# 配置 **App Rules** 限制在线视频流量

配置手册

**版本 1.0.0**

# Question/Topic

UTM: 如何配置 App Rules 限制在线视频流量

# 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 2400MX, NSA 240
**Gen5 TZ 系列:** TZ 210, TZ 210 Wireless
**Gen4: PRO 系列:** PRO 5060, PRO 4100, PRO 4060, PRO 3060
**固件/软件版本:** SonicOS 4.0 增强版以及更新版本（TZ 210 SonicOS 5.5 增强版以及更新版本）
**服务:** BWM, App Rules

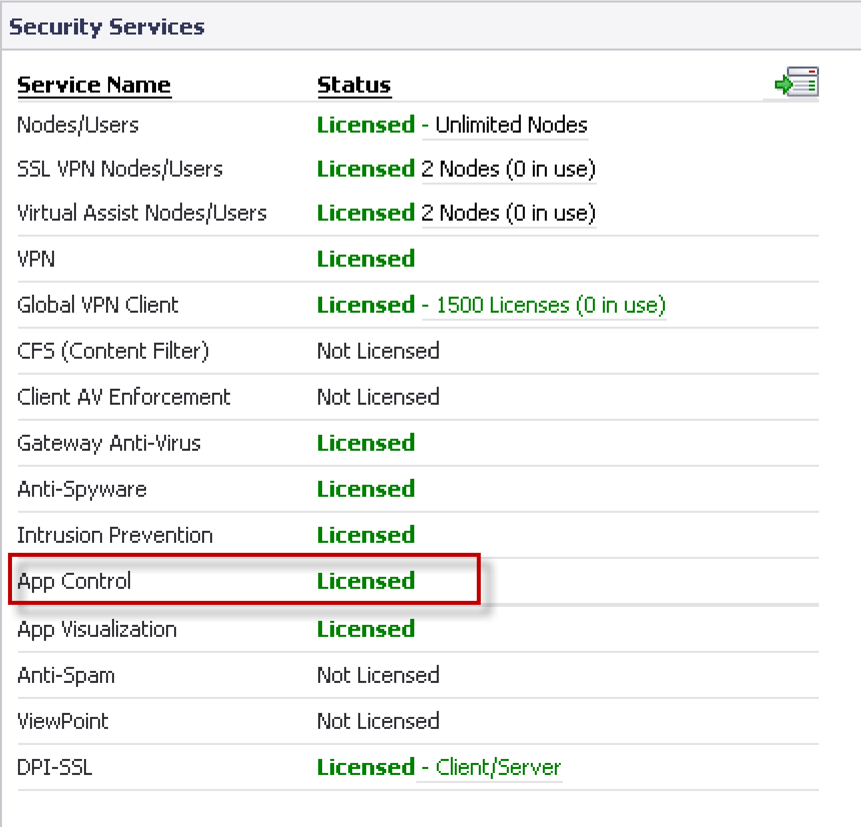
功能与应用

App Rules 扫描正在通过网关的应用层流量，并且查询与关键字匹配的内容，对其进行限制。该内容可以是文本也可以是二进制文件。在配置 App Rules 时，可以定义根据应用的类型、方向、内容或者关键字进行匹配，并针对不同的用户或者域名进行操作。
在线视频流量会消耗大量的带宽资源，本文介绍了如何通过 App Rules 对在线视频流量进行带宽管理

# 步骤

## 查看许可证

1. 登录 SonicWALL 防火墙，进入 **System->Status** 页面
2. 确认 **App Control** 已经获得许可证

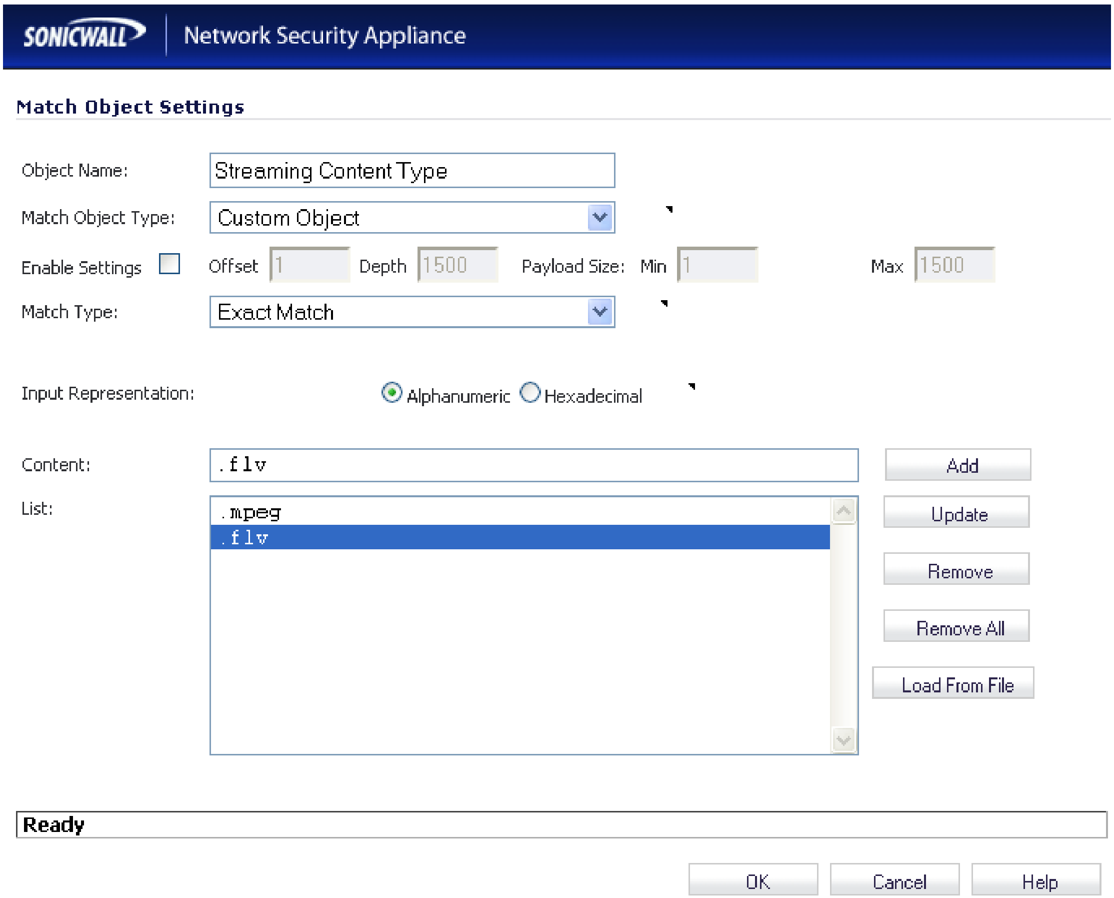


Security Services

| Service Name | Status |
|---|---|
| Nodes/Users | Licensed - Unlimited Nodes |
| SSL VPN Nodes/Users | Licensed 2 Nodes (0 in use) |
| Virtual Assist Nodes/Users | Licensed 2 Nodes (0 in use) |
| VPN | Licensed |
| Global VPN Client | Licensed - 1500 Licenses (0 in use) |
| CFS (Content Filter) | Not 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 | Licensed - Client/Server |

## 定义 Match Objects

1. 进入 **Firewall->Match Objects** 页面
2. 点击 **Add New Match Object** 按钮
3. 设置对象名称，在 **Match Object Type** 中选择 Custom Object，在 **Match Type** 中选择 Exact Match，在 **Content** 中输入需要限制的视频格式类型，点击右边的 **Add** 按钮添加到 **List** 中



Match Object Settings

Object Name: Streaming Content Type

Match Object Type: Custom Object

Enable Settings ☐ Offset 1 Depth 1500 Payload Size: Min 1 Max 1500

Match Type: Exact Match

Input Representation: ● Alphanumeric ○ Hexadecimal

Content: .flv

List:
.mpeg
.flv

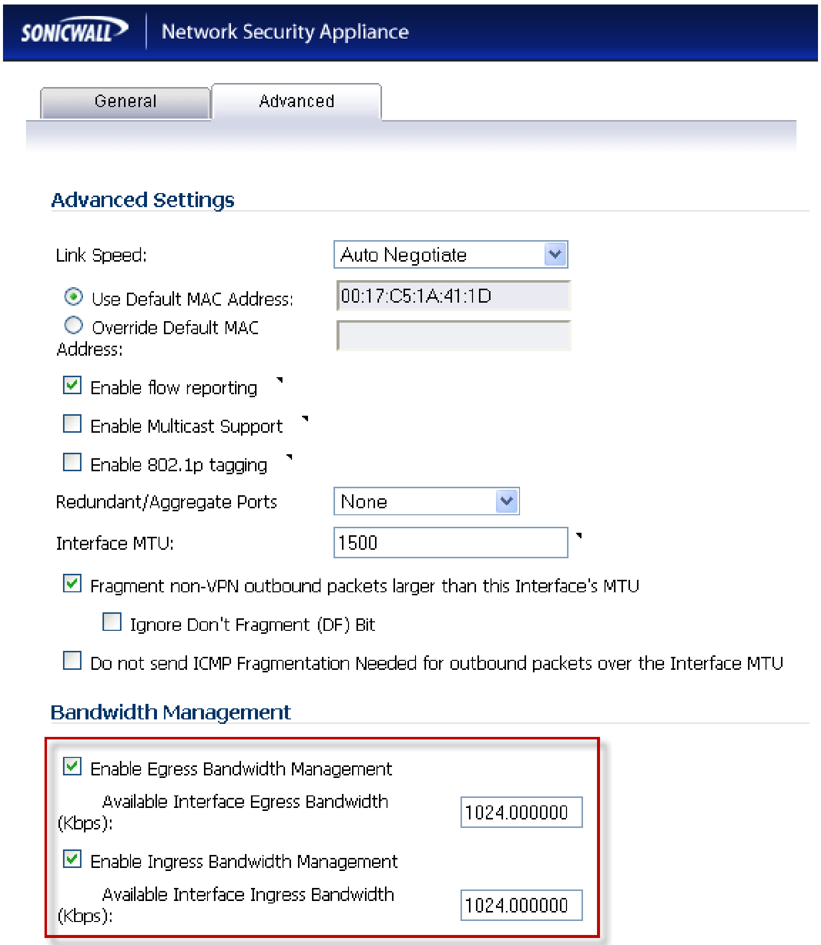
Ready

上图列出了四个常用视频类型，除此以外还有

| Media-Type | Description |
|---|---|
| **vedio/mpeg** | MPEG-1 video with multiplexed audio; Defined in RFC 2045 and RFC 2046 |
| **vedio/mp4** | MP4 video; Defined in RFC 4337 |
| **vedio/ogg** | Ogg Theora or other video(with audio); Defined in RFC 5334 |
| **vedio/quicktime** | QuickTime open media format |
| **vedio/webm** | WebM open media format |
| **vedio/x-ms-wmv** | Windows Media Video; Documented in Microsoft KB 288102 |

## 设置 WAN 接口带宽

1. 进入 **Network->Interfaces** 页面
2. 点击 WAN 接口右边的 **Configure** 按钮
3. 在 **Advanced** 选项卡，启用 Enable Egress/Ingress Bandwidth Management，在 Available Interface Egress/Ingress Bandwidth 中输入运营商提供的带宽



Advanced Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: 00:17:C5:1A:41:1D

○ Override Default MAC Address:

☑ Enable flow reporting

□ Enable Multicast Support

□ Enable 802.1p tagging

Redundant/Aggregate Ports None

Interface MTU: 1500

☑ Fragment non-VPN outbound packets larger than this Interface's MTU

□ Ignore Don't Fragment (DF) Bit

□ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

☑ Enable Egress Bandwidth Management

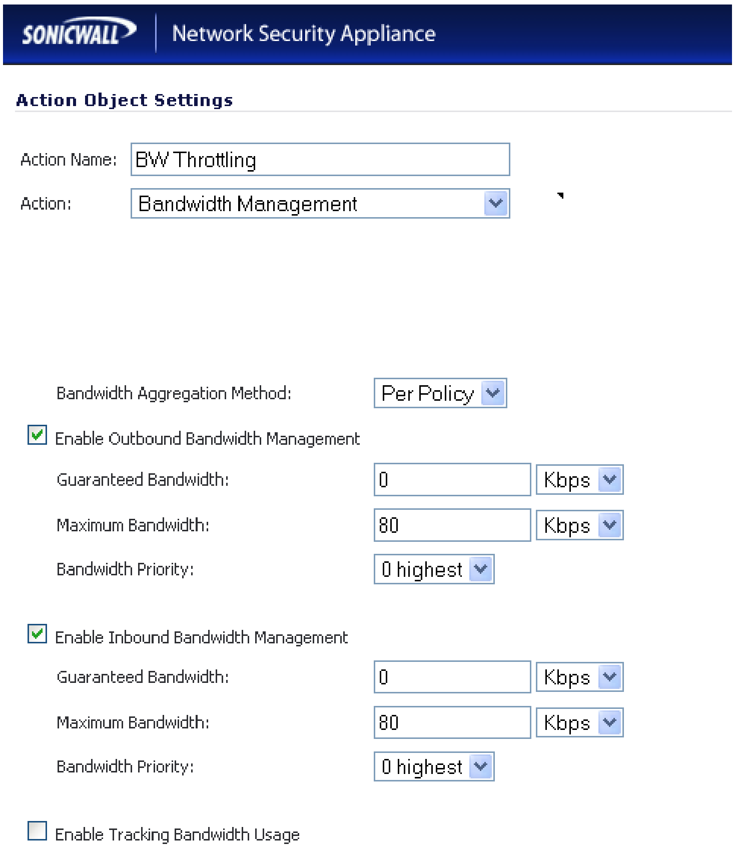
Available Interface Egress Bandwidth (Kbps): 1024.000000

☑ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 1024.000000

## 定义 Action Objects

1. 进入 **Firewall->Action Object** 页面
2. 点击 **Add New Action Object** 按钮
3. 设置对象名称，在 **Action** 中选择 Bandwidth Management，启用 Enable Outbound/Inbound Bandwidth Management，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



Action Object Settings

Action Name: BW Throttling

Action: Bandwidth Management

Bandwidth Aggregation Method: Per Policy

☑ Enable Outbound Bandwidth Management

Guaranteed Bandwidth: 0 Kbps

Maximum Bandwidth: 80 Kbps

Bandwidth Priority: 0 highest

☑ Enable Inbound Bandwidth Management

Guaranteed Bandwidth: 0 Kbps

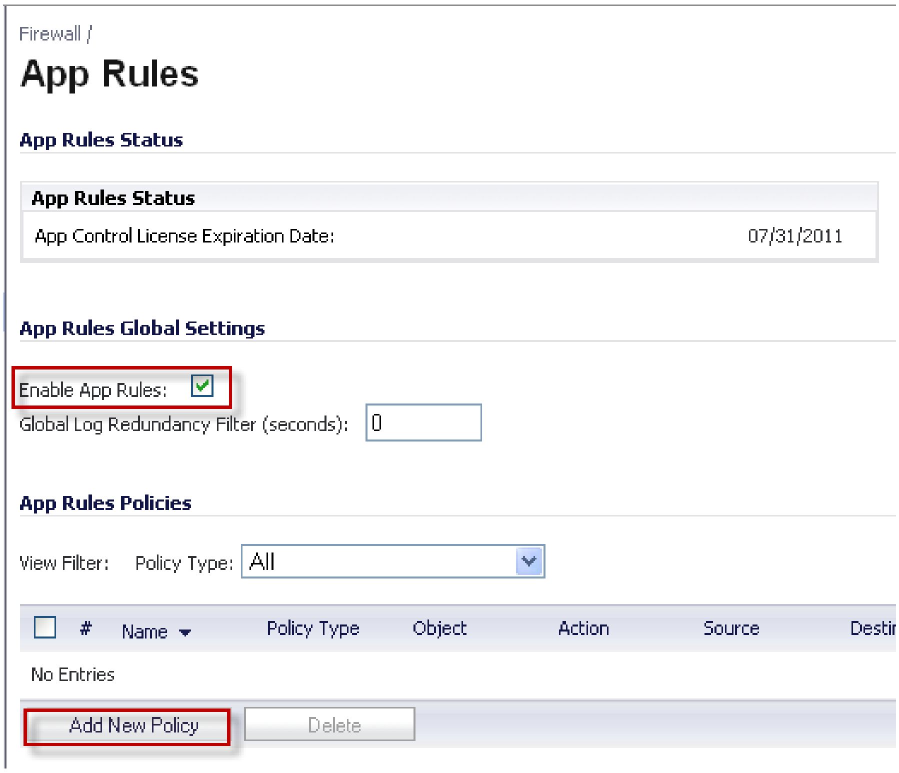
Maximum Bandwidth: 80 Kbps

Bandwidth Priority: 0 highest

□ Enable Tracking Bandwidth Usage

## 添加 App Rules Policy

1. 进入 **Firewall->App Rules** 页面
2. 启用 **Enable App Rules**，点击 **Add New Policy** 按钮



Firewall /

App Rules

App Rules Status

App Rules Status

App Control License Expiration Date: 07/31/2011

App Rules Global Settings

Enable App Rules: ☑

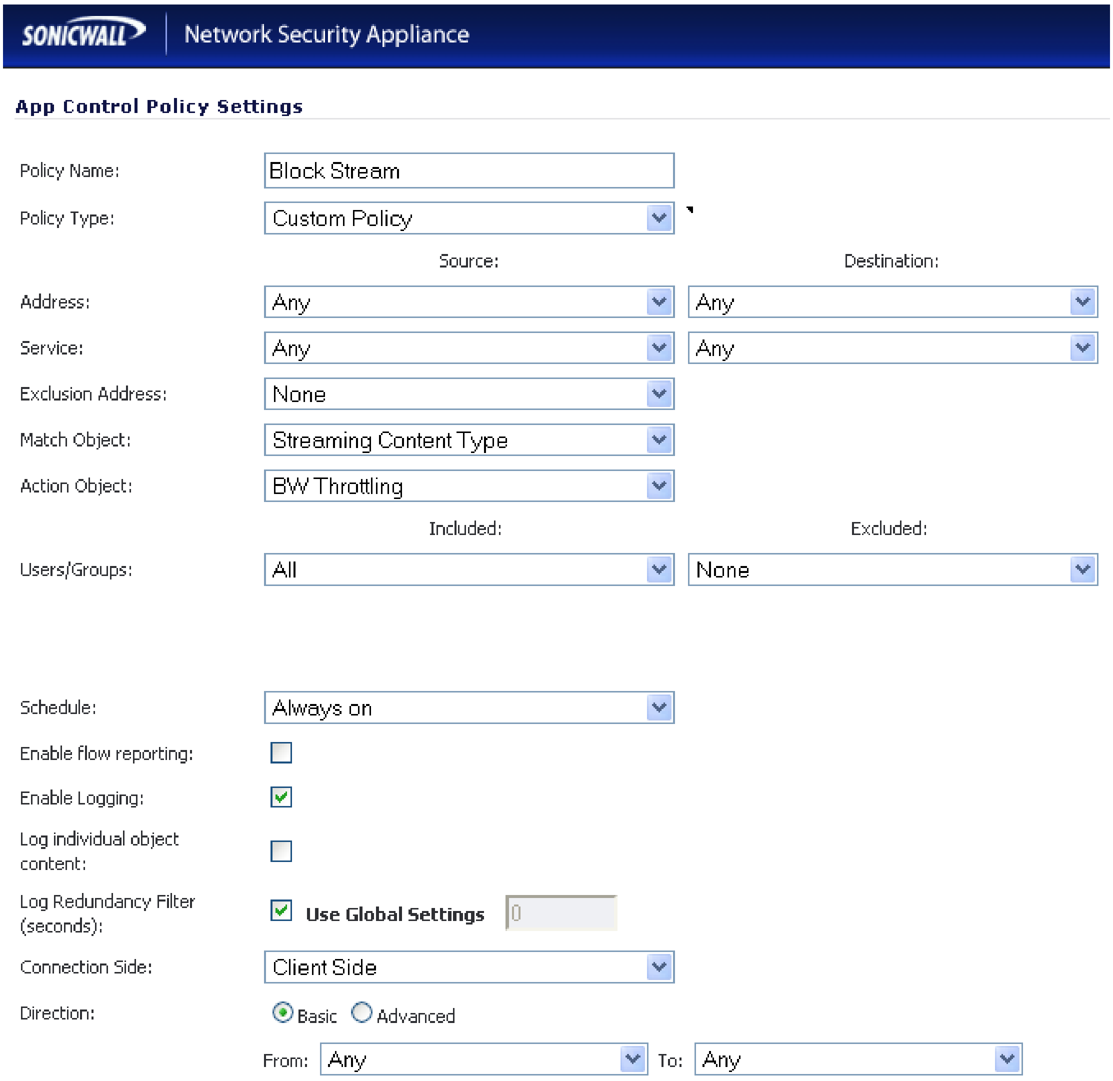
Global Log Redundancy Filter (seconds): 0

App Rules Policies

View Filter: Policy Type: All

| □ | # | Name | Policy Type | Object | Action | Source | Destir |
|---|---|---|---|---|---|---|---|
| No Entries | | | | | | | |

3. 设置策略名称，在 **Policy Type** 中选择 Custom Policy，在 **Match Object** 中选择 Streaming Content Type，在 **Action Object** 中输入 BW Throttling

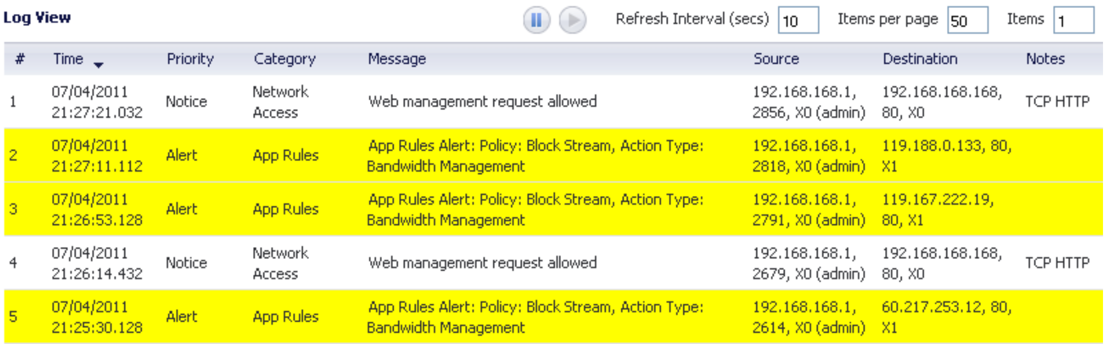


App Control Policy Settings

| | | |
|---|---|---|
| Policy Name: | Block Stream | |
| Policy Type: | Custom Policy | |
| | Source: | Destination: |
| Address: | Any | Any |
| Service: | Any | Any |
| Exclusion Address: | None | |
| Match Object: | Streaming Content Type | |
| Action Object: | BW Throttling | |
| | Included: | Excluded: |
| Users/Groups: | All | None |
| Schedule: | Always on | |
| Enable flow reporting: | □ | |
| Enable Logging: | ☑ | |
| Log individual object content: | □ | |
| Log Redundancy Filter (seconds): | ☑ Use Global Settings 0 | |
| Connection Side: | Client Side | |
| Direction: | ● Basic ○ Advanced | |
| | From: Any | To: Any |

## 测试

1. 登录 http://www.youku.com，打开一个视频，在 **log->View** 中会出现以下信息，代表 App Rules 策略已经匹配到视频流量


Log View

Refresh Interval (secs) 10 Items per page 50 Items 1

| # | Time | Priority | Category | Message | Source | Destination | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 07/04/2011 21:27:21.032 | Notice | Network Access | Web management request allowed | 192.168.168.1, 2856, X0 (admin) | 192.168.168.168, 80, X0 | TCP HTTP |
| 2 | 07/04/2011 21:27:11.112 | Alert | App Rules | App Rules Alert: Policy: Block Stream, Action Type: Bandwidth Management | 192.168.168.1, 2818, X0 (admin) | 119.188.0.133, 80, X1 | |
| 3 | 07/04/2011 21:26:53.128 | Alert | App Rules | App Rules Alert: Policy: Block Stream, Action Type: Bandwidth Management | 192.168.168.1, 2791, X0 (admin) | 119.167.222.19, 80, X1 | |
| 4 | 07/04/2011 21:26:14.432 | Notice | Network Access | Web management request allowed | 192.168.168.1, 2679, X0 (admin) | 192.168.168.168, 80, X0 | TCP HTTP |
| 5 | 07/04/2011 21:25:30.128 | Alert | App Rules | App Rules Alert: Policy: Block Stream, Action Type: Bandwidth Management | 192.168.168.1, 2614, X0 (admin) | 60.217.253.12, 80, X1 | |