

Công nghệ mạng riêng ảo SSL VPN và ứng dụng trong xây dựng hệ thống truyền tệp : Luận văn ThS / Nguyễn Đình Nghĩa ; Nghd. : PGS.TS. Nguyễn Văn Tam . - H. : ĐHCN, 2006 . - 87 tr. + CD-ROM

Tóm tắt: Giới thiệu tổng quan về mạng riêng ảo: các khái niệm, phân loại, các yêu cầu đối với mạng riêng ảo. Trình bày về công nghệ SSL trong việc xây dựng mạng riêng ảo SSL VPN bao gồm cấu trúc, nguyên lý hoạt động, các vấn đề về an ninh. Đề xuất một mô hình truyền tệp dựa trên công nghệ SSL, thiết kế và cài đặt thử nghiệm

Lời cảm ơn

Lời cam đoan

Mục lục	1
Danh mục các chữ viết tắt, thuật ngữ.....	4
Danh mục các hình vẽ.....	5
Mở đầu.....	8
Chương 1 Tổng quan về mạng riêng ảo.....	10
1.1 Khái niệm chung về mạng riêng ảo.....	10
1.2 Phân loại mạng riêng ảo.....	12
1.2.1 Phân loại VPN theo việc cung cấp dịch vụ.....	12
1.2.2 Phân loại VPN theo kỹ thuật sử dụng trong VPN.....	16
1.2.3 Phân loại VPN theo nhóm chức năng.....	16
1.2.4 Phân loại VPN theo nhóm công nghệ và mô hình OSI.....	18
1.2.5 Phân loại VPN theo nơi xử lý VPN.....	18
1.3 Các thành phần của mạng riêng ảo.....	19
1.3.1 Máy chủ phục vụ truy cập mạng NAS.....	19
1.3.2 Bộ định tuyến.....	19
1.3.3 Máy nguồn và máy đích đường hầm.....	19

1.3.4 Máy chủ phục vụ xác thực.....	20
1.3.5 Tường lửa - Firewall.....	20
1.3.6 Máy chủ chính sách.....	21
1.3.7 VPN Gateway.....	21
1.4 Đường hầm trong VPN.....	21
1.4.1 Khái niệm đường hầm.....	21
1.4.2 Các giao thức đường hầm.....	22
1.5 Các yêu cầu cơ bản đối với VPN.....	29
1.5.1 Xác thực trong VPN.....	29
1.5.2 Tính bí mật dữ liệu trong VPN.....	32
1.5.3 Tính toàn vẹn dữ liệu trong VPN.....	32
1.6 Kết luận chương.....	33
Chương 2 Công nghệ mạng riêng ảo SSL VPN.....	34
2.1 Giới thiệu.....	34
2.1.1 Lịch sử phát triển của giao thức SSL.....	34
2.1.2 SSL và mô hình OSI.....	35
2.2 Các khái niệm an ninh được sử dụng trong SSL.....	36
2.2.1 Mã hoá.....	36
2.2.2 Hàm băm và bản tóm lược thông điệp.....	37
2.2.3 Mã xác thực thông điệp.....	38
2.2.4 Mã hoá khóa công khai và chữ ký điện tử.....	38
2.2.5 Chứng chỉ số và cơ quan cung cấp chứng chỉ số.....	39
2.3 Giao thức đường hầm SSL.....	40
2.3.1 Giao thức bắt tay SSL.....	40
2.3.2 Giao thức bản ghi SSL.....	53
2.3.3 Giao thức cảnh báo SSL.....	56
2.3.4 Giao thức ChangeCipherSpec.....	57
2.3.5 Khuôn dạng các thông điệp giao thức bắt tay.....	58
2.4 Thiết lập đường hầm trong SSL VPN.....	63
2.5 So sánh SSL VPN và IPSec VPN.....	64
2.6 Kết luận chương.....	66
Chương 3 Xây dựng hệ thống truyền tệp dựa trên hoạt động của giao thức SSL...67	
3.1 Phát biểu bài toán.....	67
3.2 Thiết kế hệ thống.....	68

3.3 Giao thức trao đổi dữ liệu SSLFTP.....	69
3.4 Nguyên tắc hoạt động của hệ thống.....	69
3.4.1 Khởi tạo phiên giao tiếp.....	69
3.4.2 Các thông điệp trao đổi trong pha thiết lập liên kết.....	71
3.4.3 Xác thực máy chủ tệp.....	72
3.4.4 Tạo các tham số phiên.....	73
3.4.5 Đóng gói và gửi thông điệp.....	74
3.4.6 Các thuật toán sử dụng trong hệ thống.....	74
3.5 Thiết kế các thông điệp trao đổi dữ liệu.....	75
3.5.1 Khuôn dạng thông điệp của giao thức bản ghi SSLFTPRecord.....	75
3.5.2 Khuôn dạng thông điệp của các giao thức tầng trên.....	75
3.6 Bảo vệ các thông điệp.....	79
3.6.1 Tính toán mã xác thực thông điệp.....	80
3.6.2 Mã hoá dữ liệu.....	80
3.7 Thiết kế module chương trình.....	81
3.7.1 Module trên máy chủ xác thực.....	81
3.7.2 Module trên máy chủ tệp.....	82
3.7.3 Module trên máy khách.....	82
3.8 Cài đặt thử nghiệm.....	83
3.8.1 Cài đặt trên máy chủ xác thực.....	83
3.8.2 Cài đặt trên máy chủ tệp.....	84
3.8.3 Cài đặt trên máy khách.....	85
Kết luận chung.....	87
Tài liệu tham khảo.....	88
Phụ lục	
Phụ lục A	
Phụ lục B	
Phụ lục C	
Phụ lục D	
Phụ lục E	
Phụ lục F	

