AMRES Servis Web filtriranja

AMRES

Akademska mreža Srbije

Miloš Kukoleča

Sastanak administratora, Beograd, 12.12.2013.

AMRES Web Proxy Servis

- Proksiranje saobraćaja već postoji
- AMRES Web Proxy servis se sastoji od
  - 5 Ironport S670 uređaja
  - 1 Ironport M160 uređaja
- Ironport S670 (WSA) imaju ulogu proxy uređaja
- Ironport M160 (SMA) je uređaj za centralizovano upravljanje

Ciljevi Web Proxy servisa

- Prvobitni cilj je bio zaštita kapaciteta linkova ka Internetu za akademske potrebe
- Zaštita krajnjih korisnika od malicioznog sadržaja
- AMRES je napravio Globalnu polisu prihvatljivog sadržaja

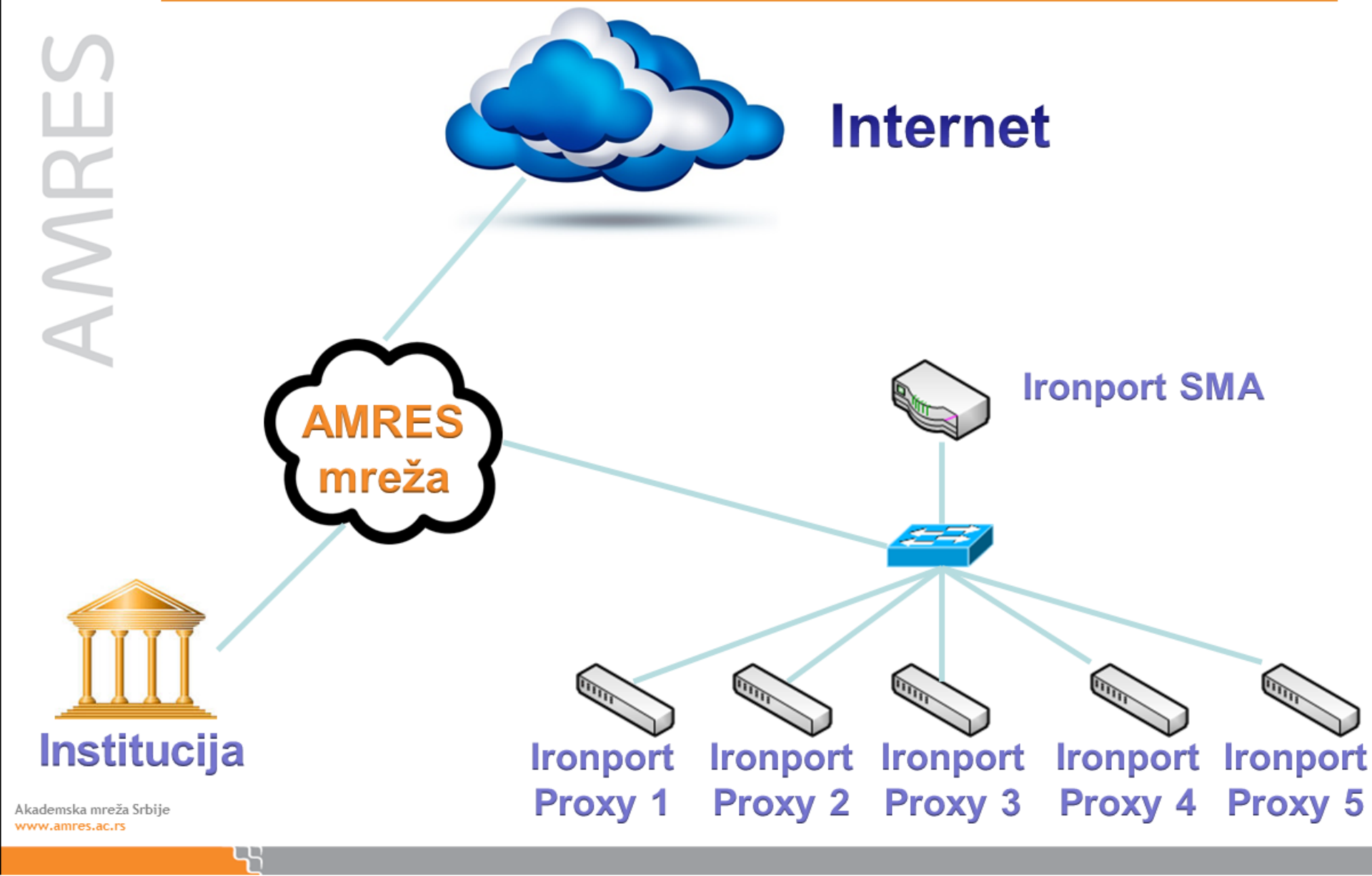
Organizacija Web Proxy Servisa

- AMRES globalna polisa obuhvata sve korisnike akademske mreže
- Institucije su zahtevale dodatne zabrane (Facebook, Youtube i sl.)
  - AMRES osoblje je kreiralo i održavalo posebne polise za pojedine institucije
- Vremenom je broj institucija sa specijalnim zahtevima postajao sve veći
  - Rešenje: AMRES Servis Web Filtriranja

AMRES Servis Web Filtriranja

- Namenjen je administratorima institucija
- Servis predstavlja Cloud rešenje
  - Hardverski i softverski resursi su centralizovani i izmešteni od korisnika
- Administratori institucija podešavaju konfiguraciju na Ironport proxy uređajima
- Administrator menja samo onaj deo konfiguracije koji se tiče njegove institucije

AMRES Servis Web Filtriranja - šema



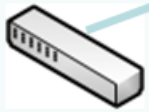
AMRES Servis Web Filtriranja - šema

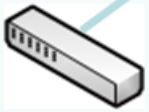
Internet

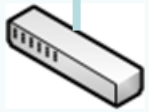
AMRES mreža

AMRES Servis Web filtriranja

Ironport SMA



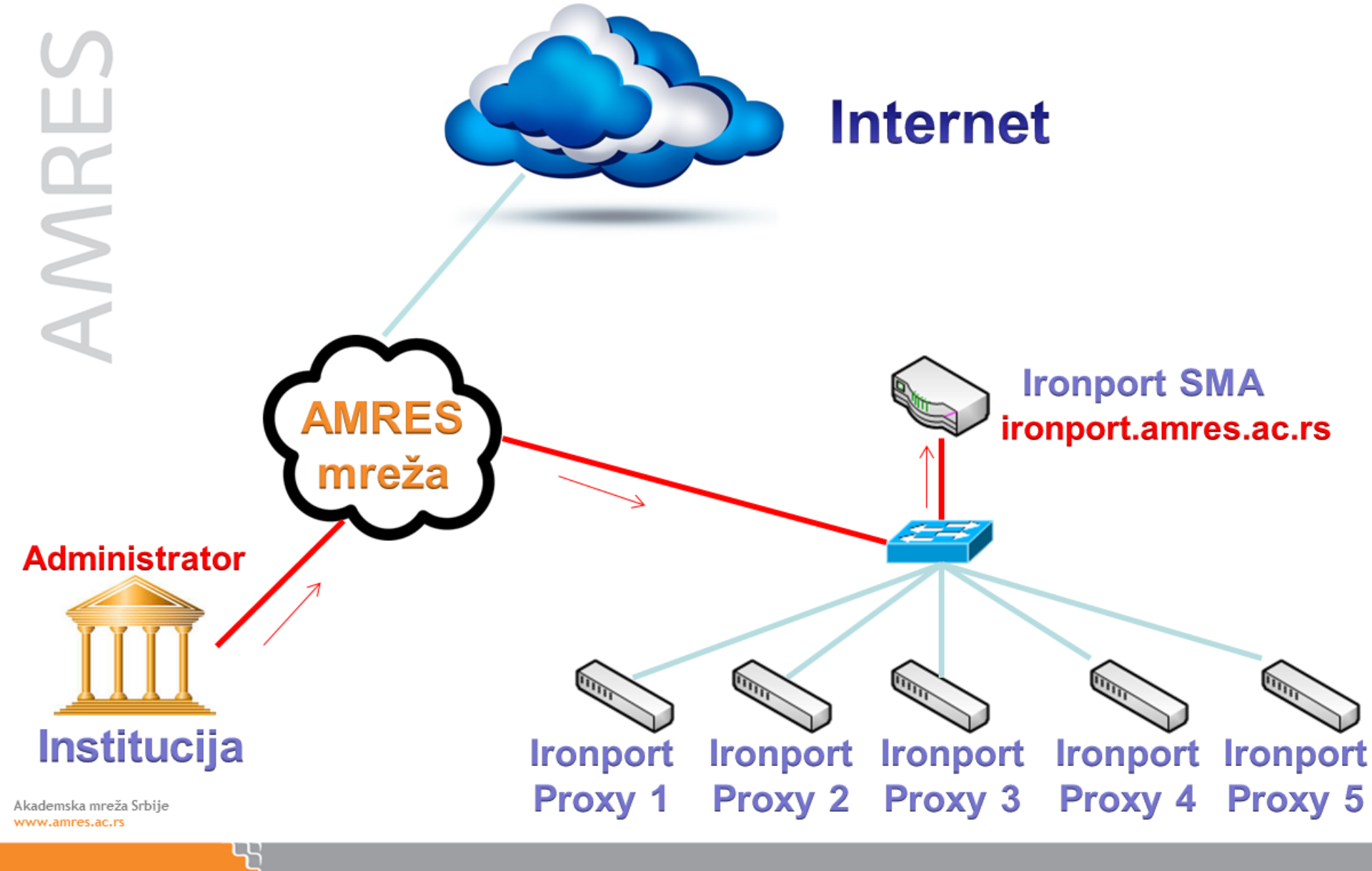




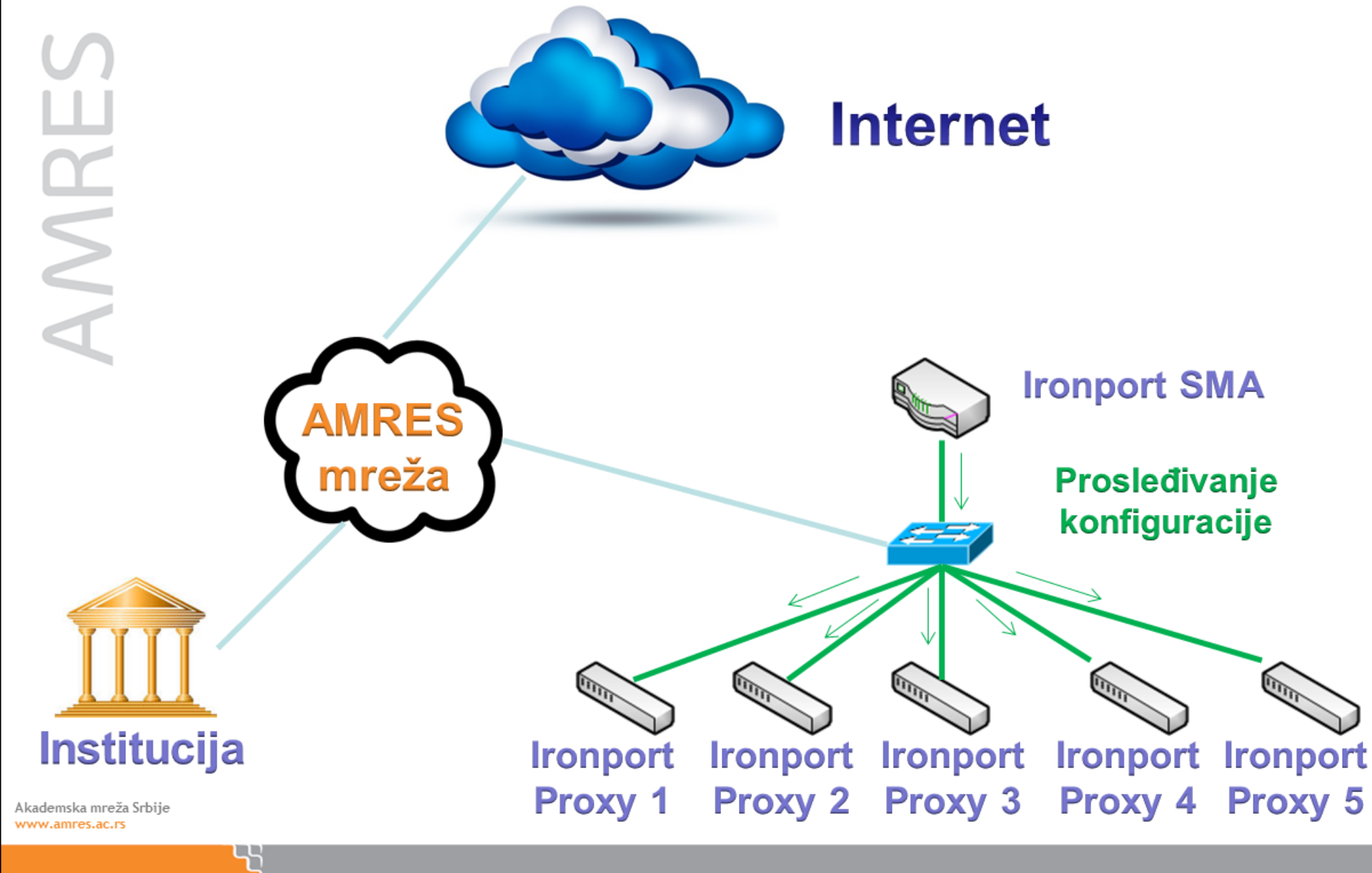
Ironport Proxy 1 | Ironport Proxy 2 | Ironport Proxy 3 | Ironport Proxy 4 | Ironport Proxy 5

Institucija

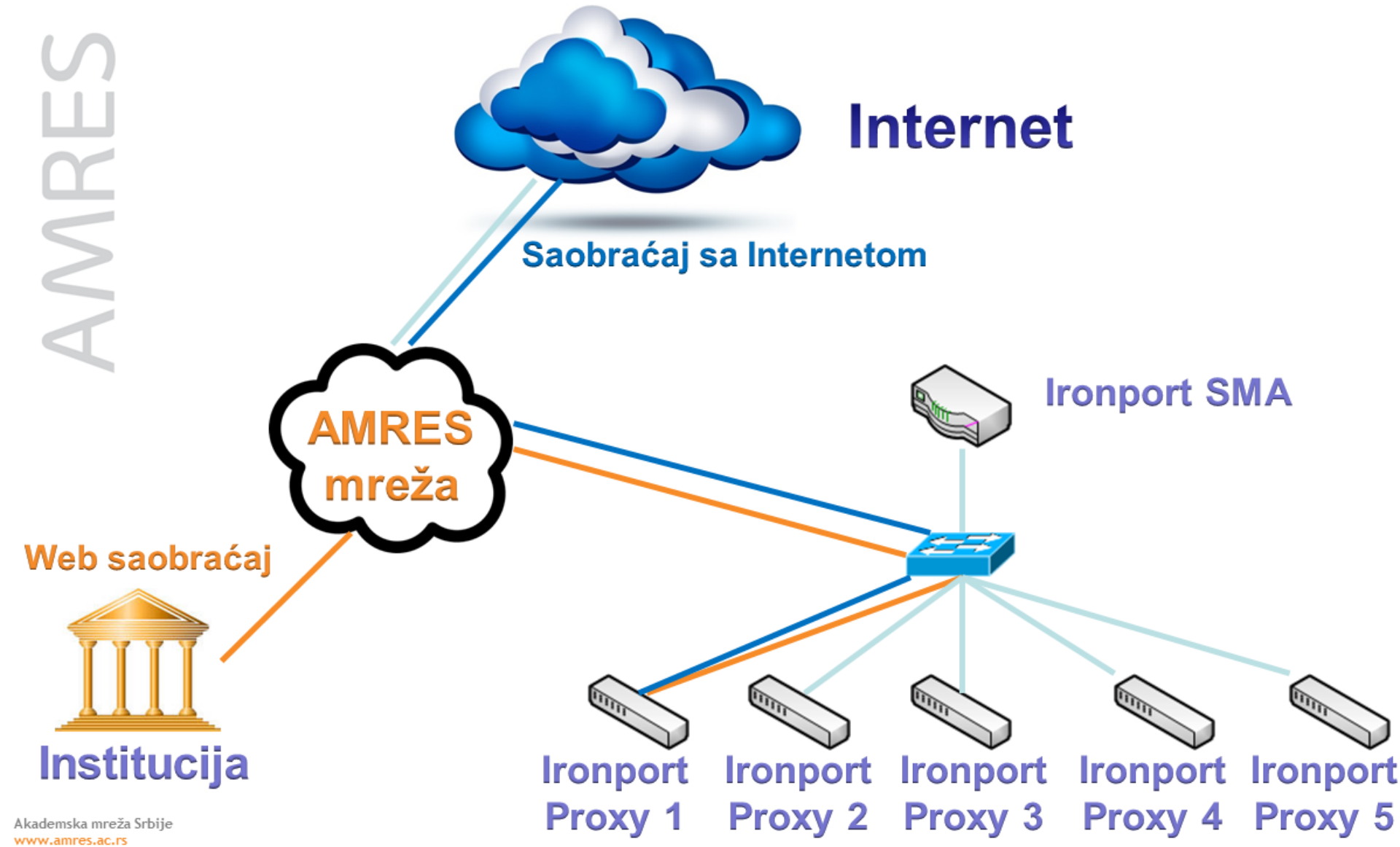
AMRES Servis Web Filtriranja - šema



AMRES Servis Web Filtriranja - šema



AMRES Servis Web Filtriranja - šema



Autentifikacija - LDAP (1)

- Autentifikacija na servis = autentifikacija na Ironport SMA uređaj
- Autentifikacija se oslanja na AMRES Admin LDAP bazu
  - Upravljanje nalozima u bazi će se vršiti preko AMRES LDAP aplikacije
- Nakon uspešne autentifikacije administrator preuzima nalog institucije na uređaju i može da menja web filtre samo za saobraćaj koji se tiče njegove institucije

AMRES Servis Web filtriranja

- Svaka institucija ima svoj nalog na Ironport SMA uređaju
- U okviru naloga svaka institucija ima pravo na:
  - 1 Access polisu – konfiguriše Web filtre za saobraćaj institucije
  - 1 Custom URL kategoriju – definiše listu eksplicitno blokiranih URL-ova
- NAPOMENA: Access polisa institucije može biti isključivo striktnija od Globalne Access polise

Access Polisa institucije

Access Policies

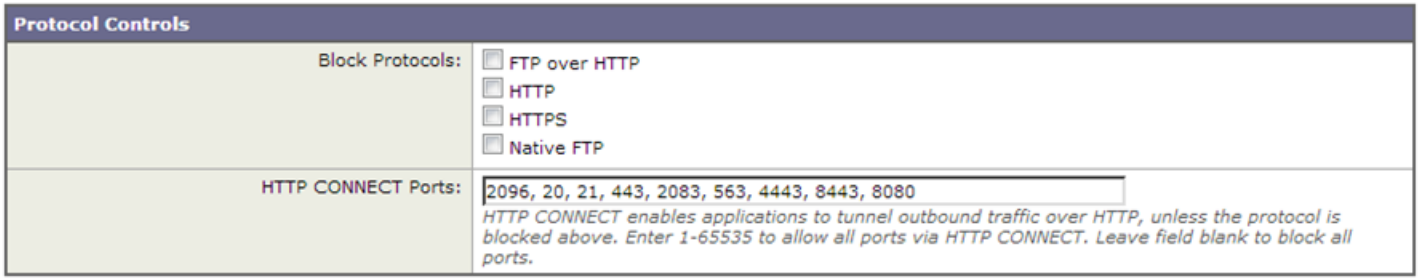
Policies

View: All Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering
7	**Polisa Institucije** Identity: Ime Institucije view	(global policy)	Block: 7 Monitor: 73 Allow: 2	(global policy)	(global policy)	(global policy)

- U okviru Access polise mogu se vršiti sledeća podešavanja:
  - Dozvoljeni protokoli i Internet pregledači
  - Dozvoljene URL kategorije
  - Dozvoljene Web Aplikacije
  - Dozvoljeni Objekti za prenos
  - Definisanje prihvatljive Web reputacije

Access Polisa - Protokoli i portovi



- U ovoj sekciji Access polise moguće je podesiti:
  - Blokadu protokola HTTP, HTTPS, FTP i FTP preko HTTP-a
  - Dopuštanje portova za HTTP Connect metodu (HTTPS)
  - Blokadu određenih Internet pregledača

Access Polisa - URL kategorije

- U ovoj sekciji Access polise podešavaju se prihvatljive URL kategorije
  - Cisco klasifikuje web sajtove u predefinisane URL kategorije
  - Postoji oko 78 predefinisanih URL kategorija
  - Inicijalno AMRES zabranjuje 6 kategorija (Child Abuse, Filter Avoidance, Gambling, Hate Speech, Illegal Drugs, Pornography)
  - Za svaku kategoriju mogu se postaviti akcije Allow, Block i Warn

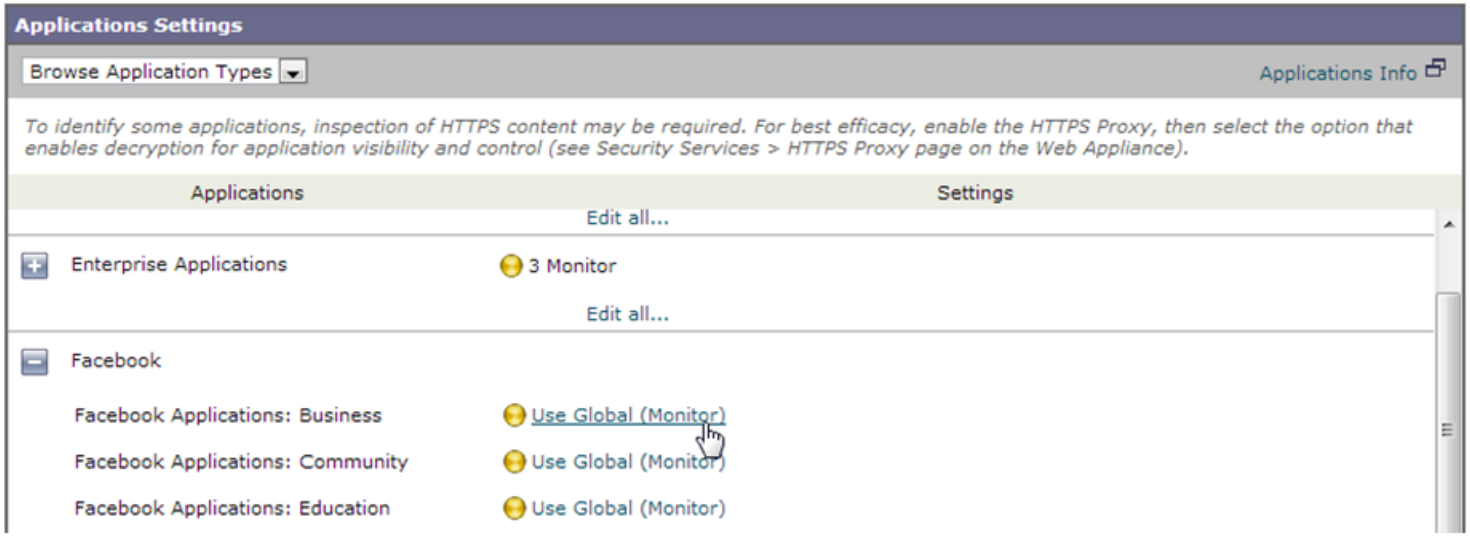
Access Polisa - URL kategorije

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

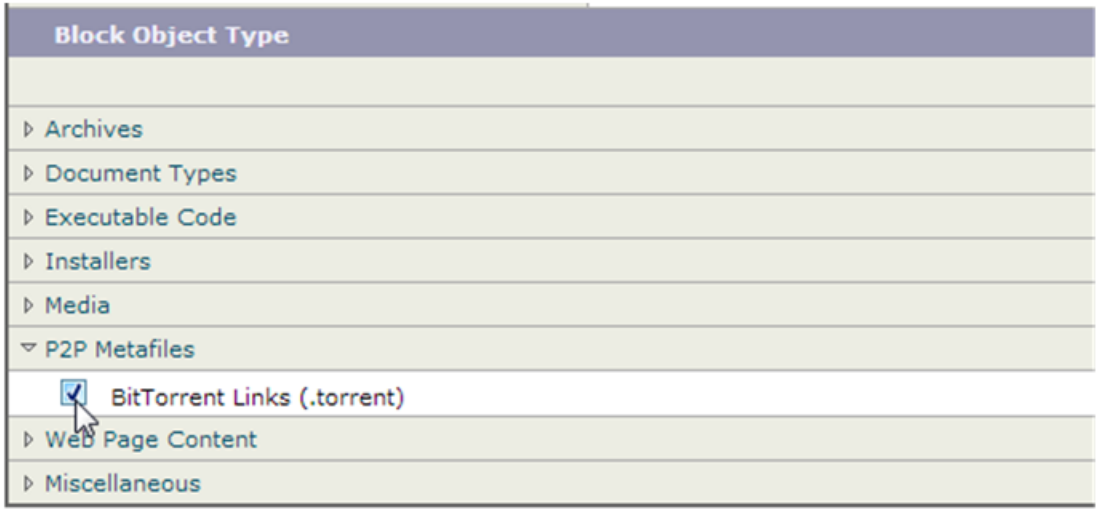
Category	Use Global Settings	Override Global Settings		
		Block	Monitor	Warn
	Select all	Select all	Select all	Select all
Photo Search and Images	✓			
Politics	✓			
Pornography	✓			
Professional Networking	✓			
Real Estate	✓			
Reference	✓			
Religion	✓			
SaaS and B2B	✓			
Safe for Kids	✓			
Science and Technology	✓			
Search Engines and Portals	✓			
Sex Education	✓			
Shopping	✓			
Social Networking		✓		
Social Science	✓			
Society and Culture	✓			
Software Updates	✓			
Sports and Recreation	✓			
Streaming Audio	✓			
Streaming Video	✓			

Access Polisa - Aplikacije



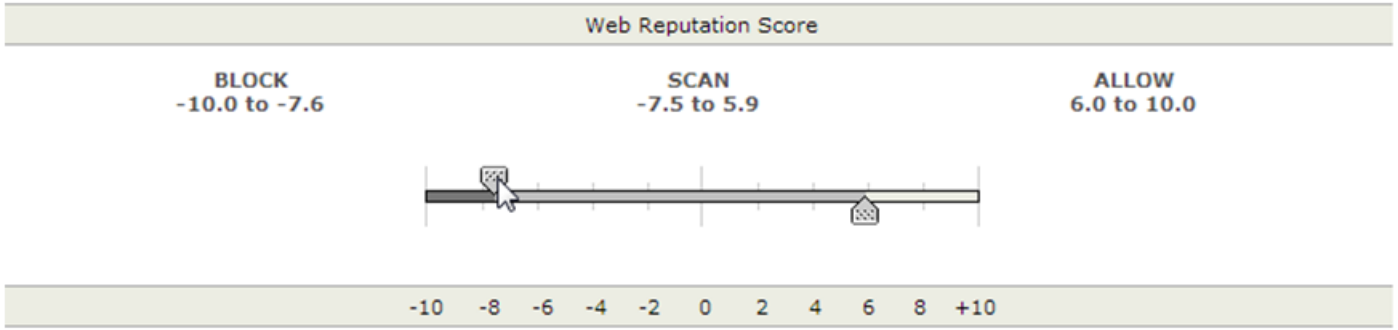
- U ovoj sekciji Access polise moguće je blokirati popularne web aplikacije
  - Cisco održava listu web aplikacija koje se mogu zabraniti
  - Ideja je da se granularno zabranjuju neki sadržaji na web servisima

Access Polisa - Objekti



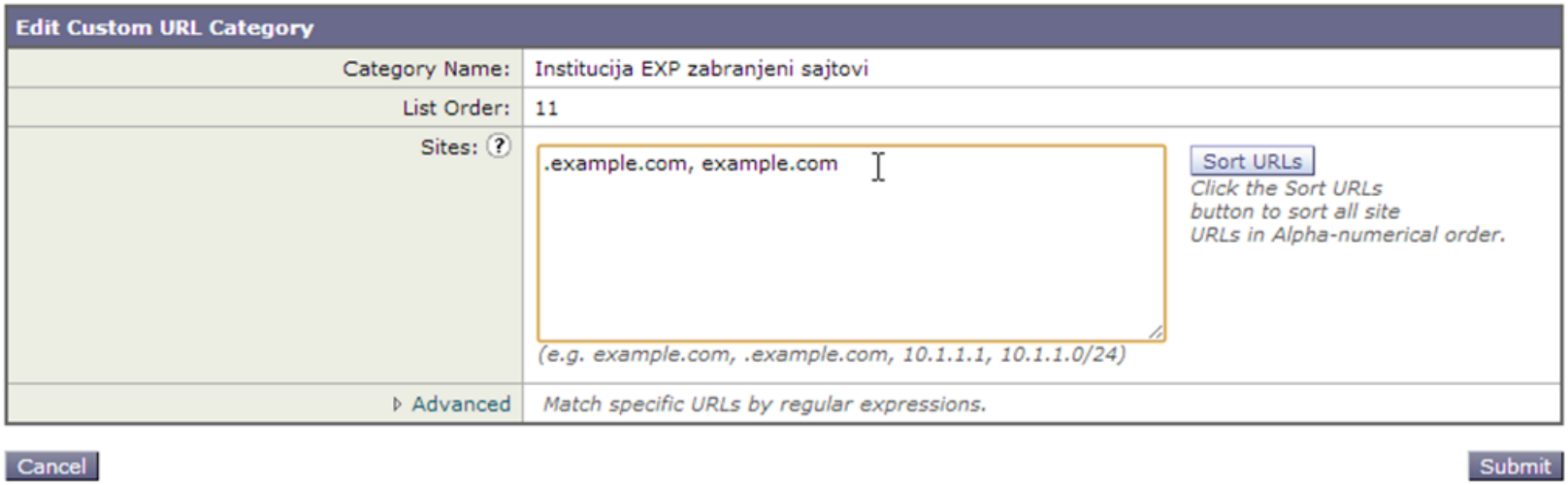
- U ovoj sekciji Access Polise može se blokirati prenos određenih fajlova
  - Ironport je objekte/fajlove podelio u 8 kategorija
  - Pored potpune blokade fajlova, moguće je uvesti i maksimalno dozvoljenu veličinu fajla (npr. 25 MB)

Access Polisa - Web reputacija



- Cisco za svaki web sajt uvodi Web reputaciju:
  - Web reputacija je mera problema koji je sajt stvarao krajnjim korisnicima
  - Web reputacija se dodeljuje u opsegu [-10,10]
    - Suviše niska Web reputacija [-10,-7.5] automatski blokira sajt bez daljeg istraživanja
    - Umerena Web reputacija [-7.4, 5.9] pokreće skeniranje sadržaja na malicionzni softver
    - Odlična Web reputacija [6,10] automatski dozvoljava prenos sadržaja bez provere

Custom URL kategorija



- Svaka institucija ima pravo na jednu Custom URL kategoriju
  - Custom URL kategorija sadrži spisak eksplicitno blokiranih sajtova
  - Služi za dodatnu blokadu web sajtova koji nisu blokirani u postojećoj konfiguraciji

AMRES Stranica obaveštenja

Tražena Web stranica je blokirana na osnovu kategorije sadržaja

Prema bezbednosnim pravilima koje je postavio administrator vaše institucije i/ili AMRES, pristup ovoj Web stranici (http://www.bet365.com/) je blokiran. Sadržaj navedene Web stranice pripada kategoriji: "Gambling" koja nije dozvoljena.

Ukoliko imate neka pitanja, ili smatrate da je ova Web stranica pogrešno klasifikovana, molimo vas kontaktirajte administratora vaše institucije. U poruku upišite i kontrolni kod prikazan dole na stranici. Spisak institucija i nadležnih administratora možete pronaći u dnu Web stranice. Ukoliko vaša institucija nije na spisku, molimo vas kontaktirajte AMRES Helpdesk (helpdesk@amres.bg.ac.rs).

Kontrolni kod: (Thu, 12 Dec 2013 01:15:37 CET, proxy2.amres.ac.rs, HTTP, BLOCK-WEBCAT, http://www.bet365.com/, www.bet365.com, Gambling, GET, 5.9, , , 147.91.255.20, Kukolecha_PC, Kukolecha_PC)

Institucija	Administrator	E-mail

- Kada korisnici ne mogu preko proxy uređaja da pristupe nekom sajtu ispisuje se AMRES stranica obaveštenja
- Administratori su dužni da obrađuju pritužbe korisnika

AMRES Stranica obaveštenja

Tražena Web stranica je blokirana na osnovu kategorije sadržaja

Prema bezbednosnim pravilima koje je postavio administrator vaše institucije i/ili AMRES, pristup ovoj Web stranici (http://www.bet365.com/) je blokiran. Sadržaj navedene Web stranice pripada kategoriji: "Gambling" koja nije dozvoljena.

Ukoliko imate neka pitanja, ili smatrate da je ova Web stranica pogrešno klasifikovana, molimo vas kontaktirajte administratora vaše institucije. U poruku upišite i kontrolni kod prikazan dole na stranici. Spisak institucija i nadležnih administratora možete pronaći u dnu Web stranice. Ukoliko vaša institucija nije na spisku, molimo vas kontaktirajte AMRES Helpdesk (helpdesk@amres.bg.ac.rs).

Kontrolni kod: (Thu, 12 Dec 2013 01:15:37 CET, proxy2.amres.ac.rs, HTTP, BLOCK-WEBCAT, http://www.bet365.com/, www.bet365.com, Gambling, GET, 5.9, , , 147.91.255.20, Kukolecha_PC, Kukolecha_PC)

Institucija	Administrator	E-mail

- Kada korisnici ne mogu preko proxy uređaja da pristupe nekom sajtu ispisuje se AMRES stranica obaveštenja
- Administratori su dužni da obrađuju pritužbe korisnika

Prijava na servis

- Institucija se prijavljuje na servis slanjem e-mail poruke na helpdesk@amres.ac.rs
  - Navodi se ime zaduženog administratora
  - E-mail adresa za pritužbe
- AMRES obezbeđuje nalog administratoru u AMRES Admin LDAP bazi
- AMRES kreira na Ironport SMA uređaju:
  - Nalog institucije
  - 1 Access polisu za potrebe institucije
  - 1 Custom URL kategoriju za potrebe institucije
- AMRES dostavlja administratoru uputstvo za korišćenje servisa