

如何在 SonicWALL 上配置 每 IP 带宽管理

配置手册

版本 1.0.0

Question/Topic

UTM: 如何在 SonicWALL 上配置每 IP 带宽管理

Answer/Article

本文适用于:

涉及到的 Sonicwall 防火墙

Gen5: NSA E7500, NSA E6500, NSA E5500, NSA 5000, NSA 4500, NSA 3500, NSA 2400, NSA 240

Gen5 TZ 系列: TZ 100, TZ 100 Wireless, TZ 200, TZ 200 W, TZ 210, TZ 210 Wireless

固件/软件版本: SonicOS 5.8.2 增强版以及更新版本

服务: BWM, App Rules

功能与应用

本文介绍了如何在 SonicWALL 防火墙上配置带宽管理。以 HTTP 下载为例，对整个局域网用户的总带宽进行限制，并针对每个用户进行更精确的限制

步骤

1. 登录 SonicWALL 防火墙
2. 进入 **System->Status** 页面，确保有 **App Control** 的 license

Security Services	
Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
SSL VPN Nodes/Users	Licensed 27 Nodes (0 in use)
Virtual Assist Nodes/Users	Licensed 2 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Licensed - 50 Licenses (0 in use)
CFS (Content Filter)	Licensed
Client AV Enforcement	Not Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
App Control	Licensed
App Visualization	Licensed
Anti-Spam	Not Licensed
ViewPoint	Not Licensed
DPI-SSL	Not Licensed

3. 进入 **Firewall Settings->BWM** 页面，将 **Bandwidth Management Type** 选择为 **Advanced** 模式

Firewall Settings /

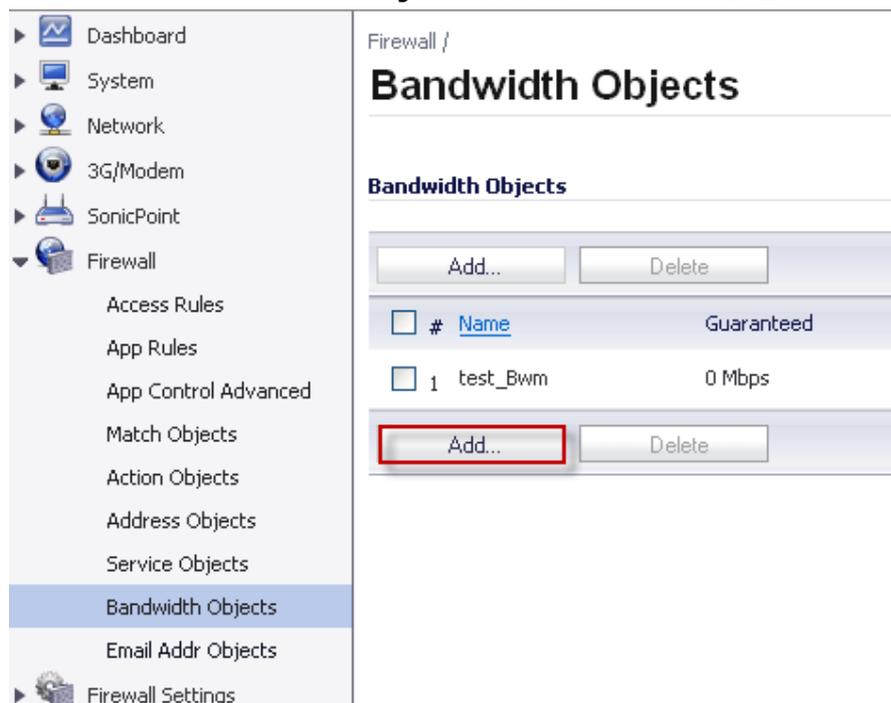
BWM

Accept Cancel

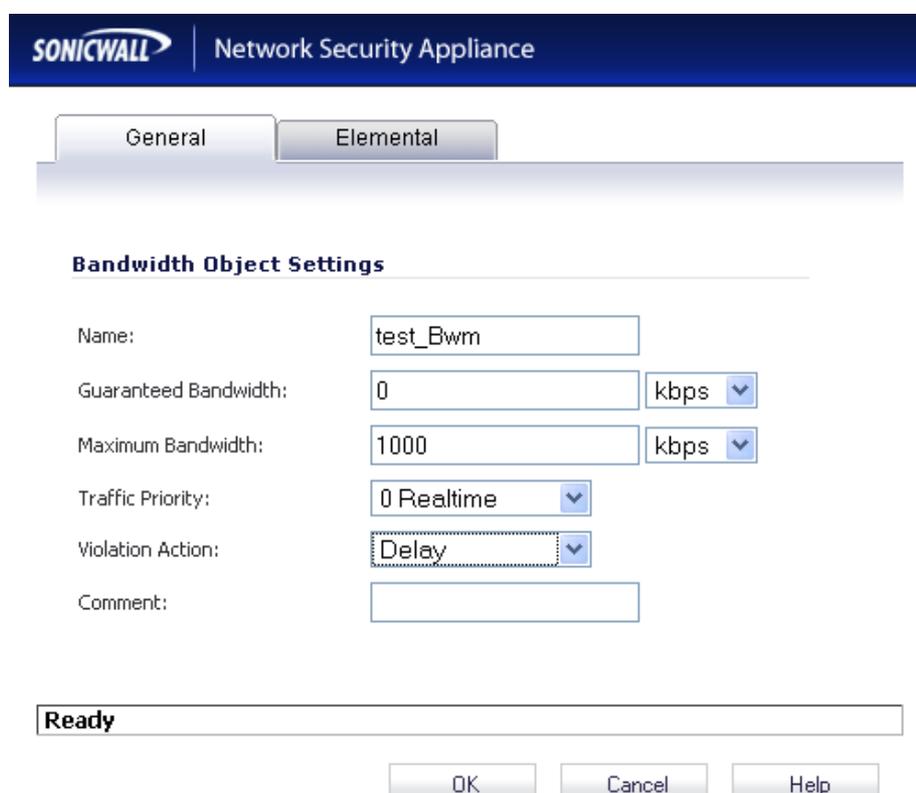
Bandwidth Management Type: Advanced Global None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

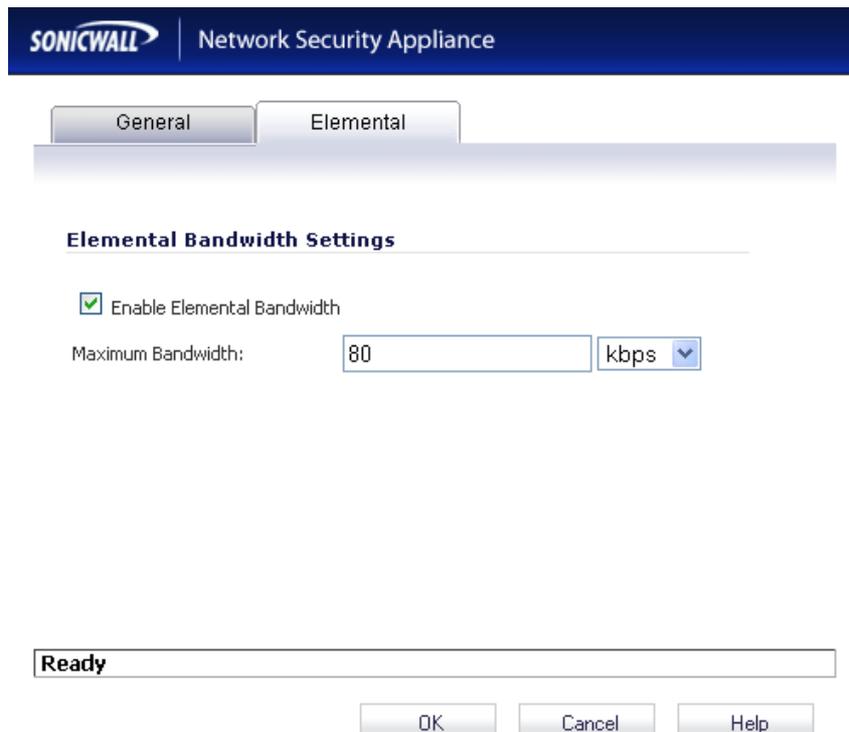
4. 进入 **Firewall->Bandwidth Objects** 页面，点击 **Add...**按钮



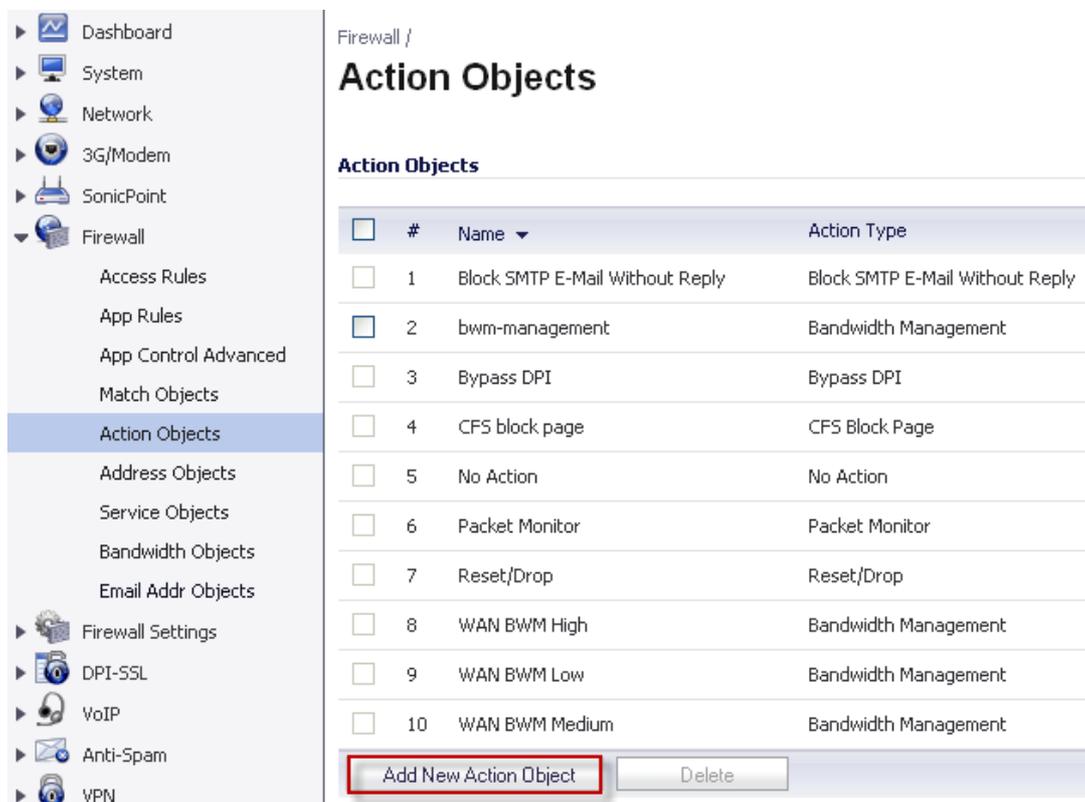
5. 进入 **General** 选项卡，将带宽对象命名为 **test_Bwm**，配置相应的带宽保证参数，有 **Guaranteed Bandwidth** 即保证带宽，**Maximum Bandwidth** 即最大带宽，单位可以选择 kbps 或者 Mbps，在 **Traffic Priority** 中选择优先级，0 Realtime 代表实时流量，在 **Violation Action** 中可以选择 Delay 即带宽管理产生冲突时延时执行，或者选择 Drop 直接断开连接



6. 在 **Elemental** 选项卡，启用 **Enable Elemental Bandwidth** 可以对每个 IP 的最大带宽进行限制，本例中设为 80kbps



7. 点击 **OK** 完成配置
8. 进入 **Firewall->Action Objects** 页面，点击 **Add New Action Object** 按钮



9. 将该 **Action Object** 命名为 bwm-management, 在 **Action** 中选择 Bandwidth Management, 启用 **Enable Egress/Ingress Bandwidth Management**, 在 **Bandwidth Object** 中选择之前配置的 test_Bwm 带宽对象

The screenshot shows the 'Action Object Settings' window for a SonicWall Network Security Appliance. The 'Action Name' is 'bwm-management'. The 'Action' is set to 'Bandwidth Management'. The 'Bandwidth Aggregation Method' is 'Per Policy'. Both 'Enable Egress Bandwidth Management' and 'Enable Ingress Bandwidth Management' are checked, with 'test_Bwm' selected as the 'Bandwidth Object' for both. 'Enable Tracking Bandwidth Usage' is unchecked. A note at the bottom states: 'Note: BWM Type: Advanced; To change go to Firewall Settings > BWM'. The status bar shows 'Ready' and there are 'OK', 'Cancel', and 'Help' buttons.

10. 进入 **Firewall->Match Objects** 页面, 点击 **Add New Match Object** 按钮为 HTTP 下载添加一个 Match Object, 将该 Match Object 命名为 HTTP_DOWNLOAD, 在 **Match Object Type** 中选择 Application Category List, 在 **Application Categories** 中选择 FILE-TYPES-HTTP, 点击 **Add** 按钮将 FILE-TYPES-HTTP 添加到 List 列表中

The screenshot shows the 'Match Object Settings' window for a SonicWall Network Security Appliance. The 'Object Name' is 'HTTP_DOWNLOAD'. The 'Match Object Type' is 'Application Category List'. The 'Application Categories' dropdown is set to 'FILE-TYPES-HTTP (72)'. Below this, a list box contains 'FILE-TYPES-HTTP (72)'. To the right of the list box are four buttons: 'Add' (highlighted with a red border), 'Update', 'Remove', and 'Remove All'. The status bar shows 'List:'.

11. 点击 **OK** 完成配置

12. 进入 **Firewall->App Rules** 页面，启用 **Enable App Rules**

Firewall /

App Rules

App Rules Status

App Rules Status

App Control License Expiration Date:

01/27/2013

App Rules Global Settings

Enable App Rules:

Global Log Redundancy Filter (seconds):

0

13. 点击 **Add New Policy** 按钮为 HTTP 下载的带宽限制添加一条策略，命名为 http_bwm_test, 在 **Policy Type** 中选择 App Control Content, 在 **Match Object** 中选择 HTTP_DOWNLOAD, 在 **Action Object** 中选择 bwm-management



Network Security Appliance

App Control Policy Settings

Policy Name:	<input type="text" value="http_bwm_test"/>
Policy Type:	<input type="text" value="App Control Content"/>
Address:	<input type="text" value="Any"/>
Exclusion Address:	<input type="text" value="None"/>
Match Object:	<input type="text" value="HTTP_DOWNLOAD"/>
Action Object:	<input type="text" value="bwm-management"/>
	Included: <input type="text" value="All"/>
	Excluded: <input type="text" value="None"/>
Users/Groups:	<input type="text" value="All"/>
Schedule:	<input type="text" value="Always on"/>
Enable flow reporting:	<input type="checkbox"/>
Enable Logging:	<input checked="" type="checkbox"/>
Log individual object content:	<input type="checkbox"/>
Log using App Control message format:	<input checked="" type="checkbox"/>
Log Redundancy Filter (seconds):	<input checked="" type="checkbox"/> Use Global Settings <input type="text" value="0"/>
Zone:	<input type="text" value="Any"/>

Note: BWM Type: Advanced; To change go to [Firewall Settings > BWM](#)

Ready

OK

Cancel

Help

14. 点击 **OK** 完成配置

提示： 本文的配置针对的是整个局域网。如果想要对局域网中某个网段进行带宽管理，可以在上图的 **Address** 下拉菜单中选择相应的网段

测试

用迅雷下载 HTTP 的速度被限制在了 $10\text{KB/s}=80\text{Kbps}$ （第 6 步）

