

Computer Security Administration  
Computing and Networking Services  
University of Toronto

---

# Endpoint Security Policy System

*A Network Access Control System with Vulnerability  
Detection and User Remediation*

*Submitted by:*

*Evgueni Martynov*

*Mike Wiseman*

## Contents

<b>Summary .....</b>	<b>3</b>
<b>Overview.....</b>	<b>3</b>
<b>ESP Network Isolation.....</b>	<b>3</b>
<b>ESP Vulnerability Detection.....</b>	<b>4</b>
<b>ESP User Remediation .....</b>	<b>4</b>
<b>Appendix I - Utilities .....</b>	<b>5</b>

## Summary

The Endpoint Security Policy (ESP) system is an implementation of Network Access Control (NAC) which is functionality used to protect an institution's computer networks from the connection of vulnerable and compromised hosts. This is a common scenario in a higher-ed environment in which students attach their desktop or laptop computers to a wired or wireless network at a residence or academic facility.

## Overview

There are three components to an ESP system: network isolation, vulnerability detection and user self-remediation. Network isolation is implemented using the well known Netreg software which uses two pools of DHCP addresses – the first to provide a zone in which a user has limited access to network services, and the second to provide full network access.

## ESP Network Isolation

Network isolation or quarantine zone is implemented in the ESP package using the open source package called NetReg ([netreg.sourceforge.net](http://netreg.sourceforge.net)) v-1.3. The basic theory behind Netreg is as follows: Netreg operates using two pools of DHCP addresses, one pool is non-routable, the other routable. It runs under UNIX and contains configuration files to set up the DHCP server as well as web documents and scripts which make up a user and an administrator interface.

Originally, NetReg components were: a DHCP server, a DNS server, and an Apache web server. We replaced DNS server with Squid Internet cache server and make use of Linux IPTables firewall to implement network isolation for non-registered users.

When an unregistered computer (client) connects to the network it gets a non-routable IP address. The Squid and the IPTables firewall are configured to allow traffic to a limited number of domains, to local university hosts to download software, to Microsoft to get the latest updates for Windows OS and applications (MS Office), to AntiVirus sites to get AntiVirus software and updates. Squid Internet cache works as a transparent proxy.

The client gets a page with a link to run vulnerability detection agent (ESP agent) in order to be checked for missing Microsoft patches and status of an AntiVirus software (running, up-to-date).

We would like to mention here that computers with non-Windows OS skip the scan and will be redirected to a Registration Page where users can provide information needed for registration (name, room number, etc). After a user types in that information the computer will receive a new routable IP address within two minutes.

We use HTTP cookies to communicate the status of client computer to the ESP server in order for the server to display the needed page – the Fail Page in the case of a missing patch or the Registration Page if

computer has all the patches and AV is up-to-date. Scan status cookie is written by the ESP Agent to the hard drive and will be later sent by the Internet Explorer browser to the ESP server.

## **ESP Vulnerability Detection**

The heart of the ESP system is the utility which makes use of Microsoft's MBSA security analysis tool to check the status of operating system and application security updates. It also detects the status of antivirus protection using two useful checks – writing an EICAR pattern to see if the AV is functional and a Windows Management Interface (WMI) check to obtain Windows Security Center data on the status of antivirus definition updates. The utility is built using the useful open source package Nullsoft Scriptable Installer System (NSIS) which provides a simple API to develop simple Windows applications.

## **ESP User Remediation**

An important design criteria of ESP is the need to have end users do as much of the repair or remediation of their computers as possible. So, when the user's system is missing critical security updates, the system directs users to MicrosoftUpdate, which is Microsoft's resource for users to install updates. All remediation instruction and guidance is provided by topical web documentation – operating system update issues detected by ESP vulnerability detection cause an update web page to be presented to the user, antivirus issues cause an AV web page to be presented, etc.

## Appendix I - Utilities

### Scripts to check for static IP addresses

**mac-detect.sh** - reports on active MAC addresses that are not registered in the ESP dhcpd.conf file. These may be the result of a user bypassing DHCP and assigning a hard-coded IP.

This is an example of what should be placed in to the crontab

```
0,15,30,45 * * * * /usr/local/bin/mac-detect.sh
10,25,40,55 * * * * /usr/local/bin/staticIPsummary.pl /var/log/mac-rpt.txt
/var/log/mac-rpt.summary
15 * * * * /usr/local/bin/staticIPcheck.sh
```

### Blocking MAC address

It's possible to block a host with a particular MAC address from accessing the outside world. There are two types of blocking. Please note that in either case the host has an unregistered (10.x.x.x) ip address obtained from the DHCP server running on the NetReg box.

### Quarantine (or Partial) blocking

The host has access to the same resources (Microsoft patches, Symantec, CNS site) as a regular unregistered client, but it cannot get a registered ip address until administrator unblock it.

That is controled via /var/lib/dhcp/netreg\_ether.deny file.

The checking is done in cgi-bin/register.cgi just before writing to the dhcpd.conf.new

The "netreg\_ether.deny" file entry format is:

MAC\_ADDRESS<space>Some text to display for a user

Blank lines and lines started with # are ignored.

example:



```
00:0c:29:5d:7c:d7 This host is blocked because of the Gaobot worm infection.
00:0c:29:c0:ec:1d The host is scanning others for LSASS vulnerability.
```

### Full Blocking

In the case of full blocking host can only access the NetReg webserver and hosts on the local network. Every attempt to go to the outside world brings the user to the status page on the NetReg box telling him that the MAC address has been blocked and the reason for the blocking (controlled via an entry in /var/lib/dhcp/netreg\_ether.deny file).

To enabling MAC blocking save the original /var/www/htdocs/index.html


under name /var/www/htdocs/index\_orig.html - it will be read and displayed by /cgi-bin/status.cgi if the user MAC is not blocked.  
 Copy ./netreg/htdocs/index\_redir.html to /var/www/htdocs/index.html  
 This file will redirect everyone to /cgi-bin/status.cgi .  
 Create a blank /var/lib/dhcp/netreg\_ether.deny file.  
 Copy ./netreg/cgi-bin/status.cgi to /var/www/cgi-bin/ if it's not there.

To fully block a MAC address click on  in /cgi-bin/admin/admin.cgi  
 for a partial block click on  or you can do it manually via  
 /usr/local/bin/netreg\_block\_mac.sh.

## Bandwidth Limiting

It is possible to limit bandwidth for a particular registered IP address.  
 It is done via a DHCP default gateway option and an IPTable firewall rule.

We have to add runlevel information for system services  
 to run /etc/init.d/netregbandw at boot time.  
 This should be added in to the crontab to save bandwidth rules between  
 reboots:  
 0-59/1 \* \* \* \* /etc/init.d/netregbandw save

To impose bandwidth limit to a specific IP click on  in /cgi-bin/admin/admin.cgi

## MAC-IP address history

To save history information about MAC-IP address mapping and times add this to crontab:

```
28 17 * * * cp /var/lib/dhcp/dhcpd.leases
/var/lib/dhcp/hist/dhcpd.leases.`/bin/date +%F\-%T`
```

The search interface is available via this script /cgi-bin/admin/hist.cgi

## Appendix II – Installation and Configuration of ESP server

The ESP server software has been tested on Linux Fedora Core 2, Core 4 and Core 5 (with some minor changes as placement of DHCP server files). SELinux was turned off.

These packages have to be installed before installing ESP server software: dhcp, squid, apache, mod\_ssl, subversion. These Perl modules Text::BasicTemplate, Net::Netmask, Net::IMAP::Simple, Mail::POP3Client, Net::LDAP. Two IP addresses have to be configured on a single interface - one for a private non-routable network and one real. These IP addresses have to be in the same networks as served by the DHCP server.

After you downloaded and uncompressed the ESP server files into a folder you can start installing and configuring it.

init.sh - initialization script. './init.sh -A' overwrites old files.  
 start.pl - copies files from local repository to needed places  
 config.pl - configurator for local box

#### POST-INSTALLATION

- run serviceconf to disabled unnessesary services and auto-start the needed ones, like httpd,squid

Add this to the root's crontab

```
0-59/1 * * * * /usr/local/bin/refresh-dhcpdconf
```

Make sure that the ESP server clock is synchronized with a NTP server

```
20 2 * * * /usr/bin/rdate -s <put_ntp-server_ip_here>
```

Dhcpd.leases file can be saved for future references. To backup them to /var/lib/dhcp/hist folder add this line to crontab:

```
28 17 * * * cp /var/lib/dhcp/dhcpd.leases /var/lib/dhcp/hist/dhcpd.leases.`/bin/date +%F-%T`
```

If you are planning to use Bandwidth limiting functionality add this to crontab after you installed netregbandw

```
0-59/1 * * * * /sbin/iptables-save > /etc/sysconfig/iptables
```

```
0-59/1 * * * * /etc/init.d/netregbandw save
```

#### CONFIGURING AN ESP SERVER TO WORK WITH AN ESP AGENT.

The ESP Agent (checker\_nr.exe) gets its real-time configuration from an ESP server. Configuration parameters are set in /etc/netreg/esp.cfg

They are configurable via <http://<ESPSEVER>/cgi-bin/admin/config.cgi>

Below is the screenshot of the configuration screen:

The screenshot shows a Mozilla Firefox browser window titled "ESP Agent Configuration File - Mozilla Firefox". The address bar displays "ESP http://10.10.10.5/cgi-bin/admin/config.cgi". The browser's menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The toolbar shows navigation buttons (back, forward, home, stop, reload) and a search bar with "Google". The page content is titled "Fill in these fields" and contains the following configuration options:

- [Display this config](#)
- ESP pass URL:
- email:
- Save Registration Info on hosts in Cookies until:  months
- Notify about static IP addresses:
- Antivirus check:
- Antivirus check Logging:
- Antivirus up-to-date check:
- EICAR check:  EICAR check Only:
- Password check:
- DHCP Vendor check:
- 

The status bar at the bottom of the browser window shows "Done".

In the ResNet ESP environment /cgi-bin/admin/ folder is protected with a password.



Here are the parameters:

```
ESPassURL= # the URL of the 'pass' page, can be left blank
email=my@email.com # email for notification about static IP addresses, can be left blank
savetimenenum=2 # number of min/hours/days/weeks/yours to save Username/Room in a cookie
savetimetyp=months # save registration Username/Room for'savetimenenum' min/hours/days/weeks/yours in a cookie

staticIPnotifiy=yes # message will be sent to 'email' if static IP monitoring scripts [1] are running and
staticIPnotifiy is set to 'yes'

avcheck=enabled # enables AntiVirus checking
avchecklog=enabled # enables AV logging to a central server where checker_nr.exe resides
avuptodatecheck=enabled # enables AV up-to-date checking

eicarcheck=enabled # enables EICAR test
eicarcheckonly=disabled # rely on EICAR test only not on presence of any AntiVirus
pwdcheck=disabled # not available

dhcpvndorcheck=enabled # enables DHCP vendor check (this will check if Windows host sends a Windows
# specific option in a DHCP request to avoid forged User-Agent info)
# dhcpd.conf has to have 'set my-vendor-class = option vendor-class-identifier;'

nextpage=/cgi-bin/auxnext.cgi # replaces /cgi-bin/next.cgi
WUSeverPass=enabled # reserved for future use with set MS Update server
```
