WireLESS, Communicate MORE

Samsung Wireless Enterprise

Samsung Security AP

WHITE PAPER

SAMSUNG

Samsung Security AP

Introduction

Due to their high speed and standardized features such as enhanced authentication and encryption, enterprise WLAN network systems are currently growing in their use as infrastructure whereby the important tasks of enterprises are handled through various handsets. Nevertheless, it is true that there are constant issues raised by customers in regard to security threats in wireless sections and the performance and management of networks. For resolution, many customers are considering establishing a Wireless Intrusion Prevention System (WIPS)/Wireless Intrusion Detection System (WIDS). Thereby, we are going to look into the pros and cons of configuration and establishment methods for various wireless intrusion protection systems available on the market, and matters you must consider when adopting such a system. In addition, we are going to introduce the differentiated features of the Samsung Security AP from the above point of view.

First, let's look at the beginning and development of WIPS. This is believed to be a good way to understand why services are provided in different structures. Most of the WIPSs were developed when early WLANs were used as "intrusion routes to enterprise networks" for hackers. In those days, hackers usually broke into APs which were mis-configured or which they were unauthorized to access and cracked their security keys, and re-intruded those APs using those keys. Initial actions to these intrusions were simply rudimentary: enterprises scanned their wireless networks manually to locate operating APs nearby and took measures manually. This method had become insufficient as WLANs expanded and hence a solution was born that monitors WLAN networks by managing multiple sensors from the center. These early WIPSs had the same structure as the IPS that was being used widely on wired networks and were stand-alone systems that were solely for the purposes of wireless intrusion prevention. In other words, the server coordinated the monitoring process over the wireless network and received information captured by the sensors (on the basis of signature, behavior, ACL, policy, etc.) and provided the information to the administrator. Then the administrator physically eliminated the rogue AP and intruder based on the information (a report or alarm). (Afterwards, this method developed into automatic blocking and isolation.)

The era of fat Standalone APs ended with the emergence of AP controllers on WLANs. The manufacturers of AP controller based WLANs started to offer their products with a limited wireless detection feature built into the controllers, and this naturally allowed APs to be used as sensors. This method where an AP monitors a WLAN was implemented in such a way that it detects the same channel as wireless service or that monitors and detects channels that are not the service channel. Despite its limited detection/blocking, compared with earlier resolution methods, this method was effective in terms of management and investment costs.

To satisfy the ever growing security needs of customers, WLAN manufactures have gradually been enhancing the performance and functions of WLAN-integrated WIPS products by Acquiring over WIPS companies. APs are being dedicated for use as full-time sensors by changing the APs software without changing hardware. This is a change from the previous method on separate WIPS servers that came out in the market where the service AP also performed the detection.

Companies responded to the change by further enhancing the scanning and monitoring abilities of their dedicated WIPS sensors; they made it where a list of authorized devices were shared and the scanning information of wireless APs was provided from the already established wireless infrastructure. However, this is currently limited between particular vendors.

In this manner, WLAN and WIPS products have mutually developed to eventually form the WIPS products and market of today. Then, let's take a look at the differences between the two kinds of products and their pros and cons.

First, A dedicated WIPS consists of a WIPS controller and a WIPS sensor. A sensor that is separate from an AP can perform full time scans and allow full channel utilization of the AP. The correlation between an increase in the channel utilization of the AP due to its WLAN service and a decrease in the detection rate of the sensor is no longer present.

Samsung Security AP

Adaptation to headquarters-branches structure becomes easy and smooth because alarms and necessary data are only transferred to the WIPS controller. This is due to the self-execution of analysis on monitoring information through a separate dedicated WIPS.
There are limits to monitoring the traffic of the physical layer and data link layer because dedicated WIPS will not get involved in the WLAN service of the already established WLAN infrastructure. Because the utilization of information about locations, RF status, and devices authorized by WLAN infrastructure is limited, there are some limitations for integrated management and systematic linkages with the existing WLAN infrastructure.
The costs of adopting a system can be burdensome because a WIPS controller, WIPS sensor, PoE switch, etc. need to be installed separately from WLAN infrastructure.

Integrated WIPS Solution: An integrated WIPS has a structure in which an AP for WLAN service stops its WLAN service on a regular basis and performs monitoring for security. There are some cases where the AP for service is changed to an AP for sensing purposes. WLAN controllers offered WIPS-related control in early days, but later, manufacturers emerged which provided separate WIPS controllers after acquiring over WLAN companies. The biggest merit of integrated WIPS solutions with this structure is their building costs being relatively cheap compared to dedicated WIPS solutions. It is because adopting a WIPS solution at a minimum cost (only at the price of licensing or purchasing a WIPS controller) is possible by the shared use of the existing WLAN infrastructure. In addition, this type of WIPS solution has an advantage in monitoring authorized WLAN service and identifying attacks and rogue devices in WLAN service. There are limits to the ability to monitor other channels and frequency bands that are not in WLAN service.
Can problems such as the one described above be resolved by using the AP for WLANs as a dedicated AP for sensing through a mode change, which is a different form of integrated WIPS solution? In this case, other problems can occur. Today, most WLAN manufacturers' APs are implemented in the form of thin APs many of whose functions are dependent on the AP controllers. If you use this kind of a thin AP as a WIPS sensor by changing its mode to monitoring, analysis cannot be performed in the sensor itself, all the monitored data are transferred to the WIPS controller or WLAN controller for analysis and then the identification and blocking of rogue devices are performed. If the system has been built in headquarters-branches structure, it may be difficult to respond reliably due to the limitations of the bandwidth of the WAN section.

In review, this table summarizes WIPS configurations.

		Dedicated	Integrated
Architecture of WIPS	Sensor	A dedicated WIPS sensor performs monitoring full-time.	The AP for WLANs also performs monitoring on a regular basis
			The AP for WLANs performs full-time as a sensor through a mode change
	Control	Dedicated WIPS Controller	Controller Built into WLAN
			Dedicated WIPS Controller
Monitoring (Detection) Analyzing/Blocking Method		Full time scanning	Time sliced scanning High probability of channel and frequency hole occurrence
			Full time scanning
		Capable of monitoring regardless of an increase in WLAN service load	Degradation in monitoring performance as WLAN service load increases
		Capable of monitoring all channels and all frequency bands Effective in blocking Flood and DoS attacks Limits same-channel monitoring due to channel hopping type monitoring	Advantageous in monitoring the WLAN (channels, frequencies) currently in service Limited monitoring of frequencies and channels other than those in service

Samsung Security AP

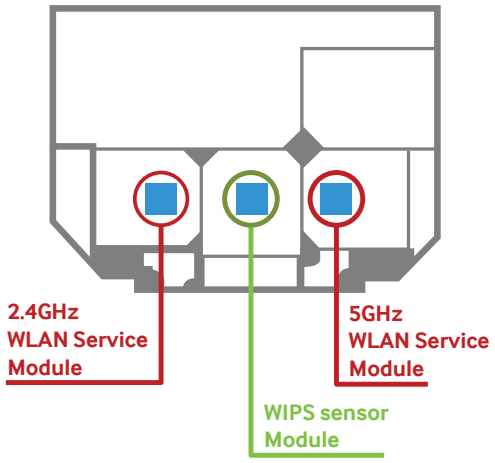
	Dedicated	Integrated
Monitoring (Detection) Analyzing/Blocking Method	Analyzing/blocking within the sensor	Usually, the sensor transfers monitored data to the controller and the controller performs blocking after analysis
Construction/Architecture	Good for both campus structure and headquarters-branches structure Configured separately from WLAN infrastructure	Difficulty in responding in headquarters-branches structure Relatively ease to manage due to the linkage of configurations between the WLAN and WIPS
Building Costs	A dedicated WIPS sensor and controller need to be purchased A switch for connections to wired networks needs to be purchased	No need to purchase a separate sensor A controller needs to be purchased depending on the manufacturer Relatively cheap compared with Dedicated WIPS

We hope that you now have a better understanding of WIPS behavior.

Then, What does Samsung offer to help deliver Wi-Fi Security to it's customers?

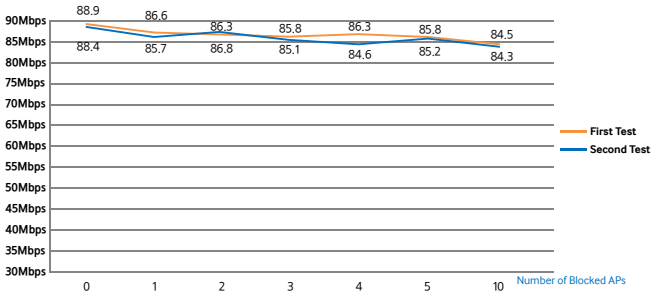
Samsung Security AP, You get 2 for 1

The Samsung Security AP is a WLAN AP with a built-in dedicated WIPS sensor. Below is an explanation in more detail.
The Samsung Security AP is not very different from the integrated WIPS described above. However, it is a wholly different story when you look inside of it. To be specific, unlike the integrated WIPS sensor whose AP for WLAN infrastructure regularly performs monitoring in between its WLAN service, the Samsung Security AP has a separate built-in WIPS sensor module that performs security monitoring, and its WLAN service module is dedicated to WLAN service. This allows it to have the merits of both the integrated WIPS and dedicated WIPS, which in turn results in perfect security performance and enables effective WLAN management.



<Figure 1. Samsung Security AP RF Structural Diagram>

As illustrated in [Figure 1], an RF module for WLAN service and an RF module for WIPS sensing are separately built into the Samsung Security AP as hardware. [Graph 1] below shows data resulted from testing the throughput of a WLAN in service while increasing the number of blocked rogue APs.

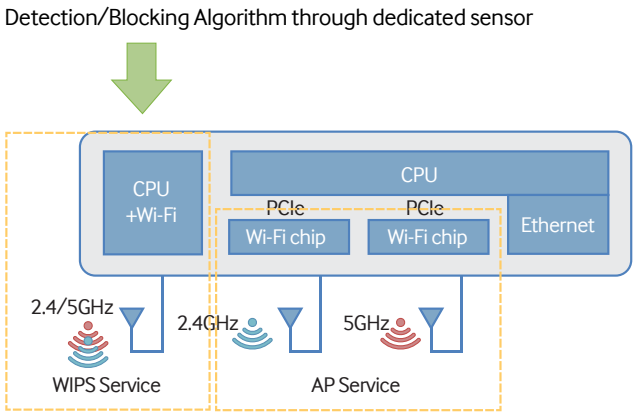


<Graph 1. Comparative Performance of WLAN as the Number of Blocked APs Increases>

In the case of an integrated WIPS sensor that regularly performs monitoring using an AP for WLANs, if WLAN service and monitoring are performed together, detection performance will be drastically degraded as channel utilization increases.

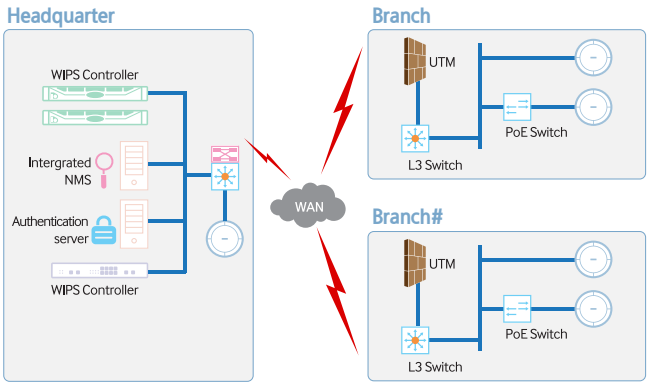
How is Samsung's Security AP different?

Samsung Security AP



<Figure 2. Detection/Blocking Algorithm Support within WIPS Module>

As illustrated in [Figure 2], the WIPS module of the Samsung Security AP contains a separate Wi-Fi chip and CPU. By utilizing these, it analyzes data collected from the security AP within the security AP itself and directly performs detection/blocking. This method provides performance and flexibility differentiated from the WIPS sensors that merely changes the mode of their AP for WLANs to sensing mode for monitoring. On top of quick detection and blocking, minimum numbers of both alarms and management frames are transferred to the WIPS controller. No load the then imposed on the existing wired network and it is not necessary to establish a WIPS controller in every region when establishing a WLAN with headquarters-branches structure.



<Figure 3. WLAN with Headquarters-Branches Structure/Wireless Security Architecture>

The architecture above is a typical architecture of an enterprise network with headquarters-branches structure. Usually, the bandwidth of the WAN section is far lower than the LAN section. Keeping a high bandwidth is definitely a cause of waste according to the costs of the dedicated line, the frequency and the purpose of use. If a WIPS sensor in a branch transfers monitored data to the WIPS controller in the headquarters in such a structure, not only a bottleneck occurs, but also smooth communications in the traffic you actually want to use become impossible. Samsung's security AP provides a flexible network architecture, which is made possible by a dedicated monitoring module that analyzes monitoring data to directly perform detection and blocking, and transfers a minimum amount of data to the WIPS controller.

Things to Consider When Adopting WIPS

So far, we have looked at the pros and cons of integrated WIPS and dedicated WIPS which constitute the mainstream of the market period. We also discussed why Samsung has a WIPS sensor built into its security AP and the merits it provides to its customers.

Putting aside the architecture of WIPS, the things to consider when adopting a WIPS are :

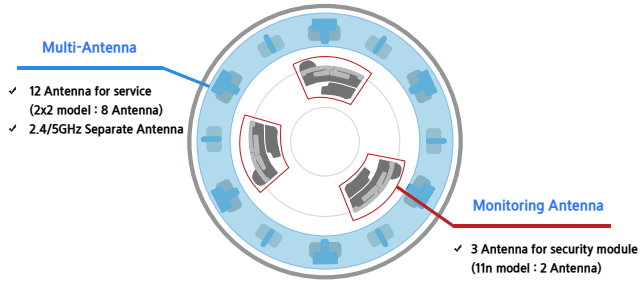
1. RF monitoring: must be capable of monitoring all 802.11-based channels. It is because attacks are possible through channels not used in the country and non-Wi-Fi interferences. In addition, how many of WIPS sensors are needed in a region and how much bandwidth the WIPS consumes must be taken into consideration.
2. Detection/blocking: when detecting threats to security whether there are any limitations needs to be checked. Detection must be able to be performed without being obstructed by the enterprise network's architecture including NAT, VLAN, and encryption. There are many methods for blocking; blocking the wireless connection, blocking the wired switch, ACL interoperating with the existing infrastructure, etc. These methods must be interoperated seamlessly and there must be no unwanted side effect. In addition, the most important thing is the blocking rate. Even if blocking has been performed in actuality, blocking may not occur due to RF strength or the lock of hardware resource.
3. Location information: displays the locations of the AP and client on the map. Accuracy is important in location information. In general, accuracy is proportional to the number of APs or sensors, which has something to do with adoption costs. The way to accurately locate rogue APs and clients must be figured out.

Samsung Security AP

4. Compliance report: must be capable of creating regular/non-regular reports automatically or on-demand. In addition, the feature that exports compliance reports in accordance with security regulations in a particular industry helps to reduce the task load of the administrator.
5. Certification: whether security-related certifications are prepared (e.g. CC EAL2, FIPS, etc.)
6. High availability and scalability: whether the WIPS sensor functions in the event of a WIPS controller failure and the amount of stored monitored data and the maximum volume of reports that can be created over the duration of the failure must be checked lest business affairs be affected.

Before adopting a WIPS solution consider the 6 items above. All items are important. However, it would be correct to say that the performance of detection and blocking, which are integral functions of a WIPS, and the accuracy of location information have the highest priority.

The Samsung Security AP is equipped with a built-in WIPS sensor module and a dedicated antenna. With these, it scans WLANS full-time for monitoring purposes and also, when a rogue AP or client has been found, performs blocking. During monitoring, detection is performed on all channels through high speed switching at 100msec intervals per channel. A speedy detection cycle of less than 4 seconds is supported and unlike the method where the server performs detection analysis and also issues blocking commands, a built-in WIPS sensor performs detection/blocking so that excellent performance is provided in terms of blocking speed and blocking rates.



<Figure 4. Antenna Dedicated for Monitoring>

[Table 1.] Below shows the results of comparative testing between the Samsung Security AP and dedicated WIPS solution of our competition. There is a maximum of an 8–10 fold difference in detection/blocking times and the difference in detection distance is about two fold.

Item			Performance Results
Performance	Detection Time	Non-Congested Environment (Shielded Room)	10–30 secs (products of other companies: 1–4 mins)
		Congested Environment (more than 500 APs)	From 30 secs–1 min (products of other companies: 1–5 mins)
	Detection Distance	Congested Environment	50m (products of other companies: 25m)
	Blocking Performance	Blocking Time (Shielded Room)	30 secs–1 min (products of other companies: 30 secs–5 mins)
		Blocking Performance (Shielded Room)	A blocking rate of 85% when blocking 8 channels simultaneously (products of other companies: 75%)

<Table 1. WIPS Performance Comparison
(Samsung Security AP vs. Dedicated WIPS Products of other companies)>

Below are the detailed results of performance testing where the abilities to detect and block 10 rogue APs are tested in the same environment. Speaking of the difference in the average blocking rate, the Samsung Security AP showed superior performance at a blocking rate of 93%, compared with the 53% blocking rate of the dedicated WIPS of our competition. What is more important is that the Samsung Security AP showed a blocking rate of more than 88% for all rogue APs while the competition's product showed a blocking rate of less than 50% and for certain APs, blocking rates dropped to even 12% and 24%. It would be correct to assume that most of these rogue APs have not been blocked successfully. This is a major security issue.

Samsung Security AP

	Samsung Security AP		When Blocking APs
Index	Rouge AP SSID	Channel	Blocking Rate
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
		Average	93.37

	Dedicated WIPS of Other Companies		When Blocking APs
Index	Rouge AP SSID	Channel	Blocking Rate
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
		Average	53.35

Closing...

Security is a necessity for WLANs and it is one of the most important network infrastructures to customers. It is true that in the market, customers have been forced to use WIPS products with limited features, dedicated or integrated, manufactured in limited environments by manufacturers without consideration for the features that customers really need.

The Samsung Security AP is a wireless security solution, which has embraced the function of a WLAN which serves as a basis for security as well as the dedicated and integrated WIPS thoroughly based on the needs of the customers.

Samsung Security AP

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

www.samsungEnterprise.co.kr