(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0099366
(43) 공개일자 2024년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 45/42* (2022.01)
(52) CPC특허분류
H04L 63/0272 (2013.01)
H04L 45/42 (2022.05)
(21) 출원번호 10-2024-7017885
(22) 출원일자(국제) 2022년06월23일
심사청구일자 없음
(85) 번역문제출일자 2024년05월28일
(86) 국제출원번호 PCT/US2022/034753
(87) 국제공개번호 WO 2023/075869
국제공개일자 2023년05월04일
(30) 우선권주장
17/515,093 2021년10월29일 미국(US)

(71) 출원인
오라클 인터내셔날 코포레이션
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500
(72) 발명자
크레거-스티클스, 루카스 마이클
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내
카르케라, 아비만 야쉬팔라
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내
(뒷면에 계속)
(74) 대리인
특허법인에이아이피

전체 청구항 수 : 총 21 항

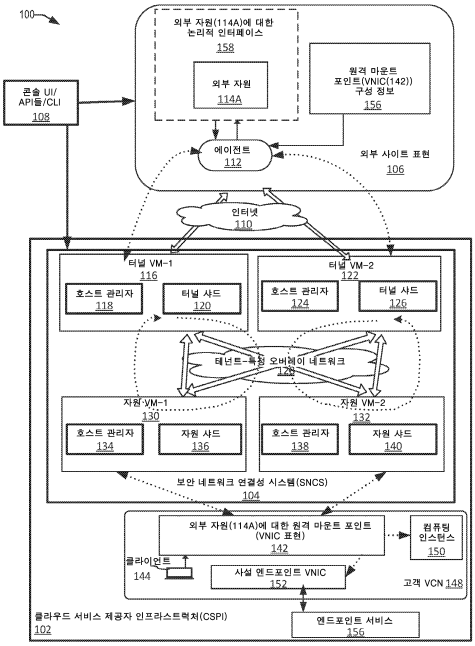
(54) 발명의 명칭 **사설 네트워크들 사이의 보안 양방향 네트워크 연결성 시스템**

(57) 요 약

고객의 사내 환경에 상주하는 외부 자원들과 클라우드에 상주하는 고객의 자원들 사이에 보안 사설 네트워크 연결성을 제공하는 클라우드 서비스 제공자 인프라스트럭처(cloud service provider infrastructure; CSPI) 내의 보안 사설 네트워크 연결성 시스템(secure private network connectivity system; SNCS)이 설명된다. SNCS는,

(뒷면에 계속)

대 표 도 - 도1



기업의 사용자(예를 들어, 관리자)가 외부 자원들을 명시적으로 구성하거나, 루트들을 광고하거나 또는 사이트-대-사이트 연결성을 셋업할 필요 없이, 고객의 외부 사이트 표현에 상주하는 외부 자원들과 클라우드 내의 고객의 VCN에 상주하는 자원들 및 서비스들 사이의 보안 사설 양방향 네트워크 연결성을 제공한다. SNCS는, 보안 사이트 대 사이트 네트워크 연결성을 제공하기 위해 사용되는 컴퓨팅 노드들 및 네트워크 요소들의 강건한 인프라스트럭처를 구현함으로써 고객의 사내 환경과 CSPI 사이의 네트워크 트래픽을 프로세싱하기 위한 고 성능, 스케일러블, 및 고도로 이용가능한 사이트-대-사이트 네트워크 연결을 제공한다.

(52) CPC특허분류
H04L 63/164 (2013.01)

(72) 발명자
샤, 드와니쉬 프람테시
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내
페이, 구안홍
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내
마고요크, 클레이튼 매튜
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내
카인카, 폴 제임스
미국, 캘리포니아 94065, 레드우드 쇼어스 엠에스 5오피7, 오라클 파크웨이 500 오라클 인터내셔날 코포레이션 내

명 세 서

청구범위

청구항 1

방법으로서,

클라우드 서비스 제공자에 구현된 보안 네트워크 연결성 시스템에 의해, 상기 클라우드 서비스 제공자의 고객과 연관된 사내 네트워크와 상기 고객에 대해 상기 클라우드 서비스 제공자에 의해 호스팅되는 가상 클라우드 네트워크(virtual cloud network; VCN) 사이의 보안 사설 네트워크 연결성을 가능하게 하기 위해 보안 네트워크 연결성 서비스를 제공하는 단계로서, 상기 보안 네트워크 연결성 시스템은 하나 이상의 컴퓨팅 노드들의 세트를 포함하는 가상 오버레이(overlay) 네트워크를 포함하는, 단계;

상기 보안 네트워크 연결성 시스템에 의해, 상기 사내 네트워크에 상주하는 외부 자원을 상기 가상 클라우드 네트워크 내의 외부 엔드포인트(endpoint)로서 등록하는 단계로서, 상기 외부 엔드포인트는 상기 가상 클라우드 네트워크 내의 인터넷 프로토콜(Internet Protocol; IP) 어드레스에 의해 식별되는, 단계;

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 제1 컴퓨팅 노드에 의해, 상기 가상 클라우드 네트워크 내의 상기 외부 엔드포인트에 대한 외부 자원 표현을 생성하는 단계로서, 상기 외부 자원 표현을 생성하는 단계는,

상기 제1 컴퓨팅 노드에 의해, 가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)를 생성하는 단계; 및

상기 제1 컴퓨팅 노드에 의해, 상기 외부 엔드포인트와 연관된 인터넷 프로토콜(IP) 어드레스를 상기 가상 네트워크 인터페이스 카드(VNIC)에 할당하는 단계를 포함하는, 상기 외부 자원 표현을 생성하는 단계;

상기 제1 컴퓨팅 노드에 의해, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 구성 정보를 상기 고객과 연관된 상기 사내 네트워크에 구성된 에이전트로 송신하는 단계;

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 제2 컴퓨팅 노드에 의해, 상기 고객과 연관된 상기 가상 클라우드 네트워크(VCN)에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신하는 단계로서, 상기 쿼리는 상기 사내 네트워크에 상주하는 상기 외부 자원에 의해 송신되며, 상기 외부 자원에는 논리적 인터페이스가 프로비저닝되는, 단계;

상기 제2 컴퓨팅 노드에 의해, 상기 사내 네트워크에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드(VNIC) 사이에 연결을 설정하는 단계;

상기 제2 컴퓨팅 노드에 의해, 상기 설정된 연결을 통해 상기 요청을 상기 가상 클라우드 네트워크에 상주하는 상기 자원으로 송신하는 단계; 및

상기 제2 컴퓨팅 노드에 의해, 상기 설정된 연결을 통해 상기 요청에 대응하는 결과를 획득하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 사내 네트워크 내의 상기 에이전트는, 상기 보안 네트워크 연결성 시스템을 포함하는 상기 하나 이상의 컴퓨팅 노드들의 세트와 상기 사내 네트워크에 상주하는 상기 외부 자원 사이에 보안 가상 사설 네트워크(Virtual Private Network; VPN) 연결을 설정하도록 구성되는, 방법.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 에이전트는, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보에 적어도 부분적으로 기초하여 상기 사내 네트워크에 상주하는 상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하도록 구성되는, 방법.

청구항 4

청구항 3에 있어서,

상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하는 단계는, 상기 에이전트에 의해, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스를 상기 논리적 인터페이스에 할당하는 단계를 포함하는, 방법.

청구항 5

청구항 3 또는 청구항 4에 있어서,

상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보는, 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스, 상기 가상 네트워크 인터페이스 카드(VNIC)와 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭(fully qualified domain name), 및 상기 고객과 연관된 상기 가상 클라우드 네트워크의 클라우드 식별자를 포함하는, 방법.

청구항 6

청구항 1 내지 청구항 5 중 어느 한 항에 있어서,

상기 제2 컴퓨팅 노드에 의해, 상기 사내 네트워크에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드 사이에 연결을 설정하는 단계는, 상기 사내 네트워크에 상주하는 상기 에이전트를 통해 상기 연결을 설정하는 단계를 포함하는, 방법.

청구항 7

청구항 1 내지 청구항 6 중 어느 한 항에 있어서,

상기 제2 컴퓨팅 노드에 의해, 상기 설정된 연결을 통해 상기 요청을 상기 가상 클라우드 네트워크에 상주하는 상기 자원으로 송신하는 단계는,

상기 제2 컴퓨팅 노드에 의해, 상기 외부 자원과 연관된 상기 물리적 IP 어드레스를 상기 고객과 연관된 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드와 연관된 상기 가상 IP 어드레스로 변환하는 단계; 및

상기 제2 컴퓨팅 노드에 의해, 상기 요청을 상기 가상 네트워크 인터페이스 카드와 연관된 상기 가상 IP 어드레스로 송신하는 단계를 포함하는, 방법.

청구항 8

청구항 1 내지 청구항 7 중 어느 한 항에 있어서,

상기 방법은, 상기 보안 네트워크 연결성 시스템에 의해, 상기 고객과 연관된 상기 사내 네트워크의 외부 사이

트 표현의 생성을 가능하게 하는 단계로서, 상기 외부 사이트 표현은 상기 사내 네트워크의 논리적 표현이고 외부 사이트 식별자 및 고객 식별자에 의해 식별되는, 단계를 더 포함하는, 방법.

청구항 9

청구항 8에 있어서,

상기 외부 자원은 상기 외부 사이트 표현에 등록되는, 방법.

청구항 10

청구항 9에 있어서,

상기 방법은, 상기 제2 컴퓨팅 노드에 의해, 상기 외부 사이트 표현에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드 사이에 상기 연결을 설정하는 단계를 더 포함하는, 방법.

청구항 11

청구항 1 내지 청구항 10 중 어느 한 항에 있어서,

상기 외부 자원은 상기 사내 네트워크에 상주하는 데이터베이스, 애플리케이션, 또는 컴퓨팅 인스턴스인, 방법.

청구항 12

클라우드 서비스 제공자의 고객과 연관된 사내 네트워크와 상기 고객에 대해 상기 클라우드 서비스 제공자에 의해 호스팅되는 가상 클라우드 네트워크(virtual cloud network; VCN) 사이의 보안 사설 네트워크 연결성을 가능하게 하기 위한 상기 클라우드 서비스 제공자에 구현된 보안 네트워크 연결성 시스템으로서, 상기 보안 네트워크 연결성 시스템은 하나 이상의 컴퓨팅 노드들의 세트를 포함하는 가상 오버레이(overlay) 네트워크를 포함하며, 상기 컴퓨팅 노드들의 세트 내의 컴퓨팅 노드는,

메모리; 및

프로세싱을 수행하도록 구성된 하나 이상의 프로세서들을 포함하며, 상기 프로세싱은,

상기 보안 네트워크 연결성 시스템에 의해, 상기 사내 네트워크에 상주하는 외부 자원을 상기 가상 클라우드 네트워크 내의 외부 엔드포인트(endpoint)로서 등록하는 동작으로서, 상기 외부 엔드포인트는 상기 가상 클라우드 네트워크 내의 인터넷 프로토콜(Internet Protocol; IP) 어드레스에 의해 식별되는, 동작;

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 제1 컴퓨팅 노드에 의해, 상기 가상 클라우드 네트워크 내의 상기 외부 엔드포인트에 대한 외부 자원 표현을 생성하는 동작으로서, 상기 외부 자원 표현을 생성하는 동작은,

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 상기 제1 컴퓨팅 노드에 의해, 가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)를 생성하는 동작; 및

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 상기 제1 컴퓨팅 노드에 의해, 상기 외부 엔드포인트와 연관된 인터넷 프로토콜(IP) 어드레스를 상기 가상 네트워크 인터페이스 카드(VNIC)에 할당하는 동작을 포함하는, 상기 외부 자원 표현을 생성하는 동작;

상기 보안 네트워크 연결성 시스템 내의 상기 제1 컴퓨팅 노드에 의해, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 구성 정보를 상기 고객과 연관된 상기 사내 네트워크에 구성된 에이전트로 송신하는 동작;

상기 보안 네트워크 연결성 시스템 내의 상기 하나 이상의 컴퓨팅 노드들의 세트의 제2 컴퓨팅 노드에 의해, 상

기 고객과 연관된 상기 가상 클라우드 네트워크(VCN)에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신하는 동작으로서, 상기 쿼리는 상기 사내 네트워크에 상주하는 상기 외부 자원에 의해 송신되며, 상기 외부 자원에는 논리적 인터페이스가 프로비저닝되는, 동작;

상기 보안 네트워크 연결성 시스템 내의 상기 제2 컴퓨팅 노드에 의해, 상기 사내 네트워크에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드(VNIC) 사이에 연결을 설정하는 동작;

상기 보안 네트워크 연결성 시스템 내의 상기 제2 컴퓨팅 노드에 의해, 상기 설정된 연결을 통해 상기 요청을 상기 가상 클라우드 네트워크에 상주하는 상기 자원으로 송신하는 동작; 및

상기 보안 네트워크 연결성 시스템 내의 상기 제2 컴퓨팅 노드에 의해, 상기 설정된 연결을 통해 상기 요청에 대응하는 결과를 획득하는 동작을 포함하는, 시스템.

청구항 13

청구항 12에 있어서,

상기 사내 네트워크 내의 상기 에이전트는, 상기 보안 네트워크 연결성 시스템을 포함하는 상기 하나 이상의 컴퓨팅 노드들의 세트와 상기 사내 네트워크에 상주하는 상기 외부 자원 사이에 보안 가상 사설 네트워크(Virtual Private Network; VPN) 연결을 설정하도록 구성되는, 시스템.

청구항 14

청구항 12 또는 청구항 13에 있어서,

상기 에이전트는, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보에 적어도 부분적으로 기초하여 상기 사내 네트워크에 상주하는 상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하도록 구성되는, 시스템.

청구항 15

청구항 14에 있어서,

상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하는 동작은, 상기 에이전트에 의해, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스를 상기 논리적 인터페이스에 할당하는 동작을 포함하는, 시스템.

청구항 16

청구항 12 내지 청구항 15 중 어느 한 항에 있어서,

상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보는, 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스, 상기 가상 네트워크 인터페이스 카드(VNIC)와 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭(fully qualified domain name), 및 상기 고객과 연관된 상기 가상 클라우드 네트워크의 클라우드 식별자를 포함하는, 시스템.

청구항 17

저장된 프로그램 코드를 갖는 비-일시적 컴퓨터-판독가능 매체로서, 상기 프로그램 코드는 동작들을 수행하기 위해 하나 이상의 프로세싱 디바이스들에 의해 실행가능하며, 상기 동작들은,

사내 네트워크에 상주하는 외부 자원을 가상 클라우드 네트워크 내의 외부 엔드포인트로서 등록하는

동작으로서, 상기 외부 엔드포인트는 상기 가상 클라우드 네트워크 내의 인터넷 프로토콜(Internet Protocol; IP) 어드레스에 의해 식별되는, 동작;

상기 가상 클라우드 네트워크 내의 상기 외부 엔드포인트에 대한 외부 자원 표현을 생성하는 동작으로서, 상기 외부 자원 표현을 생성하는 동작은,

가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)를 생성하는 동작; 및

상기 외부 엔드포인트와 연관된 인터넷 프로토콜(IP) 어드레스를 상기 가상 네트워크 인터페이스 카드(VNIC)에 할당하는 동작을 포함하는, 상기 외부 자원 표현을 생성하는 동작;

상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 구성 정보를 고객과 연관된 상기 사내 네트워크에 구성된 에이전트로 송신하는 동작;

고객과 연관된 상기 가상 클라우드 네트워크(virtual cloud network; VCN)에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신하는 동작으로서, 상기 쿼리는 상기 사내 네트워크에 상주하는 상기 외부 자원에 의해 송신되며, 상기 외부 자원에는 논리적 인터페이스가 프로비저닝되는, 동작;

상기 사내 네트워크에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드(VNIC) 사이에 연결을 설정하는 동작;

상기 설정된 연결을 통해 상기 요청을 상기 가상 클라우드 네트워크에 상주하는 상기 자원으로 송신하는 동작; 및

상기 설정된 연결을 통해 상기 요청에 대응하는 결과를 획득하는 동작을 포함하는, 비-일시적 컴퓨터-판독가능 매체.

청구항 18

청구항 17에 있어서,

상기 에이전트는, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보에 적어도 부분적으로 기초하여 상기 사내 네트워크에 상주하는 상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하도록 구성되는, 비-일시적 컴퓨터-판독가능 매체.

청구항 19

청구항 18에 있어서,

상기 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하는 동작은, 상기 에이전트에 의해, 상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스를 상기 논리적 인터페이스에 할당하는 동작을 포함하는, 비-일시적 컴퓨터-판독가능 매체.

청구항 20

청구항 17 내지 청구항 19 중 어느 한 항에 있어서,

상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 상기 구성 정보는, 상기 가상 네트워크 인터페이스 카드(VNIC)의 상기 가상 인터넷 프로토콜(IP) 어드레스, 상기 가상 네트워크 인터페이스 카드(VNIC)와 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭(fully qualified domain name), 및 상기 고객과 연관된 상기 가상 클라우드 네트워크의 클라우드 식별자를 포함하는, 비-일시적 컴퓨터-판독가능 매체.

청구항 21

컴퓨터 프로그램 명령어들을 포함하는 컴퓨터 프로그램 제품으로서, 상기 컴퓨터 프로그램 명령어들은 프로세서에 의해 실행될 때, 상기 프로세서가 동작들을 수행하게 하며, 상기 동작들은,

사내 네트워크에 상주하는 외부 자원을 가상 클라우드 네트워크(virtual cloud network; VCN) 내의 외부 엔드포인트로서 등록하는 동작으로서, 상기 외부 엔드포인트는 상기 가상 클라우드 네트워크(VCN) 내의 인터넷 프로토콜(Internet Protocol; IP) 어드레스에 의해 식별되는, 동작;

상기 가상 클라우드 네트워크(VCN) 내의 상기 외부 엔드포인트에 대한 외부 자원 표현을 생성하는 동작으로서, 상기 외부 자원 표현을 생성하는 동작은,

가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)를 생성하는 동작; 및

상기 외부 엔드포인트와 연관된 인터넷 프로토콜(IP) 어드레스를 상기 가상 네트워크 인터페이스 카드(VNIC)에 할당하는 동작을 포함하는, 상기 외부 자원 표현을 생성하는 동작;

상기 외부 자원 표현에 대한 상기 가상 네트워크 인터페이스 카드(VNIC)에 대응하는 구성 정보를 고객과 연관된 상기 사내 네트워크에 구성된 에이전트로 송신하는 동작;

고객과 연관된 상기 가상 클라우드 네트워크(virtual cloud network; VCN)에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신하는 동작으로서, 상기 쿼리는 상기 사내 네트워크에 상주하는 상기 외부 자원에 의해 송신되며, 상기 외부 자원에는 논리적 인터페이스가 프로비저닝되는, 동작;

상기 사내 네트워크에 상주하는 상기 외부 자원에 대해 프로비저닝된 상기 논리적 인터페이스와 상기 가상 클라우드 네트워크 내의 상기 외부 자원 표현에 대해 생성된 상기 가상 네트워크 인터페이스 카드(VNIC) 사이에 연결을 설정하는 동작;

상기 설정된 연결을 통해 상기 요청을 상기 가상 클라우드 네트워크(VCN)에 상주하는 상기 자원으로 송신하는 동작; 및

상기 설정된 연결을 통해 상기 요청에 대응하는 결과를 획득하는 동작을 포함하는, 컴퓨터 프로그램 제품.

발명의 설명

기 술 분 야

[0001] 관련 출원에 대한 상호 참조

[0002] 본 출원은 "Secure Bi-Directional Network Connectivity System between Private Networks"라는 명칭으로 2021년 10월 29일자로 출원된 미국 정규 특허 출원 일련번호 제17/515,093호의 PCT 출원이고 이러한 출원에 대한 35 U.S.C. 119 (e) 하에서의 이익 및 우선권을 주장하며, 이러한 출원의 내용들은 모든 목적들을 위해 그 전체가 참조로서 포함된다.

[0003] 본 출원은 "Transparent mounting of external endpoints between private networks"라는 명칭으로 2021년 10월 29일자로 출원된 출원 일련 번호 제17/515,087호와 관련되며, 이러한 출원의 전체 내용은 모든 목적들을 위해 본원에 참조로서 통합된다.

[0004] 기술분야

[0005] 본 개시내용은 전반적으로 클라우드-기반 서비스들에 관한 것이다. 더 구체적으로, 그러나 비제한적으로, 본 개시내용은, 고객의 사내(on-premise) 환경에 상주하는 외부 자원들과 클라우드에 상주하는 고객의 자원들 사이에 보안 사설 양방향 네트워크 연결성을 설정하기 위한 개선된 능력들을 포함하는 클라우드 인프라스트럭처 내의 보안 사설 네트워크 연결성 서비스를 설명한다.

배 경 기 술

[0006] 클라우드-기반 서비스들에 대한 수요는 계속해서 빠르게 증가하고 있다. 용어 클라우드 서비스는 일반적으로, 클라우드 서비스 제공자에 의해 제공되는 시스템들 및 인프라스트럭처(클라우드 인프라스트럭처)를 사용하여(예를 들어, 가입(subscription) 모델을 통해) 주문형(on demand)으로 사용자들 또는 고객들에게 이용가능하게

되는 서비스를 지칭하기 위해 사용된다. 전형적으로, 클라우드 서비스 제공자의 인프라스트럭처를 구성하는 서버들 및 시스템들은 고객의 자체적인 사내 서버들 및 시스템들로부터 분리된다. 따라서, 고객들은, 서비스들에 대한 하드웨어 및 소프트웨어 자원들을 구매할 필요 없이 클라우드 서비스 제공자에 의해 제공되는 클라우드 서비스들 자체를 이용할 수 있다. 서비스형 소프트웨어(Software as a Service; SaaS), 서비스형 플랫폼(Platform as a Service; PaaS), 서비스형 인프라스트럭처(Infrastructure as a Service; IaaS), 및 다른 것들을 포함하여 다양하고 상이한 유형들의 클라우드 서비스들이 있다.

[0007] 클라우드 서비스들에 의해 제공되는 다수의 이점들을 활용하기 위해, 기업은 흔히 기업의 로컬 데이터 센터로부터 공용(public) 클라우드 인프라스트럭처로 사내 애플리케이션들과 데이터를 마이그레이션(migrate)해야 한다. 이러한 프로세스는 전형적으로, 기업이, 그들의 사내 데이터 센터와 클라우드 인프라스트럭처 사이에 보안 연결성을 설정하기 위해 사이트-대-사이트 네트워크 연결을 설정할 것을 요구한다. 상이한 네트워크들 사이의 네트워크 트래픽을 프로세싱하기 위한 고성능이고, 스케일러블(scalable)하며, 고도로 이용가능한 사이트-대-사이트 연결을 구성하는 것은, 특히 기업의 사내 애플리케이션들 및 데이터가 다수의 상이한 네트워크들에 걸쳐 확장될 때 기업에게 복잡하고 시간-소모적인 태스크일 수 있다.

발명의 내용

[0008] 본 개시내용은 전반적으로 클라우드-기반 서비스들에 관한 것이다. 더 구체적으로, 그러나 비제한적으로, 본 개시내용은, 고객의 사내 환경에 상주하는 외부 자원들과 클라우드에 상주하는 고객의 자원들 사이에 보안 사설 양방향 네트워크 연결성을 설정하기 위한 개선된 능력들을 포함하는 클라우드 인프라스트럭처 내의 보안 사설 네트워크 연결성 서비스를 설명한다.

[0009] 특정 실시예들에서, 보안 네트워크 연결성 시스템이 개시된다. 보안 네트워크 연결성 서비스는, 클라우드 서비스 제공자의 고객과 연관된 사내 네트워크와 고객을 위해 제공되는 클라우드 서비스에 의해 호스팅되는 가상 클라우드 네트워크(virtual cloud network; VCN) 사이의 보안 사설 네트워크 연결성을 가능하게 한다. 보안 네트워크 연결성 시스템은 하나 이상의 컴퓨팅 노드들의 세트를 포함하는 가상 오버레이(overlay) 네트워크를 포함한다. 시스템은 사내 네트워크에 상주하는 외부 자원을 가상 클라우드 네트워크 내의 외부 엔드포인트(endpoint)로서 등록한다. 외부 엔드포인트는 가상 클라우드 네트워크에서 인터넷 프로토콜(Internet Protocol; IP) 어드레스에 의해 식별된다. 시스템 내의 컴퓨팅 노드들의 세트의 제1 컴퓨팅 노드는 가상 클라우드 네트워크에서 외부 엔드포인트에 대한 외부 자원 표현을 생성한다. 외부 자원 표현은, 가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)를 생성하고 외부 엔드포인트와 연관된 인터넷 프로토콜(IP) 어드레스를 VNIC에 할당함으로써 생성된다. 그런 다음, 제1 컴퓨팅 노드는 외부 자원 표현에 대한 VNIC에 대응하는 구성 정보를 고객과 연관된 사내 네트워크에 구성된 에이전트로 송신한다.

[0010] 특정 예들에서, 시스템 내의 컴퓨팅 노드들의 세트의 제2 컴퓨팅 노드는 고객과 연관된 VCN에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신한다. 쿼리는 사내 네트워크에 상주하는 외부 자원에 의해 송신된다. 특정 구현예들에서, 외부 자원에는 논리적 인터페이스가 프로비저닝된다. 제2 컴퓨팅 노드는 사내 네트워크에 상주하는 외부 자원에 대해 프로비저닝된 논리적 인터페이스와 가상 클라우드 네트워크 내의 외부 자원 표현에 대해 생성된 VNIC 사이에 연결을 설정한다. 제2 컴퓨팅 노드는 설정된 연결을 통해 가상 클라우드 네트워크에 상주하는 외부 자원으로 요청을 송신하고, 설정된 연결을 통해 요청에 대응하는 결과를 획득한다.

[0011] 특정 실시예들에서, 사내 네트워크 내의 에이전트는, 보안 네트워크 연결성 시스템을 포함하는 하나 이상의 컴퓨팅 노드들의 세트와 사내 네트워크에 상주하는 외부 자원 사이에 보안 가상 사설 네트워크(Virtual Private Network; VPN) 연결을 설정하도록 구성된다. 특정 예들에서, 에이전트는, 외부 자원 표현에 대한 VNIC에 대응하는 구성 정보에 적어도 부분적으로 기초하여 사내 네트워크에 상주하는 외부 자원에 대한 논리적 인터페이스를 프로비저닝하도록 구성된다. 특정 예들에서, 외부 자원에 대한 상기 논리적 인터페이스를 프로비저닝하는 동작은, 에이전트에 의해, 외부 자원 표현에 대한 가상 네트워크 인터페이스 카드(VNIC)의 가상 인터넷 프로토콜(IP) 어드레스를 논리적 인터페이스에 할당하는 동작을 포함한다.

[0012] 특정 예들에서, 외부 자원 표현에 대한 VNIC에 대응하는 구성 정보는, VNIC의 가상 인터넷 프로토콜(IP) 어드레스, VNIC과 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭 및 고객과 연관된 가상 클라우드 네트워크의 클라우드 식별자를 포함한다.

[0013] 특정 예들에서, 제2 컴퓨팅 노드는, 사내 네트워크에 상주하는 외부 자원에 대해 프로비저닝된 논리적 인터페이스와 가상 클라우드 네트워크 내의 외부 자원 표현에 대해 생성된 가상 네트워크 인터페이스 카드 사이에 연결

을 설정한다.

[0014] 특정 예들에서, 제2 컴퓨팅 노드는 설정된 연결을 통해 요청을 가상 클라우드 네트워크에 상주하는 자원으로 송신한다. 이러한 프로세스는, 제2 컴퓨팅 노드에 의해, 외부 자원과 연관된 상기 물리적 IP 어드레스를 고객과 연관된 가상 클라우드 네트워크 내의 외부 자원 표현에 대한 VNIC와 연관된 가상 IP 어드레스로 변환하는 단계, 및 요청을 VNIC와 연관된 가상 IP 어드레스로 송신하는 단계를 수반한다.

[0015] 특정 예들에서, 보안 네트워크 연결성 시스템은 고객과 연관된 사내 네트워크의 외부 사이트 표현의 생성을 가능하게 한다. 외부 사이트 표현은 사내 네트워크의 논리적 표현이며, 외부 사이트 식별자 및 고객 식별자에 의해 식별된다. 특정 예들에서, 외부 자원은 외부 사이트 표현에 등록된다.

[0016] 특정 예들에서, 보안 네트워크 연결성 시스템 내의 제2 컴퓨팅 노드는, 외부 사이트 표현에 상주하는 외부 자원에 대해 프로비저닝된 논리적 인터페이스와 가상 클라우드 네트워크 내의 외부 자원 표현에 대해 생성된 가상 네트워크 인터페이스 카드 사이에 연결을 설정한다. 특정 예들에서, 외부 자원은 사내 네트워크에 상주하는 데이터베이스, 애플리케이션, 또는 컴퓨팅 인스턴스이다.

[0017] 하나 이상의 프로세서들에 의해 실행가능한 프로그램들, 코드, 또는 명령어들을 저장하는 비-일시적인 컴퓨터-판독가능 저장 매체, 방법들, 시스템들, 및 유사한 것을 포함하는 다양한 실시예들에 본 명세서에서 설명된다. 이러한 예시적인 실시예들은 본 개시내용을 제한하거나 또는 정의하도록 언급되는 것이 아니라 본 개시내용의 이해를 보조하기 위한 예들을 제공하도록 언급된다. 추가적인 실시예들이 상세한 설명에서 논의되며, 추가적인 설명이 상세한 설명에서 제공된다.

도면의 간단한 설명

[0018] 도 1은 특정 실시예들에 따른, 클라우드 서비스 제공자 인프라스트럭처(cloud service provider infrastructure; CSPI) 내의 보안 사설 네트워크 연결성 서비스를 포함하는 분산형 환경(100)을 도시한다.

도 2는 특정 실시예들에 따른, 고객의 사내 네트워크에 상주하는 고객의 외부 자원과 고객의 VCN에 상주하는 자원들 및 서비스들 사이에 보안 사설 네트워크 연결성을 제공하기 위해 도 1에 도시된 시스템들 및 서브시스템들에 의해 수행되는 동작들의 추가적인 세부사항들을 도시한다.

도 3은 특정 실시예들에 따른, 보안 사설 네트워크 연결성을 제공하기 위한 도 1에 도시된 시스템들 및 서브시스템들에 의해 수행되는 프로세스의 일 예를 도시한다.

도 4는 특정 실시예들에 따른, 고객의 사내 네트워크에 상주하는 외부 자원과 고객의 가상 클라우드 네트워크 내의 외부 자원의 표현 사이의 네트워크 패킷들의 흐름을 도시하는 흐름도이다.

도 5는 특정 실시예들에 따른, 고객의 가상 클라우드 네트워크 내의 외부 자원 표현과 고객의 사내 네트워크에 상주하는 외부 자원 사이의 네트워크 패킷들의 흐름을 도시하는 흐름도이다.

도 6은 특정 실시예들에 따른, 클라우드 서비스 제공자 인프라스트럭처에 의해 호스팅되는 가상 또는 오버레이 클라우드 네트워크를 보여주는 분산형 환경의 하이 레벨 도면이다.

도 7은 특정 실시예들에 따른, CSPI 내의 물리적 네트워크 내의 물리적 구성요소들의 단순화된 아키텍처 도면을 도시한다.

도 8은 특정 실시예들에 따른, 호스트 머신이 다수의 네트워크 가상화 디바이스(network virtualization device; NVD)에 연결되는 CSPI 내의 예시적인 배열을 도시한다.

도 9는 특정 실시예들에 따른, 다중테넌시(multitenancy)를 지원하기 위한 I/O 가상화를 제공하기 위한 NVD과 호스트 머신 사이의 연결성을 도시한다.

도 10은 특정 실시예들에 따른, CSPI에 의해 제공되는 물리적 네트워크의 단순화된 블록도를 도시한다.

도 11은 적어도 일 실시예에 따른, 서비스 시스템으로서 클라우드 인프라스트럭처를 구현하기 위한 하나의 패턴을 예시하는 블록도이다.

도 12는 적어도 일 실시예에 따른, 서비스 시스템으로서 클라우드 인프라스트럭처를 구현하기 위한 다른 패턴을 예시하는 블록도이다.

도 13은 적어도 일 실시예에 따른, 서비스 시스템으로서 클라우드 인프라스트럭처를 구현하기 위한 다른 패턴을

예시하는 블록도이다.

도 14는 적어도 일 실시예에 따른, 서비스 시스템으로서 클라우드 인프라스트럭처를 구현하기 위한 다른 패턴을 예시하는 블록도이다.

도 15는 적어도 일 실시예에 따른, 예시적인 컴퓨터 시스템을 예시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 다음의 설명에서, 설명의 목적들을 위해, 특정 세부사항들이 특정 실시예들의 완전한 이해를 제공하기 위해 기술된다. 그러나 다양한 실시예들은 이러한 특정 세부사항들 없이 실시될 수 있음이 명백할 것이다. 도면들 및 설명은 제한적인 것으로 의도되지 않는다. 단어 "예시적인"은 "예, 예증, 또는 예시로서 기능함"을 의미하도록 본 명세서에서 사용된다. "예시적인" 것으로서 본 명세서에서 설명된 임의의 실시예 또는 설계는 다른 실시예들 또는 설계들에 비해 반드시 바람직하거나 또는 유리한 것으로서 해석되지는 않아야 한다.

[0020] 본 개시내용은 전반적으로 클라우드-기반 서비스들에 관한 것이다. 더 구체적으로, 그러나 비제한적으로, 본 개시내용은, 고객의 사내 환경에 상주하는 외부 자원들과 클라우드에 상주하는 고객의 자원들 사이에 보안 사설 양방향 네트워크 연결성을 설정하기 위한 개선된 능력들을 포함하는 클라우드 인프라스트럭처 내의 보안 사설 네트워크 연결성 서비스를 설명한다.

[0021] 클라우드 인프라스트럭처는, 물리적 언더레이(underlay) 네트워크의 상단에서 실행되며 기업의 사내 네트워크로부터 안전하게 액세스가능한 플렉서블(flexible) 오버레이 가상 네트워크에서 고성능 컴퓨팅, 저장, 및 네트워크 능력들을 제공할 수 있다. 클라우드 인프라스트럭처는 기업들이 그들의 사내 워크로드(workload)들을 관리하는 것과 동일한 방식으로 그들의 클라우드-기반 워크로드들을 관리하는 것을 가능하게 한다. 따라서, 기업들은 그들의 사내 네트워크와 동일한 제어, 격리, 보안 및 예측가능한 성능을 갖는 클라우드의 모든 이점들을 취할 수 있다. 기업은 클라우드에 의해 제공되는 컴퓨팅, 메모리, 및 네트워킹 자원들을 사용하여 그들 자체의 네트워크들을 구축할 수 있다. 예를 들어, 고객은, 가상 클라우드 네트워크(virtual cloud network; VCN)들로 지칭되는 하나 또는 다수의 맞춤화가능 사설 네트워크(들)를 구축하기 위해 클라우드에 의해 제공되는 자원들을 사용할 수 있다. 고객은 이러한 고객 VCN들 상에 컴퓨팅 인스턴스들과 같은 하나 이상의 고객 자원들을 배포할 수 있다. 컴퓨팅 인스턴스들은 가상 머신들, 베어 메탈(bare metal) 인스턴스들, 및 유사한 것의 형태를 취할 수 있다. 따라서, 클라우드는, 기업들(고객들)이 고도로 이용가능한 호스팅되는 환경에서 광범위한 애플리케이션 및 서비스들을 구축하고 실행하는 것을 가능하게 하는 상보적인 클라우드 서비스들의 세트 및 인프라스트럭처를 제공한다.

[0022] 클라우드 인프라스트럭처에 의해 제공되는 다수의 이점들을 활용하기 위해, 다수의 기업들은 그들의 로컬 데이터 센터로부터 공용 클라우드 인프라스트럭처로의 사내 애플리케이션들 및 데이터의 마이그레이션(migration)을 수행한다. 기업의 로컬(즉, 사내) 데이터 센터로부터 클라우드로 워크로드들을 마이그레이션하는 것은 복잡하고 어려운 프로세스일 수 있다. 클라우드 마이그레이션 동안 경험하는 일반적인 난제들은, 기업에 의해, 수행할 마이그레이션의 유형, 이동되어야 하는 자원들의 유형, 및 자원들 사이의 데이터 종속성들을 식별하는 것을 포함한다. 워크로드들을 마이그레이션하는 동안, 일부 자원들(예를 들어, 데이터베이스들, 애플리케이션들 및 유사한 것)은, 이러한 자원들이 클라우드로 성공적으로 마이그레이션될 수 있을 때까지 특정 시간 기간 동안 사내 데이터 센터에 상주해야 할 수 있다. 특정 자원들(예를 들어, 비지니스-중요(business-critical) 자원들, 데이터 이동성 제한들을 갖는 자원들 또는 엄격한 지리적 요건들을 갖는 자원들)은, 보안상의 이유들로 클라우드로 마이그레이션되지 않고 사내 데이터 센터에 남아 있는 자원들로서 식별될 수 있다. 기업이 (클라우드 내의) 그들의 VCN으로부터 이러한 사내 자원들에 안전하게 액세스할 수 있도록 하기 위해, 보안 사설 네트워크 연결성이 고객의(기업의) 사내 데이터 센터와 고객의 VCN 사이에 설정되어야 한다. 보안 사이트-대-사이트 네트워크 연결을 셋업하는 것은 기업에게 복합하고 시간-소모적인 태스크일 수 있다. 이는 전형적으로, 기업의 사용자(예를 들어, 관리자)에 의해, 사이트-대-사이트 네트워크(예를 들어, VPN) 연결을 셋업하고, 다수의 구성 파라미터들을 셋업하며, 사이트-대-사이트 네트워크 연결성에 대해 VPN 구성요소들(예를 들어, 고객 게이트웨이 디바이스, 목표 게이트웨이 디바이스)를 셋업하기 위한 등의 네트워크 정책 레벨 관리를 필요로 한다.

[0023] 추가적으로, 사이트-대-사이트 네트워크 연결을 사용하여 그들의 VCN으로부터 그들의 사내 데이터 센터에 상주하는 원격 자산(asset)(예를 들어, 데이터베이스 또는 애플리케이션과 같은 사내 자원)에 액세스하기 위해 또는 그들의 사내 데이터 센터에 상주하는 원격 자산들이 고객의 VCN 내의 자원들 및 서비스들에 안전하게 액세스하는 것을 가능하게 하기 위해, 기업의 사용자는, 고객의 외부 환경 내의 원격 자산들과 고객의 VCN 내의 자원들

사이에 보안 연결성이 달성될 수 있도록, 루트(route) 광고들 및 네트워크 어드레스 변환들을 수행하도록 게이트웨이 디바이스들을 수동으로 구성하는 것과 같은 추가적인 태스크들을 수행해야 한다. 사용자는 또한, 트래픽(예를 들어, 네트워크 패킷들)이 고객의 VCN으로부터 원격 자산들에 도달하도록 그리고 그 반대도 마찬가지가 되도록 원격 자산을 수동으로 구성하고, 사이트-대-사이트 VPN 연결에 의해 사용되는 루트들을 포함하도록 루트 테이블을 구성하며, 사이트-대-사이트 VPN 루트들을 자동으로 전파하기 위한 루트 테이블에 대한 루트 전파를 가능하게 하고, 보안 규칙들을 업데이트해야만 하는 등이다.

[0024] 특정 실시예들에서, 고객의 사내 환경에 상주하는 외부 자원들과 클라우드에 상주하는 고객의 자원들 사이에 보안 사설 양방향 네트워크 연결성을 설정하기 위한 개선된 능력들을 갖는 클라우드 서비스 제공자 인프라스트럭처(cloud service provider infrastructure; CSPI) 내의 보안 사설 네트워크 연결성 서비스가 설명된다. 보안 사설 네트워크 연결성 서비스는 클라우드 서비스 제공자 인프라스트럭처(cloud service provider infrastructure; CSPI) 내의 보안 네트워크 연결성 시스템(secure network connectivity system; SNCS)을 사용하여 구현된다. 본 개시내용에서 설명되는 SNCS는 통상적인 클라우드-기반 네트워크 연결성 서비스들에 비해 몇몇 기술적 진보들 및/또는 개선들을 제공한다. SNCS에 의해 구현되는 개시된 새롭고 개선된 아키텍처를 사용하면, 고객의 외부 사이트 표현에 상주하는 외부 자원들과 클라우드 내의 고객의 VCN에 상주하는 자원들 및 서비스들 사이의 보안 사설 양방향 네트워크 연결성은, 기업의 사용자(예를 들어, 관리자)가 외부 자원들을 명시적으로 구성하거나, 루트들을 광고하거나 또는 사이트-대-사이트 연결성을 셋업할 필요 없이 달성될 수 있다. SNCS는, 보안 사이트 대 사이트 네트워크 연결성을 제공하기 위해 사용되는 컴퓨팅 노드들 및 네트워크 요소들의 강건한 인프라스트럭처를 구현함으로써 고객의 사내 환경과 CSPI 사이의 네트워크 트래픽을 프로세싱하기 위한 고 성능, 스케일러블, 및 고도로 이용가능한 사이트-대-사이트 네트워크 연결을 제공한다. SNCS에 의해 구현되는 네트워크 요소들 및 컴퓨팅 노드들의 강건한 인프라스트럭처를 사용함으로써, 기업의 사용자는, 그 외부 자원들이 마치 그들의 VCN 내의 임의의 다른 네이티브 자원들에 연결된 것처럼 클라우드로부터 그 외부 자원들에 안전하게 액세스할 수 있다. 추가적으로, SNCS는 고객의 사내 네트워크에 상주하는 하나 이상의 자원들이 고객의 VCN(즉, 클라우드)에 상주하는 자원들 및 서비스들에 안전하게 접근하고 액세스하는 것을 가능하게 한다. 고객의 외부 사이트 표현 내의 외부 자원들과 클라우드 내의 고객의 VCN에 상주하는 자원들 및 서비스들 사이의 보안 사설 양방향 네트워크 연결성은, 기업의 사용자(예를 들어, 관리자)가 외부 자원들을 명시적으로 구성하거나, 루트들을 광고하거나 또는 사이트-대-사이트 연결성을 셋업할 필요 없이 달성될 수 있다.

[0025] 이제 도면들을 참조하면, 도 1은 특정 실시예들에 따른, 클라우드 서비스 제공자 인프라스트럭처(cloud service provider infrastructure; CSPI) 내의 보안 사설 네트워크 연결성 서비스를 포함하는 분산형 환경(100)을 도시한다. 분산형 환경(100)은 하나 이상의 통신 네트워크들을 통해 서로 통신가능하게 결합된 다수의 시스템들을 포함한다. 이러한 통신 네트워크들은 공용 네트워크 및 사설 네트워크를 포함할 수 있다. 도 1에 도시된 분산형 환경(100)은 단지 일 예이며, 청구되는 실시예들의 범위를 과도하게 제한하려고 의도되지 않는다. 많은 변형들, 대안들, 및 수정들이 가능하다. 예를 들어, 일부 구현예들에서, 도 1에 도시된 분산형 환경은 도 1에 도시된 것보다 더 많거나 또는 더 적은 시스템들 또는 구성요소들을 가질 수 있거나, 2개 이상의 시스템들을 결합할 수 있거나, 또는 시스템들의 상이한 구성 또는 배열을 가질 수 있다.

[0026] 도 1에 도시된 예에 도시된 바와 같이, 분산형 환경(100)은, 고객들이 가입할 수 있는 서비스들 및 자원들을 제공하는 CSPI(102)를 포함한다. 특정 실시예들에서, CSPI(102)는, 고객의 사내 네트워크와 CSPI(102)에 의해 호스팅되는 고객의 VCN 사이의 보안 양방향 사설 네트워크 연결성을 제공하기 위한 능력들을 포함하는 보안 사설 네트워크 연결성 서비스를 제공한다. 도 1에 도시된 예에서, 보안 사설 네트워크 연결성 서비스는 CSPI(102) 내의 보안 네트워크 연결성 시스템(secure network connectivity system; SNCS)(104)을 사용하여 구현될 수 있다. SNCS(104)에 의해 제공되는 보안 사설 네트워크 연결성 서비스는 고객의 사내 네트워크에 상주하는 하나 이상의 자원들(본 명세서에서 외부 자원들 또는 원격 자산들로도 지칭됨)이 고객의 VCN에 상주하는 자원들 및 서비스들에 안전하게 액세스할 수 있는 것을 가능하게 한다. SNCS(104)에 의해 제공되는 보안 사설 네트워크 연결성은 추가적으로 고객의 VCN 내의 자원들 및 서비스들이 고객의 사내 네트워크에 상주하는 외부 자원들에 안전하게 액세스하는 것을 가능하게 한다. 고객은, 외부 자원들이 마치 고객의 VCN에 상주하는 임의의 다른 네이티브 자원에 연결된 것처럼 그들의 VCN 내부로부터 외부 자원들에 액세스할 수 있다. 사내 외부 자원들과 고객의 VCN(즉, 클라우드)에 상주하는 자원들 사이의 보안 액세스는, 고객(예를 들어, 기업의 사용자)이 사이트-대-사이트 연결에 의해 사용될 루트들을 구성할 필요 없이 또는 고객이 그들의 외부 자원들에 대해 임의의 변경을 수행할 필요 없이, 고객이 그들의 사내 네트워크와 클라우드 사이에 정교한 사이트-대-사이트 네트워크를 설정할 필요 없이 가능하게 될 수 있다. 고객의 사내 네트워크에 상주하는 외부 자원들과 클라우드 내의 고객의 자원들 및 서비스들 사이의 보안 양방향 연결성을 가능하게 하기 위해 SNCS(104)에 의해 수행되는 프로세싱의 추

가적인 세부사항들이 이하에서 상세하게 설명된다.

[0027] 특정 접근방식들에서, 고객의 사내 네트워크에 상주하는 외부 자원과 클라우드(예를 들어, 고객의 VCN) 내의 고객의 자원들 및 서비스들 사이의 보안 양방향 연결성은 다중-스테이지 프로세스를 사용하여 SNCS(104)에 의해 달성된다. 제1 스테이지에서, 고객과 연관된 사용자(예를 들어, 관리자)는 고객의 사내 네트워크의 "외부 사이트 표현"(106)을 생성할 수 있다. 예를 들어, 사용자는, 외부 사이트 표현(106)을 생성하기 위해 사용자의 디바이스에 의해 실행되는 커맨드 라인 인터페이스(command line interface; CLI)를 통해 또는 API들을 통해, 사용자 디바이스에 의해 수행되는 애플리케이션의 콘솔 사용자 인터페이스(user interface; UI)(108)를 통해 SNCS(104)와 상호작용할 수 있다. 외부 사이트 표현(예를 들어, 106)은 고객의 외부 사이트(예를 들어, 사내 네트워크/사내 데이터 센터)의 논리적 또는 가상 표현을 나타낼 수 있으며, 외부 사이트 식별자 및 테넌트(tenant)(고객) 식별자에 의해 식별될 수 있다. 예로서, 외부 사이트 표현(106)은, 고객의 사내 네트워크의 일부분 및 사내 네트워크에 상주하는 하나 이상의 외부 자원들의 서브세트를 논리적으로 나타내는 하이 레벨 컨테이너 자원을 나타낼 수 있다.

[0028] 제2 스테이지에서, 사용자는 에이전트(112)를 다운로드하고, 에이전트(112)를 외부 사이트 표현(106)에 설치/구성한다. 특정 실시예들에서, 에이전트(112)는, 사용자가 SNCS(104)에 의해 제공되는 보안 사설 연결성 서비스들에 가입할 때 SNCS(104)에 의해 제공되는 다운로드 패키지의 부분으로서 사용자에 의해 다운로드되는 소프트웨어 애플리케이션일 수 있다. 에이전트(112)는 콘솔 UI(108)를 통해 사용자에 의해 외부 사이트 표현(106)에 설치되고 구성될 수 있다.

[0029] 제3 스테이지에서, 에이전트(112)를 외부 사이트 표현(106)에 성공적으로 설치하면, SNCS(104)는 에이전트(112)를 인증하고 고객에 대한 테넌트-특정 오버레이 네트워크(128)의 셋업을 조정(orchestrate)할 수 있다. 테넌트-특정 오버레이 네트워크(128)는, SNCS에 의해 제공되는 서비스들에 가입한 각각의 테넌트(고객)에 대해 SNCS(104)에 의해 물리적 네트워크의 상단 상에 구축된 가상 오버레이 네트워크를 나타낼 수 있다. 테넌트-특정 오버레이 네트워크(128)는 CSPI 내에서 고객의 VCN(148)과 고객의 외부 사이트 표현(106) 사이에 보안 사설 네트워크 연결성을 설정하기 위해 사용된다. 도 1에 도시된 실시예에 도시된 바와 같이, 테넌트-특정 오버레이 네트워크(128)는, 하나 이상의 터널 호스트들(본 명세서에서 터널 가상 머신들로도 지칭됨), 즉, 터널 VM-1(116) 및 터널 VM-2(122)의 세트, 및 하나 이상의 자원 호스트들(본 명세서에서 자원 가상 머신들로도 지칭됨), 즉, 자원 VM-1(130) 및 자원 VM-2(132)의 세트를 포함하는, 컴퓨팅 노드들의 분산되고 수평으로 스케일링가능한 플리트(fleet)를 포함할 수 있다. 호스트(예를 들어, 터널 호스트 또는 자원 호스트)는, 테넌트-특정 오버레이 네트워크(128)에서 서로 상호-연결되는 컨테이너들(본 명세서에서 샤드(shard)들로도 지칭됨)의 세트로 구성될 수 있다. 터널 VM들(116 및 122)은 테넌트별 터널 샤드들을 실행하기 위해 사용된다. 예를 들어, 도 1에 도시된 바와 같이, 터널 VM-1(116)은 터널 샤드(120)를 실행하기 위해 사용되며, 터널 VM-2(122)는 CSPI의 특정 테넌트/고객에 대해 터널 샤드(126)를 실행하기 위해 사용된다. 각각의 터널 샤드(120 또는 126)은 고객의 외부 사이트 표현(106)에 대한 보안 연결성을 제공하는 것을 담당한다. 자원 VM들(130 및 132)의 세트는 테넌트별 자원 샤드들을 실행하기 위해 사용될 수 있다. 예를 들어, 도 1에 도시된 바와 같이, 자원 VM-1(130)은 자원 샤드(136)를 실행하기 위해 사용되며, 자원 VM-2(132)는 테넌트/고객에 대해 자원 샤드(140)를 실행하기 위해 사용된다. 자원 샤드는, 고객의 VCN으로부터 트래픽을 수신하고 이를 고객의 외부 사이트 표현으로 포워딩하기 위해 사용될 수 있다. 고객의 외부 사이트 표현(106)과 고객의 VCN(148) 사이에 보안 연결성을 제공하기 위한 도 1에 도시된 터널 샤드들 및 자원 샤드들에 의해 수행되는 동작들의 추가적인 세부사항들은 도 1에서 상세하게 설명된다.

[0030] 각각의 터널VM(116,122) 및 자원 VM(130, 132)은 각각 호스트 관리자(118, 134)로 추가적으로 구성된다. 호스트 관리자들(118, 134)은 터널 VM들 및 자원 VM들 상에서 실행되는 프로세스들을 나타낸다. 호스트 관리자들(118 또는 134)은, 터널 및 자원 샤드들을 생성하기 위해 사용되는 API들을 구현할 수 있다. 특정 구현예들에서, 호스트 관리자들(118, 134)은 스테이트리스(stateless)일 수 있으며, 생성될 샤드의 유형(터널 또는 자원 샤드) 및 샤드의 특정 구성과 관련하여 (API들(108)을 통해) 사용자로부터 명령어(instruction)들을 수신함으로써 명령형 모드(imperative mode)로(즉, 호스트 관리자가 수행하기 위한 커맨드들의 시퀀스로서) 동작할 수 있다. 호스트 관리자들은, 터널 샤드들 및 자원 샤드들의 상태를 수집하고 모니터링하는 것을 추가로 담당할 수 있다.

[0031] SNCS(104)가 이상에서 설명된 바와 같이 고객에 대한 테넌트-특정 오버레이 네트워크(128)를 셋업한 이후에, 제4 스테이지에서, 사용자는 사내 자산(예를 들어, 외부 자원(114A))을 그들의 VCN 내의 외부 엔드포인트로서 외부 사이트 표현(106)에 등록한다. 외부 자원(114A)은, 고객이 고객의 VCN에 상주하는 자원들 및 서비스들과 보안 양방향 연결성을 설정하는 것을 의도하는 고객의 사내 네트워크에 상주하는 데이터베이스, 컴퓨팅 인스턴스, 애플리케이션 또는 유사한 것과 같은 사내 자원 또는 자산을 나타낼 수 있다. 외부 자원(114A)을 등록하기

위해, 사용자는 (콘솔 UI(108)를 통해) 그들의 VCN(148) 내로부터의 보안 사설 네트워크 연결성이 가능하게 될 외부 자원들(예를 들어, 114A)을 식별하고, 콘솔 UI(108)를 사용하여(또는 API들을 통해) 외부 자원을 그들의 VCN 내의 외부 엔드포인트로서 등록한다. 외부 자원을 등록하는 것의 부분으로서, 사용자는, SNCS에 의해 제공되는 콘솔 UI 또는 API들을 통해 외부 자원과 연관된 사내 물리적 IP 어드레스, 외부 자원들이 액세스가능한 포트 번호 및 외부 자원의 호스트명칭(또는 전체 주소 도메인 명칭(fully qualified domain name; FQDN))과 같은 외부 자원과 관련된 구성 정보를 제공한다. 사용자는 또한, 외부 자원에 대한 외부 엔드포인트가 생성될 고객의 VCN 내의 서브넷(subnet)을 선택한다. SNCS는 구성 정보를 수신하고, 고객의 VCN 내에 외부 자원에 대한 외부 엔드포인트를 생성한다. 외부 엔드포인트는 IP 어드레스, 포트 번호 및 고객의 VCN에서의 FQDN(호스트명칭)에 의해 식별된다.

[0032] 제5 스테이지에서, 그런 다음, SNCS(104)는 (제어 평면 API들을 통해) 고객의 VCN 내에 외부 엔드포인트에 대한 외부 자원 표현을 생성한다. 특정 구현예에서, 외부 자원 표현의 생성은, 원격 마운트(mount) 포인트 VNIC를 생성하는 단계 및 외부 엔드포인트와 연관된 IP 어드레스를 VNIC에 할당하는 단계를 포함한다. 그런 다음, SNCS는 (제어 평면 API들을 통해), (작업자 인터페이스를 통해) VNIC를 자원 샤드들에 논리적으로 접속(attach)시킬 수 있는 자원 VM 상에서 자원 샤드들을 생성한다.

[0033] 제6 단계에서, 에이전트(112)는 고객의 VCN(148) 내의 외부 자원 표현(114A)에 대해 생성된 VNIC(142)와 연관된 구성 정보(156)를 다운로드하고 판독하며, 구성 정보(156)를 등록된 외부 자원(114A) 상으로 카피한다. 구성 정보는, 예를 들어, VNIC의 가상 IP 어드레스, VNIC과 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭 및 고객과 연관된 가상 클라우드 네트워크의 클라우드 식별자를 포함할 수 있다. 구성 정보(156)를 사용하여, 에이전트(112)는 외부 자원(114A)에 대한 논리적 인터페이스(158)를 생성/프로비저닝한다. 논리적 인터페이스(158)는 IP 어드레스로 구성된 소프트웨어 엔티티를 나타낼 수 있다. 특정 구현예에서, 에이전트(112)에 의한 논리적 인터페이스(158)의 생성 또는 프로비저닝은, 에이전트에 의해, 외부 자원 표현에 대해 생성된 VNIC(142)에 할당된 가상 IP 어드레스를 논리적 인터페이스(158)에 할당하는 것을 포함한다.

[0034] 외부 자원(114A)에, 고객의 VCN에 상주하는 외부 자원 표현에 대한 VNIC(142)에 대응하는 가상 IP 어드레스가 할당된 논리적 인터페이스(158)가 프로비저닝되기 때문에, 이제 외부 자원은 고객의 VCN의 부분이 되며, SNCS(104)에 의해 제공된 보안 사설 네트워크 연결성 서비스들을 사용하여 클라우드 내에 있는(예를 들어, 고객의 VCN(148) 내에 있는) 자원들 및 서비스들에 안전하게 액세스할 수 있다. 예를 들어, 외부 자원(114A)은, 에이전트(112)를 통해, SNCS(104) 내의 터널 호스트들에 대한 연결을 설정함으로써, 그 논리적 인터페이스(158)를 통해 고객의 VCN 내의 서비스(152)(예를 들어, 스트리밍 서비스 또는 객체 스토리지 서비스) 또는 고객의 VCN(148) 내의 컴퓨팅 인스턴스(150)에 안전하게 도달/액세스할 수 있다. 유사하게, 고객의 VCN(148) 내의 클라이언트 애플리케이션은, 마치 외부 자원이 고객의 VCN(148) 내의 임의의 다른 네이티브 자원에 연결된 것처럼 외부 자원의 VNIC 표현(142)을 사용하여 고객의 사내 네트워크 내의 외부 자원(114A)에 안전하게 액세스하기 위해 SNCS(104)에 의해 제공되는 서비스들을 사용할 수 있다. 이러한 방식으로, 고객의 사내 네트워크에 상주하는 외부 자원과 클라우드(예를 들어, 고객의 VCN) 내의 고객의 자원들 및 서비스들 사이의 보안 양방향 연결성은 SNCS(104)에 의해 달성된다.

[0035] 도 2는 특정 실시예들에 따른, 고객의 사내 네트워크에 상주하는 고객의 외부 자원과 고객의 VCN에 상주하는 자원들 및 서비스들 사이에 보안 사설 네트워크 연결성을 제공하기 위해 도 1에 도시된 시스템들 및 서브시스템들에 의해 수행되는 동작들의 추가적인 세부사항들을 도시한다. 도 2에 도시된 시스템들 및 서브시스템들은, 컴퓨팅 시스템, 하드웨어, 또는 이들의 조합의 하나 이상의 프로세싱 유닛들(예를 들어, 프로세서들, 코어들)에 의해 실행되는 소프트웨어(예를 들어, 코드, 명령어들, 프로그램)를 사용하여 구현될 수 있다. 소프트웨어는 비-일시적 저장 매체 상에(예를 들어, 메모리 디바이스 상에) 저장될 수 있다. 도 2에 도시된 분산형 환경(200)은 단지 일 예이며, 청구되는 실시예들의 범위를 과도하게 제한하려고 의도되지 않는다. 많은 변형들, 대안들, 및 수정들이 가능하다. 예를 들어, 일부 구현예들에서, 도 2에 도시된 분산형 환경은 도 2에 도시된 것보다 더 많거나 또는 더 적은 시스템들 또는 구성요소들을 가질 수 있거나, 2개 이상의 시스템들을 결합할 수 있거나, 또는 시스템들의 상이한 구성 또는 배열을 가질 수 있다. 발명자 여러분, 우리는 발명 1(IaaS 272.1)에서 설명된 시스템 아키텍처(SNCS)에 주로 기반하여 도 2의 시스템을 설명하였다. 이하의 도 2에 대한 설명을 검토하시고, 더 명확하게 하기 위해 필요하는 경우 추가/수정을 부탁드립니다.

[0036] 이상에서 도 1에서 설명된 바와 같이, 고객의 사내 네트워크와 CSPI(102)에 의해 호스팅되는 고객의 VCN 사이에 보안 사설 네트워크 연결성을 제공하기 위해 SNCS(104)에 의해 구현되는 연결 프로세스의 부분으로서, 고객과 연관된 사용자(예를 들어, 관리자)는 고객의 사내 네트워크의 "외부 사이트 표현"(예를 들어, 106)을 생성하고,

외부 사이트 표현 내에 에이전트(예를 들어, 112)를 구성하며, 사내 자산을 외부 사이트 표현에 등록하고, 등록된 외부 자원에 대한 고객의 VCN 내의 원격 마운트 포인트(본 명세서에서 엔드포인트로도 지칭됨)를 생성한다. 외부 사이트 표현에 에이전트(예를 들어, 112)를 성공적으로 설치하면, 에이전트(112)는 공용 네트워크(예를 들어, 인터넷(110))을 통해 SNCS(104)에 대한 가상 사설 네트워크(Virtual Private Network; VPN) 연결(본 명세서에서 VPN 터널로도 지칭됨)을 설정한다. VPN 연결은 고객의 외부 사이트 표현(106)과 고객의 VCN(148) 사이의 암호화된 연결이다. 특정 구현예에서, VPN 연결은 인터넷(110)을 통해 SNCS(104)에 대한 보안 사설 네트워크 연결성을 설정하기 위해 보안 터널링 프로토콜(예를 들어, 계층 2 터널링 프로토콜(Layer 2 Tunneling Protocol; L2TP) 프로토콜)을 사용한다. 에이전트(112)가 외부 사이트 표현(106)에 설치될 때, 에이전트는, 외부 게이트웨이 어플라이언스(112)와 연관된 구획(compartment) 식별자 및 외부 사이트 표현 식별자와 같은 정보를 구성 파일로 SNCS(104)에 전달함으로써 에이전트 자신을 SNCS(104)로 활성화하기 위해 부트스트랩(bootstrap) 프로세스를 시작한다. 에이전트(112)가 자신을 부스트스트랩할 때, 이는 등록 및 활성화 프로세스를 시작하는 SNCS의 제어 평면과 통신한다. 활성화 프로세스 동안, 제어 평면은, 게이트웨이 어플라이언스가 VPN 서버에 대한 보안 터널 연결을 설정하기 위해 필요로 하는 모든 필요한 정보(예를 들어, 인증서, 공인 IP(Public IP) 및 유사한 것)를 다시 전송한다. 그런 다음, 에이전트(112)는, SNCS에 설치된 VPN 서버에 대한 보안 VPN 터널 연결을 개방하는 VPN 클라이언트 프로그램을 실행함으로써 SNCS(104)에 대한 보안 VPN 연결성을 설정한다. 보안 터널은, SNCS(104) 내의 터널 VM(예를 들어, 116) 상에 위치된 터널 샤드(예를 들어, 120)에서 종료된다.

[0037] 도 1에 도시된 특정 구현예에서, 에이전트(112)는, 각각 터널 샤드들, 즉, 터널 샤드-1(120) 및 터널 샤드-2(126)에서 실행 중인 2개의 상이한 VPN 서버들, 즉, VPN 서버-1(224) 및 VPN 서버-2(226) 상에서 종료되는 터널들을 설정하도록 각각 구성된 2개의 VPN 클라이언트들, 즉, VPN 클라이언트-1(206) 및 VPN 클라이언트-2(208)로 구성된다. 도 2에 도시된 구현예에서, 에이전트(112)의 모든 물리적 설치는 2개의 터널들의 설정을 가져오며, 따라서 하나의 터널이 다운되는 경우, 트래픽(즉, 네트워크 패킷들)은 자동으로 다른 터널을 통해 라우팅될 수 있다. 도 2에 도시된 특정 구현예가 2개의 터널들을 도시하지만, 다른 구현예들에서, SNCS(104)는 에이전트(112)의 모든 물리적 설치에 대해 3개 이상의 중복 터널들을 구현하도록 구성될 수 있거나 또는 에이전트(112)의 설치 시에 단일 터널만을 구현할 수 있다.

[0038] 특정 실시예들에서, 에이전트(112)는 터널 샤드들(120 및 126)과의 BGP 피어링 세션을 설정하기 위해 보더 게이트웨이 프로토콜(Border Gateway Protocol; BGP)과 같은 표준 외부 게이트웨이 프로토콜을 사용한다. BGP를 사용하면, 에이전트(112)는 에이전트(112) 내에 구현된 공용(public) 인터페이스(220)를 통해 터널 샤드들과 라우팅 및 도달가능성을 교환한다. BGP 피어링 세션들에 대해 필요한 구성 정보의 부분으로서, 에이전트(112)는 자신의 사내 IP 어드레스를 그 로컬 루트 테이블(212)(본 명세서에서 라우팅 정보 베이스(routing information base; RIB)로도 지칭됨)에 주입하며, 이는 터널 샤드들에 의해 수신된다. 터널 샤드들은 적절한 루트 필터링 정책들을 적용한 이후에 라우팅 정보를 그들의 로컬 루트 테이블들(228 및 236)로 임포트(import)한다. 루트 필터링은, 손상된 에이전트(112)가 임의의 루트들을 터널 샤드들에 주입하지 않는 것을 보장하기 위해 선호된다. 특정 예들에서, 에이전트(112)는 추가적으로 라우팅 관리자(214)를 포함한다. 라우팅 관리자(214)는 라우팅 스위트(예를 들어, Quagga)의 부분인 오픈 소스 라우팅 관리자(예를 들어, Zebra)를 사용하여 구현될 수 있다. BGP 피어링 세션들이 루트들을 학습하고 이들을 그 루트 테이블(212)로 임포트할 때, BGP 피어링 세션들은 최상 경로 계산을 수행하고 최상 루트들을 로컬 커널에 추가하기 위해 라우팅 관리자(214)를 사용한다.

[0039] 터널 샤드(예를 들어, 120, 126)는 하나 이상의 컨테이너들의 세트로 구성될 수 있다. 특정 구현예들에서, 터널 샤드(120 또는 126)는, 터널 샤드가 에이전트(112) 및 테넌트-특정 오버레이 네트워크(128)의 부분인 다른 샤드들(예를 들어, 자원 샤드들(136 및 140)) 둘 모두와 통신하는 것을 가능하게 하는 다양한 네트워크 인터페이스들을 셋업하기 위해 사용될 수 있는 쉘 컨테이너(shell container)를 포함할 수 있다. 도 2에 도시된 실시예에서, 터널 샤드 내의 쉘 컨테이너 내에 구현된 네트워크 인터페이스들은 외부 사이트 인터페이스(external site interface; esi), 터널 인터페이스 및 샤드 백엔드(backend) 인터페이스를 포함할 수 있다. 예를 들어, 터널 샤드-1(120) 내에 구현된 네트워크 인터페이스들은 터널 인터페이스(216), 외부 사이트 인터페이스(222) 및 샤드 백엔드 인터페이스(234)를 포함한다. 유사하게, 터널 샤드-2(126) 내에 구현된 네트워크 인터페이스들은 터널 인터페이스(218), 외부 사이트 인터페이스(223) 및 샤드 백엔드 인터페이스(235)를 포함한다. 터널 샤드(예를 들어, 120 또는 126)는 추가적으로, 외부 게이트웨이 어플라이언스(112)에서 실행되는 VPN 클라이언트(206, 208)에 대한 VPN 터널을 설정하기 위해 사용되는 VPN 서버(224, 226)로 구성된다. 외부 사이트 인터페이스(222, 223)는, VPN 클라이언트가 실행되며 터널 샤드에 대한 터널을 설정하기 위해 사용되는 에이전트(112)에게 알려진 공인 IP에 의해 식별된다. VPN 클라이언트(예를 들어, 206, 208)가 VPN 서버(224, 226)에 연결될 때, 터널

인터페이스(216, 218)가 생성되며 터널 샤드의 사전-구성된 VPN 서브넷에 위치된다.

[0040] 특정 구현예들에서, 각각의 터널 샤드(예를 들어, 120, 126)는, 외부 게이트웨이 어플라이언스와 터널 샤드들 사이에 BGP 피어링 세션들을 설정하고 터널 샤드들과 자원 샤드들 사이에 BGP 피어링 세션을 설정하기 위해 보더 게이트웨이 프로토콜(BGP)를 사용할 수 있다. BGP 피어링 세션들은, 샤드 백엔드 인터페이스들(234, 235)을 통해 자원 샤드들과 라우팅 및 도달가능성 정보를 교환하고 외부 사이트 인터페이스들(222, 223)을 통해 외부 사이트 표현(106)과 라우팅 및 도달가능성 정보를 교환하기 위해 사용된다. BGP 피어링 세션들에 대해 필요한 구성 정보의 부분으로서, 테넌트-특정 오버레이 네트워크(128)를 식별하는 IP 어드레스는 각각 터널 샤드들(120, 126)에 구현된 루트 테이블들(228, 236)(즉, 라우팅 정보 베이스(routing information base; RIB)들)에 추가된다. 특정 구현예에서, 클래스리스 인터-도메인 라우팅(Classless Inter-Domain Routing; CIDR) 기술이 IP 어드레스를 테넌트-특정 오버레이 네트워크에 할당하기 위해 사용될 수 있다. 루트 테이블들(228, 236)은 자원 샤드들(136, 140) 및 외부 사이트 표현(106)와 같은 특정 네트워크 목적지들에 대한 루트들을 리스팅한다. 일부 경우들에서, 루트 테이블들(228, 236)은 또한 이러한 루트들과 연관된 (거리들)을 리스팅한다. 자원 샤드들과의 BGP 피어링 세션들이 설정될 때, 루트 테이블 내의 루트는 자원 샤드들로 전파된다. 도 2에 도시된 바와 같이, 각각의 터널 샤드(120, 126)는 추가적으로 라우팅 관리자(228, 240)를 포함한다. 라우팅 관리자(228 또는 240)는 외부 게이트웨이 어플라이언스(112)에 구현되는 라우팅 관리자(214)와 유사한 방식으로 구현될 수 있다. BGP가 루트들을 학습하고 이들을 터널 샤드들 내의 루트 테이블들로 임포트할 때, 이는 최상 경로 계산을 수행하며, 외부 사이트 표현(106) 및 자원 샤드들(136, 140)로 최상 루트들을 푸시하기 위해 라우팅 관리자를 사용한다.

[0041] 자원 샤드(136, 140)는 컨테이너들의 세트로 구성될 수 있다. 특정 구현예들에서, 자원 샤드(136, 140)는, 터널 샤드들(116, 126)과 가상 터널 엔드포인트 VTEP(242, 243)를 셋업하기 위해 사용될 수 있는 쉘 컨테이너를 포함할 수 있다. 각각의 자원 샤드(136, 140)는, 터널 샤드들과 피어링 세션들을 설정하고 가상 터널 엔드포인트들(242, 243)을 통해 터널 샤드들과 라우팅 및 도달가능성 정보를 교환하기 위해 BGP를 사용할 수 있다. 자원 샤드(136, 140)는 추가적으로, 터널 샤드들에 구현된 라우팅 관리자(232 또는 240)와 동일한 기능성을 수행하도록 구성된 라우팅 관리자(250, 260)를 포함한다. 각각의 자원 샤드(136, 140)는 추가적으로 프록시 서버(244, 254)를 포함한다. 프록시 서버(244 또는 254)는, 고객의 VCN(148) 내의 클라이언트 애플리케이션(144)로부터의 연결들을 수락하고 외부 사이트 표현 내의 외부 자원에 대한 새로운 연결들을 개시하도록 구성될 수 있다.

[0042] 특정 구현예들에서, 모든 등록된 엔드포인트(즉, 외부 사이트 표현 내의 외부 자원에 대응함)에 대해, 고유 프록시 서버 컨테이너가 런칭되고 자원 샤드에 접속된다. 외부 자원을 등록하고 고객의 VCN 내의 등록된 외부 엔드포인트에 대한 원격 마운트 포인트 VNIC를 생성할 때, 사용자는 외부 자원의 IP 어드레스, 외부 자원의 포트 번호, 및 외부 자원의 명칭과 같은 구성 정보를 SNCS(104)에 제공할 수 있다. 이러한 구성 정보는 프록시 서버들에서 프로비저닝되고, 외부 자원에 연결하기 위해 고객의 VCN 내의 클라이언트 애플리케이션에 의해 사용된다. 외부 자원이 SNCS에 의해 고객의 VCN 내의 외부 엔드포인트로서 성공적으로 등록될 때, SNCS(104)는 (제어 평면 API들을 통해) VNIC를 생성하고 외부 엔드포인트와 연관된 IP 어드레스를 VNIC에 할당한다.

[0043] 도 2에 도시된 예에서, 등록된 외부 엔드포인트(즉, 외부 자원 표현 내의 외부 자원)는 외부 사이트 표현(106)에 상주하는 데이터베이스(202)를 나타낸다. 프록시 서버들(244, 254)은, 등록된 외부 엔드포인트(202)에 대해 생성된 VNIC(206)에 할당된 가상 IP 어드레스 상에서 리스닝(listen)한다. 이는, 동일한 VNIC IP가 외부 사이트 표현 내의 다른 등록된 외부 자원들에 액세스하기 위해 사용될 수 없다는 것을 보장한다. 고객의 VCN에서 실행중인 클라이언트 애플리케이션(144)이 외부 데이터베이스(202)에 저장된 정보를 획득하기 위한 쿼리를 수신할 때, 이는 네트워크 패킷들을 고객들의 VCN 내의 VNIC IP로 송신한다. 네트워크 패킷들은, 자원 샤드들(136, 140)에 접속된 작업자(worker) VNIC들(251, 252)에 의해 수신된다. 작업자 VNIC들은 VNIC의 가상 IP 어드레스로 구성되며, 차례로, 프록시 서버들(244, 254)을 통해 외부 사이트 표현 내의 등록된 외부 자원에 대한 연결을 개시한다. 프록시 서버들(244, 254)은, VNIC(206)에 할당된 가상 IP 어드레스를 외부 사이트 표현(106) 내의 외부 자원(114A)의 실제/물리적 IP 어드레스로 변환하기 위해 네트워크 어드레스 변환(network address translation; NAT)을 수행한다. 프록시 서버들(244, 254)을 사용하는 자원 샤드들(136, 140)은 터널 샤드들(120, 126)을 통해 에이전트(112)에 대한 연결을 개시한다. 에이전트(112)는 터널 샤드들(120, 126)로부터 네트워크 패킷들을 수신하며, 차례로, 패킷들을 외부 사이트 표현(106) 내의 등록된 외부 자원(즉, 데이터베이스(202))으로 라우팅한다. 프록시 서버들(244, 254)은 추가적으로 터널 샤드들을 통한 외부 자원으로의 네트워크 트래픽을 로드-밸런싱(load-balance)하기 위한 능력들을 포함한다. 특정 실시예들에서, 프록시 서버들(244, 254)은, 다수의 클라이언트 애플리케이션들로부터 외부 사이트 표현을 향한 단일 연결 상으로의 연결들을 멀티

플렉싱하도록 구성될 수 있다.

[0044] 유사한 방식으로, 외부 사이트 표현(106)에 상주하는 등록된 외부 자원(즉, 데이터베이스(202))은 고객의 VCN에 상주하는 자원(예를 들어, 컴퓨팅 인스턴스(150)) 또는 서비스(예를 들어, 사설 엔드포인트 VNIC(152))에 접근하고 이에 안전하게 액세스할 수 있다. 도 1에서 이상에서 설명된 바와 같이, 에이전트(112)는 외부 자원(202)에 대한 논리적 인터페이스(204)를 생성/프로비저닝한다. 외부 자원(114A)에 대한 논리적 인터페이스(158)를 생성하고 데이터베이스(202)의 VNIC 표현(206)의 가상 IP 어드레스를 논리적 인터페이스에 할당함으로써, 데이터베이스(202)(고객의 사내 네트워크에 상주함)는, SNCS(104)에 의해 제공된 보안 사설 네트워크 연결성 서비스들을 사용하여 고객의 VCN(148) 내의 사설 엔드포인트 VNIC(142)를 통해 고객의 VCN(148) 내의 컴퓨팅 인스턴스(150) 또는 서비스(156)(예를 들어, CSPI 내의 스트리밍 서비스 또는 객체 스토리지 서비스)에 안전하게 액세스할 수 있다. 예를 들어, 도 2에 도시된 실시예에서, 에이전트(112)는 고객의 VCN 내의 자원(예를 들어, 150)과 연관된 정보를 요청하는 쿼리를 데이터베이스(202)로부터 수신할 수 있다. 그런 다음, 에이전트(112)는 쿼리에 대응하는 네트워크 패킷들을 터널 샤드들(120, 126)로 송신한다. 터널 샤드들은, 결과적으로, 자원 샤드들(136, 140)에 대한 연결을 개시한다. 자원 샤드들(136, 140) 내의 프록시 서버들(244, 254)은, 외부 사이트 표현(106) 내의 외부 자원의 실제 IP 어드레스를 고객의 VCN 내의 외부 자원(예를 들어, 데이터베이스(202))의 VNIC 표현(206)의 가상 IP 어드레스로 변환하기 위해 네트워크 어드레스 변환(network address translation; NAT)을 수행한다. 자원 샤드들(136, 140)에 접속된 작업자 VNIC들(251, 252)은 결과적으로, 쿼리에 대응하는 네트워크 패킷들을 고객의 VCN 내의 요청 자원(예를 들어, 150)으로 송신하는 고객의 VCN 내의 데이터베이스(202)의 VNIC 표현(206)에 대한 연결을 개시한다. 이러한 방식으로, SNCS(104)는, 보안 사설 양방향 네트워크 연결성이 고객의 사내 네트워크에 상주하는 외부 자원(예를 들어, 데이터베이스(202))와 고객의 VCN(즉, 클라우드) 내의 자원들(예를 들어, 150) 및 서비스들(예를 들어, 152) 사이에 설정되는 것을 보장한다.

[0045] 특정 구현예들에서, 고객의 VCN(148)로부터의 사설 연결성을 필요로 하는 등록된 외부 엔드포인트는 서비스 VNIC로서 구현될 수 있으며, 이는 본 명세서에서 고객의 VCN(148) 내의 "SVNIC"로도 지칭된다. SVNIC는, 가상 클라우드 네트워크들 사이에 트래픽을 프로세싱하고 송신하기 위해 다수의 VNIC들(예를 들어, 서비스 VNIC(254))을 호스팅할 수 있는 CSPI(102)에 의해 구현되는 수평으로 스케일링가능한 서비스를 나타낼 수 있는 서비스형 VNIC(VNIC as a service; VNICaaS) 시스템(도 2에 미도시)을 사용하여 CSPI(102)에 의해 구현될 수 있다. 구체적으로, VNICaaS는, VNIC가 서비스(즉, SVNIC)로서 표현되거나 또는 사용되는 것을 가능하게 하는 가상 네트워킹 특징이다. VNICaaS는, VNIC를 호스팅하기 위한 가상 네트워크 내의 컴퓨팅 인스턴스의 호스트 또는 특정 SmartNIC를 필요로 하지 않고 VNIC의 기능성을 제공한다. 등록된 엔드포인트들을 SVNIC들로서 표현하기 위해 사용되는 기술들은 "Techniques for high performant virtual routing capabilities"이라는 명칭의 미국 특허 출원 제17/175,573호에서 상세하게 설명되었다. 미국 특허 출원 제17/175,573호에서 설명된 기술들은 단지 예들일 뿐이며, 제한적으로 의도되지 않는다. 다양한 다른 기술들이 또한 대안적인 실시예들에서 등록된 엔드포인트들을 표현하기 위해 그리고 가상 클라우드 네트워크들 사이에서 트래픽을 프로세싱하고 송신하기 위해 사용될 수 있다. SVNIC가 모든 등록된 외부 엔드포인트(예를 들어, 데이터베이스(202))에 대해 생성되기 때문에, 유연한 수의 작업자들이 SVNIC별로 구성될 수 있다. 특정 구현예에서, 매 SVNIC는, 상이한 자원 샤드들(예를 들어, 136, 140)에 접속된 2개의 작업자 VNIC들(예를 들어, 251, 252)과 연관된다. 작업자 VNIC들은 자원 샤드들로 전달되며, SVNIC IP로 구성된다.

[0046] 도 2에 도시된 특정 구현예에서, 단일 에이전트(112)가 외부 사이트 표현(106)에 설치되며, SNCS(104)에 의해 구현되는 터널 플리트 상에 위치되어야 하는 총 2개의 터널 샤드들을 야기하는 2개의 터널들을 설정하도록 구성된다. 이러한 구현예에서 설명되는 고정된 수의 터널 샤드들에 대해, 모든 자원 샤드는 이러한 피어들에 대해 정적 어드레스 레졸루션 프로토콜(Address Resolution Protocol; ARP) 엔트리들에 따라 BGP 피어들의 고정된 세트로 사전-구성될 수 있다. 특정 접근방식들에서, 터널 샤드 상의 BGP 컨테이너는, BGP가 이로부터의 인커밍 연결들을 수락할 수 있는 IP 어드레스의 CIDR 블록이 지정될 수 있는 "동적 BGP 피어"로서 구성될 수 있다. 이러한 CIDR 블록은 테넌트-특정 오버레이 네트워크의 CIDR로 설정될 수 있으며, 따라서 터널 샤드 상의 자원 샤드들이 증가/축소함에 따라 터널 샤드 상의 BGP 피어들이 또한 적절하게 변경된다. 자원 샤드들의 관점으로부터, 모든 자원 샤드는 이제 2개의 BGP 피어링 연결들을 가지며, BGP 피어들 각각이 외부 사이트 표현으로부터 학습한 동일한 CIDR 루트를 사내 네트워크로 전파하기 때문에, 모든 자원 샤드는 사내 네트워크를 향한 2개의 동일-비용 경로들을 갖는다. 유사하게 외부 게이트웨이의 관점으로부터, 에이전트(112)는 SNCS(104)를 향한 2개의 터널들을 설정하고, 터널 샤드들은 테넌트-특정 오버레이 네트워크 루트들을 에이전트(112)로 광고하며, 이는 그런 다음 테넌트-특정 오버레이 네트워크에 대한 적절한 루트를 설치한다.

[0047] SNCS(104)에 의해 구현되는 개시된 새롭고 개선된 아키텍처를 사용하면, 고객의 외부 사이트 표현 내의 외부 자원들과 클라우드 내의 고객의 VCN에 상주하는 자원들 및 서비스들 사이의 보안 사설 양방향 네트워크 연결성은, 기업의 사용자(예를 들어, 관리자)가 외부 자원을 명시적으로 구성하거나, 루트들을 광고하거나 또는 사이트-대-사이트 연결성을 셋업할 필요 없이 달성될 수 있다. 설명된 바와 같이, 보안 사설 네트워크 연결성은, 고객의 외부 사이트 표현과 고객의 VCN 사이에 암호화된 연결을 사용하는 SNCS에 의해 그리고 고객에 대한 테넌트-특정 오버레이 네트워크를 셋업하기 이전에 에이전트를 인증함으로써 설정된다. SNCS(104)는, SNCS(104)에 의해 제공되는 서비스들을 사용하는 각각의 테넌트/고객에 대해 네트워크 요소들 및 컴퓨팅 노드들의 강건한 인프라스트럭처(즉, 테넌트-특정 오버레이 네트워크(128))를 구현함으로써 고객의 사내 환경과 CSPI 사이의 네트워크 트래픽을 프로세싱하기 위한 고 성능, 스케일러블, 및 고도로 이용가능한 사이트-대-사이트 네트워크 연결을 제공한다. 테넌트-특정 오버레이 네트워크(128) 내의 터널 호스트들은 고객의 외부 사이트 표현(106)에 대한 보안 연결성을 제공하기 위해 사용되며, 자원 호스트들은 고객의 VCN으로부터 트래픽을 수신하고 이를 고객의 외부 사이트 표현으로 포워딩하기 위해 사용된다. 자원 호스트들은 추가적으로 외부 사이트 표현 내의 외부 자원으로부터 트래픽을 수신하고 이를 고객의 VCN에 상주하는 자원들 또는 서비스들로 포워딩할 수 있다. 테넌트-특정 오버레이 네트워크에 의해 구현되는 네트워크 요소들 및 컴퓨팅 노드들의 강건한 인프라스트럭처를 사용함으로써, 기업은, 그 외부 자원들이 마치 그들의 VCN 내의 임의의 다른 네이티브 자원들에 연결된 것처럼 클라우드로부터 그 외부 자원들에 안전하게 액세스할 수 있다. 기업의 사용자는, 사이트-대-사이트 연결에 의해 사용될 루트들을 구성하지 않고 그리고 그들의 외부 자원들에 대해 임의의 변경을 수행하지 않고, 그들의 사내 네트워크와 클라우드 사이에 정교한 사이트-대-사이트 네트워크를 설정하지 않고 기업의 외부 자원들에 액세스할 수 있다. 유사하게, 외부 자원에 대한 논리적 인터페이스를 생성하고 논리적 인터페이스를 외부 자원의 VNIC 표현의 가상 IP 어드레스와 연관시킴으로써, 외부 자원(고객의 사내 네트워크에 상주함)은 SNCS(104)에 의해 제공된 보안 사설 네트워크 연결성 서비스들을 사용하여 클라우드 내에 있는(예를 들어, 고객의 VCN(148) 내에 있는) 자원들 및 서비스들에 안전하게 액세스할 수 있다.

[0048] 도 3은 특정 실시예들에 따른, 보안 사설 네트워크 연결성을 제공하기 위한 도 1에 도시된 시스템들 및 서브시스템들에 의해 수행되는 프로세스의 일 예를 도시한다. 도 3에 도시된 프로세싱은 개별적인 시스템들, 하드웨어, 또는 이들의 조합의 하나 이상의 프로세싱 유닛들(예를 들어, 프로세서들, 코어들)에 의해 실행되는 소프트웨어(예를 들어, 코드, 명령어들, 프로그램)로 구현될 수 있다. 소프트웨어는 비-일시적 저장 매체 상에(예를 들어, 메모리 디바이스 상에) 저장될 수 있다. 도 3에 표현되고 이하에서 설명되는 프로세스(300)는 예시적으로 그리고 비-제한적으로 의도된다. 도 3이 특정 시퀀스 또는 순서로 발생하는 다양한 프로세싱 단계들을 도시하지만, 이는 제한적으로 의도되지 않는다. 특정한 대안적인 실시예들에서, 단계들은 어떤 상이한 순서로 수행될 수 있으며, 일부 단계들이 또한 병렬로 수행될 수 있다. 도 1에 도시된 실시예와 같은 특정 실시예들에서, 도 3에 도시된 프로세싱은 테넌트-특정 오버레이 네트워크(128)를 포함하는 컴퓨팅 노드들(예를 들어, 116, 122, 130 및 132)에 의해 수행될 수 있다.

[0049] 도 3에 도시된 프로세싱은, 고객과 연관된 사용자(예를 들어, 관리자)가 고객의 사내 네트워크의 외부 사이트 표현(예를 들어, 106)을 생성하였고 외부 사이트 표현(106)에 에이전트(112)를 구성했다고 가정한다. 도 4에 도시된 프로세싱은, SNCS(104)가 에이전트(112)를 인증하였으며 고객에 대한 컴퓨팅 노드들의 분산되고 수평으로 스케일링가능한 플리트를 포함하는 테넌트-특정 오버레이 네트워크(예를 들어, 128)를 구성/설정하였다고 추가로 가정한다. 도 1에서 설명된 바와 같이, 하나 이상의 컴퓨팅 노드들의 세트는 자원 호스트들(즉, 자원 가상 머신들(130, 132)) 및 터널 호스트들(즉, 터널 가상 머신들(116, 122))을 포함한다.

[0050] 도 3에 도시된 프로세싱은, SNCS(104)가 컴퓨팅 노드들의 분산되고 수평으로 스케일링가능한 플리트를 포함하는 테넌트-특정 오버레이 네트워크(예를 들어, 128)를 실행할 때 블록(302)에서 개시될 수 있다. 테넌트-특정 오버레이 네트워크는 CSPI 내에서 고객의 VCN(예를 들어, 148)과 고객의 외부 사이트 표현 사이에 보안 사설 네트워크 연결성을 설정하기 위해 사용된다.

[0051] 블록(304)에서, SNCS는 (제어 평면 API들을 통해) 고객 사내 네트워크에 상주하는 외부 자원을 고객의 VCN 내에 외부 엔드포인트로서 등록한다. 외부 엔드포인트는 고객의 VCN 내의 IP 어드레스에 의해 식별된다. 이상에서 설명된 바와 같이, 외부 자원은, 고객이 그들의 VCN 내로부터의 보안 양방향 사설 네트워크 연결성을 가능하게 하는 것을 의도하는 외부 사이트 표현(106) 내의 데이터베이스, 컴퓨팅 인스턴스, 또는 애플리케이션을 나타낼 수 있다. 외부 자원을 등록하는 것을 부분으로서, SNCS의 사용자는, 콘솔 UI 또는 API들을 통해 외부 자원과 연관된 사내 물리적 IP 어드레스, 외부 자원들이 액세스가능한 포트 번호 및 외부 자원의 호스트명칭(또는 전체 주소 도메인 명칭(FQDN))과 같은 외부 자원과 관련된 구성 정보를 제공한다. 사용자는 또한, 외부 자원에 대한 외

부 엔드포인트가 생성될 고객의 VCN 내의 서브넷(subnet)을 선택한다. 구성 정보에 기초하여, SCNS는 고객의 VCN 내에 외부 자원에 대한 외부 엔드포인트를 생성한다. 외부 엔드포인트는 IP 어드레스, 포트 번호 및 고객의 VCN에서의 FQDN(호스트명칭)에 의해 식별된다.

[0052] 블록(306)에서, SNCS 내의 제1 컴퓨팅 노드(예를 들어, 자원 VM(130) 또는 자원 VM(132))는 고객의 VCN 내에 외부 엔드포인트에 대한 외부 자원 표현을 생성한다. 특정 구현예에서, 외부 자원 표현의 생성은, 제1 컴퓨팅 노드에 의해, VNIC를 생성하는 단계 및 외부 엔드포인트의 IP 어드레스를 VNIC에 할당하는 단계를 수반한다.

[0053] 블록(308)에서, 제1 컴퓨팅 노드는 고객의 VCN 내의 외부 자원 표현에 대해 생성된 VNIC에 대응하는 구성 정보를 사내 네트워크에 구성된 에이전트(112)로 송신한다. 블록(308)에서 수행되는 프로세싱의 부분으로서, 에이전트(112)는 구성 정보를 다운로드하고 이를 사내 네트워크에 상주하는 등록된 외부 자원 상으로 카피한다. 이상에서 설명된 바와 같이, 구성 정보는, 예를 들어, VNIC의 가상 IP 어드레스, VNIC과 연관된 컴퓨팅 인스턴스와 연관된 전체 주소 도메인 명칭 및 고객과 연관된 가상 클라우드 네트워크의 클라우드 식별자를 포함할 수 있다. 구성 정보를 사용하여, 에이전트(112)는 외부 자원(예를 들어, 114A)에 대한 논리적 인터페이스(예를 들어, 158)를 생성/프로비저닝한다. 특정 구현예에서, 에이전트(112)에 의한 논리적 인터페이스의 생성 또는 프로비저닝은, 에이전트에 의해, 외부 자원 표현에 대해 생성된 VNIC(142)에 할당된 가상 IP 어드레스를 외부 자원(114)에 대해 프로비저닝된 논리적 인터페이스(158)에 할당하는 것을 포함한다.

[0054] 블록(310)에서, 제2 컴퓨팅 노드(예를 들어, 터널 VM(116) 또는 터널 VM(122))는 고객의 VCN에 상주하는 자원(예를 들어, 컴퓨팅 인스턴스(150))과 연관된 정보를 쿼리하기 위한 요청을 수신한다. 특정 예들에서, 요청은 사내 네트워크에 상주하는 외부 자원(예를 들어, 114A)에 의해, 그 논리적 인터페이스(158)를 통해, 송신될 수 있다. 예를 들어, 고객과 연관된 사용자는 (예를 들어, UI(108)를 통해) 고객의 VCN에 상주하는 컴퓨팅 인스턴스(150)와 연관된 정보를 쿼리하기 위한 요청을 고객의 사내 네트워크에 상주하는 외부 자원으로 송신할 수 있다. 외부 자원은, 결과적으로, 쿼리를 사내 네트워크에 상주하는 에이전트(112)로 송신할 수 있다. 에이전트(112)는 쿼리 요청을 수신하고, 쿼리 요청에 대응하는 네트워크 패킷들을 터널 VM들에서 실행 중인 터널 샤드들(120 또는 126)로 송신한다.

[0055] 블록(312)에서, 제2 컴퓨팅 노드(예를 들어, 터널 VM(116) 또는 터널 VM(122))는 자원 샤드(예를 들어, 136 또는 140)를 통해 외부 자원에 대해 프로비저닝된 논리적 인터페이스와 고객의 VCN 내의 외부 자원 표현에 대해 생성된 VNIC 사이에 연결을 설정한다. 특정 구현예에서, 터널 샤드들(예를 들어, 120 또는 126)은, 외부 자원에 할당된 실제/물리적 IP 어드레스를 VNIC(142)의 가상 IP 어드레스로 변환하고 자원 샤드들(136 또는 140)을 통해 VNIC(142)에 대한 연결을 개시하기 위한 능력들을 포함할 수 있다. 자원 샤드들은, 결과적으로, 고객의 VCN 내의 자원(예를 들어, 150)에 대한 연결을 개시한다.

[0056] 블록(314)에서, 제2 컴퓨팅 노드(예를 들어, 터널 VM(116) 또는 터널 VM(122))는 블록(410)에서 설정된 연결을 통해 고객의 VCN에 상주하는 자원으로 요청을 송신한다. 블록(412)에서, 제2 컴퓨팅 노드는 설정된 연결을 통해 요청에 대응하는 결과를 획득한다. 그런 다음, 결과는 에이전트(112)를 통해 외부 사이트 표현에 상주하는 외부 자원으로 송신된다. 예를 들어, 자원이 고객의 VCN 내에서 실행 중인 데이터베이스인 경우, 결과는 데이터베이스 내의 하나 이상의 테이블들에 저장된 정보를 포함할 수 있다.

[0057] 도 4는 특정 실시예들에 따른, 고객의 사내 네트워크에 상주하는 외부 자원과 고객의 가상 클라우드 네트워크 내의 외부 자원의 표현 사이의 네트워크 패킷들의 흐름을 도시하는 흐름도이다. 도 4에 도시된 프로세싱은 개별적인 시스템들, 하드웨어, 또는 이들의 조합의 하나 이상의 프로세싱 유닛들(예를 들어, 프로세서들, 코어들)에 의해 실행되는 소프트웨어(예를 들어, 코드, 명령어들, 프로그램)로 구현될 수 있다. 소프트웨어는 비-일시적 저장 매체 상에(예를 들어, 메모리 디바이스 상에) 저장될 수 있다. 도 4에 표현되고 이하에서 설명되는 프로세스(400)는 예시적으로 그리고 비-제한적으로 의도된다. 도 4가 특성 시퀀스 또는 순서로 발생하는 다양한 프로세싱 단계들을 도시하지만, 이는 제한적으로 의도되지 않는다. 특정한 대안적인 실시예들에서, 단계들은 어떤 상이한 순서로 수행될 수 있으며, 일부 단계들이 또한 병렬로 수행될 수 있다. 도 2에 도시된 실시예와 같은 특정 실시예들에서, 도 4에 도시된 프로세싱은 테넌트-특정 오버레이 네트워크(128)를 포함하는 컴퓨팅 노드들(예를 들어, 116, 122, 130 및 132)에 의해 수행될 수 있다.

[0058] 도 4에 도시된 프로세싱은, 고객의 사내 네트워크(즉, 고객의 외부 사이트 표현(106))에 상주하는 외부 자원(예를 들어, 데이터베이스(202))가 고객의 VCN(예를 들어, 148)에 상주하는 자원(예를 들어, 150)과 연관된 정보에 대한 쿼리를 수신할 때 블록(402)에서 개시될 수 있다. 이상에서 설명된 바와 같이, 고객과 연관된 사용자는 (예를 들어, UI(108)를 통해) 고객의 VCN에 상주하는 컴퓨팅 인스턴스(150)와 연관된 정보를 쿼리하기 위한 요

청을 고객의 사내 네트워크에 상주하는 외부 자원으로 송신할 수 있다. 외부 자원은, 결과적으로, 쿼리를 사내 네트워크에 상주하는 에이전트(112)로 송신할 수 있다.

[0059] 블록(404)에서, 에이전트(112)는 쿼리를 수신하고, 쿼리에 대응하는 네트워크 패킷들을 터널 VM들에서 실행 중인 터널 샤드들(120 또는 126)로 송신한다. 특정 예들에서, 블록(404)에서 수행되는 프로세싱의 부분으로서, 에이전트(112)는, 네트워크 패킷을 터널 샤드들로 송신하기 이전에 네트워크 패킷들을 암호화할 수 있다.

[0060] 블록(406)에서, 터널 샤드들은 암호화된 네트워크 패킷들을 수신하고, 암호화된 네트워크 패킷들을 자원 VM들에서 실행 중인 자원 샤드들(136, 140)로 송신한다. 구체적으로, 그리고 도 2에 도시된 바와 같이, 암호화된 네트워크 패킷들은, 자원 샤드들(136, 140)에 접속된 작업자 VNIC들(251, 252)에 의해 수신될 수 있다.

[0061] 블록(408)에서, 자원 샤드들(136, 140)은 네트워크 패킷들을 복호화하고, 외부 자원에 할당된 물리적 IP 어드레스를 고객의 VCN 내의 외부 자원 표현과 연관된 VNIC(예를 들어, 206)의 가상 IP 어드레스로 변환하기 위해 네트워크 어드레스 변환(network address translation; NAT)을 수행한다.

[0062] 블록(410)에서, 자원 샤드들(136, 140)은 네트워크 패킷들을 고객의 VCN 내의 외부 자원 표현에 대해 생성된 VNIC로 송신한다.

[0063] 블록(412)에서, VNIC는 쿼리에 대응하는 네트워크 패킷들을 고객의 VCN에 상주하는 자원(예를 들어, 150)으로 송신한다.

[0064] 도 5는 특정 실시예들에 따른, 고객의 가상 클라우드 네트워크 내의 외부 자원 표현과 고객의 사내 네트워크에 상주하는 외부 자원 사이의 네트워크 패킷들의 흐름을 도시하는 흐름도이다. 도 5에 도시된 프로세싱은 개별적인 시스템들, 하드웨어, 또는 이들의 조합의 하나 이상의 프로세싱 유닛들(예를 들어, 프로세서들, 코어들)에 의해 실행되는 소프트웨어(예를 들어, 코드, 명령어들, 프로그램)로 구현될 수 있다. 소프트웨어는 비-일시적 저장 매체 상에(예를 들어, 메모리 디바이스 상에) 저장될 수 있다. 도 5에 표현되고 이하에서 설명되는 프로세스(500)는 예시적으로 그리고 비-제한적으로 의도된다. 도 5가 특성 시퀀스 또는 순서로 발생하는 다양한 프로세싱 단계들을 도시하지만, 이는 제한적으로 의도되지 않는다. 특정한 대안적인 실시예들에서, 단계들은 어떤 상이한 순서로 수행될 수 있으며, 일부 단계들이 또한 병렬로 수행될 수 있다. 도 2에 도시된 실시예와 같은 특정 실시예들에서, 도 5에 도시된 프로세싱은 테넌트-특정 오버레이 네트워크(128)를 포함하는 컴퓨팅 노드들(예를 들어, 116, 122, 130 및 132)에 의해 수행될 수 있다.

[0065] 도 5에 도시된 프로세싱은, 고객의 VCN 내의 클라이언트 애플리케이션(예를 들어, 144)이 고객의 사내 네트워크(즉, 고객의 외부 사이트 표현(106))에 상주하는 외부 자원(예를 들어, 202)과 연관된 정보에 대한 쿼리를 수신할 때 블록(502)에서 개시될 수 있다. 예를 들어, 쿼리는 클라이언트 애플리케이션을 통해 고객과 연관된 사용자로부터 수신될 수 있다. 블록(502)에서 수행되는 프로세싱의 부분으로서, 클라이언트 애플리케이션(144)은, 쿼리에 대응하는 네트워크 패킷들을 고객의 VCN 내의 VNIC에 할당된 가상 IP 어드레스로 송신함으로써 외부 자원 표현과 연관된 VNIC(예를 들어, 206)에 대한 연결을 개시한다.

[0066] 블록(504)에서, 클라이언트 애플리케이션은 쿼리에 대응하는 네트워크 패킷들을 SNCS 내의 자원 VM들에서 실행 중인 자원 샤드들(136 또는 140)로 송신한다. 구체적으로, 그리고 도 2에 도시된 바와 같이, 네트워크 패킷들은, 자원 샤드들(136, 140)에 접속된 작업자 VNIC들(251, 252)에 의해 수신될 수 있다. 자원 샤드들(136, 140) 내의 프록시 서버들(244, 254)은, VNIC에 할당된 가상 IP 어드레스를 외부 사이트 표현(106)에 설치된 외부 자원의 물리적 IP 어드레스로 변환하기 위해 네트워크 어드레스 변환(network address translation; NAT)을 수행하고 터널 샤드들(120, 126)을 통해 에이전트(112)에 대한 연결을 개시한다.

[0067] 블록(506)에서, 자원 샤드들은 네트워크 패킷들을 터널 샤드들(120, 126)로 송신한다. 블록(506)에서 수행되는 프로세싱의 부분으로서, 터널 샤드들은, 패킷들을 외부 사이트 표현(106) 내의 에이전트(112)로 송신하기 이전에 자원 샤드들로부터 수신된 네트워크 패킷들을 암호화할 수 있다.

[0068] 블록(508)에서, 터널 샤드들은 고객의 외부 사이트 표현에 상주하는 에이전트(112)로 네트워크 패킷들을 송신한다. 블록(508)에서 수행되는 프로세싱의 부분으로서, 에이전트(112)는, 네트워크 패킷들을 외부 사이트 표현(예를 들어, 106) 내의 외부 자원(예를 들어, 202)으로 송신하기 이전에 네트워크 패킷들을 복호화한다.

[0069] 블록(510)에서, 에이전트(112)는 고객의 외부 사이트 표현에 상주하는 외부 자원(예를 들어, 202)으로 네트워크 패킷들을 송신한다. 외부 자원은 쿼리에 대응하는 네트워크 패킷들을 수신하고, 쿼리에 대응하는 응답 네트워크 패킷들을 생성한다. 그런 다음, 응답 네트워크 패킷들은 외부 자원에 의해 다시 클라이언트 애플리케이션으로

송신될 수 있다. 예를 들어, 응답 네트워크 패킷 흐름의 부분으로서, 쿼리에 대한 응답에 대응하는 네트워크 패킷들은 외부 자원으로부터 에이전트로 송신된다. 에이전트는 네트워크 패킷들을 암호화하고, 암호화된 네트워크 패킷들을 터널 샤드들로 송신한다. 터널 샤드들은 암호화된 패킷들을 수신하고, 패킷을 자원 샤드들로 송신한다. 자원 샤드들은 네트워크 패킷들을 복호화하고, 외부 자원에 할당된 물리적/실제 IP 어드레스를 고객의 VCN 내의 외부 자원 표현과 연관된 VNIC의 가상 IP 어드레스로 변환하기 위해 역 네트워크 어드레스 변환(network address translation; NAT)을 수행한다. 그런 다음, 자원 샤드들은 응답 네트워크 패킷들을 VNIC으로 송신하며, 이는 결과적으로 응답 패킷들을 고객의 VCN(148) 내의 요청 클라이언트 애플리케이션(144)으로 송신한다.

[0070] 예시적인 가상 네트워킹 아키텍처

[0071] 용어 클라우드 서비스는 일반적으로, CSP에 의해 제공되는 시스템들 및 인프라스트럭처(클라우드 인프라스트럭처)를 사용하여, 클라우드 서비스 제공자(cloud services provider; CSP)에 의해 (예를 들어, 가입 모델을 통해) 주문형으로 사용자들 또는 고객들에게 이용가능하게 되는 서비스를 지칭하기 위해 사용된다. 전형적으로, CSP의 인프라스트럭처를 구성하는 서버들 및 시스템들은 고객의 자체적인 사내 서버들 및 시스템들로부터 분리된다. 따라서, 고객들은, 서비스들에 대한 하드웨어 및 소프트웨어 자원들을 구매할 필요 없이 CSP에 의해 제공되는 클라우드 서비스들 자체를 이용할 수 있다. 클라우드 서비스들은, 고객이 서비스들을 제공하기 위해 사용되는 인프라스트럭처를 조달하는 데 투자할 필요 없이 가입 고객에게 애플리케이션들 및 컴퓨팅 자원들에 대한 쉽고 스케일링가능한 액세스를 제공하도록 설계된다.

[0072] 다양한 유형들의 클라우드 서비스들을 제공하는 몇몇 클라우드 서비스 제공자들이 있다. 서비스형 소프트웨어(Software as a Service; SaaS), 서비스형 플랫폼(Platform as a Service; PaaS), 서비스형 인프라스트럭처(Infrastructure as a Service; IaaS), 및 다른 것들을 포함하여 다양하고 상이한 유형들 또는 모델들의 클라우드 서비스들이 있다.

[0073] 고객은 CSP에 의해 제공되는 하나 이상의 클라우드 서비스들에 가입할 수 있다. 고객은 개인, 조직, 기업, 및 유사한 것과 같은 임의의 엔티티일 수 있다. 고객이 CSP에 의해 제공되는 서비스들에 가입하거나 또는 등록할 때, 테넌시 또는 계정이 해당 고객에 대해 생성된다. 그러면, 고객은, 이러한 계정을 통해, 계정과 연관된 가입된 하나 이상의 클라우드 자원들에 액세스할 수 있다.

[0074] 이상에서 언급된 바와 같이, 서비스형 인프라스트럭처(infrastructure as a service; IaaS)는 클라우드 컴퓨팅 서비스의 하나의 특정 유형이다. IaaS 모델에서, CSP는, 그들 자신의 맞춤화가능 네트워크들을 구축하고 고객 자원들을 배포하기 위해 고객들에 의해 사용될 수 있는 인프라스트럭처(클라우드 서비스 제공자 인프라스트럭처 또는 CSPI로 지칭됨)를 제공한다. 따라서 고객의 자원들 및 네트워크들은 CSP에 의해 제공된 인프라스트럭처에 의해 분산형 환경에서 호스팅된다. 이는, 고객의 자원들 및 네트워크들이 고객에 의해 제공된 인프라스트럭처에 의해 호스팅되는 전통적인 컴퓨팅과는 상이하다.

[0075] CSPI는, 서브스트레이트(substrate) 네트워크 또는 언더레이 네트워크로도 지칭되는 물리적 네트워크를 형성하는 다양한 호스트 머신들, 메모리 자원들 및 네트워크 자원들을 포함하여 상호연결된 고성능 컴퓨팅 자원들을 포함할 수 있다. CSPI 내의 자원들은, 하나 이상의 지리적 지역들에 걸쳐 분산될 수 있는 하나 이상의 데이터 센터들에 걸쳐 분산될 수 있다. 가상 소프트웨어는 가상화된 분산형 환경을 제공하기 위해 이러한 물리적 자원들에 의해 실행될 수 있다. 가상화는 물리적 네트워크 위에 오버레이 네트워크(소프트웨어-기반 네트워크, 소프트웨어-정의형 네트워크, 또는 가상 네트워크로 알려짐)를 생성한다. CSPI인 물리적 네트워크는, 물리적 네트워크의 상단 상에 하나 이상의 오버레이 또는 가상 네트워크들을 생성하기 위한 기본 기반을 제공한다. 물리적 네트워크(또는 서브스트레이트 네트워크 또는 언더레이 네트워크)는 물리적 스위치들, 라우터들, 컴퓨터들 및 호스트 머신들 및 유사한 것과 같은 물리적 네트워크 디바이스들을 포함한다. 오버레이 네트워크는, 물리적 서브스트레이트 네트워크의 상단 상에서 실행되는 논리적(또는 가상) 네트워크이다. 주어진 물리적 네트워크는 하나 또는 다수의 오버레이 네트워크들을 지원할 수 있다. 오버레이 네트워크들은 전형적으로 상이한 오버레이 네트워크들에 속하는 트래픽을 구별하기 위해 캡슐화 기술들을 사용한다. 가상 또는 오버레이 네트워크는 가상 클라우드 네트워크(virtual cloud network; VCN)로도 지칭된다. 가상 네트워크들은, 물리적 네트워크의 상단 상에서 실행될 수 있는 네트워크 추상화의 계층들을 생성하기 위해 소프트웨어 가상화 기술들(예를 들어, 하이퍼바이저(hypervisor)들, 네트워크 가상화 디바이스(network virtualization device; NVD)들(예를 들어, smartNIC들)에 의해 구현된 가상화 기능들, 탑-오브-랙(top-of-rack; TOR) 스위치들, NVD에 의해 수행되는 하나 이상의 기능들을 구현하는 스마트 TOR들, 및 다른 메커니즘들)을 사용하여 구현된다. 가상 네트워크들은, 피어-투-피어 네트

워크들, IP 네트워크들, 및 다른 것들을 포함하여 다수의 형태들을 취할 수 있다. 가상 네트워크들은 전형적으로 계층-3 IP 네트워크들 또는 계층-2 VLAN들이다. 가상 또는 오버레이 네트워킹의 이러한 방법은 흔히 가상 또는 오버레이 계층-3 네트워킹으로 지칭된다. 가상 네트워크들에 대해 개발된 프로토콜들의 예들은, IP-인-IP(IP-in-IP)(또는 일반 라우팅 캡슐화(Generic Routing Encapsulation; GRE), 가상 확장가능 LAN(VXLAN - IETF RFC 7348), 가상 사설 네트워크(Virtual Private Network; VPN)들(예를 들어, MPLS 계층-3 가상 사설 네트워크들(RFC 4364)), VMware의 NSX, GENEVE(Generic Network Virtualization Encapsulation), 및 다른 것들을 포함한다.

[0076] IaaS에 대해, CSP에 의해 제공된 인프라스트럭처(CSPI)는 공용 네트워크(예를 들어, 인터넷)를 통해 가상화된 컴퓨팅 자원들을 제공하도록 구성될 수 있다. IaaS 모델에서, 클라우드 컴퓨팅 서비스 제공자는 인프라스트럭처 구성요소들(예를 들어, 서버들, 저장 디바이스들, 네트워크 노드들(예를 들어, 하드웨어), 배포 소프트웨어, 플랫폼 가상화(예를 들어, 하이퍼바이저 계층), 또는 유사한 것)을 호스팅할 수 있다. 일부 경우들에서, IaaS 제공자는 또한 이러한 인프라스트럭처 구성요소들에 수반되는 다양한 서비스들(예를 들어, 청구, 모니터링, 로깅, 보안, 로드 밸런싱 및 클러스팅, 등)을 공급할 수 있다. 따라서, 이러한 서비스들이 정책-구동될 수 있기 때문에, IaaS 사용자들은 애플리케이션 가용성 및 성능을 유지하기 위한 로드 밸런싱을 구동하기 위한 정책들을 구현할 수 있다. CSPI는, 고객들이 고도로 이용가능한 호스팅되는 분산형 환경에서 광범위한 애플리케이션 및 서비스들을 구축하고 실행하는 것을 가능하게 하는 상보적인 클라우드 서비스들의 세트 및 인프라스트럭처를 제공한다. CSPI는, 고객의 사내 네트워크로부터와 같이 다양한 네트워킹된 위치들로부터 안전하게 액세스가능한 유연한 가상 네트워크에서 고성능 컴퓨팅 자원들과 능력들 및 스토리지 용량을 제공한다. 고객이 CSP에 의해 제공되는 IaaS 서비스들에 가입하거나 또는 등록할 때, 해당 고객에 대해 생성된 테넌시는, 고객이 그들의 클라우드 자원들을 생성하고, 조직하며, 관리할 수 있는 CSPI 내의 안전하고 격리된 파티션이다.

[0077] 고객들은 CSPI에 의해 제공되는 컴퓨팅, 메모리, 및 네트워킹 자원들을 사용하여 그들 자체의 가상 네트워크들을 구축할 수 있다. 컴퓨팅 인스턴스들과 같은 하나 이상의 고객 자원들 또는 워크로드들은 이러한 가상 네트워크들 상에 배포될 수 있다. 예를 들어, 고객은, 가상 클라우드 네트워크(virtual cloud network; VCN)들로 지칭되는 하나 또는 다수의 맞춤화가능 사설 가상 네트워크(들)를 구축하기 위해 CSPI에 의해 제공되는 자원들을 사용할 수 있다. 고객은 고객 VCN 상에 컴퓨팅 인스턴스들과 같은 하나 이상의 고객 자원들을 배포할 수 있다. 컴퓨팅 인스턴스들은 가상 머신들, 베어 메탈 인스턴스들, 및 유사한 것의 형태를 취할 수 있다. 따라서, CSPI는, 고객들이 고도로 이용가능한 가상 호스팅형 환경에서 광범위한 애플리케이션 및 서비스들을 구축하고 실행하는 것을 가능하게 하는 상보적인 클라우드 서비스들의 세트 및 인프라스트럭처를 제공한다. 고객은 CSPI에 의해 제공된 기초 물리적 자원들을 관리하거나 또는 제어하는 것이 아니라, 운영 체제들, 스토리지, 및 배포된 애플리케이션에 대한 제어; 및 가능하게는 선택 네트워킹 구성요소들(예를 들어, 방화벽들)의 제한된 제어를 갖는다.

[0078] CSP는, 고객들 및 네트워크 관리자들이 CSP 자원들을 사용하여 클라우드에 배포되는 자원들을 구성하고, 액세스하며, 관리하는 것을 가능하게 하는 콘솔을 제공할 수 있다. 특정 실시예들에서, 콘솔은, CSPI에 액세스하고 이를 관리하기 위해 사용될 수 있는 웹-기반 사용자 인터페이스를 제공한다. 일부 구현예들에서, 콘솔은 CSP에 의해 제공되는 웹-기반 애플리케이션이다.

[0079] CSPI는 단일-테넌시 또는 다중-테넌시 아키텍처들을 지원할 수 있다. 단일 테넌시 아키텍처에서, 소프트웨어(예를 들어, 애플리케이션, 데이터베이스) 또는 하드웨어 구성요소(예를 들어, 호스트 머신 또는 서버)는 단일 고객 또는 테넌트를 서비스한다. 다중-테넌시 아키텍처에서, 소프트웨어 또는 하드웨어 구성요소는 다수의 고객들 또는 테넌트들을 서비스한다. 따라서, 다중-테넌시 아키텍처에서, CSPI 자원들은 다수의 고객들 또는 테넌트들 사이에서 공유된다. 다중-테넌시 상황에서, 각각의 테넌트의 데이터가 격리되고 다른 테넌트들에 비가시적으로 남아 있는 것을 보장하기 위해 CSPI 내에서 예방 조치들이 취해지고 세이프가드들이 제위치에 마련된다.

[0080] 물리적 네트워크에서, 네트워크 엔드포인트("엔드포인트")는, 물리적 네트워크에 연결되며 이것이 연결된 네트워크와 앞뒤로 통신하는 컴퓨팅 디바이스 또는 시스템을 의미한다. 물리적 네트워크 내의 네트워크 엔드포인트는 근거리 네트워크(Local Area Network; LAN), 광역 네트워크(Wide Area Network; WAN), 또는 다른 유형의 물리적 네트워크에 연결될 수 있다. 물리적 네트워크 내의 전통적인 엔드포인트들의 예들은, 모뎀들, 허브들, 브리지들, 스위치들, 라우터들, 및 다른 네트워킹 디바이스들, 물리적 컴퓨터들(또는 호스트 머신들), 및 유사한 것을 포함한다. 물리적 네트워크 내의 각각의 물리적 디바이스는 디바이스와 통신하기 위해 사용될 수 있는 고정된 네트워크 어드레스를 갖는다. 이러한 고정된 네트워크 어드레스는 계층-2 어드레스(예를 들어, MAC 어드레스), 고정된 계층-3 어드레스(예를 들어, IP 어드레스), 및 유사한 것일 수 있다. 가상화된 환경 또는 가상 네트워크에서, 엔드포인트들은, 물리적 네트워크의 구성요소들에 의해 호스팅되는(예를 들어, 물리적 호스트 머신

들에 의해 호스팅되는) 가상 머신들과 같은 다양한 가상 엔드포인트들을 포함할 수 있다. 가상 네트워크 내의 이러한 엔드포인트들은 오버레이 계층-2 어드레스들(예를 들어, 오버레이 MAC 어드레스들) 및 오버레이 계층-3 어드레스들(예를 들어, 오버레이 IP 어드레스들)과 같은 오버레이 어드레스들에 의해 어드레싱된다. 네트워크 오버레이들은, 네트워크 관리자들이 (예를 들어, 가상 네트워크에 대한 제어 평면을 구현하는 소프트웨어를 통해) 소프트웨어 관리를 사용하여 네트워크 엔드포인트들과 연관된 오버레이 어드레스들을 이동시키는 것을 가능하게 함으로써 유연성을 가능하게 한다. 따라서, 물리적 네트워크와는 달리, 가상 네트워크에서, 오버레이 어드레스(예를 들어, 오버레이 IP 어드레스)는 네트워크 관리 소프트웨어를 사용하여 하나의 엔드포인트로부터 다른 것으로 이동될 수 있다. 가상 네트워크가 물리적 네트워크의 상단 상에 구축되기 때문에, 가상 네트워크 내의 구성요소들 사이의 통신들은 가상 네트워크 및 기초 물리적 네트워크 둘 모두를 수반한다. 이러한 통신들을 용이하게 하기 위해, CSPI의 구성요소들은, 가상 네트워크 내의 오버레이 어드레스들은 서브스트레이트 네트워크 내의 실제 물리적 어드레스들에 매핑하거나 또는 그 반대인 매핑들을 학습하고 저장하도록 구성된다. 그런 다음, 이러한 매핑들은 통신들을 용이하게 하기 위해 사용된다. 고객 트래픽은 가상 네트워크에서의 라우팅을 용이하게 하기 위해 캡슐화된다.

[0081] 따라서, 물리적 어드레스들(예를 들어, 물리적 IP 어드레스들)은 물리적 네트워크들 내의 구성요소들과 연관되며, 오버레이 어드레스들(예를 들어, 오버레이 IP 어드레스들)은 가상 또는 오버레이 네트워크들 내의 엔티티들과 연관된다. 물리적 IP 어드레스는 서브스트레이트 또는 물리적 네트워크 내의 물리적 디바이스(예를 들어, 네트워크 디바이스)와 연관된다. 예를 들어, 각각의 NVD는 연관된 물리적 IP 어드레스를 갖는다. 오버레이 IP 어드레스는, 고객의 가상 클라우드 네트워크(virtual cloud network; VCN) 내의 컴퓨팅 인스턴스와 같은 오버레이 네트워크 내의 엔티티와 연관된 오버레이 어드레스이다. 각각 그들 자체의 사설 VCN들을 갖는 2개의 상이한 고객들 또는 테넌트들은 잠재적으로 서로에 대해 어떠한 지식도 없이 그들의 VCN들에서 동일한 오버레이 IP 어드레스를 사용할 수 있다. 물리적 IP 어드레스들 및 오버레이 IP 어드레스들 둘 모두는 실제 IP 어드레스들의 유형들이다. 이들은 가상 IP 어드레스들과는 별개이다. 가상 IP 어드레스는 전형적으로, 다수의 실제 IP 어드레스들을 나타내거나 또는 이들에 매핑되는 단일 IP 어드레스이다. 가상 IP 어드레스는 가상 IP 어드레스와 다수의 실제 IP 어드레스들 사이의 1-대-다 매핑을 제공한다. 예를 들어, 로드 밸런서는 다수의 서버들을 나타내거나 또는 이에 매핑하기 위해 VIP를 사용할 수 있으며, 각각의 서버스는 그 자체의 실제 IP 어드레스를 갖는다.

[0082] 클라우드 인프라스트럭처 또는 CSPI는 전세계의 하나 이상의 지역들 내의 하나 이상의 데이터 센터들에서 물리적으로 호스팅된다. CSPI는 물리적 또는 서브스트레이트 네트워크 내의 구성요소들 및 물리적 네트워크 구성요소들의 상단 상에 구축된 가상 네트워크 내에 있는 가상화된 구성요소들(예를 들어, 가상 네트워크들, 컴퓨팅 인스턴스들, 가상 머신들, 등)을 포함할 수 있다. 특정 실시예들에서, CSPI는 렐름(realm)들, 지역들 및 가용성 도메인들로 조직되고 호스팅된다. 지역(region)은 전형적으로 하나 이상의 데이터 센터들을 포함하는 국부화된 지리적 영역(area)이다. 지역들은 일반적으로 서로 독립적이며, 예를 들어, 국가들에 걸쳐 또는 심지어 대륙들에 걸쳐 먼 거리로 분리될 수 있다. 예를 들어, 제1 지역은 호주에 있을 수 있고, 다른 지역은 일본에 있을 수 있으며, 또 다른 지역은 인도에 있을 수 있는 등이다. CSPI 자원들은, 각각의 지역이 CSPI 자원들의 그 자체의 독립적인 서브세트를 갖도록 지역들 사이에서 분할된다. 각각의 지역은, 컴퓨팅 자원들(예를 들어, 베어 메탈 서버들, 가상 머신, 컨테이너들 및 관련된 인프라스트럭처, 등); 저장 자원들(예를 들어, 블록 볼륨 스토리지, 파일 스토리지, 객체 스토리지, 아카이브 스토리지); 네트워킹 자원들(예를 들어, 가상 클라우드 네트워크(VCN)들, 로드 밸런싱 자원들, 사내 네트워크들에 대한 연결들), 데이터베이스 자원들; 에지 네트워킹 자원들(예를 들어, DNS); 및 액세스 관리 및 모니터링 자원들, 및 다른 것들과 같은 코어 인프라스트럭처 서비스들 및 자원들의 세트를 제공할 수 있다. 각각의 지역은 일반적으로 이를 렐름 내의 다른 지역들에 연결하는 다수의 경로들을 갖는다.

[0083] 일반적으로, 애플리케이션은, 근처의 자원들이 거리가 있는 자원들을 사용하는 것보다 더 빠르기 때문에, 애플리케이션이 가장 많이 사용되는 지역에 배포된다(즉, 해당 지역과 연관된 인프라스트럭처 상에 배포된다). 애플리케이션들은 또한, 법적 관할권들, 과세 영역들, 및 다른 사업적 또는 사회적 기준, 및 유사한 것에 대한 다양한 요건들을 충족시키기 위해, 대규모 기상 시스템들 또는 지진들과 같은 지역-전체(region-wide) 이벤트들의 위험을 완화하기 위한 중복성과 같은 다양한 이유들로 상이한 지역들에 배포될 수 있다.

[0084] 지역 내의 데이터 센터들은 가용성 도메인(availability domain; AD)들로 추가로 조직되고 세분화될 수 있다. 가용성 도메인은 지역 내에 위치된 하나 이상의 데이터 센터들에 대응할 수 있다. 지역은 하나 이상의 가용성 도메인들로 구성될 수 있다. 이러한 분산형 환경에서, CSPI 자원들은 가상 클라우드 네트워크(virtual cloud network; VCN)와 같이 지역-특정 또는 컴퓨팅 인스턴스와 같이 가용성-도메인 특정일 수 있다.

[0085] 지역 내의 AD들은 서로 격리되고, 장애에 내성이 있으며, 동시에 고장이 날 가능성이 매우 낮도록 구성된다. 이는, 지역 내의 하나의 AD에서의 장애가 동일한 지역 내의 다른 AD들의 가용성에 영향을 줄 가능성이 낮도록 네트워킹, 물리적 케이블들, 케이블 경로들, 케이블 진입 지점들과 같은 중요 인프라스트럭처 자원들을 공유하지 않는 AD들에 의해 달성된다. 동일한 지역 내의 AD들은 저 레이턴시, 고 대역폭 네트워크에 의해 서로 연결될 수 있으며, 이는, 다른 네트워크들(예를 들어, 인터넷, 고객의 사내 네트워크들, 등)에 대한 고-가용성 연결성을 제공하고 고-가용성 및 재해 복구 둘 모두를 위해 복제된 시스템들을 다수의 AD들에 구축하는 것을 가능하게 한다. 클라우드 서비스들은 고 가용성을 보장하고 자원 장애에 대해 보호하기 위해 다수의 AD들을 사용한다. IaaS 제공자들에 의해 제공되는 인프라스트럭처가 성장함에 따라, 더 많은 지역들 및 AD들에 추가적인 용량이 추가될 수 있다. 가용성 도메인들 사이의 트래픽은 일반적으로 암호화된다.

[0086] 특정 실시예들에서, 지역들은 렐름들로 그룹화된다. 렐름은 지역들의 논리적 집합이다. 렐름들은 서로 격리되며 어떠한 데이터도 공유하지 않는다. 동일한 렐름 내의 지역들은 서로 통신할 수 있지만, 상이한 렐름들 내의 지역들은 그럴 수 없다. CSP를 갖는 고객의 테넌시 또는 계정은 단일 렐름에 존재하며, 해당 렐름에 속한 하나 이상의 지역들에 걸쳐 분산될 수 있다. 전형적으로, 고객이 IaaS 서비스에 가입할 때, 테넌시 또는 계정은 렐름 내의 고객-지정 지역("홈" 지역으로 지칭됨) 내의 해당 고객에 대해 생성된다. 고객은 렐름 내의 하나 이상의 다른 지역들에 걸쳐 고객의 테넌시를 확장할 수 있다. 고객은, 고객의 테넌시가 존재하는 렐름에 있지 않는 지역들에 액세스할 수 없다.

[0087] IaaS 제공자는 다수의 렐름들을 제공할 수 있으며, 각각의 렐름은 고객들 또는 사용자들의 특정 세트에 맞춰 제공된다. 예를 들어, 상업적 렐름은 상업적 고객들에 대해 제공될 수 있다. 다른 예로서, 렐름은 해당 국가 내의 고객들에 대해 특정 국가에 대해 제공될 수 있다. 또 다른 예로서, 정부 렐름은 정부 및 유사한 것에 대해 제공될 수 있다. 예를 들어, 정부 렐름은 특정 정부에 맞춰 제공될 수 있으며, 상업적 렐름보다 높은 보안 레벨을 가질 수 있다. 예를 들어, 오라클 클라우드 인프라스트럭처(Oracle Cloud Infrastructure; OCI)는 현재 상업적 영역(region)들에 대한 렐름 및 정부 클라우드 영역들에 대한 2개의 렐름들(예를 들어, FedRAMP 인가됨 및 IL5 인가됨)을 제공한다.

[0088] 특정 실시예들에서, AD는 하나 이상의 장애 도메인(fault domain)들로 세분될 수 있다. 장애 도메인은 안티-어피티니(anti-affinity)를 제공하기 위한 AD 내의 인프라스트럭처 자원들을 그룹화한 것이다. 장애 도메인들은, 인스턴스들이 단일 AD 내의 동일한 물리적 하드웨어 상에 있지 않도록 컴퓨팅 인스턴스들의 분산을 가능하게 한다. 이는 안티-어피니티로 알려져 있다. 장애 도메인은 단일 장애 지점을 공유하는 하드웨어 구성요소들(컴퓨터들, 스위치들, 등)의 세트를 의미한다. 컴퓨팅 풀은 장애 도메인들로 논리적으로 분할된다. 이로 인해, 하나의 장애 도메인에 영향을 주는 하드웨어 장애 또는 컴퓨터 하드웨어 유지보수는 다른 장애 도메인들 내의 인스턴스들에 영향을 주지 않는다. 실시예에 의존하여, 각각의 AD에 대한 장애 도메인들의 수는 변화할 수 있다. 예를 들어, 특정 실시예들에서, 각각의 AD는 3개의 장애 도메인들을 포함한다. 장애 도메인들은 AD 내에서 논리적 데이터 센터로서 역할한다.

[0089] 고객이 IaaS 서비스에 가입할 때, CSPI로부터의 자원들은 고객에 대해 프로비저닝되고 고객의 텐넌시와 연관된다. 고객은 사설 네트워크들을 구축하고 이러한 네트워크들 상에 자원들을 배포하기 위해 이러한 프로비저닝된 자원들을 사용할 수 있다. CSPI에 의해 클라우드 내에서 호스팅되는 고객 네트워크들은 가상 클라우드 네트워크(virtual cloud network; VCN)들로서 지칭된다. 고객은 고객에 대해 할당된 CSPI 자원들을 사용하여 하나 이상의 가상 클라우드 네트워크(VCN)들을 셋업할 수 있다. VCN은 가상 또는 소프트웨어 정의형 사설 네트워크이다. 고객의 VCN에 배포된 고객 자원들은 컴퓨팅 인스턴스들(예를 들어, 가상 머신들, 베어-메탈 인스턴스들) 및 다른 자원들을 포함할 수 있다. 이러한 컴퓨팅 인스턴스들은 애플리케이션들, 로드 밸런서들, 데이터베이스들, 및 유사한 것과 같은 고객 워크로드들을 나타낼 수 있다. VCN 상에 배포된 컴퓨팅 인스턴스는, 인터넷과 같은 공용 네트워크를 통해, 공용 액세스가능 엔드포인트들("공용 엔드포인트들"), 동일한 VCN 또는 다른 VCN들(예를 들어, 고객의 다른 VCN들, 또는 고객에게 속하지 않은 VCN들) 내의 다른 인스턴스들, 고객의 사내 데이터 센터들 또는 네트워크들, 서비스 엔드포인트들, 및 다른 유형들의 엔드포인트들과 통신할 수 있다.

[0090] CSP는 CSPI를 사용하여 다양한 서비스들을 제공할 수 있다. 일부 경우들에서, CSPI의 고객들은 자신들이 서비스 제공자처럼 행동하고 CSPI 자원들을 사용하여 서비스들을 제공할 수 있다. 서비스 제공자는, 식별 정보(예를 들어, IP 어드레스, DNS 명칭 및 포트)에 의해 특징지어지는 서비스 엔드포인트를 노출할 수 있다. 고객의 자원(예를 들어, 컴퓨팅 인스턴스)는 해당 특정 서비스에 대해 서비스에 의해 노출된 서비스 엔드포인트에 액세스함으로써 특정 서비스를 소비할 수 있다. 이러한 서비스 엔드포인트들은 일반적으로, 인터넷과 같은 공용 통신 네트워크를 통해 엔드포인트들과 연관된 공인 IP 어드레스들을 사용하여 사용자들에 의해 공개적으로 액세스가능

한 엔드포인트들이다. 공개적으로 액세스가능한 네트워크 엔드포인트들은 때때로 공용 엔드포인트들로도 지칭된다.

[0091] 특정 실시예들에서, 서비스 제공자는 서비스에 대한 엔드포인트(때때로 서비스 엔드포인트로 지칭됨)를 통해 서비스를 노출할 수 있다. 그런 다음, 서비스의 고객들은 서비스에 액세스하기 위해 이러한 서비스 엔드포인트를 사용할 수 있다. 특정 구현예들에서, 서비스에 대해 제공되는 서비스 엔드포인트는 해당 서비스를 소비하려고 하는 다수의 고객들에 의해 액세스될 수 있다. 다른 구현예들에서, 해당 고객만이 해당 전용 서비스 엔드포인트를 사용하여 서비스에 액세스할 수 있도록 전용 서비스 엔드포인트가 고객에 대해 제공될 수 있다.

[0092] 특정 실시예들에서, VCN이 생성될 때, VCN은 사설 오버레이 클래스리스 인터-도메인 라우팅(Classless Inter-Domain Routing; CIDR) 어드레스 공간과 연관되며, 이는 VCN에 할당된 사설 오버레이 IP 어드레스들의 범위이다(예를 들어, 10.0/16). VCN은 연관된 서브넷들, 루트 테이블들, 및 게이트웨이들을 포함한다. VCN은 단일 지역 내에 상주하지만 지역의 가용성 도메인들 중 하나 또는 그 이상 또는 전부에 걸쳐 있을 수 있다. 게이트웨이는, VCN에 대해 구성되고 VCN으로 그리고 이로부터 VCN 외부의 하나 이상의 엔드포인트들로의 트래픽의 통신을 가능하게 하는 가상 인터페이스이다. 하나 이상의 상이한 유형들의 게이트웨이들이 상이한 유형들의 엔드포인트들로의 그리고 이로부터의 통신을 가능하게 하기 위해 VCN에 대해 구성될 수 있다.

[0093] VCN은 하나 이상의 서브넷들과 같은 하나 이상의 서브-네트워크들로 세분될 수 있다. 따라서, 서브넷은 VCN 내에 생성될 수 있는 구성의 유닛 또는 서브디비전(subdivision)이다. VCN은 하나 또는 다수의 서브넷들을 가질 수 있다. VCN 내의 각각의 서브넷은, 해당 VCN 내의 다른 서브넷들과 중첩하지 않으며 VCN의 어드레스 공간 내의 어드레스 공간 서브넷을 나타내는 오버레이 IP 어드레스들의 연속적인 범위(예를 들어, 10.0.0.0/24 및 10.0.1.0/24)와 연관된다.

[0094] 각각의 컴퓨팅 인스턴스는, 컴퓨팅 인스턴스가 VCN의 서브넷에 참여하는 것을 가능하게 하는 가상 네트워크 인터페이스 카드(virtual network interface card; VNIC)와 연관된다. VNIC는 물리적 네트워크 인터페이스 카드(Network Interface Card; NIC)의 논리적 표현이다. 일반적으로, VNIC은 엔티티(예를 들어, 컴퓨팅 인스턴스, 서비스)와 가상 네트워크 사이의 인터페이스이다. VNIC은 서브넷에 존재하고, 하나 이상의 연관된 IP 어드레스들 및 연관된 보안 규칙들 또는 정책들을 갖는다. VNIC은 스위치 상의 계층-2 포트와 동등하다. VNIC은 컴퓨팅 인스턴스에 그리고 VCN 내의 서브넷에 접속된다. 컴퓨팅 인스턴스와 연관된 VNIC는 컴퓨팅 인스턴스가 VCN의 서브넷의 부분이 되는 것을 가능하게 하고, 컴퓨팅 인스턴스가 컴퓨팅 인스턴스와 동일한 서브넷 상에 있는 엔드포인트들, VCN 내의 상이한 서브넷들 내의 엔드포인트들, 또는 VCN 외부의 엔드포인트들과 통신하는 것(예를 들어, 패킷들을 전송하고 수신하는 것)을 가능하게 한다. 따라서, 컴퓨팅 인스턴스와 연관된 VNIC은, 컴퓨팅 인스턴스가 VNIC 내부 및 외부의 엔드포인트들과 연결하는 방법을 결정한다. 컴퓨팅 인스턴스에 대한 VNIC이 생성되며, 이는, 컴퓨팅 인스턴스가 생성되고 VCN 내의 서브넷에 추가될 때 해당 컴퓨팅 인스턴스와 연관된다. 컴퓨팅 인스턴스들의 세트를 포함하는 서브넷에 대해, 서브넷은 컴퓨팅 인스턴스들의 세트에 대응하는 VNIC들을 포함하며, 각각의 VNIC는 컴퓨팅 인스턴스들의 세트 내의 컴퓨팅 인스턴스에 접속된다.

[0095] 각각의 컴퓨팅 인스턴스에는 컴퓨팅 인스턴스와 연관된 VNIC를 통해 사설 오버레이 IP 어드레스가 할당된다. 이러한 사설 오버레이 IP 어드레스는, 컴퓨팅 인스턴스가 생성되고 컴퓨팅 인스턴스로의 그리고 이로부터의 트래픽을 라우팅하기 위해 사용될 때 컴퓨팅 인스턴스와 연관된 VNIC에 할당된다. 주어진 서브넷 내의 모든 VNIC들은 동일한 루트 테이블, 보안 리스트들, 및 DHCP 옵션들을 사용한다. 이상에서 설명된 바와 같이, VCN 내의 각각의 서브넷은, 해당 VCN 내의 다른 서브넷들과 중첩하지 않으며 VCN의 어드레스 공간 내의 어드레스 공간 서브넷을 나타내는 오버레이 IP 어드레스들의 연속적인 범위(예를 들어, 10.0.0.0/24 및 10.0.1.0/24)와 연관된다. VCN의 특정 서브넷 상의 VNIC에 대해, VNIC에 할당된 사설 오버레이 IP 어드레스는 서브넷에 대해 할당된 오버레이 IP 어드레스들의 연속적인 범위로부터의 어드레스이다.

[0096] 특정 실시예들에서, 컴퓨팅 인스턴스에는 선택적으로, 사설 오버레이 IP 어드레스에 추가하여, 예를 들어, 공용 서브넷에 있는 경우 하나 이상의 공인 IP 어드레스들과 같은 추가적인 오버레이 IP 어드레스들이 할당될 수 있다. 이러한 다수의 어드레스들은 동일한 VNIC 상에 할당되거나 또는 컴퓨팅 인스턴스와 연관된 다수의 VNIC들에 걸쳐 할당된다. 그러나, 각각의 인스턴스는 인스턴스 런칭 동안 생성되고 인스턴스에 할당된 오버레이 사설 IP 어드레스와 연관된 1차(primary) VNIC를 가지며 - 이러한 1차 VNIC는 제거될 수 없다. 2차 VNIC들로 지칭되는 추가적인 VNIC들이 1차 VNIC와 동일한 가용성 도메인 내의 기존 인스턴스에 추가될 수 있다. 모든 VNIC들은 인스턴스와 동일한 가용성 도메인에 있다. 2차 VNIC는 1차 VNIC와 동일한 VCN 내의 서브넷에 있을 수 있거나, 또는 동일한 VCN 또는 상이한 VCN 내에 있는 상이한 서브넷에 있을 수 있다.

[0097] 컴퓨팅 인스턴스에는 선택적으로, 컴퓨팅 인스턴스가 공용 서브넷 내에 있는 경우 공인 IP 어드레스가 할당될 수 있다. 서브넷은 서브넷이 생성되는 시점에 공용 서브넷 또는 사설 서브넷으로 지정될 수 있다. 사설 서브넷은, 서브넷 내의 자원들(예를 들어, 컴퓨팅 인스턴스들) 및 연관된 VNIC들이 공인 오버레이 IP 어드레스들을 가질 수 없다는 것을 의미한다. 공용 서브넷은, 서브넷 내의 자원들 및 연관된 VNIC들이 공인 IP 어드레스들을 가질 수 있다는 것을 의미한다. 고객은 지역 또는 렐름 내의 단일 가용성 도메인에 또는 다수의 가용성 도메인들에 걸쳐 존재하도록 서브넷을 지정할 수 있다.

[0098] 이상에서 설명된 바와 같이, VCN은 하나 이상의 서브넷들로 세분될 수 있다. 특정 실시예들에서, VCN에 대해 구성된 가상 라우터(Virtual Router; VR)(VCN VR 또는 단지 VR로 지칭됨)는 VCN의 서브넷들 사이의 통신들을 가능하게 한다. VCN 내의 서브넷에 대해, VR은, 서브넷(즉, 해당 서브넷 상의 컴퓨팅 인스턴스들)이 VCN 내의 다른 서브넷들 상의 엔드포인트들 및 VCN 외부의 다른 엔드포인트들과 통신하는 것을 가능하게 하는 해당 서브넷에 대한 논리적 게이트웨이를 나타낸다. VCN VR은, VCN 내의 VNIC들과 VCN과 연관된 가상 게이트웨이들("게이트웨이들") 사이에서 트래픽을 라우팅하도록 구성된 논리적 엔티티이다. 게이트웨이들은 도 6과 관련하여 아래에서 추가로 설명된다. VCN VR은 계층-3/IP 계층 개념이다. 일 실시예에서, VCN에 대해 하나의 VCN VR이 있으며, 여기서 VCN VR은 잠재적으로 IP 어드레스들에 의해 어드레싱되는 무한한 수의 포트들을 가지고, 여기서 하나의 포트는 VCN의 각각의 서브넷에 대한 것이다. 이러한 방식으로, VCN VR는, VCN VR이 접속된 VCN 내의 각각의 서브넷에 대해 상이한 IP 어드레스를 갖는다. VR은 또한 VCN에 대해 구성된 다양한 게이트웨이들에 연결된다. 특정 실시예들에서, 서브넷에 대한 오버레이 IP 어드레스 범위로부터의 특정 오버레이 IP 어드레스는 해당 서브넷에 대한 VCN VR의 포트에 대해 예약된다. 예를 들어, 각각 연관된 어드레스 범위들 10.0/16 및 10.1/16을 갖는 2개의 서브넷들을 갖는 VCN을 고려해 본다. 어드레스 범위 10.0/16을 갖는 VCN 내의 제1 서브넷에 대해, 이러한 범위로부터의 어드레스는 해당 서브넷에 대한 VCN VR의 포트에 대해 예약된다. 일부 경우들에서, 그 범위로부터의 제1 IP 어드레스는 VCN VR에 대해 예약될 수 있다. 예를 들어, 오버레이 IP 어드레스 범위 10.0/16을 갖는 서브넷에 대해, IP 어드레스 10.0.0.1이 해당 서브넷에 대한 VCN VR의 포트에 대해 예약될 수 있다. 어드레스 범위 10.1/16를 갖는 동일한 VCN 내의 제2 서브넷에 대해, VCN VR은 IP 어드레스 10.1.0.1을 갖는 해당 제2 서브넷에 대한 포트를 가질 수 있다. VCN VR는 VCN 내의 각각의 서브넷에 대해 상이한 IP 어드레스를 갖는다.

[0099] 일부 다른 실시예들에서, VCN 내의 각각의 서브넷은, VR과 연관된 예약된 또는 디폴트 IP 어드레스를 사용하여 서브넷에 의해 어드레스가능한 그 자체의 연관된 VR을 가질 수 있다. 예약된 또는 디폴트 IP 어드레스는, 예를 들어, 해당 서브넷과 연관된 IP 어드레스들의 범위로부터의 제1 IP 어드레스일 수 있다. 서브넷 내의 VNIC들은 이러한 디폴트 또는 예약된 IP 어드레스를 사용하여 서브넷과 연관된 VR과 통신(예를 들어, 패킷들을 전송하고 수신)할 수 있다. 이러한 실시예에서, VR은 해당 서브넷에 대한 진입/진출(ingress/egress) 포인트이다. VCN 내의 서브넷과 연관된 VR은 VCN 내의 다른 서브넷들과 연관된 다른 VR들과 통신할 수 있다. VR들은 또한 VCN과 연관된 게이트웨이들과 통신할 수 있다. 서브넷에 대한 VR 기능은 서브넷 내의 VNIC에 대한 VNIC 기능성을 실행하는 하나 이상의 NVD들 상에서 실행 중이거나 또는 이들에 의해 실행된다.

[0100] 루트 테이블들, 보안 규칙들, 및 DHCP 옵션들은 VCN에 대해 구성될 수 있다. 루트 테이블들은 VCN에 대한 가상 루트 테이블들이며, 트래픽을 VCN 내의 서브넷들로부터 특별하게 구성된 인스턴스들 또는 게이트웨이들을 통해 VCN 외부의 목적지들로 라우팅하기 위한 규칙들을 포함한다. VCN의 루트 테이블들은, 패킷들이 VCN으로 그리고 이로부터 포워딩/라우팅되는 방법을 제어하도록 맞춤화될 수 있다. DHCP 옵션들은, 인스턴스들이 부팅(boot up)될 때 인스턴스들에 자동으로 제공되는 구성 정보를 의미한다.

[0101] VCN에 대해 구성된 보안 규칙들은 VCN에 대한 오버레이 방화벽 규칙들을 나타낸다. 보안 규칙들은 진입 및 진출 규칙들을 포함하며, (예를 들어, 프로토콜 및 포트에 기초하여) VCN 내의 인스턴스들 안팎으로 허용된 트래픽의 유형들을 지정한다. 고객은, 주어진 규칙이 스테이트풀(stateful)인지 또는 스테이트리스인지 여부를 선택할 수 있다. 예를 들어, 고객은, 소스 CIDR 0.0.0.0/0, 및 목적지 TCP 포트 22를 갖는 스테이트풀 진입 규칙을 셋업함으로써 임의의 장소로부터 인스턴스들의 세트로의 인커밍 SSH 트래픽을 허용할 수 있다. 보안 규칙들은 네트워크 보안 그룹들 또는 보안 리스트들을 사용하여 구현될 수 있다. 네트워크 보안 그룹은 해당 그룹 내의 자원들에만 적용되는 보안 규칙들의 세트로 구성된다. 반면, 보안 리스트는, 보안 리스트를 사용하는 임의의 서브넷 내의 모든 자원들에 적용되는 규칙들을 포함한다. VCN에는 디폴트 보안 규칙들과 함께 디폴트 보안 리스트가 제공될 수 있다. VCN에 대해 구성된 DHCP 옵션들은, 인스턴스들이 부팅될 때 VCN 내의 인스턴스들에 자동으로 제공되는 구성 정보를 제공한다.

[0102] 특정 실시예들에서, VCN에 대한 구성 정보는 VCN 제어 평면에 의해 결정되고 저장된다. VCN에 대한 구성 정보는, 예를 들어, 다음에 관한 정보를 포함할 수 있다: VCN과 연관된 어드레스 범위, VCN 내의 서브넷들 및

연관된 정보, VCN과 연관된 하나 이상의 VR들, VCN 내의 컴퓨팅 인스턴스 및 연관된 VNIC들, VCN과 연관된 다양한 가상화 네트워크 기능들(예를 들어, VNIC들, VR들, 게이트웨이들)을 실행하는 NVD들, VCN에 대한 상태 정보, 및 다른 VCN-관련 정보. 특정 실시예들에서, VCN 배포(Distribution) 서비스는 VCN 제어 평면 또는 이의 부분들에 의해 저장된 구성 정보를 NVD들로 퍼블리싱(publish)한다. 배포된 정보는 VCN 내의 컴퓨팅 인스턴스로 그리고 이로부터 패킷들을 포워딩하기 위해 NVD들에 의해 저장되고 사용되는 정보(예를 들어, 포워딩 테이블들, 라우팅 테이블들, 등)를 업데이트하기 위해 사용될 수 있다.

[0103] 특정 실시예들에서, VCN들 및 서브넷들의 생성은 VCN 제어 평면(Control Plane; CP)에 의해 핸들링되며, 컴퓨팅 인스턴스들의 런칭은 컴퓨팅 제어 평면에 의해 핸들링된다. 컴퓨팅 제어 평면은 컴퓨팅 인스턴스에 대한 물리적 자원을 할당하는 것을 담당하고, 그런 다음 VNIC들을 생성하여 이를 컴퓨팅 인스턴스에 접속시키기 위해 VCN 제어 평면을 호출한다. VCN CP는 또한, 패킷 포워딩 및 라우팅 기능들을 수행하도록 구성된 VCN 데이터 평면으로 VCN 데이터 매핑들을 전송한다. 특정 실시예들에서, VCN CP는, VCN 데이터 평면에 업데이트들을 제공하는 것을 담당하는 배포 서비스를 제공한다. VCN 제어 평면의 예들은 또한 도 11, 도 12, 도 13 및 도 14(참조 부호 1116, 1216, 1316, 및 1416 참조)에 도시되며 이하에서 설명된다.

[0104] 고객은 CSPI에 의해 호스팅되는 자원들을 사용하여 하나 이상의 VCN들을 생성할 수 있다. 고객 VCN 상에 배포된 컴퓨팅 인스턴스는 상이한 엔드포인트들과 통신할 수 있다. 이러한 엔드포인트들은 CSPI에 의해 호스팅되는 엔드포인트들 및 CSPI 외부의 엔드포인트들을 포함할 수 있다.

[0105] CSPI 사용하여 클라우드-기반 서비스를 구현하기 위한 다양하고 상이한 아키텍처들이 도 6, 도 7, 도 8, 도 9, 도 10, 도 11, 도 12, 도 13, 및 도 15에 도시되며 이하에서 설명된다. 도 6은 특정 실시예들에 따른, CSPI에 의해 호스팅되는 오버레이 또는 고객 VCN을 보여주는 분산형 환경(600)의 하이 레벨 도면이다. 도 6에 도시된 분산형 환경은 오버레이 네트워크 내에 다수의 구성요소들을 포함한다. 도 6에 도시된 분산형 환경(600)은 단지 일 예이며, 청구되는 실시예들의 범위를 과도하게 제한하려고 의도되지 않는다. 많은 변형들, 대안들, 및 수정들이 가능하다. 예를 들어, 일부 구현예들에서, 도 6에 도시된 분산형 환경은 도 1에 도시된 것보다 더 많거나 또는 더 적은 시스템들 또는 구성요소들을 가질 수 있거나, 2개 이상의 시스템들을 결합할 수 있거나, 또는 시스템들의 상이한 구성 또는 배열을 가질 수 있다.

[0106] 도 6에 도시된 예에 도시된 바와 같이, 분산형 환경(600)은, 고객들이 가입할 수 있고 그들의 가상 클라우드 네트워크(VCN)들을 구축하기 위해 사용할 수 있는 서비스들 및 자원들을 제공하는 CSPI(601)를 포함한다. 특정 실시예들에서, CSPI(601)는 가입 고객들에게 IaaS 서비스들을 제공한다. CSPI(601) 내의 데이터 센터들은 하나 이상의 지역들로 조직될 수 있다. 하나의 예시적인 지역인 "지역 US"(602)가 도 6에 도시된다. 고객은 지역(602)에 대해 고객 VCN(604)을 구성하였다. 고객은 VCN(604) 상에 다양한 컴퓨팅 인스턴스들을 배포할 수 있으며, 여기서 컴퓨팅 인스턴스들은 가상 머신들 또는 베어 메탈 인스턴스들을 포함할 수 있다. 인스턴스들의 예들은 애플리케이션들, 데이터베이스, 로드 밸런서들, 및 유사한 것을 포함한다.

[0107] 도 6에 도시된 실시예에서, 고객 VCN(604)는 2개의 서브넷들, 즉, "서브넷-1" 및 "서브넷-2"를 포함하며, 각각의 서브넷은 그 자체의 CIDR IP 어드레스 범위를 갖는다. 도 6에서, 서브넷-1에 대한 오버레이 IP 어드레스 범위는 10.0/16이며, 서브넷-2에 대한 어드레스 범위는 10.1/16이다. VCN 가상 라우터(605)는, VCN(604)의 서브넷들 사이의 그리고 VCN 외부의 다른 엔드포인트들과의 통신들을 가능하게 하는 VCN에 대한 논리적 게이트웨이를 나타낸다. VCN VR(605)은, VCN(604) 내의 VNIC들과 VCN(604)과 연관된 게이트웨이들 사이에서 트래픽을 라우팅하도록 구성된다. VCN VR(605)은 VCN(604)의 각각의 서브넷에 대한 포트를 제공한다. 예를 들어, VR(605)은 서브넷-1에 대한 IP 어드레스 10.0.0.1를 갖는 포트 및 서브넷-2에 대한 IP 어드레스 10.1.0.1을 갖는 포트를 제공할 수 있다.

[0108] 다수의 컴퓨팅 인스턴스들은 각각의 서브넷 상에 배포될 수 있으며, 여기서 컴퓨팅 인스턴스들은 가상 머신 인스턴스들 및/또는 베어 메탈 인스턴스들일 수 있다. 서브넷 내의 컴퓨팅 인스턴스들은 CSPI(601) 내의 하나 이상의 호스트 머신들에 의해 호스팅될 수 있다. 컴퓨팅 인스턴스는 컴퓨팅 인스턴스와 연관된 VNIC를 통해 서브넷에 참여한다. 예를 들어, 도 6에 도시된 바와 같이, 컴퓨팅 인스턴스(C1)는 컴퓨팅 인스턴스와 연관된 VNIC를 통해 서브넷-1의 부분이다. 유사하게, 컴퓨팅 인스턴스(C2)는 C2와 연관된 VNIC를 통해 서브넷-1의 부분이다. 유사한 방식으로, 가상 머신 인스턴스들 또는 베어 메탈 인스턴스들일 수 있는 다수의 컴퓨팅 인스턴스들은 서브넷-1의 부분일 수 있다. 그 연관된 VNIC를 통해, 각각의 컴퓨팅 인스턴스에는 사설 오버레이 IP 어드레스 및 MAC 어드레스가 할당된다. 예를 들어, 도 6에서, 컴퓨팅 인스턴스(C1)는 10.0.0.2의 오버레이 IP 어드레스 및 M1의 MAC 어드레스를 가지며, 반면 컴퓨팅 인스턴스(C2)는 10.0.0.3의 사설 오버레이 IP 어드레스 및 M2의 MAC

어드레스를 갖는다. 컴퓨팅 인스턴스들(C1 및 C2)을 포함하여 서브넷-1 내의 각각의 컴퓨팅 인스턴스는, 서브넷-1에 대한 VCN VR(605)의 포트에 대한 IP 어드레스인 IP 어드레스 10.0.0.1를 사용하는 VCN VR(605)에 대한 디폴트 루트를 갖는다.

[0109] 서브넷-2는, 가상 머신 인스턴스들 및/또는 베어 메탈 인스턴스들을 포함하여 그 위에 배포된 다수의 컴퓨팅 인스턴스들을 가질 수 있다. 예를 들어, 도 6에 도시된 바와 같이, 컴퓨팅 인스턴스들(D1 및 D2)은 개별적인 컴퓨팅 인스턴스들과 연관된 VNIC들을 통해 서브넷-2의 부분이다. 도 6에 도시된 실시예에서, 컴퓨팅 인스턴스(D1)는 10.1.0.2의 오버레이 IP 어드레스 및 MM1의 MAC 어드레스를 가지며, 반면 컴퓨팅 인스턴스(D2)는 10.1.0.3의 사설 오버레이 IP 어드레스 및 MM2의 MAC 어드레스를 갖는다. 컴퓨팅 인스턴스들(D1 및 D2)을 포함하여 서브넷-2 내의 각각의 컴퓨팅 인스턴스는, 서브넷-2에 대한 VCN VR(605)의 포트에 대한 IP 어드레스인 IP 어드레스 10.1.0.1를 사용하는 VCN VR(605)에 대한 디폴트 루트를 갖는다.

[0110] VCN A(604)는 또한 하나 이상의 로드 밸런서들을 포함할 수 있다. 예를 들어, 로드 밸런서는 서브넷에 대해 제공될 수 있으며, 서브넷 상의 다수의 컴퓨팅 인스턴스들에 걸쳐 트래픽을 로드 밸런싱하도록 구성될 수 있다. 로드 밸런서는 또한 VCN 내의 서브넷들에 걸쳐 트래픽을 로드 밸런싱하기 위해 제공될 수 있다.

[0111] VCN(604) 상에 배포된 특정 컴퓨팅 인스턴스는 다양하고 상이한 엔드포인트들과 통신할 수 있다. 이러한 엔드포인트들은 CSPI(700)에 의해 호스팅되는 엔드포인트들 및 CSPI(700) 외부의 엔드포인트들을 포함할 수 있다. CSPI(601)에 의해 호스팅되는 엔드포인트들을 다음을 포함할 수 있다: 특정 컴퓨팅 인스턴스와 동일한 서브넷 상의 엔드포인트(예를 들어, 서브넷-1에서 2개의 컴퓨팅 인스턴스들 사이의 통신들); 동일한 VCN 내에 있지만 상이한 서브넷 상의 엔드포인트(예를 들어, 서브넷-1 내의 컴퓨팅 인스턴스와 서브넷-2 내의 컴퓨팅 인스턴스 사이의 통신); 동일한 지역 내의 상이한 VCN 내의 엔드포인트(예를 들어, 동일한 지역(606 또는 610)) 내의 VCN 내의 엔드포인트와 서브넷-1 내의 컴퓨팅 인스턴스 사이의 통신들 또는 동일한 지역 내의 서비스 네트워크(610) 내의 엔드포인트와 서브넷-1 내의 컴퓨팅 인스턴스 사이의 통신들); 또는 상이한 지역 내의 VCN 내의 엔드포인트(예를 들어, 상이한 지역(608) 내의 VCN 내의 엔드포인트와 서브넷-1 내의 컴퓨팅 인스턴스 사이의 통신들). CSPI(601)에 의해 호스팅되는 서브넷 내의 컴퓨팅 인스턴스는 또한 CSPI(601)에 의해 호스팅되지 않는(즉, CSPI(601) 외부에 있는) 엔드포인트들과 통신할 수 있다. 이러한 외부 엔드포인트들은 고객의 사내 네트워크(616) 내의 엔드포인트들, 다른 원격 클라우드 호스팅형 네트워크들(618) 내의 엔드포인트들, 인터넷과 같은 공용 네트워크를 통해 액세스가능한 공용 엔드포인트들(614), 및 다른 엔드포인트들을 포함한다.

[0112] 동일한 서브넷 상의 컴퓨팅 인스턴스들 사이의 통신은 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스와 연관된 VNIC들을 사용하여 가능하게 된다. 예를 들어, 서브넷-1 내의 컴퓨팅 인스턴스(C1)는 서브넷-1 내의 컴퓨팅 인스턴스(C2)로 패킷들을 전송하기를 원할 수 있다. 소스 컴퓨팅 인스턴스에서 발원하며 그 목적지가 동일한 서브넷 내의 다른 컴퓨팅 인스턴스인 패킷에 대해, 패킷은 먼저 소스 컴퓨팅 인스턴스와 연관된 VNIC에 의해 프로세싱된다. 소스 컴퓨팅 인스턴스와 연관된 VNIC에 의해 수행되는 프로세싱은, 패킷 헤더들로부터 패킷에 대한 목적지 정보를 결정하는 단계, 소스 컴퓨팅 인스턴스와 연관된 VNIC에 대해 구성된 임의의 정책들(예를 들어, 보안 리스트들)을 식별하는 단계, 패킷에 대한 다음 홉(hop)을 결정하는 단계, 필요에 따라 임의의 패킷 캡슐화/캡슐화해제(decapsulation) 기능들을 수행하는 단계, 그런 다음 그 의도된 목적지로의 패킷들의 통신을 가능하게 하려는 목적으로 패킷을 다음 홉으로 포워딩/라우팅하는 단계를 포함할 수 있다. 목적지 컴퓨팅 인스턴스가 소스 컴퓨팅 인스턴스와 동일한 서브넷에 있을 때, 소스 컴퓨팅 인스턴스와 연관된 VNIC은 목적지 컴퓨팅 인스턴스와 연관된 VNIC를 식별하고 패킷을 프로세싱을 위해 해당 VNIC로 포워딩하도록 구성된다. 그런 다음, 목적지 컴퓨팅 인스턴스와 연관된 VNIC가 실행되고 패킷을 목적지 컴퓨팅 인스턴스로 포워딩한다.

[0113] 서브넷 내의 컴퓨팅 인스턴스로부터 동일한 VCN 내의 상이한 서브넷 내의 엔드포인트로 통신될 패킷에 대해, 통신은 소스 및 목적지 컴퓨팅 인스턴스들과 연관된 VNIC들 및 VCN VR에 의해 가능하게 된다. 예를 들어, 도 6에서 서브넷-1 내의 컴퓨팅 인스턴스(C1)가 서브넷-2 내의 컴퓨팅 인스턴스(D1)로 패킷을 전송하기를 원하는 경우, 패킷은 먼저 컴퓨팅 인스턴스(C1)와 연관된 VNIC에 의해 프로세싱된다. 컴퓨팅 인스턴스(C1)와 연관된 VNIC는 VCN VR의 디폴트 루트 또는 포트 10.0.0.1를 사용하여 패킷을 VCN VR(605)로 라우팅하도록 구성된다. VCN VR(605)는 포트 10.1.0.1을 사용하여 패킷을 서브넷-2로 라우팅하도록 구성된다. 그런 다음, 패킷은 D1과 연관된 VNIC에 의해 수신되고 프로세싱되며, VNIC은 패킷을 컴퓨팅 인스턴스(D1)로 포워딩한다.

[0114] VCN(604) 내의 컴퓨팅 인스턴스로부터 VCN(604) 외부에 있는 엔드포인트로 통신될 패킷에 대해, 통신은 소스 컴퓨팅 인스턴스와 연관된 VNIC, VCN VR(605), 및 VCN(604)와 연관된 게이트웨이들에 의해 가능하게 된다. 하나 이상의 유형들의 게이트웨이들이 VCN(604)과 연관될 수 있다. 게이트웨이는 VCN과 다른 엔드포인트 사이의 인터

페이스이며, 여기서 다른 엔드포인트는 VCN 외부에 있다. 게이트웨이는 계층-3/IP 계층 개념이며, VCN이 VCN 외부의 엔드포인트들과 통신하는 것을 가능하게 한다. 따라서, 게이트웨이는 VCN과 다른 VCN들 또는 네트워크들 사이의 트래픽 흐름을 가능하게 한다. 다양하고 상이한 유형들의 게이트웨이들이 상이한 유형들의 엔드포인트들과의 상이한 유형들의 통신들을 가능하게 하기 위해 VCN에 대해 구성될 수 있다. 게이트웨이에 의존하여, 통신들은 공용 네트워크들(예를 들어, 인터넷)을 통하거나 또는 사설 네트워크들을 통할 수 있다. 다양한 통신 프로토콜들이 이러한 통신들을 위해 사용될 수 있다.

[0115] 예를 들어, 컴퓨팅 인스턴스(C1)는 VCN(604) 외부의 엔드포인트와 통신하기를 원할 수 있다. 패킷은 먼저 소스 컴퓨팅 인스턴스(C1)와 연관된 VNIC에 의해 프로세싱될 수 있다. VNIC 프로세싱은, 패킷에 대한 목적지가 C1의 서브넷-1 외부에 있다는 것을 결정한다. C1과 연관된 VNIC는 패킷을 VCN(604)에 대한 VCN VR(605)로 포워딩할 수 있다. 그런 다음, VCN VR(605)은 패킷을 프로세싱하며, 프로세싱의 부분으로서, 패킷에 대한 목적지에 기초하여, 패킷에 대한 다음 홉으로서 VCN(604)과 연관된 특정 게이트웨이를 결정한다. 그런 다음, VCN VR(605)는 패킷을 특정 식별된 게이트웨이로 포워딩할 수 있다. 예를 들어, 목적지가 고객의 사내 네트워크 내의 엔드포인트인 경우, 패킷은 VCN(604)에 대해 구성된 동적 라우팅 게이트웨이(Dynamic Routing Gateway; DRG) 게이트웨이(622)로 VCN VR(605)에 의해 포워딩될 수 있다. 그런 다음, 패킷은 그 최종 의도된 목적지로의 패킷의 통신을 가능하게 하기 위해 게이트웨이로부터 다음 홉으로 포워딩될 수 있다.

[0116] 다양하고 상이한 유형들의 게이트웨이들은 VCN에 대해 구성될 수 있다. VCN에 대해 구성될 수 있는 게이트웨이들의 예들이 도 6에 도시되며 이하에서 설명된다. VCN과 연관된 게이트웨이들의 예들은 또한 도 11, 도 12, 도 13, 및 도 14(예를 들어, 참조 번호들 1134, 1136, 1138, 1234, 1236, 1238, 1334, 1336, 1338, 1434, 1436, 및 1438에 의해 참조되는 게이트웨이들)에 도시되며 이하에서 설명된다. 도 6에 도시된 실시예에 도시된 바와 같이, 동적 라우팅 게이트웨이(Dynamic Routing Gateway; DRG)(622)는 고객 VCN(604)에 추가되거나 또는 이와 연관될 수 있으며, 고객 VCN(604)과 다른 엔드포인트 사이의 사설 네트워크 트래픽 통신을 위한 경로를 제공하고, 여기서 다른 엔드포인트는 고객의 사내 네트워크(616), CSPI(601)의 상이한 지역 내의 VCN(608), 또는 CSPI(601)에 의해 호스팅되지 않는 다른 원격 클라우드 네트워크들(618)일 수 있다. 고객 사내 네트워크(616)는 고객의 자원들을 사용하여 구축된 고객 네트워크 또는 고객 데이터 센터일 수 있다. 고객 사내 네트워크(616)에 대한 액세스는 일반적으로 매우 제한된다. 고객 사내 네트워크(616) 및 CSPI(601)에 의해 클라우드에 배포되거나 또는 호스팅되는 하나 이상의 VCN들(604) 둘 모두를 갖는 고객에 대해, 고객은 그들의 사내 네트워크(616)와 그들의 클라우드-기반 VCN(604)이 서로 통신할 수 있는 것을 원할 수 있다. 이는, 고객이 CSPI(601)에 의해 호스팅되는 고객의 VCN(604) 및 그들의 사내 네트워크(616)를 포괄하는 확장된 하이브리드 환경을 구축하는 것을 가능하게 한다. DRG(622)는 이러한 통신을 가능하게 한다. 이러한 통신들을 가능하게 하기 위해, 통신 채널(624)이 셋업되며, 여기서 채널의 하나의 엔드포인트는 고객의 사내 네트워크(616) 내에 있고 다른 엔드포인트는 CSPI(601) 내에 있으며 고객 VCN(604)에 연결된다. 통신 채널(624)은 인터넷과 같은 공용 통신 네트워크를 통하거나 또는 사설 통신 네트워크들을 통할 수 있다. 인터넷과 같은 공용 통신 네트워크통한 IPsec VPN 기술, 공용 네트워크 대신에 사설 네트워크를 사용하는 오라클의 FastConnect 기술, 및 다른 것들과 같은 다양하고 상이한 프로토콜들이 사용될 수 있다. 통신 채널(624)에 대한 하나의 엔드 포인트를 형성하는 고객 사내 네트워크(616) 내의 디바이스 또는 장비는 도 6에 도시된 CPE(626)와 같은 고객 사내 장비(customer premise equipment; CPE)로 지칭된다. CSPI(601) 측 상에서, 엔드포인트는 DRG(622)를 실행하는 호스트 머신일 수 있다.

[0117] 특정 실시예들에서, 원격 피어링 연결(Remote Peering Connection; RPC)이 DRG에 추가될 수 있으며, 이는 고객이 하나의 VCN을 상이한 지역 내의 다른 VCN과 피어링하는 것을 가능하게 한다. 이러한 RPC를 사용하면, 고객 VCN(604)은 다른 지역 내의 VCN(608)과 연결하기 위해 DRG(622)를 사용할 수 있다. DRG(622)는 또한, 마이크로소프트 Azure 클라우드, 아마존 AWS 클라우드, 및 다른 것들과 같은 CSPI(601)에 의해 호스팅되지 않는 다른 원격 클라우드 네트워크들(618)과 통신하기 위해 사용될 수 있다.

[0118] 도 6에 도시된 바와 같이, 인터넷 게이트웨이(Internet Gateway; IGW)(620)는, VCN(604) 상의 컴퓨팅 인스턴스가 인터넷과 같은 공용 네트워크를 통해 액세스가능한 공용 엔드포인트들(614)과 통신하는 것을 가능하게 하는 고객 VCN(604)에 대해 구성될 수 있다. IGW(620)는, VCN을 인터넷과 같은 공용 네트워크에 연결하는 게이트웨이이다. IGW(620)는 VCN(604)와 같은 VCN 내의 공용 서브넷(여기서 공용 서브넷 내의 자원들은 공인 오버레이 IP 어드레스들을 가짐)이 인터넷과 같은 공용 네트워크(614) 상의 공용 엔드포인트들(612)에 직접 액세스하는 것을 가능하게 한다. IGW(620)를 사용하면, 연결들은 VCN(604) 내의 서브넷으로부터 또는 인터넷으로부터 개시될 수 있다.

[0119] 네트워크 어드레스 변환(Network Address Translation; NAT) 게이트웨이(628)는 고객의 VCN(604)에 대해 구성될 수 있으며, 전용 공인 오버레이 IP 어드레스를 갖지 않는 고객의 VCN 내의 클라우드 자원들이 인터넷에 액세스하는 것을 가능하게 하고, 이는, 이러한 자원들을 직접 인커밍 인터넷 연결들(예를 들어, L4-L7 연결들)에 노출하지 않고 그렇게 한다. 이는 인터넷 상의 공용 엔드포인트들에 대한 사설 액세스를 갖는 VCN(604) 내의 사설 서브넷-1과 같은 VCN 내의 사설 서브넷을 가능하게 한다. NAT 게이트웨이들에서, 연결들은 인터넷으로부터 사설 서브넷으로가 아니라 사설 서브넷으로부터 공용 인터넷으로만 개시될 수 있다.

[0120] 특정 실시예들에서, 서비스 게이트웨이(Service Gateway; SGW)(626)는 고객 VCN(604)에 대해 구성될 수 있으며, 서비스 네트워크(610) 내의 지원되는 서비스 엔드포인트들과 VCN(604) 사이의 사설 네트워크 트래픽에 대한 경로를 제공한다. 특정 실시예들에서, 서비스 네트워크(610)는 CSP에 의해 제공될 수 있으며 다양한 서비스들을 제공할 수 있다. 이러한 서비스 네트워크의 일 예는 오라클의 Services Network이며, 이는 고객들에 의해 사용될 수 있는 다양한 서비스들을 제공한다. 예를 들어, 고객 VCN(604)의 사설 서브넷 내의 컴퓨팅 인스턴스(예를 들어, 데이터베이스 시스템)는 공인 IP 어드레스들을 필요로 하지 않고 또는 인터넷에 액세스하지 않고 서비스 엔드포인트(예를 들어, 객체 스토리지)에 데이터를 백업할 수 있다. 특정 실시예들에서, VCN는 하나의 SGW만을 가질 수 있으며, 연결들은 서비스 네트워크(610)로부터가 아니라 오직 VCN 내의 서브넷으로부터만 개시될 수 있다. VCN가 다른 것과 피어링되는 경우, 다른 VCN 내의 자원들은 전형적으로 SGW에 액세스할 수 없다. FastConnect 또는 VPN 연결로 VCN에 연결된 사내 네트워크들 내의 자원들은 또한 해당 VCN에 대해 구성된 서비스 게이트웨이를 사용할 수 있다.

[0121] 특정 구현예들에서, SGW(626)는 서비스 클래스리스 인터-도메인 라우팅(Classless Inter-Domain Routing; CIDR) 라벨의 개념을 사용하며, 이는, 관심이 있는 서비스 또는 서비스들의 그룹에 대한 모든 지역적인 공인 IP 어드레스 범위를 나타내는 스트링이다. 고객은, 고객이 서비스에 대한 트래픽을 제어하기 위해 SGW 및 관련된 라우팅 규칙들을 구성할 때 서비스 CIDR 라벨을 사용한다. 고객은 선택적으로, 서비스의 공인 IP 어드레스들이 향후 변경되는 경우 이들을 조정할 필요 없이 보안 규칙들을 구성할 때 이를 사용할 수 있다.

[0122] 로컬 피어링 게이트웨이(Local Peering Gateway; LPG)(632)는, 고객 VCN(604)에 추가될 수 있으며 VCN(604)이 동일한 지역 내의 다른 VCN과 피어링하는 것을 가능하게 하는 게이트웨이이다. 피어링은, VCN들이, 트래픽이 인터넷과 같은 공용 네트워크를 통과(traverse)하지 않고 또는 고객의 사내 네트워크(616)를 통해 트래픽을 라우팅하지 않고 사설 IP 어드레스들을 사용하여 통신한다는 것을 의미한다. 선호되는 실시예들에서, VCN은 VCN이 설정한 각각의 피어링에 대해 별도의 LPG를 갖는다. 로컬 피어링 또는 VCN 피어링은 상이한 애플리케이션들 또는 인프라스트럭처 관리 기능들 사이에 네트워크 연결성을 설정하기 위해 사용되는 일반적인 관행이다.

[0123] 서비스 네트워크(610) 내의 서비스들의 제공자들과 같은 서비스 제공자들은 상이한 액세스 모델들을 사용하여 서비스들에 대한 액세스를 제공할 수 있다. 공용 액세스 모델에 따르면, 서비스들은 인터넷과 같은 공용 네트워크를 통해 고객 VCN 내의 컴퓨팅 인스턴스에 의해 공개적으로 액세스가능한 공용 엔드포인트들로서 노출될 수 있거나 또는 SGW(626)에 의해 사적으로(privately) 액세스가능할 수 있다. 특정 사설 액세스 모델에 따르면, 서비스들은 고객의 VCN 내의 사설 서브넷 내의 사설 IP 엔드포인트들로서 액세스가능하게 만들어진다. 이는 사설 엔드포인트(Private Endpoint; PE) 액세스로 지칭되며, 서비스 제공자가 그들의 서비스를 고객의 사설 네트워크 내의 인스턴스로서 노출하는 것을 가능하게 한다. 사설 엔드포인트 자원은 고객의 VCN 내의 서비스를 나타낸다. 각각의 PE는 고객의 VCN에서 고객에 의해 선택된 서브넷 내의 VNIC(하나 이상의 사설 IP들을 갖는, PE-VNIC로 지칭됨)로서 매니페스트(manifest)된다. 따라서, PE는 VNIC를 사용하여 사설 고객 VCN 서브넷 내에서 서비스를 제공하기 위한 방법을 제공한다. 엔드포인트가 VNIC로서 노출되기 때문에, 라우팅 규칙들, 보안 리스트들, 등과 같은 VNIC와 연관된 모든 특징들은 이제 PE VNIC에 대해 이용가능하다.

[0124] 서비스 제공자는 PE를 통한 액세스를 가능하게 하기 위해 그들의 서비스를 등록할 수 있다. 제공자는, 고객의 테넌시들에 대한 서비스들의 가시성을 제한하는 정책들을 서비스와 연관시킬 수 있다. 제공자는, 특히 다중-테넌트 서비스들에 대해, 단일 가상 IP 어드레스(virtual IP address; VIP) 하에서 다수의 서비스들을 등록할 수 있다. 동일한 서비스를 나타내는 (다수의 VCN들 내의) 다수의 이러한 사설 엔드포인트들이 있을 수 있다.

[0125] 그러면, 사설 서브넷 내의 컴퓨팅 인스턴스들은 서비스에 액세스하기 위해 PE VNIC의 사설 IP 어드레스 또는 서비스 DNS 명칭을 사용할 수 있다. 고객 VCN 내의 컴퓨팅 인스턴스들은 고객 VCN 내의 PE의 사설 IP 어드레스로 트래픽을 전송함으로써 서비스에 액세스할 수 있다. 사설 액세스 게이트웨이(Private Access Gateway; PAGW)(630)는, 고객 서브넷 사설 엔드포인트들로부터의/이로의 모든 트래픽에 대한 진입/진출 포인트로서 역할하는 서비스 제공자 VCN(예를 들어, 서비스 네트워크(610) 내의 VCN)에 접속될 수 있는 게이트웨이 자원이다.

PAGW(630)는 제공자가 그 내부 IP 어드레스 자원들을 사용하지 않고 PE 연결들의 수를 스케일링하는 것을 가능하게 한다. 제공자는 단일 VCN에 등록된 임의의 수의 서비스들에 대해 하나의 PAGW만을 구성하면 된다. 제공자들은 1명 이상의 고객들의 다수의 VCN들 내의 사설 엔드포인트로서 서비스를 표현할 수 있다. 고객의 관점으로부터, PE VNIC는, 고객의 인스턴트에 접속되는 대신에, 고객이 상호작용하기를 희망하는 서비스에 접속되는 것을 나타난다. 사설 엔드포인트로 향하는 트래픽은 PAGW(630)를 통해 서비스로 라우팅된다. 이들은 고객-대-서비스 사설 연결들(C2S(customer-to-service) 연결들)로 지칭된다.

[0126] PE 개념은 또한, 트래픽이 FastConnect/IPsec 링크들 및 고객 VCN 내의 사설 엔드포인트를 통해 흐르는 것을 가능하게 함으로써 서비스에 대한 액세스를 고객의 사내 네트워크들 및 데이터 센터들로 확장하기 위해 사용될 수 있다. 서비스에 대한 사설 액세스는 또한, 트래픽이 고객의 VCN 내의 PE와 LPG(632) 사이에서 흐르는 것을 가능하게 함으로써 고객의 피어링된 VCN들로 확장될 수 있다.

[0127] 고객은 서브넷 레벨로 VCN에서의 라우팅을 제어할 수 있으며, 따라서 고객은 VCN(604)과 같은 고객의 VCN에서 어떤 서브넷들이 각각의 게이트웨이를 사용할지를 지정할 수 있다. VCN의 루트 테이블들은, 특정 게이트웨이를 통해 VCN 밖으로 향하는 트래픽이 허용되는지 여부를 결정하기 위해 사용된다. 예를 들어, 특정 경우에서, 고객 VCN(604) 내의 공용 서브넷에 대한 루트 테이블은 IGW(620)를 통해 비-로컬 트래픽을 전송할 수 있다. 동일한 고객 VCN(604) 내의 사설 서브넷에 대한 루트 테이블은 SGW(626)을 통해 CSP 서비스들로 향하는 트래픽을 전송할 수 있다. 모든 남아 있는 트래픽은 NAT 게이트웨이(628)를 통해 전송될 수 있다. 루트 테이블들은 VCN 밖으로 나가는 트래픽만을 제어한다.

[0128] VCN과 연관된 보안 리스트들은 인바운드(inbound) 연결들을 통해서 게이트웨이를 통해 VCN 내로 들어오는 트래픽을 제어하기 위해 사용된다. 서브넷 내의 모든 자원들은 동일한 루트 테이블 및 보안 리스트들을 사용한다. 보안 리스트들은 VCN의 서브넷 내의 인스턴스들 안팎으로 허용된 특정 유형들의 트래픽을 제어하기 위해 사용될 수 있다. 보안 리스트 규칙들은 진입(인바운드) 및 진출(아웃바운드) 규칙들을 포함할 수 있다. 예를 들어, 진입 규칙은 허용된 소스 어드레스 범위를 지정할 수 있으며, 반면 진출 규칙은 허용된 목적지 어드레스 범위를 지정할 수 있다. 보안 규칙들은 특정 프로토콜(예를 들어, TCP, ICMP), 특정 포트(예를 들어, SSH에 대해 22, 윈도우즈 RDP에 대해 3389), 등을 지정할 수 있다. 특정 구현예들에서, 인스턴스의 운영 체제는, 보안 리스트 규칙들과 정렬된 그 자체의 방화벽 규칙들을 시행할 수 있다. 규칙들은 스테이트풀(예를 들어, 연결이 추적되며, 응답은 응답 트래픽에 대한 명시적인 보안 리스트 규칙 없이 자동으로 허용됨) 또는 스테이트리스일 수 있다.

[0129] 고객 VCN으로부터의 액세스(즉, VCN(604) 상에 배포된 자원 또는 컴퓨팅 인스턴스에 의한 액세스)는 공용 액세스, 사설 액세스, 또는 전용 액세스로 분류될 수 있다. 공용 액세스는, 공인 IP 어드레스 또는 NAT가 공용 엔드포인트에 액세스하기 위해 사용되는 액세스 모델을 의미한다. 사설 액세스는 사설 IP 어드레스들을 갖는 VCN(604) 내의 고객 워크로드들(예를 들어, 사설 서브넷 내의 자원들)이 인터넷과 같은 공용 네트워크를 통과하지 않고 서비스들에 액세스하는 것을 가능하게 한다. 특정 실시예들에서, CSPI(601)는 사설 IP 어드레스들을 갖는 고객 VCN 워크로드들이 서비스 게이트웨이를 사용하여 서비스들(이의 공용 서비스 엔드포인트들)에 액세스하는 것을 가능하게 한다. 따라서, 서비스 게이트웨이는, 고객의 VCN과 고객의 사설 네트워크 외부에 상주하는 서비스의 공용 엔드포인트 사이에 가상 링크를 설정함으로써 사설 액세스 모델을 제공한다.

[0130] 추가적으로, CSPI는 FastConnect 공용 피어링과 같은 기술들을 사용하여 전용 공용 액세스를 제공할 수 있으며, 여기서 고객 사내 인스턴스들은 인터넷과 같은 공용 네트워크를 통하지 않고 FastConnect 연결을 사용하여 고객 VCN 내의 하나 이상의 서비스들에 액세스할 수 있다. CSPI는 또한 FastConnect 사설 피어링을 사용하는 전용 사설 액세스를 제공할 수 있으며, 여기서 사설 IP 어드레스들을 갖는 고객 사내 인스턴스들은 FastConnect 연결을 사용하여 고객의 VCN 워크로드들에 액세스할 수 있다. FastConnect는 고객의 사내 네트워크를 CSPI 및 그 서비스들에 연결하기 위해 공용 인터넷을 사용하는 것에 대안적인 네트워크 연결성이다. FastConnect는, 인터넷-기반 연결들과 비교할 때 더 높은 대역폭 옵션들 및 더 신뢰할 수 있고 일관된 네트워킹 경험을 갖는 전용 사설 연결을 생성하기 위한 쉽고, 탄력적이며, 경제적인 방식을 제공한다.

[0131] 도 6 및 이상의 첨부된 설명은 예시적인 가상 네트워크 내의 다양한 가상화된 구성요소들을 설명한다. 이상에서 설명된 바와 같이, 가상 네트워크는 기초 물리적 또는 서브스트레이트 네트워크 상에 구축된다. 도 7은 특정 실시예들에 따른, CSPI(700) 내의 물리적 네트워크 내의 물리적 구성요소들의 단순화된 아키텍처 도면을 도시한다. 도시된 바와 같이, CSPI(700)는 클라우드 서비스 제공자(cloud service provider; CSP)에 의해 제공되는 구성요소들 및 자원들(예를 들어, 컴퓨팅, 메모리, 및 네트워킹 자원들)을 포함하는 분산형 환경을 제공한

다. 이러한 구성요소들 및 자원들은 가입 고객들, 즉, CSP에 의해 제공되는 하나 이상의 서비스들에 가입한 고객들에게 클라우드 서비스들(예를 들어, IaaS 서비스들)을 제공하기 위해 사용된다. 고객이 가입한 서비스들에 기초하여, CSPI(700)의 자원들(예를 들어, 컴퓨팅, 메모리, 및 네트워킹 자원들)의 서브세트가 고객에 대해 프로비저닝된다. 그러면, 고객들은 CSPI(700)에 의해 제공되는 컴퓨팅, 메모리, 및 네트워킹 자원들을 사용하여 그들 자체의 클라우드-기반(즉, CSPI-호스팅형) 맞춤화가능 사설 가상 네트워크들을 구축할 수 있다. 이상에서 표시된 바와 같이, 이러한 고객 네트워크들은 가상 클라우드 네트워크(virtual cloud network; VCN)들로 지칭된다. 고객은 이러한 고객 VCN들 상에 컴퓨팅 인스턴스들과 같은 하나 이상의 고객 자원들을 배포할 수 있다. 컴퓨팅 인스턴스들은 가상 머신들, 베어 메탈 인스턴스들, 및 유사한 것의 형태일 수 있다. CSPI(700)는, 고객들이 고도로 이용가능한 호스팅되는 환경에서 광범위한 애플리케이션 및 서비스들을 구축하고 실행하는 것을 가능하게 하는 상보적인 클라우드 서비스들의 세트 및 인프라스트럭처를 제공한다.

[0132] 도 7에 도시된 예시적인 실시예에서, CSPI(700)의 물리적 구성요소들은 하나 이상의 물리적 호스트 머신들 또는 물리적 서버들(예를 들어, 702, 706, 708), 네트워크 가상화 디바이스(network virtualization device; NVD)들(예를 들어, 710, 712), 탑-오브-랙(top-of-rack; TOR) 스위치들(예를 들어, 714, 716), 및 물리적 네트워크(예를 들어, 718), 및 물리적 네트워크(718) 내의 스위치들을 포함한다. 물리적 호스트 머신들 또는 서버들은 VCN의 하나 이상의 서브넷들에 참여하는 다양한 컴퓨팅 인스턴스들을 호스팅하고 실행할 수 있다. 컴퓨팅 인스턴스들은 가상 머신 인스턴스들 및 베어 메탈 인스턴스들을 포함할 수 있다. 예를 들어, 도 6에 도시된 다양한 컴퓨팅 인스턴스들은 도 7에 도시된 물리적 호스트 머신들에 의해 호스팅될 수 있다. VCN 내의 가상 머신 컴퓨팅 인스턴스들은 하나의 호스트 머신에 의해 또는 다수의 상이한 호스트 머신들에 의해 실행될 수 있다. 물리적 호스트 머신들은 또한 가상 호스트 머신들, 컨테이너-기반 호스트들 또는 기능들, 및 유사한 것을 호스팅할 수 있다. 도 6에 도시된 VNIC들 및 VCN VR은 도 7에 도시된 NVD들에 의해 실행될 수 있다. 도 6에 도시된 게이트웨이들은 도 7에 도시된 호스트 머신에 의해 및/또는 NVD들에 의해 실행될 수 있다.

[0133] 호스트 머신들 또는 서버들은, 호스트 머신들 상에 가상화된 환경을 생성하고 인에이블하는 하이퍼바이저(가상 머신 모니터 또는 VMM으로 지칭됨)를 실행할 수 있다. 가상화 또는 가상화된 환경은 클라우드-기반 컴퓨팅을 가능하게 한다. 하나 이상의 컴퓨팅 인스턴스들은 호스트 머신 상의 하이퍼바이저에 의해 해당 호스트 머신 상에 생성되고, 실행되며, 관리될 수 있다. 호스트 머신 상의 하이퍼바이저는, 호스트 머신의 물리적 컴퓨팅 자원들(예를 들어, 컴퓨팅, 메모리, 및 네트워킹 자원들)이 호스트 머신에 의해 실행되는 다양한 컴퓨팅 인스턴스들 사이에 공유되는 것을 가능하게 한다.

[0134] 예를 들어, 도 7에 도시된 바와 같이, 호스트 머신들(702 및 708)은 각각 하이퍼바이저들(760 및 766)을 실행한다. 이러한 하이퍼바이저들은 소프트웨어, 펌웨어, 또는 하드웨어, 또는 이들의 조합들을 사용하여 구현될 수 있다. 전형적으로, 하이퍼바이저는 호스트 머신의 운영 체제(operating system; OS)의 상단 상에 위치하며 결과적으로 호스트 머신의 하드웨어 프로세서 상에서 실행되는 프로세스 또는 소프트웨어 계층이다. 하이퍼바이저는, 호스트 머신의 물리적 컴퓨팅 자원들(예를 들어, 프로세서들/코어들과 같은 프로세싱 자원들, 메모리 자원들, 네트워킹 자원들)이 호스트 머신에 의해 실행되는 다양한 가상 머신 컴퓨팅 인스턴스들 사이에 공유되는 것을 가능하게 함으로써 가상화된 환경을 제공한다. 예를 들어, 도 7에서, 하이퍼바이저(760)는 호스트 머신(702)의 OS의 상단 상에 위치할 수 있으며, 호스트 머신(702)의 컴퓨팅 자원들(예를 들어, 프로세싱, 메모리, 및 네트워킹 자원들)이 호스트 머신(702)에 의해 실행되는 컴퓨팅 인스턴스들(예를 들어, 가상 머신들) 사이에서 공유되는 것을 가능하게 한다. 가상 머신은 그 자체의 운영 체제(게스트 운영 체제로 지칭됨)를 가질 수 있으며, 이는 호스트 머신의 OS와 동일하거나 또는 상이할 수 있다. 호스트 머신에 의해 실행되는 가상 머신의 운영 체제는 동일한 호스트 머신에 의해 실행되는 다른 가상 머신의 운영 체제와 동일하거나 또는 상이할 수 있다. 따라서, 하이퍼바이저는 다수의 운영 체제가 호스트 머신의 동일한 컴퓨팅 자원들을 공유하면서 서로 나란히 실행되는 것을 가능하게 한다. 도 7에 도시된 호스트 머신들은 동일하거나 또는 상이한 유형들의 하이퍼바이저들을 가질 수 있다.

[0135] 컴퓨팅 인스턴스는 가상 머신 인스턴스 또는 베어 메탈 인스턴스일 수 있다. 도 7에서, 호스트 머신(702) 상의 컴퓨팅 인스턴스(768) 및 호스트 머신(708) 상의 컴퓨팅 인스턴스(774)는 가상 머신 인스턴스들의 예들이다. 호스트 머신(706)은 고객에게 제공되는 베어 메탈 인스턴스의 일 예이다.

[0136] 특정 경우들에서, 전체 호스트 머신이 단일 고객에게 프로비저닝될 수 있으며, 해당 호스트 머신에 의해 호스팅되는 하나 이상의 컴퓨팅 인스턴스들(가상 머신들 또는 베어 메탈 인스턴스) 모두는 해당되는 동일한 고객에 속한다. 다른 경우들에서, 호스트 머신은 다수의 고객들(즉, 다수의 테넌트들) 사이에서 공유될 수 있다. 이러한 다중-테넌시 시나리오에서, 호스트 머신은 상이한 고객들에 속하는 가상 머신 컴퓨팅 인스턴스들을 호스팅할 수

있다. 이러한 컴퓨팅 인스턴스들은 상이한 고객들의 상이한 VCN들이 멤버들일 수 있다. 특정 실시예들에서, 베어 메탈 컴퓨팅 인스턴스는 하이퍼바이저 없이 베어 메탈 서버에 의해 호스팅된다. 베어 메탈 컴퓨팅 인스턴스가 프로비저닝될 때, 단일 고객 또는 테넌트는 베어 메탈 인스턴스를 호스팅하는 호스트 머신의 물리적 CPU, 메모리, 및 네트워크 인터페이스들의 제어를 유지하며, 호스트 머신은 다른 고객들 또는 테넌트들과 공유되지 않는다.

[0137] 이상에서 설명된 바와 같이, VCN의 부분인 각각의 컴퓨팅 인스턴스는, 컴퓨팅 인스턴스가 VCN의 서브넷의 멤버가 되는 것을 가능하게 하는 VNIC와 연관된다. 컴퓨팅 인스턴스와 연관된 VNIC는 컴퓨팅 인스턴스로의 그리고 이로부터의 패킷들 또는 프레임들의 통신을 가능하게 한다. VNIC, 컴퓨팅 인스턴스가 생성될 때 컴퓨팅 인스턴스와 연관된다. 특정 실시예들에서, 호스트 머신에 의해 실행되는 컴퓨팅 인스턴스에 대해, 해당 컴퓨팅 인스턴스와 연관된 VNIC는 호스트 머신에 연결된 NVD에 의해 실행된다. 예를 들어, 도 7에서, 호스트 머신(702)은 VNIC(776)와 연관된 가상 머신 컴퓨팅 인스턴스(768)을 실행하며, VNIC(776)은 호스트 머신(702)에 연결된 NVD(710)에 의해 실행된다. 다른 예로서, 호스트 머신(706)에 의해 호스팅되는 베어 메탈 인스턴스(772)는, 호스트 머신(706)에 연결된 NVD(712)에 의해 실행되는 VNIC(780)와 연관된다. 또 다른 예로서, VNIC(784)는 호스트 머신(708)에 의해 실행되는 컴퓨팅 인스턴스(774)와 연관되며, VNIC(784)는 호스트 머신(708)에 연결된 NVD(712)에 의해 실행된다.

[0138] 호스트 머신에 의해 호스팅되는 컴퓨팅 인스턴스들에 대해, 호스트 머신에 연결된 NVD는 또한 컴퓨팅 인스턴스들이 이의 멤버들인 VCN들에 대응하는 VCN VR들을 실행한다. 예를 들어, 도 7에 도시된 실시예에서, NVD(710)는 컴퓨팅 인스턴스(768)가 이의 멤버인 VCN에 대응하는 VCN VR(777)을 실행한다. NVD(712)는 또한 호스트 머신들(706 및 708)에 의해 호스팅되는 컴퓨팅 인스턴스들에 대응하는 VCN들에 대응하는 하나 이상의 VCN VR들(783)을 실행할 수 있다.

[0139] 호스트 머신은, 호스트 머신이 다른 디바이스들에 연결되는 것을 가능하게 하는 하나 이상의 네트워크 인터페이스 카드(network interface card; NIC)들을 포함할 수 있다. 호스트 머신 상의 NIC는, 호스트 머신이 다른 디바이스에 통신가능하게 연결되는 것을 가능하게 하는 하나 이상의 포트들(또는 인터페이스들)을 제공할 수 있다. 예를 들어, 호스트 머신은 호스트 머신 상에 그리고 NVD 상에 제공된 하나 이상의 포트들(또는 인터페이스들)을 사용하여 NVD에 연결될 수 있다. 호스트 머신은 또한 다른 호스트 머신과 같은 다른 디바이스들에 연결될 수 있다.

[0140] 예를 들어, 도 7에서, 호스트 머신(702)은, 호스트 머신(702)의 NIC(732)에 의해 제공된 포트(734) 사이에서 그리고 NVD(710)의 포트(736) 사이에 연장되는 링크(720)를 사용하여 NVD(710)에 연결된다. 호스트 머신(706)은, 호스트 머신(706)의 NIC(744)에 의해 제공된 포트(746) 사이에서 그리고 NVD(712)의 포트(748) 사이에 연장되는 링크(724)를 사용하여 NVD(712)에 연결된다. 호스트 머신(708)은, 호스트 머신(708)의 NIC(750)에 의해 제공된 포트(752) 사이에서 그리고 NVD(712)의 포트(754) 사이에 연장되는 링크(726)를 사용하여 NVD(712)에 연결된다.

[0141] NVD들은 결과적으로 통신 링크들을 통해 탑-오브-랙(top-of-the-rack; TOR) 스위치들에 연결되며, 이들은 물리적 네트워크(718)(스위치 패브릭(switch fabric)으로도 지칭됨)에 연결된다. 특정 실시예들에서, 호스트 머신과 NVD 사이의 그리고 NVD와 TOR 스위치 사이의 링크들은 이더넷 링크들이다. 예를 들어, 도 7에서, NVD들(710 및 712)은 각각 링크들(728 및 730)을 사용하여 1126 TOR 스위치들(714 및 716)에 연결된다. 특정 실시예들에서, 링크들(720, 724, 726, 728, 및 730)은 이더넷 링크들이다. TOR에 연결된 NVD들 및 호스트 머신들의 모음은 때때로 랙(rack)으로 지칭된다.

[0142] 물리적 네트워크(718)는, TOR 스위치들이 서로 통신하는 것을 가능하게 하는 통신 패브릭을 제공한다. 물리적 네트워크(718)는 다중-계층형 네트워크일 수 있다. 특정 구현예들에서, 물리적 네트워크(718)는 스위치들의 다중-계층형 클로스 네트워크(Clos network)이며, 여기서 TOR 스위치들(714 및 716)은 다중-계층형 및 다중-노드 물리적 스위칭 네트워크(718)의 리프(leaf) 레벨 노드들을 나타낸다. 비제한적으로 2-계층 네트워크, 3-계층 네트워크, 4-계층 네트워크, 5-계층 네트워크, 및 일반적으로 "n"-계층 네트워크를 포함하여 상이한 클로스 네트워크 구성들이 가능하다. 클로스 네트워크의 일 예가 도 10에 도시되고 이하에서 설명된다.

[0143] 1-대-1 구성, 다-대-1 구성, 1-대-다 구성, 및 다른 것들과 같은 다양하고 상이한 연결 구성들이 호스트 머신들과 NVD들 사이에서 가능하다. 1-대-1 구성 구현예에서, 각각의 호스트 머신은 그 자체의 별도의 NVD에 연결된다. 예를 들어, 도 7에서, 호스트 머신(702)은 호스트 머신(702)의 NIC(732)를 통해 NVD(710)에 연결된다. 다-대-1 구성에서, 다수의 호스트 머신들은 하나의 NVD에 연결된다. 예를 들어, 도 7에서, 호스트 머신들(706 및 708)은 각각 NIC들(744 및 750)을 통해 동일한 NVD(712)에 연결된다.

[0144] 1-대-다 구성에서, 하나의 호스트 머신은 다수의 NVD들에 연결된다. 도 8은, 호스트 머신이 다수의 NVD들에 연결되는 CSPI(800) 내의 일 예를 도시한다. 도 8에 도시된 바와 같이, 호스트 머신(802)은 다수의 포트들(806 및 808)을 포함하는 네트워크 인터페이스 카드(network interface card; NIC)(804)를 포함한다. 호스트 머신(800)은 포트(806) 및 링크(820)를 통해 제1 NVD(810)에 연결되고, 포트(808) 및 링크(822)를 통해 제2 NVD(812)에 연결된다. 포트들(806 및 808)은 이더넷 포트들이며, 호스트 머신(802)과 NVD들(810 및 812) 사이의 링크들(820 및 822)은 이더넷 링크들일 수 있다. NVD(810)는 결과적으로 제1 TOR 스위치(814)에 연결되고, NVD(812)는 제2 TOR 스위치(816)에 연결된다. NVD들(810 및 812)과 TOR 스위치들(814 및 816) 사이의 링크들은 이더넷 링크들일 수 있다. TOR 스위치들(814 및 816)은 다중-계층형 물리적 네트워크(818) 내의 계층-0 스위칭 디바이스들을 나타낸다.

[0145] 도 8에 도시된 배열은 물리적 스위치 네트워크(818)로부터 그리고 이로의 호스트 머신(802)으로의 그리고 이로부터의 2개의 별도의 물리적 네트워크 경로들을 제공한다: TOR 스위치(814)를 통과하여 NVD(810)를 지나 호스트 머신(802)으로의 제1 경로 및 TOR 스위치(816)를 통과하여 NVD(812)를 지나 호스트 머신(802)으로의 제2 경로. 별도의 경로들은 호스트 머신(802)의 향상된 가용성(고 가용성으로 지칭됨)을 위해 제공된다. 경로들 중 하나에 문제가 있는 경우(예를 들어, 경로들 중 하나의 경로의 링크가 다운된 경우) 또는 디바이스들 중 하나에 문제가 있는 경우(예를 들어, 특정 NVD가 기능하지 않는 경우), 다른 경로가 호스트 머신(802)으로의/으로부터의 통신들을 위해 사용될 수 있다.

[0146] 도 8에 도시된 구성에서, 호스트 머신은 호스트 머신의 NIC에 의해 제공된 2개의 상한 포트들을 사용하여 2개의 상이한 NVD들에 연결된다. 다른 실시예들에서, 호스트 머신은, 다수의 NVD들에 대한 호스트 머신의 연결성을 가능하게 하기 위해 다수의 NIC들을 포함할 수 있다.

[0147] 다시 도 7을 참조하면, NVD는, 하나 이상의 네트워크 및/또는 스토리지 가상화 기능들을 수행하는 물리적 디바이스 또는 구성요소이다. NVD는 하나 이상의 프로세싱 유닛들(예를 들어, CPU들, 네트워크 프로세싱 유닛(Network Processing Unit; NPU)들, FPGA들, 패킷 프로세싱 파이프라인들, 등), 캐시를 포함하는 메모리, 및 포트들을 갖는 임의의 디바이스일 수 있다. 다양한 가상화 기능들은 NVD의 하나 이상의 프로세싱 유닛들에 의해 실행되는 소프트웨어/펌웨어에 의해 수행될 수 있다.

[0148] NVD는 다양하고 상이한 형태들로 구현될 수 있다. 예를 들어, 특정 실시예들에서, NVD는 내장형 프로세서 온보드를 갖는 지능형 NIC 또는 smartNIC로 지칭되는 인터페이스 카드로서 구현된다. smartNIC는 호스트 머신들 상의 NIC들과는 별도의 디바이스이다. 도 7에서, NVD들(710 및 712)은 각각, 호스트 머신들(702), 및 호스트 머신들(706 및 708)에 연결된 smartNIC들로서 구현될 수 있다.

[0149] 그러나, smartNIC는 단지 NVD 구현의 일 예일 뿐이다. 다른 구현예들이 가능하다. 예를 들어, 일부 다른 구현예들에서, NVD 또는 NVD에 의해 수행되는 하나 이상의 기능들은 하나 이상의 호스트 머신들, 하나 이상의 TOR 스위치들, 및 CSPI(700)에 통합되거나 또는 이들에 의해 수행될 수 있다. 예를 들어, NVD는 호스트 머신에 구현될 수 있으며, 여기서 NVD에 의해 수행되는 기능들은 호스트 머신에 의해 수행된다. 다른 예로서, NVD는 TOR 스위치의 부분일 수 있거나, 또는 TOR 스위치는, TOR 스위치가 공용 클라우드에 대해 사용되는 다양하고 복잡한 패킷 변환(transformation)들을 수행하는 것을 가능하게 하는 NVD에 의해 수행되는 기능들을 수행하도록 구성될 수 있다. NVD의 기능들을 수행하는 TOR은 때때로 스마트 TOR로 지칭된다. 베어 메탈(bare metal; BM) 인스턴스들이 아니라 가상 머신(virtual machine; VM) 인스턴스들이 고객들에게 제공되는 또 다른 구현예들에서, NVD에 의해 수행되는 기능들은 호스트 머신의 하이퍼바이저 내부에 구현될 수 있다. 일부 다른 구현예들에서, NVD의 기능들 중 일부는 호스트 머신들의 플리트 상에서 실행 중인 중앙 집중식 서비스로 오프로딩될 수 있다.

[0150] 특정 실시예들에서, 예컨대 도 7에 도시된 바와 같은 smartNIC로서 구현될 때, NVD는, NVD가 하나 이상의 호스트 머신들에 그리고 하나 이상의 TOR 스위치들에 연결되는 것을 가능하게 하는 다수의 물리적 포트들을 포함할 수 있다. NVD 상의 포트는 호스트-방향(host-facing) 포트("사우스 포트(south port)"로도 지칭됨) 또는 네트워크-방향 또는 TOR-방향 포트("노스 포트(north port)"로도 지칭됨)로서 분류될 수 있다. NVD의 호스트-방향 포트는 NVD를 호스트 머신에 연결하기 위해 사용되는 포트이다. 도 7의 호스트-방향 포트들의 예들은 NVD(710) 상의 포트(736), 및 NVD(712) 상의 포트들(748 및 754)을 포함한다. NVD의 네트워크-방향 포트는 NVD를 TOR 스위치에 연결하기 위해 사용되는 포트이다. 도 7의 네트워크-방향 포트들의 예들은 NVD(710) 상의 포트(756), 및 NVD(712) 상의 포트(758)를 포함한다. 도 7에 도시된 바와 같이, NVD(710)는, NVD(710)의 포트(756)로부터 TOR 스위치(714)까지 연장되는 링크(728)를 사용하여 TOR 스위치(714)에 연결된다. 마찬가지로, NVD(712)는, NVD(712)의 포트(758)로부터 TOR 스위치(716)까지 연장되는 링크(730)를 사용하여 TOR 스위치(716)에 연결된다.

[0151] NVD는 호스트-방향 포트를 통해 호스트 머신으로부터 프레임들 및 패킷들(예를 들어, 호스트 머신에 의해 호스팅되는 컴퓨팅 인스턴스에 의해 생성된 패킷들 및 프레임들)을 수신하며, 필수 패킷 프로세싱을 수행한 이후에, 패킷들 및 프레임들을 NVD의 네트워크-방향 포트를 통해 TOR 스위치로 포워딩할 수 있다. NVD는 NVD의 네트워크-방향 포트를 통해 TOR 스위치로부터 패킷들 및 프레임들을 수신할 수 있으며, 필수 패킷 프로세싱을 수행한 이후에, 패킷들 및 프레임들을 NVD의 호스트-방향 포트를 통해 호스트 머신으로 포워딩할 수 있다.

[0152] 특정 실시예들에서, NVD와 TOR 스위치 사이에 다수의 포트들 및 연관된 링크들이 있을 수 있다. 이러한 포트들 및 링크들은 다수의 포트들 및 링크들의 링크 집성기 그룹(LAG(link aggregator group)로 지칭됨)을 형성하기 위해 집성(aggregate)될 수 있다. 링크 집성은, 2개의 엔드-포인트들 사이의(예를 들어, NVD와 TOR 스위치 사이의) 다수의 물리적 링크들이 단일 논리적 링크로서 취급되는 것을 가능하게 한다. 주어진 LAG 내의 모든 물리적 링크들은 동일한 속도로 풀-듀플렉스(full-duplex) 모드로 동작할 수 있다. LAG들은 2개의 엔드포인트들 사이의 연결의 대역폭 및 신뢰성을 증가시키는 것을 돕는다. LAG 내의 물리적 링크들 중 하나가 다운되는 경우, 트래픽은 LAG 내의 다른 물리적 링크들 중 하나로 동적으로 그리고 투명하게 재할당된다. 집성된 물리적 링크들을 각각의 개별적인 링크보다 더 높은 대역폭을 공급한다. LAG와 연관된 다수의 포트들은 단일 논리적 포트로서 취급된다. 트래픽은 LAG의 다수의 물리적 링크들에 걸쳐 로드-밸런싱될 수 있다. 하나 이상의 LAG들이 2개의 엔드포인트들 사이에 구성될 수 있다. 2개의 엔드포인트들은 NVD와 TOR 스위치 사이에, 호스트 머신과 NVD 사이에 있는 등일 수 있다.

[0153] NVD는 네트워크 가성화 기능들을 구현하거나 또는 수행한다. 이러한 기능들은 NVD에 의해 실행되는 소프트웨어/펌웨어에 의해 수행된다. 네트워크 가상화 기능들의 예들은 비제한적으로 다음을 포함한다: 패킷 캡슐화 및 캡슐화-해제 기능들; VCN 네트워크를 생성하기 위한 기능들; VCN 보안 리스트 (방화벽) 기능성과 같은 네트워크 정책들을 구현하기 위한 기능들; VCN 내의 컴퓨팅 인스턴스들로 그리고 이로부터 패킷들을 라우팅하고 포워딩하는 것을 가능하게 하는 기능들; 및 유사한 것. 특정 실시예들에서, 패킷의 수신 시에, NVD는 패킷을 프로세싱하고 패킷이 포워딩되거나 또는 라우팅되는 방법을 결정하기 위해 패킷 프로세싱 파이프라인을 실행하도록 구성된다. 이러한 패킷 프로세싱 파이프라인의 부분으로서, NVD는, VCN 내의 컴퓨팅 인스턴스들과 연관된 VNIC들을 실행하는 것, VCN과 연관된 가상 라우터(Virtual Router; VR)를 실행하는 것, 가상 네트워크 내에서의 포워딩 또는 라우팅을 가능하게 하기 위한 패킷들의 캡슐화 및 캡슐화해제, 특정 게이트웨이들(예를 들어, 로컬 피어링 게이트웨이)의 실행, 보안 리스트들의 구현, 네트워크 보안 그룹들, 네트워크 어드레스 변환(NAT) 기능성(예를 들어, 공용 IP를 호스트 단위로 호스트 상의 사설 IP로 변환하는 것), 스로틀링 기능들, 및 다른 기능들과 같은 오버레이 네트워크와 연관된 하나 이상의 가상 기능들을 실행할 수 있다.

[0154] 특정 실시예들에서, NVD 내의 패킷 프로세싱 데이터 경로는 다수의 패킷 파이프라인들을 포함할 수 있으며, 각각의 패킷 파이프라인은 일련의 패킷 변환 스테이지들로 구성된다. 특정 구현예들에서, 패킷의 수신 시에, 패킷은 파싱(parse)되고 단일 파이프라인으로 분류된다. 그런 다음 패킷은, 패킷이 드롭되거나 또는 NVD의 인터페이스를 통해 전송될 때까지 선형적인 방식으로 한 스테이지씩 프로세싱된다. 이러한 스테이지들은, 새로운 파이프라인들이 기존 스테이지들을 조직(compose)함으로써 구성될 수 있고 새로운 기능성이 새로운 스테이지들을 생성하고 이들을 기존 파이프라인들에 삽입함으로써 추가될 수 있도록 기본 기능 패킷 프로세싱 구축 블록들(예를 들어, 헤더들의 검증, 스로틀의 시행, 새로운 계층-2 헤더들의 삽입, L4 방화벽의 시행, VCN 캡슐화/캡슐화해제, 등)을 제공한다.

[0155] NVD는 VCN의 제어 평면 및 데이터 평면에 대응하는 제어 평면 기능 및 데이터 평면 기능 둘 모두를 수행할 수 있다. VCN 제어 평면의 예들은 또한 도 11, 도 12, 도 13 및 도 14(참조 부호 1116, 1216, 1316, 및 1416 참조)에 도시되며 이하에서 설명된다. VCN 데이터 평면의 예들은 도 11, 도 12, 도 13 및 도 14(참조 부호 1118, 1218, 1318, 및 1418 참조)에 도시되며 이하에서 설명된다. 제어 평면 기능들은, 데이터가 포워딩될 방법을 제어하는 네트워크를 구성(예를 들어, 루트들 및 루트 테이블들을 셋업하는 것, VNIC들을 구성하는 것, 등)하기 위해 사용되는 기능들을 포함한다. 특정 실시예들에서, 오버레이-대-서브스트레이트 매핑들 모두를 중앙에서 컴퓨팅하고 이들을 NVD들에 그리고 DRG, SGW, IGW, 등과 같은 다양한 게이트웨이들과 같은 가상 네트워크 에지 디바이스들에 퍼블리싱하는 VCN 제어 패널이 제공된다. 방화벽 규칙들도 또한 동일한 메커니즘을 사용하여 퍼블리싱된다. 특정 실시예들에서, NVD는 해당 NVD와 관련된 매핑들만을 획득한다. 데이터 평면 기능들은, 제어 평면을 사용하여 셋업된 구성에 기초하여 패킷의 실제 라우팅/포워딩을 위한 기능들을 포함한다. VCN 데이터 평면은, 고객의 네트워크 패킷들이 서브스트레이트 네트워크를 통과하기 이전에 고객의 네트워크 패킷들을 캡슐화함으로써 구현된다. 캡슐화/캡슐화해제 기능성은 NVD들 상에 구현된다. 특정 실시예들에서, NVD는 호스트 머신들 안팎으로의 모든 네트워크 패킷들을 인터셉트하고 네트워크 가상화 기능들을 수행하도록 구성된다.

[0156] 이상에서 표시된 바와 같이, NVD는 VNIC들 및 VCN VR들을 포함하여 다양한 가상화 기능들을 실행한다. NVD는 VNIC에 연결된 하나 이상의 호스트 머신들에 의해 호스팅되는 컴퓨팅 인스턴스들과 연관된 VNIC들을 실행할 수 있다. 예를 들어, 도 7에 도시된 바와 같이, NVD(710)는, NVD(710)에 연결된 호스트 머신(702)에 의해 호스팅되는 컴퓨팅 인스턴스(768)와 연관된 VNIC(776)에 대한 기능성을 실행한다. 다른 예로서, NVD(712)는 호스팅 머신(706)에 의해 호스팅되는 베어 메탈 컴퓨팅 인스턴스(772)와 연관된 VNIC(780)를 실행하고, 호스트 머신(708)에 의해 호스팅되는 컴퓨팅 인스턴스(774)와 연관된 VNIC(784)를 실행한다. 호스트 머신은 상이한 고객들에 속한 상이한 VCN들에 속하는 컴퓨팅 인스턴스들을 호스팅할 수 있으며, 호스트 머신에 연결된 NVD는 컴퓨팅 인스턴스들에 대응하는 VNIC들 실행할 수 있다(즉, VNIC-관련 기능성을 실행할 수 있다).

[0157] NVD는 또한 컴퓨팅 인스턴스들의 VCN들에 대응하는 VCN 가상 라우터들을 실행한다. 예를 들어, 도 7에 도시된 실시예에서, NVD(710)는 컴퓨팅 인스턴스(768)가 속하는 VCN에 대응하는 VCN VR(777)을 실행한다. NVD(712)는 호스트 머신들(706 및 708)에 의해 호스팅되는 컴퓨팅 인스턴스들이 속하는 하나 이상의 VCN들에 대응하는 하나 이상의 VCN VR들(783)을 실행한다. 특정 실시예들에서, 해당 VCN에 대응하는 VCN VR은, 해당 VCN에 속하는 적어도 하나의 컴퓨팅 인스턴스를 호스팅하는 호스트 머신들에 연결된 NVD들 모두에 의해 실행된다. 호스트 머신이 상이한 VCN들에 속하는 컴퓨팅 인스턴스들을 호스팅하는 경우, 해당 호스트 머신에 연결된 NVD는 이러한 상이한 VCN들에 대응하는 VCN VR들을 실행할 수 있다.

[0158] VNIC들 및 VCN VR들에 추가하여, NVD는 소프트웨어(예를 들어, 데몬(daemon)들)을 실행할 수 있으며, NVD에 의해 수행되는 다양한 네트워크 가상화 기능들을 가능하게 하는 하나 이상의 하드웨어 구성요소들을 포함할 수 있다. 단순성의 목적들을 위해, 이러한 다양한 구성요소들은 도 7에 도시된 "패킷 프로세싱 구성요소들"로서 함께 그룹화된다. 예를 들어, NVD(710)는 패킷 프로세싱 구성요소들(786)을 포함하며, NVD(712)는 패킷 프로세싱 구성요소들(788)을 포함한다. 예를 들어, NVD에 대한 패킷 프로세싱 구성요소들은, NVD에 의해 수신되고 이를 사용하여 통신되는 모든 패킷들을 모니터링하고 네트워크 정보를 저장하기 위해 하드웨어 인터페이스들 및 NVD의 포트들과 상호작용하도록 구성된 패킷 프로세서를 포함할 수 있다. 네트워크 정보는, 예를 들어, NVD에 의해 핸들링되는 상이한 네트워크 흐름들을 식별하는 네트워크 흐름 정보 및 흐름별 정보(예를 들어, 흐름별 통계자료)를 포함할 수 있다. 특정 실시예들에서, 네트워크 흐름 정보는 VNIC별로 저장될 수 있다. 패킷 프로세서는 패킷별 조작들을 수행할 뿐만 아니라 스테이트풀 NAT 및 L4 방화벽(FW)을 구현할 수 있다. 다른 예로서, 패킷 프로세싱 구성요소들은, NVD에 의해 저장된 정보를 하나 이상의 상이한 복제 목표 스토어들에 복제하도록 구성된 복제 에이전트를 포함할 수 있다. 또 다른 예로서, 패킷 프로세싱 구성요소는, NVD에 대한 로깅 기능들을 수행하도록 구성된 로깅 에이전트를 포함할 수 있다. 패킷 프로세싱 구성요소들은 또한, NVD의 성능 및 헬스(health)를 모니터링하며 또한 어쩌면 NVD에 연결된 다른 구성요소들의 상태 및 헬스를 모니터링하기 위한 소프트웨어를 포함할 수 있다.

[0159] 도 6은, VCN, VCN 내의 서브넷들, 서브넷들 상에 배포된 컴퓨팅 인스턴스들, 컴퓨팅 인스턴스들과 연관된 VNIC들, VCN에 대한 VR, 및 VCN에 대해 구성된 게이트웨이들의 세트를 포함하는 예시적인 가상 또는 오버레이 네트워크의 구성요소들을 도시한다. 도 6에 도시된 오버레이 구성요소들은 도 7에 도시된 물리적 구성요소들 중 하나 이상에 의해 실행되거나 또는 호스팅될 수 있다. 예를 들어, VCN 내의 컴퓨팅 인스턴스들은 도 7에 도시된 하나 이상의 호스트 머신들에 의해 실행되거나 또는 호스팅될 수 있다. 호스트 머신에 의해 호스팅되는 컴퓨팅 인스턴스에 대해, 해당 컴퓨팅 인스턴스와 연관된 VNIC는 전형적으로 호스트 머신에 연결된 NVD에 의해 실행된다(즉, VNIC 기능성은 해당 호스트 머신에 연결된 NVD에 의해 제공된다). VCN에 대한 VCN VR은, 해당 VCN의 부분인 컴퓨팅 인스턴스를 호스팅하거나 또는 실행하는 호스트 머신들에 연결된 NVD들 모두에 의해 실행된다. VCN과 연관된 게이트웨이들은 하나 이상의 상이한 유형들의 NVD들에 의해 실행될 수 있다. 예를 들어, 특정 게이트웨이들은 smartNIC들에 의해 실행될 수 있으며, 반면 다른 것들은 NVD들의 다른 구현예들 또는 하나 이상의 호스트 머신들에 의해 실행될 수 있다.

[0160] 이상에서 설명된 바와 같이, 고객 VCN 내의 컴퓨팅 인스턴스는 다양하고 상이한 엔드포인트들(여기서, 엔드포인트들은 소스 컴퓨팅 인스턴스와 동일한 서브넷 내에 있을 수 있거나, 또는 소스 컴퓨팅 인스턴스와 동일한 VCN 내에 있지만 상이한 서브넷 내에 있을 수 있음)과 통신할 수 있거나, 또는 소스 컴퓨팅 인스턴스의 VCN 외부에 있는 엔드포인트와 통신할 수 있다. 이러한 통신들은 컴퓨팅 인스턴스들과 연관된 VNIC들, VCN VR들, 및 VCN들과 연관된 게이트웨이들을 사용하여 가능하게 된다.

[0161] VCN 내의 동일한 서브넷 상의 2개의 컴퓨팅 인스턴스들 사이의 통신들에 대해, 통신은 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스와 연관된 VNIC들을 사용하여 가능하게 된다. 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스는 동일한 호스트 머신에 의해 또는 상이한 호스트 머신들에 의해 호스팅될 수 있다. 소스 컴퓨팅 인스

턴스로부터 발원하는 패킷은 소스 컴퓨팅 인스턴스를 호스팅하는 호스트 머신으로부터 해당 호스트 머신에 연결된 NVD로 포워딩될 수 있다. NVD 상에서, 패킷은 패킷 프로세싱 파이프라인을 사용하여 프로세싱되며, 이는 소스 컴퓨팅 인스턴스와 연관된 VNIC의 실행을 포함할 수 있다. 패킷에 대한 목적지 엔드포인트가 동일한 서브넷 내에 있기 때문에, 소스 컴퓨팅 인스턴스와 연관된 VNIC의 실행은 패킷들이 목적지 컴퓨팅 인스턴스와 연관된 VNIC를 실행하는 NVD로 포워딩되는 결과를 가져오며, 이는 그 후에 패킷을 프로세싱하고 이를 목적지 컴퓨팅 인스턴스로 포워딩한다. 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스와 연관된 VNIC들은 동일한 NVD 상에서 실행될 수 있거나(예를 들어, 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스 둘 모두가 동일한 호스트 머신에 의해 호스팅될 때) 또는 상이한 NVD들 상에서 실행될 수 있다(예를 들어, 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스가 상이한 NVD들에 연결된 상이한 호스트 머신들에 의해 호스팅될 때). VNIC들은 패킷에 대한 다음 홉을 결정하기 위해 NVD에 의해 저장된 라우팅/포워딩 테이블들을 사용할 수 있다.

[0162] 서브넷 내의 컴퓨팅 인스턴스로부터 동일한 VCN 내의 상이한 서브넷 내의 엔드포인트로 통신될 패킷에 대해, 소스 컴퓨팅 인스턴스로부터 발원하는 패킷은 소스 컴퓨팅 인스턴스를 호스팅하는 호스팅 머신으로부터 해당 호스트 머신에 연결된 NVD로 통신된다. NVD 상에서, 패킷은 패킷 프로세싱 파이프라인을 사용하여 프로세싱되며, 이는 하나 이상의 VNIC들, 및 VCN과 연관된 VR의 실행을 포함할 수 있다. 예를 들어, 패킷 프로세싱 파이프라인의 부분으로서, NVD는 소스 컴퓨팅 인스턴스와 연관된 VNIC에 대응하는 기능성을 실행하거나 또는 호출(invoke)한다(VNIC를 실행하는 것으로도 지칭됨). VNIC에 의해 수행되는 기능성은 패킷 상의 VLAN 태그를 확인하는 것을 포함할 수 있다. 패킷의 목적지가 서브넷 외부에 있기 때문에, 다음으로 NVD에 의해 VCN VR 기능성이 호출되고 실행된다. 그런 다음, VCN VR은 패킷을 목적지 컴퓨팅 인스턴스와 연관된 VNIC를 실행하는 NVD로 라우팅한다. 그런 다음, 목적지 컴퓨팅 인스턴스와 연관된 VNIC가 패킷을 프로세싱하고 패킷을 목적지 컴퓨팅 인스턴스로 포워딩한다. 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스와 연관된 VNIC들은 동일한 NVD 상에서 실행될 수 있거나(예를 들어, 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스 둘 모두가 동일한 호스트 머신에 의해 호스팅될 때) 또는 상이한 NVD들 상에서 실행될 수 있다(예를 들어, 소스 컴퓨팅 인스턴스 및 목적지 컴퓨팅 인스턴스가 상이한 NVD들에 연결된 상이한 호스트 머신들에 의해 호스팅될 때).

[0163] 패킷에 대한 목적지가 소스 컴퓨팅 인스턴스의 VCN 외부에 있는 경우, 소스 컴퓨팅 인스턴스로부터 발원하는 패킷은 소스 컴퓨팅 인스턴스를 호스팅하는 호스팅 머신으로부터 해당 호스트 머신에 연결된 NVD로 통신된다. NVD는 소스 컴퓨팅 인스턴스와 연관된 VNIC를 실행한다. 패킷의 목적지 엔드 포인트가 VCN 외부에 있기 때문에, 그런 다음 패킷은 해당 VCN에 대한 VCN VR에 의해 프로세싱된다. NVD는 VCN VR 기능성을 호출하며, 이는 패킷이 VCN과 연관된 적절한 게이트웨이를 실행하는 NVD로 포워딩되는 결과를 가져올 수 있다. 예를 들어, 목적지가 고객의 사내 네트워크 내의 엔드포인트인 경우, 패킷은 VCN에 대해 구성된 DRG 게이트웨이를 실행하는 NVD로 VCN VR에 의해 포워딩될 수 있다. VCN VR은 소스 컴퓨팅 인스턴스와 연관된 VNIC를 실행하는 NVD와 동일한 NVD 상에서 실행될 수 있거나 또는 상이한 NVD에 의해 실행될 수 있다. 게이트웨이는, smartNIC, 호스트 머신, 또는 다른 NVD 구현예일 수 있는 NVD에 의해 실행될 수 있다. 그런 다음, 패킷은 게이트웨이에 의해 프로세싱되고 다음 홉으로 포워딩되며, 이는 그 최종 의도된 목적지 엔드포인트로의 패킷의 통신을 가능하게 한다. 예를 들어, 도 7에 도시된 실시예에서, 컴퓨팅 인스턴스(768)로부터 발원하는 패킷은 (NIC(732)를 사용하여) 링크(720)를 통해 호스트 머신(702)으로부터 NVD(710)로 통신될 수 있다. NVD(710) 상에서, VNIC가 소스 컴퓨팅 인스턴스(768)와 연관된 VNIC이기 때문에 VNIC(776)가 호출된다. VNIC(776)는, 패킷 내의 캡슐화된 정보를 검사하고, 그 의도된 목적지 엔드포인트로의 패킷의 통신을 가능하게 하려는 목적으로 패킷을 포워딩하기 위한 다음 홉을 결정하며, 그런 다음 패킷을 결정된 다음 홉으로 포워딩하도록 구성된다.

[0164] VCN 상에 배포된 컴퓨팅 인스턴스는 다양하고 상이한 엔드포인트들과 통신할 수 있다. 이러한 엔드포인트들은 CSPI(700)에 의해 호스팅되는 엔드포인트들 및 CSPI(700) 외부의 엔드포인트들을 포함할 수 있다. CSPI(700)에 의해 호스팅되는 엔드포인트들은, 고객의 VCN들 또는 고객에게 속하지 않은 VCN들일 수 있는 동일한 VCN 또는 다른 VCN들 내의 인스턴스들을 포함할 수 있다. CSPI(700)에 의해 호스팅되는 엔드포인트들 사이의 통신들은 물리적 네트워크(718)를 통해 수행될 수 있다. 컴퓨팅 인스턴스는 또한, CSPI(700)에 의해 호스팅되지 않거나 또는 CSPI(700) 외부에 있는 엔드포인트들과 통신할 수 있다. 이러한 엔드포인트들의 예들은 고객의 사내 네트워크 또는 데이터 센터 내의 엔드포인트들, 또는 인터넷과 같은 공용 네트워크를 통해 액세스가능한 공용 엔드포인트들을 포함한다. CSPI(700) 외부의 엔드포인트들과의 통신들은 다양한 통신 프로토콜들을 사용하여 공용 네트워크들(예를 들어, 인터넷(도 7에 미도시) 또는 사설 네트워크들(도 7에 미도시)을 통해 수행될 수 있다.

[0165] 도 7에 도시된 CSPI(700)의 아키텍처는 단지 일 예이며, 제한적으로 의도되지 않는다. 대안적인 실시예들에서 변형들, 대안들, 및 수정들이 가능하다. 예를 들어, 일부 구현예들에서, CSPI(700)은 도 7에 도시된 것보다 더

많거나 또는 더 적은 시스템들 또는 구성요소들을 가질 수 있거나, 2개 이상의 시스템들을 결합할 수 있거나, 또는 시스템들의 상이한 구성 또는 배열을 가질 수 있다. 도 7에 도시된 시스템들, 서브시스템들, 및 다른 구성요소들은 개별적인 시스템들, 하드웨어, 또는 이들의 조합들의 하나 이상의 프로세싱 유닛들(예를 들어, 프로세서들, 코어들)에 의해 실행되는 소프트웨어(예를 들어, 코드, 명령어들, 프로그램)로 구현될 수 있다. 소프트웨어는 비-일시적 저장 매체 상에(예를 들어, 메모리 디바이스 상에) 저장될 수 있다.

[0166] 도 9는 특정 실시예들에 따른, 다중테넌시(multitenancy)를 지원하기 위한 I/O 가상화를 제공하기 위한 NVD과 호스트 머신 사이의 연결성을 도시한다. 도 9에 도시된 바와 같이, 호스트 머신(902)은 가상화된 환경을 제공하는 하이퍼바이저(904)를 실행한다. 호스트 머신(902)은 2개의 가상 머신 인스턴스들, 즉, 고객/테넌트 #1에 속하는 VM1(906) 및 고객/테넌트 #2에 속하는 VM2(908)를 실행한다. 호스트 머신(902)은 링크(914)를 통해 NVD(912)에 연결된 물리적 NIC(910)를 포함한다. 컴퓨팅 인스턴스들 각각은 NVD(912)에 의해 실행되는 VNIC에 접속된다. 도 9의 실시예에서, VM1(906)은 VNIC-VM1(920)에 접속되고, VM2(908)는 VNIC-VM2(922)에 접속된다.

[0167] 도 9에 도시된 바와 같이, NIC(910)는 2개의 논리적 NIC들, 즉 논리적 NIC A(916)및 논리적 NIC B(918)를 포함한다. 각각의 가상 머신은 그 자체의 논리적 NIC에 접속되고 이와 함께 작동하도록 구성된다. 예를 들어, VM1(906)은 논리적 NIC A(916)에 접속되며, VM2(908)는 논리적 NIC B(918)에 접속된다. 호스트 머신(902)이 다수의 테넌트들에 의해 공유되는 하나의 물리적 NIC(910)만을 포함하지만, 논리적 NIC들로 인해, 각각의 테넌트의 가상 머신은 이들이 그들 자체의 호스트 모신 및 NIC를 갖는다고 믿는다.

[0168] 특정 실시예들에서, 각각의 논리적 NIC에는 그 자체의 VLAN ID가 할당된다. 따라서, 특정 VLAN ID가 테넌트 #1에 대한 논리적 NIC A(916)에 할당되며 별도의 VLAN ID가 테넌트 #2에 대한 논리적 NIC B(918)에 할당된다. 패킷이 VM1(906)로부터 통신될 때, 테넌트 #1에 할당된 태그가 하이퍼바이저에 의해 패킷에 첨부되며, 그런 다음 패킷은 링크(914)를 통해 호스트 머신(902)으로부터 NVD(912)로 통신된다. 유사한 방식으로, 패킷이 VM2(908)로부터 통신될 때, 테넌트 #2에 할당된 태그가 하이퍼바이저에 의해 패킷에 첨부되며, 그런 다음 패킷은 링크(914)를 통해 호스트 머신(902)으로부터 NVD(912)로 통신된다. 따라서, 호스트 머신(902)으로부터 NVD(912)로 통신된 패킷(924)은, 특정 테넌트 및 연관된 VM을 식별하는 연관된 태그(926)를 갖는다. NVD 상에서, 호스트 머신(902)으로부터 수신된 패킷(924)에 대해, 패킷과 연관된 태그(926)는 패킷이 VNIC-VM1(920)에 의해 프로세싱될지 또는 VNIC-VM2(922)에 의해 프로세싱될지 여부를 결정하기 위해 사용된다. 그런 다음, 패킷은 대응하는 VNIC에 의해 프로세싱된다. 도 9에 도시된 구성은, 각각의 테넌트의 컴퓨팅 인스턴스가 이들이 이들 자체의 호스트 머신 및 NIC를 갖는다고 믿는 것을 가능하게 한다. 도 9에 도시된 셋업은 다중-테넌시를 지원하기 위한 I/O 가상화를 제공한다.

[0169] 도 10은 특정 실시예들에 따른 물리적 네트워크(1000)의 단순화된 블록도를 도시한다. 도 10에 도시된 실시예는 클로스 네트워크로서 구조화된다. 클로스 네트워크는 높은 이등분(bisection) 대역폭 및 최대 자원 사용을 유지하면서 연결 중복성을 제공하도록 설계된 특정 유형의 네트워크 토폴로지이다. 클로스 네트워크는 비-차단, 멀티스테이지 또는 다중-계층형 스위칭 네트워크의 일 유형이며, 여기서 스테이지들 또는 계층들의 수는 2, 3, 4, 5, 등일 수 있다. 도 10에 도시된 실시예는 계층들 1, 2, 및 3을 포함하는 3-계층형 네트워크이다. TOR 스위치들(1004)은 클로스 네트워크 내의 계층-0 스위치들을 나타낸다. 하나 이상의 NVD들이 TOR 스위치들에 연결된다. 계층-0 스위치들은 물리적 네트워크의 에지 디바이스들로도 지칭된다. 계층-0 스위치들은, 리프 스위치들로도 지칭되는 계층-1 스위치들에 연결된다. 도 10에 도시된 실시예에서, "n"개의 계층-0 TOR 스위치들의 세트는 "n"개의 계층-1 스위치들의 세트에 연결되어 함께 포드(pod)를 형성한다. 포드 내의 각각의 계층-0 스위치는 포드 내의 모든 계층-1 스위치들에 상호연결되지만, 포드들 사이의 스위치들의 연결성은 존재하지 않는다. 특정 구현예들에서, 2개의 포드들이 블록으로 지칭된다. 각각의 블록은 "n"개의 계층-2 스위치들(때때로 스파인(spine) 스위치들로 지칭됨)의 세트에 의해 서비스되거나 또는 이에 연결된다. 물리적 네트워크 토폴로지 내에 몇몇 블록들이 있을 수 있다. 계층-2 스위치들은 결과적으로 "n"개의 계층-3 스위치들(때때로 슈퍼-스파인(super-spine) 스위치들로 지칭됨)에 연결된다. 물리적 네트워크(1000)를 통한 패킷들의 통신은 전형적으로 하나 이상의 계층-3 통신 프로토콜들을 사용하여 수행된다. 전형적으로, TOR 계층을 제외한 물리적 네트워크 내의 모든 계층들은 n-방향(n-way) 중복이며 따라서 고 가용성을 허용한다. 물리적 네트워크의 스케일링을 가능하게 하기 위해 물리적 네트워크 내에서 서로에 대한 스위치들의 가시성을 제어하기 위해 포드들 및 블록들에 대해 정책들이 지정될 수 있다.

[0170] 계층-0 스위치로부터 다른 계층-0 스위치에(또는 계층-0 스위치에 연결된 NVD로부터 계층-0 스위치에 연결된 다른 NVD에) 도달하기 위한 최대 홉 카운트가 고정된다는 것이 클로스 네트워크의 특징이다. 예를 들어, 3-계층형 클로스 네트워크에서, 패킷이 하나의 NVD로부터 다른 NVD에 도달하기 위해 최대 7개의 홉들이 필요하며, 여기서

소스 및 목표 NVD들은 클로스 네트워크의 리프 계층에 연결된다. 마찬가지로, 4-계층형 클로스 네트워크에서, 패킷이 하나의 NVD로부터 다른 NVD에 도달하기 위해 최대 9개의 홉들이 필요하며, 여기서 소스 및 목표 NVD들은 클로스 네트워크의 리프 계층에 연결된다. 따라서, 클로스 네트워크 아키텍처는 네트워크 전체에 걸쳐 일관된 레이턴시를 유지하며, 이는 데이터 센터들 내의 그리고 데이터 센터들 사이의 통신에 대해 중요하다. 클로스 토폴로지는 수평으로 스케일링하며 비용 효율적이다. 네트워크의 대역폭/스루풋 용량은, 다양한 계층들에 더 많은 스위치들(예를 들어, 더 많은 리프 및 스파인 스위치들)을 추가함으로써 그리고 인접한 계층들의 스위치들 사이의 링크들의 수를 증가시킴으로써 쉽게 증가될 수 있다.

[0171] 특정 실시예들에서, CSPI 내의 각각의 자원에는 클라우드 식별자(Cloud Identifier; CID)라고 하는 고유 식별자가 할당된다. 이러한 식별자는 자원의 정보의 부분으로서 포함되며, 예를 들어, 콘솔을 통해 또는 API들을 통해 자원을 관리하기 위해 사용될 수 있다. CID에 대한 예시적인 신택스(syntax)는 다음과 같다:

[0172] ocid1.<RESOURCE TYPE>.<REALM>.[REGION][.FUTURE USE].<UNIQUE ID>

[0173] 여기서,

[0174] ocid1: CID의 버전을 표시하는 리터럴(literal) 스트링;

[0175] resource type: 자원의 유형(예를 들어, 인스턴스, 볼륨, VCN, 서브넷, 사용자, 그룹, 등);

[0176] realm: 자원이 있는 렐름. 예시적인 값들은 상업적 렐름에 대해 "c1", 정부 클라우드 렐름에 대해 "c2", 또는 연방 정부 클라우드 렐름에 대해 "c3" 등이다. 각각의 렐름은 그 자체의 도메인 명칭을 가질 수 있다;

[0177] region: 자원이 있는 지역. 지역이 자원에 적용가능하지 않은 경우, 이러한 부분은 블랭크일 수 있다;

[0178] future use: 향후 사용을 위해 예약됨.

[0179] unique ID: ID의 고유 부분. 포맷은 자원 또는 서비스의 유형에 의존하여 변화할 수 있다.

[0180] 도 11은 적어도 일 실시예에 따른 IaaS 아키텍처의 예시적인 패턴을 예시하는 블록도(1100)이다. 서비스 운영자들(1102)은 가상 클라우드 네트워크(virtual cloud network; VCN)(1106)를 포함할 수 있는 보안 호스트 테넌시(tenancy)(1104) 및 보안 호스트 서브넷(subnet)(1108)에 통신가능하게 결합될 수 있다. 일부 예들에서, 서비스 운영자들(1102)은, Microsoft Windows Mobile® 및/또는 iOS, Windows Phone, Android, BlackBerry 8, Palm OS, 및 유사한 것과 같은 다양한 모바일 운영 체제들과 같은 소프트웨어를 실행하며, 인터넷, e-메일, 단문 메시지 서비스(short message service; SMS), Blackberry®, 또는 다른 통신 프로토콜 가능형(enabled)일 수 있는, 휴대용 핸드헬드 디바이스들(예를 들어, iPhone®, 셀룰러 전화기, iPad®, 컴퓨팅 태블릿, 개인용 정보 단말기(personal digital assistant; PDA)) 또는 웨어러블(wearable) 디바이스들(예를 들어, Google Glass® 머리 착용형 디스플레이(head mounted display))일 수 있는 하나 이상의 클라이언트 컴퓨팅 디바이스들을 사용하고 있을 수 있다. 대안적으로, 클라이언트 컴퓨팅 디바이스들은, 예로서, 다양한 버전들의 Microsoft Windows®, Apple Macintosh®, 및/또는 리눅스 운영 체제들을 실행하는 개인용 컴퓨터들 및/또는 랩탑 컴퓨터들을 포함하는 범용 개인용 컴퓨터들일 수 있다. 클라이언트 컴퓨팅 디바이스들은, 비제한적으로, 예를 들어, 구글 크롬 OS와 같은 다양한 GNU/리눅스 운영 체제들을 포함하는, 다양한 상용-이용가능 UNIX® 또는 UNIX-유사 운영 체제들 중 임의의 것을 실행하는 워크스테이션 컴퓨터들일 수 있다. 대안적으로 또는 추가적으로, 클라이언트 컴퓨팅 디바이스들은, VCN(1106)에 액세스할 수 있는 네트워크 및/또는 인터넷을 통해 통신할 수 있는 임의의 다른 전자 디바이스, 예컨대 씬-클라이언트(thin-client) 컴퓨터, 인터넷-가능형 게이밍 시스템(예를 들어, Kinect® 제스처 입력 디바이스를 갖는 또는 이를 갖지 않는 마이크로소프트 Xbox 게이밍 콘솔), 및/또는 개인용 메시징 디바이스일 수 있다.

[0181] VCN(1106)은, SSH VCN(1112)에 포함된 LPG(1110)를 통해 보안 쉘(secure shell; SSH) VCN(1112)에 통신가능하게 결합될 수 있는 로컬 피어링 게이트웨이(local peering gateway; LPG)(1110)를 포함할 수 있다. SSH VCN(1112)은 SSH 서브넷(1114)을 포함할 수 있으며, SSH VCN(1112)은 제어 평면 VCN(1116)에 포함된 LPG(1110)를 통해 제어 평면 VCN(1116)에 통신가능하게 결합될 수 있다. 또한, SSH VCN(1112)은 LPG(1110)를 통해 데이터 평면 VCN(1118)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)은, IaaS 제공자에 의해 소유되거나 및/또는 운영될 수 있는 서비스 테넌시(1119)에 포함될 수 있다.

[0182] 제어 평면 VCN(1116)은 주변 네트워크(예를 들어, 기업 인트라넷과 외부 네트워크들 사이의 기업 네트워크의 부분들)로서 역할하는 제어 평면 비무장 구역(demilitarized zone; DMZ) 계층(1120)을 포함할 수 있다. DMZ-기반 서버들은 제한된 책임들을 가질 수 있으며 침해들을 억제하는 것을 도울 수 있다. 추가적으로, DMZ 계층(1120)

은 하나 이상의 로드 밸런서(load balancer; LB) 서브넷(들)(1122), 앱 서브넷(들)(1126)을 포함할 수 있는 제어 평면 앱 계층(1124), 데이터베이스(database; DB) 서브넷(들)(1130)(예를 들어, 프런트엔드 DB 서브넷(들) 및/또는 백엔드 DB 서브넷(들))을 포함할 수 있는 제어 평면 데이터 계층(1128)을 포함할 수 있다. 제어 평면 DMZ 계층(1120)에 포함된 LB 서브넷(들)(1122)은 제어 평면 앱 계층(1124)에 포함된 앱 서브넷(들)(1126) 및 제어 평면 VCN(1116)에 포함될 수 있는 인터넷 게이트웨이(1134)에 통신가능하게 결합될 수 있으며, 앱 서브넷(들)(1126)은 제어 평면 데이터 계층(1128)에 포함된 DB 서브넷(들)(1130), 서비스 게이트 웨이(1136) 및 네트워크 어드레스 변환(network address translation; NAT) 게이트웨이(1138)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1116)은 서비스 게이트웨이(1136) 및 NAT 게이트웨이(1138)를 포함할 수 있다.

[0183] 제어 평면 VCN(1116)은 앱 서브넷(들)(1126)을 포함할 수 있는 데이터 평면 미러 앱 계층(1140)을 포함할 수 있다. 데이터 평면 미러 앱 계층(1140)에 포함된 앱 서브넷(들)(1126)은 컴퓨팅 인스턴스(1144)를 실행할 수 있는 가상 네트워크 인터페이스 제어기(virtual network interface controller; VNIC)(1142)를 포함할 수 있다. 컴퓨팅 인스턴스(1144)는, 데이터 평면 미러 앱 계층(1140)의 앱 서브넷(들)(1126)을 데이터 평면 앱 계층(1146)에 포함될 수 있는 앱 서브넷(들)(1126)에 통신가능하게 결합할 수 있다.

[0184] 데이터 평면 VCN(1118)은 데이터 평면 앱 계층(1146), 데이터 평면 DMZ 계층(1148), 및 데이터 평면 데이터 계층(1150)을 포함할 수 있다. 데이터 평면 DMZ 계층(1148)은, 데이터 평면 앱 계층(1146)의 앱 서브넷(들)(1126) 및 데이터 평면 VCN(1118)의 인터넷 게이트웨이(1134)에 통신가능하게 결합될 수 있는 LB 서브넷(들)(1122)을 포함할 수 있다. 앱 서브넷(들)(1126)은 데이터 평면 VCN(1118)의 서비스 게이트웨이(1136) 및 데이터 평면 VCN(1118)의 NAT 게이트 웨이(1138)에 통신가능하게 결합될 수 있다. 데이터 평면 데이터 계층(1150)은 또한, 데이터 평면 앱 계층(1146)의 앱 서브넷(들)(1126)에 통신가능하게 결합될 수 있는 DB 서브넷(들)(1130)을 포함할 수 있다.

[0185] 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)의 인터넷 게이트웨이(1134)는, 공용 인터넷(1154)에 통신가능하게 결합될 수 있는 메타데이터 관리 서비스(1152)에 통신가능하게 결합될 수 있다. 공용 인터넷(1154)은 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)의 NAT 게이트웨이(1138)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)의 서비스 게이트웨이(1136)는 클라우드 서비스들(1156)에 통신가능하게 결합될 수 있다.

[0186] 일부 예들에서, 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)의 서비스 게이트웨이(1136)는 공용 인터넷(1154)을 거치지 않는 클라우드 서비스들(1156)에 대한 애플리케이션 프로그래밍 인터페이스(application programming interface; API) 호출(call)들을 만들 수 있다. 서비스 게이트웨이(1136)로부터 클라우드 서비스들(1156)로의 API 호출들은 1-방향일 수 있다: 서비스 게이트웨이(1136)는 클라우드 서비스들(1156)로의 호출들을 만들 수 있으며, 클라우드 서비스들(1156)은 서비스 게이트웨이(1136)로 요청된 데이터를 전송할 수 있다. 그러나, 클라우드 서비스들(1156)은 서비스 게이트웨이(1136)에 대한 API 호출들을 개시하지 않을 수 있다.

[0187] 일부 예들에서, 보안 호스트 테넌시(1104)는, 그렇지 않았다면 격리되었을 서비스 테넌시(1119)에 직접적으로 연결될 수 있다. 보안 호스트 서브넷(1108)은, 달리 격리된 시스템을 통한 2-방향 통신을 가능하게 할 수 있는 LPG(1110)를 통해 SSH 서브넷(1114)과 통신할 수 있다. 보안 호스트 서브넷(1108)을 SSH 서브넷(1114)에 연결하는 것은 서비스 테넌시(1119) 내의 다른 엔티티들에게 보안 호스트 서브넷(1108) 액세스를 제공할 수 있다.

[0188] 제어 평면 VCN(1116)은 서비스 테넌시(1119)의 사용자들이 희망되는 자원을 셋업하거나 또는 달리 프로비저닝하는 것을 가능하게 할 수 있다. 제어 평면 VCN(1116)에 프로비저닝된 희망되는 자원들은 데이터 평면 VCN(1118)에서 배포되거나 또는 달리 사용될 수 있다. 일부 예들에서, 제어 평면 VCN(1116)는 데이터 평면 VCN(1118)으로부터 격리될 수 있으며, 제어 평면 VCN(1116)의 데이터 평면 미러 앱 계층(1140)은, 데이터 평면 미러 앱 계층(1140) 및 데이터 평면 앱 계층(1146)에 포함될 수 있는 VNIC들(1142)을 통해 데이터 평면 VCN(1118)의 데이터 평면 앱 계층(1146)과 통신할 수 있다.

[0189] 일부 예들에서, 시스템의 사용자들 또는 고객들은, 메타데이터 관리 서비스(1152)로 요청들을 통신할 수 있는 공용 인터넷(1154)을 통해 요청들, 예를 들어, 생성, 판독, 업데이트 또는 삭제(create, read, update, or delete; CRUD) 동작들을 만들 수 있다. 메타데이터 관리 서비스(1152)는 요청을 인터넷 게이트웨이(1134)를 통해 제어 평면 VCN(1116)으로 통신할 수 있다. 요청은 제어 평면 DMZ 계층(1120)에 포함된 LB 서브넷(들)(1122)에 의해 수신될 수 있다. LB 서브넷(들)(1122)은 요청이 유효하다는 것을 결정할 수 있으며, 이러한 결정에 응답하여, LB 서브넷(들)(1122)은 요청을 제어 평면 앱 계층(1124)에 포함된 앱 서브넷(들)(1126)로 송신할 수 있다. 요청이 검증되고 공용 인터넷(1154)에 대한 호출을 필요로 하는 경우, 공용 인터넷(1154)에 대한 호출은 공

용 인터넷(1154)에 대한 호출을 만들 수 있는 NAT 게이트웨이(1138)로 송신될 수 있다. 요청에 의해 저장되도록 희망될 수 있는 메모리는 DB 서브넷(들)(1130)에 저장될 수 있다.

[0190] 일부 예들에서, 데이터 평면 미러 앱 계층(1140)은 제어 평면 VCN(1116)과 데이터 평면 VCN(1118) 사이의 직접 통신을 가능하게 할 수 있다. 예를 들어, 구성에 대한 변경들, 업데이트들, 또는 다른 적절한 수정들은 데이터 평면 VCN(1118)에 포함된 자원들에 적용되도록 희망될 수 있다. VNIC(1142)를 통해, 제어 평면 VCN(1116)은 데이터 평면 VCN(1118)에 포함된 자원들과 직접적으로 통신할 수 있으며, 그럼으로써 데이터 평면 VCN에 포함된 자원들에 대해 구성에 대한 변경들, 업데이트들 또는 다른 적절한 수정들을 실행할 수 있다.

[0191] 일부 실시예들에서, 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)은 서비스 테넌시(1119)에 포함될 수 있다. 이러한 경우에, 시스템의 사용자 또는 고객은 제어 평면 VCN(1116) 또는 데이터 평면 VCN(1118)를 소유하거나 또는 운영하지 않을 수 있다. 대신에, IaaS 제공자가 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)를 소유하거나 또는 운영할 수 있으며, 이들 둘 모두는 서비스 테넌시(1119)에 포함될 수 있다. 이러한 실시예는, 사용자들 또는 고객들이 다른 사용자들의 또는 다른 고객들의 자원들과 상호작용하는 것을 방지할 수 있는 네트워크들의 격리를 가능하게 할 수 있다. 또한, 이러한 실시예는 시스템의 사용자들 또는 고객들이, 저장을 위해 희망되는 위협 방지 레벨을 갖지 않을 수 있는 공용 인터넷(1154)에 의존할 필요 없이 데이터베이스들을 사적으로 저장하는 것을 가능하게 할 수 있다.

[0192] 다른 실시예들에서, 제어 평면 VCN(1116)에 포함된 LB 서브넷(들)(1122)은 서비스 게이트웨이(1136)로부터 신호를 수신하도록 구성될 수 있다. 이러한 실시예에서, 제어 평면 VCN(1116) 및 데이터 평면 VCN(1118)은, 공용 인터넷(1154)을 호출하지 않고 IaaS 제공자의 고객에 의해 호출되도록 구성될 수 있다. 고객들이 사용하는 데이터베이스(들)가 IaaS 제공자에 의해 제어될 수 있으며 공용 인터넷(1154)으로부터 격리될 수 있는 서비스 테넌시(1119) 상에 저장될 수 있기 때문에, IaaS 제공자의 고객들은 이러한 실시예를 희망할 수 있다.

[0193] 도 12는 적어도 일 실시예에 따른 IaaS 아키텍처의 다른 예시적인 패턴을 예시하는 블록도(1200)이다. 서비스 운영자들(1202)(예를 들어, 도 11의 서비스 운영자들(1102))은, 가상 클라우드 네트워크(VCN)(1206)(예를 들어, 도 11의 VCN(1106)) 및 보안 호스트 서브넷(1208)(예를 들어, 도 11의 보안 호스트 서브넷(1108))을 포함할 수 있는 보안 호스트 테넌시(1204)(예를 들어, 도 11의 보안 호스트 테넌시(1104))에 통신가능하게 결합될 수 있다. VCN(1206)은, SSH VCN(1212)에 포함된 LPG(1110)를 통해 보안 쉘(secure shell; SSH) VCN(1212)(예를 들어, 도 11의 SSH VCN(1112))에 통신가능하게 결합될 수 있는 로컬 피어링 게이트웨이(local peering gateway; LPG)(1210)(예를 들어, 도 11의 LPG(1110))를 포함할 수 있다. SSH VCN(1212)은 SSH 서브넷(1214)(예를 들어, 도 11의 SSH 서브넷(1114))을 포함할 수 있으며, SSH VCN(1212)는 제어 평면 VCN(1216)에 포함된 LPG(1210)를 통해 제어 평면 VCN(1216)(예를 들어, 도 11의 제어 평면 VCN(1116))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1216)은 서비스 테넌시(1219)(예를 들어, 도 11의 서비스 테넌시(1119))에 포함될 수 있으며, 데이터 평면 VCN(1218)(예를 들어, 도 11의 데이터 평면 VCN(1118))은 시스템의 사용자들 또는 고객들에 의해 소유되거나 또는 운영될 수 있는 고객 테넌시(1221)에 포함될 수 있다.

[0194] 제어 평면 VCN(1216)은, LB 서브셋(들)(1222)(예를 들어, 도 11의 LB 서브셋(들)(1122))을 포함할 수 있는 제어 평면 DMZ 계층(1220)(예를 들어, 도 11의 제어 평면 DMZ 계층(1120)), 앱 서브넷(들)(1226)(예를 들어, 도 11의 앱 서브넷(들)(1126))을 포함할 수 있는 제어 평면 앱 계층(1224)(예를 들어, 도 11의 제어 평면 앱 계층(1124)), 데이터베이스(DB) 서브넷(들)(1230)(예를 들어, 도 11의 DB 서브넷(들)(1130)과 유사함)을 포함할 수 있는 제어 평면 데이터 계층(1228)(예를 들어, 도 11의 제어 평면 데이터 계층(1128))을 포함할 수 있다. 제어 평면 DMZ 계층(1220)에 포함된 LB 서브(넷)(1222)은 제어 평면 앱 계층(1224)에 포함된 앱 서브넷(들)(1226) 및 제어 평면 VCN(1216)에 포함될 수 있는 인터넷 게이트웨이(1234)(예를 들어, 도 11의 인터넷 게이트웨이(1134))에 통신가능하게 결합될 수 있으며, 앱 서브넷(들)(1226)은 제어 평면 데이터 계층(1228)에 포함된 DB 서브넷(들)(1230), 서비스 게이트 웨이(1236)(예를 들어, 도 11의 서비스 게이트웨이) 및 네트워크 어드레스 변환(NAT) 게이트웨이(1238)(예를 들어, 도 11의 NAT 게이트웨이(1138))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1216)은 서비스 게이트웨이(1236) 및 NAT 게이트웨이(1238)를 포함할 수 있다.

[0195] 제어 평면 VCN(1216)은 앱 서브넷(들)(1226)을 포함할 수 있는 데이터 평면 미러 앱 계층(1240)(예를 들어, 도 11의 데이터 평면 미러 앱 계층(1140))을 포함할 수 있다. 데이터 평면 미러 앱 계층(1240)에 포함된 앱 서브넷(들)(1226)은 컴퓨팅 인스턴스(1244)(예를 들어, 도 11의 컴퓨팅 인스턴스(1144)와 유사함)를 실행할 수 있는 가상 네트워크 인터페이스 제어기(VNIC)(1242)(예를 들어, VNIC(1142))를 포함할 수 있다. 컴퓨팅 인스턴스(1244)는, 데이터 평면 미러 앱 계층(1240)에 포함된 VNIC(1242) 및 데이터 평면 앱 계층(1246)에 포함된

VNIC(1242)를 통한 데이터 평면 앱 계층(1246)(예를 들어, 도 11의 데이터 평면 앱 계층(1146))에 포함될 수 있는 앱 서브넷(들)(1226)과 데이터 평면 미러 앱 계층(1240)의 앱 서브넷(들)(1226) 사이의 통신을 가능하게 할 수 있다.

[0196] 제어 평면 VCN(1216)에 포함된 인터넷 게이트웨이(1234)는, 공용 인터넷(1254)(예를 들어, 도 11의 공용 인터넷(1154))에 통신가능하게 결합될 수 있는 메타데이터 관리 서비스(1252)(예를 들어, 도 11의 메타데이터 관리 서비스(1152))에 통신가능하게 결합될 수 있다. 공용 인터넷(1254)은 제어 평면 VCN(1216)의 NAT 게이트웨이(1238)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1216)에 포함된 서비스 게이트웨이(1236)는 클라우드 서비스들(1256)(예를 들어, 도 11의 클라우드 서비스들(1156))에 통신가능하게 결합될 수 있다.

[0197] 일부 예들에서, 데이터 평면 VCN(1218)은 고객 테넌시(1221)에 포함될 수 있다. 이러한 경우에, IaaS 제공자는 각각의 고객에 대해 제어 평면 VCN(1216)를 제공할 수 있으며, IaaS 제공자는, 각각의 고객에 대해, 서비스 테넌시(1219)에 포함된 고유 컴퓨팅 인스턴스(1244)를 셋업할 수 있다. 각각의 컴퓨팅 인스턴스(1244)는 서비스 테넌시(1219)에 포함된 제어 평면 VCN(1216)과 고객 테넌시(1221)에 포함된 데이터 평면 VCN(1218) 사이의 통신을 가능하게 할 수 있다. 컴퓨팅 인스턴스(1244)는 서비스 테넌시(1219)에 포함된 제어 평면 VCN(1216)에 프로비저닝된 자원들이 고객 테넌시(1221)에 포함된 데이터 평면 VCN(1218)에 배포되거나 또는 달리 사용되는 것을 가능하게 할 수 있다.

[0198] 다른 예들에서, IaaS 제공자의 고객은 고객 테넌시(1221)에 거주(live)하는 데이터베이스들을 가질 수 있다. 이러한 예에서, 제어 평면 VCN(1216)은 앱 서브넷(들)(1226)을 포함할 수 있는 데이터 평면 미러 앱 계층(1240)을 포함할 수 있다. 데이터 평면 미러 앱 계층(1240)은 데이터 평면 VCN(1218)에 상주할 수 있지만, 데이터 평면 미러 앱 계층(1240)은 데이터 평면 VCN(1218)에 거주하지 않을 수 있다. 즉, 데이터 평면 미러 앱 계층(1240)은 고객 테넌시(1221)에 대한 액세스를 가질 수 있지만, 데이터 평면 미러 앱 계층(1240)은 데이터 평면 VCN(1218)에 존재하지 않을 수 있거나 또는 IaaS 제공자의 고객에 의해 소유되거나 또는 운영되지 않을 수 있다. 데이터 평면 미러 앱 계층(1240)은 데이터 평면 VCN(1218)에 대한 호출들을 만들도록 구성될 수 있지만, 제어 평면 VCN(1216)에 포함된 엔티티에 대한 호출들을 만들도록 구성되지 않을 수 있다. 고객은 제어 평면 VCN(1216)에 프로비저닝된 데이터 평면 VCN(1218)에서 자원들을 배포하거나 또는 달리 사용하는 것을 희망할 수 있으며, 데이터 평면 미러 앱 계층(1240)은 고객의 자원들의 희망되는 배포 또는 다른 사용을 가능하게 할 수 있다.

[0199] 일부 실시예들에서, IaaS 제공자의 고객은 데이터 평면 VCN(1218)에 필터들을 적용할 수 있다. 이러한 실시예에서, 고객은 데이터 평면 VCN(1218)이 액세스할 수 있는 것을 결정할 수 있고, 고객은 데이터 평면 VCN(1218)으로부터 공용 인터넷(1254)에 대한 액세스를 제한할 수 있다. IaaS 제공자는 임의의 외부 네트워크들 또는 데이터베이스들에 대한 데이터 평면 VCN(1218)의 액세스에 필터를 적용하거나 또는 달리 이를 제어하지 못할 수 있다. 고객 테넌시(1221)에 포함된 데이터 평면 VCN(1218) 상에 고객에 의한 필터들 및 제어들을 적용하는 것은 데이터 평면 VCN(1218)을 다른 고객들 및 공용 인터넷(1254)으로부터 격리시키는 것을 도울 수 있다.

[0200] 일부 실시예들에서, 클라우드 서비스들(1256)은, 공용 인터넷(1254) 상에, 제어 평면 VCN(1216) 상에, 또는 데이터 평면 VCN(1218) 상에 존재하지 않을 수 있는 서비스들을 액세스하기 위해 서비스 게이트웨이(1236)에 의해 호출될 수 있다. 클라우드 서비스들(1256)과 제어 평면 VCN(1216) 또는 데이터 평면 VCN(1218) 사이의 연결은 라이브가 아닐 수 있거나 또는 연속적이지 않을 수 있다. 클라우드 서비스들(1256)은 IaaS 제공자에 의해 소유되거나 또는 운영되는 상이한 네트워크 상에 존재할 수 있다. 클라우드 서비스들(1256)은 서비스 게이트웨이(1236)로부터 호출들을 수신하도록 구성될 수 있으며, 공용 인터넷(1254)으로부터의 호출들을 수신하지 않도록 구성될 수 있다. 일부 클라우드 서비스들(1256)은 다른 클라우드 서비스들(1256)으로부터 격리될 수 있으며, 제어 평면 VCN(1216)은, 제어 평면 VCN(1216)과 동일한 지역에 있지 않을 수 있는 클라우드 서비스들(1256)로부터 격리될 수 있다. 예를 들어, 제어 평면 VCN(1216)은 "지역 1"에 위치될 수 있으며, 클라우드 서비스 "배포 11"은 지역 1 및 "지역 2"에 위치될 수 있다. 배포 11에 대한 호출이 지역 1에 위치된 제어 평면 VCN(1216)에 포함된 서비스 게이트웨이(1236)에 의해 이루어지는 경우, 호출은 지역 1 내의 배포 11로 송신될 수 있다. 이러한 예에서, 제어 평면 VCN(1216) 또는 지역 1 내의 배포 11은 지역 2 내의 배포 11과 통신가능하게 결합되지 않을 수 있거나 또는 이와 달리 통신하지 않을 수 있다.

[0201] 도 13은 적어도 일 실시예에 따른 IaaS 아키텍처의 다른 예시적인 패턴을 예시하는 블록도(1300)이다. 서비스 운영자들(1302)(예를 들어, 도 11의 서비스 운영자들(1102))은, 가상 클라우드 네트워크(VCN)(1306)(예를 들어, 도 11의 VCN(1106)) 및 보안 호스트 서브넷(1308)(예를 들어, 도 11의 보안 호스트 서브넷(1108))을 포함할 수 있는 보안 호스트 테넌시(1304)(예를 들어, 도 11의 보안 호스트 테넌시(1104))에 통신가능하게 결합될 수

있다. VCN(1306)은, SSH VCN(1312)에 포함된 LPG(1310)를 통해 SSH VCN(1312)(예를 들어, 도 11의 SSH VCN(1112))에 통신가능하게 결합될 수 있는 LPG(1310)(예를 들어, 도 11의 LPG(1110))를 포함할 수 있다. SSH VCN(1312)은 SSH 서브넷(1314)(예를 들어, 도 11의 SSH 서브넷(1114))을 포함할 수 있으며, SSH VCN(1312)는 제어 평면 VCN(1316)에 포함된 LPG(1310)를 통해 제어 평면 VCN(1316)(예를 들어, 도 11의 제어 평면 VCN(1116))에 그리고 데이터 평면 VCN(1318)에 포함된 LPG(1310)를 통해 데이터 평면 VCN(1318)(예를 들어, 도 11의 데이터 평면 VCN(1118))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1316) 및 데이터 평면 VCN(1318)은 서비스 테넌시(1319)(예를 들어, 도 11의 서비스 테넌시(1119))에 포함될 수 있다.

[0202] 제어 평면 VCN(1316)은, 로드 밸런서(LB) 서브넷(들)(1322)(예를 들어, 도 11의 LB 서브넷(들)(1122))을 포함할 수 있는 제어 평면 DMZ 계층(1320)(예를 들어, 도 11의 제어 평면 DMZ 계층(1120)), 앱 서브넷(들)(1326)(예를 들어, 도 11의 앱 서브넷(들)(1126)과 유사함)을 포함할 수 있는 제어 평면 앱 계층(1324)(예를 들어, 도 11의 제어 평면 앱 계층(1124)), DB 서브넷(들)(1330)을 포함할 수 있는 제어 평면 데이터 계층(1328)(예를 들어, 도 11의 제어 평면 데이터 계층(1128))을 포함할 수 있다. 제어 평면 DMZ 계층(1320)에 포함된 LB 서브넷(들)(1322)은 제어 평면 앱 계층(1324)에 포함된 앱 서브넷(들)(1326) 및 제어 평면 VCN(1316)에 포함될 수 있는 인터넷 게이트웨이(1334)(예를 들어, 도 11의 인터넷 게이트웨이(1134))에 통신가능하게 결합될 수 있으며, 앱 서브넷(들)(1326)은 제어 평면 데이터 계층(1328)에 포함된 DB 서브넷(들)(1330), 서비스 게이트 웨이(1336)(예를 들어, 도 11의 서비스 게이트웨이) 및 네트워크 어드레스 변환(NAT) 게이트웨이(1338)(예를 들어, 도 11의 NAT 게이트웨이(1138))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1316)은 서비스 게이트웨이(1336) 및 NAT 게이트웨이(1338)를 포함할 수 있다.

[0203] 데이터 평면 VCN(1318)은 데이터 평면 앱 계층(1346)(예를 들어, 도 11의 데이터 평면 앱 계층(1146)), 데이터 평면 DMZ 계층(1348)(예를 들어, 도 11의 데이터 평면 DMZ 계층(1148)), 및 데이터 평면 데이터 계층(1350)(예를 들어, 도 11의 데이터 평면 데이터 계층(1150))을 포함할 수 있다. 데이터 평면 DMZ 계층(1348)은, 데이터 평면 앱 계층(1346)의 신뢰할 수 있는 앱 서브넷(들)(1360)과 신뢰할 수 없는 앱 서브넷(들)(1362), 및 데이터 평면 VCN(1318)에 포함된 인터넷 게이트웨이(1334)에 통신가능하게 결합될 수 있는 LB 서브넷(들)(1322)을 포함할 수 있다. 신뢰할 수 있는 앱 서브넷(들)(1360)은 데이터 평면 VCN(1318)에 포함된 서비스 게이트웨이(1336), 데이터 평면 VCN(1318)에 포함된 NAT 게이트웨이(1338), 및 데이터 평면 데이터 계층(1350)에 포함된 DB 서브넷(들)(1330)에 통신가능하게 결합될 수 있다. 신뢰할 수 없는 앱 서브넷(들)(1362)은 데이터 평면 VCN(1318)에 포함된 서비스 게이트웨이(1336) 및 데이터 평면 데이터 계층(1350)에 포함된 DB 서브넷(들)(1330)에 통신가능하게 결합될 수 있다. 데이터 평면 데이터 계층(1350)은, 데이터 평면 VCN(1318)에 포함된 서비스 게이트웨이(1336)에 통신가능하게 결합될 수 있는 DB 서브넷(들)(1330)을 포함할 수 있다.

[0204] 신뢰할 수 없는 앱 서브넷(들)(1362)은 테넌트(tenant) 가상 머신(VM)들(1366(1)-(N))에 통신가능하게 결합될 수 있는 하나 이상의 1차 VNIC들(1364(1)-(N))을 포함할 수 있다. 각각의 테넌트 VM(1366(1)-(N))은, 개별적인 고객 테넌시들(1370(1)-(N))에 포함될 수 있는 개별적인 컨테이너 출구 VCN들(1368(1)-(N))에 포함될 수 있는 개별적인 앱 서브넷(1367(1)-(N))에 통신가능하게 결합될 수 있다. 개별적인 2차 VNIC들(1372(1)-(N))은 데이터 평면 VCN(1318)에 포함된 신뢰할 수 없는 앱 서브넷(들)(1362)과 컨테이너 출구 VCN들(1368(1)-(N))에 포함된 앱 서브넷 사이의 통신을 가능하게 할 수 있다. 각각의 컨테이너 출구 VCN들(1368(1)-(N))은, 공용 인터넷(1354)(예를 들어, 도 11의 공용 인터넷(1154))에 통신가능하게 결합될 수 있는 NAT 게이트웨이(1338)를 포함할 수 있다.

[0205] 제어 평면 VCN(1316)에 포함되고 데이터 평면 VCN(1318)에 포함된 인터넷 게이트웨이(1334)는, 공용 인터넷(1354)에 통신가능하게 결합될 수 있는 메타데이터 관리 서비스(1352)(예를 들어, 도 11의 메타데이터 관리 시스템(1152))에 통신가능하게 결합될 수 있다. 공용 인터넷(1354)은, 제어 평면 VCN(1316)에 포함되고 데이터 평면 VCN(1318)에 포함된 NAT 게이트웨이(1338)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1316)에 포함되고 데이터 평면 VCN(1318)에 포함된 서비스 게이트웨이(1336)는 클라우드 서비스들(1356)에 통신가능하게 결합될 수 있다.

[0206] 일부 실시예들에서, 데이터 평면 VCN(1318)은 고객 테넌시들(1370)과 통합될 수 있다. 이러한 통합은, 코드를 실행할 때 지원을 희망할 수 있는 경우와 같은 일부 경우들에서 IaaS 제공자의 고객들에 대해 유용하거나 또는 바람직할 수 있다. 고객은, 파괴적일 수 있거나 또는 다른 고객 자원들과 통신할 수 있거나 또는 달리 바람직하지 않은 효과들을 야기할 수 있는, 실행할 코드를 제공할 수 있다. 이에 응답하여, IaaS 제공자는 고객에 의해 IaaS 제공자에게 주어진 코드를 실행할지 여부를 결정할 수 있다.

[0207] 일부 예들에서, IaaS 제공자의 고객은 IaaS 제공자에게 일시적인 네트워크 액세스를 승인할 수 있으며, 데이터 평면 계층 앱(1346)에 첨부될 기능을 요청할 수 있다. 기능을 실행하기 위한 코드는 VM들(1366(1)-(N))에서 실행될 수 있으며, 코드는 데이터 평면 VCN(1318) 상의 다른 곳에서는 실행되도록 구성되지 않을 수 있다. 각각의 VM(1366(1)-(N))은 하나의 고객 테넌시(1370)에 연결될 수 있다. VM들(1366(1)-(N))에 포함된 개별적인 컨테이너들(1371(1)-(N))은 코드를 실행하도록 구성될 수 있다. 이러한 경우에, 이중 격리가 존재할 수 있으며(예를 들어, 코드를 실행하는 컨테이너들(1371(1)-(N)), 여기서 컨테이너들(1371(1)-(N))은 신뢰할 수 없는 앱 서브넷(들)(1362)에 포함된 적어도 하나의 VM(1366(1)-(N))에 포함될 수 있음), 이는 부정확하거나 또는 달리 바람직하지 않은 코드가 IaaS 제공자의 네트워크를 손상시키거나 또는 상이한 고객의 네트워크를 손상시키는 것을 방지하는 것을 도울 수 있다. 컨테이너들(1371(1)-(N))은 고객 테넌시(1370)에 통신가능하게 결합될 수 있으며, 고객 테넌시(1370)로 데이터를 송신하거나 또는 이로부터 데이터를 수신하도록 구성될 수 있다. 컨테이너들(1371(1)-(N))은 데이터 평면 VCN(1318) 내의 임의의 다른 엔티티로 데이터를 송신하거나 또는 이로부터 데이터를 수신하도록 구성되지 않을 수 있다. 코드 실행의 완료 시에, IaaS 제공자는 컨테이너들(1371(1)-(N))을 없애거나(kill) 또는 달리 폐기할 수 있다.

[0208] 일부 실시예들에서, 신뢰할 수 있는 앱 서브넷(들)(1360)은, IaaS 제공자에 의해 소유되거나 또는 운영될 수 있는 코드를 실행할 수 있다. 이러한 실시예에서, 신뢰할 수 있는 앱 서브넷(들)(1360)은 DB 서브넷(들)(1330)에 통신가능하게 결합될 수 있으며, DB 서브넷(들)(1330)에서 CRUD 동작들을 실행하도록 구성될 수 있다. 신뢰할 수 없는 앱 서브넷(들)(1362)은 DB 서브넷(들)(1330)에 통신가능하게 결합될 수 있지만, 이러한 실시예에서, 신뢰할 수 없는 앱 서브넷(들)은 DB 서브넷(들)(1330)에서 판독 동작들을 실행하도록 구성될 수 있다. 각각의 고객의 VM(1366(1)-(N))에 포함될 수 있으며 고객으로부터의 코드를 실행할 수 있는 컨테이너들(1371(1)-(N))은 DB 서브넷(들)(1330)과 통신가능하게 결합되지 않을 수 있다.

[0209] 다른 실시예들에서, 제어 평면 VCN(1316) 및 데이터 평면 VCN(1318)은 직접적으로 통신가능하게 결합되지 않을 수 있다. 이러한 실시예에서, 제어 평면 VCN(1316)과 데이터 평면 VCN(1318) 사이의 직접 통신이 존재하지 않을 수 있다. 그러나, 통신은 적어도 하나의 방법을 통해 간접적으로 발생할 수 있다. 제어 평면 VCN(1316)과 데이터 평면 VCN(1318) 사이의 통신을 가능하게 할 수 있는 LPG(1310)가 IaaS 제공자에 의해 수립될 수 있다. 다른 예에서, 제어 평면 VCN(1316) 또는 데이터 평면 VCN(1318)은 서비스 게이트웨이(1336)을 통해 클라우드 서비스들(1356)에 대한 호출을 만들 수 있다. 예를 들어, 제어 평면 VCN(1316)으로부터 클라우드 서비스들(1356)으로의 호출은, 데이터 평면 VCN(1318)과 통신할 수 있는 서비스에 대한 요청을 포함할 수 있다.

[0210] 도 14은 적어도 일 실시예에 따른 IaaS 아키텍처의 다른 예시적인 패턴을 예시하는 블록도(1400)이다. 서비스 운영자들(1402)(예를 들어, 도 11의 서비스 운영자들(1102))은, 가상 클라우드 네트워크(VCN)(1406)(예를 들어, 도 11의 VCN(1106)) 및 보안 호스트 서브넷(1408)(예를 들어, 도 11의 보안 호스트 서브넷(1108))을 포함할 수 있는 보안 호스트 테넌시(1404)(예를 들어, 도 11의 보안 호스트 테넌시(1104))에 통신가능하게 결합될 수 있다. VCN(1406)은, SSH VCN(1412)에 포함된 LPG(1410)를 통해 SSH VCN(1412)(예를 들어, 도 11의 SSH VCN(1112))에 통신가능하게 결합될 수 있는 LPG(1410)(예를 들어, 도 11의 LPG(1110))를 포함할 수 있다. SSH VCN(1412)은 SSH 서브넷(1414)(예를 들어, 도 11의 SSH 서브넷(1114))을 포함할 수 있으며, SSH VCN(1412)는 제어 평면 VCN(1416)에 포함된 LPG(1410)를 통해 제어 평면 VCN(1416)(예를 들어, 도 11의 제어 평면 VCN(1116))에 그리고 데이터 평면 VCN(1418)에 포함된 LPG(1410)를 통해 데이터 평면 VCN(1418)(예를 들어, 도 11의 데이터 평면 VCN(1118))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1416) 및 데이터 평면 VCN(1418)은 서비스 테넌시(1419)(예를 들어, 도 11의 서비스 테넌시(1119))에 포함될 수 있다.

[0211] 제어 평면 VCN(1416)은, LB 서브셋(들)(1422)(예를 들어, 도 11의 LB 서브셋(들)(1122))을 포함할 수 있는 제어 평면 DMZ 계층(1420)(예를 들어, 도 11의 제어 평면 DMZ 계층(1120)), 앱 서브넷(들)(1426)(예를 들어, 도 11의 앱 서브넷(들)(1126))을 포함할 수 있는 제어 평면 앱 계층(1424)(예를 들어, 도 11의 제어 평면 앱 계층(1124)), DB 서브넷(들)(1430)(예를 들어, 도 13의 DB 서브넷(들)(1330))을 포함할 수 있는 제어 평면 데이터 계층(1428)(예를 들어, 도 11의 제어 평면 데이터 계층(1128))을 포함할 수 있다. 제어 평면 DMZ 계층(1420)에 포함된 LB 서브넷(들)(1422)은 제어 평면 앱 계층(1424)에 포함된 앱 서브넷(들)(1426) 및 제어 평면 VCN(1416)에 포함될 수 있는 인터넷 게이트웨이(1434)(예를 들어, 도 11의 인터넷 게이트웨이(1134))에 통신가능하게 결합될 수 있으며, 앱 서브넷(들)(1426)은 제어 평면 데이터 계층(1428)에 포함된 DB 서브넷(들)(1430), 서비스 게이트 웨이(1436)(예를 들어, 도 11의 서비스 게이트웨이) 및 네트워크 어드레스 변환(NAT) 게이트웨이(1438)(예를 들어, 도 11의 NAT 게이트웨이(1138))에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1416)은 서비스 게이트웨이(1436) 및 NAT 게이트웨이(1438)를 포함할 수 있다.

[0212] 데이터 평면 VCN(1418)은 데이터 평면 앱 계층(1446)(예를 들어, 도 11의 데이터 평면 앱 계층(1146)), 데이터 평면 DMZ 계층(1448)(예를 들어, 도 11의 데이터 평면 DMZ 계층(1148)), 및 데이터 평면 데이터 계층(1450)(예를 들어, 도 11의 데이터 평면 데이터 계층(1150))을 포함할 수 있다. 데이터 평면 DMZ 계층(1448)은, 데이터 평면 앱 계층(1446)의 신뢰할 수 있는 앱 서브넷(들)(1460)(예를 들어, 도 13의 신뢰할 수 있는 앱 서브넷(들)(1360))과 신뢰할 수 없는 앱 서브넷(들)(1462)(예를 들어, 도 13의 신뢰할 수 없는 앱 서브넷(들)(1362)), 및 데이터 평면 VCN(1418)에 포함된 인터넷 게이트웨이(1434)에 통신가능하게 결합될 수 있는 LB 서브넷(들)(1422)을 포함할 수 있다. 신뢰할 수 있는 앱 서브넷(들)(1460)은 데이터 평면 VCN(1418)에 포함된 서비스 게이트웨이(1436), 데이터 평면 VCN(1418)에 포함된 NAT 게이트웨이(1438), 및 데이터 평면 데이터 계층(1450)에 포함된 DB 서브넷(들)(1430)에 통신가능하게 결합될 수 있다. 신뢰할 수 없는 앱 서브넷(들)(1462)은 데이터 평면 VCN(1418)에 포함된 서비스 게이트웨이(1436) 및 데이터 평면 데이터 계층(1450)에 포함된 DB 서브넷(들)(1430)에 통신가능하게 결합될 수 있다. 데이터 평면 데이터 계층(1450)은, 데이터 평면 VCN(1418)에 포함된 서비스 게이트웨이(1436)에 통신가능하게 결합될 수 있는 DB 서브넷(들)(1430)을 포함할 수 있다.

[0213] 신뢰할 수 없는 앱 서브넷(들)(1462)은, 신뢰할 수 없는 앱 서브넷(들)(1462) 내에 상주하는 테넌트 가상 머신(VM)들(1466(1)-(N))에 통신가능하게 결합될 수 있는 1차 VNIC들(1464(1)-(N))을 포함할 수 있다. 각각의 테넌트 VM(1466(1)-(N))은 개별적인 컨테이너(1467(1)-(N))에서 코드를 실행할 수 있으며, 컨테이너 출구 VCN(1468)에 포함될 수 있는 데이터 평면 앱 계층(1446)에 포함될 수 있는 앱 서브넷(1426)에 통신가능하게 결합될 수 있다. 개별적인 2차 VNIC들(1472(1)-(N))은 데이터 평면 VCN(1418)에 포함된 신뢰할 수 없는 앱 서브넷(들)(1462)과 컨테이너 출구 VCN(1468)에 포함된 앱 서브넷 사이의 통신을 가능하게 할 수 있다. 컨테이너 출구 VCN은, 공용 인터넷(1454)(예를 들어, 도 11의 공용 인터넷(1154))에 통신가능하게 결합될 수 있는 NAT 게이트웨이(1438)를 포함할 수 있다.

[0214] 제어 평면 VCN(1416)에 포함되고 데이터 평면 VCN(1418)에 포함된 인터넷 게이트웨이(1434)는, 공용 인터넷(1454)에 통신가능하게 결합될 수 있는 메타데이터 관리 서비스(1452)(예를 들어, 도 11의 메타데이터 관리 시스템(1152))에 통신가능하게 결합될 수 있다. 공용 인터넷(1454)은, 제어 평면 VCN(1416)에 포함되고 데이터 평면 VCN(1418)에 포함된 NAT 게이트웨이(1438)에 통신가능하게 결합될 수 있다. 제어 평면 VCN(1416)에 포함되고 데이터 평면 VCN(1418)에 포함된 서비스 게이트웨이(1436)는 클라우드 서비스들(1456)에 통신가능하게 결합될 수 있다.

[0215] 일부 예들에서, 도 14의 블록도(1400)의 아키텍처에 의해 예시된 패턴은 도 13의 블록도(1300)의 아키텍처에 의해 예시된 패턴에 대한 예외로서 간주될 수 있으며, IaaS 제공자가 고객과 직접적으로 통신할 수 없는 경우(예를 들어, 분리된 지역) IaaS 제공자의 고객에게 바람직할 수 있다. 각각의 고객에 대한 VM들(1466(1)-(N))에 포함된 개별적인 컨테이너들(1467(1)-(N))은 고객에 의해 실시간으로 액세스될 수 있다. 컨테이너들(1467(1)-(N))은, 컨테이너 출구 VCN(1468)에 포함될 수 있는 데이터 평면 앱 계층(1446)의 앱 서브넷(들)(1426)에 포함된 개별적인 2차 VNIC들(1472(1)-(N))에 대한 호출들을 만들도록 구성될 수 있다. 2차 VNIC들(1472(1)-(N))은, 공용 인터넷(1454)으로 호출들을 송신할 수 있는 NAT 게이트웨이(1438)로 호출들을 송신할 수 있다. 이러한 예에서, 고객에 의해 실시간으로 액세스될 수 있는 컨테이너들(1467(1)-(N))은 제어 평면 VCN(1416)으로부터 격리될 수 있고, 데이터 평면 VCN(1418)에 포함된 다른 엔티티들로부터 격리될 수 있다. 컨테이너들(1467(1)-(N))은 또한 다른 고객들의 자원들로부터 격리될 수 있다.

[0216] 다른 예들에서, 고객은 클라우드 서비스들(1456)을 호출하기 위해 컨테이너들(1467(1)-(N))을 사용할 수 있다. 이러한 예에서, 고객은, 클라우드 서비스들(1456)으로부터 서비스를 요청하는 컨테이너들(1467(1)-(N))에서 코드를 실행할 수 있다. 컨테이너들(1467(1)-(N))은, 요청을 공용 인터넷(1454)으로 송신할 수 있는 NAT 게이트웨이로 요청을 송신할 수 있는 2차 VNIC들(1472(1)-(N))로 이러한 요청을 송신할 수 있다. 공용 인터넷(1454)은 요청을 인터넷 게이트웨이(1434)를 통해 제어 평면 VCN(1416)에 포함된 LB 서브셋(들)(1422)으로 송신할 수 있다. 요청이 유효하다고 결정하는 것에 응답하여, LB 서브넷(들)은, 서비스 게이트웨이(1436)를 통해 클라우드 서비스들(1456)로 요청을 송신할 수 있는 앱 서브넷(들)(1426)로 요청을 송신할 수 있다.

[0217] 도면들에 도시된 IaaS 아키텍처들(1100, 1200, 1300, 1400)이 도시된 것들과는 다른 구성요소들을 가질 수 있다는 것이 이해되어야 한다. 추가로, 도면에 도시된 실시예는 본 발명의 일 실시예를 통합할 수 있는 클라우드 인프라스트럭처 시스템의 단지 일부 예들이다. 일부 다른 실시예들에서, IaaS 시스템들은 도면들에 도시된 것보다 더 많거나 또는 더 적은 구성요소들을 가질 수 있거나, 2개 이상의 구성요소들을 결합할 수 있거나, 또는 구성요소들의 상이한 구성 또는 배열을 가질 수 있다.

[0218] 특정 실시예들에서, 본원에서 설명된 IaaS 시스템들은, 셀프-서비스(self-service)의, 가입-기반(subscription-based)의, 탄력적 스케일러블(scalable)의, 신뢰할 수 있는, 고도로 이용가능하며, 안전한 방식으로 고객에게 전달되는 애플리케이션들, 미들웨어, 및 데이터베이스 서비스 제공(offering)들의 스위트(suite)를 포함할 수 있다. 이러한 IaaS 시스템의 일 예는 본 양수인에 의해 제공되는 오라클 클라우드 인프라스트럭처(Oracle Cloud Infrastructure; OCI)이다.

[0219] 도 15는, 다양한 실시예들이 구현될 수 있는 예시적인 컴퓨터 시스템(1500)을 예시한다. 시스템(1500)은 이상에서 설명된 컴퓨터 시스템들 중 임의의 것을 구현하기 위하여 사용될 수 있다. 도면에 도시된 바와 같이, 컴퓨터 시스템(1500)은 버스 서브시스템(1502)을 통해 복수의 주변 서브시스템들과 통신하는 프로세싱 유닛(1504)을 포함한다. 이러한 주변 서브시스템들은 프로세싱 가속 유닛(1506), I/O 서브시스템(1508), 스토리지 서브시스템(1518) 및 통신 서브시스템(1524)을 포함할 수 있다. 스토리지 서브시스템(1518)은 유형적인 컴퓨터-판독가능 저장 매체(1522) 및 시스템 메모리(1510)를 포함한다.

[0220] 버스 서브시스템(1502)은 컴퓨터 시스템(1500)의 다양한 구성요소들 및 서브시스템들이 의도된 바와 같이 서로 통신하는 것을 가능하게 하기 위한 메커니즘을 제공한다. 버스 서브시스템(1502)이 단일 버스로서 개략적으로 도시되었지만, 버스 서브시스템의 대안적인 실시예들은 복수의 버스들을 사용할 수 있다. 버스 서브시스템(1502)은, 다양한 버스 아키텍처들 중 임의의 것을 사용하는 메모리 버스 또는 메모리 제어기, 주변기기 버스, 및 로컬 버스를 포함하는 몇몇 유형들의 버스 구조들 중 임의의 버스 구조일 수 있다. 예를 들어, 이러한 아키텍처들은, 산업 표준 아키텍처(Industry Standard Architecture; ISA) 버스, 마이크로 채널 아키텍처(Micro Channel Architecture; MCA) 버스, 개량 ISA(Enhanced ISA; EISA) 버스, 비디오 전자공학 표준 위원회(Video Electronics Standards Association; VESA) 로컬 버스, 및 주변 구성요소 상호연결(Peripheral Component Interconnect; PCI) 버스를 포함할 수 있으며, 이들은 IEEE P1386.1 표준에 대하여 제조되는 메자닌 버스(Mezzanine bus)로서 구현될 수 있다.

[0221] 하나 이상의 집적 회로들(예를 들어, 통상적인 마이크로프로세서 또는 마이크로제어기)로서 구현될 수 있는 프로세싱 유닛(1504)은 컴퓨터 시스템(1500)의 동작을 제어한다. 하나 이상의 프로세서들이 프로세싱 유닛(1504) 내에 포함될 수 있다. 이러한 프로세서들은 단일 코어 또는 다중코어 프로세서들을 포함할 수 있다. 특정 실시예들에 있어서, 프로세싱 유닛(1504)은 각각의 프로세싱 유닛 내에 포함된 단일 또는 다중코어 프로세서들을 갖는 하나 이상의 독립적인 프로세싱 유닛들(1532 및/또는 1534)로서 구현될 수 있다. 다른 실시예들에 있어서, 프로세싱 유닛(1504)은 또한 2개의 듀얼-코어 프로세서들을 단일 칩 내에 통합함으로써 형성된 쿼드-코어 프로세싱 유닛으로서 구현될 수 있다.

[0222] 다양한 실시예들에 있어서, 프로세싱 유닛(1504)은 프로그램 코드에 응답하여 다양한 프로그램들을 실행할 수 있으며, 프로그램들 또는 프로세스들의 동시 다중 실행을 유지할 수 있다. 임의의 주어진 시점에, 실행될 프로그램 코드의 전부 또는 일부가 프로세서(들)(1504) 내에 및/또는 스토리지 서브시스템(1518) 내에 상주할 수 있다. 적절한 프로그래밍을 통하여, 프로세서(들)(1504)는 이상에서 설명된 다양한 기능들을 제공할 수 있다. 컴퓨터 시스템(1500)은, 디지털 신호 프로세서(digital signal processor; DSP), 특수-목적 프로세서, 및/또는 유사한 것을 포함할 수 있는 프로세싱 가속 유닛(1506)을 추가적으로 포함할 수 있다.

[0223] I/O 서브시스템(1508)은 사용자 인터페이스 입력 디바이스들 및 사용자 인터페이스 출력 디바이스들을 포함할 수 있다. 사용자 인터페이스 입력 디바이스들은, 키보드, 포인팅 디바이스들 예컨대 마우스 또는 트랙볼, 터치패드 또는 디스플레이 내에 통합된 터치 스크린, 스크롤 휠, 클릭 휠, 다이얼, 버튼, 스위치, 키패드, 음성 명령 인식 시스템들을 가진 오디오 입력 디바이스들, 마이크들, 및 다른 유형들의 입력 디바이스들을 포함할 수 있다. 사용자 인터페이스 입력 디바이스들은, 예를 들어, 사용자들이 제스처들 및 구두(spoken) 명령들을 사용하는 자연스러운 사용자 인터페이스를 통해, Microsoft Xbox® 360 게임 제어기와 같은, 입력 디바이스를 제어하고 이와 상호작용하는 것을 가능하게 하는 Microsoft Kinect® 모션 센서와 같은 모션 센싱 및/또는 제스처 인식 디바이스들을 포함할 수 있다. 사용자 인터페이스 입력 디바이스들은 또한, 사용자들로부터 눈 움직임(eye activity)(예를 들어, 사진을 찍는 동안의 및/또는 메뉴를 선택하는 동안의 '깜박임')을 검출하고 눈 제스처들을 입력 디바이스(예를 들어, Google Glass®) 내로의 입력으로서 변환하는 Google Glass® 눈 깜박임 검출기와 같은 눈 제스처 인식 디바이스들을 포함할 수 있다. 추가적으로, 사용자 인터페이스 입력 디바이스들은, 사용자들이 음성 명령들을 통하여 음성 인식 시스템(예를 들어, Siri® 네비게이터(navigator))과 상호작용하는 것을 가능하게 하는 음성 인식 센싱 디바이스들을 포함할 수 있다.

[0224] 사용자 인터페이스 입력 디바이스들은 또한, 비제한적으로, 3차원(3D) 마우스들, 조이스틱들 또는 포인팅 스틱

들, 게임패드들 및 그래픽 태블릿들, 및 음향/시각 디바이스들 예컨대 스피커들, 디지털 카메라들, 디지털 캠코더들, 휴대용 매체 플레이어들, 웹캠들, 이미지 스캐너들, 핑거프린트 스캐너들, 바코드 리더 3D 스캐너들, 3D 프린터들, 레이저 거리계들, 및 시선 추적 디바이스들을 포함할 수 있다. 추가적으로, 사용자 인터페이스 입력 디바이스들은, 예를 들어, 의료 이미징 입력 디바이스들 예컨대 컴퓨터 단층촬영, 자기 공명 이미징, 양전자 방출 단층촬영, 의료 초음파 검사 디바이스들을 포함할 수 있다. 사용자 인터페이스 입력 디바이스들은 또한, 예를 들어, 오디오 입력 디바이스들 예컨대 MIDI 키보드들, 디지털 악기들, 및 유사한 것을 포함할 수 있다.

[0225] 사용자 인터페이스 출력 디바이스들은 디스플레이 서브시스템, 표시등들, 또는 비-시각적 디스플레이들 예컨대 오디오 출력 디바이스들, 등을 포함할 수 있다. 디스플레이 서브시스템은 음극선관(cathode ray tube; CRT), 액정 디스플레이(liquid crystal display; LCD) 또는 플라즈마 디스플레이를 사용하는 것과 같은 평면-패널 디바이스, 프로젝션 디바이스, 터치 스크린, 및 유사한 것일 수 있다. 일반적으로, 용어 "출력 디바이스"의 사용은 컴퓨터 시스템(1500)으로부터 사용자 또는 다른 컴퓨터로 정보를 출력하기 위한 모든 가능한 유형들의 디바이스들 및 메커니즘들을 포함하도록 의도된다. 예를 들어, 사용자 인터페이스 출력 디바이스들은, 비제한적으로, 시각적으로 텍스트, 그래픽들 및 오디오/비디오 정보를 전달하는 다양한 디스플레이 디바이스들, 예컨대 모니터들, 프린터들, 스피커들, 헤드폰들, 자동차 네비게이션 시스템들, 플로터(plotter)들, 음성 출력 디바이스들, 및 모뎀들을 포함할 수 있다.

[0226] 컴퓨터 시스템(1500)은, 시스템 메모리(1510) 내에 현재 위치되어 있는 것으로 도시되는 소프트웨어 요소들을 포함하는 스토리지 서브시스템(1518)을 포함할 수 있다. 시스템 메모리(1510)는, 프로세싱 유닛(1504) 상에 로딩가능하며 실행가능한 프로그램 명령어들뿐만 아니라 이러한 프로그램들의 실행 동안 생성되는 데이터를 저장할 수 있다.

[0227] 컴퓨터 시스템(1500)의 구성 및 유형에 따라서, 시스템 메모리(1510)는 (랜덤 액세스 메모리(random access memory; RAM)와 같은) 휘발성일 수 있거나 및/또는 (판독-전용 메모리(read-only memory; ROM), 플래시 메모리, 등과 같은) 비-휘발성일 수 있다. RAM은 전형적으로 프로세싱 유닛(1504)에 의해 현재 실행되고 동작되고 있거나 및/또는 이에 즉시 액세스가능한 데이터 및/또는 프로그램 모듈들을 포함한다. 일부 구현예들에 있어서, 시스템 메모리(1510)는 복수의 상이한 유형들의 메모리들, 예컨대 정적 랜덤 액세스 메모리(static random access memory; SRAM) 또는 동적 랜덤 액세스 메모리(dynamic random access memory; DRAM)를 포함할 수 있다. 일부 구현예들에 있어서, 예컨대 기동 동안에 컴퓨터 시스템(1500) 내의 요소들 사이에서 정보를 전송하는 것을 돕는 기본 루틴들을 포함하는 기본 입력/출력 시스템(basic input/output system; BIOS)은 전형적으로 ROM 내에 저장될 수 있다. 예로서 그리고 비제한적으로, 시스템 메모리(1510)는 또한, 클라이언트 애플리케이션들, 웹 브라우저들, 중간-계층 애플리케이션들, 관계형 데이터 베이스 관리 시스템(relational database management system; RDBMS)들, 등을 포함할 수 있는 애플리케이션 프로그램들(1512), 프로그램 데이터(1514), 및 운영 체제(1516)를 예시한다. 예로서, 운영 체제(1516)는, 다양한 버전들의 Microsoft Windows®, Apple Macintosh®, 및/또는 리눅스 운영 체제들, (비제한적으로 다양한 GNU/리눅스 운영 체제들, Google Chrome® OS, 및 유사한 것을 포함하는) 다양한 상용-이용가능 UNIX® 또는 UNIX-유사 운영 체제들 및/또는 모바일 운영 체제들 예컨대 iOS, Windows® Phone, Android® OS, BlackBerry® 15 OS, 및 Palm® OS 운영 체제들을 포함할 수 있다.

[0228] 스토리지 서브시스템(1518)은 또한 일부 실시예들의 기능을 제공하는 기본 프로그래밍 및 데이터 구성물들을 저장하기 위한 유형적인 컴퓨터-판독가능 저장 매체를 제공할 수 있다. 프로세서에 의해 실행될 때 이상에서 설명된 기능을 제공하는 소프트웨어(프로그램들, 코드 모듈들, 명령어들)가 스토리지 서브시스템(1518) 내에 저장될 수 있다. 이러한 소프트웨어 모듈들 또는 명령어들이 프로세싱 유닛(1504)에 의해 실행될 수 있다. 스토리지 서브시스템(1518)은 또한 본 개시내용에 따라 사용되는 데이터를 저장하기 위한 저장소를 제공할 수 있다.

[0229] 스토리지 서브시스템(1500)은 또한, 추가적으로 컴퓨터-판독가능 저장 매체(1522)에 연결될 수 있는 컴퓨터-판독가능 저장 매체 리더(1520)를 포함할 수 있다. 시스템 메모리(1510)와 함께 그리고 선택적으로 이와 조합되어, 컴퓨터-판독가능 저장 매체(1522)는, 컴퓨터-판독가능 정보를 일시적으로 및/또는 더 영구적으로 포함하고, 저장하며, 송신하고, 및 검색하기 위한 저장 매체들에 더하여 원격, 로컬, 고정, 및/또는 착탈가능 저장 디바이스들을 포괄적으로 나타낼 수 있다.

[0230] 코드, 또는 코드의 부분들을 포함하는 컴퓨터-판독가능 저장 매체(1522)는 또한, 비제한적으로, 정보의 저장 및/또는 송신을 위하여 임의의 방법 또는 기술로 구현된 휘발성 및 비-휘발성, 착탈가능 및 비-착탈가능 매체와 같은 저장 매체 및 통신 매체를 포함하는 당업계에서 알려지거나 또는 사용되는 임의의 적절한 매체를 포함할 수 있다. 이는 유형의 컴퓨터-판독가능 저장 매체, 예컨대 RAM, ROM, 전기 소거가능 프로그램가능

ROM(electronically erasable programmable ROM; EEPROM), 플래시 메모리 또는 다른 메모리 기술품, CD-ROM, 디지털 다기능 디스크(digital versatile disk; DVD), 또는 광 저장장치, 자기 카세트들, 자기 테이프, 자기 디스크 저장장치 또는 다른 자기 저장 디바이스들, 또는 다른 유형의 컴퓨터 판독가능 매체를 포함할 수 있다. 이는 또한 비유형적인 컴퓨터-판독가능 매체, 예컨대 데이터 신호들, 데이터 송신들, 또는 희망되는 정보를 송신하기 위해 사용될 수 있으며 컴퓨팅 시스템(1500)에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다.

[0231] 예로서, 컴퓨터-판독가능 저장 매체(1522)는, 비-착탈가능 비휘발성 자기 매체로부터 판독하거나 또는 이에 기입하는 하드 디스크 드라이브, 착탈가능 비휘발성 자기 디스크로부터 판독하거나 또는 이에 기입하는 자기 디스크 드라이브, 및 착탈가능 비휘발성 광 디스크 예컨대 CD ROM, DVD, 및 Blu-Ray® 디스크, 또는 다른 광 매체로부터 판독하거나 또는 이에 기입하는 광 디스크 드라이브를 포함할 수 있다. 컴퓨터-판독가능 저장 매체(1522)는, 비제한적으로, Zip® 드라이브들, 플래시 메모리 카드들, 범용 직렬 버스(universal serial bus; USB) 플래시 드라이브들, 보안 디지털(secure digital; SD) 카드들, DVD 디스크들, 디지털 비디오 테이프, 및 유사한 것을 포함할 수 있다. 컴퓨터-판독가능 저장 매체(1522)는 또한, 비-휘발성 메모리 기반 고체-상태 드라이브(solid-state drive; SSD)들 예컨대 플래시-메모리 기반 SSD들, 기업 플래시 드라이브들, 고체 상태 ROM, 및 유사한 것, 휘발성 메모리 기반 SSD들 예컨대 고체 상태 RAM, 동적 RAM, 정적 RAM, DRAM-기반 SSD들, 자기저항성 RAM(magnetoresistive RAM; MRAM) SSD들, 및 DRAM 및 플래시 메모리 기반 SSD들의 조합을 사용하는 하이브리드 SSD들을 포함할 수 있다. 디스크 드라이브들 및 그들의 연관된 컴퓨터-판독가능 매체는 컴퓨터-판독가능 명령어들, 데이터 구조들, 프로그램 모듈들, 및 컴퓨터 시스템(1500)에 대한 다른 데이터의 비-휘발성 저장을 제공할 수 있다.

[0232] 통신 서브시스템(1524)은 다른 컴퓨터 시스템들 및 네트워크들에 대한 인터페이스를 제공한다. 통신 서브시스템(1524)은 컴퓨터 시스템(1500)으로부터 다른 시스템들로 데이터를 송신하고 이로부터 데이터를 수신하기 위한 인터페이스로서 역할한다. 예를 들어, 통신 서브시스템(1524)은 컴퓨터 시스템(1500)이 인터넷을 통해 하나 이상의 디바이스들에 연결하는 것을 가능하게 할 수 있다. 일부 실시예들에 있어서, 통신 서브시스템(1524)은 (예를 들어, 셀룰러 전화기 기술, 진보된 데이터 네트워크 기술, 예컨대 3G, 4G 또는 EDGE(enhanced data rates for global evolution), WiFi(IEEE 802.11 패밀리 표준들, 또는 다른 모바일 통신 기술들, 또는 이들의 임의의 조합)을 사용하여) 무선 음성 및/또는 데이터 네트워크들에 액세스하기 위한 무선 주파수(radio frequency; RF) 트랜시버 구성요소들, 위성 위치확인 시스템(global positioning system; GPS) 수신기 구성요소들, 및/또는 다른 구성요소들을 포함할 수 있다. 일부 실시예들에 있어서, 통신 서브시스템(1524)은 무선 인터페이스에 더하여 또는 그 대신에 유선 네트워크 연결(예를 들어, 이더넷)을 제공할 수 있다.

[0233] 일부 실시예들에 있어서, 통신 서브시스템(1524)은 또한 컴퓨터 시스템(1500)을 사용할 수 있는 하나 이상의 사용자들을 대표하여 구조화된 및/또는 구조화되지 않은 데이터 피드들(1526), 이벤트 스트림들(1528), 이벤트 업데이트들(1530), 및 그와 유사한 것의 형태의 입력 통신을 수신할 수 있다.

[0234] 예로서, 통신 서브시스템(1524)은 소셜 네트워크들 및/또는 다른 통신 서비스들의 사용자들로부터의 실-시간 데이터 피드들(1526) 예컨대 Twitter® 피드들, Facebook® 업데이트들, 웹 피드들 예컨대 리치 사이트 서머리(Rich Site Summary; RSS) 피드들, 및/또는 하나 이상의 제3 자 정보 소스들로부터의 실-시간 업데이트들을 수신하도록 구성될 수 있다.

[0235] 추가적으로, 통신 서브시스템(1524)은 또한, 사실상 명시적인 종료를 갖지 않는 제한이 없거나 또는 연속적일 수 있는 실-시간 이벤트들 및/또는 이벤트 업데이트들(1530)의 이벤트 스트림들(1528)을 포함할 수 있는 연속적인 데이터 스트림들의 형태로 데이터를 수신하도록 구성될 수 있다. 연속적인 데이터를 생성하는 애플리케이션들의 예들은, 예를 들어, 센서 데이터 애플리케이션들, 금융 시세표시기들, 네트워크 성능 측정 툴들(예를 들어, 네트워크 모니터링 및 트래픽 관리 애플리케이션들), 클릭스트림 분석 툴들, 자동차 트래픽 모니터링, 및 유사한 것을 포함할 수 있다.

[0236] 통신 서브시스템(1524)은 또한, 구조화되거나 및/또는 구조화되지 않은 데이터 피드들(1526), 이벤트 스트림들(1528), 이벤트 업데이트들(1530), 및 유사한 것을 컴퓨터 시스템(1500)에 결합된 하나 이상의 스트리밍 데이터 소스 컴퓨터들과 통신할 수 있는 하나 이상의 데이터베이스들로 출력하도록 구성될 수 있다.

[0237] 컴퓨터 시스템(1500)은, 핸드헬드 휴대용 디바이스(예를 들어, iPhone® 셀룰러 폰, iPad® 컴퓨팅 태블릿, PDA), 웨어러블 디바이스(예를 들어, Google Glass® 머리 착용형 디스플레이), PC, 워크스테이션, 메인프레임, 키오스크, 서버 랙, 또는 임의의 다른 데이터 프로세싱 시스템을 포함하는 다양한 유형들 중 임의의 유형일 수

있다.

[0238] 컴퓨터들 및 네트워크들의 계속해서 변화하는 성질에 기인하여, 도면에 도시된 컴퓨터 시스템(1500)의 설명은 오로지 특정한 일 예로서만 의도된다. 도면에 도시된 시스템보다 더 많거나 또는 더 적은 구성요소들을 갖는 다수의 다른 구성들이 가능하다. 예를 들어, 커스텀화된 하드웨어가 또한 사용될 수 있거나 및/또는 특정 요소들이 하드웨어, 펌웨어, (애플릿(applet)들을 포함하는) 소프트웨어, 또는 이들의 조합으로 구현될 수 있다. 추가로, 네트워크 입력/출력 디바이스들과 같은 다른 컴퓨팅 디바이스들에 대한 연결이 이용될 수 있다. 본원에 제공되는 개시 및 교시들에 기초하여, 당업자는 다양한 실시예들을 구현하기 위한 다른 방식들 및/또는 방법들을 인식할 것이다.

[0239] 실시예들은, 프로세서에 의해 실행될 때, 프로세서가 본 개시내용에서 설명된 방법들 중 임의의 것을 수행하게 하는 컴퓨터 프로그램 명령어들을 포함하는 컴퓨터 프로그램 제품을 사용함으로써 구현될 수 있다.

[0240] 특정 실시예들이 설명되었지만, 다양한 수정예들, 대안예들, 대안적인 구성들, 및 등가물들이 또한 본 개시의 범위 내에 포괄된다. 실시예들은 정확한 특정 데이터 프로세싱 환경들 내에서 동작하도록 제한되는 것이 아니라, 복수의 데이터 프로세싱 환경들 내에서 자유롭게 동작할 수 있다. 추가적으로, 실시예들이 특정한 일련의 트랜잭션(transaction)들 및 단계들을 사용하여 설명되었지만, 본 개시의 범위가 설명된 일련의 트랜잭션들 및 단계들로 한정되지 않는다는 것이 당업자들에게 명백할 것이다. 이상에서 설명된 실시예들의 다양한 특징들 및 측면들이 개별적으로 또는 함께 사용될 수 있다.

[0241] 추가로, 실시예들이 하드웨어 및 소프트웨어의 특정한 조합을 사용하여 설명되었지만, 하드웨어 및 소프트웨어의 다른 조합들이 또한 본 개시의 범위 내에 있다는 것이 이해되어야 한다. 실시예들은 오로지 하드웨어로만, 또는 오로지 소프트웨어로만, 또는 이들의 조합들을 사용하여 구현될 수 있다. 본 명세서에서 설명된 다양한 프로세스들은 동일한 프로세서 또는 임의의 조합의 상이한 프로세서들 상에 구현될 수 있다. 따라서, 구성요소들 또는 모듈들이 특정 동작들을 수행하도록 구성된 것으로 설명되는 경우, 이러한 구성은, 예를 들어, 동작을 수행하기 위한 전자 회로들을 설계함으로써, 동작을 수행하기 위하여 프로그램가능 전자 회로들(예컨대 마이크로프로세서들)을 프로그래밍함으로써, 또는 이들의 임의의 조합에 의해 달성될 수 있다. 프로세스들은 비제한적으로 프로세스-간 통신을 위한 통상적을 기술을 포함하는 다양한 기술들을 사용하여 통신할 수 있으며, 프로세스들의 상이한 쌍들이 상이한 기술들을 사용할 수 있거나, 또는 프로세스들의 동일한 쌍이 상이한 시점에 상이한 기술들을 사용할 수 있다.

[0242] 따라서 본 명세서 및 도면은 제한적인 의미라기보다는 예시적인 의미로 간주되어야 한다. 그러나, 청구항들에 기술되는 바와 같은 광범위한 사상 및 범위로부터 벗어나지 않고 이에 대한 추가들, 대체들, 삭제들, 및 다른 수정들 및 변화들이 이루어질 수 있다는 것이 명백할 것이다. 따라서, 특정 개시 실시예들이 설명되었지만, 이들은 제한적인 것으로 의도되지 않는다. 다양한 수정예들 및 등가물들이 다음의 청구항들의 범위 내에 속한다.

[0243] 개시된 실시예들을 설명하는 맥락에서(특히 다음의 청구항들의 맥락에서) 용어들 "일(a 및 an)"과 "상기(the)" 및 유사한 지시대상들의 사용은, 본원에서 달리 표시되거나 또는 문맥에 의해 명백히 모순되지 않는 한 단수형 및 복수형 둘 모두를 커버하는 것으로 해석되어야 한다. 용어들 "포함하는", "갖는", "구성되는", 및 "함유하는"은, 달리 언급되지 않는 한 개방적인 용어(즉, "포함하지만 이에 한정되지 않는")으로 해석되어야 한다. 용어 "연결되는"은, 어떤 개재물이 있는 경우에도, 부분적으로 또는 전체적으로 어떤 것 내에 포함되거나, 또는 이에 부착되거나, 또는 이와 함께 결합되는 것으로 해석되어야 한다. 본 명세서에서 값들의 범위를 언급하는 것은, 본 명세서에서 달리 표시되지 않는 한, 단지 범위 내에 속하는 각각의 개별 값을 개별적으로 참조하는 속기 방법으로서 역할하도록 의도되며, 각각의 개별적인 값은 마치 이것이 본원에서 개별적으로 언급되는 것과 같이 명세서에 통합된다. 본 명세서에서 설명된 모든 방법은, 본 명세서에서 달리 표시되지 않거나 문맥상 명백히 모순되지 않는 한 임의의 적절한 순서로 수행될 수 있다. 본원에서 제공되는 임의의 및 모든 예들 또는 예시적인 언어(예를 들어, "~와 같은")의 사용은 단지 실시예들을 더 양호하게 조명하도록 의도되며, 달리 청구되지 않는 한, 본 개시의 범위에 제한을 두지 않는다. 본 명세서의 어떤 언어도 본 개시의 실시에 필수적인 임의의 청구되지 않은 요소를 나타내는 것으로 해석되지 않아야 한다.

[0244] 구절 "X, Y, 또는 Z 중 적어도 하나"와 같은 이접적 언어는, 특별히 달리 명시되지 않는 한, 항목, 용어 등이 X, Y, 또는 Z 중 하나, 또는 이들의 조합(예를 들어, X, Y, 및/또는 Z)일 수 있음을 나타내기 위해 일반적으로 사용되는 문맥 내에서 이해되도록 의도된다. 따라서, 그러한 이접적 언어는 일반적으로, 특정 실시예가 각각 존재하기 위해 X 중 적어도 하나, Y 중 적어도 하나, 또는 Z 중 적어도 하나가 필요하다는 것을 의미하도록 의도되지 않는다.

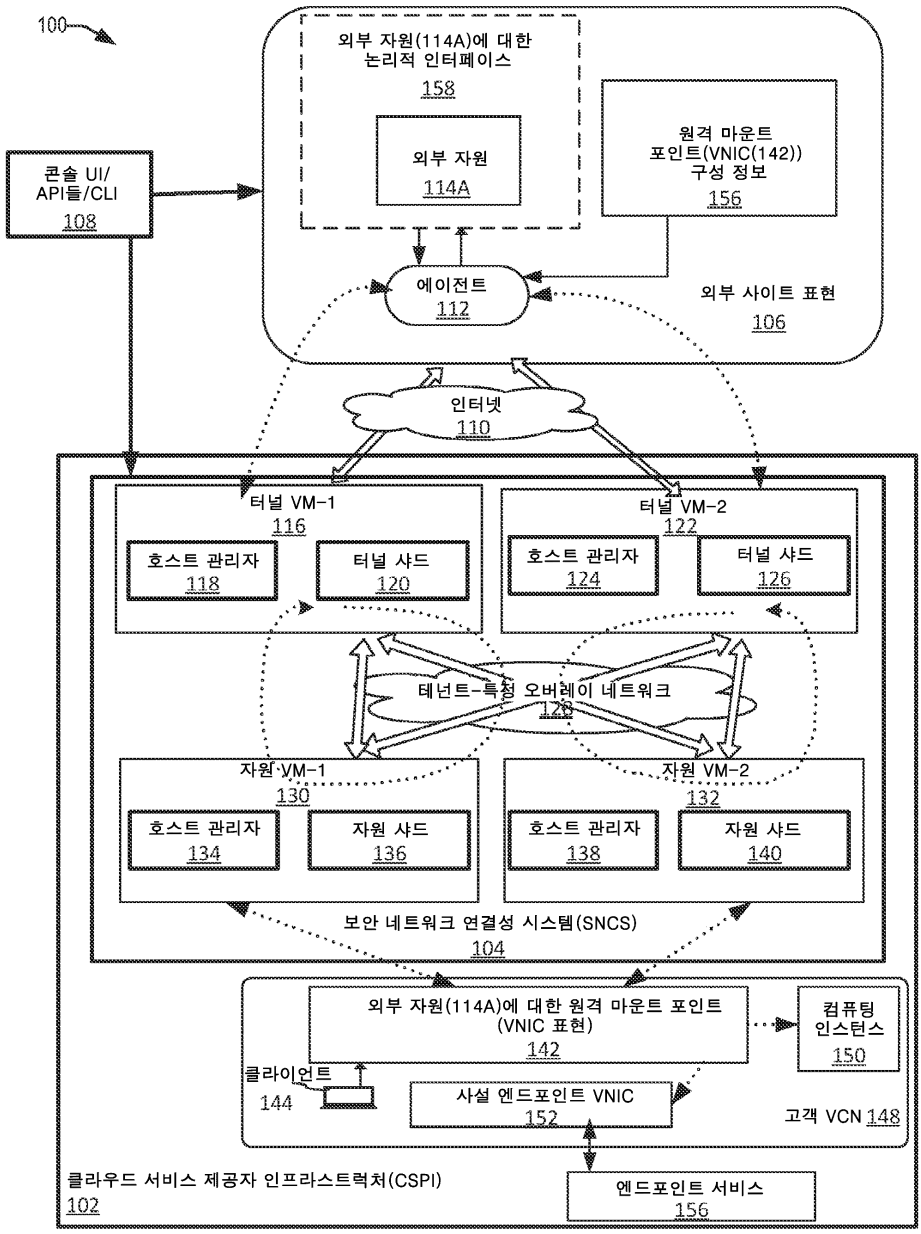
[0245] 본 개시내용을 수행하기 위해 알려진 최적 모드를 포함하여 본 개시내용의 선호되는 실시예들이 본 명세서에서 설명되었다. 이러한 선호되는 실시예들의 변형들은 이상의 설명을 숙독할 때 당업자들에게 명백해질 것이다. 당업자들은 적절한 바와 같이 이러한 변형들을 이용할 수 있어야 하며, 본 개시내용은 본 명세서에서 구체적으로 설명된 것과 달리 실시될 수 있다. 따라서, 본 개시내용은 적용가능한 법률에 의해 허용되는 바와 같이 본 명세서에 첨부된 청구항들에 언급된 주제의 모든 수정예들 및 등가물들을 포함한다. 또한, 이의 모든 가능한 변형예들에서 이상에서 설명된 요소들의 임의의 조합은 따라서 본원에서 달리 표시되지 않는 한 본 개시내용에 의해 포괄된다.

[0246] 본 명세서에서 인용된 간행물들, 특허 출원들 및 특허들을 포함하는 모든 참조문헌들은, 이로써 각각의 참조문헌이 참조로서 포함되도록 개별적으로 그리고 구체적으로 표시되고 그 전체가 본 명세서에서 기술된 것과 동일한 정도로 참조로서 본원에 포함된다.

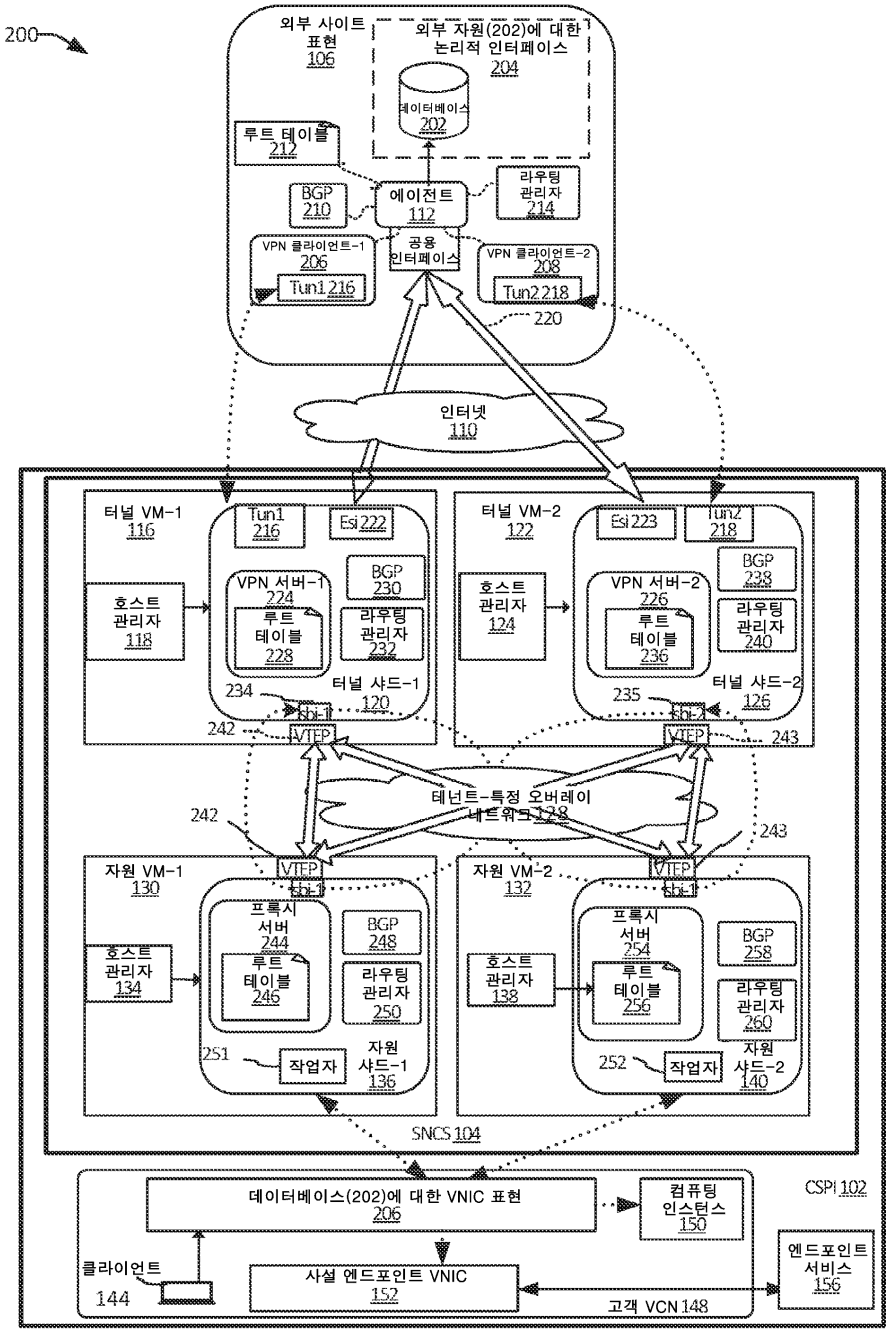
[0247] 이상의 명세서에서, 본 개시내용의 측면들이 본 개시의 특정 실시예들을 참조하여 설명되었지만, 당업자들은 본 개시내용이 이에 한정되지 않는다는 것을 인식할 것이다. 이상에서 설명된 개시내용의 다양한 특징들 및 측면들이 개별적으로 또는 함께 사용될 수 있다. 추가로, 실시예들은 본 명세서의 광범위한 사상 및 범위로부터 벗어나지 않고 본 명세서에서 설명된 것들을 넘어 임의의 수의 환경들 및 애플리케이션들에서 사용될 수 있다. 이에 따라, 본 명세서 및 도면들은 제한적인 것이 아니라 예시적인 것으로 간주되어야 한다.

도면

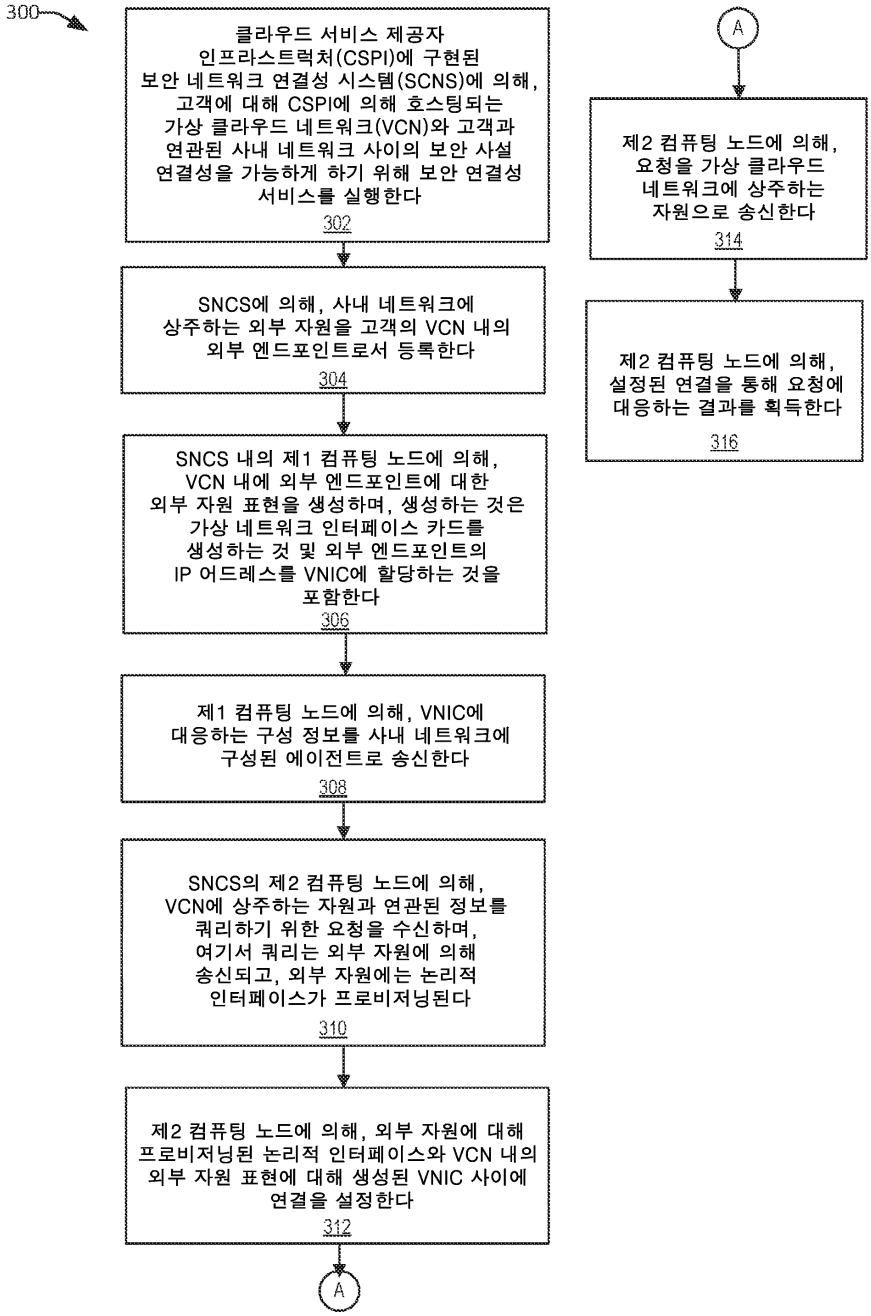
도면1


100
외부 자원(114A)에 대한
논리적 인터페이스
158
외부 자원
114A
원격 마운트
포인트(VNIC(142))
구성 정보
156
콘솔 UI/
API들/CLI
108
에이전트
112
외부 사이트 표현
106
인터넷
110
터널 VM-1
116
호스트 관리자
118
터널 샤드
120
터널 VM-2
122
호스트 관리자
124
터널 샤드
126
테넌트-특정 오버레이 네트워크
128
자원 VM-1
130
호스트 관리자
134
자원 샤드
136
자원 VM-2
132
호스트 관리자
138
자원 샤드
140
보안 네트워크 연결성 시스템(SNCS)
104
외부 자원(114A)에 대한 원격 마운트 포인트
(VNIC 표현)
142
컴퓨팅
인스턴스
150
클라이언트
144
사설 엔드포인트 VNIC
152
고객 VCN 148
클라우드 서비스 제공자 인프라스트럭처(CSPI)
102
엔드포인트 서비스
156

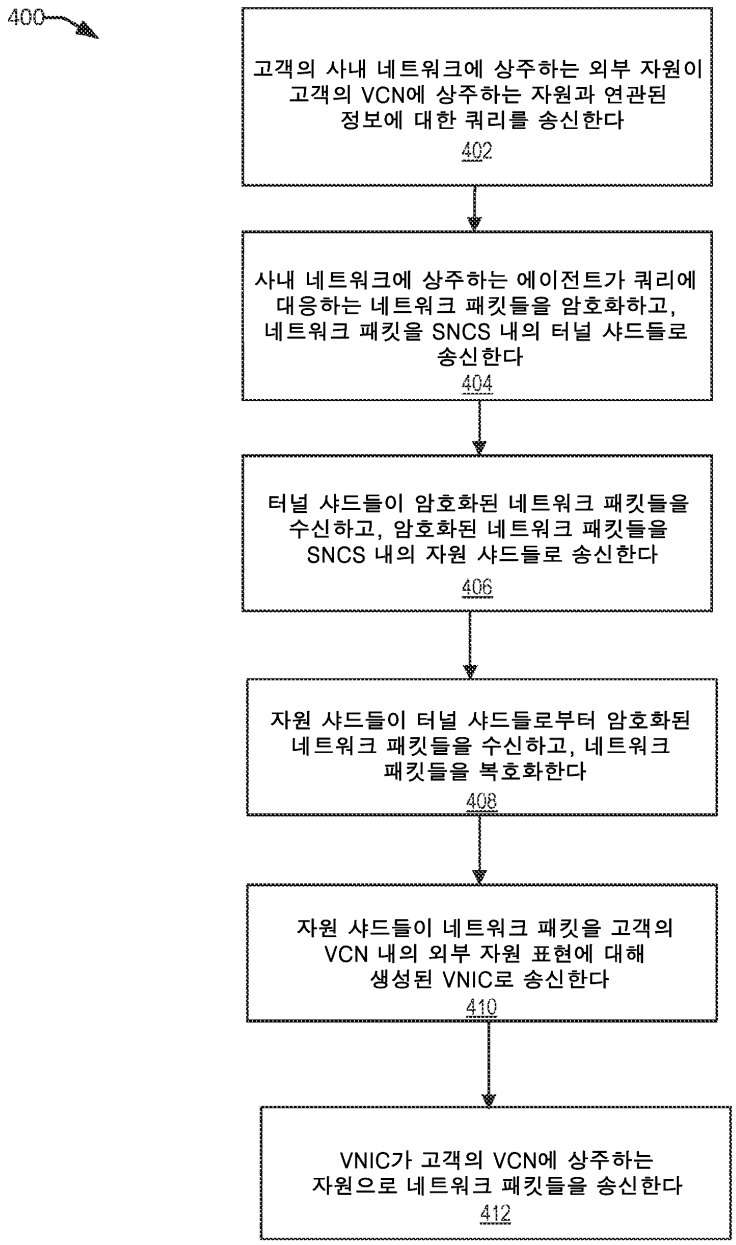
도면2


200
외부 사이트 표현 106
외부 자원(202)에 대한 논리적 인터페이스 204
데이터베이스 202
루트 테이블 212
BGP 210
에이전트 112
라우팅 관리자 214
VPN 클라이언트-1 206
Tun1 216
공용 인터페이스
VPN 클라이언트-2 208
Tun2 218
220
인터넷 110
터널 VM-1 116
Tun1 216
Esi 222
VPN 서버-1 224
BGP 230
루트 테이블 228
라우팅 관리자 232
터널 샤드-1 120
234
242
VTEP
호스트 관리자 118
터널 VM-2 122
Esi 223
Tun2 218
VPN 서버-2 226
BGP 238
루트 테이블 236
라우팅 관리자 240
터널 샤드-2 126
235
243
호스트 관리자 124
테넌트-특정 오버레이 네트워크 128
자원 VM-1 130
프록시 서버 244
BGP 248
루트 테이블 246
라우팅 관리자 250
자원 샤드-1 136
251
작업자
호스트 관리자 134
자원 VM-2 132
프록시 서버 254
BGP 258
루트 테이블 256
라우팅 관리자 260
자원 샤드-2 140
252
호스트 관리자 138
SNCS 104
CSPI 102
데이터베이스(202)에 대한 VNIC 표현 206
컴퓨팅 인스턴스 150
클라이언트 144
사설 엔드포인트 VNIC 152
고객 VCN 148
엔드포인트 서비스 156

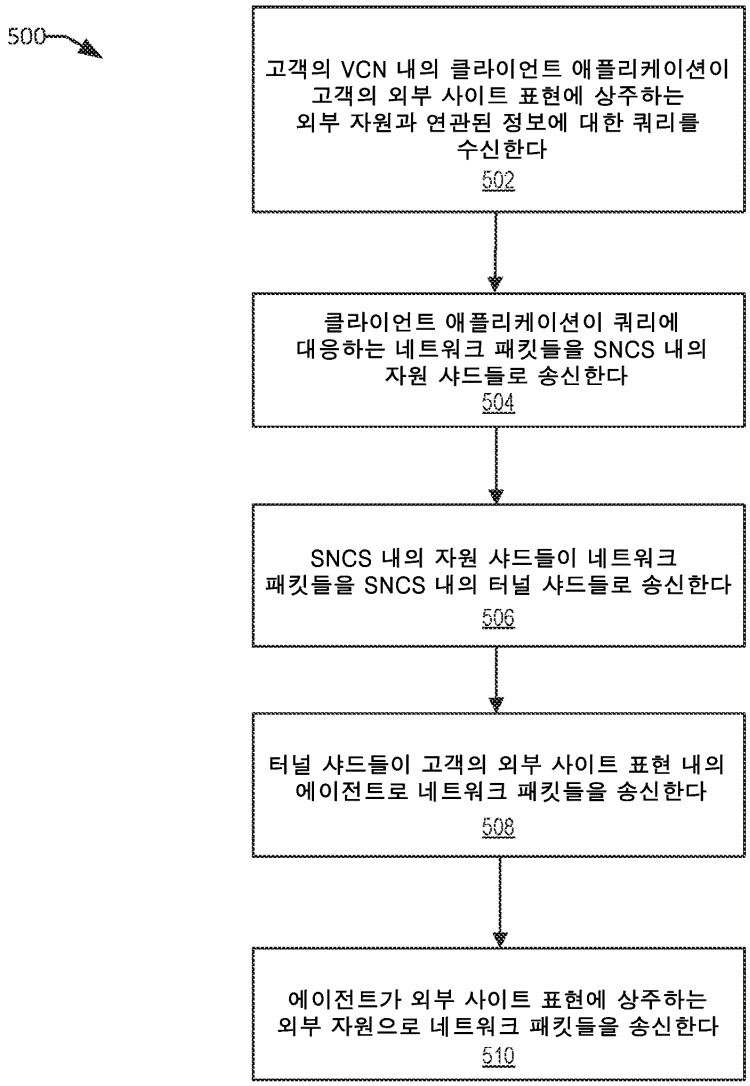
도면3


300
클라우드 서비스 제공자 인프라스트럭처(CSPI)에 구현된 보안 네트워크 연결성 시스템(SCNS)에 의해, 고객에 대해 CSPI에 의해 호스팅되는 가상 클라우드 네트워크(VCN)와 고객과 연관된 사내 네트워크 사이의 보안 사설 연결성을 가능하게 하기 위해 보안 연결성 서비스를 실행한다
302
SNCS에 의해, 사내 네트워크에 상주하는 외부 자원을 고객의 VCN 내의 외부 엔드포인트로서 등록한다
304
SNCS 내의 제1 컴퓨팅 노드에 의해, VCN 내에 외부 엔드포인트에 대한 외부 자원 표현을 생성하며, 생성하는 것은 가상 네트워크 인터페이스 카드를 생성하는 것 및 외부 엔드포인트의 IP 어드레스를 VNIC에 할당하는 것을 포함한다
306
제1 컴퓨팅 노드에 의해, VNIC에 대응하는 구성 정보를 사내 네트워크에 구성된 에이전트로 송신한다
308
SNCS의 제2 컴퓨팅 노드에 의해, VCN에 상주하는 자원과 연관된 정보를 쿼리하기 위한 요청을 수신하며, 여기서 쿼리는 외부 자원에 의해 송신되고, 외부 자원에는 논리적 인터페이스가 프로비저닝된다
310
제2 컴퓨팅 노드에 의해, 외부 자원에 대해 프로비저닝된 논리적 인터페이스와 VCN 내의 외부 자원 표현에 대해 생성된 VNIC 사이에 연결을 설정한다
312
A
A
제2 컴퓨팅 노드에 의해, 요청을 가상 클라우드 네트워크에 상주하는 자원으로 송신한다
314
제2 컴퓨팅 노드에 의해, 설정된 연결을 통해 요청에 대응하는 결과를 획득한다
316

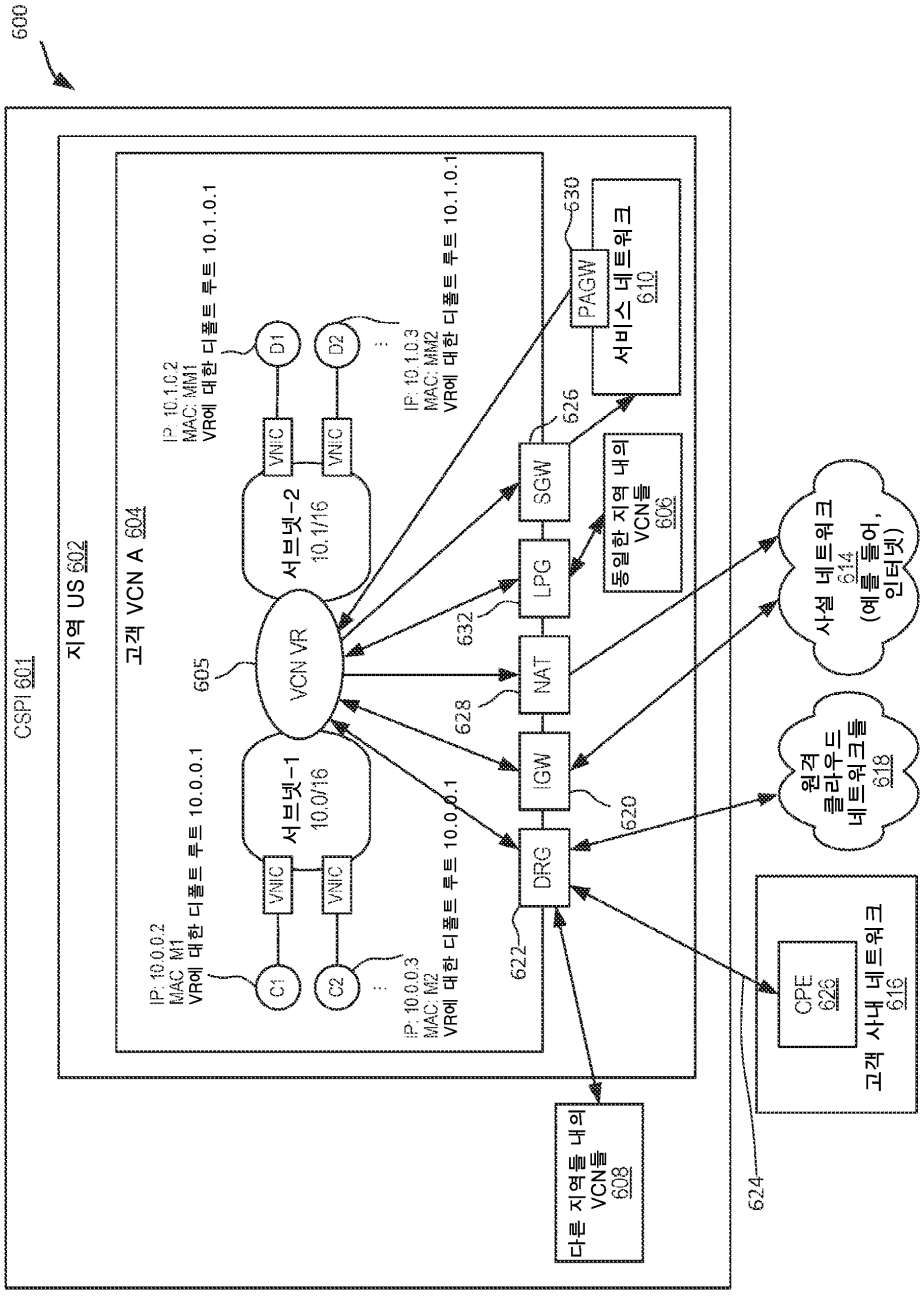
도면4


400
고객의 사내 네트워크에 상주하는 외부 자원이 고객의 VCN에 상주하는 자원과 연관된 정보에 대한 쿼리를 송신한다
402
사내 네트워크에 상주하는 에이전트가 쿼리에 대응하는 네트워크 패킷들을 암호화하고, 네트워크 패킷을 SNCS 내의 터널 샤드들로 송신한다
404
터널 샤드들이 암호화된 네트워크 패킷들을 수신하고, 암호화된 네트워크 패킷들을 SNCS 내의 자원 샤드들로 송신한다
406
자원 샤드들이 터널 샤드들로부터 암호화된 네트워크 패킷들을 수신하고, 네트워크 패킷들을 복호화한다
408
자원 샤드들이 네트워크 패킷을 고객의 VCN 내의 외부 자원 표현에 대해 생성된 VNIC로 송신한다
410
VNIC가 고객의 VCN에 상주하는 자원으로 네트워크 패킷들을 송신한다
412

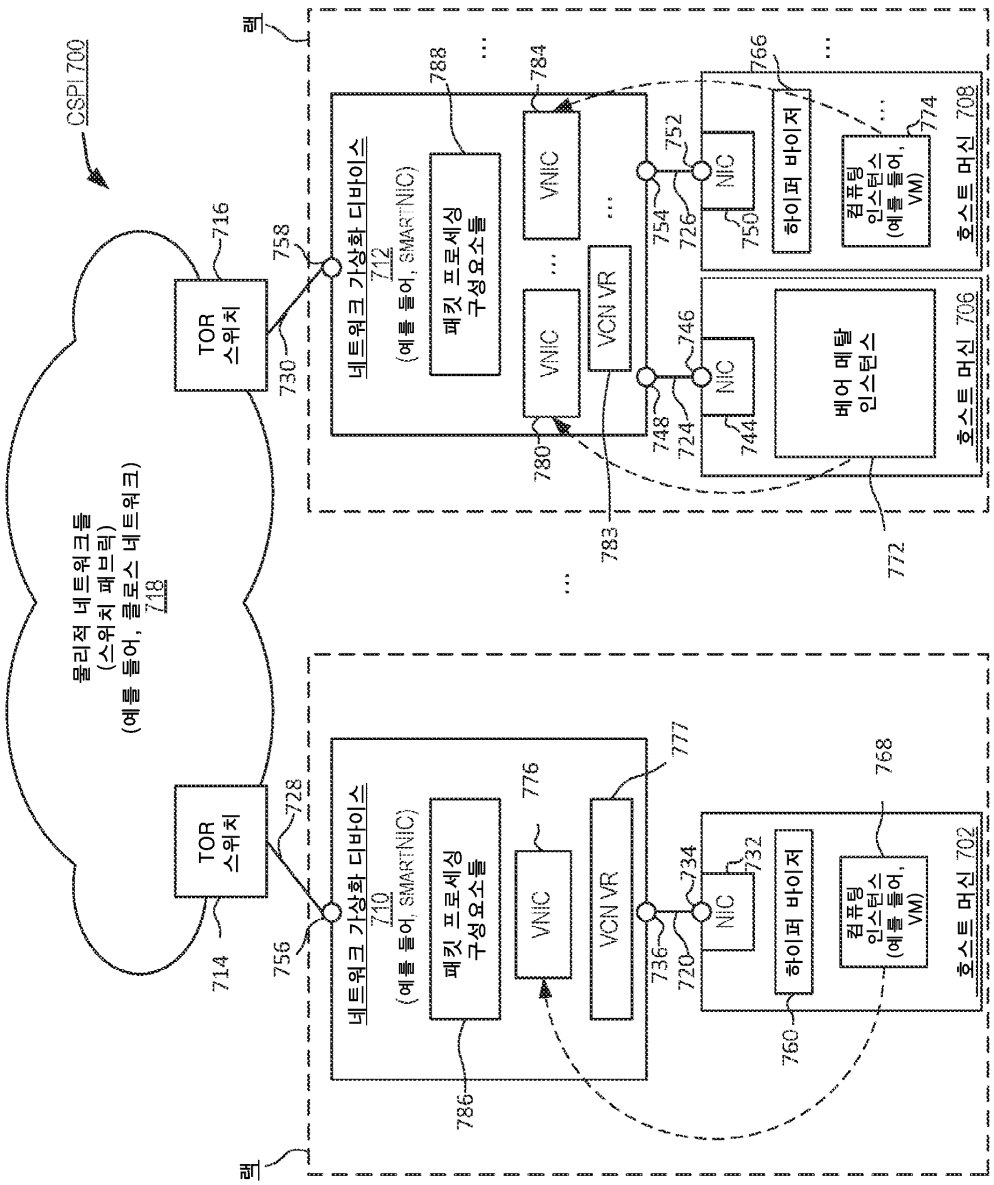
도면5


500
고객의 VCN 내의 클라이언트 애플리케이션이 고객의 외부 사이트 표현에 상주하는 외부 자원과 연관된 정보에 대한 쿼리를 수신한다
502
클라이언트 애플리케이션이 쿼리에 대응하는 네트워크 패킷들을 SNCS 내의 자원 샤드들로 송신한다
504
SNCS 내의 자원 샤드들이 네트워크 패킷들을 SNCS 내의 터널 샤드들로 송신한다
506
터널 샤드들이 고객의 외부 사이트 표현 내의 에이전트로 네트워크 패킷들을 송신한다
508
에이전트가 외부 사이트 표현에 상주하는 외부 자원으로 네트워크 패킷들을 송신한다
510

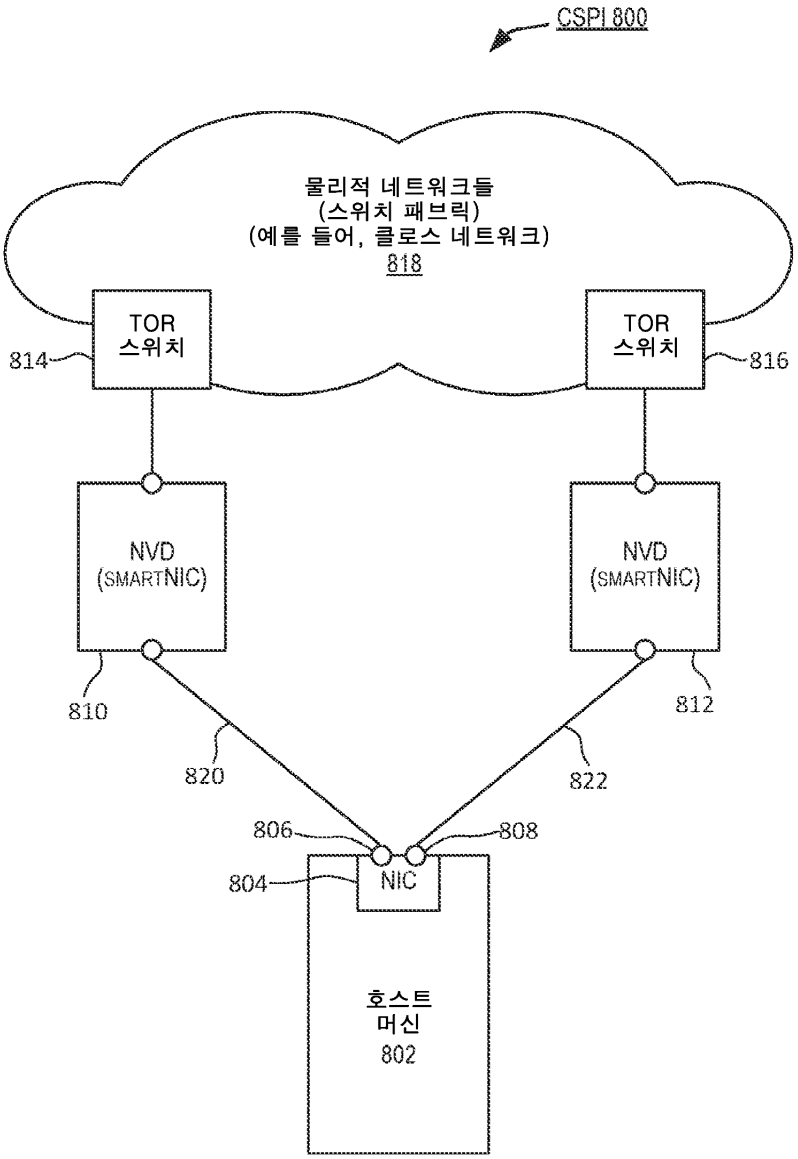
도면6


600
CSPI 601
지역 US 602
고객 VCN A 604
605
VCN VR
서브넷-1
10.0/16
서브넷-2
10.1/16
VNIC
VNIC
VNIC
VNIC
C1
C2
D1
D2
IP: 10.0.0.2
MAC: M1
VR에 대한 디폴트 루트 10.0.0.1
IP: 10.0.0.3
MAC: M2
VR에 대한 디폴트 루트 10.0.0.1
IP: 10.1.0.2
MAC: MM1
VR에 대한 디폴트 루트 10.1.0.1
IP: 10.1.0.3
MAC: MM2
VR에 대한 디폴트 루트 10.1.0.1
DRG
622
IGW
620
NAT
628
LPG
632
SGW
626
PAGW
630
서비스 네트워크
610
동일한 지역 내의
VCN들
606
다른 지역들 내의
VCN들
608
624
CPE
626
고객 사내 네트워크
616
원격
클라우드
네트워크들
618
사설 네트워크
614
(예를 들어,
인터넷)

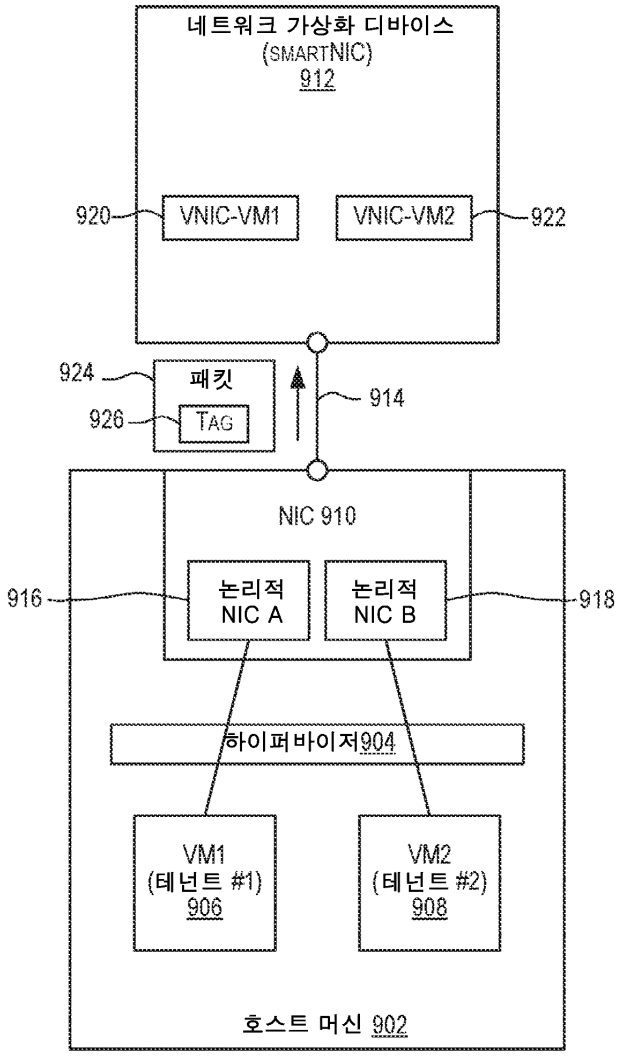
도면7


CSP 700
물리적 네트워크들
(스위치 패브릭)
(예를 들어, 클로스 네트워크)
718
TOR 스위치
714
716
TOR 스위치
730
728
랙
랙
네트워크 가상화 디바이스
710
(예를 들어, SMARTNIC)
712
(예를 들어, SMARTNIC)
패킷 프로세싱 구성요소들
786
788
VNIC
776
784
VCN VR
777
783
734
736
720
NIC
732
하이퍼 바이저
760
768
컴퓨팅 인스턴스 (예를 들어, VM)
호스트 머신 702
754
752
726
NIC
750
하이퍼 바이저
766
774
컴퓨팅 인스턴스 (예를 들어, VM)
호스트 머신 708
748
746
724
NIC
744
베어 메탈 인스턴스
772
호스트 머신 706

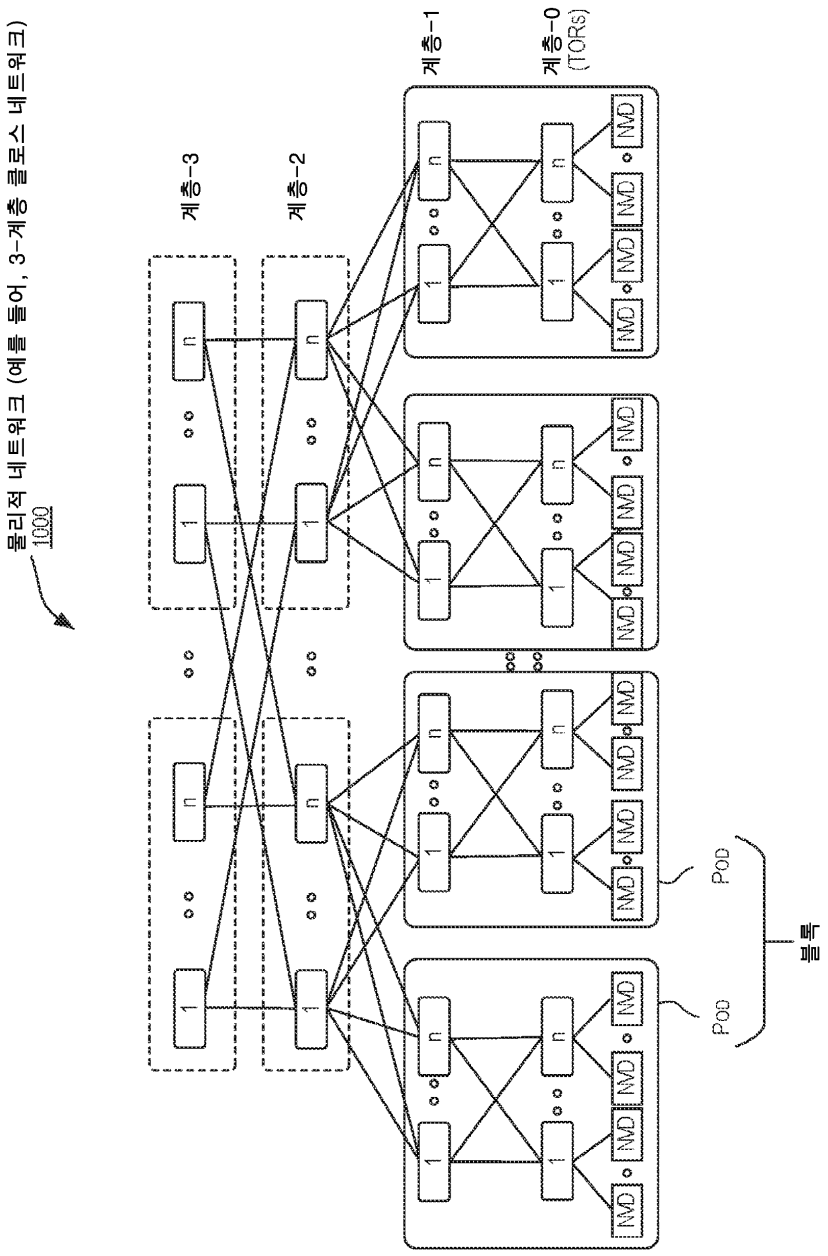
도면8


CSPI 800
물리적 네트워크들
(스위치 패브릭)
(예를 들어, 클로스 네트워크)
818
TOR
스위치
814
TOR
스위치
816
NVD
(SMARTNIC)
NVD
(SMARTNIC)
810
812
820
822
806
808
804
NIC
호스트
머신
802

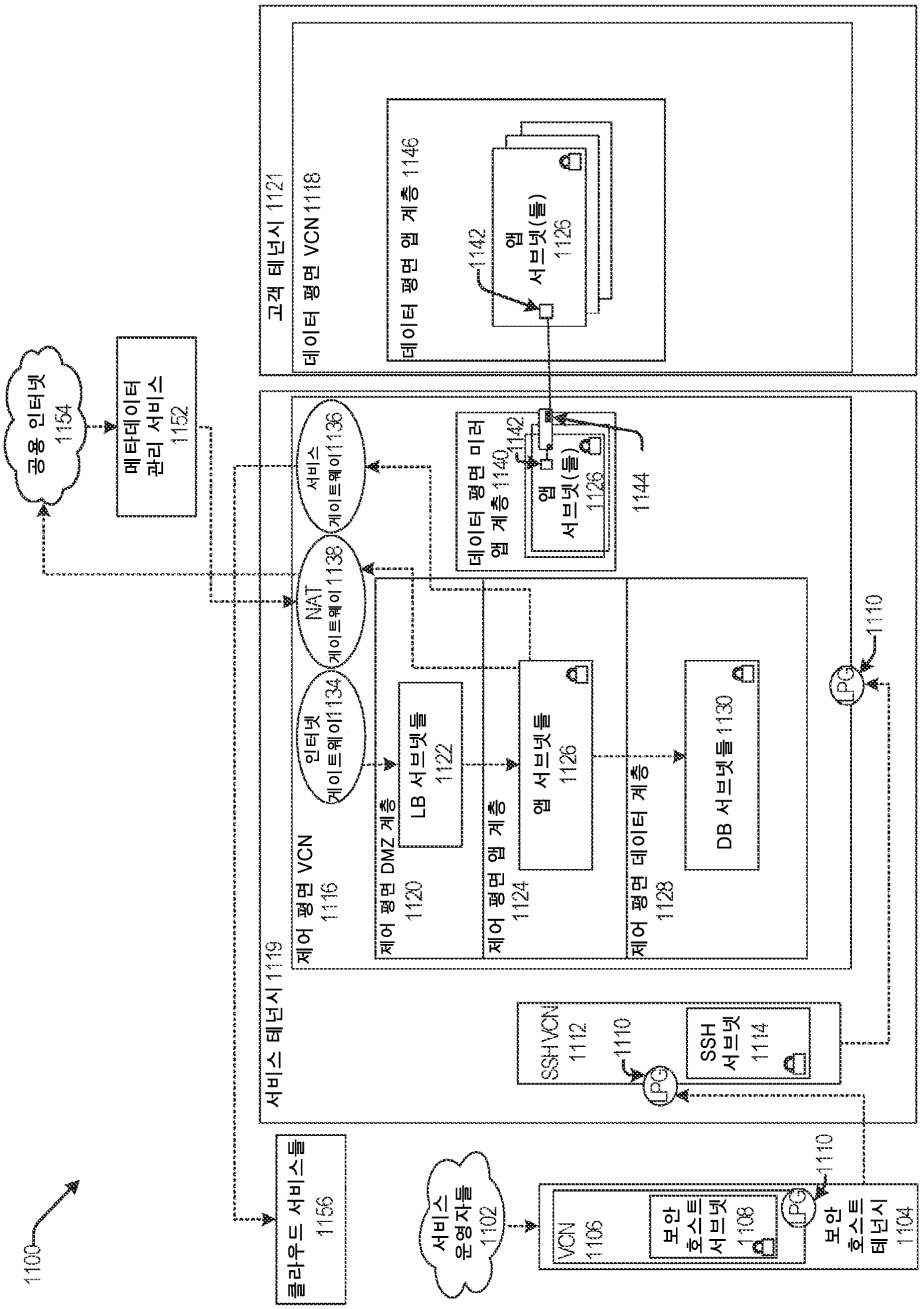
도면9


네트워크 가상화 디바이스
(SMARTNIC)
912
920
VNIC-VM1
VNIC-VM2
922
924
패킷
926
TAG
914
NIC 910
916
논리적
NIC A
논리적
NIC B
918
하이퍼바이저904
VM1
(테넌트 #1)
906
VM2
(테넌트 #2)
908
호스트 머신 902

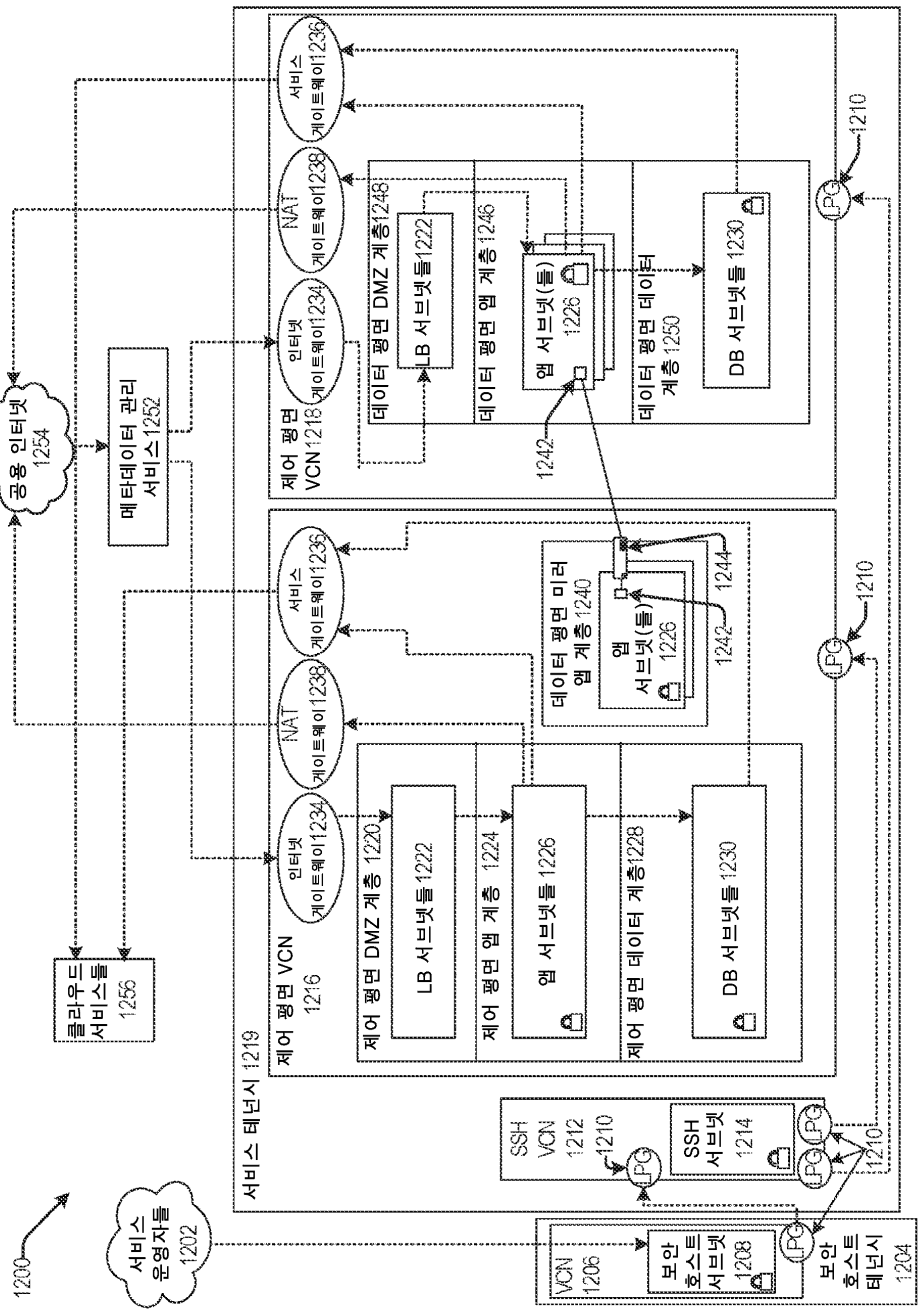
도면10


물리적 네트워크 (예를 들어, 3-계층 클로스 네트워크)
1000
계층-3
계층-2
계층-1
계층-0
(TORs)
n
1
NMD
POD
블록

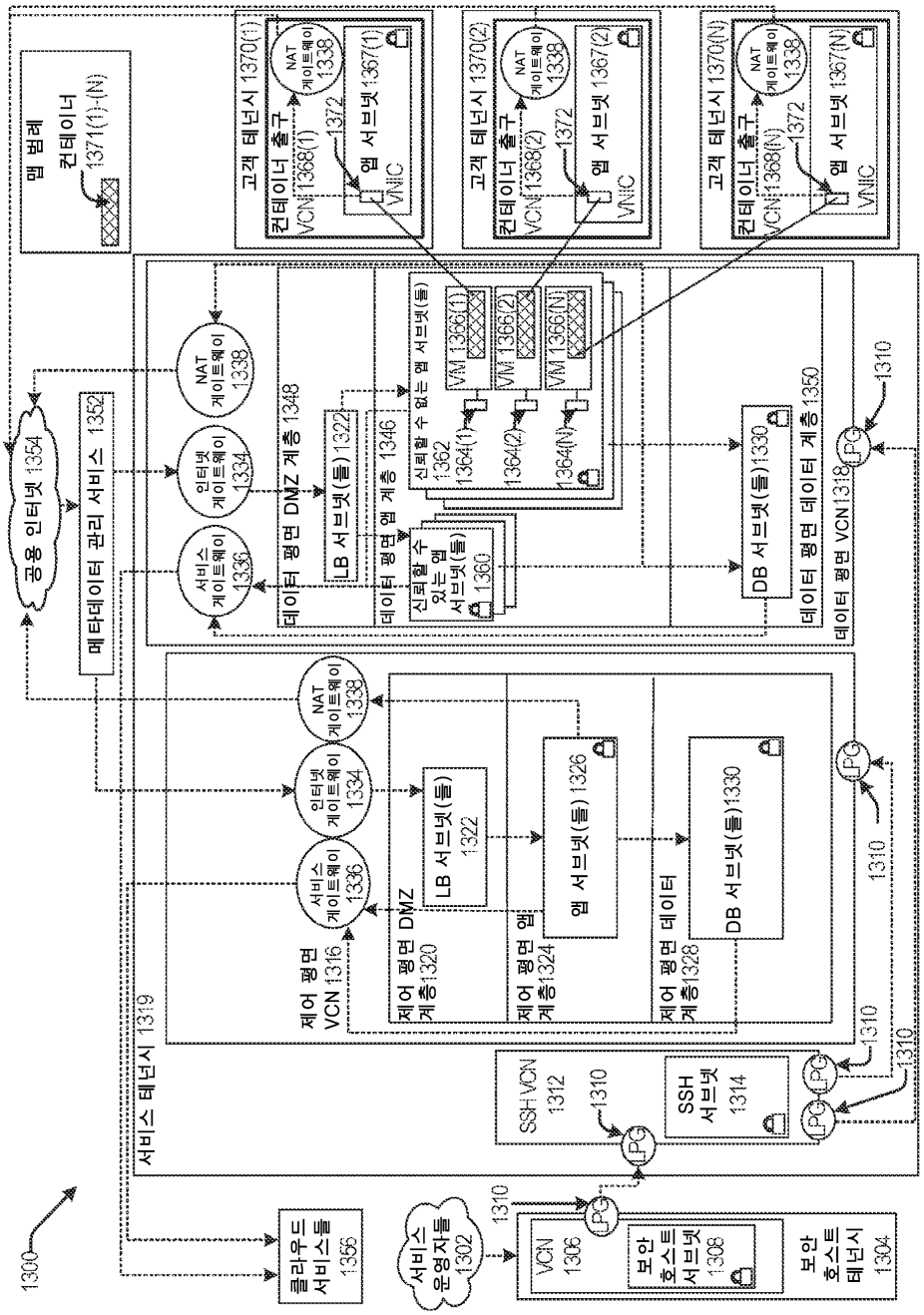
도면11


1100
클라우드 서비스들
1156
서비스 운영자들
1102
VCN
1106
보안 호스트 서브넷
1108
보안 호스트 테넌시
1104
1110
SSH VCN
1112
SSH 서브넷
1114
서비스 테넌시 1119
제어 평면 VCN
1116
제어 평면 DMZ 계층
1120
LB 서브넷들
1122
제어 평면 앱 계층
1124
앱 서브넷들
1126
제어 평면 데이터 계층
1128
DB 서브넷들 1130
인터넷 게이트웨이 1134
NAT 게이트웨이 1138
서비스 게이트웨이 1136
데이터 평면 미러 앱 계층 1140
1142
앱 서브넷(들)
1126
1144
고객 테넌시 1121
데이터 평면 VCN 1118
데이터 평면 앱 계층 1146
1142
앱 서브넷(들)
1126
공용 인터넷
1154
메타데이터 관리 서비스
1152

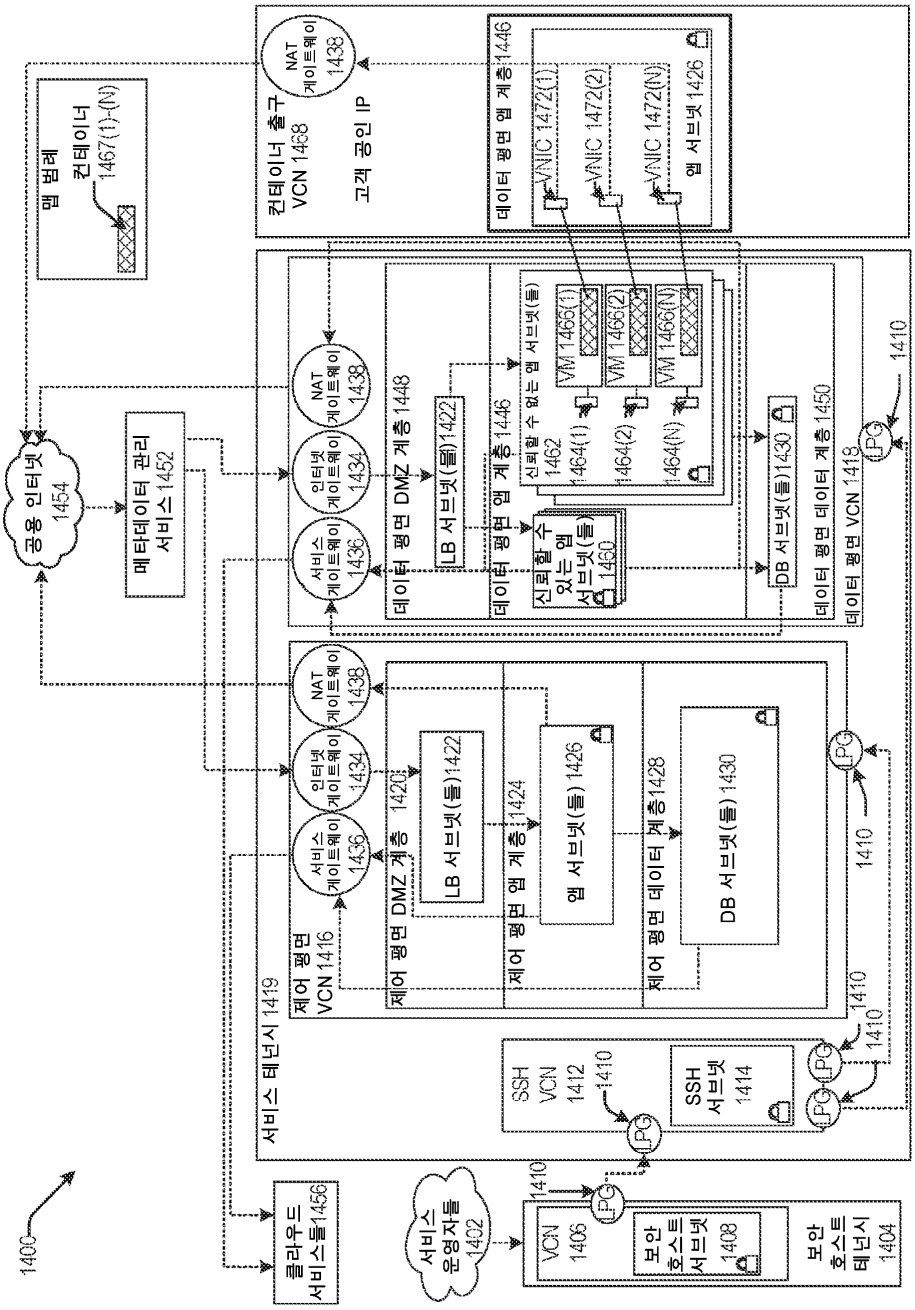
도면12


1200
서비스 운영자들 1202
서비스 테넌시 1219
VCN 1206
보안 호스트 서브넷 1208
보안 호스트 테넌시 1204
SSH VCN 1212
SSH 서브넷 1214
1210
PG
제어 평면 VCN 1216
제어 평면 DMZ 계층 1220
LB 서브넷들 1222
제어 평면 앱 계층 1224
앱 서브넷들 1226
제어 평면 데이터 계층 1228
DB 서브넷들 1230
인터넷 게이트웨이 1234
NAT 게이트웨이 1238
서비스 게이트웨이 1236
데이터 평면 미러 앱 계층 1240
앱 서브넷(들) 1226
1242
1244
제어 평면 VCN 1218
데이터 평면 DMZ 계층 1248
데이터 평면 앱 계층 1246
데이터 평면 데이터 계층 1250
DB 서브넷들 1230
클라우드 서비스들 1256
메타데이터 관리 서비스 1252
공용 인터넷 1254

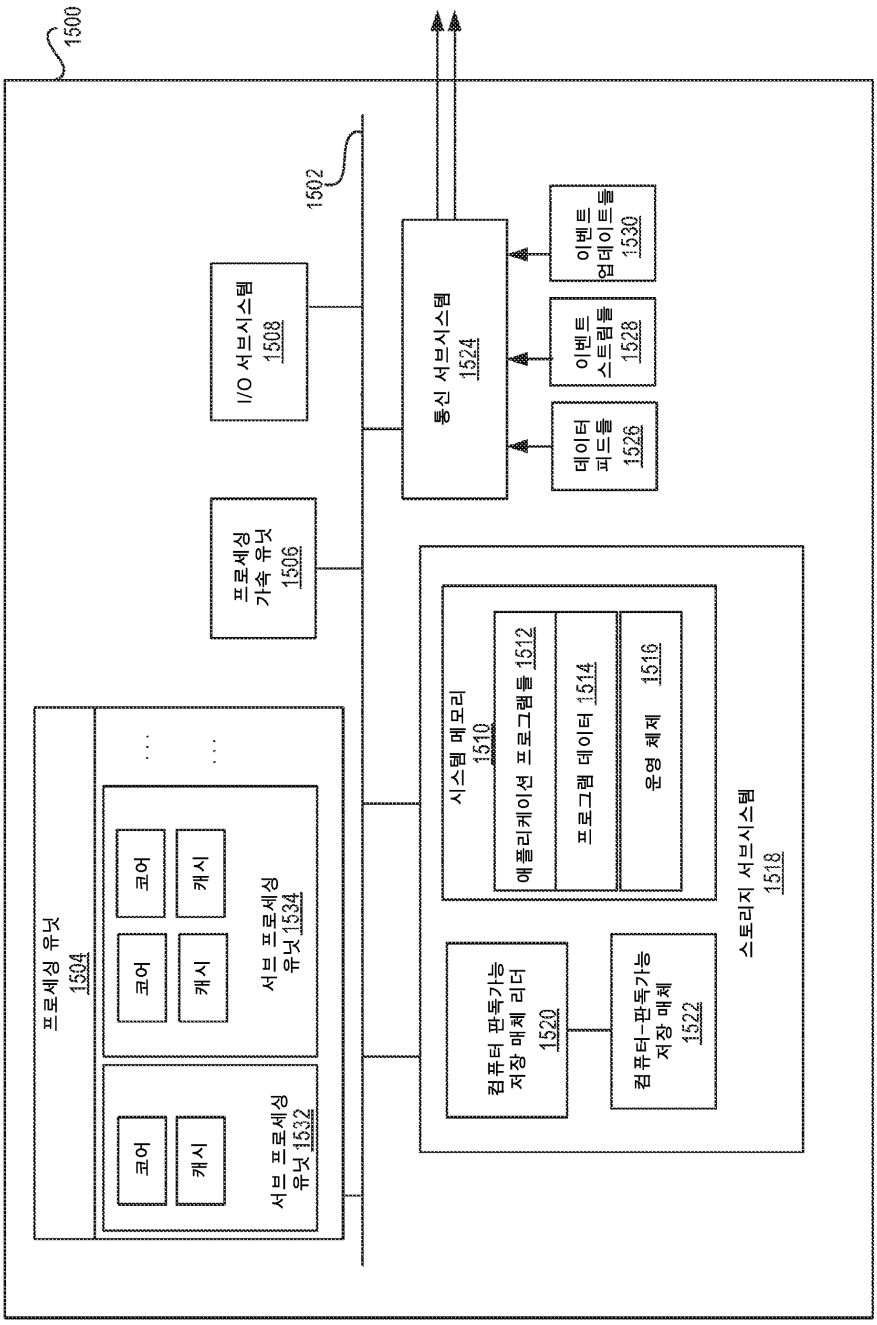
도면13


맵 빌레 컨테이너 1371(1)-(N)
고객 테넌시 1370(1)
컨테이너 출구 VCN 1368(1)
NAT 게이트웨이 1338
1372
앱 서브넷 1367(1) VNIC
고객 테넌시 1370(2)
컨테이너 출구 VCN 1368(2)
앱 서브넷 1367(2) VNIC
고객 테넌시 1370(N)
컨테이너 출구 VCN 1368(N)
앱 서브넷 1367(N) VNIC
공용 인터넷 1354
메타데이터 관리 서비스 1352
서비스 게이트웨이 1336
인터넷 게이트웨이 1334
데이터 평면 DMZ 계층 1348
LB 서브넷(들) 1322
데이터 평면 앱 계층 1346
신뢰할 수 있는 앱 서브넷(들) 1360
VM 1366(1) 1364(1)
VM 1366(2) 1364(2)
VM 1366(N) 1364(N)
데이터 평면 데이터 계층 1350
DB 서브넷(들) 1330
데이터 평면 VCN 1318
1310
서비스 테넌시 1319
제어 평면 VCN 1316
제어 평면 DMZ 계층 1320
제어 평면 앱 계층 1324
앱 서브넷(들) 1326
제어 평면 데이터 계층 1328
SSH VCN 1312
SSH 서브넷 1314
1300
클라우드 서비스들 1356
서비스 운영자들 1302
VCN 1306
보안 호스트 서브넷 1308
보안 호스트 테넌시 1304

도면14


1400
맵 범례
컨테이너 1467(1)-(N)
공용 인터넷 1454
메타데이터 관리 서비스 1452
클라우드 서비스들 1456
서비스 운영자들 1402
컨테이너 출구 VCN 1468
NAT 게이트웨이 1438
고객 공인 IP
데이터 평면 앱 계층 1446
VNIC 1472(1)
VNIC 1472(2)
VNIC 1472(N)
앱 서브넷 1426
서비스 테넌시 1419
제어 평면 VCN 1416
인터넷 게이트웨이 1434
서비스 게이트웨이 1436
제어 평면 DMZ 계층 1420
LB 서브넷(들) 1422
제어 평면 앱 계층 1424
앱 서브넷(들) 1426
제어 평면 데이터 계층 1428
DB 서브넷(들) 1430
데이터 평면 DMZ 계층 1448
데이터 평면 앱 계층 1446
신뢰할 수 있는 앱 서브넷(들) 1460
VM 1466(1)
VM 1466(2)
VM 1466(N)
1464(1)
1464(2)
1464(N)
데이터 평면 데이터 계층 1450
데이터 평면 VCN 1418
SSH VCN 1412
SSH 서브넷 1414
VCN 1406
보안 호스트 서브넷 1408
보안 호스트 테넌시 1404
PG
1410

도면15


1500
1502
I/O 서브시스템 1508
프로세싱 가속 유닛 1506
통신 서브시스템 1524
이벤트 업데이트들 1530
이벤트 스트림들 1528
데이터 피드들 1526
프로세싱 유닛 1504
서브 프로세싱 유닛 1532
서브 프로세싱 유닛 1534
코어
캐시
코어
캐시
코어
캐시
시스템 메모리 1510
애플리케이션 프로그램들 1512
프로그램 데이터 1514
운영 체제 1516
컴퓨터 판독가능 저장 매체 리더 1520
컴퓨터-판독가능 저장 매체 1522
스토리지 서브시스템 1518