

En muchas operaciones reales, es posible que no se pueda tener acceso físico a los sistemas objetivo del propio país y que sea necesaria la **instalación remota encubierta** de una solución de monitoreo remoto para poder **monitorear el objetivo desde dentro de la sede central de la agencia gubernamental**.

FinFly ISP es una solución (móvil) **estratégica y táctica de escala nacional** que se puede **integrar en la red de núcleo y/o de acceso de un proveedor de servicios de Internet** para instalar de forma remota la solución de monitorización remota en los sistemas objetivo seleccionados.

Los componentes de FinFly ISP se basan en la **tecnología de servidores de nivel de operador** y proporcionan la máxima **fiabilidad y escalabilidad** para hacer frente a casi cualquier reto relacionado con las topologías de redes. Hay una gran variedad de interfaces de red disponibles, todas ellas **protegidas con funciones de omisión**, para la conectividad de red activa.

Los múltiples métodos, activos y pasivos, de identificación de objetivos, **desde la monitorización en línea** mediante interceptación pasiva hasta la **comunicación interactiva** entre FinFly ISP y los servidores AAA, garantizan la identificación de todos los objetivos y el suministro de canales adecuados para el proceso de infección.

### Descripción General De Funciones

- Se puede instalar dentro de la **red de un proveedor de servicios de Internet**.
- Es compatible con **todos los protocolos más comunes**
- Selecciona e identifica los objetivos por **su dirección IP o el nombre de inicio de sesión de RADIUS**
- Oculta la solución de monitorización remota en las **descargas de los objetivos**.
- Disfraza la solución de monitorización en forma de **actualizaciones de software**.
- Instala de forma remota soluciones de monitorización remota a través de los sitios **Web que visita el objetivo**.

Encontrará la lista completa de funciones en las Especificaciones del producto.

DE UN VISTAZO	
Uso:	Operaciones estratégicas
Capacidades:	Implementa una solución de monitorización remota en el sistema objetivo a través de una red ISP
Contenido:	Hardware/Software

FinFly ISP puede **infectar archivos** descargados por el objetivo **en tiempo real**, o infectar el sistema objetivo **enviando falsas actualizaciones** de aplicaciones de software populares. La nueva versión integra la potente aplicación de infección remota de Gamma **FinFly Web** para que los objetivos se infecten en tiempo real con solo **visitar cualquier sitio Web**.

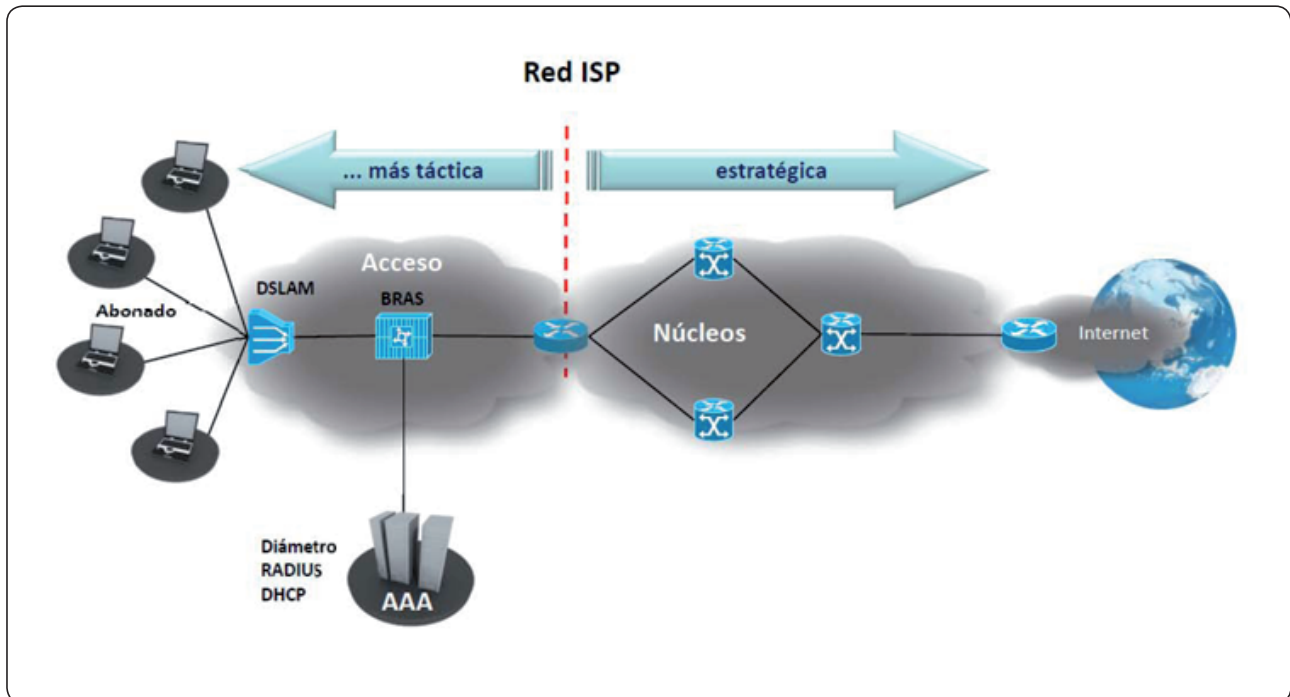
### Ejemplo De Uso: Agencia De Inteligencia

FinFly ISP se implementó en las redes del principal proveedor de servicios de Internet del país y se usó activamente para implementar de forma remota una solución de monitorización remota en los sistemas objetivo. Dado que los objetivos tienen conexiones DSL con IP dinámica, se identifican mediante su nombre de inicio de sesión de RADIUS



### Varias posibilidades de ubicación

- FinFly ISP se puede utilizar como solución táctica o estratégica en redes ISP



Una solución táctica es de naturaleza móvil, y el hardware se dedica a las tareas de infección dentro de la red de acceso, cerca de los puntos de acceso de los objetivos. Se puede implementar a corto plazo para satisfacer requisitos tácticos centrados en un objetivo específico o un número reducido de objetivos en un área determinada.

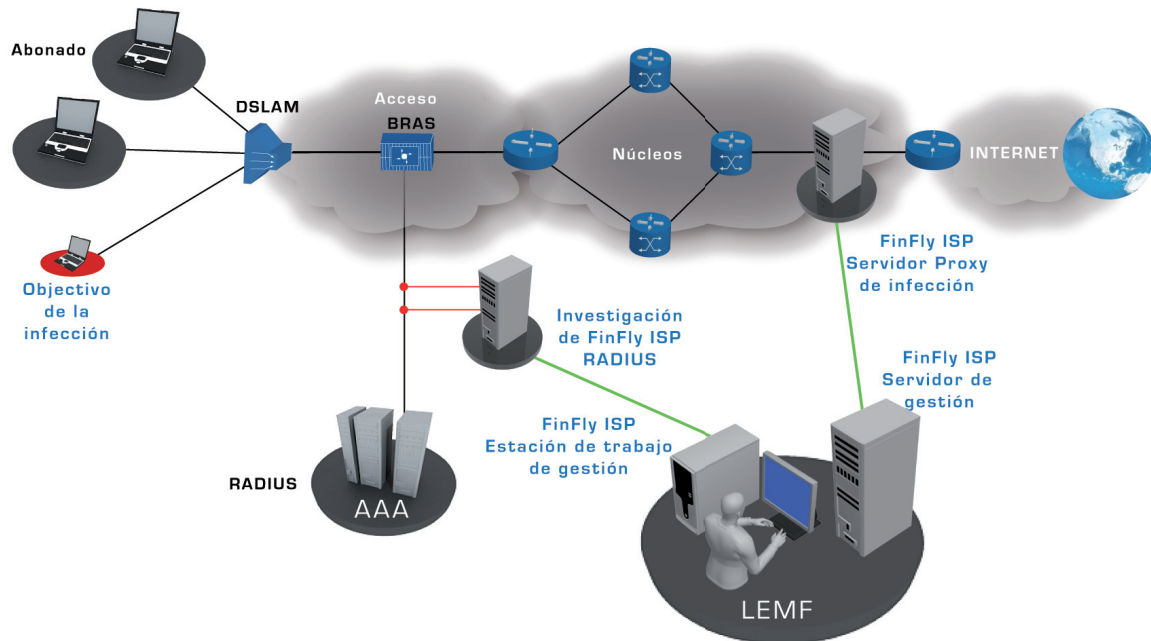
Una solución estratégica sería, por el contrario, permanente. La instalación de FinFly ISP en los sistemas de un

proveedor de servicios de Internet o a escala de todo el país permite identificar e infectar de forma remota cualquier objetivo desde la sede central de la agencia gubernamental sin necesidad de que las fuerzas y cuerpos de seguridad se desplacen al lugar en cuestión.

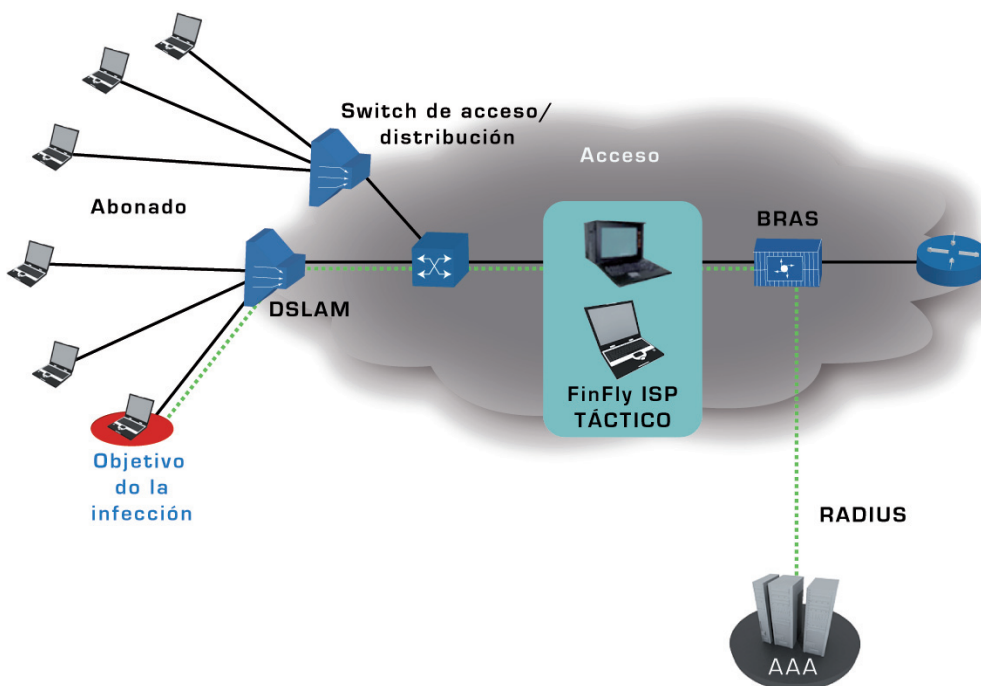
Evidentemente, es posible combinar soluciones tácticas y estratégicas para otorgar la máxima flexibilidad posible a las operaciones de infección.

### Configuración de la red

#### Implementación estratégica



#### Implementación táctica



## Componentes Del Producto

**FinFly ISP Estratégico**

Una implementación estratégica de FinFly ISP consta al menos de lo siguiente:

- Sistema de administración en el LEMF
- Servidor(es) de identificación de objetivo en el sistema AAA de la red
- Servidor(es) proxy de infección en la(s) puerta(s) de enlace de Internet, por ejemplo

Servidores FinFly ISP  
Estación de trabajo  
HP ProLiant Serie DL G7  
Estación de trabajo  
profesional



FinFly ISP  
HP Serie Z



<b>Capacidad de proceso</b>	> 20 Gbps
<b>Nº máx. de NIC:</b>	2-8 NIC
<b>Interfaces:</b>	1 GE Cobre / Fibra <b>10 GE Cobre / Fibra</b> <b>SONET/SDH OC-3 / -192</b> <b>STM-1 / -64</b> <b>ATM AAL5</b>
<b>Procesadores:</b>	De 1 a 8 Intel XEON
<b>Núcleos</b>	2 – 8 núcleos / procesador
<b>RAM:</b>	12 GB – 1 TB
<b>Capacidad de disco duro:</b>	3 SAS de 146 GB – 4,8 TB
<b>Características</b>	HP iLO 3 <b>Alimentación redundante</b> <b>Ventiladores redundantes</b> <b>Función de conmutación de derivación (si existe)</b>
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforzado

**FinFly ISP Táctico**

Un sistema FinFly ISP táctico consta de lo siguiente:

- Servidor proxy portátil de identificación de objetivos e infección
- Ordenador portátil del sistema de gestión

FinFly ISP Táctico  
Gestión portátil  
Atlas A9 17" Portable



FinFly ISP Táctico  
Lenovo Thinkpad  
Serie T



<b>Capacidad de proceso</b>	5 Gbps
<b>Nº máx. de NIC:</b>	3 NIC
<b>Interfaces:</b>	1GE Cobre / Fibra <b>SONET/SDH OC-3 / -12</b> <b>STM-1 / -4</b> <b>ATM AAL5</b>
<b>Procesadores:</b>	2 Intel Core i7
<b>Núcleos</b>	6 núcleos / procesador
<b>RAM:</b>	12 GB
<b>Capacidad de disco duro:</b>	2 SATA de 1 TB
<b>Unidad óptica</b>	DVD+/-RW SATA
<b>Monitor</b>	1 TFT de 17"
<b>Características</b>	Función de conmutación de derivación para NIC
<b>Sistema operativo</b>	Linux GNU (Debian 5.0) reforzado

Los datos técnicos y las especificaciones están sujetos a cambios sin previo aviso.