WCCP Deployment With the Cisco ASA

https://campus.barracuda.com/doc/43221889/

WCCP is a method by which a Cisco Adaptive Security Appliance (ASA) firewall can redirect traffic to a WCCP caching engine through a generic routing encapsulation (GRE) tunnel. In this case, the WCCP caching engine is the Barracuda Web Security Gateway. If you're using a WCCP-enabled router, see WCCP Deployment. This article focuses on configuring the ASA for a WCCP deployment with the Barracuda Web Security Gateway. After configuring your ASA, refer to WCCP Deployment for notes on configuring the Barracuda Web Security Gateway for WCCP. **This deployment is supported by the Barracuda Web Security Gateway 410 and 410 Vx and higher.**

Limitations and Requirements of a WCCP Deployment With an ASA

- The ASA needs to be configured to exempt Barracuda Networks IP ranges from redirection. Specifically, Barracuda Networks subnet **64.235.144.0/20** should be exempted from WCCP redirection. For example, you could configure **access-list wccp-traffic extended deny ip any 64.235.144.0 255.255.240.0** . Check your ASA documentation for correct syntax.
- The only topology that the adaptive security appliance (ASA) supports is when both the client and the cache engine (the Barracuda Web Security Gateway, in this case) are behind the same interface of the ASA and the cache engine can directly communicate with the client without going through the adaptive security appliance.
- You should choose the WCCP Router ID IP address as the highest IP address configured on the ASA. If that IP address happens to be in the DMZ interface, or in the outside interface, that IP address must be routable to the Barracuda Web Security Gateway. In other words, the Barracuda Web Security Gateway has to have a route to get to that Router-ID address pointing to the ASA's interface. See the **WCCP RouterID IP** setting on the **BASIC > IP Configuration** page in the Barracuda Web Security Gateway web interface.
- Due to the Cisco ASA limitations on redirecting DNS responses, the Barracuda Web Security Gateway is not able to log all HTTPS traffic. The only traffic that can be logged is HTTPS traffic that is being inspected and the HTTPS URLs that are blocked.

How WCCP Works With the Barracuda Web Security Gateway and the ASA

- When a client makes a request to a website, the ASA receives the request and redirects it to the Barracuda Web Security Gateway in an encapsulated GRE packet to avoid any modifications to the original packet.
- The Barracuda Web Security Gateway receives the packet, applies policies, and routes the request to the ASA or to the Internet.

How to Configure Your ASA for a WCCP Deployment With the Barracuda Web Security Gateway

1. Configure an access-list containing all Barracuda Web Security Gateways on your network. In this example, there is only one Barracuda Web Security Gateway deployed.
   ```
   ASA(config)#access-list wccp-servers permit ip host <Web Security Gateway IP> any
   ```

2. Create an access-list of the traffic that needs to be re-directed to the Barracuda Web Security Gateway.
   ```
   ASA(config)#access-list wccp-traffic permit ip <Client Network IP> <Client Subnet Mask> any
   ```

3. Enable WCCP on the ASA.
   ```
   ASA(config)#wccp web-cache group-list wccp-servers redirect-list wccp-traffic
   ```

4. Enable WCCP redirection on the inside interface (internal network). The standard service is **web-cache**, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the Barracuda Web Security Gateway.
   ```
   ASA(config)#wccp interface inside web-cache redirect in
   ```

5. Enable WCCP to redirect HTTP traffic to the Barracuda Web Security Gateway using service **web-cache**. Verify with the WCCP router provider (e.g. Cisco) regarding service IDs that are supported.
   ```
   ASA(config)#wccp interface inside service web-cache redirect in
   ```

6. Configure the ASA to redirect HTTPS traffic:
   ```
   ASA(config)#wccp 80 group-list wccp-servers redirect-list wccp-traffic
   ASA(config)#wccp 90 group-list wccp-servers redirect-list wccp-traffic
   ASA(config)#wccp 91 group-list wccp-servers redirect-list wccp-traffic
   ASA(config)#wccp 70 group-list wccp-servers redirect-list wccp-traffic
   ASA(config)#wccp interface inside 80 redirect in
   ASA(config)#wccp interface inside 90 redirect in
   ASA(config)#wccp interface inside 91 redirect in
   ASA(config)#wccp interface inside 70 redirect in
   ```

Enable SSL Inspection on the Barracuda Web Security Gateway version 8 - 10:

- For the Barracuda Web Security Gateway 610 and higher, select *Transparent* for the **SSL Inspection Method** on the **ADVANCED > SSL Inspection** page of the Barracuda Web Security Gateway web interface. See How to Configure SSL Inspection Version 7.1 for details on configuration.

- For the Barracuda Web Security Gateway 410, set **Enable SSL Inspection** to *Yes* on the **BLOCK/ACCEPT > Configuration** page of the Barracuda Web Security Gateway web interface.

Enable SSL Inspection on the Barracuda Web Security Gateway version 11:

- For the Barracuda Web Security Gateway 410 and higher, select *Transparent* for the **SSL Inspection Method** on the **ADVANCED > SSL Inspection** page of the Barracuda Web Security Gateway web interface. See How to Configure SSL Inspection Version 10 and 11 for details on configuration.

Enable SSL Inspection on the Barracuda Web Security Gateway version 12 and higher:

- For the Barracuda Web Security Gateway 410 and higher, set **SSL Inspection** to *ON* the **ADVANCED > SSL Inspection** page of the Barracuda Web Security Gateway web interface. See How to Configure SSL Inspection Version 12 and Above for details on configuration.

Finally, follow instructions in the WCCP Deployment article to configure the Barracuda Web Security Gateway.

Show and Debug Commands

Use these commands to help with configuration and debugging of the deployment.

```
show wccp web-cache

show wccp interface

debug wccp event

debug wccp packets
```