자의 여러 공용 클라우드 데이터센터를 통해 가상 네트워크를 엔티티를 위해 확립한다. 이러한 가상 네트워크가 확립될 수 있는 엔티티의 예는, 비즈니스 엔티티(예를 들어, 회사), 비영리 엔티티(예를 들어, 병원, 연구 기관 등) 및 교육 엔티티(예를 들어, 종합 대학, 단과 대학 등) 또는 기타 임의의 유형의 엔티티를 포함한다. 공용 클라우드 제공자의 예는, AWS(Amazon Web Services), Google Cloud Platform(GCP), Microsoft Azure 등을 포함한다.
- [0017] 일부 실시예들은, 가상 네트워크를, 하나 이상의 사설 네트워크(예를 들어, 엔티티의 지부들, 부문들, 부서들 또는 그들의 연관된 데이터센터들 내의 네트워크), 모바일 사용자, SaaS(Software as a Service) 제공자 머신, 공용 클라우드(들) 내의 머신 및/또는 서비스, 및 기타의 웹 애플리케이션을 상호접속하기 위해 여러 공용 클라우드 데이터센터(공용 클라우드)에 걸쳐 있는 오버레이 네트워크로서 정의한다. 일부 실시예들에서, 고속의 신뢰성있는 사설 네트워크는 2개 이상의 공용 클라우드 데이터센터를 상호접속한다.
- [0018] 일부 실시예들에서의 가상 네트워크는, 최상의 종단간 성능, 신뢰성 및 보안을 위해 목적지로의 엔티티의 데이터 메시지의 라우팅을 최적화하면서, 인터넷을 통한 이러한 트래픽의 라우팅을 최소화하려고 시도하도록 구성될 수 있다. 또한, 일부 실시예들에서의 가상 네트워크는, 네트워크를 통과하는 데이터 메시지 흐름의 계층 4 처리를 최적화하도록 구성될 수 있다. 예를 들어, 일부 실시예들에서, 가상 네트워크는 레이트 제어 메커니즘을 접속 경로에 걸쳐 분할함으로써 TCP(Transport Control Protocol) 접속의 종단간 레이트를 최적화한다.
- [0019] 일부 실시예들은 여러 공용 클라우드에 배치된 여러 컴포넌트를 구성함으로써 가상 네트워크를 확립한다. 이들 컴포넌트들은, 일부 실시예들에서 소프트웨어-기반의 측정 에이전트, 소프트웨어 포워딩 요소들(예를 들어, 소프트웨어 라우터, 스위치, 게이트웨이 등), 계층-4 접속 프로시 및 미들박스 서비스 머신(예를 들어, 기기, VM, 컨테이너 등)를 포함한다.
- [0020] 일부 실시예들은, 여러 공용 클라우드에 걸쳐 가상 네트워크를 구현하도록 공용-클라우드 컴포넌트들을 구성하는 논리적으로 중앙 집중형의 제어기 클러스터(예를 들어, 한 세트의 하나 이상의 제어기 서버들)를 이용한다. 일부 실시예들에서, 이 클러스터 내의 제어기들은, 리던던시 및 높은 가용성을 향상시키기 위해 다양한 상이한 위치들에 있다(예를 들어, 상이한 공용 클라우드 데이터센터들에 있다). 제어기 클러스터 내의 상이한 제어기들이 상이한 공용 클라우드 데이터센터들에 위치할 때, 일부 실시예들에서의 제어기들은 그들의 상태(예를

들어, 임차인을 식별하기 위해 그들이 생성하는 구성 데이터, 가상 네트워크를 통한 경로 등)를 공유한다. 일부 실시예들에서의 제어기 클러스터는, 가상 네트워크를 확립하는데 이용되는 공용 클라우드 컴포넌트들의 수, 또는 이들 컴포넌트에 할당된 컴퓨팅 또는 네트워크 자원들의 수를 확장 또는 축소한다.

[0021] 일부 실시예들은, 동일한 공용 클라우드 제공자들의 동일한 세트의 공용 클라우드들을 통해 및/또는 동일하거나 상이한 공용 클라우드 제공자들의 상이한 세트들의 공용 클라우드들을 통해 상이한 엔티티들에 대해 상이한 가상 네트워크들을 확립한다. 일부 실시예들에서, 가상 네트워크 제공자는, 상이한 임차인들이 동일하거나 상이한 공용 클라우드를 통해 상이한 가상 네트워크를 정의하는 것을 허용하는 소프트웨어 및 서비스를 제공한다. 일부 실시예들에서, 동일한 제어기 클러스터 또는 상이한 제어기 클러스터들은, 여러 상이한 엔티티들에 대해 동일하거나 상이한 세트들의 공용 클라우드들을 통해 상이한 가상 네트워크들을 구현하도록 공용 클라우드 컴포넌트들을 구성하는데 이용될 수 있다.

[0022] 아래의 논의에서 회사 가상 네트워크의 몇 가지 예가 제공된다. 그러나, 본 기술분야의 통상의 기술자라면, 일부 실시예들은, 다른 비즈니스 엔티티, 비영리 조직, 교육 엔티티 등의 다른 유형들의 엔티티에 대한 가상 네트워크를 정의한다는 것을 깨달을 것이다. 또한, 본 문서에서 사용될 때, 데이터 메시지만 네트워크를 통해 전송되는 특정한 포맷의 비트들의 모음을 말한다. 본 기술분야의 통상의 기술자라면, 데이터 메시지라는 용어는, 본 문서에서는 네트워크를 통해 전송되는 다양한 포맷화된 비트들의 모음을 지칭하기 위해 사용된다는 것을 인식할 것이다. 이들 비트의 포맷은 표준화된 프로토콜 또는 비표준화된 프로토콜에 의해 명시될 수 있다. 표준화된 프로토콜을 따르는 데이터 메시지의 예로는, 이더넷 프레임, IP 패킷, TCP 세그먼트, UDP 데이터그램 등이 포함된다. 또한, 본 문서에서 사용될 때, L2, L3, L4 및 L7 계층(또는 계층 2, 계층 3, 계층 4, 및 계층 7)에 대한 참조는, 각각, OSI(Open System Interconnection) 계층 모델의 제2 데이터 링크 계층, 제3 네트워크 계층, 제4 트랜스포트 계층, 및 제7 애플리케이션 계층에 대한 참조이다.

[0023] 도 1a는, 2개의 공용 클라우드 제공자 A 및 B의 여러 공용 클라우드 데이터센터(105 및 110)를 통해 회사에 대해 정의된 가상 네트워크(100)를 제시한다. 도시된 바와 같이, 가상 네트워크(100)는, 상이한 공용 클라우드들에 상이한 관리형 포워딩 노드(150)들을 배치하고 관리형 포워딩 노드(MFN)들을 오버레이 터널(152)을 통해 서로 접속함으로써 확립되는 보안 오버레이 네트워크이다. 일부 실시예들에서, MFN은, 다른 공용 클라우드 데이터센터의 (다른 컴포넌트들의 그룹을 갖는) 다른 MFN과 함께 하나 이상의 엔티티에 대한 하나 이상의 오버레이 가상 네트워크를 확립하는 공용 클라우드 데이터센터 내의 여러 상이한 컴포넌트들의 개념적 그룹이다.

[0024] 아래에서 더 설명되는 바와 같이, MFN을 형성하는 컴포넌트들의 그룹은, 일부 실시예들에서, (1) 공용 클라우드 데이터센터 바깥의 외부 머신 위치들인 엔티티의 컴퓨팅 노드(예를 들어, 사무실, 사설 데이터센터, 원격 사용자 등)와 VPN 접속을 확립하기 위한 하나 이상의 VPN 게이트웨이, (2) 공유된 공용 클라우드 네트워크 패브릭을 통해 오버레이 가상 네트워크를 정의하기 위해 서로간에 캡슐화된 데이터 메시지를 포워딩하기 위한 하나 이상의 포워딩 요소, (3) L4-L7 최적화뿐만 아니라 미들박스 서비스 동작을 수행하기 위한 하나 이상의 서비스 머신, 및 (4) 공용 클라우드 데이터센터들을 통한 원하는 경로를 식별하기 위해 공용 클라우드 데이터센터들 사이의 네트워크 접속 품질에 관한 측정을 획득하기 위한 하나 이상의 측정 에이전트를 포함한다. 일부 실시예들에서, 상이한 MFN들은 상이한 배치들 및 상이한 개수의 이러한 컴포넌트들을 가질 수 있고, 하나의 MFN은 리던던시 및 확장성의 이유로 상이한 개수의 이러한 컴포넌트들을 가질 수 있다.

[0025] 또한, 일부 실시예들에서, 각각의 MFN의 컴포넌트들의 그룹은 MFN의 공용 클라우드 데이터센터 내의 상이한 컴퓨터들에서 실행된다. 일부 실시예들에서, MFN의 컴포넌트들 중 수개 또는 전부는 공용 클라우드 데이터센터의 한 컴퓨터에서 실행될 수 있다. 일부 실시예들에서의 MFN의 컴포넌트들은, 다른 임차인들의 다른 머신들을 실행시키는 호스트 컴퓨터에서 실행된다. 이들 다른 머신들은 다른 임차인들의 다른 MFN들의 다른 머신들이거나, 다른 임차인들의 관련이없는 머신들(예를 들어, 컴퓨팅 VM 또는 컨테이너)일 수 있다.

[0026] 일부 실시예들에서의 가상 네트워크(100)는, 상이한 엔티티들(예를 들어, 가상 네트워크 제공자의 상이한 회사 고객들/임차인들)에 대해 동일하거나 상이한 공용 클라우드 데이터센터들을 통해 상이한 가상 네트워크를 배치하는 가상 네트워크 제공자(VNP)에 의해 배치된다. 일부 실시예들에서의 가상 네트워크 제공자는, MFN들을 배치하고 이들 MFN을 구성 및 관리하기 위한 제어기 클러스터를 제공하는 엔티티이다.

[0027] 가상 네트워크(100)는, (데이터센터들, 지사들 및 모바일 사용자들 등의) 회사 컴퓨팅 엔드포인트들을 서로 및 공용 클라우드에 상주하거나 인터넷을 통해 액세스가능한 사설 데이터센터에 상주하는 외부 서비스(예를 들어, 공용 웹 서비스, 또는 Office365 또는 Salesforce 등의 SaaS 서비스)에 접속한다. 이 가상 네트워크는 상이한 공용 클라우드들의 상이한 위치들을 활용하여 상이한 회사 컴퓨팅 엔드포인트들(예를 들어, 상이한 사설 네트워

크들 및/또는 회사의 상이한 모바일 사용자들)을 부근의 공용 클라우드에 접속한다. 회사 컴퓨팅 엔드포인트는 아래의 논의에서 회사 컴퓨팅 노드라고도 한다.

[0028] 일부 실시예들에서, 가상 네트워크(100)는 또한, 이들 공용 클라우드를 상호접속하는 고속 네트워크를 활용하여 공용 클라우드를 통해 그들의 목적지로 데이터 메시지를 포워딩하거나 인터넷을 통한 그들의 통화를 감소시키면서 그들의 목적지에 접근하게 된다. 회사 컴퓨팅 엔드포인트들이, 가상 네트워크가 걸쳐 있는 공용 클라우드 데이터센터 외부에 있을 때, 이들 엔드포인트들은 외부 머신 위치라고 한다. 회사 지사, 사설 데이터센터 및 원격 사용자의 디바이스가 여기에 해당된다.

[0029] 도 1a에 도시된 예에서, 가상 네트워크(100)는 공용 클라우드 제공자 A의 6개의 데이터센터(105a-105f) 및 공용 클라우드 제공자 B의 4개의 데이터센터(110a-110d)에 걸쳐있다. 이들 공용 클라우드에 걸쳐서, 이 가상 네트워크는, 상이한 지리적 영역들에 위치한 여러 지사들, 회사 데이터센터들, SaaS 제공자들 및 회사 임차인의 모바일 사용자들을 접속한다. 구체적으로, 가상 네트워크(100)는, 2개의 상이한 도시들(예를 들어, 캘리포니아주 샌프란시스코, 및 인도의 푸네) 내의 2개의 지사(130a 및 130b), 또 다른 도시(예를 들어, 워싱턴주 시애틀) 내의 회사 데이터센터(134), 또 다른 2개의 도시들(와싱턴주 레드몬드, 및 프랑스 파리) 내의 2개의 SaaS 제공자 데이터센터들(136a 및 136b), 및 전세계의 다양한 위치들에 있는 모바일 사용자(140)들을 접속한다. 따라서, 이 가상 네트워크는 가상 회사 WAN으로 간주될 수 있다.

[0030] 일부 실시예들에서, 지사들(130a 및 130b)은, 공용 클라우드 외부에 있는 지부 위치(branch location)들 및 지부 사설 데이터센터들에 있는 컴퓨터들을 접속하는 그들 자신의 사설 네트워크들(예를 들어, 근거리 통신망)을 갖는다. 유사하게, 일부 실시예들에서의 회사 데이터센터(134)는 그 자신의 사설 네트워크를 가지며 임의의 공용 클라우드 데이터센터 외부에 상주한다. 그러나, 다른 실시예들에서, 회사 데이터센터(134) 또는 지사(130a 및 130b)의 데이터센터는 공용 클라우드 내에 있을 수 있지만, 회사 또는 지부 데이터센터가 가상 네트워크(100)의 엣지에 접속되기 때문에, 가상 네트워크는 이 공용 클라우드까지 이르지 않는다.

[0031] 위에서 언급된 바와 같이, 가상 네트워크(100)는, 상이한 공용 클라우드들 내의 상이한 배치된 관리형 포워딩 노드(150)들을 오버레이 터널(152)을 통해 접속함으로써 확립된다. 각각의 관리형 포워딩 노드(150)는 여러 구성가능한 컴포넌트를 포함한다. 전술되고 후술되는 바와 같이, MFN 컴포넌트들은, 일부 실시예들에서 소프트웨어-기반의 측정 에이전트, 소프트웨어 포워딩 요소(예를 들어, 소프트웨어 라우터, 스위치, 게이트웨이 등), 계층 4 프록시(예를 들어, TCP 프록시) 및 미들박스 서비스 머신(예를 들어, VM, 컨테이너 등)을 포함한다. 일부 실시예들에서의 이들 컴포넌트들 중 하나 이상은, Open vSwitch, OpenVPN, strongSwan 등의 표준화되거나 흔하게 이용가능한 솔루션을 이용한다.

[0032] 일부 실시예들에서, 각각의 MFN(즉, MFN을 개념적으로 형성하는 컴포넌트들의 그룹)은, 공용 클라우드 데이터센터에 MFN들을 배치하고 구성하는 가상 네트워크 제공자의 상이한 임차인들에 의해 공유될 수 있다. 결합적으로 또는 대안으로서, 일부 실시예들에서의 가상 네트워크 제공자는 특정한 임차인을 위해 하나 이상의 공용 클라우드 데이터센터에 고유한 세트의 MFN들을 배치할 수 있다. 예를 들어, 특정한 임차인은, 보안 상의 이유로 또는 서비스 품질의 이유로 MFN 자원을 또 다른 임차인과 공유하기를 원하지 않을 수 있다. 이러한 임차인의 경우 가상 네트워크 제공자는 여러 공용 클라우드 데이터센터들에 걸쳐 그 자신의 MFN 세트를 배치할 수 있다.

[0033] 일부 실시예들에서, 논리적으로 중앙 집중형의 제어기 클러스터(160)(예를 들어, 한 세트의 하나 이상의 제어기 서버들)는 공용 클라우드들(105 및 110) 중 하나 이상의 내부 또는 외부에서 동작하고, 공용 클라우드(105 및 110)를 통해 가상 네트워크를 구현하도록 관리형 포워딩 노드(150)의 공용-클라우드 컴포넌트들을 구성한다. 일부 실시예들에서, 이 클러스터 내의 제어기들은, 리던던시 및 높은 가용성을 향상시키기 위해 다양한 상이한 위치들에 있다(예를 들어, 상이한 공용 클라우드 데이터센터들에 있다). 일부 실시예들에서의 제어기 클러스터는, 가상 네트워크를 확립하는데 이용되는 공용 클라우드 컴포넌트들의 수, 또는 이들 컴포넌트에 할당된 컴퓨팅 또는 네트워크 자원들의 수를 확장 또는 축소한다.

[0034] 일부 실시예들에서, 제어기 클러스터(160), 또는 가상 네트워크 제공자의 또 다른 제어기 클러스터는, 동일한 공용 클라우드(105 및 110)를 통해 및/또는 상이한 공용 클라우드 제공자들의 상이한 공용 클라우드들을 통해 또 다른 회사 임차인을 위한 상이한 가상 네트워크를 확립한다. 제어기 클러스터(들)에 추가하여, 다른 실시예들에서의 가상 네트워크 제공자는, 공용 클라우드에 포워딩 요소들 및 서비스 머신들을 배치하여 상이한 임차인들이 동일하거나 상이한 공용 클라우드들을 통해 상이한 가상 네트워크들을 배치하는 것을 허용한다. 도 1b는 공용 클라우드(105 및 110)를 통해 배치된 2개의 회사 임차인에 대한 2개의 가상 네트워크(100 및 180)의 한 예를 나타낸다. 도 1c는 2개의 가상 네트워크(100 및 182)의 한 예를 대안으로서 도시하며, 여기서, 하나의 네트

워크(100)는 공용 클라우드(105 및 110)를 통해 배치되고 다른 가상 네트워크(182)는 또 다른 쌍의 공용 클라우드(110 및 115)를 통해 배치된다.

[0035] MFN의 구성된 컴포넌트들을 통해, 도 1a의 가상 네트워크(100)는, 회사 임차인의 상이한 사설 네트워크 및/또는 상이한 모바일 사용자들이 이들 사설 네트워크 및/또는 모바일 사용자에게 관해 (예를 들어, 물리적 거리의 측면에서, 접속 속도, 손실, 지연 및/또는 비용의 측면에서, 및/또는 네트워크 접속 신뢰성 등의 측면에서 측정될 때) 최적의 위치에 있는 상이한 공용 클라우드들에 접속하는 것을 허용한다. 이들 컴포넌트들은 또한, 일부 실시예들에서의 가상 네트워크(100)가 공용 클라우드들을 상호접속하는 고속 네트워크를 이용하여 공용 클라우드를 통해 데이터 메시지를 목적으로 포워딩하면서 인터넷을 통한 통과를 감소시키는 것을 허용한다.

[0036] 일부 실시예들에서, MFN 컴포넌트들은 또한, 중단간 성능, 신뢰성 및 보안을 최적화하기 위해 네트워크, 트랜스포트 및 애플리케이션 계층들에서 새로운 프로세스를 실행하도록 구성된다. 일부 실시예들에서, 이들 프로세스들 중 하나 이상은, 현재 네트워크 프로토콜 골화(protocol ossification)가 없는, 전용 고성능 네트워킹 프로토콜을 구현한다. 따라서, 일부 실시예들에서의 가상 네트워크(100)는, 인터넷 자율 시스템, 라우팅 프로토콜, 또는 중단간 트랜스포트 메커니즘에 의해 제한되지 않는다.

[0037] 예를 들어, 일부 실시예들에서, MFN(150)들의 컴포넌트들은, (1) 최적화된 다중 경로 및 적응형의 집중형 라우팅을 생성하고, (2) 강력한 QoS(Quality of Service) 보장을 제공하고, (3) 중간 TCP 분할 및/또는 종료를 통한 중단간 TCP 레이트를 최적화하고, (4) 전역적 네트워크 기능 가상화(NFV)에서 확장가능한 애플리케이션-레벨 미들박스 서비스들(예를 들어, 방화벽, 침입 검출 시스템(IDS), 침입 방지 시스템(IPS), WAN 최적화 등)을 클라우드의 컴퓨팅 부분에 재배치한다. 따라서, 가상 네트워크는, 기존의 네트워크 프로토콜에 구속되지 않고 회사의 맞춤형 수요 및 변화하는 수요에 맞게 최적화될 수 있다. 또한, 일부 실시예들에서, 가상 네트워크는, 지속적인 요건 변화에 따라 수행 능력에서 및 지리적 범위 양쪽 모두에서 동적으로 탄력적으로 확장 및 축소될 수 있는 "지불형(pay as you go)" 인프라스트럭처로서 구성될 수 있다.

[0038] 가상 네트워크(100)를 구현하기 위해, 가상 네트워크가 걸쳐 있는 각각의 공용 클라우드 데이터센터(105a-105f 및 110a-110d) 내의 적어도 하나의 관리형 포워딩 노드(150)는 제어기 세트에 의해 구성되어야 한다. 도 2는 본 발명의 일부 실시예들의 관리형 포워딩 노드(150) 및 제어기 클러스터(160)의 한 예를 나타낸다. 일부 실시예들에서, 각각의 관리형 포워딩 노드(150)는 공용 클라우드 데이터센터 내의 호스트 컴퓨터에서 실행되는 머신(예를 들어, VM 또는 컨테이너)이다. 다른 실시예들에서, 각각의 관리형 포워딩 노드(150)는 하나의 공용 클라우드 데이터센터 내의 동일한 호스트 컴퓨터에서 실행되는 복수의 머신(예를 들어, 복수의 VM 또는 컨테이너)에 의해 구현된다. 또 다른 실시예에서, 하나의 MFN의 2개 이상의 컴포넌트는, 하나 이상의 공용 클라우드 데이터센터 내의 2개 이상의 호스트 컴퓨터에서 실행되는 2개 이상의 머신에 의해 구현될 수 있다.

[0039] 도시된 바와 같이, 관리형 포워딩 노드(150)는, 측정 에이전트(205), 방화벽 및 NAT 미들박스 서비스 엔진(210 및 215), 하나 이상의 최적화 엔진(220), 엣지 게이트웨이(225 및 230), 및 클라우드 포워딩 요소(235)(예를 들어, 클라우드 라우터)를 포함한다. 일부 실시예들에서, 이들 컴포넌트들(205-235) 각각은 2개 이상의 컴포넌트들의 클러스터로서 구현될 수 있다.

[0040] 일부 실시예들에서의 제어기 클러스터(160)는, 각각의 컴포넌트 클러스터를 동적으로 확장 또는 축소하여 (1) 각각의 컴포넌트의 기능을 구현하도록 머신(예를 들어, VM 또는 컨테이너)을 추가 또는 제거하거나 및/또는 (2) 그 클러스터의 컴포넌트들을 구현하는 이전에 배치된 머신들에 컴퓨팅 및/또는 네트워크 자원을 추가하거나 제거할 수 있다. 따라서, 공용 클라우드 데이터센터 내의 각각의 배치된 MFN(150)은 MFN들의 클러스터로 간주되거나, MFN의 상이한 동작들을 수행하는 복수의 상이한 컴포넌트 클러스터를 포함하는 노드로서 간주될 수 있다.

[0041] 또한, 일부 실시예들에서, 제어기 클러스터는, 제어기 클러스터가 공용 클라우드 데이터센터를 통해 가상 네트워크를 정의하는 상이한 임차인들을 위해 상이한 세트의 MFN들을 공용 클라우드 데이터센터에 배치한다. 이 접근법에서, 임의의 2개의 임차인의 가상 네트워크들은 어떠한 MFN도 공유하지 않는다. 그러나, 후술되는 실시예들에서, 각각의 MFN은 상이한 임차인들을 위해 상이한 가상 네트워크를 구현하는데 이용될 수 있다. 본 기술분야의 통상의 기술자라면, 다른 실시예들에서, 제어기 클러스터(160)는 제1 세트의 임차인들 중 각각의 임차인의 가상 네트워크를 그 자신의 전용된 세트의 배치된 MFN들로 구현하는 반면, 제2 세트 임차인들 중 각각의 임차인의 가상 네트워크를 공유된 세트의 배치된 MFN들로 구현할 수 있다는 것을 깨달을 것이다.

[0042] 일부 실시예들에서, 지부 게이트웨이(225) 및 원격 디바이스 게이트웨이(230)는, 도 2에 도시된 바와 같이, MFN(150)에 접속하는 하나 이상의 지사(130) 및 원격 디바이스(예를 들어, 모바일 디바이스(140))와 각각 보안

VPN 접속을 확립한다. 이러한 VPN 접속의 한 예는 IPsec 접속이며, 아래에서 더 상세히 설명될 것이다. 그러나, 본 기술분야의 통상의 기술자라면, 다른 실시예들에서, 이러한 게이트웨이(225 및/또는 230)가 상이한 유형들의 VPN 접속을 확립한다는 것을 깨달을 것이다.

- [0043] 일부 실시예들에서의 MFN(150)은, 방화벽 동작, NAT 동작, IPS 동작, IDS 동작, 부하 밸런싱 동작, WAN 최적화 동작 등의, 하나 이상의 미들박스 서비스 동작을 수행하는 하나 이상의 미들박스 엔진을 포함한다. 이들 미들박스 동작들(예를 들어, 방화벽 동작, WAN 최적화 동작 등)을 공용 클라우드에 배치된 MFN들에 통합시킴으로써, 가상 네트워크(100)는, 전통적으로는 회사의 데이터센터(들) 및/또는 지사(들)의 회사 WAN 인프라스트럭처에 의해 수행되는 많은 기능을 공용 클라우드에서 구현한다.
- [0044] 따라서, 많은 미들박스 서비스에 대해, 회사 컴퓨팅 노드(예를 들어, 원격 디바이스, 지사 및 데이터센터)는, 이들 서비스들이 이제는 공용 클라우드에 배치되었기 때문에, 사실 데이터센터 또는 지사에 있는 회사의 회사 WAN 인프라에 더 이상 액세스할 필요가 없다. 이 접근법은, 이들 서비스들로의 회사 컴퓨팅 노드(예를 들어, 원격 디바이스, 지사 및 데이터센터)의 액세스를 가속하고, 보통은 이러한 서비스 제공에 전용되는 사실 데이터센터에서 혼잡한 네트워크 병목 현상을 피한다.
- [0045] 이 접근법은 WAN 게이트웨이 기능을 공용 클라우드 데이터센터 내의 다양한 MFN들에 효과적으로 분산한다. 예를 들어, 일부 실시예들의 가상 네트워크(100)에서, 전통적인 회사 WAN 게이트웨이 보안 기능들(예를 들어, 방화벽 동작, 침입 검출 동작, 침입 방지 동작 등)의 대부분 또는 전부는, 공용 클라우드 MFN들(예를 들어, 컴퓨팅 엔드포인트들로부터의 데이터가 가상 네트워크 내로 수신되는 유입 MFN들)로 이전된다. 이것은, 가상 네트워크(100)를 구현하는 많은 상이한 MFN들에서 구현되는 분산형 WAN 게이트웨이를 가상 네트워크(100)가 갖는 것을 효과적으로 허용한다.
- [0046] 도 2에 도시된 예에서, MFN(150)은, 방화벽 엔진(210), NAT 엔진(215), 및 하나 이상의 L4-L7 최적화 엔진을 포함하는 것으로 도시되어 있다. 본 기술분야의 통상의 기술자라면, 다른 실시예들에서, MFN(150)은 다른 미들박스 동작들을 수행하기 위한 다른 미들박스 엔진을 포함한다는 것을 깨달을 것이다. 일부 실시예들에서, 방화벽 엔진(210)은, (1) 가상 네트워크로의 유입 경로 상의 데이터 메시지 흐름(예를 들어, 게이트웨이(225 및 230)가 지사(130) 및 모바일 디바이스(140)로부터 수신하고 처리하는 데이터 메시지 흐름), 및 (2) 가상 네트워크 외부로의 유출 경로 상의 데이터 메시지 흐름(예를 들어, NAT 엔진(215) 및 인터넷(202)을 통해 SaaS 제공자 데이터센터에 전송되는 데이터 메시지 흐름)에 관해 방화벽 규칙을 시행한다.
- [0047] 일부 실시예들에서의 MFN(150)의 방화벽 엔진(210)은 또한, 데이터 메시지 흐름이 가상 네트워크 내로 진입하는 유입 MFN과 데이터 메시지 흐름이 가상 네트워크를 빠져 나가는 유출 MFN 사이의 중간 흡에 해당하는 MFN에 방화벽 엔진이 속할 때 방화벽 규칙을 시행한다. 다른 실시예들에서, 방화벽 엔진(210)은, 방화벽이 데이터 메시지 흐름의 유입 MFN 및/또는 유출 MFN의 일부일 때에만 방화벽 규칙을 시행한다.
- [0048] 일부 실시예들에서, NAT 엔진(215)은, 인터넷(202)을 통해 가상 네트워크 외부로의 유출 경로 상의 데이터 메시지 흐름의 소스 네트워크 주소를 제3자 디바이스(예를 들어, SaaS 제공자 머신)로 변경하는 네트워크 주소 변환을 수행한다. 이러한 네트워크 주소 변환은, 제3자 머신(예를 들어, SaaS 머신)이 주소 변환없이 임차인 및/또는 공용 클라우드 제공자의 사실 네트워크 주소를 명시할 수 있는 데이터 메시지 흐름을 처리하도록 적절히 구성될 수 있도록 보장한다. 이것은, 상이한 임차인들 및/또는 클라우드 제공자들의 사실 네트워크 주소들이 중첩될 수 있기 때문에 특히 문제가 된다. 주소 변환은 또한, 제3자 디바이스(예를 들어, SaaS 머신)로부터의 응답 메시지가, 가상 네트워크에 의해(예를 들어, 메시지가 가상 네트워크를 빠져 나온 MFN NAT 엔진에 의해) 적절히 수신될 수 있도록 보장한다.
- [0049] 일부 실시예들에서의 MFN의 NAT 엔진(215)은, 가상 네트워크를 떠나 제3자 머신에 도달하거나 제3자 머신으로부터 가상 네트워크로 진입하는 각각의 데이터 메시지 흐름에 관해 이중-NAT 동작을 수행한다. 아래에서 더 설명되는 바와 같이, 2개의 NAT 동작에서 하나의 NAT 동작은, 가상 네트워크에 진입할 때 그 유입 MFN에서 이러한 데이터 메시지 흐름에 관해 수행되는 반면, 다른 NAT 동작은 가상 네트워크를 빠져 나올 때 그 유출 MFN에서 데이터 메시지 흐름에 관해 수행된다.
- [0050] 이런 이중 NAT 접근법은, 더 많은 임차인 사실 네트워크들이 공용 클라우드 제공자의 네트워크에 맵핑되는 것을 허용한다. 이 접근법은 또한, 임차인 사실 네트워크의 변경에 관한 데이터를 MFN에 배포하기 위한 부하를 감소시킨다. 유입 또는 유출 NAT 동작 전에, 일부 실시예들은, 임차인 식별자를 이용하여 임차인의 소스 네트워크 주소를 또 다른 소스 네트워크 주소에 먼저 맵핑한 다음 이것을 NAT 동작에 의해 역시 또 다른 소스 네트워크

주소에 맵핑하는 임차인 맵핑 동작을 수행한다. 이중 NAT 동작을 수행하는 것은, 임차인 사설 네트워크 변경에 관한 데이터를 배포하기 위한 데이터 배포 부하를 감소시킨다.

[0051] 최적화 엔진(220)은, 최상의 중단간 성능 및 신뢰성을 위해 엔터티의 데이터 메시지를 목적지로 포워딩하는 것을 최적화하는 새로운 프로세스를 실행한다. 이들 프로세스들 중 일부는, 현재 네트워크 프로토콜 골화가 없는, 전용 고성능 네트워킹 프로토콜을 구현한다. 예를 들어, 일부 실시예들에서, 최적화 엔진(220)은 중간 TCP 분할 및/또는 종료를 통해 중단간 TCP 레이트를 최적화한다.

[0052] 클라우드 포워딩 요소(235)는, 데이터 메시지 흐름이 목적지에 도달하기 위해 또 다른 공용 클라우드를 횡단해야 할 때 데이터 메시지 흐름을 다음 홉 MFN의 클라우드 포워딩 요소(CFE)에, 또는 데이터 메시지 흐름이 동일한 공용 클라우드를 통해 목적지에 도달할 수 있을 때 동일한 공용 클라우드 내의 유출 라우터에 포워딩하는 것을 담당하는 MFN 엔진이다. 일부 실시예들에서, MFN(150)의 CFE(235)는 소프트웨어 라우터이다. 데이터 메시지를 포워딩하기 위해, CFE는 메시지를 터널 헤더로 캡슐화한다. 상이한 실시예들은, 데이터 메시지를 터널 헤더로 캡슐화하기 위해 상이한 접근법들을 이용한다. 아래에 설명되는 일부 실시예들은 가상 네트워크에 출입하기 위한 네트워크 유입/유출 주소를 식별하기 위해 하나의 터널 헤더를 이용하고, 데이터 메시지가 하나 이상의 중간 MFN을 횡단하여 유출 MFN에 도달해야 할 때 다음 홉 MFN을 식별하기 위해 또 다른 터널 헤더를 이용한다.

[0053] 구체적으로, 일부 실시예들에서, CFE는, 2개의 터널 헤더, (1) 가상 네트워크에 출입하기 위한 유입 CFE 및 유출 CFE를 식별하는 내측 헤더, 및 (2) 다음 홉 CFE를 식별하는 외측 헤더와 함께 데이터 메시지를 전송한다. 일부 실시예들에서 내측 터널 헤더는 또한, 가상 네트워크 제공자의 복수의 상이한 임차인들이 가상 네트워크 제공자의 공통 세트의 MFN CFE들을 이용하는 것을 허용하기 위하여 임차인 식별자(TID)를 포함한다. 다른 실시예들은 오버레이 가상 네트워크를 정의하기 위해 터널 헤더들을 상이하게 정의한다.

[0054] 하나 이상의 공용 클라우드를 통해 임차인에 대한 가상 네트워크를 배치하기 위해, 제어기 클러스터는, (1) 임차인의 회사 컴퓨팅 노드들(예를 들어, 지사, 데이터센터, 모바일 사용자, 및 SaaS 제공자들)의 위치에 기초하여 임차인에 대한 가상 네트워크에 출입하기 위한 가능한 유입 및 유출 라우터들을 식별하고, (2) 가상 네트워크를 구현하는 다른 중간 공용 클라우드 라우터를 통해 식별된 유입 라우터들로부터 식별된 유출 라우터들로 횡단하는 경로들을 식별한다. 이들 경로들을 식별한 후, 제어기 클러스터는 이들 경로들을 공용 클라우드(들) 내의 MFN CFE(235)들의 포워딩 테이블들에 전파한다. OVS-기반의 가상 네트워크 라우터를 이용하는 실시예들에서, 제어기는 OpenFlow를 이용함으로써 경로들을 분산시킨다.

[0055] 일부 실시예들에서, 제어기 클러스터(160)는 또한, 최상의 중단간 성능, 신뢰성 및 보안을 달성하기 위해 여러 네트워크 처리 계층들을 최적화하도록, 가상 네트워크를 구현하는 각각의 MFN(150)의 컴포넌트들(205-235)을 구성할 수 있다. 예를 들어, 일부 실시예들에서, 이들 컴포넌트들은, (1) 계층 3 트래픽 라우팅(예를 들어, 최단 경로, 패킷 복제)을 최적화하고, (2) 계층 4 TCP 혼잡 제어(예를 들어, 세그먼트화, 레이트 제어)를 최적화하고, (3) 보안 피처(예를 들어, 암호화, 심층 패킷 검사, 방화벽)를 구현하고, (4) 애플리케이션-계층 압축 피처(예를 들어, 중복 제거, 캐싱)를 구현하도록 구성된다. 가상 네트워크 내에서, 회사 트래픽은 보안, 검사 및 기록된다.

[0056] 일부 실시예들에서, 하나의 측정 에이전트는 공용 클라우드 데이터센터 내의 각각의 MFN에 대해 배치된다. 다른 실시예들에서, 공용 클라우드 데이터센터 또는 데이터센터들의 모임(예를 들어, 하나의 가용 구역 내의 데이터센터들 등의, 근처의 연관된 데이터센터들의 모임) 내의 복수의 MFN은 하나의 측정 에이전트를 공유한다. 계층 3 및 4 처리를 최적화하기 위해, 각각의 관리형 포워딩 노드(150)와 연관된 측정 에이전트(205)는, 그 노드와 여러개의 다른 "이웃" 노드들 각각 사이의 네트워크 접속의 품질을 정량화하는 측정 값을 반복적으로 생성한다.

[0057] 상이한 실시예들은 이웃 노드를 상이하게 정의한다. 특정한 공용 클라우드 제공자의 하나의 공용 클라우드 데이터센터 내의 특정한 MFN에 대해, 일부 실시예들의 이웃 노드는, (1) 특정한 공용 클라우드 제공자의 임의의 공용 클라우드 데이터센터에서 동작하는 임의의 다른 MFN, 및 (2) 특정한 MFN과 동일한 "지역" 내에 있는 또 다른 공용 클라우드 제공자의 데이터센터에서 동작하는 임의의 다른 MFN을 포함한다.

[0058] 상이한 실시예들은 동일한 지역을 상이하게 정의한다. 예를 들어, 일부 실시예들은 특정한 관리형 포워딩 노드 주위의 경계 형상을 명시하는 거리의 관점에서 지역을 정의한다. 다른 실시예들은, 북부 캘리포니아, 남부 캘리포니아 등의, 도시, 주, 또는 지역적 영역의 관점에서 영역을 정의한다. 이 접근법의 가정은, 동일한 공용

클라우드 제공자의 상이한 데이터센터들은 초고속 네트워크 접속에 의해 접속되는 반면, 상이한 공용 클라우드 제공자들의 데이터센터들 사이의 네트워크 접속은 데이터센터들이 동일한 지역 내에 있을 때는 빠르지만 데이터센터들이 상이한 지역들 내에 있을 때는 빠르지는 않다는 것이다. 상이한 공용 클라우드 제공자들의 데이터센터들 사이의 접속은, 데이터센터들이 상이한 지역들에 있을 때 공용 인터넷을 통해 장거리를 횡단해야만 할 수도 있다.

[0059] 측정 에이전트(205)는 상이한 실시예들에서 상이하게 측정 값들을 생성한다. 일부 실시예들에서, 측정 에이전트는, 핑 메시지(예를 들어, UDP 에코 메시지)를 그 이웃하는 관리형 포워딩 노드들의 측정 에이전트들 각각에게 주기적으로(예를 들어, 매초마다, N 초마다, 매분마다, M 분마다 한번 등) 전송한다. 핑 메시지의 크기가 작다면, 많은 네트워크 접속 요금을 초래하지 않는다. 예를 들어, 각각의 노드가 10 초마다 각각의 다른 노드에게 핑을 전송하는 100개의 노드의 경우, 각각의 노드에 대해 약 10Kb/s의 유입 및 유출 측정 트래픽이 생성되고, 이것은, 현재 공용 클라우드 가격을 고려할 때, 연간 노드당 수 달러(예를 들어, \$5)의 네트워크 소비 요금으로 이어진다.

[0060] 수신되는 응답 메시지의 속도에 기초하여, 측정 에이전트(205)는, 네트워크-접속 처리 속도, 지연, 손실 및 링크 신뢰성 등의, 측정 메트릭 값을 계산하고 업데이트한다. 이들 동작들을 반복하여 수행함으로써, 측정 에이전트(205)는 그 이웃 노드들에 대한 네트워크 접속의 품질을 표현하는 측정 결과의 매트릭스를 정의하고 업데이트한다. 에이전트(205)가 이웃 노드의 측정 에이전트와 상호작용할 때, 그 측정 매트릭스는 그 로컬 노드 무리들에 대한 접속 품질만을 정량화한다.

[0061] 상이한 관리형 포워딩 노드들의 측정 에이전트는, 그들의 측정 매트릭스를 제어기 클러스터(160)에 전송하고, 제어기 클러스터(160)는, 그 다음, 모든 상이한 무리 접속 데이터를 집계하여 상이한 쌍들의 관리형 포워딩 노드들 사이의 접속에 대한 총계 메시 뷰(aggregate mesh view)를 획득한다. 제어기 클러스터(160)가 2개의 쌍의 포워딩 노드들 사이의 링크에 대한 상이한 측정치들(예를 들어, 상이한 시간들에서 하나의 노드에 의해 측정된 측정치들)을 수집할 때, 제어기 클러스터는 상이한 측정치들로부터 혼합된 값을 생성한다(예를 들어, 측정치들의 평균 또는 가중 평균을 생성한다). 일부 실시예들에서 총계 메시 뷰는, 각각의 쌍의 관리형 포워딩 노드들 사이의 모든 네트워크 접속의 전체 메시 뷰인 반면, 다른 실시예들에서는, 개개의 관리형 포워딩 노드의 측정 에이전트에 의해 생성된 것보다 더 완전한 뷰이다.

[0062] 도 2에 도시된 바와 같이, 제어기 클러스터(160)는, 하나 이상의 측정-처리 엔진(280), 하나 이상의 경로-식별 엔진(282), 및 하나 이상의 관리 인터페이스(284)의 클러스터를 포함한다. 불필요한 상세사항으로서 설명을 불명료하게 하지 않기 위해, 이들 클러스터 각각은 단일 엔진 또는 인터페이스 계층의 관점에서, 즉, 측정-처리 계층(280), 경로-식별 계층(282), 및 관리 인터페이스 계층(284)의 관점에서 아래에서 참조될 것이다.

[0063] 측정-처리 계층(280)은, 관리형 포워딩 노드의 측정 에이전트(205)로부터 측정 매트릭스를 수신하고, 이들 측정 매트릭스들을 처리하여 상이한 쌍들의 관리형 포워딩 노드들 사이의 접속 품질을 표현하는 총계 메시 매트릭스를 생성한다. 측정-처리 계층(280)은 총계 메시 매트릭스를 경로-식별 계층(282)에 제공한다. 총계 메시 매트릭스에 기초하여, 경로-식별 계층(282)은 상이한 회사 데이터 엔드포인트들(예를 들어, 상이한 지사들, 회사 데이터센터들, SaaS 제공자 데이터센터들 및/또는 원격 디바이스들)를 접속하기 위해 가상 네트워크를 통해 상이한 원하는 라우팅 경로들을 식별한다. 이 계층(282)은 관리형 포워딩 노드(150)의 클라우드 포워딩 요소(235)에 배포되는 경로 테이블에 이들 라우팅 경로를 제공한다.

[0064] 일부 실시예들에서, 각각의 쌍의 데이터 메시지 엔드포인트들에 대한 식별된 라우팅 경로는, 한 세트의 최적화 기준에 기초하여 최적인 것으로 간주되는 라우팅 경로로서, 예를 들어 가장 빠른 라우팅 경로, 가장 짧은 라우팅 경로 또는 인터넷을 최소로 이용하는 경로이다. 다른 실시예들에서, 경로-식별 엔진은, 동일한 2개의 엔드포인트들 사이의 복수의 상이한 라우팅 경로를 식별하고 (라우팅 테이블에서) 제공할 수 있다. 이들 실시예에서, 관리형 포워딩 노드(150)의 클라우드 포워딩 요소(235)들은 QoS 기준 또는 그들이 시행하고 있는 다른 런타임 기준에 기초하여 경로들 중 하나를 선택한다. 일부 실시예들에서의 각각의 CFE(235)는, CFE로부터 가상 네트워크의 유출 지점까지의 전체 라우팅 경로를 수신하지 않고, 그 경로에 대한 다음 홉을 수신한다.

[0065] 일부 실시예들에서, 경로-식별 계층(282)은 총계 메시 매트릭스에서의 측정 값을 전역적 라우팅 그래프를 구성하기 위해 실행하는 라우팅 알고리즘에 대한 입력으로서 이용한다. 이 전역적 라우팅 그래프는, 일부 실시예들에서 측정-처리 계층(280)이 생성하는 측정 그래프의 집계되고 최적화된 버전이다. 도 3은, 일부 실시예들에서 제어기 측정-처리 계층(280)이 생성하는 측정 그래프(300)의 한 예를 나타낸다. 이 그래프는, AWS 및 GCP 공용 클라우드(310 및 320)(즉, AWS 및 GCP의 데이터센터들) 내의 다양한 관리형 포워딩 노드(150)들 사이의 네트워

크 접속을 도시한다. 도 4a는, 일부 실시예들에서 제어기 경로-식별 계층(282)이 측정 그래프(300)로부터 생성하는 라우팅 그래프(400)의 한 예를 나타낸다.

[0066] 도 5는 제어기 경로-식별 계층이 제어기 측정 계층으로부터 수신된 측정 그래프로부터 라우팅 그래프를 생성하기 위해 이용하는 프로세스(500)를 나타낸다. 경로-식별 계층(282)은, 제어기 측정 계층으로부터 업데이트된 측정 그래프를 반복적으로 수신함에 따라 이 프로세스(500)를 반복적으로 수행한다(예를 들어, 새로운 측정 그래프를 수신할 때마다 매번, 또는 새로운 측정 그래프를 수신하는 매 N번째마다 프로세스(500)를 수행한다). 다른 실시예들에서, 경로-식별 계층(282)은 이 프로세스를 주기적으로(예를 들어, 12 시간 또는 24 시간마다 한번) 수행한다.

[0067] 도시된 바와 같이, 경로-식별 계층은 초기에, 라우팅 그래프가 측정 그래프와 동일하도록(즉, 동일한 쌍들의 관리형 포워딩 노드들 사이에 동일한 링크를 갖도록) 정의한다(505). 510에서, 프로세스는 측정 그래프(300)로부터 불량 링크를 제거한다. 불량 링크의 예는, 과도한 메시지 손실 또는 불량한 신뢰성을 갖는 링크(예를 들어, 마지막 15분 동안 메시지 손실이 2%를 초과하거나 마지막 2분 동안 메시지 손실이 10%를 초과하는 링크)이다. 도 4a는 측정 그래프(300)의 링크(302, 304 및 306)가 라우팅 그래프(400)에서 제외되는 것을 나타낸다. 이 도면은 이들 링크를 점선으로 도시함으로써 이들 링크의 제외를 나타낸다.

[0068] 그 다음, 515에서, 프로세스(500)는 링크 가중치 점수(비용 점수)를 여러 계산된 및 제공자-특유의 값들의 가중 조합으로서 계산한다. 일부 실시예들에서, 가중치 점수는 링크의 (1) 계산된 지연 값, (2) 계산된 손실 값, (3) 제공자 네트워크-접속 비용 및 (4) 제공자 컴퓨팅 비용의 가중 조합이다. 일부 실시예들에서, 링크에 의해 접속된 관리형 포워딩 노드들은 공용 클라우드 데이터센터(들) 내의 호스트 컴퓨터들에서 실행되는 머신들(예를 들어, VM들 또는 컨테이너들)이기 때문에, 제공자 컴퓨팅 비용이 고려된다.

[0069] 520에서, 프로세스는 가상 네트워크에서의 데이터 메시지 흐름에 대한 알려진 소스 및 목적지 IP 주소(예를 들어, 회사 엔티티에 의해 이용되는 SaaS 제공자들의 알려진 IP들)를 라우팅 그래프에 추가한다. 일부 실시예들에서, 프로세스는 가능한 메시지-흐름 엔드포인트의 각각의 알려진 IP 주소를 그 엔드포인트에 가장 가까운 라우팅 그래프 내의 노드(예를 들어, MFN을 나타내는 노드)에 추가한다. 그렇게 함에 있어서, 일부 실시예들에서의 프로세스는, 각각의 이러한 엔드포인트가 제로 지연 비용 및 제로 손실 비용으로 링크를 통해 가상 네트워크에 접속되어 있다고 가정한다. 도 4b는 2개의 SaaS 제공자들의 데이터센터들에 가장 가까운 데이터센터들에 있는 라우팅 그래프 내의 (2개의 MFN을 나타내는) 2개의 노드(402 및 404)에 이들 2개의 SaaS 제공자에 대한 알려진 IP를 추가하는 한 예를 나타낸다. 이 예에서, 하나의 노드는 AWS 공용 클라우드에 있고, 다른 노드는 GCP 공용 클라우드에 있다. 대안으로서 또는 결합하여, 일부 실시예들에서의 프로세스(500)는, 소스 및 목적지 엔드포인트를 나타내기 위해 이 그래프에 노드들을 추가하고, 이들 노드에 IP 주소를 할당하고, 라우팅 그래프 내의 다른 노드들(예를 들어, 공용 클라우드에서 MFN들을 나타내는 라우팅 그래프의 노드들)에 이들 추가된 노드들을 접속하는 링크들에 가중치 값을 할당함으로써, 알려진 소스 및 목적지 IP 주소를 라우팅 그래프에 추가한다. 흐름들에 대한 소스 및 목적지 엔드포인트가 노드로서 추가될 때, 경로-식별 엔진(282)은, 상이한 소스 및 목적지 엔드포인트들 사이에서 가상 네트워크를 통한 상이한 경로들을 식별하고 있을 때 이들 노드에 도달하는 비용(예를 들어, 거리 비용, 지연 비용 및/또는 재정 비용 등)을 감안할 수 있다.

[0070] 도 4c는, 2개의 SaaS 제공자를 나타내기 위해 2개의 노드(412 및 414)를 도 4a의 노드 그래프(400)에 추가함으로써 생성되는 라우팅 그래프(410)를 나타낸다. 이 예에서, 알려진 IP 주소들은 노드들(412 및 414)에 할당되고, 이들 노드는 가중치 W1 및 W2가 할당된 링크(416 및 418)를 통해 (2개의 MFN을 나타내는) 노드(402 및 404)에 접속된다. 이 접근법은, 2개의 SaaS 제공자의 알려진 IP 주소를 도 4b에 나타낸 접근법에 추가하기 위한 대안적 접근법이다.

[0071] 도 4d는 더 상세한 라우팅 그래프(415)를 나타낸다. 이 더 상세한 라우팅 그래프에서, AWS 및 GCP 공용 클라우드(310 및 320)에 각각 접속되는 알려진 IP 주소를 갖는 외부 회사 컴퓨팅 노드(예를 들어, 지사 및 데이터센터)를 나타내기 위해 추가 노드(422 및 424)가 추가된다. 이들 노드들(422/424) 각각은, 연관된 가중치 값 Wi를 갖는 적어도 하나의 링크(426)에 의해 MFN을 나타내는 라우팅 그래프 노드들 중 적어도 하나에 접속된다. 이들 노드 중 일부(예를 들어, 지사들 중 일부)는 복수의 링크로 동일한 MFN 또는 상이한 MFN들에 접속된다.

[0072] 그 다음, 525에서, 프로세스(500)는, 회사 엔티티의 데이터 메시지 흐름에 대한 가상 네트워크 유출 위치로서 역할할 수 있는 각각의 MFN과 각각의 다른 MFN 사이의 최저 비용 경로(예를 들어, 최단 경로 등)를 계산한다. 일부 실시예들에서의 유출 MFN은, 외부 회사 컴퓨팅 노드(예를 들어, 지사, 회사 데이터센터 및 SaaS 제공자 데

이터센터)에 접속된 MFN뿐만 아니라, 모바일 디바이스 접속 및 유출 인터넷 접속에 대한 후보 위치에 해당되는 MFN을 포함한다. 일부 실시예들에서, 이 계산은 상이한 MFN 쌍들 사이의 최단 경로를 식별하는 전통적인 최저 비용(예를 들어, 최단 경로) 식별 프로세스를 이용한다.

[0073] 각각의 후보 MFN 쌍에 대해, 최저 비용 식별 프로세스는, 계산된 가중치 점수(즉, 510에서 계산된 점수)를 이용하여 복수의 이러한 경로가 MFN 쌍 사이에 존재할 때 최저 점수를 갖는 경로를 식별한다. 최저 비용 경로를 계산하기 위한 여러 방식들이 아래에서 더 설명될 것이다. 위에서 언급된 바와 같이, 경로-식별 계층(282)은 일부 실시예들에서 2개의 MFN 쌍들 사이의 복수의 경로를 식별한다. 이것은, 클라우드 포워딩 요소(235)가 상이한 환경들 하에서 상이한 경로들을 이용하는 것을 허용하기 위한 것이다. 따라서, 이들 실시예에서, 프로세스(500)는 2개의 MFN 쌍들 사이의 복수의 경로를 식별할 수 있다.

[0074] 530에서, 프로세스는, 525에서 식별된 최저 비용 경로들 중 어느 것에 의해서도 이용되지 않는 MFN 쌍들 사이의 링크들을 라우팅 그래프로부터 제거한다. 그 다음, 535에서, 프로세스는 라우팅 그래프로부터 클라우드 포워딩 요소(235)에 대한 라우팅 테이블을 생성한다. 535에서, 프로세스는 이들 라우팅 테이블을 관리형 포워딩 노드들의 클라우드 포워딩 요소(235)들에 배포한다. 535 후에, 프로세스가 종료된다.

[0075] 일부 실시예들에서, 가상 네트워크는 2가지 유형의 외부 접속을 가지며, 이것은 다음과 같다: (1) 한 엔티티의 컴퓨팅 노드들(예를 들어, 지사들, 데이터센터들, 모바일 사용자들 등)과의 외부 보안 접속, 및 (2) 인터넷을 통한 제3자 컴퓨터(예를 들어, SaaS 제공자 서버)로의 외부 접속. 일부 실시예들은, 가상 네트워크 외부의 소스 및 목적지 노드에서 종료되는 각각의 데이터경로에 대한 최적의 가상-네트워크 유입 및 유출 위치를 발견함으로써 가상 네트워크를 최적화한다. 예를 들어, 지사를 SaaS 제공자 서버(예를 들어, salesforce.com 서버)에 접속하기 위해, 일부 실시예들은, 지사를 최적의 엣지 MFN(예를 들어, 지사로의 가장 빠른 네트워크 접속을 갖는 MFN, 또는 지사에 가장 가까운 것)에 접속하고, 최적적으로 위치한 SaaS 제공자 서버(예를 들어, 지사에 대한 엣지 MFN에 가장 가깝거나, SaaS 제공자 서버에 접속된 엣지 MFN을 통해 지사에 대한 엣지 MFN까지의 가장 빠른 경로를 갖는 SaaS)에 대한 최적의 엣지 MFN을 식별한다.

[0076] VPN 접속을 통해 한 엔티티의 각각의 컴퓨팅 노드(예를 들어, 지사, 모바일 사용자 등)를 가장 가까운 MFN에 연관시키기 위해, 일부 실시예들에서의 가상 네트워크 제공자는, 컴퓨팅 노드가 컨택하기 위한 하나 이상의 정식(authoritative) 도메인 네임 서버(DNS)를 공용 클라우드에 배치한다. 일부 실시예들에서, 일부 실시예들에서의 회사 컴퓨팅 노드가 가상 네트워크 제공자의 MFN으로의 VPN 접속을 확립(즉, VPN 접속을 초기화 또는 재초기화)할 필요가 있을 때마다, 컴퓨팅 노드는 먼저, 그 가상 네트워크(예를 들어, virtualnetworkX.net)와 연관된 주소를 이 정식 DNS 서버를 이용하여 해결하여, 이 서버가 회사 컴퓨팅 노드에 가장 가까운 MFN으로서 식별하는 MFN의 신원을 이 서버로부터 획득한다. 이 MFN을 식별하기 위해, 일부 실시예들에서, 정식 DNS 서버는 MFN 식별자(예를 들어, MFN의 IP 주소)를 제공한다. 그 다음, 회사 컴퓨팅 노드는 이 관리형 포워딩 노드로의 VPN 접속을 확립한다.

[0077] 다른 실시예들에서, 회사 컴퓨팅 노드는, VNP의 MFN으로의 VPN 접속을 확립할 필요가 있을 때마다 먼저 DNS 해결을 수행하지 않는다(즉, 특정한 도메인에 대한 네트워크 주소를 먼저 해결하지 않는다). 예를 들어, 일부 실시예들에서, 회사 컴퓨팅 노드는, 또 다른 DNS 해결을 수행하기 전에 특정한 기간 동안(예를 들어, 하루 동안, 한 주 동안 등) DNS-해결된 MFN을 고수하여 이 MFN이 여전히 접속해야 하는 최적의 것인지를 결정한다.

[0078] DNS 요청에서의 소스 IP 주소가, 노드 자체가 아닌 회사 컴퓨팅 노드의 로컬 DNS 서버의 주소일 때, 일부 실시예들에서의 정식 DNS 서버는, 회사 컴퓨팅 노드에 가장 가까운 MFN 대신에 로컬 DNS 서버에 가장 가까운 MFN을 식별한다. 이를 해결하기 위해, 일부 실시예들에서의 DNS 요청은, 점들에 의해 연결되고 구분되는 하나 이상의 부분(라벨)을 포함하는 도메인 네임의 관점에서 회사 컴퓨팅 노드를 식별하고, 여기서, 이들 부분들 중 하나는 회사를 식별하고 다른 부분은 회사의 컴퓨팅 노드를 식별한다.

[0079] 일부 실시예들에서, 이 도메인 네임은, 도메인 네임에서 우측 라벨로부터 좌측 라벨로 내려가는 도메인과 서브도메인의 계층관계를 명시한다. 최우측의 첫번째 라벨은 특정한 도메인을 식별하고, 그 첫번째 라벨 좌측에 있는 2번째 라벨은 회사 엔티티를 식별하고, 그 2번째 라벨의 좌측에 있는 3번째 라벨은, 엔티티가 하나보다 많은 외부 머신 위치를 갖는 경우 엔티티의 외부 머신 위치를 식별한다. 예를 들어, 일부 실시예들에서, DNS 요청은, 회사 컴퓨팅 노드를 회사 myCompany의 myNode로서 식별하고 주소 myNode.myCompany.virtualnetwork.net의 해결을 요청한다. 그 다음, DNS 서버는 myNode 식별자를 이용하여 회사 컴퓨팅 노드가 VPN 접속을 확립해야 하는 유입 MFN을 더 잘 선택한다. 상이한 실시예들에서, myNode 식별자는 상이하게 표현된다. 예를 들어, 이것은, IP 주소, 위치의 위도/경도 설명, GPS(Global Positioning

System) 위치, 거리 주소 등으로서 어드레싱될 수 있다.

- [0080] IP 주소가 위치를 적절하게 반영하더라도, 예를 들어, 동일한 클라우드 내의 상이한 데이터센터들에 속하거나 동일한 지역 내의 상이한 클라우드들에 속하는 여러 잠재적 유입 라우터들이 있을 수 있다. 이러한 경우에, 일부 실시예들에서의 가상 네트워크 정식 서버는 잠재적 MFN CFE들(예를 들어, C5, C8, C12)의 IP 목록을 다시 전송한다. 그 다음, 일부 실시예들에서의 회사 컴퓨팅 노드는, 그 목록 내의 상이한 CFE들을 평가하여 측정치(예를 들어, 거리 또는 속도 측정치)를 생성하고, CFE 후보 세트 중에서 측정치들을 비교함으로써 가장 가까운 것을 선택한다.
- [0081] 또한, 회사 컴퓨팅 노드는, 회사 엔티티의 다른 컴퓨팅 노드들에 의해 현재 이용되는 MFN들을 식별함으로써 이 선택을 기초로 할 수 있다. 예를 들어, 일부 실시예들에서, 회사 컴퓨팅 노드는 각각의 MFN에 접속 비용을 추가하여, 많은 회사 지부들이 주어진 클라우드에 이미 접속되어 있다면, 새로운 컴퓨팅 노드가 동일한 클라우드에 접속하기 위한 동기부여를 가지므로, 처리, 레이턴시 및 달러 측면에서 클라우드간 비용을 최소화하게 할 수 있다.
- [0082] 다른 실시예들은 상이한 DNS 해결 기술들을 이용한다. 예를 들어, 회사 컴퓨팅 노드(예를 들어, 지사, 데이터센터, 모바일 사용자 등)가 DNS 해결을 수행할 필요가 있을 때마다, 회사 컴퓨팅 노드(예를 들어, 모바일 디바이스, 또는 지사 또는 데이터센터의 로컬 DNS 해결자)는, 다수의 엔티티들에 대한 정식 DNS 해결자로서 역할하는 DNS 서비스 제공자와 통신한다. 일부 실시예들에서, 이 DNS 서비스 제공자는 하나 이상의 사설 데이터센터에 위치한 DNS 해결 머신을 갖는 반면, 다른 실시예들에서는 하나 이상의 공용 클라우드 데이터센터의 일부이다.
- [0083] 인터넷에 직접 접속하는 N개의 관리형 포워딩 노드들 중 어느 것이 SaaS 제공자 서버에 도달하기 위해 이용되어야 하는지를 식별하기 위해, 가상 네트워크(예를 들어, 유입 MFN 또는 MFN들을 구성하는 제어기 클러스터)는 일부 실시예들에서 N개의 관리형 포워딩 노드들로부터 한 세트의 하나 이상의 후보 엣지 MFN들을 식별한다. 아래에 더 설명되는 바와 같이, 일부 실시예들에서의 각각의 후보 엣지 MFN은, SaaS 제공자 서버까지의 거리, 네트워크 접속 속도, 비용, 지연 및/또는 손실, 네트워크 컴퓨팅 비용 등의, 한 세트의 기준에 기초하여 최적인 것으로 간주되는 엣지 MFN이다.
- [0084] 최적의 엣지 지점들을 식별하는 것을 보조하기 위해, 일부 실시예들의 제어기 클러스터는 엔티티를 위해 가장 인기있는 SaaS 제공자들 및 소비자 웹 목적지들 및 그들의 IP 주소 서브넷들의 목록을 유지한다. 이러한 각각의 목적지에 대해, 제어기 클러스터는, (다시 한번, 물리적 거리, 네트워크 접속 속도, 비용, 손실 및/또는 지연, 컴퓨팅 비용 등에 의해 판단되는) 최적의 MFN들 중 하나 이상을 후보 유출 노드로서 할당한다. 각각의 후보 유출 MFN에 대해, 제어기 클러스터는, 그 다음, 가능한 각각의 유입 MFN으로부터 후보 MFN까지의 최상의 경로를 계산하고, 그에 따라 MFN들에서 결과적인 다음 홉 테이블을 셋업하되, 인터넷 SaaS 제공자 또는 웹 목적지가 올바른 가상 네트워크 다음-홉 노드에 연관되도록 한다.
- [0085] 서비스 목적지가 (정식 DNS 서버에 의해 제공되는) 여러 위치들에 있는 여러 IP 서브넷들을 통해 도달될 수 있다고 가정하면, 레이턴시를 최소화하고 부하-밸런싱을 제공하는 여러개의 잠재적인 유출 노드가 있다. 따라서, 일부 실시예들에서, 제어기 클러스터는 각각의 MFN에 대한 최상의 위치 및 유출 노드를 계산하고, 그에 따라 다음-홉을 업데이트한다. 또한, SaaS 제공자(예를 들어, office365.com)에 도달하기 위한 최상의 유출 노드는 하나의 공용 클라우드 제공자(예를 들어, Microsoft Azure)를 통할 수 있지만, 순수하게 거리 또는 접속 속도로부터 나온 최상의 유입 MFN은 또 다른 공용 클라우드 제공자(예를 들어, AWS)에 있을 수 있다. 이러한 상황에서, 이것은, 가상 네트워크를 떠나기 전에 레이턴시, 처리 및 또 다른 클라우드(즉, 최상의 유출 MFN을 갖는 공용 클라우드)로 횡단하는 비용 측면에서 최적일 아닐 수 있다. 복수의 후보 엣지 노드를 제공하는 것은, 이러한 상황에서 최적의 엣지 MFN 및 선택된 엣지 MFN까지의 최적의 경로의 선택을 허용할 것이다.
- [0086] 인터넷에 접속되거나 회사 엔티티의 회사 컴퓨팅 노드에 접속되는 유출 MFN까지의 가상 네트워크를 통한 최적의 경로를 식별하기 위해, 제어기 클러스터는 MFN들 사이의 최적의 라우팅 경로를 식별한다. 위에서 언급된 바와 같이, 일부 실시예들에서의 제어기 클러스터는, 예를 들어, 추정된 레이턴시 및 재정 비용의 가중 합을 반영하는 메트릭 점수에 기초하여, 한 쌍의 직접 접속된 MFN들 사이의 각각의 링크를 먼저 계산함으로써, 임의의 2개의 MFN들 사이의 최상의 경로를 식별한다. 레이턴시 및 재정 비용은, 일부 실시예들에서, (1) 링크 지연 측정, (2) 추정된 메시지 처리 레이턴시, (3) 특정한 데이터센터로부터 동일한 공용 클라우드 제공자의 또 다른 데이터센터로의, 또는 공용 클라우드(PC) 제공자의 클라우드로의(예를 들어, 또 다른 공용 클라우드 제공자의 또 다른 공용 클라우드 데이터센터로의 또는 인터넷으로의) 송출 트래픽에 대한 클라우드 요금, 및 (4) 공용 클라우드

드의 호스트 컴퓨터에서 실행되는 MFN과 연관된 추정된 메시지 처리 비용을 포함한다.

- [0087] 이들 쌍을 이룬 링크들의 계산된 비용을 이용하여, 제어기 클러스터는, 라우팅 경로에 의해 이용되는 개개의 쌍 일 이룬 링크들의 비용을 집계함으로써 이들 쌍을 이룬 링크들 중 하나 이상을 이용하는 각각의 라우팅 경로의 비용을 계산할 수 있다. 전술된 바와 같이, 제어기 클러스터는, 그 다음, 라우팅 경로의 계산된 비용에 기초하여 라우팅 그래프를 정의하고, 정의된 라우팅 그래프에 기초하여 MFN들의 클라우드 라우터들의 포워딩 테이블들을 생성한다. 또한, 위에서 언급된 바와 같이, 제어기 클러스터는 이들 비용계산, 그래프 작성, 및 포워딩 테이블 업데이트 및 배포 동작을, 주기적으로(예를 들어, 12 시간마다, 24 시간마다 한번 등) 또는 MFN들의 측정 에이전트들로부터 측정지 업데이트를 수신할 때 반복적으로 수행한다.
- [0088] MFN CFE C_i 에 있는 포워딩 테이블이 다음-홉 MFN CFE C_j 를 가리킬 때마다, CFE C_i 는 C_j 를 이웃으로 간주한다. 일부 실시예들에서, CFE C_i 는 CFE C_j 로의 보안되고 능동적으로 유지되는 VPN 터널을 확립한다. 일부 실시예들에서의 보안 터널은, 캡슐화된 데이터 메시지의 페이로드가 암호화될 것을 요구하는 터널이다. 또한, 일부 실시예들에서, 터널은, 터널의 하나 또는 양쪽 모두의 엔드포인트가 다른 엔드포인트에 킵 얼라이브 신호(keep alive signal)를 전송함으로써 능동적으로 유지된다.
- [0089] 다른 실시예들에서, CFE는 보안되고 능동적으로 유지되는 VPN 터널을 확립하지 않는다. 예를 들어, 일부 실시예들에서, CFE들 사이의 터널은, 킵 얼라이브 신호의 전송을 통해 능동적으로 모니터링되지 않는 정적 터널이다. 또한, 일부 실시예들에서, CFE들 사이의 이들 터널은, 그들의 페이로드를 암호화하지 않는다. 일부 실시예들에서, 한 쌍의 CFE들 사이의 터널은 2개의 캡슐화 헤더를 포함하고, 여기서, 내측 헤더는 임차인 ID 및 가상 네트워크에 출입하는(즉, 공용 클라우드(들)에 출입하는) 데이터 메시지에 대한 유입 및 유출 CFE들을 식별하고, 외측 캡슐화 헤더는, 유입 CFE로부터 유출 CFE까지 0개 이상의 CFE를 통과하기 위한 소스 및 목적지 네트워크 주소(예를 들어, IP 주소)를 명시한다.
- [0090] 내부 터널에 추가하여, 일부 실시예들에서의 가상 네트워크는, 앞서 언급된 바와 같이, VPN 터널을 이용하여 회사 컴퓨팅 노드들을 그들의 옛지 MFN들에 접속한다. 따라서, CFE들을 접속하기 위해 보안 터널이 이용되는 실시예들에서, 데이터 메시지는 완전히 보안된 VPN 경로를 이용하여 가상 네트워크를 통해 운송된다.
- [0091] 가상 네트워크 데이터 메시지들이 가상 네트워크 내에서 캡슐화를 이용하여 포워딩될 때, 일부 실시예들에서의 가상 네트워크는 임차인의 상이한 사설 네트워크에 의해 이용되는 사설 주소와는 상이한 그 자신의 고유의 네트워크 주소를 이용한다. 다른 실시예들에서, 가상 네트워크는, 가상 네트워크가 정의되는 공용 클라우드들의 사설 및 공용 네트워크 주소 공간을 이용한다. 또 다른 실시예들에서, 가상 네트워크는, 그 컴포넌트들 중 일부(예를 들어, 그 MFN들, CFE들, 및/또는 서비스들 중 일부)에 대해 그 자신의 고유한 네트워크 주소들 중 일부를 이용하는 반면, 그 컴포넌트들 중 다른 것들에 대해서는 공용 클라우드의 사설 및 공용 네트워크 주소 공간을 이용한다.
- [0092] 또한, 일부 실시예들에서, 가상 네트워크는 그 자신의 전용 프로토콜과 함께 클린-슬레이트(clean-slate) 통신 플랫폼을 이용한다. 데이터 메시지가 소프트웨어 전적으로 MFN 라우터를 통해(예를 들어, 소프트웨어 CFE를 통해) 포워딩되는 실시예들에서, 가상 네트워크는 장거리 중단간 접속(long-haul end-to-end connection)을 위해 최적화된 레이트 제어를 제공할 수 있다. 이것은 일부 실시예들에서 모든 MFN(150)에서 TCP 최적화 프록시 엔진(220)을 동작시킴으로써 달성된다. (예를 들어, HTTPS로) TCP 자체를 중단하지 않는 다른 실시예들에서, 이것은, 프록시 엔진(220)이 TCP 수신자-윈도우 및 ACK 조작과 함께 중간 흐름당 버퍼링을 이용하여 레이트 제어를 세그먼트화함으로써 달성된다.
- [0093] 클린 슬레이트 속성으로 인해, 일부 실시예들에서의 가상 네트워크는 훨씬 더 나은 서비스를 제공하기 위해 많은 컴포넌트를 최적화한다. 예를 들어, 일부 실시예들에서, 가상 네트워크는 다중-경로 라우팅을 이용하여 가상 네트워크를 가로질러 라우팅되는 프리미엄 대역폭-보장형 VPN 셋업을 지원한다. 일부 실시예들에서, 이러한 VPN은 ATM/MPLS 라우팅과 유사한 상태 데이터를 각각의 MFN에 포함하며, 그들의 확립 및 제거는 중앙 제어된다. 일부 실시예들은, 송출 링크당 가용 대역폭을, (패킷 쌍 또는 유사한 프로세스를 통해) 직접 측정함으로써 또는 링크에 대해 주어진 용량을 갖고 이 링크로부터 이미 전송된 트래픽을 이 용량으로부터 감소시킴으로써 식별한다.
- [0094] 일부 실시예들은 링크의 잔여 대역폭을 제약으로서 이용한다. 예를 들어, 한 링크가 적어도 2 Mbps의 가용 대역폭을 갖지 않을 때, 일부 실시예들의 제어기 클러스터는, 임의의 목적지로의 최저 비용 경로(예를 들어, 최단 경로)를 계산하는데 이용되는 링크 세트로부터 그 링크를 제거한다(예를 들어, 그래프 400 등의, 라우팅 그래프

에서 링크를 제거한다). 이 링크의 제거 후에도 중단간 경로가 여전히 이용가능하다면, 새로운 VPN들이 이 새로운 경로를 통해 라우팅될 것이다. VPN 제거는, 가용 용량을 주어진 링크에 다시 가져 와서, 이 링크가 최저 비용 경로(예를 들어, 최단 경로) 계산에 포함될 수 있게 한다. 일부 실시예들은, 다중 경로에 걸친 트래픽의 부하 밸런싱 등의 다중-경로 라우팅을 위한 다른 옵션, 예를 들어, MPTCP(다중-경로 TCP)를 이용한다.

[0095] 일부 실시예들은, 가상 네트워크 내에서 2개의 분리된 경로(예를 들어, 최대 분리된 경로)를 통해 유입 MFN으로부터 유출 MFN으로 트래픽을 복제하기 위해 경로 병렬화 및 저렴한 클라우드 링크를 활용함으로써 프리미엄 고객에게 더 나은 서비스를 제공한다. 이 접근법 하에서, 도착한 가장 이른 메시지가 수락되고, 나중의 메시지는 폐기된다. 이 접근법은, 유출 처리 복잡성을 증가시키는 댓가로, 가상 네트워크 신뢰성을 증가시키고 지연을 감소시킨다. 일부 이러한 실시예들에서, 중복 트래픽을 감소시키면서 신뢰성을 증가시키기 FEC(Forward Error Correction) 기술이 이용된다. 클린 슬레이트 속성으로 인해, 일부 실시예들의 가상 네트워크는, 애플리케이션-계층 최적화(예를 들어, 중복 제거 및 캐싱 동작) 및 보안 최적화(예를 들어, 암호화의 추가, DPI(심층 패킷 검사) 및 방화벽) 등의, 다른 상위 계층 최적화를 수행한다.

[0096] 일부 실시예들의 가상 네트워크는, 애니캐스트 메시징(anycast messaging)을 이용함으로써 가상 네트워크 셋업을 더욱 개선하기 위해 클라우드 제공자와의 협업을 감안한다. 예를 들어, 일부 실시예들에서, 모든 MFN들이 동일한 외부 IP 주소를 획득할 때, 임의의 새로운 회사 컴퓨팅 노드를 애니캐스트 접속을 이용하여 최적의 엣지 노드(예를 들어, 가장 가까운 엣지 노드)에 접속하는 것이 더 용이하다. 마찬가지로, 임의의 SaaS 제공자는 이 IP 주소를 획득하여 최적의 MFN(예를 들어, 가장 가까운 MFN)에 접속할 수 있다.

[0097] 위에서 언급된 바와 같이, 상이한 실시예들은 상이한 유형들의 VPN 접속을 이용하여 회사 컴퓨팅 노드(예를 들어, 지부 및 모바일 디바이스)를 회사 엔티티의 가상 네트워크를 확립하는 MFN에 접속한다. 일부 실시예들은 IPsec을 이용하여 이들 VPN 접속을 셋업한다. 도 6은 일부 실시예들의 IPsec 데이터 메시지 포맷을 나타낸다. 구체적으로, 이 도면은, 회사 컴퓨팅 노드에 있는 머신에 의해 생성된 데이터 메시지(605), 및 IPsec 터널을 통한 (예를 들어, MFN으로의 또는 회사 컴퓨팅 노드로의) 전송을 위해 (예를 들어 회사 컴퓨팅 노드 또는 MFN에서) 데이터 메시지(605)가 캡슐화된 후의 IPsec 캡슐화된 데이터 메시지(610)의 원래의 포맷을 나타낸다.

[0098] 이 예에서, IPsec 터널은 ESP 터널 모드, 포트 50을 이용하여 셋업된다. 도시된 바와 같이, 이 모드는, 이 예에서는, IP 헤더 내의 TCP 프로토콜 식별자를 ESP 프로토콜 식별자로 대체함으로써 셋업된다. ESP 헤더는, 메시지(615)의 시작(즉, 헤더(620) 및 페이로드(625))을 식별한다. 메시지(615)는, IPsec 캡슐화된 데이터 메시지의 수신자에 의해(예를 들어, MFN의 IPsec 게이트웨이에 의해) 인증되어야 한다. 페이로드(625)의 시작은 메시지(615)의 다음 필드(622)의 값에 의해 식별된다. 또한, 페이로드(625)는 암호화된다. 이 페이로드는, 원본 데이터 메시지(605)의 IP 헤더, TCP 헤더 및 페이로드뿐만 아니라, 다음 필드(622)를 포함하는 패딩 필드(630)를 포함한다.

[0099] 일부 실시예들에서, 각각의 MFN IPsec 게이트웨이는 동일하거나 상이한 가상 네트워크 임차인에 대한(예를 들어, 동일한 회사 또는 상이한 회사들에 대한) 복수의 IPsec 접속을 처리할 수 있다. 따라서, 일부 실시예들에서의 MFN IPsec 게이트웨이(예를 들어, 게이트웨이(230))는, 터널 ID, 임차인 ID(TID) 및 회사 컴퓨팅 노드 서브넷의 관점에서 각각의 IPsec 접속을 식별한다. 일부 실시예들에서, 임차인의 상이한 회사 노드들(예를 들어, 상이한 지사들)은 (RFC 1579에 따라) 중첩되는 IP 서브넷을 갖지 않는다. 일부 실시예들에서의 IPsec 게이트웨이는, (IPsec 터널 헤더에 포함된) 각각의 IPsec 터널 ID를 임차인 ID에 맵핑하는 테이블을 갖는다. IPsec 게이트웨이가 처리하도록 구성된 주어진 임차인의 경우, IPsec 게이트웨이는 또한, MFN들 및 그들의 클라우드 포워딩 요소들에 의해 확립된 가상 네트워크에 접속되는 그 임차인의 모든 서브넷의 맵핑을 갖는다.

[0100] 제1 공용 클라우드 데이터센터 내의 유입 제1 MFN이 IPsec 터널을 통해 임차인 ID와 연관되고 제2 공용 클라우드 데이터센터 내의 유출 제2 MFN에 접속된 목적지(예를 들어, 지부 또는 데이터센터 서브넷, 또는 SaaS 제공자)로 예정된 데이터 메시지를 수신할 때, 제1 MFN의 IPsec 게이트웨이는 IPsec 터널 헤더를 제거한다. 일부 실시예들에서, 그 다음, 제1 MFN의 CFE는, 메시지가, 유입 제1 MFN으로부터 유출 제2 MFN까지의 경로를 직접 횡단하거나 또는 하나 이상의 다른 중간 MFN을 통해 횡단하는 것을 허용하는 2개의 캡슐화 헤더로 메시지를 캡슐화한다. 제1 MFN의 CFE는 그 제어기-구성된 라우팅 테이블을 이용함으로써 이 경로를 식별한다.

[0101] 앞서 언급된 바와 같이, 일부 실시예들에서의 2개의 캡슐화 헤더는, (1) 캡슐화된 데이터 메시지가 가상 네트워크의 MFN들을 통해 횡단하여 유출 MFN CFE에 도달하는 것을 허용하기 위해 다음 홉 MFN CFE를 명시하는 외측 헤더, 및 (2) 가상 네트워크에 출입하는 데이터 메시지의 MFN들을 식별하는 유입 및 유출 MFN CFE들 및 임차인 ID를 명시하는 내측 헤더를 포함한다.

- [0102] 구체적으로, 일부 실시예들에서, 내측 캡슐화 헤더는, 유출 제2 MFN의 CFE의 목적지 IP 주소 및 유입 제1 MFN의 CFE의 소스 IP 주소를 갖는 유효한 IP 헤더를 포함한다. 이 접근법은, 표준 IP 라우터 소프트웨어가 MFN의 모든 CFE에서 이용되는 것을 허용한다. 캡슐화는 임차인 ID(예를 들어, 고객 CID)를 더 포함한다. 메시지가 유출 제2 MFN의 CFE에 도달하면, 메시지는 제2 MFN에 의해 캡슐화되어 그 목적지로 전송된다(예를 들어, 임차인 ID 및 메시지의 목적지 서브넷과 연관된 또 다른 IPsec 터널을 통해 제2 MFN의 IPsec 게이트웨이에 의해 목적지로 전송된다).
- [0103] 소정의 클라우드 제공자는, 머신이 소스 IP를 "스푸핑(spoofing)"하는 것을 금지하거나 및/또는 TCP 및 UDP 트래픽에 대한 다른 제약을 적용한다. 이러한 가능한 제약을 다루기 위해, 일부 실시예들은 외측 헤더를 이용하여 하나 이상의 경로에 의해 이용되는 이웃하는 MFN들의 쌍을 접속한다. 일부 실시예들에서의 이 헤더는, 소스 및 목적지 IP 주소 및 UDP 프로토콜 파라미터를 명시하는 UDP 헤더이다. 일부 실시예들에서, 유입 MFN CFE는 그 외부 IP 주소를 외측 헤더의 소스 IP 주소로서 명시하는 반면, 다음 MFN CFE 홉의 IP 주소를 외측 헤더의 목적지 IP 주소로서 명시한다.
- [0104] 유출 MFN의 CFE로의 경로가 하나 이상의 중간 MFN CFE를 포함할 때, 중간 CFE는 자신이 수신하는 이중-캡슐화된 메시지의 외측 헤더 내의 소스 IP 주소를 그 IP 주소로 대체한다. 이것은 또한, 내측 헤더 내의 목적지 IP 주소를 이용하여 라우팅 테이블에서 경로 조회를 수행해 내측 헤더의 목적지 IP 주소까지의 경로에 있는 다음 홉 MFN CFE의 목적지 IP 주소를 식별한다. 그 다음, 중간 CFE는 외측 헤더 내의 목적지 IP 주소를 경로 테이블 조회를 통해 식별한 IP 주소로 대체한다.
- [0105] 이중 캡슐화된 데이터 메시지가 유출 MFN의 CFE에 도달하면, CFE는, 내측 헤더에서 목적지 IP 주소를 회수할 때 자신이 데이터 메시지에 대한 유출 노드라고 결정하고 이 목적지 IP 주소가 자신에 속한다고 결정한다. 그 다음, 이 CFE는 데이터 메시지로부터 2개의 캡슐화 헤더를 제거한 다음, 목적지에 전송한다(예를 들어, 그 MFN의 IPsec 게이트웨이를 통해, 데이터 메시지의 원본 헤더 내의 목적지 IP 주소 또는 서브넷 및 임차인 ID와 연관된 또 다른 IPsec 터널을 통해 목적지로 전송한다).
- [0106] 도 7은 일부 실시예들의 2개의 캡슐화 헤더의 한 예를 나타내는 반면, 도 8은 일부 실시예들에서 이들 2개의 헤더가 어떻게 이용되는지를 나타내는 한 예를 제시한다. 아래의 논의에서, 내측 헤더는, 임차인의 회사 컴퓨팅 엔드 노드에 접속된 가상-네트워크 유입/유출 노드들의 신원과 함께 임차인 ID를 포함하므로 임차인 헤더라고 지칭된다. 외측 헤더는, 데이터 메시지가 유입 및 유출 MFN CFE들 사이에서 가상 네트워크를 통한 경로를 횡단할 때 가상 네트워크를 통한 다음 홉을 식별하는데 이용되므로 이하에서는 VN-홉 터널 헤더라고 지칭된다.
- [0107] 도 7은, 원본 데이터 메시지(750)를 원본 헤더(755) 및 페이로드(760)로 캡슐화하는 VN-홉 터널 헤더(705) 및 임차인 터널 헤더(720)를 도시한다. 도시된 바와 같이, 일부 실시예들에서의 VN-홉 터널 헤더(705)는 UDP 헤더(710) 및 IP 헤더(715)를 포함한다. 일부 실시예들에서의 UDP 헤더는 UDP 프로토콜에 따라 정의된다. 일부 실시예들에서, VN-홉 터널은 표준 UDP 터널인 반면, 다른 실시예에서는 이 터널은 전용 UDP 터널이다. 또 다른 실시예에서, 이 터널은 표준 또는 전용 TCP 터널이다. 일부 실시예들에서의 터널 헤더(705)는 그 페이로드를 암호화하는 암호화된 것인 반면, 다른 실시예에서는 암호화되지 않은 터널이다.
- [0108] 아래에 더 설명되는 바와 같이, 일부 실시예들에서의 터널 헤더(705)는 오버레이 VNP 네트워크를 정의하는데 이용되고, 언더레이 공용 클라우드 네트워크(underlay public cloud network)를 통해 다음 홉 MFN CFE에 도달하기 위해 각각의 MFN CFE에 의해 이용된다. 따라서, 터널 헤더(705)의 IP 헤더(715)는, VNP 터널에 의해 접속된 제1 및 제2 이웃 MFN들의 제1 및 제2 CFE들의 소스 및 목적지 IP 주소들을 식별한다. 일부 경우에(예를 들어, 다음 홉 목적지 MFN이 소스 MFN과는 상이한 공용 클라우드 벤더의 상이한 공용 클라우드에 있을 때), 소스 및 목적지 IP 주소는 MFN들을 포함하는 공용 클라우드 데이터센터들에 의해 이용되는 공용 IP 주소이다. 다른 경우에, 소스 및 목적지 MFN CFE가 동일한 공용 클라우드에 속할 때, 소스 및 목적지 IP 주소는 공용 클라우드에서만 이용되는 사설 IP 주소일 수 있다. 대안으로서, 이러한 경우, 소스 및 목적지 IP 주소는 여전히 공용 클라우드 벤더의 공용 IP 주소일 수 있다.
- [0109] 도 7에 도시된 바와 같이, 임차인 터널 헤더(720)는, IP 헤더(725), 임차인 ID 필드(730) 및 가상 회로 라벨(VCL)(735)을 포함한다. 임차인 터널 헤더(720)는, 데이터 메시지를 유출 MFN의 유출 CFE에 포워딩하기 위한 다음 홉을 식별하기 위해 유입 홉 CFE 이후의 각각의 홉 CFE에 의해 이용된다. 따라서, IP 헤더(725)는, 유입 CFE의 IP 주소인 소스 IP 주소, 및 유출 CFE의 IP 주소인 목적지 IP 주소를 포함한다. VN-홉 헤더(705)의 소스 및 목적지 IP 주소에서와 같이, 임차인 헤더(720)의 소스 및 목적지 IP 주소는, 하나의 공용 클라우드 제공자의 사설 IP 주소이거나(데이터 메시지가 하나의 공용 클라우드 제공자의 데이터센터만을 거쳐가는 경로를 횡단할

때), 하나 이상의 공용 클라우드 제공자의 공용 IP 주소일 수 있다(예를 들어, 데이터 메시지가 2개 이상의 공용 클라우드 제공자의 데이터센터를 거쳐가는 경로를 횡단할 때).

[0110] 임차인 헤더(720)의 IP 헤더는, 일부 실시예들에서 임의의 표준 소프트웨어 라우터 및 IP 라우팅 테이블을 이용함으로써 라우팅될 수 있다. 임차인 ID 필드(730)는, 임차인을 고유하게 식별하기 위해 유입 및 유출 MFN들에서 이용될 수 있는 고유 임차인 식별자인 임차인 ID를 포함한다. 일부 실시예들에서의 가상 네트워크 제공자는, 제공자의 임차인들인 상이한 회사 엔티티들에 대해 상이한 임차인 ID들을 정의한다. VCL 필드(735)는, 일부 실시예들이 네트워크를 통해 메시지를 포워딩하기 위한 대안적인 방식(비 IP-기반의 방식)을 제공하기 위해 이용하는 임의적 라우팅 필드이다. 일부 실시예들에서, 임차인 터널 헤더(720)는 GUE(Generic UDP Encapsulation) 헤더이다.

[0111] 도 8은 이들 2개의 터널 헤더(705 및 710)가 일부 실시예들에서 어떻게 이용되는지를 나타내는 한 예를 제시한다. 이 예에서, 데이터 메시지(800)는, 회사의 제1 지사(805)의 제1 머신(802)(예를 들어, 제1 VM)으로부터 회사의 제2 지사(810)의 제2 머신(804)(예를 들어, 제2 VM)으로 전송된다. 2개의 머신은, 10.1.0.0 및 10.2.0.0 인 상이한 2개의 서브넷에 있고, 여기서, 제1 머신은 IP 주소 10.1.0.17을 갖고 제2 머신은 IP 주소 10.2.0.22를 갖는다. 이 예에서, 제1 지사(805)는 제1 공용 클라우드 데이터센터(830) 내의 유입 MFN(850)에 접속되는 반면, 제2 지사(810)는 제2 공용 클라우드 데이터센터(838) 내의 유출 MFN(855)에 접속된다. 또한, 이 예에서, 제1 및 제2 공용 클라우드 데이터센터 내의 유입 및 유출 MFN(850 및 855)은, 제3 공용 클라우드 데이터센터(836)의 중간 MFN(857)을 통해 간접적으로 접속된다.

[0112] 도시된 바와 같이, 머신(802)으로부터의 데이터 메시지(800)는, 제1 지사(805)를 유입 MFN(850)에 접속하는 IPsec 터널(870)을 따라 유입 MFN(850)에 전송된다. 이 IPsec 터널(870)은, 제1 지사의 IPsec 게이트웨이(848)와 유입 MFN(850)의 IPsec 게이트웨이(852) 사이에 확립된다. 이 터널은, 데이터 메시지(800)를 IPsec 터널 헤더(806)로 캡슐화함으로써 확립된다.

[0113] MFN(850)의 IPsec 게이트웨이(852)는, 데이터 메시지를 캡슐화해제하고(즉, IPsec 터널 헤더(806)를 제거하고), 캡슐화해제된 메시지를, 직접 또는 하나 이상의 미들박스 서비스를 통해(예를 들어, 도 2의 머신(210) 등의, 방화벽 머신을 통해), 이 MFN의 CFE(832)에 전달한다. 이 메시지를 전달함에 있어서, 일부 실시예들에서의 MFN(850)의 IPsec 게이트웨이 또는 어떤 다른 모듈은 메시지를 IPsec 터널의 터널 ID 및 회사의 임차인 ID와 연관시킨다. 이 임차인 ID는 가상 네트워크 제공자의 레코드에서 회사를 식별한다.

[0114] 연관된 임차인 ID 및/또는 IPsec 터널 ID에 기초하여, 유입 MFN(850)의 CFE(832)는, 상이한 공용 클라우드 데이터센터들 내의 MFN들에 의해 확립된 가상 네트워크를 통한 그 목적지 머신의 서브넷으로의(즉, 제2 지사(810))로의) 메시지에 대한 경로를 식별한다. 예를 들어, CFE(832)는 임차인 ID 및/또는 IPsec 터널 ID를 이용하여 회사에 대한 라우팅 테이블을 식별한다. 이 라우팅 테이블에서, CFE(832)는, 그 다음, 수신된 메시지의 목적지 IP 주소 10.2.0.22를 이용하여, 공용 클라우드 데이터센터(838)의 유출 MFN(855)의 CFE(853)를 식별하는 레코드를, 데이터 메시지(800)에 대한 목적지 유출 포워딩 노드로서 식별한다. 일부 실시예들에서, 식별된 레코드는 제2 지사(810)의 전체 서브넷 10.2.0.0/16을 MFN(855)의 CFE(853)에 맵핑한다.

[0115] 유출 CFE(853)를 식별한 후, 유입 MFN(850)의 CFE(832)는, 수신된 데이터 메시지를, 그 IP 헤더(725)에서 유입 CFE(832)의 소스 IP 및 유출 CFE(853)의 목적지 IP를 포함하는 임차인 터널 헤더(860)로 캡슐화한다. 일부 실시예들에서, 이들 IP 주소는 공용 IP 주소 공간에서 정의된다. 터널 헤더(860)는 또한, 유입 MFN(850)에서 데이터 메시지와 연관된 임차인 ID를 포함한다. 위에서 언급된 바와 같이, 이 터널 헤더는 또한, 일부 실시예들에서 VCL 헤더 값을 포함한다.

[0116] 일부 실시예들에서, 유입 CFE(832)는 또한, 유출 CFE(853)로의 원하는 CFE 라우팅 경로에 있는 다음 홉 MFN을 식별한다. 일부 실시예들에서, 유입 CFE(832)는, 유출 CFE(853)의 목적지 IP 주소를 이용함으로써 라우팅 테이블에서 이 다음 홉 CFE를 식별한다. 이 예에서의 다음 홉 MFN CFE는, 제3 공용 클라우드 데이터센터(836)의 제3 MFN(857)의 CFE(856)이다.

[0117] 다음 홉 MFN CFE를 식별한 후, 유입 MFN CFE는 캡슐화된 데이터 메시지(800)를 VN-홉, 제2 터널 헤더(862)로 캡슐화한다. 이 터널 헤더는 메시지가 다음 홉 CFE(856)로 라우팅되는 것을 허용한다. 이 외측 헤더(862)의 IP 헤더(715)에서, 유입 MFN CFE(832)는, 소스 및 목적지 IP 주소를, 유입 CFE(832)의 소스 IP 및 중간 CFE(856)의 목적지 IP로서 명시한다. 이것은 또한, 일부 실시예들에서 그 계층 4 프로토콜을 UDP인 것으로서 명시한다.

[0118] 제3 MFN(857)의 CFE(856)가 이중-캡슐화된 데이터 메시지를 수신하면, VN-홉, 제2 터널 헤더(862)를 제거하고,

임차인 헤더(860)로부터, 유출 MFN(855)의 CFE(853)의 목적지 IP 주소를 추출한다. 이 IP 주소는 CFE(856)와 연관되어 있지 않으므로, 데이터 메시지는 목적지에 도달하기 위해 또 다른 MFN으로 여전히 횡단해야 한다. 따라서, CFE(856)는 추출된 목적지 IP 주소를 이용하여 라우팅 테이블에서 다음 홉 MFN CFE(853)를 식별하는 레코드를 식별한다. 이것은, 그 다음, 데이터 메시지를 외측 헤더(705)로 재캡슐화 변경하고, 그 IP 헤더(715)의 소스 및 목적지 IP 주소를 자 자신의 IP 주소 및 MFN CFE(853)의 목적지 IP 주소로서 명시한다. 그 다음, CFE(856)는 공용 클라우드 데이터센터(836 및 838)의 개재하는 라우팅 패브릭을 통해 이중-캡슐화된 데이터 메시지(800)를 유출 CFE(853)에 포워딩한다.

[0119] 캡슐화된 데이터 메시지를 수신한 후, 유출 CFE(853)는 내측 헤더(860)에서 목적지 IP 주소를 회수할 때는 캡슐화된 메시지가 자신에게 향한다고 결정하고 이 목적지 IP 주소가 자신에 속하는 것으로 결정한다. 유출 CFE(853)는 데이터 메시지(800)로부터 양쪽 모두의 캡슐화 헤더(860 및 862)를 제거하고 데이터 메시지의 원본 헤더에서 목적지 IP 주소를 추출한다. 이 목적지 IP 주소는, 제2 지사의 서브넷에서 제2 머신(804)의 IP 주소를 식별한다.

[0120] 제거된 임차인 터널 헤더(860) 내의 임차인 ID를 이용하여, 유출 CFE(853)는 검색할 올바른 라우팅 테이블을 식별한 다음, 수신된 데이터 메시지의 원본 헤더 값으로부터 추출된 목적지 IP 주소에 기초하여 이 라우팅 테이블을 검색한다. 이 검색으로부터, 유출 CFE(853)는, 데이터 메시지를 그 목적지로 포워딩하는데 이용할 IPsec 접속을 식별하는 레코드를 식별한다. 그 다음, 이것은, IPsec 접속 식별자와 함께 데이터 메시지를 제2 MFN의 IPsec 게이트웨이(858)에 제공하고, 이 IPsec 게이트웨이(858)는, 이 메시지를 IPsec 터널 헤더(859)로 캡슐화한 다음, 이것을 제2 지사(810)의 IPsec 게이트웨이(854)로 포워딩한다. 그 다음, 게이트웨이(854)는 IPsec 터널 헤더를 제거하고 데이터 메시지를 목적지 머신(804)으로 포워딩한다.

[0121] 여러 개의 더 상세한 메시지-처리 예들이 이제 도 9 내지 도 15를 참조하여 설명될 것이다. 이들 예에서, 각각의 임차인 IPsec 인터페이스는, VNP 터널에서와 같이, 동일한 로컬 공용 IP 주소에 있다고 가정한다. 따라서, 일부 실시예들에서의 인터페이스는 단일 VRF(virtual routing and forwarding; 가상 라우팅 및 포워딩) 명칭공간에 부착된다. 이 VRF 명칭공간은 이하에서는 VNP 명칭공간이라고 지칭된다.

[0122] 도 9 내지 도 11은, 임차인의 2개의 상이한 외부 머신 위치(예를 들어, 지사들, 데이터센터들 등)의 2개의 컴퓨팅 디바이스들 사이에서 전송되는 메시지를 수신할 때 유입, 중간 및 유출 MFN들에 의해 각각 수행되는 메시지-처리 프로세스(900-1100)를 나타낸다. 일부 실시예들에서, 제어기 클러스터(160)는, 각각의 이러한 CFE가 임차인의 상이한 데이터 메시지 흐름들에 대한 유입, 중간 및 유출 CFE로서 역할하는 후보일 때, 각각의 MFN의 CFE를 유입, 중간 및 유출 CFE로서 동작하도록 구성한다.

[0123] 프로세스(900-1100)는 도 8 및 도 12의 2개의 예를 참조하여 아래에서 설명될 것이다. 위에서 언급한 바와 같이, 도 8은 데이터 메시지가 중간 MFN을 거쳐 유출 MFN에 도달하는 때의 한 예를 나타낸다. 도 12는 유입 및 유출 MFN들 사이에 중간 MFN을 포함하지 않는 한 예를 나타낸다. 구체적으로, 이 도면은, 2개의 지사가, 직접 접속된 2개의 MFN(1250 및 1255)을 갖는 2개의 공용 클라우드 데이터센터(1230 및 1238)에 접속될 때, 제1 지사(1205)의 제1 디바이스(1202)로부터 제2 지사(1220)의 제2 디바이스(1210)로 전송되는 데이터 메시지(1200)를 나타낸다. 도시된 바와 같이, 이들 예에서의 MFN들의 CFE들(1232 및 1253)은 각각의 MFN과 연관된 라우팅 동작을 수행한다.

[0124] 유입 MFN(850 및 1250)의 유입 CFE(예를 들어, 유입 CFE(832 또는 1232))는 일부 실시예들에서 프로세스(900)를 수행한다. 도 9에 도시된 바와 같이, 유입 프로세스(900)는, 수신된 데이터 메시지 내의 IPsec 터널의 식별자(예를 들어, 806 또는 1206)에 기초하여 임차인 라우팅 컨텍스트를 초기에 식별함으로써(905에서) 시작한다. 일부 실시예들에서, IPsec 게이트웨이 또는 다른 MFN 모듈은, IPsec 터널 ID에 대한 임차인 ID를 맵핑 테이블에 저장한다. 특정한 IPsec 터널을 따라 데이터 메시지가 수신될 때마다, IPsec 게이트웨이는 IPsec 터널 ID를 추출하고, 이 게이트웨이 또는 다른 MFN 모듈은, IPsec 터널 ID를 이용하여 맵핑 테이블을 참조하여 연관된 임차인 ID를 식별한다. 임차인 ID를 식별함으로써, 프로세스는 이용할 임차인 라우팅 테이블 또는 VRF 명칭공간의 임차인 부분을 식별한다.

[0125] 910에서, 프로세스는 식별된 IPsec 터널의 RX(수신) 카운터를 증가시켜 이 데이터 메시지 수신을 감안한다. 그 다음, 915에서, 프로세스는 식별된 임차인 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 임차인 부분에서) 경로 조회(예를 들어, 가장 긴 프리픽스 정합, LPM, 조회)를 수행하여 공용 클라우드 데이터센터를 통해 구축된 임차인의 가상 네트워크를 빠져 나가기 위한 유출 인터페이스의 IP 주소를 식별한다. 지부-대-지부 예의 경우, 유출 인터페이스는, 목적지 지부에 접속된 MFN의 유출 CFE(예를 들어, CFE 853 또는 1253)의 IP 주소이다.

- [0126] 920에서, 프로세스는 임차인 터널 헤더(예를 들어, 헤더 860 또는 1260)를 수신된 데이터 메시지에 추가하고, 유입 CFE(예를 들어, 유입 CFE 832 또는 1252)의 소스 IP 주소와 유출 CFE(예를 들어, 유출 CFE 853 또는 1253)의 목적지 IP 주소를 이 터널 헤더 내의 소스 및 목적지 IP 주소로서 내장한다. 임차인 헤더에서, 프로세스는 또한, (905에서 식별된) 임차인 ID를 임차인 헤더에 저장한다. 920에서, 프로세스는 임차인 헤더 외부에 VN-홉 터널 헤더(예를 들어, 헤더 862 또는 1262)를 추가하고 그 IP 주소를 소스 IP 주소로서 이 헤더에 저장한다. 프로세스는 또한, (920에서) VNP 터널 헤더의 UDP 파라미터(예를 들어, UDP 포트)를 명시한다.
- [0127] 그 다음, 925에서, 프로세스는 임차인에 대한 VN-전송 카운터를 증가시켜 이 데이터 메시지의 전송을 감안한다. 930에서, 프로세스는 식별된 VNP 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 VNP 부분에서) 경로 조회(예를 들어, LPM 조회)를 수행하여 이 데이터 메시지에 대한 다음 홉 인터페이스를 식별한다. 일부 실시예들에서, 이 경로 조회는 유출 CFE의 목적지 IP에 적어도 부분적으로 기초하는 LPM 조회(예를 들어, VRF 명칭공간의 VNP 부분에서)이다.
- [0128] 935에서, 프로세스는 다음 홉 유출 인터페이스가 유입 CFE의 로컬 인터페이스(예를 들어, 물리적 또는 가상 포트)인지를 결정한다. 만일 그렇다면, 프로세스는 (937에서) VN-홉 외측 터널 헤더 내의 목적지 IP 주소를 915에서 식별된 유출 인터페이스 IP 주소로서 정의한다. 그 다음, 940에서, 프로세스는 이중 캡슐화된 데이터 메시지를 그 로컬 인터페이스에 제공하여 목적지 유출 CFE로 포워딩될 수 있게 한다. 940 이후에, 프로세스(900)는 종료된다.
- [0129] 도 12는, 유입 CFE(1232)가 제1 지사(1205)의 디바이스(1202)로부터 수신하는 데이터 메시지(1200)에 대한 동작 (905-940)의 한 예를 나타낸다. 도시된 바와 같이, 이 CFE의 MFN(1250)은, 제1 지사(1205)의 IPsec 게이트웨이(1248)로부터 이 데이터 메시지를 IPsec 캡슐화된 메시지로써 IPsec 게이트웨이(1252)에서 수신한다. 유입 CFE(1232)는, 수신된 메시지(1200)를 (그 IPsec 헤더가 IPsec 게이트웨이(1252)에 의해 제거된 후) VN-홉 터널 헤더(1262) 및 임차인 터널 헤더(1260)로 캡슐화하고, 이 이중 캡슐화된 메시지를 공용 클라우드(1238)의 MFN(1255)의 유출 CFE(1253)에 포워딩한다. 도시된 바와 같이, 양쪽 터널 헤더(1260 및 1262) 모두의 소스 및 목적지 IP 주소는 이 예에서는 동일하다. 이들 2개 세트의 IP 주소들이 동일하다고 가정하면, 일부 실시예들은, 데이터 메시지가 CFE(856) 등의 어떠한 개재 CFE를 통해서도 라우팅되지 않을 때 외측 IP 헤더(1262)를 이용하는 것을 포기한다.
- [0130] 프로세스가, 다음 홉 유출 인터페이스가 유입 CFE의 로컬 인터페이스가 아니라 또 다른 라우터의 목적지 IP 주소인 것으로 (935에서) 결정할 때, 프로세스는, 다음 홉 중간 CFE(예를 들어, 중간 CFE 856)의 목적지 IP 주소를, VN-홉 터널 헤더의 목적지 IP 주소로서 VN-홉 터널 헤더에 (945에서) 내장한다.
- [0131] 그 다음, 950에서, 프로세스는 식별된 VNP 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 VNP 부분에서) 또 다른 경로 조회(예를 들어, LPM 조회)를 수행한다. 이번에는, 조회는 VNP 터널 헤더에서 식별된 중간 CFE의 IP 주소에 기초한다. 중간 CFE(예를 들어, CFE 856)는, 유입 CFE(예를 들어, CFE 832)에 대한 가상 네트워크 내의 다음 홉 CFE이므로, 라우팅 테이블은 중간 CFE에 전송된 데이터 메시지에 대한 로컬 인터페이스(예를 들어, 로컬 포트)를 식별한다. 따라서, VNP 라우팅 컨텍스트에서의 이 조회는, 유입 CFE가 (950에서) 이중 캡슐화된 메시지를 제공하는 로컬 인터페이스를 식별한다. 그 다음, 프로세스는 VN-중간 카운터를 (955에서) 증가시켜 이 데이터 메시지의 전송을 감안한다. 955 후에, 프로세스가 종료된다.
- [0132] 도 10은, 유출 MFN의 CFE(예를 들어, CFE 853 또는 1253)가 MFN에 접속된 회사 컴퓨팅 노드(예를 들어, 지사, 데이터센터, 원격 사용자 위치)로 포워딩되어야 하는 데이터 메시지를 수신할 때 일부 실시예들에서 수행하는 프로세스(1000)를 나타낸다. 도시된 바와 같이, 프로세스는 가상 네트워크와 연관된 인터페이스 상에서 데이터 메시지를 (1005에서) 초기에 수신한다. 이 메시지는, VN-홉 터널 헤더(예를 들어, 헤더 862 또는 1262) 및 임차인 터널 헤더(예를 들어, 헤더 860 또는 1260)로 캡슐화된다.
- [0133] 1010에서, 프로세스는 VN-홉 터널 헤더 내의 목적지 IP 주소가 그 CFE의 목적지 IP 주소(예를 들어, CFE 853 또는 1253의 IP 주소)라고 결정한다. 그 다음, 1015에서 프로세스는 2개의 터널 헤더를 제거했다. 그 다음, 프로세스는 제거된 임차인 터널 헤더로부터 임차인 ID를 회수한다(1020에서). 수신된 데이터 메시지를 감안하기 위해, CFE는, 그 다음, 추출된 임차인 ID에 의해 명시된 임차인에 대해 유지하는 RX(수신) 카운터를 증가시킨다 (1025에서).
- [0134] 그 다음, 1030에서, 프로세스는, 이 데이터 메시지의 다음 홉 인터페이스를 식별하기 위해 식별된 임차인 라우팅 컨텍스트에서(즉, 1020에서 추출된 임차인 ID에 의해 식별된 임차인의 라우팅 컨텍스트에서) 경로 조회(예를

들어, LPM 조회)를 수행한다. 프로세스는, 일부 실시예들에서, 수신된 데이터 메시지의 원본 헤더(예를 들어, 헤더 755) 내의 목적지 IP 주소에 기초하여 이 조회를 수행한다. 이 조회를 통해 식별된 레코드로부터, 프로세스(1000)는 데이터 메시지가 그 목적지에 전송되기 위해 거쳐야 할 IPsec 인터페이스를 식별한다. 따라서, 프로세스(1000)는, 캡슐화해제된 수신된 데이터 메시지를 그 MFN의 IPsec 게이트웨이(예를 들어, 게이트웨이 858 또는 1258)에 전송한다.

[0135] 그 다음, 이 게이트웨이는 데이터 메시지를 IPsec 터널 헤더(예를 들어, 터널 헤더 859 또는 1259)로 캡슐화하고 이것을 목적지 회사 컴퓨팅 노드(예를 들어, 목적지 지사)의 게이트웨이(예를 들어, 게이트웨이 854 또는 1254)로 포워딩하며, 여기서, 이것은 캡슐화해제되어 그 목적지로 포워딩된다. 1030 후에, CFE 또는 그 MFN은, 목적지 회사 컴퓨팅 노드로의 IPsec 접속(예를 들어, 게이트웨이를 854 및 858 사이, 또는 게이트웨이들 1254 및 1258 사이의 IPsec 접속)을 따라 메시지를 전송하기 위해 유지하는 카운터를 (1035에서) 증가시킨다.

[0136] 도 11은 중간 MFN의 CFE(예를 들어, CFE 856)가, 또 다른 MFN의 또 다른 CFE로 포워딩되어야 하는 데이터 메시지를 수신할 때 일부 실시예들에서 수행하는 프로세스(1100)를 나타낸다. 도시된 바와 같이, 프로세스는 가상 네트워크와 연관된 인터페이스 상에서 데이터 메시지를 (1105에서) 초기에 수신한다. 일부 실시예들에서, 이 메시지는, 2개의 터널 헤더, 즉, VN-터널 헤더(예를 들어, 헤더 862) 및 임차인 터널 헤더(예를 들어, 헤더 860)로 캡슐화된다.

[0137] 1110에서, 프로세스는, 이 터널 헤더 내의 목적지 IP 주소가 CFE의 목적지 IP 주소라고(예를 들어, CFE(856)의 목적지 IP 주소라고) 결정할 때 VN-홉 터널을 종료한다. 그 다음, 1115에서, 프로세스는 VN-홉 터널 헤더가 올바른 UDP 포트를 명시하는지를 결정한다. 그렇지 않으면, 프로세스는 종료된다. 그외의 경우, 1120에서, 프로세스는 VN-홉 터널 헤더를 제거한다. 수신된 데이터 메시지를 감안하기 위해, CFE는, 그 다음, 중간 홉 CFE로서 수신한 메시지들의 수를 정량화하기 위해 유지하는 RX(수신) 카운터를 (1125에서) 증가시킨다.

[0138] 1130에서, 프로세스는 식별된 VNP 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 VNP 부분에서) 경로 조회(예를 들어, LPM 조회)를 수행하여 이 데이터 메시지에 대한 다음 홉 인터페이스를 식별한다. 일부 실시예들에서, 이 경로 조회는, 내측 임차인 터널 헤더에서 식별되는 유출 CFE의 목적지 IP에 적어도 부분적으로 기초하는 (예를 들어, VRF 명칭공간의 VNP 명칭공간에서의) LPM 조회이다.

[0139] 그 다음, 프로세스는 다음 홉 유출 인터페이스가 중간 CFE의 로컬 인터페이스인지를 결정한다(1135에서). 만일 그렇다면, 프로세스는 (1140에서) VN-홉 터널 헤더를 데이터 메시지에 추가하고, 이 데이터 메시지는 임차인 터널 헤더로 이미 캡슐화되어 있다. 프로세스는, (1142에서), VN-홉 터널 헤더 내의 목적지 IP 주소를, 임차인 터널 헤더에 명시된 유출 CFE의 목적지 IP 주소로 설정한다. 이것은 또한, (1142에서) VN-홉 터널 헤더 내의 소스 IP 주소를 그 CFE의 IP 주소로 설정한다. 이 터널 헤더에서, 프로세스는 또한, UDP 속성(예를 들어, UDP 포트 등)도 설정한다.

[0140] 그 다음, 1144에서, 프로세스는 이중 캡슐화된 데이터 메시지를 (1130에서 식별된) 그 로컬 인터페이스에 제공하여 목적지 유출 CFE로 포워딩될 수 있게 한다. 이 VN-홉 터널 캡슐화해제 및 포워딩의 한 예는, 도 8의 CFE(856)의 동작들을 참조하여 위에서 설명되었다. 수신된 데이터 메시지를 감안하기 위해, CFE는, 그 다음, 중간 홉 CFE로서 전송한 메시지들의 수를 정량화하기 위해 유지하는 TX(전송) 카운터를 (1146에서) 증가시킨다. 1146 이후에, 프로세스(1100)는 종료된다.

[0141] 반면, 프로세스가, 다음 홉 유출 인터페이스가 그 CFE의 로컬 인터페이스가 아니라 또 다른 라우터의 목적지 IP 주소라고 (1135에서) 결정하면, 프로세스는 (1150에서) 이전에 VN-홉 터널 헤더를 제거한 데이터 메시지에 VN-홉 터널 헤더를 추가한다. 새로운 VN-홉 터널 헤더에서, 프로세스(1100)는, 그 CFE의 소스 IP 주소 및 다음 홉 중간 CFE의 (1130에서 식별된) 목적지 IP 주소를, VN-홉 터널 헤더의 소스 및 목적지 IP 주소로서 (1150에서) 내장한다. 이 VNP 터널 헤더는 또한, UDP 목적지 포트가 있는 UDP 계층 4 프로토콜을 명시한다.

[0142] 그 다음, 1155에서, 프로세스는 식별된 VNP 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 VNP 부분에서) 또 다른 경로 조회(예를 들어, LPM 조회)를 수행한다. 이번에는, 조회는 새로운 VN-홉 터널 헤더에서 식별된 다음 홉 중간 CFE의 IP 주소에 기초한다. 이 중간 CFE는 가상 네트워크 내의 현재의 중간 CFE의 다음-홉이므로, 라우팅 테이블은 다음-홉 중간 CFE에 전송된 데이터 메시지에 대한 로컬 인터페이스를 식별한다. 따라서, VNP 라우팅 컨텍스트에서 이 조회는, 현재의 중간 CFE가 이중 캡슐화된 메시지를 제공하는 로컬 인터페이스를 식별한다. 그 다음, 프로세스는 VN-중간 TX(전송) 카운터를 (1160에서) 증가시켜 이 데이터 메시지의 전송을 감안한다. 1160 후에, 프로세스가 종료된다.

- [0143] 도 13은, (예를 들어, 지사 내의) 임차인의 회사 컴퓨팅 디바이스로부터 (예를 들어, 또 다른 지사, 임차인 데이터센터 또는 SaaS 제공자 데이터센터 내의) 또 다른 임차인 머신에 전송된 임차인에 대한 메시지를 수신할 때 유입 MFN의 CFE에 의해 수행되는 메시지-처리 프로세스(1300)를 나타낸다. 도 9의 프로세스(900)는 이하에서 더 설명되는 바와 같이 이 프로세스(1300)의 서브세트이다. 도 13에 도시된 바와 같이, 프로세스(1300)는 인입 IPsec 터널의 식별자에 기초하여 임차인 라우팅 컨텍스트를 (905에서) 초기에 식별함으로써 시작한다.
- [0144] 1310에서, 프로세스는, 수신된 데이터 메시지의 헤더 내의 소스 및 목적지 IP 주소 양쪽 모두가 공용 IP 주소인지를 결정한다. 그렇다면, 프로세스는 (1315에서) 데이터 메시지를 삭제하고 수신된 데이터 메시지의 IPsec 터널에 대해 유지하는 누락 카운터(drop counter)를 증가시킨다. 1315에서, 프로세스는 임차인의 IPsec 터널을 통해 메시지를 수신할 때 공용 IP 주소에 및 공용 IP 주소로부터 어드레싱된 메시지를 수신하고 있지 않아야 하므로 카운터를 누락한다. 일부 실시예들에서, 프로세스(1300)는 또한, ICMP 에러 메시지를 소스 회사 컴퓨팅 머신에 다시 전송한다.
- [0145] 한편, 프로세스가, 데이터 메시지가 공용 IP 주소로부터 나와 또 다른 공용 IP 주소로 가고 있지 않다고 (1310에서) 결정하면, 프로세스는, 수신된 데이터 메시지의 헤더 내의 목적지 IP 주소가 공용 IP 주소인지를 (1320에서) 결정한다. 만일 그렇다면, 프로세스는, 프로세스(1300)의 시작에서 수행된 동작(905)을 제외하고, 도 9의 프로세스(900)를 수행하기 위해 1325로 천이한다. 1325 이후에, 프로세스(1300)는 종료된다. 한편, 프로세스(1300)가 수신된 데이터 메시지의 헤더 내의 목적지 IP 주소가 공용 IP 주소가 아니라고 (1320에서) 결정하면, 프로세스는 식별된 IPsec 터널의 RX(수신) 카운터를 (1330에서) 증가시켜 이 데이터 메시지의 수신을 감안한다.
- [0146] 그 다음, 프로세스(1300)는, 식별된 임차인 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 임차인 부분에서) 경로 조회(예를 들어, LPM 조회)를 (1335에서) 수행한다. 이 조회는, 공용 클라우드 데이터센터를 통해 구축된 임차인의 가상 네트워크를 빠져 나오기 위한 유출 인터페이스의 IP 주소를 식별한다. 도 13에 도시된 예에서, 프로세스(1300)는, 데이터 메시지가 SaaS 제공자 데이터센터 내의 머신을 위한 것일 때 조회 동작(1335)에 도달한다. 따라서, 이 조회는 임차인의 가상 네트워크를 벗어나 SaaS 제공자 머신에 도달하기 위한 유출 라우터의 IP 주소를 식별한다. 일부 실시예들에서, 모든 SaaS 제공자 경로들은, 하나의 경로 테이블에 또는 VRF 명칭공간의 한 부분에 설치되는 반면, 다른 실시예들에서는 상이한 SaaS 제공자들에 대한 경로들은 상이한 경로 테이블에 또는 상이한 VRF 명칭공간 부분들에 저장된다.
- [0147] 1340에서, 프로세스는, 수신된 데이터 메시지에 임차인 터널 헤더를 추가하고, 유입 CFE의 소스 IP 주소 및 유출 라우터의 목적지 IP 주소를, 이 터널 헤더의 소스 및 목적지 IP 주소로서 내장한다. 그 다음, 1345에서, 프로세스는 임차인에 대한 VN-전송 카운터를 증가시켜 이 데이터 메시지의 전송을 감안한다. 1350에서, 프로세스는, VNP 라우팅 컨텍스트에서(예를 들어, VRF 명칭공간의 VNP 부분에서)에서 경로 조회(예를 들어, LPM 조회)를 수행하여 그 로컬 인터페이스들 중 하나를 이 데이터 메시지에 대한 다음 홉 인터페이스로서 식별한다. 다음 홉이 (예를 들어, 다른 공용 클라우드 데이터센터 내의) 또 다른 CFE일 때, 일부 실시예들에서의 프로세스는 또한, 데이터 메시지를 VN-홉 헤더로 캡슐화하고, 그 CFE의 IP 주소 및 다른 CFE의 IP 주소를 VN-홉 헤더의 소스 및 목적지 주소로서 내장한다. 1355에서, 프로세스는 캡슐화된 데이터 메시지를 그 식별된 로컬 인터페이스에 제공하여 데이터 메시지가 유출 라우터로 포워딩될 수 있게 한다. 1355 이후에, 프로세스(1300)는 종료된다.
- [0148] 일부 경우에, 유입 MFN은, 그 CFE가 또 다른 MFN의 CFE를 거치지 않고 데이터 메시지의 목적지 머신으로 직접 포워딩할 수 있는 임차인에 대한 데이터 메시지를 수신할 수 있다. 일부 이러한 경우에, CFE가 임의의 임차인 특유의 정보를 임의의 다른 후속 VN 처리 모듈에 중계할 필요가 없거나 필요한 정보가 다른 메커니즘을 통해 후속 VN 처리 모듈에 제공될 수 있을 때 데이터 메시지는 임차인 헤더 또는 VN-홉 헤더로 캡슐화될 필요가 없다.
- [0149] 예를 들어, 임차인의 데이터 메시지를 외부 SaaS 제공자 데이터센터로 직접 포워딩하기 위해, 유입 MFN의 NAT 엔진(215)은, 이하에서 더 설명되는 바와 같이, 임차인 식별자에 기초하여 NAT 동작을 수행해야 할 것이다. 유입 MFN 내의 유입 CFE 또는 다른 모듈은, 임차인 식별자를 유입 MFN의 연관된 NAT 엔진(215)에 제공해야 한다. 유입 CFE 및 NAT 엔진이 동일한 컴퓨터에서 실행될 때, 일부 실시예들은 이 정보를 공유된 메모리 위치에 저장함으로써 이들 2개의 모듈들 사이에서 이 정보를 공유한다. 반면, CFE와 NAT 엔진이 동일한 컴퓨터에서 실행되지 않을 때, 일부 실시예들은 다른 메커니즘(예를 들어, 대역외 통신)을 이용하여 유입 CFE와 NAT 엔진 사이에서 임차인 ID를 공유한다. 그러나, 이러한 경우에, 다른 실시예들은 임차인 ID를 저장하고 유입 MFN의 상이한 모듈들 사이에서 이것을 공유하기 위해 캡슐화 헤더를 이용한다(즉, 대역내 통신을 이용한다).
- [0150] 아래에 더 설명되는 바와 같이, 일부 실시예들은, 임차인의 가상 네트워크 외부로 메시지를 전송하기 전에 데이터 메시지의 소스 IP/포트 주소에 관해 하나 또는 2개의 소스 NAT 동작을 수행한다. 도 14는 유출 라우터에서

수행되는 NAT 동작을 나타낸다. 그러나, 아래에 더 설명되는 바와 같이, 일부 실시예들은 유입 라우터에서 데이터 메시지에 대해 또 다른 NAT 동작을 수행하지만, 이러한 여분의 NAT 동작은 도 13을 참조하여 위에서 설명되지 않았다.

- [0151] 도 14는, 유출 라우터가 인터넷을 통해 SaaS 제공자 데이터센터에 포워딩되어야 하는 데이터 메시지를 수신할 때 일부 실시예들에서 수행하는 프로세스(1400)를 나타낸다. 도시된 바와 같이, 프로세스는 가상 네트워크와 연관된 인터페이스 상에서 데이터 메시지를 (1405에서) 초기에 수신한다. 이 메시지는 임차인 터널 헤더로 캡슐화된다.
- [0152] 1410에서, 프로세스는 이 터널 헤더 내의 목적지 IP 주소가 그 라우터의 목적지 IP 주소라고 결정하고, 따라서 임차인 터널 헤더를 제거한다. 그 다음, 프로세스는 제거된 터널 헤더로부터 임차인 ID를 회수한다(1415에서). 수신된 데이터 메시지를 감안하기 위해, 프로세스는, 추출된 임차인 ID에 의해 명시된 임차인에 대해 유지하는 RX(수신) 카운터를 증가시킨다(1420에서).
- [0153] 그 다음, 1425에서, 프로세스는, 데이터 메시지의 원본 헤더의 목적지 IP가 유출 라우터의 로컬 인터페이스(예를 들어, 로컬 포트)를 통해 도달가능한 공용 IP인지를 결정한다. 이 로컬 인터페이스는 VNP 터널과 연관되지 않은 인터페이스이다. 그렇지 않으면, 프로세스는 종료된다. 그 외의 경우, 프로세스는 이 메시지의 헤더 내의 데이터 메시지의 소스 IP/포트 주소를 변경하기 위해 소스 NAT 동작을 (1430에서) 수행한다. NAT 동작 및 이 동작을 수행하는 이유는, 도 16 및 도 17을 참조하여 아래에서 더 설명될 것이다.
- [0154] 1430 이후에, 프로세스는, 인터넷 라우팅 컨텍스트에서(즉, 라우팅 데이터의 인터넷 라우팅 부분, 예를 들어 라우터의 인터넷 VRF 명칭공간에서) 경로 조회(예를 들어, LPM 조회)를 (1435에서) 수행하여 이 데이터 메시지의 다음 홉 인터페이스를 식별한다. 프로세스는, 일부 실시예들에서, 수신된 데이터 메시지의 원본 헤더의 목적지 네트워크 주소(예를 들어, 목적지 IP 주소)에 기초하여 이 조회를 수행한다. 이 조회를 통해 식별된 레코드로부터, 프로세스(1400)는 데이터 메시지가 그 목적지에 전송되기 위해 거쳐야 할 로컬 인터페이스를 식별한다. 따라서, 1435에서, 프로세스(1400)는, 목적지로 포워딩하기 위해 소스 네트워크-주소 변환된 데이터 메시지를 그 식별된 로컬 인터페이스에 제공한다. 1435 이후, 프로세스는 메시지를 SaaS 제공자에게 전송하기 위해 유지하는 카운터를 (1440에서) 증가시킨 다음, 종료한다.
- [0155] 도 15는 SaaS 제공자 머신으로부터 임차인 머신으로 전송되는 메시지를 수신하는 유입 라우터에 의해 수행되는 메시지-처리 프로세스(1500)를 나타낸다. 도시된 바와 같이, 유입 프로세스(1500)는, 여러개의 또는 모든 SaaS 제공자 통신에 이용되는 공용 IP 주소를 갖는 전용 입력 인터페이스 상에서 데이터 메시지를 (1505에서) 초기에 수신함으로써 시작한다. 일부 실시예들에서, 이 입력 인터페이스는, 가상 네트워크와 통신하는데 이용되는 것과 같은 상이한 IP 주소를 갖는 상이한 인터페이스이다.
- [0156] 메시지를 수신한 후, 프로세스는, 수신된 데이터 메시지의 헤더에 포함된 목적지 IP 주소를 이용함으로써 공용 인터넷 라우팅 컨텍스트에서 경로 조회를 (1510에서) 수행한다. 이 조회에 기초하여, 프로세스는, 목적지 IP 주소가 로컬이고 인에이블된 NAT 동작과 연관되어 있는지를 (1515에서) 결정한다. 그렇지 않으면, 프로세스는 종료된다. 그외의 경우, 프로세스는 (1520에서) 인터넷 RX(수신) 카운터를 증가시켜 데이터 메시지 수신을 감안한다.
- [0157] 그 다음, 1525에서, 프로세스는, 데이터 메시지의 목적지 IP/포트 주소를 가상 네트워크가 특정한 임차인과 연관시키는 새로운 목적지 IP/포트 주소로 변환하는 역방향 NAT 동작을 수행한다. 이 NAT 동작은 또한, 임차인 ID를 생성한다(예를 들어, 임차인 ID를 변환된 목적지 IP와 연관시키는 맵핑 테이블로부터 임차인 ID를 회수하거나, 새로운 목적지 IP/포트 주소를 획득하는데 이용되는 동일한 맵핑 테이블로부터 임차인 ID를 회수한다). 일부 실시예들에서, 프로세스(1500)는, 프로세스(1400)가 (1430에서) SNAT 동작을 수행하여 (1525에서) 역방향 NAT 동작을 수행할 때 생성된 접속 레코드를 이용한다. 이 접속 레코드는, SNAT 및 DNAT 동작에 의해 이용되는 내부 및 외부 IP/포트 주소들 사이의 맵핑을 포함한다.
- [0158] 변환된 목적지 네트워크 주소에 기초하여, 프로세스는, 식별된 임차인 라우팅 컨텍스트에서(즉, 임차인 ID에 의해 명시된 라우팅 컨텍스트에서) 경로 조회(예를 들어, LPM 조회)를 (1530에서) 수행하여 임차인의 가상 네트워크를 벗어나 (예를 들어, 지사 내의) 회사 컴퓨팅 노드의 임차인 머신에 도달하기 위한 유출 인터페이스의 IP 주소를 식별한다. 이 유출 인터페이스는, 일부 실시예들에서 유출 MFN의 유출 CFE의 IP 주소이다. 1530에서, 프로세스는, 수신된 데이터 메시지에 임차인 터널 헤더를 추가하고, 유입 라우터의 IP 주소 및 유출 CFE IP 주소를, 이 터널 헤더의 소스 및 목적지 IP 주소로서 내장한다. 그 다음, 1535에서, 프로세스는 임차인에 대한

VN-전송 카운터를 증가시켜 이 데이터 메시지의 전송을 감안한다.

- [0159] 1540에서, 프로세스는, 식별된 VNP 라우팅 컨텍스트에서(예를 들어, 라우터의 VRF 명칭공간에서와 같이, 라우팅 데이터의 VNP 부분에서) 경로 조회(예를 들어, LPM 조회)를 수행하여 유입 라우터가 캡슐화된 메시지를 제공하는 그 로컬 인터페이스(예를 들어, 그 물리적 또는 가상 포트)를 식별한다. 그 다음, 프로세스는, 수신된 데이터 메시지에 VN-홉 헤더를 (1540에서) 추가하고, 유입 라우터의 IP 주소 및 다음 홉 CFE의 IP 주소를 이 VN-홉 헤더의 소스 및 목적지 IP 주소로서 내장한다. 1555 후에, 프로세스가 종료된다.
- [0160] 위에서 언급한 바와 같이, 일부 실시예들에서의 MFN은, 가상 네트워크 내로의 및 외부로의 데이터 메시지의 유입 및/또는 유출 경로에서 NAT 동작을 수행하는 NAT 엔진(215)을 포함한다. NAT 동작은 오늘날 많은 상황에서 및 많은 디바이스(예를 들어, 라우터, 방화벽 등)에 의해 흔하게 수행된다. 예를 들어, NAT 동작은, 전형적으로, 트래픽이 사설 네트워크를 빠져 나와 내부 IP 주소 공간을 인터넷에서 이용되는 규제된 공용 IP 주소 공간으로부터 분리할 때 수행된다. NAT 동작은 전형적으로 한 IP 주소를 또 다른 IP 주소에 맵핑한다.
- [0161] 인터넷에 접속된 컴퓨터들이 확산됨에 따라, 컴퓨터의 수가 이용가능한 IP 주소의 수를 초과할 것이라는 것이 해결과제이다. 불행히도, 4,294,967,296개의 가능한 고유한 주소가 있지만, 각각의 컴퓨터에 대해 고유한 공용 IP 주소를 할당하는 것은 이미 실용적이지 않다. 해결 방법 중 하나는, 사설 네트워크의 엣지 지점에 있는 라우터에만 공용 IP 주소를 할당하는 반면, 네트워크 내부의 다른 디바이스들은 그들의 내부 사설 네트워크에서만 고유한 주소를 갖는 것이다. 한 디바이스가 그 내부 사설 네트워크 외부의 디바이스와 통신하기를 원할 때, 그 트래픽은 전형적으로, NAT 동작을 수행하여 이 트래픽의 소스 IP를 인터넷 게이트웨이의 공용 소스 IP 주소로 대체하는 인터넷 게이트웨이를 통과한다.
- [0162] 사설 네트워크의 인터넷 게이트웨이는 인터넷 상에서 등록된 공용 주소를 얻지만, 이 게이트웨이에 접속된 사설 네트워크 내부의 각각의 디바이스는 등록되지 않은 사설 주소를 수신한다. 내부 사설 네트워크의 사설 주소는 임의의 범위의 IP 주소일 수 있다. 그러나 IETF(Internet Engineering Task Force)는 사설 네트워크가 이용할 여러 범위의 사설 주소들을 제안했다. 이들 범위는 일반적으로 공용 인터넷 상에서는 이용할 수 없어서, 라우터가 사설 주소와 공용 주소를 용이하게 구별할 수 있게 한다. 이들 사설 주소들의 범위는 RFC 1918로서 알려져 있고, 다음과 같다: (1) 클래스 A 10.0.0.0 - 10.255.255.255, (2) 클래스 B 172.16.0.0 - 172.31.255.255 및 (3) 클래스 C 192.168.0.0 - 192.168.255.255.
- [0163] 외부 디바이스들이 동일한 내부 IP 주소들을 이용하는 상이한 사설 네트워크들 내의 상이한 디바이스들을 구별할 수 있도록, 사설 네트워크를 빠져 나가는 데이터 메시지 흐름에 관해 소스 IP 변환을 수행하는 것이 중요하다. 외부 디바이스가 사설 네트워크 내부의 디바이스에 응답 메시지를 전송해야 할 때, 그 외부 디바이스는 인터넷 상의 고유하고 라우팅가능한 공용 주소로 그 응답을 전송해야 한다. 이것은 수많은 사설 네트워크의 수많은 디바이스에 의해 이용되는 내부 디바이스의 원본 IP 주소를 이용할 수 없다. 외부 디바이스는, 원래의 NAT 동작이 내부 디바이스의 사설 소스 IP 주소를 대체하는데 이용한 공용 IP 주소로 그 응답을 전송한다. 이 응답 메시지를 수신한 후, 사설 네트워크(예를 들어, 네트워크의 게이트웨이)는 또 다른 NAT 동작을 수행하여 응답 내의 공용 목적지 IP 주소를 내부 디바이스의 IP 주소로 대체한다.
- [0164] 사설 네트워크 내부의 많은 디바이스들 및 이들 디바이스들 상에서 실행되는 많은 애플리케이션들은, 사설 네트워크와 연관된 하나 또는 유한한 개수의 공용 IP 주소를 공유해야 한다. 따라서, NAT 동작은 전형적으로 또한, 계층 4 포트 주소(예를 들어, UDP 주소, TCP 주소, RTP 주소 등)를 변환하여 외부 메시지 흐름을 상이한 내부 머신들 및/또는 이들 내부 머신들 상의 상이한 애플리케이션들에서 시작하거나 종료하는 내부 메시지 흐름과 고유하게 연관시킬 수 있다. NAT 동작들은 또한, 많은 상황에서 이들 동작들이 접속을 추적하고, 테이블, 메시지 재조립, 타임아웃, 만료된 추적된 접속의 강제 종료 등을 동적으로 처리할 필요가 있기 때문에, 종종 상태유지 동작(stateful operation)이다.
- [0165] 앞서 언급된 바와 같이, 일부 실시예들의 가상 네트워크 제공자는 복수의 공용 클라우드를 통해 상이한 임차인들에게 가상 네트워크를 서비스로서 제공한다. 이들 임차인들은 그들의 사설 네트워크에서 공통 IP 주소들을 이용할 수 있고, 가상 네트워크 제공자의 공통 세트의 네트워크 자원들(예를 들어, 공용 IP 주소들)을 공유한다. 일부 실시예들에서, 상이한 임차인들의 데이터 트래픽은, 터널들을 통해 오버레이 네트워크의 CFE들 사이에서 운반되고 터널은 각각의 메시지를 고유한 임차인 ID로 마킹한다. 이들 임차인 식별자들은, 사설 임차인 IP 공간들이 중첩되는 때에도 메시지가 소스 디바이스에 다시 전송되는 것을 허용한다. 예를 들어, 임차인 식별자는, 소스 주소 10.5.12.1을 갖는 임차인(17)의 지사로부터 Amazon.com으로 전송된 메시지가, 동일한 소스 주소를 갖는(및 심지어 동일한 소스 포트 번호, 55331을 갖는) 임차인(235)의 지사로부터 Amazon.com으로 전송

된 메시지와 구별되는 것을 허용한다.

- [0166] RFC 1631에 따라 구현된 표준 NAT는 임차의 개념을 지원하지 않으므로, 결과적으로 동일한 사설 IP 주소를 가진 2개의 메시지를 구별할 방법이 없다. 그러나, 일부 실시예들의 많은 가상 네트워크 배치에서, 오늘날 많은 성숙한 오픈-소스 고성능 구현이 존재하기 때문에 표준 NAT 엔진을 이용하는 것이 유리하다. 사실상, 오늘날 많은 Linux 커널들은 NAT 엔진을 표준 피처로서 기능시키고 있다.
- [0167] 임차인 가상 네트워크의 상이한 임차인들에 대해 표준 NAT 엔진을 이용하기 위하여, 일부 실시예들의 가상 네트워크 제공자는 표준 NAT 엔진을 이용하기 전에 임차-맵핑(tenancy-mapping)(TM) 엔진을 이용한다. 도 16은, 인터넷으로의 가상 네트워크의 유출 경로에 있는 각각의 가상-네트워크 게이트웨이(1602)에 배치된 이러한 TM 엔진(1605)을 나타낸다. 도시된 바와 같이, 각각의 TM 엔진(1605)은, 인터넷(1625)을 통한 SaaS 제공자 데이터센터(1620)로의 메시지 유출 경로에서 NAT 엔진(1610) 앞에 배치된다. 일부 실시예들에서, MFN의 각각의 NAT 엔진(215)은, TM 엔진(TM 엔진(1605) 등) 및 표준 NAT 엔진(NAT 엔진(1610) 등의)을 포함한다.
- [0168] 도 16에 도시된 예에서, 메시지 흐름은 2개의 가상-네트워크 임차인들의 2개의 지사(1655 및 1660) 및 한 데이터센터(1665)로부터 나왔고, 동일한 유입 게이트웨이(1670)를 통해 가상 네트워크(1600)로 들어가지만, 이것은 반드시 그래야 할 필요는 없다. 일부 실시예들에서의 가상 네트워크(1600)는, 복수의 공용 클라우드 벤더의 복수의 공용 클라우드 데이터센터를 통해 정의된다. 일부 실시예들에서, 가상-네트워크 게이트웨이는 관리형 포워딩 노드의 일부이고, TM 엔진은 유출 MFN에서 NAT 엔진(1610) 앞에 배치된다.
- [0169] 데이터 메시지가 SaaS 제공자 데이터센터(1620)로 가는 도중에 가상 네트워크를 빠져 나가기 위해 유출 게이트웨이(1602)에 도달할 때, 각각의 TM 엔진(1605)은 이들 데이터 메시지들의 소스 네트워크 주소(예를 들어, 소스 IP 및/또는 포트 주소)를 새로운 소스 네트워크 주소(예를 들어, 소스 IP 및/또는 포트 주소)로 맵핑하고, NAT 엔진(1610)은 새로운 소스 네트워크 주소를 역시 또 다른 소스 네트워크 주소(예를 들어, 또 다른 소스 IP 및/또는 포트 주소)에 맵핑한다. 일부 실시예들에서, TM 엔진은 상태유지 없는 요소(stateless element)이고, 어떠한 동적 데이터 구조도 살피지않고 정적 테이블을 통해 각각의 메시지에 대한 맵핑을 수행한다. 상태유지 없는 요소로서, TM 엔진은, 데이터 메시지 흐름의 후속 메시지를 처리하기 위해 주소 맵핑을 수행하는데 있어서 이 접속 레코드를 이용하기 위하여 데이터 메시지 흐름 중 제1 데이터 메시지를 처리할 때 접속 레코드를 생성하지 않는다.
- [0170] 반면, 일부 실시예들에서의 NAT 엔진(1605)은, 그 이전의 SNAT 맵핑을 반영하는 접속 레코드를 저장하는 접속 스토리지를 참조하여 맵핑을 수행하는 상태유지 요소이다. NAT 엔진이 데이터 메시지를 수신할 때, 일부 실시예들에서의 이 엔진은 먼저, 접속 스토리지를 체크하여 수신된 메시지의 흐름에 대한 접속 레코드를 이전에 생성했는지를 결정한다. 만일 그렇다면, NAT 엔진은 이 레코드에 포함된 맵핑을 이용하여 SNAT 동작을 수행한다. 그외의 경우, 새로운 데이터 메시지 흐름에 대한 새로운 주소 맵핑을 도출하는데 이용하는 한 세트의 기준에 기초하여 SNAT 동작을 수행한다. 이를 위해, 일부 실시예들에서의 NAT 엔진은 일반적인 네트워크 주소 변환 기술을 이용한다.
- [0171] 일부 실시예들에서, NAT 엔진은 또한, 응답 데이터 메시지를 원래의 메시지를 전송한 임차인 머신에 포워딩하기 위해 DNAT 동작을 수행하기 위하여, SaaS 제공자 머신으로부터 응답 데이터 메시지를 수신할 때 일부 실시예들에서 접속 스토리지를 이용할 수 있다. 일부 실시예들에서, 각각의 처리된 데이터 메시지 흐름에 대한 접속 레코드는, 그 흐름의 식별자(예를 들어, 변환된 소스 네트워크 주소를 갖는 5개의 튜플 식별자)를 포함하는 레코드 식별자를 갖는다.
- [0172] 맵핑을 수행함에 있어서, TM 엔진은, 동일한 소스 IP 및 포트 주소를 이용하는 상이한 임차인들로부터의 데이터 메시지 흐름들이 고유의 중첩되지 않는 주소 공간에 맵핑되는 것을 보장한다. 각각의 메시지에 대해, TM 엔진은 임차인 ID를 식별하고 이 식별자에 기초하여 주소 맵핑을 수행한다. 일부 실시예들에서, TM 엔진은, 상이한 임차인들로부터의 임의의 2개의 메시지가 동일한 IP 주소에 맵핑되지 않도록, 상이한 임차인들의 소스 IP 주소들을 상이한 IP 범위들로 맵핑한다.
- [0173] 결과적으로, 상이한 임차인 ID를 갖는 각각의 네트워크 유형은, IP 주소의 전체 2^{32} 개 지역(0.0.0.0-255.255.255.255) 내의 고유한 주소로 맵핑될 것이다. 클래스 A 및 B 네트워크는, 클래스 C 네트워크보다 256 및 16배 더 많은 가능한 IP 주소를 갖는다. 클래스 A, B 및 C 네트워크들의 크기 비율을 고려하면, 256개의 클래스 A 네트워크는 다음과 같이 할당될 수 있다: (1) 240개는 240개 임차인을 클래스 A 네트워크와 맵핑, (2) 15개는 240개 임차인을 클래스 B 네트워크와 맵핑, 및 (3) 단일의 클래스 A 네트워크는 240개 임차인을 클래스

C 네트워크와 맵핑. 더 구체적으로는, 일부 실시예들에서, (0.x.x.x/24에서 시작하여, 1.x.x.x/24 ... 239.x.x.x/24까지의) 가장 낮은 범위의 클래스 A 네트워크들은, 10.x 클래스 A 네트워크로부터 나오는 주소들을 240개의 상이한 타겟 클래스 A 네트워크들에 맵핑하는데 이용될 것이다. 다음 15개의 클래스 A 네트워크 240.x.x.x/24 내지 254.x.x.x/24 각각은, 각각의 16개의 클래스 B 네트워크를 포함하는데 이용될 것이다(예를 들어, 총 240개의 네트워크(15*16)에 대해). 마지막 클래스 A 네트워크 255.x.x.x/24는 최대 256개의 사설 클래스 C 네트워크를 포함하는데 이용될 것이다. 256개의 임차인이 맞을 수 있지만, 240개만 이용되고 16개의 클래스 C 네트워크는 이용되지 않는다. 요약하면, 일부 실시예들은 다음과 같은 맵핑을 이용한다:

- [0174] ● 10.x.x.x/24 네트워크들 -> 1.x.x.x/24-239.x.x.x/24는, 각각의 임차인에 대해 240개의 상이한 맵핑을 야기한다;
- [0175] ● 172.16-31.x.x/12 네트워크들 -> 240.x.x.x/24-254.x.x.x/24는, 각각의 임차인에 대해 240개의 상이한 맵핑을 야기한다;
- [0176] ● 192.168.x.x/16 -> 255.x.x.x/24 네트워크들은, 각각의 임차인에 대해 256개의 가능한 맵핑 중 240개를 야기한다.
- [0177] 전술된 방식은, 어떤 유형의 네트워크 클래스를 임차인이 이용할지를 미리 알지 못한다고 가정할 때, 최대 240개의 임차인을 지원할 수 있다. 일부 실시예들에서, 공용 클라우드 네트워크는 사설 IP 주소를 이용한다. 이러한 경우, 다시 사설 주소 공간에 맵핑하지 않는 것이 바람직하다. 일부 실시예들은 클래스 A 네트워크 및 클래스 B 네트워크를 제거함에 따라, 이들 실시예에서 지원될 수 있는 단지 239개의 상이한 임차인들만이 존재한다. 고유한 맵핑을 달성하기 위해, 일부 실시예들은 모든 임차인 ID들을 1 내지 239까지 넘버링한 다음, 임차인 ID(8 비트로 표현됨) 모듈로 240에 대한 사설 도메인의 마스크되지 않은 부분의 최하위 8 비트에 더한다. 이 경우, 클래스 A 주소에 대해, 제1 임차인(번호 1)은, 11 xx.xx.xx/24에 맵핑되고, 마지막 임차인(239)은 9.xx.xx.xx/24에 맵핑될 것이다.
- [0178] 도 16에 도시된 구현에서, 일부 실시예들은, 임의의 잠재적인 임차인 ID 서브넷들 및 각각의 이러한 서브넷 내의 임의의 특정한 IP 주소에 다시 메시지를 라우팅하는 방식을 각각의 TM 엔진(1605)에 제공한다. 이 정보는, 임차인, 지부, 및 모바일 디바이스가 추가되거나 제거될 때 동적으로 변경될 수 있다. 따라서, 이 정보는 가상 네트워크의 인터넷 유출 게이트웨이 내의 TM 엔진들에 동적으로 배포되어야 한다. 가상 네트워크 제공자의 유출 인터넷 게이트웨이들이 많은 수의 임차인에 의해 이용될 수 있으므로 배포되고 정기적으로 업데이트되는 정보의 양이 많을 수 있다. 또한, 임차인 ID 240(또는 239)의 제약은 전역적이며 복수의 IP 주소를 유출 지점들에 추가해야만 해결될 수 있다.
- [0179] 도 17은 도 16에 나타난 단일 NAT 접근법 대신에 일부 실시예들에서 이용되는 이중-NAT 접근법을 나타낸다. 도 17에 나타난 접근법은 적은 임차인 데이터가, 전부는 아니더라도, 대부분의 TM 엔진에 배포될 것을 요구하고, 더 많은 사설 임차인 네트워크들이 가상 네트워크 제공자의 내부 네트워크에 맵핑되는 것을 허용한다. 임차인 머신으로부터 가상 네트워크(1700) 및 그 다음 인터넷(1625)을 통해 또 다른 머신으로(예를 들어, SaaS 제공자 데이터센터(1620)의 머신으로) 횡단하는 데이터 메시지 흐름에 대해, 도 17에 도시된 접근법은, 데이터 메시지 흐름의 유입 게이트웨이(1770)에 있는 NAT 엔진을 가상 네트워크 내에 배치하고 이 흐름의 유출 게이트웨이(1702 또는 1704)에 있는 NAT 엔진을 가상 네트워크 외부에 및 인터넷(1625) 내에 배치한다. 이 접근법은 또한, 유입 게이트웨이(1770)의 NAT 엔진(1712) 앞에 TM 엔진(1705)을 배치한다.
- [0180] 도 17에 도시된 예에서, 메시지 흐름은 2개의 가상-네트워크 임차인들의 2개의 지사(1755 및 1760) 및 한 데이터센터(1765)로부터 나왔고, 동일한 유입 게이트웨이(1770)를 통해 가상 네트워크(1700)로 들어가지만, 이것은 반드시 그래야 할 필요는 없다. 가상 네트워크(1600)처럼, 일부 실시예들에서의 가상 네트워크(1700)는 복수의 공용 클라우드 벤더의 복수의 공용 클라우드 데이터센터를 통해 정의된다. 또한, 일부 실시예들에서, 가상-네트워크 게이트웨이(1702, 1704 및 1770)는 관리형 포워딩 노드의 일부이며, TM 엔진은 이들 실시예에서 이들 MFN의 NAT 엔진(215) 앞에 배치된다.
- [0181] TM 엔진(1605 및 1705)은 도 16 및 17에서 유사하게 동작한다. TM 엔진(1605)처럼, TM 엔진(1705)은 가상 네트워크에 진입하는 데이터 메시지들의 소스 IP 및 포트 주소를, 이들 데이터 메시지가 SaaS 제공자 데이터센터(1620)를 향할 때(즉, SaaS 제공자 데이터센터에 대한 목적지 IP 주소를 가질 때), 새로운 소스 IP 및 포트 주소에 맵핑한다. 각각의 이러한 데이터 메시지에 대해, TM 엔진(1705)은 임차인 ID를 식별하고 이 식별자에 기초하여 주소 맵핑을 수행한다.

- [0182] TM 엔진(1605)처럼, 일부 실시예들에서의 TM 엔진(1705)은 상태유지 없는 요소이고, 어떠한 동적 데이터 구조도 살피지않고 정적 테이블을 통해 각각의 메시지에 대한 맵핑을 수행한다. 상태유지 없는 요소로서, TM 엔진은, 데이터 메시지 흐름의 후속 메시지를 처리하기 위해 주소 맵핑을 수행하는데 있어서 이 접속 레코드를 이용하기 위하여 데이터 메시지 흐름 중 제1 데이터 메시지를 처리할 때 접속 레코드를 생성하지 않는다.
- [0183] 맵핑을 수행함에 있어서, 유입 게이트웨이(1770) 내의 TM 엔진(1705)은, 동일한 소스 IP 및 포트 주소를 이용하는 상이한 임차인들로부터의 데이터 메시지 흐름들이 고유의 중첩되지 않는 주소 공간에 맵핑되는 것을 보장한다. 일부 실시예들에서, TM 엔진은, 상이한 임차인들로부터의 임의의 2개의 메시지가 동일한 IP 주소에 맵핑되지 않도록, 상이한 임차인들의 소스 IP 주소들을 상이한 IP 범위들로 맵핑한다. 다른 실시예들에서, TM 엔진(1705)은 2개의 상이한 임차인의 소스 IP 주소들을 동일한 소스 IP 범위이지만 상이한 소스 포트 범위들에 맵핑할 수 있다. 또 다른 실시예에서, TM 엔진은 2개의 임차인을 상이한 소스 IP 범위들에 맵핑하는 반면, 2개의 다른 임차인을 동일한 소스 IP 범위이지만 상이한 소스 포트 범위들에 맵핑한다.
- [0184] TM 엔진(1605)과는 달리, 가상-네트워크 유입 게이트웨이의 TM 엔진(1705)은 유입 게이트웨이에 접속된 지사, 회사 데이터센터 및 회사 컴퓨팅 노드에 대한 임차인을 식별할 필요만 있다. 이것은, 각각의 TM 엔진에 초기에 공급되고 주기적으로 업데이트되어야 하는 임차인 데이터를 크게 감소시킨다. 또한, 이전과 마찬가지로, 각각의 TM 엔진은 239/240 임차인들만 고유한 주소 공간에 맵핑할 수 있다. 그러나, TM 엔진들은 가상 네트워크 제공자의 유입 게이트웨이들에 배치되므로, TM 엔진들 각각은 239/240 임차인들을 고유하게 맵핑할 수 있다.
- [0185] 일부 실시예들에서의 유입 게이트웨이(1770)의 NAT 엔진(1712)은, 유입 게이트웨이(1770)가 상주하는 공용 클라우드(예를 들어, AWS, GCP 또는 Azure) 특유의 내부 IP 주소 또는 외부 공용 IP 주소를 이용할 수 있다. 어느 경우이든, NAT 엔진(1712)은 인입 메시지(즉, 가상 네트워크(1700)에 들어가는 메시지)의 소스 네트워크 주소를 그 유입 게이트웨이의 사설 클라우드 네트워크 내에서 고유한 IP 주소에 맵핑한다. 일부 실시예들에서, NAT 엔진(1712)은 각각의 임차인 데이터 메시지 흐름의 소스 IP 주소를 상이한 고유한 IP 주소로 변환한다. 그러나, 다른 실시예들에서, NAT 엔진(1712)은 상이한 임차인들의 데이터 메시지 흐름의 소스 IP 주소를 동일한 IP 주소로 변환하지만, 상이한 임차인들의 데이터 메시지 흐름들을 구분하기 위해 소스 포트 주소들을 이용한다. 또 다른 실시예들에서, NAT 엔진은 2개의 임차인의 소스 IP 주소를 상이한 소스 IP 범위들에 맵핑하는 반면, 2개의 다른 임차인의 소스 IP 주소들은 동일한 소스 IP 범위이지만 상이한 소스 포트 범위들에 맵핑한다.
- [0186] 일부 실시예들에서, NAT 엔진(1712)은, 이전의 SNAT 맵핑을 반영하는 접속 레코드를 저장하는 접속 스토리지를 참조하여 맵핑을 수행하는 상태유지 요소이다. 일부 실시예들에서, NAT 엔진은 또한, 응답 데이터 메시지를 원래의 메시지를 전송한 임차인 머신에 포워딩하기 위해 DNAT 동작을 수행하기 위하여, SaaS 제공자 머신으로부터 응답 데이터 메시지를 수신할 때 일부 실시예들에서 접속 스토리지를 이용할 수 있다. TM 및 NAT 엔진(1705, 1710 및 1712)은, 일부 실시예들에서, 제어기 클러스터(160)에 의해 구성된다(예를 들어, 상이한 임차인들 및 상이한 범위들의 네트워크 주소 공간에 대해 이용하기 위한 맵핑을 기술하기 위한 테이블이 제공된다).
- [0187] 도 18은 유입 NAT 엔진(1712)의 소스 포트 변환을 나타내는 한 예를 제시한다. 구체적으로, 이것은, 임차 맵핑 엔진(1705) 및 유입 NAT 엔진(1712)이, 유입 게이트웨이(1770)를 통해 가상 네트워크(1700)에 진입할 때 및 유출 게이트웨이(1702)에서 가상 네트워크를 벗어날 때의 데이터 메시지(1800)에 관해 수행하는 소스 주소 맵핑을 나타낸다. 도시된 바와 같이, 임차인 게이트웨이(1810)는 소스 IP 주소가 10.1.1.13이고 소스 포트 주소가 4432인 IPsec 게이트웨이(1805)에 도달하는 데이터 메시지(1800)를 전송한다. 일부 실시예들에서, 이들 소스 주소는 임차인 머신(미도시)에 의해 이용되는 주소인 반면, 다른 실시예들에서는, 이들 소스 주소들 중 하나 또는 양쪽 모두는 임차인 게이트웨이 또는 임차인 데이터센터 내의 또 다른 네트워크 요소에 의해 수행되는 소스 NAT 동작에 의해 생성되는 소스 주소이다.
- [0188] 이 메시지가 IPsec 게이트웨이(1805)에 의해 처리된 후, 이 게이트웨이 또는 유입 MFN의 또 다른 모듈은 이 메시지를, 메시지(1800)가 속하는 가상-네트워크 임차인을 식별하는 임차인 ID(15)와 연관시킨다. 이 임차인 ID에 기초하여, 임차인 맵핑 엔진(1705)은, 그 다음, 도시된 바와 같이, 소스 IP 및 포트 주소를, 소스 IP 및 포트 주소 쌍 15.1.1.13 및 253에 맵핑한다. 이 소스 IP 및 포트 주소는, 데이터 메시지(1800)의 메시지 흐름을 고유하게 식별한다. 일부 실시예들에서, TM 엔진(1705)은 상태유지 없는 방식으로(즉, 접속 추적 레코드를 참조하지 않고) 이 맵핑을 수행한다. 다른 실시예들에서, TM 엔진은 이 맵핑을 상태유지 방식으로 수행한다.
- [0189] 그 다음, 유입 NAT 엔진(1712)은, (1) 데이터 메시지(1800)의 소스 IP 주소를 고유한 사설 또는 공용(내부 또는 외부) IP 주소 198.15.4.33으로 변환하고, (2) 이 메시지의 소스 포트 주소를 포트 주소 714로 변환한다. 일부 실시예들에서, 가상 네트워크는, 동일하거나 상이한 임차인의 다른 데이터 메시지 흐름들에 대해 이 IP 주소를

이용한다. 따라서, 이들 실시예에서, NAT 엔진(1712)의 소스 네트워크 주소 변환(SNAT) 동작은, 소스 포트 주소를 이용하여 가상 네트워크 내에서 동일한 IP 주소를 이용하는 상이한 임차인들의 상이한 메시지 흐름들을 구별한다.

[0190] 일부 실시예들에서, 유입 NAT 엔진의 SNAT 동작에 의해 할당된 소스 포트 주소는 또한, 가상 네트워크(1700) 외부의 상이한 메시지 흐름들을 구별하는데 이용되는 소스 포트 주소이다. 이것이 도 18에 나타난 예의 경우이다. 도시된 바와 같이, 이 예에서의 유출 NAT 엔진(1710)은 SNAT 동작을 수행할 때 데이터 메시지의 소스 포트 주소를 변경하지 않는다. 대신에, 이것은 단지, 소스 IP 주소를, 일부 실시예들에서는 가상 네트워크의 유출 게이트웨이(들)의 공용 IP 주소인 외부 IP 주소 198.15.7.125로 변경한다. 일부 실시예들에서의 이 공용 IP 주소는 또한, 유입 및 유출 게이트웨이(1770 및 1702)가 동작하는 공용 클라우드 데이터센터의 IP 주소이다.

[0191] 소스 IP 및 포트 주소 198.15.7.125 및 714에 의해, 데이터 메시지는 SaaS 제공자 데이터센터의 게이트웨이(1815)에 도달하기 위해 인터넷을 통해 라우팅된다. 이 데이터센터에서, SaaS 제공자 머신은 이 메시지에 기초하여 동작을 수행하고, 응답 메시지(1900)를 다시 전송하는데, 그 처리는 도 19를 참조하여 후술될 것이다. 일부 실시예들에서, SaaS 제공자 머신은, 소스 IP 및 포트 주소 198.15.7.125 및 714를 참조하여 정의되는 하나 이상의 서비스 규칙에 기초하여, 데이터 메시지에 관해 하나 이상의 서비스 동작(예를 들어, 방화벽 동작, IDS 동작, IPS 동작 등의 미들박스 서비스 동작)을 수행한다. 이들 실시예들 중 일부에서, 상이한 임차인들에 대한 상이한 서비스 규칙들은, 규칙 식별자들에서 동일한 소스 IP 주소(예를 들어, 198.15.7.125)를 명시하면서, 이들 규칙 식별자들에서 상이한 소스 포트 주소들을 명시할 수 있다. 규칙 식별자, 데이터 메시지와 정합하는 규칙을 식별하는 조회 동작을 수행하는 동안 데이터 메시지 흐름 속성들과 비교하기 위한 한 세트의 속성들을 명시한다.

[0192] 도 19는, SaaS 머신(미도시)이 데이터 메시지(1800)의 처리에 응답하여 전송하는 응답 메시지(1900)의 처리를 나타낸다. 일부 실시예들에서, 응답 메시지(1900)는 원본 데이터 메시지(1800)와 동일하거나, 원본 데이터 메시지(1800)의 수정된 버전이거나, 완전히 새로운 데이터 메시지일 수 있다. 도시된 바와 같이, SaaS 게이트웨이(1815)는 메시지(1900)를 전송하되, 이 메시지가 SaaS 게이트웨이(1815)에 도달할 때 데이터 메시지(1800)의 소스 IP 및 포트 주소인 목적지 IP 및 포트 주소 198.15.7.125 및 714에 기초하여 전송한다.

[0193] 메시지(1900)는 가상 네트워크의 게이트웨이(미도시)에서 수신되고, 이 게이트웨이는, 이 메시지가 SaaS 제공자에게 전송되기 전에 메시지(1800)에 관한 마지막 SNAT 동작을 수행한 NAT 엔진(1710)에 데이터 메시지를 제공한다. 도 19에 나타난 예에서는 데이터 메시지(1900)가 마지막 SNAT 동작을 수행한 동일한 NAT 엔진(1710)에서 수신되지만, 이것은 각각의 배치에서 반드시 그런 것은 아니다.

[0194] (이제는 유입 NAT 엔진으로서 작동하는) NAT 엔진(1710)은 데이터 메시지(1900)에 관해 DNAT(목적지 NAT) 동작을 수행한다. 이 동작은, 외부 목적지 IP 주소(198.15.7.125)를, 공용 클라우드 라우팅 패브릭을 통해 및 가상 네트워크 컴포넌트들 사이에서 데이터 메시지(1900)를 포워딩하기 위해 가상 네트워크에 의해 이용되는 목적지 IP 주소 198.15.4.33으로 변경한다. 또한, IP 주소 198.15.4.33은 일부 실시예들에서 공용 또는 사설 IP 주소일 수 있다.

[0195] 도시된 바와 같이, (이제는 유출 NAT 엔진으로서 동작하는) NAT 엔진(1712)은, NAT 엔진(1710)이 목적지 IP 주소를 변환한 후에 메시지(1900)를 수신한다. 그 다음, NAT 엔진(1712)은, 이 메시지(1900)에 관해, 목적지 IP 및 포트 주소를 15.1.1.13 및 253으로 대체하는 제2 DNAT 동작을 수행한다. 이들 주소는 TM 엔진(1705)에 의해 인식되는 주소들이다. TM 엔진(1705)은 이들 주소를 목적지 IP 및 포트 주소 10.1.1.13 및 4432로 대체하고, 데이터 메시지(1900)를 임차인 ID(15)와 연관시키고, 메시지(1900)를 이 임차인 ID와 함께 임차인 게이트웨이(1810)에 포워딩하기 위해 IPsec 게이트웨이(1805)에 제공한다.

[0196] 일부 실시예들에서, 가상 네트워크 제공자는, 전송된 프로세스, 시스템 및 컴포넌트를 이용하여 동일하거나 또는 상이한 공용 클라우드 제공자들의 복수의 공용 클라우드를 통해 복수의 상이한 임차인(예를 들어, 복수의 회사에 대한 복수의 상이한 회사 WAN)에 대한 복수의 가상 WAN을 제공한다. 도 20은 하나 이상의 공용 클라우드 제공자의 N개 공용 클라우드(2005)에서 네트워크 인프라스트럭처와 제어기 클러스터(들)(2010)를 갖는 가상 네트워크 제공자의 M개의 임차인에 대한 M개의 가상 회사 WAN(2015)을 보여주는 한 예를 제시한다.

[0197] 각각의 임차인의 가상 WAN(2015)은, N개의 공용 클라우드(2005)의 모두 또는 이들 공용 클라우드들의 서브세트에 걸쳐 있을 수 있다. 각각의 임차인의 가상 WAN(2015)은, 하나 이상의 지사(2020), 데이터센터(2025), SaaS

제공자 데이터센터(2030), 및 임차인의 원격 디바이스들을 접속한다. 일부 실시예들에서, 각각의 임차인의 가상 WAN은, VNP의 제어기 클러스터가 임차인의 상이한 컴퓨팅 노드들(2020-2035) 사이에서 데이터 메시지들을 효율적으로 포워딩하는데 필요한 것으로 간주되는 임의의 공용 클라우드(2005)에 걸쳐 있다. 공용 클라우드를 선택함에 있어서, 일부 실시예들에서의 제어기 클러스터는 또한, 임차인이 선택하는 공용 클라우드 및/또는 임차인 또는 임차인의 적어도 하나의 SaaS 제공자가 하나 이상의 머신을 갖는 공용 클라우드를 감안한다.

[0198] 각각의 임차인의 가상 WAN(2015)은, SaaS 제공자 서비스에 액세스(즉, SaaS 제공자 머신 또는 머신 클러스터에 액세스)하기 위하여, 임차인의 원격 디바이스(2035)(예를 들어, 모바일 디바이스 또는 원격 컴퓨터)가 임의의 지사 또는 임차인 데이터센터에 있는 임차인의 WAN 게이트웨이와의 상호작용을 피하는 것을 허용한다. 일부 실시예들에서의 임차인의 가상 WAN은, 이들 WAN 게이트웨이(예를 들어, WAN 보안 게이트웨이)의 기능을 가상 WAN이 걸쳐 있는 공용 클라우드 내의 하나 이상의 머신으로 이동시킴으로써, 원격 디바이스가 지사 및 임차인 데이터센터에 있는 WAN 게이트웨이를 피하는 것을 허용한다.

[0199] 예를 들어, 원격 디바이스가 임차인 또는 그 SaaS 제공자 서비스의 컴퓨팅 자원에 액세스하는 것을 허용하기 위해, 일부 실시예들에서의 WAN 게이트웨이는 원격 디바이스가 임차인의 컴퓨터 자원 또는 그 SaaS 제공자 서비스에 액세스할 수 있는 방법을 제어하는 방화벽 규칙을 시행해야 한다. 임차인의 지부 또는 데이터센터 WAN 게이트웨이를 피하기 위해, 임차인의 방화벽 엔진(210)은, 임차인의 가상 WAN이 걸쳐 있는 하나 이상의 공용 클라우드 내의 가상 네트워크 MFN에 배치된다.

[0200] 이들 MFN 내의 방화벽 엔진(210)은, 원격 디바이스들로부터의 및 원격 디바이스들로의 데이터 메시지 흐름들에 관한 방화벽 서비스 동작을 수행한다. 하나 이상의 공용 클라우드를 통해 배치된 가상 네트워크에서 이들 동작들을 수행함으로써, 임차인의 원격 디바이스와 연관된 데이터 메시지 트래픽이, 방화벽 규칙 처리를 받기 위해 불필요하게 임차인의 데이터센터(들) 또는 지사를 통해 라우팅될 필요가 없다. 이것은, 임차인 데이터센터 및 지사에서 트래픽 혼잡을 완화하고, 이들 위치의 컴퓨팅 자원으로 향하지 않는 트래픽을 처리하기 위해 이들 위치에서 값비싼 유입/유출 네트워크 대역폭을 소비하는 것을 피한다. 이것은 또한, 이 접근법에 의해 데이터 메시지 흐름들이 그들의 목적지(예를 들어, 유입 MFN, 유출 MFN 또는 중간-홉 MFN)로 횡단할 때 가상 네트워크 내에서 개재 방화벽 규칙 처리가 발생하는 것이 허용되기 때문에, 원격 디바이스들로부터의 및 원격 디바이스들로의 데이터 메시지 트래픽의 포워딩을 가속할 수 있다.

[0201] 일부 실시예들에서, MFN의 방화벽 시행 엔진(210)(예를 들어, 방화벽 서비스 VM)은, VNP 중앙 제어기(160)로부터 방화벽 규칙을 수신한다. 일부 실시예들에서의 방화벽 규칙은 규칙 식별자 및 동작을 포함한다. 일부 실시예들에서의 규칙 식별자는, 방화벽 규칙이 데이터 메시지와 정합하는지를 결정하기 위하여, 계층 2 속성(예를 들어, MAC 주소), 계층 3 속성(예를 들어, 5개의 튜플 식별자 등), 임차인 ID, 위치 ID(예를 들어, 사무실 위치 ID, 데이터센터 ID, 원격 사용자 ID 등) 등의, 데이터 메시지 속성들과 비교될 하나 이상의 정합 값을 포함한다.

[0202] 일부 실시예들에서 방화벽 규칙의 동작은, 방화벽 규칙이 데이터 메시지의 속성과 정합할 때 방화벽 시행 엔진(210)이 데이터 메시지에 관해 취해야 하는 동작(예를 들어, 허용, 누락, 방향전환 등)을 명시한다. 복수의 방화벽 규칙이 데이터 메시지와 정합할 가능성을 해결하기 위해, 방화벽 시행 엔진(210)은, 방화벽 규칙(제어기 클러스터(160)로부터 수신한 방화벽 규칙)을, 하나의 방화벽 규칙이 또 다른 방화벽 규칙보다 높은 우선순위를 가질 수 있도록 하는 계층적 방식으로 방화벽 규칙 데이터 스토리지에 저장한다. 데이터 메시지가 2개의 방화벽 규칙과 정합할 때, 방화벽 시행 엔진은, 일부 실시예들에서 더 높은 우선순위를 갖는 규칙을 적용한다. 다른 실시예들에서, 방화벽 시행 엔진은, 또 다른 더 낮은 우선순위 규칙이 데이터 메시지와 정합할 수도 있는 경우에 더 높은 우선순위 규칙과 먼저 정합하도록 보장하기 위하여, 계층에 따라 방화벽 규칙들을 검사한다(즉, 더 낮은 우선순위 규칙에 앞서 더 높은 우선순위 규칙을 검사한다).

[0203] 일부 실시예들은, 데이터 메시지가 가상 네트워크에 진입할 때 유입 노드(예를 들어, 노드 850)에서, 가상 네트워크 상의 중간 노드(예를 들어, 노드 857)에서, 데이터 메시지가 가상 네트워크를 빠져 나갈 때 유출 노드(예를 들어, 노드 855)에서, 방화벽 서비스 엔진이 데이터 메시지를 검사하도록 제어기 클러스터가 MFN 컴포넌트들을 구성하는 것을 허용한다. 이들 노드들 각각에서, 일부 실시예들에서의 CFE(예를 들어, 832, 856 또는 858)는, CFE가 수신하는 데이터 메시지에 관해 방화벽 서비스 동작을 수행하기 위해 그 연관된 방화벽 서비스 엔진(210)을 호출한다. 일부 실시예들에서, 방화벽 서비스 엔진은, 자신을 호출한 모듈에게(예를 들어, CFE에게) 자신의 결정을 반환하여, 이 모듈이 데이터 메시지에 관해 방화벽 동작을 수행할 수 있게 하는 반면, 다른 실시예들에서는, 방화벽 서비스 엔진이 데이터 메시지에 관해 그 방화벽 동작을 수행한다.

- [0204] 일부 실시예들에서, 다른 MFN 컴포넌트들은 방화벽 서비스 엔진에게 그 동작을 수행하도록 지시한다. 예를 들어, 유입 노드에서, 일부 실시예들에서의 VPN 게이트웨이(예를 들어, 225 또는 230)는, 데이터 메시지가 유입 노드의 CFE로 전달되어 하는지를 결정하기 위하여, 그 연관된 방화벽 서비스 엔진이 그 동작을 수행하도록 지시한다. 또한, 유출 노드에서, 일부 실시예들에서의 CFE는 데이터 메시지를 그 연관된 방화벽 서비스 엔진에 전달하고, 방화벽 서비스 엔진은, 데이터 메시지가 통과하는 것을 허용하기로 결정한다면, 데이터 메시지를 외부 네트워크(예를 들어, 인터넷)를 통해 목적지에 전달하거나, 데이터 메시지를 그 연관된 NAT 엔진(215)에 전달하여, 데이터 메시지를 외부 네트워크를 통해 목적지에 전달하기 전에 NAT 동작을 수행한다.
- [0205] 일부 실시예들의 가상 네트워크 제공자는, 공용 클라우드에서 정의된 임차인의 WAN 보안 게이트웨이가 방화벽 서비스에 추가하여 또는 그 대신에 다른 보안 서비스를 구현하는 것을 허용한다. 예를 들어, (일부 실시예들에서는 임차인의 가상 네트워크가 걸쳐 있는 각각의 공용 클라우드 데이터센터에 걸쳐 분포된) 임차인의 분산형 WAN 보안 게이트웨이는, 방화벽 서비스 엔진을 포함할 뿐만 아니라, 침입 검출 엔진 및 침입 방지 엔진도 포함한다. 일부 실시예들에서, 침입 검출 엔진 및 침입 방지 엔진은 MFN(150)에 구조적으로 통합되어 방화벽 서비스 엔진(210)과 유사한 위치를 점유한다.
- [0206] 일부 실시예들에서의 이들 엔진 각각은, 중앙 제어기 클러스터(160)에 의해 배포된 침입 검출/방지 정책을 저장하는 하나 이상의 스토리지를 포함한다. 일부 실시예들에서, 이들 정책은, (여러 공용 클라우드 데이터센터들 통해 배치된) 임차인의 가상 네트워크에 대한 무단 침입을 검출/방지하고, 검출된 침입 이벤트에 응답하여 조치(예를 들어, 로그 생성, 통보 전송, 서비스 또는 머신 셧다운 등)를 취하도록 엔진을 구성한다. 방화벽 규칙처림, 침입 검출/방지 정책은, 가상 네트워크가 정의된 다양한 상이한 관리형 포워딩 노드(예를 들어, 데이터 메시지 흐름의 유입 MFN, 중간 MFN 및/또는 유출 MFN)에서 시행될 수 있다.
- [0207] 앞서 언급된 바와 같이, 가상 네트워크 제공자는, 가상 WAN이 걸쳐 있는 각각의 공용 클라우드에 적어도 하나의 MFN을 배치하고, 임차인의 데이터 흐름이 가상 WAN에 출입하는 것을 허용하는 MFN들 사이의 경로를 정의하도록 배치된 MFN들을 구성함으로써, 각각의 임차인의 가상 WAN을 배치한다. 또한, 앞서 언급된 바와 같이, 일부 실시예들에서는 각각의 MFN이 상이한 임차인들에 의해 공유될 수 있는 반면, 다른 실시예들에서는 각각의 MFN은 단 하나의 특정한 임차인을 위해 배치된다.
- [0208] 일부 실시예들에서, 각각의 임차인의 가상 WAN은, 오버레이 터널을 통해 WAN에 의해 이용되는 MFN들을 접속함으로써 확립되는 보안 가상 WAN이다. 일부 실시예들에서의 이 오버레이 터널 접근법은, 각각의 임차인에 대해 고유한, 예를 들어, 임차인을 고유하게 식별하는 임차인 식별자를 포함하는 터널 헤더로 각각의 임차인의 데이터 메시지 흐름을 캡슐화한다. 임차인의 경우, 일부 실시예들에서의 가상 네트워크 제공자의 CFE는, 하나의 터널 헤더를 이용하여 임차인의 가상 WAN에 출입하기 위한 유입/유출 포워딩 요소들을 식별하고, 또 다른 터널 헤더를 이용하여 가상 네트워크의 개재 포워딩 요소들을 횡단한다. 가상 WAN의 CFE는 다른 실시예들에서 상이한 오버레이 캡슐화 메커니즘을 이용한다.
- [0209] 하나 이상의 공용 클라우드를 통해 임차인에 대한 가상 WAN을 배치하기 위해, VNP의 제어기 클러스터는, (1) 임차인의 회사 컴퓨팅 노드(예를 들어, 지사, 데이터센터, 모바일 사용자 및 SaaS 제공자)의 위치에 기초하여 임차인에 대한 (상이한 데이터 메시지 흐름들에 대해 유입 또는 유출 MFN으로서 역할할 수 있는) 가능한 엣지 MFN들을 식별하고, (2) 모든 가능한 엣지 MFN들 사이의 경로를 식별한다. 일단 이들 경로가 식별되고 나면, 이들은 CFE들의 포워딩 테이블들에 전파된다(예를 들어, OpenFlow를 이용하여 상이한 OVS-기반의 가상 네트워크 라우터들에 전파됨). 구체적으로는, 임차인의 가상 WAN을 통한 최적의 경로를 식별하기 위해, 이 WAN과 연관된 MFN들은, 그들과 그들의 이웃 MFN들 사이의 네트워크 접속의 품질을 정량화하는 측정 값을 생성하고, 그들의 측정 값을 VNP의 제어기 클러스터에 정기적으로 제공한다.
- [0210] 위에서 언급된 바와 같이, 제어기 클러스터는, 그 다음, 상이한 MFN들로부터 측정치들을 집계하고, 이들 측정치에 기초하여 라우팅 그래프를 생성하고, 임차인의 가상 WAN을 통한 경로를 정의한 다음, 이들 경로를 MFN들의 CFE들의 포워딩 요소들에 배포한다. 임차인의 가상 WAN에 대해 정의된 경로들을 동적으로 업데이트하기 위해, 이 WAN과 연관된 MFN들은 주기적으로 그들을 측정치들을 생성하고 이들 측정치들을 제어기 클러스터에 제공하며, 제어기 클러스터는, 그 다음, 자신이 수신하는 업데이트된 측정치에 기초하여, 측정치 집계, 경로-그래프 생성, 경로 식별, 및 경로 배포를 주기적으로 반복한다.
- [0211] 임차인의 가상 WAN을 통한 경로를 정의하는데 있어서, VNP의 제어기 클러스터는, 인터넷을 통한 임차인의 데이터 흐름들의 라우팅을 최소화하려고 시도하면서, 원하는 종단간 성능, 신뢰성 및 보안을 위해 경로를 최적화한다. 제어기 클러스터는 또한, 네트워크를 통과하는 데이터 메시지 흐름의 계층 4 처리를 최적화(예를 들어, 접

속 경로에 걸쳐 속도 제어 메커니즘을 분할함으로써 TCP 접속의 중단간 속도를 최적화)하도록 MFN 컴포넌트들을 구성한다.

- [0212] 공용 클라우드의 확산에 따라, 회사의 각각의 지사에 가까운 주요 공용 클라우드 데이터센터를 발견하는 것은 종종 매우 용이하다. 마찬가지로, SaaS 벤더들은, 점점 더, 공용 클라우드 내에 그들의 애플리케이션을 호스팅하거나, 유사하게 일부 공용 클라우드 데이터센터 근처에 위치한다. 결과적으로, 가상 회사 WAN(2015)은, 공용 클라우드(2005)를, 회사 컴퓨팅 노드(예를 들어, 지사, 데이터센터, 원격 디바이스 및 SaaS 제공자) 부근에 존재하는 회사 네트워크 인프라스트럭처로서 안전하게 이용한다.
- [0213] 회사 WAN은, 비즈니스 중요 애플리케이션을 항상 수락가능한 성능에서 제공하기 위해 대역폭 보장을 요구한다. 이러한 애플리케이션은, 대화형 데이터 애플리케이션, 예를 들어, ERP, 재무 또는 조달, 마감일 중심의 애플리케이션(예를 들어, 산업 또는 IoT 제어), 실시간 애플리케이션(예를 들어, VoIP 또는 화상 회의)일 수 있다. 결과적으로 기존 WAN 인프라스트럭처(예를 들어, Frame Relay 또는 MPLS)는 이러한 보장을 제공한다.
- [0214] 복수-임차인 네트워크에서 대역폭 보장을 제공하는데 있어서 주요 장애물은, 소정의 고객을 위해 하나 이상의 경로에 관한 대역폭을 예약할 필요성이다. 일부 실시예들에서, VNP는 QoS 서비스를 제공하고 ICR(Ingress Committed Rate) 보장 및 ECR(Egress Committed Rate) 보장을 제공한다. ICR은 가상 네트워크로 들어오는 트래픽 속도를 지칭하는 반면, ECR은 임차인 사이트쪽으로 가상 네트워크를 빠져 나가는 트래픽 속도를 지칭한다.
- [0215] 트래픽이 ICR 및 ECR 한계를 초과하지 않는 한, 일부 실시예들에서의 가상 네트워크는 대역폭 및 지연 보장을 제공한다. 예를 들어, HTTP 유입 또는 유출 트래픽이 1Mbps를 초과하지 않는 한, 대역폭과 낮은 지연이 보장된다. QoS 목적을 위해, VNP가 트래픽 목적지를, 그 목적지가 ICR/ECR 한도 내에 있는 한, 추적할 필요가 없기 때문에, 이것은 포인트-투-클라우드 모델이다. 이 모델을 때때로 호스 모델(hose model)이라고 불린다.
- [0216] 고객이 포인트-투-포인트 보장을 원하는 더 엄격한 애플리케이션의 경우, 매우 중요한 트래픽을 전달하기 위해 가상 데이터 파이프(virtual data pipe)가 구성될 필요가 있다. 예를 들어, 기업은 높은 서비스 수준 계약 보장과 함께 접속된 2개의 허브 사이트 또는 데이터센터를 원할 수 있다. 이 목적을 위해, VNP 라우팅은, 각각의 고객에 대한 대역폭 제약을 충족하는 라우팅 경로를 자동으로 선택한다. 이것을 포인트-투-포인트 모델 또는 파이프 모델이라고 지칭한다.
- [0217] 최종 사용자에게 보장된 대역폭을 제공함에 있어서 VNP의 주요 장점은, 변화하는 대역폭 수요에 따라 VNP 인프라스트럭처를 조정하는 능력이다. 대부분의 공용 클라우드는, 동일한 클라우드의 상이한 지역들에 위치한 각각의 2개의 인스턴스 사이에 최소 대역폭 보장을 제공한다. 현재의 네트워크가 새로운 요청에 대한 보장된 대역폭을 제공하기에 충분한 미사용 용량을 갖지 않고 있다면, VNP는 그 설비에 새로운 자원을 추가한다. 예를 들어, VNP는 수요가 많은 지역에 새로운 CFE를 추가할 수 있다.
- [0218] 하나의 해결과제는, 경로를 계획하고 인프라스트럭처를 확장 및 축소하는데 있어서 이 새로운 차원의 성능 및 비용을 최적화하는 것이다. 알고리즘 및 대역폭 고려를 용이화하기 위해, 일부 실시예들은 중단간 대역폭 예약이 분할되지 않는다고 가정한다. 다른 방식으로, 만일 소정의 임차인의 지부 A와 지부 B 사이에 소정의 대역폭(예를 들어, 10Mbps)이 예약된다면, 그 대역폭은, 지부 A가 접속된 유입 CFE에서 시작하여, 한 세트의 제로 또는 그 이상의 중간 CFE들을 횡단해, 지부 B에 접속된 유출 CFE에 도달하는 단일 경로에 걸쳐 할당된다. 일부 실시예들은 또한, 대역폭 보장된 경로가 단일 공용 클라우드만을 횡단한다고 가정한다.
- [0219] 네트워크 토폴로지에 걸쳐 교차하는 다양한 대역폭 예약을 감안하기 위하여, 일부 실시예들에서의 VNP는, 예약된 대역폭 경로를 통한 라우팅을 정적으로 정의하여, 데이터 메시지 흐름은 대역폭 요건을 위해 예약된 동일한 경로를 항상 횡단할 수 있게 한다. 일부 실시예들에서, 각각의 경로는, 그 경로에 의해 통과된 각각의 CFE가 이 경로와 연관된 단일의 송출 인터페이스와 정합하는 단일 태그에 의해 식별된다. 구체적으로, 각각의 CFE는, 헤더에서 이 태그를 갖고 특정한 인입 인터페이스로부터 도달하는 각각의 데이터 메시지에 대해 단일의 송출 인터페이스를 정합시킨다.
- [0220] 일부 실시예들에서, 제어기 클러스터는 여러 개의 상호접속된 노드들에 의해 형성된 네트워크 그래프를 유지한다. 그래프 내의 각각의 노드 n 은, 이 노드와 연관된 할당된 총 보장된 대역폭(TBW_n) 및 이 노드(RBW_n)에 의해 이미 예약된(소정의 예약된 경로에 할당된) 대역폭의 양을 갖는다. 또한, 각각의 노드에 대해, 그래프는, 이 노드와 그래프 내의 모든 다른 노드들 사이의 트래픽 전송과 연관된 기가바이트 당 센트 단위의 비용(C_{ij}) 및 밀리초 단위의 지연(D_{ij})을 포함한다. 노드 i 와 노드 j 사이의 트래픽 전송과 연관된 가중치는 $W_{ij} = a * C_{ij} + D_{ij}$

이며, 여기서 a 는 전형적으로 1과 10 사이의 시스템 파라미터이다.

- [0221] 지부 A와 B 사이의 값 BW 의 대역폭 예약에 대한 요청이 수락될 때, 제어기 클러스터는 먼저, 그 요청을, 지부 A와 B에 각각 결속된 특정한 유입 및 유출 라우터 n 및 m 에 맵핑한다. 그 다음, 제어기 클러스터는 n 과 m 사이에서 2개의 최저 비용(예를 들어, 최단 경로) 계산을 수행하는 라우팅 프로세스를 실행한다. 첫번째는, 계산된 경로를 따라 이용가능한 대역폭에 관계없이 n 과 m 사이의 최저 비용(예를 들어, 최단 경로) 경로이다. 이 경로의 총 가중치는 W_1 로서 계산된다.
- [0222] 두번째 최저 비용(예를 들어, 최단 경로) 계산은 처음에, 모든 노드 i 를 제거함으로써 그래프를 수정하며, 여기서, $BW > TBW_i - RBW_i$ 이다. 수정된 그래프를 트리밍된 그래프(trimmed graph)라고 한다. 그 다음, 제어기 클러스터는, 트리밍된 그래프에 관해 제2의 최저 비용(예를 들어, 최단 경로) 경로 계산을 수행한다. 제2 경로의 가중치가 제1 경로보다 K 퍼센트(K 는 전형적으로 10%-30%)보다 크지 않다면, 제2 경로가 선호되는 경로로서 선택된다. 반면, 이 요건이 충족되지 않으면, 제어기 클러스터는 $TBW_i - RBW_i$ 의 최소 값을 갖는 노드 i 를 제1 경로에 추가한 다음, 2개의 최저 비용(예를 들어, 최단 경로) 계산을 반복한다. 제어기 클러스터는 이 조건이 충족될 때까지 라우터를 계속 추가할 것이다. 이 시점에서, 예약 대역폭 BW 가 모든 RBW_i 에 추가되고, 여기서 i 는 선택한 경로 상의 라우터이다.
- [0223] 이미 대역폭을 예약한 경로에 대한 추가 대역폭 요청의 특별한 경우에 대해, 제어기 클러스터는 먼저, 노드 A와 B 사이의 현재의 대역폭 예약을 삭제하고, 이들 노드들 사이의 총 대역폭 요청에 대한 경로를 계산할 것이다. 이를 위해, 일부 실시예들에서의 각각의 노드에 대해 보유된 정보는 또한, 예약된 전체 대역폭뿐만 아니라, 각각의 태그, 또는 각각의 소스 및 목적지 지부에 대해 예약된 대역폭을 포함한다. 대역폭 예약이 네트워크에 추가된 후, 일부 실시예들은, 측정된 네트워크 지연 또는 가상 네트워크를 통한 비용에 있어서 주요 변화가 없는 한 경로를 다시 방문하지 않는다. 그러나, 측정치 및/또는 비용이 변할 때, 이들 실시예는 대역폭 예약 및 경로 계산 프로세스를 반복한다.
- [0224] 도 21은 특정한 임차인에 대한 가상 WAN을 배치하고 관리하기 위해 가상 네트워크 제공자의 제어기 클러스터(160)에 의해 수행되는 한 프로세스(2100)를 개념적으로 나타낸다. 일부 실시예들에서, 프로세스(2100)는, 제어기 클러스터(160) 상에서 실행되는 여러 상이한 제어기 프로그램들에 의해 수행된다. 이 프로세스의 동작들은, 이들 동작들이 상이한 프로그램들에 의해 병렬로 또는 상이한 시퀀스로 수행될 수 있기 때문에, 반드시 도 21에 도시된 시퀀스를 따를 필요는 없다. 따라서, 이들 동작은, 제어기 클러스터에 의해 수행되는 하나의 예시적인 동작 시퀀스를 단지 설명하기 위해 이 도면에 도시된 것이다.
- [0225] 도시된 바와 같이, 제어기 클러스터는 처음에, 여러 상이한 공용 클라우드 제공자들(예를 들어, Amazon AWS, Google GCP 등)의 여러 공용 클라우드 데이터센터들 내에 여러 개의 MFN을 (2105에서) 배치한다. 일부 실시예들에서의 제어기 클러스터는, 프로세스(2100)가 도시하고 있는 특정한 임차인과는 상이한 하나 이상의 다른 임차인에 대해 이들 배치된 MFN들을 (2105에서) 구성한다.
- [0226] 2110에서, 제어기 클러스터는, 특정한 임차인으로부터 그 특정한 임차인의 외부 머신 속성들 및 위치들에 관한 데이터를 수신한다. 일부 실시예들에서, 이 데이터는, 특정한 임차인에 의해 이용되는 사설 서브넷들뿐만 아니라, 특정한 임차인이 외부 머신을 갖는 하나 이상의 임차인 사무실 및 데이터센터에 대한 식별자를 포함한다. 일부 실시예들에서, 제어기 클러스터는, API를 통해 또는 제어기 클러스터가 제공하는 사용자 인터페이스를 통해 임차인 데이터를 수신할 수 있다.
- [0227] 그 다음, 2115에서, 제어기 클러스터는, 특정한 임차인에 대한 가상 네트워크를 확립하는데 이용하기 위해 후보 MFN들인 MFN(150)들의 측정 에이전트(205)에 의해 수집된 측정치들로부터 특정한 임차인에 대한 라우팅 그래프를 생성한다. 위에서 언급된 바와 같이, 라우팅 그래프는, MFN들을 나타내는 노드들과, MFN들 사이의 네트워크 접속을 나타내는 노드들 사이의 링크들을 갖는다. 링크는, 링크가 나타내는 네트워크 접속을 이용하는 품질 및/또는 비용을 정량화하는 비용 값에 해당하는 연관된 가중치를 갖는다. 위에서 언급된 바와 같이, 제어기 클러스터는 먼저, 수집된 측정치들로부터 측정 그래프를 생성한 다음, 최적이 아닌(예를 들어, 큰 지연 또는 드롭률을 갖는) 링크를 측정 그래프로부터 제거함으로써 라우팅 그래프를 생성한다.
- [0228] 라우팅 그래프를 구성한 후, 제어기 클러스터는, 임차인의 외부 머신이 데이터 메시지를 (MFN들에 의해 배치된) 가상 네트워크에 전송하고 가상 네트워크로부터 데이터 메시지를 수신하기 위해 이용할 수 있는 상이한 쌍들의 후보 유입 및 유출 노드들(즉, MFN들) 사이의 가능한 경로를 식별하기 위해 경로 검색을 (2120에서) 수행한다.

일부 실시예들에서, 제어기 클러스터는, 알려진 후보 경로 검색 알고리즘을 이용하여 각각의 후보 유입/유출 노드 쌍 사이의 상이한 경로들을 식별한다. 이러한 쌍에 대한 각각의 경로는, 연결될 때 제로개 이상의 중간 노드를 통해 유입 노드로부터 유출 노드로 횡단하는 하나 이상의 링크를 이용한다.

[0229] 일부 실시예들에서, 임의의 2개의 MFN들 사이의 비용은, 2개의 MFN들 사이의 접속 링크에 대한 추정된 레이턴시와 재정 비용의 가중 합을 포함한다. 레이턴시 및 재정 비용은, 일부 실시예들에서, 다음 중 하나 이상을 포함한다: (1) 링크 지연 측정, (2) 추정된 메시지 처리 레이턴시, (3) 특정한 데이터센터로부터 동일한 공용 클라우드 제공자의 또 다른 데이터센터로의, 또는 공용 클라우드(PC) 제공자의 클라우드로의(예를 들어, 또 다른 공용 클라우드 제공자의 또 다른 공용 클라우드 데이터센터로의 또는 인터넷으로의) 송출 트래픽에 대한 클라우드 요금, 및 (4) 공용 클라우드의 호스트 컴퓨터에서 실행되는 MFN과 연관된 추정된 메시지 처리 비용.

[0230] 일부 실시예들은, 공용 인터넷을 통해 횡단하는 2개의 MFN 사이의 접속 링크에 대한 페널티를 평가하여, 가능할 때마다 이러한 통과를 최소화한다. 일부 실시예들은 또한, 이러한 접속을 이용하도록 경로 생성을 편향시키기 위하여(예를 들어, 접속 링크 비용을 감소시킴으로써) 2개의 데이터센터 사이의 사설 네트워크 접속의 이용을 동기부여한다. 이들 쌍을 이룬 링크들의 계산된 비용을 이용하여, 제어기 클러스터는, 라우팅 경로에 의해 이용되는 개개의 쌍일 이룬 링크들의 비용을 집계함으로써 이들 쌍을 이룬 링크들 중 하나 이상을 이용하는 각각의 라우팅 경로의 비용을 계산할 수 있다.

[0231] 그 다음, 제어기 클러스터는, 각각의 후보 유입/유출 노드 쌍 사이에서 식별된 후보 경로들의 계산된 비용(예를 들어, 최저 총 비용)에 기초하여 하나 또는 최대 N개의 식별된 경로(여기서 N은 1보다 큰 정수임)를 (2120에서) 선택한다. 일부 실시예들에서, 각각의 경로에 대한 계산된 비용은, 위에서 언급된 바와 같이, 경로에 의해 이용된 각각의 링크의 가중 비용에 기초한다(예를 들어, 각각의 링크의 연관된 가중치의 합이다). 유입 MFN 또는 중간 MFN이 다중-경로 동작을 수행하는 것을 허용하기 위해 2개의 MFN들 사이에 하나보다 많은 경로가 필요할 때, 제어기 클러스터는 한 쌍의 유입/유출 노드들 사이에서 하나보다 많은 경로를 선택할 수 있다.

[0232] 각각의 후보 쌍의 유입/유출 노드들에 대해 하나 또는 N개의 경로를 (2120에서) 선택한 후, 제어기 클러스터는, 선택된 경로에 기초하여 하나 또는 N개의 경로를 정의한 다음, 특정한 임차인의 가상 네트워크를 구현하는 MFN들에 대한 경로 테이블들 또는 경로 테이블 부분들을 생성한다. 생성된 경로 레코드들은, 특정한 임차인의 상이한 서브넷들에 도달하는 엣지 MFN들을 식별하고, 유입 MFN들로부터 유출 MFN들로 경로를 통과시키기 위한 다음 홉 MFN을 식별한다.

[0233] 2125에서, 제어기 클러스터는, 특정한 임차인에 대한 가상 네트워크를 구현하도록 이들 MFN들의 포워딩 요소(235)를 구성하기 위해 경로 레코드들을 MFN들에 배포한다. 일부 실시예들에서, 제어기 클러스터는, 호스트 컴퓨터에 걸쳐 있는 논리적 네트워크를 구현하도록 호스트 컴퓨터들 상에서 실행되는 소프트웨어 라우터를 구성하기 위해 소프트웨어 정의된 복수-임차인 데이터센터에서 현재 이용되는 통신 프로토콜을 이용함으로써 경로 레코드를 전달하기 위해 포워딩 요소와 통신한다.

[0234] 일단 MFN들이 구성되고 가상 네트워크가 특정한 임차인에 대해 동작하면, 엣지 MFN들은 임차인의 외부 머신(즉, 가상 네트워크 외부의 머신)으로부터 데이터 메시지를 수신하고 이들 데이터 메시지를 가상 네트워크 내의 엣지 MFN들에 포워딩하며, 이어서, 엣지 MFN들은 데이터 메시지를 임차인의 다른 외부 머신에 포워딩한다. 이러한 포워딩 동작을 수행하는 동안, 유입, 중간 및 유출 MFN들은 그들의 포워딩 동작에 관한 통계를 수집한다. 또한, 일부 실시예들에서, 일부 실시예들에서의 각각의 MFN 상의 하나 이상의 모듈은, 공용 클라우드 데이터센터에서의 네트워크 또는 컴퓨팅 소비에 관한 다른 통계를 수집한다. 일부 실시예들에서, 공용 클라우드 제공자는, 이러한 소비 데이터를 수집하고 수집된 데이터를 가상 네트워크 제공자에게 전달한다.

[0235] 과금 사이클에 접근할 때, 제어기 클러스터는, MFN들에 의해 수집된 통계, 및/또는 MFN들에 의해 수집되거나 공용 클라우드 제공자에 의해 제공되는 네트워크/컴퓨팅 소비 데이터를(예를 들어, 2130에서) 수집한다. 수집된 통계 및/또는 제공된 네트워크/컴퓨팅 소비 데이터에 기초하여, 제어기 클러스터는, (2130에서) 과금 보고서를 생성하고, 과금 보고서를 특정한 임차인에게 전송한다.

[0236] 위에서 언급된 바와 같이, 과금 보고서에서 청구된 금액은, (예를 들어, 2130에서) 제어기 클러스터가 수신하는 통계 및 네트워크/소비 데이터를 감안한다. 또한, 일부 실시예들에서, 청구서는 가상 네트워크 제공자가(특정한 임차인에 대한 가상 네트워크를 구현하는) MFN들을 운영하기 위해 발생시킨 비용 + 수익률(예를 들어, 10% 증가)을 감안한다. 이 과금 방식은, 특정한 임차인은 그 임차인의 가상 네트워크가 배치되어 있는 복수의 상이한 공용 클라우드 제공자들로부터의 청구서를 처리할 필요가 없기 때문에, 그 특정한 임차인에게 편리하다. 일

부 실시예들에서의 VNP의 발생 비용은 공용 클라우드 제공자에 의해 VNP에 부과된 비용을 포함한다. 2130에서, 제어기 클러스터는 또한, 과금 보고서에 반영된 요금에 대해 신용 카드를 청구하거나 은행 계좌로부터 자금을 전자적으로 인출한다.

[0237] 2135에서, 제어기 클러스터는 자신이 측정 에이전트(205)로부터 새로운 측정을 수신했는지를 결정한다. 만일 그렇지 않다면, 프로세스는 후술될 2145로 천이한다. 반면에, 제어기 클러스터가 자신이 측정 에이전트로부터 새로운 측정치를 수신했다고 결정하면, 새로운 측정치에 기초하여 특정한 임차인에 대한 라우팅 그래프를 재검토할 필요가 있는지를 (2140에서) 결정한다. MFN 고장이 없는 경우, 일부 실시예들에서의 제어기 클러스터는, 최대한, 수신된 업데이트된 측정치에 기초하여 특정한 기간 동안 한번(예를 들어, 24 시간마다 또는 매주 한번) 각각의 임차인에 대한 라우팅 그래프를 업데이트한다.

[0238] 제어기 클러스터가 자신이 수신한 새로운 측정치에 기초하여 라우팅 그래프를 재검토할 필요가 있다고 (2140에서) 결정하면, 프로세스는 새로 수신된 측정치에 기초하여 새로운 측정 그래프를 (2145에서) 생성한다. 일부 실시예들에서, 제어기 클러스터는, 측정 그래프의 링크와 연관된 측정 값이 새로운 측정치 세트가 수신될 때마다 급격히 변동하지 않도록 보장하기 위하여, 가중 합을 이용하여 각각의 새로운 측정치를 이전의 측정치와 혼합한다.

[0239] 2145에서, 제어기 클러스터는 또한, 조정된 측정 그래프에 기초하여 라우팅 그래프를 조정할 필요가 있는지를 (예를 들어, 링크와 연관된 조정된 측정치 때문에, 라우팅 그래프 링크에 대한 가중치를 조정할 필요가 있는지, 또는 라우팅 그래프에서 링크를 추가하거나 제거할 필요가 있는지를) 결정한다. 만일 그렇다면, 제어기 클러스터, (2145에서), 라우팅 그래프를 조정하고, (동작 2120 등의) 경로 검색 동작을 수행하여, 유입/유출 노드 쌍들 사이의 경로를 식별하고, 식별된 경로에 기초하여 경로 레코드를 생성하며, 경로 레코드를 MFN들에 배포한다. 2145로부터, 프로세스는 2150으로 천이한다.

[0240] 프로세스는 또한, 제어기 클러스터가 라우팅 그래프를 재검토할 필요가 없다고 (2140에서) 결정할 때 2150으로 천이한다. 2150에서, 제어기 클러스터는, 처리된 데이터 메시지 및 소비된 네트워크/컴퓨팅 자원에 관한 통계를 수집해야 하는 또 다른 과금 사이클에 접근하고 있는지를 결정한다. 만일 그렇지 않다면, 프로세스는 2135로 복귀하여 MFN 측정 에이전트로부터 새로운 측정치를 수신했는지를 결정한다. 그외의 경우, 프로세스는 2130으로 복귀하여, 통계, 네트워크/컴퓨팅 소비 데이터를 수집하고 과금 보고서를 생성 및 전송한다. 일부 실시예들에서, 제어기 클러스터는, 특정한 임차인이 공용 클라우드 데이터센터들에 걸쳐 배치된 가상 네트워크를 더 이상 필요로하지 않을 때까지 프로세스(2100)의 동작들을 반복적으로 수행한다.

[0241] 일부 실시예들에서, 제어기 클러스터는, 공용 클라우드 데이터센터에서 임차인을 위한 가상 네트워크를 배치할 뿐만 아니라, 공용 클라우드 데이터센터들에서 컴퓨팅 노드 머신 및 서비스 머신을 배치하고 구성하는데 있어서 임차인을 보조한다. 배치된 서비스 머신들은, MFN들의 서비스 머신들과는 분리된 머신들일 수 있다. 일부 실시예들에서, 특정한 임차인에 대한 제어기 클러스터 과금 보고서는 또한, 배치된 컴퓨팅 및 서비스 머신들에 의해 소비된 컴퓨팅 자원을 감안한다. 다시 한번, 임차인에게는, 복수의 공용 클라우드 제공자의 복수의 공용 클라우드 데이터센터에서 소비된 네트워크 및 컴퓨팅 자원에 대해, 복수의 공용 클라우드 제공자로부터 복수의 청구서를 수신하는 것보다, 하나의 가상 네트워크 제공자로부터의 하나의 청구서를 갖는 것이 더 바람직하다.

[0242] 전술된 많은 피치들 및 애플리케이션들은, 컴퓨터 판독가능한 저장 매체(컴퓨터 판독가능한 매체라고도 함)에 기록된 한 세트의 명령어들로서 명시되는 소프트웨어 프로세스로서 구현된다. 이들 명령어가 하나 이상의 처리 유닛(들)(예를 들어, 하나 이상의 프로세서, 프로세서의 코어 또는 기타의 처리 유닛)에 의해 실행될 때, 이들은 처리 유닛(들)로 하여금 명령어들서 표시된 동작들을 수행하게 한다. 컴퓨터 판독가능한 매체의 예는, CD-ROM, 플래시 드라이브, RAM 칩, 하드 드라이브, EPROM 등을 포함하지만 이것으로 제한되는 것은 아니다. 컴퓨터 판독가능한 매체는, 무선으로 또는 유선 접속을 통해 전달되는 캐리어파 및 전자 신호를 포함하지 않는다.

[0243] 본 명세서에서, 용어 "소프트웨어"는, 프로세서에 의한 처리를 위해 메모리 내로 판독될 수 있는, 판독 전용 메모리에 존재하는 펌웨어 또는 자기 스토리지에 저장된 애플리케이션을 포함한다. 또한, 일부 실시예들에서, 복수의 소프트웨어 발명은, 별개의 소프트웨어 발명들을 유지하면서 더 큰 프로그램의 하위 부분으로서 구현될 수 있다. 일부 실시예들에서, 복수의 소프트웨어 발명은 또한, 별도의 프로그램으로서 구현될 수 있다. 마지막으로, 여기서 설명된 소프트웨어 발명을 함께 구현하는 별개의 프로그램들의 임의의 조합은 본 발명의 범위 내에 있다. 일부 실시예들에서, 소프트웨어 프로그램은, 하나 이상의 전자 시스템에서 동작하도록 설치될 때, 소프트웨어 프로그램의 동작을 실행하고 수행하는 하나 이상의 특정한 머신 구현을 정의한다.

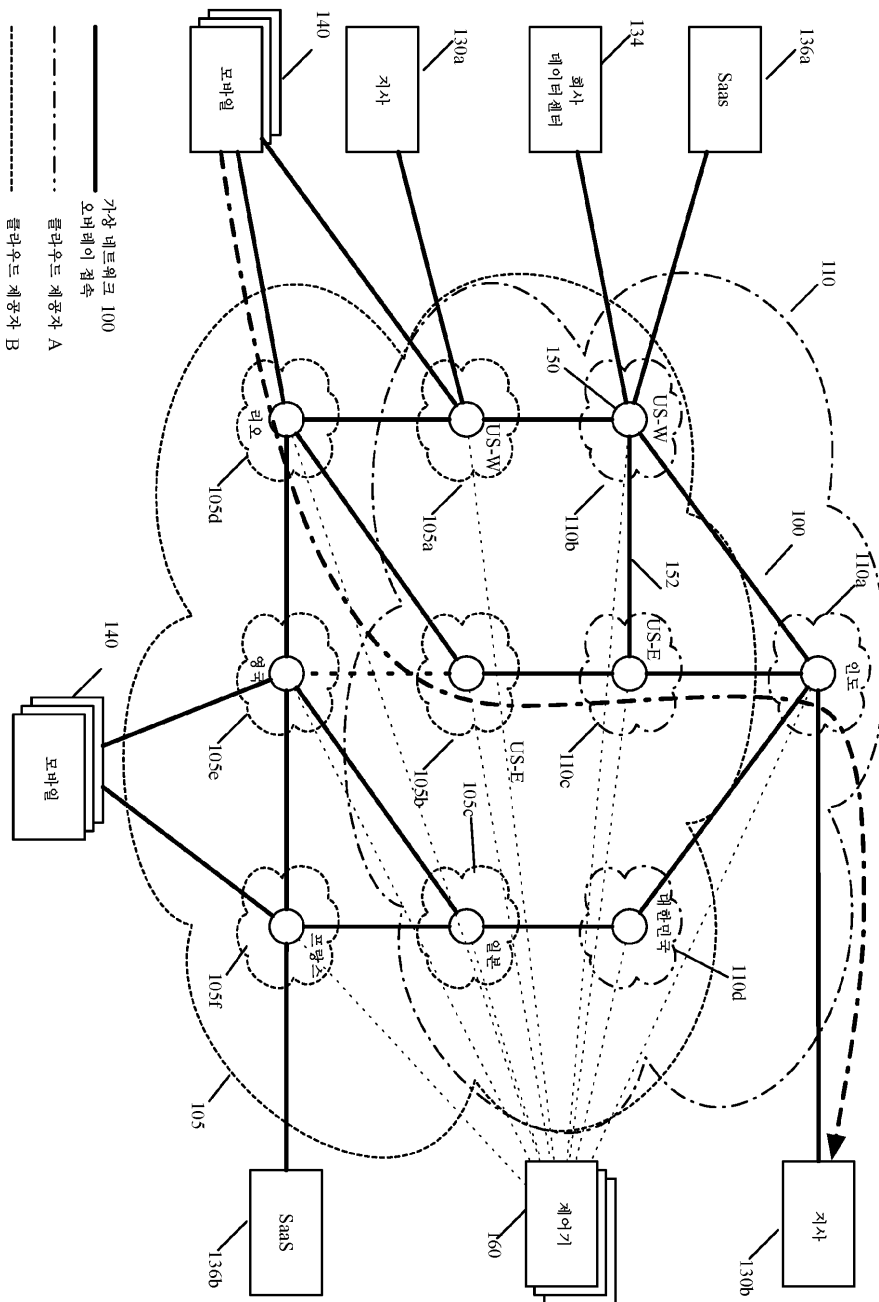
- [0244] 도 22는 본 발명의 일부 실시예들을 구현하기 위한 컴퓨터 시스템(2200)을 개념적으로 나타낸다. 컴퓨터 시스템(2200)은, 전술된 호스트, 제어기, 및 관리자 중 임의의 것을 구현하는데 이용될 수 있다. 따라서, 이것은, 전술된 프로세스들 중 임의의 것을 실행하는데 이용될 수 있다. 이 컴퓨터 시스템은, 다양한 유형의 비일시적인 머신 판독가능한 매체 및 다양한 다른 유형의 머신 판독가능한 매체를 위한 인터페이스를 포함한다. 컴퓨터 시스템(2200)은, 버스(2205), 처리 유닛(들)(2210), 시스템 메모리(2225), 판독 전용 메모리(2230), 영구 저장 디바이스(2235), 입력 디바이스(2240), 및 출력 디바이스(2245)를 포함한다.
- [0245] 버스(2205)는, 컴퓨터 시스템(2200)의 수많은 내부 디바이스들을 통신가능하게 접속하는 모든 시스템, 주변기기, 및 칩셋 버스를 집합적으로 나타낸다. 예를 들어, 버스(2205)는, 처리 유닛(들)(2210)을, 판독 전용 메모리(2230), 시스템 메모리(2225), 및 영구 저장 디바이스(2235)와 통신가능하게 접속한다.
- [0246] 이들 다양한 메모리 유닛들로부터, 처리 유닛(들)(2210)은, 본 발명의 프로세스들을 실행하기 위하여 실행할 명령어 및 처리할 데이터를 회수한다. 처리 유닛(들)은 상이한 실시예들에서 단일의 프로세서 또는 멀티-코어 프로세서일 수 있다. ROM(read-only-memory)(2230)은, 처리 유닛(들)(2210) 및 컴퓨터 시스템의 다른 모듈들이 필요로 하는 정적 데이터 및 명령어를 저장한다. 반면, 영구 저장 디바이스(2235)는 판독-및-기입 메모리 디바이스이다. 이 디바이스는 컴퓨터 시스템(2200)이 꺼져 있어도 명령어 및 데이터를 저장하는 비휘발성 메모리 유닛이다. 본 발명의 일부 실시예들은, 영구 저장 디바이스(2235)로서 (자기 또는 광 디스크 및 그 대응하는 디스크 드라이브 등의) 대용량 저장 디바이스를 이용한다.
- [0247] 다른 실시예들은, 영구 저장 디바이스로서 (플로피 디스크, 플래시 드라이브 등의) 착탈식 저장 디바이스를 이용한다. 영구 저장 디바이스(2235)처럼, 시스템 메모리(2225)는 판독-및-기입 메모리 디바이스이다. 그러나, 저장 디바이스(2235)와는 달리, 시스템 메모리는, 랜덤 액세스 메모리 등의, 휘발성 판독-및-기입 메모리이다. 시스템 메모리는, 프로세서가 런타임에 필요로 하는 명령어들 및 데이터들 중 일부를 저장한다. 일부 실시예들에서, 본 발명의 프로세스들은, 시스템 메모리(2225), 영구 저장 디바이스(2235), 및/또는 판독 전용 메모리(2230)에 저장된다. 이들 다양한 메모리 유닛들로부터, 처리 유닛(들)(2210)은, 일부 실시예들의 프로세스들을 실행하기 위하여 실행할 명령어 및 처리할 데이터를 회수한다.
- [0248] 버스(2205)는 또한, 입력 및 출력 디바이스들(2240 및 2245)에 접속된다. 입력 디바이스는, 사용자가 정보를 전달하고 컴퓨터 시스템에 대한 명령을 선택할 수 있게 한다. 입력 디바이스(2240)는, 영숫자 키보드 및 포인팅 디바이스("커서 제어 디바이스"라고도 함)를 포함한다. 출력 디바이스(2245)는 컴퓨터 시스템에 의해 생성된 이미지를 디스플레이한다. 출력 디바이스는, 프린터, 및 CRT(Cathode Ray Tube) 또는 LCD(Liquid Crystal Display) 등의, 디스플레이 디바이스를 포함한다. 일부 실시예들은, 입력 및 출력 디바이스 양쪽 모두로서 기능하는 터치스크린 등의 디바이스를 포함한다.
- [0249] 마지막으로, 도 22에 도시된 바와 같이, 버스(2205)는 또한, 네트워크 어댑터(미도시)를 통해 컴퓨터 시스템(2200)을 네트워크(2265)에 결합한다. 이러한 방식으로, 컴퓨터는, (근거리 통신망("LAN"), 광역 통신망("WAN"), 또는 인트라넷, 인터넷 등의 네트워크들의 네트워크 등의) 컴퓨터들의 네트워크의 일부일 수 있다. 컴퓨터 시스템(2200)의 임의의 또는 모든 컴포넌트는 본 발명과 연계되어 이용될 수 있다.
- [0250] 일부 실시예들은, 컴퓨터 프로그램 명령어들을 머신-판독가능한 또는 컴퓨터-판독가능한 매체(대안으로서, 컴퓨터-판독가능한 저장 매체, 머신-판독가능한 매체, 또는 머신-판독가능한 매체라고도 함)에 저장하는 스토리지 및 메모리, 마이크로프로세서 등의 전자 컴포넌트들을 포함한다. 이러한 컴퓨터-판독가능한 매체의 일부 예는, RAM, ROM, CD-ROM(read-only compact disc), CD-R(recordable compact disc), CD-RW(rewritable compact disc), 판독전용 디지털 버서타일 디스크(예를 들어, DVD-ROM, 듀얼 레이어 DVD-ROM), 다양한 기록가능한/재기록가능한 DVD(예를 들어, DVD-RAM, DVD-RW, DVD+RW 등), 플래시 메모리(예를 들어, SD 카드, 미니-SD 카드, 마이크로-SD 카드 등), 자기 및/또는 솔리드 스테이트 하드 드라이브, 판독전용 및 기록가능한 Blu-Ray® 디스크, 초 고밀도 광 디스크, 기타 임의의 광 또는 자기 매체, 및 플로피 디스크를 포함한다. 컴퓨터-판독가능한 매체는, 적어도 하나의 처리 유닛에 의해 실행가능하고 다양한 동작을 수행하기 위한 명령어 세트를 포함하는 컴퓨터 프로그램을 저장할 수 있다. 컴퓨터 프로그램 또는 컴퓨터 코드의 예는, 컴파일러에 의해 생성되는 것 등의 머신 코드, 및 인터프리터를 이용하여, 컴퓨터, 전자 컴포넌트, 또는 마이크로프로세서에 의해 실행되는 더 높은 수준의 코드를 포함하는 파일을 포함한다.
- [0251] 상기 논의는 주로 소프트웨어를 실행하는 마이크로프로세서 또는 멀티-코어 프로세서를 참조하지만, 일부 실시예들은, ASIC(application specific integrated circuit) 또는 FPGA(Field Programmable Gate Array) 등의 하나 이상의 집적 회로에 의해 수행된다. 일부 실시예들에서, 이러한 집적 회로는 회로 자체에 저장된 명령어를

실행한다.

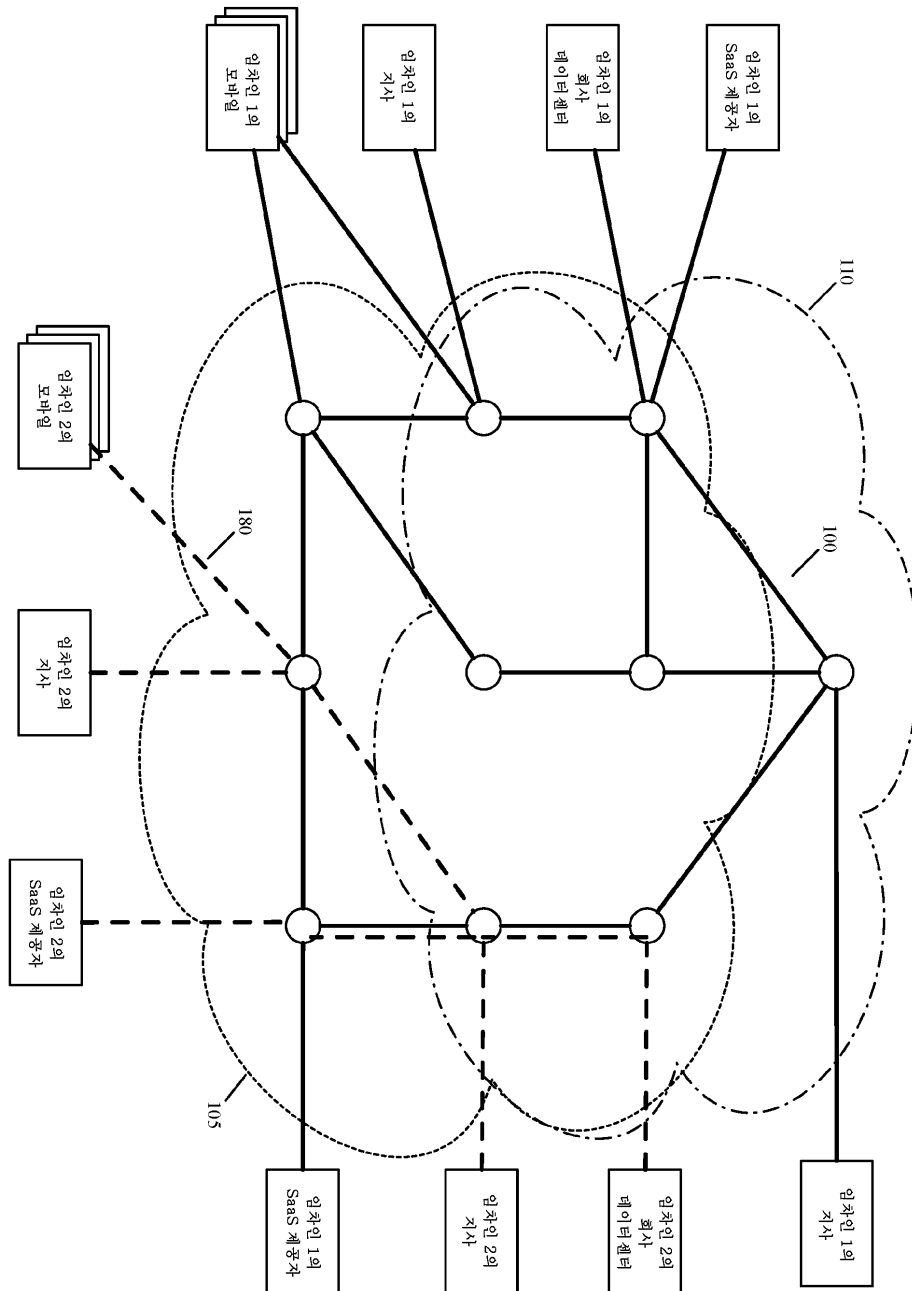
- [0252] 본 명세서에서 사용될 때, 용어 "컴퓨터", "서버", "프로세서", 및 "메모리"는, 모두, 전자적 또는 다른 기술의 디바이스를 지칭한다. 이들 용어는, 사람들 또는 사람들의 그룹을 제외한다. 본 명세서의 목적을 위해, 디스플레이 또는 디스플레이 수단이라는 용어는, 전자 디바이스 상에서의 디스플레이를 의미한다. 본 명세서에서 사용될 때, "컴퓨터 판독가능한 매체", "컴퓨터 판독가능한 매체들" 및 "머신 판독가능한 매체"라는 용어는, 컴퓨터에 의해 판독가능한 형태로 정보를 저장하는 유형의 물리적 물체로 완전히 제한된다. 이들 용어는, 임의의 무선 신호, 유선 다운로드 신호, 및 기타 임의의 임시적 또는 일시적 신호를 제외한다.
- [0253] 본 발명이 수많은 특정한 상세사항을 참조하여 설명되었지만, 본 기술분야의 통상의 기술자라면, 본 발명이 본 발명의 사상을 벗어나지 않고 다른 특정한 형태로 구현될 수 있다는 것을 인식할 것이다. 예를 들어, 위에서 설명된 몇 가지 예는, 가상 네트워크 제공자의 회사 임차인의 가상 회사 WAN을 나타낸다. 본 기술분야의 통상의 기술자라면, 일부 실시예들에서, 가상 네트워크 제공자는, 비-회사 임차인(예를 들어, 학교, 단과대학, 대학, 비영리 단체 등)을 위한 하나 이상의 공용 클라우드 제공자의 여러 공용 클라우드 데이터센터들을 통해 가상 네트워크를 배치한다는 것을 인식할 것이다. 이들 가상 네트워크는, 비-회사 엔티티의 복수의 컴퓨팅 엔드포인트(예를 들어, 사무실, 데이터센터, 컴퓨터 및 원격 사용자의 디바이스 등)를 접속하는 가상 WAN이다.
- [0254] 전술된 여러 실시예들은 오버레이 캡슐화 헤더에 다양한 데이터를 포함한다. 본 기술분야의 통상의 기술자라면, 다른 실시예들은 이 데이터 모두를 중계하기 위해 캡슐화 헤더를 이용하지 않을 수도 있다는 것을 깨달을 것이다. 예를 들어, 오버레이 캡슐화 헤더에 임차인 식별자를 포함시키는 것 대신에, 다른 실시예들은, 데이터 메시지를 포워딩하는 CFE들의 주소들로부터 임차인 식별자를 도출한다, 예를 들어, 상이한 임차인들이 공용 클라우드에 배치된 그들 자신의 MFN들을 갖는 일부 실시예들에서, 임차인 식별은 임차인 메시지를 처리하는 MFN의 식별과 연관된다.
- [0255] 또한, 여러 도면들은 본 발명의 일부 실시예들의 프로세스를 개념적으로 나타낸다. 다른 실시예들에서, 이들 프로세스의 특정한 동작은, 이들 도면에 도시되고 기술된 순서 그대로로 수행되지 않을 수 있다. 특정한 동작은, 하나의 연속된 일련의 동작들에서 수행되지 않을 수 있고, 상이한 실시예들에서는 상이한 특정한 동작이 수행될 수 있다. 또한, 프로세스는, 여러 개의 서브-프로세스를 이용하여, 또는 더 큰 매크로 프로세스의 일부로서 구현될 수 있다. 따라서, 본 기술분야의 통상의 기술자라면, 본 발명은 전술된 예시적인 상세사항에 의해 제한되는 것이 아니라, 첨부된 청구항들에 의해 정의된다는 것을 이해할 것이다.

도면

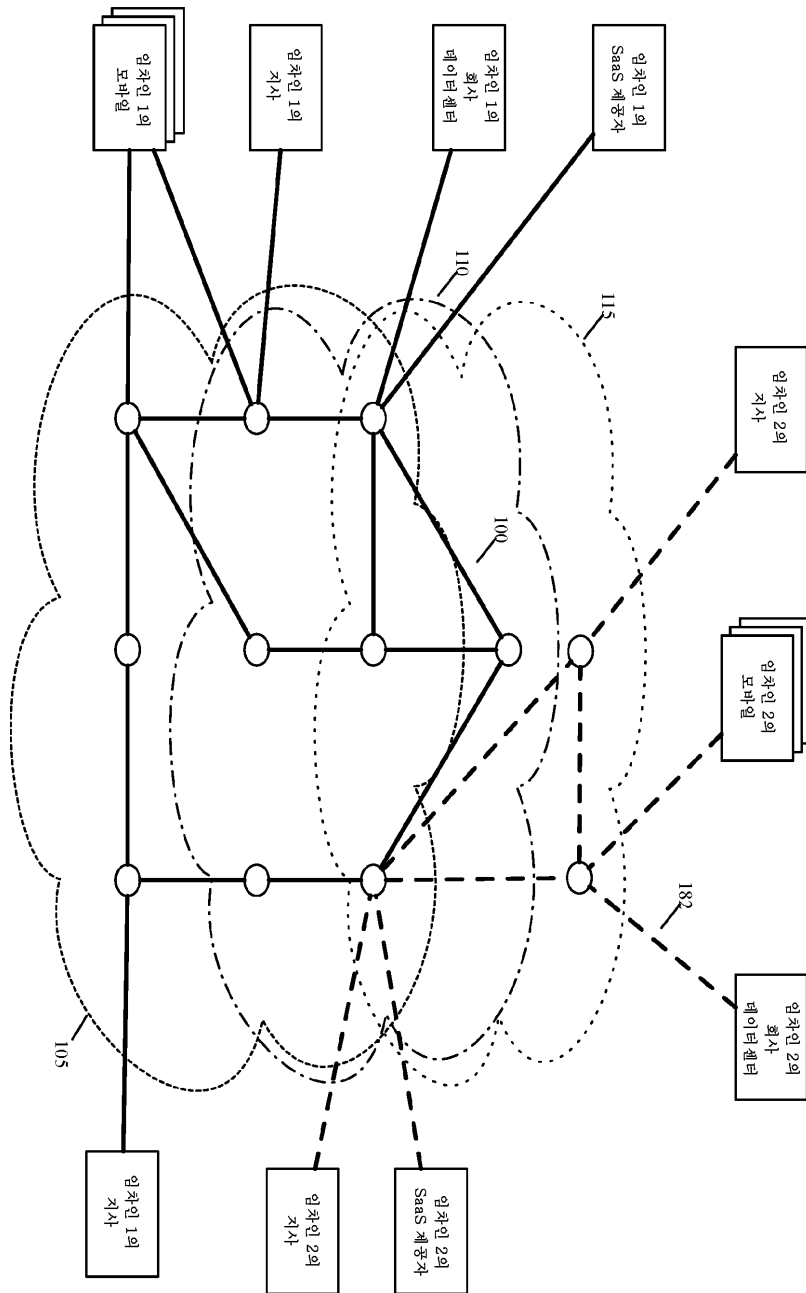
도면1a



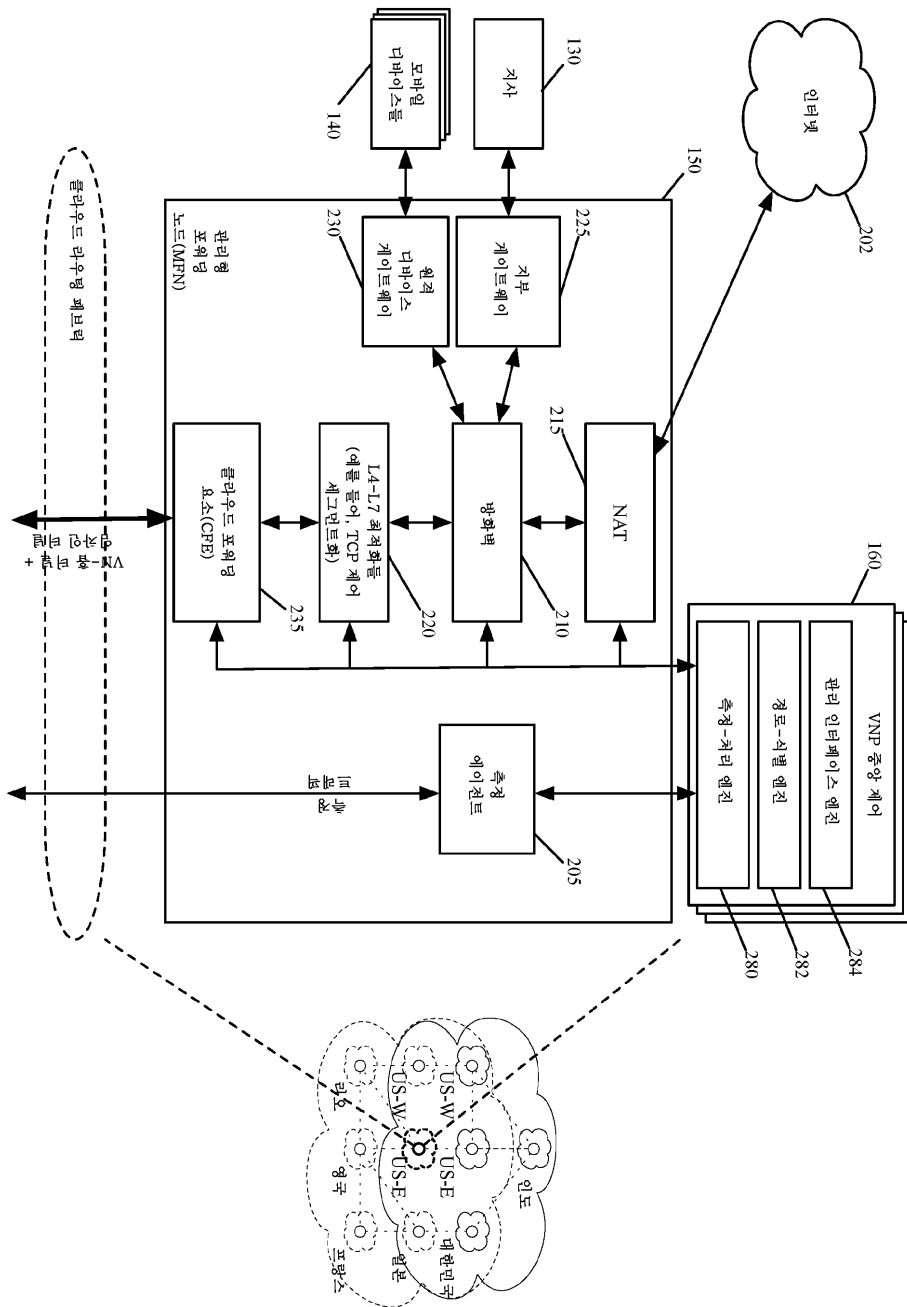
도면1b



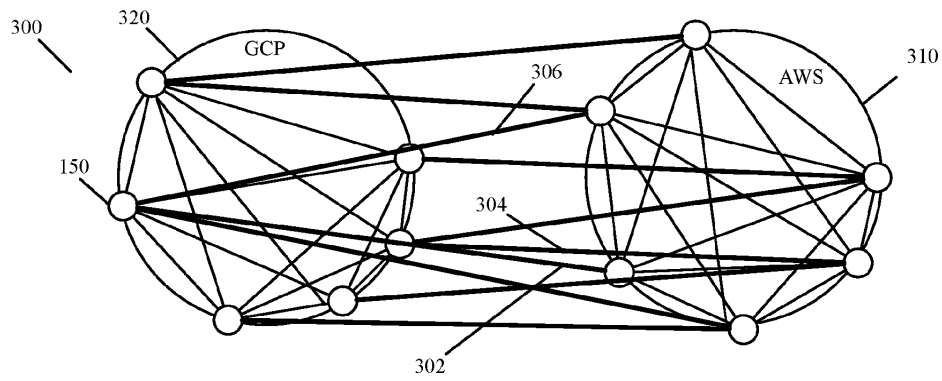
도면1c



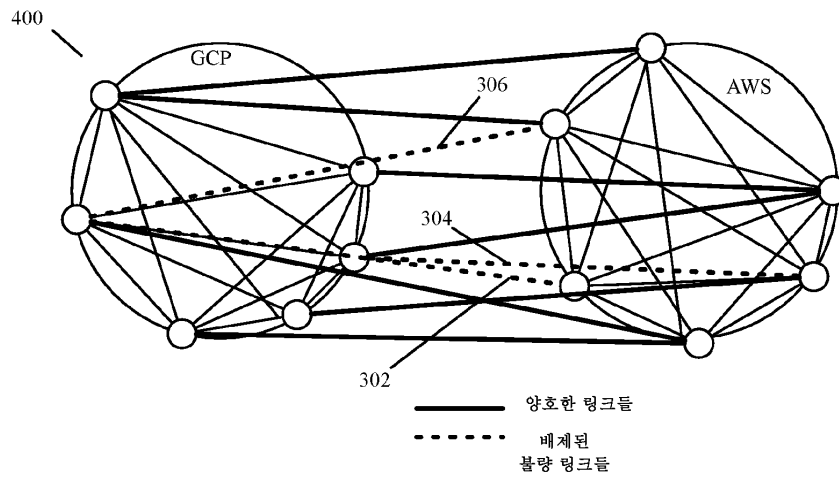
도면2



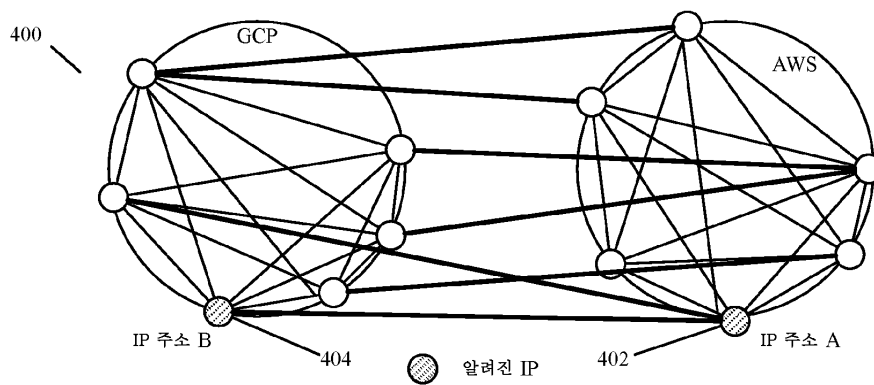
도면3



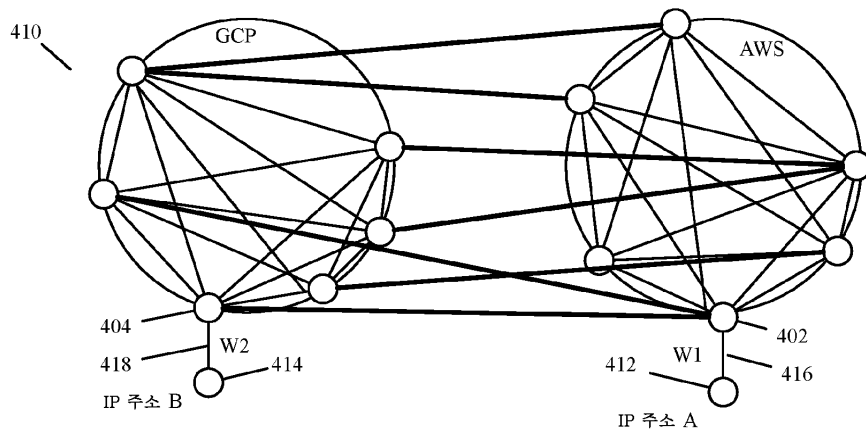
도면4a



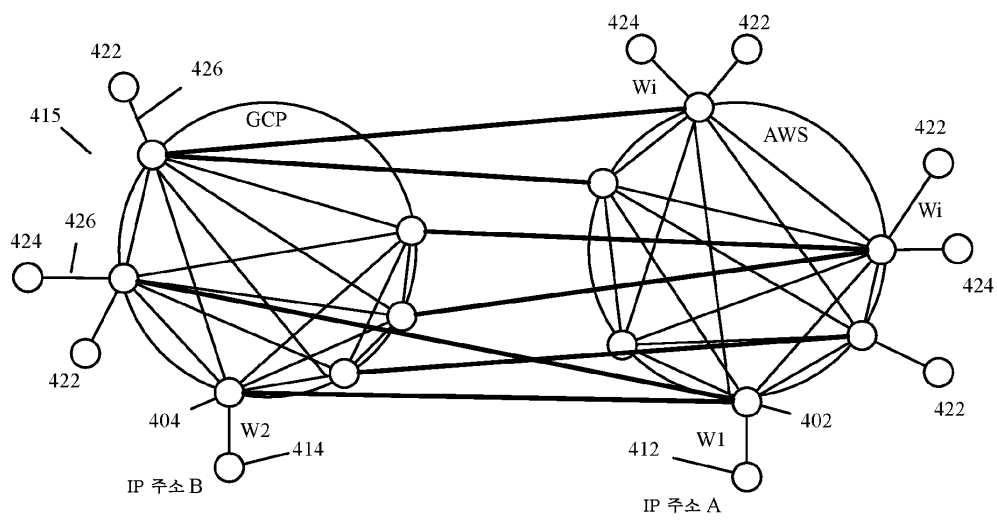
도면4b



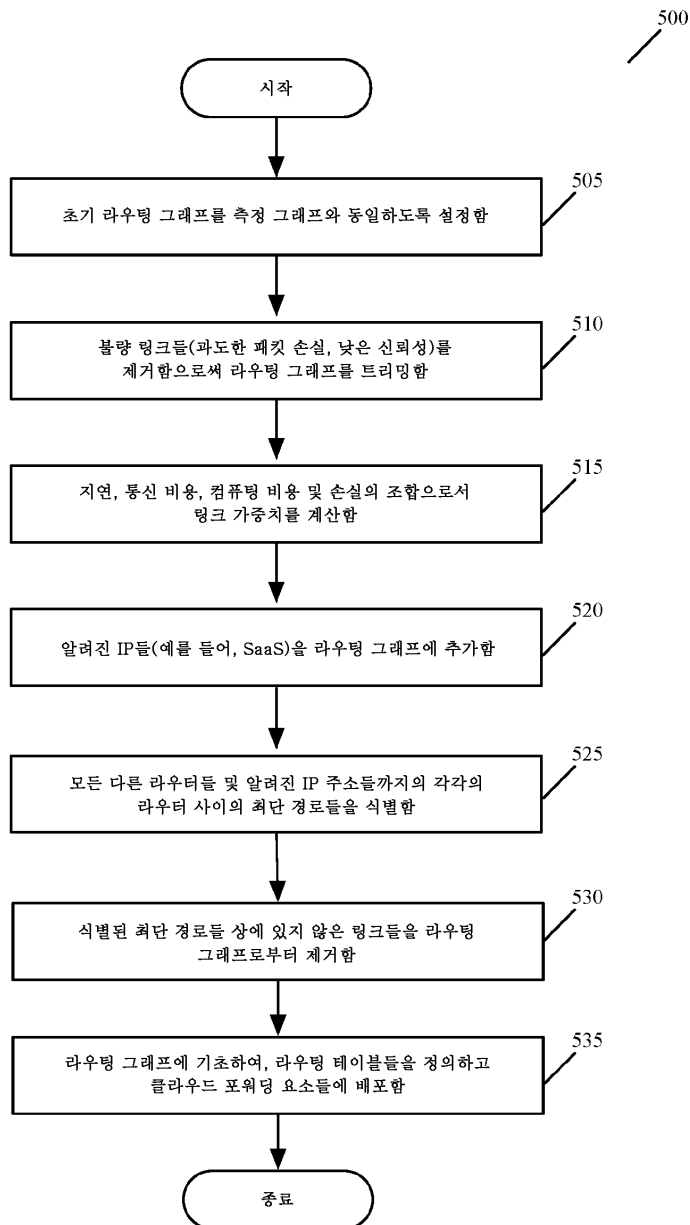
도면4c



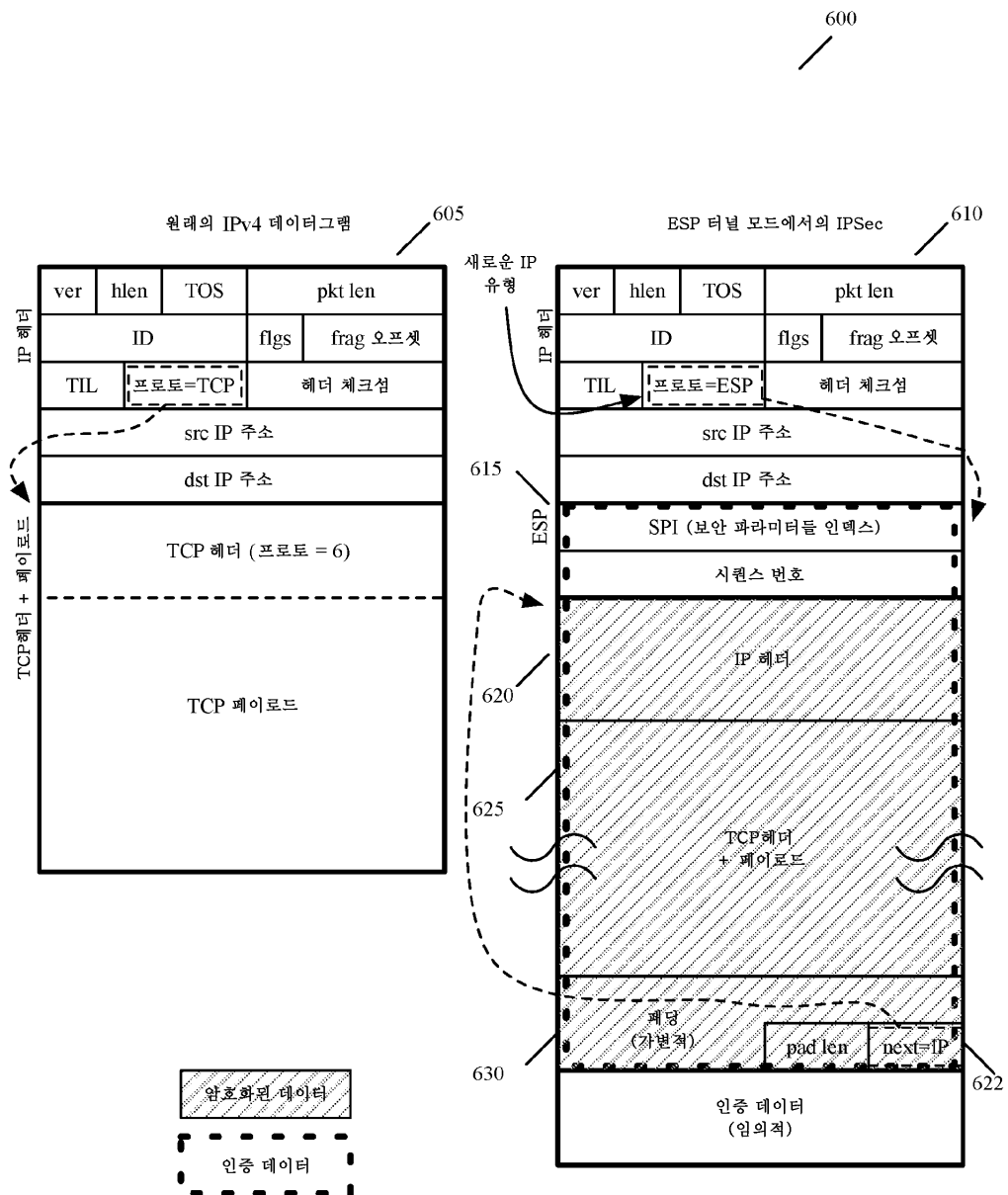
도면4d



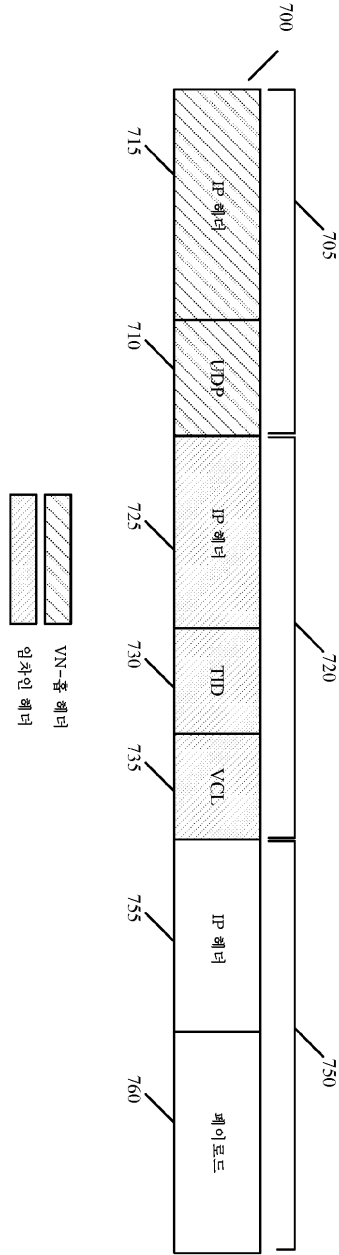
도면5



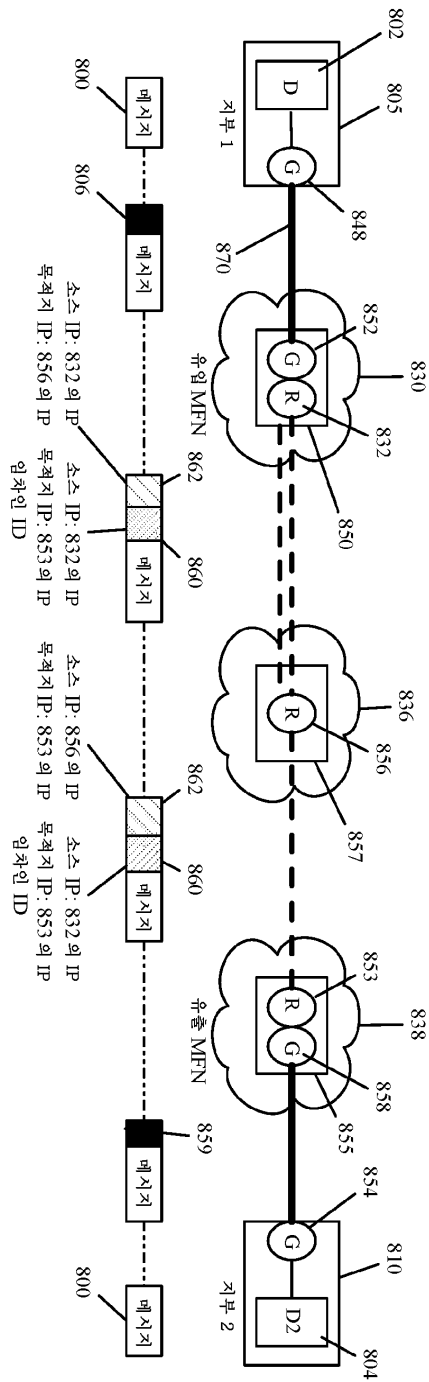
도면6



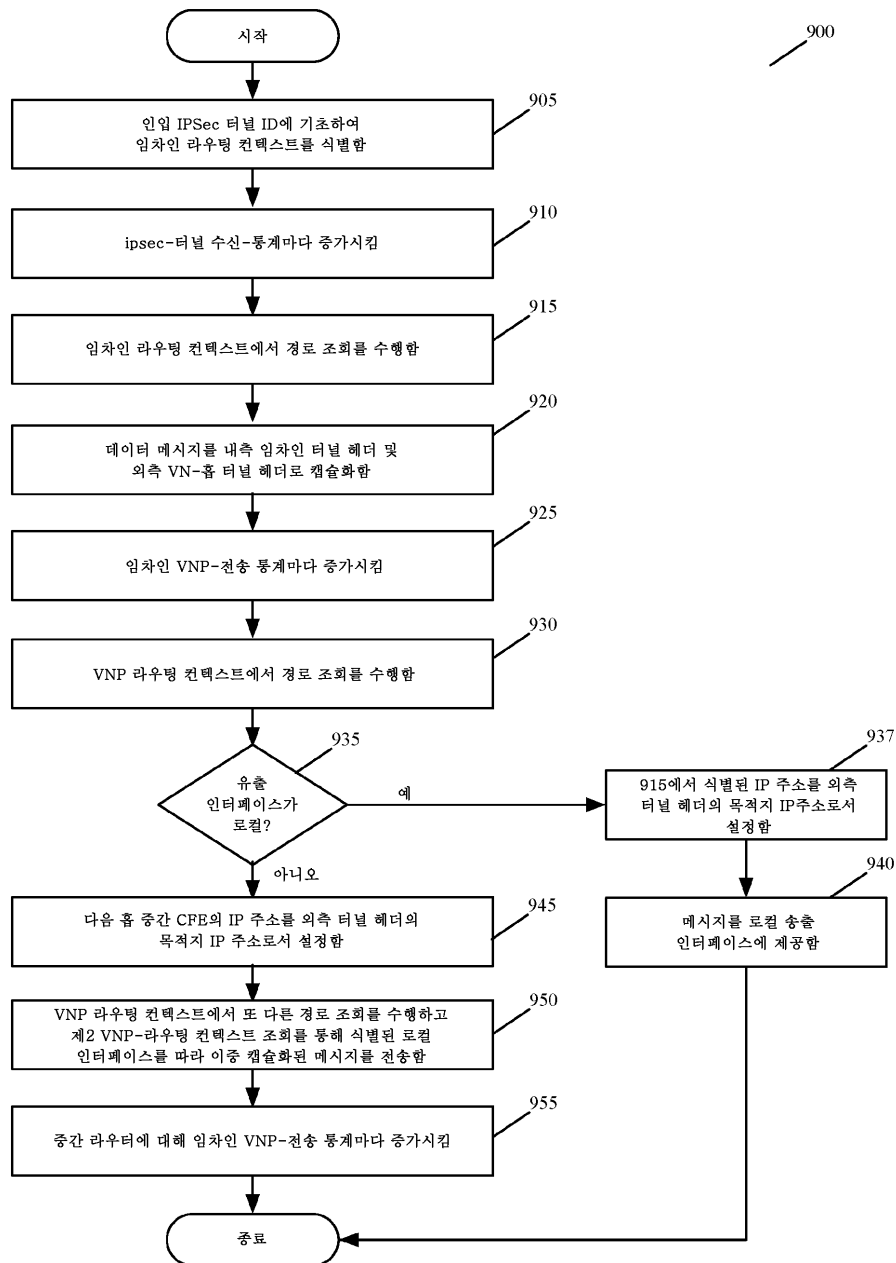
도면7



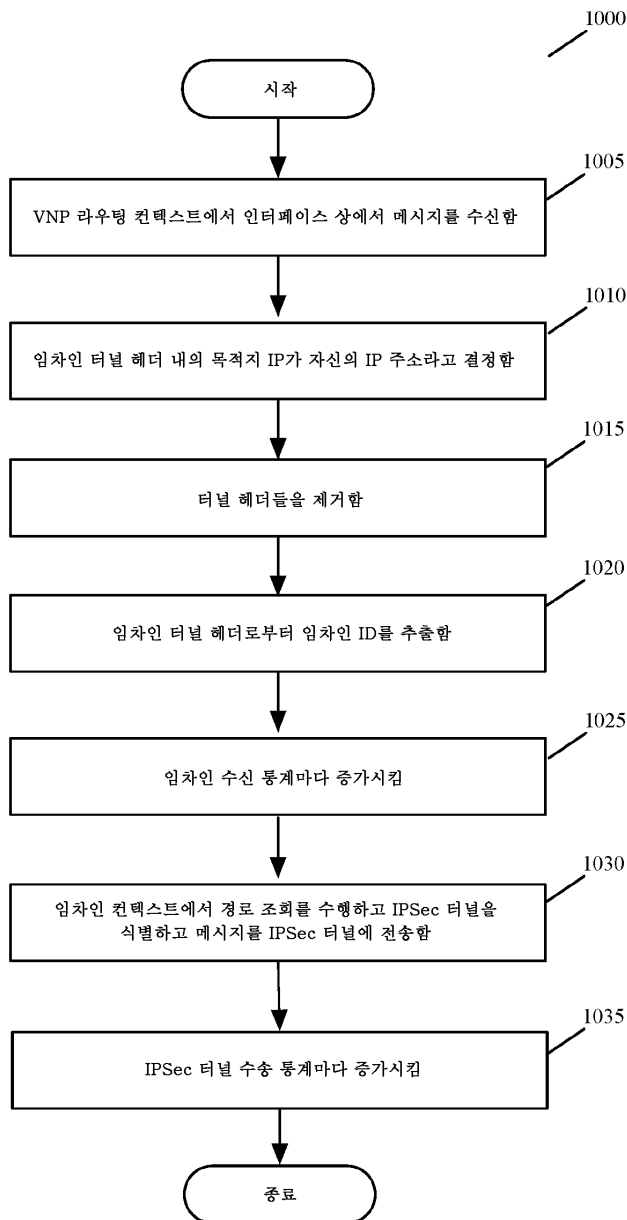
도면8



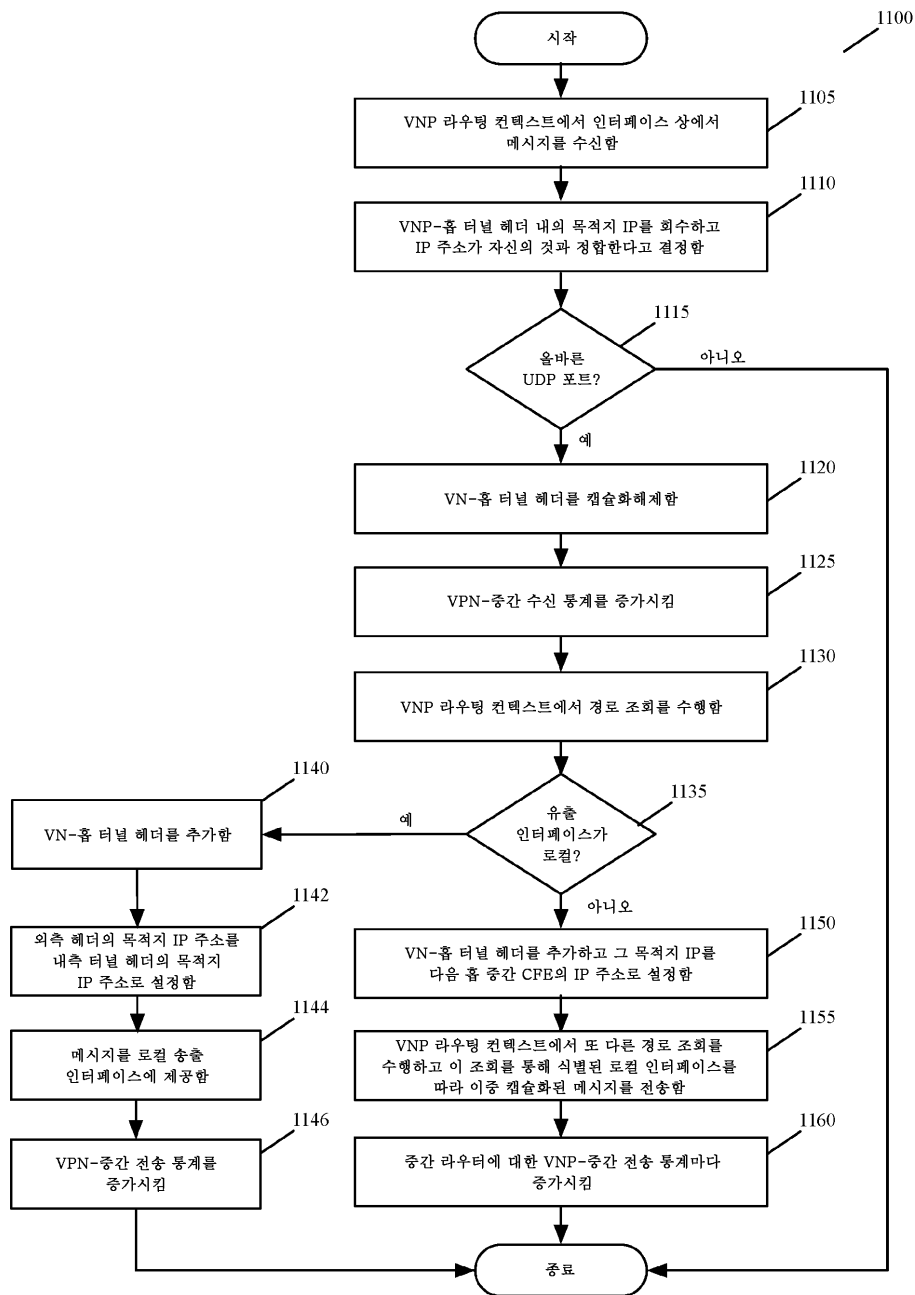
도면9



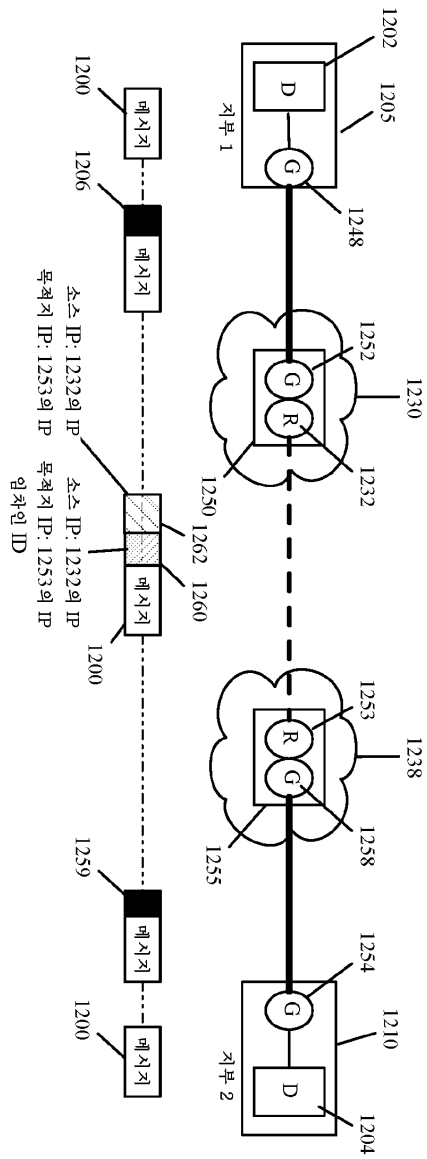
도면10



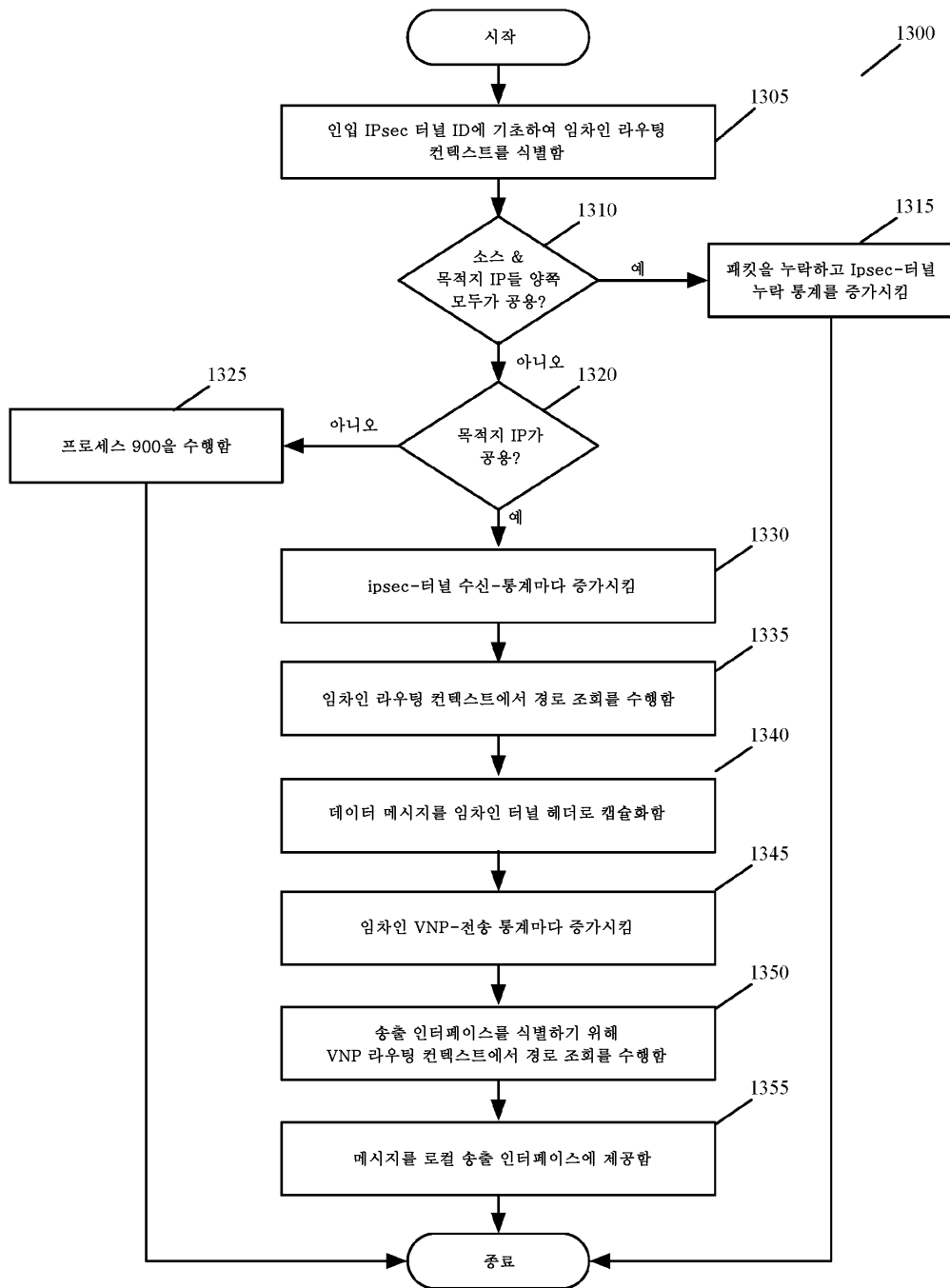
도면11



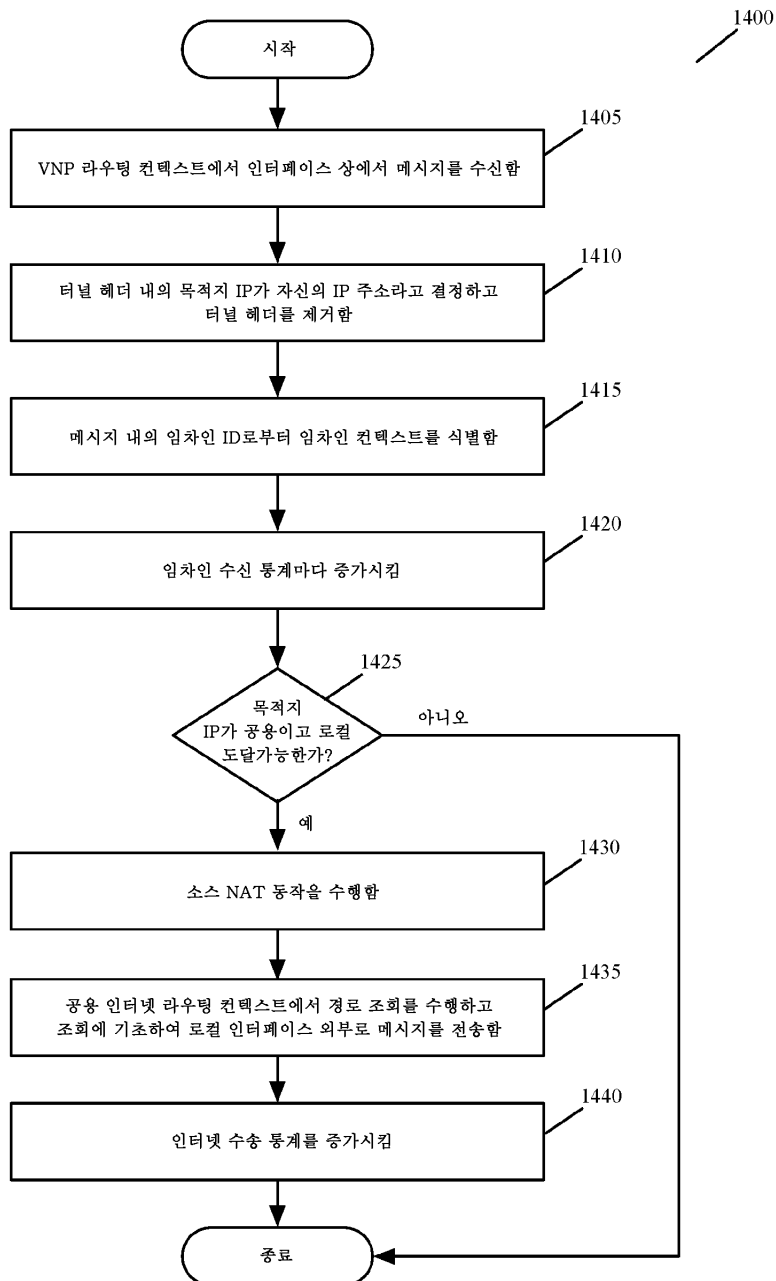
도면12



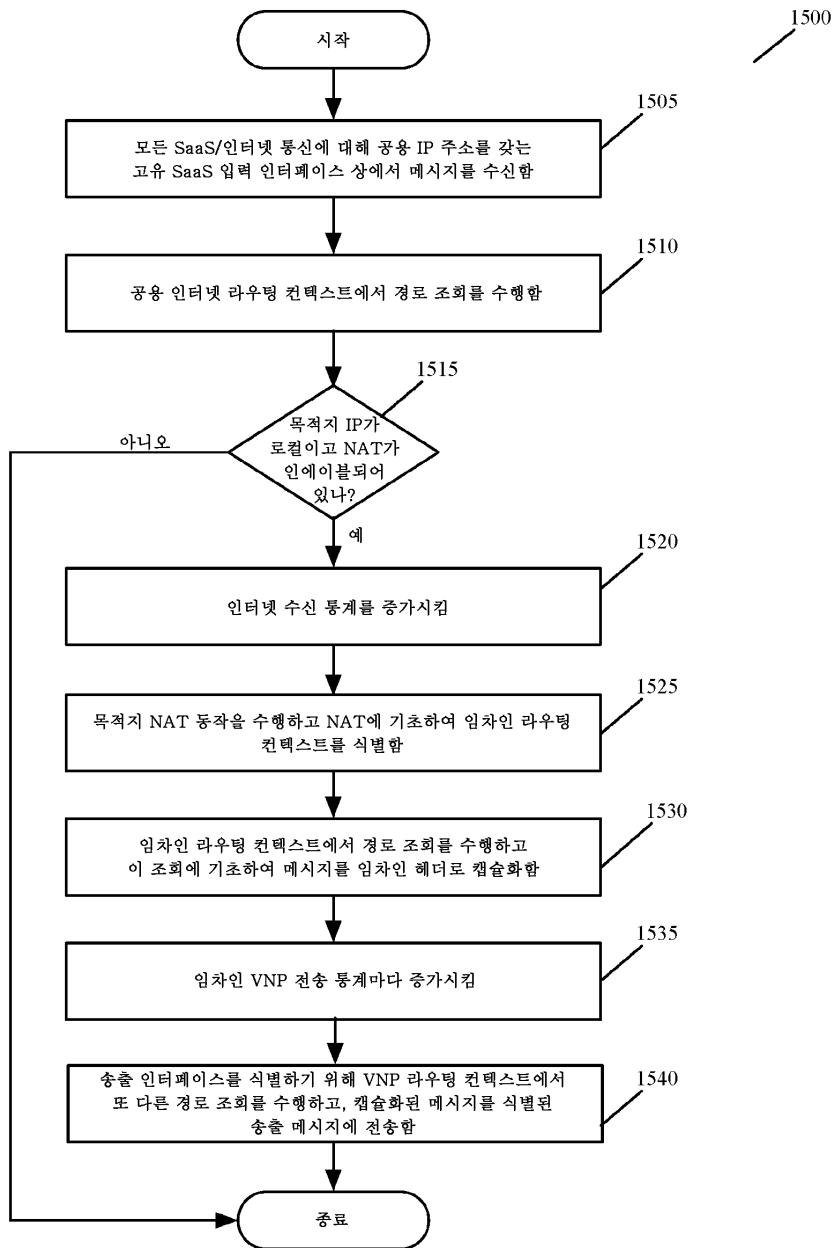
도면13



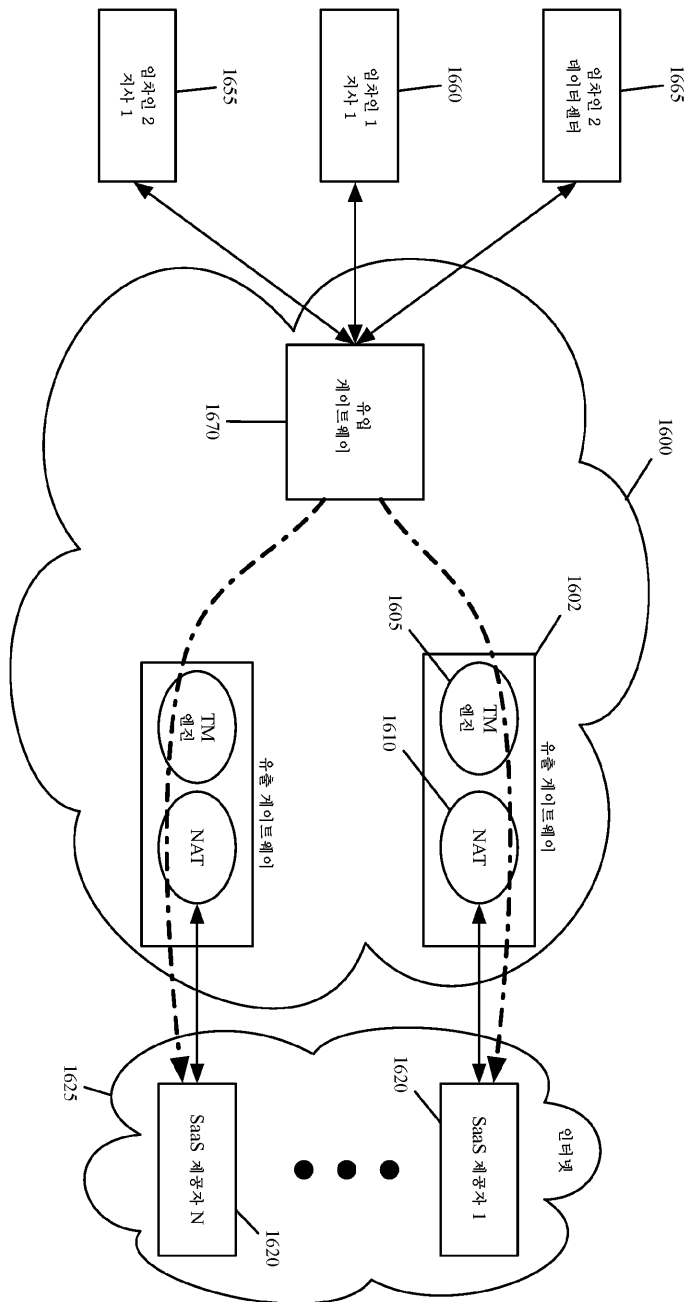
도면14



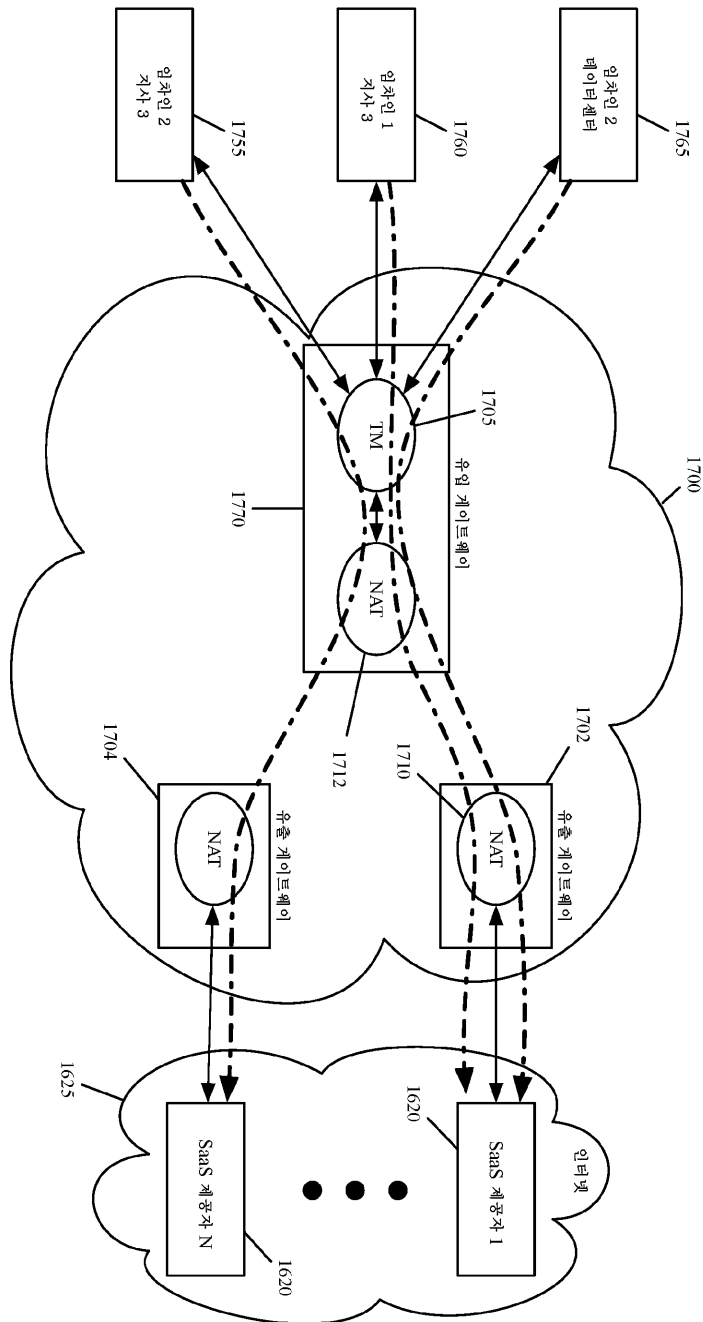
도면15



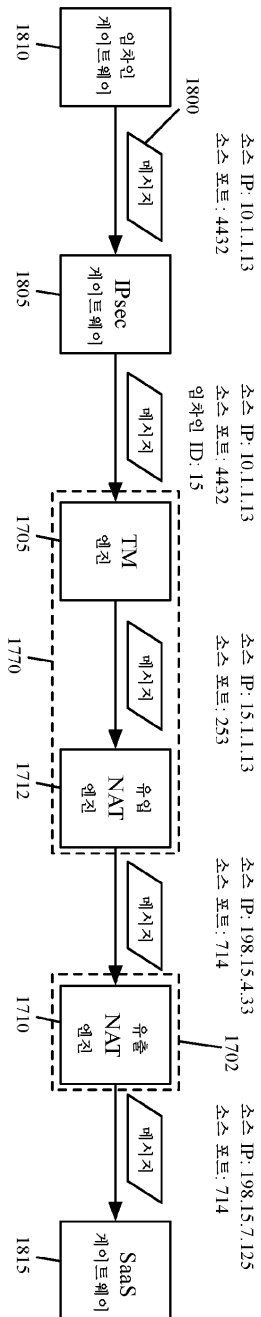
도면16



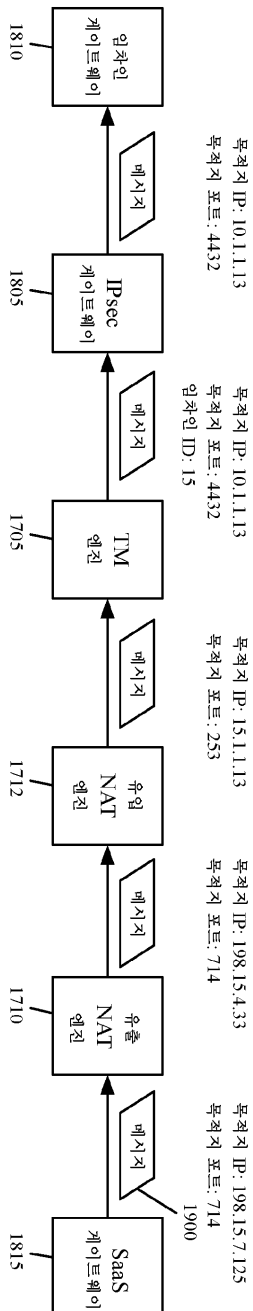
도면17



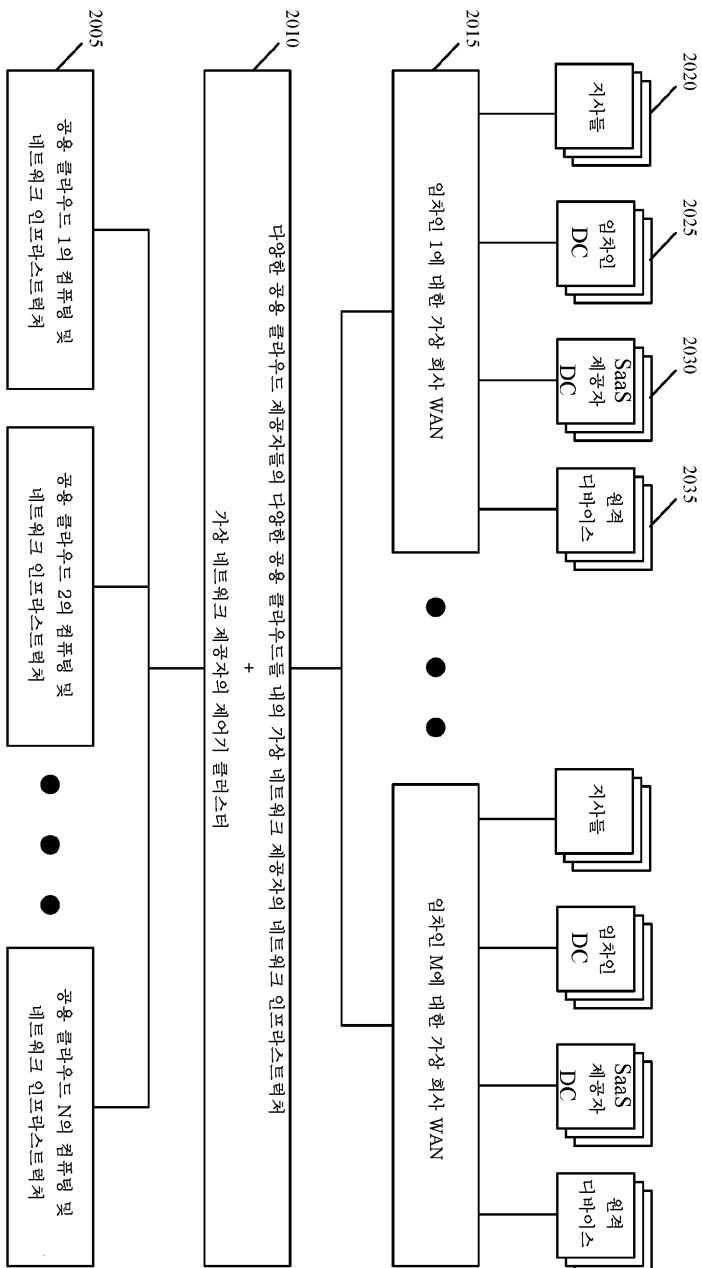
도면18



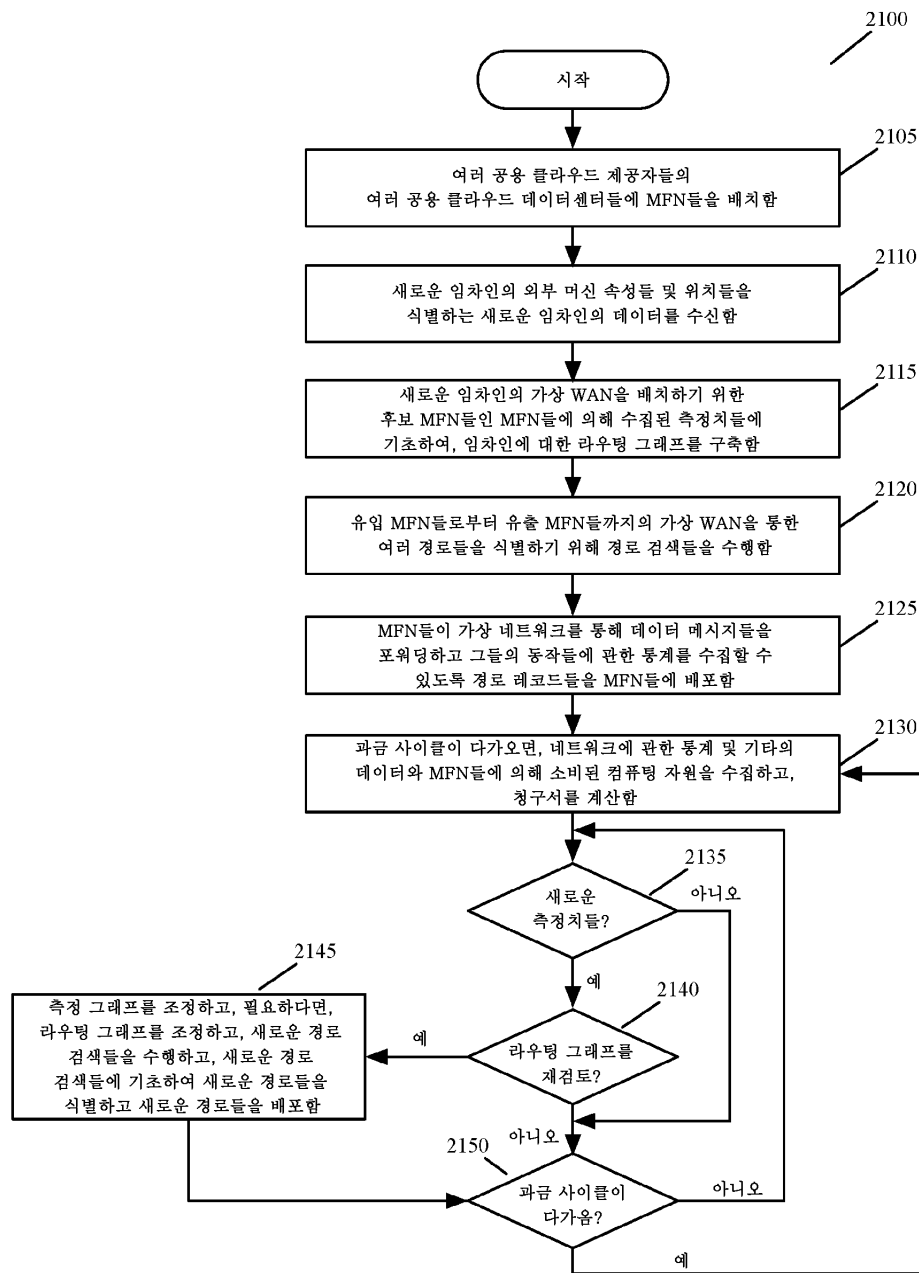
도면19



도면20



도면21



도면22

