Benefits of WiNG Application Visibility & Control (AVC)

November 2015

CONTENTS

BACKGROUND

With the explosion of consumer mobile devices and Bring Your Own Device (BYOD), application usage patterns in a typical enterprise wireless network have changed quite drastically. Organizations have lost control of application usage and prioritization on their wireless network; it has become increasingly difficult to predict application usage patterns and manage precious network bandwidth.

Organizations should have the ability to restrict applications and bandwidth consumption, and prioritize use based on the priorities and policies of the corporate resource.

The ability to predict usage behavior is critical to provide sufficient backhaul for the guest users, enforce adequate QoS policies, or block unwanted traffic during peak events. E.g. The ability to get an application usage snapshot during “Black Friday” event.

Another challenge is the number of open applications running on mobile devices. Today a single device will have dozens of data streams opened in the background, downloading data for antivirus updates, windows updates, IM exchanges, email sync, cloud storage sync etc. this traffic need to be controlled, monitored and filtered. Most IT managers install firewalls to keep people out and used proxy servers to filter the traffic inside their network. These legacy application control methods were based on IP / Port based Access Lists are outdated for today’s modern networks and workplaces.

Today we find an explosion of web-based applications that are using the same ports (e.g. YouTube vs Gmail), encrypted apps (encrypted Jabber), and applications with dynamic signatures (Bittorent). For example, employees’ device applications should be prioritized business related applications (e.g. Skype for Business, Salesforce, etc.) while other traffic could be throttled or dropped according to the company policy. However, for guest users IT administrators typically want to know application usage patterns and control the bandwidth allocation among them.

In summary, the main IT challenges in today’s wireless networks when it comes to controlling or monitoring application usage include:

- Lack of visibility of which applications are being used on the wireless network
- Having granular control methods to prioritize, or block, one application over another, or even block unwanted application category.
- Having a way to provide QoS at the edge of the network based on the application matching criteria.

Take YouTube versus Gmail as an example – both services run via HTTPS and both services are syncing with the same Google servers, but YouTube is a more bandwidth intensive service than Gmail. Depending on network capacity or usage, you may want to allow Gmail and block YouTube, or add more granular control at the application level. Another example would be to allow Skype voice calls, but block Skype video calls.

The good news is that WiNG 5 has integrated features to identify and allow, or block, applications with static signatures. With the WiNG 5.8 release, Zebra WLAN supports Application Visibility and Control that can be used to identify thousands of applications based on their signatures and enforce fine grained control on how the applications access the wireless network.

WING 5: APPLICATION VISIBILITY AND CONTROL

Application Visibility & Control (AVC) with the help of the Deep Packet Inspection (DPI) engine on the access points can easily recognize thousands of different applications grouped into multiple application categories and then enforce policies and different quality of service based on the application policy rules.

For example:

- A typical guest network peer-to-peer application such as Bittorrent may consume all the available bandwidth of your guest internet connection, therefore it has to be throttled or dropped.
- Video streaming services should be rate-limited, but also prioritized over best effort traffic.
- Popular VoIP services like Skype or Facetime should get the highest priority in order to deliver uninterrupted service.
- For a corporate network, IT administrators are highly concerned about prioritizing business critical applications like Citrix, Salesforce and Skype for Business applications, as they must be running all the time to ensure the staff is productive and not experiencing any level of connectivity loss or delay.

As an intelligent Layer 7 firewall, WiNG AVC can deliver that level of control at the edge of your network - at the access point. Additionally WiNG AVC along with Zebra NSight provides analytics and historical data about application usage patterns, as Zebra NSight is capable of storing years of historical records on application usage globally, per site or drill down to the level of one particular client.

This paper will address common use-cases and provide generic examples on how to use WiNG AVC in a typical modern guest network.

HOW AVC RECOGNIZES APPLICATIONS

The main core of WiNG Application Visibility and Control is the Deep Packet Inspection engine (DPI) that is responsible for accurate application recognition.

Deep Packet Inspection (DPI): Deep Packet Inspection engine allows the AP or the controller to not only inspect the IP headers, but also dive deep into the application payload to identify the application signatures. A wide range of applications in different categories like Gaming, Peer to Peer (P2P), Social media, etc. can be identified[1]. DPI provides 2 ways of application recognition:

- Built-in Application Signatures (1000+)

  Well-known applications and protocols grouped into different application categories, for example Facebook and Google+ as social media, Skype and Viber as VoIP, etc. This is a layer 7 traffic inspection with the most intelligent and accurate results.

- Custom Application Signatures (based on DNS name, name in the HTTPS certificate, IP port or port range or any combination of these).

  For example, the customer may want to create a custom built application signature for video streaming to prioritize it over any other traffic.

In regards to DPI and any impact on AP performance, Deep Packet Inspection (DPI) is inspecting the application payload to identify applications. When a new application session is initiated, the DPI engine inspects the first few packets exchanged to identify the application flow. For subsequent packets for that application, the packets are identified with the flow by just observing the packet headers. DPI is not needed for subsequent packet exchange on a continuous basis. Due to this, the performance impact is very limited when the AVC feature is enabled, whether on the APs or the controller platforms.

WING AVC PROVIDES GRANULAR LEVEL OF APPLICATION CONTROL

There are several action types that can be enforced for the selected application or application category. The following are the actions available[2] :

- Allow - default action if none specified.
- Deny - drop traffic for selected app / app category.
- Mark - prioritize application traffic using 802.1p or DSCP markings. This is your QoS control functions over applications or app categories.
- Rate-Limit - both ingress and egress direction.
- Traffic-Shape - assign applications or app categories of selected traffic classes for policing and shaping.

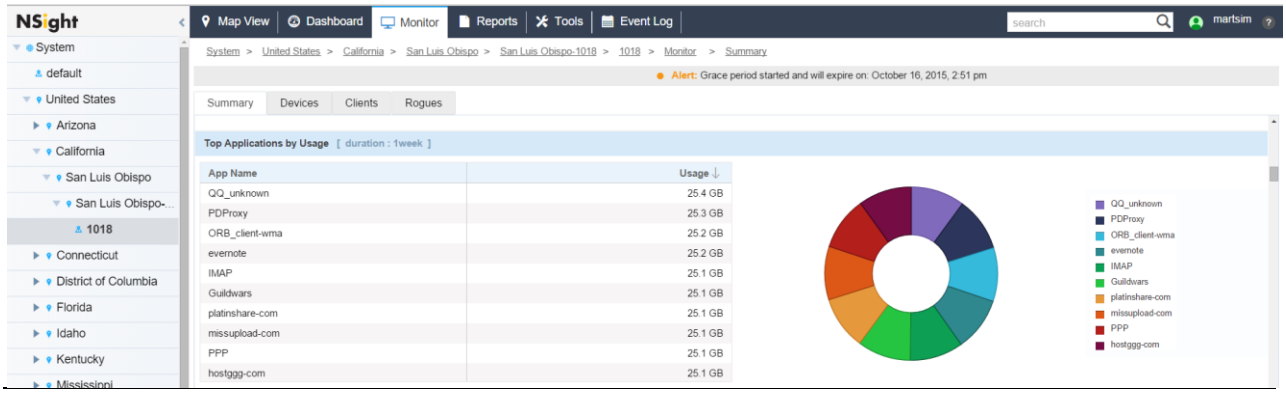
ZEBRA NSIGHT AND AVC PROVIDES APPLICATION USAGE ANALYTICS

Zebra NSight is a network analytics and management platform that is capable of providing historical data for any type of metrics. One of them is application utilization metrics. Zebra NSight is able to provide metrics at different levels as well as provide both real-time and historical view on the application usage.

Below are the Zebra NSight features that can be leveraged to get the most information out of Application Visibility feature:

- **Real-time Monitor view:**

  System or Site based metrics:



[1] DPI engine is supported on AP7522, AP7532 and AP7562 series Access Points. It is also supported on most of the NX controller platforms. Refer to AVC How To guide for further details.

[2] Refer to the AVC guide for detailed configuration instructions

All Applications Details [duration : 1week]

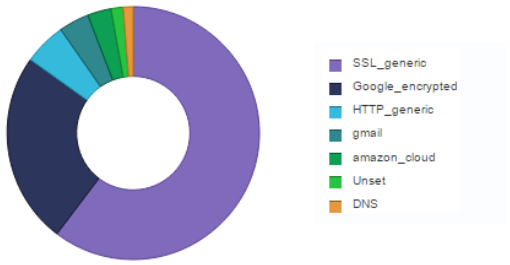
Application Name	Usage	Category	Total Clients	Top Client
gaiafile-com	24.5 GB	filetransfer	80	client-1018-8-0-7-2
BitTorrent_encrypted	23.9 GB	p2p	80	client-1018-6-0-1-2
allshares-ge	24.8 GB	filetransfer	80	client-1018-4-0-2-2
OpenVPN	23.8 GB	tunnel	80	client-1018-4-0-2-3
LDP	23.9 GB	network management	80	client-1018-10-0-1-1
PostgreSQL	24.5 GB	database	80	client-1018-10-0-4-1
bigfilez-com	23.5 GB	filetransfer	80	client-1018-5-0-1-2
WAP-WSP	23.4 GB	mobile	80	client-1018-4-0-3-3
live-share-com	23.4 GB	filetransfer	80	client-1018-10-0-1-4
edisk-cz	23.7 GB	filetransfer	80	client-1018-8-0-1-1
wupload-com	24.3 GB	filetransfer	80	client-1018-8-0-1-1

Client base metrics:

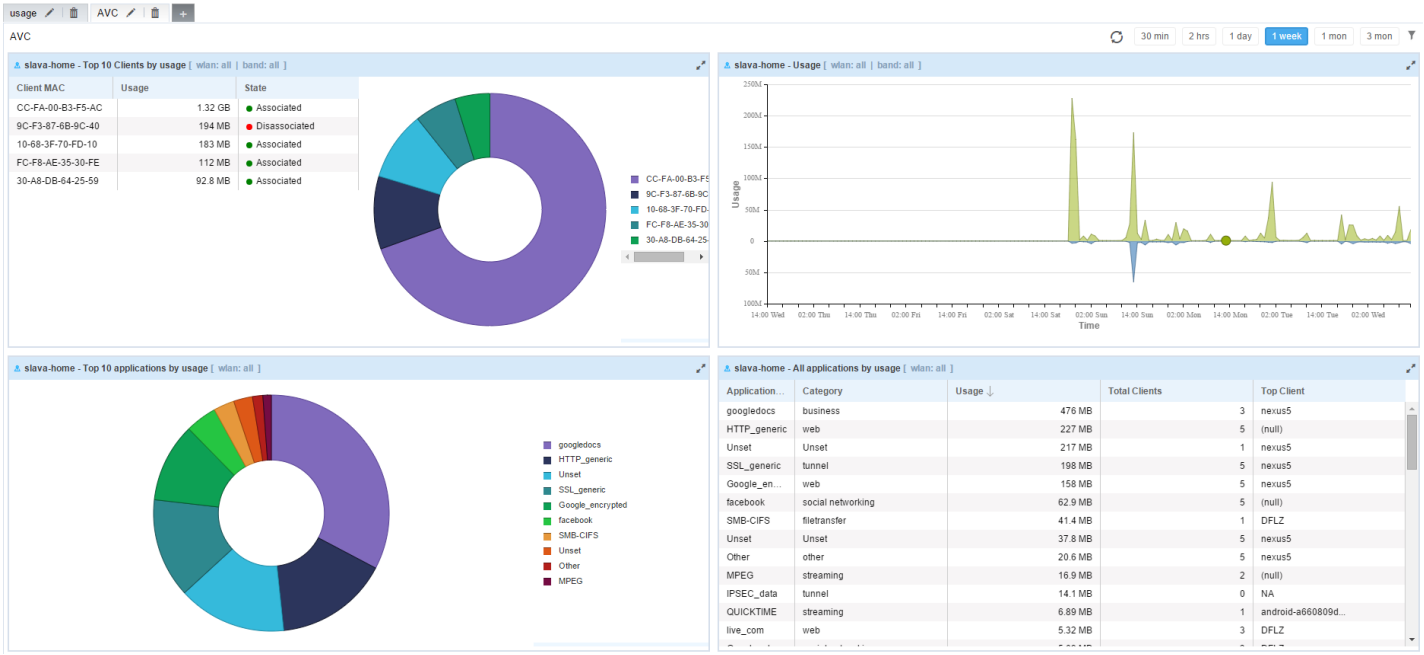
Radio Mode:	11ac	**OS:**	Unknown
Wlan:	goodluck	**MAC Address:**	30-A8-DB-64-25-59
IPv4 Address:	192.168.10.123	**IPv6 Address:**	N/A
Encryption Method:	ccmp	**BSSID:**	84-24-8D-B3-13-70
Last Transmit Rate:	229 MBps	**User Name:**	Slava
Last Recieve Rate:	138 MBps	**Auth Method:**	eap
Retry:	0	**Signal (RSSI):**	-80dBm
SNR:	12db	**Channel:**	100ww
Error Rate:	0	**SSID:**	goodluck
Client Available Capability:	5GHz-wlan	**Client Connected Capability:**	11ac
TX:	3.85 KB	**RX:**	13.0 KB
Noise:	-92dBm		

Top 10 Applications by Usage [duration : 30mins]

Application Name	Usage
SSL_generic	355 KB
Google_encrypted	144 KB
HTTP_generic	31.7 KB
gmail	22.8 KB
amazon_cloud	17.8 KB
Unset	9.05 KB
DNS	7.46 KB



- **Customized Dashboard view**

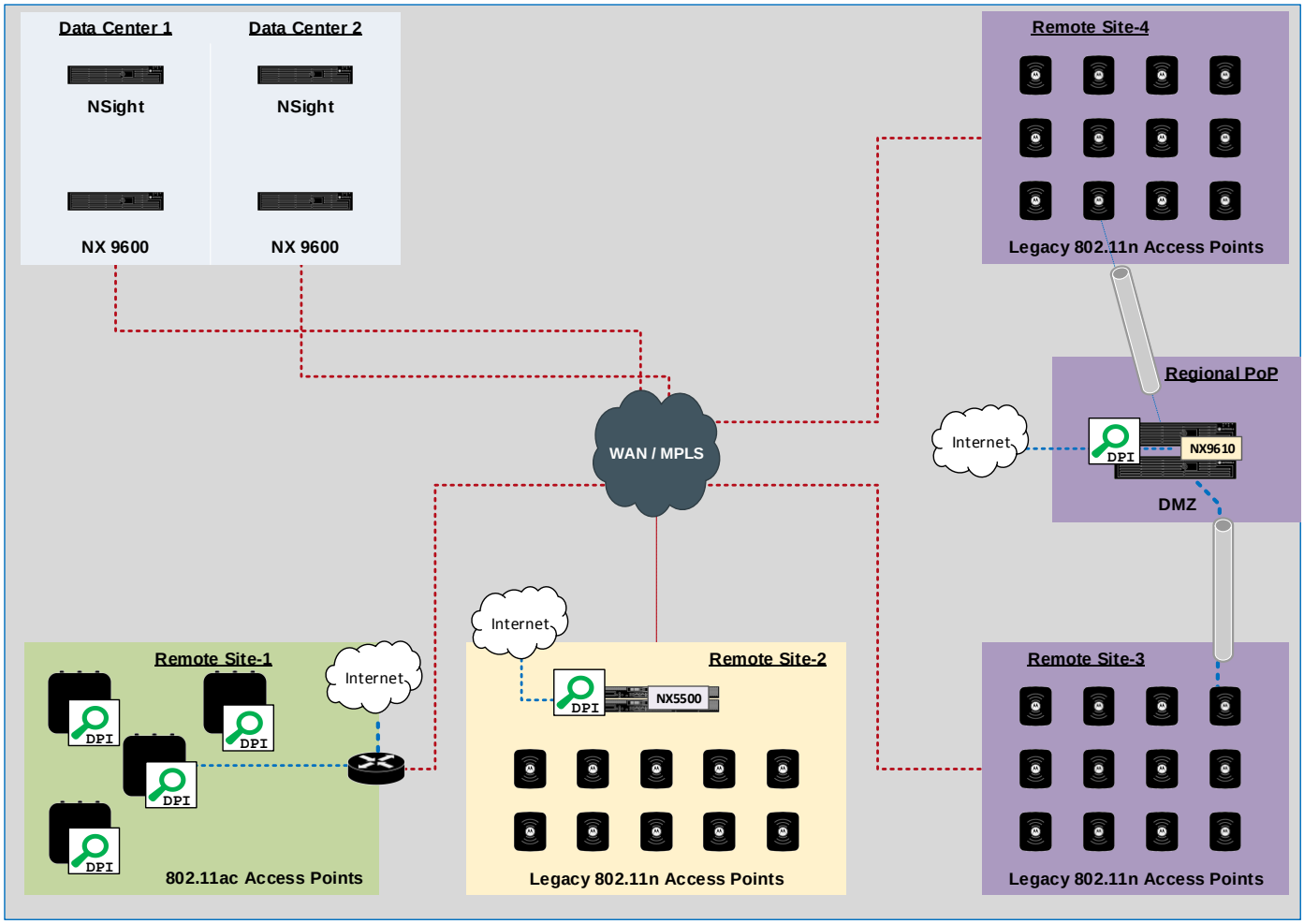


ACHIEVING CONTROL OF YOUR NETWORK USING WING AVC

As with any security and policing best practice, the recommendation is to do all these actions as close to the traffic source as possible. What this means is running the DPI engine right on the edge of the network, at the Access Point. By implementing at the AP, it will provide the most granular level of control and visibility over various applications on your network. However, WiNG 5 supports a flexible AVC function. The DPI can be enforced directly at the Access Point, as well as on the local site or NOC controller, per VLAN, per User Role or per WLAN). Please refer to How To WiNG 5.8 Application Visibility and Control guide for all types of supported deployment models.

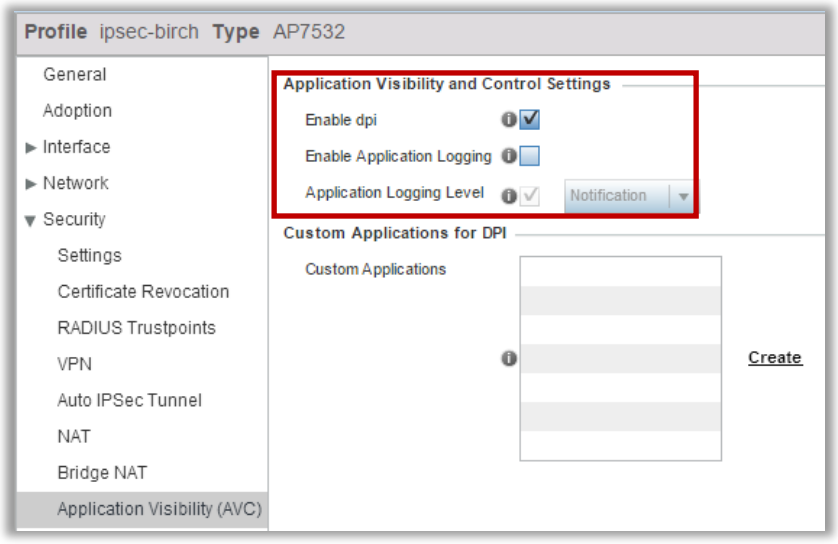
USE CASE: GUEST NETWORK FOR A MULTI-SITE DISTRIBUTED DEPLOYMENT

WiNG 5 and AVC is flexible, allowing application recognition and policing in any kind of deployment, at the AP, at the controller, or both depending on each site conditions. Below is an example topology where the Deep Packet Inspection engine is running directly on the Access Point, where AP supports it, or on a local site controller like NX5500 that will provide AVC functions for the legacy APs on-site. It can also be run on a DMZ controller that is terminating MiNT or L2TPv3 tunnels for multiple sites, like NX9610 or NX7510.



With WiNG AVC a simple flowchart can be followed in order to get the most out of the feature:

1. Ensure that DPI engine is enabled on the Access Points or the NX controller depending on the deployment model.

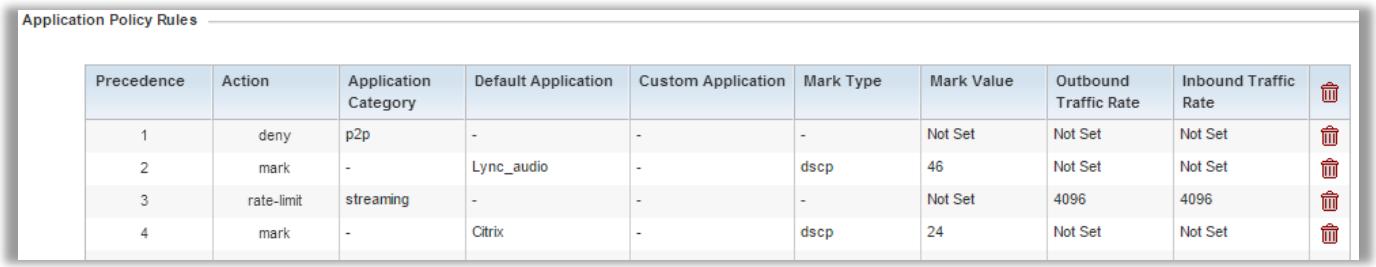


2. Using Zebra NSight look back in history to make predictive analysis and understand usage patterns at any given site. This will help answer questions such as:
   - What applications or what types of applications are being used at each site?
   - What are the top 10 application by usage across all sites or at any given site for the last week? For the last month?

- Is there any unauthorized activity that goes against your corporate or guest usage policy?
- Can we identify certain clients that show higher than expected bandwidth usage?

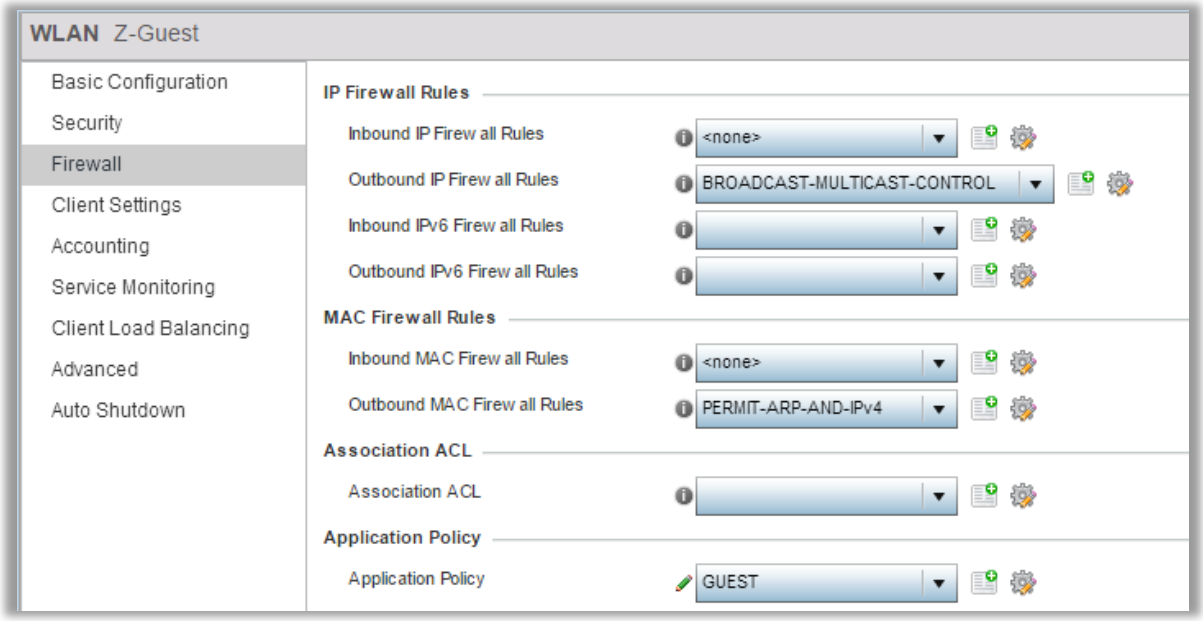
3. Getting answers to the questions above will bring up a list of actions that needs to be enforced at the Application Policy level to:

- Block unwanted traffic
- Mark business critical applications
- Rate-limit allowed, but non-critical bandwidth intensive applications
- Additionally, extend Quality of Service policing to the wired QoS by assigning applications or categories to specific wired traffic classes using Traffic Shaping functionality.



Precedence	Action	Application Category	Default Application	Custom Application	Mark Type	Mark Value	Outbound Traffic Rate	Inbound Traffic Rate
1	deny	p2p	-	-	-	Not Set	Not Set	Not Set
2	mark	-	Lync_audio	-	dscp	46	Not Set	Not Set
3	rate-limit	streaming	-	-	-	Not Set	4096	4096
4	mark	-	Citrix	-	dscp	24	Not Set	Not Set

4. Depending on your deployment model assign Application Policy to the WLAN, Bridge VLAN or User Role to apply newly created rules. Refer to the AVC HowTo guide for detailed configuration instructions.



5. *If using Traffic Shaping functionality, assign application or application categories to the wired traffic classes: