MỤC LỤC

[1. Cài đặt dịch vụ DHCP server trên máy 2](#_Toc388731482)

[2. Cài đặt dịch vụ DNS trên máy 5](#_Toc388731483)

[3. Cài đặt mail server 9](#_Toc388731484)

[4. Cài đặt dịch vụ Web trên máy 15](#_Toc388731485)

[5. Cài đặt firewall (chưa xong) 22](#_Toc388731486)

MỤC LỤC ẢNH

[Figure 1:Máy khách được phát IP 4](#_Toc388735903)

[Figure 2: Server ghi lại máy nào được phát IP 5](#_Toc388735904)

[Figure 3: phân giải tên miền server1.hhkd1570.vn 8](#_Toc388735905)

[Figure 4: tìm kiếm tên miền hhkd1570.vn 9](#_Toc388735906)

[Figure 5: gửi thư thành công trong LAN 11](#_Toc388735907)

[Figure 6: gửi không relay sẽ bị đánh dấu spam 14](#_Toc388735908)

[Figure 7: Sử dụng dịch vụ gửi - nhận mail qua Thunderbird 15](#_Toc388735909)

[Figure 8: Mai gửi relay qua gmail đã vào inbox 15](#_Toc388735910)

[Figure 9: Name-based website 18](#_Toc388735911)

[Figure 10: IP của name-based websites 18](#_Toc388735912)

[Figure 11: IP-based website 20](#_Toc388735913)

[Figure 12: IP của IP-based website 20](#_Toc388735914)

[Figure 13: UserDir website 22](#_Toc388735915)

[Figure 14: Trước khi chặn ping 24](#_Toc388735916)

[Figure 15: Sau khi chặn ping 24](#_Toc388735917)

[Figure 16: Trước khi chặn ssh 24](#_Toc388735918)

[Figure 17: Sau khi chặn ssh 24](#_Toc388735919)

TRONG BÁO CÁO, CÁC CÀI ĐẶT DC THIẾT LẬP TRÊN MÁY CHỦ CENTOS

Muốn tạo 1 server trc hết phải có 2 card mạng. 1 cái để kết nối internet với máy ngoài (bridge, hoặc NAT), 1 cái để làm host cấp cho các client (internal trog virtualbox hoặc LAN segment trog vmware.

Mô hình mạng:

eth1 eth0

SOHO Network ----------- [ROUTER B] ------------ [ROUTER A] ----------- Internet

10.0.10.0/24 10.0.10.1 | 192.168.201.2 192.168.201.1 | public-IP 0.0.0.0/0

1. Cài đặt dịch vụ DHCP server trên máy

* Thiết lập trên máy chủ Centos như sau:
* Thiết lập domain name:

nano /etc/sysconfig/network

edit domain name "server1.hhkd1570.vn"

* config custom static ip

nano /etc/sysconfig/network-scripts/ifcfg-eth1

*bootproto = static*

*nm\_controlled=no*

*ipaddr = 10.0.10.1*

*netmask = 255.255.255.0*

*network = 10.0.10.0*

*defroute = yes*

* reboot for change domainname
* Tiến hành cài đặt DHCP

yum update

yum install dhcp

rpm -qc dchp #list all configuration file for package dhcp, obtain:

/etc/dhcp/dhcpd.conf #configuration file for dhcpd

/var/lib/dhcpd/dhcpd.leases #ipv4 dhcp leases

* Cấu hình DHCP
  + Chọn NIC để cấp phát IP

sudo nano /etc/sysconfig/dhcpd

DHCPsubnDARGS=eth1

* + Cấu hình IP

nano /etc/dhcp/dhcpd.conf

*#ddns-update-style interim*

*option domain-name "hhkd1570.vn"*

*option domain-name-server 8.8.8.8, 10.0.10.1*

change DHCP to log using diffenrence facility (log-facility local6)

*subnet 10.0.10.0 netmask 255.255.255.0{*

*range 10.0.10.50 10.0.10.100;*

*#option subnet-mask ...;*

*#option broadcast-address 10.0.10.255;*

*option routers 10.0.10.1;*

*}*

then comment all other.

* Cấu hình report log

nano /etc/rsyslog.conf

thêm code:

local6.\* /var/log/dhcpd.log

service rsyslog restart

service dhcpd restart

cat /var/lib/dhcpd/dhcpd.leases

->see which computers have provided ips

* Thiết lập trên máy client:

vi /etc/sysconfig/network-manager/ifcfg-eth0

*dhcp\_hostname hhkd1570.vn*

(ubuntu)sudo vi /etc/interface/network

*hostname hhkd1570.vn*

* Kết quả:

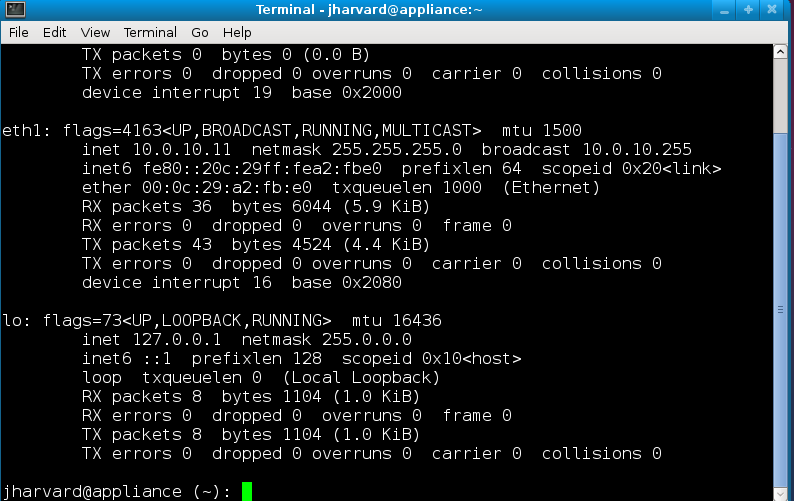


Figure : Máy khách được phát IP

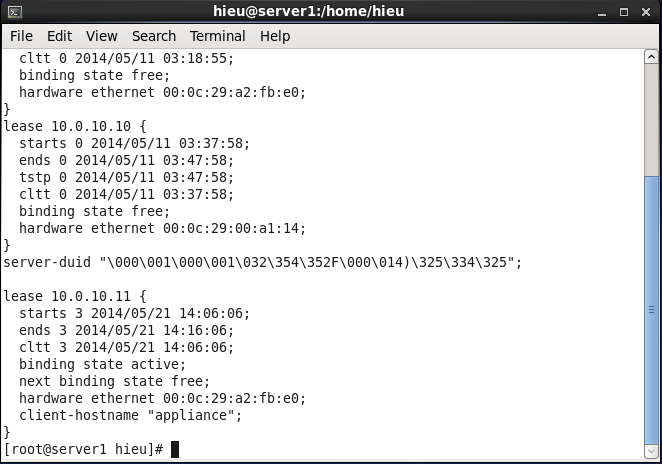


Figure : Server ghi lại máy nào được phát IP

1. Cài đặt dịch vụ DNS trên máy

* Thiết lập trên máy chủ:
* Cài đặt dịch vụ bind, named

yum install bind

* Cấu hình tên miền

vi /etc/named.conf

listen-on port 53 { 127.0.0.1; 10.0.10.1; }; ### Master DNS IP ###

*allow-query { localhost; 10.0.10.0/24; }; ### IP Range ###*

Thêm zone ứng với tên miền (thuận)

*zone "hhkd1570.vn" {*

*type master;*

*file "hhkd1570.vn.forward";*

*allow-update {none;};*

*};*

Thêm zone tra ngược từ IP sang domain name

*zone "10.0.10.in-addr.arpa" {*

*type master;*

*file "hhkd1570.vn.reverse";*

*allow-update {none;};*

*}*

* Thiết lập cho tên miền được tạo

vi /var/named/hhkd1570.vn.forward

$TTL 1D

@ IN SOA server1.hhkd1570.vn. root.hhkd1570.vn. (

2014041001 ;id

28800 ;

14400 ;

3600000 ;

86400 ;

)

@ IN NS server1.hhkd1570.vn.

@ IN A 10.0.10.1

@ IN A 10.0.10.10

www IN CNAME server1.hhkd1570.vn. ;canonical name

server1 IN A 10.0.10.1

client1 IN A 10.0.10.10

vi /var/named/hhkd1570.vn.reverse

$TTL 1D

@ IN SOA server1.hhkd1570.vn. root.hhkd1570.vn. (

2

014041001 ;id

28800 ;Refresh

14400 ;Retry

3600000 ;Expire

86400 ;Minimum TTL

)

@ IN NS server1.hhkd1570.vn.

@ IN PTR hhkd1570.vn.

server1 IN A 10.0.10.1

client1 IN A 10.0.10.10

1 IN PTR server1.hhkd1570.vn.

10 IN PTR client1.hhkd1570.vn.

Lưu ý: không được để tab hoặc space ở đầu mồi dòng code

* Tiến hành chạy dịch vụ

service named start

chkconfig named on

* Cấu hình firewall cho phép chạy dịch vụ dns trên port 53

nano /etc/sysconfig/iptables

*-A INPUT -p udp -m state --state NEW --dport 53 -j ACCEPT*

*-A INPUT -p tcp -m state --state NEW --dport 53 -j ACCEPT*

service iptables restart

* Thiết lập trên máy client:

nano /etc/resolv.conf

*search hhkd1570.vn*

*nameserver 10.0.10.1*

* Kết quả:

Tiến hành phân giải tên miền

dig server1.hhkd1570.vn

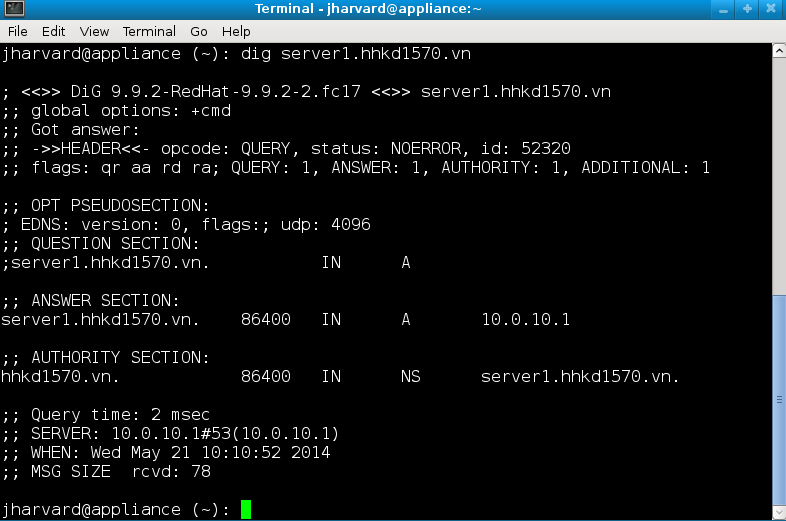


Figure : phân giải tên miền server1.hhkd1570.vn

nslookup hhkd1570.vn

nslookup 10.0.10.1

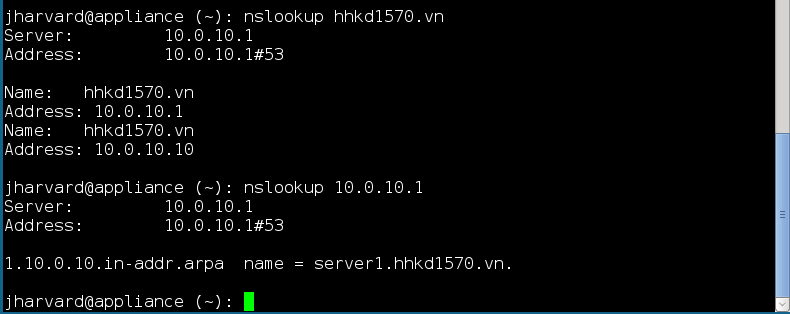


Figure : tìm kiếm tên miền hhkd1570.vn

1. Cài đặt mail server
2. Cài đặt postfix để gửi mail:

yum -y install postfix

* Thêm mail record cho domain

vi /var/named/hhkd1570.vn.forward

IN MX 10 mail.hhkd1570.vn.

mail IN CNAME server1.hhkd1570.vn.

* cấu hình postfix

nano /etc/postfix/main.cf

*myhostname = mail.hhkd1570.vn*

*mydomain = hhkd1570.vn*

*myorigin = $myhostname*

*inet\_interfaces = all*

*mydestination = $myhostname, localhost.$mydomain, localhost, $mydomainmynetworks = 10.0.10.0/24, 127.0.0.0/8*

*home\_mailbox = Maildir/*

* chạy dịch vụ

service postfix restart

chkconfig --level 235 postfix on

* thêm user để sử dụng dịch vụ (user này chỉ để gửi và nhận mail, k dùng để login như user bình thường khác

useradd -m testmail -s /sbin/nologin

* Phía client sử dụng dịch vụ: sử dụng qua telnet hoặc thunderbird

telnet mail.hhkd1570.vn smtp

*helo mail.hhkd1570.vn*

*mail from:hieu*

*rcpt to:testmail*

*data*

*Subject: something*

*type something...*

*<enter>*

*.*

*<enter>*

* Kết quả:
* Server xem thư mới:

ls /home/testmail/Maildir/new



Figure : gửi thư thành công trong LAN

1. Cài đặt imap service để đọc mail

yum install dovecot

nano /etc/dovecot/dovecot.conf

uncomment dòng sau:

*protocol = ......*

nano /etc/dovecot/conf.d/10-mail.conf

*mail\_location = maildir:~/Maildir*

nano /etc/dovecot/conf.d/10-auth.conf

disable\_plaintext\_auth = no

*auth\_mechanisms = plain login*

nano /etc/dovecot/conf.d/10-master.conf

*unix\_listener auth-userdb {*

*mode = 0600*

*user = postfix*

*group = postfix*

*}*

service dovecot restart

chkconfig --level 235 dovecot on

* phía client sử dụng dịch vụ:

telnet mail.hhkd1570.vn imap

*a login testmail 123*

*a list "" \**

*a examine inbox (b select inbox)*

*a fetch 1 body[]*

*a logout*

* Kết quả:



1. Gửi mail ra ngoài internet

Thông thường các mail gửi từ domain không được đăng ký sẽ bị các mail server khác cho vào spam. Vì vậy nếu muốn gửi vào inbox thì phải thông qua relay

Kết quả gửi không qua relay:

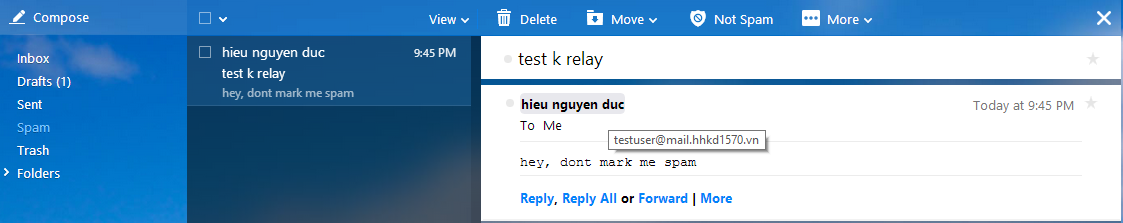


Figure : gửi không relay sẽ bị đánh dấu spam

* Thiết lập postfix cho phép relay

nano /etc/postfix/main.cf

*relayhost = [smtp.gmail.com]:587*

*smtp\_use\_tls=yes*

*smtp\_sasl\_auth\_enable = yes*

*smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd*

*smtp\_tls\_CAfile = /etc/postfix/cacert.pem*

*smtp\_sasl\_security\_options = noanonymous*

* thiết lập account ta sẽ relay thông qua

nano /etc/postfix/sasl\_passwd

[smtp.gmail.com]:587 bk.ict.k56@gmail.com:mothaiba

* cài đặt certificate cho google services

postmap /etc/postfix/sasl\_passwd

chmod 600 /etc/postfix/sasl\_passwd

cd /etc/pki/tls/certs

make hostname.pem

Fill-up the necessary information and copy the file on /etc/postfix as cacert.pem

cp /etc/pki/tls/certs/hostname.pem /etc/postfix/cacert.pem

Sau đó đổi: *inet\_protocols = ipv4* trên file main.cf

service postfix restart

* Kết quả gửi qua relay:

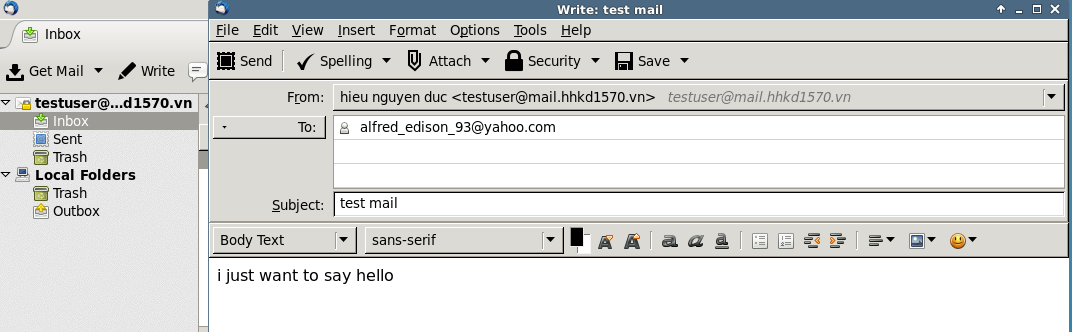


Figure : Sử dụng dịch vụ gửi - nhận mail qua Thunderbird

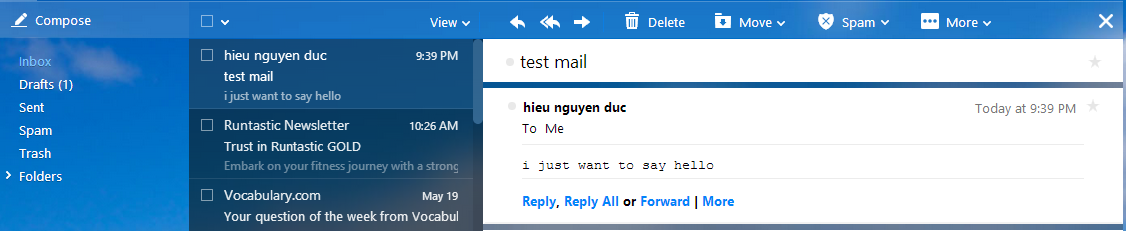


Figure : Mai gửi relay qua gmail đã vào inbox

1. Cài đặt dịch vụ Web trên máy

* cài đặt dịch vụ httpd – apache server

yum install httpd

1. name-based website:

* tạo thư mục cho 2 trang web ta sẽ tiến hành cài đặt trên cùng 1 IP

mkdir /var/www/html/hhkd1570.vn/

mkdir /var/www/html/hhkd1570.com/

* Thiết lập webserver:

nano /etc/httpd/conf/httpd.conf

* thêm trang web hhkd1570.vn

*NameVirtualHost \*:80*

*<VirtualHost \*:80>*

*ServerAdmin root@server1.hhkd1570.vn*

*DocumentRoot /var/www/html/hhkd1570.vn*

*ServerName www.hhkd1570.vn*

*ServerAlias hhkd1570.vn*

*ErrorLog logs/www.hhkd1570.vn-error\_log*

*CustomLog logs/www.hhkd1570.vn-access\_log common*

*</VirtualHost>*

* để tạo trang hhkd1570.com, thêm dns zone sau:

*zone "hhkd1570.com" {*

*type master;*

*file "hhkd1570.com.forward";*

*allow-update {none;};*

*};*

Và cấu hình file forward

nano /var/named/hhkd1570.com.forward

*$TTL 1D*

*@ IN SOA hhkd1570.com. root.hhkd1570.vn. (*

*2014041002 ;id*

*28800 ;*

*14400 ;*

*3600000 ;*

*86400 ;*

*)*

*@ IN NS hhkd1570.vn.*

*@ IN A 10.0.10.1*

*www IN CNAME hhkd1570.vn. ;canonical name*

* thêm web hhkd1570.com trong file httpd.conf

*<VirtualHost \*:80>*

*ServerAdmin root@server1.hhkd1570.vn*

*DocumentRoot /var/www/html/hhkd1570.com*

*ServerName www.hhkd1570.com*

*ErrorLog logs/www.hhkd1570.com-error\_log*

*CustomLog logs/www.hhkd1570.com-access\_log common*

*</VirtualHost>*

* chạy dịch vụ httpd

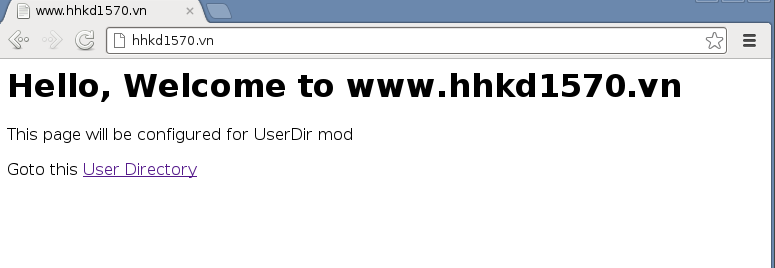
httpd -t

service httpd restart

chkconfig --level 35 httpd on

iptables -F #clear all rules, allow to connect via http port

* Kết quả:



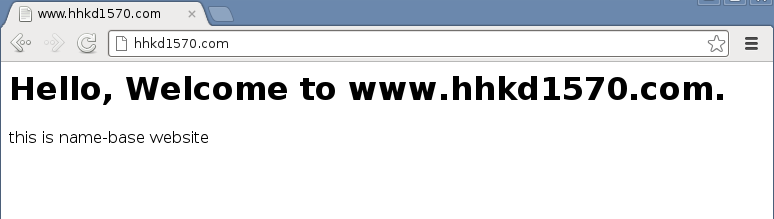
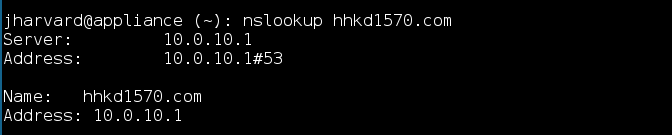


Figure : Name-based website



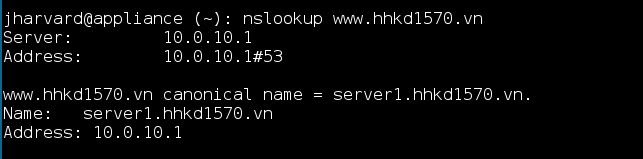


Figure : IP của name-based websites

1. IP-based website:

* Tạo card mạng ảo để tạo ip mới cho IP-based website:

cd /etc/sysconfig/network-scripts/

cp ifcfg-eth0 ifcfg-eth0:0

cp ifcfg-eth0 ifcfg-eth0:1

-> change ip and name (remove defroute)

* Thêm zone mới cho trang web

*zone "hhkd1570.net" {*

*type master;*

*file "hhkd1570.net.forward";*

*allow-update {none;};*

*};*

* Thêm ip vào file reverse để có thể tra ngược dns từ ip sang domain name

*2 IN PTR hhkd1570.net.*

* Tạo file forward mới cho trang vừa tạo

nano /var/named/hhkd1570.net.forward

*$TTL 1D*

*@ IN SOA hhkd1570.com. root.hhkd1570.vn. (*

*2014041002 ;id*

*28800 ;*

*14400 ;*

*3600000 ;*

*86400 ;*

*)*

*@ IN NS hhkd1570.vn.*

*@ IN A 10.0.10.1*

*www IN CNAME hhkd1570.vn. ;canonical name*

* Tạo thư mục chứa trang web mới

mkdir /var/www/html/hhkd1570.vn

* Cấu hình file httpd.conf cho IP-based website:

vi /etc/httpd/conf/httpd.conf

*Listen 10.0.10.1:80*

*Listen 10.0.10.2:80*

*#This is for IP-based website*

*<VirtualHost 10.0.10.2:80>*

*ServerAdmin root@server1.hhkd1570.vn*

*DocumentRoot /var/www/html/hhkd1570.net*

*ServerName www.hhkd1570.net*

*ErrorLog logs/www.hhkd1570.net-error\_log*

*TransferLog logs/www.hhkd1570.net-access\_log*

*</VirtualHost>*

* Kết quả:

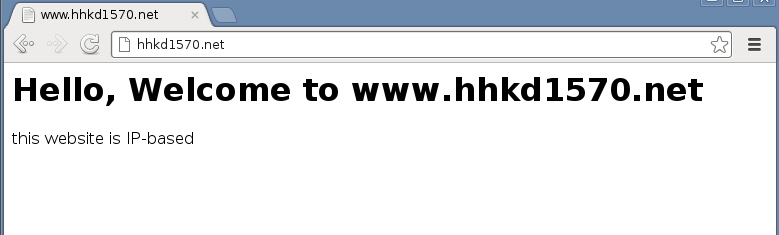


Figure : IP-based website

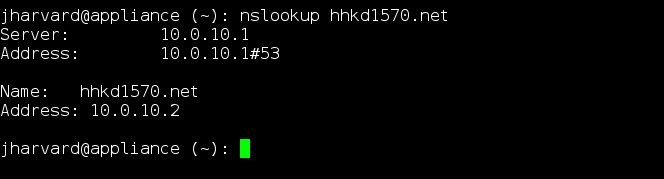


Figure : IP của IP-based website

1. public\_html cho userdir

* ta sẽ cấu hình trang hhkd1570.vn cho phép userdir

vi /etc/httpd/conf/httpd.conf

thêm cấu hình sau vào hhkd1570.vn virtualhost

*<IfModule mod\_userdir.c>*

*UserDir enable testuser*

*UserDir public\_html*

*</IfModule>*

*<Directory /home/\*/public\_html>*

*AllowOverride FileInfo AuthConfig Limit*

*Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec*

*<Limit GET POST OPTIONS>*

*Order allow,deny*

*Allow from all*

*</Limit>*

*<LimitExcept GET POST OPTIONS>*

*Order deny,allow*

*Deny from all*

*</LimitExcept>*

*</Directory>*

* thiết lập quyền truy cập cho thư mục public\_html

chown testuser:apache public\_html/

chmod 711 /home/testuser

chmod 755 /home/testuser/public\_html/

chmod 604 /home/\*/public\_html/\*.html

* máy chủ Centos có sử dụng dịch vụ SELinux. Chúng ta nên tắt dịch vụ vày đi để tiện quản lý các dịch vụ khác. Nhưng trong trường hợp không muốn tắt dịch vụ này, ta cần phải thiết lập thêm để có thể sử dụng user website:

### Enable User Website

setsebool -P httpd\_enable\_homedirs true

chcon -v -R -h -u user\_u -t httpd\_user\_content\_t /home/\*/public\_html

### Disable User Website

setsebool -P httpd\_enable\_homedirs false

chcon -v -R -h -u user\_u -t user\_home\_t /home/\*/public\_html)

* Kết quả:



Figure : UserDir website

1. Cài đặt firewall
2. Cấu hình firewall là trạm trung chuyển giữa 2 máy khác, cấu hình cho hoặc không cho phép traffic giữa 2 máy (accept, drop, reject,…)

* Trước hết cần forward traffic từ private network 10.0.10.0/24 trên eth1 sang network trên eth0
* Thêm cấu hình vào file *cfg-eth1* để có gateway forward:

*GATEWAY=192.168.201.129 (có thể thêm BROADCAST=10.0.10.255)*

* Cấu hình cho phép forward IPv4

nano /etc/sysctl.conf

*net.ipv4.ip\_forward = 1*

* Cấu hình chuyển gói dữ liệu

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables --append FORWARD --in-interface eth1 -j ACCEPT

* Hiện danh sách các lệnh (rules) và lưu iptables

iptables -L -v

service iptables save

service iptables restart

* Tiến hành lọc (filter) các gói tin:
* Chặn ping

iptables -A FORWARD -p icmp -m icmp --icmp-type 8 -j DROP

* Chặn chia sẻ bittorrents

iptables -A FORWARD -p tcp --dport 6881 -j DROP

* Chặn ftp

iptables -A FORWARD -p tcp --dport 20:21 -j DROP

* Chặn kết nối SSH

iptables -A FORWARD -p tcp --dport 22 -j REJECT --reject-with icmp-net-prohibited

* Kết quả:

Thực hiện kết nối giữa 2 máy:

+ 1 máy client Ubuntu trong mạng nội bộ ta vừa tạo với IP 10.0.10.11 (tên máy: localhost.localdomain)

+ 1 máy client Fedora trong mạng ngoài (thuộc mạng 192.168.201.0/24) với IP 192.168.201.132 (tên máy: appliance.localdomain)

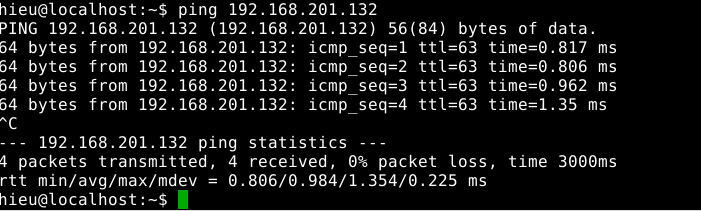
* Trước khi chặn ping, ta ACCEPT các gói tin, việc ping diễn ra thành công với 100% packet received (0% lost)

Figure : Trước khi chặn ping

Sau khi chặn, các gói tin bị DROP, 100% packet loss

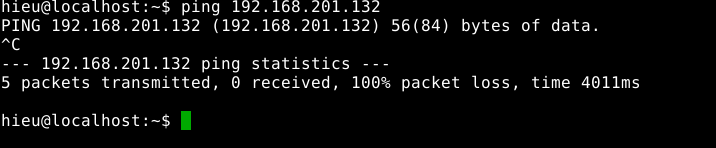


Figure : Sau khi chặn ping

* Trước khi chặn giao thức ssh, việc kết nối được FORWARD qua firewall. Chính vì vậy log record thông báo login thành công và với IP của firewall (192.168.201.129)

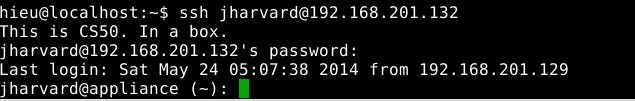


Figure : Trước khi chặn ssh

Sau khi chặn ssh, kết nối bị REJECT và console thông báo lại việc kết nối bị lỗi

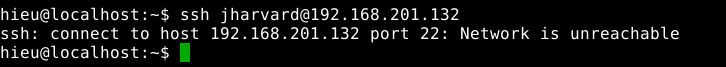


Figure : Sau khi chặn ssh

1. Viết ít nhất 4 lệnh (access rules) thuộc dạng INPUT và OUTPUT

# allow http, https

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# allow smtp

iptables -A INPUT -p tcp --dport 25 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

# allow pop3

iptables -A INPUT -p tcp --dport 110 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT

# allow imap

iptables -A INPUT -p tcp --dport 143 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT