aruba
a Hewlett Packard Enterprise company

APPRF 6.X & 8.X

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
Nov 27th, 2018

Presenter: Pagalavan Karunanidhi

Pagalavan-karunanidhi@hpe.com

AIRHEADS COMMUNITY

AGENDA

- **Platform Support and DPI enabling**
- **Application DPI Engine and Categories**
- **Application Control**
- **Dashboard Application based blocking workflow**
- **Application Bandwidth Contracts**
- **High-Level Datapath and Controller Architecture**
- **Troubleshooting Tips**
- **AppRF in 8.x**

What is AppRF?

AppRF is a PEF feature on the ArubaOS controllers. It is designed to give network administrators insight into the applications that are running on their network, and who is using them.
Aruba has extended the network intelligence offered by our unique, market leading firewall to include powerful heuristics and visualization techniques. Together, these give customers a real-time and historical (using airwave) view of who is using what applications, and when.

AppRF collects data from the network activity of authenticated users and uses this data to build pie charts and lists of the top applications (approximately 150 applications), destinations, WLANs, users, and device types. These results are based on the volume of traffic in each of these categories.

AppRF 2.0 Platform Support

- Supported on the 72xx and 70xx platforms
- Not supported on the M3, 3000, 650
- Solution supports mixed 7xxx/older controllers as follows:
  - App level rules can be configured on ‘legacy’ master controllers
  - App rules get pushed to local controllers, but won’t take effect on legacy controllers

Features	Controller Platform				
	72xx	70xx	3600 / M3	3400 / 3200	650 / 620
AppRF Control (6.4)	Y	Y	N	N	N
URL Content Filter (WebCC) (6.4.2)	Y	Y	N	N	N
AppRF Visibility (6.3)	Y	Y	Y	Y	N

What is Application-Aware DPI?

Uses a combination of advanced techniques for application identification:

1. Website URL information identifies popular websites
2. Signatures are used for “easy to identify” applications
   Allows advanced REGEX to be used for performance scaling
3. Uses protocol grammar analysis to understand complex applications and their current state
4. Uses advanced heuristics when required
5. Detects encrypted applications via certificate common names

•To be leveraged in a future releases:

- •Decodes applications inside *unencrypted* tunnels such as ICA
- •Understands and extracts metadata to increase context

AOS 6.4 - AppRF 2.0

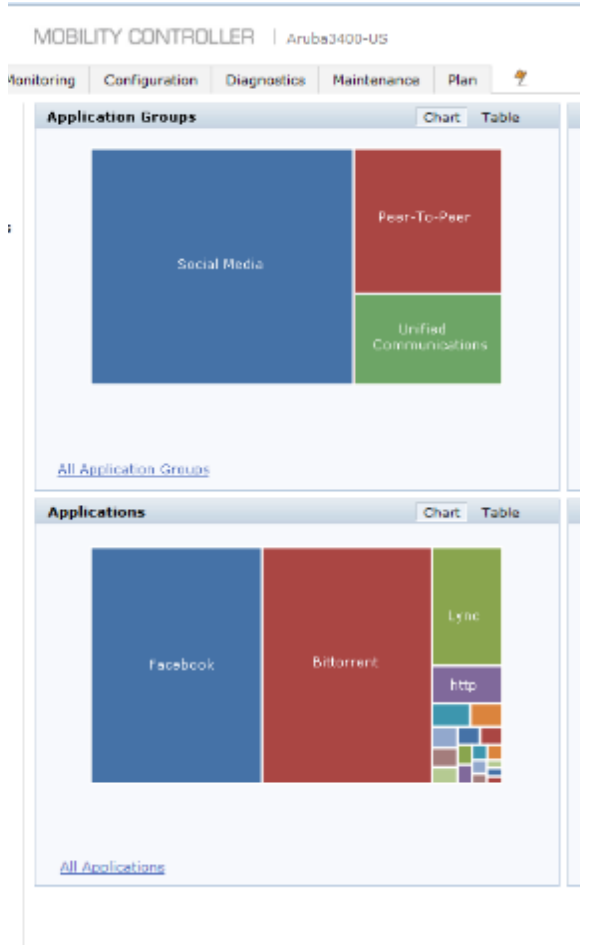
1)Incorporates Application-Aware Deep Packet Inspection technology
Uses next-gen techniques, not just signatures
Over 1500 Applications

2)Operates at user role level to provide application control
Block application or categories of apps

- QoS applications
- Bandwidth contracts for applications

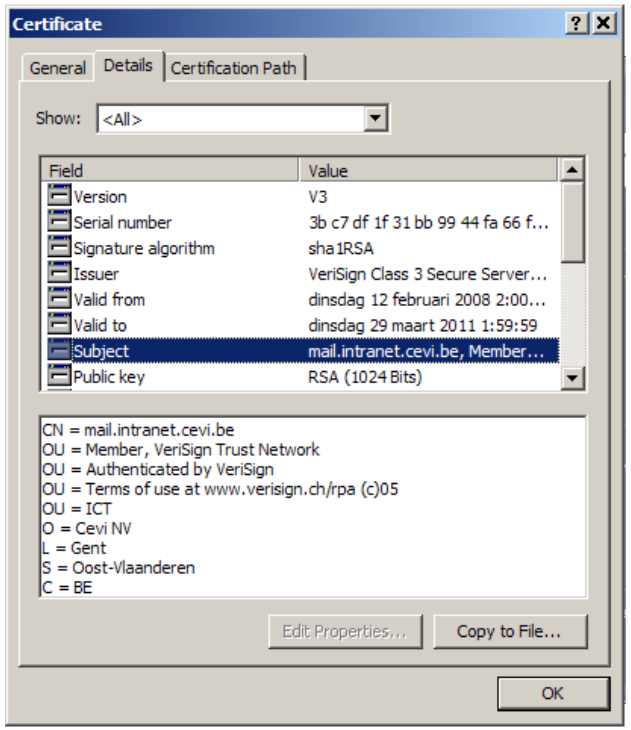
AOS 6.4 - AppRF 2.0

- New Category Dashboard element
- Shows apps by category such as Peer-to-Peer, Streaming video
- New Graphically based application blocking work flow
- New “Global Policy” for easy application of ACLs to all users



Encrypted Applications

- Primary method of classification for encrypted flows is use of the unencrypted certificate information
  - Primarily Common Name
- Certificate is exchanged as part of the initial application startup
- Only allows granularity reflected in the cert name
  - All of facebook, for example, uses a cert with “Facebook” as the CN
- Extraction of metadata or any deeper analysis isn’t possible



Application Categories

- Categories are designed to be actionable – control a specific type of user traffic

- Can be used exactly the same way as applications or L4 rules in security policies
  - With a few exceptions, still processed top to bottom – more later

- Can also be used interchangeably with applications in Bandwidth contracts
  - Most specific takes precedence – more on BW contracts later

- Static – built into the image
  - Will likely change slightly over time

- In a future release, users will be able to create their own categories

AOS 6.4 - AppRF 2.0

```
(1810-7210) #show dpi application category all

Application Categories
----------------------
Name                    App Category ID
Applied
----                    ---------------  ------
-
antivirus               1                0
authentication          2                0
cloud-file-storage      3                0
collaboration           4                0
encrypted               5                0
enterprise-apps         6                0
gaming                  7                0
im-file-transfer        8                0
instant-messaging       9                0
mail-protocols          10               0
mobile-app-store        11               0
```

```
Name                    App Category ID
Applied
----                    ---------------  -----
-
network-service         12               0
peer-to-peer            13               0
social-networking       14               0
standard                15               0
streaming               16               0
thin-client             17               0
tunneling               18               0
unified-communications  19               0
web                     20               0
webmail                 21               0

Total application groups = 21
```

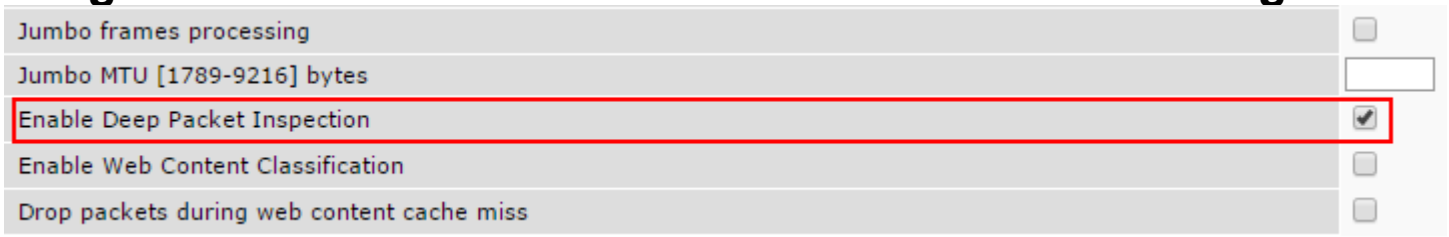
Showing the contents of an individual category

```
(1810-7210) #show dpi application category gaming

List of Applications
--------------------
Name              App ID  App Category  Default Ports                                                    Applied
----              ------  ------------  -------------
all-slots-casino  762     gaming        tcp 80                                                           0
cstrike           23      gaming        tcp 27030-27039  udp 1200 27000-27015                            0
eve-online        1112    gaming        tcp 80 26000                                                     0
everquest         1282    gaming        tcp 80 7000 7100  udp 3016-3021 9100 9700-9703 32800-33000
0
halflife          590     gaming        udp 6003 7002 27010 27015 27025                                  0
imvu              809     gaming        tcp 80                                                           0
lineage2          1283    gaming        tcp 53 80 2009 2106 7777  udp 53 80 2009 2106 7777               0
poker-stars       899     gaming        tcp 80 443                                                       0
psn               601     gaming        tcp 80 443                                                       0
quake             157     gaming        tcp 27650 27950 27952 27960 27965 28004  udp 27650 27950 27952 27960
27965 28004    0
runescape         309     gaming        tcp 80 443 43594-43595                                           0
steam             339     gaming        tcp 80 27014-27050  udp 1024-65535                               0
wfc               591     gaming        tcp 443                                                          0
wiiconnect24      600     gaming        tcp 80                                                           0
wow               340     gaming        tcp 80 1119-1120 3724 4000  udp 6112-6114 6881-6999              0
xboxlive          342     gaming        tcp 53 80 3074  udp 53 80 3074                                   0

Total applications in this category = 16
```

Enabling DPI

WebUI:

Configuration-> Advanced Services->Stateful Firewall -> global Settings



CLI:

```
(MM7210) (config) #firewall dpi
Warning: Application visibility is enabled, this change would take effect after controller reload
```

If controller is not rebooted, 'show firewall' output:

```
DPI Classification    Enabled (*Requires controller reload to take effect*) [Cfg: enabled, PEF
license: installed]
```

Note: 'firewall dpi' is a local command to be enabled per controller

AppRF 2.0 - Features

Application-Aware Deep Packet Inspection (DPI)

Over 1500 applications (6.4.2.5)

Categories of Application on Dashboard

21 application categories (6.4.2.5)

Application Control at the user role level

- Block applications/categories of apps
- QoS applications
- Throttle applications through bandwidth contracts

Graphically based application blocking workflow

Application Bandwidth Contracts

ArubaOS Layer 4 Firewall Behavior

- **Policy is defined as**
  - *Source ip, dest ip, source(6.3+)/proto-port/service, action*
- **ACL actions**
  - *Firewall actions - permit and deny*
  - *Forwarding actions - src-nat, dst-nat, dual-nat and redirect*
  - *Other actions – blacklist, log, mirror, dot1p-priority, time-range, tos*
- **Other than deny, all actions mean implicit permit**
  - *src-nat implicitly means permit and src-nat*
- **Current ACL behavior – Stop on first ACE match**
  - *Also followed by every firewall vendor as best practice*

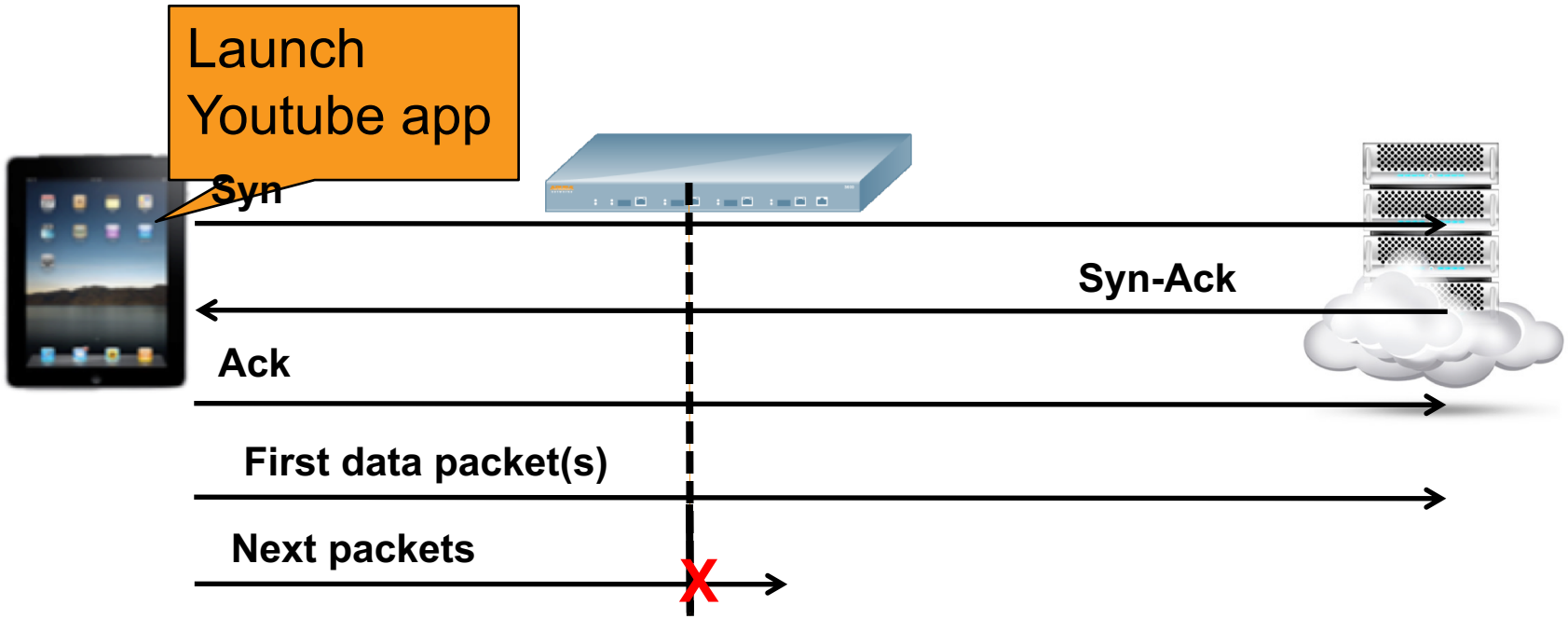
ArubaOS Layer 7 Firewall

- **Policy definition extended to include applications:**

```
(MM7210) (config-sess-test_app)#any any ?
<0-255>                 IP protocol number
STRING                  Name of network service
any                     Match any traffic
app                     Application Name
appcategory             Application Category Name
icmp                    Internet Control Message Protocol
tcp                     Match TCP traffic
udp                     Match UDP traffic
```

- **Application classification requires matching packet contents -**
  - *May need one or more packets in both directions before taking action*
  - *Worse case classification can **take 9 round trips***
- Therefore, rules matching any app rule must "leak" packets until the classification is complete

App-based rules create (temporary) implicit Allow



Example:

```
ip access-list session no-gmail
   any any app gmail deny
   any any any permit
```

Pre-classification: the ACL will be converted in datapath as follows, assuming that gmail is served in TCP 443:

```
ip access-list session no-gmail
   any any tcp 443 permit
   any any any permit
```

Post-classification: the ACL is enforcement will be:

```
ip access-list session no-gmail
   any any [tcp 443 & appID "gmail"] deny
   any any any permit
```

Policies restrictions

Datapath functional design:

IP/TCP/UDP headers of a leaked session SHOULD NOT change after classification.

Two Constraints/restrictions:

1. **App rules with forwarding actions do not make sense and will not be allowed.**
2. **In case of policies with mixed forwarding and application rules, the processing order is as follows:**
   Forwarding rules are processed FIRST in the flow
   When classification is complete, the actions (permit/deny/QoS) specified in the application rules are implemented

No Mixing of Application and Forwarding in a Rule

```
any any app facebook src-nat
any any app twitter dst-nat
any any deny
```

What is wrong with the above example?

- **Should we scr-nat all traffic until we classify it?**
- **What to do with non-facebook traffic after classification, since they are already established in datapath with NAT?**
- **The second rule will never be hit with traditional layer 4 rules.**

Mixing forwarding and application rules

- **How do we handle a mix of forwarding and application rules such as these?**

```
any any app netflix permit tos 60
any any tcp 443 src-nat
any any any deny
```

1. **We scan the policy for forwading rules to process first:**
   - All tcp 443 traffic will get source NAT'ed until classification is complete
2. **Once the app is classified, we process the app rule:**
   - Netflix traffic is permitted with tos 60 AND remain src-nat'ed

DPI Policies Example - 1

```
ip access-list session app-acl
    any any app facebook permit
    any any appcategory social-networking deny
    any any any permit
```

```
(MM7030) #show datapath session dpi | include facebook,linkedin
```

Source IP	Destination IP	Prot	SPort	DPort	Int-Flag	AppID	AceIdx	Flags
10.163.160.111	173.252.88.66	6	58049	443	145	facebook (244)	852/846	FC
173.252.122.1	10.163.160.111	6	443	58048	144	facebook (244)	852/846	
108.174.10.10	10.163.160.111	6	80	58093	144	linkedin (305)	851/847	FD
10.163.160.111	108.174.10.10	6	58093	80	145	linkedin (305)	851/847	FDC
173.252.88.66	10.163.160.111	6	443	58049	144	facebook (244)	852/846	F
10.163.160.111	173.252.122.1	6	58048	443	145	facebook (244)	852/846	C

DPI Policies Example - 2

```
ip access-list session appcat-acl
    any any appcategory social-networking deny
    any any app facebook permit
    any any any permit
```

```
(MM7030) #show datapath session dpi | include facebook
Source IP       Destination IP  Prot SPort DPort  Int-Flag AppID             AceIdx   Flags
--------------- --------------- ---- ----- -----  -------- --------------- --------- -----
10.163.160.111  173.252.88.68   6    57926 443    145      facebook (244 )  820/814  FDYC
173.252.88.128  10.163.160.111  6    443   57927  144      facebook (244 )  820/814  FD
173.252.88.68   10.163.160.111  6    443   57926  144      facebook (244 )  820/814  FDY
173.252.88.68   10.163.160.111  6    443   57925  144      facebook (244 )  820/814  FD
10.163.160.111  173.252.88.68   6    57925 443    145      facebook (244 )  820/814  FDYC
10.163.160.111  173.252.88.128  6    57927 443    145      facebook (244 )  820/814  FDC
```

Unclassified Applications

After some 8-9 packets of round trips, we will give up on classifying the application

Unclassified Applications  Unknown Traffic Flow

Unclassified applications not matching any L3 rules will take the default action specified in the ACL list

Unclassified apps not matching L3 rules will be blocked in this example

```
any any app facebook permit tos 60
any any tcp 443 permit
any any any deny log
```

Unknown flow on port 80 will hit the default action in this ACL.

New Policy Containers

- **New Dashboard-based Workflow introducing two policy containers (ACL) created by default:**
  - Global ACL, namely global-sacl
  - AppRF user-role ACL, namely apprf-role_name-sacl
- **Rules under Global ACL apply to all user-roles**
- **Global ACL will always be in position 1 of every user-role**
- **Rules under AppRF user-role ACL apply to only specific role**
- **AppRF user-role ACL will always be in position 2 of every user-role**
- **These ACLs support only App based rules and their positions can not be altered**

Global and AppRF policies in every user role

Security > Access Control > User Roles

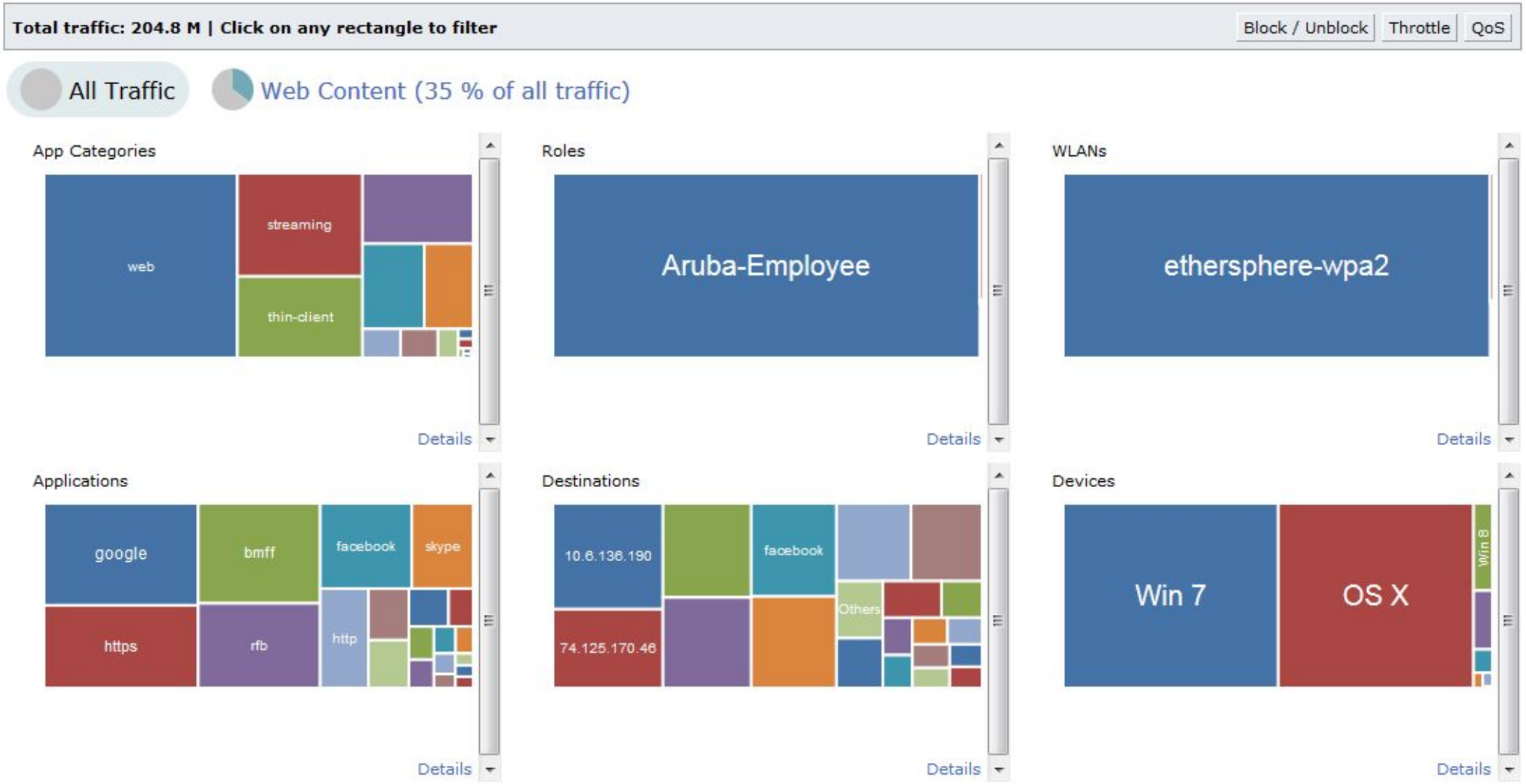
User Roles | System Roles | Policies | Time Ranges | Guest Access

Name	Firewall Policies
authenticated	global-sacl/,apprf-authenticated-sacl/,ra-guard/,allowall/,v6-allowall/
default-via-role	global-sacl/,apprf-default-via-role-sacl/,allowall/
default-vpn-role	global-sacl/,apprf-default-vpn-role-sacl/,ra-guard/,allowall/,v6-allowall/
guest	global-sacl/,apprf-guest-sacl/,ra-guard/,http-acl/,https-acl/,dhcp-acl/,icmp-acl/,dns-acl/ dhcp-acl/,v6-icmp-acl/,v6-dns-acl/
guest-logon	ra-guard/,logon-control/,captiveportal/,v6-logon-control/,captiveportal6/
logon	ra-guard/,logon-control/,captiveportal/,vpnlogon/,v6-logon-control/,captiveportal6/

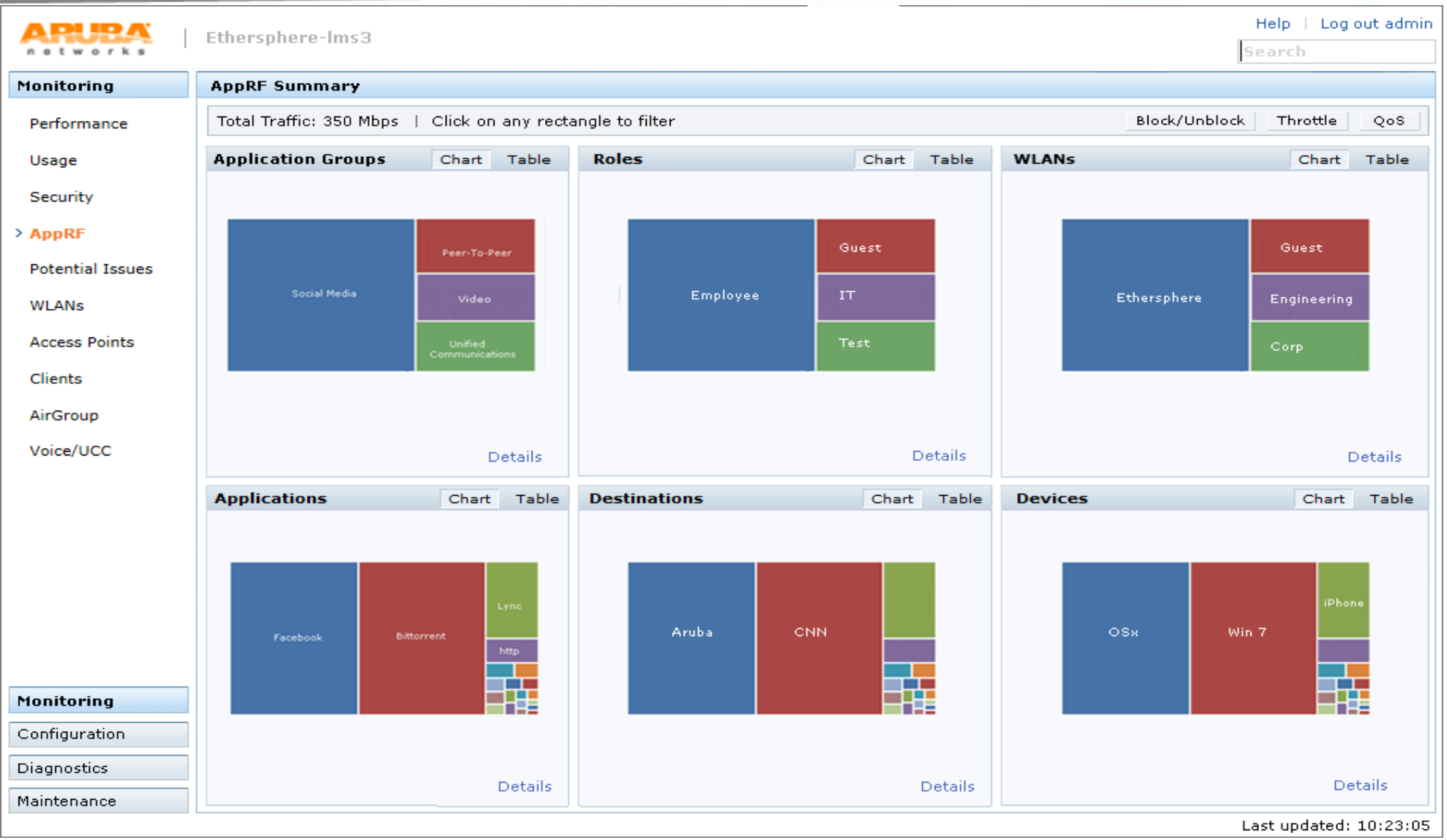
Global and Per-Role ACLs

```
access-list List
----------------
Position  Name                Type     Location
--------  ----                ----     --------
1         global-sacl         session
2         apprf-wpa2psk-sacl  session
3         wireless            session


global-sacl
-----------
Priority  Source  Destination  Service  Application      Action  TimeRange  Log  Expired  Queue  TOS
--------  ------  -----------  -------  -----------      ------  ---------  ---  -------  -----  ---
1         any     any                   app bittorrent   deny                           Low


apprf-wpa2psk-sacl
------------------
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS  802
--------  ------  -----------  -------  -----------  ------  ---------  ---  -------  -----  ---  ---
1         any     any                   app netflix  deny                           Low


wireless
--------
Priority  Source  Destination  Service    Application                    Action             TimeRange
--------  ------  -----------  -------    -----------                    ------             ---------
1         any     any                     appcategory instant-messaging  permit
2         any     any                     app facebook                   deny
3         any     any                     app amazon                     permit
5         any     any          tcp 3389                                  deny
7         any     any          any                                       redirect tunnel 1
```

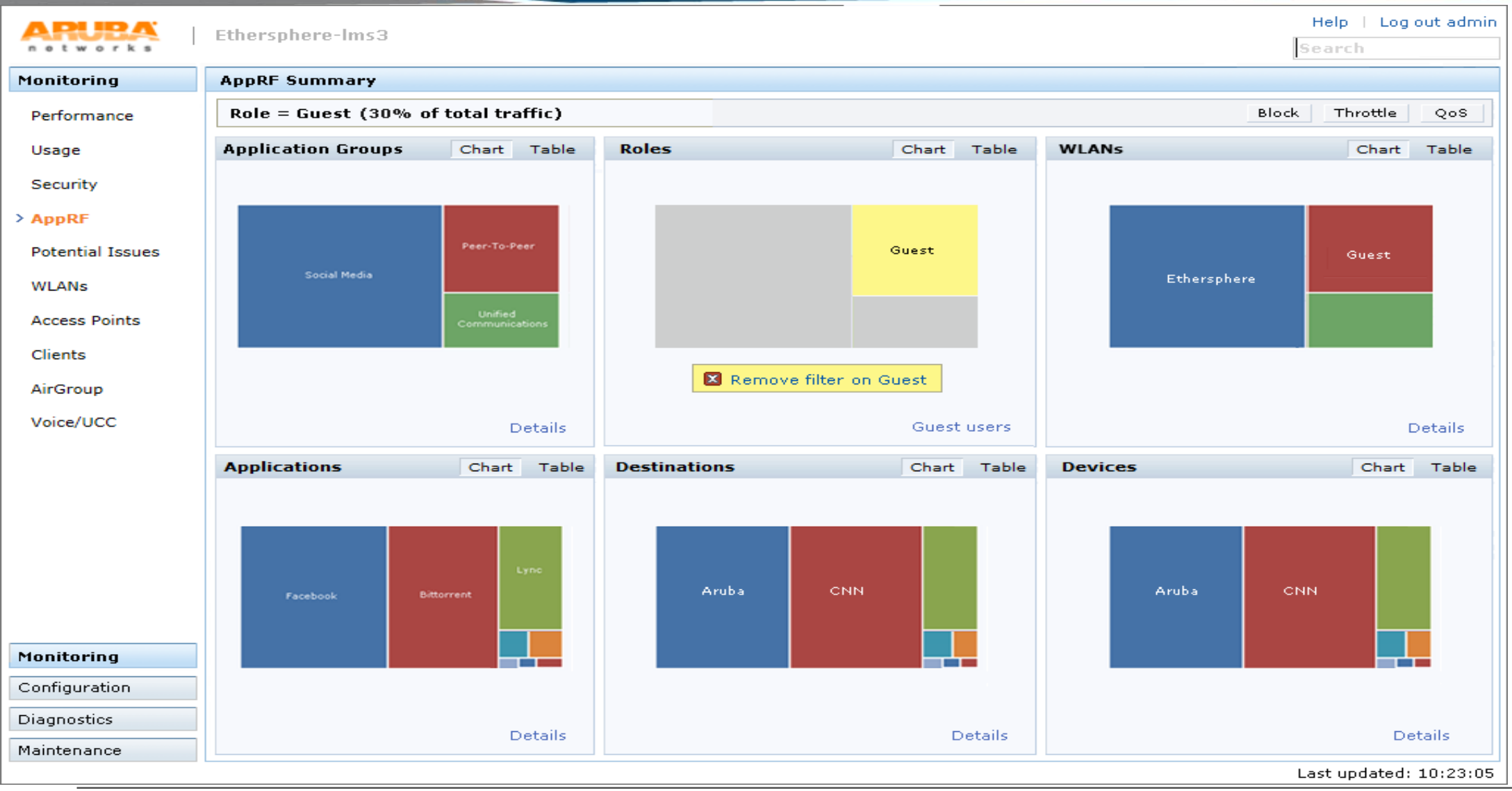
Improved Application Visibility and Control



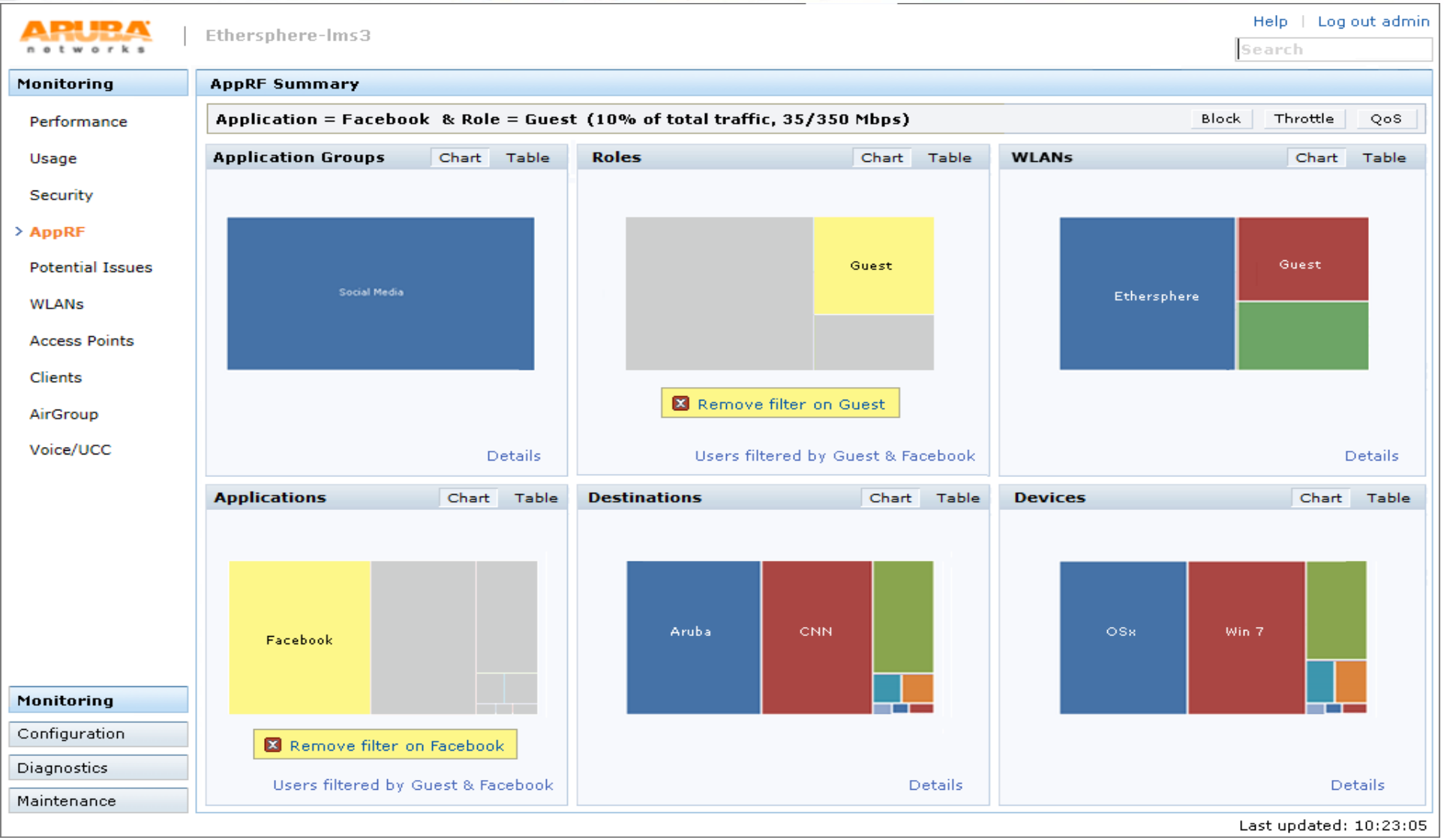
Improved Application Visibility and Control



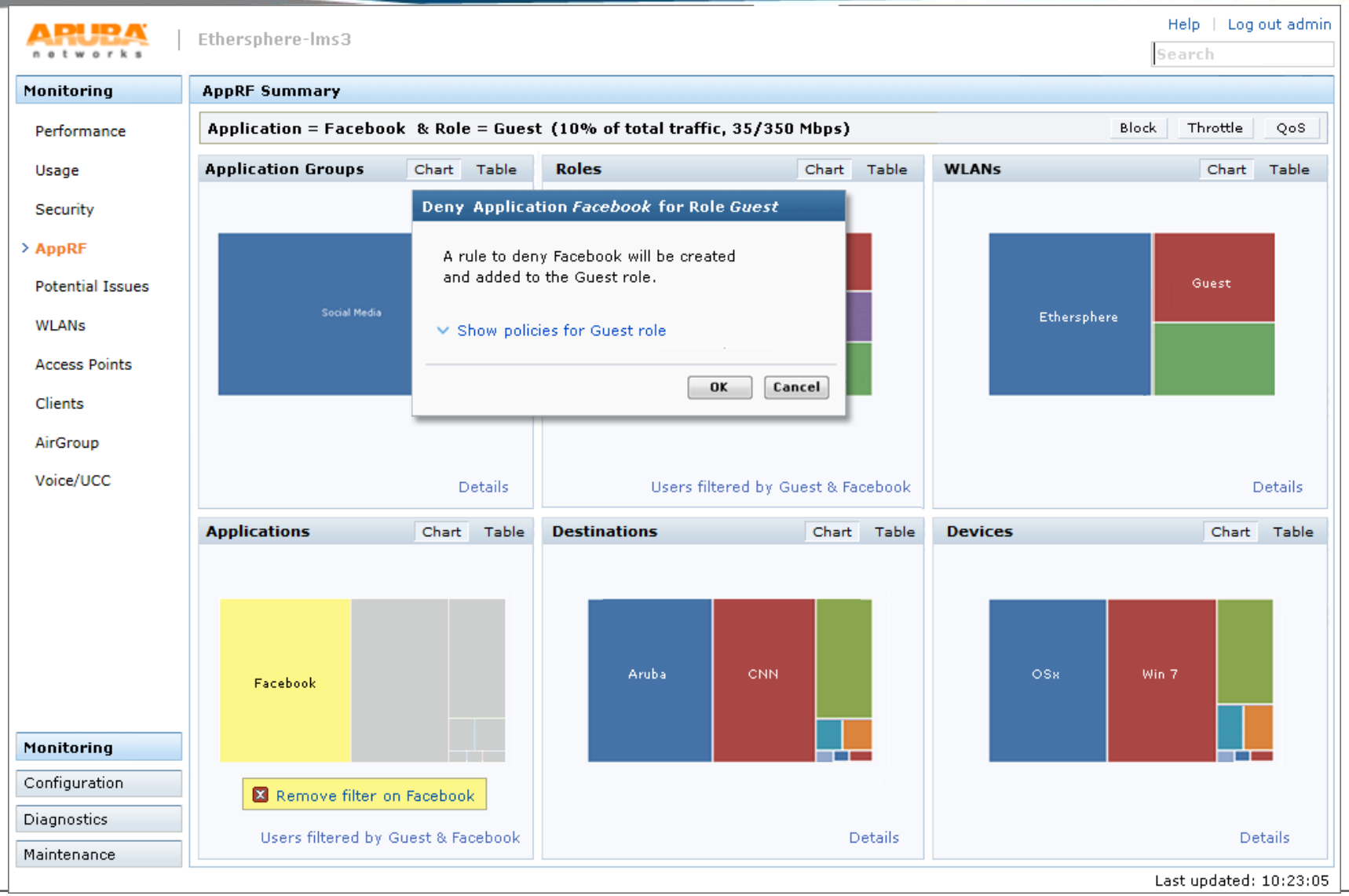
Cont..


ARUBA networks
Ethersphere-lms3
Help | Log out admin
Search
Monitoring
Performance
Usage
Security
AppRF
Potential Issues
WLANs
Access Points
Clients
AirGroup
Voice/UCC
Monitoring
Configuration
Diagnostics
Maintenance
AppRF Summary
Role = Guest (30% of total traffic)
Block
Throttle
QoS
Application Groups
Chart
Table
Social Media
Peer-To-Peer
Unified Communications
Details
Roles
Chart
Table
Guest
Remove filter on Guest
Guest users
WLANs
Chart
Table
Ethersphere
Guest
Details
Applications
Chart
Table
Facebook
Bittorrent
Lync
Details
Destinations
Chart
Table
Aruba
CNN
Details
Devices
Chart
Table
Aruba
CNN
Details
Last updated: 10:23:05

Cont..


ARUBA networks
Ethersphere-lms3
Help | Log out admin
Search
Monitoring
Performance
Usage
Security
AppRF
Potential Issues
WLANs
Access Points
Clients
AirGroup
Voice/UCC
Monitoring
Configuration
Diagnostics
Maintenance
AppRF Summary
Application = Facebook & Role = Guest (10% of total traffic, 35/350 Mbps)
Block
Throttle
QoS
Application Groups
Chart
Table
Social Media
Details
Roles
Chart
Table
Guest
Remove filter on Guest
Users filtered by Guest & Facebook
WLANs
Chart
Table
Ethersphere
Guest
Details
Applications
Chart
Table
Facebook
Remove filter on Facebook
Users filtered by Guest & Facebook
Destinations
Chart
Table
Aruba
CNN
Details
Devices
Chart
Table
OSx
Win 7
Details
Last updated: 10:23:05

Cont..


ARUBA networks
Ethersphere-lms3
Help | Log out admin
Search
Monitoring
Performance
Usage
Security
AppRF
Potential Issues
WLANs
Access Points
Clients
AirGroup
Voice/UCC
Monitoring
Configuration
Diagnostics
Maintenance
AppRF Summary
Application = Facebook & Role = Guest (10% of total traffic, 35/350 Mbps)
Block
Throttle
QoS
Application Groups
Chart
Table
Social Media
Details
Roles
Chart
Table
Deny Application Facebook for Role Guest
A rule to deny Facebook will be created and added to the Guest role.
Show policies for Guest role
OK
Cancel
Users filtered by Guest & Facebook
WLANs
Chart
Table
Ethersphere
Guest
Details
Applications
Chart
Table
Facebook
Remove filter on Facebook
Users filtered by Guest & Facebook
Destinations
Chart
Table
Aruba
CNN
Details
Devices
Chart
Table
OSx
Win 7
Details
Last updated: 10:23:05

Application Bandwidth Contracts

- **Global Bandwidh contracts for applications and application groups**

Apr 2 14:26:00 webui[3281]: USER:admin@104.36.248.10 COMMAND:<**dpi global-bandwidth-contract appcategory "mobile-app-store" upstream mbits 2** > -- command executed successfully

Apr 2 14:26:00 webui[3281]: USER:admin@104.36.248.10 COMMAND:<**dpi global-bandwidth-contract appcategory "mobile-app-store" downstream mbits 10** > -- command executed successfully

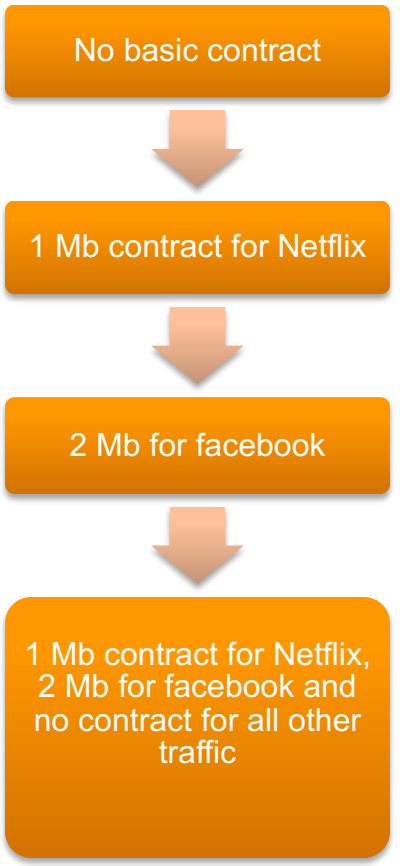
- **AppRF supports only Role-Based Bandwidth contracts**
  - Not Per-User or AP-Group

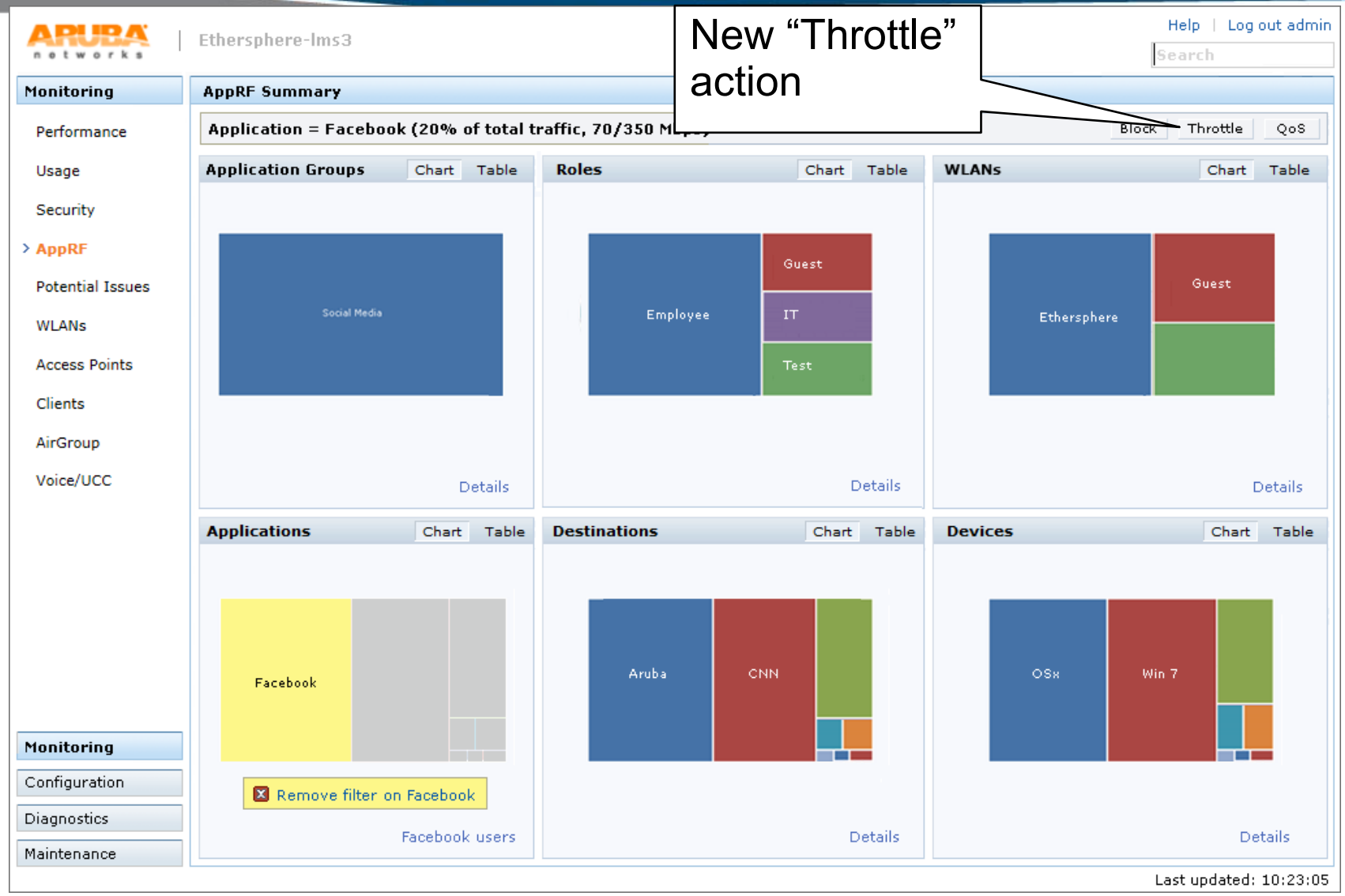
Apr 2 14:47:42 webui[3281]: USER:admin@104.36.248.10 COMMAND:<**aaa bandwidth-contract "authenticated-netflix-dw-bw" mbits 5** > -- command executed successfully

Apr 2 14:47:42 webui[3281]: USER:admin@104.36.248.10 COMMAND:<**user-role "authenticated" bw-contract app "netflix" "authenticated-netflix-dw-bw" downstream** > -- command executed successfully

- **Application-based and "generic bandwidth based" contracts can co-exist**

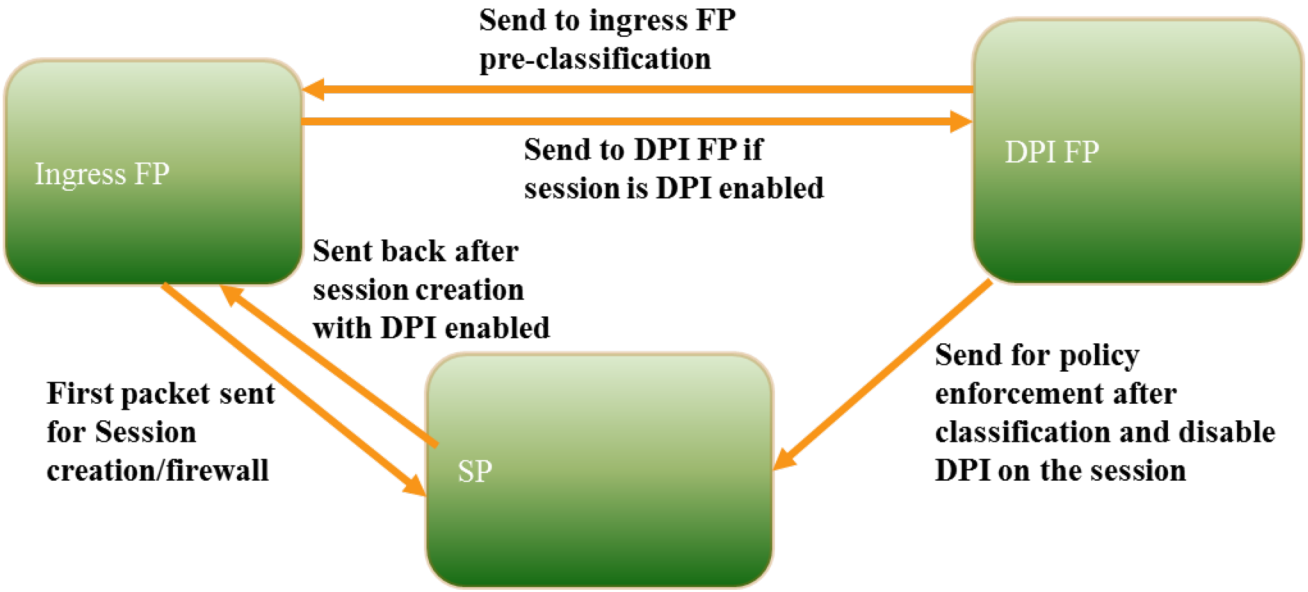
Bandwidth Contract Examples



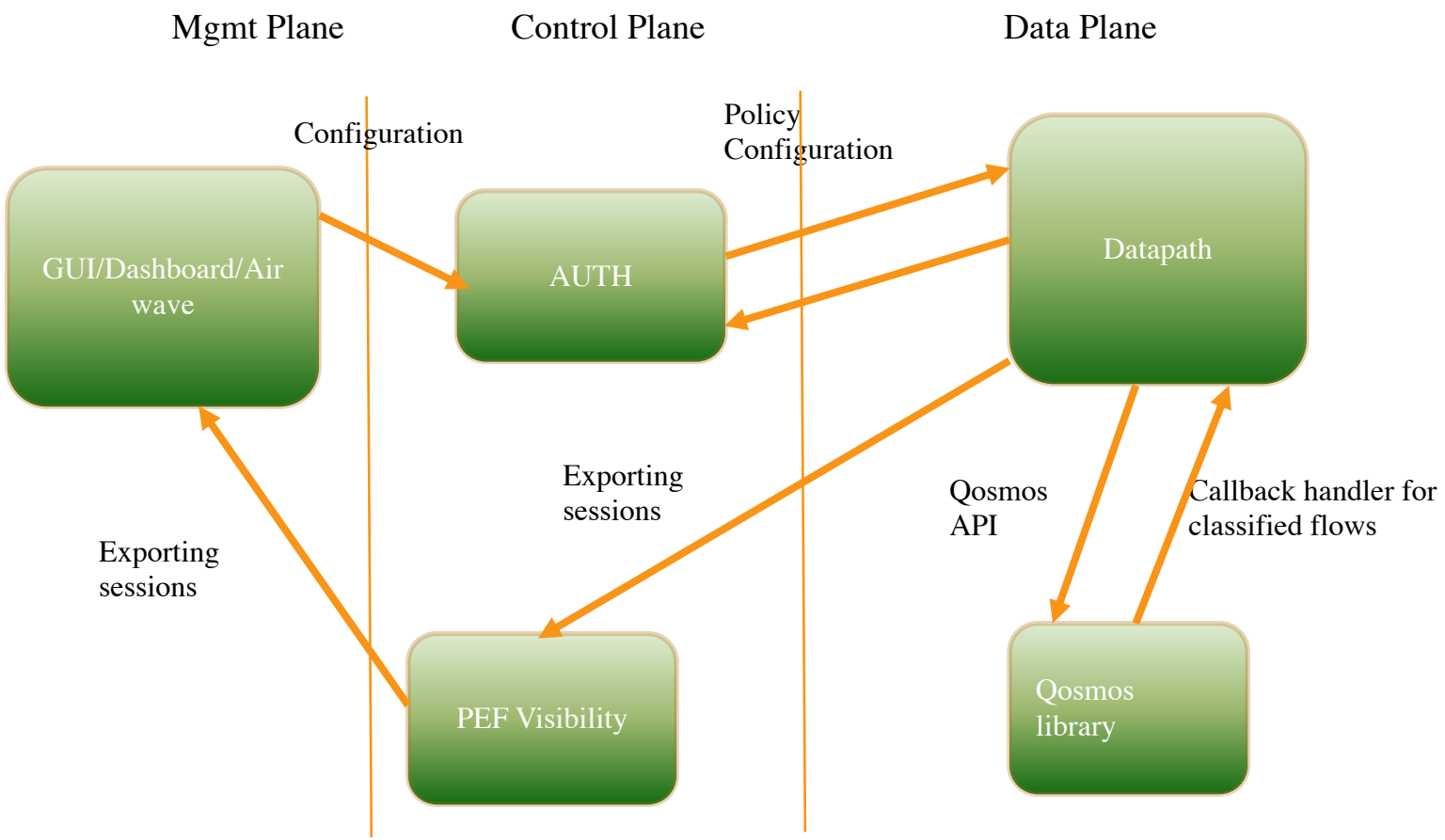

New “Throttle” action
Ethersphere-lms3
Help | Log out admin
Search
Monitoring
Performance
Usage
Security
AppRF
Potential Issues
WLANs
Access Points
Clients
AirGroup
Voice/UCC
AppRF Summary
Application = Facebook (20% of total traffic, 70/350 M
Block
Throttle
QoS
Application Groups
Chart
Table
Social Media
Details
Roles
Chart
Table
Employee
Guest
IT
Test
Details
WLANs
Chart
Table
Ethersphere
Guest
Details
Applications
Chart
Table
Facebook
Remove filter on Facebook
Facebook users
Destinations
Chart
Table
Aruba
CNN
Details
Devices
Chart
Table
OSx
Win 7
Details
Monitoring
Configuration
Diagnostics
Maintenance
Last updated: 10:23:05

High-Level Datapath Architecture

- New DPI thread added for the classification
  - 1 thread used on 7210 and 70xx
  - 4 threads used on 7220, 7240
- Packets will be sent to this thread until they are classified or we give up
  - After 8-9 packets, we will classify as “Not-Classified”
- Flow returned to fast path post classification



High-Level Controller Architecture



Note on Performance Impact

- **There is no performance impact for a flow if there are no DPI rules configured for its policy**
- **Once DPI rules are applied, there will be an impact on session establishment, since the packets must be sent to the DPI slow path**
  - Varies by application
- **Crypto throughput numbers with DPI turned on are 25-30% less on 7240 than DPI Disabled as we take out 4 FPCPUs for DPI**
- **There is no increase in latency after a connection is classified and exits the DPI slow path**

APPRF TROUBLESHOOTING TIPS

aruba
a Hewlett Packard Enterprise company

Know your ACLs

- **show acl acl-table | include <User-role>** => Role ACL number
- **Show acl ace-table acl xx** => list of ACE numbers in datapath
- **show datapath acl id 65** => ACL hits in datapath
- **Check ACLs hits in the datapath**
- **Examples:**

```
(MM7030) (config) # show acl acl-table | include dpi-role
ACL  Type        ACE Index  Rule Count  Ace Count  Name
---  ----        ---------  ----------  ---------  ----
53   session     0          0           1          apprf-dpi-role-sacl
65   role        497        8           9          dpi-role

(MM7030) # show rights dpi-role
1         global-sacl          session
2         apprf-dpi-role-sacl  session
3         apprules             session
```

ACE entries Dump

```
ip access-list session apprules
      any any app netflix permit tos 60
      any any app facebook permit
      any any appcategory gaming deny
      any any svc-dhcp  permit
      user any svc-dns  src-nat pool extern
      user any svc-https  src-nat pool extern
      user any svc-http  src-nat pool extern
      user any svc-icmp  src-nat pool extern

(MM7030) (config) #show acl ace-table acl 65
  497: any any app 734 f8081001:permit tos/sendresp
  498: any any app 244 f8080001:permit
  499: any any appcategory 7 f8080000:deny
  500: any any  17  0-65535  67-68  f80001:permit
  501: user any  17  0-65535  53-53  f80011:permit snat  pool:2
  502: user any  6  0-65535  443-443  f80011:permit snat  pool:2
  503: user any  6  0-65535  80-80  f80011:permit snat  pool:2
  504: user any  1  0-65535  0-65535  f80011:permit snat  pool:2
  505: any any  0  0-0  0-0  f180000:deny
```

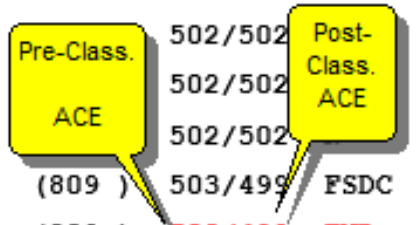
Datapath rules hits

```
(MM7030) #show datapath acl id 65

Datapath ACL 65 Entries
-----------------------
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
       S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
       I - Invert SA, i - Invert DA, H - high prio, O - set prio
       A - DPI PEF, T - set TOS, 4 - IPv4, 6 - IPv6
       C - Classify Media, a - Disable Scanning
----------------------------------------------------------------
 1:  any  any  app 734  PTA4  hits 29  0,
 2:  any  any  app 244  PA4  hits 49  0,
 3:  any  any  appcategory 7  A4    0,
 4:  any  any  17 0-65535 67-68  P4  hits 14  0,
 5:  user  any  17 0-65535 53-53  PS4  hits 2706  0,
 6:  user  any  6 0-65535 443-443  PS4  hits 1180  0,
 7:  user  any  6 0-65535 80-80  PS4  hits 3755  0,
 8:  user  any  1 0-65535 0-65535  PS4    0,
 9:  any  any  any  46  hits 546  0,
```

Datapath DPI Table

```
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT  D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS  C - client, M - mirror, V - VOIP
       Q - Real-Time Quality analysis   I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal   A - Application Firewall Inspect
```

Source IP	Destination IP	Prot	SPort	DPort	ToS	Int-Flag	PktsDpi	AppID		AceIdx	Flags
10.163.160.113	74.125.129.103	6	44707	443	24	1145	1	google	(54)	502/502	STC
216.58.192.14	10.163.160.90	6	443	33782	24	144	1	google	(54)	502/502	N
10.163.160.112	216.58.192.14	6	39418	443	24	145	1	google	(54)	502/502	STC
10.163.160.113	216.58.192.14	6	33782	443	24	1145	1	google		502/502	
74.125.129.103	10.163.160.90	6	443	44707	24	144	3	google		502/502	
216.58.192.14	10.163.160.90	6	443	39418	24	144	0	google		502/502	
10.163.160.112	204.225.145.60	6	39414	80	0	145	1	imvu	(809)	503/499	FSDC
204.225.145.60	10.163.160.90	6	80	39413	0	144	0	imvu	(809)	503/499	FND
173.252.88.68	10.163.160.90	6	443	40721	0	144	1	facebook	(244)	502/498	N
10.163.160.113	173.252.88.68	6	40721	443	0	1145	1	facebook	(244)	502/498	SC
10.163.160.111	54.244.248.250	6	51947	443	60	145	1	netflix	(734)	502/497	STC
54.244.248.250	10.163.160.90	6	443	51947	60	144	0	netflix	(734)	502/497	NT



AppRF Datapath Session Counters

```
(MM7030) # show datapath session dpi counters

Datapath Session DPI counters
-----------------------------
G - Global Counters
----+-----+--------------------+------------------+---------------+----------------+
    |     |Application         |Application       |Current Active |Total           |
Cpu |AppID|Name                |Category          |Sessions       |Sessions        |
----+-----+--------------------+------------------+---------------+----------------+
 G  |0    |Not Classified      |Not Classified    |           25  |       11602    |
 G  |32   |dns                 |network-service   |            0  |          57    |
 G  |54   |google              |web               |            0  |          64    |
 G  |67   |http                |web               |            0  |         145    |
 G  |68   |https               |web               |            2  |          38    |
 G  |70   |icmp                |network-service   |            0  |          38    |
 G  |92   |isakmp              |encrypted         |            0  |           2    |
 G  |128  |nbns                |network-service   |            2  |         288    |
 G  |137  |ntp                 |network-service   |            0  |         124    |
 G  |185  |smb                 |network-service   |            0  |         137    |
 G  |199  |ssl                 |encrypted         |            0  |           7    |
```

Issues? What To Collect?

- **Application Classification issue**
  - Client tcp/ip packet capture exhibiting the issue
  - Show datapath session dpi table | include <client_ip>
  - Controller logs
  - Replicate the issue
- **Bandwidth Contract issue**
  - Same as above
  - Show datapath bwm
- **High Datapath CPU (DPI suspected)**
  - Multiple iterations of ‘show datapath message-queue’
  - Controller logs

8.x-Custom Applications & Category in AppRF & proto bundle upgrade

aruba
a Hewlett Packard Enterprise company

Introduction

- Support for updating newer applications signature set without controller reload.
- Mechanism to create newer application at run-time on MM and push this new application/signature to all the local controllers.
- Support to use any internal apps/sites for classification other than standard apps.
- Creating user defined/custom app category.
- This PPT covers following features,
- Protobundle upgrade
- Custom Applications
- Custom App category
-

Feature Description

The AppRF 2.0 on MM can be sub divided into:

- Support for PDB - Protocol Database Bundle - Upgrade obviating controller reload.
- Creation of customized Application configuration (custom-app) on the MM and pushing it into MD's on the fly.
- Custom app category creation.

The scope of the protocol bundle update changes are as below:

- The protocol database image is provided by Aruba to the customer. This could happen more frequently than a patch release.
- We have to copy this file to MM flash and activate the proto bundle.

The scope of the custom-app creation change is as below:

- Users can define new applications for DPI on the MM. This application definition is stored in the MM in a binary application signature format. When the configuration is pushed to the MDs, this binary format of the application signature is appended to the active protocol signature set on the MD's. The MD's thus can support the customer defined application on the fly.

The scope of custom app category:

- User define category can map to user defined custom applications. Thus we can configure rules based on category.

Continuation…

- Custom app/category and proto bundle activation configuration should be done under /md.
- Custom applications of maximum limit is 64. In Each custom app,16 rules is the max limit.
- Custom app categories of maximum limit is 32.
- Custom app can be delete only after deleting all the rules in the custom app.
- Custom app has precedence over standard apps while classifying.
- Maximum string length of custom app each param is 127.
- We don't support changing the custom app ports from default(80,443).
- We have to input 1-64 id's while configuring the custom app then once config synced to MD. Each app will assign from DPI app id(6145-6208).

  Both id's will display in "show dpi application custom-app all" in MD.

  Ex: user defined app id is 1 → 6145

  user defined app id is 10 → 6155

- We have to input 1-32 id's while configuring the custom app category then once config synced to MD.Each app category will get assign from DPI app id(32-63).

  Both id's will display in "show dpi application category user-defined all" in MM and MD.

  Ex: User-Defined CatID is 1 → 32

  User-Defined CatID is 22 → 53

Configuration

- custom Apps can be configured for both http and https protocols.

- For http custom app, users can configure a given custom app based on following combinations:
  - ✓ Based on http host/server name and http uri parameters.
  - ✓ Based on http referrer name.

- For https custom app, users can configure a given custom app based on following combinations:
  - ✓ Based on https common name parameter.

Configuration(Cont…)

Input character support, Custom App

```
(PAVAN-SCM-21) ^[md] (config) #dpi custom-app

<appname>               Name of custom application; Allowed char set is a-z, 0-9 and '_'

(PAVAN-SCM-21) [md] (config) #dpi custom-app aruba

<appID>                 Unique ID of the application between 1 and 64

(PAVAN-SCM-21) [md] (config) #dpi custom-app aruba 1

(PAVAN-SCM-21) ^[md] (config-submode)#

appcategory             Application Category Name String

http                    HTTP

https                   HTTPS

no                      Delete Command

(PAVAN-SCM-21) ^[md] (config-submode)#http hostname-param

<hostname>              HTTP Host Name String; Allowed char set alpha-num, -, and  .

(PAVAN-SCM-21) ^[md] (config-submode)#

(PAVAN-SCM-21) ^[md] (config-submode)#http hostname-param arubanetowrks.com uri-param

<uri>                   HTTP Uniform Resource Identifier String; Allowed char set alpha-num, ?,  - , _,  /, &,
=,  ., +, and %

(PAVAN-SCM-21) ^[md] (config-submode)#
```

Configuration(Cont…)

```
(PAVAN-SCM-21) ^[md] (config-submode)#https common-name
<commonname>            HTTPS Common Name String; Allowed char set is alpha-num, -, and .
(PAVAN-SCM-21) ^[md] (config-submode)#
```

CUSTOM APP CATEGORY:

```
(PAVAN-SCM-21) ^[md] (config) #dpi appcategory
STRING                  Name of application Category; Allowed char set is a-z,
                        0-9 and '_', '-`
(PAVAN-SCM-21) ^[md] (config) #
(PAVAN-SCM-21) [md] (config) #dpi appcategory aruba
<categoryId>            Provide Unique ID for the category between 1 and 32
```

Configuration(Cont…)

```
(PAVAN-SCM-21) [md] (config) #dpi custom-app aruba 1
(PAVAN-SCM-21) [md] (config-submode)#http hostname-param arubanetworks.com
(PAVAN-SCM-21) ^[md] (config-submode)#http hostname-param arubanetworks.com uri-param /solutions
(PAVAN-SCM-21) ^[md] (config-submode)#https common-name arubanetworks.com
(PAVAN-SCM-21) ^[md] (config-submode)#http referer-param arubanetworks
(PAVAN-SCM-21) ^[md] (config-submode)#!
(PAVAN-SCM-21) ^[md] (config) #write memory
(PAVAN-SCM-21) [md] (config) #show dpi custom-app aruba

Custom Application Detailed Output
----------------------------------
Rule ID  Custom Name  Protocol  Hostname           CommonName         Referrer           Uri
-------  -----------  --------  --------           ----------         --------           ---
1        aruba        http      arubanetworks.com  --                 --                 --
2        aruba        http      arubanetworks.com  --                 --                 /solutions
3        aruba        http      --                 --                 arubanetworks      --
4        aruba        https     --                 arubanetworks.com  --                 --
(PAVAN-SCM-21) [md] (config) #
(PAVAN-SCM-21) [md] (config) #
```

NOTE:

=====

- ✓ For hostname/common-name arubanetworks.com, ".*" regexp paatern will prepend in backend. It will be "(.*\\.)?arubanetworks\\.com"
- ✓ Suppose if we add hostname as www.arubanetworks.com. Rule will be "(.*\\.)?www\\.arubanetworks\\.com"
- ✓ For referrer we should add only arubanetworks, ".*" will be prepend and append the rule. Rule will be "(.*\\.)?arubanetworks\\..*" We should not add www.arubanetworks.com or arubanetworks.com.

Configuration(Cont…)

→Config in MD. By default custom app fall under web category.

```
(PAVAN-MN-7220) #show dpi custom-app aruba

Custom Application Detailed Output
----------------------------------
Rule ID  Custom Name  Protocol  Hostname           CommonName         Referrer           Uri
-------  -----------  --------  --------           ----------         --------           ---
1        aruba        http      arubanetworks.com  --                 --                 --
2        aruba        http      arubanetworks.com  --                 --                 /solutions
3        aruba        http      --                 --                 arubanetworks      --
4        aruba        https     --                 arubanetworks.com  --                 --
(PAVAN-MN-7220) #
```

→This Command output available only in MD.it has user defined app id,dpi app id,appname and category details. App id(6145) will use for classification.

```
(PAVAN-MN-7220) #show dpi application custom-app aruba

Custom Applications
-------------------
Name   App ID  App Category  Default Ports  User-Defined AppID  Applied
----   ------  ------------  -------------  ------------------  -------
aruba  6145    web           tcp 80,443     1                   0
(PAVAN-MN-7220) #
(PAVAN-MN-7220) #
```

Configuration(Cont…)

→Creation of custom app category and assigning the custom app to custom app category.

```
(PAVAN-SCM-21) [md] (config) #dpi appcategory aruba 1
(PAVAN-SCM-21) ^[md] (config) #dpi custom-app aruba 1
(PAVAN-SCM-21) ^[md] (config-submode)#appcategory aruba
(PAVAN-SCM-21) ^[md] (config-submode)#!
(PAVAN-SCM-21) ^[md] (config) #write memory
(PAVAN-SCM-21) [md] (config) #show dpi application category user-defined all

User-defined Application Categories
-----------------------------------
Name   App Category ID  User-Defined CatID  Applied
----   ---------------  ------------------  -------
aruba  32               1                   0

Total application groups = 1

(PAVAN-SCM-21) [md] (config) #
```

→appcategory of app changed from web to aruba.

```
(PAVAN-SCM-21) [md] (config) #show dpi custom-app all

Custom Applications Summary
---------------------------
Custom Name  App ID  App Category  Num of Rules
-----------  ------  ------------  ------------
aruba        1       aruba         4
great        47      web           1

Total applications = 2

(PAVAN-SCM-21) [md] (config) #
```

Configuration(Cont..)

→MD output.

```
(PAVAN-MN-7220) #show dpi application custom-app aruba

Custom Applications
-------------------
Name   App ID  App Category  Default Ports  User-Defined AppID  Applied
----   ------  ------------  -------------  ------------------  -------
aruba  6145    aruba         tcp 80,443     1                   0
(PAVAN-MN-7220) #
(PAVAN-MN-7220) #show dpi application category user-defined all

User-defined Application Categories
-----------------------------------
Name   App Category ID  User-Defined CatID  Applied
----   --------------  ------------------  -------
aruba  32               1                   0

Total application groups = 1

(PAVAN-MN-7220) #show dpi application category user-defined aruba

List of Applications
--------------------
Name   App ID  App Category  Default Ports  Applied
----   ------  ------------  -------------  -------
aruba  6145    aruba         tcp 80,443     0

Total applications in this category = 1

(PAVAN-MN-7220) #
```

Classification of custom app

Aruba app classification. Providing the one session for each rule classification.
hostname rule classification,
show datapath session dpi output.

```
10.15.100.110   115.112.3.4     6    49374 80     0/0     0    0   0   tunnel 16   1    173        11527
3bab6    ca3      401      1          none      aruba            (6145)  644/0    C
00:00:00:00:00:00 6b
115.112.3.4     10.15.100.110   6    80    49374  0/0     0    0   0   tunnel 16   4    0          0
8486d    0        400      0          none      aruba            (6145)    0/0
00:00:00:00:00:00 6b
```

```
▷ Frame 2034: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface 0
▷ Ethernet II, Src: IntelCor_71:1f:44 (00:1e:65:71:1f:44), Dst: ArubaNet_01:b6:d8 (00:1a:1e:01:b6:d8)
▷ Internet Protocol Version 4, Src: 10.15.100.110, Dst: 115.112.3.4
▷ Transmission Control Protocol, Src Port: 49374 (49374), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 372
◢ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: www.arubanetworks.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI: http://www.arubanetworks.com/]
    [HTTP request 1/10]
    [Response in frame: 2915]
    [Next request in frame: 2935]
```

Classification(Cont…)

Referrer param rule classification,

show datapath session dpi output.

```
10.15.100.110   208.89.12.87    6    49252 80     0/0     0    0   0   tunnel 16   5e   0          0
95b87    ca3      401      1          none      aruba            (6145)  644/0    C
00:00:00:00:00:00 a2

208.89.12.87    10.15.100.110   6    80    49252  0/0     0    0   0   tunnel 16   66   3          400
4bc40    0        400      0          none      aruba            (6145)  0/0
```

```
Frame 4127: 797 bytes on wire (6376 bits), 797 bytes captured (6376 bits) on interface 0
Ethernet II, Src: IntelCor_71:1f:44 (00:1e:65:71:1f:44), Dst: ArubaNet_01:b6:d8 (00:1a:1e:01:b6:d8)
Internet Protocol Version 4, Src: 10.15.100.110, Dst: 208.89.12.87
Transmission Control Protocol, Src Port: 49252 (49252), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 743
Hypertext Transfer Protocol
  [truncated]GET /api/js/15299416?sid=1iUVMU0oSxOX-ZndUW4SlA.0e05246cbb277fae478b02d7a69a35a0a5aa87d0&cb=lpCb97929x53223&t=sp&ts=1466335981953&pid=7467656342&tid=2582505288&vid=cqi0hLm4Qni8jl9UrvxVzw&rvt=1466
  Host: va.v.liveperson.net\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Referer: http://www.arubanetworks.com/\r\n
  Cookie: LPSessionID=1iUVMU0oSxOX-ZndUW4SlA.0e05246cbb277fae478b02d7a69a35a0a5aa87d0; LPVisitorID=cqi0hLm4Qni8jl9UrvxVzw\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI [truncated]: http://va.v.liveperson.net/api/js/15299416?sid=1iUVMU0oSxOX-ZndUW4SlA.0e05246cbb277fae478b02d7a69a35a0a5aa87d0&cb=lpCb97929x53223&t=sp&ts=1466335981953&pid=7467656342&tid=25825
  [HTTP request 1/21]
  [Response in frame: 5285]
  [Next request in frame: 5473]
```

Classification(Cont…)

https rule classification,

show datapath session dpi output.

```
10.15.100.110   10.1.3.77       6    49260 443    0/0      0    0   0   tunnel 16   3    11          1656
790bb    ca3      1        2          none      aruba             (6145)  644/0    FC
00:00:00:00:00:00 52

10.1.3.77       10.15.100.110   6    443   49260  0/0      0    0   0   tunnel 16   3    11          4714
8144f    0        0        2          none      aruba             (6145)    0/0    F
```

```
▷ Frame 19756: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface 0
▷ Ethernet II, Src: ArubaNet_13:55:c0 (00:1a:1e:13:55:c0), Dst: IntelCor_71:1f:44 (00:1e:65:71:1f:44)
▷ Internet Protocol Version 4, Src: 10.1.3.77, Dst: 10.15.100.110
▷ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49260 (49260), Seq: 1087, Ack: 213, Len: 647
▷ [2 Reassembled TCP Segments (1316 bytes): #19755(1016), #19756(300)]
◢ Secure Sockets Layer
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1311
    ◢ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1307
        Certificates Length: 1304
      ◢ Certificates (1304 bytes)
          Certificate Length: 1301
        ◢ Certificate: 30820511308203f9a00302010202106e32489d18b6bd7032... (id-at-commonName=ctg-internal.arubanetworks.com,id-at-organizationalUnitName=TAC,id-at-organizationName=Aruba Networks, Inc.,id-at-local
          ▷ signedCertificate
          ▷ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted: 1e7875624c2e62ff6fbc5e6e9615de88789c56566f772f6a...
▷ Secure Sockets Layer
```

Classification(Cont…)

URI rule usecase is, if we want apply bandwidth contract on particular uri on an app/website.

```
(PAVAN-MN-7220) #show dpi custom-app idle


Custom Application Detailed Output

---------------------------------

Rule ID  Custom Name  Protocol  Hostname       CommonName  Referrer  Uri

-------  -----------  --------  --------       ----------  --------  ---

1        idle         http      idlebrain.com  --          --        /download/index.html

(PAVAN-MN-7220) #

(PAVAN-MN-7220) #show dpi application custom-app idle


Custom Applications

------------------

Name  App ID  App Category  Default Ports  User-Defined AppID  Applied

----  ------  ------------  -------------  ------------------  -------

idle  6147    web           tcp 80,443     3                   0

(PAVAN-MN-7220) #
```

Classification(Cont…)

```
10.15.100.110   184.107.210.194 6    49644 80     0/0     0    0   1   tunnel 17   24   1          41
123d1    ca3      1401     1          none      idle              (6147  )  644/0    C
00:00:00:00:00:00 48

184.107.210.194 10.15.100.110   6    80    49644  0/0     0    0   0   tunnel 17   25   1          52
55be2    0        400      1          none      idle              (6147  )    0/0
00:00:00:00:00:00 48
```

```
▷ Frame 1448: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface 0
▷ Ethernet II, Src: IntelCor_71:1f:44 (00:1e:65:71:1f:44), Dst: ArubaNet_01:b6:d8 (00:1a:1e:01:b6:d8)
▷ Internet Protocol Version 4, Src: 10.15.100.110, Dst: 184.107.210.194
▷ Transmission Control Protocol, Src Port: 49644 (49644), Dst Port: 80 (80), Seq: 593, Ack: 56000, Len: 350
◢ Hypertext Transfer Protocol
  ◢ GET /download/index.html HTTP/1.1\r\n
    ▷ [Expert Info (Chat/Sequence): GET /download/index.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /download/index.html
      Request Version: HTTP/1.1
    Host: www.idlebrain.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.idlebrain.com/index1.html\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.idlebrain.com/download/index.html]
    [HTTP request 3/4]
    [Prev request in frame: 688]
    [Response in frame: 1550]
    [Next request in frame: 1551]
```

Classification(Cont…)

- **Proto bundle activation.**
- Few apps(license, ndtv-test,pavan,internalaruba) added as part of this bundle. Respective traffic will get classify when new app signatures matched after bundle activation.

```
(PAVAN-SCM-21) [mynode] #copy scp: 10.20.22.120 anupama /tftpboot/pavan_pbundle_54417.txt flash:
pavan_pbundle_54417.txt

Password:********



Press 'q' to abort.


Secure File Copy:........

(PAVAN-SCM-21) [mynode] #

(PAVAN-SCM-21) [mynode] #change-config-node /md

(PAVAN-SCM-21) [md] #

(PAVAN-SCM-21) [md] #

(PAVAN-SCM-21) [md] #configure t

Enter Configuration commands, one per line. End with CNTL/Z

(PAVAN-SCM-21) [md] (config) #dpi proto-bundle activate pavan_pbundle_54417.txt

(PAVAN-SCM-21) ^[md] (config) #write memory   <<<<<<<<<<<<<<<<config gets syncs to MD after write memory.
```

Classification(Cont…)

→New apps added in MD after proto bundle activation once config successful.

```
(PAVAN-MN-7220) #show running-config | include proto
Building Configuration...
dpi protobundle activate  pavan_pbundle_54417.txt
(PAVAN-MN-7220) #

(PAVAN-MN-7220) #show dpi application all | include 300
flurry               2300    web             tcp 80,443             0
learninganalytics    3003    web             tcp 80,443             0
license              3007    web             tcp 80,443             0     <<<<<<<<<<<<<<<<<
ndtv-test            3009    web                                    0     <<<<<<<<<<<<<<<<<
pavan                3006    web             tcp 80,443             0     <<<<<<<<<<<<<<<<<
pearsonvue           3002    web                                    0
youtubeeducation     3005    web             tcp 80                 0
(PAVAN-MN-7220) #
(PAVAN-MN-7220) #show dpi application all | include 3010
internalaruba        3010    web                tcp 80,443          0     <<<<<<<<<<<<<<<<<
(PAVAN-MN-7220) #
(PAVAN-MN-7220) #
```

Logs

proto bundle activation,

Logs from MM,

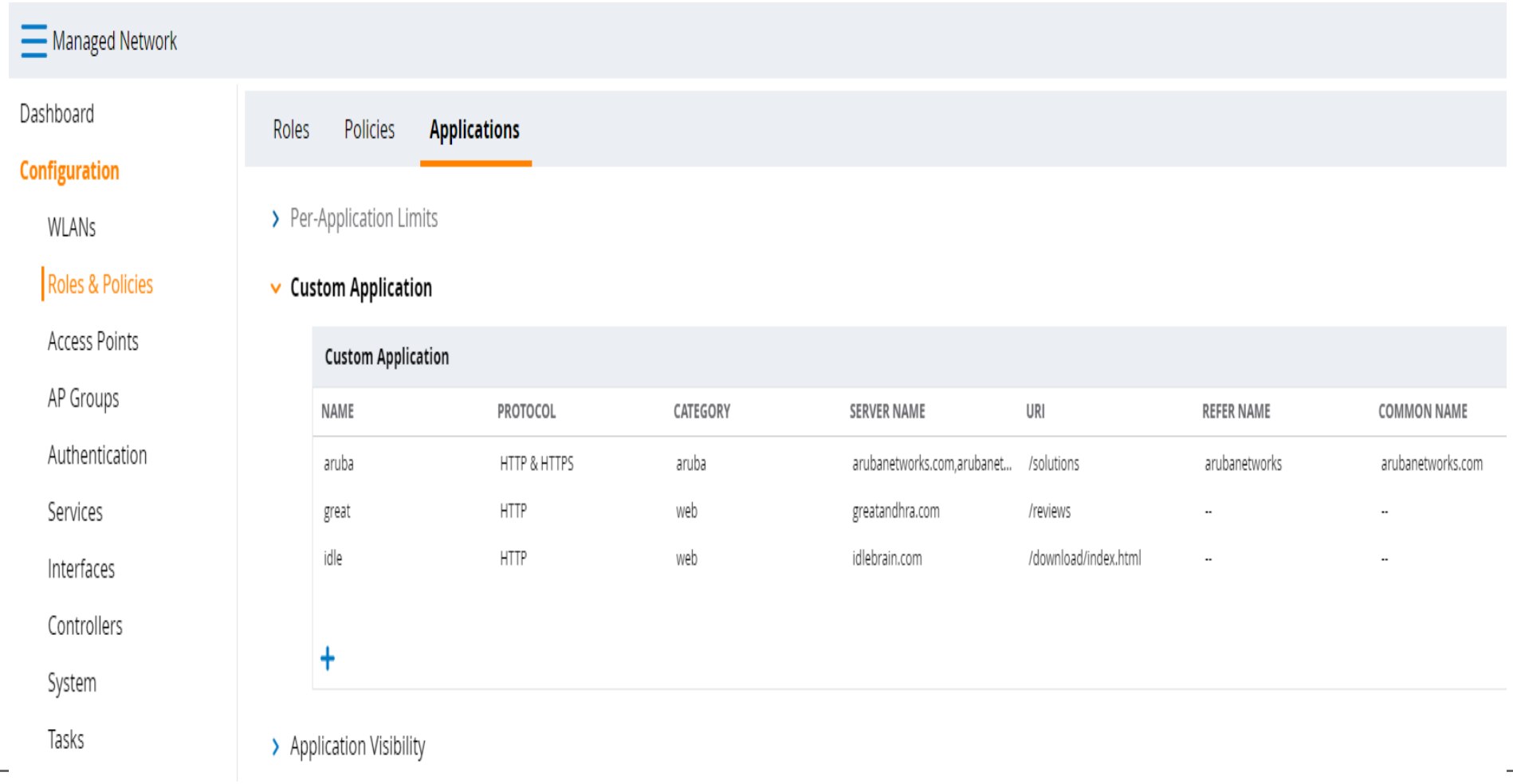
```
Jun 19 06:35:13 :391006:  <DBUG> |appRF|  Validated file name /flash/config/pavan_pbundle_55457.txt  ret is 0
validate_protobundle appRF_config.c:2372

Jun 19 06:35:14 :391006:  <DBUG> |appRF|  Decrypted file is dpi_pdb_base64.txt   validate_protobundle
appRF_config.c:2409

Jun 19 06:35:14 :391006:  <DBUG> |appRF|  Decrypted file is dpi_pdb_base64.txt   decodeInstallProtobundle
appRF_config.c:2423

Jun 19 06:35:14 :391006:  <DBUG> |appRF|  Decoded file successful dpi_pdb_base64.txt
decodeInstallProtobundle appRF_config.c:2433
```

Logs from MD,proto bundle activation

```
Jun 19 07:35:23  appRF[3705]: cmd is  rsync --address=10.15.100.50 -a
10.15.101.21::apprf/pavan_pbundle_55457.txt /flash/folder_appRF/pavan_pbundle_55457.txt  :line 297  Status is
0 Local filename is /flash/folder_appRF/pavan_pbundle_55457.txt

Jun 19 07:35:30 :391006:  <DBUG> |appRF|  Validated file name /flash/folder_appRF/pavan_pbundle_55457.txt  ret
is 0   validate_protobundle appRF_config.c:2372

Jun 19 07:35:34 :391006:  <DBUG> |appRF|  Decrypted file is dpi_pdb_base64.txt   validate_protobundle
appRF_config.c:2409

Jun 19 07:35:34 :391006:  <DBUG> |appRF|  Decrypted file is dpi_pdb_base64.txt   decodeInstallProtobundle
appRF_config.c:2423

Jun 19 07:35:35 :391006:  <DBUG> |appRF|  Decoded file successful dpi_pdb_base64.txt
decodeInstallProtobundle appRF_config.c:2433
```

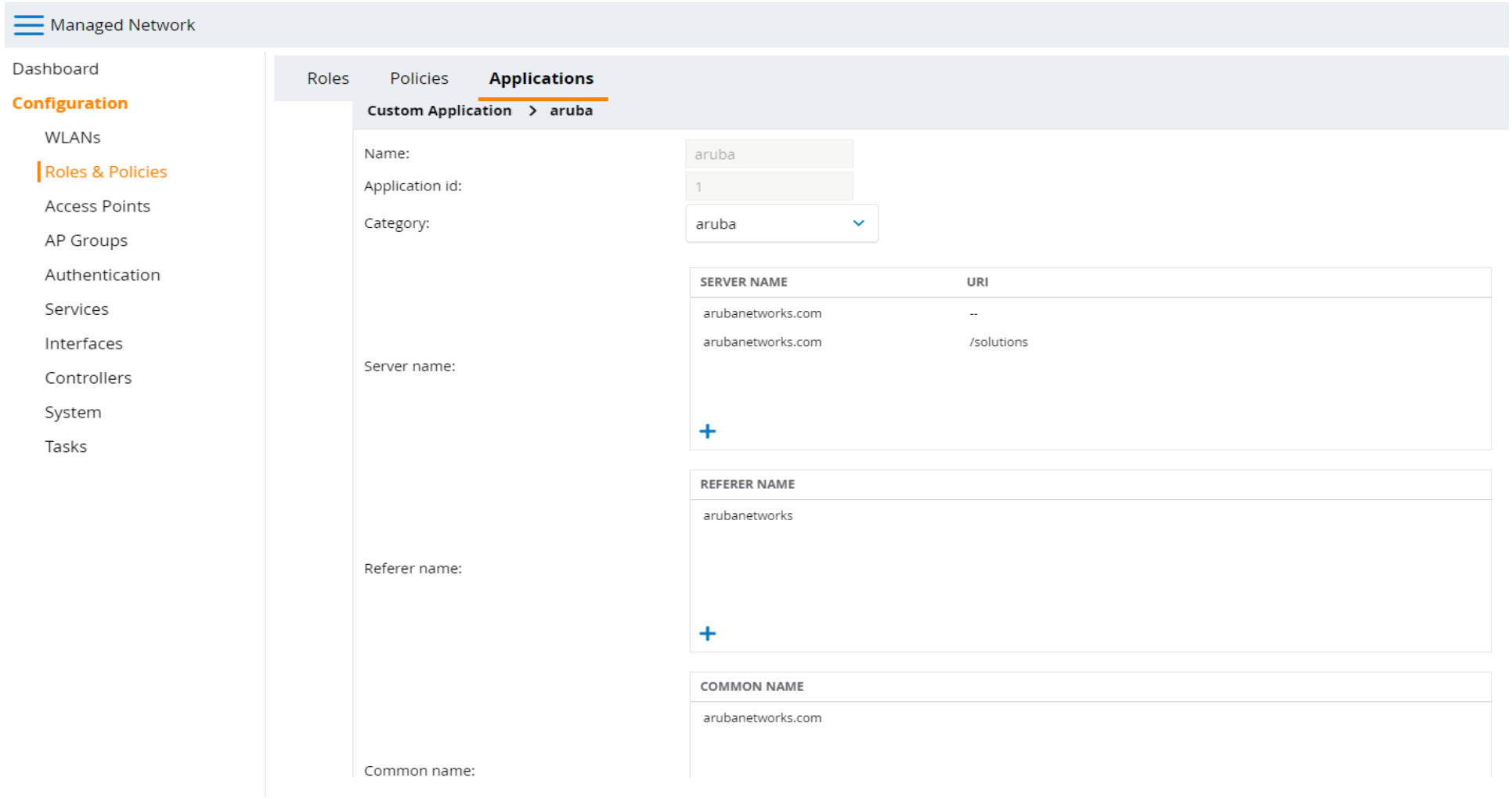
UI snapshots

Configuration – Roles & Policies -- Applications



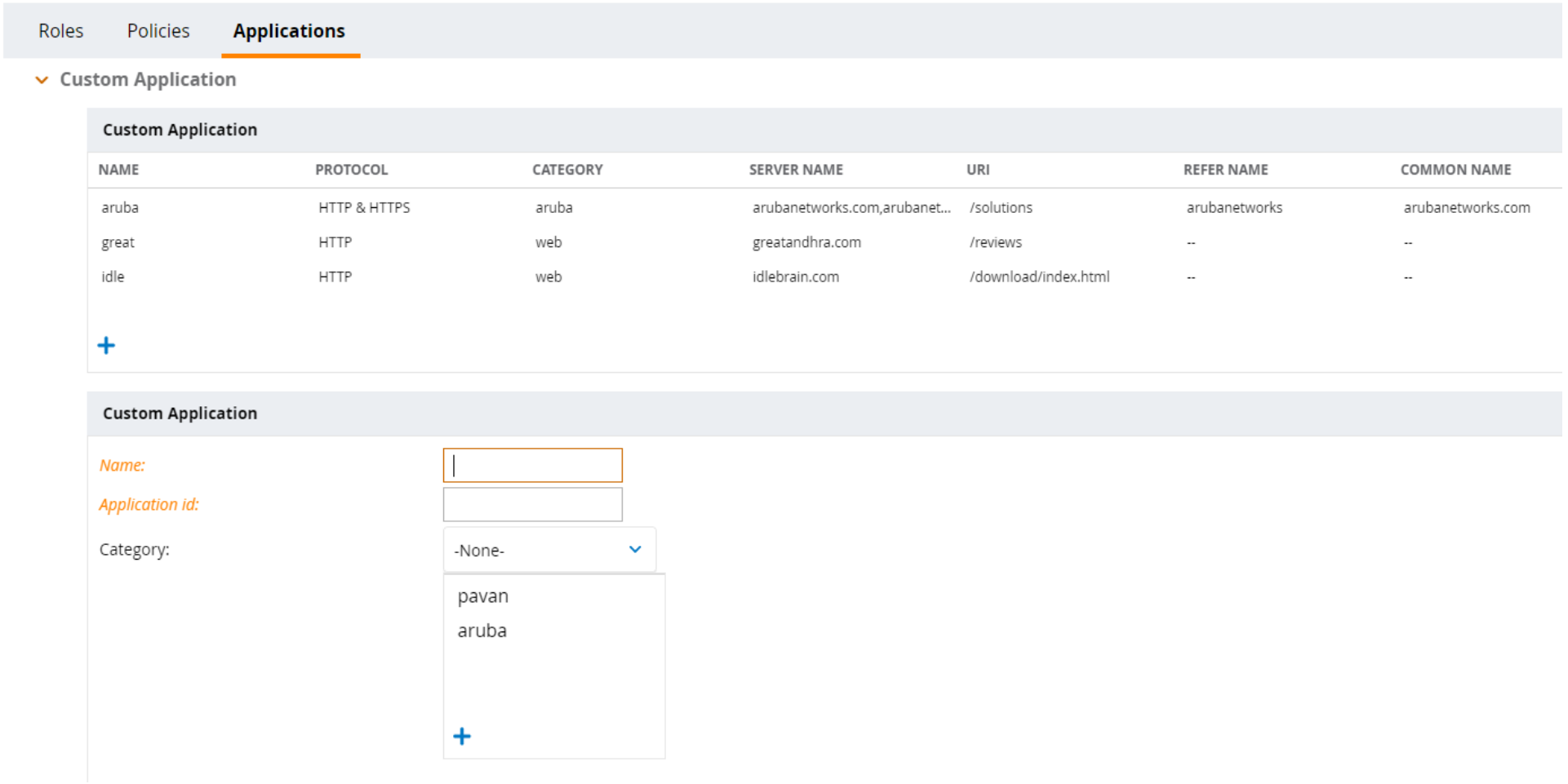
UI snapshots

Custom app config in brief.



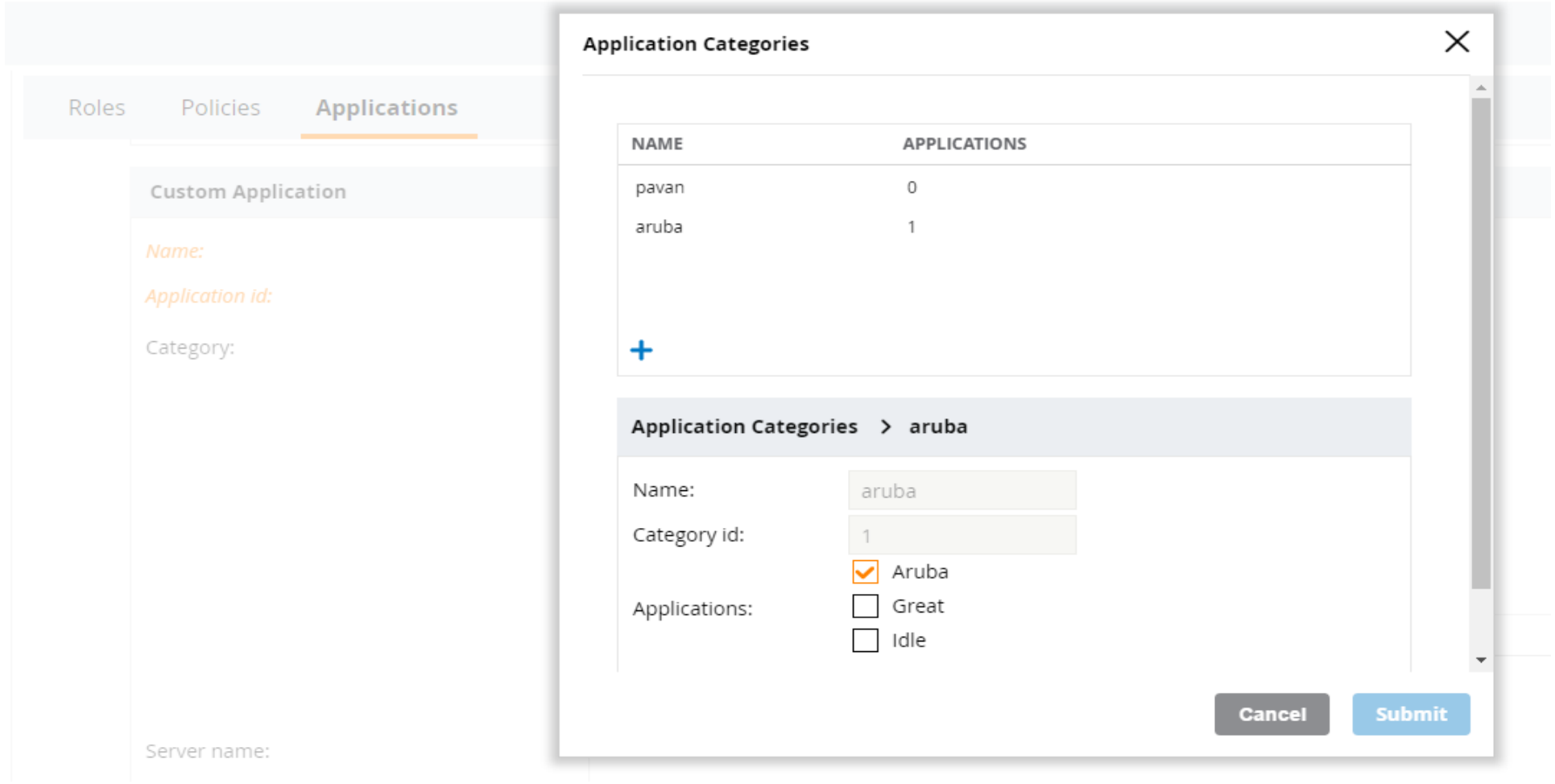
UI snapshots

Creation of new custom app.Click on the + in custom app.Click on the + button to check the custom app category.



UI snapshots

Click on + button to create custom app category.Click on the check boxes of Applications to map to the custom apps to the custom app category.



Logging and debugging

→Enable logging level license & Commands to capture for debugging an issue.

From MM and MD,

```
logging level debugging system process apprf
show log system all | include appRF
show log all | include appRF
tar logs tech-support
```

From MM,

```
Show dpi custom-app all
show dpi custom-app <appname>
show dpi application category user-defined all
```

From MD,

```
Show dpi custom-app all
show dpi custom-app <appname>
show dpi application custom-app all
show dpi application custom-app <appname>
show dpi application category user-defined all
show dpi application category user-defined <category-name>
```

Q&A

aruba
a Hewlett Packard
Enterprise company

Thank You

aruba
a Hewlett Packard
Enterprise company