

**Documento de descripción del producto**

**Panda GateDefender Performa**

1.	Ficha del producto .....	4
1.1.	Nombre .....	4
1.2.	Definiciones .....	4
1.2.1.	25 palabras .....	4
1.2.2.	50 palabras .....	4
1.2.3.	100 palabras .....	4
1.2.4.	150 palabras .....	4
1.3.	Modelos .....	5
1.4.	Módulos comercializados.....	5
1.5.	Slogan.....	5
1.6.	Beneficios .....	5
1.7.	Características destacables .....	6
1.7.1.	Protección Completa .....	6
1.7.2.	Estructura Modular .....	6
1.7.3.	Alto Rendimiento.....	7
1.7.4.	Auto Actualizaciones .....	7
1.7.5.	Conectar y Olvidar.....	7
1.7.6.	Garantía de Recepción de Información.....	7
1.7.7.	Balanceo de Carga.....	8
1.7.8.	Políticas de Seguridad .....	8
1.7.9.	Integración con LDAP/AD.....	8
1.7.10.	Configuración Centralizada.....	9
1.7.11.	Informes Gráficos Detallados.....	9
1.7.12.	Niveles de acceso a la Consola.....	9
1.7.13.	Monitorización Centralizada.....	9
1.7.14.	Garantía de Flujo de Tráfico .....	9
2.	Descripción detallada .....	10
2.1.	Análisis de protocolos de comunicación.....	10
2.2.	Sistema operativo y software de interceptación.....	11
2.3.	Estructura modular .....	11
2.4.	Módulo Anti-malware.....	11
2.4.1.	Protección Antimalware. ....	12
2.4.2.	Protección Content Filter. ....	13
2.5.	Módulo Anti-spam .....	15
2.6.	Módulo de Filtrado Web .....	17

2.6.1.	Protección Filtrado de URLs:.....	17
2.6.2.	Protección Bloqueo de aplicaciones P2P .....	19
2.6.3.	Bloqueo de Mensajería Instantánea (IM) .....	20
2.6.4.	FILTRADO TEMPORAL.....	20
2.7.	Auto actualización .....	20
2.8.	Cuarentenas.....	21
2.8.1.	Cuarentena de malware. ....	22
2.8.2.	Cuarentena de Content Filter. ....	22
2.8.3.	Cuarentena de Spam .....	22
2.9.	Integración con LDAP/AD .....	23
2.10.	Diferentes Perfiles de usuario .....	24
2.11.	Configuración centralizada .....	26
2.12.	Niveles de acceso a consola .....	26
2.13.	Informes gráficos de la actividad del sistema.....	27
2.14.	Alertas y eventos .....	27
2.14.1.	Envío de información a través de SNMP .....	27
2.14.2.	Sistema para almacenar eventos (Syslog) .....	31
2.15.	Monitorización centralizada (CACTI) .....	32
2.16.	Sincronización con servidores horarios (NTP).....	33
2.17.	Modelos de hardware .....	33
2.18.	Sistema de auto-reparación: .....	34
2.19.	Watchdog .....	34
2.20.	Balanceo de carga.....	34
2.21.	Garantía de flujo de tráfico (bypass) .....	35
2.22.	Rendimiento.....	35

## **1. Ficha del producto**

### **1.1. Nombre**

Panda GateDefender Performa

### **1.2. Definiciones**

#### **1.2.1. 25 palabras**

Panda GateDefender Performa es un appliance de seguridad que aporta la máxima protección al principal punto de entrada de la red. Evita que malware, spam y contenidos web no deseados entren en la organización.

#### **1.2.2. 50 palabras**

Panda GateDefender Performa es un appliance de seguridad que aporta la máxima protección al principal punto de entrada de la red. Evita que entren en la organización malware, spam y contenidos web no deseados. Su sencillo manejo "conectar y olvidar" y protección siempre actualizada lo convierten en una potente solución de bajo coste de propiedad.

#### **1.2.3. 100 palabras**

Panda GateDefender Performa es un appliance de seguridad que aporta la máxima protección al principal punto de entrada de la red. Bloquea malware, spam, contenidos web no deseados y otras amenazas procedentes de Internet antes de que entren en la empresa. Su sencillo manejo "conectar y olvidar" y completa protección siempre actualizada lo convierten en una potente solución de bajo coste de propiedad. Proporciona una protección adaptable a las necesidades de cada usuario de la red. Los tres modelos disponibles y el balanceo de carga nativo permiten su adaptación a las necesidades de cualquier empresa, desde PYMEs a grandes empresas o ISPs

#### **1.2.4. 150 palabras**

Panda GateDefender Performa es un appliance de seguridad que aporta la máxima protección al principal punto de entrada de la red. Bloquea malware, spam, contenidos web no deseados y otras amenazas procedentes de Internet antes de que entren en la empresa. Su sencillo manejo "conectar y olvidar" y completa protección siempre actualizada lo convierten en una potente solución de bajo coste de propiedad. Proporciona una protección adaptable a las necesidades de cada usuario de la red. Existen cuatro modelos, GateDefender Performa 9050, GateDefender Performa 9100, GateDefender Performa 9200 y GateDefender Performa 9500.

El balanceo de carga nativo permite su adaptación a las necesidades de cualquier empresa, desde PYMEs a grandes empresas o ISPs. Dispone de un sistema automático de actualización que verifica continuamente la existencia de nuevos ficheros identificadores de virus. Es la protección

más actualizada de la empresa, con un funcionamiento óptimo y mínimo impacto en la velocidad de la red.

### **1.3. Modelos**

Existen cuatro modelos hardware

- Panda GateDefender Performa 9050
- Panda GateDefender Performa 9100
- Panda GateDefender Performa 9200
- Panda GateDefender Performa 9500

### **1.4. Módulos comercializados**

Existen tres módulos que se pueden adquirir juntos o por separado.

- **Anti-malware**
  - Protección Anti-malware
  - Protección Content Filter
- **Anti-spam**
- **Filtrado web**
  - Protección de filtrado de URLs
  - Bloqueo de aplicaciones P2P e IM

### **1.5. Slogan**

Su primera línea de defensa proactiva

### **1.6. Beneficios**

**Refuerza el sistema de Gestión de Riesgos** porque es altamente preventivo para detectar y desinfectar amenazas desconocidas, en el perímetro sin intervención del administrador.

**Incrementa la productividad de los usuarios** gracias a la liberación del spam en sus correos; el uso restringido de aplicaciones Peer to peer y de Mensajería Instantánea; y el control de los contenidos web a los que pueden acceder.

**Contribuye a que la compañía cumpla los estándares reguladores** evitando la pérdida de datos críticos, basándose en el contenido mismo o personalizado según el perfil del cliente.

**Evita la complejidad** debido a su comportamiento en modo bridge transparente que permite una fácil instalación sin necesidad de cambiar nada en la arquitectura de la red.

**Posibilita la Continuidad de Negocio** optimizando el uso del ancho de banda al bloquear todo el tráfico inútil procedente de Internet (alrededor del 70%) antes de que entre en la red.

**Reduce los costes de operación** gracias a las actualizaciones continuas que permiten su funcionamiento desatendido tras la instalación.

## **1.7. Características destacables**

Panda GateDefender Performa es un sistema de protección a nivel de Gateway. Está diseñado para implantarse fácilmente en cualquier red, sin interferir en la productividad y rendimiento de la misma. No afecta al rendimiento de otros sistemas críticos como firewalls y servidores de aplicaciones / web.

Además, la Tecnología Proactiva integrada: el **motor heurístico genético**; la **Inteligencia Colectiva** y la **Cuarentena**, combinados en el perímetro evitan la llegada de cualquier amenaza posible, garantizando la recepción de la información importante.

Las principales características de Panda GateDefender Performa se describen a continuación.

### **1.7.1. Protección Completa**

Ofrece protección completa contra amenazas basadas en contenidos. Incluye protecciones Best of breed (mejor del ramo) contra Malware y contenidos potencialmente peligrosos (Panda); spam (Cloudmark); y contenidos web no deseados (Cobion). Además, permite bloquear el uso de herramientas P2P e IM que pueden suponer pérdida de productividad en la organización y riesgos de infección no controlables a nivel perimetral.

Analiza todos los protocolos (HTTP, SMTP, FTP, IMAP4, POP3 y NNTP) en busca de amenazas, reforzando así el sistema de gestión de riesgos.

Analiza todo el tráfico entrante y saliente contribuyendo al cumplimiento de las normativas de seguridad

Dado que incluye todo lo necesario, no requiere protección extra, reduciendo la complejidad.

Como además, no son necesarios otros dispositivos de protección de contenidos, también se reduce el coste de operación.

### **1.7.2. Estructura Modular**

GateDefender Performa ofrece diferentes protecciones para distintos tipos de amenazas, reforzando el sistema de gestión de riesgos allí donde es necesario.

La complejidad se ve reducida dado que sólo es necesario configurar la protección que se necesita.

Igualmente, el coste se optimiza, dado que la organización solo paga por la protección necesaria.

#### **1.7.3. Alto Rendimiento**

Las unidades hardware de Panda GateDefender Performa están concebidas para funcionar de forma transparente en el perímetro de la red, analizando grandes cantidades de tráfico en tiempo real.

Cada unidad hardware ofrece un rendimiento diferente, proporcionando una capacidad de análisis adaptable para el tráfico de cada organización, lo que optimiza el sistema de gestión de riesgos.

El alto rendimiento evita retrasos en la recepción de tráfico, mejorando la productividad del usuario y garantizando el cumplimiento de las normativas estándar de seguridad y la continuidad del negocio.

Como la administración del tráfico es transparente y automática, además se elimina cualquier complejidad.

#### **1.7.4. Auto Actualizaciones**

Las actualizaciones se realizan automáticamente cada 90 minutos en el caso del malware y cada minuto en el caso del spam. Esto hace que la protección siempre esté actualizada contra las últimas amenazas, mejorando constantemente el sistema de gestión de riesgos; contribuyendo al cumplimiento de las normativas de seguridad; y garantizando la continuidad del negocio.

La administración continua es innecesaria, eliminando la complejidad y reduciendo los costes de operación.

#### **1.7.5. Conectar y Olvidar**

Funciona como un Bridge Transparente, por lo que la instalación no requiere cambios o redirecciones en la configuración actual de la red, eliminando así cualquier complejidad. La configuración se puede hacer fuera de línea y una vez conectado, comienza a funcionar al instante, lo que reduce los costes de operación.

#### **1.7.6. Garantía de Recepción de Información**

Cuando un correo entrante contiene un malware desconocido, un proceso automático es capaz de enviar el malware a PandaLabs, para que allí sea analizado y desinfectado. Una vez recuperado el fichero

adjunto, el correo se envía restaurado a su destinatario sin intervención del administrador.

Esta eliminación automática de amenazas desconocidas refuerza el sistema de gestión de riesgos y evita la pérdida de información crítica, mejorando así la productividad de los usuarios.

Esta opción protege la organización contra amenazas conocidas y desconocidas, ayudando al cumplimiento de las normativas de seguridad y, como no es necesaria la intervención del administrador, se reducen drásticamente los costes de operación.

#### **1.7.7. Balanceo de Carga**

Si el tráfico utilizado por la organización crece, el rendimiento del sistema de seguridad puede crecer, gracias a su Balanceo de Carga nativo y automático, que asegura la alta disponibilidad del servicio en caso de fallo inesperado, optimiza la inversión en equipos de la organización y mejora el sistema de gestión de riesgos.

El balanceo de carga evita retrasos en la recepción de tráfico, mejorando la productividad de los usuarios y garantiza la continuidad del negocio.

Al ser nativo y automático, elimina la complejidad de configuración y reduce costes de operación.

#### **1.7.8. Políticas de Seguridad**

Se pueden definir diferentes perfiles de usuarios y grupos para establecer Políticas de Seguridad diferentes para cada miembro de la red, reforzando así el sistema de gestión de riesgos. Cualquier contenido entrante o saliente se analiza de acuerdo al tipo de contenido y el perfil particular de cada remitente o destinatario.

Como cada usuario tiene diferentes restricciones, se optimiza la productividad de los usuarios.

También se pueden crear normativas diferentes para distintos grupos de riesgo y así cumplir las distintas normativas de seguridad.

Al haber usuarios sin restricciones innecesarias se garantiza la continuidad del negocio.

#### **1.7.9. Integración con LDAP/AD**

La integración con sistemas de directorio existentes en la red permite la identificación del responsable de cada una de las acciones que se producen en la red, mejorando el sistema de gestión de riesgos.

Además, el control de todos los usuarios internos mejora el cumplimiento de las distintas normativas de seguridad.

### **1.7.10. Configuración Centralizada**

Se pueden configurar todas las unidades desplegadas a lo largo de toda la red desde una única consola

La gestión centralizada de diferentes puntos de acceso mejora el sistema de gestión de riesgos.

Además, al estar todos los dispositivos administrados desde un solo punto y por un único administrador, se reducen la complejidad y el coste de operación.

### **1.7.11. Informes Gráficos Detallados**

Los informes de actividad de la protección en tiempo real proporcionan un refuerzo importante del sistema de gestión de riesgos.

Los administradores y operadores conocen toda la información importante a primera vista, reduciéndose así la complejidad y el coste de operación.

### **1.7.12. Niveles de acceso a la Consola**

Distintos niveles de acceso a la consola refuerzan la seguridad del sistema de gestión de riesgos, pues las configuraciones de seguridad están protegidas y se garantiza la continuidad del negocio.

El acceso a diferentes necesidades de diferentes usuarios, elimina la complejidad para los menos expertos.

### **1.7.13. Monitorización Centralizada**

Se pueden monitorizar todas las unidades desplegadas de forma centralizada a través de herramientas de gestión que utilicen SNMP o recepción de eventos de gestión.

Cualquier evento de seguridad ocurrido en cualquiera de las unidades desplegadas, se recibe en un solo punto, lo que reduce la complejidad y los costes de operación.

Además, proporciona una mayor eficiencia en la resolución de errores para garantizar la continuidad del negocio.

### **1.7.14. Garantía de Flujo de Tráfico**

Los modelos hardware para grandes organizaciones incluyen la opción de bypass para nunca detener el flujo de tráfico a pesar de posibles fallos del sistema, lo que confiere una garantía de continuidad del negocio.

## 2. Descripción detallada

Panda GateDefender Performa es un dispositivo que, se sitúa preferentemente en el perímetro de la red corporativa, con el fin de hacer frente a las amenazas basadas en contenidos procedentes de Internet. Desde este punto intercepta y analiza todo el tráfico entrante y saliente de la organización. De este modo, puede ofrecer una protección completa contra amenazas basadas en contenidos, incluyendo distintas protecciones:

- **Anti-malware**
- **Filtrado de contenidos**
- **Anti-spam**
- **Filtrado web**
- **Bloqueo de aplicaciones P2P e IM**

### 2.1. Análisis de protocolos de comunicación

Panda GateDefender Performa intercepta y analiza el tráfico de los protocolos HTTP, FTP, SMTP, POP3, IMAP4 y NNTP. El administrador podrá activar o desactivar el análisis de cada protocolo.

Estado de las protecciones						
	HTTP	FTP	SMTP	POP3	IMAP4	NNTP
Protección anti-malware						
Antivirus	✓	✓	✓	✓	✓	✓
anti-jokes	✓	✓	✓	✓	✓	✓
anti-dialers	✓	✓	✓	✓	✓	✓
anti-spyware	✓	✓	✓	✓	✓	✓
anti-phishing	—	—	✓	✓	✓	—
heurística	✓	✓	✓	✓	✓	✓
otros riesgos	✓	✓	✓	✓	✓	✓
Protección antispam	—	—	✓	✓	✓	—
Protección Content Filter	✓	✓	✓	✓	✓	✓
Filtrado web	✓	—	—	—	—	—

Para interceptar y filtrar el tráfico para cada uno de los protocolos el sistema usa por defecto los siguientes puertos estándar:

- E-mail (SMTP): 25
- Transferencia de ficheros (FTP): 21
- Acceso a Web (HTTP): 80
- Descarga de correo (POP3): 110
- Descarga de correo (IMAP): 143
- Acceso a News (NNTP): 119

Desde la consola de administración, el usuario puede introducir puertos adicionales para cada protocolo. Así se usan tanto los puertos estándar como los puertos adicionales introducidos por el usuario.

## **2.2. Sistema operativo y software de interceptación**

El software de Panda GateDefender Performa está basado en el sistema operativo Linux Debian. Este sistema operativo está blindado – protegido contra modificaciones – y optimizado para ofrecer la máxima seguridad y alto rendimiento. Además, se ha simplificado para que cuente únicamente con los servicios y procesos necesarios para funcionar correctamente. Esto redundará en un mejor rendimiento del sistema.

Panda GateDefender Performa actúa como un puente o “bridge” transparente entre Internet y la red corporativa. Es decir, el tráfico pasa a través del appliance de forma transparente. El appliance intercepta las sesiones de los protocolos que se hayan configurado para analizar.



## **2.3. Estructura modular**

La estructura de protección de Panda GateDefender Performa se basa en tres módulos de seguridad. Estos módulos pueden adquirirse juntos o por separado y son:

- **Módulo Anti-malware:** Incluye la protección Antimalware y la protección Content Filter.
- **Módulo Anti-spam.** Bloquea el correo basura o no solicitado.
- **Módulo Filtrado web.** Incluye el Filtrado de URLs y el Bloqueo de aplicaciones IM y P2P.

Cada módulo se contrata por un periodo (1, 2 ó 3 años) válido para cada unidad hardware específica. Cuando los módulos están activos (han sido contratados), el usuario puede activar o desactivar las distintas protecciones de cada módulo según sus necesidades.

## **2.4. Módulo Anti-malware**

El módulo Anti-malware de Panda GateDefender Performa incluye dos tipos de protección:

- Protección Antimalware
- Protección Content Filter

### **2.4.1. Protección Antimalware.**

Detecta y bloquea el malware de diferentes tipos que intenta atravesar GateDefender Performa tanto hacia el interior de la red como hacia el exterior:

- **Virus.-** El administrador define qué acciones efectuar sobre los virus detectados, tanto en navegación como en tráfico de correo y news. Puede elegir entre desinfectar el archivo o eliminar el virus.

Si el virus llega adjunto a un mensaje de correo SMTP, se podrá seleccionar entre eliminar el adjunto o eliminar todo el mensaje

Los virus enviados masivamente por correo, generalmente por gusanos o troyanos, conocidos como fake-from se eliminan automáticamente. Igualmente se elimina el correo en el que van adjuntos.

- **Spyware.-** El software espía son programas que roban información relevante de la empresa como códigos de acceso, datos contables, etc. Después, envían esta información a manos ajenas a la compañía. Activando la detección de spyware se protege la red contra la entrada de software espía a través de Internet.
- **Dialers.-** Los Dialers son programas de marcación telefónica automática. Cambian la configuración de acceso telefónico a redes de los ordenadores con conexión vía módem. Esto provoca que estos ordenadores se conecten a números telefónicos de pago. Activando la detección de Dialers se protege la red contra la entrada de Dialers a través de Internet.
- **Phishing.-** Es una táctica para obtener información personal o privada a través de la suplantación de identidades. Por ejemplo, los usuarios reciben un e-mail con la imagen corporativa de su banco. En el correo se solicita que accedan a una página web y rellenen sus datos bancarios. Al acceder a la web, la imagen del banco es exactamente igual. Por este motivo, el usuario no sospecha que es víctima de un fraude.

Activando el análisis anti-phising, se eliminan los mensajes de correo que intentan utilizar este tipo de fraude.

- **Jokes.-** Los Jokes o bromas no son virus, sino programas inofensivos que simulan acciones de virus en el ordenador. Su objetivo no es atacar, sino gastar una broma a los usuarios, haciéndoles creer que están infectados. Aunque su actividad es molesta, no producen realmente efectos dañinos, salvo la pérdida de tiempo de los usuarios.

La protección anti-jokes impide que este tipo de amenaza pueda llegar a los usuarios de la red corporativa.

- **Análisis heurístico.-** Existen programas maliciosos que no están catalogados como malware en el momento en que llegan a GateDefender Performa. El análisis heurístico compara el código de los ficheros con patrones de malwares conocidos para catalogarlos como potencialmente peligrosos.
- **Otros riesgos.-** Hay software que no es malware propiamente dicho. Sin embargo, su uso podría suponer un riesgo para la red de la compañía. En concreto, Panda GateDefender Performa es capaz de detectar:
  - **Hacking tools.** Son todas aquellas herramientas que se puedan utilizar para robar información, accesos no permitidos, etc.
  - **Security risks.** Son aplicaciones que suponen una amenaza clara para la seguridad, y que no se pueden catalogar como virus. Por ejemplo, un programa dedicado a la creación de virus o troyanos.
- **Sitios de confianza.-** La definición de sitios de confianza, excluye la información procedente de dichos sitios del análisis, optimizando así el rendimiento.

#### **2.4.2. Protección Content Filter.**

Analiza los contenidos de los documentos que llegan a la red, a través diferentes tipos de tráfico:

- Tráfico de correo y news (SMTP, POP3, IMAP4 y NNTP),
- Tráfico de descargas y navegación (FTP y http)

El administrador puede configurar el análisis de contenidos en mensajes y en mensajes anidados dentro de otros. Además, se puede configurar un buzón común al que redirigir los mensajes bloqueados por Content Filter. Existe también una lista blanca de sitios de confianza. Los mensajes procedentes de estos sitios no serán analizados por Content Filter. Igualmente, hay una lista blanca de archivos que no serán filtrados. Todas las listas de configuración de Panda GateDefender Performa se pueden exportar e importar.

Al filtrar correo se pueden configurar alertas o notificaciones para enviar al remitente y/o al destinatario del correo filtrado. Del mismo modo, se puede notificar al administrador sobre los contenidos filtrados en navegación o en transferencia de archivos.

El Content Filter permite filtrar distintos tipos de contenidos según se trate de archivos o correos

#### **Filtrado de archivos**

- **Archivos comprimidos anidados:** Se define el nivel máximo de anidamiento
- **Archivos comprimidos de gran tamaño:** Se define el tamaño máximo de fichero
- **Archivos comprimidos con gran nº de ficheros:** Definible por el administrador
- **Archivos tipo MIME peligrosos:** Definidos en una lista importable y exportable
- **Archivos cuyo tipo MIME difiere de su extensión**
- **Archivos ActiveX y Applets:** Listas blanca y negra de remitentes y dominios con controles ActiveX y Applets, a filtrar.
- **Archivos con macros o información incrustada:** Documentos Office, flash ...
- **Archivos con Passwords:** Archivos zip, pdf y Microsoft Office
- **Archivos con extensiones trucadas:** CLSID, con espacios, caracteres ilegales ...
- **Archivos cifrados en HTTP:** Cifrados mediante PGP
- **Scripts en HTML:** Embebidos o referenciados en el código
- **Referencias externas en cuerpo y adjuntos HTML:** Ficheros referenciados

### **Filtrado de mensajes de correo**

- **Por contenido textual:** Permite definir reglas de filtrado de los mensajes y sus adjuntos, según su contenido textual para los protocolos SMTP, POP3, IMAP y NNTP y filtrar por:
  - Asunto
  - Nombre de los archivos adjuntos
  - Cuerpo (tanto texto como html)
  - Contenido de los archivos adjuntos
- **Por nº de destinatarios:** Se puede definir el número máximo de destinatarios de correo entrante y saliente, por separado.
- **Mensajes anidados:** Se filtran los mensajes anidados, así como los adjuntos de los mensajes principales y los adjuntos de los mensajes anidados.
- **Mensajes cifrados:** Activando esta opción se filtrarán los archivos recibidos que hayan sido cifrados mediante PGP.
- **Mensajes malformados:** Se filtran los mensajes con contenido no analizable.
- **Mensajes fragmentados:** Permite filtrar los mensajes que lleguen fragmentados, que son un riesgo de seguridad al no poder ser analizados por completo

Las acciones a llevar a cabo sobre los elementos filtrados por Content Filter dependen del tipo de contenido filtrado:

**Acciones Referidas al propio mensaje**

- Borrar el mensaje. El mensaje se elimina por completo en SMTP y se sustituye la cabecera en POP3 e IMAP4.
- Redirigir el mensaje. Se reenviará el mensaje a un buzón definido por el usuario.
- Desviar a cuarentena. Se guarda temporalmente en la cuarentena Content Filter.
- Solo informar. No se ejecutan acciones sobre el contenido o elemento filtrado.

**Acciones Referidas a archivos adjuntos al mensaje**

- Borrar el adjunto. Se eliminará del mensaje el archivo adjunto.
- Borrar el mensaje. El mensaje se elimina por completo en SMTP y se sustituye la cabecera en POP3 e IMAP4.
- Redirigir el mensaje. Se reenvía el mensaje a un buzón definido por el usuario.
- Desviar a cuarentena. Se guarda temporalmente en la cuarentena Content Filter.
- Solo informar. Sólo se registra el evento correspondiente si así está configurado.

**Acciones Referidas a transferencia de archivos por HTTP y FTP**

- Bloquear/Eliminar. Se bloquea la transferencia del archivo o se elimina el archivo
- Solo informar. Sólo se registra el evento correspondiente si así está configurado.

## **2.5. Módulo Anti-spam**

Panda GateDefender Performa, verifica el correo electrónico de la compañía por medio del módulo anti-spam, Así se reduce el impacto negativo del spam en la productividad de las empresas.

Para el análisis Antispam, Panda GateDefender Performa incorpora la tecnología de Cloudmark ([www.cloudmark.com](http://www.cloudmark.com)).

Cloudmark utiliza también una red de Inteligencia Colectiva, que es una combinación de firmas avanzadas de mensajes, corroboradas por un

feedback global y un análisis de datos automatizado que proporciona La respuesta más rápida a nuevos spams con una seguridad inigualable.

Los **algoritmos avanzados de firmas de mensajes**, permiten la detección automática de mensajes spam. Estos algoritmos apuntan a distintos atributos de spam incrustados en los mensajes. Según aparece un mensaje, los algoritmos generan una firma que representa aspectos únicos de cada mensaje. Una vez una firma se asocia a un spam verificado, todos los mensajes actuales y futuros que incluyan esta firma serán automáticamente bloqueados. Como resultado, el motor de Cloudmark incluido en GateDefender Performa es capaz de identificar mutaciones y variantes en prácticamente tiempo real.

Ante nuevas amenazas de spam, Cloudmark proporciona una respuesta extremadamente rápida, gracias a su **Red Global de Amenazas** que cuenta con 700 millones de fuentes de información distribuidas por 190 países y consta de proveedores de servicios, administradores de sistemas, honeypots y usuarios de confianza. La información de estas fuentes permite la detección de los últimos spams en minutos desde su aparición.

Todo el feedback obtenido de la red global de amenazas es corroborado por un **sistema de evaluación de confianza**, que analiza la reputación del informador y determina la clasificación de la firma basado en el nº de informes que la relacionan y la reputación de los informadores. La reputación se gana con el tiempo al informar consistentemente con datos correctos. Como el feedback es corroborado continuamente, cualquier inexactitud como falsos positivos o falsos negativos es corregida sin intervención manual.

**El motor de Cloudmark** instalado en GateDefender Performa se actualiza cada minuto con los nuevos mensajes spam conocidos. El motor genera una firma con cada mensaje que atraviesa el appliance y lo comprueba con las firmas de malos mensajes conocidos para determinar si el mensaje es spam. El sistema determina la clasificación del mensaje como spam, probable spam o no spam.

Se puede activar el análisis antispam para los protocolos SMTP, POP3 e IMAP4, tanto para correo entrante como saliente.

El administrador puede definir el nivel de sensibilidad del análisis entre Alto, Medio y Bajo.

- **Alto.** Más spam detectado pero mayor riesgo de falsos positivos
- **Medio.** Relación equilibrada entre spam detectado y falsos positivos
- **Bajo.** Menos spam detectado (90%) pero ningún falso positivo

Se puede configurar qué acciones realizar según la clasificación del mensaje. Tanto para spam como para probable spam y por separado, se puede:

- Marcar el asunto.
- Redirigir el mensaje a una dirección de correo.
- Almacenar el mensaje en la cuarentena de spam.
- Bloquear el mensaje en SMTP o sustituir cabecera en POP3 e IMAP4.

Adicionalmente se pueden configurar **listas blanca y negra** de direcciones y/o dominios. Los correos cuyo remitente esté en una lista no serán analizados. Serán automáticamente clasificados como No spam o como spam respectivamente.

Las listas se pueden exportar e importar en formato de texto estándar.

## **2.6. Módulo de Filtrado Web**

El módulo de Filtrado Web permite al administrador de la red controlar el uso de los recursos de la red corporativa. Incluye dos tipos de protección diferentes:

### **2.6.1. Protección Filtrado de URLs:**

Bloquea inmediatamente la recepción o acceso a contenidos web que no sean considerados interesantes para el desarrollo del trabajo. Estos contenidos pueden afectar al ambiente y rendimiento laboral. Además, pondrían en peligro la imagen de la compañía si se reenvían o reproducen por los empleados.

Esta protección analiza las URLs a las que se intenta acceder desde dentro de la red. Automáticamente se bloquea el acceso a las que no estén permitidas según la configuración, evitando el consumo de recursos como el ancho de banda y la pérdida de productividad de los usuarios de la red. Para el bloqueo de direcciones se puede configurar por categorías o listas manuales.

### **Filtrado por categorías predefinidas:**

Existen 60 categorías predefinidas de contenidos. El administrador marca las categorías a las que el acceso será restringido:

<b>Pornografía / Desnudez</b>	<b>Sitios extremos</b>
Pornografía	Violencia / Sitios extremos
Erotismo / Sexo	
Bañadores / Ropa interior	<b>Informática</b>
	Vendedores / Distribuidores de sw/hw
<b>Pedidos online</b>	Servicios de comunicación
Compras online	Seguridad informática / Información
Subastas / Anuncios	Traducción de sitios web
	Proxies anónimos
<b>Sociedad / Educación / Religión</b>	
Organizaciones gubernamentales	<b>Drogas</b>
ONGs	Drogas ilegales
Ciudades / Regiones / Países	Alcohol
Educación	Tabaco
Partidos políticos	Autoayuda / Adicción
Religión y espiritualidad	
Sectas	<b>Estilo de vida</b>

## Documento de Descripción del producto

### ***Panda GateDefender Performa***

---

	Citas / Relaciones
<b>Actividades de naturaleza ilegal</b>	Restaurantes / Bares
Actividades ofensivas o delictivas	Viajes
Crímenes informáticos	Moda / Cosméticos / Joyas
Extremismo político / Xenofobia	Deportes
Piratería / Hacking / Software ilegal	Construcción / Hogar / Arquitectura
	Naturaleza / Medio ambiente / Animal
<b>Juegos / Apuestas</b>	<b>Páginas personales</b>
Apuestas	
Juegos informáticos	<b>Búsqueda de empleo</b>
Juguetes	
	<b>Finanzas / Inversiones</b>
<b>Entretenimiento / Cultura</b>	Agentes de bolsa / Acciones
Cine / Televisión	Servicios financieros/Inversión/ Seguros
Instalaciones de ocio/Diversión/Parques	Bancos / Banca online
Arte / Museos / Monumentos	
Música	<b>Vehículos / Transporte</b>
Literatura / Libros	
Humor / Comics	<b>Armas</b>
<b>Información / Comunicación</b>	<b>Medicina</b>
Noticias / Periódicos / Revistas	Salud
Correo web	Aborto
Chat	
Grupos de noticias / BBS / discusión	<b>Spam</b>
SMS / Aplicaciones divertidas para teléfonos móviles	Spam URLs
Postales digitales	
Motores de búsqueda / Catálogos web /	<b>Spyware</b>

### **¿Cómo se categorizan las páginas web?**

Una serie de potentes servidores distribuidos alrededor del mundo analizan secuencialmente millones direcciones web, asociando cada URL con las diferentes categorías existentes. Para ello, se realizan varios tipos de análisis:

- **Análisis de textos**
  - Análisis del contenido de todo el texto de una página
  - Un OCR (Reconocedor óptico de caracteres) analiza el texto insertado en imágenes
- **Análisis de imágenes**
  - Reconocimiento de logotipos (ej. VISA, Master Card...)
  - Reconocimiento de pornografía o desnudos
  - Reconocimiento de caras
  - Reconocimiento de formas similares que agiliza el análisis.

Además, existe la opción de activación de la tecnología "WebLearn", que realiza un análisis automático de todas las URLs visitadas desde dentro

de la red, con el fin de asignarlas a categorías e introducir las en la base de datos. De este modo, El filtrado web de panda GateDefender Performa se adapta a la experiencia de cada organización.

#### **Filtrado por listas manuales:**

Existen 3 tipos de listas que se pueden definir.

- **Lista blanca** de direcciones web: El acceso se permite siempre.
- **Lista negra** de direcciones web: El acceso se prohíbe siempre.
- **Lista VIP** de usuarios. Los usuarios de la lista están exentos de todo filtrado.

#### **2.6.2. Protección Bloqueo de aplicaciones P2P**

Las aplicaciones Peer to Peer sirven para compartir ficheros en una red de ordenadores distribuida. Cada ordenador puede establecer una conexión con los demás, así como enviar y descargar archivos de los mismos. Esto supone un importante hueco de seguridad. Para evitarlo se bloquean:

- Acceso a servidores P2P
- Conexiones finales entre usuarios P2P

Las conexiones finales entre usuarios se bloquean con aplicaciones P2P que no usen servidores intermedios.

Panda GateDefender Performa permite bloquear los protocolos P2P:

- BitTorrent (Azureus, BitComet, Shareaza, MIDonkey...)
- eDonkey (eDonkey2000, MIDonkey)
- FastTrack (Kazaa, Grokster, iMesh, MIDonkey)
- Gnutella (BearShare, Shareaza, Casbos, LimeWire, MIDonkey)
- Gnutella2 (Shareaza, Trustyfiles, Kiwi Alpha, FileScope, MIDonkey...)
- OpenNap (Napster, Lopster, Teknap, MIDonkey)

Es posible bloquear cada protocolo Peer to Peer independientemente de los demás.

La configuración consiste en marcar los protocolos y aplicaciones a bloquear. Es posible elegir el **Nivel de protección** para garantizar el correcto uso de los recursos de red: para cada protocolo se pueden elegir 3 niveles de protección:

- **Nivel de rendimiento.** Prioriza el rendimiento del sistema general a la protección contra uso de las aplicaciones a filtrar.
- **Nivel de seguridad.** Prioriza la protección contra las aplicaciones sobre el rendimiento a través de los puertos o protocolos bloqueados.

- **Nivel de equilibrio.** Intenta equilibrar la protección con el rendimiento del sistema.

### **2.6.3. Bloqueo de Mensajería Instantánea (IM)**

La mensajería instantánea puede afectar al rendimiento de los usuarios de la red interna. Es posible bloquear las diferentes conexiones de aplicaciones de mensajería instantánea y Chat utilizables en Internet. GateDefender Performa puede bloquear las siguientes aplicaciones IM:

- ICQ/AOL
- IRC
- MSN Messenger
- Windows Messenger
- MSN Messenger File Transfer
- MSN Web Messenger
- Yahoo! Messenger
- Skype
- Jabber (Google Talk)

Es posible bloquear cada aplicación independientemente de las demás.

### **2.6.4. FILTRADO TEMPORAL**

Tanto en el caso del Filtrado de URLs, como para el bloqueo de aplicaciones P2P, como para aplicaciones IM es posible definir ventanas temporales independientes para cada protección.

Estas ventanas temporales permiten desactivar cada una de estas protecciones durante ciertos horarios definidos por el administrador. Por ejemplo, se podría permitir en una organización el tráfico P2P durante sábados y domingos o permitir la navegación sin filtrado de URLs durante ciertas horas del día.

## **2.7. Auto actualización**

El sistema de actualizaciones contra nuevas amenazas (virus, spam y contenidos no deseados) se realiza automática y continuamente.

- Las actualizaciones de ficheros de identificadores de malware son incrementales y se realizan automáticamente cada 90 minutos.
- Los datos de URLs clasificadas para el filtrado de contenidos web se actualizan igualmente cada 90 minutos.

- Los datos necesarios para la detección de spam son actualizados mediante microactualizaciones cada minuto.

Todos los procesos de actualización ocurren de forma automática sin intervención del usuario para garantizar que Panda GateDefender Performa posea todo el conocimiento y la potencia de detección de la Inteligencia Colectiva de Panda Security.

## **2.8. Cuarentenas**

Panda GateDefender Performa incorpora diferentes tipos de cuarentena para las distintas protecciones posibles, a saber:

- **Cuarentena de malware.** Para malware desconocido o no desinfectable.
- **Cuarentena de Content Filter.** Para archivos bloqueados por política de seguridad.
- **Cuarentena de spam.** Para correos spam o probable spam y su posterior verificación.

En la configuración general de la cuarentena, el administrador puede definir varios parámetros:

- **Antigüedad máxima** de los elementos almacenados en las cuarentenas. Al alcanzar la antigüedad máxima permitida, los elementos serán eliminados de la cuarentena.
- **Tamaño máximo de ficheros** a almacenar en las cuarentenas. Se puede elegir de 0 a 100 MB. Por defecto el tamaño máximo es 20 MB.
- **Envío automático a PandaLabs** de los ficheros introducidos en la cuarentena de malware. Los ficheros de más de 5 MB no se podrán enviar a PandaLabs. En este caso, Pandalabs determina si el fichero:
  - **Es malware**, incluyéndolo en el fichero de firmas y comenzando el desarrollo de su vacuna inmediatamente.
  - **No es malware**, marcando el fichero de la cuarentena como **falso positivo**.

Un mismo elemento puede llegar a la cuarentena varias veces, por protocolos diferentes, con diferentes destinatarios, etc. En las cuarentenas se muestran los elementos almacenados y el nº de veces o instancias de los mismos que ha llegado.

Las acciones posibles a realizar sobre los ficheros almacenados en la cuarentena son:

- **Ver instancias.**
- **Enviar a PandaLabs** elementos de la cuarentena de malware de forma manual para determinar si son malware o no.
- **Eliminar elemento.** Borra físicamente el elemento del almacén de cuarentena.
- **Excluir fichero de la cuarentena.** De este modo este fichero no volverá a ser enviado a cuarentena. Funciona como una marcación

manual de que no es un falso positivo y la inclusión del fichero en una lista blanca.

- **Descargar fichero.**

Además, para cada instancia se podrá:

- **Descargar el fichero original** (manteniendo el formato original para ficheros llegados por HTTP y FTP).
- **Restaurar el mensaje original** (con el mismo remitente y destinatario). Sólo para ficheros llegados por SMTP.
- **Redirigir el mensaje a otra cuenta de correo.** Sólo para instancias llegadas a través de SMTP, POP3, IMAP4 o NNTP.

Cada elemento que se envía a cualquiera de las cuarentenas tendrá un código identificador (CRC). Todos los elementos iguales enviados a la cuarentena tendrán el mismo CRC. Así es posible agruparlos y facilitar el acceso a los datos de cuarentena.

Los distintos tipos de cuarentena proporcionan tratamientos diferentes para los diferentes tipos de información almacenada.

#### **2.8.1. Cuarentena de malware.**

Permite almacenar dos tipos de ficheros:

- **Ficheros con malware desconocido.** Estos ficheros sospechosos son detectados por el motor heurístico de la protección Anti-malware de GateDefender Performa.
- **Ficheros con malware no desinfectable.** Estos son ficheros malware conocidos que aún no tienen vacuna. Sin embargo, sí existe la firma que detecta que el fichero es malware.

El fichero se almacena hasta que se marque como falso positivo o exista una vacuna. En este momento se puede restaurar y enviar automáticamente al destinatario. Esta acción sólo es posible si el fichero llegó por correo a través del protocolo SMTP.

#### **2.8.2. Cuarentena de Content Filter.**

Panda GateDefender Performa dispone de una cuarentena específica para los ficheros y mensajes bloqueados por Content Filter. En este caso el bloqueo se corresponde con una regla específica de la Política de Seguridad de la compañía. Con la cuarentena de Content Filter se asegura que el administrador podrá recuperar los ficheros bloqueados si lo desea.

En el informe de la cuarentena de Content Filter se muestra la regla que provocó su almacenamiento en la cuarentena.

#### **2.8.3. Cuarentena de Spam**

Los correos clasificados como spam y como Probable spam, pueden enviarse a la cuarentena de spam.

En el informe de cuarentena se especifica si fue considerado spam o probable spam para su almacenamiento en la cuarentena.

Cuando un correo se almacena en la cuarentena, se envía al destinatario el mismo correo. En este correo se incluye:

- la marca correspondiente (spam, probable spam...)
- un aviso de que se ha enviado a la cuarentena
- El código CRC de recuperación

El administrador puede establecer que esta notificación no se envíe al destinatario para los mensajes que lleguen por SMTP.

Los datos relevantes sobre el estado de las cuarentenas se muestran en la pantalla de estado de la consola web. En esta pantalla se muestran datos como:

- Porcentaje de ocupación de la cuarentena de malware
- Porcentaje de ocupación de la cuarentena de Content Filter
- Porcentaje de ocupación de la cuarentena de Spam

Si una cuarentena alcanza el 100% de ocupación y siguen llegando elementos a la cuarentena, el administrador puede elegir entre:

- Empezar a eliminar los elementos almacenados más antiguos para almacenar los nuevos.
- Dejar de almacenar elementos en la cuarentena.

## 2.9. Integración con LDAP/AD

Muchos administradores han instalado servicios de directorio en las redes de su empresa. Así facilitan la gestión de nombres de usuarios y grupos y la asignación de rangos de IPs por áreas.

El sistema más extendido es LDAP (Lighweight Directory Access Protocol). Es un servicio de directorio ordenado y distribuido para buscar distintos tipos de información en un entorno de red. Un caso particular de LDAP es Active Directory o AD. Active Directory es el nombre utilizado por Microsoft para referirse a su implementación del protocolo LDAP en los servidores. Al estar disponible en los sistemas operativos Windows, se encuentra muy extendido a nivel mundial.

Es interesante que el appliance perimetral disponga de información acerca de la organización lógica de la red interna. Existen muchas posibilidades de intercambio de información entre el dispositivo y los miembros de la red.

**Ejemplo:** Simplemente para la realización de informes detallados es importante conocer el usuario objeto de la línea de informe. Este usuario podría ser el destinatario de un virus o quien intenta acceder a un sitio web

prohibido. En una red con servidores DHCP<sup>1</sup>, la IP no es suficiente para identificar al usuario, porque las IPs varían. Con un sistema LDAP la información del usuario es completa y el informe es más detallado.

Panda GateDefender Performa incorpora la integración con LDAP y particularmente con Active Directory. Puede importar la configuración de usuarios y grupos de la red sincronizándose con los servidores LDAP de la misma. Así se podrán definir distintos tipos de interacción con los usuarios.

El sistema de administración de directorios de una empresa puede no ser LDAP ni Active Directory. En este caso, se puede definir cualquier sistema, con solo introducir los parámetros de control en la consola.

Además, Panda GateDefender Performa incorpora un servidor LDAP interno dentro del dispositivo. Esto permite definir directamente una estructura de red con usuarios, grupos, rangos de direcciones IP, etc. Es decir, para empresas sin LDAP, GateDefender Performa proporciona los mecanismos de identificación de IPs con usuarios y grupos, al mismo tiempo que se mantiene una copia local de los directorios para evitar múltiples accesos innecesarios al mismo. De este modo se conoce la identidad de cada IP de la red. También se pueden definir distintas formas de interactuar con cada usuario.

## **2.10. Diferentes Perfiles de usuario**

En una misma red existen distintas necesidades de seguridad para depende qué miembros de la red. Por ejemplo en cuanto al filtrado de URLs, algunos usuarios no deben poder visitar ciertas páginas web. Otros, en cambio, sí deben tener acceso a dichas páginas pero no a otras. En un ejemplo de Content Filter puede que algunos usuarios no deban enviar o recibir ficheros de cierto tipo. Otros en cambio, deben poder enviarlos sin problemas.

La existencia de usuarios con diferentes necesidades implica poder tener **diferentes políticas de seguridad**, dentro de la misma compañía. Esta posibilidad se materializa en GateDefender Performa a través de los **Perfiles de usuario**.

El concepto consiste en generar diferentes combinaciones de configuración de las protecciones. Los perfiles diferentes son aplicables a todas las protecciones presentes en la solución. Las reglas para la creación de perfiles son:

- **Perfil por defecto.** Siempre existe una configuración (perfil) por defecto que se define como política de seguridad general.
- **Perfiles modulares.** Un perfil puede realizar cambios sobre la política general del módulo o módulos de protección que el administrador desee.
- **Asignación de perfiles a usuarios y grupos.** Cada perfil se puede asignar indistintamente a usuarios, grupos, rangos de IPs, etc., combinaciones de estos datos.

---

<sup>1</sup> DHCP es un Protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP

La mejor forma de ver la utilidad de los perfiles de usuario es un ejemplo.

#### **Enunciado:**

En una empresa se necesita definir una política de filtrado web que impida el acceso a:

- Páginas de entretenimiento
- Páginas de compras y subastas
- Páginas de información y comunicación
- Páginas de Búsqueda de empleo

Por otro lado, todo el departamento de Recursos Humanos sí necesita acceder a las páginas de búsqueda de empleo.

Además, el dpto. de comunicación necesita acceder a las páginas de información y comunicación para comprobar la repercusión de la compañía en los medios. Dos personas de Marketing (Juan y Pedro) necesitan también acceder a esta información para hacer estudios de mercado.

Por último, el director general puede acceder a cualquier página.

En cuanto a la protección Anti-spam es necesario que los correos probable spam se guarden en cuarentena, excepto para el departamento de Recursos Humanos, que puede recibir ofertas de empresas de contratación temporal. Para ellos los mensajes probable spam deberían llegar marcados.

#### **Solución:**

**1.- Creación de la política general.** En el filtrado web se bloquea el acceso a las categorías

- Páginas de entretenimiento
- Páginas de compras y subastas
- Páginas de información y comunicación
- Páginas de Búsqueda de empleo

Dentro de esta política se incluirá la IP o el nombre de usuario del Director General en la lista VIP.

Además se configura que los correos probable spam se envíen a cuarentena y los que sean spam se eliminen.

**2.- Creación de un nuevo perfil llamado RRHH.** En este perfil se incluirán cambios sobre el módulo Anti-spam y sobre el de Filtrado web. Para las demás protecciones será válida la configuración del perfil general.

En el filtrado web se prohibirá el acceso a las mismas categorías que en la política general, excepto a la de Búsqueda de empleo

En el Anti-spam se elegirá la opción de marcar los mensajes probable spam y dejarlos pasar

**3.- Creación de un nuevo perfil llamado COMUNIC.** En este perfil se incluirán cambios sobre el módulo de Filtrado web. Para las demás protecciones será válida la configuración del perfil general.

En el Filtrado web se prohibirá el acceso a la mismas categorías que en la política general excepto a la de Información y Comunicación

#### **4.- Asignar perfiles.**

Asignar al grupo de usuarios de Recursos Humanos el perfil de seguridad RRHH

Asignar al grupo de usuarios de Comunicación el perfil de seguridad COMUNIC

Asignar a los usuarios Juan y Pedro el perfil de seguridad COMUNIC

Como se ve las posibilidades de los perfiles de seguridad diferenciados son infinitas y permite la adaptación a la arquitectura de red de cualquier empresa.

### **2.11. Configuración centralizada**

Panda GateDefender Performa permite la configuración individual o centralizada de varios appliances desde una única consola.

En redes donde existan varios appliances, bien en balanceo de carga, bien distribuidos protegiendo distintas zonas de red, se pueden crear grupos de appliances. Cada appliance se puede asignar a un grupo.

Por otro lado, distintas configuraciones se pueden asignar a diferentes appliances o grupos de appliances. Del mismo modo, un perfil de protección o un conjunto de perfiles de protección se pueden asignar a un appliance o a un grupo de appliances.

### **2.12. Niveles de acceso a consola**

Panda GateDefender Performa se gestiona de forma remota y segura con una intuitiva consola web. El administrador disfruta de la flexibilidad de poder acceder a sus appliances desde cualquier ordenador.

Existen diferentes niveles de acceso a la consola web de administración:

- **Monitorización:** Permite el acceso a las pantallas de estado, Actividad, Informes y Servicios
- **Configuración de Protecciones:** Permite el acceso a todas las pantallas excepto a las de configuración del sistema, Actualizaciones, Gestión de Licencias y Herramientas
- **Configuración del Sistema:** Permite el acceso a todas las pantallas excepto a las de Actualizaciones, Gestión de Licencias y Herramientas
- **Administración:** Permite el acceso a todas las pantallas y menús.

## **2.13. Informes gráficos de la actividad del sistema**

Panda GateDefender Performa incorpora en el interfaz de la consola web de administración informes gráficos de la actividad de las distintas protecciones que permiten ver gráficamente la evolución en el tiempo de las diferentes protecciones activas. Esta visualización gráfica en tiempo real, permite fácilmente ver las amenazas detenidas por GateDefender Performa y valorar su eficacia de acuerdo con datos reales de la actividad registrada en la red corporativa en la que GateDefender Performa está instalado.

## **2.14. Alertas y eventos**

Panda GateDefender Performa proporciona alertas y notificaciones personalizadas en el idioma que desee el usuario. Además, permite enviar los eventos importantes a través de diferentes formatos:

- **SMTP.** Correos de alerta que se envían a una dirección de correo
- **Syslog.** Permite al administrador analizar todo lo que ocurre en sus unidades GateDefender Performa con un sistema que puede utilizar con otros dispositivos de la red.
- **SNMP.** Permite la monitorizar de forma centralizada todos los dispositivos instalados en la red.

Cualquier herramienta de monitorización centralizada que lea estos formatos pueden ser configurada para leer los datos exportados por las unidades Panda GateDefender Performa.

### **2.14.1. Envío de información a través de SNMP**

SNMP (Simple Network Management Protocol o Protocolo Simple de Gestión de Red) es un protocolo que funciona a nivel de aplicación para la gestión de redes. Funciona enviando mensajes a diferentes componentes de la red. Estos dispositivos, llamados agentes, almacenan información sobre su estado o los eventos que se producen en ellos en un MIB (Management Information Base o Base de Gestión de la Información), que es una base de datos de objetos que se pueden monitorizar a través de un gestor de red SNMP. Dichos dispositivos son capaces de responder con esta información ante peticiones SNMP.

De esta forma un administrador de una red puede monitorizar el rendimiento de la red, detectar y solucionar problemas en la red, o incluso preparar la red para su crecimiento de manera controlada.

Las unidades GateDefender Performa presentes en una red se pueden monitorizar de manera centralizada desde cualquier herramienta de gestión de redes SNMP.

En general para gestionar una red a través de SNMP, se necesitan los siguientes elementos:

## Documento de Descripción del producto

### ***Panda GateDefender Performa***

---

- Sistema gestor de red
- Agentes
- Dispositivos gestionados

Un dispositivo gestionado es cualquier elemento de una red que sea capaz de transmitir información de su estado a través del protocolo SNMP. Por tanto, dentro de una red podrían ser un router, un servidor, un switch, un hub, un equipo host o incluso una impresora.

En cada dispositivo gestionado habrá un agente que es el que tiene el conocimiento del protocolo SNMP y es el que se encarga de transmitir la información solicitada.

Por último, el sistema gestor de red se encarga de recolectar la información de los dispositivos monitorizados de la red y ofrecérsela al administrador. En una red podrá existir uno o más de estos gestores de red, y además un gestor podría funcionar a la vez como agente y reportar a un gestor de jerarquía superior.

El sistema SNMP implementado para GateDefender Performa es de lectura, de forma que el gestor de red puede consultar los valores de las variables ofrecidas por cada unidad.

Además, cada GateDefender Performa tiene un sistema de alertas asíncronas o traps, que permiten comunicar al gestor los eventos que se vayan produciendo en la unidad, aunque no estuvieran solicitadas por el gestor central. Estas alertas se utilizan sólo para eventos importantes y se envían sin esperar respuesta.

La información que contiene el MIB de GateDefender Performa es la siguiente:

<b>Sistema</b>	
Estadísticas de conexiones	Conexiones establecidas por cada protocolo
	Conexiones falladas por cada protocolo
Estadísticas de actividad	Conexiones abiertas actuales
	Tasa de Tráfico en el appliance
	Porcentaje de uso de CPU
Estadísticas de tráfico en tarjetas de red	Tráfico de entrada Mbytes para cada tarjeta
	Tráfico de entrada bytes LSB para cada tarjeta
	Tráfico de entrada bytes MSB para cada tarjeta
	Tráfico de salida Mbytes para cada tarjeta
	Tráfico de salida bytes LSB para cada tarjeta
	Tráfico de salida bytes MSB para cada tarjeta
	Dirección MAC de cada tarjeta
Estado de dispositivos en balanceo de carga	Nombre del nodo
	Dirección IP del nodo
	Modo de funcionamiento del nodo (Maestro/esclavo)
Estado de tarjetas de red	Estado de la conexión para cada tarjeta (conectada/desconectada)

## Documento de Descripción del producto

### ***Panda GateDefender Performa***

	Modo de funcionamiento de cada tarjeta (fullduplex/halfduplex)
	Dirección MAC de cada tarjeta
	Capacidad de cada tarjeta en Mbps
Otros	Fecha de última actualización
	Fecha de caducidad de la licencia
	Actualizaciones pendientes
	Tiempo de ejecución del appliance en segundos
	Fecha y hora de inicio de estadísticas
<b>Anti-malware</b>	
Información de Licencia	Estado de la licencia (enabled/disabled)
Información de protecciones	Protección contra Virus en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección contra Jokes en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección contra Dialers en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección contra Spyware en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección contra phishing en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección de Heuristic en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
	Protección de Other Risks en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
Estadísticas de Anti-malware	Número de Ficheros analizados
	Número de Ficheros con malware
<b>Content Filter</b>	
Información de protecciones	Protección Content Filter en HTTP, FTP, SMTP, POP3, IMAP4 y NNTP (No definido/enabled/disabled)
Estadísticas de Content-Filter	Nº elementos analizados para cada protocolo
	Nº elementos filtrados para cada protocolo
<b>Anti-spam</b>	
Información de Licencia	Estado de la licencia (enabled/disabled)
Información de protecciones	Protección Anti-spam para SMTP, POP3 e IMAP4 (No definido/enabled/disabled)
Estadísticas de Anti-spam	Nº de correos analizados para cada protocolo
	Nº de correos clasificados como spam para cada protocolo
	Nº de correos clasificados como Probable spam para cada protocolo
<b>Filtrado web</b>	
Información de Licencia	Estado de la licencia (enabled/disabled)
Información de protecciones	Protección Filtrado web (No definido/enabled/disabled)
Estadísticas de filtrado web	Peticiones analizadas
	Peticiones filtradas
<b>Filtrado de aplicaciones IM&amp;P2P</b>	
Información de Licencia	Estado de la licencia (enabled/disabled)
Información de protecciones	Protección Filtrado IM&P2P (No definido/enabled/disabled)
Estadísticas de filtrado	Conexiones detectadas

## Documento de Descripción del producto

### ***Panda GateDefender Performa***

IM&P2P	Conexiones bloqueadas
--------	-----------------------

Además, dispone de los siguientes traps para envío de alertas críticas:

<b>TRAPS enviados desde GateDefender Performa</b>	
Detección de virus, Jokes...	Alerta resumen de malware (con detección de malware)
Error del sistema	Alerta resumen de malware (ningún malware detectado)
Archivo potencialmente peligroso	Elemento filtrado por Content-Filter
Actualización del software de sistema pendiente	Aviso de caída da Appliance maestro en balanceo de carga
Elemento borrado por no haberse podido analizar	Aviso de caída da Appliance esclavo en balanceo de carga
Actualización del fichero de identificadores de virus correcta	Filtro de controles ActiveX
Actualización del fichero de identificadores de virus fallida	Filtro de applets Java
Actualización del fichero de identificadores de spam correcta	Filtro de discordancia entre formato, extensión y tipo MIME
Actualización del fichero de identificadores de spam fallida	Filtro de archivos con macro
Actualización de base de datos de Filtrado de URLs correcta	Filtro de archivos con contraseña
Actualización de base de datos de Filtrado de URLs fallida	Filtro de archivos/mensajes cifrados
Actualización del motor antivirus correcta	Filtro de archivos por tamaño máximo
Actualización del motor antivirus fallida	Filtro de referencias a scripts externos
Actualización del motor antispam correcta	Filtro de referencias a URLs externas
Actualización del motor antispam fallida	Filtro de tipos MIME peligrosos
Actualización del motor de Filtrado de URLs correcta	Filtro de contenido textual
Actualización del motor de Filtrado de URLs fallida	Filtro de mensajes malformados
La licencia de Antivirus va a expirar	Filtro de numero de destinatarios
La licencia de Antispam va a expirar	Filtro de mensajes parciales
La licencia de URL Filtering va a expirar	Filtro de archivos comprimidos peligrosos
La licencia de Antivirus ha expirado	Filtro de extensiones peligrosas
La licencia de Antispam ha expirado	Filtro de extensiones múltiples o extensiones trucadas
La licencia de URL Filtering ha expirado	El mensaje SMTP no ha podido ser redirigido
El mensaje SMTP no ha podido ser enviado	Se ha encontrado Appliance esclavo
Se ha encontrado Appliance Maestro	No ha sido posible redirigir los mensajes
Software del sistema actualizado con éxito	Detectado acceso a aplicaciones de mensajería e intercambio de datos
Espacio dedicado a cuarentena a punto de agotarse	Espacio dedicado a cuarentena agotado

## Documento de Descripción del producto

### ***Panda GateDefender Performa***

---

Elemento eliminado de cuarentena	Elemento borrado de cuarentena
Elemento de cuarentena enviado a cuarentena	Detección de malware en elemento de cuarentena
Elemento movido a cuarentena	Error grave del sistema
Error de conexión con el servidor para envíos a Panda desde cuarentena de malware	Error de conexión con el servidor ldap
El servidor de ldap ha devuelto un error	Cuarentena purgada

En cuanto al agente SNMP interno de GateDefender Performa, el administrador podrá definir distintos gestores a los que enviar distintos grupos de variables o alertas. Estos gestores pertenecen a comunidades de usuarios y para cada comunidad se pueden definir:

- Nombre de la comunidad
- Lista de managers SNMP que pueden monitorizar el appliance a los cuales se enviarán los traps.
- Queries permitidas en cada puerto y versión del protocolo SNMPv1 o SNMPv2. Por defecto las queries se definen a través del puerto 161 UDP del GateDefender Performa.
- Si se permiten traps SNMP, en qué puerto y para qué versión del protocolo (SNMPv1 ó SNMPv2). Por defecto los traps se envían al puerto 162 UDP.

Como se ve, cada comunidad tiene su propia configuración de traps y queries, y en cada una de ellas podrá haber uno o más gestores.

#### **2.14.2. Sistema para almacenar eventos (Syslog)**

Syslog es una utilidad que sirve para exportar todos los eventos que se vayan produciendo en una aplicación, así como información acerca del estado de la misma, que se ha llegado a convertir en un estándar en el mercado, de forma que un administrador de redes que tenga distintos tipos de dispositivos, incluso de distintos fabricantes, puede realizar un seguimiento de todos ellos a través de la información que cada uno ha enviado a través de Syslog.

GateDefender Performa incorpora esta posibilidad de reportar logs a un servidor Syslog remoto. Para ello el administrador puede configurar el servicio indicando en una pantalla todos los datos necesarios como Servidor: dirección IP o nombre del dominio; Puerto (514 por defecto) al que se enviarán los eventos; Facility (local0, local1,..., local7);...

Los eventos de GateDefender Performa que pueden generar una nueva entrada en el Syslog remoto son los siguientes:

##### **Sistema**

- Error del sistema
- Actualización
- Actualización del software de sistema pendiente

**Anti-Malware**

- Detección de malware
- Detección de elementos potencialmente peligrosos
- Elemento borrado por no haberse podido analizar

**Content Filter**

- Detección de controles ActiveX
- Detección de Applets de Java
- Detección de discordancia entre formato, extensión y tipo MIME
- Detección de múltiples extensiones o extensiones trucadas
- Detección de archivos con macros
- Detección de archivos protegidos por contraseña
- Detección de archivos adjuntos con tamaño superior al límite configurado
- Eliminación de scripts
- Eliminación de referencias a URLs externas
- Detección de archivos con extensiones peligrosas
- Detección de archivos con tipo MIME peligroso
- Detección de mensajes por contenido textual
- Detección de mensajes malformados
- Eliminar mensajes parciales
- Detección de archivos comprimidos sospechosos
- Mensaje filtrado por número de destinatarios

**Anti-spam**

- Detección de spam
- Detección de Probable spam

**Filtrado Web**

- Pagina web restringida visitada

**2.15. Monitorización centralizada (CACTI)**

Panda GateDefender Performa se integra con una adaptación de la aplicación Cacti para realizar la monitorización centralizada.

Cacti es una herramienta «Open source» que incorpora una consola de acceso web para monitorizar varias unidades de GateDefender Performa a la vez. La monitorización se hace a través de plantillas predefinidas que realizan peticiones SNMP a las distintas unidades monitorizadas en paralelo, creando informes gráficos de actividad de cualquier evento que ocurra en los distintos sistemas.

Cacti, a través de un plugin para integración con syslog, permite también la recepción de eventos de syslog de todas las unidades GateDefender Performa desplegadas. Es posible realizar búsquedas en los eventos recibidos, para ver, por ejemplo todos los eventos de malware de una determinada IP o usuario, etc.

Además, el administrador podrá definir nuevos gráficos y plantillas si así lo desea para incrementar el nivel de la información obtenida.

## 2.16. Sincronización con servidores horarios (NTP)

En redes grandes y complejas pueden entrar en juego procesos de actualizaciones masivas o retardos relativamente grandes. En estas redes es deseable que los dispositivos de la red implementen el protocolo NTP (Network Time Protocol o Protocolo de Tiempo de Red). Este protocolo permite sincronizar los relojes de los diferentes dispositivos de la red. Dicha sincronización se hace con un servidor que cubre una zona horaria determinada, realiza.

GateDefender Performa incorpora el protocolo NTP. Esto permite precisar en qué momento exacto se ha producido cualquier evento, en cada unidad de la red. Disponer de un sistema horario preciso es de gran ayuda para solucionar los problemas de la forma más eficiente. Es crucial ante situaciones de ataques masivos, errores en las descargas, caídas de los firewalls de la red, etc.

## 2.17. Modelos de hardware

Panda GateDefender Performa serie 9000 cuenta con cuatro modelos hardware que se adaptan a las necesidades de organizaciones de distintos tamaños. Los modelos hardware de la serie 9000 de Panda GateDefender Performa se describen en la siguiente tabla:

Feature	Performa 9050	Performa 9100	Performa 9200	Performa 9500
<b>Processor</b>	1 x AMD Opteron Dual Core 1220 (2,8 GHz)	1 x AMD Opteron Dual Core 1222 (3Ghz GHz)	1x2,33 Ghz Quad Core (Intel)	2x AMD Opteron Dual Core 2220 (2.8GHz)
<b>Memory</b>	2 GB (2 X 1GB) DIMM DDR2 667	4 GB (4 X 1GB) DIMM DDR2 667	4 GB (4 X 1GB) DIMM DDR2 667	8 GB (4 x 2GB) DIMM DDR2 667
<b>HDD</b>	1 x 250 GB / 7200 rpm / SATA II	1 x 250 GB / 7200 rpm / SATA II	1x 73GB 10K RPM 2.5" SAS HDD	2x 73GB 10K RPM 2.5" SAS HDD RAID 1
<b>NICs</b>	10/100/1000 ethernet	10/100/1000 ethernet	10/100/1000 ethernet	10/100/1000 ethernet
<b>USB</b>	YES	YES	YES	YES

<b>Bypass</b>	NO	NO	NO	YES (1 Silicom bypass card) 2 x 10/100/1000
<b>Console/Monitor</b>	Yes	Yes	Yes	Yes
<b>Serial</b>	Yes	Yes	Yes	Yes
<b>Optical Drive</b>	DVD	DVD	DVD	DVD
<b>Power Suply</b>	1	1	2	2
<b>Size</b>	1 Rack Unit	1 Rack Unit	1 Rack Unit	1 Rack Unit
<b>Maximum Recommended users</b>	100	500	1200	2500

### **2.18. Sistema de auto-reparación:**

Panda GateDefender Performa cuenta con sistema de control de actividad de los servicios del sistema.

Si el sistema de auto-reparación detecta que algún servicio no funciona correctamente lo echa abajo. A continuación lo reestablece de forma transparente al administrador, asegurando así la continuidad de la protección.

### **2.19. Watchdog**

Podría ocurrir, en situaciones extremas (excesos de calor, etc.) que GateDefender Performa sufriera daños a nivel de hardware. En estos casos, algunos componentes clave podrían no funcionar correctamente.

Como prevención, las unidades hardware de todos los modelos cuentan con un sistema de monitorización continua, llamado watchdog. Este sistema levanta una alerta en tiempo real al observar una anomalía en un componente hardware. Esto permite al sistema lanzar contramedidas para superar la situación y recuperar el comportamiento normal.

### **2.20. Balanceo de carga**

El balanceo de carga aporta mayor rendimiento y alta disponibilidad al sistema de protección perimetral. Consiste en la instalación de varias unidades GateDefender Performa en paralelo. De este modo se puede distribuir la carga de tráfico del sistema entre las unidades instaladas.

El sistema de balanceo de GateDefender Performa no precisa instalar dispositivos, hardware o software adicionales. La interconexión de las unidades se puede hacer con dos dispositivos concentradores. Se pueden utilizar tanto Switches, como Hubs, aunque se recomienda la utilización de Switches.

Sólo un appliance asumirá el rol del "maestro". El resto asumirán el rol de "esclavo". Desde la consola de administración se puede ver el modo de funcionamiento de cada appliance en cada momento.

Al instalar varios GateDefender Performa en paralelo se inicia la auto-negociación del rol de cada uno. Si después se añade un nuevo appliance, se volverán a negociar los modos de funcionamiento.

El maestro implementa un algoritmo de balanceo que redirige las conexiones a los esclavos. Además el maestro se encarga de analizar las conexiones, y permitir el paso del tráfico que ha sido limpiado.

Los appliances esclavos no dejan pasar tráfico al interior de la red. Se limitan a analizar las conexiones que les son redirigidas por el maestro, devolviendo al maestro el tráfico limpio.

Además, para redes complejas donde otros equipos de misión crítica pueden necesitar comportamientos especiales, Panda GateDefender Performa permite definir manualmente todos los parámetros del balanceo de carga:

- Bridge priority
- Bridge forward delay
- Bridge hello time
- Maximum address age
- Ethernet address ageing time
- Bridge cost (eth0)
- Bridge cost (eth1)

Cada unidad hardware añadida proporciona un rendimiento cercano al 100% por lo que la capacidad de análisis crece linealmente al añadir nuevas unidades.

### **2.21. Garantía de flujo de tráfico (bypass)**

El modelo superior de la serie, Panda GateDefender Performa 9500, incorpora una tarjeta de red con la opción de bypass. Esta tarjeta garantiza que ante caídas imprevistas del sistema, el tráfico de la organización no será bloqueado por el appliance, atravesando el perímetro todo el tráfico entrante y saliente de forma transparente y sin ser analizado.

### **2.22. Rendimiento**

Panda GateDefender Performa proporciona un rendimiento óptimo. El rendimiento es un valor muy importante para los dispositivos que se instalan en el gateway de la red. Esto se debe a la cantidad de tráfico tanto entrante como saliente que lo atraviesa.

En las pruebas realizadas en el laboratorio de Panda Security se han obtenido los resultados que se muestran en las siguientes tablas:

**Pruebas de análisis en HTTP:**

Modelo	Rendimiento Througput en HTTP
GateDefender Performa 9050	40 Mbps
GateDefender Performa 9100	80 Mbps
GateDefender Performa 9200	170 Mbps
GateDefender Performa 9500	360 Mbps

**Pruebas de análisis en SMTP:**

Modelo	Rendimiento máximo en SMTP
GateDefender Performa 9050	80 mensajes/segundo
GateDefender Performa 9100	160 mensajes/segundo
GateDefender Performa 9200	350 mensajes/segundo
GateDefender Performa 9500	720 mensajes/segundo