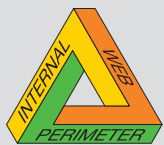


Building Secure Wireless LANs

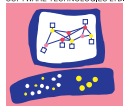
In this Document

- 1 Wireless LANS –Threats?
- 2 Wireless Insecurity – 802.11 and WEP
- 3 Check Point Secure VPN Solutions – Enabling Wireless Security
- 4 Summary



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Wireless LANs – Threats?

Wireless LANs provide enterprises with a flexible technology that reduces deployment costs when compared to traditional “wired” networks. At the same time, they enable workers to move from area to area without losing connectivity. Because of this, the wireless LAN market is expected to grow from \$2.4 billion to \$5.2 billion by 2005.

The benefits of wireless LANs come with a cost. Unlike wired networks, wireless LANs make it difficult, if not impossible, to control physical access to the network. Departmental units can purchase and deploy wireless LANs at a low cost with no IT department involvement – creating holes in the security perimeter. Widely available software and antennas allow attackers to surreptitiously participate in the wireless LAN from remote locations, eavesdropping on information and access the corporate network.

Because wireless LANs bypass corporate network perimeters, it is critical that organizations revise their views on Perimeter, Internal and Web security. This paper discusses the threats associated with wireless LANs and how Check Point solutions can be used to connect wireless LAN users securely.

Wireless Insecurity – 802.11 and WEP

The leading wireless LAN protocols – 802.11a and 802.11b – contain methods meant to protect against eavesdropping and attack. Wired Equivalent Privacy (WEP) includes authentication and encryption which limits access to information and the corporate network. Recent studies have found that WEP is vulnerable to simple attacks and is not strong enough to provide proper confidentiality or authentication.

Security weaknesses in wireless protocols

WEP uses a flawed implementation of the RC4 encryption algorithm to provide confidentiality. Any radio-transmitted data that is intercepted by an attacker – a simple task – can be used to discover the key used to encrypt it and other transmitted data, allowing the attacker to examine it at will. This encryption key is also used for authentication between wireless access points and wireless clients. Attackers can misuse the encryption key and pose as legitimate users with access to corporate resources.

Many wireless LAN vendors have sought to address security concerns by incorporating 802.1X but have not fully addressed every issue. 802.1X, an IEEE standard, is designed to strengthen authentication and improve encryption key handling. Yet this standard has been shown to be insecure when combined with wireless LAN standards. A paper by two University of Maryland scientists, (Mishra, Arunesh, and Arbaugh, William A. (2002,) An Initial Security Analysis of the IEEE 802.1X Standard. College Park, MD: University of Maryland) demonstrates possible attacks against the standard.

Possible attacks against wireless LANs

The vulnerabilities detailed make the corporate network vulnerable to many possible attacks. These attacks can compromise the organization’s information assurance, reducing its trustworthiness. Three possible security gaps for attack include radio waves, corporate network, and wireless client machine.

Radio-based attacks

The insecurities found in WEP allow attackers to circumvent the encryption of wireless transmitted data. Attackers can passively eavesdrop on message content or analyze traffic on the wireless LAN for future attacks. Intruders can also launch active assaults such as replay or message modification attacks. Another common attack floods a wireless access point with radio noise. The attacker can then set up a bogus access point and hijack communications systems by posing as legitimate resources.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Attacks against the corporate network

Legitimate corporate resources are threatened in two ways by wireless LANs. First, weak authentication mechanisms allow unauthorized intruders to easily join the corporate network and access corporate resources. Second, most wireless implementations place very little access control between the wireless network segment and the wired network. Attackers can direct whatever traffic they wish against corporate resources. When compared to the Internet gateway, wireless access points do little or nothing to detect and protect against malicious traffic.

Attacks against client machines

Wireless clients are located outside the corporate firewall, yet many network architectures treat them as internal clients. Attackers can compromise individual clients, using them to collect information or to act as tunnels into the corporate network. In “ad-hoc” mode of 802.11, client machines are allowed to directly connect to one another – providing an avenue of attack for intruders.

It is important to understand that intruders can launch attacks against a wireless LAN without leaving the forensic evidence found in traditional attacks. The intruder does not leave an audit trail – such as a traceable IP address assigned by an ISP – when he or she ceases participation in the WLAN. There have been cases where an intruder uses a wireless LAN to download copyrighted material or to launch attacks. With no audit trails, the wireless LAN operator may be held responsible for any illegal activities that intruders launch from the network.

With the risks presented by wireless LANs, it is critical that they be considered untrusted networks. Users must be treated as unknown until properly authenticated by proven methods. Sensitive data must be properly encrypted with accepted encryption algorithms. Network traffic must be inspected and have proper access control rules applied. Wireless LAN clients need the same level of security as remote access clients using broadband connections. Only by treating a wireless LAN as insecure can security personnel ensure the integrity of their wired corporate network.

Check Point SecureVPN Solutions – Enabling Wireless Security

Check Point’s philosophy is that security should be seamless – the Internet, the intranet, the extranet and the wireless LAN need a common architecture to ensure consistent security enforcement with proven technologies. SecureVPN solutions such as VPN-1® Pro™ and VPN-1 SecureClient™ enable integration of the wireless LAN into the enterprise security architecture. By deploying them, organizations can gain the data privacy, reliability, user authentication, and access control needed to securely connect wireless clients.

End-to-End Data Confidentiality and Integrity

Because of WEP’s vulnerabilities, the current best practice for wireless LAN security is to deploy an IPSec virtual private network (VPN). SecureVPN solutions are IPSec-compliant and offer proven data confidentiality and integrity. Corporations can choose between DES, 3DES, or Advanced Encryption Standard (AES), the new United States federal encryption standard, to protect information in transit.



Intelligent Security

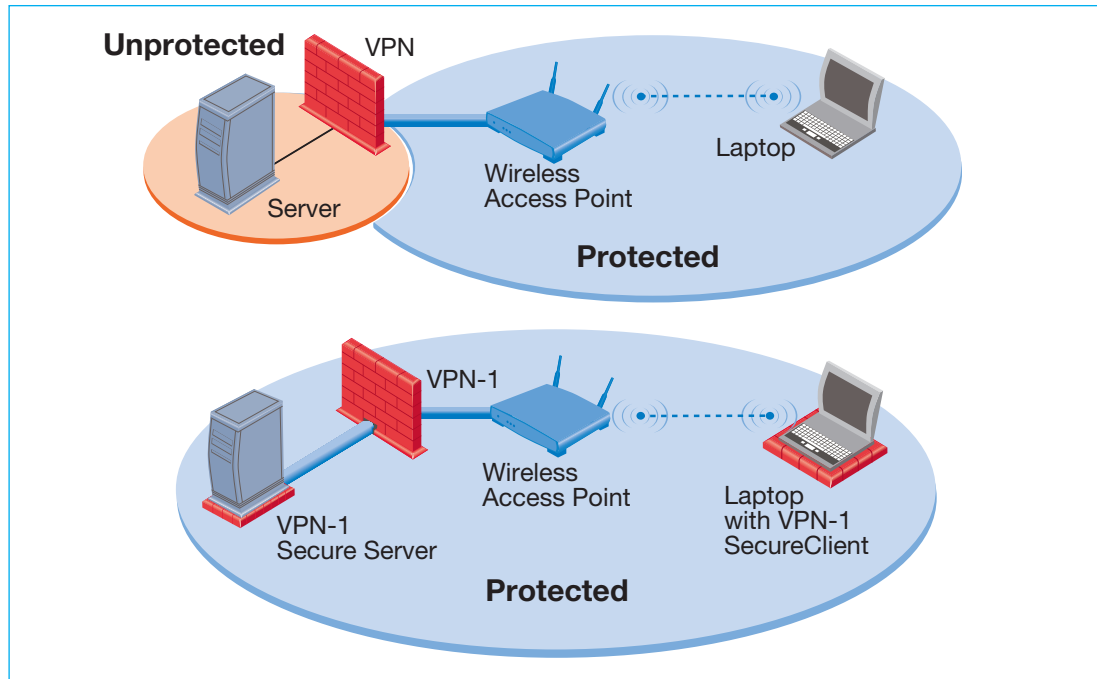


Figure 1: SecureVPN solutions can be used to encrypt sensitive information from client to server. Other products leave data exposed on the wired network.

With VPN-1, network administrators gain the ability to encrypt information from end-to-end. Because other solutions are client-gateway solutions, information is decrypted at the edge of the wired LAN and not protected. With intelligent VPN routing, VPN-1 examines traffic as it enters the wired network and then re-encrypts it – if desired – before sending it on to its final destination in the corporate network, enhancing internal security. Organizations can deploy VPN-1 SecureServer on individual servers to act as end points.

Flexible Authentication

Check Point provides an authentication framework that is flexible, cost-effective and simple to manage. Unlike current wireless LAN authentication methods, SecureVPN solutions can identify individual users through passwords, tokens, biometrics, certificates, and more. Check Point's user-based authentication increases accountability while leveraging existing authentication methods. Organizations can opt to use the integrated Certificate Authority for out-of-the-box digital certificates. A key component of Check Point's One-Click VPN technologies is the integrated Certificate Authority enables strong authentication for wireless LAN users without the need to deploy a separate third-party Public Key Infrastructure (PKI).

Integrated FireWall-1 Protection

All SecureVPN solutions integrate the same Stateful Inspection engine found in FireWall-1® to inspect network traffic and protect against attacks. By deploying Stateful Inspection in both the VPN gateway and client, organization's can ensure the security of the corporate network and workers on the untrusted wireless segments.

VPN-1 SecureClient extends network security down to individual computers with a centrally-managed personal firewall containing a customizable security policy. Organizations can prevent an insecure wireless client – for instance, a client using an out-of-date browser with known vulnerabilities – from accessing the corporate network until it is secure. Unlike other VPN clients, VPN-1 SecureClient fully integrates the firewall and the VPN client – enabling administrators to manage both from a single interface.



We Secure the Internet.

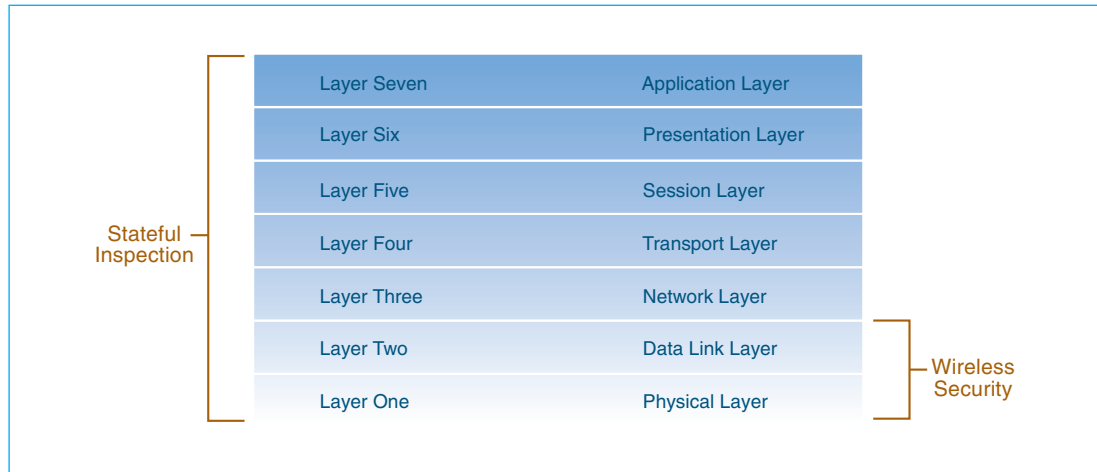


Figure 2: VPN-1 solutions offer more complete protection against attacks than wireless protocols. They inspect all layers of communications up to the application level.

Using VPN-1 Pro™ to segregate the wireless LAN from the corporate network enables organizations to develop more flexible, customizable policies. For example, an organization can limit access to the ERP application to authorized employees during regular working hours. If someone from the wireless LAN attempts to access the application during non-business hours, alarms can be set allowing administrators to investigate. Unlike wireless security methods that work at a much lower level, it can detect and inspect over 150 different applications – enabling it to block malicious traffic from entering the corporate network.

Universal VPN Access

Check Point's Secure VPN solutions provide a single architecture that can be used to secure both wireless LAN users and remote access clients. VPN-1 SecureClient can be installed on all mobile devices running on Windows platforms, including Pocket PCs.

VPN-1 SecureClient offers two major benefits when used for universal access: ease-of-use and client maintenance. With the majority of wireless clients being laptops and PDAs, these machines will very likely be used remotely as well. Deploying a single VPN client for both reduces the training and complexity for end users. VPN-1 SecureClient reduces maintenance overhead as well. It can be automatically updated without administrator involvement, eliminating the need for personnel to manually update each wireless client and greatly increasing management efficiency.

When compared with Other VPN products, Check Point SecureVPN solutions also enhance usability within the wireless environment. When an end user moves from one access point's coverage to another area, other VPN products have traditionally forced the end user to reauthenticate and to restart web, ftp, email, or any other sessions. Check Point SecureVPN solutions enable transparent roaming throughout the whole wireless environment without the need for complex technical solutions.

To ensure interoperability, the Open Platform for Security (OPSEC) program certifies that wireless LAN products work with SecureVPN solutions. A list of certified products is available at http://www.opsec.com/solutions/perf_wireless.html.



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Summary

Corporations need to plan for wireless LANs within their enterprise security policy or face a loss of network integrity as departments deploy their own wireless LANs without IT involvement. Check Point SecureVPN solutions based on the VPN-1 family enable organizations to quickly connect wireless clients to the corporate network and protect them against Perimeter, Internal and Web attacks.

When deciding what security systems to deploy for wireless communications, it is important to consider the flexibility and reputation that that system provides. Even as new wireless protocols are developed, they will lack flexibility and will need to prove their reliability. Check Point SecureVPN solutions for wireless LANs provide proven security for both small businesses and global enterprises. With Check Point SecureVPN solutions, users can travel between remote locations and wireless LANs seamlessly and securely.

About Check Point Software

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Check Point provides Intelligent Security Solutions for Perimeter, Internal and Web Security. Based on INSPECT, the most adaptive and intelligent inspection technology and, SMART Management, which provides the lowest TCO for managing a security infrastructure, Check Point's solutions are the most reliable and widely deployed worldwide. Check Point solutions are sold, integrated and serviced by a network of 1,900 certified partners in 86 countries. For more information, please call us at (800) 429-4391 or (650) 628-2000 or visit us on the Web at <http://www.checkpoint.com> or at <http://www.opsec.com>.

CHECK POINT OFFICES

International Headquarters

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@Checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, and VPN-1 VSX are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

P/N 000000

