



AMPEC

Академска мрежа Србије



Упутство за коришћење услуге веб-филтрирања

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0	30.07.2015.	МК	Прва верзија овог документа

Садржај

1	УВОД	4
2	ПОВЕЗИВАЊЕ НА <i>IRONPORT</i> MANAGEMENT APPLIANCE	6
3	УРЕЂИВАЊЕ <i>ACCESS</i> ПОЛИСА	7
3.1	УРЕЂИВАЊЕ ПРИХВАТЉИВИХ ПРОТОКОЛА И ПОРТОВА	9
3.2	УРЕЂИВАЊЕ ПРИХВАТЉИВИХ URL КАТЕГОРИЈА	10
3.3	УРЕЂИВАЊЕ ПРИХВАТЉИВИХ АПЛИКАЦИЈА	13
3.4	УРЕЂИВАЊЕ ПРИХВАТЉИВИХ ОБЈЕКТА	16
3.5	УРЕЂИВАЊЕ СКЕНИРАЊА САОБРАЋАЈА	18
4	УРЕЂИВАЊЕ <i>CUSTOM URL</i> КАТЕГОРИЈА	20
5	СНИМАЊЕ КОНФИГУРАЦИЈЕ	23
6	РЕШАВАЊЕ ПРИТУЖБИ КОРИСНИКА	26

1 Увод

AMRES услуга веб филтрирања се састоји од 5 прокси уређаја (*Cisco Ironport S670*) и једног уређаја за централизовано управљање (*Cisco Ironport M160*). За прослеђивање саобраћаја користе се прокси уређаји на следећим IP адресама:

- ❖ Прокси 1 – 147.91.1.41
- ❖ Прокси 2 – 147.91.1.42
- ❖ Прокси 3 – 147.91.1.43
- ❖ Прокси 4 – 147.91.1.44
- ❖ Прокси 5 – 147.91.1.45

Уређај за централизовано управљање служи за конфигурисање правила према којима *Ironport* прокси уређаји процесирају саобраћај од корисника ка Интернету. Уређај за централизовано управљање се налази на следећој IP адреси:

- ❖ *Cisco Ironport Management Appliance* - 147.91.1.38

AMRES услуга веб филтрирања је замишљена као својеврсно *Cloud* решење где администратори институција могу да приступају уређају за централизовано управљање и на њему дефинишу садржаје којима корисници могу да приступе. На овај начин, свака институција има својеврсну *Access* полису за своје кориснике у којој може забранити следеће садржаје:

- ❖ Коришћење одређеног протокола (*HTTP, HTTPS, FTP, FTP over HTTP*)
- ❖ Коришћење одређеног порта за потребе *HTTP* саобраћаја
- ❖ Приступ веб сајтовима одређене категорије (*Gambling, Social Networks, Adult* итд)
- ❖ Приступ експлицитно наведеном веб сајту (нпр. *example.com*)
- ❖ Коришћење одређене апликације (односи се на веб-апликације, нпр. *Facebook Chat*)
- ❖ Пренос одређених типова фајлова (нпр. *flash, streaming media, PDF, ActiveX plugin*, одређене *MIME* категорије итд)
- ❖ Пренос фајлова чија величина превазилази неку дефинисану границу

У оквиру *Ironport* уређаја за централизовано управљање дефинисана је следећа структура:

- ❖ *Access* полиса – одређује правила приступа Интернету за одређену групу корисника (за одређену институцију)
- ❖ *Custom URL* категорија – листа веб-сајтова или сервера за које се може поставити одређена акција *Ironport* система

Услуга веб-филтрирања подразумева следећа правила коришћења:

1. Свака институција има право на једну *Access* полису. Институција може да поседује и више *Access* полиса уколико жели да примењује различита правила на своје кориснике (нпр. да раздвоји професоре и студенте). Уколико институција жели да има више *Access* полиса неопходно је да образложи разлоге због којих то чини.
2. Свака институција има право на једну *Custom URL* категорију у коју може да убацује *URL* адресе сајтова које жели да експлицитно забрани

У овом упутству биће детаљно објашњено како администратор институције може да креира и одржава политику прихватљивог садржаја за своје кориснике. Администратор креира политику прихватљивог садржаја тако што уређује *Access* Полису и *Custom URL* категорију своје институције. Правила која тамо дефинише важе само за кориснике његове институције. Даље, биће објашњен и принцип притужби које корисници шаљу администраторима.

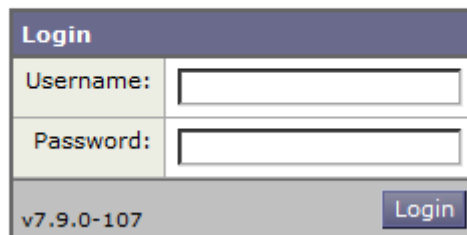
2 Повезивање на *Ironport Management Appliance*

Сва подешавања у услузи веб-филтрирања се врше на *Ironport Management* уређају. Администратор институције се повезује на *Ironport Management* уређај тако што у свој Интернет прегледач уписује *URL* адресу уређаја:

➤ <https://ironport.amres.ac.rs>

На екрану ће се приказати **Log-in** страница

Welcome



Слика 2-1

Неопходно је да администратор унесе своје корисничко име и лозинку коју има у LDAP бази за AMRES администраторе. Након успешне аутентификације, администратор ће бити пребачен на **Account Privileges** страницу.

Web Policy Configuration

Configuration Master 7.5

- Access Policies: 1
- Custom URL Categories: 1

Publish Configurations

Configure policies for web administration.

Слика 2.2

На овој страници администратор има увид колико *Access* полиса и *Custom URL* категорија може да мења. По правилу, администратор ће имати привилегију да мења једну или више *Access* полиса и само једну *Custom URL* категорију.

Уколико администратор жели да уређује *Access* полису неопходно је да кликне опцију **Access Policies**.

Уколико администратор жели да уређује *Custom URL* категорију неопходно је да кликне на опцију **Custom URL Categories**.

3 Уређивање Access полиса

На страници **Access Policies** администратор може видети Access полисе које се тичу његове институције. У општем случају, администратор ће имати само једну Access полису, али може их имати и више. У Access полиси постоји 5 секција које уређују политику прихватљивог садржаја:

- ✦ **Protocols And User Agents** – дефинишу се прихватљиви протоколи, портови за комуникацију и дозвољени Интернет прегледачи
- ✦ **URL filtering** – дефинишу се прихватљиве URL категорије садржаја
- ✦ **Applications** – дефинишу се прихватљиве веб-апликације
- ✦ **Objects** – дефинишу се прихватљиви објекти (типови фајлова, типови саобраћаја) и максимална величина објеката који се могу преузети
- ✦ **Web Reputation and Anti-Malware Filtering** – дефинише када је неопходно скенирати саобраћај на разне типове малициозног садржаја

Уколико администратор жели да уређује прихватљиве протоколе и портове неопходно је да кликне на поље испод секције **Protocols and User Agents** (1).

Access Policies

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)

Слика 3-1

Уколико администратор жели да уређује прихватљиве URL категорије неопходно је да кликне на поље испод секције **URL filtering** (2).

Access Policies

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)

Слика 3-2

Уколико администратор жели да уређује прихватљиве веб-апликације неопходно је да кликне на поље испод секције **Applications** (3).

Access Policies

Policies						
View: All Policies 3						
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)

Слика 3-3

Уколико администратор жели да уређује прихватљиве објекте неопходне је да кликне на поље испод секције **Objects** (4).

Access Policies

Policies						
View: All Policies 4						
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)

Слика 3-4

Уколико администратор жели да уређује скенирање саобраћаја неопходно је да кликне на поље испод секције **Web Reputation and Anti-Malware Filtering** (5).

Access Policies

Policies						
View: All Policies 5						
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)

Слика 3-5

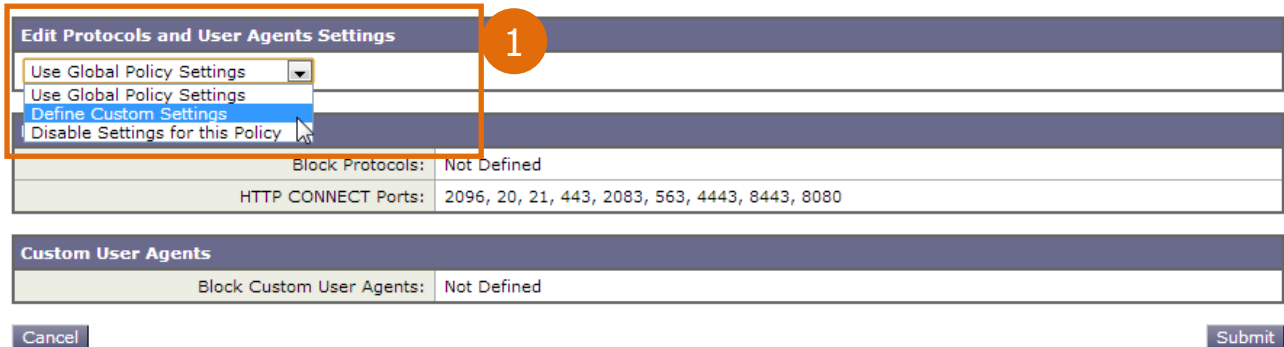
3.1 Уређивање прихватљивих протокола и портова

Уређивање прихватљивих протокола и портова се врши на страници **Protocols and User Agents**. Страница садржи три секције:

- ❖ *Edit Protocols and User Agents Settings*
- ❖ *Protocol Controls*
- ❖ *Custom User Agents*

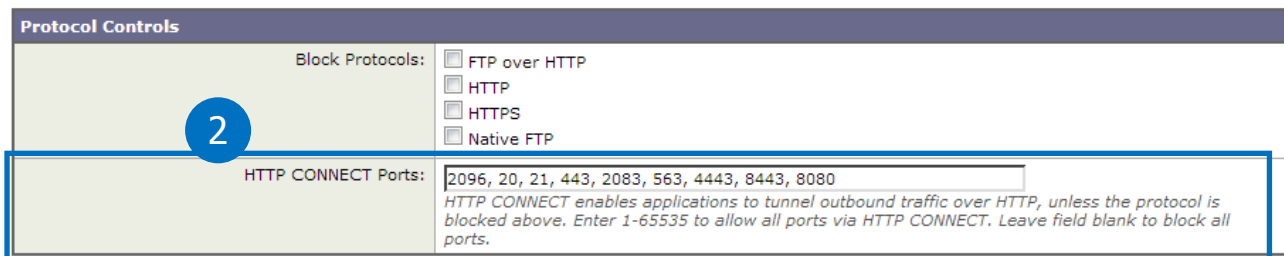
Иницијално, администратор ће на овој страници видети предефинисана подешавања које је поставио AMRES. Уколико администратор жели да промени, односно допуни, посматрану конфигурацију неопходно је да у горњем левом углу у секцији **Edit Protocols and User Agents Settings** (1) из падајућег менија изабере опцију **Define Custom Settings**.

Access Policies: Protocols and User Agents: Polisa Institucije



Слика 3-6

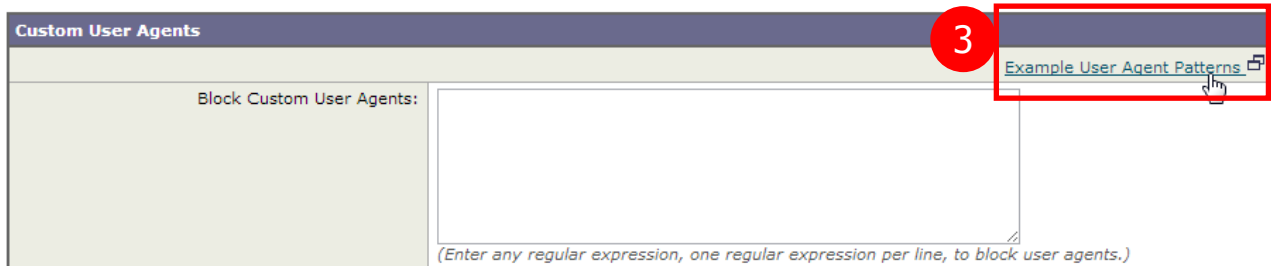
Одабиром ове опције страница се откључава и могуће је унети промене. У секцији **Protocol Controls** (слика 3-7) администратор може блокирати одређени протокол тако што ће штиклирати поље поред имена протокола. У *Ironport* уређајима могуће је блокирати неки од четири протокола: *HTTP*, *HTTPS*, *FTP* или *FTP over HTTP*. Опција **HTTP CONNECT Ports** (2) оставља могућност администратору да упише дозвољене портове. Апликације крајњих корисника потом могу тунеловати свој саобраћај преко *HTTP* протокола употребом ових портова. AMRES је предвидео да дозвољени портови буду 2096, 20, 21, 443, 2083, 563, 4443, 8443 и 8080. Администратори могу мењати ову листу и додавати портове према њиховим потребама.



Слика 3-7

У секцији **Custom User Agents** (слика 3-8) администратор може блокирати употребу одређених Интернет прегледача (*IE*, *Firefox*, *Chrome* и сл.). Да би администратор блокирао одређени Интернет прегледач неопходно је да у поље **Block Custom User Agents** упише одговарајући регуларни израз који одговара неком прегледачу. Пример израза се може добити кликом на опцију **Example User**

Agent Patterns (3) која се налази у горњем десном углу секције. Кликом на ову опцију отвориће се нови прозор у коме се могу видети примери блокирања појединачних Интернет прегледача.



Слика 3-8

Након што корисник комплетира сва подешавања на страници **Protocols and User Agents** је да кликне на дугме **Submit** како би запамтио подешавања.

3.2 Уређивање прихватљивих URL категорија

Уређивање прихватљивих *URL* категорија се врши на страници **URL Categories**. Страница садржи четири секције:

- ❖ *Custom URL Category Filtering*
- ❖ *Predefined URL Category Filtering*
- ❖ *Uncategorized URLs*
- ❖ *Content Filtering*

Category	Use Global Settings	Override Global Settings					Time-Based
		Block	Redirect	Allow (?)	Monitor	Warn (?)	
Eksplicitno puštени сајтови	Select all	Select all	Select all	Select all	Select all	Select all	(Unavailable)
CabFiles	Select all						
Institucije EXP zabranjeni сајтови		Select all					

Слика 3-9

Прва секција, **Custom URL Category Filtering** (слика 3-9) приказује које *Custom URL* категорије се користе у *Access* полиси институције. По правилу, овде увек стоје три *Custom URL* категорије и то:

- ❖ Експлицитно пуштени сајтови (AMRES предефинисани)
- ❖ *CabFiles* (AMRES предефинисани)
- ❖ <име институције> EXP забрањени сајтови

У овој секцији администратори не би требало ништа да мењају јер свака *Custom URL* категорија има своју функцију. **Експлицитно пуштени сајтови** садрже листу сајтова које је Cisco погрешно класификовао. Да би био омогућен приступ оваквим сајтовима AMRES је направио посебну *URL* категорију у коју смешта погрешно класификоване сајтове. Уколико администратор у току свог рада пронађе још неке странице које су погрешно класификоване и забрањене неопходно је да пријави странице на helpdesk@amres.ac.rs. AMRES ће потом убацити те странице у *URL* категорију **Експлицитно пуштени сајтови**.

CabFiles садржи *URL* које *Windows* користи за ажурирање оперативног система. AMRES експлицитно дозвољава приступ овим *URL* адресама. Категорије **Експлицитно пуштени сајтови** и **CabFiles** уређује AMRES и корисник нема привилегију да мења ове категорије. По правилу саобраћај за ове категорије се експлицитно допушта и корисник то не сме да мења у секцији *Custom URL Category filtering*.

Последња *Custom URL* категорија у овој секцији је **<име институције> EXP забрањени сајтови**. Ову *Custom URL* категорију уређује администратор институције. Уређивање ове категорије се не врши на овом месту већ се овде уређује само понашање *Ironport* уређаја када треба да процесира захтеве ка сајтовима који потпадају под ову *Custom URL* категорију. Према правилима AMRES-а понашање за *Custom URL* категорију **<име институције> EXP забрањени сајтови** увек мора бити **Block** и администратори ово не смеју да мењају!

Category	Use Global Settings	Override Global Settings			
		Block	Monitor	Warn (?)	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)
Adult	<input checked="" type="checkbox"/>				--
Advertisements	<input checked="" type="checkbox"/>				--
Alcohol	<input checked="" type="checkbox"/>				--
Arts	<input checked="" type="checkbox"/>				--
Astrology	<input checked="" type="checkbox"/>				--
Auctions	<input checked="" type="checkbox"/>				--

Слика 3-10

Друга секција, **Predefined URL Category Filtering** (слика 3-10) приказује које предефинисане *URL* категорије саобраћаја су дозвољене у *Access* полиси институције. На основу садржаја *Ironport* смешта велики број сајтова у предефинисане *URL* категорије. Тако се рецимо у категорији **Social Networking** налазе сви сајтови који се тичу социјалних мрежа (*Facebook*, *MySpace*, *Twitter* и сл.). На *Ironport* систему тренутно постоји 78 предефинисаних *URL* категорија. Уколико администратор жели да забрани својим корисницима да приступају социјалним мрежама, неопходно је да кликне на одговарајуће поље (**Block**) у реду **Social Networking** (слика 3-11) (1).

Category	Use Global Settings	Override Global Settings			
		Block	Monitor	Warn (?)	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)
Safe For Kids	<input checked="" type="checkbox"/>				--
Science and Technology	<input checked="" type="checkbox"/>				--
Search Engines and Portals	<input checked="" type="checkbox"/>				--
Sex Education	<input checked="" type="checkbox"/>				--
Shopping	<input checked="" type="checkbox"/>				--
Social Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			--
Social Science	<input checked="" type="checkbox"/>				--

Слика 3-11

На сличан начин институција може забранити одређену категорију садржаја за своје кориснике. Треба напоменути да ни AMRES ни администратори не могу да уређују садржај *URL* категорија већ то ради искључиво произвођач *Ironport* опреме – компанија *Cisco*. AMRES и администратори могу само забранити одређени садржај у својој мрежи и надати се да је *Cisco* обухватио све сајтове у овој предефинисаној *URL* категорији. Уколико администратор утврди да неки сајт није обухваћен предефинисаном *URL* категоријом која се блокира, онда може посматрани сајт поставити у своју *Custom URL* категорију **<име институције> EXP забрањени сајтови** која се по правилу блокира.

Администратор може поставити три типа понашања *Ironport* уређаја када корисници приступају одређеној УРЛ категорији:

- Block
- Monitor

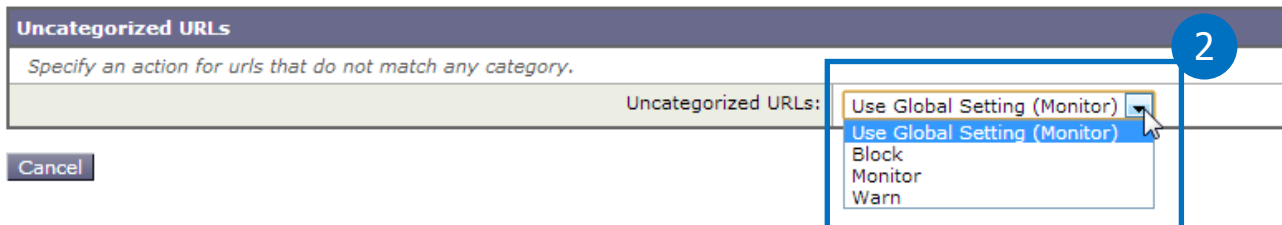
❖ Warn

Уколико администратор постави акцију **Block**, *Ironport* уређаји ће блокирати посматрану *URL* категорију. Уколико администратор постави акцију **Monitor**, *Ironport* уређаји ће допустити приступ посматраној *URL* категорији али ће саобраћај бити скениран како би се спречио евентуални пренос малициозног софтвера. Уколико администратор постави акцију **Warn**, *Ironport* уређаји ће корисницима приказати страницу упозорења где корисници морају потврдити да желе да виде тражени садржај. Уколико корисници дају потврду, *Ironport* уређаји ће их пустити да приступе траженом садржају. Страница упозорења ће излазити на сваких сат времена.

На почетку рада са предефинисаним *URL* категоријама администратор може видети да ће бити селектоване све *URL* категорије у колони *Use Global Settings*. Ово практично значи да се за посматрану *URL* категорију користи правило које је поставио AMRES. AMRES блокира 6 предефинисаних *URL* категорија:

- ❖ *Child Abuse Content*
- ❖ *Filter Avoidance*
- ❖ *Gamblin*
- ❖ *Hate Speech*
- ❖ *Illegal Drugs*
- ❖ *Pornography*

Администратори не смеју својим корисницима дозволити категорије које је блокирао AMRES, али могу додатно блокирати неке категорије које AMRES није блокирао. На крају рада са предефинисаним *URL* категоријама неопходно је кликнути на дугме **Submit** како би се сачувала подешавања. Дугме **Submit** се налази одмах испод посматране секције.

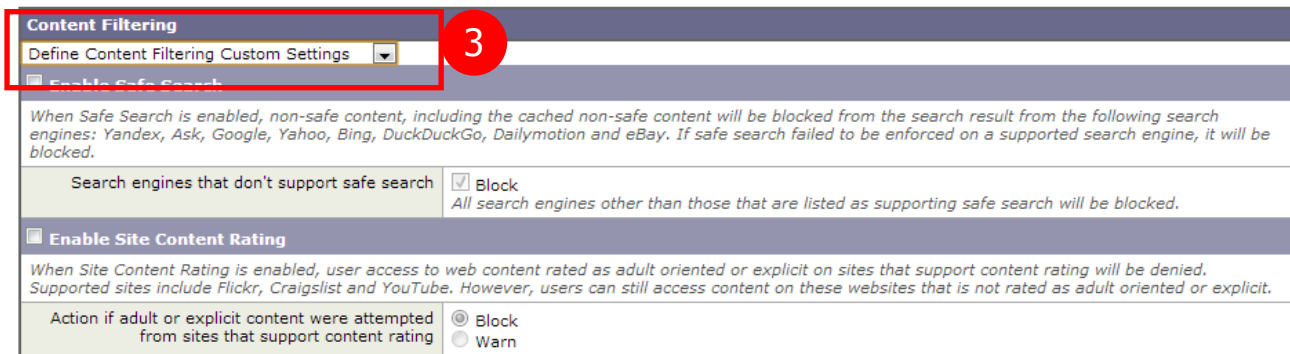


Слика 3-12

Трећа секција **Uncategorized URLs** уређује понашање *Ironport* уређаја када корисници захтевају неку веб-страницу која није категоризована (слика 3-12). Корисник овде може поставити 4 акције:

- ❖ *Use Global Setting (Monitor)* – предефинисана опција
- ❖ *Block*
- ❖ *Monitor*
- ❖ *Warn*

Акције су потпуно идентичне као и у претходној секцији. С обзиром да се релативно често догађа да корисници приступају страницама које *Cisco Ironport* није успео да категоризује, AMRES препоручује администраторима да не мењају предефинисано подешавање – **Monitor**. Уколико администратори ипак одлуче да промене подешавање, неопходно је да из падајуће листе (2) (слика 3-12) изабере одговарајућу опцију и кликну на дугме **Submit** како би запамтили подешавање.



Content Filtering

Define Content Filtering Custom Settings 3

Enable Safe Search

When Safe Search is enabled, non-safe content, including the cached non-safe content will be blocked from the search result from the following search engines: Yandex, Ask, Google, Yahoo, Bing, DuckDuckGo, Dailymotion and eBay. If safe search failed to be enforced on a supported search engine, it will be blocked.

Search engines that don't support safe search Block
 All search engines other than those that are listed as supporting safe search will be blocked.

Enable Site Content Rating

When Site Content Rating is enabled, user access to web content rated as adult oriented or explicit on sites that support content rating will be denied. Supported sites include Flickr, Craigslist and YouTube. However, users can still access content on these websites that is not rated as adult oriented or explicit.

Action if adult or explicit content were attempted from sites that support content rating Block
 Warn

Слика 3-13

Последња секција **Content Filtering** уређује понашање *Ironport* уређаја приликом приступа садржају кога је категоризовао неки други популарни сервис (слика 3-13). AMRES не користи ову опцију, међутим администратори је могу укључити у своју *Access* полису. Да би се откључала ова опција неопходно је у падајућој листи одмах испод наслова секције одабрати опцију **Define Content Filtering Custom Settings** (3). Након тога откључавају се две подсекције:

- ❖ *Enable Safe Search*
- ❖ *Enable Site Content Rating*

Кликом на поље у наслову подсекције може се укључити посматрана опција. Уколико администратор укључи опцију **Safe Search** *Ironport* уређаји ће се ослонити на категоризацију следећих претраживача: *Yandex, Ask, Google, Yahoo, Bing, DuckDuckGo, Dailymotion* и *eBay*. Приликом претраге на овим сајтовима, корисницима ће бити блокирани резултати који нису прошли **Safe Search** контролу. Уколико администратори планирају да користе ову опцију AMRES препоручује да се прво информишу на Интернету о **Safe Search** сервису.

Уколико Администратор укључи опцију **Site Content Rating** *Ironport* неће допустити приступ садржају који је оцењен као експлицитан или садржај за одрасле на сајтовима као што су *Flickr, Craigslist* и *Youtube*. Сви други садржаји на овим сајтовима ће бити доступни крајњим корисницима. У овој опцији администратор може потпуно блокирати приступ овим садржајима или подесити да се прво покаже *Ironport* страница упозорења пре него што се допусти приступ проблематичном садржају.

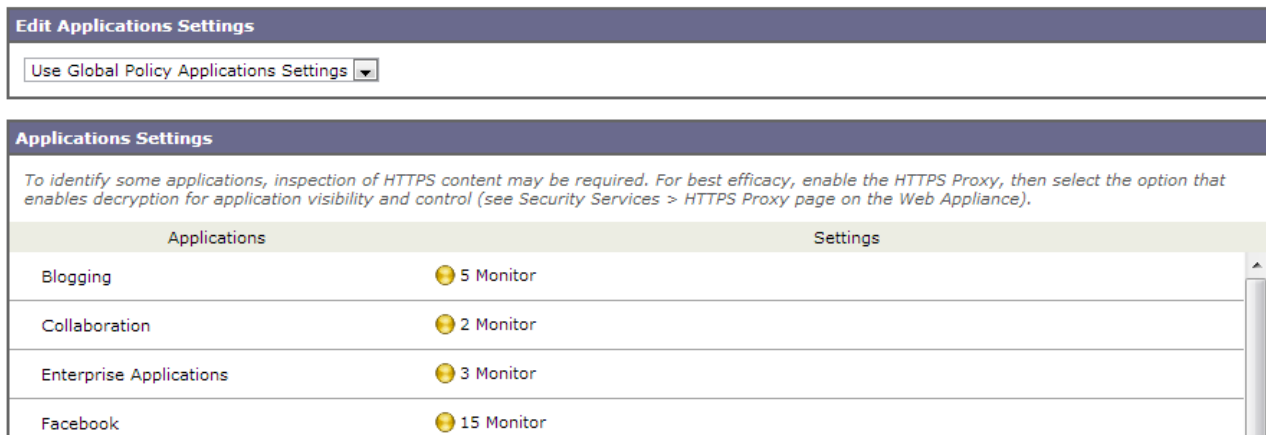
Након измене подешавања на секцији **Content Filtering** неопходно је кликнути на дугме **Submit** које се налази одмах испод секције како би се сачувала начињена подешавања.

3.3 Уређивање прихватљивих апликација

Уређивање прихватљивих веб-апликација се врши на страници **Application Visibility and Control** и састоји се из две секције:

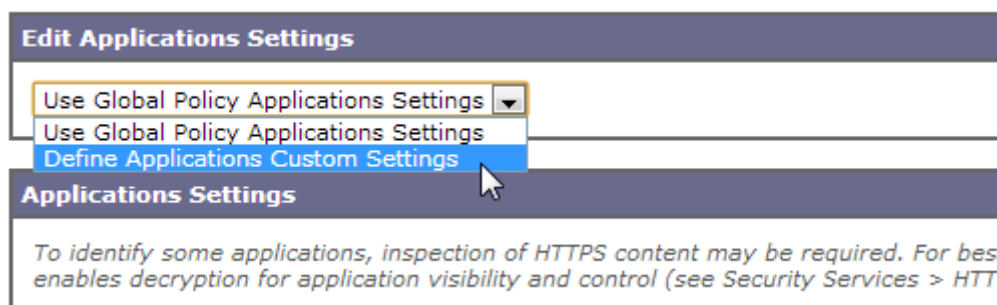
- ❖ *Edit Application Settings*
- ❖ *Application Settings*

Access Policies: Applications Visibility and Control: Polisa Institucije



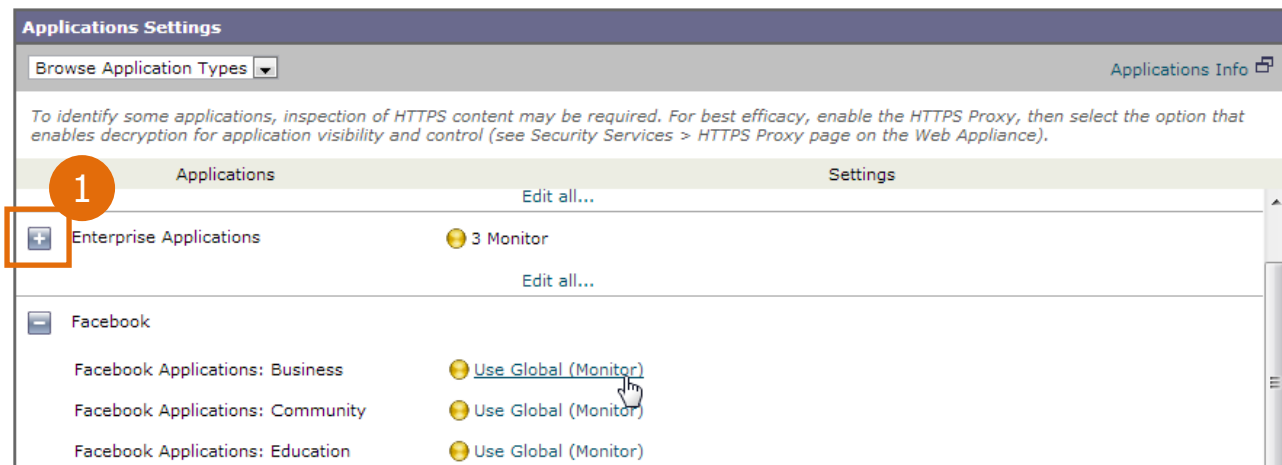
Слика 3-14

AMPEC је као предефинисано понашање *Ironport* уређаја поставио да су све апликације дозвољене и да се прате (*Monitor*) како би се спречио евентуалан трансфер малициозног садржаја. Уколико администратор жели да промени подешавања, неопходно је да у првој секцији **Edit Applications Settings** из падајуће листе изабере опцију **Define Custom Applicatons Settings** (слика 3-15).



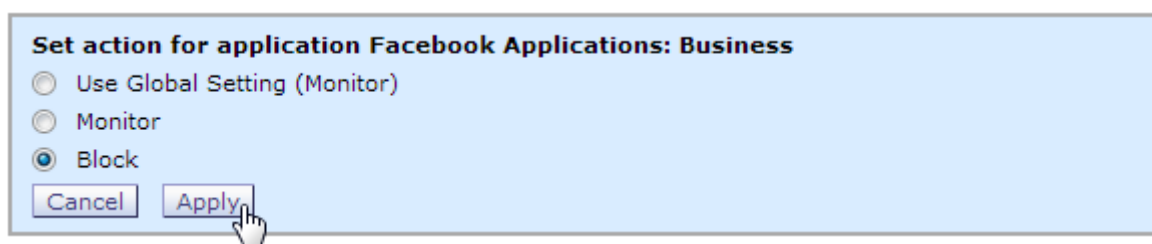
Слика 3-15

Након овога секција **Application Settings** ће се откључати и биће омогућено манипулисање апликацијама. *Ironport* смешта апликације у одређене категорије те се на уређајима може манипулисати са 18 категорија веб-апликација (*Blogging, Collaboration, Facebook* итд.). У оквиру сваке категорије постоји неколико апликација за које администратор може поставити одговарајуће акције. Поред имена сваке категорије (са леве стране) стоји знак "+" (1)(слика 3-18). Кликом на овај знак појављује се падајућа листа са свим апликацијама које припадају посматраној категорији. Иницијално, за сваку апликацију ће бити постављена предефинисана AMPEC акција **Use Global (Monitor)**.



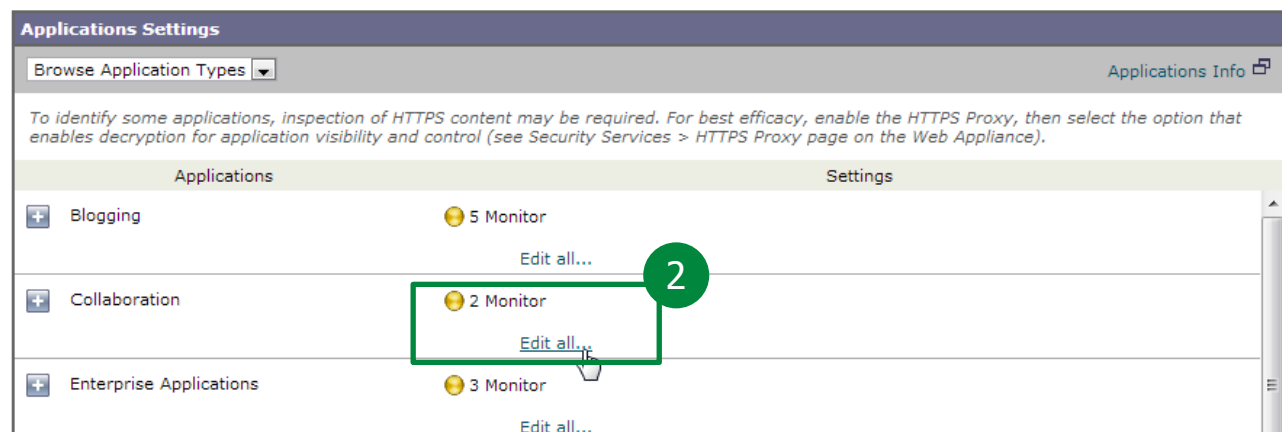
Слика 3-16

Уколико администратор жели да промени постојећу акцију, неопходно је да кликне на опцију која је тренутно постављена (слика 3-16). Након тога отвориће се нова секција у којој ће администратор моћи да постави нову акцију (слика 3-17). Неопходно је да администратор постави нову акцију и кликне на дугме **Apply**.



Слика 3-17

На овај начин администратор може блокирати било коју апликацију у било којој категорији. AMRES препоручује администраторима да истраже све доступне апликације на *Ironport* уређају и тестирају оне апликације које желе да блокирају.



Слика 3-18

Уколико администратор жели да блокира све апликације у одређеној категорији, то може учинити директно кликом на опцију **Edit all...** (2) која се налази испод назива категорије (слика 3-18). На страници ће се отворити нова секција као на слици 3-17.

Након завршетка рада са апликацијама, неопходно је да администратор кликне на дугме **Submit** у дну странице како би са сачувала начињена подешавања.

3.4 Уређивање прихватљивих објеката

Уређивање прихватљивих објеката се врши на страници **Objects** и састоји се из две секције:

- ❖ Edit Object Blocking Settings
- ❖ Custom MIME Types

Edit Objects Blocking Settings	
Use Global Policy Objects Blocking Settings ▾	
Objects Blocking Settings	
Object Size	
HTTP/HTTPS Max Download Size:	No Maximum
FTP Max Download Size:	No Maximum
Block Object Type	
Not Defined	
Custom MIME Types	
Block Custom MIME Types:	Not Defined

Слика 3-19

AMRES је као предефинисано понашање *Ironport* уређаја поставио да је пренос свих објеката дозвољен. Објекти се прате (*Monitor*) како би се спречио евентуалан трансфер малициозног садржаја. Уколико администратор жели да промени подешавања, неопходно је да у првој секцији **Edit Objects Blocking Settings** из падајуће листе изабере опцију **Define Custom Objects Blocking Settings** (слика 3-20).

Edit Objects Blocking Settings	
Use Global Policy Objects Blocking Settings ▾	
Use Global Policy Objects Blocking Settings Define Custom Objects Blocking Settings Disable Object Blocking for this Policy	
Object Size	
HTTP/HTTPS Max Download Size:	No Maximum
FTP Max Download Size:	No Maximum
Block Object Type	
Not Defined	

Слика 3-20

Након овога, секција **Edit Objects Blocking Settings** ће бити откључана и администратор ће моћи да манипулише објектима. У оквиру прве подсекције администратор ће моћи да ограничи максималну величину објеката која се преноси путем *HTTP/HTTPS* или *FTP* саобраћаја. Важно је напоменути да се овде постављена ограничења односе по кориснику. Дакле уколико администратор жели да постави ограничење објекта на *25 MB* за *HTTP/HTTPS* саобраћај, неопходно је да обележи прво „радио-дугме“ и у поље поред упише „25“ (слика 3-21).

Objects Blocking Settings	
Object Size	
HTTP/HTTPS Max Download Size:	<input checked="" type="radio"/> 25 MB <input type="radio"/> No Maximum
FTP Max Download Size:	<input type="radio"/> 0 MB <input checked="" type="radio"/> No Maximum

Слика 3-21

У секцији **Block Object Type** администратор може блокирати одређени тип објекта/фајла. *Ironport* је објекте поделио у 8 категорија (*Archives, Document Types, Executable Code, Installers* итд.). Кликом на одређену категорију отвара се падајући мени у ком се налазе сви типови објекта који су дефинисани за ту категорију. АМРЕС препоручује администраторима да истраже типове објеката на Интернету пре него што потпуно блокирају објекте за своје крајње кориснике. Уколико нпр администратор жели да блокира пренос торент фајлова (*.torrent*) за своје клијенте неопходно је кликнути на категорију **P2P Metafiles** и штиклирати поље поред објекта **BitTorrent Links (.torrent)** (слика 3-22).

Block Object Type	
▶	Archives
▶	Document Types
▶	Executable Code
▶	Installers
▶	Media
▼	P2P Metafiles
<input checked="" type="checkbox"/>	BitTorrent Links (.torrent)
▶	Web Page Content
▶	Miscellaneous

Слика 3-22

Секција **Custom MIME Types** служи да се блокирају одређени објекти према *MIME* типу. АМРЕС препоручује уређивање ове секције само уз претходно детаљно истраживање о *MIME* типовима на Интернету. Да би се блокирао одређени *MIME* тип, неопходно је у поље ове секције уписати израз који одговара одређеном *MIME* типу. Администратор треба сваки нови *MIME* тип да уписује у посебан ред. Као помоћ при раду, администратори могу погледати неке примере уколико кликну на опцију **Object and MIME Type Reference** која се налази у горњем десном углу ове секције (слика 3-23).

Custom MIME Types	
Object and MIME Type Reference	
Block Custom MIME Types:	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div> <p><small>(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries.)</small></p>

Слика 3-23

Након извршених промена на овој страни, неопходно је притиснути дугме **Submit** како би се сачувала начињена подешавања.

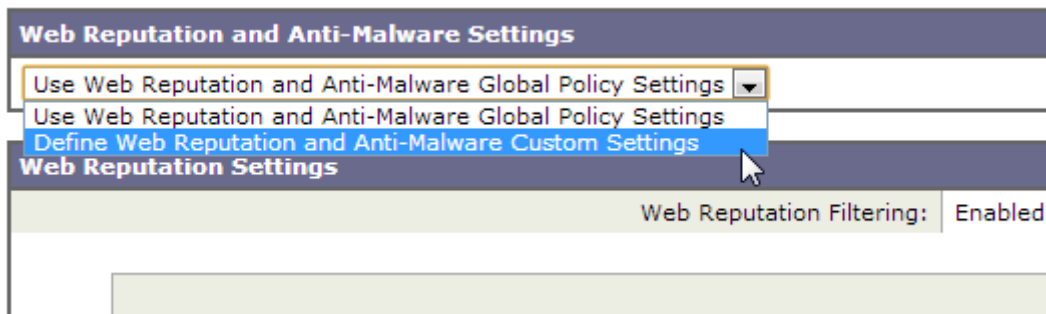
3.5 Уређивање скенирања саобраћаја

Уређивање скенирања саобраћаја се врши на страници **Web Reputation and Anti-Malware Settings**. На страници се налазе три секције:

- ❖ Web Reputation and Anti-Malware Settings
- ❖ Web Reputation Settings
- ❖ Cisco *Ironport* DVS Anti-Malware Settings

Администраторима се препоручује да не мењају подешавања које је поставио AMPEC, посебно не секцију **Web Reputation Settings** јер то може довести до већег оптерећења рада уређаја.

Уколико корисници одлуче да мењају подешавања на овој страници неопходно је да у секцији **Web Reputation and Anti-Malware Settings** из падајуће листе изаберу опцију **Define Web Reputation and Anti-Malware Custom Settings** (слика 3-24). Након овога, све секције ће бити откључане и биће омогућено њихово мењање.

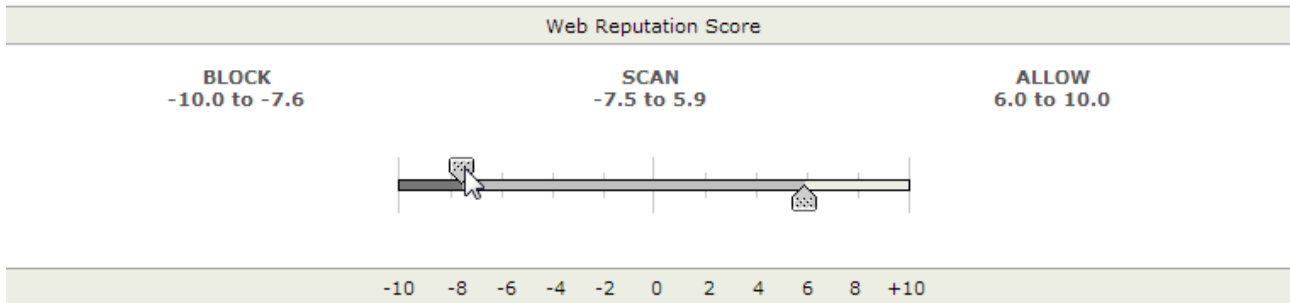


Слика 3-24

Секција **Web Reputation Settings** уређује када ће *Ironport* уређаји скенирати саобраћај а све то према параметру веб-репутације. *Cisco* за велики број сајтова води статистику о веб-репутацији. Сваки сајт се оцењује оценом од -10 до +10, при чему је -10 најгора оцена док је +10 најбоља. Сајтови се оцењују према томе колико проблема су правили свим Интернет корисницима који су им приступали. Под проблемима се подразумевају *phishing* напади, појава *malware-a*, *spyware-a*, вируса или *spam* порука. Број сајтова за који се води статистика о веб-репутацији је огроман и сваког дана је све већи. Ипак у свакодневном коришћењу Интернет-а корисници ће скоро сигурно наићи на сајт за који *Ironport* нема веб-репутацију. У **Web Reputation Settings** секцији се могу подешавати две границе: доња и горња граница за скенирање. Уколико неки сајт има веб-репутацију испод доње границе, *Ironport* уређаји ће аутоматски блокирати приступ посматраном сајту. *Ironport* сматра да је тражени сајт веома опасан и скоро сигурно би нанео штету кориснику који му приступа. Уколико неки сајт има веб-репутацију између доње и горње границе, *Ironport* уређаји ће скенирати саобраћај који се размењује у потрази за *malware* софтвером који би могао евентуално да се појави. На овај начин *Ironport* спречава да у мреже крајњих корисника улазе вируси, *spyware* и сличан садржај. Уколико неки сајт има веб-репутацију изнад горње границе скенирања, *Ironport* уређаји ће аутоматски допустити комуникацију без било каквог скенирања саобраћаја.

Оперативним радом у дужем временском периоду AMPEC је дошао до тренутних вредности граница и администраторима се препоручује да не мењају постављене границе! Уколико администратори ипак

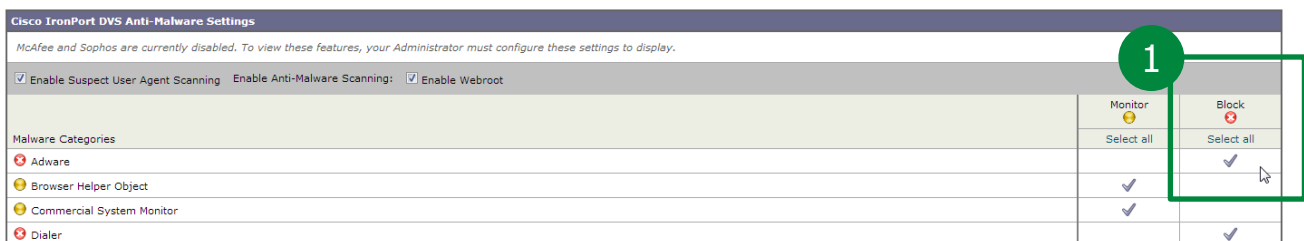
одлуче да промене границе то могу учинити померањем граничника у леву или десну страну (слика 3-25).



Слика 3-25

Сав саобраћај који се размењује са сајтовима који немају *Cisco Ironport* веб-репутацију ће бити аутоматски скениран. Приликом скенирања саобраћаја користи се *Webroot* антивирусно решење.

У секцији ***Cisco Ironport DVS Anti-Malware Settings*** могу се блокирати *malware* садржаји. *Ironport* је разврстао *malware* у посебне категорије (*Adware*, *Browser Helper Object*, *Commercial System Monitor*, *Dialer* итд.). Оперативним радом у дужем временском периоду АМРЕС је дошао до тренутне праксе да се блокирају одређене *malware* категорије. Администраторима се не препоручује да мењају акције које је поставио АМРЕС. Уколико администратори ипак одлуче да промене акцију за одређену *malware* категорију, неопходно је да кликну на поље **Block** (1) у реду за одговарајућу *malware* категорију (слика 3-26).



Слика 3-26

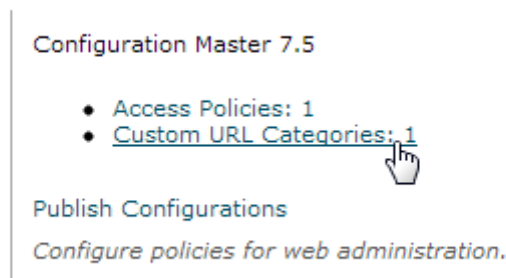
Након извршених промена на овој страни, неопходно је притиснути дугме **Submit** како би се сачувала начињена подешавања.

4 Уређивање Custom URL категорија

На *Ironport* уређајима се могу направити *Custom URL* категорије. У *Custom URL* категорије се потом убацују појединачни веб-сајтови за које је потребно подесити другачије акције. Администратори немају право да креирају *Custom URL* категорију већ их прави АМРЕС и потом дозвољава администраторима да их уређују према својим потребама. У складу са тим АМРЕС свакој институцији додељује само једну *Custom URL* категорију под називом "**<име институције> ЕХР забрањени сајтови**". Администратор користи ову *Custom URL* категорију како би блокирао неке сајтове који се не блокирају у постојећој конфигурацији *Ironport* уређаја. Дешава се да неки сајтови нису категоризовани, па је могуће да не буду блокирани иако је у конфигурацији *Ironport* уређаја подешено да се сајтови таквог садржаја блокирају. Како би администратор блокирао овакав сајт, може га убацити у *Custom URL* категорију своје институције и тако га забранити.

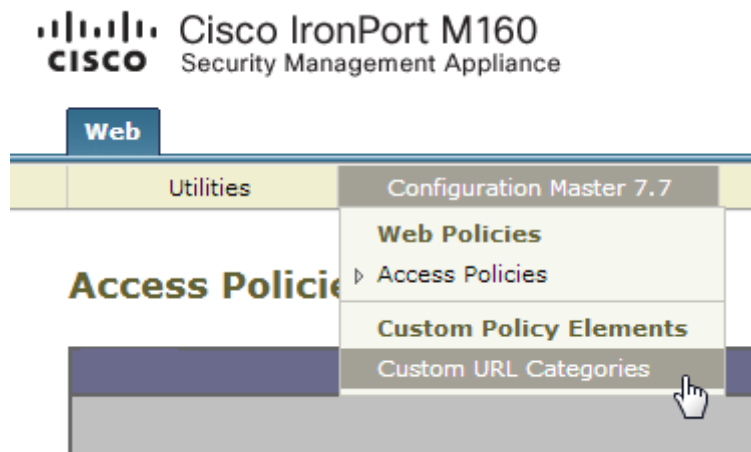
НАПОМЕНА: "**<име институције> ЕХР забрањени сајтови**" се користи за блокирање појединачних сајтова а не за њихово допуштање! Подешавање акције за посматрану *Custom URL* категорију се поставља у *Access* полиси и администратори не смеју да мењају акцију **Block** коју је поставио АМРЕС! Администратори могу да у ову категорију убацују сајтове које желе да блокирају и то се врши у посебној секцији *Ironport* подешавања. Убацавање сајтова односно уређење *Custom URL* категорије ће бити објашењено у овом поглављу.

Приступ страници на којој се врши уређење *Custom URL* категорије се може обавити на два начина. Први начин је преко почетне странице, када се администратор тек пријави на *Ironport* систем. Неопходно је кликнути на опцију **Custom URL Categories:1** (слика 4-1)



Слика 4-1

Други начини приступа страници је преко хоризонталног менија који се налази на свакој страници *Ironport* система. Потребно је одабрати мени **Configuration Master 7.7** и у падајућем менију одабрати опцију **Custom URL Categories** (слика 4-2)



Слика 4-2

На екрану ће се појавити страница **Custom URL Categories** и на њој табела у којој постоји само једна *Custom URL* категорија - "**<име институције> EXP забрањени сајтови**". Да би администратор могао да убаца сајтове у ову категорију, неопходно је да кликне на њу (слика 4-3)

Custom URL Categories

Custom URL Categories	
Order	Category
11	Institucija EXP zabranjeni sajtovi

Слика 4-3

На екрану ће се коначно појавити страница **Edit Category** у којој се могу убацивати сајтови које администратор жели да блокира. Да би блокирао неки сајт (нпр. *example.com*) неопходно је у поље **Sites** уписати доменско име сајта или његову *IP* адресу. Сајтови требају да буду одвојени зарезом и једним знаком размака (слика 4.4).

Edit Custom URL Category	
Category Name:	Institucija EXP zabranjeni sajtovi
List Order:	11
Sites: ?	<div style="border: 1px solid #ccc; padding: 5px;"> .example.com, example.com </div> <p><small>(e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)</small></p>
<input type="button" value="Sort URLs"/>	<p><small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small></p>
<input type="button" value="Advanced"/>	<p><small>Match specific URLs by regular expressions.</small></p>
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

Слика 4-4

Препорука администраторима је да сајтове блокирају са уписом сличним "*example.com*". На овај начин биће забрањени и сви поддоменски простори *example.com* домена (нпр. *akademija.example.com*, *www.example.com*, *vesti.example.com* и сл.). Ипак са уносима треба бити опрезан јер уколико нема

поддоменских простора, сајт са оваквим уписом неће бити блокиран. У том случају неопходне је користити унос без тачке испред. AMRES препоручује администраторима да тестирају блокиране сајтове и увере се у исправност својих уноса. Након одређеног оперативног рада, администратори ће стећи рутину у блокирању појединачних веб-сајтова.

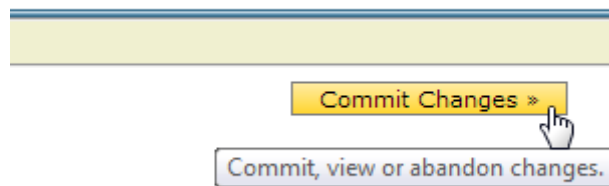
Након извршених промена на овој страни, неопходно је притиснути дугме **Submitt** како би се сачувала начињена подешавања.

5 Снимање конфигурације

Администратор се повезује на *Ironport Management* уређај и на њему подешава жељену конфигурацију. Након што администратор направи сва подешавања која је замислио неопходно је снимити начињену конфигурацију и потом је проследити свим *Ironport* прокси уређајима у мрежи.

На почетку администратор се повезује на *Ironport Management* уређај и подешава одређене секције *Access* Полисе или *Custom URL* категорије. Да би била снимљена сва начињена подешавања, у свакој секцији која је мењана неопходно је притиснути дугме **Submitt**. Овим се чувају подешавања у секцијама конфигурације.

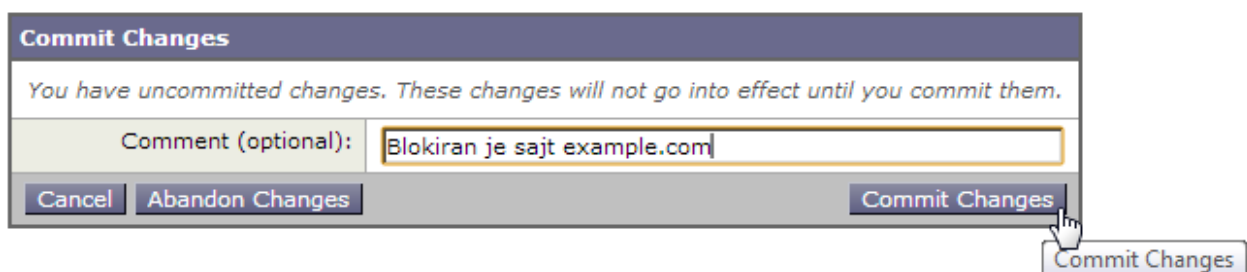
Након што направи све промене у својој *Access* полиси и *Custom URL* категорији, неопходно је сачувати комплетну конфигурацију на *Ironport Management* уређају. Ово се чини притиском на дугме **Commit Changes**, које се налази у горњем десном углу на свакој страници *Ironport* система (слика 5-1).



Слика 5-1

Потом ће се појавити нова страница у којој се уноси коментар. Коментар је пожељно унети приликом сваке промене конфигурације како би биле документоване све промене на уређају. Уколико је администратор мењао *Custom URL* категорију, требало би у пар речи описати шта је мењано у конфигурацији (пример слика 5-2) и потом притиснути дугме **Commit Changes**.

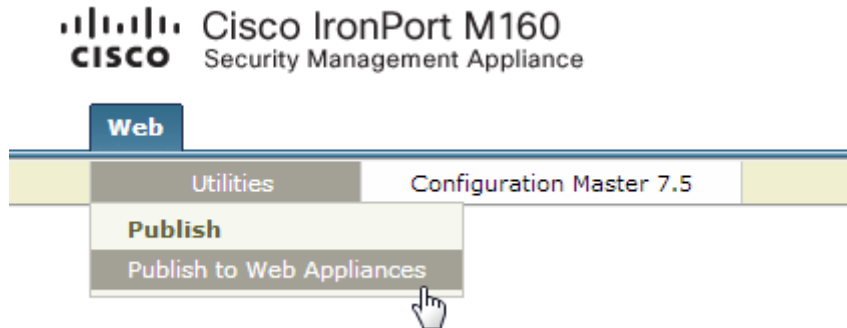
Uncommitted Changes



Copyright © 2003-2012 Cisco Systems, Inc. All rights reserved.

Слика 5-2

Након што је снимљена конфигурација на *Ironport Management* уређају, неопходно је конфигурацију проследити свим *Ironport* прокси уређајима у мрежи. То се врши преко хоризонталног менија и поља **Utilities** и потом из падајућег менија избора опције **Publish to Web Appliances** (слика 5-3).



Слика 5-3

Након тога ће се појавити нова страница у којој је потребно притиснути дугме **Publish Configuration Now...** (слика 5-4)

Publish Configuration Now

Settings for Publishing	
Job Name:	<input checked="" type="radio"/> System-generated job name (example: stevan.stevic.18_Oct_2012.17:08) <input type="radio"/> User-defined job name: <input type="text"/>
Start Time:	Now 18 Oct 2012 17:08 (GMT +02:00)
Configuration Master to Publish:	Configuration Master 7.5
Web Appliances: (?)	Options... Options... All assigned appliances Select appliances in list

Note: Publishing will take place immediately when the Publish button is pressed. It is not necessary to "commit" these changes.

Cancel Publish

Слика 5-5

Након тога ће се појавити страница **Publish in progress** на којој ће администратор видети како се извршава прослеђивање конфигурације на свих 5 *Ironport* прокси уређаја. Тек након што конфигурација буде успешно прослеђена на свих 5 *Ironport* прокси уређаја (слика 5-6), администратор може притиснути дугме **Close**.

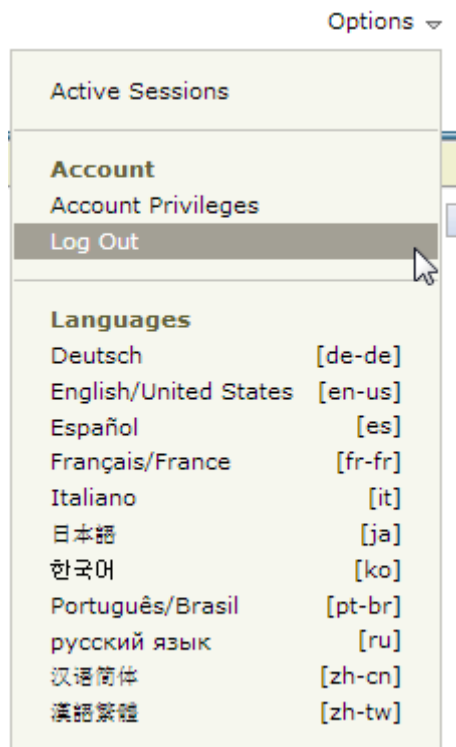
Job stevan.stevic.18_Oct_2012.17:12 Started at 18 Oct 2012 17:12 (GMT +02:00)		
Web Appliances	Progress	Status
proxy1	<div style="width: 100%; height: 10px; background-color: green;"></div>	Success
proxy2	<div style="width: 100%; height: 10px; background-color: green;"></div>	Success
proxy3	<div style="width: 100%; height: 10px; background-color: green;"></div>	Success
proxy4	<div style="width: 100%; height: 10px; background-color: green;"></div>	Success
proxy5	<div style="width: 100%; height: 10px; background-color: green;"></div>	Success

Close

Слика 5-6

Овим се успешно имплементира промена у политици прихватљивог садржаја коју је замислио администратор.

Администратор се може излоговати одабиром опције **Options** у горњем десном углу било које *Ironport* странице и из падајућег менија одабиром опције **Log Out** (слика 5-7).



Слика 5-7

6 Решавање притужби корисника

Када је нека страница блокирана или је недоступна, корисницима ће се на екрану приказати *EUN (End User Notification)* страница. На *Ironport* систему постоји 55 различитих *EUN* страница. Свака страница се приказује у зависности од случаја који се догодио: блокиран приступ због *URL* категорије, блокиран приступ због веб-репутације, тражени сервер није доступан и слично. На слици 6-1 може се видети пример *EUN* странице када је приступ блокиран на основу *URL* категорије.

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 blokirana. 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.ac.rs).

Kontrolni kod: (Tue, 04 Aug 2015 14:18:31 CEST, proxy2.amres.ac.rs, HTTP, BLOCK-WEBCAT, <http://www.bet365.com/>, www.bet365.com, Gambling, GET, 1.5, , , 147.91.255.20, lme_institucije, Polisa_institucije)

Institucija	Administrator	E-mail

Слика 6-1

Свака трансакција је једнозначно одређена контролним кодом (1). На основу контролног кода, администратор има информације ко, када и зашто није могао да приступи одређеном садржају. На *EUN* страници се сваки корисник саветује да копира контролни код и пошаље га свом администратору. Имејл адресе администратора се налазе у табели испод контролног кода. У табели се налазе имејл адресе свих администратора који самостално уређују политику прихватљивог садржаја за своје кориснике.

НАПОМЕНА: Сваки администратор који изрази жељу да самостално уређује политику прихватљивог садржаја мора да приложи имејл адресу на коју ће стизати притужбе.

Контролни код има неколико поља која се ређају са леве на десну страну у следећем распореду (пример на слици 6-1)

- ❖ Дан у недељи (*Tue - Tuesday*)
- ❖ Датум и време (*04 Aug 2015 14:18:31 CEST*)
- ❖ Прокси уређај на коме се догодила трансакција (*proxy2.amres.ac.rs*)
- ❖ Протокол који је коришћен (*HTTP*)
- ❖ Акција коју је спровео *Ironport* систем (*BLOCK-WEBCAT* – блокирана *URL* категорија)
- ❖ *URL* који је корисник укуцао у Web browser (<http://www.bet365.com/>)
- ❖ Сервер који је корисник покушао да контактира (www.bet365.com)
- ❖ *URL* категорија којој припада тражени сајт (*Gambling*)
- ❖ Метод који је клијент користио (*GET*)
- ❖ Веб-репутација сајта/сервера (1.5)

- ❖ *Malware* категорија (нема *Malware* – празно поље)
- ❖ Име *Malware* софтвера (нема *Malware* – празно поље)
- ❖ *IP* адреса која је покушала трансакцију (147.91.255.20)
- ❖ Институција којој корисник припада (*Ime_Institucije*)
- ❖ *Access* полиса која је третирала посматрану трансакцију (*Polisa_Institucije*)

На основу ових информација администратор може да закључи шта се догодило и зашто корисник није могао да приступи траженом садржају. Уколико администратор не може да закључи зашто је трансакција била неуспешна или не може да реши проблем, може контактирати amres@helpdesk.ac.rs како би АМРЕС асистирао у решавању проблема.

Најзначајније поље у контролном коду је свакако акција коју је спровео *Ironport* систем. У следећој табели су дате све акције *Ironport* система.

Табела 1. Акције *Ironport* система

Акција <i>Ironport</i> система	Објашњење
<i>ALLOW_ADMIN</i>	Трансакција је дозвољена на основу секције <i>Applications</i> у <i>Access</i> полиси
<i>ALLOW_ADMIN_ERROR_PAGE</i>	Трансакција је дозвољена на <i>Ironport EUN</i> страницу
<i>ALLOW_CUSTOMCAT</i>	Трансакција је дозвољена на основу <i>Custom URL</i> категорије
<i>ALLOW_WBRS</i>	Трансакција је дозвољена на основу веб-репутације
<i>BLOCK_ADMIN</i>	Трансакција је блокирана на основу секције <i>Applications</i> или <i>Objects</i> у <i>Access</i> полиси
<i>BLOCK_ADMIN_CONNECT</i>	Трансакција је блокирана на основу <i>TCP</i> портова који су дозвољени у <i>Access</i> полиси
<i>BLOCK_ADMIN_CUSTOM_USER_AGENT</i>	Трансакција је блокирана на основу забрањеног Интернет прегледача у <i>Access</i> полиси
<i>BLOCK_ADMIN_DLP</i>	Трансакција је блокирана на основу забрањеног <i>MIME</i> типа у секцији <i>Objects</i> у <i>Access</i> полиси
<i>BLOCK_ADMIN_FILE_TYPE</i>	Трансакција је блокирана на основу типа фајла у <i>Access</i> полиси
<i>BLOCK_ADMIN_PROTOCOL</i>	Трансакција је блокирана на основу протокола у <i>Access</i> полиси
<i>BLOCK_ADMIN_SIZE</i>	Трансакција је блокирана на основу максималне величине објекта у <i>Access</i> полиси
<i>BLOCK_ADMIN_SIZE_DLP</i>	Трансакција је блокирана на основу величине захтева
<i>BLOCK_AMW_REQ</i>	Трансакција је блокирана на основу <i>Anti-Malware</i> политике. <i>Malware</i> се јавио у захтеву
<i>BLOCK_AMW_RESP</i>	Трансакција је блокирана на основу

	<i>Malware</i> подешавања у секцији <i>Web Reputation and Anti-Malware Filtering</i>
BLOCK_AMW_RESP_URL	Трансакција је блокирана јер постоји сумња у <i>HTTP</i> захтев. Болкада је уследила услед <i>Malware</i> подешавања у секцији <i>Web Reputation and Anti-Malware Filtering</i>
BLOCK_AVC	Трансакција је блокирана на основу секције <i>Application y Access</i> полиси
BLOCK_CONTENT_UNSAFE	Трансакција је блокирана на основу рејтинга садржаја. Клијент је захтевао садржај који је означен као <i>Adult</i> а тај садржај је блокиран у <i>Access</i> полиси
BLOCK_CONTINUE_CONTENT_UNSAFE	Трансакција је привремено блокирана док корисник на страници упозорења не потврди да жели да приступи траженом садржају. Односи се на <i>Adult</i> садржај.
BLOCK_CONTINUE_CUSTOMCAT	Трансакција је привремено блокирана док корисник на страници упозорења не потврди да жели да приступи траженом садржају. Односи се на <i>Custom URL</i> категорије
BLOCK_CONTINUE_WEBCAT	Трансакција је привремено блокирана док на страници упозорења не потврди да жели да приступи траженом садржају. Односи се на <i>URL</i> категорије у <i>Access</i> полиси
BLOCK_CUSTOMCAT	Трансакција је блокирана на основу <i>Custom URL</i> категорије
BLOCK_ICAP	Трансакција је блокирана на основу <i>AMPEC</i> подешавања за екстерни <i>DLP (Data Loss Prevention)</i> систем
BLOCK_SEARCH_UNSAFE	Трансакција је блокирана на основу <i>Safe Search</i> опције у секцији <i>URL</i> категорије у <i>Access</i> полиси
BLOCK_SUSPECT_USER_AGENT	Трансакција је блокирана на основу сумњивих Интернет прегледача подешених у <i>Access</i> полиси
BLOCK_UNSUPPORTED_SEARCH_APP	Трансакција је блокирана на основу блокаде сајтова Интернет претраживача који не поседују <i>Safe Search</i> . Блокада је постављена у секцији <i>Content Filtering y URL</i> категоријама у <i>Access</i> полиси
BLOCK_WBRS	Трансакција је блокирана на основу лоше веб-репутације
BLOCK_WBRS_DLP	<i>Upload</i> трансакција је блокирана на основу <i>AMPEC</i> подешавања за веб-репутацију
BLOCK_WEBCAT	Трансакција је блокирана на основу <i>URL</i> категорије

BLOCK_WEBCAT_DLP	Трансакција је блокирана на основу АМРЕС подешавања за <i>URL</i> категорије
DEFAULT_CASE	Трансакција је дозвољена јер ниједан сервис (веб-репутација или <i>anti-malware</i> скенирање) није предузимао никакве акције
MONITOR_AMW_RESP	Трансакција је надгледана у погледу <i>Anti-Malware</i> скенирања
MONITOR_AMW_RESP_URL	Трансакција је надгледана јер <i>Anti-Malware</i> подешавања у <i>Access</i> полиси сумњају у тражени <i>URL</i>
MONITOR_AVC	Трансакција је надгледана због подешавања у секцији <i>Applications</i> у <i>Access</i> полиси
MONITOR_CONTINUE_CONTENT_UNSAFE	Трансакција је надгледана након што је корисник потврдио да је свестан каквом садржају приступа (акција <i>Warn</i> у <i>Access</i> полиси). Ово се односи на рејтинг садржаја који је означен као <i>Adult</i>
MONITOR_CONTINUE_CUSTOMCAT	Трансакција је надгледана након што је корисник потврдио да је свестан каквом садржају приступа (акција <i>Warn</i> у <i>Access</i> полиси). Ово се односи на <i>Custom URL</i> категорије у <i>Access</i> полиси
MONITOR_CONTINUE_WEBCAT	Трансакција је надгледана након што је корисник потврдио да је свестан каквом садржају приступа (акција <i>Warn</i> у <i>Access</i> полиси). Ово се односи на <i>URL</i> категорије у <i>Access</i> полиси
MONITOR_DLP	<i>Upload</i> трансакција је надгледана
MONITOR_SUSPECT_USER_AGENT	Трансакција је надгледана због сумњивог Интернет прегледача. Подешавања су направљена у <i>Access</i> полиси
MONITOR_WBR	Трансакција се надгледа због веб-репутације која је подешена у <i>Access</i> полиси
NO_AUTHENTICATION	Трансакција није дозвољена јер се корисник није аутентификовао према подешавањима које је поставио АМРЕС у <i>SAAS Application Authentication</i> полиси
NO_PASSWORD	Трансакција није дозвољена јер се корисник није исправно аутентификовао
REDIRECT_CUSTOMCAT	Трансакција је редиректована на основу подешавања у <i>Custom URL</i> категорији
SAAS_AUTH	Трансакција је дозвољена јер се корисник исправно аутентификовао према подешавањима која је поставио АМРЕС у <i>SAAS Authentication</i> полиси
OTHER	Трансакција није комплетирана услед

	грешке која се јавила приликом обраде захтева.
--	--

Током свог рада, администратори вероватно неће доћи у контакт са многим акцијама које су овде представљене. Када администратор у контролном коду уочи неку акцију, потребно је да прегледа ову табелу и утврди шта та акција представља.