

AMRES VPN usluga



AMRES

Akademski mreža Srbije

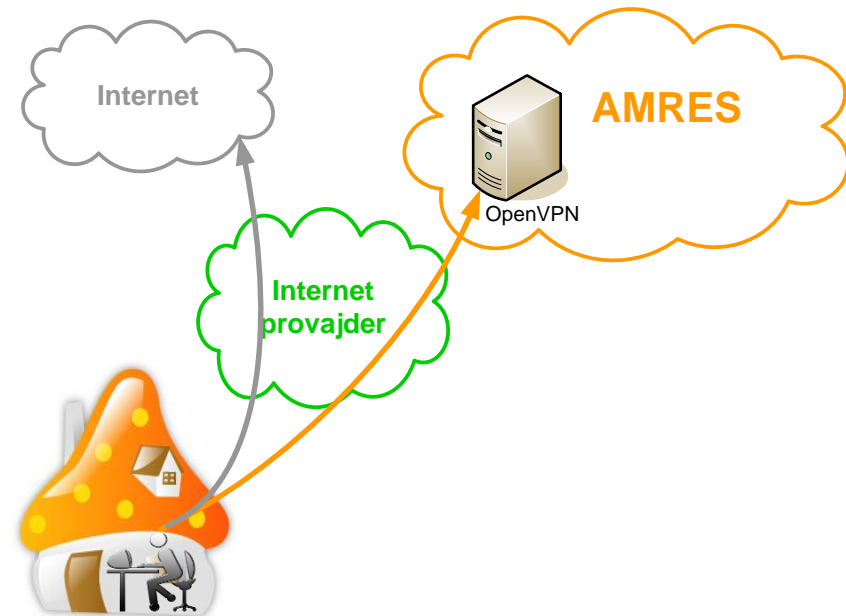
Jovana Palibrk

Sastanak administratora, Beograd, 12.12.2013.



AMRES VPN servis

- AMRES VPN servis udaljenim AMRES korisnicima obezbeđuje pristup određenim AMRES servisima pod istim uslovima koje imaju kada im pristupaju posredstvom lokalne računarske mreže svoje institucije.





Realizacija AMRES VPN servisa

- ❖ Opšti zahtevi
 - ❖ autentifikacija korisnika na osnovu kombinacije korisničkog imena i lozinke
 - ❖ autorizacija koja implementira dodelu IP adrese korisniku
 - ❖ mehanizmi praćenja aktivnosti korisnika (*accounting*)
- ❖ Zahtevi sa stanovišta sigurnosti
 - ❖ mehanizme za zaštitu poverljivosti i integriteta informacija potrebnih za autentifikaciju korisnika
 - ❖ mehanizme za zaštitu poverljivosti i integriteta korisnički podataka





Realizacija AMRES VPN servisa

- ❖ VPN server se nalazi na centralnoj lokaciji Akademske mreže
- ❖ Servis se oslanja na već postojeću RADIUS infrastrukturu koja se koristi u okviru eduroam servisa
- ❖ RADIUS infrastruktura se sastoji iz dva nivoa:
 - ❖ VPN TLR (*Top-Level RADIUS*) server koji ima ulogu *proxy* RADIUS servera. On sadrži listu domena AMRES institucija korisnica VPN servisa.
 - ❖ RADIUS serveri krajnjih institucija koji su odgovorni za autentifikaciju svojih korisnika





Realizacija AMRES VPN servisa

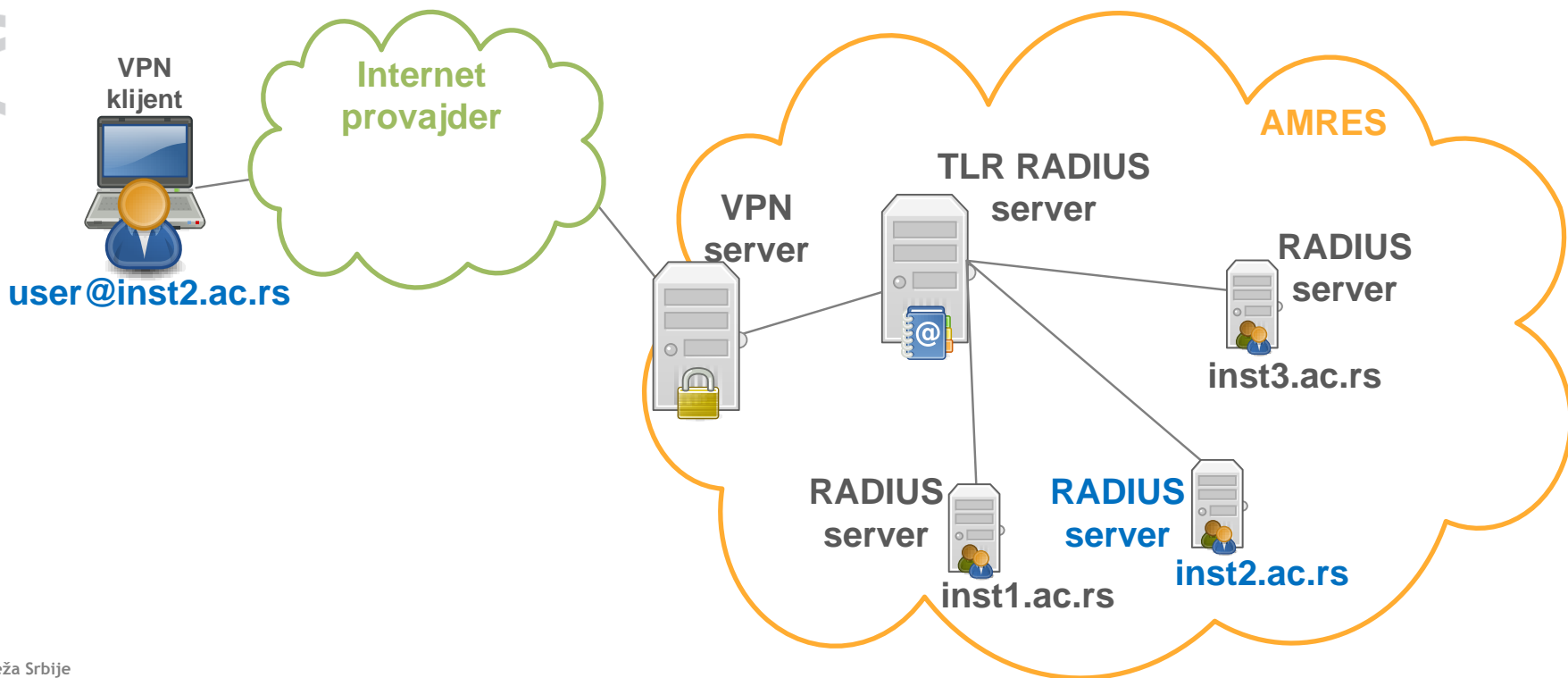
- ❧ Matične institucije su odgovorne za održavanje podataka i kredencijala svojih korisnika
- ❧ S obzirom da se radi o istoj infrastrukturi na koju se oslanja i eduroam servis, na ovaj način se postiže da korisnici mogu da koriste iste autentifikacione kredencijale za oba servisa





Realizacija AMRES VPN servisa

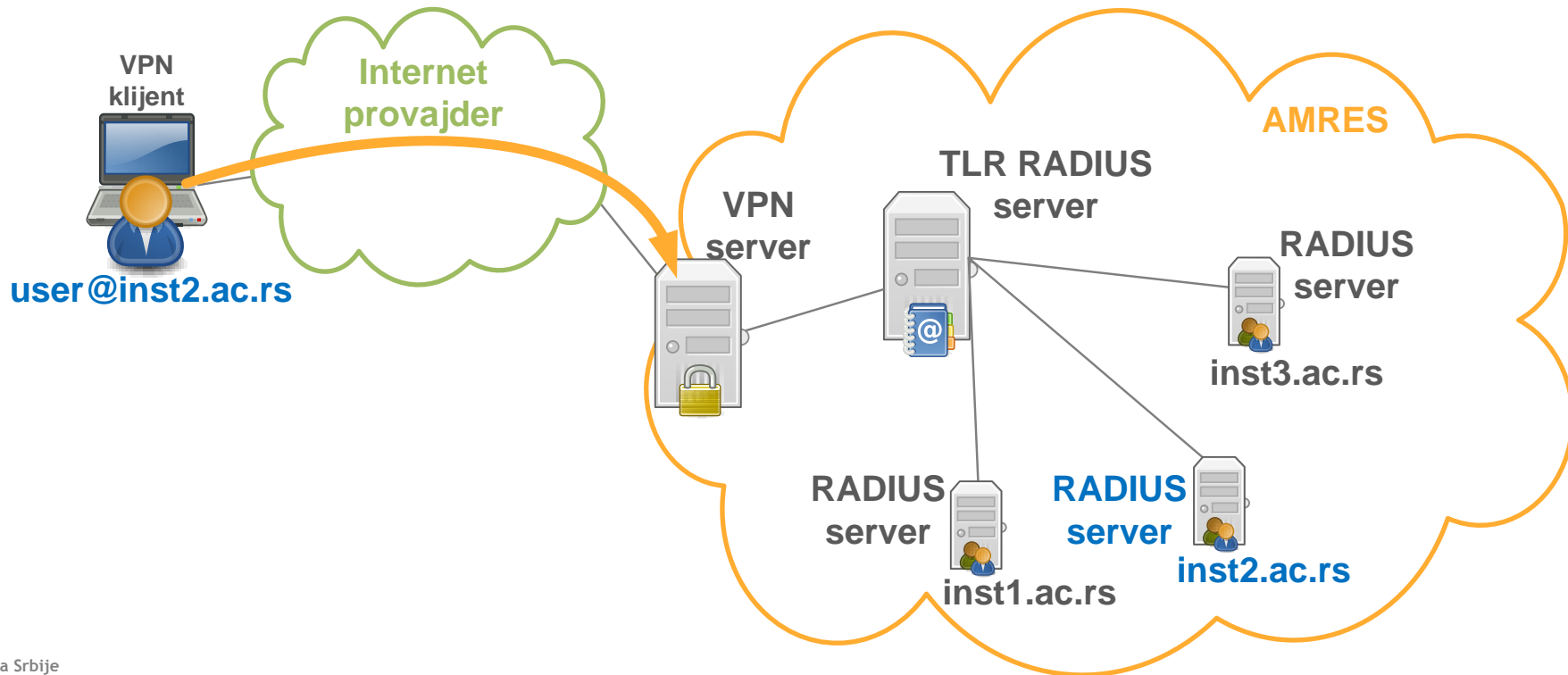
- » Autentifikacija korisnika
 - » Svaki korisnik prilikom prijavljivanja na VPN servis mora da upotrebi svoje korisničko ime u formi *korisničko-ime@domen-institucije*





Realizacija AMRES VPN servisa

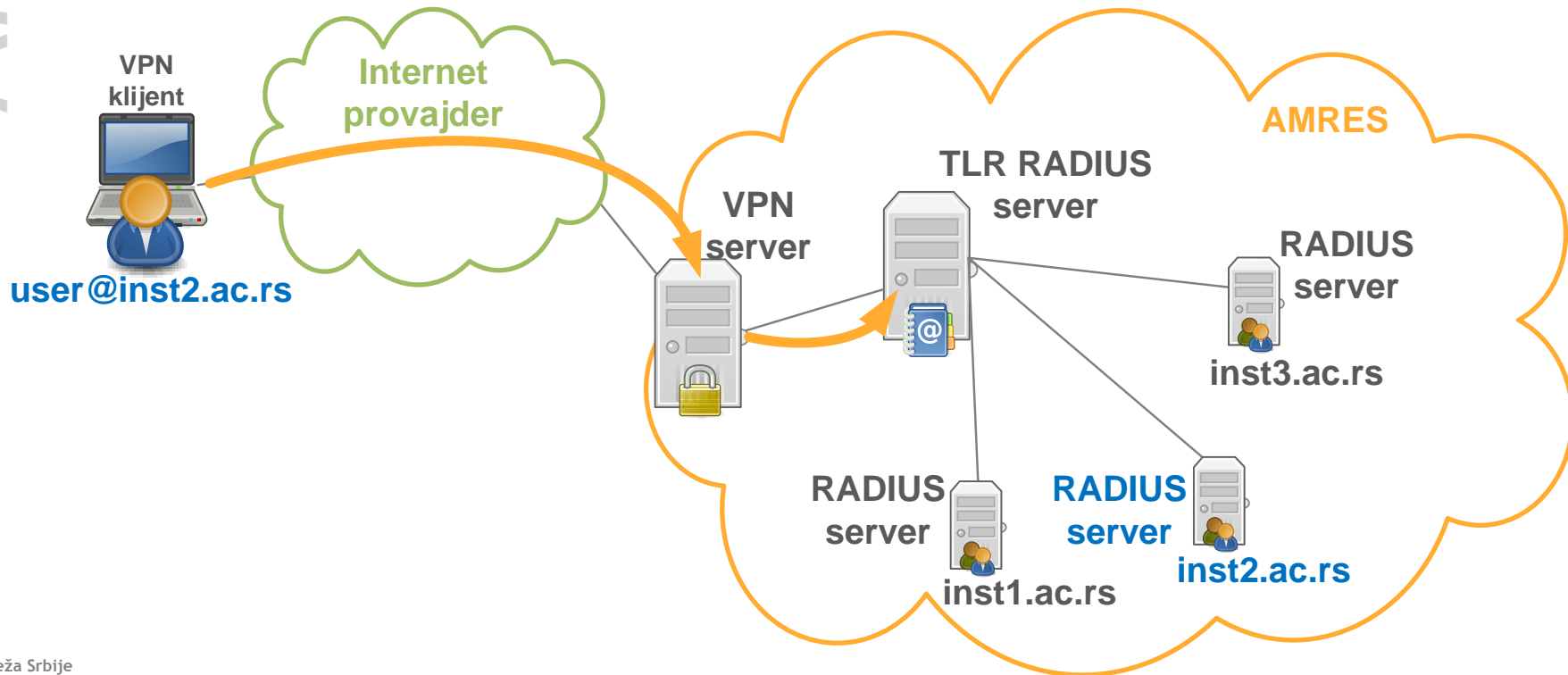
- » Autentifikacija korisnika
 - » Korisnički kredencijali se šalju preko mreže Internet servis provajdera do VPN servera kriptovani





Realizacija AMRES VPN servisa

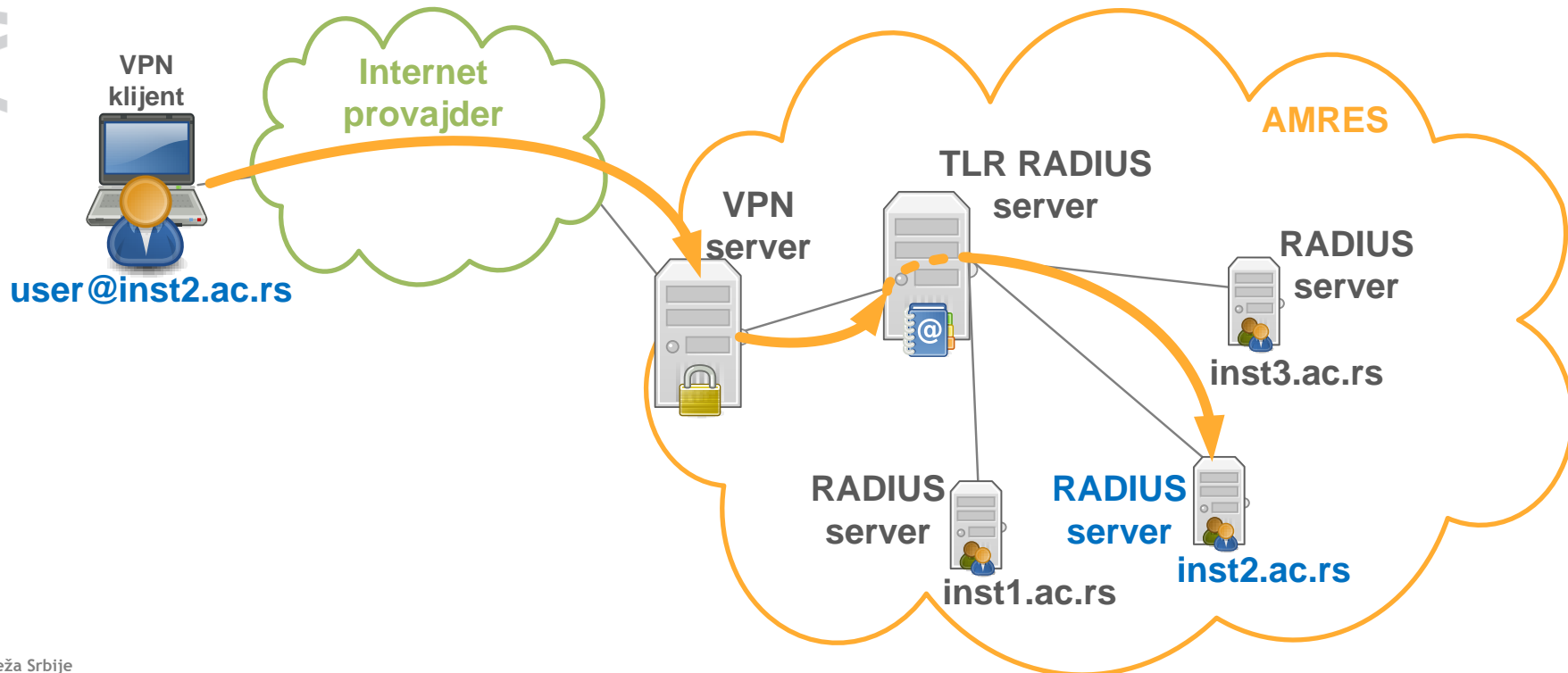
- » Autentifikacija korisnika
 - » VPN server šalje zahtev za autentifikaciju korisnika TLR serveru





Realizacija AMRES VPN servisa

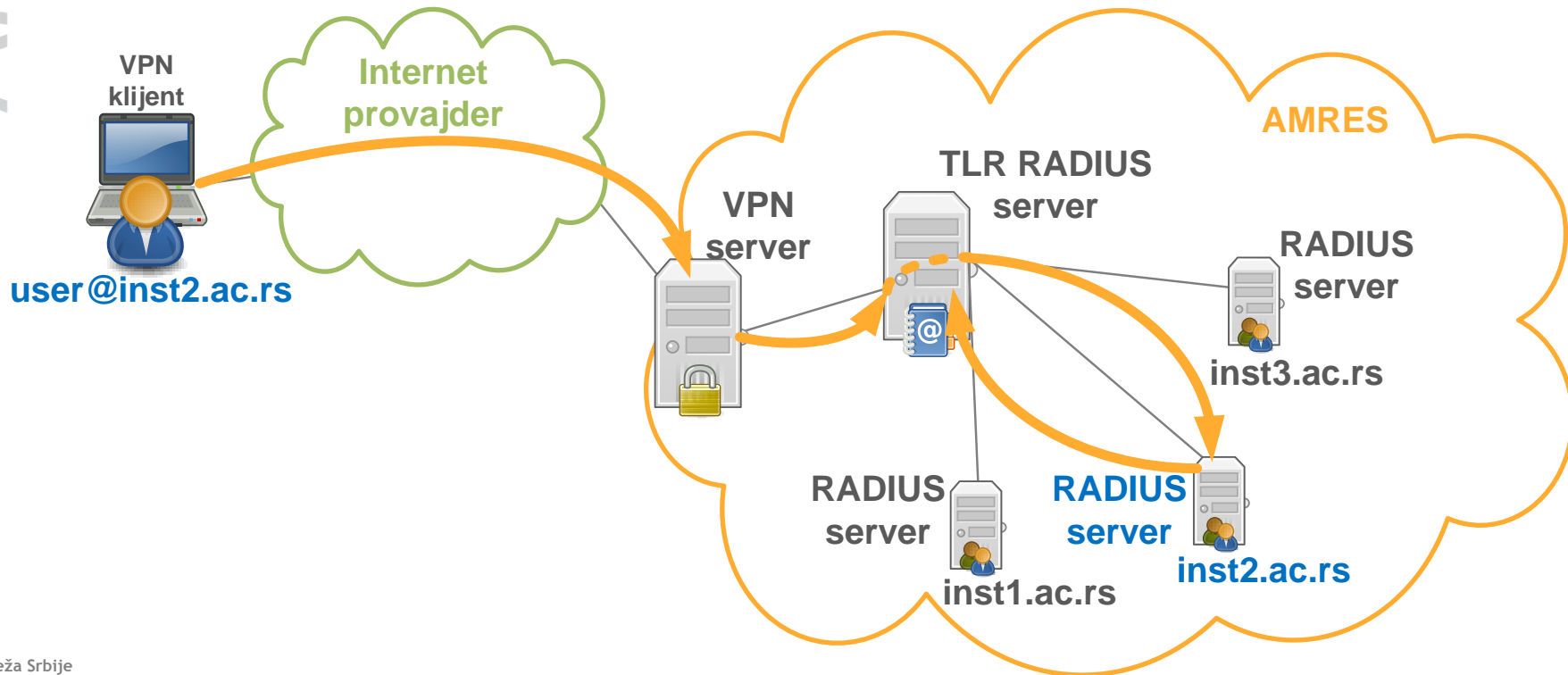
- » Autentifikacija korisnika
 - » TLR server koristi informaciju o domenu institucije kako bi zahtev prosledio RADIUS serveru institucije kojoj korisnik pripada





Realizacija AMRES VPN servisa

- » Autentifikacija korisnika
 - » RADIUS server institucije, zatim, obrađuje pristigli zahtev i šalje odgovor TLR serveru





Realizacija AMRES VPN servisa

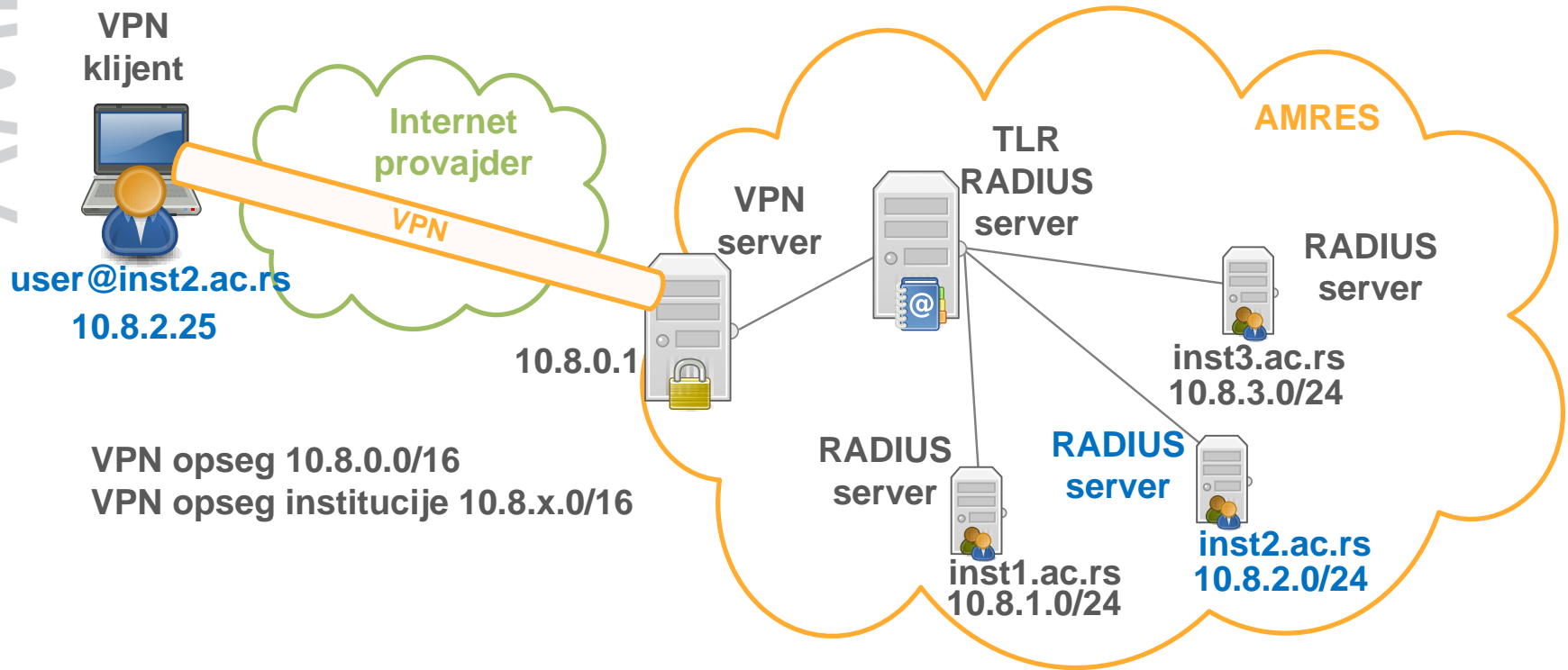
- ❖ Nakon autentifikacije korisnika TLR server korisničkom uređaju dodeljuje IP adresu iz VPN opsega njegove institucije
- ❖ Za AMRES VPN opseg odabran je 10.8.0.0/16, dok svaka institucija učesnica AMRES VPN servisa dobija jednu C klasu IP adresa iz opsega 10.8.0.0/16
- ❖ Dodeljeni opseg može dalje da se podeli na podopsege u okviru jedne institucije, na primer za **studente** i **zaposlene**, na osnovu čega institucija može da vrši filtriranje saobraćaja u skladu sa svojom politikom pristupa





Realizacija AMRES VPN servisa

- » Raspodela IP adresa u okviru AMRES VPN servisa





Realizacija AMRES VPN servisa

- ❧ VPN tunel se formira između između klijentskog uređaja i VPN servera
- ❧ Kriptografska zaštita saobraćaja je obezbeđena samo unutar VPN tunela
- ❧ Kada VPN server primi saobraćaj od korisnika, saobraćaj se dekriptuje i prosleđuje u originalnoj formi do destinacije kroz akademsku mrežu





Realizacija AMRES VPN servisa

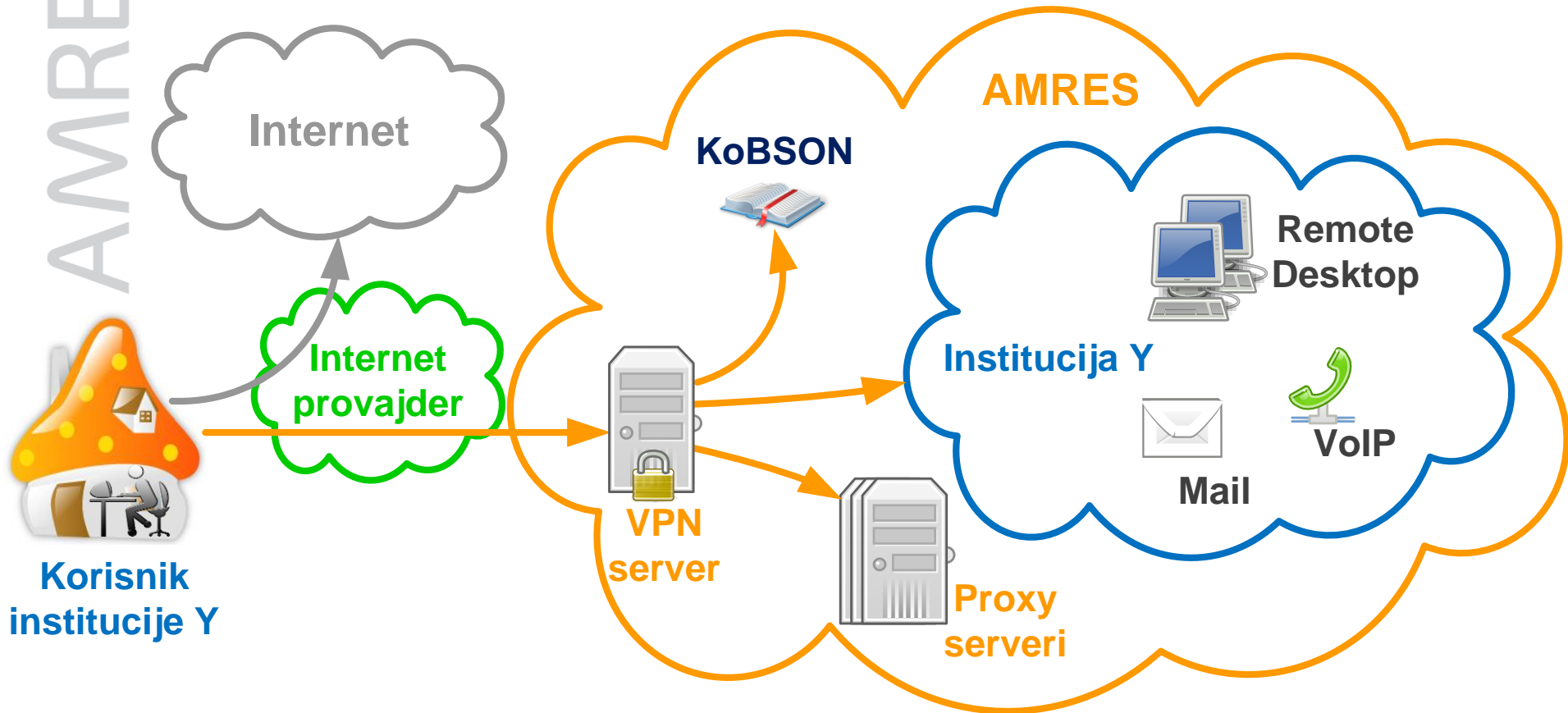
- ❖ AMRES VPN servis podržava *split tunneling*
 - ❖ Saobraćaj ka svim AMRES adresnim opsezima od uređaja VPN korisnika se šalje kroz VPN tunel
 - ❖ Sav ostali saobraćaj korisnički uređaj šalje kroz lokalnu mrežnu konekciju
 - ❖ Na ovaj način se postiže veća efikasnost i očuvanje propusnog opsega, jer je značajno smanjena količina saobraćaja koja se šalje kroz VPN tunel.





Dostupni servisi

AMRES

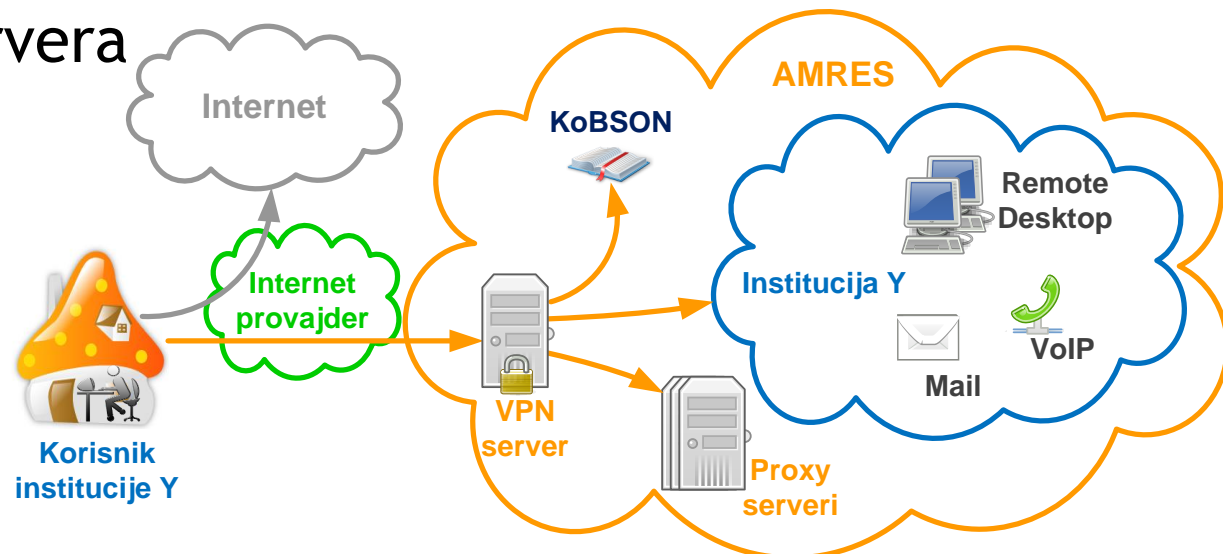




Dostupni servisi

❧ KOBSON

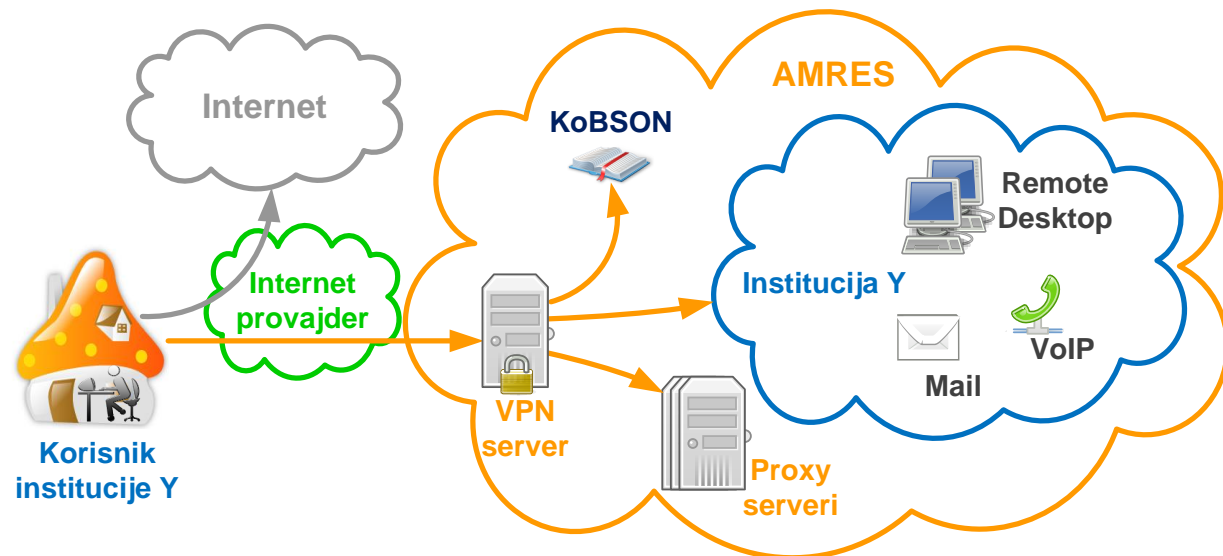
- ❧ Pravo na njegovo korišćenje ostvaruje se samo sa akademske mreže korišćenjem jednog od registrovanih *proxy* servera u KOBSON sistemu
- ❧ Zahvaljujući AMRES VPN servisu korisnici AMRES mreže mogu KOBSON koristiti i kada se nalaze van akademske mreže preko istih registrovanih *proxy* servera





Dostupni servisi

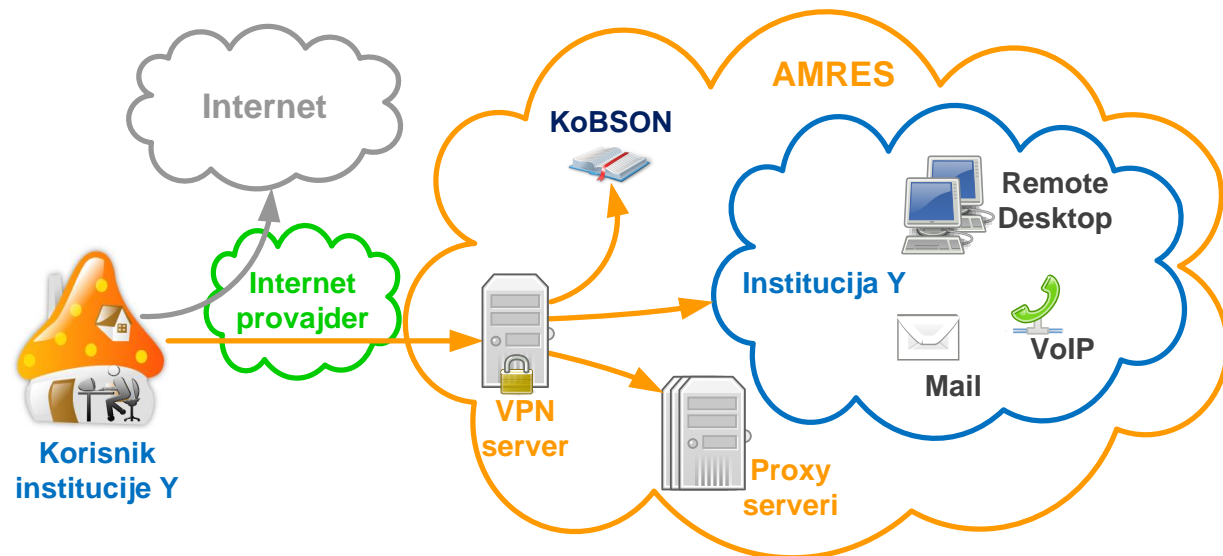
- Proxy servis
- Servis za izdavanje sertifikata
- eLearning server
- E-mail
- Remote desktop na korisnički računar





Dostupni servisi

- Pristup specijalizovanim informacionim sistemima i servisima (npr. univerzitetski IS, fakultetski servisi itd.)
- Dodatni servisi čija realizacija zavisi od logičke arhitekture računarske mreže AMRES institucije





Prijava na servis

- ❧ U AMRES VPN servisu može da učestvuje svaka institucija koja je članica AMRES-a i koja učestvuje u AMRES eduroam servisu kao davalac identiteta
- ❧ Prijava se vrši slanjem zahteva za pristup servisu na helpdesk@amres.ac.rs
- ❧ Podešavanje RADIUS servera
- ❧ Institucija dobija svoj VPN adresni opseg
- ❧ Korisnici se moraju pridržavati pravila definisanih u Pravilniku o korišćenju Akademske mreže Srbije - AUP





Korisnički servisi	Korisnici	Projekti	Novosti / ostalo
eduroam			
VPN >>		Za krajnje korisnike	
Helpdesk >>		Za AMRES članice	
DNS >>		Spisak povezanih institucija	
Proxy >>			
e-mail >>			
Dial-up >>			
Web Hosting			
Monitoring			
KoBSON			
eLearning			
Media >>			
Federacija Identiteta >>			





The screenshot shows the website for 'Campus Best Practice' at the Računarski Centar Univerziteta u Beogradu. The page features a dark header with the title 'Campus Best Practice' and a navigation menu with items 'CBP', 'CBP DOKUMENTA', and 'RADNE GR'. A dropdown menu is open under 'CBP DOKUMENTA', listing 'Monitoring mrežne infrastrukture i servisa', 'Sigurnost', 'Wireless', 'Voice & Video', and 'Fizička Infrastruktura'. The main content area has a section titled 'CBP' with two paragraphs of text.

Campus Best Practice

RAČUNARSKI CENTAR UNIVERZITETA U BEOGRADU

CBP

Cilj GÉANT projekta jeste da omogući naprednu saradnju naučno-istraživačkih zajednica i unapređenje svih aspekata evropskog naučno-istraživačkog i obrazovnog umrežavanja. (pojedinačnih korisnika sa 8000 institucija iz 40 zemalja.

CBP task, koji se u okviru GÉANT projekta zove NA3/T2 (Network Activity 3 Task 2) predstavlja deo GÉANT projekta koji za cilj ima da krajnjim administratorima u okviru kampus okruženja pruži rešenje za najčešće probleme sa kojima se susreću.

- Monitoring mrežne infrastrukture i servisa
- Sigurnost**
- Wireless
- Voice & Video
- Fizička Infrastruktura





Campus Best Practice

RAČUNARSKI CENTAR UNIVERZITETA U BEOGRADU

CBP CBP DOKUMENTA RADNE GRUPE AKTIVNOSTI OBAVEŠTENJA

Sigurnost

Paralelno sa razvojem savremenih tehnologija i sve većim korišćenjem interneta, razvijan je niz malicioznih softvera i alata koji su imali za cilj da iskoriste ranjivosti koje postoje na mrežnim uređajima, operativnim sistemima i servisima. Cilj dokumenata koji su razvijeni u okviru radne grupe za sigurnost je da pruže administratorima uvid u tehnologije i metodologije koje mogu koristiti prilikom zaštite svoje mrežne infrastrukture.

Novosti

Dokumenta:

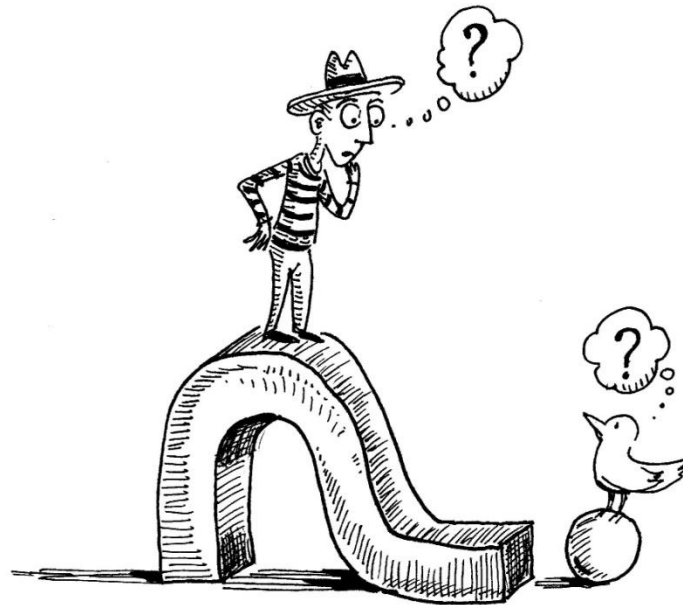
- Centralizovani sistem za filtriranje web saobraćaja
- Filtriranje saobraćaja – uvid u tehnologije i mesta njihove primene u AMRESu
- Upotrebom digitalnih sertifikata do sigurnog pristupa servisima
- Implementacija AMRES VPN servisa





Pitanja

AMRES





Hvala na pažnji

