

Integrating WiMax into a Secure Environment

Abstract

As WiMAX emerges as a new industry standard for wireless, the advantages for users can be clearly seen. With its potential transfer speed and operational range WiMAX provides another option for connectivity. For example a company that has two connections from separate Internet providers could lose connectivity if both connections utilize the same local exchange carrier (CLEC) and share the same physical pipe from the company's office to the CLEC's location. An accidental cut in the pipe would mean both connections would be lost.

WiMAX eliminates the need for the CLEC and provides true multi-tier connectivity. It can be used to provide Internet for businesses in rural areas, to interconnect offices located in the same geographical area or even allow employees wireless access to the company's internal network resources.

However security remains the key issue when integrating WiMAX into a corporate environment. Unlike a physical network, a perimeter approach cannot be taken with wireless. In a physical network most malicious attacks come from the Internet, thus securing the perimeter is the most important step in securing a physical network. However with wireless, an attack can be generated anywhere. Every link and piece of hardware on the wireless network will need to be protected.

The designers of WiMAX were aware of inherent security issues found in Wi-Fi. And as a result greater security functionality was built into the base of the 802.16 standard. The current 802.16-2004 (fixed WiMAX) standard specifies using a key management protocol, which adheres to server/client architecture and uses the X.509 digital certificates to authenticate subscriber stations (SS).

Every SS comes with it's own factory installed certificate, containing the station's Public Key and media access control (MAC) address. The SS presents the certificate to the base station upon initial negotiation and allows the base station to establish the identity of the SS. After the identity is established, the key management protocol allows for periodic refreshing of the keys, making communications more secure.

The 802.16-2004 standard also specifies more advanced encryption algorithms such as 3DES and AES. However hardware companies seeking certification are not required to support all specified encryption standards. As an example AES-CCM probably offers the most comfortable level of security. However it is not clear how many manufacturers will support it, and what key sizes they will allow.

There is also the question of compatibility between different vendors gear. At this point we can assume that the above-mentioned X.509 digital certificate based authentication, DES and 3DES encryption algorithms should be compatible across all WiMAX certified hardware.

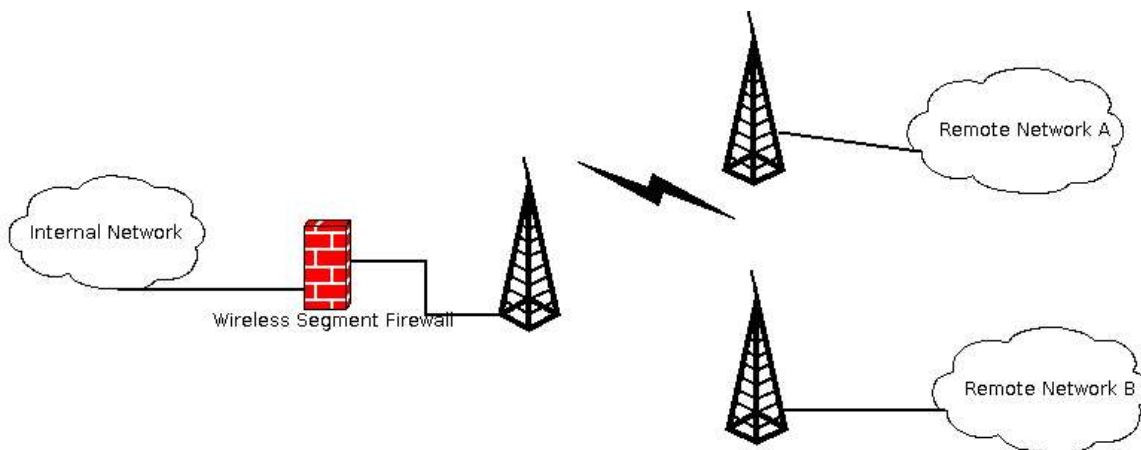
But is that enough to meet security standards of the enterprise? Hardware makers like Intel and Terabeam do not seem to think so. They claim that the authentication facilities of WiMAX are limited and encryption standards like 3DES, which come to us from the VPN world are simply outdated and inadequate. Thus Intel is pushing to implement EAP and AES with up to 256bit keys into the 802.16 standard.

At this point it's not clear how successful those hardware makers will be and how many manufactures will jump on their band wagon. So this paper will assume we are working with today's current standards.

Listed below are steps that can be taken to ensure a wireless network doesn't present a serious security risk to the company.

Segment Segregation

A wireless network should be treated as having a higher security risk than an internal physical network. It is always a good idea to separate the wireless network from sensitive resources. System administrators should police all traffic passing between a wireless segment and the rest of the network.



- Figure 1 -

Figure 1 illustrates a wireless segment separated from the rest of the network by a firewall. In this case "firewall" is a logical concept and can mean just another Ethernet port on your existing firewall.

The advantage of segment separation rests in being able to control the traffic flow to and from a wireless segment by applying policies to the firewall. For example, if all you want is to allow wireless users to browse the web and access your intranet web server, then you can specify rules

to that effect ensuring that no other type of traffic will traverse the firewall, and cause a problem in the internal network.

In addition most enterprise level firewalls support “per policy” authentication methods. This allows system administrators to configure policies preventing traffic outside of clearly defined policies until they authenticate using either HTTP, TELNET or FTP protocols, thus adding another authentication layer to the security.

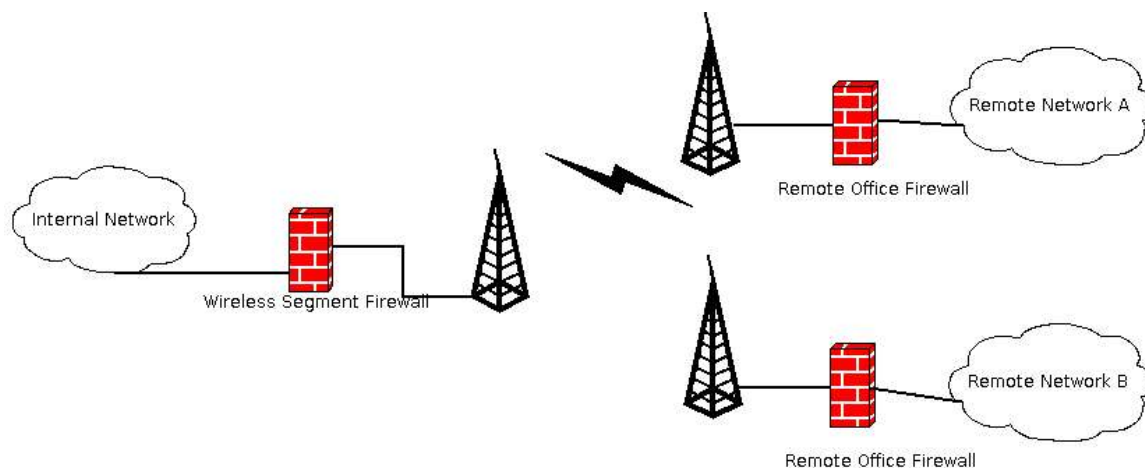
User databases can either be maintained locally on the device, or by using selected firewalls, which support the use of existing RADIUS or TACACS+ servers.

It is possible to go one step further and integrate per policy authentication with two factor authentication technologies like RSA SecurID®, which provides physical tokens with rotating security PINs. These do provide a much more secure user authentication system than reusable passwords.

Another Level of Encryption

If your company provides Internet services to end customers, 3DES encryption might be more than enough. However if you are a financial enterprise or a company dealing with personal data, a more secure wireless implementation might be desired. 3DES may be secure enough to discourage most basic attacks, but it might not be enough to prevent corporate espionage, government snooping or the more persistent attackers.

If AES with at least 256bit is not supported across your WiMAX equipment it might be a good idea to implement another level of encryption. Current VPN technology can be used for this purpose.



- Figure 2 -

Figure 2 illustrates a wireless environment with a firewall at every location participating in a Hub-and-Spoke Virtual Private Network.

The “Wireless Segment Firewall” acts as a hub and end point for VPN tunnels originating from “Remote Network A” and “Remote Network B”. All traffic is encrypted before it even gets to a wireless network, and since the “Wireless Segment Firewall” is configured to drop all non-VPN traffic, even if someone does manage to break the security and successfully authenticates with a Base Station, they will not gain access to any network resources.

An extra encryption layer also secures traffic against snooping. Attackers will have to combat two layers of encryption making the task of snooping exponentially more difficult.

VPN technologies provide a wider range of authentication facilities, allowing deployment of VPN clients installed on individual systems at remote ends of the link. This eliminates the need for costly firewalls at each remote end, making the entire setup more cost effective.

Intrusion Detection Systems

Modern enterprise level firewalls afford users the ability to do more than just police traffic based on source and destination addresses. They can integrate technologies like stateful inspection, examine packets on an application layer and even implement basic intrusion detection techniques. These features separate firewalls from routers with ACL capabilities.

However in some scenarios it might be desirable to implement a full intrusion detection system (IDS) in a wireless segment. This allows administrators to monitor the links for traffic anomalies, attack signatures and other malicious traffic.

In the Figure 1 & 2 scenario IDS can be deployed just after the “Wireless Segment Firewall”. If malicious traffic manages to evade the security measures of the firewall, it will be caught by the IDS system.

Some IDS systems will allow you to implement advanced technologies like Honeypot or Darknet, allowing proactive monitoring of hacker activity on both wireless and wired networks.

Conclusion

As the release of certified WiMAX hardware approaches, it is important to understand the security challenges presented by current standards as well as those to come in the future. Designing a network with a wireless segment is not an easy task and should be approached only after carefully weighing all the facts.

NetSieben provides superior services and products that enables the customer to secure their network environment and concentrate on their core business. Our team of security experts have worked with many of the worlds most sophisticated environments. These include the large ISP and telecommunications companies such as Sprint PCS, Williams Communications, Tiscali and Cegetel.