Palo Alto Networks
PAN-OS

RSA Security Analytics Ready Implementation Guide

Last Modified: November 24th, 2014

Partner Information

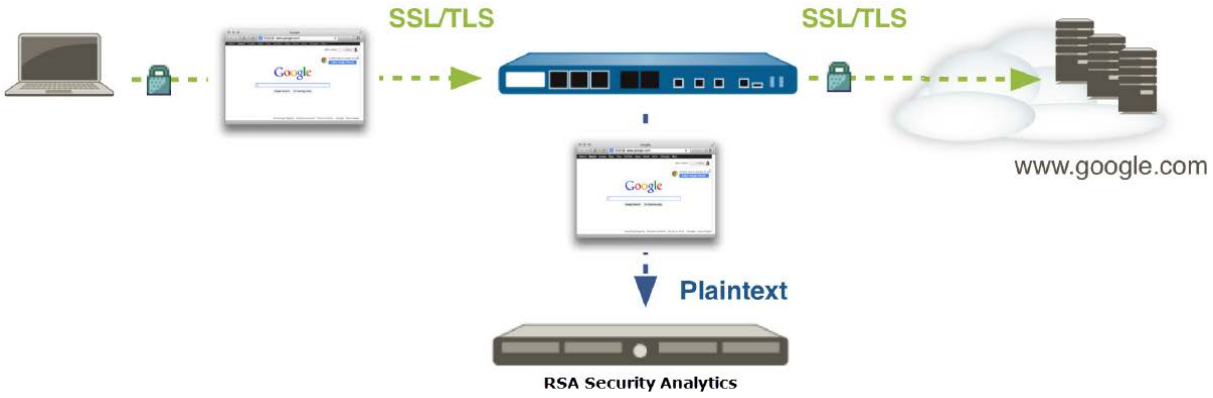
Product Information	
Partner Name	Palo Alto Networks
Web Site	www.paloaltonetworks.com
Product Name	PAN-OS (PA-7050, PA-5000 and PA-3000 series)
Version & Platform	6.1.0
Product Description	Palo Alto Networks firewalls provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Decryption on a Palo Alto Networks firewall includes the capability to enforce security policies on encrypted traffic, where otherwise the encrypted traffic might not be blocked and shaped according to your configured security settings. Use decryption on a firewall to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted traffic. Supported only on PA-5000 Series and the PA-3000 Series only.

Solution Summary

Secure Sockets Layer also known as SSL is getting more and more common. We see many common applications now turning in to HTTPS as twitter, facebook, gmail by default/supported. It gives the user a certain amount of privacy. Unfortunately, SSL is also used as evasion tactics by hackers and cyber criminals. It's used to hide the activity within the SSL package. This is why we are interested in decrypting SSL packages for visibility controlling and granular security.

This is where the Palo Alto comes in. A handful of networking vendors inspect SSL encrypted HTTPS traffic (HTTPS). Palo Alto goes further by inspecting compliant SSL traffic, no matter the protocol encapsulated by it. The firewall can unwrap the encapsulation to expose the underlying protocol and applications.

Policy-based identification, decryption and inspection of outbound SSL traffic (from users to the web) can be applied to make sure that applications and threats are not hiding within SSL traffic. The Palo Alto uses a 'man-in-the-middle' approach in which device certificates are installed in the user's browser. By default, SSL decryption is disabled and will need to be enabled for the configuration of this guide.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Palo Alto PAN-OS with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Palo Alto components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Palo Alto PAN-OS Configuration

SSL Forward Proxy Configuration

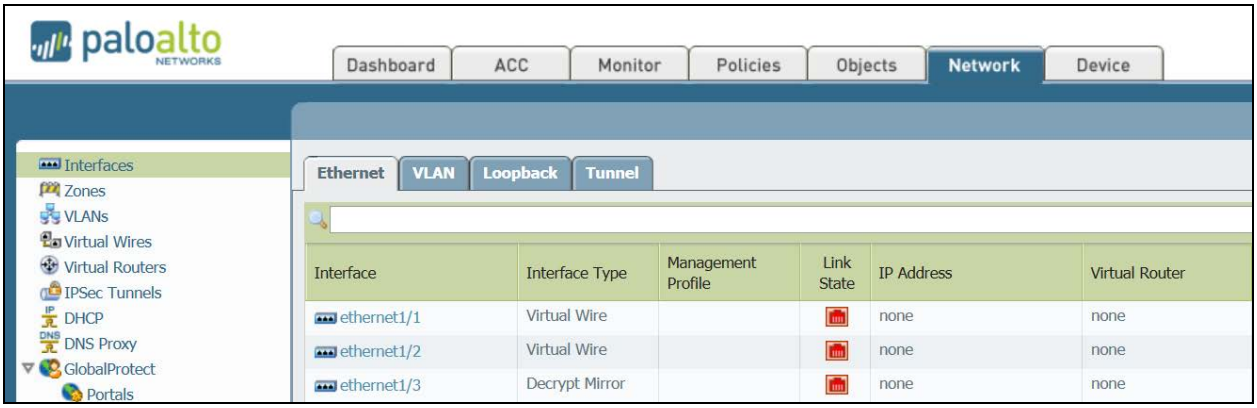
Use an SSL Forward Proxy decryption policy to decrypt and inspect SSL/TLS traffic from internal users to the web. Configuring SSL Forward Proxy decryption on the firewall requires setting up the certificates needed for SSL Forward Proxy decryption and creating an SSL Forward Proxy decryption policy. The firewall can use self-signed certificates or certificates signed by an enterprise CA to perform SSL Forward Proxy decryption.

! Important: For information on generating certificate, please see the Palo Alto Administrator's Guide. DO NOT continue until the certificate has been created and imported into the Palo Alto device.

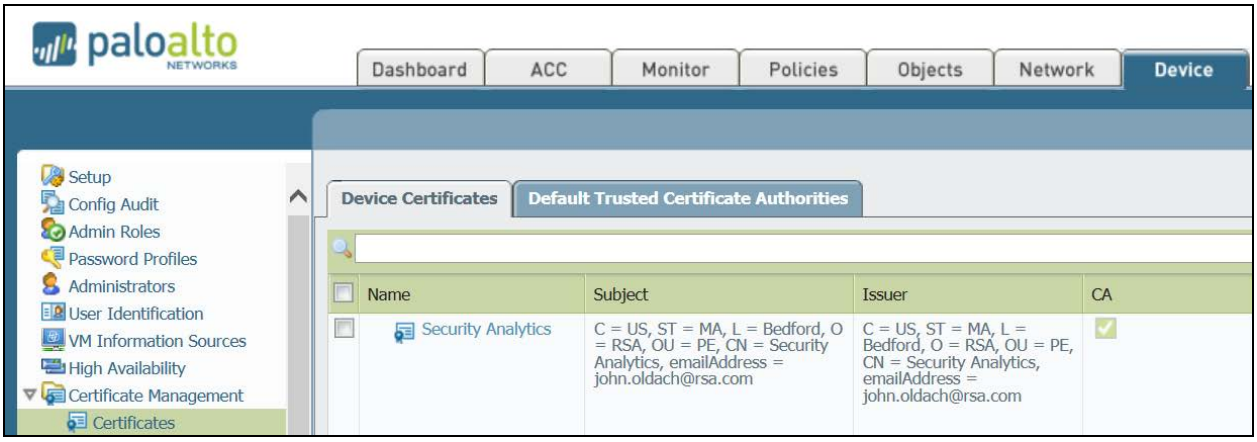
1. From a web browser, log-in to the Palo Alto Web Interface (e.g. **https://mgmt_ip_address**)

2. From the Palo Alto administration menu, click **Network** > **Interfaces** > **Ethernet** tab.

3. Make sure the interfaces you are using in your environment is either a **Virtual Wire**, **Layer 2** or **Layer 3** interface. The interfaces used should be in-line to the outbound web traffic.



4. Next, we'll check the options on the certificate that was previously imported. Click **Device** > **Certificates**. Select the certificate you have previously imported.



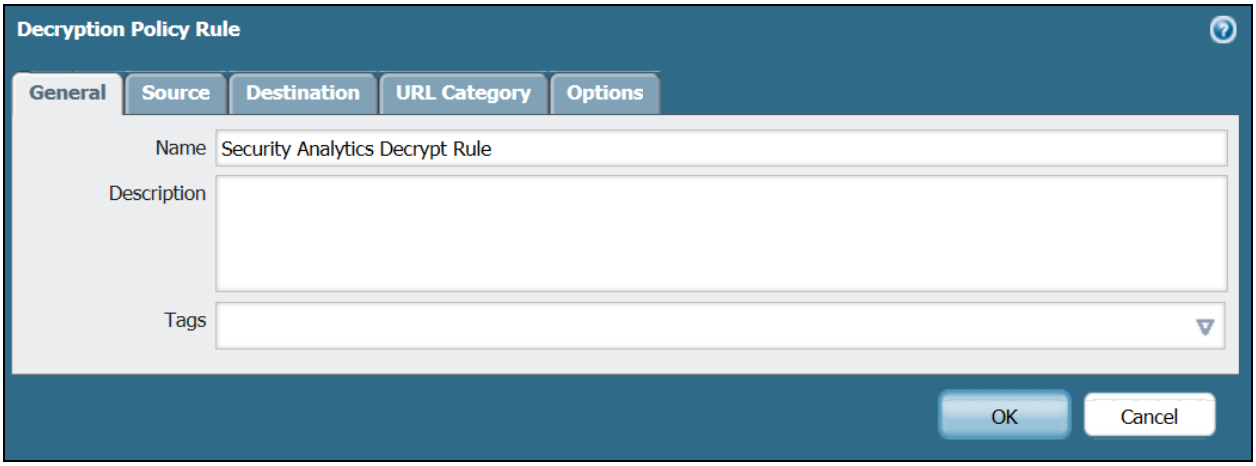
5. Be sure the following check boxes are selected for the certificate:
   - **Certificate Authority**
   - **Forward Trust Certificate**
   - **Forward Untrust Certificate**
   - **Trusted Root SA**

6. (***Optional***) Create a **Decryption Profile**. If you do not wish to create a **Decryption Profile**, skip to **step 11**.

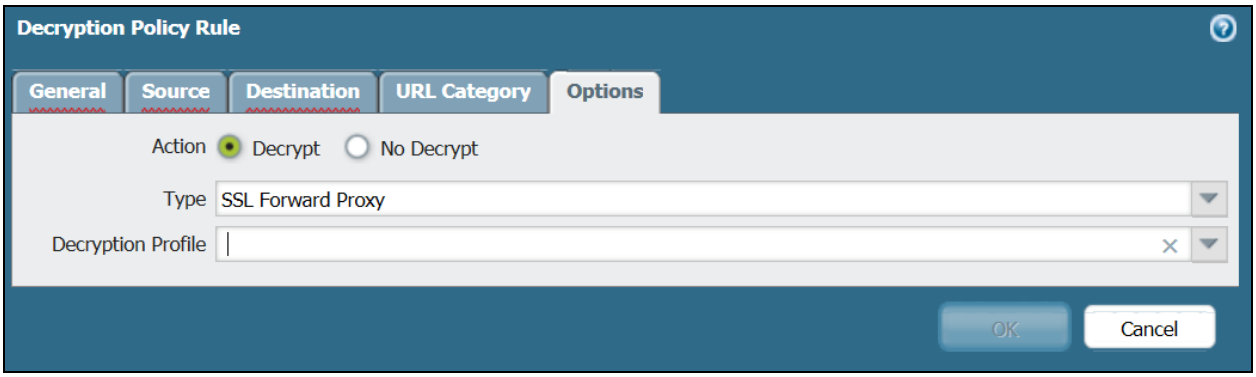
> **Note: Decryption profiles can be associated with a decryption policy, enabling the firewall to block and control various aspects of traffic that is being decrypted. An SSL Forward Proxy decryption profile can be used to perform checks for server certificates, unsupported modes, and failures and block or restrict traffic accordingly. For a complete list of checks that can be performed, navigate to Objects > Decryption Profiles on the firewall and click the help icon.**

7. Click **Objects** > **Decryption Profile** and click **Add**.
8. Click the **SSL Forward Proxy** tab to block and control specific aspects of SSL tunneled traffic.
9. Select the appropriate actions for your environment.
10. Click **OK** to save the profile.

11. Next, click **Policies** > **Decryption** and Click **Add**.



12. On the **General** tab, give the policy a descriptive **name**.
13. On the **Source** and **Destination** tabs, select **Any** for the Source Zone and Destination Zone to decrypt all SSL traffic destined for an external server. If you want to specify traffic from or to certain sources or destinations for decryption, click **Add**.
14. In the URL Category tab, leave **Any** to decrypt all traffic. If you only want to apply this profile to certain website categories, click **Add**.
15. On the **Options** tab, select **Decrypt** and select **SSL Forward Proxy** as the **Type** of decryption to perform.



16. (***Optional***) Select a **Decryption Profile** to apply additional settings to decrypted traffic (see *Step 6*).
17. Click **OK** to save.
18. Click **Commit** to save the configuration.

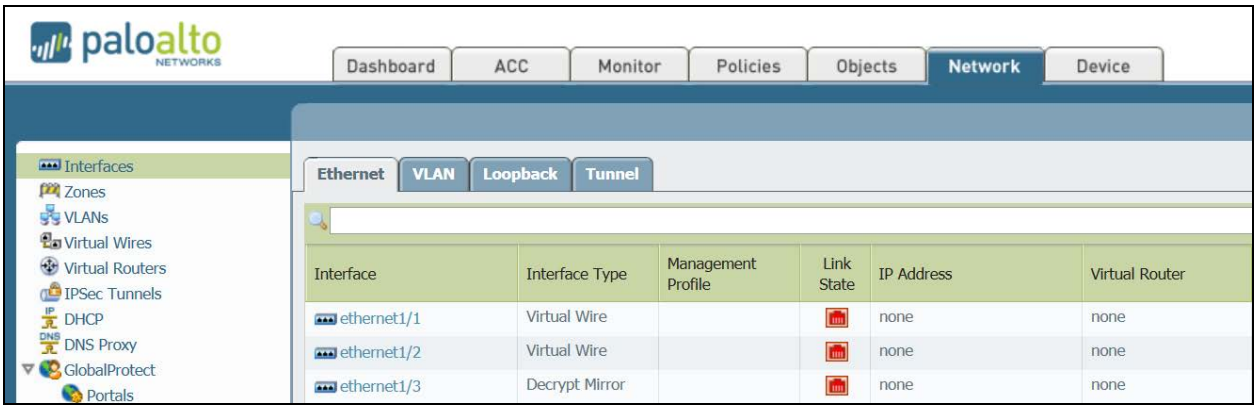
! Important: With an SSL Forward Proxy decryption policy enabled, all traffic identified by the policy is decrypted. Decrypted traffic is blocked and restricted according to the profiles configured on the firewall (including the decryption profiles associated with the policy and Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking profiles). Traffic is re-encrypted as it exits the firewall.

SSL Inbound Inspection Configuration

Configuring SSL Inbound Inspection includes installing the targeted server's certificate on the firewall and creating an SSL Inbound Inspection decryption policy.

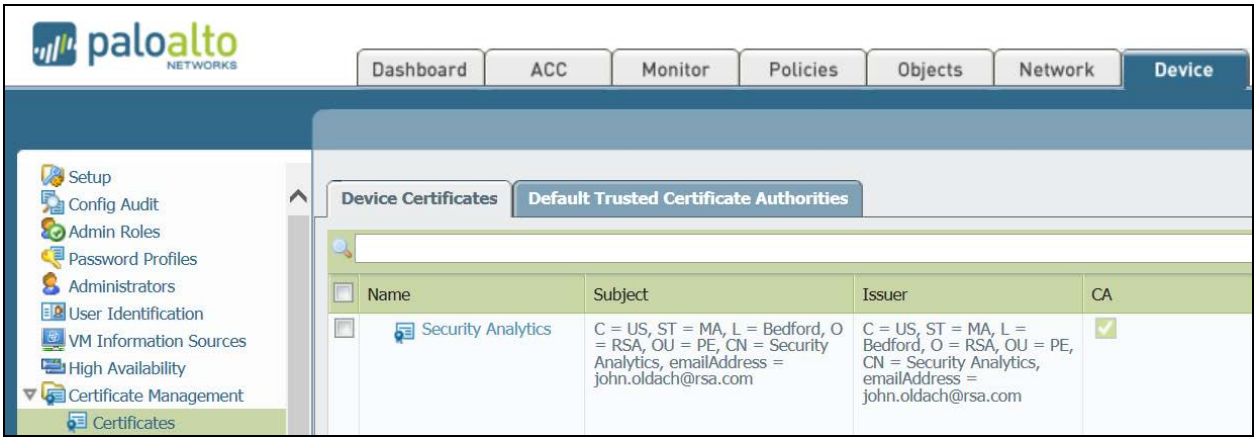
1. From a web browser, log-in to the Palo Alto Web Interface (e.g. **https://mgmt_ip_address**)

2. From the Palo Alto administration menu, click **Network** > **Interfaces** > **Ethernet** tab.
3. Make sure the interfaces you are using in your environment is either a **Virtual Wire**, **Layer 2** or **Layer 3** interface. The interfaces used should be in-line to the outbound web traffic.

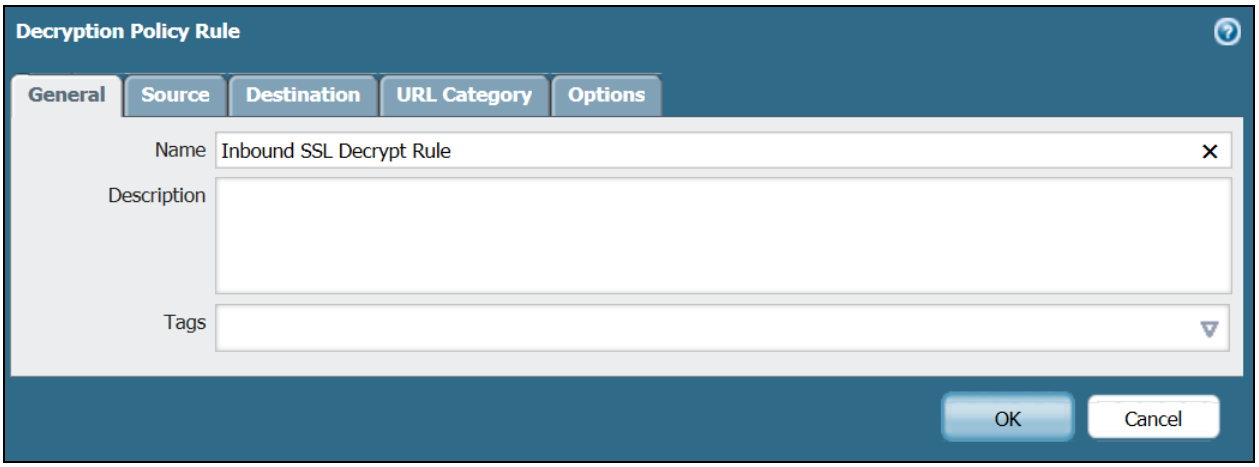


4. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates.**
5. On the Device Certificates tab, select **Import.**
6. Enter a descriptive **Certificate Name**.

7. **Browse** for and select the targeted server's **Certificate File**.
8. Click **OK**.

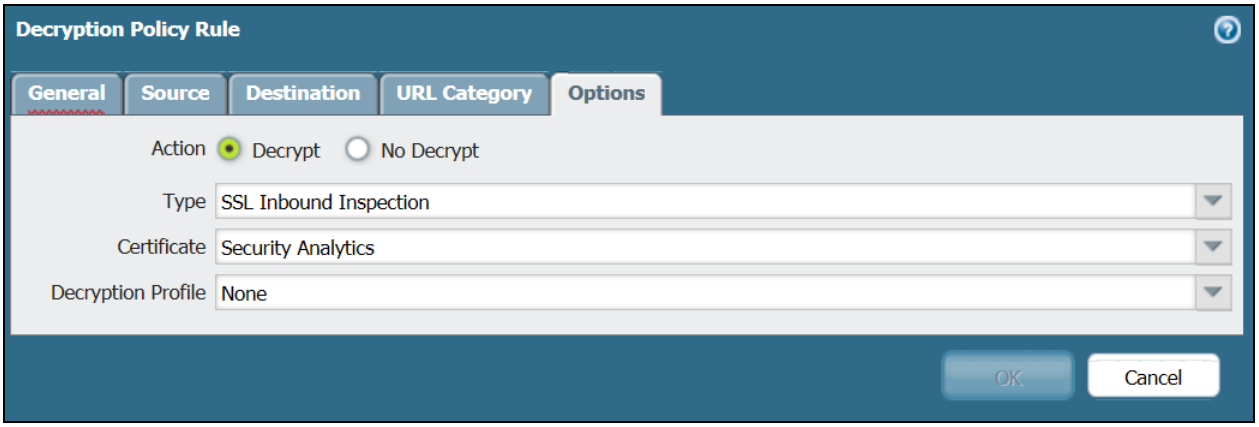


9. (***Optional***) Create a **Decryption Profile**. If you do not wish to create a **Decryption Profile**, skip to **step 13**.
10. Click **Objects** > **Decryption Profile** and click **Add**.
11. Select the SSL Inbound Inspection tab to block and control specific aspects of SSL traffic. For example, you can choose to terminate sessions if system resources are not available to process decryption by selecting Block sessions if resources not available.
12. Click **OK** to save the profile.
13. Next, click **Policies** > **Decryption** and Click **Add**.
14. On the **General** tab, give the policy a descriptive **name**.



15. On the **Source** and **Destination** tabs, select **Any** for the Source Zone and Destination Zone to decrypt all SSL traffic destined for an external server. If you want to specify traffic from or to certain sources or destinations for decryption, click **Add**.
16. In the URL Category tab, leave **Any** to decrypt all traffic. If you only want to apply this profile to certain website categories, click **Add**.

17. On the Options tab, select **Decrypt** and select **SSL Inbound Inspection** as the *Type* of decryption to perform.



18. (***Optional***) Select a **Decryption Profile** to apply additional settings to decrypted traffic (see *Step 9*).
19. Click **OK** to save.
20. Click **Commit** to save the configuration.

Note: With an SSL Inbound Inspection decryption policy enabled, all SSL traffic identified by the policy is decrypted and inspected. Decrypted traffic is blocked and restricted according to the profiles configured on the firewall (including the decryption profiles associated with the policy and Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking profiles). Traffic is re-encrypted as it exits the firewall.

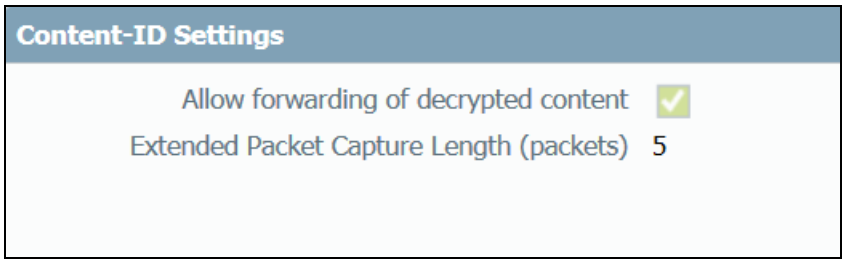
Decryption Port Mirror Configuration

The Decryption Port mirror feature provides the capability to create a copy of decrypted traffic from a firewall and send it to RSA Security Analytics for archiving and analysis. This feature is necessary for organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality. Decryption port mirroring is available on PA-7050, PA-5000 Series and PA-3000 Series platforms only and requires that a free license be installed to enable this feature.

Note: Please see the Palo Alto Admin documentation for further instructions to obtain and install the necessary license for Palo Alto.

On a Firewall with a Single Virtual System

1. Select **Device** > **Setup** > **Content - ID**.
2. Select the **Allow forwarding of decrypted content** check box.



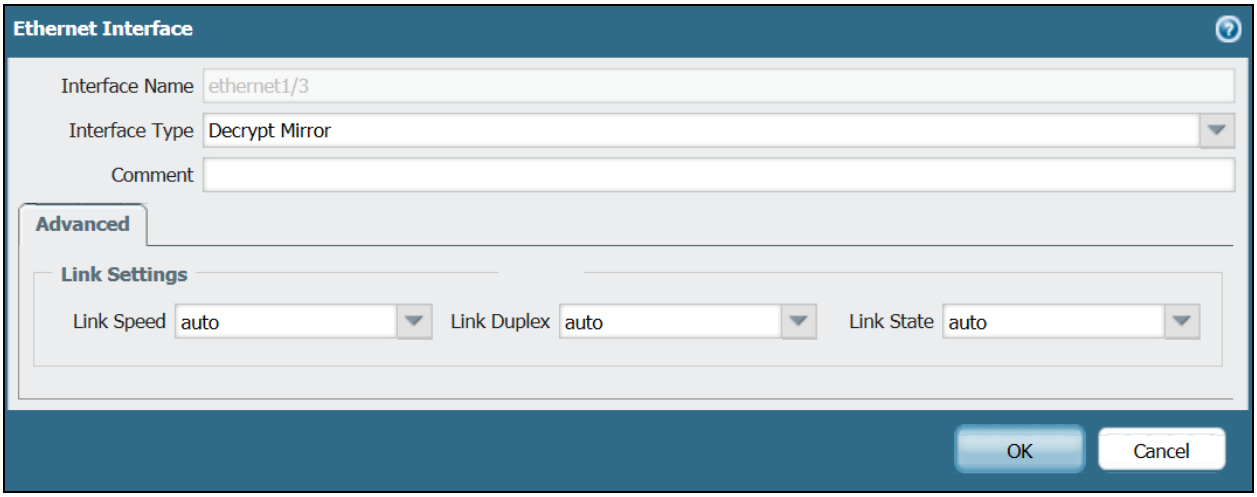
3. Click **OK** to save.

On a Firewall with Multiple Virtual Systems

1. Select **Device** > **Virtual System**.
2. Select a Virtual System to edit or create a new Virtual System by selecting **Add**.
3. Select the **Allow forwarding of decrypted content** check box.
4. Click **OK** to save.

Configure a Decrypt Mirror Interface

1. Select **Network** > **Interfaces** > **Ethernet**.
2. Select the Ethernet interface that you want to configure for decryption port mirroring.
3. Select **Decrypt Mirror** as the Interface Type. This interface type will only appear if the Decryption Port Mirror license is installed.

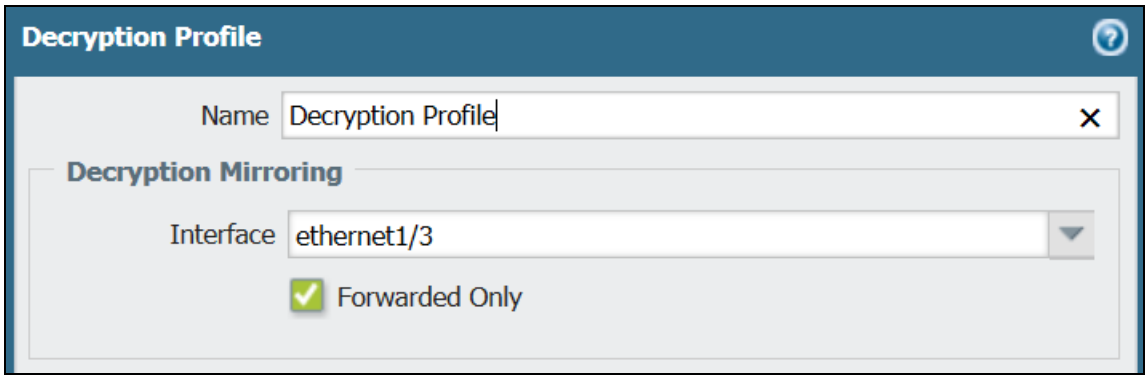


4. Click **OK** to save.

Configure a Decryption Profile to Enable Decryption Port Mirroring

1. Select **Objects** > **Decryption Profile.**
2. Select the Interface to use for Decryption Mirroring. The Interface drop-down contains all Ethernet interfaces that have been defined as the type: **Decrypt Mirror**.

> **Note: This is the interface that will be connected to the Security Analytics Packet Decoder.**



3. Specify whether to mirror decrypted traffic before or after policy enforcement.

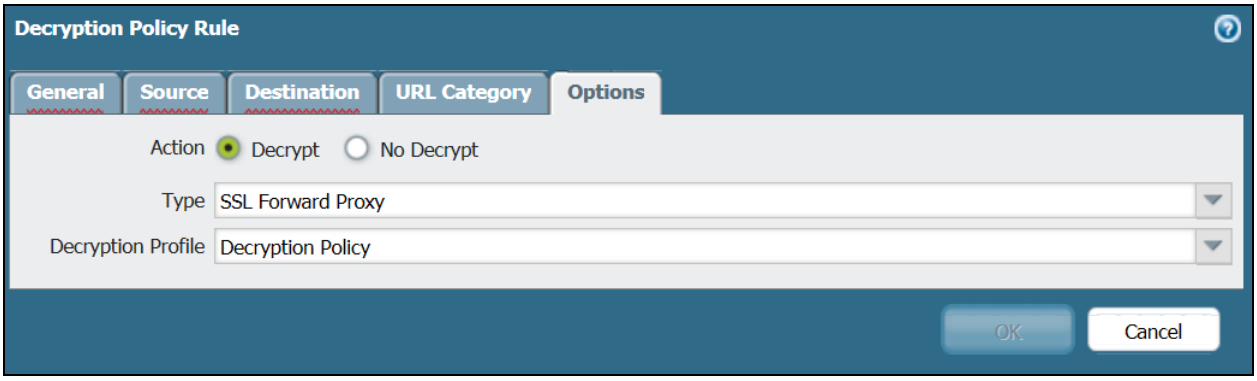
> **Note: By default, the firewall will mirror all decrypted traffic to the interface before security policies lookup, which allows you to replay events and analyze traffic that generates a threat or triggers a drop action. If you want to only mirror decrypted traffic after security policy enforcement, select the Forwarded Only check box. With this option, only traffic that is forwarded through the firewall is mirrored. This option is useful if you are forwarding the decrypted traffic to other threat detection devices, such as a DLP device or another intrusion prevention system (IPS).**

4. Click **OK** to save the decryption profile.

Set a decryption policy for decryption port mirroring

1. Select **Policies** > **Decryption**.
2. Click **Add** to configure a decryption policy or select an existing decryption policy to edit.

3. On the Options tab, select **Decrypt** and the **Decryption Profile** created in the above steps.



4. Click **OK** to save the policy.
5. Click **Commit**.

Certification Checklist for RSA Security Analytics

Date Tested: November 24th, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4	Virtual Appliance
Palo Alto PA-5050	6.1.0	Appliance

Security Analytics Test Case	Result
Outbound SSL Decryption	
HTTPS	
Google Search	✓
Bing Search	✓
Facebook	✓
YouTube	✓
Twitter	✓
LinkedIn	✓
Reddit	✓
WEBMAIL	
GMail	✓
Yahoo	✓
Live	✓
AOL	✓
Inbound SSL Decryption	
HTTPS	
Web Server	✓

JJO / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function