

TRIPKIT++

Un nuovo prototipo di TripKit per il wi-fi
degli eventi INFN

M. Corosu - INFN Genova



Presentazione: The INFN TRIP Project
(M. Corosu - mobility group)



Presentazione: WiFi security appliance for
authentication solution during conferencing and
seminars (R. Veraldi)



Workshop CCR 2013:
Stato di TRIP ed il nuovo TRIP KIT
(R. Veraldi)

- Device di dimensioni contenute
- AP configurati e pronti per l'uso
- INFN-Dot1x, eduroam, INFN-Web
- Captive portal (TINO) + AAI (SAML)
- Sistema operativo standard (CentOS) + configurazione custom

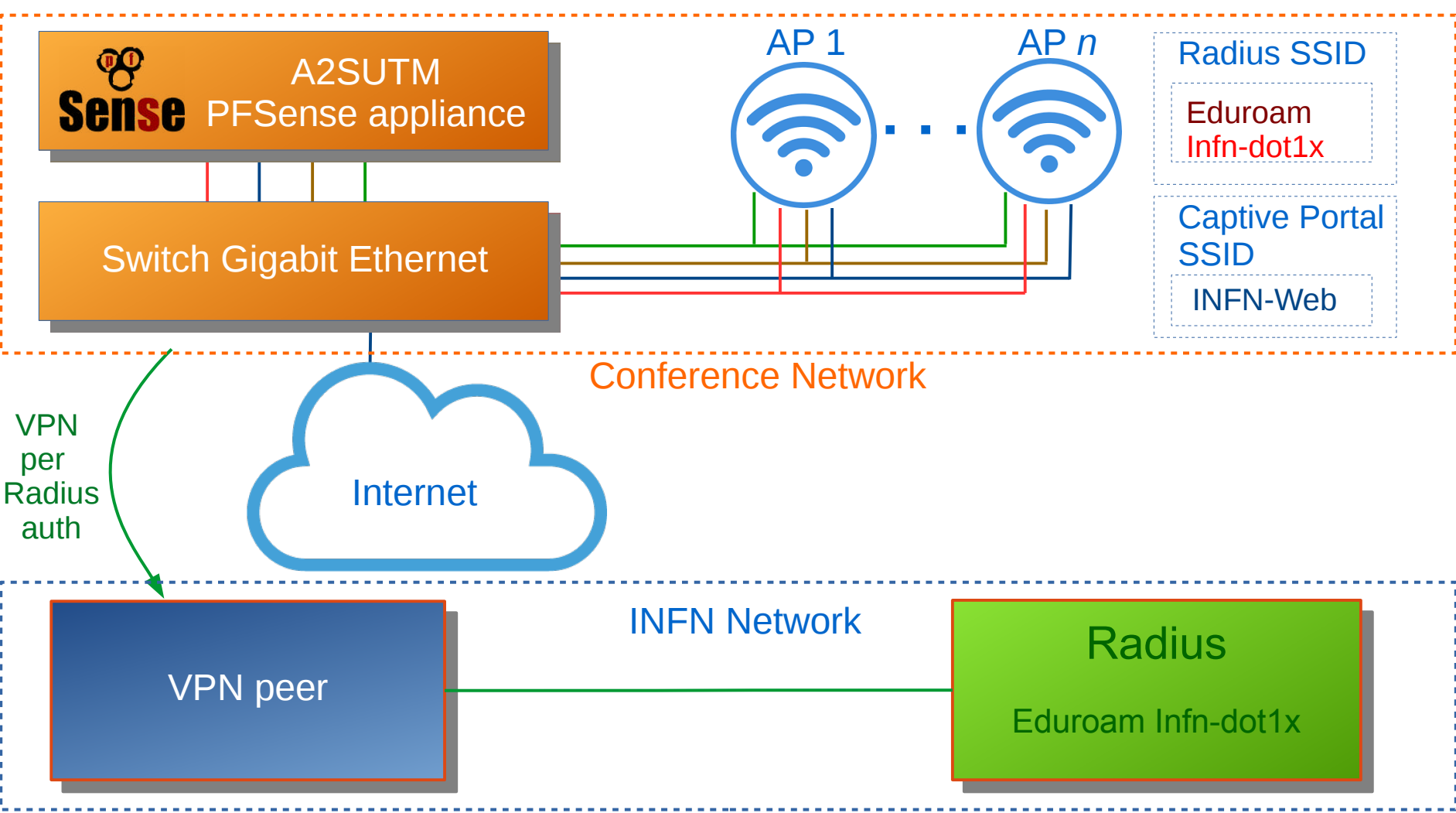
- Rinnovare l'appliance acquistando nuovo hardware dedicato:
 - Firewall con software supportato, diffuso e possibilmente opensource
 - Captive portal
 - Tool di configurazione intuitivo (possibilmente web)
 - Budget: 2KEuro



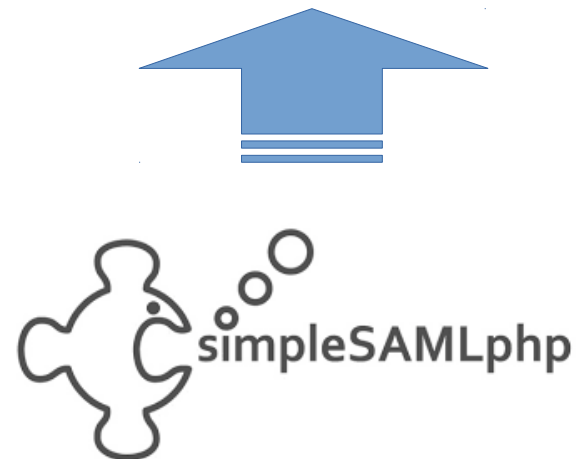
- Firewall opensource basato su FreeBSD
- OpenVPN, IPsec, L2TP
- Captive Portal (local user, radius, voucher)
- Traffic shaping
- Monitoring di traffico, performance e captive portal users
- DNS resolver, DNS forwarder, DHCP



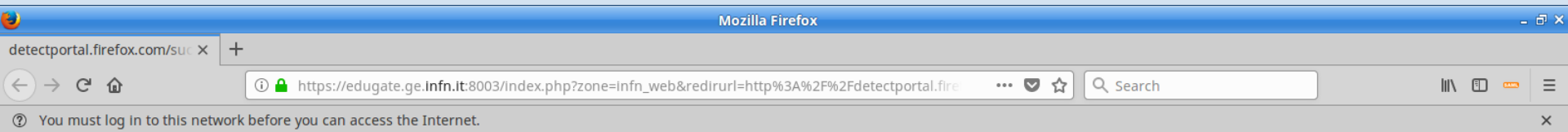
- 8 GB RAM
- 32 GB HD SSD
- 8 interfacce GE
- modulo GSM 4G/LTE
- Connettività' frontale: seriale, VGA, USB
- tre anni garanzia



- Integrazione di SAML nel captive portal
- PFSense web services: Nginx + php-fpm + Suhosin
 - Creazione di configurazione di una istanza Nginx ad-hoc
 - Disabilitata (solo per le URL SAML) la cifratura dei file di sessione PHP
- Il codice che controlla l'autorizzazione include le librerie php del captive portal per aprire il firewall e redirigere la connessione http
- <https://baltig.infn.it/corosu/tripkit-pfsense-saml/>



- Eccezioni al captive portal per tutti gli IdP (attraverso il FQDN, non l'indirizzo ip)
 - <https://technical.edugain.org/entities>
- Download dei metadati IdP in cron
- Risoluzione del nome dell'SP configurata sul DNS interno al device (punta all' ip dell' interfaccia INFN-Web del firewall)
 - Grazie della dritta a Dael Maselli.....
- Configurazione del discovery service di SimpleSAMLphp (modulo discopower)



INFN wifi login portal

INFN AAI Login

OR

Username

Password

Layout di test,
funzionante ma
da sostituire

Select your identity provider

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámegiella](#) | [Dansk](#) | [Deutsch](#) | [Svenska](#) | [Suomeksi](#) | [Español](#) | [Français](#) | [Italiano](#) | [Nederlands](#) | [Lëtzebuergesch](#) | [Čeština](#) | [Slovenščina](#) | [Lietuvių kalba](#) | [Hrvatski](#) | [Magyar](#) | [Język polski](#) | [Português](#) | [Português brasileiro](#) | [Türkçe](#) | [日本語](#) | [简体中文](#) | [繁體中文](#) | [русский язык](#) | [eesti keel](#) | [עברית](#) | [Bahasa Indonesia](#) | [Srpski](#) | [Latviešu](#) | [Românește](#) | [Euskara](#)

Incremental search...

Copyright © 2007-2017 [UNINETT AS](#)



Select your identity provider

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámegiella](#) | [Dansk](#) | [Deutsch](#) | [Svenska](#) | [Suomeksi](#) | [Español](#) | [Français](#) | [Italiano](#) | [Nederlands](#) | [Lëtzebuergesch](#) | [Čeština](#) | [Slovenščina](#) | [Lietuvių kalba](#) | [Hrvatski](#) | [Magyar](#) | [Język polski](#) | [Português](#) | [Português brasileiro](#) | [Türkçe](#) | [日本語](#) | [简体中文](#) | [繁體中文](#) | [русский язык](#) | [eesti keel](#) | [עברית](#) | [Bahasa Indonesia](#) | [Srpski](#) | [Latviešu](#) | [Românește](#) | [Euskara](#)

Garr IDEM

INFN

Incremental search...



[TEST] Perun

Cagliari State University (new)

CINECA

ENEA Italian National Agency for New Technologies, Energy and Sustainable Economic Development

EUI

Free University of Bolzano

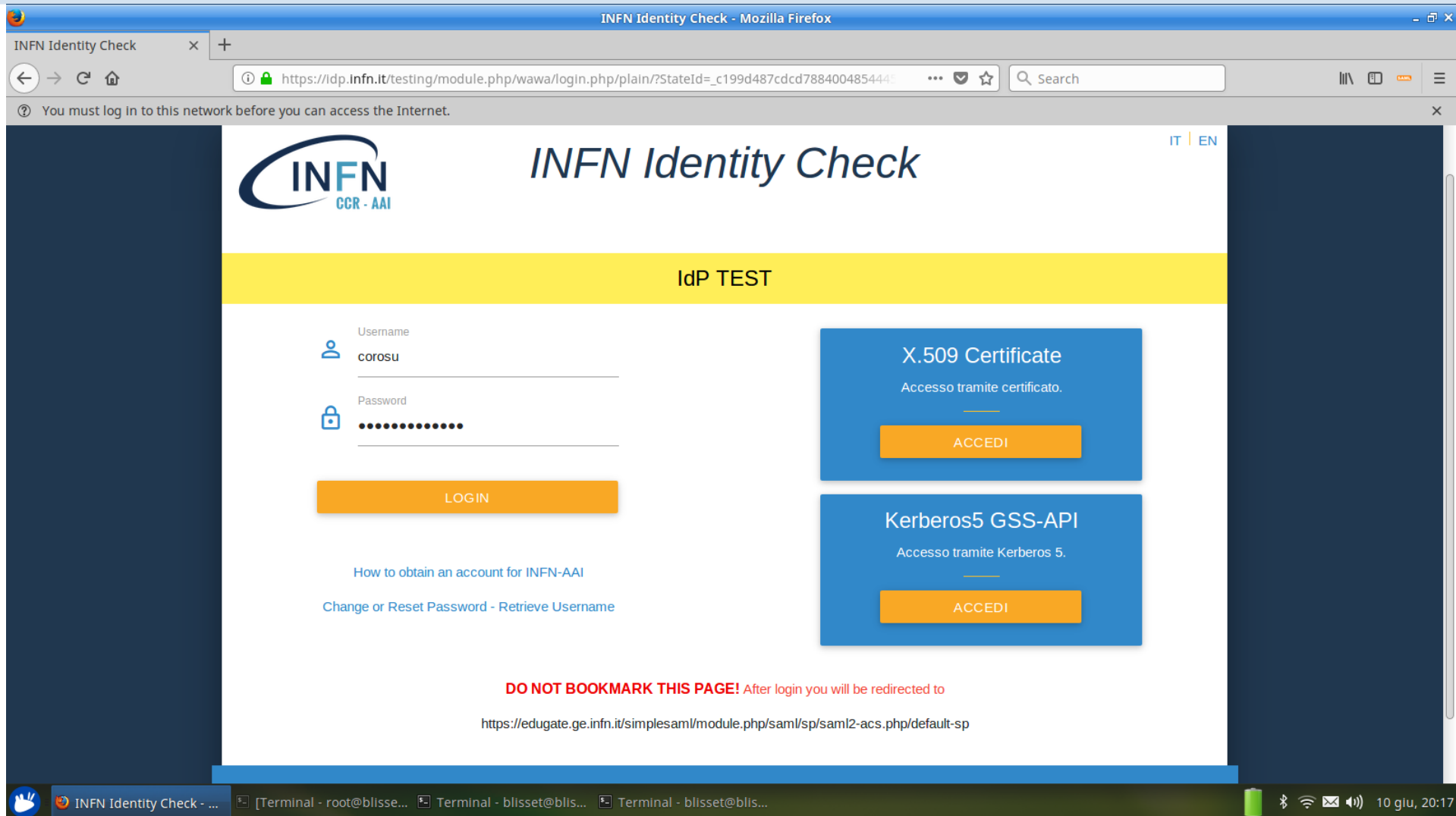
GARR CSD

GARR idp311

Gran Sasso Science Institute

Gran Sasso Science Institute

Groupier AA



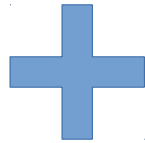
The screenshot shows a Mozilla Firefox browser window displaying the INFN Identity Check page. The browser's address bar shows the URL: `https://idp.infn.it/testing/module.php/wawa/login.php/plain/?StateId=_c199d487cdcd788400485444`. The page features the INFN logo and the text "INFN Identity Check". A yellow banner reads "IdP TEST". The login form includes fields for "Username" (containing "corosu") and "Password" (masked with dots), a "LOGIN" button, and a link for "How to obtain an account for INFN-AAI". Two alternative login methods are shown in blue boxes: "X.509 Certificate" and "Kerberos5 GSS-API", each with an "ACCEDI" button. A red warning at the bottom states: "DO NOT BOOKMARK THIS PAGE! After login you will be redirected to `https://edugate.ge.infn.it/simplesam/module.php/saml/sp/saml2-accs.php/default-sp`". The system tray at the bottom shows the time as 10 giu, 20:17.

Users Logged In (1)

IP address	MAC address	Username	Session start	Actions
10.10.30.52	88:53:2e:91:4d:35	mirko.corosu@infn.it	06/10/2018 20:26:08	

[+ Show Last Activity](#) [Disconnect All Users](#)

- Attributo *mail* ricevuto dall'IdP
- Viene richiesto insieme al CN dal service provider



- Utilizzato per la conferenza internazionale Pixel 2016 a Sestri Levante
 - Necessita' eduroam
 - Connettivita' ADSL < 1Mb/s
- Soluzione: ponte radio con il Comune di Sestri
- Il ruolo dell'appliance era svolto da un pc CentOS 7

- 2 antenne Ubiquiti NanoBridge M
- 2 AP Cisco Air SAP2602e-e-k9
- 1 Switch Extreme Summit 200-24

- Il SAML SP (captive portal) e' registrato nella federazione IDEM di test, a breve lo sara' in quella di produzione
- Richiesta di registrazione in EDUGAIN
- Il portale necessita di una veste grafica piu' curata
- Lo stesso hardware e' stato acquistato in ambito INFN nazionale: **possibilita' di esportare la configurazione**
- Il kit genovese debuttera' al corso nazionale amministrativo sul personale che si terra' a Genova il 19-20 Settembre

Grande