Technology Partner Program Integration Guide

Author: Saasyan

Revision History	
15/2/2020	Re-validated the integration on PAN-OS 9.1 Conducted a feasibility analysis to leverage the dynamic user groups feature and the User-ID API to provide opt-in type Web Override functionality in a future release of Assure

Partner Information	
Date	April 24, 2020
Partner Name	Saasyan
Website	www.saasyan.com.au
Product Name	Saasyan Assure & Saasyan Advance
Partner Contact	Greg Margossian – Managing Director Phone: +61400239460 Email: greg@saasyan.com.au
Support Contact	Support Email: support@saasyan.com.au Support Phone Number: +61 2 8001 6632
Product Description	**Saasyan Assure** Saasyan Assure adds industry-best student cyber-welfare capability to next generation firewalls from Palo Alto Networks®. Alerts and reporting allow schools to act before an incident takes place, halting damage – and saving lives. Assure makes reporting and classroom control simple and intuitive, saving schools time and effort. Thanks to its deep integration with the PAN OS API, Assure enables schools to democratize access to the tools and the data non-ICT staff need to ensure the student's cyber-wellbeing. This makes it possible for schools to proactively safeguard students from inappropriate online content, promote good digital citizenship and protect students from cyberbullying and self-harm, while maintaining a modern and engaging learning environment. **Saasyan Advance** is a User-ID broker for Palo Alto Networks® Next Generation Firewalls. It enables schools to adopt BYOD policies without sacrificing security, functionality and ease of use.

Palo Alto Networks Products for Integration

Table 1: Integration Details by Product

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	Saasyan Versions Tested
AutoFocus			
Cortex XDR Prevent			
Cortex XDR Pro			
Next-Generation Firewall	Validated	PAN-OS 8.1; PAN-OS 9.0, PAN-OS 9.1	4.01.x,4.02.x,4.03.x
Panorama	Validated	PAN-OS 8.1; PAN-OS 9.0, PAN-OS 9.1	4.01.x,4.02.x,4.03.x
Prisma Access			

Prisma Cloud Compute			
Prisma Cloud Enterprise			
Prisma SaaS			
VM-Series	Validated	PAN-OS 8.1; PAN-OS 9.0, PAN-OS 9.1	4.01.x,4.02.x,4.03.x
WildFire			
Other			

Use Cases for Integration with the Palo Alto Networks

Use case #1

Challenge: Schools need to keep an eye on the online activity of the students who are deemed to be at risk of self-harm.

Solution: Through its industry leading signature based application control, user Identification and web Filtering capabilities, Palo Alto Networks® Next Generation Firewalls allows students to access to only the applications and web sites sanctioned by the school. It also performs SSL decryption on selected traffic. Assure analyzes log and packet capture data from the NGFW to allows schools to act before an incident takes place and halting damage.

It does this by:

1) Continuously scanning the web searches performed, the streaming content accessed and chat messages sent and received by these students
2) Identifying the activities that are indicative of self-harm
3) Notifying the school's staff about these activities

Use Case #2

Challenge: Schools need to recognize and promote good digital citizenship among students

Solution: Through their industry leading Web Filtering and user identification capabilities, Palo Alto Networks® Next Generation Firewalls provide granular logs on the sites accessed and applications used by each and every student. Saasyan Assure makes use of these logs to calculate each student's web and cyber rating on a daily basis and highlights the ones who are at risk. Schools can also allow students to log on to Assure to have visibility into their own internet usage.

Use Case #3

Challenge: Teachers need to easily and temporarily allow access to online content without being reliant on the ICT team.

Solution: Self-service firewall and web filter management allows Teachers and non-ICT staff to grant temporary access to online content that's normally blocked, allowing teaching activities to continue unimpeded – and integration with leading Learning Management Systems allows access to be controlled within the LMS. Assure leverages the feature rich Palo Alto Networks® PAN-OS API to allow non-technical staff to perform these tasks on demand and in a truly self-service manner.

Integration Benefits

Saasyan Assure

- **Effortless Reporting**
  Assure is designed for ease of use by Teachers and other School staff. Our reports quickly and simply display the websites visited, the applications and bandwidth used, the searches performed and the videos viewed.

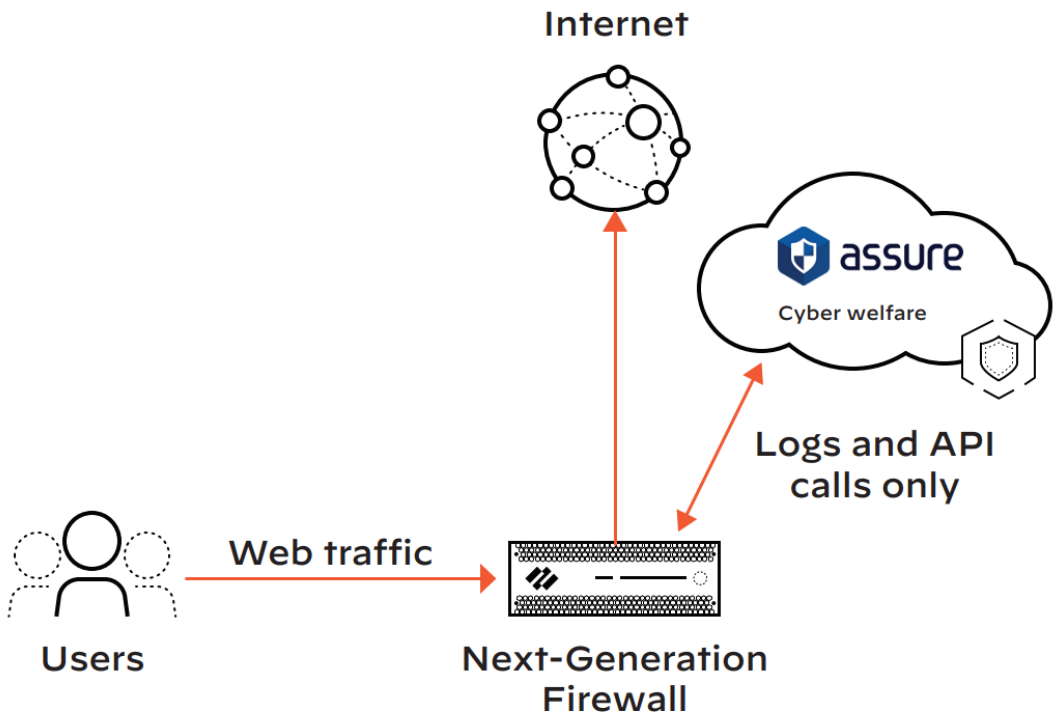
- **Alerting**
  The school staff can subscribe to alert notifications in order to get informed when students attempt to access inappropriate websites and videos, use potentially dangerous search keywords, or are involved in negative social media activity. Artificial Intelligence built into Assure helps teachers by automatically categorizing abusive content.

- **Self-Service Web Overrides**
  Self-service web filter management allows teachers and non-ICT staff to grant temporary access to sites/content that's normally blocked, allowing teaching activities to continue unimpeded.

Saasyan Advance

- Saasyan Advance enables schools to protect their students and environment by leveraging firewall policies that make use of User-ID information gathered from any device - whether BYOD, or school provided.
- It enables schools to adopt BYOD policies without sacrificing security, functionality and ease of use

Integration Diagram



Data shared between our products:

- Assure receives the URL Filtering, Traffic and Threat logs from the Palo Alto Networks NGFW via Syslog. It also interacts with the PAN OS API in order to create temporary custom web categories, schedules and security policies to facilitate self-service classroom control. The PAN OS API is also used to create vulnerability definitions that instruct the NGFW to perform packet captures whenever it encounters chat sessions over the supported social media chat applications.
- The two interfaces that are used for integration are the syslog facility and the PAN-OS API. The bulk of the data is transferred via syslog form the NGFW to Assure.
- The log data is parsed, and the following metadata is added to it:
  - student name/surname
  - group membership
  - the school period during which the activity took place
  - for web searches, the search phrases are extracted
  - for YouTube videos, the video title is fetched from the YouTube API
- This enriched data is then:
  - Stored in a data warehouse and made available for easy reporting
  - Passed through a classifier which identifies activities that are indicative of self-harm, cyber-bullying, profanity, etc and alert messages are sent to the relevant people at the school

Before You Begin

- The NGFW/Panorama needs to be running PAN-OS 8.1 or later
- The NGFW needs to have a URL Filtering license
- SSL Decryption needs to be set up on the NGFW

Integration Configuration

- **Saasyan Advance**: https://docs.saasyan.com.au/docs/index.php/Advance_DeploymentGuide
- **Saasyan Assure**: https://docs.saasyan.com.au/docs/index.php/Assure_DeploymentGuide

Troubleshooting

- Common troubleshooting steps:
  - Subscribers can click on the Request Support button within the UI to report issues and request assistance. Assure is provided as a fully managed service. The Saasyan team is in charge of troubleshooting
- Contact information for support:
  Subscribers can click on the Request Support button within the UI, send an email to support@saasyan.com.au or call our support number.
- Saasyan is a member of the Palo Alto Networks NextWave TSANet group
- Helpful resources:
  - Recorded Demo: https://www.youtube.com/watch?v=G2poTJOoSc8
  - Product Page: https://www.saasyan.com.au/products/assure/

Technical Details

Mechanism of the Interaction

Saasyan Assure

The Assure Collector appliance ingests Syslog messages generated by the Palo Alto Networks® Next Generation Firewall (Threat logs and Traffic logs). It then aggregates these logs with metadata from Active Directory (full name of the user, year group/boarding house group membership) and streams these logs to the cloud based data warehouse. This data warehouse acts as the source of truth for reports and alerts.

The Assure collector also proxies XML API requests from the cloud hosted service to the on premise Palo Alto Networks® Next Generation Firewall. This is required for the overrides function whereby an Assure user can create override rules (both custom web categories and security rules are configured programmatically and cleansed upon expiry).

The web categories defined on the Palo Alto Networks® Next generation Firewall (including the custom web categories) flow through the system are saved in the data warehouse where they are overlayed with a user editable rating. These per category ratings are used to calculate the user ratings (to determine whether students are visiting appropriate sites).

Saasyan Advance

The Saasyan Advance virtual appliance ingests logs form the Windows Server running NPS and DHCP roles (we recommend using NxLog to forward logs from these nodes to the Advance virtual appliance), aggregates them and sends the resulting User-ID – IP Address tuple to the Palo Alto Networks® Next generation Firewall(s) via the XML API. The frequency of the User-ID injection is a parameter that can be adjusted and so is the TTL of the User-ID object.

- If applicable list the name of API calls that are being leveraged
- If this is a syslog integration list out the types of log that are being used (Traffic, threat, HIP Match, Config, System, TRAPS logs, etc…)
- List out any additional technical details on how the two technologies integrate

Saasyan Assure

Syslog

Assure acts as a log receiver for URL and Traffic logs generated by the Palo Alto Networks® next generation firewalls. It makes use of the following custom log formats on the NGFW.

Log Type	Custom Format
Traffic	k12wstraffic $receive_time | $device_name | $type | $subtype | $action | $app | $category | $proto | $srcuser | $src | $sport | $dst | $dport | $bytes_sent | $bytes_received | $elapsed |
URL	k12wsthreat $receive_time | $device_name | $type | $subtype | $action | $app | $category | $proto | $srcuser | $src | $sport | $dst | $dport | $contenttype | $misc |

It makes use of the pipe character as a delimiter to parse the log message and extract the following values:

Log Type	Values Parsed/Extracted
Traffic	receive_time device_name type subtype action app category proto srcuser src sport dst dport bytes_sent bytes_received elapsed
URL	receive_time device_name type subtype action app category proto srcuser src sport dst dport contenttype misc

RESTful API

Assure makes use of the Palo Alto networks® OS Restful API to allow users to create Web Override rules. The following table lists the associated functions and the corresponding API calls:

Variables are shown in {}

	API Call
Create Custom URL Category	https://{pan_ngf_address}/api/?type=config&action=set&key={api_key}&xpath=/config/devices/entry[@name='{pan_ngf_hostname}']/vsys/entry[@name='{vsys_name}']/profiles/custom-url-category/entry[@name='ASSURE-{unique_rule_id}']&element=<list><member>{base_url}</member></list>
Create Policy Rule	https://{pan_ngf_address}/api/?type=config&action=set&key={api_key}&xpath=/config/devices/entry[@name='{pan_ngf_hostname}']/vsys/entry[@name='{vsys_name}']/rulebase/security/rules/entry[@name='ASSURE-{unique_rule_id}']&element=<profile-setting><profiles><url-filtering><member>default</member></url-filtering></profiles></profile-setting><from><member>{from_zone}</member></from><to><member>{to_zone}</member></to><source><member>any</member></source><destination><member>any</member></destination><source-user><member>{domain_name}\{group_or_user_name}</member></source-user><category><member>ASSURE-{unique_rule_id}</member></category><application><member>any</member></application><service><member>application-default</member></service><hip-profiles><member>any</member></hip-profiles><action>{allow_or_deny}</action>
Move Policy Rule to the top of the ruleset	https://{pan_ngf_address}/api/?type=config&action=move&key={api_key}&xpath=/config/devices/entry[@name='{pan_ngf_hostname}']/vsys/entry[@name='{vsys_name}']/rulebase/security/rules/entry[@name='ASSURE-{unique_rule_id}']&where=top
Delete Custom URL Category	https://{pan_ngf_address}/api/?type=config&action=delete&key={api_key}&xpath=/config/devices/entry[@name='{pan_ngf_hostname}']/vsys/entry[@name='{vsys_name}']/profiles/custom-url-category/entry[@name='ASSURE-{unique_rule_id}']&
Delete Policy Rule	https://{pan_ngf_address}/api/?type=config&action=delete&key={api_key}&xpath=/config/devices/entry[@name='{pan_ngf_hostname}']/vsys/entry[@name='{vsys_name}']/rulebase/security/rules/entry[@name='ASSURE-{unique_rule_id}']&
Commit Configuration	https://{pan_ngf_address}/api/?type=commit&cmd=<commit><description>ASSURE</description></commit>&key={api_key}&

Saasyan Advance

RESTful API

Advance makes use of the Palo Alto networks® OS Restful API to inject and remove User-ID to IP Address Mappings which it derives from log messages it receives from Windows NPS servers and DHCP servers. The following table lists the associated functions and the corresponding API calls:

Variables are shown in {}

Function	API Call	Userid_mods.xml contents
Insert User-ID to IP Address mappings	https://{pan_ngf_address}/api/?type=user-id&key={api_key}&action=set&client=wget&file-name=userid_mods.xml	<uid-message> <type>update</type> <payload> <login> <entry name="{domain_name}\{user_name}" ip="{ip_address}" timeout="{timeout}"/> <entry name="{domain_name}\{user_name}" ip="{ip_address}" timeout="{timeout}"/> </login> </payload> </uid-message>
Remove User-ID to IP Address mappings	https://{pan_ngf_address}/api/?type=user-id&key={api_key}&action=set&client=wget&file-name=userid_mods.xml	<uid-message> <type>update</type> <payload> <logout> <entry name="{domain_name}\{user_name}" ip="{ip_address}" timeout="{timeout}"/> <entry name="{domain_name}\{user_name}" ip="{ip_address}" timeout="{timeout}"/> </logout> </payload> </uid-message>