



CLOUDI-FI – VERSA WI-FI GUEST PROJECT

Prepared by Paul Christian Ella Versa Networks

© Copyright 2020





Abstract

Cloudi-Fi is a Guest WiFi service provider. They are looking for a partnership with Versa Networks. For more information about the partnership model, visit : <u>https://www.dropbox.com/s/e5ouh3ono5hld43/Cloudi-Fi-Versa-11-20.pdf?dl=0</u>

Purpose of this document

POC Results on Guest WiFi integration between Cloudi-Fi and Versa Networks using SAML authentication with Captive Portal.

Document Control

Name	Modified By	Modification Date	Modification	Created By	Creation Date
Cloudi-Fi – Versa partnership Level – v0.1				Paul Christian Ella	15/12/2020
Cloudi-Fi – Versa partnership Level – v0.2	Paul Christian Ella	16/12/2020	* Comments from John*/ Remove section 5; Add software version used during demo; Add introduction		





Contents

1.	Introduction	5
2.	Versa SAML Authentication Overview	8
3.	Cloudi-Fi SAML Authentication Configuration in Versa	10
3	3.1 Requirements	10
3	3.2 Roles	10
3	3.3 Configuration	11
4.	Call Flow verification using SAML-Tracer Extension	17
5.	Service verification in Versa Director	21
2	4.1 User identification under Monitor tab	21
2	4.2 Logs > Authentication in Analytics	21
6. /	ANNEX	22





Glossary

Term	Definition
SP Entity	Service Provider Entity
IdP Entity	Identity Provider Entity
SAML	Security Assertion Markup language
NG-FW	Next-Generation Firewall
DNS	Domain Name Server
LEF	Log Exporter function
POC	Proof Of Concepts
SSO	Single Sign-On
URL	Uniform Resource Locator





1. Introduction

Founded in 2014, Cloudi-Fi offers WI-FI to guests and customers of large multinational companies. Their solution is 100% cloud-based, secured and compliant, deployed globally and can be personalized to fit customer's core business. They leverage data and offer better guest WI-FI experience using marketing digital tools (Acquisition, Ad page, Retargeting campaigns, Messaging and Analytics).



Source : <u>https://www.cloudi-fi.com/</u>

How Cloudi-Fi leverages Versa Networks offer?

Cloudi-Fi brings the guest wifi captive portal feature without any development needed

- Cloudi-Fi opens a way to access the business lines through the content providers partners we support and explore new
 business opportunities
- Cloudi-Fi provides the phygital reconciliation and brings your team the digital world
- Cloudi-Fi integration within your environment is smooth and transparent at every levels







API

Smooth and transparent integration

Technical complexity with simplicity

- Cloudi-Fi mission is to bring compliant and customizable captive portals to technology leaders to augment their value proposal.
- Cloudi-Fi is 100% cloud & open platform. The integration is easy with the use of API, scripting and templates.
- Cloudi-Fi guest wifi services are activated instantly from the partner admin UI or Web:
 - Seamless setup for an immediate benefit
 - Instant access to **Freemium** service from the partner admin UI/Web
 - Customizable active portals on demand



Compliance Which challenges do Cloudi-Fi solve ?

DIFFERENT CAPTIVE PORTAL / REGULATION	DIFFERENT AUTHENTICATION LEVELS	ENCRYPTION OF DATA COLLECTED	LEGAL ASSISTANCE	
· ·	STRONG			
Votacime to he to R	SMS LOCAL SOCIAL NETWORKS COUNTRY SPECIFIC ID			
	MEDIUM			
Comparison C	SOCIAL NETWORKS EMAIL			
LART NUME	LOW	Developing of Internet Inc.	I la cità Tanza (cas 8 Décara	
Creation of captive portals according to country requirements	DECLARATIVE ONLY CLICK THROUGH	Log storage in compliance with local regulation (duration, location & how)	Dolicy with terms of Use & Frivacy policy with te-up <u>Option</u> : surrogate legal responsibility to Cloudi-Fi	CLOUDI-FI







The purpose of this document is to demonstrate the integration between Versa and Cloudi-Fi.

A user should connect to guest wifi, authenticate through a captive portal provided by Cloudi-Fi and then get connected to Internet or specific URL categories.

Using Versa NG-FW capabilities, we will configure authentication policies to bypass SSO URL & DNS and authenticate all remaining user traffic. User/Group authentication and authorization between Versa and Cloudi-Fi is achieved using SAML.

Depending on customer's requirement, we also have ability to apply security profiles like URL filtering, IP filtering, SSL decryption, Web proxy, etc...

With Versa Analytics, log collectors can send syslog data to 3rd party systems to comply with regulations as expected by Cloudi-Fi.





2. Versa SAML Authentication Overview

Security Assertion Markup Language (SAML) authenticates users to access multiple services and applications. SAML configuration is useful when you want to access multiple services or applications and have to authenticate for each service or application, for example, Google and its related services. SAML is a common standard for exchanging authentication between parties, most commonly used for web browser-based single sign-on (SSO).

You can configure SAML SSO to log in with a single sign-on and access multiple services and applications. Similarly, you can configure SAML single sign-out to end sessions for multiple services and applications and log out using only one session. You can use SAML authentication for services and applications that are external or internal to your organization.

- FlexVNF supports user-identification from external identity providers using SAML protocol.
- Customer can use any third party identity provider (IDP) to authenticate users and apply user, group, roles and location based policies.
- Multiple branches or appliances can use single centrally located authentication server to authenticate users using SAML.
- Authentication will be done outside of FlexVNF and it will have knowledge of only users.
- Identity control module will generate required AuthN-request and parse AuthN-response.
- Captive portal module will be used to send redirection.



Figure 1: Secure Access SAML Authentication





Clie	ent C/	AS	ID	P
-	GET request	1. Check for Versa-Auth cookie. 2. If found, extract user information and proceed with final response with Auth-token and without set-cookie. 3. If not have, then proceed with following		
_	Connect to IDP and present AuthN-request	to login consumer service with Auth	N-response	1. Authentioates User 2. Provide AuthN-response and redirect to consumer service
<	Submit AuthN-response to consumer service	Verify response Verify Signature Setract Username Generate Auth-token Greate Versa-Auth cookie Redirect to original URL with Auth-token and with Set-cookie.		

Figure 2: Workflow in Central Auth-server (CAS)





3. Cloudi-Fi SAML Authentication Configuration in Versa

3.1 Requirements

Software Version: 20.2 and later License Tier: Prime Secure SD-WAN Feature used: NG-FW and DNS Proxy

3.2 Roles

SPEntity : Versa VOS

IdPEntity : Cloudi-Fi

The purpose of DNS Proxy is to redirect DNS requests to *cloud-fi.versa-networks.com* to an internal DNS server managed by customer to resolv this domain to Versa CPE LAN IP address. All other requests will be managed by public DNS hosted in Internet.

The Versa Central Auth-Server functionality is handled by NG-FW feature.

In this demo, we are going to configure DNS resolution into our windows hosts file as below:

Go to C:\Windows\System32\drivers\etc\hosts and add the following line:

192.168.3.1 cloud-fi.versa-networks.com

The high-level architecture diagram used during our demo is displayed below:



Figure 3: Cloudi-Fi and Versa Integration

Hardware used: Versa CSG770 Software used: Versa VOS 20.2.3





3.3 Configuration

Do the following configuration for SAML Authentication:

- 1 > Upload certificates
- Get certificate (Cloud-fi-ca-cert) from Cloudi-Fi to secure communication (Assertion and Attributes) between Versa VOS and Cloudi-Fi;
- Get certificate (Cloud-Fi-Cert) from Versa/Customer to secure communication (AuthN request and AuthN response, services granted to user) between Guest Client (user browser) and Versa VOS
- Load Certificates in versa Director and then on appliances

VERSA			H	pella (paul-lab) ~
NETWORKS	Monitor Analytics Cor	figuration Administration		
Home Home-CSG-Dev	→ Organization: p	aul-lab 🗸		Build C
* 🗘 😚 🗞	Director Appliance			
🗳 Objects 🔍 🗸				< 1 ▶ 25 ×
Address Address Groups	Chain Name	Chain File Name	Date Uploaded	
 Persistent Actions Schedules 	Cloud-FI-Cert	Cloud-Fi_chain.crt	Fri, Dec 04 2020, 10:51	
Cloud Profiles				
🐔 Custom Objects 🛛 🗸				
Applications				
Application Filters				
Application Groups Scanners				
WRL Categories				
Services				
 Vulnerability Rules 				
Captive Portal Cust URL File				
Address Files				
User Defined Actio Q Certificates				
Keys				

							pella (paul-lab) 🗡
	Monitor Analytics	Configuration Administratio					
Home Home-CSG-Dev	✓ Organizati	ion: paul-lab	×				Build C
* 🗘 📀 😒	Director Appliance						
💲 Objects 🛛 🗸 🗸					G		1 1 25 2
Address	Chain Name	Common Name (CN)	Organization Unit (OU)	Organization (O)	Valid Till	Status	
Address Groups		DST Root CA X3	organization onic (ob)	Let's Encrypt	2021-03-17 16:40:46	Valid	
Persistent Actions	Cloud-FI-Cert	Let's Encrypt Authority X3			2021-02-27 18:27:08	Valid	
Schedules	cloud-fi-ca-cert	login.cloudi-fi.net	Captive Portal,	Cloudi-fi	2027-08-26 12:31:23	Valid	
Cloud Profiles Pre-defined							
Custom Objects							
Applications							
Application Filters							
Application Groups							
Scanners							
W URL Categories							
Services							
PAC Files							
Vulnerability Rules							
Address Eiles							
Subser Defined Actio							
O Certificates							
😚 Keys							
🚔 CA Chains							







2 > Create SAML Profile

Go to:

Flexvnf > Click on Object & Connectors icon > Connector > Users / Group > SAML Profile

Edit SAML Profile - Cloud-Fi-SAML-Profile	×
Name*	
Cloud-Fi-SAML-Profile	
Description	
Host	Prefix ID
https://cloud-fi.versa-networks.com:44991	
Single Sign-on URL	
https://login-uat.cloudi-fi.net/start/ebd2613d4b6d34da	afb516c3f25326b2e/c11aed16a26be518863a55c1820dac
Single Sign-out URL	
SP Entity ID	IDP Entity ID
https://cloud-fi.versa-networks.com:44991/metadata	https://login-uat.cloudi-fi.net/auth/saml2/idp/metada
SP Certificate	IDP Certificate
default 🗸 🗸	cloud-fi-ca-cert 🗸 🗸
	OK Cancel

Figure 5: SAML Profile Configuration in Versa Director

3 > Create Authentication Profile for SAML

Go to:

Flexvnf > Click on Object & Connectors icon > Connector > Users / Group > Authentication Profiles

Edit Authentication Profile - Cloud-Fi-SAML-Auth-Profile				
Name*				
Cloud-Fi-SAML-Auth-Profile				
Description				
Tags				
Kerberos Profile	LDAP Profile	SAML Profile		
Select	Select	Cloud-Fi-SAML-Profile 🛛 🗸		
+ Create Kerberos Profile	+ Create LDAP Profile	+ Create SAML Profile		
Cache Expiration (mins)	Cookie Name			
10				
Concurrent Login	Routing Instance	Expiration Mode		
1	Select	Inactivity 🗸 🗸		
Authenticator Profiles	I FF Profile			
Select V	Default-Logging-Profile V	Default Profile		
		OK Cancel		

Figure 6: SAML Authentication Profile Configuration in Versa Director





4 > Create Custom URL category for bypass Single Sign-on URL

Go to:

Flexvnf > Objects & Connectors > Click on Objects > Custom Objects > URL Categories

Edit URL Category - cloud-fi-sso-url-filter				
Name* cloud-fi-sso-url-filter				
Description				
Tags				
Confidence URL File	~			
URL Patterns URL Strings				
Q Se	earch		1	
Pattern 🗢	Reputation			
	Select	~	+	
.*cloudi-fi*	trustworthy		ū	
		•		
	0	к	Cancel	

Figure 7: URL Category of Cloudi-Fi authentication servers

5 > Create Authentication Rule for bypass DNS Traffic

Go to:

Flexvnf > Click on Services icon > Next Gen Firewall > Authentication > Policies > Rules

Edit Rules - Cloud-fi-bypass-DNS	
General Source/Destination Applications/URL H	Headers/Schedule Enforce
Applications	URL Categories
Application List	+ - URL Category List + -
DNS	
+ New Group + New Filter + Ne	ew Application + New URL Category
	OK Cancel





Edit Rules -	Cloud-fi-bypass-DNS			
General	Source/Destination	Applications/URL	Headers/Schedule	Enforce
Action O Do not AuthenticateSelect			Log O Do not Log • Log using Profile Select	
				OK

Figure 8: authentication rule to bypass DNS traffic authentication

- 6 > Create Authentication Rule for bypass Single Sign on URL
 - Go to:

Flexvnf > Click on Services icon > Next Gen Firewall > Authentication > Policies > Rules

Edit Rules - Cloud-fi-bypass-sso				×
General Source/Destination	Applications/URL	Headers/Schedule	Enforce	
Applications		URL	Categories	
Application List		+-	URL Category List	+ -
			cloud-fi-sso-url-filter	
+ Nev	w Group + New Filter +	New Application		+ New URL Category
				OK Cancel
Edit Rules - Cloud-fi-bypass-sso				×
General Source/Destination	Applications/URL	Headers/Schedule	Enforce	
Action				
Do not Authenticate	Authenticate usi	ng Profile	O Do not Log	
Select			Log using Profile	
L			Select	Default Profile
				OK Cancel

Figure 9: authentication rule to bypass Cloudi-Fi authentication servers

7 > Create Authentication Rule for SAML

Go to:

Flexvnf > Click on Services icon > Next Gen Firewall > Authentication > Policies > Rules

Edit Rules - Cloud-Fi-auth-Pol		×
General Source/Destination	Applications/URL Headers/Schedule Enforce	
Action Do not Authenticate Cloud-Fi-SAML-Auth-Profile View Authentication Profile	O Authenticate using Profile ○ Do not Log O Log using Profile Default-Logging-Profile View LEF Profile	
	ОК Сапсе	

Figure 10: authentication rule for all wifi guest traffic





8 > Configure Captive Portal

Go to:

Flexvnf > Click on Services icon > Captive Portal

Edit Captive	e Portal Settings				×
General	Authentication	Custom Redirect Pa	arameters		
HTTP Port 8080		Anchoring Select	~	Global Expiration Tir 30	me(min)
SSL Port 44991		Provider Organi: Select	zation ~	PAC Server Domain	
Routing paul-lab	; Instance (+ -LAN-VR				
Server St	art Mode	SSL CA Certifica	te	SSL Certificate	
Server UR	L ersa-networks.com		Cookie Auth Ur Select	l Certificate	~
PAC Url Ce Select	ertificate Viri	tual Url Certificate Select 🗸 🗸	SSL Redirect Url	Certificate	~
				ок	Cancel

Figure 11 : Captive portal configuration in versa Director

9 > Configure DNS Proxy

 Configure SNAT Under Objects & Connectors > Objects > SNAT Pol
Edit SNAT Pool - SNAT-Pool X
Name*
SNAT-Pool
Description
Tags
Routing Instance
paul-lab-LAN-VR V
IPv4 Addresses IPv6 Addresses Egress Networks
Egress Network
Egress Network
UI-FI-5G
OK Cancel

Figure 12: SNAT Pool Configuration for DNS Proxy in versa Director





• Configure DNS Proxy Profile under Networking > DNS > Proxy Profiles



Figure 13: DNS Proxy Profile Configuration in versa Director



Configure DNS Proxy Policy under Networking > DNS > Policies

Figure 14: DNS Proxy Policy Configuration in versa Director





4. Call Flow verification using SAML-Tracer Extension

Step 1: Request Resource and Redirect to IDP

🔍 SAM	L-tracer	—		×
× Clear	il Pause 🛓 Autoscroli 🔽 Filter resources 👌 Colorize 👌 Export			
GET GET GET GET POST POST GET GET	http://www.mst.connectiest.com/reduced. http://www.mst.connectiest.com/reduced. https://login-uat.cloudi-finet/tauth/solida/bd/d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?SAMLRequest=JVLBblswDL33KwyttoNjS47dRE https://login-uat.cloudi-finet/tauth/solida/bd/d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?SAMLRequest=JVLBblswDL33KwyttoNjS47dRE https://login-uat.cloudi-finet/tauth/solida-bph/multiauth/selectsource.php?AuthState=_f0b96c4792eb0acb0de795790c98ee3400c60f512c%3Ahttps%3A%2F%2Fin https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-uat.cloudi-finet/template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://login-template/cloudifi_base_v2/fonts/avenir/Avenir-Book woff2 https://www.msn.com/rocid=wispr&pc=u477	gCeA2k ogin-uat	:Bei6(SA cloudi-fi.n cloudi-fi.n SA	ML 1et%2 1et%2
HTTP				
GET http Upgrade- User-Age Accept: Accept: Accept-L HTTP/1.1 Location SAMLRequ S1%2bB3s zP1XmQoh ZfcfQndH mSry50U7 Access-C Access-C Access-C Allow: * Content- Pragma: Cache-Co Connecti Proxy-Co	<pre>://www.msftconnecttest.com/redirect HTTP/1.1 Insecure-Requests: 1 nt: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 text/html,application/xhtml+xml,application/xml;q=0.9, image/avif,image/webp,image/apng,*/*;q=0.8, application/signed-exchange;v=b3;q maguage: en-US,en;q=0.9 307 Temporary Redirect : https://login-uat.cloudi-fi.net/start/ebd2613d4b6d3d4dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1? est=jVLBbtswD133KwjftoHj547dRtgCeA2KBei6oM162GWgJboVJkuZJKfd309ysm49rNhB84p8j3yPXDjoJYFLg3%2FUd%2FhjOcvku5SV9qxMbVNB6uZA5cd09CjY56 ac223NDQNut1%2bk4P5r3%2f1rZd5Wazy66Agp5KI5y5CqEWQ0d1101sv0frAnKZBqTYb6055oH2NnRZpjELWaFu%2bF72emR3bsCNdh60D51CFhmH6Znu5Cv0yej111i vAT7gyg58ZjycafR64rW%2bxFb0mp2i2t5inArq2IjUv0lqYt64p5pwQCFqCCFNQVZdQJVxMqDFAW7JefjRvA95C6kf3natPRU59nG%2f32bbz7t9pG%2f2v2thyEch%2be31ltBt6tDu %2b%2b9Uv&RelayState=http%3a%2f%2fwww.msftconnecttest.com%2fredirect ontrol-Allow-Origin : * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol-Allow-Methods: * ontrol.Allow-Methods: * ontrol.Allow-Me</pre>	i=0.9 5zXfPphi 1DqKl8 iØR8nxy5 i⊙ZZ6uL1	:FJwQ7Wei į8SP3p%2: 33NHymjgi IIPB%2bL∙	MON fcC Dj% tgG
170 reque	ists received (125 hidden)			~

Figure 15: URL Redirect sent by Versa CPE

SAML AuthN request sent by Versa CPE to Client Browser:

SAN	Al-tracer	_		×
× Clear	Il Pause			
GET	http://www.msftconnecttest.com/redirect			
GET	https://login-uat.cloudi-fi.net/start/ebd2613d4b6d34dafb516c3125326b2e/c11aed16a26be518863a55c1820dacc1?SAMLRequest=jVLBbtswDL33KwyftoNjS47dR	EgCeA2	KBei6c <mark>S</mark> A	ML
GET	https://login-uat.cloudi-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_f0b96c4792eb0acb0de795790c98ee3400c60f5f2c%3Ahttps%3A%2F%2F	login-uat	.cloudi-fi.r	et%2
GET	https://login-uat.cloudi-fi.net/template/cloudifi_base_v2/fonts/avenir/Avenir-Book.woff2			
GET	https://login-uat.cloudi-fi.net/template/cloudifi_base_v2/fonts/avenir/Avenir-Heavy.woff2			
POST	https://login-uat.cloudi-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_10b96c4/92eb0acb0de/95/90c98ee3400c60t5t2c%3Ahttps%3A%2F%2F https://login-uat.cloudi-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_10b96c4/92eb0acb0de/95/90c98ee3400c60t5t2c%3Ahttps%3A%2F%2F	login-uat	.cloudi-fi.r	et%2
PUST	nups //cloud-li.versa-networks.com.44991/versa-ilexvni/sso/tp/login-consumer		SA SA	ML
GET	http://www.msitcomecuest.com/editect			
GET	nups//www.insit.com/?ocid=wspidpc=u411			· · ·
HTTP	Parameters SAML Summary			
<samlp:#< td=""><td><pre>AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:assertion" ID="(null)_bbf31887f0a0131f1c215ea6da296fba" Version="2.0" ProviderName="Versa-flexVNF" IssueInstant="2020-12-14T15:23:272" Destination="https://login-uat.cloudi-fi.net/start/ebd2613d4b6d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POSt_com:44991/versa-flexvnf/sso/tp/login-consumer"</pre></td><td></td><td></td><td>•</td></samlp:#<>	<pre>AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:assertion" ID="(null)_bbf31887f0a0131f1c215ea6da296fba" Version="2.0" ProviderName="Versa-flexVNF" IssueInstant="2020-12-14T15:23:272" Destination="https://login-uat.cloudi-fi.net/start/ebd2613d4b6d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POSt_com:44991/versa-flexvnf/sso/tp/login-consumer"</pre>			•
<san <san <td>nl:ISsuer>https://cloud-fi.versa-networks.com:44991/metadata nlp:nameIDFOILCy Format= urn:oasis:names:tc:>APL:1.1:nameid=Tormat:emailAddress" AllowCreate="true" /> AuthnRequest></td><td></td><td></td><td></td></san </san 	nl:ISsuer>https://cloud-fi.versa-networks.com:44991/metadata nlp:nameIDFOILCy Format= urn:oasis:names:tc:>APL:1.1:nameid=Tormat:emailAddress" AllowCreate="true" /> AuthnRequest>			

Figure 16: SAML AuthN request





Step 2: Client Browser connects to IDP, present AuthN request and gets authentication page

🔍 SAM	IL-tracer —		\times
imesClear	li Pause ± Autoscroli ⊽ Filter resources 👌 Colorize 💩 Export 🛓 Import		
GET GET	http://www.msftconnecttest.com/redirect https://login-uat.cloudi-fi.net/start/ebd2613d4b6d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?SAMLRequest=jVLBbtswDL33KwyftoNjS47dREgCeA2KI	Bei6c <mark>SAN</mark>	1
GET GET POST POST GET GET	https://iogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp/2AuthState=_00b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.net/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_0b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/module.ptp/multiauth/selectsource.ptp?AuthState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/module.ptp/multiauth/selectsource.ptp?//authState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/selectsource.ptp?//authState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/selectsource.ptp?/authState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/selectsource.ptp?/authState=_10b96c4792eb0acb0de795790c98ee3400c60/5/2c%3Ahttps%3A%2F%2Flogin-uat.cloudi-fi.se/auth/selectsource.ptp?/authStat	:loudi-fi.nel :loudi-fi.nel SAN	₩2 11
HTTP	Parameters		
GET http uat.clou networks 863a55c1 Upgrade- User-Age Accept: Sec-Fetc Sec-Fetc Sec-Fetc Sec-Fetc Accept-E Accept-L Cookie:	<pre>si//login-ust.cloudi-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_f0096c4792c00ac00dr95790c98e3400c60f5f2c%3Ahttps%3Av25F did-fi.net%2Fstart%2Fobd2613d46d3dafb516c375235026x%2Fc1laed16a26bs518863a55c1820dac1%3Fspentiyid%3Dhttps%253Av25Fr%25Fc1oud-fi.versa- .com%253A44991%25Fmetadata%26Relay5tate%3Dhttp%253A%252F%252Fwww.msftconnecttest.com%252Fredirect%26cookieTime%3D1607959405%261h%3Dc11aed .god%cc1%256c4%3D0ed26513d4b6d3dafb516c3f25326b2e HTTP/1.1 Insecure=Requests: 1 int: Moxilla(5.0 (Windows NT 10.0; Win64; x6d) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 h-Site: none h-Mede: navigate h-User: ?1 h-Dest: document incoding: gzip, deflate, br anguage: en-US_en;q=0.9 Cookie-FI-Prd=kfhvk2rvc0cc34p854qb51sq31</pre>	%2Flogin- 16a26be51	. 4
HTTP/1.1 Server: Date: Mo Content- Transfer Connecti Vary: Ac	200 OK nginx ng 14 Dec 2020 15:23:26 GMT Type: text/html; charset=UTF-8 -Encoding: chunked con: keep-alive cept-Encoding		
Access-C Access-C Set-Cook Expires: Cache-Co Pragma:	iontrol Allow Origin: login-uat.cloudi-fi.net iontrol-Allow Methods: GET, POST, PUT, DELETE, OPTIONS ie: Cookie-FI.Prd-ktNkZrvC0cc240554b51sq31; expires=Tue, 15-Dec-2020 01:23:26 GMT; Max-Age=36000; path=/; domain=.cloudi-fi.net; secure; Thu, 19 Nov 1981 08:52:00 GMT ontrol: no-store, no-cache, must-revalidate no-cache	HttpOnly	r •
170 reque	ests received (125 hidden)		

Cloudi-Fi × +						-	٥	\times
\leftarrow \rightarrow \circlearrowright \land https://login-uat.cloudi-fi.net/a	uth/module.php/multiauth/selectsource.php?AuthState=_9885	於	5∕≡	団	Pas en cours de	e synchronisation	2	
	CLOUDI-FI CONNECT WITH YOUR GUESTS Bienvenue sur notre accès Wi-Fi							
	Se connecter avec vos identifiants							
	Identifiant [*]							
	Mot de passe [®]							
	☐ J'accepte les <u>conditions d'utilisation</u> [*]							
	S'authentifier							
	S'enregistrer avec votre sponsor •							
	S'enregistrer avec votre mobile							•

Figure 17: Captive Portal authentication page





Step 3: Enter credentials (Id and Password), accept user conditions and click at authentication button

SAM	L-tracer —	×	<
Y Clear	II Pauso + Autoscrall C Eiller resources A Coloriza + Evont + Imont		
GET GET GET GET GET POST	In Page 2 Addoction of nutle resolutes to contract a Laport 2 import http://www.mstconnectlest.com/redirect https://login-uat.cloud-fi.net/atr/bd2b13ddbb33ddbb53ddbb5186532532b2e/c11aed162bbe518863a55c1820dacc19SAMLRequest=/VLBbtswDL33KwytoNjS47dREgCeA2KBe6d https://login-uat.cloud-fi.net/atr/bd2b13ddbb33ddbb51862b2b2e/c11aed162bbe518863a55c1820dacc19SAMLRequest=/VLBbtswDL33KwytoNjS47dREgCeA2KBe6d https://login-uat.cloud-fi.net/atr/bd2b13ddbb33ddbb51862b2e/c11aed162bbe518863a55c1820dacc19SAMLRequest=/VLBbtswDL33KwytoNjS47dREgCeA2KBe6d https://login-uat.cloud-fi.net/template/cloudifi_base_v2/fonts/avenir/Avenir-Beok woff2 https://login-uat.cloud-fi.net/template/cloudifi_base_v2/fonts/avenir/Avenir-Beok woff2 https://login-uat.cloud-fi.net/template/cloudifi_base_v2/fonts/avenir/Avenir-Beok woff2	5AML fi.net%	^
POST	https://cloud-fiversa-networks.com.44991/versa-flexvnf/sso/tp/login-consumer	SAML	j .
GET	ntp://www.msuconnectues.com/earlest https://www.msuconn/ecid=wispt&pc=u477		•
нттр	Darametars		
POST AuthStat fi.net/s networks 613d4b6d Error: accept_a checkAup hash: eb opt_defa password source: source: username	e: _f0096c4792eb0acb0de795790c98ee3400c60f5f2:https://login-uat.cloudi- tart/ebd26134db634dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?spentityid=https%3A%2F%2Fcloud-fi.versa- .com%3A44991%2Fmetadata&RelayState=http%3A%2F%2Fvwwv.msftconnecttest.com%2Fredirect&cookieTime=1607959405&lh=c11aed16a26be518863a55c1820dacc1&ch 34dafb516c3f25326b2e up: 1 : 1 d2613d4b634dafb516c3f25326b2e uitlocate: en : nyjyh8 umKnowntype unknowntype unknowntype unknowntype unknowntype unknowntype	=ebd2	•
170 reque	ists received (125 hidden)		~

Figure 18: login credentials submitted to Cloudi-Fi

Step 4: IDP (Cloudi-Fi) sends SAML response to client with AuthN response







🔍 SAN	1L-tracer											—		×
× Clear	II Pause ± A	utoscroll	♥ Filter resource	es 👌 Colorize 🛕 🗄	Export 🛓 Im	nport								
GET GET GET GET POST GET GET	http://www.msf https://login-ua https://login-ua https://login-ua https://login-ua https://login-ua https://cloud-fi http://www.msf https://www.msf	ftconnecti at cloudi-fi at cloudi-fi at cloudi-fi at cloudi-fi at cloudi-fi versa_ne ftconnecti sn.com/?e	est com/redirect net/start/ebd261: net/auth/module net/template/clou net/template/clou net/auth/module set com/redirect ccid=wispr&pc=u4	3d4b6d34dafb516c3f2 php/multiauth/selects udfi_base_v2/fonts/av difi_base_v2/fonts/av php/multiauth/selects t/versa-flexvnf/sso/tp/	25326b2e/c1 source.php?A venir/Avenir-E venir/Avenir-F source.php?A /login-consum	11aed16a26be518 AuthState=_00b96 Book.woff2 Heavy.woff2 AuthState=_f0b960 mer	863a55c1820c c4792eb0acb0 c4792eb0acb0	de795790c986	equest=jVLBb ee3400c60f5f2 ee3400c60f5f2	tswDL33Kwyfi c%3Ahttps%3 c%3Ahttps%3	to <mark>NjS47dRE</mark> A%2F%2FI A%2F%2FI	EgCeA2 ogin-ua ogin-ua	KBei6c <mark>S</mark> t.cloudi-fi. t.cloudi-fi. S	AML net%2 AML
Issuer Subject NameID Attribut * defau * accep * usern * profi * token * token * tsssi * issto	restatement: it_locale t_aup hame le ied h tt ryId on_duration	SAUNE	summary = https://logi = user6@cloudi = user6@cloudi	n-uat.cloudi-fi.ne -fi.net -fi.net	et/auth/sam	<pre>ml2/idp/metada1 = en = 1 = +3368822787: = Radius = 1 = user6@cloud: = 1 = 47021938 = 14400</pre>	ia.php 3 i-fi.net							•

🔩 SAM	L-tracer			-		\times
× Clear	II Pause 🛓	Autoscroll	♥ Filter resources Colorize			
GET GET GET GET POST POST GET GET	http://www.m https://login-u https://login-u https://login-u https://login-u https://cloud- https://cloud- http://www.m	sftconnectt uat.cloudi-fi uat.cloudi-fi uat.cloudi-fi uat.cloudi-fi iat.cloudi-fi fi.versa-ne sftconnectt nsn.com/?e	st.com/redirect net/start/ebd2613d4b6d34dalb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?SAMLRequest=jVLBbtswDL33KwyfloNj net/auth/module.php/multiauth/selectsource.php?AuthState=_10b96c4792eb0acb0de795790c98ee3400c60f5f2c%3Ahttps%3A% net/template/cloudifbase_v2/fonts/avenir/Avenir-Beok woff2 net/template/cloudifbase_v2/fonts/avenir/Avenir-Heavy woff2 net/template/cloudifbase_v2/fonts/avenir/Avenir-Heavy woff2 net/template/cloudif_base_v2/fonts/avenir/Avenir-Beok woff2 net	S47dREgCeA2 2F%2Flogin-ua 2F%2Flogin-ua	2KBei6c <mark>57</mark> at.cloudi-fi.r at.cloudi-fi.r S <i>f</i>	net%2
HTTP	Parameters	SAML	Summary			
Issuer Subject NameID		:	: https://login-uat.cloudi-fi.net/auth/saml2/idp/metadata.php :user6@cloudi-fi.net :user6@cloudi-fi.net			•
Attribut * defau * accep * usern * profi * Verif * token * resul * histo * sessi	eStatement: lt_locale t_aup ame le ied t ryId on_duration		= en - 1 = +33688227873 = Radius = 1 = user6@cloudi-fi.net = 1 = 47021938 = 14400			

Figure 19: SAML AuthN response sent by Cloudi-Fi





5. Service verification in Versa Director

4.1 User identification under Monitor tab

earch	Summary Services System Tools	5			Shell	Config Status • Upgrade Subscr
aul-lab	Home-CSG-Dev : 10.1.64.20	D5 Location 🔮 4 Squ	uare Edgar Degas,Soisy-sur-seine, Franc	e 91450		Reachable
	Services		Networking			
	SDWAN NGFW CGNAT	G PSEC Sessions VPN Clients	Interfaces	SPF SPFv3 BFD DHC	P DNS Stats COS VRP	Image: Second
			iGMP issi RIP	Switching LLDP		
	Anti Virus Decryption DNS Filter ne Protection	ring DoS Policies File Filtering IP Filter	ring Persistent Action Policies Sec	urity Packages Sessions URL Filtering	User Identification Vulnerability	Vulnerability Signature Web Proxy
	Live Users V Brief	\sim				Search III
	IP Address	Name	Status	Session Hits	Time To Expiry	Expiration Mode
	192.168.3.2	user1@cloudi-fi.net	Live	203	599	inactivity

Figure 20: User identification profile in Versa CPE

4.2 Logs > Authentication in Analytics

VERSA											8	🕕 🛈 pella (paul-l	lab (
V NETWORKS		Monitor	Configuration	Workflows	Administration	Analytics							
Analytics-Cluster-Analytics	-1 V									Europe	/Paris	~ 🖸	
<u>ه</u>	20	pau	l-lab		• Las	t day	~						
Dashboards	\sim												
SD-WAN	\sim	AUTH	Logs/										
Sites		Events	Policies Charts										
Sites Map													
Paths		Lad A	Authentication Events										
Security	>												
System	>	Sea	rch: Click to set a filter								Show 10	✓ entries	
.ogs	~										Com. (5		
Alarms		in Tin		Appliance	Profile	Mathod	Status	Status Mossago	Time Taken	User	Source Addres	nor Dectini	
DHCP	_	ve mi	1e		Fione		Status	Status message		USEI II	Source Addres	is to besuite	
Eirowall		5th 2	2020, 11:29:38 AM CE	I Home-CSG-Dev	Cloud-HI-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	Ums	user1@cloudi-fi.net	192.168.3.2	192.10	
CGNAT		5th 2	2020, 11:14:31 AM CE	T Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	Oms	user1@cloudi-fi.net	192.168.3.2	192.10	
Threat Detection		4th 2	2020, 4:23:11 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	0ms	user6@cloudi-fi.net	192.168.3.2	192.1(
Threat Filtering		4th 2	2020, 4:10:54 PM CET	Home-CSG-Dev	CIOUG-FI-SAML-AUTO-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	ums	user6@cloudi-fi.net	192.168.3.2	192.11	
Traffic Monitoring		4th 2	2020, 4:07:47 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	Oms	user6@cloudi-fi.net	192.168.3.2	192.16	
Web Monitoring		4th 2	2020, 4:03:26 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	0ms	user6@cloudi-fi.net	192.168.3.2	192.1(
SDWAN		4th 2	2020, 4:03:18 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	Oms	user6@cloudi-fi.net	192.168.3.2	192.1(
SSI Decryption		4th 2	2020, 4:00:21 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	Oms	user6@cloudi-fi.net	192.168.3.2	192.1(
ADC		4th 2	2020. 3:56:00 PM CET	Home-CSG-Dev	Cloud-Fi-SAMI -Auth-Profile	SAMI -authentication	success	SAML: Authentication Succeeded.	0ms	user5@cloudi-fi.net	192,168,3,2	192.1(
Guest VNF events		4										•	
DNS Proxy Packets captures			Showing 1 to 9 of 9 entries								Previous 1	Next	

Figure 21: Successful SAML Authentication logs in versa Analytics





6. ANNEX

What is a captive portal?

Technically speaking, an authentication screen is displayed when a wireless user is not authorized to access the network resources. The authentication page is called a captive portal login.

A Captive Portal can be triggered on the client device in 2 ways

- 1. DNS Redirection
- 2. Splash page

DNS redirection works as the simple DNS hijacking where all the user DNS requests are hijacked and resolved to the captive portal login page. But, after widespread use of HSTS header implementation, DNS redirection hits a low success ratio providing no better service to the users.

Whereas, a Splash Page works in a little different fashion. It also uses DNS redirections but, it responds to the requests acc. to the operating systems which trick the O.S in believing there is a captive portal login in place and forcing the O.S to automatically trigger the login page to the user.

What is splash page

When a client device is connected to the WiFi, if unauthorized to access the Internet, A screen automatically pops up to display the captive portal.

A Splash page not only bypasses HSTS implementations on most websites but also gives you the flexibility of showing O.S specific login pages.

Every operating system has its own different way of detecting Internet access.

The mechanism is this basically:

GET/POST http://foo.com/bar.html

If bar.html == [expected content] > Open Internet

If bar.html != [expected content] > Captive Portal

If bar.html[status] != SUCCESS > No Network

If a Captive Portal is not in place, the result will match the expected one and the OS will know that there is full access to the Internet.

If the URL returns a result other than the expected one, then the OS will detect that there is a Captive Portal in place and that it's needed to proceed with authentication in order to get full access to the Internet: In this case, the OS will open the Splash Page automatically.

All client devices use the above-described strategy to find out if they are behind a captive portal, but the URL might vary depending on the specific model of smartphone, tablet, laptop and depending on the specific OS version. In the following, you can find the list of domains that are contacted by each model in order to detect the captive portal.

Windows

www.msftconnecttest.com

www.msftncsi.com

Windows uses hardcoded IPv4 and ipv6 addresses to match the request response to verify the Internet connection.