



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년02월18일
(11) 등록번호 10-1948598
(24) 등록일자 2019년02월11일

(51) 국제특허분류(Int. Cl.)
H04L 12/46 (2006.01) G06F 9/455 (2018.01)
H04L 29/12 (2006.01)
(52) CPC특허분류
H04L 12/4633 (2013.01)
G06F 9/45558 (2013.01)
(21) 출원번호 10-2017-7010247
(22) 출원일자(국제) 2015년09월18일
심사청구일자 2017년04월14일
(85) 번역문제출일자 2017년04월14일
(65) 공개번호 10-2017-0057357
(43) 공개일자 2017년05월24일
(86) 국제출원번호 PCT/US2015/051027
(87) 국제공개번호 WO 2016/044769
국제공개일자 2016년03월24일
(30) 우선권주장
14/491,758 2014년09월19일 미국(US)
(56) 선행기술조사문헌
US20110075667 A1*
(뒷면에 계속)

(73) 특허권자
아마존 테크놀로지스, 인크.
미국 98108-1226 워싱턴주 시애틀 피오 박스 81226
(72) 발명자
밀러, 케빈 크리스토퍼
미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410
시한, 리차드 알렉산더
미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410
(뒷면에 계속)
(74) 대리인
양영준, 백만기

전체 청구항 수 : 총 15 항

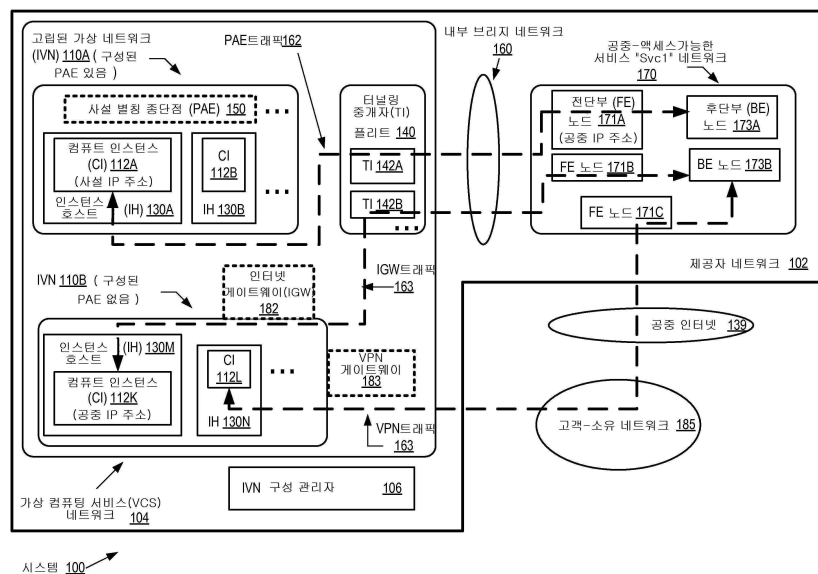
심사관 : 전용해

(54) 발명의 명칭 **고립된 가상 네트워크에 대한 사설 별칭 중단점**

(57) 요약

제공자 네트워크의 고립된 가상 네트워크 내로부터 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 사설 별칭 중단점의 지정에 따라, 터널링 중개자는 컴퓨터 인스턴스에서 발생한 기초 패킷을 수신한다. 기초 패킷은 목적지로서 서비스의 공중 IP(인터넷 프로토콜) 주소를, 그리고 소스로서 컴퓨터 인스턴스의 사설 IP 주소를 표시한다. 터널링 프로토콜에 따라, 터널링 중개자는 고립된 가상 네트워크를 표시하는 헤더 및 기초 패킷의 적어도 일부를 포함하는 캡슐화 패킷을 발생시킨다. 캡슐화 패킷은 서비스의 노드에 송신된다.

대표도 - 도1



(52) CPC특허분류

H04L 61/6004 (2013.01)

H04L 61/6059 (2013.01)

G06F 2009/45595 (2013.01)

(72) 발명자

로렌스, 더글라스 스튜어트

미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410

오웨이스, 마르완 살라 엘-딘

미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410

디킨슨, 앤드류 브루스

미국 98109-5210 워싱턴주 시애틀 테리 애비뉴 노스 410

(56) 선행기술조사문헌

US20120099602 A1

WO2012170016 A1

Anonymous: "Amazon Virtual Private Clude - User Guide", 2014.05.18

JP2014502066 A

US20140006638 A1

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

방법으로서,

제공자 네트워크의 터널링 중개자에서, 클라이언트를 대행하여 확립된 제1 고립된 가상 네트워크(isolated virtual network: IVN)에서 유래하는 트래픽에 대한 라우팅 표적으로서 제1 사설 별칭 종단점(private alias endpoint: PAE)이 지정되었음을 결정하는 단계 - 상기 트래픽은 상기 제공자 네트워크에 구현된 특정 공중-엑세스가능한 서비스에 전달되어야 함 -;

상기 터널링 중개자에서, 상기 제1 PAE가 상기 라우팅 표적으로서 지정된 상기 특정 공중-엑세스가능한 서비스의 공중-광고된 네트워크 주소로 지향된 기초 패킷(baseline packet)을 상기 제1 IVN의 제1 컴퓨트 인스턴스로부터 수신하는 단계;

상기 터널링 중개자에서, (a) 상기 기초 패킷의 콘텐츠 및 (b) 소스 IVN으로서 상기 제1 IVN의 표시를 포함하는 캡슐화 패킷을 생성하는 단계;

상기 터널링 중개자에 의해, 상기 캡슐화 패킷을 상기 제공자 네트워크 외부의 네트워크 링크들을 통과하지 않고 상기 특정 공중-엑세스가능한 서비스의 제1 노드에 송신하는 단계

를 포함하는, 방법.

청구항 2

제1항에 있어서, 상기 캡슐화 패킷은 IPv6(인터넷 프로토콜 버전 6)에 따라 포맷팅되고, 그리고 상기 기초 패킷은 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅되는, 방법.

청구항 3

제1항에 있어서, 상기 특정 공중-엑세스가능한 서비스는 복수의 객체에 대한 복수의 연산 유형을 지원하고,

상기 제1 IVN의 구성 관리자에서, 상기 제1 PAE에 제1 액세스 제어 정책을 적용하라는 요청을 상기 클라이언트로부터 수신하는 단계 - 상기 제1 액세스 제어 정책은, 라우팅 표적으로서 상기 제1 PAE를 사용하여 제출된 요청에 대해, (a) 상기 복수의 연산 유형 중 허용된 연산 유형, (b) 상기 복수의 연산 유형 중 금지된 연산 유형, (c) 상기 복수의 연산 유형 중 특정 연산 유형이 허용되는 시간 구간, 또는 (d) 상기 복수의 연산 유형 중 특정 연산 유형이 허용되는 상기 복수의 객체 중 특정 객체 중 하나 이상을 표시함 -; 및

상기 제1 액세스 제어 정책에 의해 제1 연산이 허용됨을, 상기 기초 패킷에 표시된 특정 요청에 따라 상기 제1 연산을 실행하기 이전에, 검증하는 단계

를 더 포함하는, 방법.

청구항 4

제1항에 있어서,

상기 제1 IVN에서 유래하는 부가적 트래픽에 대한 라우팅 표적으로서 제2 PAE를 지정하는 단계를 더 포함하되, 상기 부가적 트래픽은 다른 서비스에 전달되어야 하는, 방법.

청구항 5

제1항에 있어서, 상기 제1 컴퓨트 인스턴스는 상기 클라이언트의 요청시 상기 제1 컴퓨트 인스턴스에 배정된 특정 사설 IP 주소를 갖고,

제2 IVN으로서 제2 컴퓨트 인스턴스를 포함하는 상기 제2 IVN을 상기 클라이언트를 대행하여 확립하는 단계;

상기 클라이언트의 요청 시에, 상기 제2 컴퓨트 인스턴스에 상기 특정 사설 IP 주소를 배정하는 단계;

상기 제2 IVN에서 유래하고 상기 특정 공중-엑세스가능한 서비스로 지향되는 트래픽을 라우팅하는데 사용될 제2 PAE를 확립하는 단계;

상기 특정 공중-엑세스가능한 서비스의 특정 노드에서, 상기 터널링 중개자에 의해 발생된 캡슐화 헤더의 조사에 기초하여, 상기 특정 노드에서 수신된 특정 기초 패킷이 상기 특정 사설 IP 주소가 배정된 상기 제1 컴퓨터 인스턴스에서 발생되었는지, 아니면 상기 특정 사설 IP 주소가 배정된 상기 제2 컴퓨터 인스턴스에서 발생되었는지를 결정하는 단계

를 더 포함하는, 방법.

청구항 6

제1항에 있어서, 상기 캡슐화 패킷은 상기 제공자 네트워크에서 구현된 사유 터널링 프로토콜에 따라 포맷팅되는, 방법.

청구항 7

제1항에 있어서, 상기 캡슐화 패킷은 상기 제1 PAE의 식별자의 표현을 포함하는 헤더를 포함하는, 방법.

청구항 8

제1항에 있어서,

상기 제1 PAE를 발생시키라는 상기 클라이언트로부터의 요청을, 프로그램 인터페이스를 통하여 상기 제공자 네트워크의 구성 관리자에서, 수신하는 단계; 및

상기 제1 PAE를 표현하는 메타데이터 엔트리를, 상기 요청에 응답하여 상기 구성 관리자에 의해, 저장하는 단계를 더 포함하는, 방법.

청구항 9

제1항에 있어서,

PAE를 사용하는 액세스에 다른 서비스를 등록하라는 요청을, 프로그램 인터페이스를 통하여 상기 제공자 네트워크의 구성 관리자에서, 수신하는 단계; 및

특정 PAE와의 연관을 위해 상기 클라이언트에 의해 특정 서비스가 선택될 수 있는 서비스의 집합에 상기 다른 서비스를, 상기 요청에 응답하여 상기 구성 관리자에 의해, 추가하는 단계를 더 포함하는, 방법.

청구항 10

제9항에 있어서, 상기 다른 서비스는 상기 제공자 네트워크의 자원의 세트를 사용하여 상기 제공자 네트워크의 다른 클라이언트에 의해 구현되고,

상기 다른 서비스로 지향된 기초 패킷으로부터 유도된 캡슐화 패킷의 콘텐츠를 추출하도록 구성된 특정 전단부 노드를 포함하는, 상기 다른 서비스에 대한 하나 이상의 전단부 노드를 확립하는 단계를 더 포함하는, 방법.

청구항 11

시스템으로서,

하나 이상의 메모리를 포함하는 하나 이상의 컴퓨터 시스템을 포함하고, 상기 하나 이상의 메모리는 실행시 상기 시스템으로 하여금

클라이언트를 대행하여 제공자 네트워크에 확립된 제1 고립된 가상 네트워크(IVN)로부터 상기 제공자 네트워크에 구현된 특정 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 지정된 제1 사설 별칭 중단점(PAE)을 식별하고;

상기 제1 IVN의 제1 컴퓨터 인스턴스에서 발생된 기초 패킷을 수신하고 - 상기 기초 패킷은 상기 라우팅 표적으로서 지정된 상기 제1 PAE에 대한 상기 특정 서비스의 공중 IP(인터넷 프로토콜) 주소를 당해 목적지 주소로서 표시함 -;

선택된 터널링 프로토콜에 따라, (a) 상기 기초 패킷의 콘텐츠 중 적어도 일부 및 (b) 소스 IVN으로서 상기 제1 IVN을 표시하는 헤더 컴포넌트를 포함하는 캡슐화 패킷을 발생시키고; 그리고

상기 캡슐화 패킷을 상기 특정 서비스의 제1 노드에 송신하게 하는 명령어들을 포함하는, 시스템.

청구항 12

제11항에 있어서, 상기 캡슐화 패킷은 IPv6(인터넷 프로토콜 버전 6)에 따라 포맷팅되고, 그리고 상기 기초 패킷은 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅되는, 시스템.

청구항 13

제11항에 있어서, 상기 하나 이상의 메모리는 실행시 상기 시스템으로 하여금

상기 제1 IVN의 제2 컴퓨트 인스턴스에서 발생된 제2 기초 패킷의 표현을, 상기 제1 IVN으로부터 다른 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 제2 PAE의 지정에 따라, 수신하되, 상기 제2 기초 패킷은 당해 목적지 주소로서 상기 다른 서비스의 공중 IP 주소를 표시하고;

(a) 상기 제2 기초 패킷의 콘텐츠 중 적어도 일부 및 (b) 소스 IVN으로서 상기 제1 IVN을 표시하는 헤더 컴포넌트를 포함하는 제2 캡슐화 패킷을, 상기 선택된 터널링 프로토콜에 따라, 발생시키고; 그리고

상기 제2 캡슐화 패킷을 상기 다른 서비스의 다른 노드에 송신하게 하는 명령어들을 포함하는, 시스템.

청구항 14

제11항에 있어서, 제1의 상기 캡슐화 패킷은 상기 제1 컴퓨트 인스턴스의 사설 IP 주소의 표시를 포함하고, 그리고 상기 하나 이상의 메모리는 실행시 상기 시스템으로 하여금

제2 IVN의 제2 컴퓨트 인스턴스에서 발생된 제2 기초 패킷의 표현을, 상기 클라이언트를 대행하여 확립된 상기 제2 IVN으로부터 상기 특정 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 제2 PAE의 지정에 따라, 수신하되, 상기 제2 기초 패킷은 당해 목적지 주소로서 상기 특정 서비스의 상기 공중 IP 주소를 표시하고;

(a) 상기 제2 기초 패킷의 콘텐츠 중 적어도 일부 (b) 소스 IVN으로서 상기 제2 IVN을 표시하는 헤더 컴포넌트 및 (c) 상기 사설 IP 주소의 표시를 포함하는 제2 캡슐화 패킷을, 상기 선택된 터널링 프로토콜에 따라, 발생시키고; 그리고

상기 제2 캡슐화 패킷을 상기 특정 서비스의 상기 제1 노드에 송신하게 하는 명령어들을 포함하되, 상기 특정 서비스의 상기 제1 노드는, 상기 제2 기초 패킷이 상기 제1 컴퓨트 인스턴스에서 발생되었는지, 아니면 상기 제2 컴퓨트 인스턴스에서 발생되었는지를, 상기 제2 캡슐화 패킷의 조사에 기반하여, 결정하도록 구성되는, 시스템.

청구항 15

제11항에 있어서, 상기 캡슐화 패킷은 상기 제1 PAE의 식별자의 표현을 포함하는 헤더를 포함하는, 시스템.

발명의 설명

기술 분야

배경 기술

[0001] 많은 회사 및 다른 조직은, (예컨대, 로컬 네트워크의 일부분으로서) 병설되거나 또는 대신에 (예컨대, 하나 이상의 사설 또는 공중 중간 네트워크를 통하여 접속된) 다수의 구별되는 지리적 위치에 위치하는 컴퓨팅 시스템과 같이, 그들 연산을 지원하기 위해 수많은 컴퓨팅 시스템을 상호접속하는 컴퓨터 네트워크를 운용한다. 예컨대, 상당한 수의 상호접속된 컴퓨팅 시스템을 하우스징하는 데이터 센터는, 단일 조직에 의해 그리고 그것을 대행하여 운용되는 사설 데이터 센터, 및 컴퓨팅 자원을 고객에 제공하기 위한 사업으로서 개체에 의해 운용되는 공중 데이터 센터와 같이, 아주 흔하게 되었다.

[0002] 몇몇 제공자는 그들 고객이 그러한 데이터 센터에 위치하는 자원을 사용하여 논리적으로 고립된 네트워크를 생

성할 수 있게 한다. 예컨대, 고객은 제공자에 의해 관리되는 호스트에서 구현된 소정 세트의 가상화된 서버 및/또는 다른 자원을 배정받을 수 있고, 그리고 고객은 자원의 네트워킹 구성에 대해 상당한 융통성을 제공할 수 있다. 고객은, 예컨대, 서버에 대한 IP(인터넷 프로토콜) 주소를 선택할 수 있고, 그들 선택의 서브넷을 정의할 수 있고 등이다. 제공자 자원을 사용하여 구현된 그러한 고객-구성가능한 네트워킹은, "고립된 가상 네트워크" 또는 "가상 사설 클라우드"를 포함하는, 다양한 명칭으로 지칭될 수 있다. 일부 시나리오에서, 고객은, 예컨대, 고립된 가상 네트워크 바깥의 자원에 대해 주소의 고유함에 대해 걱정할 필요 없이, 사설 IP 주소(즉, 고립된 가상 네트워크 바깥에는 보이지 않거나 광고되지 않은 주소)를 고립된 가상 네트워크 내에서의 일부 자원에 배정할 수 있다. 제공자는 그러한 환경에서 높은 레벨의 보안, 네트워크 고립성, 및 가용성을 지원할 수 있어서, 고객이 고립된 가상 네트워크에서 비즈니스-중대한 애플리케이션을 실행시키고 고객-소유 부지에서 달성가능한 것과 유사한(또는 더 높은) 품질의 서비스를 경험하는 것을 가능하게 한다.

[0003]

고립된 가상 네트워크를 지원하는 적어도 일부 제공자는 또한, 저장 서비스, 데이터베이스 서비스 등과 같은, 다양한 다른 서비스를 구현할 수 있다. 이들 다른 서비스 중 일부는 공중 인터넷으로부터 액세스가능하도록 설계될 수 있다 - 예컨대, 일 세트의 공중-광고된 IP 주소 또는 대응하는 URI(uniform resource identifier)는 클라이언트가 그러한 서비스의 자원에 액세스하도록 셋업될 수 있다. 적어도 일부 환경에서, 그들의 고도 보안 고립된 가상 네트워크 내로부터 그러한 공중-광고된 서비스에 액세스하기를 바라는 고객이 잠재적으로 보안을 감축하거나 상당한 비용을 발생시키지 않고 그렇게 하는 것은 간단하지 않을 수 있다.

도면의 간단한 설명

[0004]

도 1은, 적어도 일부 실시형태에 따라, 고객 네트워크를 순회하지 않고 그리고 IVN에서 공중 IP 주소를 배정하지 않고 하나 이상의 공중-액세스가능한 서비스와 제공자 네트워크의 고립된 가상 네트워크(isolated virtual network: IVN) 간 네트워크 트래픽의 라우팅을 가능하게 하도록 사설 별칭 종단점(private alias endpoint: PAE)이 확립될 수 있는 일례의 시스템 환경의 예시도,

도 2는, 적어도 일부 실시형태에 따라, 고립된 가상 네트워크의 컴퓨터 인스턴스에서 유래하는 패킷을 공중-액세스가능한 서비스에서의 목적지로 향하여 지향시키는데 관여된 예시적 컴포넌트의 예시도,

도 3a 및 도 3b는, 적어도 일부 실시형태에 따라, 고립된 가상 네트워크의 컴퓨터 인스턴스에서 유래하는 패킷을 프로세싱할 수 있는 대안의 서비스-측 컴포넌트의 각각의 예의 예시도,

도 4는, 적어도 일부 실시형태에 따라, 컴퓨터 인스턴스에서 유래하는 기초 패킷에 대한 캡슐화 포맷의 예의 예시도,

도 5는, 적어도 일부 실시형태에 따라, PAE 구성 요청 및 응답의 예의 예시도,

도 6은, 적어도 일부 실시형태에 따라, PAE 구성 데이터베이스 콘텐츠의 예의 예시도,

도 7은, 적어도 일부 실시형태에 따라, 동일한 사설 IP 주소를 갖는 컴퓨터 인스턴스로부터 서비스에서 수신된 요청들 간을 구별하기 위한 IVN 및 PAE 식별자의 사용의 일례의 예시도,

도 8은, 적어도 일부 실시형태에 따라, PAE를 구성하도록 수행될 수 있는 연산의 태양을 예시하는 순서도,

도 9는, 적어도 일부 실시형태에 따라, 컴퓨터 인스턴스로부터 공중-액세스가능한 서비스로 패킷을 송신하기 위한 터널링 프로토콜의 사용을 예시하는 순서도, 및

도 10은 적어도 일부 실시형태에서 사용될 수 있는 일례의 컴퓨팅 디바이스를 예시하는 블록 선도.

여기에서는 수 개의 실시형태 및 예시적 도면에 대하여 예로서 실시형태가 설명되고 있기는 하지만, 당업자는 실시형태가 설명된 실시형태 또는 도면으로 한정되는 것은 아님을 인식할 것이다. 거기에서의 도면 및 상세한 설명은 개시된 특정 형태로 실시형태를 한정하려는 의도가 아니라, 반대로, 첨부 청구범위에 의해 정의되는 바와 같은 취지 및 범위 내에 드는 모든 수정물, 균등물 및 대안물을 망라하려는 의도임을 이해하여야 한다. 여기에서 사용되는 제목은 단지 편성 목적일 뿐이고 청구범위 또는 설명의 범위를 제한하도록 사용되려는 의미는 아니다. 본 출원의 곳곳에서 사용될 때, 단어 "할 수 있다"는 의무적 의미(즉, 필수를 의미)보다는 허용적 의미(즉, 잠재성을 가짐을 의미)로 사용된다. 유사하게, 단어 "포함한다" 및 그 활용형은 포함하지만 국한되지는 않음을 의미한다.

발명을 실시하기 위한 구체적인 내용

- [0005] 제공자 네트워크에서 사설 별칭 중단점(PAE)을 지원하기 위한 방법 및 장치의 다양한 실시형태가 설명된다. 인터넷 및/또는 다른 네트워크를 통하여 분산형 클라이언트 세트에 액세스가능한 (다양한 유형의 멀티-테넌트 및/또는 단일-테넌트 클라우드-기반 컴퓨팅 또는 저장 서비스와 같은) 하나 이상의 서비스를 제공하도록 공중 부문 조직 또는 회사와 같은 개체에 의해 셋업된 네트워크는 여기에서 제공자 네트워크라고 칭해질 수 있다. 적어도 일부 제공자 네트워크는 "공중 클라우드" 환경이라고도 지칭될 수 있다. 소정 제공자 네트워크는, 제공자에 의해 제공되는 기반구조 및 웹 서비스를 구현, 구성 및 분산시키는데 필요로 되는, 물리적 및/또는 가상화된 컴퓨터 서버, 저장 디바이스, 네트워킹 장비 등의 집합과 같은, 다양한 자원 풀을 호스팅하는 수많은 데이터 센터를 포함할 수 있다. 적어도 일부 실시형태에서, 제공자 네트워크에서 구현된 가상 컴퓨팅 서비스는 클라이언트가, 하나 이상의 컴퓨터 인스턴스가 대형 플리트의 인스턴스 호스트 중 하나의 인스턴스 호스트 상에서 실행되는, 그들 애플리케이션에 대한 (여기에서는 "컴퓨터 인스턴스" 또는 단순히 "인스턴스"라고 지칭될 수 있는) 하나 이상의 게스트 가상 머신을 이용하는 것을 가능하게 할 수 있다. 대형 제공자 네트워크 내에서, 일부 데이터 센터는 다른 것들과는 다른 도시, 주 또는 지역에 위치할 수 있고, 그리고 일부 실시형태에서 소정 애플리케이션에 할당되는 자원은 소망 레벨의 가용성, 장애-허용성 및 성능을 달성하기 위해 수 개의 그러한 장소 간에 분산될 수 있다.
- [0006] 적어도 일부 실시형태에서, 제공자 네트워크는 고객이 제공자의 데이터 센터에서의 "고립된 가상 네트워크"(IVN)의 확립을 요청하는 것을 가능하게 할 수 있다. (일부 환경에서는 "가상 사설 클라우드" 또는 VPC라고 지칭될 수도 있는) IVN는, 고객이 통하여 네트워킹 구성에 대해 상당한 제어를 승인받는, 제공자 네트워크의 논리적으로 고립된 섹션에서의 컴퓨팅 및/또는 다른 자원의 집합을 포함할 수 있다. 일부 실시형태에서, 예컨대, 고객은 다양한 컴퓨터 인스턴스와 같은 IVN 자원에 사용될 IP(인터넷 프로토콜) 주소 범위를 선택하고, IVN 내에서의 서브넷의 생성, 및 IVN에 대한 루트 테이블 등의 구성을 관리할 수 있다. 일부 실시형태에서 IVN 내에서의 디바이스 중 적어도 일부에 대해, IP 주소는, 적어도 디폴트에 의해서, IVN 바깥에서는 보이지 않을 수 있다. 그러한 IP 주소는, BGP(보더 게이트웨이 프로토콜) 또는 다른 유사한 프로토콜을 통하여 공중 인터넷 상에서 직접적으로 또는 간접적으로 광고되는 결과로서 공중 인터넷으로부터 액세스가능한 "공중" IP 주소와는 대조적으로, 여기에서는 "사설" IP 주소라고 지칭될 수 있다. 사설 주소의 사용은, 예컨대, 클라이언트가 인터넷으로부터 유래하는 잠재적 공격으로부터 그들 애플리케이션을 보호하는 것을 가능하게 할 수 있다. IVN 지원은 일부 실시형태에서는 제공자 네트워크의 더 일반적인 가상 컴퓨팅 서비스(VCS)의 특징 중 하나일 수 있다. 예컨대, VCS는 또한 IVN의 일부분이 아닌 컴퓨터 인스턴스의 할당 또는 예비할당을 지원할 수 있고, 그리고 그에 대해 (인스턴스가 할당되는 클라이언트라기보다는) VCS는 요구되는 네트워킹 구성 중 많은 것 또는 전부를 수행한다.
- [0007] 하나 이상의 저장 서비스 또는 데이터베이스 서비스와 같은, 제공자 네트워크에서 구현된 서비스 중 적어도 일부는 공중 액세스가능할 수 있다. 즉, 서비스에 액세스하는데 사용될 수 있는 소정 세트의 IP 주소(또는 대응하는 호스트네임/URI)는 공중 광고될 수 있고, 그래서 클라이언트는 인터넷으로의 접속성을 갖는 디바이스로부터 그러한 서비스에 서비스 요청을 제출할 수 있을 수 있다. 예컨대, "SvcX"라고 명명된 저장 서비스는 <https://SvcX.<providername>.com>과 같은 공중 광고된 URI를 통하여 클라이언트에 의해 액세스가능할 수 있고, 그리고 그러한 서비스에 대한 IP 주소는 하나 이상의 도메인 네임 서비스(DNS) 서버로부터 획득될 수 있다.
- [0008] 클라이언트를 대행하여 IVN 내에서 실행되는 일부 애플리케이션은 그러한 공중-액세스가능한 서비스로의 액세스를 필요로 할 수 있다. 예컨대, IVN에서의 클라이언트의 컴퓨터 인스턴스 상에서 실행되는 전자-상거래 애플리케이션은 제공자 네트워크의 공중-액세스가능한 저장 서비스에 데이터를 기록 또는 판독할 필요가 있을 수 있다. 공중-액세스가능한 서비스로의 접속성을 확립하기 위한 하나의 방법은 IVN 내에서의 자원에 하나 이상의 공중 IP 주소를 지정하는 것(및/또는 IVN에 대한 인터넷-액세스가능한 게이트웨이를 셋업하는 것)을 수반할 수 있는데, IVN 클라이언트의 고립 및 보안 요건에 다소 거스르는 실시일 수 있다. 공중-액세스가능한 서비스의 자원과 IVN에서 실행되는 컴퓨터 인스턴스 간 접속성을 확립하기 위한 다른 방법은 우선 IVN과 고객 네트워크 간 VPN(가상 사설 네트워크) 접속을 확립하고, 그 후 고객 네트워크를 통하여 IVN으로부터 공중-액세스가능한 서비스로 간접적으로 트래픽을 보내는 것일 수 있다. 그렇지만, 적어도 일부 환경에서, 그러한 VPN-기반 접속성은 상당히 비쌀 수 있고, 그리고 트래픽에 사용된 간접 경로는 반드시 클라이언트 애플리케이션 요건을 만족하기에 (예컨대, 단부-대-단부 레이턴시에 대해) 충분히 빠르지는 않을 수 있다.
- [0009] 따라서, IVN 자원과 적어도 일부 공중-액세스가능한 서비스 간 효율적 접속성을 용이하게 하기 위해, 일부 실시형태에서 제공자 네트워크 오퍼레이터는 IVN에 대해 사설 별칭 중단점의 확립을 지원할 수 있다. 명칭이 내포하듯이, PAE는 공중-액세스가능한 서비스를 표현하는 "가상" 중단점으로서 역할할 수 있고, 그리고 PAE는 그 사용

이 IVN 내에서의 어느 개체에도 공중 네트워크 주소의 배정을 요구하지 않는다는 점에서 "사설"일 수 있다. PAE는 또한 일부 환경에서는 "가상 사설 종단점"이라고 지칭될 수도 있다. 적어도 일부 실시형태에서, PAE는 클라이언트를 대항하여 셋업된 IVN 내에서 실행되는 애플리케이션이, 예컨대, 제공자 네트워크 바깥의 네트워크 링크를 순회하지 않고 그리고 공중 인터넷에 IVN을 노출시킬 필요 없이, 제공자 네트워크 내 다른 곳에서 구현된 공중-액세스가능한 서비스에 서비스 요청을 보내는 것(및 그로부터 응답을 수신하는 것)을 가능하게 할 수 있다. 터널링 프로토콜은 아래에서 설명되는 바와 같이 공중-액세스가능한 서비스가 구현되는 제공자 네트워크의 부분으로의 송신을 위해 IVN에서 유래하는 트래픽의 패킷을 캡슐화하는데 사용될 수 있다. 다양한 실시형태에서, IVN에서 실행되는 클라이언트 애플리케이션도, 그리고 클라이언트 서비스 요청을 구현하는 공중-액세스가능한 서비스의 자원도, 반드시 터널링 프로토콜의 사용을 알고 있게 될 필요는 없다. 즉, 그러한 실시형태에서, 서비스 자원에서 클라이언트 요청에 서비스 제공하는데 관여된 로직에 또는 클라이언트 애플리케이션에 변경은 필요로 되지 않을 수 있다.

[0010] 적어도 하나의 실시형태에서, PAE의 확립은 클라이언트가, 전형적으로는 클라이언트에 의해 수행된 IVN 네트워킹 구성의 다른 태양에 요구되는 종류의 단계와 사용-용이성에서 매우 유사한, IVN 구성의 몇몇 추가적 단계를 수행하는 것을 수반할 수 있다. 클라이언트는, 예컨대, 프로그램 관리/행정 인터페이스(예컨대, 콘솔 또는 애플리케이션 프로그래밍 인터페이스(API))를 통하여 IVN에 대한 PAE의 생성을 요청하고, 그 후 사용자-친화적 서비스 명칭에 의해 식별된 선택된 서비스와 PAE를 연관시킬 수 있다. 클라이언트는 그 후 일부 실시형태에서는, 목적지가 공중-액세스가능한 서비스의 어느 노드 또는 자원인 트래픽에 대한 표적으로서, 예컨대, IVN의 하나 이상의 서브넷에 대해 셋업된 루트 테이블에서 PAE를 특정할 수 있다. 일부 구현에서, (서비스 명칭 "Svc1"과 같은) 일반적 별칭은 루트 테이블에서 목적지로서 서비스를 표시하는데 사용될 수 있고, 그리고 PAE에 배정된 식별자는 표적으로서 표시될 수 있다. 그러한 구현에서, 클라이언트는 목적지를 특정할 때 서비스에 대한 어느 IP 주소도 식별시킬 필요가 없을 수 있다. 적어도 일부 실시형태에서, 클라이언트는, 예컨대, IVN 바깥에서 구현된 여러 다른 서비스로의 액세스를 가능하게 하도록, 소정 IVN에서 수 개의 다른 PAE를 셋업할 수 있다.

[0011] 특정 IVN으로부터 서비스로 의도된 트래픽에 대한 표적으로서 PAE가 구성 및 표시된 후에, (공중 IP 주소가 아니라 사설 IP 주소가 컴퓨터 인스턴스에 배정된) IVN의 컴퓨터 인스턴스 상에서 실행되는 클라이언트 애플리케이션은 그러한 요청이 인터넷-접속된 디바이스로부터 발행되는 방식과 유사하게 서비스에 요청을 발행할 수 있다. 예컨대, DNS 요청은 서비스의 공중 IP 주소를 획득하도록 컴퓨터 인스턴스로부터 (예컨대, 제공자 네트워크의 DNS 서버에) 발행될 수 있다. 애플리케이션은, 컴퓨터 인스턴스의 운영 체제 또는 다른 컴포넌트에 의해 목적지로서 서비스의 공중 IP 주소 및 소스로서 인스턴스의 사설 IP 주소를 갖는 하나 이상의 기초 패킷으로 변환될 수 있는, 서비스 요청을 웹 서비스 API를 (또는 서비스에 의해 지원된 어느 유사한 프로그램 인터페이스라도) 사용하여 제출할 수 있다.

[0012] 앞서 언급된 바와 같이, 컴퓨터 인스턴스는 인스턴스 호스트 상에서 실행되는 게스트 가상 머신으로서 구현될 수 있다. 적어도 일부 실시형태에서, 인스턴스 호스트는, (흔히 "dom-0" 또는 도메인 제로 인스턴스라고 칭해지는) 특권 운영 체제 인스턴스 및/또는 하이퍼바이저와 같은, 가상화 관리 소프트웨어 스택의 다양한 컴포넌트를 포함할 수 있다. (여기에서는 VMC라고 지칭될 수 있는) 그러한 가상화 관리 컴포넌트는 게스트 가상 머신에서 발행된 자원 요청을 하드웨어 자원에서 수행된 물리적 연산으로 변환하는 것을 책임지고 있을 수 있다. 일 실시형태에서, 인스턴스 호스트에서 실행되는 VMC는 컴퓨터 인스턴스로부터 발행된 기초 패킷을 가로챌 수 있고, 그리고 VMC는 인스턴스 호스트가 배속되는 물리적 네트워크를 통한 송신을 위해 기초 패킷이 변환되어야 하는 방법(또는 여부)을 결정하는 것을 책임지고 있을 수 있다. 일부 구현에서, VMC는 서비스로 지향된 트래픽에 대한 표적으로서 PAE의 선택을 표시하는 IVN 메타데이터 레코드로의 액세스를 가질 수 있고, 그리고 또한 서비스의 공중 IP 주소의 리스트로의 액세스를 가질 수 있다. 그래서, VMC는 가로채인 기초 패킷이 PAE와 연관된 서비스로 송신되어야 한다고 결정할 수 있을 수 있다.

[0013] 적어도 일부 실시형태에서, (IVN이 구성되는 가상 컴퓨팅 서비스, 및 PAE에 배정된 목적지 서비스를 포함하는) 다양한 서비스는 제공자 네트워크의 각각의 논리적으로 구별되는 부분에 배정될 수 있다. 소정 쌍의 서비스 간 트래픽은 소스 서비스로부터 목적지 서비스에 도달하기 위해 (보더 네트워크라고 지칭될 수도 있는) 브리지 네트워크를 순회해야 할 수 있다. 그러한 브리지 네트워크는 또한, 소스 및 목적지 서비스 네트워크가 제공자 네트워크의 서브셋이라고 생각될 수 있는 것처럼, 제공자 네트워크의 특수-목적 서브셋이라고 생각될 수 있다. 명칭이 내포하듯이, 브리지 네트워크는 제공자 네트워크의 다양한 논리적으로 구별되는 부분들 간 중개자 네트워크로서(그리고, 일부 경우에는, 제공자 네트워크와 외부 네트워크 간 중개자로서) 역할할 수 있다. VMC는 목적지 서비스에 도달하기 위해 순회되어야 하는 브리지 네트워크로의 직접 액세스를 갖지는 않을 수 있고, 그래서

그러한 브리지 네트워크 상으로 패킷을 라우팅할 수 있는 중개자의 사용을 필요로 할 수 있다. 적어도 일부 실시형태에서는, 그에 따라, VMC는 기초 패킷의 콘텐츠를 터널링 중개자에, 예컨대, 제1 캡슐화된 버전의 패킷으로 전달할 수 있다. 이러한 제1 캡슐화 패킷은 그 후 터널링 중개자에 의해 선택된 터널링 프로토콜에 따라 변환될 수 있고, 그리고 제2 캡슐화 버전의 패킷은 브리지 네트워크 경로 또는 터널을 통하여 목적지 서비스의 노드에 송신될 수 있다. 다양한 다른 캡슐화 접근법 중 어느 것이라도 다양한 실시형태에서 캡슐화의 어느 하나의 단계에 사용될 수 있고; 캡슐화 기술의 일부 특정 예는 아래에서 더 상세히 설명된다.

[0014] 일 실시형태에서, 터널링 중개자에 의해 부가된 헤더 또는 헤더들은 목적지 서비스와 연관된 PAE 및/또는 소스 IVN의 표현 또는 인코딩을 포함할 수 있다. 일 구현에서, 예컨대, 터널링 프로토콜은, IPv6 주소 비트 중 일부가 IVN 및/또는 PAE 식별자를 인코딩하는데 사용되는, IPv6-호환가능한 패킷 포맷 내에 IPv4 기초 패킷의 캡슐화를 수반할 수 있다. 목적지 서비스에서, (예컨대, 서비스 요청, 및 소스 컴퓨터 인스턴스의 사설 IP 주소를 포함하는) 기초 패킷의 콘텐츠는, PAE 및/또는 IVN의 식별자와 함께, 캡슐화된 버전으로부터 추출될 수 있다. 일부 실시형태에서, IVN 또는 PAE 식별자는, 아래에서 더 상세히 설명되는 바와 같이, 동일한 사설 IP 주소가 배정되었을 수 있는 (다른 IVN들에서의) 소스 컴퓨터 인스턴스들 간을 구별하는데 유용할 수 있다. 기초 패킷 바디에 표시된 요청된 연산이 수행될 수 있고 그리고, 예컨대, 역방향으로 유사한 유형의 터널링 및 캡슐화 기술을 사용하여 소스 인스턴스 호스트에서의 요청하는 애플리케이션으로 반환될 수 있다.

[0015] 클라이언트는 적어도 일부 실시형태에서는, 예컨대, 앞서 언급된 종류의 관리 프로그램 인터페이스를 사용하여 액세스 제어 정책을 PAE에 적용할 수 있을 수 있다. 액세스 제어 정책은, 예컨대, 허용(또는 금지)되는 서비스 요청 또는 연산의 유형, 연산이 허용/금지되는 객체(예컨대, 저장-관련 서비스에서의 파일 또는 디렉터리), 정책이 적용되는 시간 기간(예컨대, 근무일의 특정 시간), 정책이 적용되는 대표사용자(예컨대, 특정 사용자 또는 그룹) 등을 표시할 수 있다. 그러한 정책이 PAE에 배정되는 일부 실시형태에서, 서비스에서 캡슐화 패킷으로부터 추출된 요청은 그것들이 해당 정책을 위반하지 않음을 보장하도록 체크될 수 있다. 다른 실시형태에서, 잠재적 정책 위반은 목적지 서비스에서 체크되는 것에 부가하여 또는 그 대신에 IVN측에서 체크될 수 있다 - 예컨대, VMC는 요청이 사용될 PAE와 연관된 정책을 위반한다고 그것이 결정하였으면 요청의 송신을 중단할 수 있다.

[0016] 일 실시형태에서, PAE는 제공자 네트워크에 의해 구현된 서비스와 IVN 간 패킷을 라우팅하는데 뿐만 아니라, 제공자 네트워크에서의 다른 곳에서 구현되는 제3자 서비스와 IVN 간 패킷을 라우팅하는데에도 사용될 수 있다. 그러한 실시형태에서, 제3자(예컨대, 제공자 네트워크의 가상 컴퓨팅 서비스의 다른 고객)는 제공자 네트워크 자원의 소정 세트를 사용하여 서비스를 셋업하고, 그리고 서비스가 액세스될 수 있는 공중 IP 주소를 광고할 수 있다. 제3자 제공자는, 예컨대, 제공자 네트워크의 구성 관리자에 요청을 제출함으로써, PAE 액세스에 그들 서비스를 등록할 수 있다. 구성 관리자는 PAE가 표적으로서 표시되는 루트를 통한 액세스를 후보 제3자 서비스에 지원할 수 있음을 검증할 수 있다. 예컨대, 구성 관리자는 일부 실시형태에서는 제3자 서비스에 (지능형 부하 밸런서와 같은) 터널링 프로토콜을 구현할 수 있는 전단부 노드의 배정을 개시할 수 있다. 다른 실시형태에서, 제3자 서비스 오퍼레이터가 터널링 프로토콜을 구현하도록 의도되는 노드를 이미 셋업하였으면, 그러한 노드의 능력이 검증될 수 있다. 제3자 서비스가 등록되었고, 그리고 터널링 프로토콜에 따라 패킷을 캡슐화 및 추출(캡슐화-해제)할 수 있는 전단부 노드가 셋업된 후에, 클라이언트는 제3자 서비스에 액세스하도록 그들 IVN에서 PAE를 구성할 수 있다. 예컨대, 제3자 서비스의 명칭 또는 별칭(예컨대, "ThirdPartySvc1")은 프로그램 인터페이스를 사용하여 클라이언트에 의해 PAE와 연관될 수 있는 서비스 목적지 옵션(예컨대, PAE 지원에 대해 이미 구성되어 있는 공중-액세스가능한 서비스를 표현하는 "StorageSvc1", "DBSvc1" 등)의 리스트에 추가될 수 있다.

[0017] 예시적 시스템 환경

[0018] 도 1은, 적어도 일부 실시형태에 따라, 고객 네트워크를 순회하지 않고 그리고 IVN에서 공중 IP 주소를 배정하지 않고 하나 이상의 공중-액세스가능한 서비스와 제공자 네트워크의 고립된 가상 네트워크 간 네트워크 트래픽의 라우팅을 가능하게 하도록 사설 별칭 종단점(PAE)이 확립될 수 있는 일례의 시스템 환경을 예시한다. 도시된 바와 같이, 시스템(100)은 공중-액세스가능한 서비스(Svc1)(즉, 그 클라이언트가 공중-광고된 IP 주소 또는 URI를 통하여 요청을 제출할 수 있게 하는 서비스) 및 가상 컴퓨팅 서비스(VCS)를 포함하는 복수의 서비스가 구현되는 제공자 네트워크(102)를 포함한다. 공중-액세스가능한 서비스(Svc1)는, 예컨대, 임의-크기의 저장 객체로의 웹-서비스-기반 액세스를 제공하는 저장 서비스, 비-관계형 데이터베이스 서비스, 관계형 데이터베이스 서비스, 통지 서비스, 메시지 큐 서비스, 또는 각종 다른 유형의 서비스 중 어느 것이라도 포함할 수 있다. 이들 서비스의 각각은, 예컨대, 그 자신의 관리 또는 제어-평면 계층을 갖는 제공자 네트워크의 논리적으로 별개의 부분을 집합적으로 형성하는 복수의 호스트, 저장 디바이스 및 다른 컴퓨팅 장비를 포함할 수 있다. 도 1에서, 예

컨대, VCS의 자원은 VCS 네트워크(104) 내에 위치하는 한편, Svc1의 자원은 Svc1 네트워크(170) 내에 위치한다.

[0019] VCS 네트워크(104) 내에는, IVN(110A) 및 IVN(110B)과 같은 여러 다른 고립된 가상 네트워크(IVN)(110)가 다양한 클라이언트를 대행하여 확립될 수 있다. 대행하여 조정 IVN(110)이 확립되는 클라이언트는 IVN의 네트워킹 구성에 대해 상당한 융통성을 승인받을 수 있다 - 예컨대, 클라이언트는 IP 주소가 IVN 바깥에서 사용 중인 다른 것들과 중첩하지 않음을 보장해야 할 필요 없이 소망의 IP 주소를 다양한 컴퓨트 인스턴스(112)에 배정하고, 서브넷을 셋업하고, 루트 테이블을 파플레이팅하고 등을 할 수 있다. 도시된 바와 같이, 각각의 IVN은 IVN(110A)에서의 IH(130A, 130B), 및 IVM(110B)에서의 IH(130M, 130N)와 같은 복수의 인스턴스 호스트(IH)(130)를 포함할 수 있다. 하나 이상의 컴퓨트 인스턴스(CI)(112)는, IH(130A)에서의 CI(112A), IH(130B)에서의 CI(112B), IH(130M)에서의 CI(112K), 및 IH(130N)에서의 CI(112L)와 같이, 각각의 IH(130)에서 인스턴스화될 수 있다. 컴퓨트 인스턴스의 각각은 하나 이상의 클라이언트 애플리케이션 또는 애플리케이션 서브컴포넌트에 사용될 수 있다.

[0020] 도 1에 도시된 실시형태에서, 서비스(Svc1)는 자원의 적어도 2개의 계층을 포함한다: 인커밍 서비스 요청을 수신하고 그리고 아웃바운드 서비스 응답을 송신하도록 구성되는 (부하 밸런서 및/또는 요청 라우터와 같은) 전단부(FE) 노드(171), 및 서비스 요청을 이행하기 위한 서비스의 로직이 구현되는 후단부(BE) 노드(173). FE 노드(171A, 171B, 171C)와 같은, FE 노드 중 적어도 일부는 그것들에 배정된 사설 IP 주소를 가질 수 있고, 그리하여 Svc1이, 예컨대, 공중 인터넷(139)의 디바이스에 그리고 네트워크(185)와 같은 고객-소유 네트워크에서의 인터넷-접속된 디바이스에 공중 액세스가능하게 할 수 있다.

[0021] 묘사된 실시형태에서, 사설 별칭 종단점(PAE)(150)은, 예컨대, CI(110A)가 그것에 배정된 공중 IP 주소를 가질 것을 필요로 하지 않고, 그리고 트래픽이 공중 인터넷(139)의 링크 또는 고객-소유 네트워크(185)를 통과할 것을 필요로 하지 않고, Svc1 네트워크(170)와 (공중 인터넷으로부터 직접 액세스가능하지 않은 사설 IP 주소를 갖는) CI(110A) 간에 Svc1-관련 패킷이 흐를 수 있게 하도록 IVN(110A)에서 확립되었다. 아래에서 더 상세히 설명되는 바와 같이, IVN(110A)에 대한 루트 테이블 엔트리는 일부 실시형태에서는 (CI(110A)가 구성되는 서브넷을 포함하는) IVN(110A)의 하나 이상의 서브넷에서 유래하고 Svc1를 목적지로 하는 트래픽이 PAE(150)로 겨냥되어야 함을 표시하도록 셋업될 수 있다. Svc1의 공중 IP 주소의 리스트와 같은 다른 메타데이터뿐만 아니라, 이러한 루트 테이블 엔트리도, 적어도 일부 실시형태에서는 IVN(110A)의 인스턴스 호스트(130)의 각각 상에서 실행되는 가상화 관리 컴포넌트(VMC)(예컨대, 하이퍼바이저 컴포넌트)에 이용가능할 수 있다. IVN 구성 관리자(106)는 클라이언트가 PAE의 생성, PAE와 특정 서비스의 연관, IVN에 대한 루트 테이블 엔트리의 생성 또는 수정 등을 요청할 수 있게 하는 (애플리케이션 프로그래밍 인터페이스(API), 웹-기반 콘솔, 커맨드 라인 툴, 또는 그래픽 사용자 인터페이스 등과 같은) 하나 이상의 프로그램 인터페이스를 구현할 수 있다.

[0022] 인스턴스 호스트(130A)에서의 VMC는 CI(112A)에서 발생되고 그리고 Svc1로 지향된 서비스 요청을 포함하고 있는 아웃바운드 기초 네트워크 패킷을 가로챌 수 있다. (일부 서비스 요청 및 그들 연관된 요청 파라미터는 하나보다 많은 패킷을 필요로 할 수 있음을 주목한다. 제시를 단순화하기 위해, 이하의 논의에서 서비스 요청은 기초 패킷에 들어맞는다고 가정된다. 그러한 서비스 요청에 대해 여기에서 설명되는 터널링 기술은 또한 다양한 실시형태에서는 패킷 경계를 가로지르는 서비스 요청에 사용될 수 있다.) 서비스 요청은, HTTP(HyperText Transfer Protocol), HTTPs(secure HTTP), XML(Extensible Markup Language) 등과 같은, Svc1에 의해 지원되는 어느 적합한 인터페이스에 따라 포맷팅될 수 있다. 기초 패킷은 소스로서 CI의 사설 IP 주소 및 목적지로서 Svc1의 공중 IP 주소를 표시할 수 있다. VMC는 묘사된 실시형태에서는 제1 캡슐화 프로토콜에 따라 기초 패킷으로부터 제1 캡슐화 패킷을 발생시킬 수 있다. 제1 캡슐화 패킷 내에서, 일부 구현에서 기초 패킷은 바디에 포함될 수 있는 한편, 제1 캡슐화 프로토콜의 하나 이상의 부가적 헤더는 (다른 정보 중에서도) 패킷이 PAE 트래픽을 포함하고 있다는 표시를 포함할 수 있다. 제1 캡슐화 패킷은 묘사된 실시형태에서는, PAE 트래픽(162)에 대해 파선 화살표에 의해 표시된 바와 같이, 인스턴스 호스트(112A)로부터 터널링 중개자의 플리트(140)의 TI(142A)와 같은 터널링 중개자(TI)로 송신될 수 있다. (TI(142A, 142B 등)와 같은 TI로서 셋업된 복수의 컴퓨팅 디바이스를 포함할 수 있는) TI 플리트(140)는, Svc1의 네트워크(170)를 포함하는, 제공자 네트워크의 다양한 다른 논리적으로 분리된 네트워크와 VCS 네트워크(104) 간에 트래픽이 흐를 수 있게 하도록 확립되었을 수 있다. 터널링 중개자는 일부 실시형태에서는 네트워크-관련 프로세싱에 최적화된 특수-목적 컴퓨팅 디바이스를 포함할 수 있다. 다른 실시형태에서, 터널링 중개자는 범용 컴퓨팅 디바이스에서의 실행의 프로세스 또는 스레드를 포함할 수 있다.

[0023] 적어도 일부 실시형태에서, 제1 캡슐화 패킷을 수신시, TI(142A)는 VMC에 의해 부가된 헤더뿐만 아니라 기초 패킷의 콘텐츠도 추출할 수 있다. 일 실시형태에서, TI(142A)는 여러 다른 소스 및 목적지 주소를 각각 기초 패킷

의 소스 및 목적지 주소로부터 발생시키도록 특정 터널링 프로토콜과 연관된 매핑 데이터베이스를 이용할 수 있다. 예컨대, 일 구현에서, 기초 패킷 소스 및 목적지 IP 주소는 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅될 수 있고, 그리고 TI(142A)는 그것들을 내부 브리지 네트워크(160)를 통하여 Svc1 네트워크(170)에 보내질 제2 캡슐화 패킷에 대한 더 긴, IPv6(인터넷 프로토콜 버전 6) 주소로 교체할 수 있다. 내부 브리지 네트워크(160)는 제공자 네트워크에서의 크로스-서비스 트래픽에 대한, 예컨대, 가상 컴퓨팅 서비스로부터 공중-액세스가능한 서비스를 목적지로 하는 트래픽에 대한 경로로서 사용될 수 있다. 일부 실시형태에서, 내부 브리지 네트워크(160)는 보더 네트워크라고 지칭될 수 있고 그리고 공중 인터넷과 가상 컴퓨팅 서비스 간에 흐르는 트래픽에 사용될 수도 있다.

[0024] 일 구현에서는, TI(142A)에서, 기초 패킷의 소스 IP 주소는 아웃바운드 제2 캡슐화 패킷에서 사용될 대응하는 소스 주소를 특업하도록 매핑 데이터베이스에서 키로서 사용될 수 있다. 유사하게, 기초 패킷의 목적지 IP 주소는 그러한 구현에서 아웃바운드 제2 캡슐화 패킷에서 사용될 대응하는 목적지 주소를 특업하도록 매핑 데이터베이스에서 키로서 사용될 수 있다. 적어도 일부 실시형태에서, 제2 캡슐화 패킷에 대한 소스 및 목적지 주소에 대한 더 큰 수의 비트는 TI(142A)가 제2 캡슐화 패킷에 PAE(예컨대, PAE(150))의 식별자 및/또는 소스 IVN(예컨대, CI(112A)에서 유래하는 패킷의 경우에는 IVN(110A))의 식별자의 인코딩을 포함시킬 수 있게 할 수 있다. 일부 실시형태에서, IVN 및/또는 PAE의 식별자는 제1 캡슐화 패킷에서 VMC에 의해 부가된 헤더에 포함될 수 있고, 그리고 TI(142)는 그러한 헤더로부터 식별자를 획득할 수 있다. 다른 실시형태에서, 매핑 데이터베이스로부터 획득된 소스 및 목적지 주소는 PAE 및/또는 IVN의 인코딩된 식별자를 포함할 수 있다.

[0025] TI(142A)에서 발생된 제2 캡슐화 패킷은 브리지 네트워크(160)를 통하여 목적지 서비스(Svc1)의 전단부 노드(171)(예컨대, 171A)로 송신될 수 있다. 전단부 노드(171)는, 라우팅에 사용되는 PAE(예컨대, PAE(150))의 식별자 및/또는 소스 IVN(예컨대, IVN(110A))의 식별자뿐만 아니라, (소스 CI 사설 IP 주소를 포함하는) 기초 패킷의 콘텐츠도 추출하도록 터널링 프로토콜에 따라 캡슐화-해제를 수행할 수 있을 수 있다. 적어도 일부 실시형태에서, 소스 IVN 및/또는 PAE의 식별은, 아래에서 더 상세히 설명되는 바와 같이, 동일한 소스 사설 IP 주소를 갖는 여러 다른 컴퓨터 인스턴스로부터의 서비스 요청들 간을 Svc1 노드가 구별하는 것을 가능하게 할 수 있다. 기초 패킷에 표시된 서비스 요청은 프로세싱을 위해 후단부 노드(173)(예컨대, 173A)로 전달될 수 있다. 요청이 프로세싱된 후에, 기초 응답 패킷은 후단부 노드에서 발생되고, 터널링 프로토콜에 따라 캡슐화되고, 그리고 역방향으로 되돌아 요청의 소스(CI(112A))로 향하여 송신될 수 있다. TI(142)(예컨대, TI(142A)든 또는 다른 TI든)는 내부 브리지 네트워크(160)를 통하여 캡슐화된 응답을 수신하고, 제1 캡슐 프로토콜을 사용하여 수정된 캡슐화 버전을 발생시키고, 그것을 IH(130A)에서의 VMC에 송신할 수 있다. VMC는 기초 응답 패킷을 추출하고 그것을 소스 CI(112A)에 제공할 수 있다.

[0026] 2개의 다른 캡슐화 프로토콜이 위에서 논의되었기는 하지만, 일부 실시형태에서는 공중 액세스가능한 서비스와 컴퓨터 인스턴스 간 트래픽을 용이하게 하도록 단일의 캡슐화 프로토콜만이 요구 또는 사용될 수 있음을 주목한다. 예컨대, 하나의 그러한 실시형태에서, VMC는 내부 브리지 네트워크를 통한 트래픽에 사용되는 터널링 프로토콜을 구현할 수 있을 수 있고, 그리하여 VMC 자체는 터널링 중개자로서 역할할 수 있다. 그러한 실시형태에서, VMC는 목적지로서 PAE(150)와 연관된 공중-액세스가능한 서비스를 갖는 패킷을 가로채고, PAE 및/또는 소스 IVN의 인코딩을 포함하고 있는 캡슐화된 패킷을 발생시키고, 그리고 캡슐화된 패킷을 브리지 네트워크 디바이스 상으로 송신할 수 있다.

[0027] Svc1로 향하여 지향된 트래픽에 대해 루트 테이블 엔트리에서 표적으로서 PAE를 사용함으로써, 클라이언트는, 양자가 또한 도 1에 예시되어 있는, IVN과 Svc1 간 트래픽을 라우팅하는 것에 대한 2개의 다른 접근법을 회피할 수 있을 수 있다. 대행하여 IVN(110B)이 셋업되는 클라이언트는 그 IVN에 대한 인터넷 게이트웨이(182)를 확립하고 그리고/또는 CI(112K)와 같은 그 인스턴스 중 하나에 (공중 인터넷으로부터 액세스될 수 있는) 공중 IP 주소를 배정하기로 결정할 수 있다. 그러한 시나리오에서, CI(112K)에서 발생된 Svc1 요청을 포함하고 있는 기초 패킷은 위에서 설명된 종류의 터널링 프로토콜을 사용하지 않고, 예컨대, 인터넷 게이트웨이(IGW) 트래픽에 대해 표시된 경로(163)와 유사한 경로를 통하여 Svc1 노드(예컨대, FE 노드(171B))에 송신될 수 있다. 일부 경우에서, 공중 IP 주소에서 유래하는 트래픽에 사용된 경로는 공중 인터넷의 링크(139)를 포함할 수 있다. 인터넷 게이트웨이 접근법을 사용하는 것에 비해 PAE 접근법을 사용하는 하나의 잠재적 이점은 IVN(110B)이 (공중 IP 주소가 배정될 필요가 없는) IVN(110A)보다 (공중 IP 주소를 노출하는 것 때문에) 공중 인터넷으로부터의 공격에 더 취약할 수 있다는 것이다.

[0028] PAE의 사용에 대한 제2의 대안에서, 클라이언트는 IVN(110B)과 고객-소유 네트워크(185) 간 보안 접속성을 제공하도록 VPN(가상 사설 네트워크) 게이트웨이(183)를 확립할 수 있다. CI(112L)와 같은 인스턴스로부터 Svc1로

지향되는 패킷은 우선 고객-소유 네트워크(185)로 보내지고, 그리고 그 후 (예컨대, 공중 인터넷 링크(139)를 통하여) (FE 노드(171C)와 같은) Svc1 노드로 보내질 수 있다. 확립된 VPN 게이트웨이(185)를 갖는 (110B)와 같은 IVN은 공중 IP 주소를 이용할 필요가 없고 셋업된 인터넷 게이트웨이(182)를 가질 필요가 없고, 그리고 VPN 게이트웨이만을 사용하는 클라이언트는 그로써 위에서 언급된 보안 취약성을 회피할 수 있음을 주목한다. 그렇지만, 많은 경우에서, 제공자 네트워크 내에서(예컨대, IVN 내에서의 인스턴스에서) 유래하고 제공자 네트워크 내에서의 목적지(예컨대, Svc1 노드)로 겨냥되는 트래픽에 대해 외부 네트워크로의 VPN 접속을 사용하는 것은 여러 면에서 비효율적일 수 있다. 예컨대, 적어도 일부 실시형태에서, PAE 접근법에 비해, VPN 접근법이 사용되면 더 높은 레이턴시에 직면할 수 있고, 더 낮은 처리율이 지속될 수 있고, 그리고/또는 더 높은 과금 비용이 초래될 수 있다. 위에서 논의된 3개의 대안의 라우팅 접근법(즉, PAE를 사용한 라우팅, 소스 IP 주소로서 공중 IP 주소를 사용한 라우팅, 및 VPN을 사용한 라우팅)에 각각 대응하여, 3개의 별개의 FE 노드(171A, 171B, 171C)가 도 1에 도시되어 있기는 하지만, 적어도 일부 실시형태에서는 대안 중 어느 것이라도 사용하여 송신된 트래픽을 어느 소정의 FE 노드라도 취급할 수 있을 수 있다. 그리하여, 3개의 FE 노드의 예시는 FE 노드의 각각의 세트가 다른 접속성 대안에 필요로 됨을 내포한다는 의미는 아니다.

[0029] 일 실시형태에서, 가상 컴퓨팅 서비스는 IVN의 컴퓨트 인스턴스 상에서 실행되는 애플리케이션으로부터 PAE를 사용하여 공중-엑세스가능한 서비스에 액세스하도록 인보크될 수 있는 API의 세트를 노출하는 서비스 접속성 라이브러리(SCL)를 제공할 수 있다. 그러한 시나리오에서, 애플리케이션은 표적 서비스(Svc1)를 표시하는 API 호출을 발행할 수 있고, 여기서 서비스 요청의 콘텐츠는 API 호출의 파라미터에 의해 표시된다. SCL은 애플리케이션이 서비스 요청을 Svc1에 제출하도록 의도한다고 결정할 수 있고, 그리고 서비스 요청을 Svc1에 송신하는데 필요한 적합한 캡슐화의 구현을 개시할 수 있다. 그리하여, 애플리케이션이 기초 패킷의 발생을 개시하는 전통적 접근법을 사용하는 대신에, 서비스 요청으로부터 패킷을 생성하는 작업은 SCL에 의해 취급될 수 있다. 일부 그러한 실시형태에서, 애플리케이션은 표적 서비스의 특정 공중 IP 주소를 획득하는 것조차 필요하지 않다; 예컨대, 서비스 요청의 목적지는 특정 네트워크 주소에 의해서라기보다 서비스 명칭에 의해 표시될 수 있다. 일 실시형태에서, 애플리케이션이 API 호출에서 서비스의 특정 표적 공중 주소를 표시하더라도, SCL은 (SCL에 의해 선택된 실제 목적지가 서비스 요청에 적합하게 응답할 수 있는 한) 서비스 요청의 캡슐화된 버전을 표적 서비스의 다른 공중 또는 사설 IP 주소로 송신할 수 있다.

[0030] 패킷 흐름 예

[0031] 도 2는, 적어도 일부 실시형태에 따라, 고립된 가상 네트워크의 컴퓨트 인스턴스에서 유래하는 패킷을 공중-엑세스가능한 서비스에서의 목적지로 향하여 지향시키는데 관여된 예시적 컴포넌트를 예시한다. 도시된 바와 같이, IVN(210)의 인스턴스 호스트(230)는, 인스턴스(112A, 112B)와 같은, 복수의 컴퓨트 인스턴스(112)를 포함할 수 있다. 각각의 인스턴스(112)는 게스트 가상 머신 상에서 실행되는 각각의 운영 체제 인스턴스를 포함할 수 있다. 클라이언트 애플리케이션의 하나 이상의 컴포넌트는, 컴퓨트 인스턴스(112A)에서의 애플리케이션 프로세스(220A) 및 컴퓨트 인스턴스(112B)에서의 애플리케이션 프로세스(220B)와 같이, 각각의 컴퓨트 인스턴스에서 실행될 수 있다. (네트워크 트래픽에 사용되는 네트워크 인터페이스 카드 또는 NIC와 같은) 인스턴스 호스트의 하드웨어 컴포넌트와 컴퓨트 인스턴스 간 상호작용은 VMC(240)와 같은 하나 이상의 가상화 관리 컴포넌트(VMC)에 의해 관리될 수 있다. VMC는, 예컨대, (때로는 도메인 제로 또는 dom0 운영 체제 인스턴스라고 지칭될 수 있는) 특권 운영 체제 인스턴스 및/또는 하이퍼바이저를 포함할 수 있다.

[0032] 애플리케이션 중 적어도 일부는 묘사된 실시형태에서는 IVN 바깥에서 구현된 하나 이상의 서비스로의 액세스를 필요로 할 수 있다(예컨대, 그것에 서비스 요청을 제출할 수 있고, 그리고 그것으로부터 서비스 응답을 수신할 수 있다). 예컨대, 애플리케이션 프로세스(220B)는 공중-엑세스가능한 서비스(Svc1)로의 액세스를 필요로 할 수 있다. 따라서, 도 2에서 라벨 "1"이 붙은 화살표에 의해 표시된 바와 같이, DNS 질의(204)는 컴퓨트 인스턴스로부터 DNS 서버(252)(예컨대, IVN(210)이 구현되어 있는 가상 컴퓨팅 서비스 네트워크 내로부터 액세스가능한 DNS 서버)로 제출되어 Svc1의 IP 주소를 요청할 수 있다. DNS 서버(252)는, 라벨 "2"이 붙은 화살표에 의해 표시된 바와 같이, Svc1에 의해 광고 또는 노출된 공중 IP 주소(205)를 제공할 수 있다. 적어도 일부 실시형태에서, DNS 룩업은 애플리케이션이 얼마 동안 Svc1과 상호작용하지 않은 경우에만 수행되면 된다. 즉, Svc1의 주소가 획득되고 나면, 그것은 DNS 서버(252)와의 추가적 상호작용 없이 (예컨대, 주소가 유효한 채로 있는 한) 인스턴스(112B)에 의해 오랜 기간 동안 사용될 수 있다.

[0033] Svc1로 지향된 서비스 요청은 묘사된 실시형태에서는 인스턴스(112B)에서 발생한 기초 패킷(250)의 바디에 포함되고 그리고 Svc1로 향한 전파를 위해 컴퓨트 인스턴스의 네트워킹 스택으로 보내질 수 있다. 기초 패킷(250)은 그 소스 주소로서 인스턴스(112B)의 사설 IP 주소, 및 목적지로서 Svc1의 공중 IP 주소를 표시할 수 있다.

다른 네트워크 패킷에서와 같이, 기초 패킷은, 라벨 "3"이 붙은 화살표에 의해 표시된 바와 같이, (물리적 네트워크 송신을 책임지고 있을 수 있는) VMC(240)에 의해 가로채일 수 있다.

[0034] VMC(240)는 묘사된 실시형태에서는, Svc1 공중 IP 주소의 리스트(236) 및 루트 테이블(235)과 같은, PAE-관련 메타데이터 및 다른 IVN 메타데이터로의 액세스를 가질 수 있다. 루트 테이블(235)은 다양한 목적지로 의도된 패킷을 라우팅하도록 사용되어야 하는 표적을 표시하는 엔트리를 포함할 수 있다 - 예컨대, 범위(N1.N2.N3.*)에 있는 목적지 주소를 갖는 패킷에 대해서는, 표적(K.L.M.N)이 사용되어야 한다. Svc1의 어느 노드로 의도된 패킷에 대한 루트 테이블이 도 2에 도시된 예에서 생성되었으며, 사실 별칭 종단점(PAE-1)이 표적으로서 표시되어 있다. 기초 패킷(250)에 표시된 목적지 및 그것에 이용가능한 PAE-관련 메타데이터의 분석에 기반하여, VMC(240)는 묘사된 실시형태에서는 제1 캡슐화 패킷(251)을 발생시킬 수 있다. 패킷(251)의 바디는 (그 소스 및 목적지 정보를 포함하는) 기초 패킷(250)의 콘텐츠를 편입하고 있을 수 있는 한편, 부가적 헤더(260)는 VMC와 터널링 중개자(242) 간 통신에 사용되는 제1 캡슐화 프로토콜(P1)에 따라 VMC(240)에 의해 발생될 수 있다. 캡슐화된 패킷(251)은, 라벨 "4"이 붙은 화살표에 의해 표시된 바와 같이, VMC(240)로부터 특정 터널링 중개자(242)로 보내질 수 있다. 적어도 일부 실시형태에서, P1 헤더(260)는 기초 패킷이 PAE1과 연관되고 그리고/또는 IVN(210)에서 유래된다는 표시를 포함할 수 있다. VMC(240)와 터널링 중개자(242) 간 경로는 자체가, 예컨대, 다양한 홉에 대한 표적이 도 2에는 도시되지 않은 루트 테이블 엔트리에 기반하여 선택되는 수 개의 홉을 포함할 수 있음을 주목한다.

[0035] 터널링 중개자(242)는 캡슐화된 패킷(251)에 포함되어 있는 기초 패킷(250)의 소스/목적지 헤더 및/또는 P1 헤더(260)를 조사할 수 있다. (여기에서는 터널링 프로토콜이라고 지칭될 수도 있는) 제2 캡슐화 프로토콜(P2)의 매핑 데이터베이스(262)를 사용하여, 터널링 중개자(242)는 하나 이상의 P2 헤더(261) 및 기초 패킷(250)을 포함하는 제2 캡슐화 패킷(255)을 발생시킬 수 있다. 기초 패킷의 소스 및 목적지 주소는 패킷(255)에 사용될 패킷 헤더 및 새로운 소스를 식별시키도록 일부 실시형태에서는 매핑 데이터베이스(262) 내로 인덱스로서 사용될 수 있다. 일부 구현에서, 프로토콜(P2)에 따라, IPv4 기초 패킷(250)은, 예컨대, SIIT(Stateless IP/ICMP(Internet Protocol/Internet Control Message Protocol) Translation) 또는 유사한 IPv4-IPv6 헤더 변환 메커니즘을 사용하여 IPv6-호환가능한 패킷(255) 내에 캡슐화될 수 있다. 다른 실시형태에서는, 제공자 네트워크의 사유 캡슐화 프로토콜이 캡슐화 패킷(255)을 발생시키는데 사용될 수 있다. 일부 실시형태에서는, IPv6를 사용하는 대신에, TCP 옵션 헤더와 같은 부가적 IPv4 헤더가 터널링 중개자에 의해 사용될 수 있거나, 또는 UDP(User Datagram Protocol) 캡슐화가 (예컨대, UDP 메시지 내에 기초 패킷 콘텐츠를 편입시킴으로써) 사용될 수 있다. 일부 실시형태에서 P1 헤더(260) 및 P2 헤더(261) 내에 포함될 수 있는 정보의 종류의 예는 도 4에서 제공되고 아래에서 설명된다. 캡슐화 패킷(255)은 Svc2 노드에 도달하기 위해 순회되어야 하는 적합한 브리지 네트워크(160)의 디바이스로 터널링 중개자(242)로부터 송신될 수 있다.

[0036] 도 3a 및 도 3b는, 적어도 일부 실시형태에 따라, 고립된 가상 네트워크의 컴퓨터 인스턴스에서 유래하는 패킷을 프로세싱할 수 있는 서비스-측 컴포넌트의 각각의 예를 예시한다. 앞서 언급된 바와 같이, 일부 실시형태에서, 적어도 2개 유형의 서비스는 PAE가 구성되어 있는 IVN으로부터 클라이언트 액세스를 지원할 수 있다. 제1 유형의 서비스는 제공자 네트워크 오퍼레이터에 의해 구현될 수 있는 한편, 제2 유형은 제공자 네트워크의 고객과 같은 제3자에 의해 구현된 서비스를 포함할 수 있다. 도 3a에 도시된 제공자 네트워크-구현된 서비스(376)와 같은 제1 유형의 서비스에 대해, 전단부 노드(374)는 터널링 중개자(242)에 의해 사용된 캡슐화 프로토콜(P2)에 정통할 수 있다(즉, 구현할 수 있다). 즉, 프로토콜(P2)에 따라 포맷팅된 패킷(255)을 수신시, 서비스(376)의 전단부 노드(374)는 기초 패킷 콘텐츠를 추출하고 그리고 프로세싱을 위해 후단부 노드(374)에 보내질 수 있는 대응하는 내부 요청(350)을 발생시킬 수 있을 수 있다. 일부 경우에, 제공자 네트워크-구현된 서비스는, 예컨대, HTTP(Hypertext Transfer Protocol)에 따라 포맷팅된 서비스 요청을 지원할 수 있고, 그리고 전단부 노드는 기초 패킷을 라우팅하는데 사용된 PAE 및/또는 기초 패킷이 발생된 소스 IVN의 식별자를 표시하기 위해 기초 요청에 하나 이상의 엑스-포워드드-포-헤더(X-Forwarded-For header)를 부가할 수 있다. 요청된 연산이 후단부 노드에서 수행된 후에, 응답은, 예컨대, 응답 경로에서 유사한 캡슐화 기술을 사용하여 요청 컴퓨터 인스턴스로 되돌려 송신될 수 있다. 예컨대, 서비스(376)의 P-2 정통 전단부 노드(374)는 기초 응답의 적어도 일부를 포함하는 P2-준수 캡슐화 패킷을 발생시키고 그것을 브리지 네트워크(160)를 통하여, 순차로 P1-준수 캡슐화 패킷을 발생시키고 그것을 적합한 VMC(240)에 송신할 수 있는, 터널링 중개자(242)에 보낼 수 있다. VMC(240)는 P1-준수 패킷으로부터 기초 응답을 추출하고 그것을 (112B)와 같은 소스 컴퓨터 인스턴스에 제공할 수 있다.

[0037] 제공자 네트워크 오퍼레이터에 의해 구현된 서비스의 노드와는 대조적으로, (도 3b에 도시된 제3자 서비스(378)와 같은) 적어도 일부 제3자 서비스는 프로토콜(P2)에 따라 발생된 캡슐화 패킷(255)으로부터 기초 패킷을 추

출할 수 있는 노드를 포함하지 않을 수 있다. 일부 경우에, 예컨대, P2의 상세는 제3자 서비스 오퍼레이터에 이용가능하지 않을 수 있거나, 또는 그러한 오퍼레이터는 P2-준수 서비스 노드를 구축할 전문 지식 또는 자원을 가지고 있지 않을 수 있다. 따라서, 적어도 일부 구현에서, PAE-기반 라우팅에 대해 그러한 제3자 서비스를 등록하라는 요청에 응답하여 또는 후-등록 요청에 응답하여, 제공자 네트워크의 구성 또는 제어-평면 컴포넌트는 하나 이상의 서비스-측 P2-정통 중개자(370)를 확립할 수 있다. 그러한 서비스-측 중개자(370)는 캡슐화 패킷(255)으로부터 기초 패킷(250)을 추출하고, 그것들을 제3자 서비스(378)의 전단부 노드(375)에 송신할 수 있다. 전단부 노드(375)는 그 후 기초 패킷(250)을, 사유 제3자 포맷, HTTP, 또는 서비스(378)의 후단부 노드(380)에 의해 예상된 어느 다른 인터페이스에 따라 발생될 수 있는, 내부 요청(352)으로 변환할 수 있다. 내부 요청(352)에 대응하는 연산은 그 후 후단부 노드에서 이행될 수 있고, 그리고 응답은 요청이 유래한 컴퓨터 인스턴스로 역방향으로 중개자(370)에서의 캡슐화 후에 송신될 수 있다.

[0038] 캡슐화 포맷

[0039] 도 4는, 적어도 일부 실시형태에 따라, 컴퓨터 인스턴스에서 유래하는 기초 패킷에 대한 캡슐화 포맷의 예를 예시한다. 도시된 바와 같이, 기초 패킷(402)은 묘사된 실시형태에서는 소스 및 목적지 IP 버전 4 주소를 표시할 수 있다. 예컨대, 고립된 가상 네트워크 내에서, (IVN 바깥에 광고되지 않은) 사설 IP 주소 "10.0.1.2"는 클라이언트에 의해 컴퓨터 인스턴스(112)에 지정되었을 수 있고, 그리고 이러한 사설 IP 주소는 기초 패킷(402)에서 소스 주소로서 표시될 수 있다. 공중 IP 버전 4 주소 "176.32.101.25"는 컴퓨터 인스턴스로부터 액세스되어야 하는 특정 공중-액세스가능한 서비스(Svc1)의 주소에 대한 DNS 질의에 응답하여 DNS 서버에 의해 제공되었을 수 있다. 서비스의 이러한 공중 주소는 기초 패킷(402)의 목적지로서 표시될 수 있다. 또한, TCP 포트 번호가 기초 패킷에 표시될 수 있다. 예컨대, 컴퓨터 인스턴스에서의 소스 포트로서 포트 4321 그리고 목적지 서비스 포트로서 포트 80. 기초 패킷(402)의 페이로드 또는 바디 부분은, 서비스 요청의 파라미터뿐만 아니라, 저장 서비스로 지향된 판독 또는 기록 요청과 같은, 송신되고 있는 서비스 요청의 유형을 표시할 수 있다.

[0040] 기초 패킷(402)은 묘사된 실시형태에서는 터널링 중개자와의 통신에 사용된 제1 캡슐화 프로토콜(P1)에 따라 인스턴스의 호스트에서 가상화 관리 컴포넌트(예컨대, VMC-x)에 의해 캡슐화될 수 있다. P1-호환가능한 패킷(404)에서, 기초 패킷은 바디에 포함될 수 있고, 그리고 하나 이상의 P1 헤더가 부가될 수 있다. VMC의 식별자는 소스로서 표시될 수 있고, 그리고 터널링 중개자 플리트는 일부 구현에서는 목적지로서 표시될 수 있다. 예컨대, 목적지로서 Svc1을 특정하는 루트 테이블 엔트리에 표시된 PAE를 표시하고 그리고/또는 기초 패킷이 발생된 소스 IVN을 식별시키는 다른 P1-특정 헤더가 일부 실시형태에서는 패킷(404)에 포함될 수 있다. P1-호환가능한 포맷은 적어도 일부 실시형태에서는 다양한 헤더 필드에 IP 버전 4 포맷을 사용할 수 있다.

[0041] 터널링 중개자에서, P1-호환가능한 패킷(404)은 묘사된 실시형태에서는 그 P1 헤더가 벗겨질 수 있고, 그리고 브리지 네트워크를 가로질러 목적지 서비스로의 통신에 사용될 터널링 프로토콜(P2)에 따라 다른 세트의 헤더가 부가될 수 있다. 묘사된 실시형태에서, 터널링 중개자에 의해 발생된 P2-호환가능한 패킷(406)은 IPv6 소스 및 목적지 필드를 포함할 수 있다. IPv6에서 소스 주소에 이용가능한 128 비트의 32-비트 서브세트는 일부 실시형태에서는 소스 컴퓨터 인스턴스의 사설 IPv4 주소를 표시하는데 사용될 수 있다. 유사하게, IPv6에서 목적지 주소에 이용가능한 128 비트의 32-비트 서브세트는 목적지 서비스의 IPv4 공중 주소를 표시하는데 사용될 수 있다. 예컨대, 패킷(406)의 소스 주소의 낮은-차수 비트는 소스 IPV4 주소 10.0.1.2의 대체 표현인 0A00:0102이고, 그리고 패킷(406)의 목적지 주소의 낮은-차수 비트는 IPv4 목적지 주소 176.32.101.25의 대체 표현인 B020:657D이다.

[0042] 일 구현에서, 도 4에 도시된 주소 구조(408)에 표시된 바와 같이, IPv6에서 이용가능한 128 주소 비트는 터널링 프로토콜(P2)에 따라 다음과 같이 사용될 수 있다. 가장 낮은-차수 32 비트(비트 0 내지 31)는 소스 또는 목적지 IPv4 주소에 사용될 수 있고, 비트 40-71는 PAE 식별자를 표시하는데 사용될 수 있고, 그리고 비트 80-127는 소스 IVN 또는 목적지 서비스가 구현되고 있는 제공자 네트워크 장소 또는 데이터 센터에 할당된 48-비트 IPv6 전치부호에 사용될 수 있다. PAE 식별자를 위해 확보된 32 비트의 24 비트(예컨대, 더 높은-차수 24 비트)는 묘사된 실시형태에서는 소스 IVN 식별자를 표시할 수 있다. 그리하여, 적어도 일부 실시형태에서, IVN 식별자는 PAE 식별자 내에 매립되고, 그리하여 그로부터 추출가능할 수 있다. 다른 구현에서는 소스 IVN 식별자, PAE 식별자, 또는 양자를 표현하기 위한 다른 인코딩 기술이 사용될 수 있다. 어떤 번호의 비트는, 비트 31-39 및 비트 72-80과 같이, 예컨대, PAE를 고유하게 식별하는데 필요로 되는 비트 수에서의 가능한 장래 증가에 부응하도록 장래 사용을 위해 예비할당(RFU)될 수 있다. 도시된 바와 같이 (예컨대, 최하위 32 비트가 IPv4 소스/목적지 주소를 인코딩하는데 사용되게) P2-호환가능한 캡슐화 패킷 주소를 구조화하는 이점은 적어도 일부 부하 밸런서는 그것들이 그러한 IPv6-호환가능한 패킷을 수신할 때 128 비트의 바로 그 IPv4 부분이 목적지로서 표시되면

선택될 것과 동일한 목적지를 선택할 수 있다는 것이다. 다른 실시형태에서는 IPv6-호환가능한 주소 구조를 파 티셔닝하는데 다른 접근법이 사용될 수 있다, 예컨대, 거기에서는 다른 서브세트의 비트가 IVN 식별자 및/또는 PAE 식별자를 표시하는데 사용된다.

[0043] 적어도 일부 실시형태에 따라, 터널링 프로토콜은, 예컨대, 별개의 터널링 중개자 플리트에 대한 필요성 없이 소스 컴퓨트 인스턴스가 실행되는 인스턴스 호스트에서 구현될 수 있다. 그러한 실시형태에서, 도 4에 예시된 2-스텝 캡슐화는 인스턴스 호스트에서 실행되는 다른 서비스 접속성 컴포넌트에서 그리고/또는 VMC에서 구현된 단일 논리적 스텝으로 조합될 수 있다. 그러한 실시형태에서 VMC 및/또는 서비스 접속성 컴포넌트는 소스 컴퓨 트 인스턴스와 목적지 서비스 간 터널링 중개자라고 생각될 수 있다.

[0044] PAE 구성

[0045] 도 5는, 적어도 일부 실시형태에 따라, PAE 구성 요청 및 응답의 예를 예시한다. 도시된 바와 같이, 제공자 네 트워크의 구성 관리자(592)는, API, 웹-기반 콘솔, 커스텀 GUI 또는 커맨드-라인 툴과 같은, 하나 이상의 프로 그램 인터페이스(550)를 구현할 수 있다. 그러한 인터페이스를 사용하여, 클라이언트(502)는, 예컨대, 요청에서 파라미터로서 IVN 식별자를 표시하여, 특정된 IVN에서 사실 별칭 종단점을 생성하라는 "IVN-에서-PAE-생성" 요 청(505)을 제출할 수 있다. 응답하여, 구성 관리자(592)는 그 구성 데이터베이스에서 요청된 PAE에 대한 하나 이상의 엔트리를 발생 및 저장하고, 그리고 응답(507)에서 새롭게 생성된 PAE의 식별자를 제공할 수 있다. 일부 실시형태에서, 하나 이상의 PAE는 클라이언트에 대해 IVN이 확립될 때 IVN에 대해 자동으로 셋업될 수 있고, 그 러한 시나리오에서는 명시적 PAE 생성 요청이 필요로 되지 않을 수 있다.

[0046] 클라이언트(502)는, 트래픽이 PAE를 사용하여 라우팅되어야 하는 특정 서비스를 표시하여, PAE가 생성된 후에 "PAE-에-서비스-배정" 요청(509)을 구성 관리자(592)에 제출할 수 있다. 일부 구현에서, PAE 식별자 및 서비스 식별자는 그러한 요청에서 파라미터로서 공급될 수 있다. 응답하여, 구성 관리자(592)는 PAE에 관하여 그 구성 메타데이터를 업데이트하고 서비스 배정의 확인응답(511)을 제공할 수 있다. 일부 실시형태에서, 프로그램 인터 페이스(550)는 구성되고 있는 PA와의 연관에 하나가 선택될 수 있는 등록된 서비스 명칭의 리스트를 (예컨대, 드롭-다운 메뉴에서) 제공할 수 있다.

[0047] 다양한 유형의 액세스 제어 정책은 일부 실시형태에서는, 예컨대, 정책 및 PAE를 특정하는 "PAE-에-정책-배정" 요청(513)에 응답하여 PAE에 배정될 수 있다. 해당 정책의 예는 도 6에서 도시되고 아래에서 설명된다. 구성 관 리자(592)는 PAE와 정책의 연관 및 표시된 정책의 표현을 저장하고, 그리고 연관의 확인응답(515)을 클라이언트 에 제공할 수 있다. 적어도 일부 실시형태에서, 정책의 연관이 PAE에 대해 요청될 수 있기는 하지만, 정책의 실 제 시행은 (a) PAE에 배정된 서비스 (n) 정책을 시행하도록 PAE에 배정된 서비스에 의해 인보크될 수 있는, 제 공자 네트워크의 권한부여 및 인증 서비스와 같은, 다른 서비스 또는 (c) PAE에 따라 서비스 요청이 라우팅되는 인스턴스 호스트의 VMC 중 하나 이상에서 수행될 수 있다. 일부 실시형태에서, 정책의 표시는, 예컨대, 확인응 답(515)이 클라이언트에 제공되기 전에, PAE에 배정된 서비스의 제어 평면 컴포넌트에 구성 관리자에 의해 송신 될 수 있다.

[0048] 제공자 네트워크의 클라이언트는 또한 일부 실시형태에서는 PAE-지원된 라우팅에 서비스를 등록하라는 요청 (517)을 제출할 수 있다. 예컨대, 제3자 서비스(즉, 제공자 네트워크 오퍼레이터에 의해 직접 관리되지 않는 서 비스)는 제공자 네트워크의 자원의 어떤 세트를 사용하여 확립될 수 있고, 그리고 그러한 제3자 서비스의 오퍼 레이터는 공중 IP 주소가 IVN에서에 의해 사용될 것을 필요로 하지 않고 IVN 내로부터 서비스로의 액세스를 가 능하게 하기를 바랄 수 있다. 그러한 시나리오에서는, 서비스 구성의 상세(예컨대, 서비스의 전단부 노드의 주 소)를 제공하는 "PAE-에-서비스-등록" 요청이 클라이언트(502)에 의해 제출될 수 있다. 적어도 일부 구현에서는, PAE를 확립하는 것을 책임지고 있는 구성 관리자와는 다른 구성 관리자가 서비스를 등록하는 것을 책임지고 있을 수 있고, 그리고 다른 세트의 프로그램 인터페이스가 서비스 등록 요청에 사용될 수 있다. 서비 스 등록 요청에 응답하여, 구성 관리자는 서비스를 수락하고 응답(519)에서 등록된 서비스의 등록된 명칭 또는 식별자를 클라이언트에 제공하기 전에, 예컨대, 제안된 등록될 서비스가 PAE 호환성에 대한 특정 기준을 만족함 을 검증하기 위해 하나 이상의 검정 연산을 수행할 수 있다. 일 구현에서, 예컨대, 서비스의 전단부 컴포넌트는 그것이 제공자 네트워크의 캡슐화 프로토콜을 사용하는 터널링 중개자에 의해 발생된 요청을 수신할 수 있음을 보장하도록 질의 또는 시험될 수 있다.

[0049] 일부 실시형태에서, 부가적 구성 요청 유형은 도 5에서 예시된 것들 이상으로 지원될 수 있다. 예컨대, (도 3b 의 P2-정통 중개자(370)와 같은) 서비스-측 터널링 중개자를 구성하라는 요청은 일부 실시형태에서는 제3자 서 비스를 셋업한 클라이언트에 의해 제출될 수 있다. 일 실시형태에서, 클라이언트는 PAE를 다른 서비스에 제-배

정하거나, 또는 부가적 유형의 구성 요청을 사용하여 하나보다 많은 서비스를 PAE에 배정할 수 있을 수 있다. 일부 구현에서는, 도 5에 도시된 구성 요청의 모든 유형이 지원되지는 않을 수 있다. 앞서 언급된 바와 같이, 클라이언트는 (예컨대, 동일한 IVN 내로부터 여러 다른 서비스에 액세스하도록) 소정 IVN과 연관된 다수의 PAE를 확립할 수 있고, 그리고 다수의 IVN을 갖는 클라이언트는 각각의 그러한 IVN에서 하나 이상의 PAE를 셋업할 수 있다.

[0050] 도 6은, 적어도 일부 실시형태에 따라, PAE 구성 데이터베이스 콘텐츠의 예를 예시한다. 구성 관리자(592)의 도움으로 2개의 PAE가 확립된 특정 IVN(IVN-j)에 대한 구성 데이터베이스가 도시되어 있다. PAE(604A)에는, 서비스 식별자 필드(606A)에 표시된 바와 같이, 서비스 "StorageSvc1"(제공자 네트워크에서 구현된 저장 서비스)가 배정되는 한편, PAE(604A)에는, 서비스 식별자 필드(606B)에 표시된 바와 같이, 서비스 "DBSvc1"(제공자 네트워크에서 구현된 데이터베이스 서비스)가 배정된다. PAE(604A)는 그것에 배정된 액세스 정책(608A)을 갖는 한편, PAE(604B)는 2개의 액세스 정책(608B, 608C)을 갖는다.

[0051] 액세스 정책(608A)은 묘사된 예에서는 범위 CI-IP-주소-범위(610A)에 있는 IP 주소를 갖는 컴퓨터 인스턴스로 또는 그로부터 지향된 StorageSvc1 트래픽에 적용된다. 일부 실시형태에서는, 정책이 적용되어야 하는 트래픽을 표시하는데 IP 주소를 사용하는 대신에, 컴퓨터 인스턴스의 인스턴스 명칭 또는 다른 식별 데이터가 사용될 수 있다. 주소 범위(610A)로부터 요청이 허용되는 연산 유형의 리스트(예컨대, 판독 대 기록)는 정책(608A)의 허용된-연산-유형 필드(612A)에 표시될 수 있고, 그리고 그들 연산이 지향될 수 있는 서비스 StorageSvc1의 객체(예컨대, 디렉터리 "/xyz"에 저장된 객체)는 객체 리스트(614A)에 표시된다. 묘사된 예에서, 정책(608A)이 적용되어야 하는 시간 범위(예컨대, 각각의 근무 요일의 특정 시간, 또는 주간 특정 요일)는 해당 시간 범위 필드(616A)에 표시될 수 있다. 대표사용자의 리스트(예컨대, 사용자 또는 그룹의 식별자)(618A)는 또한 정책(608A)에 대해 연관되어, 정책(608A)에 표시된 규칙에 의해 서비스 요청이 지배되어야 하는 개체를 표시할 수 있다.

[0052] PAE(604B)에 대해 시행될 액세스 정책(608B, 608C)의 각각은, 정책의 규칙이 적용되어야 하는 컴퓨터 인스턴스를 표시하는, 그들 각각의 CI-IP-주소-범위(610)를 표시할 수 있다. (608B)와 같은 일부 정책에서는, 예컨대, 허용되는 연산의 유형에 부가하여 또는 그 대신에, 금지되는 연산의 유형이 (예컨대, 금지된-연산-유형 필드(613)에) 표시될 수 있다. 객체 리스트(614B)에서 "*"에 의해 표시된 바와 같이, 필드(613)에 표시된 연산은 묘사된 예에서는 대표사용자-리스트(618B)에 표시된 대표사용자에 대해 DBSvc1의 모든 객체에 대해 금지될 수 있다. 도시된 바와 같이, 정책에 포함될 수 있는 엔트리의 모든 유형이 모든 정책마다 특정될 필요가 있는 것은 아니다 - 예컨대, 정책(608B)은 해당 시간 범위를 포함하지 않는 한편, 정책(608C)은 대표사용자 리스트를 포함하지 않는다. 정책에 포함되지 않는 엔트리의 유형에 대해서는 디폴트 값이 사용될 수 있다 - 예컨대, 전체 요일이 해당 시간 범위라고 상정될 수 있고, 그리고 정책 규칙은 특정 대표사용자가 열거되지 않으면 모든 대표사용자에 적용될 수 있다. 묘사된 예에서, 필드(612B)는 해당 시간 범위(616C) 동안 필드(614C)에 열거된 객체에 대해 허용된 연산 유형을 표시할 수 있다.

[0053] 일부 실시형태에서, 소정 PAE에 대해 특정 액세스 정책이 클라이언트에 의해 특정되지 않으면, 제공자 네트워크는 대응하는 서비스에 제출된 서비스 요청에 적용될 규칙을 결정하도록 소정 디폴트 세트를 적용할 수 있다. 디폴트는 일부 구현에서는 서비스마다 다를 수 있다. 앞서 언급된 바와 같이, 일부 실시형태에서 PAE가 배정된 서비스는 (서비스의 자신의 노드에서든, 또는, 신원 및 권한부여 관리 서비스와 같은, 제공자 네트워크의 다른 서비스에 요청을 제출함으로써) 정책을 시행하는 것을 책임지고 있을 수 있다. 일부 서비스에 대한 서비스 요청은 요청이 서비스에 도달한 후에 요청되고 있는 연산의 유형을 결정하는 것이 가능할 뿐인 그러한 방식으로 암호화될 수 있고, 그리고 결과로서 액세스 정책은 서비스 단부에서 적용되어야 할 수 있다. 그러한 경우에, 정책은 클라이언트에 의해 정책이 표시되는 구성 관리자(예컨대, IVN 구성 관리자)에 의해 서비스에(예컨대, 서비스의 제어-평면 또는 관리 컴포넌트에) 통신될 수 있다. 다른 실시형태에서, 정책의 규칙 중 적어도 일부는 요청자 단부(예컨대, IVN 단부)에서 시행될 수 있다 - 예컨대, 대응하는 사용자가 해당 정책의 대표사용자 리스트에 열거되고 모든 기록이 열거된 대표사용자에 대해 금지되면 VMC가 컴퓨터 인스턴스로부터 발행된 기록 요청을 거절하는 것이 가능할 수 있다.

[0054] 재-사용된 사설 IP 주소로부터의 요청들 간 구별

[0055] 클라이언트는, 예컨대, 동일한 주소가 다른 곳에서(예컨대, 다른 IVN에서 또는 공중 인터넷에서) 사용 중인지 고려하지 않고, 위에서 설명된 바와 같이 일부 실시형태에서는 그들 선택의 사설 IP 주소를 IVN 컴퓨터 인스턴스에 배정하도록 IVN 네트워크 구성에 승인된 융통성을 사용할 수 있다. 일부 경우에, 클라이언트는 다른 IVN에서의 인스턴스에 동일한 IP 주소를 배정할 수 있다. (서비스에서 수신되는 요청이 오는 소스의 정확한 레코딩을

위해서와 같은) 여러 이유로, 동일한 소스 IP 주소가 요청에 표시될 수 있더라도, 서비스가 다른 IVN으로부터의 요청들 간을 구별할 수 있는 것이 유용할 수 있다.

[0056] 도 7은, 적어도 일부 실시형태에 따라, 동일한 사설 IP 주소를 갖는 컴퓨터 인스턴스로부터 서비스에서 수신된 요청들 간을 구별하기 위한 IVN 및 PAE 식별자의 사용의 일례를 예시한다. 도시된 바와 같이, 각각의 IVN(702A, 702B)은 클라이언트(C1)에 의해 셋업될 수 있으며, IVN(702A)은 클라이언트의 조직의 엔지니어링 부서에 의한 사용을 위해 셋업되고, 그리고 IVN(702B)은 조직의 마케팅 부서에 의한 사용을 위해 셋업된다. 양 조직은 묘사된 예에서는 동일한 공중-액세스가능한 저장 서비스 "StorageSvc1"에 저장된 객체에 액세스할 필요가 있을 수 있다. PAE(750A)는 IVN(702A)으로부터 StorageSvc1에 액세스하도록 확립될 수 있고, 그리고 PAE(750B)는 IVN(702B)으로부터 StorageSvc1에 액세스하도록 확립될 수 있다.

[0057] 클라이언트(C1)는 IVN(702A)에서의 컴퓨터 인스턴스(710A)에 그리고 IVN(702B)에서의 컴퓨터 인스턴스(710K)에 동일한 사설 IP 주소 10.4.5.6를 (예컨대, 의도적으로 또는 우연히) 배정할 수 있다. StorageSvc1로 지향된 서비스 요청은 양 컴퓨터 인스턴스(710A, 710K)에서 발생될 수 있다. 위에서 설명된 바와 같이 제공자 네트워크의 터널링 중개자에서 구현될 수 있는 캡슐화 프로토콜에 따라, StorageSvc1의 객체(X)를 판독하라는 IVN(702A)으로부터의 요청을 표시하는 캡슐화 서비스 요청 패킷(774A)은 전단부 노드(771)에 송신될 수 있다. 캡슐화 패킷(774A)은 요청의 원래 소스로서 사설 IP 주소 10.4.5.6를 표시할 수 있고, 그리고 또한 요청을 라우팅하는데 사용된 PAE(750A) 및 IVN 식별자(702A)의 인코딩을 포함할 수 있다. 유사하게, 서비스의 객체(Y)를 판독하라는 요청을 표시하는 캡슐화 패킷(774B)은 전단부 노드(771)에서 수신될 수 있다. 패킷(774B)은 또한 묘사된 실시형태에서는 그 요청을 라우팅하는데 사용된 PAE(750B), 소스 IVN(702B), 및 그 소스 인스턴스의 사설 IP 주소(패킷(774A)에 표시된 것과 똑같은 10.4.5.6)를 표시할 수 있다.

[0058] 전단부 노드(771)(및/또는 요청된 작업이 수행되는 후단부 노드(773))는, 패킷(774A, 774B)에 표시된 소스 IP 주소가 똑같더라도, 요청의 소스를 구별하도록 수신된 패킷에 포함된 IVN 및/또는 PAE 식별 정보를 사용할 수 있을 수 있다. 그리하여, X를 판독하라는 요청이 수신 또는 프로세싱된 타임스탬프(T1), 요청하는 컴퓨터 인스턴스의 사설 IP 주소 10.4.5.6, PAE(750A) 및 IVN(702A)의 식별자를 표시하는 로그 레코드(733A)는 (FE 노드에 의해서든 BE 노드에 의해서든) 발생될 수 있다. 수신 또는 프로세싱의 타임스탬프(T2), 소스 IP 주소 10.4.5.6, PAE(750B) 및 IVN(702B)의 식별자를 표시하는 유사한 로그 레코드(733B)는 Y를 판독하라는 요청에 대해 발생될 수 있다. 일부 실시형태에서는, 어느 하나가 요청의 소스를 명확화하기에 충분할 수 있으므로, IVN의 식별자 또는 PAE의 식별자만이 로그 레코드에(또는 캡슐화 패킷에) 포함될 수 있다.

[0059] 위에서 설명된 바와 같이 터널링 중개자가 캡슐화 패킷(774)의 소스 헤더 내에 IVN 또는 PAE 식별자를 편입시키는 실시형태에서는, (전단부 노드(771) 및/또는 후단부 노드(773)와 같은) 서비스-측 노드가 반드시 소스 헤더의 콘텐츠를 파싱할 수 있지는 않을 수 있는 시나리오에서도 다른 IVN들로부터의 트래픽은 명확화될 수 있음을 주목한다. 예컨대, 제3자 서비스가 PAE-기반 라우팅을 사용하도록 등록되고, 그리고 IPv6가 캡슐화에 사용되고 있으면, 제3자 서비스의 노드는 IPv6 헤더의 어느 특정 비트가 소스 IVN 정보 또는 소스 PAE 정보를 인코딩하는데 사용되는지 알고 있지 않을 수 있다. 그렇지만, IVN(702A)으로부터의 패킷(P1)에 대한 IPv6 소스 헤더는 IVN(702B)으로부터의 패킷(P2)에 대한 IPv6 소스 헤더와는 다를 것이므로, 제3자 서비스 노드는, IVN 식별자 및/또는 PAE 식별자에 관한 상세가 제3자 서비스 노드에서 확인되지 않더라도, 적어도 P1과 P2가 다른 소스로부터임을 결정할 수 있을 것이다. 물론, 제3자 서비스 노드가 도 6에서 예시된 것들과 유사한 액세스 제어 정책을 구현하는 것을 책임지고 있고, 그리고 액세스 제어 정책이 특정 IVN 또는 특정 PAE와 연관되면, 제3자 서비스 노드는 IVN/PAE 식별자를 획득해야 할 수 있다.

[0060] 사설 별칭 중단점을 위한 방법

[0061] 도 8은, 적어도 일부 실시형태에 따라, PAE를 구성하도록 수행될 수 있는 연산의 태양을 예시하는 순서도이다. 요소(801)에서 제시된 바와 같이, 하나 이상의 고립된 가상 네트워크는, 예컨대, 가상 컴퓨팅 서비스의 자원을 사용하여, 제공자 네트워크에서 클라이언트(C1)를 대행하여 셋업될 수 있다. 각각의 IVN은 (서브넷 셋업, IP 주소 배정 등과 같은) 내부 네트워킹 구성 선택이 클라이언트에 의해 이루어질 수 있는 컴퓨터 인스턴스 등과 같은 소정 자원 세트를 포함할 수 있다. 예컨대, 클라이언트는 소정 사설 IP 주소가 IVN 바깥의 자원에 대해 고유함을 보장해야 할 필요 없이 사설 IP 주소(IVN 바깥에 광고되지 않은 주소)를 컴퓨터 인스턴스의 가상 네트워크 인터페이스에 배정할 수 있다. 클라이언트가 2개의 다른 IVN(IVN1, IVN2)에서 동일한 사설 IP 주소 "a.b.c.d"를 사용하기를 바라면, 그 주소는, 예컨대, IVN1에서의 컴퓨터 인스턴스(CI1) 및 IVN2에서의 다른 컴퓨터 인스턴스(CI1)에 배정될 수 있다. IP 주소에 대한 고유함은 적어도 일부 실시형태에서는 소정 IVN 내에서 여전히 요구될

수 있음을 주목한다 - 예컨대, 동일한 IP 주소는 동일한 IVN 내에서 론칭되는 2개의 인스턴스에는 배정가능하지 않을 수 있다.

[0062] 묘사된 실시형태에서, 가상 컴퓨팅 서비스는 클라이언트가 IVN과 연관된 사설 종단점 별칭(PAE)을 사용하여 사설 IP 주소를 갖는 IVN 컴퓨터 인스턴스로부터의 서비스 요청을 공중-액세스가능한 서비스(예컨대, 제공자 네트워크 오퍼레이터에 의해 구현된 저장 또는 데이터베이스 서비스, 및/또는 제공자 네트워크의 다른 고객에 의해 구현된 제3자 서비스)에 제출하는 것을 가능하게 할 수 있다. 요소(804)에서 제시된 바와 같이, C1을 대행하여 IVN1에 대해 확립된 특정 PAE(PAE1)를 표현하는 메타데이터 레코드는, 예컨대, 제공자 네트워크 또는 가상 컴퓨팅 서비스의 구성 관리자 컴포넌트에 의해 생성 및 저장될 수 있다. 적어도 일부 구현에서, PAE1이 (예컨대, C1로부터의 프로그램 요청에 응답하여) 생성될 때, PAE1은 어느 특정 서비스에도 연관 또는 구속될 필요가 없다. IVN1과 연관된 루트 테이블 내에서, PAE1은 결국에는, 요소(807)에서 표시된 바와 같이, 예컨대, 선택된 서비스가 PAE1에 배정되는 별개의 구성 단계 후에, IVN1 내에서 유래하고 제공자 네트워크에서의 다른 곳에서(즉, IVN1 바깥에서) 구현된 선택된 서비스로 향하여 지향된 네트워크 트래픽에 대한 루트 표적으로서 표시될 수 있다.

[0063] 적어도 일부 실시형태에서는, 예컨대, 제공자 네트워크 오퍼레이터가 IVN에서의 사설 IP 주소를 갖는 인스턴스와, 서비스 단부에서의 공중 IP 주소를 갖는 서비스 노드 간 패킷을 송신하는데 사용된 캡슐화 프로토콜을 구현하기 위해 필요로 될 수 있는 (터널링 중개자와 같은) 컴포넌트를 셋업 및 시험/검증한 후에, 여러 서비스가 PAE 지원에 등록되었을 수 있다. 서비스의 공중 IP 주소는 또한 일부 실시형태에서는 IVN의 인스턴스 호스트에서의 가상화 관리 컴포넌트 및/또는 터널링 중개자에게는 액세스가능한 구성 데이터베이스 내에서 검증(및 필요에 따라 업데이트)되어야 할 수 있다. 적어도 하나의 실시형태에서, 클라이언트(C1)에 이용가능한 프로그램 인터페이스는 서비스(Svc1)를 PAE1에 배정할 때 클라이언트가 그러한 등록된 세트 중으로부터 서비스를 선택하는 것을 가능하게 할 수 있다(요소(807)) - 즉, 클라이언트는 미리-승인된 서비스를 그들 IVN에 대해 셋업된 PAE에 연관시키도록 허용될 수 있을 뿐이다. 일 구현에서, PAE1과 같은 PAE와 Svc1과 같은 서비스 간 연관은 PAE의 "서비스" 속성의 값을 설정함으로써 IVN 구성 데이터베이스 내에서 표현될 수 있다.

[0064] 하나 이상의 액세스 정책은 일부 실시형태에서는 PAE1과 같은 소정 PAE와 연관될 수 있다(요소(810)). 액세스 정책은, 예컨대, PAE1을 사용하여 허용 또는 금지되는 서비스 요청 또는 연산의 유형, PAE1을 통하여 액세스가 승인되는 객체 유형, 정책 규칙이 적용되는 대표사용자(예컨대, 사용자 또는 그룹), 정책 규칙이 적용되는 시간 기간 등을 표시할 수 있다. 일부 실시형태에서, 클라이언트(C1)는, 예컨대, 프로그램 인터페이스를 사용하여, PAE1에 대한 그들 선택의 액세스 정책을 표시할 수 있다. 클라이언트가 하나를 표시하지 않으면 일부 구현에서는 디폴트 액세스 정책이 PAE에 적용될 수 있다. 정책은 또한 일부 구현에서는 PAE의 속성으로서 표현될 수 있다. 소정 PAE에 다수의 정책이 배정될 수 있는 일부 실시형태에서, 구성 관리자는 다른 정책들 간 상충을 검출하는 것을 책임지고 있을 수 있다. 예컨대, 하나의 정책은 특정 객체에 대해 특정 유형의 연산을 허용할 수 있는 한편, 다른 정책은 그 유형의 연산을 금지할 수 있다. 일부 구현에서, 구성 관리자는 상충하는 정책들 간 우선순위를 정하거나 상충을 제거하라고 클라이언트에 요청할 수 있다. 다른 실시형태에서, 구성 관리자는 단순히 특정된 정책을 소정 디폴트 우선순위 순서(예컨대, 디폴트로 더 최근-적용된 정책이 예전 정책보다 우선함)로 적용하고 그에 따라 상충은 해결될 수 있다.

[0065] 목적지가 Svc1인 트래픽에 대한 표적으로서 PAE1을 표시하는 루트 테이블 엔트리는 묘사된 실시형태에서는 IVN1의 하나 이상의 서브넷에 (예컨대, 프로그램 인터페이스를 사용하여 제출된 요청을 통하여 C1에 의해) 생성 및 배속될 수 있다(요소(813)). 루트 테이블 엔트리에 대한 소스 및 목적지로서 특정 IP 주소 범위를 특정하는 대신에, 서비스의 등록된 명칭이 목적지로서 표시될 수 있고, 그리고 PAE1이 생성되었을 때 PAE1에 배정된 명칭 또는 식별자는 표적으로서 표시될 수 있고, 그리하여 클라이언트(C1)의 관점에서 IVN1과 Svc1 간 루트 관리를 상당히 단순화한다. 루트 테이블 엔트리가 배속된 후에, Svc1과 서브넷의 인스턴스 간 트래픽 흐름이 시작될 수 있다.

[0066] 적어도 일부 실시형태에서, 하나 이상의 PAE(예컨대, PAE1)에 배정된 서비스(예컨대, Svc1)와 연관된 공중 IP 주소의 세트는 시간의 흐름에 따라 변할 수 있는 경우가 있을 수 있다. Svc1과 같은 등록된 서비스의 제어 평면 또는 관리 컴포넌트, 및/또는 가상 컴퓨팅 서비스의 구성 관리자는, 묘사된 실시형태에서는, 공중 IP 주소의 리스트 및/또는 다른 PAE-관련 구성 정보에 대한 업데이트를 그러한 주소가 사용될 수 있는 컴포넌트에 전파하는 것을 책임지고 있을 수 있다(요소(816)). 그러한 업데이트는, 예컨대, 위에서 설명된 종류의 캡슐화 프로토콜이 구현되어야 하는 터널링 중개자로부터 액세스가능한 구성 데이터베이스, 및/또는 IVN 인스턴스 호스트의 가상화

관리 컴포넌트로부터 액세스가능한 데이터베이스에 이루어질 수 있다.

[0067] 도 9는, 적어도 일부 실시형태에 따라, 컴퓨터 인스턴스로부터 공중-액세스가능한 서비스로 패킷을 송신하기 위한 터널링 프로토콜의 사용을 예시하는 순서도이다. 요소(901)에서 제시된 바와 같이, 액세스될 서비스(Svc1)에 대한 공중 IP 주소 "Addr1"는 Svc1로/로부터의 트래픽에 대해 PAE(PAE1)가 확립된 IVN(IVN1)에서 구현된 컴퓨터 인스턴스(CI1)에서 (예컨대, DNS 질의를 사용하여) 결정될 수 있다. 컴퓨터 인스턴스(CI1)에서, 바다가 서비스 요청(SR1)의 적어도 일부를 표시하는 기초 패킷(BP1)이 발생될 수 있다(요소(904)). CI1의 사설 IP 주소는 BP1의 소스 주소로서 표시될 수 있고, 그리고 Addr1은 목적지로서 표시될 수 있다. BP1은, 예컨대, CI1에 배속된 가상 네트워크 인터페이스를 사용하여 CI1으로부터 Addr1로 향하여 송신될 수 있다.

[0068] 묘사된 실시형태에서, 기초 패킷(BP1)은 CI1이 실행되는 인스턴스 호스트에서, 하이퍼바이저 또는 특권 도메인 운영 체제와 같은, 가상화 관리 컴포넌트(VMC)에 의해 가로채일 수 있다(요소(907)). VMC는, 예컨대, 인스턴스 호스트의 (물리적 네트워크 인터페이스 카드와 같은) 하드웨어 컴포넌트와 (가상 네트워크 인터페이스와 같은) 가상화된 자원 간 중개자로서 역할할 수 있다. VMC는, CI1로부터 Svc1로의 트래픽이 PAE1로 겨냥되어야 함을 표시하는 루트 테이블 엔트리와 같은, PAE 구성 정보의 하나 이상의 요소 및/또는 BP1의 목적지 주소를 분석할 수 있다. 적어도 하나의 실시형태에서, VMC는 또한 또는 대신에 Svc1의 공중 IP 주소의 리스트에서 Addr1을 록업할 수 있을 수 있다. 구성 정보의 조사에 기반하여, VMC는 BP1로부터 유도된 제1 캡슐화 패킷(EP1)이, 예컨대, 브리지 네트워크를 통하여 Addr1로 향한 추가적 송신을 위해, 터널링 중개자로 향하여 보내져야 한다고 결정할 수 있을 수 있다(요소(910)). 터널링 중개자는, 예컨대, 내부 브리지 네트워크를 통하여 (Svc1과 같은) 공중-액세스가능한 서비스의 노드와 (CI1과 같은) 가상 컴퓨팅 서비스의 노드 간 트래픽을 라우팅하도록 셋업된 멀티-노드 플리트의 하나의 노드일 수 있다. 제1 캡슐화 패킷(EP1)은 일부 실시형태에서는 가상 컴퓨팅 서비스의 다양한 컴포넌트 내에서의 라우팅에 사용되는 제1 캡슐화 프로토콜(P1)에 따라 포맷팅될 수 있다. EP1 내에서, (BP1의 소스 및 목적지 헤더를 포함하는) BP1은 바다 컴포넌트 내에 편입될 수 있고, 그리고 하나 이상의 P1 헤더가 일부 구현에서는 VMC에 의해 부가될 수 있다. EP1의 부가된 헤더는, 예컨대, 소스로서 VMC(또는 VMC가 실행되는 인스턴스 호스트)를 그리고 목적지로서 터널링 플리트(또는 특정 터널링 중개자)를 표시할 수 있다. 일 구현에서는, PAE1 및/또는 IVN1의 식별자가 또한 EP1 헤더에 포함될 수 있다. 일부 실시형태에서, EP1 헤더는 반드시 PAE1의 식별자를 표시하지는 않을 수 있지만, EP1이 PAE와 연관된 패킷임을 표시하는 필드를 포함할 수 있다.

[0069] EP1은 결국에는, 예컨대, 가상 컴퓨팅 서비스의 네트워크의 하나 이상의 홉을 순회한 후에, 묘사된 실시형태에서는 터널링 중개자에 도달할 수 있다. BP1은 추출될 수 있고 그리고 EP1 헤더의 콘텐츠는 조사될 수 있다. BP1의 소스 및 목적지 주소(즉, CI1의 사설 IP 주소 및 Svc1 주소(Addr1))는, 제2 캡슐화 패킷(EP2)에서 특정되어야 하는, 터널링 프로토콜(P2)의 매핑 데이터베이스에서 대응하는 소스 및 목적지 주소를 록업하는데 사용될 수 있다(요소(913)). 일부 실시형태에서, 기초 패킷(Bp1)(및/또는 EP1)은 IPv4에 따라 포맷팅될 수 있는 한편, 터널링 프로토콜에서 사용될 소스 및 목적지 주소는, 예컨대, SIIT 또는 유사한 IPv4-IPv6 변환 프로토콜을 사용하여, IPv6에 따라 포맷팅될 수 있다. 다른 실시형태에서, 터널링 프로토콜은 사유일 수 있다, 예컨대, IPv6-스타일 주소가 반드시 사용될 필요는 없다. 터널링 프로토콜에 IPv6가 사용되지 않는 일부 실시형태에서, 기초 패킷의 캡슐화는 TCP 옵션 헤더와 같은 부가적 IPv4 헤더를 사용하여 수행될 수 있다. 적어도 하나의 실시형태에서는, UDP(User Datagram Protocol) 캡슐화가 (예컨대, UDP 메시지 내에 기초 패킷을 편입시킴으로써) 사용될 수 있다. EP1 헤더는 묘사된 실시형태에서는 터널링 중개자에서 제거되고 EP2 헤더에 의해 교체될 수 있다. 도 4에서 예시된 바와 같이, 일부 실시형태에서 하나 이상의 EP2 헤더는 각각 (a) (예컨대, 32-비트 BP1 소스 IP 주소를 인코딩하는데 128-비트 EP2 소스 주소 헤더의 32 비트를 사용하여, 그리고 32-비트 Bp1 목적지 IP 주소를 인코딩하는데 128-비트 EP2 목적지 주소 필드의 32 비트를 사용하여) BP1 소스 및 목적지 주소를 그리고/또는 (b) 라우팅에 사용된 PAE(PAE1) 및 소스 IVN(IVN1)의 식별자를 표시 또는 인코딩할 수 있다. 일부 구현에서, IP2 헤더에 포함될 수 있는 PAE 식별자는 자체가 대응하는 IVN의 식별자의 인코딩을 포함할 수 있고, 그래서 PAE 식별자는 수신된 요청이 오는 PAE 및 IVN 양자를 결정하도록 서비스에서 사용가능할 수 있다. 적어도 하나의 구현에서, BP1 목적지 주소는 BP1 목적지 주소가 사용되는지, 아니면 EP2 목적지 주소가 사용되는지에 무관하게 부하 밸런서가 소정 패킷을 동일한 서비스 전단부 노드로 라우팅하는 그러한 방식으로 각각 EP2 소스 및 목적지 헤더 내에 (예컨대, 가장 낮은 32 비트에) 포함될 수 있다.

[0070] EP2는, 예컨대, 제공자 네트워크 내에 확립된 브리지 네트워크의 선택된 경로를 통하여, 터널링 중개자로부터 Svc1의 전단부 노드로 송신될 수 있다(요소(916)). 일부 실시형태에서, EP2는 제공자 네트워크 오퍼레이터에 의해 관리 및/또는 소유된 사설 네트워크 링크만을 사용하여 Svc1에 도달할 수 있다. 다른 실시형태에서, EP2에 사용된 경로는 공중 네트워크 링크를 포함할 수 있다(예컨대, 패킷은 제공자 네트워크 바깥에 있거나, 또는 제

공자 네트워크 오퍼레이터 이외의 개체에 의해 관리/소유된 네트워크 디바이스를 통과할 수 있다). Svc1의 전단부 노드에서, 서비스 요청(SR1)을 표시하는 BP1 콘텐츠가 추출될 수 있다(요소(919)). 부가적으로, 예컨대, 다른 IVN의 다른 인스턴스에 지정되는 것과 동일한 IP 주소가 CI1에 지정되더라도, EP2 헤더를 사용하여 서비스에 서 소스 인스턴스(CI1)의 고유 식별이 가능할 수 있다. 예컨대, EP2 헤더 또는 헤더들로부터 추출될 수 있는, BP1의 콘텐츠를 라우팅하는데 사용된 PAE 및/또는 소스 IVN의 식별자는 각각의 IVN이 특정 사설 IP 주소를 갖는 단일 인스턴스만을 포함할 수 있는 실시형태에서 그러한 인스턴스들로부터의 서비스 요청들을 명확화하도록 사용될 수 있다. 적어도 일부 실시형태에서, 서비스 요청(SR1)은 PAE와 연관된 하나 이상의 액세스 제어 정책에 따라 서비스측에서 검정될 수 있다. 액세스 허용이 체크된 후에, 요청된 연산은, 예컨대, 서비스(Svc1)의 후단부 노드에서 수행될 수 있다. 적어도 일부 실시형태에서, 적어도 일부 유형의 요청에 대해 응답이 발생될 수 있고, 그리고 응답은 역순으로 동일한 프로토콜을 사용하여 CI1로 향하여 역방향으로 송신될 수 있다. 예컨대, 후단부 서비스 노드에서 콘텐츠가 발생하는 기초 응답은 서비스의 전단부 노드에서 터널링 프로토콜(P2)에 따라 포맷팅되고 브리지 네트워크를 가로질러 가상 컴퓨팅 서비스의 터널링 중개자에 송신될 수 있다. 터널링 중개자에서, 응답은 추출되고, 제1 캡슐화 프로토콜(P1)에 따라 포맷팅되고, 그리고 CI1이 실행되는 인스턴스 호스트에서의 VMC로 전달될 수 있다. VMC는 기초 응답을 추출하고 그것을 CI1에 제공할 수 있다.

[0071] 다양한 실시형태에서는, 사설 별칭 종단점을 지원하기 위한 기술 중 적어도 일부를 구현하도록 도 8 및 도 9의 순서도에서 예시된 것들 이외의 연산이 사용될 수 있음을 주목한다. 제시된 연산 중 일부는 일부 실시형태에서는 구현되지 않을 수 있거나, 도 8 또는 도 9에서 예시된 것과는 다른 컴포넌트에서 또는 다른 순서로 구현될 수 있거나, 또는 순차적으로라기보다는 병렬로 구현될 수 있다. 적어도 하나의 실시형태에서, 터널링 중개자 및 VMC에 대해 설명된 기능성은 예컨대 조합될 수 있다 - 예컨대, 별개의 중개자에 의한 추가적 캡슐화 없이 선택된 경로를 통하여 서비스로 패킷이 송신될 수 있게 하는 터널링 프로토콜은 VMC에서 구현될 수 있다. 다른 실시형태에서, 기초 패킷은 VMC에 의해 캡슐화되지 않고 비-가상화된 컴퓨팅 디바이스로부터 또는 컴퓨터 인스턴스로부터 터널링 중개자로 송신될 수 있다.

[0072] 사용례

[0073] 고립된 가상 네트워크의 컴퓨터 인스턴스로부터 공중-액세스가능한 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 역할할 사설 별칭 종단점을 확립하는 위에서 설명된 기술은 다양한 시나리오에서 유용할 수 있다. 점점 더 많은 분산형 애플리케이션이 제공자 네트워크 환경으로 이주되고, 그리고 네트워크-기반 공격자의 정교함이 증가함에 따라, 공중 인터넷에서 유래하는 네트워크 침입으로부터 클라이언트 애플리케이션의 보안 및 고립에 대한 필요성도 증가하고 있다. 고립된 가상 네트워크는 클라이언트가 공중 인터넷에 광고되지 않거나 그로부터 액세스가능하지 않은 컴퓨터 인스턴스에 사설 IP 주소를 지정하는 것을 가능하게 하기는 하지만, 그러한 인스턴스로부터 요청이 공중 IP 주소에서 유래할 것으로 예상하는 서비스에 액세스하는 것은 문제가 있을 수 있다. 사설 별칭 종단점은 잠재적 보안 절충을 필요로 하지 않고 그리고 VPN 접속을 통한 요청의 비효율적/비싼 라우팅 없이 그러한 서비스 요청이 송신되는 것을 가능하게 할 수 있다.

[0074] 본 발명의 실시형태는 이하의 조항을 고려하여 설명될 수 있다:

[0075] 1. 시스템으로서,

[0076] 제공자 네트워크의 구성 관리자;

[0077] 인스턴스 호스트의 가상화 관리 컴포넌트(VMC)로서, 클라이언트를 대행하여 확립된 제1 고립된 가상 네트워크(IVN)의 제1 컴퓨터 인스턴스는 인스턴스 호스트에서 인스턴스화되고, 그리고 제1 컴퓨터 인스턴스는 클라이언트에 의해 선택된 사설 네트워크 주소를 갖는 가상화 관리 컴포넌트; 및

[0078] 터널링 중개자를 포함하되,

[0079] 구성 관리자는 제1 IVN에서 유래하고 특정 서비스로 지향되는 패킷에 대한 라우팅 표적으로서 제1 사설 별칭 종단점(PAE)의 지정을 표현하는 제1 메타데이터 엔트리를 저장하도록 구성되되, 패킷은 소스 주소로서 공중-광고된 네트워크 주소를 표시하지 않고 특정 서비스에 전달되어야 하고;

[0080] VMC는 VMC에서 가로채인 기초 패킷으로부터 유도된 제1 캡슐화 패킷을, 제1 메타데이터 엔트리의 조사에 적어도 부분적으로 기반하여, 터널링 중개자에 송신하도록 구성되되, 기초 패킷은 제1 컴퓨터 인스턴스에서 발생되고 특정 서비스의 공중-광고된 네트워크 주소로 지향되고; 그리고

[0081] 터널링 중개자는

- [0082] 제1 캡슐화 패킷으로부터 제2 캡슐화 패킷을, 터널링 프로토콜에 따라, 발생시키되, 제2 캡슐화 패킷은 소스 IVN으로서 제1 IVN을 표시하는 헤더 컴포넌트를 포함하고; 그리고
- [0083] 제2 캡슐화 패킷을 특정 서비스의 하나 이상의 노드 중 제1 노드에 송신하도록 구성되되, 제1 노드는 (a) 제1 IVN의 식별자 및 사실 네트워크 주소를, 제2 캡슐화 패킷으로부터, 결정하고, 그리고 (b) 기초 패킷에 표시된 서비스 요청을 이행하기 위한 하나 이상의 연산을 개시하도록 구성되는, 시스템.
- [0084] 2. 제1 조항에 있어서, 제2 캡슐화 패킷은 IPv6(인터넷 프로토콜 버전 6)에 따라 포맷팅되고, 그리고 기초 패킷은 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅되는, 시스템.
- [0085] 3. 제1 조항에 있어서, 특정 서비스는 복수의 객체에 대한 복수의 연산 유형을 지원하되, (a) 특정 서비스의 제1 노드 또는 (b) VMC 중 하나 이상은
- [0086] 서비스 요청이 제1 PAE에 배정된 제1 액세스 제어 정책을 준수하고 있는지에 관한 결정을, 하나 이상의 연산의 개시 이전에, 개시하도록 구성되되, 제1 액세스 제어 정책은, 라우팅 표적으로서 제1 PAE를 사용하여 제출된 요청에 대해, (a) 복수의 연산 유형 중 허용된 연산 유형, (b) 복수의 연산 유형 중 금지된 연산 유형, (c) 복수의 연산 유형 중 특정 연산 유형이 허용되는 시간 구간, 또는 (d) 복수의 연산 유형 중 특정 연산 유형이 허용되는 복수의 객체 중 특정 객체 중 하나 이상을 표시하는, 시스템.
- [0087] 4. 제1 조항에 있어서, 구성 관리자는
- [0088] 제1 IVN에서 유래하는 부가적 패킷에 대한 라우팅 표적으로서 제2 PAE를 지정하도록 더 구성되되, 부가적 패킷은 다른 서비스에 전달되어야 하는, 시스템.
- [0089] 5. 제1 조항에 있어서, 구성 관리자는
- [0090] 클라이언트의 요청시, 클라이언트의 제2 IVN에서 확립된 제2 컴퓨트 인스턴스에 사실 네트워크 주소를 배정하고;
- [0091] 제2 IVN에서 유래하고 특정 서비스로 지향되는 트래픽을 라우팅하는데 사용될 제2 PAE를 확립하도록 더 구성되고,
- [0092] 그리고 서비스의 제1 노드는
- [0093] 제1 노드에서 추출된 특정 기초 패킷이 제1 컴퓨트 인스턴스에서 발생되었는지, 아니면 제2 컴퓨트 인스턴스에서 발생되었는지, 터널링 중개자에 의해 발생된 특정 캡슐화 헤더의 조사에 기반하여, 결정하도록 구성되는, 시스템.
- [0094] 6. 방법으로서,
- [0095] 클라이언트를 대행하여 확립된 제1 고립된 가상 네트워크(IVN)에서 유래하는 트래픽에 대한 라우팅 표적으로서 제1 사실 별칭 중단점(PAE)이 지정되었음을, 제공자 네트워크의 터널링 중개자에서, 결정하는 단계로서, 트래픽은 특정 공중-액세스가능한 서비스에 전달되어야 하는 결정하는 단계;
- [0096] 제1 IVN의 제1 컴퓨트 인스턴스로부터 특정 공중-액세스가능한 서비스의 공중-광고된 네트워크 주소로 지향된 기초 패킷을, 터널링 중개자에서, 수신하는 단계; 및
- [0097] (a) 기초 패킷의 콘텐츠 및 (b) 소스 IVN으로서 제1 IVN의 표시를 포함하는 캡슐화 패킷을, 터널링 중개자에 의해 특정 서비스의 제1 노드에, 송신하는 단계를 포함하는, 방법.
- [0098] 7. 제6 조항에 있어서, 캡슐화 패킷은 IPv6(인터넷 프로토콜 버전 6)에 따라 포맷팅되고, 그리고 기초 패킷은 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅되는, 방법.
- [0099] 8. 제6 조항에 있어서, 특정 서비스는 복수의 객체에 대한 복수의 연산 유형을 지원하고,
- [0100] 제1 PAE에 제1 액세스 제어 정책을 적용하라는 요청을, 클라이언트로부터 제1 IVN의 구성 관리자에서, 수신하는 단계로서, 제1 액세스 제어 정책은, 라우팅 표적으로서 제1 PAE를 사용하여 제출된 요청에 대해, (a) 복수의 연산 유형 중 허용된 연산 유형, (b) 복수의 연산 유형 중 금지된 연산 유형, (c) 복수의 연산 유형 중 특정 연산 유형이 허용되는 시간 구간, 또는 (d) 복수의 연산 유형 중 특정 연산 유형이 허용되는 복수의 객체 중 특정 객체 중 하나 이상을 표시하는 수신하는 단계; 및
- [0101] 제1 액세스 제어 정책에 의해 제1 연산이 허용됨을, 기초 패킷에 표시된 특정 요청에 따라 제1 연산을 실행하기

이전에, 검증하는 단계를 더 포함하는, 방법.

- [0102] 9. 제6 조항에 있어서,
- [0103] 제1 IVN에서 유래하는 부가적 트래픽에 대한 라우팅 표적으로서 제2 PAE를 지정하는 단계를 더 포함하되, 부가적 트래픽은 다른 서비스에 전달되어야 하는, 방법.
- [0104] 10. 제6 조항에 있어서, 제1 컴퓨터 인스턴스는 클라이언트의 요청시 그것에 배정된 특정 사설 IP 주소를 갖고,
- [0105] 제2 IVN으로서 제2 컴퓨터 인스턴스를 포함하는 제2 IVN을 클라이언트를 대행하여 확립하는 단계;
- [0106] 제2 컴퓨터 인스턴스에 특정 사설 IP 주소를, 클라이언트의 요청시, 배정하는 단계;
- [0107] 제2 IVN에서 유래하고 특정 서비스로 지향되는 트래픽을 라우팅하는데 사용될 제2 PAE를 확립하는 단계;
- [0108] 특정 노드에서 수신된 특정 기초 패킷이 특정 사설 IP 주소가 배정된 제1 컴퓨터 인스턴스에서 발생되었는지, 아니면 특정 사설 IP 주소가 배정된 제2 컴퓨터 인스턴스에서 발생되었는지, 터널링 중개자에 의해 발생한 캡슐화 헤더의 조사에 기반하여 특정 서비스의 특정 노드에서, 결정하는 단계를 더 포함하는, 방법.
- [0109] 11. 제6 조항에 있어서, 캡슐화 패킷은 제공자 네트워크에서 구현된 사유 터널링 프로토콜에 따라 포맷팅되는, 방법.
- [0110] 12. 제6 조항에 있어서, 캡슐화 패킷은 제1 PAE의 식별자의 표현을 포함하는 헤더를 포함하는, 방법.
- [0111] 13. 제6 조항에 있어서,
- [0112] 제1 PAE를 발생시키라는 클라이언트로부터의 요청을, 프로그램 인터페이스를 통하여 제공자 네트워크의 구성 관리자에서, 수신하는 단계; 및
- [0113] 제1 PAE를 표현하는 메타데이터 엔트리를, 요청에 응답하여 구성 관리자에 의해, 저장하는 단계를 더 포함하는, 방법.
- [0114] 14. 제6 조항에 있어서,
- [0115] PAE를 사용하는 액세스에 다른 서비스를 등록하라는 요청을, 프로그램 인터페이스를 통하여 제공자 네트워크의 구성 관리자에서, 수신하는 단계; 및
- [0116] 특정 PAE와의 연관을 위해 클라이언트에 의해 특정 서비스가 선택될 수 있는 서비스의 집합에 다른 서비스를, 요청에 응답하여 구성 관리자에 의해, 추가하는 단계를 더 포함하는, 방법.
- [0117] 15. 제14 조항에 있어서, 다른 서비스는 제공자 네트워크의 자원의 세트를 사용하여 제공자 네트워크의 다른 클라이언트에 의해 구현되고,
- [0118] 다른 서비스로 지향된 기초 패킷으로부터 유도된 캡슐화 패킷의 콘텐츠를 추출하도록 구성된 특정 진단부 노드를 포함하는, 다른 서비스에 대한 하나 이상의 진단부 노드를 확립하는 단계를 더 포함하는, 방법.
- [0119] 16. 하나 이상의 프로세서 상에서 실행될 때 제공자 네트워크의 터널링 중개자를 구현하는 프로그램 명령어를 저장하는 비-일시적 컴퓨터-액세스가능한 저장 매체로서, 터널링 중개자는
- [0120] 제1 IVN의 제1 컴퓨터 인스턴스에서 발생한 기초 패킷을, 클라이언트를 대행하여 제공자 네트워크에서 확립된 제1 고립된 가상 네트워크(IVN)로부터 특정 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 제1 사설 별칭 종단점(PAE)의 지정에 따라, 수신하되, 기초 패킷은 그 목적지 주소로서 특정 서비스의 공중 IP(인터넷 프로토콜) 주소를 표시하고;
- [0121] (a) 기초 패킷의 콘텐츠 중 적어도 일부 및 (b) 소스 IVN으로서 제1 IVN을 표시하는 헤더 컴포넌트를 포함하는 캡슐화 패킷을, 선택된 터널링 프로토콜에 따라, 발생시키고; 그리고
- [0122] 캡슐화 패킷을 특정 서비스의 제1 노드에 송신하도록 구성되는 비-일시적 컴퓨터-액세스가능한 저장 매체.
- [0123] 17. 제16 조항에 있어서, 캡슐화 패킷은 IPv6(인터넷 프로토콜 버전 6)에 따라 포맷팅되고, 그리고 기초 패킷은 IPv4(인터넷 프로토콜 버전 4)에 따라 포맷팅되는 비-일시적 컴퓨터-액세스가능한 저장 매체.
- [0124] 18. 제16 조항에 있어서, 터널링 중개자는
- [0125] 제1 IVN의 제2 컴퓨터 인스턴스에서 발생한 제2 기초 패킷의 표현을, 제1 IVN으로부터 다른 서비스로 지향된 트

래픽에 대한 라우팅 표적으로서 제2 PAE의 지정에 따라, 수신하되, 제2 기초 패킷은 그 목적지 주소로서 다른 서비스의 공중 IP 주소를 표시하고;

- [0126] (a) 제2 기초 패킷의 콘텐츠 중 적어도 일부 및 (b) 소스 IVN으로서 제1 IVN을 표시하는 헤더 컴포넌트를 포함하는 제2 캡슐화 패킷을, 선택된 터널링 프로토콜에 따라, 발생시키고; 그리고
- [0127] 제2 캡슐화 패킷을 다른 서비스의 다른 노드에 송신하도록 더 구성되는 비-일시적 컴퓨터-액세스가능한 저장 매체.
- [0128] 19. 제16 조항에 있어서, 제1 캡슐화 패킷은 제1 컴퓨터 인스턴스의 사설 IP 주소의 표시를 포함하되, 터널링 중개자는
- [0129] 제2 IVN의 제2 컴퓨터 인스턴스에서 발생된 제2 기초 패킷의 표현을, 클라이언트를 대행하여 확립된 제2 IVN으로부터 특정 서비스로 지향된 트래픽에 대한 라우팅 표적으로서 제2 PAE의 지정에 따라, 수신하되, 제2 기초 패킷은 그 목적지 주소로서 특정 서비스의 공중 IP 주소를 표시하고;
- [0130] (a) 제2 기초 패킷의 콘텐츠 중 적어도 일부 (b) 소스 IVN으로서 제2 IVN을 표시하는 헤더 컴포넌트 및 (c) 사설 IP 주소의 표시를 포함하는 제2 캡슐화 패킷을, 선택된 터널링 프로토콜에 따라, 발생시키고; 그리고
- [0131] 제2 캡슐화 패킷을 특정 서비스의 제1 노드에 송신하도록 더 구성되되, 특정 서비스의 제1 노드는, 제2 기초 패킷이 제1 컴퓨터 인스턴스에서 발생되었는지, 아니면 제2 컴퓨터 인스턴스에서 발생되었는지, 제2 캡슐화 패킷의 조사에 기반하여, 결정하도록 구성되는 비-일시적 컴퓨터-액세스가능한 저장 매체.
- [0132] 20. 제16 조항에 있어서, 캡슐화 패킷은 제1 PAE의 식별자의 표현을 포함하는 헤더를 포함하는 비-일시적 컴퓨터-액세스가능한 저장 매체.
- [0133] 예시적 컴퓨터 시스템
- [0134] 적어도 일부 실시형태에서, 구성 관리자, VMC, 터널링 중개자, 및 공중-액세스가능한 서비스의 노드와 같은, 사설 별칭 종단점을 지원하는 데 사용되는 컴포넌트 중 하나 이상을 구현하는 서버는 하나 이상의 컴퓨터-액세스가능한 매체를 포함하거나 그에 액세스하도록 구성되는 범용 컴퓨터 시스템을 포함할 수 있다. 도 10은 그러한 범용 컴퓨팅 디바이스(9000)를 예시한다. 예시된 실시형태에서, 컴퓨팅 디바이스(9000)는 입/출력(I/O) 인터페이스(9030)를 통하여 (비-휘발성 및 휘발성 메모리 모듈 양자를 포함할 수 있는) 시스템 메모리(9020)에 결합된 하나 이상의 프로세서(9010)를 포함한다. 컴퓨팅 디바이스(9000)는 I/O 인터페이스(9030)에 결합된 네트워크 인터페이스(9040)를 더 포함한다.
- [0135] 다양한 실시형태에서, 컴퓨팅 디바이스(9000)는 하나의 프로세서(9010)를 포함하는 유니프로세서 시스템, 또는 수 개의 프로세서(9010)(예컨대, 2개, 4개, 8개 또는 다른 적합한 수)를 포함하는 멀티프로세서 시스템일 수 있다. 프로세서(9010)는 명령어를 실행할 수 있는 어느 적합한 프로세서라도 될 수 있다. 예컨대, 다양한 실시형태에서, 프로세서(9010)는, x86, PowerPC, SPARC, 또는 MIPS ISA, 또는 어느 다른 적합한 ISA와 같은 각종 명령어 세트 아키텍처(ISA) 중 어느 것이라도 구현하는 범용 또는 내장 프로세서일 수 있다. 멀티프로세서 시스템에서, 프로세서(9010)의 각각은, 반드시 아니지만, 공통으로 동일한 ISA를 구현할 수 있다. 일부 구현에서는, 관용적 프로세서에 부가하여 또는 그 대신에 그래픽 프로세싱 유닛(GPU)이 사용될 수 있다.
- [0136] 시스템 메모리(9020)는 프로세서(들)(9010)가 액세스가능한 데이터 및 명령어를 저장하도록 구성될 수 있다. 적어도 일부 실시형태에서, 시스템 메모리(9020)는 휘발성 부분도 그리고 비-휘발성 부분도 포함할 수 있다; 다른 실시형태에서는, 휘발성 메모리만이 사용될 수 있다. 다양한 실시형태에서, 시스템 메모리(9020)의 휘발성 부분은, 정적 램(SRAM), 동기식 동적 RAM 또는 어느 다른 유형의 메모리와 같은, 어느 적합한 메모리 기술이라도 사용하여 구현될 수 있다. (예컨대, 하나 이상의 NVDIMM를 포함할 수 있는) 시스템 메모리의 비-휘발성 부분에 대해, 일부 실시형태에서는 NAND-플래시 디바이스를 포함하는 플래시-기반 메모리 디바이스가 사용될 수 있다. 적어도 일부 실시형태에서, 시스템 메모리의 비-휘발성 부분은, 슈퍼커패시터 또는 다른 전력 축적 디바이스(예컨대, 배터리)와 같은, 전원을 포함할 수 있다. 다양한 실시형태에서, 메모리스터 기반 저항성 램(ReRAM), 3-차원 NAND 기술, 강유전성 RAM, 자기저항성 RAM(MRAM), 또는 다양한 유형의 상 변화 메모리(PCM) 중 어느 것이라도 적어도 시스템 메모리의 비-휘발성 부분에 사용될 수 있다. 예시된 실시형태에서, 위에서 설명된 그들 방법, 기술 및 데이터와 같은, 하나 이상의 소망 기능을 구현하는 프로그램 명령어 및 데이터는 코드(9025) 및 데이터(9026)로서 시스템 메모리(9020) 내에 저장되는 것으로 도시되어 있다.
- [0137] 일 실시형태에서, I/O 인터페이스(9030)는 프로세서(9010)와, 시스템 메모리(9020)와, 네트워크 인터페이스

(9040) 또는 다양한 유형의 영속적 그리고/또는 휘발성 저장 디바이스와 같은 다른 주변 인터페이스를 포함하는, 디바이스 내 어느 주변 디바이스 간 I/O 트래픽을 조정하도록 구성될 수 있다. 일부 실시형태에서, I/O 인터페이스(9030)는 어느 필요한 프로토콜, 타이밍, 또는 다른 데이터 변환이라도 수행하여 하나의 컴포넌트(예컨대, 시스템 메모리(9020))로부터의 데이터 신호를 다른 컴포넌트(예컨대, 프로세서(9010))에 의한 사용에 적합한 포맷으로 변환할 수 있다. 일부 실시형태에서, I/O 인터페이스(9030)는, 예컨대, 주변 컴포넌트 상호접속(PCI) 버스 표준 또는 범용 직렬 버스(USB) 표준의 변종과 같이 다양한 유형의 주변 버스를 통해 배속된 디바이스에 대한 지원을 포함할 수 있다. 일부 실시형태에서, I/O 인터페이스(9030)의 기능은, 예컨대, 노스 브리지 및 사우스 브리지와 같은 2개 이상의 별개 컴포넌트로 나뉠 수 있다. 또한, 일부 실시형태에서, 시스템 메모리(9020)로의 인터페이스와 같은, I/O 인터페이스(9030)의 기능성 중 일부 또는 전부는 프로세서(9010)에 직접 편입될 수 있다.

[0138] 네트워크 인터페이스(9040)는 컴퓨팅 디바이스(9000)와, 예컨대, 도 1 내지 도 9에 예시된 바와 같은 다른 컴퓨터 시스템 또는 디바이스와 같이 네트워크 또는 네트워크들(9050)에 배속된 다른 디바이스(9060) 간 데이터가 교환될 수 있게 하도록 구성될 수 있다. 다양한 실시형태에서, 네트워크 인터페이스(9040)는, 예컨대, 이더넷 네트워크 유형과 같은 어느 적합한 유선 또는 무선 일반 데이터 네트워크라도 통하여 통신을 지원할 수 있다. 부가적으로, 네트워크 인터페이스(9040)는 아날로그 음성 네트워크 또는 디지털 광섬유 통신 네트워크와 같은 원격통신/전화 네트워크를 통하여, 광섬유 채널 SAN과 같은 저장소 영역 네트워크를 통하여, 또는 어느 다른 적합한 유형의 네트워크 및/또는 프로토콜이라도 통하여 통신을 지원할 수 있다.

[0139] 일부 실시형태에서, 시스템 메모리(9020)는 대응하는 방법 및 장치의 실시형태를 구현하도록 도 1 내지 도 9에 대해 위에서 설명된 바와 같은 프로그램 명령어 및 데이터를 저장하도록 구성된 컴퓨터-액세스가능한 매체의 일 실시형태일 수 있다. 그렇지만, 다른 실시형태에서, 프로그램 명령어 및/또는 데이터는 여러 다른 유형의 컴퓨터-액세스가능한 매체 상에서 수신, 송신 또는 저장될 수 있다. 일반적으로 말하면, 컴퓨터-액세스가능한 매체는 자기 또는 광학 매체, 예컨대, I/O 인터페이스(9030)를 통하여 컴퓨팅 디바이스(9000)에 결합된 디스크 또는 DVD/CD와 같은 메모리 매체 또는 비-일시적 저장 매체를 포함할 수 있다. 비-일시적 컴퓨터-액세스가능한 저장 매체는 또한 시스템 메모리(9020) 또는 다른 유형의 메모리로서 컴퓨팅 디바이스(9000)의 일부 실시형태에 포함될 수 있는 RAM(예컨대, SDRAM, DDR SDRAM, RDRAM, SRAM 등), ROM 등과 같은 어느 휘발성 또는 비-휘발성 매체라도 포함할 수 있다. 더욱, 컴퓨터-액세스가능한 매체는 네트워크 인터페이스(9040)를 통하여 구현될 수 있는 바와 같은 네트워크 및/또는 무선 링크와 같은 통신 매체를 통하여 전해지는 전기, 전자기 또는 디지털 신호와 같은 신호 또는 전송 매체를 포함할 수 있다. 도 10에 예시된 것과 같은 다수의 컴퓨팅 디바이스 중 일부 또는 전부는 다양한 실시형태에서 설명된 기능성을 구현하도록 사용될 수 있다; 예컨대, 다양한 다른 디바이스 및 서버 상에서 실행되는 소프트웨어 컴포넌트는 기능성을 제공하도록 협업할 수 있다. 일부 실시형태에서, 설명된 기능성 중 일부는, 범용 컴퓨터 시스템을 사용하여 구현되는 대신에 또는 그에 부가하여, 특수용 컴퓨터 시스템, 네트워크 디바이스, 또는 저장 디바이스를 사용하여 구현될 수 있다. 용어 "컴퓨팅 디바이스"는, 여기에서 사용될 때, 적어도 모든 이들 유형의 디바이스를 지칭하고, 이들 유형의 디바이스로 한정되지는 않는다.

[0140] 결론

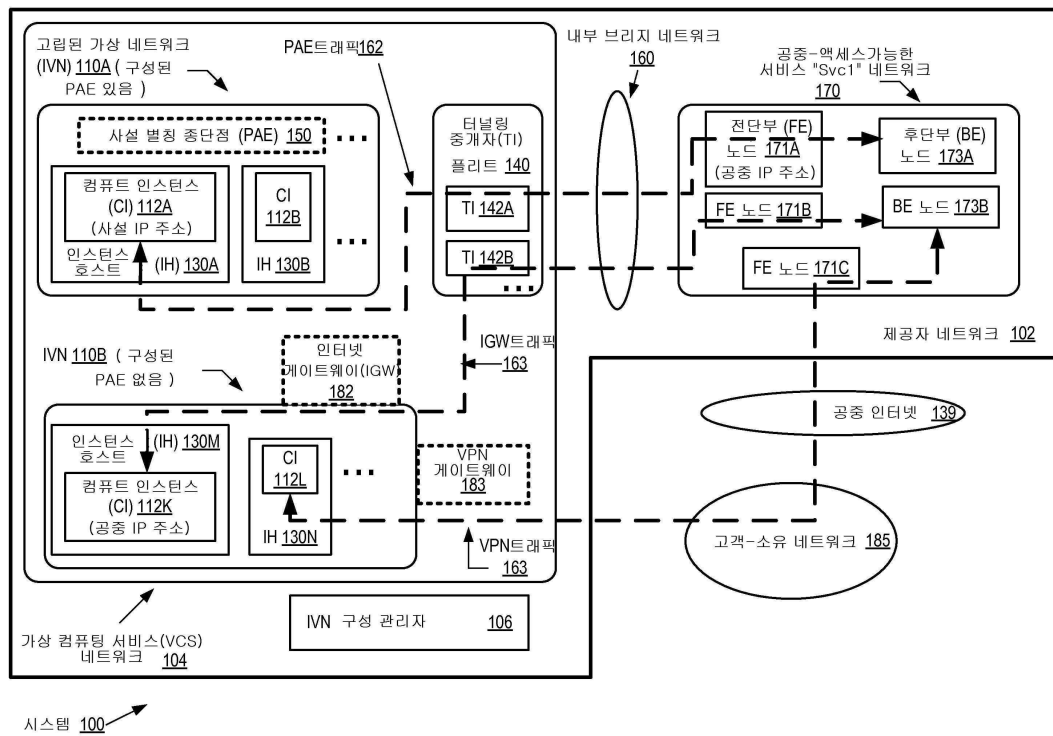
[0141] 다양한 실시형태는 컴퓨터-액세스가능한 매체 상에서 상기 설명에 따라 구현된 명령어 및/또는 데이터를 수신, 송신 또는 저장하는 것을 더 포함할 수 있다. 일반적으로 말하면, 컴퓨터-액세스가능한 매체는 자기 또는 광학 매체, 예컨대, 디스크 또는 DVD/CD-ROM, RAM(예컨대, SDRAM, DDR, RDRAM, SRAM 등), ROM과 같은 휘발성 또는 비-휘발성 매체 등과 같은 메모리 매체 또는 저장 매체는 물론, 네트워크 및/또는 무선 링크와 같은 통신 매체를 통하여 전해지는 전기, 전자기 또는 디지털 신호와 같은 신호 또는 전송 매체도 포함할 수 있다.

[0142] 여기에서 설명되고 도면에서 예시된 바와 같은 다양한 방법은 방법의 대표적 실시형태를 표현한다. 방법은 소프트웨어, 하드웨어, 또는 그 조합으로 구현될 수 있다. 방법의 순서는 변경될 수 있고, 다양한 요소가 부가, 순서변경, 조합, 생략, 수정 등이 될 수 있다.

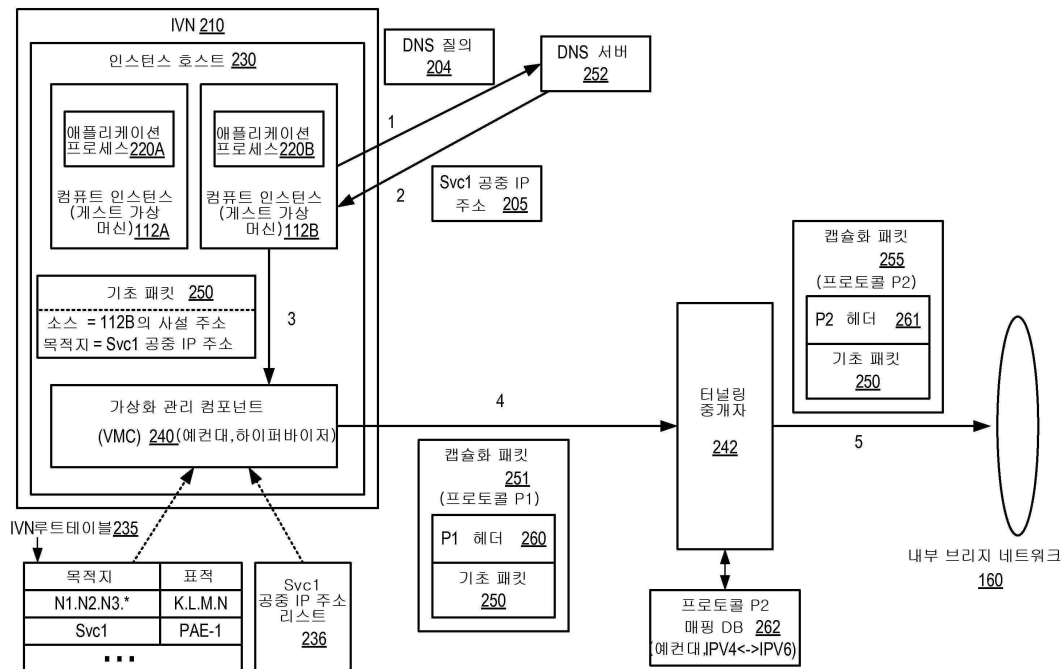
[0143] 본 개시가 유익한 당업자에게 자명할 바와 같이 다양한 수정 및 변경이 이루어질 수 있다. 모든 그러한 수정 및 변경을 포괄하려는 의도이고, 그에 따라, 위 설명은 제한적 의미라기보다는 예시적으로 간주되려는 의도이다.

도면

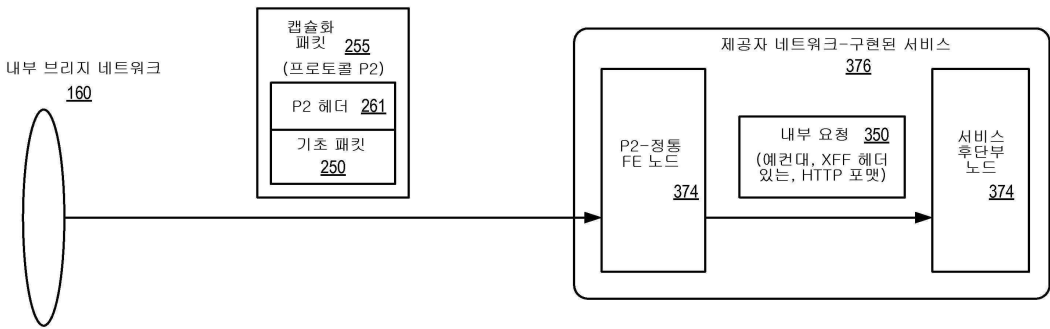
도면1



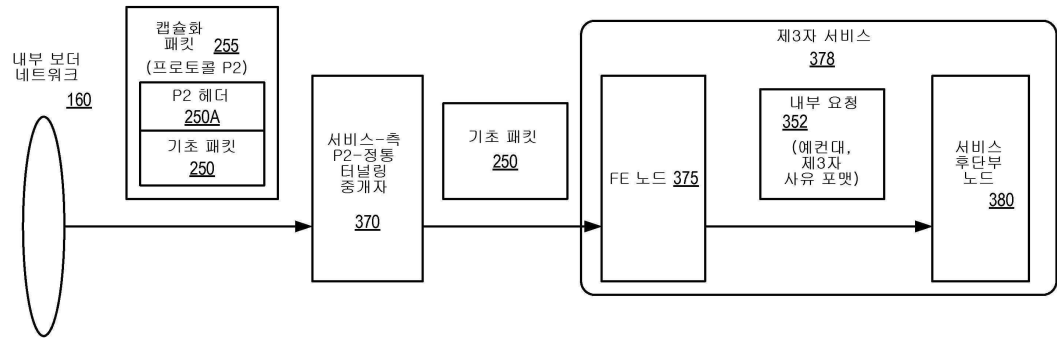
도면2



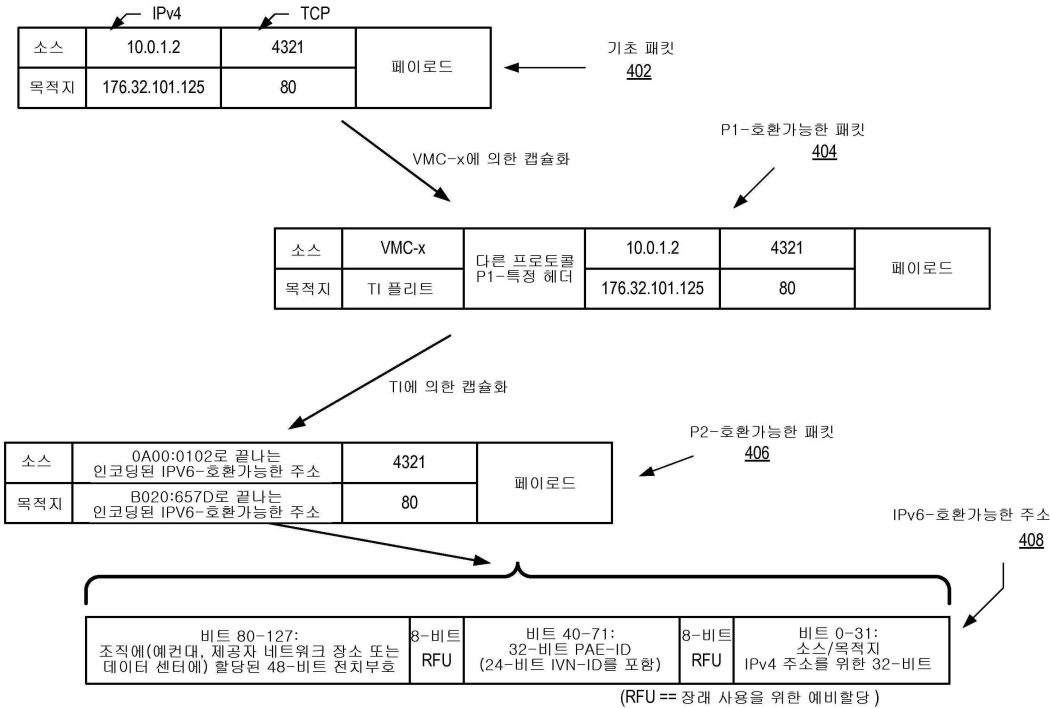
도면3a



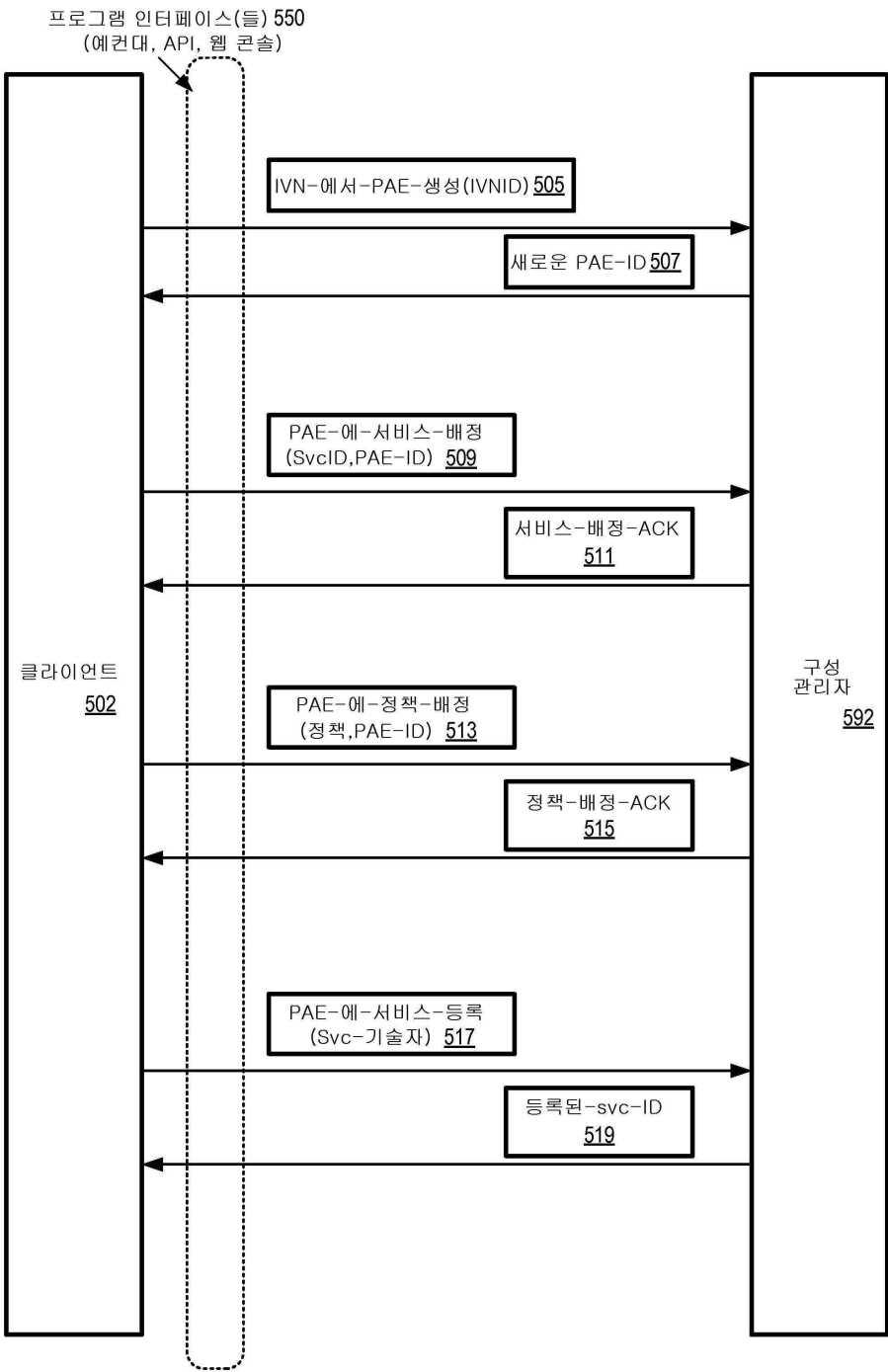
도면3b



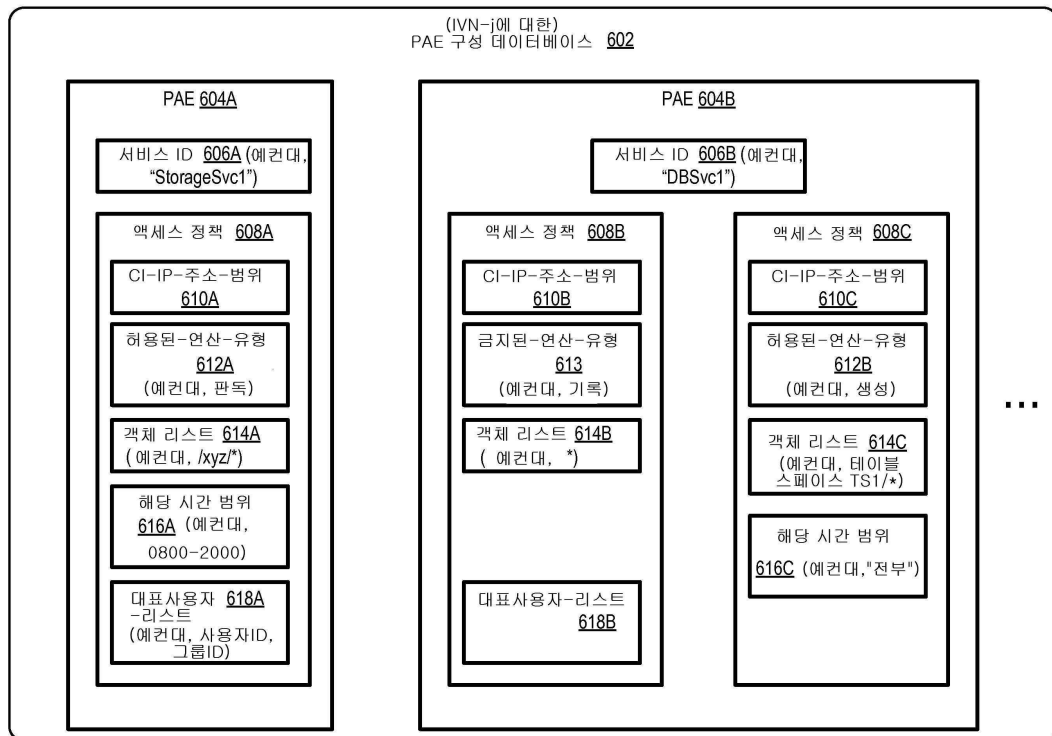
도면4



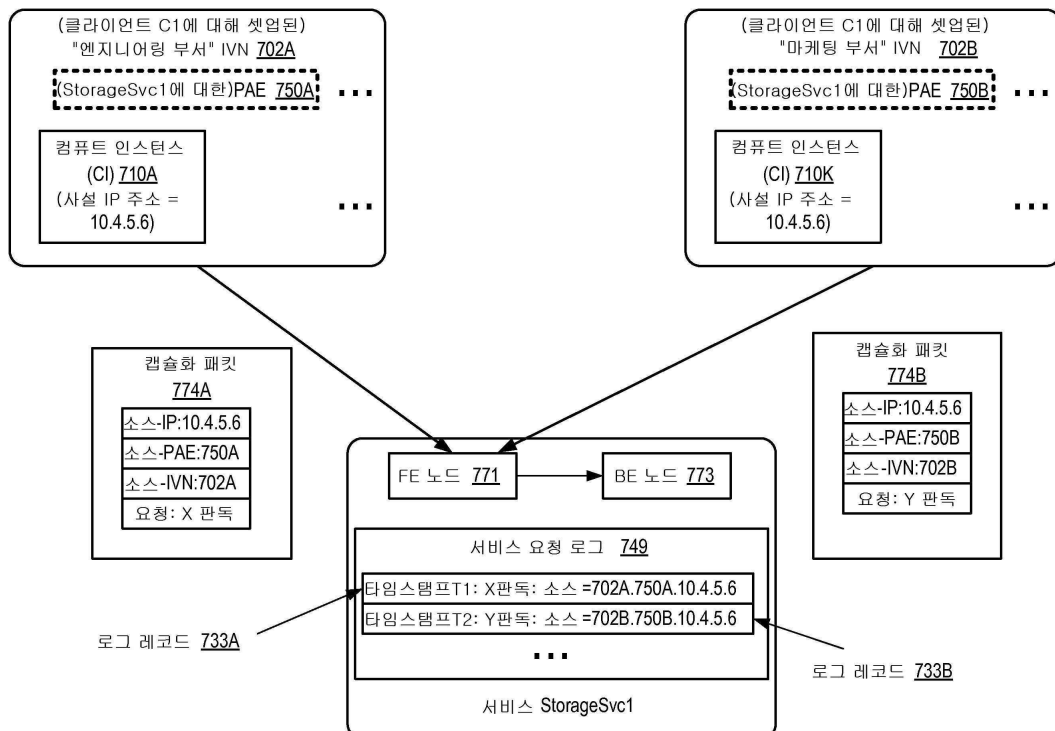
도면5



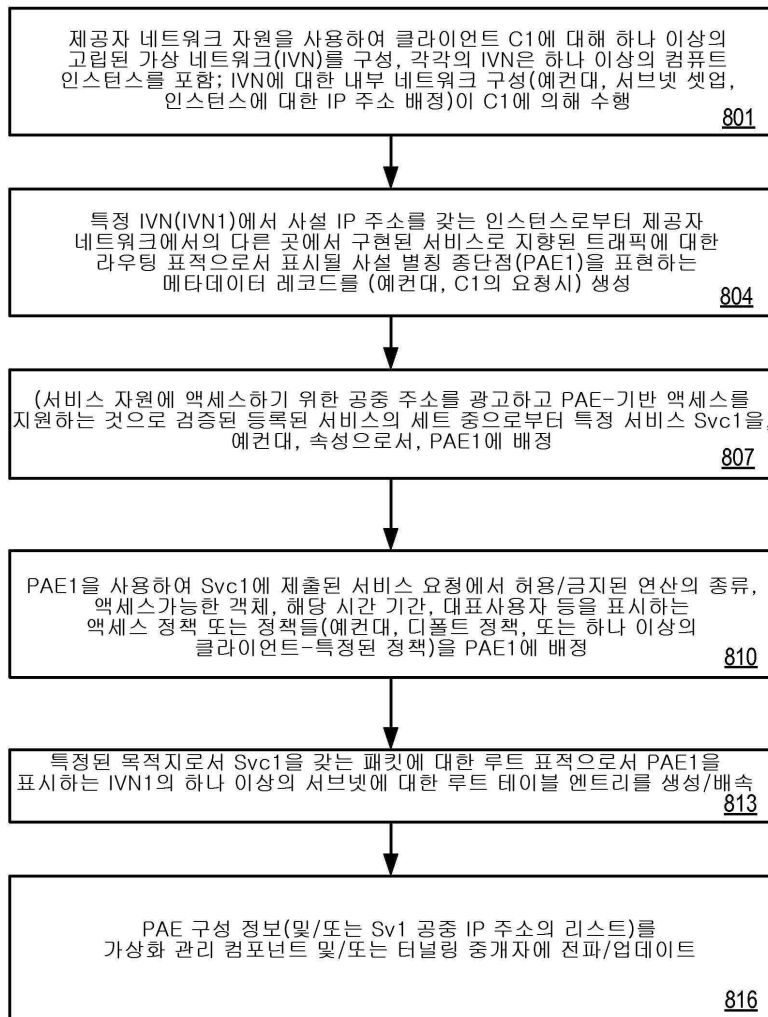
도면6



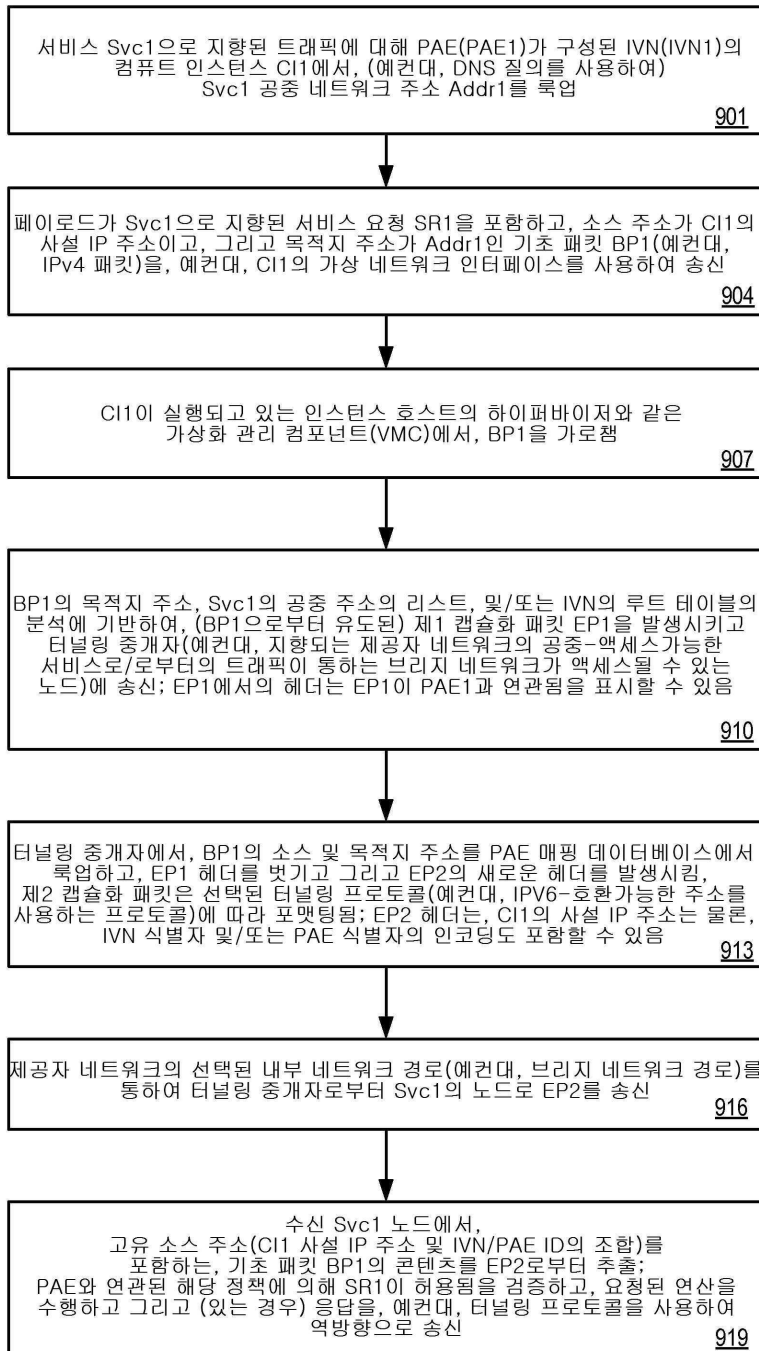
도면7



도면8



도면9



도면10

