IDPS/NGFW Service Description

Scope, Features, and Responsibilities

Trustwave Security Technology Management (STM) provides a comprehensive set of solutions for IDPS/NGFW. IDPS/NGFW provides perimeter protection and inspection, threat, and data protection. Trustwave offers services for IDPS/NGFW solutions created by Trustwave and Trustwave's third-party partners.

Managed Security Services

This addendum is applicable to the following Trustwave services:

Table 1: ***Applicable Security Technology Management Service Description***

IDPS/NGFW Architecture Set-up	Applicable Service Description
Fully Cloud Platform	Security Technology Management (Cloud)
Fully On-Prem Architecture	Security Technology Management (On-Prem/Hybrid)
Hybrid – Cloud Management and On-Premise Appliances	Security Technology Management (On-Prem/Hybrid)

The Managed Detection service provides integration to core 24x7 threat detection capabilities. The relevant service descriptions are as follows:

Table 2: Applicable Threat Detection and Response Service Description

Monitoring Service Options	Applicable Service Description
Managed Detection Essentials or Complete	Threat Detection and Response: Managed Detection

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

Service Scope

Support Features

Trustwave offers support features to improve security. STM can enhance Client's technology by providing the correct configurations that meet Client's risk tolerance and security position. These support features include:

- **Threat Prevention**: a subscription that assists with protection against known viruses, spyware, and worms. Depending on the vendor, additional capabilities include drive-by protection and behavioral-botnet detection.
- **Sandbox Analysis** is a static and dynamic analysis over multiple operating systems and application versions. This feature analyzes samples of files and links and tags items for further investigation. Automatic contamination will occur when categorization is malicious.
- **High Availability** provides for continuous operation of the technology.
- **URL Filtering** allows for control of access to internal resources by granting or denying access to resources based on predetermined criteria and threat intelligence databases.
- **Web Content Filtering** provides web content classification to prevent users from access known malicious sites or inappropriate content.
- **Application Control** provides OSI model Layer 7 classification of applications.
- **Virtual Private Networks (VPN)** are encrypted communication links between supported devices for a site-to-site VPN or enablement of remote users to a supported device.

Table 3: Support Capabilities for Solution Vendor Subscriptions

Feature	IDPS	NGFW
Threat Prevention	X	X
Sandbox Analysis	X*	X*
High Availability	X	X
URL Filtering		X
Web Content Filtering		X
Application Control		X
VPN		X**
Network DMZ		X**

* Additional fee required.

** Default support is limited to one configuration. For additional configurations will require an additional fee.

Optional Premium Services

Such services enhance Client's experience and are offered at additional charge.

Co-Management

Co-Management provides Client with administrative access to non-managed features within a Managed Technology through its management UI.

Supported Features

Software-defined wide area networks (SD-WAN) allows Client to improve the application experience, security, and cloud connectivity optimization by simplifying the management and operation of a wide area network.

Supported Technology

Table 4: Approved Third Party Technology and Features

Third-party Vendor	Supported features for Co-Management
Fortinet	• SD-WAN
Palo Alto	• SD-WAN

RACI Model

The co-management RACI model describes how Trustwave and Client may work together to ensure the smooth operation of the Managed Technology.

R - Responsible, A - Accountable, C - Consulted, I - Informed

Table 5: SD-WAN RACI

Phase	Task	Client	Trustwave
Implementation	Project kick-off and discovery	CI	RA
	Creation of administration and Client direct accounts	CI	RA
	Implementation of device	CI	RA
	Initial network configuration	CI	RA
	SD-WAN and Network configuration	RA	CI
	Creation and implementation of security features and functions	I	RA
MSS Provisioning	Rack, stack, installation of Trustwave Connect Appliances, if applicable.	RA	CI
	Establish connectivity between Trustwave Fusion Portal and appliances to enable event collection, security monitoring and change management	I	RA

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.

Phase	Task	Client	Trustwave
	Trustwave Fusion Portal account creation	CI	RA
Operations	Threat detection and response	I	RA
	Health monitoring, backup and restoration, certificate management, product upgrades, and security patches	CI	RA
	Configuration maintenance and updates as described by a change request	CI	RA
	Updating security policies and features as described by a change request	CI	RA
	Updating Network and SD-WAN configuration and policies	RA	CI
	Updating of threat protection policies with new signatures	I	RA
	Recommended threat protection policy change by Trustwave	CI	RA
	Generation and viewing of reports	RA	I
	Technical assistance	CI	RA
	Escalation to solution vendor	I	RA

Co-Management Service Acknowledgements

Trustwave acknowledges:

- Trustwave will provide local user accounts to personnel identified by Client and the correct permissions to view and modify the features within the Managed Technology.
- For incidents in which it is unclear who has caused them, Trustwave will troubleshoot the incident until a classification is determined for accountability within RACI Matrix.
- Trustwave will not be held responsible for any outages, degradation in service or other incidents due to Client's changes on the Managed Technology(ies).

Client acknowledges:

- Client will have the skills necessary to support the Managed Technologies.
- Client will provide a list of contacts to be provided local accounts on the device for access to the Managed Technology.
- Device accounts will have limited write access to the Managed Technology(ies)
- Client accepts the risk of having multiple parties having the ability to make changes in the Managed Technology(ies)
- Client will record all changes made in a Ticket.
- Client will coordinate any changes that affect the security policy with the Trustwave SOC within the STM SLAs.
- Client is fully responsible for the configuration of any virtualization feature it modifies, which includes any configurations before and after deployment.

Definitions

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between Trustwave and Client.

IDPS means Intrusion Detection and Prevention Systems.

IPS means Intrusion Prevention Systems.

Managed Technology(ies) means Client's management console technology(ies) covered under the Service.

NGFW means the Next-Generation Firewall solution.

SLA means the service level agreement targets referred to in this Service description.

Ticket is a record of activities or alerts and documented within the Trustwave Fusion Platform.

Trustwave Fusion Portal means the Trustwave managed security service infrastructure utilized in providing the Service.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved.