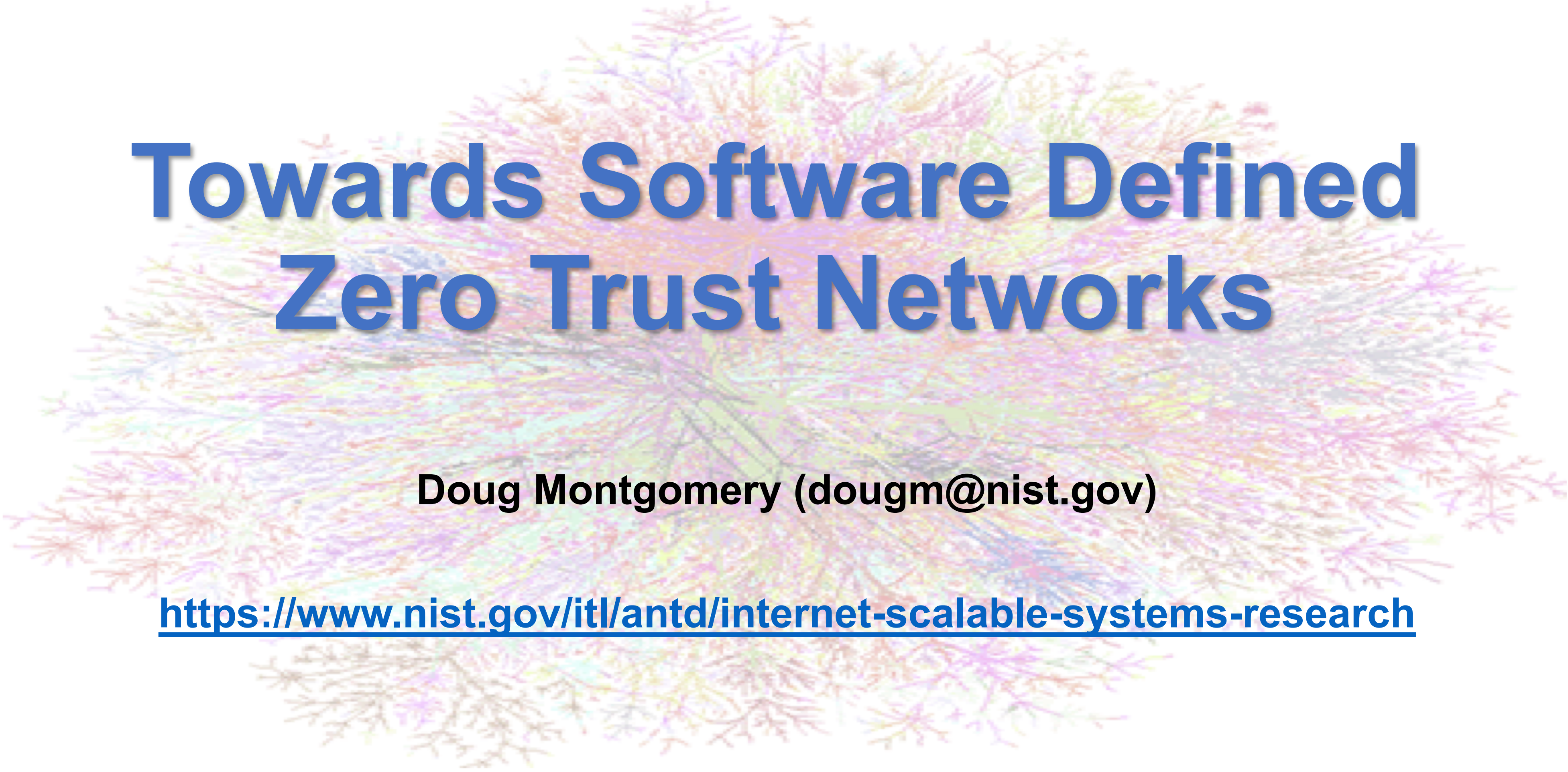
National Institute of Standards and Technology
U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

Establishing the Technical Basis for Trustworthy Networking



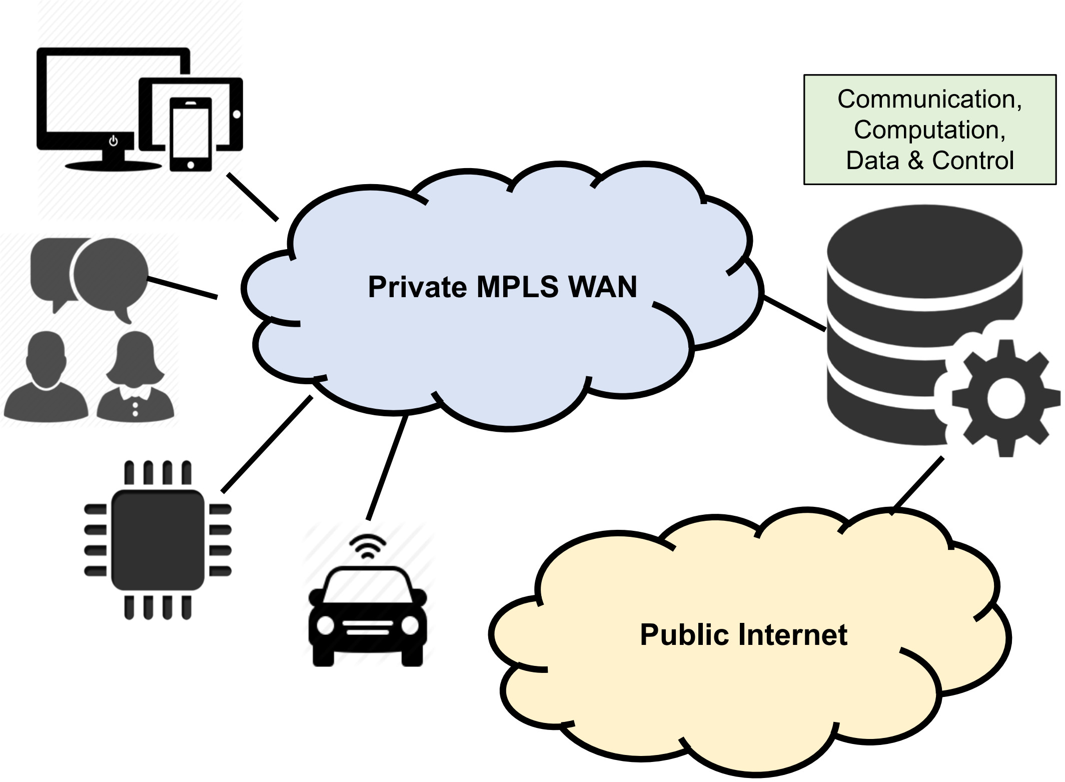
Towards Software Defined Zero Trust Networks

Doug Montgomery (dougm@nist.gov)

https://www.nist.gov/itl/antd/internet-scalable-systems-research

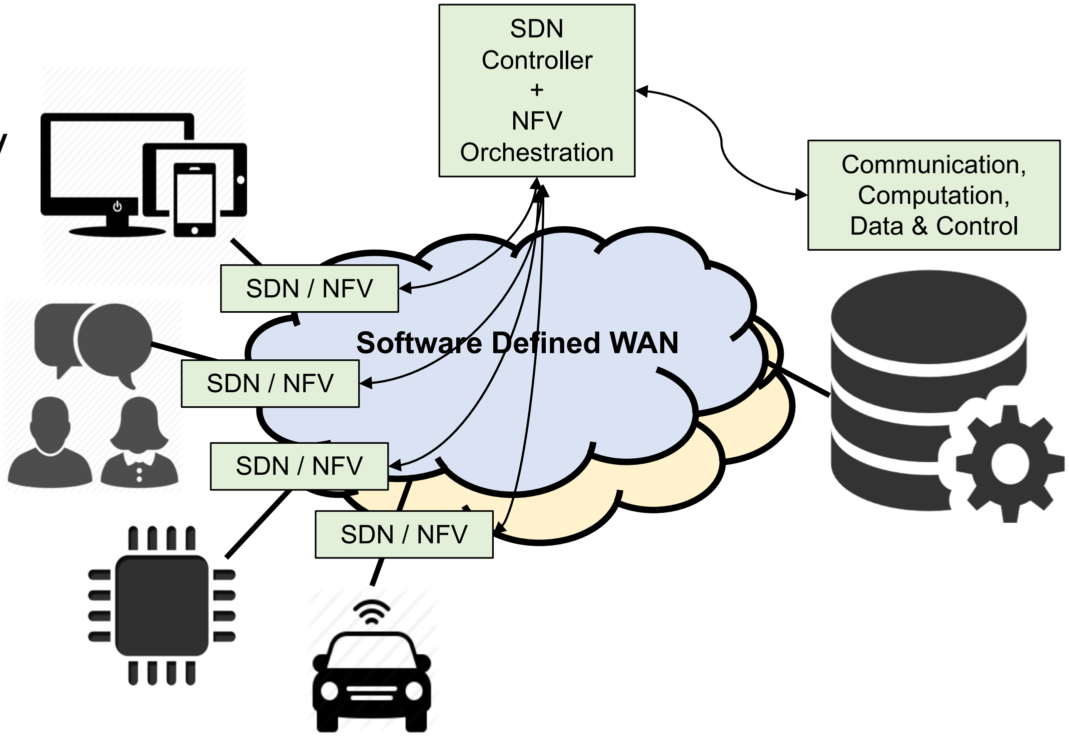
Traditional Enterprise and WAN Networks

- **Traditional Private WAN:**
  - Data center VPN back haul.
  - Decoupled network & application policy.
  - Limited control / computing at network edge.
  - Limited ability to exploit / manage multiple communication paths.
  - Disjoint / inflexible measurement / monitoring and security awareness.



Software Defined & Virtualized Networks

- **SD WAN + NFV:**
  - Application / user aware policy at network edge.
  - Micro segmentation of traffic based upon managed policy.
  - Distributed virtualized network functions.
  - Application / users policy aware telemetry at network edge.
  - Scalable holistic network monitoring and anomaly detection.
  - Automated load balancing over multiple transport sources.


SDN Controller + NFV Orchestration
Communication, Computation, Data & Control
SDN / NFV
SDN / NFV
SDN / NFV
SDN / NFV
Software Defined WAN

Software Defined & Virtualized Networks

- **NIST Research & Standards Efforts:**
  - Application / user aware policy at network edge.
  - Micro segmentation of traffic based upon managed policy.
  - Distributed virtualized network functions.
  - Application / users policy aware telemetry at network edge.
  - Scalable holistic network monitoring and anomaly detection.
  - Automated load balancing over multiple transport sources.

Software Defined Security for IoT

Programmable Measurement and Monitoring for Software Defined Networks

Trustworthy Networking

- **ISOC 2017 Report on the Future of the Internet**
  - *"Perhaps the **most pressing danger to the future of the Internet** is the rising scope and breadth of Cyber Threats."*
  - ***"Addressing cyber threats should be the priority"***
  - *"The scale of cyberattacks is steadily growing, and many anticipate the **likelihood of catastrophic cyberattacks in the future**."*
  - *"Inadequate management of cyber threats will put users increasingly at risk, **undermine trust in the Internet and jeopardize its ability to act as a driver for economic and social innovation.**"*
- **Cultivating Trust is not Easy …**
  - Challenges are technical, economic, often dominated by prevailing business models, complicated by massive installed bases, and fears of governmental interference.

Internet Society

2017

INTERNET SOCIETY GLOBAL INTERNET REPORT

Paths to Our Digital Future

Establishing the Technical Basis for Trustworthy Networking

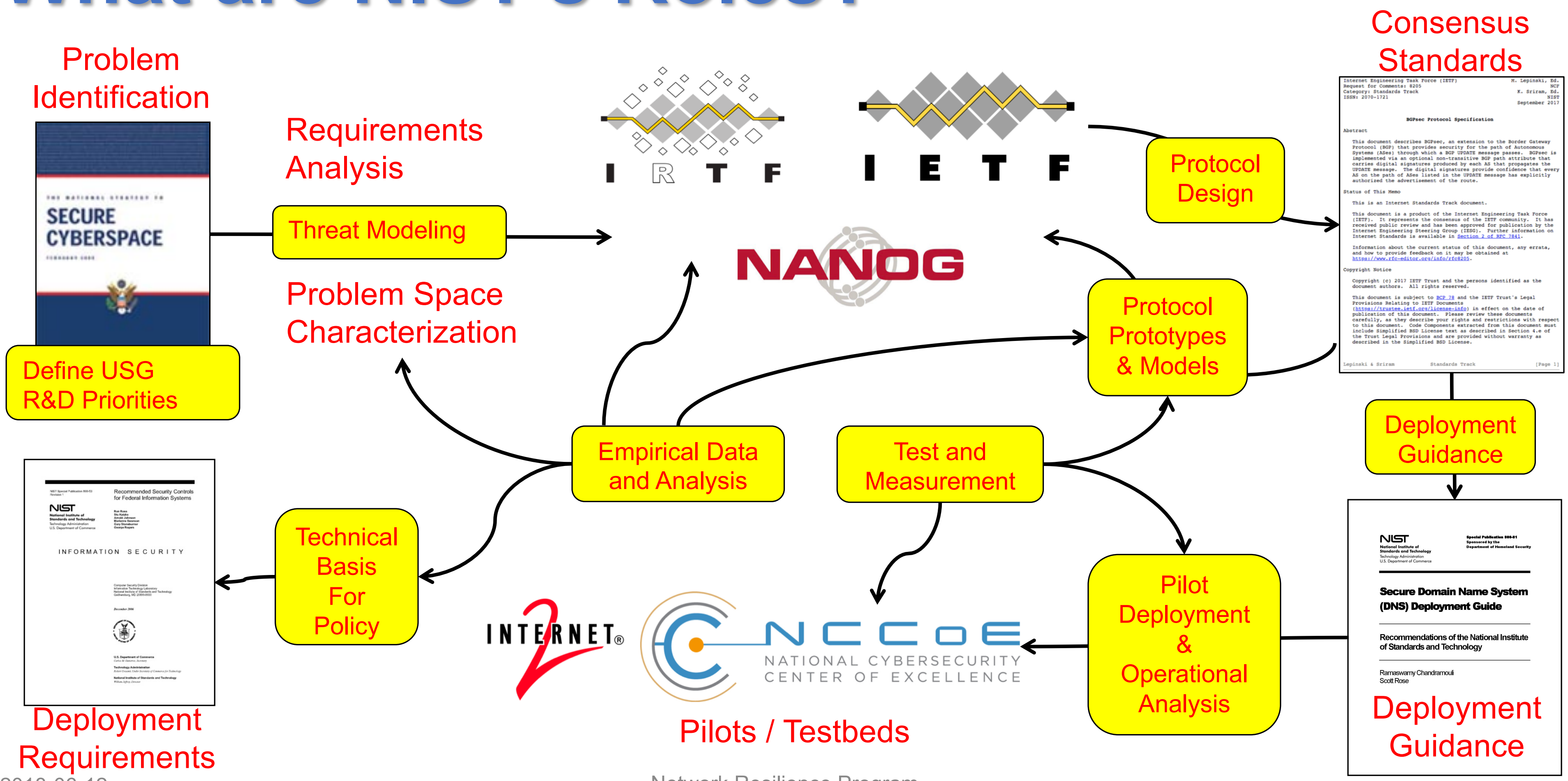
Network Resilience Program

- **Understanding / Controlling Network Behavior**
  - *"[Despite] society's profound dependence on networks, fundamental knowledge about them is primitive. Global communication networks have quite advanced technological implementations but their behavior under stress still cannot be predicted reliably.…There is no science today that offers the fundamental knowledge necessary to design large complex networks [so] that their behaviors can be predicted prior to building them."* Network Science, a report from the National Research Council [4].

- **The Need for NIST:**
  - **Advance Network Metrology** – with emphasis on innovating and applying advanced measurement science to Internet-scale systems.
  - **Foster Trustworthy Network Technology** – work with industry to improve the quality and timeliness of emerging specifications and foster adoption of trustworthy Internet technologies.
  - **Our efforts focus on Internet Scale problems, solutions and measurement techniques.**

Establishing the Technical Basis for Trustworthy Networking

What are NIST's Roles?



```
Internet Engineering Task Force (IETF)                    M. Lepinski, Ed.
Request for Comments: 8205                                             NCF
Category: Standards Track                                   K. Sriram, Ed.
ISSN: 2070-1721                                                       NIST
                                                            September 2017

                       BGPsec Protocol Specification

Abstract

   This document describes BGPsec, an extension to the Border Gateway
   Protocol (BGP) that provides security for the path of Autonomous
   Systems (ASes) through which a BGP UPDATE message passes.  BGPsec is
   implemented via an optional non-transitive BGP path attribute that
   carries digital signatures produced by each AS that propagates the
   UPDATE message.  The digital signatures provide confidence that every
   AS on the path of ASes listed in the UPDATE message has explicitly
   authorized the advertisement of the route.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF).  It represents the consensus of the IETF community.  It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG).  Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8205.

Copyright Notice

   Copyright (c) 2017 IETF Trust and the persons identified as the
   document authors.  All rights reserved.

   This document is subject to BCP 78 and the IETF Trust's Legal
   Provisions Relating to IETF Documents
   (https://trustee.ietf.org/license-info) in effect on the date of
   publication of this document.  Please review these documents
   carefully, as they describe your rights and restrictions with respect
   to this document.  Code Components extracted from this document must
   include Simplified BSD License text as described in Section 4.e of
   the Trust Legal Provisions and are provided without warranty as
   described in the Simplified BSD License.

Lepinski & Sriram            Standards Track                    [Page 1]
```

NIST Special Publication 800-53
Revision 1

Recommended Security Controls for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-81
Sponsored by the
Department of Homeland Security

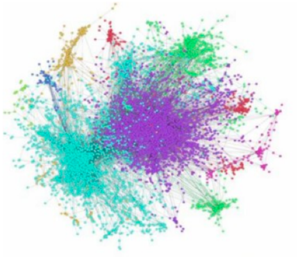
Secure Domain Name System (DNS) Deployment Guide

Recommendations of the National Institute of Standards and Technology

Ramaswamy Chandramouli
Scott Rose

Related Program Areas.

- **Robust Inter-Domain Routing – Kotikalapudi Sriram & Oliver Borchert**
  - https://www.nist.gov/programs-projects/robust-inter-domain-routing
- **High Assurance Domains – Scott Rose**
  - https://www.nist.gov/programs-projects/high-assurance-domains
- **Measurement Science for Complex Systems – Kevin Mills**
  - https://www.nist.gov/programs-projects/measurement-science-complex-information-systems
- **Software Defined and Virtual Networks – Yang Guo**
  - https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques



NIST National Institute of Standards and Technology U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

Software Defined Security for Scalable IoT Defense

Establishing the Technical Basis for Trustworthy Networking

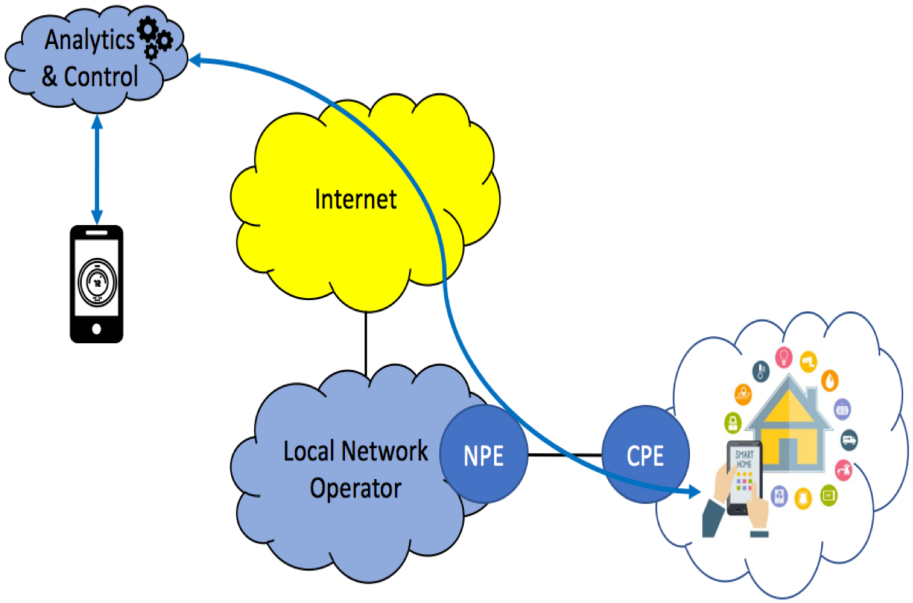
Doug Montgomery, Mudumbai Ranganathan, Charif Mahmoudi,

Laurence Chang, Max Kimmelman

proj-sdn@nist.gov, https://www.nist.gov/programs-projects/software-defined-virtual-networks

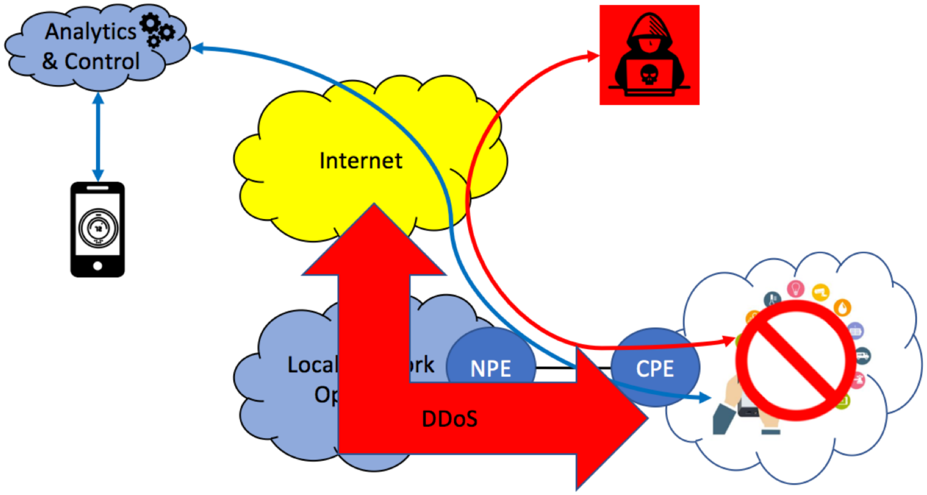
Things on the Internet

- **Explosion of networked things**
  - Key enabler for smart environments (e.g., homes, transportation, health).
  - Things themselves often limited in capabilities / uses.
- **Cloud based business models**
  - Things often controlled, accessed, provide data to cloud based services.
  - Creates giant attack surface for networked things.



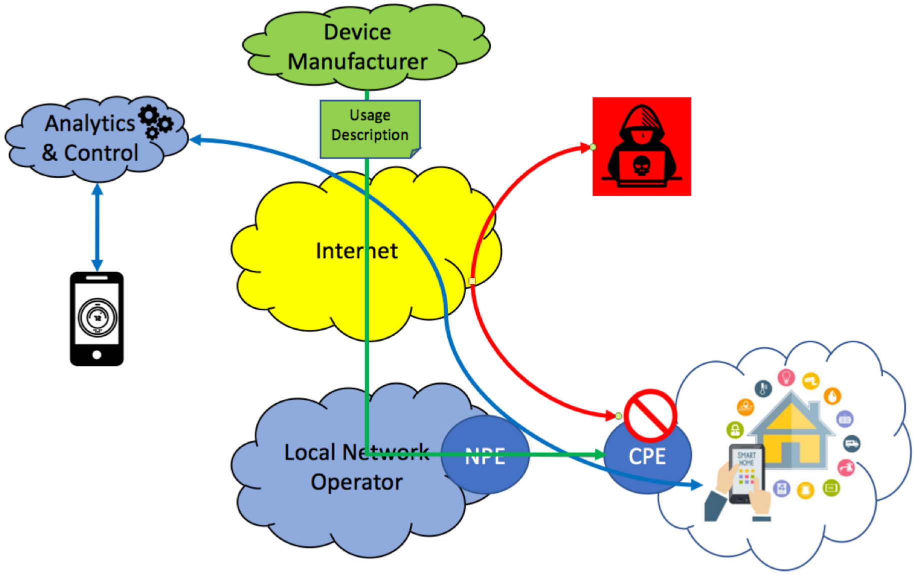
Hackers Like Things Too

- **Things are vulnerable targets**
  - Typically not general purpose computers, thus lack the ability to protect themselves.
  - Often "networked" as an add-on to original design.
  - Poorly maintained – lack ability for secure software update, or are no longer supported.
- **Hacked things …**
  - Used to disable / alter their basic service.
  - Used to attack other systems on the network.



Pragmatic Solutions

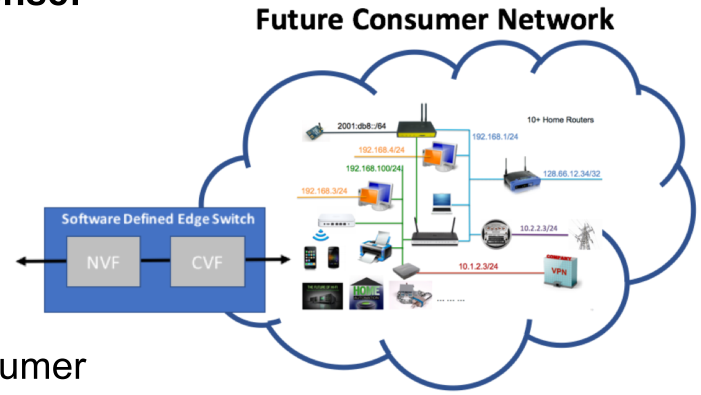
- **Thing manufacturers …**
  - ..are in a position to significantly leverage this problem.
  - They know what their thing is supposed to do!
  - Network needs to know:
    - What is this thing?
      - Who made it?
      - Who owns it?
    - **What network access does it need?**
- **Manufacturer Usage Description**
  - IETF specifications under development.
- **Strict Policy Based Networking**
  - Any commination not explicitly specified MUP profile is not permitted.



I E T F®

Software Defined IoT Defense

- **Project Goals:**
  - **Explore future architectures for software defined IoT Defense:**
  - Support **policy driven security profiles** for individual device types.
    - Move to a policy-based model of network security for limited functionality devices.
  - Support **authentication of attached devices** / types.
    - Authentication to the network and within the network.
  - Support **complex consumer networks and requirements for segmentation** and security within the consumer network.
    - Potentially controlled by the manufacturer / consumer.
  - Support **policy driven security profiles for Internet access**.
    - Controlled by the network operator.
  - Support both proactive and **reactive defense mechanisms using virtualized IDS / Firewall functions**.

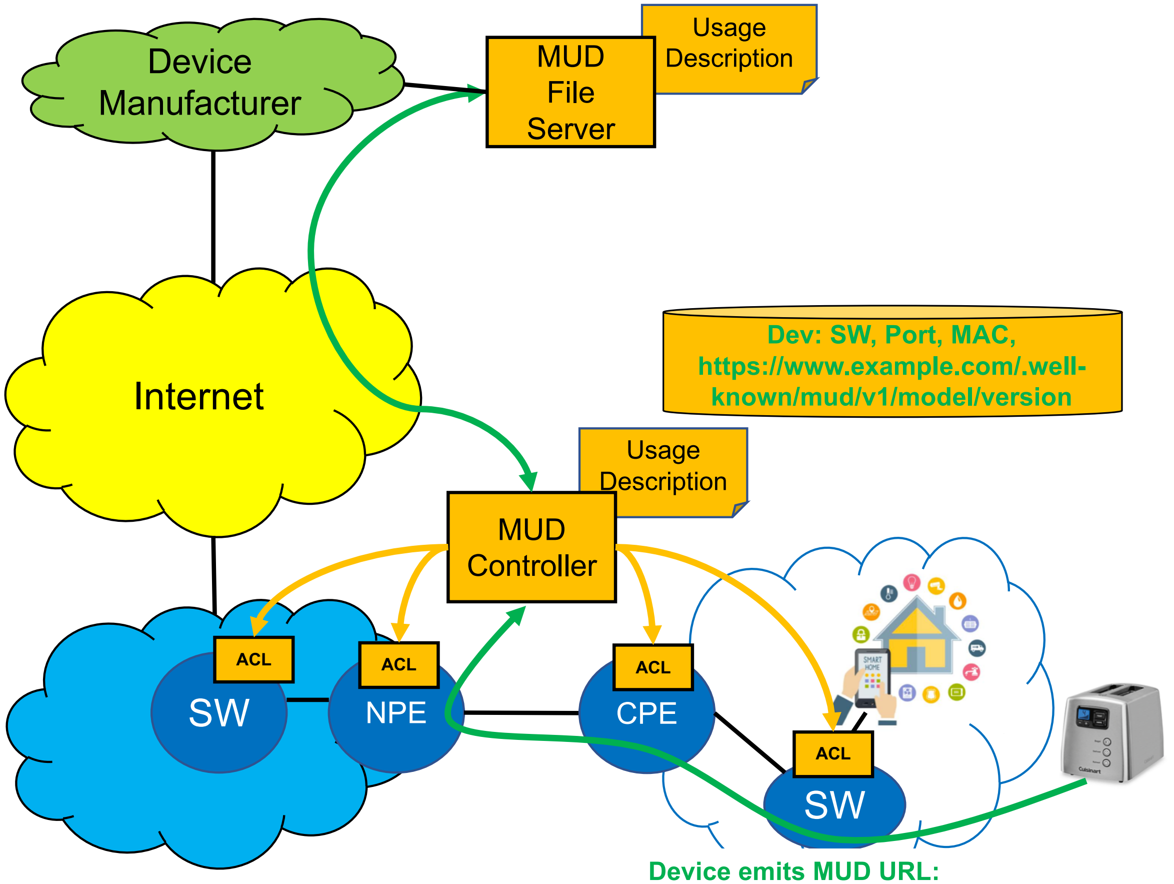

Future Consumer Network

Establishing the Technical Basis for Trustworthy Networking

NIST National Institute of Standards and Technology U.S. Department of Commerce

ITL INFORMATION TECHNOLOGY LABORATORY

So How Will MUD Work?

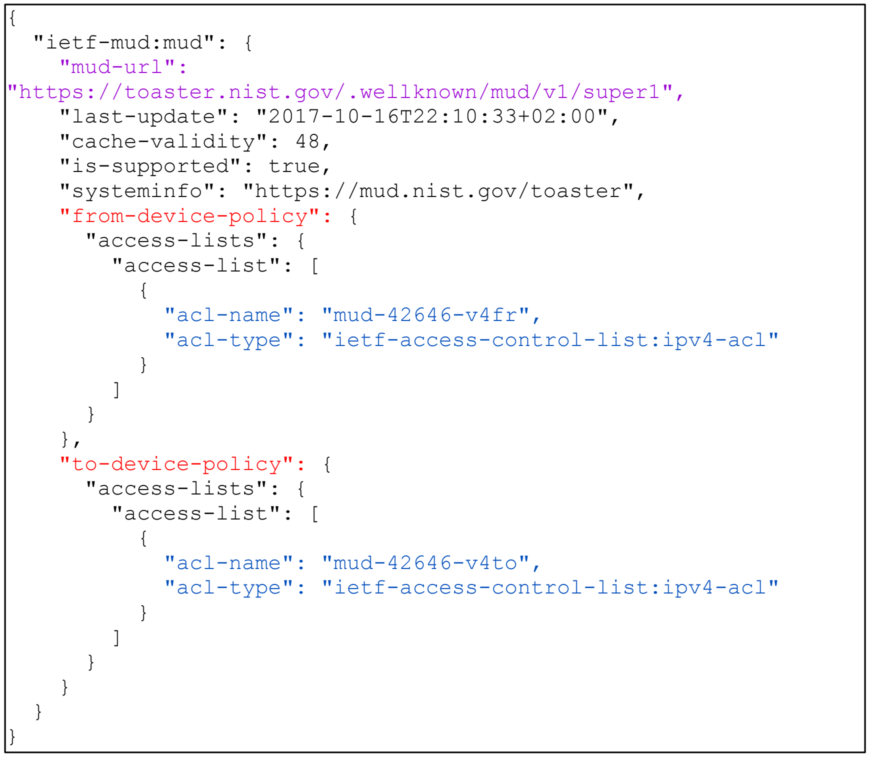


Device emits MUD URL:
https://www.example.com/.well-known/mud/v1/model/version

MUD Profiles

- **What is this thing?**
  - MUD URL
- **What network access does it need?**
  - MUD File
  - YANG model of extended access control lists (ACLs).
  - Meta data for MUD Controller

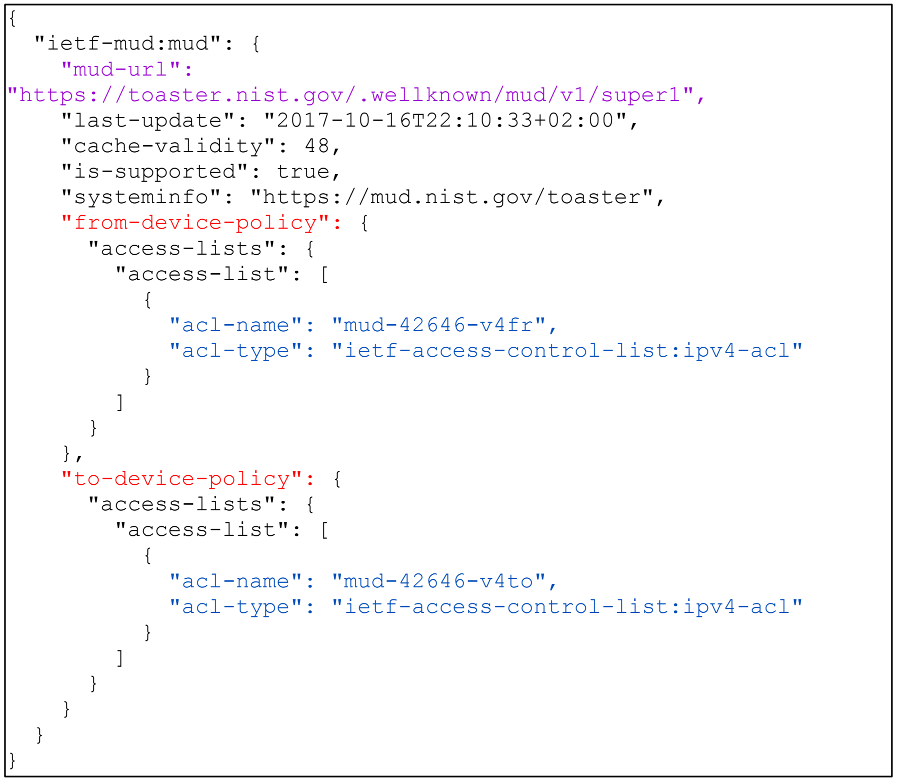
https://www.example.com/.well-known/mud/v1/model/version



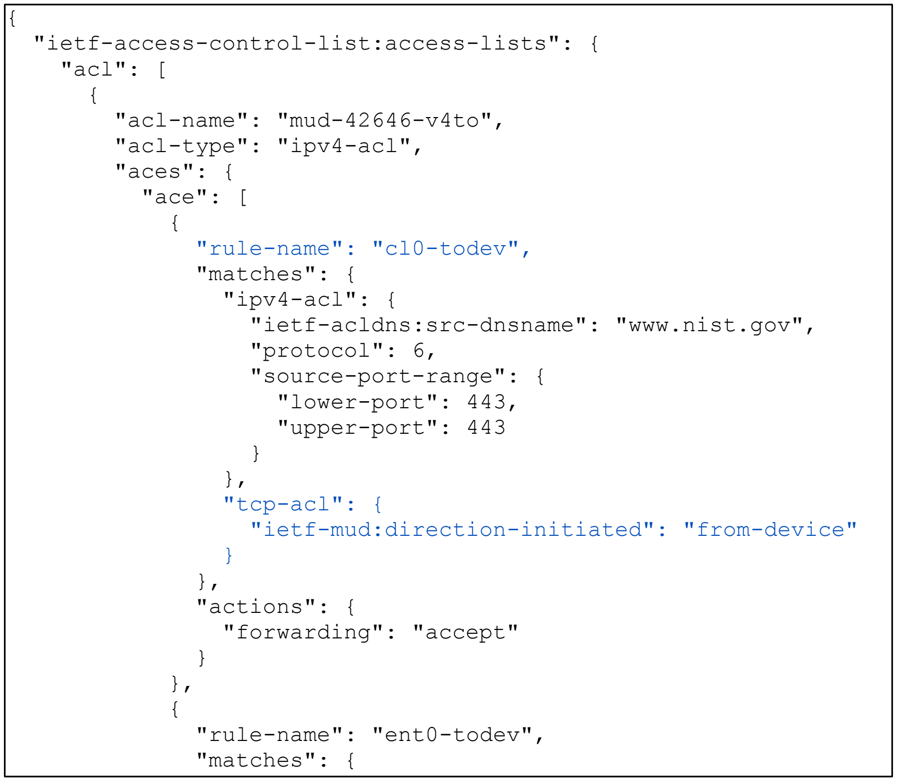
```
{
  "ietf-mud:mud": {
    "mud-url":
"https://toaster.nist.gov/.wellknown/mud/v1/super1",
    "last-update": "2017-10-16T22:10:33+02:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "https://mud.nist.gov/toaster",
    "from-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "acl-name": "mud-42646-v4fr",
            "acl-type": "ietf-access-control-list:ipv4-acl"
          }
        ]
      }
    },
    "to-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "acl-name": "mud-42646-v4to",
            "acl-type": "ietf-access-control-list:ipv4-acl"
          }
        ]
      }
    }
  }
}
```

Establishing the Technical Basis for Trustworthy Networking

MUD Profiles



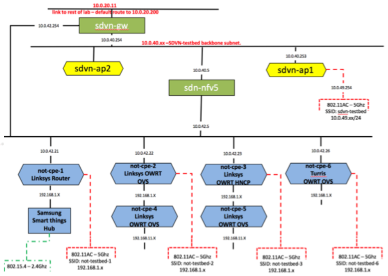
```
{
  "ietf-mud:mud": {
    "mud-url":
"https://toaster.nist.gov/.wellknown/mud/v1/super1",
    "last-update": "2017-10-16T22:10:33+02:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "https://mud.nist.gov/toaster",
    "from-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "acl-name": "mud-42646-v4fr",
            "acl-type": "ietf-access-control-list:ipv4-acl"
          }
        ]
      }
    },
    "to-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "acl-name": "mud-42646-v4to",
            "acl-type": "ietf-access-control-list:ipv4-acl"
          }
        ]
      }
    }
  }
}
```

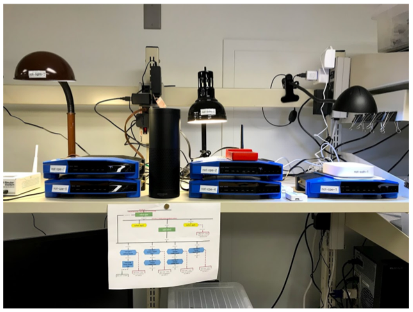


```
{
  "ietf-access-control-list:access-lists": {
    "acl": [
      {
        "acl-name": "mud-42646-v4to",
        "acl-type": "ipv4-acl",
        "aces": {
          "ace": [
            {
              "rule-name": "cl0-todev",
              "matches": {
                "ipv4-acl": {
                  "ietf-acldns:src-dnsname": "www.nist.gov",
                  "protocol": 6,
                  "source-port-range": {
                    "lower-port": 443,
                    "upper-port": 443
                  }
                },
                "tcp-acl": {
                  "ietf-mud:direction-initiated": "from-device"
                }
              },
              "actions": {
                "forwarding": "accept"
              }
            },
            {
              "rule-name": "ent0-todev",
              "matches": {
```

Phase 1 Prototypes

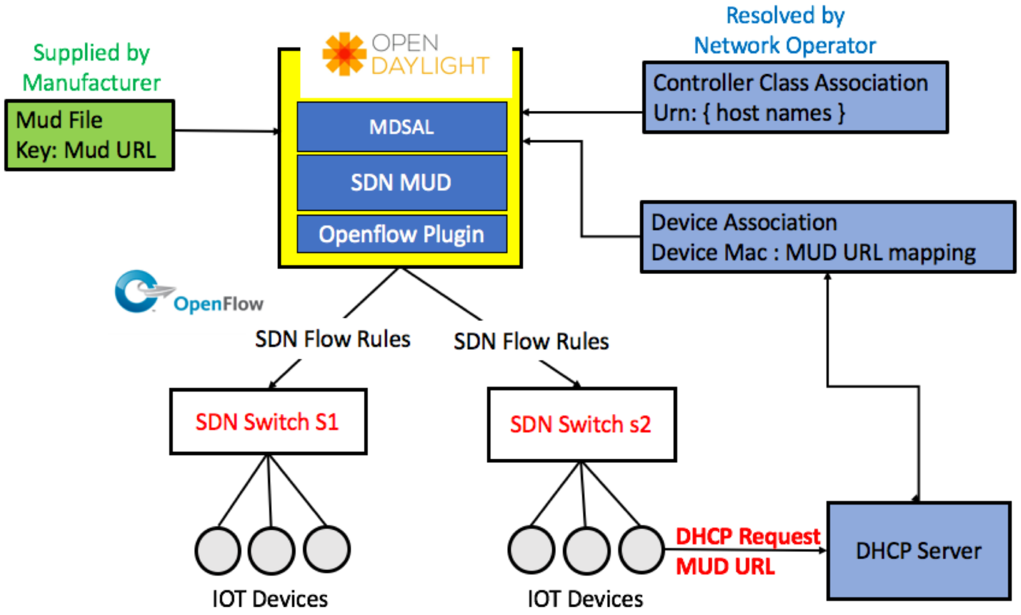
- **SDN-based MUD Architecture**
  - Simple MUD Controller,
  - SDN ACL application
  - MUD DHCP Client / Server Extension
- **SDN-based CPE**
  - Integrated OpenVswitch on consumer grade CPEs.
  - ACLs / Segmentation on ports and wifi.
- **OpenStack Elastic NFV IDS**
  - Load balanced Snort using open stack components.





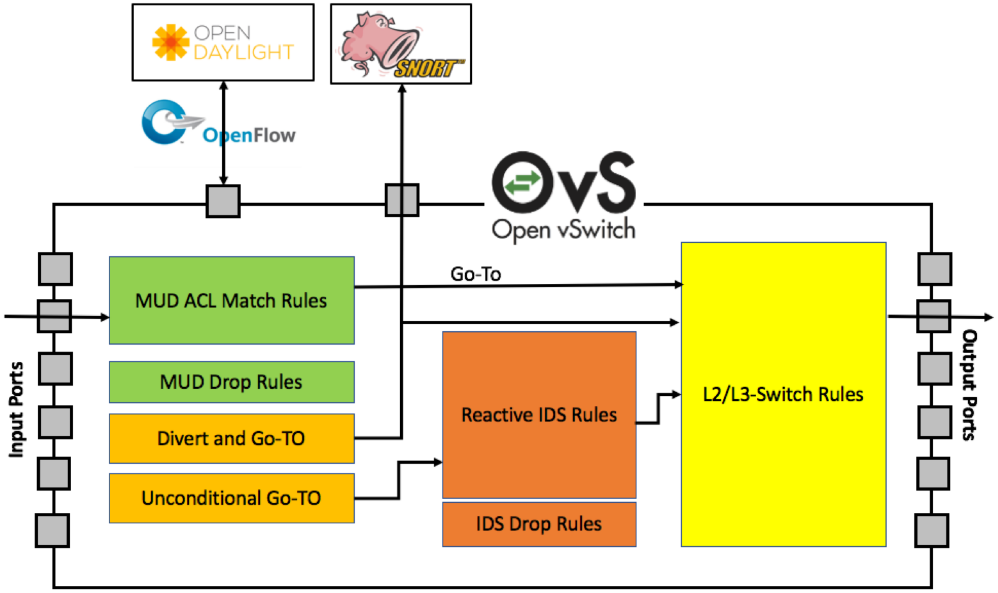
Prototype SDN / MUD Controller

- **SDN Aware MUD Controller**
  - Maps MUD ACLs into SDN Flow rules.
  - Resolves late bindings from MUD profiles and local network context



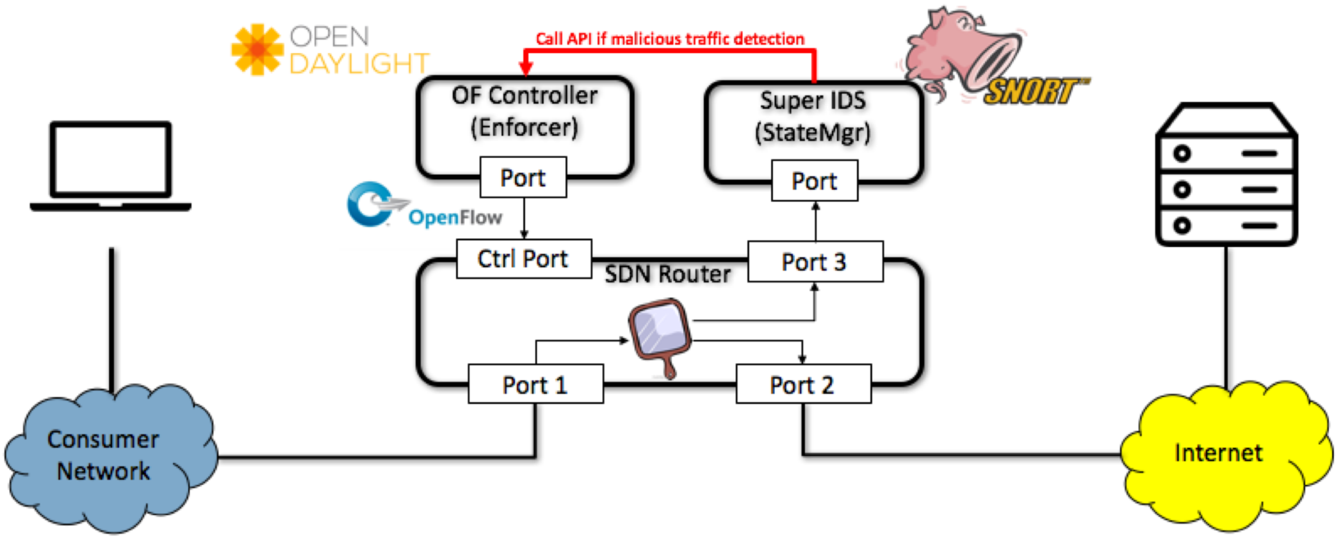
Multiple Flow Tables

- **Mapping of Network Control Polices to Flows**
  - Proactive MUD Policies
  - Reactive IDS Policies



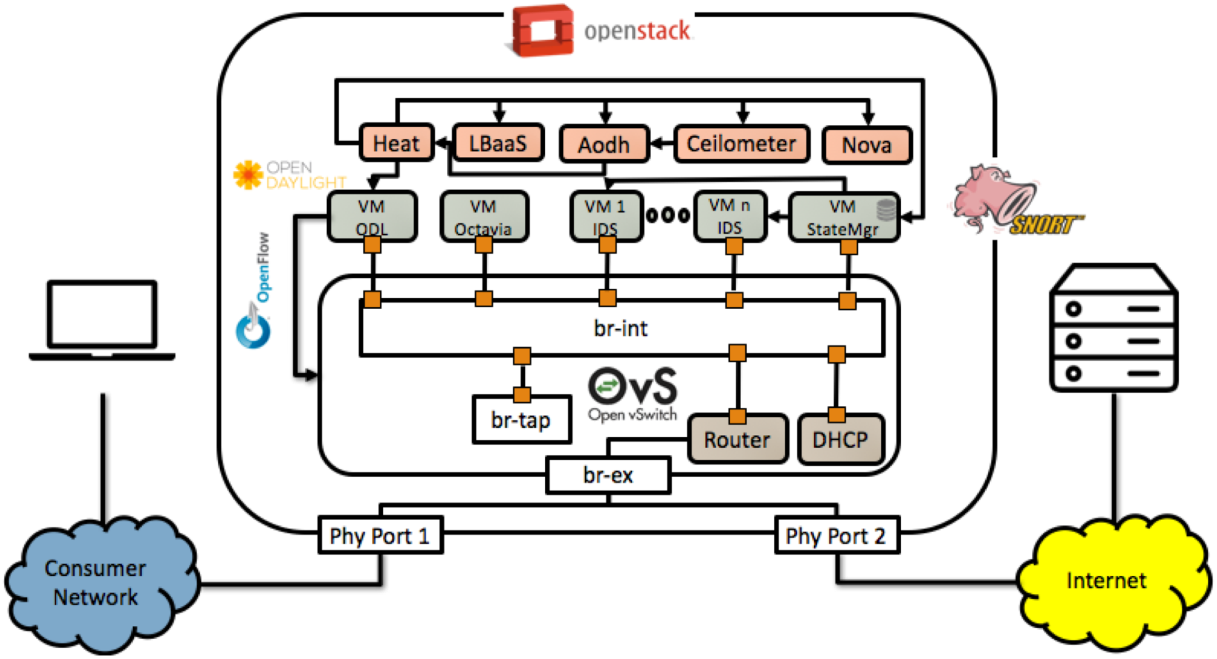
Elastic IDS NFV

- **SDN-Based Programmable Port Mirroring**
  - Suspicious flows diverted to deep packet inspection
- **Malicious Flows Blocked by SDN ACL Rules.**
  - Reactive ACLs use similar interface as proactive MUD ACLs



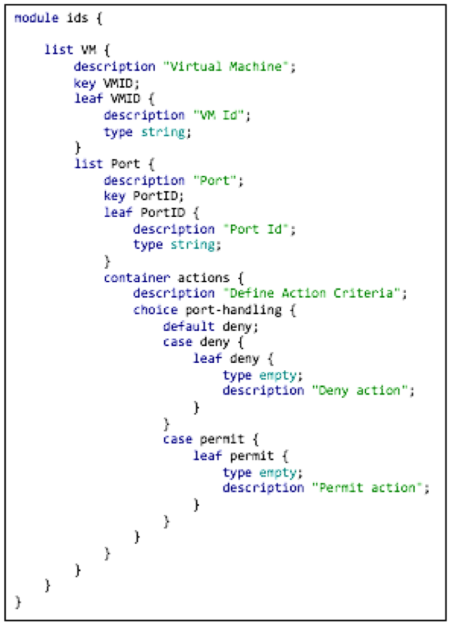
Scaling IDS NVF

- **OpenStack Virtualization Environment**
  - Using industry standard components for virtualization, load balancing, orchestration, and event management.



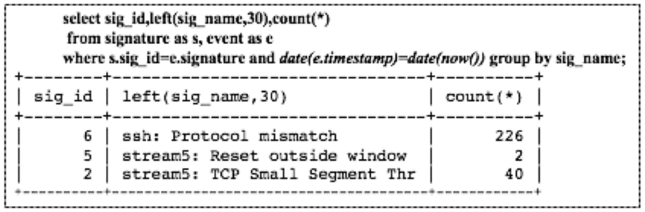
Reactive IDS Rules

- **OpenStack Telemetry and Alarming Infrastructure**
  - Process IDS alarms into REST API calls to ODL Enforcer application

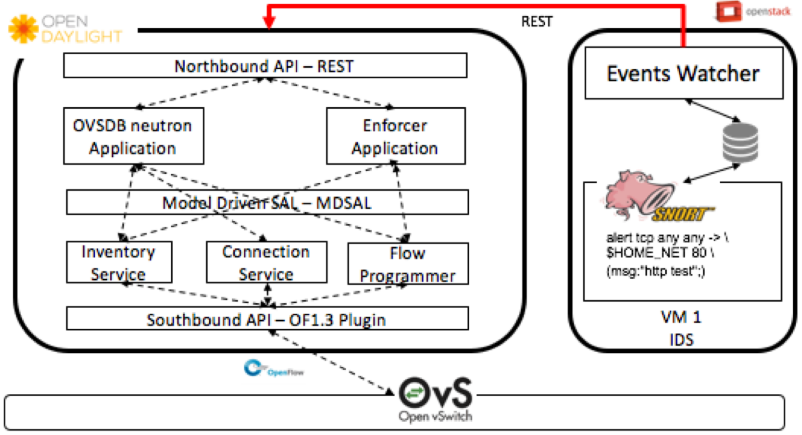


```
module ids {

    list VM {
        description "Virtual Machine";
        key VMID;
        leaf VMID {
            description "VM Id";
            type string;
        }
        list Port {
            description "Port";
            key PortID;
            leaf PortID {
                description "Port Id";
                type string;
            }
            container actions {
                description "Define Action Criteria";
                choice port-handling {
                    default deny;
                    case deny {
                        leaf deny {
                            type empty;
                            description "Deny action";
                        }
                    }
                    case permit {
                        leaf permit {
                            type empty;
                            description "Permit action";
                        }
                    }
                }
            }
        }
    }
}
```



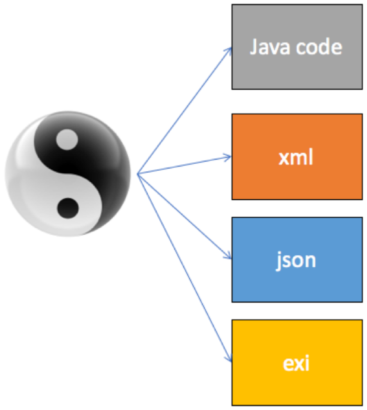
```
select sig_id,left(sig_name,30),count(*)
 from signature as s, event as e
where s.sig_id=e.signature and date(e.timestamp)=date(now()) group by sig_name;
+--------+------------------------------+----------+
| sig_id | left(sig_name,30)            | count(*) |
+--------+------------------------------+----------+
|      6 | ssh: Protocol mismatch       |      226 |
|      5 | stream5: Reset outside window |       2 |
|      2 | stream5: TCP Small Segment Thr |      40 |
+--------+------------------------------+----------+
```



Establishing the Technical Basis for Trustworthy Networking

Future Work

- **Research Prototypes → Industry Reference Implementations**
  - Re-implement SDN MUD Controller on OpenDaylight SDN Controller.
  - Use industry standard YANG models and tools to generate APIs.
- **Full Support of MUD Controller Semantics**
  - Support for MUD Controller classes (late binding) and other abstractions.
  - Stateful ACL rules, management of topology events, ACL placement algorithms.
  - Signature verification on MUD files.
- **Implement MUD support on widely used DHCP server**
  - DNSMasq for CPEs, BIND and/or OpenDaylight for Enterprise
  - Explore other means of announcing MUD URL – LLDP, IEEE 802.11AR, ANIMA.
- **Explore other means of generating MUD profiles.**
  - Use of machine learning and other means to create MUD profiles of legacy systems.
  - Explore usage profiles created by local network operator.
- **Enhance elastic IDS NVF**
  - Support topology placement algorithms and IDS optimization for different classes of traffic.
  - Couple with elastic IDS system for non-MUD devices.
- **Publish research results and release reference implementations.**



OPEN NETWORKING FOUNDATION

THE LINUX FOUNDATION

Questions and Discussion

- **For more information:**
  - Network Resilience Program
    - https://www.nist.gov/itl/antd/internet-scalable-systems-research
  - Advanced Network Technologies Division.
    - https://www.nist.gov/itl/antd
  - Information Technology Laboratory
    - https://www.nist.gov/itl