WCCP Deployment

https://campus.barracuda.com/doc/9011807/

For maximum security, Barracuda Networks recommends placing your Barracuda Web Security Gateway behind a corporate firewall.

The Barracuda Web Security Gateway 410 and 410 Vx and above can be deployed as a WCCP cache engine on a network with a WCCP capable core routing platform. Because the WCCP control router or layer 3 switch transparently redirects content requests, you don't need to configure end users' browsers to use the Barracuda Web Security Gateway as an HTTP proxy. Note the two different deployment diagrams for filtering HTTP traffic only versus filtering *both* HTTP and HTTPS traffic. **HTTPS support with this deployment requires running the Barracuda Web Security Gateway 8.1.0.005 or higher.**

In addition to compatibility with other WCCP capable routers, the Barracuda Web Security Gateway supports a Cisco layer 3 switch with at least one VLAN, WCCPv2, GRE encapsulation, and the HASH routing method. Layer 2 masks are *not* supported. Check your Cisco Systems documentation for the recommended router/switch/firewall interface configurations; also see examples below.

Using a Cisco Adaptive Security Appliance (ASA)

This article refers to deployment with a WCCP-enabled router or layer 3 switch. If you are using WCCP with a Cisco Adaptive Security Appliance (ASA), see WCCP Deployment With the Cisco ASA to configure your ASA to work with the Barracuda Web Security Gateway.

Make sure to use the Barracuda Web Security Gateway LAN port to connect to your WCCP enabled router or switch. If you are using the Barracuda Web Security Gateway 1010 or 1011, you must use the LAN1 port.

High Availability and Load Balancing

Enabling WCCP on your Barracuda Web Security Gateway 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 Gateways connected to the router in a proxy configuration. For large installations requiring high availability and fault tolerance, this is an attractive deployment option. Other ways to achieve high availability with or without using WCCP are discussed in High Availability and the Barracuda Web Security Gateway.

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 Gateway only accepts HTTP/HTTPS traffic (port 80/443) in this configuration. WCCP also allows multiple Cisco routers to be connected to the same web cache server. The Barracuda Web Security Gateway does not support this feature and can only be connected to one WCCP router/switch. However, as always, multiple Barracuda Web Security Gateways can be connected to a single router/switch.

Also note the following:

- NTLM and Kerberos authentication mechanisms will not work because they both require that the Barracuda Web Security Gateway 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 Gateway receives outgoing traffic via the Cisco Router.
- Application blocking will not work.
- Outbound spyware will not be blocked.

HTTPS traffic will be also be filtered if (if you are running version 6.0.1 or higher) if **Enable HTTPS Filtering** is set to **Yes** on the **BLOCK/ACCEPT > Configuration** page.To filter HTTPS traffic in this mode, make sure to configure the Cisco WCCP services as follows:

- Enable Service ID 80 for HTTPS
- Enable Service ID 90 for DNS UDP traffic
- Enable Service ID 91 for DNS TCP traffic
- Enable Service ID 0 for web cache

Figure 1 shows deployment with a WCCP router for filtering HTTP traffic only. For filtering HTTP and HTTPS traffic, see Figure 2. See the **BASIC > IP Configuration** page to select and configure WCCP deployment.

Figure 1: WCCP Deployment for filtering HTTP traffic only

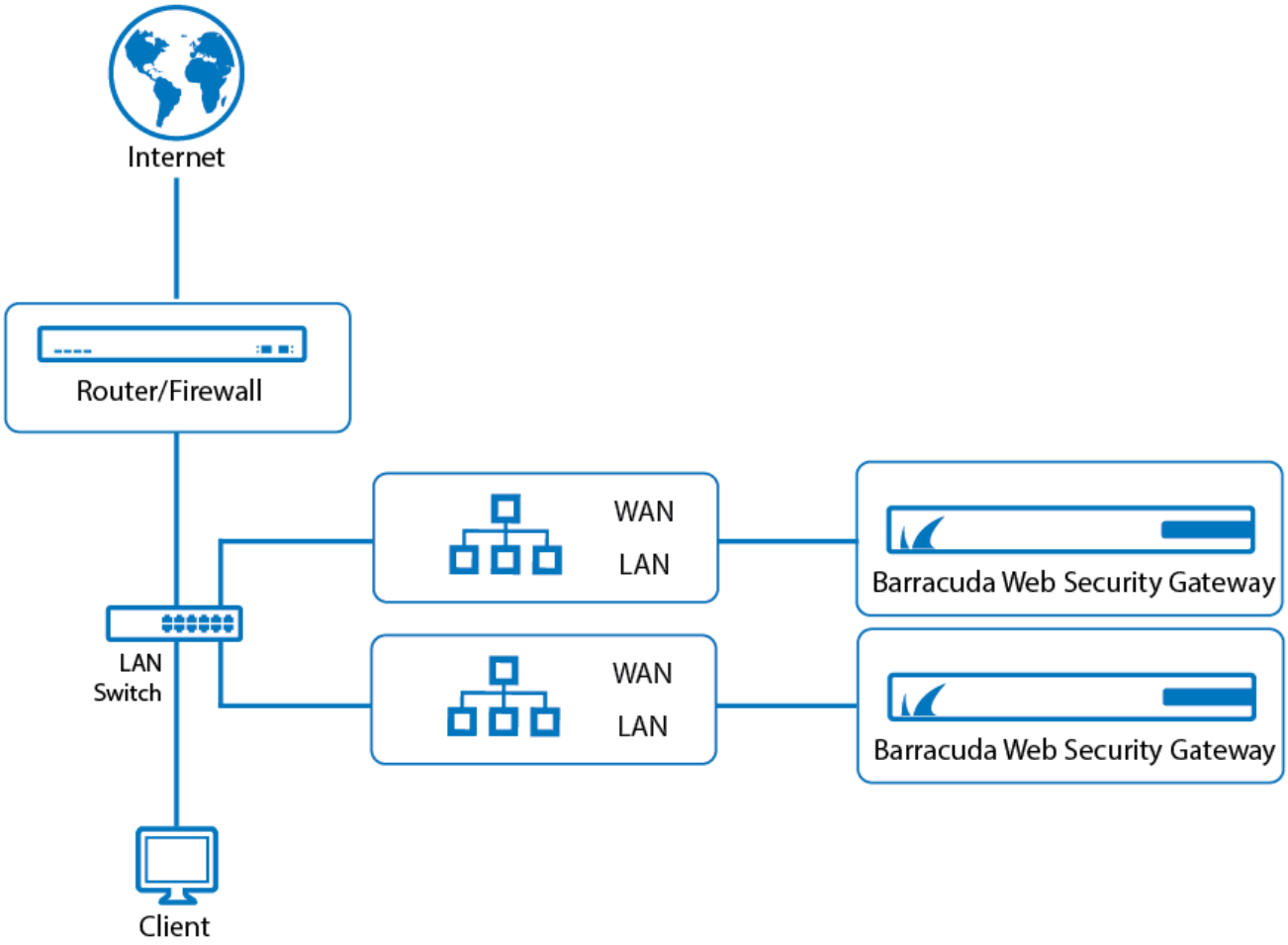


Figure 2 below shows deployment with a WCCP router for filtering both HTTP and HTTPS traffic. In this deployment, the Barracuda Web Security Gateway uses a physically separate gateway to the internet relative to the WCCP router. This configuration is appropriate if your switch does not support VLANs and you want to filter both HTTP and HTTPS traffic with your WCCP router. See the **BASIC > IP Configuration** page to select and configure WCCP deployment.

Figure 2: WCCP Deployment for filtering HTTP and HTTPS traffic with a separate gateway for the Barracuda Web Security Gateway.

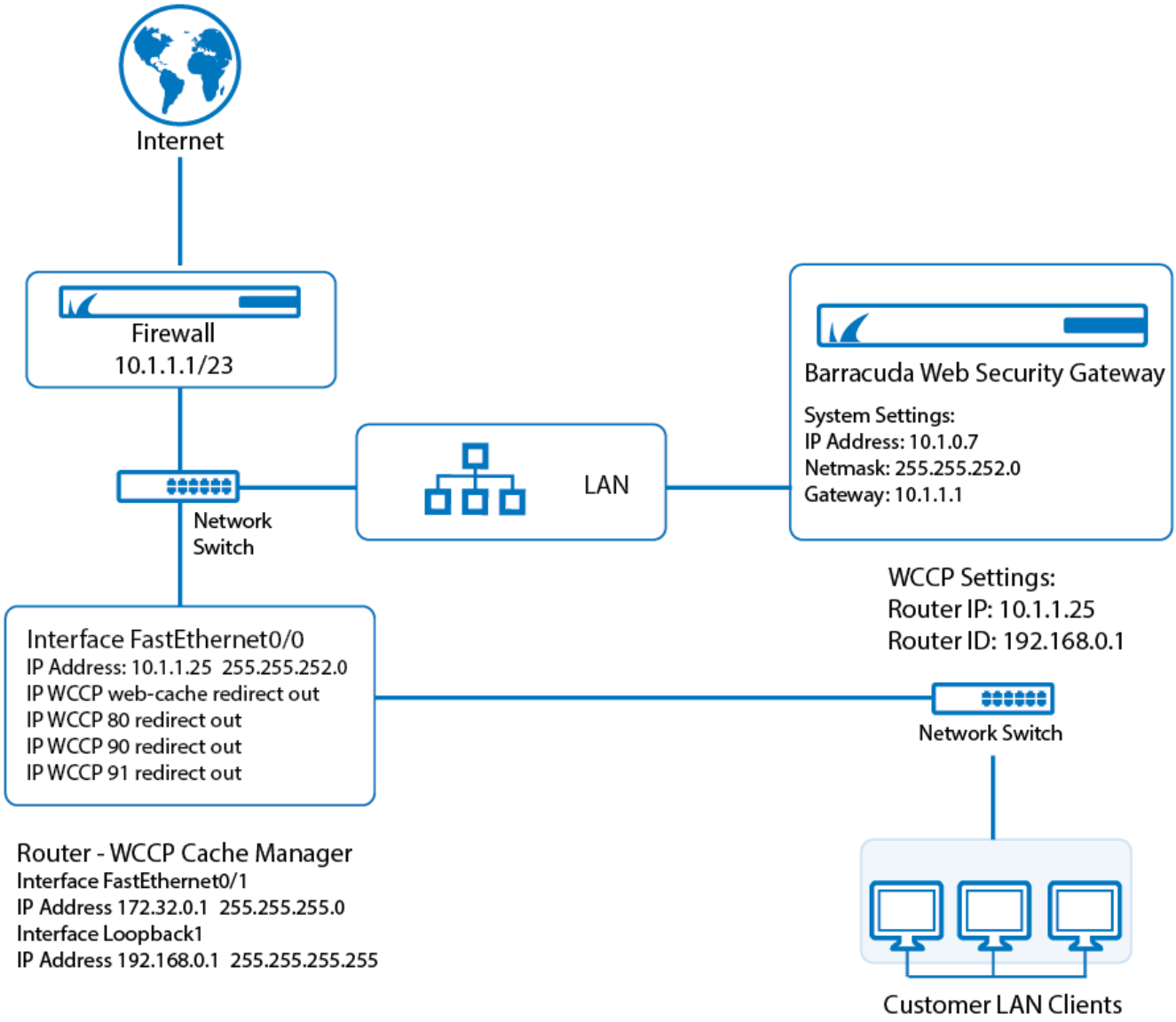
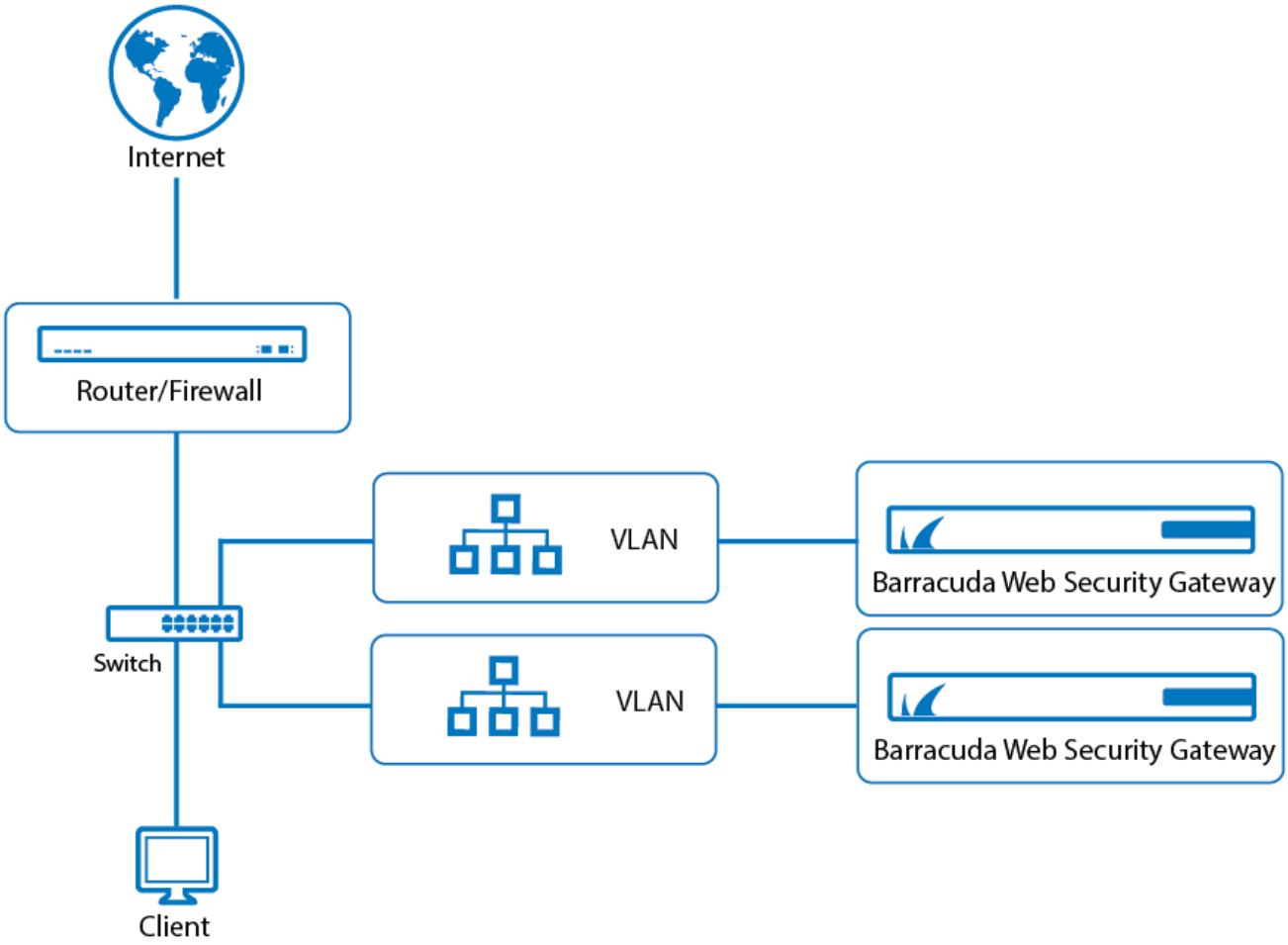


Figure 3 below shows deployment with a WCCP router for filtering both HTTP and HTTPS traffic, and a high availability (HA) deployment of two Barracuda Web Security Gateways. In this deployment, each Barracuda Web Security Gateway connects to your enterprise-class switch via a separate VLAN. This configuration is appropriate if your switch supports VLANs and you want to filter both HTTP and HTTPS traffic with your WCCP router. See the **BASIC > IP Configuration** page to select and configure WCCP deployment. Note that you can filter both HTTP and HTTPS traffic with just one Barracuda Web Security Gateway or with multiple, as shown in this example.

Figure 3: WCCP Deployment for filtering HTTP and HTTPS traffic with the Barracuda Web Security Gateway on a separate VLAN.


Internet
Router/Firewall
VLAN
Barracuda Web Security Gateway
Switch
VLAN
Barracuda Web Security Gateway
Client

Figures

1. WCCP_BWSG.png
2. WCCPWithHTTPS_BWSG.png
3. WCCP VLAN HTTPS_BWSG.png