(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 6 월 29 일 (29.06.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/111404 A1

(51) 국제특허분류:
H04L 29/12 (2006.01) *H04L 29/06* (2006.01)

(21) 국제출원번호: PCT/KR2016/014850

(22) 국제출원일: 2016 년 12 월 19 일 (19.12.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0185419 2015 년 12 월 23 일 (23.12.2015) KR
10-2015-0189064 2015 년 12 월 29 일 (29.12.2015) KR

(71) 출원인: **주식회사 케이티 (KT CORPORATION)** [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).

(72) 발명자: **서경덕 (SEO, Kyung-Deok)**; 55087 전라북도 전주시 완산구 삼천천변 1 길 32, 101 동 1802 호, Jeollabuk-do (KR). **김태균 (KIM, Tae-Gyun)**; 13618 경기도 성남시 분당구 미금로 215, 806 동 1502 호, Gyeonggi-do (KR). **이정일 (LEE, Jung Il)**; 13567 경기도 성남시 분당구 양현로 138, 813 동 801 호, Gyeonggi-do (KR). **장덕문 (CHANG, Deok-Moon)**; 06762 서울시 서초구 바우뫼로 7 길 51, 104 동 1403 호, Seoul (KR).

(74) 대리인: **유미특허법인 (YOU ME PATENT AND LAW FIRM)**; 06134 서울시 강남구 테헤란로 115, Seoul (KR).

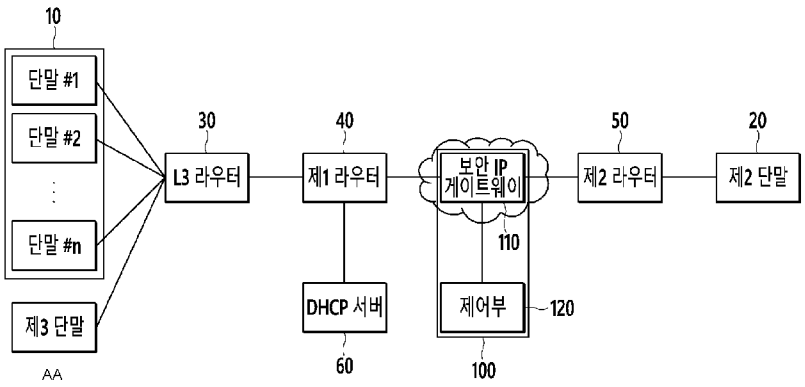
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: DEVICE, METHOD, AND COMMUNICATION SYSTEM FOR PROVIDING SECURITY IP COMMUNICATION SERVICE

(54) **발명의 명칭** : 보안 IP 통신 서비스를 제공하기 위한 장치, 방법 및 통신 시스템



10 ... Terminal
20 ... Second terminal
30 ... L3 router
40 ... First router
50 ... Second router
60 ... DHCP server
110 ... Security IP gateway
120 ... Control unit
AA ... Third terminal

(57) **Abstract**: In order to provide a security IP communication service between a first terminal and a second terminal by a security IP communication service providing device, the security IP communication service providing device checks whether the first terminal and the second terminal are formed into one group, on the basis of a first security core IP and a second security core IP which are included in an IP packet transmitted from the first terminal, and transfers the IP packet having been transmitted from the first terminal to the second terminal when the first terminal and the second terminal are formed into one group.

(57) **요약서**:

[다음 쪽 계속]

WO 2017/111404 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

보안 IP 통신 서비스 제공 장치가 제 1 단말과 제 2 단말 사이에 보안 IP 통신 서비스를 제공하기 위하여, 보안 IP 통신 서비스 제공 장치는 제 1 단말로부터 전송되는 IP 패킷에 포함된 제 1 보안 코어 IP 와 제 2 보안 코어 IP 를 토대로, 제 1 단말과 제 2 단말이 하나의 그룹으로 형성되어 있는지 확인하고, 제 1 단말과 제 2 단말이 그룹으로 형성되어 있으면 제 1 단말로부터 전송된 IP 패킷을 제 2 단말로 전달한다.

명세서

발명의 명칭: 보안 IP 통신 서비스를 제공하기 위한 장치, 방법 및 통신 시스템

기술분야

[1] 본 발명은 보안 IP 통신 서비스를 제공하기 위한 장치, 방법 및 통신 시스템에 관한 것이다.

배경기술

[2] 일반적으로 인터넷 서비스를 이용하고자 하는 단말들은 공중 IP 주소를 할당받은 후 공중 인터넷망에 접속하여 서비스를 이용한다. 인터넷 서비스를 이용하는 단말들은 다양한 형태가 있으며, POS 단말이나 CCTV, IoT 단말 등 다양한 형태가 있으며, 이들 단말들은 개인이 사용할 수도 있으나 사용자 그룹 형태로 묶여 기업 내에 설치될 수도 있다.

[3] 이때, 악의적인 제3자가 공중 인터넷망을 통해 단말에 제공되는 서비스를 변형시키거나 단말로 제공되는 IP 주소를 변경시키거나, DDos와 같은 IP 주소의 공격, 또는 사용자 그룹 형태로 묶인 단말에 할당된 IP 주소를 가로채는 경우에는, POS를 운영하는 매장형 프랜차이즈나 본사-지사/지점간 안전한 접속이 필요한 기업, CCTV 운영 기업이나 기관들은 안전한 서비스를 제공하지 못하는 문제점이 있다.

[4] 이를 위해, 트래픽을 암호화하거나 별도의 VPN 장비를 설치하여 서비스를 제공하고 있으나, VPN 헤더나 트래픽 암호화에 따른 통신 속도가 보장되지 않고, 고비용의 별도의 장비 설치에 따른 비용이 부과되는 단점이 있다.

[5] 이에 따라, 사용자 그룹을 외부에 노출시키지 않으면서도 별도의 VPN 장비 없이도 안전하게 인터넷 통신 환경의 제공이 요구되며, 사용자 그룹을 그룹핑하여 트래픽 암호화 없이도 통신 서비스를 이용할 수 있도록 하는 기술의 개발이 요구된다.

발명의 상세한 설명

기술적 과제

[6] 따라서, 본 발명은 따라서, 본 발명은 공중 인터넷 망에서 지정된 그룹간 폐쇄적인 통신 접속을 가능하게 하는 보안 IP 통신 서비스를 제공하는 보안 인터넷망에서 지정된 그룹간 폐쇄적인 통신 접속을 통해 IP 통신 서비스를 제공하기 위한 장치, 방법 및 통신 시스템을 제공한다.

과제 해결 수단

[7] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 하나의 특징인 보안 IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 보안 IP 통신 서비스를 제공하는 방법은,

[8] 상기 보안 IP 통신 서비스 제공 장치는 상기 제1 단말로부터 전송되는 IP

패킷에 포함된 제1 보안 코어 IP와 제2 보안 코어 IP를 토대로, 상기 제1 단말과 제2 단말이 하나의 그룹으로 형성되어 있는지 확인하는 단계; 및 상기 제1 단말과 제2 단말이 그룹으로 형성되어 있으면, 상기 제1 단말로부터 전송된 IP 패킷을 상기 제2 단말로 전달하는 단계를 포함한다.

[9] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 보안 IP 통신 서비스 제공 장치가 단말에 보안 IP 통신 서비스를 제공하는 방법은,

[10] 상기 보안 IP 통신 서비스 제공 장치는 공중 인터넷 망에 위치한 제2 서버를 통해 통신 서비스를 이용하고자 하는 상기 단말로부터 IP 패킷을 수신하는 단계; 상기 IP 패킷에 포함되어 있는 상기 제2 서버의 IP 주소를 토대로, 상기 보안 IP 통신 서비스 제공 장치에 연결되어 있는 보안 DNS에 상기 제2 서버의 IP 주소에 대응되어 미리 저장된 제1 웹 서버의 IP 주소가 있는지 확인하는 단계; 및 상기 제1 웹 서버의 IP 주소가 있으면, 상기 보안 IP 통신 서비스 제공 장치는 제1 웹 서버를 통해 상기 제2 웹 서버에서 제공하는 통신 서비스의 정보를 수신하여 상기 단말로 전달하는 단계를 포함한다.

[11] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 단말에 보안 IP 통신 서비스를 제공하는 보안 IP 통신 서비스 제공 장치는,

[12] 소스 단말이 생성한 IP 패킷에 포함되어 있는, 상기 소스 단말의 제1 보안 액세스 IP를 제1 보안 코어 IP로 변환하는 제1 NAT; 상기 제1 NAT에서 변환된 제1 보안 코어 IP와 상기 IP 패킷에 포함되어 있는 목적지 단말의 제2 보안 코어 IP를, 외부로부터 입력되어 미리 저장되어 있는 그룹 매핑 정보에서 확인하여, 상기 소스 단말과 목적지 단말이 동일한 그룹에 포함되어 있는지 확인하는 보안 그룹 판단 장치; 및 상기 제2 보안 코어 IP를 제2 보안 액세스 IP로 변환하는 제2 NAT를 포함한다.

[13] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 단말에 보안 IP 통신 서비스를 제공하는 보안 IP 통신 서비스 제공 장치를 포함하는 보안 IP 통신 시스템은,

[14] 하나의 그룹으로 설정되어 있는 복수의 단말 각각에 할당되어 있는 보안 코어 IP들을 그룹으로 형성하여 그룹 매핑 정보를 생성하는 제어부; 및 단말에 할당된 보안 액세스 IP와 보안 코어 IP에 NAT를 실행하고, 보안 IP 통신 서비스의 이용을 위해 IP 패킷을 생성하는 소스 단말과, 상기 소스 단말이 생성한 IP 패킷을 수신할 목적지 단말이 동일한 그룹에 속해 있는지 확인하는 보안 IP 게이트웨이를 포함한다.

[15] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 단말에 보안 IP 통신 서비스를 제공하는 IP 통신 서비스 제공 장치는,

[16] IP 변경 관리 정보를 저장하고, 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 상기 IP 변경 관리 정보에 따라 다른 IP로 변환을 수행할 수 있는 IP 변경 관리부; 보안 IP 통신 서비스를 제공하기 위한 복수의 보안 IP의 주소를 포함하는 라우팅 테이블을 관리하는 라우팅 테이블 관리부; 상기 IP 변경

관리부에서 변환 또는 변환되지 않은 목적지 IP가 상기 라우팅 테이블에 포함되는지 확인하고, 확인 결과에 따라 상기 IP 패킷에 포함되어 있는 제1 소스 IP를 제2 소스 IP로 변경하는 IP 처리부; 및 상기 IP 처리부에서 변경한 제2 소스 IP와 상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP를 토대로, IP 패킷을 공중 IP 통신 또는 보안 IP 통신 중 어느 하나의 통신을 통해 제2 단말로 전송하는 통신부를 포함한다.

[17] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 IP 통신 서비스를 제공하는 방법은,

[18] 상기 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 소정의 IP 변경 관리 정보에 따라 제2 목적지 IP로 변환 여부를 결정하는 단계; 제2 목적지 IP로 변환 결정된 경우 상기 변환된 제2 목적지 IP가 라우팅 테이블에 포함되는지 확인하고, 제2 목적지 IP로 변환되지 않은 경우 상기 제1 목적지 IP가 상기 라우팅 테이블에 포함되어 있는지 확인하는 단계; 상기 확인 결과에 따라 IP 패킷에 포함된 제1 소스 IP를 제2 소스 IP로 변경하는 단계; 및 변경된 제2 소스 IP와 목적지 IP를 토대로 상기 제1 단말에서 전송한 IP 패킷을 상기 제2 단말로 보안 IP 통신 또는 공중 IP 통신 중 어느 하나의 통신으로 전송하는 단계를 포함한다.

[19] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 단말에 IP 통신 서비스를 제공하는 IP 통신 시스템은,

[20] 외부로부터 제1 IP 및 제2 IP를 할당 받고 제어 정보를 수신하며, 상기 단말로부터 전송되는 IP 패킷에 포함된 목적지 IP와, 상기 목적지 IP를 토대로 상기 제1 IP 또는 제2 IP 중 어느 하나의 IP로 변환되는 소스 IP에 따라, IP 패킷을 제1 IP 통신 또는 제2 IP 통신 중 어느 하나의 통신으로 전송할지 결정하는 IP 통신 서비스 제공 장치; 상기 IP 통신 서비스 제공 장치로 상기 제어 정보를 전달하는 제어부; 상기 IP 통신 서비스 제공 장치로 상기 제1 IP 및 제2 IP를 할당하여 제공하는 DHCP 서버; 상기 IP 통신 서비스 제공 장치가 상기 IP 패킷을 제1 통신을 통해 전송하는 것으로 결정하면, 상기 IP 패킷을 목적지 단말로 전송하는 제1 게이트웨이; 및 상기 IP 통신 서비스 제공 장치가 상기 IP 패킷을 제2 통신을 통해 전송하는 것으로 결정하면, 상기 IP 패킷을 목적지 단말로 전송하는 제2 게이트웨이를 포함한다.

발명의 효과

[21] 본 발명에 따르면 사용자 그룹을 용이하게 설정하여, 그룹에 속하지 않는 단말로부터의 접속 시도를 차단할 수 있어 안전하게 인터넷 서비스를 제공할 수 있다.

[22] 또한, 듀얼 IP인 보안 IP와 공중 IP가 모두 할당된 IP 서비스 제공 장치를 통해 공중망에서 공중 IP 통신 서비스와 보안 IP 통신 서비스를 모두 제공할 수 있다.

도면의 간단한 설명

[23] 도 1은 본 발명의 제1 실시예에 따른 보안 IP 통신 서비스를 제공하는 환경의 예시도이다.

[24] 도 2는 본 발명의 제1 실시예에 따른 보안 IP 게이트웨이의 예시도이다.

[25] 도 3은 본 발명의 제1 실시예에 따른 그룹핑된 단말 사이의 보안 IP 통신 방법에 대한 흐름도이다.

[26] 도 4는 본 발명의 제1 실시예에 따른 보안 IP 통신의 예시도이다.

[27] 도 5는 본 발명의 제2 실시예에 따른 보안 IP 통신 서비스를 제공하는 환경의 예시도이다.

[28] 도 6은 본 발명의 제3 실시예에 따른 보안 IP 통신 서비스를 제공하는 통신 시스템의 예시도이다.

[29] 도 7은 본 발명의 제3 실시예에 따른 보안 IP 라우터의 구조도이다.

[30] 도 8은 본 발명의 제3 실시예에 따른 IP 통신 방법에 대한 흐름도이다.

발명의 실시를 위한 최선의 형태

[31] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 하나의 특징인 보안 IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 보안 IP 통신 서비스를 제공하는 방법은,

[32] 상기 보안 IP 통신 서비스 제공 장치는 상기 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 보안 코어 IP와 제2 보안 코어 IP를 토대로, 상기 제1 단말과 제2 단말이 하나의 그룹으로 형성되어 있는지 확인하는 단계; 및 상기 제1 단말과 제2 단말이 그룹으로 형성되어 있으면, 상기 제1 단말로부터 전송된 IP 패킷을 상기 제2 단말로 전달하는 단계를 포함한다.

[33] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 보안 IP 통신 서비스 제공 장치가 단말에 보안 IP 통신 서비스를 제공하는 시스템은,

[34] 하나의 그룹으로 설정되어 있는 복수의 단말 각각에 할당되어 있는 보안 코어 IP들을 그룹으로 형성하여 그룹 매핑 정보를 생성하는 제어부; 및 단말에 할당된 보안 액세스 IP와 보안 코어 IP에 NAT를 실행하고, 보안 IP 통신 서비스의 이용을 위해 IP 패킷을 생성하는 소스 단말과, 상기 소스 단말이 생성한 IP 패킷을 수신할 목적지 단말이 동일한 그룹에 속해 있는지 확인하는 보안 IP 게이트웨이를 포함한다.

[35] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 단말에 IP 통신 서비스를 제공하는 IP 통신 서비스 제공 장치는,

[36] IP 변경 관리 정보를 저장하고, 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 상기 IP 변경 관리 정보에 따라 다른 IP로 변환을 수행할 수 있는 IP 변경 관리부; 보안 IP 통신 서비스를 제공하기 위한 복수의 보안 IP의 주소를 포함하는 라우팅 테이블을 관리하는 라우팅 테이블 관리부; 상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP가 상기 라우팅 테이블에

포함되는지 확인하고, 확인 결과에 따라 상기 IP 패킷에 포함되어 있는 제1 소스 IP를 제2 소스 IP로 변경하는 IP 처리부; 및 상기 IP 처리부에서 변경한 제2 소스 IP와 상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP를 토대로, IP 패킷을 공중 IP 통신 또는 보안 IP 통신 중 어느 하나의 통신을 통해 제2 단말로 전송하는 통신부를 포함한다.

[37] 상기 본 발명의 기술적 과제를 달성하기 위한 본 발명의 또 다른 특징인 IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 IP 통신 서비스를 제공하는 방법은,

[38] 상기 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 소정의 IP변경 관리 정보에 따라 제2 목적지 IP로 변환 여부를 결정하는 단계; 제2 목적지 IP로 변환 결정된 경우 상기 변환된 제2 목적지 IP가 라우팅 테이블에 포함되는지 확인하고, 제2 목적지 IP로 변환되지 않은 경우 상기 제1 목적지 IP가 상기 라우팅 테이블에 포함되어 있는지 확인하는 단계; 상기 확인 결과에 따라 IP 패킷에 포함된 제1 소스 IP를 제2 소스 IP로 변경하는 단계; 및 변경된 제2 소스 IP와 목적지 IP를 토대로 상기 제1 단말에서 전송한 IP 패킷을 상기 제2 단말로 보안 IP 통신 또는 공중 IP 통신 중 어느 하나의 통신으로 전송하는 단계를 포함한다.

발명의 실시를 위한 형태

[39] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[40] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[41] 본 명세서에서 단말(terminal)은, 이동국(Mobile Station, MS), 이동 단말(Mobile Terminal, MT), 가입자국(Subscriber Station, SS), 휴대 가입자국(Portable Subscriber Station, PSS), 사용자 장치(User Equipment, UE), 접근 단말(Access Terminal, AT) 등을 지칭할 수도 있고, 이동 단말, 가입자국, 휴대 가입자 국, 사용자 장치 등의 전부 또는 일부의 기능을 포함할 수도 있다.

[42] 이하 도면을 참조로 하여, 본 발명의 실시예에 따른 보안 IP 통신 서비스를 제공하기 위한 장치 및 방법에 대해 설명한다. 본 발명의 실시예에서는 공중 인터넷 망에서 미리 지정된 그룹간에 폐쇄적인 통신 접속을 가능하게 하는 서비스를 '보안 IP 통신 서비스'라 지칭하나 반드시 이와 같이 한정되는 것은 아니다.

[43] 도 1은 본 발명의 제1 실시예에 따른 보안 IP 통신 서비스를 제공하는 환경의 예시도이다.

[44] 도 1에 대해 설명하기 앞서, n개의 단말들과 제2 단말(20)은 하나의 그룹으로 형성되어 있으며, 제3 단말은 그룹에 포함되지 않은 단말이라 가정한다. 그룹에 포함된 n개의 단말들 각각을 제1 단말(10)이라 지칭하며, 제1 단말(10)에서 제2 단말(20)로 IP 패킷을 송신한다고 가정한다.

[45] 여기서 제1 단말(10), 제3 단말은 보안 IP 통신 서비스를 제공하는 사내 망에 위치한 개인 컴퓨터 등이 될 수 있고, 제2 단말(20)은 사내 망에 위치한 서버가 될 수 있다. 그리고 제1 단말(10)에 부여된 IP인 소스 IP는 이후 설명할 DHCP(Dynamic Host Configuration Protocol) 서버(60)에 의해 생성된 보안 IP이고, 제2 단말(20)에 부여된 IP인 목적지 IP 역시 보안 IP라 가정한다. 각각의 단말에는 일반 IP도 부여되어 있으며, DHCP 서버(60)가 보안 IP를 생성하여 부여하는 방법에 대한 상세한 설명은 생략한다.

[46] 또한, 코어(Core) 영역 즉, 그룹핑 장치(100)에서 사용되는 IP를 보안 코어 IP(Secure Core IP)라 지칭한다. 그리고 액세스 영역, 즉 제1 단말(10)과 그룹핑 장치(100) 사이, 그룹핑 장치(100)와 제2 단말(20) 사이에서 사용되는 IP를 보안 액세스 IP(Secure Access IP)라 지칭하나, 반드시 이와 같이 한정되는 것은 아니다.

[47] 제1 단말(10)이 IP 패킷을 생성하여 목적지 IP인 보안 코어 IP로 IP 통신을 시작하면, 제1 단말(10)에 연결된 L3 라우터(30)는 제1 단말(10)로부터 IP 패킷과 함께, 소스 IP인 보안 액세스 IP(Secure Access IP) 및 목적지 IP에 대응하는 보안 코어 IP도 수신한다. 여기서 제1 단말(10)은 보안 코어 IP에 대해 이미 알고 있다고 가정하며, 제1 단말(10)이 제2 단말(20)의 보안 코어 IP를 획득하는 방법은 여러 방법을 통해 수행할 수 있으므로 본 발명의 실시예에서는 상세한 설명을 생략한다.

[48] L3 라우터(30)는 제1 단말(10)에 대한 보안 액세스 IP와 제2 단말(20)에 대한 보안 코어 IP가, 미리 저장되어 있는 ACL(Access Control List)에 포함되어 있는지 확인한다. 여기서 ACL은 단말이 보안 IP 통신 서비스를 이용하기 위해 허용된 IP들에 대한 리스트로, 복수의 보안 액세스 IP들과 보안 코어 IP들에 대한 리스트가 저장되어 있다.

[49] IP 패킷에 포함된 두 개의 IP 중 적어도 하나의 IP라도 ACL에 의해 허용되지 않은 IP라면, L3 라우터(30)는 제1 단말(10)로부터 전송되는 IP 패킷을 차단하여 보안 IP 통신 서비스를 이용하지 못하도록 제어한다. L3 라우터(30)는 IP 패킷의 차단여부를 결정하는 기능 이외에도, 일반적인 L3 라우터(30)로의 기능도 수행하며 이에 대한 사항은 이미 알려진 것으로 본 발명의 실시예에서는 상세한 설명을 생략한다.

[50] L3 라우터(30)를 통과한 IP 패킷은 제1 라우터(40)로 전달되는데, 제1 라우터(40)에는 DHCP 서버(60)가 연결되어 있다. DHCP 서버(60)는 제1

단말(10)에 보안 IP 주소를 할당하는 장비로, DHCP 서버(60)의 기능이나 보안 IP 주소를 할당하는 방법은 이미 알려진 것으로 본 발명의 실시예에서는 상세한 설명을 생략한다. 그리고 제1 라우터(40)의 기능도 일반적인 라우터의 기능을 수행하므로, 본 발명의 실시예에서는 상세한 설명을 생략한다.

[51] 제1 라우터(40)를 통과한 IP 패킷은 인터넷 망에 위치한 보안 IP 게이트웨이(110)로 유입된다. 보안 IP 게이트웨이(110)는 보안 액세스 IP를 보안 코어 IP로 변환하거나, 보안 코어 IP를 보안 액세스 IP로 변환하는 NAT(Network Address Translation)를 수행한다. 또한, 보안 IP 게이트웨이(110)는 미리 그룹핑되어 저장되어 있는 그룹 매핑 정보를 토대로 소스 IP에 대한 제1 단말(10)과 목적지 IP를 갖는 제2 단말(20)이 하나의 그룹에 포함되어 있는지를 확인한다.

[52] 그리고 보안 IP 게이트웨이(110)는 그룹으로 설정되지 않은 단말에서 생성된 IP 패킷이 목적지 IP를 갖는 단말에 전달되지 않도록 차단하며, 이 외에도 일반적인 게이트웨이의 기능도 수행한다. 이러한 보안 IP 게이트웨이(110)의 구조는 이후 설명한다.

[53] 보안 IP 게이트웨이(110)는 CMS(Control & Management System)(이하, 설명의 편의를 위하여 '제어부'라 지칭함)(120)과 연동한다. 제어부(120)는 미리 그룹으로 설정된 단말들에 대한 그룹 매핑 정보를 생성하여 보안 IP 게이트웨이(110)에 제공한다. 그룹 매핑 정보는 그룹 식별 정보, 그룹에 속한 단말들 각각의 보안 코어 IP 정보들을 포함한다.

[54] 이를 위해 제어부(120)는 외부로부터 그룹에 포함되는 단말들 각각에 설정되어 있는 보안 코어 IP 정보를 수신하여 그룹으로 생성하며, 그룹 생성 방법은 이미 알려진 사항으로 상세한 설명을 생략한다. 본 발명의 실시예에서는 제어부(120)가 물리적으로 분리되어 보안 IP 게이트웨이(110)와 연동하는 것을 예로 하여 설명하나, 제어부(120)의 기능을 보안 IP 게이트웨이(110)가 수행하도록 프로그램으로 보안 IP 게이트웨이(110)에 설치될 수도 있다. 이 경우에는 외부로부터 수동으로 그룹 매핑 정보가 보안 IP 게이트웨이(110)로 입력된다.

[55] 보안 IP 게이트웨이(110)는 제2 라우터(50)와 연결되어 있으며, 제2 라우터(50)를 거친 IP 패킷은 목적지인 제2 단말(20)로 전달된다. 제1 라우터(40)와 제2 라우터(50)의 기능에는 일반적인 라우터 기능을 포함하여 여러 기능들을 수행할 수 있으며, 이에 대해서는 본 발명의 실시예에서는 상세한 설명을 생략한다.

[56] 이상의 환경에서 그룹핑 장치(100)에 포함되어 있는 보안 IP 게이트웨이(110)의 예에 대해 도 2를 참조로 설명한다.

[57] 도 2는 본 발명의 제1 실시예에 따른 보안 IP 게이트웨이의 예시도이다.

[58] 도 2에 도시된 바와 같이 보안 IP 게이트웨이(110)는 제1 NAT(111), 보안 그룹 판단 장치(112) 및 제2 NAT(113)를 포함한다.

[59] 제1 NAT(111)는 제1 라우터(40)로부터 IP 패킷을 수신하면, 수신한 IP 패킷을 전송한 제1 단말(10)에 대한 소스 IP인 제1 보안 액세스 IP 주소를 NAT를 실행하여 제1 보안 코어 IP로 변환 생성한다.

[60] 보안 그룹 판단 장치(112)는 제1 보안 코어 IP, 제2 보안 코어 IP 및 패킷을 포함하는 IP 패킷을 제1 NAT(111)로부터 수신하면, 제1 보안 코어 IP에 대한 그룹 매핑 정보를 확인하여 소스 단말인 제1 단말(10)과 목적지 단말인 제2 단말(20)이 동일한 그룹에 그룹핑된 단말인지 확인한다. 그룹 매핑 정보는 제어부(120)로부터 수신하여 보안 그룹 판단 장치(112)에 미리 저장되어 있는 것으로, 그룹 매핑 정보에는 그룹에 포함되어 있는 복수의 단말들 각각에 대한 보안 코어 IP와 그룹 매핑 식별 정보가 포함되어 있다.

[61] 보안 그룹 판단 장치(112)는 소스측 단말이 그룹에 형성되어 있지 않은 것으로 확인하면, 목적지 단말로 전송하고자 하는 IP 패킷의 전송을 차단한다.

[62] 제2 NAT(113)는 보안 그룹 판단 장치(112)를 통과한 IP 패킷을 수신하면, IP 패킷에 포함된 제2 보안 코어 IP를 제2 보안 액세스 IP로 NAT를 수행한다. 제1 NAT(111)와 제2 NAT(113)에서 NAT를 수행할 때 변환되는 보안 코어 IP와 보안 액세스 IP는 각각의 IP가 변환되어 생성되는 IP가 결정되어 있는 것을 예로 하여 설명한다.

[63] 본 발명의 실시예에서는 보안 IP 게이트웨이(110) 내에 제1 NAT(111), 보안 그룹 판단 장치(112) 및 제2 NAT(113)가 포함되는 형태로 예를 들어 설명하나, 제1 NAT(111), 보안 그룹 판단 장치(112) 및 제2 NAT(113)가 보안 IP 게이트웨이(110)에 포함되지 않고 물리적으로 독립된 세 개의 구성 요소로 그룹핑 장치(100)에 포함될 수도 있다. 이 경우, 물리적으로 독립된 보안 그룹 판단 장치(112)는 제어부(120)로부터 그룹 매핑 정보를 수신하여 소스측 단말과 목적지 단말이 동일한 그룹에 포함되어 있는지 확인하게 된다.

[64] 또한, 본 발명의 실시예에서는 제1 NAT(111), 보안 그룹 판단 장치(112) 및 제2 NAT(113)가 하드웨어적인 구성 요소로 도시하였으나, 프로그램 형태로 구현되어 기능으로 수행될 수도 있다. 프로그램 형태로 구현될 경우, 본 발명의 실시예에서와 같이 보안 IP 게이트웨이(110)가 NAT 기능과 보안 그룹 판단 기능을 수행할 수도 있다. 또는 보안 IP 게이트웨이(110)가 아닌 다른 구성 요소들에 해당 기능을 수행하도록 프로그램이 구동될 수도 있다.

[65] 만약 기능으로 임의의 구성 요소에 설치되는 경우에는, 보안 그룹 판단 기능을 수행하기 위해, 임의의 구성 요소는 제어부(120)로부터 그룹 매핑 정보와 그룹 정책 등을 수신할 수도 있다.

[66]

[67] 이상에서 설명한 환경에서 그룹핑된 단말 사이에 IP 통신을 수행하는 방법에 대해 도 3을 참조로 설명한다. 도 3에서는 보안 IP 통신을 위해 필요한 구성 요소들만을 도시하였으나, 반드시 이와 같이 한정되는 것은 아니다. 또한 제1 단말(10)에 할당된 소스 IP를 제1 보안 액세스 IP, 제1 보안 액세스 IP가 NAT를

실행하여 생성되는 IP를 제1 보안 코어 IP라 지칭한다. 그리고 제2 단말(200)에 할당된 목적지 IP를 제2 보안 액세스 IP, 제2 보안 액세스 IP 주소에 NAT를 실행하여 생성되는 IP를 제2 보안 코어 IP라 지칭한다.

[68] 도 3은 본 발명의 제1 실시예에 따른 그룹핑된 단말 사이의 보안 IP 통신 방법에 대한 흐름도이다.

[69] 도 3에 도시된 바와 같이, 제1 단말(10)이 제1 IP 패킷을 생성하고, 패킷을 전송할 목적지 단말인 제2 단말(20)의 제2 보안 코어 IP를 이용하여 L3 라우터(30)로 전송한다(S100). 이때, 제1 IP 패킷에는 제2 단말(20)로 전송할 패킷, 제1 단말(10)의 제1 보안 액세스 IP 및 제2 단말(20)의 제2 보안 코어 IP가 포함되어 있다.

[70] L3 라우터(30)는 S100 단계에서 수신한 제1 IP 패킷 중, 제1 보안 액세스 IP와 제2 보안 코어 IP가 사전에 보안 IP 통신을 위해 허가된 IP인지, ACL에 설정되어 있는지 확인한다(S101). L3 라우터(30)에 저장되어 있는 ACL에는 보안 IP 통신을 위해 사전에 허가된 복수의 IP 리스트들이 저장되어 있으며, 이 외의 IP의 경우에는 보안 IP 통신 서비스를 이용하지 못하도록 제어하고 있다.

[71] 따라서, S101 단계에서 확인한 결과 제1 보안 액세스 IP와 제2 보안 코어 IP 중 적어도 하나의 IP가 ACL에 의해 설정되지 않은 것으로 확인하면, L3 라우터(30)는 제1 IP 패킷의 통과를 차단한다. 그러나, 제1 보안 액세스 IP와 제2 보안 코어 IP가 모두 ACL에 설정된 IP에 해당하면, L3 라우터(30)는 제1 IP 패킷을 보안 IP 게이트웨이(110)로 전달한다(S102).

[72] 보안 IP 게이트웨이(110)의 제1 NAT(111)는 S102 단계에서 수신한 제1 IP 패킷의 제1 보안 액세스 IP를 NAT 실행을 통해 제1 보안 코어 IP로 변환한다(S103). S103 단계에서 변환된 제1 보안 코어 IP는 IP 패킷에 포함되며, 이렇게 생성된 제2 IP 패킷이 보안 그룹 판단 장치(112)로 전달된다(S104).

[73] 보안 그룹 판단 장치(112)는 제2 IP 패킷에 포함되어 있는 제1 보안 코어 IP와 제2 보안 코어 IP가 하나의 그룹에 포함되어 있는지 그룹 매핑 정보를 확인한다(S106). 만약 제1 보안 코어 IP가 할당된 단말(10)이 어떠한 그룹에도 속해 있지 않거나, 제1 보안 코어 IP가 그룹에 속해 있으나 해당 그룹에 제2 보안 코어 IP가 부여된 단말(20)이 속해있지 않은 것으로 확인하면, 보안 그룹 판단 장치(112)는 제2 단말(20)로 전송되던 IP 패킷을 차단한다.

[74] S106 단계에서 확인한 결과, 제1 보안 코어 IP와 제2 보안 코어 IP가 동일한 그룹에 속해 있는 것으로 설정되어 있다면, 보안 그룹 판단 장치(112)는 제2 IP 패킷을 제2 NAT(113)로 전달한다(S107). 제2 NAT(113)는 제2 IP 패킷에 포함되어 있는 제2 보안 코어 IP에 NAT를 실행하여 제2 보안 액세스 IP를 변환한다(S108).

[75] S108 단계에서 생성된 제2 보안 액세스 IP는 제2 보안 코어 IP 대신 IP 패킷에 포함되며, 제2 보안 액세스 IP를 포함하는 패킷은 제3 IP 패킷으로 생성된다. 생성된 제3 IP 패킷은 제2 보안 액세스 IP가 할당되어 있는 제2 단말(20)로

전송된다(S109).

[76] 제2 단말(20)은 S109 단계에서 전송된 제3 IP 패킷을 수신하여, 제1 단말(10)로부터 전송된 패킷을 확인한다(S110). 제2 단말(20)이 패킷을 수신하였음을 알리는 응답 절차는 상기 S100 단계 내지 S109 단계에서 설명한 절차를 역으로 실행하게 된다.

[77] 응답 절차에서는 제2 단말(20)의 제2 보안 액세스 IP가 소스 IP가 되고, 제1 단말(10)의 제1 보안 코어 IP가 목적지 IP가 된다. 소스 IP인 제2 보안 액세스 IP는 제2 NAT(113)에서 제2 보안 코어 IP로 변환되고, 목적지 IP인 제1 보안 코어 IP는 제1 NAT(111)에서 제1 보안 액세스 IP로 변환된다. 이 외의, 다른 절차는 상기에서 설명한 절차와 동일하다.

[78]

[79] 이상에서 설명한 보안 IP 통신에 대해 도 4를 참조로 예를 들어 설명한다. 도 4에서 언급되는 IP 주소나 변환되어 생성된 IP는 하나의 예로, 반드시 이와 같이 한정되는 것은 아니다.

[80] 도 4는 본 발명의 제1 실시예에 따른 보안 IP 통신의 예시도이다.

[81] 도 4에 도시된 바와 같이, 제1 단말에 할당되어 있는 제1 보안 IP는 169.208.0.1이고, 제2 단말에 할당되어 있는 제2 보안 IP는 39.28.0.3이라 가정한다. 그리고, L3 라우터(30)에 설정되어 있는 ACL에 포함되어 있는 보안 IP는 169.208.0.1에서부터 169.208.0.254까지의 보안 액세스 IP와, 이들 보안 액세스 IP가 변환된 보안 코어 IP인 39.28.0.1에서부터 39.28.0.254까지의 IP들에 해당한다. 이 외의 IP를 소스 IP나 목적지 IP로 이용하는 경우, L3 라우터(30)에서 IP 패킷이 차단된다.

[82] 보안 IP 게이트웨이(110)에는 보안 액세스 IP와 보안 코어 IP 상호 변환에 따라 변환되어 생성된 IP들이 지정되어 있다. 즉, 보안 액세스 IP가 169.208.0.1인 경우 이를 NAT 적용할 경우 39.28.0.1의 보안 코어 IP로 변환된다. 보안 코어 IP는 보안 액세스 IP로부터만 생성되는 것이 아니라 공중 IP 통신을 위해 사용되는 일반 IP로부터도 변환될 수 있다.

[83] 즉, 도 4에 나타나 있는 바와 같이, 공중 IP가 2.2.2.2인 경우, 이에 NAT를 실행할 경우 39.28.0.2의 보안 코어 IP로 변환되도록 설정되어 있다. 이와 반대로, 보안 코어 IP에 NAT를 실행하면 보안 액세스 IP로 변환되기도 한다.

[84] 또한, 보안 IP 게이트웨이(110)에는 제어부(120)에서 설정한 그룹 매핑 정보도 저장, 관리한다. 그룹 매핑 정보에는 그룹을 형성하는 복수의 단말들 각각에 할당되어 있는 복수의 보안 코어 IP들과, 그룹 식별 정보가 포함되며, 도 4에서는 그룹 식별 정보를 #01이라 가정하였으며, 39.28.0.1과 39.28.0.2의 보안 코어 IP를 갖는 두 대의 단말이 하나의 그룹을 형성하는 것을 나타내었다.

[85] 도 4에 도시된 제1 단말(10)이 제2 단말(20)로 패킷을 전송하고자 할 때, 제1 단말(10)은 제2 단말(20)의 보안 코어 IP인 39.28.0.2로 IP 패킷을 생성하여 통신을 시작한다. IP 패킷에는 제2 단말(20)로 전송할 패킷, 제1 단말(10)의 보안 액세스

IP인 169.208.0.1, 제2 단말(20)의 보안 코어 IP인 39.28.0.2가 포함되어 있다.

[86] L3 라우터(30)는 제1 단말(10)에서 전송된 IP 패킷에서 두 개의 IP 정보인 169.208.0.1과 39.28.0.2를 확인하여 ACL에 설정되어 있는지 확인한다. 두 IP 모두 L3 라우터(30)에 설정되어 있으므로, L3 라우터(30)는 IP 패킷을 보안 IP 게이트웨이(110)로 전달한다.

[87] 보안 IP 게이트웨이(110)의 제1 NAT(111)는 IP 패킷에 포함된 제1 단말(10)의 보안 액세스 IP인 169.208.0.1을 보안 코어 IP인 39.28.0.1로 변환한다. 그리고, 변환된 39.28.0.1과 목적지 단말 즉, 제2 단말(20)에 대한 보안 코어 IP인 39.28.0.2가 그룹을 형성하고 있는지 확인한다. 그룹 매핑 정보 #01에 따르면, 두 단말은 그룹을 형성하고 있으므로, IP 패킷이 제2 단말(20)로 전달되도록 한다.

[88] 이를 위해, 제2 NAT(113)는 IP 패킷에 포함되어 있는 제2 단말(20)의 보안 코어 IP 39.28.0.2에 NAT를 실행하여 목적지 IP인 2.2.2.2로 변환한다. 그리고 2.2.2.2를 IP 주소로 갖는 제2 단말(20)로 IP 패킷이 전달된다.

[89]

[90] 한편, 도 4의 제3 단말로 도시한 단말이, 그룹으로 형성된 제2 단말로 보안 IP 통신을 시도한다고 가정한다. 제3 단말은 그룹에 포함되지 않은 단말이며, 제 3 단말의 보안 액세스 IP는 169.208.0.3이고, NAT 실행 시 변경되는 보안 코어 IP는 39.28.0.3이라고 가정한다.

[91] 이때, 두 가지의 형태로 제3 단말이 IP 패킷의 전송을 시도할 수 있다. 먼저 ①에 나타낸 바와 같이, 소스 IP를 169.208.0.3으로 하고 목적지 IP를 공중 IP인 2.2.2.2로 하여 통신을 시작한다고 가정한다.

[92] 그러면, 생성된 IP 패킷에는 목적지 단말로 전송될 패킷과 169.208.0.3 및 2.2.2.2가 포함되어 있으므로, L3 라우터(30)는 저장되어 있는 ACL를 통해 두 IP가 보안 IP 통신을 위해 허용된 IP인지 확인한다. 이 경우 소스 IP는 허용된 IP이나, 목적지 IP인 2.2.2.2는 ACL에 따라 보안 IP 통신에 허용되지 않은 IP이므로, L3 라우터(30)는 제3 단말이 생성한 IP 패킷을 차단한다.

[93] 한편, ②에 나타낸 바와 같이, 소스 IP를 169.208.0.3으로 하고 목적지 IP를 보안 코어 IP인 39.28.0.2로 하여 통신을 시도한다고 가정한다. 그러면, L3 라우터(30)는 두 IP인 169.208.0.3과 39.28.0.2가 모두 ACL을 통해 허용된 IP이므로, 제3 단말이 생성한 IP 패킷을 보안 IP 게이트웨이(110)로 전달한다.

[94] 그러나, 보안 IP 게이트웨이(110)가 그룹 매핑 정보를 확인하는 과정에서 제3 단말이 그룹에 속하지 않은 단말인 것을 확인한다. 즉, 제1 NAT(111)를 통해 제3 단말의 소스 IP가 보안 코어 IP인 39.28.0.3으로 변경되면, IP 주소가 39.28.0.2인 그룹에는 39.28.0.3의 IP 주소를 갖는 단말이 속해 있지 않음을 알 수 있다. 따라서, 보안 IP 게이트웨이(110)는 전송되는 IP 패킷을 차단하게 된다.

[95] 이와 같이, 그룹에 속하지 않은 단말이 IP 통신을 시도하거나, ACL에 허용되지 않은 IP로 통신을 시도하는 경우 모두 L3 라우터(30) 또는 보안 IP 게이트웨이(110)에서 차단된다.

[96] 이 외에도 제3 단말의 사용자가 그룹으로 형성된 제1 단말의 사용자이나 외부에서 보안 IP 통신을 통해 그룹으로 설정된 제2 단말(20)로 패킷을 전송하고자 하는 경우가 있을 수 있다. 이때, 제3 단말의 소스 IP는 169.208.0.3이나 사용자가 제1 단말에 할당된 169.208.0.1로 IP 설정을 변경한 뒤 IP 패킷을 전송할 수도 있다.

[97] 이 경우, 시스템 설계에 따라 보안 IP 게이트웨이(110)에 저장된 그룹 매핑 정보에 보안 코어 IP 정보, 그룹 식별 정보 이외에 단말에 할당된 고유 식별 정보도 포함하여 관리하도록 할 수 있다.

[98] 그리고, 보안 IP 게이트웨이(110)는 제3 단말로부터 전송되는 변경된 보안 액세스 IP와 더불어 제3 단말의 고유 식별 정보도 함께 수신하여, 미리 저장된 정보와 비교한 후 IP 패킷을 차단하도록 설계할 수 있다. 또는 보안 IP 게이트웨이(110)가 제3 단말과의 통신을 통해 사용자 인증을 수행한 후, 해당 사용자가 제1 단말(10)의 사용자임을 확인하면 제2 단말(20)로 전송할 IP 패킷을 전송할 수 있도록 할 수도 있다. 보안 액세스 IP가 변경된 단말을 소스 단말로 하는 예에 대해서는 상세한 설명을 생략한다.

[99]

[100] 상기에서는 보안 IP 통신 서비스를 제공함에 있어 그룹에 속한 단말들 사이의 보안 IP 통신 서비스 제공 방법에 대해 설명하였다. 다음은 보안 IP 통신 서비스 제공 장치를 이용하여 폐쇄망에서 서비스를 제공하는 것과 같은 효과를 얻도록 하는 또 다른 실시예에 따라 보안 IP 통신 서비스를 제공하는 방법에 대해 도 5 및 도 6을 참조로 설명한다.

[101] 도 5는 본 발명의 제2 실시예에 따른 보안 IP 통신 서비스를 제공하는 환경의 예시도이다.

[102] 도 5에 도시된 바와 같이, 본 발명의 제2 실시예에 따라 보안 IP 통신 서비스를 제공하는 환경은 상기 도 1에서 설명한 환경과 유사하다. 다만, 도 5에서는 보안 IP 게이트웨이(110)에 보안 DNS(130), 사내 웹 서버(140), 기업 라우터(70), 프록시 서버(80) 및 기업 서버(90)가 추가로 연동한다.

[103] 보안 DNS(130)는 단말(10)이 통신 서비스를 이용하기 위하여 접속하는 주소를 사내 웹 서버(140)로 이동하도록, 접속 주소와 사내 웹 서버(140)의 IP 주소를 저장한다. 그리고 보안 IP 게이트웨이(110)로 해당 주소가 올라올 때, 사내 웹 서버(140)로 접속되도록 제어한다

[104] 사내 웹 서버(140)는 보안 IP 게이트웨이(110)로부터 웹 접속 주소를 수신하면, 해당 웹 접속 주소에서 통신 서비스를 제공하는 기업 서버(90)로부터 정보를 수신한다. 이때, 프록시 서버(80)와 기업 라우터(70)를 통해서 기업 서버(90)로부터 전송되는 정보를 보안 IP 게이트웨이(110)가 수신하여 사내 웹 서버(140)로 전달한다. 그리고, 사내 웹 서버(140)는 수신한 정보를 보안 IP 게이트웨이(110)를 통해 단말(10)의 사용자에게 제공한다.

[105] 이 외에 보안 DNS(130), 사내 웹 서버(140), 기업 라우터(70), 프록시 서버(80) 및

기업 서버(90)의 기능은 일반적인 DNS, 웹 서버, 라우터, 프록시 서버의 기능과 동일하므로, 본 발명의 실시예에서는 상세한 설명을 생략한다. 즉, 단말(10)에서 보안 IP 게이트웨이(110)까지 IP 패킷이 전송되는 과정은 상기 본 발명의 제1 실시예에서 설명한 절차와 동일하게 수행된다. 이때 제2 단말(10)은 도 5의 사내 웹 서버(140)가 될 수 있다.

[106] 이와 같이, 보안 IP 통신 서비스를 이용하기 위해 통신 환경에 위치한 단말(10)이 사외에서 제공하는 서비스를 이용하기 위해 접속을 시도하더라도, 접속 시도에 따른 패킷을 사외로 내보내지 않더라도 사외의 정보를 사내 웹 서버를 통해 확인할 수 있도록 한다. 또한, 미리 설정된 시간(예를 들어, 지정된 근무시간 등)에 사내 단말을 이용하여 외부의 사이트에 접속을 방지하는 등의 폐쇄적인 통신 서비스를 제공할 수도 있다.

[107]

[108] 이와 같이 폐쇄적인 통신 서비스를 제공하는 환경에서 보안 IP 통신 서비스를 제공하는 방법에 대해 예를 들어 설명하면 다음과 같다.

[109] 임의의 기업 내 사용자가 단말(10)을 이용하여 사외 기업 서버(90)에서 제공하는 통신 서비스를 이용하고자 한다고 가정한다. 이때, 사용자는 www.abc.com이라는 인터넷 주소를 입력하여, 해당 웹 서버인 기업 서버(90)에서 제공하는 정보를 획득하고자 한다고 가정하며, www.abc.com에 대한 IP 주소는 202.175.1.1이라 가정한다.

[110] 그리고 보안 DNS(130)에는 IP 통신을 위해 접속을 시도하는 사내 단말이 목적지 IP 주소를 202.175.1.1로 하여 IP 패킷을 전송하는 경우에는, 해당 주소에서 통신 서비스를 제공하는 기업 서버(90)로 단말이 접속되지 않고 사내 웹 서버(140)로 접속되도록 사내 웹 서버(140)의 IP 주소인 39.28.0.5가 202.175.1.1과 함께 저장된다.

[111] 즉, 보안 IP 게이트웨이(110)는 단말(10)로부터 202.175.1.1을 목적지로 하는 IP가 전달되면, 보안 DNS(130)에 의해 설정된 주소가 있는지 확인한다. 그리고 설정 주소가 있으면 202.175.1.1이 목적지인 기업 서버(90)로 IP 패킷을 전달하지 않고 사내 웹 서버(140)로 IP 패킷을 전달한다.

[112] 사내 웹 서버(140)는 보안 IP 게이트웨이(110)로부터 전달된 IP 패킷으로부터 목적지 주소를 확인한 후, 사내 웹 서버(140)가 목적지 주소인 기업 서버(90)로부터 정보를 수신하여 단말(10)에 제공한다. 이와 같이 보안 IP 통신 서비스를 제공하는 환경 내의 단말(10)이 일반적인 망에 연결된 서버로부터 제공하는 통신 서비스를 이용하기 위하여 IP 패킷을 생성한다 하더라도, 패킷이 외부로 나가지 않은 채 외부의 정보를 사내 웹 서버를 통해 확인할 수 있다.

[113]

[114] 다음은 본 발명의 또 다른 실시예에 따른 보안 IP 통신 서비스를 제공하는 장치 및 방법에 대해 설명한다. 본 발명의 또 다른 실시예에서는 공중 인터넷 망에서 단말에 폐쇄적인 통신 서비스를 제공하는 서비스를 '보안 IP 통신 서비스'라

지칭하나 반드시 이와 같이 한정되는 것은 아니다.

[115] 그리고 본 발명의 실시예에서는 IP의 종류에 따라 공중 인터넷 망에서 IP 통신을 통해 IP 패킷을 전송하는 데 사용되는 IP를 '공중 IP'라 지칭한다. 그리고 보안 IP 통신을 통해 IP 패킷을 전송하는 데 사용되는 IP를 '보안 IP'라 지칭한다.

[116]

[117] 도 6은 본 발명의 제3 실시예에 따른 보안 IP 통신 서비스를 제공하는 통신 시스템의 예시도이다.

[118] 도 6에 도시된 바와 같이 보안 IP 통신 서비스를 제공하기 위한 환경은, 제1 단말(10')이 IP 통신을 위해 IP 패킷을 목적지 단말인 제2 단말(20')로 전송한다고 가정한다. 여기서 제1 단말(10')은 IP 패킷을 전송하기 위하여 보안 IP 라우터(200)로 IP의 할당을 요청한다.

[119] 그리고 제1 단말(10')이 전송한 IP 패킷에는 제1 단말(10')의 소스 IP, 제2 단말(20')의 목적지 IP 및 패킷이 포함되어 있다. 제1 단말(10')은 제2 단말(20')에 대한 목적지 IP에 대해 이미 알고 있다고 가정하며, 제1 단말(10')이 목적지 IP를 획득하는 방법은 여러 방법을 통해 수행할 수 있으므로 본 발명의 실시예에서는 상세한 설명을 생략한다. 그리고 목적지 IP는 DHCP(Dynamic Host Configuration Protocol) 서버(60')가 제2 단말(20')의 공중 IP 또는 공중 IP를 통해 생성한 보안 IP 중 어느 하나이며, DHCP 서버(60')가 보안 IP를 생성하여 단말에 제공하는 방법의 상세한 설명은 생략한다.

[120] 보안 IP 라우터(200)는 CMS(Control & Management System)(이하, 설명의 편의를 위하여 '제어부'라 지칭함)(400), 제1 단말(10'), DHCP 서버(60'), 게이트웨이(500) 및 보안 IP 게이트웨이(300)와 연동하며, 제어부(400)로부터 제어 정보를 수신하여 갱신한다. 여기서 제어 정보는 IP 변경 관리 정보, 라우팅 테이블 정보 그리고 보안 정책을 포함한다.

[121] 여기서 IP 변경 관리 정보는, 제1 단말(10')이 IP 패킷의 전송을 시도할 때, IP 패킷에 포함된 목적지 IP를 확인하여 다른 IP로 변경할 지 여부를 결정하기 위한 기준 정보이다. 즉, IP 패킷에 포함된 목적지 IP가 IP 변경 관리 정보에 의해 미리 설정되어 있는 복수의 특정 목적지 IP 중 하나인 경우, 목적지 IP를 IP 변경 관리 정보에 따라 변경하여 변경 목적지 IP를 생성하도록 한다. 이를 위해, IP 변경 관리 정보는 복수의 IP들 중 미리 설정한 복수의 특정 IP들과, 특정 IP들에 NAT를 실행하여 변경할 변경 IP들이 포함되어 있다.

[122] 라우팅 테이블 정보는 보안 IP 통신을 통해 IP 패킷을 전송하도록 미리 설정되어 있는 복수의 보안 IP들의 정보가 포함되어 있다.

[123] 보안 정책은 사전에 미리 설정되어 있는 통신 차단 대상 정보(예를 들어, IP, 포트(port) 또는 프로토콜 정보 등)를 포함하고 있다. 통신 차단 대상 정보로 설정되어 있는 IP를 통해 IP 패킷의 전송이 시도되는 경우, 통신이 차단되도록 제어하는 기준 정보이다.

[124] 그리고 보안 IP 라우터(100)는 제1 단말(10')로부터 전송된 IP 패킷에 포함된

목적지 주소를 제어 정보와 비교한 후, NAT(Network Address Translation)를 실행하여 목적지 IP를 변경한다.

[125] 또한 보안 IP 라우터(200)는 IP 패킷을 생성한 제1 단말(10')의 소스 IP나 목적지 IP 등을 미리 저장되어 있는 보안 정책과 비교하여, IP 패킷을 전송하기 위한 통신을 차단할지 여부를 결정하기도 한다. 그리고, 보안 IP 라우터(200)는 소스 IP의 종류(공중 IP 또는 보안 IP)나 목적지 IP의 종류에 따라 공중망을 이용하여 IP 패킷이 전달되도록 라우팅하거나, 보안 IP 게이트웨이를 통해 IP 패킷이 전달되도록 라우팅한다.

[126] 또한, 보안 IP 라우터(200)는 DHCP 서버(60')로 보안 IP 라우터(200) 자신에 대한 IP 할당을 요청하거나, 보안 IP 라우터(200)가 제1 단말(10')의 IP를 할당할 수도 있다. 그리고 보안 IP 라우터(200)는 일반적인 라우터의 기능도 수행할 수 있으며, 본 발명의 실시예에서는 상세한 설명을 생략한다. 이러한 보안 IP 라우터(200)를 본 발명의 실시예에서는 IP 통신 서비스 제공 장치라 지칭하며, 보안 IP 라우터(200)의 구조는 도 7을 참조로 이후 설명한다.

[127] 보안 IP 라우터(200)를 통과한 IP 패킷은 보안 IP 게이트웨이(300) 또는 게이트웨이(500) 중 어느 하나로 전달된다. 즉, 제1 단말(10')에 공중 IP 통신 서비스를 제공하는 경우에는 게이트웨이(500)로 IP 패킷을 전달하고, 제1 단말(10')에 보안 IP 통신 서비스를 제공하는 경우에는 보안 IP 게이트웨이(300)로 IP 패킷을 전달한다.

[128] DHCP 서버(60')는 보안 IP 라우터(200)와 연결되어 있으며, 보안 IP 라우터(200)에 대한 보안 IP와 공중 IP를 할당한다. DHCP 서버(60')가 보안 IP 주소와 공중 IP 주소를 할당하는 방법은 여러 방법을 통해 할당할 수 있으므로 본 발명의 실시예에서는 상세한 설명을 생략한다.

[129] 보안 IP 게이트웨이(300)는 공중 인터넷 망에서 폐쇄적인 통신 서비스를 제공하는 게이트웨이로, 일반적인 게이트웨이의 기능뿐만 아니라 폐쇄적인 통신 서비스를 제공하기 위한 별도의 기능을 수행한다. 이를 위해, 보안 IP 게이트웨이(300)로 전달되는 IP 패킷은, IP 패킷을 생성한 제1 단말(10')의 소스 IP가 보안 IP인 경우, 또는 보안 IP 라우터(200)에서 확인한 보안 정책을 토대로 보안 IP 게이트웨이(300)로 전달되는 것을 예로 하여 설명하나, 반드시 이와 같이 한정되는 것은 아니다.

[130] 제어부(400)는 보안 IP 게이트웨이(300) 및 보안 IP 라우터(200)와 연동하며, 보안 IP 라우터(200)로 IP 변경 관리 정보와 보안 정책, 그리고 라우팅 테이블 정보를 제공한다. IP 변경 관리 정보, 보안 정책 그리고 라우팅 테이블 정보는 미리 설정된 주기로 보안 IP 라우터(200)에 전달하는 것을 예로 하여 설명하나, 반드시 이와 같이 한정되는 것은 아니다.

[131] 게이트웨이(500)는 보안 IP 라우터(200) 및 제2 단말(20')과 연결되어 있으며, 보안 IP 라우터(200)로부터 전달되는 IP 패킷을 공중 인터넷 망을 통해 제2 단말(20')로 전달한다. 이를 위해, 게이트웨이(500)로 전달되는 IP 패킷은, IP

패킷을 생성한 제1 단말(10')의 소스 IP가 공중 IP인 경우 또는 보안 IP 라우터(200)에서 확인한 정책에 따라 공중 IP 통신을 통해 IP 패킷을 전달하는 것으로 결정한 경우 게이트웨이(500)로 전달되는 것을 예로 하여 설명하나, 반드시 이와 같이 한정되는 것은 아니다. 게이트웨이(500)의 기능은 이미 알려진 사항으로, 본 발명의 실시예에서는 상세한 설명을 생략한다.

[132] 제2 단말(20')은 보안 IP 게이트웨이(300) 또는 게이트웨이(500) 중 어느 하나의 게이트웨이를 통해 전송되는 IP 패킷을 수신한다.

[133]

[134] 이상에서는 보안 IP 통신을 공중망에서 제공하기 위해 필요한 구성 요소들만 도시하였으며, 도 6에 도시되지 않은 구성 요소들을 더 포함할 수 있다. 이상의 환경에서 보안 IP 라우터(200)의 구조에 대해 도 7을 참조로 설명한다.

[135] 도 7은 본 발명의 제3 실시예에 따른 보안 IP 라우터의 구조도이다.

[136] 도 2에 도시된 바와 같이, 보안 IP 라우터(200)는 IP 주소 요청부(201), IP 주소 할당부(202), IP 변경 관리부(203), 라우팅 테이블 관리부(204), IP 처리부(205), 보안 정책 관리부(206) 및 통신부(207)를 포함한다.

[137] IP 주소 요청부(201)는 DHCP 서버(60')로 보안 IP 라우터(200) 자신의 IP의 할당을 요청한다. 그리고 DHCP 서버(60')로부터 할당된 IP를 수신하는데, DHCP 서버(60')에서 할당된 IP는 공중 IP와 보안 IP를 포함한다.

[138] IP 주소 할당부(202)는 제1 단말(10')로부터 제1 단말(10')에 대한 IP 할당을 요청받으면, DHCP 서버(60')와 같이 미리 정해진 규칙(Rule)에 의해 IP를 할당하여 준다. 제1 단말(10')에 할당되는 IP는 사설 IP 인 것을 예로 하여 설명하며, 제1 단말(10')은 할당된 사설 IP를 이용하여 보안 IP 라우터(200)로 IP 패킷을 전송한다. 그리고, IP 주소 할당부(202)가 제1 단말(10')에 대한 IP를 할당하는 방법 역시 여러 방법을 통해 수행될 수 있으므로 본 발명의 실시예에서는 어느 하나의 방법으로 한정하여 설명하지 않는다.

[139] IP 변경 관리부(203)는 제어부(400)로부터 미리 설정된 주기에 따라 전송되는 IP 변경 관리 정보를 수신하여 갱신, 저장한다. 그리고 제1 단말(10')로부터 전송이 시도되는 IP 패킷에 포함되어 있는 목적지 IP를 확인하고, 확인한 목적지 IP가 제어 정보에 따라 변환 대상인 IP인지 확인한다.

[140] IP 변경 관리 정보에는 미리 설정된 복수의 특정 IP들과, 특정 IP들에 NAT를 실행하여 변경할 변경 IP들이 포함되어 있다. 따라서, IP 변경 관리부(203)는 목적지 IP가 특정 IP에 해당하는지 확인하고, IP 패킷에 포함되어 있는 목적지 IP가 특정 IP에 해당하지 않는다면, 목적지 IP를 변환하지 않는다.

[141] 그러나, 특정 IP에 해당한다면 목적지 IP에 NAT를 실행하여 변경 목적지 IP로 변환한다. 여기서 IP 변경 관리부(203)를 통해 변경되는 목적지 IP는 공중 IP일 수도 있고 보안 IP일 수도 있다. 본 발명의 실시예에서는 설명의 편의를 위하여, IP 패킷에 포함되어 있는 목적지 IP를 제1 목적지 IP, IP 변경 관리부(203)를 통해 변경되거나 변경되지 않은 목적지 IP를 제2 목적지 IP라 지칭한다.

[142] 라우팅 테이블 관리부(204)는 제어부(400)로부터 미리 설정된 주기에 따라 전송되는 라우팅 테이블 정보를 수신하여 갱신, 저장한다. 라우팅 테이블 정보는 단말이 보안 IP 통신 서비스를 이용하고자 할 경우, 보안 IP 통신 서비스를 이용하기 위해 미리 허용된 IP들에 대한 리스트로, 복수의 보안 IP들에 대한 리스트가 라우팅 테이블로 저장되어 있다.

[143] IP 처리부(205)는 IP 변경 관리부(203)에서 출력된 제2 목적지 IP를 확인하고, 제2 목적지 IP와 라우팅 테이블 관리부(204)에 저장되어 있는 라우팅 테이블 정보를 비교한다. 그리고 제2 목적지 IP가 라우팅 테이블로 저장된 보안 IP 중 하나이면, IP 처리부(205)는 IP 패킷에 포함되어 있는 소스 IP를 보안 IP 라우터(200)에 할당된 보안 IP로 변경한다.

[144] 그러나 제2 목적지 IP가 라우팅 테이블로 저장된 보안 IP가 아니면, IP 처리부(205)는 IP 패킷에 포함되어 있는 소스 IP를 보안 IP 라우터(200)에 할당되어 있는 공중 IP로 변경한다. 본 발명의 실시예에서는 설명의 편의를 위하여, IP 패킷에 포함되어 있던 제1 단말(10')의 소스 IP를 '제1 소스 IP'라 지칭하고, IP 처리부(205)에서 보안 IP 라우터(200)의 공중 IP 또는 보안 IP 중 어느 하나의 IP로 변경된 소스 IP를 '제2 소스 IP'라 지칭한다.

[145] 보안 정책 관리부(206)는 제어부(400)로부터 미리 설정된 주기에 따라 전송되는 보안 정책을 수신하여 갱신, 저장한다. 여기서 보안 정책은 사전에 미리 설정되어 있는 통신 차단 대상 정보(예를 들어, IP, 포트(port) 또는 프로토콜 정보 등)를 포함하고 있다. 본 발명의 실시예에서는 보안 정책 관리부(206)가 제어부(400)로부터 보안 정책을 수신하는 것을 예로 하여 설명하나, 미리 설정되어 있을 수도 있다.

[146] 또한, 보안 정책 관리부(206)는 IP 처리부(205)로부터 전달된 IP 패킷에 포함되어 제2 소스 IP나 제2 목적지 IP 또는 IP 패킷을 전송하고자 하는 포트 정보나 프로토콜 등의 정보가 통신 차단 대상 정보에 포함되는지 확인한다. 그리고 확인한 보안 정책에 따라 통신을 차단 여부를 결정한다.

[147] 통신부(207)는 보안 정책 관리부(206)에서 IP 패킷의 전송을 허용하면, IP 패킷에 포함되어 있는 제2 소스 IP와 제2 목적지 IP를 토대로 보안 IP 통신 또는 공중 IP 통신 중 어느 하나의 통신 방법을 통해 IP 패킷을 제2 단말(20')로 전달한다.

[148]

[149] 이상에서 설명한 보안 IP 라우터(200)를 포함하는 통신 망에서 IP 주소에 따라 보안 IP 통신 또는 공중 IP 통신을 수행하는 방법에 대해 도 8을 참조로 설명한다.

[150] 도 8은 본 발명의 제3 실시예에 따른 IP 통신 방법에 대한 흐름도이다.

[151] 도 8에 도시된 바와 같이, 보안 IP 라우터(200)는 DHCP 서버(60')로 자신에 대한 IP 할당을 요청한다(S200). DHCP 서버(606)는 S200 단계의 요청에 따라 보안 IP 라우터(200)의 공중 IP와 보안 IP를 할당하여 보안 IP 라우터(200)로 전달한다(S201). 그리고 보안 IP 라우터(200)는 제어부(400)로부터 제어 정보를

미리 설정한 주기에 따라 수신한다(S202). 여기서 제어 정보는 IP 변경 관리 정보, 라우팅 테이블 정보 및 보안 정책을 포함한다.

[152] 그리고 보안 IP 라우터(200)에 연결된 제1 단말(10')이 제2 단말(20')과의 IP 통신을 위해 보안 IP 라우터(200)로 IP 할당을 요청하면(S203), 보안 IP 라우터(200)는 제1 단말(10')에 대한 사설 IP를 생성하여 제1 단말(10')로 전달한다(S204, S205). 여기서 S204 단계에서 보안 IP 라우터(200)가 제1 단말(10')에 대한 사설 IP를 생성하는 방법은 DHCP 서버(60')가 IP를 생성할 때 이용하는 미리 설정된 규칙에 따라 생성한다.

[153] 제1 단말(20)은 S205 단계에서 보안 IP 라우터(200)로부터 수신한 사설 IP를 이용하여 IP 패킷을 전송한다(S206). 여기서 IP 패킷에는 제1 단말(10')의 사설 IP를 제1 소스 IP로, 제2 단말(20')에 대한 제1 목적지 IP 및 패킷이 포함된다. 제1 단말(10')이 제2 단말(20')에 대한 제1 목적지 IP를 획득하는 방법은 여러 방법을 통해 얻을 수 있으며, 본 발명의 실시예에서는 상세한 설명을 생략한다.

[154] IP 변경 관리부(203)는 S206 단계에서 수신한 IP 패킷에 포함된 제1 목적지 IP를 확인한다(S207). 그리고 확인한 제1 목적지 IP가 S202 단계에서 수신한 제어 정보 내 IP 변경 관리 정보에 포함되어 있는 IP 인지 확인한다(S208).

[155] 만약 제1 목적지 IP가 IP 변경 관리 정보에 포함되어 있는 IP라면, 제1 목적지 IP에 NAT를 실행하여 제2 목적지 IP로 변경한다(S209). 여기서 변경된 제2 목적지 IP는 보안 IP일 수도 있고 공중 IP일 수도 있다. 그러나, S209 단계에서 확인한 결과 제1 목적지 IP가 IP 변경 관리 정보에 포함되어 있지 않은 IP라면, 제1 IP 목적지 IP를 제2 목적지 IP로 설정한다.

[156] 다음 IP 처리부(205)는 IP 변경 관리부(203)에서 생성된 제2 목적지 IP와 라우팅 테이블 관리부(204)에 저장되어 있는 라우팅 테이블 정보를 비교하여, 제2 목적지 IP가 보안 IP인지 확인한다(S210). 라우팅 테이블에는 보안 IP들에 대한 주소가 포함되어 있다. 라우팅 테이블에 보안 IP 주소 이외에 추가적인 정보가 포함될 수도 있다.

[157] 따라서, IP 처리부(205)는 S210 단계에서 확인한 제2 목적지 IP와 라우팅 테이블 관리부(204)가 관리하는 라우팅 테이블을 토대로, 제2 목적지 IP가 보안 IP인 경우에는 제1 소스 IP를 DHCP 서버(60')가 보안 IP 라우터(200)에 할당한 보안 IP로 변경하여 제2 소스 IP를 결정한다. 만약 제2 목적지 IP가 라우팅 테이블에 포함되어 있지 않은 IP라면, 보안 IP 라우터(200)에 할당되어 있는 공중 IP를 제2 소스 IP로 변경한다(S211). S210 단계 및 S211 단계를 통해, 보안 IP 라우터(200)는 공중 IP 통신으로 IP 패킷을 전송할지, 보안 IP 통신으로 IP 패킷을 전송할지 인식하게 된다.

[158] 이상의 절차를 통해 제2 소스 IP와 제2 목적지 IP가 결정되면, 보안 정책 관리부(206)는 저장된 보안 정책들을 토대로 IP 패킷을 전송할 통신을 허용할지 말지를 결정한다(S212). 보안 정책은 제어부(400)로부터 전송되거나 보안 IP 라우터(200)에 미리 설정되어 있을 수 있으며, IP 처리부(205)로부터 전달된 IP

패킷에 포함되어 제2 소스 IP나 제2 목적지 IP 또는 IP 패킷을 전송하고자 하는 제1 단말(10')의 포트 정보나 프로토콜 등의 정보가 통신 차단 대상 정보에 포함되어 있는지 확인하여 통신을 차단 여부를 결정한다.

[159] S212 단계에서 통신 차단으로 결정되면, 통신부(207)는 IP 패킷의 전송을 차단한다(S213). 그러나, S212 단계에서 통신 허용으로 결정되면, 통신부(207)는 공중망을 통해 제2 단말(20')로 IP 패킷을 전송하거나(S214, S215), 보안 IP 게이트웨이(300)를 통해 제2 단말(20')로 IP 패킷을 전송한다(S216, S217).

[160]

[161] 이상의 절차에 대해 하나의 예를 들어 설명하면 다음과 같다.

[162] 보안 IP 라우터(100)가 DHCP 서버(60')로부터 할당 받은 공중 IP를 168.126.0.1이라 가정하고, 보안 IP를 169.208.0.1이라 가정한다. 그리고, 보안 IP 라우터(200)가 제1 단말(10')에 할당한 IP를 192.168.0.1이라 가정하고, 제2 단말(20')의 공중 IP는 2.2.2.2, 보안 IP는 39.28.0.2이라 가정한다.

[163] 또한, 라우팅 테이블에는 보안 IP 통신을 위해 허용된 IP로 169.208.0.1에서부터 169.208.0.254까지의 보안 액세스 IP와, 이들 보안 액세스 IP가 변환된 보안 코어 IP인 39.28.0.1에서부터 39.28.0.254까지의 IP들에 해당한다고 정의되어 있다고 가정한다.

[164] 그리고, IP 변경 관리 정보에는 특정 IP로 2.2.2.2가 저장되어 있고, 2.2.2.2는 39.28.0.2로 변환되도록 설정되어 있다고 가정한다. 본 발명의 실시예에서는 설명의 편의를 위하여 IP 변경 관리 정보에 특정 IP인 2.2.2.2에 대한 사항만 언급하고 있으나, 이와 같이 한정되는 것은 아니다.

[165] 이상에서 가정한 IP들을 예로 하여 설명하면, 제1 단말(10')이 목적지 IP를 2.2.2.2로 하여 IP 패킷 전송을 시도한다고 가정하면, 보안 IP 라우터(200)가 수신한 IP 패킷에는 제1 소스 IP가 192.168.0.1, 제1 목적지 IP가 2.2.2.2 그리고 패킷이 포함되어 있다. 여기서 제1 소스 IP는 제1 단말(10')에 할당된 사설 IP에 해당한다.

[166] IP 변경 관리부(203)는 수신한 IP 패킷에서 제1 목적지 IP를 확인한다. 제1 목적지 IP가 IP 변경 관리 정보에 포함되어 있으므로, IP 변경 관리부(203)는 제1 목적지 IP인 2.2.2.2를 39.28.0.2로 변환하여 제2 목적지 IP를 생성한다. 제2 목적지 IP가 생성되면, IP 처리부(205)는 제2 목적지 IP가 보안 IP 통신을 위한 IP로 설정되어 있는 라우팅 테이블에 포함되어 있는지 확인한다.

[167] 제2 목적지 IP인 39.28.0.2는 보안 코어 IP에 해당하여 라우팅 테이블에 포함되어 있으므로, IP 처리부(205)는 제2 목적지 IP가 보안 IP임을 확인한다. 따라서, IP 처리부(205)는 제1 단말(10')의 IP로 설정되어 있는 제1 소스 IP를 보안 IP 라우터(200)에 할당된 보안 IP인 169.208.0.1로 변경하여 제2 소스 IP를 결정한다.

[168] 이에 따라 IP 패킷에 포함되어 있는 제2 소스 IP는 169.208.0.1, 제2 목적지 IP는 39.28.0.2가 되며, 보안 IP 통신을 통해 IP 패킷을 제2 단말(20')로 전송할 수 있게

된다. 제2 소스 IP와 제2 목적지 IP가 결정된 후, 보안 정책 관리부(206)는 미리 저장되어 있는 보안 정책에 따라 IP 패킷의 전송을 위한 통신을 허용할지 결정한다. 그리고 통신을 허용하는 것으로 결정하면 통신부(207)는 보안 IP 게이트웨이(300)를 통해 제2 단말(20')로 전달한다. 여기서 보안 정책을 어느 하나의 형태로 한정하지 않았으므로, 실시예에서도 이에 대한 설명을 생략한다.

[169]

[170] 상기에서는 보안 IP 통신을 예로 하여 설명한 것이고, 공중 IP 통신을 예로 하여 설명하면 다음과 같다. 제1 단말(10')이 제1 목적지 IP를 202.175.1.1로 하여 IP 패킷 전송을 시도한다고 가정하면, 보안 IP 라우터(200)가 수신한 IP 패킷에는 제1 소스 IP가 192.168.0.1, 제1 목적지 IP가 202.175.1.1 그리고 패킷이 포함되어 있다. 여기서 제1 소스 IP는 제1 단말(10')에 할당된 사설 IP에 해당한다.

[171] IP 변경 관리부(203)는 수신한 IP 패킷에서 제1 목적지 IP를 확인한다. 제1목적지 IP인 202.175.1.1가 IP 변경 관리 정보에 포함되지 않으므로, 제2 목적지 IP 역시 202.175.1.1로 결정된다. IP 처리부(205)는 제2 목적지 IP가 라우팅 테이블 관리부(204)의 라우팅 테이블에 포함되어 있는지 확인한다.

[172] 상기 설정 사항에는 202.175.1.1이 라우팅 테이블에 포함되어 있지 않은 것으로 하였으므로, IP 처리부(205)는 제2 목적지 IP가 공중 IP임을 확인한다. 그리고 제1 단말(10')의 IP로 설정되어 있는 제1 소스 IP를 보안 IP 라우터(100)에 할당된 공중 IP인 168.126.0.1로 변경하여 제2 소스 IP를 결정한다. 이에 따라 IP 패킷에 설정되어 있는 제2 소스 IP는 168.126.0.1, 제2 목적지 IP는 202.175.1.1가 되며, 공중 IP 통신을 통해 IP 패킷을 제2 단말(20')로 전송할 수 있게 된다.

[173] 제2 소스 IP와 제2 목적지 IP가 결정된 후, 보안 정책 관리부(206)는 미리 저장되어 있는 보안 정책에 따라 IP 패킷의 전송을 위한 통신을 허용할지 결정하고, 통신을 허용하는 것으로 결정하면 통신부(207)는 게이트웨이(500)를 통해 제2 단말(20')로 전달한다. 여기서 보안 정책을 어느 하나의 형태로 한정하지 않았으므로, 실시예에서도 이에 대한 설명을 생략한다.

[174] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

청구범위

[청구항 1] 보안 IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 보안 IP 통신 서비스를 제공하는 방법에 있어서,
상기 보안 IP 통신 서비스 제공 장치는 상기 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 보안 코어 IP와 제2 보안 코어 IP를 토대로, 상기 제1 단말과 제2 단말이 하나의 그룹으로 형성되어 있는지 확인하는 단계; 및
상기 제1 단말과 제2 단말이 그룹으로 형성되어 있으면, 상기 제1 단말로부터 전송된 IP 패킷을 상기 제2 단말로 전달하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 2] 제1항에 있어서,
상기 하나의 그룹으로 형성되어 있는지 확인하는 단계 이전에,
상기 제1 단말이 제1 IP 패킷을 생성하고, 제2 단말에 할당된 제2 보안 코어 IP를 이용하여 통신을 시작하는 단계;
상기 통신 서비스 제공 장치와 연동하는 L3 라우터가 상기 제1 단말에 대한 제1 보안 액세스 IP와 상기 제2 보안 코어 IP가 보안 IP 통신을 위해 허가된 IP인지 확인하는 단계;
제1 보안 액세스 IP와 제2 보안 코어 IP가 모두 허가된 IP라면, 상기 제1 IP 패킷을 상기 보안 IP 통신 서비스 제공 장치로 전달하는 단계; 및
상기 제1 보안 액세스 IP 또는 제2 보안 코어 IP 중 적어도 하나의 IP가 허가된 IP가 아니라면, 상기 제1 IP 패킷을 차단하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 3] 제2항에 있어서,
상기 L3 라우터는 보안 IP 통신을 위해 미리 설정된 ACL(Access Control List)을 이용하여 상기 제1 보안 액세스 IP와 제2 보안 코어 IP가 허가된 IP인지 확인하는 보안 IP 통신 서비스 제공 방법.

[청구항 4] 제2항에 있어서,
상기 보안 IP 통신 서비스 제공 장치로 전달하는 단계 이후에,
상기 보안 IP 통신 서비스 제공 장치는 수신한 제1 IP 패킷에 포함된 상기 제1 보안 액세스 IP에 NAT(Network Address Translation)를 실행하여 제1 보안 코어 IP로 변환하는 단계; 및
상기 생성된 제1 보안 코어 IP와 제2 보안 코어 IP, 패킷을 포함하는 제2 IP 패킷을 생성하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 5] 제4항에 있어서,
상기 하나의 그룹으로 형성되어 있는지 확인하는 단계는,

상기 제1 단말에 대한 제1 보안 코어 IP와 제2 단말에 대한 제2 보안 코어 IP가 하나의 그룹에 포함되어 있는지 확인하는 단계;
상기 제1 단말과 제2 단말이 하나의 그룹에 포함되어 있지 않으면, 상기 제2 IP 패킷을 차단하는 단계;
상기 제1 단말과 제2 단말이 하나의 그룹에 포함되어 있으면, 상기 제2 단말의 제2 보안 코어 IP에 NAT를 실행하여 제2 단말에 대한 목적지 IP로 변환하는 단계; 및
상기 제1 보안 코어 IP, 목적지 IP 및 패킷을 포함하는 제3 IP 패킷을 생성하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 6] 제1항에 있어서,
상기 보안 IP 통신 서비스 제공 장치는 공중 인터넷 망에 위치한 제2 서버를 통해 통신 서비스를 이용하고자 하는 상기 단말로부터 IP 패킷을 수신하는 단계;
상기 IP 패킷에 포함되어 있는 상기 제2 서버의 IP 주소를 토대로, 상기 보안 IP 통신 서비스 제공 장치에 연결되어 있는 보안 DNS에 상기 제2 서버의 IP 주소에 대응되어 미리 저장된 제1 웹 서버의 IP 주소가 있는지 확인하는 단계; 및
상기 제1 웹 서버의 IP 주소가 있으면, 상기 보안 IP 통신 서비스 제공 장치는 제1 웹 서버를 통해 상기 제2 웹 서버에서 제공하는 통신 서비스의 정보를 수신하여 상기 단말로 전달하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 7] 제6항에 있어서,
상기 단말로 전달하는 단계는,
상기 보안 IP 통신 서비스 제공 장치는 상기 제2 웹 서버에서 제공하는 통신 서비스의 정보를 수신하여 상기 제1 웹 서버로 전달하는 단계; 및
상기 제1 웹 서버는 상기 보안 IP 통신 서비스 제공 장치를 통해 수신한 정보를 상기 단말로 제공하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 8] 하나의 그룹으로 설정되어 있는 복수의 단말 각각에 할당되어 있는 보안 코어 IP들을 그룹으로 형성하여 그룹 매핑 정보를 생성하는 제어부; 및
단말에 할당된 보안 액세스 IP와 보안 코어 IP에 NAT를 실행하고, 보안 IP 통신 서비스의 이용을 위해 IP 패킷을 생성하는 소스 단말과, 상기 소스 단말이 생성한 IP 패킷을 수신할 목적지 단말이 동일한 그룹에 속해 있는지 확인하는 보안 IP 게이트웨이
를 포함하는 보안 IP 통신 시스템.

[청구항 9] 제8항에 있어서,
상기 보안 IP 게이트웨이는,
소스 단말이 생성한 IP 패킷에 포함되어 있는, 상기 소스 단말의 제1 보안 액세스 IP를 제1 보안 코어 IP로 변환하는 제1 NAT;
상기 제1 NAT에서 변환된 제1 보안 코어 IP와 상기 IP 패킷에 포함되어 있는 목적지 단말의 제2 보안 코어 IP를, 외부로부터 입력되어 미리 저장되어 있는 그룹 매핑 정보에서 확인하여, 상기 소스 단말과 목적지 단말이 동일한 그룹에 포함되어 있는지 확인하는 보안 그룹 판단 장치; 및
상기 제2 보안 코어 IP를 제2 보안 액세스 IP로 변환하는 제2 NAT
를 포함하는 보안 IP 통신 시스템.

[청구항 10] 제9항에 있어서,
상기 소스 단말이 생성한 IP 패킷을 수신하고, 수신한 IP 패킷에 포함되어 있는 목적지 단말의 상기 제2 보안 코어 IP와 상기 소스 단말의 제1 보안 액세스 IP를 토대로, 소스 단말과 목적지 단말에 각각 할당된 IP들이 보안 IP 통신 서비스를 제공하기 위해 허용된 IP인지 확인하는 L3 라우터
를 더 포함하는 보안 IP 통신 시스템.

[청구항 11] 제10항에 있어서,
공중 인터넷 망의 제1 웹 서버를 목적지로 하는 IP가 입력되면, 입력된 IP를 갖는 IP 패킷을 보안 IP 네트워크에 위치한 제2 웹 서버로 전달되도록, 상기 제1 웹 서버의 IP와 상기 제2 웹 서버의 IP가 대응되도록 설정하는 보안 DNS; 및
상기 제1 웹 서버로부터 정보를 수신하여, 상기 제1 웹 서버에서 제공하는 정보를 상기 소스 단말로 전달하는 상기 제2 웹 서버
를 더 포함하는 보안 IP 통신 시스템.

[청구항 12] 제9항에 있어서,
상기 보안 그룹 판단 장치는,
상기 소스 단말과 목적지 단말이 동일한 그룹에 속한 것으로 확인하면, 상기 IP 패킷을 제2 NAT로 전달하고,
상기 소스 단말과 목적지 단말이 동일한 그룹에 속하지 않은 것으로 확인하면, 상기 IP 패킷을 차단하는 보안 IP 통신 시스템.

[청구항 13] 단말에 IP 통신 서비스를 제공하는 IP 통신 서비스 제공 장치에 있어서,
IP 변경 관리 정보를 저장하고, 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 상기 IP 변경 관리 정보에 따라 다른 IP로 변환을 수행할 수 있는 IP 변경 관리부;
보안 IP 통신 서비스를 제공하기 위한 복수의 보안 IP의 주소를

포함하는 라우팅 테이블을 관리하는 라우팅 테이블 관리부;
상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP가 상기 라우팅 테이블에 포함되는지 확인하고, 확인 결과에 따라 상기 IP 패킷에 포함되어 있는 제1 소스 IP를 제2 소스 IP로 변경하는 IP 처리부; 및
상기 IP 처리부에서 변경한 제2 소스 IP와 상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP를 토대로, IP 패킷을 공중 IP 통신 또는 보안 IP 통신 중 어느 하나의 통신을 통해 제2 단말로 전송하는 통신부
를 포함하는 보안 IP 통신 서비스 제공 장치.

[청구항 14] 제13항에 있어서,
상기 IP 처리부는,
상기 IP 변경 관리부에서 변환 또는 변환되지 않은 목적지 IP가 공중 IP이면 제1 단말에 할당된 IP인 제1 소스 IP를 상기 IP 통신 서비스 제공 장치에 할당된 공중 IP로 변경하여 제2 소스 IP로 생성하고,
상기 변환 또는 변환되지 않은 목적지 IP가 보안 IP이면, 상기 제1 소스 IP를 상기 IP 통신 서비스 제공 장치에 할당된 보안 IP로 변경하여 제2 소스 IP로 생성하는 보안 IP 통신 서비스 제공 장치.

[청구항 15] 제13항에 있어서,
상기 보안 IP 통신 서비스 제공 장치와 연동하는 DHCP(Dynamic Host Configuration Protocol) 서버로 상기 보안 IP 통신 서비스 제공 장치에 대한 IP의 할당을 요청하고, 상기 DHCP 서버로부터 공중 IP 및 보안 IP를 포함하는 IP를 수신하는 IP 주소 요청부; 및
상기 IP 패킷을 전송하는 제1 단말로부터 IP 주소의 할당을 요청 받으면, 상기 제1 단말에 대한 제1 소스 IP를 생성하여 전달하는 IP 주소 할당부
를 포함하는 보안 IP 통신 서비스 제공 장치.

[청구항 16] 제15항에 있어서,
상기 통신부가 제2 단말로 상기 IP 패킷의 전송 허용 여부를 결정하도록 하는 보안 정책을 외부로부터 수신하여 관리하는 보안 정책 관리부
를 더 포함하는 보안 IP 통신 서비스 제공 장치.

[청구항 17] 제15항에 있어서,
상기 IP 통신 서비스 제공 장치로 제어 정보를 전달하는 제어부;
상기 IP 통신 서비스 제공 장치로 상기 제1 IP 및 제2 IP를 할당하여 제공하는 상기 DHCP 서버;
상기 IP 통신 서비스 제공 장치가 상기 IP 패킷을 제1 통신을 통해

전송하는 것으로 결정하면, 상기 IP 패킷을 목적지 단말로 전송하는 제1 게이트웨이; 및

상기 IP 통신 서비스 제공 장치가 상기 IP 패킷을 제2 통신을 통해 전송하는 것으로 결정하면, 상기 IP 패킷을 목적지 단말로 전송하는 제2 게이트웨이

를 포함하는 보안 IP 통신 서비스 제공 장치.

[청구항 18] IP 통신 서비스 제공 장치가 제1 단말과 제2 단말 사이에 IP 통신 서비스를 제공하는 방법에 있어서,

상기 제1 단말로부터 전송되는 IP 패킷에 포함된 제1 목적지 IP를 소정의 IP변경 관리 정보에 따라 제2 목적지 IP로 변환 여부를 결정하는 단계;

제2 목적지 IP로 변환 결정된 경우 상기 변환된 제2 목적지 IP가 라우팅 테이블에 포함되는지 확인하고, 제2 목적지 IP로 변환되지 않은 경우 상기 제1 목적지 IP가 상기 라우팅 테이블에 포함되어 있는지 확인하는 단계;

상기 확인 결과에 따라 IP 패킷에 포함된 제1 소스 IP를 제2 소스 IP로 변경하는 단계; 및

변경된 제2 소스 IP와 목적지 IP를 토대로 상기 제1 단말에서 전송한 IP 패킷을 상기 제2 단말로 보안 IP 통신 또는 공중 IP 통신 중 어느 하나의 통신으로 전송하는 단계

를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 19] 제18항에 있어서,

상기 제2 목적지 IP로 변환 여부를 결정하는 단계는,

상기 IP 변경 관리 정보는 미리 설정된 복수의 IP와 상기 복수의 IP를 변환할 복수의 변환 IP들이 각각 설정되어 있고,

상기 제1 목적지 IP가 상기 IP 변경 관리 정보에 포함된 복수의 IP 중 하나이면, 상기 제1 목적지 IP에 대응되어 설정되어 있는 변환 IP를 제2 목적지 IP로 변환하는 것으로 결정하는 단계; 및

상기 제1 목적지 IP가 상기 IP 변경 관리 정보에 포함되지 않으면, 상기 제1 목적지 IP를 제2 목적지 IP로 변환하지 않는 것으로 결정하는 단계;

를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 20] 제18항에 있어서,

상기 제2 소스 IP로 변경하는 단계는,

상기 제2 목적지 IP 또는 제2 목적지 IP로 변환되지 않은 제1 목적지 IP 중어느 하나인 목적지 IP가 상기 라우팅 테이블에 포함되어 있으면, 상기 목적지 IP가 보안 IP인 것으로 확인하는 단계; 및

제1 단말의 사설 IP인 상기 제1 소스 IP를 상기 IP 통신 서비스 제공 장치에 할당된 보안 IP로 변경하여 제2 소스 IP를 생성하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 21] 제20항에 있어서,
상기 제2 소스 IP로 변경하는 단계는,
상기 목적지 IP가 상기 라우팅 테이블에 포함되어 있지 않으면,
상기 목적지 IP가 공용 IP인 것으로 확인하는 단계; 및
상기 제1 소스 IP를 상기 IP 통신 서비스 제공 장치에 할당된 공중 IP로 변경하여 제2 소스 IP를 생성하는 단계
를 더 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 22] 제18항에 있어서,
상기 어느 하나의 통신으로 전송하는 단계는,
상기 제2 소스 IP와, 제2 목적지 IP 또는 제2 목적지 IP로 변환되지 않은 제1 목적지 IP 중 어느 하나인 목적지 IP가 각각 보안 IP이면 상기 IP 패킷을 보안 IP 통신으로 상기 제2 단말에 전송하고,
상기 제2 소스 IP와 목적지 IP가 각각 공중 IP이면 상기 IP 패킷을 공중 IP 통신으로 상기 제2 단말에 전송하는 보안 IP 통신 서비스 제공 방법.

[청구항 23] 제22항에 있어서,
상기 어느 하나의 통신으로 전송하는 단계는,
상기 제2 소스 IP와 목적지 IP를 미리 저장된 보안 정책과 비교하여, 통신 차단 여부를 결정하는 단계
를 더 포함하는 보안 IP 통신 서비스 제공 방법.

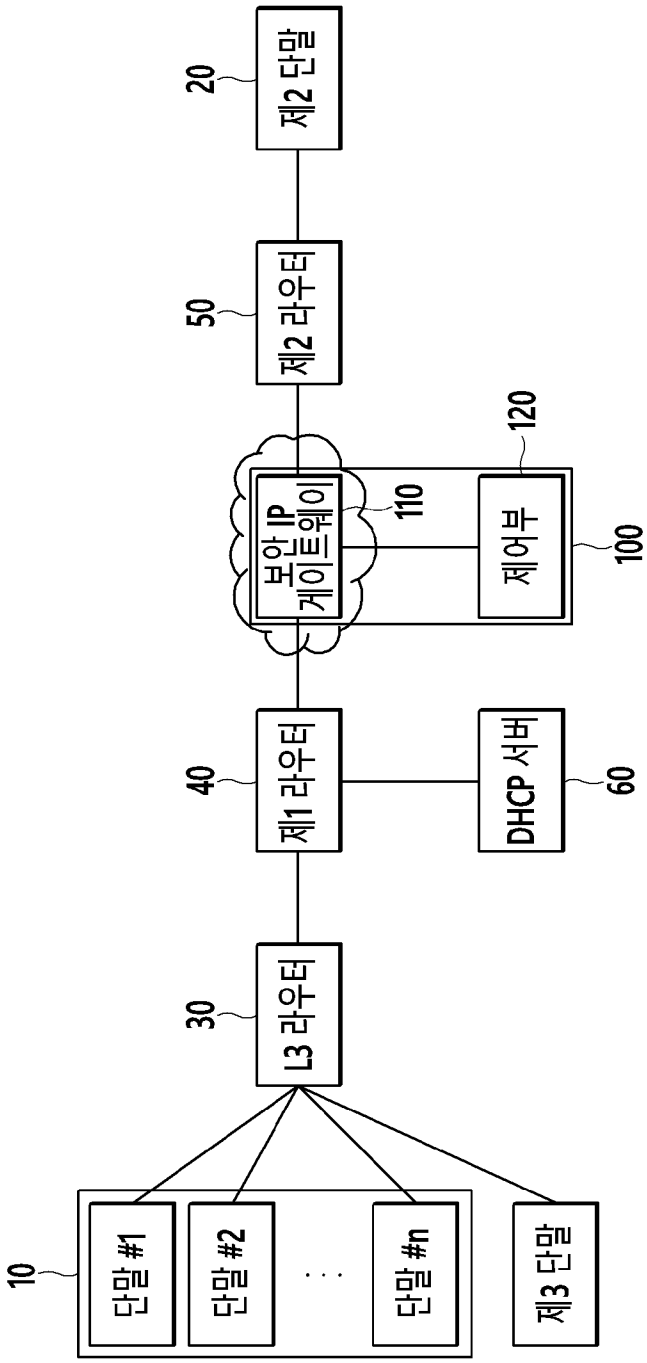
[청구항 24] 제18항에 있어서,
상기 제2 목적지 IP로 변환 여부를 결정하는 단계 이전에,
상기 보안 IP 통신 서비스 제공 장치가 연동하는 DHCP 서버로 상기 보안 IP 통신 서비스 제공 장치에 대한 IP의 할당을 요청하는 단계; 및
상기 DHCP 서버로부터 공중 IP 및 보안 IP를 포함하는 IP를 수신하는 단계
를 포함하는 보안 IP 통신 서비스 제공 방법.

[청구항 25] 제24항에 있어서,
상기 제2 목적지 IP로 변환 여부를 결정하는 단계 이전에,
상기 제1 단말로부터 IP 할당을 요청 받는 단계; 및
상기 제1 단말에 대한 사설 IP를 생성하여 상기 제1 단말로 제공하는 단계
를 더 포함하는 보안 IP 통신 서비스 제공 방법.

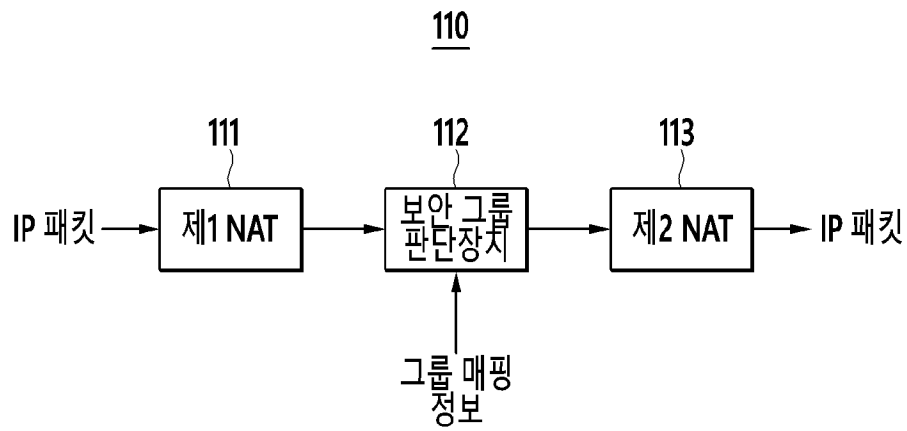
[청구항 26] 제24항에 있어서,

상기 제2 목적지 IP로 변환 여부를 결정하는 단계 이전에,
상기 IP 통신 서비스 제공 장치와 연동하는 제어부로부터 IP 변경 관리 정보, 라우팅 테이블 정보 및 보안 정책을 포함하는 제어 정보를 수신하는 단계
를 더 포함하는 보안 IP 통신 서비스 제공 방법.

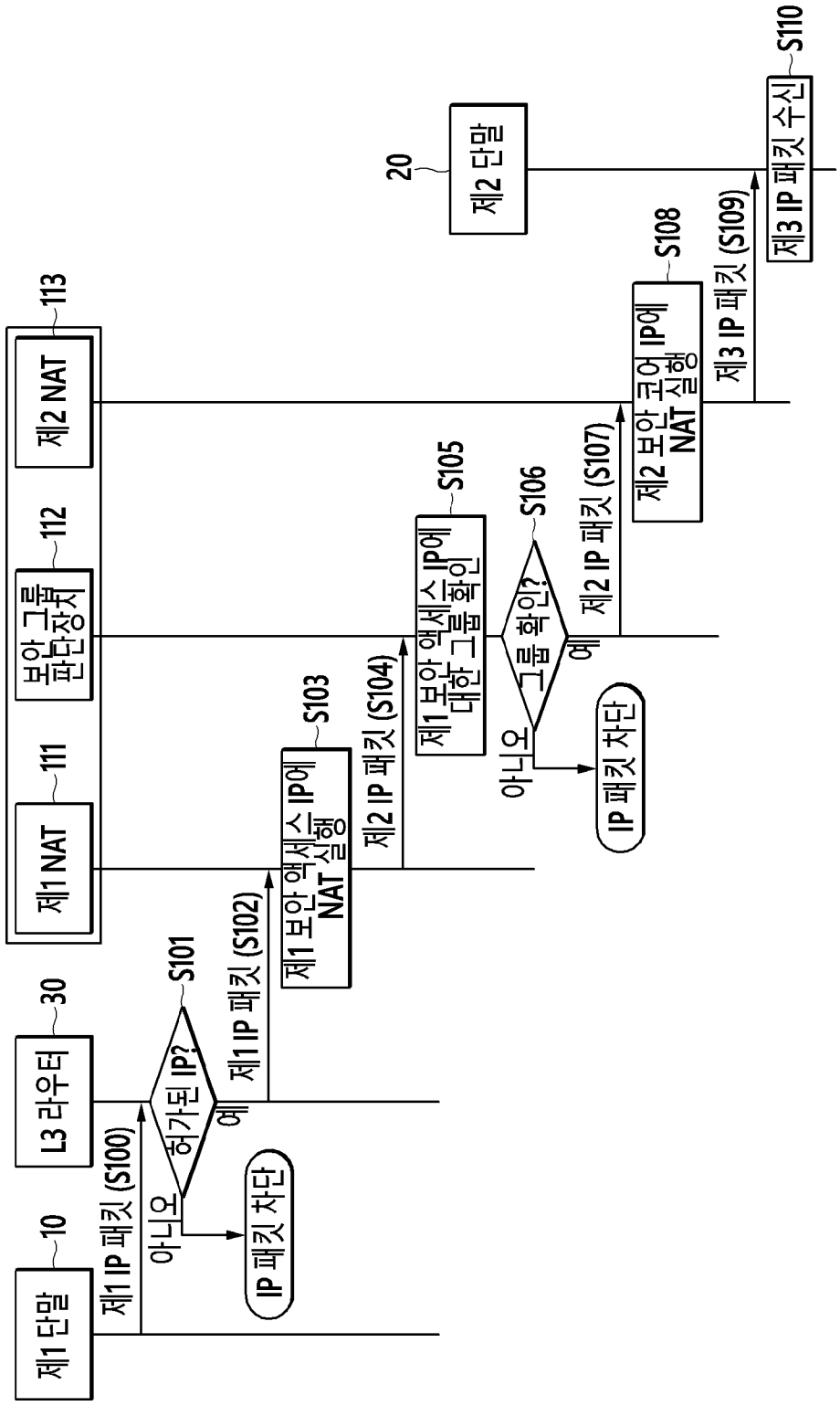
[Fig. 1]


20
제2 단말
50
제2 라우터
120
110
보안 IP 게이트웨이
제어부
100
40
제1 라우터
DHCP 서버
60
30
L3 라우터
10
단말 #1
단말 #2
. . .
단말 #n
제3 단말

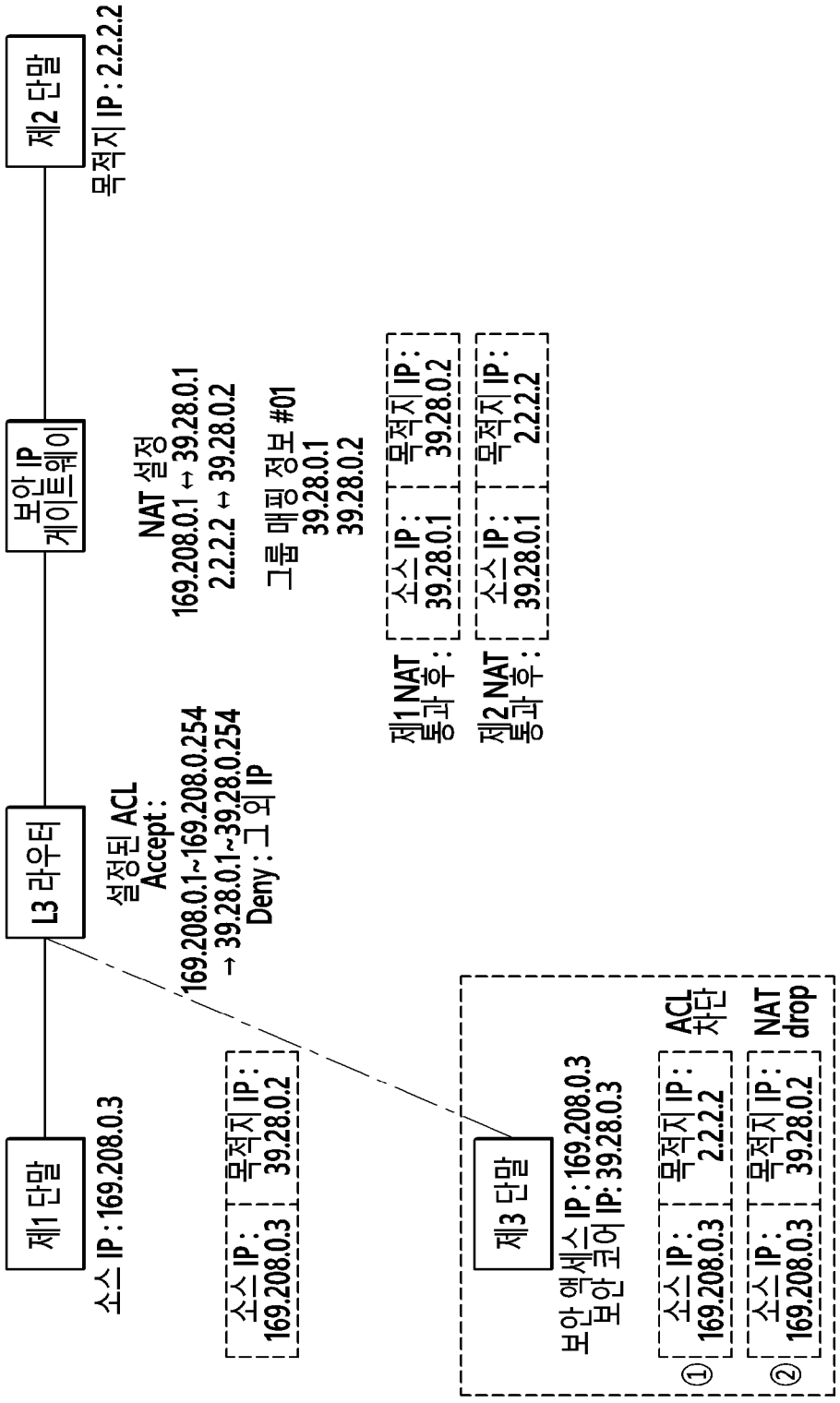
[Fig. 2]


110
111
112
113
IP 패킷
제1 NAT
보안 그룹 판단장치
제2 NAT
IP 패킷
그룹 매핑 정보

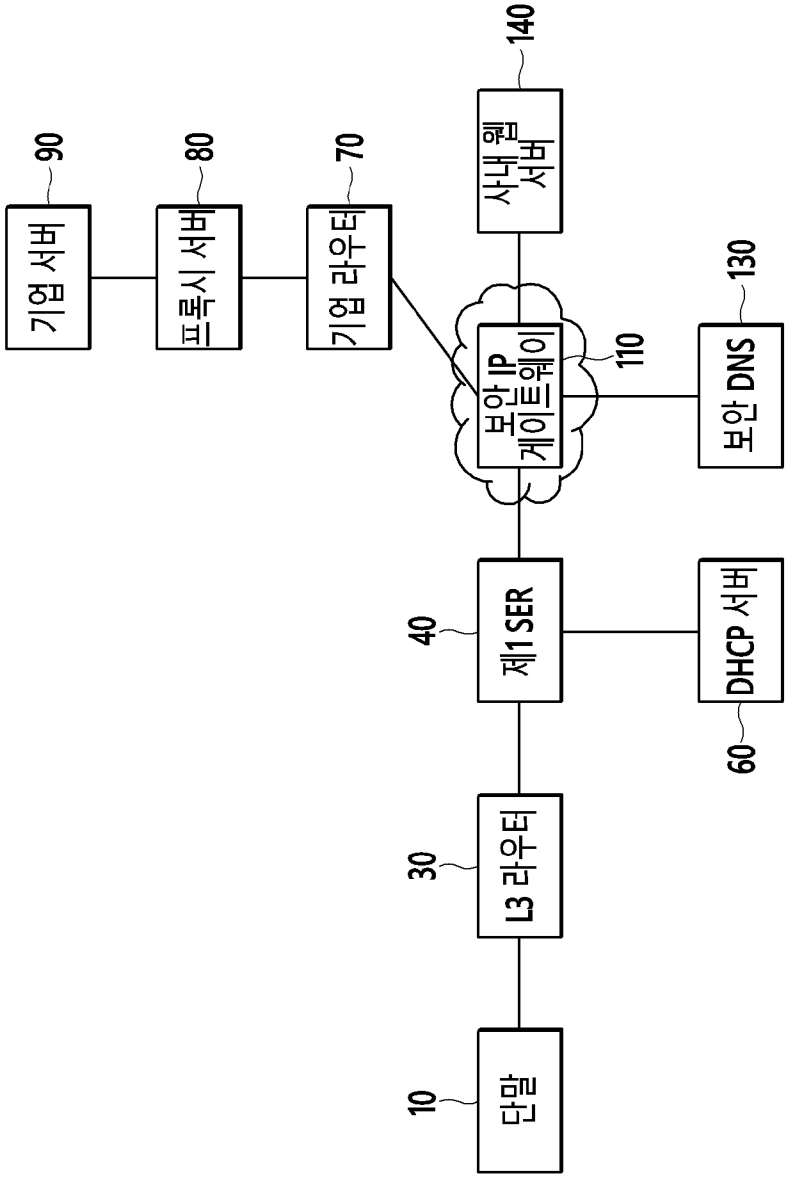
[Fig. 3]


제1 단말
10
제1 IP 패킷 (S100)
L3 라우터
30
S101
허가된 IP?
아니오
IP 패킷 차단
예
제1 IP 패킷 (S102)
제1 NAT
111
제1 보안 액세스 IP에 NAT 실행
S103
제2 IP 패킷 (S104)
보안 단말장치
112
제1 보안 액세스 IP에 대한 그룹 확인
S105
그룹 확인?
S106
아니오
IP 패킷 차단
예
제2 IP 패킷 (S107)
제2 NAT
113
제2 보안 코어 IP에 NAT 실행
S108
제3 IP 패킷 (S109)
20
제2 단말
제3 IP 패킷 수신
S110

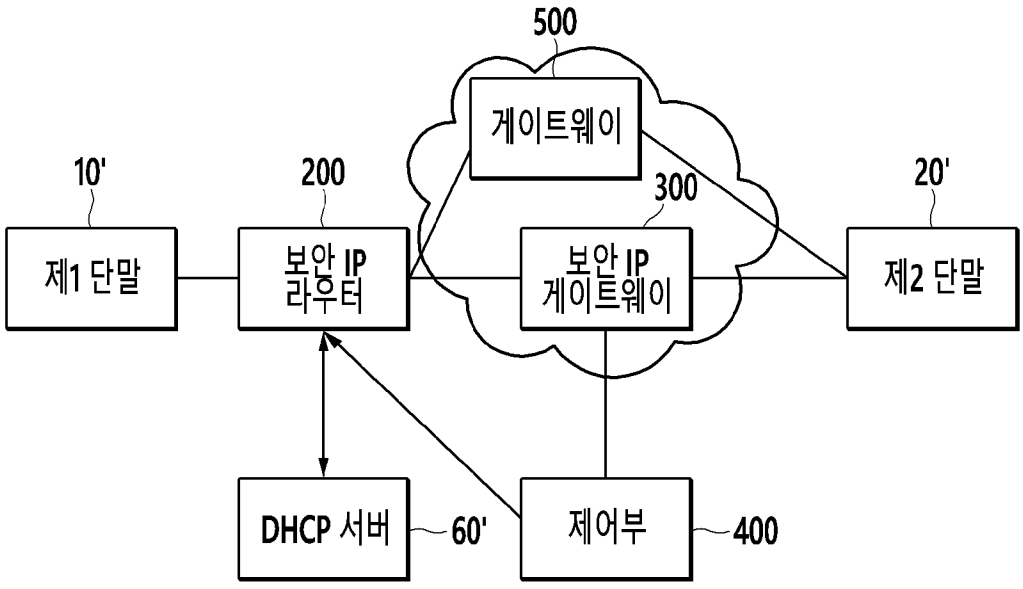
[Fig. 4]


제1 단말
소스 IP : 169.208.0.3
L3 라우터
보안 IP 게이트웨이
제2 단말
목적지 IP : 2.2.2.2
설정된 ACL
Accept :
169.208.0.1~169.208.0.254
→ 39.28.0.1~39.28.0.254
Deny : 그 외 IP
NAT 설정
169.208.0.1 ↔ 39.28.0.1
2.2.2.2 ↔ 39.28.0.2
그룹 매핑 정보 #01
39.28.0.1
39.28.0.2
제1 NAT 통과 후 :
소스 IP : 39.28.0.1
목적지 IP : 39.28.0.2
제2 NAT 통과 후 :
소스 IP : 39.28.0.1
목적지 IP : 2.2.2.2
소스 IP : 169.208.0.3
목적지 IP : 39.28.0.2
제3 단말
보안 액세스 IP : 169.208.0.3
보안 코어 IP: 39.28.0.3
① 소스 IP : 169.208.0.3
목적지 IP : 2.2.2.2
ACL 차단
② 소스 IP : 169.208.0.3
목적지 IP : 39.28.0.2
NAT drop

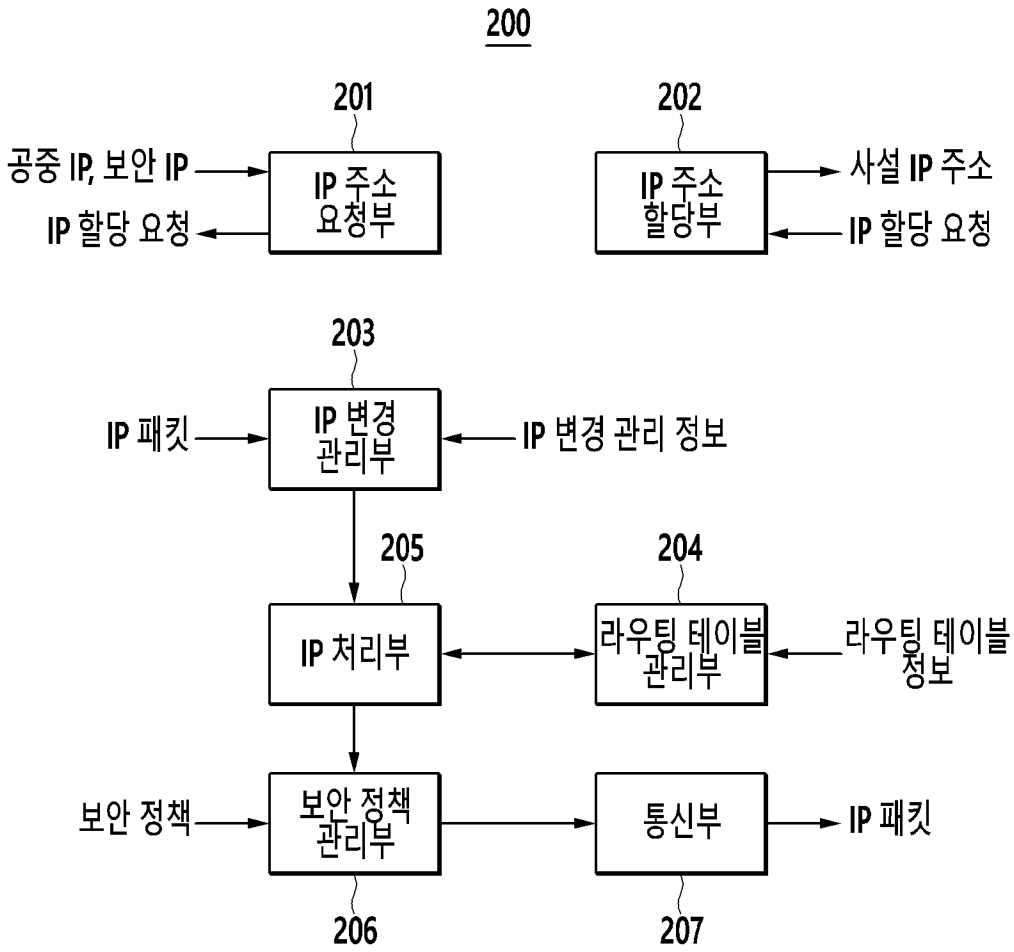
[Fig. 5]


140
사내 DNS 서버
90
기업 서버
80
프록시 서버
70
기업 라우터
130
보안 DNS
110
보안 IP 게이트웨이
40
제1 SER
DHCP 서버
60
30
L3 라우터
10
단말

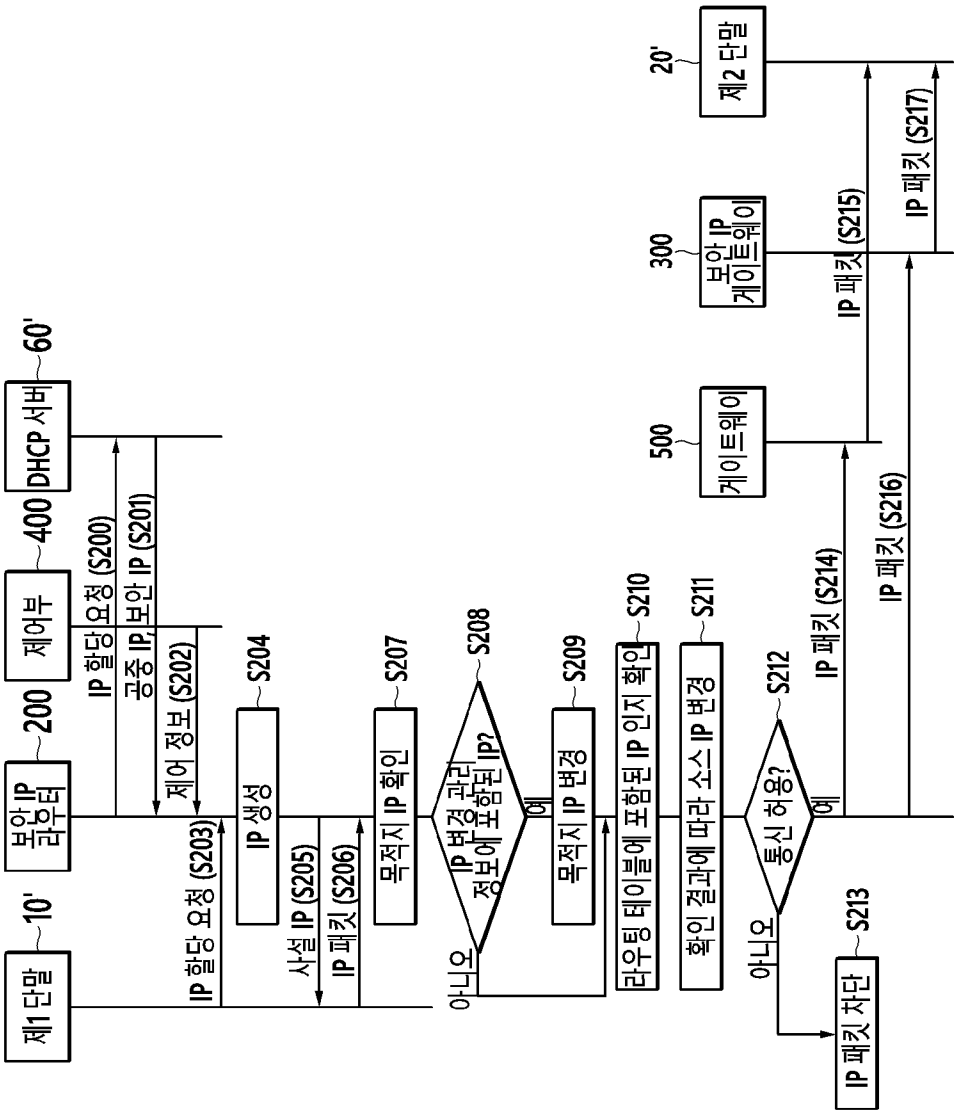
[Fig. 6]


500
게이트웨이
10'
제1 단말
200
보안 IP 라우터
300
보안 IP 게이트웨이
20'
제2 단말
DHCP 서버
60'
제어부
400

[Fig. 7]


200
201
IP 주소 요청부
공중 IP, 보안 IP
IP 할당 요청
202
IP 주소 할당부
사설 IP 주소
IP 할당 요청
203
IP 변경 관리부
IP 패킷
IP 변경 관리 정보
205
IP 처리부
204
라우팅 테이블 관리부
라우팅 테이블 정보
보안 정책
보안 정책 관리부
206
통신부
IP 패킷
207

[Fig. 8]


제1 단말
10'
보안 IP 라우터
200
제어부
400
DHCP 서버
60'
제2 단말
20'
보안 IP 게이트웨이
300
게이트웨이
500
IP 할당 요청 (S200)
공중 IP 보안 IP (S201)
제어 정보 (S202)
IP 할당 요청 (S203)
IP 생성
S204
사설 IP (S205)
IP 패킷 (S206)
목적지 IP 확인
S207
IP 변경 관리 정보에 포함된 IP?
S208
아니오
예
목적지 IP 변경
S209
라우팅 테이블에 포함된 IP 인지 확인
S210
확인 결과에 따라 소스 IP 변경
S211
통신 허용?
S212
아니오
예
IP 패킷 차단
S213
IP 패킷 (S214)
IP 패킷 (S215)
IP 패킷 (S216)
IP 패킷 (S217)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/014850

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/12(2006.01)i, H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/12; H04L 12/46; H04L 29/08; G06F 21/20; H04L 29/06; H04L 12/28; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: IP packet, group, terminal, security, communication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007-0081530 A1 (NOMURA, Yuji et al.) 12 April 2007 See paragraphs [0066], [0099], [0112]-[0116], [0156], [0161]-[0162], [0190], [0193]; and figures 2-3, 8.	1-12
Y	WO 2009-062504 A1 (TNM FARMGUARD APS) 22 May 2009 See page 10, line 14-page 11, line 27; and figure 1.	1-12
Y	JP 2009-163546 A (NEC CORP.) 23 July 2009 See paragraphs [0048]-[0050]; claims 2-3; and figures 1, 3.	6-7
Y	KR 10-2002-0040102 A (HYNIX SEMICONDUCTOR INC.) 30 May 2002 See pages 2-3; and figure 2.	6-7
A	KR 10-2010-0086640 A (WINNERSTEK, INC.) 02 August 2010 See paragraphs [0013]-[0040]; and figure 1.	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 APRIL 2017 (26.04.2017)	**26 APRIL 2017 (26.04.2017)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/014850

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The invention of group 1: claims 1-12 pertain to a security IP communication service based on security IP group confirmation.
The invention of group 2: claims 13-26 pertain to an IP communication service allowing communication by converting IP according to IP change information.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Claims 1-12

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/014850

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2007-0081530 A1	12/04/2007	CN 1839592 A	27/09/2006
		EP 1667382 A1	07/06/2006
		EP 1667382 A4	04/10/2006
		WO 2005-027438 A1	24/03/2005
WO 2009-062504 A1	22/05/2009	NONE	
JP 2009-163546 A	23/07/2009	JP 5239341 B2	17/07/2013
KR 10-2002-0040102 A	30/05/2002	NONE	
KR 10-2010-0086640 A	02/08/2010	KR 10-1015464 B1	22/02/2011

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/014850

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/12(2006.01)i, H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 29/12; H04L 12/46; H04L 29/08; G06F 21/20; H04L 29/06; H04L 12/28; H04L 12/56

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: IP 패킷, 그룹, 단말, 보안, 통신

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2007-0081530 A1 (YUJI NOMURA 등) 2007.04.12 단락 [0066], [0099], [0112]-[0116], [0156], [0161]-[0162], [0190], [0193]; 및 도면 2-3, 8 참조.	1-12
Y	WO 2009-062504 A1 (TNM FARMGUARD APS) 2009.05.22 페이지 10, 라인 14 - 페이지 11, 라인 27; 및 도면 1 참조.	1-12
Y	JP 2009-163546 A (NEC CORP.) 2009.07.23 단락 [0048]-[0050]; 청구항 2-3; 및 도면 1, 3 참조.	6-7
Y	KR 10-2002-0040102 A (주식회사 하이닉스반도체) 2002.05.30 페이지 2-3; 및 도면 2 참조.	6-7
A	KR 10-2010-0086640 A ((주) 위너스텍) 2010.08.02 단락 [0013]-[0040]; 및 도면 1 참조.	1-12

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 04월 26일 (26.04.2017)	2017년 04월 26일 (26.04.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
김성우
전화번호 +82-42-481-3348

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/014850

제2기재란 일부 청구항을 조사할 수 없는 경우의 의견(첫 번째 용지의 2의 계속)

PCT 제17조(2)(a)의 규정에 따라 다음과 같은 이유로 일부 청구항에 대하여 본 국제조사보고서가 작성되지 아니하였습니다.

1. ☐ 청구항:
이 청구항은 본 기관이 조사할 필요가 없는 대상에 관련됩니다. 즉,

2. ☐ 청구항:
이 청구항은 유효한 국제조사를 수행할 수 없을 정도로 소정의 요건을 충족하지 아니하는 국제출원의 부분과 관련됩니다. 구체적으로는,

3. ☐ 청구항:
이 청구항은 종속청구항이나 PCT규칙 6.4(a)의 두 번째 및 세 번째 문장의 규정에 따라 작성되어 있지 않습니다.

제3기재란 발명의 단일성이 결여된 경우의 의견(첫 번째 용지의 3의 계속)

본 국제조사기관은 본 국제출원에 다음과 같이 다수의 발명이 있다고 봅니다.

제1군 발명: 청구항 제1항-제12항은 보안 IP 그룹 확인에 따른 보안 IP 통신 서비스에 관한 것입니다.
제2군 발명: 청구항 제13항-제26항은 IP 변경 정보에 따라 IP를 변환하여 통신을 수행할 수 있는 IP 통신 서비스에 관한 것입니다.

1. ☐ 출원인이 모든 추가수수료를 기간 내에 납부하였으므로, 본 국제조사보고서는 모든 조사 가능한 청구항을 대상으로 합니다.

2. ☐ 추가수수료 납부를 요구하지 않고도 모든 조사 가능한 청구항을 조사할 수 있었으므로, 본 기관은 추가수수료 납부를 요구하지 아니하였습니다.

3. ☐ 출원인이 추가수수료의 일부만을 기간 내에 납부하였으므로, 본 국제조사보고서는 수수료가 납부된 청구항만을 대상으로 합니다. 구체적인 청구항은 아래와 같습니다.

4. ☒ 출원인이 기간 내에 추가수수료를 납부하지 아니하였습니다. 따라서 본 국제조사보고서는 청구범위에 처음 기재된 발명에 한정되어 있으며, 해당 청구항은 아래와 같습니다. 청구항 1-12

이의신청에 관한 기재

☐ 출원인의 이의신청 및 이의신청료 납부(해당하는 경우)와 함께 추가수수료가 납부되었습니다.

☐ 출원인의 이의신청과 함께 추가수수료가 납부되었으나 이의신청료가 보정요구서에 명시된 기간 내에 납부되지 아니하였습니다.

☐ 이의신청 없이 추가수수료가 납부되었습니다.

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/014850

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2007-0081530 A1	2007/04/12	CN 1839592 A	2006/09/27
		EP 1667382 A1	2006/06/07
		EP 1667382 A4	2006/10/04
		WO 2005-027438 A1	2005/03/24
WO 2009-062504 A1	2009/05/22	없음	
JP 2009-163546 A	2009/07/23	JP 5239341 B2	2013/07/17
KR 10-2002-0040102 A	2002/05/30	없음	
KR 10-2010-0086640 A	2010/08/02	KR 10-1015464 B1	2011/02/22