SGA2 JRA2 Network Services Development
All-Hands Meeting - T6

David Schmitz
Leibniz Supercomputing Center

GÉANT GN4-2 JRA2 All-Hands Meeting, Malaga
01/02 June 2016

Outline

- Work items of T6
- Interworking between work items
- Interworking/Interfaces to other tasks/activities

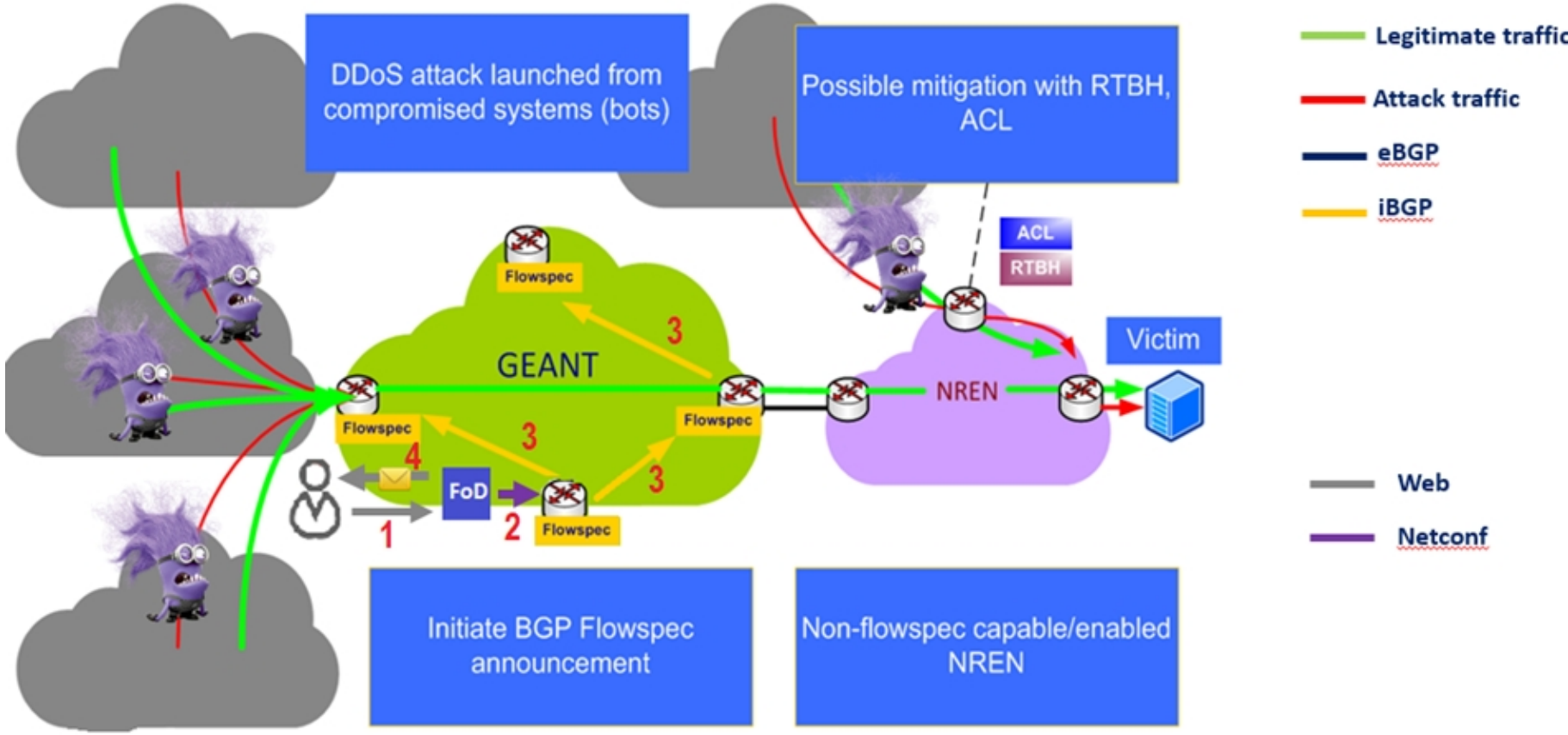
Work Items of T6 (from DoW)

- FOD, FwaaS
- (Generic) Security Event Processing: mainly input for FOD/FwaaS
- Security Testbed: maybe no man power for this
- Certificate Transparency

FOD = Firewall On Demand

- Goal: DDOS attack mitigation
- How
  - Filter normally routed Geant IP traffic based on BGP Flowspec (RFC5575) rules
  - Web GUI for NREN NOCs
- Status: from SA3T1, productive in near-term
- To be enhanced:
  - Currently no automated rules, only manual entering
  - Currently only DROP rule supported

FOD = Firewall On Demand (2)



FwaaS = Firewall as a Service

- Evolve FOD further
  - Currently only DROP and IPv4: further reactions, IPv6
  - Currently only use for GEANT routers
  - Use for GTS projects, e.g. as GTS component (also relation to Sec Testbed)
  - Use SDN/Openflow for more flexible filtering
  - Automated rule proposal (see next work item)

Security Event Processing

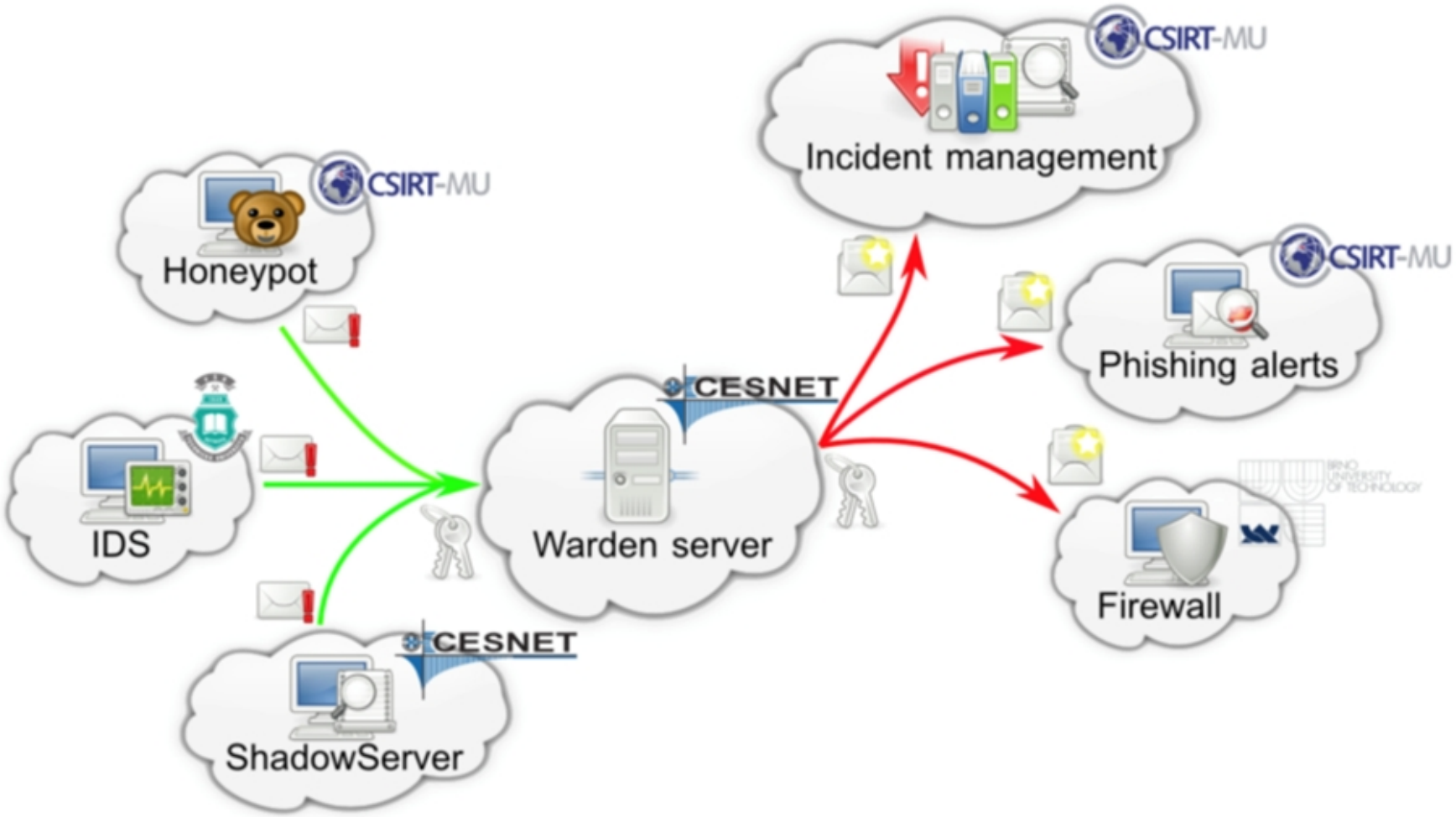
- Generic event processing framework
- But used in particular for input of FwaaS
- Existing or projected components (CESNET)
  - Warden: Event hub for alert/event sharing
  - Rep(utation)Shield: Estimation of reputation of network ntities, e.g. IP address (spaces)

Generic Security Event Processing: mainly input for FwaaS - Warden

- Event hub for alert/event sharing
- Uses IDEA format (https://idea.cesnet.cz/en/index)
- Receiving events from different sources: e.g.
  - GEANT NSHaRP (Network Security Handling and Response Process)
  - NREN alert systems
  - Security Testbed (next work item)
- Distributing received events to different listeners: e.g.
  - RepShield

(https://warden.cesnet.cz/)

Generic Security Event Processing: mainly input for FwaaS - Warden (2)



Generic Security Event Processing: mainly input for FwaaS - Rep(utation)Shield

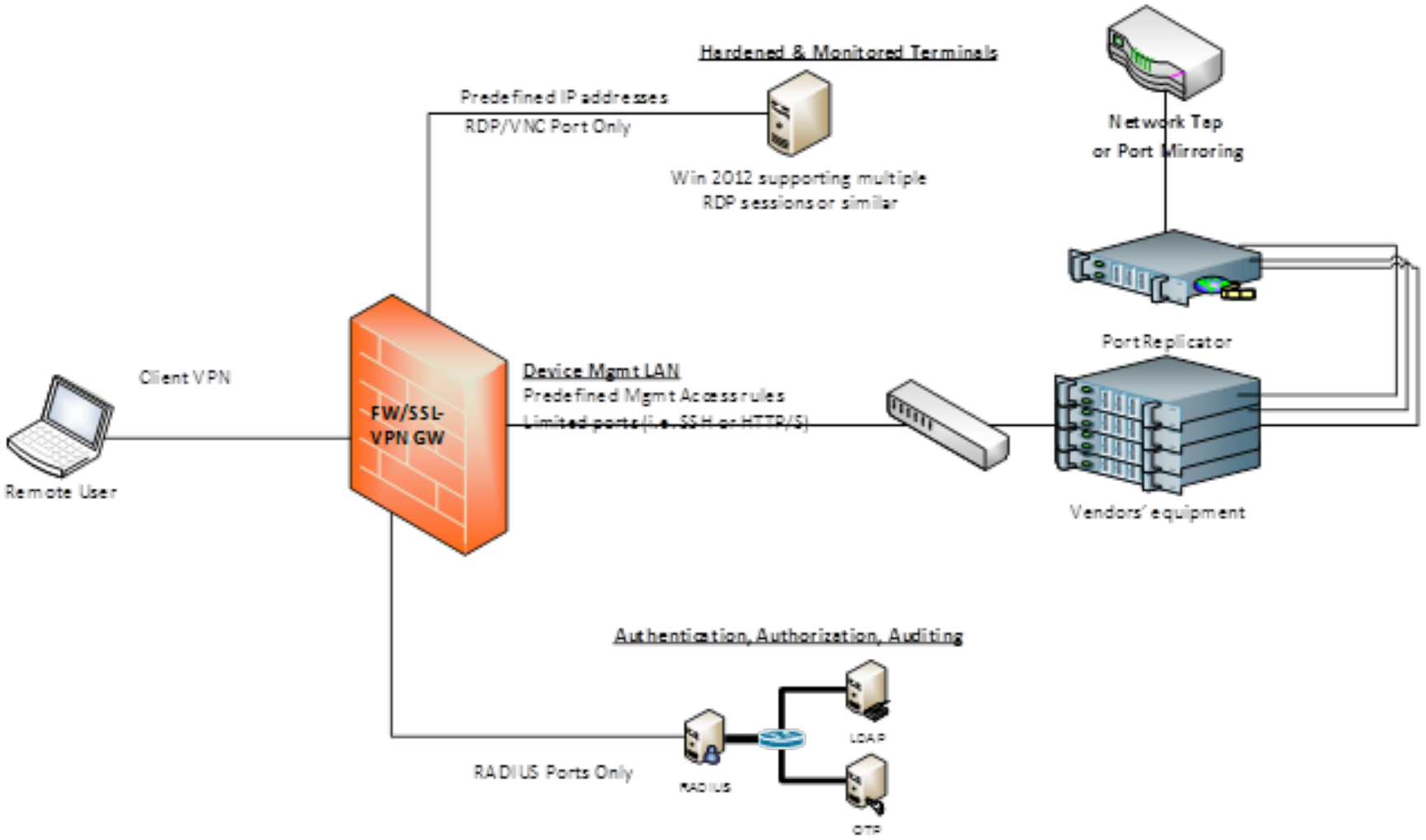
- Analyzing alerts/events
- Correlating with various other information sources
- Estimation of Reputation Score for network entities, e.g.,
  - IP address
  - Network (IP prefix)
  - AS
  - Domain
- Reputation Score: probability and severity of future attacks
- Use as input for proposing FOD/FwaaS rules

(https://www.cesnet.cz/wp-content/uploads/2015/12/Reputation-Shield-BARTOS.pdf)

Security Testbed (1)

- Idea inherited from GN4P1 SA3T1
  - Give vendors tap port access of GEANT IP traffic to test new security appliances
  - Get to know interesting security products
  - Get back current security events: for event processing
- Legal Issues, but idea interesting, especially when performed internally by GEANT, NRENs, institutions

Security Testbed (2) - Architecture



Security Testbed (3) - Potential Further ideas

- Use for security education
- Test security threats in isolated environment
- "Testing version security testbed" (CESNET)
  - Provide referential toolset for security detecting (operational in CESNET)
  - Open-source, Easily deployable by NRENs (maybe using GTS)
  - Share generated events via Warden
  - Compare results of detection with other 3rd-party detectors

- Currently no man power,
- But some open-source tools already exist

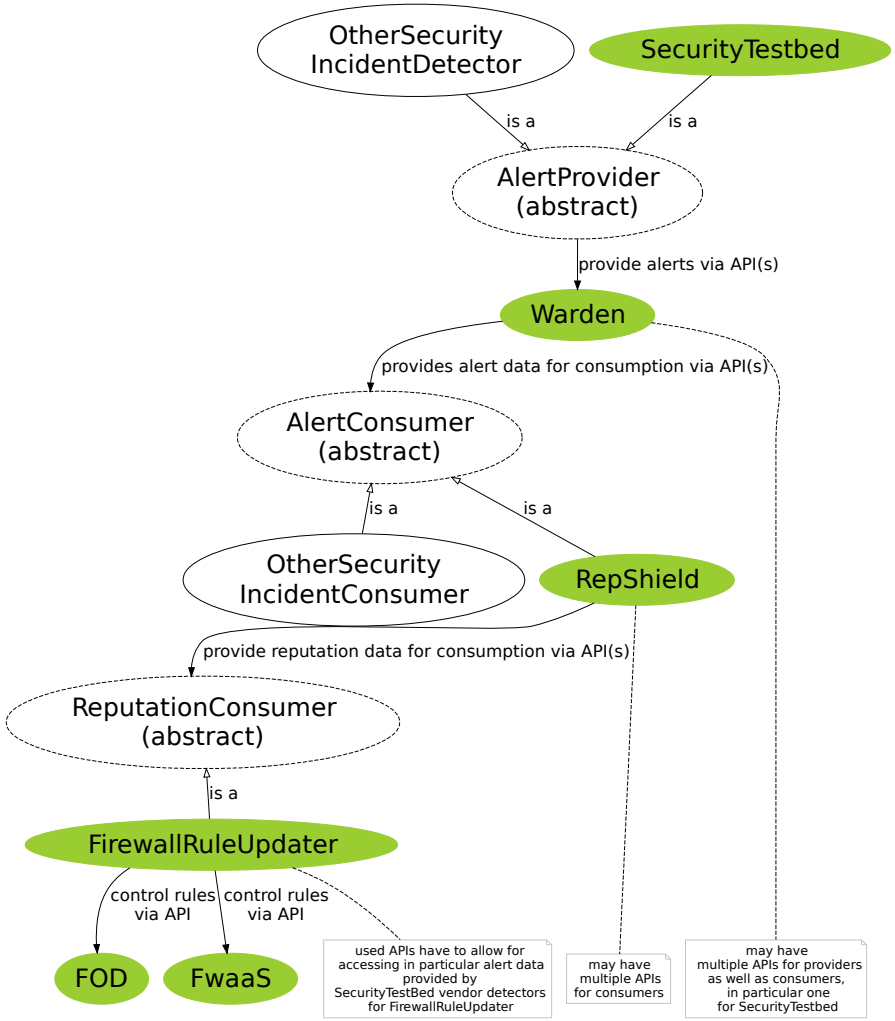
Certificate Transparency

- For verifying certificates by CAs, domain owner, end users (web browser) (RFC 6962)
- Identifying fraudulent and revoked certificates
- Existing work performed by NORDUnet
- Continued in phase2

Interworking of the Work Items

- Security Testbed, and other information sources produce security events
- Warden receives and centrally distributes them, especially to RepShield
- RepShield analyzes and enhances them with info from other sources
- And estimates Reputation Score of IP addresses (and address ranges)
- Reputation info is used to propose FOD/FwaaS rules
- FOD/FwaaS users can accept/decline them
- (Potentially: Include events from Certificate Transparency Log for rule generation)

GN4P1 SA3T1 Security Architecture



Based On

- Defined Scenario and
- Derived Requirements

(in deliverable GN4P1 SA3-T1: D7.1 Multi-Domain Service Security Architecture)

T6 Team

- FOD*/FwaaS
  - Evangelos Spatharas* (GEANT)
  - Nino Ciurleo (GARR)
- Event Processing: Warden*, RepShield*
  - Tomas Cejka (CESNET)
  - Vaclav Bartos* (CESNET)
- Certificate Transparency+
  - Linus Nordberg (NORDUnet)
  - Magnus Ahltorp (KTH)
- David* (LRZ)

*: already in GN4P1 SA3-T1
+: already in GN4P1

(Potential) Interworking/Interfaces to other tasks (1)

- T1: clearly defined connection-oriented network services (including multi layer/domain/virtual topology)
  - To be protected/supported by FwaaS
  - To be used in security events (IDEA format)
- T2: clearly defined generic services and their support/management functions (in general)
  - To be protected/supported by FwaaS
  - To be used in security events (IDEA format)

(Potential) Interworking/Interfaces to other tasks (2)

- T3
  - As a user of GTS: Security Testbed
  - New (virtual) components of GTS: e.g. FwaaS instance, event processing components
  - Securing GTS itself by FwaaS
- T4
  - Possibly: provide basic measurement information for generating security events
- T5
  - Provision function for management software to users, e.g., to be applied for CESNET's event detection software for 'Testing Version Security Testbed' to NRENs

(Potential) Interworking/Interfaces to other activities

- JRA1
  - SDN/Openflow for enhanced, flexible FOD: per testbed project, per user group
- SA1 (also in general for whole JRA2)
  - Operating (and needed education for this) of security (management) functionality in services
- SA2 (also in general for whole JRA2)
  - Introduction and CSI of security (management) "services"/functionalities, e.g. FwaaS
  - Operating (and needed education for this) of security (management) functionality in services

GÉANT

Networks • Services • People

www.geant.org

GEANT ed on behalf of the GN4 Phase 1 project.
The rese ading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1

Further Questions To Discuss (regarding general service notion used in JRA2)

- Should (connection-oriented network) service model definition include security (management) functionalities right from start?

  Examples for functionalities (provided via respective virtual components):

  - FwaaS functionalities
  - Event collection/distribution functionalities
  - Reporting functionalities
- What QoS Parameters/KPIs are defined regarding security (management) functionalities and when?
- How is/are management access point(s) defined regarding security management and when?
- How are defined security (management) functionalities mapped to realizing components/used sub services?

GÉANT

Networks • Services • People

www.geant.org

GEANT ed on behalf of the GN4 Phase 1 project.
The rese ading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1

Existing SW Components - FOD

Existing SW Components - Warden

Existing SW Components - RepShield

Existing SW Components - Security Detection Referential Toolset

Existing SW Components - CT

GÉANT

Networks • Services • People

www.geant.org

GEANT ed on behalf of the GN4 Phase 1 project.
The rese ading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1

Multi-Domain Service Security Architecture - Requirements for integration of existing security monitoring solutions

ID	Description	Weight
AS-1	Definition of an exchange format for security alert sharing	3
AS-2	Capabilities to filter, anonymise or pseudonymise alerts before forwarding	2
AS-3	Procedure to subscribe before forwarding and mechanism to authenticate alert providers	3
AS-4	Mechanisms to process alerts provided by various security solutions and map them to the defined exchange format	3
AS-5	Real-time, push-based forwarding of security information to central aggregation component	3

Multi-Domain Service Security Architecture - Requirements for Security Testbed

ID	Description	Weight
ST-1	SPAN port or tape device to forward network traffic to monitoring solutions	3
ST-2	Replication of traffic to allow up to 20 vendors	3
ST-3	Capabilities to filter certain traffic (NREN?s opt-out) or forward filtered traffic to dedicated security solutions	3
ST-4	Provision of secure, multi-tenant access allowing vendors to access their own security products	3
ST-5	Definition of a procedure for initial auditing of the provided security solution before connecting it to the security testbed as well as re-auditing on a regular basis and after major	2

Multi-Domain Service Security Architecture - Requirements for Security Information and Event Sharing System

ID	Description	Weight
SI-1	Provide a central system to which security alerts raised by detection of malicious activities can be forwarded	3
SI-2	Definition of a database scheme to store security alert information on this central system	3
SI-3	Provide pre-processing components that allow filtering, anonymisation/pseudonymisation, event parsing and extraction of relevant fields	2
SI-4	Specification and implementation of a web-based configuration interface for authenticated users (CERT members, administrators)	1

Multi-Domain Service Security Architecture - Requirements for Reputation Scoring

ID	Description	Weight
RS-1	Specification and implementation of report normalisation, aggregation and enrichment components	3
RS-2	Definition and implementation of a reputation-scoring method	3
RS-3	Definition of aging algorithm for reputation	2
RS-4	Definition of automated adaptation algorithm reflecting the evolving threat landscape	2
RS-5	Specification of API into reputation database	3
RS-6	Specification of a web interface for manual interaction and access to data stored in the reputation database	2

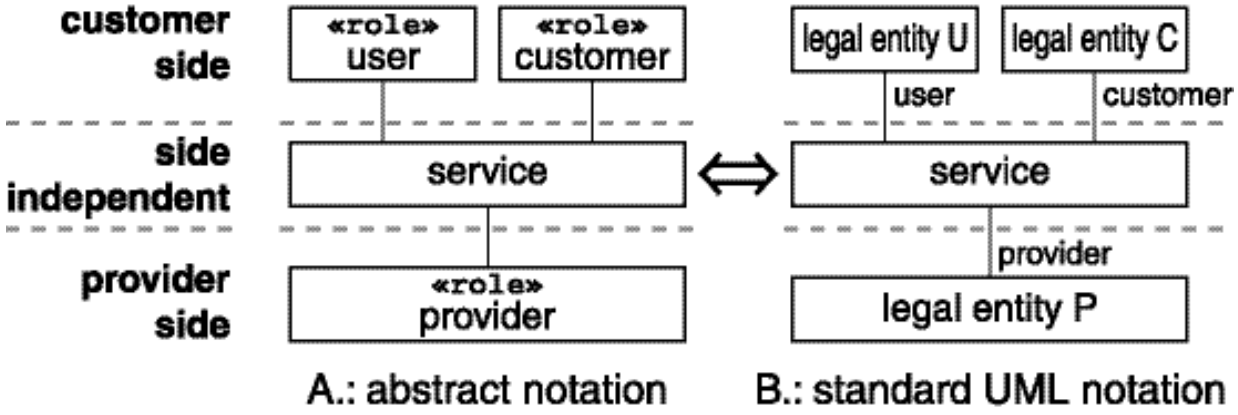
Multi-Domain Service Security Architecture - Requirements for Automated Response

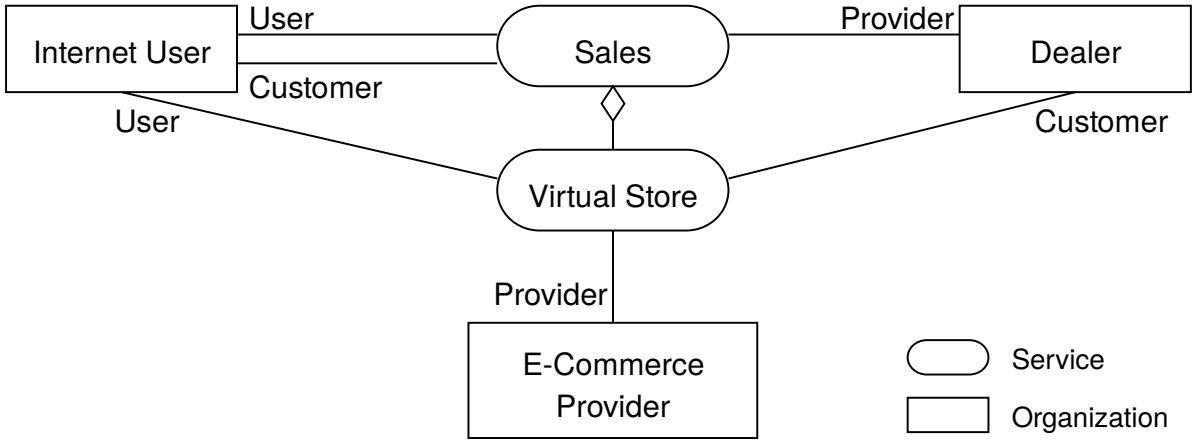
ID	Description	Weight
AR-1	Automated response system should provide different, active and passive mechanisms, e.g. mail notification, (semi-)automated blocking,	3
AR-2	Role-based access control to the system and definition of fine-grained capabilities for users	3
AR-3	Multi-tenancy to ensure that successfully authenticated users can trigger automated responses only for networks/systems they are responsible for	3
AR-4	Logging of user interaction with the system, e.g. trigger notification, activating filter rules,	2

Proposal: MNM Service Model

- Generic model for IT services
- Developed 15 years ago by MNM (Munich Network Management) Team
- Common view/terms between provider and customer/user
- Separate specification from realization
- Explicit notion of management vs. usage functionalities
- Covering whole service life cycle
- Allow for recursion: customer/user of service being provider for upper service
- Instantiation Methodology for concrete scenarios

Proposal: MNM Service Model - Basic View

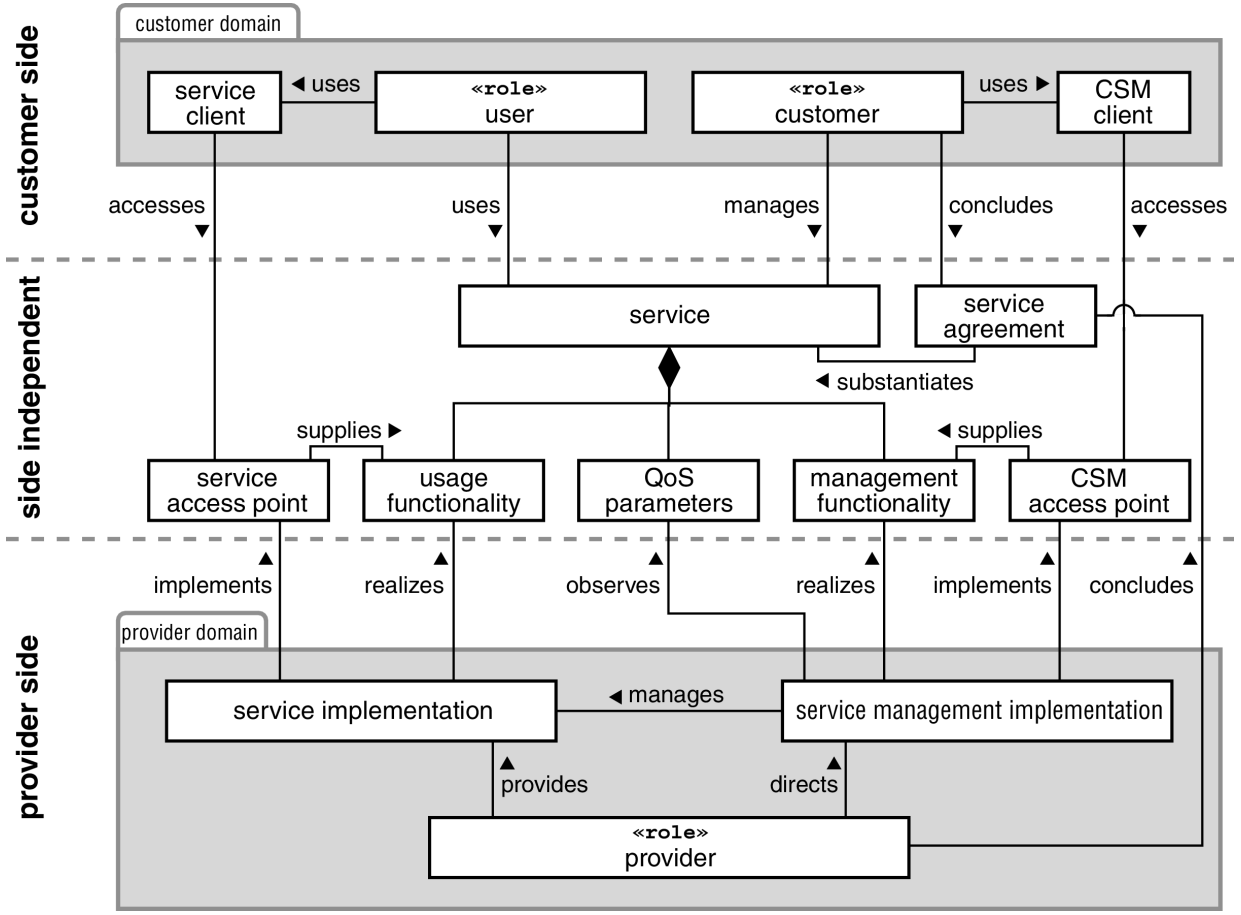




- Roles for proper service usage vs. management
  - User vs.
  - Customer

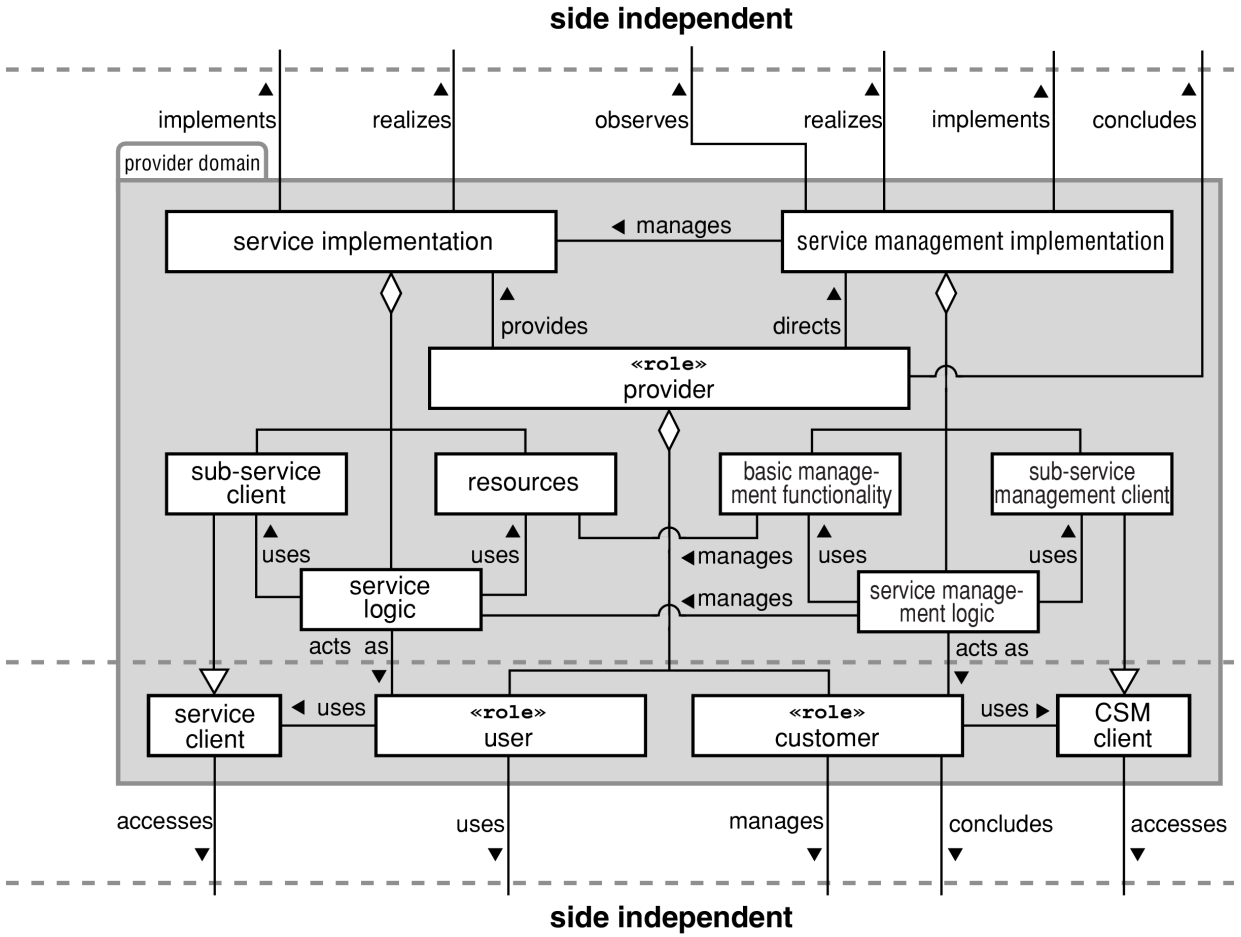
Example Service Scenario

Proposal: MNM Service Model - Service View



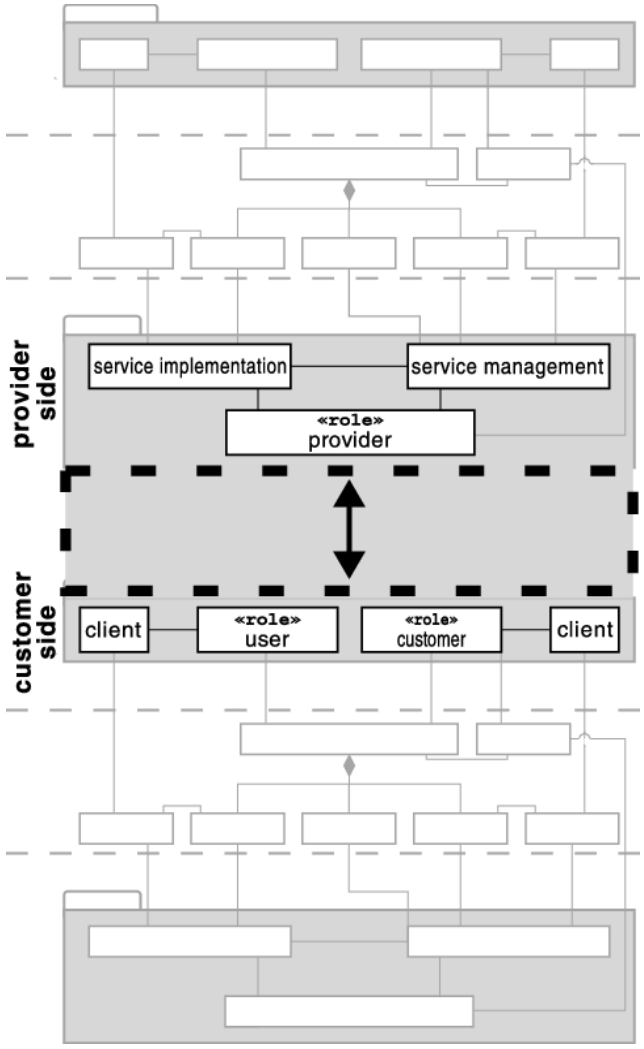
- Common view between user/customer and provider
- Only specification, no provider-internal realization
- Usage vs. Management functionalities

Proposal: MNM Service Model - Realization View



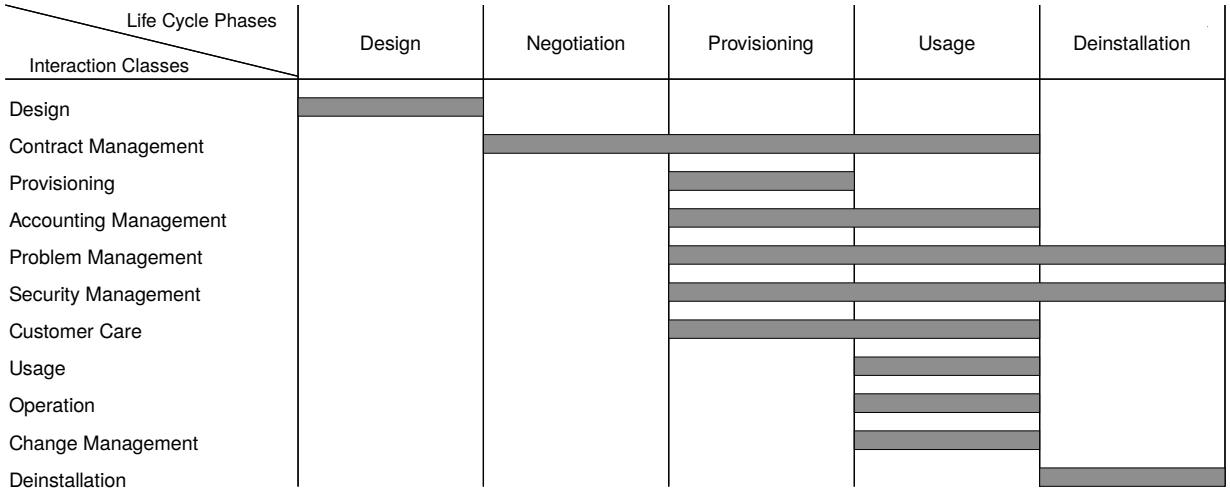
- Provider-internal view
- Separation between usage vs. management realization

Proposal: MNM Service Model - Recursive Application



- Provided low-level service as sub service (part of realization) of high-level service
- Provider of high-level service as customer/user of low-level service

Proposal: MNM Service Model - Proposal (2001) of Classes for Management functionality



- Covering whole service life cycle
- Based on TOM (Telecom Operations Map)

Proposal: MNM Service Model - References

- M. Garschhammer, R. Hauck, H.-G. Hegering, B. Kempter, M. Langer, M. Nerb, I. Radisic, H. Roelle, and H. Schmidt. Towards generic Service Management Concepts - A Service Model Based Approach. In G. Pavlou, N. Aner- ousis, and A. Liotta, editors, Proceedings of the 7th International IFIP/IEEE Symposium on Integrated Management (IM 2001), pages 719-732, Seattle, Washington, USA, May 2001. IFIP/IEEE, IEEE Publishing.
- M. Garschhammer, R. Hauck, B. Kempter, I. Radisic, H. Roelle, and H. Schmidt. The MNM Service Model - Refined Views on Generic Service Management. Journal of Communications and Networks, 3(4):297-306, Dezember 2001.
- M. Garschhammer, R. Hauck, H.-G. Hegering, B. Kempter, I. Radisic, H. Roelle, and H. Schmidt. A Case-Driven Methodology for Applying the MNM Service Model. In R. Stadler and M. Ulema, editors, Proceedings of the 8th International IFIP/IEEE Network Operations and Management Symposium (NOMS 2002), pages 697-710, Florence, Italy, April 2002. IFIP/IEEE, IEEE Publishing.