



Contents

Networks	4
Private DNS	4
Connecting a Private DNS to a Network	4
Connecting a Private DNS server to a Region	6
AWS Route 53 DNS	7
DNS Filtering	8
Understanding DNS Filtering	8
Activating DNS Filtering	8
Routes	9
Split Tunneling	. 11
The Default Configuration is Automatic (Full Tunnel)	11
Split tunneling: Automatic Configuration	11
	12
Site-to-Site Interconnectivity	. 12
IPSec based connections	1.13
Wile Guard based connections	. 14
Multi-Turneling	. 10
Dynamic-IP Tunnels	16
WireGuard based connections	10
Whitelisting Resources	. 10
Benefits of Whitelisting	. 19
Microsoft Azure	19
SalesForce	21
AWS-EC2 Security Groups	
Google Cloud Platform	24
Client-Based Access	. 27
MDM App Deployment	27
.msi Installation Flags	. 27
.pkg Installation Flags	. 28
SCCM Agent Deployment	. 28
Deployment Flags	28
Manage Engine	. 29
System Center Configuration Manager (SCCM)	29
JAMF Cloud	29

Client-less Access (Zero Trust Applications)	33
URL Aliasing	.33
Upload domain SSL certificates	. 33
Creating a URL alias for your application	. 35
RDP Security Mode	35
SonicWall Support	. 37
About This Document	. 38

Networks

Topics:

- Private DNS
- DNS Filtering
- Routes
- Split Tunneling
- Site-to-Site Interconnectivity
- Multi-Tunneling
- Dynamic-IP Tunnels
- Whitelisting Resources

Private DNS

This article describes how to configure a private DNS.

Private DNS will enable you to reach an internal resource by its hostname (as published by your local DNS server). This can ease your workflow, as you will now longer need to specify the resource's IP address.

You can assign Private DNS on two different levels: on the Network level (for the entire Network) or on the Region level (for a specific region in your Network).

The Private DNS will allow you to utilize your organization's DNS servers, as well as local domain names while the Regional DNS will allow your users to resolve resources via a local DNS server rather than waiting for a response from a remote one.

Connecting a Private DNS to a Network

A Private DNS server can be connected to the Network by following those steps:

Before you proceed, If your private DNS server(s) do not have a public IP address, you'll need to set up a Site-to-Site connection to the internal network containing the server(s). 1. Click on the (...) icon on the Network section.

saset	olrqa							(+) Add Licenses
Manage a	nd edit the network for your 1	eam needs.					Available g	ateway licenses : 4/10
= (sasebirqa birsasepankygrp-pxmz900h	Regions	Gateways 3	Tunnels 3	Access Group1	s Groups	Tags —	• Active
Regions		Gc	iteways			Tur	nnels	Edit Network Add Regions
٢	Bangalore birsasepankygrp-pxmz900h	•	blrsas 143.11	sepankygrp-xt5oe 0.182.203	•••		(S) WireSnwlT	Manage Access Split Tunneling Private DNS DNS Filtering
							BLRCorpor	Routes Table Delete Network

- 2. Click on Private DNS.
- 3. Turn-on the Enable Private DNS toggle.



If your Private DNS Server(s) supports DoT you'll need to turn the DNS over TLS on (otherwise your requests will be sent over HTTPS).

- 4. Enter the IP address of each one of your DNS servers. You can enter up to four different IP addresses.
 - () NOTE: All private DNS servers should be fully synced as the system will only be resolving addresses through one of the servers. Do not configure public DNS servers (such as 8.8.8.8, 1.1.1.1, etc.), as all requests will be forwarded to them if the private DNS server won't resolve the address.
- 5. Wait for the Network status to change from Deploying to Active.

Connecting a Private DNS server to a Region

1. Click on the (...) icon on the desired Region.



2. Turn-on the Enable Private DNS toggle.

Add Private DNS Specify Internal DNS servers for resolving your processed by the public DNS. Learn More	© resources before
Enable Private DNS* (If disabled, resources resolve on public DNS only)	
Server IP Address*	DNS over TLS 💿
10.50.30.51	
+ Add Server IP Address	
Search Domains 💿	
sonicwall.com	
+ Add Search Domain	
	Cancel Apply

If your Private DNS Server(s) supports DoT you'll need to turn the DNS over TLS on (otherwise your requests will be sent over HTTPS).

- 3. Enter the IP address of each one of your DNS servers. You can enter up to four different IP addresses.
 - () NOTE: All private DNS servers should be fully synced as the system will only be resolving addresses through one of the servers. Do not configure public DNS servers (such as 8.8.8.8, 1.1.1.1, etc.), as all requests will be forwarded to them if the private DNS server won't resolve the address.
- 4. Enter any suffix that you'd like to add to the DNS query (for example, if you enter sonicwall.com as a search domain, and then type in the address bar support, you'll be directed to support@sonicwall.com.



5. Select apply, then wait for the Network status to change from Deploying to Active.

AWS Route 53 DNS

Many of you may have instances and VPC's in AWS and you are very likely utilizing AWS's Route53 DNS infrastructure. In addition to public domain zone management, AWS offers to expose certain zones via private IP access. The proper term for this is inbound and outbound endpoints. We'll be focusing on inbound endpoints in order to better architect SonicWall Cloud Edge's Private DNS feature into your network.

It is considered a good network security practice to make sure that internal resources for your organization's prod or perhaps dev environment are permitted access via a private subnet, making sure that valuable resources aren't on the public internet even if you have security rules in place. Managing a list of public IP's is sure to inflate the more complexity and more people you have.

Accessing internal resources by name is a huge benefit for any environment. There are always a handful set of tools that you may not want to expose to the public.

If you've spun up a tunnel from SonicWall Cloud Edge to AWS using Site to Site, then we need to spin up Inbound Endpoints and create a security group allowing requests on port 53.

Navigate to Route 53 > Resolver > Inbound endpoints.

Create a new resolver:



You should now have a resolver for each of the subnets you've selected. The resolvers will be in the form of IP addresses that you are able to configure within sonicwall Cloud Edge's Private DNS feature.

ite 53 > Resolver > Inbound endpoints >					Edit Delete
					·, ·
vlad_PrivateDNS Configuration					
ID	Status		Host VPC		
rslvr-in-a73f6864ab15404b8	Operational		vpc-0af819c29894	lcca27	
Name	Security group				
vlad_PrivateDNS	sg-0c64e13828fe8	8f2a7			
19 - 1 1 (2)					[
IP addresses (2)				Remove from endpoint	Add IP address
Q					< 1 > @
IP address	IP address ID	Status	Subnet	Availability Zone	
0 10.25.6.72	mi-735b09636a7843778	 Attached 	subnet-0587a4eb47645a229	us-east-1a	

DNS Filtering

This article describes how you can add many powerful security features to your networks such as DNS Filtering to further limit exposure on your network.

Understanding DNS Filtering

DNS filtering allows you to block users in your network from navigating to webpage URLs with their internet browser. Its ability to filter out bad websites and allow access to approved ones is accomplished with blacklisting and whitelisting tools, respectively, and URLs can be blocked on an individual basis or by category (gambling, social networks, etc.). When you blacklist a URL with our DNS filtering feature, you are telling the DNS Resolver not to resolve the website associated with its unique IP address. Instead, it will display a custom message notifying users that their access to the page is restricted. Accordingly, DNS filtering is crucial for productivity and protection as well.

Activating DNS Filtering

1. Open **Networks**from the **Management Platform** and navigate to the network on which you'd like to configure DNS filtering. Select the three-dotted icon on the right side, then select **DNS Filtering**.

saseblrqa								
Manage and edit the network for your tea	am needs.							Add Licenses
							Available g	ateway licenses: 4/10
Ŧ		0-1	Turnels	Accord	Groups			Active
sasebirqa birsasepankygrp-pxmz900h	Regions	3 3	3	Group1	Groups	-	ags -	
								Edit Network
Regions	Gc	iteways			Tu	nnels		Add Regions
								Manage Access
Bangalore birsasepankygrp-pxmz900h		blrsas	epankygrp-xt5oe			(%)	WireSnwlT	Split Tunneling
		C						Private DNS
								DNS Filtering
						\sim		Routes Table
					1	٢	BLRCorpor	Delete Network

- 2. Fill in the following information:
- Enable DNS Filtering.
- URL Blacklist Categories: Block access to websites by content category (select none, one or more).
- Whitelisted/Blacklisted URLs: Manually enter one or more specific URL(s) you'd like to make sure stay
 unblocked/blocked, or upload a .CSV file containing the addresses. Make sure that the .CSV file contains
 only one column, and that every cell contains one URL (as shown in the attached example). The file must
 contain no more than 1000 addresses. Each address must follow the form domain.com (that is, without
 www/http/https prefixes).

	А
1	badpineapple.com
2	fakenews.co.uk
3	loveistheanswer.fr

- 3. Select Apply.
- 4. A successful message appears. Once it has been closed the new settings will be applied the next time a user connects to the network.

Routes

The article describes how to use routes. In most cases, once you set up the tunnel, you can specify remote subnets to be automatically added as propagated Routes. However, if you defined the Remote Gateway Proposal Subnets parameter as 0.0.0.0/0 (any), it is still possible to add manual routes and associate them with the corresponding tunnel as the exit point.

Please follow the steps below:

1. Go to the **Networks** tab and select the network to which you'd like to add a route. Select the three-dotted icon (...), then **Routes Table**.

saseblrqa								
Manage and edit the network for your to	eam needs.							Add Licenses
							Available g	ateway licenses : 4/10
1								
	Regions	Gateways	Tunnels	Access (Groups	Τας]s	Active
blrsasepankygrp-pxmz900h	()	3	3	Group1		_		
								Edit Network
Regions	Gate	ways			Tunne	els		Add Regions
								Manage Access
Bangalore	(blrsase	pankygrp-xt5oe			S	WireSnwlT	Split Tunneling
birsusepunkygrp pxm2500n		143.110	.182.203		Ì	-		Private DNS
L								DNS Filtering
								Routes Table
					i (۲	BLRCorpor	Delete Network

The following window displays:

tal-test Routes Table	
To add route entries, you have to create a tunnel, then click "Add Route". Learn More	Apply Configuration Add Route
You have no routes y	et
To add route entries, you have to create a tunnel, then	n click "Add Route".

- 2. Select Add Route and choose the relevant tunnel.
- 3. Insert the desired range for the route then select **Add Route**.
- 4. The route will be added to the table.

Id route entries, you have to create a tunnel, then click "A	Add Route". Learn More	oply Configuration Ad	d Rout
Tunnels	Subnets	Туре	
ConnectorTest test-2-e5ijsygcwk.pzero.sonicwalledge.biz	172.16.126.0/24	Propogated	

5. Select Apply Configuration.

Split Tunneling

This article describes how to incorporate split tunneling into your network. If you would like to select specific network subnets to go through from the client to the SonicWall network, instead of full tunnel mode (where all the traffic is encrypted and proxied through the SonicWall CloudEdge network), you will need to manually specify which subnets you'd like to include through the tunnel.

The Default Configuration is Automatic (Full Tunnel)

saseblrqa							
Manage and edit the network for you	r team needs.						Add Licenses
						Available g	ateway licenses: 4/10
╤ saseblrqa blrsasepankygrp-pxmz900h	Regions	Gateways 3	Tunnels 3	Access (Group1	Groups T -	ags -	• Active
							Edit Network
Regions	Gc	iteways			Tunnels		Add Regions
Bangalore birsasepankygrp-pxmz900h	•	blrsas 143.110	epankygrp-xt5oe. 0.182.203	··· •• •		WireSnwlT	Manage Access Split Tunneling Private DNS DNS Filtering
						BLRCorpor	Routes Table Delete Network

Split tunneling: Automatic Configuration



Split Tunneling: Manual Configuration



(i) **IMPORTANT:** Some Operating Systems have limitations to the amount of Split Tunneling they allow on a VPN client connection:

IKEv2 - The integration with Windows limits the allows up to 25 different Subnets in Split Tunneling, Mac limit is 254.

OpenVPN, Wireguard - As many subnets as allowed on the local Routing Table (Usually less than 4,000 addresses)

() **IMPORTANT:** If you have defined more than 25 different subnets, make sure that any end-users connected using the agent are operating on either OpenVPN protocol or WireGuard protocol. In any case, it is not recommended to insert more than 254 different subnets.

After defining the split tunneling subnets, this information will be available on the Networks page.



Site-to-Site Interconnectivity

This article describes how to ensure that two sites are connected securely using the SonicWall Platform.

If the two sites are both tunneled to your SonicWall network, you can enable the two to communicate, regardless of their location or dependency so that both sites will have a full and secure line between them.

Please follow the steps below:

IPSec based connections

- 1. Ensure both tunnels are route-based tunnels; that is, they do not depend on a specific internal subnet to create a handshake between the sites, but a route is configured on each device's separate Route Table indicating which subnets to forward into the tunnel.
- 2. On the **Management Platform**, set both tunnel's "Gateway Proposal Subnets" and "Remote gateway Proposal Subnets" to ANY (0.0.0.0/0).

This may make the tunnel go down! Please make sure the device you are using supports route-based VPN. This means the tunnel is set up to 0.0.0.0/0 and a route is added separately.

3. Make sure the Routes Table on the SonicWall side has all of the routes of all of the sites configured (Network/ Route Tables) so in case you had them defined within the tunnel module, instead you need to add them here.

dd Route". Learn More	aply Configuration Add Ro	ute
Subnets	Туре	
172.16.126.0/24	Propogated	
	dd Route". Learn More Subnets 172.16.126.0/24	dd Route". Learn More Apply Configuration Add Ro Subnets Type 172.16.126.0/24 Propogated

4. Click Add Route and add the routing to the internal LAN subnets that are behind each tunnel.

Add Route		
Tunnel		
9 ₀ Site1		× v
Subnets		
192.168.0.0/16		
	Cancel	Add Route

5. After you are done, click Apply Configuration.

frica Routes Table			
add route entries, you have to create a tunnel, then click '	'Add Route". Learn More	pply Configuration	Add Route
Tunnels	Subnets	Туре	
ConnectorTest	172.16.126.0/24	Propogated	

- 6. Go to the first site's (labeled Site1) routing table, and in addition to the route that indicates all subnets (usually 10.255.0.0/16) to go through the Site to site tunnel, add a route dictating all traffic that goes to the second site's LAN subnet as well.
- 7. Go to the second site's (labeled Site2) routing table, and set up a static route indicating both the LAN subnet and Site1's LAN subnet to go through the IPSEC Site-2-Site tunnel.

WireGuard based connections

1. In order to establish a connection from one resource to another, you'll need to reinstall the connector, as the default installation (Accessor mode) does not allow it.

Uninstall Commands

Ubuntu

```
# Locate the WireGuard packages (the output of this command is the full
package name)
dpkg -l | grep wireguard
# Delete all packages found that are associated with WireGuard (replace pkg
with the output from the previous command)
apt-get remove --purge pkg
```

CentOS

```
# Locate the WireGuard packages (the output of this command is the full
package name)
yum list installed | grep wireguard
# Delete all packages found that are associated with WireGuard (replace pkg
with the output from the previous command)
yum remove pkg
```

- 2. Once you successfully removed the files mentioned in the commands above, reboot the machine and execute the connector installation script (the curl command that you copied from the Management Platform).
- 3. When you reach the 4th step, choose NO (n), which will prevent accessor mode installation.
- 4. Proceed with the installation. Make sure to select YES (y) for both IP Forwarding and Routing all traffic.
- 5. Open the route table of the network in which the WireGuard connector is installed (usually your router or firewall).
- 6. Configure a static route dictating all traffic from your SonicWall LAN subnet (10.XXX.0.0/16) to go through the IP of the machine that hosts the connector.
- 7. Open the terminal of the machine that hosts the connector and execute the following command: **Shell**

```
# Temporarily shut the connector down
wg-quick down wg0
# Open the connector's route table.
vi /etc/wireguard/wg0.conf
```

Enter the subnets of the resources you'd like to communicate with each other set AllowedIPs = <SonicWall Subnet>, <Site1 Subnet>,< Site 2 Subnet> # Turn the connector up wg-quick up wg0 # Make sure that the desired change has taken place wg show

Multi-Tunneling

SonicWall Cloud Edge does not limit the number of tunnels that can be connected to a single gateway, so in case you only have one gateway in a particular network, but your company's infrastructure consists of a hybrid environment (a mixture of different on-prem and cloud-based resources) you don't need to worry.

Regions	Gateways	Tunnels	
San Jose supportyourapperimeter81.com		er81.com 🛞 Site1	
		T ♥	

(i) **IMPORTANT:** Before you configure a second tunnel, make sure that the remote network's subnet does not overlap with the existing network's subnet.

Once the two tunnels are up and running, you'll be able to set up a communication line between the two (see Interconnectivity).

Dynamic-IP Tunnels

In order to establish a site-to-site tunnel (IPSec or WireGuard) between your SonicWall Cloud Edge gateway and a firewall/router with a dynamic public IP address, you will need to apply some modifications to the tunnel creation process. Follow the instructions below.

(i) NOTE: This option is not supported by cloud IaaS providers (such as AWS, GCP, or Azure).

IPSec based connections

1. When creating the tunnel at the SonicWall Cloud Edge platform fill in the General Settings section with the following information:

Shared Secret* 💿
Enter shared secret Generate
Remote ID 💿
Enter remote ID
Remote Gateway Proposal Subnets* 💿
Any (0.0.0/0) Specified Subnets

- Name: Enter a name of your choice.
- Shared Secret: Enter a string of at least 8 characters or use the Generate button. Make sure to copy and save it, as it'll be required when setting up the tunnel on your firewall/router management interface.
- Public IP: Enter 0.0.0.0
- **Remote ID:** Enter a string of your own choice. This parameter will use as an additional shared secret, providing an extra level of security. Copy and save it as it'll be used as the left ID (local ID or local identification) when setting the tunnel on your firewall/router management interface.

(i) **IMPORTANT:** 0.0.0.0 is not an acceptable value for the Remote ID.

- SonicWall Gateway Proposal Subnet: Specify your SonicWall network subnet (do not choose any).
- Remote Gateway Proposal Subnet: Specify your on-premises internal network subnet.
- 2. In the Advanced Settings section make sure to select IKEv2 only. The rest of the values remain the same as appropriate.
- 3. When setting up the tunnel at the firewall/router management interface fill in the following information:
 - Local IP: Since you're using a dynamic IP, enter a default value (this will vary between different vendors).
 - Local Identification/Local ID/My identifier: Fill in the same value you set for Remote ID at the SonicWall Cloud Edge platform.
 - Remote IP/Remote ID/Peer Identifier: Enter your SonicWall Cloud Edge gateway IP address.
 - IKE Version: IKEv2

Must match the setting chosen on the remote side.	
Negotiation mode Main -	
Aggressive is more flexible, but less secure.	
My identifier Distinguished name The Remote ID you see	t on the CE Platform

4. Fill in the rest of the fields as appropriate.

WireGuard based connections

1. When creating the tunnel at the SonicWall Cloud Edge platform fill in the General Settings section with the following information:

WireGuard	Connector SCP/other DC with easy to use connector. Learn More
Requirements	2 Configuration — Confirm
Name* 💿	
Enter the name	
Endpoint* 📀	
Enter the IP address	
Subnets* @	
Enter the subnets	
	Back Next

- Name: Enter a name of your choice.
- Endpoint: Enter 0.0.0.0
- Subnets: Enter your internal on-premises network's subnet.
- 2. Follow the rest as appropriate.

Whitelisting Resources

Topics:

- Benefits of Whitelisting
- Microsoft Azure
- SalesForce
- AWS-EC2 Security Groups
- Google Cloud Platform

Benefits of Whitelisting

This article describes what whitelisting is. Whitelisting is the practice of explicitly allowing some identified entities access to a particular privilege, service, mobility, access, or recognition.

While IP whitelisting does not encrypt your data the way a site-to-site connection does, it can come in handy if you'd like to save time and avoid the trouble to set one up, as it still limits access to your resources - an entire network or a specific machine or application. Once whitelisting your gateway IP, the resource will be accessible only for devices using this particular IP, that is, connected to the SonicWall.

Microsoft Azure

This article describes how to whitelist your SonicWall Cloud Edge Gateway at the Microsoft Azure Portal, which allows you to restrict access to a certain resource within an Azure Virtual Network to users connected to the secure SonicWall Cloud Edge gateway only. While this method needs to be applied to every particular resource, it is a good alternative for those who'd like to avoid setting up a Site-to-Site connection to a VNet.

- 1. Open the Azure Portal and select the resource which you'd like to restrict access to.
- 2. Navigate to the Networking tab and select Add inbound port rule.
- 3. Fill in the following information:

Add inbound security rule	×
🧷 Basic	
Source * ①	
IP Addresses	\checkmark
Source IP addresses/CIDR ranges * ①	
176.229.148.22	~
Source port ranges * ①	
*	
Destination * ①	
Any	\checkmark
Destination port ranges * (i)	
*	\checkmark

- Source: IP Addresses
- Source IP addresses/CIDR ranges: Insert your Gateway IP
- Source port ranges: (all)
- Destination: Any
- Destination port ranges: (all)

Protocol *			
Any	TCP	UDP	ICMP
Action *			
Allow	Deny)	
Priority * 🛈)		
120			
Name *			
Sonicwa	I		\checkmark
Description			

- Protocol: Any
- Action: Allow
- Priority: Leave default value
- Name: Connector
- Description: Optional
- 4. Select Add rule.

SalesForce

This article describes how to whitelist SalesForce for your network. Trusted IP ranges in Salesforce block unauthorized access as there are no location restrictions with the platform's default settings. After specifying a Trusted IP range, only authorized SonicWall users from your Private Server will have access to Salesforce resources.

Setting up SalesForce

- 1. Navigate to the Setup section of Salesforce and in the Quick Find search box type "Network Access".
- 2. Select **New** and then fill in the Private Server IP address, entering both the start and end of the IP range and adding a description.
- 3. Select Save.

Setup Home Object	Manager 🗸	
	The construction of the second construction of the second se	ALLET MANY JUST THE CONCENTED MANY JUST CONSIST OF A CONCENTED AND A DESCRIPTION OF A CONCENTER OF A CONCENTE OF A CONCENTER OF A CONCENTE OF
Q, network	Serup	
✓ Security	Network Access	
Network Access		
	Network Access	Help for this Plage 🥹
and the second strategies at a	Trusted IP Range Edit	
Didn't find what you're looking for? Try using Global Search.	Enter the range of valid IP addresses from which user logins are trusted. Users logging in from the client such as Connect for Outlook, Connect Olfline, Connect for Office, Connect for Lotus Notes,	ied IP addresses are not asked to activate their computers and may use their user password instead of a security token to log in to the API or a decidop the Data Lodder.
	Please specify IP range	+ Required Information
	Start IP Address	End IP Address
	LARKAPPEON	
	Save Cancel	

AWS-EC2 Security Groups

This article describes how to whitelist your SonicWall Cloud Edge Gateway at the AWS Management Console, which will allow you to restrict the access to a certain resource within a VPC to users connected to the secure SonicWall Cloud Edge Gateway only. While this method needs to be applied to every particular resource, it is a good alternative for those who'd like to avoid setting up a Site-to-Site connection to a VPC.

- Create a security group
- Attach resources to the security group

Please follow the steps below:

Create a security group

- 1. Open the AWS Management Console EC2 dashboard.
- 2. Navigate to Security Groups.



3. Select **Create** and fill in the following information:

2 > Security Groups > Create security group	Security Groups Create security group Create security group Create security group Info rity group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below. Sic details Surfly group name Info StytebServerGroup ne cannot be edited after creation. Security Info Ilows SSH access to developers		
Create security group ats as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below. Basic details Security group name info MyWebServerGroup Name cannot be added after creation. Description info Allows SSH access to developers VPC info [ypc-0851a4aB314b63b94 (P81 Staging)	Practe Security group Info rify group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below. sic details surfy group name Info htWebServerGroup ne cannot be edited after creation. scription Info llows SSH access to developers	2 > Security Groups > Create security group	
security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below. Basic details Security group name info MyWebServerGroup Name cannot be edited after creation. Description info Allows SSH access to developers VPC info (ypc-0851a4a8314b63b94 (P81 Staging)	rity group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below. sic details utify group name info tyWebServerGroup ne cannot be edited after creation. scription info llows SSH access to developers	reate security group Info	
Basic details Security group name Info MyWebServerGroup Name cannot be edited after creation. Description Info Allows SSH access to developers VPC Info [vpc-0851a4a8314b63b94 (P81 Staging)	sic details curity group name info tyWebServerGroup ne cannot be edited after creation. cription info llows SSH access to developers	ecurity group acts as a virtual firewall for your instance to control inbound and outbound traffic.	To create a new security group, complete the fields below.
Security group name info MyWebServerGroup Name cannot be edited after creation. Description info Allows SSH access to developers VPC info Vpc-0851a4a8314b63b94 (P81 Staging)	surity group name info tyWebServerGroup ne cannot be edited after creation. scription Info Illows SSH access to developers	Basic details	
MyWebServerGroup Name cannot be edited after creation. Description Info Allows SSH access to developers VPC Info vpc-0851a4a8314b63b94 (P81 Staging)	h/WebServerGroup ne cannot be edited after creation. scription Info Illows SSH access to developers	Security group name Info	
Name cannot be edited after creation. Description Info Allows SSH access to developers VPC Info Vpc-0851a4a8314b63b94 (P81 Staging)	ne cannot be edited after creation. scription Info Ilows SSH access to developers	MyWebServerGroup	
Description Info Allows SSH access to developers VPC Info Vpc-0851a4a8314b63b94 (P81 Staging)	Illows SSH access to developers	Name cannot be edited after creation.	
Allows SSH access to developers VPC Info Vpc-0851a4a8314b63b94 (P81 Staging)	llows SSH access to developers	Description Info	
VPC Info vpc-0851a4a8314b63b94 (P81 Staging)		Allows SSH access to developers	
vpc-0851a4a8314b63b94 (P81 Staging)	C Info	VPC Info	
	pc-0851a4a8314b63b94 (P81 Staging)	vpc-0851a4a8314b63b94 (P81 Staging)	

- Security group name: Enter a name of your choice.
- **Description:** Describe the use case of the group. The description can be up to 255 characters long.
- VPC: Select the appropriate VPC. If you are using VPC peering, you can later update the rules for your VPC security groups to reference security groups in the peered VPC. In case you are using a Transit Gateway, note that spoke Amazon VPCs cannot reference security groups in other spokes connected to the same AWS Transit Gateway.
- Add an inbound rule according to the following
 - Type: All traffic
 - Protocol: All
 - Port range: All
 - Source: Custom; Insert your SonicWall Cloud Edge Gateway IP
 - **Description:** (optional)

Type Info	Protoco l Info	Port range Info	Source Info	Description - optional Info
All traffic	All	All	Custom Q	De

• Select Create security group.

Attach resources to the security group

- 1. Return to the EC2 dashboard.
- 2. Select the Instances tab within the Instances section.



3. Select the instance you'd like to apply the Security Group to. Select **Actions** /**Networking** /**Change Security Groups**.

Launch Instance Connect	Actions A			∆ ⊕ ♥ Ø
Q Filter by tags and attributes or search	Connect Get Windows Password		ØK	< 1 to 12 of 12 $>$ $>$
Name	Create Template From Instance Launch More Like This	nce Type 👻 Availability Zone 👻	Instance State + Stat	tus Checks 👻 Alarm Statu:
Windows Server 2019	Instance State	cro us-east-1a	stopped	None
Elinoy-Test	Instance Settings	no us-east-1a	stopped	None
WatchGuard	Image 🕨 🕨	na us sost 1d	stopped	None
Cisco ASA	Networking	Change Security Groups	stopped	None
Fortigate		Detach Network Interface	stopped	None
Linux TEQT3	i Nac/DDacdf6fDD3hc t2 mi	Disassociate Elastic IP Address	a stannad	Nono
Instance: i-060f1155c7625f514 (Wir	dows Server 2019) Private IP:	Change Source/Dest. Check		
		Manage IP Addresses		
Description Status Checks	Monitoring Tags			

4. Select the newly created security group, then select Assign security group.

Sel	ect Security Group(s) to assoc	ciate with your instance	
	Security Group ID	Security Group Name	Description
	sg-00324a49c54d664ba	launch-wizard-2	launch-wizard-2 created 2019-09-20T17:26:22.605-07:00
	sg-0c293616a2921b697	launch-wizard-3	launch-wizard-3 created 2019-10-13T17:51:21.367+03:00

Google Cloud Platform

This article describes how to whitelist your SonicWall Cloud Edge Gateway at Google Cloud Platform, which will allow you to restrict the access to a certain VPC to users connected to the secured SonicWall Cloud Edge gateway only. The following steps are required:

- Querying your gateway IP address
- Configuring a rule in Google Cloud Platform Firewall

Querying your gateway IP Address

- 1. Open the SonicWall Cloud Edge Management Platform.
- 2. At the left toolbar, select the Networks tab.
- 3. Select the network that contains the gateway which you'd like to whitelist.
- 4. Copy the gateway IP as shown in the screenshot.

Regions			Gateways	
۲	Dallas test-2-fn3xqa54nicwalledg	•	 test-2-e5ijsy cwalledge	

Configuring a rule in Google Cloud Platform Firewall

- 1. Open the GCP console.
- 2. In the left toolbar, select VPC network, then Firewall rules.
- 3. Select Create Firewall Rule, and fill in according to the following:

Frewail rules control incoming or outgoing traffic to an instance. By traffic from outside your network is blocked. Learn more	/ default, incoming
Name *	
Sonicwall - Whitelist	0
Lowercase letters, numbers, hyphens allowed	
Description	
.ogs furning on firewall logs can generate a large number of logs which can in Stackdriver. <u>Learn more</u> O On	ncrease costs in
Off	
Network *	- 0
.	
Priority *	•

- Name: Choose the name of your own choice.
- Description: Let other administrators know what this rule serves for (optional).
- **Logs**: You can choose to log traffic related to the rule (this may lead to additional costs on Google's side).
- Network: Choose the network that contains the resources that you'd like to whitelist.
- Priority: Leave default values.

Direction of traf	fic 🔞	
Ingress		
C Egress		
Action on match	n @	
Allow		
O Deny		
Targets		
All instances in	n the network 🔹	0
Course filter		
IP ranges	•	0
Source IP rand	* 291	0
oodroo in rang		•
Second source	filter	
None	•	0
Protocols and p	orts 🕑	
Allow all		
Specified pr	otocols and ports	
tcp :	20, 50-60	
udp :	all	
Other p	rotocols	
protocols,	comma separated, e.g. ah, sctp	
protocols,	comma separated, e.g. ah, sctp	
protocols,	.E	
protocols,	Comma separated, e.g. ah, sctp	
protocols,	Comma separated, e.g. ah, sctp	

- Direction of traffic: Ingress
- Action on match: Allow
- **Targets**: Depending on your needs, choose the entire network (**All instances in the network**) or choose resources that are labeled with a certain tag (**Specified target tags**).
- Source filter: IP ranges
- Source IP ranges: Paste the IP address of the gateway and add /32, for instance 37.142.39.122/32.
- Second source filter: None
- Protocols and ports: Allow all.
- 4. Select Create.

2

Client-Based Access

Topics:

- MDM App Deployment
- SCCM Agent Deployment
- JAMF Cloud

MDM App Deployment

The deployment process of SonicWall Cloud Edge varies depending on your MDM (Mobile Device Management) provider and is done utilizing a public app deployment process.

- Connector for Android: Download from the SonicWall Cloud Edge portal, https://static.sonicwalledge.com/apps/android/SonicWallCloudEdge.apk
- Connector for iOS: https://www.apple.com/in/search/sonicwall?src=serp
- Connector for MacOS: https://static.sonicwalledge.com/apps/osx/sdp/SonicWallCloudEdge.dmg

Below are links to deployment guides for common MDM providers:

- VMWare AirWatch
- MobileIron SonicWall Cloud Edge deployment is done using the App Catalog. Follow the link below for how to add an app from the Public App Stores.: http://mi.extendedhelp.mobileiron.com/45/all/en/desktop/App_Catalog.htm
- Microsoft EndPoint Manager (InTune)
- JAMF Cloud
- Meraki

.msi Installation Flags

Silent Installation:

• msiexec /quiet /i SonicWallCloudEdge.msi

Silent Installation and get the installation status back to the deployment service:

- start /wait msiexec /quiet /i "SonicWallCloudEdge.msi"
- echo %errorlevel%

Uninstallation:

• msiexec /x "SonicWallCloudEdge.msi"

.pkg Installation Flags

Silent Installation:

• \$ sudo installer -pkg SonicWallCloudEdge.pkg -target /

SCCM Agent Deployment

If the devices in your organization are managed through a central desktop management tool you may prefer remote installation instead of having team members download and install the app on their own. The following guide contains instructions for **ManageEngine**, **JAMF Cloud** and **SCCM**. If using a different tool, please contact us via email and our engineers will be happy to provide you with a suitable solution.

Deployment Flags

Some SCCM solutions may require deployment flags in order to silently install the CloudEdge agents.

Windows Installation, example 1:

• msiexec /quiet /i SonicWallCloudEdge.msi

Windows Installation, example 2:

- start /wait msiexec /quiet /i "SonicWallCloudEdge.msi"
- echo %errorlevel%

Uninstallation:

• msiexec /x "SonicWallCloudEdge.msi"

MacOS:

• sudo installer -pkg SonicWallCloudEdge.dmg -target /

MARNING: Only the above flags are allowed via the .msi installation.

Manage Engine

- 1. Navigate to Software Deployment > Install/Uninstall Software Configuration > Computer configuration.
- 2. Provide a name and description for the configuration.
- 3. Select the Package.
- 4. Select the **Operation Type** as Install, Uninstall, or Advertise as the case may be.
- 5. Specify the user account as which the software needs to be installed as a system user or any specific user.
- 6. If you wish to involve user interaction while deploying the software, enable the appropriate checkbox.
- 7. Configure the scheduler settings and choose the deployment policy.
- 8. Upon defining the target, select **Deploy**.

System Center Configuration Manager (SCCM)

- 1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Application Management**, and select the **Applications** node.
- 2. From the Home tab, select Create group and select Import Application from the ribbon.
- 3. On the General page of the Import Application Wizard, specify the network path to the File to import.
- 4. On the **File Content** page, select the action to take if this application is a duplicate of an existing application. Create a new application, or ignore the duplicate and add a new revision to the existing application.
- On the Summary page, review the actions, and finish the wizard. The new application appears in the Applications node.

JAMF Cloud

This guide demonstrates how to distribute the SonicWall Cloud Edge endpoint application to macOS users using JAMF.

Follow the steps below:

- Upload the SonicWall Cloud Edge application
- Set an installation policy

1. Open the JAMF console/Computers/Management Settings.



2. Select Computer Management/Package.

ŝ	All Settings	Computer I	Management						
101 ()))	System Settings Global Management	Packages	Scripts	Printers	Directory Bindings	Disk Encryption Configurations	Dock Items	Configurations	Patch Management
Ø	Self Service	Computer I	Management -	Managemer	t Framework	c			
Å	Server Infrastructure	Ê		0	0	Ê	~		
	Network Organization		*			<u></u>	69		
		Collection	Display	Check-In	security	Attributes	Imaging	MAC Addresses	App opdates
	Computer Management								
Ē	Device Management								
Ð	User Management								
i	Jamf Pro Information								

3. Fill in the SonicWall Cloud Edge information and upload the installation file.

Settings : Computer Management > Packages ← New Package
General Options Limitations
Display Name Display name for the pockage
SonicWall
Filename Filename of the puckage on the distribution point (e.g. "big/Package.dmg") Ohange File Sonic/Wall plag
Manifes Flie
Uplead Manfest File
Internation to display to the administrator when the package is deployed or uninstalled
Netes Notes to display about the package (b.g. who built it and when It was built)

4. Open the JAMF console/policies.

mputers : Policies - New Policy	
Options Scope Self Service	User Interaction
0 General	
Packages 0 Packages	>
(Software Updates Not Configured	
Scripts 0 Scripts	
Printers 0 Printers	
Disk Encryption Not Configured	
Dock Items 0 Dock Items	
Local Accounts 0 Accounts	
Management Accounts Not Configured	
Directory Bindings O Bindings	
EFI Password Not Configured	
Restart Options Not Configured	
Maintenance Not Configured	
Files and Processes Not Configured	

5. Select New Policy.

Con ←	New Policies				
0	ptions Scope	Self Serv	ice User Interaction		
[8]	General		Packages		Packages Settings
			NAME	CATEGORY	
-	Packages 0 Packages	>	SonicWall	No category assigned	Add
(3)	Software Updates Not Configured				Cancel
N -	Scripts 0 Scripts				
8	Printers 0 Printers				
Ó	Disk Encryption Not Configured				

6. Select the package.

Cor ←	nputers : Policies - New Policy				
c 	Options Scope S	Self Service	User Interaction		
چ (ه)	Packages 1 Package Software Updates Not Configured	>	Packages Distribution Point Distribution point to download the package(s) from Each computer's default distribution point		
	Scripts O Scripts Printers O Printers		SonicWall Action to take on computers		× +
Ó	Disk Encryption Not Configured		Install Update Autorun data Add or remove the package from each computer's Autorun data		
1	0 Dock Items Local Accounts 0 Accounts				
	Management Accounts Not Configured			(X) Cancel	E Save

- 7. Add SonicWall Cloud Edge and configure the rest of the tabs for your requirements.
- 8. Select Save.

Client-less Access (Zero Trust Applications)

3

Topics:

- URL Aliasing
- RDP Security Mode

URL Aliasing

This article describes how to configure a URL alias for a Zero Trust application, thus enabling you to connect to the application with a domain-associated user-friendly URL.

- Uploading domain SSL certificates
- Creating a URL alias for your application

Upload domain SSL certificates

A domain-validated certificate (DV) is an X.509 digital certificate typically used for Transport Layer Security (TLS) where the domain name of the applicant is validated by proving some control over a DNS domain.

1. To add Application Domain Certificates, go to Settings/Certification Manager.

Certificate M Here you store your ce	fanager rtificates in order to create a	secure connections to your appl	ications. Learn more	⊙ Upload Certificate
Name	Domain Name	Additional Names	Signature Algorithm	
TestCert	portal1.snwl.com		sha1WithRSAEncryption	

2. The Upload Certificate screen displays. Fill in the Certificate Body, PrivateKey, and Chain.

Ipload Certificate	re.		
Select Certificate		ß	What is SSL Certificate?
Certificate name*		Ħ	cryptographic key to an organization's details. When installed on a web server, allows secure connections from a web server
Enter certificate name			to a prowser.
ertificate body*	Ů Upload PEM/CERT/PFX File		
BEGIN CERTIFICATE MIDDDCCAoygAwlBAgIGAVyqGLcMA00 JMIDDDDQEBcm5pYTEWMBQGA1UE CONTIFICATE C	iCSqG5Ib3G5QswCQYDVQQGEw		
Certificate private key*	1 Upload PEM/CERT/PFX File		

3. Select **Validate** to ensure this certificate is correct:

Domains:	safervpn.com, *.safervpn.com
Expires in:	26 Days
Public key info:	RSA - 2048
Signature algorithm:	SHA256WITHRSA
Certificate body*	
Certificate private ke BEGIN CERTIFIC	y* ATE
MIIDpDCCAoygAwl CQYDVQQGEwJVU	BAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw eTMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Certificate chain	
BEGIN CERTIFIC	ATE
MIIDpDCCAoygAwl	BAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
COYDVOOGEwIVU	ETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE

4. Select **Apply** to upload the certificate.

Creating a URL alias for your application

1. URL aliasing can be configured for any zero trust application. When creating the app follow these additional steps.

() | IMPORTANT: Once the app has been created, you won't be able to add a URL alias.

Applications Choose the application you would like	e to manage. <mark>Learn More</mark>			O	Add application
Filter by applications Q				Available Ap	plications: 992/1000
ApacheSSH 33133.116.5	Network AWSDEMO	Access Groups All Users	Policy —	Enabled	Edit
Apache 3.133.116.5	Network AWSDEMO	Access Groups All Users	Policy —	Enabled	Delete

2. Enable URL Alias. Choose a CNAME associated with your domain and the correlating certificate (for example *myapplication.mydomain.com*).

URL Alias					
External Domain (CNAME)* 💿	SSL Certificate* 💿				

 Go to your DNS administrator (for instance GoDaddy or R53 in AWS). Define a CNAME under your domain (identical to the CNAME you inserted in the SonicWall Cloud Edge) and point it to application FQDN (the FQDN will appear in the app settings once you click to apply).

FQDN 📀	
fFVCdmpsZq.pzero. sonicwall.com	ß

RDP Security Mode

This article describes how to configure RDP Security Mode for a Zero Trust RDP Application to a remote Windows instance, such as Windows Server 2016 / Windows 10.

(i) NOTE: Make sure you are familiar with the server's authentication methods (username and password or RDP keys) and that you have a tunnel connecting your network and the environment that hosts the Windows instance.

This mode dictates how data will be encrypted and what type of authentication will be performed if any. By default, a security mode is selected based on a negotiation process that determines what both the client and the server support.

Possible values are:

- **any:** Automatically select the security mode based on the security protocols supported by both the client and the server. This is the default.
- **nla:** Network Level Authentication, sometimes also referred to as "hybrid" or CredSSP (the protocol that drives NLA). This mode uses TLS encryption and requires the username and password to be given in advance. Unlike RDP mode, the authentication step is performed before the remote desktop session actually starts, avoiding the need for the Windows server to allocate significant resources for users that may not be authorized.
- **nla-ext:** Extended Network Level Authentication. This mode is identical to NLA except that an additional "Early User Authorization Result" is required to be sent from the server to the client immediately after the NLA handshake is completed.
- **tls:** RDP authentication and encryption implemented via TLS (Transport Layer Security). Also referred to as RDSTLS, the TLS security mode is primarily used in load-balanced configurations where the initial RDP server may redirect the connection to a different RDP server.
- vmconnect: Automatically select the security mode based on the security protocols supported by both the client and the server, limiting that negotiation to only the protocols known to be supported by Hyper-V / VMConnect.
- **rdp:** Standard RDP encryption. This mode is generally only used for older Windows servers or in cases where a standard Windows login screen is desired. Newer versions of Windows have this mode disabled by default and will only accept NLA unless explicitly configured otherwise.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

(i) | NOTE: A NOTE icon indicates supporting information.

- (i) | IMPORTANT: An IMPORTANT icon indicates supporting information.
- (i) | TIP: A TIP icon indicates helpful information.
- CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
- M WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Cloud Edge Secure Access Advanced Settings Updated - March 2022 232-005538-00 Rev E

Copyright © 2022 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request Attn: Jennifer Anderson 1033 McCarthy Blvd Milpitas, CA 95035