Connecting wired and wireless networks

Two significant factors in the security of any network are the measures that exist to ensure accountability for and privacy of traffic: in other words, to control the ability to send packets to the network and to read packets from the network.

Different networks have different characteristics. For example:

- The public Internet is unlikely to have effective restrictions on either sending or reading packets, so neither accountability nor privacy can be assumed.
- Wired networks in organisations often rely on the difficulty of physical access to a live network socket for both accountability (building entry logs show who was in the room) and privacy (unauthorised visitors are kept outside).
- Wireless networks have no physical limits on access (their signals pass through building walls) but often require a user to authenticate before they can send packets and use encryption to protect packets on the network from being read. A wireless network with strong authentication and encryption may offer better protection than a typical wired network with neither.

At any boundary where different security models meet, controls are needed to preserve the security of both sides. Just as firewalls and virtual private networks are used to ensure consistent privacy and accountability when traffic passes between the internal network and the Internet, so the boundary between wireless and wired networks may also need a protective gateway.

Providing Privacy and Accountability

Most gateways implement two types of control. To ensure that traffic from the wireless network can be traced, users must authenticate before they can send traffic to the organisation’s internal network or onto JANET. An authentication gateway will often be part of the access control system for the wireless network itself.

To protect privacy, packet filters may be used. If a wireless network is not encrypted then packet filters can prevent unencrypted traffic leaking from the wired network, where it has some privacy protection, to the wireless where it will have none. For a wireless network with network level encryption (e.g. using WPA/WPA2), filters may be used to avoid exposing traffic on the unencrypted wired side. Packet filters can also block attempts to use insecure application protocols.

Keeping Networks Apart

Although these controls could be implemented on every wireless access point, it is often simpler to connect the access points together and then provide controls at a single gateway where this access point network connects to the external and internal wired networks. This

arrangement, similar to a perimeter de-militarised zone, is shown in the diagram overleaf.

An access point network allows services such as local web pages to be provided to wireless users before they authenticate; at least a DHCP server will be needed to provide clients with their IP address, gateway, etc. Any servers on the access point network must be designed and maintained for security as they will be exposed to untraceable attacks from unauthenticated wireless clients.

There are a number of ways to provide a separate access point network:

- Access points may be connected to dedicated physical network segments;
- Access points may be placed in fixed VLANs (Virtual Local Area Networks), with the gateway providing the only route for traffic between the wired and wireless VLANs;
- Individual clients may be allocated to a VLAN based on their login details (e.g. different VLANs for local and visiting users) using the IEEE 802.1X protocol.

The access point network may also be a suitable place to connect visitors with wired connections, as these should not need direct access to the internal network. If visitor use is planned, the gateway should be placed logically close to the organisation's JANET connection so visitor traffic does not pass across the internal network.

Gateway Function: Packet Filtering

Packet filtering may be implemented using router Access Control Lists or a firewall. since traffic from unauthenticated wireless clients has the same lack of security controls as the public Internet, the filter rules are likely to be similar to those applied where the organisation connects to JANET. Restrictions on insecure protocols and access to sensitive servers should be considered. Packet filters may also be used to force traffic between the wireless and internal networks to use encrypted protocols (e.g. ssL, ssH, VPN) if the wireless network does not provide strong encryption.

An alternative approach is to block all direct traffic between the wired and wireless networks and require all access to be done through application-level proxies.

Gateway Function: Authentication

Two main alternatives are available to force a user to authenticate before sending their packets beyond the access point network.

- IEEE 802.1X is technically superior, since it works at the network layer and prevents any IP packets being sent before the user has authenticated. 802.1X requires software to be configured on the client – once this is done, the connection process is secure and transparent to the user. However, client software is not yet built in to all platforms.
- With web redirect gateways users open a web browser and enter their username and password. If authentication succeeds then the gateway allows IP packets to pass from the client to the wired network. Users must protect their password by checking that the gateway is genuine and not a rogue access point set up to steal user credentials. In future, web redirect systems are likely to be replaced by the more secure IEEE 802.1X on both wireless and wired networks.

References

- Wireless 802.11 standards factsheet: http://community.ja.net/library/advisory-services/wireless-80211-standards [1]
- User Authentication factsheet: http://community.ja.net/library/advisory-services/user-authentication [2]
- Safe Use of 802.1X Wireless Networks factsheet: http://community.ja.net/library/advisory-services/safe-use-8021x-wireless-networks [3]

Links
[1] https://community.ja.net/library/advisory-services/wireless-80211-standards
[2] https://community.ja.net/library/advisory-services/user-authentication
[3] https://community.ja.net/library/advisory-services/safe-use-8021x-wireless-networks