Trusted Wireless Environment Test Guide

This guide describes how to test your wireless network security for the six known threats defined by the Trusted Wireless Environment framework.

What is a Trusted Wireless Environment?

A Trusted Wireless Environment is a framework used to build a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure.

A Trusted Wireless Environment is based on these three core concepts:

- **Market-Leading Performance:** You should never be forced to compromise security to achieve adequate performance to support your environment with the speed, connections and density that it requires.
- **Scalable Management:** With easy set-up and management, you should be able control your entire wireless network, big or small, from a single interface and execute key processes to safeguard the environment and its users.
- **Verified Comprehensive Security:** You should be able to prove that your security solution defends your business against Wi-Fi attacks and can deliver on these benefits:
    - Provide automatic protection from the six known Wi-Fi threat categories:
        - Rogue access point
        - Rogue client
        - Neighbor access point
        - Ad-hoc connection
        - Evil Twin access point
        - Misconfigured access point
    - Allow legitimate external access points to operate in the same airspace
    - Prevent user connections to unauthorized Wi-Fi access points

For more information, see the Trusted Wireless Environment web site.

What is a Wireless Intrusion Prevention System?

A Wireless Intrusion Prevention System (WIPS) monitors your wireless airspace to detect unauthorized access points, wireless clients, and other Wi-Fi enabled devices connected to or operating in the vicinity of your network.

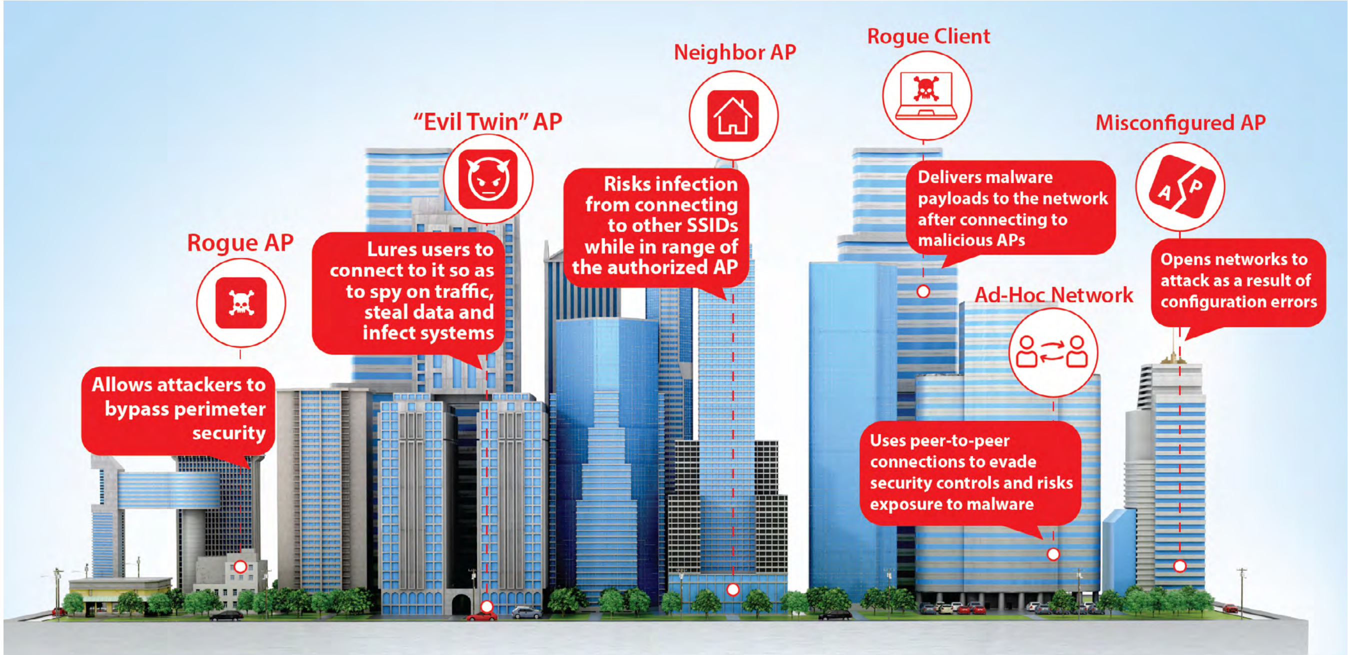
A complete WIPS solution must provide effective and reliable client and AP detection, classification, and prevention.

- **Detection** – The ability to discover all devices (including APs, wireless clients, smartphones, tablets, laptops, and any connected devices such as multi-function printers) in your airspace.
- **Classification** – The ability to quickly and accurately classify each AP and client as authorized, external (neighbor), or harmful (rogue).
- **Prevention** – The ability to immediately block and quarantine any rogue AP or client from your airspace to prevent malicious activity before it occurs.

How to Test your Wireless Network for the Six Known Threats

You can test your own wireless network security measures to see if they are able to detect and prevent these six known threats.

For more information and videos describing these threats, see:
https://www.trustedwirelessenvironment.com/wi-fi-hacks/


Rogue AP
Allows attackers to bypass perimeter security
"Evil Twin" AP
Lures users to connect to it so as to spy on traffic, steal data and infect systems
Neighbor AP
Risks infection from connecting to other SSIDs while in range of the authorized AP
Rogue Client
Delivers malware payloads to the network after connecting to malicious APs
Ad-Hoc Network
Uses peer-to-peer connections to evade security controls and risks exposure to malware
Misconfigured AP
A P
Opens networks to attack as a result of configuration errors

Recommended WIPS Testing Tools

To test your WIPS deployment against the six known wireless threats, we recommend you have these devices and tools available:

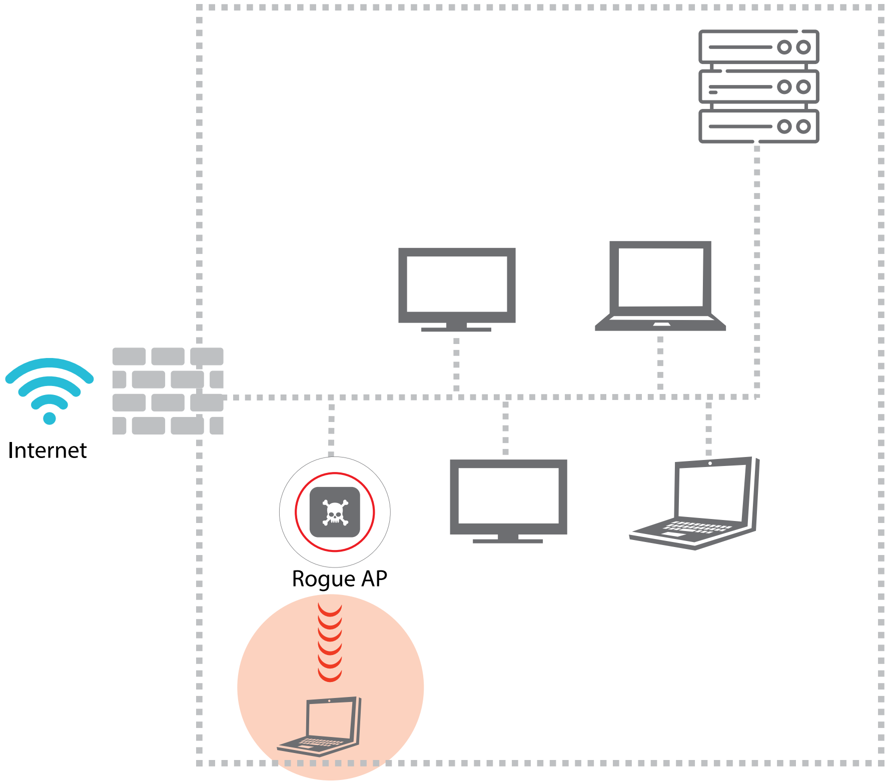
- **Access Point (AP) or Mobile Hotspot** – You can use a dedicated access point hardware device, or with your mobile phone or laptop, you can create a mobile hotspot to use as an internal authorized AP (known and trusted by your Wi-Fi security system), or an external neighbor or rogue access point. For instructions on how to configure your access point or create a mobile hotspot on your device, see your device manual.
- **WiFi Pineapple** – The WiFi Pineapple is a leading Wi-Fi penetration test toolkit that enables you to emulate the behavior of a malicious access point, and execute attacks and vulnerability tests on your Wi-Fi network.
- **Wireless Clients** – You can use any Wi-Fi capable device as a wireless client, such as a laptop, mobile phone, smart device, or tablet. In these tests, you will use wireless clients as an authorized Wi-Fi client

(known and trusted by your Wi-Fi security system), or as external neighbor or rogue Wi-Fi clients. You can also use most Wi-Fi clients to create ad-hoc networks.

- **Wi-Fi Network Monitoring Tools** – You can use the monitoring tools provided by your deployed wireless network controller to view the APs, broadcast SSIDs, clients, and network traffic for these tests. In addition, we recommend you use additional advanced monitoring tools such as NetSpot or inSSIDer to provide detailed information about your network.

Rogue Access Point

Rogue APs are a dangerous Wi-Fi security threat where a malicious user connects an unauthorized AP to a private wired network and broadcasts hidden wireless SSIDs so that attackers within range can gain access to internal network resources over-the-air. Common targets include PCI compliance risks such as usernames and passwords, credit card data, building-automation controls for alarms, door locks, and video cameras.



Requirements:

- A device that will operate as the Rogue AP. The device must be physically connected to your network with an Ethernet cable.
  - You can use any AP as the Rogue AP, but we recommend that the Rogue APs contain
    - Ethernet (wired) MAC address ranges that vary significantly from their radio (wireless) MAC address ranges. Recommended Rogue APs include easily available consumer-grade routers such as:
      - Apple Airport Express
      - TP-Link N300, C50, TL-WR841N, and similar TP-Link models
- A wireless client
  - The client will connect to the rogue SSID broadcast by the Rogue AP.
- A host connected to your wired network that can accept a ping request.

Test Steps:

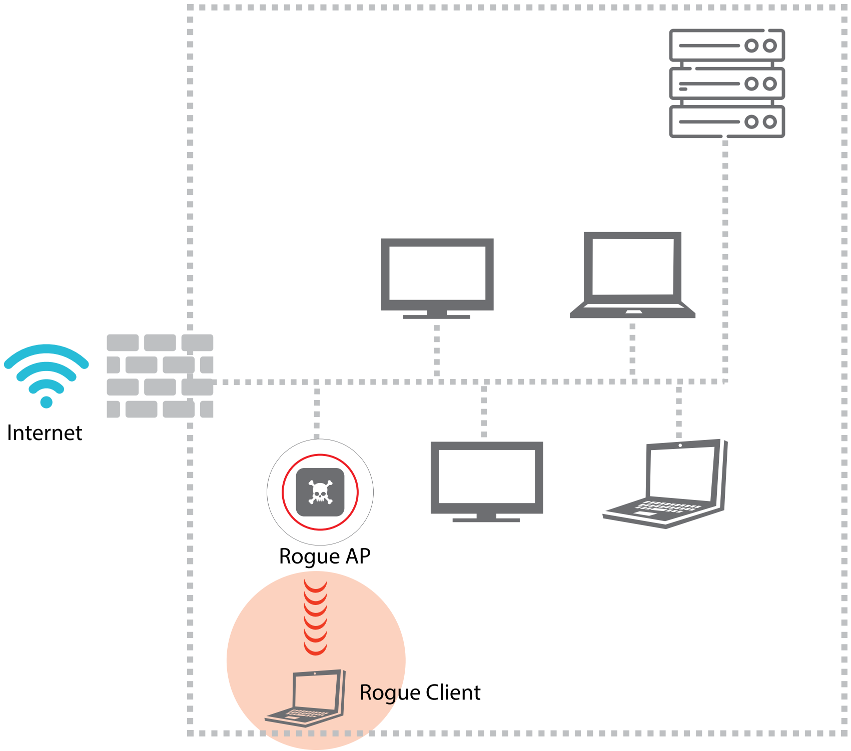
1. Check your Wi-Fi security system configuration and enable Rogue AP detection and prevention measures.
2. On the device that will operate as the Rogue AP, configure an SSID on the 2.4 and 5 GHz radios with WPA2/PSK security.
3. Use a Wi-Fi monitoring application such as NetSpot or inSSIDer to see when the SSID is broadcasting from the Rogue AP.
4. Start a timer so that you can see how long it takes for your Wi-Fi security system to detect the presence of your Rogue AP.
5. Connect your Rogue AP to your wired network.
6. Periodically refresh the management user interface of your Wi-Fi security system and note the approximate time it takes for the system to detect the Rogue AP connected to your wired network.
7. Start a timer so that you can see how long it takes for your Wi-Fi security system to prevent and block client associations to the Rogue AP.
8. Connect and associate your wireless client to the Rogue AP's SSID.
9. From the wireless client, continually ping a host on your local wired network.
10. Note the approximate time it takes for the ping activity from the wireless client on the Rogue AP's SSID to stop. This indicates when your Wi-Fi security features have prevented and blocked client associations to the Rogue AP.

Rogue AP Test Pass/Fail Summary:

- **Detection:** If the Rogue AP is detected in step 4, regardless of detection time, the Wi-Fi security system has passed the test.
- **Prevention:** If the ping activity from the wireless client associated to the Rogue AP in step 10 stops, the Wi-Fi security system has passed the test.

Rogue Client

A Rogue Client is any client previously connected to a Rogue AP or other malicious AP within range of your private Wi-Fi network. This client may have been the victim of a man-in-the-middle attack that installed ransomware, malware, or backdoors on the client while they were connected to the malicious AP.



Requirements:

- Rogue AP
  - An AP connected to your wired network that will operate as the Rogue AP.
  - This AP must be previously unknown and untrusted by your Wi-Fi security system.
  - Before you start your tests, make sure this AP is correctly detected and classified by your Wi-Fi security system as a Rogue AP after you connect the AP to your wired network.
- Authorized AP
  - An AP connected to your wired network that is known and trusted by your Wi-Fi security system as a legitimate AP.
- Wireless Client
  - This client will be tested as the Rogue Client.
  - Make sure this client is considered untrusted or uncategorized by your Wi-Fi security system.
- A host connected to your wired network that can accept a ping request.

Test Steps:

1. Temporarily disable the prevention (containment) measures of your Wi-Fi security system.
2. Connect the AP that will operate as the Rogue AP to your wired network.
3. Create and broadcast an SSID on the Rogue AP.
   - Make sure your Wi-Fi security system has already detected the AP and classified it as a Rogue AP.
4. Start a timer so that you can see how long it takes for your Wi-Fi security system to detect the presence of your Rogue Client.
5. From your wireless client, connect and associate to the SSID broadcast by the Rogue AP.
   - Make sure the client you use to connect is previously unknown to your Wi-Fi security system and considered an uncategorized client.
6. Periodically refresh the management user interface of your Wi-Fi security system and note the approximate time it takes for the system to detect the Rogue Client connected to your network.
7. Disconnect the wireless client from the Rogue AP. This client should now be considered a Rogue Client by your Wi-Fi security system.
8. Enable the prevention (containment) measures of your Wi-Fi security system.
9. Start a timer so that you can see how long it takes for your Wi-Fi security system to prevent the Rogue Client from associating to a legitimate authorized AP.
10. From the Rogue Client, connect and associate to a known, authorized AP on your wireless network.
11. From the Rogue Client, continuously ping another host on your local wired network.
12. Note the approximate time it takes for the ping activity from the wireless client to stop. This indicates when your Wi-Fi security features have prevented and blocked association of the Rogue Client to your authorized AP.

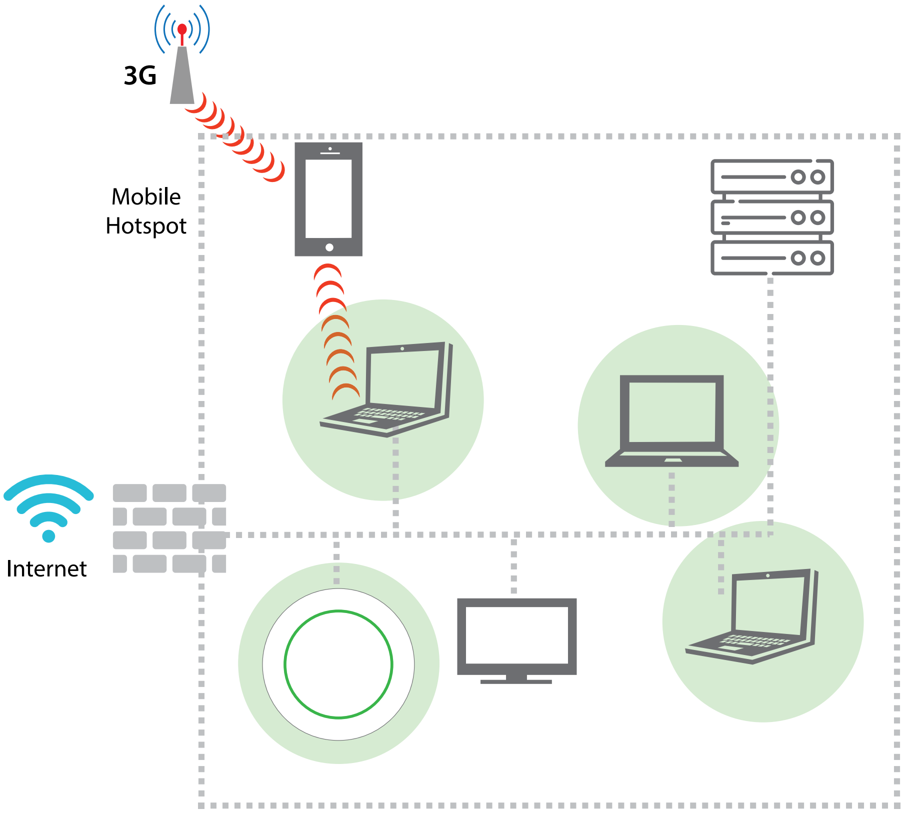
Rogue Client Test Pass/Fail Summary:

- **Detection**: If the Rogue Client is detected in step 6, regardless of detection time, the Wi-Fi security system has passed the test.
- **Prevention:** If the ping activity from the Rogue Client in step 12 stops, the Wi-Fi security system has passed the test.

Neighbor Access Point

Environments such as offices, airports, hospitals, retail stores, and restaurants often contain a mixture of company-managed Wi-Fi client devices that are intended to connect only to internal private company-managed SSIDs. This ensures that the company's network security controls, encryption, and traffic visibility is maintained.

Company-managed Wi-Fi clients should never be allowed to connect to nearby third-party (neighbor) SSIDs. For example, in a corporate office, a clever employee can connect their company-managed smartphones, laptops, or tablets to a nearby mobile or public Wi-Fi hotspot, or open guest Wi-Fi SSIDs at neighboring businesses to bypass corporate security and content-filtering policies.



Requirements:

- Authorized AP
  - An AP connected to your wired network that is known and trusted by your Wi-Fi security system as a legitimate AP.
- External neighbor AP
  - This is an AP not physically connected to your wired network but broadcasting within your air space.
  - You can easily create a neighbor AP with a mobile hotspot on your smartphone.
- Authorized wireless client
  - This client must already be known to your Wi-Fi security system as an authorized client on your network.
- External wireless client
  - This is an external client not known to your network that will connect to the external neighbor AP.
- A host connected to your wired network that can accept a ping request.

Test Steps:

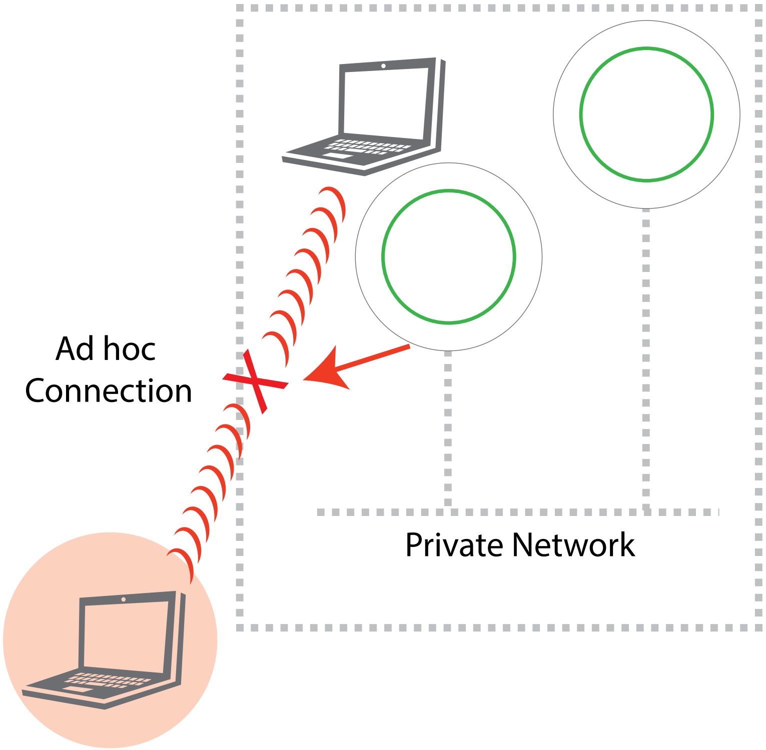
1. Verify that your authorized AP and authorized client are already detected and classified by your Wi-Fi security system as known authorized devices.
2. Enable an External Neighbor AP in the vicinity of your network. For example, you can enable a hotspot on your mobile device. Verify that your Wi-Fi security system has classified the External Neighbor AP correctly.
3. Enable the prevention (containment) features of your Wi-Fi security system.
4. Connect and associate the external client to the Neighbor AP.
5. From the external client, continuously ping a host on your local wired network.
6. Connect and associate the authorized client to the Neighbor AP.
7. Start a timer so that you can see how long it takes for your Wi-Fi security detection and prevention measures to detect the presence of your authorized client connected to the neighbor AP.
8. From the authorized wireless client, continuously ping a host on your local wired network.
9. Note the approximate time it takes for the ping activity from the authorized wireless client to be interrupted. This indicates when your Wi-Fi security features have detected that the authorized client is associated to a neighbor AP. The connectivity is stopped, forcing the authorized client to re-associate to the Authorized AP.

Neighbor AP Test Pass/Fail Summary:

- **Detection:** If the Neighbor AP is detected in step 2, the Wi-Fi security system has passed the test.
- **Prevention**: If the ping activity from the wireless client in step 9 is interrupted, the Wi-Fi security system has passed the test.

Ad-hoc Connection

An ad-hoc connection is a direct peer-to-peer connection between wireless clients instead of through an access point. This ad-hoc connection bypasses any corporate content controls and security policies on your network. Corporate data on an authorized client is vulnerable if it is communicated to an unauthorized client in an ad-hoc connection.



Requirements:

- A wireless device with an ad-hoc wireless network enabled.
- Authorized Wireless client
  - This client must already be known to your Wi-Fi security system as an authorized client on your network.
- A host connected to the same wired network as the ad-hoc device that can accept a ping request.

Test Steps:

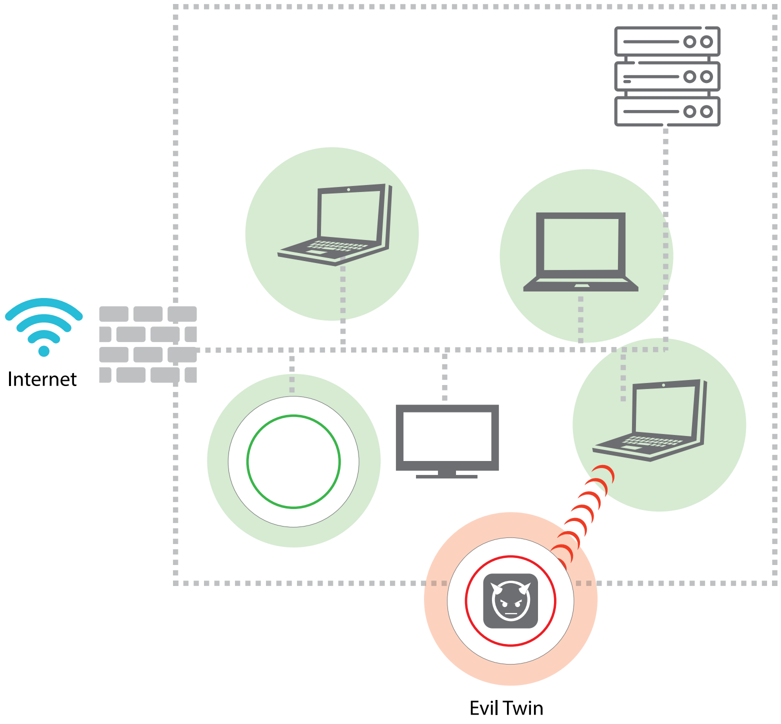
1. Configure a wireless device on your network to offer an ad-hoc connection.
2. Use the NetSpot or inSSIDer software to make sure you can see the ad-hoc SSID on the network.
3. Enable the prevention measures of your Wi-Fi security system.
4. Start a timer so that you can see how long it takes for your Wi-Fi security detection and prevention measures to detect the presence of your authorized client connected via an ad-hoc connection.
5. From your authorized wireless client, connect and associate to the ad-hoc network. From this wireless client, continuously ping a host on the local wired network.
6. Note the approximate time it takes for the ping activity from the authorized wireless client to stop. This indicates when your Wi-Fi security features have detected and prevented the authorized client from associating to the ad-hoc connection.

Ad-hoc Test Pass/Fail Summary:

- **Detection:** If the Ad-hoc connection is detected in step 4, the Wi-Fi security system has passed the test.
- **Prevention:** If the ping activity from the wireless client in step 6 stops, the Wi-Fi security system has passed the test.

Evil Twin Access Point

An Evil Twin is a type of AP where a malicious user duplicates and broadcasts the same SSID name of a legitimate AP within the range of the network. The Evil Twin can also spoof the MAC address of the legitimate AP. Wi-Fi clients connect to the Evil Twin AP unaware that this is not a legitimate AP. When the unsuspecting Wi-Fi client is connected to an Evil Twin AP, the malicious user can execute various man-in-the-middle attacks to intercept the client's communications and data.



Requirements:

- An AP to operate as the Evil Twin AP
  - This can be a WiFi Pineapple device, or any hardware or software-based access point or mobile hotspot with MAC spoofing capabilities.
    Note: The WiFi Pineapple Nano only operates on 2.4 GHz. For best results, consider the WiFi Pineapple Tetra for 2.4 and 5 GHz operation.
- Authorized AP
  - An AP connected to your wired network that is known and trusted by your Wi-Fi security system as a legitimate AP.
- One authorized wireless client
- A host connected to your wired network that can accept a ping request.

Test Steps:

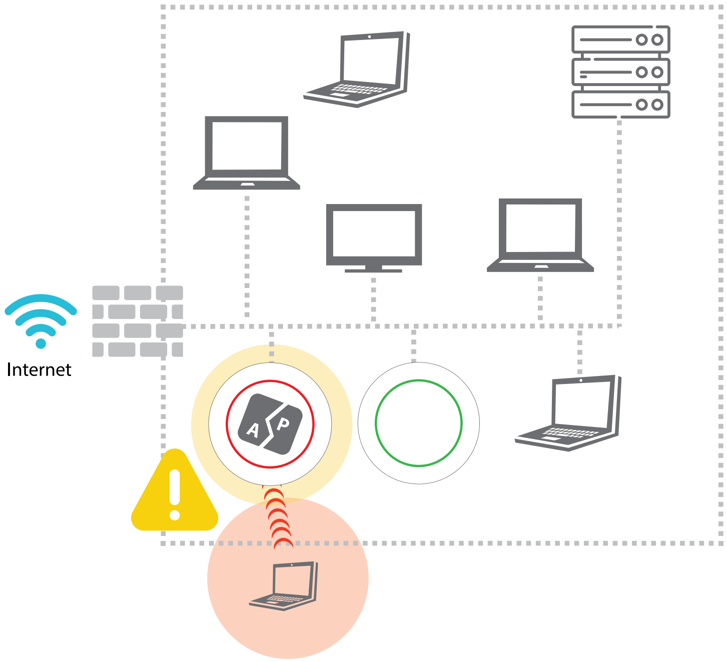
1. Configure an SSID on the Authorized AP. This SSID will act as the legitimate SSID. Note the subnet of your authorized network (for example: 192.168.x.x).
2. Verify this legitimate SSID is detected as an authorized AP by your Wi-Fi security system.
3. Enable the prevention (containment) measures of your Wi-Fi security system.
4. On the AP that will operate as the Evil Twin AP, configure the Evil Twin AP to spoof and broadcast the same SSID as the Authorized AP (case sensitive). Configure the subnet of the Evil Twin AP to be different than your authorized network (for example: 172.16.42.x).
5. Configure the Evil Twin AP to only allow associations from your own wireless client (MAC filtering). This is important to avoid disruption to the legitimate Wi-Fi network you are testing.
6. Use the NetSpot or inSSIDer software to make sure you can see the Evil Twin AP's SSID on the network.
7. Start a timer so that you can see how long it takes for your Wi-Fi security system to detect the presence of the Evil Twin AP.
8. Periodically refresh the management user interface of your Wi-Fi security system and note the approximate time it takes for the system to detect the Evil Twin AP.
9. From the authorized wireless client, connect and associate to the Evil Twin AP's SSID. Note the subnet of the DHCP assigned IP address that the client has received from the Evil Twin AP (for example: 172.16.42.50).
10. Note the approximate time it takes for the authorized wireless client to have its IP address subnet changed from the Evil Twin subnet (172.16.42.x) back to the legitimate authorized AP's sub net (192.168.x.x). This indicates when your Wi-Fi security features have detected and automatically prevented the authorized client from associating to the Evil Twin's spoofed SSID, and forced the client to re-associate to the legitimate authorized AP.

Evil Twin AP Test Pass/Fail Summary:

- **Detection:** If the Evil Twin AP is detected in step 7, the Wi-Fi security system has passed the test.
- **Prevention**: If the authorized client's IP subnet automatically changes from the Evil Twin subnet to the authorized AP subnet, the Wi-Fi security system has passed the test.

Misconfigured Access Point

A Misconfigured AP is an access point that has a configuration (such as encryption or other security requirements) that do not adhere to your network security policies. In busy networks where new APs are deployed, it can be easy for a network administrator to make a configuration error and enable a private SSID with open security and no encryption that potentially exposes sensitive information to interception over-the-air.



Requirements:

- Authorized AP
  - This AP must already be known to your Wi-Fi security system as an authorized AP on your network.
- Two authorized wireless clients
  - These clients must already be known to your Wi-Fi security system as authorized clients on your network.
  - One client will connect to a correctly configured authorized AP with an SSID set up with WPA2/PSK security.
  - The other client will connect to the misconfigured AP with an SSID set up with Open security.
  - A host connected to your wired network that can accept a ping request.

Test Steps:

1. On the Authorized AP, add an SSID with Open security. Use the same SSID name as an existing authorized SSID with WPA2/PSK security.
2. Enable the prevention (containment) measures of your Wi-Fi security system.
3. Associate a wireless client to the correctly configured authorized SSID with WPA2/PSK security enabled. From this wireless client, continuously ping a host on the local wired network.
4. Associate another wireless client to the Misconfigured AP SSID with Open security.
5. Start a timer so that you can see how long it takes for your Wi-Fi security detection and prevention measures to detect the presence of your authorized client connected to the Misconfigured AP.
6. From the wireless client connected to the Misconfigured AP, continuously ping a host on the wired network.
7. Note the approximate time it takes for the ping activity from the wireless client to stop. This indicates when your Wi-Fi security features have detected and prevented the authorized client from associating to the Misconfigured AP.

Misconfigured AP Test Pass/Fail Summary:

- **Detection:** If the Misconfigured AP's SSID is detected in step 5, the Wi-Fi security system has passed the test.
- **Prevention:** If the ping activity from the wireless client in step 7 stops, the Wi-Fi security system has passed the test.

Conclusion

This guide described how to test your Wi-Fi security system for the six known threats defined by the Trusted Wireless Environment framework. Use this check list to summarize the results of your security tests:

Wi-Fi Threat	Detection		Prevention		Notes
	Pass	Fail	Pass	Fail	
Rogue Access Point					
Rogue Client					
Neighbor Access Point					
Ad-Hoc Connection					
Evil Twin Access Point					
Misconfigured Access Point					

If your Wi-Fi security system failed to detect or block any of these threats:

- Check your configuration and security policies to make sure that your APs and Wi-Fi security system are set up to correctly detect and prevent these threats.
- Make sure that only known Wi-Fi devices can connect to your Wi-Fi network, and that all managed APs and client devices are correctly identified and classified by your Wi-Fi security system.
- Make sure your Wi-Fi security policies are applied to unofficial devices introduced by employees or nearby unauthorized users.
- Compare your vendor's Wi-Fi security system against other competitive solutions to make sure you have the best security system for your Wi-Fi deployment that can effectively detect and prevent all of these threats.