SAFE:
무선 LAN 보안 심층 분석

저자

본 백서의 주 저자는 Sean Convery (CCIE #4232)와 Darrin Miller (CCIE #6447)입니다. 본 백서의 상당 부분을 기고한 Mark Doering, Pej Roshan, Sri Sundaralingam는 미국 캘리포니아주 산 호세에 위치한 시스코 지사에서 reference implementation을 담당한 주요 기술자들입니다. 이 세 사람은 무선 LAN, VPN, 보안 문제 등을 주로 담당하는 네트워크 전문가들입니다.

요약

본 백서는 SAFE 블루프린트의 구성 요소를 활용하여 네트워크에서 WLAN(wireless LAN) 보안을 설계 및 구현하는데 관심이 있는 분들을 위해 최상의 업무 방식에 관한 정보를 알려줍니다. 모든 SAFE 백서는 SAFE 웹 사이트인 http://www.cisco.com/go/safe에 마련되어 있습니다. 이 백서들은 네트워크 보안과 VPN(virtual-private-network) 설계에 대한 최상의 업무 방식에 관한 정보를 알려주기 위해 마련되었습니다. 보안 설계와 관련된 주요 문서인 "SAFE Enterprise"나 "SAFE Small, Midsize and Remote-User Networks"를 읽지 않고도 본 문서를 읽는데 지장은 없지만, 먼저 그 문서들을 읽은 다음에 본 문서를 읽는 것이 바람직합니다. 본 백서는 전반적인 보안 설계 차원에서, WLAN 구현에 관한 기본 내용을 제시합니다. SAFE는 시스템 기반의 보안 및 VPN 설계에 대한 일종의 접근 방식으로서, 전반적인 설계 목표에 초점을 맞추면서 그러한 목표를 구체적인 시스템 구성과 토폴로지로 구현합니다. 무선 테크놀러지의 맥락에서, 전반적인 WLAN 설계를 결정할 때 이동성이나 QoS와 같은 네트워크 설계 요소들도 고려하는 것이 좋습니다. SAFE는 시스코 제품과 시스코의 파트너들의 제품에 기초한 것입니다.

본 문서에서는 먼저 아키텍처 개요를 소개한 다음, 고려할 구체적인 설계를 상세하게 설명합니다. 본 문서는 두 가지 주요 설계 변형(design variations)을 중심으로 내용을 설명하므로, 먼저 이 두 가지 주요 설계 형태를 일반적인 의미로 설명한 다음에 SAFE에 적용합니다. 다음과 같은 설계 형태를 상세하게 설명합니다.

- 대형 네트워크 WLAN 설계
- 중형 네트워크 WLAN 설계
- 소형 네트워크 WLAN 설계
- 원격 사용자 WLAN 설계

각 설계에는 WLAN 테크놀러지의 서로 다른 양상들을 다루는 여러 모듈들이 있을 수 있습니다. 모듈의 개념은 SAFE 보안 백서들에서 다룹니다.

구체적인 설계 형태들을 설명한 다음, 부록 A에서는 SAFE 무선 테크놀러지 검증 랩을 상세히 설명하고 구성 스냅샷도 함께 소개합니다. 부록 B는 WLAN에 대한 기본 지식입니다. 기본적인 WLAN 개념을 잘 모른다면, 본 문서의 나머지 부분을 읽기 전에 이 부분을 읽어야 합니다.

본 문서의 대상 독자

본 문서는 내용 상 기술적이기는 하지만, 독자의 관심 수준에 따라 심도 있게 읽을 수도 있고 그렇지 않을 수도 있습니다. 예를 들어, 네트워크 관리자들은 각 분야의 개요 부분만 읽어도 보안 설계 전략과 WLAN 네트워크 관련 고려 사항을 개괄적으로 충분히 파악할 수 있습니다. 네트워크 엔지니어나 설계자는 본 문서 전체를 독파하여 설계 정보와 위험 요소 분석과 관련된 세부 사항을 알아낼 수 있으며, 관련된 장치들에 대한 실제 시스템 구성 스냅샷까지 마련되어 있습니다. 본 문서가 매우 다양한 WLAN 배치 형태를 다루고 있으므로, 먼저 개요 부분을 읽은 다음에 곧바로 배치하고자 하는 WLAN 유형으로 넘어갈 수 있습니다.

유의 사항

본 문서는 이미 보안 정책을 시행하고 있는 경우를 전제로 한 내용입니다. WLAN 또는 그 외의 다른 네트워킹 테크놀러지를 관련된 보안 정책을 사용하지 않고 배치하는 것은 바람직하지 않습니다. 본 문서에서 네트워크 보안 기반에 대해 언급하기는 하지만, 자세히 설명하지는 않습니다. 본 문서에서 언급하는 보안은 항상 WLAN과 관계가 있습니다.

본 문서의 지침에 따른다고 해서 보안상 안전한 환경이 보장되는 것은 아니며, 모든 침입을 막을 수 있다고 보장할 수도 없습니다. 요즘과 같은 무선 네트워크의 경우에는 특히 그러합니다. 본 문서에서 설명하는 것처럼, 무선 LAN에서 완벽한 보안을 구현할 수 있는 방법은 없습니다. 네트워크에 무선 LAN을 배치하면 유선으로만 연결된 네트워크에 비해 보안 위험이 증가한다는 점을 기억해야 합니다. 본 백서에서는 그러한 위험에 대처하는 방법을 설명하지만, 그런 위험을 완전히 없애는 것은 불가능하다는 점을 잊지 마십시오. 많은 조직체들은 무선 테크놀러지로 인해 발생하게 되는 잠재적인 보안 위험에도 불구하고 무선 테크놀러지를 사용하기로 결정했습니다. 이러한 조직체들은 무선 네트워크를 이용함으로써 대두될 수 있는 취약한 보안 문제보다는 생산성의 이득이 더욱 중요한 것으로 간주합니다. 본 논문에서는 그런 조직체들이 염려하는 점과 WLAN을 처음 도입하는데 신중한 입장인 보안 공동체들이 염려하는 점들을 다룹니다.

본 문서에는 무선 보안 문제으이 다양한 내용에 관한 많은 양의 세부 정보가 담겨있기는 하지만, 그렇다고 모든 내용을 설명하는 것은 아닙니다. 특히, 본 문서는 무선 브리지, PDA(personal digital assistants), 비 802.11 기반 WLAN 테크놀러지 등에 대해서는 다루지 않습니다. 뿐만 아니라, 본 문서에서는 보안과 관련이 없는 일반적인 WLAN 배치와 설계 문제에 대해서는 구체적인 최상의 업무 방식을 알려주지 않습니다.

SAFE를 검증하는 동안, 실제 제품들은 본 문서에서 설명한 것과 정확하게 일치하는 네트워크 구현 형태로 구성되었습니다. 랩에서 나온 특정한 시스템 구성 스냅샷은 부록 A, "검증 랩"에 포함되어 있습니다.

본 문서 전체에서 "해커"라는 용어는 악의적인 의도로 네트워크 리소스를 권한없이 액세스하려고 하는 사람을 가리킵니다. 이런 종류의 사람들을 가리키는데는 일반적으로 "크래커"라는 용어가 더 정확한 단어로 인정되지만, 여기서는 읽기 쉽도록 해커로 통일하였습니다.

아키텍처 개요

설계 기반

SAFE 무선 테크놀러지는 요즘의 네트워크에서 요구하는 기능 조건들을 가능한한 가장 가깝게 에뮬레이션합니다. 구현 형태 결정은 필요한 네트워크 기능에 따라 차이가 있습니다. 하지만, 우선 순위대로 열거된 다음 설계 목표를 기준으로 결정을 내렸습니다.

- 정책에 기초한 보안 및 공격 대처 방법
- 유선 네트워크 리소스를 사용하도록 무선 네트워크를 인증하고 권한을 부여하는 것
- 무선 데이터 기밀성
- AP(Access-point) 관리
- 네트워크 리소스 사용자 인증
- 고가용성을 위한 옵션 (대기업체만 해당됨)

무엇보다도, SAFE 무선 테크놀러지는 주로 유선 LAN을 사용하는 사람들에게 대체 연결 옵션이 되어야 합니다. 대체 연결 옵션이므로, 유선 네트워크에서 이용할 수 있는 모든 서비스와 호스트를 액세스해야 하는 것은 아니지만, 조직체의 보안 정책이 허용하는 한 그렇게 하려고 노력해야 합니다. SAFE 무선 테크놀러지는 기존의 유선 LAN의 특징을 가능한한 그대로 유지해야 한다는 점을 인정하면서 가능한한 안전하게 그러한 액세스를 제공해야 합니다. 이것은 보기보다 쉽지 않습니다. 끝으로, SAFE 무선 테크놀러지는 SAFE 보안 아키텍처에 기초한 기존의 네트워크 설계와 통합이 되어야 합니다.

SAFE 무선 LAN 기본 원칙

무선 네트워크는 공격 대상이다

무선 네트워크는 요즘 해커들이 가장 좋아하는 공격 대상 중의 하나가 되었습니다. 요즘의 조직체들은 대부분의 IT 부서들이 따라잡을 수 없을 정도로 빠른 속도로 무선 테크놀러지를 배치하고 있습니다. 이런 빠른 배치는 부분적으로는 저렴한 장치 비용, 손쉬운 배치 방법, 그리고 큰 생산성 이득 덕분입니다. 하지만, WLAN 장치들은 출하될 때 모든 보안 기능을 사용하지 않도록 설정되기 때문에, 이처럼 폭넓게 배치되면서 해커계의 관심을 끌게 되었습니다. 현재 여러 웹 사이트들에서 자유롭게 이용할 수 있는 전국의 무선 연결망 목록을 문서로 정리하기 시작했습니다. 대부분의 해커들이 이러한 연결을 인터넷을 공짜로 이용하거나 자신의 신분을 감추는 수단으로 사용하고 있기는 하지만, 소수의 사람들은 이 상황을 다른 방법으로는 인터넷에서 공격하기 어려웠던 네트워크로 침입해 들어갈 수 있는 기회로 봅니다. 유선 네트워크와는 달리, 무선 네트워크는 허공으로 데이터를 전송하며 일반적으로 조직체의 물리적인 경계선 너머로 뻗어 있기 때문입니다. 특히, 강력한 지향성 안테나를 사용하는 경우, WLAN은 설계된 건물들을 벗어난 먼 곳까지 도달할 수 있습니다. 이 시나리오에서는 기존의 물리적인 보안 제어 기능이 무력화되는 환경이 만들어집니다. 무선 주파수 범위 내의 모든 사람이 패킷을 볼 수 있기 때문입니다. 예를 들어, LINUX 랩탑 컴퓨터와 TCPDUMP와 같은 프로그램만 있으면, 누구든지 이 문제점을 이용하여 임의의 WLAN 상에서 돌아다니는 모든 패킷을 받아서 저장할 수 있습니다.
또한 무선 통신에 끼어드는 것도 쉽습니다. 간단한 재밍 트랜스미터만 있으면 통신을 불가능하게 만들 수 있습니다. 예를 들어, AP를 액세스 요청으로 계속 두들기면, 그 요청이 성공하든 하지 않든 간에, 결국 그 AP의 가용 무선 주파수대가 고갈되어 네트워크가 다운되어 버립니다. 동일한 주파수대로 제공되는 다른 무선 서비스로 인해 WLAN 테크놀러지의 주파수대와 대역폭이 줄어들 수도 있습니다. 현재 WLAN 장치와 동일한 무선 주파수를 사용하는 많은 테크놀러지 중의 하나는 전화기와 다른 정보 기기 사이에서 통신을 하는데 사용되는 "블루투스" 테크놀러지입니다. 이러한 의도적이거나 무의도적인 DoS(denial-of-service) 공격으로 인해 WLAN 장치를 사용할 수 없게 될 수 있습니다.

일반적인 보안 상의 허점

대부분의 WLAN 장치들은 DSSS(direct sequencing spread spectrum) 통신 방식을 사용합니다. 대부분의 WLAN 장치들은 표준에 일치하기 때문에, 공격자에게는 동일한 스프레딩 시퀀스로 튜닝을 할 수 있는 WLAN 카드가 있다고 가정해야 합니다. 따라서, DSSS 테크놀러지만으로는 개인 정보 보호 기능이나 인증 기능이 될 수 없습니다.

WLAN 액세스 포인트는 버닝 기법으로 카드에 인쇄된 고유한 MAC(Media Access Control) 주소를 기준으로 제조된 모든 무선 카드를 식별할 수 있습니다. 일부 WLAN에서는 무선 서비스를 사용하려면 먼저 카드를 등록하게 합니다. 그 다음에 액세스 포인트는 사용자를 기준으로 카드를 식별합니다. 하지만, 이 시나리오는 복잡합니다. 모든 액세스 포인트가 이 목록을 액세스할 수 있어야 하기 때문입니다. 설사 그렇게 구현을 한다 해도, 펌웨어를 로드할 수 있지만 내장된 MAC 주소를 사용하지 않고 임의로 선택되거나 의도적으로 스푸핑한 주소를 사용하는 해커를 당해낼 수는 없습니다. 해커는 이 스푸핑한 주소를 사용하여 네트워크 트래픽을 끼워 넣거나 정당한 사용자를 스푸핑하려고 시도할 수 있습니다.

애드혹(Ad Hoc) 모드 대 인프라 모드

조직체에서 배치한 대부분의 WLAN은 "인프라"라고 하는 모드로 작동합니다. 이 모드에서는, 모든 무선 클라이언트가 모든 통신에 대해 AP를 이용하여 연결할 수 있습니다. 하지만, 독립적인 피어 투 피어 네트워크가 되도록 WLAN 테크놀러지를 배치할 수도 있습니다. 이 방식을 흔히 애드혹 WLAN이라고 합니다. 애드혹 WLAN에서는, 호환이 되는 WLAN 어댑터를 장착하고 있고 서로 연결 범위 내에 존재하는 랩탑 컴퓨터나 데스크탑 컴퓨터는 AP를 사용하지 않고 직접 파일을 공유할 수 있습니다.

연결 가능 범위는 WLAN 시스템의 종류에 따라 차이가 있습니다. 802.11b WLAN 카드를 내장하고 있는 랩탑 컴퓨터와 데스크탑 컴퓨터는 서로의 거리가 최소한 500 피트 이내이면 애드혹 네트워크를 만들 수 있습니다.

애드혹 WLAN이 보안에 미치는 영향은 상당합니다. PC 제조업체들이 기본 부품으로 내장하는 카드를 포함하여, 많은 무선 카드는 애드혹 모드를 사용하도록 설정된 상태로 출하됩니다. 역시 애드혹 모드를 사용하도록 구성이 된 해커는 이러한 카드를 사용하여 PC에 즉시 연결하여 권한없이 액세스하려고 시도할 수 있습니다. 이러한 공격에 대처하는 것이 본 백서의 요점이지만, 모든 WLAN 장치가 따라야 하는 몇 가지 기본적인 제안이 있습니다. 최소한, 다음과 같이 해야 합니다.

- 액세스 포인트 보안 관련 제안:
  - 관리 인터페이스에 대한 사용자 인증 기능을 사용하십시오.
  - SNMP(Simple Network Management Protocol)에 대해 강력한 공동체 문자열을 선택하고 자주 변경하십시오.
  - 관리 인프라에서 허용한다면 SNMP Read Only를 사용하는 것을 고려하십시오.
  - 제조업체에서 제공하는 보안이 확실하지 않고 꼭 필요한 것이 아닌 관리 프로토콜은 사용하지 못하게 설정하십시오.
  - 네트워크 관리 트래픽을 전용 유선 서브넷으로 제한하십시오.
  - 가능한 경우 모든 관리 트래픽을 암호화하십시오.
  - 가능하다면 무선 프레임 암호화 기능을 사용하도록 설정하십시오.
- 클라이언트 보안 관련 제안:
  - 애드혹 모드를 사용하지 않도록 설정하십시오.
  - 가능하다면 무선 프레임 암호화 기능을 사용하도록 설정하십시오.

무선 네트워크는 무기이다

나쁜 마음을 먹은 해커의 수중에 AP가 들어가면 네트워크 리소스를 공격하는데 멋진 도구가 될 수 있습니다. 가장 큰 위험은 권한없이 빌딩을 액세스한 다음 AP를 네트워크 안에 설치하는 것입니다. 일반적으로 사용자는 자기 뒤에 유효한 액세스 뱃지를 "붙이거나" 다른 어떤 방법으로 게스트 뱃지를 받아서 빌딩 액세스 권한을 따냅니다. AP는 비교적 크기가 작고 전세계의 많은 전자 부품점에서 구입할 수 있기 때문에, 해커가 AP를 수중에 넣고 교묘하게 설치하는 것은 쉬운 일입니다. AP를 회의실 테이블 밑에 붙여 놓고 가동 중인 네트워크에 연결시켜 놓으면 해커가 주차장에 주차된 비교적 안전한 자동차 안에서 네트워크로 침입할 수 있습니다. MITM(man-in-the-middle) 공격의 가능성도 고려해 보십시오. 해커는 믿을 수 있는 AP인것처럼 가장할 수 있는 장치를 사용하여 무선 프레임이 자기 장치를 지나갈 때 조작할 수 있습니다.

정책과 프로시저는 조직체가 이러한 위협에 대응하는데 사용하는 두 가지 주요 무기입니다. 정책의 관점에서 보면, 조직체가 전반적인 보안 정책 뿐만 아니라 완벽한 무선 네트워크 정책도 갖추는 것이 좋습니다. 이 무선 정책은 최소한 비 IT 지원 AP가 네트워크에 연결하는 것을 허용하지 말아야 합니다. 프로시저 측면에서 보면, IT 부서가 사무실 공간을 정기적으로 검색하여 해커 AP가 있는지 확인해야 합니다. 이러한 검색에는 물리적인 검색과 무선 검색이 모두 포함됩니다. 특정한 지역에 무선 AP가 존재하는지 찾아내도록 설계된 툴을 마련하고 있는 업체들도 몇몇 있습니다.

구현 방식 측면에서 보면, 현재 많은 이더넷 스위치들은 연결 클라이언트의 MAC 주소를 기초로 특정한 포트 액세스를 제한할 수 있는 기능을 갖추고 있습니다. 이러한 제어 기능들은 포트에 연결하는 첫번째 MAC 주소를 알아낸 다음 그 이후의 MAC 주소는 연결하지 못하게 하도록 설정할 수 있습니다. 또한 지정된 수 이상의 MAC 주소가 연결하지 못하게 하는 방식으로 제어 기능을 설정할 수도 있습니다. 이러한 기능들은 모두 해커 AP 문제에 대처하는데 도움이 됩니다. 하지만, 이런 기능을 사용하려면 시스템 관리 측면에서 상당한 출혈이 생긴다는 점을 기억해야 합니다. 대기업체에서 MAC 주소 테이블을 관리하는 것은 그 자체로도 정규 업무 중의 하나가 될 수 있습니다. 또한, 회의실의 경우 각 네트워크 포트에 어떤 종류의 시스템을 연결하게 될지 알기 어렵습니다.

회의실은 AP를 수중에 넣은 해커의 타겟이 될 가능성이 높기 때문에, 모든 회의실에서 유선 네트워크를 액세스하지 못하게 하는 것이 도움이 될 수도 있습니다. 하지만, 회의실에서 네트워크에 무선으로 액세스하게 하는 것이 기업체들이 현재 무선 LAN 테크놀러지를 배치하기로 선택하는 주된 이유 중의 하나입니다.

802.11b의 미흡한 보안 기능

본 문서의 기초 지식 부분에서 설명했듯이, 802.11b는 현재 가장 널리 배치된 WLAN 테크놀러지입니다. 유감스럽게도, 802.11b의 보안 기능의 기초는 WEP(Wired Equivalent Privacy)라고 하는 프레임 암호화 프로토콜에 따른 것입니다. 여기서는 WEP의 문제점을 어느 정도 자세히 설명할 것입니다. 그리고 본 문서의 나머지의 상당 부분에서는 이러한 문제의 해결책을 제시합니다.

WEP (Wired Equivalent Privacy)

802.11 표준은 WLAN 액세스 포인트와 NIC(network interface cards) 사이의 공중을 통한 전송을 보호하는 간단한 메커니즘으로 WEP를 정의합니다. 데이터 링크 레이어에서 작동하는 WEP는 통신을 하고 있는 모든 사람이 동일한 비밀 키를 공유하게 합니다. 표준이 개발된 시기에 적용되던 미국 수출 규제 조항을 지키기 위하여, IEEE 802.11b는 40 비트 암호화 키를 요구했습니다. 물론, 지금은 많은 업체들이 선택적인 128 비트 표준을 지원합니다. 하지만, 인터넷 상에서 쉽게 구할 수 있는 툴을 사용하면 40 비트 형태 WEP이든 128 비트 형태의 WEP이든 쉽게 해킹할 수 있습니다. 본 백서를 기록하고 있는 현재, 복잡한 네트워크에서, 겨우 15분 정도면 128 비트 정적 WEP 키를 알아낼 수 있습니다. 이러한 공격에 대해서는 아래에서 좀더 자세히 설명합니다.

기초 지식 부분에서 언급한 것처럼, WEP는 RSADSI(RSA Data Security, Inc.)의 Ron Rivest가 암호화를 위하여 창안한 RC4 스트림 암호 기법을 사용합니다. RC4 암호화 알고리즘은 가변 길이 키를 지원하는 대칭형 스트림 암호입니다. IEEE 802.11 표준은 WEP에서 RC4 알고리즘과 키를 사용하는 것에 대해 설명하지만, 구체적인 키 배포 방식은 규정하지 않습니다. 자동화된 키 배포 방식이 없으면, 어떤 암호화 프로토콜이든 키 입력, escrow, 관리 등과 관련하여 사람이 실수할 가능성 때문에 구현에 문제가 생기게 됩니다. 본 문서 뒷 부분에서 설명하는 것처럼, IEEE에서 승인한 802.1X가 WLAN 관련 업체들이 키 배포 문제를 해결할 가능성이 있는 방법으로 인정받고 있습니다.

WEP가 관련된 대부분의 문제들의 핵심은 초기화 벡터입니다. IV(initialization vector)는 일반적인 텍스트로 전송되어 802.11 헤더에 들어가기 때문에, WLAN을 슬쩍 들여다보는 사람은 누구나 볼 수 있습니다. 길이가 24 비트인 IV의 가능한 값의 범위는 16,777,216입니다. 캘리포니아 주립 대학 버클리 분교의 한 논문에서는 암호화된 패킷에 동일한 키를 넣어서 동일한 IV를 사용하면(IVcollision이라고 함), 해커가 데이터 프레임을 잡아서 데이터 뿐만 아니라 네트워크에 관한 정보도 뽑아낼 수 있다는 사실을 밝혔습니다. 더 자세한 내용은, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html에 있는 논문을 참조하십시오. 작년에, 캘리포니아 주립 대학교 버클리 분교, 메릴랜드 주립 대학교, 시스코 시스템즈 등의 암호 분석가들은 IEEE 802.11 WLAN 표준의 인증 및 WEP 암호화 기법에 숨어 있는 약점을 보고했습니다. 이 연구가들은 이러한 결점을 완화시킬 수 있는 정교한 키 관리 솔루션이 필요하다고 주장했습니다. 메릴랜드 주립 대학교의 논문은 http://www.cs.umd.edu/~waa/wireless.pdf에서 볼 수 있습니다.

최근에, 암호 해독가인 Fluhrer, Mantin, Shamir 등은 RC4 키 스케줄링 알고리즘에 숨어 있는 결점을 찾아내었습니다. 즉, WEP에 구현된 RC4는 24 비트 IV를 사용하기로 선택하고 암호화 키를 동적으로 로테이션시키지 않으므로, 이 결점을 이용하여 WEP를 사용하는 802.11 프레임을 해독하는데 실제로 응용할 수 있는 것으로 증명되었습니다. 본 논문에서 설명하는 공격은 RC4가 생성할 수 있는 많은 종류의 약한 IV에 초점을 맞추고 IV의 특정한 패턴을 사용하여 키를 깨뜨리는 방법을 부각시킵니다. 이러한 공격은 실용적이지만, 가장 불안한 사실은 공격이 완전히 수동적이라는 점입니다. 본 논문에서는, 이러한 공격을 FMS 공격이라고 합니다. FMS 공격은 동일한 키를 사용하여 암호화된 100,000개에서 1,000,000개 사이의 패킷에서 이론적인 WEP 키 도출 과정에 대해 설명합니다. 더 자세한 내용은 http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps의 논문에서 직접 찾아볼 수 있습니다.

최근의 실제로 구현된 FMS 공격은 약 백만 개의 패킷을 잡아서 정적인 WEP 키를 도출해 낼 수 있었습니다. 이것은 http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf에 있는 AT&T Labs and Rice University의 논문에 증명되어 있습니다. 그 다음에 여러 명의 독립적인 개발자들이 나름대로 구현한 FMS 공격을 발표하였습니다. 이러한 FMS 공격 중에서 가장 많이 시도되는 것이 AirSnort입니다. 이것은 http://airsnort.sourceforge.net/에서 다운로드받을 수 있습니다.

확장된 보안 기능이 필요하다

시스코는 앞에 나온 기본 원칙들에서 설명한 연구 논문에서 밝힌 점들에 동의하며 IEEE 802.11에서 규정된 WEP의 대안으로 이러한 기본 원칙들에서 설명한 세 가지 테크놀러지의 기능들을 배치할 것을 권합니다. 설명된 테크놀러지 중에는 IPSec(IP Security)에 기초한 네트워크 레이어 암호화 방식, 상호 인증 방식의 802.1X를 사용하는 키 배포 방식, 그리고 시스코가 최근에 구현한 WEP의 몇 가지 향상된 독점적인 기능 등이 포함됩니다. 뿐만 아니라, IEEE 802.11 Task Group "i"는 현재 WLAN 암호화 기능 향상을 표준화하는 작업을 하고 있습니다.

IPSec

IPSec는 IP 네트워크를 통한 보안상 안전한 비공개 통신을 보장하는 개방형 표준의 골격입니다. IPSec VPN은 IPSec 내에 정의된 서비스를 사용하여 인터넷과 같은 공공망을 통한 데이터 통신의 기밀성, 무결성, 인증성을 보장합니다. IPSec에는 cleartext 802.11 무선 트래픽 위에 IPSec를 겹쳐 놓아서 WLAN을 보호하는 실용적인 애플리케이션도 갖추고 있습니다.

WLAN 환경에 IPSec를 배치하면, 무선 네트워크에 연결된 모든 PC에 IPSec 클라이언트가 존재하게 되고, 사용자는 트래픽을 유선 네트워크로 라우팅하려면 IPSec 터널을 만들어야 합니다. 무선 트래픽이 VPN 게이트웨이와 DHCP/DNS 서버 이외의 다른 곳으로 가지 못하게 하기 위하여 필터를 배치합니다. IPSec는 IP 트래픽의 기밀성, 인증 기능, 그리고 재생 방지 기능 등을 규정하고 있습니다. 3DES(Triple DES)라고 하는 변형 DES(Data Encryption Standard)를 사용한 암호화 방식으로 기밀성을 달성합니다. 3DES는 최대 3가지 키를 사용하여 데이터를 세 번 암호화하는 방식입니다.

주로 데이터 기밀성을 위하여 IPSec를 사용하기는 하지만, 확장 표준에서는 IPSec 프로세스의 일부로 사용자 인증과 권한 부여도 수행할 수 있습니다. 이 시나리오는 본 논문 뒷 부분에서 약술하는 WLAN에서의 사용자 차별화 문제에 대한 가능성이 있는 솔루션이 됩니다. IPSec에 대한 더 자세한 내용은, 다음 URL의 SAFE VPN 논문에서 VPN 기초 지식을 참조하십시오. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm.

EAP/802.1X

대체 WLAN 보안 방식은 중앙 집중식 인증과 동적인 키 배포를 위한 프레임워크를 개발하는데 초점을 맞추고 있습니다. 시스코 시스템즈, Microsoft, 그리고 그 외의 조직체들이 IEEE에 공동으로 제출한 제안서에서는 이러한 향상된 기능을 제공하기 위하여 802.1X와 EAP(Extensible Authentication Protocol)를 사용하는 엔드 투 엔드 프레임워크를 소개하였습니다. 이 제안의 핵심은 다음 두 가지 요소입니다.

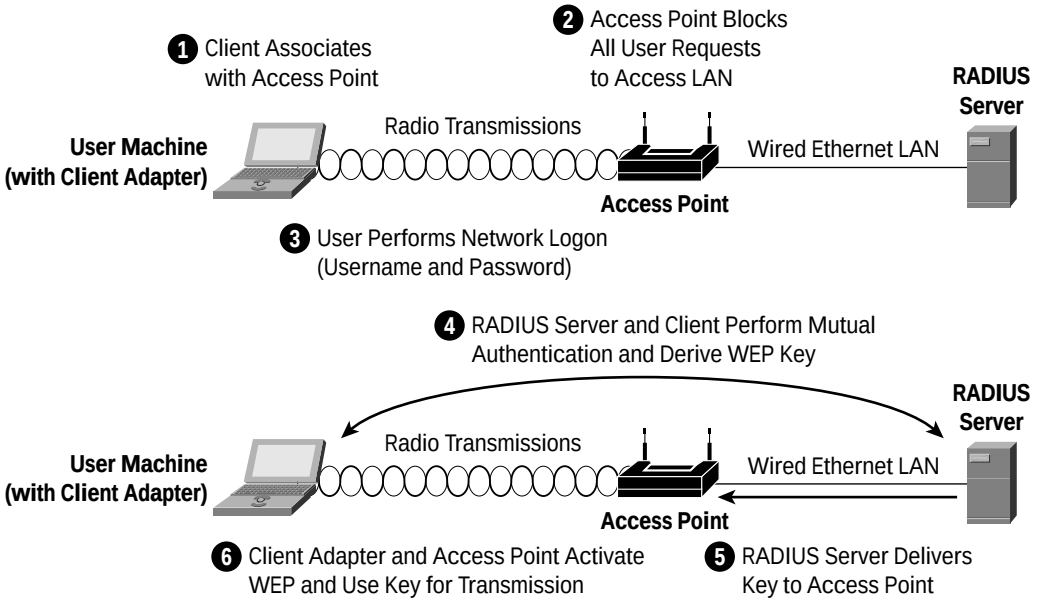
- EAP를 이용하면 다양한 인증 유형을 지원할 수 있는 무선 클라이언트 어댑터들이 RADIUS(Remote Access Dial-In User Service)와 같은 다른 종류의 백엔드 서버와 통신을 할 수 있습니다.
- IEEE 802.1X, 즉 포트 기반 네트워크 액세스 제어를 위한 표준

이러한 기능들이 구현되면, AP와 관련된 무선 클라이언트는 사용자가 네트워크 로그온을 수행할 때까지 네트워크를 액세스할 수 없습니다. 사용자가 네트워크 로그온 대화 상자나 그에 해당하는 것에 사용자 이름과 비밀번호를 입력하면, 클라이언트와 RADIUS 서버가 상호 인증을 수행하며, 클라이언트는 제시된 사용자 이름과 비밀번호를 기준으로 인증이 됩니다. 그 다음에 RADIUS 서버와 클라이언트는 현재 로그온 세션에서 클라이언트가 사용할 클라이언트 관련 WEP 키를 도출합니다. 사용자 비밀번호와 세션 키는 절대로 무선 링크를 통하여 공개적으로 전송되지 않습니다.

이벤트 진행 순서는 다음과 같습니다.

- 무선 클라이언트가 액세스 포인트와 연결지어집니다.
- 액세스 포인트는 클라이언트가 네트워크에 로그온할 때까지 클라이언트가 네트워크 리소스를 액세스하려고 하는 시도를 전부 차단합니다.
- 클라이언트 측의 사용자가 네트워크 로그온 대화 상자나 그에 해당하는 것에 사용자 이름과 비밀번호를 입력합니다.
- 유선 LAN 상의 무선 클라이언트와 RADIUS 서버는 802.1X와 EAP를 사용하여 액세스 포인트를 통한 상호 인증을 수행합니다. 여러 가지 인증 방식이나 유형 중의 하나를 사용할 수 있습니다. RADIUS 서버는 시스코 인증 유형 LEAP을 사용하여 클라이언트로 인증 요청을 보냅니다. 클라이언트는 사용자가 입력한 비밀 번호의 단방향 해시를 사용하여 그 요청에 대한 응답을 만들어서 RADIUS 서버로 보냅니다. RADIUS 서버는 사용자 데이터베이스의 정보를 사용하여 자체에서 응답을 만든 다음 그것을 클라이언트가 보낸 응답과 비교합니다. RADIUS 서버가 클라이언트를 인증하면, 클라이언트는 이 프로세스를 정반대로 반복하여 RADIUS 서버를 인증할 수 있습니다.
- 상호 인증이 성공적으로 끝나면, RADIUS 서버와 클라이언트는 클라이언트에게 고유한 WEP 키를 결정합니다. 클라이언트는 이 키를 로드하여 로그온 세션에서 사용할 준비를 합니다.
- RADIUS 서버는 유선 LAN을 통하여 액세스 포인트로 세션 키라고 하는 WEP 키를 보냅니다.
- 액세스 포인트는 세션 키를 사용하여 브로드캐스트 키를 암호화한 다음 그 암호화된 키를 클라이언트로 보냅니다. 그러면, 클라이언트는 세션 키를 사용하여 암호를 해독합니다.
- 클라이언트와 액세스 포인트는 WEP를 활성화시키고 세션의 나머지 시간 동안 모든 통신에 대해 그 세션 키와 브로드캐스트 WEP 키를 사용합니다.
- 세션 키와 브로드캐스트 키는 모두 RADIUS 서버에 설정된대로 일정한 간격으로 변경됩니다.

그림 1: LEAP 인증 프로세스



LEAP은 기본 WEP에 비해 두 가지 중요한 장점을 지니고 있습니다. 첫번째 장점은 위에서 설명한 상호 인증 방식입니다. 이 기법을 이용하면 해커 액세스 포인트와 RADIUS 서버에 의한 "man-in-the-middle 공격"을 효과적으로 없앨 수 있습니다. 두번째 장점은 WEP가 사용하는 암호화 키의 중앙집중식 관리와 배포입니다.

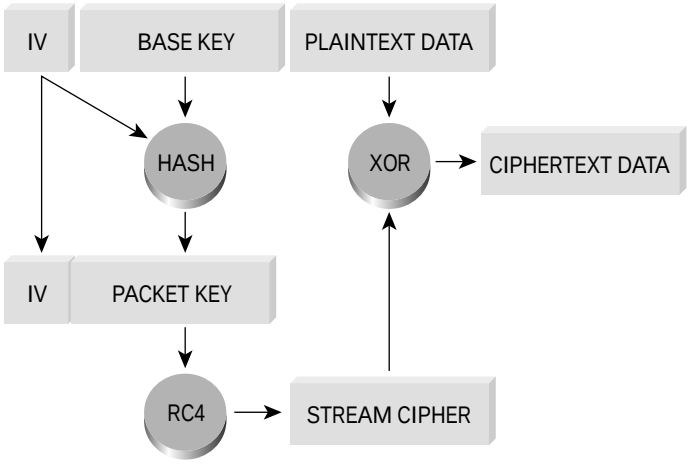
RC4의 WEP 구현 방식에 아무 결함이 없다해도, 정적인 키를 네트워크의 모든 AP와 클라이언트에게 배포하는 관리상의 문제는 여전히 존재합니다. 무선 장치가 사라질 때마다, 네트워크는 키를 다시 배포하여 사라진 시스템이 권한없는 액세스를 할 수 없게 해야 합니다.

향상된 WEP 기능

WEP 키 해싱

WEP에 대한 공격이 동일한 키를 사용하는 암호화된 트래픽의 스트림 안에 있는 다수의 약한 IV를 이용하는 방식에 의존하고 있기 때문에, 패킷마다 다른 키를 사용하는 것은 그 문제를 완화시키는 한 가지 방법이 됩니다. 그림 2에 나오는 것처럼, IV와 WEP 키를 해싱하여 (임시 키라고 하는) 고유한 패킷 키를 만든 다음, 그 키를 IV와 결합하고 plaintext와 XOR합니다. WEP에서 RC4 암호 해독을 하는 표준적인 802.11 방식은 본 문서의 기초 지식 부분에서 설명합니다.

그림 2: 패킷별 WEP 키 해싱



이 시나리오에서는 약한 IV를 사용하여 기본 WEP 키를 도출할 수 없습니다. 약한 IV에서는 패킷별 WEP 키만 도출할 수 있기 때문입니다. IV 충돌로 인한 공격을 방지하려면, IV가 키를 반복하기 전에 기본 키를 변경해야 합니다. 복잡한 네트워크의 IV는 시간의 흐름에 따라 반복하게 되므로, LEAP와 같은 메커니즘을 사용하여 키 재생성 동작을 수행해야 합니다.

메시지 무결성 검사

WEP와 관련하여 염려할 또 다른 문제는 replay 공격에 취약하다는 점입니다. MIC(message integrity check)는 WEP 프레임을 변조하지 못하게 보호하는 역할을 합니다. MIC는 seed value, 수신지 MAC, 발신지 MAC, 페이로드 등에 기초한 것입니다. (즉, 이런 요소들이 변경되면 MIC 값에 영향을 줍니다). MIC는 WEP 암호화 페이로드에 포함되어 있습니다. MIC는 해싱 알고리즘을 사용하여 그 결과 값을 도출합니다. 이것은 표준 방식 WEP에서 수행하는 CRC(cyclic redundancy check)-32 체크섬 기능을 향상시킨 것입니다. CRC-32의 경우, "CRC를 취한 메시지의 비트 차이를 기초로 두 CRC의 비트 차이를 계산하는 것이 가능합니다. 바꾸어 말하면, 메시지의 비트 n을 뒤집으면 수정된 메시지에서 정확한 체크섬이 되게 하기 위해 뒤집어야 하는 CRC의 결정적인 비트가 나오게 됩니다. 비트를 뒤집는 것은 RC4 암호 해독 후에 수행되므로, 공격자가 암호화된 메시지에서 임의의 비트를 뒤집은 다음 그 결과 메시지가 유효한 것처럼 보이도록 체크섬을 정확하게 조정할 수 있습니다."[1]

요약

조직체들은 IPSec나 이하의 내용에서 LEAP라고 하는 EAP/802.1X 중의 하나를 배치하기로 선택해야 하지만, 일반적으로 두 가지 모두 선택하지 않습니다. 이 두 가지를 동시에 사용하는 특정한 설계 방식을 SAFE 랩에서 테스트하였고, 그에 대해서는 아래 나오는 설계의 "대안" 부분에서 설명합니다. 조직체들은 전송된 데이터의 중요성이 매우 염려되는 경우에 IPSec를 사용해야 하지만, 이 솔루션은 LEAP에 비해 배치하고 관리하기가 더 복잡하다는 점을 기억하십시오. LEAP은 조직체가 기밀성과 투명한 사용자 보안 경험을 합리적인 정도까지 보장하려는 경우에 사용해야 합니다. WEP가 구현되어 있는 곳이면 어디서든지 향상된 기본 WEP 기능을 사용할 수 있습니다.

절대 다수의 네트워크의 경우, LEAP이 제공하는 보안으로 충분합니다. 표 1은 WLAN 설계에서 사용되는 IPSec와 LEAP에 대한 찬반 양론을 상세하게 정리한 것입니다.

표 1: 무선 암호화 테크놀러지 비교

	LEAP	IPSec	정적 WEP
키 길이 (비트)	128	168	128
암호화 알고리즘	RC4	3 DES	RC4
패킷 무결성	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
장치 인증	없음	사전 공유형 비밀 또는 인증서	없음
사용자 인증	사용자 이름/비밀번호	사용자 이름/비밀번호 또는 OTP	없음
사용자 차별화*	아니오	예	아니오
투명한 사용자 경험	예	아니오	예
ACL 요건	없음	실질적임	해당 없음
추가 하드웨어	인증 서버	인증 서버와 VPN 게이트웨이	아니오
사용자별 keying	예	예	아니오
프로토콜 지원	전부	IP 유니캐스트	전부
클라이언트 지원	PC 및 하이엔드 PDA. 시스코에서 지원하는 매우	PC 및 하이엔드 PDA. 다양한 OS. 시스코 및 외부 업체에서 지원하는 매우 다양한 OS	모든 클라이언트 지원
개방형 표준	아니오	예	예
시간 기준 키 로테이션	설정 가능	설정 가능	아니오
클라이언트 하드웨어 암호화	예	이용 가능함. 소프트웨어가 가장 일반적인 방식임	예
추가 소프트웨어	아니오	IPSec 클라이언트	아니오
플로우 별 QoS 정책 관리	액세스 스위치에서 실행	VPN 게이트웨이 다음에 실행	액세스 스위치에서 실행

*아래 나오는 "WLAN 사용자 차별화 관련 문제" 항목에서 더 자세히 설명함.

네트워크 가용성은 무선 테크놀러지에 영향을 준다

가용성이 높은 무선 네트워크를 설계하고 구현하는 것에 관심이 있는 네트워크 설계자들은 설계에서 유선 요소와 무선 요소를 모두 고려해야 합니다. SAFE 무선 테크놀러지에서, 본 백서는 보안 관련 서비스를 제공하는 네트워크 요소의 가용성 요건만 설명합니다. 특히, 다음 세 가지 장치에서 높은 가용성이 꼭 필요합니다.

- DHCP
- RADIUS
- IPSec

이어지는 내용에서는 WLAN을 안전하게 보호하기 위하여 서비스를 배치할 때 고려해야 하는 점들을 상세하게 설명합니다. 멀리 떨어진 곳에 있는 중소형 네트워크 설계에서는, SAFE 유선 네트워크에서도 고가용성을 제공하지 않으므로, 무선 네트워크가 고가용성을 지니고 있을 것이라고 기대해서는 안된다는 점에 유의하십시오.

DHCP(Dynamic Host Configuration Protocol)

- 초당 요청-DHCP 서버 하드웨어와 소프트웨어는 WLAN을 도입하면서 발생할 것으로 예상되는 수의 새로운 DHCP 요청을 수용할 수 있어야 합니다. DHCP 서버가 과부하 상태이면, 무선 사용자들은 DHCP 주소를 알아낼 수 없으므로, LEAP 사용자는 인증 후에 IP 연결을 하지 못하게 되고, IPSec 사용자는 VPN 게이트웨이를 사용하여 보안상 안전한 터널을 만들지 못하게 됩니다.
- DHCP Safe 장애 복구 프로토콜-네트워크 설계자들은 draft RFC DHCP Safe 장애 복구 프로토콜을 통하여 듀얼 서버에서 장애 대비 능력을 제공하는 DHCP 서버를 구현해야 합니다. 네트워크 설계자들은 이 프로토콜을 구현하여 일반적인 무선 사용자들의 네트워크 가용성을 증가시킬 수 있습니다.
- 주소 관리-네트워크 설계자들은 WLAN을 구현하면서 필요하게 된 가외의 IP 주소 지정 요건을 고려해야 합니다. 또한, 네트워크 설계자가 IPSec VPN을 사용하여 무선 환경을 안전하게 보호하기로 선택한다면, 구축되는 VPN 터널용으로 IP 주소를 더 지정해야 합니다. 어느 경우에도 DHCP 서비스를 사용할 수 없다면, 무선 사용자는 기업 네트워크를 액세스하지 못하게 됩니다.
- 네트워크 설계 관련 고려 사항-네트워크 설계자들은 서비스를 액세스하는 일반 사용자들과 관련하여 DHCP 서비스를 어디에 마련해야 하는지 고려해야 합니다. 고가용성을 갖추게 하려면 두 위치 사이에 이중 구성 방식의 네트워크가 있어야 합니다. 또한, 네트워크 설계자들이 한 서브넷에 모든 DHCP 서비스를 그룹으로 묶어 놓지 않는 것이 좋습니다. 그 서브넷에 DoS 공격이 가해지면 모든 무선 사용자가 DHCP 서비스를 이용하지 못하게 되기 때문입니다.

RADIUS

- 초당 요청-RADIUS 서버 하드웨어와 소프트웨어는 무선 LAN을 도입하는 것으로 인해 발생할 것으로 예상되는 초당 새로운 RADIUS 요청의 수를 수용할 수 있어야 합니다. RADIUS 서버가 과부하 상태이면, 무선 액세스 포인트와 VPN 게이트웨이는 사용자를 인증할 수 없기 때문에, 무선 사용자들이 기업 네트워크에 연결하지 못하게 됩니다. 또한, 네트워크 설계자들이 사용자 인증을 위하여 백엔드 데이터베이스를 사용하기로 선택하는 경우, 그 백엔드 데이터베이스도 무선 LAN을 도입하면서 발생할 것으로 예상되는 초당 사용자 인증 요청의 수를 수용할 수 있도록 설계되어야 합니다.
- 장애 대비형 서버 배치-인증 장치 (무선 액세스 포인트나 VPN 게이트웨이)가 인증 요청을 처리하는데 1차 옵션과 2차 옵션을 선택할 수 있게 하려면 복수의 RADIUS 서버를 배치해야 합니다. 또한 네트워크 설계자들은 인증 장치들을 그룹으로 묶어 1차 RADIUS 서버와 2차 RADIUS 서버의 목록을 번갈아 사용하게 해야 합니다. 이렇게 구성하는 목적은 두 가지입니다. 즉, 서버 장애가 발생하는 경우 장애 도메인을 제한하는 것과 각 RADIUS 서버를 보다 효과적으로 확장할 수 있게 하는 것입니다.
- 사용자 관리-RADIUS 서버는 사용자 인증에 필요한 사용자 데이터베이스 액세스의 높은 가용성을 제공해야 합니다. 네트워크 설계자들은 사용자 데이터베이스가 로컬 영역에 저장되어 있는 경우 데이터를 동기화시키는 서버를 구현하는 것을 고려해야 합니다. 이렇게 구성하면 단일 위치에서 네트워크를 관리할 수 있으며, 사용자 정의가 한 RADIUS 서버에는 존재하는데 다른 RADIUS 서버에는 존재하지 않을 가능성이 없어집니다. 사용자 데이터베이스가 외부(LDAP, NT 도메인)에 저장되어 있다면, 네트워크 설계자들은 RADIUS 서버를 백엔드 데이터베이스에 배치하는 것을 고려해야 합니다. 두 리소스 사이의 네트워크가 가동을 멈추면 무선 사용자가 기업 네트워크를 액세스하지 못하게 되기 때문입니다.

IPSec(IP Security Protocol)

- 초당 연결-VPN 게이트웨이 하드웨어와 소프트웨어는 무선 LAN을 도입하면서 발생할 것으로 예상되는 초당 새로운 IPSec 연결 수를 수용할 수 있어야 합니다.

- 암호화 처리량-VPN 게이트웨이 하드웨어와 소프트웨어는 무선 LAN을 도입하면서 발생할 것으로 예상되는 암호화 처리량을 수용할 수 있어야 합니다. VPN 게이트웨이는 비교적 큰 패킷 하나가 아니라 비교적 작은 패킷 여러 개를 암호화하기 때문에, VPN 게이트웨이의 암호화 처리량이 줄어듭니다. 네트워크 설계자들이 무선 네트워크 환경에 맞게 VPN 게이트웨이의 크기를 적절하게 조정하려면 유선 네트워크의 패킷 크기 분포를 이해하는 것이 중요합니다.
- 동시 IPSec 세션-VPN 게이트웨이 하드웨어와 소프트웨어는 무선 LAN을 도입하면서 발생할 것으로 예상되는 수의 동시 IPSec 세션을 수용할 수 있어야 합니다. VPN 게이트웨이는 제한된 수의 동시 IPSec 세션을 처리하도록 설계되어 있습니다.

위와 같은 구성을 염두에 두고 IPSec 환경을 설계하지 못하면 무선 사용자들이 기업 네트워크를 액세스하지 못하게 되거나, 액세스하게 된다 해도 성능이 심각하게 저하됩니다. VPN 판매업체들은 전용 클러스터링 테크놀러지를 도입하여 앞에 언급한 세 가지 문제를 처리하였습니다. 클러스터링 테크놀러지는 새로운 IPSec 연결에 가능한 최상의 서비스를 제공하기 위하여 새로운 IPSec 연결을 가장 부하가 적은 VPN 게이트웨이로 분배합니다.

IPSec 네트워크 설계에 대한 좀더 자세한 내용은 SAFE VPN: IPSec Virtual Private Networks in Depth에서 다룹니다.

WLAN 사용자 차별화 관련 문제

유선 네트워크에서, 종종 레이어 3 세그먼트화 기법을 사용하여 공동체를 기준으로 사용자를 구분하는 것이 가능합니다. 예를 들어 SAFE 엔터프라이즈의 경우, 마케팅 부문과 R&D 부문이 구분되어 있습니다. 이러한 세그먼트 구분은 빌딩 분배 모듈에서 이루어집니다. 빌딩 분배 모듈은 사용자 공동체를 위한 네트워크에서 레이어 3의 첫번째 위치입니다. SAFE 엔터프라이즈의 나머지 영역에서는, 다른 사용자 공동체가 액세스하는 IP 주소를 걸러내어 이러한 세그먼트 구분을 유지할 수 있습니다. 유선 네트워크에서도, 이런 종류의 세그먼트 구분은 관리면에서 복잡합니다. 기능면의 구분과 물리적인 구분이 종종 전혀 다르게 되어 있기 때문입니다. 예를 들어, 조직체의 회계 시스템을 액세스해야 하는 재무 조정실이 기본적인 서비스만 액세스하면 되는 접견실 바로 옆에 있을 수 있습니다.

유선 네트워크에서는 이러한 세그먼트 분할이 어렵기는 하지만 가능한 반면, 무선 네트워크에서는 요즘의 무선 테크놀러지로는 거의 불가능하게 됩니다. (앞에서 설명한) IPSec와 같은 오버레이 보안 메커니즘을 배치하는 방법으로만 이런 수준의 차별화를 할 수 있습니다. 핵심 문제는 임의의 장소 내에 물리적인 경계선을 두지 않는 무선 네트워크와 관련된 것입니다. 앞에 언급한 예의 재무 조정실과 접견실은 모두 동일한 AP를 액세스하게 됩니다.

현재로서는 이런 세그먼트 구분을 할 수 있는 것이 전혀 없으므로, IPSec WLAN을 배치하지 않는 한, 사용자 공동체를 기준으로, 일반적으로 액세스할 때 레이어 3 제어 기능을 사용하는 시스템이 무선 네트워크를 이용하여 액세스하지 못하게 차단하는 것이 좋습니다. 예를 들어, 정상적인 경우 개발자 서브넷만 액세스할 수 있는 R&D 시스템이 있다면, 무선 구현 형태에서 그 시스템 사용을 완전히 차단시켜야 합니다.

앞서 간단하게 언급한 것처럼, 사용자들이 엔드 호스트에서 VPN 클라이언트를 실행하게 한다면, 무선 네트워크는 전적으로 이동 중에만 사용하게 하고 보안 제어 기능은 VPN이 처리하게 할 수 있습니다. 이런 설계에서는 사용자 차별화가 가능하며 이 점은 본 문서 뒷 부분에서 자세히 설명합니다.

설계 방식

SAFE 무선 테크놀러지는 기본 원칙 부분에서 약술한 일반적인 WLAN 보안 관련 문제들을 처리합니다. 본 설계 섹션에서는 기본 원칙 섹션에서 소개한 문제 및 해결 방법을 통합한 다음 매우 다양한 종류의 네트워크에 적용합니다. 특정한 설계의 규모 및 보안 관련 문제들에 따라 WLAN 설계에 적용되는 해결 기법이 결정됩니다. 따라서, 네트워크 설계자는 SAFE 설계와 관련된 테크놀러지의 장점과 단점에 따라 구현할 문제 해결 테크놀러지를 선택할 수 있습니다. 문제 해결 테크놀러지는 모든 SAFE 설계에서 일관성이 있으므로, 선택할 수 있는 두 가지 주요 테크놀러지의 네트워킹 요소에 대한 검토를 먼저 소개합니다. 테크놀러지를 검토한 후에, 네트워크 설계자에게 각 SAFE 설계를 제시하고 그와 함께 SAFE 내에서 특정한 문제 해결 테크놀러지를 구현하는 것의 장/단점을 함께 설명합니다.

SAFE 설계 내에서 문제 해결 테크놀러지를 구현하는 것의 독특한 특징도 제시합니다. 선택할 수 있는 두 가지 주요 설계 방식은 다음과 같습니다.

- LEAP이라고 하는 EAP 및 802.1X를 사용한 동적인 WEP keying 모델 구현
- IPSec를 사용하는 오버레이 VPN 네트워크 구현

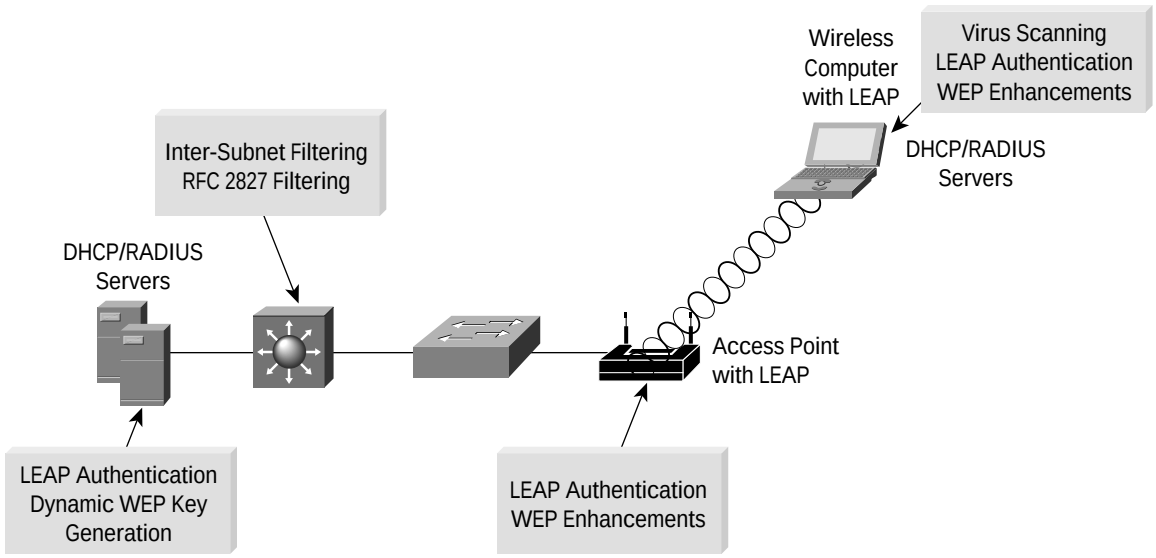
표준 WLAN 설계 지침

WLAN 설계의 많은 부분이 SAFE 설계 전체에서 공통적이기 때문에 이 섹션에서는 WLAN 설계의 일반적인 요소들을 약술합니다. 이 섹션을 읽은 후에, 가장 흥미있는 WLAN 설계 부분으로 넘어가면 됩니다. 기본 개념은 이런 식으로 한 번 포함시키고 특정한 SAFE 설계에서 설명한 특정한 변이형과 대안도 함께 설명이 됩니다. 표준 WLAN 설계에서는, 모든 WLAN 장치들이 고유한 IP 서브넷에 연결되어 있기 때문에 다양한 설계들에서 일반 사용자의 이동성이 보장된다고 가정합니다. 이 설계들에서는 유선 네트워크에서 사용할 수 있는 대부분의 서비스를 추가된 무선 네트워크 부분에서도 이용할 수 있다고 가정합니다.

표준 LEAP WLAN 설계

이 설계 방식은 생산 기업 네트워크를 액세스하는 보안 메커니즘으로 LEAP을 사용하는 일반적인 방식을 상세히 설명합니다.

그림 3: 표준 LEAP WLAN 설계를 위한 공격 대처 역할



주요 LEAP 장치

- 무선 클라이언트 어댑터와 소프트웨어-AP와의 무선 통신에 필요한 하드웨어와 소프트웨어를 제공하는 소프트웨어 솔루션. 이 솔루션은 LEAP를 통하여 AP에 상호 인증 기능을 제공합니다.
- 무선 액세스 포인트-LEAP를 통하여 무선 클라이언트를 상호 인증합니다
- 레이어 2/3 스위치-WLAN AP와 기업 네트워크 사이에서 이더넷 연결 기능과 레이어 3/4 필터링 기능을 제공합니다
- RADIUS 서버-무선 클라이언트를 위한 사용자 기준 인증과 액세스 포인트 인증을 무선 클라이언트에게 제공합니다
- DHCP 서버-무선 LEAP 클라이언트를 위한 IP 구성 정보를 전달합니다

처리된 위협

- 무선 패킷 스니퍼-무선 패킷 스니퍼는 이미 알고 있는 WEP 공격을 이용하여 암호화 키를 도출할 수 있습니다. 이러한 위협은 향상된 WEP 기능("향상된 보안 기능이 필요합니다" 항목 참조)과 LEAP를 사용한 키 로테이션으로 대처할 수 있습니다.
- 인증되지 않은 액세스-인증된 사용자들만이 무선 네트워크와 유선 네트워크를 액세스할 수 있습니다. 레이어 3 스위치의 선택적인 액세스 제어 기능이 유선 네트워크 액세스를 제한합니다.
- Man in the middle-LEAP의 상호 인증 방식은 MIC와 결합이 되어 해커가 무선 통신 통로 안으로 끼어들어오지 못하게 막습니다.
- IP 스푸핑-해커가 IP 스푸핑을 하려면 먼저 WLAN에 인증을 받아야 합니다. 인증을 한 후에 레이어 3 스위치의 선택적인 RFC 2827 필터링은 로컬 서브넷 범위로의 스푸핑을 제한합니다.
- ARP 스푸핑-해커들이 ARP 스푸핑을 하려면 먼저 WLAN에 인증을 받아야 합니다. 인증을 한 후에는 유선 네트워크 환경에서와 동일한 방식으로 ARP 스푸핑 공격을 실행하여 다른 사용자의 데이터를 가로챌 수 있습니다.
- 네트워크 토폴로지 발견-해커들은 인증을 할 수 없으면 네트워크를 찾아낼 수 없습니다. LEAP를 통하여 인증이 되면, 유선 네트워크에서 가능한 것과 동일한 방식으로 표준 토폴로지 발견이 이루어집니다.

처리되지 않은 위협

- 비밀번호 공격-LEAP은 OTP(one-time passwords)를 지원하지 않으므로, 사용자 인증 프로세스는 비밀번호 공격 방식에 약합니다. 선택된 비밀번호의 약점을 검사하고 일정한 회수 동안 비밀번호 입력 시도가 있으면 계정을 잠궈버리는 비밀번호 사용 정책을 준수하면 이 공격에 대처할 수 있습니다.

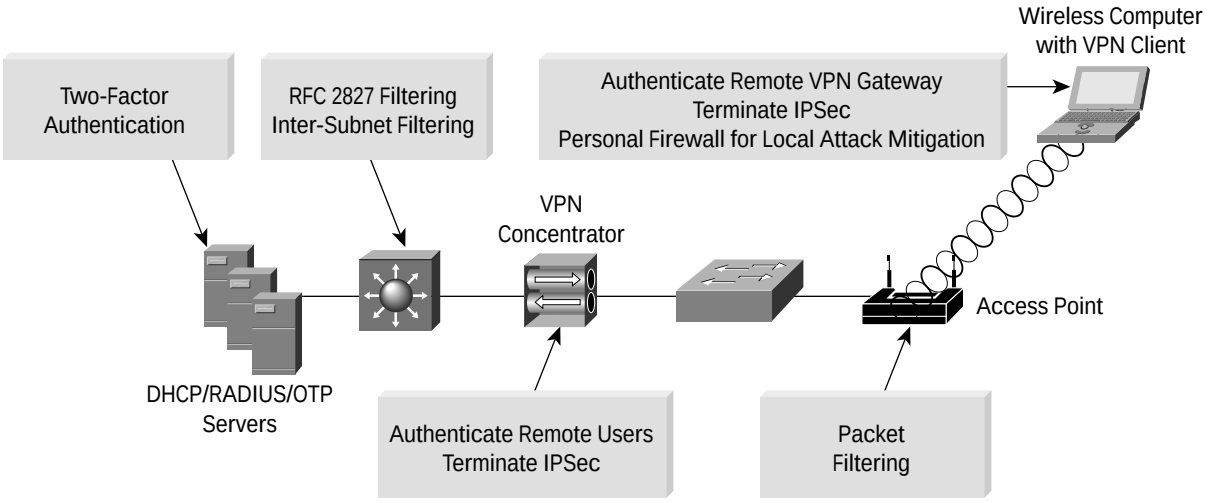
LEAP 설계 지침

대부분의 경우, WLAN 액세스 포인트는 이미 존재하는 레이어 2 액세스 스위치에 연결되어 있습니다. RADIUS 서버와 DHCP 서버는 기업 네트워크의 서버 모듈에 있습니다. 설계에 포함된 보안은 RADIUS 서비스 장애가 발생하면 네트워크 액세스를 금지시키는 방식으로 유지됩니다. 보안 위험을 해결하는 대부분의 방법은 RADIUS 서비스에 의존하기 때문에, 이 방법을 사용해야 합니다. 전반적으로 DHCP 서비스가 장애를 일으키면 솔루션을 관리할 수 없습니다. 무선 클라이언트와 AP는 LEAP을 사용하여 WLAN 클라이언트 장치와 일반 사용자를 RADIUS 서버에서 인증합니다. LEAP 프로세스는 OTP를 지원하지 않기 때문에, 네트워크에 보안상 상당히 큰 허점이 생기게 된다는 점에 유의해야 합니다. 공격자들은 LEAP 인증 프로세스를 강제로 뚫고 들어가려고 시도할 수 있기 때문입니다. 반드시 사용자들이 쉽게 알아낼 수 없는 비밀번호를 선택하고 잘못된 로그인 시도가 몇 번 있으면 계정을 잠그도록 요구(하고 확인)해야 합니다. RADIUS 서버에서 이렇게 설정할 수 있습니다. 확장성과 관리 편이성을 위하여, IP 구성에 DHCP 프로토콜을 사용하도록 WLAN 클라이언트 장치들을 설정할 수 있습니다. DHCP는 장치 다음에 이루어지며 최종 사용자는 LEAP를 통하여 성공적으로 인증이 됩니다. DHCP가 성공적으로 구성되면, 무선 네트워크와 사용자가 기업 네트워크를 액세스하도록 허용됩니다. 첫번째 레이어 3 스위치에 필터링 기능을 배치하면 조직체의 보안 정책에 규정된 대로 무선 네트워크가 유선 네트워크의 일부를 액세스하지 못하게 됩니다. 예를 들어, SAFE에서는, 부서 서버, 음성 네트워크, 또는 그 외의 사용자 네트워크를 무선 방식으로 액세스하지 못하게 하기 위하여 필터링 기능을 내장시켰습니다. 네트워크 설계자들은 LEAP가 사용하는 RADIUS 서버와 DHCP 서버의 위치를 특별히 고려해야 합니다.

표준 VPN WLAN 설계

이 설계에서는 WLAN에서 생산 기업 네트워크를 액세스하는 오버레이 보안 메커니즘으로 IPSec VPN을 사용하는 일반적인 방법을 상세히 규정합니다.

그림 4: 표준 VPN WLAN 설계의 공격 처리 역할



주요 VPN 장치

- 무선 클라이언트 어댑터와 소프트웨어-AP와의 무선 통신에 필요한 하드웨어와 소프트웨어를 제공하는 소프트웨어 솔루션
- 개인 방화벽 소프트웨어를 갖춘 원격 액세스 VPN 클라이언트-각 PC와 기업 무선 VPN 게이트웨이 사이에 엔드 투 엔드 암호화된 터널을 마련하는 소프트웨어 클라이언트. 개인용 방화벽 소프트웨어는 각 PC를 장치 수준에서 보호합니다
- 무선 액세스 포인트-WLAN과 기업 네트워크 사이에서 최초의 IP 프로토콜 필터링 기능을 제공합니다
- 레이어 2 스위치-WLAN AP와 기업 네트워크 사이에서 이더넷 연결 통로를 제공합니다
- 레이어 3 스위치-모듈 사이에서 생산 네트워크 데이터를 라우팅 및 스위칭합니다. 무선 트래픽을 프로토콜 수준에서 필터링하여 정책을 더욱 확실하게 시행합니다
- RADIUS 서버-VPN 게이트웨이에서 터미네이션되는 무선 사용자를 인증하고, 선택에 따라 OTP 서버와 통신을 합니다
- OTP 서버-RADIUS 서버에서 중계된 일회성 비밀번호 정보를 인증합니다
- DHCP 서버-VPN을 구축하기 전과 구축한 후에 무선 VPN 클라이언트의 IP 구성 정보를 전달합니다
- VPN 게이트웨이-각 원격 사용자를 인증하고 그 사용자의 IPSec 터널을 터미네이션시킵니다

처리된 위협

- 무선 패킷 스니퍼-이러한 위협은 무선 클라이언트 트래픽을 IPSec 방식으로 암호화하면 대처할 수 있습니다.
- Man in the middle-이러한 위협은 무선 클라이언트 트래픽을 IPSec 방식으로 암호화하면 대처할 수 있습니다.
- 권한없는 액세스-초기 IP 구성(DHCP)과 VPN 액세스(DNS, IKE〔Internet Key Exchange〕 및 ESP〔Encapsulating Security Payload〕)용으로 알려진 프로토콜만이 AP와 레이어 3 스위치에서 필터링을 거쳐서 WLAN에서 기업 네트워크로 전달될 수 있습니다. 각 사용자 그룹의 VPN 게이트웨이에 대해 권한 부여 정책을 선택적으로 실행할 수 있습니다.

- IP 스푸핑-해커들은 무선 LAN에서 트래픽을 스푸핑할 수 있지만, 인증이 된 유효한 IPSec 패킷만이 생산 유선 네트워크에 도달합니다.
- ARP 스푸핑-ARP 스푸핑 공격을 실행할 수는 있지만 데이터가 암호화되어 VPN 게이트웨이로 보내지므로 해커는 데이터를 읽을 수 없습니다.
- 비밀번호 공격-이러한 공격은 강력한 비밀번호 정책과 감사 기능을 사용하고 선택에 따라서는 OTP를 사용하여 막을 수 있습니다.
- 네트워크 토폴로지 발견-이 세그먼트에서 기업 네트워크로 들어오도록 허용되는 것은 IKE, ESP, DNS, DHCP 밖에 없습니다.

처리되지 않은 위협

- 인증되지 않은 사용자의 MAC/IP 스푸핑-무선 클라이언트가 IPSec를 사용하여 연결을 안전하게 보호할 때까지는 ARP 스푸핑과 IP 스푸핑이 WLAN 서브넷에 계속 영향을 줍니다.

표준 VPN WLAN 설계 지침

WLAN AP는 전용 VLAN의 빌딩 모듈 레이어에 있는 레이어 2 스위치에 연결되어 IPSec를 사용하여 WLAN에서 유선 LAN으로 트래픽을 포워딩하여 트래픽이 유선 네트워크에 도달할 때까지 흐름을 보호합니다. 이 설계에서는 WEP를 사용하도록 설정하지 않았음을 유의하는 것이 중요합니다. 무선 네트워크 자체는 신뢰할 수 없는 네트워크로 간주되므로, IPSec 트래픽의 이동 네트워크로만 적합합니다. 이 신뢰할 수 없는 네트워크를 분리시키기 위하여, 시스템 관리자들은 WLAN 사용자의 VLAN을 유선 네트워크와 혼성으로 구성해서는 안됩니다. 이렇게 구성하면 무선 네트워크의 해커들이 유선 네트워크의 사용자를 공격할 가능성이 있습니다. WLAN 클라이언트는 무선 AP와 연결되어 레이어 2의 캠퍼스 네트워크로 연결되는 통로를 만듭니다. 그 다음에 무선 클라이언트는 서버 모듈의 DHCP 서비스와 DNS 서비스를 사용하여 레이어 3의 캠퍼스로 연결되는 통로를 만듭니다. 무선 클라이언트가 캠퍼스 네트워크와 통신을 하고 있지만 IPSec 터널을 만들기 전이라면 클라이언트 트래픽을 보안상 안전하다고 간주할 수 없다는 점에 유의해야 합니다. 명시된 모든 WLAN 보안 문제들은 무선 클라이언트가 IPSec VPN과의 통신을 안전하게 보호할 수 있을 때까지 사라지지 않습니다. 따라서, 두 가지 문제 처리 기법을 제안합니다:

먼저, AP는 기업체의 무선 사용 방식 정책을 기초로 ethertype, 프로토콜, 포트 필터 등을 갖추도록 구성해야 합니다. SAFE WLAN은 VPN 게이트웨이로 연결되는 보안상 안전한 터널을 만드는데 필요한 프로토콜만을 허용하는 제한적인 필터를 권합니다. 이러한 프로토콜에는 초기 클라이언트 구성을 위한 DHCP, VPN 게이트웨이의 이름 해석을 위한 DNS, VPN 관련 프로토콜인 IKE (UDP 포트 500)와 ESP (IP 프로토콜 50) 등이 포함됩니다. VPN 게이트웨이의 DNS 이름으로 VPN 클라이언트를 설정해야 하는지 아니면 한 IP 주소만으로 충분한지에 따라 DNS 트래픽은 선택적입니다.

두 번째로, 개인 방화벽 소프트웨어는 무선 클라이언트에 포함되어 클라이언트를 보호하며, 동시에 IPSec의 보호를 받지 않는 신뢰할 수 없는 WLAN 네트워크에도 연결되어 있습니다. 일반적인 의미에서, VPN 게이트웨이는 신뢰할 수 있는 유선 네트워크와 신뢰할 수 없는 WLAN 사이를 규정하는 것입니다. 무선 클라이언트는 VPN 게이트웨이로 연결되는 VPN 연결 통로를 만들고 기업 네트워크와 보안상 안전한 통신을 시작합니다. 그렇게 하는 과정에서, VPN 게이트웨이는 IPSec VPN을 통하여 장치와 사용자를 인증합니다.

이러한 필터링 방식에서도, DNS 서버와 DHCP 서버는 애플리케이션 프로토콜 자체에 대한 직접적인 공격에 여전히 노출되어 있습니다. 이러한 시스템이 호스트 수준에서 가능한한 안전하게 보호가 되게 하려면 각별히 주의를 기울여야 합니다. 그 중에는 OS와 애플리케이션의 최신 패치를 적용하고 HIDS(host-based intrusion-detection system)를 실행하는 것이 포함됩니다.

VPN 게이트웨이는 무선 장치 인증을 위하여 디지털 인증서나 사전 공유키를 사용할 수 있습니다. 그 다음에 VPN 게이트웨이는 OTP를 이용하여 사용자를 인증합니다. OTP가 없으면, VPN 게이트웨이는 VPN 게이트웨이가 사용하는 공유 IPSec 키를 알아낸 해커의 무작위 로그인 시도에 그대로 노출됩니다. VPN 게이트웨이는 RADIUS 서비스를 활용하며, RADIUS 서비스는 사용자 인증을 위하여 OTP 서버에 연결합니다. VPN 게이트웨이는 WLAN 클라이언트가 VPN 터널을 통하여 통신할 수 있도록 IP 주소 구성을 위하여 DHCP를 사용합니다. VPN 게이트웨이나 RADIUS 서비스가 장애를 일으키면 네트워크 액세스를 못하게 만들어서 설계의 보안 상태를 유지합니다. 클라이언트가 생산 트래픽이 있는 유선 네트워크에 도달하게 하려면 이 두 가지 서비스가 모두 필요합니다.

대안

네트워크 설계자들은 아직도 해커에 대한 방어 무기를 추가하려는 노력의 일환으로 모든 장치에 정적인 WEP 키를 사용하게 하는 것을 고려할 수 있습니다. MIC나 WEP 키 해싱과 같은 향상된 WEP 기능들이 현재 식별된 WEP의 취약점의 위험 수준을 완화시키는데 효과적이기는 하지만, 정적인 키 변경을 처리하는 시스템 관리 업무때문에 이 대안은 대규모 WLANP 배치에서는 이상적이 아닙니다. 이 시스템 관리 업무는 정적인 WEP 키를 절대로 변경하지 않으면 완화되지만, 이 솔루션은 "security-through-obscurity"의 범주로 곧장 전락하게 됩니다.

DNS 서비스와 DHCP 서비스를 좀더 안전하게 보호하려면, 네트워크 설계자들은 VPN WLAN DHCP와 DNS 배치를 위해 전용 호스트를 사용하는 것을 고려해야 합니다. 이렇게 하면 유선 리소스에 영향을 줄 수 있는 다음 두 가지 잠재적인 공격을 막아낼 수 있습니다.

- 유선 사용자에게 영향을 줄 수 있는 DHCP와 DNS 서비스에 대한 DoS 공격
- DNS 질의나 리버스 룩업을 사용한 네트워크 정찰

전용 DNS 서버에 대한 대안으로, 설계자들은 VPN 클라이언트에 대해 VPN 게이트웨이의 IP 주소를 하드코딩하는 것을 고려할 수 있습니다. 이 솔루션의 약점은 VPN 게이트에이의 IP 주소가 변경되면, 모든 클라이언트가 게이트웨이 엔트리를 갱신해야 한다는 점입니다.

대기업체 WLAN 설계

대기업체 WLAN 설계는 SAFE 엔터프라이즈 블루프린트의 캠퍼스 부분의 위에 무선 LAN을 올려놓습니다. 문제 처리 기법을 구현하는데 필요한 모든 컴포넌트는 대기업체 빌딩, 분배 모듈, 서버 모듈 등에 들어 있습니다. 이러한 컴포넌트들은 엔터프라이즈 캠퍼스 내의 엔터프라이즈 일반 사용자에게 WLAN 액세스를 허용하려는 것입니다. 각 문제 처리 기법을 구현하는 구체적인 방법은 아래에서 자세히 설명합니다.

설계 지침

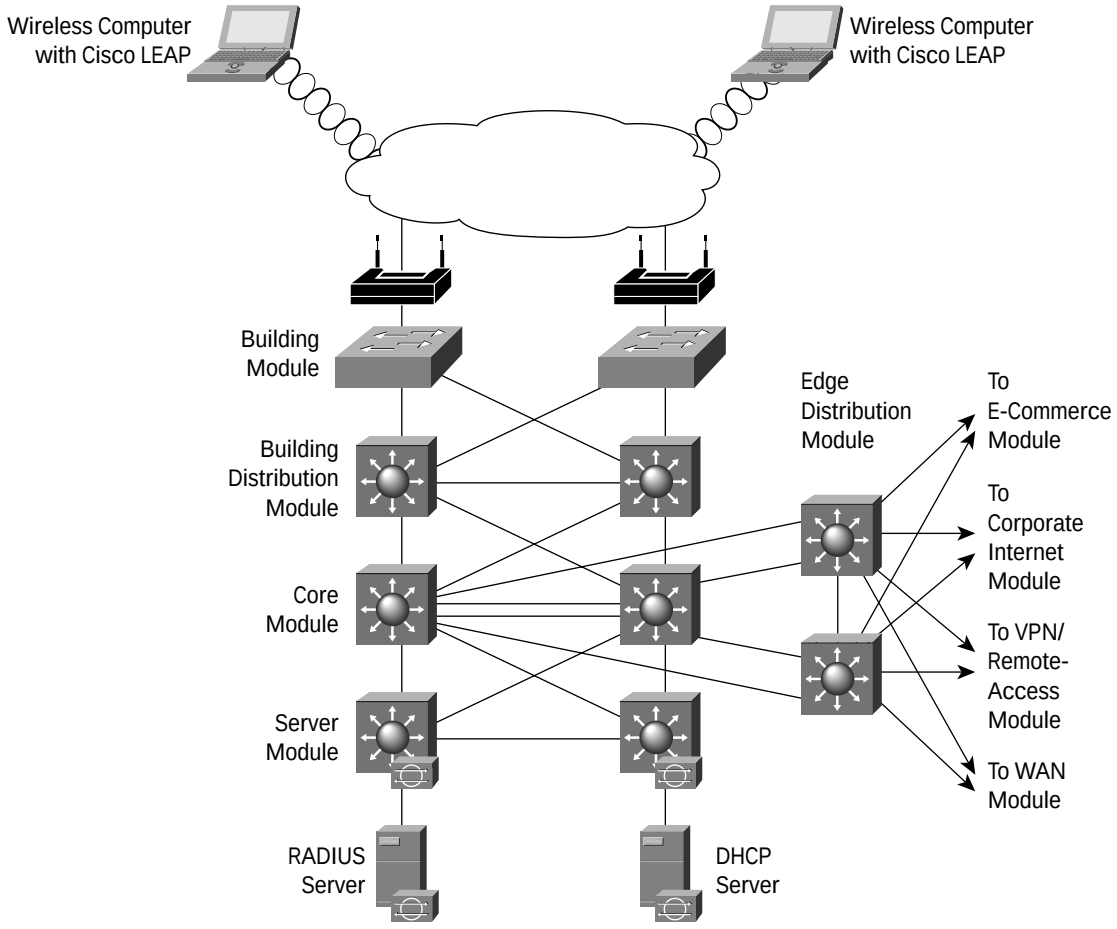
대기업체 WLAN 설계에서, 문제 처리 테크놀러지를 구현할 때 주된 관심사는 확장성과 고가용성이었습니다. LEAP과 VPN은 모두 대기업체 WLAN 설계에서 가능한 보안 옵션으로 간주됩니다. 네트워크 설계자들은 네트워크에 가장 적합한 테크놀러지를 선택하기 전에 기업 보안 정책과 관련하여 두 테크놀러지의 업무 상의 장점을 저울질 해 보아야 합니다.

네트워크 관리

AP의 네트워크 관리는 빌딩 분배 레이어 3 스위치에서 ACL을 구현하여 네트워크 관리 서브넷으로 제한됩니다. AP가 한 가지 유선 인터페이스만 지원하므로, 모든 관리는 인밴드로 수행되었다는 점에 유의해야 합니다. 이것은 SAFE 엔터프라이즈에서 제안하는 아웃오브밴드 관리와 비교가 됩니다. 이런 설정에서는 관리 트래픽을 공중을 통해 각 AP로 보내야 하므로 네트워크에 보안상 허점이 생기게 됩니다.

LEAP 옵션

그림 5: 대기업체 LEAP WLAN 설계



무선 네트워크를 통한 LEAP 액세스는 SAFE 엔터프라이즈 아키텍처의 다음 세 가지 컴포넌트를 활용합니다. :

- 빌딩 모듈
- 빌딩 분배 모듈
- 서버 모듈

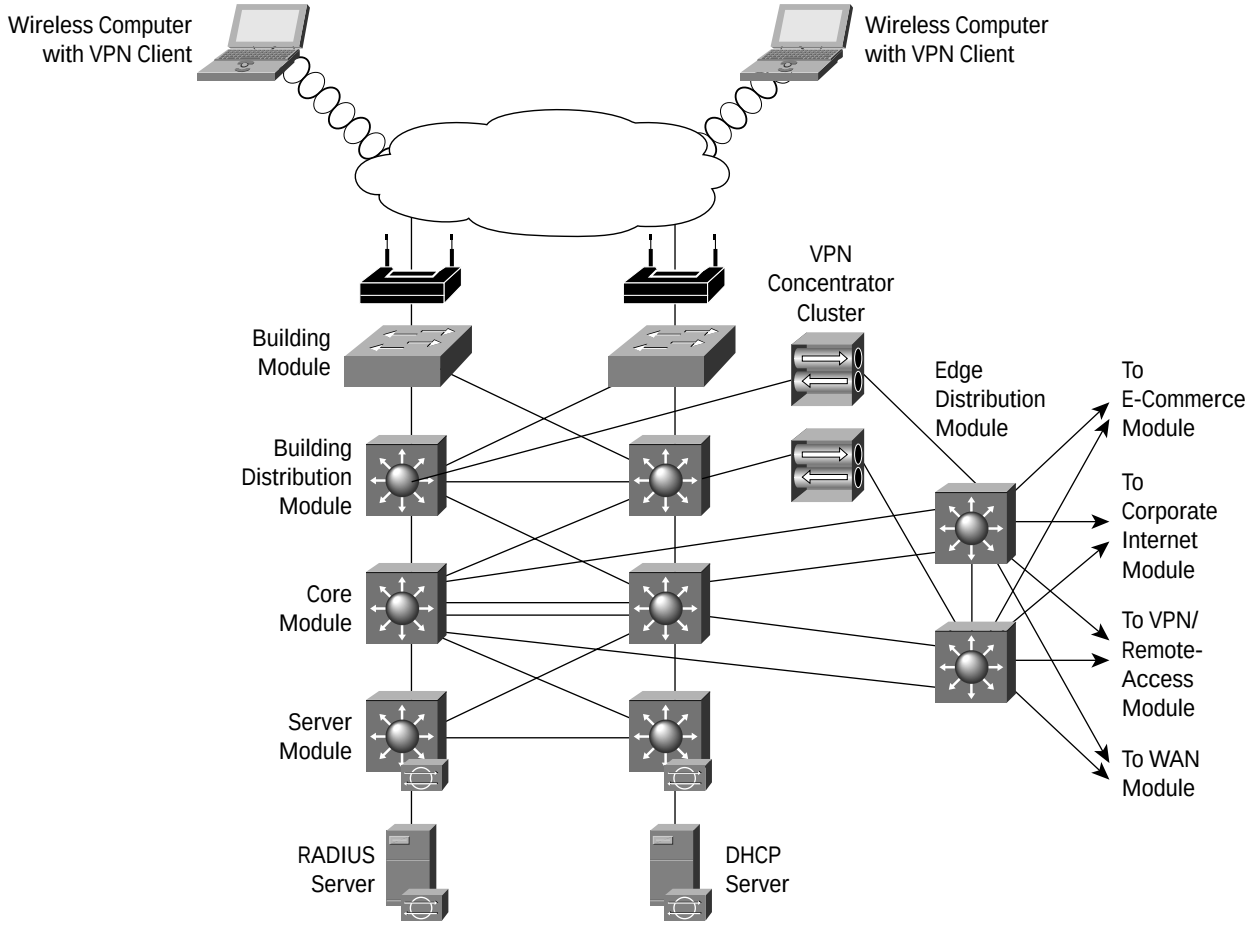
대형 WLAN 설계에서, 무선 AP는 기업 캠퍼스 전체에서 빌딩 모듈의 이미 존재하는 레이어 2 액세스 스위치에 연결되어 있습니다. RADIUS 서버와 DHCP 서버는 서버 모듈 안에 있습니다. 대형 WLAN 설계에서 LEAP와 관련된 주된 문제는 서버의 가용성과 확장성입니다. 기본 원칙 섹션의 내용대로, RADIUS 서버와 DHCP 서버는 서로 다른 네트워크 서브넷에서 이중 구성 방식으로 배치되므로 고가용성과 확장성이 보장됩니다. 위에 열거한 점들 외에는, 연결 방식은 위에서 언급한 표준 LEAP WLAN 설계와 동일합니다.

대안

인증과 암호화를 위한 주된 보안 도구로 LEAP를 선택할 때, 네트워크 설계자는 선택에 따라 무선 클라이언트가 웹 브라우징과 같은 기본 수준의 보안으로 충분한 애플리케이션만 액세스하도록 제한하는 정책을 만들어서 WLAN의 보안 수준을 더욱 향상시킬 수 있습니다. 그 다음에 LEAP에 더하여 IPSec를 사용하면 권한이 있는 사용자를 VPN 게이트웨이에 인증한 다음 중요한 업무용 시스템(HR, 회계, 등등)을 액세스하도록 허용할 수 있습니다. 그림 6은 IPSec를 구체적으로 그린 것입니다.

IPSec VPN 옵션

그림 6: 대기업체 VPN WLAN 설계



무선 네트워크를 통한 IPSec VPN 액세스는 SAFE 엔터프라이즈 아키텍처의 다음 모듈을 사용합니다.:

- 빌딩 모듈
- 빌딩 분배 모듈
- 에지 분배 모듈
- 서버 모듈

설계 지침

대형 WLAN 설계의 주된 목표에는 보안 위험 요소를 처리하는 것과 기업체가 감당할 수 있는 비용으로 구현할 수 있는 확장성이 있는 설계를 만드는 것 사이에서 균형을 잡는 것이 관련됩니다. 본 문서의 표준 VPN WLAN 설계 지침에서는 WLAN 환경을 안전하게 보호하도록 VPN을 구현하는 일반적인 방법을 약술합니다.

대형 WLAN 환경의 맥락에서 보면, 설명된 지침은 레이어 2 스위칭 인프라와 케이블 배선을 별도로 마련해야 하기 때문에 대부분의 기업체들의 경우 비용면에서 허용이 되지 않습니다. 따라서, 대규모 네트워크 환경에서 VPN WLAN을 구현할 수 있게 하려면 보안 기능을 어느 정도 양보해야 합니다. 이어지는 내용에서는 네트워크 설계자들이 VPN이 자신의 환경에 맞는 솔루션인지 여부를 결정하는데 도움이 되도록 이러한 부면에 대해 설명합니다.

WLAN 클라이언트들은 빌딩 모듈의 무선 AP에 연결하여 레이어 2의 캠퍼스 네트워크로 연결되는 연결 통로를 만듭니다. 그 다음에 무선 클라이언트들은 서버 모듈의 DHCP 서비스와 DNS 서비스를 사용하여 레이어 3의 캠퍼스로 연결되는 연결 통로를 만듭니다. 무선 클라이언트가 WLAN 네트워크와 통신을 하고 있지만 IPSec 터널을 만들기 전이라면 네트워크 트래픽이 안전하게 보호되고 있다고 볼 수 없다는 점에 유의해야 합니다. 언급된 모든 WLAN 보안 문제들은 무선 클라이언트가 IPSec VPN과의 통신을 안전하게 보호할 때까지는 사라지지 않습니다. 일반적인 VPN WLAN 설계에서 언급된 AP의 필터 외에도, 빌딩 분배 모듈 레이어 3 스위치에는 VPN 연결과 네트워크 관리에 필요한 프로토콜만 허용하는 ACL가 설정됩니다. 무선 클라이언트는 빌딩 분배 모듈과 에지 분배 모듈을 연결하는 VPN 게이트웨이로 연결되는 VPN 연결 통로를 만듭니다. 이중 구성된 VPN 게이트웨이는 부하 분배 형식으로 구성하여 고가용성과 확장성을 제공할 수 있습니다. 이러한 VPN 게이트웨이는 잠재적으로 다수의 레이어 2 빌딩 모듈이 공유하는 중앙 집중식 리소스입니다. VPN 게이트웨이가 사용하는 RADIUS 서버와 DHCP 서버는 서버 모듈 내의 다양한 네트워크 서브넷에서 이중 구성 방식으로 배치되어 VPN 클라이언트 터널에 제공되는 해당 서비스의 높은 가용성과 확장성을 보장합니다.

대안

무선 사용자 트래픽이 생산 유선 네트워크로 들어오기 전에 VPN 게이트웨이 뒤에 NIDS(network-based intrusion-detection system)와 방화벽을 배치하면 보안 상태를 더욱 향상시킬 수 있습니다. 이렇게 구성하면 네트워크가 무선 클라이언트에서 기업 네트워크로 보내는 사용자 트래픽을 조직체의 보안 정책에 정의된 대로 감사, 검사, 필터링할 수 있습니다. 장치와 사용자를 인증한 후에, VPN 게이트웨이는 무선 사용자가 연결된 그룹을 기준으로 사용자 권한을 선택적으로 부여할 수 있습니다. VPN 사용자 인증 정책에서 OTP를 사용하지 않기로 선택하는 경우 위에 나오는 모든 향상된 보안 기능을 강력하게 권합니다.

또한, 위에서 설명한 설계 방식보다 강력한 보안 상태를 원하는 네트워크 설계자는 WLAN 액세스를 위하여 물리적으로 분리되어 있는 인프라를 구축하는 방식의 장점을 고려해야 합니다. 전용 네트워킹 하드웨어에 구축된 물리적으로 분리되어 있는 레이어 2 세그먼트와 레이어 3 세그먼트는 VPN 게이트웨이에서 트래픽을 암호화하여 생산 유선 네트워크로 라우팅할 때까지 신뢰할 수 없는 WLAN을 완전히 고립시키는데 사용됩니다.

중형 WLAN 설계

중형 네트워크 WLAN은 SAFE 중형 네트워크 설계의 캠퍼스 부분 위에 무선 네트워크를 배치합니다. 문제 처리 기법을 구현하는데 쓰이는 모든 컴포넌트는 중형 캠퍼스 모듈 내에 들어 있습니다. 이러한 컴포넌트들은 중형 네트워크 캠퍼스 내의 일반 사용자들에게 WLAN 액세스를 허용하기 위한 것입니다. 각 문제 처리 기법을 구현하는 구체적인 방법은 아래에서 자세히 설명합니다.

설계 지침

중형 WLAN 설계에서는, 모든 WLAN 장치가 단일 IP 서브넷에 연결되어 있기 때문에 중형 WLAN 설계 전체에서 일반 사용자 이동성이 가능하다고 가정합니다. 중형 유선 네트워크에서 이용할 수 있는 대부분의 서비스는 중형 WLAN 설계에서도 이용할 수 있도록 설계되었다고 가정합니다. SAFE 중형 네트워크의 설계 기초에 맞추어, 중형 WLAN 설계는 높은 가용성을 제공하지 않습니다. LEAP와 VPN은 모두 중형 WLAN 설계의 구현 가능한 보안 옵션으로 간주됩니다. SAFE 중형 네트워크 설계의 캠퍼스 모듈에서는 LEAP 옵션과 VPN 옵션의 주요 장치들을 모두 지원합니다. 두 가지 옵션 모두, 네트워크 설계자들은 LEAP 솔루션과 VPN WLAN 솔루션이 사용하는 RADIUS 서버와 DHCP 서버의 위치를 특별히 고려해야 합니다. 서버의 위치는 중형 네트워크 WLAN이 대표하는 사무실의 종류, 즉 본사 사무실이냐 지사 사무실이나에 따라 달라집니다. 중형 네트워크가 기업 본사이면, DHCP 서버와 RADIUS 서버는 로컬 네트워크에 배치됩니다. 중형 네트워크가 지사 사무실이면, DHCP 서버와 RADIUS 서버를 본사 사무실에 둘 수 있으며, 연결은 WAN 모듈 또는 기업 인터넷 모듈의 VPN을 통하여 이루어집니다.

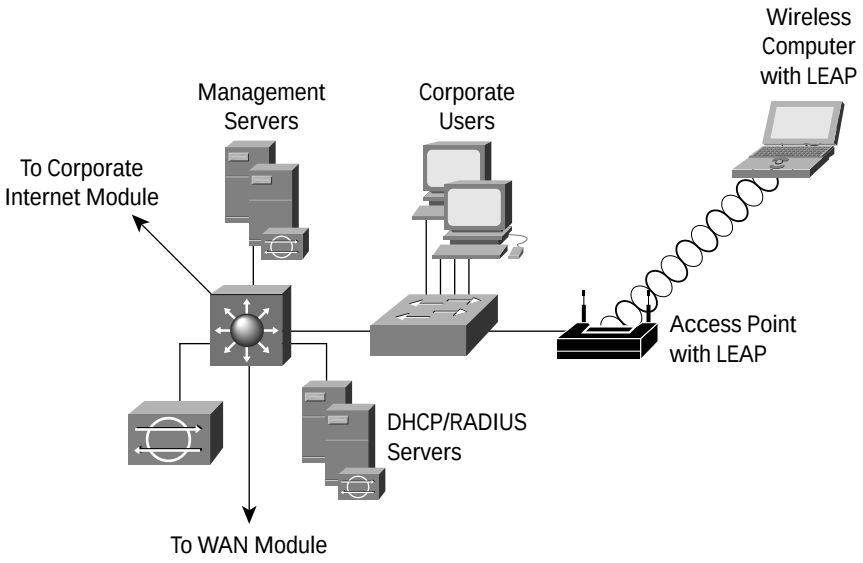
DHCP 서버와 RADIUS 서버가 본사 사무실에 있는 경우, VPN 게이트웨이가 WAN 연결 통로를 잃어버리는 것과 같은 어떤 이류론가 RADIUS 서버와 통신할 수 없다면 액세스 포인트가 로컬 네트워크를 액세스하지 못하게 됩니다. 또한, 중형 네트워크에서 DHCP 서버를 이용할 수 없다면, 무선 클라이언트는 캠퍼스 네트워크와 IP 연결 통로를 만들 수 없습니다. RADIUS 서비스가 장애를 일으키면 네트워크 액세스를 못하게 하는 방법으로 설계에 구현된 보안 수준을 유지합니다. 보안 위험 요소들에 대한 대부분의 처리 방법은 RADIUS 서비스에 의존하므로, 이렇게 해야 합니다. 전반적으로, DHCP 서비스가 장애를 일으키면 솔루션 관리를 하지 못하게 됩니다. 위의 목표를 달성하는 구체적인 방법은 각 문제 처리 기법 섹션에서 상세히 설명합니다.

네트워크 관리

관리 세그먼트에서 AP로 보내는 네트워크 관리 트래픽은 캠퍼스 레이어 3 스위치에서 ACL을 구현하면 네트워크 관리 서브넷으로 제한이 됩니다. 대부분의 AP가 cleartext 관리 프로토콜(HTTP, SNMP, 등등)만 지원하므로, SAFE 중형 네트워크 설계에서 제안하는대로 암호화된 인밴드 관리를 수행할 수 없습니다. 이렇게 구성을 하면 관리 트래픽을 공중으로 각 AP로 보내야 하므로 네트워크 보안에 허점이 생기게 됩니다.

Cisco LEAP 옵션

그림 7: 중형 네트워크 LEAP WLAN 설계



중형 네트워크에서 시스코 LEAP 액세스를 하려면 중형 캠퍼스 모듈의 기존의 레이어 2 액세스 스위치에 연결된 무선 AP가 있어야 합니다. RADIUS 서버와 DHCP 서버도 캠퍼스 모듈에 있지만, 중앙의 캠퍼스 레이어 3 스위치에 있는 별도의 레이어 3 서브넷은 분리되어 있습니다. 무선 LEAP 사용자들이 중형 캠퍼스 네트워크를 액세스하려면 DHCP와 RADIUS 인증 서비스가 필요합니다. 중형 네트워크가 지사 사무실이라면, DHCP 서버와 RADIUS 서버를 본사 사무실에 둘 수 있습니다.

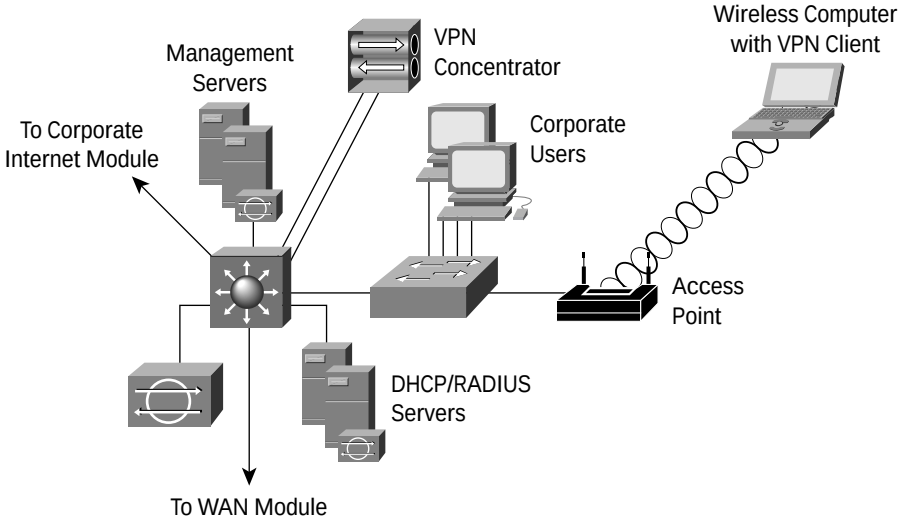
중형 네트워크를 액세스하는 과정은 표준 WLAN 설계 지침에서 약술한 것과 동일합니다.

대안

대형 LEAP WLAN 설계에서 언급한 것처럼, 네트워크 설계자들은 무선 클라이언트가 웹 브라우징과 같은 기본 수준의 보안으로 충분한 애플리케이션만 액세스하도록 제한하는 정책을 만들어서 WLAN의 보안 수준을 더욱 향상시키는 방법을 선택할 수 있습니다. 그 다음에 LEAP 외에 IPSec를 사용하여 중요한 업무 시스템 액세스를 허용할 수 있습니다. 그림 8은 중형 WLAN 설계의 IPSec를 자세히 표현한 것입니다.

IPSec VPN 옵션

그림 8: 중형 네트워크 VPN WLAN 설계



중형 네트워크의 IPSec VPN 옵션은 대형 WLAN 설계를 위한 VPN 옵션과 아주 비슷합니다. 주된 차이는 무선 네트워크와 무선 네트워크를 분리시키는 VPN 게이트웨이의 물리적인 연결 통로에 있습니다. VPN 게이트웨이는 두 가지 VLAN을 사용하여 캠퍼스 모듈 레이어 3 스위치에 인터페이스를 연결시킵니다. 이 제안이 핵심 SAFE 보안 문서의 "스위치가 타겟이다" 기본 원칙와 직접 충돌한다는 점에 유의해야 합니다. 보안 역할에서 VLAN을 사용하는 것은 보안 경계선을 확장시켜 스위치 자체를 포함시키는 효과적인 방법입니다. 해커는 스위치를 장악하여 VPN 집중기를 우회할 수 있습니다. 이러한 VLAN 기반 옵션을 선택한 이유는 여기서 설명한 대안이 재정적인 이유에서 기업체들이 중형 네트워크를 배치할 가능성이 없었기 때문입니다. 가외의 장비를 더 사용하는 보안이 보다 확실한 옵션은 아래의 대안을 참조하십시오.

VPN 게이트웨이는 무선 액세스 포인트에 연결할 수 있는 하나의 VLAN에 공개 인터페이스를 연결합니다. VPN 게이트웨이의 비공개 인터페이스는 유선 네트워크를 액세스하는 VLAN에 연결됩니다. 무선 AP는 전용 VLAN의 캠퍼스 모듈 액세스 레이어에 있는 기존의 레이어 2 스위치에 연결이 되어 WLAN에서부터 VPN 연결 통로가 있는 VLAN으로 트래픽을 포워딩합니다. 대형 WLAN과 일반적인 VPN WLAN 설계처럼, 빌딩 분배 모듈 레이어 3 스위치에는 VPN 연결과 관리에 필요한 프로토콜만 허용하는 ACL을 설정합니다.

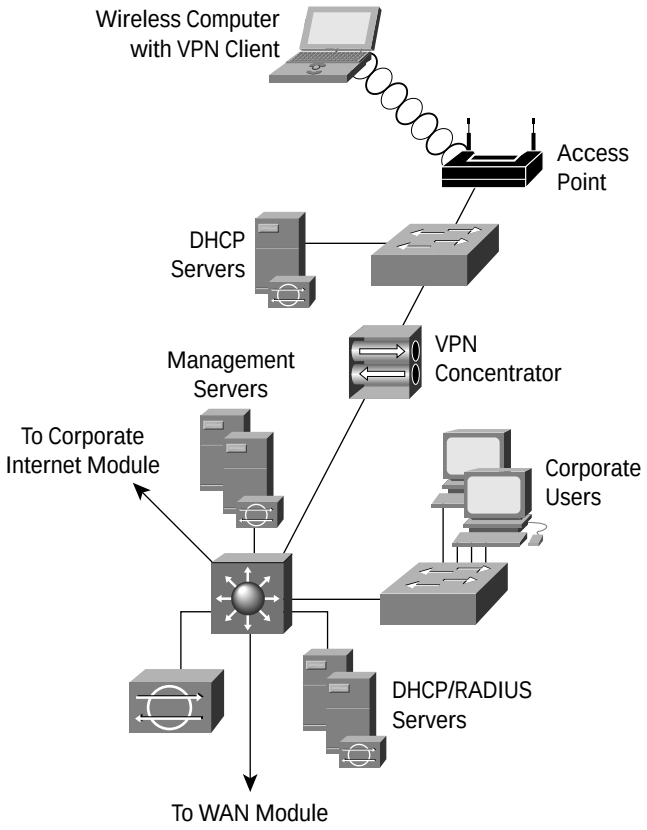
무선 클라이언트는 무선 VPN 게이트웨이로 IPSec 연결 통로를 만듭니다. 그렇게 하는 과정에서, VPN 게이트에이는 IPSec VPN을 통하여 장치와 사용자를 인증합니다. VPN 게이트웨이는 무선 클라이언트 장치 인증을 위하여 디지털 인증서나 사전 공유 키를 사용할 수 있습니다. VPN 최종 사용자는 OTP를 사용하여 VPN 게이트웨이에 인증을 합니다. VPN 게이트웨이는 RADIUS 서비스를 사용하며, RADIUS 서비스는 OTP 서버에 연결하여 사용자를 인증합니다. VPN 게이트웨이는 WLAN 클라이언트가 VPN 터널을 통하여 통신을 할 수 있도록 DHCP를 사용하여 IP 주소 지정 정보를 알아냅니다.

대안

무선 사용자 트래픽이 생산 유선 네트워크로 들어오기 전에 VPN 게이트웨이 뒤에 NIDS와 방화벽을 배치하면 보안 상태를 더욱 향상시킬 수 있습니다. 이렇게 설정하면 조직체의 보안 정책에서 정의된대로 무선 클라이언트에서 중형 네트워크로 전송되는 사용자 트래픽을 네트워크가 감사, 검사, 필터링할 수 있습니다. VPN 사용자 인증 정책에서 OTP를 사용하지 않기로 선택하는 경우, 위의 두 가지 향상된 보안 방식을 모두 사용하도록 강력히 권합니다.

또한, 위의 설계보다 강력한 보안을 찾고 있는 네트워크 설계자는 표준 VPN WLAN 옵션과 비슷한 설계의 장점을 고려해야 합니다. 중형 WLAN과 관련된 설계는 그림 9에 나옵니다. 제일 큰 장점은 VPN 게이트웨이의 공개 인터페이스와 비공개 인터페이스 사이를 명확하게 구분짓는 것입니다. 이 설계의 주된 장애 요소는 단순히 무선 AP를 연결하기 위해서 레이어 2 스위치를 추가 배치하고 WLAN 클라이언트 장치의 IP 구성에 필요한 전용 DHCP 서버를 배치하면서 발생할 가능성이 있는 많은 비용입니다.

그림 9: 중형 네트워크 VPN WLAN 설계



소형 WLAN 설계

소형 WLAN 설계는 SAFE 소형 네트워크 설계 위에 WLAN을 배치하는 것입니다. 소형 WLAN 설계는 캠퍼스 모듈 안에 들어 있습니다. 이 섹션에서는 WLAN 사용자에게 유선 캠퍼스 연결 통로를 마련해 주는 LEAP 옵션에 대해 설명합니다. IPSec는 이 정도 규모의 네트워크에 전용 WLAN VPN을 구현하는 것과 관련된 재정적인 부담 때문에 옵션으로 제시하지 않습니다.

설계 지침

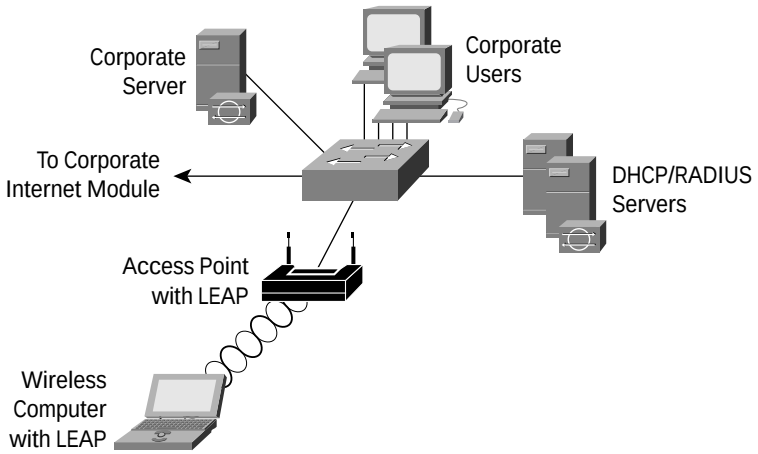
이어지는 내용에서는 소형 WLAN 설계를 상세하게 설명합니다. 소형 네트워크 설계에는 캠퍼스 연결을 위한 레이어 2 스위치가 하나 있으므로, 모든 장치들에는 액세스 포인트 로밍이 가능한 하나의 IP 서브넷 네트워크가 있다고 가정합니다.

네트워크 관리

관리 호스트에서 AP로 보내는 네트워크 관리 트래픽은 소규모 캠퍼스에 레이어 3 장치가 없기 때문에 제한이 되지 않습니다. 관리 트래픽은 공중을 통해 각 AP로 전달되며, SAFE 소형 설계의 나머지 부분에서도 마찬가지입니다.

시스코 LEAP 옵션

그림 10: 소형 네트워크 LEAP WLAN 설계



소형 WLAN 설계에서 시스코 LEAP 액세스에는 소형 캠퍼스 모듈에 이미 존재하는 레이어 2 액세스 스위치에 무선 AP들이 연결되어 있습니다. 무선 LEAP 사용자들이 소형 캠퍼스 네트워크를 액세스하려면 DHCP와 RADIUS 인증 서비스가 필요합니다. 소형 네트워크의 단일 사이트 특성 때문에, RADIUS 서버와 DHCP 서버는 캠퍼스 모듈의 레이어 2 스위치에 로컬 방식으로 연결되어 있습니다.

소형 네트워크를 액세스하는 과정은 표준 WLAN 설계 지침에서 약술한 바와 동일합니다.

대안

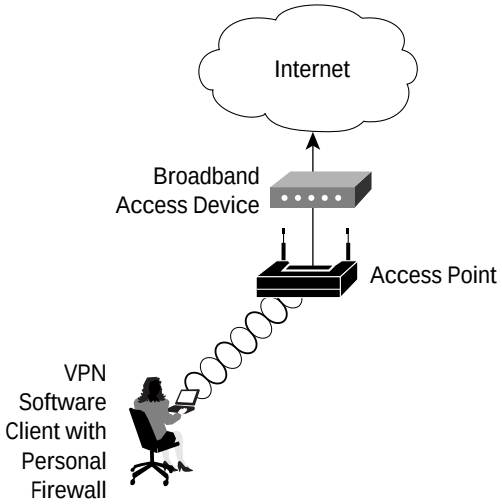
권장하는 것은 아니지만, 주요 배포 문제를 관리하는데 별 어려움이 없다면, (앞서 언급된 암호 해독 방식이 수정된) 정적인 WEP를 LEAP이 대안으로 사용할 수 있습니다.

원격 WLAN 설계

원격 WLAN 설계는 SAFE가 정의한 두 가지 종류의 주요 원격 VPN 연결 통로, 즉 소프트웨어 기반 VPN과 하드웨어 기반 VPN을 위한 원격 무선 솔루션을 보여줍니다. 이 섹션에서는 WLAN 사용자에게 SAFE 설계 내의 중심 사무실(중소기업이나 대기업) 연결 통로를 마련해 주는 이 두 가지 옵션에 대해 설명합니다.

소프트웨어 VPN 원격 WLAN 설계

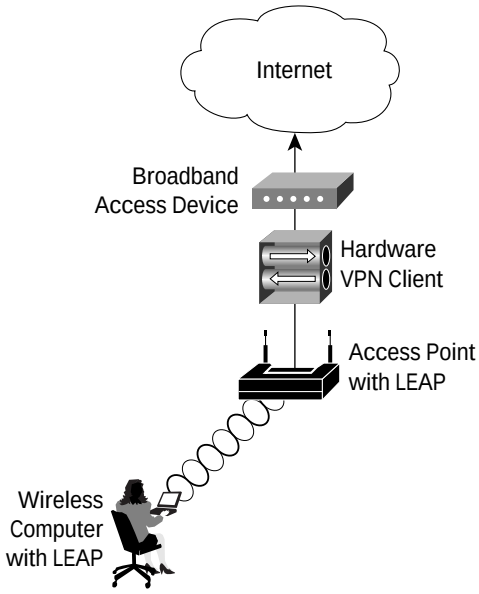
그림 11: 소프트웨어 VPN 원격 네트워크 WLAN 설계



무선 사용자에게 무선 장치에서 기업 네트워크로 연결되는 보안이 필요한 경우에는 원격 네트워크의 IPSec VPN 옵션이 바람직합니다. 이것은 원격 위치에 IT 관리 하드웨어 리소스가 없는 원격 작업자들에게 가장 흔한 구성입니다. 시간제 재택근무자들이 이 범주에 속합니다. 개인 방화벽 소프트웨어를 갖춘 VPN 클라이언트를 통하여 보안을 처리하기 때문에 광대역 장치 연결이 가능한 거의 모든 구성으로 AP를 설정할 수 있습니다.

하드웨어 VPN 원격 WLAN 설계

그림 12: 하드웨어 VPN 원격 네트워크 WLAN 설계



조직체의 IT 부서가 사용자의 원격 위치에서 VPN과 무선 기어를 관리하는 구성의 경우, PC에서 AP까지는 LEAP을 사용하고 하드웨어 VPN 장치에서 중앙의 사무실까지는 IPSec를 사용하면 원격 작업자를 위한 강력한 보안 수준이 마련됩니다. 이런 시스템 구

원격 위치가 무선 통신을 위하여 하드웨어 VPN과 LEAP을 사용하는 경우, 설계는 소형 WLAN 설계와 거의 동일합니다. RADIUS 액세스와 관련된 동일한 주의 사항이 적용된다는 점을 기억해야 합니다. IPSec VPN 연결 통로가 없어지는 것과 같은 어떤 이유에선가 액세스 포인트가 RADIUS 서버와 통신을 할 수 없다면 무선 사용자의 로컬 네트워크 액세스가 거부됩니다. 이 설계에서는 원격 네트워크에 원격 AP의 IT 관리가 원활하게 이루어질 수 있는 고유한 IP 범위가 있어야 합니다. 하드웨어 장치가 원격 사이트에서 한 IP 주소로 보내는 모든 트래픽에 대해 NAT(Network Address Translation)를 사용한다면, IT 부서는 AP를 관리할 수 없습니다.

부록 A: 검증 랩

본 문서에서 설명한 기능을 검증하는 레퍼런스 SAFE WLAN 구현 형태가 존재합니다. 본 부록에서는 각 모듈 내에서 WLAN 기능과 관련이 있는 특정한 장치들의 구성과 일반적인 장치 구성에 대한 전반적인 지침을 상세하게 설명합니다. 다음은 랩에서 실제로 사용되는 장치들의 시스템 구성 스냅샷입니다. 이러한 구성을 생산 네트워크에 직접 적용하는 것은 바람직하지 않습니다.

전반적인 지침

이 섹션에서 제시된 명령 샘플은 부분적으로 본 문서의 앞 부분에서 제시된 SAFE WLAN 설계 지침에 대응이 됩니다.

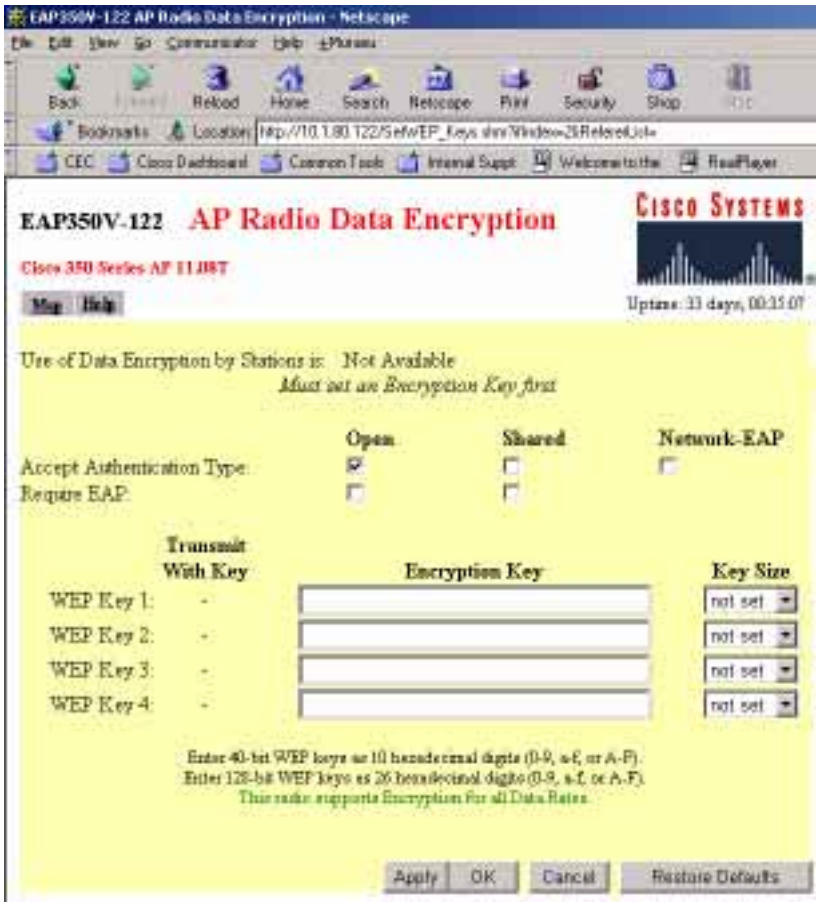
액세스 포인트를 위한 SAFE WLAN 표준 구성

이어지는 내용에서는 본 문서의 기본 원칙 섹션과 설계 지침 섹션에서 상세히 설명한 것처럼 VPN이나 (화면 캡춰에 나오는) LEAP을 사용하기 위해 AP에 필요한 샘플 구성을 상세히 설명합니다. 샘플 구성 화면 캡춰는 대기업체 설계에서 잡은 것입니다. 하지만, VPN AP(또는 LEAP AP)의 시스템 구성은 모든 설계에서 동일합니다.

VPN 액세스 포인트

그림 A-1에 나오는 것처럼, AP는 개방형 인증이 가능하도록 구성되어 있으며, 유선 네트워크에 인증을 하는 VPN 무선 클라이언트에 대해서는 WEP 암호화를 사용하지 않습니다.

그림 A-1: VPN 액세스 포인트의 WEP 구성



LEAP 액세스 포인트

그림 A-2에는 LEAP 무선 클라이언트를 RADIUS 서버가 인증할 수 있도록 구성된 AP의 Authenticator Configuration 창(Setup 〉〉 Security 섹션 밑)이 나옵니다. RADIUS 서버 자체나 (Windows NT 서버와 같은) 네트워크 OS 서버에는 유효한 사용자와 그 사용자의 비밀번호로 이루어진 데이터베이스가 들어 있다고 가정합니다.

그림 A-2: LEAP 액세스 포인트의 Authenticator Configuration 창

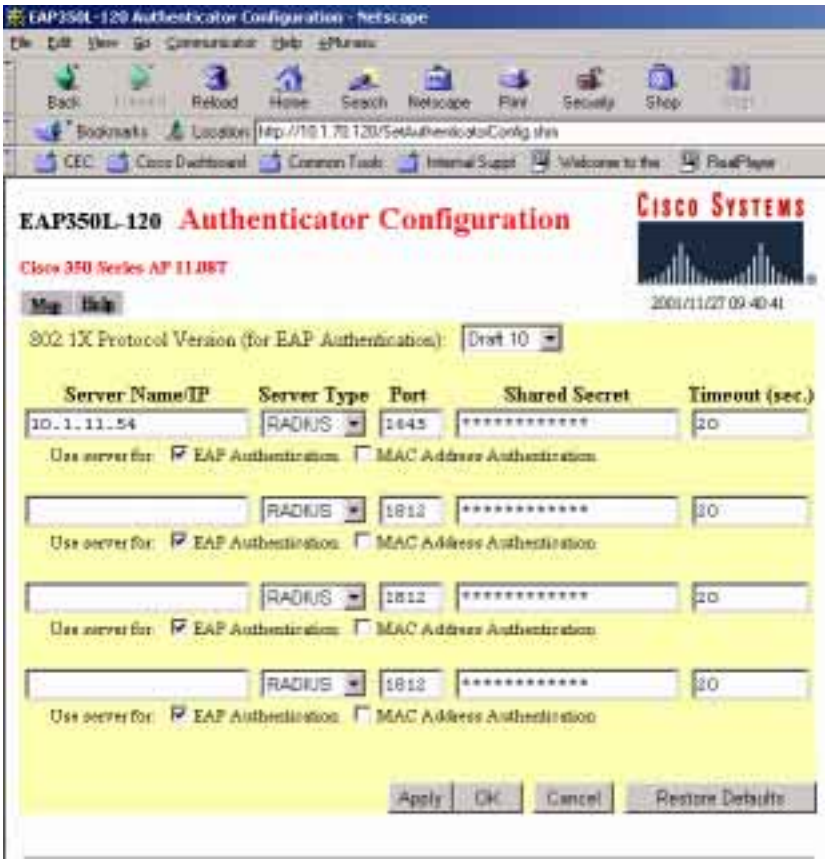
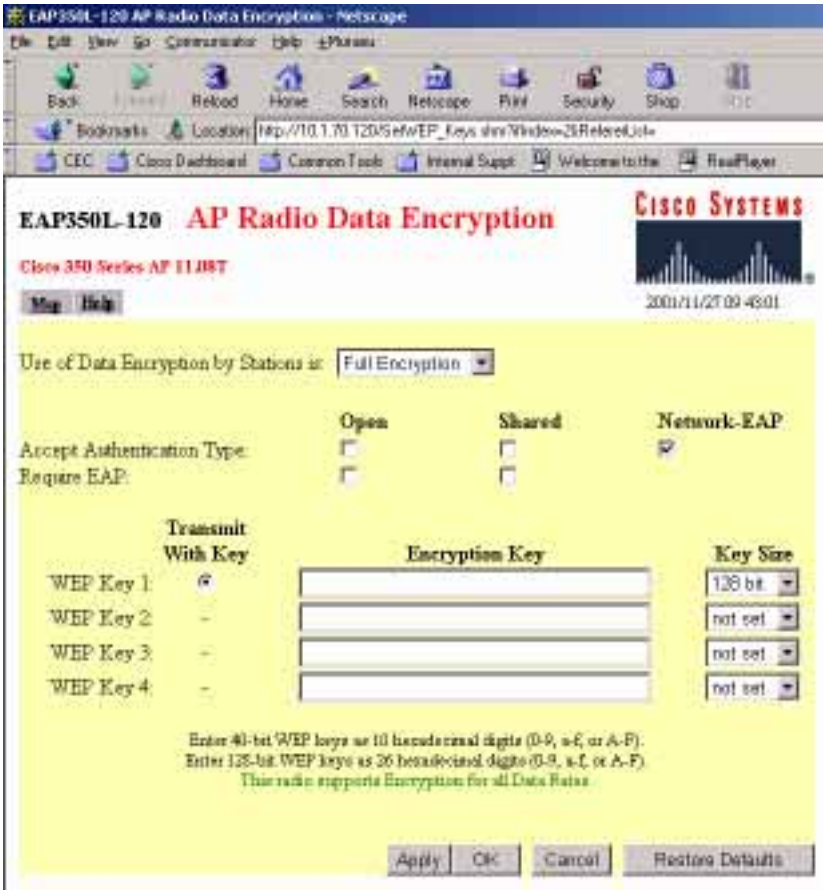


그림 A-3은 AP의 WEP 구성을 보여줍니다. AP는 "Full Encryption" (WEP)을 시행할 뿐만 아니라, 액세스 포인트를 이용하면 네트워크 EAP가 유일한 인증 방식이 되게 할 수도 있습니다. 게다가, AP에 대해 128 비트 WEP 키(Key 1)가 (브로드캐스트 키로 사용되도록) 설정되어 있습니다.

그림 A-3: LEAP 액세스 포인트의 WEP 구성



클라이언트를 위한 SAFE 무선 LAN 표준 구성

이어지는 내용에서는 본 문서의 기본 원칙 섹션과 설계 지침 섹션에서 상세히 설명한 것처럼 무선 클라이언트가 (화면 캡춰에 나오는) VPN이나 LEAP을 사용할 수 있게 하는데 필요한 샘플 구성을 상세히 설명합니다. 샘플 구성 화면 캡춰는 대기업체 설계에서 잡은 것입니다. 하지만, VPN 무선 클라이언트 (또는 LEAP 무선 클라이언트)의 시스템 구성은 모든 설계에서 동일합니다.

VPN 클라이언트

VPN 클라이언트를 사용하여 유선 네트워크에 연결하는 무선 사용자의 경우, 무선 클라이언트에서는 WEP과 LEAP을 사용하지 않도록 설정되어 있습니다. 그림 A-4와 A-5는 샘플 셋업입니다:

그림 A-4: VPN 클라이언트의 시스템 파라미터 구성

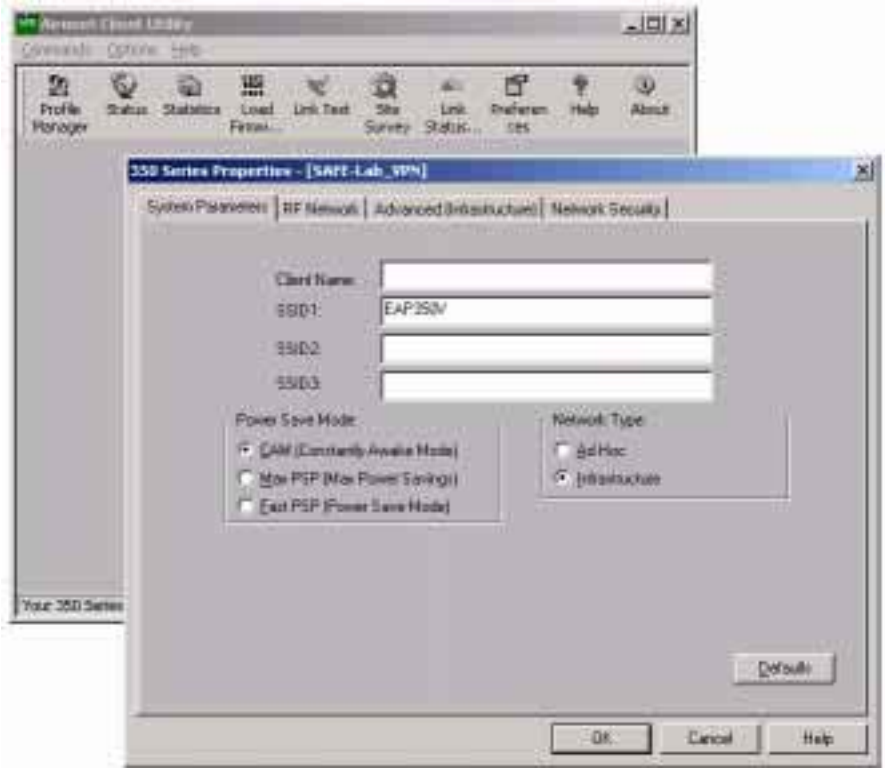
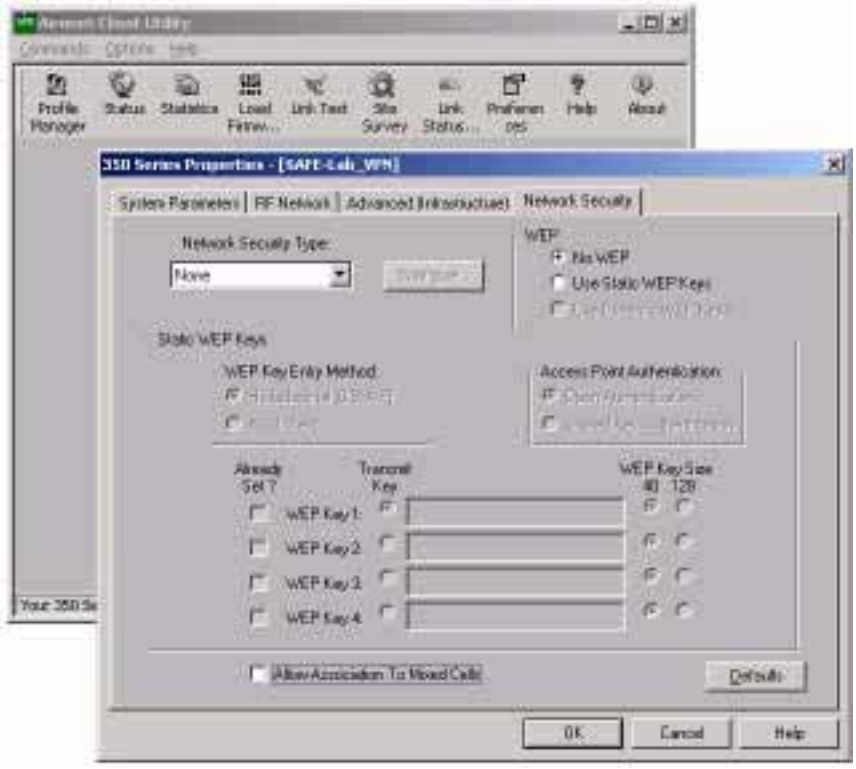


그림 A-5: VPN 클라이언트의 네트워크 보안 구성



본 문서의 설계 섹션에서 설명한 것처럼, VPN AP에는 기업체의 무선 사용방법 정책을 기준으로 ethertype, 프로토콜, 포트 필터 등이 구성되어 있어야 합니다. SAFE WLAN은 VPN 게이트웨이로 연결되는 안전한 터널을 만드는데 필요한 프로토콜만 허용하는 제한적인 필터를 권장합니다. 다음 표는 VPN AP의 무선 인터페이스에서 설정할 인바운드(수신) 필터와 아웃바운드(송신) 필터 목록입니다:

표 A-1-VPN AP 무선 프로토콜 필터-인바운드 (수신)

필터 종류	프로토콜	값	Disposition
Ethertype	ARP	0x0806	포워드
Ethertype	IP	0x0800	포워드
IP 프로토콜	UDP	17	포워드
IP 프로토콜	ESP	50	포워드
IP 포트	BootPC	68	포워드
IP 포트	DNS	53	포워드
IP 포트	IKE	500	포워드

표 A-2-VPN AP 무선 프로토콜 필터-아웃바운드 (송신)

필터 종류	프로토콜	값	Disposition
Ethertype	ARP	0x0806	포워드
Ethertype	IP	0x0800	포워드
IP 프로토콜	UDP	17	포워드
IP 프로토콜	ESP	50	포워드
IP 포트	BootPS	67	포워드
IP 포트	DNS	53	포워드
IP 포트	IKE	500	포워드

위의 필터 세트를 만들 때, 반드시 다음에 유의해야 합니다.

- 설치된 필터의 "Default Disposition"을 "block"으로 설정해야 합니다.
- "Special Cases"에 (위의 표에 나오는) 지정된 값을 추가하고 각 special case에 대해 Disposition으로 "forward"를 선택하여 특정한 트래픽 유형이 흐를 수 있게 해야 합니다

모든 필터 세트를 만든 다음, 반드시 그 필터 세트를 AP의 무선 인터페이스에 적용하십시오 (Setup 〉〉 (AP Radio) Filters)

LEAP 클라이언트

Aironet? 클라이언트 유틸리티를 사용하여 LEAP와 WEP를 사용하도록 설정하면 무선 클라이언트가 LEAP에 맞게 구성됩니다. 그림 A-6, A-7, 그리고 A-8은 LEAP 클라이언트의 샘플 구성입니다.

그림 A-6: LEAP 무선 클라이언트의 시스템 파라미터 구성

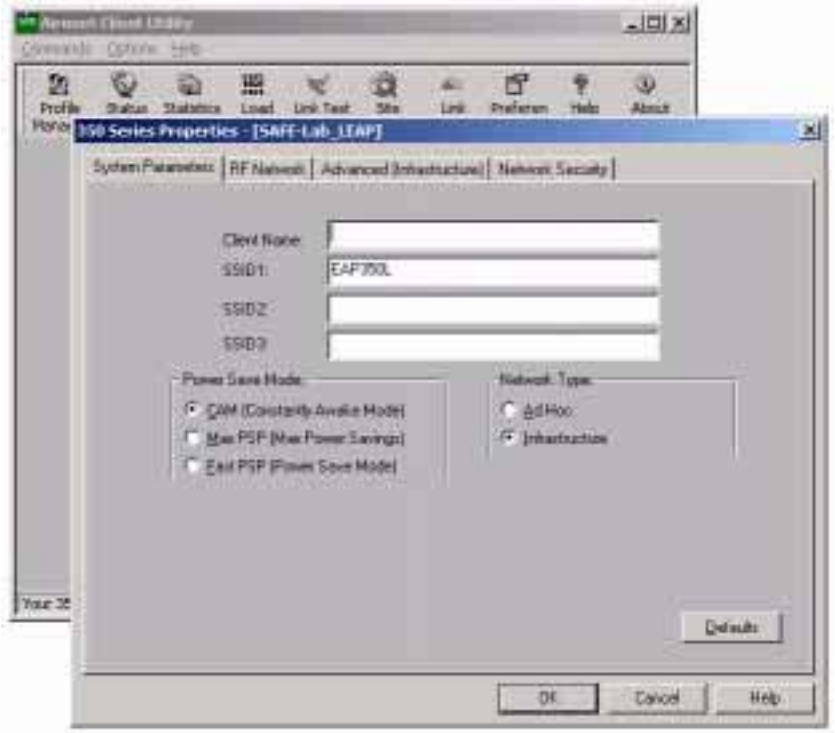


그림 A-7: LEAP 무선 클라이언트의 네트워크 보안 구성

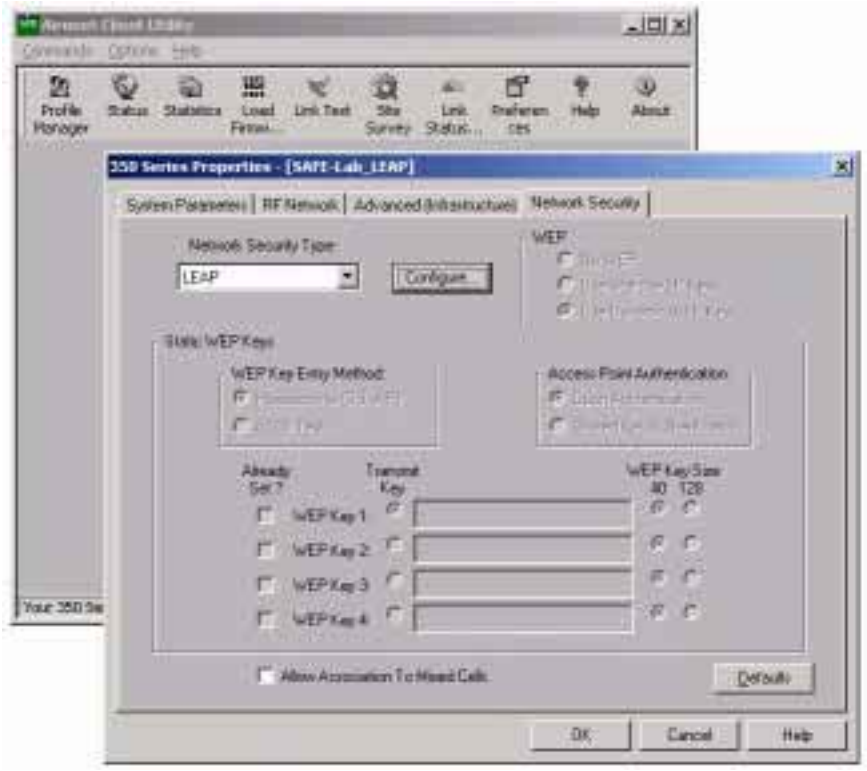
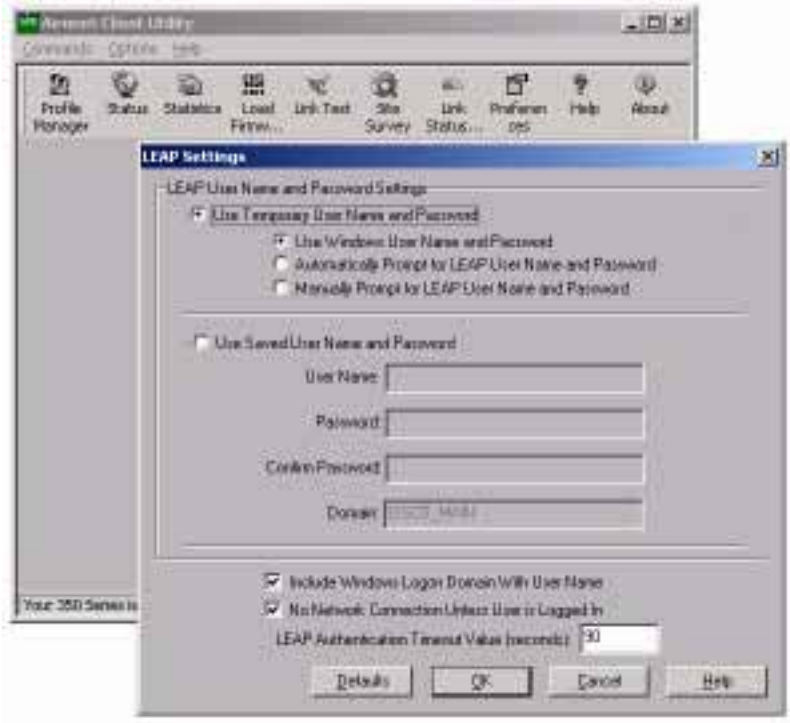


그림 A-8: LEAP 무선 클라이언트의 LEAP 셋팅 구성



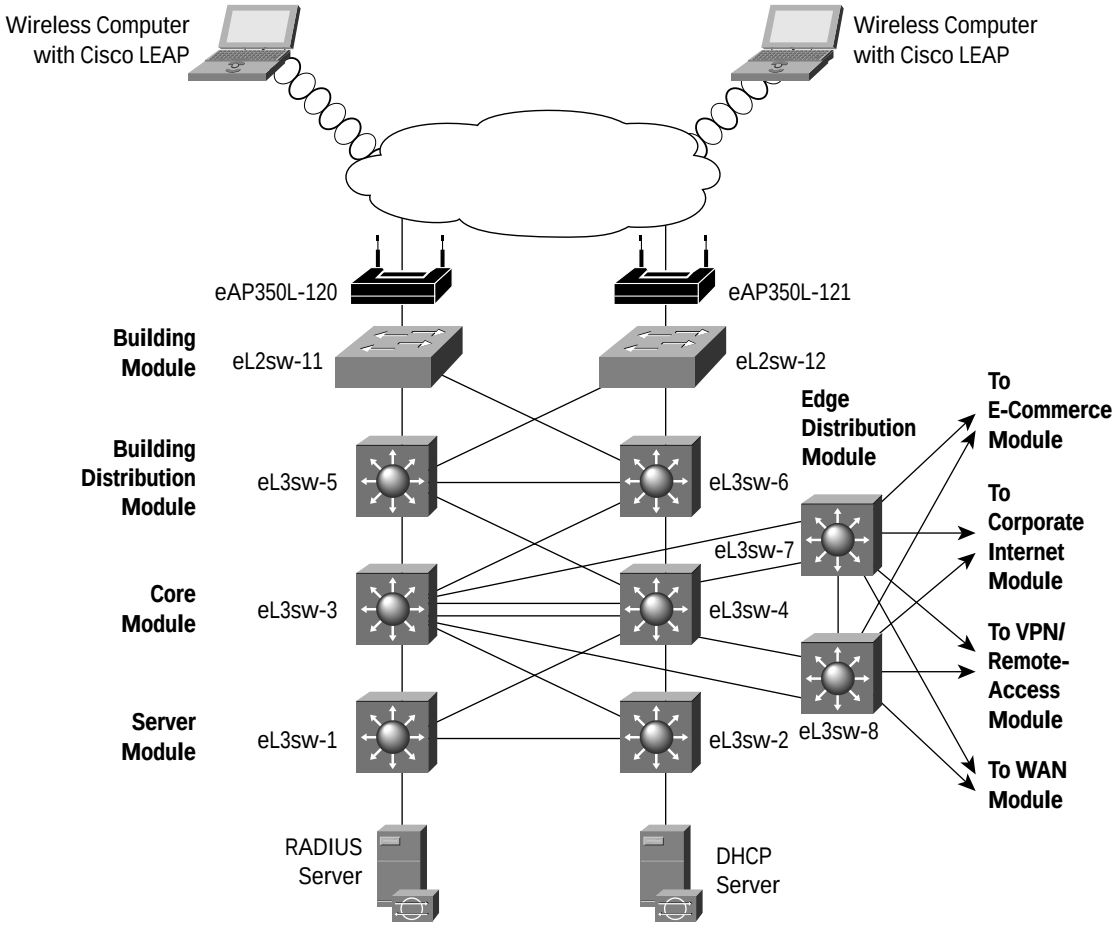
대기업체 설계 모듈 구성

이 섹션에서는 대기업체 네트워크 설계의 엔드 투 엔드 LEAP 및 VPN 아키텍처 구성을 상세히 설명합니다.

LEAP 아키텍처

다음은 SAFE 대기업체 LEAP WLAN 설계의 시스템 구성 스냅샷입니다. 그림 A-9는 대기업체 네트워크의 LEAP 설계입니다.

그림 A-9: 대기업체 LEAP WLAN 설계



사용된 제품의 일부는 다음과 같습니다:

- Cisco Catalyst 6506 레이어 3 스위치 (eL3sw-1에서 eL3sw-8까지)
- Cisco Catalyst 4003 레이어 2 스위치 (eL2sw-11에서 L2sw-12까지)
- Cisco Aironet 350 액세스 포인트 및 클라이언트 (eAP350L-120에서 121까지 및 무선 클라이언트)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP 서버

이어지는 내용에서는 SAFE WLAN 대형 네트워크 설계와 관련된 구성을 설명합니다. 대기업체 네트워크에 대한 일반적인 네트워크 구성 지침은, "Cisco SAFE: A Security Blueprint for Enterprise Networks"를 참조하십시오.

eL3sw-5와 eL3sw-6 (WLAN 빌딩 모듈에서 빌딩 분배 모듈 상호 연결까지):

```
! AP는 캠퍼스 네트워크의 독립적인 VLAN에 배치됩니다
interface Vlan70
  ip address 10.1.70.5 255.255.255.0
  ip access-group 170 in
  ip access-group 171 out
  ip helper-address 10.1.11.50
  no cdp enable

! AP 뒤에 있는 클라이언트에서 보호형 유선 세그먼트의 클라이언트로 보내는 모든 트래픽을 거부합니다
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.5.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.6.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.7.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.8.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.15.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.16.0 0.0.0.255 log
access-list 170 deny ip 10.1.70.0 0.0.0.255 10.1.80.0 0.0.0.255 log

! DHCP 요청과 BOOTP 요청만이 DHCP 서버로 전달되도록 허용됩니다
access-list 170 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

! 유효한 IP 주소를 지닌 사용자가 보낸 트래픽을 허용하고 그 외의 트래픽을 전부 거부합니다
access-list 170 permit ip 10.1.70.0 0.0.0.255 any
access-list 170 deny ip any any log

! 보호형 유선 서브넷에서 무선 클라이언트로 보내는 모든 트래픽을 거부합니다
access-list 171 deny ip 10.1.5.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.6.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.7.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.8.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.15.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.16.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.70.0 0.0.0.255 10.1.70.0 0.0.0.255 log
access-list 171 deny ip 10.1.80.0 0.0.0.255 10.1.70.0 0.0.0.255 log

! 관리를 위하여 AP로 나가는 웹 트래픽을 허용합니다
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.120 eq www
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.121 eq www

! AAA 서버에서 보내는 RADIUS 응답을 허용합니다
access-list 171 permit udp host 10.1.11.54 eq 1645 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.11.54 eq 1645 host 10.1.70.121 gt 1023

! AP로 보내는 그 외의 모든 IP 트래픽을 거부합니다
access-list 171 deny ip any host 10.1.70.120 log
access-list 171 deny ip any host 10.1.70.121 log

! 유선 네트워크에서 무선 네트워크로 보내는 모든 IP 트래픽을 허용합니다
access-list 171 permit ip any 10.1.70.0 0.0.0.255
access-list 171 deny ip any any log
```

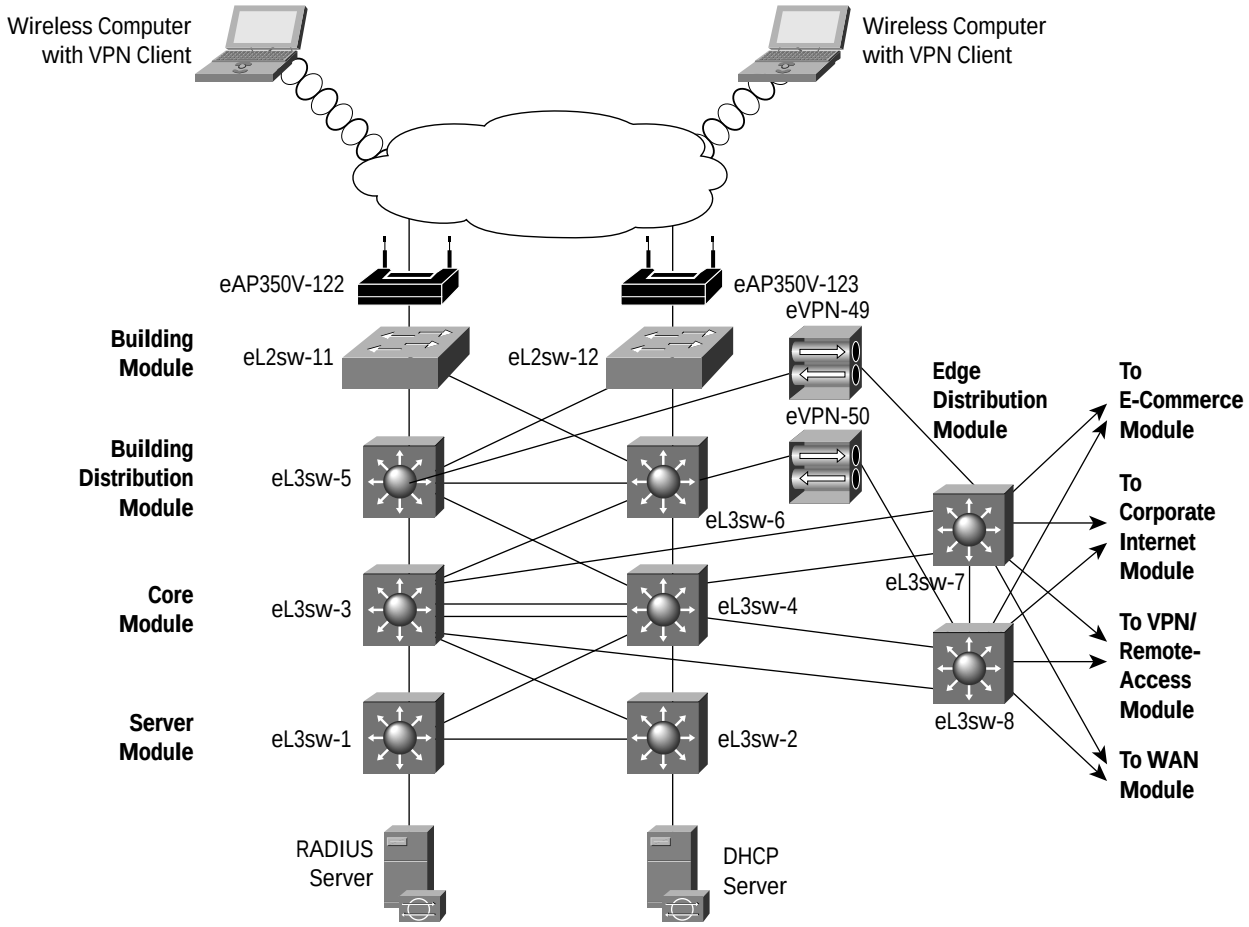
eAP350L-120에서 121까지 및 무선 클라이언트:

LEAP에 맞게 AP와 무선 클라이언트를 구성하는 것에 대해서는 본 부록의 "전반적인 지침" 섹션의 구성 샘플을 참조하십시오.

VPN 아키텍처

다음은 SAFE 대기업체 VPN WLAN 설계의 시스템 구성 스냅샷입니다. 그림 A-10은 대기업체의 WLAN을 위한 VPN 설계입니다.

그림 A-10: 대기업체 VPN WLAN 설계



사용된 제품의 일부는 다음과 같습니다:

- Cisco Catalyst 6506 레이어 3 스위치 (eL3sw-1에서 eL3sw-8까지)
- Cisco Catalyst 4003 레이어 2 스위치 (eL2sw-9에서 eL2sw-14까지)
- Cisco VPN 3015 Concentrator (eVPN-49에서 50까지)
- Cisco Aironet 350 액세스 포인트 및 클라이언트 (eAP350V-122에서 123까지 및 무선 클라이언트)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP 서버
- Cisco IDS Host Sensor

이어지는 내용에서는 SAFE WLAN 대형 네트워크 설계와 관련된 구성을 설명합니다. 대기업체 네트워크에 대한 일반적인 네트워크 구성 지침은, "Cisco SAFE: A Security Blueprint for Enterprise Networks"를 참조하십시오.

eL3sw-5와 eL3sw-6 (WLAN 빌딩 모듈에서 빌딩 분배 모듈 상호 연결):

```
! AP는 캠퍼스 네트워크의 독립적인 VLAN에 배치됩니다
interface Vlan80
  ip address 10.1.80.5 255.255.255.0
  ip access-group 180 in
  ip access-group 181 out
  ip helper-address 10.1.11.50
  no cdp enable

! VPN 게이트웨이 서브넷으로 보내는 IPSec 트래픽을 허용합니다
access-list 180 permit esp 10.1.80.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq isakmp 10.1.50.0 0.0.0.255 eq isakmp

! 문제 해결을 위한 Full ICMP를 허용합니다
access-list 180 permit icmp 10.1.80.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 180 permit icmp 10.1.80.0 0.0.0.255 host 10.1.80.5

! 무선 클라이언트의 초기 IP 할당을 위한 DHCP 요청을 허용합니다
access-list 180 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.1.80.0 0.0.0.255 eq bootpc host 10.1.11.50 eq bootps

! 관리를 위하여 AP에서 보내는 웹 응답을 허용합니다
access-list 180 permit tcp host 10.1.80.122 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 180 permit tcp host 10.1.80.123 eq www 10.1.20.0 0.0.0.255 gt 1023 established

! 그 외의 모든 트래픽을 거부합니다. Windows 파일 공유 브로드캐스트를 로그 처리하지 마십시오
access-list 180 deny udp 10.1.80.0 0.0.0.255 any eq netbios-ns
access-list 180 deny udp 10.1.80.0 0.0.0.255 any eq netbios-dgm
access-list 180 deny ip any any log

! 무선 서브넷으로 보내는 IPSec 트래픽을 허용합니다
access-list 181 permit esp 10.1.50.0 0.0.0.255 10.1.80.0 0.0.0.255
access-list 181 permit udp 10.1.50.0 0.0.0.255 eq isakmp 10.1.80.0 0.0.0.255 eq isakmp

! 문제 해결을 위한 Full ICMP를 허용합니다
access-list 181 permit icmp 10.1.50.0 0.0.0.255 10.1.80.0 0.0.0.255

! 무선 클라이언트의 초기 IP 할당을 위한 DHCP 응답을 허용합니다
access-list 181 permit udp host 10.1.11.50 eq bootps host 255.255.255.255 eq bootpc
access-list 181 permit udp host 10.1.11.50 eq bootps 10.1.80.0 0.0.0.255 eq bootpc

! 관리를 위하여 AP로 들어오는 웹 응답을 허용합니다
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.122 eq www
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.123 eq www

! 그 외의 모든 트래픽을 거부합니다
access-list 181 deny ip any any log
```

eAP350V-122에서 123까지 및 무선 클라이언트

WLAN을 통한 VPN 연결을 하도록 AP와 무선 클라이언트를 설정하려면 본 부록의 "전반적인 지침" 섹션의 구성 샘플을 참조하십시오.

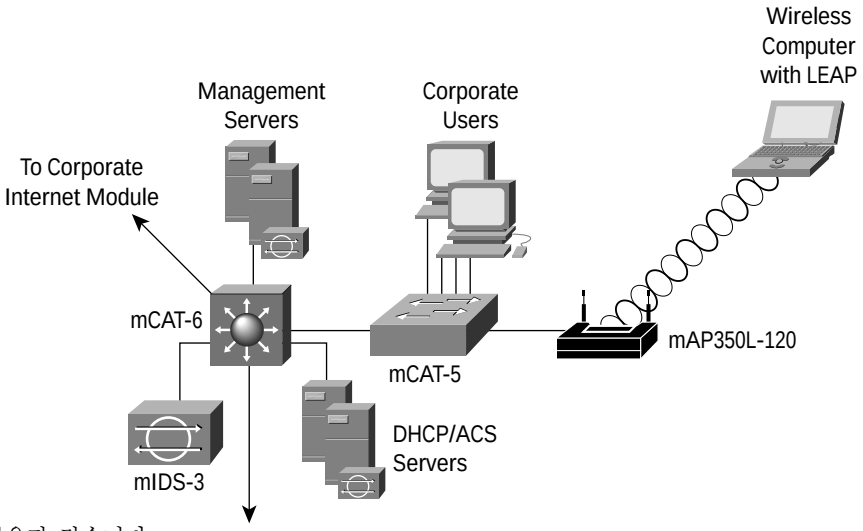
중형 네트워크 구성

이 섹션에서는 중간 규모 기업체 네트워크 설계의 엔드 투 엔드 LEAP 및 VPN 아키텍처 구성을 상세히 설명합니다.

LEAP 아키텍처

다음은 LEAP 옵션을 사용하는 SAFE 중간 규모 기업체 WLAN 설계의 시스템 구성 스냅샷입니다. 그림 A-11은 중간 규모 기업체 네트워크의 LEAP WLAN 설계입니다.

그림 A-11: 중형 LEAP WLAN 설계



사용된 제품의 일부는 다음과 같습니다:

- Cisco Catalyst 레이어 3 스위치 (mCAT-6)
- Cisco Catalyst 레이어 2 스위치 (mCAT-5)
- Cisco Aironet 액세스 포인트와 클라이언트 (mAP350L-120과 무선 클라이언트)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP 서버

이어지는 내용에서는 SAFE WLAN 중형 네트워크 설계(LEAP 옵션 사용)와 관련된 구성을 설명합니다. 중간 규모 기업체 네트워크에 대한 일반적인 네트워크 구성 지침은, "SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks"를 참조하십시오.

MCAT-6:

```
! AP가 중간 규모 기업체 네트워크의 독립적인 VLAN에 배치됩니다
interface Vlan70
  ip address 10.3.70.1 255.255.255.0
  ip access-group 170 in
  ip access-group 171 out
  ip helper-address 10.3.2.50
  no ip redirects
  no cdp enable

! AP 뒤에 있는 클라이언트에서 보호형 유선 세그먼트의 클라이언트로 보내는 모든 트래픽을 거부합니다
access-list 170 deny ip 10.3.70.0 0.0.0.255 10.3.1.0 0.0.0.255

! DHCP 요청과 BOOTP 요청만이 DHCP 서버로 전달되도록 허용됩니다
access-list 170 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

! 유효한 IP 주소를 지닌 사용자가 보낸 트래픽을 허용하고 그 외의 트래픽을 전부 거부합니다
access-list 170 permit ip 10.3.70.0 0.0.0.255 any
access-list 170 deny ip any any log

! 보호형 유선 서브넷에서 무선 클라이언트로 보내는 모든 트래픽을 거부합니다
access-list 171 deny ip 10.3.1.0 0.0.0.255 10.3.70.0 0.0.0.255 log
access-list 171 deny ip 10.3.70.0 0.0.0.255 10.3.70.0 0.0.0.255 log
access-list 171 deny ip 10.3.80.0 0.0.0.255 10.3.70.0 0.0.0.255 log

! 관리를 위하여 AP로 나가는 웹 트래픽을 허용합니다
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq www

! AAA 서버에서 보내는 RADIUS 응답을 허용합니다
access-list 171 permit udp host 10.3.8.253 eq 1645 host 10.3.70.120 gt 1023

! AP로 보내는 그 외의 모든 IP 트래픽을 거부합니다
access-list 171 deny ip any host 10.3.70.120 log

! 유선 네트워크에서 무선 네트워크로 보내는 모든 IP 트래픽을 허용합니다
access-list 171 permit ip any 10.3.70.0 0.0.0.255
```

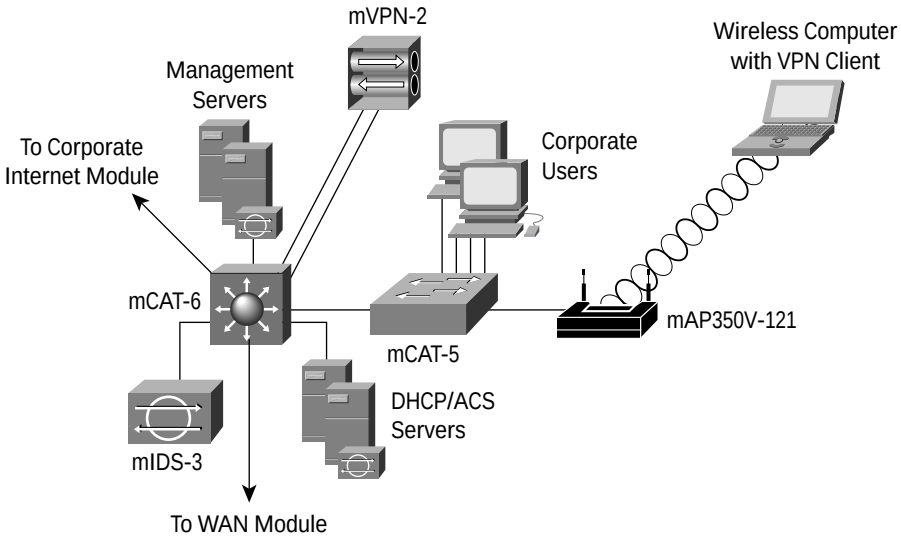
mAP350L-120과 무선 클라이언트:

LEAP 옵션에 맞게 AP와 무선 클라이언트를 설정하려면 본 부록의 "전반적인 지침" 섹션의 구성 샘플을 참조하십시오.

VPN 아키텍처

다음은 VPN 옵션을 사용하는 SAFE 중형 WLAN 설계의 시스템 구성 스냅샷입니다. 그림 A-12는 중형 네트워크의 VPN WLAN 설계입니다.

그림 A-12: 중형 VPN WLAN 설계



사용된 제품의 일부는 다음과 같습니다:

- Cisco Catalyst 레이어 3 스위치 (mCAT-6)
- Cisco Catalyst 레이어 2 스위치 (mCAT-5)
- Cisco Aironet 액세스 포인트와 클라이언트 (mAP350V-121와 무선 클라이언트)
- Cisco VPN 3000 시리즈 집중기 (mVPN-2)
- Cisco Secure Access Control Server (ACS v2.6)
- Windows 2000 DHCP 서버
- Cisco IDS Host Sensor

MCAT-6:

```
! AP는 캠퍼스 네트워크의 독립적인 VLAN에 배치됩니다
interface Vlan80
  ip address 10.3.80.1 255.255.255.0
  ip access-group 180 in
  ip access-group 181 out
  ip helper-address 10.3.2.50
  no ip redirects
  no cdp enable

! 관리를 위하여 AP에서 보내는 웹 응답을 허용합니다
access-list 180 permit tcp host 10.3.80.121 eq www 10.3.8.0 0.0.0.255 gt 1023 established

! VPN 게이트웨이 서브넷으로 보내는 IPSec 트래픽을 허용합니다
access-list 180 permit esp 10.3.80.0 0.0.0.255 10.3.16.0 0.0.0.255
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq isakmp 10.3.16.0 0.0.0.255 eq isakmp

! 문제 해결을 위한 Full ICMP를 허용합니다
access-list 180 permit icmp 10.3.80.0 0.0.0.255 10.3.16.0 0.0.0.255
access-list 180 permit icmp 10.3.80.0 0.0.0.255 host 10.3.80.1

! 무선 클라이언트의 초기 IP 할당을 위한 DHCP 요청을 허용합니다
access-list 180 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 180 permit udp 10.3.80.0 0.0.0.255 eq bootpc host 10.3.2.50 eq bootps

! 그 외의 모든 트래픽을 거부합니다. Windows 파일 공유 브로드캐스트를 로그 처리하지 마십시오
access-list 180 deny udp 10.3.80.0 0.0.0.255 any eq netbios-ns
access-list 180 deny udp 10.3.80.0 0.0.0.255 any eq netbios-dgm
access-list 180 deny ip any any log

! 무선 서브넷으로 보내는 IPSec 트래픽을 허용합니다
access-list 181 permit esp 10.3.16.0 0.0.0.255 10.3.80.0 0.0.0.255
access-list 181 permit udp 10.3.16.0 0.0.0.255 eq isakmp 10.3.80.0 0.0.0.255 eq isakmp

! 문제 해결을 위한 Full ICMP를 허용합니다
access-list 181 permit icmp 10.3.16.0 0.0.0.255 10.3.80.0 0.0.0.255

! 무선 클라이언트의 초기 IP 할당을 위한 DHCP 응답을 허용합니다
access-list 181 permit udp host 10.3.2.50 eq bootps host 255.255.255.255 eq bootpc
access-list 181 permit udp host 10.3.2.50 eq bootps 10.3.80.0 0.0.0.255 eq bootpc

! 관리를 위하여 AP로 들어오는 웹 응답을 허용합니다
access-list 181 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.80.121 eq www

! 그 외의 모든 트래픽을 거부합니다
access-list 181 deny ip any any log
```

mAP350V-121와 무선 클라이언트:

VPN 옵션에 맞게 AP와 무선 클라이언트를 설정하려면 본 부록의 “전반적인 지침” 섹션의 구성 샘플을 참조하십시오.

소형 설계와 원격 설계에는 고유한 구성 요소가 없기 때문에 해당 네트워크 구성은 제공하지 않습니다. 관련된 지침은 본 섹션의 시작 부분에 마련된 일반적인 제안을 참조하십시오.

부록 B: 무선 보안 기초 지식

무선 테크놀러지의 필요성

표준 802.11에 기초한 WLAN(wireless LANs)은 네트워크 사용자들에게 이동성을 제공하면서 동시에 꼭 필요한 기업 리소스 연결 상태를 유지합니다. 업무 현장에서 랩탑 컴퓨터가 좀더 널리 보급됨에 따라, 사용자들은 주 컴퓨팅 장치로 랩탑 컴퓨터를 사용하는 경향이 더 많아졌으며, 회의나 컨퍼런스에서 그리고 출장 중에 휴대하는 일이 더 많아졌습니다. WLAN을 도입하면서 기업체들은 이전에는 불가능했던 현장에서 기존의 네트워크에 계속 연결할 수 있게 마련하여 직원별 생산성을 더욱 향상시키게 됩니다.

무선 네트워크 연결 기능은 기업용으로 제한되지 않습니다. 무선 네트워크 연결 기능은 회의 전후 뿐만 아니라 기존의 사무실 환경 밖에서도 생산성을 증가시킬 수 있습니다. 무수하게 많은 WISP(wireless Internet service providers)들이 공항, 커피숍, 호텔, 컨퍼런스, 컨벤션 센터 등에 모습을 드러내고 있기 때문에 기업체 사용자들이 공공 액세스 시설에 연결할 수 있게 되었습니다.

무선 테크놀러지의 종류

무선 근거리 네트워킹은 여러 해 동안 존재하면서, 특정한 업무 환경에서 이동성이 필수 조건인 경우에 유선 인프라 연결 통로를 제공했습니다. 이러한 초기 네트워크들은 주파수 홉핑과 직접 시퀀싱 라디오 테크놀러지(나중에 설명함)을 모두 이용하였습니다. 이러한 초기 무선 네트워크는 비표준 구현 방식이었으며, 속도는 1 MB에서 2 MB 사이였습니다. WLAN 테크놀러지의 원동력이 되는 표준이 전혀 없는 상태에서, 이 초기 WLAN 구현 형태는 업체별 구현 형태로 전락했고, 호환성을 위한 대비가 전혀 없었기 때문에 표준에 기초한 WLAN 테크놀러지의 성장을 저해하는 요인이 되었습니다. 현재, WLAN 애플리케이션 표준으로는 802.11, HiperLAN, HomeRF SWAP, Bluetooth 등이 있습니다.

기능 개요

기능 면에서 보면, WLAN은 피어 투 피어 무선 LAN, 다중 셀 무선 LAN, 그리고 빌딩간 무선 네트워크 (포인트 투 포인트와 포인트 투 멀티포인트) 등과 같이 분류할 수 있습니다. 피어 투 피어 무선 LAN에서, 무선 NIC(network interface cards)를 갖춘 무선 클라이언트는 AP를 사용하지 않고도 서로 통신을 할 수 있습니다. 통신 범위는 피어 투 피어 LAN으로 제한되며, 무선 클라이언트는 유선 리소스를 액세스할 수 없습니다. 다중 셀 무선 LAN은 서로 겹쳐지는 셀을 이용하여 통신 범위를 확대하는 것입니다. 셀의 통신 범위는 무선 클라이언트의 무선 리소스 사용을 조정하는 액세스 포인트(무선 브리지)의 특성에 따라 결정됩니다.

빌딩간 무선 네트워크는 캠퍼스 영역 네트워크에서 LAN(빌딩) 사이의 필요한 연결 조건을 처리합니다. 빌딩간 무선 네트워크에는 포인트 투 포인트와 포인트 투 멀티포인트의 두 가지 종류가 있습니다. 빌딩 사이의 포인트 투 포인트 무선 링크는 라디오 기반의 포인트 투 포인트 링크와 레이저 기반의 포인트 투 포인트 링크입니다. 빌딩 사이의 라디오 기반 포인트 투 포인트 브리징 링크는 지향성 안테나를 사용하여 신호 파워를 좁은 빔에 집중시켜 전송 거리를 극대화시킵니다. 빌딩 사이에 존재하는 레이저 기반의 포인트 투 포인트 브리징 링크는 레이저 광선(일반적으로 적외선 광선)을 데이터 전송을 위한 전달 매체로 사용합니다. 라디오 기반의 포인트 투 멀티포인트 브리징 네트워크는 빔 폭이 넓은 안테나를 사용하여 캠퍼스 영역 네트워크에서 다수의 빌딩(LAN)을 연결합니다.

테크놀러지 개요

본 논문의 대부분의 내용은 802.11 WLAN(아래에서 설명함)에 초점을 맞추고 있지만, 현재 시중에 나와 있는 다른 무선 표준을 이해하는 것이 좋습니다.

HiperLAN

HiperLAN은 1996년에 승인이 된 ETSI(European Telecommunications Standards Institute) 표준입니다. HiperLAN/1 표준은 5-GHz 라디오 밴드에서 최대 24 Mbps로 작동합니다. ETSI는 최근에 HiperLAN/2를 승인했는데, 이것은 5-GHz 밴드에서 최대 54 Mbps로 작동하며, 일반 사용자 장치들 사이에서 액세스를 공유할 수 있도록 연결 중심 프로토콜을 사용합니다.

HomeRF SWAP

1988년에, HomeRF SWAP Group은 가정에서 PC와 소비자 가전 장치 사이의 무선 디지털 통신을 위한 SWAP(Shared Wireless Access Protocol) 표준을 발표했습니다. SWAP은 2.4-GHz 밴드에서 주파수 홉핑과 스프레드-스펙트럼 기법을 사용하여 1 Mbps와 2 Mbps의 데이터 속도로 공용 무선 인터페이스를 통한 음성과 데이터를 지원합니다.

Bluetooth

Bluetooth는 2.4-GHz 주파수 환경에서 주파수 홉핑 스프레드 스펙트럼을 사용하여 파워가 낮고 거리가 짧은 무선 연결 통로를 마련할 수 있도록 Bluetooth Special Interest Group에서 지정한 PAN(personal-area network)입니다.

802.11 무선 테크놀러지

IEEE는 802.11 기반 표준을 관리하며, 802.3 Ethernet과 같은 그 외의 802 기반 네트워킹 표준도 관리합니다. WECA(Wireless Ethernet Compatibility Alliance)라고 알려진, 판매업체와 관련이 없는 비영리 단체는 Wi-Fi라고 알려진 802.11 기반 테크놀러지를 위한 branding을 제공합니다. Wi-Fi-호환 장치는 WECA 실험실에서 호환성 테스트를 통과해야 하며, 사용자에게 장비가 다른 모든 Wi-Fi-인증 업체의 제품과 호환성이 있음을 보장합니다.

표준 802.11 기반 무선 테크놀러지는 대중이 사용할 수 있는 것으로 간주되는 라디오 스펙트럼을 활용합니다. 이 스펙트럼은 ISM 밴드 즉, Industrial, Scientific, and Medical 밴드로 알려져 있습니다. 802.11 표준은 구체적으로 세 가지 주파수 밴드 중의 두 가지를 활용합니다. 즉, 802.11와 802.11b 네트워크용으로 사용되는 2.4 GHz-to-2.4835 GHz UHF 밴드와 802.11a 기반 네트워크용으로 사용되는 5.15 GHz-to-5.825 GHz SHF 밴드를 활용합니다.

이 스펙트럼은 무허가 영역으로 분류됩니다. 즉, 스펙트럼의 소유주가 없으므로 누구든지 FCC 규정에만 일치하면 이 스펙트럼을 사용할 수 있습니다. FCC가 적용되는 다른 영역 중에는 라디오의 최대 송신력과 사용할 수 있는 엔코딩 및 주파수 변조 방식이 있습니다.

무선 LAN 라디오 주파수 방식

(802.11b가 사용하는) 2.4-GHz ISM 밴드는 스프레드 스펙트럼 테크놀러지를 활용합니다. 스프레드 스펙트럼 테크놀러지는 데이터를 무수하게 많은 주파수대에 분산시켜 전송하는 방법입니다. 이렇게 하는 이유는 2.4-GHz 밴드에는 다른 주 소유주가 있기 때문입니다. 주 소유주는 자신이 사용할 스펙트럼을 구입하였거나 다른 무엇보다도 그 스펙트럼에 대한 법적인 액세스가 허용된 엔티티입니다. 2.4-GHz 밴드의 일반적인 주 소유주는 마이크로웨이브 오븐 제조업체들입니다. 마이크로웨이브 오븐은 동일한 주파수 범위로 전송하지만 파워 수준은 훨씬 더 높습니다 (일반적인 802.11 네트워크 카드는 100 mW에서 작동하는 반면, 마이크로웨이브 오븐은 600 W에서 작동합니다.). 스프레드 스펙트럼 테크놀러지의 경우, 주 소유주와 겹쳐지는 부분이 있다해도, 주 소유주에게는 'RF 권리'라고 하는 부분이 있습니다.

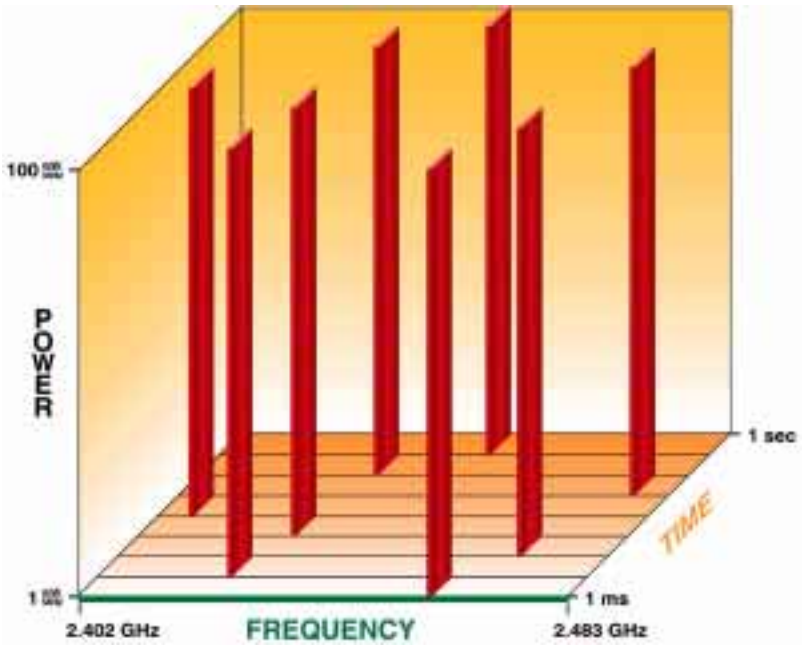
802.11 표준은 라디오 기반 장치에 대해 두 가지 종류의 레이어 1 물리적 인터페이스를 규정합니다. 한 종류는 주파수 홉핑 아키텍처를 사용하는 반면, 다른 한 종류는 직접 시퀀싱이라고 하는 보다 직선적인 단일 주파수 방식을 사용합니다.

주파수 홉핑

2.4-GHz ISM 밴드는 83.5 MHz의 가용 주파수 스펙트럼을 제공합니다. 주파수 홉핑 아키텍처는 한 번에 0.4 초 이하 동안 79개의 1-MHz 폭의 주파수 중의 하나를 전송하는 홉핑 패턴을 만들어서 가용 주파수 범위를 활용합니다. (그림 B-1 참조). 이렇게 설정하면 간섭에 강한 네트워크가 됩니다. 어느 한 채널이 간섭의 영향을 받는다 해도, 그 간섭은 작은 시간 조각 하나에 불과합니다. 주파수 홉핑 라디오가 신속하게 밴드를 홉핑하면서 다른 주파수에서 데이터를 재전송하기 때문입니다.

주파수 홉핑의 주된 단점은 달성할 수 있는 최대 데이터 속도가 2 Mbps라는 점입니다. 79개의 다른 홉 셋에 주파수 홉핑 액세스 포인트를 배치할 수 있기는 하지만, 간섭이 발생할 가능성을 낮추고 주파수 홉핑 테크놀러지의 비교적 큰 총 처리 속도와 확장성이 가능하게 하는 것은 배치에서 문제가 됩니다. 와이드밴드 주파수 홉핑과 관련된 작업이 진행되고 있기는 하지만, 이 개념은 현재 IEEE에서 표준화되어 있지 않습니다. 와이드밴드 주파수 홉핑은 10 Mbps 수준의 높은 데이터 속도를 약속합니다.

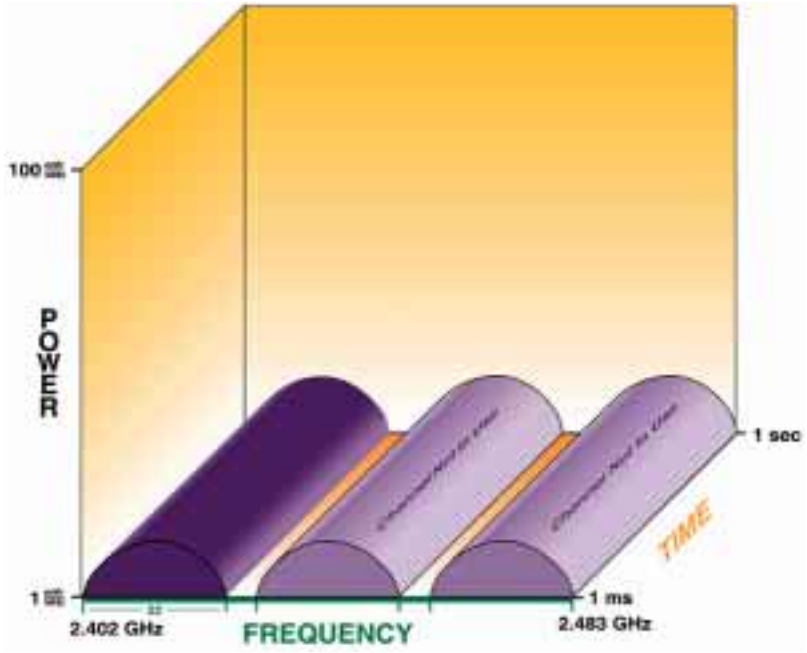
그림 B-1: 주파수 홉핑



직접 시퀀싱과 802.11b

직접 시퀀싱 네트워크는 데이터 전송에 대한 다른 접근 방식을 취합니다. 직접 시퀀싱은 2.4-GHz 스펙트럼 내에서 83 MHz의 11가지 서로 중복되는 채널을 제공합니다. 11개의 서로 중복되는 채널 내에는, 폭이 22-MHz인 3개의 중복되지 않는 채널이 있습니다(그림 B-2 참조). 직접 시퀀싱이 제공하는 CCK(complementary code keying)에 기초한 큰 대역폭과 고성능 변조는 직접 시퀀싱이 주파수 홉핑보다 높은 데이터 속도를 지원할 수 있는 주된 이유입니다. 뿐만 아니라, 이 세 채널은 서로 중복되지 않으므로, 세 개의 AP를 동시에 사용하여 임의로 구성된 세 개의 가용 채널의 총 데이터 속도를 제공할 수 있습니다. 1999년에, IEEE는 802.11b 표준을 승인했는데, 이 표준에서는 이 세 개의 서로 중복되지 않는 채널을 함께 사용할 때 직접 시퀀싱 네트워크가 11 Mbps나 33 Mbps의 높은 데이터 속도를 낼 수 있는 비교적 새로운 고급 변조 방식을 규정하였습니다. 직접 시퀀싱은 주파수 홉핑에 비해 간섭 내성 면에서 단점이 있습니다. 이 두 방식 모두 간섭의 영향을 받기는 하지만, 직접 시퀀싱 네트워크의 처리 속도는 간섭이 발생하면 엄청나게 떨어집니다.

그림 B-2: 직접 시퀀싱



802.11a 네트워크

1999년에 IEEE는 802.11a라고 하는 또 하나의 레이어 1 물리적 인터페이스를 승인했습니다. 802.11a 표준은 5-GHz SHF 밴드를 사용하여 54 Mbps의 높은 데이터 속도를 냅니다.

802.11 표준이나 802.11b 표준과는 달리, 802.11a 표준은 OFDM(orthogonal frequency-division multiplexing)이라고 하는 FDM(frequency-division multiplexing) 방식을 사용합니다. FDM 시스템에서, 가용 대역폭은 다수의 데이터 반송파로 나누어집니다. 그 다음에 전송할 데이터를 이 하위 반송파 사이에서 나눕니다. 각 반송파는 다른 반송파와는 독립적으로 처리되기 때문에, 주파수 가드 밴드를 그 주위에 배치해야 합니다. 이 가드 밴드로 인해 대역폭 효율성이 낮아집니다. OFDM에서는, 다수의 반송파 (즉 톤)을 사용하여 가용 스펙트럼 사이에서 데이터를 나눕니다. 이것은 FDM과 비슷합니다. 하지만, OFDM 시스템에서, 각 톤은 인접 톤과 직각으로 교차 (서로 독립적이거나 관련이 없음) 하는 것으로 간주되므로, 가드 밴드가 필요하지 않습니다. 그렇기 때문에, OFDM은 FDM에 비해 스펙트럼 효율성이 높으며, 라디오 주파수 간섭 현상과 하위 멀티패스 왜곡 현상에 대한 대처 능력도 지니고 있습니다.

FCC는 이 5-GHz 스펙트럼을 세 개의 덩어리로 나누어 U-NII(Unlicensed National Information Infrastructure)의 일부로 만들었습니다. 세 개의 U-NII의 대역폭은 각가 100 MHz이며 폭이 20 MHz인 네 개의 서로 중복되지 않는 채널로 구성되어 있습니다. 그 결과, 20-MHz의 각 채널은 폭이 300-kHz인 52개의 하위 채널로 구성됩니다. 이 하위 채널 중의 48개는 데이터 전송용으로 사용되고 나머지 4개는 오류 교정용으로 사용됩니다. 세 개의 U-NII 밴드를 사용할 수 있습니다.

- U-NII 1 장치는 5.15-GHz에서 5.25-GHz 주파수 범위에서 작동합니다. U-NII 1 장치의 최대 전송 파워는 50 mW이고 최대 안테나 게인은 6 dBi이며, 완벽한 하나의 장치가 되려면 안테나와 라디오가 있어야 합니다 (착탈식 안테나 없음). U-NII 1 장치는 실내에서만 사용할 수 있습니다.
- U-NII 2 장치는 5.25- GHz에서 5.35-GHz까지의 주파수 범위에서 작동합니다. U-NII 2 장치의 최대 전송 파워는 250mW이고 최대 안테나 게인은 6 dBi입니다. U-NII 1 장치와는 달리, U-NII 2 장치는 실내나 실외에서 모두 사용할 수 있으며, 착탈식 안테나도 있습니다. FCC는 하나의 장치가 U-NII 1 스펙트럼과 U-NII 2 스펙트럼을 모두 처리하는 것을 허용하지만, 그런 식으로 사용하는 경우 그 장치는 U-NII 1 관련 규정에 일치해야 한다고 요구합니다.

- U-NII 3 장치는 5.725- GHz에서 5.825-GHz 까지의 주파수 범위에서 작동합니다. 이 장치의 최대 전송 파워는 1W이며 착탈식 안테나도 사용할 수 있습니다. U-NII 1 장치나 U-NII 2 장치와는 달리, U-NII 3 장치는 실외 환경에서만 사용할 수 있습니다. 그렇기 때문에, FCC는 포인트 투 포인트 설치의 경우 최대 23-dBi 게인 안테나 사용을 허용하며, 포인트 투 멀티포인트 설치의 경우에는 6-dBi 게인 안테나 사용을 허용합니다.

무선 LAN 로밍

802.11 규격은 로밍을 위한 특별한 메커니즘을 규정하지 않습니다. 따라서, WLAN 클라이언트가 로밍 결정을 하는 알고리즘을 정의하는 것은 각 업체에 맡겨져 있습니다.

802.11 스테이션 로밍을 어느 정도 파악하기 위하여, 먼저 802.3 이더넷 네트워크 아키텍처를 검토해 봅시다. 표준 802.3 기반 이더넷 LAN은 CSMA/CD(carrier sense multiple access collision detect) 아키텍처를 사용합니다. 데이터를 다른 스테이션으로 전송하려는 스테이션은 먼저 매체가 사용 중인지 확인합니다. 이것이 CSMA/CD의 반송파 감지 기능입니다. 매체에 연결되어 있는 모든 스테이션은 매체 액세스 권한이 동일합니다. 이것이 CSMA/CD의 다중 액세스 부분입니다. 스테이션은 매체를 사용할 수 있다고 확인하면 전송을 시작합니다. 두 스테이션이 매체를 이용할 수 있다고 감지하고 동시에 전송을 시작하면, 그 스테이션들의 프레임이 "충돌"하게 되고 그 매체에서 전송된 데이터는 쓸모없게 됩니다. 송신 스테이션은 충돌을 감지하고 대체 알고리즘을 실행하여 프레임을 재전송할 수 있습니다. 이것이 CSMA/CD의 충돌 감지 기능입니다.

802.3 이더넷 아키텍처는 유선 네트워크용으로 설계되었습니다. 설계자들은 송신 스테이션에서 원하는 수신지로 프레임을 전달하는 유선 매체에 상당한 신뢰성을 부여하였습니다. 그런 이유에서, 802.3에는 프레임이 수신 스테이션에 도달했는지 판단하는 메커니즘이 없습니다. 802.3은 상위 레이어 프로토콜에 의존하여 프레임 재전송을 처리합니다.

802.11 네트워크는 공중으로 전송되며, 무수하게 많은 간섭 발생 요인에 부딪히게 됩니다. 802.11의 설계자들은 이 문제를 이해했기 때문에, 수신 스테이션이 프레임을 수신하였음을 송신측에 통지하는 링크 레이어 확인 기능을 마련하였습니다. 전송된 모든 프레임에 대해, 수신 스테이션은 ACK(acknowledgement) 프레임으로 응답합니다.

클라이언트 스테이션은 액세스 포인트에서 얼마나 멀리 이동하였는지 판단하는 수단으로 ACK 메시지를 사용합니다. 클라이언트 스테이션은 데이터를 전송할 때, 수신 스테이션에서 ACK 메시지를 수신할 것으로 예상되는 시간대를 정합니다. 이 ACK 메시지가 시간 종료 상태가 되면, 클라이언트는 액세스 포인트에서 너무 멀리 떨어져 있기 때문에 통신 품질이 저하되기 시작하는 것을 알게 됩니다.

액세스 포인트는 비콘이라고 하는 주기적인 관리 프레임도 보냅니다. 비콘에는 SSID(service set identifier), 지원 데이터 속도, 액세스 포인트가 주파수 홉핑을 지원하는지 직접 시퀀싱을 지원하는지 여부, 용량 등과 같은 액세스 포인트 정보가 들어 있습니다. 비콘 프레임은 정기적인 간격으로 액세스 포인트에서 브로드캐스트되며, 이 간격은 시스템 관리자가 조정할 수 있습니다.

ACK 프레임과 비콘은 클라이언트 스테이션에 로밍 결정을 해야 하는지 여부를 결정하는 기준점을 제공합니다. 지정된 수의 비콘 메시지가 사라지면, 클라이언트는 비콘 메시지가 연결된 액세스 포인트의 범위 밖으로 나갔다고 추정할 수 있습니다. 뿐만 아니라, 예상된 ACK 메시지가 수신되지 않으면, 클라이언트는 역시 동일한 가정을 할 수 있습니다.

실제로 로밍을 하는 방법은 업체마다 차이가 있습니다. 기본적인 로밍 방법은 로밍 결정을 한 다음, 로밍할 새 액세스 포인트를 찾아내는 것입니다. 이 시나리오에는 액세스 포인트 검색을 다시 시작하는 것이 관련됩니다. 이것은 처음 초기화할 때 하는 방법과 동일하거나 이전 연결 중에 만들어 둔 테이블을 참조하는 것과 같은 다른 방법으로 이루어집니다.

WLAN 로밍의 타이밍도 업체에 따라 차이가 있지만, 대부분의 경우 1초 미만이며, 가장 좋은 경우에도 200 msec 미만입니다. 로밍이 업체별로 차이가 있기 때문에, 여러 업체의 액세스 포인트 사이에서 로밍을 하면 로밍 시간이 늘어날 수 있다는 점에 유의하는 것도 중요합니다.

IEEE에서 표준화한 것처럼, 802.11 네트워크의 보안은 두 가지 주요 요소, 즉 암호화와 인증으로 단순화시킬 수 있습니다. 이러한 요소들의 구현 형태는 보안 공동체에 의해 대체로 안전하지 않은 것으로 입증이 되었습니다. 그런 요소들을 여기서 제시하는 것은 그 내용이 본 문서의 기본 원칙 섹션에 나올 때 독자들이 근본적인 결점을 이해할 수 있게 하려는 것입니다.

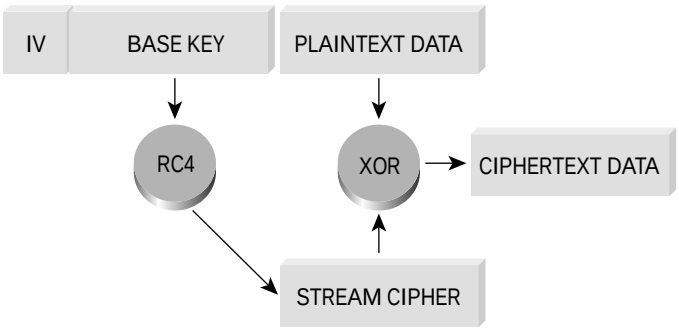
프레임 암호화

암호화가 적절하게 수행되면 기밀성을 지닐 수 있습니다. 암호화는 cleartext라고 하는 메시지를 가져다가 수학적인 알고리즘을 거쳐서 ciphertext라고 하는 것을 만들어내는 프로세스입니다. 암호 해독은 이 프로세스를 역으로 진행하는 것입니다. 일반적으로 암호화 알고리즘은 키라고 하는 값에 의존하여 데이터를 암호화하고 암호를 해독합니다. 요즘 사용되는 두 가지 주요 암호화 형태는 대칭형 암호화(공유 키 암호화라고도 함)와 비대칭형 암호화(공개/비공개 암호화라고도 함)입니다. 대칭형 암호화는 비대칭형 암호화보다 약 1000배 더 빠르므로 데이터를 대량으로 암호화하는데 사용됩니다. 일반적으로 잘 설계된 암호화 알고리즘의 경우, 키가 길수록 보안 수준이 더 높아지게 됩니다. 암호화된 메시지를 해독하려면 가능한 모든 키(키 공간이라고 함)를 시도해 보려면 더 힘이 들기 때문입니다. IEEE는 WEP(Wired Equivalent Privacy)를 802.11 데이터 프레임을 암호화는 수단으로 사용하도록 규정했습니다. WEP는 RSA RSADSI(Data Security, Inc.)의 Ron Rivest가 암호화를 위하여 창안한 RC4 스트림 cipher를 사용합니다. RC4 암호화 알고리즘은 가변 길이 키를 지원하는 대칭형 스트림 암호입니다. 스트림 암호는 한 단위의 plaintext(이 경우에는 802.11b 프레임)에 대해 암호화/암호 해독 기능을 사용하는 방식입니다. 이 암호는 각 암호/암호 해독 기능에서 고정된 바이트를 처리하는 블록 암호와 대조가 됩니다. 대칭형 암호화의 경우, 키는 암호화 엔드포인트와 암호 해독 엔드포인트 모두에서 공유해야 하는 한 조각의 정보입니다. RC4에서는 일정한 길이로 고정된 키를 사용해야 하는 것이 아니라 키 길이를 최대 256 바이트까지 가변적으로 사용할 수 있습니다. IEEE는 802.11 장치가 40 비트 키를 지원해야 하며 좀더 긴 길이의 키를 사용할 수 있는 옵션도 두도록 규정하고 있습니다. 여러 업체의 WLAN 솔루션에서 128 비트 WEP 암호화를 지원합니다.

WEP는 스트림 암호이므로, 동일한 plaintext에서 동일한 ciphertext가 생성되지 않게 하는 메커니즘이 필요합니다. IEEE는 스트림 ciphertext를 생성하기 전에 대칭형 키와 연결시킬 IV(initialization vector)를 사용하도록 규정했습니다.

IV는 (범위가 0에서 16777215까지인) 24비트 값입니다. IEEE는 IV를 프레임별로 바꾸는 방법을 제안 - 명령은 아님 - 하고 있습니다. 송신측에서 표준 기법이나 스케줄이 없는 IV를 생성하기 때문에, 802.11 데이터 프레임의 헤더 부분이 암호화되지 않은 상태로 수신측으로 보내야 합니다. 그러면, 수신측은 수신된 IV를 로컬 영역에 저장된 WEP 키(기본 키)와 연결시켜 데이터 프레임의 암호를 해독합니다. 그림 B-3에 나오는 것처럼, plaintext 자체는 RC4 cipher를 거치지 않지만, RC4 cipher를 사용하여 그 특정한 802.11 프레임의 고유한 키스트림을 생성하며 IV와 기본 키를 keying 자료로 사용합니다. 그 결과 만들어진 고유한 키스트림은 plaintext와 결합되어 XOR이라고 하는 수학 함수를 거치게 됩니다. 이렇게 하여 ciphertext가 만들어집니다.

그림 B-3: WEP 암호화 프로세스



인증 메커니즘

IEEE는 802.11 기반 네트워크를 위한 두 가지 인증 알고리즘을 규정했습니다. 먼저, 공개 인증은 null 인증 알고리즘입니다. 인증을 요청하는 모든 스테이션에 액세스 권한이 부여되기 때문입니다. 두 번째 인증 형태는 공유 키 인증이라고 합니다. 공유 키 인증에서는 요청 스테이션과 승인 스테이션이 모두 서로 일치하는 WEP 키로 구성되어 있어야 합니다. 요청 스테이션은 승인 스테이션으로 인증 요청을 보냅니다. 승인 스테이션은 요청 스테이션으로 plaintext 요청 프레임을 보냅니다. 요청 스테이션 WEP는 요청 프레임을 암호화하여 승인 스테잇으로 다시 보냅니다. 승인 스테이션은 그 프레임의 암호를 해독하려고 시도하고, 그 결과 해독된 plaintext가 승인 스테이션이 원래 보낸 것과 일치하면, 요청 스케이션이 유효한 키를 지닌 것이므로 액세스 권한을 부여합니다.

공유 키 인증 개념에는 유명한 결함이 있다는 점에 유의해야 합니다. 요청 패킷은 공개된 상태로 요청 스테이션으로 보내지고 요청 스테이션은 암호화된 요청 패킷으로 응답하므로, 공격자가 plaintext와 ciphertext를 모두 분석하면 스트림 암호를 도출해낼 수 있습니다. 이 정보는 그 특정한 WEP 키의 암호 해독 사전을 만드는데 사용할 수 있습니다. IEEE에서 표준화한 WEP의 이 유명한 보안 문제는 본 문서의 기본 원칙 섹션에서 설명합니다.

무선 LAN 컴포넌트

WLAN의 구성 요소는 AP(Acces Points), NIC(Network Interface Cards)/클라이언트 어댑터, 브리지, 안테나 등입니다.

액세스 포인트-AP는 특정한 주파수 스펙트럼 내에서 작동하며 802.11 표준에서 지정한 변조 기법을 사용합니다. 또한 AP는 무선 클라이언트에게 AP 이용 가능 여부를 알려주고 무선 클라이언트를 무선 네트워크에 인증하여 연결시킵니다. 또한 AP는 무선 클라이언트의 유선 리소스 사용을 조정합니다.

NIC(Network interface card)/클라이언트 어댑터-PC나 워크스테이션은 무선 NIC를 사용하여 무선 네트워크에 연결합니다. NIC는 연결에 이용할 수 있는 주파수 스펙트럼을 스캔하여 액세스 포인트나 다른 무선 클라이언트에 연결시킵니다. NIC는 소프트웨어 드라이버를 사용하여 PC/워크스테이션 운영 체제와 짝지어집니다.

브리지-무선 브리지는 MAC(Media Access Control) 레이어 수준에서 다수의 LAN을 연결하는데 사용됩니다. 빌딩간 무선 연결에서 사용되는 무선 브리지는 AP보다 통신 범위가 더 넓습니다. (IEEE 802.11 표준은 AP의 최대 통신 범위를 1 마일로 규정합니다).

안테나-안테나는 변조된 신호를 공중으로 방사하므로 무선 클라이언트가 그 신호를 수신할 수 있습니다. 안테나의 특성은 전달 패턴(지향성 대 전방향성), 게인, 전송 파워, 등등을 기준으로 정의됩니다. 안테나는 AP/브리지와 클라이언트 모두에 마련되어 있어야 합니다.

참조 자료

SAFE 백서

SAFE: A Security Blueprint for Enterprise Networks:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm

SAFE VPN: IPSec Virtual Private Networks in Depth:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

SAFE: Nimda Attack Mitigation: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/snam_wp.htm

SAFE: Code-Red Attack Mitigation: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/scdam_wp.htm

기타 참조 자료

Security of the WEP Algorithm: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Your 802.11 Wireless Network has No Clothes: http://www.cs.umd.edu/~waa/wireless.pdf

Weaknesses in the Key Scheduling Algorithm of RC4: http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP:
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

AirSnort: http://airsnort.sourceforge.net/

파트너 제품 레퍼런스

RSA SecureID OTP System-http://www.rsasecurity.com/products/securid/

감사의 말

저자들은 본 SAFE 블루프린트 확장판과 본 문서 집필에 도움을 준 모든 개인들에게 공개적으로 감사하기를 원합니다. 시스코 본사와 현장의 모든 직원들에게서 들어온 귀중한 자료와 검토 의견이 없었더라면 본 문서를 성공적으로 끝낼 수 없었을 것이 분명합니다. 검토 단계나 랩 검증 단계에서 더 수고해 준 사람들도 다수입니다. 이 그룹의 중심은 Andy Balinsky, Bruce McMurdo, Brian Cox, Roland Saville 등입니다. 여러분 모두의 특별한 노력에 감사드립니다.