**Không rõ**

Lựa chọn bảo mật mới cho mạng doanh nghiệp Việt Nam

Chào mừng các bạn đón đọc đầu sách từ dự án sách cho thiết bị di động

*Nguồn:* [*http://vnthuquan.net/*](http://vnthuquan.net/)
Tạo ebook: Nguyễn Kim Vỹ.

**MỤC LỤC**

[Lựa chọn bảo mật mới cho mạng doanh nghiệp Việt Nam](%22%20%5Cl%20%22bm2)

**Không rõ**

Lựa chọn bảo mật mới cho mạng doanh nghiệp Việt Nam

Những giải pháp bảo mật mang tính tổng thể dành cho doanh nghiệp vừa và nhỏ, hiệu quả hơn với chi phí thấp hơn, vừa được hãng Juniper chính thức giới thiệu tại Việt Nam.
Nguy cơ bảo mật đang gia tăng
Hiện tại, thị trường bảo mật Việt Nam bắt đầu phát triển do nhu cầu ứng dụng công nghệ mạng của các doanh nghiệp, tổ chức đang gia tăng. Các nhu cầu như e-mail, lập website, video meeting, sử dụng điện thoại VoIP, truy cập và làm việc từ xa... ngày càng trở nên phổ biến, trở thành những phương tiện giao dịch và kinh doanh thiết yếu. Tuy nhiên, đó cũng là lúc các nguy cơ tiềm ẩn về bảo mật mạng trở nên thường trực hơn, và hệ thống luôn có thể trở thành nạn nhân của các loại virus, những cuộc tấn công xâm nhập của hacker để ăn cắp dữ liệu, tài khoản...
Việc đầu tư một hệ thống bảo mật đồ sộ tương đương như của các nhà cung cấp dịch vụ Internet hoặc các tập đoàn lớn sẽ là điều không thể với các doanh nghiệp vừa và nhỏ, vốn có ngân sách hạn chế. Các hình thức bảo mật thông thường như phần mềm chống virus, tường lửa... đang ngày càng dễ bị qua mặt bởi những hình thức tấn công tinh vi mới.
Để khắc phục thực trạng này, Juniper đã đưa ra một mô hình giải pháp phù hợp với điều kiện ngân sách của các doanh nghiệp vừa và nhỏ tại Việt Nam, có mô hình tương tự như các hệ thống bảo mật của các nhà cung cấp dịch vụ, nhưng ở quy mô nhỏ hơn.
Giải pháp truy cập bảo mật từ xa SSL VPN
Truy cập từ xa là một trong những yêu cầu chính của mạng doanh nghiệp, vì nó cho phép các nhân viên có thể làm việc từ bất cứ nơi nào có kết nối Internet. Tuy nhiên, việc kết nối từ có thể tạo ra những nguy cơ bảo mật nghiêm trọng. Chẳng hạn, với kiểu tấn công quay đầu "U-turn" mới, một hacker tên Joe có thể xâm nhập qua hệ thống IPSEC VPN của hãng Acme để lấy trộm mọi e-mail theo kịch bản như sau:
1. Joe tự tạo một chương trình Trojan riêng, sử dụng hình thức xâm nhập và lấy email phổ biến, nhưng được nguỵ trang để các phần mềm diệt virus thông dụng không phát hiện được. Joe giấu kèm Trojan này vào một e-mail được thiết kế với tiêu đề hấp dẫn, để Trojan có thể kích hoạt ngay khi e-mail được mở ra. Sau đó, Joe gửi e-mail đó tới hòm thư AOL của một nhân viên hãng Acme có tên Jane.
2. Jane kiểm tra e-mail AOL bằng máy tính xách tay (laptop) và mở bức thư vì có tiêu đề quá hẫp dẫn, đây cũng là laptop cô sử dụng để kết nối vào hệ thống IPSEC của Acme. Trojan đã nhiễm vào laptop của Jane ngay lập tức sẽ đi theo đường này để xâm nhập vào mạng doanh nghiệp của Acme. Vì trojan sử dụng địa chỉ IP của Jane, nên hệ thống firewall của Acme coi đó là một truy cập MAPI hợp lệ, và không hề ngăn chặn.
3. Khi Jane ngắt kết nối, con trojan đã xâm nhập thành công vào máy chủ của Acme và ăn cắp mọi email để gửi về cho hacker Joe.
Để ngăn chặn kiểu tấn công này, Juniper đã đưa ra giới thiệu giải pháp Secure Acess SSL VPN (truy cập bảo mật qua mạng riêng ảo, dùng giao thức lớp socket bảo mật), cho phép mạng doanh nghiệp thực hiện truy cập bảo mật từ xa, với các mức quản lý ở cấp ứng dụng. Sản phẩm NetScreen Remote Acces 500 của Juniper là giải pháp SSL VPN thừa hưởng nền tảng giải pháp hoàn thiện, với thiết kế dành riêng cho các doanh nghiệp vừa và nhỏ.
Đặc điểm của việc quản lý từ lớp mạng ứng dụng của SSL VPN là xác định riêng từng ứng dụng xem truy cập nào là hợp lệ hay không. Chẳng hạn, cùng là cổng 80 trên máy chủ, nhưng nếu truy cập từ trình duyệt Internet Explorer thì được chấp nhận, còn các ứng dụng khác thì không cho phép. Không phải mọi trao đổi MAPI đều là hợp lệ, nếu xuất phát từ ứng dụng Outlook thì cho phép, còn từ các ứng dụng khác (trong ví dụ trên là truy cập của trojan vào máy chủ) thì bị chặn lại.
Ngoài ra SSL VPN còn cung cấp khả năng quản trị máy trạm Zero client administration, tự động cài các phần mềm cần thiết lên máy trạm qua ActiveX và Java của trình duyệt, hay xác định tình trạng bảo mật và nâng cấp chống virus của một máy tính trước khi cho phép kết nối vào máy chủ. SSL VPN cũng cho phép quét một máy trạm để phát các chương trình ăn cắp dữ liệu hoặc xâm nhập như Key logger (chặn bắt tín hiệu nhập từ bàn phím để ăn cắp mật khẩu), Malware, Spyware (phần mềm do thám hoạt động truy cập của người sử dụng để phá hoại)... Như ở ví dụ trên, SSL VPN sẽ dễ dàng phát hiện và ngăn chặn trojan truy cập qua giao thức MAPI khi không phải là ứng dụng Outlook.
JUNOS - Giải pháp ISP, chi phí doanh nghiệp
Juniper cũng đã giới thiệu giải pháp nền tảng hạ tầng hệ thống vững chắc với các model router và hệ điều hành mạng JUNOS của mình. Phần mềm này có đặc tính tuỳ biến để đáp ứng các nhu cầu sử dụng khác nhau, từ các nhà cung cấp dịch vụ lớn tới những doanh nghiệp nhỏ.
Khi các nhà cung cấp dịch vụ chuyển từ cùng cấp các kết nối mạng IP sang các giải pháp đảm bảo và nhiều khả năng hơn, họ cần có những hệ điều hành có chứa các tính năng Intranet, các dịch vụ và khả năng bảo mật. Phần mềm thiết bị mạng JUNOS của Juniper không chỉ cung cấp một hệ điều hành cực mạnh và ổn định, mà còn có rất nhiều bộ công cụ dịch vụ IP phong phú. Thông qua khả năng bảo mật và ổn định tốt nhất, phần mềm JUNOS đảm bảo một nền tảng IP có thể dự đoán trước và hoạt động hiệu quả. Với tác động ổn định và khả năng sẵn có của hệ thống mạng, khách hàng có thể trao đổi giữa các bộ phận hệ thống một cách rất linh hoạt, tạo ra các môi trường ứng dụng riêng biệt, hoặc triển khai các dịch vụ IP tạo ra doanh thu.
Khả năng tuỳ biến - JUNOS có thể sử dụng một thiết kế phần mềm linh động, cung cấp khả năng "đàn hồi" đặc biệt và đảm bảo các tính năng mới như IPv6 có thể được tích hợp dễ dàng.

Chuyên môn về Routing - Kinh nghiệm chuyên môn đặc biệt về routing của Juniper Networks IP mang lại một giao thức định tuyến được củng cố vững chắc.

Hợp chuẩn - JUNOS tuân theo các chuẩn công nghiệp về routing, MPLS, và các cơ chế sẵn có như Protocol Graceful Restart để tăng cường độ ổn định và giảm phức tạp khi vận hành cho khách hàng.

Bảo mật - JUNOS kết hợp việc xử lý gói tin thông minh với hiệu suất xử lý cao để cung cấp cho khách hàng một bộ công cụ bảo mật IP hiệu quả.

Phong phú về dịch vụ - bất kể là một thuê bao cá nhân, doanh nghiệp, hay nhà cung cấp dịch vụ, các danh mục dịch vụ IP của JUNOS cũng cho phép khách hàng triển khai các dịch vụ mạng đảm bảo tới bất kỳ nhóm người dùng cuối nào.

Kiểm soát và chính sách - Nền tảng Juniper Networks SDX và NMC cho phép khách hàng sử dụng và kiểm soát các khả năng rất mạnh của JUNOS; Ngoài ra, giao diện Juniper Networks JUNOScript XML cũng đơn giản hoá và tăng tốc độ tích hợp OSS với cấu trúc phần mềm Modular.
Là sản phẩm đã được chứng tỏ về hiệu quả trong các mạng IP lớn nhất thế giới, hệ điều hành JUNOS sẽ giúp các khách hàng chuyển đổi nền tảng hạ tầng mạng IP của họ sang một mạng Infranet – một con đường giúp nhà cung cấp dịch vụ gặt hái được thành công về lợi nhuận.

Lời cuối: Cám ơn bạn đã theo dõi hết cuốn truyện.
Nguồn: http://vnthuquan.net
Phát hành: Nguyễn Kim Vỹ.

Nguồn: Theo VietnamNet
Được bạn: mickey đưa lên
vào ngày: 5 tháng 12 năm 2004