Information Model of Interface to Network Security Functions Capability Interface

draft-xia-i2nsf-capability-interface-im-04

Liang Xia	Huawei
DaCheng Zhang	Alibaba
Edward Lopez	Fortinet
Nicolas BOUTHORS	Qosmos

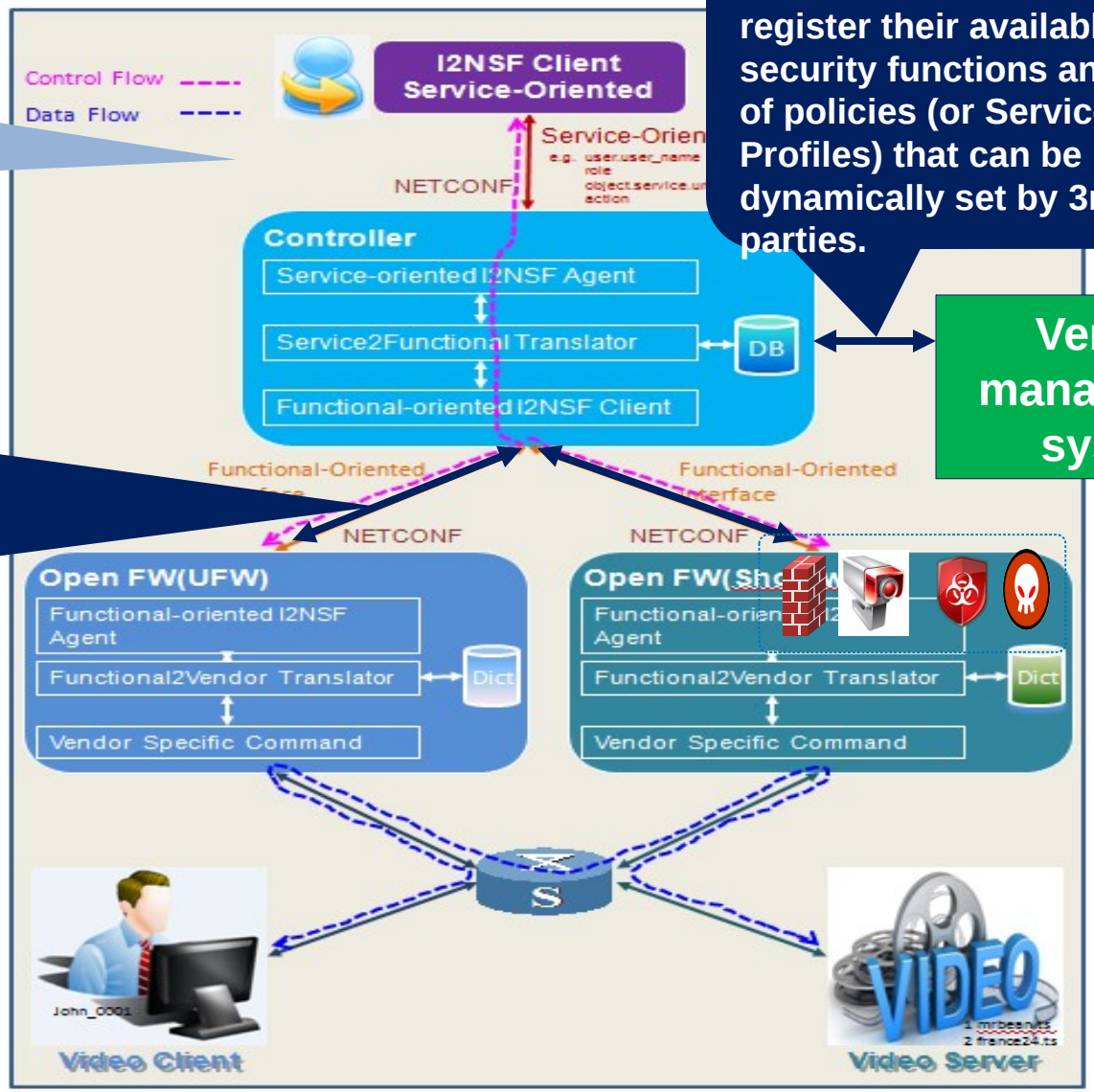
November 2015 Yokohama

Introduction of I2NSF Architecture

Security Service Layer
For clients or App Gateway to express and monitor security policies for their specific flows,

NSF Registration
For NSF vendors to register their available security functions and set of policies (or Service Profiles) that can be dynamically set by 3rd parties.

Capability Layer
For Controller to control and monitor the limited number of attributes (or Security capabilities) that are allowed by the respective vendors to the



Vendor management system

Current Situations of NSF (or Security Capability) Provisioning

- Security vendors use proprietary interfaces for NSF provisioning (i.e., SNMP, MIB, Restful, xml, syslog, etc);
- Various network security capabilities/functions provided by security vendors can not be integrated and applied as a whole. Furthermore, new network security capabilities are appearing quickly;
- NSaaS market grows very fast, which requires the automatic provisioning of massive NSF instances with high efficiency and flexibility.

Solution to Address the Problems Related with NSF Provisioning

- *A standard capability interface(by I2NSF)*
  - Decouple network security controller from security devices of specific vendors, and vice versa;
  - Only be oriented to the logic network security capabilities, independent with specific device implementation;
  - Flow-based paradigm builds a concrete basis for a large number of security capabilities.

Overview of Security Capabilities

- Network security control:
  - inspecting and processing the network packet/flow;
  - differ in the depths of packet headers and/or payloads they can inspect, the variou s flow and context states they can maintain, and the actions they can apply;
  - use a "Subject-Object-Action-Function" paradigm;
- Content security control:
  - one category of security capabilities applied to application layer that requires: Flex ibility, Generality, Scalability, Automation;
  - detecting the malicious contents: file, url, data block, etc;
  - Security profiles with standardized and configurable input/output parameters to co ntrol its specific functions and output results;
  - Standardized interface for updating its intelligence: signature, and algorithm.
- Attack mitigation control:
  - one category of security capabilities specially used to detect and mitigate various t ypes of network attacks: DDoS attacks, Single-packet attacks;
  - A standard interface is essential through which the security controller can choose and customize the given security capabilities to fight against various kinds of netw ork attacks.

Overall Structure for Information Model for security capability management

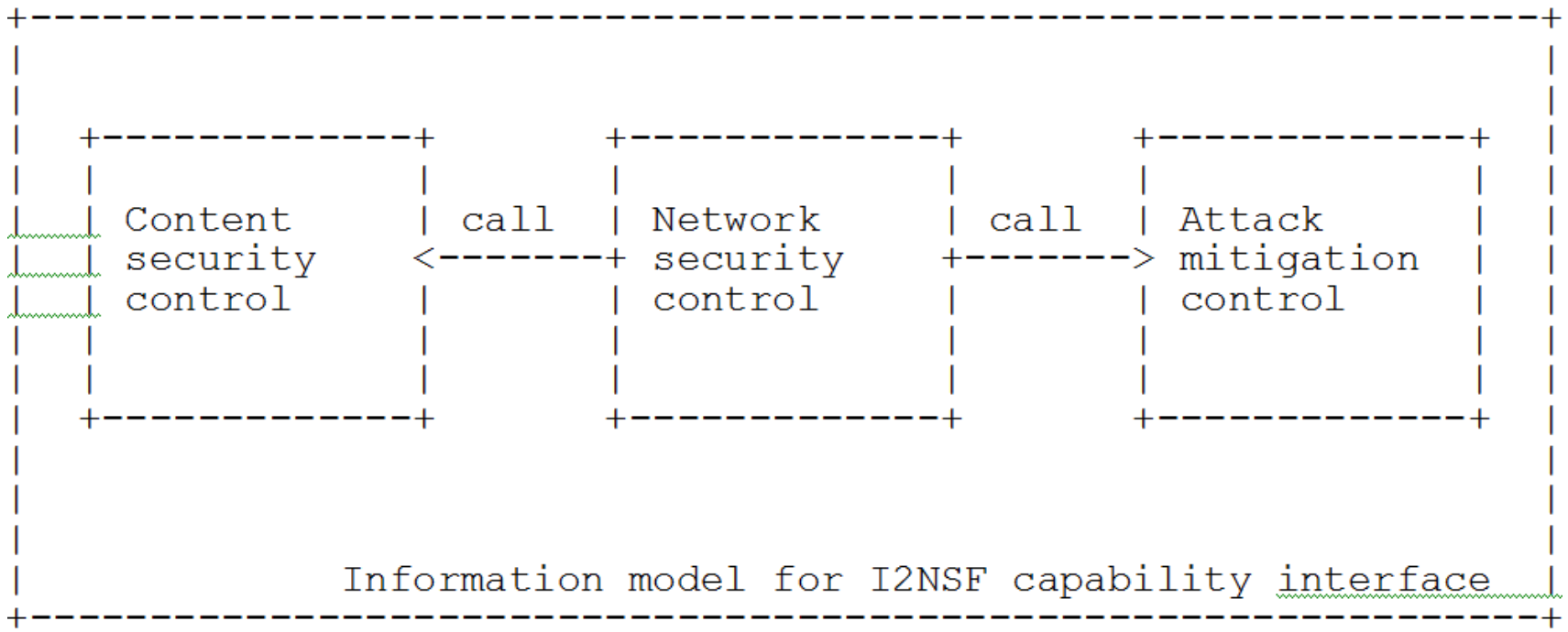


Figure 1. The overall structure of information model for I2NSF Capability Interface

Information Model for Network Security C ontrol Block

- Match values based on packet data

L2/L3/L4 Packet header
Packet payload

– Match values based on context

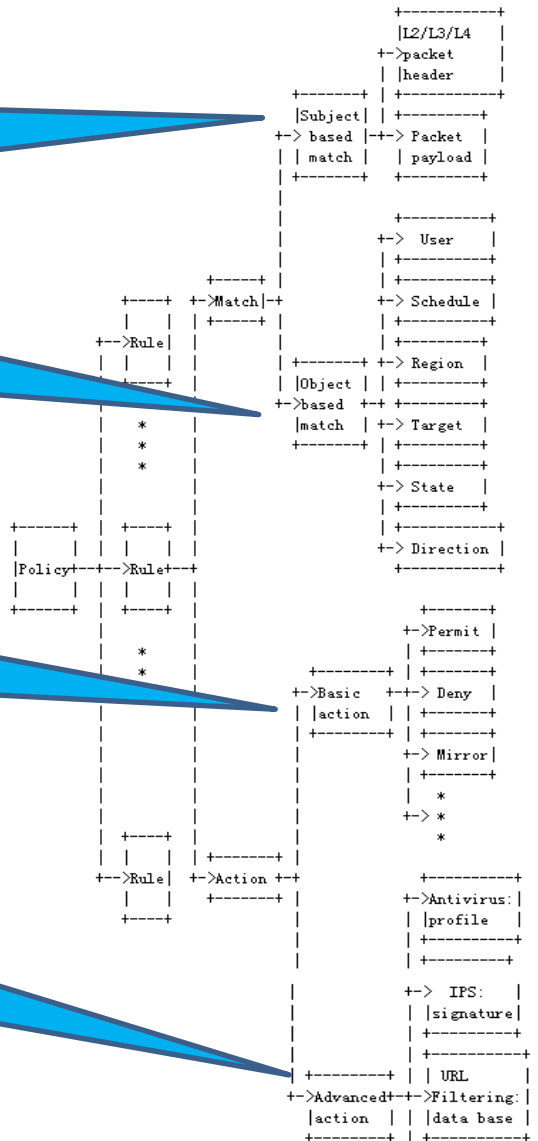
Ex.: user, Schedule, Region, Target, State, Direction, etc.
Many can (and should) be standardized, but many also from NSF capabilities

– Egress processing

Invoke signaling
Packet forwarding and/or transformation
Possibility for SDN/NFV integration

- Vendor Unique Innovation , Vendor specific

e.g. IPS:<Profile>
Profile: signature, Anti-virus, URL filtering, etc.
Integrated and one-pass checks on the content of packets



Key goal:

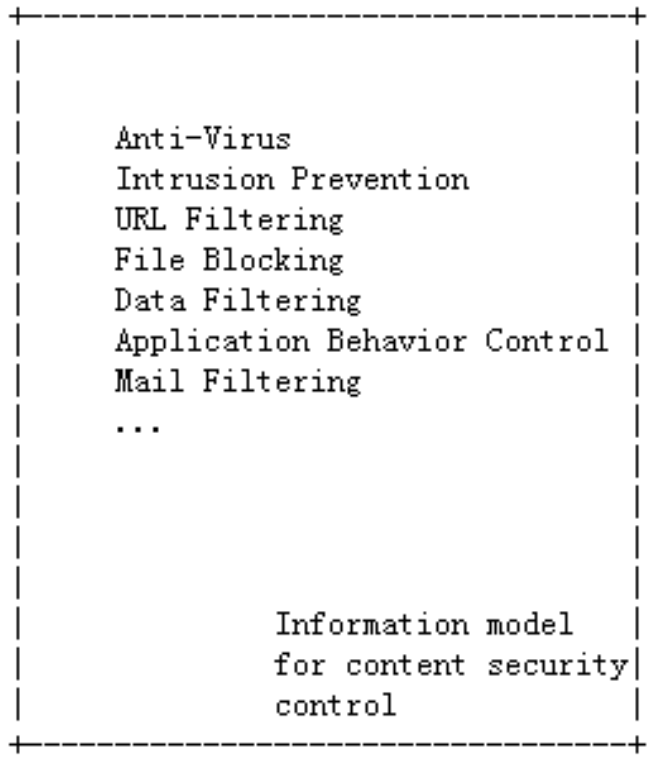
- Flexible and comprehensive semantics;
- extensible IM for containing different vendors' security capabilities, in essence, respective difference or innovation.

Match Condition Details

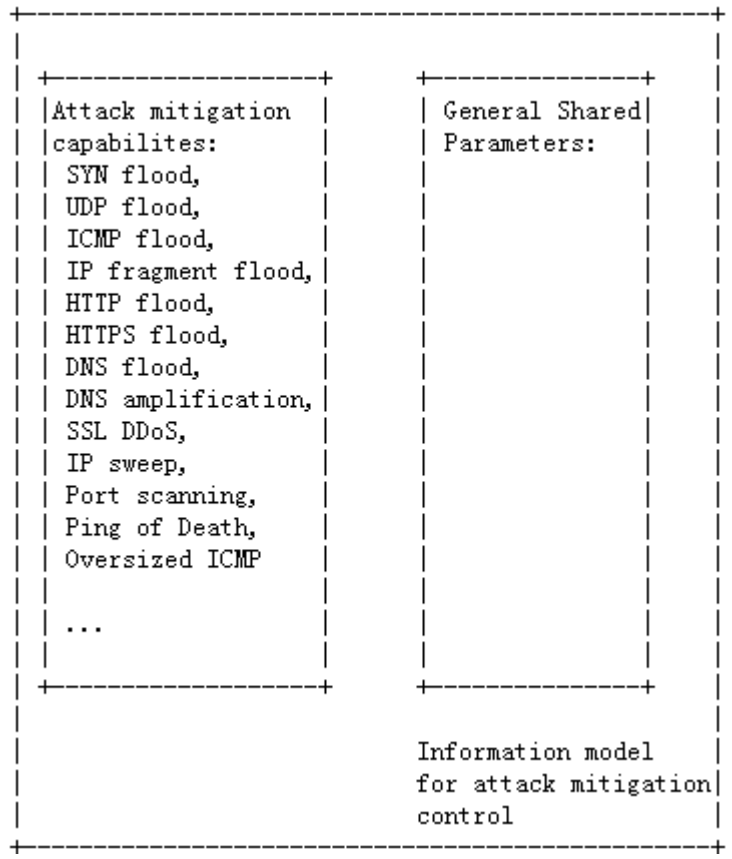
Match Condition	Attributes: Values
Ethernet Frame Header	Source/Destination address s-VID/c-VID/EtherType
IPv4 Packet Header	src/dest address protocol src/dest port length flags ttl
IPv6 Packet Header	src/dest address protocol/nh src/dest port length traffic class hop limit flow label
TCP SCTP DCCP	Port syn ack fin rst psh urg window

	sockstress
User	
Schedule	time span days, minutes, seconds,
Region	country, province, city IP address, network section, network domain
Target	service: TCP, UDP, ICMP, HTTP... application: Gmail, QQ, MySQL... device: mobile phone, tablet, PC...
State	session state: new, established, related invalid, untracked access mode: WIFI, 802.1x, PPPOE, SSL...
Direction	Direction: from_client, from_server, bidirection, reversed

Information Model for Content Security Control



Information Model for Attack Mitigation Control



Information Model Grammar Details

<Policy> ::= <policy-name> <policy-id> (<Rule> ...)

<Rule> ::= <rule-name> <rule-id> <Match> <Action>

<Match> ::= [<subject-based-match>] [<object-based-match>]

<subject-based-match> ::= [<L234-packet-header> ...] [<packet-payload> ...]

<L234-packet-header> ::= [<address-scope>] [<layer-2-header>] [<layer-3-header>] [<layer-4-header>]

<address-scope> ::= <route-type> (<ipv4-route> | <ipv6-route> | <mpls-route> | <mac-route> | <interface-route>)

<route-type> ::= <IPV4> | <IPV6> | <MPLS> | <IEEE_MAC> | <INTERFACE>

<ipv4-route> ::= <ip-route-type> (<destination-ipv4-address> | <source-ipv4-address> | (<destination-ipv4-address> <source-ipv4-address>))

<destination-ipv4-address> ::= <ipv4-prefix>

<source-ipv4-address> ::= <ipv4-prefix>

<ipv4-prefix> ::= <IPV4_ADDRESS> <IPV4_PREFIX_LENGTH>

<ipv6-route> ::= <ip-route-type> (<destination-ipv6-address> | <source-ipv6-address> | (<destination-ipv6-address> <source-ipv6-address>))

<destination-ipv6-address> ::= <ipv6-prefix>

<source-ipv6-address> ::= <ipv6-prefix>

<ipv6-prefix> ::= <IPV6_ADDRESS> <IPV6_PREFIX_LENGTH>

<ip-route-type> ::= <SRC> | <DEST> | <DEST_SRC>

<layer-3-header> ::= <ipv4-header> | <ipv6-header>

<ipv4-header> ::= <SOURCE_IPv4_ADDRESS> <DESTINATION_IPv4_ADDRESS> <PROTOCOL> [<TTL>] [<DSCP>]

<ipv6-header> ::= <SOURCE_IPV6_ADDRESS> <DESTINATION_IPV6_ADDRESS> <NEXT_HEADER> [<TRAFFIC_CLASS>] [<FLOW_LABEL>] [<HOP_LIMIT>]

<object-based-match> ::= [<user> ...] [<schedule>] [<region>] [<target>] [<state>]

<user> ::= (<login-name> <group-name> <parent-group> <password> <expired-date> <allow-multi-account-login> <address-binding>) | <tenant> | <VN-id>

<schedule> ::= <name> <type> <start-time> <end-time> <weekly-validity-time>

<type> ::= <once> | <periodic>

<service> ::= <name> <id> <protocol> [<protocol-num>] [<src-port>] [<dest-port>]

<protocol> ::= <TCP> | <UDP> | <ICMP> | <ICMPv6> | <IP>

<application> ::= <name> <id> <category> <subcategory>
<data-transmission-model> <risk-level> <signature>

<category> ::= <business-system> | <Entertainment> | <internet> | <network> |
<general>

<subcategory> ::= <Finance> | <Email> | <Game> | <media-sharing> |
<social-network> | <web-posting> | <proxy> | ...

<data-transmission-model> ::= <client-server> | <browser-based> |<networking> |
<peer-to-peer> | <unassigned>

<risk-level> ::= <Exploitable> | <Productivity-loss> | <Evasive> | <Data-loss> |
<Malware-vehicle> |<Bandwidth-consuming> | <Tunneling>

<signature> ::= <server-address> <protocol> <dest-port-num> <flow-direction>
<object> <keyword>

<flow-direction> ::= <request> | <response> | <bidirection>

<object> ::= <packet> | <flow>

<context based match> ::= [<user-group> ...] [<session-state>] [<schedule>]
[<region-group>]

<user-group> ::= <user>...

<user> ::= (<login-name> <group-name> <parent-group> <password>
<expired-date> <allow-multi-account-login> <address-binding>) |
<tenant> | <VN-id>

<session-state> ::= <new> | <established> | <related> | <invalid> | <untracked>

<schedule> ::= <name> <type> <start-time> <end-time> <weekly-validity-time>

<type> ::= <once> | <periodic>

<action> ::= <basic-action> [<advanced-action>]

<basic-action> ::= <pass> | <deny> | <mirror> | <call-function> | <encapsulation>

<advanced-action> ::= [<profile-antivirus>] [<profile-IPS>] [<profile-url-filtering>]

Next Step

- Solicit Comments

  - Keep on improvement, including:
    - control security control IM;
    - attack mitigation control IM;
    - improving information model structure and grammar.

Thanks!

Liang Xia (Frank)