



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 :

<https://www.dropbox.com/s/e5ouh3ono5hld43/Cloudi-Fi-Versa-11-20.pdf?dl=0>

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
3.1 Requirements	10
3.2 Roles	10
3.3 Configuration.....	11
4. Call Flow verification using SAML-Tracer Extension.....	17
5. Service verification in Versa Director	21
4.1 User identification under Monitor tab	21
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).

Thanks to the cloud, we are free from any border!

100M+ Unique users	82% of users sign in to be retargeted	3sec time to connect to internet
------------------------------	---	--



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

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

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
<p>Creation of captive portals according to country requirements</p>	<p>STRONG</p> <p>SMS LOCAL SOCIAL NETWORKS COUNTRY SPECIFIC ID</p> <p>MEDIUM</p> <p>SOCIAL NETWORKS EMAIL</p> <p>LOW</p> <p>DECLARATIVE ONLY CLICK THROUGH</p>	<ul style="list-style-type: none"> - Pseudonymisation of Internet logs - Log storage in compliance with local regulation (duration, location & how) 	<p>Help with Terms of use & Privacy policy write-up Option: surrogate legal responsibility to Cloudi-Fi</p>

Cloudi-Fi common criteria with Versa Networks

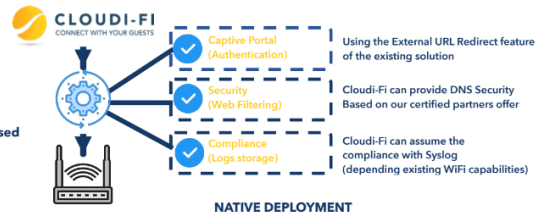
- Cloudi-Fi targets common verticals with Velocloud
 - Financial Services
 - Healthcare
 - Education
 - Industry
 - Retail
- We are the only Guest Wifi provider
 - Addressing both Corporate and Hotspots
 - With an international presence
 - That integrates with Captive Portal's key players such as Resellers and Content Providers



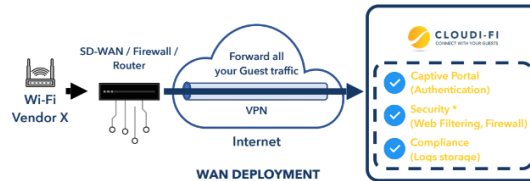
Smooth and transparent integration

Our deployments modes

- « Usual » Guest Wi-Fi deployment
- Cloudi-Fi enabled in the Customer **Wi-Fi infrastructure**
- Authentication, Security and Compliance **separately addressed**



- Cloudi-Fi enabled in the **Cloud : Easy deployment**, light configuration on site
- One VPN needed from your **SD-WAN / Firewall / Router**
- **All-in-One solution** (Authentication, Security* and Compliance natively)
- *Based on our certified partners offer



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.

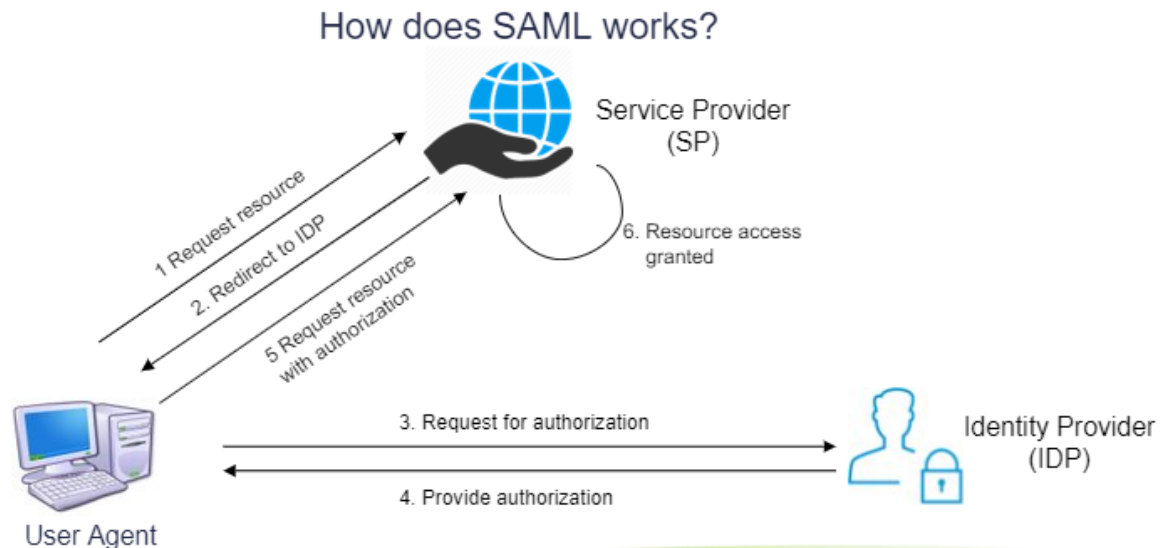


Figure 1: Secure Access SAML Authentication

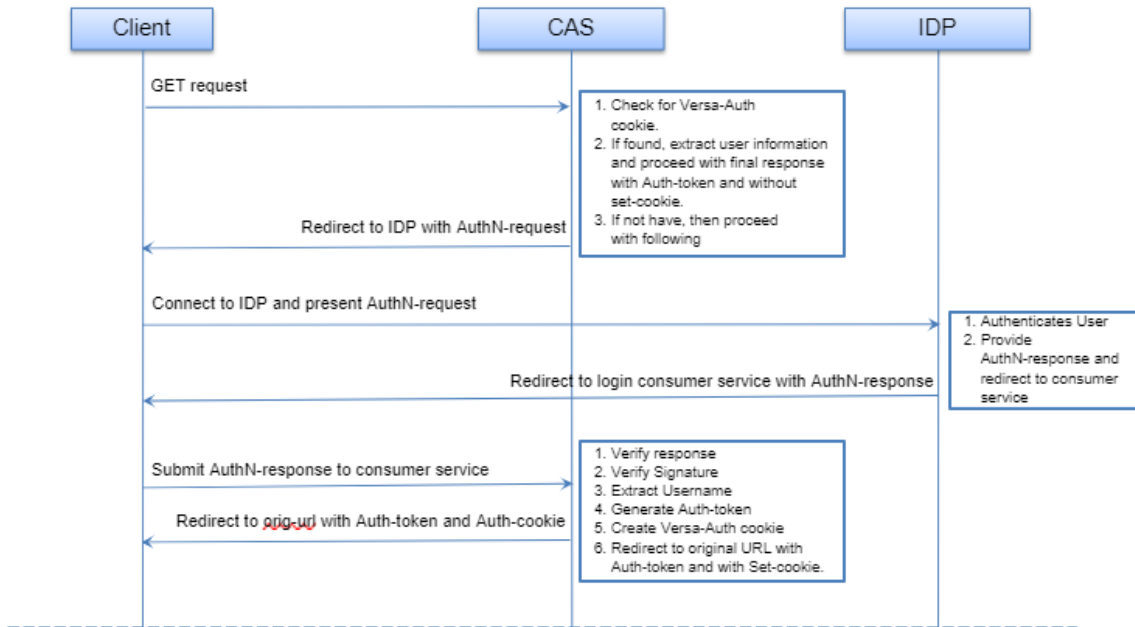


Figure 2: Workflow in Central Auth-server (CAS)

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 resolve 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:

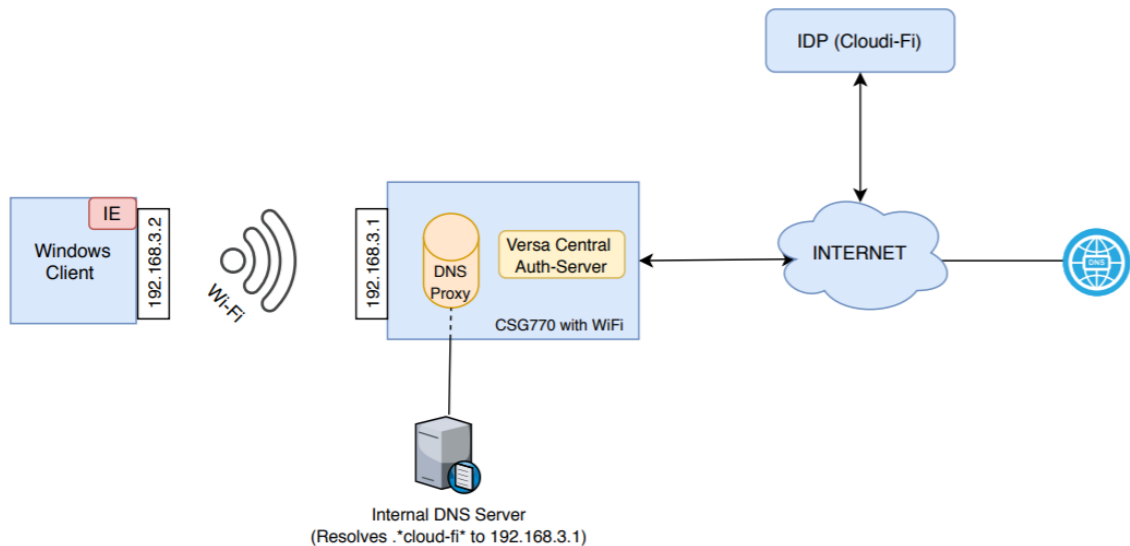


Figure 3: Cloudi-Fi and Versa Integration

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 Cloudfi to secure communication (Assertion and Attributes) between Versa VOS and Cloudfi;
- 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

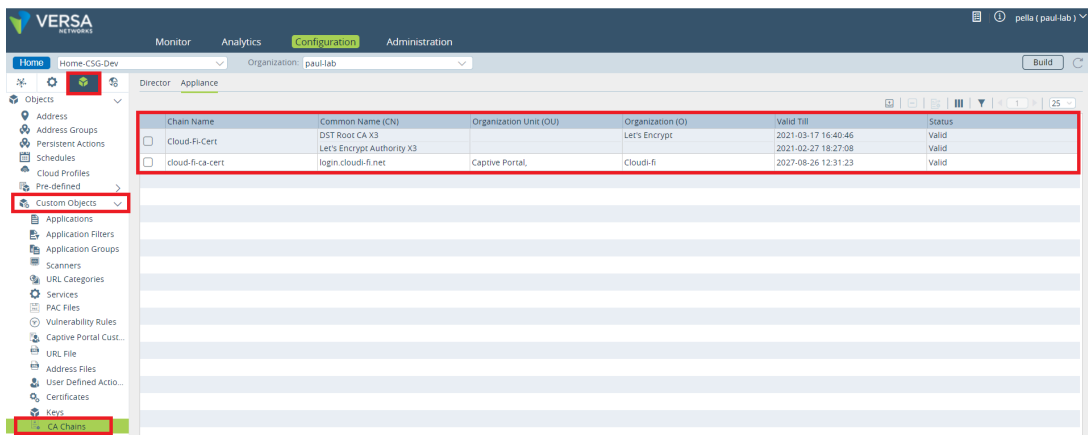
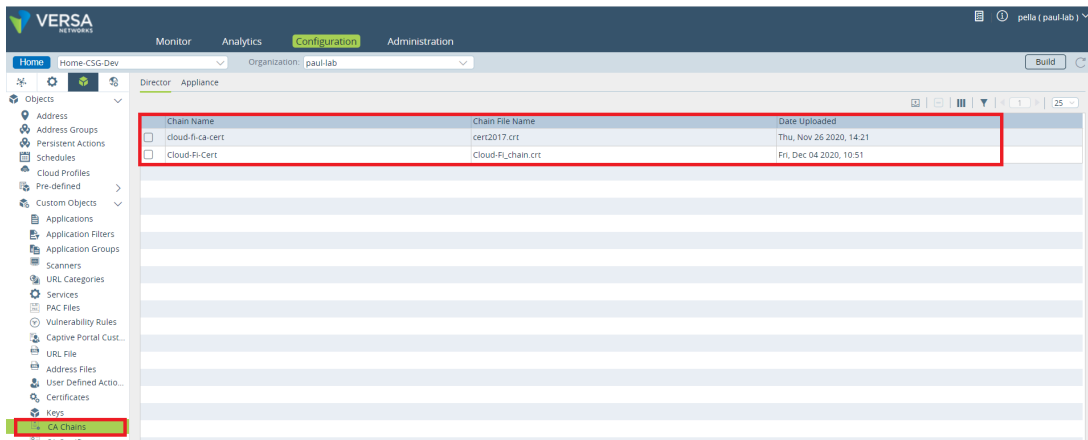


Figure 4: Upload Certificates in Versa Director

2 > Create SAML Profile

Go to:

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

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

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-ss0-url-filter

Name *
cloud-fi-ss0-url-filter

Description

Tags

Confidence URL File
--Select--

URL Patterns URL Strings

Search

Pattern	Reputation	
cloudi-fi	trustworthy	+

OK 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 Headers/Schedule Enforce

Applications

Application List

DNS

URL Categories

URL Category List

+ New Group + New Filter + New Application + New URL Category

OK Cancel

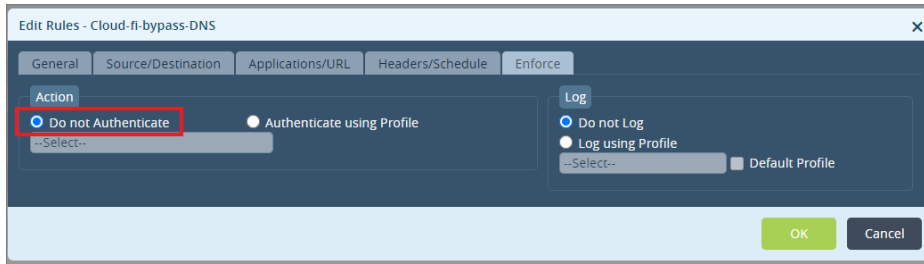


Figure 8: authentication rule to bypass DNS traffic authentication

6 > Create Authentication Rule for bypass Single Sign on URL

Go to:

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

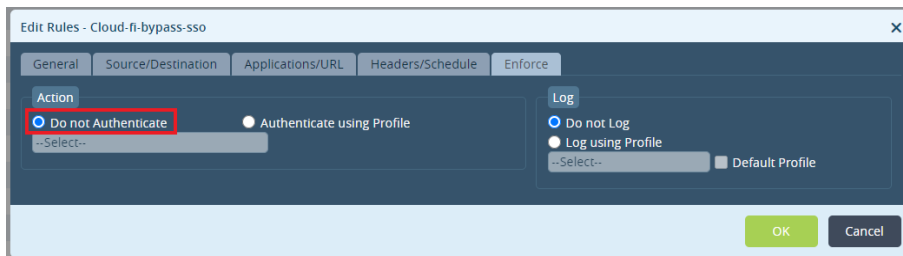
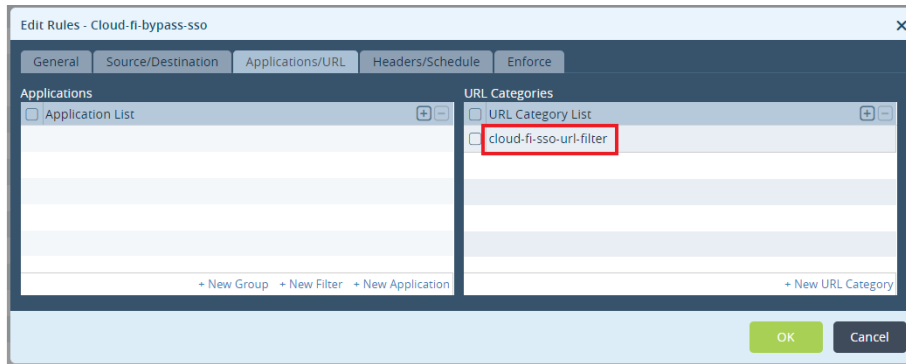


Figure 9: authentication rule to bypass Cloudi-Fi authentication servers

7 > Create Authentication Rule for SAML

Go to:

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

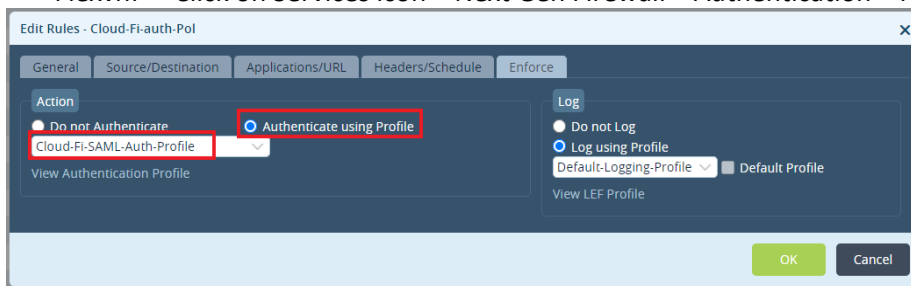


Figure 10: authentication rule for all wifi guest traffic

8 > Configure Captive Portal

Go to:

Flexvnf > Click on Services icon > Captive Portal

Figure 11 : Captive portal configuration in versa Director

9 > Configure DNS Proxy

o Configure SNAT Under Objects & Connectors > Objects > SNAT Pool

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

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

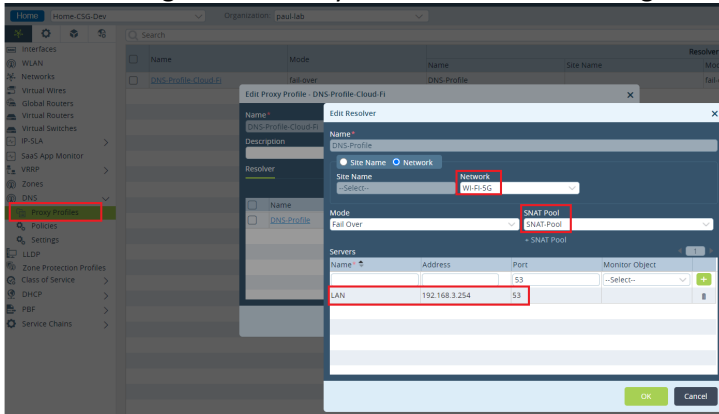


Figure 13: DNS Proxy Profile Configuration in versa Director

○ Configure DNS Proxy Policy under Networking > DNS > Policies

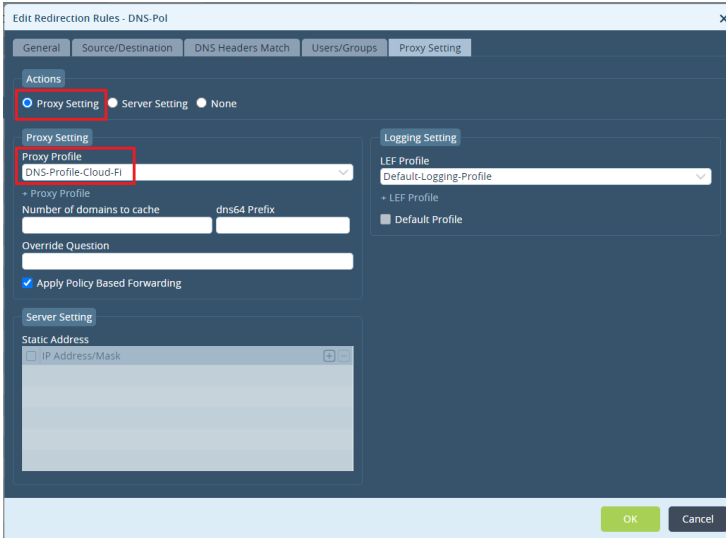
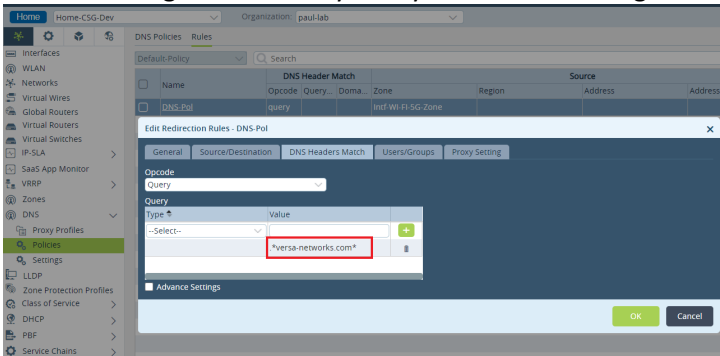


Figure 14: DNS Proxy Policy Configuration in versa Director

4. Call Flow verification using SAML-Tracer Extension

Step 1: Request Resource and Redirect to IDP

Figure 15: URL Redirect sent by Versa CPE

SAML AuthN request sent by Versa CPE to Client Browser:

Figure 16: SAML AuthN request

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

The screenshot shows a SAML-tracer window with a list of HTTP requests and responses. A specific GET request is highlighted with a red box:

```
GET https://login-uaat.cloudi-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_f0b96c4792eb0acb0de795790c98ee3400c60f5f2c%3Ahttps%3A%2F%2Flogin-uaat.cloudi-fi.net%2Fstart%2Febd2613d4b6d34dafb516c3f25326b2e%2Fc11aed16a26be518863a55c1820dacc1%3Fspentidyid%3Dhttps%253A%252F%252Fcloud-fi.versa-networks.com%253A44991%252Fmetadata%26RelayState%3Dhttps%253A%252F%252Fwww.msftconnecttest.com%252FRedirect%26cookieTime%3D1607959405%261h%3Dc11aed16a26be518863a55c1820dacc1%26ch%3D0ebd2613d4b6d34dafb516c3f25326b2e HTTP/1.1
```

The response is:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 14 Dec 2020 15:23:26 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: login-uaat.cloudi-fi.net
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Set-Cookie: Cookie-FI-Prd=kfhvk2rvc0cc34p854qbs1sq31; expires=Tue, 15-Dec-2020 01:23:26 GMT; Max-Age=36000; path=/; domain=.cloudi-fi.net; secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

The screenshot shows a captive portal authentication page for Cloudi-Fi. The page is in French and features a login form with the following elements:

- Cloudi-Fi logo and tagline: "CONNECT WITH YOUR GUESTS"
- Greeting: "Bienvenue sur notre accès Wi-Fi"
- Form title: "Se connecter avec vos identifiants"
- Input fields for "Identifiant*" and "Mot de passe*"
- Checkbox: "J'accepte les conditions d'utilisation*" with a link to "conditions d'utilisation"
- Buttons: "S'authentifier", "S'enregistrer avec votre sponsor", and "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

The screenshot shows the SAML-tracer interface with a list of HTTP requests. A POST request to `https://login-uat.cloud-fi.net/auth/module.php/multiauth/selectsource.php?AuthState=_f0b96c4792eb0acb0de795790c98ee3400c60f5f2c%3Ahttps%3A%2F%2Flogin-uat.cloud-fi.net%2Fstart/ebd2613d4b6d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?spentropyid=https%3A%2F%2Fcloud-fi.versa-networks.com%3A44991%2Fmetadatas&RelayState=http%3A%2F%2Fwww.msftconnecttest.com%2Fredirect&cookieTime=1607959405&hsc=11aed16a26be518863a55c1820dacc1&ch=ebd2613d4b6d34dafb516c3f25326b2e` is highlighted. The parameters section shows the following data:

```

AuthState: _f0b96c4792eb0acb0de795790c98ee3400c60f5f2c:https://login-uat.cloud-fi.net/start/ebd2613d4b6d34dafb516c3f25326b2e/c11aed16a26be518863a55c1820dacc1?spentropyid=https%3A%2F%2Fcloud-fi.versa-networks.com%3A44991%2Fmetadatas&RelayState=http%3A%2F%2Fwww.msftconnecttest.com%2Fredirect&cookieTime=1607959405&hsc=11aed16a26be518863a55c1820dacc1&ch=ebd2613d4b6d34dafb516c3f25326b2e
Error:
accept_aup: 1
checkAup: 1
hash: ebd2613d4b6d34dafb516c3f25326b2e
opt-default_locale: en
password: nyjvh8
source: unknowntype
source: unknowntype
source: unknowntype
username: +33688227873
    
```

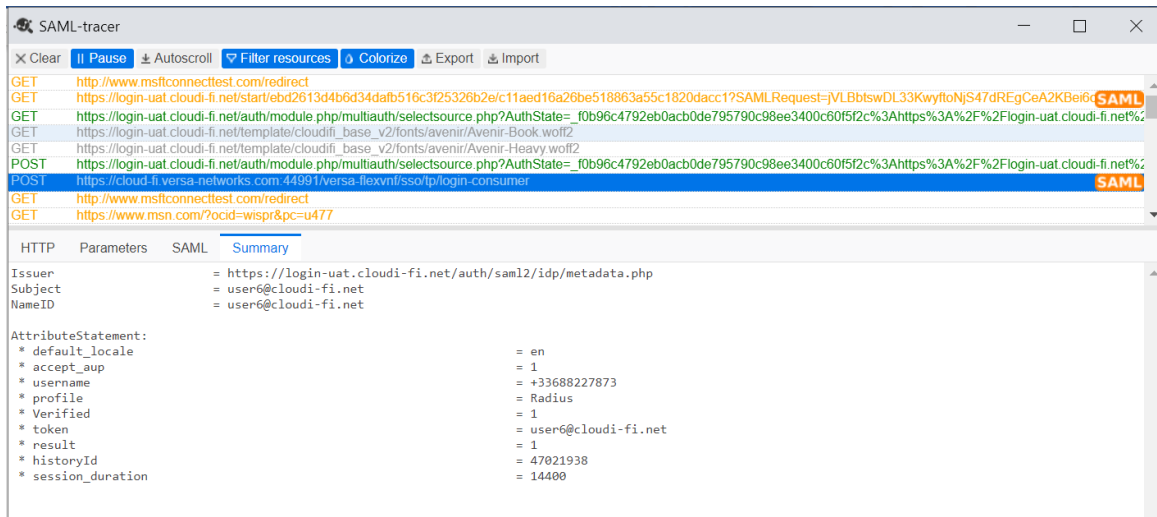
Figure 18: login credentials submitted to Cloudi-Fi

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

The screenshot shows the SAML-tracer interface with a SAML response highlighted. The response is a POST request to `https://cloud-fi.versa-networks.com:44991/versa-flexvnt/sso/tp/login-consumer`. The SAML response content is as follows:

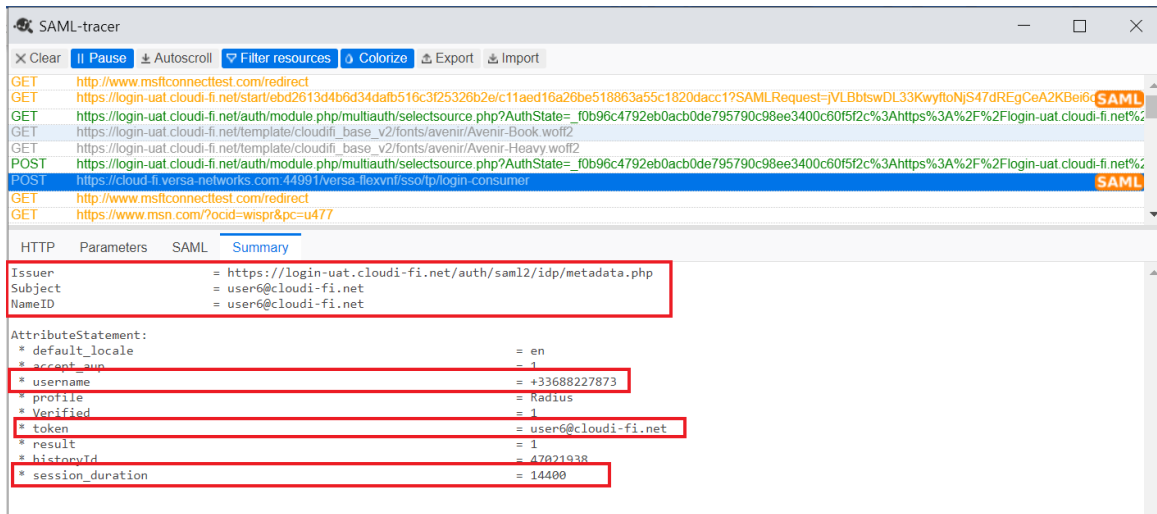
```

<saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_9b8f4a4388daf76f0b06a69dd43a6d07d117e3ee3"
  Version="2.0"
  IssueInstant="2020-12-14T15:23:38Z"
  Destination="https://cloud-fi.versa-networks.com:44991/versa-flexvnt/sso/tp/login-consumer"
  InResponseTo="(null)_bbf31887f0a0131f1c215ea6da296fba">
  <saml:Issuer>https://login-uat.cloud-fi.net/auth/saml2/idp/metadata.php</saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#_9b8f4a4388daf76f0b06a69dd43a6d07d117e3ee3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
        <ds:DigestValue>wAm7J12m19/74jY2o5Lmznckw/gYdreI+G/NV3tj0</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>eb+9MeYf0eXDJiFYxRbX9BiZoMVR2E39ywhuEz265XThPp7JddwaBxmEnM+hScPbHMW5A0ouDuVwfgT3rTA0k65ZJR+sXD+pIY1Jeaou0W6+x9Kq462MHiEwP/8gzXfcpjQFevjs2oELP/daVX5Xl9r15cbFR2uQuF/1eyizYV1rHlHirTo1wiq8CdLjBc50CC+8PXs+jQ09RkpIcYvgFt+Enrnc2mQdU5jH80pRhpvn752Y4IbBx7IpuLaa/z7PUmE71oF8MarZ7ZCJqX2ZFKAWAyoiAwwCDF2z2kd/cr/CQUFoDKGYP0WgnILb1SPhxJqjIw6KjgAa=</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
    
```



SAML-tracer interface showing a SAML response summary. The summary includes the following details:

- Issuer: https://login-uat.cloudi-fi.net/auth/saml2/idp/metadata.php
- Subject: user6@cloudi-fi.net
- NameID: user6@cloudi-fi.net
- AttributeStatement:
 - * default_locale: en
 - * accept_aup: 1
 - * username: +33688227873
 - * profile: Radius
 - * Verified: 1
 - * token: user6@cloudi-fi.net
 - * result: 1
 - * historyId: 47021938
 - * session_duration: 14400



SAML-tracer interface showing a SAML response summary with red boxes highlighting specific fields:

- Issuer: https://login-uat.cloudi-fi.net/auth/saml2/idp/metadata.php
- Subject: user6@cloudi-fi.net
- NameID: user6@cloudi-fi.net
- AttributeStatement:
 - * default_locale: en
 - * accept_aup: 1
 - * username: +33688227873
 - * profile: Radius
 - * Verified: 1
 - * token: user6@cloudi-fi.net
 - * result: 1
 - * historyId: 47021938
 - * session_duration: 14400

Figure 19: SAML AuthN response sent by Cloudi-Fi

5. Service verification in Versa Director

4.1 User identification under Monitor tab

The screenshot shows the Versa Director interface for a device named 'Home-CSG-Dev'. The 'Monitor' tab is active, and the 'User Identification' service is highlighted in the 'Services' section. Below, a table displays the 'Live Users' profile:

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

The screenshot shows the Versa Director Analytics interface for 'AuthN Logs'. The 'Authentication Events' table is displayed with the following data:

#	Time	Appliance	Profile	Method	Status	Status Message	Time Taken	User	Source Address	Desti
5th	2020, 11:29:38 AM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	0ms	user1@cloudi-fi.net	192.168.3.2	192.11
5th	2020, 11:14:31 AM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	0ms	user1@cloudi-fi.net	192.168.3.2	192.11
4th	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	192.11
4th	2020, 4:10:54 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	192.11
4th	2020, 4:07:47 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	192.11
4th	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	192.11
4th	2020, 4:03:18 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	192.11
4th	2020, 4:00:21 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	192.11
4th	2020, 3:56:00 PM CET	Home-CSG-Dev	Cloud-Fi-SAML-Auth-Profile	SAML-authentication	success	SAML : Authentication Succeeded.	0ms	user5@cloudi-fi.net	192.168.3.2	192.11

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.