

How to Block UDP Port 443 on CloudGen Firewalls

<https://campus.barracuda.com/doc/104366520/>

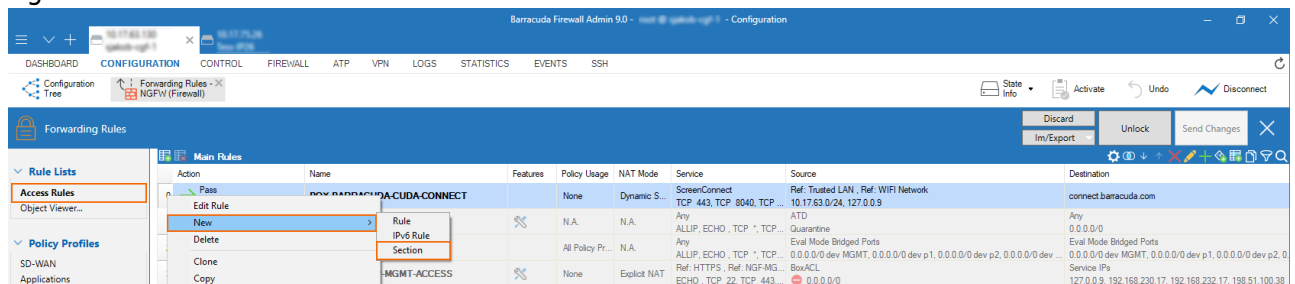
On the Barracuda CloudGen Firewall, rule **BOX-BLOCK-UDP443** blocks UDP port 443 (QUIC) per default in order to force browsers to use TCP. However, this does not apply for units connected to SecureEdge over pvpn84. For security inspection to work on connected SecureEdge Access clients, traffic must be blocked by a manually created rule in order to force SecureEdge Access client browsers to use TCP instead of QUIC on UDP port 443.

Block QUIC for Browsers

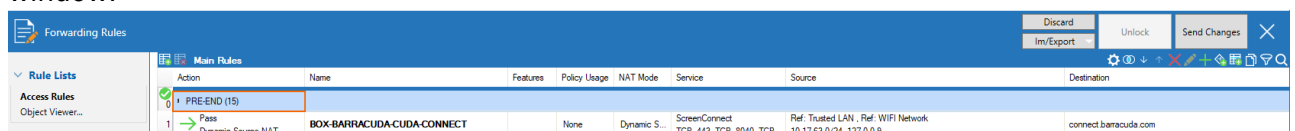
Create a DENY rule on the Barracuda CloudGen Firewall and place it on top of the cloud-maintained/autogenerated rules.

Step 1. Create a Rule Section

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the **Access Rules** window, either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Section**.



4. As the **Name** for the section, enter **PRE-END**. The section should be shown on top of the rules window.



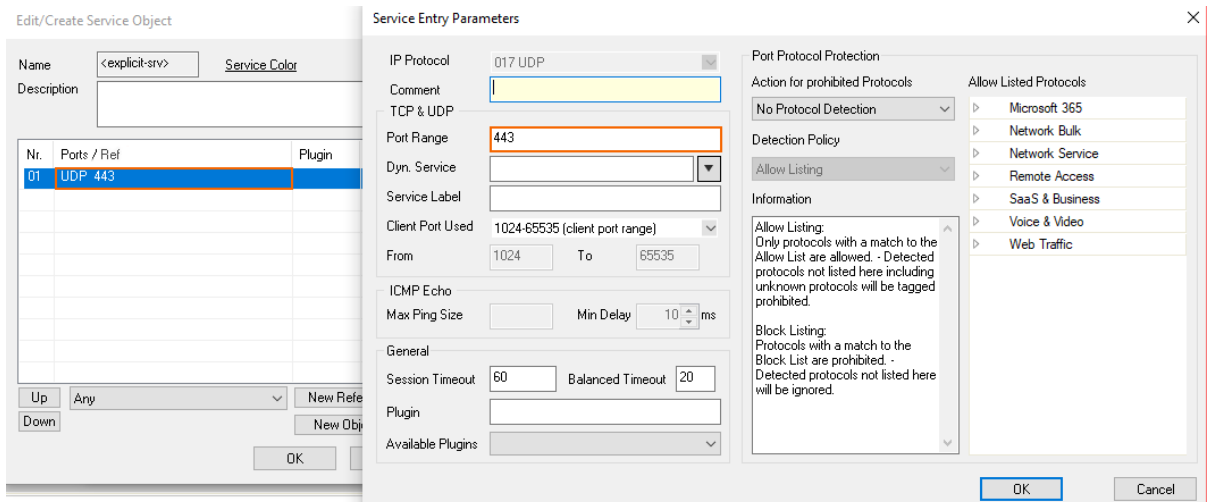
Step 2. Create a Rule to Block UDP Port 443

On top of the new section, create an access rule to block UDP port 443

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and

select **New > Rule**.

4. Select **Deny** as the action.
5. Enter a **Name** for the rule, e.g.: MY-RAC-ZTNA-BLOCK-UDP-443
6. Specify the following settings to match your web traffic:
 - **Source** – Select **<explicit>** and chose the service object for pvpn84.
 - **Service** – Select **<explicit>** and create or select the service object for UDP 443.



The screenshot displays two overlapping configuration windows in the Barracuda SecureEdge interface.

The background window is titled "Edit/Create Service Object". It has a "Name" field with the value "<explicit-srv>" and a "Description" field. Below these is a table with columns "Nr.", "Ports / Ref", and "Plugin". The first row is highlighted with a blue selection bar and contains the text "01 UDP 443". At the bottom of this window are buttons for "Up", "Down", "Any", "New Ref", "New Obj", and "OK".

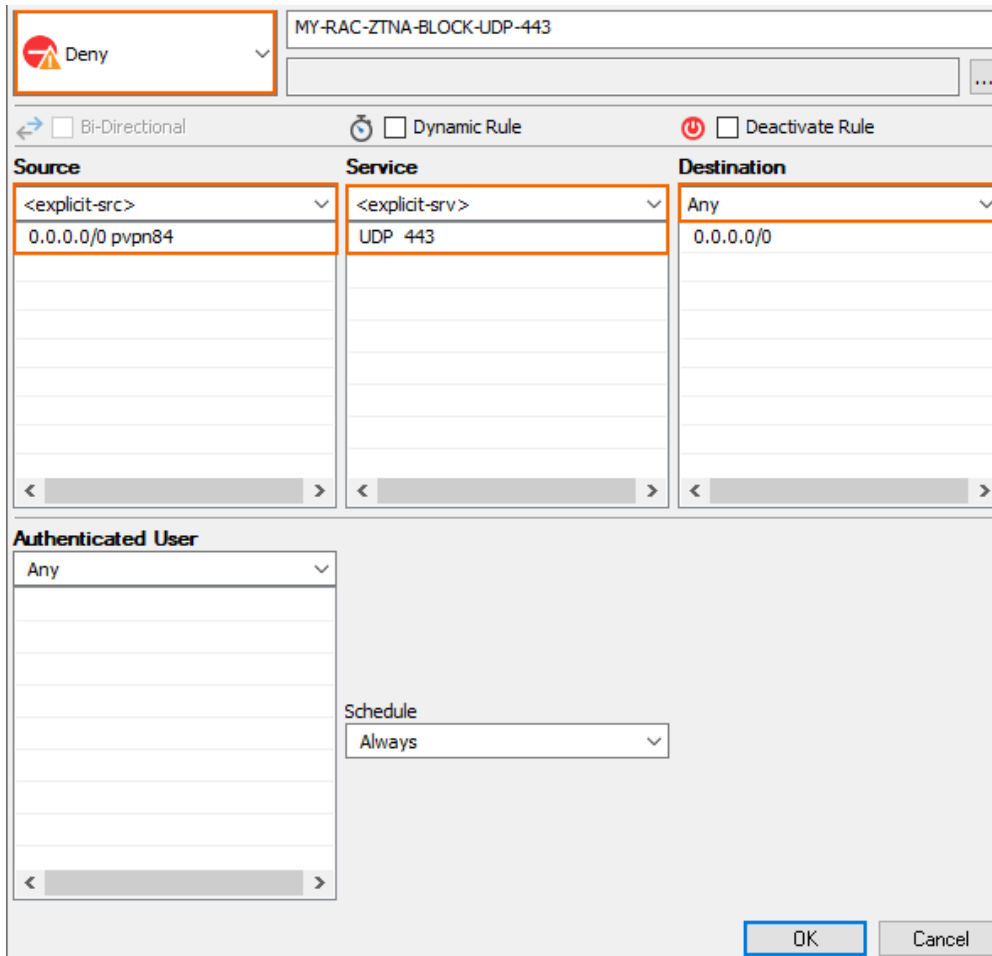
The foreground window is titled "Service Entry Parameters". It contains several configuration sections:

- IP Protocol:** A dropdown menu set to "017 UDP".
- Comment:** An empty text field.
- TCP & UDP:** A section containing a "Port Range" field set to "443".
- Dyn. Service:** A dropdown menu.
- Service Label:** An empty text field.
- Client Port Used:** A dropdown menu set to "1024-65535 (client port range)".
- From:** Two input fields for "From" (1024) and "To" (65535).
- ICMP Echo:** A section with "Max Ping Size" and "Min Delay" (10 ms) fields.
- General:** A section with "Session Timeout" (60) and "Balanced Timeout" (20) fields.
- Plugin:** An empty text field.
- Available Plugins:** A dropdown menu.
- Port Protocol Protection:** A section with "Action for prohibited Protocols" (No Protocol Detection), "Detection Policy" (Allow Listing), and "Information" (Allow Listing: Only protocols with a match to the Allow List are allowed. - Detected protocols not listed here including unknown protocols will be tagged prohibited. Block Listing: Protocols with a match to the Block List are prohibited. - Detected protocols not listed here will be ignored).
- Allow Listed Protocols:** A list of protocols with expandable arrows: Microsoft 365, Network Bulk, Network Service, Remote Access, SaaS & Business, Voice & Video, and Web Traffic.

At the bottom right of the "Service Entry Parameters" window are "OK" and "Cancel" buttons.

For more information, see [How to Create Service Objects](#) in the CloudGen Firewall documentation.

- **Destination** – Select **Any**.



MY-RAC-ZTNA-BLOCK-UDP-443

☐ Deny

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

| Source | Service | Destination |
|------------------------------------|---------------------------|------------------|
| <explicit-src> 0.0.0.0/0 pvpn84 | <explicit-srv> UDP 443 | Any 0.0.0.0/0 |

Authenticated User: Any

Schedule: Always

OK Cancel

7. Click **OK**.
8. Make sure that the access rule is placed above the section PRE - END created in Step 1.
9. Click **Send Changes** and **Activate**.

The rule is now displayed in the list, and all SecureEdge Access client browsers are forced to use TCP instead of QUIC on UDP port 443.

Forwarding Rules

Rule Lists

Access Rules

Object Viewer...

Policy Profiles

SD-WAN

Applications

URL Filtering

Malware Protection

TLS Inspection

IPS

File Content

User Agent

Firewall Objects

Networks

Named Networks

Applications

URL Filter

TLS Inspection

Services

User and Groups

Connections

Schedules

Interface Groups

Proxy ARPs

Rule List Verification

Main Rules

| Action | Name | Features | Policy Usage | NAT Mode | Service | Source | Destination |
|-------------------------------|----------------------------|----------|------------------|--------------|---|---|---|
| <div><div>Deny</div></div> | MY-RAC-ZTNA-BLOCK-UDP-443 | | N.A. | N.A. | UDP 443 | 0.0.0.0/0 vpn84 0.0.0.0/0 dev vpn84 | Any 0.0.0.0/0 |
| PRE-END (15) | | | | | | | |
| <div><div>Pass</div></div> | BOX-BARRACUDA-CUDA-CONNECT | | None | Dynamic S... | ScreenConnect TCP 443, TCP 8040, TCP ... | Ref: Trusted LAN , Ref: WIFI Network 10.17.63.0/24, 127.0.0.9 | connect.barracuda.com |
| <div><div>Block</div></div> | BlockATDQuarantine | | N.A. | N.A. | Any | ATD Quarantine | Any 0.0.0.0/0 |
| <div><div>Pass</div></div> | BOX-EVAL-MODE-BRIDGE | | All Policy Pr... | N.A. | Any | Eval Mode Bridged Ports | Eval Mode Bridged Ports |
| <div><div>Det NAT</div></div> | BOX-SERVICEIP-MGMT-ACCESS | | None | Explicit NAT | Ref: HTTPS , Ref: NGF-MG... ECHO , TCP 22, TCP 443 | 0.0.0.0/0 dev MGMT, 0.0.0.0/0 dev p1, 0.0.0.0/0 dev p2, 0.0.0.0/0 dev ... BoxACL | 0.0.0.0/0 dev p1, 0.0.0.0/0 dev p2, 0.0.0.0/0 dev p1, |

Figures

1. 05_CGF_PoE_manual_add_new_sec.png
2. 06_CGF_PoE_manual_name_section_PR-END.png
3. 07_CGF_PoE_manual_MY-RAC-ZTNA-BLOCK-UDP-443_object.png
4. 07_CGF_PoE_manual_MY-RAC-ZTNA-BLOCK-UDP-443.png
5. 07_CGF_PoE_manual_MY-RAC-ZTNA-BLOCK-UDP-443_over_PR-END_section.png

© 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.