(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0119549
(43) 공개일자 2016년10월14일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)
H04L 12/713 (2013.01)
(52) CPC특허분류
H04L 63/0272 (2013.01)
H04L 41/28 (2013.01)
(21) 출원번호 10-2015-0048365
(22) 출원일자 2015년04월06일
심사청구일자 2015년04월06일

(71) 출원인
주식회사 모바일컨버전스
경기도 성남시 분당구 판교역로 231, 에스-905 (삼평동, 에이치스퀘어)
(72) 발명자
이상화
서울특별시 강남구 광평로10길 50 청솔빌리지, 106동 303호(일원동)
(74) 대리인
이형우

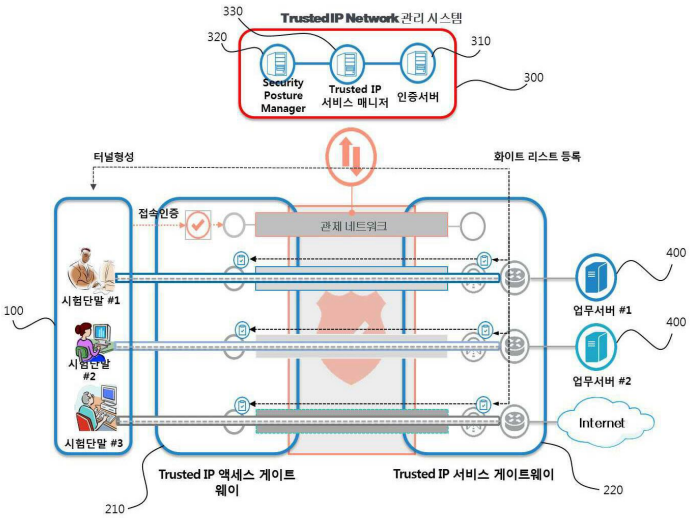
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **네트워크 ＶＰＮ 기반의 네트워크 가상화 시스템**

(57) 요 약

본 발명은 네트워크 가상화 시스템에 관한 것으로서, 보다 상세하게는 인증된 디바이스에 한하여 업무서버로의 네트워크 접근을 허용하되, 인증시에 디바이스와 특정 업무서버 상호간을 가상 라우터(VR : Virtual Router)에 의해 연결하는 다중 터널링을 구축하여 엔드 투 엔드(end-to-end signaling) 방식으로 직접 연결시킴으로써, 망분리를 위한 물리적 구조를 추가하지 않고도 네트워크 자체를 가상 사설망(VPN)처럼 망분리시켜 사용할 수 있게 하며, 그로 인하여 내부뿐만 아니라 외부에 있는 디바이스를 이용하여서도 인증된 권한 범위 내에서 해당 업무서버들에의 자유로운 접근을 보장함과 아울러, 인증된 디바이스로 접근할 수 있는 특정 업무서버를 제외한 다른 업무서버로는 터널 자체가 형성되지 않게 하여 보안성도 동시에 향상시킬 수 있게 한 네트워크 VPN 기반의 네트워크 가상화 시스템에 관한 것이다.

대 표 도



(52) CPC특허분류
H04L 45/586 (2013.01)
H04L 63/029 (2013.01)
H04L 63/08 (2013.01)

명 세 서

청구범위

청구항 1

디바이스와 특정 업무서버 상호간을 가상 라우터(VR)에 의해 연결되는 적어도 하나 이상의 VPN 터널에 의해 엔드 투 엔드 방식(end-to-end signaling)으로 직접 연결시켜 디바이스가 업무서버에 접근하는 네트워크망을 가상화함으로써, 디바이스에서 업무서버에 접근할 수 있는 네트워크망을 분리할 수 있도록 구성된 네트워크 VPN 기반의 네트워크 가상화 시스템.

청구항 2

제1항에 있어서,

유무선 통신망을 이용하여 업무서버에의 접근을 요청하는 디바이스;

상기 디바이스가 유무선 통신망상에서 업무서버에 접속하는 적어도 하나 이상의 VPN 터널을 형성하여 인증된 디바이스와 특정 업무서버를 연결하는 게이트웨이;

상기 게이트웨이를 통하여 인증된 디바이스와의 분리된 네트워크망을 형성하기 위한 적어도 하나 이상의 VPN 터널을 가상 라우팅 기반으로 형성하도록 제어하는 관리시스템; 및

상기 관리시스템에서 가상 라우팅 기반으로 형성된 적어도 하나 이상의 VPN 터널에 의해 상기 디바이스와 엔드 투 엔드 방식으로 연결되는 업무서버;를 포함하는 것을 특징으로 하는 네트워크 VPN 기반의 네트워크 가상화 시스템.

청구항 3

제2항에 있어서,

상기 인증된 디바이스와 특정 업무서버 상호간을 연결하는 VPN 터널은 가상 라우터(VR)에 기반하여 상기 디바이스가 게이트웨이에 연결되는 터널과 상기 업무서버가 게이트웨이에 연결되는 터널을 형성하게 되며, 상기 디바이스가 게이트웨이에 연결되는 부분은 디바이스의 접근성을 확보하기 위한 액세스 게이트웨이를 형성하고, 상기 업무서버가 게이트웨이에 연결되는 부분은 상기 게이트웨이를 통하여 접근하는 디바이스에게 업무서버를 통하여 구현되는 서비스를 제공하기 위한 서비스 게이트웨이를 형성하도록 구성되는 것을 특징으로 하는 네트워크 VPN 기반의 네트워크 가상화 시스템.

청구항 4

제3항에 있어서,

상기 VPN 터널은 다중 터널링(Tunnel-in-Tunnel)에 의해 서로 다른 속성을 갖는 복수의 터널들 상호간을 실시간 효율적으로 연동시킬 수 있도록 구성되는 것을 특징으로 하는 네트워크 VPN 기반의 네트워크 가상화 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 네트워크 가상화 시스템에 관한 것으로서, 보다 상세하게는 인증된 디바이스에 한하여 업무서버로의 네트워크 접근을 허용하되, 인증시에 디바이스와 특정 업무서버 상호간을 가상 라우터(VR : Virtual Router)에 의해 연결하는 다중 터널링을 구축하여 엔드 투 엔드(end-to-end signaling) 방식으로 직접 연결시킴으로써, 망분리를 위한 물리적 구조를 추가하지 않고도 네트워크 자체를 가상 사설망(VPN)처럼 망분리시켜 사용할 수 있게 하며, 그로 인하여 내부뿐만 아니라 외부에 있는 디바이스를 이용하여서도 인증된 권한 범위 내에서 해당 업무서버들에의 자유로운 접근을 보장함과 아울러, 인증된 디바이스로 접근할 수 있는 특정 업무서버를 제외한 다른 업무서버로는 터널 자체가 형성되지 않게 하여 보안성도 동시에 향상시킬 수 있게 한 네트워크 VPN 기반의 네트워크 가상화 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 초고속 인터넷망의 확충과 이동통신망(3G/LTE) 및 WiFi 기술의 진보로 언제 어디서나 디바이스를 이용하여 업무서버에 접속할 수 있는 업무환경이 구축되어 가고 있다.

[0003] 이처럼 퍼스널 컴퓨터나 노트북 또는 휴대용 스마트 기기를 이용하여 통신망 상에서 업무서버에 접속하기 위해서는 IP 네트워크를 이용함이 일반적인데, 이러한 종래의 IP 네트워크는 우수한 개방성으로 인하여 접근의 편의성은 향상되지만, 정상적인 사용자뿐만 아니라, 해커 등 악의적인 사용자의 접근도 용이할 뿐만 아니라, 내부 내트워크에 접속한 후에는 해당 내부 네트워크에 연결되어 있는 모든 서버에의 접근이 가능하게 되므로 보안상 커다란 취약점을 갖고 있을 수 밖에 없었다.

[0004] 이처럼 IP 패킷을 이용하여 구성되는 종래의 IP 패킷 네트워크는 패킷(Packet)에 있는 IP Prefix를 보고 라우팅(Routing) 하여 목적지로 전달하는 역할만 수행하므로, 해당 패킷에 있는 트래픽에 따라 업무서버에 접속할 수 있게 되어 위조된 패킷이나 위조된 단말로부터 전송된 패킷도 정상적인 패킷과 같이 처리하게 될 수 있어 업무망 전체가 악의적인 사용자들에게 노출되는 것을 방어하기 어려운 문제점이 있었다.

[0005] 그에 따라, 근래에는 유선기반의 업무망과 인터넷망을 분리하여 운용하는 물리적 망분리를 국가나 공공기관 등에서 시행하면서 이를 권장하고 있으나, 외부에서 업무망에의 접근이 어려울 뿐만 아니라, 내부에서도 업무와 인터넷의 교차사용에 따른 번거로움을 피하기 어려운 문제점이 있었다. 그에 따라, 업무망과 인터넷망의 분리에 따른 이중화로 인하여 실질적인 사용자들의 불편이 증가될 뿐만 아니라, 분리된 망구축을 위해 소요되는 비용이 크게 증가하게 되는 문제점이 있었다.

[0006] 또한 물리적으로 분리된 망 일부에서 업무망과 인터넷망의 접점이 발생하게 됨으로 인하여 전체 망의 보안성이 저하될 우려가 있음은 물론, 부처별 또는 기관별로 두 개의 망을 구축하고 이를 유지하며, 퍼스널 컴퓨터나 프린터 등 업무환경을 이중으로 구성해야 하였는바 구축을 위해 소요되는 비용 부담이 증가하게 될 밖에 없었다.

[0007] 또한, 최근 이용이 증가하고 있는 가상 사설망(VPN : Virtual Private Network)은 인트라넷(사설망)에 연결된 단말이 인터넷을 이용하여 사설망에 접속할 수 있게 한 것인데, 이러한 가상 사설망의 경우에도 LAN기반의 구조로 이루어지므로, IP Prefix를 이용하는 경우처럼 모든 서버가 해커 등 악의적인 사용자들로부터의 공격위험에 노출될 수 밖에 없었다.

[0008] 이러한 가상 사설망(VPN)을 구축할 경우 각 VPN 디바이스별로 존재하는 관제서버의 통합 관리가 어려운 문제점이 있었으며, 각 VPN 디바이스별로 별개의 네트워크를 구성할 수 있는 통합 VPN 게이트웨이가 필요하게 되는바, 디바이스가 증가하게 됨에 따른 통합 VPN 게이트웨이를 추가하기 위해 망을 구축하고 이를 유지 관리하기 위한 비용과 인력이 지속적으로 증가하게 되는 문제점이 있었다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 대한민국 공개특허공보 제10-2014-0045214호

(특허문헌 0002) 대한민국 공개특허공보 제10-2014-0099598호

발명의 내용

해결하려는 과제

[0010] 본 발명은 인증된 디바이스에 한하여 업무서버로의 네트워크 접근을 허용하되, 인증시에 디바이스와 특정 업무서버 상호간을 가상 라우터(VR : Virtual Router)에 의해 연결하는 다중 터널링을 구축하여 엔드 투 엔드(end-to-end signaling) 방식으로 직접 연결시킴으로써, 망분리를 위한 물리적 구조를 추가하지 않고도 네트워크 자체를 가상 사설망(VPN)처럼 망분리시켜 사용할 수 있게 하며, 그로 인하여 내부뿐만 아니라 외부에 있는 디바이스를 이용하여서도 인증된 권한 범위 내에서 해당 업무서버들에의 자유로운 접근을 보장함과 아울러, 인증된 디바이스로 접근할 수 있는 특정 업무서버를 제외한 다른 업무서버로는 터널 자체가 형성되지 않게 하여 보안성도 동시에 향상시킬 수 있게 한 네트워크 VPN 기반의 네트워크 가상화 시스템을 제공하기 위한 것이다.

과제의 해결 수단

[0011] 상기 과제를 해결하기 위한 네트워크 VPN 기반의 네트워크 가상화 시스템은, 디바이스와 특정 업무서버 상호간을 가상 라우터(VR)에 의해 연결되는 적어도 하나 이상의 VPN 터널에 의해 엔드 투 엔드 방식(end-to-end signaling)으로 직접 연결시켜 디바이스가 업무서버에 접근하는 네트워크망을 가상화함으로써, 디바이스에서 업무서버에 접근할 수 있는 네트워크망을 분리할 수 있도록 구성되는 것을 특징으로 한다.

[0012] 또한, 본 발명은 유무선 통신망을 이용하여 업무서버에의 접근을 요청하는 디바이스; 상기 디바이스가 유무선 통신망상에서 업무서버에 접속하는 적어도 하나 이상의 VPN 터널을 형성하여 인증된 디바이스와 특정 업무서버를 연결하는 게이트웨이; 상기 게이트웨이를 통하여 인증된 디바이스와의 분리된 네트워크망을 형성하기 위한 적어도 하나 이상의 VPN 터널을 가상 라우팅 기반으로 형성하도록 제어하는 관리시스템; 및 상기 관리시스템에서 가상 라우팅 기반으로 형성된 적어도 하나 이상의 VPN 터널에 의해 상기 디바이스와 엔드 투 엔드 방식으로 연결되는 업무서버;를 포함하는 것을 특징으로 한다.

발명의 효과

[0013] 본 발명은 디바이스와 특정 업무서버 상호간을 가상 라우터(VR : Virtual Router)에 의해 연결하는 다중 터널링을 구축하여 엔드 투 엔드(end-to-end signaling) 방식으로 직접 연결시킴으로써, 망분리를 위한 물리적 구조를 추가하지 않고도 네트워크 자체를 가상 사설망(VPN)처럼 망분리시켜 사용할 수 있게 하며, 그로 인하여 내부뿐만 아니라 외부에 있는 디바이스를 이용하여서도 인증된 권한 범위 내에서 해당 업무서버들에의 자유로운 접근을 보장함과 아울러, 인증된 디바이스로 접근할 수 있는 특정 업무서버를 제외한 다른 업무서버로는 터널 자체가 형성되지 않게 하여 보안성도 동시에 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

[0014] 도 1은 종래 IP Prefix 기반 네트워크의 예시도.

도 2는 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 상태를 나타내는 예시도.

도 3은 본 발명에 따라 VPN 터널을 이용하여 망 분리된 네트워크 가상화 상태를 나타내는 예시도.

도 4는 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 상태를 나타내는 시스템 구성도.

도 5는 본 발명에 따라 가상 라우터에 의한 다중 터널링을 이용하여 디바이스와 서버를 연결하는 터널을 형성하는 것을 나타내는 구성도.

발명을 실시하기 위한 구체적인 내용

[0015] 이하에서는 본 발명의 구체적인 실시예를 도면을 참조하여 상세히 설명하도록 한다.

[0016] 도 1은 종래 IP Prefix 기반 네트워크의 예시도이고, 도 2는 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 상태를 나타내는 예시도이며, 도 3은 본 발명에 따라 VPN 터널을 이용하여 망 분리된 네트워크 가상화 상태를 나타내는 예시도이고, 도 4는 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 상태를 나타내는 시스템 구성도이다.

[0017] 도 2 내지 도 4를 참조하면, 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 시스템은, 디바이스와 특정 업무서버 상호간을 가상 라우터(VR : Virtual Router)에 의해 연결되는 적어도 하나 이상의 VPN 터널에 의해 엔드 투 엔드 방식(end-to-end signaling)으로 직접 연결시켜 디바이스가 업무서버에 접근하는 네트워크망을 가상화함으로써, 디바이스에서 업무서버에 접근할 수 있는 네트워크망을 분리할 수 있도록 구성된다.

[0018] 이와 같이 가상 라우터와 VPN 터널에 의해 디바이스와 특정 업무서버 상호간을 엔드 투 엔드 방식으로 연결시켜 디바이스를 이용하여 접근할 수 있는 업무서버를 VPN 터널에 의해 연결되어 있는 특정 업무서버로 한정함으로써, 터널이 형성되어 있지 않은 다른 업무서버에 접근할 수 있는 네트워크망과는 분리할 수 있게 되므로, 기업이나 조직의 기관 단위별, 또는 서비스 단위별로 전용 보안 터널을 형성할 수 있게 된다.

[0019] 이를 위하여, 본 발명에 따른 네트워크 VPN 기반의 네트워크 가상화 시스템은, 유무선 통신망을 이용하여 업무서버에의 접근을 요청하는 디바이스(100)와, 상기 디바이스가 유무선 통신망상에서 업무서버에 접속하는 적어도 하나 이상의 VPN 터널을 형성하여 인증된 디바이스와 특정 업무서버를 연결하는 게이트웨이(200)와, 상기 게이

트웨이를 통하여 인증된 디바이스와의 분리된 네트워크망을 형성하기 위한 적어도 하나 이상의 VPN 터널을 가상 라우팅 기반으로 형성하도록 제어하는 관리시스템(300)과, 상기 관리시스템에서 가상 라우팅 기반으로 형성된 적어도 하나 이상의 VPN 터널에 의해 상기 디바이스와 엔드 투 엔드 방식으로 연결되는 업무서버(400)를 포함하여 구성된다.

[0020] 이때, 상기 VPN 터널은 기존 인터넷과 호환성이 있도록 형성되지만, 상기 VPN 터널을 형성함에 있어 상기 디바이스(100)와 업무서버(400)를 직접 연결하여 데이터의 처리가 가능하게 하는 도메인과, 상기 디바이스(100)를 인증하고 인증된 권한 범위 내에서 특정 업무서버와의 연결을 위한 VPN 터널의 생성을 제어하는 관리시스템(300)의 도메인을 격리하여 상호 분리시킴으로써, 보안성을 향상시킬 수 있도록 구성된다.

[0021] 이와 같이 VPN 터널에 의해 디바이스(100)가 업무서버(400)에 연결되기 위한 도메인과, 관리시스템(300)에서 인증하고 VPN 터널을 형성하는 도메인이 상호 분리될 뿐만 아니라, 디바이스가 접속할 수 있는 각 업무서버들의 경우에도 각 디바이스(100)와 업무서버(400) 상호간을 연결하는 VPN 터널마다 네트워크망을 분리할 수 있게 되므로, 해킹 등을 통하여 하나의 업무서버에 접근한 악의의 사용자도 해당 VPN 터널에 의해 연결되어 있지 않은 다른 업무서버나 관리시스템에 접근할 수 없게 되어 보안성을 향상시킬 수 있게 된다.

[0022] 이와 같이 인증된 디바이스와 특정 업무서버 상호간을 연결하는 VPN 터널은 가상 라우터(VR)에 기반하여 상기 디바이스(100)가 게이트웨이(200)에 연결되는 터널과 상기 업무서버(400)가 게이트웨이(200)에 연결되는 터널을 형성하게 된다. 이때, 상기 디바이스가 게이트웨이에 연결되는 부분은 디바이스의 접근성을 확보하기 위한 액세스 게이트웨이(210)를 형성하고, 상기 업무서버가 게이트웨이에 연결되는 부분은 상기 게이트웨이를 통하여 접근하는 디바이스에게 업무서버를 통하여 구현되는 서비스를 제공하기 위한 서비스 게이트웨이(220)를 형성하게 된다.

[0023] 또한, 상기 VPN 터널은 디바이스가 상기 액세스 게이트웨이에 연결되는 터널과, 상기 액세스 게이트웨이가 서비스 게이트웨이에 연결되는 터널과, 터널 양 종단에서의 암호화 통신을 제공하는 터널 등 서로 다른 속성을 갖는 복수의 터널을 포함하게 되는바, 다중 터널링(Tunnel-in-Tunnel)에 의해 서로 다른 속성을 갖는 복수의 터널들 상호간을 실시간 효율적으로 연동시킬 수 있도록 구성된다.

[0024] 이와 같이 다중 터널링에 의해 연동되도록 구성된 VPN 터널을 이용하여 디바이스가 특정 업무서버에 접근할 수 있게 한 후 트래픽을 전달하면, 터널의 출구지점인 특정 업무서버 전단까지 트래픽이 자동 전달될 수 있게 된다.

[0025] 또한, 상기 관리시스템(300)은, 디바이스나 사용자를 인증할 수 있는 인증정보를 포함하고 있어 네트워크에 접속하는 디바이스를 인증하는 인증서버(310)와, 상기 액세스 게이트를 통하여 접속되는 디바이스에 대한 인증 및 접속관리를 위한 트래픽을 독립적으로 수행한 후 특정 업무서버에의 접근을 허용하고 디바이스의 상태변화를 주기적으로 점검하는 Security Posture Manager(320)와, 상기 디바이스에서 요청하는 서비스에 대한 트래픽을 상기 VPN 터널을 통하여 특정 업무서버로 전송하는 서비스 매니저(330)를 포함하여 구성된다.

[0026] 또한, 상기 가상 라우터(VR) 기반으로 생성되는 VPN 터널은 이동성과 품질보장 기능을 동시에 갖춘 IP-in-IP 터널링 기술을 근간으로 동종 터널을 집중(concentration)시키거나 이기종 터널간을 연동하여 계층적으로 구성할 수 있는 Tunnel-in-Tunnel 기술로 이루어진다.

[0027] 이상에서는 본 발명에 대한 기술사상을 첨부 도면과 함께 서술하였지만 이는 본 발명의 바람직한 실시예를 예시적으로 설명한 것이지 본 발명을 한정하는 것은 아니다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 이라면 누구나 본 발명의 기술적 사상의 범주를 이탈하지 않는 범위 내에서 다양한 변형 및 모방이 가능함은 명백한 사실이다.

부호의 설명

[0028] 100 - 디바이스

200 - 게이트웨이 210 - 액세스 게이트웨이

220 - 서비스 게이트웨이

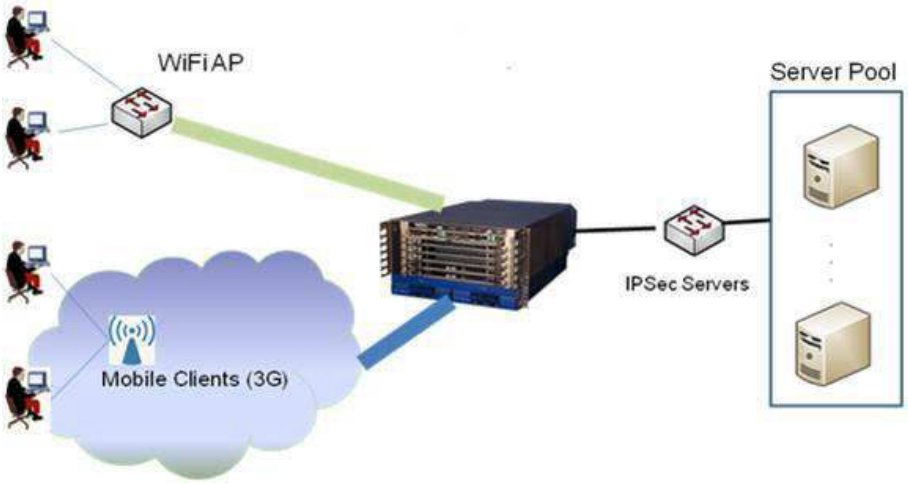
300 - 관리시스템 310 - 인증서버

320 - Security Posture Manager 330 - 서비스 매니저

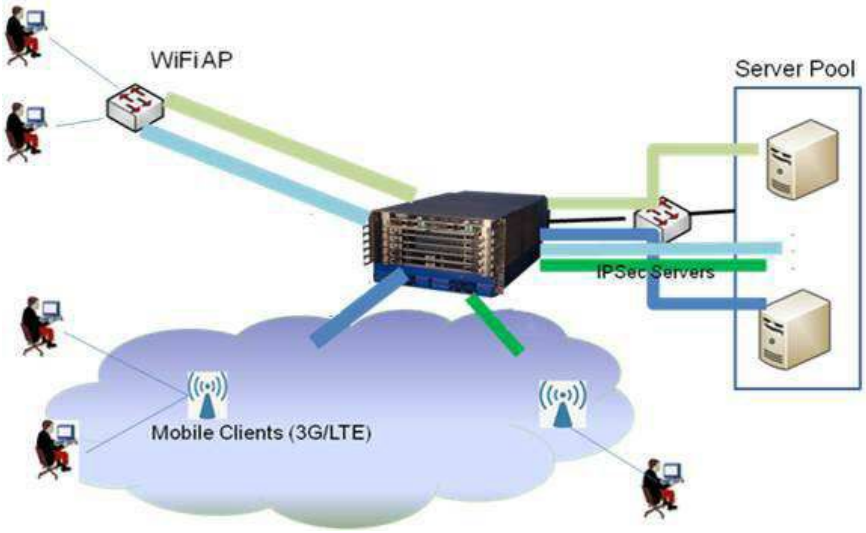
400 - 업무서버

도면

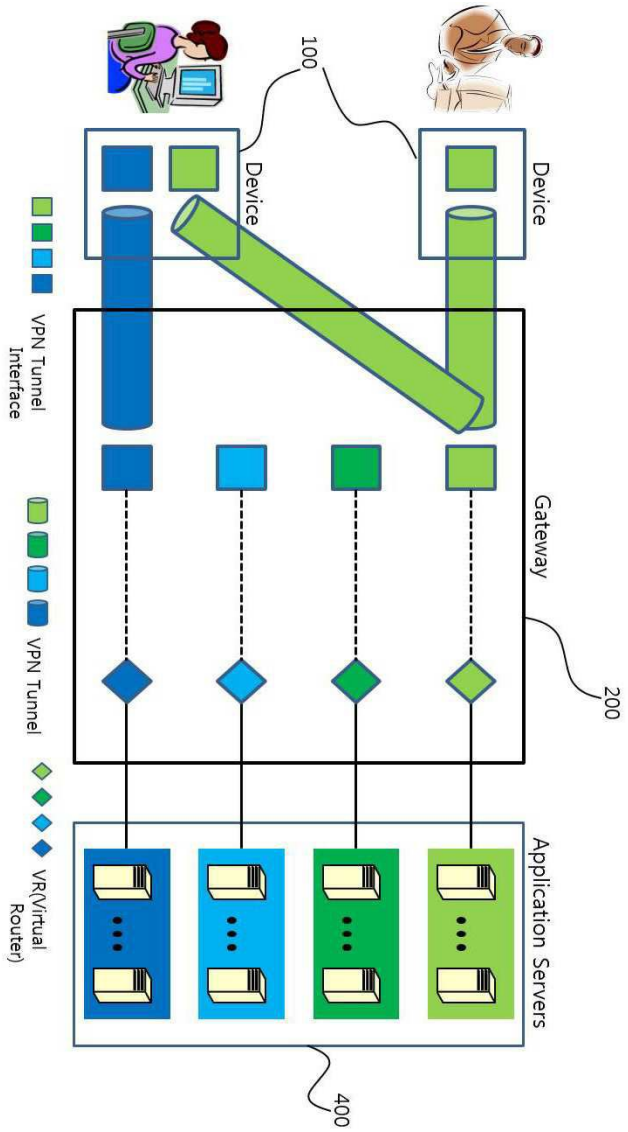
도면1



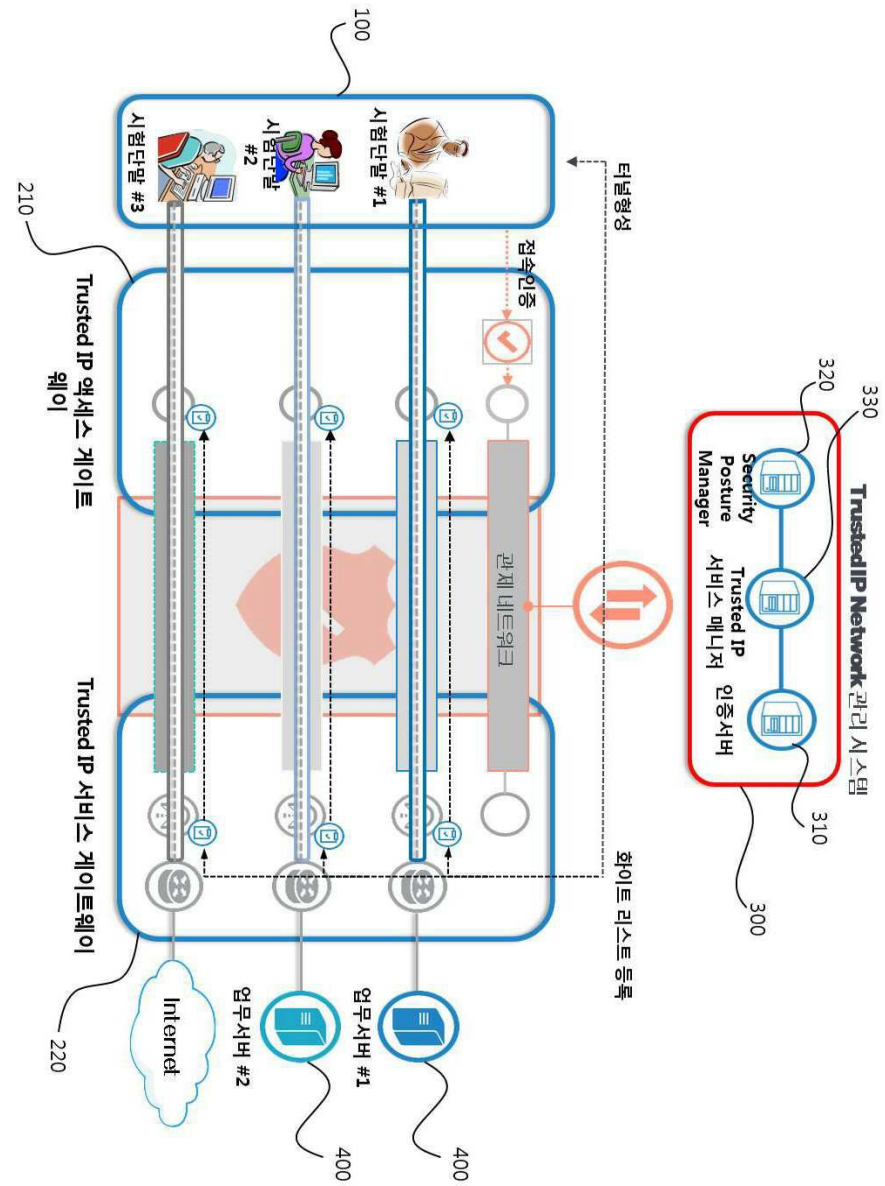
도면2



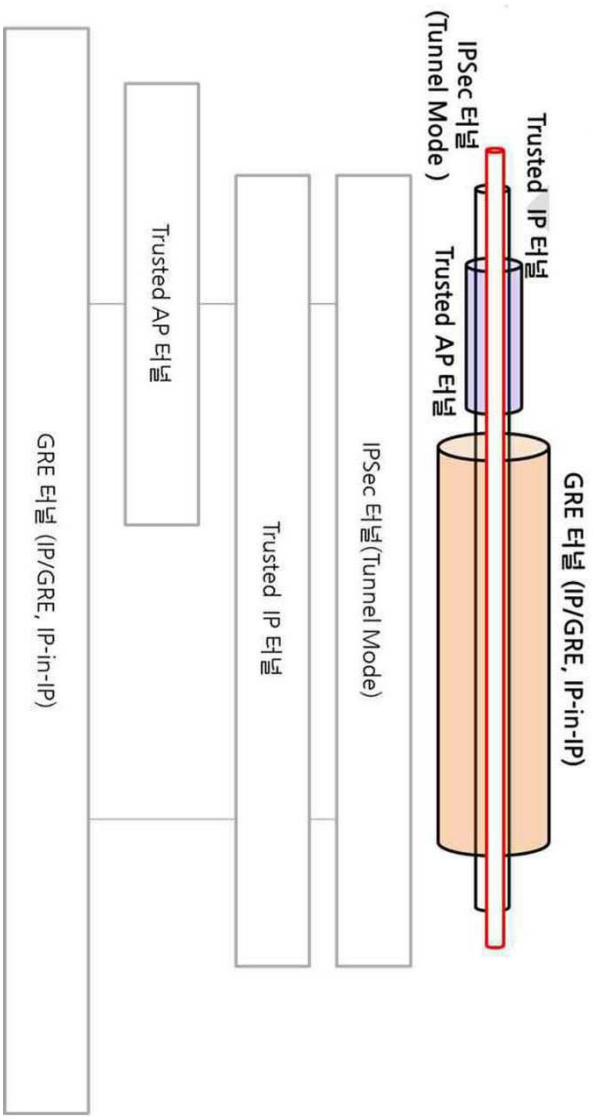
도면3


100
Device
Device
VPN Tunnel Interface
VPN Tunnel
VR(Virtual Router)
Gateway
200
Application Servers
400

도면4


100
시험단말 #1
시험단말 #2
시험단말 #3
터널형성
접속인증
210
Trusted IP 액세스 게이트웨이
관제 네트워크
Trusted IP 서비스 게이트웨이
220
Internet
업무서버 #2
업무서버 #1
400
400
화이트 리스트 등록
Trusted IP Network 관리 시스템
320
330
Security Posture Manager
Trusted IP 서비스 매니저
인증서버
310
300

도면5


GRE 터널 (IP/GRE, IP-in-IP)
Trusted AP 터널
Trusted IP 터널
IPSec 터널(Tunnel Mode)
IPSec 터널
(Tunnel Mode)
Trusted IP 터널
Trusted AP 터널
GRE 터널 (IP/GRE, IP-in-IP)