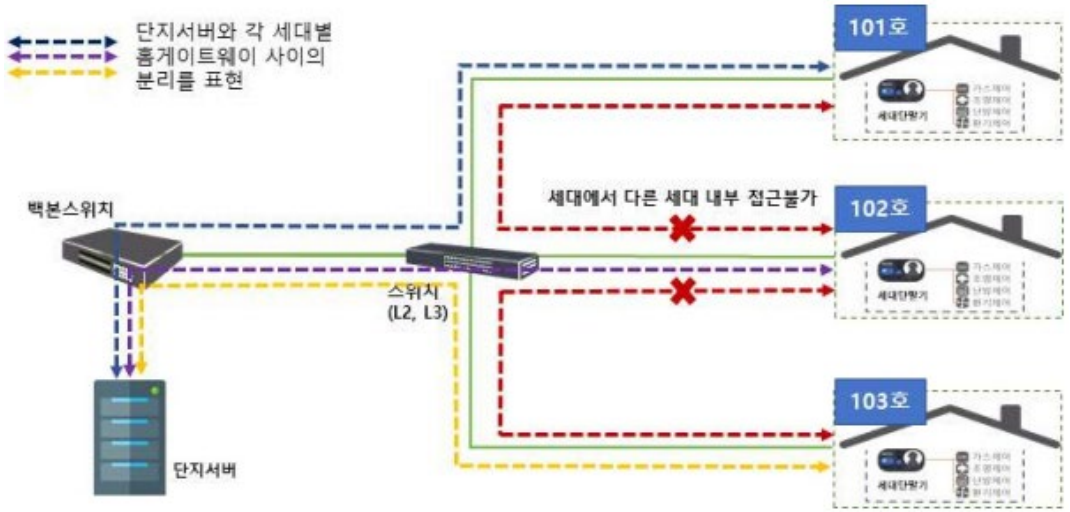
홈네트워크 보안가이드

한국인터넷진흥원 (KISA) 제정 (2022.12.16)

세대별 홈네트워크 기술 기준

- 각 세대와 단지서버 사이의 망은 전송되는 데이터의 노출, 탈취 등을 방지하기 위해 분리하여 구성
- 각 세대망은 단지서버 외에 다른 세대의 내부로 접근할 수 없어야 한다

세대별 홈네트워크 구성 요건 개념도



홈네트워크 보안가이드

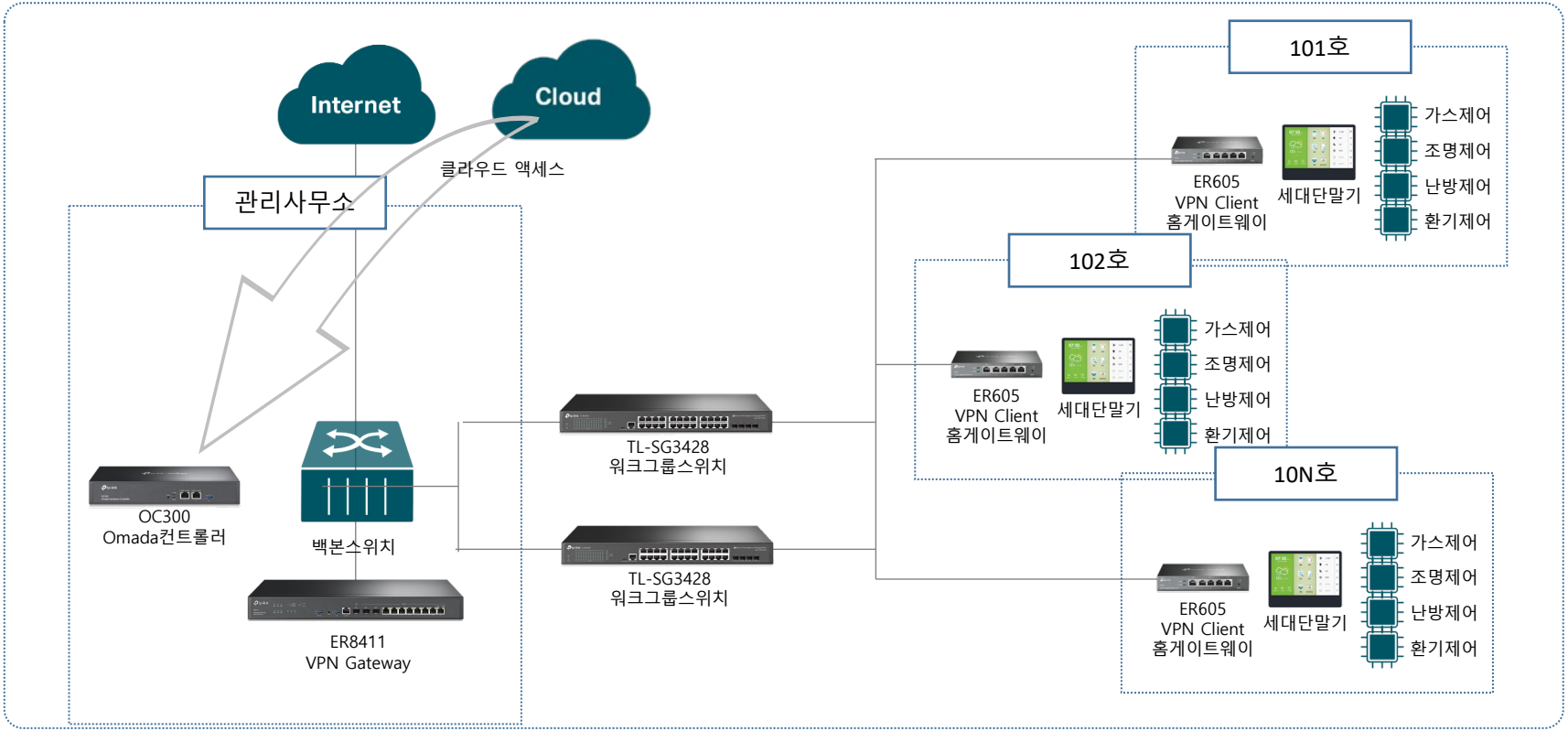
한국인터넷진흥원 (KISA) 제정 (2022.12.16)

분리 방법	기술 예시	상세 사항
물리적 분리 방법	1.1 전용선 라우터	(1) 단지서버로부터 각 세대망까지 성형배선 등의 방식으로 케이블을 연결하여 물리적으로 회선을 분리하여 구축하는 방법 등을 사용한다. (2) 단지서버에서 각 세대로 통신을 위해 인입되는 물리적인 네트워크 케이블을 세대별로 각각 설치하여야 한다. 전용선 라우터 등을 활용하여 세대망을 단일회선으로 구성하여 연결한다.
	1.2 망분리 솔루션	(1) 망분리 솔루션을 이용하여 단지서버망과 개별 세대망을 각각 구성하고 개별 세대망과 서버망을 연계시켜 통신이 가능하게 하도록 구성한다. (2) 세대에서는 단지서버로만 통신가능하며, 세대에서 다른 세대의 내부로의 접속은 불가능하게 구성한다.
논리적 분리 방법	2.1 VPN	(1) 가상사설통신망(VPN)은 VPN 게이트웨이와 VPN 클라이언트간 가상경로를 설정하는 채널(터널)을 만들고 이를 통해 송수신되는 데이터를 암호화하는 기술이다. 이를 통해 각 세대망은 단지서버 외에 다른 세대의 내부로 접근 할 수 없도록 한다. ※VPN의 구성은 IPSec VPN, SSL VPN, L2 VPN(Layer 2 VPN) 등의 방식으로 구현할 수 있다. (2) 단지서버와 각 세대망 간에는 홈네트워크 서비스 및 운영을 위해 필요한 통신만 허용하고 세대에서 다른 세대의 내부로 접속이 불가능하도록 접근제어(IP 주소, Port 등)를 설정하여 관리한다
	2.2 VLAN	(1) 가상근거리통신망(VLAN)은 네트워크 스위치를 이용하여 각 세대별로 개별 네트워크를 별도로 할당함으로써 개별 세대 네트워크망을 논리적으로 분리하는 기술로 각 세대망은 단지 서버 외에 다른 세대의 내부로 접근 할 수 없도록 한다. ※ VLAN은 일반적인 VLAN(IEEE 802.1Q)과 VxLAN(Virual Extensible LAN) 등의 방식으로 구현할 수 있다. (2) 네트워크 스위치(L2, L3 등) 를 이용하여 세대별 가상근거리통신망(VLAN)을 구성한다. 구성 방식에는 포트 기반 구성, IP 주소 기반 구성, MAC 기반 구성 등이 있다. (3) 단지서버와 각 세대망 간에는 홈네트워크 서비스 및 운영을 위해 필요한 통신만 허용하고 세대에서 다른 세대의 내부로 접속이 불가능하도록 접근제어(IP 주소, Port 등)를 설정하여 관리한다.

*Please go to https://omada.tplinkcloud.com to log in with your TP-Link ID.

TP-Link 솔루션

2.1 VPN을 이용한 기술



*Please go to https://omada.tplinkcloud.com to log in with your TP-Link ID.

TP-Link 솔루션 VPN을 이용한 기술

주요 제품 (1/2)

ER605

VPN Client + 홈게이트웨이

ER605
데이터시트

- **Omada SDN에 통합**
  Omada 컨트롤러인 OC300을 통해서 중앙 집중식 관리 및 지능형 모니터링 지원
- **5개의 기가비트 포트**
  고속 유선 연결
- **고성능 VPN**
  최대 20*IPsec, 16*OpenVPN, 16*L2TP, 16*PPTP
- **풍부한 보안 기능**
  강화된 방화벽 정책, DoS 방어, IP/MAC/URL 필터링

ER8411

VPN Gateway

ER8411
데이터시트

- **Omada SDN에 통합**
  Omada 컨트롤러인 OC300을 통해서 중앙 집중식 관리 및 지능형 모니터링 지원
- **강력한 성능**
  2*10G(SFP+) + 1*1G(SFP) + 8*1G(RJ45)
- **고성능 VPN**
  최대 300*IPsec, 110*OpenVPN, 300*L2TP, 300*PPTP (L2TP, PPTP 최대 터널 수 공유)
- **이중 전원 공급 장치**

TP-Link 솔루션 VPN을 이용한 기술

주요 제품 (2/2)

OC300

Omada Hybrid Cloud 컨트롤러

OC300
데이터시트

- **중앙 집중식 관리**
  최대 100대의 Omada 라우터(ER605), 100대의 Omada 스위치(TL-SG3428), 500대의 Omada AP 관리
- **무료 클라우드 액세스**
  언제, 어디서나 Omada 앱 또는 Web UI로 관리 및 모니터링이 가능
- **온프레미스 관리**
  최상의 보안과 안정성으로 로컬에서 장치 관리
- Omada 클라우드 SDN에 대해 더 알아보기

TL-SG3428

24(RJ45)+4(SFP) 기가비트이더넷 스위치

TL-SG3428
데이터시트

- **Omada SDN에 통합**
  Omada 컨트롤러인 OC300을 통해서 중앙 집중식 관리 및 지능형 모니터링 지원
- **고급 L2+ 기능**
  L2/L3/L4 QoS, ACL, 스태틱 라우팅
- **강력한 보안 기능**
  IP-MAC-Port 바인딩, DoS 방어, 스톰 제어, DHCP 스누핑, 802.1x, RADIUS 인증
- **엔터프라이즈급 기능**
  802.1Q VLAN, 포트 미러링, STP/RSTP/MSTP, LACP