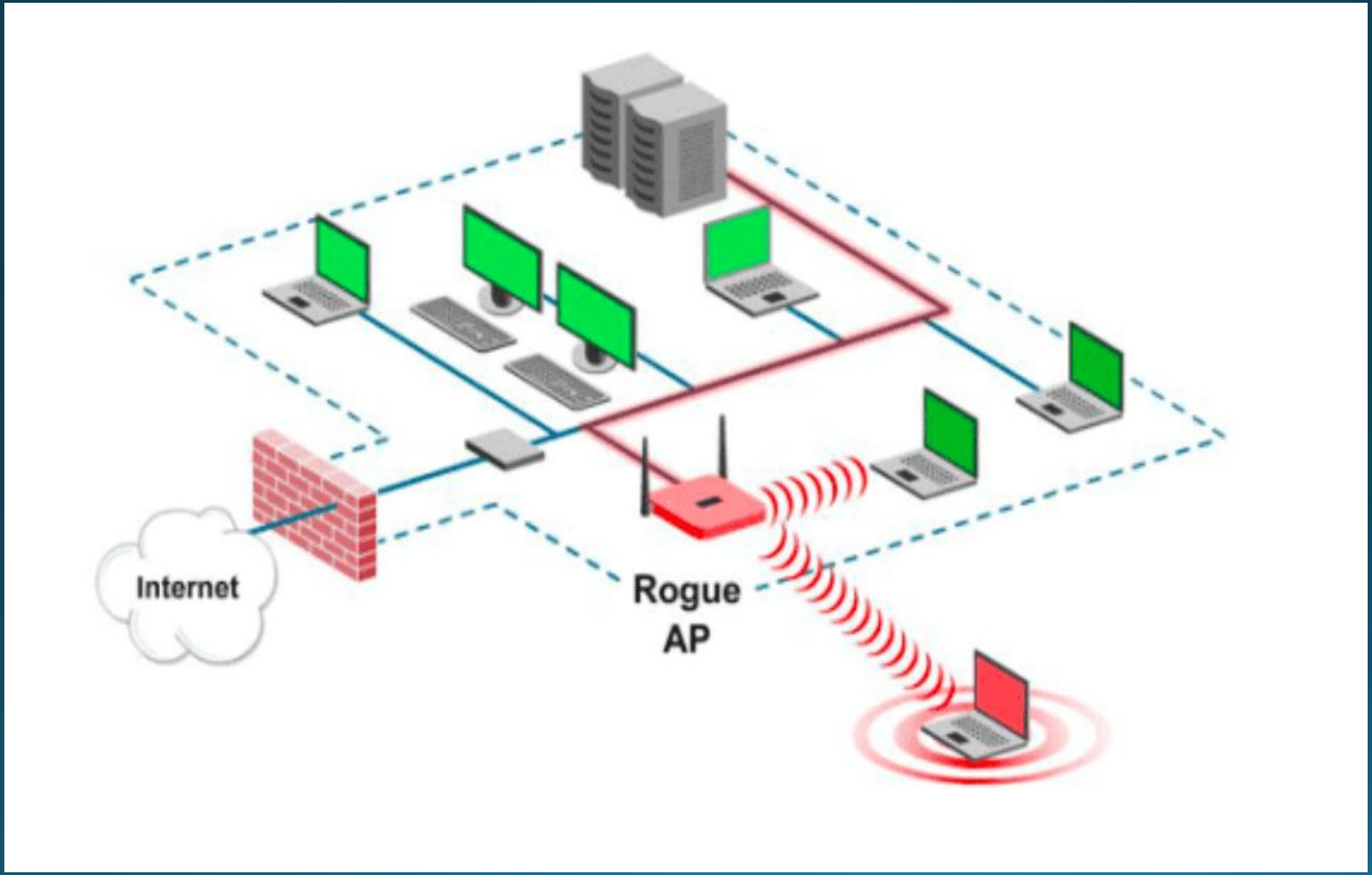
BLOCK - 4

Access Points and the Future of Wireless Security

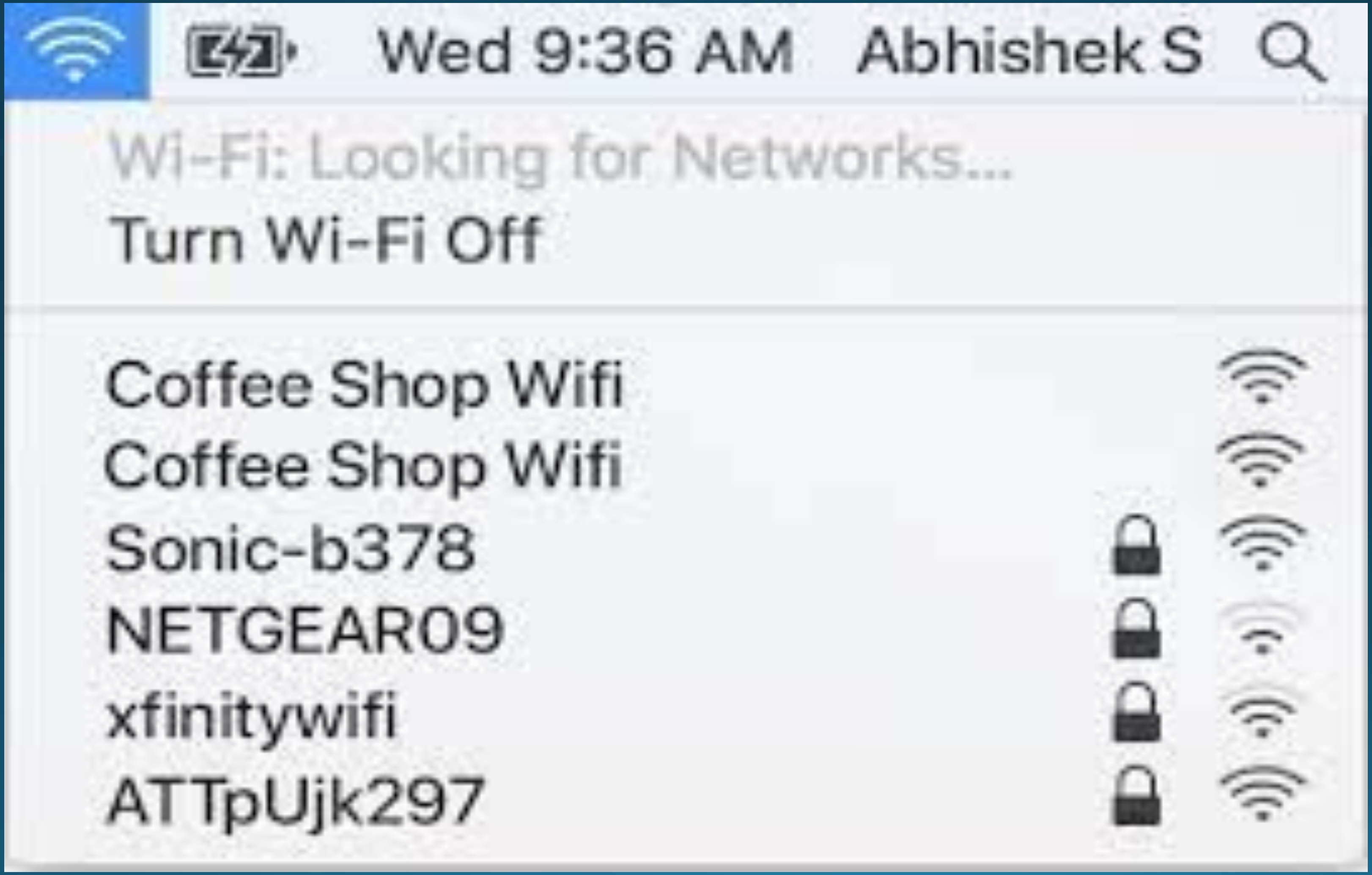
What is a rogue access point?

- A rogue access point is a wireless access point installed on a secure network without the knowledge of the system administrator.
- An unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router.
- A rogue access point could be a small wireless access point plugged into an existing firewall or switch, or into an unused wall network connector (like at a personal desk), etc.
- It could be a mobile device attached to a USB that creates a wireless access point, or even a wireless card plugged into a server.

Rogue Access Point



Rogue Access Point



- Because they are installed behind an organization’s firewall, rogue access points can be lethal to security.

<u>Here are three main dangers of a rogue access point:</u>

- Someone authenticated to it is allowed access into the network (could be good guys or bad guys).
- It’s not being monitored or managed by the system administrator.
- It doesn’t follow normal security procedures of other wireless access points on the same network.

Handling Rogue Access Points

- Rogue access points have become a sort of hot-button issue.
- Rogue access points are any wireless access points that exist on your network without the consent of the business.
- Even secure rogue access points that are connected to your network can pose a security risk.
- Preventing rogue access points can be a little tricky, although not impossible.
- Not only is it critical for you to find and remove rogue access points from your network, but it can actually be pretty fun!
- Remember that regardless of the intent, a rogue access point does pose serious security risks.

Detection of Rogue Wireless Networks

- Besides relying on the manual approach, you can also use certain technologies to assist in finding rogue wireless networks.
- Some of these technologies will simply aid you, whereas some of the more sophisticated technologies will almost handle the entire job for you.
- Many solutions use your existing wireless infrastructure to scan the wireless frequencies and alert you to any rogue access points.

Detection of Rogue Wireless Networks

- Lightweight access point solutions typically have this functionality built right into the access points and controllers.
- Many of these systems offer really interesting functionality beyond simple alerting.
- For example, they might allow you to estimate an approximate position of the rogue access point based on the signal strength from multiple access points.

Preventing Rogue Wireless Networks

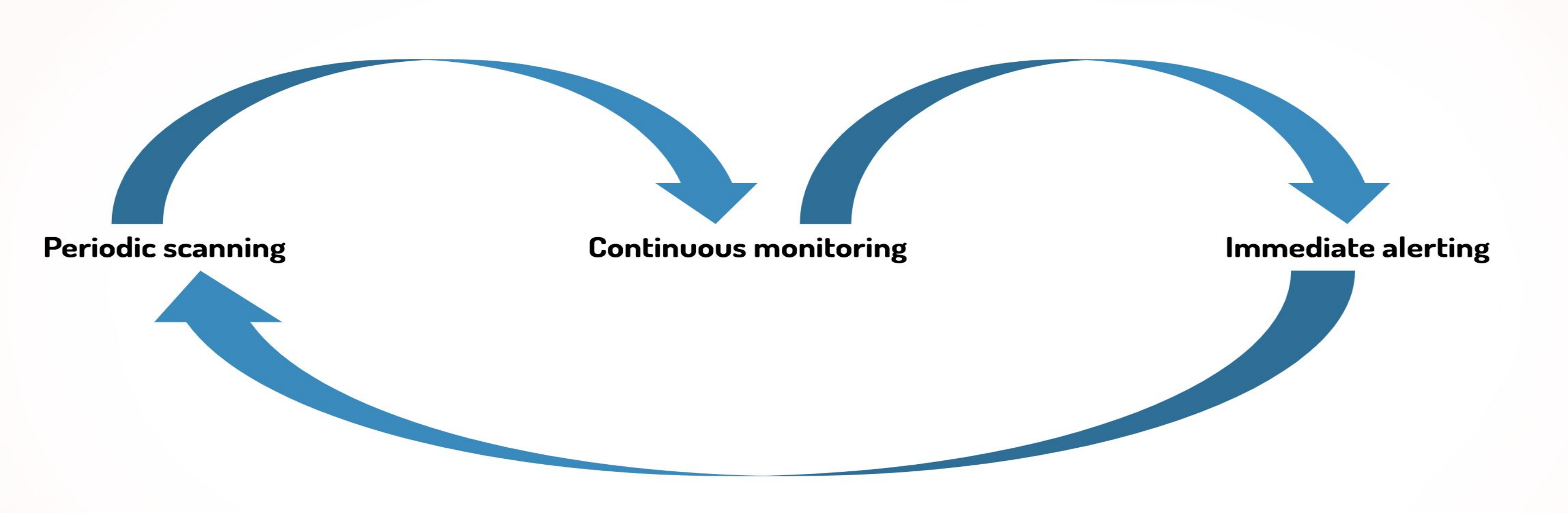
- Wireless networks are inherently less secure than wired networks. With traditional (non-wireless) networks, data flows over physical and continuously-monitored circuits.
- On the other hand, in wireless networks, data is transmitted using radio signals. Because your IP network is designed to provide distributed access, it's porous and intended to be accessible by many types of devices.
- Therefore the objective of IT administrators should be to limit access to only authorized devices.
- Controlling which devices can connect to your network is crucial for ensuring the privacy and integrity of corporate assets and data.

Rogue Network Device Detection

1. **Periodic scanning:**
   - One popular method of rogue device prevention from having unrestricted access to your network is to scan your office for wireless devices on a daily, weekly, or monthly basis.
2. **Continuous monitoring:**
   - If you periodically scan your office, you will probably find many wireless devices that belong to your company, your neighbors, and your guests.
   - Every time a scan is done, new sets of devices will be found. Continuously monitoring your network allows you to maintain a list of known devices so that you can tell when a new one shows up.

3.Immediate alerting:

- If a new device is discovered in your network or the status of a device changes suddenly, an IT engineer needs to be informed immediately.
- This is why you need a comprehensive alerting system in your network, especially if it contains a large number of devices.



Next-Gen Solutions

Lightweight Access Points

- The term ‘lightweight’ refers to the fact that these devices cannot work independently.
- They rely on an external wireless LAN controller (WLC).
- Through this independent controller, many lightweight access points can be configured to work on the same network.
- This design is intended to make it easier to expand a wireless network. The dependent lightweight controllers pull their configuration from the WLC.

- That means that they essentially operate as plug and play expansions to the network. A new lightweight device can be powered on.
- It will search for the WLC and download configurations from it.
- This includes protocols, security and everything else tied to the configuration.

Cloud-managed Access Points

- A cloud-managed access point or networking solution allows business owners to manage Wi-Fi and network infrastructure over the cloud.
- This means businesses can connect to the cloud by subscribing to a pay-as-you-go, on-demand model.
- While the biggest benefit of cloud-based wireless access points for business is high-end connectivity, it also brings down the cost of managing the network infrastructure and a hiring dedicated team for network management.
- Earlier, it became hard for small and medium businesses to manage their networking requirements and wireless networks.
- With a cloud-based wireless access point installed in the office, business owners can take advantage of industry-leading technology at a fraction of a cost.

Here are some of the benefits of installing a cloud-managed access point:

1. Simplified Network Management

- Cloud-managed **wireless and networking solutions** offer a single point of management for installation, configuration, network management and diagnosis.
- With a central interface and one-click self-servicing, cloud networking solutions simplifies the task of handling the dynamic networking needs of the business.
- Also, in case of any issue, it is easier to diagnose and troubleshoot the issue quickly with minimal help and support.
- Most of the issues can be resolved by a central wireless access point management dashboard. Not only this gives a business greater control over its networks but brings down network management cost.

2. Cost Efficiency

- Cloud-managed access point work on a subscription-based, on-demand model.
- This gives businesses greater control over expenses and reduces capital expenditure.
- With a cloud-based solution, businesses are not required to invest in purchasing hardware and deploying on-premise solutions.

3. On-demand Scalability

- It is so much easier to increase your networking capabilities when you have cloud-managed access points installed in your office.
- One of the biggest benefits of cloud architecture is the scalability it offers its users.
- Entrepreneurs can grow their networks as their business grows without capital expenditure on additional hardware

4. Enhanced Security

- Cloud-based **wireless access points** are equipped with sophisticated security frameworks to ensure minimal business vulnerability.
- Instead of spending additionally on creating a security framework for a business network, a company can just use cloud-managed solution for its security advantages and benefits.

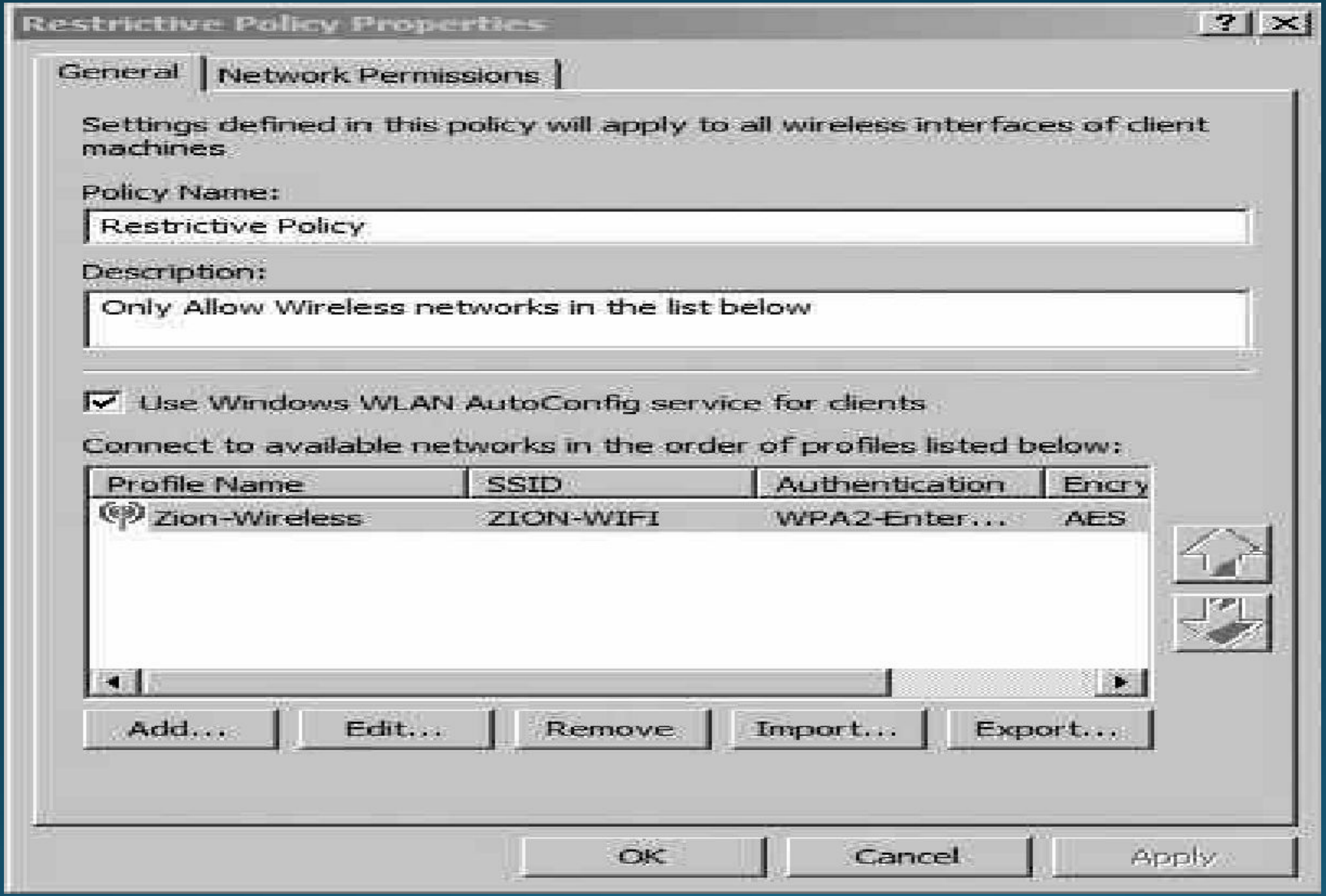
5. Deeper Analytics & Reporting

- Cloud solutions are equipped with far greater capabilities than a standard wireless access point.
- With the help of a cloud solution, any business can monitor its network round-the-clock, get real-time updates on security incidents, gather analytics about network usage and access insightful reports that can assist in decision making.

Client Protection

- **User Education**
- One of the most important things you can do to increase the security of your endpoints is to properly train the people responsible for them! Many companies offer automated
- Training (typically via videos accessible over the Internet) or classroom-based training.
- However, after reading this book, you now have all the information you need to craft a
- Great security-awareness training program.

- **Group Policy Objects**
- You can use the Windows wireless settings within Group Policy to restrict what users are able to connect to.
- Create a new Group Policy Object and expand Computer Configuration
- | Policies | Security Settings | Wireless Network (IEEE 802.11) Policies.
- Then right-click in the right screen and choose Create a New Wireless Network Policy for Windows Vista and Later Releases.
- The first window you'll see is similar to Figure 11-10. In this window, add any of the wireless networks you want this client to be able to connect to.



Settings defined in this policy will apply to all wireless interfaces of client machines

Policy Name: Restrictive Policy

Description: Only Allow Wireless networks in the list below

☑ Use Windows WLAN AutoConfig service for clients

Connect to available networks in the order of profiles listed below:

Profile Name	SSID	Authentication	Encry
Zion-Wireless	ZION-WIFI	WPA2-Enter...	AES