

Using Application Control 2.0 with HTTP(S) Proxies

<https://campus.barracuda.com/doc/41115759/>

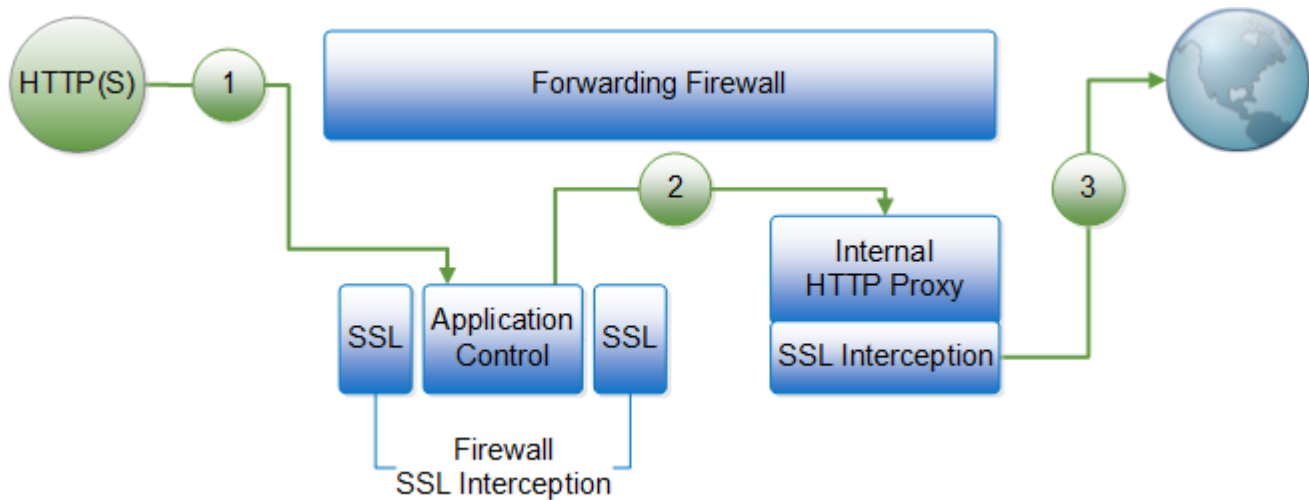
You can use Application Control with the internal HTTP Proxy service and external proxies. Depending on what type of proxy is used, Application Control might be limited or require additional configuration.

Proxy Type	Application Control 2.0	Sub-application Detection	SSL Interception	ATP	Application Based Provider Selection
HTTP Proxy Service (Forward Proxy on ports 3128 and 8080)	Yes (only for HTTP)	No	Yes (via HTTP Proxy service)	Yes	No
HTTP Proxy Service (Transparent Proxy)	Yes	Yes (with a firewall rule for HTTPS)	Yes (with a firewall rule for HTTPS)	Yes	No
External HTTP(S) Proxy	Yes	Yes	Yes	Yes	-
External HTTP + HTTPS Proxies	Yes	Yes	Yes	Yes	-

HTTP Proxy Service (Forward Proxy)

When the client is configured to use the HTTP Proxy service for both HTTP and HTTPS, Application Control 2.0 can be used to detect applications for HTTP connections. Clients contact the HTTP Proxy service directly on port 3128 or 8080 for both HTTP and HTTPS connections. SSL Interception is handled in the HTTP Proxy service

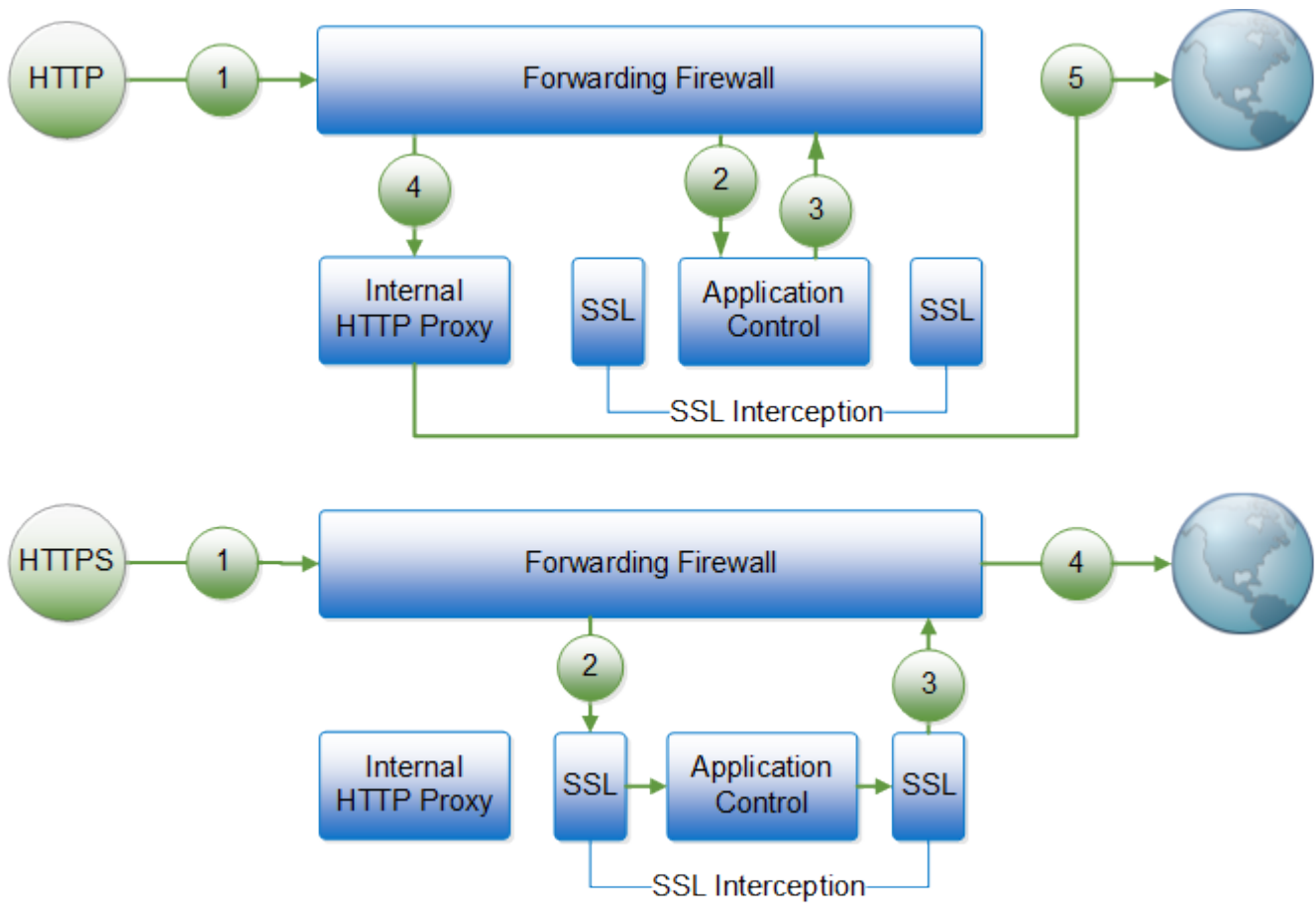
Please note that this setup does not work if you are using a [load balanced HA deployment](#) where the Forwarding Firewall service and the HTTP Proxy service are not on the same virtual server.



HTTP Proxy Service (Transparent Proxy)

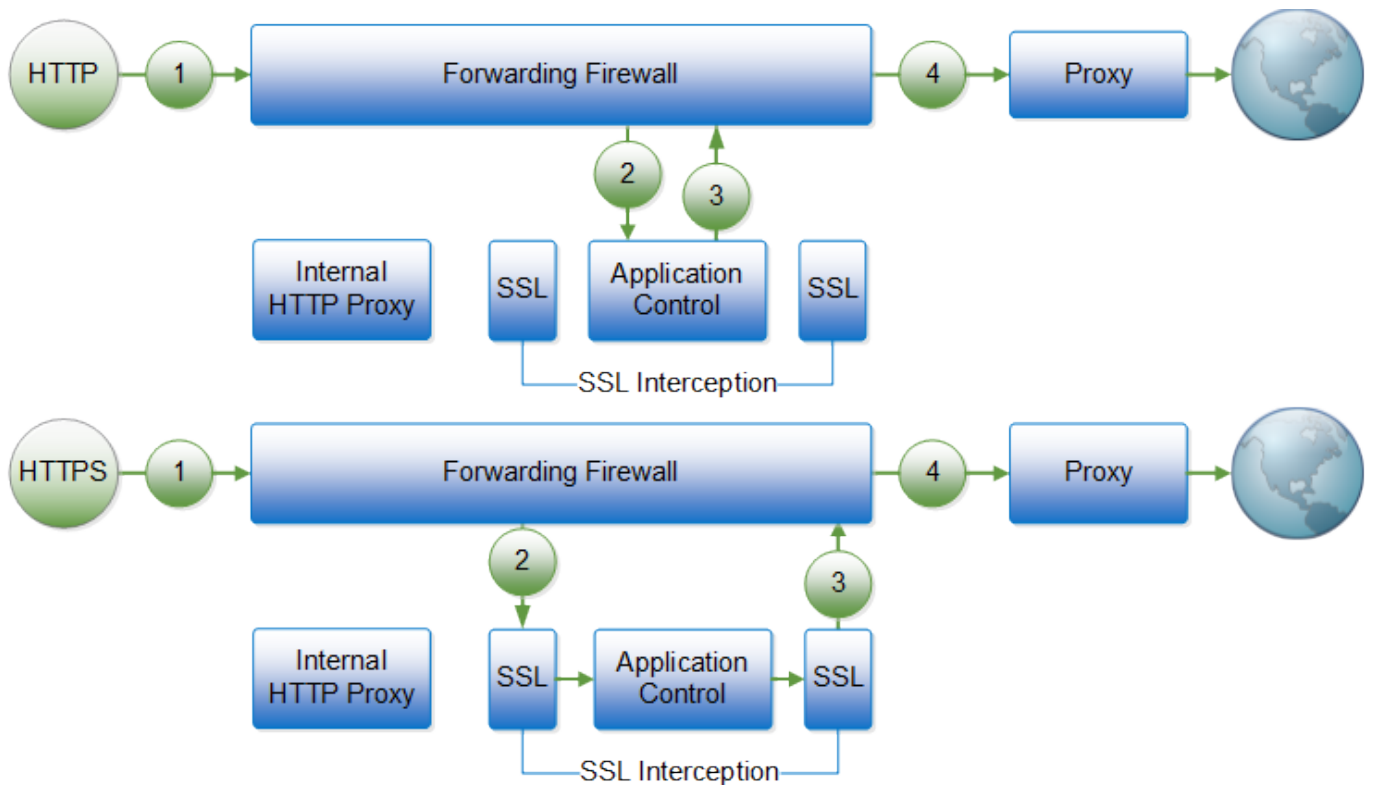
When the HTTP Proxy service on the Barracuda NG Firewall is configured as a transparent proxy, only HTTP traffic is sent to the HTTP proxy. To pass HTTPS traffic through Application Control and SSL Interception, you must configure an explicit firewall rule.

It is not possible to use the built-in SSL Interception in the HTTP proxy in a transparent proxy configuration.



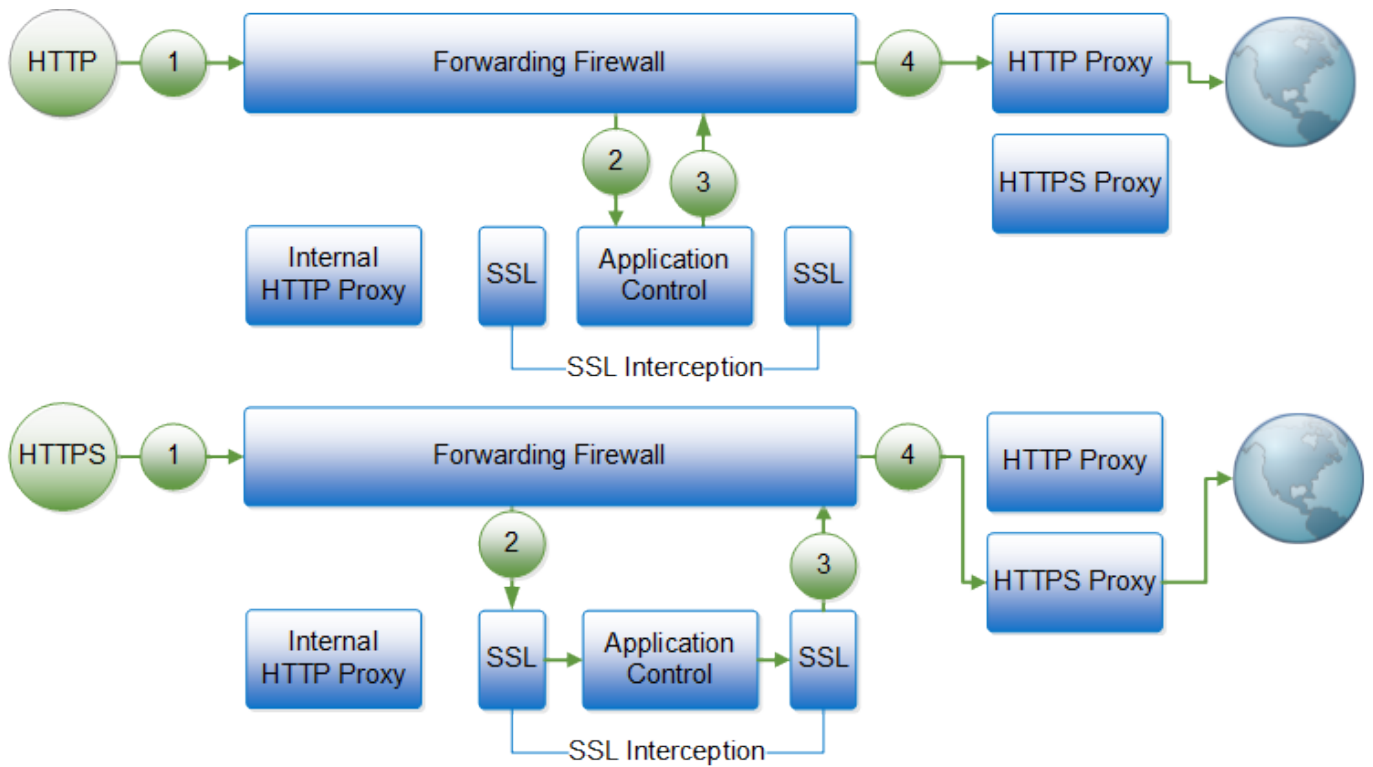
External Proxy

When clients use an external proxy for both HTTP and HTTPS traffic, there are no restrictions. Application Control 2.0 can inspect all traffic coming from or going to the proxy.



Separate HTTP and HTTPS (SSL) Proxies

No limitations apply when clients are configured to use separate external HTTP and HTTPS proxies. Application Control and SSL Interception can inspect all traffic coming from and going to the HTTP and HTTPS proxies.



Figures

1. AppidFWDProxy2.png
2. AppidTranparentProxy2.png
3. AppidExtAllinOnePROXY2.png
4. AppidExtHTTPandSSLProxy2.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.