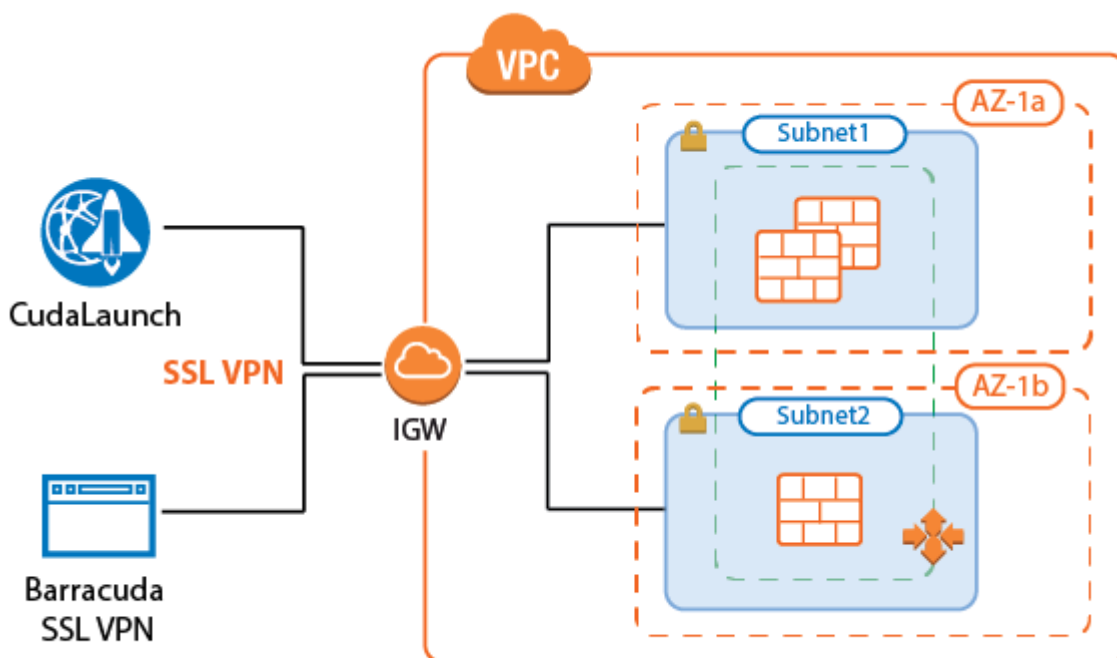


How to Configure the SSL VPN Services for AWS Auto Scaling Clusters

<https://campus.barracuda.com/doc/70584567/>

Let your users connect to a network in an AWS Auto Scaling cluster using SSL VPN. Enable the SSL VPN service and CudaLaunch, create a group access policy, and configure the login and authentication settings for the SSL VPN connections. To use SSL VPN, you must upload a certificate to the AWS certificate manager. For CudaLaunch on iOS, NextGen Firewall Auto Scaling Clusters are supported for CudaLaunch 2.3.0 or higher.



Before You Begin

- Configure an external authentication server or NGF local authentication. For more information, see [Authentication](#).

Step 1. Disable Port 443 for Site-to-Site and Client-to-Site VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN > VPN Settings**.
2. Click **Lock**.

- Click the **Click here for Server Settings** link. The **Server Settings** window opens.
- Set **Use Port 443** to **No**.

Server Configuration

Use port 443	No
CRL Poll Time (min)	0
Global TOS Copy	Off
Global Replay Window Size, Packets(0...Use Default)	

- Click **OK**.
- Click **Send Changes** and **Activate**.

Step 2. Configure SSL VPN General Service Settings

Enable the SSL VPN service and add the listening IP addresses.

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.
- Click **Lock**.
- Set **Enable SSL VPN** to **Yes**.
- (optional) Set **Enable CudaLaunch** to **yes**.
- Click **+** to add a **Listen IP**.
- Enter the IP address of the VPN service. E.g., 127.0.0.9

General Service Settings

Enable SSL VPN

Enable CudaLaunch

Listen IPs






Restrict to Strong Ciphers Only

Allow SSLv3

- (recommended) Enable **Restrict to Strong Ciphers Only**.
- Select the **Identification Type**:
 - Generated-Certificate** - The certificate and the private key is automatically created by the firewall.
 - Self-Signed-Certificate** - Click **New** to create a **Self-Signed Private Key** and then **Edit** to create the **Self-Signed Certificate**.

- **External-Certificate** – Click **Ex/Import** to import the CA-signed **External Certificate** and the **External-Signed Private Key**.

Service Identification

Identification Type	Generated-Certificate		
Self-Signed Private Key	New Key...	Ex/Import ▾	No key present 
Self-Signed Certificate	Show ▾	Edit...	No certificate present 
External-Signed Private Key	New Key...	Ex/Import ▾	No key present 
External-Signed Certificate	Show...	Ex/Import ▾	No certificate present 

9. Click **Send Changes** and **Activate**.

Step 3. Configure User Identity Access Control Policy

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Service > VPN-Service > SSL-VPN**.
2. In the left menu, click **Access Control Policies**.
3. Click **Lock**.
4. Click **+** to add an **Access Control Policy**.
5. Enter the **Name** for the access control policy.
6. Click **OK**.
7. In the **Access Control Policy** section, select the **Active** check box.

Access Control Policy

Active 

8. In the **Group Access** section, click **+** to add **Allowed Groups** and **Blocked Groups**. Click **x** to remove the entry from the table.

In **Allowed Groups**, either add an asterisk (*) to allow all groups, or enter one or more group names. Leaving the **Allowed Groups** empty causes the **Access Control Policy** to block all authentication attempts.

9. In the **Authentication** section, click **+** to add an **Authentication Scheme**.

Authentication


Authentication Schemes

Authentication Scheme

10. Select **Use Identity** from the **Authentication Scheme** drop-down list.

Authentication Options

Authentication Scheme Other 

11. Click **OK**.
12. Click **Send Changes** and **Activate**.

Step 4. Configure Login to Log In with User Identity

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, click **Login**.
3. Click **Lock**.
4. In the **Login** section, set the **Identity Scheme** to your preferred authentication method, e.g., **MS-Active Directory**.
5. Click **+** to add your access control policy to the list of **Access Control Policies**.

Login

Identity Scheme Other 


Access Control Policies   


6. From the pop-up menu, select the access control policy that you configured in Step 3 for **Use Identity**, i.e., ACCE01.


ACCE01
Default

7. Configure the following settings:
 - **Use Max Concurrent Users** - Set to **no**.
 - **Session Timeout (m)** - Set to 30. This setting must match with the timeout on the ELB.

Configuration

Use Max. Concurrent Users 

Max. Concurrent Users 

Session Timeout [m] 

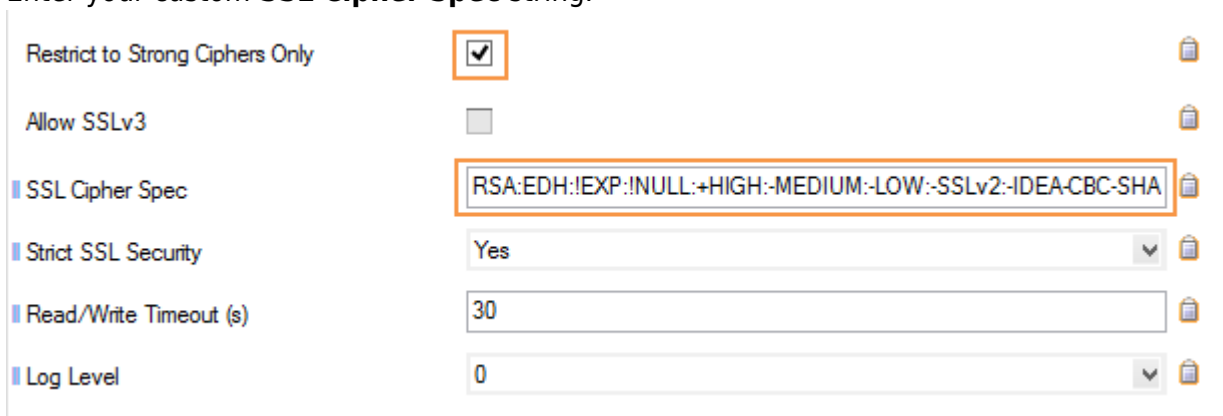
Deny Remember Me 







8. (optional) Customize the login messages and logos:
 - Import a 200 x 66-pixel PNG or JPG image to customize the **Logo**.
 - Enter a plain text **Login Message**. E.g., Welcome to the Barracuda NextGen Firewall SSL VPN.
 - Enter an HTML **Help Text**.
9. Click **Send Changes** and **Activate**.

Step 5. (optional) Use Custom Cipher String

Configure a custom cipher string to be used by the SSL VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, click **Basic Setup**.
3. Click **Lock**.
4. In the left menu, expand **Configuration Mode** and click on **Switch to Advanced View**.
5. Disable **Allow SSLv3**.
6. Enable **Restrict to Strong Ciphers Only**.
7. Enter your custom **SSL Cipher Spec** string.



Restrict to Strong Ciphers Only	<input checked="" type="checkbox"/>	
Allow SSLv3	<input type="checkbox"/>	
SSL Cipher Spec	<input type="text" value="RSA:EDH:!EXP:!NULL:+HIGH:-MEDIUM:-LOW:-SSLv2:-IDEA-CBC-SHA"/>	
Strict SSL Security	<input type="text" value="Yes"/>	
Read/Write Timeout (s)	<input type="text" value="30"/>	
Log Level	<input type="text" value="0"/>	

8. Set **Strict SSL Security** to **yes**.
This setting might break access for some older client SSL implementation. Disable if you experience problems when using older browsers.
9. Click **Send Changes** and **Activate**.

Step 5. Create Access Rules

Verify the the access rule CLOUD-SERVICE-VPN-ACCESS is present in the forwarding ruleset. If not, create the rule. Use the following settings:

- **Action** – Select **App Redirect**.
- **Source** – Select **Any**.
- **Service** – Select **NGF-VPN-HTTPS**.
- **Destination** – Select the network object containing all firewall IPs.
- **Redirection** – Enter the IP address of the VPN service. E.g., 127.0.0.9.

Edit Rule: CLOUD-SERVICE-VPN-ACCESS [Rule] ✕

Views ⬆

- Rule
- Advanced
- ICMP Handling

Object Viewer ⬆

Object Viewer

↻ App Redirect

CLOUD-SERVICE-VPN-ACCESS

UDP 691 and TCP 443 to the VPN service listening on the virtual server IP address. ⋮

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source	Service	Destination
Any 0.0.0.0/0	NGF-VPN-HTTPS Ref: HTTPS Ref: NGF-VPN	All Firewall IPs Ref: Management IP Ref: Service IPs <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Redirection Local Address 127.0.0.9 </div>

Authenticated User

Any

Policies

IPS Policy: Default Policy

Application Policy: No AppControl

Schedule: Always

QoS Band (Fwd): VoIP (ID 2)

QoS Band (Reply): Like-Fwd

OK Cancel

Troubleshooting

- If the **sslvpn** log contains the following line: `http_listener: failed to listen on @443` verify that no other service on the firewall is running on that port and that no Dst NAT access rules are forwarding TCP port 443 (HTTPS) traffic.
- Updating certificates requires the SSL VPN service to be restarted. To do this in an ASG, scale the ASG to a size of one. Then restart the VPN (SSL VPN) service. Then scale out, or wait for the scaling policies to scale your ASG out to the desired size.

Figures

1. aws_autoscale_cluster_sslvpn.png
2. disable_s2s_443.png
3. sslvpn01.png
4. sslvpn02.png
5. activate_auth_scheme_00.png
6. add_authentication_scheme_00.png
7. add_auth_scheme_user_identity_00.png
8. add_access_control_policy_00.png
9. select_access_control_policy_00.png
10. login_conf.png
11. strong_ciphers_00.png
12. ssl_vpn_rule.png

© Barracuda Networks Inc., 2019 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.