Best Practice - Hostname List for Barracuda Online Services

https://campus.barracuda.com/doc/79462714/

Access to hosts and domains in the Barracuda Cloud is required for the proper operation of a Barracuda CloudGen Firewall or Control Center. Ensure that the proper ACLs are in place to allow access to these services:

Servers for determining the Timezone and the Location of a Firewall, Port 443

- geoip.cudasvc.com

Telemetry Information - Different Ports

Telemetry information will be sent to:

- backfeed.barracuda.com:443
- airlockstatic.nap.aws.cudaops.com:80,443
- airlock.nap.aws.cudaops.com:80,443
- 3.18.232.73:80,443

Update Servers - Different Ports

- updates.cudasvc.com:80, 8000, 443
- cnt12.upd.cudasvc.com:80, 8000
- cnt13.upd.cudasvc.com:80, 8000
- cnt14.upd.cudasvc.com:80, 8000
- cnt15.upd.cudasvc.com:80, 8000
- cnt20.upd.cudasvc.com:80, 8000
- cnt21.upd.cudasvc.com:80, 8000

These update servers deliver pattern updates for the following services and features:

- **IPS Patterns** – For more information, see Intrusion Prevention System (IPS).
- **Avira and ClamAV Virus Scanning Patterns** – For more information, see Virus Scanner.
- **Application Control Definitions** – For more information, see Application Control.
- **SSL VPN Templates** – For more information, see SSL VPN.
- **File Content Patterns** – For more information, see File Content Filtering in the Firewall.
- **User Agent Definitions** – For more information, see User Agent Filtering in the Firewall.

- **Geolocation database updates**
- **Spyware and Botnet protection DNS Block List** – For more information, see Botnet and Spyware Protection in the Firewall.

Download Servers - Port 443

- dlportal.barracudanetworks.com
- d.barracudanetworks.com

The download portal hosts all update packages, as well as hotfixes, and the associated tools and utilities used to run the CloudGen Firewall. The firewall queries the download portal for a list of available hotfixes and updates that match the firmware version.

For more information, see DASHBOARD General Page and Updating CloudGen Firewalls and Control Centers.

License Activation

License Activation Server - Port 443

- bcc.barracudanetworks.com
- api.bcc.barracudanetworks.com
- ng-activation.cudasvc.com

Used to send license activation service, and to continuously poll for licenses available for the serial number associated with the firewall or Control Center.

For more information, see How to License a CloudGen Firewall and Licensing CloudGen Firewalls in the Control Center.

License Activation for CloudGen WAN - Port 443

- cloudgenwan-licensing.cudasvc.com

License Activation for IoT-Connect - Port 443

- iotc-licensing.cudasvc.com

Zero Touch Deployment - Port 443

- ztd.barracudanetworks.com

The Control Center queries the list of available Zero Touch-enabled firewalls from this service and pushes the minimal configurations to the cloud service, pending retrieval from firewalls ordered with Zero Touch Deployment.

For more information, see Zero Touch Deployment.

Firewall Authentication Servers - Port 80

- auth.useast1.aws.svc.fusion.cudasvc.com
- auth.eucentral1.aws.svc.fusion.cudasvc.com
- auth.uswest1.aws.svc.fusion.cudasvc.com
- auth.euwest1.aws.svc.fusion.cudasvc.com
- auth.svc.fusion.cudasvc.com
- auth.fra.svc.fusion.cudasvc.com
- auth.rdn.svc.fusion.cudasvc.com
- auth.rzc.svc.fusion.cudasvc.com OR auth.*.svc.fuction.cudasvc.com

ATP Servers - Multiple Ports

Port 443

- 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

Barracuda ATP cloud services. If ATP is enabled, the firewall uploads files to be scanned via ATP to these services.

Port 60080

In case you have ATP activated, the firewall also uses port 60080 to detect requests for asynchronous ATP downloads.

The reachability of port 60080 will be treated in a special way by the firewall and does not pose a security hole.

Depending on the firmware version, port 60080 must be treated differently:

- On older firmware versions: In case ATP is activated, the firewall uses port 60080 to detect requests for asynchronous ATP downloads. This will not pose a security hole.
- For freshly installed firmware versions higher than or equal to 8.0.5 OR higher than or equal to 8.2.0: By default, port 60080 is no longer used by the ATP "Scan First, then Deliver" mechanism and is no longer open, even if ATP is activated.

For more information on ATP, see Advanced Threat Protection (ATP).

URL Categorization Servers - Port 443

- api.useast1.aws.wcs.cudasvc.com
- api.apsoutheast2.aws.wcs.cudasvc.com
- api.euwest1.aws.wcs.cudasvc.com
- api.uswest1.aws.wcs.cudasvc.com
- api.eucentral1.aws.wcs.cudasvc.com
- api.apnortheast1.aws.wcs.cudasvc.com OR *.wcs.cudasvc.com

Barracuda online URL categorization services used by the Barracuda URL Filter in the firewall.

For more information, see URL Filtering in the Firewall.

DNS Block List - Port 443

- b.barracudacentral.org

If the DNS block listing is configured, the firewall checks the hostnames in the DNS queries against this online service.

For more information, see Botnet and Spyware Protection in the Firewall.

Link Protection - Port 443

- linkprotect.useast1.aws.cudaops.com
- linkprotect.eucentral1.aws.cudaops.com
- linkprotect.uswest1.aws.cudaops.com
- linkprotect.euwest1.aws.cudaops.com
- linkprotect.apsoutheast2.aws.cudaops.com
- linkprotect.apnortheast1.aws.cudaops.com
- linkprotect.cudasvc.com

If the Mail Security in the Firewall and Link Protection is configured, the firewall checks the hostnames in the DNS queries against this online service.

For more information, see How to Configure Link Protection for Mail Security in the Firewall.

CloudGen WAN - Port 443

- cloudgenwan-configuration.cudasvc.com
- cloudgenwan-status.cudasvc.com

AWS / Azure and Google Cloud APIs

Firewalls and Control Centers deployed to the public cloud use API calls for Cloud Integration features.

For more information, see Public Cloud.

Public Cloud Data Center Network Objects

- https://www.microsoft.com/en-us/download/confirmation.aspx?id=41653
- https://ip-ranges.amazonaws.com/ip-ranges.json

To fill network objects with up-to-date IP ranges used by Azure and AWS data centers, the firewall queries these two services.

For more information, see How to Configure Network Objects for AWS and Azure Datacenter Networks.

© Barracuda Networks Inc., 2024 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.