WireLESS, Communicate MORE

Samsung
Wireless Enterprise

삼성 보안 AP

WHITE PAPER

SAMSUNG

삼성 보안 AP

들어가며...

현재 기업용 무선랜 네트워크는 빠른 속도, 강화된 인증과 암호화 등의 표준화를 기반으로 다양한 단말을 통하여 기업의 중요 업무를 담당하는 인프라로 성장하고 있습니다. 그럼에도 불구하고 고객은 지속적으로 무선구간에서의 보안위협과 성능 및 운영의 이슈를 제기하고 있는 것도 사실입니다. 이에 많은 고객들은 무선침입차단시스템(WIPS) / 무선침입탐지시스템(WIDS)의 도입을 고려하고 구축하고 있습니다. 이에 본고에서는 시장에 다양하게 판매되고 있는 무선침입방지시스템의 구성 및 구축방법의 장단점과 도입 시 반드시 고려해야 할 사항을 알아보고, 마지막으로 상기와 같은 관점에서 삼성 보안 AP의 차별화 기능을 소개 드리고자 합니다.

먼저 WIPS가 나온 배경과 발전과정을 살펴보겠습니다. 이는 현재의 제품들이 왜 서로 다른 구조로 서비스를 하고 있는지 이해할 수 있는 좋은 방법이라고 생각됩니다.
대부분의 WIPS는 초기의 무선랜이 해커들의 "기업 네트워크의 침입경로"로 사용되었을 때부터입니다. 보통 잘못 설정된 AP 또는 허가받지 않은 AP에 접속하여 보안Key를 Cracking 하고 그 Key를 사용하여 재 침입하는 방식이었습니다. 이에 대한 초기 대응은 수동적으로 무선네트워크를 스캐닝하여 주변의 동작하고 있는 AP를 찾아 수동으로 조치하는 수준이었습니다. 이러한 방법은 WLAN이 성장함에 따라 부족할 수 밖에 없었으며, 이에 중앙에서 여러 센서를 관리하여 무선네트워크를 모니터링하는 솔루션이 탄생하게 되었습니다. 이러한 초기 WIPS는 유선 네트워크에서 이미 광범위하게 사용되고 있었던 IPS와 동일한 구조였고, 순수하게 WIPS 만을 목적으로 하는 단독형 WIPS 솔루션이었습니다. 즉 무선네트워크를 모니터링하는 센서와 센서로부터 취합되는 정보를 중앙에서 서버가 분석 (시그니쳐 기반, 행위 기반, ACL, Policy 기반 등)하여 관리자에게 정보를 제공하고, 관리자는 그 정보(보고서나 알람)를 보고 해당 불법 AP 및 침입자를 물리적으로 제거하는 방식이었습니다.
(이후 자동 차단 및 격리로 발전하게 됩니다.)

Fat AP 시대를 지나 WLAN 에 AP Controller가 등장하기 시작했습니다. AP Controller를 기반으로 하는 무선랜 제조사들은 제한적인 무선 탐지 기능을 Controller에 탑재하여 제공하기 시작했고, 이를 통해 자연스럽게 AP가 센서로 활용되기 시작했습니다. 이러한 AP가 무선랜을 모티터링하는 방식은 무선서비스와 동일한 채널을 탐지하거나 주기적으로 서비스 채널이 아닌 다른 채널을 감시하는 방식으로 구현되었습니다. 이러한 방식은 제한적인 탐지/차단 방식이었지만 초기 대응 방법과 비교하면 운영 및 투자비 관점에서 효율적인 면이 있었습니다.

점차 무선랜 업체들은 고객의 커져만 가는 보안 Needs에 대응하기 위해 WIPS 업체를 인수하여 무선랜 통합형 WIPS 제품의 성능과 기능을 더욱 강화시키고 있습니다. 서비스 AP에서 탐지를 동시에 수행하던 방식에서 서비스 AP의 소프트웨어를 변경하여(하드웨어 변경 없이) 센서 역할을 하도록 한 Full-time 센서 용 AP와 Controller가 아닌 별도의 WIPS 서버도 시장에 출시 됩니다.

반면 독립적인 WIPS 제품을 보유한 업체들도 가만히 지켜만 보지 않았습니다. 기 구축된 무선랜 인프라로부터 인가된 장비의 리스트를 공유받고 무선랜 AP의 스캔 정보도 제공받아 독립적인 WIPS 센서의 스캔 및 모니터링 능력을 추가적으로 보강하여 대응하였습니다. 하지만 특정 벤더 간에 국한되어 있는 실정입니다.

이와 같은 형태로 무선랜과 WIPS 제품은 상호 발전하여 오늘날과 같은 WIPS 제품 및 시장으로 형성되었습니다. 그러면 이제 두 종류의 제품의 차이점과 장단점을 살펴보도록 하겠습니다.

먼저 독립형 WIPS는 별도의 WIPS Controller 와 WIPS 센서로 이루어져 있다고 앞서 설명 드렸습니다. 즉 WIPS 센서 측면에서 보면 무선 서비스를 하는 AP와 별도의 센서가 보안을 위하여 무선랜을 모니터링하고 있는 것입니다. 이렇게 함으로써 무선랜에 대하여 센서의 Full Time Scanning이 가능해집니다. 또한 무선랜 서비스 때문에 AP의 Channel Utilization이 증가하더라도 센서의 Detection rate가 떨어지는 상관 관계는 없어집니다. 또한 별도의 전용 WIPS 센서를 통하여 모니터링한 정보에 대한 분석을 센서 자체적으로 수행하여 알람 및 필요정보만WIPS Controller로 전송함으로써 본-지사 구조에 유연하게 대처할 수 있습니다.
한편 독립형 WIPS는 기 구축되어 있는 무선랜 인프라의 무선랜 서비스에 관여하지 않음으로 Physical Layer 와 Data Link layer의 트래픽을 모니터링하는데 한계가 있습니다. 또한 무선랜 인프라의 인가된 디바이스, RF 상태, 위치 정보 등의 활용에 제한적이기 때문에 기 무선랜 인프라와 유기적인 연동 및 통합 운영에 제약이 있습니다. 구축 비용 측면에서 살펴보면 무선랜 인프라와는 별개로 WIPS Controller, WIPS 센서, PoE 스위치 등을 추가로 설치해야 함으로 도입 비용이 부담스러울 수 있습니다.

이제는 통합형 WIPS 솔루션에 대하여 알아보겠습니다. 통합형 WIPS의 구조는 무선랜 서비스용 AP가 무선랜 서비스를 하다가 주기적으로 무선랜 서비스를 중단하고 보안을 위해 모니터링하는 구조로 되어 있습니다. 또한 서비스용 AP를 센서 전용 모드로 변경하여 사용하기도 합니다. WIPS Controller 측면에서 보면 초기에는 무선랜 Controller에서 WIPS 관련 제어를 같이 제공하다가 무선랜 업체를 인수하면서 별도의 WIPS Controller를 사용하는 제조사도 생겨났습니다.

삼성 보안 AP

이러한 구조의 통합형 WIPS 솔루션의 가장 큰 장점은 구축 비용이 독립형 WIPS보다 상대적으로 저렴하다는 점입니다. 기존 무선랜 인프라를 공통으로 사용함으로써 최소의 비용(라이선스 비용 또는 WIPS Controller만 구매 등)으로 WIPS 솔루션을 도입할 수 있기 때문입니다. 또한 인가된 무선랜 서비스를 모니터링하고 무선랜 서비스 내의 공격과 불법 디바이스를 파악하는데 유리합니다. 반면, 무선랜 서비스 중이 아닌 다른 채널 및 주파수 대역을 모니터링하는 능력에는 한계가 있습니다.
또 다른 통합 WIPS 솔루션의 형태인 무선랜용 AP를 모드 변경을 통하여 센서 전용으로 사용한다면 상기와 같은 문제점이 해결 될까요? 이 경우에는 다른 문제점이 발생할 수 있습니다. 오늘날 대부분의 무선랜 제조사의 AP는 AP Controller에 많은 기능을 의존하는 Thin AP 형태로 구현되어 있습니다. 이러한 Thin AP를 모니터링 모드로 변경하여 WIPS 센서로 활용할 경우에는 센서 내에서 분석기능을 수행할 수 없기 때문에 모니터링한 데이터를 모두 WIPS Controller나 무선랜 Controller로 전송하여 분석 처리 후 불법 디바이스 판단 및 차단을 수행하게 됩니다. 이런 경우 본-지사 구조로 구축 시 WAN 구간 대역폭의 제약으로 인해 유연한 대처가 어려울 수 있습니다.

지금까지 말씀 드린 내용을 표로 정리해 보았습니다.

		독립형	통합형
WIPS구성	센서	전용 WIPS 센서로 Full Time 모니터링 하는 방식	무선랜용 AP 에서 주기적으로 모니터링을 같이 하는 방식
			무선랜용 AP를 센서모드로 변경하여 Full Time 모니터링하는 방식
	제어	전용 WIPS Controller	무선랜 Controller 내장형
			전용 WIPS Controlle
모니터링 (탐지) 분석/차단 방식		Full Time Scanning	Time Sliced Scanning 채널, 주파수 Hole 발생 가능성 높음
			Full Time Scanning
		무선랜 서비스 Load 증가와 관계없이 모니터링 가능	무선랜 서비스 부하 증가에 따라 모니터링 능력 저하됨

	독립형	통합형
모니터링 (탐지) 분석/차단 방식	모든 채널 및 주파수 대역 모니터링 가능 Flood attack, DoS Attack 차단에 효과적 channel hopping 방식으로 모니터링 함으로 지속적인 동일 채널 모니터링에 제한적	현재 서비스 중인 무선랜(채널, 주파수) 모니터링에 유리 서비스 중인 채널 및 주파수 외 다른 채널, 주파수 모니터링은 제한적
	센서 내 분석/차단 기능 수행	일반적으로 센서는 모니터링한 데이터를 컨트롤러로 전송하고 컨트롤러는 분석 후 차단 명령 수행
구축 / 구성	캠퍼스 구조, 본-지사 구조 모두 용이 무선랜 인프라와 별개로 각각 설정	본-지사 구조 대응 어려움 무선랜, WIPS 설정 기능 연동으로 관리가 상대적으로 용이함
구축 비용	전용 WIPS 센서, Controller 구매 유선망 연결용 스위치 구매	별도 센서 추가 구매 없음 제조사에 따라 Controller 구매 필요 독립형 WIPS에 비하여 상대적으로 저렴

충분하지는 않지만 독립형 WIPS와 통합형 WIPS의 탄생 배경 및 동작 방식 그리고 각각의 장단점을 파악하셨다고 생각됩니다.

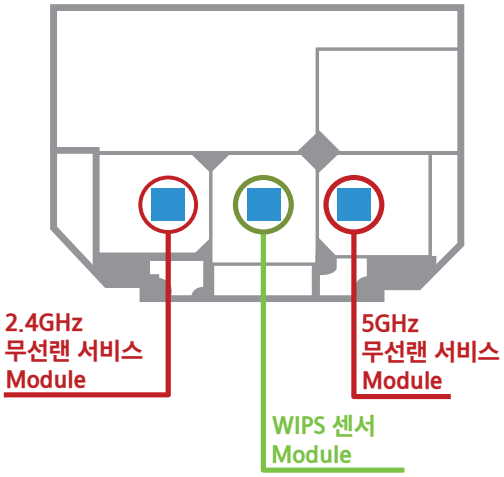
그렇다면 삼성 보안 AP는 어떠한 형태이고 어떻게 동작하며, 어떤 장점을 가지고 있을까요? 이에 대하여 알아보도록 하겠습니다.

한번에 두마리 토끼를 잡는 삼성 보안 AP

결론부터 이야기하자면 삼성 보안 AP는 전용 WIPS 센서가 추가로 내장된 무선랜 AP 입니다. 좀 더 자세히 설명드리겠습니다. 겉으로 보기엔 위에서 설명드린 통합형 WIPS 와 다르지 않습니다. 하지만 내부를 들여다보면 얘기가 달라집니다. 즉 무선랜 인프라용 AP가 무선랜 서비스를 하다가 주기적으로 모니터링을 하는 통합형 WIPS 센서와는 달리 삼성 보안 AP는 내장되어 있는 별도의 WIPS 센서 모듈이 보안 모니터링을 담당하고, 무선랜 서비스용 모듈은 무선랜 서비스에 충실하게 됩니다. 이렇게 함으로써 서두에 말씀드린 통합형

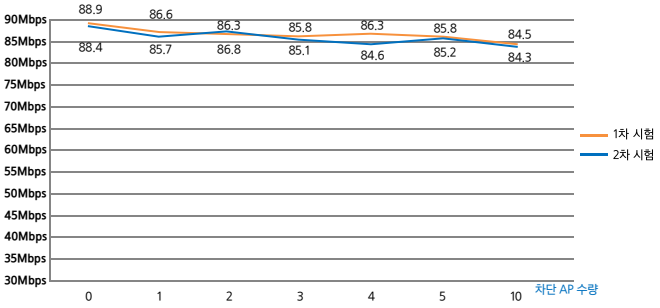
삼성 보안 AP

WIPS 와 단독형 WIPS의 장점을 모두 수용하여 완벽한 무선랜 보안 성능과 효율적인 무선랜 운영을 할 수 있도록 합니다.



<그림1. 삼성 보안 AP RF 구조도>

[그림1] 에서와 같이 무선 서비스용 RF 모듈과 WIPS 센서 용 RF모듈을 HW기반으로 별도 탑재하고 있습니다. 아래 [그래프1]은 불법 AP의 차단 수를 증가시키면서 동시에 서비스 되고 있는 무선랜의 Throughput 성능을 시험한 자료입니다.

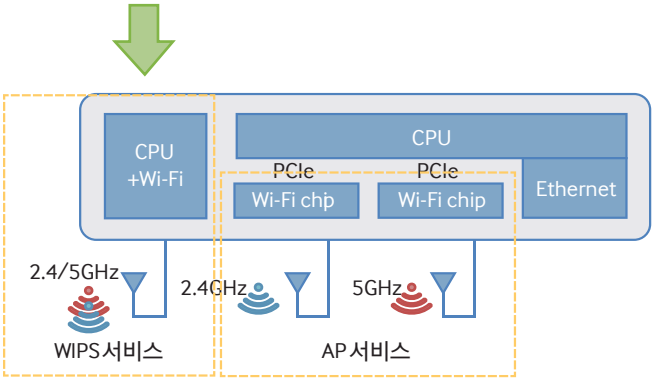


<그래프 1. 차단 AP 증가에 따른 무선랜 성능 비교>

만약 무선랜용 AP로 주기적으로 모니터링하는 통합형 WIPS 센서의 경우 무선랜 서비스와 모니터링을 동시에 수행하면 Channel Utilization이 증가할수록 Detection 능력이 급격히 악화되는 현상이 발생할 것입니다.

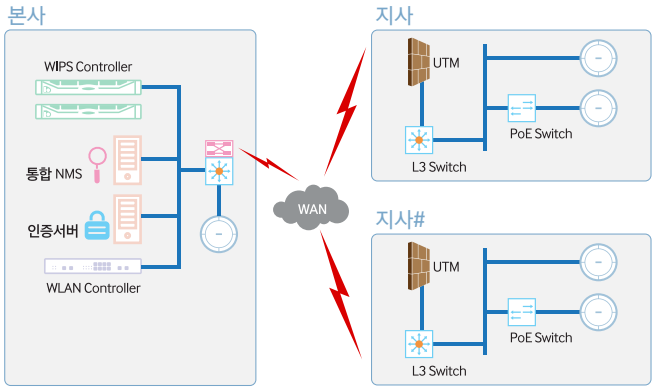
그렇다면 무선랜용 AP의 모드를 센서 모드로 변경하여 Full Time Scanning하는 WIPS 센서는 삼성 보안 AP와 무엇이 다를까요?

전용 센서를 통해 탐지/차단 알고리즘 수행



<그림2. WIPS 모듈 내 탐지/차단 알고리즘 지원>

[그림2]와 같이 삼성 보안 AP의 WIPS 모듈은 별도의 Wi-Fi Chip과 CPU를 보유하고 있습니다. 이를 활용하여 보안 AP 에서 모니터링(취합)한 데이터를 보안 AP 내에서 분석하고 탐지/차단을 직접 수행합니다. 이러한 방법은 무선랜용 AP를 센서모드로 변경하여 모니터링만 하는 WIPS 센서와는 차별화된 성능과 유연성을 제공합니다. 신속한 탐지 및 차단 뿐만 아니라 WIPS Controller로 최소의 알람 및 Management Frame만 전송함으로써 기존 유선망에 부하를 주지 않아 특히 본-지사 무선랜망 구축 시 WIPS Controller를 지역마다 구축할 필요가 없습니다.



<그림3. 본-지사 무선랜/무선보안 구성도>

위의 구성은 전형적인 기업의 본-지사 네트워크 구성입니다. 일반적으로 WAN 구간의 대역폭은 LAN 구간보다 훨씬 부족합니다. 전용선 비용문제와 사용빈도 및 용도에 따라 큰 대역폭을 유지한다는 것은 당연히 낭비요소이기도 합니다. 이러한 구조에서 지사에 있는 WIPS 센서가 모니터링한 데이터를 본사의 WIPS Controller로 전송한다면 WAN 구간의 병목현상은 물론 실제 사용하고자 하는 트래픽 역시

삼성 보안 AP

원활한 통신을 할 수 없을 것입니다.
삼성의 보안 AP는 전용 모니터링 모듈에서 모니터링 데이터를 분석하여 탐지/차단을 직접 수행하고 최소의 관리 데이터만 WIPS Controller에 전달함으로써 유연한 네트워크 구성을 제공합니다.

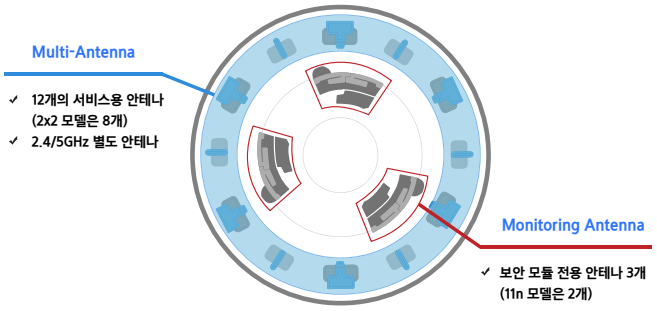
WIPS 도입 시 고려사항

지금까지 시장의 주류를 형성하고 있는 통합형 WIPS 와 단독형 WIPS의 장단점을 살펴보고 삼성의 보안 AP가 왜 WIPS 센서를 내장했는지, 그렇게 함으로써 고객에게 어떠한 장점을 제공할 수 있는지를 살펴 보았습니다.

이제 WIPS의 Architecture는 잠시 접어두고 WIPS 도입 시 고려해야 할 사항을 알아보도록 하겠습니다.

1. RF Monitoring : 802.11 기반의 모든 채널을 모니터링할 수 있어야 합니다. 나라마다 사용하지 않는 채널, non-WiFi interference를 통하여 공격이 가능하기 때문입니다. 또한 동일한 지역에 몇 개의 WIPS 센서가 필요한지, WIPS가 Bandwidth를 얼마나 소모하는지도 고려해야 합니다.
2. 탐지/차단 : 보안 위협에 대한 탐지 시 제약 사항이 있는 지 확인해야 합니다. 기업 네트워크의 NAT, VLAN, Encryption 과 같은 구성에 방해 받지 않고 탐지가 가능해야 합니다. 차단 기능에는 무선 연결 차단, 유선 스위치 차단, 기존 인프라와 ACL 연동 등 여러 가지 방법이 있습니다. 이러한 방법들이 유기적으로 연동되고 원하지 않은 Side Effect가 없어야 합니다. 또한 가장 중요한 것은 차단율입니다. 실질적으로 차단을 수행했지만 RF 세기 및 HW Resource 부족으로 차단이 안될 수 있습니다.
3. 위치 정보 : AP와 Client의 위치를 지도상에 표시하는 기능입니다. 위치 정보는 정확도가 중요합니다. 보통 정확도는 센서나 AP의 수에 비례하며 이는 도입 비용과도 관계가 있습니다. 어떻게 불법 AP와 Client의 위치를 정확하게 제공할 수 있는지 확인해야 합니다.
4. Compliance Report : 정기적/비정기적 리포트를 자동 또는 On-demand type으로 생성할 수 있어야 합니다. 또한 특정 산업에서 규정하고 있는 보안 규정의 Compliance Report를 Export 하는 기능으로 관리자의 업무를 줄일 수 있습니다.
5. Certification : 보안 관련 인증 보유 여부 (예, CC EAL2, FIPS 등)
6. High availability and scalability : WIPS Controller 장애 시 WIPS 센서 동작 여부와 장애 시간 동안 모니터링된 데이터의 저장 분량과 리포트 생성 가능 용량을 확인하여 업무에 영향을 주지 않아야 합니다.

WIPS 도입 고려 시 적어도 상기 6항목 정도는 상세히 따져보고 WIPS를 도입해야 할 것입니다. 또한 모든 항목이 중요하지만 WIPS 본연의 기능인 탐지/차단 성능과 위치정보의 정확도가 가장 우선순위가 높다고 할 수 있습니다.
삼성 보안 AP는 내장된 WIPS 센서 모듈에 전용 안테나를 탑재하고 있습니다. 이를 통하여 Full time scanning으로 무선랜을 모니터링하고 불법 AP나 Client가 발견되면 동일한 전용 센서 및 안테나를 통해 차단을 수행합니다. 모니터링 시 채널 당 100msec간격의 고속 채널 스위칭으로 전체 채널을 탐지하는데 4초 이내의 빠른 탐지 싸이클을 지원하며, 탐지 분석을 서버에서 수행하고 서버에서 차단 명령을 내리는 방식과 다르게 내장 WIPS 센서에서 탐지/차단을 수행하여 차단 속도 및 차단율에서 탁월한 성능을 제공할 수 있습니다.



<그림4. 모니터링 용 전용 안테나>

아래 [표1.]은 실제 타사 단독형 WIPS 솔루션과 비교 시험한 자료입니다. 탐지/차단 시간은 최대 8~10배 차이가 나며, 탐지 거리 역시 2배 정도 거리 차이를 보이고 있습니다.

구분			성능 결과
성능	탐지 시간	비혼잡 환경 (쉴드룸)	10 ~ 30초 (타사 1~ 4분)
		혼잡 환경 (주변 AP 500개 이상)	30초 ~ 1분 이내 (타사 1~ 5분)
	탐지 거리	혼잡 환경	50M (타사 25M)
	차단 성능	차단 시간 (쉴드룸)	30초 ~ 1분 (타사 30초 ~ 5분)
		차단 성능 (쉴드룸)	동시 8개채널 차단시 85% 차단율 제공 (타사 75%)

<표1. WIPS 성능 비교(삼성 보안 AP vs 타사 단독형 WIPS 제품) >

삼성 보안 AP

아래의 시험 결과는 동일한 환경에서 불법 AP 10대를 탐지 및 차단하는 성능 시험 상세 결과입니다. 평균 차단율의 차이도 삼성 보안 AP는 93%의 차단율로 타사 단독형 WIPS의 53% 차단율보다 월등한 성능을 보였습니다. 더욱 중요한 부분은 삼성 보안 AP의 경우 모든 불법 AP에 대하여 88% 이상의 차단율을 보인 반면, 타사의 경우는 50% 미만의 차단율을 보였고, 12%, 24%의 차단율을 보인 AP도 있습니다. 이런 불법 AP는 거의 차단을 못했다고 판단하는 것이 맞을 것입니다. 다른 표현으로 보안에 구멍이 뚫렸다고 표현할 수 있을 것입니다.

	삼성 보안 AP		AP 차단 시
Index	Rouge AP SSID	채널	차단율
1	BMT_Rogue_15	9	89.2
2	BMT_Rogue_17	9	93.3
3	BMT_Rogue_5	13	92.7
4	BMT_Rogue_14	9	91.7
5	BMT_Rogue_16	13	88
6	BMT_Rogue_7	149	97.7
7	BMT_Rogue_18	153	98.3
8	BMT_Rogue_20	157	98.3
9	BMT_Rogue_10	161	95.1
10	BMT_Rogue_9	149	89.4
		평균	93.37

	타사 단독형 WIPS		AP 차단 시
Index	Rouge AP SSID	채널	차단율
1	BMT_Rogue_17	9	95.9
2	BMT_Rogue_5	13	64.3
3	BMT_Rogue_14	9	54.8
4	BMT_Rogue_16	13	44.4
5	BMT_Rogue_15	9	100
6	BMT_Rogue_4	149	58.7
7	BMT_Rogue_3	153	41.2
8	BMT_Rogue_13	157	37.8
9	BMT_Rogue_8	161	24
10	BMT_Rogue_12	165	12.4
		평균	53.35

글을 마치며..

이제 무선랜에서 보안은 필수 사항이고, 고객에게 아주 중요한 네트워크 인프라 중 하나입니다. 그러나 시장에서는 고객이 필요한 기능이 아닌 제한된 환경 속에서 제조사들이 만들어 낸 단독형 또는 통합형 WIPS 라는 제한된 기능의 제품을 강요받아온 것이 사실입니다. 삼성 보안 AP는 철저하게 고객의 Needs에 기반하여 보안이 기본이 되는 무선랜, 그리고 단독형/통합형의 장점만 아우르는 무선 보안 솔루션입니다.

Samsung Electronics Co., Ltd.
(Maetan dong) 129, Samsung-ro,
Yeongtong-gu, Suwon-si,
Gyeonggi-do 443-772,
Korea

www.samsungEnterprise.co.kr