

如何配置 **Application Control Advanced** 禁止访问某些网站

配置手册

版本 1.0.0

Question/Topic

UTM: 如何配置 Application Control Advanced 禁止访问某些网站

Answer/Article

本文适用于:

涉及到的 Sonicwall 防火墙

Gen5: NSA E8500, NSA E7500, NSA E6500, NSA E5500, NSA 5000, NSA 4500, NSA 3500, NSA 2400, NSA 240

Gen5 TZ 系列: TZ 210, TZ 210 Wireless

固件/软件版本: SonicOS 5.8.0.0 增强版以及更新版本

Gen5 TZ 系列: TZ 200, TZ 200 Wireless, TZ100, TZ100 Wireless

固件/软件版本: SonicOS 5.8.0.2 增强版以及更新版本

服务: App Control, App Rules

功能与应用

本特征码数据库之前集成在 SonicWALL Intrusion Prevention Service (IPS) 中, 现在已经划入到 Application Control 中。这些特征码数据库可以保护使用者免受蠕虫、木马、间谍软件和后门的攻击。Application Control Advanced 里的设置作为全局策略, 独立于任何其他自定义的 App Rule Policy。本文演示了如何禁止三大社交网站: Facebook、Orkut 和 Myspace

步骤

1. 登陆 SonicWALL 防火墙
2. 进入 **Firewall->App Control Advanced** 页面
3. 勾选 **Enable App Control**, 点击 **Accept** 按钮

Firewall /

App Control Advanced

Accept Cancel

App Control Status

App Control Status	
App Signature Database:	Downloaded
App Signature Database Timestamp:	UTC 04/06/2011 16:07:16.000 <input type="button" value="Update"/>
Last Checked:	04/07/2011 18:53:46.880
App Signature DB Expiration Date:	05/07/2011
Note: Enable App Control per zone from the Network > Zones page.	

App Control Global Settings

Enable App Control

4. 在 **View Style: Category** 里选择 SOCIAL NETWORKING
5. 在 **Application** 里依次选择需要禁止的网站, 在本例中选择 Facebook

App Control Global Settings

Enable App Control

App Control Advanced

View Style: Category: **SOCIAL-NETWORKING** Application: **Facebook** Viewed By: **Application**

#	Application	Block	Log	Comments	Configure
1	Facebook				<input type="button" value="Configure"/>

6. 点击 **Configure** 按钮，在弹出的窗口中将 **Block** 和 **Log** 设置为 **Enable**

SONICWALL | Network Security Appliance

App Control App Settings

App Category: SOCIAL-NETWORKING

App Name: Facebook

Block: Enable

Log: Enable

Included Users/Groups: Use Category Settings (All)

Excluded Users/Groups: Use Category Settings (None)

Included IP Address Range: Use Category Settings (All)

Excluded IP Address Range: Use Category Settings (None)

Schedule: Use Category Settings (Always On)

Log Redundancy Filter (seconds): Use Category Settings 0

Ready

OK Cancel Help

7. 点击 **OK** 按钮完成配置

8. 依次为 **Orkut** 和 **Myspace** 进行相同的配置

测试

连接在 SonicWALL 防火墙后面的将 PC 访问 www.facebook.com, www.myspace.com 和 www.orkut.com, 并且日志将会记录如下:

Log View Refresh Interval (secs) 10 Items per page

#	Time	Priority	Category	Message	Source	Destination	Notes
1	04/07/2011 19:23:19.416	Alert	Application Control	Application Control Prevention Alert: SOCIAL-NETWORKING MySpace -- Browsing Attempt, SID: 827, AppID: 301, CatID: 76	192.168.168.65, 3259, X0 (admin)	216.178.39.11, 80, X1	
2	04/07/2011 19:22:28.176	Alert	Application Control	Application Control Prevention Alert: SOCIAL-NETWORKING Orkut -- Browsing Activity, SID: 1734, AppID: 602, CatID: 76	192.168.168.65, 3210, X0 (admin)	72.14.213.85, 80, X1	