# Centralizovani sistem za filtriranje web saobraćaja

Dokument najbolje prakse
(smernice i preporuke)

Izrađen u okviru AMRES tematske grupe za oblast sigurnost
(AMRES BPD 113)

**Autori: Ivan Ivanović, Miloš Kukoleča, Jovana Palibrk**
**Saradnici: Dušan Pajin**

**Mart 2013**

Dokument broj: GN3-NA3-T4-AMRES-BDP-113
Verzija / datum: Mart 2013.
Izvorni jezik : Srpski
Originalni naslov: “Centralizovani sistem za filtriranje web saobraćaja”
Originalna verzija / datum: Verzija 1 / 19. Mart 2013.
Kontakt: ivan.ivanovic@rcub.bg.ac.rs, milos.kukoleca@amres.ac.rs, jovana.palibrk@amres.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za oblast sigurnost organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.



Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)”.



# Sadržaj

# Executive Summary

The purpose of this document is to introduce the reader to an IronPort firewall technical solution for web traffic filtering that could be used in a campus environment. In addition to the design, configuration and positioning of the centralized IronPort firewall system, the document also deals with some important recommendations regarding the mechanisms that ensure a redirection and even distribution of web traffic toward the firewall devices and the collection and analysis of the data on user activity in the network. The document also looks into the advantages and shortcomings of such a centralised system. Although the document describes the operation of the specialised IronPort firewall equipment, certain ideas and techniques can be also applied to the equipment of any other manufacturer.

# Rezime

Cilj ovog dokumenta ja da se čitalac uputi u tehničko rešenje filtriranja web saobraćaja u okviru kampus okruženja pomoću specijalizovanih IronPort *firewall* uređaja. Pored dizajna, konfigurisanja i pozicioniranja IronPort *firewall* sistema, dokument obuhvata i druge bitne preporuke kao što su mehanizmi za ravnomernu distribuciju web saobraćaja ka *firewall* uređajima i prikupljanja i analize aktivnosti korisnika na mreži. Dokument takođe obuhvata prednosti i mane korišćenja ovakvog centralizovanog sistema. Iako dokument opisuje rad sa specijalizovanom IronPort *firewall* opremom, pojedine ideje i tehnologije se mogu primeniti i na opremi bilo kojeg drugog proizvođača.

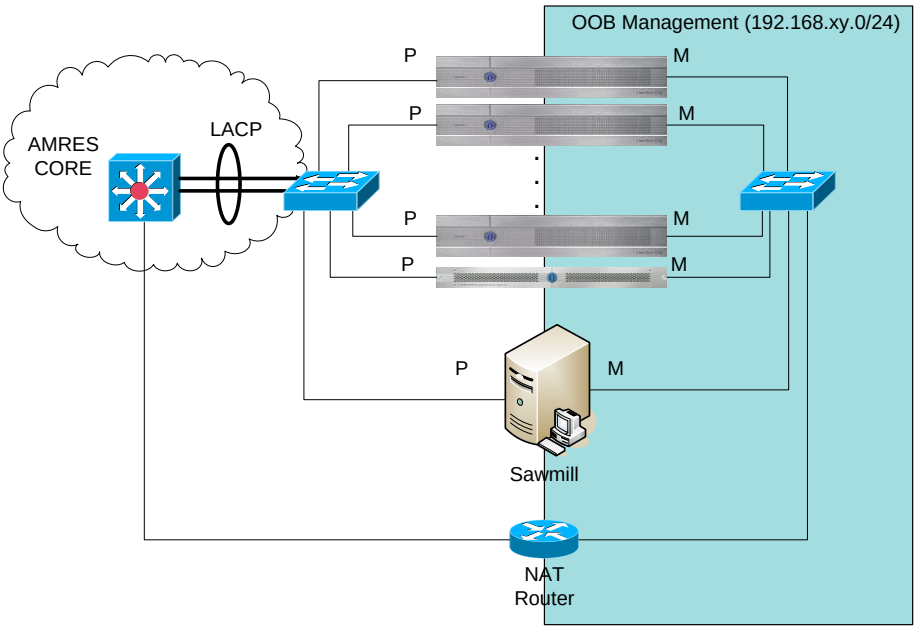
# Uvod

Usled povećanja aktivnosti korisnika na Internetu i razvoja sofisticiranih malicioznih softvera za napad javila se potreba za povećanjem nivoa sigurnosti korisnika u okviru AMRES mreže. Dosadašnje metode koje su se koristile za filtriranje web saobraćaja i zaštitu korisnika su se oslanjale na *access* liste koje su postavljane na ruterskim platformama ili proksi serverima. Ovakav način filtriranja web saobraćaja ima ograničenja jer omogućava filtriranje samo na osnovu protokola, portova i IP adresa.

Filtriranje i inspekcija saobraćaja iznad L4 sloja OSI modela se nije obavljala i to je glavni razlog zašto se javila potreba za postavljanjem *firewall* sistema koji bi imao ovakvu mogućnost.

# 1 Arhitektura i dizajn sistema

Na slici 1 je data arhitektura sistema koji se koristi u okviru AMRES-a. Na slici se vidi da je mrežni deo sistema razdvojen na dva dela. Prvi deo se odnosi na mrežu kroz koju prolazi produkcioni saobraćaj dok drugi deo obuhvata mrežu kroz koju prolazi menadžment saobraćaj. Kako IronPort uređaji poseduju više mrežnih gigabitnih interfejsa, jedan interfejs je iskorišćen za produkcioni saobraćaj (P interfejs) a drugi za menadžment saobraćaj (M interfejs). Na ovaj način je izvršeno fizičko razdvajanje produkcionog i menadžment saobraćaja pomoću OOB (*Out of Band*) mreže. M i P portovi svih IronPort uređaja su povezani na ostatak mreže preko gigabitnih svičeva u cilju ostvarivanja što većih protoka. Ulazak u OOB deo mreže se ostvaruje preko NAT rutera na kome je dozvoljen pristup samo sa IP adresa administratora IronPort sistema.




*Slika 1 – Arhitektura sistema*

P (produkcioni) interfejsi se koriste za rad se produkcionim web saobraćajem.

M (menadžment) interfejsi se koriste za menadžment uređaja, odnosno za:

- Pristup i administraciju IronPort uređaja preko WEB-a i SSH protokola.
- Prenos logova o aktivnosti korisnika na Sawmill server u OOB delu mreže.
- Pristup i administraciju uređaja pomoću centralnog IronPort M160 menadžment uređaja.
- Nadgledanje uređaja putem SNMP protokola

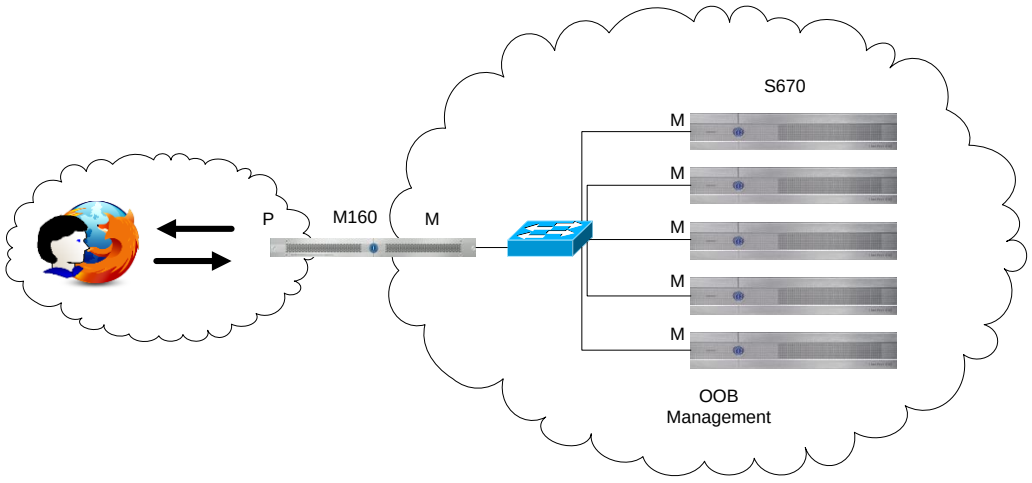
# 2 Centralizovani menadžment

Jezgro sistema za filtriranje web saobraćaja čine jedan uređaj za centralizovano upravljanje IronPort M160, i 5 *firewall* uređaja IronPort S670. IronPort M160 je centralizovani menadžment uređaj koji administratoru omogućava da istovremeno primeni konfiguraciju na sve dostupne IronPort S670 *firewall* uređaje. IronPort S670 su *firewall* uređaji koji obrađuju web saobraćaj na osnovu niza pravila koje definiše administrator.

Na ovaj način se izbegava ponavljanje istog posla na više *firewall* uređaja i samim tim se smanjuje mogućnost greške u konfiguraciji. Takođe se postiže konzistentnost konfiguracija na svim *firewall* uređajima. IronPort M160 uređaj takođe poseduje mogućnost prikupljanja i obrade log informacija, međutim ovakvo rešenje zahteva kupovinu dodatne licence. U slučaju rešenja koje je primenjeno u okviru AMRES-a prikupljanje log informacija je rešeno na drugi način i to je opisano u daljem tekstu.

U daljem tekstu će se koristiti "*firewall*" naziv za sve IronPort S670 uređaje koji imaju mogućnost filtriranja i blokiranja web saobraćaja, dok će se naziv "uređaj za centralizovani menadžment" odnositi na IronPort M160 uređaj koji se koristi za centralizovani menadžment svih IronPort S670 uređaja.

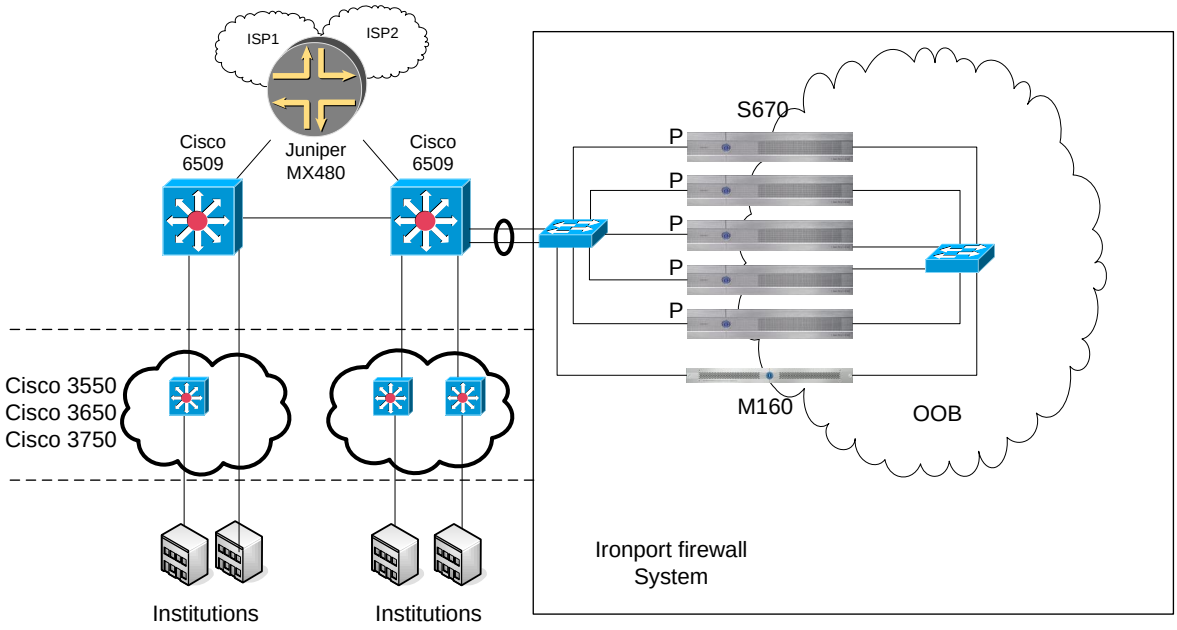
Na slici 2 je prikazan princip OOB menadžmenta, gde se koristi zasebna fizička infrastruktura za konfigurisanje *firewall* uređaja. U okviru OOB opsega se koristi privatni adresni opseg koji se ne oglašava kroz ostatak mreže i na taj način se uvodi dodatni nivo sigurnosti i kontrole pristupa *firewall* sistemu. Menadžment uređaj poseduje dva porta, prvi je P port, preko koga se prilazi opcijama za konfigurisanje kroz produkcioni deo mreže, a drugi je menadžment M port, koji je izolovan u okviru OOB dela mreže i preko koga se primenjuje željena konfiguracija na sve *firewall* uređaje.




*Slika 2 – OOB menadžment pomoću* WEB *pretraživača*

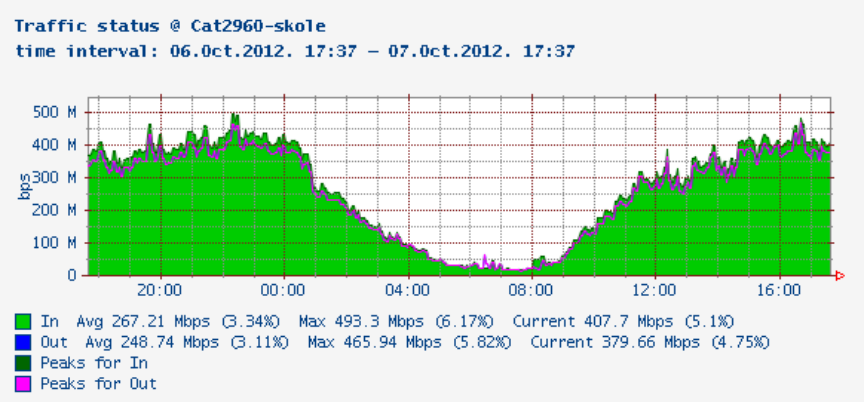
# 3 Pozicija *firewall* sistema

Sistem za filtriranje web saobraćaja je pozicioniran u *core* delu mreže. Slika 3 predstavlja poziciju sistema u odnosu na ostale uređaje u mreži.

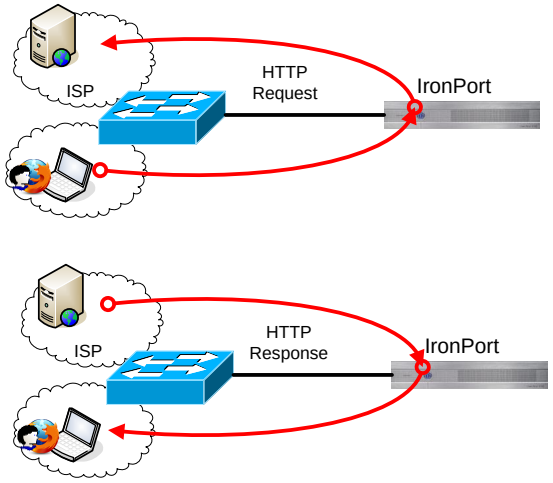



Slika 3 - Pozicija *firewall* sistema

*Firewall* uređaji se ponašaju kao proksi serveri, odnosno sav generisani web saobraćaj mora prvo doći do *firewall* uređaja, gde se vrši filtriranje i skeniranje, a zatim se obrađeni web saobraćaj prosleđuje do krajnje destinacije. Povratni web saobraćaj se takođe skenira na osnovu nekoliko definisanih parametara. Kako sav odlazni i dolazni saobraćaj mora proći kroz *firewall* sistem dolazi do dupliranja saobraćaja na linkovima, odnosno ulazni i izlazni saobraćaj na portovima *firewall* uređaja je približno isti. Na slici 4 je dat primer statistike dupliranog ulaznog i izlaznog produkcionog web saobraćaja za period od 24h, dok slika 5 ilustruje primer ove situacije.




*Slika 4 – Primer statistike* ulaznog i izlaznog *saobraćaja na glavnom linku ka firewall sistemu*




*Slika 5 – Primer dupliranja ulaznog i izlaznog saobraćaja*

Usled dupliranja saobraćaja potrebno je obratiti pažnju na linkove koji povezuju *firewall* sistem sa ostatkom infrastrukture. Preporučuje se da se koristi agregacija linkova (npr. LACP protokol) da bi se izbeglo zagušenje na linkovima između *core* dela mreže i *firewall* sistema.

Pozicija sistema u okviru *core* dela mreže se preporučuje obzirom da se sav saobraćaj ka Internetu iz *access* dela mreže agregira ka *core* delu mreže, tako da se ovakvom pozicijom *firewall* sistema postiže optimalno iskorišćenje mrežnih resursa.

# 4 Redirekcija saobraćaja ka *firewall* sistemu

## 4.1 Metode redirekcije saobraćaja

Da bi se optimalno koristili resursi *firewall* sistema potrebno je ravnomerno preusmeriti web saobraćaj krajnjih korisnika ka svakom od *firewall* uređaja. U daljem tekstu je dat niz primera i preporuka kako se to može uraditi bez korišćenja specijalizovane opreme.

Mogući su sledeći scenariji preusmeravanja web saobraćaja:

- Preusmeravanje web saobraćaja na osnovu proksi konfiguracije u okviru Internet pretraživača
- Preusmeravanje web saobraćaja na osnovu *policy based* rutiranja
- Preusmeravanje web saobraćaja pomoću WCCP (Web *Cache Communication Protocol*) protokola

U okviru sva tri moguća principa rada akcenat je postavljen na mogućnosti ravnomerne distribucije web saobraćaja ka više *firewall* uređaja, a u cilju njihovog ravnomernog opterećenja.

## 4.2 Konfiguracija u okviru Internet pretraživača

Konfiguracija u okviru Internet pretraživača se obavlja podešavanjem odgovarajućih opcija u proksi konfiguraciji samog pretraživača. Moguće su dve vrste konfiguracije:

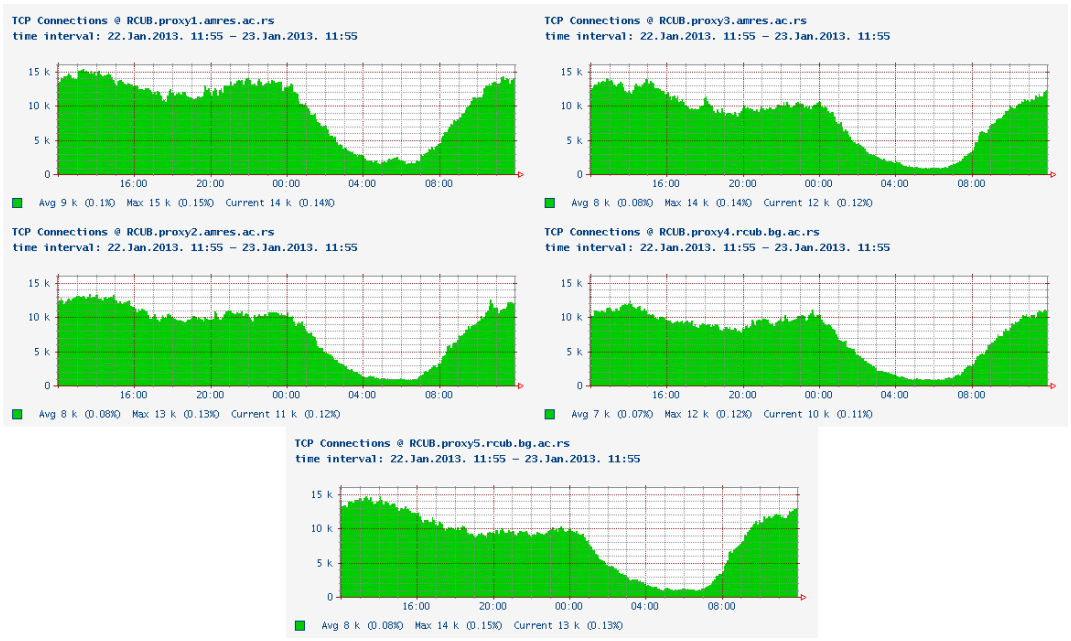
- Statička konfiguracija
- Dinamička autokonfiguracija

### 4.2.1 Statička konfiguracija

#### 4.2.1.1 *Ručna konfiguracija upisivanjem IP adrese ili DNS naziva firewall uređaja*

Preusmeravanje saobraćaja se obavlja na osnovu informacije o IP adresi ili DNS nazivu *firewall* uređaja koju korisnik mora sam da unese u okviru proksi podešavanja svog Internet pretraživača. Preporučuje se da se koristi DNS naziv iz više razloga:

- Promena IP adrese *firewall* uređaja je transparentna za korisnika. U slučaju promene IP adrese korisnik ne mora ponovo da podešava Internet pretraživač, obzirom da će DNS servis uvek vratiti pravu/izmenjenu IP adresu *firewall* uređaja.
- U slučaju da se koristi više *firewall* uređaja preporučuje se da se za sve IP adrese *firewall* uređaja podesi isti DNS naziv, a da se DNS servis konfiguriše tako da razrešava DNS ime *firewall* uređaja u *round-robin* režimu. Na ovaj način se korisniku omogućava da podjednako koristi IP adrese svih *firewall* uređaja.
- Na slici 6 je prikazan primer raspodele produkcionog web saobraćaja pomoću DNS *round-robin* metode u okviru AMRES mreže. Slika 6 prikazuje broj uspostavljenih konekcija ka 5 različitih *firewall* uređaja. Na slici 6 se vidi da prikupljene vrednosti o broju uspostavljenih konekcija nisu iste na svim *firewall* uređajima i to je očekivano obzirom da neki AMRES korisnici i dalje koriste IP adresu u okviru proksi konfiguracije svog web pretraživača umesto DNS naziva.




*Slika 6 – Raspodela* web *saobraćaja pomoću DNS round-robin metode razrešavanja*

### 4.2.1.2 *Ručna konfiguracija upisivanjem lokacije PAC (Proxy Auto Configuration) fajla*

U ovom rešenju korisnik mora da unese URL putanju do PAC fajla u okviru proksi podešavanja svog Internet pretraživača. PAC fajl predstavlja *javascript* koji sadrži pravila o tome kako će Internet pretraživač vršiti prosleđivanje web saobraćaja. Na slici 7 je dat primer sadržaja jednog PAC fajla. Sekcije 1-4 na slici 7 definišu kako će se Internet pretraživač ponašati u zavisnosti od toga šta je upisano u njegovo URL polje.

Prva sekcija definiše da se ne koristi *firewall* sistem ako je u URL polje upisan samo naziv bez tačke. U ovom slučaju Internet pretraživač neće koristiti *firewall* sistem zato što se pretpostavlja da je URL samo naziv uređaja iz lokalnog domena u kome se nalazi i računar sa Internet pretraživačem.

U drugoj sekciji se proverava da li je korišćeni URL deo lokalnog domena i u tom slučaju se ne koristi redirekcija ka *firewall* sistemu.

U trećoj sekciji se posmatra da li se URL razrešava u neku od IP adresa iz lokalnog domena i u tom slučaju se ne koristi redirekcija ka *firewall* sistemu.

U četvrtoj sekciji se koristi proksiranje u *fail-over* režimu. To znači da ako nije ispunjena nijedna od sekcija 1-3, prvo će se koristiti DNS naziv *proxy.mydomain.com:8080* (DNS će razrešavati *proxy.mydomain.com* URL u *round-robin* režimu). U slučaju da je DNS server nedostupan koristiće se prvo 172.16.0.1:8080 uređaj, a ako je on nedostupan koristiće se respektivno 172.16.0.2:8080 pa potom 172.16.0.3:8080 uređaji. Ako nijedan od IronPort uređaja nije dostupan neće se koristiti proksiranje i Internet pretraživač će pokušati direktno da izađe na Internet.

```
function FindProxyForURL(url, host) {

// Section 1. If URL has no dots in host name, send traffic direct.
        if (isPlainHostName(host))
                return "DIRECT";

// Section 2. If specific URL needs to bypass proxy, send traffic direct.
        if (shExpMatch(url,"*.myfirst.domain1.com*") ||
                shExpMatch(url,"*.mysecond.domain2.com*") ||
                shExpMatch(url,"*localhost*"))
                return "DIRECT";

// Section 3. If IP address is internal or hostname resolves to internal
IP, send direct.

        var resolved_ip = dnsResolve(host);
        if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||
                isInNet(resolved_ip, "172.16.0.0", "255.255.0.0") ||
                isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
                isInNet(resolved_ip, "127.0.0.0",  "255.255.255.0"))
        return "DIRECT";

// Section 4. All other traffic uses below proxies, in fail-over order.
        return "PROXY proxy.mydomain.com:8080; PROXY 172.16.0.1:8080; PROXY
172.16.0.2:8080; PROXY 172.16.0.3:8080; DIRECT";
```

*Slika 7 – Primer konfiguracije PAC fajla*

### 4.2.2 Dinamička autokonfiguracija

Dinamička autokonfiguracija pomoću WPAD (Web *Proxy Auto-Discovery* Protocol) protokola se pokreće u okviru proksi podešavanja Internet pretražvača tako što se selektuje polje za autodetekciju proksi servera.

Primeri opcija u najpopularnijim Internet pretraživačima su:

- Mozilla Firefox
  - “Autodetect proxy settings for this network”
- Google Chrome & Internet Explorer
  - “Automatically detect settings”

WPAD protokol funkcioniše tako što proveri u kom domenu se nalazi korisnički računar i pokušava da pronađe *wpad.dat* fajl u tom domenu. Pretpostavljeno je da je računar koji je podešen da automatski detektuje proksi server u *mydomain.example.com* domenu, a da se *wpad.dat* fajl nalazi na web lokaciji *wpad.example.com*. Koraci u radu WPAD protokola su sledeći:

- Pretraživač će prvo pokušati da pronađe *wpad.dat* fajl na lokaciji *http://wpad.mydomain.example.com/wpad.dat*
- Kada ustanovi da *wpad.dat* na toj lokaciji ne postoji pokušaće da potraži fajl na narednom višem domenu (*parent domain*), odnosno pokušaće da priđe lokaciji *http://wpad.example.com/wpad.dat* i tu će pronaći *wpad.dat* fajl.

I u ovom slučaju će se u okviru *wpad.dat* fajla koristiti DNS naziv *firewall* uređaja, odnosno DNS razrešavanje u *round-robin* režimu će omogućiti ravnomernu distribuciju web saobraćaja ka svim *firewall* uređajima. WPAD fajl ima identičnu sintaksu kao PAC fajl.

## 4.3 Redirekcija na osnovu PBR rutiranja

Preusmeravanje se može obaviti i pomoću PBR (*Policy Based Routing*) rutiranja odnosno na samim ruterskim platformama u *core* delu mreže. Potrebno je izdvojiti željeni web saobraćaj pomoću *access* listi i zatim ga preusmeriti ka *firewall* uređajima. Problem sa ovakvim pristupom je što se ne mogu optimalno iskoristiti svi *firewall* uređaji obzirom da je nemoguće ostvariti ravnomernu raspodelu saobraćaja pomoću PBR rutiranja. Redirekcija web saobraćaja se može obaviti samo ka jednom *firewall* uređaju. Ovakvo rešenje ne zahteva konfiguraciju na strani korisnika ali je potrebno da se *firewall* uređaji pokrenu u transparentnom režimu rada. Na slici 8 je dat primer konfiguracije na Cisco 6500 uređaju. Sav TCP saobraćaj koji se generiše iz mreže 10.20.30.0/24 ka bilo kojoj IP adresi sa odredišnim portom 80 ili 443 će biti preusmeren ka *firewall* uređaju sa *next-hop* IP adresom 172.16.0.1. Ovaj princip ima smisla koristiti kada postoji samo jedan *firewall* uređaj ka kome treba preusmeravati web saobraćaj.

```
ip access-list extended WEB
permit tcp 10.20.30.0 0.0.0.255 any eq 80
permit tcp 10.20.30.0 0.0.0.255 any eq 443
!
route-map REDIRECT2IRONPORT permit 10
match ip address WEB
set ip next-hop 172.16.0.1
!
interface GigabitEthernet0/0
ip policy route-map REDIRECT2IRONPORT
```

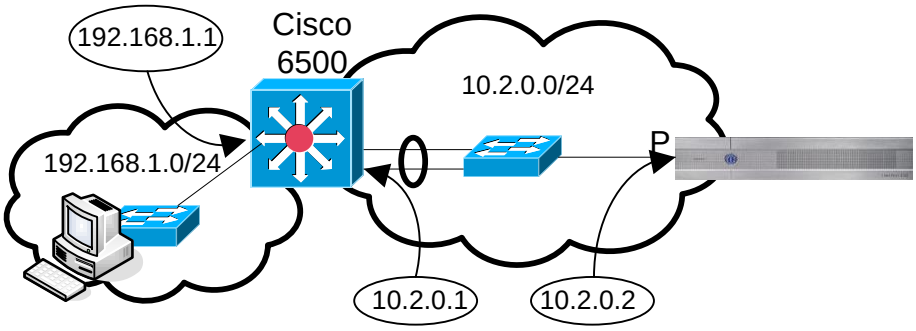
*Slika 8 – Primer konfiguracije na Cisco 6500 uređaju*

## 4.4 Redirekcija pomoću WCCP protokola

WCCP (Web *Cache Communication Protocol*) je protokol koji je razvijen od strane Cisco kompanije i danas je podržan i kod drugih proizvođača mrežne i serverske opreme. Trenutno postoje dve verzije protokola, V1 i V2. Preporučuje se korišćenje verzije 2 zato što donosi nove funkcionalnosti kao što su, podrška i za druge servise osim HTTP-a, grupisanje WCCP rutera u klastere, MD5 autentifikaciju i ravnomernu distribuciju saobraćaja. Za razliku od PBR rutiranja WCCP protokol ima mogućnost ravnomerne distribucije saobraćaja i zbog toga se preporučuje da se koristi u situacijama gde postoji više *firewall* uređaja i gde je neophodno ravnomerno rasporediti saobraćaj ka svakom od njih. WCCP se može konfigurisati na dva načina u zavisnosti od topologije

mreže i veze između mrežnih uređaja. Preporučuje se da se *firewall* uređaji povežu sa *core* ruterima direktno na L2 nivou i u tom slučaju je moguće vršiti direktno prosleđivanje web saobraćaja u hardveru. U suprotnom, ako su *firewall* uređaji u nekom posebnom, odvojenom L3 segmentu, WCCP će koristiti GRE (*Generic Routing Encapsulation*) protokol da bi izvršio tunelovanje preusmerenog web saobraćaja.

Prilikom konfigurisanja WCCP protokola potrebno je obratiti pažnju na tip uređaja na kom se WCCP pokreće. Kod Cisco 6500 serije uređaja WCCP protokol podržava hardversko prosleđivanje paketa samo kada je na interfejsu uređaja pokrenuta WCCP redirekcija u dolaznom (*in*) smeru. Ako se na interfejsu pokrene WCCP redirekcija u odlaznom (*out*) smeru Cisco 6500 uređaj će vršiti prosleđivanje u softveru i zbog toga može doći do većeg opterećenja procesora, što može drastično umanjiti performanse uređaja. U slučaju kada se koristi WCCP protokol sav web saobraćaj će biti preusmeren na *firewall* uređaje i korisnici neće morati da izvrše podešavanje u svojim Internet pretraživačima. Na slici 9 se nalazi primer WCCP topologije dok se na slici 10 nalazi primer konfiguracije WCCP protokola na Cisco 6500 uređaju. U slučaju da se koristi više *firewall* uređaja, WCCP proces na Cisco 6500 uređaju bi koristio *load-balancing* metodu u cilju što ravnomernije raspodele saobraćaja ka *firewall* uređajima. Iako je WCCP protokol razvijen od strane Cisco kompanije, može se koristiti i kod drugih vendora kao što je BlueCoat a i kod *opensource* rešenja kao što je Squid proxy.




*Slika 9 – Primer L2 topologije na kojoj se pokreće WCCP protokol*

```
ip wccp 50 redirect-list WCCP-REDIRECT
!
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip wccp 50 redirect in
!
ip access-list extended WCCP-REDIRECT
permit tcp 192.168.1.0 0.0.0.255 any eq 80
permit tcp 192.168.1.0 0.0.0.255 any eq 443
```

*Slika 10 – Primer konfiguracije WCCP protokola na Cisco 6500 uređaju*

# 5 Ironport *cloud* servis

Centralizovani web *firewall* sistem je zamišljen da funkcioniše kao *cloud* servis. Osoblje AMRES-a upravlja i održava *firewall* sistem u cilju pružanja *cloud firewall* servisa institucijama i krajnjim korisnicima. Tehnički kontakti AMRES institucija imaju strogo definisane privilegije na centralizovanom *firewall* sistemu tako da mogu da podešavaju parametre za filtriranje i skeniranje koji utiču samo na web saobraćaj koji potiče iz njihove institucije. *Cloud* rešenje podrazumeva da tehnički kontakt institucije može pristupiti izmeštenim (centralizovanim) hardverskim i softverskim resursima i prilagođavati ih prema potrebama korisnika svoje institucije. Centralizovanim *firewall* sistemom se služe svi krajnji AMRES korisnici u cilju zaštite od malicioznog saobraćaja na Internetu.

Tehničkom kontaktu institucije je dodeljeno pravo konfigurisanja pristupne polise koja vrši skeniranje i filtriranje saobraćaja iz matične institucije tog tehničkog kontakta. U slučaju da institucija ne želi da administrira svoju pristupnu polisu sav saobraćaj te institucije će biti obuhvaćen krajnjom *default* pristupnom polisom koju uređuje osoblje AMRES-a.

Sav web saobraćaj koji prolazi kroz *firewall* uređaje mora da bude obrađen u okviru neke od definisanih pristupnih polisa dok se svaka pristupna polisa odnosi na određeni adresni opseg. Na ovaj način su pristupne polise povezane sa saobraćajem pojedinačnih institucija. Prilikom skeniranja web transakcije, *firewall* uređaji ispituju redom pristupne polise u potrazi za onom koja odgovara adresnom opsegu pomenute web transakcije. Ukoliko se pronađe odgovarajuća pristupna polisa, web transakcija se tretira *firewall* parametrima koji su definisani u posmatranoj pristupnoj polisi. Poslednja u nizu pristupnih polisa je *default* pristupna polisa koja će obraditi sav saobraćaj koji nije obuhvaćen prethodnim polisama.

Krajnja *default* pristupna polisa definiše osnovna pravila kojih se moraju pridržavati sve institucije. Institucije mogu u okviru svoje pristupne polise dodatno pooštriti *firewall* parametre ali ih nikako ne smeju ublažiti. *Firewall* parametri u pristupnoj polisi se grupišu u 5 sekcija:

- Dozvoljeni protokoli i Internet pretraživači
- URL filtriranje
- Kontrola aplikacija
- Kontrola objekata
- Web reputacija

## 5.1 Dozvoljeni protokoli i Internet pretraživači

U ovoj sekciji je moguće zabraniti neki od sledećih protokola:

- HTTP
- HTTPS
- FTP
- FTP preko HTTP-a

Dodatno je moguće zabraniti korišćenje određenih Internet pretraživača prilikom pristupa Internetu.Ukoliko se ustanovi da neki Internet pretraživač ne zadovoljava sigurnosne standarde institucije, tehnički kontakt može uvesti zabranu njegovog korišćenja za korisnike matične insitucije.*Default* pristupna polisa ne blokira nijedan od navedenih protokola niti zabranjuje bilo koji Internet pretraživač.

## 5.2 URL filtriranje

Ovom sekcijom se definiše skup URL kategorija kojima je dozvoljen pristup putem Interneta. Cisco kompanija vrši kategorizaciju web prezentacija na osnovu njihovog sadržaja. Informacije o URL kategorijama se periodično dodaju u baze podataka na *firewall* uređajima na kojima se vrši kategorizacija web stranica. U trenutku pisanja dokumenta bilo je dostupno 78 različitih kategorija web sajtova i Cisco kompanija periodično dodaje nove kategorije. U okviru IronPort URL filtering sistema postoji mogućnost da pojedini sajtovi budu svrstani u pogrešnu kategoriju. Stoga je u AMRES-u napravljena posebna kategorija koja eksplicitno pušta sajtove koji su u okviru nje definisani. Ukoliko se operativnim radom ustanovi da je sajt pogrešno kategorizovan i greškom blokiran, sajt se smešta u posebnu kategoriju koja eksplicitno dozvoljava pristup toj web stranici. Time se pristup sajtu privremeno dopušta a greška se naknadno prijavljuje Cisco podršci. Na taj način se privremeno rešava problem pogrešno kategorizovanih sajtova sve dok se na naprave globalne izmene u Cisco bazi kategorija, a nakon toga se web sajt uklanja iz ove posebne kategorije.

*Default* pristupna polisa blokira sledeće WEB kategorije:

- Child Abuse Content
- Filter Avoidance
- Gambling
- Hate Speech
- Illegal Drugs
- Pornography

## 5.3 Kontrola aplikacija

U ovoj sekciji je moguće blokirati rad pojedinih web aplikacija. Cisco je kreirao bazu najpoznatijih web aplikacija nad kojima se može uspostavljati blokada. Baza se povremeno dopunjuje dodavanjem novih poznatih aplikacija. Aplikacije uglavnom potiču sa najpopularnijih servisa na Internetu kao što su Facebook, Google+,

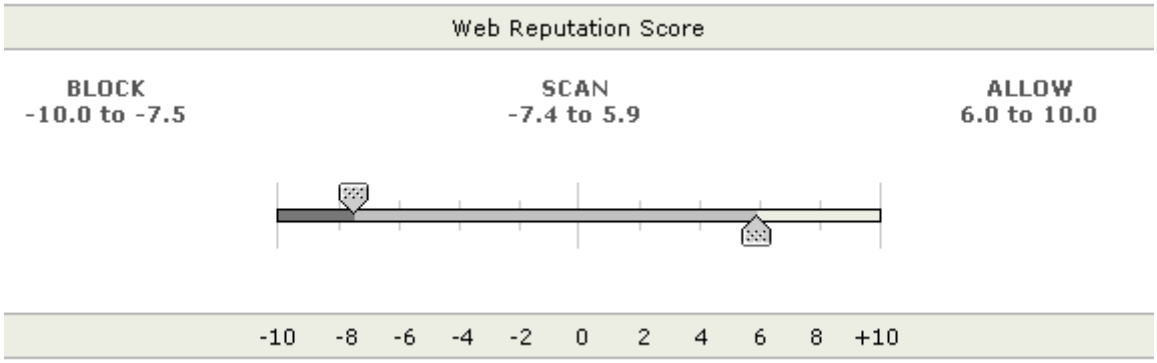
iTunes, LinkedIn itd. *Default* pristupna polisa ne vrši blokadu nijedne web aplikacije. Tehnički kontakti mogu blokirati web aplikacije korisnicima iz svoje institucije ukoliko smatraju da je to potrebno.

## 5.4 Kontrola objekata

Sekcija kontrole objekata omogućava zabranu prenosa pojedinih objekata do krajnjih klijenata. Moguće je zabraniti fajlove sa određenom ekstenzijom ili tip saobraćaja kao što je video ili audio *streaming*. Tehnički kontakti mogu zabraniti i pojavu *flash* ili *Javascript* funkcija u Internet pretraživačima krajnjih korisnika. Sekcija dozvoljava i blokadu pojedinačnih MIME (*Multipurpose Internet Mail Extensions*) tipova podataka čime se obezbeđuje dodatna granularnost. Sekcija omogućava i uvođenje ograničenja u zavisnosti od veličini objekta koji se prenosi.Tako je moguće sprečiti preuzimanje velikih fajlova kako bi se sačuvali kapaciteti u mrežama institucija. *Default* pristupna polisa ne vrši blokadu nijednog objekta u AMRES mreži niti uvodi ograničenja u veličini objekta koji se može preuzeti sa Interneta.

## 5.5 Web reputacija

Ovom sekcijom je moguće definisati u kojim situacijama će se vršiti blokiranje sajtova, skeniranje na maliciozni sadržaj ili će biti omogućen pristup web sajtu bez skeniranja. Odluka o ovim akcijama se donosi na osnovu web reputacije web sajta. Cisco je oformio sistem ocenjivanja web sajtova na osnovu sumnjivih i malicioznih aktivnosti i u sistem je uključio veliki broj web sajtova. Web sajtovi se svakodnevno ispituju kako bi pokrivenost sistema bila dobra,a ocene fer. Ocena web sajta predstavlja meru problema koju je neki web sajt pravio svojim korisnicima po pitanju *malware*-a, *phishing* aktivnosti, *spyware*-a, virusa ili *spam* poruka. Ocenjivanje se obavlja na skali od -10 do +10, pri čemu je -10 najgora a +10 najbolja ocena. Kada krajnji korisnik pokušava da pristupi određenom web sajtu, *firewall* uređaj proverava web reputaciju sajta i ukoliko je ocena zadovoljavajuća dopušta pristup web sajtu. Važno je optimalno odrediti granične vrednosti za preduzimanje akcija da bi se napravio kompromis između opterećenja uređaja i mogućnosti detekcije malicioznog web sajta. Na slici 8 je dat primer *default* ponašanja za AMRES korisnike.




*Slika 8 – Filtriranje i skeniranje na osnovu* web *reputacije*

Na slici 8 se vidi da će pristup ka sajtu kod koga je ocena (Web *Reputation Score*) manja od -7.4 biti blokiran. Ako je ocena sajta između -7.5 i 5.9 onda će ka sajtu biti omogućen pristup samo ako prođe skeniranje pomoću Web*root anti-malware* softvera za skeniranje. Ako je ocena sajta veća od +6 onda je pristup sajtu dozvoljen bez skeniranja.

# 6 Pristup konfigurisanju uređaja

AMRES ima oko 100.000 korisnika usled čega je obrada web saobraćaja veoma zahtevna. Uzimajući u obzir broj korisnika AMRES mreže, neophodno je korišćenje više *firewall* uređaja kako bi se ravnomerno raspodelila obrada web saobraćaja. Da bi centralizovani *firewall* sistem radio ispravno neophodno je održati konzistentnu konfiguraciju na svim *firewall* uređajima. Nabavkom uređaja za centralizovano upravljanje IronPort M160 i odgovarajuće licence, akademska mreža je u mogućnosti da preko uređaja za centralizovano upravljanje podešava jedinstvenu konfiguraciju na svih 5 *firewall* uređaja. Ovo unosi značajnu skalabilnost u sistem jer se sa povećanjem broja korisnika i količine saobraćaja može dodati još nekoliko *firewall* uređaja kako bi sistem funkcionisao efikasno.

Konfigurisanje parametara u *firewall* sistemu se obavlja preko uređaja za centralizovano upravljanje. Uređaj za centralizovano upravljanje sistemom ima dva mrežna interfejsa: P interfejs koji ima javnu IP adresu i M interfejs koji ima privatnu IP adresu (Slika 2). Upisom odgovarajuće URL adrese u svoj Internet pretraživač tehnički kontakti se povezuju na P interfejs menadžment uređaja. U Internet pretraživaču se prikazuje stranica za prijavljivanje na menadžment uređaj. Nakon upisa kredencijala tehničkog kontakta, u LDAP bazi se vrši autentifikacija i autorizacija. Nakon toga se tehničkom kontaktu dodeljuje pravo da menja polisu koja obuhvata samo saobraćaj koji potiče iz njegove institucije.

Nakon konfiguracije željenih parametara i odabirom odgovarajuće komande prosleđuje se kreirana konfiguracija na sve *firewall* uređaje koji su pod ingerencijom menadžment uređaja. Konfiguracija se prosleđuje preko M interfejsa menadžment uređaja i preko OOB mreže stiže do svih *firewall* uređaja u sistemu. Na ovaj način se održava konzistentna konfiguracija na svim *firewall* uređajima u centralizovanom web *firewall* sistemu.

Administratori AMRES-a se takođe povezuju na P interfejs menadžment uređaja ali imaju privilegije da uređuju sve parametre *firewall* sistema. Osoblje AMRES-a ima mogućnost da se povezuje i na ostale *firewall* uređaje preko M interfejsa tih uređaja. Podešavanje određenih delova konfiguracije kao što su prikupljanje log informacija ili nadogradnja softvera se moraju vršiti na svakom pojedinačnom *firewall* uređaju i ta podešavanja vrši isključivo AMRES osoblje.

# 7 LDAP autentifikacija

Implementacija *cloud* servisa u AMRES mreži zahteva rešenje autentifikacije i autorizacije tehničkih kontakata institucija članica. Optimalno rešenje treba da uzme u obzir sledeće preduslove:

- Jedna institucija članica može imati više tehničkih kontakata koji uređuju *firewall* parametre
- Tehnički kontakti već imaju korisničke naloge koji su otvreni za potrebe nekog drugog AMRES servisa
- Autentifikacijom na centralizovani web *firewall* sistem tehnički kontakti stiču pravo da uređuju *firewall* parametre koji utiču samo na saobraćaj njihove matične institucije.

Autentifikacija tehničkih kontakata se obavlja na menadžment uređaju. Tehnički kontakti institucija autorizacijom stiču pravo da na menadžment uređaju menjaju *firewall* konfiguraciju. Izmenjena *firewall* konfiguracija se potom preko OOB dela mreže prosleđuje do svih *firewall* uređaja u centralizovanom web *firewall* sistemu. Moguće procedure autentifikacije na menadžment uređaju su:

- Autentifikacija pomoću lokalne baze (interna autentifikacija)
- Autentifikacija pomoću RADIUS protokola (eksterna autentifikacija)
- Autentifikacija pomoću LDAP protokola (eksterna autentifikacija)

Uzimajući u obzir sve postavljene preduslove, postojeća rešenja autentifikacije u AMRES mreži i dostupne procedure autentifikacije na menadžment uređaju kao najoptimalnije rešenje se nameće autentifikacija pomoću LDAP protokola.

Za potrebe autentifikacije u AMRES mreži, AMRES održava LDAP direktorijum gde se nalaze podaci o tehničkom osoblju AMRES institucija. U posebnom LDAP direktorijumu se nalazi grana sa nalozima AMRES servisa. U LDAP direktorijumu sa nalozima za AMRES servise nalazi se i administratorski nalog za *firewall* sistem. Pomoću ovog naloga, menadžment uređaj se povezuje na LDAP direktorijum i proverava informacije o korisniku koji pokušava da koristi *firewall* servis. Grana sa tehničkim kontaktima sadrži sve naloge tehničkih kontakata institucija članica. Svaki nalog čini skup LDAP atributa, a najvažniji atributi su:

- *Uid* – korisničko ime tehničkog kontakta
- *Password* – lozinka tehničkog kontakta
- *Organization* – ime institucije kojoj pripada tehnički kontakt
- *EduPersonEntitlement* – atribut koji definiše da li je tehnički kontakt korisnik određenog AMRES servisa

Svaki administrator *firewall* sistema je jednoznačno definisan korisničkim imenom, lozinkom i privilegijama koje ima. Korisničko ime i lozinka se nalaze u LDAP direktorijumu, u grani sa tehničkim kontaktima, a skup privilegija se nalazi na centralizovanom menadžment uređaju. Postoji nekoliko predefinisanih skupova privilegija (*User Roles*) na menadžment uređaju, ali je moguće napraviti i nove skupove sa posebnim privilegijama (*Custom User Role*). Kreiranjem novog skupa privilegija na menadžment uređaju je moguće napraviti polisu koja će imati uticaj samo na web saobraćaj specifične AMRES članice. Prilikom dodavanja institucije na *firewall cloud* servis, kreira se novi skup privilegija (*Custom User Role*) koji nosi ime institucije. U

okviru novog skupa se precizira da se može menjati samo određena polisa koja se tiče nove institucije. Vezivanje naloga tehničkog kontakta iz LDAP baze i seta privilegija na centralizovanom menadžment uređaju se postiže pomoću dva atributa u okviru korisničkih naloga u LDAP direktorijumu:

- *EduPersonEntitlement*
- *Organization*

Na slici 9 se može videti primer naloga tehničkog kontakta u LDAP direktorijumu. Ukoliko tehnički kontakt institucije ima prava da koristi *firewall cloud* servis, njegov nalog u LDAP direktorijumu sadrži atribut *eduPersonEntitlement* koji ima vrednost „*Ironport*“. Ovaj atribut dozvoljava tehničkom kontaktu da se autorizuje na centralizovani menadžment uređaj. Atribut *Organization* sadrži ime institucije iz koje dolazi tehnički kontakt i ovaj atribut vezuje odgovarajući skup privilegija za autentifikovani tehnički kontakt.

```
uid:                          john_doe
Password:                     ********
EduPersonEntitlement:         Ironport
Organization:                 Institution_Name
```

*Slika 9 - Primer naloga tehničkog kontakta u LDAP direktorijumu*

Procedura autentifikacije tehničkog kontakta se obavlja u nekoliko koraka. Tehnički kontakt se preko P interfejsa (Slika 2) povezuje na centralizovani menadžment uređaj i upisuje svoje korisničko ime i lozinku. Centralizovani menadžment uređaj se preko porta 389 povezuje na LDAP server i pomoću posebnog AMRES servisnog naloga vrši proveru kredencijala korisnika. Nakon autentifikacije sa AMRES servisnim nalogom menadžment uređaj stiče pravo da pregleda granu sa tehničkim kontaktima kako bi izvršio njihovu autentifikaciju i autorizaciju. U grani sa tehničkim kontaktima se proverava korisnik koji pokušava da se autentifikuje. Ukoliko korisnik postoji, proveravaju se njegovi kredencijali. Nakon što se utvrdi da su kredencijali ispravni, centralizovani menadžment uređaj proverava da li tehnički kontakt u svom nalogu u LDAP direktorijumu ima atribut eduPersonEntitlement sa odgovarajućom vrednosti „*Ironport*“. Ukoliko ovaj atribut postoji, centralizovani menadžment uređaj može da autentifikuje tehnički kontakt. Potom se proverava atribut *Organization* koji se povezuje sa istoimenim skupom privilegija (*Custom User Role*) na samom centralizovanom menadžment uređaju. Ukoliko postoji odgovarajući skup privilegija, centralizovani menadžment uređaj dodeljuje tehničkom kontaktu taj skup privilegija i autorizuje ga. Nakon autorizacije, tehnički kontakt može da menja konfiguraciju na centralizovanom menadžment uređaju, i to samo onaj deo konfiguracije koji odgovara dodeljenom skupu privilegija.

# 8 Prikupljanje, analiza i skladištenje logova

Svaki *firewall* uređaj zasebno registruje web konekcije i prikuplja log informacije te se podešavanje prikupljanja logova mora obavljati na svakom uređaju pojedinačno. Log informacije se grupišu u log fajlove u zavisnosti od tipa informacija koje se beleže. Logovi se grubo mogu podeliti u dve grupe:

- Logovi koji prate stanje, procese i rad uređaja – Sistemski logovi
- Logovi koji prate aktivnost krajnjih korisnika – *Access* logovi

Logovi koji prate stanje, procese i rad uređaja zapisuju poruke o radu pojedinačnih komponenti *firewall* uređaja. Postoji veliki broj ovakvih logova i oni su korisni u situacijama kada treba istražiti određene probleme koji se javljaju u radu samog uređaja. Praksa AMRES-a je da sistemske logove čuva na samom *firewall* uređaju. Sistemskim logovima se može pristupiti preko web interfejsa *firewall* uređaja. Logovi koji prate stanje i rad uređaja su konfigurisani da sadrže informacije za jedan celi dan. Na uređaju se čuva po 10 fajlova svakog sistemskog loga, odnosno osoblje AMRES-a ima u svakom trenutku poslednjih 10 dana log informacija o radu komponenti samog uređaja. Nakon toga sistemski logovi se brišu kako se ne bi opterećivala memorija uređaja. Dosadašnja praksa je pokazala da nema potrebe duže čuvati ove logove budući da se oni pregledaju prilikom pojave nekog problema a problemi se rešavaju u najkraćem mogućem roku.

Logovi koji prate aktivnosti krajnjih korisnika beleže svaku web transakciju korisnika AMRES mreže ka Internetu. Ovi logovi se nazivaju *Access* logovi i baziraju se na formi sličnoj *Squid* logovima. *Access* logovi čuvaju informacije o web transakciji do 7 OSI sloja što predstavlja vrlo korisnu informaciju za eventualnu forenzičku analizu. U ove logove se zapisuju sledeće informacije o web transakciji:

- Tačno vreme transakcije (*Unix time*)
- Trajanje transakcije
- IP adresa krajnjeg korisnika
- Rezultat upita u keš memoriju uređaja
- Odgovor udaljenog servera
- Veličina prenetih podataka
- HTTP metoda
- URL koji je krajnji korisnik zahtevao
- MIME tip
- Institucija/mreža kojoj korisnik pripada
- *Access* polisa na *firewall* uređaju koja je obradila transakciju
- Web reputacija udaljenog servera
- Informacije o eventualnoj pojavi *malware*-a
- Da li je web transakcija bila uspešna a ako nije koji je razlog blokade

*Access* logovi se mogu dodatno prilagoditi potrebama organizacije dodavanjem dodatnih polja na kraj log unosa. AMRES u Access logove dodaje dva polja: „*X Forwarded For*“ polje i tačno vreme transakcije u formatu

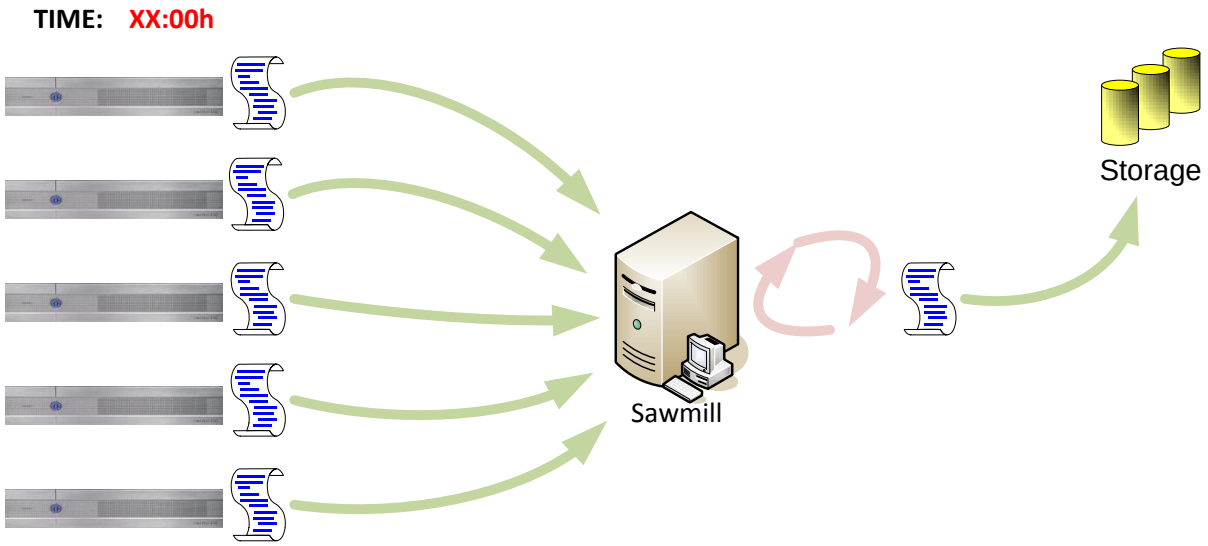
*HH:MM:SS*. „*X Forwarded For*“ informacija je pogodna budući da neke institucije članice imaju svoje proksi servere pa se pomoću ovog polja mogu detektovati klijenti koji se kriju iza proksi servera svoje krajnje institucije. Tačno vreme transakcije u formatu *HH:MM:SS* je prigodno u situacijama kada se vrši analiza log fajla jer je lakše tako pratiti transakcije nego na osnovu *Unix epoch* vremena.

Budući da se zapisuju sve web transakcije koje prolaze kroz uređaj, veličina *Access* log fajlova je veoma velika pa je nepraktično čuvati ih na samom *firewall* uređaju. U AMRES mreži se *Access* logovi prebacuju sa *firewall* uređaja na poseban server za obradu a potom na udaljeni server za skladištenje. Jedan log fajl može sadržati informacije o proizvoljnom vremenskom intervalu – pola sata, jedan ili više sati, dan ili više dana. Praksa u AMRES mreži je da *Access* log fajl sadrži jedan sat log informacija. Procedura formiranja logova ima nekoliko koraka. Na početku svakog sata, *firewall* uređaj kreira novi log fajl i počinje da upisuje informacije o web transakcijama. Kada istekne jedan sat *firewall* uređaj zatvara fajl i prebacuje ga na server za obradu. Prebacivanje na server za obradu se može vršiti nekom od sledećih metoda:

- SCP (*Secure Copy Protocol*)
- FTP (*File Transfer Protocol*)
- *Syslog push* metodom

Log fajl se prenosi preko OOB mreže što uvodi sigurnost u čitav proces. U početku, log fajlovi su bili prenošeni SCP metodom ali se povremeno dešavalo da *firewall* uređaj i server za obradu logova ne mogu da uspostave SCP konekciju. Vremenom se odustalo od takvog prenosa i sada se koristi FTP metod prenosa.

U samom prenosu i operacijama sa logovima javljaju se dva problema. Prvi problem je što svaki *firewall* uređaj formira svoj log fajl za prethodnih sat vremena. Tokom jednog sata rada celokupnog *firewall* sistema, na server za obradu logova (Sawmill) se prebaci 5 posebnih log fajlova, odnosno sa svakog *firewall* uređaja po jedan log fajl. Pregled, analiza i skladištenje log informacija za jedan sat rada *firewall* sistema je stoga veoma neefikasno. Zato se na serveru za čuvanje log fajlova, svakog sata pokreće skripta koja spaja svih 5 log fajlova u jedan log fajl koji sadrži informacije o svim transakcijama koje su prošle kroz *firewall* sistem u poslednjih sat vremena. Na slici 10 je prikazana procedura skladištenja *Access* logova.




*Slika 20 – Prikupljanje, analiza i skladištenje logova u AMRES mreži.*

Jedinstveni jednosatni log fajl dobija ime u vremenskom formatu *YYYY-MM-DD-HH*, pri čemu *HH* predstavlja sat u 24-časovnom formatu kada je fajl kreiran. U okviru jedinstvenog log fajla se sve transakcije sortiraju po

vremenu nastanka čime se postiže lakša preglednost i analiza log informacija. Veličina jedinstvenog jednosatnog *Access* log fajla je u rasponu od 200MB do 3GB u zavisnosti od doba dana. Skladištenje log fajlova u originalnom obliku je veoma problematično sa stanovišta raspoloživog memorijskog prostora. Iz tog razloga se svi log fajlovi kompresuju i čuvaju na udaljenom serveru za skladištenje (*storage server*). Kompresovani *Access* log fajlovi se svode na veličinu od 50 do 500MB čime se ostvaruje znatna ušteda memorijskog prostora. Jedan mesec log informacija o aktivnostima korisnika u kompresovanom formatu zauzima od 100 do 200GB memorijskog prostora dok je na godišnjem nivou neophodno oko 1.5TB memorijskog prostora. Ukoliko se ukaže potreba za analizom web saobraćaja od pre par meseci, lako se pregledom kompresovanih log fajlova mogu naći jednosatni log fajlovi od interesa.

Drugi problem prikupljanja i skladištenja logova predstavlja sistem kreiranja logova na *firewall* uređajima. Kreiranje log fajla i početak upisa log informacija u fajl se mora pokrenuti ručno na samom *firewall* uređaju. Tada se može izabrati opcija nakon koliko vremena će se postojeći log fajl zatvoriti a kreirati novi (30 min, jedan ili više sati). Nakon toga je proces automatizovan, odnosno nakon definisanog vremenskog intervala postojeći log fajl se zatvara i šalje na server a novi log fajl se kreira i započinje upis log informacija. Dakle, veoma je važan prvi trenutak definisanja log konfiguracije. Tu dolazi do problema sinhronizacije kreiranja log fajlova na svih 5 *firewall* uređaja jer je praktično nemoguće u istom trenutku ručno podesiti *Access* log konfiguraciju na svim *firewall* uređajima. Efikasnije rešenje bi bilo kada bi postojala opcija u log konfiguraciji koja omogućava kreiranje novog log fajla u tačno određeno vreme, npr. svakog sata u 0. minutu. Nažalost *firewall* uređaji nemaju ovu opciju pa je neophodno paralelno podešavati *Access* log konfiguraciju na svim *firewall* uređajima u željeno vreme. Posebnu opreznost zahteva i činjenica da bilo koja promena u konfiguraciji *Access* loga dovodi do automatskog kreiranja novog fajla. Iz ovog razloga se u AMRES mreži vodi računa da se sve promene u *Access* log konfiguraciji rade paralelno na svim *firewall* uređajima tačno u 0. minutu nekog sata.

Za potrebe analize saobraćaja i vođenja web statistike u akademskoj mreži nabavljena je aplikacija „*Sawmill for Ironport 7.3.3*“ koja se nalazi na serveru za obradu log fajlova. Svi jednosatni *Access* logovi se čuvaju na serveru u toku dana. Kada u ponoć pristigne i poslednji log fajl za posmatrani dan, *Sawmill* aplikacija započinje čitanje svih log fajlova iz posmatranog dana i formira svoju bazu podataka o web transakcijama. Nakon što *Sawmill* aplikacija pročita sve log fajlove, oni se kompresuju i skladište na udaljeni server za skladištenje na kom se čuvaju 12 meseci. Baza *Sawmill* aplikacije sadrži parsirane log informacije iz *Access* log fajlova *firewall* uređaja. Na osnovu informacija iz baze, Sawmill kreira nekoliko predefinsanih izveštaja koji pružaju opštu sliku o količini web saobraćaja, trendovima u mrežama institucija, obrascima ponašanja krajnjih korisnika i potencijalnim sigurnosnim pretnjama kojima su krajnji korisnici izloženi. Na osnovu ovih izveštaja, mogu se locirati *malware*-om zaraženi računari ili web serveri koji predstavljaju sigurnosnu pretnju po korisnike AMRES mreže. U *Sawmill* aplikaciji je moguće vršiti i upite u bazu aplikacije kako bi se pregledala određena transakcija od interesa. Baza *Sawmill* aplikacije čuva informacije o aktivnostima korisnika u prethodne dve nedelje a moguće je i snimanje predefinisanih izveštaja u PDF formatu za skladištenje i kasnije korišćenje u izveštajima o radu servisa i mreže. Na osnovu statističke analize log informacija mogu se izvesti zaključci o efektima postavljenih *firewall* parametara.

# 9 Monitoring IronPort *firewall* sistema

Najveći deo web saobraćaja AMRES mreže prolazi kroz IronPort *firewall* sistem i veoma je bitno da sistem funkcioniše sa visokom pouzdanošću. Praćenje radnih parametara *firewall* uređaja u realnom vremenu je jedan od najvažnijih zadataka AMRES osoblja. Web interfejs svakog pojedinačnog *firewall* uređaja sadrži sekciju „*Reporting*“ koja daje radne parametre uređaja, statističke podatke o korisnicima, web sajtovima, *malware* softverima i slično. Prikazuju se i podaci o procesorskoj opterećenosti uređaja, zauzetosti RAM memorije i zauzetosti memorijskog prostora za čuvanje log fajlova. U pomenutoj sekciji se može pronaći još i prosečan mrežni protok, prosečno vreme odziva uređaja i ukupan broj trenutnih konekcija na uređaju. Aktivno praćenje rada celokupnog *firewall* sistema zahteva da se osoblje AMRES-a povezuje na svaki pojedinačni uređaj i paralelno prati „*Reporting*“ sekcije. Ovakvo rešenje je krajnje nepraktično jer ne pruža uvid u radne parametre svih *firewall* uređaja na jednom mestu. AMRES je zbog toga odlučio da integriše praćenje rada *firewall* sistema u sopstveni sistem za praćenje i nadgledanje mrežnih uređaja – NetIIS.

NetIIS je sistem za nadgledanje računarske mreže koji je razvijen u Računarskom centru Univerziteta u Beogradu. NetIIS aktivno prati rad elemenata računarske mreže kao što su ruteri, svičevi, serveri, veze između uređaja i slično. Sistem se bazira na korišćenju SNMP (*Simple Network Management Protocol*) protokola kako bi prikupio podatke o radu mrežnih uređaja i stanja na linkovima u mreži. AMRES osoblje u NetIIS-u aktivno prati performanse celokupne akademske mreže i rad pojedinačnih servisa. Svaki servis u akademskoj mreži ima posebnu sekciju u NetIIS-u u kojoj se prati rad servisa u realnom vremenu. Integracija monitoringa *firewall* sistema u NetIIS omogućava pregled svih radnih parametara *firewall* uređaja na jednom mestu. Praktično, AMRES osoblje na jednoj Web stranici može pratiti rad svih *firewall* uređaja u realnom vremenu i na vreme reagovati u slučaju da radni parametri *firewall* sistema nisu zadovoljavajući.

IronPort *firewall* uređaji podržavaju SNMP protokol verzije 1,2 i 3 a za potrebe monitoringa u okviru AMRES-a se koristi SNMP v2. SNMP poruke se razmenjuju preko P produkcionog interfejsa *firewall* uređaja. NetIIS sam generiše alarme na osnovu rezultata SNMP zahteva i optimalnih graničnih vrednosti koje su podešene u NetIIS-u.

Na slici 11 prikazana je sekcija u NetIIS sistemu koja aktivno prati parametre jednog *firewall* uređaja. Za svaki *firewall* uređaj se prate sledeći radni parametri:

- Status i trenutni mrežni protok na produkcionom P interfejsu
- Status i trenutni mrežni protok na menadžment M interfejsu
- Procesorska opterećenost i zauzeće RAM memorije na uređaju
- Prosečan broj TCP konekcija u poslednjem minutu
- Prosečan broj aktivnih TCP konekcija u poslednjem minutu
- Prosečan broj pasivnih TCP konekcija u poslednjem minutu
- Ispravnost proksiranja saobraćaja i vreme odziva

- Ping monitor

| proxy2.amres.ac.rs | |
|---|---|
| P&T@Cat2960-skole.Gi0/26 [IW2-D1] | Up / Up , 184.14 Mbps / 165.90 Mbps |
| P&T@proxy2.amres.ac.rs.P1 [P1] | Up / Up , 155.15 Mbps / 171.84 Mbps |
| P&T@proxy2.amres.ac.rs.Management [Management] | Up / Up , 1.63 Kbps / 11.33 Kbps |
| CPU & Mem Monitor@proxy2.amres.ac.rs | 16 % / 79 % |
| TCP Connections@proxy2.amres.ac.rs | 11856 |
| TCP Active Opens@proxy2.amres.ac.rs | 111.01 |
| TCP Passive Opens@proxy2.amres.ac.rs | 267.97 |
| facebook.com monitor@proxy2.amres.ac.rs | HTTP OK: HTTP/1.1 302 Found - 322 bytes in 0.207 second response time / time=0.206528s;;;0.000000 size=322B;;;0 / 0 (OK) / 1 / 0.206528 |
| Ping monitor@proxy2.amres.ac.rs | 0.33 ms / 0.49 ms / 0.37 ms / 10 / 10 / 0 % |

*Slika 11 – Radni parametri jednog firewall uređaja*

Za potrebe praćenja *firewall* uređaja AMRES koristi samo dva OID identifikatora preuzeta iz zvaničnog Cisco MIB modela:

- Procesorska opterećenost uređaja (IronPort CPU)
- Zauzeće RAM memorije na uređaju (IronPort Memory)

Ovi OID identifikatori su smešteni u jedan SNMP monitor „CPU & Mem Monitor“. TCP OID identifikatori su preuzeti iz standardnog TCP MIB modela koji podržavaju svi vendori na tržištu.

Ispitivanje ispravnog funkcionisanja *firewall* uređaja je ključno u nadgledanju sistema. Sajt-monitor ispituje proksiranje saobraćaja na *firewall* uređaju (slika 12). Sajt-monitor u NetIIS sistemu se implementira pomoću *Nagios* dodatka (*plug-in*) „*check_http*“. Na svakom *firewall* uređaju se ispituje proksiranje ka bar dva web sajta na Internetu. Ispitivanje različitih web sajtova omogućava AMRES osoblju da sa sigurnošću utvrdi da se eventualni problem proksiranja javlja na *firewall* uređaju, a ne na samom web sajtu koji se proverava. Ključno je proveriti da li krajnji korisnici preko *firewall* sistema mogu pristupiti web sajtovima na Internetu i koliko je vreme odziva sistema. Na slici 12 se može videti jedna provera proksiranja *firewall* uređaja gde se uspešno može pristupiti sajtu *facebook.com* i gde je vreme odziva sistema 0.207 sekundi što je prilično dobar rezultat. Ukoliko bi proksiranje bilo neuspešno to bi značilo da verovatno postoji problem sa funkcionisanjem *firewall* uređaja ili sa AMRES mrežom. Vreme odziva se pažljivo prati jer može ukazivati na eventualna kašnjenja u AMRES mreži ili na problem proksi funkcionalnosti *firewall* uređaja.

| | |
|---|---|
| facebook.com monitor@proxy2.amres.ac.rs | HTTP OK: HTTP/1.1 302 Found - 322 bytes in 0.207 second response time / time=0.206528s;;;0.000000 size=322B;;;0 / 0 (OK) / 1 / 0.206528 |

*Slika 12 – Sajt monitor koji ispituje ispravnost proksiranja na firewall uređaju*

Pored aktivnog monitoringa *firewall* uređaja u AMRES-u se sprovodi i pasivni monitoring. *Firewall* uređaji imaju mogućnost slanja alarmnih poruka u slučaju da neka komponenta sistema ne funkcioniše ispravno. Alarmne poruke su *e-mail* poruke koje sadrže obaveštenja o radu specifičnih funkcija *firewall* uređaja. Alarmne poruke mogu biti:

- Sistemske – prenose informacije o funkcionalnosti samog *firewall* uređaja
- Hardverske – prenose informacije o radu hardverskih komponenti
- Poruke o ažuriranju softvera – prenose informacije o ažiriranju pojedinih delova softvera
- Poruke o web proksiranju – prenose informacije o proksi funkcionalnosti uređaja

Pored različitih tipova poruka, svaka poruka se obeležava merom kritičnosti. Razlikuju se poruke koje nose samo informaciju o događaju, poruke koje nose upozorenje na rad uređaja i poruke koje ukazuju na kritične

događaje koji ugrožavaju funkcionalnost uređaja. U cilju adekvatnog praćenja rada *firewall* sistema formirana je *mailing* lista na koju *firewall* uređaji šalju sve alarmne poruke. Članovi mailing liste su inženjeri AMRES-a koji održavaju rad *firewall* sistema. Putem alarmnih poruka, AMRES osoblje se obaveštava o problemu na uređaju istog trenutka kada se problem dogodi. Ranija iskustva u radu *firewall* uređaja su pokazala da su ove poruke izuzetno efikasne u situacijama kada dođe do otkaza pojedinih hardverskih komponenti ili prilikom neuspeha prenosa log informacija na udaljeni server. Pravovremenim obaveštavanjem o problemu, AMRES osoblje je bilo u mogućnosti da brzo deluje i povrati punu ispravnost rada *firewall* sistema.

# 10 Zaključak

Iako je IronPort *firewall* sigurnosni sistem dizajniran tako da zadovolji veći broj potreba zatvorenih organizacija kao što su banke i preduzeća čiji profil posla zahteva visok nivo sigurnosti, pojedine komponente sistema se mogu veoma dobro iskoristiti i u drugim organizacijama gde nivo sigurnosti organizacije i nije toliko bitan, već je akcenat na zaštiti pojedinačnih krajnjih korisnika. Osnovne škole, srednje škole, fakulteti i biblioteke predstavljaju primer ovakvih organizacija. Trenutni trendovi razvoja tehnologije pored inovativnosti donose i pojedine loše aspekte kao što su krađa indentiteta, širenje destruktivnih virusa i zloupotrebe anonimnosti koje internet pruža. Veliki broj parametara ukazuju na to da je potrebno više obratiti pažnju na sigurnost korisnika Interneta, a naručito mlađe populacije. Ovakav sigurnosni sistem ima veliku primenu u zaštiti krajnjih korisnika akademskih institucija i očekuje se njegova sve veća upotreba u skorijoj budućnosti.