

# Cisco RV120W

## Disable SIP ALG

The screenshot shows the Cisco RV120W WebUI interface. The top header displays the Cisco logo and the device model: "Small Business RV 120W Wireless-N VPN Firewall". On the left, a navigation menu is visible with the following items: "Getting Started", "Status", "Networking", "Wireless", "Firewall" (highlighted), "Basic Settings" (expanded), "Access Control", "VPN", "Security", "QoS", and "Administration". Under "Basic Settings", the following sub-items are listed: "Attack Checks", "UPnP", "SIP ALG" (underlined), "Port Triggering", "Port Forwarding", "Session Settings", "Remote Management", and "One-to-One NAT". The main content area is titled "SIP ALG" and contains the "SIP ALG Settings" section. In this section, the "SIP ALG" checkbox is checked, and a red circle highlights the checkbox. Below the settings, there are "Save" and "Cancel" buttons.

## UDP Timeout

The screenshot displays the configuration interface for a Cisco RV 120W Wireless-N VPN Firewall. The left sidebar contains a navigation menu with the following items: Getting Started, Status, Networking, Wireless, Firewall (selected), Basic Settings (expanded), Attack Checks, UPnP, SIP ALG, Access Control, Port Triggering, Port Forwarding, Session Settings (underlined), Remote Management, One-to-One NAT, VPN, Security, QoS, and Administration. The main content area is titled "Session Settings" and contains the following configuration items:

Parameter	Value	Range / Default
Maximum Unidentified Sessions:	32	(Range: 2 - 128, Default: 32)
Maximum Half Open Sessions:	128	(Range: 0 - 3000, Default: 128)
TCP Session Timeout Duration:	1800	Seconds (Range: 0 - 4294967, Default: 1800)
UDP Session Timeout Duration:	300	Seconds (Range: 0 - 34294967, Default: 120)
Other Session Timeout Duration:	60	Seconds (Range: 0 - 34294967, Default: 60)
TCP Session Cleanup Latency:	10	Seconds (Range: 0 - 34294967, Default: 10)

At the bottom of the configuration area, there are two buttons: "Save" and "Cancel".

## Attack Checks

Small Business  
Cisco **RV 120W Wireless-N VPN Firewall**

- Getting Started
- ▶ Status
- ▶ Networking
- ▶ Wireless
- ▶ Firewall
  - ▶ Basic Settings
  - ▶ Access Control
    - Port Triggering
    - Port Forwarding
    - Session Settings
    - Remote Management
    - One-to-One NAT
- ▶ VPN
- ▶ Security
- ▶ QoS
- ▶ Administration

### Attack Checks

**ICSA Settings**

Respond to Ping on Internet:  Enable

Stealth Mode:  Enable

Block TCP flood:  Enable

**LAN Security Checks**

Block UDP flood:  Enable

**ICSA Settings**

Block ICMP Notification:  Enable

Block Fragmented Packets:  Enable

Block Multicast Packets:  Enable

**Save** **Cancel**