CLOUDI-FI – VERSA WI-FI GUEST PROJECT

Prepared by Paul Christian Ella
Versa Networks

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		

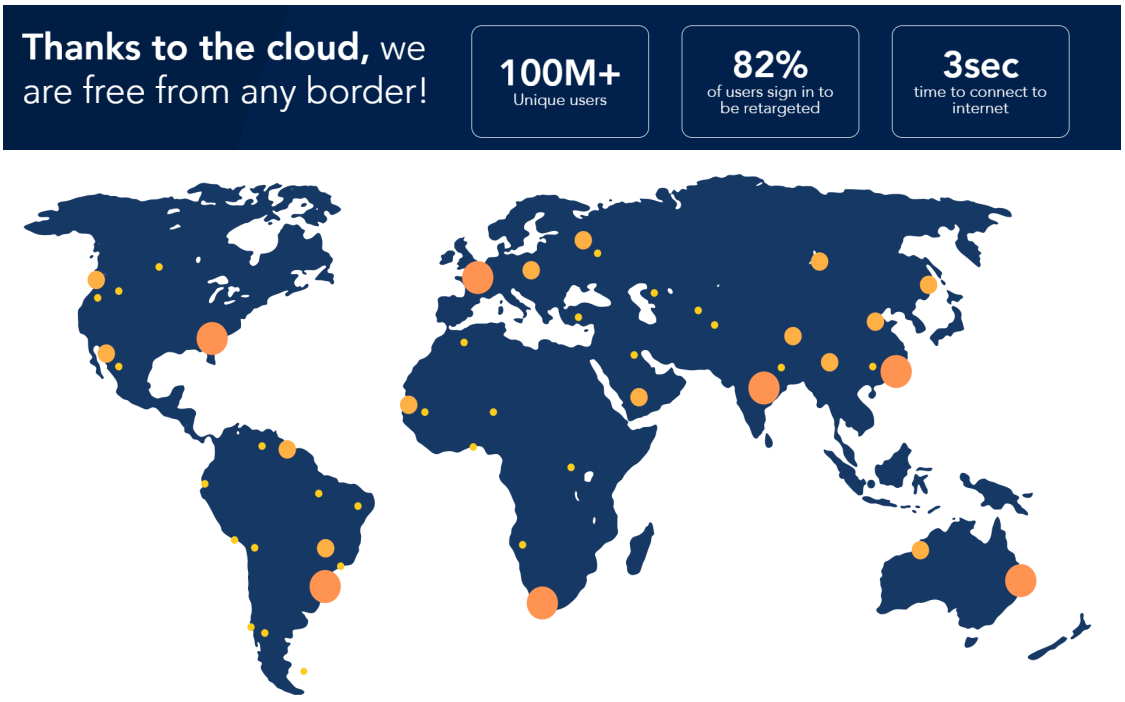
Contents

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 : https://www.cloudi-fi.com/

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

Creation of captive portals according to country requirements

DIFFERENT AUTHENTICATION LEVELS

STRONG

SMS
LOCAL SOCIAL NETWORKS
COUNTRY SPECIFIC ID

MEDIUM

SOCIAL NETWORKS
EMAIL

LOW

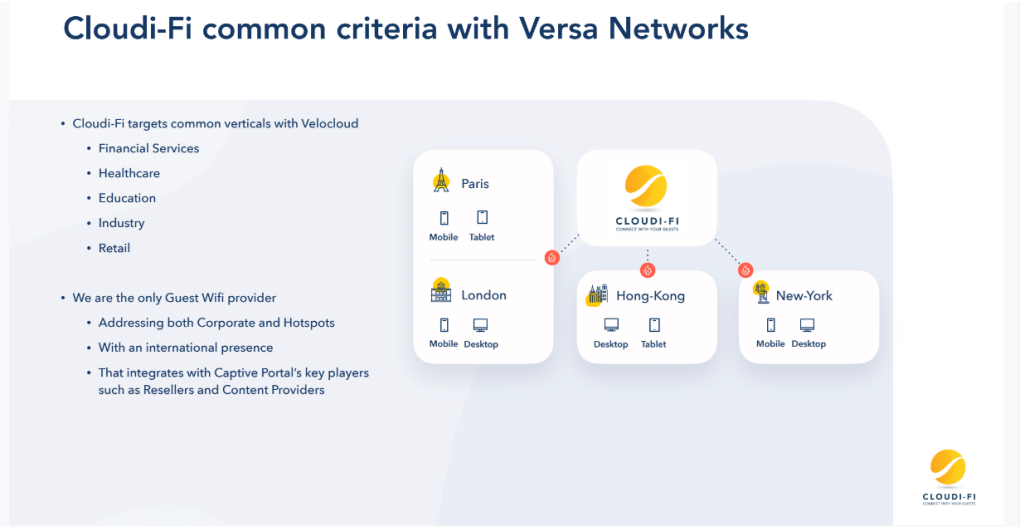
DECLARATIVE ONLY
CLICK THROUGH

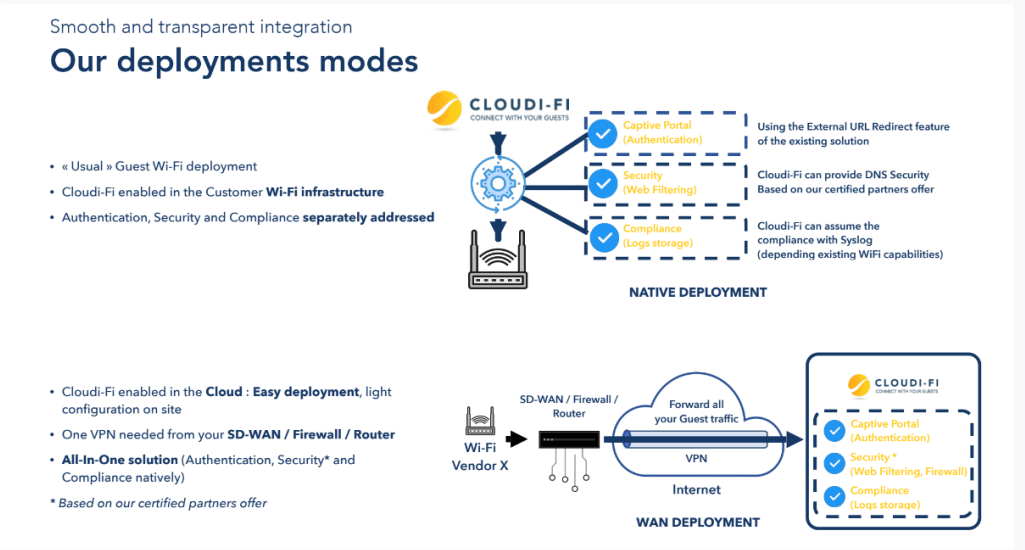
ENCRYPTION OF DATA COLLECTED

- Pseudonimysation of Internet logs
- Log storage in compliance with local regulation (duration, location & how)

LEGAL ASSISTANCE

Help with Terms of use & Privacy policy write-up
Option: surrogate legal responsibility to 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.

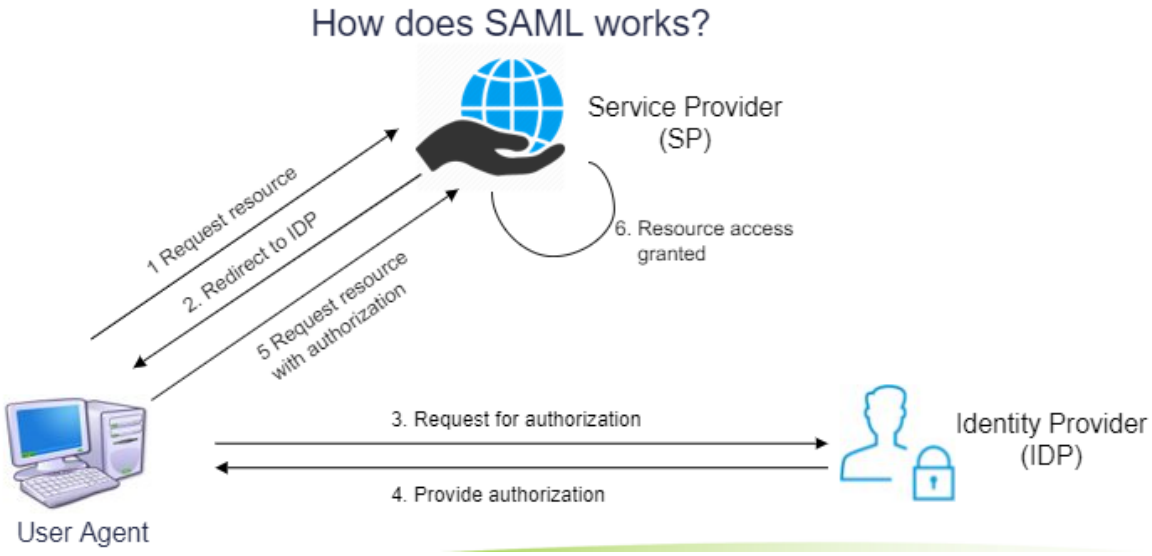


Figure 1: Secure Access SAML Authentication

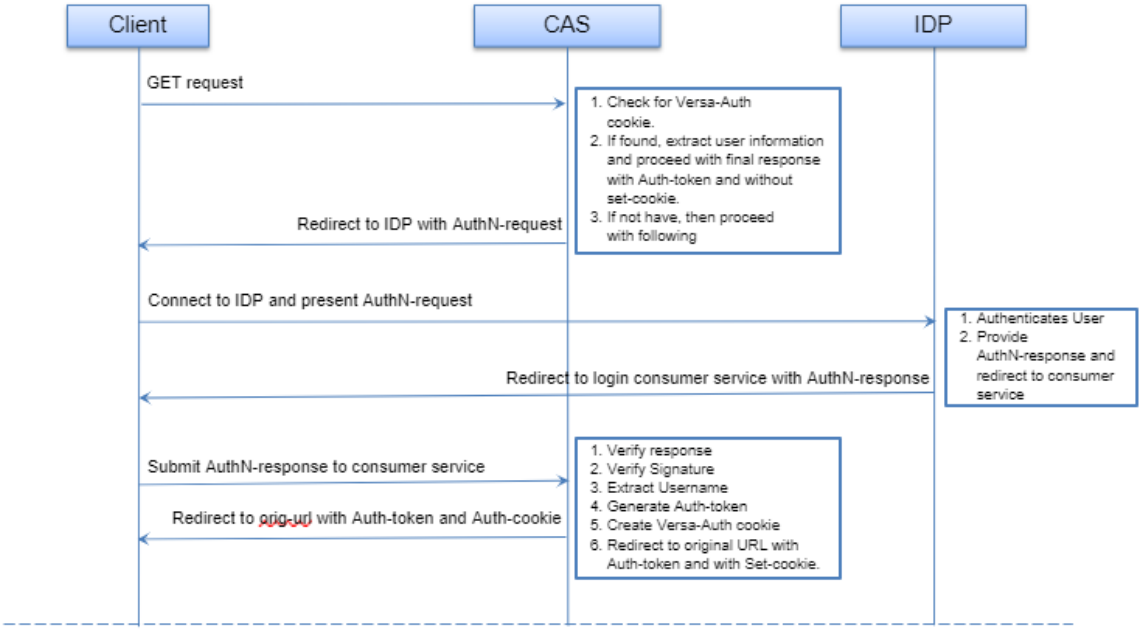


Figure 2: Workflow in Central Auth-server (CAS)

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:

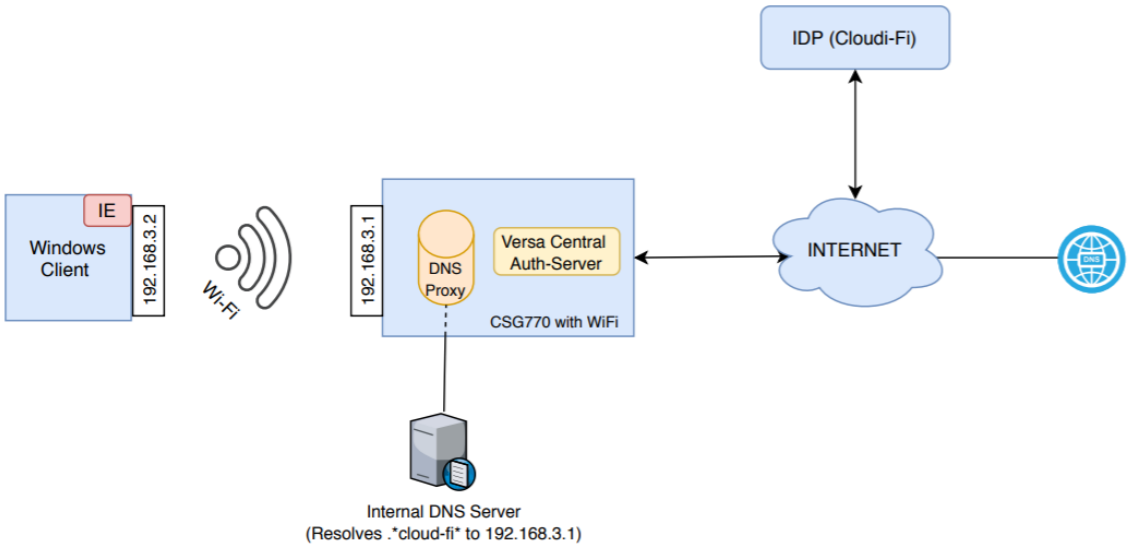


Figure 3: Cloudi-Fi and Versa Integration

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

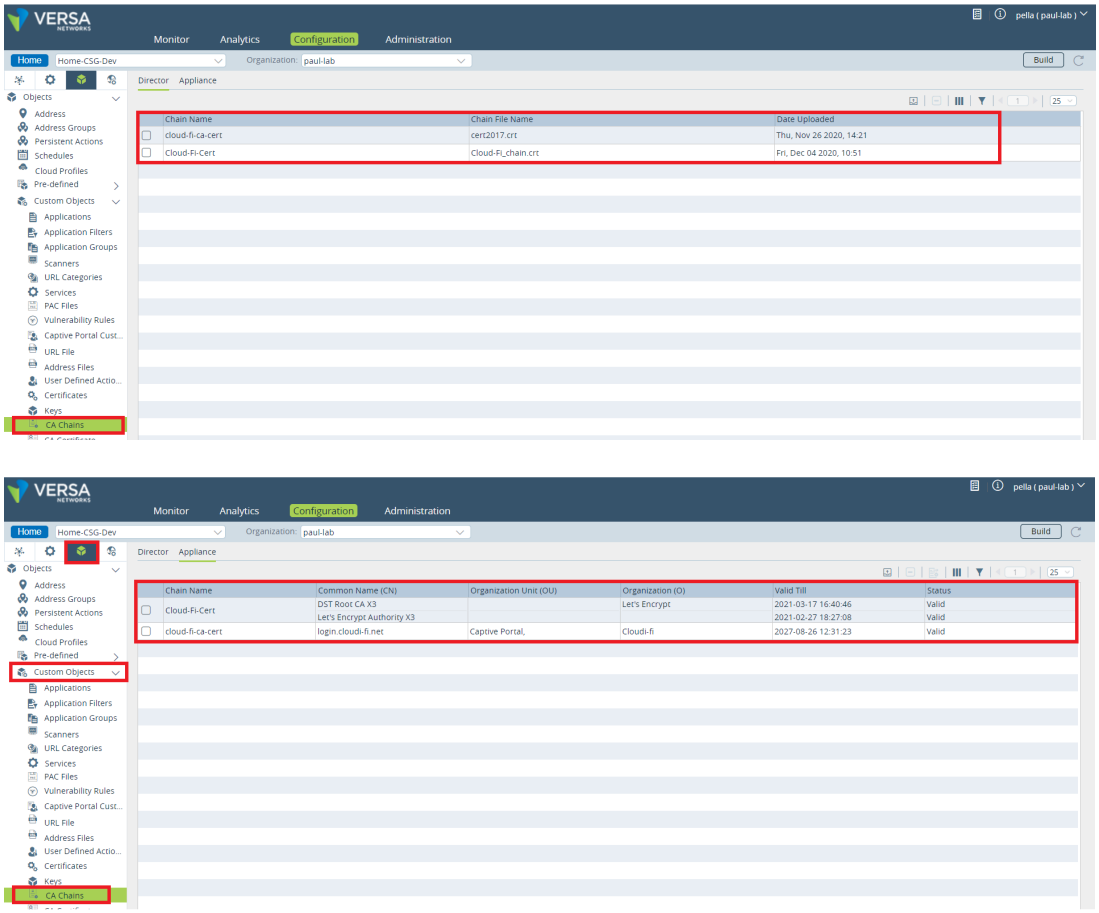


Figure 4: Upload Certificates in Versa Director

2 > Create SAML Profile

Go to:

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

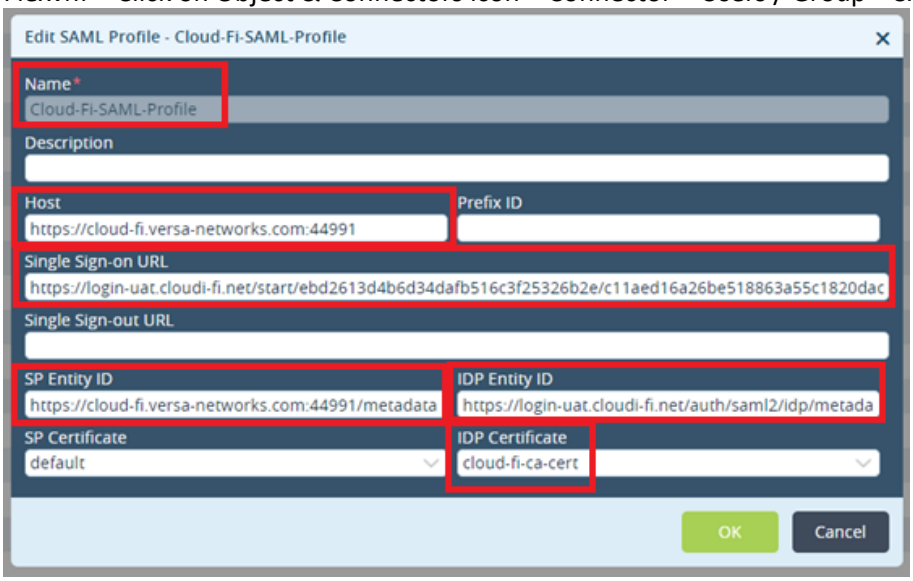


Figure 5: SAML Profile Configuration in Versa Director

3 > Create Authentication Profile for SAML

Go to:

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

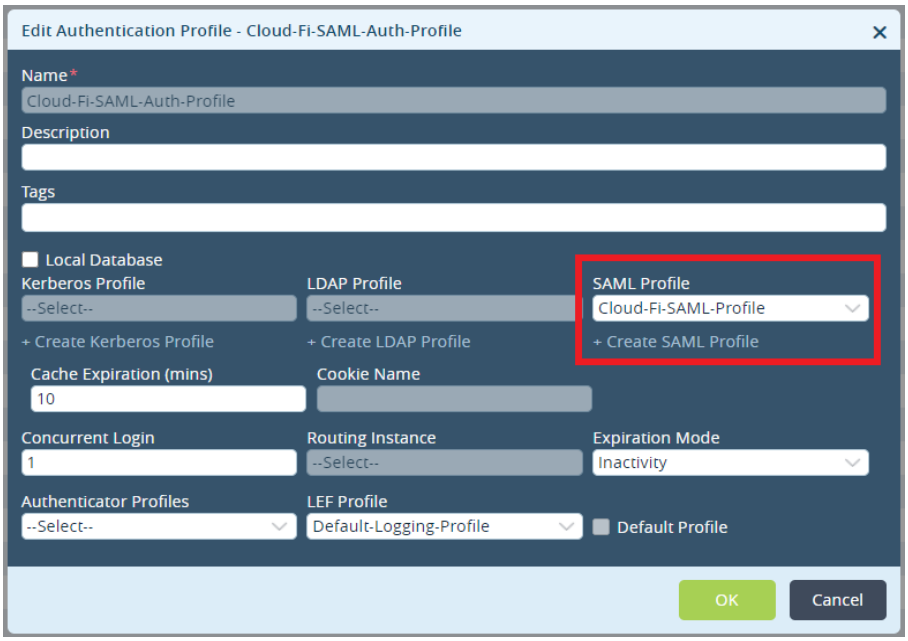


Figure 6: SAML Authentication Profile Configuration in Versa Director

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

Go to:

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

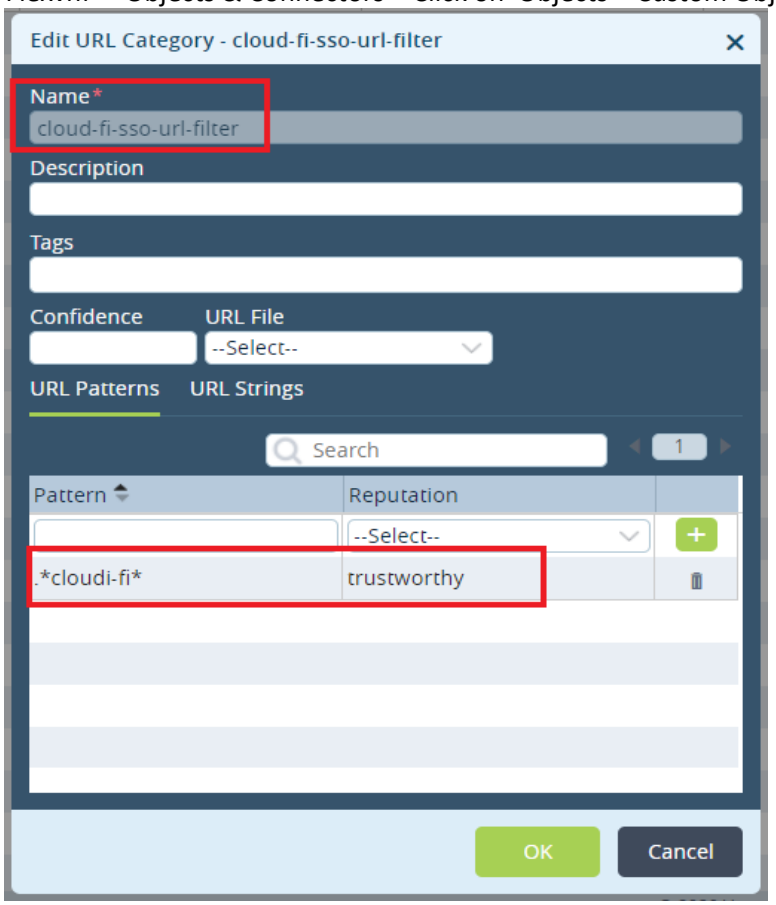
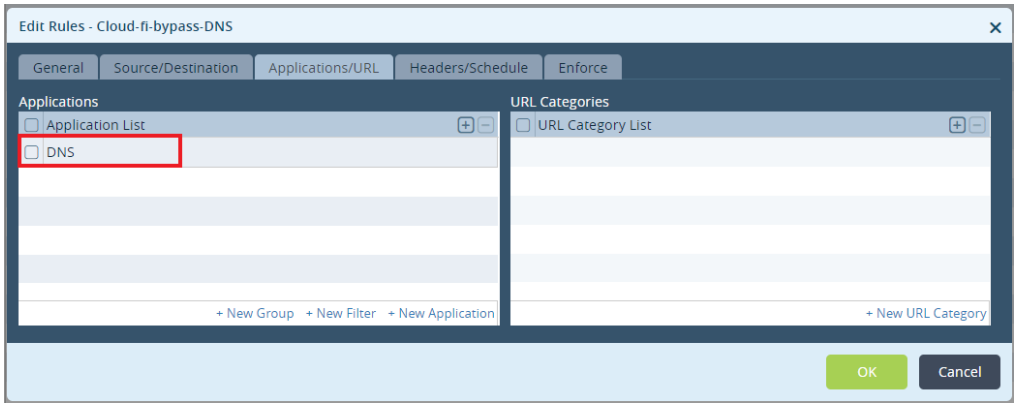


Figure 7: URL Category of Cloudi-Fi authentication servers

5 > Create Authentication Rule for bypass DNS Traffic

Go to:

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



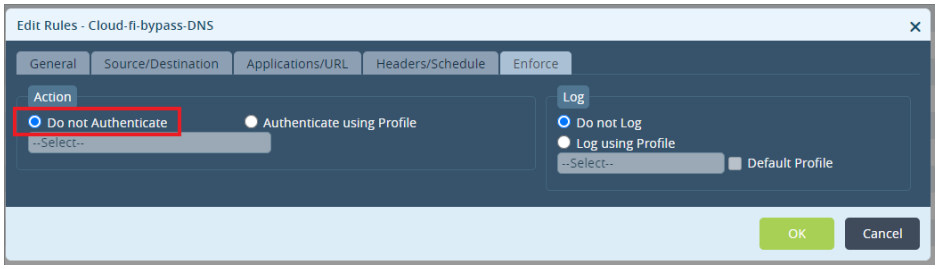
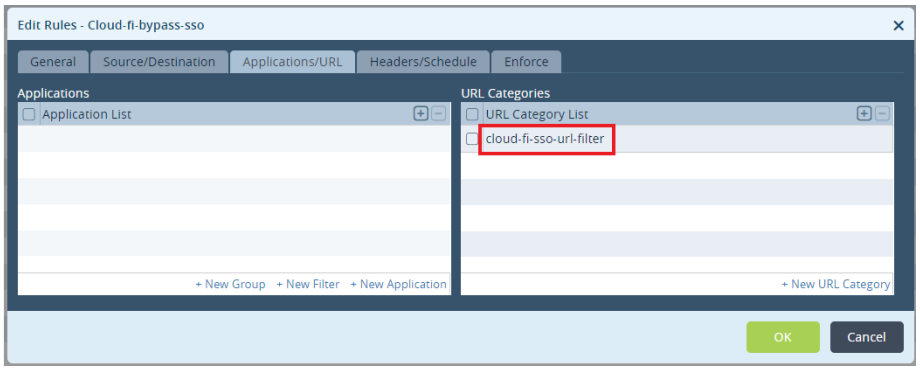


Figure 8: authentication rule to bypass DNS traffic authentication

6 > Create Authentication Rule for bypass Single Sign on URL

Go to:

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



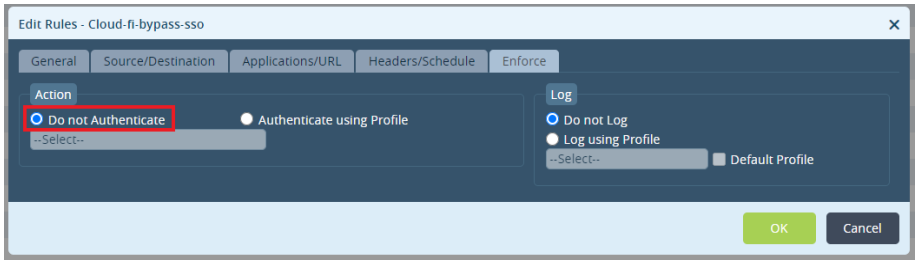


Figure 9: authentication rule to bypass Cloudi-Fi authentication servers

7 > Create Authentication Rule for SAML

Go to:

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

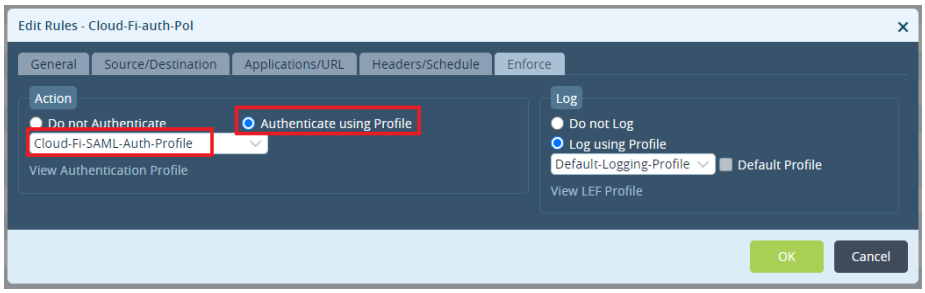


Figure 10: authentication rule for all wifi guest traffic

8 > Configure Captive Portal

Go to:

Flexvnf > Click on Services icon > Captive Portal

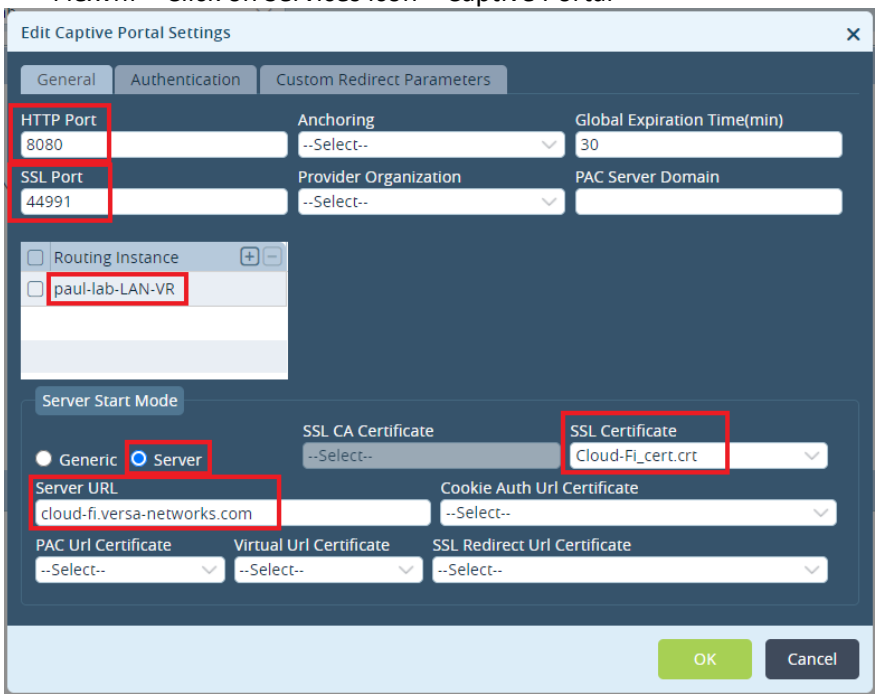


Figure 11 : Captive portal configuration in versa Director

9 > Configure DNS Proxy

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

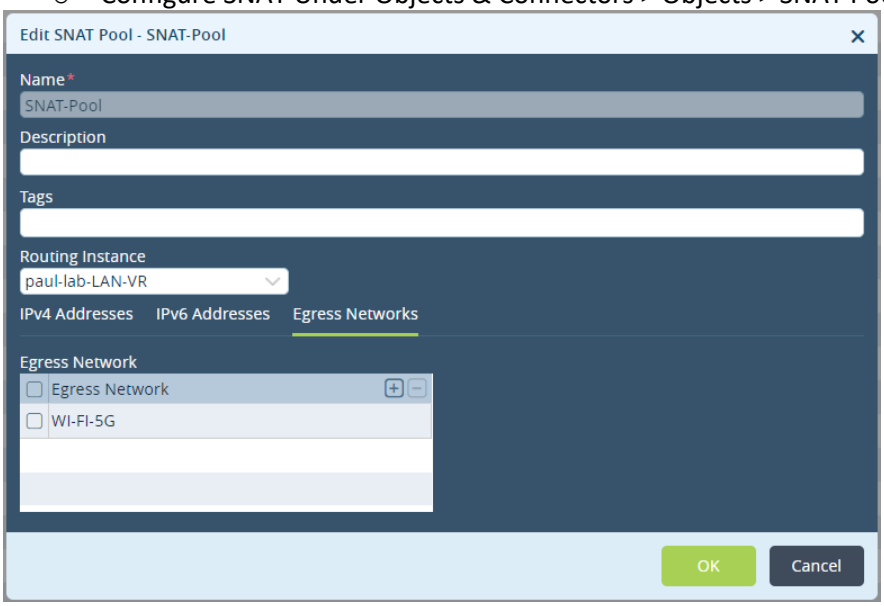


Figure 12: SNAT Pool Configuration for DNS Proxy in versa Director

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

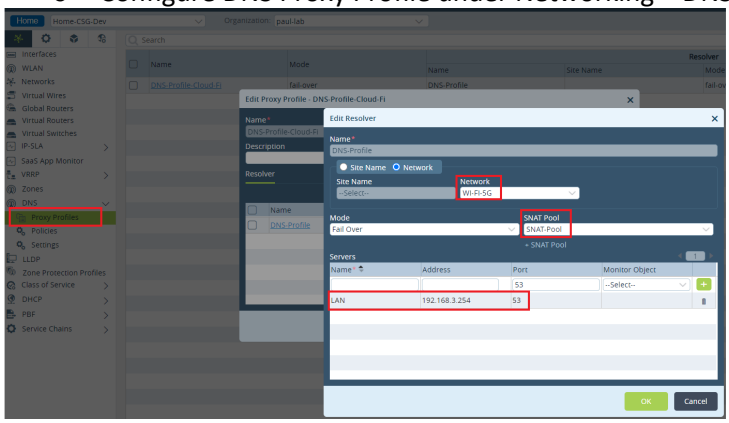
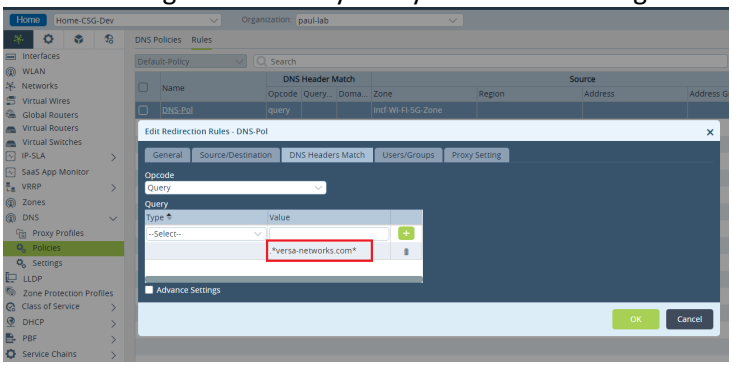


Figure 13: DNS Proxy Profile Configuration in versa Director

- Configure DNS Proxy Policy under Networking > DNS > Policies



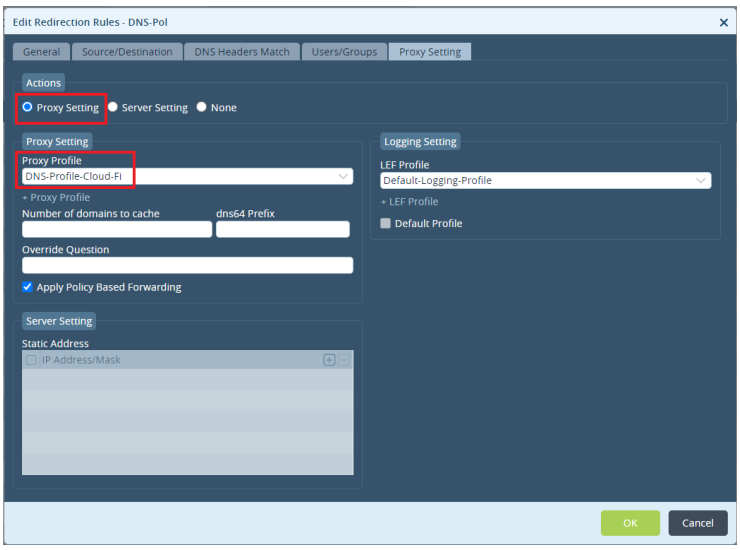


Figure 14: DNS Proxy Policy Configuration in versa Director

4. Call Flow verification using SAML-Tracer Extension

Step 1: Request Resource and Redirect to IDP

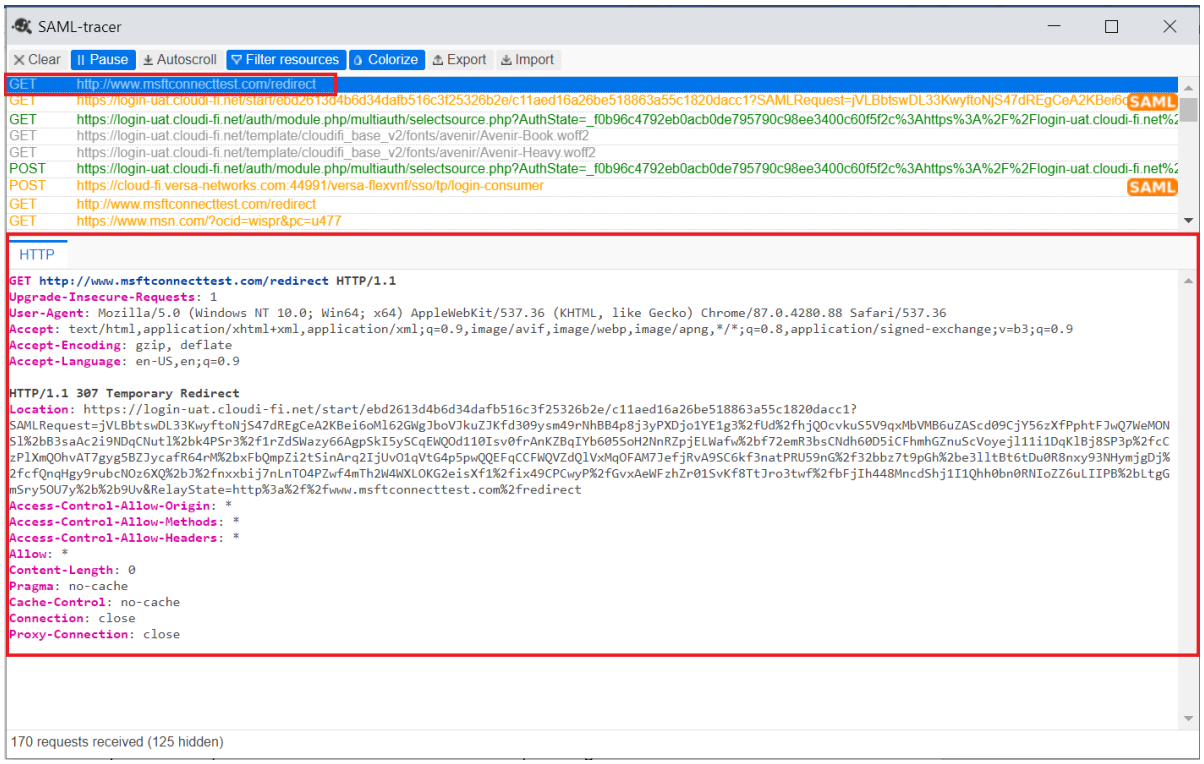


Figure 15: URL Redirect sent by Versa CPE

SAML AuthN request sent by Versa CPE to Client Browser:

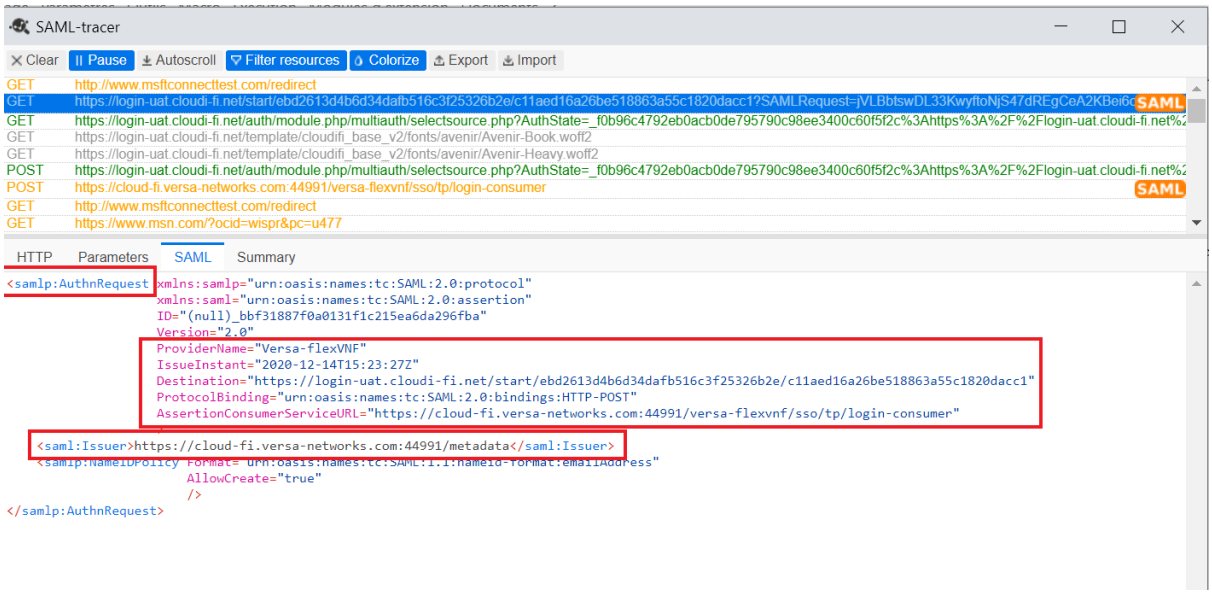
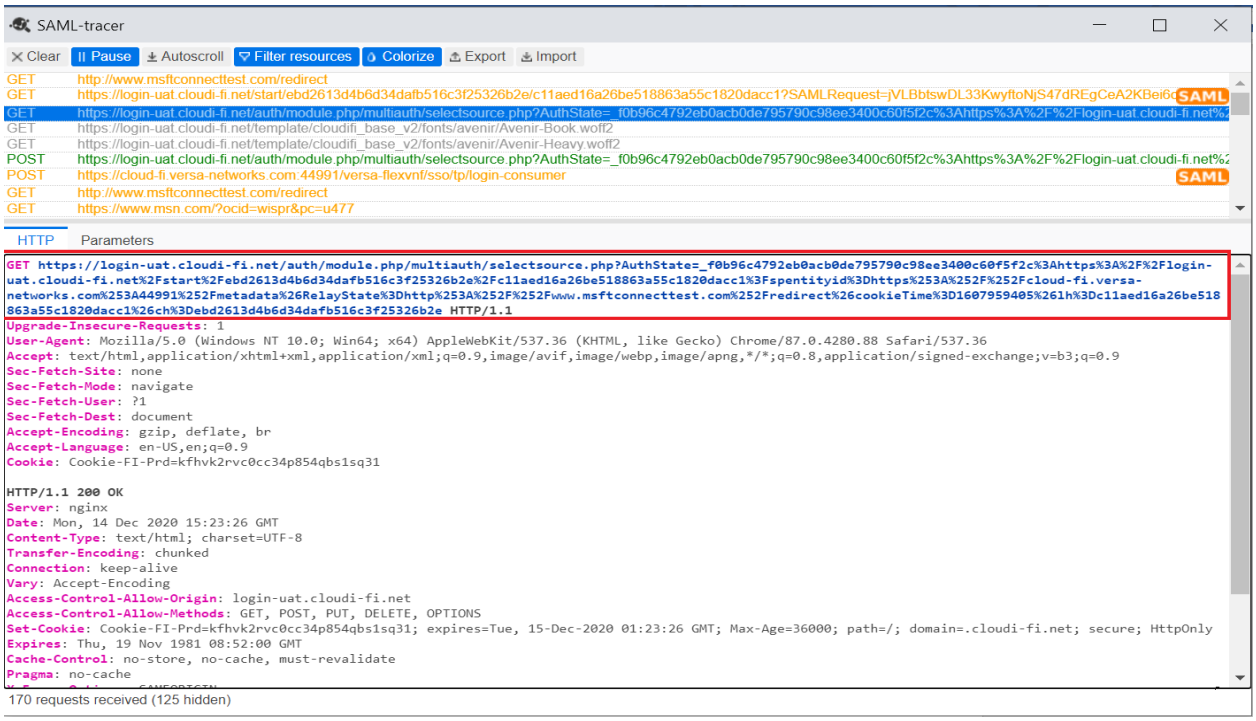


Figure 16: SAML AuthN request

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



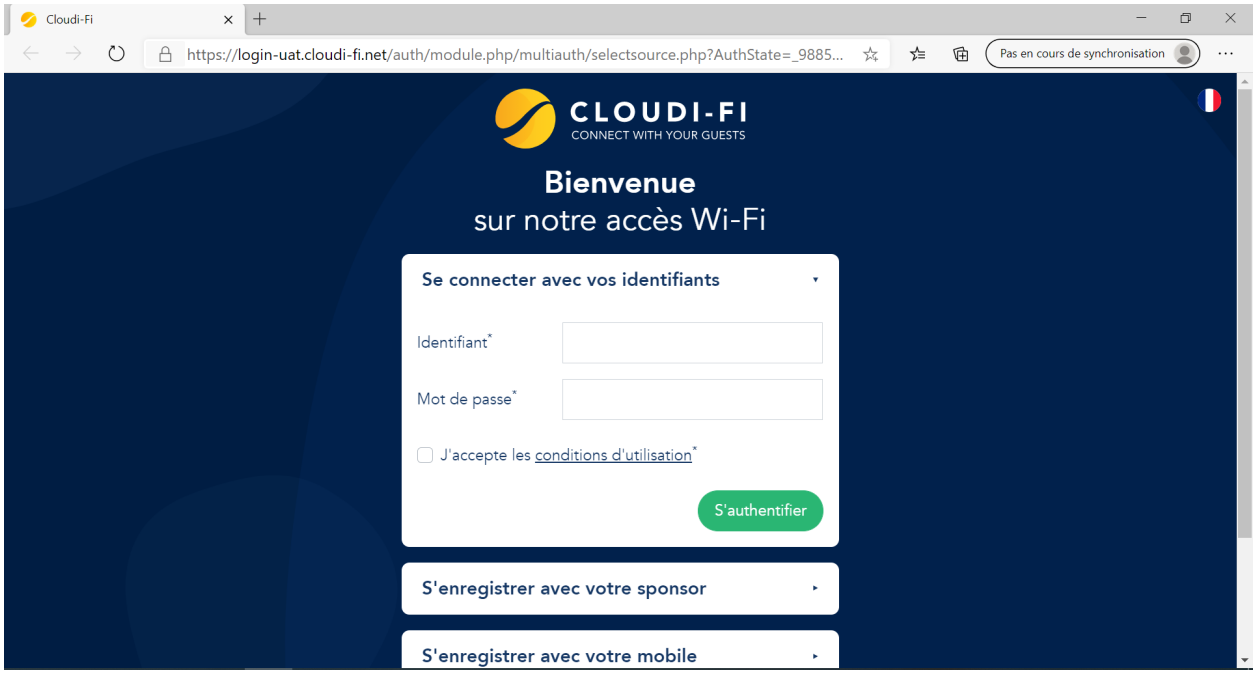


Figure 17: Captive Portal authentication page

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

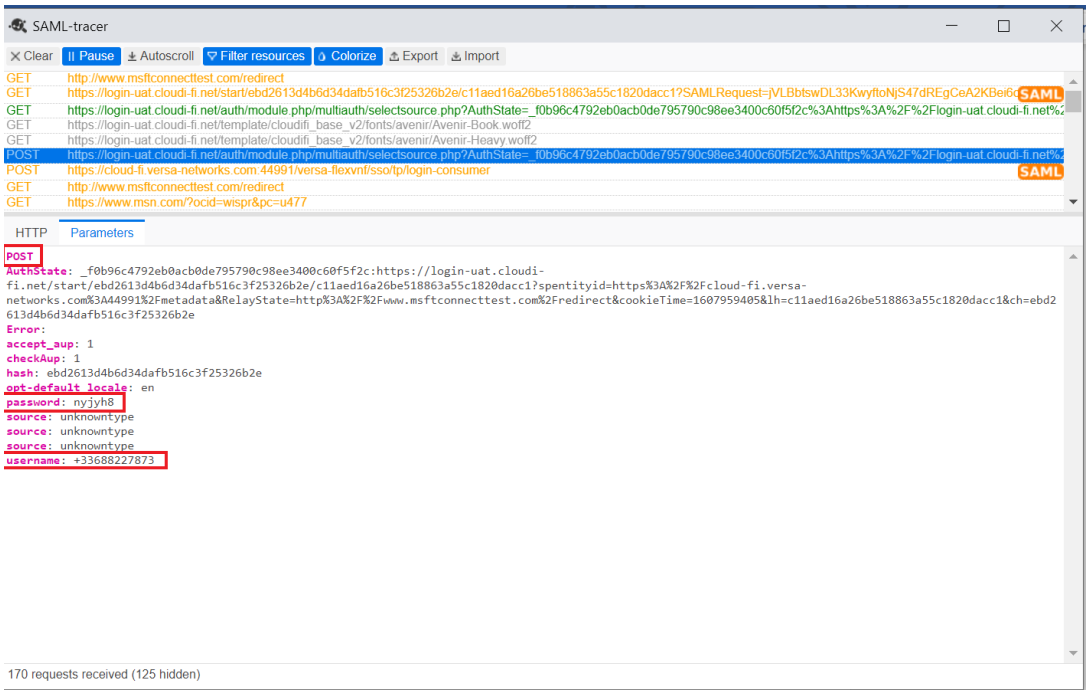
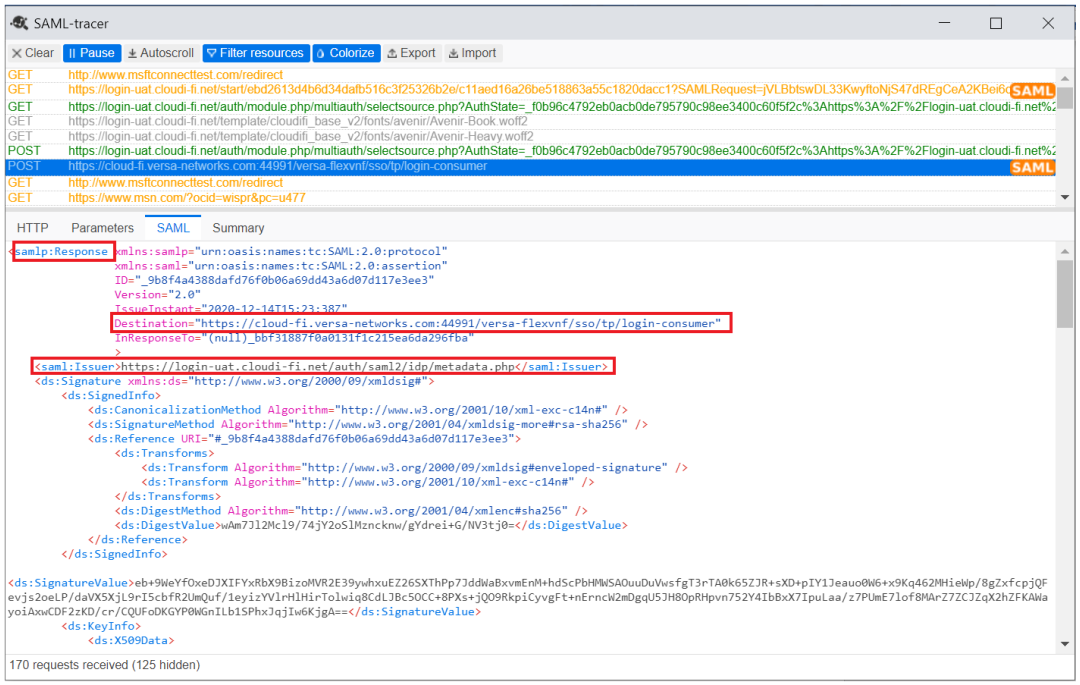
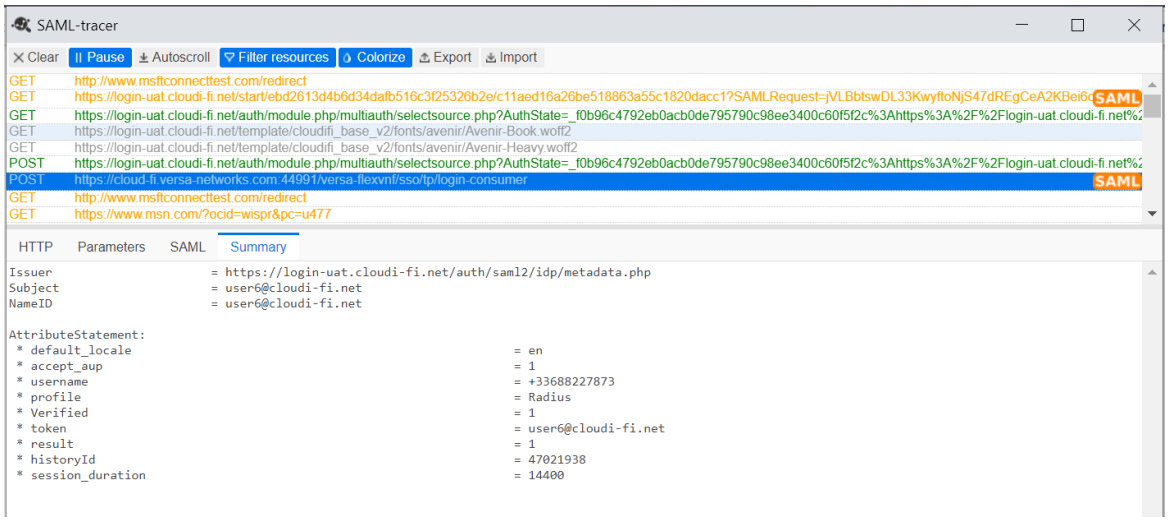


Figure 18: login credentials submitted to Cloudi-Fi

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





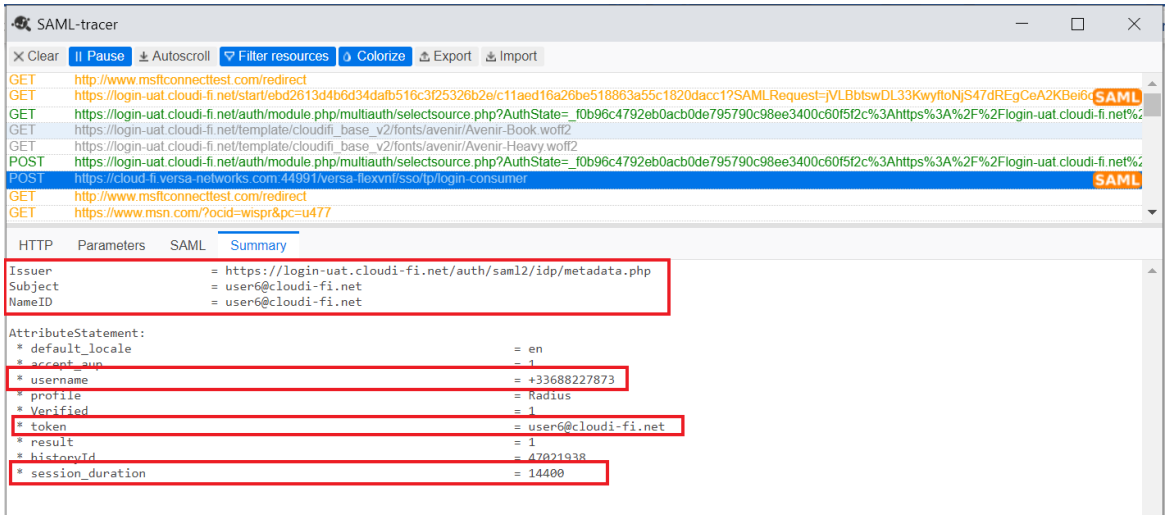


Figure 19: SAML AuthN response sent by Cloudi-Fi

5. Service verification in Versa Director

4.1 User identification under Monitor tab

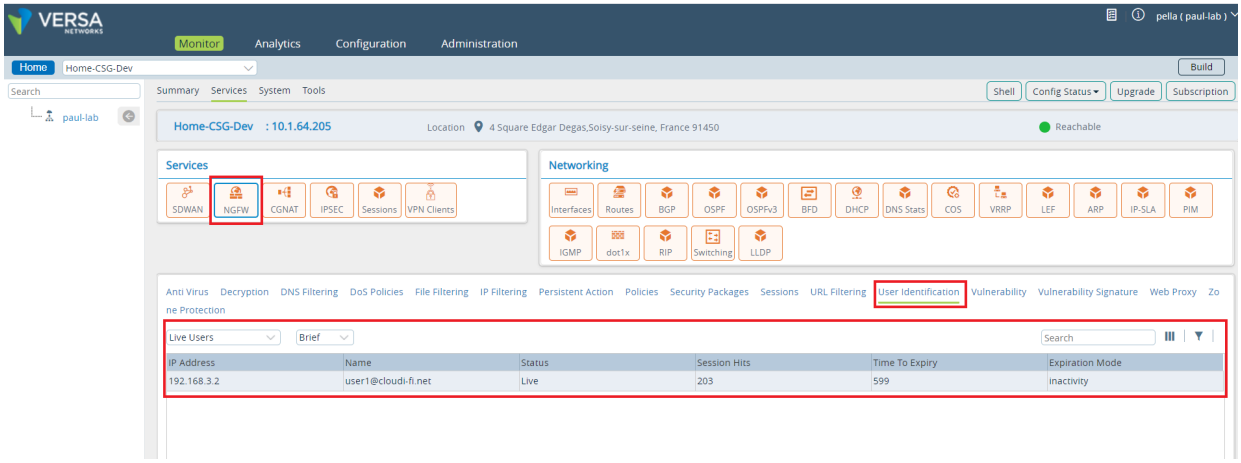


Figure 20: User identification profile in Versa CPE

4.2 Logs > Authentication in Analytics

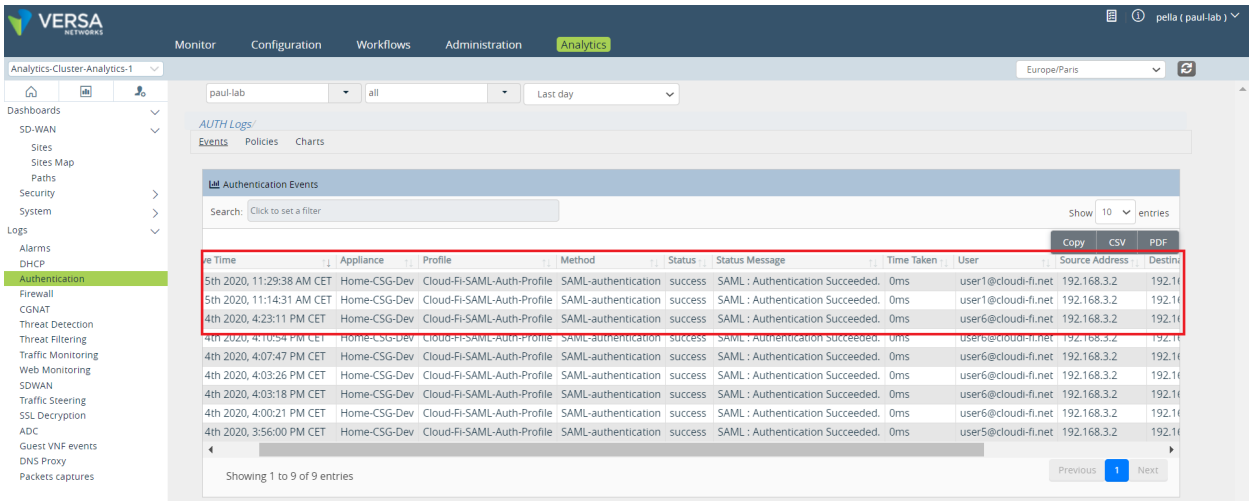


Figure 21: Successful SAML Authentication logs in versa Analytics

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.