

WIRELESS SOLUTIONS FOR THE

Secure Enterprise

Wireless security — Is it enough?

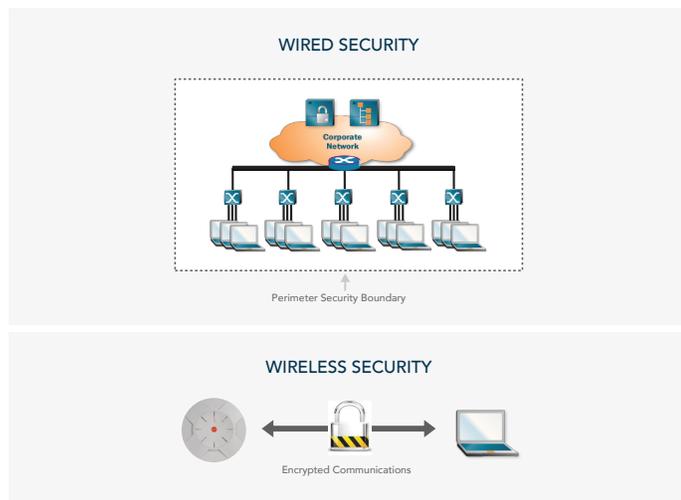
With the influx of tablets, smartphones, and the BYOD (bring your own device) phenomenon, wireless is quickly becoming the new norm for network connectivity. The days of network security being dependent on a directory server profile are over.

The security considerations of operating wired local area networks (LANs) and clients are well known. Ubiquitous wireless networks on the other hand are newer to many IT administrators and so are the aspects of operating these networks. Shortcomings in the initial Wi-Fi standards tainted the perception of wireless security, but these limitations were solved with the 802.11i advancements put in place in 2004, paving the way for the broad adoption of wireless networks in all types of applications. In the end, both wired and wireless media are able to provide strong security if deployed correctly.

Comparison of wired and wireless security

Wired network security, perimeter security, is based on the principle that communications are contained within the network (cables), and as long as only authorized users have access to that media, communications are secure. Physical protection for the wired infrastructure comes from fences, walls, doors, guards, receptionists, etc.

Wireless network security is fundamentally different because wireless communication propagation cannot be completely contained within a specific physical area, and as a result, additional security measures are required. These include user authentication, encryption of the communication, and RF monitoring of the environment.



Maintaining a secure environment

Building a wireless infrastructure that not only meets connectivity and performance requirements but also addresses security concerns is attainable by focusing on some key best practices.

The three key challenges to deploy a secure wireless solution include:

1. Controlling user access
2. Securing communication across the air
3. Monitoring for wireless threats

User access control

If deploying free internet for the local coffee shop, little access control is required; however the corporate environment is clearly different. Network users, whether employees, contractors, or guests may all require network access, however each class of user should be restricted by policy to the resources that they can access, when they can access it, how much they can access, etc. The first challenge of any wireless or wired network security policy is controlling access to the network.

Secured communications

Wireless communication propagates beyond the physical boundaries of an organization; as such there is no way to restrict access to the physical medium. Corporate communications, even if not considered secret, should always be considered proprietary and as such require a level of protection. Wireless communication, not intended for public distribution, requires encryption services able to protect the data without degrading network performance.

Wireless threat monitoring

While wireless solutions improve access and productivity, their ubiquitous coverage also enables the potential for non-conforming or even malicious devices to be deployed within the network, having the potential to impact network operation. When wireless is deployed as a primary mode of network connection, interruptions of the service can have serious corporate implications. As a result enterprise-class monitoring is required, not ad hoc or other non-continuous solutions.

Key benefits:

- Unlimited SECURE mobility
- Distributed security processing
- 24/7 ubiquitous security monitoring

Key features:

- Dedicated 24/7 threat monitor
- Line-rate encryption processing
- Simplified security management
- Device identification and classification

Recommended actions:

- Define a security policy
- ID and classify all clients
- Secure communication with WPA2 Enterprise
- Verify client security posture

Engineering a secured wireless network

Today, a wireless network designed properly is widely considered equal to or in many cases more secure than most deployed wired networks. This is accomplished by applying multiple layers of security through mechanisms such as authentication, encryption, client classification, and IDS/IPS (intrusion detection and intrusion prevention services) the wireless network can be assuredly secured. The following sections will discuss each of these security layers and how they can be applied in production networks with the Xirrus Wi-Fi solution.

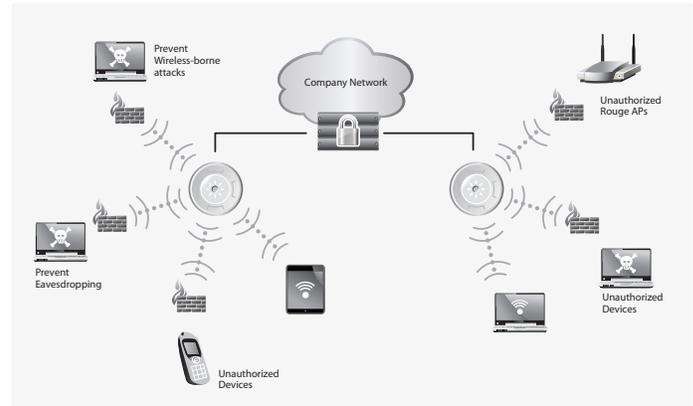
Key security protocols and mechanisms include the following:

1. Device identification and management
2. User authentication
3. Data encryption
4. RF environment monitoring

Device identification and management

Just because a user has the credentials to access the network that does not mean that user should get access to all of the corporate resources. For instance, a corporate employee on his company-provided laptop may get access to all of the corporate resources. However that same employee, using his own iPad, may only be provided access to corporate email and the web. A guest may only need access to the Internet. Xirrus Arrays allow different user groups to be created with each group being mapped to specific VLANs, access control list, and QoS parameters. By assigning devices and users to a specific group IT administrators can easily control who has access to which information from what devices.

Xirrus' Device Fingerprinting identifies the device operating systems such as iOS, Windows, BlackBerry, or Android and can then classify the device type such as tablet, laptop, or smartphone. Once the device has been identified, a policy can be applied to control a device's reach and behavior. The device ID, along with the user ID, can be used together to map that instance to a specific user group.



Security threats

Authentication — controlling user access

Authentication ensures users are who they say they are, and occurs when users attempt to join the wireless network and periodically after that.

The following authentication methods are integrated in the Xirrus Solution:

- RADIUS 802.1x — Arrays support standard 802.1x allowing them to support internal or external RADIUS services for client authentication. Third-party RADIUS is also supported.
- Pre-shared key (PSK) — Uses a pass-phrase or key that is manually distributed to all authorized users. The same pass-phrase is given to client devices and entered in each Array.
- MAC access control lists (ACLs) — MAC access control lists provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network.
- Web page redirect (captive portal) — Integrated in the Array offers web-based authentication against an internal or external RADIUS server.

Pepperdine, founded in 1937, is an independent Christian university with approximately 8,300 graduate and undergraduate students in five colleges and schools in Malibu, CA. Its required a wireless network in its administrative offices and dormitories that delivered greater performance with uncompromised security.

Requirements

- Support high density of users with complete security
- Provide high bandwidth for each user in a device-rich environment
- Install minimum number of devices since new cable had to be pulled
- Support for data and voice over Wi-Fi
- Integration with NAC solution
- Easy and secure Internet access for students, faculty, and guests

Solution

- Xirrus Array deployment
- 75% less equipment, reducing the number of APs by almost 500
- 75% fewer cables
- 75% fewer switch ports
- 75% less time to install
- Integration into NAC and AAA environment

Encryption — securing the communication

High performance encryption/decryption in the enterprise Wi-Fi network is a MUST. As a result a Wi-Fi network needs to support each client using the highest level of encryption possible (WPA2/AES) and without degrading the overall performance of the network. The Xirrus Wi-Fi Array supports all standard encryption types, including WEP, WPA, and WPA2.

Encryption/decryption processing is processor intensive and if all traffic (as recommended) needs to be protected a central processor is quickly oversubscribed. Xirrus engineered hardware-based encryption/decryption into each Array, enabling a Xirrus solution to deliver line-rate encryption no matter how many access devices or clients are connected. By distributing the security processing to the edge of the network, instead of at a centralized controller, higher performance and stronger security are achieved.

RF monitoring — intrusion detection and prevention

The Xirrus Wi-Fi Array provides the maximum level of security for 802.11n networks by integrating a dedicated 24/7 threat sensor. The threat sensor scans all channels (2.4GHz and 5GHz) for security threats and automatically mitigates them. This varies from the design of other vendors whose threat sensors time-slice between client services and security scan function, compromising both services.

The Array also monitors for known wireless attack signatures, currently including over 20 types of DoS (denial of service) and impersonation threats.

Summary

No single device, feature, or protocol can protect your wireless or even wired network. It will always require a layered approach. A Xirrus wireless solution will provide this level of service with the ability to ID and classify users, securely protect data as it traverses the network, and also monitor the surrounding RF environment for threats. All these capabilities are integrated in a single device, thus allowing a secured, high performance wireless network to replace existing wired networks and be deployed with 75% fewer components than any other wireless solution.

For more information

For more details on how Xirrus can help you solve the security challenges caused by the influx of Wi-Fi devices, visit us at www.xirrus.com or send us an email at info@xirrus.com.

About Xirrus

Xirrus provides unique, high-performance, array-based wireless solutions that perform under the most demanding conditions, while delivering wired-like reliability, superior security, and less infrastructure requirements. Xirrus is a privately held company headquartered in Thousand Oaks, CA.



1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit:
xirrus.com or
email info@xirrus.com