THUYẾT TRÌNH ĐỒ ÁN MẠNG MÁY TÍNH

L1

Kính thưa các thầy cô trong hội đồng, cùng toàn thể các bạn sinh viên, em tên là Lê Trung Tiến sinh viên K54KMT.

Với sự hướng dẫn của thầy đỗ duy cốp đến này em đã hoàn thành đề tài tìm hiểu về ssl vpn

Sau đây em xin phép trình bầy về đồ án

L2

Đồ án của em gồm các nội dung chính sau đây:

Phần 2: trình bầy về 2 khái niệm vpn và ssl vpn, đưa ra một số khái niệm liên quan để ta hiểu rõ ưu điểm của công nghệ này.

Phần 3: hoạt động của ssl vpn, và việc sử dụng SSL để tạo nên VPN,. các cải tiến quan trọng trong SSL VPN, các dịch vụ trong SSL VPN và các thành phần của nó. Qua đó chúng ta có thể có một cái nhìn sâu hơn về hoạt động của SSL VPN.

Phần 4: Phương pháp bảo mật trong SSL VPN, các khái niệm, và vấn đề bảo mật xảy ra với SSL VPN cũng như cách giải quyết các vấn đề này. Qua đó chúng ta có thể hiểu rõ hơn về bảo mật trong SSL VPN

L3

Ngày nay, sự phát triển của khoa học công nghệ đã làm thay đổi nhiều mặt trong cuộc, đóng góp vào sự phát triển của kinh tế thế giới. Trong đó, công nghệ

thông tin và truyền thông có một vai trò rất quan trọng. Cùng với sự phát triển đó nhu cầu trao đổi thông tin giữa các vùng, các tôt v.v ngày càng lớn, kéo theo đó là sự mất an toàn bảo mật thông tin vì vậy công nghệ VPN đã ra đời giúp bảo mật dữ liệu mà vẫn sử dụng hạ tầng internet có sẵn. Trong đề tài này em xin trình bầy giải pháp SSL VPN.

L4

Sau đây em xin trình bầy chi tiết từng phần:

Trước tiên khi đi vào khái niệm ssl vpn em sẽ trình bầy về khái niệm vpn: khi người dùng hoặc một tổ chức truy cập một mạng Internet công cộng thì hacker sẽ dễ dàng tấn công và đánh cắp dữ liệu người dùng điều này sẽ gây ra hậu quả vô cùng nghiêm trọng, nhưng nếu ta không sử dụng mạng công cộng mà sử dụng một mạng riêng để kết nối với nhau thì sẽ rất tốn kém vì vậy VPN ra đời.

VPN viết tắt của Virtual Private Network (mạng riêng ảo) là một kết nối bảo mật giữa hai hoặc nhiều điểm qua một mạng công cộng. Mạng riêng ảo VPN giúp người dùng tạo ra một mạng riêng từ một kết nối Internet công cộng qua đó thiết lập các kết nối được mã hóa nâng cao tính bảo mật cho dữ liệu.

Trên đây là những giao thức thường sử dụng nhất trong VPN với những giao thức này thì 3 giao thức đầu là được sử dụng nhiều nhất. Trong đồ án này em xin giới thiệu về SSL VPN.

L6

SSL VPN viết tắt của Secure Socket Layer có nghĩa là Lớp socket bảo mật là một trong những phương thức để bảo mật dữ liệu qua internet sử dụng trong vpn.

+ SSL cung cấp khả năng mã hóa dữ liệu trên mạng. Nó có khả năng quản lý kênh truyền thông được bảo mật và mã hóa giữa server và client, SSL hỗ trợ hầu hết các trình duyệt thông dụng như: Explorer, Firefox và Chrome

- Một trong những chức năng chính của SSL là đảm bảm bí mật của tệp tin, ssl có thể mã hóa một phiên giữa client và server do đó các ứng dụng có thể truyền và xác thực tên đăng nhập và mật khẩu mà không bị nghe trộm vì ssl sẽ mã hóa dữ liệu, nếu hacker có lấy được dữ liệu thì việc giải mã nó cũng rất khó khăn và thời gian để giải mã các tổ hợp với các máy tính hiện nay có thể lên đến hàng chục năm sau khoảng thời gian này thì dữ liệu đã không còn có giá trị nữa.

- Một chức năng quan trọng nữa của SSL là khả năng cung cấp cho client và server có thể chứng thực được chúng qua việc trao đổi các chứng thực. Tất cả lưu lượng giữa SSL server và SSL client được mã hóa bằng cách sử dụng một khóa chia sẻ và một thuật toán mã hóa và cuối cùng ssl đảm bảo bản tin giữa hệ thống gửi và hệ thống nhận không bị giả mạo trong suốt quá trình truyền.

=> Như vậy SSL VPN cung cấp được một kênh bảo mật an toàn giữa máy khách và máy chủ giúp chúng ta truy trao đổi thông tin một cách an toàn hơn

L7

- Mạng tin cậy : Một mạng tin cậy của một công ty là một mạng mà công ty sử dụng để quản lý hoạt động. Trong nhiều trường hợp, một mạng tin cậy thường được định nghĩa như một vùng an toàn. Mạng tin cậy thường có các hệ thống đầu cuối, các trang web nội bộ, xử lý dữ liệu, tin nhắn nội bộ.

- Vùng cách ly DMZ: là một mạng cách ly, được đặt như là một vùng đệm giữa một mạng tin cậy của công ty và các mạng không tin cậy (Internet luôn được xem như là một mạng không tin cậy). Mục đích ban đầu của DMZ sẽ ngăn chặn người dùng bên ngoài trực tiếp kết nối vào một mạng tin cậy

Dưới đây là một vài chức năng mà DMZ có thể thực hiện:

- Chặn các cuộc quét cổng vào mạng tin cậy.
- Chặn các truy cập vào mạng tin cậy qua một cổng TCP đơn lẻ.
- Chặn DOS (Denial of Service Attack – Tấn công từ chối dịch vụ).
- Quét vius, nội dung, kích cỡ các e-mail.
- Chặn các cuộc nghe trộm / thay đổi gói.

L8

Một trong những chức năng bảo mật chính của một DMZ là khả năng hủy kết nối IP ở nhiều điểm trong DMZ và mạng tin cậy. nhờ vậy nhân viên trong cty có thể truy cập tài nguyên nội bộ ở ngoài công ty mà ko sợ hacker

L9

Sử dụng mạng riêng: nhiều công ty sẽ có những mạng riêng của mình, mạng này có thể trải rộng trên toàn cầu, mỗi điểm kết nối vào mạng là nơi hacker có thể tấn công vì vậy ta tạo một kết nối ssl….

L10

Chương 2: hoạt động của ssl vpn

SSL VPN cho phép người dùng thiết lập các kết nối an toàn từ trình duyệt kết nối internet, cho phép người dùng truy cập email, tài nguyên mạng khác ở bất kỳ nơi nào, hiện nay không có một chuẩn nào cho công nghệ ssl vpn , các nhà sản xuất cũng không công khai các công nghệ mình sử dụng trong ssl vpn nhưng về cơ bản chúng vẫn có những đặc điểm chung.

L11

Trong thị trường hiện nay, các sản phẩm bảo mật như SSL VPN thường được bán dưới dạng *thiết bị*, thiết bị thường được xem như là một hộp đen, có nghĩa là người quản trị mạng không cần thiết phải hiểu cách chúng thực hiện. Về lý thuyết, các thiết bị giảm chi phí trong việc cài đặt, cấu hình, và bảo trì một hệ thống công nghệ thông tin.

Mặc dù có một vài sự khác biệt trong các công nghệ bên trong, đứng trên quan điểm bảo mật, thực chất không có các điểm khác biệt khi thực hiện SSL VPN bằng

thiết bị so với SSL VPN bằng phần mềm, phần mềm này có thể được cài đặt trên các máy chủ của người mua.

Lịch sử ra đời: giao thức ssl ra đời để đáp ứng bảo mật cho các trang web sử sụng giao thức HTTP khi đó còn sơ khai chưa có một cách thức bảo vệ hiệu quả dễ dàng bị xem trộm bởi hacker.

SSL phiên bản 1.0 được giới thiệu trong trình duyệt Mosaic năm 1994 và liên tục cải tiến cho đến nay.

Tóm lược lại ssl có những công dụng sau:

- Bảo mật truyền thông.
- Đảm bảo toàn vẹn dữ liệu.
- Xác thực máy chủ.
- Xác thực máy trạm.

L12

SSL sử dụng thuật toán mật mã (cryptography) để mã hóa dữ liệu, vì vậy chỉ có hai máy tính có khả năng đọc bản tin và hiểu được nó. Điều này gọi là bảo vệ dữ liệu tin cậy. SSL hỗ trợ nhiều thuật toán mật mã khác nhau

Có hai loại thuật toán mật mã được sử dụng trong mỗi phiên SSL, đối xứng và bất đối xứng. Trong khi mật mã đối xứng được sử dụng để mã hóa tất cả các giao tiếp trong một phiên SSL thì thuật toán mật mã bất đối xứng được sử dụng để chia sẻ khóa phiên đối xứng một cách an toàn giữa người dùng và SSL VPN.

Mã khóa:

Một khóa là một đoạn dữ liệu (thường là một số lớn), nó giúp cho một thuật toán mật mã để mã hóa văn bản thông thường thành văn bản mật, hoặc để giải mã văn bản mật thành văn bản ban đầu.

Đối xứng:

Thuật toán đối xứng sử dụng cùng một khóa để mã hóa và giải mã, và do đó cả hai bên đối thoại cần phải chia sẻ khóa như hình 2.3. Quá trình xử lý thuật toán mật mã đối xứng cần ít vòng CPU hơn quá trình xử lý bất đối xứng. Tuy nhiên, thuật toán

mật mã đối xứng có một nhược điểm lớn là làm thế nào một bên chia sẻ khóa bí mật với bên kia nếu như phải truyền qua môi trường Internet không tin cậy.

Bất đối xứng:

Thuật toán mật mã bất đối xứng giải quyết vấn đề chuyển đổi khóa nói trên. Nó sử dụng một cặp khóa, một khóa gọi là khóa bí mật và một khóa gọi là khóa công cộng. Khóa công cộng không phải là bí mật và nó được chia sẻ tới tất cả trong khi khóa bí mật thì thuộc quyền sở hữu của một máy tính nào đó.

Tuy nhiên, thuật toán mật mã bất đối xứng cần một bộ xử lý phức tạp và không thể mã hóa khối lượng dữ liệu lớn. Nó không thể được sử dụng để mã hóa tất cả phiên SSL. Do đó, người ta đã nghĩ đến việc dùng thuật toán mật mã bất đối xứng để truyền khóa bí mật. Và SSL đã sử dụng ý tưởng này, SSL sử dụng thuật toán mật mã bất đối xứng để truyền khóa bí mật giữa người dùng đầu xa và máy chủ, và sau đó thực hiện thuật toán mật mã đối xứng để truyền dữ liệu trong suốt phiên làm việc

L16

Bảo mật trong ssl vpn được chia làm 3 phần chính:
Chứng thực có thể thực hiện bằng những cách sau:
Trong công nghệ SSL VPN, xác thực đại diện cho khả năng một người dùng đã chứng thực được phép truy cập các ứng dụng cụ thể và đọc, thay đổi hoặc xóa các file hoặc dữ liệu cụ thể. Xác thực được thực hiện theo nhiều cách khác nhau: