Full ISO 7-layer stack fulfilment, activation and orchestration of VNFs in carrier networks

The following normative disclaimer shall be included on the front page of a PoC report:

Submission of this NFV ISG PoC Report as a contribution to the NFV ISG does not imply any endorsement by the NFV ISG of the contents of this report, or of any aspect of the PoC activity to which it refers.

B.1 NFV ISG PoC Report

B.1.1 PoC Project Completion Status

Indicate the PoC Project Status. Can the PoC be considered completed? If this is a multi-stage PoC project, indicate the Reported Stage status and plans for future Project Stages.

- Overall PoC Project Completion Status: Completed
- PoC Stage Completion Status (Optional - for Multi Stage projects only): _____

B.1.2 NFV PoC Project Participants

PoC Project Name: Full ISO 7-layer stack fulfilment, activation and orchestration of VNFs in carrier networks

- Network Operators/ Service Providers: Telstra Contact: david.r.robertson@team.telstra.com
- Manufacturer A: Hewlett-Packard Enterprise Contact: jeff.higgs@hpe.com
- Manufacturer B: F5 Networks Contact: P.Synnott@F5.com
- Manufacturer C: Alcatel Lucent Contact: albert.saunig@alcatel-lucent.com

B.1.3 Confirmation of PoC Event Occurrence

To be considered complete, the PoC should have been physically demonstrated with evidence provided that the demonstration has taken place.

Provide details on venue and content of PoC demonstration event. Provide pictures and supporting literature where available. Please identify who was present at the demonstration event (optional).

- PoC Demonstration Event Details: SDN & OpenFlow World Congress, Dusseldorf, Germany (13-16 Oct 2015)

  This POC will demonstrate an E2E NFV solution based on ETSI NFV architectural framework, which shows the overall architecture of our PoC. The PoC includes VNFs with their respective VNF manager, an NFV Orchestrator, a VIM, an NFVI and SDN components: SDN controller and SDN virtual network.

  This POC will contribute to 3 Hot Topic areas:

  - PoC Project Contribution #1 (GS NFV-REL004): This PoC will investigate the active monitoring and failure detection of a deployed VNF in NFV environments. This will be provided in the form of a report describing our findings and responding to REL Hot Topic questions.
  - POC Project Contribution #2 (GS-NFV-EVE005): This PoC will report on SDN usage in NFV architectural framework. This will be provided in the form of a report describing our findings by filling in the EVE005 Hot Topic template.

- POC Project Contribution #3 (GS-NFV-TST002): This POC will perform some interoperability testing and will share best practice & test descriptions with TST WG by filling TST002 Hot Topic template.

Attendees: Telstra - David Robertson; Jatin Agarwal; Andrew Harris
F5 Network – Peter Synnott, Max Iftkhar
Alcatel Lucent – Albert Saunig, Gavin Rego; William Brioschi
HPE – Jeff Higgs, Davina Padlie, Marie-Paule Odini

- **POC demonstration at MWC'16 in Barcelona**

This POC was demonstrated on HPE booth at MWC'16.

B.1.4 PoC Goals Status Report

Specify PoC Goals from NFV ISG PoC Proposal (clause A.1.2). Identify any changes from the original NFV ISG PoC Proposal with an explanation as to why the changes were made. Indicate the extent that each goal was met. Provide sufficient information for those not familiar with the PoC goals to understand what has been achieved and/or learned.

• *PoC Project Goal #1:*	E2E Lifecycle management	*Goal Status (Demonstrated/Met?)*	Demonstrated
• *PoC Project Goal #2:*	Customer Self-service automation	*Goal Status (Demonstrated/Met?)*	Demonstrated
• *PoC Project Goal #3:*	Flexibility to deliver NFV Services to new customers	*Goal Status (Demonstrated/Met?)*	Demonstrated
• *PoC Project Goal #4:*	VNF Service Chaining	*Goal Status (Demonstrated/Met?)*	Demonstrated
• *PoC Project Goal #5:*	VNF Resiliency	*Goal Status (Demonstrated/Met?)*	Demonstrated
• *PoC Project Goal #6:*	VNF Portability	*Goal Status (Demonstrated/Met?)*	Demonstrated

B.1.5 PoC Feedback Received from Third Parties (Optional)

- Where applicable, provide in a free text, feedback received from potential customers, Ecosystem partners, event audience and/or general public.

  Positive feedback and a lot of it was received during the SDN World Congress held in October 2015 in Dusseldorf where this POC was demonstrated to potential customers, analysts and media at large. Some of the specific feedback included that this was a unique demonstration of not only multiple facets of different use cases but also where NFV and SDN technologies were in symbiosis and well integrated to provide compelling value proposition for the service providers/carriers. Also, much feedback was provided as how this POC demonstrated the unique capabilities of three different suppliers each a leader in their domain all accomplishing use cases that are deployment ready.

  - *"Looking forward to the final report" and "Are there plans to productised the PoC?" were consistant comments received from numerous ETSI members during our public demonstration at SDN World Congress*
  - *"It's great to see collaboration between 3 best of breed vendors for an intergrated outcome"*
  - *It's assumed that Telstra's sponsorship and support was critical to the success of the PoC.*

B.2 NFV PoC Technical Report (Optional)

PoC Teams are encouraged to provide technical details on the results of their PoC using the PoC Scenario Report template below.

B.2.1 PoC Scenario Report

Use the table structure below and refer back to the Scenarios in the NFV ISG PoC Proposal (clause A.2.2) and provide information for each of them. Feel free to include additional Scenarios developed during the implementation of the PoC. Do not eliminate Scenarios that were not performed, instead provide a brief status for each with a reason why the scenario was not performed. Do not hesitate to fill multiple instances of the table if several objectives have been demonstrated for each scenario.

B.2.1.1. Scenario 1 – E2E Lifecycle management

Objective Id:	**SCE1**	
Description:	**E2E Lifecycle management** The PoC goal demonstrates the capability of the solution to manage the lifecycle of a VNF from deployment through to decommission.	
Pre-conditions	Prior to executing these test cases the PoC environment was required to be setup and available.	
Procedure:	**1**	A VNF deployment request is initiated from the customer portal.
	2	The VNF deployment request is received by the MANO layer
	3	The MANO application passes a request to the VIM to deploy a virtual machine
	4	The VIM passes a request to deploy a virtual machine to the virtualisation layer
	5	The virtualisation layer deploys a virtual machine using the image requested and once complete pass this back to the MANO systems through the VIM.
	6	The MANO systems configure the virtual machine as well pass a request to the SDN controller to configure the network
	7	All configuration items are completed and the MANO systems receive confirmation.
	8	VNF connectivity is tested and confirmed
	9	VNF decommission request is sent to the MANO systems from the client portal
	10	The NFVO sends a decommission request to the VIM

	11	The VIM decommissions and removes the VNF
Results Details:	The tests show that the VNF was successfully deployed in under 20 minutes and connectivity to the internet was confirmed. Upon completion of testing a decommission request was executed and the VNF removed in under 20 seconds	
Lessons Learnt & Recommendations	The reference NFV standard aligns with the procedures used in the PoC to demonstrate E2E lifcycle managements.	

B.2.1.2. Scenario 2 – Customer Self-service automation

Objective Id:	**SCE2**	
Description:	**Customer Self-Service Automation** This PoC goal demonstrates the customer self-service activation capability of the solution and its ability to be provision the requested services in an automated manner.	
Pre-conditions	Customer self-service portal developed and integrated with the solution.	
Procedure:	**1**	User logs into their account as a customer via the self-service portal.
	2	User navigates to their services web page and requests for an Internet connection via a firewall by dragging and dropping the 'Firewall' icon from 'My Services'
	3	Ensure that firewall is instantiated automatically and connected to the customer's VPN. Customer should now have Internet access via the firewall.
	4	Customer now requests for the FItering service to be added their Internet connection by dragging and dropping the 'Filtering' icon under 'My Services'
	5	Ensure that the filtering service is instantiated automatically and service-chained to the customer's VPN. Also verify that the filtering service functions as expected.
Results Details:	The tests show that the solution allows for the customers to order their services via a self-service portal and these services are provisioned automatically.	
Lessons Learnt & Recommendations	The MANO layer in the ETSI reference architecture is comphrensive, but also flexible enough to enable numerous interaction points for the connection of a portal. The challenge is whether to have multiple portals (interaction points) for the various stakeholders (customers, operations, engineers) or one comprehensive one. We found that seperation is best, particularly for diagnosis of faults and events, but requires displine to understand the impact to the overall service if making a change at lower levels, without interaction from the higher levels in the MANO layer.	

B.2.1.3. Scenario 3 – Flexibility to deliver NFV Services to new customers

Objective Id:	**UC1/SCE3**	
Description:	**Modify VNF** • Change VNF parameter by company operator. The operator shall be able to reconfigure parameters of the VNF. • Change VNF parameter by customer. The customer shall be able to reconfigure parameters of the VNF. • Change of VNF parameters by customer via a company branded or unbranded customer self-service portal.The customer shall be able to reconfigure parameters of the VNF via a company portal. • Demonstrate how the solution can dynamically change the traffic traversing a specific VNF by changing the parameters of the service chain.The solution should be able to granularly control the service chains, i.e. send traffic into service chain based on: a. customer site b. host or device c. application type • Horizontal scaling - Demonstrate how the solution can dynamically trigger the instantiation of additional VMs based on pre-defined triggers. The solution should be able to provide dynamic horizontal scaling in response to pre-defined trigger conditions. • Modify service chain by adding or removing VNFs to/from it. The solution should provide flexibility by adding or removing product features without the need to augment the hardware platform.	
Pre-conditions	The test case dependency was to be executed with a previously deployed operational VNF and with the service functioning.	
Procedure:	1	Add the DNS firewall and remove it via orchestration.
	2	Measure time to start and stop.
	3	Measure length of time that service is disrupted.
Results Details:	Passed The completion of VNF Service chaining occurred within expected timeframe.	
Lessons Learnt & Recommendations	Certain traffic can be excluded from or included in service chains. An example could be to add or remove a particular customer site from VNF without changing the traffic flows from other sites in this VPN. The NFVI can dynamically adjust to resource utilisation and deploy additional VMs in response to e.g. growth in traffic or other service parameters. The completion of VNF Service chaining occurred within expected timeframe. Considerstaions needs to be given to how the traffic needs to be distributed across multiple VNF instances providing the same service for the same network.	

Objective Id:	**UC2/SCE3**	

Description:	**Decommission of VNF**
	
	• Measure time to decommission VNF.
	  • An instantaneous decommissioning of infrastructure or customer service shall be achieved.
	• Qualify the service or network impact of VNF decommissioning.
	  • The decommissioning of VNF should not result in a customer impact,
	
	  OR
	
	  • The decommissioning of VNF shall only result into a small customer impact.	

Pre-conditions	The test case was only able to be executed with a firewall VNF operational that was previously deployed and the service functioning	
Procedure:	1	Verify that the F5 Firewall VNF and associated service is operational.
	2	The following two tasks need to be executed prior to the second VNF decommission being triggered: a. A continuous ping to an external site needs to be started prior to initiating the test. The ping would need to run for the duration of the VNF deployment which is determined after completing test 1a. b. An SSH session needs to be established to the BIG-IP VNF deployed in test case 1a
	3	The test case can then be initiated.
	4	Initiate the VNF decommission workflow for the second VNF.
	5	Complete test case initiate then initiate the next test case
	6	Confirm that the VNF has been removed from within hypervisor, Nuage and BIG-IQ
Results Details:	Passed	
Lessons Learnt & Recommendations	The test was passed successfully with the decommission not impacting the environment. All VNF elements were noted to have been removed from hypervisor, Nuage and BIG-IQ and the freed up resources were returned to the pool.	

Objective Id:	**UC3/SCE3**
Description:	**Relocation of VNF** • Measure time to relocate VNF between sites. A timely relocation of VNF shall be achieved. • Quantify the service or network impact of VNF relocation between sites. The relocation of VNF between sites should not result in a customer impact, OR The relocation of VNF between sites shall only result into a small customer impact. • Measure time to relocate VNF within same site, e.g. as part of hardware maintenance. A timely relocation of VNF shall be achieved. • Quantify the service or network impact of VNF relocation within site. The relocation of VNF within site should not result in a customer impact, OR The relocation of VNF within sites shall only result into a small customer impact.
Pre-conditions	Dependent on primary use case – i.e. deployed and functioning layer 1-7 VNF deployment. This test case assumes that the network traffic has to converge to a different site.
Procedure:	1 The aim of the Use Case is to demonstrate a VNF is relocated between sites with no impact to the service of an existing VNF
Results Details:	Passed
Lessons Learnt & Recommendations	It was proven that recovery of network services could be automatic and non impacting whether this be between sites or between same site infrastructure. Live VNF migration and recovery is dependant on deployment,hypervisor and VNF.

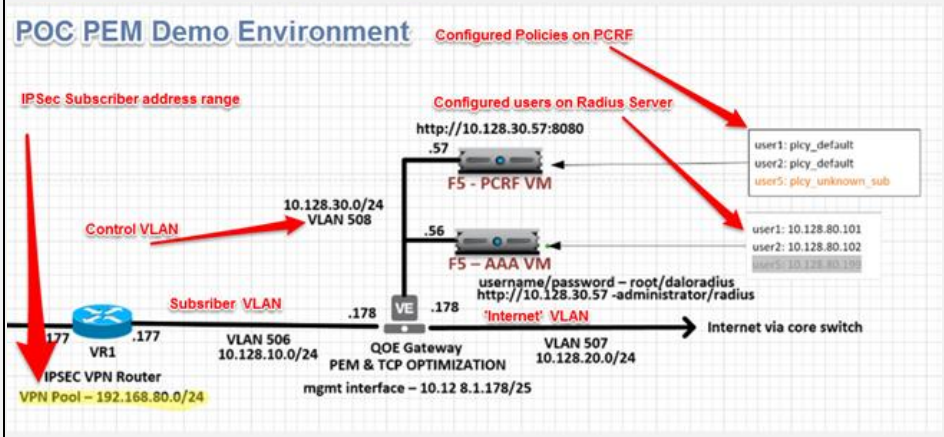
Objective Id:	UC4/SCE3	
Description:	**Resiliency of NFVI** • Demonstrate backup and restore function for NFVI. The solution should support automatic backup functions, AND The solution should support restoration of VMs from created backups. • Demonstrate the re-instantiation of a VNF in response to server hardware failure. The solution should support the manual re-instantiation of VNFs after server hardware failure, OR • The solution should support the automatic re-instantiation of VNFs after server hardware failure. • Demonstrate the relocation of a VNF in response to connectivity failure. The solution should support the manual re-instantiation of VNFs after connectivity failure, OR • The solution should support the automatic re-instantiation of VNFs after connectivity failure.	
Pre-conditions	It should be assumed that some VNFs are configured by the customer and backup/restore function is provided by the Service Provider.	
Procedure:	1	Verifying that the VNF and associated service is deployed and functioning.
	2	Manually deleting the VNF from the CS8 portal which will mimic a hardware failure.
	3	Confirming that NFV-D has restarted the VNF instantiation in response to the VNF being removed
Results Details:	The VNF was restored after the server hardware failure	
Lessons Learnt & Recommendations	The solution supports the manual re-instantiation of VNFs after server hardware failure and the solution support the automatic re-instantiation of VNFs after server hardware failure. The solution demonstrated integrated capability to back up an entire blade chassis, and restore it, including F5 and Nuage configurations.	

B.2.1.4. Scenario 4 – VNF Service Chaining

Objective Id:	SCE4	
Description:	This PoC scenario demonstrates the service chaining capability of the solution and its ability to provision connectivity between a client and a set of requested services.	
Pre-conditions	Individual VNFs deployed and functioning, including all network connections from clients to virtualised infrastructure and the Internet.	
Procedure:	1	Through a network control API, provision a connection for a client to a pre-provisioned firewall and confirm user has access as defined in the firewall configuration.
	2	Through the same network control API, modify the client connection policy to force all user traffic through an application management (DPI) application as well as the firewall. Confirm that the user has both the firewall and application management policies applied.
	3	Through the same API, provision a firewall-only policy for another client. Confirm that the policy applied to the new client is working correctly, and that the behaviour of the existing client has not changed.
	4	Through the same API, modify the policy applied to the first client to only apply to a single host, while another host on the same connection has a firewall-only policy.
	5	Through the same API, modify the policy applied to the first client so that all traffic is directed to the firewall and confirm that the application management function has been removed.

Results Details:	Passed
Lessons Learnt & Recommendations	The tests show that the process of creating service chains can be automated. A high level of collaboration is required between the configuration of VNFs (both routing and policy rules) and the configuration of network policy to achieve the desired result. If there were a standardised way to specify packet handling policies (such as forwarding, filtering and load-balancing) it would greatly reduce the complexity of orchestrating multiple physical and virtual network elements to create customised network services. The functions provided by APIs controlling packet forwarding between network functions are foundational to the operation of service chaining. However, the most important and difficult problem to be solved is orchestrating the configuration of the network functions themselves with the forwarding rules in the network. It would be valuable for ETSI to investigate the creation of a standardised open approach to interfacing network functions to facilitate orchestration. Although it is acknowledged this will be challenging given the broad range of network function providers and the different approaches used.

B.2.1.5. Scenario 5 – VNF Resiliency

Objective Id:	**SCE5**	
Description:	**F5 PCEF/LITE VNF Resiliency** This PoC goal demonstrates the resiliency of F5 VNFs.In the use-case F5 VNF with a base configuration was used and then F5 REST driver demo portal was used to showcase how we can recover from a failure quickly or convert an existing VNF to a different function. 	
Pre-conditions	F5 REST driver demo portal VM is up and running	
Procedure:	1	Reset F5 VNF configuration to base build or use HP NFV-D to orchestrate a F5 VNF with a base configuration
	2	Navigate to F5 REST driver demo portal and click on 'Device Inventory'.
	3	Select a device with 'PEM' listed in the 'Modules' column.
	4	From the pull-down list, select 'PEM Use Case #11', the click on the gear symbol to the right.
	5	Select 'Deploy Use Case' after reviewing the use case settings.
	6	The above step restore F5 PEM VNF configuration using REST API calls
	7	Ensure configuration on the BIG-IP VNF is consistent with a PCEF
	8	Connect an external device as a client (using IPSEC VPN into the network) and observe policy being assigned
	9	Ensure that browsing, downloading etc is possible
	10	Observe download speed are commensurate with the policy in effect

Results Details:	Passed
Lessons Learnt & Recommendations	F5 supports live migration of **idle** BIG-IP VNFs which mean we should follow the procedure below for stateful services such as SIP. VNF Migration: • Failover all user traffic to standby F5 VNF • Migrate Primary VNF to another compute node • Failback all user traffic to primary F5 VNF

B2.1.6. Scenario 6 – VNF Portability

Objective Id:	**SCE6**	
Description:	This PoC goal demonstrates the VNF portability capability of the solution and its ability to move a VNF within different virtualisation platforms.	
Pre-conditions	Prior to executing these test cases a VNF was required to be deployed in the PoC environment.	
Procedure:	**1**	A deployed and functioning VNF in the PoC environment was removed at the virtualisation layer
	2	The NFVO system detected the removal of the VNF and instigated a recovery process
	3	The VNF recovery process was configured to be carried out on a second set of infrastructure that was managed by a second VIM. The second NFVI installation was part of the PoC and was used to model a second site for failover testing. The different sets of the same VIM and NFVI components were used to build the two stacks.
	4	Upon completion of VNF recovery connectivity to a test site was verified.
Results Details:	The tests show that the VNF was successfully recovered on separate infrastructure and connectivity to the test site was verified. The recovery process involved the deployment of a new VNF and was completed in under 20 minutes with connectivity to the internet being confirmed.	
Lessons Learnt & Recommendations	The PoC demonstrates that VNF portability is viable within the NFV standard and that it requires capabilities within the application service layer to support non disruptive services.	

B.2.2 PoC Contribution to NFV ISG

Use the table below to list any contributions to the NFV ISG resulting from this PoC Project.

Contribution	WG/EG	Work Item (WI)	Comments
	NFV-TST	DGS/NFV-TST002 (GS)	Hot Topic Report being submitted to the TST WG
	NFV-EVE	DGS/NFV-EVE004 (GS)	WG closed and contribution accepted for publication October 2015; *Published Link:* http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_NFV-EVE005v010101p.pdf
	NFV-REL	DGS/NFV-REL005 (GS)	Contribution to REL HT#3 Posted as https://docbox.etsi.org/ISG/NFV/REL/05-CONTRIBUTIONS/2015/NFVREL(15)000239_HT_3_-_POC_38_contribution_on_E2E_Fault_Correlation_and_Faul.doc Presented in REL WG Meeting Sept 29th 2015: **NFVREL#124**

B.2.3 Gaps identified in NFV standardization

Use the table below to indicate Gaps in standardization identified by this PoC Team including which forum(s) would be most relevant to work on closing the gap(s).Where applicable, outline any action(s) the NFV ISG should take.

Gap Identified	Forum (NFV ISG, Other)	Affected WG/EG	WI/Document Ref	Gap details and Status
Yyyyy	NFV	EVE	DGS/NFV-EVE004 (GS)	*The tests show that the process of creating service chains can be automated. A high level of collaboration is required between the configuration of VNFs (both routing and policy rules) and the configuration of network policy to achieve the desired result.* *If there were a standardised way to specify packet handling policies (such as forwarding, filtering and load-balancing) it would greatly reduce the complexity of orchestrating multiple physical and virtual network elements to create customised network services.* *The functions provided by APIs controlling packet forwarding between network functions are foundational to the operation of service chaining. However, the most important and difficult problem to be solved is orchestrating the configuration of the network functions themselves with the forwarding rules in the network.* *It would be valuable for ETSI to investigate the creation of a standardised open approach to interfacing network functions to facilitate orchestration. Although it is acknowledged this will be challenging given the broad range of network function providers and the different approaches used.*
.Zzzzz	NFV	OaM	ETSI GS NFV-MAN 001	*The PoC demonstrated integration of F5 VNFs with HPE NFV Director which is HPE NFV-O. The ISG NFV specifications envision this integration to be plug-and-play based on open and standards REST APIs, but unfortunately, at this early stage of NFV adoption, it is most definitely not plug and play. Every integration be it between one vendor's VNFs and another vendor's NFV-O or VNF-M and also between VNFs and a SDN Controller is a major customization project and needs the vendors in context to work closely together to make the integration successful. In the future we hope that these integration efforts will become easier utilising open and standard APIs and will ultimately result in true plug-and-play.*

B.2.4 PoC Suggested Action Items

- Provide suggested Action Items and/or further work required from the NFV ISG and/or external forums.
  - **Standardised integration ie: between VNFs, OSS and BSS**
    - If there were a standardised way to specify VNF polices and information exchange it would greatly reduce the complexity of orchestrating multiple physical and virtual network elements to create customised network services and integration with OSS and BSS solutions. It would be worth investigating whether or not there was an existing standardise approach that could be used that VNF providers could adopt to be compliant with the ETSI ISG reference architecture.
  - **Continue to promote adoption of existing industry standards rather than develop new standards whenever possible**
    - In the future we hope that integration efforts will become easier utilising open and standard APIs and will ultimately result in true plug-and-play. Avoiding creating new standards that were unique to the ETSI ISG reference architecture would be a better approach than creating another "standard" that was unique to the ETSI ISG reference architecture.
  - **Bringing together the various forums ie: SDN World Congress, MW Congress, OpenStack, Open Summit**
    - Given the ETSI ISG approach is to use existing standards and open APIs, rather than create new standards, then the ETSI ISG needs to have active involvement in each of the major standards and their associated events relied upon to evolve the ETSI reference architecture.

B.2.5 Any Additional messages the PoC Team wishes to convey to the NFV ISG as a whole?

- Please indicate whether the team wishes any specific message to be published or publically quoted.

  This multi-vendor POC successfully demonstrates the power and effectiveness of multiple vendors each a leader in their domain in the industry coming together to address specific challenges that the carriers are facing in the advent of exploding traffic demands and increasing demand for newe services and apps to be deployed in a rapid manner. This POC in a very visible manner proves the value of the NFV eco-system that the industry needs to hasten the adoption of NFV/SDN in the industry.

B.2.6 Any Additional messages the PoC Team wishes to convey to Network Operators and Service Providers?

- Are there any specific requests/messages that the team would like to convey to Network Operators and Service Providers?

  This successful demonstration of the various use cases and capabilities in this POC shows clearly that NFV is deployment ready and operators can introduce NFV in to their network infrastructure to increase service velocity, to dynamically scale on demand as well as Capex/Opex savings in the long run. Also, this POC shows the effectiveness of integration of NFV and SDN technologies to offer compelling value to the carriers.

Glossary

HPE	Hewlett-Packard Australia Pty Ltd or Hewlett-Packard Enterprise
F5	F5 Networks
ALU	Alcatel-Lucent Nuage Systems
VNF	Virtual Network Function
SIP	Session Initiation Protocol
BIG IQ	F5 BIG-IQ