

# “강력한 보안과 안정적인 유무선 네트워크 서비스 필수”

중소기업 대상의 네트워크·보안 장비 전문기업인 자이젤코리아(대표 김상현)의 각 산업분야별 구축사례 리뷰를 통해 성공적인 유무선 네트워크 구축 방안을 살펴본다. 이번 호에서는 서울 강남에 위치한 한 공유 오피스(Share Office)의 유무선 네트워크 구축 사례를 통해 최적의 인프라 구축 방안을 제시한다. 공유 오피스는 수많은 입주 기업들이 유무선 네트워크 자원을 공유해 사용하는 만큼 보안은 물론 끊임 없는 안정적인 유무선 네트워크 서비스 제공이 중요하다. 여기에 다양한 요구에 맞는 펌웨어 업데이트 및 정책 설정 등도 필요해 공유 오피스 환경에 적합한 인프라 구현이 필수다. <편집자>



# “유무선 네트워크·보안 최적화로 IT 자원 활용 극대화”

‘통합보안·무선튜닝·현장기술지원’ 중요 ... 자이젤 ‘UTM·스위치·AP·관제 플랫폼’ 주목

최근 공유 오피스에 대한 관심과 이용률이 빠르게 높아지고 있다. 공유 오피스는 건물의 여러 층 또는 전체를 다수의 공간으로 분리해 사무 공간으로 임대하는 한편 회의실이나 로비 등을 공동으로 사용하는 사무실을 의미한다. 여기에 각종 편의시설, 셔틀버스 등 다양한 혜택도 제공되는 등 국내외 기업들이 경쟁적으로 공유 오피스 시장에 진출하면서 급성장하고 있다.

공유 오피스 입주 기업들은 다종다양한 입주 기업 간의 네트워크 형성이 가능하고 타 업종과의 협업을 통한 시너지 창출도 가능하다. 또한 부담 없는 임대료와 함께 도심이나 지하철역과 가까운 곳에 위치해 출퇴근이 용이하다는 이점을 기반으로 공유 오피스 입주 기업들이 빠르게 늘어나고 있다.

## 공유 오피스 네트워크 환경과 이슈

공유 오피스는 많은 스타트업이나 중소기업들이 한정된 공간을 공동으로 사용해 각자의 업무를 처리하게 된다. 다양한 업종의 기업들이 입주해 유무선 네트워크를 공유해 사용하고, 디지털 시대를 대변하듯 수많은 종류의 비즈니스 애플리케이션과 멀티미디어 콘텐츠를 활발하게 사용하면서 트래픽 발생 또한 많다.

이처럼 공유 오피스는 많은 기업들이 물리적 공간만 공유하는 것이 아니라 한정된 네트워크 자원을 공유하기 때문에 예상하지 못한 문제들이 발생할 수 있다. 공유된 네트워크 대역폭을 특정 입주 기업이 전부 사용하게 된다면 전체 네트워크 서비스 품질이 저하될 수 있다. 또한 와이파이 사용을 위해 개별적으로 공유기를

사용하면 무선 채널 간섭이나 신호 중첩에 따라 속도 저하나 접속이 불가할 수도 있다.

공유 오피스는 많은 기업들이 한 곳에 모여 네트워크 등의 제한적인 IT 자원을 사용하기 때문에 다양한 문제들이 발생할 수 있다. 대표적인 문제점은 다음과 같다.

1. 보안: 공유 오피스 환경에서 보안은 늘 위협받는다. 신원 미상자가 정보탈취를 위해 해킹을 시도할 수 있으며, DDoS 공격으로 입주 기업들이 정상적인 서비스를 이용하지 못할 수도 있다. 또한 손쉽게 접근 가능한 게스트 네트워크 접속을 통해 입주 기업들이 자체 구축한 서버를 해킹할 수도 있고, 보안이 불안하면 랜섬웨어에도 쉽게 감염될 수 있다.
2. 와이파이: 수많은 입주 기업이 다양한 무선 단말을 사용해 와이파이에서 접속하기 때문에 속도 저하나 접속 불가 등의 문제가 상시 존재한다. 또한 개별적으로 공유기를 설치해 사용하는 경우 DHCP 교란을 비롯해 무선 신호 중첩이나 채널 간섭으로 인해 유선 네트워크 장애와 와이파이기가 느려지거나 끊김 현상이 나타날 수 있다.
3. 네트워크 자원 분배: 한정된 네트워크 자원의 제어가 없다면 특정 입주 기업이 네트워크 자원을 일방적으로 사용할 수도 있다. 이는 네트워크 병목현상을 발생시키고, 다른 입주 기업들의 인터넷 사용이 느려지는 등의 피해를 유발할 수 있다.
4. 각종 OS와 애플리케이션과 호환: 입주 기업을 위해 다양한 OS와 애플리케이션이 네트워크와의 안정적

인 연결을 보장해야 한다. 유닉스, 맥, iOS, 윈도우, 리눅스, 안드로이드 등 다양한 OS 및 서버가 네트워크를 통해 통신하는 만큼 예상하지 못한 호환 이슈가 간헐적으로 발생할 수도 있기 때문이다.

### 공유 오피스 필수 네트워크 서비스

공유 오피스는 네트워크 자원을 공유해 많은 기업들이 사용하는 만큼 강력한 보안과 끊임 없는 유무선 네트워크 서비스 그리고 펌웨어 업데이트 및 정책 설정 등이 필수로 요구된다. 특히 보안이 허술한 네트워크는 각종 공격의 표적이 되고, 바이러스에 쉽게 감염될 수밖에 없다. 또한 다수의 무선 AP(Access Point)와 공유기의 신호 및 채널 중첩이 존재된 환경이라면 원활한 무선 네트워크 서비스를 위한 무선 튜닝이 반드시 필요하다.

∴ 사용자 보안 위한 통합보안

공유 오피스는 입주 기업을 위해 유무선 네트워크를 서비스하고 있으며 많은 트래픽이 오가고 있다. 여기에는 입주 기업들의 중요한 정보들이 있지만 외부에서 침입할 수도 있다. 만약 네트워크 보안이 허술하다면 입주 기업들의 중요 정보들이 탈취를 당하거나 DDoS 공격으로 업무가 마비될 수 있다. 또한 주요 서버나 PC가 악성코드, 랜섬웨어, 바이러스 등에 감염돼 심각한 피해를 입을 수도 있다.

내부 네트워크에 침투하는 트로이 목마나 백도어 같은 악성 코드를 이용해 정보 탈취를 시도할 수도 있다. 이메일 등 자체 서버를 운영하

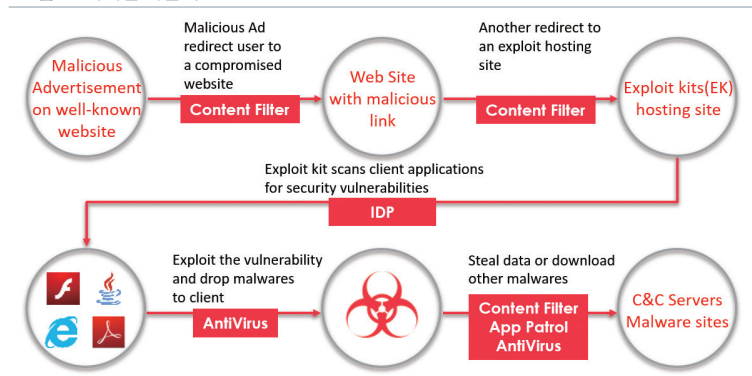
고 있는 공유 오피스 입주 기업들도 있어 유무선 네트워크 보안은 필수로 요구된다.

특히 안티바이러스, 안티스팸, IDP, 콘텐츠 필터링, 앱 패트롤 등 다양한 기능을 지원하는 최적의 네트워크 통합 보안 솔루션 구축이 중요하다. 이에 자이젤은 카스퍼스키, 트렌드마이크로, 사이렌 등 글로벌 보안 기업의 엔진을 통합보안 장비인 USG 시리즈에 탑재해 주기적인 업데이트를 통해 최신 보안 위협으로부터 빠르고 정확한 실시간 보호 기능을 수행한다.

∴ 무선 튜닝으로 신호 중첩·채널 간섭 최소화

공유 오피스는 사무실은 물론 회의실과 휴식공간을 제공한다. 입주 기업들은 와이파이를 연결해 어느 곳에

<그림 1> 자이젤 다단계 보호



<그림 2> 실제 공유 오피스 무선 신호 중첩 현황



서나 업무를 수행할 수 있다. 그러나 한정된 공간 내에서 다수의 입주 기업들이 송수신하는 데이터를 처리하기 위해 많은 AP가 설치된다.

특히 대량의 무선 트래픽 분산을 위해 짧은 거리에 다수의 AP가 설치되며 이로 인해 눈에 보이지 않는 신호 중첩, 채널 간섭이 발생해 와이파이 서비스가 원활하지 않은 경우가 있다. 또한 개별적으로 사용하는 공유기를 연결하면 신호 중첩, 채널 간섭이 더욱 심해질 수 있어 이러한 현상은 와이파이 서비스 장애를 유발해 끊김 및 속도 저하가 일어나지만 눈에 보이지 않아 해결이 쉽지 않다.

이러한 현상 해결을 위해 무선 환경 분석을 통한 무선 튜닝 수행이 필요하다. 주변 무선 네트워크 환경을 분석해 클라이언트의 위치에 따라 안테나 패턴을 변경하는 고성능 AP와 한정된 공간 내에 설치되는 수많은 AP와 공유기로 인한 채널 중첩을 최소화하는 DCS(Dynamic Channel Selection) 기능을 제공하는 높은 수준의 엔터프라이즈급 와이파이 서비스를 지원해야 한다.

**:: 긴밀한 현장 기술 지원 필수**

디지털 시대의 네트워크는 매우 중요하고, 활용도가 높다. 특히 공유 오피스에서는 다양한 입주 기업들이 네트워크를 사용하는 만큼 여러 요구사항이 있다. 웹서버 서비스를 위해 별도의 공인 IP가 필요한 경우, 별도의 보안을 요청하는 경우, 특정 포트 오픈이 필요한 경우, 하나의 공인IP로만 통신이 필요한 경우 등 사용 환경이 천차만별이다.

그러나 네트워크 자원 공유에 따라 특정 입주 기업을 위한 정책 설정 시 전체 네트워크에 영향을 주며, 신규 입주 기업의 또 다른 요구사항이 있다면 수시로 정책 적용 및 설정 변경이 필요하다. 따라서 전문 네트워크 관리자 또는 현장 기술 지원이 필수로, 요구사항에 의

해 정책이나 설정 변경이 진행되는 장비는 테스트 환경이 아닌 실제 운용되고 있는 장비에서 지속적으로 방화벽뿐 아니라 라우팅, NAT 등의 IP 및 경로에 대한 정책 적용 및 변경을 수행해야 한다.

특히 설정 오류는 전체 네트워크에 영향을 주며 인터넷 사용 자체가 불가능한 경우도 있고, 개별 공유기를 잘못 연결하면 다른 입주 기업들은 잘못된 DHCP 할당으로 인해 인터넷 사용이 불가능하거나 잘못된 장비 연결로 인해 루핑이 발생하면 네트워크 장애를 유발한다. 또한 다양한 OS로 인해 장비간의 호환성 이슈가 발생돼 특정 OS는 통신이 불가할 수도 있다.

이렇듯 공유 오피스는 다양하고 변수가 많은 환경인 만큼 예상하기 어려운 문제가 발생할 수 있다. 공유 오피스 네트워크의 지속적인 안정화를 위해 유지보수 담당 기업은 환경에 맞는 세심한 장비 세팅을 수행하며 문제 개선을 위한 솔루션을 제조사에 지속적으로 요청해야 한다.

제조사 역시 요구 환경에 적합하도록 펌웨어를 지속적으로 업데이트해야 하는데 현장의 기술 지원이 없다면 이슈에 대한 트러블 슈팅이 불가하며, 문제에 대처하기 어렵다. 입주 기업들이 네트워크를 공유하는 만큼 유지보수 기업과 장비제조 기업의 전문화된 기술 지원이 필수다.



공유 오피스 적용 장비

모델	상세 사양	수량	수량	수량	수량
		2-4층	5-6층	7-8층	전체
통합보안 장비 USG310	차세대 어드밴스드 통합 보안 게이트웨이 8xGbE RJ-45 포트 (configurable), 2xUSB 인터페이스, 랙마운팅 키트5,000Mbps 방화벽 스크루트, 650Mbps VPN, 550Mbps UTM 모든 라이선스 1년 번들 (AV, IDP, 콘텐츠 필터링, 안티스팸) AP 컨트롤러 지원, 관리되는 AP 갯수 (기본 2 / 최대 34), CC 인증	1	1	1	3
백본 스위치 XGS2210-28	24-포트 GbE L3 라이트 매니지드 스위치/4 SFP+ 업링크 (24xGbE RJ-45 + 4x10GbE SFP+) 정적 라우팅 물리적 스택킹 최대 2대 (96xGbE 포트) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	1	1	1	3
AP 컨트롤러 NXC2500	올인원 무선 컨트롤러 (기본 8 / 최대 64개 AP 관리) 기본 8 / 최대 64 AP 관리 1GbE 스크루트, 정적 방화벽 (6xGbE LAN 포트 + 2xUSB 포트) 자동 치유, 자이메시 (ZyMESH), 부하분산, 캡티브 포털 자이젤 원 네트워크 (ZON 유틸리티) 및 CLI 지원	1	1	1	3
L2 스위치 GS1920-48	48-포트 GbE 스마트 웹 매니지드 L2 스위치 (44 x GbE (RJ-45) + 4xGbE 콤보 (SFP/RJ-45) + 2xSFP) 네트워크 보호기능 (루프 가드, IP 소스 가드 등 지원) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 지원	7	8	9	24
L2 PoE 스위치 GS1920-24HP	28-포트 GbE 스마트 웹 매니지드 L2 802.3at PoE 스위치/24xPoE + 4xGbE 콤보 (SFP/RJ-45) 포트당 30W, 최대 375W PoE 전원 지원 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 지원	4	4	4	12
무선 AP WAC6303D-S	802.11ac 웨이브2 듀얼-라디오 3x3 스마트 안테나 AP 웨이브2 MU-MIMO, 1.6Gbps 결합 데이터 전송 속도 Tx 전력 최대 28dBm, 수신 감도 최소 -103dBm 투인원 스탠드얼론/매니지드 AP 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	41	39	32	112

공유 오피스 실제 구축 사례

다음은 실제 공유 오피스에 적용된 UTM, 무선 최적화와 함께 자이젤의 얼라이(Ally) 서비스를 통한 유무선 통합 네트워크를 구축한 사례다.

공유 오피스 적용 솔루션

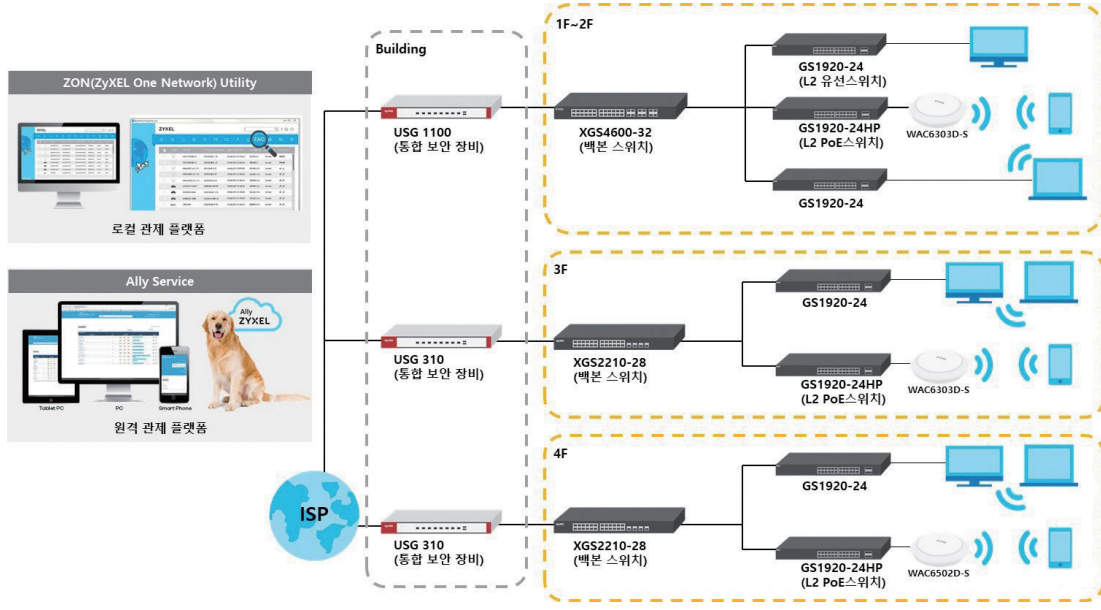
1. 유무선 네트워크 솔루션: 보안 강화를 위한 네트워크 통합보안, 신호 간섭 및 채널 중첩 최소화를 위한 무선 튜닝, QoS(Quality of Service)
2. 네트워크 관제 시스템: 자이젤 얼라이 서비스(원격 네트워크 관제 플랫폼), ZON 유틸리티 로컬 네트

워크 관리 툴, 시큐리포터(SecuReporter)

공유 오피스 각 층별 독립 네트워크 구축

공유 오피스는 보통 하나의 건물 여러 층을 사용한다. 각 층마다 많은 입주 기업들로부터 발생하는 다양한 애플리케이션과 네트워크 트래픽의 증가로 여러 방화벽 정책을 필요로 한다. 만약 한 대의 네트워크 통합 보안 장비로 각 층에 입주한 각각의 입주 기업이 요구하는 애플리케이션 및 보안/게이트웨이 정책 등을 적용하게 되면 너무 많은 정책들을 하나의 장비에서 수시로 업데이트 및 처리하게 된다.

〈그림 3〉 공유 오피스 층별 독립 네트워크 구성도



이는 공유 오피스 전 층의 네트워크에 영향을 줄 수 있고, 많은 트래픽이 오고 가는 공유 오피스 환경에서 하나의 장비가 모든 것을 처리하면 그 처리량에 대한 장비의 부담은 배가 된다. 이러한 문제 방지를 위해 한 대의 장비로 구성하기보다는 각 층별로 회선 및 통합보안 장비를 나눠 독립적인 구성을 하게 되면 효율적으로 네트워크를 구성할 수 있다. 〈그림 3〉과 같이 각 층별로 USG 통합보안 장비를 구축했다.

**공유 오피스 유무선 네트워크 솔루션**

1. 네트워크 통합보안

최근 사이버 공격 트렌드는 금전적 이득을 위해 개인 정보 탈취, 쇼핑몰 웹 솔루션 취약점 공격, 랜덤크랩 랜섬웨어, 액티브엑스 취약점 위협, 암호화폐 거래소 해킹 등 막대한 피해를 주고 파일을 인질화해 금전을 요구하고 있다. 이에 많은 기업들이 보안에 신경을 쓰고 있으며 해킹 피해 최소화를 위해 노력하고 있다. 공유 오피스 또한 많은 기업들이 입주해 유무선 네트워크를 통해

업무를 수행하는 만큼 네트워크 보안 강화는 필수다.

자이젤 USG 시리즈는 차세대 통합보안 장비로 바이러스, 악성코드, 웹 피싱, 스파이웨어, 스팸 등 외부의 불법 침입 시도를 차단한다. 각 기능별로 글로벌 보안 선도 기업인 카스퍼스키 안티바이러스, 사이렌 안티스팸 및 콘텐츠 필터링, 트렌드마이크로 IDP와 앱 패트롤 등을 탑재하고 있다. 또한 스마트 싱글패스 스캐닝 엔진을 사용해 트래픽 처리 지연 시간과 낮은 성능 등을 개선하고, 안티바이러스, IDP, 애플리케이션 패트롤을 동시에 비교해 대기 시간을 크게 줄이고 높은 속도와 커버리지를 제공해 복잡하고 다양한 공유 오피스 각 층의 네트워크를 보호한다.

2. 무선 튜닝

공유 오피스에서는 PC, 노트북, 태블릿 등 다양한 단말을 사용해 사무공간에서 업무를 보고, 회의실에서 회의도 진행한다. 하지만 수많은 공유기와 AP로 인해 동일한 무선 대역 전파 간섭이 증가할 수 있다. 무선 네트

워크에 연결된 클라이언트는 전파 간섭으로 인해 네트워크가 느려지거나 끊김 현상이 나타나며 정상적인 서비스가 안 되는 경우도 있다.

### 자이젤 USG 시리즈 주요 보안 기능 ◇◇◇◇◇◇◇◇

**1. 안티바이러스: 멀웨어, 악성코드 등 바이러스 차단**  
바이러스, 트로이 목마, 웜, 악성웨어를 포함한 멀웨어 등과 HTTP, HTTPS, FTP 등 주요 프로토콜에서 트래픽을 검사해 위협으로부터 보호한다. 또한 패스트-스트림 기반 스캐닝으로 파일 크기에 제한 없이 실시간 보호를 제공하며 클라우드 데이터베이스를 지원해 최신 유형의 바이러스를 실시간으로 업데이트해 차단한다.

**2. IDP: DDoS, 백도어 등 침입 탐지 및 방어**  
제로데이 공격에 대한 보안을 수립하고 비정상적인 트래픽 탐지 및 방지를 통해 네트워크 환경을 보호한다. 자이젤 IDP는 레이어 7 상황에 따른 보안 위험요소를 분석하며 DPI(Deep Packet Inspection) 기능으로 침입 및 탐지와 함께 클라이언트 및 서버 취약점을 보호한다.

**3. 안티스팸: 악성 스팸 메일 차단**  
메일을 통해 들어오는 멀웨어 및 스팸, 피싱 공격을 클라우드 기반의 안티스팸을 활용해 보호한다. RPD(Recurrent Pattern Detection) 기술을 사용해 수집된 메일의 트래픽을 자동 분석해 전 세계적으로 유포되는 스팸 메일을 탐지 및 차단한다. 또한 클라우드 기반 프라-페리미터(Pre-perimeter) 방어 시스템을 활용해 악성 프로그램으로부터 메일을 보호한다.

**4. 콘텐츠 필터 2.0: 웹 URL 기반 제어**  
콘텐츠 필터는 URL 기반 웹 제어를 지원한다. 카테고리를 통해 부적절한 사이트와 소셜 네트워킹 사이트 등 특정 유형의 웹 콘텐츠를 쉽게 차단한다. 지속적으로 분석하고 쌓인 1400억 개 이상의 대규모 클라우드 기반 URL 데이터베이스를 바탕으로 악성 웹 콘텐츠에 대해 높은 정확도와 광범위한 즉각적인 보호를 제공한다. 또한 원하는 특정 웹사이트만 허용 또는 차단을 지원해 웹 접속을 제어한다.

**5. 앱 패트롤: 애플리케이션 제어**  
앱 패트롤은 레이어 7 애플리케이션에 대한 관리 및 제어를 제공한다. 최대 19개의 카테고리 및 수천 개의 애플리케이션 관리 및 제어를 제공하며, DPI 엔진을 사용해 관리자가 애플리케이션을 식별하고 분류할 수 있도록 한다. 다양한 제어 모드(Prioritize, BWM, Block)를 제공해 적합한 애플리케이션 제어를 효과적으로 적용한다.

이러한 신호 간섭과 채널 중첩 현상 완화를 위해 자이젤 무선 솔루션은 대다수 공유기가 사용하는 2.4GHz가 아닌 5GHz 채널 대역에서 DFS(Dynamic Frequency Selection) 기능을 통해 기존 5GHz 대역 이외에 추가적인 8개 가용 채널을 확장해 채널 대역을 확보한다. 그리고 DCS 기능을 통해 무선 환경을 최적화한다.

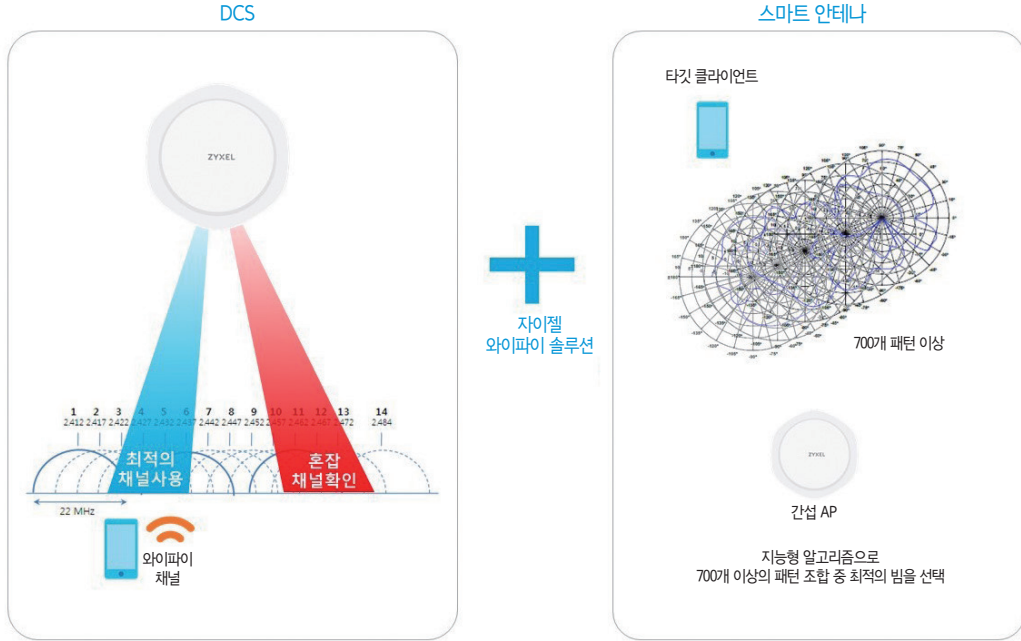
DCS의 메커니즘은 BSS(Basic Service Set) 내에 AP와 클라이언트 간의 새로운 채널이 필요한지 여부를 검색하고 결정한다. DCS가 동작하기 위해 AP는 여러 클라이언트에 채널에 대한 신호 품질 측정을 요청하고, BSS 내의 클라이언트에서 탐지한 모든 채널의 수신 신호 강도(RSSI) 및 패킷 에러율(PER)을 기반으로 채널 신호 품질 보고서를 AP에 보내준다.

신호 품질 보고를 토대로 품질이 좋지 않다면 새로운 채널을 검색한다. 다른 공유기 또는 AP와의 파장 간섭이 발생하지 않으며, 안정적이고 양호한 채널을 선택하게 되며, 최적의 선택으로 채널간섭을 최소화한다.

DCS와 더불어 자이젤의 지능형 스마트 안테나는 최적의 무선 환경을 제공한다. 자이젤 스마트 안테나 기술은 내장된 지능형 알고리즘을 사용해 클라이언트의 위치와 현재 무선 네트워크 환경을 분석해 700개 이상의 안테나 패턴 조합에서 클라이언트에 맞는 최적의 안테나 패턴 계산과 동시에 주변 환경의 신호 간섭을 감지해 최소화된 신호 간섭과 클라이언트의 상황에 맞는 최적의 안테나 패턴을 분석해 형성한다.

이 동작은 1초안 안에 이뤄지며 클라이언트는 최적의 와이파이 신호를 받게 된다. 연결되는 모든 클라이언트에 따라 각각 안테나 패턴이 적용되며 클라이언트가 이동 중에도 끊임없이 안테나 패턴을 분석하고 선택한다. DBS(Dynamic Beam Shaping)를 적용해 최고 수준의 성능을 보장하며, 360도 커버리지를 통해 클라이언트가 어디에 있던 항상 최적의 와이파이 서비스를 제공할 수 있다.

〈그림 4〉 DCS + 스마트 안테나



### 3. QoS

QoS는 입주 기업이나 애플리케이션의 우선순위에 따라 트래픽과 대역폭을 정적으로 특정 수준의 품질을 보장하거나 한정된 네트워크 자원 내에서 각 입주 기업에 대역폭 제한을 수행해 모든 입주 기업들의 서비스 품질을 유지한다. 이렇듯 특정 입주 기업의 한정된 네트워크 자원의 과도한 사용을 제어해 안정적으로 네트워크 품질을 관리할 수 있다.

## 네트워크 관리 시스템

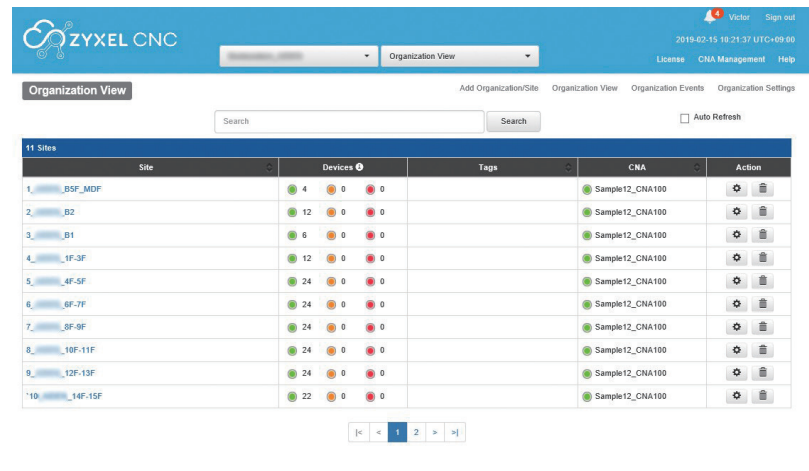
### 1. 자이젤 얼라이 서비스

공유 오피스는 각 층별로 네트워크를 별도로 구축하기 때문에 이를 통합 관리하는 솔루션이 필요하다. 자이젤

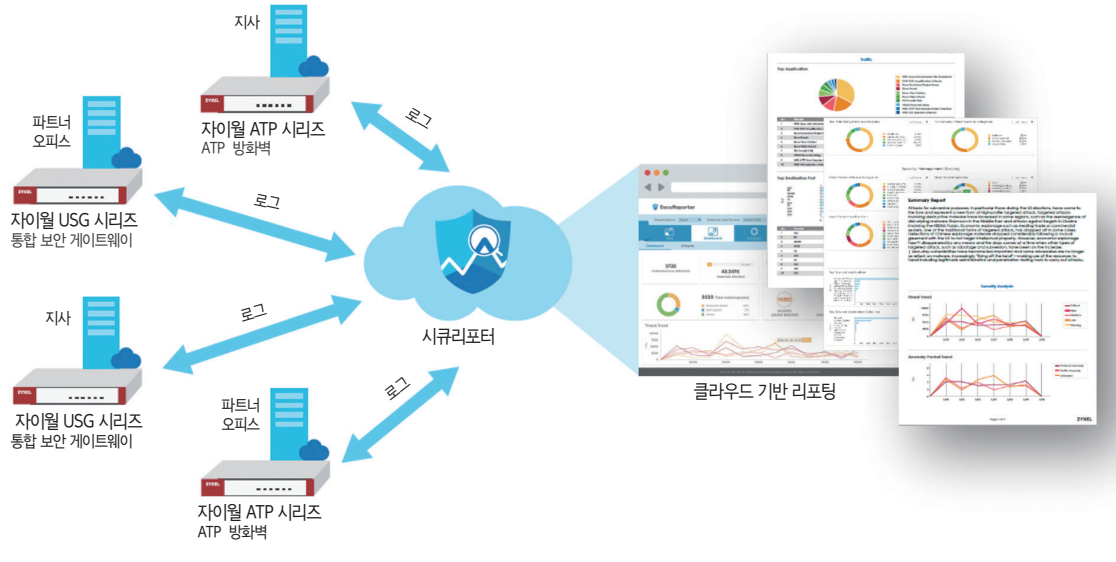
얼라이 서비스는 클라우드 플랫폼 기반으로 공유 오피스의 각 층별로 구축된 자이젤 장비의 실시간 원격 관제가 가능하며 설치돼 있는 장비들의 위치와 장비 수량을 쉽게 파악할 수 있다.

메인 화면에 장비의 상태가 각각 초록/주황/빨간색으

〈그림 5〉 자이젤 얼라이 서비스 메인 화면



〈그림 6〉 자이젤 시큐리포터



로 표시돼 장애 여부를 빠르게 판단할 수 있으며 이벤트 발생 시 이벤트 로그가 기록돼 어떤 장애가 발생했는지 확인할 수 있다. 또한 이벤트 발생 시 플랫폼에 설정한 메일로 이벤트 정보가 발송돼 외부에서도 장애 발생을 실시간으로 파악할 수 있다.

설정된 날마다 자동으로 클라우드 서버로 컨피그 백업이 이뤄지며 장비 장애 발생 시 관제 플랫폼에서 컨피그를 다운받아 대체 장비에 컨피그를 복사해 장애 복구 시간을 단축시킬 수 있다. 24시간 서비스를 보장해야 하는 공유 오피스에서 안정적인 유무선 네트워크 서비스 제공은 물론 언제 어디서든 장비들의 이상 유무를 한눈에 파악할 수 있는 원격관제 플랫폼은 공유 오피스 운영에 있어 필수다.

## 2. ZON 유틸리티 로컬 네트워크 관리 툴

ZON(ZyXEL One Network)은 UTM, 스위치, AP 등을 한 번에 관리할 수 있는 네트워크 통합 관리 솔루션이다. 자이젤은 자체 R&D와 생산공장을 보유한 제조 능력과 더불어 모든 네트워크 제품 라인에 대한 핵심

기술을 바탕으로 프로그램을 개발했다. 이 프로그램은 자이젤 홈페이지에서 무료로 다운로드 받아 사용할 수 있다.

## 3. 시큐리포터

시큐리포터는 자이젤 제품을 위해 설계된 클라우드 기반 지능형 리포트다. 이상 트래픽 발생 로그 확인이 가능하고, IDP/안티바이러스/안티스팸 등 보안 트래픽 정보 확인과 자이젤 USG 장비의 IP정보/CPU/인터페이스/세션 등 장비의 상세정보를 확인할 수 있다.

특히 구글 맵 기반으로 위치, 장비 이름, IP주소 등의 정보를 표시할 수 있으며 대시보드 커스터마이징, 관리 계정별 권한 등급 부여, 일간/주간 리포트 PDF 발송 등 다양한 기능을 제공한다.

### 자이젤 원 네트워크 솔루션(공유 오피스 추천 모델)

분류	장비군	모델	상세 사양	비고
UTM	방화벽	USG1100	차세대 익스트림 통합 보안 게이트웨이 8xGbE RJ-45 포트 (configurable), 2xUSB 인터페이스. 랙 마운팅 킷 6,000Mbps 방화벽 쓰루풋, 800Mbps VPN, 650Mbps UTM 모든 라이선스 1년 번들 (AV, IDP, 콘텐츠 필터링, 안티스팸) AP 컨트롤러 지원, 관리되는 AP (기본 2대 / 최대 130대) CC 인증	대형 공유 오피스
		USG310	차세대 어드밴스드 통합 보안 게이트웨이 8xGbE RJ-45 포트 (configurable), 2xUSB 인터페이스, 랙마운팅 킷 5,000Mbps 방화벽 쓰루풋, 650Mbps VPN, 550Mbps UTM 모든 라이선스 1년 번들 (AV, IDP, 콘텐츠 필터링, 안티스팸) AP 컨트롤러 지원, 관리되는 AP (기본 2대 / 최대 34대) CC 인증	중소형 공유 오피스
스위치	백본 스위치	XGS4600-32F	32-포트 GbE L3 매니지드 스위치/4 SFP+ 업링크 (24xSFP + 4xGbE 콤보 (SFP/RJ-45) + 4x10GbE SFP+) 플래시/RAM (64MB/1GB), 전원 이중화 탑재 물리적 스택킹 최대 4대 (112xGbE 포트) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	대형 공유 오피스
		XGS2210-28	24-포트 GbE L3 라이트 매니지드 스위치/4 SFP+ 업링크 (24xGbE RJ-45 + 4x10GbE SFP+) 정적 라우팅 물리적 스택킹 최대 2대 (96xGbE 포트) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	중소형 공유 오피스
	L2 워크그룹 스위치	GS1920-48	48-포트 GbE 스마트 웹 매니지드 L2 스위치/44xGbE (RJ-45) + 4xGbE 콤보 (SFP/RJ-45) + 2x SFP 네트워크 보호 기능 (루프 가드, IP 소스 가드 등 지원) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 지원	48포트 L2 스위치
		GS1920-24	28-포트 GbE 스마트 웹 매니지드 L2 스위치/24xGbE (RJ-45) + 4xGbE 콤보 (SFP/RJ-45) 네트워크 보호 기능 (루프 가드, IP 소스 가드 등 지원) 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 지원	24포트 L2 스위치
	PoE 스위치	GS1920-24HP	28-포트 GbE 스마트 웹 매니지드 L2 802.3at PoE 스위치/24xPoE + 4xGbE 콤보 (SFP/RJ-45) 포트당 30W, 최대 375W PoE 전원 지원 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 지원	
AP	무선 AP	WAC6303D-S	AP802.11ac 웨이브2 듀얼-라디오 3x3 스마트 안테나 AP 웨이브2 MU-MIMO, 1.6Gbps 결합 데이터 전송 속도 최대 Tx 전력 28dBm, 최소 수신 감도 -103dBm 투인원 스탠드얼론/매니지드 AP 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	웨이브2 MU-MIMO 스마트 안테나 AP
		WAC6502D-S	802.11ac 듀얼-라디오 2x2 스마트 안테나 AP, 1.2Gbps 결합 데이터 전송 속도 최대 Tx 전력 28dBm, 최소 수신 감도 -100dBm 투인원 스탠드얼론/매니지드 AP 자이젤 원 네트워크 (ZON 유틸리티, 스마트 커넥트) 및 CLI 지원	스마트 안테나 AP
AP 컨트롤러	AP 컨트롤러	NXC2500	올인원 무선랜 컨트롤러 (기본 8대 / 최대 64대 AP 관리) 1GbE 쓰루풋, 정적 방화벽 (6xGbE LAN 포트 + 2xUSB 포트) 자동 치유, 자이메시 (ZyMESH), 부하분산, 캡티브 포털 자이젤 원 네트워크 (ZON 유틸리티) 및 CLI 지원	최대 64대 AP 관리
로컬 NMS	ZON	ZON 유틸리티	로컬 네트워크 통합관리 솔루션 디바이스 발견 / IP 주소 셋팅 / 디바이스 공장 초기화 (최대 250대)	
실시간 NMS	원격 관제 플랫폼	얼라이 서비스	원격 관제 플랫폼 (클라우드 네트워크 센터) 1. 실시간 네트워크 헬스 체크 2. 문제 발생 시 실시간 안내 및 리포트 3. 스케줄링 (펌웨어 업그레이드, 컨피그 백업) 4. 원격 접속	