Chương 3 :

BẢO MẬT VÀ QUẢN LÝ MẠNG KHÔNG DÂY

3.1 ACCESS POINT

Access Points (APs) đầu tiên được thiết kế cho các khu trường sở rộng rãi. Nó cung cấp các điểm đơn mà người quản trị có thể cấu hình nó. Nó có những đặc thù cho phép một hoặc hai sóng vô tuyến cho mỗi AP. Về mặt lý thuyết, AP hỗ trợ hàng trăm người dùng cùng một lúc. AP được cấu hình bởi ESSID (Extended Service Set ID). Nó là một chuỗi các nhận dạng mạng không dây. Nhiều người sử dụng chương trình máy khách để cấu hình và có một mật khẩu đơn giản để bảo vệ các thiết lập của mạng.

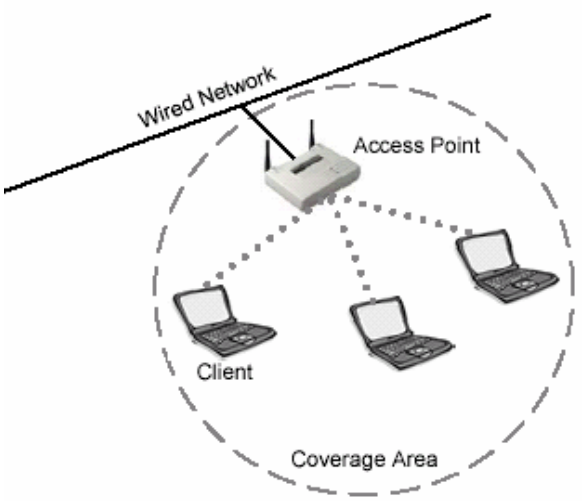
Hầu hết các AP đều tăng cường cung cấp các tính năng, như là :

- Tính năng lọc địa chỉ MAC. Một sóng vô tuyến của máy khách cố gắng truy cập phải có địa chỉ MAC trong bảng địa chỉ của AP trước khi AP cho phép kết hợp với AP.
- Tính năng đóng mạng. Thông thường, một máy khách có thể chỉ định một ESSID của bất cứ sự kết hợp nào với bất cứ một mạng hiện hữu nào. Trong tính năng đóng mạng, máy khách phải chỉ định ESSID rõ ràng, hoặc nó không thể kết hợp với AP.
- Tính năng Anten ngoài.
- Tính năng kết nối liên miền.
- Bản ghi mở rộng, thống kê, và thực hiện báo cáo.

Access point

Một tính năng tăng cường khác bao gồm quản lý khóa WEP động, khóa mã hóa trao đổi công cộng, kết ghép kênh, và các đồ chơi trẻ con khác. Nhưng đáng tiếc, những kiểu mở rộng hoàn toàn các hãng sản xuất (kiểu mẫu), và không có bảo hộ bởi bất cứ chuẩn nào, và không hoạt động với các sản phẩm khác. Điều đó có nghĩa là, một máy khách phải kết hợp nó với một AP, và nó sẽ không đi xa hơn các hạn chế của AP trên những dịch vụ mà máy khách có thể truy cập.

APs là sự lựa chọn lý tưởng cho những mạng cá nhân với nhiều máy khách đặt trong một khoảng không vật lý, đặc biệt là các đoạn mạng có cùng Subnet (giống như là doanh nghiệp hoặc khu trường sở). AP cung cấp mức độ điều khiển cao để có thể truy cập bằng dây, nhưng giá của nó không rẻ (giá trung bình của một AP từ 800 đến 1000 USD).



Mô hình cài đặt Access Point

Một lớp khác của AP thỉng thoảng được xem như là cổng nhà riêng. The Apple AirPort, Orinoco RG-1000 và Linksys WAP11 là các ví dụ cụ thể của các AP cấp thấp. Các sản phẩm này phải có giá thành thấp hơn các sản phẩm thương mại khác. Nhiều Modems được sản xuất, cho phép truy cập mạng không dây bằng cách quay số. Những dịch vụ cung cấp cân bằng nhất là Network Address Translation (NAT), DHCP, và dịch vụ cầu nối cho các máy khách. Trong khi các dịch vụ đó không thể hỗ trợ đồng thời nhiều máy khách như là AP cao cấp, thì chúng lại có thể cung cấp truy cập rẻ và đơn giản cho nhiều ứng dụng. Cấu hình một AP không đắt tiền cho kiểu bắt cầu mạng cục bộ, bạn có trình độ điều khiển cao hơn các máy khách riêng lẻ để có thể truy cập mạng không dây.

Không kể những AP giá cao, những AP là nơi để xây dựng hệ thống thông tin mạng không dây. Chúng là một dãy đặc biệt tốt để điều khiển sự lặp lại các vị trí, vì chúng dễ dàng cấu hình, tiêu thụ năng lượng thấp, và thiếu những bộ phận di chuyển.

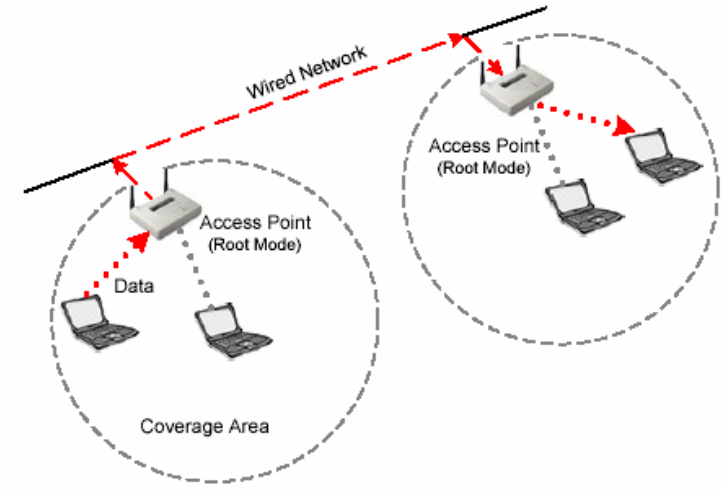
3.1.1 CÁC MODE CỦA AP

APs thông tin với những máy khách, với mạng hữu tuyến, và với một AP khác. Có ba chế độ trong AP mà chúng ta có thể cấu hình :

- Chế độ gốc
- Chế độ lặp
- Chế độ cầu nối

3.1.1.1 CHẾ ĐỘ GỐC (ROOT MODE)

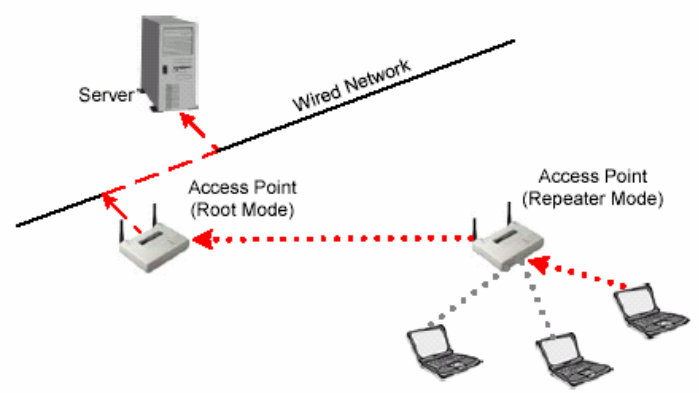
Chế độ gốc được dùng khi AP kết nối với mạng xương sống thông qua giao diện mạng cục bộ. Những AP mới nhất hỗ trợ những chế độ cao hơn chế độ gốc cũng cấu hình từ chế độ gốc mặc định. Khi AP kết nối tới đoạn mạng hữu tuyến thông qua cổng cục bộ, nó sẽ cấu hình mặc định ở chế độ gốc. Khi trong chế độ gốc, AP kết nối tới những đoạn mạng phân bổ giống nhau để có thể giao tiếp với các đoạn mạng khác. AP giao tiếp với mỗi chức năng lang thang có sắp xếp như là kết hợp lại. Các máy khách có thể thông tin với các máy khách khác ở các ô khác nhau thông qua AP tương ứng để đi qua đoạn mạng hữu tuyến.



Access Point trong chế độ gốc

3.1.1.2 CHẾ ĐỘ LẶP (REPEATER MODE)

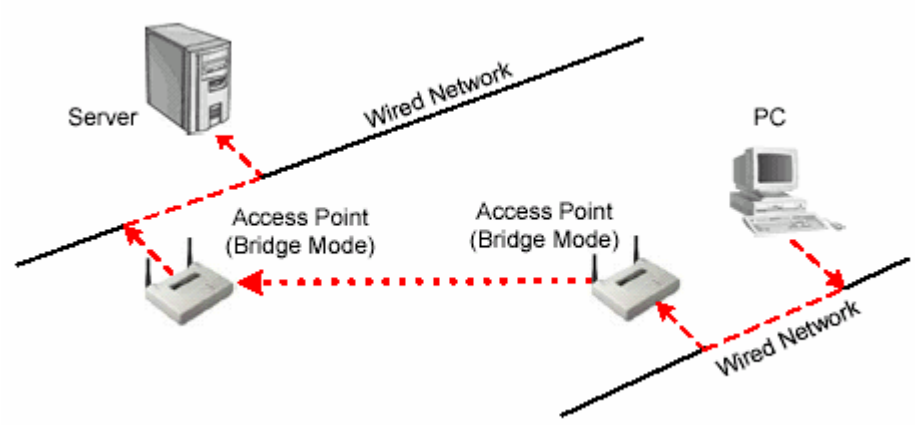
Trong chế độ lặp, APs có khả năng cung cấp những liên kết ngược trong mạng hữu tuyến khá hơn một liên kết hữu tuyến bình thường. Một AP được thỏa mãn như là một AP gốc và các AP khác giống như là các bộ lặp. AP ở chế độ lặp kết nối tới máy khách như là một AP và kết nối tới AP gốc ngược như là chính máy khách. Không đề nghị sử dụng AP ở chế độ lặp trừ khi cần sự tuyệt đối an toàn bởi vì các ô xung quanh mỗi AP trong viễn cảnh này phải được chồng lấp nhỏ nhất là 50%. Cấu hình này phải đủ mạnh để giảm bớt các kết nối của các máy khách tới AP ở chế độ lặp. Ngoài ra, AP ở chế độ lặp là sự truyền đạt với những máy khách chẳng khác gì AP ngược với liên kết không dây, giảm số lượng trên một đoạn mạng không dây. Người dùng gắn bó với AP ở chế độ lặp sẽ có kinh nghiệm hạn chế số lượng và những sự tiềm tàng cao trong viễn cảnh này. Đây là điển hình để vô hiệu hóa mạng cục bộ hữu tuyến trong chế độ lặp.



Access Point trong chế độ lặp

3.1.1.3 CHẾ ĐỘ CẦU NỐI (BRIGDE MODE)

Trong chế độ cầu nối, APs hành động chính xác như là những chiếc cầu không dây. Trên thực tế, nó trở thành những chiếc cầu không dây trong khi cấu hình trong kiểu đó. Chỉ có một số lượng nhỏ AP có chức năng cầu nối, sự trang bị có ý nghĩa so với giá phải trả. Các máy khách không kết hợp với nhữngcầu nối, nhưng đúng hơn, những cầu nối sử dụng liên kết hai hoặc nhiều hơn đoạn mạng hữu tuyến với mạng không dây.



Access Point trong chế độ cầu nối

AP được coi như là một cái cổng bởi vì nó cho phép máy khách kết nối từ mạng 802.11 đến những mạng 802.3 hoặc 802.5. AP có sẵn với nhiều chọn lựa phần cứng và phần mềm khác nhau.

3.2 BẢO MẬT

Trước đây, cài đặt thiết bị không dây thường là một việc vô cùng phức tạp nhưng trong vài năm trở lại đây, các nhà sản xuất đã cố gắng đơn giản hoá quá trình này một cách đáng kể. Thực tế, nhiều sản phẩm sẽ hoạt động tốt khi bạn lấy chúng ra khỏi hộp, đọc hướng dẫn, cắm đúng cáp vào đúng đầu nối và khởi động lại thiết bị của bạn theo đúng trình tự. Phần lớn các nhà sản xuất phần cứng nối mạng không dây cung cấp các trình thuật sĩ "dễ làm theo" để giúp bạn hoàn thành quá trình cài đặt và rất nhiều nhà sản xuất cung cấp hỗ trợ kỹ thuật 24 giờ/ngày, 7 ngày/tuần.

Để quá trình cài đặt dễ dàng nhất có thể, hầu hết các nhà sản xuất khi xuất xưởng các sản phẩm của họ đều đặt tất cả các lựa chọn an ninh ở chế độ tắt. Vì vậy, các mạng gia đình khi được lắp đặt xong là hoàn toàn không được bảo vệ. ở mức tối thiểu, bạn cũng cần phải thay đổi tên mạng mặc định (SSID) và mật khẩu của người quản trị-cả hai thứ này được giới hacker biết rất rõ-và đặt chế độ an ninh ở mức cao nhất mà các sản phẩm hỗ trợ. Bảo vệ tương đương hữu tuyến (WEP) hiện là tính năng an ninh được sử dụng rộng rãi nhất trong các thiết bị gia đình. Nhưng tất cả các sản phẩm mới sẽ sớm hỗ trợ WPA (truy nhập được bảo vệ không dây) thay thế.

Hơn một năm trước, những nhà phân tích và truyền thông đã có văn bản và xuất bản có tính chất có hại đến mạng không dây, như là tính mã hóa có thể bị bẻ gãy và những kẻ xâm nhập AP để kết nối tới mạng của bạn. Chú ý những điều nguy hiểm của WLAN dẫn tới khả năng vài hãng sẽ chính thức cấm WLAN hoàn toàn, nhưng bất cứ một tổ chức nào cũng sử dụng máy tính xách tay, điều đó là nguy hiểm ví nó dễ dàng trở thành những trạm không dây dẫn tới sự rủi ro cho việc bảo mật.

Tuy nhiên, sự bảo mật – các hãng đã nhận ra là phải củng cố mạng không dây của họ với những lớp gần như bảo mật. Điều đó có nghĩa là chấp nhận những bảo mật thực tiễn của mạng hữu tuyến. Tầng này gần như bảo mật những địa chỉ của những thành phần trong mạng bởi khóa ngay từ vành đai của WLAN, bảo mật thông tin qua WLAN, và kiểm tra lưu lượng mạng.

Trên thực tế, Gartner đã phát thảo ra ba đề nghị “phải” cho mạng không dây WLAN :

1) Cài đặt một tường lửa quản lý trung tâm trên tất cả các mát tính xách tay gắn card mạng không dây hoặc tích hợp. Điều này chống lại các kết nối ad

hoc (kết nối ngang hàng) và sự tấn công từ internet khi người dùng kết nối tới những nhà cung cấp internet.

2) Thực hiện dò tìm sự xâm phạm đến WLAN để khám phá sự xâm nhập AP, các thiết bị ngoại vi kết nối đến một nhóm các AP và ngẫu nhiên kết hợp với những AP gần chúng và những Ap này sẽ được sử dụng bởi các công ty khác.

3) Bật tính năng mã hóa và chứng thực hổ trợ cho việc sử dụng WLAN.

3.2.1 CÁC GIẢI PHÁP BẢO MẬT

3.2.1.1 WEP

WEP là một phương tiện như điểm đầu mút của giải pháp bảo mật mạng không dây. Môi trường bảo vệ không dây chỉ với WEP là môi trường không bảo mật. Khi sử dụng WEP, không sử dụng các khóa của WEP liên quan tới SSID hoặc tới tổ chức. Tạo các khóa WEP rất khó khăn để nhớ. Trong nhiều trường hợp, khóa WEP có thể dễ dàng đoán ra khi nhìn SSID hoặc tên của tổ chức.

WEP là một giải pháp hiệu quả cho việc giảm sự rình mò lén lút. Bởi vì một kẻ xấu cố gắng truy cập, nhưng chỉ có thể nhìn thấy được mạng của bạn, sẽ không thấy được khóa WEP, mà một cá nhân sẽ bị ngăn chặn nếu truy cập mạng mà không có khóa WEP.

3.2.1.2 KÍCH THƯỚC Ô

Trong lệnh giảm bớt cơ hội nghe trộm, người quản trị mạng nên chắc chắn rằng những kích thước ô của những AP là thích hợp. Phần lớn những hacker tìm kiếm các vị trí rất nhỏ và khả năng bị mất năng lực trong mạng để tấn công. Vì lí do đó, điều quan trọng là AP sẽ không phát ra những tín hiệu dư thừa để chuyển những gói tin cho tổ chức (hoặc những vị trí không bảo mật) trừ khi rất cần thiết. Vài mức AP của doanh nghiệp cho phép cấu hình nguồn điện xuất, với những điều khiển có hiệu quả với kích cỡ của ô RF (Radio Frequency) xung quanh AP. Nếu kẻ nghe trộm gói dữ liệu không thể tìm ra mạng của bạn, lúc đó mạng của bạn sẽ không dễ bị tấn công.

Điều này có thể thúc giục những nhà quản trị luôn luôn sử dụng nguốn điện xuất thiết lập trên tất cả các thiết bị WLAN trong việc cố gắng đặt một thông lượng cực

đại và mức độ bao phủ, nhưng những cấu hình không nhìn thấy sẽ dẫn đến sự phí tổn bảo mật. Một AP phải có một kích cỡ ô để có thể điều khiển bởi lượng nguồn điện mà AP phát ra và lợi ích của việc sử dụng ăng ten. Nếu ô đó không phù hợp với điểm mà khách qua đường tìm thấy, hoặc sẽ truy cập một cách trơn tru, thì chỗ yếu của mạng đó không cần thiết để bị tấn công. Kích thước ô thích hợp nên được ghi lại cùng với các cấu hình của AP hoặc cầu nối cho mỗi phần của khu vực. Điều này có thể cần thiết để cài đặt hai AP với khích thước ô nhỏ hơn nhằm ngăn ngừa để có thể bảo mật những chỗ yếu trong vài trường hợp.

Cố gắng định vị những AP của bạn về phía trung tâm nhà bạn hay trung tâm của văn phòng chính. Điều này sẽ giảm thiểu sự rò rỉ tín hiệu ra ngoài vùng kiểm soát. Nếu bạn đang sử dụng ăng ten ngoài, hãy chọn kiểu đúng của ăng ten có thể hữu ích cho việc giảm thiểu sự rò rỉ tín hiệu. Tắt AP khi không sử dụng. Điều này sẽ giảm thiểu sự phơi bày cho các hacker và giảm gánh nặng cho việc quản lý mạng.

3.2.1.3 CHỨNG THỰC NGƯỜI DÙNG

Từ khi sự chứng thực người dùng là liên kết kém cỏi nhất của WLAN, và chuẩn 802.11 không chỉ định các phương pháp chứng thực người dùng, thì đó là điều cấp bách mà người quản trị mạng thực thi chứng thực người dùng cơ bản ngay khi có thể thực hiện được trong lúc đang cài đặt cơ sở hạ tầng WLAN. Chứng thực người dùng cơ bản nên thực hiện trên các lược đồ thiết bị độc lập như là tên và mật khẩu người dùng, card thông minh, các hệ thống mã thông báo cơ bản (token-based) hoặc vài kiểu bảo mật khác như là nhận diện người dùng, không qua phần cứng. Giải pháp bạn thực thi nên hỗ trợ chứng thực hai chiều giữa chứng thực máy chủ (như là RADIUS) và chứng thực máy khách không dây.

RADIUS trên thực tế là một chuẩn trong hệ thống chứng thực người dùng tốt nhất trong thị trường công nghệ thông tin. Những AP gửi các yêu cầu chứng thực người dùng tới các máy chủ RADIUS, có thể xây dựng cơ sở dữ liệu người dùng hay cấp phép cho các yêu cầu chứng thực thông qua người điều khiển trung tâm (Domain Controller – DC), như là máy chủ NDS, máy chủ AD (Active Directory), hoặc ngay cả LDAP.

Người quản trị của máy chủ RADIUS có thể rất đơn giản hoặc rất phức tạp, quyết định bởi sự bổ sung. Bởi vì các giải pháp bảo mật không dây dễ bị ảnh hưởng, vì thế nên cẩn trọng khi chọn giải pháp máy chủ RADIUS để chắc rằng người quản

trị mạng có thể quản trị nó hoặc có thể làm việc hiệu quả với một máy chủ RADIUS có sẵn.

3.2.2 NHU CẦU BẢO MẬT

Chọn một giải pháp bảo mật mà thích hợp với nhu cầu và ngân sách của công ty, cả cho hiện tại và mai sau. WLAN phổ biến có ích đến mức là một phần chắc chắn vì chúng có thể bổ sung thoải mái. Điều đó có nghĩa là WLAN đã bắt đầu bằng một AP và 5 máy khách rồi phát triển tới 15 AP và 300 máy khách. Những kỹ thuật bảo mật giống nhau làm việc chỉ tốt cho môt AP sẽ không thể chấp nhận được, hoặc khi bảo mật, cho 300 người dùng. Một tổ chức có thể sẽ tốn nhiều tiền cho các giải pháp bảo mật khi mà chúng phát triển nhanh chóng như là WLAN. Trong nhiều trường hợp, những tổ chức đã thật sự có sự bảo mật như là kiểm tra sự xâm nhập hệ thống, tường lửa, và máy chủ RADIUS.

3.2.3 SỬ DỤNG THÊM CÁC CÔNG CỤ BẢO MẬT

Nắm được sự thuận lợi của các công nghệ, như là VPN, tường lửa, kiểm tra sự xâm nhập hệ thống – Intrustion Detection Systems (IDS), những chuẩn và giao thức như là 802.1x và EAP, và chứng thức máy khách với RADIUS có thể giúp tạo nên các giải pháp bảo vệ cao và xa hơn chuẩn 802.11 yêu cầu. Chi phí và thời gian là phương tiện cho các giải pháp tốt hơn từ các giải pháp SOHO đến các giải pháp cho các doanh nghiệp lớn.

3.2.4 THEO DÕI VIỆC LỪA ĐẢO PHẦN CỨNG

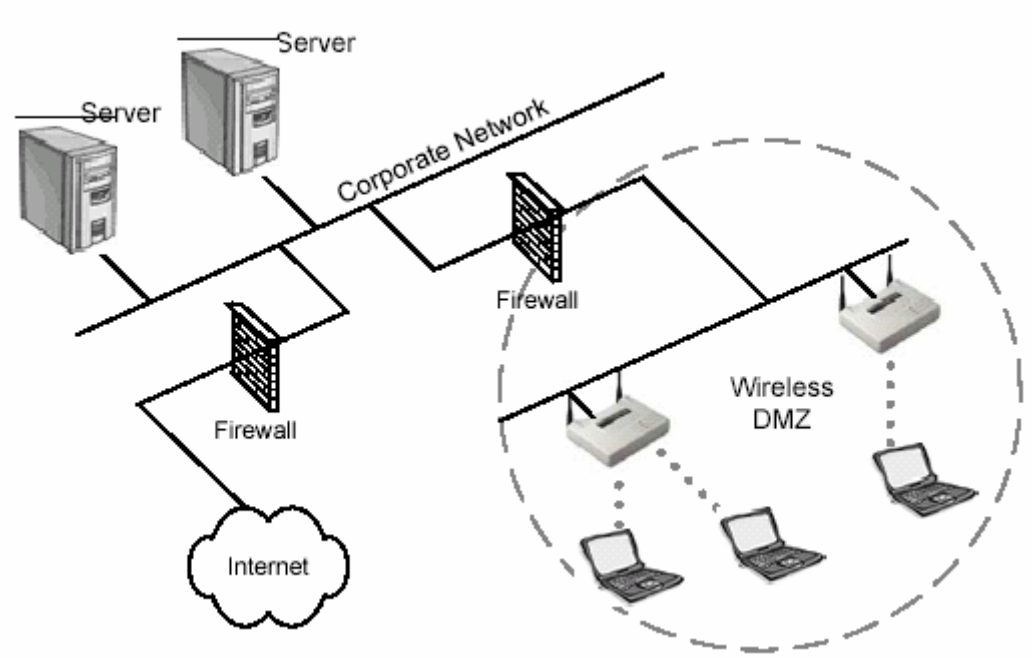
Phát hiện ra các AP lừa đảo, sự phát hiện ra các phiên của AP nên lập biểu nhưng không loan báo. Khám phá sự hoạt động và xóa các AP lừa đảo, sẽ giống như là loại bỏ hacker và cho phép người quản trị điều khiển duy trì mạng và bảo mật. Các kiểm định bảo mật nên được thực hiện cho các cấu hình không đúng của các AP mà các cấu hình này có thể gây nên sự nguy hiểm cho việc bảo mật. Tác vụ này có thể kết thúc trong khi theo dõi các AP lừa đảo như là một phần của một sự bảo mật bình thường. Các cấu hình hiện tại nên được so sánh đến các cấu hình trong quá khứ để có thể biết nếu người dùng hoặc hacker cấu hình lại AP. Việc ghi lại các truy cập nên là phương tiện và theo dõi cho mục đích của sự tìm ra bất cứ sự truy cập không chính đáng nào trên các đoạn mạng không dây. Kiểu theo dõi này có thể giúp tìm ra sự những thiết bị máy khách không dây đã mất hoặc bị lấy trộm.

3.2.5 SWITCH, KHÔNG PHẢI HUB

Một sự chỉ dẫn đơn giản khác là luôn luôn kết nối các AP với các Swicth thay vì các Hub. Các Hub là các thiết bị phát rộng, mỗi gói tin được nhận bởi một Hub sẽ được gửi cho tất cả các Hub khác. Nếu những AP đã kết nối đến Hub, thì mỗi gói tin đi qua đoạn mạng hữu tuyến sẽ bị phát tán. Chức năng này cho đem lại cho các hacker có được các thông tin như là mật mã và những địa chỉ IP.

3.2.6 DMZ KHÔNG DÂY

Một ý tưởng khác trong công cụ bảo mật cho các đoạn mạng WLAN là một tạo vùng phi quân sự không dây – Wireless Demilitarized zone (WDMZ). Tạo những WDMZ sử dụng tường lửa hoặc những bộ định tuyến (Router) có thể phụ thuộc vào chi phí của các công cụ. Những WDMZ là các công cụ thông thường trong sự triển khai sắp xếp trung bình – và lớn – của WLAN. Bởi vì các AP về cơ bản không có bảo mật và những thiết bị không đáng tin cậy, những AP này tách rời với các đoạn mạng khách bởi một thiết bị tường lửa.



DMZ không dây

3.2.7 PHẦN MỀM HỆ THỐNG VÀ NÂNG CẤP PHẦN MỀM

Nâng cấp phần mềm hệ thống và các bộ phận điều khiển (driver) trong các AP và các card không dây. Điều này luôn luôn đúng để sử dụng phần mềm hệ thống

mới nhất và các bộ phận điều khiển trong các AP và các card không dây. Những nhà sản xuất thường thường đưa ra những sữa chữa, bảo mật các lỗ hổng mạng, và bật những tính năng mới với những sự nâng cấp này.

3.2.8 CÁC THIẾT BỊ BẢO MẬT

Giống như gắn một cánh cửa vào một tòa nhà để tránh kẻ trộm, những doanh nghiệp phải điều khiển vành đai mạng của họ. Theo truyền thống của mạng hữu tuyến, tường lửa là lựa chọn hoàn hảo cho việc này. Tuy nhiên, WLAN giới thiệu một lựa chọn tốt hơn từ sự điều khiển tự nhiên của truyền sóng vô tuyến.

Với dữ liệu và những kết nối mạng phát rộng thông qua không khí và đi qua cửa sổ, tường, trần nhà và sàn nhà, vành đai của WLAN có thể gặp khó khăn để điều khiển cũng như xác định chúng. Tuy nhiên, nhiều doanh nghiệp có thể điều khiển vành đai của WLAN bởi những thiết bị bảo mật hoạt động như là điểm cuối của mạng.

Điều khiển vành đai của WLAN bắt đầu với việc triển khai các tường lửa cá nhân trên chiếc mỗi tính máy sách tay và cũng bao gồm triển khai những AP của các doanh nghiệp có sự bảo mật và khả năng quản lý cao. WLAN nên cách ly với mạng hữu tuyến để cho phép quản lý cụ thể và những chính sách bảo mật không ảnh hưởng đến mạng hữu tuyến.

Tất cả các AP phải hoàn toàn được khóa lại và cấu hình lại từ các thiết lập mặc đinh. SSIDs và những mật khẩu của AP phải thay đổi từ những tên mặc định ban đầu. Vài tổ chức được thành lập để thiết lập những kênh của thao tác cho mỗi AP để nhận dạng tất cả các kênh đã tắt khi có những hành động nghi ngờ.

3.2.9 BẢO MẬT THÔNG TIN – CHỨNG THỰC VÀ MÃ HÓA

Trong sự triển khai bảo mật WLAN, điều khó nhất cho người quản lý mạng và bảo mật là lựa chọn làm sao để bảo mật thông tin WLAN với nhiều loại chứng thực và mã hóa.

Giống như việc cài đặt khóa và những chìa khóa để điều khiển cho ai có thể mở nó, tầng tiếp theo của bảo mật WLAN là điều khiển người dùng có thể truy cập WLAN. Để cung cấp những chứng thực cơ bản, AP hỗ trợ địa chỉ lọc MAC, duy trì một danh sách những địa chỉ MAC hợp lệ. Trong khi điều này không mấy rõ ràng,

lọc địa chỉ MAC cung cấp những điều khiển cơ bản vượt lên những trạm có thể kết nối tới mạng của bạn.

Những tổ chức tin vào cách lọc địa chỉ mạng ở trên cho việc điều khiển cho phép chính họ tấn công đến kẻ đột nhập. Những doanh nghiệp lớn hơn với WLAN phức tạp có hàng trăm trạm và hàng tá AP yêu cầu việc điều khiển truy cập tinh xảo hơn thông qua dịch vụ hợp nhất chứng thực quay số từ xa – Remote authentication dial-in service (RADIUS). Cisco Systems, Microsoft, và Funk Software là những tập đoàn dẫn đầu trong lĩnh vực này.

Quan tâm đến những công nghệ tiêu chuẩn, IEEE giới thiệu chuẩn 802.1x cung cấp các điểm điều khiển truy cập đơn giản, xác nhập với việc máy chủ chứng thực. tuy nhiên, vài phiên bản của 802.1x đã có vài lỗ hổng. Cisco giới thiệu Giao thức chứng thực có thể mở rộng - LightWeight Extensible Authentication Protocol (LEAP) như là giải pháp chứng thực riêng dựa trên chuẩn 802.1x nhưng thêm vào những phần tử riêng của bảo mật. LEAP là một phần thêm của việc bảo mật, và Cisco chuyển từ LEAP sang Giao thức Chứng thực bảo vệ mở rộng – Protected Extensible Authentication Protocol (PEAP).

Sự mã hóa cung cấp lõi của bảo mật cho WLAN bằng cách bảo vệ dữ liệu mà giao với sóng không khí. Tuy nhiên, những lỗi của các chuẩn mã hóa và chứng thực vẫn chưa được bổ sung. Giao thức toàn bộ khóa biểu thị thời gian – Temporal Key Integrity Protocol (TKIP) được giới thiệu đến những địa chỉ thiếu sót của WEP với mỗi gói dữ liệu có khóa trộn lẫn, một thông báo kiểm tra toàn bộ và một bộ máy gán lại khóa.

Những công nghệ chuẩn mới và những giải pháp độc quyền giờ đây đã được giới thiệu cả hai kênh điều khiển mã hóa và chứng thực. Cisco, RSA Security, và Microsoft phát triển PEAP như là một trong những giải pháp độc quyền. Tuy nhiên, Microsoft và Cisco đã tách rời PEAP của họ để nổ lực phát triển và giới thiệu những phiên bản của giao thức này. Phiên bản PEAP của Microsoft không làm việc với các phiên bản PEAP của Cisco. Trong khi phiên bản PEAP của Microsoft gói gọn trong máy tính sách tay, thì phiên bản PEAP của Cisco đề nghị phải cài phần mềm cho máy khách và quản lý trên mỗi trạm người dùng trong WLAN.

Trong tháng 6 năm 2003, khối liên minh Wi-Fi Bảo Vệ truy cập Wi-Fi – Wi-Fi Protected Access (WPA) như là một chuẩn cấp thấp của chuẩn bảo mật tương lai

802.11i trong TKIP. Những đại lý tốt nhất loan báo rằng những AP đang hoạt động có thể được nâng cấp phần sụn từ sự hỗ trợ của WPA. Tuy nhiên, những AP mới sẽ cần một chuẩn 802.11i phiên bản cuối.

Mạng riêng ảo – Virtual Private Network (VPN) của những cổng vào WLAN cung cấp một chuẩn riêng khác về mã hóa và chứng thực. Tường lửa và các đại lý cổng vào VPN, như là Check Point và NetScreen Technologies, VPN về cơ bản là một đường hầm internet dùng để vận chuyển giao thức ngoại lai ngang qua mạng. Những giải pháp của VPN là dùng giao thức IPSec (IP Security) và không làm việc tốt với WLAN khi người dùng đi lang thang giữa AP hoặc tín hiệu có thể bị biến đổi và hạ thấp, và sẽ có nhiều người dùng chứng thực lại và bắt đầu một tác vụ mới.

Những đại lý, như là Bluesocket, ReefEdge, và Vernier Networks, cung cấp cổng vào WLAN bao gồm những tính năng thêm vào cho việc lang thang trên mạng và quản lý băng thông làm cho nó thích ứng với WLAN. Một phần khác của các đại lý VPN không dây, là bao gồm Fortress Technologies và Crantie Systems, cung cấp thêm những giải pháp bảo mật với Layer 2 được mã hóa.

Trong khi VPN cung cấp sự mã hóa và chứng thực mạnh mẽ, thì vấn đề hóc búa của quản lý máy khách là các phần mềm cài trên nó.

3.3 QUẢN LÝ

3.3.1 THEO DÕI WLAN

Như là một chiếc máy quay phim, theo dõi tất cả các hoạt động trong ngày, theo dõi nhận dạng những kẻ xâm nhập WLAN, dò tìm những kẻ xâm phạm và những mối đe dọa sắp đến, và gán các chính sách bảo mật cho WLAN (enforce policies).

Một ví dụ cho việc cần thiết phải theo dõi : AP được nâng cấp bởi WPA, AP phải được theo dõi để chắc rằng AP đó vẫn có cấu hình đúng.

Theo dõi WLAN của các doanh nghiệp cần phải rõ ràng rành mạch. Vài giải pháp đã được thực hiện cho các tổ chức nhỏ nhưng không đủ qui mô cho các doanh nghiệp lớn hơn với hàng tá hoặc hàng trăm công ty trên khắp thế giới. Những doanh nghiệp lớn yêu cầu những giải pháp có hiệu quả, có sự quản lý trung tâm và không đòi hỏi nhiều tài nguyên con người.

3.3.2 YÊU CẦU CHO QUẢN TRỊ WLAN

Bảo mật WLAN cũng giống như sự bảo mật của mạng hữu tuyến, dẫn đến sự quản lý đúng đắn cho việc quản lý WLAN. Những nhà quản lý mạng nên thật sự biết rõ những yêu cầu cơ bản của việc quản lý WLAN nhưng phải có những giải pháp chủ chốt trong việc chẩn đoán lỗi, cấu hình quản lý, tạo trương mục sử dụng mạng, thực hiện việc theo dõi, và gán các chính sách (policy).

Quản lý một mạng không dây nhỏ có khoảng 5 hoặc 10 AP có thể dễ dàng hoàn thành với việc xây dựng chức năng trong những AP. Tuy nhiên, quản lý một mạng không dây lớn hơn khoảng từ 12 đến hàng trăm AP trong phạm vi trường sở hoặc trong phạm vi nhiều khu vực của cả nước yêu cầu cần phải có thêm những giải pháp để có thể hỗ trợ, phân bổ một cách tự nhiên trong mạng.

Quản lý những mạng không dây sẽ cảm thấy hài lòng với sự kết hợp của các giải pháp cung cấp cơ sở hạ tầng cho mạng không dây, như là Cisco System và Symbol Technologies, nhiều công ty đã bắt đầu, như là Aruba Networks và Trapeze Networks. Tuy nhiên, hệ thống quản lý mạng không dây tốt nhất là tính đến sự giới hạn bởi những khả năng để chỉ quản lý AP sản xuất bởi đại lý cung cấp của hệ thống WLAN.

3.3.3 QUẢN LÝ CẤU HÌNH

Quản lý các cấu hình của mạng không dây thông qua tất cả các AP và các trạm thường đưa ra những thách thức lớn cho việc quản lý mạng. Trong mức độ khó nhất, mỗi thiết bị phải có quan hệ chắc chắn đến các thiết lập thích hợp cho việc bảo mật, sự thực thi và những chính sách đúng đắn. Có nhiều sự đề nghị để quản lý mạng WLAN, như là Cisco’s Wireless LAN Solution Engine (WLSE) hoặc Symbol’s Wireless Switch System, có thể quản lý từ xa các cấu hình AP và áp dụng nhiều các cấu hình tạm thời đến các đoạn mạng khác nhau của một mạng không dây.

Quản lý các cấu hình người dùng gặp phải những thách thức lớn hơn bởi vì những người quản lý mạng có thể không hướng dẫn truy cập người dùng tới tất cả các trạm, và một số ít trạm có thể là những dự án tốn nhiều thời gian.

Theo dõi tốc độ xử lý của máy và cấu hình phần dây phụ để chắc rằng những AP và những trạm còn lại vẫn trong trạng thái cấu hình xác định. Sự tràn năng lượng

hoặc ngưng hoạt động có thể làm cho AP tự động xác lập lại các thiết lập mặc định. Các nhân viên có thể thay đổi những thiết lập cho thiết bị để có thể truy cập mạng trở lại. Phân tích lưu lượng của mạng không dây để nhận dạng các mạng cấu hình sai.

3.3.4 CHẨN ĐOÁN LỖI

Các nhân viên và những người dùng có thể có lợi ích từ mạng không dây chỉ khi nó hoạt động. Đáp ứng các cuộc gọi hỗ trợ có thể là một thao tác làm át hẳn phạm vi hoạt động của IT (Information Technology) để đáp ứng sự hỗ trợ mạng không dây trong các vị trí điều khiển.

Những thiết bị quản lý mạng không dây, được cung cấp bởi Cisco và Symbol, có thể thăm dò những thiết bị mạng từ mạng hữu tuyến để quan sát những nét đặc trưng và thuộc tính của các thiết bị đó, rồi báo cho các nhân viên các kết quả thu được. Trong một mức cao hơn của việc chuẩn đoán lỗi : việc theo dõi tốc độ xử lý của máy, khảo sát những thiết bị WLAN, phân tích những kiểu dáng lưu lượng và báo cáo những thiết bị lỗi và những tạp nhiễu quá mức trong không khí dẫn đến làm tê liệt mạng không dây.

3.3.5 THEO DÕI SỰ THỰC THI

Sau lần đầu tiên chắc rằng mạng đã hoạt động, những người quản lý mạng phải theo dõi và phân tích việc hoạt động của một WLAN bảo đảm mạng này hoạt động tốt nhất. Những công cụ quản lý WLAN, như là Cisco WLSE, có thể cung cấp vài thông tin thực thi từ mạng hữu tuyến. Thêm vào đó, theo dõi tốc độ xử lý máy tính sẽ xác định được những thực thi phát sinh mà có thể chỉ thấy được từ không khí, như là tín hiệu bị hạ thấp từ sự chồng lấp kênh, sự can thiệp tầng số từ những thiết bị có chuẩn 802.1x, và lượng quá tải của một AP.

3.3.6 TRƯƠNG MỤC – CÁCH SỬ DỤNG MẠNG

Nhiều như những việc chẩn đoán lỗi và kiểm tra thực thi, trương mục cho việc sử dụng mạng là thực hiện việc nối gần các nền tảng quản lý và theo dõi 24x7. Những nền tảng quản lý mạng từ những nền tảng giống của Cisco và Symbol kết nối các trạm của WLAN tới những ứng dụng khác nhau trên mạng cho mục đích tiến hành tạo trương mục.

Kiểm tra lưu lượng mạng WLAN thông qua sóng không khí cho phép những người quản lý mạng kiểm tra việc sử dụng mạng cơ bản trên công suất cao nhất của mỗi AP và băng thông cao nhất – những trạm chi phối và những AP. Điều này cho phép những người quản lý mạng có sơ đồ cho việc tăng công suất khi cần thiết và đối phó với những người dùng riêng lẻ lạm dụng WLAN để tải xuống những tập tin không liên quan đến công việc của công ty, như là MP3,…

3.3.7 GÁN CHÍNH SÁCH (POLICY)

Sự bằng lòng cho các chính sách đi qua WLAN ảnh hưởng đến hầu hết mỗi khía cạnh của việc quản lý và bảo mật mạng. Các chính sách khống chế các cấu hình, việc sử dụng, các thiết lập bảo mật, và những giới hạn thực thi của WLAN. Tuy nhiên, các chính sách bảo mật và quản lý sẽ vô ích khi mạng đã đặt sự theo dõi cho các chính sách được ưng thuận và tổ chức có những bước hoạt động để gán các chính sách.

Theo dõi tốc độ xử lý máy tính, theo dõi 24x7 của lưu lượng không dây phát sinh các vi phạm chính sách sau :

- Những kẻ lừa đảo WLAN – bao gồm cả phần mềm cho các AP.
- Không có chứng thực hoặc mã hóa.
- Những trạm không được phép.
- Các mạng ngang hàng.
- Các SSID mặc định hoặc không thích hợp.
- Những AP và những trạm trung tâm trên các kênh không được phép.
- Lưu lượng trong thời gian không phải cao điểm.
- Các đại lý phần cứng không được cấp phép.
- Tỷ lệ dữ liệu không cho phép.
- Những giới hạn thực thi biểu thị sức ổn định của WLAN.

3.4 TỔNG KẾT

Với sự bùng nổ của công nghệ không dây, vai trò của những nhà sản xuất phần cứng và các tổ chức như là FCC, IEEE, WECA, WLANA sẽ tăng thêm phần quan trọng để giải quyết các giải pháp của mạng không dây. Những quy định được đặt vào các tổ chức điều tiết như là FCC với những chuẩn, và những tổ chức như là IEEE, WLANA và WECA sẽ là tiêu điểm của kỹ nghệ sản xuất mạng không dây.

WLAN sẽ cải tiến tốt hơn trong giới hạn của tốc độ, sự tiện lợi, và bảo mật. Sự chứng thực và các kỹ thuật PKI chỉ là sự bắt đầu cho việc hạ giá WLAN để bạn có thể điều khiển truy cập tới bất cứ tài nguyên nào trong mạng.

Một phần quan trọng nhất, là phải ngăn ngừa sự nguy hiểm tới mạng của bạn trước khi nó xảy ra. Tránh xa các cặp mắt nghi ngờ và phải chắc chắn rằng thông báo cho những người dùng trong mạng biết rằng hãy cảnh giác với những người truy cập mạng và những điều luật thông qua các chính sách để chỉ những người dùng được phép mới có thể truy cập tới các tài nguyên trong mạng. Nếu bạn kiểm tra và thấy rằng tất cả đã kết nối, bạn phải chắc chắn rằng bạn có thể cung cấp đủ sự bảo mật một cách tận tâm cho mạng của bạn.

Công nghệ không dây ra đời đã làm thay đổi diện mạo của nền công nghệ thông tin trên toàn thế giới. Nó mang đến cho thế giới một cách nhìn mới về các công nghệ tiên tiến. Công nghệ không dây đã trãi qua một quá trình dài từ khi nó là ý tưởng của quân đội. Sự ưa chuộng và mức độ của công nghệ sử dụng mạng không dây vẫn tiếp tục mọc lên với tỷ lệ cao đến không ngờ. Sản xuất và tạo ra vô số giải pháp cho những mạng không dây là cần thiết. Sự thuận tiện, phổ biến, có lợi và giá cả của các phần cứng của mạng không dây cung cấp cho chúng ta nhiều lựa chọn khác nhau. bạn đã sẵn sàng gia nhập vào đội ngũ những người chuyển sang nối mạng không dây. Bạn sẽ thấy rằng một thế giới không có dây thì ít rối rắm phức tạp hơn và việc sử dụng mạng không dây trong gia đình của bạn sẽ được cải thiện đáng kể.