

# FORTHcert

Foundation for Research  
and Technology – Hellas  
Institute of Computer Science

**31<sup>st</sup> TF-CSIRT Meeting**

September 2010 - Istanbul, Turkey



Internet-Sicherheit  
fördern – kritische  
Infrastrukturen schützen

# Overview

- Updates from FORTHcert
- Staff Exchange
- Updates from CERT.at

# Profile



- Established in June 2007
- FORTHcert team operates within the Department of Systems and Networks of FORTH – ICS
- Authorized to use CERT, Jul 2008  
Accredited by TI/CSIRT, Jan 2009  
Accredited by FIRST, May 2009
- 2 person dedicated staff  
3 part time network specialists  
2 part time system engineers

# Constituency

- FORTH community
- Academic institutions
- Government organizations
- Banking industry
- Private sector
- .gr Registrars

# Activities

- Incidence analysis & Vulnerability handling
- Information dissemination
- Awareness building
- Vulnerability assessment
- Penetration testing
- Artifact handling
- EWIS (Early Warning Intrusion System)

# EWIS - CONCEPTS

- An IDS based on a wide network of sensors
- Sensors (appliances) to be deployed to an assortment of medium and large organizations on a national or even international level
- To establish a trend of intrusion traffic at a large scale
- To predict upcoming attacks and issue alerts when necessary
- To built a weathermap of intrusion statistics

# EWIS - SENSOR

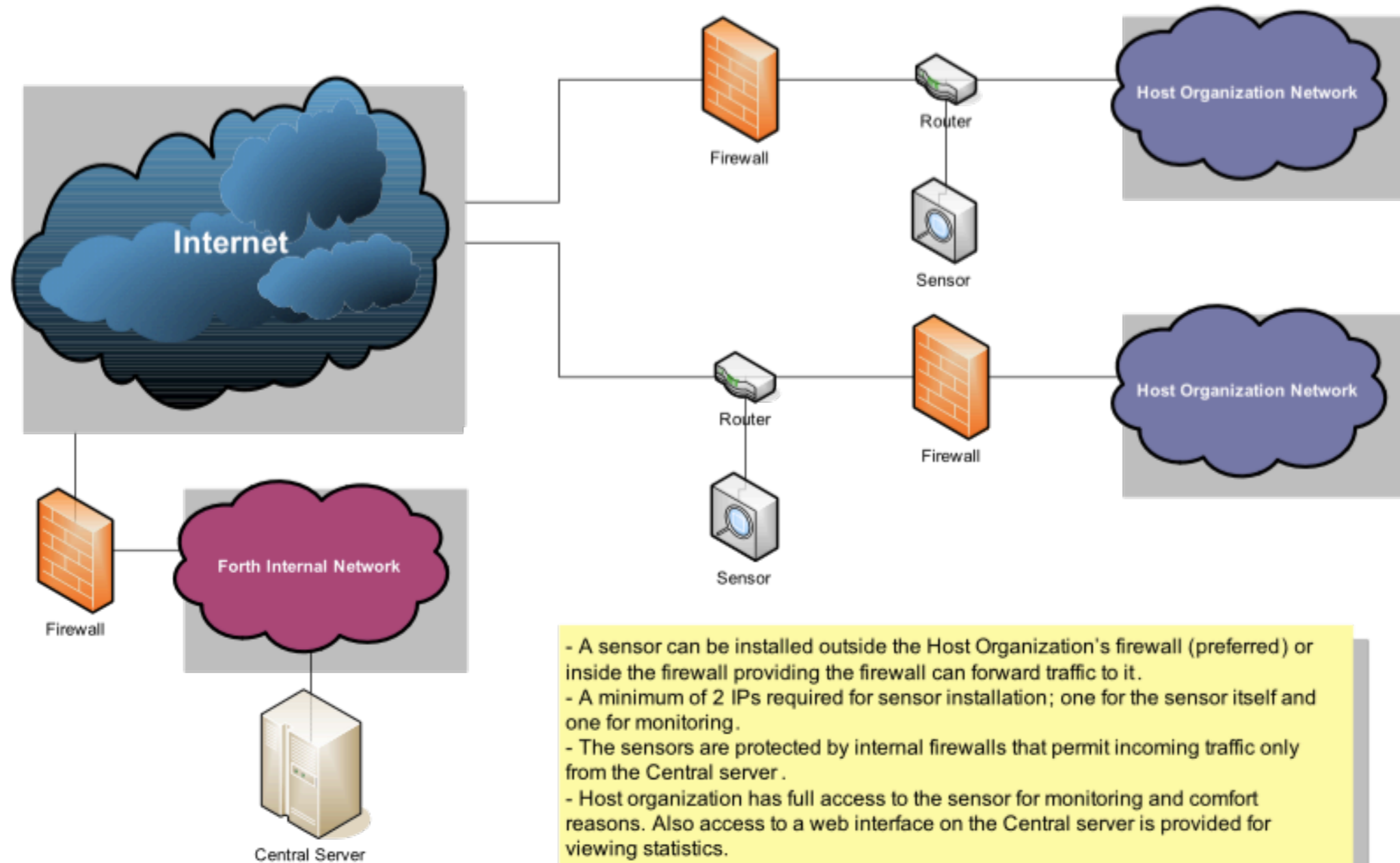
- Linux based appliance on generic hardware
- Non intrusive installation and hardened OS
- Passive darknet logging assures no hosting organization information is stored on the device
- Communicates statistics back to a central site via a secure encrypted tunnel
- Functionality was implemented in-house and based on research done internally at the ICS

# EWIS - CENTRAL SITE



- Accepts statistics from remote sensors and logs them to central database
- Presents custom (per client) statistics via a secured web interface
- A sensor management interface will be running here in the near future
- Alerts will be issued to FORTHcert subscribed clients
- Programming was done in-house and also based on research work done by the ICS

# EWIS - ARCHITECTURE



- A sensor can be installed outside the Host Organization's firewall (preferred) or inside the firewall providing the firewall can forward traffic to it.
- A minimum of 2 IPs required for sensor installation; one for the sensor itself and one for monitoring.
- The sensors are protected by internal firewalls that permit incoming traffic only from the Central server .
- Host organization has full access to the sensor for monitoring and comfort reasons. Also access to a web interface on the Central server is provided for viewing statistics.
- Each sensor pushes data to the server through an SSL tunnel on timely intervals .
- The Central server processes and stores data on a database for further analysis and presentation.

# Contacts



- <http://www.forth.gr/forthcert/>, [cert@forth.gr](mailto:cert@forth.gr)
- **Demos Panagopoulos** - *Department of System and Networks*  
Tel: +30 2810391640 , [dimos@ics.forth.gr](mailto:dimos@ics.forth.gr)
- **Dimitra Vitsa** - *Department of System and Networks*  
Tel: +30 2810391463 , [dvitsa@ics.forth.gr](mailto:dvitsa@ics.forth.gr)
- **Panos Chatziadam** - *Department of System and Networks*  
Tel: +30 2810391443 , [panosc@ics.forth.gr](mailto:panosc@ics.forth.gr)
- **Vaggelis Segredakis** - *Administration of .GR Top Level Domain*  
Tel: +30 2810391450 , [segred@ics.forth.gr](mailto:segred@ics.forth.gr)

# Staff Exchange

- Idea of a staff exchange by .GR registry
- May 2010: A. Kaplan went to Heraklion
- FORTH Cert  $\leftrightarrow$  CERT.at learn each other's tools and tricks.
- Panos Chatziadam will go to Vienna

# Results of staff exchange

1/2



- Discussed ideas and future considerations for enhancing the EWIS sensor network
- Implemented enhancements to the database structure and functionality
- Began to work on a port of the data as Netflow format output so tools such as NFSen / NFDump or Carmentis can be used to analyze the data (-> thx P. Haag!)
- Discussed interfacing EWIS with other IDS created by other CERTs

# Results of staff exchange

2/2



- Discussed using the ASN number for automated AS abuse notification
- Considered and tested visualization tools for better visual representation of the collected data
- Enjoyed the Cretan countryside, wine, olive oil and Mediterranean cuisine :-)
- Planned for a FORTHcert member to visit Austria and continue cooperation

# EWIS - TO DO LIST

- Expand the network further by installing more sensors
- Interface with other IDS systems and exchange data
- Interface with the RIPE and BGP database for ASN lookup (AS identification for aggregating & alerting)
- Use Netflow tools to analyze data
- Anomaly detection and Alerting
- Enhance the statistics interface, streamline the sensor management process and tune the server and database for performance

# EWIS Viz





# Updates from CERT.at



- New MiniBis
- Passive DNS

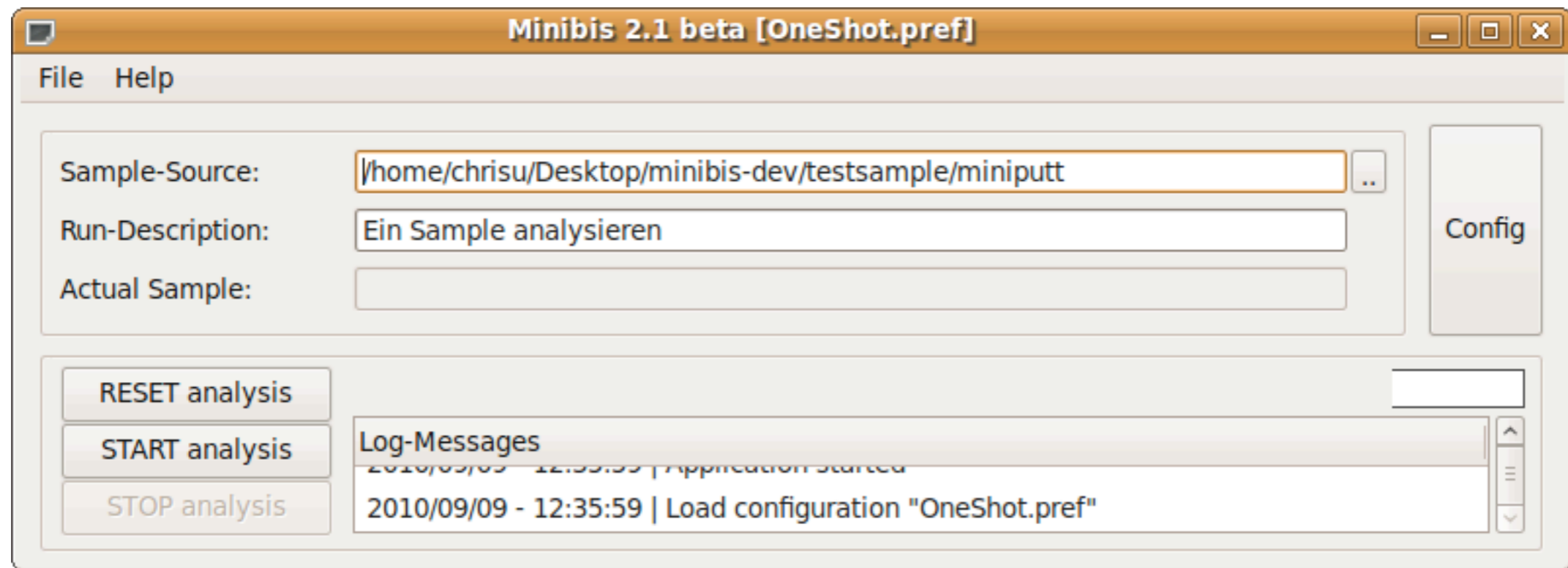
# Minibis 2.1

- Idea: “mini Anubis” – mass malware Analysis
- Runs on Linux and Windows
- New features:
  - define profiles for execution of DLLs, .EXEs, .URLs , SWF etc
  - better filesystem structure for results
  - Everything now works with cmd line params. GUI is now only a profile file generator
- Next version:
  - Parallelization & Workload distribution
  - other VMs (not only VBox)
- Follow [http://twitter.com/CERTat\\_Minibis](http://twitter.com/CERTat_Minibis)

# Minibis 2.1



# Minibis 2.1



# Minibis 2.1

**MINIBIS - Configuration**

General Settings | Researcher Scripting | Proband Scripting | Sample-Types

Results

Directory:

Researcher-Proband-Communications:

Counter-Detection:

Virtual Machine Management

Virtual Machine Solution:  Virtual Machine Instance:

Command to Start Virtual Machine Instance:  Timeout (s):

Command to Stop Virtual Machine Instance:  Timeout (s):

Command to Revert Virtual Machine Instance:  Timeout (s):

Bugfixes for Virtual Box Commandline Client

Killall -9 VBoxSVC      Killall -9 VBoxXPCOMIPCD      Killall -9 VirtualBox

# Minibis 2.1

**MINIBIS - Configuration**

General Settings | **Researcher Scripting** | Proband Scripting | Sample-Types

Actions BEFORE Proband gets started:

Actions WHILE Proband runs: every:  s

Actions AFTER Proband got stopped:  After zipping

# Minibis 2.1

**MINIBIS - Configuration**

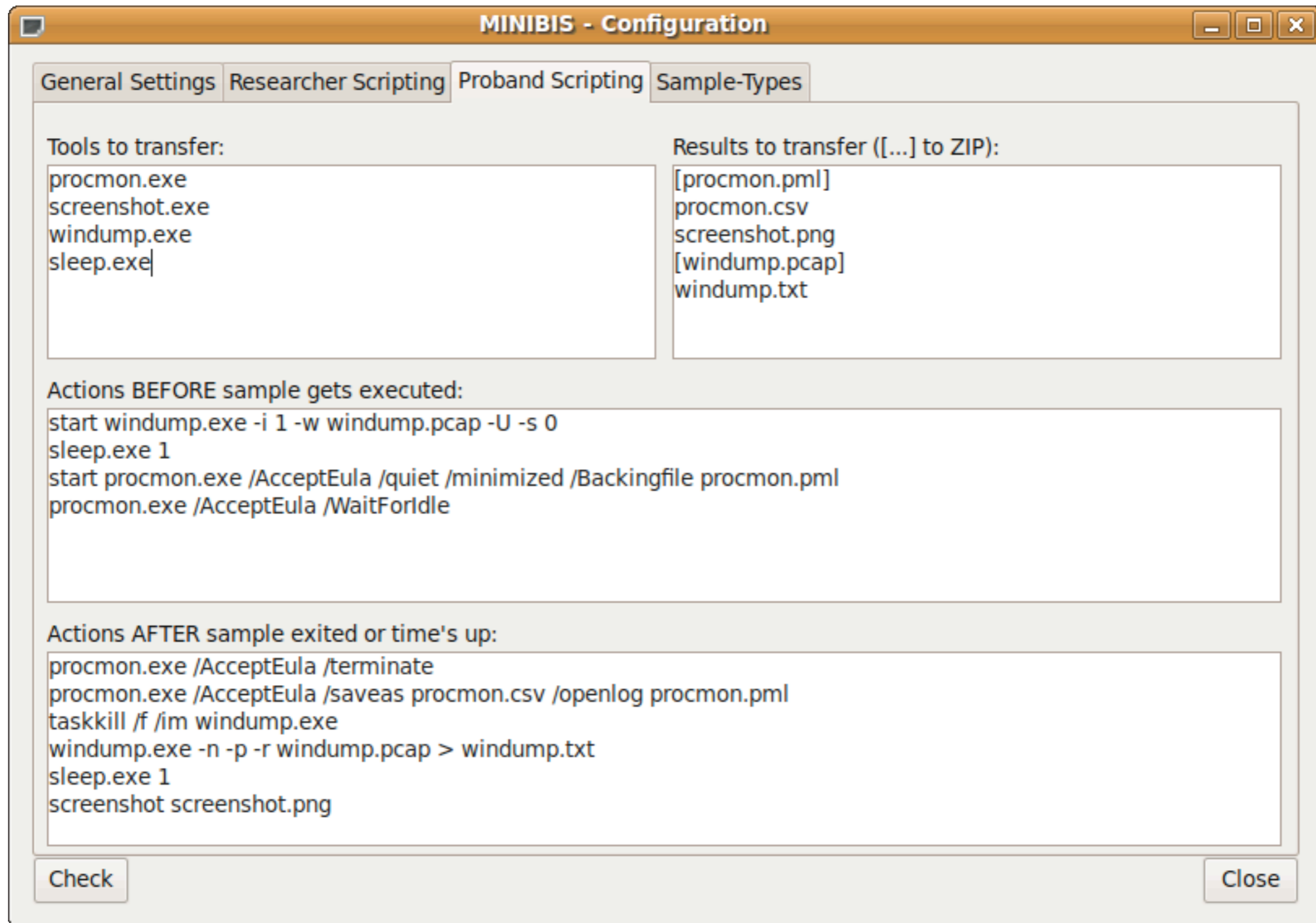
General Settings | **Researcher Scripting** | Proband Scripting | Sample-Types

Actions BEFORE Proband gets started:

Actions WHILE Proband runs: every:  s

Actions AFTER Proband got stopped:  After zipping

# Minibis 2.1



# Minibis 2.1

**MINIBIS - Configuration**

General Settings | Researcher Scripting | Proband Scripting | **Sample-Types**

Select Sample-Type

Type-Name

- exe
- dll**
- URL
- Javascript
- Flash\_swf
- pdf

**General**

Type-Name:  Override Suffix:

Description:

**Filterrules (Suffix and Regular Expressions for Program-Output)**

Suffix(es):

**=**

**and**

**≠**

**Timing**

CPR:  s    CPP:  s    +     s

**Execution-Script**

```
rundll32.exe %sample%
```

**Thanks!**