[Untangle]
Open Source Firewall

lwh@debian.kr
[SarangIran.net]

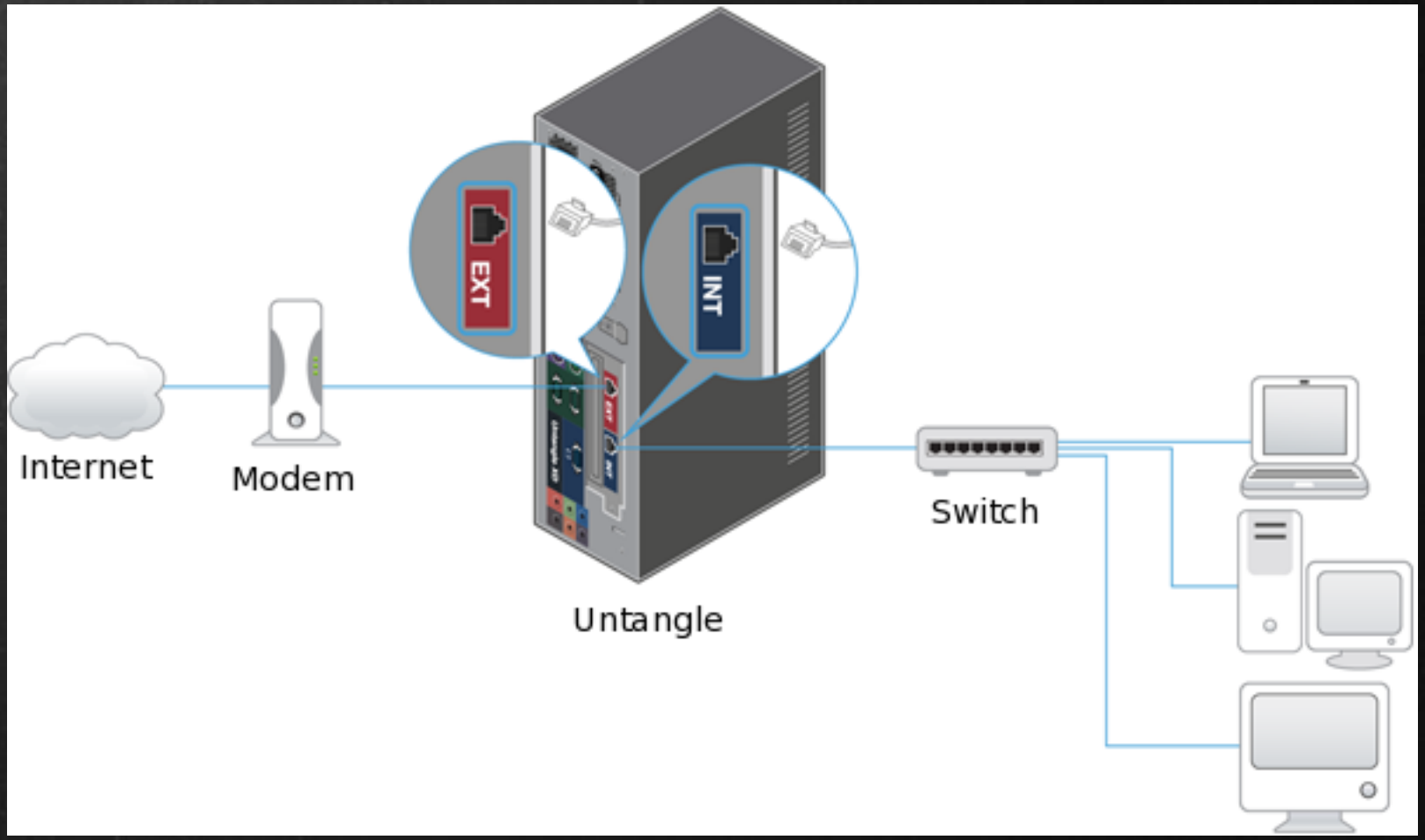
Feb, 2012 Ubuntu Seminar @Seoul

Firewall? IPS? UTM?

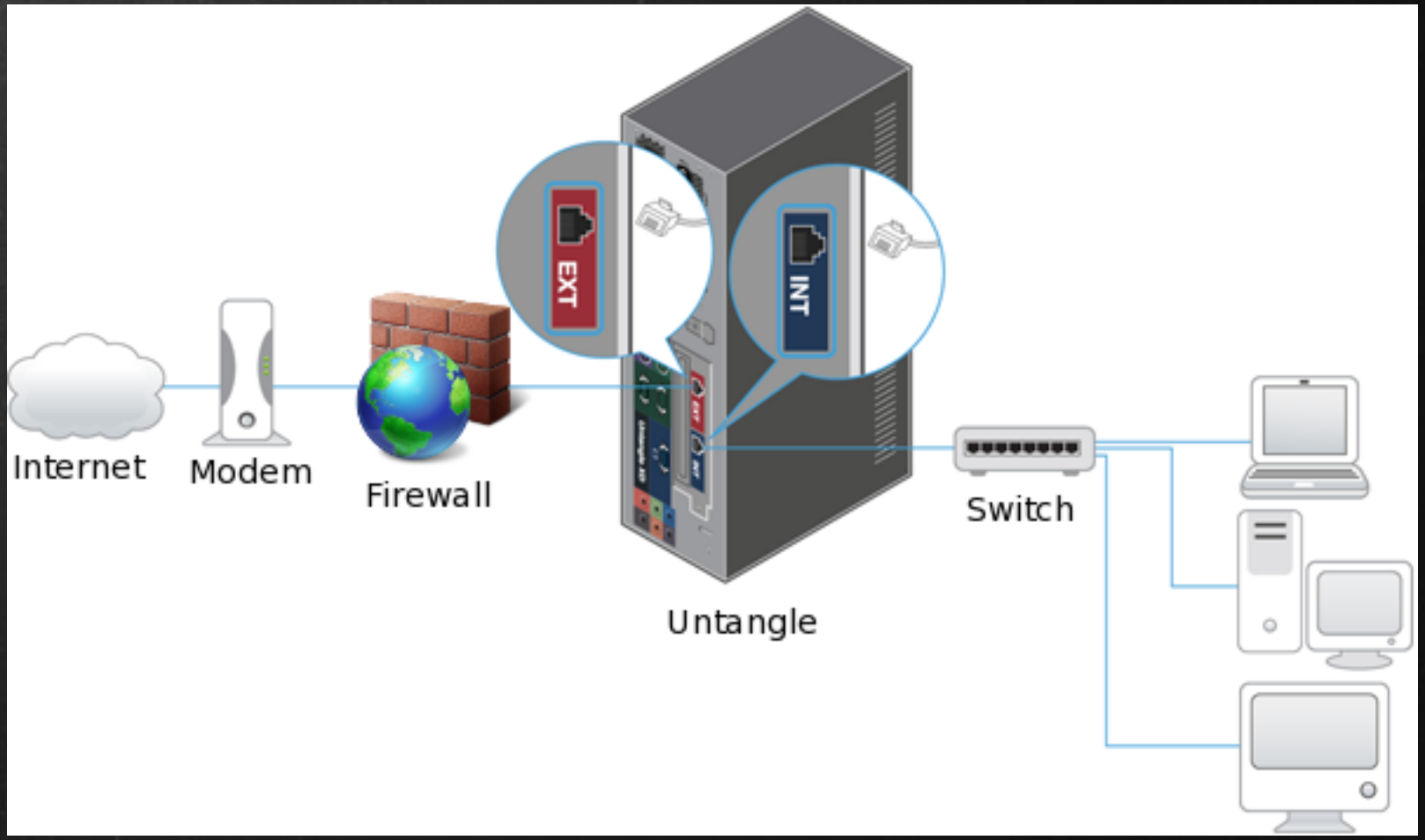
- Firewall
- IPS
- UTM

Open source Firewalls

- EFW(Endian Firewall)
- Untangle Firewall
- pfSense
- IpCOP
- Astro Firewall
- &... so on...



Router Mode



Bridge Mode - Stealth/Screen/tranceparnt/Inlie

About Untangle

by Untangle Inc. (http://www.untangle.com)
Free Software(GW Platform, Apps is GPLv2)
UTM

Why Open Source ?

Features

- Protect

Web Filter(Lite), Virus Blocker(Lite), Spam Blocker(Lite), Application Control(Lite), FW, IPS, Ad Blocker, Phish Blocker Spyware Blocker, Attack Blocker(Anti DoS)

- Connect

IPsec VPN, OpenVPN(Free), Captive Portal(Free)

- Manage

Policy Manager, Directory Connector, WAN Failover, WAN Balancer, Reports(Free)

- Perform

Web Cache, Bandwidth Control


untangle


DVD
untangle
intel
Pentium

Size Guidance

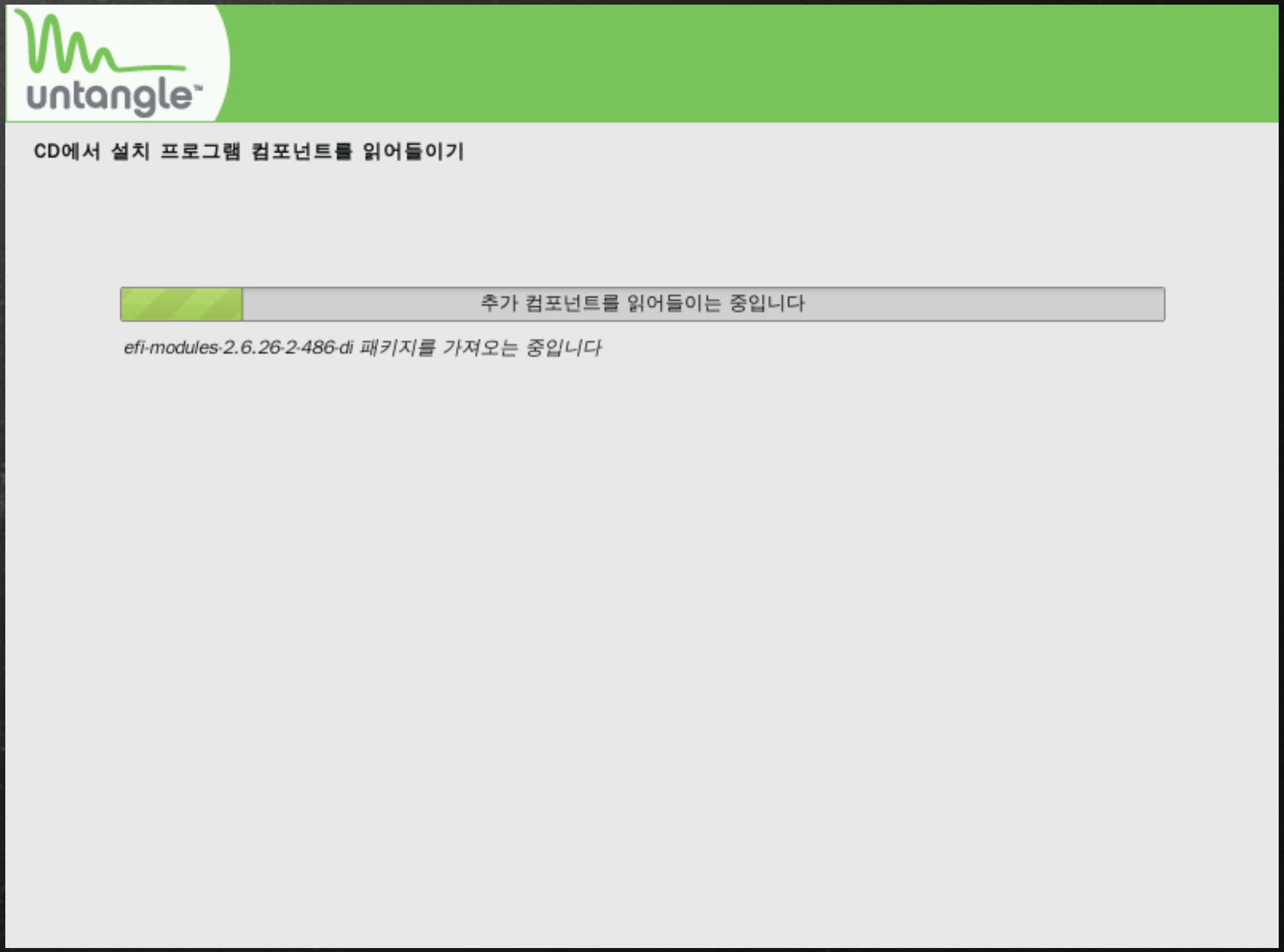
Resource	Processor	Memory	Hard Drive	NICs	Notes
Minimum	Intel/AMD-compatible Processor (800+ Mhz)	512 MB	20 GB	2	
1-50 Users	Pentium 4 equivalent or greater	1 GB	80 GB	2 or more	
51-150 Users	Dual Core	2 GB	80 GB	2 or more	
151-500 Users	2 or more Cores	2 or more GB	80 GB	2 or more	
501-1500 Users	4 Cores	4 GB	80 GB	2 or more	64-bit
1501-5000 Users	4 or more Cores	4 or more GB	80 GB	2 or more	64-bit


Untangle installer
Graphical install (normal mode)
Graphical install (expert mode)
Text install (normal mode)
Text install (expert mode)
Press [Tab] to edit options
untangle


untangle
Choose language
Please choose the language used for the installation process. This language will be the default language for the final system.
Choose a language:
Greek - Ελληνικά
Gujarati - ગુજરાતી
Hebrew - עברית
Hindi - हिन्दी
Hungarian - Magyar
Indonesian - Bahasa Indonesia
Irish - Gaeilge
Italian - Italiano
Japanese - 日本語
Khmer - ខ្មែរ
Korean - 한국어
Kurdish - Kurdî
Latvian - Latviski
Lithuanian - Lietuviškai
Macedonian - Македонски
Malayalam - മലയാളം
Marathi - मराठी
Go Back
Continue


키보드 배치 선택
사용할 키맵:
노르웨이
덴마크
독일 (데드키 없음)
드보락
라트비아
라틴 아메리카
러시아
루마니아
리투아니아
마케도니아
미국 영어
벨기에
벨라루시아
불가리아
브라질 (ABNT2 배치)
브라질 (EUA 배치)
세르비아 (키릴)
스웨덴
스위스 독일어
스위스 프랑스어
스페인어
뒤로 가기
계속


untangle™
CD-ROM 찾기 및 마운트
하드웨어를 검색해 CD-ROM 드라이브를 찾는 중입니다
하드웨어를 검색하는 중입니다. 잠시 기다리십시오...


untangle™
CD에서 설치 프로그램 컴포넌트를 읽어들이기
추가 컴포넌트를 읽어들이는 중입니다
efi-modules-2.6.26-2-486-di 패키지를 가져오는 중입니다


네트워크 하드웨어 찾기
네트워크 하드웨어 찾기
하드웨어를 검색하는 중입니다. 잠시 기다리십시오...

Untangle system

Summary:.

Total memory: insufficient
Processor speed: ok

계속


Untangle system
Untangle must format the disk to continue
WARNING: ALL DATA ON YOUR DISK WILL BE LOST!
Do you want to proceed and format your disk?
아니오
예
계속

디스크 찾기

디스크 및 기타 하드웨어를 찾는 중입니다

하드웨어를 검색하는 중입니다. 잠시 기다리십시오...


untangle™
디스크 파티션하기
파티션 포맷하는 중입니다
SCSI1 (0,0,0) (sda) 장치의 파티션 #1의 /에 마운트한 ext3 파일 시스템을 만드는 중입니다...


베이스 시스템 설치
베이스 시스템을 설치하는 중입니다
베이스 패키지의 의존 패키지를 추가로 찾았습니다: exim4 exim4-base exim4-config exim4-daemon-light libept0 libgdbm3 lib

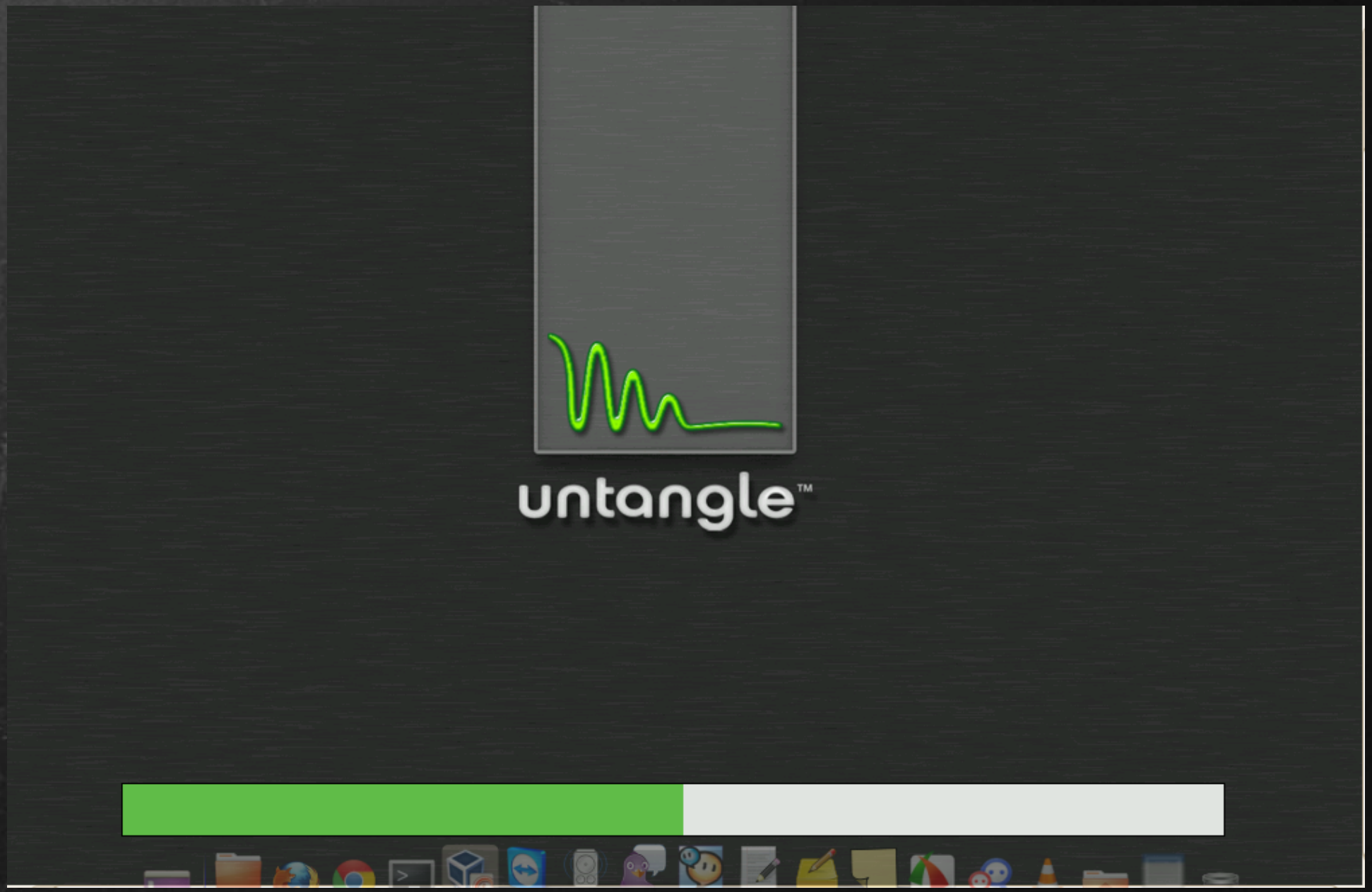
설치 마치기

설치를 마쳤습니다

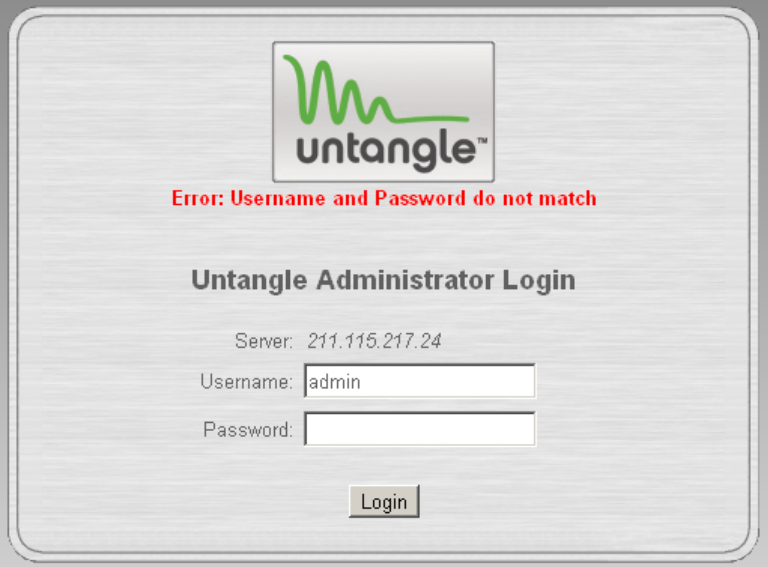
설치를 마쳤습니다. 이제 새 데비안 시스템으로 부팅합니다. CD-ROM, 플로피 등 설치 미디어가 들어 있으면 반드시 빼십시오. 그래야 데비안을 설치한 디스크로 부팅합니다.

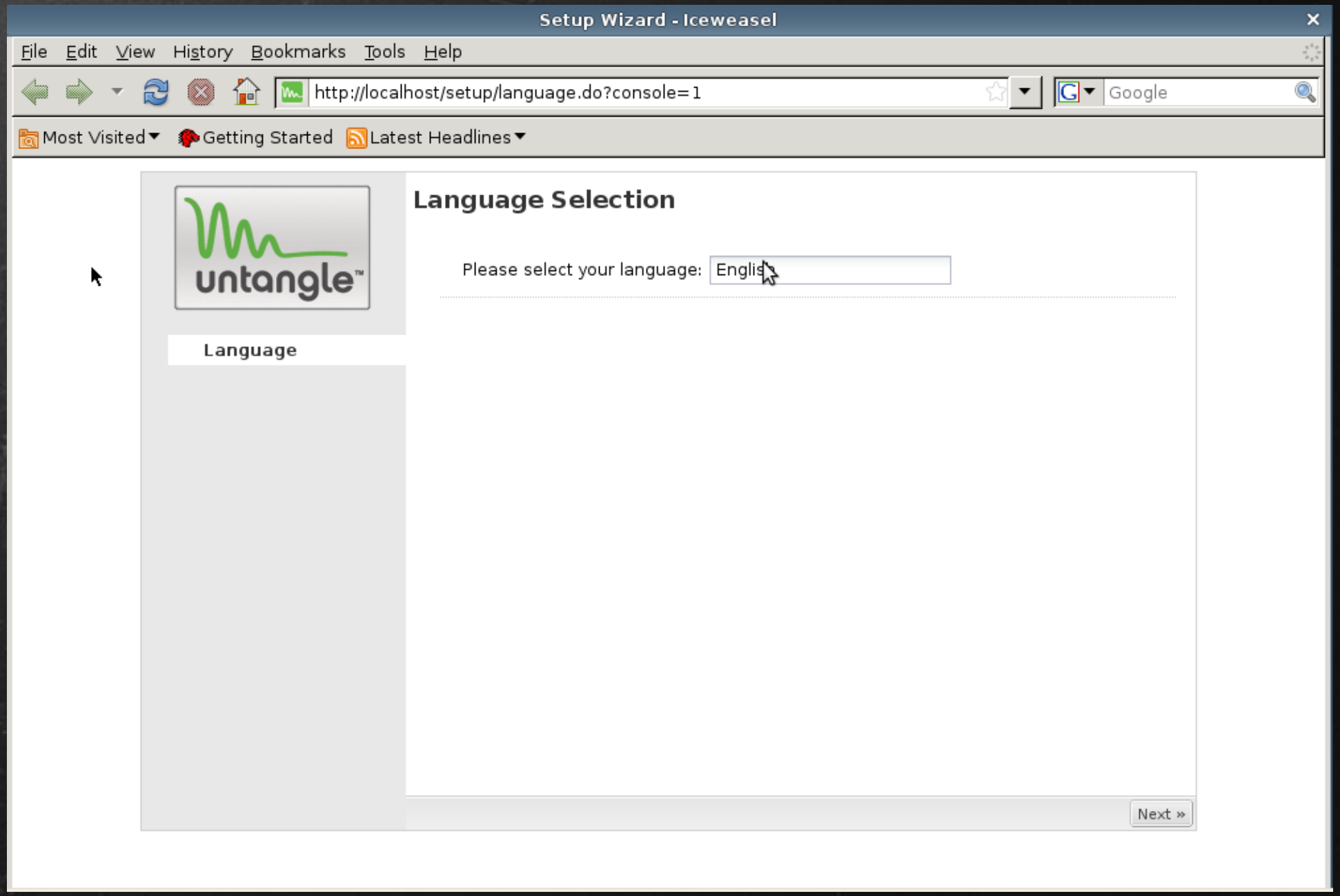
뒤로 가기 계속

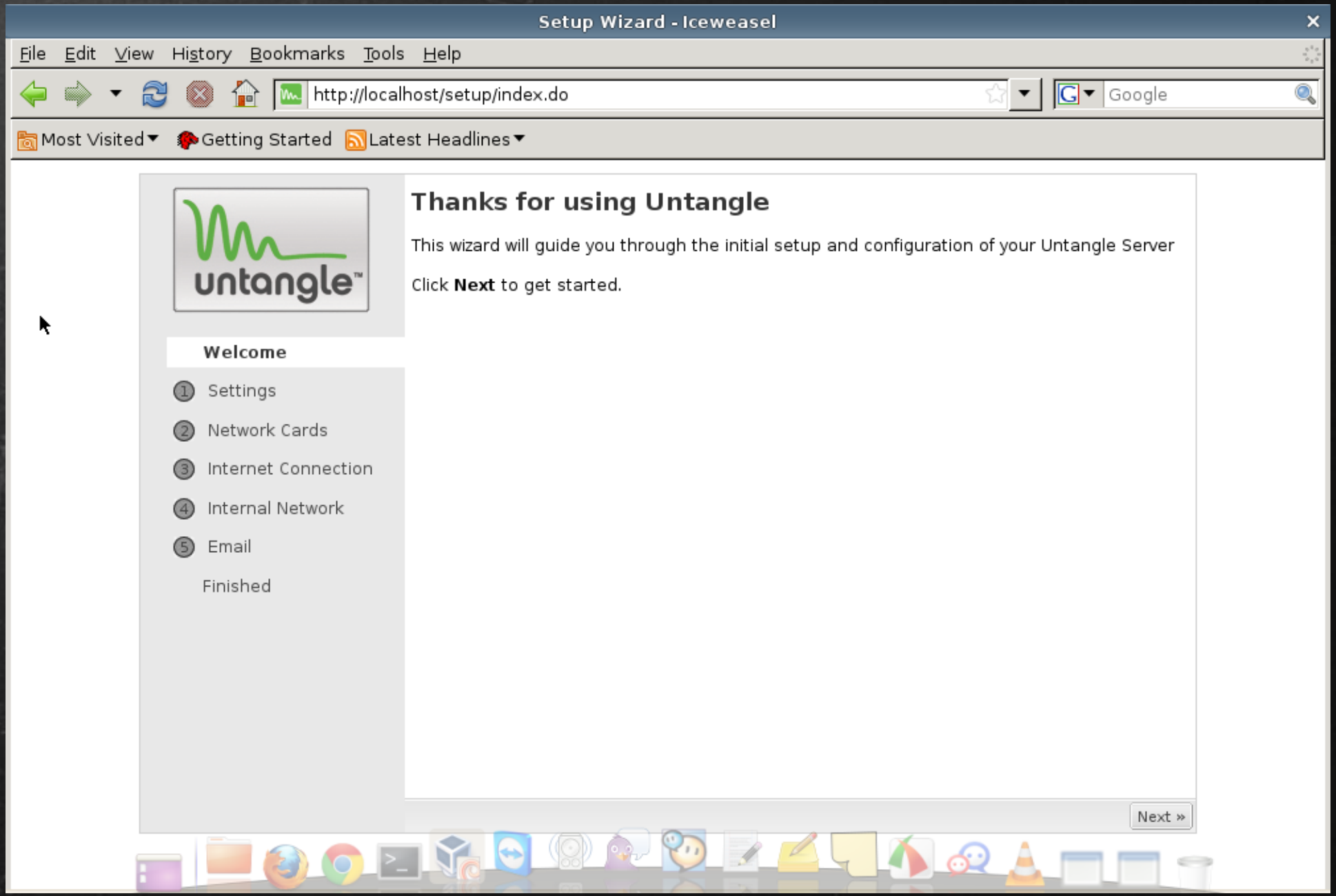
Chap 2. Setting

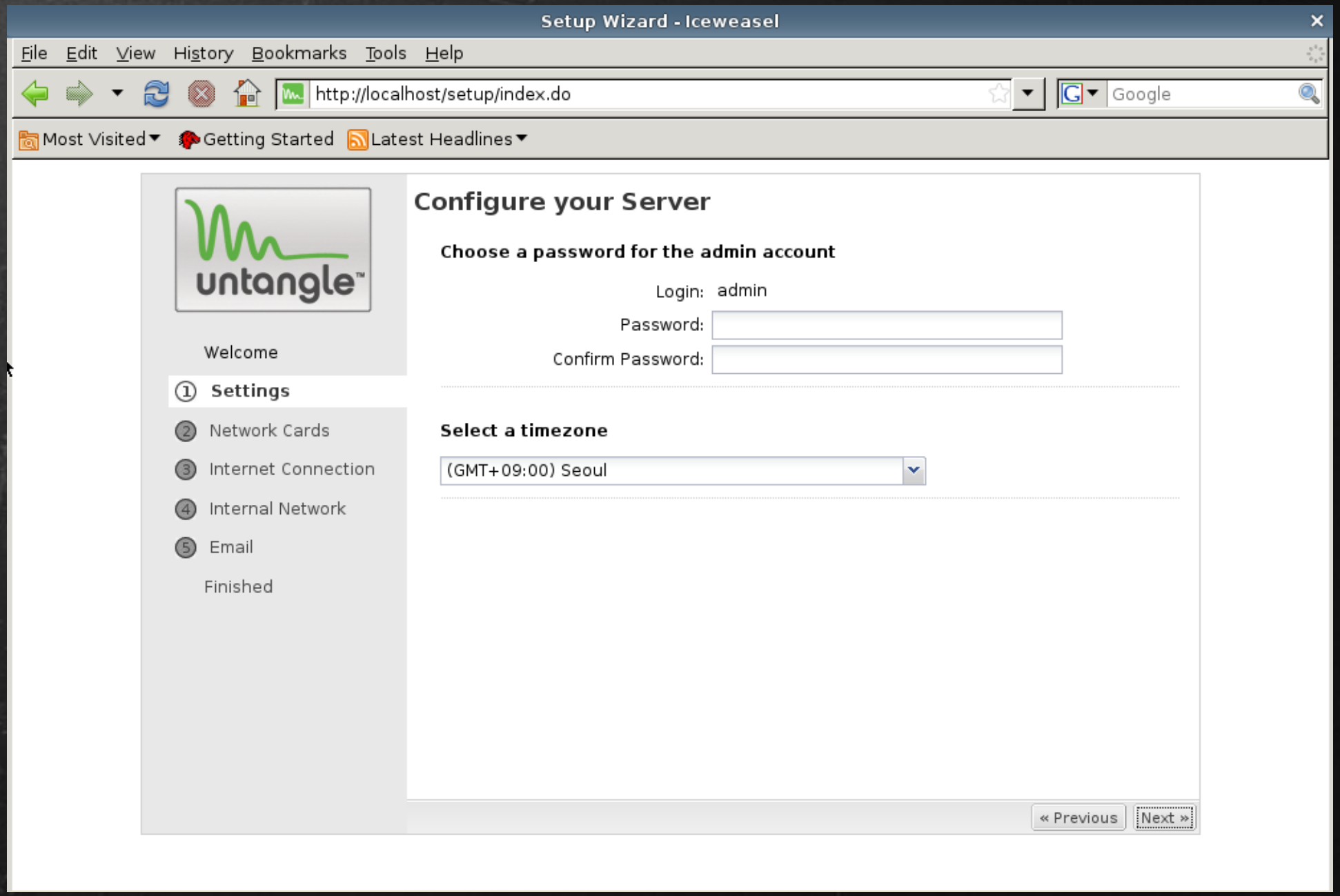

untangle™

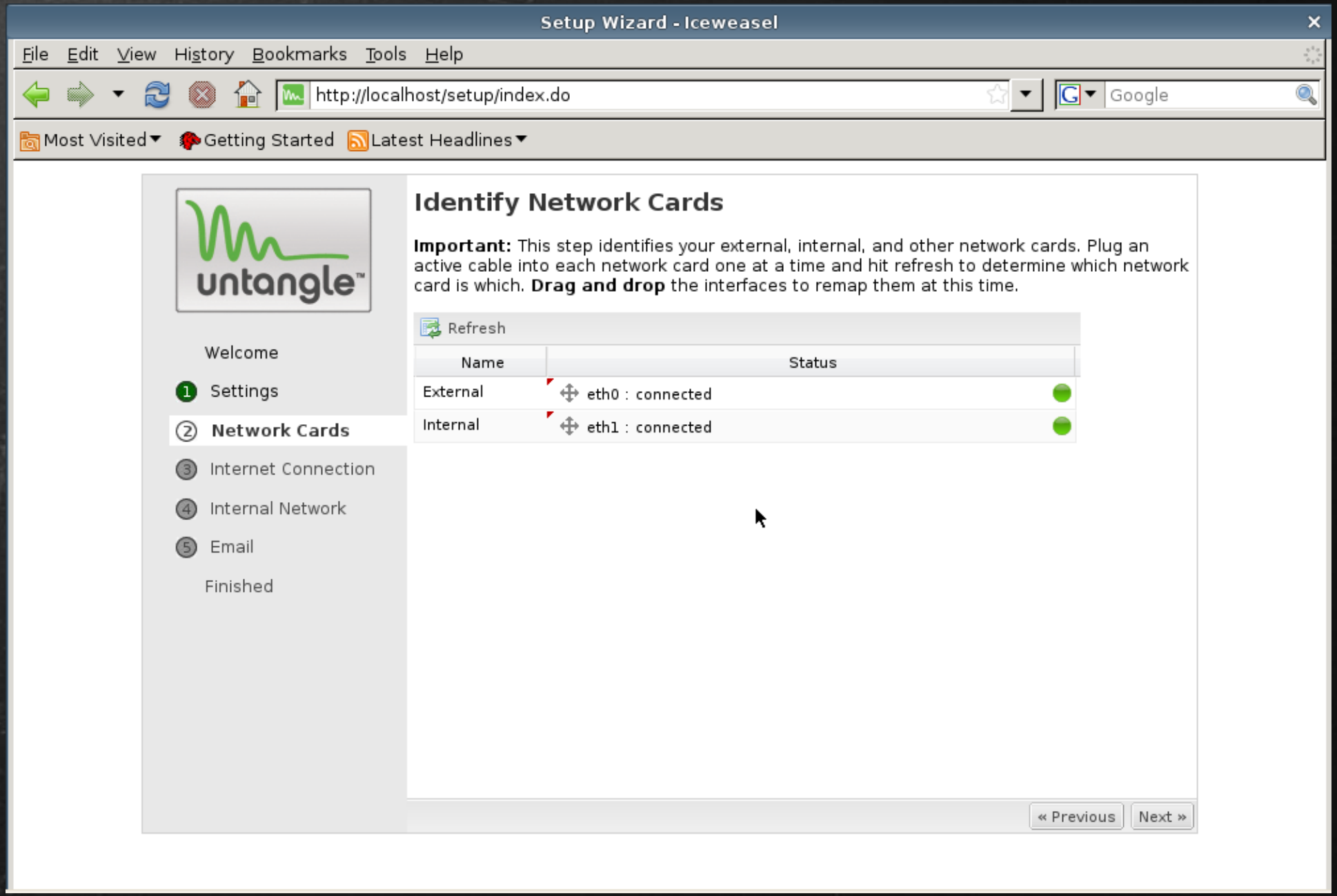

untangle™
Use the button bar below to launch the Untangle Client.
Launch Client
Change resolution
Turn On Screensaver
Turn Off Screensaver
Reboot
Shutdown
Recovery Utilities
Terminal

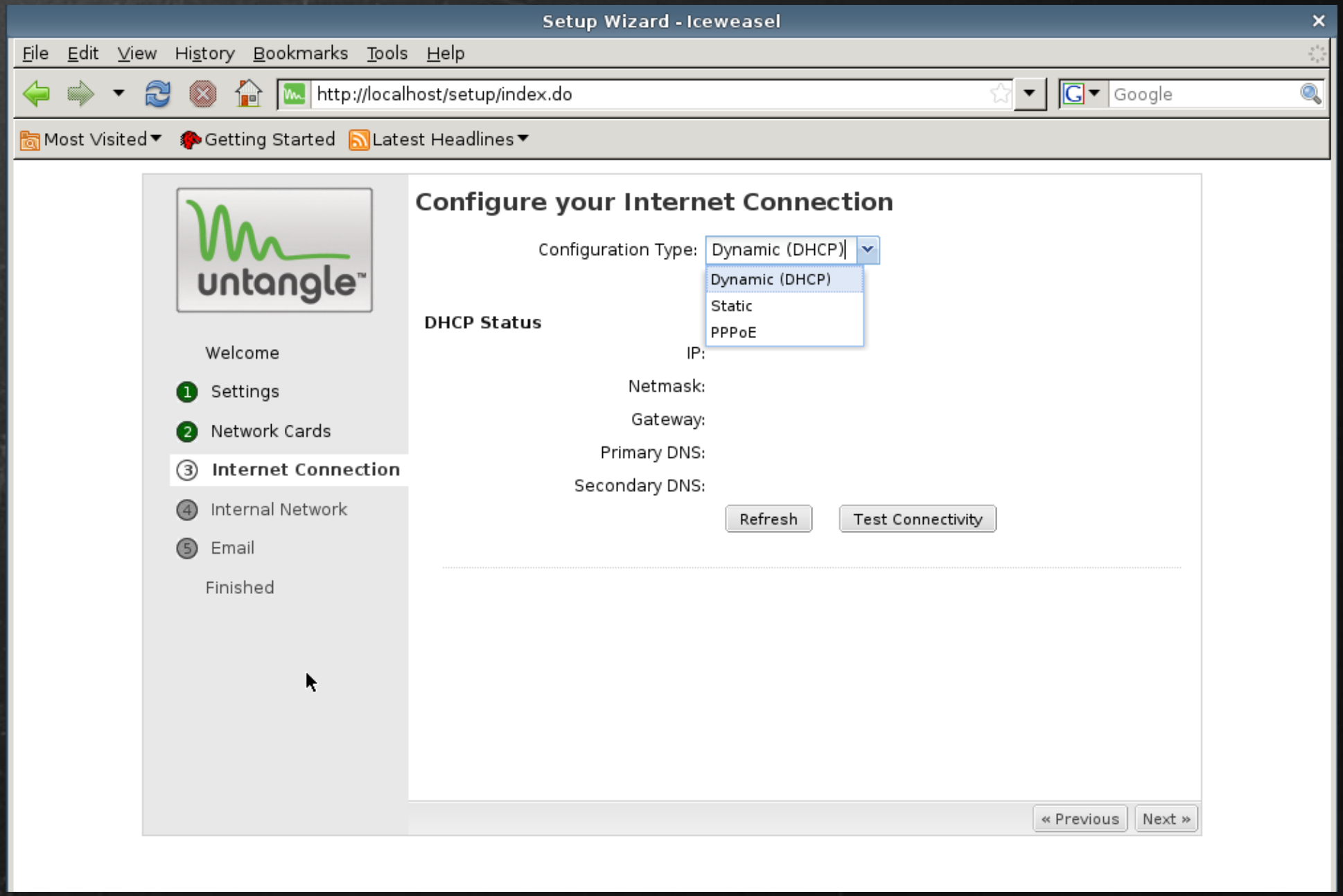

untangle
Error: Username and Password do not match
Untangle Administrator Login
Server: 211.115.217.24
Username: admin
Password:
Login

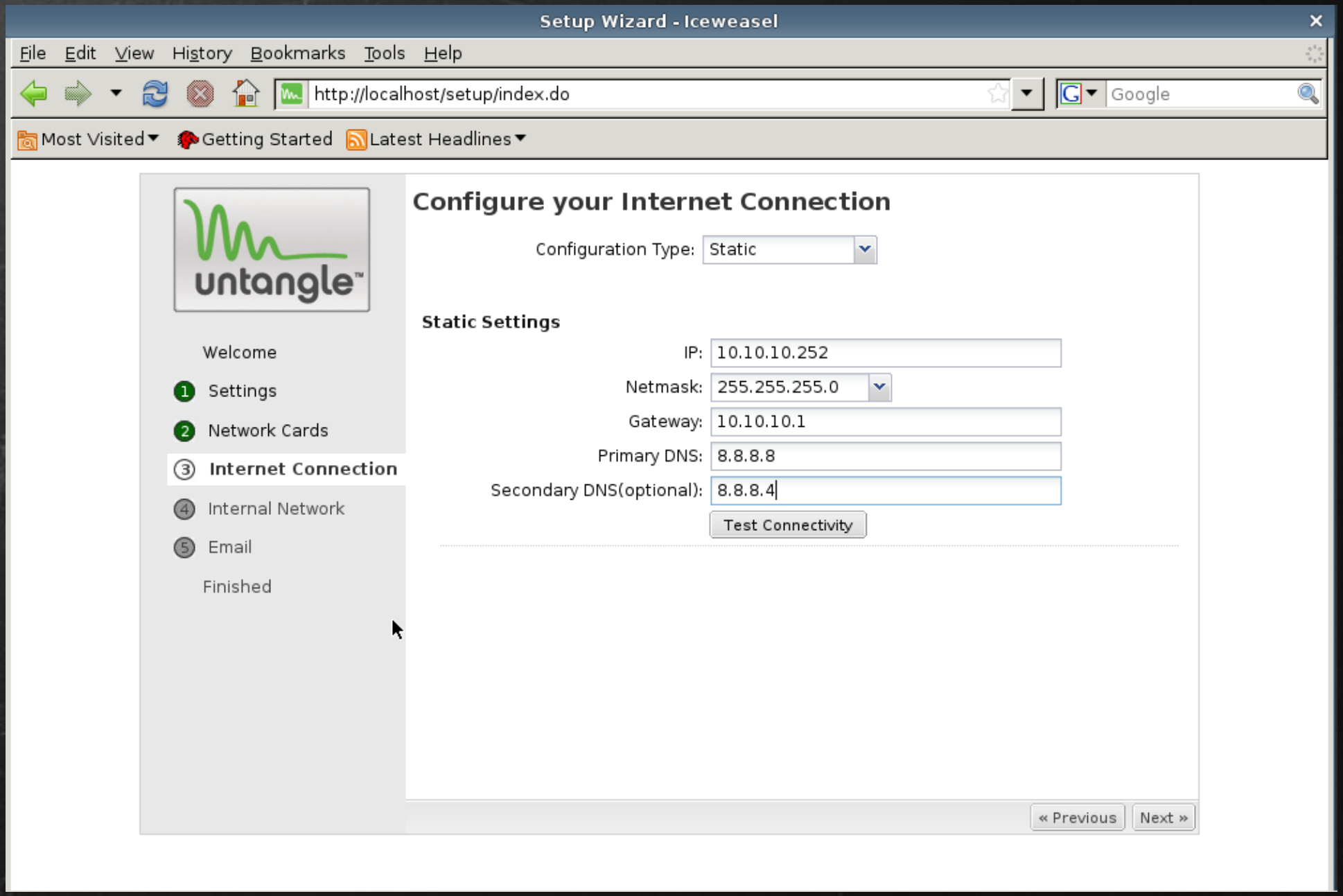

Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/language.do?console=1
Google
Most Visited
Getting Started
Latest Headlines
untangle
Language
Language Selection
Please select your language:
English
Next »


Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/index.do
Google
Most Visited
Getting Started
Latest Headlines
untangle
Welcome
1 Settings
2 Network Cards
3 Internet Connection
4 Internal Network
5 Email
Finished
Thanks for using Untangle
This wizard will guide you through the initial setup and configuration of your Untangle Server
Click Next to get started.
Next »


Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/index.do
Google
Most Visited
Getting Started
Latest Headlines
untangle
Welcome
1 Settings
2 Network Cards
3 Internet Connection
4 Internal Network
5 Email
Finished
Configure your Server
Choose a password for the admin account
Login: admin
Password:
Confirm Password:
Select a timezone
(GMT+09:00) Seoul
« Previous
Next »


Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/index.do
Google
Most Visited
Getting Started
Latest Headlines
untangle
Welcome
1 Settings
2 Network Cards
3 Internet Connection
4 Internal Network
5 Email
Finished
Identify Network Cards
Important: This step identifies your external, internal, and other network cards. Plug an active cable into each network card one at a time and hit refresh to determine which network card is which. Drag and drop the interfaces to remap them at this time.
Refresh
Name
Status
External
eth0 : connected
Internal
eth1 : connected
« Previous
Next »


Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/index.do
Google
Most Visited
Getting Started
Latest Headlines
untangle
Welcome
1 Settings
2 Network Cards
3 Internet Connection
4 Internal Network
5 Email
Finished
Configure your Internet Connection
Configuration Type: Dynamic (DHCP)
Dynamic (DHCP)
Static
PPPoE
DHCP Status
IP:
Netmask:
Gateway:
Primary DNS:
Secondary DNS:
Refresh
Test Connectivity
« Previous
Next »


Setup Wizard - Iceweasel
File Edit View History Bookmarks Tools Help
http://localhost/setup/index.do
Google
Most Visited
Getting Started
Latest Headlines
untangle
Welcome
1 Settings
2 Network Cards
3 Internet Connection
4 Internal Network
5 Email
Finished
Configure your Internet Connection
Configuration Type: Static
Static Settings
IP: 10.10.10.252
Netmask: 255.255.255.0
Gateway: 10.10.10.1
Primary DNS: 8.8.8.8
Secondary DNS(optional): 8.8.8.4
Test Connectivity
« Previous
Next »

Setup Wizard - Iceweasel

File Edit View History Bookmarks Tools Help

http://localhost/setup/index.do

Google

Most Visited Getting Started Latest Headlines

untangle™

- Welcome
- 1 Settings
- 2 Network Cards
- 3 Internet Connection
- 4 Internal Network
- 5 Email
- Finished

Configure your Internal Network Interface

Transparent Bridge

This is recommended if the external port is plugged into a firewall/router. This bridges Internal and External and disables DHCP.

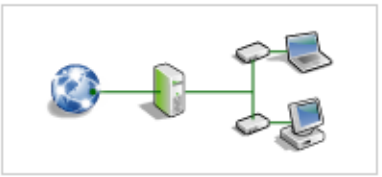
Router

This is recommended if the external port is plugged into your internet connection. This enables NAT on the Internal Interface and DHCP.

Internal Address: 192.168.2.1

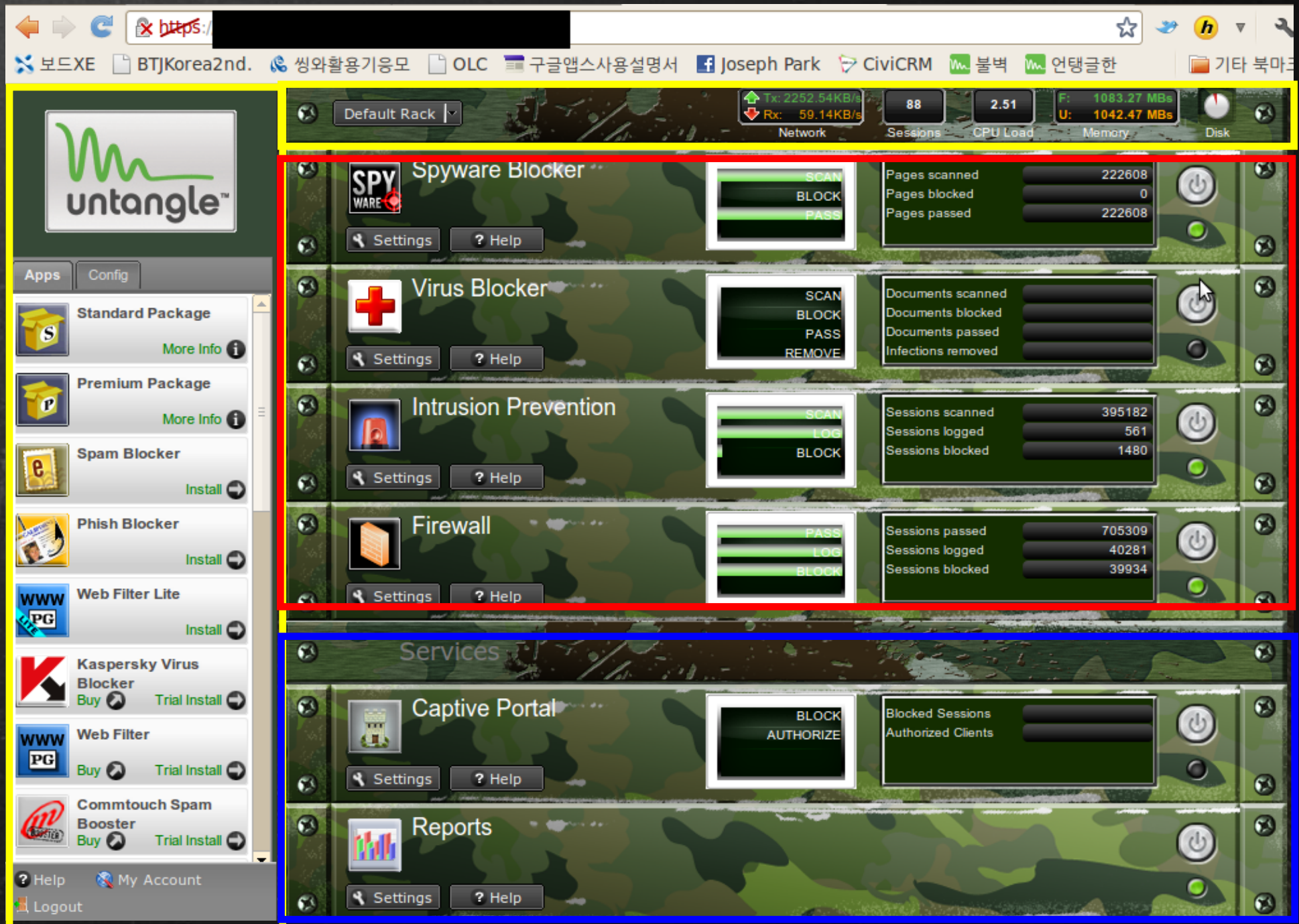
Internal Netmask: 255.255.255.0

Enable DHCP Server (default)

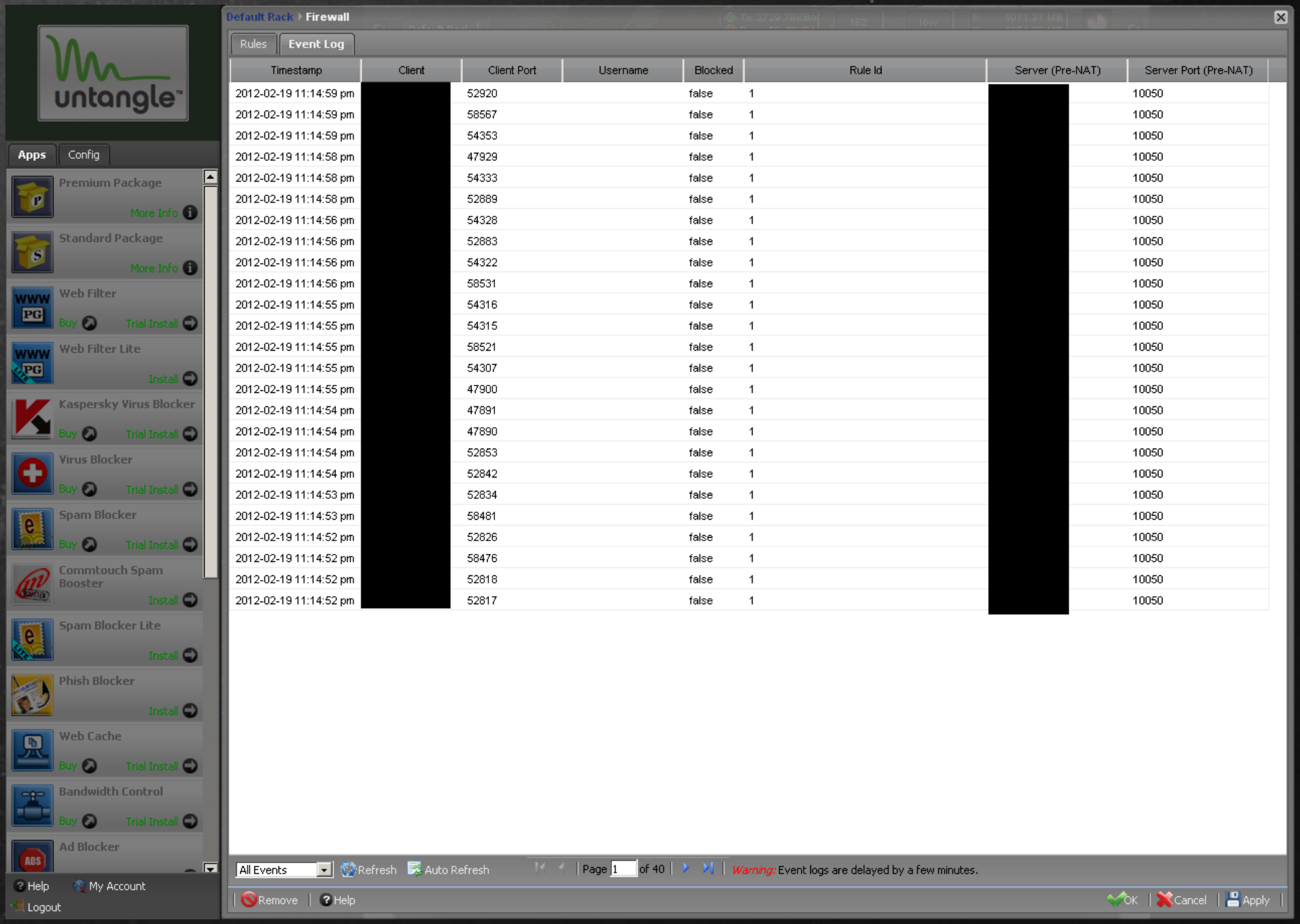


« Previous Next »

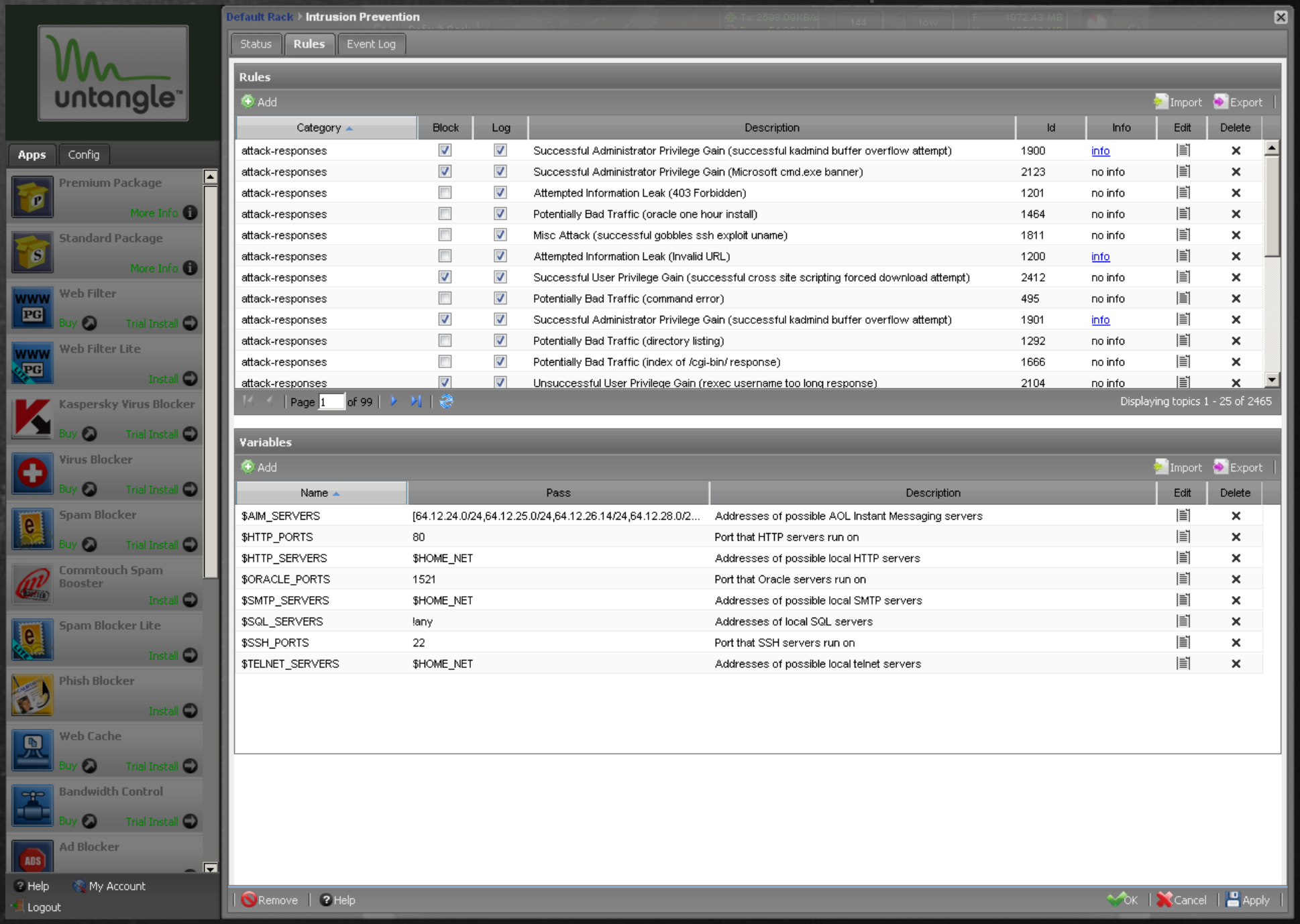
Chap 3. Configure


https:/
보드XE
BTJKorea2nd.
씽와활용기응모
OLC
구글앱스사용설명서
Joseph Park
CiviCRM
불벽
언탱글한
기타 북마크
untangle
Apps
Config
Standard Package
More Info
Premium Package
More Info
Spam Blocker
Install
Phish Blocker
Install
Web Filter Lite
Install
Kaspersky Virus Blocker
Buy
Trial Install
Web Filter
Buy
Trial Install
Commtouch Spam Booster
Buy
Trial Install
Help
My Account
Logout
Default Rack
Tx: 2252.54KB/s
Rx: 59.14KB/s
Network
88
Sessions
2.51
CPU Load
F: 1083.27 MBs
U: 1042.47 MBs
Memory
Disk
Spyware Blocker
SCAN
BLOCK
PASS
Pages scanned 222608
Pages blocked 0
Pages passed 222608
Settings
Help
Virus Blocker
SCAN
BLOCK
PASS
REMOVE
Documents scanned
Documents blocked
Documents passed
Infections removed
Settings
Help
Intrusion Prevention
SCAN
LOG
BLOCK
Sessions scanned 395182
Sessions logged 561
Sessions blocked 1480
Settings
Help
Firewall
PASS
LOG
BLOCK
Sessions passed 705309
Sessions logged 40281
Sessions blocked 39934
Settings
Help
Services
Captive Portal
BLOCK
AUTHORIZE
Blocked Sessions
Authorized Clients
Settings
Help
Reports
Settings
Help

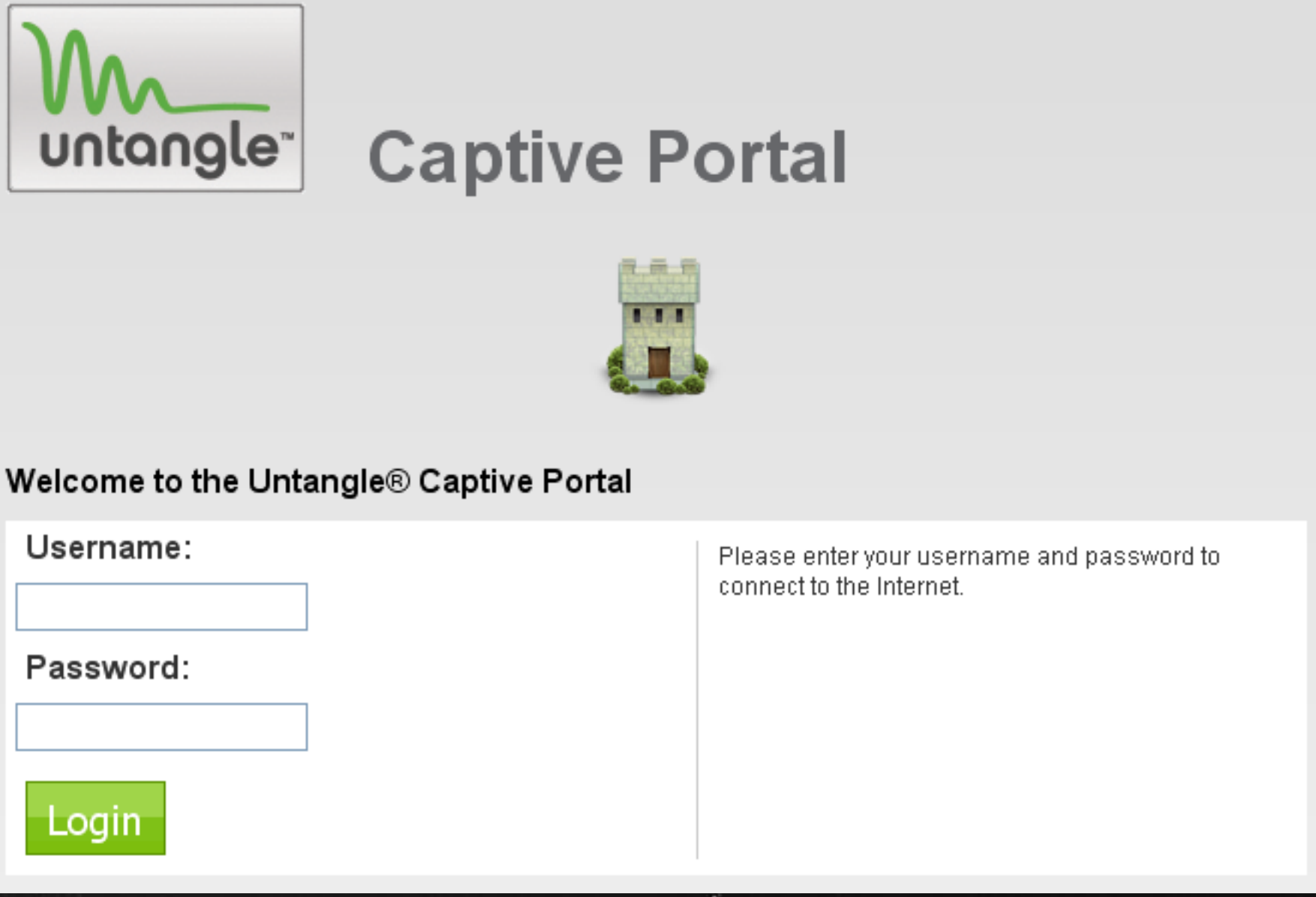
Chap 4. Operation



Firewall Event Logs


untangle
Apps
Config
Premium Package
More Info
Standard Package
More Info
Web Filter
Buy
Trial Install
Web Filter Lite
Install
Kaspersky Virus Blocker
Buy
Trial Install
Virus Blocker
Buy
Trial Install
Spam Blocker
Buy
Trial Install
Commtouch Spam Booster
Install
Spam Blocker Lite
Install
Phish Blocker
Install
Web Cache
Buy
Trial Install
Bandwidth Control
Buy
Trial Install
Ad Blocker
Help
My Account
Logout
Default Rack
Intrusion Prevention
Status
Rules
Event Log
Rules
Add
Import
Export
Category
Block
Log
Description
Id
Info
Edit
Delete
attack-responses
Successful Administrator Privilege Gain (successful kadmind buffer overflow attempt)
1900
info
attack-responses
Successful Administrator Privilege Gain (Microsoft cmd.exe banner)
2123
no info
attack-responses
Attempted Information Leak (403 Forbidden)
1201
no info
attack-responses
Potentially Bad Traffic (oracle one hour install)
1464
no info
attack-responses
Misc Attack (successful gobbles ssh exploit uname)
1811
no info
attack-responses
Attempted Information Leak (Invalid URL)
1200
info
attack-responses
Successful User Privilege Gain (successful cross site scripting forced download attempt)
2412
no info
attack-responses
Potentially Bad Traffic (command error)
495
no info
attack-responses
Successful Administrator Privilege Gain (successful kadmind buffer overflow attempt)
1901
info
attack-responses
Potentially Bad Traffic (directory listing)
1292
no info
attack-responses
Potentially Bad Traffic (index of /cgi-bin/ response)
1666
no info
attack-responses
Unsuccessful User Privilege Gain (rexec username too long response)
2104
no info
Page 1 of 99
Displaying topics 1 - 25 of 2465
Variables
Add
Import
Export
Name
Pass
Description
Edit
Delete
$AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/2...
Addresses of possible AOL Instant Messaging servers
$HTTP_PORTS
80
Port that HTTP servers run on
$HTTP_SERVERS
$HOME_NET
Addresses of possible local HTTP servers
$ORACLE_PORTS
1521
Port that Oracle servers run on
$SMTP_SERVERS
$HOME_NET
Addresses of possible local SMTP servers
$SQL_SERVERS
!any
Addresses of local SQL servers
$SSH_PORTS
22
Port that SSH servers run on
$TELNET_SERVERS
$HOME_NET
Addresses of possible local telnet servers
Remove
Help
OK
Cancel
Apply

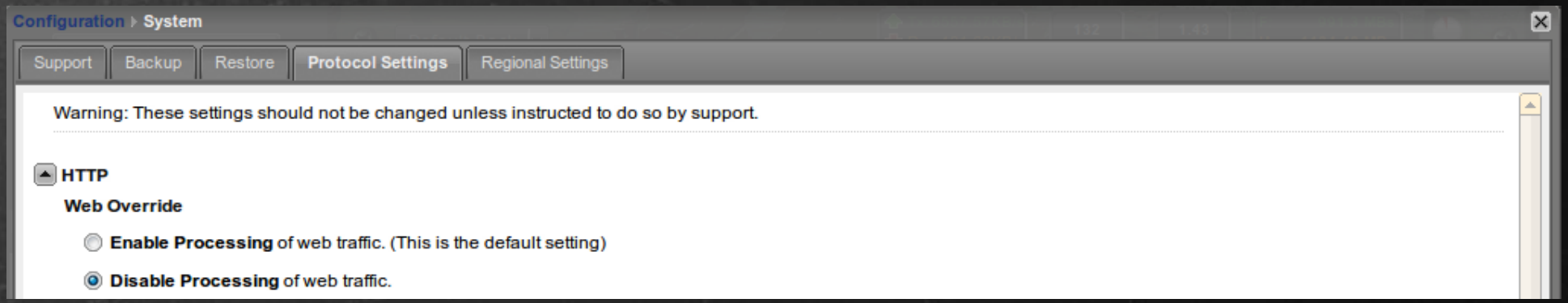
IPS Rule Set

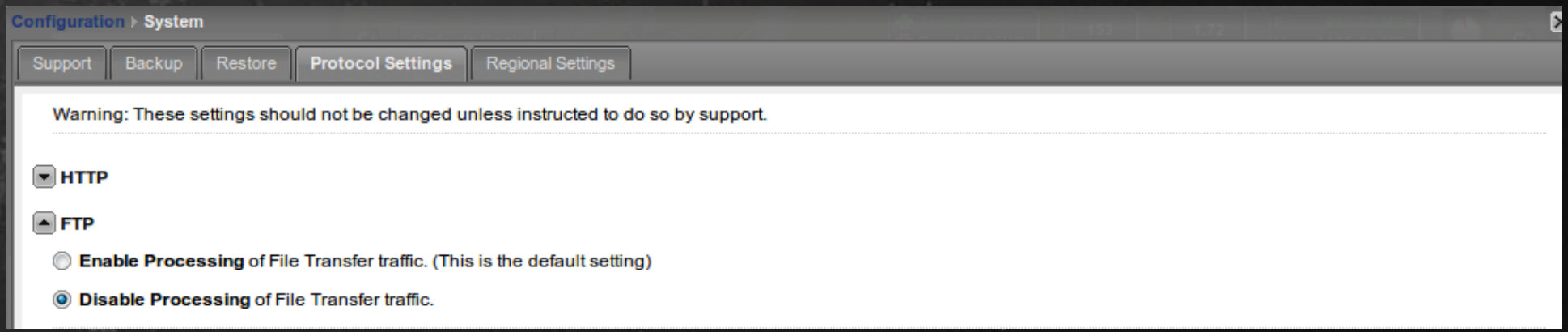


Captive Portal Login Page

Chap. 5 Trouble Shooting

Config -> System


Configuration
System
Support
Backup
Restore
Protocol Settings
Regional Settings
Warning: These settings should not be changed unless instructed to do so by support.
HTTP
Web Override
Enable Processing of web traffic. (This is the default setting)
Disable Processing of web traffic.


Configuration
System
Support
Backup
Restore
Protocol Settings
Regional Settings
Warning: These settings should not be changed unless instructed to do so by support.
HTTP
FTP
Enable Processing of File Transfer traffic. (This is the default setting)
Disable Processing of File Transfer traffic.

ETC - Hack Untangle

- Customizing Untangle Captive Portal page

Branding Logo

/var/www/images/BrandingLogo.gif

Captive Portal Icon

/var/www/skins/default/images/user/icon_captive_portal.png

Green Login button

/var/www/skins/default/images/user/green-button-background-3.gif

,green-button-background-3_f2.gif (MouseOver)

Captive Portal Favicon

/var/www/images/favicon-captive-portal.png

ETC - Regional Setting

- http://pootle.untangle.com/ko/
- http://forums.untangle.com/korean/

QnA

Thx.