TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: ERICOM SHIELD

Contents

Partner Information

Partner information	
Date	January 24, 2019
Partner Name	Ericom Software
Web Site	https://www.EricomShield.com
Product Name	Ericom Shield
Partner Contact	James Lui, VP Product Management, +1 (201) 767-2210 x4317
Support Contact	CA@Ericom.com, + (201) 767-2210 x5
Partner Product for Integration	Ericom Shield
Product Description	**Ericom Shield** is an award-winning Remote Browser Isolation (RBI) platform that offers a secure approach to protect corporate end-user devices against web-borne and zero-day threats. With Shield, a secure execution environment is created between users and the Internet. While users access websites, virtual browsers located in air-gapped and remote, isolated, and disposable Linux containers are executing each web session. A secure visual stream is transmitted from the container back to the browser on the user's device providing a natural experience. Users can access business-critical Internet services, while protecting endpoints and the corporate networks from malware, phishing, crypto mining and other such threats. The centrally-managed solution is compatible with all common browsers, operating systems and devices.

Use cases for integration into Palo Alto Networks Next Generation Firewall

Rather than just blocking certain websites from reaching the Internet, such sites are redirected from Palo Alto to Ericom Shield for safe viewing and usage.

Challenge: Cyber-insurance investigators need to browse the dark web to research victim cases. The investigators need to browse safely without themselves being victimized.

Solution: With the Palo Alto Networks Next Generation Firewall and Ericom Shield integrated solution, URL filtering tailored for investigators to gather data on the relevant dark web sites, which would otherwise be blacklisted for most users. The Palo Alto Networks Firewall detects and denies the bulk of the known attacks stemming from those sites. Using Ericom Shield, the uncategorized, unknown, and suspicious websites are rendered by an isolated browser remote from the endpoint in the DMZ, so that any potential malware cannot infect endpoint devices and from there, enter internal corporate networks. In the course of their research, investigators can freely and naturally interact with sites without concern of infection. Once the users leave the website – permanently or just for a few moments -- the ephemeral virtual browsers are safely destroyed, along with all content the sites without impacting the end-user experience.

Palo Alto Networks Products for Integration

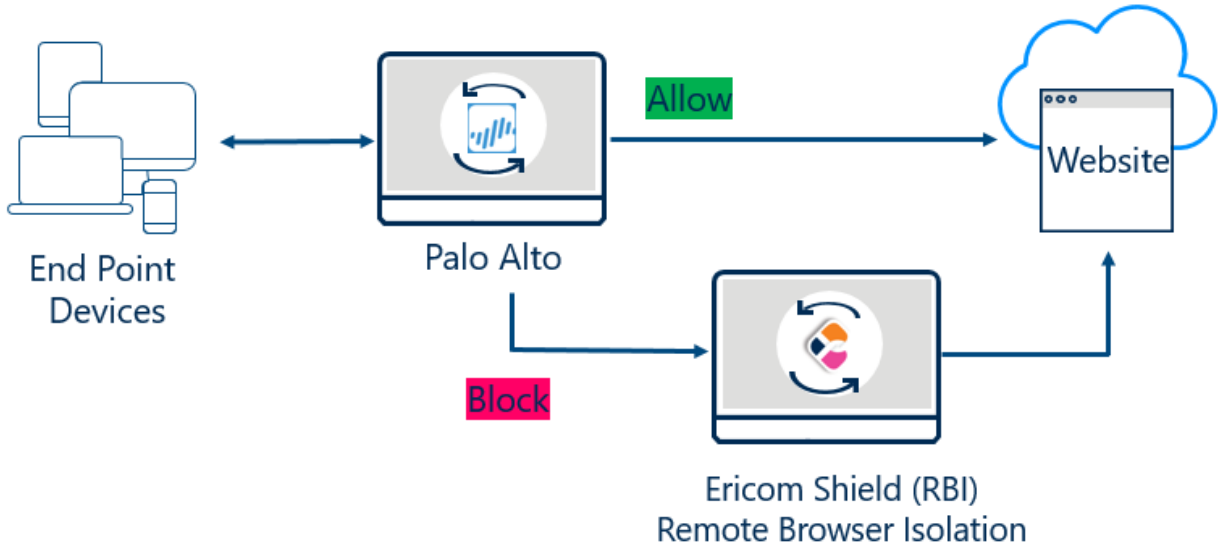
Palo Alto Networks Product	Integration Status	Versions Supported
Aperture		
Application Framework		
Autofocus		
Evident.io		
GlobalProtect		
GlobalProtect Cloud Service		
Logging Service		
MineMeld		
NGFW	Completed	PAN-OS 8.1.2
Panorama		
Traps		
VM-Series		
Wildfire		
Other		

Integration Benefits

With the integrated Ericom Shield-Palo Alto Networks Next Generation Firewall solution, uncategorized websites are automatically routed to Ericom Shield, where each is rendered by a virtual browser located in an air-gapped, isolated virtual container remote from the endpoint, in the DMZ or cloud. A safe media stream enables end-users to interact natively with the website, via whichever web browser they prefer. When a user closes a tab or stops browsing, the container is destroyed along with all content from the website, including any possible malicious content. Ericom Shield is centrally managed and requires no installation or agents on endpoint devices.

Organizations can now achieve Continuous Adaptive Risk and Trust Assessment (CARTA) and Zero Trust security reference architectures that include safe and agile access to even the darkest corners of the Internet.

Integration Diagram – Redirection Mode



Palo Alto Firewall is the first line of defense. Requests that are received in the Palo Alto Firewall and are either passed or blocked (based on the Palo Alto URL Filtering).

The blocked requests are redirected to Shield and processed in Shield according to the pre-defined policies and settings.

- *What data is shared between our products – A target URL is passed one-way from Palo Alto to Ericom Shield for isolation*
- *How is the data shared? – The URL is passed using URL redirection or proxy chain*
- *What is the action taken as a result of this sharing? – Once Ericom receives the URL from Palo Alto, it opens it in a container and retrieves the content from the Internet.*

Before you begin – Redirection Mode

Dependencies:

- Linux Ubuntu 16.04 LTS / 18.04 LTS X64
- SSH access to Ericom Shield
- Administrator access to Ericom Shield and Palo Alto

Palo Alto Networks Configuration – Redirection Mode

Customize the Palo Alto URL Filtering response page by following these steps:

- Go to **Device** | **Response Pages**
- Select the **URL Filtering and Category Match Block Page** response page to download and modify it (save locally)
- Select the checkbox next to 'Predefined' then click **Export**
- Using a text editor, edit the HTML page to redirect to Shield.

- For example:

  Highlight the content between the * * and * * sections and replace it entirely with the following (enter the Shield Server IP or Fully Qualified Domain Name)

  When specifying the URL for Ericom Shield, ensure that you enter 'https://' to prevent an additional HTTP redirect from http to https

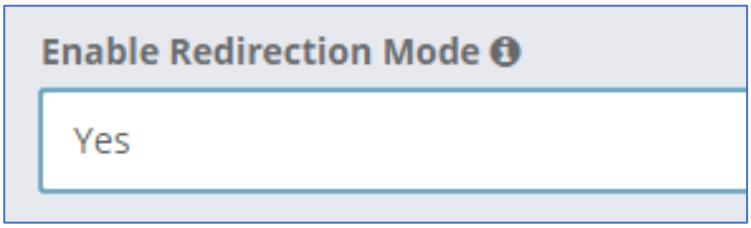
  <script language="javascript">
  window.location = "https://192.168.50.84/?url=http://<url/>";
  </script>

- Save the file (make sure it retains its UTF-8 encoding)
- Go to **Device** | **Response Pages**, select the **URL Filtering and Category Match Block Page** response page, click **Import** and browse to the location of the modified response page, then click **OK** and **Close** to import the newly saved file
- Commit the changes and verify that the redirection works (browse to a blocked URL and confirm that it is opened via Shield)

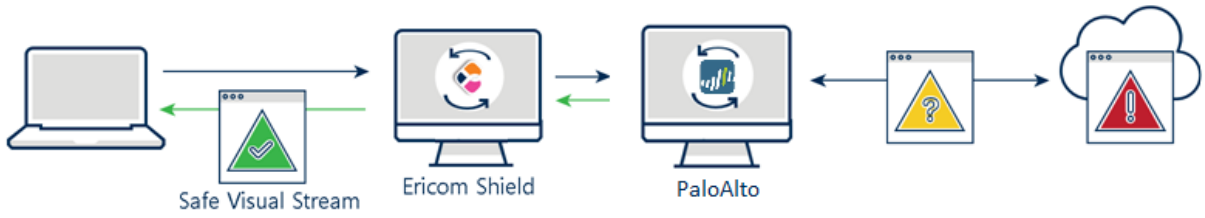
Ericom Shield Configuration – Redirection Mode

Login to Ericom Shield Admin Console and go to Settings | Proxy & Integration section.

Set the Enable Redirection Mode to Yes.



Integration Diagram – Proxy Chain Mode



Before you begin – Proxy Chain Mode

Dependencies*:*

- Linux Ubuntu 16.04 LTS / 18.04 LTS X64
- SSH access to Ericom Shield
- Administrator access to Ericom Shield and Palo Alto

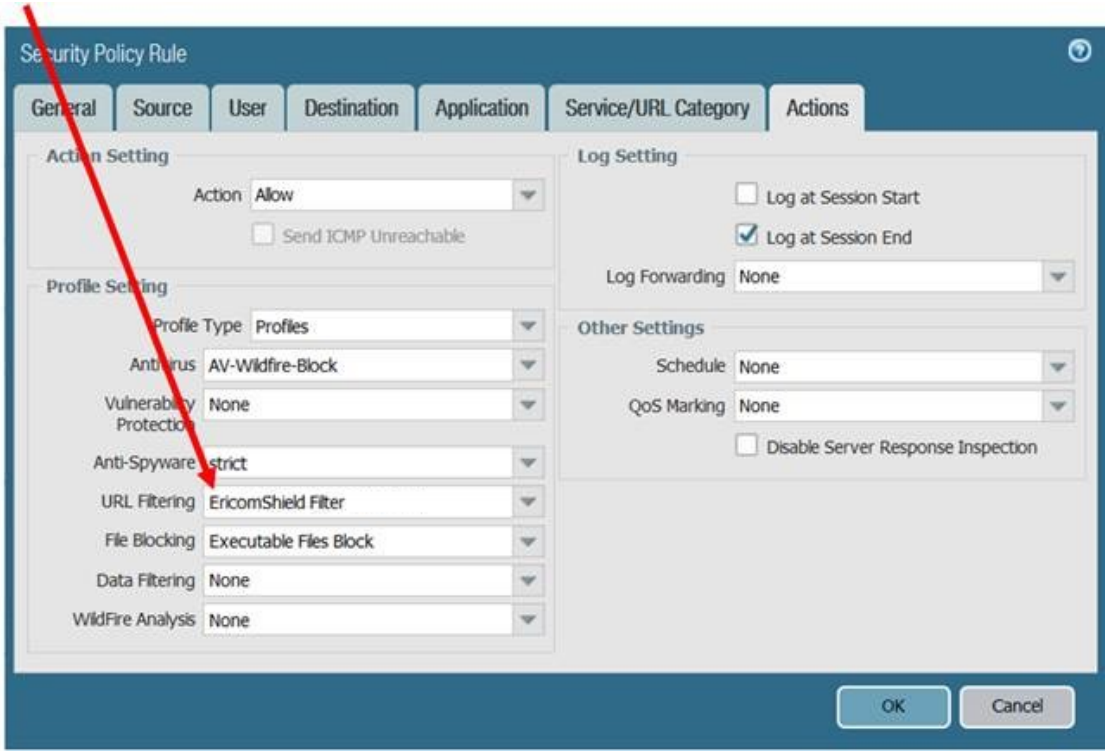
Palo Alto Networks Configuration – Proxy Chain Mode

In order to have visibility of the end-user in Palo Alto, the XXF has to be configured.

- Go to Device | Setup | Content-ID
- Open settings option (gear icon) for **X-Forwarded-For Headers** widget
- Select both “Use X-Forwarded-For Header in User-ID” and “Strip X-Forwarded-For Header” checkboxes and select **OK** to apply changes.
- Go to Objects | Security Profiles | URL Filtering and define a dedicated URL Filtering security profile.
- Within the URL Filtering security profile select relevant categories (as usual), and in addition, go to URL Filtering Settings tab and check the X-Forwarded-For checkbox and select **OK** to apply changes:

- On the security policy that handles egress traffic from the Ericom Shield server, apply the relevant URL Filtering security profile:

- Open the Security Policy Rule, then go to **Actions** | modify the **URL Filtering profile** to select the EricomShield Filter | select **OK** to save changes and **Commit** to install the policy

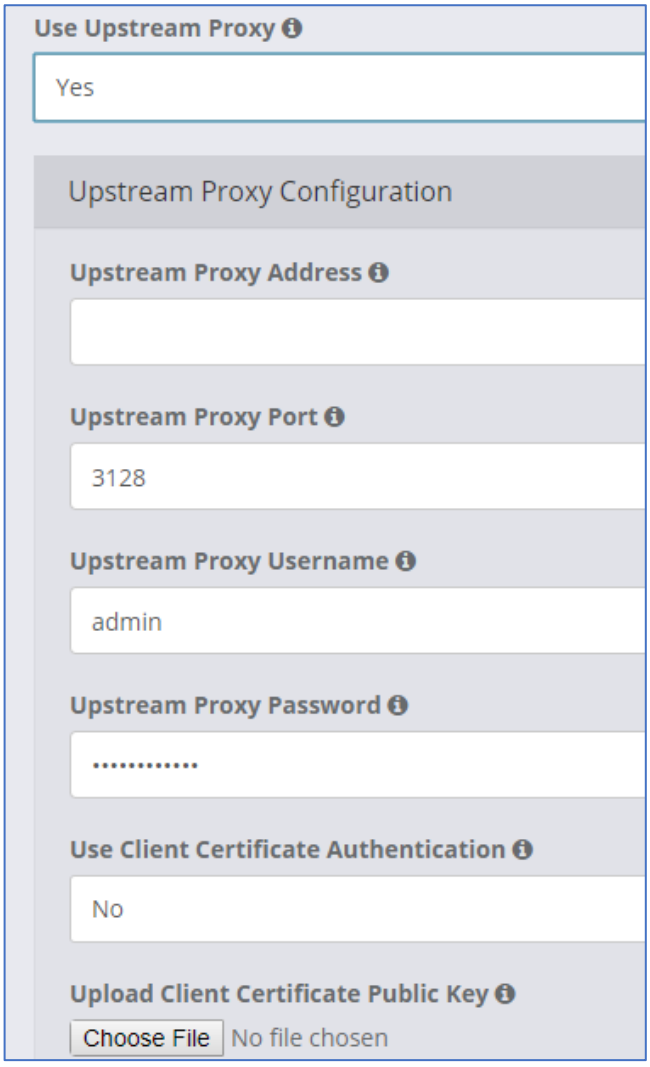


Ericom Shield Configuration – Proxy Chain Mode

When Palo Alto is used as an **upstream proxy**, it needs to be configured in the Shield Admin Console.

- Go to Admin Console | Settings | Proxy & Integration section
- Set the “Use Upstream Proxy” to Yes
- Enter the Upstream Proxy Configuration fields: address, port, username & password

- Upload the Palo Alto client Certificate (public & private keys)



End-User Configuration

The end-user's browser requires a valid certificate (such as ericomshield.crt) for navigating to HTTPS sites. Instructions vary for different browsers, to view the instructions from a Shield-enabled browser navigate to the URL: http://install-certificate/instructions

The Ericom Shield certificate may be downloaded from a Shield-enabled browser by navigating to the URL: http://icap-server:1345/cert/ericomshield.crt

Troubleshooting

- Isolate the issue by testing each solution individually.
- If there is an issue with the proxy chain method, try the URL redirection method, and vice versa.
- In proxy chain configuration, verify that the Palo Alto CA certificate, in ".pem" format, is configured as a trusted CA to shield
- Import the Ericom Shield CA certificate to end-user browser store

Troubleshooting – Escalation Details

Technical support information may be found in the TSANet Palo Alto program site.

Ericom partner technical support contact email: **PaloAlto@Ericom.com**