Barracuda Web Security Service Connector Deployment Configurations

https://campus.barracuda.com/doc/6553637/

The Barracuda Web Security Service Connector can be deployed in an inline or forward proxy deployment configuration. In either case it can be operated in either enforcement mode.

Inline Barracuda Web Security Service Connector Deployment

The Barracuda Web Security Service Connector can be deployed inline with your core network components so all network traffic to the Internet passes through the Barracuda Web Security Service Connector. User and Group policies can be enforced, and application blocking is available. All traffic flowing through your corporate network is subject to configured filtering policies with this configuration. The Barracuda Web Security Service Connector in Service Enforcement mode proxies all requests to the Barracuda Web Security Service after attaching authenticated user information to the request. In Local Enforcement mode, the Barracuda Web Security Service Connector does not proxy any traffic to the Barracuda Web Security Service, but sends only reporting information viewable with the Barracuda Web Security Service Manager. Policies are enforced by the Barracuda Web Security Service Connector locally with policies configured and downloaded from the Barracuda Web Security Service Manager.

> Note that NTLM and Kerberos authentication mechanisms are not available with inline deployment.

Deploying your Barracuda Web Security Service Connector inline also allows automatic pass-through in the event of a system failure, and does not require users to configure web browser proxy settings. Client IP addresses are exposed, allowing enforcement of corporate firewall rules.

Forward Proxy Barracuda Web Security Service Connector Deployment

The forward proxy deployment uses the Barracuda Web Security Service Connector as an intermediary between a client and the Barracuda Web Security Service Manager. In a forward proxy deployment, only HTTP Internet traffic passes through the Barracuda Web Security Service Connector. After the Barracuda Web Security Service Connector authenticates the user, it either attaches user information to the clients' requests and sends them out to the Barracuda Web Security Service Manager, or enforces policies locally in local enforcement mode.

When deployed as a forward proxy, the Barracuda Web Security Service Connector shows all HTTP traffic as coming from its own IP address instead of from the individual client IP addresses as it does

in the inline pass-through deployment. Setting up a Forward Proxy Barracuda Web Security Service Connector does not require interruptions to your network traffic.

You may want to deploy the Barracuda Web Security Service Connector in forward proxy mode if:

- You need to replace an existing forward proxy (such as Microsoft ISA Server) with the Barracuda Web Security Service Connector.
- You do not want the Barracuda Web Security Service Connector to reside inline with all your network traffic and are satisfied with the system only scanning HTTP traffic for viruses and spyware. **Application blocking is not available in this configuration.**
- You want to use either NTLM or Kerberos authentication mechanisms.

When deploying a forward proxy Barracuda Web Security Service Connector, the web browser makes a request to a website through the Barracuda Web Security Service Connector based on its proxy configuration. The Barracuda Web Security Service Connector receives the request, and performs any user identification and group lookup associated with the request. In Service Enforcement mode, the Barracuda Web Security Service Connector passes the request to the Barracuda Web Security Service. In local enforcement mode, the policies are enforced locally by the Barracuda Web Security Service Connector. The appropriate response or web page based on the web rules that you specify is returned to the client.

To implement a Barracuda Web Security Service Connector as a forward proxy, you need to configure your firewall to allow the following accesses:

- Internal clients to the Barracuda Web Security Service Connector on TCP Port 8080
- Barracuda Web Security Service Connector to Active Directory and domain controller on TCP Ports 389, 445
- Barracuda Web Security Service Connector to the Barracuda Web Security Service on TCP Ports 8080
- Web browsers configured to use the Barracuda Web Security Service Connector as their proxy

WCCP Deployment of the Barracuda Web Security Service Connector

Barracuda Web Security Service Connectors can be deployed as Web Cache Control Protocol (WCCP) cache engines on a network with a WCCP capable core routing platform. Because the WCCP control router or switch transparently redirects content requests, end users need not configure browsers to use the Barracuda Web Security Service Connector as an proxy.

In addition to compatibility with other WCCP-capable routers, the Barracuda Web Security Service Connector supports Cisco v1 and v2 routers. Enabling WCCP on your Barracuda Web Security Service

Connector allows you to take full advantage of your WCCP-capable Cisco router's ability to provide for failover and load balancing for multiple Barracuda Web Security Service Connectors connected to the router in a proxy configuration. For large installations requiring high availability and fault tolerance, this is an attractive deployment option.

Considerations when using the WCCP deployment

WCCP allows Cisco routers/switches to forward non-HTTP traffic to web cache servers, but the Barracuda Web Security Service Connector only accepts HTTP traffic (port 80) in this configuration. WCCP also allows multiple Cisco routers to be connected to the same web cache server. The Barracuda Web Security Service Connector does not support this feature and can only be connected to one WCCP router/switch. However, as always, multiple Barracuda Web Security Service Connectors can be connected to a single router/switch.

- Application blocking will not work.
- Outbound spyware will not be blocked.
- HTTPS traffic will not be filtered.

NTLM and Kerberos authentication mechanisms will not work in this deployment configuration, because they both require that the Barracuda Web Security Service Connector be a trusted host in the Windows Domain and that it receive traffic directly from users (as a proxy). In WCCP deployments the Barracuda Web Security Service Connector receives outgoing traffic via the Cisco Router.