

In many real-life operations, physical access to in-country Target Systems cannot be achieved and covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within the Headquarters**.

FinFly ISP is a strategic, **countrywide, as well as a tactical** (mobile) solution that can be **integrated into an ISP's Access and/or Core Network** to remotely install the Remote Monitoring Solution on selected Target Systems.

FinFly ISP appliances are based on **carrier grade server technology**, providing the maximum **reliability and scalability** to meet almost every challenge related to network topologies. A wide-range of Network Interfaces – all **secured with bypass functions** – are available for the required active network connectivity.

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communications** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic is provided for the infection process.

FinFly ISP is able to **infect Files** that are downloaded by the Target **on-the-fly** or infect the Target by **sending fake Software Updates** for popular Software. The new release now integrates Gamma's powerful remote infection application **FinFly Web** to infect Targets on-the-fly by just **visiting any website**.

Feature Overview

- Can be installed inside the **Internet Service Provider Network**
- Handles **all common Protocols**
- Selected Targets by **IP address or Radius Logon Name**
- Hides Remote Monitoring Solution in **Downloads by Targets**
- Injects Remote Monitoring Solution as **Software Updates**
- Remotely installs Remote Monitoring Solution through **Websites visited by the Target**

For a full feature list please refer to the Product Specifications.

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through ISP Network
Content:	· Hardware/Software

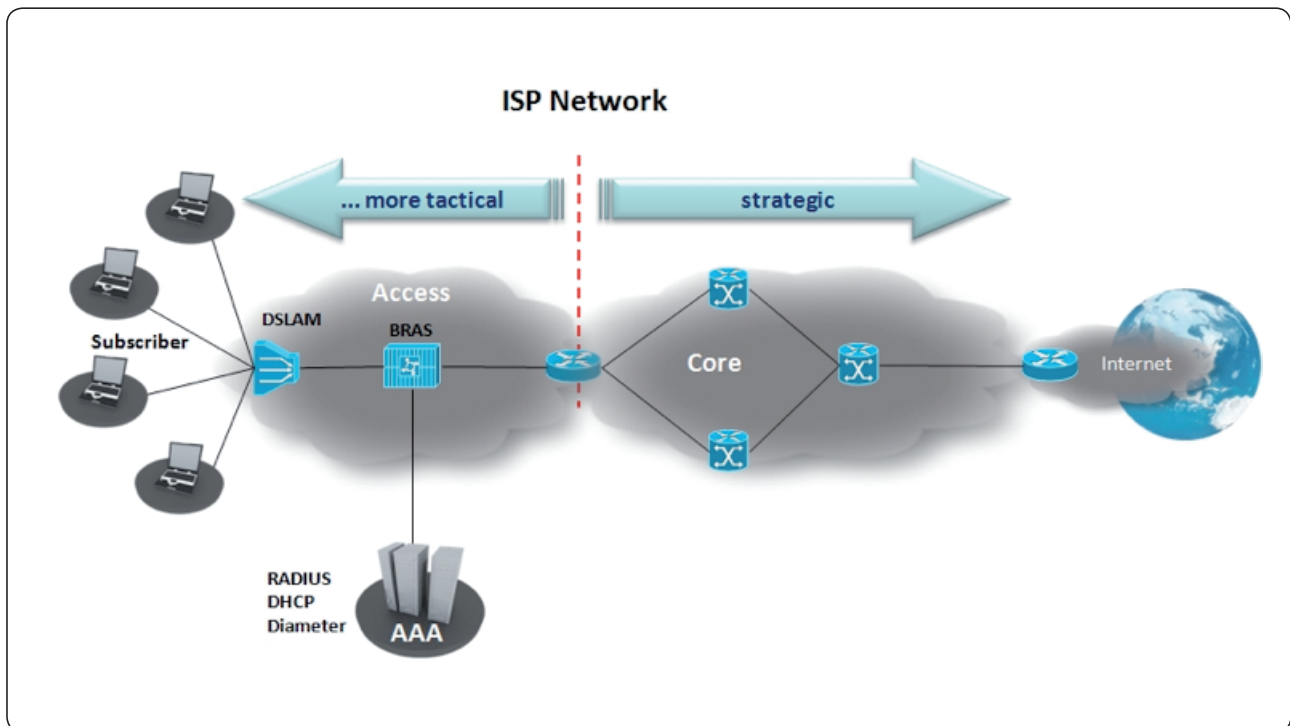
Usage Example: Intelligence Agency

FinFly ISP was deployed in the main Internet Service Provider networks of the country and was actively used to remotely deploy a Remote Monitoring Solution on Target Systems. As the Targets have Dynamic-IP DSL Accounts, they are identified with their Radius Logon Name.



Different Location Possibilities

- FinFly ISP can be used as a tactical or strategic solution within ISP networks



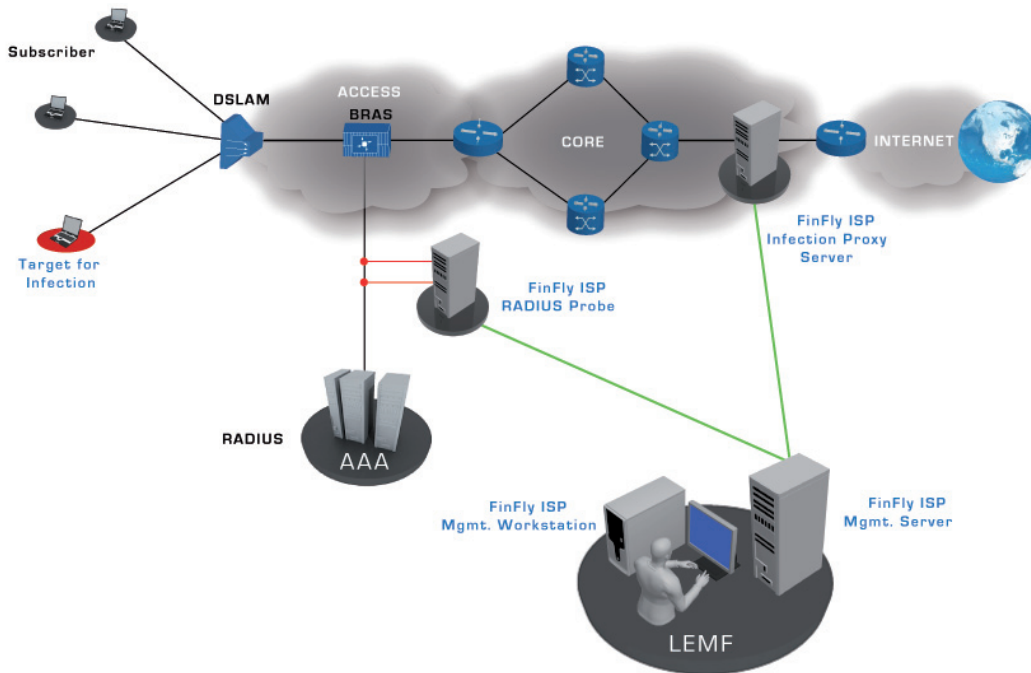
A tactical solution is mobile and the hardware is dedicated to the infection tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical requirements focused on either a specific target or a small number of targets in an area.

A strategic solution would be a permanent ISP/countrywide installation of FinFly ISP to select and infect any target from the remote headquarters without the need for the LEA to be on location.

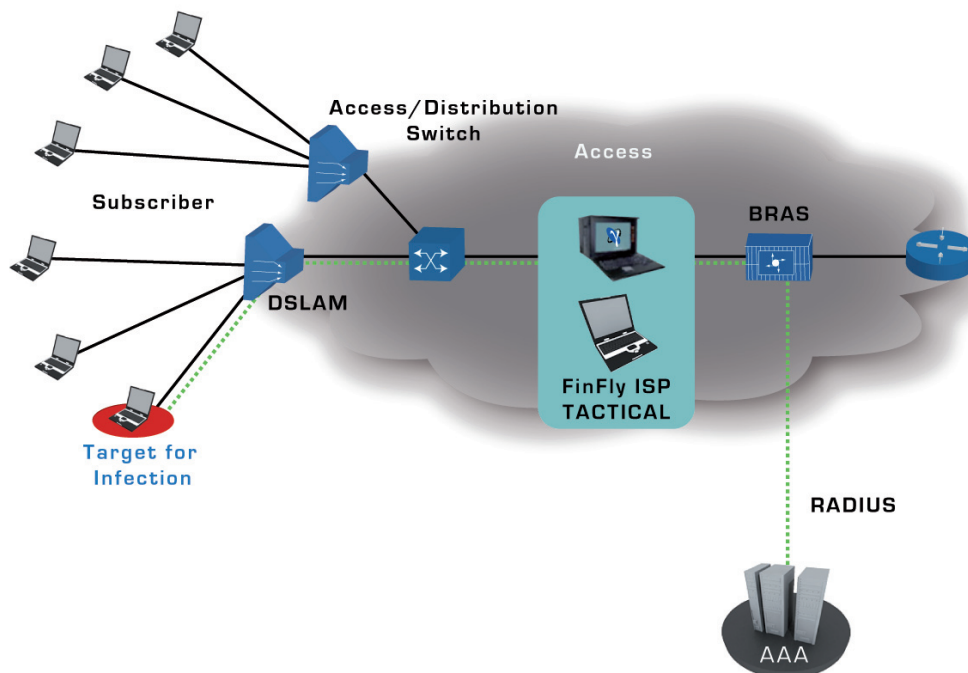
Of course, it is possible to combine tactical and strategic solutions to reach a maximum of flexibility for the infection operations.

Network Setup

Strategic Deployment



Tactical Deployment



Product Components

FinFly ISP Strategic

A strategic deployment of FinFly ISP consists at least of the following:

- Management System at the LEMF
- Target Identification Probe Server(s) at the AAA-System of the network
- Infection Proxy Server(s) at, for example, the Internet Gateway(s)

FinFly ISP Servers Workstation

HP ProLiant DL-Series G7 Business WS



FinFly ISP HP Z-Series



Throughput: > 20 Gbps

Max. no. of NICs: 2 - 8 NICs

Interfaces: 1GE Copper / Fiber
10GE Copper / Fiber
SONET / SDH OC-3 / -192
STM-1 / -64
ATM AAL5

Processors: 1x – 8x Intel XEON

Core: 2 - 8 Cores / Processor

RAM: 12GB -1TB

HDD Capacity: 3 x 146GB - 4.8TB SAS

Features: HP iLO 3
Redundant Power
Redundant Fans
Bypass Switch Function (if applicable)

Operating System: Linux GNU (Debian 5.0) hardened

FinFly ISP Tactical

A tactical FinFly ISP System consists of the following:

- Target Identification & Infection Proxy Server Portable
- Management System Notebook

FinFly ISP Tactical Portable Mgmt.

Atlas A9 17" Portable



FinFly ISP Tactical

Lenovo Thinkpad T-Series



Throughput: 5 Gbps

Max. no. of NICs: 3 NICs

Interfaces: 1GE Copper / Fiber
SONET / SDH OC-3 / -12
STM-1 / -4
ATM AAL5

Processors: 2 x Intel Core i7

Core: 6 Cores / Processor

RAM: 12GB

HDD Capacity: 2 x 1TB SATA

Optical Drive: DVD+/-RW SATA

Monitor: 1 x 17" TFT

Features: Bypass Switch Function for NICs

Operating System: Linux GNU (Debian 5.0) hardened

The technical data /specifications are subject to change without notice.