(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년04월05일
(11) 등록번호 10-1966574
(24) 등록일자 2019년04월01일

(51) 국제특허분류(Int. Cl.)
H04L 12/713 (2013.01) *H04L 12/46* (2006.01)
H04L 12/741 (2013.01)
(52) CPC특허분류
H04L 45/586 (2013.01)
H04L 12/4633 (2013.01)
(21) 출원번호 10-2017-7024959
(22) 출원일자(국제) 2015년12월03일
심사청구일자 2017년09월05일
(85) 번역문제출일자 2017년09월05일
(65) 공개번호 10-2017-0128270
(43) 공개일자 2017년11월22일
(86) 국제출원번호 PCT/US2015/063783
(87) 국제공개번호 WO 2016/126313
국제공개일자 2016년08월11일
(30) 우선권주장
62/112,457 2015년02월05일 미국(US)
14/630,550 2015년02월24일 미국(US)
(56) 선행기술조사문헌
US20060037072 A1*
US20090031415 A1*
US20020026503 A1*
US7673048 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
크리프트존 노스 아메리카, 아이엔씨.
미국 메사추세츠 02453, 월섬, 빌딩 3 스위트 610, 터너가 130
(72) 발명자
그라체마카스 쿠르트
벨기에 그렘베르겐 9200, 로미에스트라트 28
알랑송 빼 요한
스웨덴 쿵스바카 43447, 트롱봉바겐 66
(74) 대리인
특허법인(유한) 대아

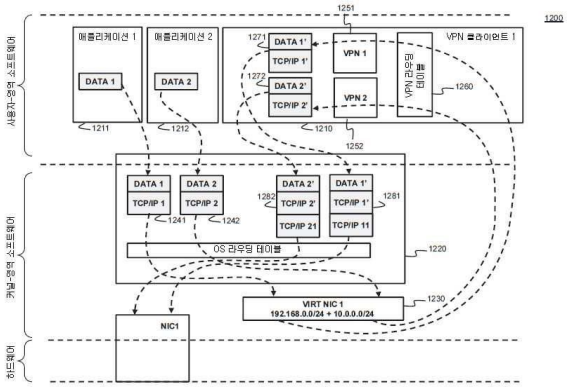
전체 청구항 수 : 총 13 항 심사관 : 윤태섭

(54) 발명의 명칭 **멀티-터널링 가상 네트워크 어댑터**

(57) 요 약

무엇보다도, 본 발명의 실시예들은 관리 특권에 대한 필요 없이 멀티 가상 사설 네트워크 연결을 생성할 수 있고, 각각의 가상 네트워크 연결에 대한 전용 가상 어댑터 대신 하나의 가상 어댑터를 이용하여 네트워크 트래픽이 라우트되게 할 수 있다.

대 표 도



(52) CPC특허분류
H04L 45/54 (2013.01)
H04L 49/354 (2013.01)
H04L 63/0272 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터 시스템에서 실행되는 운영 체제의 사용자 영역 부분에 존재하는 가상 사설 네트워크(VPN) 클라이언트의 라우팅 컴포넌트에 의해 네트워크를 통해 데이터 패킷(data packet)을 수신하는 단계;

상기 라우팅 컴포넌트에 의해, 상기 네트워크에서의 상기 데이터 패킷에 대한 목적지를 식별하는 단계;

상기 VPN 클라이언트에 의해, 상기 데이터 패킷에 대한 상기 목적지에 대응하는 게이트웨이로 연결을 생성하는 단계; 및

상기 게이트웨이를 통해 목적지로 상기 데이터 패킷을 전송하는 단계를 포함하는 컴퓨터-구현 방법.

청구항 2

제1항에 있어서, 상기 데이터 패킷은 상기 운영 체제의 커널 영역 부분에서 작동하는 가상 어댑터(virtual adapter)를 통해 수신되는, 컴퓨터-구현 방법.

청구항 3

제1항에 있어서, 상기 데이터 패킷에 대한 목적지를 식별하는 단계는 상기 데이터 패킷에 대한 목적지에 대응하는 게이트웨이를 식별하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 4

제1항에 있어서, 상기 게이트웨이로 연결을 생성하는 단계는 전송 제어 프로토콜(transmission control protocol) 연결을 생성하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 5

제1항에 있어서, 상기 게이트웨이로 연결을 생성하는 단계는 사용자 데이터그램 프로토콜(datagram protocol) 연결을 생성하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 6

제1항에 있어서, 상기 게이트웨이 연결을 제거하는 것을 더 포함하는, 컴퓨터-구현 방법.

청구항 7

제1항에 있어서,

상기 라우팅 컴포넌트에 의해, 복수의 데이터 패킷을 수신하는 단계;

상기 복수의 데이터 패킷으로부터 각각의 데이터 패킷에 대한 네트워크에서의 각각의 목적지를 식별하는 단계;

상기 복수의 데이터 패킷에서 각각의 데이터 패킷에 대한 각각의 목적지에 대응하는 게이트웨이로 각각의 연결을 생성하는 단계; 및

상기 각각의 게이트웨이 연결을 통해 각각의 목적지로 각각의 데이터 패킷을 전송하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 8

제7항에 있어서, 상기 복수의 게이트웨이 연결 중 하나 이상을 제거하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 9

제7항에 있어서, 상기 복수의 데이터 패킷은 상기 운영 체제의 커널 영역에서 작동하는 하나의 가상 어댑터를 통해 각각 라우트되는, 컴퓨터-구현 방법.

청구항 10

제1항에 있어서, 상기 라우팅 컴포넌트는 라우팅 테이블(routing table)을 포함하는, 컴퓨터-구현 방법.

청구항 11

제10항에 있어서, 상기 라우팅 테이블은 데이터 패킷에 대한 목적지 어드레스를 식별하는, 컴퓨터-구현 방법.

청구항 12

실행될 때 컴퓨터 시스템이 하기 단계들을 야기하는 명령어를 저장하는, 비-일시적 컴퓨터-판독가능 매체:

컴퓨터 시스템에서 실행되는 운영 체제의 사용자 영역 부분에 존재하는 가상 사설 네트워크(VPN)의 라우팅 컴포넌트에 의해 네트워크를 통해 데이터 패킷을 수신하는 단계;

상기 라우팅 컴포넌트에 의해, 상기 네트워크에서의 데이터 패킷에 대한 목적지를 식별하는 단계;

상기 VPN의 클라이언트에 의해, 상기 데이터 패킷에 대한 목적지에 대응하는 게이트웨이로 연결을 생성하는 단계; 및

상기 게이트웨이를 통해 상기 목적지로 상기 데이터 패킷을 전송하는 단계.

청구항 13

프로세서(processor); 및

상기 프로세서와 연결되고, 상기 프로세서에 의해 실행되는 경우 컴퓨터 시스템이 하기 단계들을 야기하는 명령어를 저장하는 메모리를 포함하는 컴퓨터 시스템:

상기 컴퓨터 시스템에서 실행되는 운영 체제의 사용자 영역 부분에 존재하는 가상 사설 네트워크(VPN) 클라이언트의 라우팅 컴포넌트에 의해 네트워크를 통해 데이터 패킷(data packet)을 수신하는 단계;

상기 라우팅 컴포넌트에 의해, 상기 네트워크에서의 상기 데이터 패킷에 대한 목적지를 식별하는 단계;

상기 VPN 클라이언트에 의해, 상기 데이터 패킷에 대한 상기 목적지에 대응하는 게이트웨이로 연결을 생성하는 단계; 및

상기 게이트웨이를 통해 목적지로 상기 데이터 패킷을 전송하는 단계.

발명의 설명

기 술 분 야

[0001] 본 발명은 2015년 2월 24일 출원되고 "다중-터널링 가상 네트워크 어댑터(MULTI-TUNNELING VIRTUAL NETWORK ADAPTER)"을 제목으로 하는 미국 특허출원 일련번호 제14/630,550호와, 2015년 2월 5일 출원되고 "멀티-터널링 가상 네트워크 어댑터(MULTI-TUNNELING VIRTUAL NETWORK ADAPTER)"을 제목으로 하는 미국 가출원 번호 제62/112,457호에 대한 우선권을 주장하고, 이의 개시 내용은 본 명세서에 참고로 포함된다.

[0002] 본 발명은 2014년 12월 19일에 출원되고 "네트워크 장치를 보호하기 위한 시스템 및 방법(SYSTEMS AND METHODS FOR PROTECTING NETWORK DEVICES)"를 제목으로 하는 미국 특허출원번호 제14/578,140호와 관련되고, 본 명세서에 참고로 포함된다.

배 경 기 술

[0003] 클라이언트-서버 네트워크 모델에서, 회사 또는 서비스 공급자는 일반적으로 컴퓨터 네트워크를 통해 클라이언트 컴퓨터 및 다른 서비스에 서비스 및/또는 응용 프로그램을 제공한다. 서버 및 관련 서비스는 예를 들어 메일 서버, 파일 서버, 고객 관계 관리 또는 CRM 서비스, 기업자원관리(Enterprise Resource Planning) 또는 ERP 서비스, 문서 관리 서비스 등을 포함할 수 있다.

[0004] 한편으로, 이러한 서비스에 대한 접근(acess)을 신뢰할 수 있는 사용자 및 클라이언트에게만 제한함으로써 보안을 보장해야한다. 반면에, 신뢰할 수 있는 사용자는 쉽고 간단한 방식으로 서비스에 접근하는 것이 필요하다. 바람직하게는, 언제 어디서나 서비스에 도달할 수 있는 것이다. 기업에서 점점 더 많이 용인되는 "자신의 장치 가져오기"(또는 "BYOD")에 따라, "어떠한 것(anything)" 즉, 예를 들어 태블릿 컴퓨터, 노트북, 집에 있는 컴퓨터 또는 스마트폰과 같은 신뢰할 수 있는 사용자 소유의 임의의 장치로부터 서비스를 받을 수 있어야한다.

[0005] 이러한 애플리케이션 서버 또는 해당 애플리케이션 서버에서 제공하는 서비스나 애플리케이션에 대한 무단 접근을 방지하기 위해 시도하는 다양한 방법이 있다. 예를 들어, 사설 네트워크 내에 애플리케이션 서버를 배치하는 것은 기업 네트워크, 인터넷에서의 LAN(Local Area Network) 또는 기타 외부 공용 네트워크를 격리할 수 있기 때문에 자체로 보안 조치이다. 사설 네트워크 내의 장치 및 서비스는 공용 네트워크에서 볼 수 없다. 사설 네트워크의 트래픽 양과 트래픽이 회사 네트워크 경계를 통과할 수 있는 방식은 NAT(Network Address Translation), 방화벽 규칙 및 회사 사설 네트워크에서 WAN를 분리하는 게이트웨이 장치에서의 프록시를 사용하여 규제 및 모니터링할 수 있다. 사설 네트워크는 회사 사설 네트워크 내에서 클라이언트에 의해 잠재적인 무단 엑세스로부터 응용 프로그램 서버를 추가로 분리하기 위해 예를 들어 가상 LAN에 의해 물리적 또는 가상으로 추가로 세분화될 수 있다.

[0006] 네트워크 레벨 보안은 인증 서버에만 엑세스하도록 클라이언트의 방화벽을 구성하는 것에 의해(디폴트(default)로) 사용자별 또는 클라이언트별로 시행될 수 있다. 클라이언트가 인증되면 클라이언트의 방화벽이 열리고 모든 네트워크 장치는 클라이언트의 네트워크 트래픽을 엑세스 권한이 승인된 애플리케이션 서버로 전달하도록 구성된다.

[0007] 또한 클라이언트 또는 사용자 수준의 네트워크 레벨 보안은 ID 프로필 및 상태 프로필을 기반으로 사용자에 대한 엑세스 권한을 생성하는 컨트롤러(controller)에서 시도될 수 있다. 그런 다음, 컨트롤러는 보호 장치를 구성하여 일련의 서버에 대한 네트워크 엑세스를 제공한다.

[0008] 호스트 수락에서의 네트워크 레벨 보안의 강화는 컨트롤러에 의해 호스트를 구성하는 것에 의해 시도될 수 있다. 호스트 초기화가 호스트 수락에 대한 엑세스 권한을 가질 때 컨트롤러는 호스트 초기화로부터 네트워크 연결을 수락하도록 호스트 수락을 구성한다.

[0009] 사설 네트워크 내의 보안은 사용자 또는 클라이언트가 인증 후 서버 상에서 서비스에 엑세스할 수 있는 애플리케이션 레벨 보안에 의해 추가로 강화될 수 있다. 이러한 경우 클라이언트는 네트워크 내의 애플리케이션 서버를, 예를 들어 IP 네트워크 어드레스에 의해 찾을 수 있으며, TCP 또는 UDP 포트 넘버에 의해 응용 프로그램 서버에서 서비스가 실행되고 있는 것을 발견할 수 있지만, 서비스 또는 응용 프로그램 자체가 인증 자격 증명에 기반하여 사용자 또는 클라이언트를 거부할 수 있다. 이러한 인증은 개별 서비스에 의해 로컬로 관리하거나 인증 서버에서 중앙에서 관리될 수 있다. 그런 다음 서비스는 특정 서비스에 대한 사용자 및/또는 클라이언트 엑

세스 권한을 승인하기 전에 이러한 인증 서버에 대한 인증 자격 증명을 확인한다.

[0010] 회사의 사설 네트워크에 대한 엑세스는 클라이언트 장치와 사설 네트워크간 보안 네트워킹 터널이 셋업(setup)되는 VPN 또는 가상 사설 네트워크에 의해 설정될 수 있다. 이러한 터널 셋업은 VPN 서버를 통한 인증으로만 승인된다. 신뢰할 수 있는 사용자 및/또는 클라이언트만 VPN에 참여할 수 있도록 여러 인증 체계가 존재한다.

[0011] 회사 사설 네트워크에서 서비스에 대한 엑세스를 제공하는 또 다른 방법은 일부 서비스에 대한 외부 엑세스를 개방하는 것이다. 예를 들어 이메일 서버는 회사 외부에 있는 사용자가 이들의 이메일을 확인할 수 있도록 외부에서 연결을 허용 할 수 있다. 이러한 서비스는 때로는 회사의 웹사이트를 통해 특정 인터페이스를 통한 엑세스만 제공하여 클라이언트가 서비스를 실행하는 서버에 대한 물리적 네트워크 엑세스가 없이 서비스의 서브 세트를 제공하는 웹 서버에만 엑세스하도록 제한되는 경우가 있다 .

[0012] 리스크 기반 인증에서, 서비스에 대한 엑세스가 인증 자격 증명에 의한 사용자 및/또는 클라이언트의 식별을 기반으로 승인될 뿐만 아니라 리스크 레벨에 적합한 신뢰 수준을 유도하기 위해 추가 메트릭스(metrics)를 기반으로 한다. 이러한 메트릭스는 예를 들어, 사용자의 위치, 클라이언트 유형, 운영 체제(operating system), 설치된 모든 보안 패치가 설치된 경우 사용자의 로그온 기록 등이다. 이러한 방식으로 VPN에 로그온하는 사용자는 서비스에서 제한될 수 있고, 사설 네트워크 내에서 로그온할 때 제한되지 않는다. 또는 자신의 장치로 사설 네트워크 내에서 로그온한 사용자가 일부 서비스를 거부할 수 있다.

[0013] 가상 네트워크 어댑터는 VPN 연결을 셋업할 때 사용되며, 이에 의해 운영 시스템이 가상 어댑터를 통해 VPN으로 향하는 패킷(packet)을 라우팅한다. 가상 어댑터는 운영 체제의 커널(kernel) 영역에서 실행된다. VPN 소프트웨어, 즉 사용자-영역에서 실행되는 전용 소프트웨어 응용 프로그램은 완전한 패킷을 암호화하여 목적지(역 프로세스가 발생하는 다른 쪽의 VPN 서비스)로 전송한다. 그러나 종래 시스템에서 어댑터가 커널 영역에 존재하므로 가상 어댑터를 생성하려면 관리 권한이 필요하다. 또한 만들어진 모든 VPN 연결마다 새로운 가상 어댑터가 필요하다. 본 발명의 실시예들은 이들 및 다른 문제들을 다룬다.

발명의 내용

해결하려는 과제

[0014] 무엇보다도, 본 발명의 실시예들은 관리 권한을 필요로 하지 않고 멀티 가상 사설 네트워크 연결을 생성할 수 있게 하고, 각각의 가상 네트워크 연결을 위한 사설 가상 어댑터 대신에 단일 가상 어댑터를 사용하여 네트워크 트래픽을 라우팅할 수 있다.

과제의 해결 수단

[0015] 본 발명의 일 실시예에 따른 컴퓨터-구현 방법은 가상 사설 네트워크(VPN) 클라이언트의 라우팅 컴포넌트에 의해 네트워크를 통해 데이터 패킷을 수신하는 단계, 상기 VPN 클라이언트는 운영 시스템에서 실행되는 운영 체제의 사용자 영역 부분에 존재; 상기 라우팅 컴포넌트에 의해, 상기 네트워크상의 상기 데이터 패킷에 대한 목적지를 식별하는 단계; 상기 VPN 클라이언트에 의해, 상기 데이터 패킷에 대한 목적지에 대응하는 게이트웨이에 대한 연결을 생성하는 단계; 및 상기 게이트웨이를 통해 상기 목적지로 상기 데이터 패킷을 전송하는 단계를 포함한다.

[0016] 본 발명은 이러한 방법을 수행하는 다양한 방법, 장치(컴퓨터 시스템 포함) 및 컴퓨터 시스템에 의해 실행될 때 컴퓨터 시스템이 이러한 방법을 수행하게 하는 명령어(instruction)를 포함하는 컴퓨터 판독 가능 매체를 포함한다.

[0017] 다른 특징은 첨부된 도면 및 하기 상세한 설명으로부터 명백해질 것이다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 다양한 양태에 따라 신뢰하지 않는 클라이언트 장치에 의한 네트워크 엑세스로부터 네트워크 장치를 보호하기 위한 예시적인 시스템이다.

도 2는 본 발명의 다양한 양태에 따라 보호된 네트워크 장치에 대한 네트워크 엑세스를 얻기 위해 클라이언트

장치에 의해 실행되는 예시적인 프로세스이다.

도 3은 클라이언트 엑세스 및 터널 리스트를 클라이언트 장치에 제공하여 이 러한 클라이언트 네트워크가 본 발명의 다양한 양태에 따라 네트워크 장치를 보호할 수 있게 하는 인증 서버에 의해 실행되는 예시적인 프로세스이다.

도 4는 본 발명의 다양한 양태에 따라 이러한 게이트웨이에서 방화벽 뒤의 보호된 네트워크 장치에 클라이언트 엑세스를 제공하기 위해 게이트웨이에 의해 실행되는 예시적인 프로세스이다.

도 5는 본 발명의 다양한 양태에 따라 이들 네트워크 장치의 제1 선택에 대한 엑세스를 얻은 후 게이트웨이의 방화벽 뒤에 있는 네트워크 장치의 제2 선택에 대한 네트워크 엑세스를 얻기 위해 클라이언트 장치에 의해 실행되는 예시적인 프로세스이다.

도 6은 본 발명의 다양한 양태에 따라 클라이언트와 클라이언트 장치 사이의 네트워킹 터널을 유지하기 위해 클라이언트 장치와 게이트웨이 간 킵 얼라이브 메시지(keep alive message)의 예시적인 교환을 도시한다.

도 7은 본 발명의 다양한 양태에 따라 신뢰하지 않는 클라이언트 장치에 의한 네트워크 엑세스로부터 네트워크 장치를 보호하기 위한 예시적인 시스템을 도시한다.

도 8은 본 발명의 다양한 양태에 따라 신뢰하지 않는 클라이언트 장치에 의한 네트워크 엑세스로부터 네트워크 장치를 보호하기 위한 예시적인 시스템을 도시한다.

도 9는 본 발명의 다양한 양태에 따라 게이트웨이의 네트워킹 부하가 제2 게이트웨이에 의해 밸런스된, 신뢰되지 않은 클라이언트 장치에 의한 네트워크 엑세스로부터 네트워크 장치를 보호하기 위한 예시적인 시스템을 도시한다.

도 10은 본 발명의 다양한 양태에 따른 예시적인 컴퓨터 시스템을 도시한다.

도 11은 VPN 연결 및 라우팅 패킷을 생성하기 위한 종래 방법을 나타내는 예시적인 시스템을 도시한다.

도 12는 본 발명의 다양한 양태에 따른 다중-터널링 가상 네트워크 어댑터를 이용하는 예시적인 시스템을 도시한다.

도 13은 본 발명의 다양한 양태에 따른 다중-터널링 가상 네트워크 어댑터를 이용하는 다른 예시적인 시스템을 도시한다.

도 14는 본 발명의 다양한 양태에 따른 예시적인 프로세스이다.

발명을 실시하기 위한 구체적인 내용

[0019] 청구 대상은 본 명세서의 일부를 형성하고 예시로서 특정 예시적인 실시예를 나타내는 첨부 도면을 참조하여 보다 상세하게 설명될 것이다. 그러나, 청구 대상은 다양한 다른 형태로 구체화될 수 있으므로, 포괄된 또는 청구된 대상이 본 명세서에서 설명된 임의의 예시적인 실시예에 제한되지 않는 것으로 해석되어야한다; 예시적인 실시예들은 단지 예시적인 것으로 제공된다. 유사하게, 포괄된 또는 청구된 청구 대상에 대한 합리적으로 넓은 범위가 의도된다. 그 중에서도, 예를 들어 청구 대상은 방법, 장치, 컴포넌트 또는 시스템으로 구체화될 수 있다. 따라서, 실시예는 예를 들어 하드웨어, 소프트웨어, 펌웨어 또는 소프트웨어 그 자체와는 다른 이들의 임의의 조합의 형태를 취할 수 있다. 그러므로, 다음의 상세한 설명은 제한적인 의미가 아닌 것으로 의도된다.

[0020] 첨부된 도면에서, 일부 특징은 특정 컴포넌트의 세부 사항(도면에 도시된 임의의 크기, 재료 및 유사한 세부 사항은 예시적이고 제한적인 것이 아니다)을 나타내기 위해 과장될 수 있다. 따라서, 본 명세서에 개시된 특정 구조 및 기능적 세부 사항은 제한적으로 해석되어서는 안되며, 단순히 개시된 실시예를 다양하게 사용하기 위해 당업자에게 교시하기 위한 대표적인 기초로서 해석되어야한다.

[0021] 본 명세서에서 "일 실시예"또는 "실시예"로 언급되는 것은 실시예와 관련하여 기술된 특정 특징, 구조 또는 특성이 본 발명의 적어도 하나의 실시예에 포함됨을 의미한다. 본 명세서의 다양한 곳에서 "일 실시예"라는 어구의 나타남은 반드시 동일한 실시예를 모두 지칭하는 것이 아니며, 다른 실시예와 상호 배타적인 별개의 또는 대안적인 실시예가 아니다. 또한, 일부 실시예들에 의해 표현될 수 있고 다른 실시예에 의해 나타나지 않는 다양한 특징들이 설명된다. 유사하게, 일부 실시예에 대한 요건일 수 있지만 다른 실시예에 대한 요건은 아닐 수 있는 다양한 요건이 설명된다.

[0022] 본 발명에 도시된 방법의 요소들의 임의의 조합 및/또는 서브 세트는 서로 결합되거나, 다양한 조건에 기초하여 선택적으로 수행되거나 수행되지 않을 수 있고, 임의의 원하는 횟수만큼 반복될 수 있으며, 임의의 적합한 순서로 그리고 임의의 적합한 시스템, 장치 및/또는 프로세스와 함께 실시될 수 있다. 본 명세서에서 기술되고 도시된 방법들은 하나 이상의 컴퓨터 시스템상에서 작동하는 소프트웨어를 통하는 것과 같은 임의의 적절한 방식으로 구현될 수 있다. 소프트웨어는 컴퓨터 시스템의 메모리와 같은 구체적인 컴퓨터-판독 가능 매체에 저장된 컴퓨터-판독 가능 명령어를 포함할 수 있으며, 다양한 실시예의 방법을 수행하기 위한 하나 이상의 프로세서에 의해 실행될 수 있다.

[0023] 도 1은 본 발명의 다양한 양태에 따라 원하지 않는 네트워크 엑세스로부터 네트워크 장치를 보호하기 위한 예시적인 시스템을 도시한다. 이러한 실시예에서, 3개의 네트워크 장치(애플리케이션 서버 (141, 142 및 143))는 사설 네트워크 (140)의 일부이다. 서버 (141-143)에 대한 엑세스는 사설 네트워크 어드레스를 통해 사설 네트워크 (140) 내에서 얻어진다. 이러한 맥락에서, 용어 "전용(private)"은 애플리케이션 서버 (141-143)가 전세계적으로 라우팅할 수 없다는 사실을 나타낸다. 다시 말해, 애플리케이션 서버 (141-143)는 사설 네트워크 (140) 외부로부터 이들 사설 네트워크 어드레스에 의해 어드레싱(address)될 수 없다.

[0024] 도 1에서 사설 네트워크 (140) 및 다른 컴포넌트들은 인터넷 프로토콜 (IP), 또는 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP)로도 지칭되는 임의 수 및 유형의 통신 프로토콜을 이용할 수 있다. 예를 들어, 사설 네트워크 (140)는 인터넷 프로토콜 버전 4 또는 IPv4를 위한 RFC 1918 또는 인터넷 프로토콜 버전 6 또는 IPv6를 위한 RFC 4193에 의해 설정되는 바와 같이 어드레스 범위를 가질 수 있다.

[0025] 응용 프로그램 서버 (141-143)는 네트워크 (140)를 통해 다른 컴퓨터 장치에 서비스를 제공한다. 메일 서버, 파일 서버, 고객 관계 관리 또는 CRM 서비스, 기업 자원 관리 또는 ERP 서비스 및/또는 문서 관리 서비스와 같은 임의의 수 및 유형의 애플리케이션 서버가 본 발명의 실시예와 함께 사용될 수 있다.

[0026] 데이터 연결은 서비스와 관련된 포트 (또는 포트 범위)상의 각각의 애플리케이션 서버로 통신 소켓을 개방함으로써 애플리케이션 서버 (141-143) 중 임의의 서버로 설정될 수 있다. 애플리케이션 서버 (141-143)는 사설 네트워크 어드레스와 관련된 물리적 네트워킹 인터페이스를 갖는 물리 장치에 대응할 수 있다. 대안으로, 애플리케이션 서버 (141-143)는 하나 이상의 물리적 서버에서 실행되는 가상 서버 인스턴스(instance)에 대응할 수도 있다. 가상 서버 인스턴스는 관련된 사설 네트워크 어드레스를 갖는 가상 네트워크 인터페이스를 각각 가질 수 있다. 가상 서버 인스턴스는 하나 이상의 사용자 영역 인스턴스 (소프트웨어 컨테이너(software container), 가상 엔진(virtual engine), 가상 사설 서버 및/또는 자일(jail)로 알려짐)를 포함할 뿐 아니라, 이들과 함께 작동될 수 있다. 이러한 사용자 영역 인스턴스는 DOCKER 소프트웨어 툴을 통한 것을 포함하여 임의의 적절한 방식으로 구현될 수 있다.

[0027] 도 1에 도시된 실시예에서, 사설 네트워크 (140)는 게이트웨이 (100)에 의해 외부 네트워크 (180)로부터 분리되어, 제어된 방식으로 외부 네트워크 (180)와 사설 네트워크 (140) 사이의 네트워크 트래픽을 허용한다. 도 1의 시스템은 사설 네트워크 (140) 내의 하나 이상의 애플리케이션 서버 (141-143)에 대한 엑세스 권한을 갖는 "신뢰된 클라이언트"로서 라이언트 (121, 122)를 식별할 수 있어 실행되는 서비스를 사용할 수 있다. 클라이언트 (121, 122)는 물리적 하드웨어 및/또는 가상 컴포넌트이거나 또는 이들을 포함할 수 있다. 예를 들어, 클라이언트 (121, 122)는 모바일 장치와 같은 물리 장치에서 실행되는 가상 운영 체제를 포함할 수 있다. 시스템은 또한 클라이언트 (121, 122)가 엑세스하도록 허용된 애플리케이션 서버 (141-143)의 선택에 네트워크 엑세스를 허가할 수 있고, 클라이언트 (121, 122)가 엑세스할 수 없는 임의의 애플리케이션 서버에 대한 네트워크 엑세스를 거부할 수 있다.

[0028] 애플리케이션 서버 (141-143)로 클라이언트 (121, 122)에 의한 엑세스를 제어하기 위해, 게이트웨이 (100)는 외부 네트워크 (180)에서 클라이언트 (121, 122)에 의한 요청에 따라 네트워킹 터널을 설정하기 위한 터널 모듈 (101)을 포함한다. 도 1에 나타낸 실시예에서, 네트워킹 터널 (181, 182)은 각각 터널 모듈 (101)과 클라이언트 (121,122) 사이에 설정되어, 사설 네트워크 (140)를 클라이언트들 (121,122)로 연장된다. 일부 실시예에서, 가상 사설 네트워크(또는 VPN)는 터널 (181, 182)을 통해 설정된다. 이러한 방법에서, 클라이언트 (121, 122)가 비록 네트워크 (180) 내에 있지만 사설 네트워크 (140)의 범위에서 사설 네트워크 어드레스가 제공되므로, 잠재적으로 이들 각각의 사설 네트워크 어드레스에 의해 모든 애플리케이션 서버 (141-143)가 엑세스될 수 있다(아래에서 더욱 상세히 설명되는 바와 같이 제공된 엑세스가 허용됨).

[0029] 터널은 클라이언트 (121, 122)의 요청에 따라 설정되어, 터널 인증 정보를 터널 모듈 (101)에 제공한다. 임의의 양 및 유형의 인증 정보는 사용자명 및 패스워드와 같고, 본 발명의 실시예와 함께 사용될 수 있다. 터널 인증

정보는 또한 (또는 대안적으로) 생체 인증(biometrics), 2-요소 인증 및/또는 다른 암호 방법을 포함할 수 있다. 터널 (181, 182)에서 이동하는 데이터는 인터넷 프로토콜 보안 (또는 IPsec 프로토콜), 전송 계층 보안 (또는 TLS) 및/또는 데이터 그램 전송 계층 보안 (또는 DTLS)에 따른 것과 같은 암호화에 의해 추가로 보호될 수 있다. 터널 인증 모듈 (105)은 터널 인증 정보를 검증하고, 인증에 성공하면 개개 클라이언트와의 네트워크 터널을 설정한다.

[0030] 도 1에서 게이트웨이 (100)는 각각의 터널 (181, 182)이 설정된 후에 클라이언트 (121, 122)와 애플리케이션 서버 (141-143) 사이의 네트워크 트래픽을 제어하기 위한 방화벽 (102)을 포함한다. 방화벽 (102)은 방화벽 구성 모듈 (103) 또는 다른 소스로부터 제공된 방화벽 규칙에 따라 이러한 트래픽을 제어할 수 있다. 일부 실시예에서, 방화벽 구성 모듈 (103)은 차례로 인증 서버 (160)로부터 클라이언트 엑세스 리스트를 수신하는, 개개 클라이언트 (121, 122)로부터 수신된 클라이언트 엑세스 리스트로부터 방화벽 규칙을 획득한다.

[0031] 이들 중에서, 방화벽 규칙은 클라이언트 (121, 122)가 애플리케이션 서버 (141, 142 및 143)와의 네트워크 연결을 설정하고 유지할 수 있게 한다. 클라이언트 (121, 122)가 엑세스할 수 있는 애플리케이션 서버 (141-143)의 선택은 방화벽 규칙이 획득된 클라이언트 엑세스 목록으로부터 결정될 수 있다. 방화벽 규칙은 임의의 원하는 정보가 포함될 수 있다. 일부 실시예에서, 예를 들어 방화벽 규칙은 클라이언트가 엑세스할 수 있는 정보를 정의하는 인타이틀먼트 토큰(entitlement token)을 포함한다. 이러한 인타이틀먼트 토큰은 네트워크 트래픽 엑세스를 허가/거부할 뿐만 아니라, 다양한 파일(예를 들어, 기밀로 분류됨(메타 데이터 포함))에 대한 엑세스 가능하도록 방화벽을 구성하는데 사용될 수 있다.

[0032] 방화벽 (102)은 임의의 수 및 유형의 시스템, 장치, 하드웨어 컴포넌트 및/또는 소프트웨어 컴포넌트일 수 있거나 포함할 수 있다. 예를 들어, 방화벽 (102)은 복수의 하드웨어 및/또는 소프트웨어 컴포넌트를 포함하는 분산형 방화벽으로서 구현될 수 있다. 일부 실시예에서, 방화벽 (102)은 기본적으로 보안 터널 (180, 181)을 통해 클라이언트 (121, 122)로부터의 모든 트래픽을 차단하지만, 방화벽 규칙에 응답하여 트래픽을 허용하도록 구성될 수 있다. 예를 들어, 클라이언트 엑세스리스트가 클라이언트 (121)가 애플리케이션 서버 (141)에 엑세스할 수 있음을 나타내면, 방화벽 구성 모듈 (103)은 대응하는 규칙을 획득하고, 방화벽 (102)에서 그것을 활성화한다. 규칙의 활성화 후에, 방화벽 (102)은 클라이언트 (121)와 애플리케이션 서버 (141) 사이의 사설 네트워크 (140)에서의 네트워크 트래픽을 더 이상 차단하지 않는다.

[0033] 도 1의 시스템은 클라이언트 (121, 122)를 인증하고 클라이언트 정보를 생성하기 위한 인증 모듈 (162)을 포함하는 인증 서버 (160)를 포함한다. 도 1에 나타낸 실시예에서, 클라이언트 (121, 122)가 사설 네트워크 (140)에서 애플리케이션 서버 (141-143)로 엑세스하기 위해, 먼저 인증 서버 (160)로 자신을 인증할 필요가 있다.

[0034] 인증 서버 (160)는 하드웨어 및 소프트웨어 컴포넌트의 임의의 원하는 조합을 사용하여 구현될 수 있고, 임의의 원하는 방식으로 다른 하드웨어 및 소프트웨어 컴포넌트와 통신할 수 있다. 도 1에 나타낸 예시적인 시스템에서, 인증 서버 (160)는 사설 네트워크 (140)의 일부가 아니라, 네트워크 (180)를 통해 클라이언트 (121, 122)에 의해 엑세스 가능한 것이다. 클라이언트 (121, 122)에 의해 제공되는 인증 정보는 사용자명 및 패스워드를 제공하는 것에 의해 클라이언트 또는 클라이언트의 사용자를 유일하게 식별한다.

[0035] 클라이언트 (121, 122)는 임의의 수 및 유형의 상이한 인증 방법을 사용하여 인증될 수 있다. 예를 들어, 패스워드 인증을 추가하여(또는 대안으로서), 인증은 클라이언트 하드웨어의 사용 내역 및 클라이언트의 하드웨어 속성과 같은 클라이언트 (121, 122)의 하드웨어에 기초한 인증을 이용할 수 있다. 일 실시예에서, 이러한 정보는 클라이언트 장치에서의 레코드에 저장될 수 있으며, 이에 의해 다른 기계로의 레코드 이동의 검출은 인증 실패를 초래한다. 추가적인 무결성(integrity)을 제공하기 위해 레코드는 암호화 및/또는 키-사인(key-sign)될 수 있다. 또한, 클라이언트 (121, 122)가 미리 결정된 시간 윈도우(window) 외부에서 인증을 시도하는 경우, 인증이 거부(또는 추가 인증이 요구됨)되는 것과 같은 인증이 시간 윈도우에 기초할 수 있다.

[0036] 인증은 클라이언트 (121, 122)의 인터넷 프로토콜(IP) 어드레스 또는 클라이언트 (121, 122)와 관련된 글로벌 위치 정보와 같은 위치-기반 정보에 기초하여 수행될 수 있다. 예를 들어, 클라이언트 (121, , 122)의 물리적 위치가 글로벌 위치 정보, 특정 IP 어드레스, 또는 클라이언트의 IP 어드레스의 국가 코드로부터 결정될 수 있으며, 클라이언트 (121, 122)가 진짜 클라이언트인지 또는 클라이언트인 체하는 제3 자(예를 들어 헤커)인지를 결정하는데 사용될 수 있다. IP 어드레스(국가 코드 등에 기반한 개인 또는 범위)가 전의 기록(예를 들어, 해킹 시도, 인증 실패 등)을 기초로 블랙리스트에 올라 있거나 허용 목록에 포함될 수 있다. 마찬가지로, 인증을 위해 사용되는 위치-기반 정보는 또한 연결을 시도할 때 클라이언트 (121, 122)에 의해 사용되는 물리적 네트워크(들)로부터 도출될 수 있다.

[0037] 인증 모듈 (162)은 또한 클라이언트 (121, 122)로부터 직접적으로 상황 정보(context) 또는 상태 정보를 수신할 수 있다. 이러한 정보가 클라이언트로부터 직접 수신되어, 인증 서버에 의해 검증될 수 없는 경우, 이는 신뢰할 수 없는 "클라이언트 상황 정보"로서 처리될 수 있다. 클라이언트 정보에 포함될 수 있는 클라이언트 상황 정보는 다음과 같은 정보를 포함할 수 있다: "host.domain.com"과 같은 완전히 자격이 주어진 도메인 이름(또는 FQDN); 호스트에서 실행되는 운영 체제의 패밀리 및 버전 번호; 운영 체제에 적용된 패치를 나타내는 패치 레벨; 클라이언트에 설치된 바이러스 백신 소프트웨어의 상태; 및/또는 클라이언트 장치의 사용자가 클라이언트로 로그인된 지속 시간.

[0038] 인증 모듈 (162)은 또한 클라이언트 정보에 "신뢰할 수 있는 클라이언트 정보"를 추가할 수 있으며, 이는 사용자가 속해 있는 사용자 그룹 및 부서를 나타내는 사용자 멤버쉽 정보와 같은 정보를 포함할 수 있다. 신뢰할 수 있는 클라이언트 정보는 경량 디렉토리 엑세스 프로토콜(LDAP) 또는 액티브 디렉토리(AD) 서비스를 사용하여 사용자 디렉토리 시스템에 의해 제공될 수 있다. 신뢰할 수 있는 클라이언트 정보는 인증 서버 (160)와 클라이언트의 이전 세션에 대한 기록 정보(예를 들어, 마지막 로그인 타임 스탬프(time stamp) 및 로그인 시도 실패 횟수)와 같은 정보를 포함할 수 있다.

[0039] 도 1에 나타낸 실시예에서, 인증 모듈 (162)은 클라이언트 리스트 엔진 (client list engine, 163) 및 터널 리스트 엔진 (tunnel list engine, 165)을 포함한다. 인증 모듈 (162)에 의한 성공적인 인증시, 터널 리스트 엔진 (165)은 클라이언트 터널 리스트를 생성하고, 인증 모듈에 의해 제공된 클라이언트 정보에 기초한 클라이언트 엑세스 리스트를 생성한다.

[0040] 클라이언트 터널 리스트는 인증된 클라이언트 (121, 122)가 각각의 터널 (181, 182)을 설정하기 위한 모든 정보를 포함할 수 있다. 클라이언트 터널 리스트는 예를 들어, 네트워크 어드레스 정보(예를 들어, 목적지 IP 어드레스 및/또는 게이트웨이 (100)의 목적지 포트 번호)를 포함하여, 클라이언트 (121, 122)가 클라이언트 터널 리스트에서 특정된 IP 어드레스 및 포트 번호에서 터널의 셋업을 요청함으로써 각각의 터널 (181, 182) 설정을 초기화할 수 있다. 클라이언트 터널 리스트는 또한 게이트웨이 (100)에서 인증 모듈 (105)로 클라이언트 (121, 122)를 인증하기 위해 터널 인증 정보를 포함할 수 있다. 클라이언트 터널 리스트는 클라이언트를 다양한 게이트웨이에 연결하는데 필요한 정보를 포함하는 예를 들어 가상 사설네트워크 (VPN) 토큰을 포함할 수 있다.

[0041] 터널 리스트 엔진 (165)에 의해 생성된 터널 인증 정보는 동적일 수 있다 (즉, 사전에 게이트웨이 (100)의 인증 모듈 (105)에 의해 알려지지 않음). 이러한 경우에, 인증 서버는 인증 서버 (160)와 게이트웨이 (100) 사이의 통신 링크 (communication link, 168)에 의해 터널 인증 정보를 게이트웨이 (100)에 전송할 수 있다. 따라서, 통신 링크 (168)는 게이트웨이 (100)와 인증 서버 (160) 사이에 채널을 제공할 수 있고, 사용자 및/또는 세션이 인증 서버 (160)에서 삭제되는 경우 구성 업데이트가 교환되게 하고 사용자 또는 세션에 의해 엑세스가 취소된다. 사용자 또는 세션이 제거될 수 있는 다양한 이유가 있다: 1) 서비스 데이터베이스가 변경되고 관리자는 모든 사용자에 대해 변경을 실시함; 2) 사용자가 자신의 인증 방법을 변경함; 또는 3) 사용자 또는 클라이언트가 시스템에서 금지됨. 통신 링크 (168)는 인증 서버 (160)와 하나 이상의 게이트웨이들 사이의 통신만을 허용하는 하이퍼텍스트 전송 프로토콜 보안 (HTTPS) 채널과 같은 임의의 원하는 방식을 통해 구현될 수 있다.

[0042] 클라이언트 엑세스 리스트는 클라이언트에게 엑세스 권한이 부여된 애플리케이션 서버 (141-143)의 선택을 식별한다. 일부 실시예에서, 클라이언트 리스트 엔진 (163)은 방화벽 (102)에 대한 방화벽 규칙을 생성하고, 클라이언트 엑세스 리스트에 이들 규칙을 포함한다. 방화벽 규칙은 게이트웨이 (100)에서 방화벽 구성 모듈 (103)에 의해 클라이언트 엑세스 리스트로부터 추출된 다음, 방화벽 (102)에 적용된다. 클라이언트 엑세스 리스트는 애플리케이션 서버 (141-143)의 어드레싱 정보에 조건을 추가할 수 있다. 클라이언트 엑세스 리스트의 예시적인 예를 하기 표에 나타낸다.

표 1

[0043] 조건부 애플리케이션 서버를 갖는 클라이언트 엑세스 리스트

IP 어드레스	조건
10.0.0.1	시간 간격(09.00-17.00)
10.0.0.11	도메인("domain.com")
10.0.0.3	스트링프리픽스(StringPrefix)(사용자명, "adm_")

[0044] 표 1의 첫 번째 열은 클라이언트가 네트워크 엑세스 권한을 부여받은 애플리케이션 서버의 IP 어드레스를 지정

한다. 두 번째 열은 엑세스 권한을 얻기 위해 수행될 필요가 있는 조건을 지정한다. 첫 번째 조건은 클라이언트가 애플리케이션 서버 10.0.0.1에 대한 엑세스 권한을 부여받는 특정 시간 간격을 지정한다. 두 번째 조건은 요청이 시작되어야하는 특정 도메인을 지정한다(즉, 클라이언트가 애플리케이션에 엑세스할 수 있는 도메인을 지정). 두 번째 조건은 예를 들어 회사에서 자체 도메인 (즉, 회사 네트워크 내)에서 엑세스만 허용하는 데 사용될 수 있다. 세 번째 조건은 특정 애플리케이션 서버 또는 다른 네트워크 장치에 엑세스할 수 있어야하는 특정 사용자 또는 그룹(예를 들어, 회사 관리자)을 식별하는 데 사용할 수 있다.

[0045] 도 1에 나타낸 예시적인 시스템에서, 인증 서버 (160)는 서명된 클라이언트 엑세스 리스트 및 서명된 클라이언트 터널 리스트와 같은 디지털-서명된 리스트를 생성하기 위한 서명 모듈 (164)을 포함한다. 서명 모듈 (164)에 의해 생성된 디지털 서명은 클라이언트 엑세스 및 터널리스트의 수신시 게이트웨이 (100)에서 서명 검증 모듈 (104)에 의해 검증될 수 있다. 게이트웨이 (100)가 인증 서버 (160)에 통지하지 않고 클라이언트 엑세스 리스트 및 클라이언트 터널 리스트가 클라이언트 (121, 122)에 의해 변경될 수 없도록 서명은 게이트 웨이 및 인증 서버 (160) 사이에서 공유하는 서명 키에 의해 생성되고 검증될 수 있다. 하나의 예시적인 실시예에서, 개인/공용 키 메커니즘을 사용하는 X.509 인증서가 인증서를 검증하기 위해 사용된다.

[0046] 일부 실시예에서, 서명 인증을 시도하는 동안 게이트웨이 (100)는 클라이언트 엑세스 리스트 또는 클라이언트 터널 리스트가 변화되었는지 결정하고, 게이트웨이 (100)는 인증 서버 (160)에 변경 사항을 통지 및/또는 클라이언트와의 네트워크 터널을 끊는다. 인증 서버 (160)는 클라이언트와 향후 상호 작용할 때 클라이언트와 관련된 "신뢰된 클라이언트 정보"의 일부로서 이러한 통지를 사용할 수 있다. 일부 실시예에서, 게이트웨이 (100)는 자신의 의도에 따라 설정된 네트워킹 터널 (181, 182)을 파괴 할 수있다(예를 들어, 전술한 바와 같이 클라이언트 엑세스 리스트 또는 클라이언트 터널리스트에서의 변화를 검출하는 것에 응답함). 부가적으로 또는 대안으로, 터널 모듈이 네트워크 터널을 끊고 개개 클라이언트를 허용하는 방화벽으로부터 방화벽 규칙을 제거하는 것을 지시하는 메시지를 통신 링크 (168)를 통해 게이트웨이 (100)에 전송함으로써 인증 서버 (160)는 게이트웨이 (100)가 설정된 네트워킹 터널을 끊도록 조정될 수 있다.

[0047] 도 2, 3 및 4는 도 1에 나타낸 예시적인 시스템의 컴포넌트, 즉 클라이언트 (121, 122), 인증 서버 (160) 및 게이트웨이(미도시)를 각각 포함하는 본 발명의 실시예와 함께 작동하는 다양한 컴포넌트에 의해 실행될 수 있는 예시적인 프로세스를 나타낸다. 여기서 설명되는 프로세스는 상이한 하드웨어 및/또는 소프트웨어 컴포넌트의 임의의 다른 조합에 의해 (전체적으로 또는 부분적으로) 수행될 수 있다.

[0048] 도 2, 3 및 4에서의 프로세스는 애플리케이션 서버 (141, 142 및 143)모두가 신뢰된 클라이언트 (121, 122)에게 보호된 방법으로 애플리케이션 서버의 서비스를 제공하는 것을 목표로 하는 회사에 속하는 경우와 같이 다양한 상황 및 상황에서 구현될 수 있다. 이러한 경우, "신뢰된 클라이언트"는 회사에 알려져 있고, 하나 이상의 애플리케이션 서버로 엑세스를 제공할 수 있는 사용자 또는 장치 자체인 클라이언트 장치이다. 각각의 클라이언트 (121, 122)는 애플리케이션 서버 (141-143)에 의해 이용 가능하게 된 서비스를 엑세스하고 사용할 수 있는 컴퓨터 하드웨어 및/또는 소프트웨어의 임의의 조합으로서 실행될 수 있다. 클라이언트는 예를 들어 데스크탑 컴퓨터, 랩탑 컴퓨터, 스마트 폰 및/또는 태블릿 컴퓨터일 수 있다(또는 포함할 수 있다). 클라이언트는 예를 들어 자신을 인증하기 위해 인증서를 사용하는 서버일 수도 있다((또는 포함). 도 2, 3 및 4에서의 프로세스는 클라이언트 (121, 122)가 게이트웨이를 통해서만 엑세스를 제공하는 대신(도 1에서의 게이트웨이 (100)) 사설 네트워크에 직접 엑세스하는 것을 방지하도록 돕는다. 이러한 제한은 회사의 사설 네트워크 내에서 작동하는 클라이언에 대해서도 적용될 수 있다. 이러한 시나리오의 예로서, 도 1을 다시 참조하면, 네트워크 (180)와 네트워크 (140) 모두는 분리된 "사설 네트워크"일 수 있지만, 클라이언트 (121, 122)와 애플리케이션 서버 (141-143) 간의 네트워크 통신은 여전히 게이트웨이 (100)에 의해 제어된다 .

[0049] 도 2는 애플리케이션 서버 (141-143)에서의 하나 이상의 서비스를 엑세스하기 위해 임의의 클라이언트 (121, 122)에 의해 실행될 수 있는 예시적인 프로세스를 나타낸다. 도 2의 프로세스는 클라이언트가 활동 중일 때 백그라운드에서 자동으로 실행되는 클라이언트 장치상의 소프트웨어 애플리케이션을 통하는 것과 같은 임의의 적절한 방식으로 구현될 수 있다. 소프트웨어 애플리케이션은 클라이언트 시작시 자동으로 작동되거나 사용자 또는 클라이언트에 작동하는 다른 프로세스에 의해 수동으로 시작될 수 있다. 클라이언트 (121, 122)는 애플리케이션 서버 (141-143) 중 하나로 클라이언트 장치의 네트워크 엑세스를 모니터링한다 (201). 애플리케이션 서버 (141-143)의 네트워크 어드레스는 애플리케이션 서버의 서비스를 이용하는 클라이언트 애플리케이션에서 구성 옵션일 수 있다. 예를 들어, 애플리케이션 서버는 메일 클라이언트 애플리케이션에 구성된 네트워크 어드레스 및 포트를 갖는 메일 서버; 네트워크 공유로서 네트워크 어드레스로 구성돈 파일 서버; CRM 서비스를 엑세스하기 위해 설치된 전용 클라이언트 애플리케이션을 갖는 CRM 서비스 또는 클라이언트; 및/또는 브라우저 애플리케

이션의 어드레스 바에서 어드레스를 특정하는 웹 서비스 및 사용자일 수 있다(또는 포함한다).

[0050] 클라이언트 애플리케이션은 목적지 네트워크 어드레스를 토대로 사설 네트워크 (140) 내의 애플리케이션 서버에 엑세스하려고 시도한다는 것을 검출할 수 있다 (202). 클라이언트는 인증 서버 (160)에 전송할 인증 정보를 검색한다 (203). 인증 정보의 검색은 예를 들어 사용자가 이전에 로그온하기 위해 제출한 인증 증명서를 사용함으로써 자동으로 수행될 수 있다. 대안으로, 인증 정보의 검색은 사용자에게 사용자명 및 패스워드와 같은 인증 증명서를 제공하도록 요청하는 것을 포함할 수 있다. 도 2의 단계 (201-203) 대신에, 클라이언트는 애플리케이션 서버 (141-143) 중 하나로 네트워크 엑세스 시도를 기다리지 않고 인증 서버 (160)로 직접 인증할 수 있다. 예를 들어, 클라이언트의 사용자가 클라이언트에 로그온하거나 클라이언트가 부팅할 때, 클라이언트는 인증 서버 (160)로 인증할 수 있다.

[0051] 클라이언트의 인증은 저장된 인증 증명서, 사용자의 로그온 증명서 및/또는 사용자로부터 요청된 별도의 인증 증명서를 사용하는 것과 같은 임의의 원하는 방식으로 수행될 수 있다. RSA, Oauth, 인증서, Radius, SAML 등을 포함하여 임의의 수 및 유형의 신원 제공자(identity provider)가 본 발명의 실시예와 결합하여 사용될 수도 있다. 응답시, 클라이언트는 인증 서버 (160)로부터 클라이언트 터널 리스트 및 클라이언트 엑세스 리스트를 수신한다 (205).

[0052] 클라이언트 (121, 122)는 예를 들어 클라이언트 터널 리스트로부터 게이트웨이 (100)의 네트워크 어드레스를 검색하고 터널을 설정하기 위해 게이트웨이 (100)에 요청을 전송함으로써 게이트웨이 (100)로 네트워크 터널 (181, 182)을 설정한다 (206). 터널을 설정하면 (206), 클라이언트는 클라이언트 터널 리스트를 인증으로서 게이트웨이로 제공할 수 있다. 클라이언트 터널 리스트는 인증 서버 (160)의 서명을 가지며, 이로부터 게이트웨이 (100)는 클라이언트가 신뢰되는지를 검증하고, 인증 증명서의 추가 교환없이 터널을 설정할 수 있다. 네트워크 터널이 설정된 후, 사설 네트워크 (140)는 터널을 통해 클라이언트로 확장되지만, 클라이언트는 애플리게이션 서버 (141-143) 중 임의의 것에 엑세스가 여전히 불가능할 수 있으며, 이는 서버로의 네트워크 엑세스가 게이트웨이 (100)의 방화벽에 의해 차단될 수 있기 때문이다.

[0053] 클라이언트는 인증 서버 (160)로부터 수신된 클라이언트 엑세스 리스트를 게이트웨이 (100)로 전송하고 (207), 클라이언트가 클라이언트 엑세스 리스트로부터 어떤 애플리케이션 서버에 엑세스할 수 있는지 기록한다 (211). 클라이언트는 또한 엑세스 가능한 애플리케이션 서버 또는 서비스를 클라이언트 장치의 사용자에게 신호를 주거나 표시할 수 있다. 성공적으로 인증되면, 게이트웨이 (100)는 클라이언트 엑세스 리스트에 나열된 애플리케이션 서버상의 모든 애플리케이션 서버 또는 서비스로 클라이언트 네트워크 엑세스를 제공한다.

[0054] 도 3은 도 1에서의 인증 서버 (160)와 같은 인증 서버에 의해 실행될 수 있는 클라이언트 엑세스 및 터널 리스트를 클라이언트에 제공하기 위한 예시적인 프로세스이다. 이러한 예시적인 프로세스에서, 인증 서버는 각각의 클라이언트 (301)로부터 요청을 수신한다. 요청에서, 클라이언트는 도 2의 단계 (204)에서와 같이 인증 서버로 식별을 위한 인증 정보를 제공한다. 인증 서버는 클라이언트를 식별하려고 시도한다 (302). 클라이언트가 인증 서버에 알려지지 않고 신뢰할 수 없는 경우, 서버는 흐름을 중단한다 (303). 클라이언트가 알려지면, 인증 서버는 신뢰된 클라이언트 정보를 검색하고, 클라이언트 정보에 이를 추가한다 (304). 단계 301에서 인증 정보로 수신된 클라이언트 상황 정보는 또한 클라이언트 정보에 추가될 수 있다.

[0055] 인증 모듈은 클라이언트가 엑세스하도록 허용된 애플리케이션 서버의 선택을 식별한다 (310). 클라이언트 정보와 함께 애플리케이션 서버의 선택은 인증 서버 (160)의 클라이언트 리스트 엔진 (163) 및 터널 리스트 엔진 (165)으로 전달될 수 있다. 터널 리스트 엔진 (165)은 예를 들어, 게이트웨이 (100)로 네트워킹 터널을 설정하기 위한 인증 증명서와 함께 게이트웨이 (100)이 IP 어드레스를 제공하는 것에 의해 클라이언트 정보에 기초하여 터널리스트를 생성한다. 클라이언트 터널 리스트는 서명 엔진 (164)에 의해 서명된다 (306). 인증 서버는 클라이언트가 엑세스하도록 허용된 서버의 선택에 기초하여 클라이언트 엑세스 리스트를 생성한다 (307). 클라이언트 정보에 기초하여, 추가 조건부 제한(conditional restriction)이 클라이언트 엑세스 리스트에 추가될 수 있다. 그런 다음, 또한 클라이언트 엑세스 리스트가 서명된다 (308). 인증 서버는 클라이언트 엑세스 및 터널리스트를 클라이언트에 전송한다 (309).

[0056] 도 4는 도 1의 게이트웨이 (100)와 같이, 본 발명의 실시예와 함께 작동하는 게이트웨이에 의해 실행될 수 있는 클라이언트로 네트워크 엑세스를 제공하기 위한 예시적인 프로세스를 나타낸다. 이러한 예시적인 프로세스에서, 게이트웨이 (101)는 클라이언트 (121 또는 122)로부터 요청을 수신하여 (401), 그 클라이언트와의 네트워킹 터널 (예를 들어, VPN 접속)을 설정할 수 있다. 이에 대응하여, 게이트웨이는 클라이언트로부터 인증 증명서를 요청하고 (402), 클라이언트 터널 리스트의 형태로 인증 증명서를 수신한다 (408). 클라이언트를 인증하기 위해,

게이트웨이 (100)는 인증 서버 (160)와 공유된 서명 키(signature key)를 사용하여 클라이언트 터널 리스트에서의 서명을 검증한다 (404). 서명이 정확하고, 클라이언트 터널 리스트가 클라이언트에 의해 수정되지 않으면, 게이트웨이 (100)는 클라이언트와의 네트워킹 터널을 설정하여 (405), 터널을 통해 사설 네트워크 (140)를 클라이언트로 확장한다. 게이트웨이의 방화벽은 기본적으로 클라이언트의 모든 네트워크 엑세스를 차단하도록 추가로 구성된다. 게이트웨이는 인증 서버에 의해 생성된 클라이언트로부터 클라이언트 엑세스 리스트를 수신하고 (406), 이러한 클라이언트 엑세스 리스트에서 서명을 검증한다 (407). 클라이언트 엑세스 리스트로부터, 게이트웨이는 클라이언트 엑세스 리스트 (및 클라이언트 엑세스 리스트에도 제공되는 이러한 엑세스에 대한 조건)에 열거된 애플리케이션 서버로 네트워크 엑세스를 허용하기 위한 방화벽 규칙을 획득한다 (408). 게이트웨이는 방화벽 규칙을 활성화 (409)함으로써, 클라이언트가 클라이언트 엑세스 리스트에 나열된 애플리케이션 서버의 선택에 엑세스할 수 있다.

[0057] 일부 실시예에서, 인증 서버 (160)는 이러한 강화된 인증 요건을 충족시킬 때 엑세스 될 수 있는 애플리케이션 서버의 제2 선택과 함께 클라이언트 엑세스 리스트에 강화된 인증 요건을 추가할 수 있다. 이러한 강화된 요건은 인증 메커니즘 자체와 관련될 수 있으며, 예를 들어 보다 안전한 인증 메커니즘 (애플리케이션 서버의 제1 선택과 관련됨)을 사용해야 한다고 명시할 수 있다. 예를 들어, 사용자/암호 조합 (애플리케이션 서버의 제1 세트에 대한 인증 요건을 만족할 수 있음)을 제공하는 대신, 강화된 요건은 두개의 인자 인증이 애플리케이션 서버의 제2 세트에 엑세스를 얻는 것이 필요함을 지정할 수 있다. 요건은 클라이언트 자체의 상황 또는 상태 정보와 관련될 수도 있다. 임의의 바람직한 요건은 하기 요건과 같은 것이 사용될 수 있다: 특정 애플리케이션 서버에 엑세스하기 위해 모든 패치가 클라이언트 운영 체제에 적용될 필요가 있음; 바이러스 스캐너가 실행 중이어야 하며 특정 애플리케이션 서버에 엑세스하기 위해 최신 상태여야함; 및/또는 애플리케이션 서버가 공용 무선 네트워크에서 엑세스되지 않을 수 있음.

[0058] 인증 서버와의 인증시에, 인증 서버 (160, 예를 들어, 클라이언트 리스트 엔진 (163)을 통해)는 이러한 강화된 인증을 요구하는 애플리케이션 서버의 제2 선택과 함께 강화된 인증 요건을 포함하는 서명된 클라이언트 엑세스 리스트를 제공한다. 클라이언트가 강화된 인증 요건을 인증하고 충족하면, 인증 서버는 업데이트된 클라이언트 엑세스 리스트를 클라이언트에 발행할 수 있으며, 여기서 클라이언트의 엑세스가 허용된 애플리케이션 서버 중에서 애플리케이t션 서버의 제2 선택이 나열된다. 여러 수준의 강화된 인증 요건(및 해당 애플리케이션 서버 세트)이 클라이언트 엑세스 리스트에 나열될 수 있다.

[0059] 도 5는 강화된 인증 요건을 갖는 애플리케이션 서버로 네트워크 엑세스를 얻기 위해 클라이언트에 의해 실행될 수 있는 예시적인 프로세스를 나타낸다. 이러한 예시적인 프로세스에서, 클라이언트는 제1 클라이언트 엑세스 리스트(여기서는 "베이스 클라이언트 엑세스리스트"라고도 함)에 열거된 사설 네트워크 (140) 내의 애플리케이션 서버의 제1 선택으로 네트워크 엑세스 (501)를 설정한다. 단계 501은 베이스 클라이언트 엑세스 리스트가 애플리케이션 서버의 제2 선택 및 강화된 인증 요건을 포함하여, 이러한 제2 선택에 대한 네트워크 엑세스를 얻을 수 있는 차이를 가지면서 도 2에서 개략적으로 나타낸 순서도에 따라 추가로 구현될 수 있다.

[0060] 클라이언트는 클라이언트 장치에서 실행중인 애플리케이션 및 사설 네트워크 (140)로 이러한 애플리케이션의 네트워크 엑세스를 모니터한다 (502). 클라이언트 애플리케이션이 제1 선택의 일부가 아닌 애플리케이션 서버에 연결을 시도되면 클라이언트는 애플리케이션 서버가 제2 선택의 부분이 아닌지 확인한다 (503). 그렇지 않은 경우, 클라이언트는 이러한 애플리케이션 서버에 엑세스할 수 없으며, 클라이언트 또는 애플리케이션의 사용자에게 거부된 엑세스가 통지될 수 있다 (504). 애플리케이션 서버가 제2 선택의 일부인 경우, 클라이언트는 지문 스캔, 홍채 스캔, 사용자에 대한 추가 생체 정보 (biometric information) 및/또는 외부 키 생성기에 의해 생성된 키와 같은 강화된 인증 증명서를 제공하도록 요청하는 것을 포함하는 인증 서버 (505)로 강화된 인증 프로세서를 시작한다. 또한 클라이언트는 사용자가 클라이언트 장치의 상황 및/또는 상태를 업데이트하도록 요청할 수 있다. 예를 들어, 사용자는 다음과 같이 요청할 수 있다; 클라이언트를 유선 네트워크에 연결하십시요; 공용 무선 네트워크를 통해 클라이언트를 연결하지 마십시오; 클라이언트 운영 체제의 최신 패치를 설치하십시오; 바이러스 스캐너를 설치하십시오; 및/또는 바이러스 스캐너의 데이터베이스를 업데이트 하십시오.

[0061] 사용자가 강화된 인증 요건을 성공적으로 수행하면 (506), 클라이언트는 인증 서버 (160)로부터 제2 또는 업데이트된 클라이언트 엑세스 리스트를 수신한다 (507). 강화된 인증이 성공적이지 않은 경우, 네트워크 엑세스를 요청하는 사용자 또는 소프트웨어 애플리케이션은 네트워크 엑세스가 거부되었음을 신호하거나 경고한다 (504). 업데이트된 클라이언트 엑세스 리스트는 클라이언트가 엑세스할 수 있는 애플리케이션 서버의 제1 선택 및 제2 선택 모두를 열거하고, 그에 따라 방화벽 (102)을 구성하는 게이트웨이 (100)로 전송한다 (508). 그런 다음, 클라이언트는 클라이언트 애플리케이션 및 사용자에게 어떤 애플리케이션 또는 서비스가 허용되는지 신호한다

(509).

[0062] 도 6은 본 발명의 다양한 양태에 따른 예시적인 시스템을 나타낸다. 이러한 예시적인 시스템에서, 게이트웨이 (600)는 킵 얼라이브 모듈 (607)을 포함한다. 게이트웨이 (600)는 설정된 네트워킹 터널 (182)을 통해 클라이언트 (621)와 연결되고, 킵 얼라이브 확인하도록 구성된다. 킵 얼라이브 메시지가 제시간에 수신되지 않으면, 킵 얼라이브 모듈은 방화벽 구성 모듈 (103)에게 방화벽 (102)으로부터 클라이언트 (621)에 대한 방화벽 규칙을 지우도록 명령하고, 터널 모듈 (101)에게 네트워킹 터널 (182)을 끊도록 명령한다. 킵 얼라이브 모듈 (605)은 또한 클라이언트 (621)에 대한 소정의 미리 정의된 상태 또는 상황 정보가 킵 얼라이브 메시지에 존재하는지와 미리 정의된 특정 요건을 충족하는지 여부를 확인하도록 구성될 수 있다. 이러한 요건에는 예를 들어 클라이언트의 바이러스 스캐너 및/또는 방화벽이 활성화되어 있어야 함을 포함할 수 있다.

[0063] 클라이언트 (621)는 게이트웨이 (600)에 킵 얼라이브 메시지를 전송하기 위해 단계 601 내지 604에 의해 예시된 프로세스를 실행할 수 있다. 제1 단계 (601)에서, 게이트웨이 (600)에 대한 네트워킹 터널 (182)이 설정된다. 네트워킹 터널 (182)은 도 2 및 5에 도시된 프로세스 (또는 이의 일부)를 사용하는 것을 포함하여 임의의 원하는 방식으로 설정될 수 있다. 클라이언트는 필요한 상황 및 상태 정보를 수집하고 (602), 그것을 킵 얼라이브 메시지로 포맷한다. 킵 얼라이브 메시지는 네트워킹 터널 (182)을 통해 게이트웨이 (600)의 킵 얼라이브 모듈 (605)로 전송된다 (603). 상기 메시지가 전송되면, 미리 정의된 시간 간격으로부터 카운트 다운하도록 타이머가 활성화된다 (604). 타이머가 만료되면, 단계 602 내지 604의 새로운 사이클이 수행되어 다음의 킵 얼라이브 메시지를 전송한다.

[0064] 도 7은 본 발명의 다양한 양태에 따라 애플리케이션 서버 (741 내지 746)를 비인증 엑세스로부터 보호하기 위한 예시적인 시스템을 도시한다. 이러한 실시예에서, 애플리케이션 서버 (741-746)는 각각 게이트웨이 (700, 701 및 702)에 의해 보호되는 사설 네트워크 (750, 751 및 752)의 일부이다. 클라이언트 (721)는 인증 서버 (760)로 인증하여, 클라이언트 터널 리스트 및 클라이언트 엑세스 리스트를 얻을 수 있다. 클라이언트 터널 리스트는 모든 사설 네트워크 (740-744)를 클라이언트 (721)로 확장하기 위해 각각의 게이트웨이 (700-702)와 네트워킹 터널을 설정하기 위해 필요한 정보를 포함한다. 클라이언트 터널 리스트는 단일의 데이터 객체(date object), 모든 게이트웨이를 식별하는 단일 서명을 갖는 파일, 별도의 서명된 데이터 객체 및/또는 게이트웨이 (700-702) 중 하나를 식별하는 각각의 파일을 포함할 수 있다. 클라이언트 터널 리스트의 수신시, 클라이언트 (721)는 각각의 게이트웨이 (700-702)로 네트워킹 터널 (781, 782, 783)을 설정한다.

[0065] 클라이언트 엑세스 리스트는 클라이언트가 네트워킹 터널 (781, 782 및 783)을 통해 접속할 수 있는 애플리케이션 서버 (741-747)의 선택을 포함한다. 클라이언트 (721)는 수신된 클라이언트 엑세스 리스트에 따라 이들의 방화벽을 차례로 구성하는 게이트웨이에 클라이언트 엑세스 리스트를 전송하고, 이에 의해 클라이언트 (721)가 애플리케이션 서버의 선택에 엑세스할 수 있다.

[0066] 일부 실시예에서, 인증 서버 (760)는 클라이언트 (721)의 인증을 위해 또는 클라이언트 (721)에 대한 정보를 검색하기 위해 다른 서버에 엑세스할 수 있다. 이를 도 7에 도시하고, 여기서 인증 서버 (760)는 인증 서버(760)에 대한 인증 백엔드 역할하는 라디우스 서버 (radius server, 762)를 엑세스할 수 있다. 인증 서버 (760)에서의 인증 모듈 (162)은 서버 (762)가 실제 인증을 수행하는 동안 클라이언트 (721)에 대한 인증 인터페이스로 역할한다. 인증 서버 (760)는 또한 클라이언트 (721)의 사용자에 대한 추가 프로파일 정보를 검색하기 위해 인증 서버 (760)에 능동 디렉토리 서비스를 제공하는 서버 (761)에 접속할 수 있다.

[0067] 도 8은 라디우스 서버 (846) 및 능동 디렉토리 서버 (847)가 게이트웨이 (702) 뒤의 사설 네트워크 (744) 내 애플리케이션 서버에 대응하고, 이에 의해 서버 (846-847)를 인증되지 않은 엑세스로부터 보호하는 것을 돕는, 또 다른 예시적인 시스템을 도시한다. 서버 (846-847)에 엑세스하기 위해, 인증 서버 (760)는 서버 (846 및 847)를 보호하는 게이트웨이 (702)를 갖는 영구 네트워킹 터널 (884)을 포함할 수 있다. 대안으로, 네트워크 터널을 사용하는 대신 표준 HTTPS 트래픽을 활용하기 위해 제이슨(JSON)을 통한 LDAP와 같이, 서버 (846-847)에 대한 엑세스를 제공하는 다른 매커니즘을 사용할 수 있다. 인증 서버 (760)와 서버 (846-847) 사이의 네트워크 연결을 설정하기 위해 필요한 클라이언트 터널 리스트 또는 클라이언트 엑세스 리스트가 필요하지 않도록 미리 인증 서버 (760)가 서버에 엑세스할 수 있게 하는 방화벽 규칙이 게이트웨이 (702)에서 구성될 수 있다.

[0068] 도 9는 복수의 게이트웨이 (900, 901)가 동일한 사설 네트워크 (940) 내에서 애플리케이션 서버 (941-944)를 보호하기 위해 사용되는 실시예를 도시한다. 이러한 토폴로지(topology)는 복수의 게이트웨이 (900, 901) 간의 네트워크 트래픽 로드의 균형을 맞추기 위해 사용될 수 있다. 인증 서버 (960)는 클라이언트 (921 및 922)로 상이한 게이트웨이를 지정하는 클라이언트 터널 리스트를 제공한다. 특히, 클라이언트 (921)는 게이트웨이 (900)와

네트워킹 터널 (981)을 설정하고, 클라이언트 (922)는 게이트웨이 (901)와 네트워킹 터널 (982)을 설정한다.

[0069] 본 명세서의 예시적인 실시예는 애플리케이션 서버를 비인가 엑세스로부터 보호하는 본 발명의 실시예를 도시한다. 애플리케이션 서버와는 별도로, 서비스를 제공하고 네트워크를 통해 어드레싱 가능한 임의의 다른 유형의 네트워크 장치가 본 발명의 실시예에 의해 보호될 수 있다. 마찬가지로, 본 발명의 실시예에 의해 보호될 수 있는 네트워크 장치는 라우터 및 네트워크 레벨 스위치에 관리자 인터페이스를 제공하는 네트워킹 장비를 포함한다.

[0070] 도 10은 본 발명에 개시된 실시예와 관련하여 이용될 수 있는 예시적인 컴퓨터 시스템 (1000)을 도시한다. 컴퓨터 시스템 (1000)은 클라이언트 장치, 게이트웨이, 인증 서버 및/또는 임의의 다른 적합한 시스템으로서 사용될 수 있다. 컴퓨터 시스템 (1000)은 버스 (1010), 프로세서 (1002), 로컬 메모리 (1004), 하나 이상의 선택적 입력 인터페이스 (1014), 하나 이상의 선택적 출력 인터페이스 (1016), 통신 인터페이스 (1012), 저장 요소 인터페이스 (1006) 및 하나 이상의 저장 요소 (1008)를 포함한다.

[0071] 버스 (1010)는 컴퓨터 시스템 (1000)의 컴포넌트간의 통신을 허용하는 하나 이상의 컨덕터(conductor)를 포함할 수 있다. 프로세서 (1002)는 프로그램 명령어를 해석하고 실행하는 임의 유형의 프로세서를 포함할 수 있다. 로컬 메모리 (1004)는 랜덤 엑세스 메모리 (RAM) 또는 프로세서 (1002)에 의한 실행을 위해 정보 및 명령어를 저장하는 다른 유형의 동적 저장 장치 및/또는 읽기용 메모리 (ROM) 또는 프로세서 (1002)에 의한 사용을 위한 정적 정보(static information) 및 명령어를 저장하는 다른 유형의 정적 저장 장치를 포함할 수 있다. 입력 인터페이스 (1014)는 키보드 (1020), 마우스 (1030), 펜, 음성 인식 및/또는 생체 인식 매커니즘 등과 같은, 정보를 오퍼레이터(operator)가 컴퓨터 장치 (1000)로 정보를 입력할 수 있는 하나 이상의 종래 메커니즘을 포함할 수 있다.

[0072] 출력 인터페이스 (1016)는 디스플레이 (1040), 프린터 (1050), 스피커 등과 같은 정보를 오퍼레이트에게 출력하는 하나 이상의 종래 메커니즘을 포함할 수 있다. 통신 인터페이스 (1012)는 예를 들어 컴퓨팅 시스템 (1000)이 다른 장치 및/또는 시스템 (1100)과 통신할 수 있게 하는 하나 이상의 이더넷(Ethernet) 인터페이스인 임의의 트랜스시버형 매커니즘을 포함할 수 있다. 컴퓨터 시스템 (1000)의 통신 인터페이스 (1012)는 근거리 통신망 (LAN) 또는 예를 들어 인터넷과 같은 광역 통신망 (WAN)에 의해 다른 컴퓨터 시스템에 연결될 수 있다. 저장 요소 인터페이스 (1006)는 버스 (1010)를 예를 들어 SATA 디스크 드라이브인 하나 이상의 로컬 디스크와 같은 하나 이상의 저장 요소 (1008)에 연결하기 위한 예를 들어 시리얼 고급 기술 부착(SATA) 인터페이스 또는 소형 컴퓨터 시스템 인터페이스(SCSI)를 포함할 수 있고, 이러한 저장 요소 (1008)에서 및/또는 이러한 저장 요소로부터 데이터를 읽고 쓰는 것을 제어할 수 있다. 상기 저장 요소 (1008)가 로컬 디스크로 기술되었지만, 일반적으로 제거 가능한 자기 디스크, CD 또는 DVD와 같은 광학 저장 매체, ROM 디스크, 고체 상태 드라이브, 플래시 메모리 카드와 같은 일반적으로 임의의 다른 적합한 컴퓨터-판독가능 매체가 사용될 수 있다. 상기에서 전술한 시스템 (1000)은 또한 물리적 하드웨어 위에 가상 머신으로서 실행될 수 있다.

[0073] 본 명세서에 도시된 방법은 이의 프로세서 (1002)에 의한 실행을 위해 컴퓨터 시스템 (1000)의 로컬 메모리 (1004)에 저장된 프로그램 명령어를 통해 구현될 수 있다. 대안으로, 명령어는 저장 요소 (1008)에 저장되거나 통신 인터페이스 (1012)를 통해 다른 컴퓨터 시스템으로부터 엑세스 가능할 수 있다.

[0074] 시스템 (1000)은 도 1, 도 6, 도 7, 도 8 및 도 9 각각에 의해 예시된 실시예의 클라이언트 (121, 122, 621, 721, 921, 922)에 해당할 수 있다. 이러한 경우, 시스템 (1000)은 통신 인터페이스 (1012)에 의해 게이트웨이 및 인증 서버로 연결될 수 있다. 도 2, 도 5 및 도 6에 도시된 방법의 단계는 실행 중에 프로세서 (1002)에서의 명령어로서 수행될 수 있고, 메모리 스토리지 (storage, 1004 또는 1008)에 저장된다.

[0075] 시스템 (1000)은 도 1, 도 6, 도 7, 도 8 및 도 9에 각각 도시된 실시예의 게이트웨이 (100, 600, 700, 701, 702, 900 및 901)에 해당할 수 있다. 이러한 경우, 시스템은 2개의 통신 인터페이스 (1012), 사설 네트워크에 연결하기 위한 하나의 통신 인터페이스 및 클라이언트로 연결하는 다른 네트워크에 연결하기 위한 하나의 인터페이스를 포함할 수 있다. 도 4에 도시된 방법의 단계들은 실행 동안 프로세서 (1002)에서의 명령어로서 수행될 수 있고, 메모리 스토리지 (1004 또는 1008)에 저장될 수 있다.

[0076] 시스템 (1000)은 도 1, 도 6, 도 7, 도 8 및 도 9에 도시된 실시예의 인증 서버 (160, 760 및 960)에 해당할 수 있다. 이러한 경우, 통신 인터페이스 (1012)는 시스템 (1000)을 클라이언트 및 게이트웨이로 연결하는데 사용될 수 있다. 도 3에 도시된 방법의 단계들은 실행 중에 프로세서 (1002)에서의 명령어로서 수행될 수 있고, 메모리 스토리지 (1004 또는 1008)에 저장될 수 있다.

[0077] 인증 서버 및 게이트웨이에 의해 수행되는 방법은 동일한 컴퓨터 시스템, 별도의 컴퓨터 시스템 또는 동일하거나 상이한 물리적 컴퓨터 시스템에서의 별도의 가상 컴퓨터 시스템에서 추가로 실행될 수 있다.

[0078] 다중-터널링 가상 네트워크 어댑터

[0079] 클라이언트의 운영 체제 내에서, 가상 어댑터는 하드웨어, 소프트웨어 또는 이들의 조합으로 구현되는지 여부에 관계없이 다른 네트워크 어댑터 또는 네트워크 인터페이스와 함께 작동하는 소프트웨어-구현 컴포넌트이다. 데이터 패킷이 가상 어댑터로 전송하기 위해 소프트웨어 프로그램(운영 체제 내에서 실행됨)에 의해 전송되는 경우 패킷은 물리적 통신 인터페이스를 통해 전송되지 않는다. 대신, 패킷은 가상 어댑터와 운영 시스템의 모든 작업이 실행되는 커널-영역과 달리 운영 시스템의 사용자-영역 부분에서 실행되는 전용 소프트웨어 애플리케이션으로 재라우트(reroute)된다. 가상 어댑터로부터 이러한 패킷을 수신하는 것 외에도, 전용 소프트웨어 애플리케이션은 패킷을 가상 어댑터에 전달하여 다른 방향으로 통신을 수행한다. 이러한 경우에서 가상 어댑터는 이러한 패킷을 운영-시스템 네트워크 스택(stack)에 전달(또는 "주입")하여 외부 소스로부터 이의 수신을 대리 실행(emulate)한다. 가상 네트워크 어댑터는 두 가지 기존 유형의 이름으로 명명되는 TUN/TAP 인터페이스를 의미한다. TUN 인터페이스 (즉 네트워크 터널)는 네트워크 계층 장치를 시뮬레이트하고, IP 패킷과 같은 계층 3 패킷으로 작동한다. TAP 인터페이스 (즉, 네트워크 탭)는 링크 계층 장치를 시뮬레이트하고, 이더넷 프레임과 같은 계층 2 패킷으로 작동한다.

[0080] 가상 네트워크 인터페이스 컨트롤러 (NIC)는 커널 영역에 존재하는 TUN/TAP 장치이다. NIC는 IP 패킷과 프로토콜 헤더 (TUN의 경우) 또는 이더넷 헤더 (TAP의 경우)를 포함하는 데이터의 가상 인터페이스 패킷을 전달하므로, 데이터 패킷을 사용자 영역에서 완전한 패키지로 처리할 수 있다. 따라서 NIC는 트래픽을 새로운 패킷으로 캡슐화하여 일반적으로 가상 사설 네트워크에서 사용되는 원격 목적지로 터널링할 수 있다. 다중 터널을 설정하려면 각각의 터널마다 하나씩 다중 TUN/TAP 인터페이스가 필요하다.

[0081] 종래의 시스템에서, 필요한 터널의 양이 미리 알려지지 않은 경우 (일반적으로 그렇지 않음), 새로운 터널을 설정하는 것은 운영 체제에 대한 관리 권한이 필요하여, 운영 시스템의 커널 영역에 가상 TUN/TAP 장치를 추가로 만들어야 한다. 또한, 각각의 가상 연결마다 별도의 가상 TUN/TAP 장치를 만들어야 한다.

[0082] 종래의 시스템의 실시예가 도 11에 도시되어있다. 이러한 실시예에서, 2개의 가상 네트워크 어댑터가 커널-영역(VIRT NIC 1 및 VIRT NIC 2)에 설치된다. 제1 사용자-영역 애플리케이션(APPLICATION 1)은 제1 VPN에서 네트워크 목적지로 데이터 패킷(DATA 1)을 보낸다. 운영 체제(OS)의 TCP/IP 스택에서, 패킷은 제1 VPN(TCP/IP 1)에서로의 목적지 어드레스로 추가된다. 그런 다음, 운영 체제는 제1 VPN, 즉 VIRT NIC 1로 어드레스가 지정된 패킷을 처리해야하는 네트워크 어댑터로 패킷을 라우팅한다. 이는 가상 어댑터이므로, 패킷이 암호화되고(DATA 1' 및 TCP/IP 1') VPN 터널의 다른 말단에서 VPN 서버를 어드레스하는 목적지로서 OS(TCP/IP 11)에 의해 새로운 패킷으로 삽입되는 제1 VPN 애플리케이션으로 재라우트된다. 그 후 OS는 이러한 패킷을 물리적 네트워크 인터페이스 NIC 1로 라우트한다.

[0083] 제2 애플리케이션(APPLICATION 2)이 제2 VPN에서의 목적지로 데이터 패킷(DATA 2)을 보내는 경우 유사한 흐름이 발생한다. 그런 다음, 이러한 패킷은 제2 VPN 애플리케이션(VPN 클라이언트 2)으로 전달되는 제2 가상 인터페이스(VIRT NIC 2)로 라우트된다. 그 후 이러한 제2 VPN 애플리케이션은 패킷을 암호화하고, 제2 VPN 서버(TCP/IP 21)로 이를 보낸다.

[0084] 도 11에서의 기존 시스템에는 적어도 두 가지 중요한 문제가 있다. 가상 어댑터를 만들기 위해, 어댑터가 커널 영역에 존재하기 때문에 관리 권한이 필요하다. 두번째, 모든 VPN 연결을 만들려면 새로운 가상 어댑터를 만들어야 한다. 본 발명의 다양한 양태에 따른 예시적인 시스템을 도 12에 도시한다. 도 12에서의 시스템은 도 11에서의 두 가지 문제를 해결하는데, 이는 VPN을 설정하는 사용자-영역 애플리케이션에 라우팅 컴포넌트를 추가하여 서로 다른 VPN을 하나의 가상 어댑터로 만드는 것이 가능하기(그리고 운영 체제의 커넬 영역으로 관리 권한이 필요 없음) 때문이다.

[0085] 도 12에 나타낸 예시적인 시스템 (1200)에서, DATA 1 및 DATA 2는 운영 체제에 의해 동일한 가상 어댑터 (1230)로 라우팅된다. 이는 동일한 가상 어댑터(VIRT NIC 1, 1230)로 두개의 VPN (1251 및 1252)의 네트워크 트래픽을 연결하기 위해 운영 시스템(OS) 라우팅 테이블을 업데이트함으로써 이루어진다. VPN 클라이언트 1 (1210)은 데이터를 암호화하고 새로운 패킷에 이를 삽입할 뿐만 아니라, VPN 라우팅 테이블 (1260)을 사용하여 어느 VPN으로 패킷이 운행되는지를 결정한다. 라우팅 테이블 (1260)을 사용하여, VPN 1 (1251)에 대한 패킷은 VPN 1 암호화 모듈로 보내지고, VPN 2 (1252)에 대한 패킷은 VPN 2 암호화 모듈로 전송된다. VPN 1 및 2에 대한 패킷

은 다른 목적지, 즉 터널의 말단인 다른 VPN 서버로 보내진다.

[0086] 도 13은 본 발명의 다양한 양태에 따른 다중 터널링 가상 어댑터를 이용하는 시스템의 또 다른 실시예를 도시한다. 이러한 실시예에서, 두개의 서로 다른 네트워크 192.168.0.0/24 (1310) 및 10.0.0.0/24 (1320)이 있다. 모든 네트워크는 TUN/TAP 인터페이스인 tun0 인터페이스 (1330)를 향해 라우팅된다. 패킷이 tun0 인터페이스 (1330)를 향해 라우트되는 경우, CZ VPN 클라이언트 (1340)는 전체 패킷을 읽을 수 있다.

[0087] 기존의 VPN 클라이언트에서, 패킷은 즉시 캡쳐되고(가능한 암호화됨) eth0의 소스 IP와 패킷을 분석하는 원하는 게이트웨이의 목적지 IP를 포함하는 TCP 또는 UDP 연결로 캡슐화된다. 대조적으로, 도 13에서의 시스템은 원본 패킷의 목적지 IP 어드레스를 식별하고 어떤 터널 (및 해당 암호화)을 사용해야하는지 식별하는 라우팅 모듈을 구현한다. 도 13에 나타낸 실시예에서, 192.168.0.0/24 네트워크 내의 목적지 IP를 갖는 패킷은 게이트웨이 A (1350)의 암호화기/캡슐화기로 보내지는 반면, 10.0.0.0/24 경로와 일치할 패킷은 게이트웨이 B (1360)로 암호화되고 캡슐화된다.

[0088] 일단 패킷이 CZ VPN 클라이언트 (1340)에 의해 픽업되면, 대응하는 게이트웨이로 새로운 연결 (TCP 또는 UDP 일 수 있음)을 만들 것이고, TUN/TAP으로부터 수신된 원본 패킷의 암호화된 버전을 포함할 것이다. 이 패킷은 해당 게이트웨이에 도달하기 위해 다시 정상적인 OS 라우팅 테이블에 의해 처리될 것이다.

[0089] 라우팅 컴포넌트는 운영 체제의 사용자 영역 부분에 존재하기 때문에 관리 권한 없이도 더 많거나 적은 터널을 동적으로 추가할 수 있다. 도 13에서의 시스템의 또 다른 이점은 서로 다른 터널에 대해 동일한 클라이언트 IP를 사용하므로, 하나의 가상 인터페이스가 모든 사설 트래픽을 처리할 수 있다는 것이다. 따라서 하나의 가상 어댑터는 각각의 게이트웨이에 대한 단일 어댑터가 필요한 기존 시스템과 달리 많은 가상 게이트웨이를 서비스할 수 있다. 따라서, 본 발명의 실시예들은 각각의 클라이언트의 커널 영역에 엑세스하기 위한 관리 권한을 필요로 하지 않으며, 이는 종래의 시스템, 특히 다수의 개별 클라이언트를 갖는 종래 시스템에 큰 문제가 될 수 있다. 또한 많은 모바일 장치 운영 체제는 하나의 가상 어댑터만 지원한다. 본 발명의 실시예들은 트래픽을 부하 균형(loadbalance)되게 하거나, 하나의 가상 어댑터를 사용하여 동일한 사설 네트워크를 보호하는 둘 이상의 독립된 게이트웨이로 과잉의 터널을 만드는데 사용될 수 있다.

[0090] 도 14는 본 발명의 다양한 양태에 따른 예시적인 프로세스를 도시한다. 프로세스 (1400)는 도 13에 나타낸 시스템뿐만 아니라 본 발명에 기술된 것을 포함하여 임의의 다른 방법과 함께(전체적으로 또는 부분적으로) 임의의 원하는 시스템과 결합하여 구현될 수 있다.

[0091] 이러한 실시예에서, 프로세스 (1400)는 가상 사설 네트워크 (VPN) 클라이언트 (1410)의 라우팅 컴포넌트에 의해 네트워크를 통한 하나 이상의 데이터 패킷을 수신하는 단계, 하나 이상의 데이터 패킷에 대한 목적지를 라우팅 컴포넌트로 식별하는 단계 (1420), 하나 이상의 데이터 패킷에 대한 목적지에 대응하는 하나 이상의 연결을 VPN 클라이언트로 생성하는 단계, 하나 이상의 데이터 패킷을 각각의 목적지에 전송하는 단계, 하나 이상의 게이트웨이 연결을 제거하는 단계 (1450)를 포함한다.

[0092] 상술한 바와 같이, 많은 데이터 패킷이 본 발명의 실시예에 의해 수신되고 전송될 수 있다. 다양한 실시예에서, 하나 이상의 데이터 패킷은 VPN 클라이언트를 실행하는 운영 체제의 커널 영역 부분에서 작동하는 가상 어댑터를 통해 수신될 수있다 (1410). 또한, 데이터 패킷에 대한 목적지를 식별하는 단계 (1420)는 데이터 패킷에 대한 목적지에 대응하는 게이트웨이를 식별하는 단계를 포함할 수 있고, 게이트웨이에 대한 연결을 생성하는 단계 (1430)는 사용자 데이터그램 프로토콜(UDP) 연결을 생성하는 단계를 포함할 수 있다. 게이트웨이 연결은 임의의 적절한 방식으로 제거될 수 있다 (1450). 게이트웨이 연결의 제거는 예를 들어, 연결 숨기기, 연결의 추가 사용 방지, 연결 해제 등을 포함할 수 있다. 일부 실시예에서, 예를 들어, 일단 VPN이 설정되면, 게이트웨이 연결은 클라이언트가 연결이 끊어지거나 시스템이 연결이 더 이상 유효하지 않다고 결정할 때까지(해지된 엑세스, 만료된 연결 등) 유지된다.

[0093] 복수의 데이터 패킷이 처리되는 경우에, 데이터 패킷은 운영 체제의 커널 영역에서 작동하는 하나의 가상 어댑터를 통해 라우트될 수 있다. 라우팅 컴포넌트는 임의의 크기, 유형 및 구성일 수 있으며, 예를 들어 라우팅 테이블을 포함할 수 있다. 라우팅 테이블은 차례로 하나 이상의 데이터 패킷에 대한 하나 이상의 목적지 어드레스를 포함하는, 하나 이상의 데이터 패킷을 처리하기 위한 임의의 적합한 정보를 포함할 수 있다.

[0094] 본 발명의 실시예와 관련하여 작동하는 시스템, 장치 및 컴포넌트 간의 통신은 예를 들어 전화 네트워크, 엑스트라넷(extranet), 인트라넷, 인터넷, 포인트 오브 인터액션 장치(포인트 오브 세일 장치, 개인 정보 단말기(예를 들어, 아이폰, 팜 파일럿, 블랙 베리, 휴대 전화, 키오스크(kiosk) 등), 온라인 통신, 위성 통신, 오프-라인

통신, 무선 통신, 트랜스 폰더 통신, 근거리 통신망(LAN), 원거리 통신망(WAN), 가상 사설 네트워크(VPN), 네트워크 또는 링크된 장치, 키보드, 마우스 및/또는 임의의 적절한 통신 또는 데이터 입력 방식을 포함할 수 있다. 본 발명의 시스템 및 장치는 TCP/IP 통신 프로토콜뿐 아니라. IPX, 애플토크(Appletalk), IP-6, NetBIOS, OSI, 임의의 터널링 프로토콜(예를 들어, IPsec, SSH) 또는 많은 기존 또는 향후 프로토콜을 사용할 수 있다.

[0095] 일부 실시예가 완전히 작동하는 컴퓨터 및 컴퓨터 시스템에서 구현될 수 있으며, 다양한 실시예는 다양한 형태의 컴퓨터 제품으로 분배될 수 있으며, 분배에 실질적으로 영향을 미치는데 사용되는 특정 유형의 기계 또는 컴퓨터-판독가능 매체에 상관없이 적용될 수 있다.

[0096] 기계 판독 가능 매체는 데이터 처리 시스템에 의해 실행되는 경우 시스템으로 하여금 다양한 방법을 수행하게 하는 소프트웨어 및 데이터를 저장하는데 사용될 수 있다. 실행 가능한 소프트웨어 및 데이터는 예를 들어 ROM, 휘발성 RAM, 비 휘발성 메모리 및/또는 캐시를 포함하는 다양한 장소에 저장될 수 있다. 이러한 소프트웨어 및/또는 데이터의 일부는 이러한 저장 장치 중 하나에 저장될 수 있다. 또한, 데이터 및 명령어는 중앙식 서버 또는 피어 투 피어(peer to peer) 네트워크로부터 얻을 수 있다. 데이터 및 명령어의 서로 다른 부분은 상이한 시간 및 상이한 통신 세션 또는 동일한 통신 세션에서의 상이한 중앙식 서버 및/또는 피어 투 피어 네트워크로부터 얻을 수 있다. 데이터 및 명령어는 애플리케이션의 실행 전에 전체적으로 얻을 수 있다. 대안으로, 데이터 및 명령어의 일부는 실행이 필요할 때, 시간상 동적으로 얻어질 수 있다. 따라서, 데이터 및 명령어가 시간의 특정 인스턴스에서 전체적으로 머신 판독 가능 매체에 존재할 필요는 없다.

[0097] 컴퓨터 판독 가능 매체의 예는 특히 휘발성 및 비-휘발성 메모리 장치, 읽기용 메모리(ROM), 랜덤 엑세스 메모리(RAM), 플래시 메모리 장치, 플로피 및 다른 제거가능한 디스크, 자기 디스크 저장 매체, 광학 저장 매체(예를 들어, CD ROM (Compact Disk Read-Only Memory), 디지털 다목적 디스크(DVD) 등)와 같은 판독 가능 및 비-판독 가능 유형 매체를 포함하고, 이에 제한되는 것은 아니다. 컴퓨터-판독 가능 매체는 명령어를 저장할 수 있다.

[0098] 다양한 실시예들에서, 배선 회로는 기술들을 구현하기 위해 소프트웨어 명령어와 조합하여 사용될 수 있다. 따라서, 이러한 기술은 하드웨어 회로 및 소프트웨어의 임의의 특정 조합이나 데이터 처리 시스템에 의해 실행되는 명령어에 대한 특정 소스에 제한되지 않는다.

[0099] 일부 도면은 특정 순서로 복수의 작동을 도시하지만, 순서에 의존하지 않는 작동은 재정렬될 수 있고, 다른 작동은 결합되거나 분리될 수 있다. 일부 재정렬 또는 다른 그룹화가 구체적으로 언급되지만, 다른 것들은 당업자에게 명백할 것이므로, 대안의 완전한 리스트를 제공하지는 않는다. 또한, 단계는 하드웨어, 펌웨어, 소프트웨어 또는 이들의 임의의 조합으로 구현될 수 있는 것으로 인지되어야 한다.

[0100] 간결함을 위해, 종래의 데이터 네트워킹, 애플리케이션 개발 및 시스템의 다른 기능적 측면(및 시스템의 개별 작동 컴포넌트의 컴포넌트)은 본 명세서에서 상세히 기술되지 않을 수 있다. 또한, 본 명세서에 포함된 다양한 도면에 도시된 연결 라인은 다양한 요소들 간의 예시적인 기능적 관계 및/또는 물리적 결합을 나타내기 위한 것이다. 실용적인 시스템에는 많은 대체 또는 추가 기능적 관계 또는 물리적 연결이 있을 수 있다.

[0101] 본 명세서에서 논의된 다양한 시스템 컴포넌트는 다음 중 하나 이상을 포함 할 수 있다: 디지털 데이터를 처리하기 위한 프로세서를 포함하는 호스트 서버 또는 다른 컴퓨터 시스템; 디지털 데이터를 저장하기 위해 상기 프로세서에 연결된 메모리; 디지털 데이터를 입력하기 위해 상기 프로세서에 연결된 입력 디지타이저(digitizer); 상기 프로세서에 의해 디지털 데이터의 처리를 지시하기 위해 상기 메모리에 저장되고 상기 프로세서에 의해 엑세스 가능한 애플리케이션 프로그램; 상기 프로세서에 의해 처리된 디지털 데이터로부터 도출된 정보를 표시하기 위해 상기 프로세서 및 메모리에 연결된 디스플레이 장치; 및 복수의 데이터베이스. 본 발명에서 사용된 다양한 데이터베이스는 시핑 데이터(shipping data), 패키지 데이터 및/또는 시스템의 작동에 유용한 임의의 데이터를 포함할 수 있다.

[0102] 다양한 기능이 웹 브라우저 및/또는 웹 브라우저를 이용한 애플리케이션 인터페이싱을 통해 수행될 수 있다. 이러한 브라우저 애플리케이션은 다양한 기능을 수행하기 위해 컴퓨터 장치 또는 시스템 내에 설치된 인터넷 브라우징 소프트웨어를 포함할 수 있다. 이러한 컴퓨팅 장치 또는 시스템은 컴퓨터 또는 한 세트의 컴퓨터의 형태를 취할 수 있으며, 랩톱, 노트북, 태블릿, 핸드 헬드 컴퓨터, 개인 정보 단말기, 셋-톱 박스, 워크 스테이션, 컴퓨터-서버, 메인 프레임 컴퓨터, 미니-컴퓨터, PC 서버, 컴퓨터의 네트워트 세트, iPads, iMAC 및 MacBook과 같은 개인용 컴퓨터 및 태블릿 컴퓨터, 키오스크, 단말기, 포인트 오브 세일(POS) 장치 및 / 또는 터미널, 텔레비전, 또는 네트워크를 통해 데이터를 수신할 수 있는 임의의 다른 장치를 포함하여 사용될 수 있다. 다양한 실시

예는 마이크로소프트 인터넷 익스플로러(Microsoft Internet Explorer), 모질라 파이어폭스(Mozilla Firefox), 구글 크롬(Google Chrome), 애플 사파리(Apple Safari), 또는 인터넷을 브라우징하기 위해 이용가능한 무수한 소프트웨어 패키지 중 임의의 다른 하나를 사용할 수 있다.

[0103] 다양한 실시예는 임의의 적합한 운영 체제(예를 들어, Windows NT, 95/98/2000/CE/Mobile/Windows 7/8, OS2, UNIX, Linux, Solaris, MacOS, PalmOS 등)뿐 아니라, 일반적으로 컴퓨터와 관련된 다양한 종래 지원 소프트웨어 및 드라이버와 결합하여 작동될 수 있다. 다양한 실시예는 임의의 적합한 개인용 컴퓨터, 네트워크 컴퓨터, 워크 스테이션, 개인 정보 단말기, 셀룰러 폰, 스마트 폰, 미니 컴퓨터, 메인 프레임 등을 포함할 수 있다. 실시예들은 보안 소켓 계층(SSL), 전송 계층 보안(TLS) 및 보안 쉘(SSH)과 같은 보안 프로토콜을 구현할 수 있다. 실시예들은 http, https, ftp 및 sftp를 포함하는 원하는 애플리케이션 계층 프로토콜을 구현할 수 있다.

[0104] 다양한 시스템 컴포넌트는 예를 들어 표준 모뎀 통신(standard modem communication), 케이블 모뎀, 위성 네트워크(satellite network), ISDN, 디지털 가입자 라인(Digital Subscriber Line: DSL) 또는 다양한 무선 통신 방법과 관련하여 사용되는 로컬 루프(local loop)를 통한 인터넷 서비스 제공자(ISP)로의 연결을 포함하는 데이터 링크를 통해 네트워크에 독립적으로, 개별적으로 또는 집합적으로 적절히 결합될 수 있다. 본 발명의 실시예들은 상호작용 텔레비전(ITV) 네트워크와 같은 임의의 적합한 유형의 네트워크와 함께 작동할 수 있다.

[0105] 시스템은 클라우드 컴퓨팅을 사용하여 부분적으로 또는 완전히 구현될 수 있다. "클라우드(Cloud)" 또는 "클라우드 컴퓨팅(Cloud computing)"은 최소 관리 노력 또는 서비스 제공자 상호작용으로 급격하게 제공되고 릴리스될 수 있는 구성가능한 컴퓨팅 자원(예를 들어, 네트워크, 서버, 스토리지, 애플리케이션 및 서비스)의 공유 풀에 대한 편리한, 온-디맨드 네트워크 엑세스(on-demand network access)를 가능하게 하기 위한 모델을 포함한다. 클라우드 컴퓨팅은 위치-독립적 컴퓨팅(location-independent computing)을 포함할 수 있고, 여기서 공유 서버는 수요에 따라 컴퓨터 및 다른 디바이스에 자원, 소프트웨어 및 데이터를 제공한다.

[0106] 다양한 실시예가 웹 서비스(web service), 유틸리티 컴퓨팅(utility computing), 편재형 및 개별화 컴퓨팅(pervasive and individualized computing), 보안 및 아이덴티티 솔루션(security and identity solution), 자율성 컴퓨팅(autonomic computing), 클라우드 컴퓨팅(cloud computing), 상품 컴퓨팅(commodity computing), 이동성 및 무선 솔루션(mobility and wireless solution), 오픈 소스(open source), 생체인식, 그리드 컴퓨팅(grid computing) 및/또는 메시 컴퓨팅(mesh computing)과 함께 사용될 수 있다.

[0107] 여기에 설명된 데이터베이스는 관계형, 계층형, 그래픽 또는 객체-지향 구조 및/또는 기타 데이터베이스 구성을 포함할 수 있다. 또한, 데이터베이스는 임의의 적절한 방법, 예를 들어 데이터 테이블 또는 룩업(lookup) 테이블로 구성될 수 있다. 각각의 기록은 단일 파일, 일련의 파일, 연결된 일련의 데이터 필드 또는 기타 데이터 구조가 될 수 있다. 특정 데이터의 연관성은 당업계에 공지되거나 실행된 것과 같은 임의의 바람직한 데이터 연관 기술을 통해 달성될 수 있다. 예를 들어, 수동 또는 자동으로 연결을 수행할 수 있다.

[0108] 시스템의 임의의 데이터베이스, 시스템, 장치, 서버 또는 다른 컴포넌트는 단일 위치 또는 다중 위치에 위치할 수 있으며, 각각의 데이터베이스 또는 시스템은 방화벽, 엑세스 코드, 암호화, 복호화, 압축, 압축 해제 등을 포함할 수 있다.

[0109] 암호화는 당업계에서 현재 이용 가능하거나 이용하게 될 임의의 기술, 예를 들어 투피쉬(Twofish), RSA, El Gamal, Schorr 서명, DSA, PGP, PKI 및 대칭 및 비대칭 암호시스템(cryptosystem)의 방법으로 수행될 수 있다.

[0110] 실시예는 표준 전화 접속, 케이블, DSL 또는 당업계에 공지된 임의의 다른 인터넷 프로토콜을 사용하여 인터넷 또는 인트라넷에 접속할 수 있다. 트랜잭션(transaction)은 다른 네트워크의 사용자가 무단으로 엑세스하지 못하도록 방화벽을 통과하여 전달될 수 있다.

[0111] 본 발명에서 설명된 컴퓨터는 사용자에 의해 엑세스할 수 있는 적합한 웹사이트 또는 다른 인터넷-기반의 그래픽 사용자 인터페이스를 제공할 수 있다. 예를 들어, 마이크로소프트 인터넷 정보 서버(IIS), 마이크로소프트 트랜잭션 서버(MTS) 및 마이크로소프트 SQL 서버는 마이크로소프트 운영 체제, 마이크로소프트 NT 웹 서버 소프트웨어, 마이크로소프트 SQL 서버 데이터베이스 시스템 및 마이크로소프트 상업 서버(MCS)와 함께 사용될 수 있다. 또한 Access 또는 Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase 등과 같은 컴포넌트를 사용하여 활성 데이터 객체(ADO) 호환 데이터베이스 관리 시스템을 제공할 수 있다. 또 다른 실시예에서, Apache 웹 서버는 Linux 운영 시스템, MySQL 데이터베이스 및 Perl, PHP 및 / 또는 Python 프로그래밍 언어와 함께 사용할 수 있다.

[0112] 여기에 설명된 통신, 입력, 저장, 데이터베이스 또는 디스플레이 중 임의는 웹 페이지가 있는 웹 사이트를 통해

쉽게 이용할 수 있다. 여기에서 사용된 바와 같이 용어 "웹 페이지(web page)"는 사용자와 상호작용하는 데 사용될 수 있는 문서 및 애플리케이션의 유형을 제한하는 것이 아니다. 예를 들어 일반적인 웹사이트는 표준 HTML 문서에 추가하여 다양한 형태, 자바 애플릿, 자바스크립트(JavaScript), 활성 서버 페이지(ASP), 공통 게이트웨이 인터페이스 스크립트(common gateway interface script: CGI), 확장가능 마크업 언어(extensible markup language: XML), 동적 HTML, 캐스캐이딩 스타일 시트(cascading style sheet: CSS), AJAX(Asynchronous Javascript And XML), 헬퍼 애플리케이션(helper application), 플러그-인(plug-in) 등을 포함할 수 있다. 서버는 URL 및 IP 어드레스를 포함하는 요청을 웹 서버로부터 수신하는 웹 서비스를 포함할 수 있다. 웹 서버는 적절한 웹 페이지를 검색하고, 웹 페이지에 대한 데이터 또는 애플리케이션을 IP 어드레스로 보낸다. 웹 서비스는 인터넷과 같은 통신 수단을 통해 다른 애플리케이션과 상호 작용할 수 있는 애플리케이션이다.

[0113] 다양한 실시예는 브라우저-기반 문서 내에 데이터를 표시하기 위한 임의의 바람직한 수의 방법을 사용할 수 있다. 예를 들어, 데이터는 표준 텍스트 또는 고정 리스트, 스크롤 리스트, 드롭-다운 리스트, 편집 가능한 텍스트 필드, 고정된 텍스트 필드, 팝업 윈도우 등 내에서 표현될 수 있다. 동일하게, 실시예는 예를 들어 키보드를 사용하는 프리 텍스트 엔트리, 메뉴 항목의 선택, 체크 박스, 옵션 박스 등과 같은 웹 페이지에서 데이터를 수정하기 위한 바람직한 많은 방법을 이용할 수 있다.

[0114] 본 발명에서 기술된 예시적인 시스템 및 방법은 기능적인 블록 컴포넌트, 스크린 샷, 선택적 선택 및 다양한 처리 단계의 관점에서 설명될 수 있다. 이러한 기능적인 블록은 특정 기능을 수행하도록 구성된 복수의 하드웨어 및/또는 소프트웨어 컴포넌트에 의해 실현될 수 있는 것으로 이해되어야한다. 예를 들어, 시스템은 하나 이상의 마이크로 프로세서 또는 다른 제어 장치하에서 다양한 기능을 수행할 수 있는 메모리 요소, 처리 요소, 논리 요소, 룩-업 테이블 등과 같은 다양한 집적 회로 컴포넌트를 사용할 수 있다. 유사하게, 시스템의 소프트웨어 요소는 C, C ++, C#, 자바, 자바스트립트, VBS스크립트, 매크로매체 콜드퓨전(Macromedia ColdFusion), 코볼(COBOL), 마이크로소프트 활성 서버 페이지(Microsoft Active Server Pages), 어셈블리, PERL, PHP, AWK, 파이썬(Python), 비주얼 베이직(Visual Basic), SQL 저장된 프로시져, PL/SQL, 임의의 유닉스 쉘 스크립트 및 데이터 구조, 객체, 프로세서, 루틴 또는 다른 프로그래밍 요소의 임의의 조합으로 구현되는 다양한 알고리즘을 갖는 확장성 생성 언어(XML)와 같은 임의의 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 또한, 시스템은 자바 스크립트, VB스크립트 등과 같은 클라이언트-측 스크립팅 언어로 보안 문제를 탐지하거나 방지하는데 사용될 수 있다.

[0115] 본 발명의 시스템 및 방법은 기존 시스템, 애드-온 제품(add-on product), 업그레이드된 소프트웨어를 실행하는 처리 장치, 독립형 시스템, 분산형 시스템, 방법, 데이터 처리 시스템, 데이터 처리 장치 및/또는 컴퓨터 프로그램 제품의 맞춤화(customization)로 구현될 수 있다. 따라서, 시스템 또는 모듈의 임의의 부분은 코드를 실행하는 처리 장치, 인터넷 기반 합체, 전체 하드웨어 합체, 또는 인터넷, 소프트웨어 및 하드웨어의 양태가 조합된 합체의 형태를 취할 수 있다. 또한, 시스템은 저장 매체에 구현된 컴퓨터-판독 가능 프로그램 코드 수단을 갖는 컴퓨터-판독 가능 저장 매체에 컴퓨터 프로그램 제품의 형태를 취할 수 있다. 하드 디스크, CD-ROM, 광학 저장 장치, 자기 저장 장치 등을 포함하는 임의의 적합한 컴퓨터-판독 가능 저장 매체가 이용될 수 있다

[0116] 본 발명에서 기술된 시스템 및 방법은 다양한 실시예에 따른 방법, 장치(예를 들어, 시스템) 및 컴퓨터 프로그램 제품의 스크린 샷, 블록도 및 흐름도를 참조하여 설명된다. 블록도 및 흐름도의 각각의 기능적 블록 및 블록도 및 흐름도에서의 기능적 블록의 조합은 각각 컴퓨터 프로그램 명령어에 의해 구현될 수 있는 것으로 이해될 것이다.

[0117] 이들 컴퓨터 프로그램 명령어는 범용 컴퓨터, 특수 목적 컴퓨터 또는 다른 프로그램 가능한 데이터 처리 장치에서 로딩될 수 있어, 컴퓨터 또는 다른 프로그램 가능한 데이터 처리 장치에서 실행되는 명령어는 흐름도 블록 또는 블록에서 지정되는 기능을 구현하기 위한 수단을 생성한다. 이들 컴퓨터 프로그램 명령어는 컴퓨터 또는 다른 프로그램 가능한 데이터 처리 장치가 특정 방식으로 기능하도록 연결할 수 있는 컴퓨터-판독 가능한 메모리에 저장될 수 있어, 컴퓨터-판독 가능한 메모리에 저장된 명령어가 흐름도 블록 또는 블록에서 지정된 기능을 구현하는 명령어 수단을 포함하는 제조 물품(article of manufacture)을 생산할 수 있다. 또한, 컴퓨터 또는 다른 프로그램 가능한 장치에서 실행되는 명령어가 흐름도 블록 또는 블록에서 지정된 기능을 구현하기 위한 단계를 제공할 수 있도록 컴퓨터-구현 프로세스를 생산하기 위한 컴퓨터 또는 다른 프로그램 가능한 장치에서 일련의 작동 단계가 실행되게 하여 컴퓨터 또는 다른 프로그램 가능한 데이터 처리 장치에서 컴퓨터 프로그램 명령어가 로딩될 수 있다.

[0118] 따라서, 블록도 및 흐름도의 기능적 블록은 특정 기능을 수행하기 위한 수단의 조합, 특정 기능을 수행하기 위

한 단계의 조합 및 특정 기능을 수행하기 위한 프로그램 명령어 수단을 지원한다. 또한, 블록도 및 흐름도의 각 각 기능적 블록, 및 블록도 및 흐름도의 기능 블록의 조합은 특정 기능 또는 단계에 의해 구현되는 특수 목적의 하드웨어-기반 컴퓨터 시스템, 또는 특별한 목적의 하드웨어 및 컴퓨터 명령어의 적절한 조합에 의해 구현될 수 있는 것으로 이해될 것이다. 또한, 프로세스 흐름의 설명 및 이들 기술은 사용자 윈도우, 웹페이지, 웹사이트, 웹 폼, 프롬프트 등을 참조할 수 있다. 본 발명에서 설명된 예시된 단계는 윈도우, 웹페이지, 웹 폼, 팝업 윈도우, 프롬프트 등의 사용을 포함하는 많은 수의 구성을 포함할 수 있는 것으로 이해될 것이다. 도시되고 설명된 복수의 단계들은 하나의 웹 페이지 및/또는 윈도우로 결합될 수 있지만, 간략화를 위해 확장된 것으로 이해해야 한다. 다른 경우, 단일 프로세스 단계로 도시되고 설명된 단계는 복수의 웹페이지 및/또는 윈도우로 분리될 수 있지만 단순화를 위해 결합된다.

[0119] 용어 "비일시적(non-transitory)"은 청구 범위로부터 단지 전파하는 일시적 신호 그 자체를 제거하는 것이고 전파하는 일시적 신호 그 자체가 아닌 모든 표준 컴퓨터 판독가능 매체에 대한 권한을 포기하는 것이 아님이 이해될 것이다. 다른 방식으로 서술하면, 용어 "비일시적 컴퓨터 판독가능 매체(non-transitory computer-readable medium)"의 의미는 35 U.S.C. § 101 하에서 특허가능한 대상(patentable subject matter)의 범위 밖에 속하도록 In Re Nuijten에서 발견된 그와 같은 타입의 일시적 컴퓨터 판독가능 매체만을 배제하는 것으로 해석되어야 한다.

[0120] 혜택, 다른 이점 및 문제점에 대한 해결책은 특정 실시예와 관련하여 본 발명에서 설명되었다. 그러나, 임의의 혜택, 이점 또는 해결책이 일어나거나 더욱 두드러지게 할 수 있는 혜택, 장점, 문제점에 대한 해결책 및 임의의 요소는 본 발명의 핵심(critical), 요청된 또는 본질적 특징 또는 요소로서 해석되는 것이 아니다.

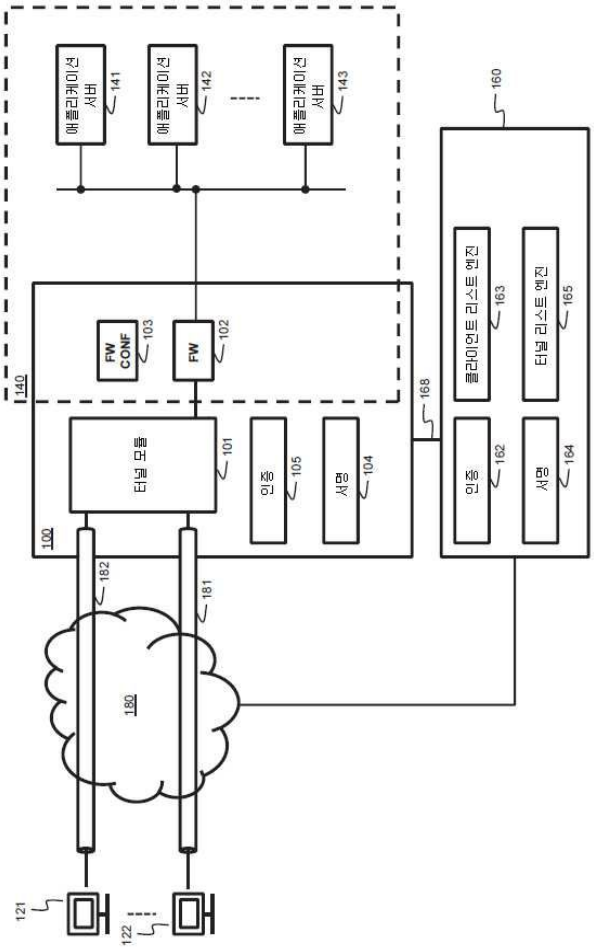
[0121] 본 발명은 방법을 포함하지만, 자기 또는 광학 메모리 또는 자기 또는 광학 디스크와 같은 탠저블 컴퓨터 판독가능 캐리어(tangible computer-readable carrier) 상에 컴퓨터 프로그램 명령으로서 구현될 수 있는 것이 고려된다. 당업자에게 알려지는 상술한 예시적인 실시예의 요소에 대한 모든 구조적, 화학적 및 기능적 등가물(equivalent)은 참조에 의해 본원에 명시적으로 포함되고 본 청구범위에 의해 열거되는 것으로 의도된다. 더욱이, 장치 또는 방법이 본 발명에 의해 해결되도록 추구되는 각각의 그리고 모든 문제점이 해결되어야 하거나 본 청구범위에 의해 열거되어야 하는 것은 아니다. 또한, 본 발명에서의 어떠한 요소, 컴포넌트 또는 방법 단계도 요소, 컴포넌트 또는 방법 단계가 청구범위에 명시적으로 인용되는지에 관계없이 공공에 전용되는 것으로 의도되지 않는다. 본원의 어떠한 청구범위 요소도 그 요소가 명시적으로 어구 "~하기 위한 수단(means for)"을 사용하여 인용되지 않는 한, 35 U.S.C. 112, 제 6 조의 규정에 의거하여 해석되어서는 안된다. 본 발명에서 사용된 바와 같이, 용어 "포함하다(comprise)", "포함하는(comprising)", 또는 임의의 변형은 요소의 리스트를 포함하는 프로세스, 방법, 물품 또는 장치가 단지 그 요소를 포함하는 것이 아니라 그와 같은 프로세스, 방법, 물품 또는 장치에 명시적으로 목록화되지 않거나 내재적이지 않은 다른 요소를 포함할 수 있도록, 비-배타적 포함(non-exclusive inclusion)을 포괄하는 것으로 의도된다.

[0122] "A, B, 또는 C 중 적어도 하나(at least on of A, B or C)", "A, B 및 C 중 적어도 하나(at least one of A, B, and C)" 또는 "A, B, 및 C 중 하나 또는 그 이상(one or more of A, B, and C)"과 유사한 어구가 사용되는 경우에, 그 어구는 A 단독으로 실시예에 제시될 수 있고, B 단독으로 실시예에 제시될 수 있고, C 단독으로 실시예에 제시될 수 있거나, 요소 A, B 및 C의 임의의 조합이 단일 실시예; 예를 들어, A 및 B, A 및 C, B 및 C, 또는 A 및 B 및 C로 제시될 수 있음을 의미하도록 해석되는 것이 의도된다.

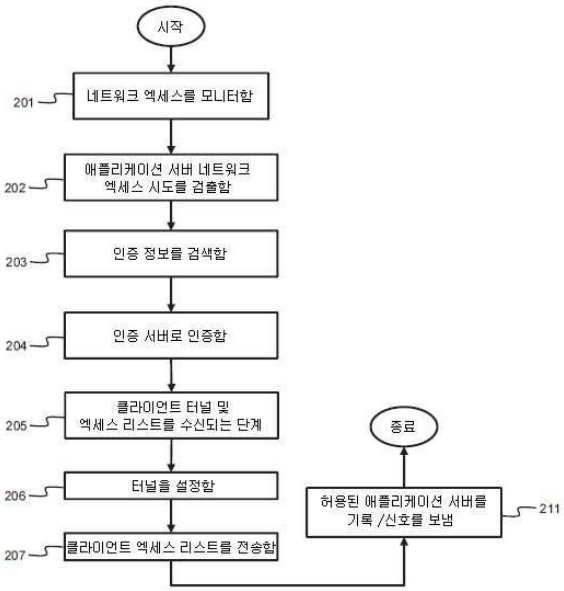
[0123] 본 발명의 범위를 벗어나지 않고 개시된 실시예에 대한 변경 및 수정이 이루어질 수 있다. 이들 및 다른 변경 또는 수정은 하기 청구 범위에 표현된 바와 같이 본 발명 내용의 범위 내에 포함되는 것으로 의도된다.

도면

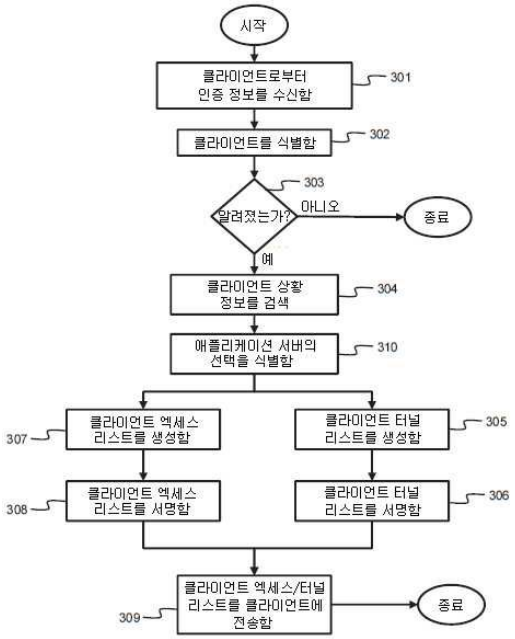
도면1


애플리케이션 서버
141
애플리케이션 서버
142
애플리케이션 서버
143
160
클라이언트 리스트 엔진
163
터널 리스트 엔진
165
FW CONF
103
FW
102
140
168
터널 모듈
101
인증
105
서명
104
인증
162
서명
164
100
182
181
180
121
122

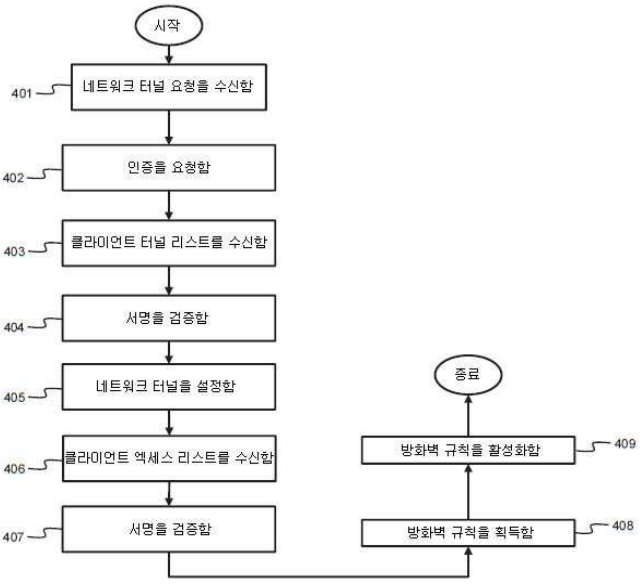
도면2


시작
201
네트워크 엑세스를 모니터함
202
애플리케이션 서버 네트워크 엑세스 시도를 검출함
203
인증 정보를 검색함
204
인증 서버로 인증함
205
클라이언트 터널 및 엑세스 리스트를 수신되는 단계
206
터널을 설정함
207
클라이언트 엑세스 리스트를 전송함
종료
허용된 애플리케이션 서버를 기록 /신호를 보냄
211

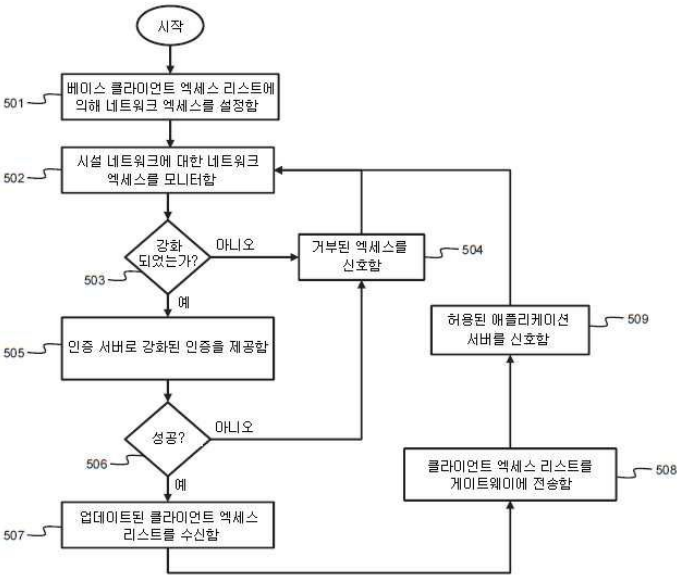
도면3


시작
클라이언트로부터 인증 정보를 수신함
301
클라이언트를 식별함
302
303
알려졌는가?
아니오
종료
예
클라이언트 상황 정보를 검색
304
애플리케이션 서버의 션택을 식별함
310
307
클라이언트 엑세스 리스트를 생성함
클라이언트 터널 리스트를 생성함
305
308
클라이언트 엑세스 리스트를 서명함
클라이언트 터널 리스트를 서명함
306
309
클라이언트 엑세스/터널 리스트를 클라이언트에 전송함
종료

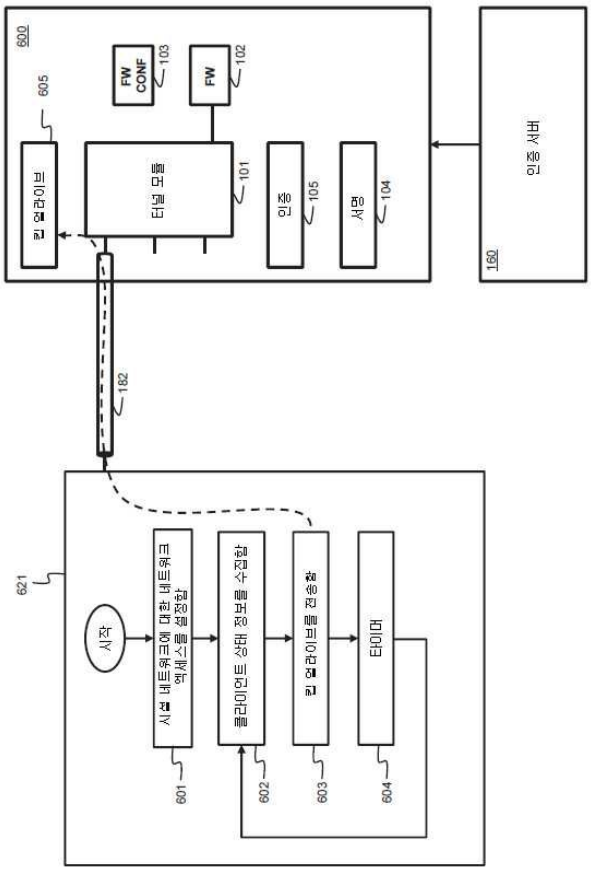
도면4


시작
401
네트워크 터널 요청을 수신함
402
인증을 요청함
403
클라이언트 터널 리스트를 수신함
404
서명을 검증함
405
네트워크 터널을 설정함
406
클라이언트 엑세스 리스트를 수신함
407
서명을 검증함
종료
방화벽 규칙을 활성화함
409
방화벽 규칙을 획득함
408

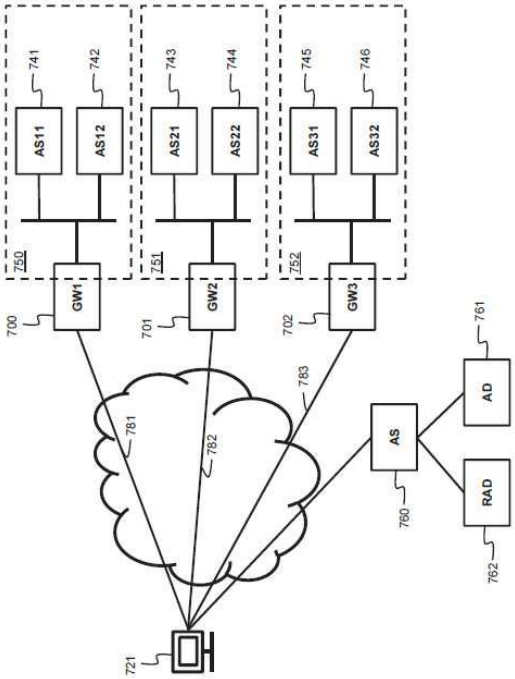
도면5


시작
베이스 클라이언트 엑세스 리스트에 의해 네트워크 엑세스를 설정함
501
시설 네트워크에 대한 네트워크 엑세스를 모니터함
502
강화 되었는가?
503
아니오
거부된 엑세스를 신호함
504
예
인증 서버로 강화된 인증을 제공함
505
허용된 애플리케이션 서버를 신호함
509
성공?
506
아니오
클라이언트 엑세스 리스트를 게이트웨이에 전송함
508
예
업데이트된 클라이언트 엑세스 리스트를 수신함
507

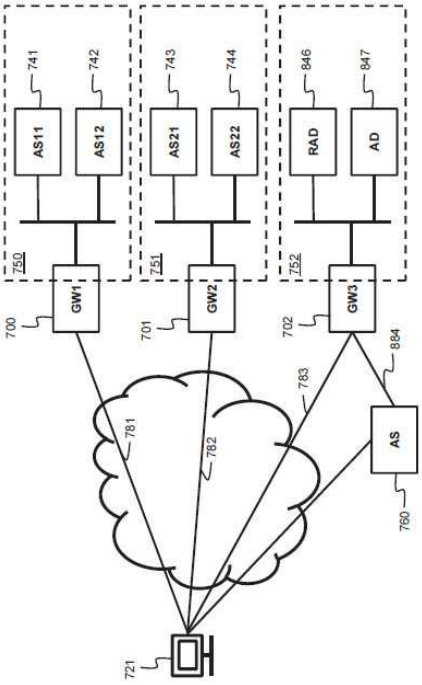
도면6


600
605
FW CONF
103
FW
102
킬 어플라이브
터널 모듈
101
인증
105
서명
104
인증 서버
160
162
621
시작
시스템 네트워크에 대한 네트워크 엑세스를 설정함
601
클라이언트 상태 정보를 수집함
602
킬 어플라이브를 전송함
603
타이머
604

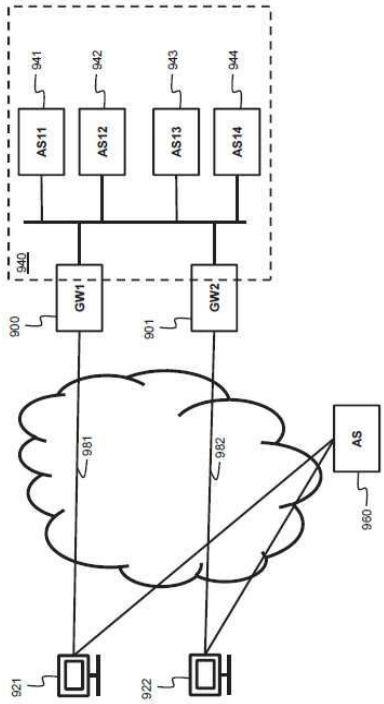
도면7


741
742
743
744
745
746
AS11
AS12
AS21
AS22
AS31
AS32
750
751
752
GW1
GW2
GW3
700
701
702
761
783
781
782
AS
AD
RAD
760
762
721

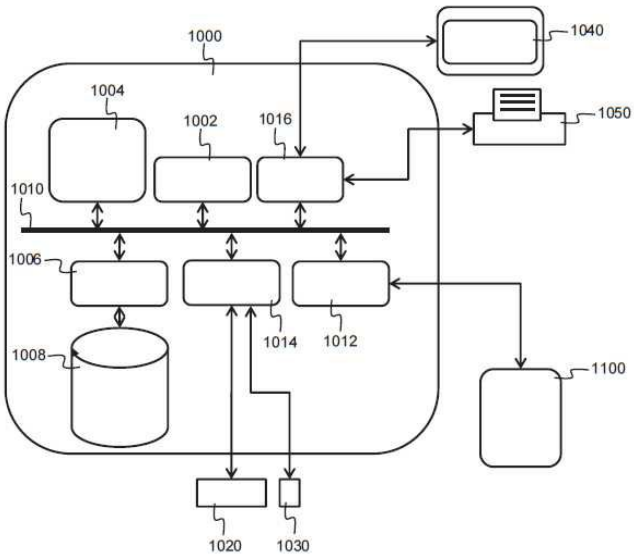
도면8


741
742
743
744
846
847
AS11
AS12
AS21
AS22
RAD
AD
750
751
752
GW1
GW2
GW3
700
701
702
884
783
781
782
AS
760
721

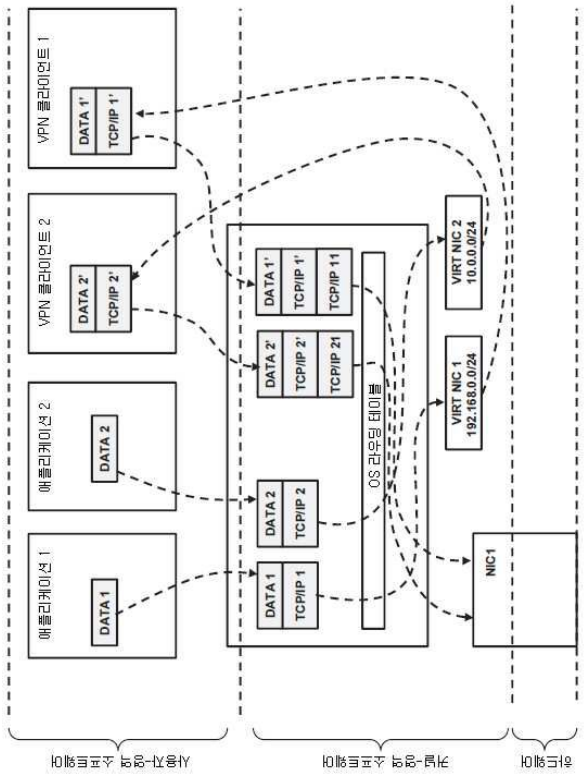
도면9


941
942
943
944
AS11
AS12
AS13
AS14
940
GW1
GW2
900
901
981
982
AS
960
921
922

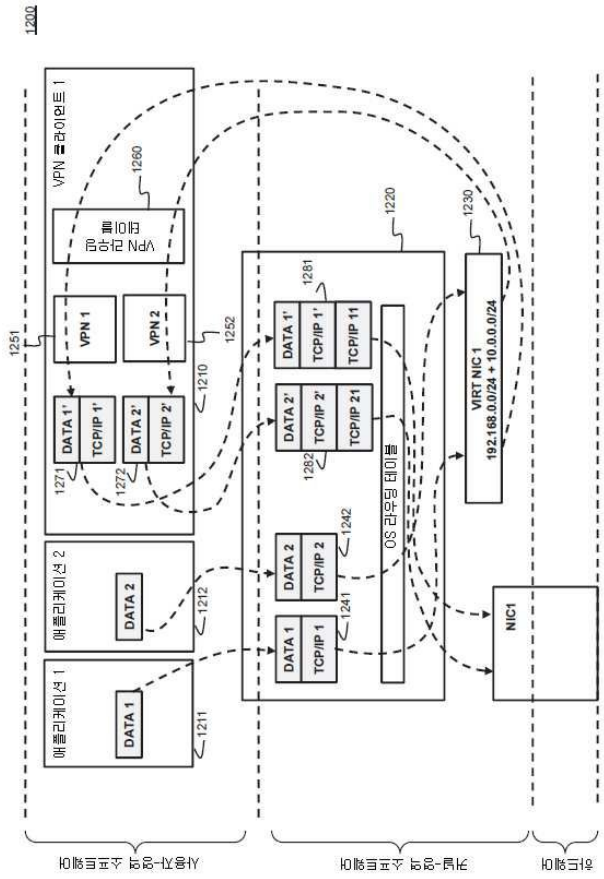
도면10


1000
1040
1004
1002
1016
1050
1010
1006
1014
1012
1008
1100
1020
1030

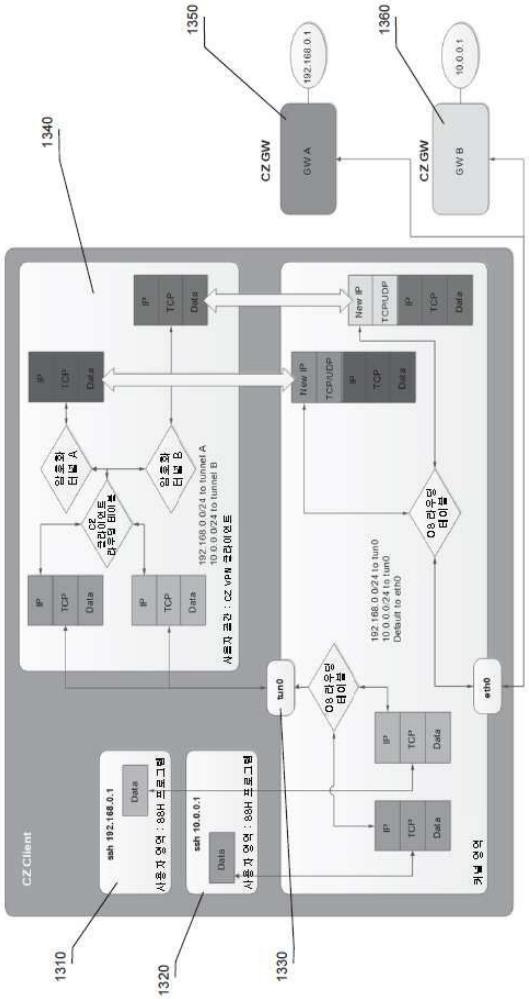
도면11


VPN 클라이언트 1
DATA 1'
TCP/IP 1'
VPN 클라이언트 2
DATA 2'
TCP/IP 2'
애플리케이션 2
DATA 2
애플리케이션 1
DATA 1
DATA 1'
TCP/IP 1'
TCP/IP 11
DATA 2'
TCP/IP 2'
TCP/IP 21
DATA 2
TCP/IP 2
DATA 1
TCP/IP 1
OS 라우팅 테이블
VIRT NIC 2
10.0.0.0/24
VIRT NIC 1
192.168.0.0/24
NIC1
사용자-영역 소프트웨어
커널-영역 소프트웨어
하드웨어

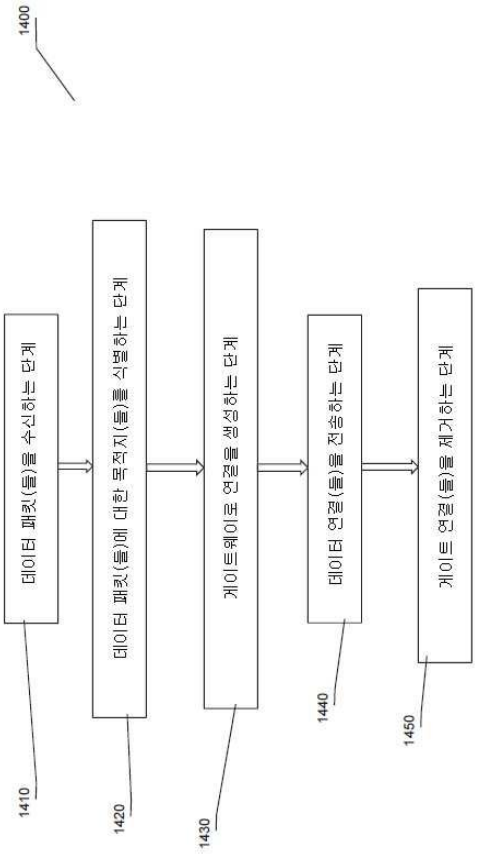
도면12


1200
VPN 클라이언트 1
1260
VPN 라우팅 테이블
VPN 1
VPN 2
1251
1252
1210
DATA 1'
TCP/IP 1'
DATA 2'
TCP/IP 2'
1271
1272
애플리케이션 2
DATA 2
1212
애플리케이션 1
DATA 1
1211
1220
1230
1261
DATA 1'
TCP/IP 1'
TCP/IP 11
DATA 2'
TCP/IP 2'
TCP/IP 21
1282
1242
DATA 2
TCP/IP 2
1241
DATA 1
TCP/IP 1
OS 라우팅 테이블
VIRT NIC 1
192.168.0.0/24 + 10.0.0.0/24
NIC1
사용자-영역 소프트웨어
커널-영역 소프트웨어
하드웨어

도면13


1350
1360
1340
CZ GW
GW A
GW B
192.168.0.1
10.0.0.1
CZ Client
사용자 영역 : SSH 프로그램
ssh 192.168.0.1
ssh 10.0.0.1
Data
사용자 공간 : CZ VPN 클라이언트
암호화 터널 A
암호화 터널 B
CZ 라이언트 라우팅 테이블
192.168.0.0/24 to tunnel A
10.0.0.0/24 to tunnel B
IP
TCP
Data
New IP
TCP/UDP
tun0
eth0
OS 라우팅 테이블
OS 응용 테이블
192.168.0.0/24 to tun0
10.0.0.0/24 to tun0
Default to eth0
커널 영역
1310
1320
1330

도면14


1400
데이터 패킷(들)을 수신하는 단계
데이터 패킷(들)에 대한 목적지(들)를 식별하는 단계
게이트웨이로 연결을 생성하는 단계
데이터 연결(들)을 전송하는 단계
게이트 연결(들)을 제거하는 단계
1410
1420
1430
1440
1450