

SecureFirst

How to allow wireless traffic over a site to site VPN when the WLAN is bridged to the LAN

KNOWLEDGE DATABASE



How to allow wireless traffic over a site to site VPN when the WLAN is bridged to the LAN

Procedure:

When setting up a site to site VPN with the WLAN bridged, even though the WLAN is in the same subnet as the LAN, it will not be able to pass traffic over the site to site VPN. This is due to the zone based rules. By default rules are created for the LAN zone or the zone/subnet specified in the VPN. If X0 subnet, LAN subnets, or LAN primary subnet is selected as the local network in the VPN it will include the subnet of the WLAN network, but not the zone. If wireless traffic should be allowed to pass over the VPN, please go to the access rules and create two rules. The first rule should be from zone WLAN and to zone VPN where the source network is the W0 subnet or WLAN subnet and the destination network is the remote network that is reached through the VPN. The service on this rule by default should be set to Any. The second rule should be from zone VPN to zone WLAN. It should have the source network as the remote VPN network and the destination network should be the WLAN subnet, W0 subnet or the wireless subnet in question. Please see the screen shots below.

General Advanced QoS Setting Action Ope From : WLAN VPN To: Source Ports Any Any Sources W0 Subnet Destination Network Users Induded: All Users Excluded: None searc will be denie Always on Scheduler VPN Access rule Enable Looging Enable Geo-IP Filter Allow Fragmented Packets Enable Botnet Filter Enable flow reporting Enable packet monito Enable Management

TCorporation[®]

Add Close Help

SONICWALL' Network Security Appliance

Genera	Advanced (QoS
Settings		
Action:	● Allow ○ Deny ○ Discard	
From :	VPN	~
To :	WLAN	~
Source Port:	Any	~ ·
Service:	Any	~
Source:	Destination Network	~
Destination:	W0 Subnet	~
Users Included:	All	these users will be allowed if not excluded,
Users Excluded:	None	these users will be denied.
Schedule:	Always on	~
Comment:	VPN Access rule	
Enable Logging		Enable Geo-IP Filter
Allow Fragmented Packets		Enable Botnet Filter
Enable flo	w reporting	
Enable pa	cket monitor	
Enable Ma	anagement	

RESOLUTION FOR SONICOS 6.5 AND LATER

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

Procedure:

When setting up a site to site VPN with the WLAN bridged, even though the WLAN is in the same subnet as the LAN, it will not be able to pass traffic over the site to site VPN. This is due to the zone based rules. By default rules are created for the LAN zone or the zone/subnet specified in the VPN. If X0 subnet, LAN subnets, or LAN primary subnet is selected as the local network in the VPN it will include the subnet of the WLAN network, but not the zone. If wireless traffic should be allowed to pass over the VPN, please go to the access rules and create two rules. The first rule should be from zone WLAN and to zone VPN where the source network is the W0 subnet or WLAN subnet and the

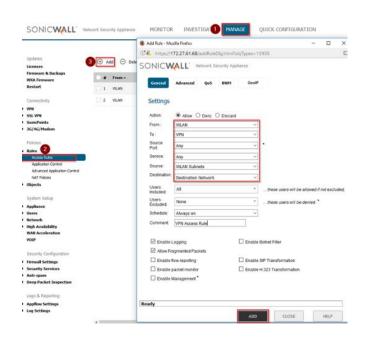
> Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01



destination network is the remote network that is reached through the VPN. The service on this rule by default should be set to Any. The second rule should be from zone VPN to zone WLAN. It should have the source network as the remote VPN network and the destination network should be the WLAN subnet, W0 subnet or the wireless subnet in question. Please see the screen shots below.

Login to Sonicwall Device.

- 1. Click Manage in the top navigation menu
- 2. Click on Rules | Access Rules
- 3. Click on Add and Create the rule as below



General	Advanced QoS BWM	GeolP	
Settings			
Action:	● Allow ○ Deny ○ Disca	rd	
From :	VPN	~	
To :	WLAN	~	
Source Port	Any	•	
Service:	Any	~	
Source:	Destination Network	~	
Destination:	WLAN Subnets	~	
Users Included:	All	* these users will be allowed if not excluded,	
Users Excluded:	None	* these users will be denied.	
Schedule:	Always on	~	
Comment	VPn Access Rule		
Enable Logging		Enable Botnet Filter	
Allow Fra	agmented Packets		
Enable flow reporting		Enable SIP Transformation	
Enable packet monitor		Enable H.323 Transformation	
Enable M	lanagement *		
Beady			
Ready			
		ADD CLOSE HELP	

