RESPUESTAS A CONSULTAS DE LA LICITACIÓN ABREVIADA 37/2018

Pregunta 1: Cuando se habla de DLP (Data Loss Prevention), es un requerimiento opcional u obligatorio dentro de los servicios que debe incluir el UTM?
Respuesta 1: Es obligatorio.

Pregunta 2: En las especificaciones se habla de Antivirus y Antispam y dentro se solicita "Detección y detención de trafico spyware, adware, malware/grayware, etc". Lo que se solicita entonces ademas del Antivirus y el Antispam es un Advance Threats Detection ?
Respuesta 2: No es necesario un cotizar un Advance Threats Detection, la solución tiene que poder detectar los tráficos mencionados.

Pregunta3: Los servicios de AntiSPAM son para SMTP y/o IMAP? Ademas se requiere de un servidor de cuarentena?
Respuesta 3: No se requiere un servidor de cuarentena.

Pregunta 4: En los requerimientos de Firewall se dice que PPTP es valorado, comentamos que este ultimo a nivel de seguridad se comprobó que es inseguro y a sido eliminado o sustituido en su defecto por L2TP o IPSec. Se sugiere eliminar o en su defecto sustituir por L2TP.
Respuesta 4: Se elimina el valorado del PPTP.

Pregunta 5: En el Item 2.1.1 dice: "Actualmente el MSP cuenta con la solución de monitoreo PRTG)
Los Firewalls deben contar con la posibilidad de ser administrador con una herramienta que permita la gestión centralizada de las tareas.
También debe contar con una solución de logs e informes centralizados para los Firewall externos."

Esta claro que la herramienta de administración es para los 2 equipos, Data Center Pando y Centro, ademas deben de tener su propio Syslog, pero no queda claro cual o cuales son los otros Firewall externos, entendiendo que su hay otros, estos ya están integrados a la solución de PRTG.

Pregunta: La solución deberá tener un syslog para integrar en forma centralizada los logs pero para las cajas nuevas que se instalen, eso es correcto?
Respuesta 5: Es correcto, las cajas nuevas deben de contar un sistema de monitoreo centralizado (syslog)

Pregunta 6: El pliego habla de una solución de "alta disponibilidad, que la misma debe ejecutarse de manera automática, configurarse en modo activo-activo ya que ambos equipos tiene que atender requerimientos (request)".

En otro lado habla de "Configuración activo-activo - NO NECESARIAMENTE CLUSTER"

En la respuestas del 28 de marzo de 2019, Referente al Lote A Item 1, Pregunta 3, la Respuesta 3 habla de una solución Activo - Pasivo.

Entonces:
Escenario 1 : Entendiendo que el sitio con mas carga atiende peticiones hacia el mundo y el

sitio secundario también tiene una conexión a internet para que los usuarios salgan a internet, vemos recomendable que los 2 equipos tengan las funcionalidades de UTM, o sea que ambos funcionen como ACTIVO-ACTIVO.

Escenario 2: Caso contrario se tendría que rutear el trafico para que por ejemplo "Pando" sea el UTM Activo y este ultimo se encargue de sacar el trafico a internet y en ese caso funcionar como ACTIVO-PASIVO.

Cual de los dos escenarios es el que busca tener el Ministerio de Salud Pública?
Respuesta 6: La solución tiene que ser Activo-Activo, pero no es necesario que sea en Cluster. Cada sitio tiene sus servicios y en caso que un Firewall caiga el que está vivo tome los servicios de este.