UiO : University of Oslo

Information & Cyber Security Research Group

Timely Incident Response

OpenC2

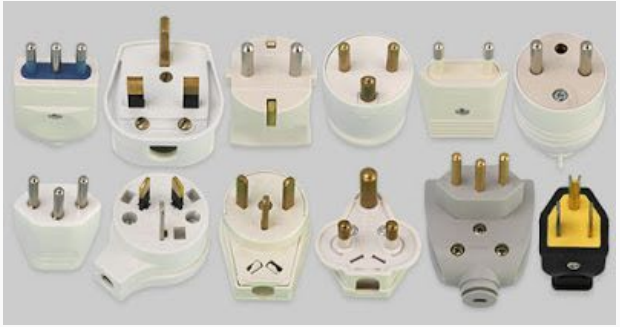
Vasileios Mavroeidis, *Security Researcher*
Information and Cyber Security Research Group
University of Oslo, Norway
Email: vasileim@ifi.uio.no

Kamer Vishi, *Security Researcher*
Information and Cyber Security Research Group
University of Oslo, Norway
Email: kamerv@ifi.uio.no

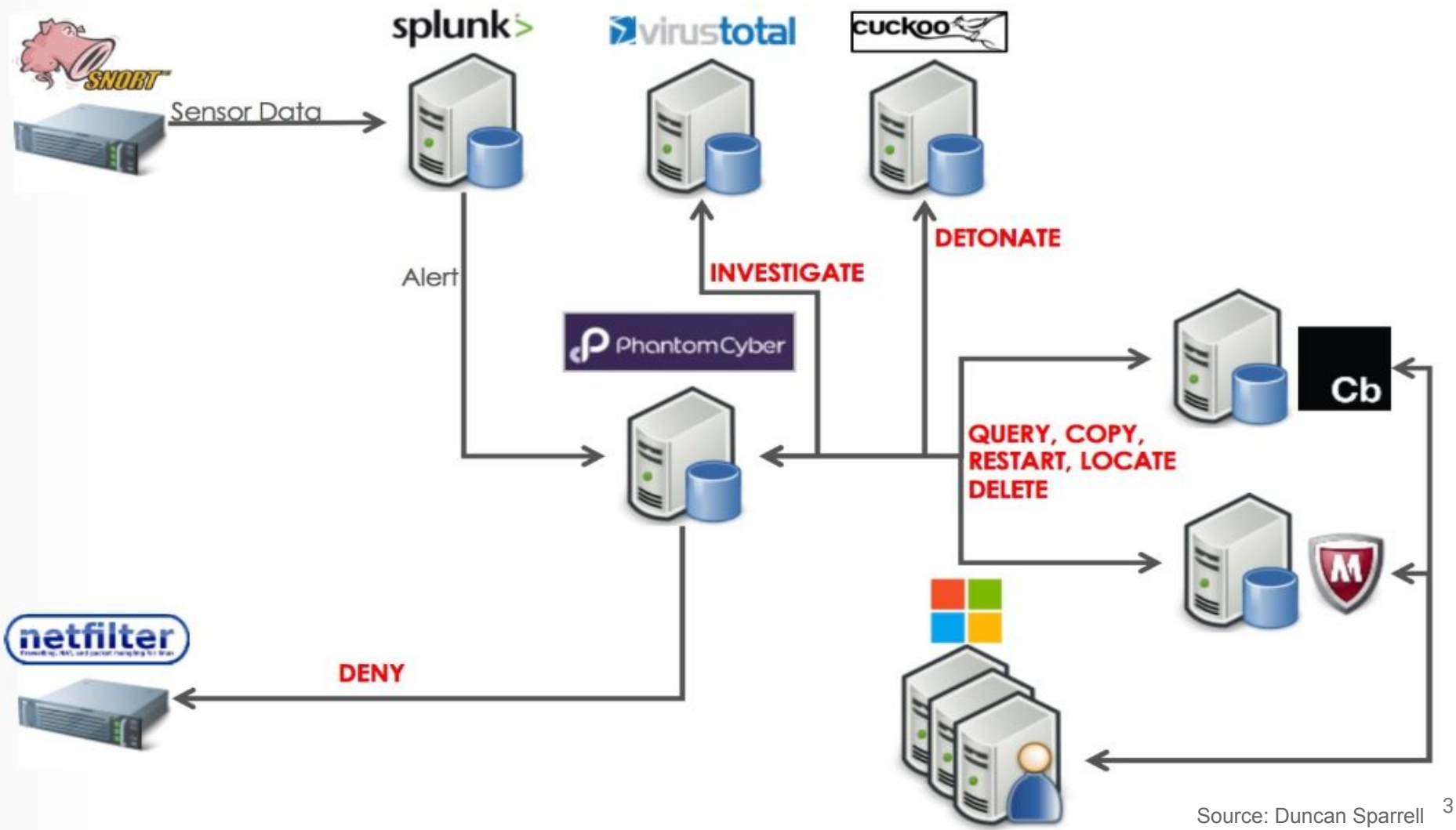
Cyber Defense of Today

- **Defenses are statically configured and operate in isolation**

- **Cyber Response**
  - **Slow - Time to implement**
  - **Manual**



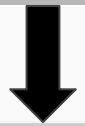
On average, it takes 214 days to identify a malicious or criminal attack, and 77 days to contain and recover [Carbon Black]



Source: Duncan Sparrell

Cyber Defense of Tomorrow

Defenses are DYNAMICALLY configured and are part of an ORCHESTRATION process



Coordinated Defense (multi-part response actions) in Cyber Relevant Time

"IOC might take 60 minutes to investigate manually can be researched in 30 seconds with Orchestration" [FireEye]

How?

- Need to speak the same language and protocols
- Need to share what we know about attacks in cyber-relevant time (CTI)


OpenC2

OpenC2 -- Automated Courses of Action?

Open Command and Control (OpenC2) is a concise and extensible language to enable machine to machine communications for purposes of command and control of cyber defence components, subsystems and/or systems in a manner that is agnostic of the underlying products, technologies, transport mechanisms or other aspects of the implementation.

3 Specifications

Title	Work In Progress (Google Doc)	Latest Published CSD (HTML)	Committee Specification / OASIS Standard
Language Specification	WD09	CSD07 / PDR01 17 Oct 18 PR01 CRM	Future
Stateless Packet Filtering Actuator Profile	WD05	CSD04 / PRD01 17 Oct 18 PR01 CRM	Future
HTTPS Transfer Specification	WD04	CSD03 / PRD01 17 Oct 18 PR01 CRM	Future

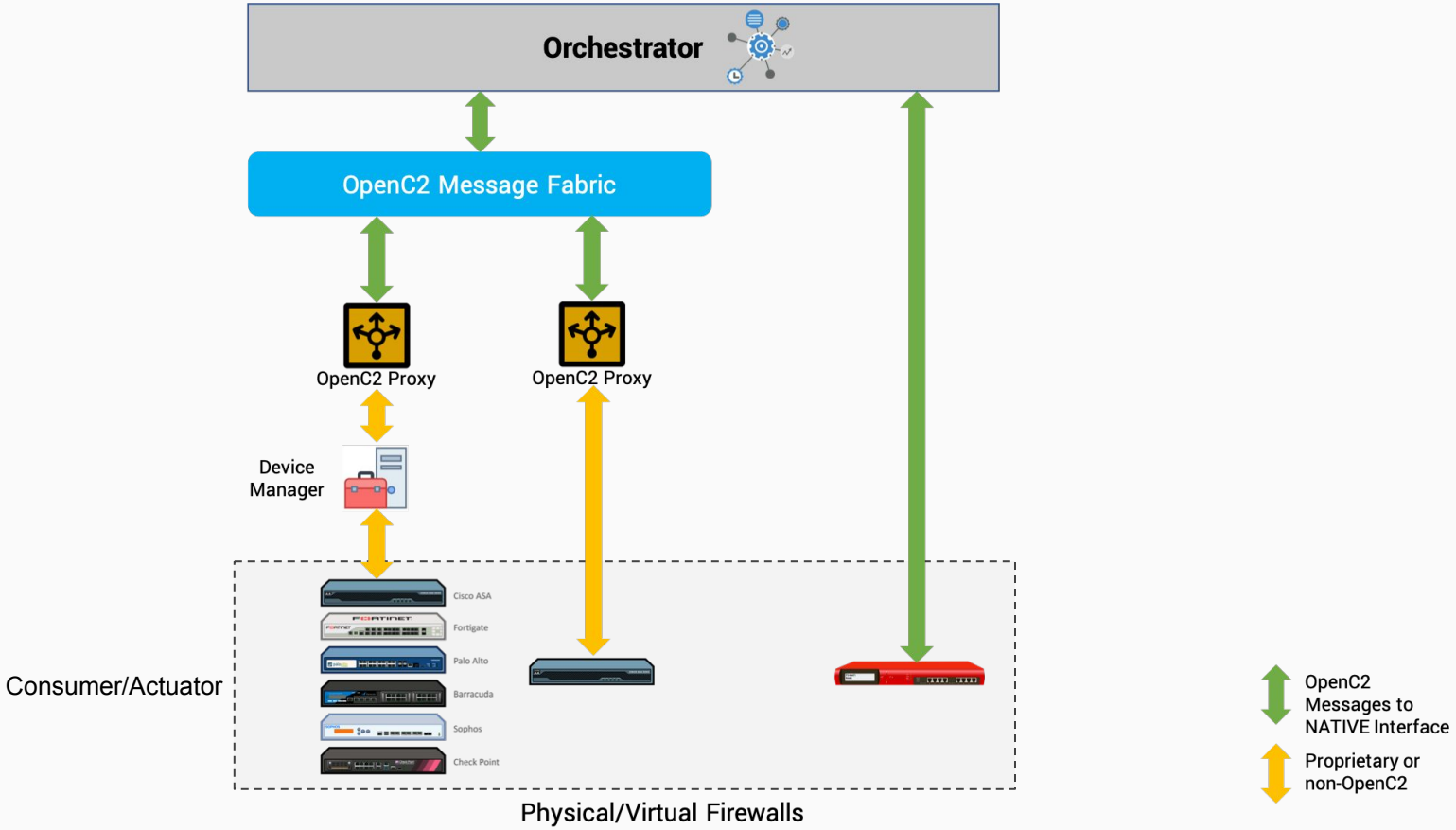
OpenC2 at a glance

- **Unambiguous Machine-to-Machine Communication**
- **Simplicity**
  - Low overhead on sensor and actuator
- **Focuses on the ‘Acting’ portion of cyber defense**
- **OpenC2 assumes the following has been done:**
  - Sensing: *What* triggers the action
  - Analytics: *Why*
  - Decision: *Which* action

OpenC2 Terminology

- **Actuator:** The device or sensor that executes a native OpenC2 command
- **Orchestrator:** Is a mission manager that will issue the OpenC2 commands to the appropriate actuators, and in the synchronous case, ensure the commands are executed in the correct order
- **Profile:** A minimum to implement set of OpenC2 commands that a class of actuators support
- **OpenC2 Proxy:** Provides a mapping of OpenC2 commands to and from devices that do not natively support OpenC2.

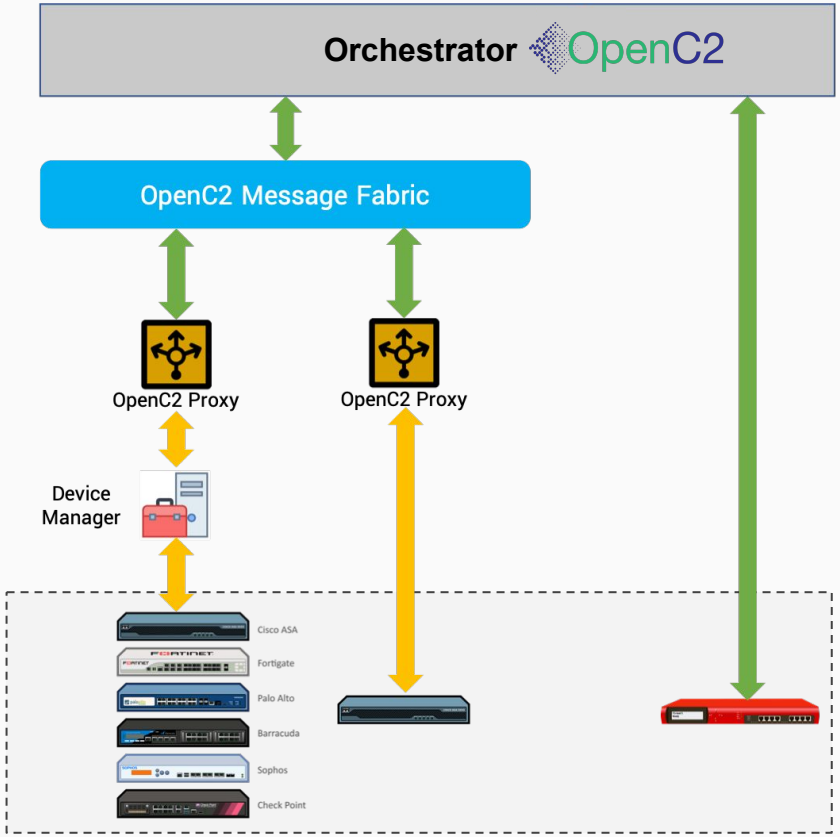
Notional OpenC2 Implementation for Firewalls



CTI + CoA = Automated CoA

CTI + OpenC2 = **Orchestrated** Automated CoA

Notional OpenC2 Implementation



+

STIX

Consumer /Actuator

OpenC2 Messages to NATIVE Interface

Proprietary or non-OpenC2

OpenC2 Syntax

- **Action**: The task or activity to be performed
- **Target:** The object of the action
- **Actuator:** The entity that performs the action
- **Arguments and Specifiers:** Additional precision to the commands or the actuators

OpenC2 - Stateless Packet Filtering (SLPF)

- **Example: Deny a particular connection**
  - Block a particular connection within the domain and do not send a host unreachable

OpenC2 Command

```
{
  "action": "deny",
  "target": {
    "ip_connection": {
      "protocol": "tcp",
      "src_addr": "192.168.1.1",
      "dst_addr": "81.167.155.132",
      "dst_port": 80
    }
  },
  "args": {
    "start_time": 1534775460000,
    "duration": 500,
    "response_requested": "ack",
    "slpf": {
      "drop_process": "none"
    }
  },
  "actuator": {
    "slpf": {
      "asset_id": "30"
    }
  }
}
```

OpenC2 Response

```
{
    "status": 200
}
```

OpenC2 Terminology

ID	Name	Description
3	**query**	Initiate a request for information. Used to communicate the supported options and determine the state or settings.
6	**deny**	Prevent traffic or access.
8	**allow**	Permit traffic or access.
16	**update**	Instructs the actuator to update its configuration by retrieving and processing a configuration file and update.
20	**delete**	Remove an access rule.

Actions Applicable to SLPF

ID	Name	Type	Description
10	**file**	File	Properties of a file.
11	**ip_addr**	IP-Addr	The representation of one or more IP addresses (either version 4 or version 6) expressed using CIDR notation.
15	**ip_connection**	IP-Connection	A network connection that originates from a source and is addressed to a destination. Source and destination addresses may be either IPv4 or IPv6; both should be the same version
16	**features**	Features	A set of items such as action target pairs, profiles versions, options that are supported by the actuator. The target is used with the query action to determine an actuator's capabilities.
1024	**slpf**	slpf:Target	Targets defined in the Stateless Packet Filter profile.

Targets Applicable to SLPF

Use Case

OpenC2 to Cisco

OpenC2 Schema

+ ASN.1 = JADN

```
...
{
  "action": "query",
  "target": {
    "openc2": ["schema"]
  }
}
...
```

Mapping: OpenC2 - Cisco

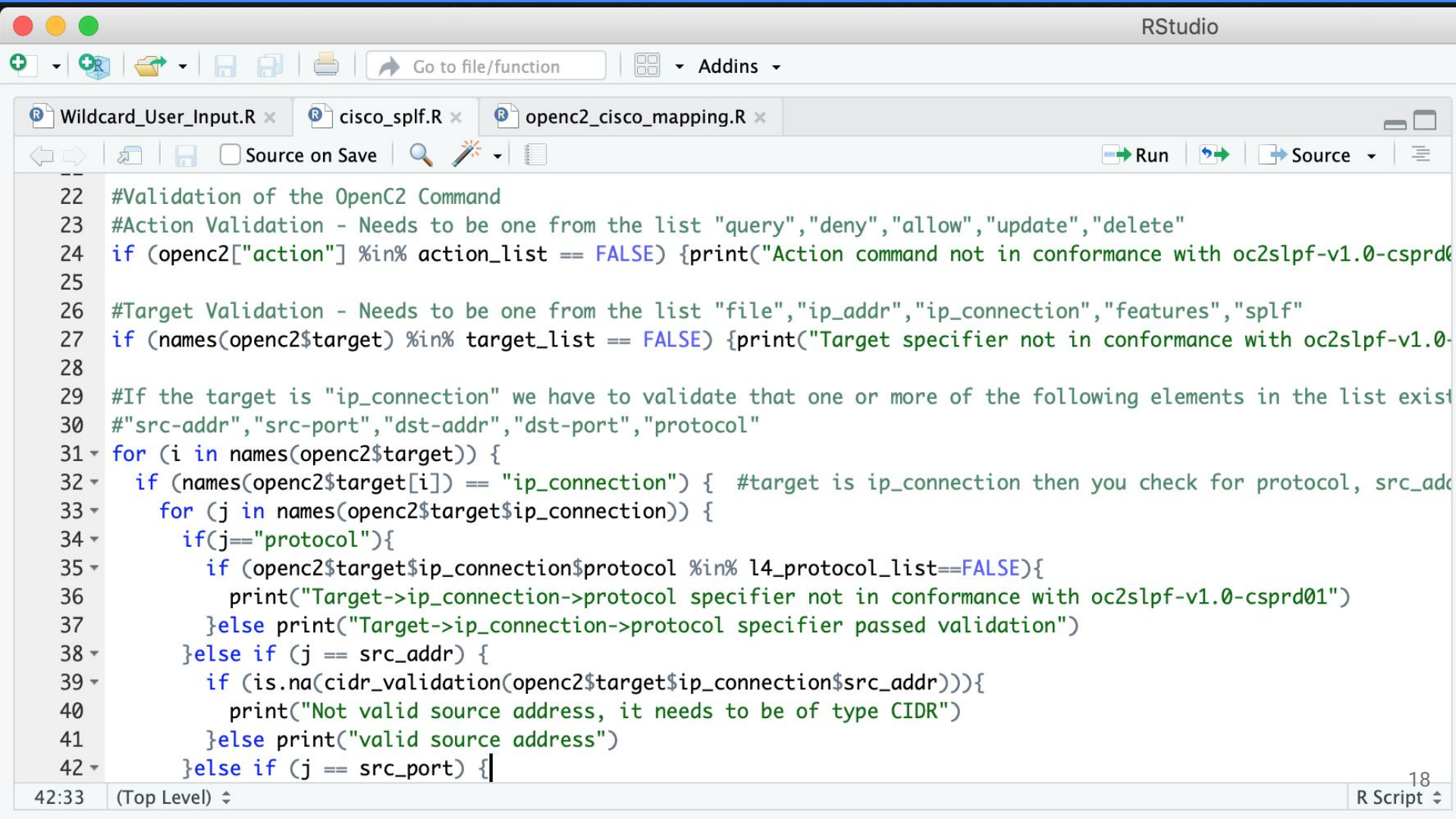
DENY

```
{
  "action": "deny",
  "target": {
    "ip-connection": {
      "protocol": "tcp",
      "dst_port": "22",
      "dst_addr": "172.20.52.0/24",
      "src_addr": "171.69.198.0/24"
                        }
              },
  "actuator": {
    "slpf": {"asset_id":"uio"}
                },
  "args": {
    "command_id": "tekna19_05022019",
    "response_requested": "ack",
          }
}
```

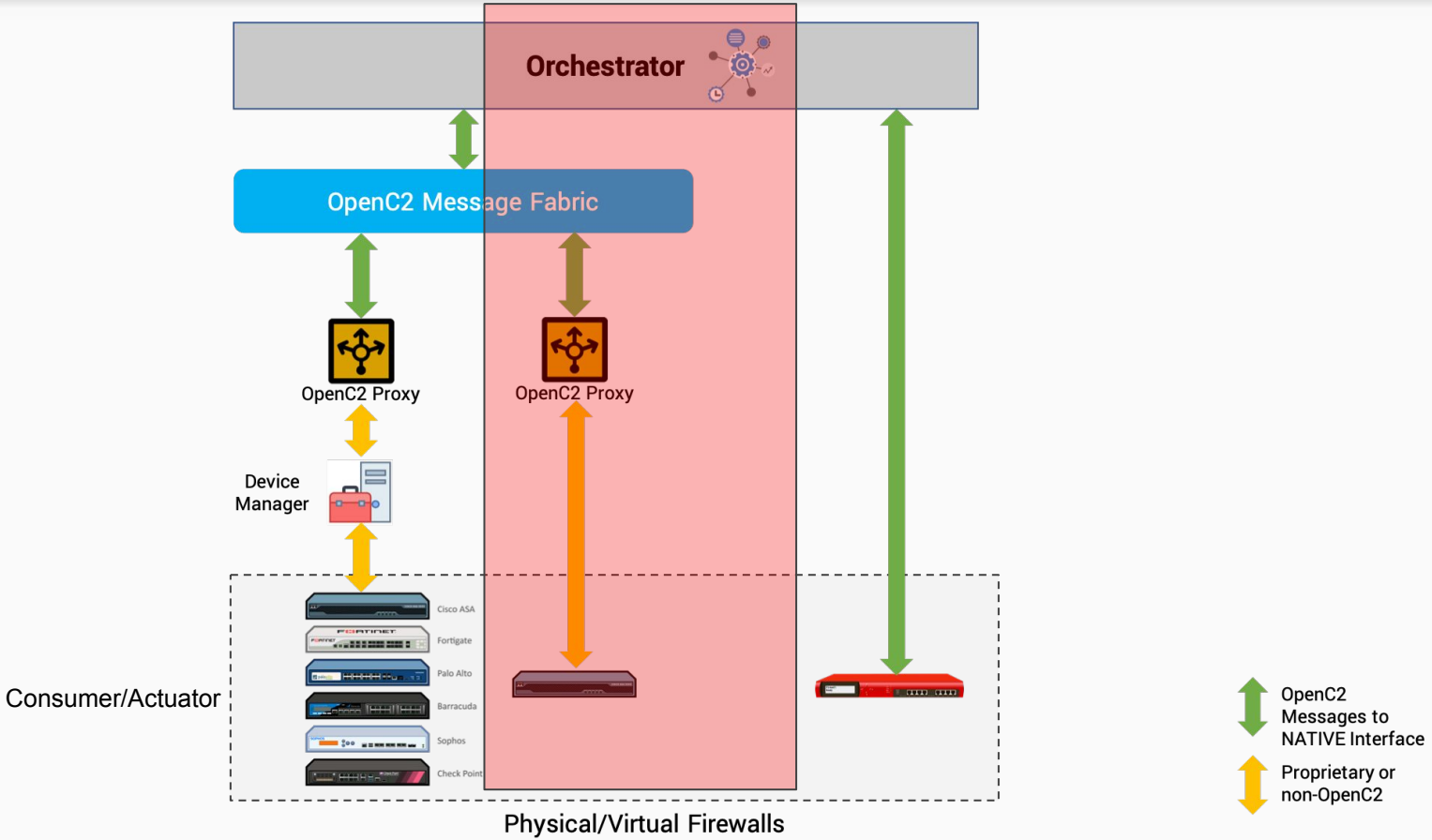
ALLOW

```
{
  "action": "allow",
  "target": {
    "ip-connection": {
      "protocol": "tcp",
      "dst_addr": "0.0.0.0/0",
      "src_addr": "0.0.0.0/0"
                        }
              },
  "actuator": {
    "slpf": {"asset_id":"uio"}
                },
  "args": {
    "command_id": "tekna20_05022019",
    "response_requested": "ack",
          }
}
```

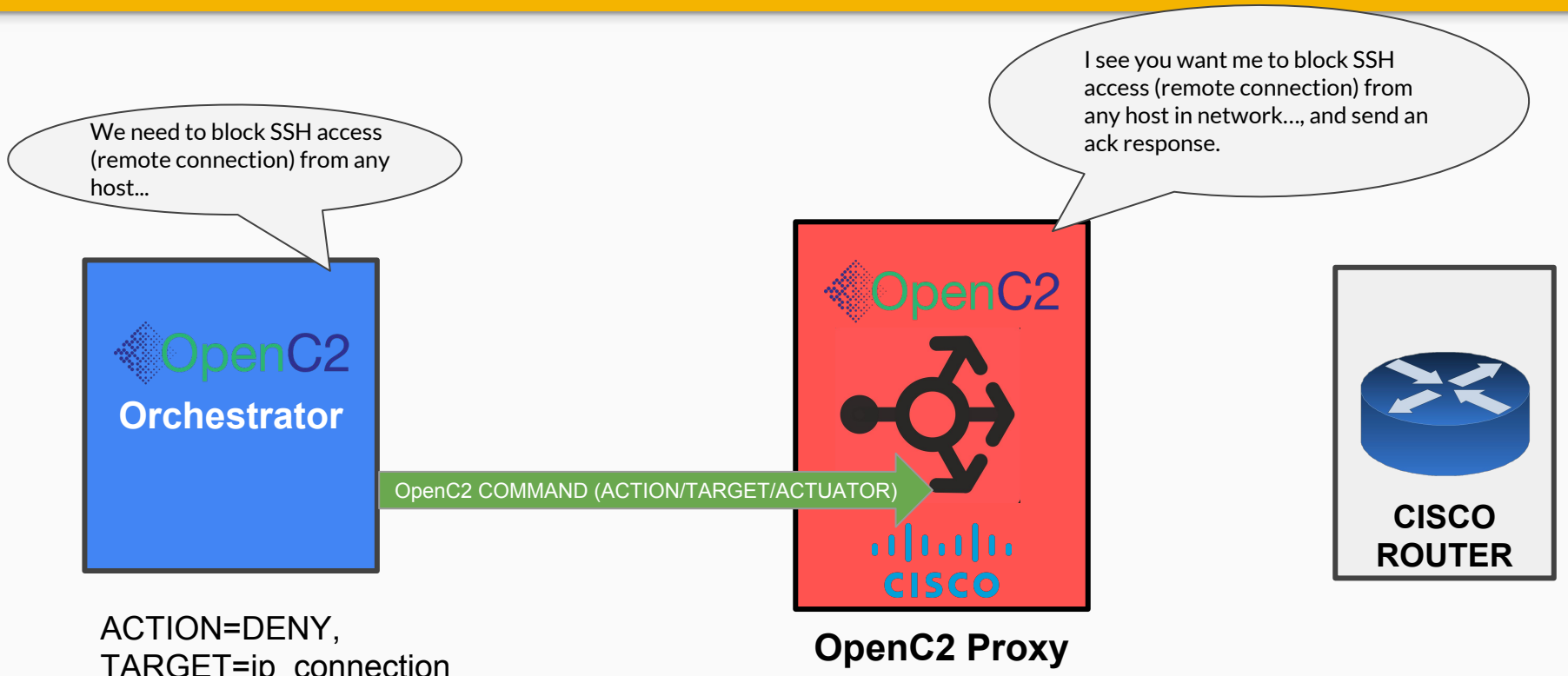
```
uio(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq ssh
uio(config)# access-list 102 permit tcp any any
```


RStudio
Go to file/function
Addins
Wildcard_User_Input.R
cisco_splf.R
openc2_cisco_mapping.R
Source on Save
Run
Source
#Validation of the OpenC2 Command
#Action Validation - Needs to be one from the list "query","deny","allow","update","delete"
if (openc2["action"] %in% action_list == FALSE) {print("Action command not in conformance with oc2slpf-v1.0-csprd0
#Target Validation - Needs to be one from the list "file","ip_addr","ip_connection","features","splf"
if (names(openc2$target) %in% target_list == FALSE) {print("Target specifier not in conformance with oc2slpf-v1.0-
#If the target is "ip_connection" we have to validate that one or more of the following elements in the list exist
#"src-addr","src-port","dst-addr","dst-port","protocol"
for (i in names(openc2$target)) {
if (names(openc2$target[i]) == "ip_connection") { #target is ip_connection then you check for protocol, src_add
for (j in names(openc2$target$ip_connection)) {
if(j=="protocol"){
if (openc2$target$ip_connection$protocol %in% l4_protocol_list==FALSE){
print("Target->ip_connection->protocol specifier not in conformance with oc2slpf-v1.0-csprd01")
}else print("Target->ip_connection->protocol specifier passed validation")
}else if (j == src_addr) {
if (is.na(cidr_validation(openc2$target$ip_connection$src_addr))){
print("Not valid source address, it needs to be of type CIDR")
}else print("valid source address")
}else if (j == src_port) {
42:33
(Top Level)
R Script

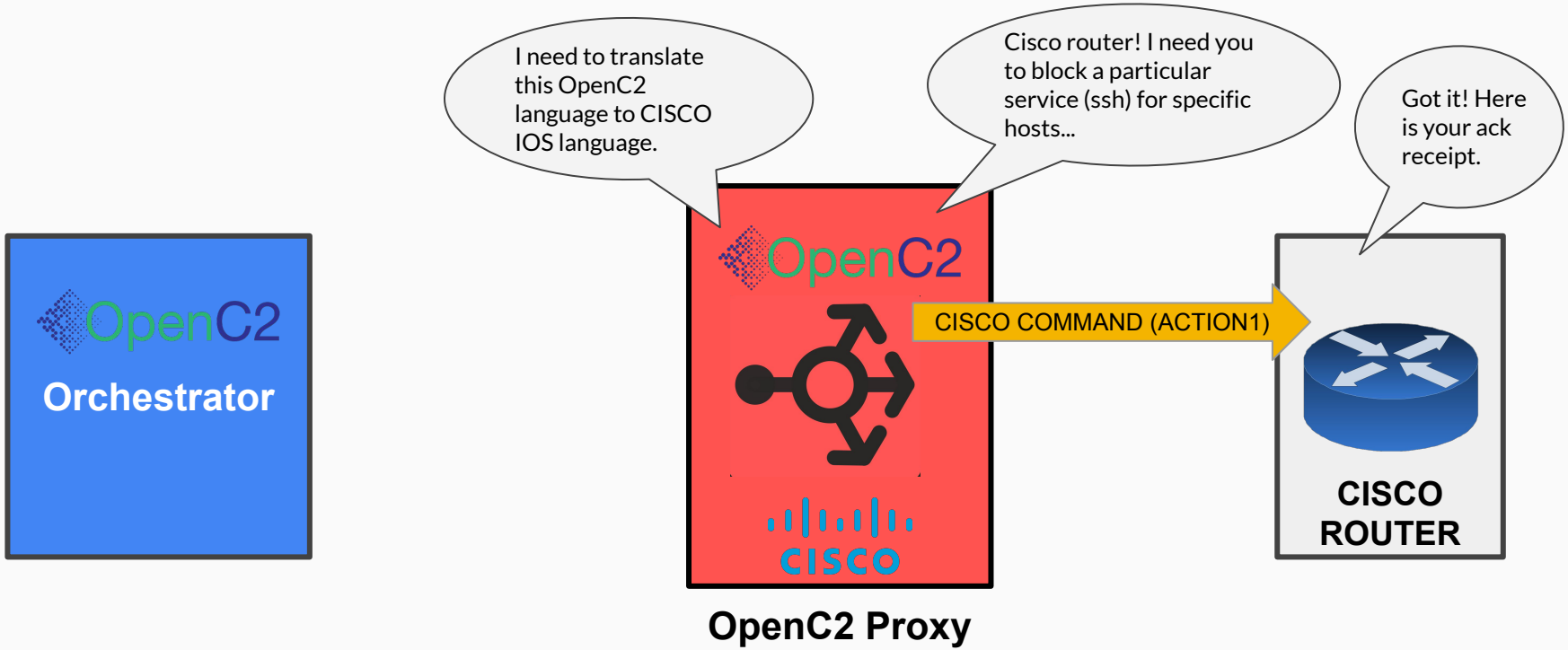
Notional OpenC2 Implementation for Firewalls



Command Workflow Overview

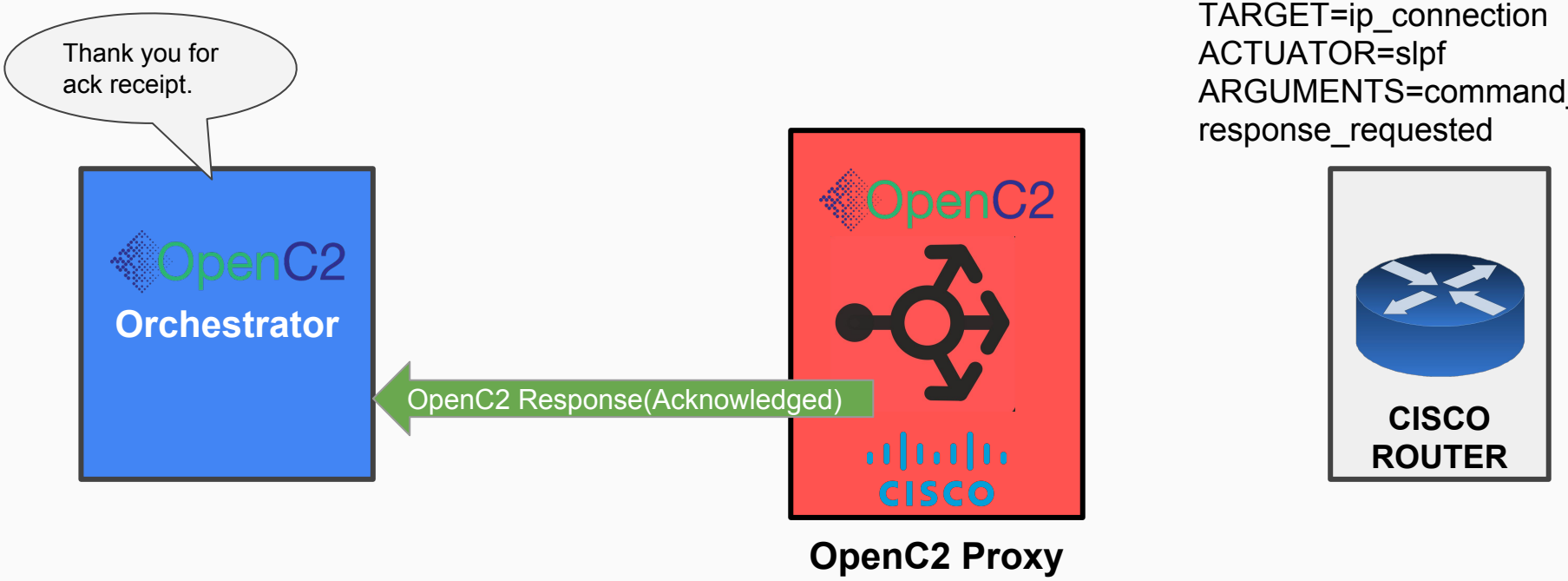


Command Workflow Overview



Command Workflow Overview

ACTION=DENY,
TARGET=ip_connection
ACTUATOR=slpf
ARGUMENTS=command_id,
response_requested



Who is OpenC2?

OASIS
Open standards. Open source.

CISCO

THREATCONNECT

Bank of America

Symantec

McAfee
Together is power.

FireEye

NEC

NCI AGENCY
NATO Communications and Information Agency

intel Security

TREND MICRO

eclectic iq

splunk>

SIEMENS

AT&T

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

IBM

MITRE

THREATQUOTIENT

... and many more!

visit OpenC2.org

Information & Cyber Security
Research Group

UiO : Department of Informatics
University of Oslo