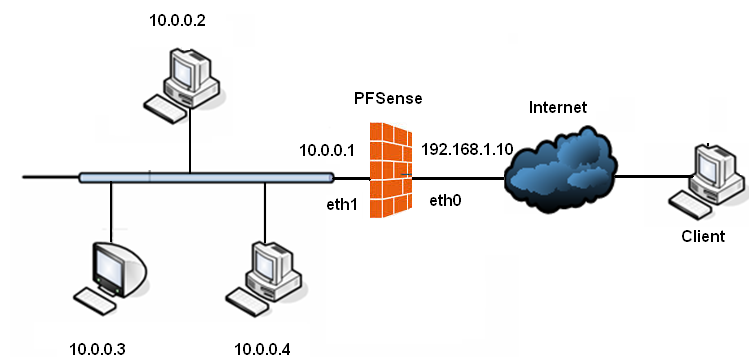
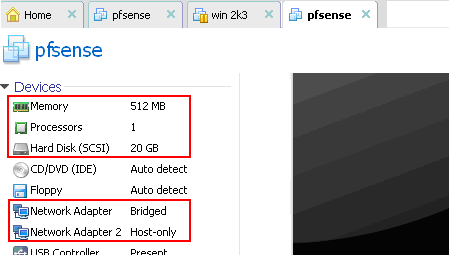
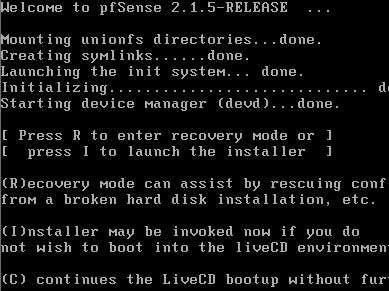
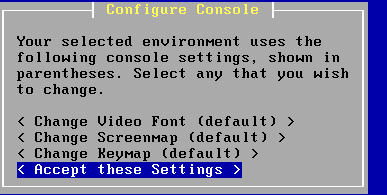
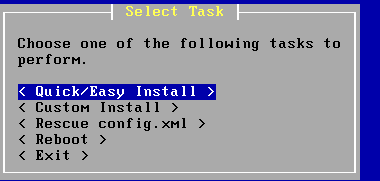
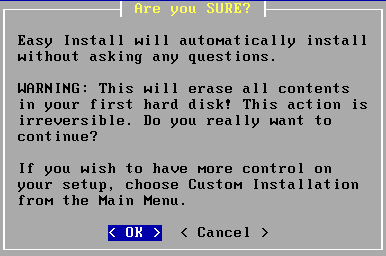
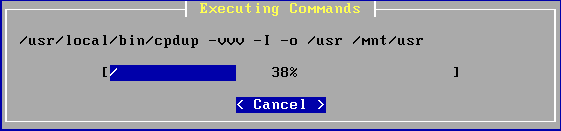
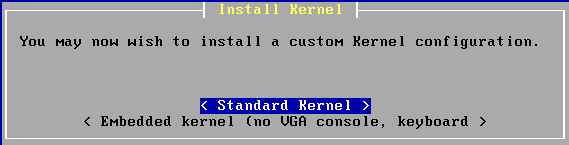
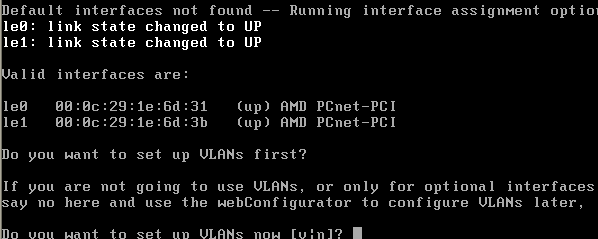
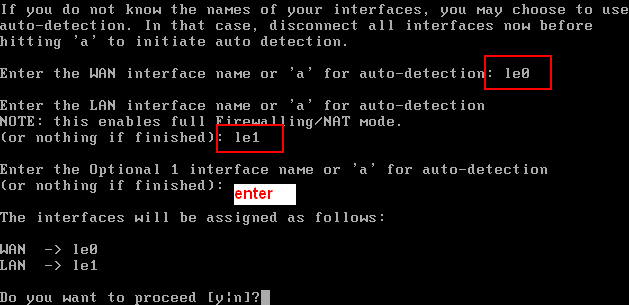
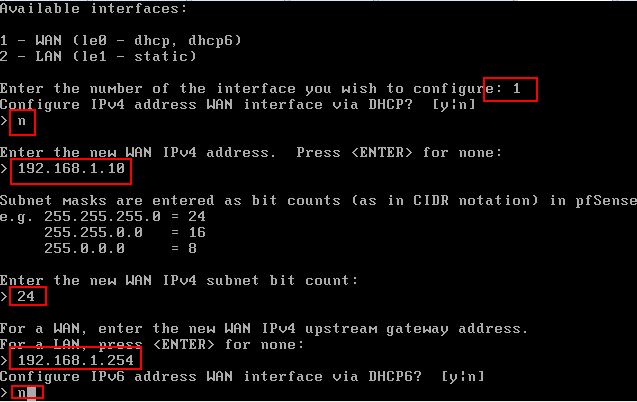
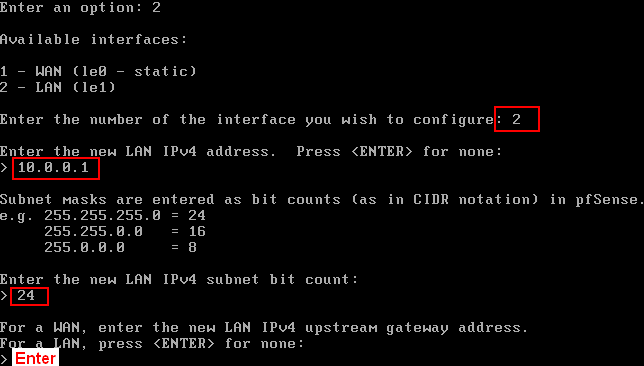
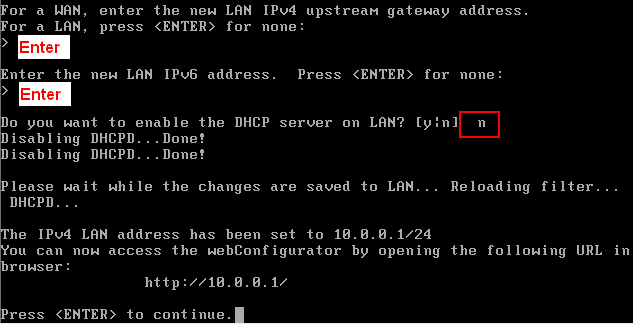
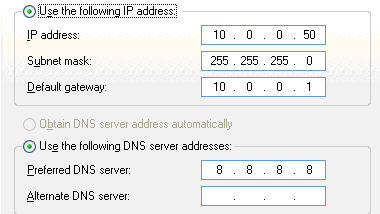
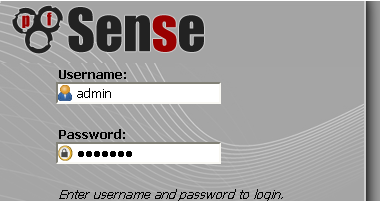
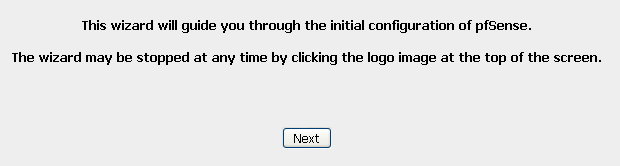
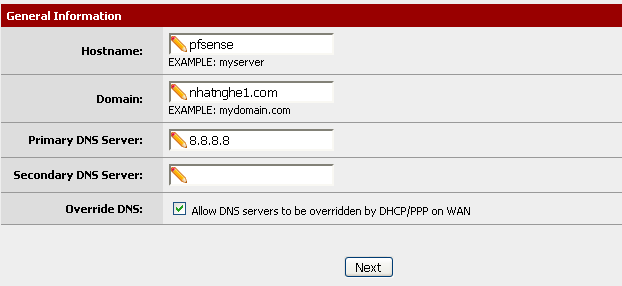
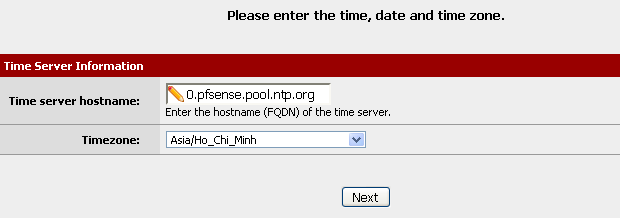
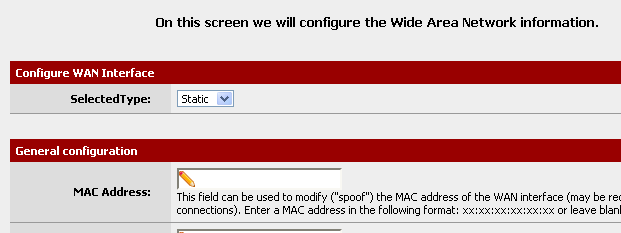
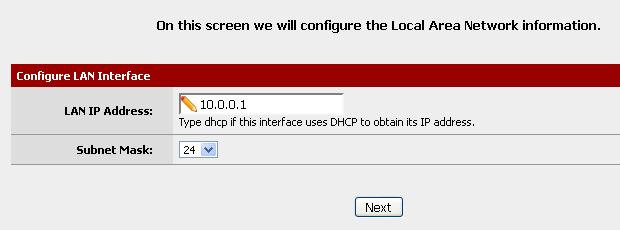
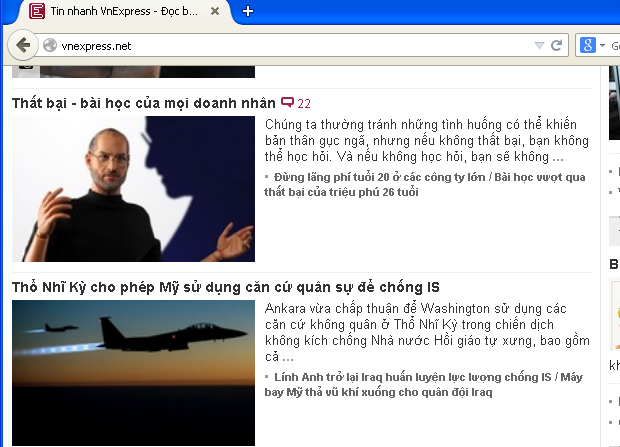
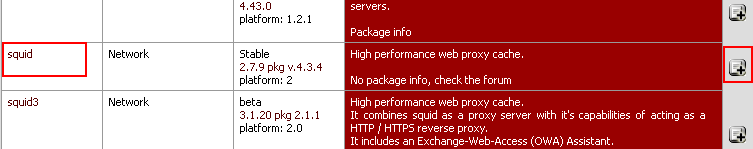
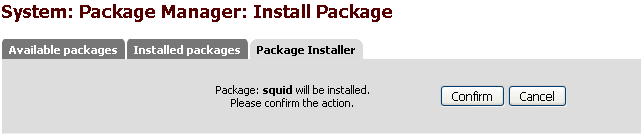
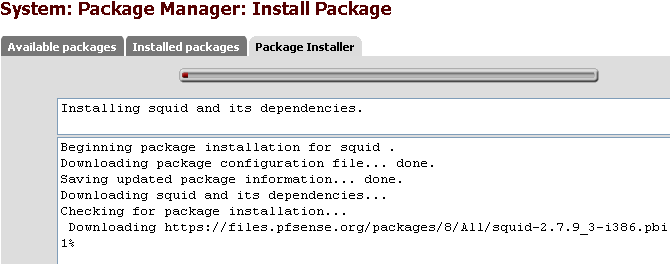
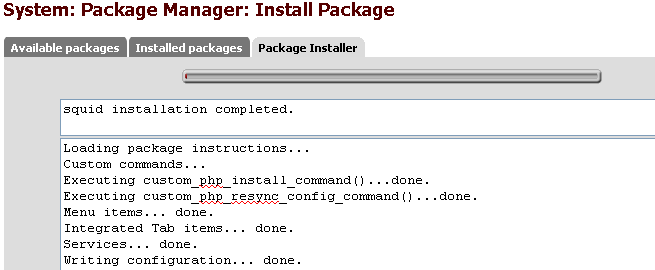
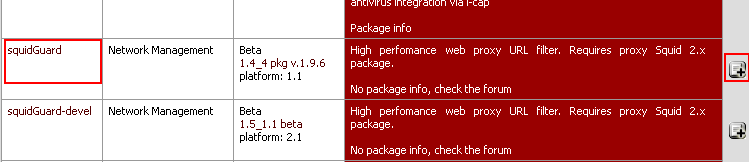
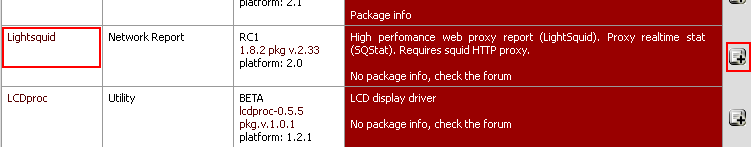
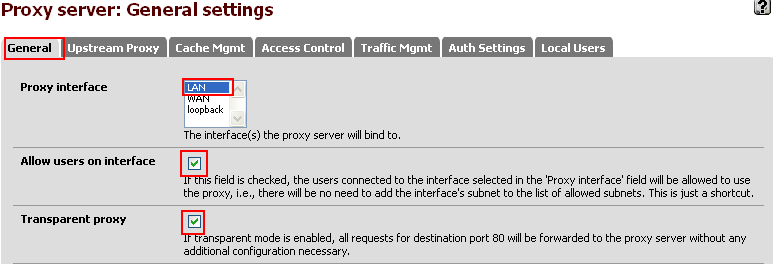
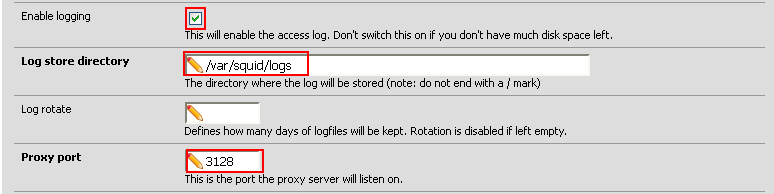
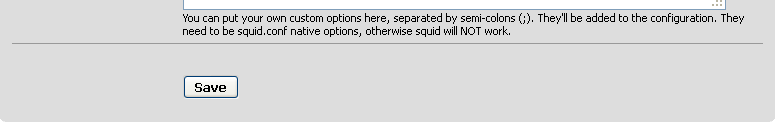
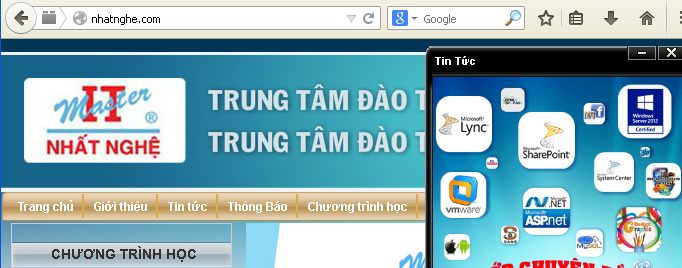
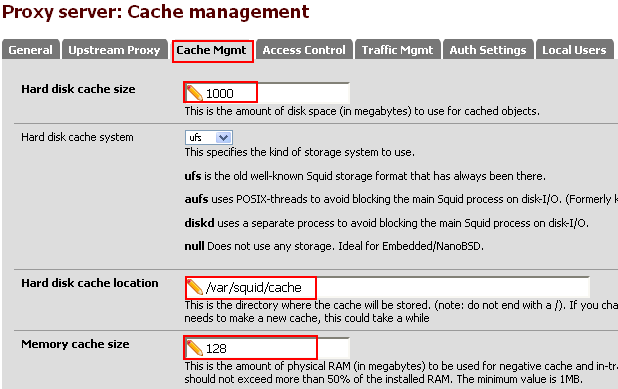
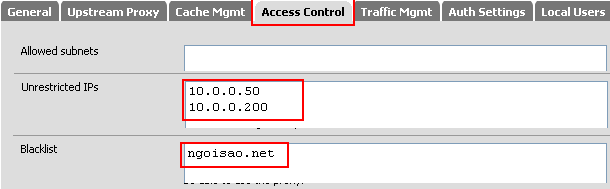
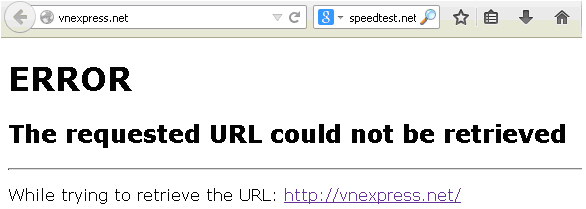
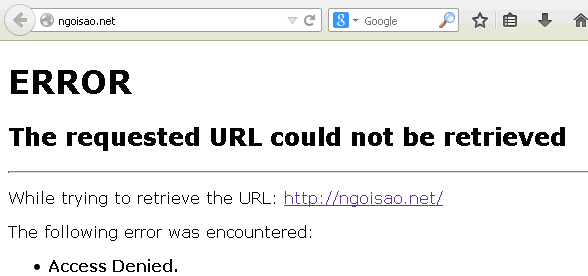
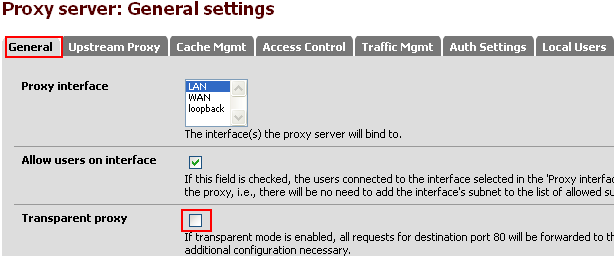
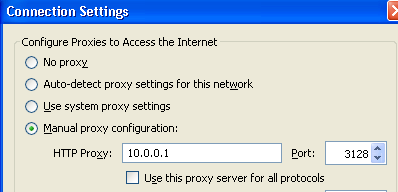
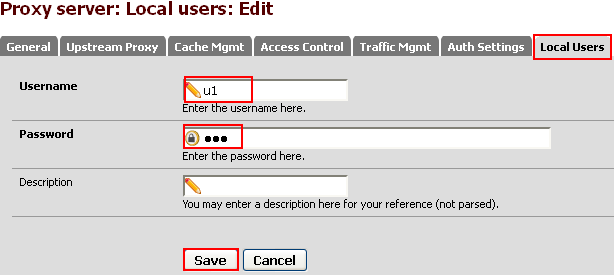
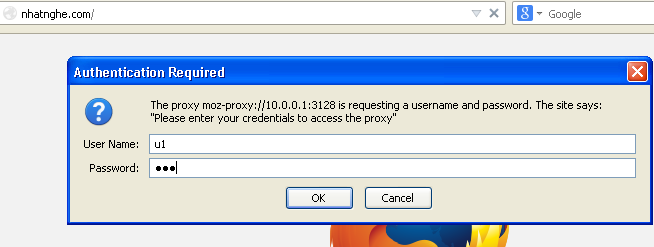
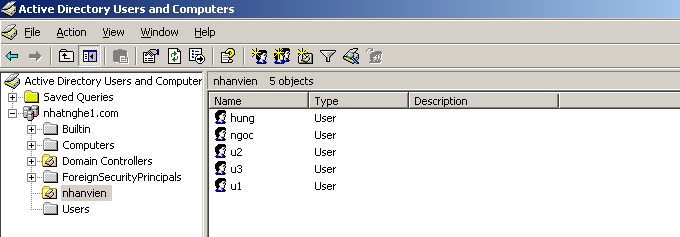
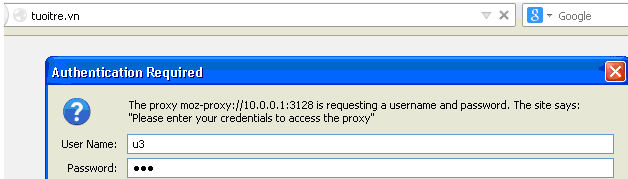
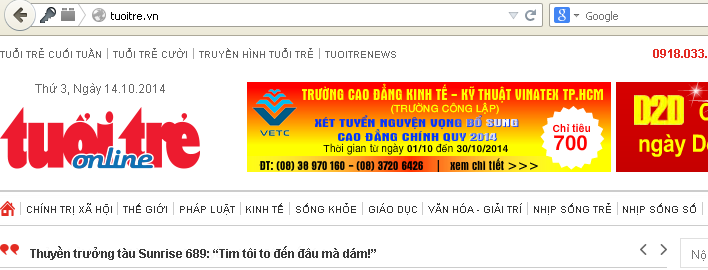
**Phần 1: Cài đặt Pfsense**

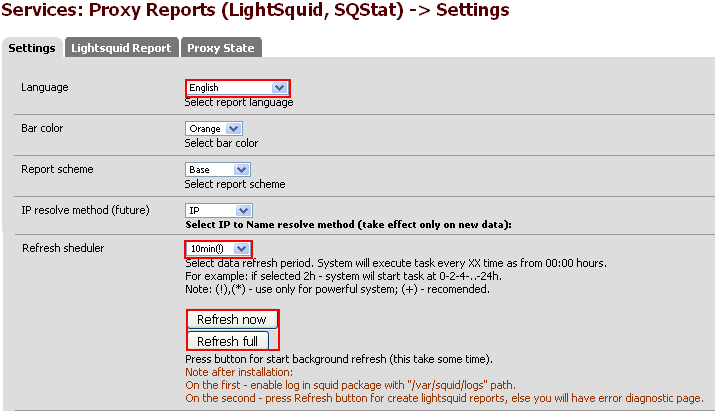
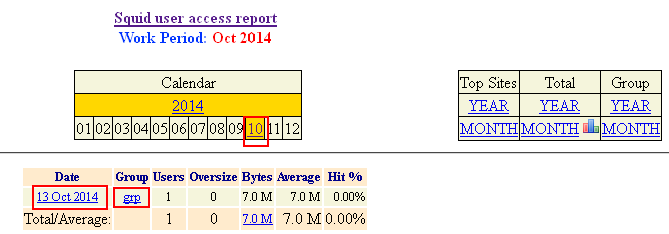
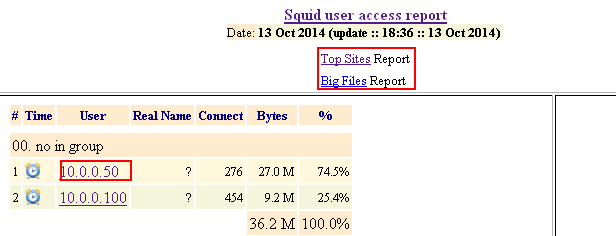
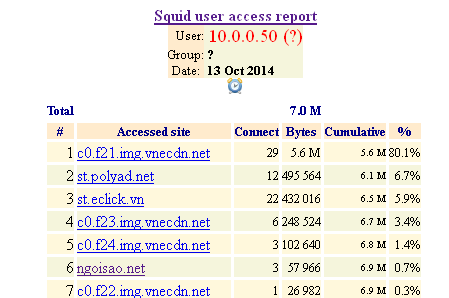
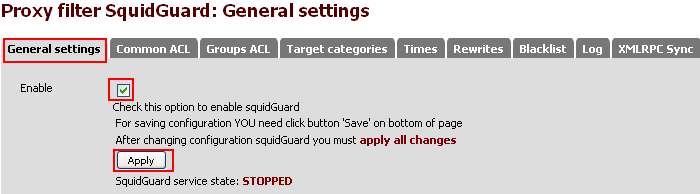
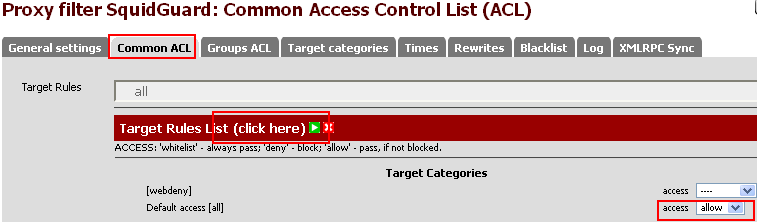
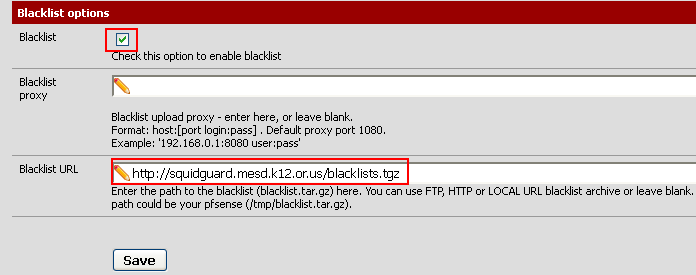
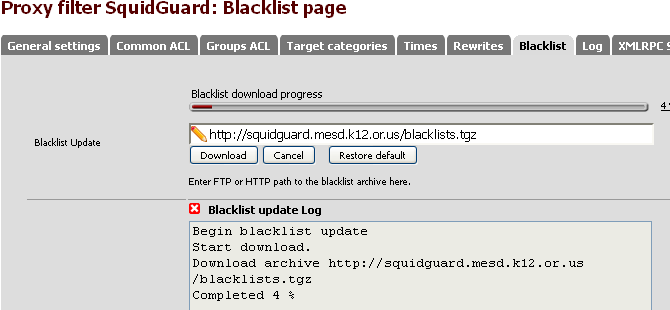
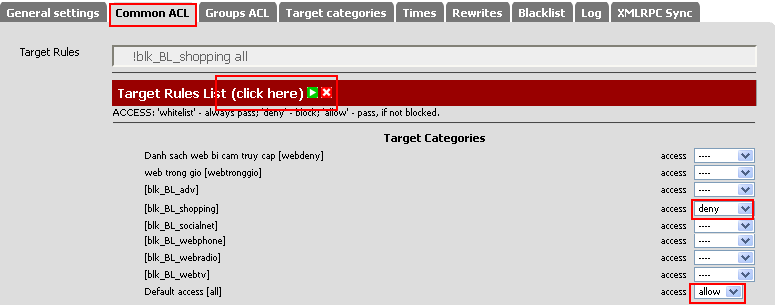
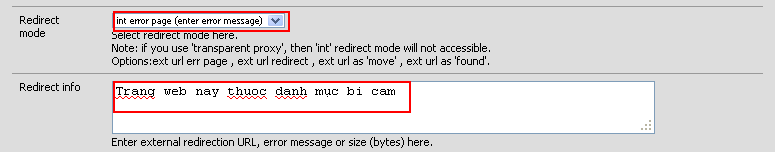
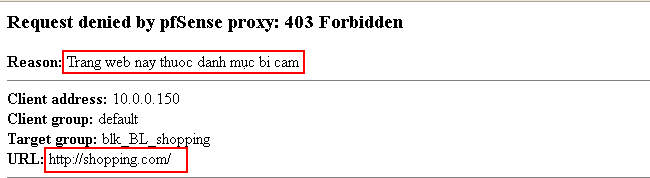
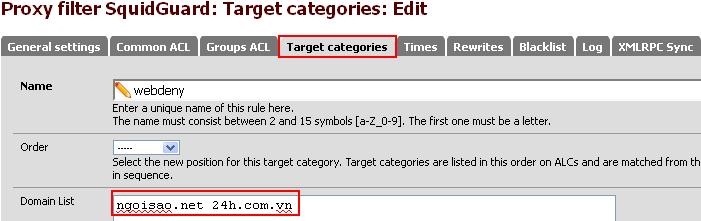
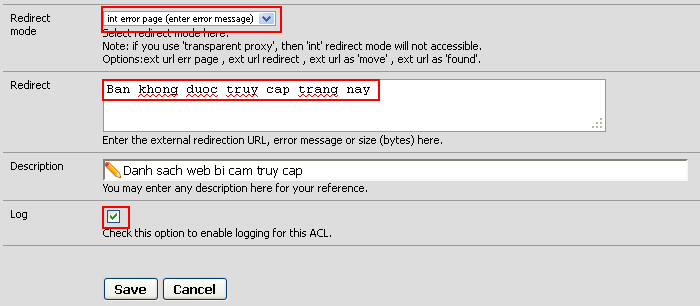
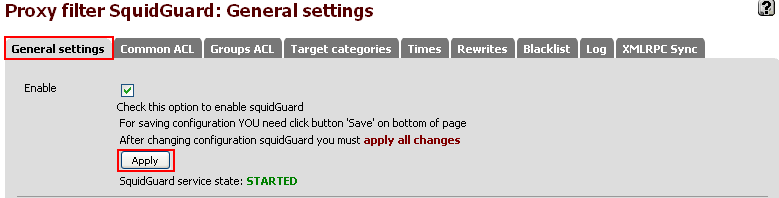
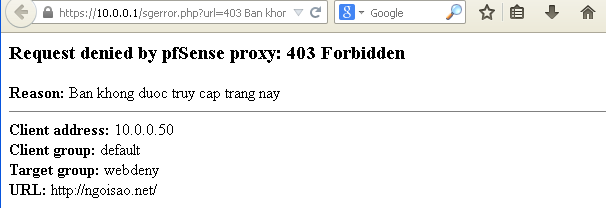
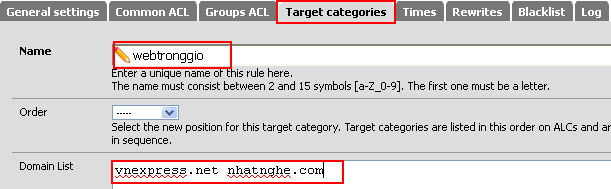
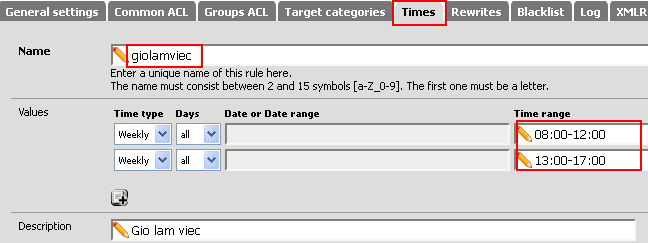
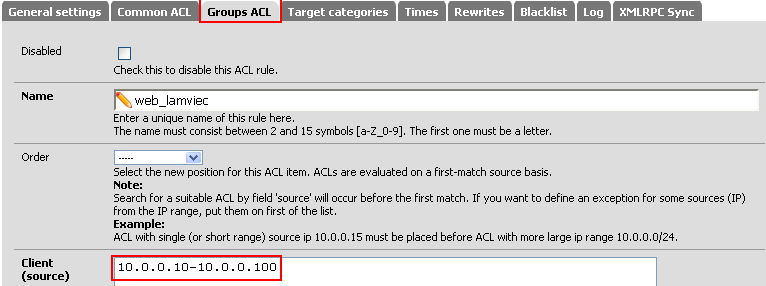
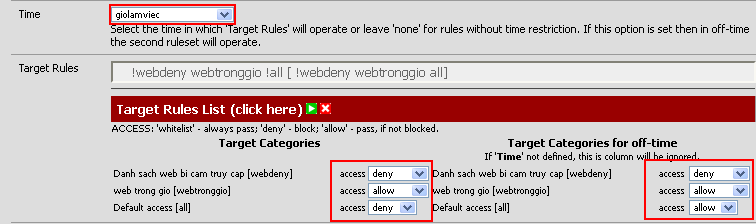
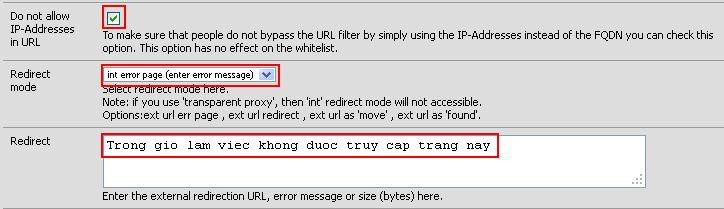
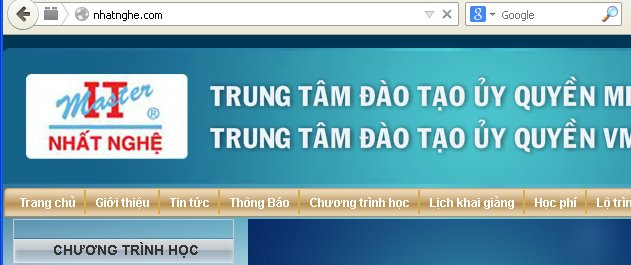
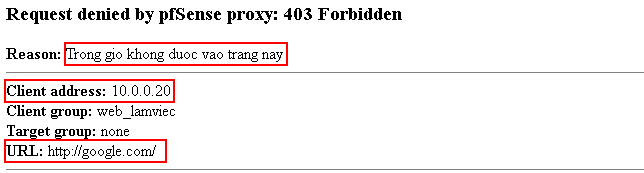
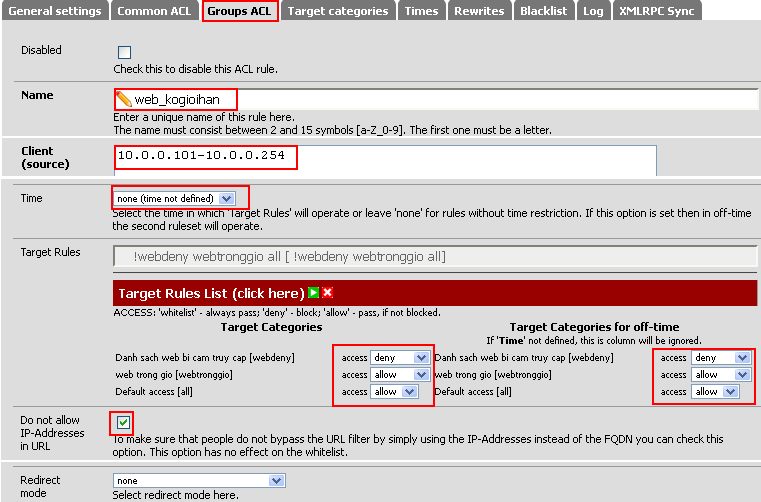
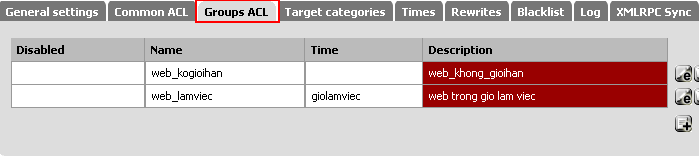
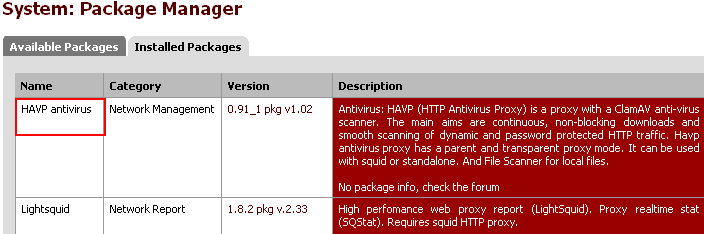
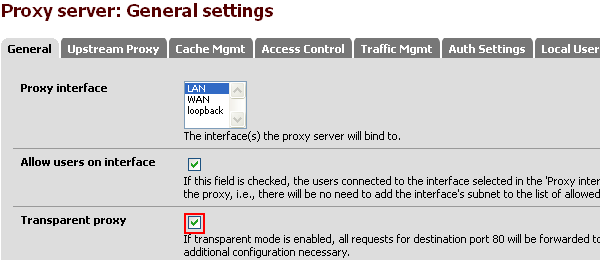
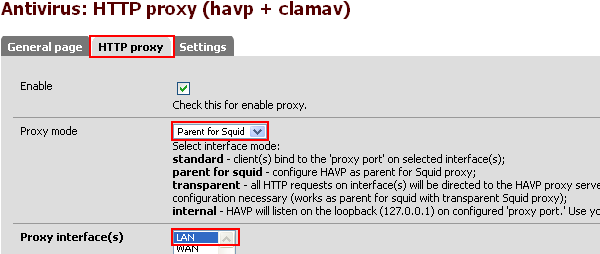
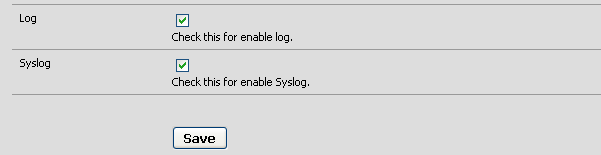
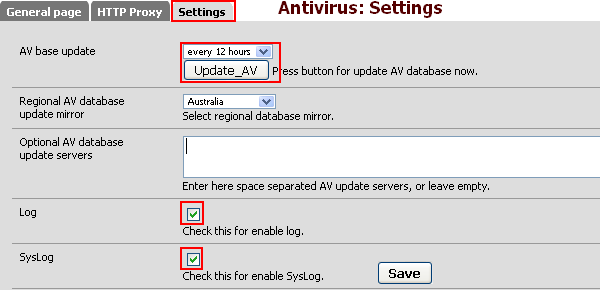
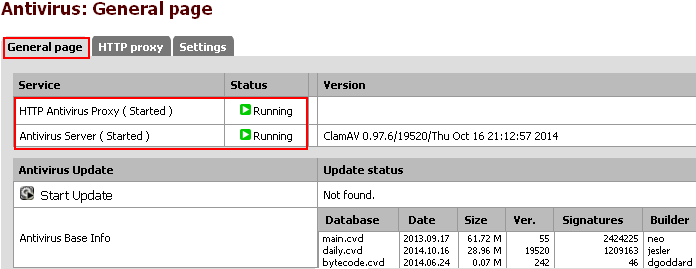
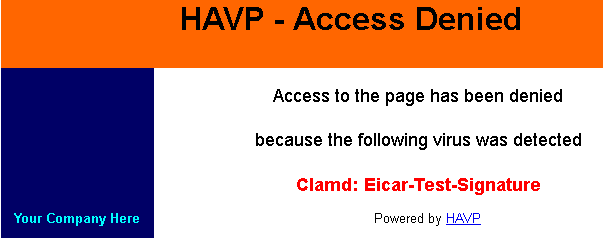
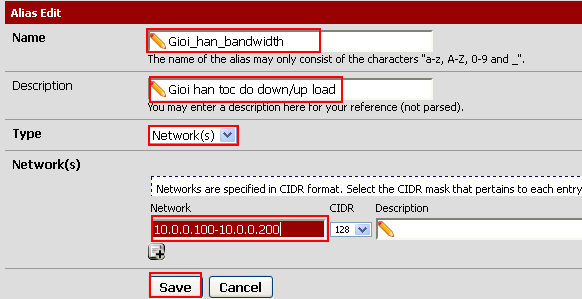
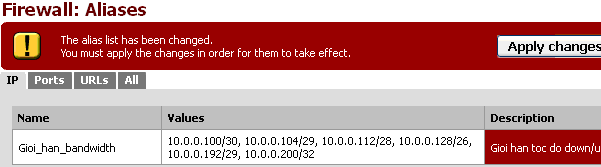
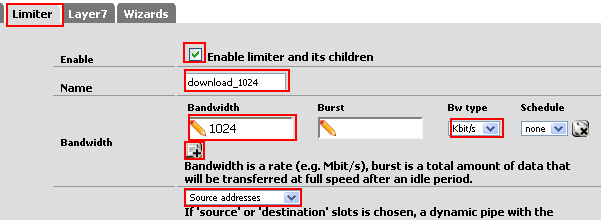
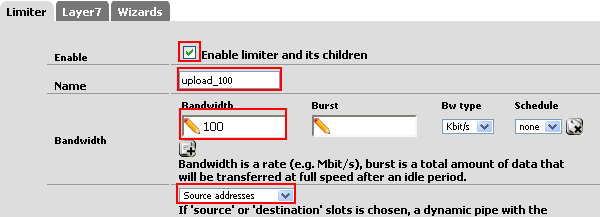
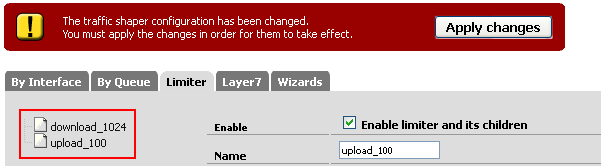
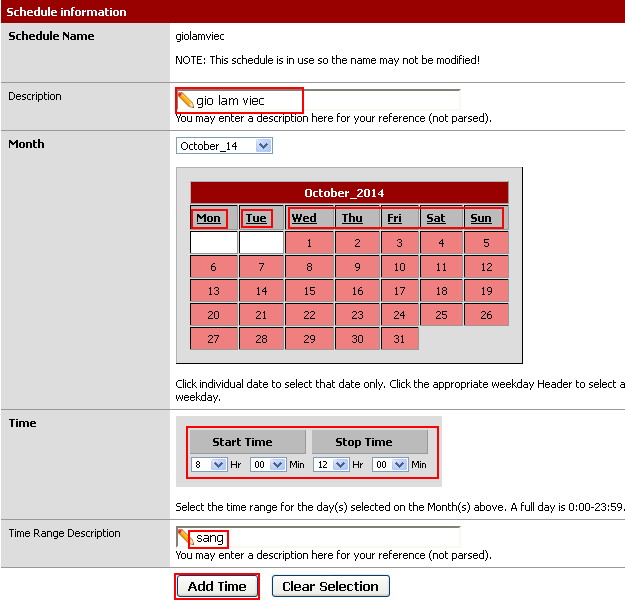
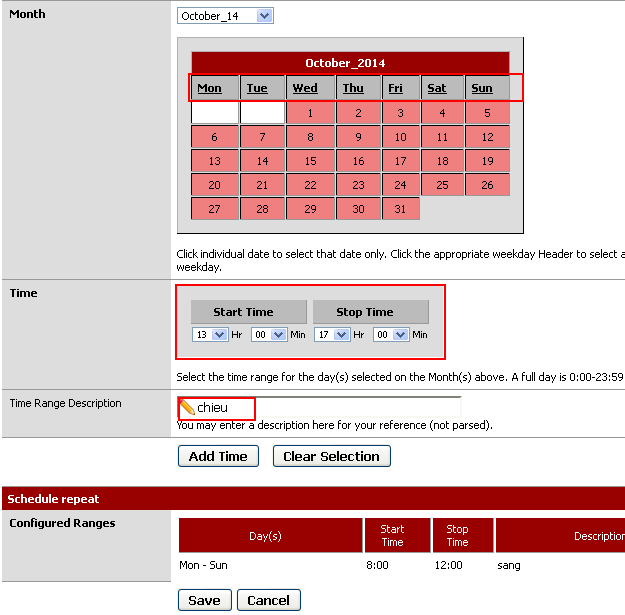
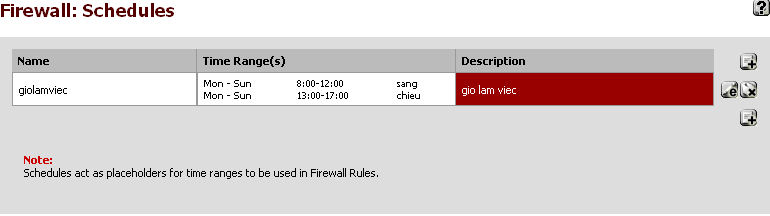
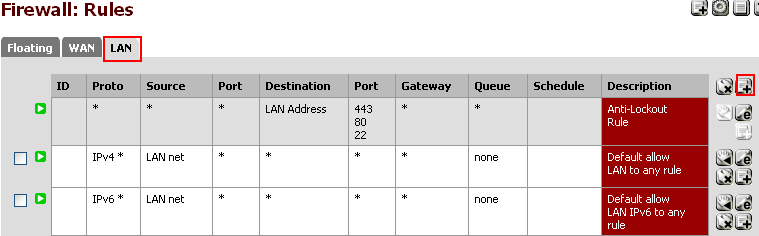
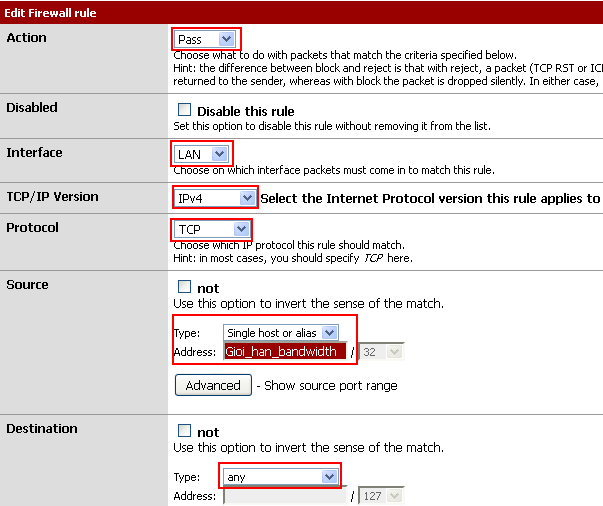
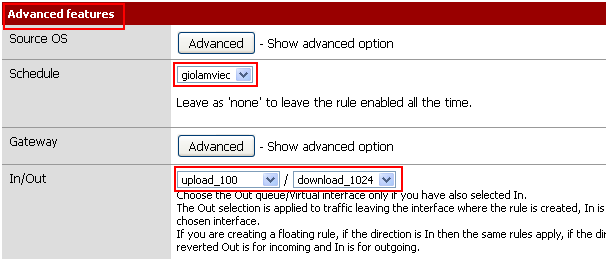
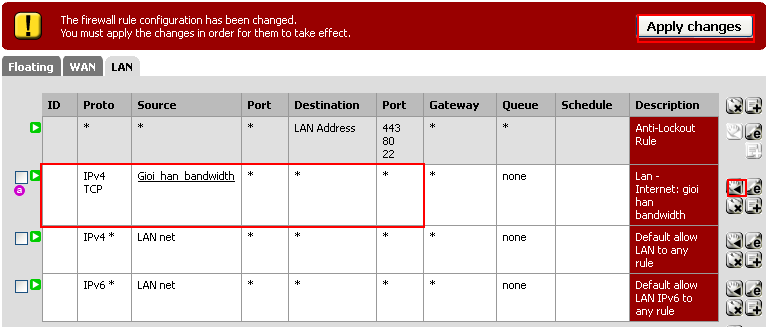
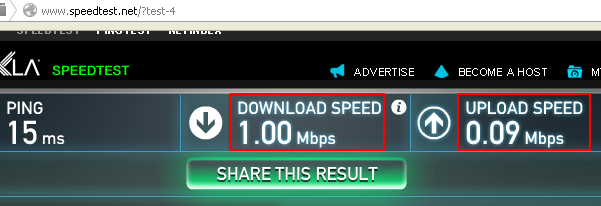
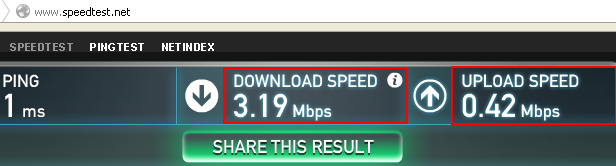
**Giảng viên: Đỗ Quang Ngọc**

[Xây dựng tường lửa với PFSense - Phần 2](http://www.nhatnghe.com/forum/showthread.php?p=2000492#post2000492)  
  
Mô hình mạng  
  
**1. Cài máy PFsense**  
B1. Trên VMWare, Tạo máy ảo có cấu hình như sau  
  
  
  
  
  
  
  
B2. Nhấn Enter  
  
  
B3. Nhấn I để cài đặt (press I to launch the installer)   
  
  
B4. Chọn Accept these settings ,chấp nhận các tham.   
  
B5. Chọn Quick/Easy Install  
  
  
B6. Nhấn OK để bắt đầu cài đặt   
  
Quá trình cài đặt bắt đầu  
  
  
B7. Chọn Standard Kernel  
  
  
B8. Chọn Reboot để khởi động máy   
  
  
B9. Chọn N, không cấu hình V-LAN  
  
  
B10. Nhập tên Lan card:   
kết nối WAN, nhập le0,  
kết nối LAN, nhập le1. Nhấn Enter, chọn Y  
  
  
  
B11. Chọn mục 2 để gán IP cho Lan card  
  
  
  
B12. Chọn 1, Nhấn N.   
- Nhập IP 192.168.1.10 cho WAN interface  
- Nhập 24 cho độ dài Subnet  
- Nhập IP 192.168.1.254, khai báo default gateway  
- Chọn N, bỏ qua Ipv6 cho WAN interface  
  
  
B13. Chọn mục 2 để gán IP cho Lan card  
  
  
  
B14. Chọn 2,   
- Nhập IP 10.0.0.1 cho LAN interface  
- Nhập 24 cho độ dài Subnet  
- Nhấn Enter  
  
  
  
  
B15. Nhấn Enter, Chọn N, nhấn Enter để kết thúc  
  
  
  
**2. Quản trị Pfsense**  
  
B1. Máy client trong mạng LAN, đặt IP như hình  
  
B2. Nhập username: admin  
Password: pfsense   
  
B3. Nhấn Next, Next  
  
  
B4. Nhập tên máy, tên domain và DNS  
Nhấn Next  
  
  
B5. Nhập Timezone, Nhấn Next  
  
  
  
B6. Khai báo thông tin cho WAN interface, nhấn Next đẻ bỏ qua  
  
  
B7. Khai báo thông tin cho LAN interface, nhấn Next đẻ bỏ qua  
  
  
  
B8. đổi password cho user admin, nhấn Reload  
  
B9. tại đây máy client trong LAN có thể truy xuất Internet theo cơ chế NAT  


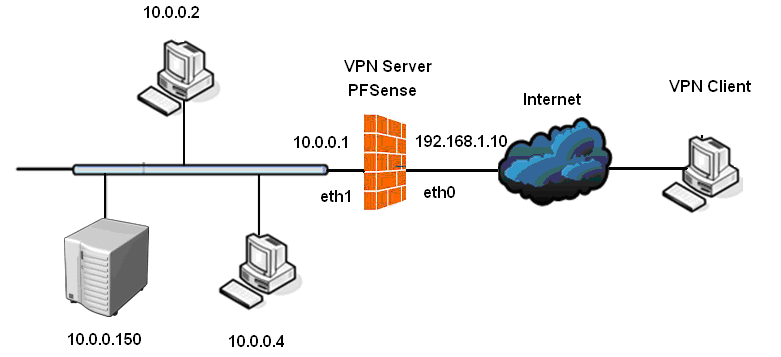
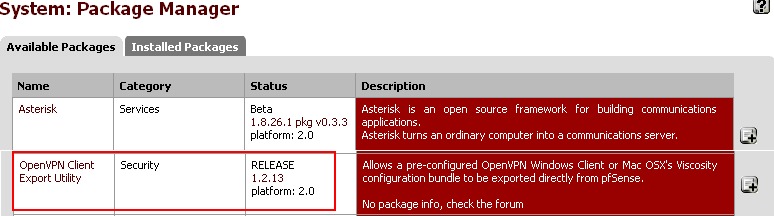
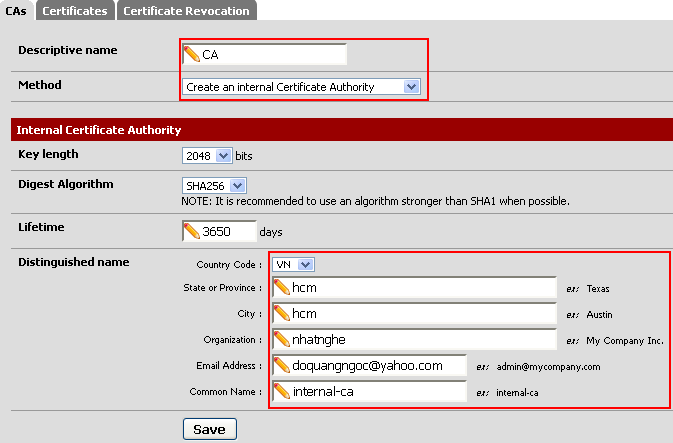
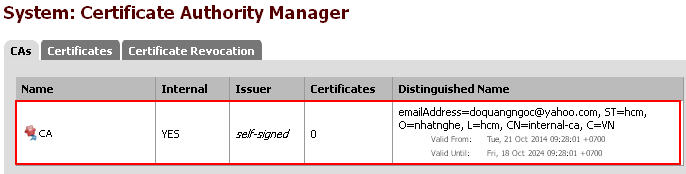
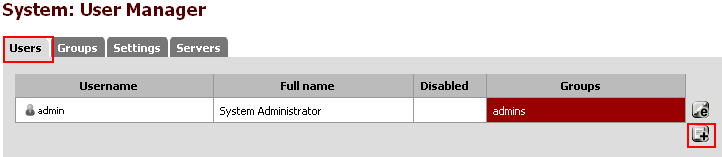
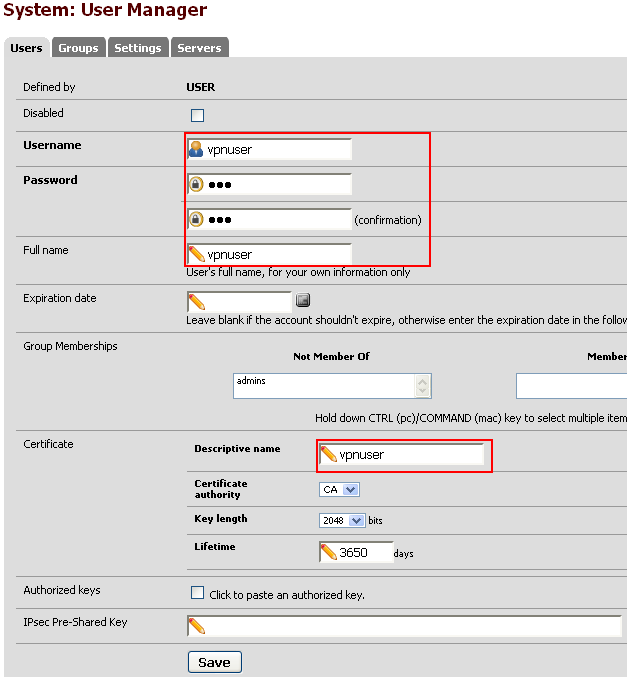
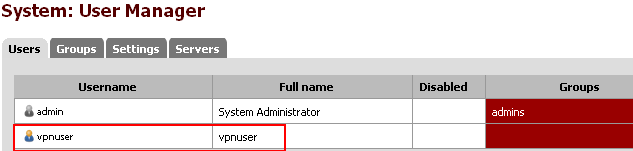
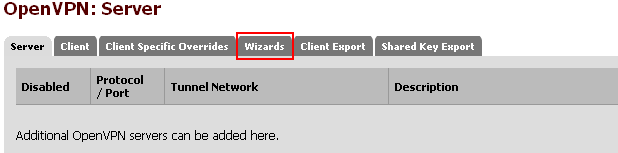
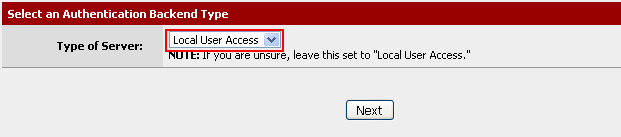
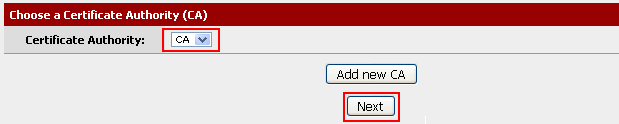
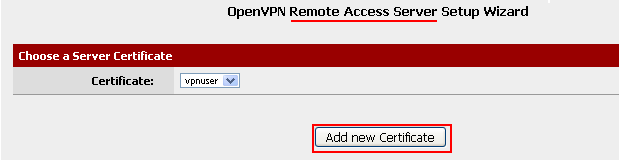
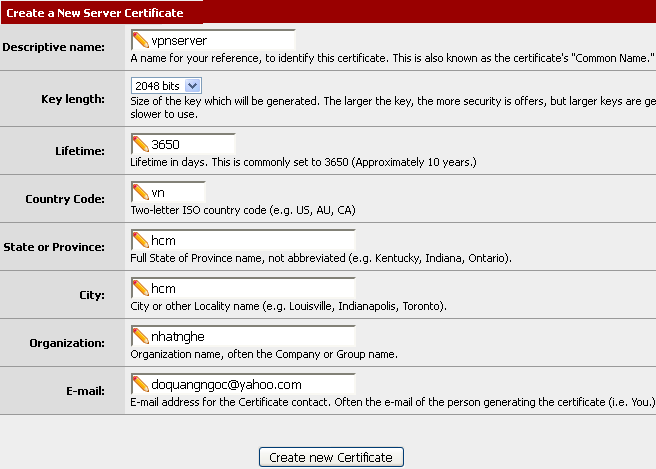
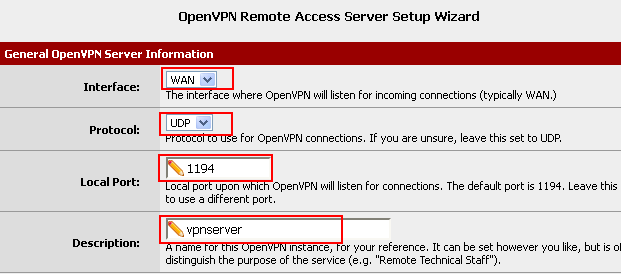
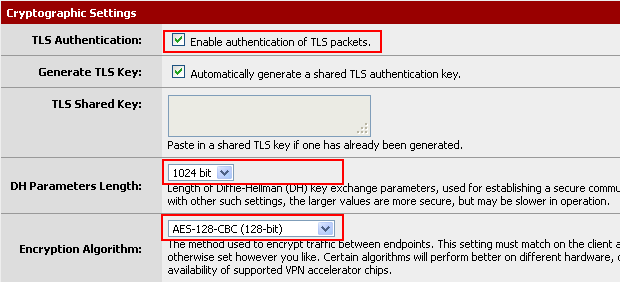
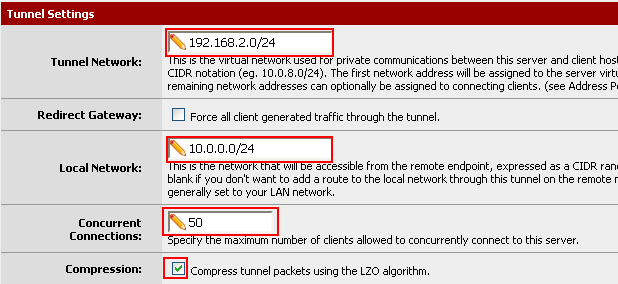
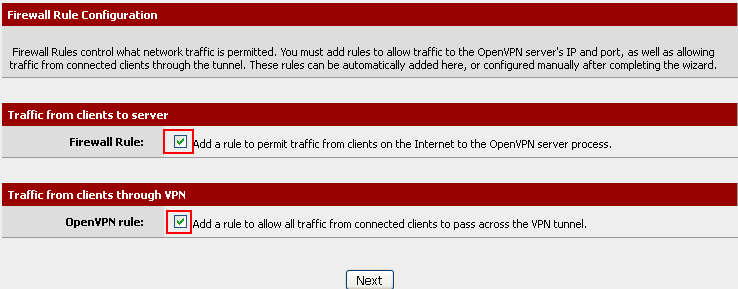
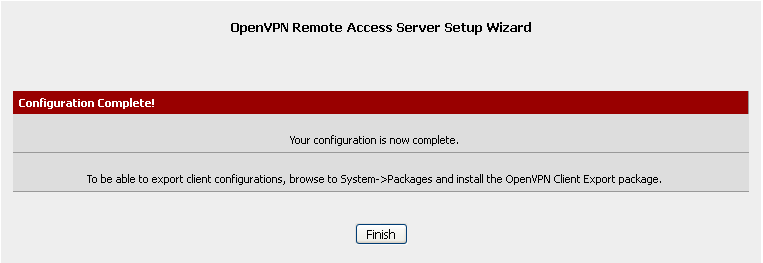
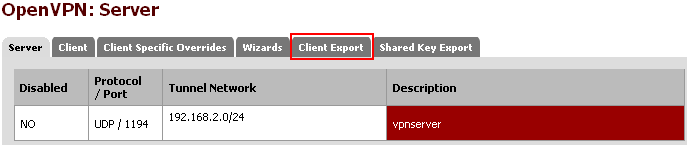
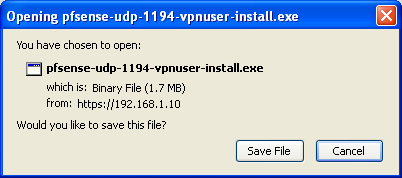
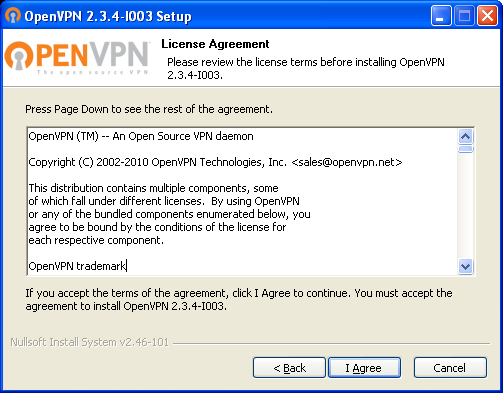
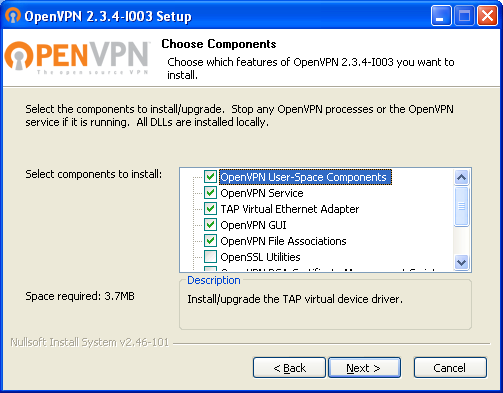
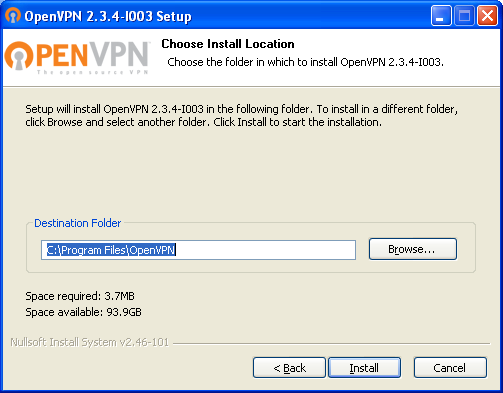
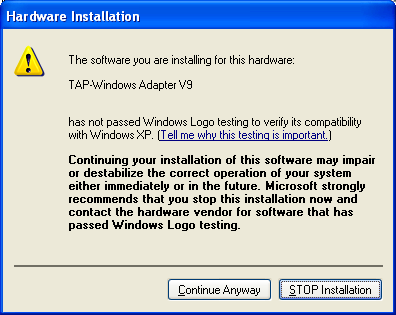
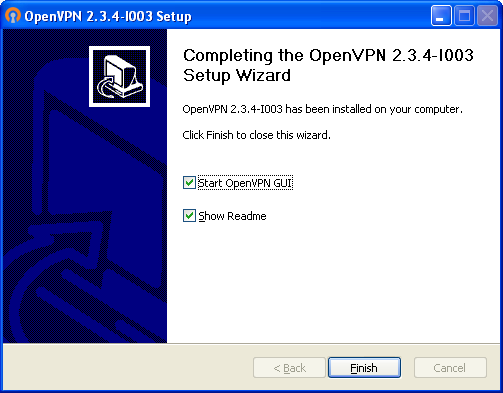
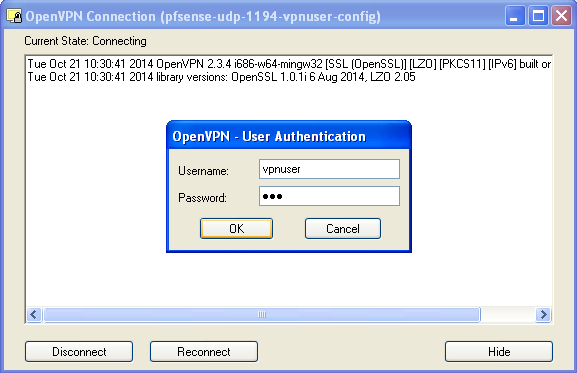
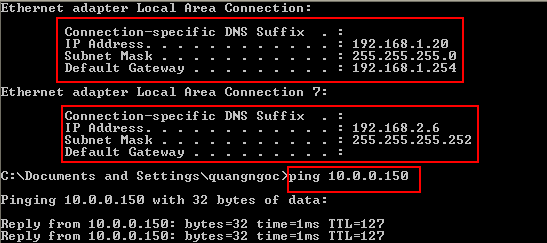
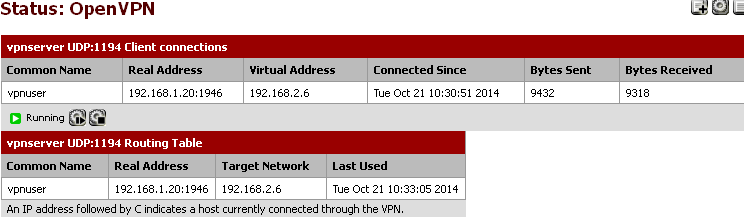
**Proxy server (1)**

[Xây dựng tường lửa với PFSense - Phần 1](http://www.nhatnghe.com/forum/showthread.php?t=820061)  
  
Mục đích: Quản lý, giám sát truy cập internet  
  
**1. Chuẩn bị**  
Cài các gói cần thiết  
  
**1.1 cài gói squid**  
- System, Packages, chọn squid, nhấn dấu +  
  
  
  
- Chọn Confirm  
  
  
  
- Quá trình cài bắt đầu  
  
  
  
Quá trình cài kết thúc  
  
  
**1.2 cài gói squidGuard**  
- System, Packages, chọn squidGuard, nhấn dấu +  
  
  
  
**1.3 cài gói Lightsquid**  
- System, Packages, chọn Lightsquid, nhấn dấu +  
  
  
  
**2. Cấu hình Proxy server:  
2.1. Cấu hình chung**  
- Service, chọn Proxy server, General  
  
+ Proxy interface: chọn LAN  
+ Allow users on interface: check  
+ Transparent proxy: check  
  
  
+ Enable logging: check  
+ Log store directory: /var/squid/logs  
  
  
  
- Chọn Save  
  
  
  
- Tại máy client có thể truy cập Internet (không cần phải cấu hình proxy tại client)  
  
  
  
**2.2. Cấu hình C ache - Tăng tốc độ truy cập web**  
- Service, chọn Proxy server, C ache mgmt  
+ Hard disk c ache size: dung lượng ổ cứng làm cache  
+ Hard disk c ache location: vị trí cache lưu trữ trên ổ cứng  
+ Memory c ache size: dung lượng RAM lách c ache  
  
  
- Chọn save  
  
**3. Giới hạn truy cập**  
- Service, chọn Proxy server, Access control  
- Banned host addresses: Nhập danh sach địa chỉ IP cấm truy cập  
- Blacklist : Danh sach web site cấm truy cập   
  
- Chọn Save  
  
  
  
- Tại máy 10.0.0.50 truy cập web sẽ báo lỗi  
  
  
  
- Tại máy 10.0.0.51 truy cập ngoisao.net sẽ báo lỗi  
  
  
**4. Chứng thực user truy cập web**  
- Service, chọn Proxy server, General  
- Transparent proxy: bỏ check  
- Chọn Save  
  
  
  
Tại client cấu hình chỉ trình duyệt đến proxy server  
  
  
**4.1 Chứng thực Local user**  
- B1. Service, chọn Proxy server, Local user  
- Add user  
  
+ User name: u1  
+ Password: 123  
+ Chọn Save  
  
  
  
  
- B2. Service, chọn Proxy server, Auth Settings  
+ Authentication method: chọn Local  
+ Chọn Save  
  
  
- B3. Máy client truy cập web phải nhập username và password   
  
  
  
**4.2 Chứng thực DC user**  
- B1. Tại máy DC 10.0.0.150 tạo các user u1, u2, u3  
  
  
  
- B2. Service, chọn Proxy server, Auth Settings  
Nhập các thông tin:  
+ Authentication method: LAP  
+ LDAP version: 3  
+ Authentication server: 10.0.0.150  
+ Authentication server port: 389  
+ LDAP server user DN: cn=u1,ou=nhanvien,dc=nhatnghe1,dc=com  
+ LDAP password: 123  
+ LDAP base domain: dc=nhatnghe1,dc=com  
+ LDAP username DN attribute: uid  
+ LDAP search filter: sAMAccountName=%s  
  
- Chọn Save  
  
  
  
B3. Máy client truy cập web nhập username u3, password: 123  
  
  
- Truy cập thành công  
  


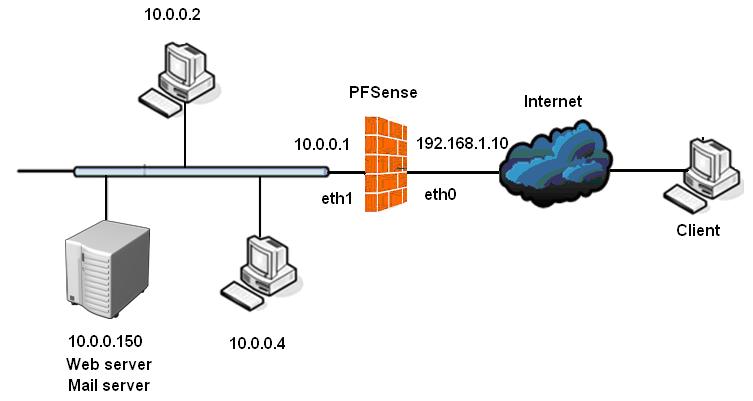
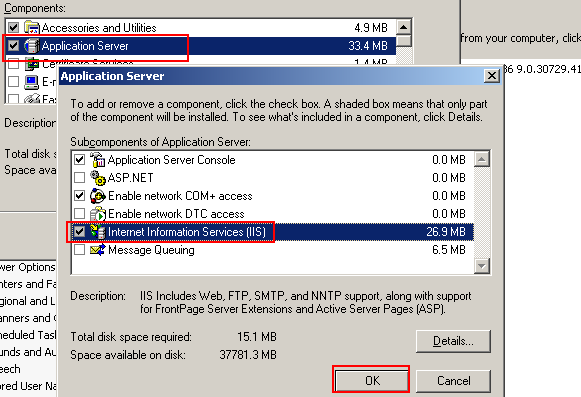
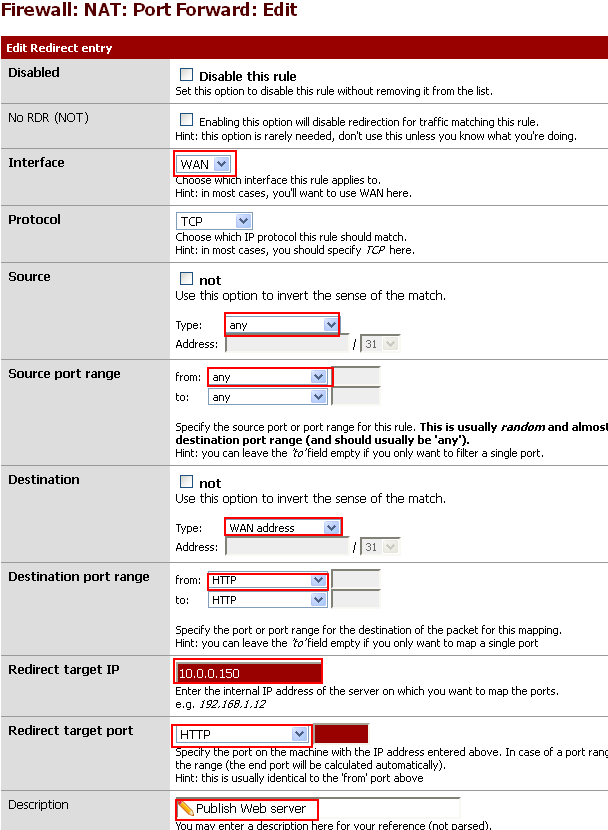
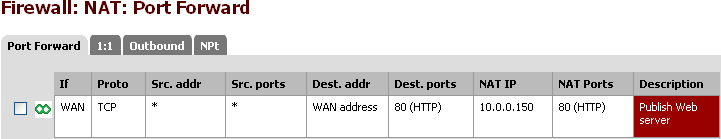
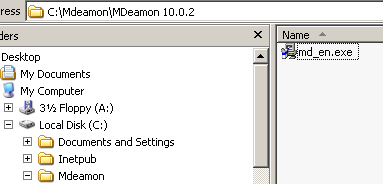
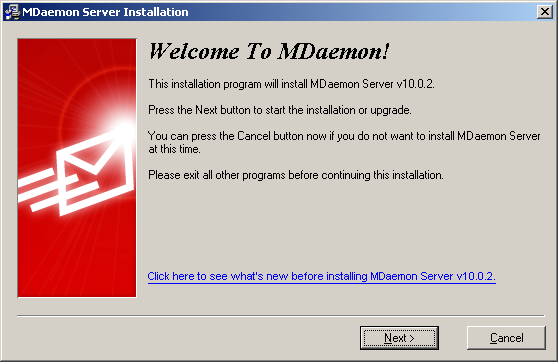
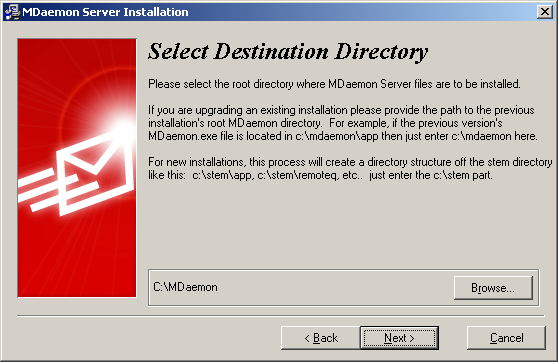
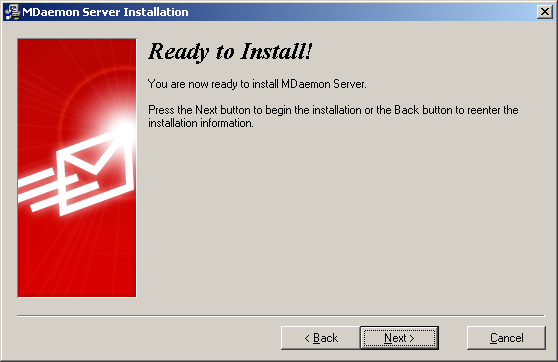
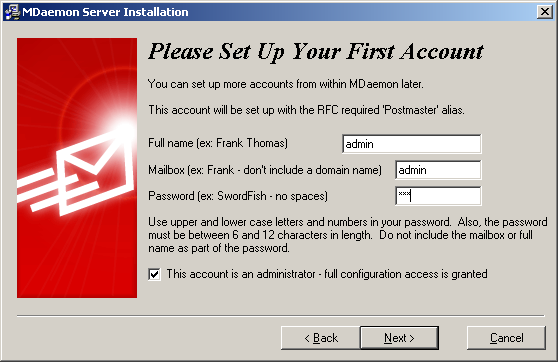
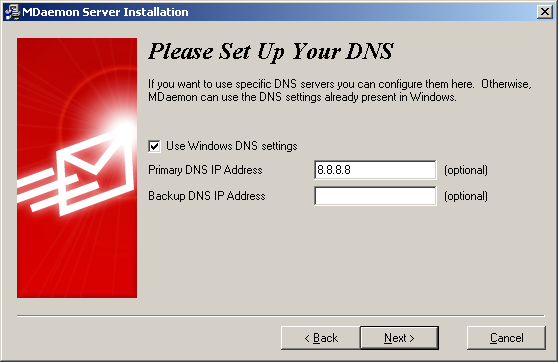
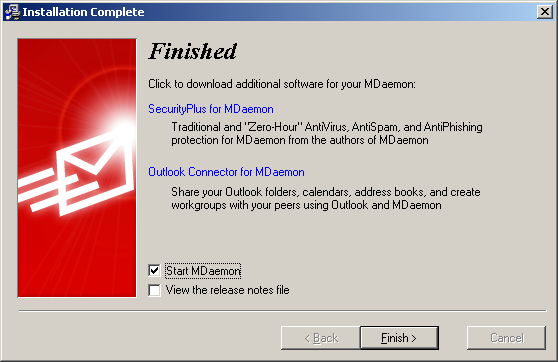
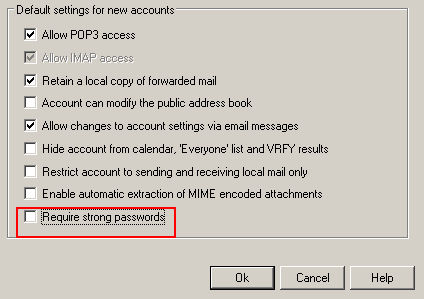
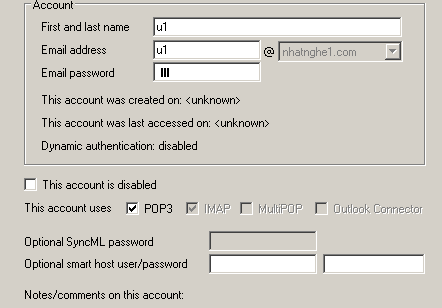
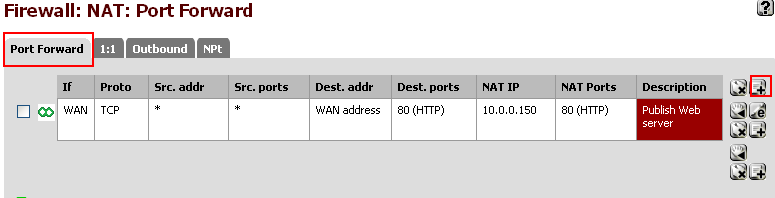
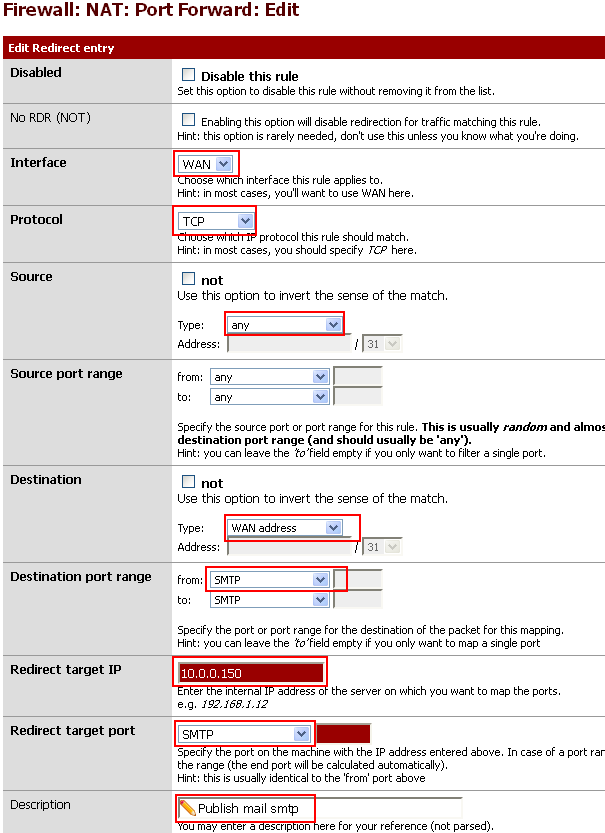
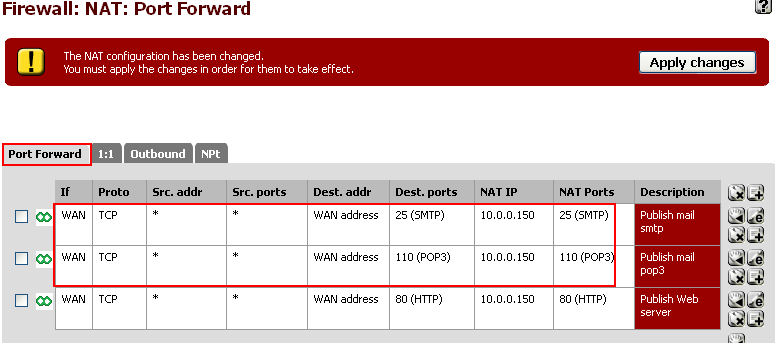
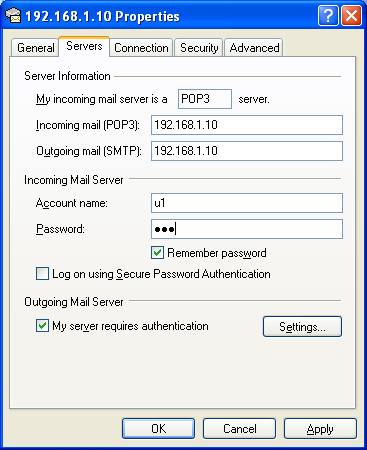
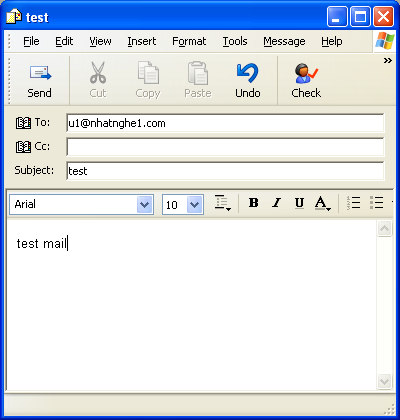
**Proxy Server (2)**

Giảng viên hướng dẫn: Đỗ Quang Ngọc  
  
[Xây dựng tường lửa PFSense - Phần 1](http://www.nhatnghe.com/forum/showthread.php?t=820061)  
  
[Xây dựng tường lửa PFSense - Phần 2](http://nhatnghe.com/forum/showthread.php?p=2000492#post2000492)  
  
**5. Thống kê truy cập**  
  
**5.1 Cấu hình chung**  
- Status, Proxy reports, settings  
  
+ Language: chọn English  
+ Refresh sheduler: chọn 10min  
+ Nhấn: Refresh  
+ Chọn Save  
  
  
  
**5.2 Xem báo cáo truy cập**  
- Status, Proxy reports, Lightsquid Report  
  
+ Chọn tháng, ngày, Group cần xem báo cáo  
  
  
  
  
+ Thống kê theo User hoặc Top sites, Big files  
  
  
  
+ Thống kê theo User  
  
  
  
**6. Squid Guard**  
- Lọc web nâng cao  
  
SquidGuard can be used to   
• limit the web access for some users to a list of accepted/well known web servers and/or URLs only.   
• block access to some listed or blacklisted web servers and/or URLs for some users.   
• block access to URLs matching a list of regular expressions or words for some users.   
• enforce the use of domainnames/prohibit the use of IP address in URLs.   
• redirect blocked URLs to an info page.   
• redirect banners to an empty GIF.   
• have different access rules based on time of day, day of the week, date etc.   
  
- Service, Proxy filter, General Setting  
+ Check Enable, chọn apply  
  
  
  
- Chọn Common ACL, nhấn click here  
+ Default access [all]: chọn allow  
+ chọn: Save  
  
  
  
Các máy client truy cập web bình thường  
  
  
**6.1 Blacklist**  
- Service, Proxy filter, General Setting  
  
+ Blacklist URL:   
+ Nhập <http://squidguard.mesd.k12.or.us/blacklists.tgz>   
hoặc <http://www.shallalist.de/Downloads/shallalist.tar.gz>  
+ Chọn Save  
  
  
  
- Chọn thẻ Blacklist, nhấn download   
  
  
  
- Khi download kết thúc, chọn Common ACL  
  
+ [blk\_BL\_shopping] : Chọn Deny  
+ Default access [all] : Chọn Allow  
  
- Redirect mode: int error page  
- Redirect info: Nhập thông báo lỗi  
  
  
  
- Chọn Save, Apply  
- Tại máy client truy cập trang shopping.com  
  
  
  
**6.2 Cấu hình truy cập web**  
  
Tất cả các PC trong LAN không được truy cập:  
ngoisao.net   
24h.com.vn  
  
  
- Service, Proxy filter, General Setting, Target categories  
+ Name: nhập webdeny  
+ Domain List: ngoisao.net 24h.com.vn  
  
  
  
+ Redirect mode: int error page(enter error message)  
+ Nếu chọn “ext err page(enter URL)“ sẽ chuyển hướng đến web site khác   
+ Redirect: [http://nhatnghe.com](http://nhatnghe.com/)  
+ Redirect: “Ban khong duoc truy cap trang nay”  
- Chọn Save  
  
  
  
- Chọn Common ACL  
  
- Danh sach web bi cam truy cap [webdeny] chọn deny  
  
  
  
- Chọn General settings, Apply  
  
  
  
- Mở trình duyệt , truy cập trang ngoisao.net sẽ báo lỗi   
- Chú ý: xóa cache trình duyệt nếu cần  
  
  
  
**6.2 Giớ hạn giờ truy cập web**  
- Chú ý: deny tất cả các rule trong common ACL  
  
  
**Rule1.Các pc 10.0.0.10-10.0.0.100  
Trong giờ làm việc  
Chỉ được truy cập trang web: vnexpress.net nhatnghe.com  
Ngoài giờ truy cập không giới hạn**  
  
**Rule 2: Các pc 10.0.0.101-10.0.0.254 truy cập web không giới hạn ở bất kỳ thời đểm nào**  
  
B1. Service, Proxy filter, General Setting, Target categories  
- Nhấn + tạo rule mới  
  
+ Name: nhập webtronggio  
+ Domain List: nhập vnexpress.net nhatnghe.com  
+ Chọn Save  
  
  
  
B2. Service, Proxy filter, General Setting, Times  
+ Name: giolamviec  
+ Values: weekly 08:00-12:00  
weekly 13:00-17:00  
+ Description: Gio lam viec  
+ Chọn Save  
  
  
  
B.3 Service, Proxy filter, General Setting, Groups ACL  
+ Name: web\_lamviec  
+ Client (source) 10.0.0.10-10.0.0.100  
+ Time giolamviec  
+ Target Rules chọn   
+ Danh sach web bi cam truy cap [webdeny] deny deny  
+ web trong gio [webtronggio] allow allow  
+ Default access [all] deny deny  
+ Redirect Nhập thông báo lỗi  
  
  
  
  
  
  
  
- Chọn Save  
  
B4. Kiểm tra  
  
a. Trong giờ làm việc truy cập thành công vnexpress.net nhatnghe.com  
  
  
  
b. Trong giờ làm việc truy cập không được google.com và các trang khác.  
  
  
  
c. Ngoài giờ làm việc, truy cập bất cứ trang web nào  
  
d. Máy client không thuộc dải IP 10.0.0.10-10.0.0.100 cũng không truy cập web do chưa được phép  
  
B5. Các pc 10.0.0.101-10.0.0.254 truy cập web không giới hạn ở bất kỳ thời đểm nào  
  
- Service, Proxy filter, General Setting, Groups ACL  
- Nhấn + tạo rule mới  
+ Name: web\_kogioihan  
+ Client (source) 10.0.0.101-10.0.0.254  
+ Time none  
+ Target Rules chọn  
  
+ Danh sach web bi cam truy cap [webdeny] deny deny  
+ web trong gio [webtronggio] allow allow  
+ Default access [all] allow allow  
+ Redirect none  
  
  
Chọn Save  
  
Kết quả có 2 rule được tạo  
  
  
  
Kiểm tra: tại pc có ip thuộc dải 10.0.0.101-10.0.0.254 truy cập web thành công ở bất kỳ thời gian nào  
  
  
  
**7. HAVP (HTTP Antivirus Proxy)**  
- System, Packages, cài gói HAVP Antivirus  
  
  
  
Scheme: {internet}->[HAVP]->[Squid cache]->{clients}  
Setup  
Squid:   
• - Disable upstream proxy (also will auto-disabled by HAVP)   
HAVP:   
• - Select Proxy mode field as Parent for Squid and Save   
• - Scan Squid cache with Antivirus: File scanner for removing cached viruses.   
• - If you are planning to use Transparent Proxy mode: Squid transparent on   
  
B1. Kiểm tra Proxy server đamh ở chế độ Transparent proxy  
  
  
B2. Cấu hình HTTP proxy  
  
+ Service, Antivirus, chọn HTTP proxy   
+ Enable check  
+ Proxy mode parent for squid ;HAVP đứng trước Squid proxy)  
(Chọn transparent nếu HAVP đứng sau Squid proxy)  
+ Proxy interface(s) chọn Lan  
  
  
  
  
  
+ Log check  
+ Syslog check  
  
- Chọn Save  
  
B3. Cấu hình cập nhập ClamAV  
- Service, Antivirus, chọn Setting   
+ AV base update Chọn thời gian cập nhật  
+ Regional AV database Nơi cập nhật  
+ Log check  
+ Syslog check  
+ Chọn Save  
  
  
  
B4. Kiểm tra các dịch vụ đã chạy  
  
  
  
B5. Kiểm tra  
- Tại máy client truy cập trang [http://www.eicar.org](http://www.eicar.org/)  
- Chọn download (http)  
  
  
  
Khi download các file nhiễm virus sẽ gặp báo lỗi như trên  
  
**8. Limit bandwidth**  
**Giới hạn các pc 10.0.0.100 – 10.0.0.200 có bandwidth  
+ Download: max 1024 Kps  
+ Upload: max 100 Kbp  
Ngoài giờ làm việc thì không giới hạn download**  
  
B1. Firewall, liases, IP, nhắp dấu +  
  
  
  
  
+ Name: Nhập Gioi\_han\_bandwidth  
+ Description: Gioi han toc do down/up load  
+ Type: chọn Network  
+ Network Nhập 10.0.0.100-10.0.0.200  
  
- Nhấn Save  
  
  
  
- Nhấn Apply Change  
  
  
  
B2. Firewall, Traffic Shaper, Limiter  
  
  
  
- Chọn Create new limiter   
+ Enable Check  
+ Name download\_1024  
+ Bandwidth 1024 Kbps  
+ Mask Source address (chọn des sẽ giới hạn được IDM)  
+ Description Gioi han download  
  
- Chọn Save  
  
  
  
Tương tự, chọn Create new limiter để giới hạn tốc độ upload  
+ Enable Check  
+ Name upload\_100  
+ Bandwidth 100 Kbps  
+ Mask Source address (chọn des sẽ giới hạn được IDM)  
+ Description Gioi han upload  
- Chọn Save  
  
  
  
- Nhấn Apply changes  
  
  
  
B3. Khai báo giờ làm việc  
- Firewall, Schedules, nhấn +  
  
  
  
- Khai báo thông tin như hình, chọn Add Time  
  
- Nhập thông tin buổi chiều  
  
  
  
- Chọn save  
  
  
B4. Tạo rules  
- Firewall, Rules, LAN, nhắp +  
  
  
  
Khai báo các thông tin sau:  
+ Action Pass  
+ Interface Lan  
+ TCP/IP Version Ipv4  
+ Protocol TCP  
+ Source Sigle host or alias  
+ Nhập Address: Gioi\_han\_bandwidth  
  
+ Destination any  
+ Description Lan - Internet: gioi han bandwidth  
  
  
- Schedule giolamviec  
+ In: upload\_100   
+ Out: download\_1024  
  
  
  
- Chọn save  
Rule vừa tạo phải di chuyển lên trên cùng  
  
  
  
B4. Kiểm tra các máy thuộc dải IP 10.0.0.100-100.0.0.200 (chú ý giờ trên firewall)  
  
  
  
Kiểm tra các máy không thuộc dải IP 10.0.0.100-100.0.0.200  
Các máy nà không bị ảnh hưởng bởi chính sách giới hạn download/uoload  
  


**OPEN VPN (1)**

**1. Client to site - OpenVPN with TLS and local User Authentication**  
  
  
  
B1. Cài gói OpenVPN Client Export Utility   
+ System, Package, chọn gói OpenVPN Client Export Utility, nhấn +  
  
  
  
B2. Tạo chứng chỉ cho vpn server System, Cert Manager, CA, nhắp +  
  
  
  
Khai báo các thông tin cho CA:  
+ Descriptive name: CA  
+ Method: Create an internal Certificate Authority  
+ State or Province : hcm  
+ City : hcm  
+ Organization : nhatnghe  
+ Email Address : [doquangngoc@yahoo.com](mailto:doquangngoc@yahoo.com)  
+ Common Name : internal-ca  
  
- Chọn Save  
  
  
  
- CA đã được tạo  
  
  
  
B3. Tạo user  
- System, User Manager, Users, nhấn +  
  
  
  
- Khai báo các thông tin cho user:  
  
+ Username vpnuser  
+ Password 123  
+ Full name vpnuser  
+ Certificate check, tạo cetificate cho user vpnuser nhập vpnuser  
+ Chọn Save  
  
  
  
- User vpnuser đã được tạo  
  
  
  
B4. Cấu hình openvpn  
  
- VPN, chọn OpenVPN, chọn Wizard  
  
  
  
B5. Chọn kiểu chứng thực  
+ Type of Server: chọn Local user Access  
+ Nhấn Next  
  
  
  
B6. Chọn CA  
- Chọn CA, Nhấn Next  
  
  
  
B7. Tạo chứng chỉ cho openvpn server  
- Nhấn Add new Certificate  
  
  
  
Nhập thông tin cho chứng chỉ  
+ Descriptive name: vpnserver  
+ Country Code: vn  
+ State or Province: hcm  
+ City: hcm  
+ Organization: nhatnghe  
  
- Nhấn Create new Certificate  
  
  
  
B8. Cấu hình vpn  
- Chọn interface, giao thức, port cho kết nối VPN  
  
  
  
- Chọn thuật toán mã hóa cho việc chứng thực và mã hóa data  
  
  
  
Cấu hình tunnel:  
+ Tunnel Network: 192.168.2.0/24 (vpn)  
+ Local Network: 10.0.0.0/24 (internal network)  
+ Concurrent Connections: 50  
+ Compression: Check  
- Nhấn Next  
  
  
  
B9. Tạo rule cho phép liên lạc giữa mạng LAN và vpn client  
+ Firewall Rule: Check  
+ OpenVPN rule: Check  
- Nhấn Next  
  
  
  
B10. Nhấn finish  
  
  
  
B11. Xuất file cài đặt và cấu hình cho client  
  
  
  
- Chọn 2.3-x86  
  
  
  
- Chọn Save file  
  
  
  
B12. Cài vpn client  
  
- Thực thi file pfsense-udp-1194-vpnuser-install.exe vừa download  
  
  
- Nhấn Next  
  
  
  
- Chọn I Agree  
  
Nhấn   
- Next  
  
- Chọn Install  
  
Chọn continue Anyway  
  
  
Chọn start OpenVPN GUI  
Finish  
  
  
  
- B13. kết nối VPN  
Mở OpenVPN GUI, connect  
  
  
  
Kết nối thành công  
  
  
  
B14. Xem thông tin kết nối  
Status, chọn OpenVPN  
  


**SERVER PUBLISHING**

  
  
**1. Publish Web server**  
B1. Máy 10.0.0.150 cài IIS và tạo trang web  
- Control Panel, Add/Remove Program, Application Server, IIS, OK  
- Tạo file C:\Inetpub\wwwroot\ default.htm có nội dung:  
  
Web dat ben trong mang LAN  
  
  
  
B2. Tạo rules Firewall, NAT, chọn Port Forward WAN, nhấn +  
  
  
Khai báo các thông số:  
+ Interface: WAN  
+ Protocol: TCP   
+ Source: Any  
+ Destination: Wan address  
+ Redirect target port: http  
+ Redirect target IP: 10.0.0.150  
+ Redirect target port: http  
+ Description: Publish Web server  
  
  
  
- Chọn Save  
- Nhấp Apply changes  
  
  
  
B3. Tại máy client từ bên ngoài Internet, mở IE, truy cập vào IP mặt ngoài của Firewall  
  
  
  
**2. Publish Mail server (POP3 & SMTP)**  
- Máy 10.0.0.150 cài Mdaemon làm mail server  
B1. Cài Mdeamon 10.0.2  
  
  
  
- Chọn Next  
  
  
- Chọn I Agree  
  
  
- Chọn thư mục cài đặt  
  
  
- Nhấn Next bắt đầu cài đặt  
  
  
  
- Nhập tên domain: nhatnghe1.com  
  
  
  
- Tạo mailbox admin  
  
  
  
- Khai báo DNS  
  
  
  
- Nhấn Finish  
  
- Account, Account setting, bỏ check yêu cầu password phức tạp  
  
  
  
  
  
- Account, Account Manage, Tạo mailbox u1  
  
  
  
B2. Tạo rule  
  
- Firewall, NAT, chọn Port Forward WAN, nhấn +  
  
  
  
  
  
Khai báo các thông số:  
+ Interface: WAN  
+ Protocol: TCP   
+ Source: Any  
+ Destination: Wan address  
+ Redirect target port: smtp  
+ Redirect target IP: 10.0.0.150  
+ Redirect target port: smtp  
+ Description Publish mail: smtp  
  
B3. Lặp lại bước trên để nat trên port 110  
  
Khai báo các thông số:  
+ Interface: WAN  
+ Protocol: TCP   
+ Source: Any  
+ Destination: Wan address  
+ Redirect target port: pop3  
+ Redirect target IP: 10.0.0.150  
+ Redirect target port: pop3  
+ Description: Publish mail pop3  
  
  
  
- Nhấn Apply changes  
  
B4. Tại máy client từ bên ngoài Internet, mở Outlook Express  
- Cấu hình mail cho [u1@nhatnghe1.com](mailto:u1@nhatnghe1.com)  
  
  
- Soạn email, nhấn send  
  
  
  
- U1 nhận được mail do chính mình gởi  
  
