Tech Note--Audit Support for Palo Alto Firewalls

Symantec CloudSOC Tech Note

Copyright statement

Table of Contents

Introduction

This Tech Note describes how the CloudSOC Audit application supports log files from Palo Alto Networks firewall devices.

Minimum supported version

The minimum supported version for Palo Alto firewall is PAN-200.

Palo Alto log formats

Palo Alto firewalls produce several types of log files. The two log formats that are required by the CloudSOC Audit application are Traffic and URL or URL Filtering logs. In near future, we would also be adding support to extract information from other types of logs such as 'THREATs'.

Palo Alto Network firewall generates separate Traffic and URL log files. Both files should be combined in a single archive before upload or transfer to the CloudSOC Audit app.

Traffic log format

The following sections describe the heading row and required fields for the Traffic log, and shows typical examples in both CSV and Syslogs outputs.

Typical heading row

```
Domain,Receive Time,Serial #,Type,Threat/Content Type,Config Version,Generate
Time,Source address,Destination address,NAT Source IP,NAT Destination IP,Rule,Source
User,Destination User,Application,Virtual System,Source Zone,Destination Zone,Inbound
Interface,Outbound Interface,Log Action,Time Logged,Session ID,Repeat Count,Source
Port,Destination Port,NAT Source Port,NAT Destination Port,Flags,IP
Protocol,Action,Bytes,Bytes Sent,Bytes Received,Packets,Start Time,Elapsed Time
(sec),Category,Padding,seqno,actionflags,Source Country,Destination
Country,cpadding,pkts_sent,pkts_received
```

Required traffic log fields

The following table shows the traffic log fields required to get the most benefit from the Audit Application.

Field	**Value mandatory**
Receive Time	Yes
Threat/Content Type (Subtype in syslog doc)	Yes
Source address (Source IP in syslog doc)	Yes
Destination address (Destination IP in syslog doc)	Yes
NAT Source IP	
NAT Destination IP	
Application	
Source User	Desirable. Anonymize if you have privacy concerns
Session ID	Yes
Source Port	Yes
Destination Port	Yes
Action	
Bytes	Yes
Bytes Sent	Yes
Bytes Received	
Packets	Yes
Start Time	
Elapsed Time (sec)	Yes
Category	
pkts_sent	Yes
pkts_received	

CSV sample log

```
1,2013/05/21 16:00:00,007000001131,TRAFFIC,end,1,2013/05/21
16:00:01,192.168.1.53,192.168.1.15,,,Vwire Proxy
In,,,ssl,vsys1,Untrusted,Proxied,ethernet1/2,ethernet1/3,Verbose,2013/05/21
16:00:00,40345,1,56262,3128,0,0,0x0,tcp,allow,3992,1480,2512,24,2013/05/21
15:59:31,0,internet-communications,0,2518865,0x0,192.168.0.0-192.168.255.255,192.168.
0.0-192.168.255.255,0,13,11
```

Syslogs sample Log

```
May 22 00:00:06 syslog.abc.com 1,2014/05/22
06:59:59,001901000402,TRAFFIC,deny,1,2014/05/22
06:59:58,10.140.214.38,95.211.37.197,168.161.192.15,95.211.37.197,HR Legal Blocked
Applications,,,teamviewer-base,vsys1,inside,outside,ethernet1/22,ethernet1/21,Burbank
_syslog,2014/05/22
06:59:59,2058887,1,50722,80,30005,80,0x400000,tcp,deny,501,435,66,4,2014/05/22
06:59:59,0,any,0,29701895181,0x0,10.0.0.0-10.255.255.255,Netherlands,0,3,1
```

URL filtering log format

Typical heading row

```
Domain,Receive Time,Serial #,Type,Threat/Content Type,Config Version,Generate
Time,Source address,Destination address,NAT Source IP,NAT Destination IP,Rule,Source
User,Destination User,Application,Virtual System,Source Zone,Destination Zone,Inbound
Interface,Outbound Interface,Log Action,Time Logged,Session ID,Repeat Count,Source
Port,Destination Port,NAT Source Port,NAT Destination Port,Flags,IP
Protocol,Action,URL,Threat/Content
Name,Category,Severity,Direction,seqno,actionflags,Source Country,Destination
Country,cpadding,contenttype
```

Required URL filtering log fields

URL Filtering Logs fall under the broader category of ‘Threat Logs’. If the device is not configured to decrypt traffic, it can only generate URL logs for sites that were browsed with HTTP (not encrypted). URL Log information is essential to get the maximum benefit from Audit Application.

Log in to PAN User Interface and check the policies that allow traffic between the untrusted and trusted zones. Make sure you have logging enabled on it. For maximum detail in, enable traffic decryption policy on your network so that your firewall logs details of user sessions that are going over HTTPs.

The following table shows the URL filtering log fields required to get the most benefit from the Audit Application.

Field	Value Mandatory
Receive Time	
Threat / Content Type (Subtype in syslog doc)	Yes
Source address	Yes
Destination address	Yes
Application	
Session ID	Yes
Source Port	Yes
Destination Port	Yes
Action	Yes
URL	Yes
Category	
Direction	
contenttype	

CSV sample Log

```
1,2013/06/20 16:00:00,007000001131,THREAT,url,1,2013/06/20
15:59:54,192.168.1.53,192.168.1.15,,,Vwire Proxy
In,,,ssl,vsys1,Untrusted,Proxied,ethernet1/2,ethernet1/3,Verbose,2013/06/20
16:00:00,40443,1,56286,3128,0,0,0x8000,tcp,alert,"*.livechatinc.com/",(9999),internet
-communications,informational,client-to-server,58479,0x0,192.168.0.0-192.168.255.255,
192.168.0.0-192.168.255.255,0,
```

Syslogs sample log

```
May 22 00:00:09 syslog.abc.com 1,2014/05/22
06:59:59,001901000402,THREAT,url,1,2014/05/22
06:59:59,10.140.194.87,198.211.102.164,168.161.192.15,198.211.102.164,Allow
Outbound,elastica\xjjlee,,web-browsing,vsys1,inside,outside,ethernet1/22,ethernet1/21
,Burbank_syslog,2014/05/22
06:59:59,4030828,1,65056,80,39233,80,0x408000,tcp,alert,"api.readdle.com/api/ppcloud/
q/9/1/9132b2e5-20b2-4173-bf37-7bf60c8ad0df",(9999),business-and-economy,informational
,client-to-server,14734103362,0x0,10.0.0.0-10.255.255.255,United States,0,text/html
```

Exporting logs

Exporting logs from a shell on the firewall

To export logs from an SSH shell on the firewall using SCP, we recommend that you use an intermediate server as a staging point for your data instead of directly sending logs to CloudSOC servers. That way it will be easier to isolate any issues. The instructions below assume that:

- Your firewall ip is ‘firewall_ip_address'
- Your firewall admin account is 'admin_user_id'
- You have an SCP server called ‘your_scp_server' with user id of ‘your_user_id’

1. Log into your firewall

   ssh admin_user_id@firewall_ip_address

2. Export logs to a server that you have ssh access to. Change the time period depending on how much data your firewall has. This command may limit the amount of data you can export.

   scp export log traffic start-time equal 2014/01/01@12:00:00 end-time equal 2014/02/10@12:00:00 to your_user_id@your_scp_server:~/traffic.txt

3. Repeat above with other logs files.

   scp export log url start-time equal 2014/01/01@12:00:00 end-time equal 2014/02/10@12:00:00 to your_user_id@your_scp_server:~/url.txt

   scp export log threat start-time equal 2014/01/01@12:00:00 end-time equal 2014/02/10@12:00:00 to your_user_id@your_scp_server:~/threat.txt

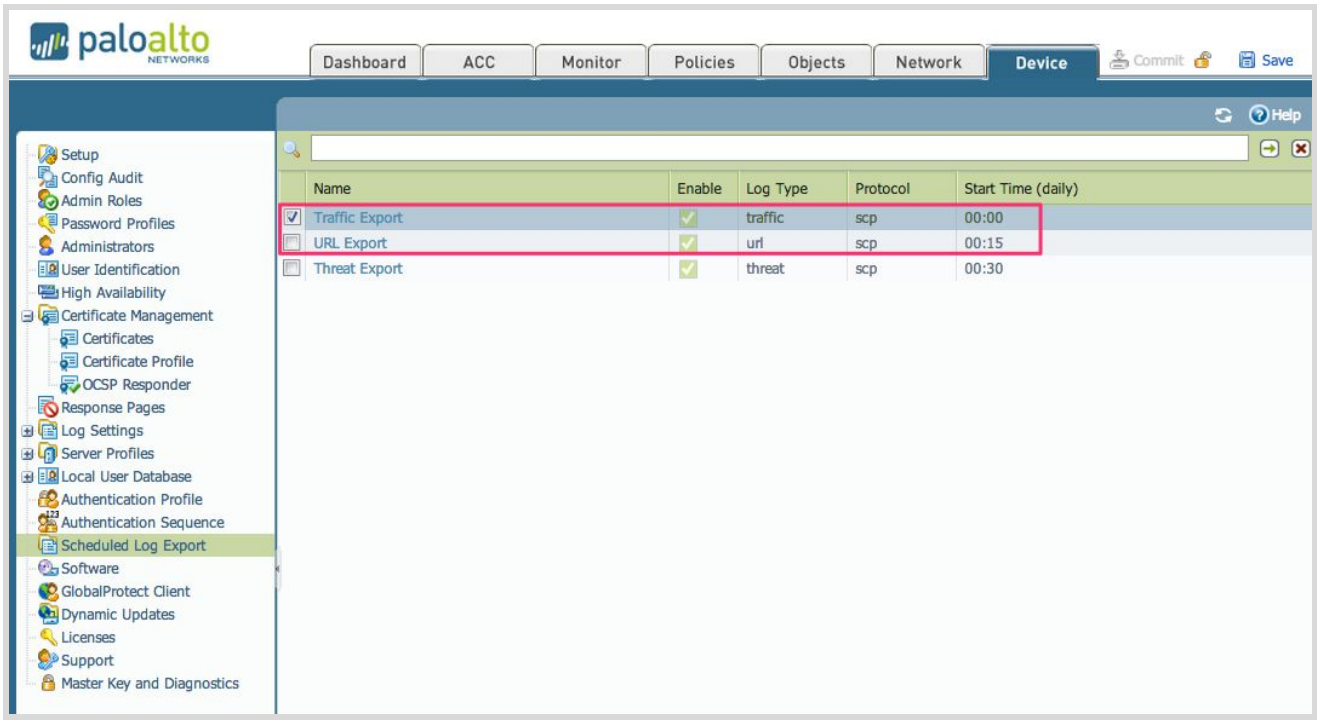
4. Log in to your server and copy the files to the CloudSOC servers using SFTP as described in the CloudSOC Tech Note *Managing Data Sources for the CloudSOC Audit App*.

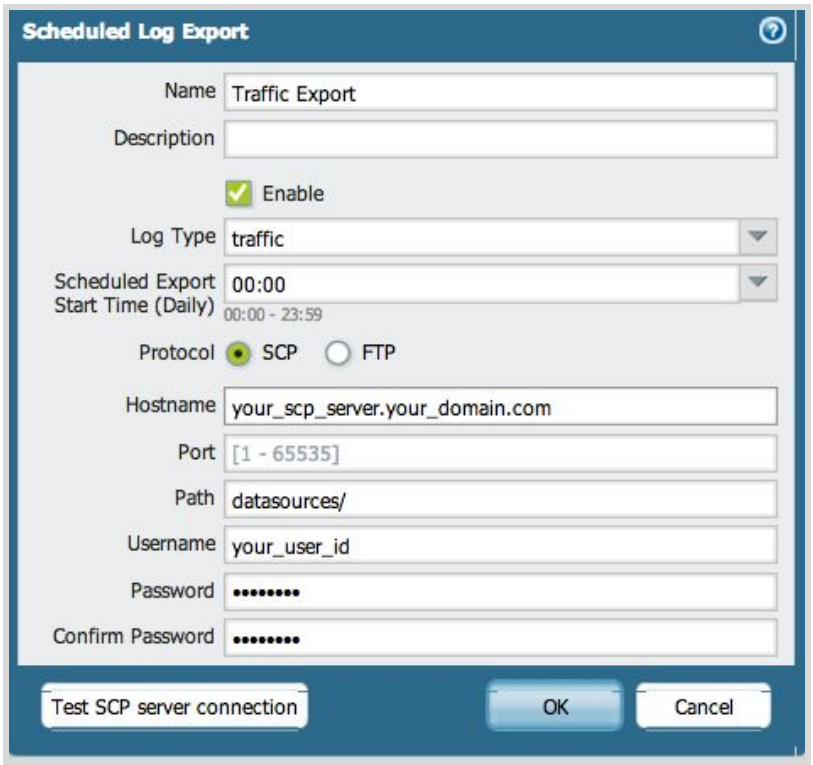
Using the scheduled log export feature

Important: Direct upload from PAN over SCP to the CloudSOC SCP servers is not supported because of PAN implementation of SCP where they try to run ssh commands. You can collect logs locally using a local SFTP/SCP server. You can also use a CloudSOC SpanVA on-premises virtual appliance, which can receive logs from PAN via FTP and SCP, compress and anonymize them, and send them to CloudSOC for use in the Audit application.

Palo Alto firewalls have a feature that lets them upload logs to an FTP or SCP server on a fixed schedule. This can be handy for transferring logs on daily basis. Log into the firewall and go to ‘Device’ configuration tab and select ‘Scheduled Log Export’.

Depending on its OS version, your Palo Alto firewall may not support SFTP transfers. When using scp export, it may require SSH access to the server as well and therefore may not be able to upload logs directly to CloudSOC servers. It is best that you either use an intermediate server as a staging point for your data instead of directly sending logs to CloudSOC servers or use CloudSOC SpanVA as an on-prem FTP/SFTP/Syslog Server. For more information, see the CloudSOC Tech Note *Installing and Configuring SpanVA*.


paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Save
Help
Setup
Config Audit
Admin Roles
Password Profiles
Administrators
User Identification
High Availability
Certificate Management
Certificates
Certificate Profile
OCSP Responder
Response Pages
Log Settings
Server Profiles
Local User Database
Authentication Profile
Authentication Sequence
Scheduled Log Export
Software
GlobalProtect Client
Dynamic Updates
Licenses
Support
Master Key and Diagnostics
Name
Enable
Log Type
Protocol
Start Time (daily)
Traffic Export
traffic
scp
00:00
URL Export
url
scp
00:15
Threat Export
threat
scp
00:30


Scheduled Log Export
Name
Traffic Export
Description
Enable
Log Type
traffic
Scheduled Export Start Time (Daily)
00:00
00:00 - 23:59
Protocol
SCP
FTP
Hostname
your_scp_server.your_domain.com
Port
[1 - 65535]
Path
datasources/
Username
your_user_id
Password
Confirm Password
Test SCP server connection
OK
Cancel

Using syslog export

Palo Alto firewalls can stream logs over syslog to a syslog server. You can use syslog in lieu of the file-based logging discussed previously. To send syslogs to CloudSOC Audit application, you can choose to deploy your own syslog server such as syslog-ng. In that case, you would need to write some scripts to periodically transfer the logs collected by your syslog server to CloudSOC using SFTP or SCP for processing. Check your syslog server's documentation on how you can achieve that.

A much simpler and efficient alternative is to use the CloudSOC SpanVA appliance as your syslog server. SpanVA not only acts as a syslog server to receive logs from your network devices, it can also anonymize them, compress the logs and transfer them to CloudSOC. See the CloudSOC Tech Note *Installing and Configuring SpanVA*.

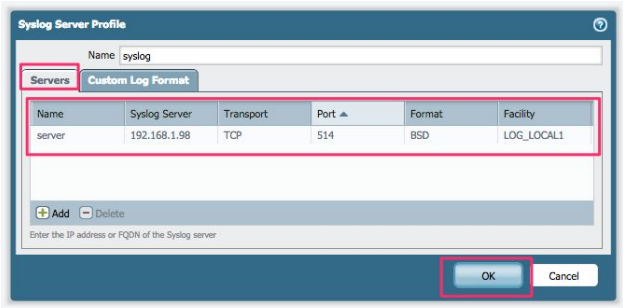
Setting Palo Alto syslog push to a syslog server involves four steps:

1. Creating a syslog server profile
2. Creating a log forwarding profile
3. Configure log formats
4. Updating security and decryption policies and URL filtering
5. Save and commit the changes

These steps are described in the following sections.

Creating a syslog server profile

1. Log into the firewall and open the admin console.
2. Open the **Device** tab and navigate to **Server Profiles** > **Syslog** in the side menu.
3. Click **Add** to add a new server profile.



4. Enter the information for your syslog server.

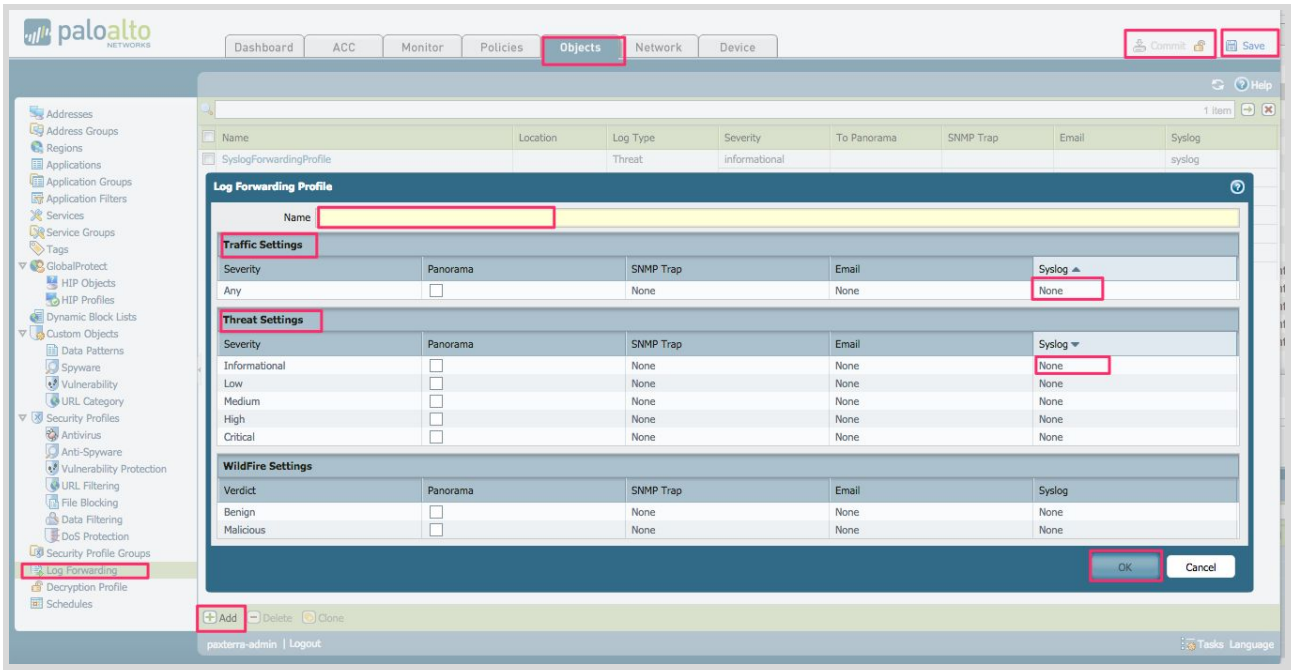
   If you are using CloudSOC SpanVA as the syslog server, you get the information from the CloudSOC Create SpanVA datasource panel. In CloudSOC, choose **Audit** > **Sources** and choose **+ New Data Source** > **SpanVA Datasource** to create a new data source. "Syslog Server" will be the IP address of the SpanVA appliance and the port it is listening on. Set Transport to either TCP or UDP.

If you are using a different syslog server, you should set it to match your syslog server IP and port number (usually port 514).

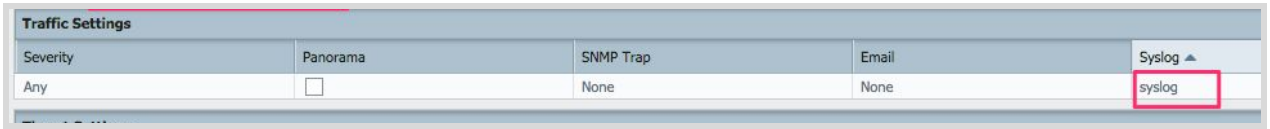
5. Click **OK**.

Create a log forwarding profile

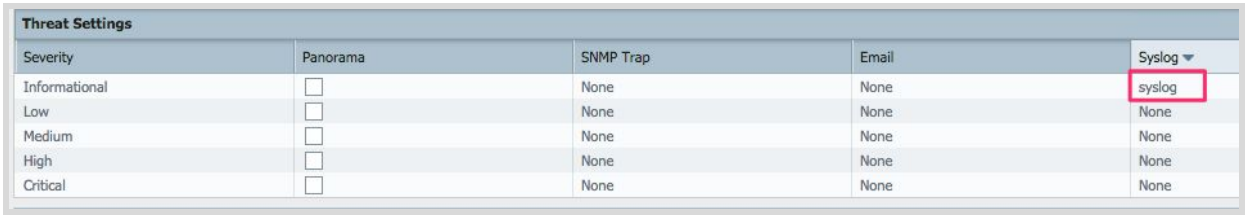
1. Open the **Objects** tab and navigate to **Log Forwarding** in the side menu.



2. Click **Add** to create a new log forwarding profile.
3. For **Name**, enter a descriptive name.
4. Under Traffic Settings, locate the row for Any and set the syslog column to **syslog**.



5. Under Threat Settings, locate the row for Informational and set the syslog column to **syslog**.

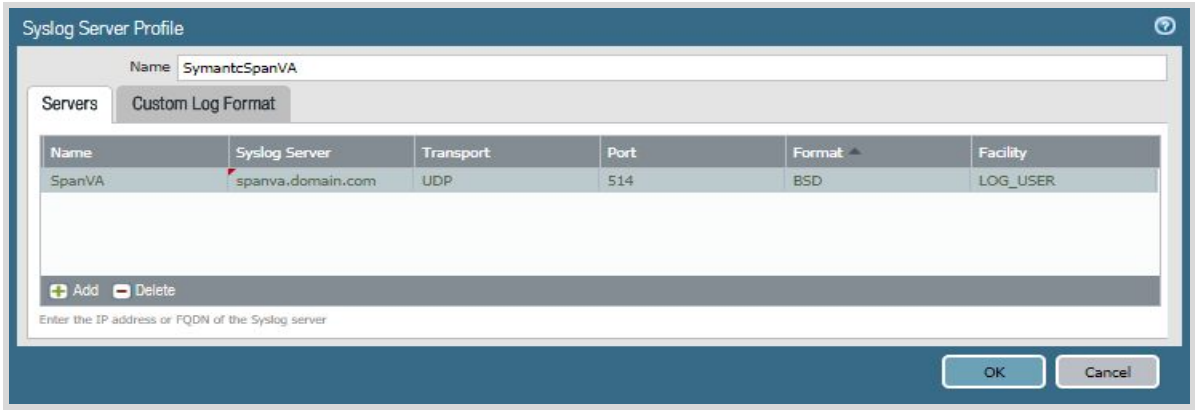


6. Click **OK**.

Configure log formats

Update the device configuration so that the device sends logs in the formats expected by CloudSOC:

1. In Panorama, navigate to **Server Profiles** > **Syslog**.
2. Create a new syslog server profile as shown below:



3. In the new profile, enter the following custom formats as shown below:

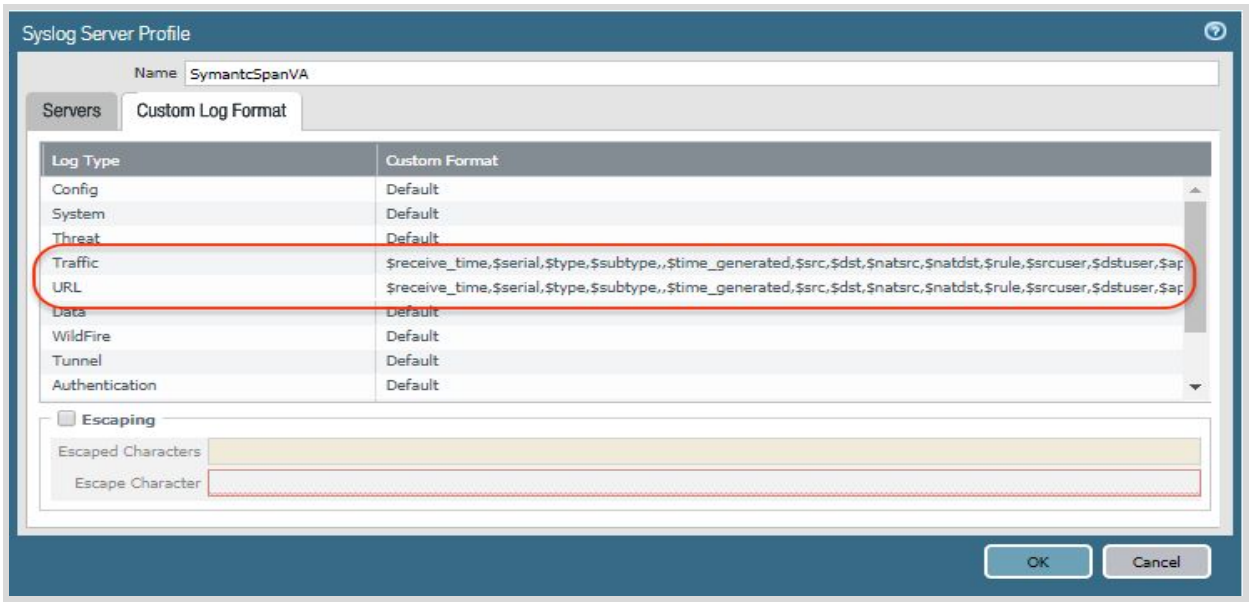
   Note: Do NOT copy & paste directly as it may have new line characters that will change the log format. Ensure for each format that the fields are on a single line.

   Traffic log:

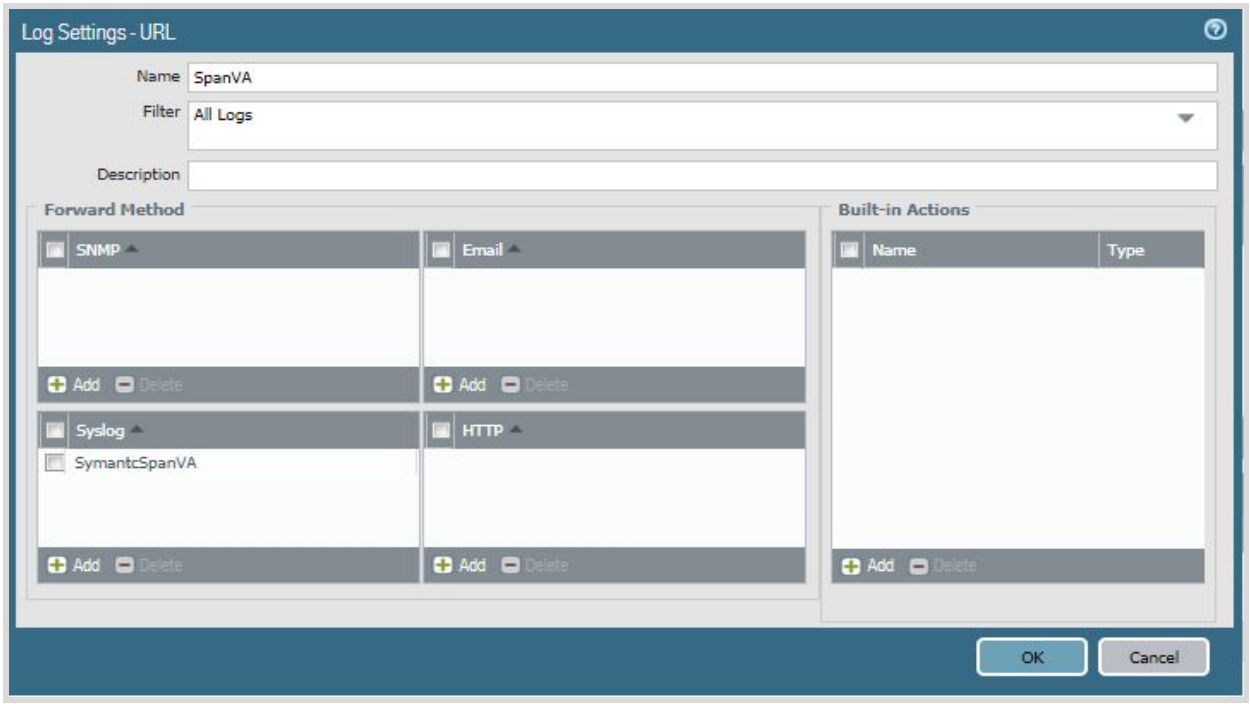
   ```
   $receive_time,$serial,$type,$subtype,,$time_generated,$src,$dst,$na
   tsrc,$natdst,$rule,$srcuser,$dstuser,$app,$vsys,$from,$to,$inbound_
   if,$outbound_if,,$time_received,$sessionid,$repeatcnt,$sport,$dport
   ,$natsport,$natdport,$flags,$proto,$action,$bytes,$bytes_sent,$byte
   s_received,$packets,$start,$elapsed,$category,$padding,$seqno,$acti
   onflags,$srcloc,$dstloc,,$pkts_sent,$pkts_received
   ```

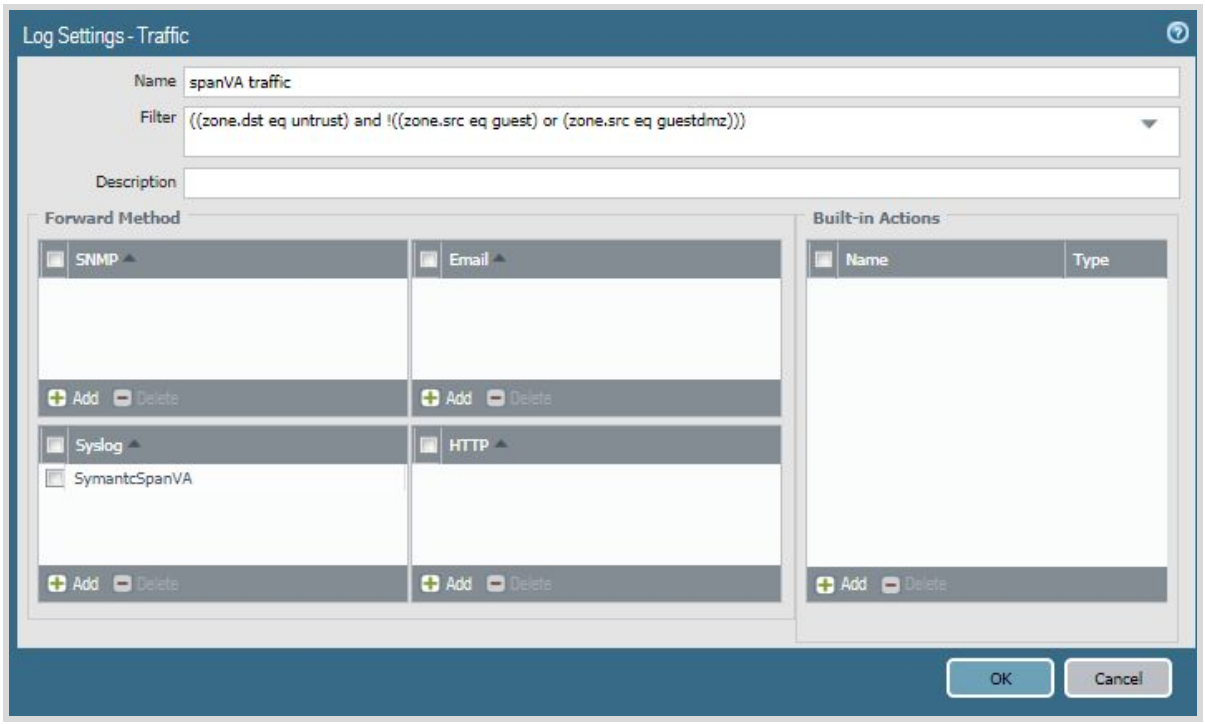
   URL log:

   ```
   $receive_time,$serial,$type,$subtype,,$time_generated,$src,$dst,$na
   tsrc,$natdst,$rule,$srcuser,$dstuser,$app,$vsys,$from,$to,$inbound_
   if,$outbound_if,,$time_received,$sessionid,$repeatcnt,$sport,$dport
   ,$natsport,$natdport,$flags,$proto,$action,$misc,$threatid,$categor
   y,$severity,$direction,$seqno,$actionflags,$srcloc,$dstloc,,$conten
   ttype,$dstloc,,,
   ```



4. Configure the device to forward the URL and Traffic logs to SpanVA as shown below.

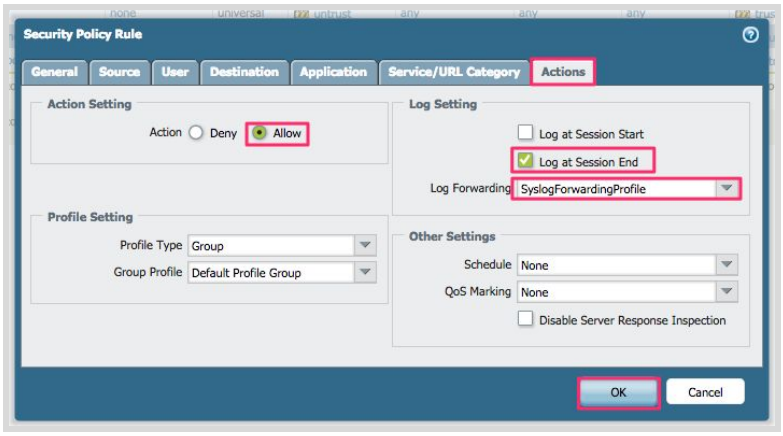




Update security, decryption policies, and URL filtering

Update all your security policies that monitor SaaS traffic. Typically these are the rules that control your user's outbound access to the Internet. Enable logging on these rules so a log is generated at the end of each TCP session.

1. Click the **Policies** tab and choose **Security** from the side menu.
2. For each security policy, click the **Action** tab and configure the following settings:
    a. For Action Setting, choose **Allow.**



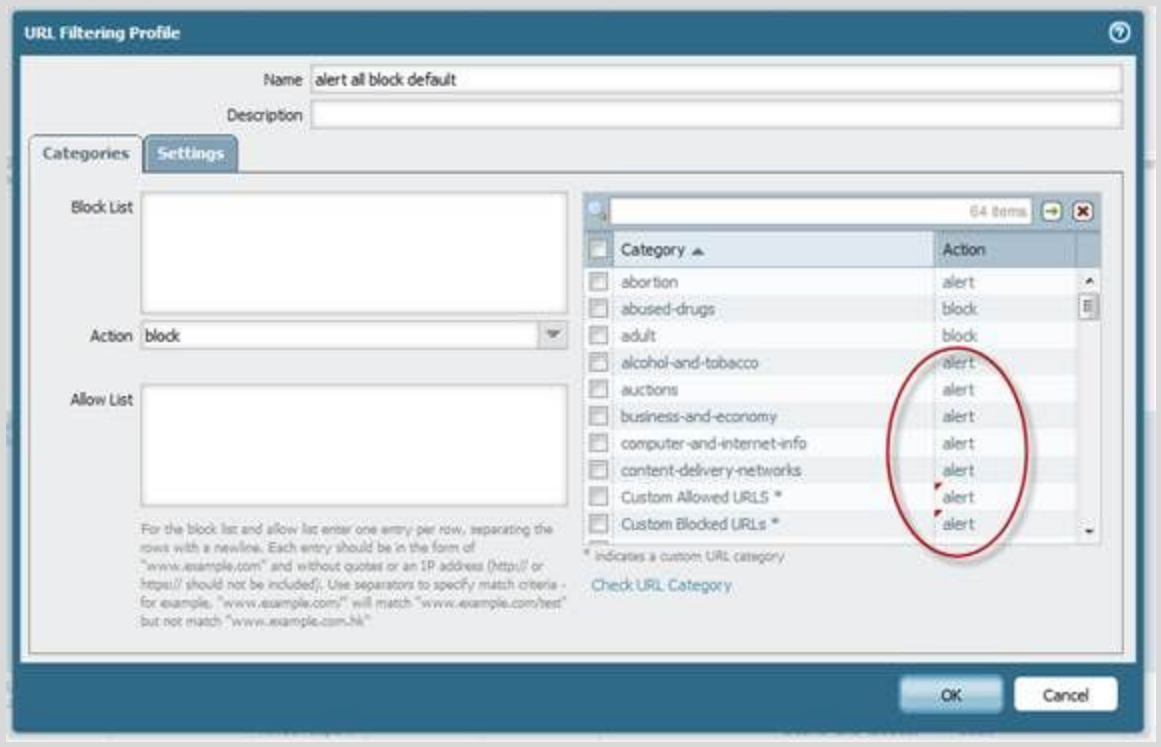
    b. For Log at Session End, mark the checkbox to enable it.
    c. From the Log Forwarding menu, choose the log forwarding profile you created in [Create]

a Log Forwarding Profile.

d. Click **OK**.

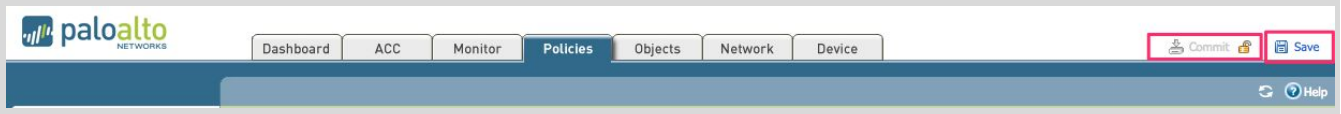
3. When you have configured the Actions settings for applicable security policies, click **Save**.

It is highly desirable that you have decryption turned on and are logging HTTP/HTTPs transactions as well. Follow similar procedure for enabling logging on decryption profiles and configure URL filtering to alert (generate logs) on all categories for which access is allowed.



Save and commit

After all changes are made, save and commit them.



Revision history

Date	Version	Description
2014	1.0	Initial release
5 November 2015	1.1	Minor revisions
26 April 2018	2.0	Address log format configuration
26 September 2019	2.1	Update log format configuration