

How to Create a Secure Connector Site Configuration in Barracuda CloudGen WAN

<https://campus.barracuda.com/doc/97520370/>

The [Barracuda Secure Connector](#) is a hardware device that allows administrators to connect remote appliances and micro-networks to the corporate data center via VPN. The Secure Connector is available for both the Barracuda CloudGen Firewall and Barracuda CloudGen WAN. Note, however, that as soon as you associate it with one of them, you will no longer be able to associate it with the other one.

To integrate a Secure Connector device in your Barracuda CloudGen WAN deployment, you must create a site configuration with the basic settings for each CloudGen WAN appliance. If your appliance has already been ordered and installed on site, it will wait for the site configuration and apply the configuration as soon as it is available. If, however, the appliance is not yet installed, it will apply the configuration as soon as it is connected to the Internet.

Due to the method of UDP fragmentation in Microsoft Azure, Windows and Linux clients based behind a Secure Connector that is attached to an Azure gateway must use an MTU of 1300.

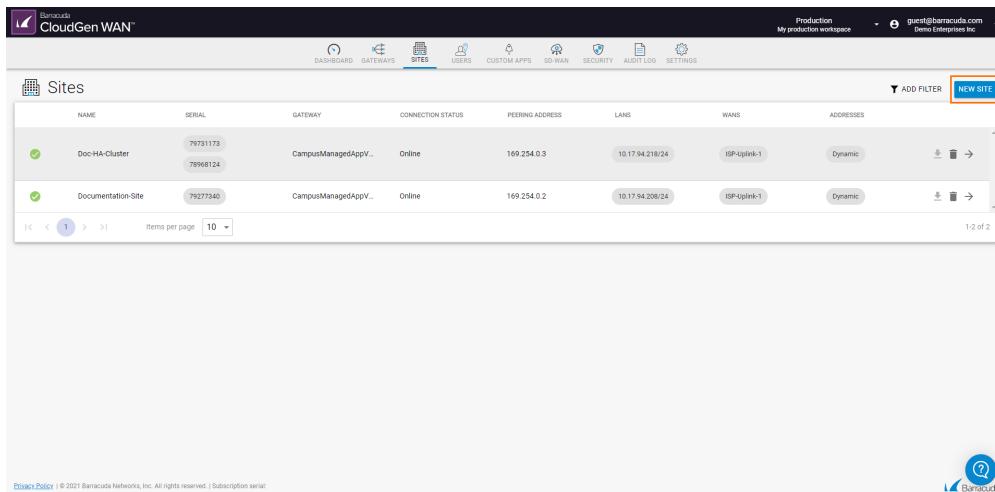
Before You Begin

- Create a Virtual WAN in Microsoft Azure. For more information, see [How to Create a Microsoft Azure Virtual WAN](#).
- Create a Barracuda CloudGen WAN gateway. For more information, see [How to Create a Barracuda CloudGen WAN Gateway in Microsoft Azure](#).

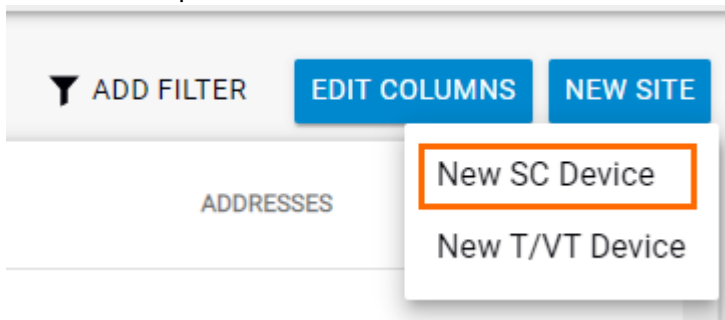
The Barracuda Secure Connector sends all traffic to the Azure gateway. If you want to apply an access control list (ACL) to the Secure Connector, you must use a Gateway ACL. For more information, see [Gateway ACL](#).

Step 1. Create the Site Configuration

1. Go to <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Click **SITES**.
3. The **SITE** page opens. To create a new site configuration, click **NEW SITE**.

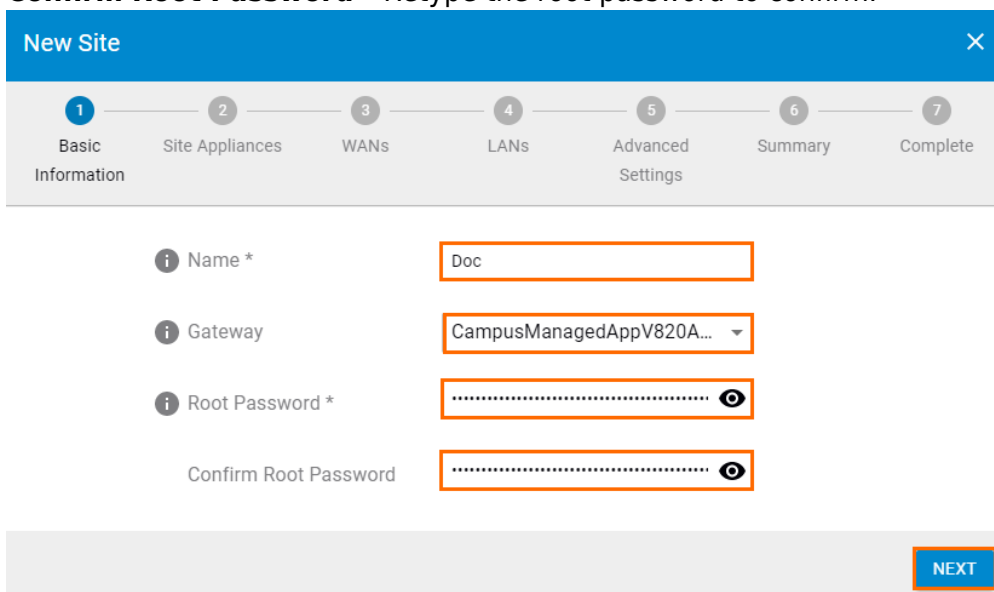


4. From the drop-down menu, select **New SC Device**.



5. The **New Site Basic Information** blade opens. Enter values for the following:

- **Name** – Enter the name of the site.
- **Gateway** – Select the gateway from the drop-down menu you want your site to connect to.
- **Root Password** – Enter the root password.
- **Confirm Root Password** – Retype the root password to confirm.



6. Click **NEXT**.

7. The **Site Appliances** blade opens.

1. Select your Secure Connector appliance from the list of appliances linked to your

account. Note: After ordering, it might take up to 3 hours before your device is listed.

New Site

1

Basic Information

2

Site Appliances

3

WANs

4

LANs

5

Advanced Settings

6

Summary

7

Complete

Q Search Serials

< < 1 > >

1-10 of 10

Selected Serials

56965

✓ Add missing appliance by serial and linking code/license token

BACK

NEXT

2. If your Secure Connector appliance is not listed, you can add it by using the serial number and the linking code found on the back of the Quick Start Guide delivered with your appliance. Note: After ordering, it might take up to 3 hours before your device is listed.

1. Click **Add missing site appliance by serial/linking code**. Then, specify values for the following:
 - **Serial** – Enter the serial number of your appliance.
 - **Code/Token** – Enter the linking code (located on the back of the Quick Start Guide shipped with your hardware appliance), or the token of your VTx appliance.

New Site

1

2

3

4

5

6

7

Basic Information

Site Appliances

WANs

LANs

Advanced Settings

Summary

Complete

<input type="checkbox"/>	56965	FSC2	Pulau Ujong, 9Q8F+75, Singapore	1664267	2022-01-18
<input type="checkbox"/>	253399	FSC2	Beijing, China	1664267	2022-01-18
<input type="checkbox"/>	955544	FSC2	Hong Kong, China	1664267	2022-01-18
<input type="checkbox"/>	323430	FSC2	Yinchuan, Ningsia Hui Autonomous Region, China	1664267	2022-01-18

<<

<

1

>

>>

1-10 of 10

Add missing appliance by serial and linking code/license token

These are found on your Barracuda Networks confirmation email

Serial *

<your_serial>

Code/Token *

<your_token>

ADD

BACK

NEXT

2. Click **ADD** to add the device to your account.

8. Click **NEXT**.

9. The **WANs** blade opens. Enable **WAN Failover**.

New Site

1

2

3

4

5

6

7

Basic Information

Site Appliances

WANs

LANs

Advanced Settings

Summary

Complete

1

2

3

Your device can have up to 2 WAN connections (a primary and a failover).
Do you want to configure a failover for this site?

WAN Failover *

☒

Number of WANs *

2

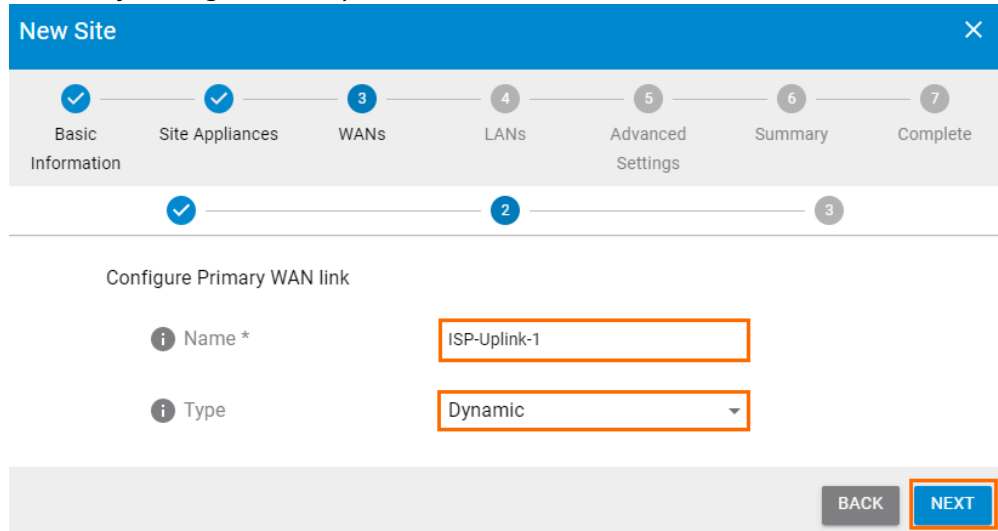
BACK

NEXT

10. Click **NEXT**.

11. The **Configure Primary WAN link** blade opens. Specify values for the following:

- **Name** – Enter a name for your uplink.
- **Type** – Select either dynamic (for configuration using DHCP) or static if you want to manually configure the uplink.



New Site

Basic Information Site Appliances WANS LANs Advanced Settings Summary Complete

Configure Primary WAN link

Name * ISP-Uplink-1

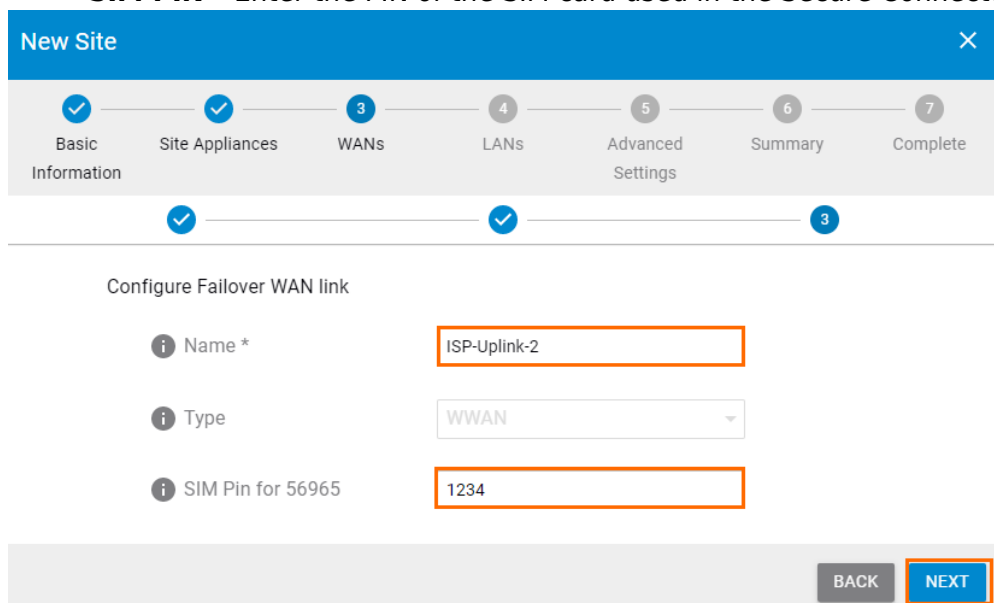
Type Dynamic

BACK NEXT

12. Click **NEXT**.

13. The **Configure Failover WAN link** blade opens. Specify values for the following:

- **Name** – Enter a Name.
- **SIM PIN** – Enter the PIN of the SIM card used in the Secure Connector.



New Site

Basic Information Site Appliances WANS LANs Advanced Settings Summary Complete

Configure Failover WAN link

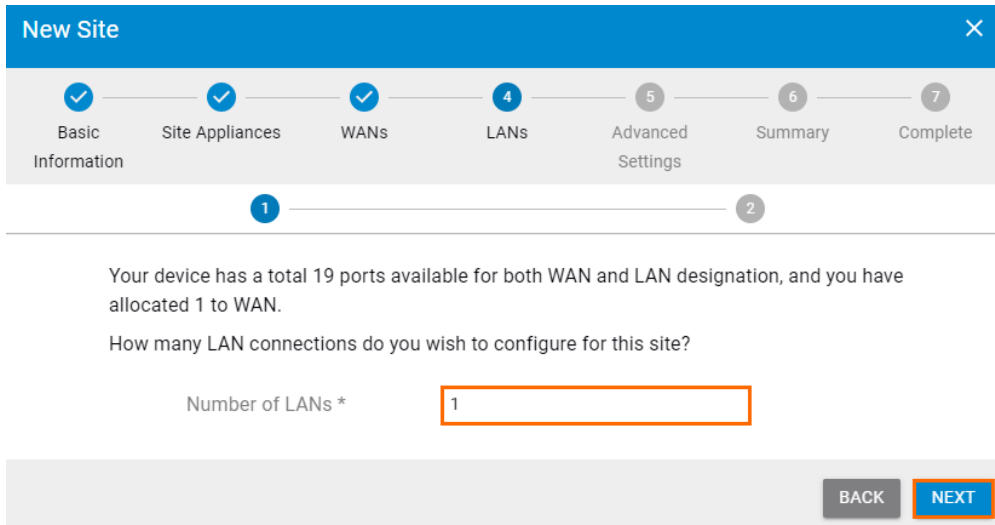
Name * ISP-Uplink-2

Type WWAN

SIM Pin for 56965 1234

BACK NEXT

14. The **LANs** blade opens. Select the number of desired LAN connections from the drop-down list.



New Site [Close]

Progress: Basic Information (✓), Site Appliances (✓), WANS (✓), **LANs (4)**, Advanced Settings (5), Summary (6), Complete (7)

1 ————— 2

Your device has a total 19 ports available for both WAN and LAN designation, and you have allocated 1 to WAN.

How many LAN connections do you wish to configure for this site?

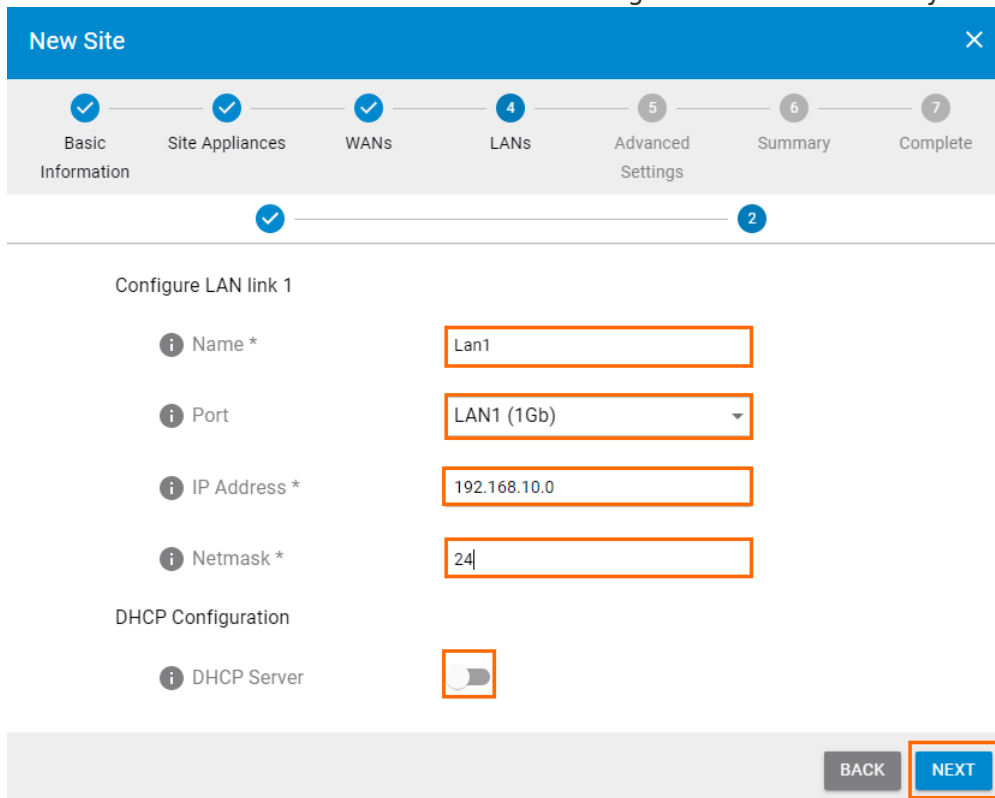
Number of LANs *

[BACK] [NEXT]

15. Click **NEXT**.

16. The **Configure LAN link** blade opens. Specify values for the following:

- **Name** – Enter a name for your LAN.
- **Port** – Select a port from the drop-down list where the LAN is attached to. Note: Port 1 is reserved for high availability.
- **IP Address** – Enter the IP address.
- **Netmask** – Enter a number between 0 and 32 for the subnet mask.
- **DHCP Server** – Click to enable. If enabled, you must enter the **First IP Address** and the **Last IP Address**. IP addresses within this range will be automatically assigned via DHCP.



New Site [Close]

Progress: Basic Information (✓), Site Appliances (✓), WANS (✓), **LANs (4)**, Advanced Settings (5), Summary (6), Complete (7)

1 ————— 2

Configure LAN link 1

Name *

Port

IP Address *

Netmask *

DHCP Configuration

DHCP Server ☐

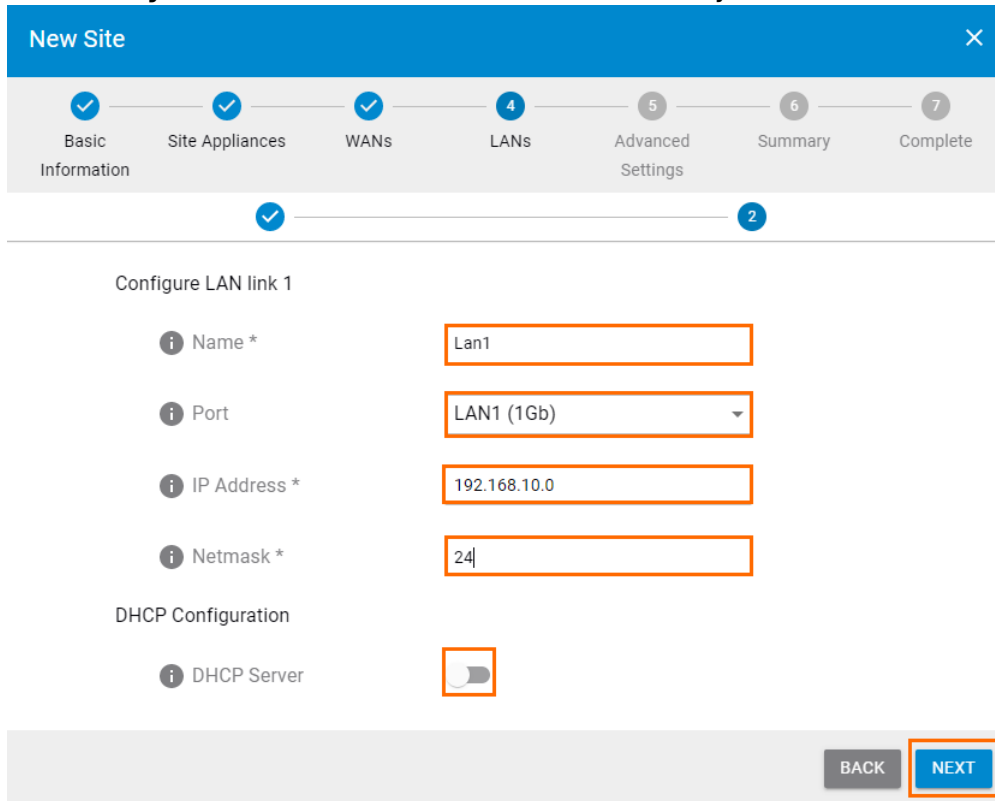
[BACK] [NEXT]

17. Click **NEXT**.

18. The **Advanced Settings blade** opens. Specify values for the following:

- **Primary DNS** – Enter the IP address of the primary DNS server.

- **Secondary DNS** - Enter the IP address the secondary DNS server.



New Site [X]

Progress: Basic Information (✓) | Site Appliances (✓) | WANS (✓) | **LANs (4)** | Advanced Settings (5) | Summary (6) | Complete (7)

Configure LAN link 1

Name *

Port

IP Address *

Netmask *

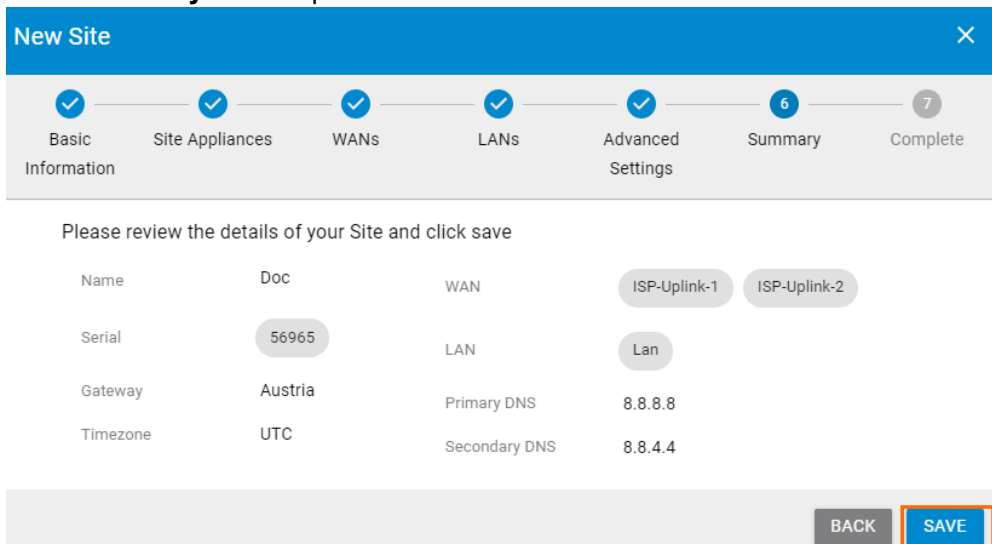
DHCP Configuration

DHCP Server ☐

[BACK] [NEXT]

19. Click **Next**.

20. The **Summary** blade opens.



New Site [X]

Progress: Basic Information (✓) | Site Appliances (✓) | WANS (✓) | LANs (✓) | Advanced Settings (✓) | **Summary (6)** | Complete (7)

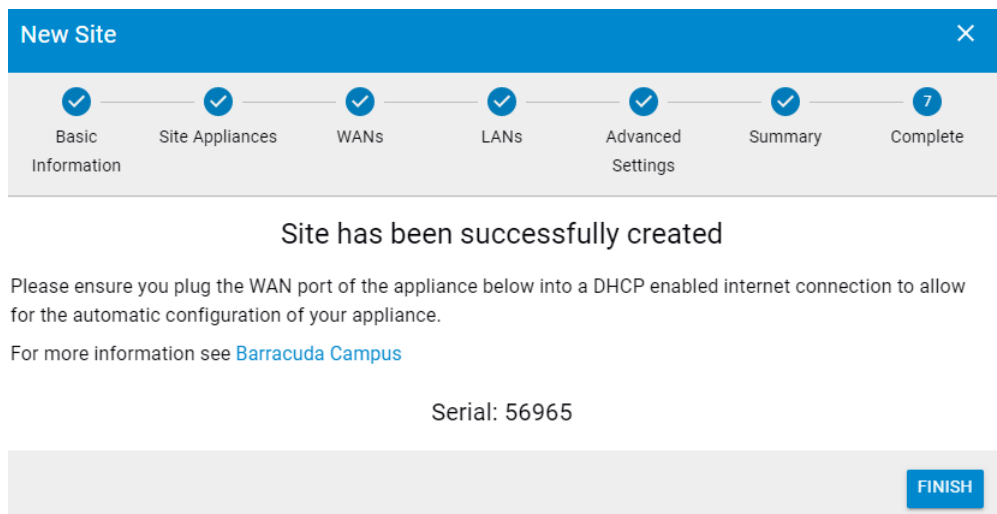
Please review the details of your Site and click save

Name	Doc	WAN	ISP-Uplink-1	ISP-Uplink-2
Serial	56965	LAN	Lan	
Gateway	Austria	Primary DNS	8.8.8.8	
Timezone	UTC	Secondary DNS	8.8.4.4	

[BACK] [SAVE]

21. Review your specifications. If everything is correct, click **SAVE**.

22. Your site configuration has been created successfully.



New Site

Basic Information Site Appliances WANs LANs Advanced Settings Summary Complete 7

Site has been successfully created

Please ensure you plug the WAN port of the appliance below into a DHCP enabled internet connection to allow for the automatic configuration of your appliance.

For more information see [Barracuda Campus](#)

Serial: 56965

FINISH

23. Click **FINISH**.

The appliance will automatically apply the configuration upon its first boot.

Step 2. Deploy the Site Appliance

For more information, see the [Quick Start Guide](#) shipped with the Secure Connector.

Figures

1. new_site821.png
2. new_sc_device.png
3. basic821.png
4. sc_appliance_basictab.png
5. sc_add_token.png
6. sc_wan1.png
7. sc_dynamic_wan.png
8. sc_wan_failover.png
9. number_of_lans_821.png
10. sc_lan.png
11. sc_lan.png
12. sc_summary.png
13. sc_finish.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.