Cisco Expo 2008

Podrobno pregledovanje paketov

Cisco Expo – Bled 2008

Silvo Lipovšek

Enable Your Network
Empower Your Business

Podrobno pregledovanje paketov

- Današnja definicija PPP
- Flexible Packet Matching
- Kam vse to spada v dizajnu
- Zaključek

Podrobno pregledovanje paketov – današnja definicija

Podrobno pregledovanje paketov

- Zakaj želimo vedno bolj podrobno pregledovanje paketov?
- Različni tipi prometa (aplikacij) zahtevajo različne vire (npr. pasovna širina, prioriteta,…).
- Bolj podrobno razumevanje toka podatkov nam omogoča:

  Boljši nadzor in kontrolo nad aplikacijami

  Boljšo optimizacijo prometa

  Večjo varnost
- Da to dosežemo, moramo pogledati v paket bolj globoko kot samo do nivoja 4 (Layer 4 OSI)
- Mreža je pomemben element varnosti, oz. varnostne storitve, ki jih ponuja mreža. Mreža je stična točka vseh elementov, zagotavljanje varnosti v mreži je smiselno.
- Zato moramo mreži omogočiti podrobno pregledovanje paketov.

"Deep packet inspection (DPI) is a form of computer network packet filtering that examines the data part of a through-passing packet, searching for non-protocol compliance or predefined criteria to decide if the packet can pass. This is in contrast to shallow packet inspection (usually called just packet inspection) which just checks the header portion of a packet.

DPI devices have the ability to look at Layer 2 through Layer 7 of the OSI model. This includes headers and data protocol structures. The DPI will identify and classify the traffic based on a signature database and will allow the user to perform many things. A classified packet can be redirected, marked/tagged (see QoS), blocked, rate limited, and of course, reported to a reporting agent in the network.

Many DPI devices also perform the ability to identify flows rather than a packet by packet analysis.

DPI allows phone and cable companies to "readily know the packets of information you are receiving online--from e-mail, to websites, to sharing of music, video and software downloads"[1] - as would a network analysis tool.

DPI is also increasingly being used in security devices to analyze flows, compare them against policy, and then treat the traffic appropriately (i.e., block, allow, rate limit, tag for priority, mirror to another device for more analysis or reporting)."

Source : http://en.wikipedia.org/wiki/Deep_packet_inspection

Podrobno pregledovanje paketov

- **Packet Filter:** Prva generacija požarnih zidov. Filtrira pakete na osnovi podatkov v paketu (IP naslova, protokol, port). Nič ne vemo o aplikaciji.
- **Stateful filter:** Se zaveda toka paketov – seje. Nič ne vemo o aplikaciji
- **Aplikativni nivo:** Uporaba posrednikov (proxy). Razume protokole. “Nič ne vemo o aplikaciji.”
- **Deep packet inspection** (**DPI**)

  Filtriranje paketov v določeni točki.

  Pregleduje več kot samo zaglavje paketa - L2 do L7 v OSI modelu

  Glava (header), podatki o protokolu, sporočilo (payload).

Podrobno pregledovanje paketov

- Na osnovi pregleda paket klasificiramo in ukrepamo – preusmerimo, postavimo QoS oznako, blokiramo, omejimo hitrost, syslog,…
- Prepoznavanje aplikacije:

  Glede na TCP port (problem z naključno izbranimi porti in s tuneliranjem aplikacij znotraj drugih aplikacij – Kazaa znotraj http)

  Glede na ujemanje niza (iskanje niza znakov znotraj paketa)
- Bistveno vprašanje je prepoznavanje prometa/aplikacije. Od tu naprej so zadeve standardne.
- Enkripcija seveda zakomplicira zadeve.

Cilj napadov so aplikacije

75% napadov cilja na to povezavo

Kdo pripravlja varnostne popravke za vašo aplikacijo?
Kdo preverja varnost vaših aplikacij?
Kdaj ste nazadnje namestili servisni paket za vašo aplikacijo?

Zakaj ne bi popravili programske kode?

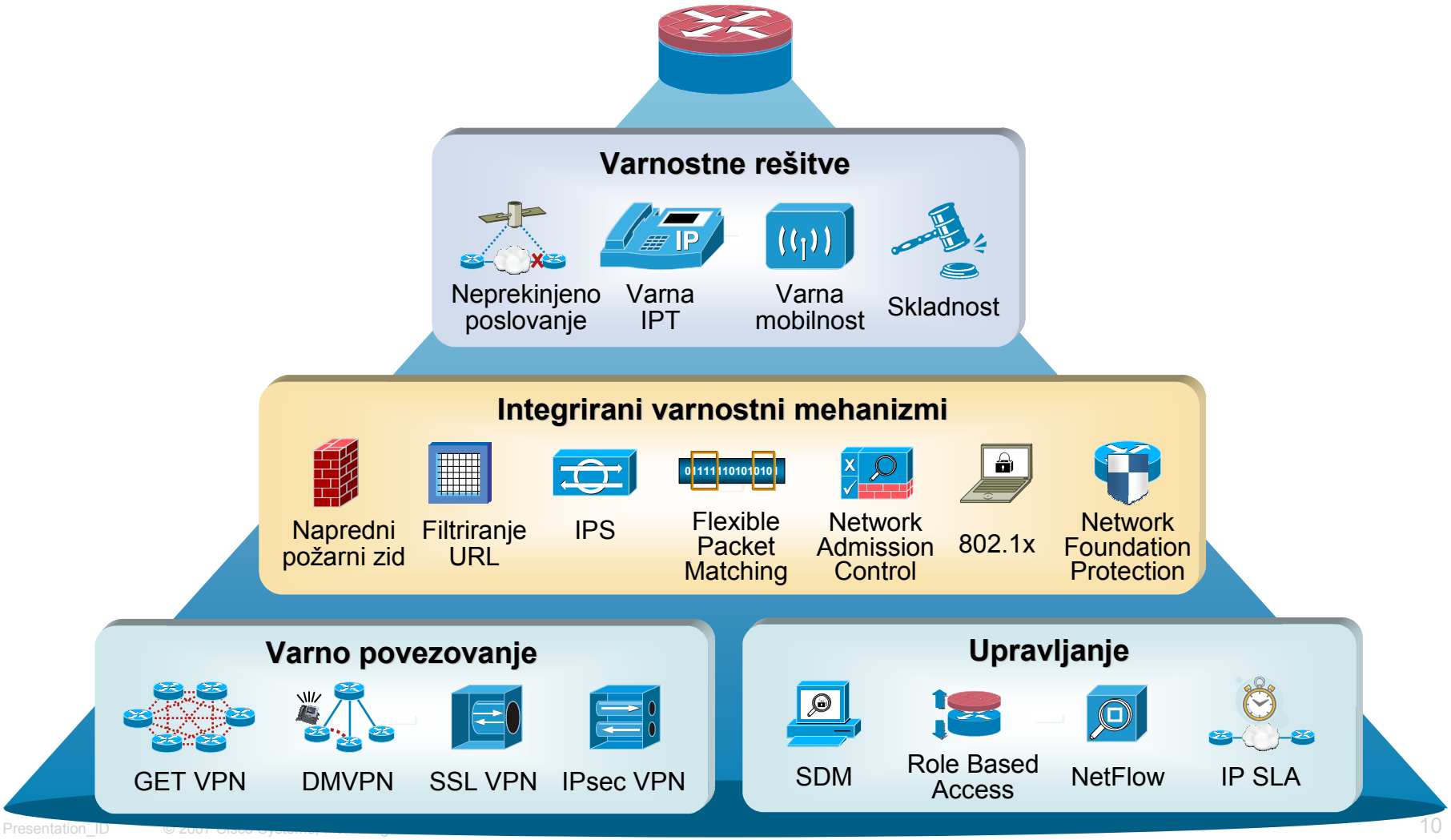
Vsakih 1000 vrstic programske kode prinese v povprečju 15 varnostnih problemov
(US Dept of Defense)

Povprečna poslovna aplikacija ima 150,000-250,000 vrstic programske kode
(Software Magazine)

Varnostni popravek zahteva 75 minut za diagnozo problema in 6 ur za popravo
(5 letna študija Pentagona)

- Razvijalci so fokusirani na nove funkcionalnosti in ne na napake
- Popravljanje varnostnih lukenj je zelo drago

Usmerjevalniki in varnost



FPM – Flexible Packet Matching

Kaj rešuje?

- Napadi so vedno bolj kompleksni. Paket moramo pregledovati bolj podrobno kot do sedaj.
- Klasificirati želimo na osnovi več atributov naenkrat.

  Lastnost SQL Slammerja je, da napada vrata 1434, ima dolžino paketa 404 byte in točno določeno zaporedje byte-ov znotraj paketa.
- Klasični ACLi so manj natančni – lahko zaustavijo tudi legitimen promet

  SQL Slammerja lahko zaustavimo z ACL tako, da blokiramo dostop do vrat 1434. To pa pomeni, da smo preprečili tudi dostop do Microsoft SQL strežnika.
- Iščemo način kako hitro definirati in klasificirati promet, da odbijemo neznane napade.

  Obstoječi načini so omejeni na znano polje ali dogodek.

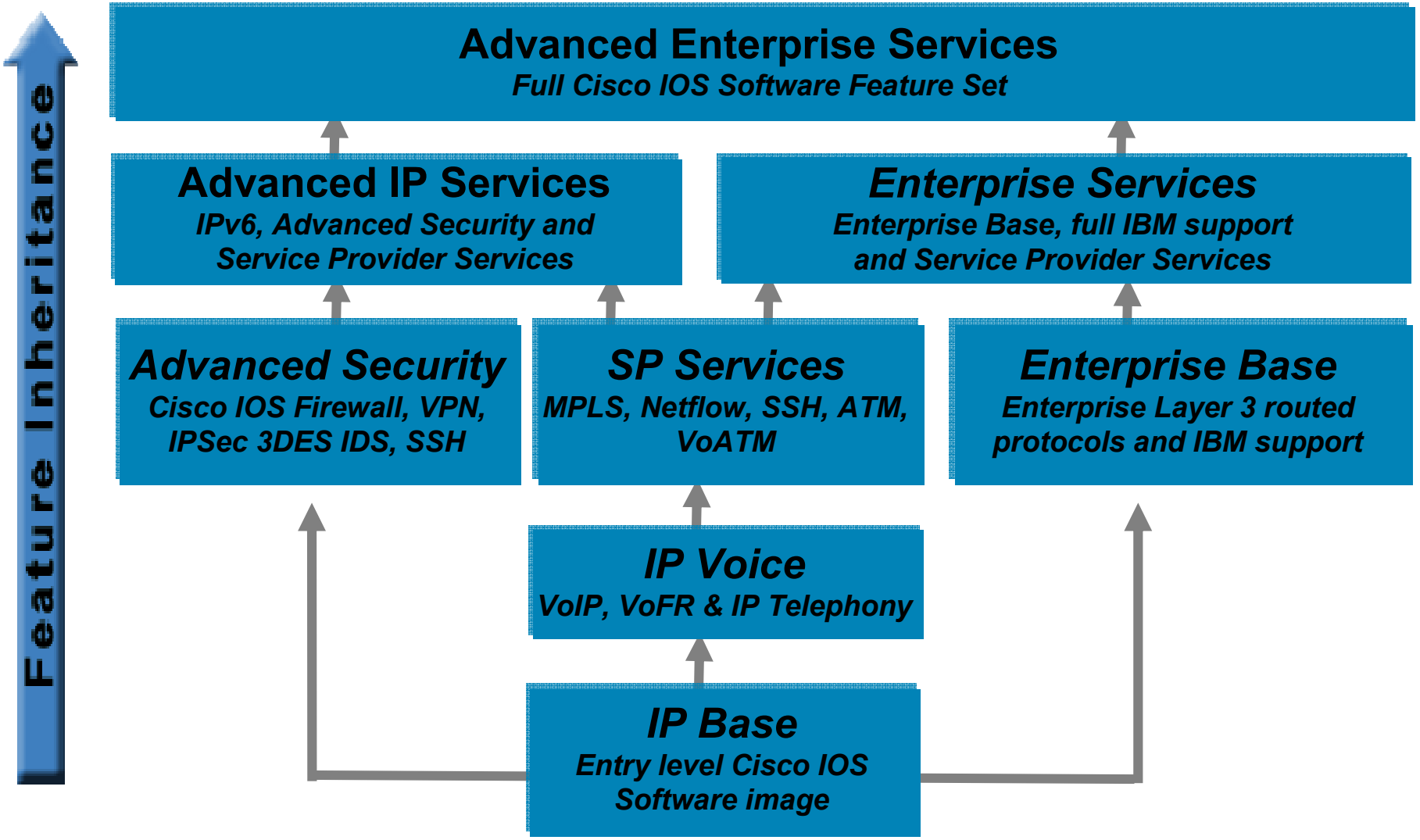
Flexible Packet Matching (FPM)

- Flexible Packet Matching (FPM) je naslednja generacija Access control List (ACL).
- Je fleksibilna in hitra prva obrambna črta, ki varuje pred škodljivim prometom na vstopni točki v mrežo.
- Klasificiranje na OSI nivoju 2-7, brez upoštevanja stanja (stateless).
- FPM je bil prvič vključen v Cisco IOS Release 12.4(4)T.

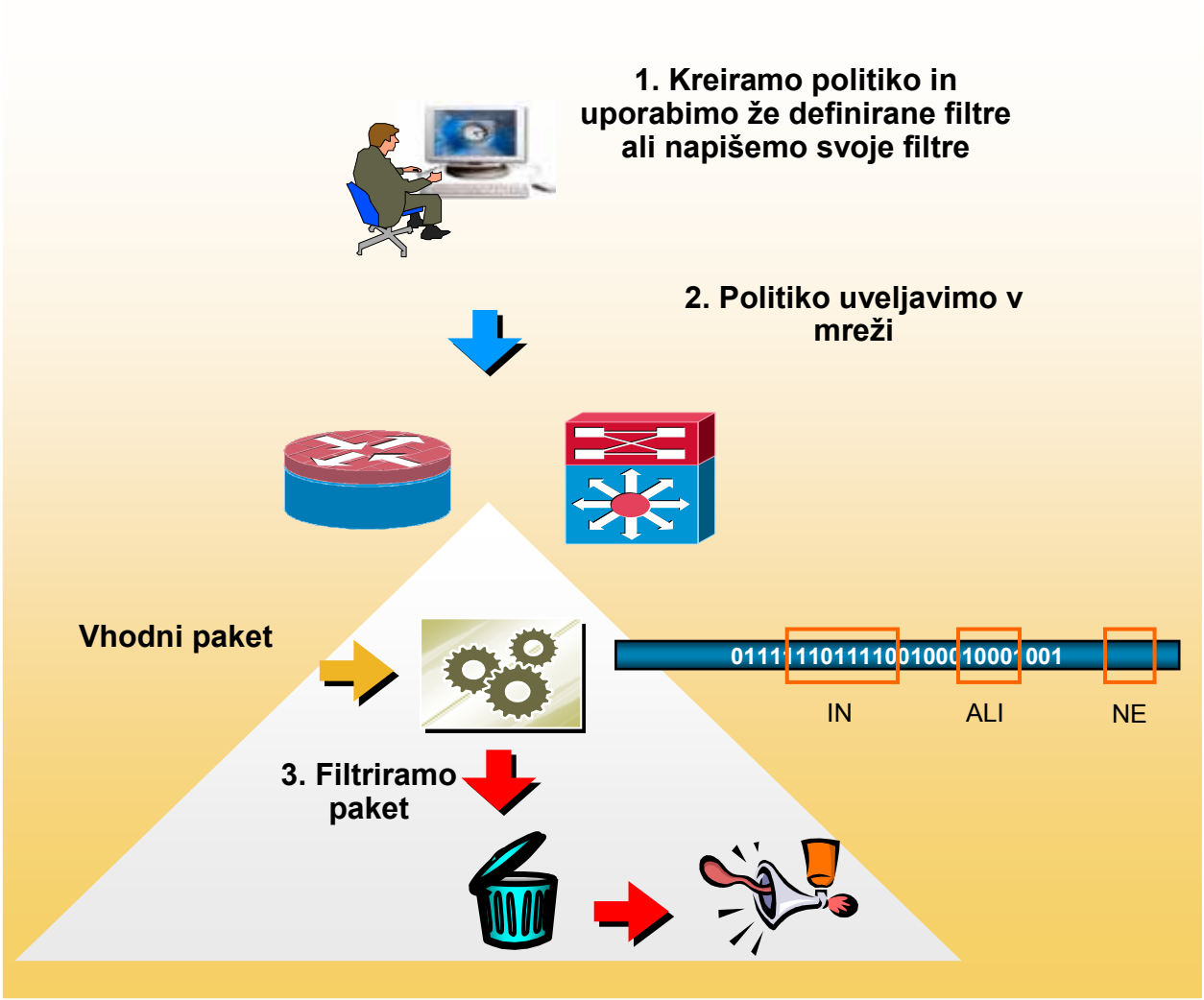
Flexible Packet Matching (FPM)

- V prvi verziji je lahko iskal vzorce dolžine do 32 byte-ov v prvih 256 byte-ih paketa.
- Cisco IOS Release 12.4(15)T omogoča iskanje vzorcev, ki so lahko dolgi do 256 byte-ov kjerkoli v paketu.
- FPM je podprt na usmerjevalnikih serije 800, 1800, 2800, 3800, 7301 in 7200. Pred uporabo je potrebno preveriti podporo v Feature Navigatorju na www.cisco.com/go/fn.
- Podprt je v paketih Advanced Security, Advanced IP Services in Advanced Enterprise.

IOS paketi za usmerjevalnike



Kako deluje



Elementi FPM

CLASS MAPS	=	prometni tokovi
POLICY MAPS	=	akcije
SERVICE POLICIES	=	vmesnik

Flexible Packet Matching (FPM)

- **Akcije**, ki jih lahko naredimo (policy map), ko filter klasificira paket:

  Zavržemo (Drop)

  Zabeležimo (Log)

  Pošljemo ICMP-Unreachable

- FPM uporablja Protocol Header Definition Files (PHDF) za definiranje glave protokola (protocol header). FPM lahko spreminjamo med delovanjem usmerjevalnika, brez ponovnega zagona.
- Filtre definiramo z uporabo Cisco Common Classification policy Language (C3PL) CLI ali z uporabo XML.

XML na hitro

- HTML = oznake, ki določajo *format* web strani (npr.: poudarjeno označimo z <b>, tabele z <td><tr>, barve <font>, …) – usmerjen na prikazovanje (format) strani in ne na vsebino
- XML = usmerjen na *vsebino*.XML nima vnaprej definiranih oznak. Ne obstaja <b>, <h1> ….

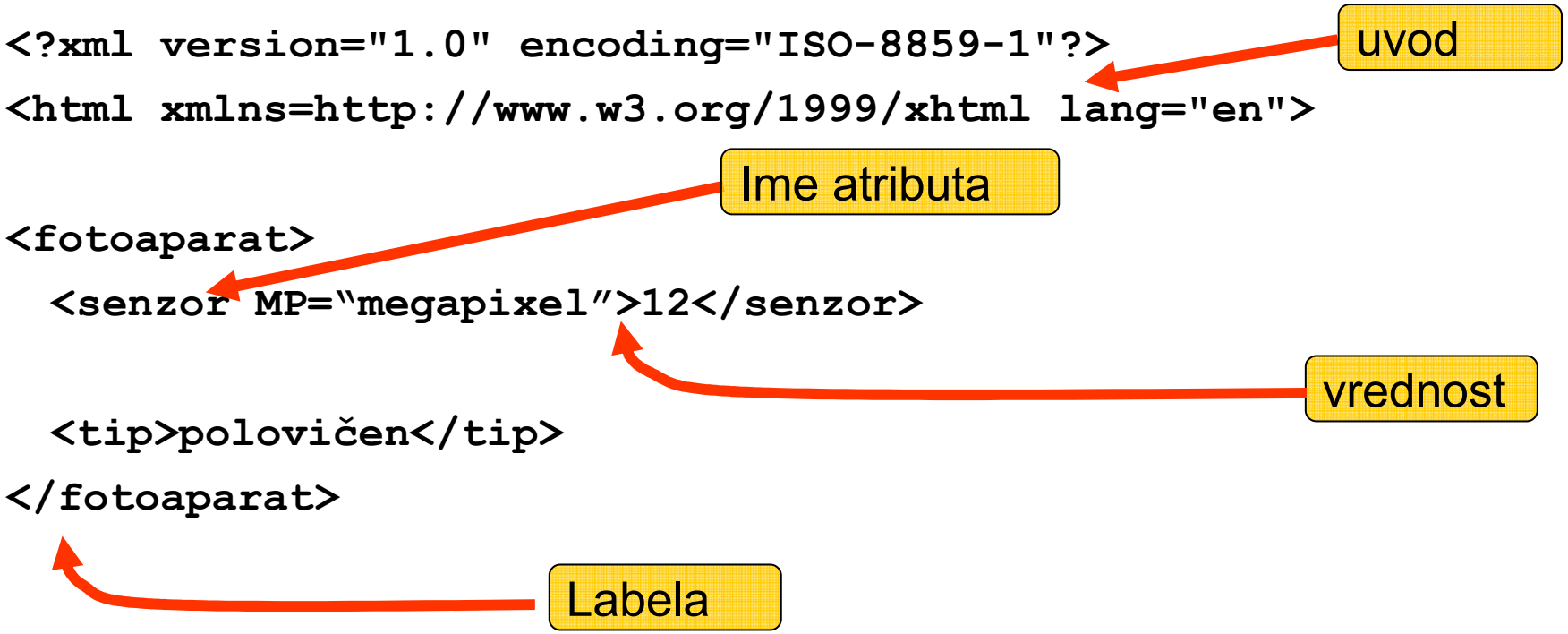
HTML

```
<h1>Stranka</h1>
<h2>Ga.</h2>
<h2>Ime</h2>
Alenka Novak
<h2>Naslov</h2>
Čopova 13
3000 Celje
```

XML

```
<stranka>
<ime>
<naziv>Ga.</naziv>
<ime>Alenka</ime>
<priimek>Novak</priimek>
</ime>
<ulica>Čopova 13</ulica>
<mesto>Celje</mesto>
<postna>3000</postna>
</stranka>
```

XML elementi



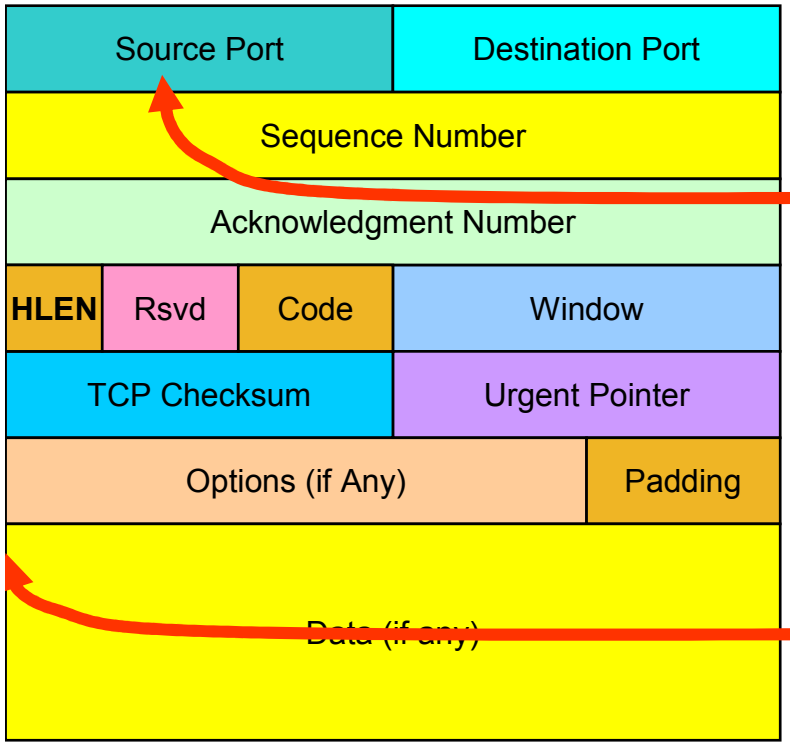

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<html xmlns=http://www.w3.org/1999/xhtml lang="en">

<fotoaparat>
  <senzor MP="megapixel">12</senzor>

  <tip>polovičen</tip>
</fotoaparat>
```

XML nima vnaprej definiranih oznak za uporabniške podatke. Dokument pa mora upoštevati sintaktična pravila.

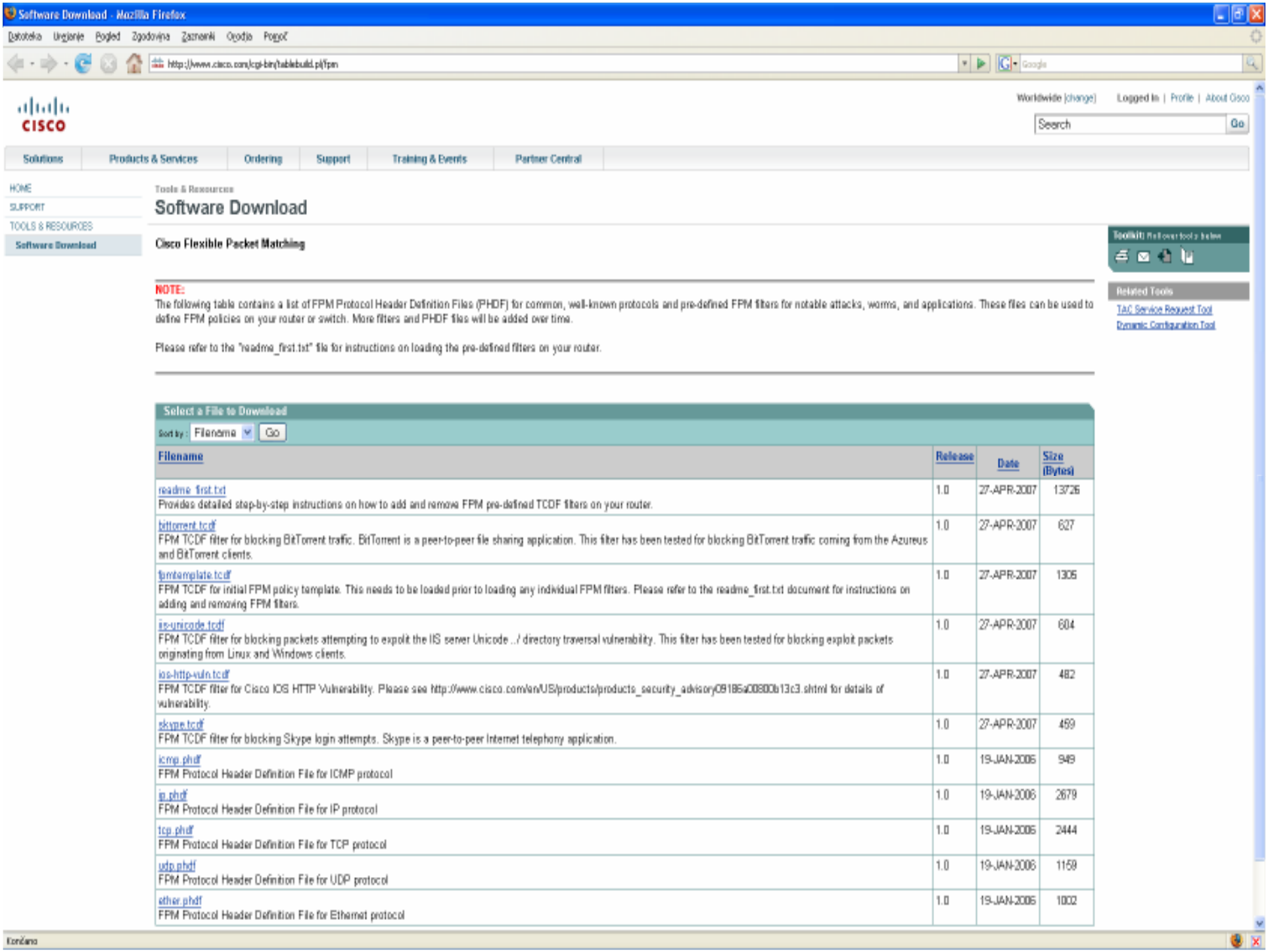
Flexible Packet Matching

- **PHDF** opisuje strukturo paketa v XML formatu.
- Z XML-om lahko opišemo glavo (header) kateregakoli protokola.
- Pomembni elementi PHDF-ja so:
  - Verzija
  - Lokacija XML sheme
  - Definicije polj protokola
- Polje protokola:
  - Ime polja
  - Opis polja
  - Lokacija polja znotraj glave (odmik od začetka glave)
  - Dolžina polja
- Enota mere so byte ali bit.
- “show run” ne pokaže naloženih PHDF-jev, ker so zapisani v XML.
- “show protocol phdf all”
- Standardne PHDF-je lahko prenesemo iz Cisco web strani:
  - http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

PHDF




```
<?xml version="1.0" encoding="utf-8" ?>
<phdf>
<version>1</version>
<protocol name="tcp" description="TCP-Protocol">
        <field name="source-port" description="TCP-Source-Port">
                <offset type="fixed-offset" units="bits">0</offset>
                <length type="fixed" units="bits">16</length>
        </field>
        <field name="dest-port" description="TCP-Destination-Port">
                <offset type="fixed-offset" units="bits">16</offset>
                <length type="fixed" units="bits">16</length>
        </field>
        <field name="seqnum" description="TCP-Sequence-Number">
                <offset type="fixed-offset" units="bits">32</offset>
                <length type="fixed" units”="bits">32</length>
        </field>
…
        <field name="payload-start" description="TCP-Payload-Start">
                <offset type="fixed-offset" units="bytes">20</offset
                <length type="fixed" units="bytes">0</length>
        </field>
        <headerlength type="fixed" value="20"/>
</protocol>
</phdf>
```



Software Download - Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

Worldwide (change) Logged In | Profile | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

HOME
SUPPORT
TOOLS & RESOURCES
Software Download

Tools & Resources

Software Download

Cisco Flexible Packet Matching

Toolkit: Follow tools below

Related Tools
TAC Service Request Tool
Dynamic Configuration Tool

NOTE:
The following table contains a list of FPM Protocol Header Definition Files (PHDF) for common, well-known protocols and pre-defined FPM filters for notable attacks, worms, and applications. These files can be used to define FPM policies on your router or switch. More filters and PHDF files will be added over time.

Please refer to the "readme_first.txt" file for instructions on loading the pre-defined filters on your router.

Select a File to Download

Sort by : Filename Go

Filename	Release	Date	Size (Bytes)
readme_first.txt Provides detailed step-by-step instructions on how to add and remove FPM pre-defined TCDF filters on your router.	1.0	27-APR-2007	13726
bittorrent.tcdf FPM TCDF filter for blocking BitTorrent traffic. BitTorrent is a peer-to-peer file sharing application. This filter has been tested for blocking BitTorrent traffic coming from the Azureus and BitTorrent clients.	1.0	27-APR-2007	627
fpmtemplate.tcdf FPM TCDF for initial FPM policy template. This needs to be loaded prior to loading any individual FPM filters. Please refer to the readme_first.txt document for instructions on adding and removing FPM filters.	1.0	27-APR-2007	1305
iis-unicode.tcdf FPM TCDF filter for blocking packets attempting to exploit the IIS server Unicode ../ directory traversal vulnerability. This filter has been tested for blocking exploit packets originating from Linux and Windows clients.	1.0	27-APR-2007	604
ios-http-vuln.tcdf FPM TCDF filter for Cisco IOS HTTP Vulnerability. Please see http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13c3.shtml for details of vulnerability.	1.0	27-APR-2007	482
skype.tcdf FPM TCDF filter for blocking Skype login attempts. Skype is a peer-to-peer Internet telephony application.	1.0	27-APR-2007	459
icmp.phdf FPM Protocol Header Definition File for ICMP protocol	1.0	19-JAN-2006	949
ip.phdf FPM Protocol Header Definition File for IP protocol	1.0	19-JAN-2006	2679
tcp.phdf FPM Protocol Header Definition File for TCP protocol	1.0	19-JAN-2006	2444
udp.phdf FPM Protocol Header Definition File for UDP protocol	1.0	19-JAN-2006	1159
ether.phdf FPM Protocol Header Definition File for Ethernet protocol	1.0	19-JAN-2006	1002

Končano

FPM – Vnaprej definirani PHDF-ji

icmp.phdf FPM Protocol Header Definition File for ICMP protocol
ip.phdf FPM Protocol Header Definition File for IP protocol
tcp.phdf FPM Protocol Header Definition File for TCP protocol
udp.phdf FPM Protocol Header Definition File for UDP protocol
ether.phdf FPM Protocol Header Definition File for Ethernet protocol

Flexible Packet Matching

- FPM XML Configuration: omogoča uporabo XML-a za definiranje prometa (traffic class) in akcij (policy).
- Ta XML datoteka se imenuje **TCDF** - Traffic Classification Definition File
- TDCF moramo naložiti v usmerjevalnik (load).
- Definicijo prometa in akcijo lahko napišemo tudi z uporabo CLI.
- Več informacij o TCDF in primeri uporabe:
  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_tcdf.html

FPM izrazi

- Relacijske operacije

  Eq, NEq, Gt, Lt ; Tudi na bitnem nivoju

- Logične operacije

  AND, OR

- Niz ali Regularni izraz
- Aritmetični izraz za določanje odmika v glavi, ki ima variabilno dolžino
- Iskalni niz v regularnem izrazu je lahko v decimalnem ali hex zapisu;
- Npr. 17 ali 0x11 najde enak znak

Regularni izraz	**Pomen**	**Primer**
ASCII znak	Znak	abcd predstavlja niz znakov "abcd" kjerkoli v iskalnem področju
.	Katerikoli znak	t..t predstavlja niz znakov kot sta npr. test in tekst
[ ]	Niz znakov ali območje znakov (-)	[02468a-z] predstavlja 0, 2, in v, ne predstavlja pa 1, 9 ali K
*	Nič ali več ponovitev znakov	5* predstavlja pojavljaje cifre *5* nič krat ali poljubno krat
?	Nič ali en znak	ba?b predstavlja *bb* in *bab*
\	Določa znak in ne meta-znak	18\..* predstavlja zaporedje *18.* in vsak znak, ki sledi *18.*

FPM - primer

Flexible Packet Matching

- Kreiranje filtra
  1. **Naložimo datoteko protokola** (#load protocol flash:ip.phdf)
  2. **Class-map**: definiramo kriterij ujemanja (match)
     1. Description
     2. Match field
     3. Match start
  3. Show class-map
  4. **Policy-map**: definiramo akcijo, ki naj se izvede (binds match to an action)
     1. Description
     2. Class <class-name>
     3. Drop
     4. Service-policy <policy-map-name> (kreiranje hierarhičnih service-policy)
  5. **Interface <interface name>**:povežemo vmesnik in service-policy
     1. Service-policy
- Če PHDF ni naložen, lahko uporabljamo le “match start” ukaz. Sicer lahko uporabljamo tudi “match field” ukaz.
- PRIMER

FPM Primer 1 – preprečitev Skype prometa

- Ko se Skype klient poveže na Skype strežnik, mu pošlje paket, ki vsebuje zaporedje 0x1603010000, ki po drugi strani predstavlja veljaven del začetka SSL seje (handshake)
- Skype strežnik odgovori s TCP paketom, ki vsebuje zaporedje 0x1703010000, ki pa ni del SSL protokola.
- Zato lahko uporabimo FPM in iščemo pakete, ki prihajajo in vsebujejo to zaporedje znakov in jih blokiramo. In hkrati ne preprečujemo SSL sej.
- Najprej naložimo PHDF datoteki za IP in TCP

```
load protocol flash:ip.phdf
load protocol flash:tcp.phdf
```

FPM Primer 1 – preprečitev Skype prometa

- Definiramo class-map, da povemo FPM-ju, da naj pregleduje TCP pakete

```
class-map type stack match-all ip-tcp
  match field IP protocol eq 6 next TCP
```

- Definiramo class-map, ki išče zaporedje 0x17030100

```
class-map type access-control match-all skype
 match start TCP payload-start offset 0 size 4 eq
0x17030100
```

- Class-map povežemo v hierarhično policy-map

```
policy-map type access-control skype-policy
  class skype
 drop
```

Seznam IPv4 protokolov: http://en.wikipedia.org/wiki/List_of_IPv4_protocol_numbers

FPM Primer 1 – preprečitev Skype prometa

- Povežemo policy-mape skupaj

```
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy skype-policy
```

- Na koncu še povežemo policy-map in vmesnik, na katerem je priključen PC

```
Interface Fastethernet1/0
service-policy type acess-control output fpm-policy
```

FPM Primer 2 – preprečitev Bittorrent prometa

```
<?xml version="1.0" encoding="UTF-8" ?>
<tcdf>

<class name="bittorrent" type="access-control" match="any“>
    <match>
            <regex start="l2-start" offset="54" size="32" value="\x13BitTorrent\x20protocol" />
            <regex start="l2-start" offset="54" size="32" value="GET\x20.*\?info_hash=" />
            <regex start="l2-start" offset="54" size="32" value="[a|A][z|Z][v|V][e|E][r|R]\x01" />
    </match>
 </class>

<policy type="access-control" name="tcp_policy">
    <class name="bittorrent" />
    <action>drop</action>
 </policy>

 </tcdf>
```

Flexible Packet Matching

- Omejitve:

  Ne moremo uporabiti za preprečitev napadov, ki zahtevajo informacijo o stanju povezave (statefull).

  Zaradi tega ne moremo uporabljati za dinamično dogovorjene porte.

  Pozna samo IPv4 unicast pakete (ne podpira multicast).

  Ne zna pregledovati tunelov in MPLS vmesnikov.

  Odmik v definiciji je lahko le konstanta.

  Ne more pregledovati preko enega paketa.

FPM – Vpliv na zmogljivost usmerjevalnika

Flexible Packet Matching – Vpliv na CPU usmerjevalnika

- Vpliv na zmogljivost usmerjevalnika je odvisen od števila in vrste filtrov in protokolov.
- Primer vpliva na zmogljivost je meritev, ki je bila narejena na usmerjevalniku 7206VXR (128MB RAM, IOS 12.4(4)T).
- Meritev:

  Opisana v dokumentu “Flexible Packet Matching Deployment Guide”

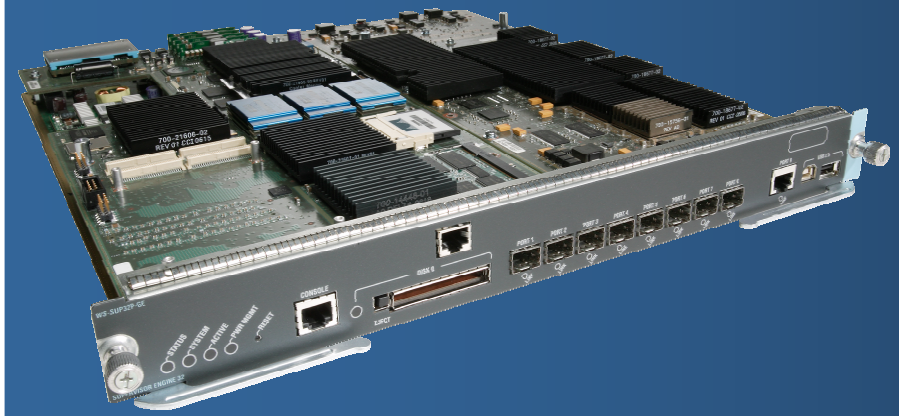
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6723/prod_white_paper0900aecd803936f6.html

Flexible Packet Matching – Vpliv na CPU usmerjevalnika

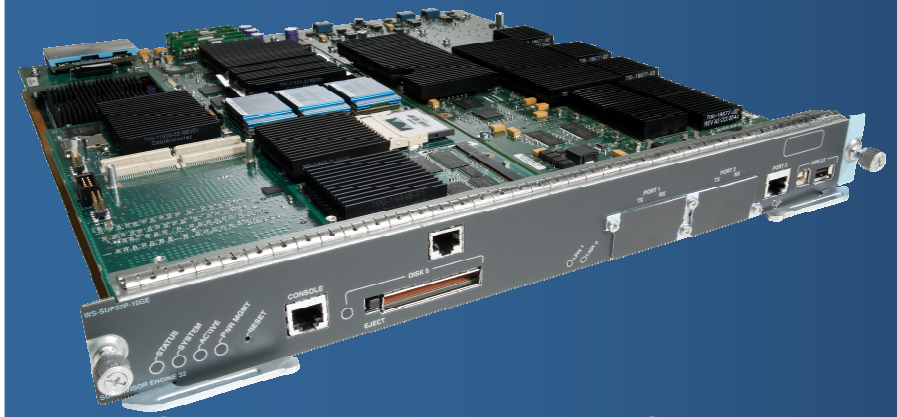
- Konfigurirano 10 FPM klas ali 10 ACL-ov
- 10 tokov (traffic streams)
- 50% tokov se ujame na 1., 5. ali 10. stavku ujemanja (match statement)
- STD: FPM politike ali ACL filtrira glede na IP izvorni naslov
- EXT: filtrira glede na IP naslov (izvor, ponor), TCP vrata (izvor, ponor), TCP protokol
- ALL: filtrira glede na IP naslov (izvor, ponor), območje TCP izvornih vrat, TCP ponorna vrata, TCP SYN zastavica

ACL-ALL-10-MATCH	39%	32%	40%	39%	39%

Supervisor Engine 32 PISA
= Sup32 + NBAR & FPM v strojni opremi



Supervisor Engine 32 PISA
8x1GE Uplinks + 1x 10/100/1000



Supervisor Engine 32 PISA
2x10GE Uplinks + 1x 10/100/1000

- NBAR
  - Prepoznavanje aplikacij in inteligentna klasifikacija
  - Multigigabit Performance

- Flexible Packet Matching
  - Hitra izvedba zaščite
  - Multigigabit Performance

- Idealen za varen dostop v LANu, distribucijski nivo, majhno in srednje veliko jedro, WAN dostop, SP dostop.

- Sup32 + NBAR & FPM v strojni opremi

FPM – Primerjava

Flexible Packet Matching – IOS FW in IOS IPS

- FPM je dopolnilna tehnologija IOS IPS-u in IOS FW-u in jima pomaga pri odstranjevanju škodljivega prometa iz mreže.
- FPM lahko uporabimo kot orodje za preprečevanje širjenja virusov, črvov ali drugih napadov. In to še prej preden pride podpis za IPS napravo.

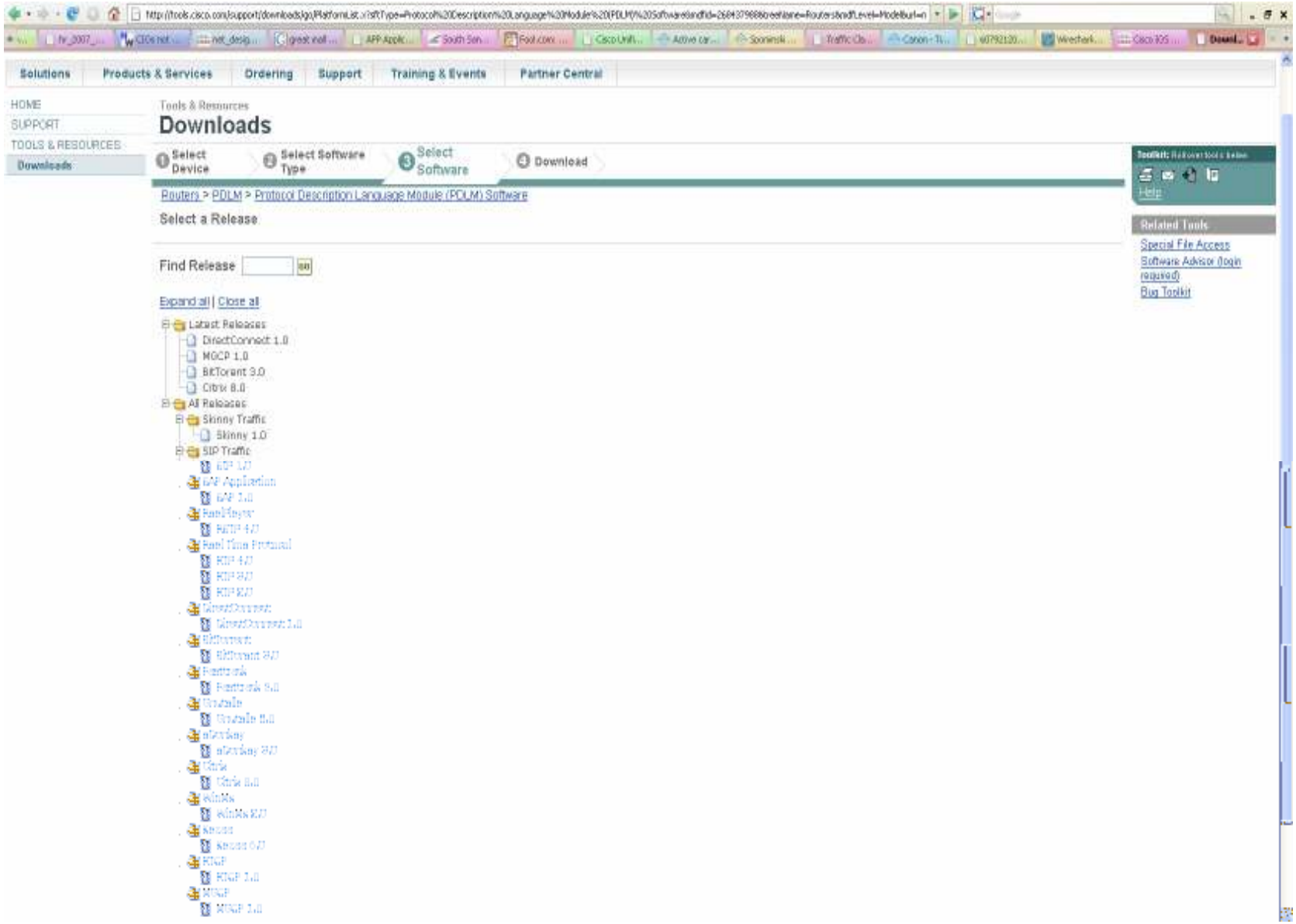
Flexible Packet Matching - NBAR

- **Razlika med FPM in NBAR**
- FPM je klasifikacija paketa brez upoštevanja stanja povezave (stateless) in je izboljšava obstoječi ACL tehnologiji. FPM pregleduje en paket naenkrat, brez zavedanja kaj je prišlo prej.
- NBAR se zaveda stanja seje (statefull). Informacija o seji (flow) je shranjena v pomnilniku in vsi naslednji paketi, ki so del te seje (flow), bodo obravnavani enako, brez tega, da bi bilo potrebno izvajati dodatno pregledovanje paketa.
- NBAR je namenjen zagotavljanju QoS (differentiated class of service).
- NBAR podpira le protokole za katere podporo napiše Cisco. Trenutno preko 90.
- Ko NBAR prepozna aplikacijo, jo lahko označi (marking), uveljavi politiko (policing) in jo nadzira (monitoring).
  - Zagotavljanje pasovne širine z uporabo algoritma Class-Based Weighted Fair Queuing (CBWFQ)
  - Omejevanje pasovne širine
  - Označevanje za potrebe Qos (ToS ali Diff Serv code points [DSCP])
  - Politika zavračanja paketov, ko pride do gneče (congestion) (Weighted Random Early Detection [WRED])

Protokoli, ki jih prepozna NBAR

Poslovne aplikacije	Varnost in tuneli	Elektronska pošta	Splet
Citrix ICA	GRE	IMAP	FTP
PCAnywhere	IPINIP	POP3	Gopher
Novadigm	IPsec	Exchange	HTTP
SAP	L2TP	Notes	IRC
Usmerjevalni protokoli	MS-PPTP	SMTP	Telnet
BGP	SFTP	**Direktoriji**	TFTP
EGP	SHTTP	DHCP/BOOTP	NNTP
EIGRP	SIMAP	Finger	NetBIOS
OSPF	HTTPS	R-commands	NTP
RIP	SIRC	DNS	Print
Upravljanje omrežja	SLDAP	Kerberos	X-Windows
ICMP	SNNTP	LDAP	**Multimedia**
SNMP	SPOP3	**P2P**	CU-SeeMe
Syslog	STELNET	BitTorrent	Netshow
RPC	SOCKS	Direct Connect	Real Audio
NFS	SSH	eDonkey/eMule	StreamWorks
SUN-RPC	**Glasovne komunikacije**	FastTrack	VDOLive
Podatkovne baze	H.323	Gnutella	RTSP
SQL*NET	RTCP	KaZaa2	RTP
MS SQL Server	MGCP	WinMX	MGCP
	SIP	**Signalizacija**	
	SCCP/Skinny	RSVP	

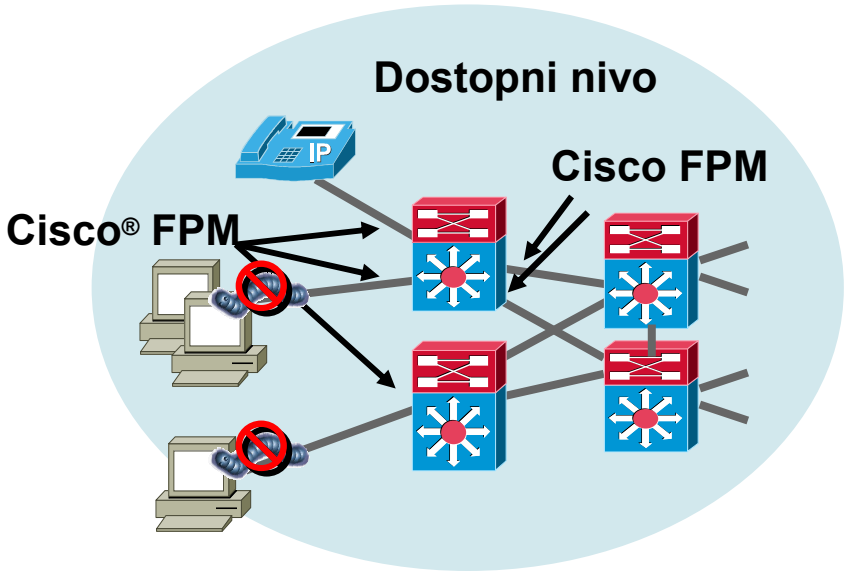
NBAR – PDLM datoteke na CCO

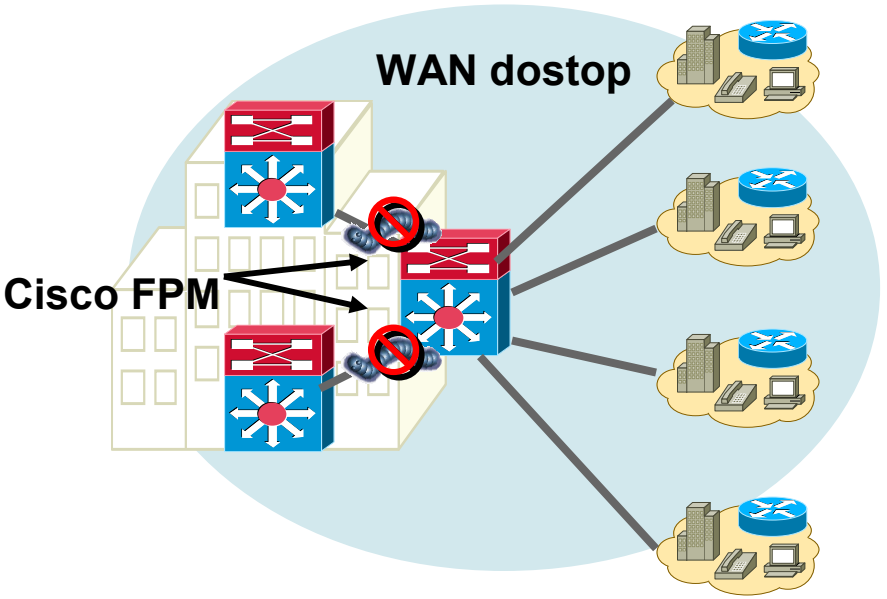


Kje uporabimo FPM?

Kje uporabimo FPM?

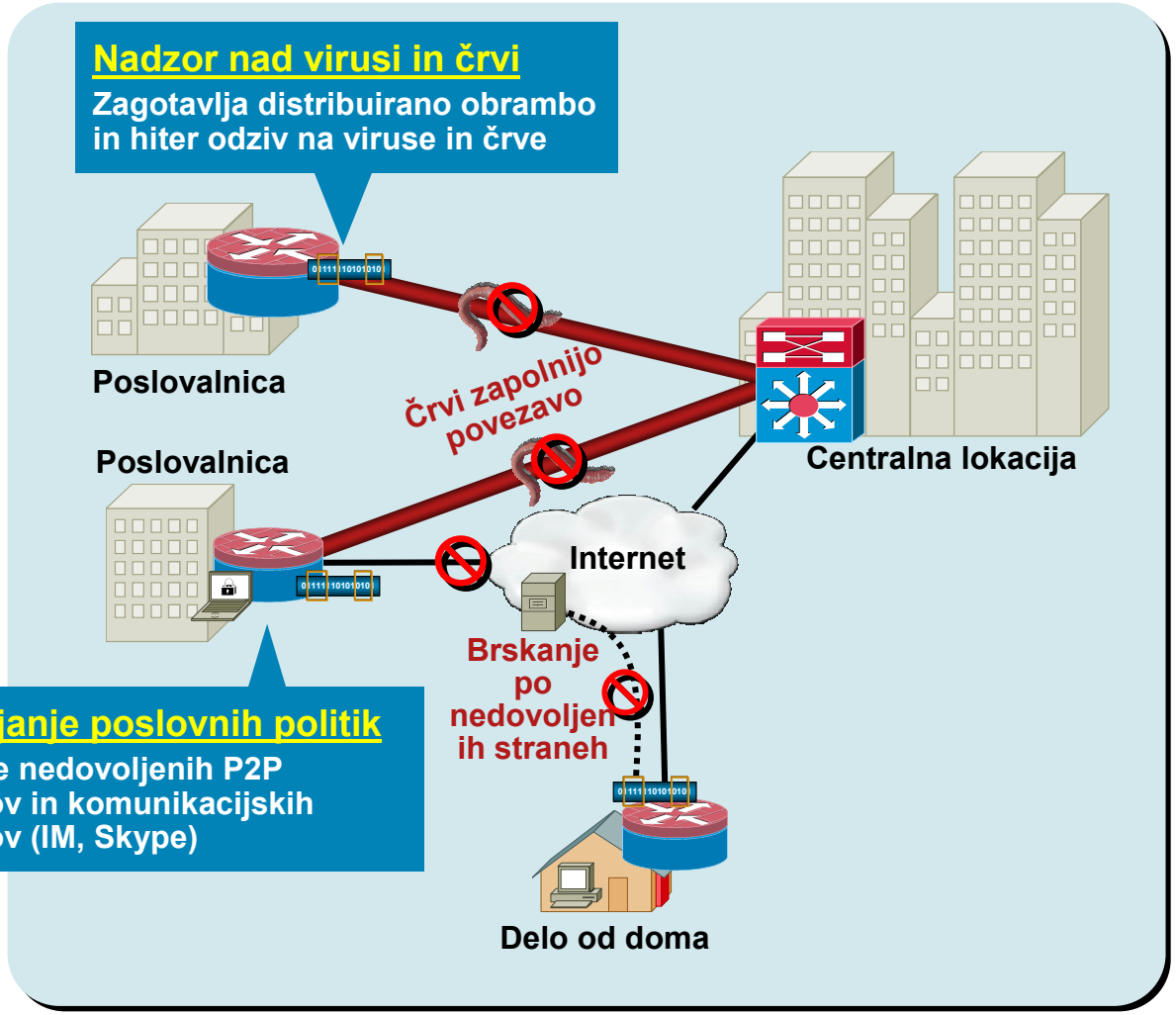
- Zaščita pred virusi in črvi na vstopnih točkah v omrežje (LAN in WAN)
- Uporabimo čimbolj na robu omrežja kot lahko
- Hiter odgovor na nove napade, preden se razširijo v ostale dele omrežja: zato je pomembna delitev omrežja v skladu z ECNM



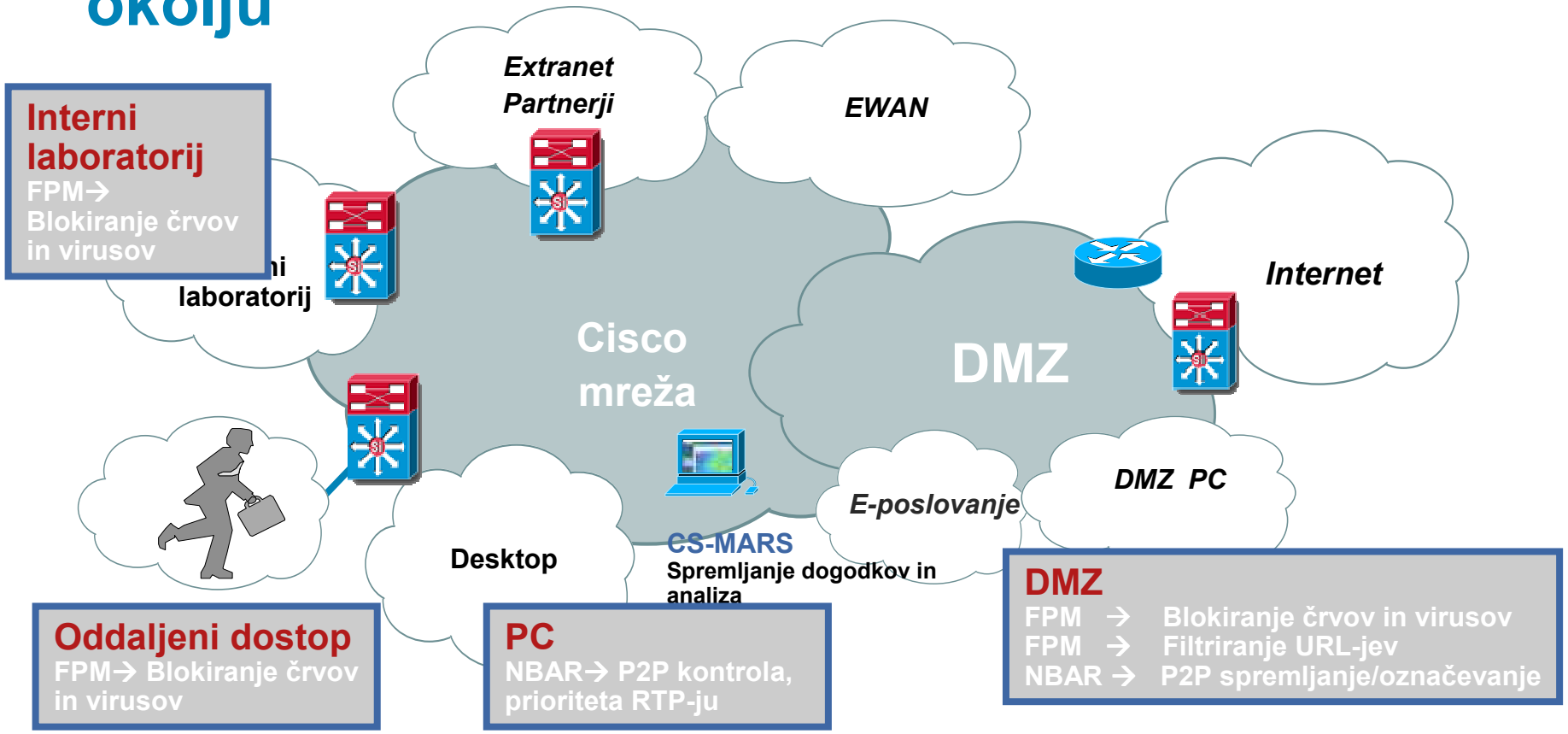


FPM na oddaljeni lokaciji

- Če viruse in črve zaustavimo preden se začnejo širiti preko WAN omrežja, prihranimo kapacitete povezav
- Uveljavljamo politike in zaustavimo P2P aplikacije, Skype in podobno



Kako Cisco uporablja PISA FPM v svojem okolju



- "Cisco IT is excited about the PISA hardware's ability to perform FPM to greatly extend the capabilities of access-control lists to more intelligently use the network infrastructure to filter emerging security threats. The ability to dynamically classify P2P and RTP protocols allows us to make better decisions about which packets should receive preferential scheduling in our internet DMZs. We are exploring the opportunity to deploy this new technology into our DMZ, extranet and remote access hub locations."
  -- Ben Irving, Cisco IT Architect

Flexible Packet Matching - Povzetek

- Naslednja generacija ACL-ov
- Pregledovanje enega paketa naenkrat, brez zavedanja seje
- Preprečevanje širjenja virusov in črvov
- Del IOS-a na usmerjevalnikih in Supervisor 32 PISA
- Sami definiramo protokole
- Uporaba XML-a za opis protokolov in prometa (class-map)

Vprašanja in odgovori