

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE
Nº 004-2007-AMAG/INF
"FIREWALL"

1. NOMBRE DEL ÁREA:

JEFATURA DE INFORMATICA

2. RESPONSABLE DE LA EVALUACIÓN

LUIS LA MATTA CASTRO

3. CARGO

JEFE DE INFORMATICA

4. FECHA

22 DE OCTUBRE DEL 2007

5. JUSTIFICACIÓN:

La academia de la Magistratura, para el desarrollo de sus actividades de capacitación utiliza diversos medios electrónicos, principalmente el Internet a través de su línea dedicada.

El servicio que se proporciona por estos medios expone a nuestra RED de datos, a situaciones que atentan contra la seguridad y disponibilidad de dichos servicios, perjudicando directa o indirectamente a los usuarios finales de los mismos. Algunos de los ataques más frecuentes a los que nos enfrentamos son:

- Rastreadores o Sniffers.
- Ataques de denegación de servicio, Denial of Service (ataques DoS)
- Ataques a nivel de aplicación para explorar vulnerabilidades conocidas.
- Caballos de Troya, Virus y otros códigos maliciosos.

En la actualidad, la protección perimetral de los servicios de red de la AMAG es efectuada por el producto Firewall/IDS - SafeInternet - Conectiva Linux Multinetwork Firewall 2, instalado sobre una PC en ambiente LINUX, el cual ha permitido implementar un esquema de seguridad que nos protege en algún grado de los ataques a los que estamos expuestos

Desafortunadamente este producto además de ser poco flexible se ha mostrado muy restrictivo en los controles que se deben realizar para un adecuado manejo de la seguridad de la RED, no resolviendo en forma adecuada y oportuna las situaciones de riesgo a los que se estuvo expuesto, por otro lado el escaso soporte en el mercado del mismo hace que no sea recomendable continuar con la renovación de su licencia, la misma que se encuentra próxima a su vencimiento.



Ante esta situación y tomando en cuenta los nuevos retos que la institución debe afrontar, esta Sub Dirección recomienda que se analicen nuevas propuestas que impliquen una Solución de Seguridad Perimetral Integral con garantía de Soporte Técnico al mas alto nivel y tiempos de respuestas adecuados a las exigencias institucionales

6. ALTERNATIVAS

Los Productos de Software a ser analizados por sus características similares de funcionamiento son de las marcas

Check Point
Juniper Firewall

7. ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico se hará sobre productos finales, Para lo cual se debe:

- Comparar el producto con otros productos competitivos.
- Seleccionar un producto entre productos alternativos.
- Valorar tanto el aspecto positivo, como el negativo, cuando está en uso.
- Decidir cuando mejorar o reemplazar un producto.

Se utilizara la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada Por Resolución Ministerial N° 139-2004-PCM. En el cual se establece el modelo de calidad basada en los criterios de evaluación mostrados en el Anexo N°1.

En esta evaluación se considera la Funcionalidad, Fiabilidad, Usabilidad y eficiencia como características del tipo de "Calidad Externa", es decir aplicables a productos finales, como los que consideramos en el numeral 6. Mientras que Capacidad de Mantenimiento y Portabilidad se considera del tipo de "Calidad Interna", aplicable a productos que se desarrollan a medida como son los sistemas propios de las instituciones, esto no significa necesariamente que los productos de software terminados no tengan métricas de calidad interna, igual se debe evaluar su Capacidad en Mantenimiento y su Portabilidad pero con menos rigurosidad.

Finalmente la 'Calidad de Uso', definida por las características que se evaluarán y básicamente está relacionada con el grado de satisfacción y los esfuerzos que los usuarios experimentan al usar los productos.

Para la AMAG es de vital importancia evaluar con mayor rigurosidad las métricas que se definan para la calidad externa, para este caso la puntuación será mayor, para las métricas que se definen para la calidad interna tendrán una menor puntuación. El detalle de la puntuación considerada para evaluar la 'Actualización de Software de Seguridad Firewall' se detalla en el Anexo N° 1, haciendo un total de 100 puntos.



Considerando que los Productos de Seguridad para el caso de Firewall provistas por Check Point, Juniper son las de mayor uso en el mercado, se procederá a su evaluación, para ello se definieron las métricas con sus puntajes respectivos mostradas en el Anexo N° 1.

Como se observa en el cuadro, la eficiencia del producto, productividad, satisfacción, funcionalidad y usabilidad son las principales características que la institución considera necesario evaluar de los productos y por tanto se les ha ponderado con un mayor puntaje.

En el mismo Anexo N° 1, se muestra los resultados de la evaluación de los productos, además se muestra un análisis comparativo técnico de los mismos

8. ANÁLISIS COMPARATIVO COSTO – BENEFICIO

Los costos estimados en el mercado para las alternativas seleccionadas son los siguientes

PRODUCTO	PRECIO TOTAL
01 Equipo Firewall Check Point UTM-1 Model 450, Check Point Floodgate-1 Add-on for VPN-1 UTM Gateway, Check Point SmartDefense Services plus Content Inspection(IPS/IDS+AV+URL) incluye capacitación para 02 personas	US\$ 15,529.96 mas IGV
Collaborative Enterprise Support –Standard 2 años Servicio de Soporte técnico en modalidad 24 x7	US\$ 3754.40 mas IGV
Total Producto	US\$ 19,284.36 mas IGV

PRODUCTO	PRECIO TOTAL
01 Equipo Firewall Juniper Networks Netscreen 208	US\$ 18,500.00 mas IGV
Plan Anual de Mantenimiento a todo costo 01 Core plus Support for Netscreen 208 (incluye capacitación para 02 personas por 04 horas)	US\$ 3,150.00 mas IGV
Total Producto	US\$ 21,650.00 mas IGV

9. CONCLUSIONES

1.-La escasa flexibilidad de la herramienta actual así como lo restrictivo y poco flexible de sus funcionalidades, situación que se agrava por no contarse con un equipo de características adecuadas sobre el cual esta o una solución similar se pueda implementar en forma Segura y Confiable

La permanente falta de oportunidad en la atención de nuestros requerimientos de Soporte Técnico que por ser esta una función de seguridad prioritaria, merece un trato mas ágil y oportuno

Por todo lo anterior se sugiere no renovar la licencia del actual FIREWALL que la Academia de la Magistratura viene utilizando



2.- Siendo de necesidad que nuestra institución por sus funciones cuente con herramientas que garanticen en forma efectiva nuestra Seguridad Perimetral, esta Jefatura recomienda que se opte por una Solución de Seguridad Perimetral Integral con garantía de Soporte Técnico al mas alto nivel y tiempos de respuestas adecuados a las exigencias institucionales, para lo cual sugiere considerar como base de características minimas a ser consideradas las mostradas en el presente análisis, debiendo tomar en cuenta el monto estimado del costo de estas soluciones para que se proyecte la respectiva partida presupuestal



ANEXO 1 HOJA DE EVALUACION

CALIDAD DEL PRODUCTO

TIPO CALIDAD	CARACTERISTICAS	SUB CARACTERISTICAS	PUNTAJE MAXIMO	CRITERIOS DE CALIFICACION	PUNTAJE	Check Point UTM-1	Juniper Firewall
CALIDAD INTERNA Y EXTERNA	FUNCIONALIDAD	Adecuacion	3	SI	3	3	3
				NO	0		
		Exactitud	3	ALTA	3	3	2
				MEDIA	2		
				BAJA	1		
		Interoperatividad	3	SI	3	3	3
				NO	0		
		Seguridad (Vulnerabilidad)	3	ALTA	3	3	3
				MEDIA	2		
				BAJA	1		
		Conformidad de funcionalidad	2	SI	2	2	2
				NO	0		
	FIABILIDAD	Madurez	3	ALTA	3	3	3
				MEDIA	2		
				BAJA	1		
		Tolerancia a fallas	2	SI	2	2	2
				NO	0		
		Recuperabilidad	3	ALTA	3	3	3
				MEDIA	2		
				BAJA	1		
	Conformidad de fiabilidad	2	SI	2	2	2	
			NO	0			
	USABILIDAD	Entendimiento	3	ALTA	3	3	2
				MEDIA	2		
				BAJA	1		
		Aprendizaje	3	ALTA	3	2	2
				MEDIA	2		
				BAJA	1		
		Operatividad	3	ALTA	3	3	2
				MEDIA	2		
				BAJA	1		
		Atraccion (amigable)	3	SI	3	3	3
NO	0						
Conformidad de uso	2	SI	2	2	2		
		NO	0				
EFICIENCIA	Comportamiento de tiempos (Performance)	4	ALTA	4	4	4	
			MEDIA	2			
			BAJA	1			
	Utilización de recursos	4	SI	2	4	4	
NO			4				
Conformidad de eficiencia	4	SI	4	4	4		
		NO	1				
CAPACIDAD DE MANTENIMIENTO	Facilidad de mantenimiento	2	SI	2	2	2	
PORTABILIDAD	Adaptabilidad	2	SI	2	2	2	
			NO	0			
	Facilidad de Instalación	3	ALTA	3	2	2	
			MEDIA	2			
			BAJA	1			
	Coexistencia	3	ALTA	3	2	1	
MEDIA			2				
Reemplazabilidad (upgrade)	1	SI	1	1	1		



				NO	0		
				SI	1		
CALIDAD DE USO	EFICIENCIA	Conformidad de portabilidad	1	NO	0	1	1
				SI	1		
	EFICIENCIA	Alcanzar las metas con exactitud e integridad	12	NO	0	12	12
				ALTA	12		
				MEDIA	6		
	PRODUCTIVIDAD	Alcanzar los objetivos a menores	12	BAJA	1	12	12
				SI	12		
	SEGURIDAD	Riesgo de propiedad	2	NO	6	2	2
				SI	2		
	SATISFACCION	Usuarios satisfechos	12	ALTA	12	12	12
				MEDIA	6		
				BAJA	1		
TOTAL OBTENIDO			100		97	93	

ANÁLISIS TECNICO

CARACTERISTICAS	Checkpoint UTM-1	Juniper NetScreen – 208
Características generales	<ul style="list-style-type: none"> - Tecnología tipo hardware dedicado (appliance). - Soporta servicios NAT (Networks Address Traslacion) y PAT (Port Address Traslacion). - Protección DoS, Ddos. - Asignación de dir. IP Estática, DHCP, DHCP Relay. - IPS integrado. - Soporte para PKI - Soporte para VoIP. 	<ul style="list-style-type: none"> - Tecnología tipo hardware dedicado (appliance). - Soporta servicios NAT (Networks Address Traslacion) y PAT (Port Address Traslacion). - Protección DoS, Ddos. - Asignación de dir. IP Estática, DHCP, DHCP Relay. - IPS integrado. - Soporte para PKI - Soporte para VoIP.
Usuarios soportados	Irrestringido	Irrestringido
Nº de Interfases	4 - 10/100/1000	8 - 10/100
Throughput máx.	400 Mb FW 190 Mb VPN	375 Mb FW 175 Mb 3DES VPN.
Nº sesiones máx.	500,000	128000 concurrentes. 11500 sesiones nuevas por segundo.
Nº políticas máx.	NO DECLARADO	4000.
Nº VLAN soportados	256	32.
Nº zonas de seguridad	4 FISICAS + 256 VIRTUALES(VPN)	8.
Nº routers virtuales	NO DECLARADO	3.
Protocolos de ruteo soportados	OSPF, BGP, EGP, IGRP, RIP.	OSPF, BGP, RIPv1/v2. Soporta hasta 4096 rutas estáticas.
Antivirus integrado	SI	NO



Definiciones de alta disponibilidad	Activo / Pasivo. Activo / Activo. Sincronización para FW y VPN	Activo / Pasivo. Activo / Activo. Activo / Activo full mesh mode. Interfaces redundantes.
Consola administrativa	SO propietario. Control de acceso mediante usuario y contraseña. Registro de eventos SYSLOG. Envío de reportes via email, SMNP. Integración a Directorio Activo MS	SO Base ScreenOS 5.4 (propietario). Control de acceso mediante usuario y contraseña. Registro de eventos SYSLOG. Envío de reportes via email, SMNP. MB personalizable VPN túnel monitor.
Idioma	Inglés	Inglés
Servicio de Mantenimiento	Actualizaciones gratuitas, soporte técnico-operativo durante el tiempo de vigencia del contrato (anual) en modo 24x7. Renovable anualmente a elección del usuario.	Actualizaciones gratuitas, soporte técnico-operativo durante el tiempo de vigencia del contrato (anual) en modo 24x7. Renovable anualmente a elección del usuario.

Certificaciones de Seguridad que la Solucion debe cumplir:

Certificaciones

- Certificación ICSA para el FireWall.
- Certificación de Common Criteria EAL4 o superior para el FireWall.
- Certificación de Common Criteria EAL4 o superior para la VPN.
- Certificación de Common Criteria EAL4 o superior como IDS/IPS
- Certificación ITSEC E3 o superior para el FireWall.
- Certificación FIPS 140 -Level 2 o superior para el FireWall.
- Certificación de ICSA para VPN's basadas en IPSEC.
- Certificación VPNC para la VPN




 Luis Alberto La Plata
 Sub Director
 Oficina de Informática