Simplified NIF for GN4 Input

Purpose: This NIF form is to be used for the submission of New Ideas suggested for inclusion in the GN4 Phase1 and beyond proposals. Budget estimates, information about objectives, impact, benefits, etc. as well as scope must all be supplied.

Submit to: pmo@GÉANT.net by January 31st, 2014 with the subject label starting: GN4Input

Overview

Project Name:	Denial of service attack detection and mitigation solutions	**Project Proposer:**	Teemu Kiviniemi - Funet

Project Type: GN4 Phase1 or longer term	Longer term	**Estimated Project Costs (best effort!)**	
Duration proposed	3 years	Manpower in person-months also identifying specific expertise required	Evaluation: 18 person-months Design: 18 person-months Deployment: 18 person-months Project management: 3 person-months
Deliverables proposed (If any can be defined at this stage)	Evaluation of DDoS detection and mitigation solutions. Design of a multi-domain DDoS detection and mitigation solution.	Hardware and equipment:	500 000 €
Milestones proposed (If any can be defined at this stage)	Year 1 (evaluation): Finding and evaluating existing and possible DDoS detection and mitigation solutions. Year 2 (design): Designing a multi-domain DDoS detection and mitigation solution. Year 3 (deployment): Deploying the planned solution.	Other costs	Travel and workshops: 60 000€

1 Background and Reasoning

Provide background information and the context of the project. Explain the reason for the project. What do you want to be different? What do you hope to improve? Why is the project needed? This should be the reason for the project, not the solution.

The size of distributed denial of service attacks (DDoS) seen on the Internet is continuously growing. Large attacks cause traffic congestion even on high bandwidth NREN backbone links, which considerably affects network quality and reliability experienced by network users. The ongoing transition to 100Gbit/s Ethernet in the backbone mitigates the problem, but only temporarily, as DDoS sizes continue to increase.

There is a need to develop longer term solutions to the DDoS problem. The distributed nature of attacks calls also for co-operation between network domains.

2 Objectives, Impact and Benefits

Provide one or more bullet points to briefly describe the primary objective(s) of the project in terms of the desired outcomes. This should be expressed in the form: 'To ensure…', 'To implement…', 'To service...', 'To improve...', 'To innovate...', 'To optimize...', 'To save...', etc. For each objective mention the benefits to identified stakeholders (e.g. end-users, NRENs, large international research projects, industrial research partners, high level education, etc.) should be mentioned. A description of the expected overall impact must also be provided.

- To find and evaluate solutions that help detecting and mitigating DDoS attacks.
- To design a multi-domain solution to protect NREN backbone networks and end-users by detecting and mitigating DDoS attacks.
- To deploy the planned solution, increasing network quality and reliability for all network users.

3 Scope

Describe the areas expected to be covered or impacted by the proposed activity, such as organisational areas, systems, processes, resources.. i.e. what is 'in scope'. This is not a list of what will be done but identifying the services, areas or what, will be affected.

Also please enumerate specific items which although they could perhaps be related are intentionally not addressed by your proposal ("Out of Scope").

1. In Scope

- Automatic DDoS attack detection solutions
- Automatic or manual DDoS mitigation solutions
- Multi-domain DDoS detection and mitigation solutions

2. Out of Scope

- Legal and administrative solutions to DDoS attacks.

4 General Information

Outline any potential issues, risks, dependencies, assumptions, constraints and limitations or any other points that may be useful to help assess the proposal.

- Deployed automatic detection and mitigation solutions may affect normal end-user traffic (false positives).
- The planned solutions may not be deployed widely enough, affecting the performance or coverage of the DDoS protection mechanisms.