

satec 



fwat

1. Seguridad de los sistemas TIC
2. Problemas en la seguridad perimetral: Administración de cortafuegos
3. Gestión actual del flujo de modificación de reglas
4. FWAT
5. Funcionamiento y gestión de reglas
6. Arquitectura de la solución
7. Beneficios de FWAT
8. Servicios gestionados de seguridad
9. Sumario



- El fundamento de los estándares de seguridad **son los procesos, no las aplicaciones**. Es necesario entender la seguridad como un **ciclo de mejora continua**.
- Los sistemas TIC, se encuentran en **permanente evolución**, modificaciones, instalación de nuevos dispositivos, aplicaciones...
- Los **Firewalls o Cortafuegos** son los dispositivos encargados de controlar las comunicaciones de estos dispositivos, o aplicaciones, con el exterior de la red
- De la gestión de los cortafuegos pueden derivarse **vulnerabilidades** en la red y complicaciones para administradores y usuarios.



Problemas en la seguridad perimetral: Administración de Cortafuegos

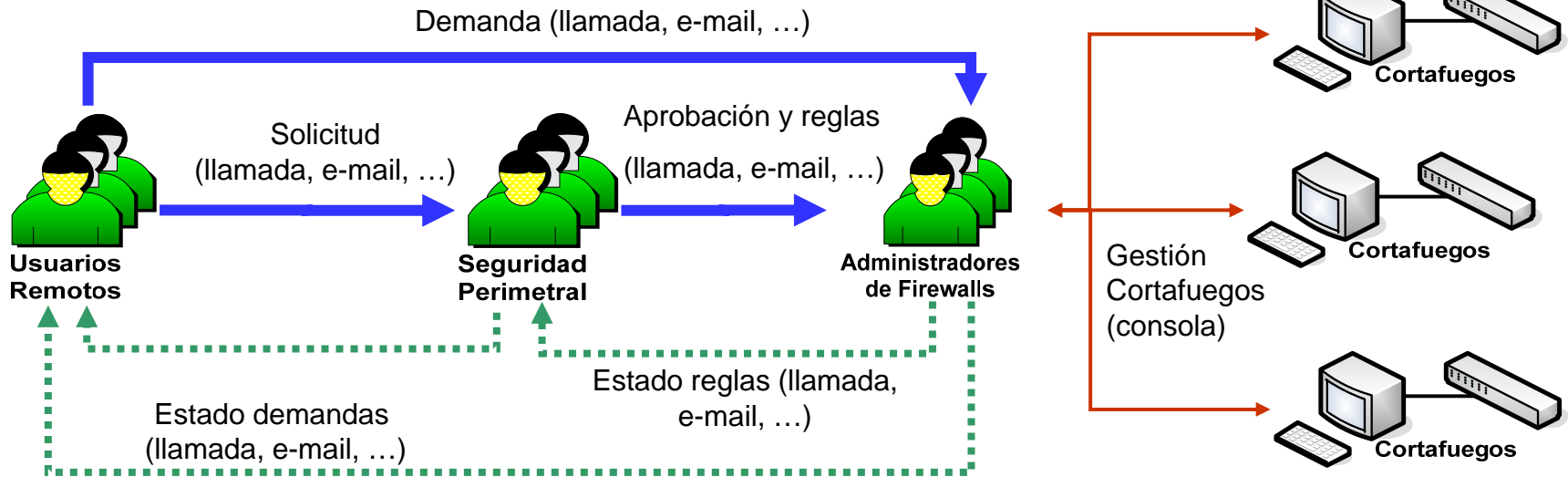
- **Entorno Cambiante:** La apertura temporal de puertos o la implantación de nuevas aplicaciones, llevan a la **necesidad de realizar frecuentes modificaciones** en las reglas de seguridad. Dando lugar a **vulnerabilidades** en la seguridad perimetral.
- **Comunicación Informal:** Las peticiones de apertura o modificación de los puertos se realizan habitualmente por medios como Teléfono o correo electrónico, no permitiendo un seguimiento adecuado de estas peticiones, en consecuencia:
 - Se produce la pérdida de peticiones
 - No es posible medir el nivel de servicio.
 - Los usuarios desconocen que datos suministrar en sus peticiones.
 - Escasa supervisión de la modificación de las reglas

Problemas en la seguridad perimetral: Administración de Cortafuegos

- **Falta de Información para auditorias:** La carencia de registros históricos de las modificaciones realizadas, la razón de las modificaciones, o los usuarios que las solicitaron, Imposibilitan prevenir los mismos errores en el futuro.
- **Carencia de un punto de control único:** Al emplear cortafuegos de diferentes fabricantes, se requieren aplicaciones específicas para poder comprobar la coherencia de las reglas de los distintos Firewalls desde una única herramienta.



Gestión actual del flujo de modificación de reglas



En la figura superior puede observarse la administración de las reglas de seguridad perimetral en una organización sin una aplicación de gestión, como FWAT. En organizaciones donde se han segregado los roles de Responsable de Seguridad Perimetral y Administrador de Firewalls; se observa un incremento de los procesos de comunicación, llevados a cabo mediante herramientas informales se facilitan los errores que pueden dar lugar a una degeneración de la seguridad perimetral.

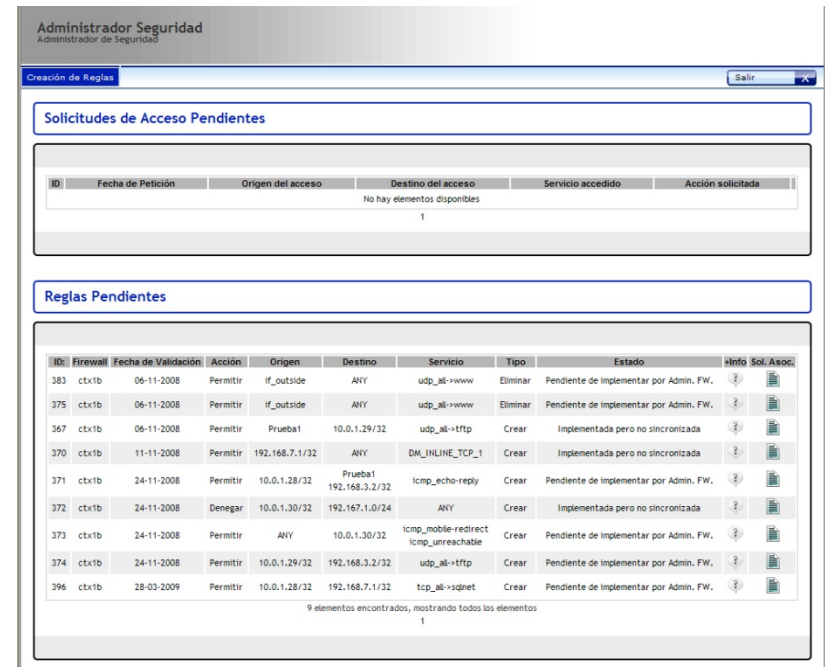
FWAT

Firewall Administration Tool

FWAT es la solución de SATEC, orientada al **control y gestión del flujo de modificaciones** de las reglas de acceso a la red de comunicaciones de la organización

Se fundamenta en:

- La Implantación de procesos que contribuyan a evitar vulnerabilidades en las reglas de acceso a la red.
- Elevar la productividad del personal del área de seguridad.
- Facilitar las peticiones de los usuarios



Administrador Seguridad
Administrador de Seguridad

Creación de Reglas Salir

Solicitudes de Acceso Pendientes

ID	Fecha de Petición	Origen del acceso	Destino del acceso	Servicio accedido	Acción solicitada
No hay elementos disponibles					
1					

Reglas Pendientes

ID	Firewall	Fecha de Validación	Acción	Origen	Destino	Servicio	Tipo	Estado	Info	Sol.	Asoc.
383	ctx1b	06-11-2008	Permitir	if_outside	ANY	udp_al->www	Eliminar	Pendiente de implementar por Admin. FW.	?		
375	ctx1b	06-11-2008	Permitir	if_outside	ANY	udp_al->www	Eliminar	Pendiente de implementar por Admin. FW.	?		
367	ctx1b	06-11-2008	Permitir	Prueba1	10.0.1.29/32	udp_al->tftp	Crear	Implementada pero no sincronizada	?		
370	ctx1b	11-11-2008	Permitir	192.168.7.1/32	ANY	DM_INLINE_TCP_1	Crear	Implementada pero no sincronizada	?		
371	ctx1b	24-11-2008	Permitir	10.0.1.28/32	Prueba1 192.168.3.2/32	icmp_echo-reply	Crear	Pendiente de implementar por Admin. FW.	?		
372	ctx1b	24-11-2008	Denegar	10.0.1.30/32	192.167.1.0/24	ANY	Crear	Implementada pero no sincronizada	?		
373	ctx1b	24-11-2008	Permitir	ANY	10.0.1.30/32	icmp_mobile-redirect icmp_unreachable	Crear	Pendiente de implementar por Admin. FW.	?		
374	ctx1b	24-11-2008	Permitir	10.0.1.29/32	192.168.3.2/32	udp_al->tftp	Crear	Pendiente de implementar por Admin. FW.	?		
396	ctx1b	28-03-2009	Permitir	10.0.1.28/32	192.168.7.1/32	tcp_al->sqnet	Crear	Pendiente de implementar por Admin. FW.	?		

9 elementos encontrados, mostrando todos los elementos
1

Arquitectura de la solución

La solución FWAT esta compuesta de un **Core** que integra el portal y las funcionalidades de la herramienta y de diversos **Plug-Ins** que incorporan la capacidad de comunicarse con los **diferentes fabricantes de cortafuegos**

El Core cuenta de los siguientes módulos:

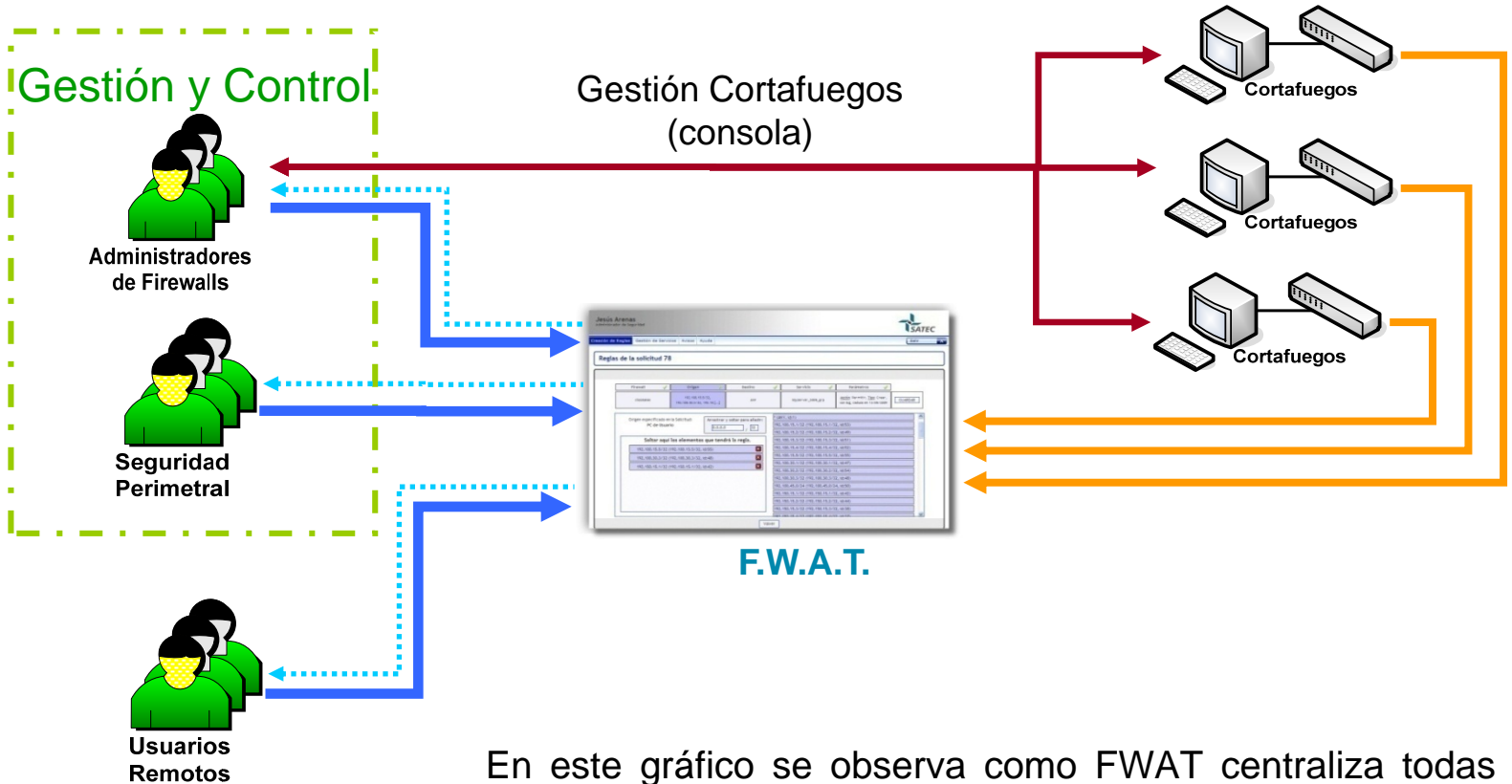
- **Módulo de Gestión:**
 - Lógica del sistema para cada uno de los roles.
- **Módulo de Sincronización:**
 - Análisis de Solicitudes
 - Análisis de reglas implementadas
 - Análisis inteligente de coherencia entre solicitudes e implementación de reglas.
- **Módulo de administración:**
 - Gestión de usuarios del sistema.
 - Configuración de los firewalls.

Plug-Ins de gestión de cortafuegos

- Cisco
- Fortinet
- CheckPoint

SATEC puede desarrollar plug-Ins para otros fabricantes de Cortafuegos. Así como nuevos módulos o funcionalidades para adaptarse a las necesidades de la organización del cliente.

Funcionamiento y gestión de reglas



En este gráfico se observa como FWAT centraliza todas las peticiones y gestiones de apertura de puertos, comprobando las reglas aprobadas con el estado real de los cortafuegos.

Beneficios de FWAT

Usuario Remoto
Usuario Remoto

Solicitudes Salir

Solicitudes

Nueva Solicitud

ID	Fecha de Petición	Origen del acceso	Destino del acceso	Servicio accedido	Validez	Acción solicitada	Estado	+Info
41	28-03-2009	Mi PC	Acceso servidor Oracle s...	Conexion BD Oracle 10	Permanente	Alta	Enviada	?
40	27-03-2009	Mi PC	Maquina de Francisco Gon...	Compartición de ficheros SAMBA	Permanente	Alta	Enviada	?
39	27-03-2009	192.168.10.1	servidor central de base...	SQL	Permanente	Alta	Enviada	?

3 elementos encontrados, mostrando todos los elementos
1

En la **seguridad de la red** de comunicación:


- **Previendo vulnerabilidades** debidas a fallos humanos y de coordinación.
- **Con un único punto de control** permite monitorizar firewalls de diferentes fabricantes dentro de una sola herramienta, y comprobar con mayor sencillez la **coherencia** de sus reglas.
- **Separando los roles** de administrador de seguridad y el administrador de firewalls. Permite una mayor especialización del personal y formaliza los procesos entre ellos.

Beneficios de FWAT


Administrador Seguridad
Administrador de Seguridad

Creación de Reglas Salir

Reglas de la solicitud 42

Firewall 
Sin Seleccionar GUARDAR

Información completa de la Solicitud:

ID	Fecha de Petición	Autor	Origen del acceso	Destino del acceso	Servicio accedido	Acción solicitada	Comentarios	Estado	Validez	+Info
42	28/03/2009	Usuario Remoto	Mi PC	Servidor Base de Datos Oracle. Sede Bilbao	Acceso a BD Oracle 10	Alta		Pendiente de definir reglas	Permanente	

ctx1b Elegir firewall

Volver

En la **flexibilidad** para adaptarse a las necesidades del cliente. La estructura modular de FWAT y la capacidad de desarrollo de SATEC permiten adaptar la solución a los diferentes requisitos de cada organización.

Beneficios de FWAT



Información completa de la solicitud con ID: 42 - Microsoft Internet Expl...

ID	42
Fecha de Petición	28/03/2009
Autor	Usuario Remoto
Origen del acceso	Mi PC
Destino del acceso	Servidor Base de Datos Oracle. Sede Bilbao
Servicio accedido	Acceso a BD Oracle 10
Acción solicitada	Alta
Comentarios	
Estado	Enviada
Validez	Permanente
Ha sido reenviada:	No

Aumentando la productividad, de administradores; y **simplificando** las peticiones a los usuarios

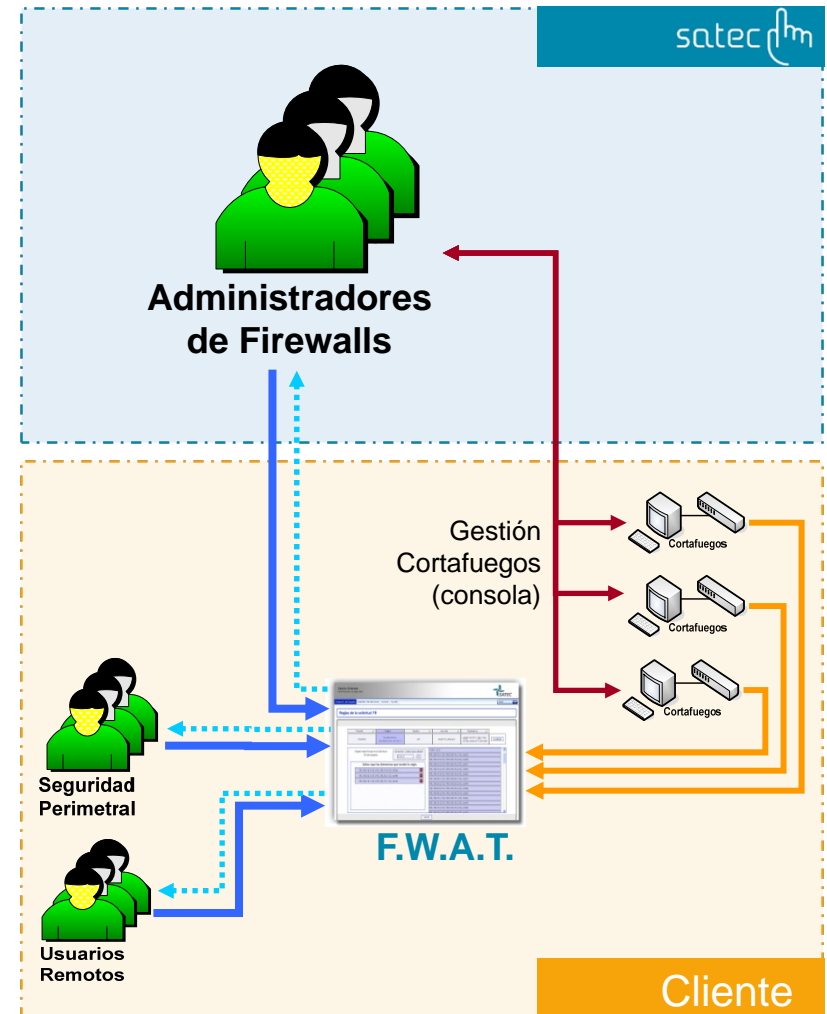
- **Usuarios:** Les suministra formularios, envía notificaciones con las modificaciones en reglas y les permite consultar el estado de sus peticiones.
- **Responsable de seguridad:** Pueden conceder los accesos a la red, monitorizar el estado de las reglas, y recibir notificaciones cuando se produzcan incoherencias con las reglas asignadas y las reglas implementadas.
- **Administrador de los cortafuegos:** Reciben un flujo ordenado de modificación de las reglas, notificaciones indicando cuando deben modificarse éstas; así como una herramienta de mensajería, para facilitar la comunicación con los usuarios.

FWAT / Servicios de explotación para redes y seguridad

FWAT puede combinarse con los **servicios de explotación TIC de Redes y Seguridad**, de SATEC. Permitiendo, de este modo, delegar el rol de administrador de cortafuegos en nuestro personal especializado.

Junto a los beneficios de FWAT este servicio permite:

- Prescindir de los costes de formación del personal en las tecnologías de diferentes fabricantes de cortafuegos.
- Dedicar mas tiempo a la planificación y control de las políticas de seguridad que a su implementación.
- Mayor flexibilidad ante cargas de trabajo variables



- FWAT contribuye a introducir procesos destinados **evitar las vulnerabilidades** en las reglas de acceso a la red.
- FWAT **simplifica el trabajo** del personal del área de seguridad **y facilita las peticiones** a los usuarios.
- FWAT puede **ser modificado, desarrollado o integrado** con otras aplicaciones de modo que se adapte a las necesidades concretas de cada cliente.
- FWAT puede ser **empleado conjuntamente con los servicios gestionados de seguridad**, de SATEC; permitiendo delegar la operación de los cortafuegos.

