



NAC y Gestión de Vulnerabilidades

Luis Herreros Sánchez
lhsanchez@satec.es





Estado del acceso a la red

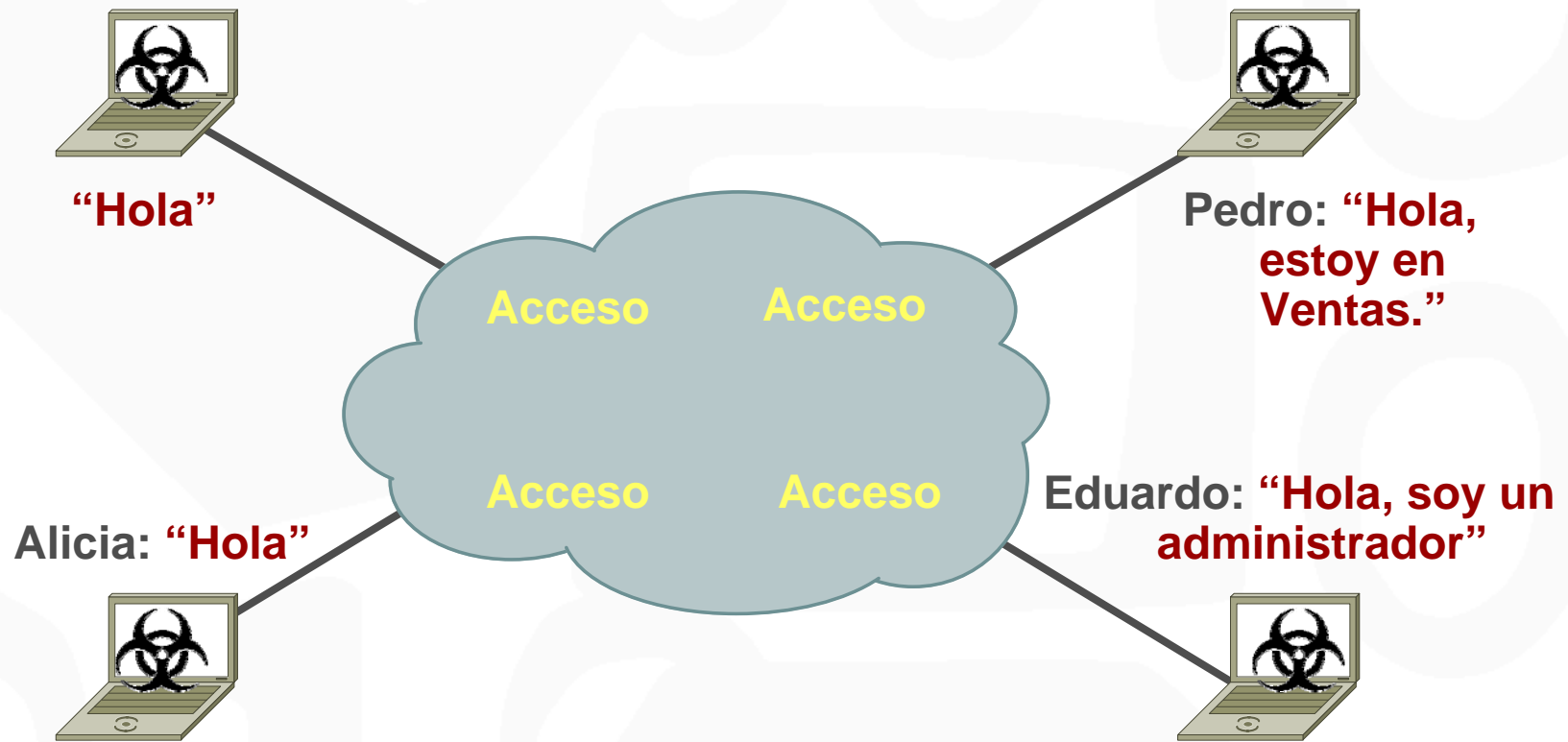


- Situación habitual
 - Acceso estático a la red
 - Todos los dispositivos están permitidos
 - Los dispositivos infectados o no parcheados son a menudo la causa de un problema de seguridad en la organización
- Los dispositivos de acceso insuficientemente protegidos son la causa de la infección y de su transmisión
 - Asegurar que los dispositivos cumplen con la política de seguridad (herramientas, actualizaciones, etc ...) es difícil y caro de mantener.



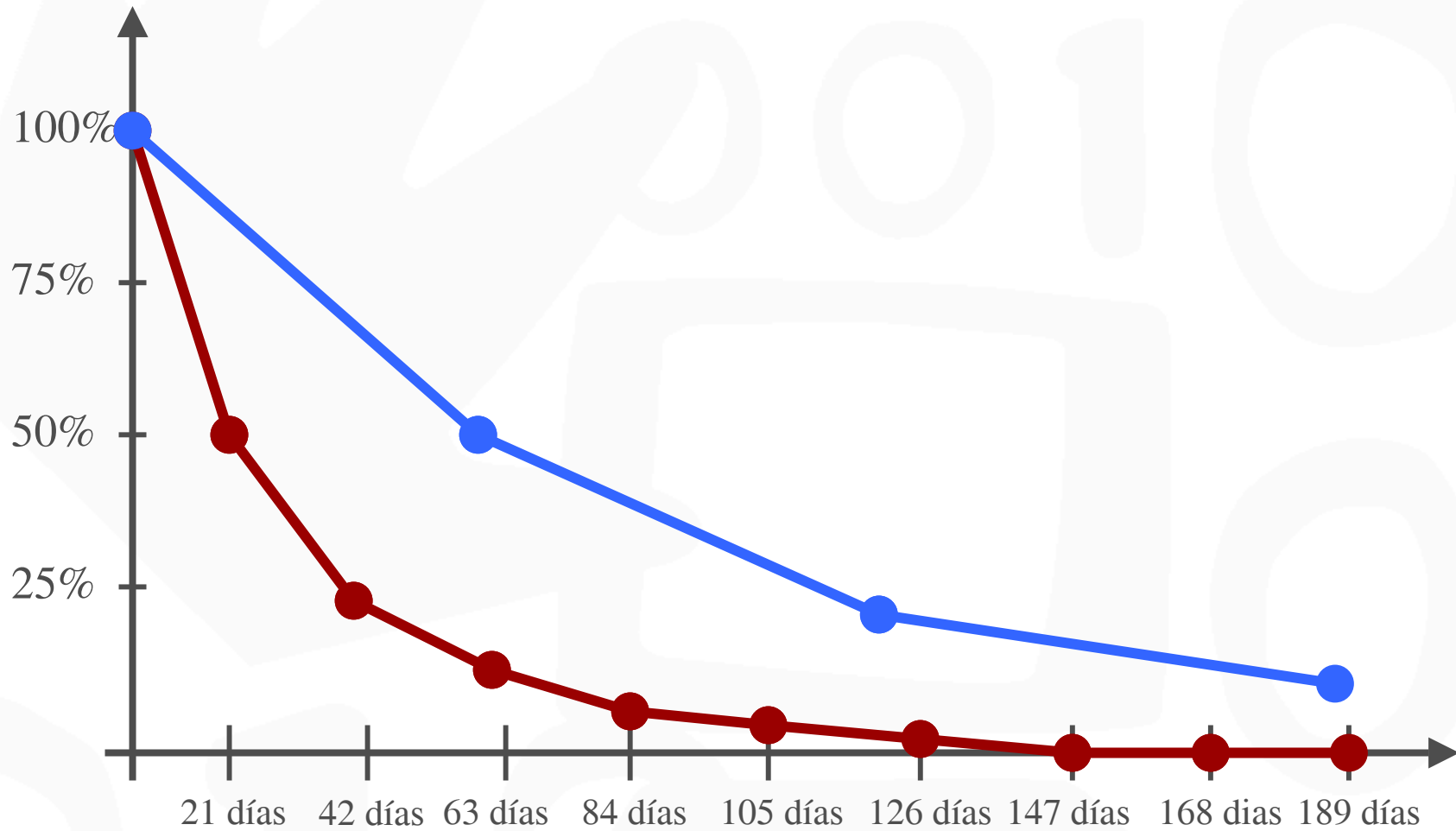
Antes de los mecanismos de control de acceso

Pedro: “Estoy en un sistema sin actualizar, infectado con el ultimo virus y ni siquiera se que lo estoy”





Evolución de vulnerabilidades internas vs externas





Evolución del acceso a la red

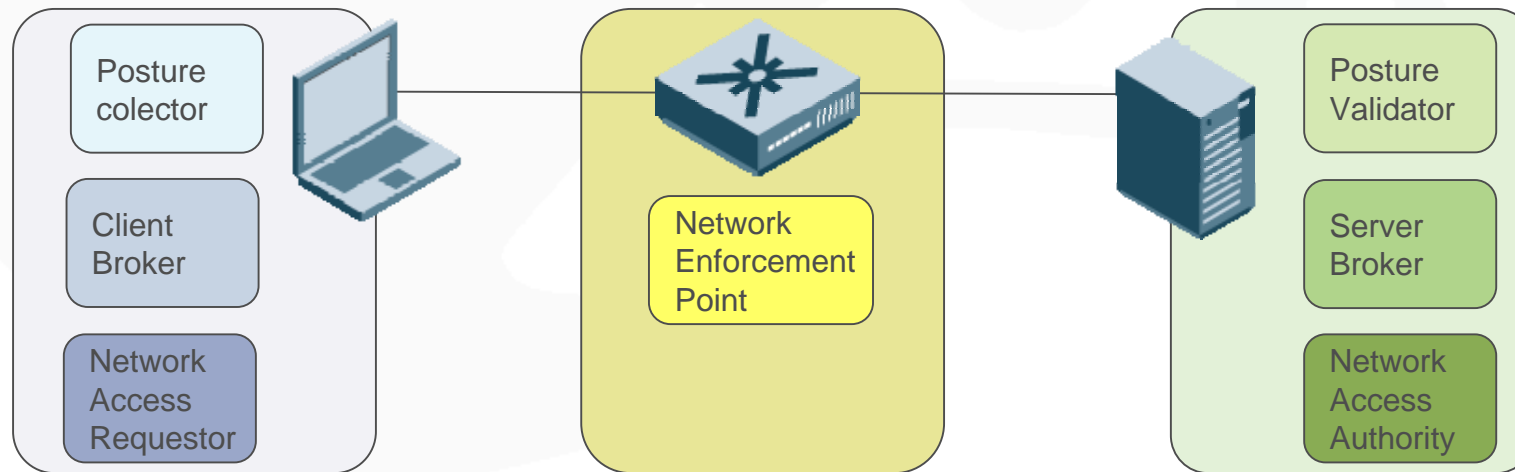
- En la actualidad
 - Acceso dinámico a la red basado en políticas
 - Se evalúan los dispositivos antes de permitirles acceder a la red
 - Los dispositivos infectados o no parcheados se aíslan y tratan con recursos dedicados (servidores)
- Objetivo de NAC: Eliminar la existencia de vulnerabilidades críticas rápidamente. Focalizado en prevención
 - Una solución a nivel de red permite alcanzar todos los dispositivos/aplicaciones
 - Permite reutilizar los elementos ya existentes en la red para reforzar la seguridad
 - Comprueba la identidad del usuario y el dispositivo desde el que accede





Componentes de una solución NAC

¿Qué es?
Posture collector: Software de terceros que corre en el cliente y recolecta información sobre el estado de la seguridad del cliente y de las aplicaciones que corren en él como antivirus activado y actualizado.
Client Broker: "Middleware" que corre en el cliente y habla con el Posture Collector, recogiendo sus datos y pasándoselos al Network Access Requestor
Network Access Requestor: Software que conecta el cliente a la red como por ejemplo un suplicante 802.1x o un cliente IPSEC. Se usa para autenticar al usuario



¿Qué es?
Network Enforcement Point Componente de la infraestructura de red que refuerza la política de seguridad como por ejemplo un switch compatible 802.1x, un firewall o un terminador de VPN.
Posture Validator Software de terceros que recibe la información de estado del Posture Collector y valida la misma contra la política de red configurada
Server Broker "Middleware" que actúa como interface entre los Posture Validators y el Network Access Authority
Network Access Authority Servidor encargado de validar la autenticación y la postura (estado) del cliente. Pasará la política resultante de esta evaluación al Network Enforcement Point.

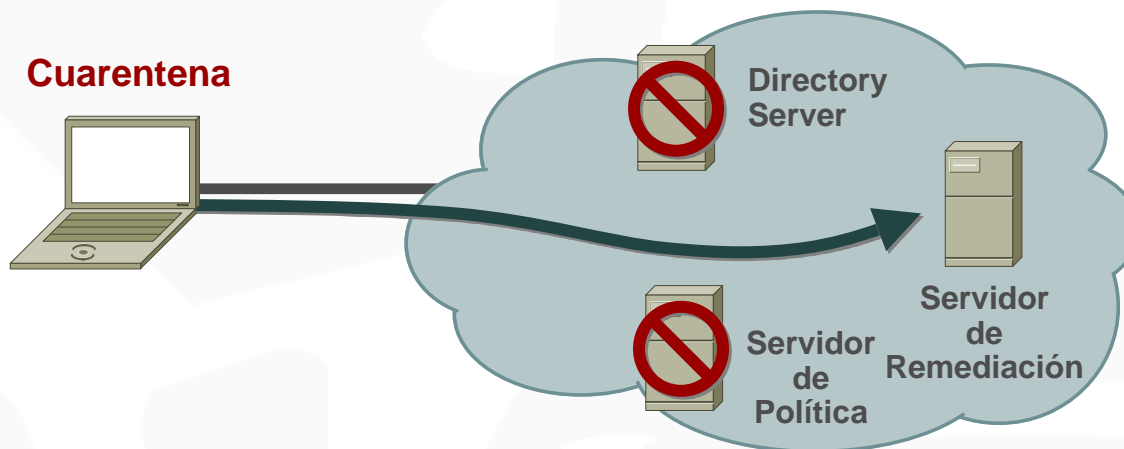


La gestión de accesos con un sistema NAC

Pedro: Dpto. Ventas
Windows 2000
Sin Service Pack
Sin Anti-Virus
Sin Gestión de Parches

Política de Admisión:

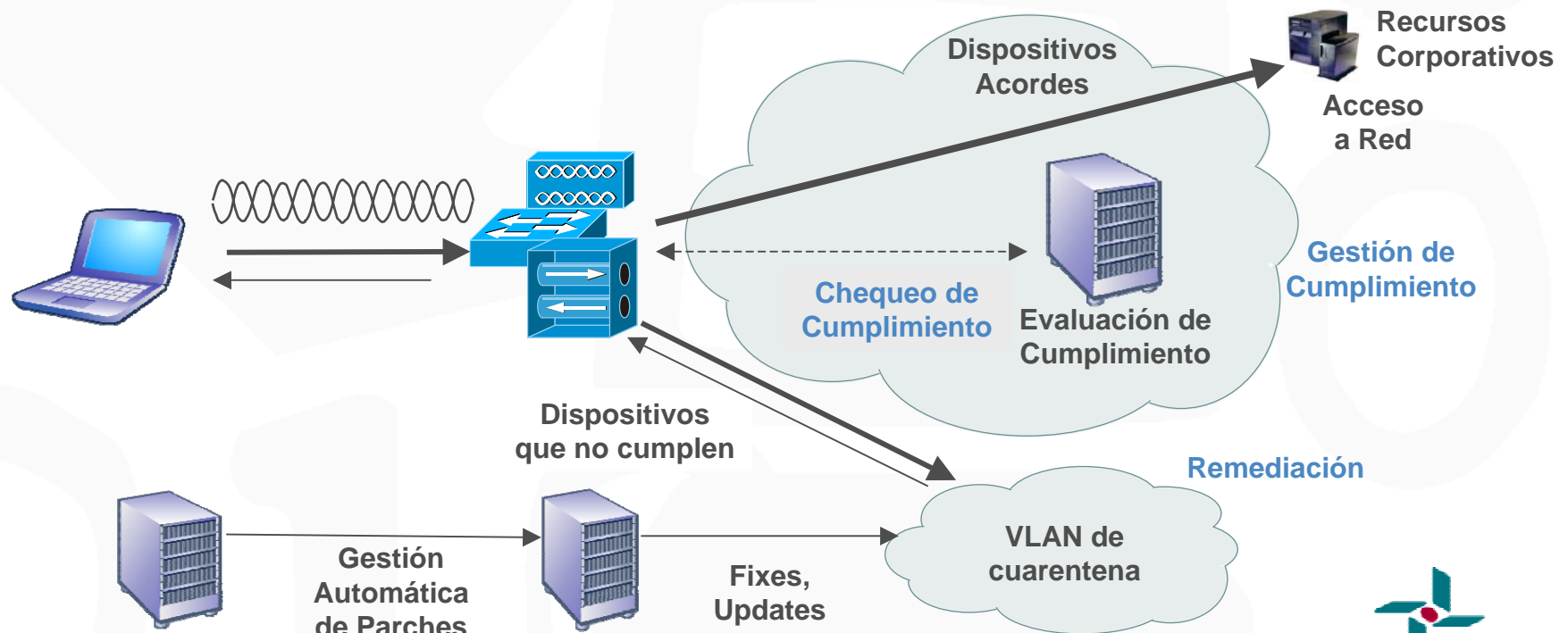
1. Identidad
2. Windows XP
3. Service Pack 2
4. Anti-Virus
5. Gestión de Parches





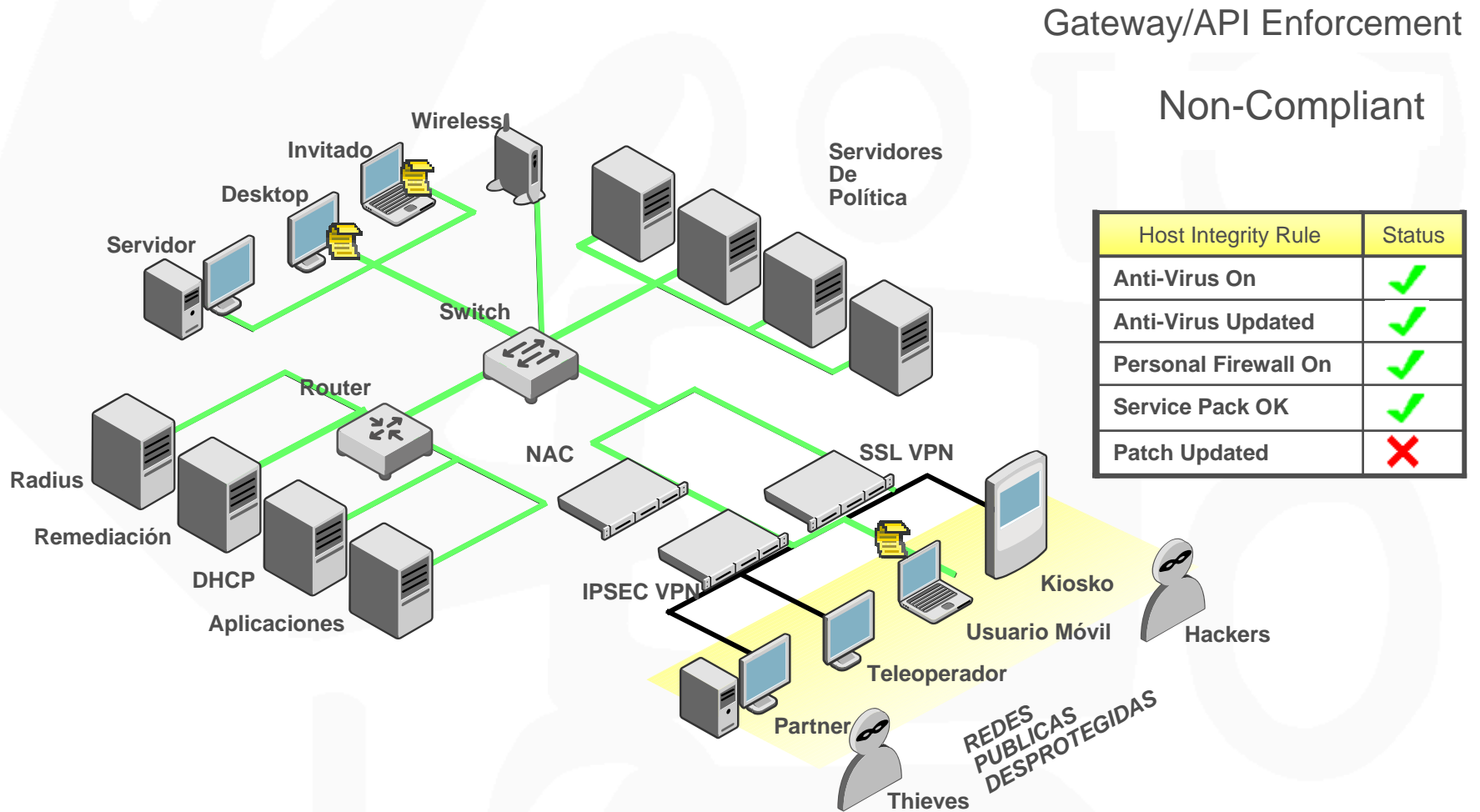
Ventajas de una solución NAC

- Las decisiones de admisión a la red son efectivas porque inspeccionan y comprueban en el momento del ingreso, con una enorme flexibilidad en los criterios de control
- Se evalúa que es necesario? Que esta permitido? ... y demas cosas que se puedan encontrar



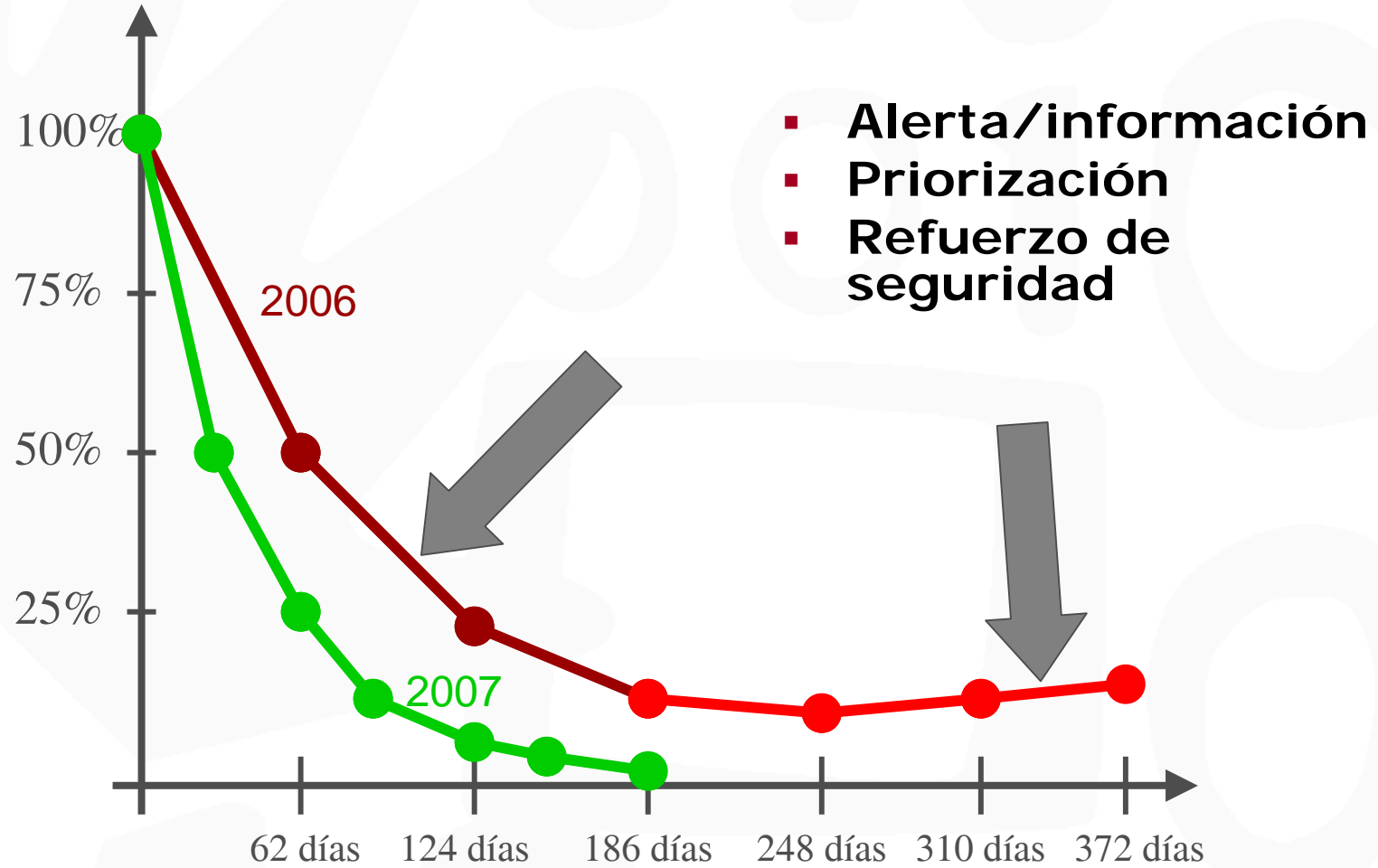


Diferentes escenarios





Vulnerabilidades en la red interna





Gestión de Vulnerabilidades



- Inventario dinámico
- Control de la instalación
- Gestión de configuraciones
- Cumplimiento de normativas



Conclusiones

Aumenta el estado de la seguridad

- Asegura los endpoints (laptops, PCs, PDAs, servidores, etc.) conforme a la política de seguridad
- Protección proactiva contra gusanos, virus, spyware y malware
- Focaliza las operaciones en "Que es necesario"

Incrementa la resistencia de la empresa

- Proporciona una mejor comprensión del acceso a través de todos los métodos de ingreso a la red (LAN, WAN, Wireless, VPN, etc.)
- Previene de las máquinas que no cumplen la política y el uso de la red por parte de elementos no controlados
- Reduce el tiempo de riesgos por ataques "Zero-day"



Muchas gracias

“Ser vulnerable es estar en desventaja ante determinadas situaciones”

Luis Herreros Sánchez
lhsanchez@satec.es