UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

SEGURIDAD PREVENTIVA ACTIVA (IDPS) PARA INTERCONEXION DE REDES EMPRESARIALES

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MILTON EDWIN ALVAREZ VILCA

PROMOCION
1991- I

LIMA – PERU

SEGURIDAD PREVENTIVA ACTIVA (IDPS) PARA INTERCONEXION DE REDES EMPRESARIALES

Dedico esto a mis padres Nery y Ronald por la educación brindada, y mi esposa Charo, hija Cynthia por su paciencia y apoyo.

SUMARIO

El presente informe de suficiencia trata en primera instancia los principios y fundamentos de la tecnología IDPS y las características a considerar en la implementación, operación y mantenimiento. Se describe la implementación de una solución de seguridad basada en IDPS en una empresa en modalidad de servicio y finalmente se brinda recomendaciones para su implementación justificado por mejor costo beneficio frente a una solución propia.

El desarrollo de este informe consta de 3 capítulos, estructurados de la siguiente manera:

En el Capítulo I: Principios de la detección y prevención de intrusos.

Se describen el porqué del uso de los IDPS y cuáles son sus funciones básicas, así como las metodologías y tecnologías en que se basan para su funcionamiento.

En el Capítulo II: Fundamentos de la tecnología IDPS

Se hace mención a los componentes y arquitectura de red de una solución IDPS, así también su capacidad para brindar funciones de seguridad. Adicionalmente se brinda recomendaciones generales para la implementación, operación y mantenimiento de este tipo de soluciones.

En el Capítulo III: Implementación de IDPS en una empresa comercial en modalidad de servicio.

En este capítulo se describe el proyecto de implementación de una solución IDPS en modalidad de servicios realizado en una empresa en sus fases de evaluación, planeamiento, implementación, operación y mantenimiento.

En la parte final se encuentra las conclusiones y recomendaciones para la implementación de soluciones de seguridad basada en IDPS, así como la bibliografía y los acrónimos.

INDICE

CAPITULO III

SEGURIDAD PREVENTIVA ACTIVA (IDPS) PARA INTERCONEXION DE REDES EMPRESARIALES

PROLOGO

La seguridad es un complemento natural y esencial par las empresas por ese motivo mas y mas corporaciones requieren adicionar a la funcionalidad básica de filtrado de los Firewalls, medidas preventivas contra ataques hostiles y actividades contra sus sistemas, redes, aplicaciones y servicios a nivel de aplicaciones.
La prevención activa es un elemento natural a los servicios de seguridad, integrada con los servicios de firewall. La prevención activa también tiene la habilidad para llegar a ser un aliado natural en un en un enfoque granular holístico, seguridad multi-capa, que requiere los ambientes de negocio hoy en día.

La inspección del IDPS dada con la prevención activa tiene la habilidad para operar, identificar y bloquear en tiempo real, actividad sospechosa o maliciosa que atraviesa sobre toda la red. Mantener actualizado políticas de seguridad con una frecuente actualización de firmas, esto refleja las actuales amenazas y la capacidad para proteger a los clientes de red contra nuevos ataques.

La Prevención Activa usa una arquitectura de tres capas que consiste de la inspección (también conocidos como 'censores' o Dispositivos IDPS o cajas IDPS). El Network Storage Management Server y la administración de Interfase de Usuario.
La inspección del IDPS mira todo el tráfico de la red y son puntos de cumplimientos que implementan las Políticas de Seguridad.

CAPITULO I
PRINCIPIOS DE LA DETECCION Y PREVENCION DE INTRUSOS

La detección de intrusos es el proceso de monitoreo de los eventos ocurridos en un sistema de computadoras o red y los analiza por signos de posibles incidentes, cuales son violaciones o inminentes amenazas de violaciones de las políticas de seguridad, uso aceptable de las políticas o prácticas de seguridad estándares. Los incidentes tienen muchas causas, tales como malware (ejemplos, gusanos, spyware), atacantes ganando acceso no autorizados de internet, y usuarios autorizados de los sistemas quienes hacen mal uso de sus privilegios o intentos para ganar privilegios adicionales que ellos no están autorizados. Aunque muchos incidentes son maliciosos por naturaleza, muchos otros no lo son; por ejemplo, una persona escribe en forma errada una dirección de una computadora e intenta accidentalmente conectarse a un sistema diferente sin autorización.

Un sistema de detección de intrusos es software que automatiza el proceso de detección. Un sistema de prevención es software que tiene toda la capacidad de un sistema de detección de intrusos y también puede intentar parar los posibles incidentes.

Las tecnologías de IDS y IPS ofrecen mucha de las mismas capacidades, y los administradores pueden usualmente deshabilitar características de prevención en los productos IPS, causando que funcionen como IDS. De acuerdo a esto, para abreviar se usará el termino IDPS para sistema de detección de intrusos y sistemas de prevención (intrusion detection and prevention systems) para referirse de ambas tecnologías.

1.1 Uso de las tecnologías de IDPS

Los IDPS están primariamente enfocados en identificar posibles incidentes. Por ejemplo, un IDPS podría detectar cuando un atacante tiene éxito al comprometer a un sistema explotando una vulnerabilidad en un sistema. Los IDPS podrían entonces reportar incidentes a los administradores de seguridad, quienes podrían rápidamente iniciar acciones de respuestas al incidente para minimizar los daños causados por el incidente. Los IDPS podrían también registrar información que podría ser usado por los encargados de

incidentes. Los IDPS podrían también ser configurados para reconocer violaciones de políticas de seguridad. Por ejemplo, algunos IDPS pueden ser configurados con reglas configuradas en los Firewalls, permitiéndoles identificar tráficos de red que viola la política de seguridad o el uso aceptable de las políticas. También, algunos IDPS pueden monitorear trasferencia de archivos y identifican a los que podrían ser sospechosos, tal como copiar una gran base de datos en el usuario de una portátil.

Muchos IDPS también pueden identificar actividades de reconocimiento, cuales indicarían que un ataque es inminente. Por ejemplo, algunas herramientas de ataques y formas de malware, particularmente gusanos, ejecutan actividades de reconocimiento tales como revisión de equipos y puertos tcp para identificar objetivos para el subsiguiente ataque.

Un IDPS debería ser capaz de bloquear el reconocimiento y notificar al administrador de seguridad, quienes pueden tomar acción si requiere alterar otro control de seguridad para prevenir el incidente relacionado. Porque las actividades de reconocimiento son frecuentes en Internet, la detección de reconocimiento es a menudo ejecutado primariamente en la protección de redes internas.

En suma para identificar incidentes y soportar los esfuerzos de respuestas a los incidentes, las organizaciones han encontrado otros usos para los IDPS, incluyendo lo siguiente:

Identificar problemas en políticas de seguridad. Un IDPS puede proveer algún grado de control de calidad para la implementación de las políticas, tales como duplicando las reglas del firewall y alertándolo cuando observa trafico en la red que debería haber sido bloqueado por el firewall pero no estaba porque había un error en la configuración.

Documentar las amenazas existentes a una organización. Los IDPS registra la información de las amenazas que detecta. Entendiendo la frecuencia y las características de los ataques contra un recurso computacionales de la organización es de mucha ayuda para identificar las apropiadas medidas de seguridad para proteger los recursos. La información puede también ser usado para educar a los gerentes acerca de las amenazas que enfrenta la organización.

Desalentar a los individuos de violar las políticas de seguridad. Si los individuos son capaces que sus acciones están siendo monitoreados por las tecnologías de IDPS para violaciones de políticas de seguridad, ellos seguramente estarán menos alentados de realizar tales violaciones por el riesgo de ser detectados. Por el incremento de la

dependencia de los sistemas de información y la prevalencia y potencial impacto en contra de las intrusiones de estos sistemas, los IDPS han llegado a ser una necesidad adicional a la infraestructura de seguridad de cada organización.

1.2 Funciones claves de la tecnología IDPS.

Hay muchas tecnologías de IDPS, cuales están diferenciadas primariamente por el tipo de eventos que ellas pueden reconocer y las metodologías que usan para identificar incidentes. En suma el monitoreo y análisis de eventos para identificar actividad indeseada, todo tipo de tecnología de IDPS típicamente ejecuta las siguientes funciones:

a) Registrar información relacionada para observar eventos. Información es usualmente registrada localmente, y también será enviada a sistemas separados tal como servidores de eventos centralizados, información se seguridad y solución de administración de eventos, y sistemas empresariales de administración.

b) Notificar a los administradores de seguridad de eventos importantes observados. Esta notificación conocida como una alerta, ocurre a través de cualquiera de los varios métodos, incluyendo los siguientes: correos electrónicos, paginas, mensajes sobre las interfaces de usuarios de los IDPS, Simple Network Management Protocol (SNMP), traps, mensajes syslog, y programas definidos por los usuarios y scripts. Un mensajes de notificación típicamente incluye solo información básica considerando un evento; los administradores requieren acceder a los IDPS para información adicional.

c) Reportes producido. Reportes resumen de los eventos monitoreados o detalles dados en eventos particulares de interés.

Algunos IDPS son también capaces de cambiar su perfil de seguridad cuando una nueva amenaza es detectada. Por ejemplo un IDPS sería capaz a coleccionar mas información detallada para una sesión en particular después una actividad maliciosa es detectada dentro de esa sesión. Un IDPS seria también alteraría las configuraciones para cuando ciertas alertas son disparadas o que prioridades deberían ser asignadas para alertas después una amenaza en particular es detectada.

Las tecnologías IPS son diferenciadas de las tecnologías IDS por una característica: las tecnologías IPS pueden responder a una amenaza detectada intentando prevenirla de que logre su cometido. Ellas usan varias técnicas de respuesta, cuales pueden ser divididas en los siguientes grupos:

- **El IPS detiene el ataque por si mismo**. Ejemplo esto podría ser hecho como sigue:

  Termina la conexión de la red o sesión de usuario que están siendo usados para el ataque.

  Bloquea el acceso al objetivo desde la cuenta de usuario agresor, dirección IP, u otro atributo del atacante.

  Bloquea todo acceso a los host objetivos, servicio, aplicación, u otro recurso.

- **El IPS cambia el entorno de seguridad.** El IPS podría cambiar la configuración de otros controles de seguridad para interrumpir un ataque. Ejemplos comunes son reconfigurar un dispositivo de red (ejemplo firewall, router, switch) para bloquear accesos desde los atacantes o al objetivo, y alterar un firewall basado en host en un objetivo para bloquear ingreso de ataques. Algunos IPS pueden aun causar aplicar parches a los host si el IPS detecta que los host han sido vulnerados.

- **El IPS cambia el contenido de los ataques.** Algunas tecnologías de IPS pueden remover o reemplazar la porción de un ataque para hacerlo benigno. Un simple ejemplo es un IPS removiendo un archivo infectado anexo en un correo electrónico y entonces permite el correo limpiado alcanzar su recipiente. Un mas complejo ejemplo es un IPS que actúa como un Proxy y normalice los requerimientos de ingreso, cual significa que el Proxy repaquetiza las etiquetas de los requerimientos, descartando las cabeceras de información. Esto causaría ciertos ataques para ser descartados como parte del proceso de normalización.

Otro atributo común de las tecnologías de IDPS es que ellos no pueden dar completamente detección segura. Cuando un IDPS identifica incorrectamente una actividad benigna como maliciosa, un falso positivo ha ocurrido. Cuando un IDPS falla para identificar actividad maliciosa, un falso negativo ha ocurrido. No es posible eliminar todo los falsos positivos y negativos; en muchos casos, reducir la ocurrencia de uno incrementa la ocurrencia de la otra.

Muchas organizaciones escogen reducir falsos negativos con el costo de incrementar los falsos positivos, cual significa que mayores eventos son detectados pero mas recursos de análisis son necesitados para diferenciar falsos positivos de eventos maliciosos verdaderos. Alterando la configuración de un IDPS para mejorar su detección predictiva es conocido como afinamiento (tunning).

Las mayorías de IDPS también ofrecen características que compensen el uso de técnicas comunes de evasión. La evasión se realiza modificando el formato o tiempo de actividad malicioso que también los cambios de apariencia pero sus efectos es el mismo. Los atacantes usan técnicas de evasión para tratar para prevenir tecnologías de IDPS de su detección de sus ataques. Por ejemplo, un atacante podría codificar caracteres en una forma en particular, conociendo que el destino entiende la codificación y esperando que ningún IDPS lo monitoree. La mayoría de las tecnologías de IDPS pueden superar técnicas comunes de evasión duplicando el procesamiento especial realizado por los objetivos. Si los IDPS pueden ver la actividad en la misma forma que los objetivos pueden, entonces técnicas de evasión generalmente no serán exitosas en esconder ataques.

1.3 Metodología común para la detección.

Las tecnologías IDPS utilizan muchas metodologías para detectar incidentes: basado en firmas, basado en anomalías, análisis del protocolo stateful, respectivamente. La mayoría de las tecnologías de IDPS usa múltiples metodologías, separadas o integradas, para brindar un mayor espectro y seguridad de detección.

Para este trabajo se nombrará metodologías primarias: basado en firmas, basado en anomalías, y análisis del protocolo stateful. Las mayorías de las técnicas de IDPS usan múltiples metodologías de detección, que separadamente o integrada, puede proveer más amplitud y segura detección.

1.3.1 Detección basada en firmas: Una firma es un patrón que corresponde a una amenaza conocida. La detección basada en firmas es el proceso de comparar firmas contra eventos observados para identificar posibles incidentes. Ejemplo de firmas son las siguientes:

- Un intento de Telnet con un usuario “root”, cual es una violación de una política de seguridad.
- Un e-mail con un asunto de “Free Pictures!” y un archivo adjunto de “freepics.exe”, cual son características de conocidas formas de malware.
- Una entrada de registro del sistema operativo con una entrada con valor 645, cual indica que auditoria de hosts ha sido deshabilitado.

La detección basada en firmas es muy eficiente en detectar amenazas conocidas pero totalmente inefectivas en detectar amenazas desconocidas, las amenazas se esconden por el

uso de estas técnicas de evasión, y muchas variantes de las amenazas conocidas. Por ejemplo, si un ataque modificado de malware en el ejemplo previo usa un archivo con nombre de "freepics2.exe", una búsqueda de la firma para "freepics.exe" no se encontraría.

La detección basada en firma es un simple método de detección y solo compara la unidad actual de actividad, tal como un paquete o entrada en el registro, para una lista de firmas usando cadenas operativas de comparación.

La tecnología de detección basada en firmas tiene poco entendimiento de muchas redes o protocolos de aplicaciones y no puede seguir y entender al estado de las comunicaciones complejas. Por ejemplo, ellos no pueden juntar una solicitud con una respuesta correspondiente, tal como conocer que una respuesta a un servidor Web para una particular pagina generado a repuesta al estado código 403, significa que el servidor rechaza llenar la solicitud. También carece la habilidad para recordar previas solicitudes cuando procesan una respuesta actual. Esta limitación previene al método basado en firmas de detectar ataques que comprometen múltiples eventos si ningunos de los eventos contienen una clara indicación de un ataque.

1.3.2 Detección basada en anomalías.

La detección basada en anomalías es el proceso de comparar definiciones de que actividad es considerada norma contra eventos observados para identificar desviaciones significativas. Un IDPS usando este tipo de detección tiene perfiles que representan el normal comportamiento de tales cosas como usuarios, hosts, conexiones de red, o aplicaciones. Los perfiles son desarrollados monitoreando las características de actividades típicas sobre un período de tiempo. Por ejemplo, un perfil para una red mostraría que la actividad Web es parte de un promedio de 13% de un ancho de banda de Internet durante las horas de trabajo. El IDPS entonces utiliza métodos estadísticos que comparan las características de la actividad actual para un umbral relativo al perfil, tal como detectar cuando la actividad Web es parte significativa del uso del ancho de banda del esperado y alerta al administrador de la anormalidad. Los perfiles pueden ser desarrollados para muchos atributos de comportamiento, tal como los números de correos enviados por un usuario, el número de intentos fallidos de ingreso para un host, y el nivel de uso de procesador para un host en período de tiempo determinado.

El mayor beneficio de método basado en detección por anomalías es que pueden ser efectivos en detectar amenazas desconocidas. Por ejemplo, suponer que un computador

llega a ser infectado con un nuevo tipo de malware. El malware puede consumir los recursos de procesamiento del computador, enviando números grandes de correos, iniciando grandes números de conexiones, y ejecutar otro comportamiento que sería significativamente diferente del perfil establecido por el computador.

Un perfil inicial es generado por un periodo de tiempo (típicamente días, a veces semanas) algunas veces llamado período de aprendizaje. Los perfiles para detección basada en anomalías pueden también ser estáticos o dinámicos. Una vez generado, un perfil estático es cambiado a menos que el IDPS es específicamente dirigido a generar un nuevo perfil. Un perfil dinámico es ajustado constantemente con eventos adicionales que son observados. Porque los sistemas y las redes cambian en el tiempo, las medidas correspondientes de el comportamiento normal también cambia, un perfil estático eventualmente llegará a ser inseguro, por lo que necesita ser regenerado periódicamente. Perfiles dinámicos no tienen este problema, pero ellos son susceptibles para intentos de evasión de los atacantes. Por ejemplo, un atacante puede ejecutar pequeñas cantidades de actividades maliciosas ocasionalmente, entonces incrementa lentamente la frecuencia y la cantidad de la actividad. Si la cantidad de cambios es pequeña, el IDPS pensaría que la actividad normal es un comportamiento normal e incluido en su perfil. Actividad maliciosa sería también observada por un IDPS mientras construye su inicial perfil.

Inadvertidamente la inclusión de actividad maliciosa como parte de un perfil es común con producto IDPS basado en anomalías. (En algunos casos, administradores pueden modificar el perfil para excluir actividad en el perfil que es conocido ser malicioso). Otro problema con construir perfiles es que puede ser muy retador en algunos casos hacer que sean seguros, porque computan actividad demasiada compleja. Por ejemplo, si una actividad de mantenimiento en particular que ejecuta grandes transferencias de archivos ocurre una vez al mes, no sería observado durante el período de aprendizaje: cuando el mantenimiento ocurre, es seguro que será considerado una desviación significativa del perfil y disparará una alerta.

Los productos IDPS basados en anomalías a menudo produce muchos falsos positivos porque actividad benigna que desvía significativamente de los perfiles, especialmente en ambientes dinámicos.

Otro problema resaltante con el uso de esta técnica es que a menudo difícil para el análisis determinar porque una alerta particular fue generado y validado que una alerta es

segura y no un falso positivo, porque de la complejidad de los eventos y su número generaría alertas.

1.3.3 Análisis de Protocolo Stateful

Análisis de protocolo stateful es el proceso de comparar perfiles predeterminado de definiciones generalmente aceptadas de actividad de protocolo benigna para cada estado del protocolo contra los eventos observados para identificar desviaciones. A diferencia del protocolo anterior, cual usa perfiles específicos para los servidores o redes, análisis protocolo stateful es soportado por un perfil universal desarrollado por los fabricantes que especifica como los protocolos particulares deberían ser usados o no. Los "stateful" en el análisis del protocolo stateful significa que el IDPS es capaz de entender y hacer seguimiento del estado de la red, transporte, y protocolos de aplicación que tiene una noción de estado. Por ejemplo, cuando un usuario comienza a sesión de File Transfer Protocol (FTP), la sesión es inicialmente en un estado no autenticado. Usuarios no autenticados deberían solo ejecutar unos pocos comandos en este estado, tal como vemos en la información de ayuda o entregar usuarios y claves. Un importante parte de entender el estado es emparejar solicitudes y respuestas, cuando una autenticación FTP intenta ocurrir, el IDPS puede determinar si fue exitoso encontrar el código del estado en respuesta correspondiente.

Uno de los usuarios tiene exitosamente autenticado, la sesión esta en estado autenticado, y usuarios son esperados para ejecutar cualquier docena de comandos. Ejecutar la mayoría de estos comandos mientras en el estado no autenticado debería ser considerado sospechoso, pero en la ejecución del estado de autenticación la mayoría de ellos son considerados correctos.

Análisis del protocolo stateful puede identificar secuencias no esperadas de comandos, tal como emitir el mismo comando repetidamente o emitir un comando sin primero emitir un comando debajo el cual es dependiente.

Otro estado de la característica del seguimiento del análisis del protocolo stateful es que para los protocolos que ejecutan autenticación, los IDPS pueden mantener el seguimiento de los autenticadotes usados para cada sesión, y registrar el autenticador usado para la actividad sospechosa. Esto es de mucha ayuda cuando se investiga un incidente. Algunos IDPS pueden también usar la información del autenticador para definir aceptable actividad diferenciándola de los múltiples usuarios o usuarios específicos.

El análisis del protocolo ejecutado por este método usualmente incluye razonables chequeos para comandos individuales, tal como mínimos o máximos longitudes para los argumentos. Si un comando típicamente tiene un argumento de nombre de usuario, y tiene máximo 20 caracteres, entonces un argumento con una longitud de 1000 caracteres es sospechoso. Si el argumento contiene data binaria, entonces es aún más sospechoso.

Este método usa modelos de protocolos, cual esta típicamente basado primariamente el en el protocolo estándar de los vendedores de software y entidades (Ejemplo Internet Engineering Task Force [IETF] Request for Comments [RFC]). El modelo de protocolo también tópicamente toma en cuenta variantes en cada implementación del protocolo. Muchos estándares no son completamente exhaustivos en explicar el detalle de los protocolos, cual causa variaciones entre las implementaciones. También, muchos vendedores también violan estándares o añaden nuevas características, algunos de cuales reemplazarían características de los estándares. Para los protocolos propietarios, detalles completos acerca de los protocolos no están a menudo disponibles, haciendo esto difícil para la tecnología de los IDPS ejecutar un análisis preciso y seguro. Como protocolos son revisados y los vendedores alteran sus protocolos implementados, los modelos de protocolos IDPS necesitan ser actualizados para reflejar estos cambios.

La principal desventaja para este método es que son muy demandantes de recursos por su complejidad de análisis y la sobrecarga involucrada en ejecutar seguimiento de los estados para cada sesión simultanea. Otro serio problema es que este método no puede detectar ataques que no violan las características de comportamiento generales aceptables del protocolo, tal como ejecutar muchos acciones benignas en un período corto para causar denegación del servicio. Aún otro problema es que el modelo del protocolo usado por un IDPS entraría en conflicto con la manera del protocolo es implementado en un particular versión de aplicaciones especificas y sistemas operativos, o como cliente diferente y implementaciones de servidores de los protocolos interactivos.

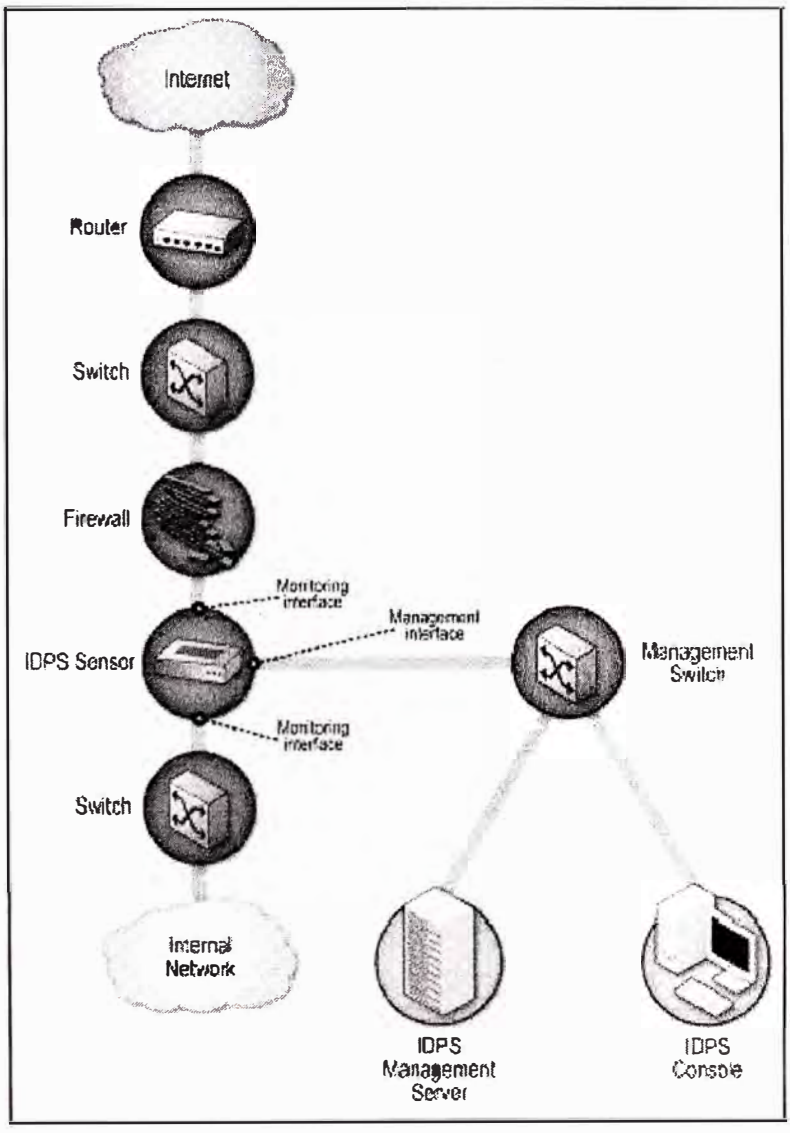
1.4. Tipos de Tecnologías IDPS

Hay muchos tipos de tecnologías IDPS, para el propósito de este trabajo, se han divididos en los siguientes cuatro grupos basados en el tipo de eventos que se monitorea y la forma en el cual son implementados:

1.4.1 Basado en redes: cuyos monitores de tráficos de red para segmentos de redes o dispositivos y análisis de red y actividad de protocolo de aplicaciones para identificar

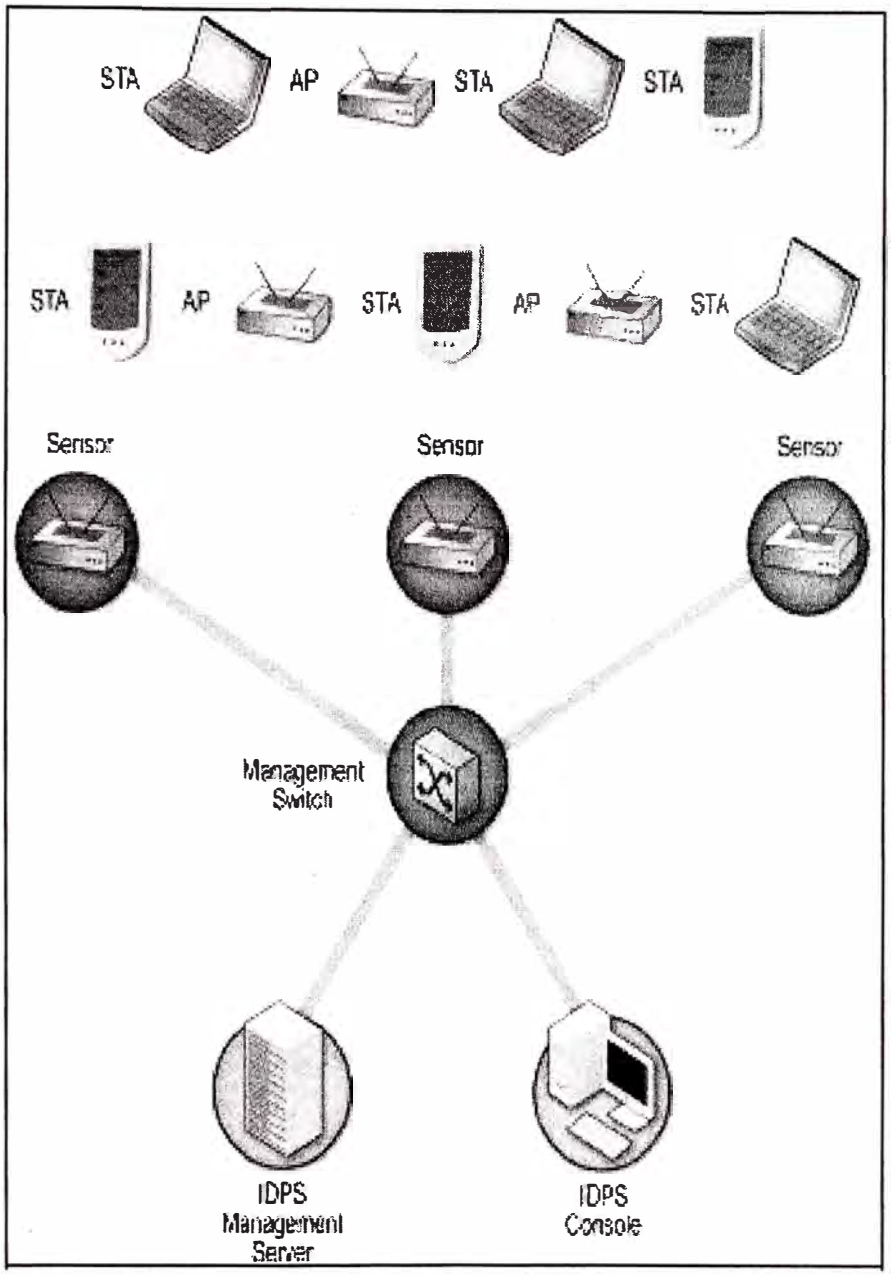
actividad sospechosa. Puede identificar muchos tipos diferentes de eventos de interés. Es más comúnmente implementada en los bordes entre redes, tal como en proximidades de firewall o routers de borde, servidores de redes VPN, servidores de acceso remoto, y redes inalámbricas (Wireless).

Figura 1: Ejemplo de arquitectura IDPS basado en redes



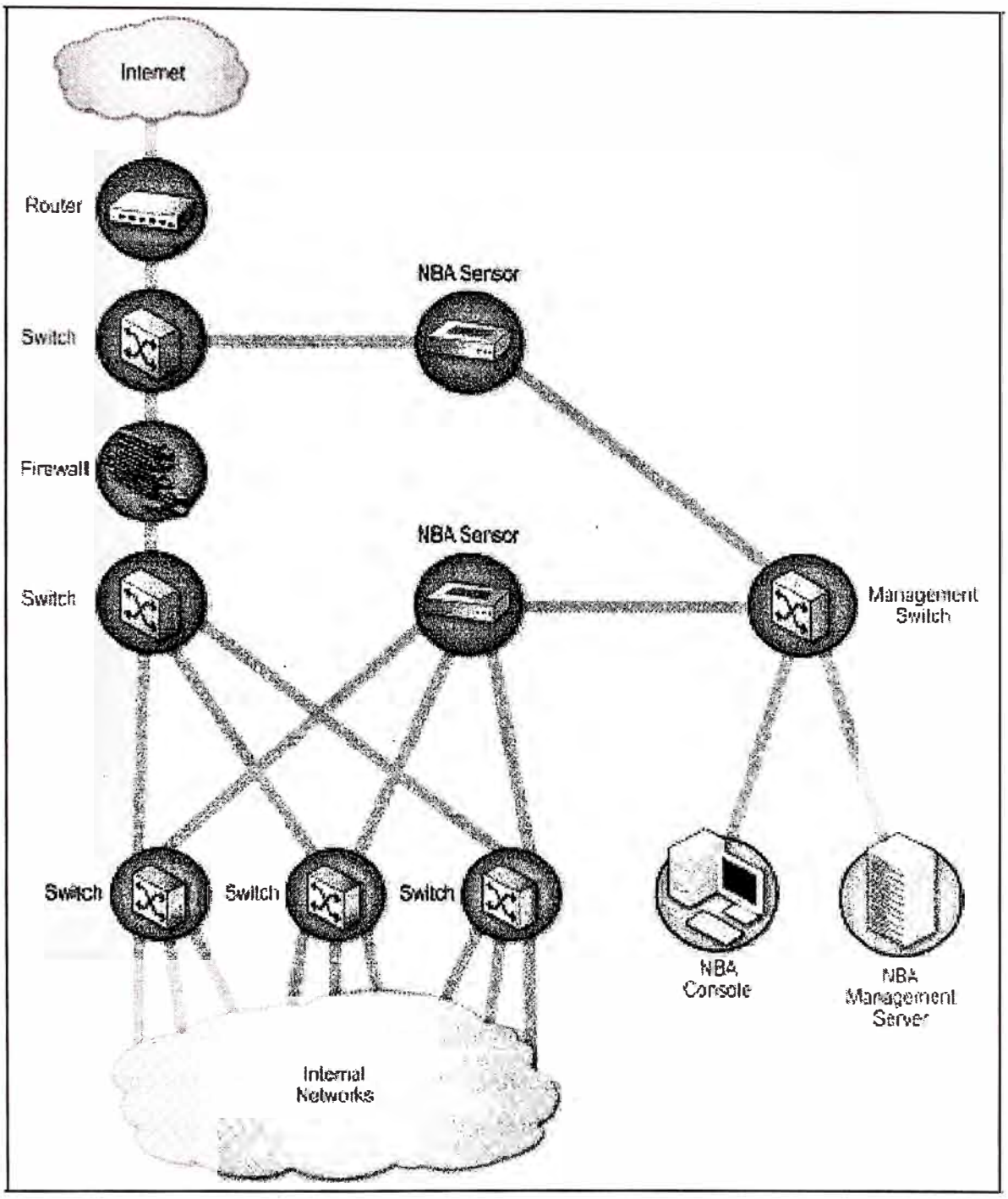
1.4.2 Basado en Wireless: cuyos monitores de tráfico de red de wireless y análisis son protocolos de redes wireless para identificar actividad sospechosa en si mismo los protocolos. No puede identificar actividad sospechoso en la aplicación o protocolos a nivel de capas más altas de protocolos (ejemplo TCP, UDP) que el tráfico de redes Wireless es transfiriendo. Es mas comúnmente implementado dentro rango de una red wireless de una organización monitorearla, pero puede también ser implementada en ubicaciones donde redes wireless no autorizados pueden suceder.

Figura 2:Ejemplo de arquitectura IDPS basado en Wireless



1.4.3 Basado en análisis de comportamiento de redes (NBA-Network Behavior Analysis), cual examina tráfico de redes para identificar amenazas que genera flujo tráfico inusual, tal como distribuir ataques de denegación de servicio (DoS), ciertos formas de malware (ejemplo gusanos, puertas traseras), y violación de políticas (ejemplo un sistema de cliente que provee servicios de redes a otros sistemas), sistemas NBA son mas a menudo implementado para monitorear flujos en redes internas, y son también algunas veces implementados donde pueden ser flujos monitoreados entre unas redes de la organización y redes externas (ejemplo el Internet, redes de socios de negocio).

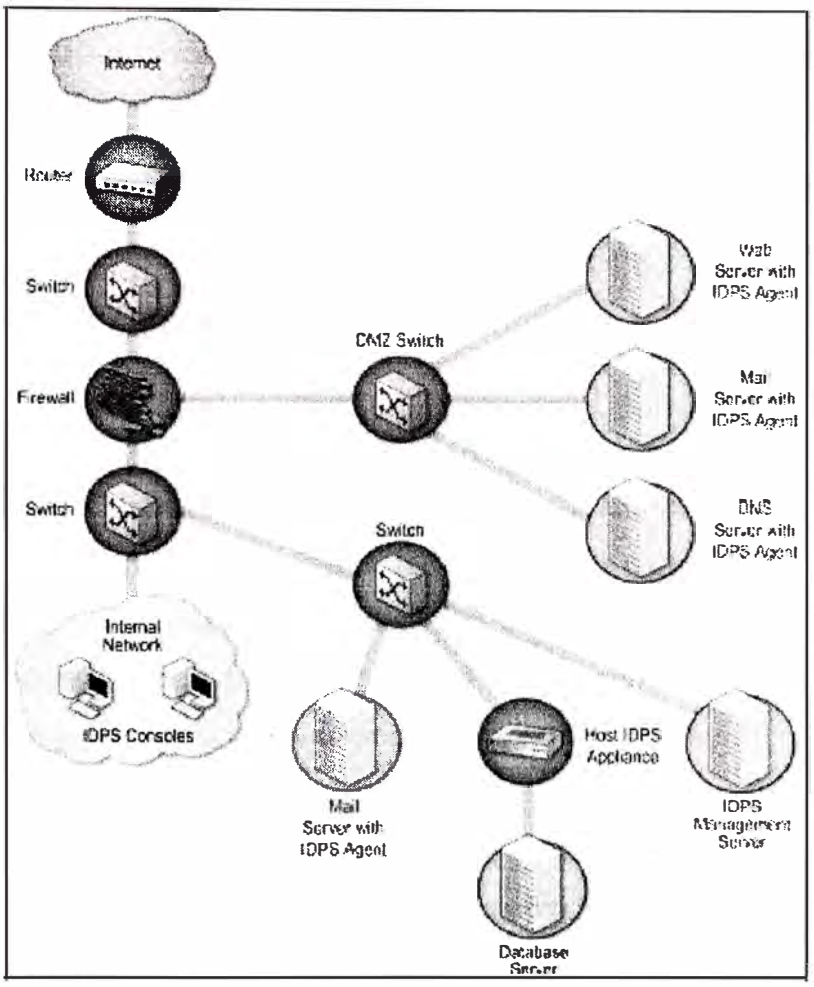
Figura 3: Ejemplo de arquitectura IDPS para análisis de redes (NBA)



1.4.4 Basado en Host, cual monitorea las características de un simple host y los eventos ocurridos dentro que los host por actividad sospechosa. Ejemplos de los tipos de características un IDPS basado en host monitorearía estos tráfico de redes (solo para este host), logs del sistema, procesos ejecutándose, actividad de las aplicaciones, accesos a archivos y modificaciones, y cambios en las configuraciones de aplicaciones y sistemas.

IDPS basado en host son mas comúnmente implementado donde los hosts son críticos tal como servidores accesibles públicamente y servidores conteniendo información sensible.

Figura 4: Ejemplo de arquitectura IDPS basado em Host



Algunas formas de IDPS son mas maduras que otras porque han estado en uso mucho más tiempo. IDPS basado en redes y algunas formas de IDPS basado en host han sido comercialmente disponible por sobre diez años. Software de análisis de comportamiento de redes es un relativamente nuevas formas de IDPS que evoluciona en parte forma productos creado primariamente para ataques de denegación de servicio (DoS), y en parte de productos desarrollados para monitorear flujos de tráfico en redes internas. Tecnología de inalámbrica (Wíreless) son un nuevo tipo relativamente de tipo de IDPS, desarrollado en respuesta para la popularidad de redes locales inalámbricas (WLAN) y el crecimiento de amenazas contra las WLANs y clientes WLAN.

CAPITULO II
FUNDAMENTOS DE LA TECNOLOGIA IDPS.

2.1 Componentes y arquitectura

Este capitulo describe los componentes de una solución IDPS e ilustra la mayoría de los componentes de red para esta arquitectura.

2.1.1 Componentes típicos

Los componentes típicos en una solución IDPS son los siguientes:

1) **Censor o agente**: Censores y agentes monitorean y analizan actividad. El termino censor es típicamente usado para los IDPS que monitorean redes, incluyendo basados en red, wireless, y tecnologías basado en análisis del comportamiento de redes. El término agente es típicamente usado para tecnologías basado en host en IDPS.

2) **Servidor de administración (Management Server)**. Un servidor de administración es un dispositivo centralizado que recibe información de los censores o agentes y los administra. Algunos servidores de administración ejecutan análisis sobre la información de eventos que los censores o agentes proveen y pueden identificar eventos que el censor individual o agente no puede. Comparar información de eventos de múltiples censores o agentes, tal como encontrar eventos producidos por la misma dirección IP, es conocido como correlación. Los servidores de administración están disponibles como appliance y productos basados en software. Algunas implementaciones pequeñas de IDPS no usan servidores de administración, pero la mayoría de implementación de IDPS lo hace. En grandes implementaciones de IDPS, hay muchos servidores de administración, y en algunos casos hay dos capas de servidores de administración.

3) **Servidor de base de datos**. Un servidor de base de datos es un repositorio para los eventos de información grabada por los censores, agentes, y/o servidores de administración. Muchos IDPS proveen soporte para servidores de base de datos.

4) **Consola**. Una consola es un programa que provee una interfase para el usuario IDPS y administrador. El software de consola es típicamente instalado sobre una PC estándar o una portátil. Algunas consolas son usadas para administración de IDPS solamente, tal como

configurar censores y agentes y aplicar actualizaciones de software, mientras otras consolas son usadas estrictamente para monitorear y análisis. Algunas consolas de IDPS proveen ambas capacidades de administración y monitoreo.

2.1.2 Arquitectura de red.

Los componentes pueden ser conectados cada uno a través de redes estándares de la organización o a través a red separada estrictamente diseñada para administración de software de seguridad de redes conocido como una red administrada.

Si una red administrada es usada, cada censor o agente host tiene una interfase adicional de red conocido como interfase de administración que conecta a una red administrada.

También cada censor o agente es incapaz pasar cualquier tipo de tráfico entre su interfase de administración y cualquier de sus interfaces de red. Los servidores de administración, servidores de base de datos, y consolas son conectados a la red de administración solamente. Esta arquitectura efectivamente aísla la red de administración de redes en producción.

Los beneficios de hacer este son para esconder la existencia e identidad de los IDPS de los atacantes, y asegurar que los IDPS tengan un adecuado ancho de banda para funcionar sobre condiciones adversas (ejemplo ataque de gusanos o denegación de servicio en redes monitoreadas).

La desventaja de usar una red administrada incluye un costo adicional en redes equipadas y otros equipos (ejemplo PC para consolas) y el inconveniente para los usuarios de IDPS y administradores de usar computadoras separadas para la administración y monitoreo.

Si un IDPS es implementado sin una red separada para administración, otra forma de mejorar la seguridad de IDPS es crear una red virtual de administración usando VLAN dentro de las redes estándares. Usando una VLAN provee protección para las comunicaciones del IDPS, pero no tanta protección como un red separada de administración. Por ejemplo, mala configuración de una VLAN podría dejar expuesto los datos del IDPS.

Otro problema es que bajo condiciones adversas, tal como ataques de denegación de servicio o incidentes mayores de malware, los dispositivos de redes compartidos por redes principales de la organización y VLAN podrían llegar a estar completamente saturadas, impactando negativamente la disponibilidad y performance de los IDPS.

2.2 Capacidad de seguridad

La mayoría de las tecnologías de IDPS pueden proveer una variedad de capacidades de seguridades, a continuación se describen dimidos en cuatro categorías: recolectar información, registro, detección y prevención respectivamente:

2.2.1 Capacidad de recolectar información

Algunas tecnologías de IDPS ofrecen capacidades de recolectar información, tal como información de actividad de hosts y redes observadas. Ejemplo incluye identificar hosts y sistemas operativos y aplicaciones que se usa, e identifica las características generales de la red.

2.2.2 Capacidades de registro

Los IDPS típicamente ejecutan extensos registros de data relacionada para detectar eventos entre los IDPS y otras fuentes de registros. Campos de datos usados por los IDPS incluyendo eventos de fecha y tiempo, tipo de evento, calificación de la importancia (ejemplo prioridad, severidad, impacto, seguridad), y acciones preventivas ejecutadas. Los tipos específicos de registro de los IDPS de campos adicionales, tal como IDPS basados en redes ejecutando paquetes de captura y IDPS basados en host registran la identificación del usuario (user IDs). La tecnología de los IDPS típicamente permiten a los administradores almacenar registros locamente y enviar copias de los registros a servidores centralizados de registros (ejemplo syslog, software de administración de seguridad de información y manejo de eventos). Generalmente, los registros deben almacenarse en ambos localmente y centralizadamente para soportar la integridad y disponibilidad de la data (ejemplo compromiso de los IDPS podría permitir a los atacantes alterar o destruir sus registros). También los IDPS deberían tener sus relojes sincronizados usando el protocolo de sincronización de hora (NTP) o a través de ajustes manuales frecuentes para que sus entradas de registros tengan asegurada el sello de tiempo.

2.2.3 Capacidad de detección

La tecnología de IDPS típicamente ofrece extensivos, y amplias capacidades de detección. La mayoría de los productos usa una combinación de técnicas, las cuales soportan una mayor detección segura y mayor flexibilidad en ajuste y personalización. Los tipos de eventos detectados y la seguridad típica de detección varían grandemente dependiendo sobre los tipos de tecnologías de IDPS. La mayoría de IDPS requiere al menos algunos ajustes y personalización para mejorar su seguridad de detección, usabilidad, y efectividad,

tal como configurar las acciones preventivas a ser ejecutadas y alertas particulares. Las tecnologías varían ampliamente en sus ajustes y capacidades de personalización. Típicamente, el mayor poder esta en la capacidad de ajustes y personalización de un producto, la mayor seguridad de detección puede ser mejorada de la configuración por defecto. Las organizaciones deberían cuidadosamente considerar las capacidades de ajustes y personalización de las tecnologías de IDPS cuando evalúan un producto. Ejemplo de tales capacidades son:

- **Umbrales.** Un umbral es un valor que coloca el límite entre un comportamiento normal y anormal. Los umbrales usualmente especifican un nivel máximo aceptable, tal como por una conexión fallida intentados en 60 segundos, o por caracteres para la longitud de nombre de archivo. Los umbrales son mas común usados para detección basado en anomalías y análisis de protocolo stateful.
- **Listas negras y blancas.** Una lista negra es una lista de entidades discretas, tal como hosts, número de puertos TCP o UDP, tipos ICMP y código, aplicaciones, nombres de usuarios, URLs, nombre de archivos, o extensiones de archivos, que han sido previamente determinada para ser asociadas con actividad maliciosa. Las listas negras, también son conocidas como listas calientes, son típicamente usadas para permitir a los IDPS reconocer y bloquear actividad tiene un alta seguridad que es malicioso, y también seria usado para asignar una alta prioridad para alertar y alertas comparar entradas sobre las listas negras. Algunos IDPS dinámicamente generan listas negras que son usadas para que temporalmente bloqueen recientes amenazas detectadas (ejemplo actividad desde direcciones IP de un atacante). Una lista blanca es una lista de entidades discretas que son conocidas para ser benigna. Las listas blancas son típicamente usadas sobre una base granular, como una selección de protocolo, para reducir o ignorar falsos positivos involucrando actividad benigna conocida de hosts conocidos. Listas blancas y listas negras son mas comúnmente usados en detecciones basados en firmas y análisis protocolo stateful.
- **Configuración de alertas.** La mayoría de tecnologías de IDPS permiten a los administradores personalizar cada tipo de alerta.

Ejemplo de las acciones que pueden ser ejecutadas sobre un tipo de alerta incluyen los siguientes:

Cambiarlo prendido o apagado.

Configurar una prioridad por defecto o nivel de severidad.

Especificar que información debería ser registrada y que métodos de notificaciones deberían ser usada.

Especificar que capacidades de prevención debería ser usada.

- **Ver y editar código**. Algunas tecnologías de IDPS permiten a los administradores ver algunos o todos de los códigos relacionados a la detección. Esto es usualmente limitado a firmas, pero algunas tecnologías permiten a los administradores ver código adicionales tal como programas usados para ejecutar análisis de protocolo stateful. Observar el código puede ayudar a los analistas a determinar porque una alerta particular fueron generados, ayudando a alertas e identificar falsos positivos.

La habilidad para editar todos códigos relativos a la detección y escribir nuevos códigos (ejemplo, nuevas firmas) es necesario personalizar completamente ciertos tipos de capacidades de detección. Por ejemplo, una alerta particular sería generada por una serie complejo de eventos involucrada en varios códigos de módulos; personalización de IDPS para entender a una característica de una organización específica no seria posible sin editar el código directamente.

Editar el código requiere habilidades de programación y detección de intrusos; también, algunos IDPS usan lenguajes de programación propietaria, el cual necesitaría al programador aprender un nuevo lenguaje.

Errores introducidos en el código durante el proceso de personalización podría causar al IDPS funcionar incorrectamente o fallar en conjunto, por lo que los administradores deberían tratar de personalizar el código tanto como no alteren el código de los sistemas de producción.

Los administradores deberían revisar el ajuste y personalización periódicamente para asegurar que están aún seguros. Por ejemplo listas blancas y negras deberían ser revisadas regularmente y todas las entradas validadas para asegurar que están aun son seguras y necesarias.

Umbrales y configuraciones de alertas necesitarían ser ajustadas periódicamente para compensar cambios en el entorno y en las amenazas. Ediciones de los códigos de detección necesitaría ser replicados cuando el producto es actualizado (ejemplo parchado o actualizado).

Los administradores deberían también asegurarse que cualquier producto colecta líneas base para detección basada en anomalías tienen sus líneas bases reconstruidas periódicamente tanto como sea necesario para soportar una segura detección.

2.2.4 Capacidad de prevención

La mayoría de los IDPS ofrecen múltiples capacidades de prevención; las capacidades específicas varían por tipo de tecnología de IDPS.

Los IDPS usualmente permiten a los administradores especificar la configuración de la capacidad de prevención para cada tipo de alerta.

Esto usualmente incluye habilitar o deshabilitar la prevención, tanto como especificar cualquier tipo de capacidades de prevención debería ser usado.

Algunos censores IDPS tienen un modo de aprendizaje o simulación que suprime toda acción de prevención y su lugar indica cuando una acción preventiva habría sido ejecutada.

Esto permite a los administradores monitorear y afinar la configuración de las capacidades de prevención antes de habilitar las acciones de prevención, cual reduce los riesgos de inadvertidamente bloquear cualquier actividad benigna.

2.3 Administración

La mayoría de los productos ofrecen capacidades similares de administración. A continuación se describe los principales aspectos de administración (implementación, operación, y mantenimiento) y se da recomendaciones para ejecutarlos efectivamente y eficientemente.

2.3.1 Implementación

Una vez un producto IDPS han sido seleccionado, las necesidades administradores necesitan diseñar una arquitectura, ejecutan IDPS componentes de pruebas, y implementan y seguro los componentes IDPS.

a) Diseño de arquitectura: El primer paso en una implementación IDPS es diseñar una arquitectura. Las consideraciones de diseño incluye:

Donde los censores y agentes deben ser colocados

Como asegurar la solución debería ser y que medidas deberían ser usados para alcanzar la seguridad, tal como tener múltiples censores monitoreando la misma actividad en caso una falla del censor, o usar servidores de administración múltiples que un servidor de backup puede ser usado cuando el servidor primario falla.

Donde otros componentes de los IDPS serán colocados (ejemplo servidores de administradores, servidores de base datos, consolas), y cuantos de cada componente serán necesarios para lograr usabilidad requerida, redundancia, y las metas de balanceo de carga.

Con cualquier otro sistema los IDPS necesitan requiere interfaces, incluyendo los siguientes:

- Sistema que provee datos. Tal como la información de seguridad y software de administración de eventos, servidores de registros centralizados, servidores de correos.
- Sistemas sobre el cual inicia las respuestas de prevención (ejemplo firewalls, routers, switches).
- Sistemas que administran los componentes IDPS, tal como software de administración de redes (para una red administrada) o software de manejo de parches (para mantener las consolas de sistema operativo y aplicaciones y la actualización de las aplicaciones).
- Si o no una red de administración será usada; si es si, que diseño tendrá, y si no, como las comunicaciones de los IDPS será protegida sobre las redes estándares.
- Que otros controles de seguridad y tecnologías necesitan ser alterada para albergar implementaciones de IDPS tal como cambiar firewall para permitir parámetros componentes de los IDPS para comunicar.

b) Componentes de pruebas e implementación. Las organizaciones deberían considerar implementar los componentes en ambientes de prueba primero, en vez de un ambiente de producción, para reducir la posibilidad de problemas disruptivos en las redes en producción. Cuando los componentes están siendo implementados en redes productivas, las organizaciones deberían inicialmente activar solo pocos agentes o censores de los IDPS, con la capacidad de prevención deshabilitada. Porque una nueva implementación será seguramente generación de un número grande de falsos positivos hasta que este completamente afinado y personalizado, activar muchos censores y agentes a la vez saturaría los servidores y consolas de administración, haciéndolos difíciles a los administradores ejecutar afinar y personalizar.

Muchos falsos positivos son seguramente por el cruce de censores y agentes, por lo que es de mucha ayuda identificar estos falsos positivos también durante el proceso de prueba o cuando se implementa los primeros censores y agentes, por lo que esos falsos positivos pueden ser identificados antes de una implementación masiva. Una fase de implementación de un censor o agente es también de utilidad en identificar potenciales problemas con la estabilidad.

IDPS basados en appliance son típicamente simples a implementar. Los administradores necesitarían ejecutar actualizaciones de software y firmas para asegurar el software del IDPS este actualizado. Por otro lado, los administradores usualmente solo

necesitan encender y conectar los cables, inicializar el equipo, y ejecutar configuraciones básicas (ejemplo entrar la llave de la licencia, asignar un nombre al censor).

Los IDPS basados en componentes de software usualmente toma tiempo implementarlos que los basados en cajas. Las organizaciones necesitan primero adquirir el hardware apropiado, cual incluiría comprar tarjetas de redes de alta velocidad, y otros que aseguren que el hardware es lo suficiente robusto para los IDPS.

Luego los administradores necesitan instalar el sistema operativo que es compatible con el software de los IDPS, y asegurar los servidores tanto como sea posible. El aseguramiento debería incluir actualizaciones del servicio del sistema operativo, aplicaciones, incluyendo el software de los IDPS. Los administradores también necesitan ejecutar configuraciones básicas del software de IDPS, similar a los que se hace a los componentes de los IDPS basados en cajas.

Después de implementar cualquiera de los componentes basado en cajas o en software, esfuerzos considerables serian necesarios para configurar las capacidades de detección y prevención de los productos, dependiendo del tipo de IDPS. Sin ejecutar este trabajo de configuración, algunos IDPS serian capaces de detectar solo un pequeño número de antiguos, y fáciles ataques identificados.

c) Asegurar los componentes de los IDPS. Asegurar los componentes de los IDPS es muy importante porque son a menudo objetivo de los atacantes. Si un atacante puede comprometer un IDPS, puede ser causante del desuso en detección de los subsiguientes ataques contra otros servidores.

También, los IDPS pueden contener información sensible tal como configuraciones de servidores y conocer las vulnerabilidades que podrían ayudar en planear ataques adicionales. En suma para asegurar componentes de IDPS basados en software y asegurar que los componentes de los IDPS este completamente actualizados, los administradores deberían ejecutar acciones adicionales para asegurar que los componentes de los IDPS por ellos mismos estén seguros apropiadamente. Las recomendaciones especificas de seguridad son las siguientes:

Los Administradores deberían crear cuentas separadas para cada usuario y administrador de los IDPS, y asignar cada cuenta solo con los privilegios necesarios.

Los administradores deberían configurar los firewalls, routers, y otros dispositivos de filtrados de paquetes para limitar el acceso directo a los componentes de los IDPS y solo a los servidores necesarios.

Los administradores deberían asegurar que la comunicación de la administración de los IDPS estén protegidas apropiadamente, tanto física (ejemplo administración de red) o lógica (ejemplo VLAN de administración) separación, o a través encripción de las comunicaciones. Muchos de los productos encriptan sus comunicaciones usando Transport Layer Security (TLS); para los productos que no proveen suficiente protección a través de encripción, las organizaciones debería considera usando virtual private network (VPN) o otros métodos de túneles encriptadas para proteger el tráfico.

2.3.2 Operación y Mantenimiento.

Muchos de los productos IDPS son diseñados para ser operados y mantenidos a través de una interfase gráfica (GUI), también llamada consola. La consola típicamente permite a los administradores configurar y actualizar los censores y administrar los equipos, tanto como monitorear su estado (ejemplo falla de agente, bloqueo de paquetes). Los administradores también puede ejecutar muchas funciones a través de la consola, incluyendo monitoreo y analizar los datos de IDPS y generar reportes. La mayoría de IDPS permite a los administradores configurar cuentas usuarios individuales a cada administrador y usuario, y otorgar cada cuenta solo el privilegio necesario para cada rol personal. La consola a menudo refleja este mostrando diferentes menús y opciones basadas sobre las actuales cuentas autenticadas roles asignados. Algunos productos también proveen control de acceso granular, tal como especificar para cada censor y agentes los usuarios particulares que pueden monitear o analizar datos o generar reportes o que puedan alterar configuraciones a los administradores específicos. Esto permite en una gran implementación ser dividido en unidades lógicas para propósitos operacionales.

Algunos productos IDPS también ofrecen interfaces de comandos en línea (CLI). A diferencia de las consolas gráficas, cuales son típicamente usadas para la administración remota de censores o agentes y servidores de administración, CLI son típicamente usados para administración local de los componentes. Algunas veces un CLI puede ser alcanzado remotamente a través de una conexión encriptada establecida a través de shell segura (SSH) o otros parecidos. Las consolas típicamente son mucha más fácil que usar CLI, y los CLI a menudo ofrecen solo algunas más funcionalidades que las consolas.

a) **Uso típico.** La mayoría de las consolas IDPS ofrece muchas características para asistir a los usuarios en sus tareas diarias. Por ejemplo, la mayoría de las consolas ofrecen capacidades de drill-down, cual significa que cuando un usuario examina una alerta, a mayor detalle, la información está disponible por capas. Esto permite a los usuarios ver

información básica en muchas alertas a la vez, y mostrar información adicional sobre eventos particulares de interés como se necesite. Algunos productos permiten a los usuarios ver información de soporte extensiva, tal como capturas de paquetes (ambos simples y especializados con un analizador de protocolo) y alertas relacionadas (ejemplo otras alertas para la misma fuente o destino), tan igual como documentación sobre las alertas en si mismas. Algunas consolas también ofrecen características de respuestas a incidentes, tal como el cambio de una alerta en un caso de incidente y provee mecanismos de flujos de trabajo que permiten a los usuarios documentar información adicional sobre las alertas y rutas para alertar a usuarios particulares o grupos de usuarios para una posterior revisión.

La mayoría de las consolas también ofrecen varias funciones de reportes. Por ejemplo, administradores o usuarios serían capaces de usar la consola para tener ciertos tipos de reportes ejecutando en horas programadas y enviado por correo o transfiriendo los reportes para los apropiados usuarios y servidores. Muchas consolas también permiten a los usuarios generar reportes como se necesiten (incluyendo reporte para los incidentes específicos) y para personalizar reportes como sean necesarios. Si un producto IDPS almacena sus registros de eventos en un base de datos o en un archivo especifico formato (ejemplo valores separados por comas en archivo texto), las búsquedas en la base de datos o scripts pueden también ser usadas para generar reportes personalizados, particularmente si la consola no ofrece suficientemente personalización de reportes flexibles.

b) **Solución de mantenimiento de operación.** Los administradores deben mantener los IDPS en una operación básica. Esto debería incluir lo siguiente:

- Monitorear los componentes de los IDPS de problemas operacionales y de seguridad.
- Verificar periódicamente que los IDPS están funcionando apropiadamente (ejemplo eventos de procesamiento, alertas apropiadas sobre actividades sospechosas).
- Realizar regulares auditorías de vulnerabilidades.
- Recibir notificaciones de los fabricantes de problemas de seguridad con los componentes de los IDPS (Incluyendo el sistema operativo y las aplicaciones que no son del IDPS) y respondiendo apropiadamente de las notificaciones.
- Recibir notificaciones de los fabricantes de IDPS de actualizaciones, y ejecutar pruebas y despliegue de las actualizaciones.

c) **Adquirir y aplicando actualizaciones.** Hay dos tipos de de actualizaciones para los IDPS: actualizaciones de software y de firmas. Las actualizaciones de software arreglan

fallas en el software del IDPS o añade nuevas funcionalidades, mientras las actualizaciones de firmas añaden nuevas capacidades para la detección o refina las capacidades existentes (ejemplo reduciendo falsos positivos). Para muchos IDPS, la actualización de firmas reemplazan ó alteran código de programas, por lo que son realmente una forma especializada de actualización de software. Para los IDPS, las firmas no son escritas en código, sino una actualización de firmas es un cambio de la configuración de datos para los IDPS.

La actualización de software puede incluir alguno o todos los componentes de los IDPS, incluyendo censores, agentes, servidores de administración, y consolas. La actualización de software para censores y servidores de administración, particularmente para dispositivos basados en cajas, estos a menudo aplicados para reemplazar un existente CD (Compact Disc) del IDPS con uno nuevo y reiniciando el dispositivo. Muchos IDPS, ejecutan los software directamente desde el CD, por lo que software de instalación no es requerido. Otros componentes, tal como agentes, requieren un administrador para instalar software o aplicar parches, también manualmente en cada servidor o automáticamente a través de software de administración de IDPS. Algunos fabricantes hacen software y actualizaciones de firmas disponibles para bajarlos desde sus Web sites o de otros servidores, a menudo, las interfaces de los administradores para IDPS tienen características para bajar e instalar tales actualizaciones.

Los administradores deberían verificar la integridad de las actualizaciones antes de aplicarlas, porque las actualizaciones podrían haber sido inadvertidamente o intencionalmente alteradas o reemplazadas. El método de verificación recomendada depende del formato de la actualización, como sigue:

Bajada de archivos desde la Web o FTP. Los administradores deberían comparar el archivo dado por el fabricante con el cheksums que computa los archivos bajados.

Actualización automática bajada a través de la interfase del usuario del IDPS. Si una actualización es bajado como un simple archivo o serie de archivos, también los checksums dados por el fabricante debería ser comparado con los checksums generados por el administrador

Media removible (Ejemplo CD, DVD). Los fabricantes no proveerían métodos específicos para los clientes para verificar la legitimidad de la media removible aparentemente enviada por los vendedores. Si la verificación de la media es un problema, los administradores deberían contactar con los fabricantes para determinar como la media

puede ser verificada, tal como comparar los checksum. Los administradores deberían también considerar escanear la media de malware, con la consideración que falsos positivos serian disparados por las firmas de IDPS para malware sobre la media.

Los IDPS son típicamente diseñados para aplicar actualizaciones de software y firmas, no tienen efecto sobre el afinamiento y configuración personalizada. La excepción primaria es la personalización del código, que a menudo tiene que ser repetida cuando las actualizaciones de código de los fabricantes son instalados. Para algunos IDPS, los administradores deberían respaldar las configuraciones periódicamente y antes de aplicar una actualización de firmas o software para asegurar que las configuraciones existentes no sean inadvertidamente perdida.

Los administradores deben probar las actualizaciones de software y firmas antes de aplicarlas exceptuando las situaciones de emergencias (ejemplo una nueva firma identificada, una amenaza activa que esta afectando a la organización y no puede de otra forma ser detectada o bloqueada). Es beneficiosa tener al menos un censor o agente (uno para cada tipo de agente) para ser usado estrictamente para pruebas de actualizaciones. Las nuevas capacidades de detección pueden ser a menudo causar un número grande de alertas, por lo que pruebas de actualizaciones de firmas sobre un simple censor o agente, aun pequeña, puede ayudar a identificar firmas que seguramente seria problemático y debería posiblemente ser deshabilitado. En situaciones de no emergencias, las actualizaciones de firmar y software deberían ser probadas y desplegadas usando las mismas practicas que serian usadas para actualizar cualquier cambio en el control principal de seguridad, tal como firewalls y software de antivirus. Cuando una actualización es implementado en producción, los administradores deberían estar listos para deshabilitar firmas particulares o ejecutar otras menores reconfiguraciones como sea necesario.

CAPITULO III

SEGURIDAD PREVENTIVA ACTIVA (IDPS) PARA INTERCONEXION DE REDES EMPRESARIALES

Se describe la solución de seguridad basada en IDPS realizada en una empresa que comercializa productos de belleza y cuidado personal, que cuenta con una oficina principal ubicada en Perú (casa matriz) y quince oficinas en el exterior y con más de 4000 empleados. Debido a los esquemas de trabajo actuales, las necesidades de interconexión han crecido ya que requiere que sus proveedores se conecten a sus sistemas, cuenta conexión con bancos para pagos, cobranza, proveedores logísticos que proveen información del estado de las ordenes y a través de Internet se realiza compras, adicionalmente se tiene empresas conectadas que brindan servicios de soporte técnico, fábrica de software, soporte de 2do nivel, hosting se ERP, soporte de 3er nivel a sistemas especializados, y los empleados que se conectan remotamente por Internet.

Debido a lo anterior, la empresa se ve en la necesidad de mejorar su nivel de seguridad y por requerimientos de auditorías realizadas a nivel financiero. El proyecto tuvo las siguientes etapas:

- Evaluación
- Planeamiento
- Implementación
- Operación

3.1 Evaluación

3.1.1 Situación actual de los sistemas y entornos de redes

a) Se realizó una revisión de los sistemas y redes de la compañía, adicionalmente por recomendación de auditorías externas se llegó a la conclusión que era necesario implementar un sistema de IPS capaz de monitorear los eventos de interés sobre los sistemas y redes que se cuentan, para reducir el riesgo de ataques.

b) Se realizó un inventario de las especificaciones técnicas de los entornos de tecnología actuales.

d) Se actualizó los diagramas de red especificando la arquitectura (lógica y geográfica) de las redes, incluyendo todas las conexiones a otras redes, y el número y ubicaciones de los hosts.

e) Se realizó un inventario de los sistemas operativos, servicios de redes, y ejecución de aplicaciones para cada host que necesitan ser protegidos por los IDPS.

f) Se planteó los atributos de un sistema de seguridad con cual los IDPS necesitarían ser integrados, tal como sistemas de administración de redes.

g) Se realizó un inventario de las especificaciones técnicas de las existentes protecciones de seguridad actuales:

h) Antimalware, software de antivirus y antispyware instalado en los equipos de escritorio.

i) Software de filtro de contenido, incluyendo software de antispam.

j) Firewall de redes, routers, proxies, y otros dispositivos de filtro de paquetes y software.

k) Servicios de encripción de comunicación, incluyendo encripción de enlaces, Virtual Private Networks (VPN), y Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

3.1.2 Metas y objetivos

Después de ganar el entendimiento de los sistemas existentes y los entornos de redes actuales, se estableció metas técnicas, operacionales y negocio y objetivos que a conseguir usando un IDPS, teniendo en cuenta lo siguiente:

- Los tipos de amenazas por los cuales los IDPS deberían proveer protección. Los equipos que serán incluidos en la protección son los que se encuentran expuestos a terceros ya sea por Internet o por la red interna.
- Necesidad de monitorear sistemas y uso de redes para una aceptable uso de violaciones o razones de no seguridad, para evitar saturación en la red por ataques externos o fallas en los sistemas de antivirus, antispam.

3.1.3 Seguridad y otras políticas de IT.

Se realizó una revisión de las políticas existentes de seguridad y otras políticas que se tienen pendientes implementar. Estas políticas sirvieron como premisa para la configuración inicial.

a) **Las metas de las políticas**. Se estableció las siguientes metas en las políticas de seguridad:

- La solución debe ser altamente redundante y alta disponibilidad.
- Que el equipo que administre los equipos de seguridad sea diferente al área de soporte de operación de usuarios.
- No incrementar la complejidad a los sistemas actuales.

b) **El razonable uso de políticas u otras provisiones de administración.** Se realizó una revisión de las políticas de uso de los sistemas y como estas deben quedar reflejadas en la configuración de los IDPS.

c) Los procesos para gestionar las violaciones de las políticas de seguridad. Se estableció el procedimiento y proceso para tratar internamente los eventos de seguridad, así la matriz de escalamiento, tanto interno como del proveedor. El cual establece en caso de un evento tiene que validar con el equipo interno conocido si es tráfico normal o que acción se debe realizar. Si el tráfico es externo por defecto se bloquea, y luego se consulta e investiga su procedencia.

Figura 5: Proceso de gestión de alertas.

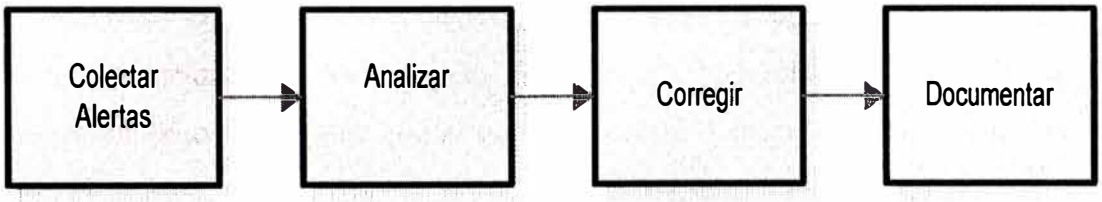
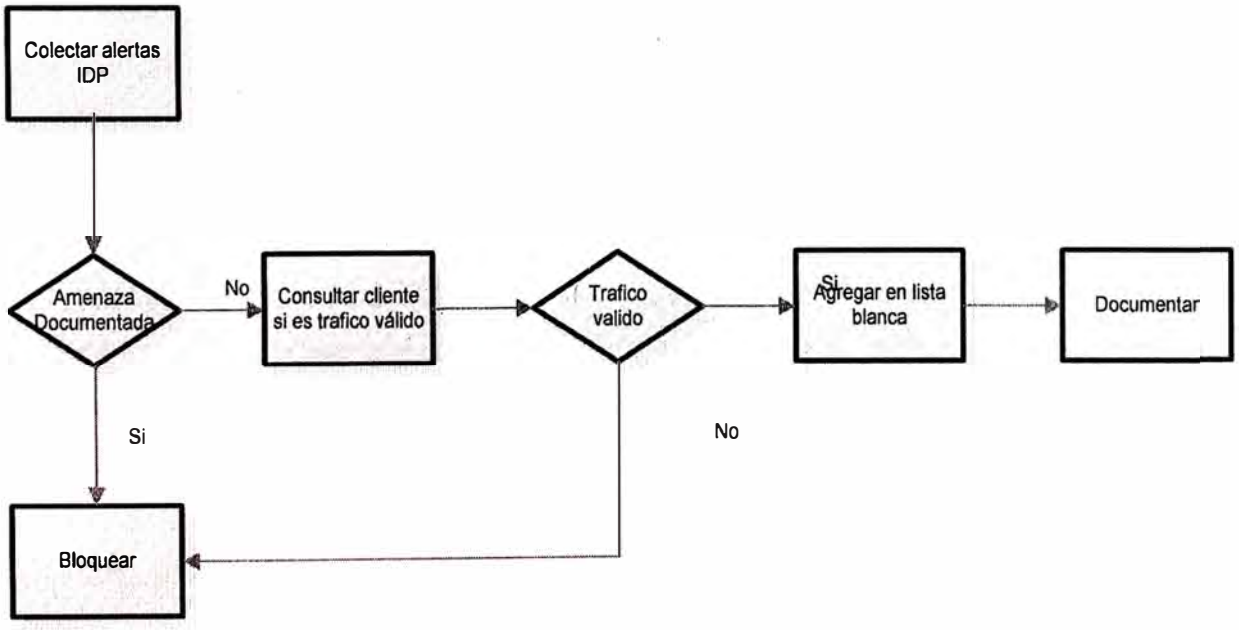


Figura 6: Diagrama de flujo de gestión de alertas



3.1.4 Requerimientos externos.

La organización constantemente esta trabajando para mejorar sus estándares de seguridad y cumplir con:

- **Requerimientos de auditorias para las mejores prácticas de seguridad**. Seguir las recomendaciones de auditorías financieras de los sistemas internos.
- **Requerimientos de sistemas de acreditación**. La empresa tiene acreditado un certificado ISO para el proceso de producción y que anualmente se evalúa.

3.1.5 Restricciones de recursos.

Los IDPS pueden proteger los sistemas de la empresa, pero tiene un precio. Se realizó una evaluación de costo/beneficio de contar con una solución inhouse o en outsourcing (tercerizada) para ello se consideró lo siguiente:

- Los presupuestos para la adquisición y el ciclo de vida para soportar el hardware IDPS, software e infraestructura. El costo total de propiedad de los IDPS también excede el costo de adquisición. Otros costos serian asociados con adquirir sistemas sobre el cual ejecuta los componentes de software, implementando redes adicionales, proveer suficiente almacenamiento a los datos de los IDPS, obteniendo asistencia especializada en la instalación y configurando el sistema, y entrenando al personal.
- La necesidad el personal para monitorear y mantener un IDPS. Algunos IDPS están diseñados bajo la premisa que el personal estará disponible para monitorear y mantenerlos todo el tiempo.

Si los evaluadores no anticipan tener el personal disponible, desearían explorar que estos sistemas se acomoden menos que una atención a tiempo completo o están diseñados para uso desatendido, o podrían considerar la posibilidad de externalizar el monitoreo y posiblemente también el mantenimiento de los IDPS.

3.1.6 Los requerimientos de capacidad de seguridad.

En suma para definir los requerimientos generales, se tuvo en cuenta la performance, administración y el costo del ciclo de vida de los requerimientos.

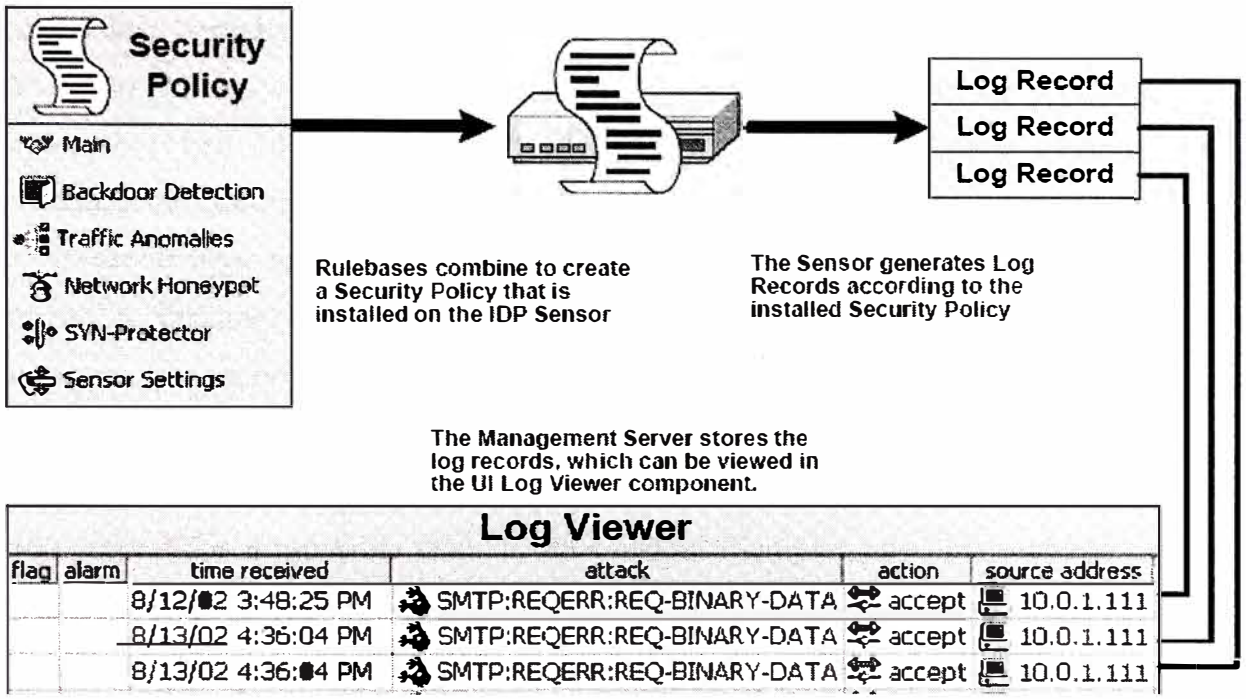
La evaluación de las capacidades de seguridad de cada producto IDPS es obviamente muy importante. Por tal motivo se tuvo en cuenta los siguientes:

a) Capacidad de registrar eventos.

Se tuvo en cuenta las capacidades de registrar los eventos y alertas de la solución de IDPS propuesta por el proveedor. También se tuvo en cuenta la calidad de registro, completa y precisa, que permita un rápido análisis, confirmar la seguridad de las alertas, y

correlacionar registros de eventos con las otras fuentes (ejemplo otros controles de seguridad, registros de sistema de operativo). Los productos IDPS registran por defecto información mínima, tal como la hora, el tipo de evento detectado. El proveedor brinda una consola donde se puede realizar consultas de los eventos en línea a través de una página de Internet y utilizando un certificado digital.

Figura 7: Registro de eventos



b) Capacidad de detección.

- La empresa evaluó la capacidad de detección de cada solución de IDPS propuesta. Para muchas implementaciones, la capacidad de detección son las más importantes funciones. Comparar las capacidades de detección es un trabajo complejo porque cada producto ejecuta típicamente detecciones con una ligera diferencia serie de eventos usando metodologías diferentes.
- ¿Qué tipos de incidentes puede identificar?, tal como Ataques de denegación de servicio, puertas traseras, violaciones de políticas, escaneo de puertos, malware (ejemplo, gusanos, troyanos, código malicioso), y uso de aplicaciones/protocolos no autorizados.
- Cuan compresivo es su detección para cada tipo de incidente que puede identificar (ejemplo cuantos gusanos, cuantos tipos de ataques de denegación de servicio)
- Cuan efectivo es por defecto la configuración fuera de la caja. Cuando un IDPS es por primera vez activada, la configuración por defecto debería ser razonable. Por ejemplo, las firmas y políticas tienden a generara gran número de falsos positivos debería ser

deshabilitadas, y las firmas o políticas que son seguridad e identificar importantes ataques recientes debería ser habilitados. Umbrales de detección (ejemplo x eventos en y minutos) debería ser configurado en valores intentando balanceando los falsos positivos y falsos negativos. También, características que son particularmente intensivas en recursos deberían ser deshabilitadas.

- Cuan efectiva es detectando eventos maliciosos conocidos, tal como ataques, búsquedas, o malware. Las técnicas basadas en firmas típicamente ejecuta mejor que detección en anomalías y técnicas de análisis protocolo stateful en reconocer eventos conocidos. Esto debería incluir la habilidad de los IDPS para estar configurado precisamente contra la debilidad y vulnerabilidad de cual fue objeto.
- Cuan efectiva es detectando previamente eventos maliciosos desconocidos, tal como un ataque o variante de ataques existentes, sin reconfigurar o actualizar los IDPS. La detección por anomalías y técnicas de análisis del protocolo stateful típicamente ejecutan mejor que las técnicas basadas en firmas en reconocer eventos desconocidos.
- Cuan efectiva es detectando previamente eventos maliciosos desconocidos que han sido escondidos a través de técnicas de evasión. Ejemplos tal como técnicas que incluye fragmentación de paquetes IP inusuales, uso de puertos no estándares para aplicaciones, y configuraciones de caracteres alternos y otros caracteres codificados.
- Cuan seguro puede determinar le éxito o falla de un ataque.
- Que mecanismos de respuestas, excluyendo respuestas de prevención. Ejemplo incluye registro de eventos (ambos localmente y para servidores de registros remotos), mostrar alertas en la consola, y enviar avisos de seguimiento Simple Network Management Protocol (SNMP), correos y mensajes de texto. Los criterios también incluyen efectiva priorización de eventos, tal como tomar acciones diferentes cuando cierto tipo de eventos ocurre o cuando un evento involucre un cierto sistema o servicio.
- Cuan efectivamente el producto puede usar datos de otras fuentes, tal como una vulnerabilidad resultado de búsquedas y registros de otros IDPS, para correlación de eventos y mejorar la priorización de las alertas.

3.1.7 Requerimientos de performance.

Para satisfacer los requerimientos de performance se tuvo en cuenta lo siguiente:

- La performance es altamente dependiente sobre la configuración y ajustes de cada producto. Aunque probar puede ser ejecutado usando las configuraciones por defecto de

cada producto son diseñados con la consideración que se necesitará adicionales personalizaciones y ajustes.

- La performance y detección son a menudo opuestos; por lo que solo se definió detectar solo los servicios críticos que están expuestos por la interconexión de redes con terceros, para reducir la complejidad y capacidades de detección, así como la capacidad de procesamiento y memoria.
- Se utilizó IDPS basadas en cajas (appliances) que brindan mejores niveles de performance que los equipos basados en software, ya que éstos no dependen de otros factores, como el afinamiento del sistema operativo y hardware genérico.
- El dimensionamiento de la capacidad se basó en las estadísticas de red recolectadas y sobre los modelos que el proveedor ofrecía. Los fabricantes típicamente clasifican sus productos por capacidad máxima, tal como el volumen de tráfico de redes o número de paquetes por segundos monitoreados para IDPS basados en redes, los números de eventos monitoreados por segundo para los IDPS basado en host, o el flujo monitoreado por segundo o el numero de hosts que pueden ser personalizados para sistemas NBA. Y se consideró:

- La actividad registrada por dos semanas, incluyendo los de mayor carga, cierre de mes y campaña.
- La actividad de todos los proveedores conectados.
- Se realizó una estimación de crecimiento de tráfico para los próximos tres años.
- Características de afinamiento como umbrales.

Se eligió un equipo Juniper IDPS 600 basado en lo anterior y en las recomendaciones del proveedor.

Características y modelos de hardware disponibles

Modelo	Juniper IDPS 50	Juniper IDPS 200	Juniper IDPS 600	Juniper IDPS 1100
Puertos LAN	2x 10/100/1000	8x 10/100/1000	10x 10/100/1000 or 8 FiberSX Gigabit +2x 10/100/1000	10x 10/100/1000 or 8 FiberSX Gigabit +2x 10/100/1000
Puertos de administración	1x 10/100/1000	1x 10/100/1000	1x 10/100/1000	1x 10/100/1000
Puertos de Alta disponibilidad	n/a	1x 10/100/1000	1x 10/100/1000	1x 10/100/1000
RAM	1 GB	1 GB	4 GB	4 GB
Sesiones (máx)	10,000	70,000	220,000	500,000
Throughput (mbps)	50	250	500	1000

3.1.8 Resultado de la evaluación.

Se evaluaron las opciones en el mercado y se realizó una comparación costo/beneficio si se tenía en forma inhouse (interna, propia de la empresa) o como servicio en outsourcing.

Comparativo de una solución inhouse y en outsourcing

	Solución inhouse	Outsourcing
Operación		
Atención 7x24	En horario de oficina	Centro de Operaciones
Expertos de 2do nivel	Mínimo 2 expertos	Incluido en el servicio
Reportes	A mejor esfuerzo, es necesario herramientas	Realizado por herramientas especializadas
Análisis	A mejor esfuerzo	Realizado por expertos
Gestión de incidentes	Reactivo cuando	Proactivo,
Entrenamiento	Inversión necesaria	Incluido en el servicio
Niveles de servicio		
SLA contratado	Mejor esfuerzo	Definido en el contrato

Evaluación de costos de una solución inhouse vs interna.

	Costo primer año		Costo 2do año		Costo 3er año	
	Solución inhouse	Outsourcing	Solución inhouse	Outsourcing	Solución inhouse	Outsourcing
Costos Iniciales						
Hardware	$40.000		$4.000		$4.000	
Adecuación física	$2.000		$0		$0	
Licenciamiento	$10.000		$0		$0	
Instalación	$5.000	$20.000	$0	$0	$0	$0
Personalización	$1.000		$1.000		$1.000	
Entrenamiento	$2.000		$2.000		$2.000	
Total costos iniciales	$60.000	$20.000	$7.000	$0	$7.000	$0
Costos de mantenimiento						
Servicio anual		$102.000		$102.000		$102.000
Personal anual	$60.000		$60.000		$60.000	
Mantenimiento licencias	$10.000		$10.000		$10.000	
Soporte técnico	$2.000		$2.000		$2.000	
Entrenamiento	$2.000		$2.000		$2.000	
Personalización	$2.000		$2.000		$2.000	
Adicionales	$5.000		$5.000		$5.000	
Total costos de mant	$81.000	$102.000	$81.000	$102.000	$81.000	$102.000
Total anual	**$141.000**	**$122.000**	**$88.000**	**$102.000**	**$88.000**	**$102.000**

Finalmente, la recomendación a la empresa fue realizar una implementación a través de un outsourcing, ya que a nivel de servicios era mejor y la diferencia de precios no era significativa en línea a las políticas de selección de soluciones.

3.2 Planeamiento

3.2.1 Cronograma:

Para el proyecto se estableció un cronograma, fases, tareas, fechas y responsables, y que sirvió para llevar un control.

				Fecha	
Fase	**Tarea**	**Detalle**	**Responsable**	**Inicio**	**Fin**
Planeamiento	Levantamiento de información	Revisar como esta la infraestructura actual física/logica	Cliente		
	Planeamiento de la capacidad	Revisar el uso de la red y dimensionar equipos	Proveedor		
	Elaboración diseño	Plantear el diseño final	Proveedor		
Implementación	Provisionamiento	Entrega de equipos			
	Habilitación física	Instalación de tomas red/electricas	Proveedor		
	Configuración inicial de equipos	Montaje físico de equipos y encendido	Proveedor		
	Configuración de monitoreo	Configuración de monitoreo y acceso	Proveedor		
	Activación del servicio	Conectar hardware IDP y activado registrado	Proveedor		
	Inventario de recursos iniciales	Inventario de la linea base completa de la seguridad	Proveedor		
	Freeze de la red	No acciones	Proveedor		
Operación	Reporte inicial de tráfico	Generación de reportes gráficos de 2 semanas despues de instalación IDP	Proveedor		
	Actualización de inventario de recursos	Utilizar el último reporte para actualizar el inventario	Cliente		
	Identificación de Ataques	Identificacion de ataques cual deberia ser parte de las políticas	Proveedor		
	Creación política inicial	Creación de la política de IDP (regla base) linea base (solamente logs)	Proveedor		
	Afinamiento y analisis de logs	Afinamiento fino de la política IDP	Proveedor		
	Provisionamiento de politicas de IDP	Proveer recomendaciones sobre la implementación de políticas IDP	Proveedor		
	Aprobación de políticas IDP	Decisiòn de llevar a cabo o no de las recomendaciones	Cliente		
	Activación de políticas IDP	Activar las políticas IDP (Acción bloquear)	Proveedor		
	Operación completa IDP	Entrega de servicio a expertos Centro de Operación	Proveedor		

3.2.2 Descripción del Diseño.

La mayoría de los aspectos del diseño de los IDPS son específicos a cada tipo de tecnología de IDPS. Adicionalmente se consideró los criterios generales relativos a seguridad, interoperatividad, escalabilidad, y seguridad.

- Seguridad

Las consideraciones para seguridad que se incluyeron fueron las siguientes:

- Hardware redundante que incluye fuentes de poder duplicadas, interfaces de red, dispositivos de almacenamiento.
- Software redundante en caso de falla uno automáticamente el equipo activo realiza
- El proveedor utiliza múltiples consolas remotas ubicadas en 4 centros de monitoreo a nivel mundial.
- Si un equipo falla se tiene un contrato de mantenimiento con el fabricante con SLA para tiempo de reposición y entrega de partes.

- Interoperatividad

Los equipos IDPS seleccionados interoperan con los sistemas del proveedor de seguridad, se integran a su sistema de gestión y permite tomar correcciones sobre los otros equipos Firewalls, antispam, antivirus de red y filtro de contenido.

Adicionalmente los integraron con su sistema de gestión, que permite administrar en forma remota, realizar cambios y copias de seguridad (eventos y configuraciones)

- Escalabilidad

Para selección del modelo no solo se incluyó las necesidades actuales, sino también las necesidades futuras, por lo que se escogió productos que sean lo suficiente escalables. Consideraciones para escalabilidad incluye lo siguiente:

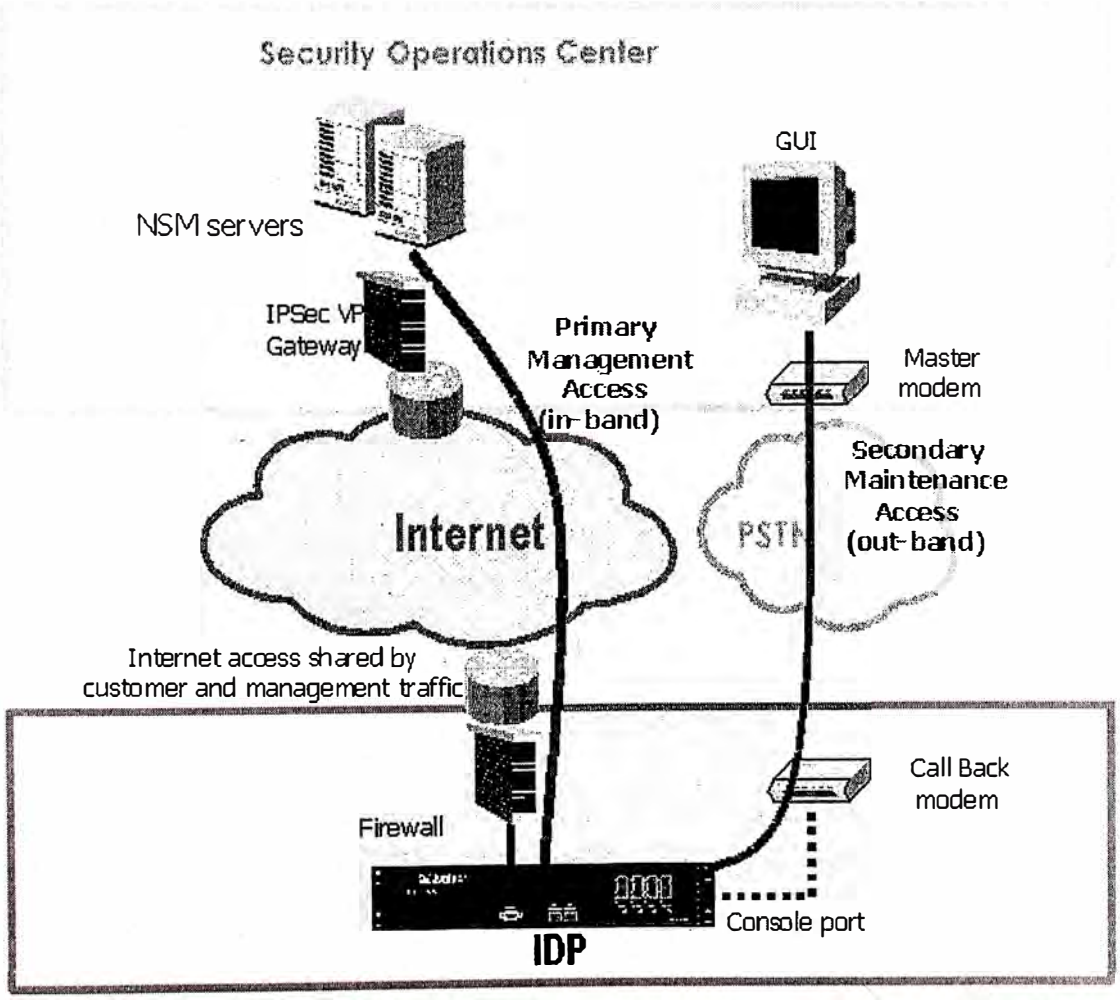
- ¿Cuántas redes en basados en red wireless, o censor NBA puede monitorear simultáneamente?; ¿cuántas interfaces de red un agente basado en host puede monitorear simultáneamente?
- ¿Cómo la capacidad de almacenamiento de los IDPS puede ser expandido y mejorado (ejemplo, archivado de data antigua, uso de dispositivo de almacenamiento separado)?
- ¿Qué nivel de actividad (ejemplo, tráfico de red, sistema de llamadas, entradas de registros) cada uno de los componentes del IDPS puede soportar?
- ¿Cuan bien la solución IDPS se integra la administración y monitoreo de múltiples censores y agentes, servidores de administración, y otros componentes?
- El costo y recursos necesarios para cada opción de escalabilidad.

- Seguridad

Cuando se evalúa los productos IDPS, la empresa consideró los requerimientos de seguridad para la solución en sí. Las consideraciones de seguridad que se incluyó fueron los siguientes:

- La data se almacena (incluyendo registros) y comunicaciones entre todos los componentes IDPS son protegidos, tal como usar canales de datos alternos o encripción y algoritmos de firmas digitales para soportar la confiabilidad de los datos y la integridad cuando sea necesaria.
- La administración, control de acceso, y características de auditoria ejecutadas para el uso de IDPS y administración.
- La resistencia de los IDPS a ataques, tal como denegación de servicio.

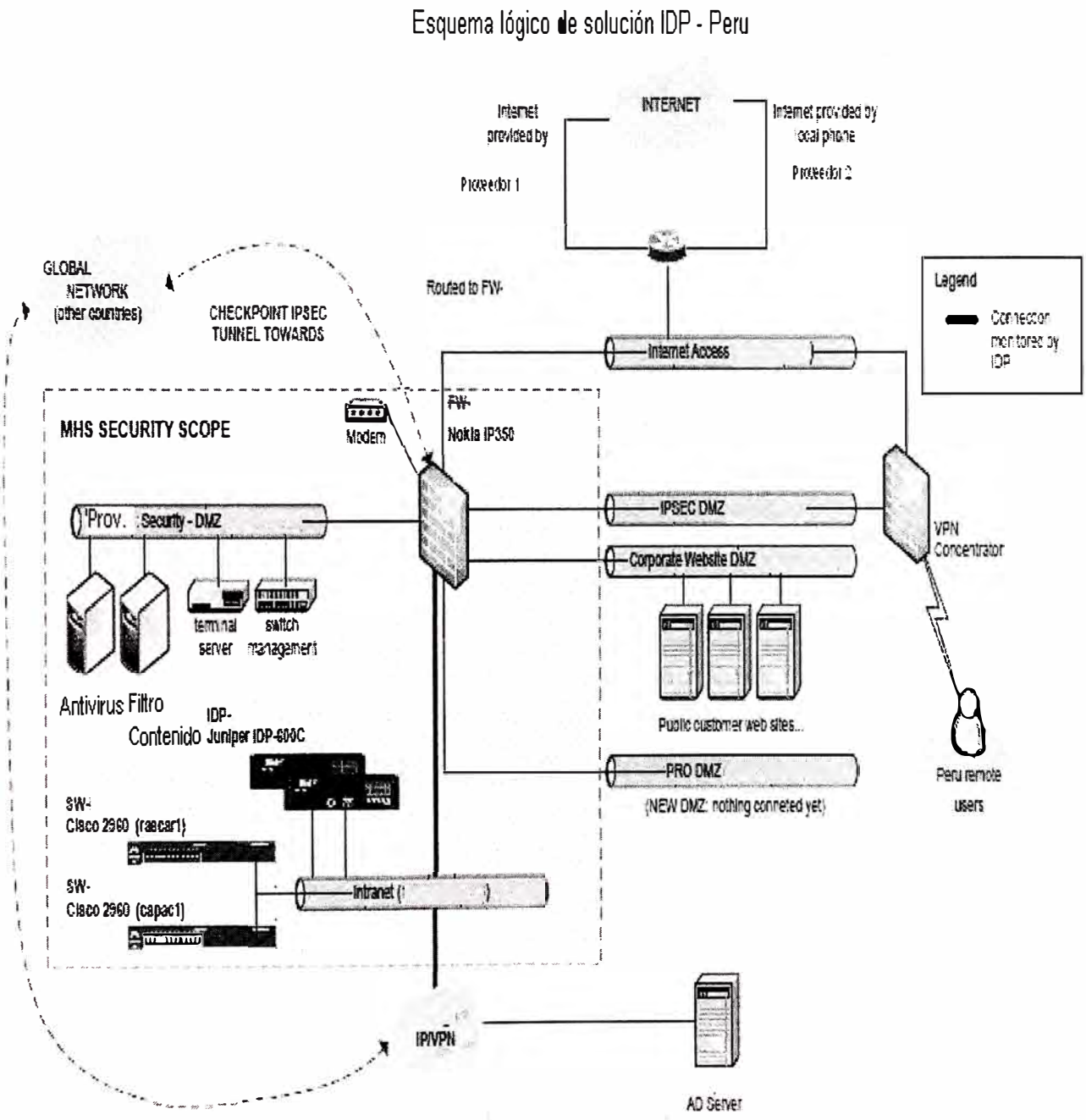
Figura 8: Esquema de conexión de los IDPS con la red del proveedor.



3.3. Implementación

Se realizó la instalación física y lógica de acuerdo a lo planeado.

Figura 9: Esquema implementado



3.3.1 Descripción del diseño lógico de la solución final.

Con el inventario y diagramas de red se estableció el diseño final en la Figura 9. donde tuvo en cuenta los componentes de seguridad que la empresa cuenta:

Firewalls para protección perimetral.

- Antivirus de navegación, para proteger a los equipos cuando navegan por Internet.
- Filtro de contenido, para controlar las páginas a donde se navegue.
- Zonas desmilitarizadas, para segmentar el nivel de seguridad.
- Vlans, para optimizar la red y control de seguridad por rangos de direcciones.

Adicionalmente se estableció políticas de seguridad para los equipos expuestos a Internet, así como a proveedores externos y solos se asigno los accesos necesarios.

Se definieron las redes de los proveedores que deben accesar y también los hosts que se tengan acceso:

- Servidores web
- Servidores ftp
- Servidores de base de datos de desarrollo.
- Servidores de archivos.
- Servidores de chat
- Servidores de correo

Y se estableció una configuración inicial con las políticas de seguridad recomendadas y aceptadas por la empresa, con la que se procedió a dejar el equipo por dos semanas en modo de monitoreo/prueba.

Ejemplo de inventario de servicios

Cust Node	OS Platform	OS version	Patch level	IP address	Function	Product
DEV	WINDOWS	W2000S	4	10.21.1.16	Pruebas	web
DOM	WINDOWS	W2003SE	1	10.21.1.30	DNS DMZ	DNS
ANH	WINDOWS	W2000S	4	10.21.1.50	Interfaces	web

Luego de las dos semanas se procedió a realizar el afinamiento de la configuración basado en el reporte de monitoreo y en el inventario inicial de servicios, clasificando las diferencias como sigue:

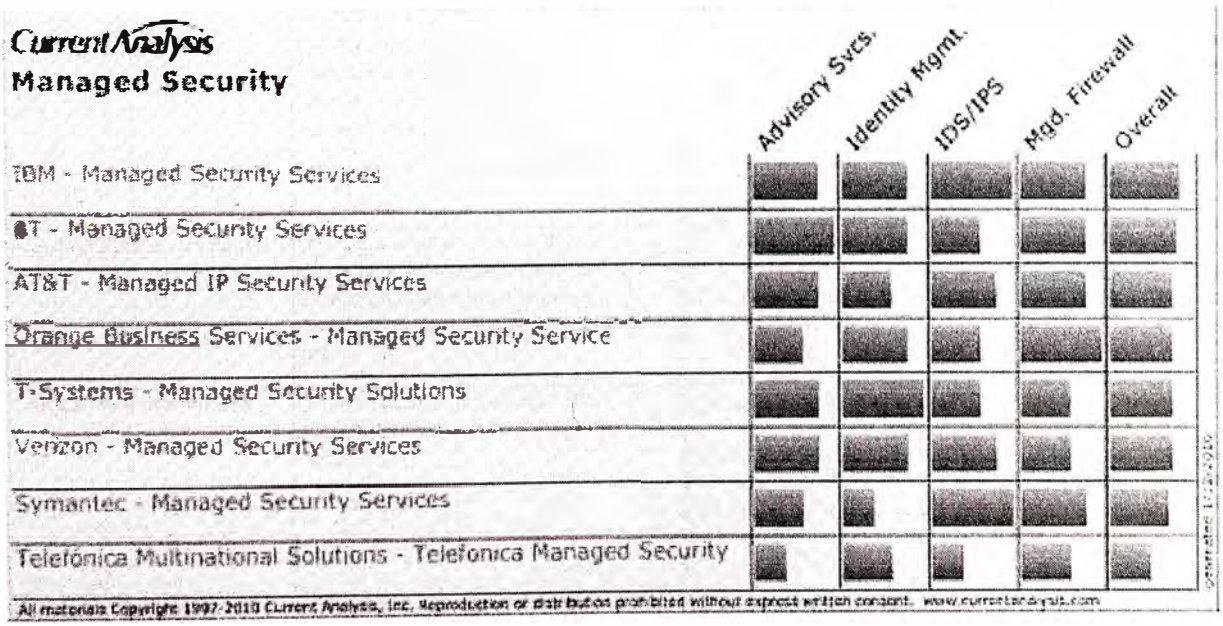
- Tipo 1: parte del inventario inicial y confirmado por IDPS durante el periodo de prueba.
- Tipo 2: parte del inventario inicial que el IDPS no a detectado.
- Tipo 3: recursos adicionales que el IDPS ha registrado durante el período de prueba y en el inventario no ha sido mencionado.
- Tipo 4: consultas adicionales para entender las necesidades de protección.

Luego se realizó la configuración de tal forma que no afectará los servicios, y tampoco generará falsos positivos, ajustando en varias ocasiones la configuración.

3.4 Operación.

Las empresas tienen múltiples paradojas para hacer frente a la actualidad. Uno de los más importantes es proporcionar un entorno más abierto y compartido entorno de TI para una población en crecimiento que pueden ser clientes, personal interno, socios, proveedores. De los recursos clave de su apertura a las personas adecuadas en el momento adecuado, garantizando que sus activos clave estén bien protegidos es un desafío clave. Aprovechando de este concepto de la llamada "empresa extendida" no es sólo un desafío desde un punto de vista técnico, sino también de procesos y el punto de vista de la organización. Cualquiera que sea la solución que uno elija, el controlador final detrás de todo ello sigue siendo la conducción de su negocio, hacer crecer su base de clientes, optimizar sus procesos y hacer crecer sus ingresos. Se debe considerar a este respecto y la aplicación del nivel adecuado de seguridad a la población con derecho a los servicios adecuados es una gran parte de la toma de TI una base de éxito de su negocio.

Por tal motivo se tiene empresas que brindar servicios de seguridad administrados ejemplo:



Para efectos de este trabajo de titulación se ha considerado describir el servicio de prevención activa ofrecen los proveedores en forma general como parte de la operación.

3.4.1 Beneficios claves.

Servicio de Prevención Activa		Propuesta de valor
Caracteristicas	**Beneficios**	
Servicio Completamente administrado	Permite a las empresas centrarse en sus negocios.	Los clientes pueden reducir y controlar el coste total de propiedad (TCO) y aumentar el retorno de la inversión (ROI), permitiendo que los recursos internos de la hora de centrarse en el core-business, generadores de ganancias o de actividades de desarrollo de auxiliares. Como alternativa, estos recursos internos podría ser completamente eliminado para reducir aún más los costos. Los clientes pueden realizar un aumento en los ingresos al permitir que más eficaz y eficiente operatividad de gestión de seguridad. Los clientes se beneficiarán de una disminución de las interrupciones causadas por problemas de seguridad de red, lo que disminuye el riesgo de pérdida de ingresos debido a los sistemas de tiempo de inactividad.
Cobertura Global	Nuestros servicios gestionados de seguridad están disponibles en todo el mundo en más de 140 países, 30 idiomas y con presencia local en más de 165 países. Los clientes pueden confiar en nosotros para manejar algunos elementos o toda su infraestructura de seguridad de red en todas partes.	La externalización de seguridad de la red de infraestructuras a escala mundial, garantiza la coherencia global, que conduce a una mucho más escalable, manejable y fiable infraestructura de seguridad de la red. El cliente no tiene que configurar y utilizar un equipo de seguridad global para gestionar su infraestructura de seguridad de red, lo que consiguen un mejor retorno de la inversión (ROI) de sus inversiones en seguridad, así como un menor costo total de propiedad (TCO) para su solución de seguridad
Flexible management	Gestionado sondas de desplazados internos y otros elementos de seguridad se pueden administrar ya sea a través de la intranet o conexiones seguras a Internet encriptados. Para muchos servicios fuera de banda (OOB) de gestión o de marcado la conectividad es también una opción. Las diversas opciones disponibles permiten al cliente a seleccionar la solución más eficaz de acuerdo con sus necesidades particulares.	Empresas de las que el ancho de banda de red es un producto crítico puede optar por utilizar conexiones de Internet para tener a su infraestructura de monitoreo de seguridad en lugar de tener la gestión del tráfico enviado a través de conexiones privadas. Esto se traduce en un ahorro en el uso de ancho de banda. Las empresas que tienen sitios que no tienen conexiones de Internet pueden optar por tener uno de nuestra conexión instalado para supervisar la gestión de los dispositivos no conectados a Internet. Así, las empresas no tienen que hacer inversiones adicionales en las conexiones de Internet a fin de que sus dispositivos de seguridad gestionados y controlados.
Administración del cambio	Los clientes ya no necesitan mantener los consultores de seguridad, pero escasos e ingenieros altamente cualificados para apoyar su seguridad de red.	Los clientes pueden reducir los costes operativos derivados de la contratación de consultores de seguridad de TI ya que va a proporcionar este servicio de outsourcing.
Cargos fijos mensuales	Cliente puede con exactitud hacer el presupuesto para los servicios de seguridad.	Ventajas para el cliente de un coste fijo para gestionar toda la infraestructura de seguridad de red, reduciendo así el riesgo de aumentos de costos en TI salarios, la formación y la inversión en equipos, que repercutirán en los costos de operación, y por lo tanto el ingreso neto de la sociedad en su conjunto.
Provisionamiento y configuración	La configuración inicial del sistema, gestión de proyectos y los recursos disponibles para el cliente. Contar con un contacto único para las soluciones de seguridad.	Los clientes pueden reducir los costes de explotación de tener personal experto en TI de recuento de la gestión de proyectos, la migración, y de la red mediante el uso de Servicios Profesionales de Orange.

3.4.2 Descripción del servicio.

Los servicios prevención activa es un servicio integral y en capas que se enfoca a los requisitos de seguridad preventiva de los clientes mediante la detección y bloqueo de la actividad maliciosa.

Las principales características de servicios de prevención activas incluyen:

a) Apoyo a través de centros de operaciones de seguridad a nivel mundial,
b) Servicio de Gestión Global y Apoyo 24 x 7.
c) Gestión de dispositivos.
d) Optimización del sistema de prevención de intrusiones monitorización en tiempo real y / o el bloqueo durante la operación.
e) Gestión de incidentes en tiempo real y el asesoramiento de intervención.
f) Objetivos de Nivel de Servicio definidos.
g) Entrega de informes.
h) Regulares actualizaciones de software y firmas,
i) Consultoría de Seguridad.

Opciones de servicio

Prevención activa propone 3 opciones que combinan perfectamente con cada uno de los 3 niveles de servicio disponibles. Las 3 opciones son:

- Opción 1: Prevención modo, también conocido como el modo activo
- Opción 2: Alta Disponibilidad
- Opción 3: Stand Alone.

Opción 1: Modo de Prevención

El modo de prevención permite que el equipo IDPS actuar no sólo como un "sniffer" que simplemente detecta comportamientos maliciosos o sospechosos y envía una alarma.

El modo de Prevención da un paso más en la prestación integral de seguridad de manera efectiva por inhalación, la alerta y bloquear o dejar caer todo el tráfico malicioso o sospechoso que no está claramente autorizada por la política de seguridad en el lugar.

Opción 2: Alta Disponibilidad

Alta disponibilidad (High Availability HA) consiste en la interconexión 2 equipos para hacer que funcionen como un par también se llama un cluster. La alta disponibilidad se utiliza para garantizar la continuidad del servicio, haciendo que al menos uno de los 2 equipos se encuentre en funcionamiento. Aplicada a la prevención activa, la alta

disponiblidad proporciona un modo de fail-over entre 2 unidades de IDPS. La alta disponibilidad puede ser aplicado de 2 formas: activo / activo o activo / pasivo.

Activo / Activo indica que tanto trabajo de investigación de forma simultánea en todo momento. Ambas sondas manejar al final las solicitudes de conexión de usuarios de acuerdo a la disponibilidad de sus recursos respectivos.

Un modo activo / activo implica el balanceo de carga entre ambas unidades. Si una unidad de colapso, el otro se hace cargo de inmediato y automáticamente. Este cambio es totalmente transparente para el usuario final.

Activo / pasivo indica que una unidad actúa como el maestro, el segundo como copia de seguridad o de esclavos. El equipo esclavo no está activo por sí en el sentido de que no se ocupa de las solicitudes de conexión de los diferentes usuarios finales.

Sin embargo, el equipo esclavo continuamente comparte con el estado del maestro y datos de configuración. El cambio de la copia de seguridad del equipo esclavo se realiza de forma automática y es transparente para el usuario final.

La prevención activa ofrece alta disponibilidad en ambos modos. La función de balanceo de carga es manejada directamente por los equipos. Se recomienda aplicar el modo activo / activo para una seguridad óptima.

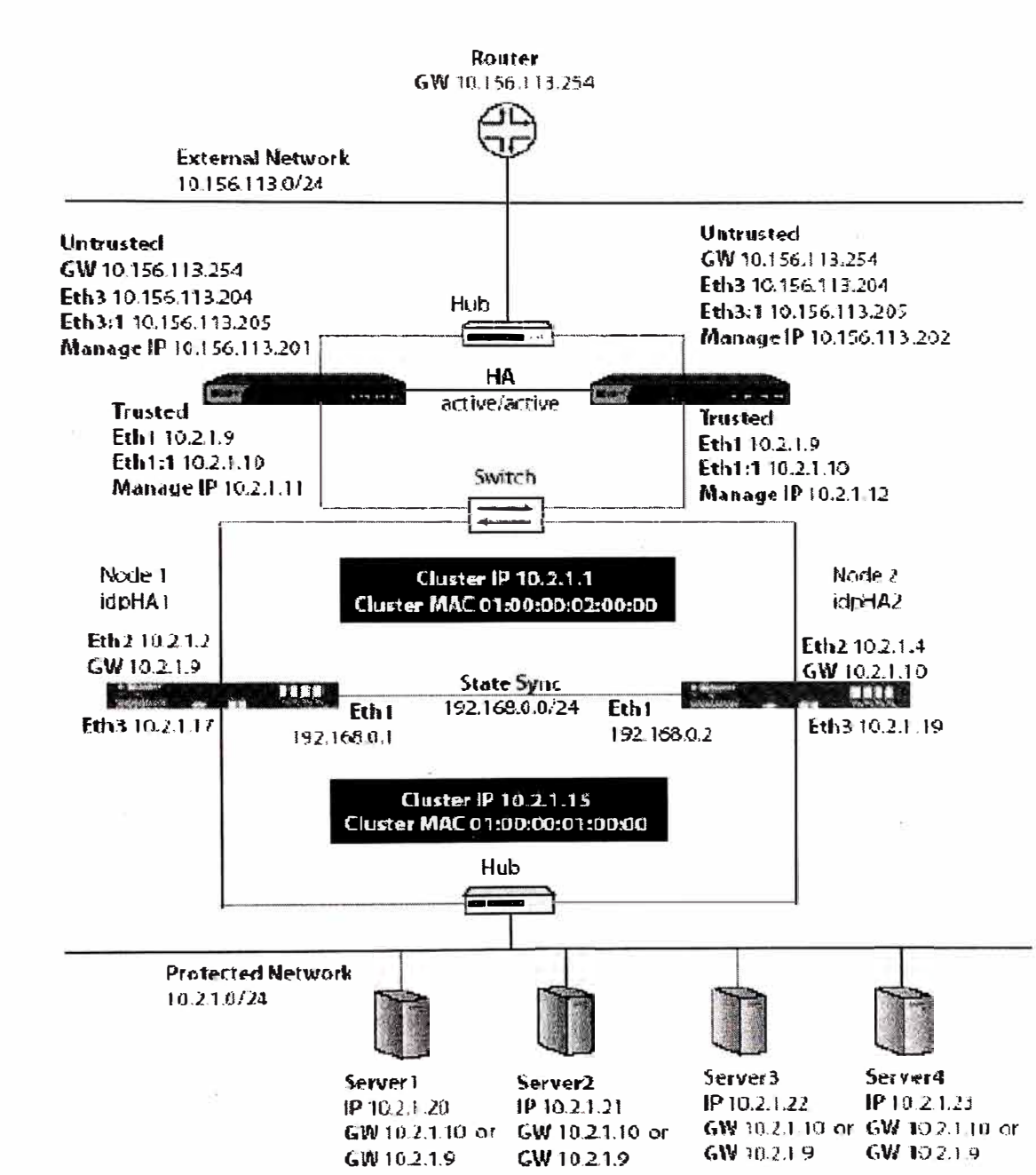
La alta disponibilidad de los equipos en Cluster aparece a la red como una sola unidad IDPS. Si una de las unidades de IDPS en un cluster falla, todas las conexiones establecidas son mantenidos por la otra unidad IDPS de en el clúster en alta disponibilidad. La agrupación continúa procesando el tráfico de red y proporcionar los servicios normales en los IDPS con prácticamente ninguna interrupción desde la perspectiva del usuario final.

Cabe señalar que dependiendo del fabricante y software normalmente esta configuración activo/pasivo tienen costos menores que la opción activo/activo, principalmente por el licenciamiento del software.

Es importante tener en cuenta que a nivel de hardware es necesaria una conexión física entre ambos equipos para mantener la sincronización de la información de configuración, por lo que normalmente implica ocupar una interfase de red la cual debe ser considerada durante el diseño.

Otro consideración es la conexión eléctrica y cableado de red que deben tener las soluciones de alta disponibilidad, que los equipos deben estar conectadas eléctricamente a dos sub-estaciones diferentes así como a equipos de red de la central diferentes para mantener una duplicidad de elementos para ser coherentes con este tipo de soluciones.

Figura 10: Ejemplo de esquema en alta disponibilidad.



Opción 3: Stand-Alone

La prevención activa por defecto es aplicado independiente de otros servicios de seguridad gestionada para una protección complementaria y sólidas para las redes internas de los clientes de las amenazas y comportamientos maliciosos provenientes de las redes públicas como Internet.

Otros servicios que brindan son los siguientes:

- Firewall Gestionado
- Anti-Virus Gestionado

- Filtro de contenido gestionado para acceso a empleados a Internet.
- Servicios administrados de caché de proxy y proxy inverso.

Todas estas características distintas, pero complementarias se pueden unir entre sí para formar barreras de Internet potente y robusta, principalmente para las multinacionales.

Gestión del cambio

Un documento de análisis detallado se completa antes de configurar el dispositivo de prevención activa, que debe firmarse.

Tras la aceptación inicial de servicio, sólo se acepta solicitudes de cambios en la configuración de los contactos de seguridad designadas dentro de la organización. Tras la recepción de una solicitud de cambio, se ponen en contacto con los contactos de seguridad propuestos y verificar el cambio.

Todos los detalles están documentados en la Guía de operaciones del cliente siempre a la aceptación del servicio.

- **Solicitud de cambio ordinario**

  Una solicitud regular se realiza el cambio dentro de 48 horas, (o 2 días laborables) después se notifica al cliente vía e-mail que se ha aceptado tal solicitud de cambio.

  • 90% dentro de 2 días hábiles
  • 100% en un plazo de 5 días hábiles
  • 4 horas de tiempo de respuesta de acuse de recibo de la solicitud de cambio

- **Solicitud de cambio Urgentes**

  Se lleva a cabo una solicitud de cambio urgente en las 6 horas después se notifica al cliente vía e-mail que se ha aceptado tales Urgente Solicitud de cambio.

  • 90% dentro de 6 horas de Negocios
  • 100% dentro de 1 día laborable
  • 1 hora de tiempo de respuesta de acuse de recibo de la solicitud de cambio.

Manejo de incidentes

En general, el cliente clasifica el nivel de gravedad en función del impacto en el negocio cuando se abre un ticket en la mesa de ayuda y con el código que identifica a cada equipo administrado la mesa de ayuda puede encontrar los datos relacionados al equipo, de tal forma de comprobar los datos básicos y sino seguir la matriz de escalamiento.

Definición de niveles de severidad

Nivel de severidad	Descripciones para este servicio
1	Crítico Incidente que causó impacto crítico a la función de negocio (s) o cliente (s). Justifica la atención inmediata y la aplicación de los recursos dedicados esfuerzos continuos para resolver tan pronto como sea posible. Ejemplo: equipo IDPS no responde, problemas críticos con los sistemas.
2	Alta La degradación del incidente causante del servicio resulta en un impacto a la función de negocios de los clientes. Impacto justifica la atención prioritaria y la aplicación de recursos para resolver de manera oportuna. Ejemplo: uso de CPU de alta o crítico problema de la capacidad de memoria que conducen a retrasos o demoras.
3	Medio Incidente causa bajo impacto en las funciones de negocio (s) y cliente (s). Requiere la resolución oportuna para minimizar los impactos futuros. Los recursos deben asignarse de acuerdo con la planificación normal de prioridades de gestión. Ejemplo: desglose repetitivo de la entrada al portal de información
5*	Bajo o planeado Solicitud de información a otras peticiones que no tienen ningún impacto inmediato a la prestación del servicio .. Ejemplo: cualquier solicitud de información

Nota : No hay nivel de severidad 4

Gestión de versiones

El fabricante proporcionará la gestión de versiones del sistema operativo y diversos elementos del servicio.

Actualizaciones del servidor puede incluir la adición de parches para el sistema operativo que son de naturaleza de seguridad y los que afectaría el funcionamiento del Software.

La actualización a un nuevo nivel de sistema operativo también se hará si el vendedor lo considere necesario por razones de seguridad o para el apoyo del Software.

No obstante cualquier disposición en contrario aquí contenida, el vendedor tiene la obligación de proporcionar a todos los nuevos lanzamientos de software de los proveedores

de hardware de servidor y licencias de software, y el vendedor, a su sola discreción, decidirá cuando las actualizaciones tienen lugar.

Gestión de versiones

Tipo de cambio	Descripción	Detalle
1	Hot Fix	Todas las revisiones de software se incluyen en el servicio. Estas acciones se ejecutarán por el fabricante, si procede. El cliente será informado si se verán afectados por la modificación.
2	Patch	Todos los parches de software se incluyen en el servicio. Estas acciones se ejecutarán por el fabricante en su caso, el cliente será informado si se verán afectados por la modificación.
3	Service Pack	Todos los paquetes de software de servicio se incluyen en el servicio. Estas acciones se ejecutarán por el fabricante, si procede. El cliente será informado si se verán afectados por la modificación.
4	Version	Todos los paquetes de software de servicio se incluyen en el servicio. Estas acciones se ejecutarán por el fabricante, si procede. El cliente será informado si se verán afectados por la modificación.
5	Release	Todos los paquetes de software de servicio se incluyen en el servicio. Estas acciones se ejecutarán por el fabricante, si procede. El cliente será informado si se verán afectados por la modificación.

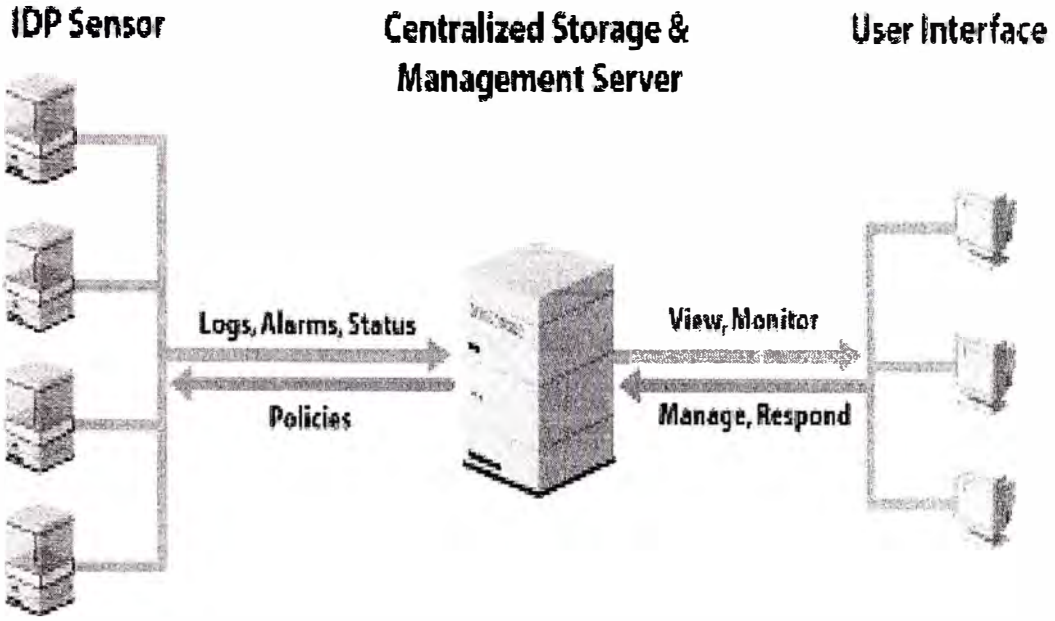
3.4.3 Arquitectura del servicio.

La prevención activa utiliza una arquitectura de tres capas que consiste de equipos IDPS instalados internamente (también conocido como "censores" o "dispositivos internos" o "cajas internas"), los servidores NSM (también conocidos como servidores de gestión), y la interfaz de gestión del usuario.

Los equipos internos ven todo el tráfico de la red y son los puntos de aplicación que aplican las políticas de seguridad.

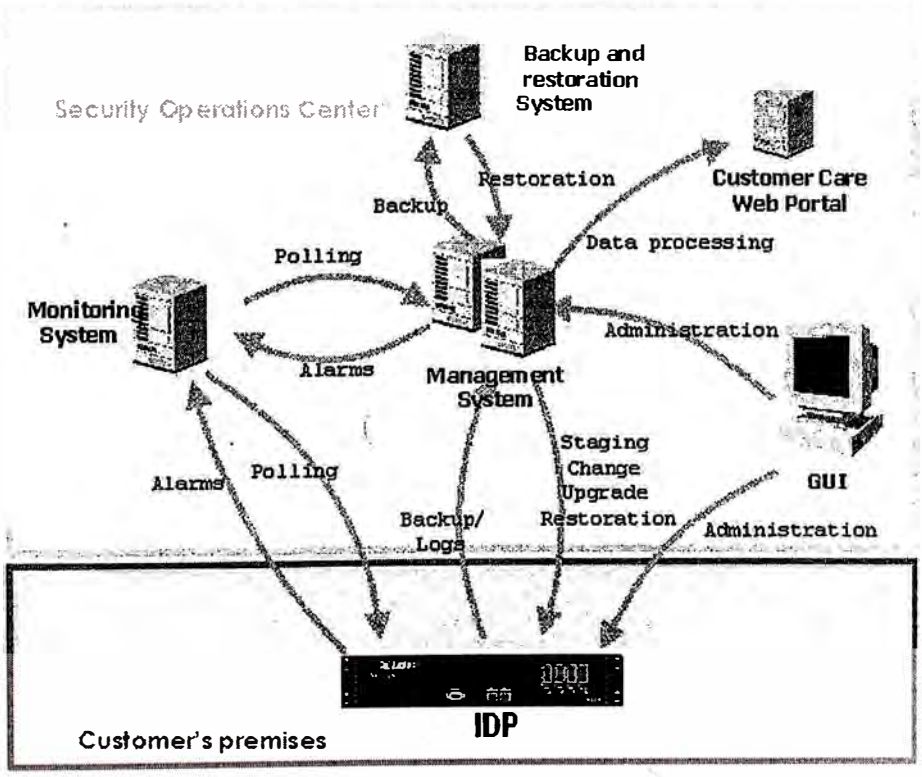
Los servidores NSM almacenan y gestionan todos los objetos de ataque (incluida la firma de ataque y de anomalías de protocolo), la información de registro, bases de reglas y políticas de seguridad. La interfaz de usuario gráfica (GUI) es una aplicación de interfaz para interactuar con el sistema de los equipos internos. Usamos la interfaz gráfica de usuario para acceder remotamente y manipular la información almacenada en el servidor de administración.

Figura 11: Esquema de tres capas



Los servicios de prevención activa considera que solo los equipos se encuentra en el cliente y todos los demás equipos: servidores de gestión, backup, monitoreo, interface se encuentra en el Centro de Operaciones de Seguridad que lo brinda el proveedor ubicado regiones geográficas distintas.

Figura 12: Esquema de Operación



3.4.4 Esquema de soporte.

Se estableció una matriz de responsabilidades en el proveedor y la empresa en caso de falla, se llama a la mesa de ayuda y se abre un ticket con el código del equipo, el cual se tiene registrado en la base de datos.

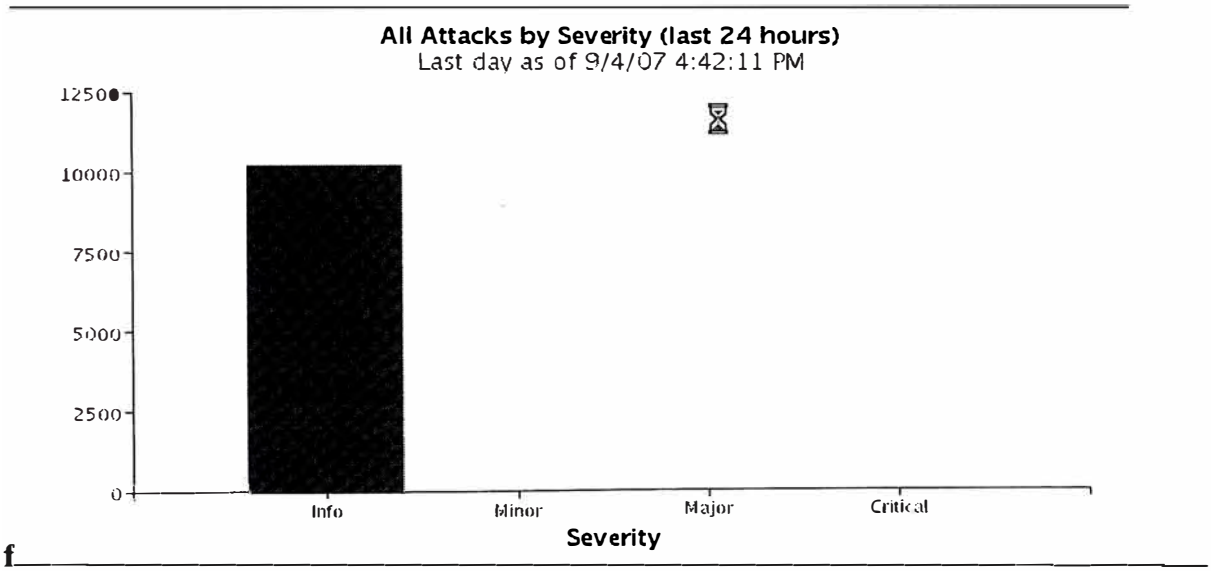
3.4.5 Manejo de incidentes.

Se estableció procedimiento de escalamiento en caso de incidentes de seguridad que son detectados por IDPS y que requieren confirmación de bloqueo o colocarlo en lista blanca.

3.4.6 Entrega de reportes e informes mensuales.

Se estableció entrega de un reporte mensual con estadísticas y estado de los equipos para realizar gestión y un resumen ejecutivo. También incluye el indicador Nivel de Servicio alcanzado por el proveedor.

Figura 13: Ejemplo de reporte



CONCLUSIONES Y RECOMENDACIONES

1. Todo proyecto de seguridad debe responder a necesidades del negocio y se debe encontrar un equilibrio entre el costo y beneficio.

2. Las soluciones de seguridad y en especial los IDPS requieren personal experto para su implementación y operación.

3. El dimensionamiento de los equipos depende las particularidades que cada empresa, teniendo en cuenta el momento de su implementación y planes futuros.

4. El esquema de trabajar en modo outsourcing los servicios tienen un beneficio financiero para las empresas ya que no se adquieren activos, sino servicios que se consideran como gasto.

5. Se recomienda que uno de los objetivos en los proyectos de seguridad sea que las políticas de seguridad no deben generar problemas de rendimiento en la red o accesos, y solo cerrar brechas que pueden ser utilizados para ataques.

6. En los proyectos de seguridad lo más importante es el mantenimiento de las políticas y procesos de seguridad en el tiempo, ya que si no se actualizan los sistemas operativos, firmas, con la evolución de los ataques, lo que una vez se implementó queda obsoleto, por ello se recomienda realizar auditorías periódicas para revisar el estado de la solución.

7. Las soluciones de seguridad generan alertas las 24 horas del día, y requiere un monitoreo constante 7x24x365 días por ello se recomienda contratarlo como servicio ya que a una empresa significaría contar con herramientas y personal experto las 24 horas del día.

8. Las interconexión entre empresas ya sea a través de enlaces privados ó Internet genera el reto de mantener esquemas de seguridad capaces de evitar problemas de virus, ataques, por ello las empresas deben constantemente actualizar sus herramientas para este fin.

ANEXO
ACRONIMOS

ACRONIMOS

AD: Active Directory – Directorio Activo

AP: Access Point.

DMZ: Demilitarized zone – Zona desmilitarizada.

DNS: Domain Name System – Sistema de nombres de dominios

DoS: Denial of Services – Denegación de servicios

FTP: File transfer protocol – Protoloco para tranferencia de archivos

FW: Firewall

GHz: Gigahertz

GUI: Graphical User Interface – Interface gráfica de usuarios

HTTP: Hipertext Transfer Protocol

HTTPS: Hipertext Transfer Protocol sobre SSL

ICMP: Internet Control Message Protocol

IDPS: Intrusion Detection and Prevention System

IDP: Intrusion Detection and Prevention

IDS: Intrusion Detection System

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IM: Instant Messaging

IP: Internet Protocol

IPS: Intrusion Prevention System

LAN: Local Área Network – Redes de área local

MAC: Media access control

NBA: Network Behavior Analysis – Análisis de comportamiento de red.

NFAT: Network Forensic Analysis Tool – Herramienta de análisis forence de red.

NIC: Network Interface Card – Tarjeta interface de red.

NTP: Network Time Protocol – Protocolo de tiempo de red.

OS: Operating System – Sistema operativo

RFC: Request for Comment

RPC: Remote Procedure Call.

SEM: Security Event Management – Administración de eventos de seguridad

SIM: Security Information Management – Administración de información de seguridad

SIP: Session Initiation Protocol – Protocolo de iniciación de sesion.

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SSH: Secure Shell

SSL: Secure Sockets Layer

STA: Station

SW: Switch

TCP: Transmition Control Protocol

TLS: Transport Layer Security

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

BIBLIOGRAFIA

1) An introduction to intrusión Detection System
http://www.securityfocus.com/infocus/1520

2) Comparison of Firewall, Intrusion Prevention and Antivirus Technologies.
http://www.juniper.net/solutions/literature/white_papers/200063.pdf

3) Evaluating Intrusion Prevention Systems
http://www.cioupdate.com/article.php/3563306

4) IDS: Intrusion Detection System http://www.javvin.com/networksecurity/ids.html

5) Intrusion Detection System Frecuently Asked Questions
http://www.sans.org/resources/idfaq

6) Intrusion Detection System Overview
http:///webopedia.com/TERM/intrusion_detection_system.html

7) Intrusion Detection: Implementation and Operational Issues
http://www.stsc.hill.af.mil/crosstalk/2001/01/mchugh.html

8) Intrusion Prevention Systems http://www.ntr.com/resource/downloads/SentivistIPS-WP.pdf

9) Intrusion Prevention System (IPS) http://www.securecomputing.com/pdf/Intru-preven-wp1.aug03-vf.pdf

10) Intrusion Prevention System (IPS) http://hosteddocs.ittoolbox.com/BW013004.pdf

11) Intrusion Prevention System: the Next Step in the Evolution of IDS
http://www.securityfocus.com/infocus/1670

12) Recommendations for Deploying an Intrusion-Detection System
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci781471,00.html

13) SANS Glossary of Terms Used in Security and Intrusion Detection
http://www.sans.org/resources/glossary.php

14) The Evolution of Intrusion Detection Systems
http://www.securityfocus.com/infocus/1514