CALEA Compliance

First Network Group Inc
1-800-578-6381
www.DHCPatriot.com

The DHCPatriot™ can help a network achieve CALEA compliance while maintaining or moving to the freedom of a DHCP network and so much more!

What is the DHCPatriot™?

The DHCPatriot™ is a DHCP server that requires customers to authenticate themselves prior to using the network. This allows Internet Service Providers to easily track customer identification without need of special software, stability problems, manual record keeping, or extra overhead. The DHCPatriot™ is a secure, stable, simple to use/manage, and flexible platform for management of broadband subscribers.

The DHCPatriot™ employs the proven firewall technology of Linux® in a white-list-style configuration to protect from outside intrusion. With its CLI based system configuration menu interface, and web based administration interface, the DHCPatriot™ provides the network visibility and easy to use configuration options that administrators need without the burden to customers that comes with PPPoE or the time consuming task of assigning and maintaining static IP addresses.

Any type of broadband that supports DHCP can benefit from the DHCPatriot™. Easy access to both session data and IP address utilization information is standard.

For further details regarding the DHCPatriot™, please visit www.dhcpatriot.com

What is CALEA and why do I have to comply with it?

The Internet introduces a new method of communication and information seeking in our everyday lives. Law enforcement has been forced to upgrade their communications surveillance capabilities.

In 1994, US Congress passed the Communications Assistance for Law Enforcement Act (CALEA) which obligates service providers to facilitate court ordered communication surveillance by law enforcement agencies. In 2005, the FCC ruled that this includes broadband and VOIP providers. Service providers have until May 2007 to be compliant. Communications surveillance is highly complex in today's environment, and law enforcement has neither the resources nor expertise required to perform lawful interception without help from service providers. Therefore, Congress and the FCC have placed the initial resource outlay and technical details of implementation squarely in the hands of the service providers.

Law enforcement is interested in two categories of information during a lawful interception of a target: "Call Data" and "Call Content." Call Data is identifying information (example: target login and logout times) that can be used to identify a target on the Internet as well as the target's communications, known as Call Content. Almost all warrants will require Call Data. Some will require Call Content as well.

The interception is achieved via three types of network elements performing three functions: Access, Mediation and Collection. The Access Function refers to the network elements responsible for the interception and transfer of the Call Data and Call Content to the Mediation Function. The

Mediation Function is responsible for the formatting of the intercepted information and its delivery to the LEA (Law Enforcement Agency). The Collection Function is performed by a network element in the LEA's network for storage, formatting and review.

CALEA requires that two facets of privacy be protected. The LEA can only be allowed to access information that is covered by warrant, and no other information regarding the Target, or any other customer on the service provider's network. Secondly, if multiple LEAs are engaged in surveillance of a particular target, they can not be aware of each other. The purpose of the Mediation Function is to insure that these two requirements are met.

CALEA also requires that the target must not be able to detect the surveillance activities of the LEA. Therefore, no changes to a target's access may be made in order to facilitate a lawful interception. Changing a target to a static IP address when they usually get their IP address via DHCP or changing the path their traffic takes to facilitate an interception allow possible detection by the target, and therefore cannot be used under CALEA.

CALEA does allow a service provider to utilize a "Trusted Third Party" vendor, a contracted company to provide mediation device services for the Mediation Function between law enforcement and the service provider. Placing this portion of the solution in the hands of a Trusted Third Party vendor is often the most viable solution. This also greatly reduces the effort involved in implementing the solution.

Many service providers will be reluctant to invest the resources needed to a platform used strictly for CALEA compliance such as the Mediation Function and will take full advantage of this scenario. Others will choose to purchase their own mediation device. The DHCPatriot™ can help in either case.

For further information regarding CALEA visit www.askcalea.org

How can the DHCPatriot™ help with CALEA Compliance?

The goal of law enforcement is to monitor a specific targets activities in real time. Many ISPs currently do not have a method of identifying customers in real time. Some ISPs may not be able to accurately identify a customer that is using a specific IP address.

The DHCPatriot™ provides this much needed service to ISPs. Identities of customers are known on a DHCP network when the DHCPatriot™ is used. Each customer is forced to authenticate their device(s) before being allowed to use the network. Each customer device on the network is easily linked to a username via this method. This functionality is desirable outside of CALEA compliance as it is important to be able to quickly and easily identify problem customers for network security purposes.

The DHCPatriot™ integrates as part of the CALEA Access Function. It becomes an integral part of the Call Data transmission to the CALEA Mediation Function. In order to provide Call Data for a target of lawful interception, authentication is required. The ISP cannot suddenly introduce authentication into the network when a warrant is served as the target must not be able to detect that surveillance is occurring. Implementing a DHCPatriot™ in the network now is the best choice. The DHCPatriot™ can supply call data indirectly.

The DHCPatriot™ can optionally use an external RADIUS server for this authentication. This allows it to integrate into environments where the target Call Data is collected by a probe listening to RADIUS communications. The DHCPatriot™ is indirectly providing Call Data with this method.

RADIUS Authentication and Accounting

The DHCPatriot™ ties a username to each IP address in use on your dynamic network. It does this in real time satisfying CALEA requirements. Since the DHCPatriot optionally utilizes RADIUS authentication and accounting, it is ready to interface with the many mediation devices that are able to interface with a RADIUS server to receive information regarding a specific targets current status and IP address, collectively termed Call Data. The mediation device can then use this information to configure one or more probes to send a specific targets IP traffic, termed Call Content, to the mediation device. This requires no special configuration on the DHCPatriot™ as it is designed to force user authentication and accounting in a broadband environment.
Figure 1-1 shows an example of this type of setup.

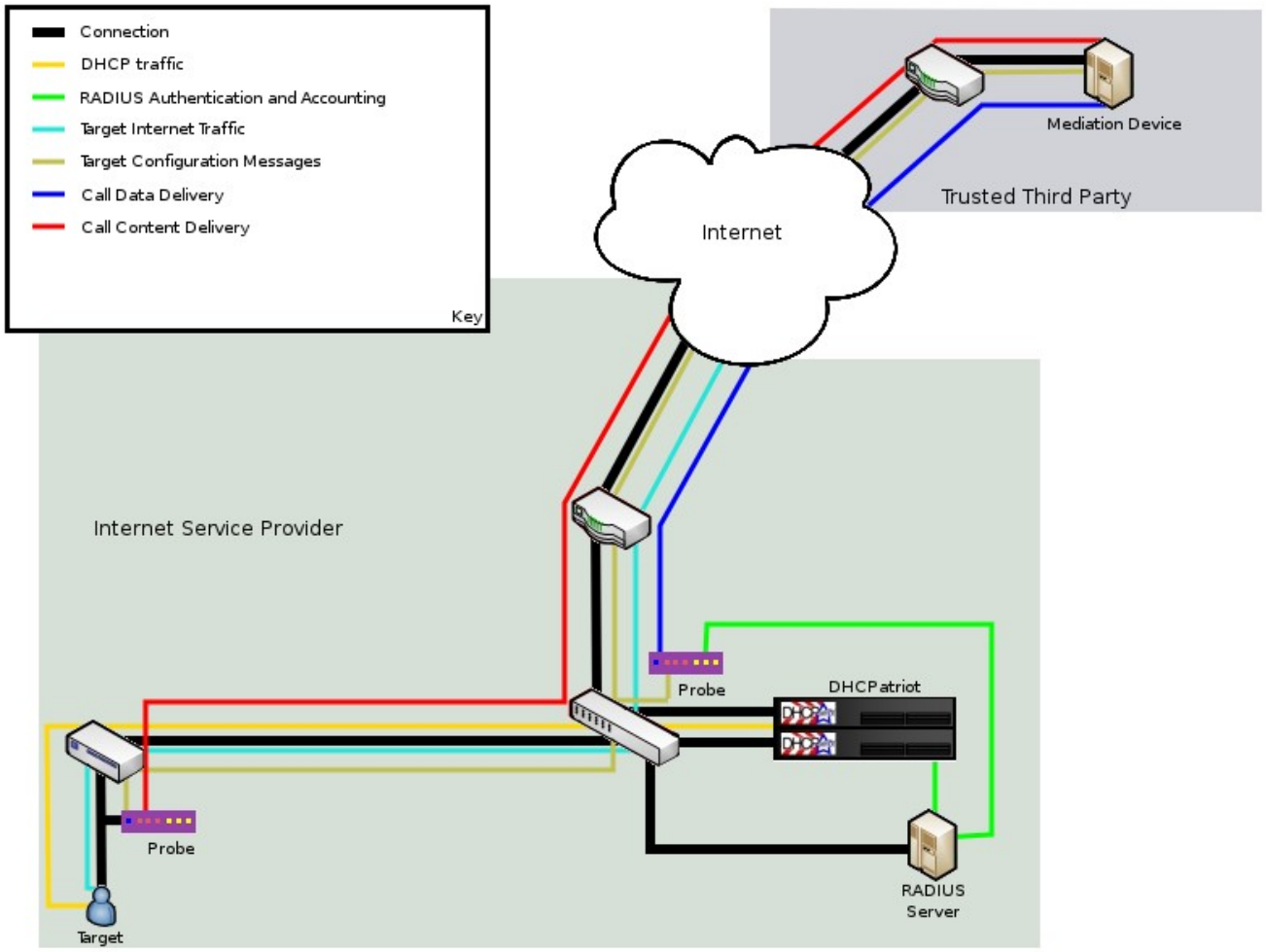

Figure 1-1: DHCPatriot™ in a generic CALEA environment

As shown in Figure 1-1, the DHCPatriot is authenticating DHCP users such as the target. This authentication and accounting is passed from the RADIUS server to the call data probe device (the probe on the right in figure 1-1). The probe then sends this information (of the Target only – other customers authentication is ignored by the probe) to the mediation device, a device that collects the Lawful Intercept data and presents it to law enforcement in real time, at the Trusted Third Party. The mediation device uses the call data to configure the call content probe device (the probe on the left in figure 1-1) to send the target's call content to the mediation device at the Trusted Third Party. A RADIUS server is required in this scenario.

Advantages of using the DHCPatriot™ beyond CALEA compliance

The DHCPatriot™ is advantageous beyond CALEA compliance. It allows the ISP to have a robust dynamic DHCP network, therefore minimizing maintenance costs and tedious record keeping tasks. At the same time, it gives the network administrator a clear view of who is using the network by using authentication without the customer affecting problems associated with PPPoE.

CALEA compliance is a non-revenue generating cost to the ISP. The DHCPatriot™ can ease some of this burden by assisting with the CALEA Access Function and being useful to the network overall outside of CALEA compliance. In today's competitive ISP market, cost control is important. The DHCPatriot™ will free network administrators for other tasks therefore further decreasing costs.

The DHCPatriot™ is an invaluable tool in it's conventional role as a tool for identifying customers to the ISP. This is important for network administrators in abuse complaint resolution, as well as locating resource abusing users on the network. Authenticating users on a DHCP network allows administrators to easily identify customers by username while maintaining the power and ease of a DHCP network.

Contact First Network Group Inc. today!

Requirements

- DHCP must be the method the customers will use to get an IP address.
- The gateway routers for the customers must support the BOOTP/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), as do many other types of routers.
- User authentication via either the Built-in Authentication, or an external RADIUS server.
  - External RADIUS server:
    - If an external RADIUS server is used, it should comply with RFC 2138/RFC 2139/RFC 2865/RFC 2866.
    - The RADIUS server must at least send the Framed-IP-Address attribute in the authentication response packet.
    - A more complete response packet would contain:
      - 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
- As of Version 4.2.0 Total DHCP Edition, the DHCPatriot™can provide Authenticated DHCP services to CPE (Customer Premise Equipment) such as computers, routers or router/modems. The DHCPatriot™can also provide non-authenticated (Standard) DHCP services as well as TFTP (Trivial File Transfer Protocol) services to other types of equipment such as FTTH (Fiber to the home) ONT (Optical Network Termination) devices, cable modems, or just simply to any network that doesn't require authentication.

How to Purchase

The DHCPatriot™ may be purchased direct, or through one of our reseller partners. If purchased direct, no discount from MSRP will be available.

To purchase through a reseller, please contact your reseller of choice. For a current list of resellers, with contact information, please visit https://www.dhcpatriot.com, email DHCPatriot@network1.net or call 800-578-6381 x7 (419-739-9240 if outside the United States of America) with your request.

To purchase direct or receive pre-sale support, please use the following contact information:

DHCPatriot@network1.net

800-578-6381 x7 (419-739-9240 x7 if outside the United States of America)

First Network Group, Inc.
P.O. Box 1662
4-6 Perry St.
Wapakoneta, OH 45895
United States of America