

At a Glance

- ▶ Captive portal forced authentication of DHCP clients
- ▶ Standard RADIUS server authentication and accounting
- ▶ Local storage of session information on the DHCPatriot
- ▶ Temporary/Permanent suspend with customer messaging support
 - Suspend by username, MAC Address, or multiple usernames
- ▶ Easy to use web-based administration interface
- ▶ Full white list based firewall protection
- ▶ Supports multiple subnets on the same interface, as well as multiple subnets across multiple interfaces via standard DHCP Relay Agent protocol
 - Additional subnets can be attached to a main subnet on the same physical network.
 - Other physical networks can be supported by adding more main subnets.
 - Static IP subnets can also be attached to a main subnet. These static IP Addresses are handed out via RADIUS and the Framed-IP-Address attribute like dial-up methods.
 - Unauthenticated subnets are also configurable and attached to main subnets.
- ▶ Support for network integration with the NetEnforcer® by Allot Communications
 - Auto host generation by username
 - Auto Virtual Channel generation in the fallback pipe by username
 - Auto assignment of QoS and host lists via information received from RADIUS
 - Makes monitoring and traffic modification of specific users easily done by username.
- ▶ Powerful search mechanisms to identify customers for abuse complaint resolution, law enforcement compliance, and acceptable use policy violations
 - Existing RADIUS server tools for session discovery can be used as well as the DHCPatriot itself
- ▶ Customer Service Representatives can authenticate users via the web-based Administration Interface so even devices without a web browser can be used on the network.
- ▶ Ability to add administrators on the fly

Requirements:

- ▶ DHCP must be the method the customers will use to get an IP Address.
- ▶ The gateway routers for the customers must support the DHCP Relay Agent protocol (helper address command on a CISCO Router).
- ▶ The unauthenticated (and in some cases the authenticated) addresses must be routed to the DHCPatriot. This is usually accomplished via source based policy routing. Policy routing location is configured based on the network layout
 - Most CISCO devices support policy based routing via ACL(s).
- ▶ A RADIUS server is required for the DHCPatriot to authenticate the users against.
 - A standard RADIUS server complying with RFC's 2865, 2138, 2866, 2139.
 - The RADIUS server must at least send the Framed-IP-Address attribute in the authentication response packet
 - A more complete response packet would contain the following:
 - Service-Type=Framed-User,Framed-Protocol=PPP,Framed-IP-Address=255.255.255.254,Framed-IP-Netmask=255.255.255.255,Framed-Compression=Van-Jacobsen-TCP-IP)
 - OPTIONAL: For NetEnforcer speed control (QoS) setup and auto addition to host lists, the Class attribute must be sent in addition to the other attributes in the authentication response packet. The format of this packet is as follows:
 - Class="NetEnforcer:[speed package]:[Group1],[Group2],...[Group10],...."
- ▶ NetEnforcer® from Allot Communications integration requires NetEnforcer® version 5.2 build 9 or higher

Note: The DHCPatriot does not replace the bootp and tftp server arrangement for cable modems in cable networks. These servers will need to remain in place. The DHCPatriot is meant for the client devices (Customer Premises Equipment) only.

Features and Benefits

The DHCPatriot provides the following security benefits as a standalone product:

Required Authentication Solution for broadband connections

- ▶ A valid username and password is required to receive a valid routable IP address

- Authentication is completed via a customizable web page
- One-time authentication unless user is suspended
- ▶ Unknown/unauthenticated clients receive a non-routable address
 - Fully configurable address scheme
- ▶ Compatible with RADIUS based authentication systems
- ▶ Session management based on lease status
- ▶ Transmits start and stop records to the RADIUS server and stores all information locally
- ▶ Can prevent address hijacking alone, or along with compliant network systems, such as routers using RBE, etc.
 - Able to enforce routing policies by stopping outbound packets from unauthenticated hosts
 - Can also team with a NetEnforcer® from Allot Communications to provide this service easily between devices
- ▶ Enforce simultaneous usage limits on a global basis
 - Multiple use groups will automatically suspend the oldest connection first when a new one is requesting
- ▶ White list firewall access
 - Only allowed ranges and ports can access
 - Configurable via the DHCPatriot's web based administration interface

The DHCPatriot provides enhanced security in conjunction with a NetEnforcer® from Allot Communications:

- ▶ Centralize authentication enforcement at the border
- ▶ Control traffic within the NetEnforcer® based on traffic authentication status from the DHCPatriot
 - Traffic can be controlled based on a combination of factors, authentication, port, size, etc.
- ▶ DHCPatriot can configure hosts and Virtual Channels on the NetEnforcer based on usernames and groups
- ▶ DHCPatriot can automatically apply QoS to a NetEnforcer® Virtual Channel based on attributes set in RADIUS
 - This can greatly speed up customer access changes and reduce trained employee overhead
- ▶ DHCPatriot is also capable of automatically assigning customers to host-lists on the NetEnforcer® via attributes set in RADIUS
 - Allows for flexible groupings of users via host-lists to shape traffic where appropriate, such as business vs. non-business customers (See example in Implementation Section)

Search Database

Compile a list of results based on username, MAC address or IP address. Supports wildcard searches and date/time delimiters for easier and faster searches with more relevant results.

Example of usage:

You have received a complaint regarding someone connected to your network sending spam. Using the IP address from the complaint you can easily search the DHCPatriot's logs and locate the user info to expedite correcting the situation.

Search DHCP Logs

Search through the current day's raw DHCP logs by MAC address.

Example of usage:

A customer is unable to maintain a consistent connection. They contact Technical Support and after searching the raw DHCP logs, Technical Support discovers that the user is renewing their IP Address repeatedly, followed by a DHCPDISCOVER at the end of the lease. This tells Support Technician that the user likely has a firewall that is blocking ports 67 or 68 TCP/UDP. They help the user correct the problem, and the customer is able to maintain a connection.

IP Address Usage

This report shows a summary of all configured networks and their corresponding unauthenticated networks. It also shows any associated dynamic subnets and static IP subnets. A common relationship among all of these networks can be tracked via a Shared Network naming system. The report also contains the number of IP addresses configured, the number currently in use, and the percentage of the network that is currently in use.

Customer Usage

A summary report of each network that includes, the amount of IP Addresses and devices in use, as well as the amount of unique customers. With this report you can quickly summarize the amount of usage on the network to help you to determine if you need to allocate additional networks due to over-subscription.

Suspend User

This feature grants an administrator the ability to suspend a user(s) from their current session on the DHCPatriot. Suspensions via single MAC address will only suspend that device, whereas suspensions via username will suspend all devices attached to that username. The suspension can be annotated to display information specifically to that user during their next login attempt.

Example of usage:

A customer is spreading a virus and his connection has been located and verified via the DHCPatriot records. A temporary suspension can be performed using the Suspend User function. This suspension will direct him back to the DHCPatriot login screen on his next attempt at using the internet service. Additionally you can leave a note for him that will display on this login screen, such as, a warning about the issue and advice to contact Technical Support for further assistance. Permanent suspension of the customer's account is still centrally handled on the RADIUS server via your current methods.

View Suspended

This is a summary report of all users who have been suspended. This report includes MAC address, username, reason of suspension and any notes left for the user by the person who suspended the account.

Implementation

Required Items

1. Any router that supports the DHCP Relay Agent protocol. (All Cisco routers support this option.)
2. Router(s) nearest the DHCPatriot must support Policy Based Routing. (All Cisco routers support this option.)
3. A RADIUS server.

Optional Items

1. A NetEnforcer® from Allot Communications
2. A RADIUS server that supports the Class reply attribute, Free RADIUS and Radiator both support this method (RFC 2138).

Typical Installation

1. DHCPatriot is installed in the central data center.
 - ▶ The DHCPatriot is able to handle multiple connection types, including DSL, Cable Access, Wireless, Ethernet and Fiber-to-the-home (FTTH) or any combination of these types.
2. Router interfaces are setup to relay DHCP messages to the DHCPatriot
 - ▶ The DHCPatriot knows where to respond based on the source address of the DHCP Relay Agent
3. Unauthenticated clients are assigned an IP Address from the Unauthenticated Address Range and are not routable outside the network
 - ▶ The DHCPatriot receives ALL outbound traffic from the Unauthenticated Range thru Policy Routing
 - ▶ The only web page served to the Unauthenticated Range will be the DHCPatriot Login Page
4. After successful authentication and the connected device has been power-cycled the user will receive an IP Address from the Authenticated Address Range.
 - ▶ All further data transactions are seamless to the user and the user will not be asked for his information again on this hardware configuration

Address Hijacking Prevention

Without a NetEnforcer® from Allot Communications:

- ▶ The router will need to support both ATM and RBE routing and be able to be setup to disallow routing if an IP Address was not obtained via DHCP (Cable Access and Cisco Routers support this).

- OR -

- ▶ Use the DHCPatriot in Controlled Routing mode. The DHCPatriot will only route outbound traffic from the Authenticated Addresses.

With a NetEnforcer® from Allot Communications:

- ▶ The fallback Virtual Channel (VC) in the Fallback Pipe on the NetEnforcer® is setup to cause all unauthenticated packets to drop.

Advantages of a DHCPatriot & NetEnforcer® team:

1. The DHCPatriot automatically configures a Host Entry and Virtual Channel (VC) in the Fallback Pipe for each username. The Host Entries and Virtual Channels are retained even during periods where the user is offline which will allow rules set on the NetEnforcer® to be retained for a user indefinitely and not just per session.

Example: User *johnqinternet* would have a host entry and VC on the NetEnforcer® named *johnqinternet*. If this user had multiple IP Addresses available to them they would all be listed under this one entry.

- The DHCPatriot is able to convey Quality of Service (QoS) speed controls and information from your RADIUS server directly to the NetEnforcer for enforcement. The Quality of Service setting in RADIUS must exactly match an existing QoS setting on the NetEnforcer® for this to function.
- The DHCPatriot is able to convey Host list attributes from RADIUS to the NetEnforcer® as well. The Host list (or Host List Option) on the NetEnforcer® allows a group of hosts (users) to be placed together and have special rules applied to all of them. Users can belong to multiple Host lists to allow for limitless configuration.

Example: Rules can be setup to enforce speed limits, for example: Gold = 1mb, Silver = 512kb, Bronze = 256kb. Rules can also be setup to limit or prevent certain types of traffic, for example: NoP2P = all common peer-to-peer file sharing access is blocked, NoFTP = only FTP functionality is blocked, NoGame = all common internet gaming access is blocked.

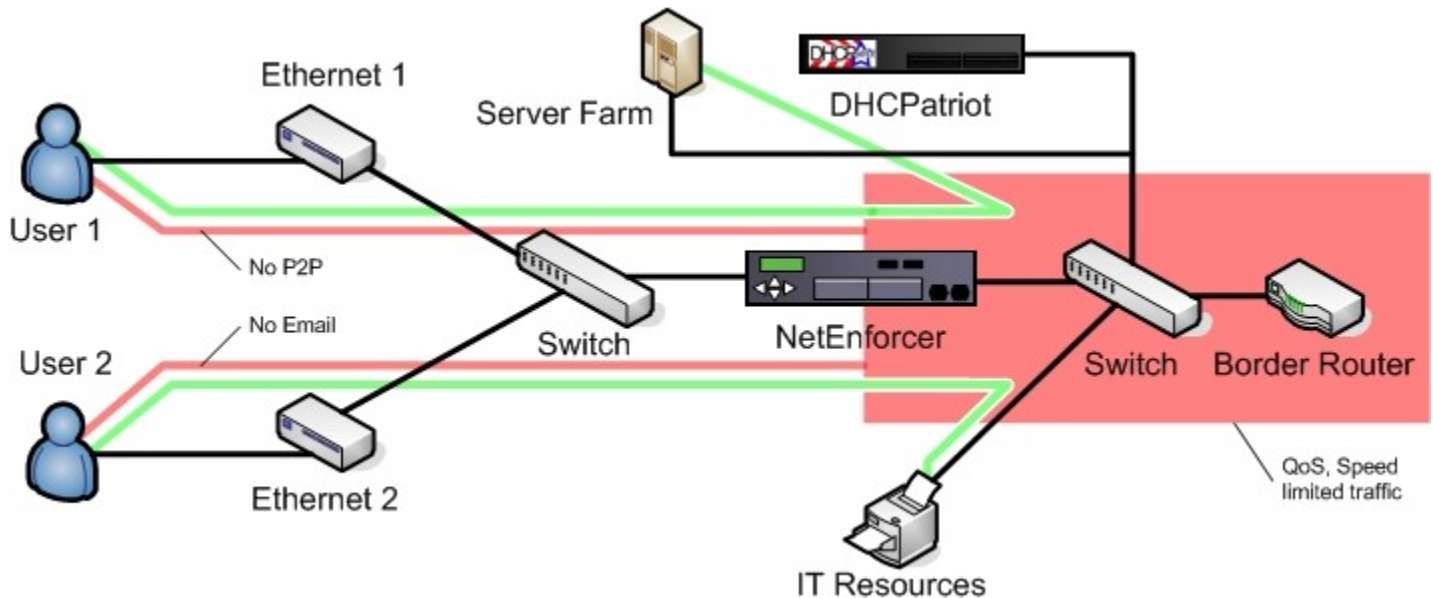


Diagram 1

Scenario:

A user on your network has been abusing P2P file sharing on his Gold tier connection and the access needs to be shut off. This user still requires full access to the company's server farm to administer a server there. Another user has been reported as transmitting a virus infection via email. Before this spread becomes worse all email access needs to be shut off to contain the outbreak. However this cannot limit their access to network's IT Resources such as a network printer and they still need their QoS access tier to the internet maintained.

Scenario Solution using the DHCPatriot and NetEnforcer® combination:

- The DHCPatriot and NetEnforcer® can force authentication for all users on the network
- The DHCPatriot and NetEnforcer® can enforce QoS speed limited traffic to each user automatically according to their RADIUS setting regarding this.
- Placing a Pipe above the Fallback Pipe on the NetEnforcer® specifying the destination network of the IT resources will guarantee that users of the network can access these resources at line speed.
- User 1 has been abusing P2P (peer-to-peer) file sharing and the administrator wants to block his access to it. The NetEnforcer® is capable of application layer examination of the traffic and has a predefined host list for all currently known P2P software. A pipe can be made, above the fallback pipe, on the NetEnforcer® for the purpose of blocking all P2P software connections. Then a "NoP2P" host list can be made and applied to that Pipe. In the RADIUS server this host list can be applied to different users via the Class attribute as described earlier. Once the "NoP2P" class in RADIUS has been set to active for a user, that user's ability to access P2P will be disabled and not affect any other users on the network.
- Users who are sending virus emails can be blocked in the same way as described in number 4. A Pipe is created above the Fallback Pipe called "NoEmail". A host list is then created called "NoEmail" and is applied to the "NoEmail" Pipe. The RADIUS server is then configured to specify the user as belonging to the "NoEmail" host list via the Class Attribute. When the DHCPatriot receives this information it will pass it onto the NetEnforcer® and the user will not be able to receive email at any device he is logged into on the network, no matter where he connects or what IP Address he receives.
- User 1 is an administrator of the server farm and thus must be allowed full access to the server farm. This can be accomplished by creating a pipe that allows full line speed access to the server farm via destination network. Create a host list called "ServerFarmAccess" and apply this host list to the previously created pipe. The RADIUS server will then be configured to send ServerFarmAccess in the host list list portion of the Class attribute when User 1 authenticates. The DHCPatriot will then apply the host for User 1 to the host list ServerFarmAccess at the time of authentication. This will grant full line speed access to the server farm to User 1 no matter what IP Address he obtains.

Any combination of the above rules can be used on any user. The modifications are all made on the RADIUS server for predefined rules and host lists on the NetEnforcer.

