How to Configure the PKI Service

https://campus.barracuda.com/doc/79463197/

The Barracuda Firewall Control Center Public Key Infrastructure (PKI) uses ITU-T x509 v3 certificates and is similar to the Microsoft PKI that is delivered with Microsoft Windows 2000/2003 servers. A certificate with the V3 basic 'Constraints' extension set to CA:TRUE is handled as a CA. This CA can sign end-user certificates or other CAs. An x.509v3 certificate contains the fully distinguished name and V3 extensions defining the range of application. To mark a certificate as revoked, there are certificate revocation lists. Applications can fetch certificate revocation lists from LDAP or HTTP servers. These servers are specified in the certificate as V3 extension 'crlDistributionPoints'.

The Barracuda CloudGen Firewall supports certificates of the following types:

- SSL/TLS encryption and authentication of TCP-based protocols like HTTP, SMTP, POP, IMAP, and LDAP
- S/MIME encryption and signature of emails
- IPSec, L2TP
- VPN connections

Before You Begin

Before configuring PKI, you must create a PKI service on the Box Layer of the Barracuda Firewall Control Center.

Install and Configure PKI

1. Log into the box layer of the Barracuda Firewall Control Center.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > PKI Service**.
3. Click **Lock**.
4. Edit the following settings according to your requirements:
   - **HA Sync Mode** – Enables or disables synchronization with an optional HA partner.
   - **Log Level** – Specifies the amount of logging. You can select the following options:
     - **Silent** – No logging except for fatal logs.
     - **Normal** – Regular logging.
     - **Verbose** – Regular logging including additional logs (for example, for troubleshooting).
   - **Start LDAP Server** – Starts an LDAP server on the Barracuda Firewall Control Center box. The service listens on the IP addresses defined in the PKI **Service Properties** page. The listening ports are port 389 (LDAP) and port 636 (LDAPs).

- **Log Connections** – Enables connection logging on the internal LDAP server.
- **External LDAP Server** – If you are using an external LDAP server, enter its IP address or DNS-resolvable name.
- **Base DN** – Specifies the Base Distinguished Name for inserting and searching CRLs on the LDAP server, e.g.: `dc=barracuda,dc=com`
- **Root DN** – Specifies the distinguished name of the LDAP user for importing CRLs on the LDAP server.
- **Root Password** – You can change the password for writing on the LDAP server.

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Continue with How to Configure PKI Certificates.