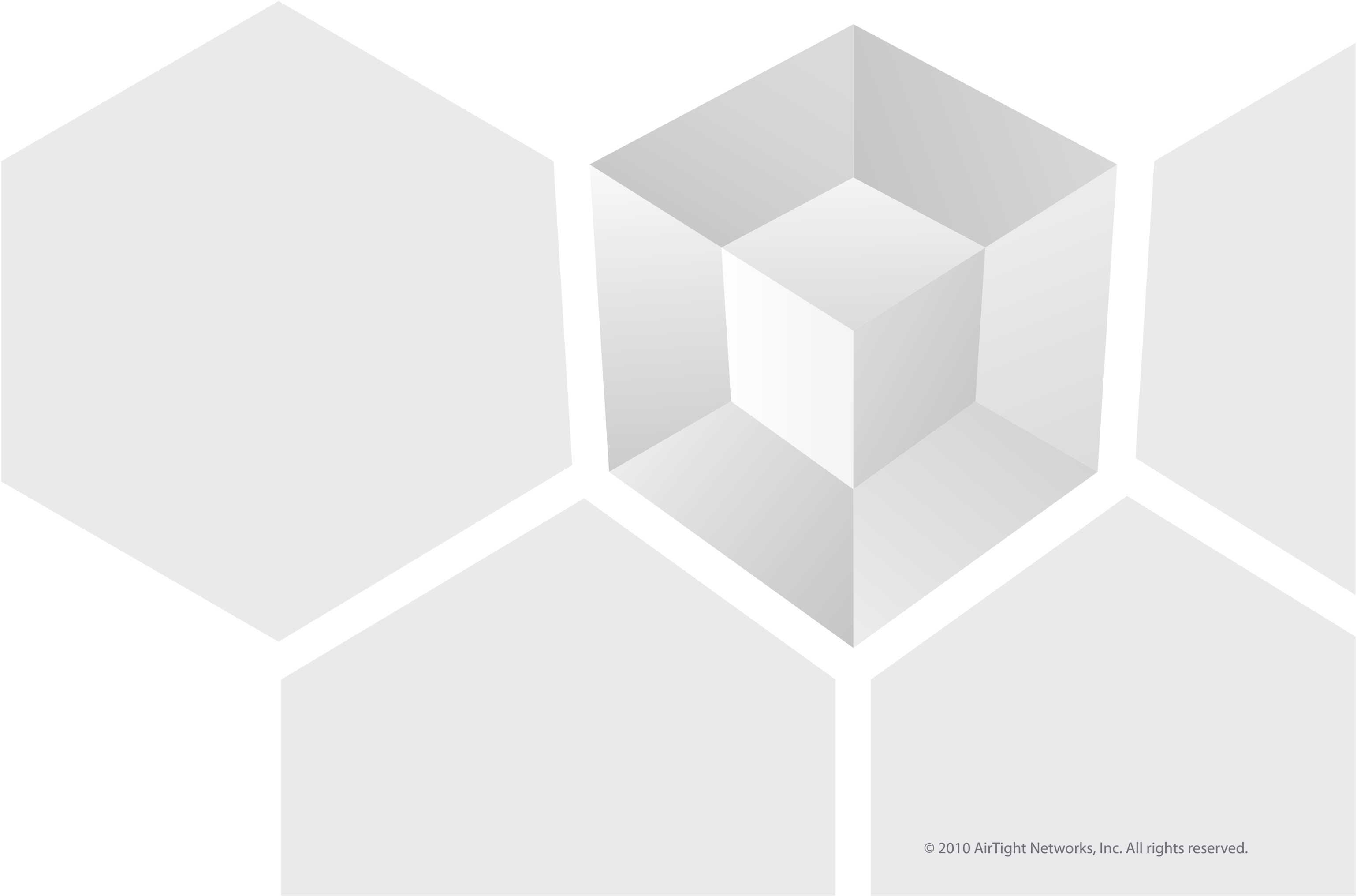
Windows 7 Virtual Wi-Fi:
The Easiest Way to Install a Rogue AP on Your Corporate Network

A Whitepaper by AirTight Networks, Inc.

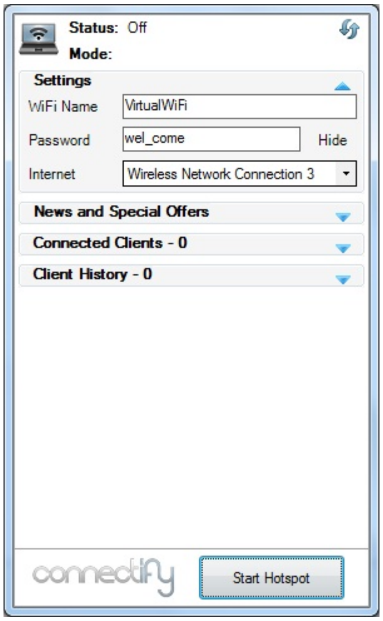
339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com



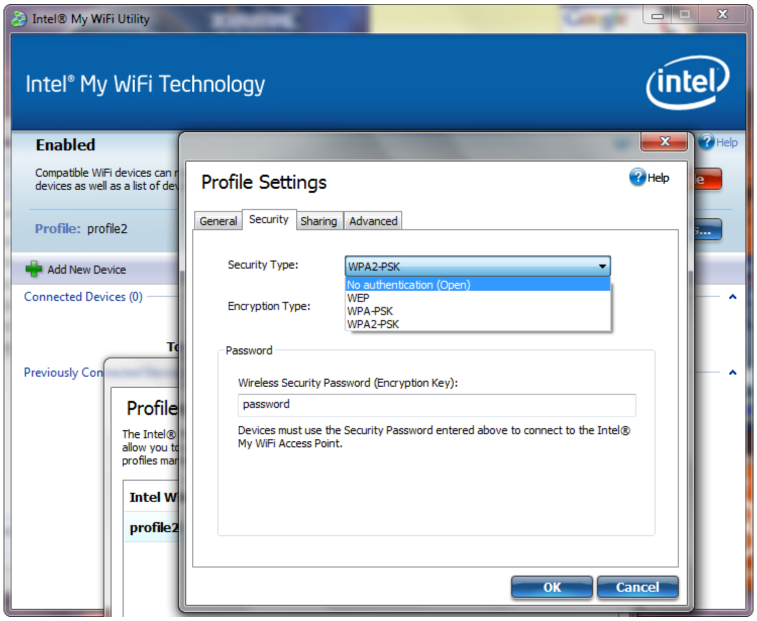
Introduction

Last few years have seen a sweeping commoditization of IT, more so in the mobile wireless space, with hardware and software vendors innovating to make their devices and applications easy and convenient for end-users.

Virtual WiFi, one of the many cool features in Windows 7, is a great example of this shift. With Virtual Wi-Fi, users can now turn their Windows 7 laptops into a Wi-Fi access point (AP). Free utilities such as *Connectify* and Intel *MyWiFi* make it very easy to set up a personal Virtual Wi-Fi hotspot in less than a minute in two simple steps.



Status: Off
Mode:
Settings
WiFi Name: VirtualWiFi
Password: wel_come
Internet: Wireless Network Connection 3
News and Special Offers
Connected Clients - 0
Client History - 0



Intel® My WiFi Utility
Intel® My WiFi Technology
Enabled
Compatible WiFi devices can r
devices as well as a list of dev
Profile: profile2
Connected Devices (0)
Previously Con
Profile Settings
Security Type: WPA2-PSK
No authentication (Open)
WEP
WPA-PSK
WPA2-PSK
Encryption Type:
Password
Wireless Security Password (Encryption Key): password
Devices must use the Security Password entered above to connect to the Intel® My WiFi Access Point.

This is not the first time that a laptop can be converted into a "Soft AP." But it is the first time that a laptop can be used both as a Client and as a Soft AP simultaneously. In other words, while staying connected to an AP, a Windows 7 laptop can now share that connection, using Virtual Wi-Fi, with other Wi-Fi devices and users. Using this personal Wi-Fi hotspot, users can now easily synch up music files on their laptop with a Zune or iPod, transfer photos from their iPhone onto their laptop, and share their Wi-Fi Internet connection.

What does this mean for enterprise security?

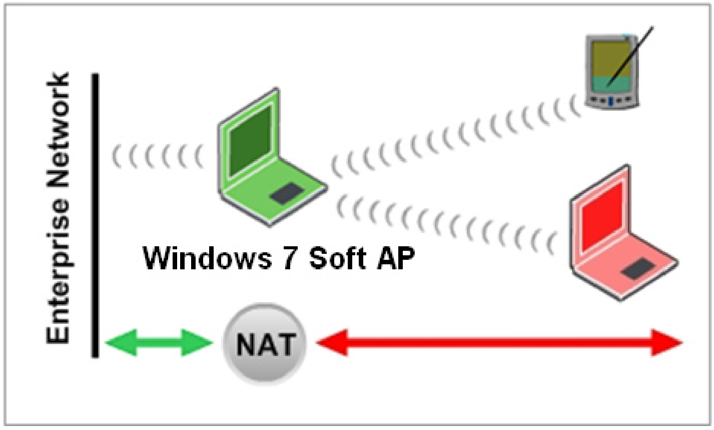
Using Virtual WiFi, Windows 7 laptops can now be connected to your enterprise

Wi-Fi network while sharing their enterprise network access with other unauthorized Wi-Fi devices or users.

This means that every Windows 7 laptop is a potential Rogue AP[1] that can be used to bypass your wired security and access your private enterprise LAN. Using a Rogue AP, an attacker could compromise your servers, access sensitive data, and launch network reconnaissance and disruption attacks[2] .

As Windows 7 becomes the de-facto standard for PC users in the near future, a typical enterprise security administrator may have to deal with tens if not hundreds of Rogue APs every day! Yet without the right security tools, a security administrator will have no visibility and control over how many of these Rogue APs are present on the corporate network and how many unauthorized devices or users are connecting to them.

Interestingly, not much has been written about this issue yet. Robert Graham of Errata caught it right away and discussed it back in November of 2009 noting that users could previously set up Ad-hoc Wi-Fi and connection sharing, but that the Windows Virtual Wi-Fi capability will cause "rogue access points to proliferate in companies."



A Virtual Wi-Fi Soft AP operates similar to a Network Address Translation (NAT) Wi-Fi router. All Wi-Fi devices that are part of the Virtual Wi-Fi hosted network are assigned private IP addresses. All traffic from these devices bound to the enterprise network or the Internet is tunneled using the IP and MAC addresses of the Virtual

[1] All You Want to Know About Rogue APs
http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf

[2] Rogue AP: 5 Ways to (Mis)Use It
http://blog.airtightnetworks.com/wifi-rogue-ap-5-ways-to-%e2%80%9cuse%e2%80%9d-it/

Wi-Fi Soft AP. This means that all traffic entering the wire is seen as coming from the authorized Windows 7 laptop. Naturally, all wired security measures such as network access control (NAC), 802.1x, firewall, wired IDS/IPS, and content filters are rendered useless.

What can security administrators do about it?

Windows user group policy

Turning ON Virtual Wi-Fi on a Windows 7 laptop requires local administrative privileges. By defining user group policies in Active Directory, you can shutdown this privilege for your users. However, the ability to do this is currently supported only in Windows 2008 server R2. Further, this approach lacks flexibility. You may want to disallow Virtual Wi-Fi when a Windows 7 laptop is connected to your enterprise network (via Wi-Fi or Ethernet), but allow users to take advantage of the convenience when they are travelling or at home. This is not possible using Windows user group policy.

Wireless endpoint security agent

A wireless endpoint security agent such as AirTight's SpectraGuard SAFE can enable flexibility in enforcing your security policies on client devices. SAFE allows you to define granular laptop security policies, for instance, disallow use of Wi-Fi when laptop is connected to the wired enterprise network, or disallow Virtual Wi-Fi at work and allow when laptop is away, or allow WiFi hotspot connections only using VPN, and so on. It also saves you the trouble of configuring individual laptops. You can simply push your policies to all enterprise laptops from a central server.

Wireless intrusion prevention system (WIPS)

A WIPS can proactively protect your enterprise network from wireless threats by scanning the airspace 24x7. However, when it comes to Rogue AP detection, most WIPS solutions including those integrated into your WLAN infrastructure, rely on wire-side scanning. It cannot be stressed enough that wire-side scanning alone is incapable[3] of detecting Virtual WiFi Rogue APs because of the NAT operation and given that this new type of Rogue APs can connect to your enterprise network via Wi-Fi.

The ability to correlate traffic in the air with that on the wire is the key for accurately

[3] **Wireside-only rogue detection: Inadequate for both security and compliance**
http://blog.airtightnetworks.com/rogue-ap-detection-pci-compliance/

and automatically detecting the presence of a Virtual Wi-Fi Soft AP on your enterprise network. SpectraGuard Enterprise, powered with AirTight's patented Marker Packet technology, is the only WIPS that has visibility on both the wired and wireless sides. Unsurprisingly then, SpectraGuard Enterprise is able to instantly detect a Soft AP, pinpoint its physical location, and automatically block it over the air.

Summary

- Windows 7 Virtual Wi-Fi enables a laptop to operate as a client and as an AP simultaneously, making it very easy to deploy Rogue APs on enterprise networks
- This is the first time that a Rogue AP can connect to your enterprise network using Wi-Fi
- Wire-side security measures such as 802.1X, NAC, wired IDS/IPS and firewall cannot protect you against this and other wireless threats
- WIPS solutions that rely on wire-side scanning alone are equally ineffective in detecting Virtual Wi-Fi Rogue APs
- A WIPS that correlates wired and wireless traffic can automatically detect the presence of Virtual Wi-Fi Rogue APs

About AirTight Networks

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WVM) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 12 U.S. patents and two international patents granted (UK and Australia), and more than 20 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com

The Global Leader in Wireless Security Solutions

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 **www.airtightnetworks.com info@airtightnetworks.com**

AirTight® NETWORKS