I2NSF 11/3/2015 9:00am - 11:00am Japan time

Meeting Recording:
http://recs.conf.meetecho.com/Playout/watch.jsp?recording=IETF94_I2NSF&chapter=chapter_1

Administrivia and Agenda Bash
Chairs (5 minutes : 5/150)
Discussion:

- Any changes to the agenda?

2. Reminder of Purpose and Focus of I2NSF
Chairs (10 minutes : 15/150)
Discussion:

- Daniel Migault (Ericsson): You mention that it is not the policy for the working group will work on. I saw in the use cases there are policies like “I want my son not be able to access some website during certain period of time”. Is it policy or not policy for the client?
- Linda Dunbar (Chair) This is about policy, but it is at more abstract level. We are focusing on policies/rule sets that can be implementable, such as Zone 1 can talk to Zone 2, which can be mapped to implementable.
- Daniel Migault (Ericsson): (missed)
- Linda Dunbar (chair): We are trying to focus on what can be implemented.
- Edward Lopez (Fortinet): Your example is what we do, but not at implementable way. Our intent has to be technical capability that can be implementable. This is invocation of what we do. One of the problems we are attempting to defined what a policy. This cannot be just architected, it must be defined and implemented.

3. Deliverables and Milestones
Chairs (10 minutes : 25/150)
Discussion:

- Luyan: In general things the header is correct, but there are differences. I would like to talk offline about these errors.
- (xxx): light blue shirt:

4. Problem statement
draft-dunbar-i2nsf-problem-statement
Sue Hares (15 minutes : 40/150)
(see the comments from jabber room)

Adrian: We are all security people now. But it reminds me to check who you consider you are, please raise your hand if you consider yourself as Security person, Networking person or YANG/OpsManagement person.

[About 1/3 raised their hand for considering themselves as “Security person”.] We will be leaning on the security people for the work.

Adrian: During the BOF, there is overlap between problem and use cases. Is there anyone not thinking Sue hasn’t covered the problem space and the use cases?

Ed Lopez: it is not that you haven’t covered anything. Suggests "new forms of security" will emerge from this work. That is not a missing piece of the problem statement, but may be an important outcome. When you talk about networking/forwarding, there is form of security to guide where the traffic can go. Our company is already releasing new Restful APIs for traffic security.

Sue: Chairs: should this to be captured.

Adrian: we may need to capture it as the possible outcome of the work.

Xxx: The charter says that Service Layer and Capability are pretty same. But this graph clearly shows that there are clearly differences between Service Layer and Capability Layer.

Adrian: I am not saying they are the same. But the translation from Service Layer to is out of the scope.

XXX:

Roland Dobbins (Arbor Networks): one of the desires is to facilitate security orchestration.

Sue: That policy validation is what I have done for a long time as a Chair to IDR.

LuYuan Fong (Microsoft): when we talk about policy validation, we need to have exchange information. Today, we don’t have this interface.

Sue: In BGP, we have T

Roland: A lot of what have done is policy.

Sue: if you could send me the policies validation that I have missed, please send to me.

John Strassner: There are also verification elements for policy. There is one thing of the policy is what I said, there is another thing to validate if the policy is accurate. I hope you add this to the problem statement.

Daniel (Ericsson): We only need to verify if the policy match my intent.

John Strassner: it is deeper than that. My intent is move X to Y, but what happens is moving X to Z. is there any recovery path to move data from Z back to Y?

Diego Lopez (Telefornic): asks about combination of policies

John Strassner: it is one thing to say Adrian getting Gold Service. But if I don’t know Adrian, the service may not be correct.

Diego Lopez: let me remark: the

Sue: my question: are you considering federate policies, or individual policies on top of another?

Diego: both.

Adrian: We need to work with SUPA to draw a line on the policies done by SUPA and by I2NSF.

5. Use Cases and Gap Analysis
draft-hares-i2nsf-use-case-gap-analysis
Sue Hares (20 minutes : 60/150)
(see the comments)

LuYuan (Microsoft): For Cloud Providers, there are virtual security functions within my cloud, there are also virtual security function services that cloud providers provide to their client. Virtual Security Functions vs cloud provider: I hope we cover both including cloud-based security service. I.e. security for cloud and security provided by cloud

Ed Lopez: the difference is if we are responsible for instantiating the service functions. Taking the instantiation out, relative to our work, it doesn’t make any difference whether the FN is virtual or not.

Ed: when we talk about use cases, it makes sense to talk about virtual NSF. But for our work, it doesn’t make much difference.

XXX: the first bullet is contradicting to what we just said.

Sue: that is right. The creation of NSF is out of scope.

Kathleen Moriarty (via Jabber room): Don't worry, I will put mic: in front of it. I don't think that comment was worth interrupting, but can talk to Sue about it and the types of sensitive data going into hosted environments connected to the Internet (not public clouds).

Dean Bogdanovic: the ACL didn’t do any stateful filter. Hope you can cover.

Jamal speaks: asks what are stateful filters for. Who installs the state?:

Ed Lopez: There is dependency that the mechanisms to deliver packets to NSF, and how NSF treat packets presented to it. Statefulness is within NSF itself.

Sue: is there anything in the policy to state symmetry in the services. There is symmetry for traffic.

Linda: enforcement for the direction of traffic, for example, Zone 1 can only send traffic out, and can only receive traffic responding to its own initiated traffic. I2NSF only covers the expression of the policy, but doesn't cover how NSF enforce the "State".

Ed: when I say "symmetry", I mean traffic following the same path. How policy delivery packets to NSFs. There is also the state within NSFs. That is why we need a terminology document. Otherwise we will run into trouble. Ed volunteered to do a terminology document.

Jamal: what happens when the NSFs are not capable of taking the "stateful"

Adrian: when NSFs can't handle "stateful", it should deny the requests.

Roland: when you try to have overlay paradigm, don't you want to move to outcome method? Clients only need to express the outcome. The security orchestration takes the requests from Clients and choose whatever NSFs that can fulfill the requests.

Eric Wang (Cisco): Policy filtering should be in the scope.

Diego Lopez: We need common ground.

Sue: we need to work on the terminology with Ed.

Adrian: editorial question. The charter says that those two documents can be merged together.

Sue: I will work with Ed on terminologies and then merge the document.

6. Framework
draft-merged-i2nsf-framework
Diego Lopez (15 minutes : 75/150)
[scribe needs to have names for speakers at the mike]

Comment:

- Diego: DevOp is popular, we may need to include the DevOps. Looking forward to integrate what we don't know

- Uri: (Intel) - I am involve with the SFC work. Are putting Service funtion chaining or optimizer is in the security framework or not? Is Security devices separate from other devices?

- Ed Lopez: SFC is about delivering traffic to the door. I2NSF is about how to treat packets delivered to my door.
- Uri (Intel): we are really focusing how to treat packets, but not how the traffic is delivered to my door.
-
- Dan: We are looking at what happens when the service
- Uri (Intel): There are two interfaces for NSFs: one interface is how NSF is connected to network; another interface is for informing how to treat packets for packets delivered to my door. Are we connected to the network and what entity is the security person of the device?
- Ed Lopez: my believe is that one job of Security Function is to determine if a packet should be forwarded. Therefore, Forwarding is part of Security Functions.

- Dan: (missed)
- XX (red shirt): The key is the translation of the service oriented policy down to the implemented
- XX(black shirt): The packet passes through the node you operate it based on rules. Is it not possible to operate on a packet as a service function.
- Uri (Intel): I think based on the packet processing being handle by multiple devices as network elements are creating the service function. If we are taking to regarding the security function. If we are carving out a special domain for policy with one area for network policy and one for
- Ed Lopez: If a router is capability of filtering, it may present this to the INSF manager. The router has the possibility of forwarding and filter. This is the composite devices.
- Xx (Red shirt): Multiple devices have a scenario where multiple instances operate to do the security and routing. We have a con
- Ed Lopez: It may be subject to the vendor/organization that craetes the device.
- xx (black shirt): Each device that handles packets have security (routers, forwarders, security). The precedence between these is key, and policy sets.
- Ed: I agree with you. My personal opinion is that security device.
- [Adrian] We need to provide

[Discussion 2]

- Eric Wang [Cisco] What is the scope of the subject of header versus payload? Do we include or interface?
- Ed: In my viewpoint, it is the packet that we receive is “Subject”.

- Eric Wang [Cisco]: This is a match criteria.
- Ed: The time of day, interface, and other is context. The object matches on the context.

- Eric (xx): My question was the policy model will cover what happens based on the match criteria (Match packet data, match on context). Will I learn from my policy match processes?
- Ed: This outside outside our scope. This the green
- Adrian: I
- Uri (intel): If wE agree to our topology is out of the framework.
- (red shirt): What is a email gateway? Is it NSF packets.
- Ed: My viewpoint that it is a packet.
- Diego: We have a terminology gap. What receives the action? Is it about circumstance or conditions? We see block, filters, and other issues. We can have simple devices, and then complex devices with lots of filters and analysis. I hope we will be able to review.
- John: There is a large body of policy of literature which states the policy - not as the match condition but the objects. The action to perform the function is part of the outcome.
- Ed: In my first work, I suggested that the function was an output.
- John: This is declarative or imperative.
- Luyang: Our interest in the service layer.
- Diego: My colleague back who is in Italy is also interest in the service layer.
- John: I will volunteer myself because this overlaps with SUPA.

Question:
- John: In PICM (3460), the roles are broken. SUPA builds and fixes it.
- Dan: I agree with you. I look to the others

[10:34am JT)

Adrian - This is one of the most constructive discussions.

7. Information Model of Interface to Network Security Functions Capability Interface
draft-xia-i2nsf-capability-interface-im
Frank Xia (15 minutes : 90/150)
Discussion on slide 5:
- Diego: Reading the draft, we have described functions without the terminology. We need to carefully define the characteristics. Our distinctions we are making between about the terms network security, content, and attack mitigation.
- Frank: We are pleased to get comments from all of you. If the detail is too detailed, then we need aid to be careful about the details of the terms.
- (light blue shirt): Can you use time of day for my employee?
- Frank:
- Diego: Did you plan to put this in yang model?
- Frank: Just information model?
- Diego: The models can be derived from the XML. There exist 90 models that you should ex
- Frank: We need to get better and determine how to
- Diego: This should be part of the agent.

- (Black shirt): What about the flow based paradigm? what do you mean by flow characteristics.
- Frank: Flow based means that the network function tracks the packet and network content to track the details.
- [Adrian]: We need more work on the definitions.

8. Software-Defined Networking Based Security Services using Interface to Network Security Functions
draft-jeong-i2nsf-sdn-security-services
Jaehoon Paul Jeong (15 minutes : 105/150)
[jouri (blue shert): Just like Susan's presentation, you need to carefully define the virtual function - whether it is data sets or (red shirt): How do you see this is in scope for I2NSF? Jaehoon: How is this different that the use cases different than the use cases.
Adrian: This is a valid question. We should let Paul complete his presentation and we'll discuss this point.
Diego: I would suggest we use the top controller (?) one.
[rest of presentation]

Adrian: Jaehoon is describing how these services work. We'll decide what we should bring into this work.

9. User-group based Mechanism for Service Layer
draft-you-i2nsf-user-group-based-policy
Jianjie You (10 minutes : 115/150)
Adrian: Thank for you presentation.

[Adrian: These are three drafts recently published.
This is 3 minutes to
10. Introduction to new I-Ds
  a. draft-fang-i2nsf-inter-cloud-ddos-mitigation-api
     Luyuan Fang (5 minutes : 120/150)
  b. draft-pastor-i2nsf-vnsf-attestation
     Diego Lopez (5 minutes : 125/150)
  c. draft-zhou-i2nsf-capability-interface-monitoring
     Cathy Zhou (5 minutes : 130/150)

10.a Introduction to new I-Ds
● draft-fang-i2nsf-inter-cloud-ddos-mitigation-api
Luyuan Fyang (5 minutes : 120/150)

- Robert: This is good because this completes the other root in DOTS. This links how this work links to DOTS.
- Luyuan: I am willing to have the DOTS controller: 4 have 4 interests.
- Adrian:

10.b draft-pastor-i2nsf-vnsf-attestation
Diego Lopez (5 minutes : 125/150)

- Dealing with Attestation to virtual, may be applied to virtual.
- Addresed by mutual authentication, attestation of the virtual platform and the vNSFs.
- Adrian: Thank you for the presentation.

10.c draft-zhou-i2nsf-capability-interface-monitoring Cathy Zhou (5 minutes : 130/150)

- Bob Moskowitz: We do not have infrastructure for these alerts.
  - input of these events in a standard alterts. MILES and

11.Any other business – open mic (10 minutes : 140/150)
12.Summary of WG actions and next steps
Chairs (10 minutes : 150/150)