# QoS in PAN-OS

Tech Note

PAN-OS 4.1

Revision A

## Contents

# Overview

A next-generation firewall not only identifies and controls applications, but also ensures that those applications are afforded preferential treatment required to operate at a level of performance set by the administrator. This tech note will provide the reader with QoS terminology, processing model, available options, and how to configure QoS on Palo Alto Networks firewalls.

## Why QoS

Bandwidth is finite and certain types of traffic can be sensitive to latency or packet loss, or can be bandwidth intensive or critical to internal business operations. QoS is a useful tool for optimizing the performance of various applications in your network. QoS provides the capability to adjust some quality aspects of selected flows in network traffic. While QoS is a basic feature of any networking/security device, PAN-OS extends this feature to provide QoS; not just to a network or a subnet, but also for a selected application i.e. PAN-OS provides “Application Quality of Service”.

Providing application availability is one of the key elements of network security. Facilitating unencumbered access to mission critical application on the network using QoS requires that we first properly identify the application. Application Identification and providing QoS to those application sessions is the new mantra in the security space. Palo Alto Networks leads this innovation.

## Learn about Applications in your Network

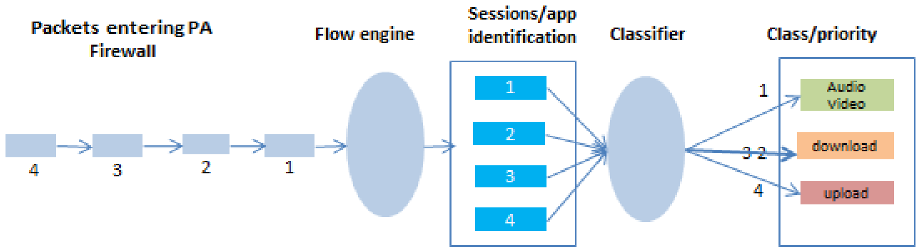
Before implementing QoS, identify the application traffic that is important to your company. Identify traffic that is bandwidth intensive and traffic that is sensitive to latency or packet loss. For example, a company might want to guarantee bandwidth to revenue producing traffic, such as E-Commerce traffic. Organizations need to ensure that transactions can be completed and the customers do not experience service delays and interruptions. At the same time the company may need to ensure low latency for voice over IP (VoIP) traffic used by sales and support and limit the amount of bandwidth used by non-business critical and bandwidth intensive applications such as Hulu, YouTube and other streaming media services.

# Terms and Concepts

- Classification and Bandwidth Limitation
- Forwarding class, priority queues and schedulers
- Packet marking
- Policing and shaping

## Classification

Classification is the act of associating received packets with a defined QoS class, which in turn maps to a priority queue. Classification is a critical aspect of QoS functionality. In Palo Alto Networks devices, packets will be assigned to a QoS class after the session is created and the application is determined.



The above figure shows how different traffic flows and applications are subjected to a classifier function, which in turn maps to a defined forwarding class. PAN-OS support eight different classes. These classes are wrapped under QoS profiles.

Competitive firewall devices classify packets based on IP precedence or DSCP markings, while this type of classification helps in basic networking scenarios, it doesn't provide richness to QoS from the standpoint of application classification. A QoS profile on the Palo Alto Networks firewall supports eight classes. The number of queues that the device supports is dependent on the platform. Refer to the platform specific data section for details.

## Priority Queues

Each class can be associated with a priority queue; PAN-OS support the following four priority queues:

- real-time
- high
- medium
- low

The queues structure is hierarchical in nature and the details of which are explained below. There is also a built-in "bypass" queue. Management traffic and protocol specific traffic (ARP, OSPF, BGP, etc.) is mapped to this internal "bypass" queue. This queue is not configurable by the user.

## Limiting Bandwidth

At the egress interface a class in a QoS profile is used to link the packet to the right priority queue. In PAN-OS, a class essentially maps to a queue. It's possible there could be many-to-one mapping of a class in a QoS profile to a priority queue.

| QoS profile Class | Priority Queue |
|---|---|
| Class1 | Real-time |
| Class2 | High |
| Class3 | High |
| Class4 | Medium |
| Class5 | Medium |
| Class6 | Low |
| Class7 | Low |
| Class8 | Low |

You could also assign a max bandwidth and guaranteed bandwidth to a particular class. Bandwidth is enforced on the egress interfaces on all PAN-OS platforms. While Bandwidth limitation is applied to a class, priority queues helps in determining how packets are serviced by the scheduler.

## Schedulers

A simple scheduler algorithm determines how often a queue is serviced. The scheduler selects the next packet to de-queue based on the priority of that queue and the positive credits that the queue has. PAN-OS uses Hierarchical Fair Service Curve (HFSC) algorithm for scheduling. The same algorithm is used in most Linux implementations and now in FreeBSD. In simple terms, HFSC provides ability to filter traffic to prioritized queues and limit the associated queue sizes. The algorithm does a great job of keeping the latency low.

QoS is implemented in software on certain platforms and is implemented in both software and hardware (hybrid) in other platforms. The following table shows the various implementations:

| Platform | QoS Implementation |
|---|---|
| PA-200 | S/W only |
| PA-500 | S/W only |
| PA-2000 Series | S/W only |
| PA-4000 Series | Hybrid |
| PA-5000 Series | Hybrid |

The management traffic is mapped to an internal "bypass" queue, while tunnel traffic is always processed by software implementation only.

## Congestion Management

When a queue is filling faster than it can be emptied, the device has two choices as to where to drop traffic. It can wait until the queue is full and simply drop packets as they arrive (tail dropping), or it can detect incipient congestion and proactively begin to drop packets based on probability function that is tied to average depth of the queue. This technique is called random early drop (RED). PAN-OS uses weighted RED (WRED) algorithm.

## Packet Marking/Rewriting

As discussed previously, the PAN-OS QoS module is application centric and packets are forwarded to a class/queue based on the application, user and the type of traffic, but not based on IP precedence or DSCP bits. However if an upstream device marks the DSCP bits, PAN-OS maintains those bits as is. PAN-OS provides the flexibility to mark the DSCP or IP precedence bits in the packet to facilitate classification in downstream nodes. This functionality is decoupled from the QoS module, whether or not QoS is configured, you can still configure the system to mark certain flows. The configuration of which is in the options settings of the security policy rule.

## Policing and Shaping

Policing is performed to avoid unintentional starvation of the QoS priority queues. Policers mark packets that go above the burst rate as out of conformance, which alerts the scheduler to allow the packets to be forwarded only if the interface is not experiencing congestion. When the interface is experiencing congestion, out of conformance packets are either automatically discarded or reclassified.

Not all Palo Alto Networks firewalls support policing, refer to the following table:

| Platform | Policing |
|---|---|
| PA-200 | Not Supported |
| PA-500 | Not Supported |
| PA-2000 Series | Not Supported |
| PA-4000 Series | Supported (on ingress interface) |
| PA-5000 Series | Supported (on ingress interface) |

Policing is performed on the ingress interface in PA-4000/5000 Series platforms. Policing is done in hardware on the PA-4000 Series and PA-5000 Series platforms. However, PA-200/500/2000 Series devices do not support Policing. The downside of not Policing is that the security engine of the firewall could be overwhelmed with "out of conformance traffic", which is processed and dropped at the egress. The workaround for this situation is to configure Policing on the upstream switch or router. Please keep in mind that even though we support Policing in PA-4000 and PA-5000 Series, QoS Policing elements like loss priority, burst size and queue depth of the Policer is not configurable.

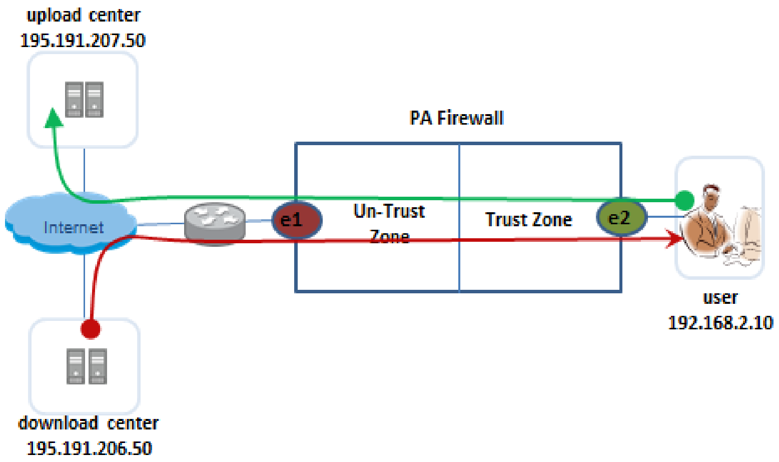
The Shaper smooths the peaks and valleys by buffering traffic and letting it leak out at a specified rate. The upside to the Shaping is that packet-buffering requirements are reduced in downstream nodes or the systems that are connected to the firewall. The reason is traffic bursts are taken care by the Shaper. The downside is the need for buffering within the Shaper, which adds delay. All platforms support shaping, which is at the egress interface only. In PA-200/500 and PA-2000 Series devices, Shaping is performed in software only. However, in PA-4000/5000 Series devices, Shaping is performed in hardware.

## Determining the Egress Interface in Palo Alto Networks Firewalls

By now you are aware that QoS in the Palo Alto Networks firewalls is implemented on the egress interface only. In the below illustration the user is performing two actions:

- Uploading project files to internet (in green)
- Downloading music and data from the internet (in red)

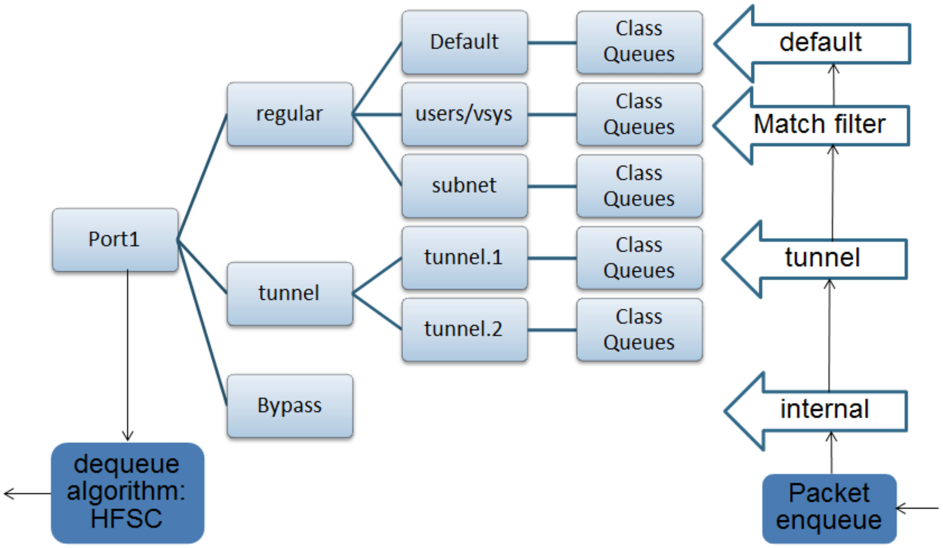
From the security session standpoint both of these actions are initiated by the user. However, from the QoS standpoint, both actions result in a different egress interface.



When the user initiated upload (green) occurs, the ingress interface is e2 and the egress is e1. However, when the user downloads music (red), the packet hits e1 interface first, which is considered as the ingress interface and e2 as the egress interface.

## QoS Queue Structure and Packet Flow

The following illustration is the QoS queue structure in platforms where QoS is implemented in software only. The queue structure is hierarchical in nature; packets are classified to a class/queue based on a filter, tunnel or internal traffic. The match criteria in the filter could be a source interface or a subnet. The filter is applicable to both regular traffic (clear text) and tunnel traffic as well. Traffic that is not classified defaults to class 4 and filters are applied on egress interface.



QoS queue structure in platforms where QoS is implemented in S/W only

# QoS use cases

## Case 1 – Traffic Prioritization

The intent of this use case is to prioritize traffic based on application or achieve QoS based on Application.
Key points to remember from the standpoint of configuration:

- Configure  QoS policy based on application (and/or source-user) into a different class
- Assign priorities accordingly
- Assign bandwidth constraint on the interface

## Case 2 – Sharing Bandwidth with Fairness

The intent of this use case is to achieve fairness among different subnets or classes or different users in an organization or a college environment.
Key points to remember from the standpoint of configuration:

- Configure same priority among different QoS classes
- Configure traffic groups by subnet, tunnel interface etc. on the interface QoS section.

## Case 3 – Upload Data to the Cloud (Internet)

When the user uploads data, the packet hits internal facing interfaces first, which is considered as the ingress interface and external facing interface as egress interface. In this case, you need to apply QoS on the external interface.
Key points to remember from the standpoint of configuration:

- Configure a QoS policy
- Enable QoS on the external interface
- Assign bandwidth limitations as per your requirement

## Case 4 – Download Data from the Cloud (Internet)

When the user downloads data, the packet hits external facing interfaces first, which is considered as the ingress interface and the internal interface as the egress interface. In this case, you need to apply QoS on the internal interface.
Key points to remember from the standpoint of configuration:

- Configure a QoS policy
- Enable QoS on the internal interface
- Assign bandwidth limitations as per your requirement

## Case 5 – Low Latency/Real-time Traffic

If your goal is to ensure low latency for certain application used by sales or you don't want your customers to experience delays with certain applications, you might want to consider prioritizing the traffic to real-time.
Key points to remember from the standpoint of configuration:

- Identify such traffic by a QoS policy and assign it to a special class
- Assign "real-time" priority to the class
    - Specify bandwidth to cap the maximum
    - Do not assign too much bandwidth (guaranteed to max)
- Apply QoS profile accordingly (on internal or external interface)

## Case 6 – Traffic Profiling

The intent of this use case is to profile applications for bandwidth usage requirements.
Key points to remember from the standpoint of configuration:

- Configure QoS policy
- Configure QoS queuing hierarchy
- Do not assign any bandwidth at any level
- Assign same priorities to all classes

QoS counters will give an idea about the application bandwidth consumption. Please keep in mind that application traffic might be dropped by other networking devices in the network.

## QoS Configuration in PA firewalls

Broadly speaking, there are three steps involved in configuring QoS on the firewall as follows:

1) **Configure QoS policy**
    a. Specify the application and a QoS class (ex: class7) that you want to classify traffic on.
    b. QoS policy is just like a security policy that you apply between two security zones.
2) **Configure QoS profile and class**
    a. Give a name to the profile, set a egress max and egress guaranteed bandwidth for the profile.
    b. You could configure at most 8 classes in a QoS profile. Create a class where your traffic is classified in QoS policy.
    c. Specify priority, egress maximum and egress guaranteed bandwidth for the traffic class that you have classified in the QoS policy.
    d. The sum of the egress max bandwidths of the classes in the profile should be less or equal to the profile's egress max bandwidth. On the same note, the sum of the egress guaranteed bandwidth of the classes in the profile should be less or equal to the profile's egress guaranteed bandwidth.
3) **Configure QoS on the interface**
    a. Set interface name, egress max bandwidth for this interface and turn on QoS.
    b. You will notice clear text traffic and tunnel traffic tabs. The sum of the "Egress Max" bandwidth on clear text tab and tunnel traffic tab should be less or equal to the interfaces egress max bandwidth.
    c. Clear Text Traffic – set Egress Max and Egress guaranteed bandwidth. You could add clear text nodes in this section. These nodes form the QoS queuing hierarchy. The match criteria on a node is – source subnet or source interface. On a match, the nodes QoS profile is applied on that traffic.

       When there is no match, the default clear text profile listed in the physical interface tab is applied. Note that the sum of all the bandwidths in profiles listed in the QoS nodes including the default profile listed on the physical interface should be less than or equal to the clear text's Egress Max.
    d. Tunnel Traffic – Set the Egress Max and Egress guaranteed bandwidth. You could add QoS profile on a tunnel interface in this section. The match criteria on these nodes are the tunnel interfaces itself. On a match, the corresponding QoS profile is applied on that traffic.

The number of QoS nodes or clear text subnets or tunnel interfaces per port that you could configure on a firewall varies with platform and is mentioned in the "platform specific data" section.

## Configure and Test QoS

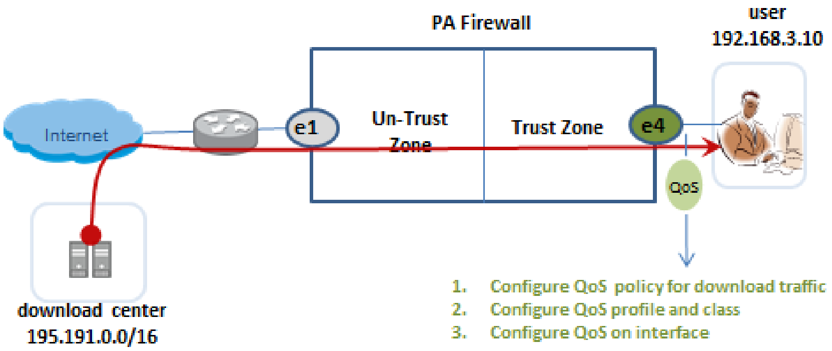
In this section we will go through the steps needed to configure and test the QoS feature. In particular, these steps will help to understand the following:

1) Configuring a QoS policy
2) Rate limit application
3) Configuring QoS in multi-vsys environments

We will also show you how to configure QoS in a single vsys as well as in multi-vsys environment.

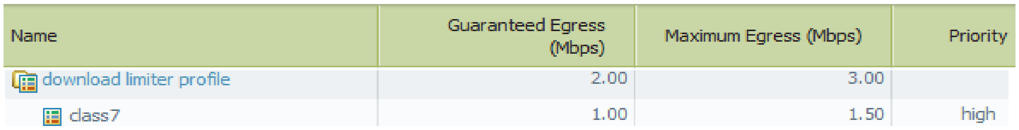
### QoS in Single-vsys environment -

In this scenario we will demonstrate how to configure QoS, which will rate limit download traffic from uploading.com. We will also show the output of QoS statistics.



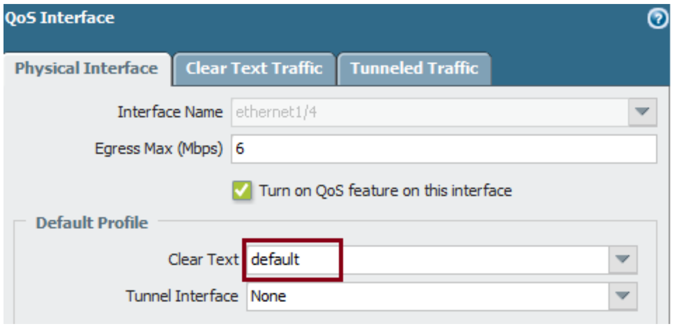
1. Configure QoS policy for download traffic
2. Configure QoS profile and class
3. Configure QoS on interface

1) Create a QoS policy to identify traffic from uploading.com and assign it to a QoS class. In this example, we classified traffic to class 7. The QoS policy for traffic from uploading.com is applied on the egress interface e2.
2) Create a QoS profile. Go to the Network tab > Network Profiles > QoS profiles screen. Assign Maximum Egress and Guaranteed Egress limit for this class 7 "download" traffic. Assign priority for this class.



| Name | Guaranteed Egress (Mbps) | Maximum Egress (Mbps) | Priority |
|---|---|---|---|
| download limiter profile | 2.00 | 3.00 | |
| class7 | 1.00 | 1.50 | high |

Apply the QoS profile we created in step 2 on the egress interface e4 and set an egress Max bandwidth (6 Mbps in the example below). In the example below we did not set a custom profile to be the default or catchall profile. We show examples of the default profile in multi-vsys environment example. The catch all profile will be applied if none of the QoS rules are matched for that flow.



QoS Interface

Interface Name: ethernet1/4

Egress Max (Mbps): 6

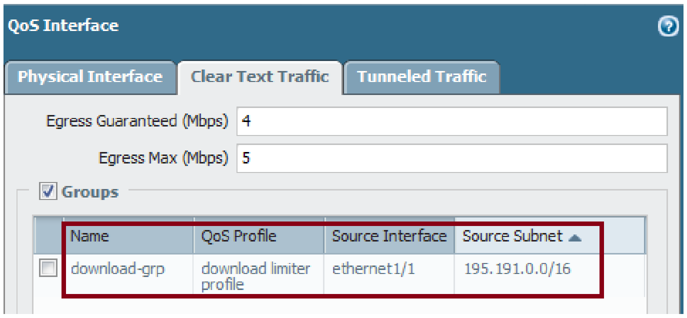
☑ Turn on QoS feature on this interface

Default Profile

Clear Text: default

Tunnel Interface: None

3) In the clear text traffic tab set Egress Guaranteed and Max bandwidths. Add a QoS node and apply QoS profile with source interface as Ethernet 1/1. As described previously for the download traffic, the egress interface is e4 and the ingress interface is Ethernet 1/1. The QoS profile used in this example is "download limiter profile".



QoS Interface

Egress Guaranteed (Mbps): 4

Egress Max (Mbps): 5

☑ Groups

| | Name | QoS Profile | Source Interface | Source Subnet ▲ |
|---|---|---|---|---|
| □ | download-grp | download limiter profile | ethernet1/1 | 195.191.0.0/16 |

4) Since the source interface of the download traffic is Ethernet1/1 with a source subnet of 195.191.0.0/16, the traffic will match download limiter profile Apply QoS profile. The egress Max of 3 Mbps set on the class7 traffic of profile “download limiter profile” is less than egress Max of 4 Mbps of Clear Text Traffic, which is less than the Egress Max of the interface, which is 6 Mbps.

5) From the CLI you can check the match rule that will be applied for the download traffic that we are interested as follows:

```
admin@PA-200> show qos interface ethernet1/4 match-rule

QoS match rule for interface ethernet1/4:
Qid    node           node-id src-i/f        src-addr
----------------------------------------------------------------
1    download-grp    2      ethernet1/1     195.191.0.0/16
0                    0      any               any
```

## Quick Test

1) From the PC, we have downloaded a file from the uploading.com site. The traffic is identified as uploading.

```
admin@PA-200> show session all
--------------------------------------------------------------------------------
ID              Application    State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                           Dst[Dport]/Zone                    (translated IP[Port])
--------------------------------------------------------------------------------
17681   uploading     ACTIVE  FLOW  NS   192.168.3.10[54480]/l3-trust/6  (10.16.0.79[15911])
vsys1                          195.191.207.47[80]/l3-untrust  (195.191.207.47[80])
```

2) For this download traffic, QoS node download-grp is matched. The QoS profile that is applied is “download limiter profile” and the QoS rule applied  is “rate limit downloading”

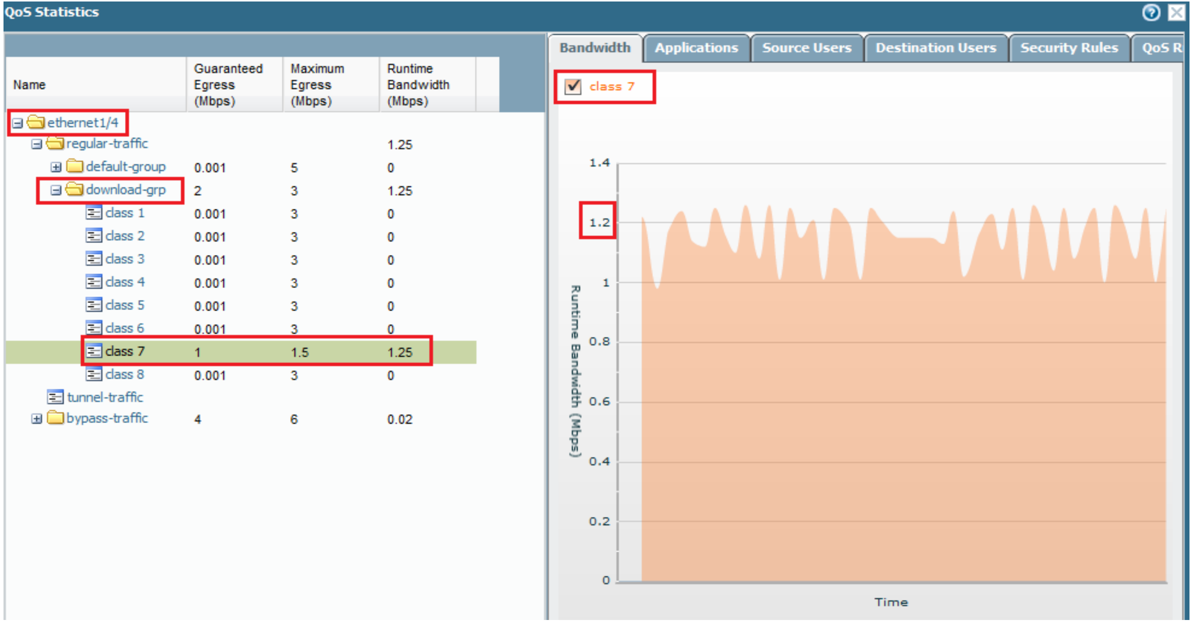
```
admin@PA-200> show session id 17681
  c2s flow:
          source:      192.168.3.10 [l3-trust]
          dst:         195.191.207.47
          src user:    paloaltonetwork\krishna somu
          qos node:    ethernet1/1, qos member N/A Qid 0

      s2c flow:
          source:      195.191.207.47 [l3-untrust]
          dst:         10.16.0.79
          dst user:    paloaltonetwork\krishna somu
          qos node:    ethernet1/4, qos member download-grp Qid 1
          match src interface:  ethernet1/1
          match src address:    ('195.191.0.0/16       ',)

      application                     : uploading
      rule                            : let_go
      ingress interface               : ethernet1/4
      egress interface                 : ethernet1/1
      session QoS rule                : rate limit downloading (class 7)
```

From the above details, QoS egress interface is Ethernet 1/4 and QoS matching node is “download-grp Qid 1”. Don’t get confused with the sessions egress interface, which is Ethernet 1/1

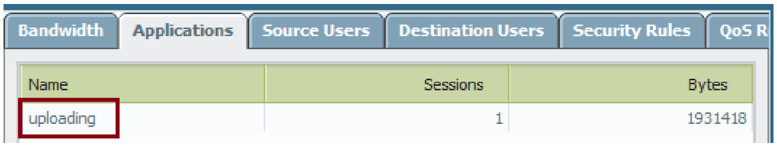
3) To check the QoS statistics, go to Network tab > QoS on interface Ethernet 1/4, click statistics and you will see the runtime bandwidth and the class that this traffic is classified to in an easy to view graph.



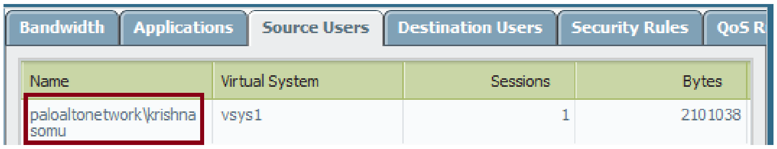
| Name | Guaranteed Egress (Mbps) | Maximum Egress (Mbps) | Runtime Bandwidth (Mbps) |
|---|---|---|---|
| ⊟ ethernet1/4 | | | |
| ⊟ regular-traffic | | | 1.25 |
| ⊞ default-group | 0.001 | 5 | 0 |
| ⊟ download-grp | 2 | 3 | 1.25 |
| class 1 | 0.001 | 3 | 0 |
| class 2 | 0.001 | 3 | 0 |
| class 3 | 0.001 | 3 | 0 |
| class 4 | 0.001 | 3 | 0 |
| class 5 | 0.001 | 3 | 0 |
| class 6 | 0.001 | 3 | 0 |
| class 7 | 1 | 1.5 | 1.25 |
| class 8 | 0.001 | 3 | 0 |
| tunnel-traffic | | | |
| ⊞ bypass-traffic | 4 | 6 | 0.02 |

You will notice multiple tabs for applications, source/Destination users, Security rules, QoS rules matched for this flow.

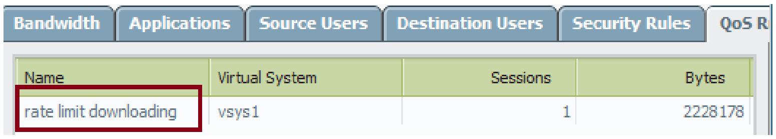
Here are the details of Application, User information, and QoS Rules.



| Name | Sessions | Bytes |
|---|---|---|
| uploading | 1 | 1931418 |



| Name | Virtual System | Sessions | Bytes |
|---|---|---|---|
| paloaltonetwork\krishna somu | vsys1 | 1 | 2101038 |

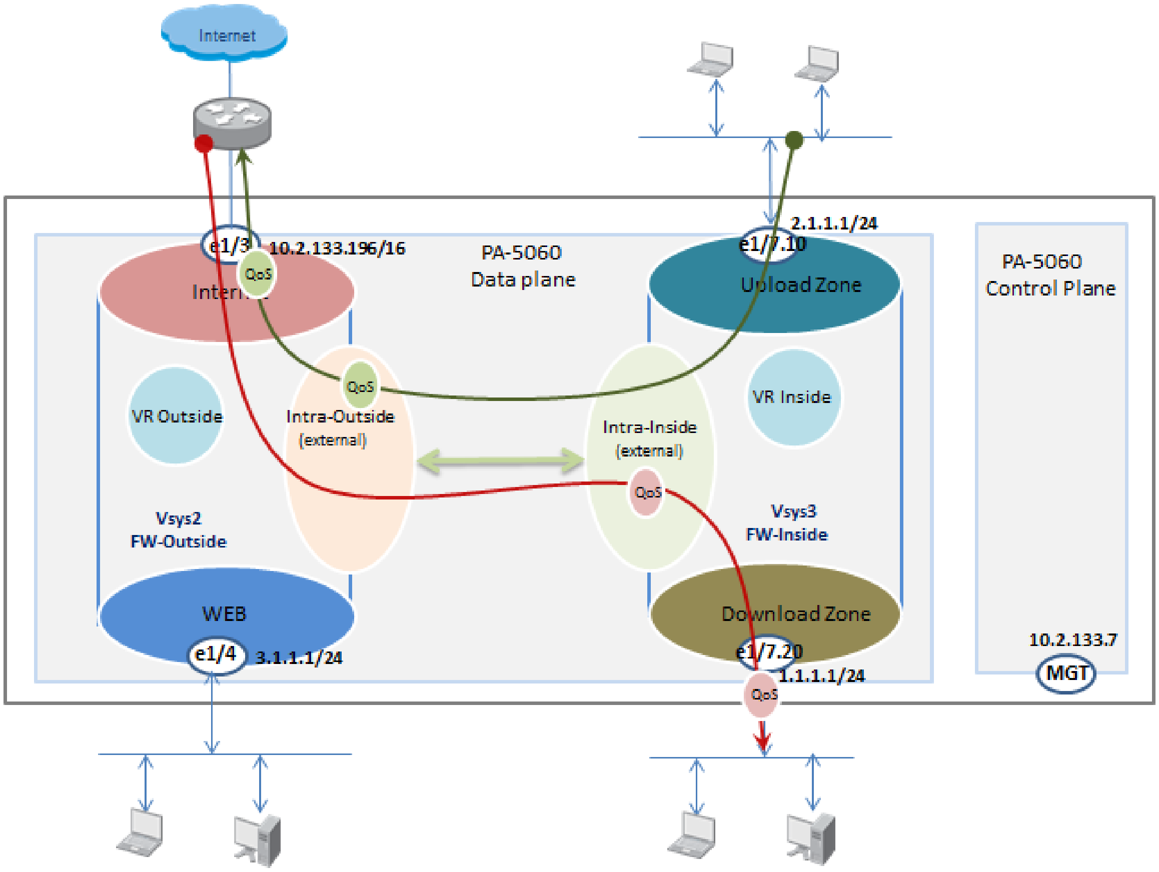


| Name | Virtual System | Sessions | Bytes |
|---|---|---|---|
| rate limit downloading | vsys1 | 1 | 2228178 |

## QoS in Multi-vsys Environment

In this test we will configure multiple virtual systems or tiers. We are using two tiers (vsys2 and vsys3) for this demonstration purposes. We will configure a download zone (olive color); where we will let users download from the uploading.com site. We will demonstrate how to write a QoS policy which identifies uploading.com and will rate limit the **download** traffic from that site. We will also configure an upload zone (green color), where we will let users upload data to uploading.com. We will also demonstrate how to write a QoS policy which identifies uploading.com and rate limit **upload** traffic.

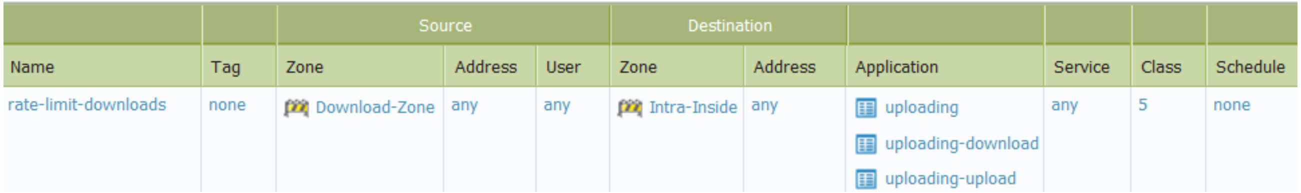
The following diagram represents this multi-tier design being virtualized within a single PA-5060 firewall.



Since, QoS is implemented on the egress interface. Configure the following for download traffic in the FW-Inside (Vsys3) VSYS.

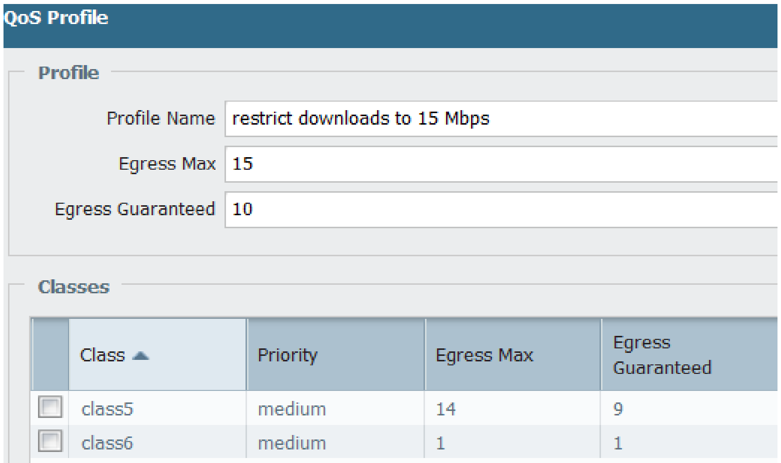
1) Create a QoS policy to identify download traffic from uploading.com and assign it to a QoS class. In this example, we classified traffic to class 5. The QoS policy for download traffic to Download Zone is applied on the inside or clients facing Vsys i.e. in FW-Inside. Essentially the QoS rule is written between Download Zone and Intra-Inside (external) zone.

To create the QoS policy in Vsys "FW-Inside", go to Policies tab → QoS screen. Create a rule as follows:



| | | Source | | | Destination | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Name | Tag | Zone | Address | User | Zone | Address | Application | Service | Class | Schedule |
| rate-limit-downloads | none | Download-Zone | any | any | Intra-Inside | any | uploading<br>uploading-download<br>uploading-upload | any | 5 | none |

2) Create a QoS profile. Go to Network tab > Network Profiles > QoS profiles screen. Create a New QoS profile. Define a QoS profile that will assign a maximum egress limit for class 5 "download" traffic. Your QoS profile will look something like the following:



QoS Profile

Profile

Profile Name: restrict downloads to 15 Mbps

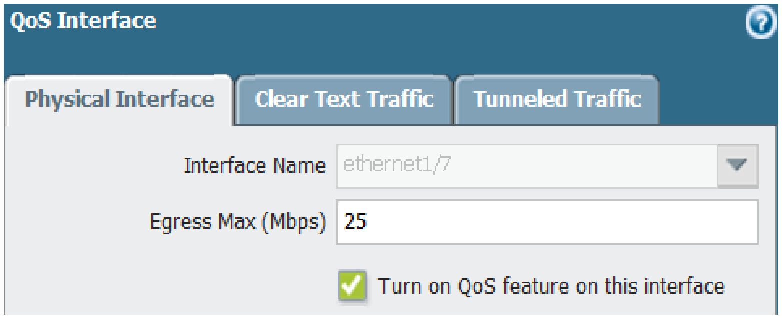
Egress Max: 15

Egress Guaranteed: 10

Classes

| | Class | Priority | Egress Max | Egress Guaranteed |
|---|---|---|---|---|
| □ | class5 | medium | 14 | 9 |
| □ | class6 | medium | 1 | 1 |

3) Apply QoS on the interface e1/7 and set an egress Max bandwidth (25 Mbps in the example below). In the clear text traffic tab set Egress Guaranteed and Max bandwidths. Add a QoS node and apply QoS profile with source interface as Ethernet 1/3. As described before for download traffic the egress interface is e1/7 and ingress interface is e1/3. The QoS profile used in this example is "restrict downloads to 15 Mbps".

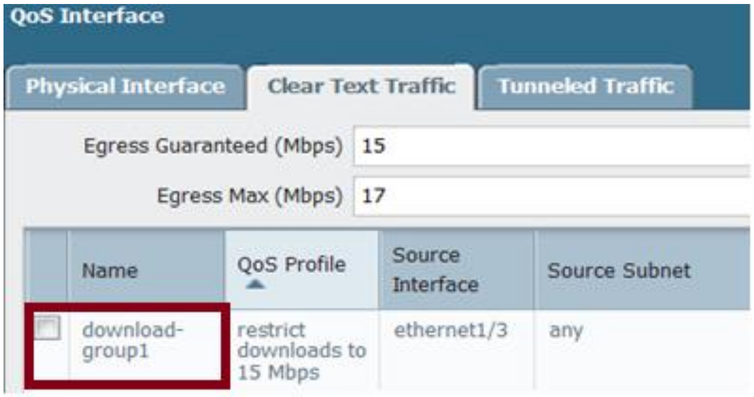


Interface Name: ethernet1/7

Egress Max (Mbps): 25

☑ Turn on QoS feature on this interface

4) The egress Max of 15 Mbps set on the class 5 traffic of profile "restrict downloads to 15 Mbps" is less than egress Max of 17 Mbps of Clear Text Traffic, which is less than the Egress Max of the interface, which is 25 Mbps.



Egress Guaranteed (Mbps): 15

Egress Max (Mbps): 17

| | Name | QoS Profile | Source Interface | Source Subnet |
|---|---|---|---|---|
| □ | download-group1 | restrict downloads to 15 Mbps | ethernet1/3 | any |

## Quick Test

4) From the PC in download zone (figure 10), we have downloaded a file from the uploading.com site. The traffic is identified as uploading-download.

```
admin@PA5060-7> show session all
--------------------------------------------------------------------------------
ID          Application       State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                          Dst[Dport]/Zone                          (translated IP[Port])
--------------------------------------------------------------------------------
524916  uploading-download ACTIVE  FLOW      1.1.1.10[49519]/Download-Zone/6  (1.1.1.10[49519])
vsys3                         195.191.207.47[80]/Intra-Inside  (195.191.207.47[80])
524917  uploading-download ACTIVE  FLOW  NS   1.1.1.10[49519]/Intra-Outside/6 (10.2.133.196[30612])
vsys2                         195.191.207.47[80]/Internet        (195.191.207.47[80])
```

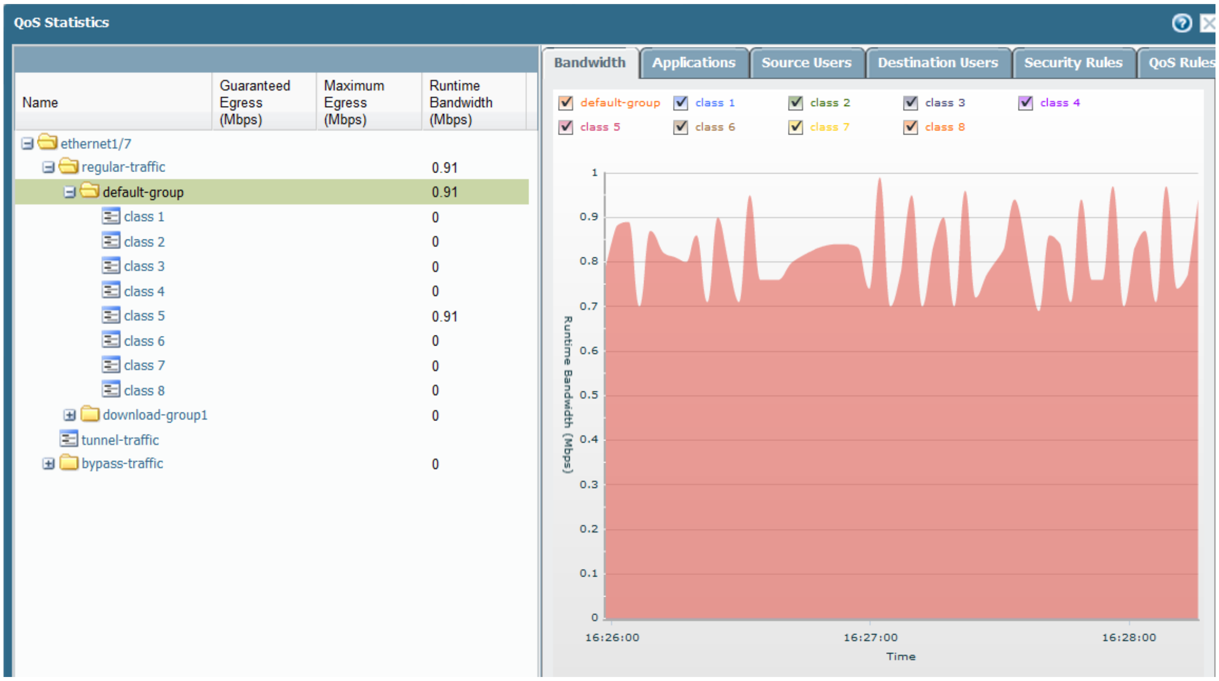
5) For this download traffic, QoS node download-group1 is matched. The QoS profile that is applied is "restrict downloads to 15 Mbps" and the QoS rule applied  is "download-1"

```
admin@PA5060-7> show session id 524916
Session         524916
        c2s flow:
                source:     1.1.1.10 [Download-Zone]
                dst:        195.191.207.47
                state:      ACTIVE        type:      FLOW
                qos node:   ethernet1/3, qos member  Qid 0
        s2c flow:
                source:     195.191.207.47 [Intra-Inside]
                dst:        1.1.1.10
                state:      ACTIVE        type:      FLOW
                qos node:   ethernet1/7.20, qos member download-group1 Qid 1
                match src interface:  ethernet1/3

       total byte count(c2s)          : 4005779
       total byte count(s2c)          : 199047400
       vsys                           : vsys3
       application                    : uploading-download
       rule                           : internet access for all zones
       ingress interface              : ethernet1/7.20
       egress interface               : ethernet1/3
       session QoS rule               : download-1 (class 5)
```

From the above details, the QoS egress interface is Ethernet 1/7.20 and QoS matching node is "download-group1 Qid 1". Don't get confused with the sessions egress interface, which is ethernet 1/3

6) To check the QoS statistics, go to Network tab > QoS on interface Ethernet 1/7, click statistics and you will see the runtime bandwidth and the class that this traffic is classified to in an easy to view graph.



QoS Statistics

| Name | Guaranteed Egress (Mbps) | Maximum Egress (Mbps) | Runtime Bandwidth (Mbps) |
|---|---|---|---|
| ⊟ ethernet1/7 | | | |
| ⊟ regular-traffic | | | 0.91 |
| ⊟ default-group | | | 0.91 |
| class 1 | | | 0 |
| class 2 | | | 0 |
| class 3 | | | 0 |
| class 4 | | | 0 |
| class 5 | | | 0.91 |
| class 6 | | | 0 |
| class 7 | | | 0 |
| class 8 | | | 0 |
| ⊞ download-group1 | | | 0 |
| tunnel-traffic | | | |
| ⊞ bypass-traffic | | | 0 |

7) You could check the statistics via the CLI as well.

```
admin@PA5060-7> show qos interface ethernet1/7 counter
QoS counter for interface ethernet1/7:
number of queued packets: 0
Parent  Qid node              base-bw  ldshare  max-bw  pass-pak  drop-pak  time-out vtime qlen qlmt
------------------------------------------------------------------------------------------------------
   2     0  default-group           1   16999   17000     0         0         0        0    0  150
   2     1  download-group1     10000    5000   15000     0         0         0        0    0  150
   5     2  regular-traffic     15000    2000   17000     0         0         0        0    0  150
   5     3  tunnel-traffic       4000    1000    5000     0         0         0        0    0  150
   5     4  bypass-traffic      19000    6000   25000     0         0         0        0    0  150
  -1     5  ethernet1/7         19000    6000   25000     0         0         0        0    0  150
  -1     5  ethernet1/7         19000    6000   25000     0         0         0        0    0  150
```

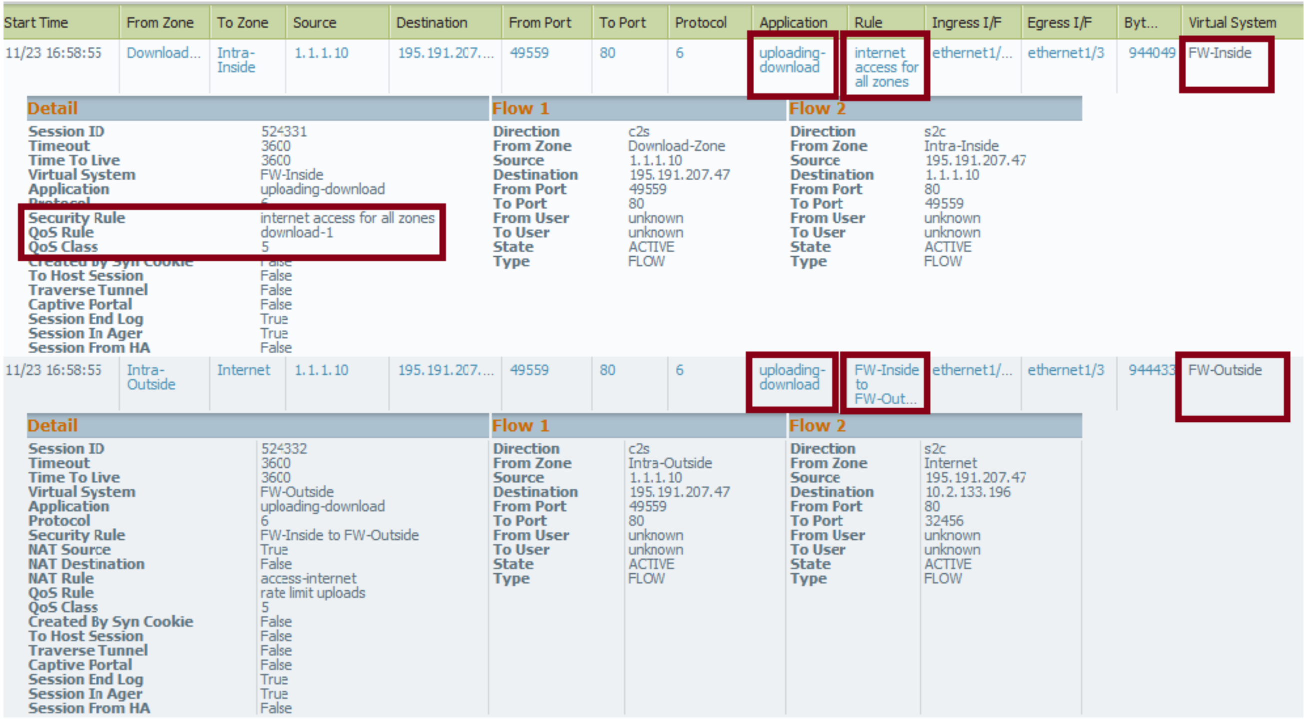
8) In the above display, you will notice that the pass-pak and drop-pak are zeroed out. The reason is that we are testing a PA-5060, where QoS is assisted by both H/W and S/W. Issue the following command for details:

```
admin@PA5060-7> show qos interface ethernet1/7 hw-counter

qid   name                pass bytes     WRED drop   policing drop
------------------------------------------------------------------
 0    default              232616228          0            0
 1    download-group1              0          0            0
-2    bypass                     932          0            0
```

This download session, internally creates two sessions since it has to pass two virtual systems (VSYS). One is from "Download-Zone" to "Intra-Inside" and the other is from "Intra-Outside" to "Internet". Sessions cannot span across virtual systems. For any inter-vsys traffic, PA device will create two sessions.

Here are the details from Monitor > session browser tab.



| Start Time | From Zone | To Zone | Source | Destination | From Port | To Port | Protocol | Application | Rule | Ingress I/F | Egress I/F | Byt... | Virtual System |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11/23 16:58:55 | Download... | Intra-Inside | 1.1.1.10 | 195.191.207.... | 49559 | 80 | 6 | uploading-download | internet access for all zones | ethernet1/... | ethernet1/3 | 944049 | FW-Inside |

| Detail | | Flow 1 | | Flow 2 | |
|---|---|---|---|---|---|
| Session ID | 524331 | Direction | c2s | Direction | s2c |
| Timeout | 3600 | From Zone | Download-Zone | From Zone | Intra-Inside |
| Time To Live | 3600 | Source | 1.1.1.10 | Source | 195.191.207.47 |
| Virtual System | FW-Inside | Destination | 195.191.207.47 | Destination | 1.1.1.10 |
| Application | uploading-download | From Port | 49559 | From Port | 80 |
| Protocol | 6 | To Port | 80 | To Port | 49559 |
| Security Rule | internet access for all zones | From User | unknown | From User | unknown |
| QoS Rule | download-1 | To User | unknown | To User | unknown |
| QoS Class | 5 | State | ACTIVE | State | ACTIVE |
| Created By Syn Cookie | False | Type | FLOW | Type | FLOW |
| To Host Session | False | | | | |
| Traverse Tunnel | False | | | | |
| Captive Portal | False | | | | |
| Session End Log | True | | | | |
| Session In Ager | True | | | | |
| Session From HA | False | | | | |

| Start Time | From Zone | To Zone | Source | Destination | From Port | To Port | Protocol | Application | Rule | Ingress I/F | Egress I/F | Byt... | Virtual System |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11/23 16:58:55 | Intra-Outside | Internet | 1.1.1.10 | 195.191.207.... | 49559 | 80 | 6 | uploading-download | FW-Inside to FW-Out... | ethernet1/... | ethernet1/3 | 944433 | FW-Outside |

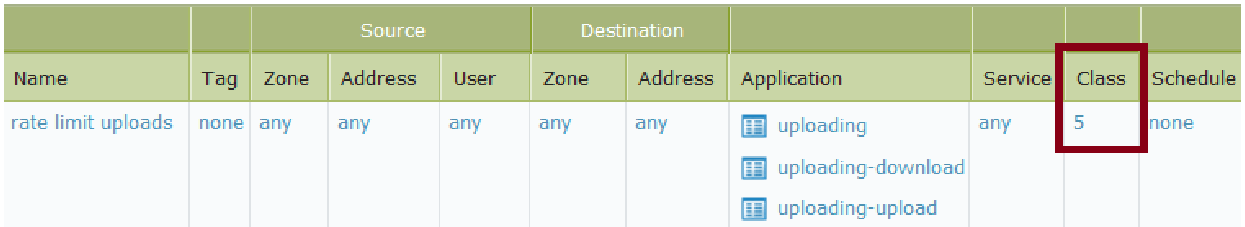
| Detail | | Flow 1 | | Flow 2 | |
|---|---|---|---|---|---|
| Session ID | 524332 | Direction | c2s | Direction | s2c |
| Timeout | 3600 | From Zone | Intra-Outside | From Zone | Internet |
| Time To Live | 3600 | Source | 1.1.1.10 | Source | 195.191.207.47 |
| Virtual System | FW-Outside | Destination | 195.191.207.47 | Destination | 10.2.133.196 |
| Application | uploading-download | From Port | 49559 | From Port | 80 |
| Protocol | 6 | To Port | 80 | To Port | 32456 |
| Security Rule | FW-Inside to FW-Outside | From User | unknown | From User | unknown |
| NAT Source | True | To User | unknown | To User | unknown |
| NAT Destination | False | State | ACTIVE | State | ACTIVE |
| NAT Rule | access-internet | Type | FLOW | Type | FLOW |
| QoS Rule | rate limit uploads | | | | |
| QoS Class | 5 | | | | |
| Created By Syn Cookie | False | | | | |
| To Host Session | False | | | | |
| Traverse Tunnel | False | | | | |
| Captive Portal | False | | | | |
| Session End Log | True | | | | |
| Session In Ager | True | | | | |
| Session From HA | False | | | | |

While the above example covered download traffic, we will now show the configuration details for the upload traffic.

**Configure the following for upload traffic in the FW-Outside (Vsys2) VSYS.**

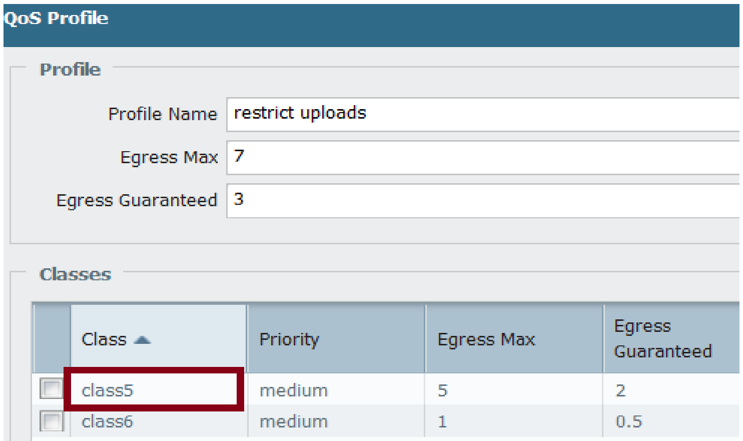
1) Create a QoS policy to identify upload traffic from uploading.com site and then assign it to a QoS class. In this example we classified traffic to class 5. The QoS policy is applied between Intra-Outside Zone (external) and zone Internet.

To create the QoS policy in VSYS "FW-Outside", go to the Policies tab > QoS screen and create a rule as follows:



| | | Source | | | Destination | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Name | Tag | Zone | Address | User | Zone | Address | Application | Service | Class | Schedule |
| rate limit uploads | none | any | any | any | any | any | uploading<br>uploading-download<br>uploading-upload | any | 5 | none |

5) Create a QoS profile. Go to Network tab > Network Profiles > QoS profiles screen. Create a new QoS profile. Define a QoS profile that will assign a maximum egress limit for class 5 "upload" traffic. The Egress Max for this profile is 7 Mbps. Your QoS profile will look something the following:


QoS Profile

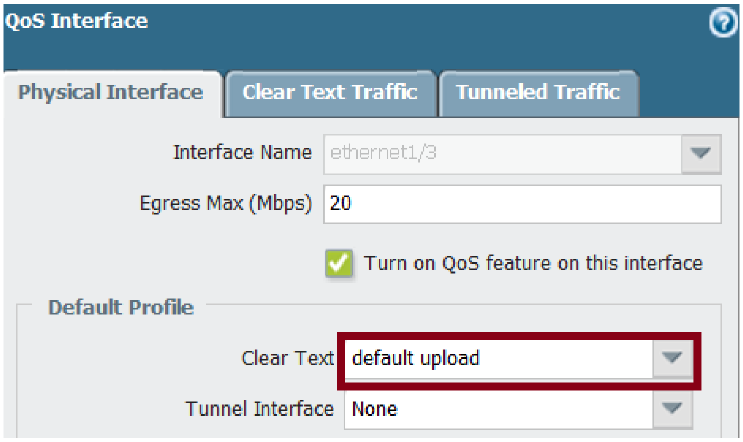
Profile

| | |
|---|---|
| Profile Name | restrict uploads |
| Egress Max | 7 |
| Egress Guaranteed | 3 |

Classes

| | Class | Priority | Egress Max | Egress Guaranteed |
|---|---|---|---|---|
| □ | class5 | medium | 5 | 2 |
| □ | class6 | medium | 1 | 0.5 |

6) Apply QoS on the interface e1/3 and set an egress Max bandwidth (20 Mbps in the example below). In the clear text traffic tab set Egress Guaranteed and Max bandwidths. Add a QoS node and apply the QoS profile with source interface as Ethernet 1/7.10. As described before for upload traffic, the egress interface is e1/3 and ingress interface is e1/7. The QoS profile used in this example is "restrict uploads".


QoS Interface

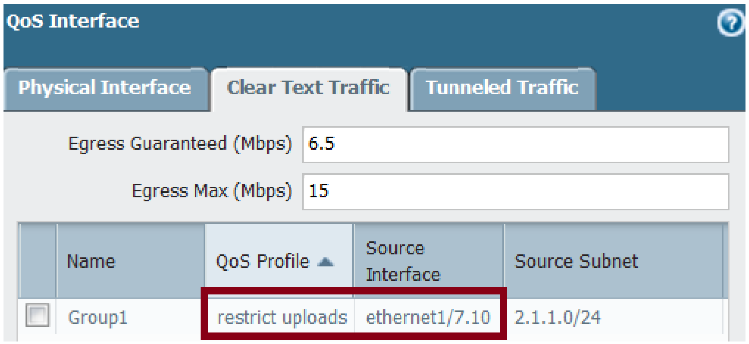
| | |
|---|---|
| Interface Name | ethernet1/3 |
| Egress Max (Mbps) | 20 |

☑ Turn on QoS feature on this interface

Default Profile

| | |
|---|---|
| Clear Text | default upload |
| Tunnel Interface | None |

7) The egress Max of 7 Mbps is set on the profile "restrict uploads"(above in item 5) is less than egress Max of 15 Mbps of clear Text traffic(see below), which is less than the Egress Max of the interface, which is 20 Mbps( see just above in item 6).


QoS Interface

| | |
|---|---|
| Egress Guaranteed (Mbps) | 6.5 |
| Egress Max (Mbps) | 15 |

| | Name | QoS Profile | Source Interface | Source Subnet |
|---|---|---|---|---|
| □ | Group1 | restrict uploads | ethernet1/7.10 | 2.1.1.0/24 |

## Quick Test

1) From the PC in upload zone (figure 10), we have downloaded a file to uploading.com site. The traffic is identified as uploading-upload.

```
 admin@PA5060-7> show session all
--------------------------------------------------------------------------------
ID     Application    State   Type Flag  Src[Sport]/Zone/Proto (translated IP[Port])
Vsys                                      Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------------------------
524335 uploading-upload  ACTIVE  FLOW     2.1.1.10[52817]/Upload-Zone/6    (2.1.1.10[52817])
vsys3                    195.191.207.49[80]/Intra-Inside  (195.191.207.49[80])

524336 uploading-upload  ACTIVE  FLOW  NS 2.1.1.10[52817]/Intra-Outside/6 (10.2.133.196[44417])
vsys2                    195.191.207.49[80]/Internet  (195.191.207.49[80])
```

2) For this upload traffic, QoS node Group1 is matched. The QoS profile that is applied is “restrict uploads” and the QoS rule applied  is “rate limit uploads”

   Here are a few details of the QoS rule that matched

```
        application                : uploading-upload
        rule                         : FW-Inside to FW-Outside
        nat-rule                     : access-internet(vsys2)

        ingress interface           : ethernet1/7.10
        egress interface            : ethernet1/3
        session QoS rule            : rate limit uploads (class 5)
```

3) To check the QoS statistics, go to Network tab > QoS on interface Ethernet 1/7, click statistics, you will see the runtime bandwidth and the class the traffic is classified to in a nice graph. Alternatively you could issue the following commands on CLI to view the QoS statistics:
   a. show qos interface ethernet1/3 counter
   b. show qos interface ethernet1/3 hw-counter

## Platform specific data

The maximum number of ports and subnets that you can configure on a Palo Alto Networks firewall varies by platform. The following table lists the platform specific capacities for QoS elements. This information could change with time and release. Please refer to www.paloaltonetworks.com for the latest platform information.

| Model | PA-5060 | PA-5050 | PA-5020 | PA-4060 | PA-4050 /PA-4020 | PA-2000 Series | PA-500 | PA-200 |
|---|---|---|---|---|---|---|---|---|
| Number of QoS policies | 4000 | 2000 | 1000 | 2000 | 2000 | 1000 | 100 | 100 |
| Physical interfaces | 12 | 12 | 12 | 6 | 12 | 6 | 6 | 4 |
| Clear text nodes per interface | 64 | 64 | 32 | 64 | 32 | 32 | 32 | 32 |
| DSCP marking per policy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

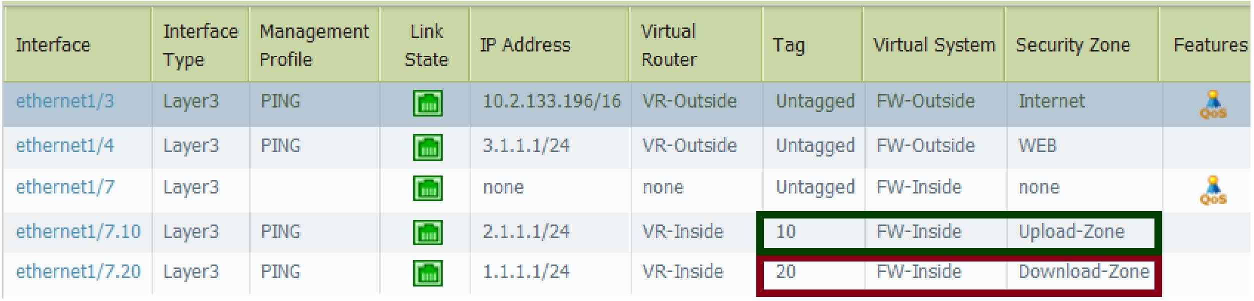
## Things to Remember

- Traffic that does not match a QoS policy is assigned a default class 4. Keep this in mind when configuring guaranteed bandwidth and priority for this class.
- The guaranteed and maximum egress settings defined for the classes must not exceed the guaranteed and maximum egress settings defined for the QoS profile itself.

# Appendix

To implement QoS in the virtualized firewall design on a Palo Alto Networks next generation firewall, you will need to create virtual systems and associate the appropriate interfaces, virtual router, and security zones with each VSYS. Following are the details.

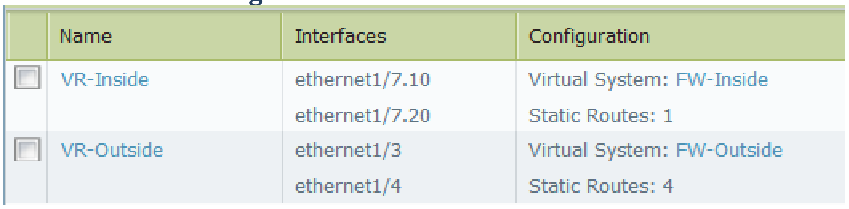
### Interface Configuration



| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router | Tag | Virtual System | Security Zone | Features |
|---|---|---|---|---|---|---|---|---|---|
| ethernet1/3 | Layer3 | PING | 🟩 | 10.2.133.196/16 | VR-Outside | Untagged | FW-Outside | Internet | QoS |
| ethernet1/4 | Layer3 | PING | 🟩 | 3.1.1.1/24 | VR-Outside | Untagged | FW-Outside | WEB | |
| ethernet1/7 | Layer3 | | 🟩 | none | none | Untagged | FW-Inside | none | QoS |
| ethernet1/7.10 | Layer3 | PING | 🟩 | 2.1.1.1/24 | VR-Inside | 10 | FW-Inside | Upload-Zone | |
| ethernet1/7.20 | Layer3 | PING | 🟩 | 1.1.1.1/24 | VR-Inside | 20 | FW-Inside | Download-Zone | |

Each interface belongs to the appropriate VR, Zone, and Virtual System.

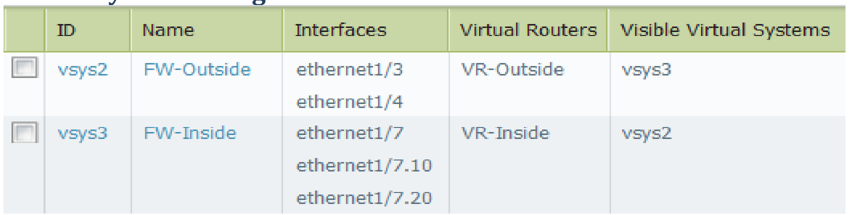
### Virtual Router Configuration



| | Name | Interfaces | Configuration |
|---|---|---|---|
| □ | VR-Inside | ethernet1/7.10<br>ethernet1/7.20 | Virtual System: FW-Inside<br>Static Routes: 1 |
| □ | VR-Outside | ethernet1/3<br>ethernet1/4 | Virtual System: FW-Outside<br>Static Routes: 4 |

Each Interface belongs to a VR that is appropriate for that VSYS. In our example, Ethernet 1/7.10 and Ethernet 1/7.20 are in VR-Inside and Ethernet 1/3 and 1/4 are in VR-Outside. VR-Inside belongs to Virtual system FW-Inside and VR-Outside belongs to Virtual System FW-Outside. The following shows the virtual system configuration:

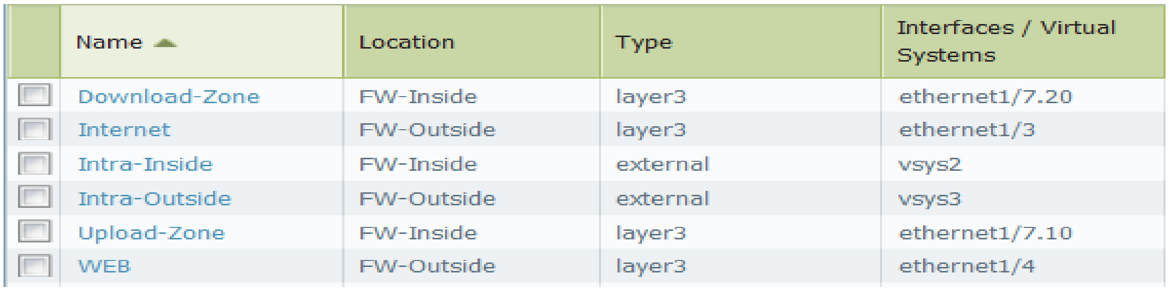
### Virtual System Configuration



| | ID | Name | Interfaces | Virtual Routers | Visible Virtual Systems |
|---|---|---|---|---|---|
| □ | vsys2 | FW-Outside | ethernet1/3<br>ethernet1/4 | VR-Outside | vsys3 |
| □ | vsys3 | FW-Inside | ethernet1/7<br>ethernet1/7.10<br>ethernet1/7.20 | VR-Inside | vsys2 |

The virtual systems in our configuration (vsys2 and vsys3) have the appropriate interfaces and virtual routers associated. In order for them to communicate properly with each other, we also need to ensure that they can communicate with each other. You can enable this in each of the VSYS configuration (by clicking on the VSYS ID) and also see it in the last field of the VSYS configuration above.

### Zone Configuration



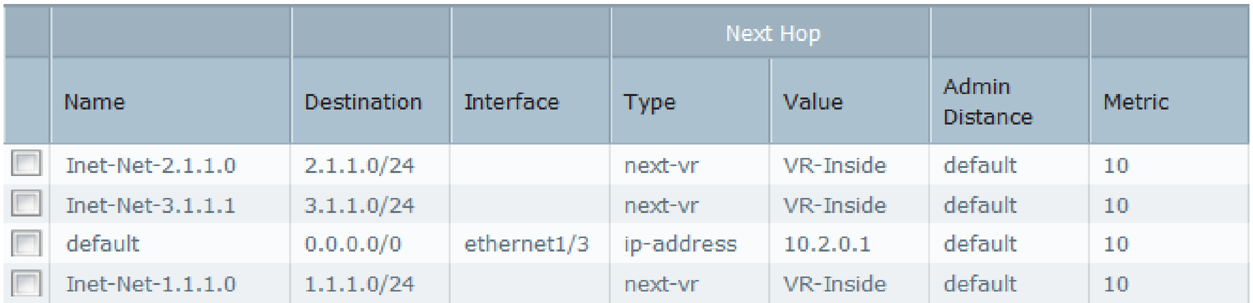
| | Name | Location | Type | Interfaces / Virtual Systems |
|---|---|---|---|---|
| □ | Download-Zone | FW-Inside | layer3 | ethernet1/7.20 |
| □ | Internet | FW-Outside | layer3 | ethernet1/3 |
| □ | Intra-Inside | FW-Inside | external | vsys2 |
| □ | Intra-Outside | FW-Outside | external | vsys3 |
| □ | Upload-Zone | FW-Inside | layer3 | ethernet1/7.10 |
| □ | WEB | FW-Outside | layer3 | ethernet1/4 |

Each of the layer 3 zones (Internet, Web, Download-zone, upload-zone) is associated with interfaces, which are then associated with the appropriate VSYS. There are two special zones that need to be created and they are of type external and belong directly to a VSYS rather than an interface. In our configuration, there are two external zones, Intra-Inside and Intra-Outside; one belongs to VSYS2 and the other toVSYS3. These external zones will enable you to write security policy to control communications between two virtual systems.

## Route Configuration (for Inter-VSYS communication)

Routes for communication between the VRs need to be added to allow traffic to be forwarded across the virtual systems. The configuration of the VRs for our example design from above follows:

### Virtual Router – VR-Outside configuration

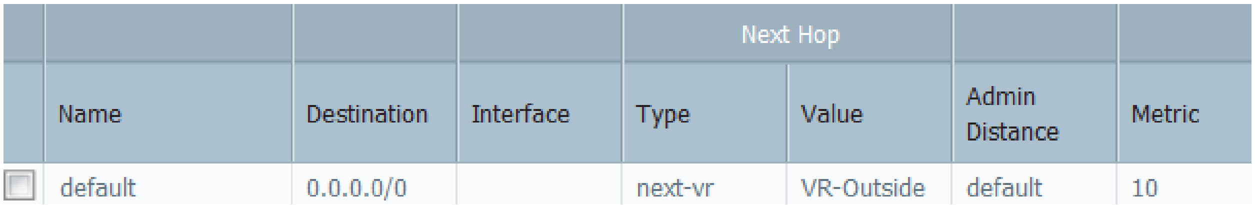


| | | | | Next Hop | | | |
|---|---|---|---|---|---|---|---|
| | Name | Destination | Interface | Type | Value | Admin Distance | Metric |
| □ | Inet-Net-2.1.1.0 | 2.1.1.0/24 | | next-vr | VR-Inside | default | 10 |
| □ | Inet-Net-3.1.1.1 | 3.1.1.0/24 | | next-vr | VR-Inside | default | 10 |
| □ | default | 0.0.0.0/0 | ethernet1/3 | ip-address | 10.2.0.1 | default | 10 |
| □ | Inet-Net-1.1.1.0 | 1.1.1.0/24 | | next-vr | VR-Inside | default | 10 |

In this virtual router configuration, we have the default route pointing to the Internet gateway of 10.2.0.1 out our Interface Ethernet1/3 on VSYS2 (FW-Outside). The routes for the internal subnets of 1.1.1.0/24 (download-zone), 2.1.1.0/24 (upload-zone) have next hops of the virtual router that is associated with our FW-Inside VSYS (VSYS3), which is VR-Inside in our example.

This allows the packet to be forwarded to the other VR through the external zones previously defined. The security policy still needs to be configured to allow this forwarding to take place from a policy perspective. The local segments are also included in our forwarding table based on the interfaces being selected above.

### Virtual Router – VR-Inside configuration

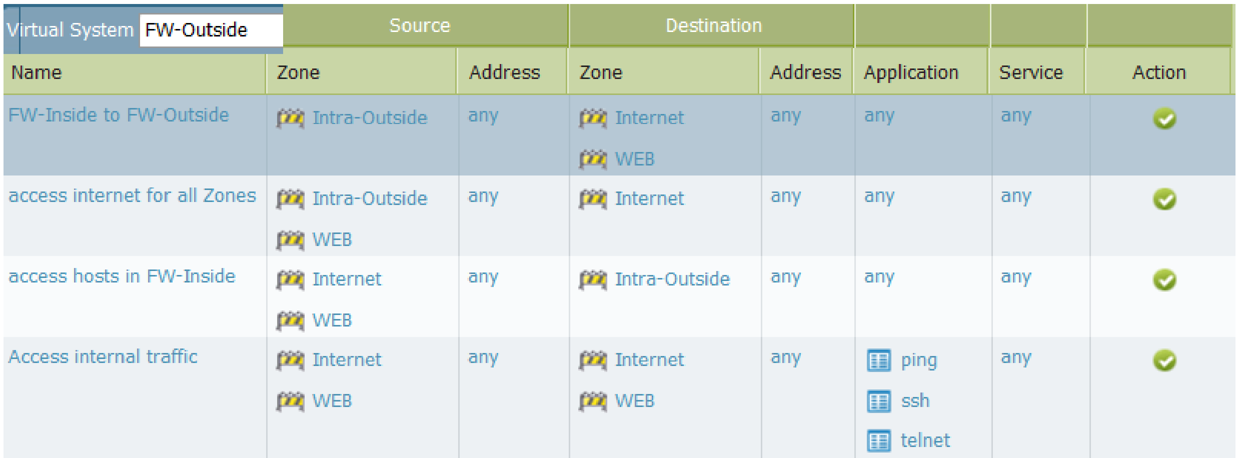


| | | | | Next Hop | | | |
|---|---|---|---|---|---|---|---|
| | Name | Destination | Interface | Type | Value | Admin Distance | Metric |
| □ | default | 0.0.0.0/0 | | next-vr | VR-Outside | default | 10 |

We only need a default route that point to the next hop of VR-Inside to get to all of the networks that are in the design. If more internal networks existed internally, they would need to be added to this virtual router configuration with the next hop being out of the interface Ethernet 1/7 with a next hope type of IP and the address of the internal router that supports the additional subnets.

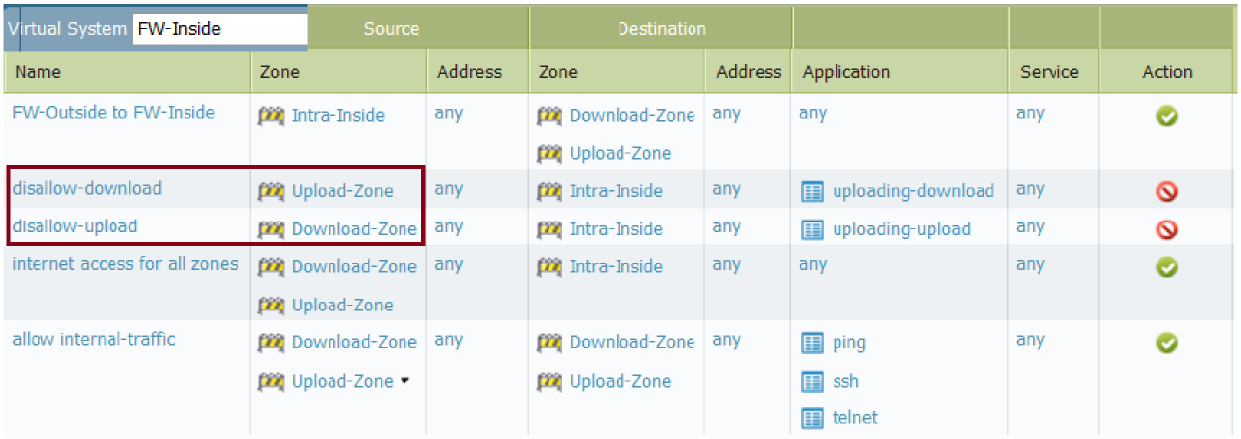
## Security Policies

Apart from setting up the routing for Intra-VSYS communications, we also need to setup the appropriate security policy rules to control the desired access through the FW-Outside (VSYS2) and FW-Inside (VSYS3) VSYS.



| Virtual System FW-Outside | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| Name | Zone | Address | Zone | Address | Application | Service | Action |
| FW-Inside to FW-Outside | Intra-Outside | any | Internet<br>WEB | any | any | any | ✓ |
| access internet for all Zones | Intra-Outside<br>WEB | any | Internet | any | any | any | ✓ |
| access hosts in FW-Inside | Internet<br>WEB | any | Intra-Outside | any | any | any | ✓ |
| Access internal traffic | Internet<br>WEB | any | Internet<br>WEB | any | ping<br>ssh<br>telnet | any | ✓ |

We have restricted uploading from download-zone and downloading from upload-zone



| Virtual System FW-Inside | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| Name | Zone | Address | Zone | Address | Application | Service | Action |
| FW-Outside to FW-Inside | Intra-Inside | any | Download-Zone<br>Upload-Zone | any | any | any | ✓ |
| disallow-download | Upload-Zone | any | Intra-Inside | any | uploading-download | any | ⊘ |
| disallow-upload | Download-Zone | any | Intra-Inside | any | uploading-upload | any | ⊘ |
| internet access for all zones | Download-Zone<br>Upload-Zone | any | Intra-Inside | any | any | any | ✓ |
| allow internal-traffic | Download-Zone<br>Upload-Zone | any | Download-Zone<br>Upload-Zone | any | ping<br>ssh<br>telnet | any | ✓ |