How to Make the Client IP Address Available to the Backend Server in Proxy Mode

https://campus.barracuda.com/doc/4259883/

When deployed in proxy mode, the Barracuda Web Application Firewall appears by default as the source IP address in the requests it forwards to the backend servers. For servers on the backend needing to access the actual client IP address, the Barracuda Web Application Firewall provides two configurable ways to achieve this:

- Client Impersonation
- X-Forwarded-For Header

Although both of these options provide the client IP address to the servers, consider the following before deciding which option to use:

Client Impersonation	X-Forwarded-For Header
Provides the client IP address in the source IP address of the request. Requires a networking change. Performance impact.	Provides the client IP address in the header "X-Forwarded-For" of the request. Requires a logging change.

Using the Client IP Address from the X-Forwarded-For Header

By default, the client IP address is inserted by the Barracuda Web Application Firewall in the request Header "X-Forwarded-For" when the request is forwarded to the backend server.

To use the embedded IP address with Apache servers or with IIS 7 or IIS 7.5 servers, refer to the following articles:

- Logging Actual Client IP Address on the Apache Server
- Logging Actual Client IP Address In the IIS 7 and IIS 7.5 Server

Logging Client IP Address When the Barracuda Web Application Firewall is Deployed Behind a Proxy

If the Barracuda Web Application Firewall is deployed behind a proxy server, all requests have their client IP address as the address of the proxy server, which is logged as the **Client IP** on the **BASIC >**

Access Logs page. To log the actual client IP address, specify the header name appended by the proxy server that contains the actual client IP address in the **Header for Client IP Address** field on the **BASIC > Services** page.

Configure the Header Name

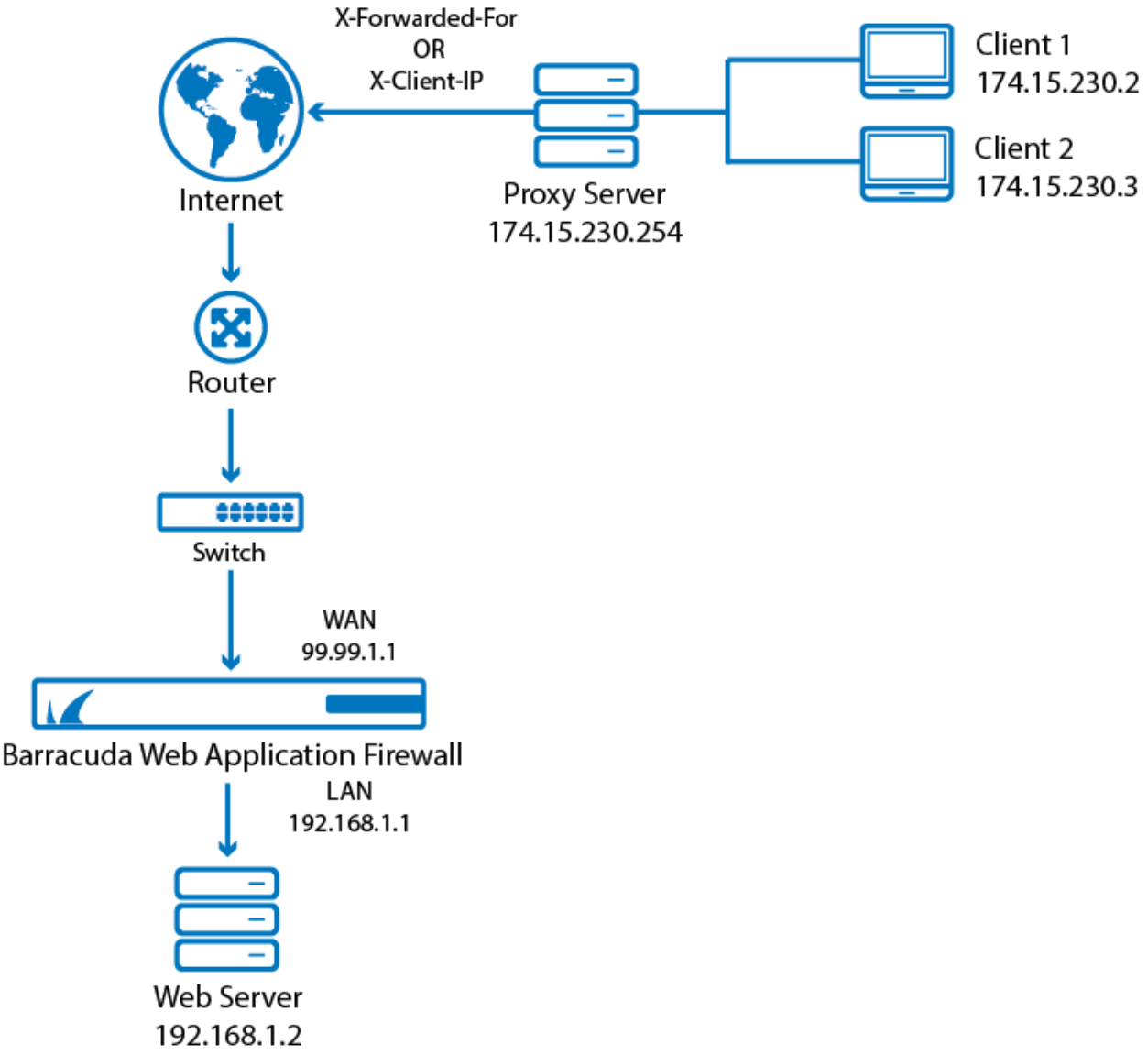
1. Edit the service from the **BASIC > Services** page.
2. Scroll down to the **Basic Security** section and specify the header name in the **Header for Client IP Address** field. The standard headers used to store the actual client IP address are:
    - X-Forwarded-For
    - X-Client-IP
- Specify values for other fields as required and click **Save**. For more information on how to edit a service, see Step 3: Configuring Basic Service Settings.

If the proxy is appending a custom header, specify that header in the **Header for Client IP Address** field.

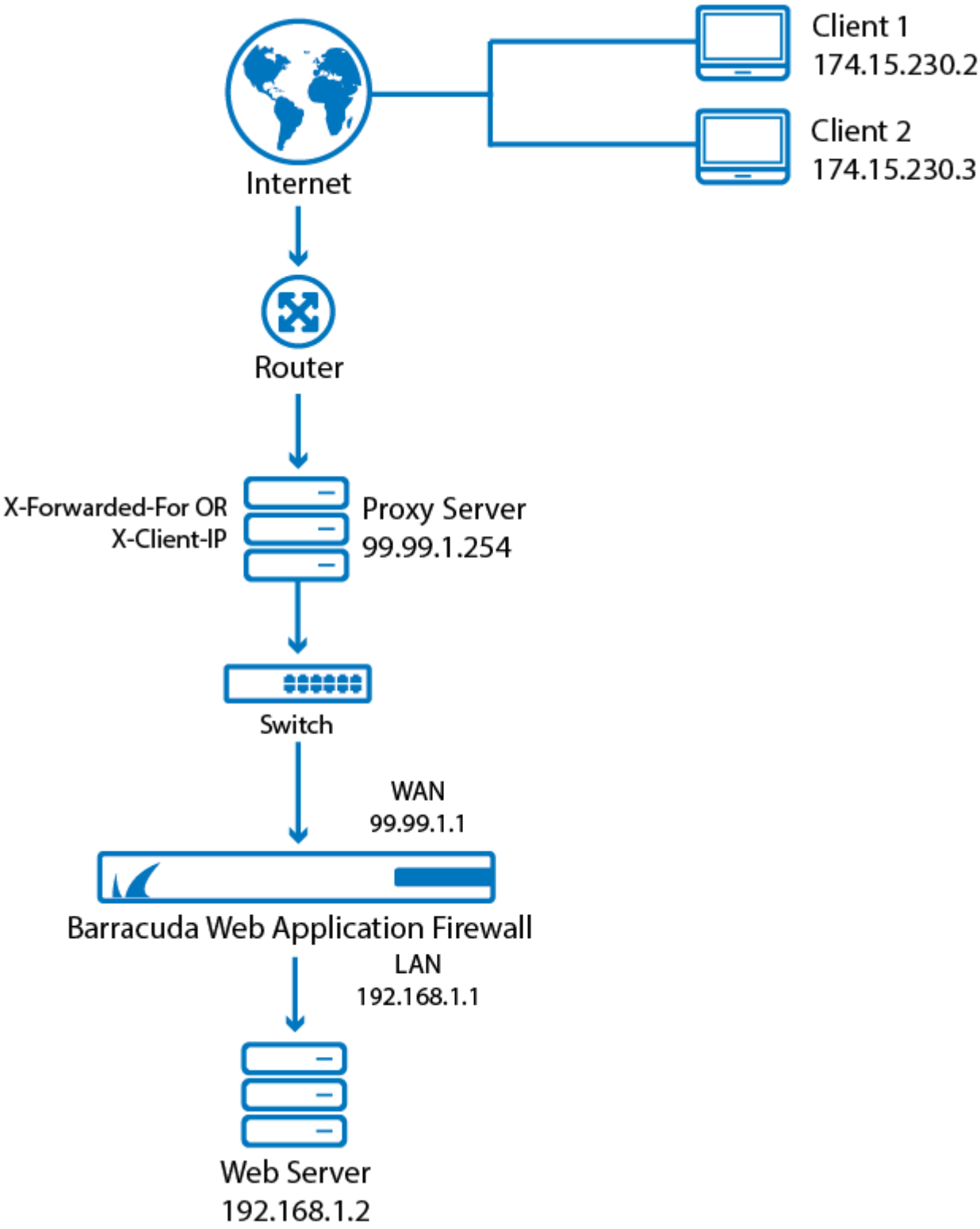
When a request is received, the Barracuda Web Application Firewall gets the actual client IP address from the specified header and displays it in the **Client IP** field of the **Access Logs**.

For example, consider the client IP addresses 174.15.230.2 and 174.15.230.3, and proxy IP address 174.15.230.254. When the client sends a request, the proxy receives the request and stores the IP address of the client in the **X-Forwarded-For** or **X-Client-IP** header, and forwards the request to the Barracuda Web Application Firewall. The Barracuda Web Application Firewall extracts the client IP address from the specified header and displays it in the Access Logs.

Scenario 1:


X-Forwarded-For
OR
X-Client-IP
Client 1
174.15.230.2
Client 2
174.15.230.3
Internet
Proxy Server
174.15.230.254
Router
Switch
WAN
99.99.1.1
Barracuda Web Application Firewall
LAN
192.168.1.1
Web Server
192.168.1.2

Scenario 2:


Client 1
174.15.230.2
Client 2
174.15.230.3
Internet
Router
X-Forwarded-For OR
X-Client-IP
Proxy Server
99.99.1.254
Switch
WAN
99.99.1.1
Barracuda Web Application Firewall
LAN
192.168.1.1
Web Server
192.168.1.2

Figures

1. x_forwarded_for-01.png
2. x_forwarded_for_1-01.png