Prepare for the Installation

https://campus.barracuda.com/doc/4259914/

Before installing your Barracuda Web Application Firewall:

- Certain changes might be required to the existing network depending upon the network configuration and the deployment mode you choose. Network changes can be classified as:
  - Hardware changes – Changes related to cabling, switches, routers, network interfaces, etc.
  - Configuration changes – Changes related to DNS databases, IP addresses of hosts and services, router configuration, etc.
- (*Reverse proxy deployment only*) If **Client Impersonation** is set to **Yes** in the **BASIC > Services** page, an additional IP address should be configured on the LAN subnet of the Barracuda Web Application Firewall. This should be the default gateway configured on the back-end real servers.
- Note the server IP address and TCP port of the web applications you want to protect.
- Verify that you have the necessary equipment:
  - Barracuda Web Application Firewall (check that you have received the correct model)
  - AC power cord
  - Ethernet cables
  - Mounting rails (model 660 and higher) and screws
  - VGA monitor (recommended)
  - PS2 keyboard (recommended)

Open Network Address Ranges on Firewall

If your Barracuda Web Application Firewall is located behind a network firewall, allow outbound traffic from the Barracuda WAF to the following Barracuda Networks destinations and the ports mentioned on the network firewall to ensure proper operation:

The following services require outbound connections from all Barracuda Networks appliances.

Hostname	Port	TCP/UDP	Direction	Purpose
updates.cudasvc.com	80,8000,443	TCP	Outbound	Update Infrastructure (Definitions, Firmware, Patches, Provisioning)
cnt12.upd.cudasvc.com	80, 8000	TCP	Outbound	
cnt13.upd.cudasvc.com	80, 8000	TCP	Outbound	
cnt14.upd.cudasvc.com	80, 8000	TCP	Outbound	
cnt15.upd.cudasvc.com	80, 8000	TCP	Outbound	
cnt20.upd.cudasvc.com:80, 8000	80, 8000	TCP	Outbound	
cnt21.upd.cudasvc.com:80, 8000	80, 8000	TCP	Outbound	

auth.svc.fusion.cudasvc.com	80, 443	TCP	Outbound	**Federated Authentication Service -** Used for IP reputation checks and Advanced Bot Protection.
auth.rzc.svc.fusion.cudasvc.com	80,443	TCP	Outbound	
auth.rdn.svc.fusion.cudasvc.com	80,443	TCP	Outbound	
auth.fra.svc.fusion.cudasvc.com	80,443	TCP	Outbound	
api.eucentral1.aws.grip.cudasvc.com	80,443	TCP	Outbound	IP Reputation lookup to GRIP. The Barracuda WAF will use one of these four (4) FQDNs. The FQDN is selected at run time.
api.euwest1.aws.grip.cudasvc.com	80,443	TCP	Outbound	
api.useast1.aws.grip.cudasvc.com	80,443	TCP	Outbound	
api.uswest1.aws.grip.cudasvc.com	80,443	TCP	Outbound	
prod.ap.batic.cudasvc.com	443	TCP	Outbound	Advanced Bot Protection – lookup service endpoint (Required only if ABP subscription is enabled)
batic.barracudanetworks.com	443	TCP	Outbound	Advanced Bot Protection Dashboard access (Required only if ABP subscription is enabled)
brainiac-prod-access-logs-eh-ns-dedicated.servicebus.windows.net brainiac-prod-web-firewall-logs-eh-ns-dedicated.servicebus.windows.net brainiac-prod-system-logs-eh-ns-dedicated.servicebus.windows.net brainiac-prod-ingestion-eh-ns-dedicated.servicebus.windows.net	5671, 5672, 443	TCP	Outbound	Advanced Bot Protection – Ingestion endpoint (Required only if ABP subscription is enabled)
Upstream Barracuda CloudGen Firewall	443	TCP	Outbound	Only required if there is a Barracuda CloudGen Firewall deployed and when the Barracuda Web Application Firewall needs to connect to the firewall to update blocked IPs.
CRL Downloads	Check CRL URL and port	TCP	Outbound	Required if CRL is configured

OCSP Responder URL	Check the OCSP Responder URL and port	TCP	Outbound	Required if OCSP Stapling is configured
acme-v02.api.letsencrypt.org	443	TCP	Outbound	Required if Let's Encrypt service is used to generate certificates
www.google.com	443	TCP	Outbound	Google reCAPTCHA endpoint (For using reCAPTCHA v2 and v3)
ntp.barracudacentral.com	123	UDP	Outbound	Default Barracuda NTP server
backfeed.barracuda.com	443	TCP	Outbound	Backfeed Traffic
airlockstatic.nap.aws.cudaops.com	80, 443	TCP	Outbound	
airlock.nap.aws.cudaops.com	80, 443	TCP	Outbound	
term.cuda-support.com	22, 443, 8788	TCP	Outbound	Support tunnel connection
fttcp.prod.bac.barracudanetworks.com	80, 8000, 23557, 48320	TCP	Outbound	Configuration Backups to the Cloud

- For more information about opening support connections, see How to Open a Support Tunnel.
- For more information about outbound connections, see Required Outbound Connections for Barracuda Networks Appliances.

Apart from this, the Barracuda WAF can optionally connect to services on different ports based on the configuration enabled. A list of such services and commonly used ports is listed below:

Hostname	Port	TCP/UDP	Direction	Purpose
term.cuda-support.com	22 (Primary Port)	TCP	Outbound	Technical Support connections
	443 (Backup Port)			
	8788 (Backup Port)			
	443	TCP	Outbound	Initial VM Provisioning *
	8788	TCP	Outbound	Proxy port for support connections

	25	TCP	Outbound	Email alerts
	53	TCP	Outbound	Domain Name Service (DNS)
ntp.barracudacentral.com	123	UDP	Outbound	Network Time Protocol (NTP) By default, the NTP is set to ntp.barracudacentral.com
	32575	TCP	Inbound/Outbound (between HA peers)	Synchronize configuration between clustered units
	8002	TCP	Inbound/Outbound (between HA peers)	HA communication with Peer unit
	32576	UDP	Inbound/Outbound (between HA peers)	For exchanging cluster heartbeat packets between cluster peers
	42832	TCP	Inbound	Re-provisioning of License (applicable for virtual machine deployments)
* The initial provisioning port can be disabled once the initial provisioning process is complete.				

Required Outbound Connections for Advanced Bot Protection Dashboard Access

The following outbound connections are to be allowed for Advanced Bot Protection Dashboard access:

Hostname	Port	TCP/UDP	Direction	Purpose
tunnel-gateway.cudadps.com (For Tunnel Server)	443	TCP	Outbound	To enable connection between Barracuda Web Application Firewall and ATI dashboard.
manage.cudadps.com (For API's)	443	TCP	Outbound	Back-end API calls used to establish UI connection every time customer opens a dashboard.
manage.ui.cudadps.com (For UI)	443	TCP	Outbound	Front-end URL for ATI dashboard.

Barracuda Advanced Threat Protection (BATP) Servers

The following outbound connections are to be allowed for Advanced Threat Protection:

Hostname	Port	TCP/UDP	Direction	Purpose

api-euwest1-aws.batd.cudasvc.com api-uswest1-aws.batd.cudasvc.com api-apsoutheast1-aws.batd.cudasvc.com api-useast1-aws.batd.cudasvc.com api-eucentral1-aws.batd.cudasvc.com api-apsoutheast2-aws.batd.cudasvc.com api-useast2-aws.batd.cudasvc.com api-apnortheast1-aws.batd.cudasvc.com api-cacentral1-aws.batd.cudasvc.com OR *.batd.cudasvc.com	443	TCP	Outbound	Advanced Threat Protection